MARKETSANDMARKETS™

AI SECURITY OPERATIONS CENTER (SOC) MARKET

GLOBAL FORECAST TO 2031

BY SOFTWARE PLATFORMS (AI-NATIVE SOC, AI SOC AGENTS, SECURITY DATA PLATFORMS), SERVICES (AI-AUGMENTED MDR, AI SOC-AS-A-SERVICE, INCIDENT RESPONSE & FORENSICS), APPLICATION, VERTICAL

www.marketsandmarkets.com

MarketsandMarkets™ is the world's largest revenue impact company, serving over 7500 customers. 80% of top 2000 companies globally rely on us for identifying new high growth and niche revenue opportunities. In the face of constant technology innovation and market disruption, we help organizations plan and operationalize their future revenue mix decisions by identifying over 30,000 high growth opportunities ranging from $1B to $500B across 90+ industry trends and markets. Organizations choose MarketsandMarkets™ to stay ahead of the curve and accelerate their revenue decisions and implementations by 6 – 12 months, giving them a unique, first-mover advantage. Our revenue impact methodology provides quantified and actionable insights on converged, granular and connected market eco-systems that result from disruptive technologies and high-growth markets. We provide an extended lens on not only what will impact our client's revenue but also what will impact their clients' revenues, continually uncovering latent opportunities.

We work across all major B2B industries with C-level executives in functions such as Strategy, Marketing, Sales, R&D, Product, and M&A. MarketsandMarkets™ brings exclusive high-growth markets intelligence generated by over 850 SMEs and analysts along with its proprietary Revenue Impact platform (KnowledgeStore).

Copyright © 2026 MarketsandMarkets™
All Rights Reserved. This document contains highly confidential information and is the sole property of MarketsandMarkets™. No part of it shall be circulated, copied, quoted, or otherwise reproduced without the prior written approval of MarketsandMarkets™.

TABLE OF CONTENTS

1 INTRODUCTION 37

1.1 STUDY OBJECTIVES 37
1.2 MARKET DEFINITION 37
1.3 STUDY SCOPE AND SEGMENTATION 37
1.3.1 MARKET SEGMMENTATION & REGION COVERAGE 38
1.3.2 INCLUSIONS AND EXCLUSIONS 39
1.3.3 YEARS CONSIDERED 43
1.4 CURRENCY CONSIDERED 43
1.5 STAKEHOLDERS 44

2 EXECUTIVE SUMMARY 45

2.1 MARKET HIGHLIGHTS AND KEY INSIGHTS 45
2.2 KEY MARKET PARTICIPANTS: MAPPING OF STRATEGIC DEVELOPMENTS 47
2.3 DISRUPTIVE TRENDS SHAPING MARKET 48
2.4 HIGH-GROWTH SEGMENTS & EMERGING FRONTIERS 49
2.5 SNAPSHOT: GLOBAL MARKET SIZE, GROWTH RATE, AND FORECAST 51

3 PREMIUM INSIGHTS 52

3.1 ATTRACTIVE OPPORTUNITIES FOR PLAYERS IN AI SOC MARKET 52
3.2 AI SOC MARKET, BY OFFERING 53
3.3 AI SOC MARKET, BY SOFTWARE PLATFORM 53
3.4 AI SOC MARKET, BY SERVICE 54
3.5 AI SOC MARKET, BY ORGANIZATION SIZE 54
3.6 AI SOC MARKET, BY APPLICATION 55
3.7 AI SOC MARKET, BY VERTICAL 55
3.8 AI SOC MARKET, BY REGION 56

4 MARKET OVERVIEW 57

4.1 INTRODUCTION 57
4.2 MARKET DYNAMICS 57
4.2.1 DRIVERS 58
4.2.1.1 Rising AI-powered cyber threats 58
4.2.1.2 Increasing adoption of cloud, hybrid, and identity-centric infrastructures 59
4.2.1.3 Expansion of autonomous AI agents across enterprise environments 59
4.2.1.4 Growing shortage of skilled cybersecurity professionals 60
4.2.2 RESTRAINTS 60
4.2.2.1 Limited trust in autonomous AI decision-making 60
4.2.2.2 Evolving AI governance and regulatory landscape 60

JULY 2026 © MarketsandMarkets™

4.2.3 OPPORTUNITIES 61
4.2.3.1 AI SOC adoption among small and medium-sized enterprises (SMEs) 61
4.2.3.2 AI security for agentic and generative AI environments 61
4.2.3.3 Unified AI-native security platforms 62
4.2.3.4 AI SOC-as-a-service and managed AI security operations 62
4.2.4 CHALLENGES 63
4.2.4.1 Ensuring accuracy and reliability of AI-generated security decisions 63
4.2.4.2 Addressing AI model security and adversarial threats 63
4.3 UNMET NEEDS AND WHITE SPACES 63
4.4 INTERCONNECTED MARKETS AND CROSS-SECTOR OPPORTUNITIES 65
4.4.1 INTERCONNECTED MARKETS 65
4.4.2 CROSS-SECTOR OPPORTUNITIES 66
4.5 STRATEGIC MOVES BY TIER -1/2/3 PLAYERS 66
4.5.1 CROSS-TIER STRATEGIC PATTERNS 67
4.5.2 STRATEGIC TRENDS 68
4.5.2.1 Rise of Agentic AI in security operations 68
4.5.2.2 Human-AI collaborative security 69
4.5.2.3 AI-Powered Continuous Threat Exposure Management (CTEM) 69
5 INDUSTRY TRENDS 70
5.1 PORTER'S FIVE FORCES ANALYSIS 70
5.1.1 THREAT OF NEW ENTRANTS 71
5.1.2 BARGAINING POWER OF SUPPLIERS 71
5.1.3 BARGAINING POWER OF BUYERS 72
5.1.4 THREAT OF SUBSTITUTES 72
5.1.5 INTENSITY OF COMPETITIVE RIVALRY 72
5.2 MACROECONOMIC INDICATORS 73
5.2.1 INTRODUCTION 73
5.2.2 GDP TRENDS AND FORECAST 73
5.2.3 TRENDS IN GLOBAL ICT INDUSTRY 75
5.2.4 TRENDS IN GLOBAL AI SOC INDUSTRY 76
5.3 VALUE CHAIN ANALYSIS 76
5.3.1 AI & SECURITY INFRASTRUCTURE 77
5.3.2 CORE SECURITY DATA & DETECTION PLATFORMS 78
5.3.3 AI SOC PLATFORM & AGENTIC AI PROVIDERS 78
5.3.4 AUTOMATION, ORCHESTRATION & INTEGRATION PARTNERS 78
5.3.5 MANAGED AI SOC SERVICES (CROSS-STAGE LAYER) 78
5.3.6 END USER GROUPS 78
5.4 ECOSYSTEM ANALYSIS 79

JULY 2026 © MarketsandMarkets™

5.5 PRICING ANALYSIS 81
5.5.1 AVERAGE ANNUAL SELLING PRICE OF KEY AI SOC VENDORS FOR A 500-ENDPOINT DEPLOYMENT 82
5.5.2 INDICATIVE PRICING ANALYSIS FOR KEY PLAYERS 84
5.6 KEY CONFERENCES & EVENTS, 2026 85
5.7 TRENDS AND DISRUPTIONS IMPACTING CUSTOMER BUSINESS 85
5.8 INVESTMENT AND FUNDING SCENARIO 87
5.9 CASE STUDY ANALYSIS 87
5.9.1 KEY ENTERPRISE USE CASES OF AI SOC 88
5.9.1.1 AI-Driven Phishing and Business Email Compromise (BEC) Response 88
5.9.1.2 Autonomous Alert Triage and Threat Investigation 88
5.9.1.3 Identity and Insider Threat Detection 88
5.9.1.4 Cloud Security Investigation and Response 89
5.9.1.5 AI-driven Data Loss Prevention (DLP) and Sensitive Data Protection 89
5.9.2 CASE STUDIES 90
5.9.2.1 St. Luke's University Health Network Enhances Healthcare Cyber Defense with Microsoft Security Copilot and AI-Driven SOC Operations 90
5.9.2.2 Mondelēz International Modernizes Global Security Operations Through CrowdStrike's AI-Native Falcon Platform 90
5.9.2.3 Fortune 500 Oil & Gas Company Transforms Legacy SOC into an AI-Driven Security Operations Center with Palo Alto Networks Cortex XSIAM 91
5.9.2.4 US Financial Services Firm Unifies Enterprise Security Operations with Stellar Cyber's AI-Native SecOps Platform 91
5.9.2.5 CarbonHelix Accelerates MSSP Growth Through Intezer's AI-Powered Autonomous Security Operations Center 92
5.10 IMPACT OF 2025 US TARIFFS – AI SOC MARKET 92
5.10.1 INTRODUCTION 92
5.10.2 KEY TARIFF RATES 94
5.10.3 PRICE IMPACT ANALYSIS 95
5.10.4 IMPACT ON COUNTRY/REGION 96
5.10.4.1 North America 96
5.10.4.2 Europe 97
5.10.4.3 Asia Pacific 99
5.10.5 IMPACT ON END-USE INDUSTRIES 100

6 TECHNOLOGICAL ADVANCEMENTS, AI-DRIVEN IMPACT, PATENTS, INNOVATIONS, AND FUTURE APPLICATIONS 102

6.1 TECHNOLOGY ANALYSIS 102
6.1.1 KEY EMERGING TECHNOLOGIES 102
6.1.1.1 Agentic AI for Autonomous Security Operations 102
6.1.1.2 AI-Powered Continuous Threat Exposure Management (CTEM) 103
6.1.1.3 Large Language Model (LLM)-Driven Security Copilots 103

JULY 2026 © MarketsandMarkets™

6.1.1.4 AI-Native Extended Detection and Response (XDR) 103
6.1.1.5 Multi-Agent Security Orchestration and Autonomous Incident Response 104
6.1.2 COMPLEMENTARY TECHNOLOGIES 104
6.1.2.1 Cloud-Native Application Protection Platform (CNAPP) 104
6.1.2.2 Identity Threat Detection and Response (ITDR) 105
6.1.2.3 Threat Intelligence Platforms (TIPs) 105
6.1.3 ADJACENT TECHNOLOGIES 105
6.1.3.1 Cyber Asset Attack Surface Management (CAASM) 105
6.1.3.2 Breach and Attack Simulation (BAS) 106
6.1.3.3 Secure Access Service Edge (SASE) 106
6.2 TECHNOLOGY/PRODUCT ROADMAP 107
6.2.1 SHORT-TERM (2026–2027) | FOUNDATION & EARLY COMMERCIALIZATION 107
6.2.2 MID-TERM (2027–2030) SCALING, AUTONOMY & ECOSYSTEM EXPANSION 108
6.2.3 LONG-TERM (2030–2035+) | AUTONOMOUS, PREDICTIVE & SELF-OPTIMIZING SECURITY OPERATIONS 109
6.3 PATENT ANALYSIS 110
6.4 FUTURE APPLICATIONS 112
6.4.1 PREDICTIVE CYBER DEFENSE AND CYBER RESILIENCE 113
6.4.2 AI-NATIVE REGULATORY COMPLIANCE AND CONTINUOUS AUDIT OPERATIONS 113
6.4.3 CYBER FUSION CENTERS FOR ENTERPRISE RISK INTELLIGENCE 113
6.4.4 AUTONOMOUS THIRD-PARTY AND SUPPLY CHAIN RISK MONITORING 114
6.4.5 EXECUTIVE CYBER DECISION INTELLIGENCE AND BUSINESS RISK FORECASTING 114
6.5 IMPACT OF AI/GEN AI ON AI SOC MARKET 114
6.5.1 BEST PRACTICES IN AI SOC MARKET 115
6.5.2 CASE STUDIES OF AI IMPLEMENTATION IN AI SOC MARKET 116
6.5.3 INTERCONNECTED ADJACENT ECOSYSTEM AND IMPACT ON MARKET PLAYERS 117
6.5.4 CLIENTS' READINESS TO ADOPT GENERATIVE AI IN AI SOC MARKET 118
6.6 SUCCESS STORIES AND REAL-WORLD APPLICATIONS 118
6.6.1 PALO ALTO NETWORKS: IMAGINATION TECHNOLOGIES – AI-POWERED SOC MODERNIZATION 119
6.6.2 MICROSOFT: CITY OF JOHANNESBURG – AI-ENABLED SECURITY OPERATIONS 119
7 REGULATORY LANDSCAPE 120
7.1 REGIONAL REGULATIONS AND COMPLIANCE 120
7.1.1 REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS 121
7.1.2 INDUSTRY STANDARDS 127

JULY 2026 © MarketsandMarkets™

8 CONSUMER LANDSCAPE & BUYER BEHAVIOR 130
8.1 DECISION-MAKING PROCESS 130
8.2 KEY STAKEHOLDERS & BUYING CRITERIA 132
8.2.1 KEY STAKEHOLDERS IN BUYING PROCESS 132
8.2.2 BUYING CRITERIA 132
8.3 ADOPTION BARRIERS & INTERNAL CHALLENGES 133
8.4 UNMET NEEDS IN VARIOUS END-USE INDUSTRIES 135
9 AI SOC MARKET, BY OFFERING 137
9.1 INTRODUCTION 138
9.1.1 OFFERING: AI SOC MARKET DRIVERS 138
9.2 SOFTWARE PLATFORMS 140
9.2.1 RISING ENTERPRISE DEMAND FOR UNIFIED AI SECURITY PLATFORMS TO DRIVE SOFTWARE PLATFORM ADOPTION 140
9.2.2 AI-ENABLED DETECTION AND ANALYTICS PLATFORMS 143
9.2.2.1 AI-driven threat detection and contextual security analytics are redefining modern security operations 143
9.2.3 AI-ORCHESTRATED RESPONSE AND AUTOMATION PLATFORMS 144
9.2.3.1 Intelligent security orchestration and agentic automation are transforming incident response operations 144
9.2.4 AI-NATIVE SOC PLATFORMS 145
9.2.4.1 Unified AI-native security operations platforms are driving the transition toward autonomous cyber defense 145
9.2.5 AI SOC AGENT SOLUTIONS 147
9.2.5.1 Agentic AI is enabling autonomous security operations through intelligent AI SOC agents 147
9.2.6 SECURITY DATA PLATFORMS 148
9.2.6.1 Unified security data foundations are enabling AI-ready security operations at enterprise scale 148
9.2.7 THREAT INTELLIGENCE PLATFORMS 149
9.2.7.1 Real-time threat intelligence to enable proactive and context-aware AI security operations 149
9.2.8 AI GOVERNANCE, RISK, AND COMPLIANCE SOLUTIONS 150
9.2.8.1 Responsible AI governance and continuous compliance are emerging as core components of AI-native security operations 150
9.3 SERVICES 152
9.3.1 AI-DRIVEN MANAGED SECURITY SERVICES ARE ENABLING ENTERPRISES TO SCALE SECURITY OPERATIONS WITHOUT EXPANDING INTERNAL SOC TEAMS 152
9.3.2 AI-AUGMENTED MANAGED DETECTION AND RESPONSE (MDR) 154
9.3.2.1 AI-augmented MDR services are enabling continuous threat defense through expert-led and AI-powered security operations 154
9.3.3 AI SOC-AS-A-SERVICE (SOCAAS) 156
9.3.3.1 Cloud-delivered AI security operations are expanding access to enterprise-grade cyber defense 156

JULY 2026 © MarketsandMarkets™

9.3.4 INCIDENT RESPONSE AND FORENSICS SERVICES 157
9.3.4.1 AI-powered incident response and digital forensics are accelerating cyber recovery and operational resilience 157
9.3.5 THREAT INTELLIGENCE AND ADVISORY SERVICES 158
9.3.5.1 Intelligence-led cyber advisory services are strengthening proactive risk management in AI-enabled security operations 158

10 AI SOC MARKET, BY ORGANIZATION SIZE 160
10.1 INTRODUCTION 161
10.1.1 ORGANIZATION SIZE: AI SOC MARKET DRIVERS 161
10.2 LARGE ENTERPRISES 163
10.2.1 COMPLEX DIGITAL ECOSYSTEMS AND LARGE-SCALE SECURITY OPERATIONS ARE ACCELERATING AI SOC ADOPTION ACROSS LARGE ENTERPRISES 163
10.3 SMES 164
10.3.1 CLOUD-NATIVE AI SOC SERVICES ARE ENABLING SMES TO ACCESS ENTERPRISE-GRADE CYBERSECURITY CAPABILITIES 164

11 AI SOC MARKET, BY APPLICATION 166
11.1 INTRODUCTION 167
11.1.1 APPLICATION: AI SOC MARKET DRIVERS 168
11.2 THREAT DETECTION AND MONITORING 169
11.2.1 SHIFT FROM ALERT-CENTRIC SECURITY TO CONTINUOUS RISK OBSERVABILITY IS ACCELERATING AI-DRIVEN THREAT DETECTION 169
11.3 ALERT TRIAGE AND PRIORITIZATION 170
11.3.1 BUSINESS-CONTEXT–DRIVEN ALERT PRIORITIZATION IS IMPROVING SOC DECISION QUALITY AND REDUCING ANALYST FATIGUE 170
11.4 INCIDENT INVESTIGATION AND ANALYSIS 172
11.4.1 AI-ASSISTED INVESTIGATIONS ARE SHIFTING SECURITY OPERATIONS FROM EVIDENCE COLLECTION TO RAPID DECISION-MAKING 172
11.5 THREAT HUNTING 173
11.5.1 PROACTIVE ADVERSARY HUNTING IS SHIFTING SECURITY OPERATIONS FROM REACTIVE DEFENSE TO CONTINUOUS CYBER RESILIENCE 173
11.6 INCIDENT RESPONSE AND REMEDIATION 174
11.6.1 RAPID BUSINESS RECOVERY IS DRIVING AI-ENABLED INCIDENT RESPONSE AND REMEDIATION CAPABILITIES 174
11.7 INSIDER THREAT DETECTION 176
11.7.1 HUMAN RISK INTELLIGENCE IS EMERGING AS A STRATEGIC APPLICATION OF AI SOC PLATFORMS 176
11.8 CLOUD SECURITY MONITORING 177
11.8.1 CONTINUOUS MULTICLOUD VISIBILITY IS EMERGING AS A STRATEGIC REQUIREMENT FOR AI-DRIVEN SECURITY OPERATIONS 177
11.9 IDENTITY AND ACCESS MONITORING 178
11.9.1 CONTINUOUS IDENTITY VISIBILITY IS BECOMING CENTRAL TO AI-DRIVEN SECURITY OPERATIONS 178

JULY 2026 © MarketsandMarkets™

11.10 COMPLIANCE MONITORING AND REPORTING 180
11.10.1 CONTINUOUS COMPLIANCE ASSURANCE IS BECOMING A STRATEGIC FUNCTION OF AI-POWERED SECURITY OPERATIONS 180
11.11 SECURITY ANALYTICS AND VISUALIZATION 181
11.11.1 VISUAL SECURITY INTELLIGENCE IS ENABLING FASTER CYBER RISK DECISIONS ACROSS MODERN SECURITY OPERATIONS 181

12 AI SOC MARKET, BY VERTICAL 183
12.1 INTRODUCTION 184
12.1.1 VERTICAL: AI SOC MARKET DRIVERS 185
12.2 BFSI 187
12.2.1 RISING AI-ENABLED FINANCIAL FRAUD AND REGULATORY REQUIREMENTS ARE ACCELERATING AI SOC ADOPTION ACROSS THE BFSI SECTOR 187
12.3 GOVERNMENT AND DEFENSE 188
12.3.1 NATIONAL CYBER RESILIENCE INITIATIVES AND DEFENSE AI MODERNIZATION ARE ACCELERATING AI SOC ADOPTION 188
12.4 HEALTHCARE & LIFE SCIENCES 189
12.4.1 EXPANDING DIGITAL HEALTH ECOSYSTEMS AND PROTECTION OF SENSITIVE PATIENT DATA ARE DRIVING AI SOC ADOPTION 189
12.5 IT & TELECOMMUNICATIONS 191
12.5.1 EXPANDING AI-NATIVE NETWORKS AND HYPERSCALE DIGITAL INFRASTRUCTURES ARE ACCELERATING AI SOC DEPLOYMENTS ACROSS THE IT AND TELECOMMUNICATIONS SECTOR 191
12.6 MANUFACTURING 192
12.6.1 INDUSTRY 4.0 AND IT-OT CONVERGENCE ARE ACCELERATING AI SOC ADOPTION ACROSS THE MANUFACTURING SECTOR 192
12.7 RETAIL & ECOMMERCE 193
12.7.1 EXPANDING DIGITAL COMMERCE AND AI-DRIVEN CUSTOMER ENGAGEMENT ARE DRIVING AI SOC ADOPTION ACROSS THE RETAIL AND ECOMMERCE SECTOR 193
12.8 ENERGY & UTILITIES 195
12.8.1 MODERNIZATION OF CRITICAL ENERGY INFRASTRUCTURE AND IT-OT CONVERGENCE ARE DRIVING AI SOC ADOPTION ACROSS THE ENERGY AND UTILITIES SECTOR 195
12.9 MEDIA & ENTERTAINMENT 196
12.9.1 PROTECTING DIGITAL CONTENT, STREAMING PLATFORMS, AND AI-DRIVEN MEDIA ECOSYSTEMS IS ACCELERATING AI SOC ADOPTION ACROSS THE MEDIA AND ENTERTAINMENT INDUSTRY 196
12.10 EDUCATION 197
12.10.1 DIGITAL LEARNING EXPANSION AND RISING CYBER THREATS ARE ACCELERATING AI SOC ADOPTION ACROSS EDUCATIONAL INSTITUTIONS 197
12.11 OTHER VERTICALS 199

JULY 2026 © MarketsandMarkets™

13 AI SOC MARKET, BY REGION 201
13.1 INTRODUCTION 202
13.2 NORTH AMERICA 203
13.2.1 NORTH AMERICA: AI SOC MARKET DRIVERS 204
13.2.2 US 210
13.2.2.1 Federal AI cybersecurity modernization accelerating autonomous SOC adoption 210
13.2.3 CANADA 215
13.2.3.1 National cybersecurity strategy and trusted AI governance strengthening AI SOC growth 215
13.3 EUROPE 220
13.3.1 EUROPE: AI SOC MARKET DRIVERS 220
13.3.2 UK 226
13.3.2.1 Trusted AI governance and financial sector digitalization advancing intelligent security operations 226
13.3.3 GERMANY 231
13.3.3.1 Industrial digitalization and smart manufacturing increasing demand for autonomous cyber defense 231
13.3.4 FRANCE 236
13.3.4.1 Cyber sovereignty initiatives and trusted AI governance reinforcing national digital resilience 236
13.3.5 ITALY 241
13.3.5.1 AI strategy and public sector digitalization accelerating cyber modernization 241
13.3.6 REST OF EUROPE 246
13.4 ASIA PACIFIC 251
13.4.1 ASIA PACIFIC: AI SOC MARKET DRIVERS 251
13.4.2 CHINA 258
13.4.2.1 Indigenous AI innovation and cloud security leadership transforming intelligent cyber resilience 258
13.4.3 JAPAN 263
13.4.3.1 AI-security research and resilient digital infrastructure advancing next-generation cyber defense 263
13.4.4 INDIA 268
13.4.4.1 AI-native security operations and cybersecurity services ecosystem accelerating cyber modernization 268
13.4.5 REST OF ASIA PACIFIC 273
13.5 MIDDLE EAST & AFRICA 278
13.5.1 MIDDLE EAST & AFRICA: AI SOC MARKET DRIVERS 278
13.5.2 GULF COOPERATION COUNCIL (GCC) 284
13.5.2.1 Sovereign AI investments and regional cybersecurity cooperation strengthening intelligent cyber resilience 284
13.5.2.2 KSA 290
13.5.2.2.1 Vision 2030 and national AI governance accelerating intelligent cybersecurity transformation 290

JULY 2026 © MarketsandMarkets™

13.5.2.3 UAE 295
13.5.2.3.1 AI-native government and sovereign AI ecosystem transforming digital security 295
13.5.2.4 Rest of GCC 300
13.5.3 REST OF MIDDLE EAST 305
13.5.4 AFRICA 310
13.5.4.1 Expanding AI-enabled security operations strengthening cyber resilience across digital economies 310
13.6 LATIN AMERICA 315
13.6.1 LATIN AMERICA: AI SOC MARKET DRIVERS 315
13.6.2 BRAZIL 321
13.6.2.1 National AI investments and regulatory modernization accelerating AI-driven security operations 321
13.6.3 MEXICO 326
13.6.3.1 Nearshoring-driven industrial digitalization and national cybersecurity modernization accelerating AI-enabled security operations 326
13.6.4 REST OF LATIN AMERICA 331
14 COMPETITIVE LANDSCAPE 336
14.1 KEY PLAYER STRATEGIES/RIGHT TO WIN 336
14.2 REVENUE ANALYSIS 338
14.3 MARKET SHARE ANALYSIS 339
14.4 BRAND/PRODUCT COMPARISON 342
14.5 COMPANY VALUATION AND FINANCIAL METRICS 343
14.5.1 COMPANY VALUATION 343
14.5.2 FINANCIAL METRICS USING EV/EBIDTA 344
14.6 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2025 344
14.6.1 STARS 345
14.6.2 EMERGING LEADERS 345
14.6.3 PERVASIVE PLAYERS 345
14.6.4 PARTICIPANTS 345
14.6.5 COMPANY FOOTPRINT: KEY PLAYERS 347
14.6.5.1 Company footprint 347
14.6.5.2 Offering footprint 348
14.6.5.3 Organization Size footprint 348
14.6.5.4 Vertical footprint 349
14.6.5.5 Regional footprint 350
14.7 COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2025 351
14.7.1 PROGRESSIVE COMPANIES 351
14.7.2 RESPONSIVE COMPANIES 351
14.7.3 DYNAMIC COMPANIES 352
14.7.4 STARTING BLOCKS 352

JULY 2026 © MarketsandMarkets™

14.7.5 COMPETITIVE BENCHMARKING: STARTUPS/SMES 353
14.7.5.1 Detailed list of key startups/SMEs 353
14.7.5.2 Competitive benchmarking of key startups/SMEs 355
14.7.5.2.1 Offering footprint 355
14.7.5.2.2 Organization size footprint 356
14.7.5.2.3 Vertical footprint 357
14.7.5.2.4 Regional footprint 358
14.8 COMPETITIVE SCENARIO AND TRENDS 359
14.8.1 PRODUCT LAUNCHES 359
14.8.2 DEALS 364
14.8.3 EXPANSIONS 370
15 COMPANY PROFILES 372
15.1 KEY PLAYERS 372
15.1.1 MICROSOFT 372
15.1.1.1 Business overview 372
15.1.1.2 Products/Solutions/Services offered 373
15.1.1.3 Recent developments 375
15.1.1.3.1 Product launches/enhancements 375
15.1.1.3.2 Deals 377
15.1.1.4 MnM view 378
15.1.1.4.1 Key strengths 378
15.1.1.4.2 Strategic choices 379
15.1.1.4.3 Weaknesses & competitive threats 379
15.1.2 CISCO 380
15.1.2.1 Business overview 380
15.1.2.2 Products/Solutions/Services offered 381
15.1.2.3 Recent developments 384
15.1.2.3.1 Product launches/enhancements 384
15.1.2.3.2 Deals 385
15.1.2.4 MnM view 386
15.1.2.4.1 Key strengths 386
15.1.2.4.2 Strategic choices 386
15.1.2.4.3 Weaknesses & competitive threats 386
15.1.3 CROWDSTRIKE 387
15.1.3.1 Business overview 387
15.1.3.2 Products/Solutions/Services offered 388
15.1.3.3 Recent developments 390
15.1.3.3.1 Product launches/enhancements 390
15.1.3.3.2 Deals 391
15.1.3.3.3 Expansions 393

JULY 2026 © MarketsandMarkets™

15.1.3.4 MnM view....393
15.1.3.4.1 Key strengths....393
15.1.3.4.2 Strategic choices....393
15.1.3.4.3 Weaknesses & competitive threats....394
15.1.4 PALO ALTO NETWORKS....395
15.1.4.1 Business overview....395
15.1.4.2 Products/Solutions/Services offered....396
15.1.4.3 Recent developments....398
15.1.4.3.1 Product launches/enhancements....398
15.1.4.3.2 Deals....398
15.1.4.3.3 Expansions....400
15.1.4.4 MnM view....400
15.1.4.4.1 Key strengths....400
15.1.4.4.2 Strategic choices....401
15.1.4.4.3 Weaknesses & competitive threats....401
15.1.5 GOOGLE....402
15.1.5.1 Business overview....402
15.1.5.2 Products/Solutions/Services offered....403
15.1.5.3 Recent developments....406
15.1.5.3.1 Product launches/enhancements....406
15.1.5.3.2 Deals....408
15.1.5.3.3 Expansions....410
15.1.5.4 MnM view....410
15.1.5.4.1 Key strengths....410
15.1.5.4.2 Strategic choices....411
15.1.5.4.3 Weaknesses & competitive threats....411
15.1.6 SWIMLANE....412
15.1.6.1 Business overview....412
15.1.6.2 Products/Solutions/Services offered....413
15.1.6.3 Recent developments....414
15.1.6.3.1 Product launches and enhancements....414
15.1.6.3.2 Deals....415
15.1.7 LUMU TECHNOLOGIES....416
15.1.7.1 Business overview....416
15.1.7.2 Products/Solutions/Services offered....417
15.1.7.3 Recent developments....417
15.1.7.3.1 Product launches/enhancements....417
15.1.7.3.2 Deals....418
15.1.7.3.3 Expansions....419

JULY 2026 © MarketsandMarkets™

15.1.8 EXAFORCE 420
15.1.8.1 Business overview 420
15.1.8.2 Products/Solutions/Services offered 421
15.1.8.3 Recent developments 422
15.1.8.3.1 Product launches and enhancements 422
15.1.8.3.2 Deals 422
15.1.8.3.3 Expansions 423
15.1.9 SOPHOS 424
15.1.9.1 Business overview 424
15.1.9.2 Products/Solutions/Services offered 425
15.1.9.3 Recent developments 426
15.1.9.3.1 Product launches/enhancements 426
15.1.9.3.2 Deals 427
15.1.10 IBM 428
15.1.10.1 Business overview 428
15.1.10.2 Products/Solutions/Services offered 429
15.1.10.3 Recent developments 431
15.1.10.3.1 Product launches/enhancements 431
15.1.10.3.2 Deals 432
15.1.10.3.3 Expansions 433
15.1.11 FORTINET 434
15.1.11.1 Business overview 434
15.1.11.2 Products/Solutions/Services offered 435
15.1.11.3 Recent developments 438
15.1.11.3.1 Product launches/enhancements 438
15.1.11.3.2 Deals 439
15.1.12 ARCTIC WOLF 440
15.1.12.1 Business overview 440
15.1.12.2 Products/Solutions/Services offered 441
15.1.12.3 Recent developments 442
15.1.12.3.1 Product launches/enhancements 442
15.1.12.3.2 Deals 443
15.1.13 ELASTIC 444
15.1.13.1 Business overview 444
15.1.13.2 Products/Solutions/Services offered 445
15.1.13.3 Recent developments 447
15.1.13.3.1 Product launches/enhancements 447
15.1.13.3.2 Deals 448

JULY 2026 © MarketsandMarkets™

15.1.14 RAPID7 449
15.1.14.1 Business overview 449
15.1.14.2 Products/Solutions/Services offered 450
15.1.14.3 Recent developments 451
15.1.14.3.1 Product launches/enhancements 451
15.1.14.3.2 Deals 452
15.1.14.3.3 Expansions 453
15.1.15 SENTINELONE 454
15.1.15.1 Business overview 454
15.1.15.2 Products/Solutions/Services offered 455
15.1.15.3 Recent developments 458
15.1.15.3.1 Product launches/enhancements 458
15.1.15.3.2 Deals 459
15.1.15.3.3 Expansions 460
15.2 OTHER KEY PLAYERS 461
15.2.1 RELIAQUEST 461
15.2.2 EXABEAM 462
15.2.3 ESENTIRE 463
15.2.4 EXPEL 464
15.2.5 HUNTRESS 465
15.2.6 UNDERDEFENSE 466
15.2.7 STELLAR CYBER 467
15.2.8 RADIANT SECURITY 468
15.2.9 TORQ 469
15.2.10 INTEZER 470
15.2.11 CONIFERS 471
15.2.12 DROPZONE AI 472
15.2.13 SIMBIAN 473
15.2.14 PROPHET SECURITY 474
15.2.15 LEGION SECURITY 475
15.2.16 CYBERSILO 476
15.2.17 BRICKLAYER AI 477
15.2.18 AUGUR 478
15.2.19 BLINKOPS 479
15.2.20 GRUVE 480
15.2.21 CYBERNX 481
15.2.22 ANVILOGIC 482
15.2.23 AISTRIKE 483
15.2.24 D3 SECURITY 484
15.2.25 RIVERSAFE 485
15.2.26 SOC JEDI.AI 486
15.2.27 VULNURIS 487

JULY 2026 © MarketsandMarkets™

16 RESEARCH METHODOLOGY 488
16.1 RESEARCH DATA 488
16.1.1 SECONDARY DATA 490
16.1.2 PRIMARY DATA 490
16.1.2.1 Breakup of primary profiles 491
16.1.2.2 Key industry insights 491
16.2 DATA TRIANGULATION 492
16.3 MARKET SIZE ESTIMATION 493
16.4 MARKET FORECAST 497
16.5 RESEARCH ASSUMPTIONS 498
16.6 LIMITATIONS & RISK ASSESSMENT 499
17 APPENDIX 500
17.1 DISCUSSION GUIDE 500
17.2 KNOWLEDGESTORE: MARKETSANDMARKETS' SUBSCRIPTION PORTAL 504
17.3 CUSTOMIZATION OPTIONS 506
17.4 RELATED REPORTS 506
17.5 AUTHOR DETAILS 507

JULY 2026 © MarketsandMarkets™

LIST OF TABLES

TABLE 1	USD EXCHANGE RATES, 2022–2025	44
TABLE 2	UNMET NEEDS AND WHITE SPACES IN AI SOC MARKET	64
TABLE 3	STRATEGIC MOVES BY PLAYERS IN AI SOC MARKET	67
TABLE 4	CROSS-TIER STRATEGIC PATTERNS OF VENDORS	68
TABLE 5	PORTER'S FIVE FORCES' IMPACT ON AI SOC MARKET	71
TABLE 6	GDP PERCENTAGE CHANGE, BY KEY COUNTRY, 2021–2030	74
TABLE 7	AI SOC MARKET: ECOSYSTEM	80
TABLE 8	AVERAGE ANNUAL SELLING PRICE OF KEY AI SOC VENDORS, FOR 500-ENDPOINT DEPLOYMENT, 2025 (USD)	83
TABLE 9	INDICATIVE PRICING OF AI SOC OFFERINGS, BY KEY PLAYER, 2025 (USD)	84
TABLE 10	AI SOC MARKET: DETAILED LIST OF CONFERENCES & EVENTS, 2026	85
TABLE 11	KEY TARIFF RATES	94
TABLE 12	LIST OF TOP PATENTS IN AI SOC MARKET, 2024–2026	111
TABLE 13	TOP USE CASES AND MARKET POTENTIAL	115
TABLE 14	BEST PRACTICES: COMPANIES IMPLEMENTING USE CASES	115
TABLE 15	AI SOC MARKET: CASE STUDIES RELATED TO GEN AI IMPLEMENTATION	116
TABLE 16	INTERCONNECTED ADJACENT ECOSYSTEM AND IMPACT ON MARKET PLAYERS	117
TABLE 17	NORTH AMERICA: REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	121
TABLE 18	EUROPE: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	122
TABLE 19	ASIA PACIFIC: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	123
TABLE 20	MIDDLE EAST & AFRICA: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	125
TABLE 21	LATIN AMERICA: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	126
TABLE 22	GLOBAL INDUSTRY STANDARDS IN AI SOC MARKET	128
TABLE 23	INFLUENCE OF STAKEHOLDERS ON BUYING PROCESS FOR TOP THREE VERTICALS	132
TABLE 24	KEY BUYING CRITERIA FOR TOP THREE VERTICALS	133
TABLE 25	UNMET NEEDS AI SOC MARKET, BY END-USE INDUSTRY	135
TABLE 26	AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	139
TABLE 27	AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	139
TABLE 28	AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	141
TABLE 29	AI SOC MARKET, BY SOFTWARE PLATFORMS, 2026–2031 (USD MILLION)	142
TABLE 30	AI SOC SOFTWARE PLATFORMS MARKET, BY REGION, 2022–2025 (USD MILLION)	142
TABLE 31	AI SOC SOFTWARE PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)	142
TABLE 32	AI-ENABLED DETECTION AND ANALYTICS PLATFORMS MARKET, BY REGION, 2022–2025 (USD MILLION)	143
TABLE 33	AI-ENABLED DETECTION AND ANALYTICS PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)	144
TABLE 34	AI-ORCHESTRATED RESPONSE AND AUTOMATION PLATFORMS MARKET, BY REGION, 2022–2025 (USD MILLION)	145

JULY 2026 © MarketsandMarkets™

TABLE 35	AI-ORCHESTRATED RESPONSE AND AUTOMATION PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)	145
TABLE 36	AI-NATIVE SOC PLATFORMS MARKET, BY REGION, 2022–2025 (USD MILLION)	146
TABLE 37	AI-NATIVE SOC PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)	146
TABLE 38	AI SOC AGENT SOLUTIONS MARKET, BY REGION, 2022–2025 (USD MILLION)	147
TABLE 39	AI SOC AGENT SOLUTIONS MARKET, BY REGION, 2026–2031 (USD MILLION)	148
TABLE 40	AI SECURITY DATA PLATFORMS MARKET, BY REGION, 2022–2025 (USD MILLION)	149
TABLE 41	AI SECURITY DATA PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)	149
TABLE 42	AI THREAT INTELLIGENCE PLATFORMS MARKET, BY REGION, 2022–2025 (USD MILLION)	150
TABLE 43	AI THREAT INTELLIGENCE PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)	150
TABLE 44	AI GOVERNANCE, RISK, AND COMPLIANCE SOLUTIONS MARKET, BY REGION, 2022–2025 (USD MILLION)	151
TABLE 45	AI GOVERNANCE, RISK, AND COMPLIANCE SOLUTIONS MARKET, BY REGION, 2026–2031 (USD MILLION)	151
TABLE 46	AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	153
TABLE 47	AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	153
TABLE 48	AI SOC SERVICES MARKET, BY REGION, 2022–2025 (USD MILLION)	154
TABLE 49	AI SOC SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)	154
TABLE 50	AI-AUGMENTED MANAGED DETECTION AND RESPONSE (MDR) MARKET, BY REGION, 2022–2025 (USD MILLION)	155
TABLE 51	AI-AUGMENTED MANAGED DETECTION AND RESPONSE (MDR) MARKET, BY REGION, 2026–2031 (USD MILLION)	155
TABLE 52	AI SOC-AS-A-SERVICE (SOCAAS) MARKET, BY REGION, 2022–2025 (USD MILLION)	156
TABLE 53	AI SOC-AS-A-SERVICE (SOCAAS) MARKET, BY REGION, 2026–2031 (USD MILLION)	157
TABLE 54	INCIDENT RESPONSE AND FORENSICS SERVICES MARKET, BY REGION, 2022–2025 (USD MILLION)	158
TABLE 55	INCIDENT RESPONSE AND FORENSICS SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)	158
TABLE 56	THREAT INTELLIGENCE AND ADVISORY SERVICES MARKET, BY REGION, 2022–2025 (USD MILLION)	159
TABLE 57	THREAT INTELLIGENCE AND ADVISORY SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)	159
TABLE 58	AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	162
TABLE 59	AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	162
TABLE 60	AI SOC MARKET FOR LARGE ENTERPRISES, BY REGION, 2022–2025 (USD MILLION)	164
TABLE 61	AI SOC MARKET FOR LARGE ENTERPRISES, BY REGION, 2026–2031 (USD MILLION)	164
TABLE 62	AI SOC MARKET FOR SMES, BY REGION, 2022–2025 (USD MILLION)	165
TABLE 63	AI SOC MARKET FOR SMES, BY REGION, 2026–2031 (USD MILLION)	165
TABLE 64	AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	168
TABLE 65	AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	169
TABLE 66	AI SOC MARKET FOR THREAT DETECTION AND MONITORING, BY REGION, 2022–2025 (USD MILLION)	170
TABLE 67	AI SOC MARKET FOR THREAT DETECTION AND MONITORING, BY REGION, 2026–2031 (USD MILLION)	170

JULY 2026 © MarketsandMarkets™

TABLE 68	AI SOC MARKET FOR ALERT TRIAGE AND PRIORITIZATION, BY REGION, 2022–2025 (USD MILLION)	171
TABLE 69	AI SOC MARKET FOR ALERT TRIAGE AND PRIORITIZATION, BY REGION, 2026–2031 (USD MILLION)	171
TABLE 70	AI SOC MARKET FOR INCIDENT INVESTIGATION AND ANALYSIS, BY REGION, 2022–2025 (USD MILLION)	172
TABLE 71	AI SOC MARKET FOR INCIDENT INVESTIGATION AND ANALYSIS, BY REGION, 2026–2031 (USD MILLION)	173
TABLE 72	AI SOC MARKET FOR THREAT HUNTING, BY REGION, 2022–2025 (USD MILLION)	174
TABLE 73	AI SOC MARKET FOR THREAT HUNTING, BY REGION, 2026–2031 (USD MILLION)	174
TABLE 74	AI SOC MARKET FOR INCIDENT RESPONSE AND REMEDIATION, BY REGION, 2022–2025 (USD MILLION)	175
TABLE 75	AI SOC MARKET FOR INCIDENT RESPONSE AND REMEDIATION, BY REGION, 2026–2031 (USD MILLION)	175
TABLE 76	AI SOC MARKET FOR INSIDER THREAT DETECTION, BY REGION, 2022–2025 (USD MILLION)	176
TABLE 77	AI SOC MARKET FOR INSIDER THREAT DETECTION, BY REGION, 2026–2031 (USD MILLION)	177
TABLE 78	AI SOC MARKET FOR CLOUD SECURITY MONITORING, BY REGION, 2022–2025 (USD MILLION)	178
TABLE 79	AI SOC MARKET FOR CLOUD SECURITY MONITORING, BY REGION, 2026–2031 (USD MILLION)	178
TABLE 80	AI SOC MARKET FOR IDENTITY AND ACCESS MONITORING, BY REGION, 2022–2025 (USD MILLION)	179
TABLE 81	AI SOC MARKET FOR IDENTITY AND ACCESS MONITORING, BY REGION, 2026–2031 (USD MILLION)	179
TABLE 82	AI SOC MARKET FOR COMPLIANCE MONITORING AND REPORTING, BY REGION, 2022–2025 (USD MILLION)	180
TABLE 83	AI SOC MARKET FOR COMPLIANCE MONITORING AND REPORTING, BY REGION, 2026–2031 (USD MILLION)	181
TABLE 84	AI SOC MARKET FOR SECURITY ANALYTICS AND VISUALIZATION, BY REGION, 2022–2025 (USD MILLION)	182
TABLE 85	AI SOC MARKET FOR SECURITY ANALYTICS AND VISUALIZATION, BY REGION, 2026–2031 (USD MILLION)	182
TABLE 86	AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	186
TABLE 87	AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	186
TABLE 88	AI SOC MARKET IN BFSI, BY REGION, 2022–2025 (USD MILLION)	187
TABLE 89	AI SOC MARKET IN BFSI, BY REGION, 2026–2031 (USD MILLION)	188
TABLE 90	AI SOC MARKET IN GOVERNMENT AND DEFENSE, BY REGION, 2022–2025 (USD MILLION)	189
TABLE 91	AI SOC MARKET IN GOVERNMENT AND DEFENSE, BY REGION, 2026–2031 (USD MILLION)	189
TABLE 92	AI SOC MARKET IN HEALTHCARE & LIFE SCIENCES, BY REGION, 2022–2025 (USD MILLION)	190
TABLE 93	AI SOC MARKET IN HEALTHCARE & LIFE SCIENCES, BY REGION, 2026–2031 (USD MILLION)	190
TABLE 94	AI SOC MARKET IN IT & TELECOMMUNICATIONS, BY REGION, 2022–2025 (USD MILLION)	191
TABLE 95	AI SOC MARKET IN IT & TELECOMMUNICATIONS, BY REGION, 2026–2031 (USD MILLION)	192

JULY 2026 © MarketsandMarkets™

TABLE 96	AI SOC MARKET IN MANUFACTURING, BY REGION, 2022–2025 (USD MILLION)	193
TABLE 97	AI SOC MARKET IN MANUFACTURING, BY REGION, 2026–2031 (USD MILLION)	193
TABLE 98	AI SOC MARKET IN RETAIL & ECOMMERCE, BY REGION, 2022–2025 (USD MILLION)	194
TABLE 99	AI SOC MARKET IN RETAIL & ECOMMERCE, BY REGION, 2026–2031 (USD MILLION)	194
TABLE 100	AI SOC MARKET IN ENERGY & UTILITIES, BY REGION, 2022–2025 (USD MILLION)	195
TABLE 101	AI SOC MARKET IN ENERGY & UTILITIES, BY REGION, 2026–2031 (USD MILLION)	196
TABLE 102	AI SOC MARKET IN MEDIA & ENTERTAINMENT, BY REGION, 2022–2025 (USD MILLION)	197
TABLE 103	AI SOC MARKET IN MEDIA & ENTERTAINMENT, BY REGION, 2026–2031 (USD MILLION)	197
TABLE 104	AI SOC MARKET IN EDUCATION, BY REGION, 2022–2025 (USD MILLION)	198
TABLE 105	AI SOC MARKET IN EDUCATION, BY REGION, 2026–2031 (USD MILLION)	198
TABLE 106	AI SOC MARKET IN OTHER VERTICALS, BY REGION, 2022–2025 (USD MILLION)	200
TABLE 107	AI SOC MARKET IN OTHER VERTICALS, BY REGION, 2026–2031 (USD MILLION)	200
TABLE 108	AI SOC MARKET, BY REGION, 2022–2025 (USD MILLION)	203
TABLE 109	AI SOC MARKET, BY REGION, 2026–2031 (USD MILLION)	203
TABLE 110	NORTH AMERICA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	205
TABLE 111	NORTH AMERICA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	205
TABLE 112	NORTH AMERICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	206
TABLE 113	NORTH AMERICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	206
TABLE 114	NORTH AMERICA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	206
TABLE 115	NORTH AMERICA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	207
TABLE 116	NORTH AMERICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	207
TABLE 117	NORTH AMERICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	207
TABLE 118	NORTH AMERICA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	208
TABLE 119	NORTH AMERICA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	208
TABLE 120	NORTH AMERICA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	209
TABLE 121	NORTH AMERICA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	209
TABLE 122	NORTH AMERICA: AI SOC MARKET, BY COUNTRY, 2022–2025 (USD MILLION)	209
TABLE 123	NORTH AMERICA: AI SOC MARKET, BY COUNTRY, 2026–2031 (USD MILLION)	210
TABLE 124	US: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	210
TABLE 125	US: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	211
TABLE 126	US: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	211
TABLE 127	US: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	211
TABLE 128	US: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	212
TABLE 129	US: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	212
TABLE 130	US: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	212
TABLE 131	US: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	212
TABLE 132	US: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	213
TABLE 133	US: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	213

JULY 2026 © MarketsandMarkets™

TABLE 134	US: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	214
TABLE 135	US: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	214
TABLE 136	CANADA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	215
TABLE 137	CANADA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	215
TABLE 138	CANADA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	216
TABLE 139	CANADA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	216
TABLE 140	CANADA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	216
TABLE 141	CANADA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	217
TABLE 142	CANADA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	217
TABLE 143	CANADA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	217
TABLE 144	CANADA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	218
TABLE 145	CANADA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	218
TABLE 146	CANADA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	219
TABLE 147	CANADA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	219
TABLE 148	EUROPE: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	221
TABLE 149	EUROPE: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	221
TABLE 150	EUROPE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	221
TABLE 151	EUROPE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	222
TABLE 152	EUROPE: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	222
TABLE 153	EUROPE: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	222
TABLE 154	EUROPE: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	223
TABLE 155	EUROPE: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	223
TABLE 156	EUROPE: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	223
TABLE 157	EUROPE: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	224
TABLE 158	EUROPE: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	224
TABLE 159	EUROPE: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	225
TABLE 160	EUROPE: AI SOC MARKET, BY COUNTRY, 2022–2025 (USD MILLION)	225
TABLE 161	EUROPE: AI SOC MARKET, BY COUNTRY, 2026–2031 (USD MILLION)	225
TABLE 162	UK: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	226
TABLE 163	UK: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	226
TABLE 164	UK: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	227
TABLE 165	UK: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	227
TABLE 166	UK: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	227
TABLE 167	UK: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	228
TABLE 168	UK: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	228
TABLE 169	UK: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	228
TABLE 170	UK: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	229
TABLE 171	UK: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	229
TABLE 172	UK: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	230
TABLE 173	UK: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	230
TABLE 174	GERMANY: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	231
TABLE 175	GERMANY: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	231
TABLE 176	GERMANY: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	232

JULY 2026 © MarketsandMarkets™

TABLE 177	GERMANY: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	232
TABLE 178	GERMANY: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	232
TABLE 179	GERMANY: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	233
TABLE 180	GERMANY: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	233
TABLE 181	GERMANY: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	233
TABLE 182	GERMANY: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	234
TABLE 183	GERMANY: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	234
TABLE 184	GERMANY: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	235
TABLE 185	GERMANY: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	235
TABLE 186	FRANCE: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	236
TABLE 187	FRANCE: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	236
TABLE 188	FRANCE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	237
TABLE 189	FRANCE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	237
TABLE 190	FRANCE: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	237
TABLE 191	FRANCE: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	238
TABLE 192	FRANCE: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	238
TABLE 193	FRANCE: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	238
TABLE 194	FRANCE: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	239
TABLE 195	FRANCE: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	239
TABLE 196	FRANCE: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	240
TABLE 197	FRANCE: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	240
TABLE 198	ITALY: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	241
TABLE 199	ITALY: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	241
TABLE 200	ITALY: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	242
TABLE 201	ITALY: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	242
TABLE 202	ITALY: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	242
TABLE 203	ITALY: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	243
TABLE 204	ITALY: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	243
TABLE 205	ITALY: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	243
TABLE 206	ITALY: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	244
TABLE 207	ITALY: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	244
TABLE 208	ITALY: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	245
TABLE 209	ITALY: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	245
TABLE 210	REST OF EUROPE: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	246
TABLE 211	REST OF EUROPE: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	246
TABLE 212	REST OF EUROPE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	247
TABLE 213	REST OF EUROPE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	247
TABLE 214	REST OF EUROPE: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	247
TABLE 215	REST OF EUROPE: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	248
TABLE 216	REST OF EUROPE: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	248

JULY 2026 © MarketsandMarkets™

TABLE 217	REST OF EUROPE: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	248
TABLE 218	REST OF EUROPE: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	249
TABLE 219	REST OF EUROPE: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	249
TABLE 220	REST OF EUROPE: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	250
TABLE 221	REST OF EUROPE: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	250
TABLE 222	ASIA PACIFIC: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	253
TABLE 223	ASIA PACIFIC: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	253
TABLE 224	ASIA PACIFIC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	253
TABLE 225	ASIA PACIFIC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	254
TABLE 226	ASIA PACIFIC: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	254
TABLE 227	ASIA PACIFIC: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	254
TABLE 228	ASIA PACIFIC: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	255
TABLE 229	ASIA PACIFIC: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	255
TABLE 230	ASIA PACIFIC: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	255
TABLE 231	ASIA PACIFIC: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	256
TABLE 232	ASIA PACIFIC: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	256
TABLE 233	ASIA PACIFIC: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	257
TABLE 234	ASIA PACIFIC: AI SOC MARKET, BY COUNTRY, 2022–2025 (USD MILLION)	257
TABLE 235	ASIA PACIFIC: AI SOC MARKET, BY COUNTRY, 2026–2031 (USD MILLION)	257
TABLE 236	CHINA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	258
TABLE 237	CHINA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	258
TABLE 238	CHINA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	259
TABLE 239	CHINA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	259
TABLE 240	CHINA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	259
TABLE 241	CHINA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	260
TABLE 242	CHINA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	260
TABLE 243	CHINA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	260
TABLE 244	CHINA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	261
TABLE 245	CHINA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	261
TABLE 246	CHINA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	262
TABLE 247	CHINA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	262
TABLE 248	JAPAN: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	263
TABLE 249	JAPAN: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	263
TABLE 250	JAPAN: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	264
TABLE 251	JAPAN: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	264
TABLE 252	JAPAN: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	264
TABLE 253	JAPAN: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	265
TABLE 254	JAPAN: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	265
TABLE 255	JAPAN: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	265
TABLE 256	JAPAN: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	266

JULY 2026 © MarketsandMarkets™

TABLE 257	JAPAN: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	266
TABLE 258	JAPAN: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	267
TABLE 259	JAPAN: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	267
TABLE 260	INDIA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	268
TABLE 261	INDIA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	268
TABLE 262	INDIA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	269
TABLE 263	INDIA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	269
TABLE 264	INDIA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	269
TABLE 265	INDIA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	270
TABLE 266	INDIA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	270
TABLE 267	INDIA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	270
TABLE 268	INDIA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	271
TABLE 269	INDIA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	271
TABLE 270	INDIA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	272
TABLE 271	INDIA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	272
TABLE 272	REST OF ASIA PACIFIC: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	273
TABLE 273	REST OF ASIA PACIFIC: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	274
TABLE 274	REST OF ASIA PACIFIC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	274
TABLE 275	REST OF ASIA PACIFIC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	274
TABLE 276	REST OF ASIA PACIFIC: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	275
TABLE 277	REST OF ASIA PACIFIC: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	275
TABLE 278	REST OF ASIA PACIFIC: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	275
TABLE 279	REST OF ASIA PACIFIC: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	275
TABLE 280	REST OF ASIA PACIFIC: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	276
TABLE 281	REST OF ASIA PACIFIC: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	276
TABLE 282	REST OF ASIA PACIFIC: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	277
TABLE 283	REST OF ASIA PACIFIC: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	277
TABLE 284	MIDDLE EAST & AFRICA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	279
TABLE 285	MIDDLE EAST & AFRICA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	279
TABLE 286	MIDDLE EAST & AFRICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	280
TABLE 287	MIDDLE EAST & AFRICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	280
TABLE 288	MIDDLE EAST & AFRICA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	280
TABLE 289	MIDDLE EAST & AFRICA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	281
TABLE 290	MIDDLE EAST & AFRICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	281
TABLE 291	MIDDLE EAST & AFRICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	281

JULY 2026 © MarketsandMarkets™

TABLE 292	MIDDLE EAST & AFRICA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	282
TABLE 293	MIDDLE EAST & AFRICA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	282
TABLE 294	MIDDLE EAST & AFRICA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	283
TABLE 295	MIDDLE EAST & AFRICA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	283
TABLE 296	MIDDLE EAST & AFRICA: AI SOC MARKET, BY COUNTRY, 2022–2025 (USD MILLION)	283
TABLE 297	MIDDLE EAST & AFRICA: AI SOC MARKET, BY COUNTRY, 2026–2031 (USD MILLION)	284
TABLE 298	GCC: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	285
TABLE 299	GCC: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	285
TABLE 300	GCC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	285
TABLE 301	GCC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	286
TABLE 302	GCC: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	286
TABLE 303	GCC: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	286
TABLE 304	GCC: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	287
TABLE 305	GCC: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	287
TABLE 306	GCC: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	287
TABLE 307	GCC: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	288
TABLE 308	GCC: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	288
TABLE 309	GCC: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	289
TABLE 310	GCC: AI SOC MARKET, BY COUNTRY, 2022–2025 (USD MILLION)	289
TABLE 311	GCC: AI SOC MARKET, BY COUNTRY, 2026–2031 (USD MILLION)	289
TABLE 312	KSA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	290
TABLE 313	KSA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	290
TABLE 314	KSA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	291
TABLE 315	KSA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	291
TABLE 316	KSA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	291
TABLE 317	KSA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	292
TABLE 318	KSA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	292
TABLE 319	KSA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	292
TABLE 320	KSA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	293
TABLE 321	KSA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	293
TABLE 322	KSA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	294
TABLE 323	KSA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	294
TABLE 324	UAE: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	295
TABLE 325	UAE: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	295
TABLE 326	UAE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	296
TABLE 327	UAE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	296
TABLE 328	UAE: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	296
TABLE 329	UAE: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	297
TABLE 330	UAE: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	297

JULY 2026 © MarketsandMarkets™

TABLE 331	UAE: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	297
TABLE 332	UAE: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	298
TABLE 333	UAE: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	298
TABLE 334	UAE: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	299
TABLE 335	UAE: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	299
TABLE 336	REST OF GCC: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	300
TABLE 337	REST OF GCC: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	300
TABLE 338	REST OF GCC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	301
TABLE 339	REST OF GCC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	301
TABLE 340	REST OF GCC: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	301
TABLE 341	REST OF GCC: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	302
TABLE 342	REST OF GCC: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	302
TABLE 343	REST OF GCC: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	302
TABLE 344	REST OF GCC: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	303
TABLE 345	REST OF GCC: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	303
TABLE 346	REST OF GCC: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	304
TABLE 347	REST OF GCC: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	304
TABLE 348	REST OF MIDDLE EAST: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	305
TABLE 349	REST OF MIDDLE EAST: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	305
TABLE 350	REST OF MIDDLE EAST: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	306
TABLE 351	REST OF MIDDLE EAST: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	306
TABLE 352	REST OF MIDDLE EAST: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	306
TABLE 353	REST OF MIDDLE EAST: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	307
TABLE 354	REST OF MIDDLE EAST: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	307
TABLE 355	REST OF MIDDLE EAST: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	307
TABLE 356	REST OF MIDDLE EAST: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	308
TABLE 357	REST OF MIDDLE EAST: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	308
TABLE 358	REST OF MIDDLE EAST: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	309
TABLE 359	REST OF MIDDLE EAST: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	309
TABLE 360	AFRICA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	310
TABLE 361	AFRICA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	310
TABLE 362	AFRICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	311
TABLE 363	AFRICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	311
TABLE 364	AFRICA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	311
TABLE 365	AFRICA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	312

JULY 2026 © MarketsandMarkets™

TABLE 366	AFRICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	312
TABLE 367	AFRICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	312
TABLE 368	AFRICA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	313
TABLE 369	AFRICA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	313
TABLE 370	AFRICA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	314
TABLE 371	AFRICA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	314
TABLE 372	LATIN AMERICA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	316
TABLE 373	LATIN AMERICA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	316
TABLE 374	LATIN AMERICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	316
TABLE 375	LATIN AMERICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	317
TABLE 376	LATIN AMERICA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	317
TABLE 377	LATIN AMERICA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	317
TABLE 378	LATIN AMERICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	318
TABLE 379	LATIN AMERICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	318
TABLE 380	LATIN AMERICA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	318
TABLE 381	LATIN AMERICA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	319
TABLE 382	LATIN AMERICA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	319
TABLE 383	LATIN AMERICA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	320
TABLE 384	LATIN AMERICA: AI SOC MARKET, BY COUNTRY, 2022–2025 (USD MILLION)	320
TABLE 385	LATIN AMERICA: AI SOC MARKET, BY COUNTRY, 2026–2031 (USD MILLION)	320
TABLE 386	BRAZIL: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	321
TABLE 387	BRAZIL: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	321
TABLE 388	BRAZIL: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	322
TABLE 389	BRAZIL: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	322
TABLE 390	BRAZIL: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	322
TABLE 391	BRAZIL: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	323
TABLE 392	BRAZIL: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	323
TABLE 393	BRAZIL: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	323
TABLE 394	BRAZIL: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	324
TABLE 395	BRAZIL: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	324
TABLE 396	BRAZIL: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	325
TABLE 397	BRAZIL: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	325
TABLE 398	MEXICO: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	326
TABLE 399	MEXICO: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	326
TABLE 400	MEXICO: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	327
TABLE 401	MEXICO: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	327
TABLE 402	MEXICO: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	327
TABLE 403	MEXICO: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	328
TABLE 404	MEXICO: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	328
TABLE 405	MEXICO: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	328
TABLE 406	MEXICO: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	329

JULY 2026 © MarketsandMarkets™

TABLE 407	MEXICO: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	329
TABLE 408	MEXICO: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	330
TABLE 409	MEXICO: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	330
TABLE 410	REST OF LATIN AMERICA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)	331
TABLE 411	REST OF LATIN AMERICA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)	331
TABLE 412	REST OF LATIN AMERICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)	332
TABLE 413	REST OF LATIN AMERICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)	332
TABLE 414	REST OF LATIN AMERICA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)	332
TABLE 415	REST OF LATIN AMERICA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)	333
TABLE 416	REST OF LATIN AMERICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)	333
TABLE 417	REST OF LATIN AMERICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	333
TABLE 418	REST OF LATIN AMERICA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)	334
TABLE 419	REST OF LATIN AMERICA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)	334
TABLE 420	REST OF LATIN AMERICA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)	335
TABLE 421	REST OF LATIN AMERICA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	335
TABLE 422	OVERVIEW OF STRATEGIES ADOPTED BY KEY AI SOC VENDORS, 2024–2026	336
TABLE 423	AI SOC MARKET: DEGREE OF COMPETITION	339
TABLE 424	AI SOC MARKET: OFFERING FOOTPRINT, 2025	348
TABLE 425	AI SOC MARKET: ORGANIZATION SIZE FOOTPRINT, 2025	348
TABLE 426	AI SOC MARKET: VERTICAL FOOTPRINT, 2025	349
TABLE 427	AI SOC MARKET: REGIONAL FOOTPRINT, 2025	350
TABLE 428	DETAILED LIST OF KEY STARTUPS/SMES, 2025	353
TABLE 429	AI SOC MARKET: OFFERING FOOTPRINT OF STARTUPS/SMES, 2025	355
TABLE 430	AI SOC MARKET: ORGANIZATION SIZE FOOTPRINT OF STARTUPS/SMES, 2025	356
TABLE 431	AI SOC MARKET: VERTICAL FOOTPRINT OF STARTUPS/SMES, 2025	357
TABLE 432	AI SOC MARKET: REGIONAL FOOTPRINT OF STARTUPS/SMES, 2025	358
TABLE 433	AI SOC MARKET: PRODUCT LAUNCHES, JANUARY 2024–JULY 2026	359
TABLE 434	AI SOC MARKET: DEALS, JANUARY 2024–JULY 2026	364
TABLE 435	AI SOC MARKET: EXPANSIONS, JANUARY 2024–JULY 2026	370
TABLE 436	MICROSOFT: COMPANY OVERVIEW	372
TABLE 437	MICROSOFT: PRODUCTS/SOLUTIONS/SERVICES OFFERED	373
TABLE 438	MICROSOFT: PRODUCT LAUNCHES/ENHANCEMENTS	375
TABLE 439	MICROSOFT: DEALS	377
TABLE 440	CISCO: COMPANY OVERVIEW	380
TABLE 441	CISCO: PRODUCTS/SOLUTIONS/SERVICES OFFERED	381

JULY 2026 © MarketsandMarkets™

TABLE 442	CISCO: PRODUCT LAUNCHES/ENHANCEMENTS	384
TABLE 443	CISCO: DEALS	385
TABLE 444	CROWDSTRIKE: COMPANY OVERVIEW	387
TABLE 445	CROWDSTRIKE: PRODUCTS/SOLUTIONS/SERVICES OFFERED	388
TABLE 446	CROWDSTRIKE: PRODUCT LAUNCHES/ENHANCEMENTS	390
TABLE 447	CROWDSTRIKE: DEALS	391
TABLE 448	CROWDSTRIKE: EXPANSIONS	393
TABLE 449	PALO ALTO NETWORKS: COMPANY OVERVIEW	395
TABLE 450	PALO ALTO NETWORKS: PRODUCTS/SOLUTIONS/SERVICES OFFERED	396
TABLE 451	PALO ALTO NETWORKS: PRODUCT LAUNCHES/ENHANCEMENTS	398
TABLE 452	PALO ALTO NETWORKS: DEALS	398
TABLE 453	PALO ALTO NETWORKS: EXPANSIONS	400
TABLE 454	GOOGLE: COMPANY OVERVIEW	402
TABLE 455	GOOGLE: PRODUCTS/SOLUTIONS/SERVICES OFFERED	403
TABLE 456	GOOGLE: PRODUCT LAUNCHES/ENHANCEMENTS	406
TABLE 457	GOOGLE: DEALS	408
TABLE 458	GOOGLE: EXPANSIONS	410
TABLE 459	SWIMLANE: BUSINESS OVERVIEW	413
TABLE 460	SWIMLANE: PRODUCTS/SOLUTIONS/SERVICES OFFERINGS	413
TABLE 461	SWIMLANE: PRODUCT LAUNCHES AND ENHANCEMENTS	414
TABLE 462	SWIMLANE: DEALS	415
TABLE 463	LUMU TECHNOLOGIES: COMPANY OVERVIEW	416
TABLE 464	LUMU TECHNOLOGIES: PRODUCTS/SOLUTIONS/SERVICES OFFERED	417
TABLE 465	LUMU TECHNOLOGIES: PRODUCT LAUNCHES/ENHANCEMENTS	417
TABLE 466	LUMU TECHNOLOGIES: DEALS	418
TABLE 467	LUMU TECHNOLOGIES: EXPANSIONS	419
TABLE 468	EXAFORCE: BUSINESS OVERVIEW	421
TABLE 469	EXAFORCE: PRODUCTS/SOLUTIONS/SERVICES OFFERINGS	421
TABLE 470	EXAFORCE: PRODUCT LAUNCHES AND ENHANCEMENTS	422
TABLE 471	EXAFORCE: DEALS	422
TABLE 472	EXAFORCE: EXPANSIONS	423
TABLE 473	SOPHOS: COMPANY OVERVIEW	424
TABLE 474	SOPHOS: PRODUCTS/SOLUTIONS/SERVICES OFFERED	425
TABLE 475	SOPHOS: PRODUCT LAUNCHES/ENHANCEMENTS	426
TABLE 476	SOPHOS: DEALS	427
TABLE 477	IBM: COMPANY OVERVIEW	428
TABLE 478	IBM: PRODUCTS/SOLUTIONS/SERVICES OFFERED	429
TABLE 479	IBM: PRODUCT LAUNCHES/ENHANCEMENTS	431
TABLE 480	IBM: DEALS	432
TABLE 481	IBM: EXPANSIONS	433
TABLE 482	FORTINET: COMPANY OVERVIEW	434
TABLE 483	FORTINET: PRODUCTS/SOLUTIONS/SERVICES OFFERED	435
TABLE 484	FORTINET: PRODUCT LAUNCHES/ENHANCEMENTS	438
TABLE 485	FORTINET: DEALS	439

JULY 2026 © MarketsandMarkets™

TABLE 486	ARCTIC WOLF: COMPANY OVERVIEW	440
TABLE 487	ARCTIC WOLF: PRODUCTS/SOLUTIONS/SERVICES OFFERED	441
TABLE 488	ARCTIC WOLF: PRODUCT LAUNCHES/ENHANCEMENTS	442
TABLE 489	ARCTIC WOLF: DEALS	443
TABLE 490	ELASTIC: COMPANY OVERVIEW	444
TABLE 491	ELASTIC: PRODUCTS/SOLUTIONS/SERVICES OFFERED	445
TABLE 492	ELASTIC: PRODUCT LAUNCHES/ENHANCEMENTS	447
TABLE 493	ELASTIC: DEALS	448
TABLE 494	RAPID7: COMPANY OVERVIEW	449
TABLE 495	RAPID7: PRODUCTS/SOLUTIONS/SERVICES OFFERED	450
TABLE 496	RAPID7: PRODUCT LAUNCHES/ENHANCEMENTS	451
TABLE 497	RAPID7: DEALS	452
TABLE 498	RAPID7: EXPANSIONS	453
TABLE 499	SENTINELONE: COMPANY OVERVIEW	454
TABLE 500	SENTINELONE: PRODUCTS/SOLUTIONS/SERVICES OFFERED	455
TABLE 501	SENTINELONE: PRODUCT LAUNCHES/ENHANCEMENTS	458
TABLE 502	SENTINELONE: DEALS	459
TABLE 503	SENTINELONE: EXPANSIONS	460
TABLE 504	FACTOR ANALYSIS	497
TABLE 505	RESEARCH ASSUMPTIONS	498

JULY 2026 © MarketsandMarkets™

LIST OF FIGURES

FIGURE 1	MARKET SEGMENTATION AND REGIONS COVERED	38
FIGURE 2	STUDY YEARS CONSIDERED	43
FIGURE 3	MARKET SCENARIO	46
FIGURE 4	GLOBAL AI SOC MARKET, 2022–2031 (USD MILLION)	46
FIGURE 5	MAJOR STRATEGIES ADOPTED BY KEY PLAYERS IN AI SOC MARKET, 2022–2026	47
FIGURE 6	DISRUPTIVE TRENDS IMPACTING GROWTH OF AI SOC MARKET	48
FIGURE 7	HIGH-GROWTH SEGMENTS & EMERGING FRONTIERS IN THE AI SOC MARKET, 2026	49
FIGURE 8	ASIA PACIFIC TO REGISTER HIGHEST GROWTH DURING FORECAST PERIOD	51
FIGURE 9	RISING AI-POWERED CYBER THREATS, AUTONOMOUS SECURITY OPERATIONS, AND ENTERPRISE AI ADOPTION CONTINUE TO DRIVE AI SOC MARKET	52
FIGURE 10	SOFTWARE PLATFORMS TO ACCOUNT FOR LARGER MARKET SHARE DURING FORECAST PERIOD	53
FIGURE 11	AI-ENABLED DETECTION & ANALYTICS PLATFORMS TO HOLD HIGHEST MARKET SHARE DURING FORECAST PERIOD	53
FIGURE 12	AI-AUGMENTED MANAGED DETECTION AND RESPONSE (MDR) SEGMENT TO HOLD HIGHEST MARKET SHARE DURING FORECAST PERIOD	54
FIGURE 13	LARGE ENTERPRISES SEGMENT TO HOLD HIGHEST MARKET SHARE DURING FORECAST PERIOD	54
FIGURE 14	THREAT DETECTION & MONITORING SEGMENT TO HOLD HIGHEST MARKET SHARE DURING FORECAST PERIOD	55
FIGURE 15	BFSI SEGMENT TO HOLD LARGEST SHARE DURING FORECAST PERIOD	55
FIGURE 16	NORTH AMERICA TO EMERGE AS MOST SIGNIFICANT MARKET FOR NEXT FIVE YEARS	56
FIGURE 17	AI SOC MARKET: DRIVERS, RESTRAINTS, OPPORTUNITIES, AND CHALLENGES	58
FIGURE 18	AI SOC MARKET: PORTER'S FIVE FORCES ANALYSIS	70
FIGURE 19	AI SOC MARKET: VALUE CHAIN ANALYSIS	77
FIGURE 20	AI SOC MARKET: ECOSYSTEM ANALYSIS	80
FIGURE 21	AVERAGE ANNUAL SELLING PRICE OF KEY AI SOC VENDORS, FOR 500-ENDPOINT DEPLOYMENT, 2025 (USD)	83
FIGURE 22	TRENDS/DISRUPTIONS INFLUENCING CUSTOMER BUSINESS	86
FIGURE 23	LEADING GLOBAL AI SOC VENDORS, BY TOTAL FUNDING VALUE AND NUMBER OF FUNDING ROUNDS (USD MILLION)	87
FIGURE 24	PATENTS GRANTED IN AI SOC MARKET, 2016–2026	110
FIGURE 25	REGIONAL ANALYSIS OF PATENTS GRANTED IN AI SOC MARKET	111
FIGURE 26	FUTURE APPLICATIONS: AI SOC MARKET	112
FIGURE 27	SUCCESS STORIES AND REAL-WORLD APPLICATIONS	118
FIGURE 28	AI SOC MARKET: DECISION-MAKING FACTORS	131
FIGURE 29	INFLUENCE OF STAKEHOLDERS ON BUYING PROCESS FOR TOP THREE VERTICALS	132
FIGURE 30	KEY BUYING CRITERIA FOR TOP THREE VERTICALS	132
FIGURE 31	ADOPTION BARRIERS AND INTERNAL CHALLENGES	134
FIGURE 32	SERVICES SEGMENT TO GROW AT HIGHER CAGR DURING FORECAST PERIOD	138
FIGURE 33	AI SOC AGENT SOLUTIONS SEGMENT TO GROW AT HIGHER CAGR DURING FORECAST PERIOD	141

JULY 2026 © MarketsandMarkets™

FIGURE 34	AI SOC-AS-A-SERVICE (SOCAAS) SEGMENT TO GROW AT HIGHER CAGR DURING FORECAST PERIOD	153
FIGURE 35	LARGE ENTERPRISES SEGMENT TO ACCOUNT FOR LARGER MARKET DURING FORECAST PERIOD	161
FIGURE 36	THREAT DETECTION AND MONITORING SEGMENT TO ACCOUNT FOR LARGEST MARKET BY 2031	167
FIGURE 37	HEALTHCARE & LIFE SCIENCES VERTICAL TO ACHIEVE FOR HIGHEST CAGR DURING FORECAST PERIOD	185
FIGURE 38	ASIA PACIFIC TO REGISTER HIGHEST CAGR DURING FORECAST PERIOD	202
FIGURE 39	NORTH AMERICA: AI SOC MARKET SNAPSHOT	205
FIGURE 40	ASIA PACIFIC: AI SOC MARKET SNAPSHOT	252
FIGURE 41	SEGMENTAL REVENUE ANALYSIS OF KEY PLAYERS, 2022–2025 (USD MILLION)	338
FIGURE 42	SHARE OF LEADING COMPANIES IN AI SOC MARKET, 2025	339
FIGURE 43	AI SOC MARKET: COMPARISON OF VENDORS' BRANDS/PRODUCTS	342
FIGURE 44	COMPANY VALUATION, 2025 (USD BILLION)	343
FIGURE 45	EV/EBIDTA, 2025	344
FIGURE 46	AI SOC MARKET: COMPANY EVALUATION MATRIX (KEY PLAYERS), 2025	346
FIGURE 47	AI SOC MARKET: COMPANY FOOTPRINT, 2025	347
FIGURE 48	AI SOC MARKET: COMPANY EVALUATION MATRIX (STARTUPS/SMES), 2025	352
FIGURE 49	MICROSOFT: COMPANY SNAPSHOT	373
FIGURE 50	CISCO: COMPANY SNAPSHOT	381
FIGURE 51	CROWDSTRIKE: COMPANY SNAPSHOT	388
FIGURE 52	PALO ALTO NETWORKS: COMPANY SNAPSHOT	396
FIGURE 53	GOOGLE: COMPANY SNAPSHOT	403
FIGURE 54	IBM: COMPANY SNAPSHOT	429
FIGURE 55	FORTINET: COMPANY SNAPSHOT	435
FIGURE 56	ELASTIC: COMPANY SNAPSHOT	445
FIGURE 57	RAPID7: COMPANY SNAPSHOT	450
FIGURE 58	SENTINELONE: COMPANY SNAPSHOT	455
FIGURE 59	AI SOC MARKET: RESEARCH DESIGN	489
FIGURE 60	BREAKUP OF PRIMARY PROFILES, BY COMPANY TYPE, DESIGNATION, AND REGION	491
FIGURE 61	KEY INSIGHTS FROM INDUSTRY	491
FIGURE 62	DATA TRIANGULATION	492
FIGURE 63	AI SOC MARKET: RESEARCH FLOW	493
FIGURE 64	APPROACH 1 (SUPPLY-SIDE ANALYSIS): REVENUE OF SOFTWARE PLATFORMS/SERVICES IN AI SOC MARKET	494
FIGURE 65	MARKET SIZE ESTIMATION METHODOLOGY: APPROACH 1, SUPPLY-SIDE ANALYSIS	495
FIGURE 66	APPROACH 2, BOTTOM-UP (SUPPLY SIDE): COLLECTIVE REVENUE FROM ALL OFFERINGS IN AI SOC MARKET	495
FIGURE 67	MARKET SIZE ESTIMATION METHODOLOGY (TOP-DOWN APPROACH): DEMAND-SIDE ANALYSIS	496
FIGURE 68	LIMITATIONS & RISK ASSESSMENT	499

JULY 2026 © MarketsandMarkets™

LIST OF ABBREVIATIONS

ABBREVIATION	FULL FORM
AI	Artificial Intelligence
AI RMF	AI Risk Management Framework
AIMS	Artificial Intelligence Management System
AISI	AI Security Institute
AMI	Advanced Metering Infrastructure
APCERT	Asia Pacific Computer Emergency Response Team
APTs	Advanced Persistent Threats
ATOM	Autonomous Threat Operations Machine
AU	African Union
BEC	Business Email Compromise
BFSI	Banking, Financial Services, and Insurance
BIS	Bank for International Settlements
BYOML	Bring Your Own ML
CAD	Canadian Dollar
CAISI	Center for AI Standards and Innovation
CEO	Chief Executive Officer
CESER	Cybersecurity, Energy Security, and Emergency Response
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officers
CRA	Cyber Resilience Act
CREATE	Center for Research on AI Security and Technology Evolution
CSA	Cloud Security Alliance
CSF	Cybersecurity Framework

JULY 2026 © MarketsandMarkets™

CTDR	Cloud Threat Detection and Response
CTEM	Continuous Threat Exposure Management
DEB	Digital Enterprise Blueprint
DLP	Data Loss Prevention
DORA	Digital Operational Resilience Act
DSIT	Department for Science, Innovation and Technology
DSPM	Data Security Posture Management
ECLAC	Economic Commission for Latin America and the Caribbean
EDPB	European Data Protection Board
EHR	Electronic Health Records
ENISA	European Union Agency for Cybersecurity
ESCO	European Cyber Security Organization
EU	European Union
EUR	Euro
GBP	Great British Pound
GCC	Gulf Cooperation Council
GDP	Gross Domestic Product
GDPL	General Data Protection Law
GRC	Governance, Risk, And Compliance
HHS	Health and Human Services
IAM	Identity And Access Management
ICS	Industrial Control Systems
ICT	Information And Communications Technology
ICTC	Information and Communications Technology Council
IIOT	Industrial Internet of Things
INR	Indian Rupee
IOC	Indicators of Compromise

JULY 2026 © MarketsandMarkets™

IoMT	Internet of Medical Things
IoT	Internet of Things
IR	Incident Response
ISMS	Information Security Management System
ISSA	Information Systems Security Association
IT	Information Technology
ITDR	Identity Threat Detection and Response
ITU	International Telecommunication Union
JPY	Japanese Yen
KSA	Kingdom of Saudi Arabia
LLM	large language models
MDR	Managed Detection and Response
MeitY	Ministry of Electronics and Information Technology
MHRA	Medicines and Healthcare products Regulatory Agency
ML	Machine Learning
MSP	Managed Service Providers
MSSPs	Managed Security Service Providers
NCA	National Cybersecurity Authority
NCCoE	National Cybersecurity Center of Excellence
NCSC	National Cyber Security Centre
NDR	Network Detection and Response
NIST	National Institute of Standards and Technology
NYDFS	New York Department of Financial Services
OAS	Organization of American States
OCSF	Open Cybersecurity Schema Framework
OT	Operational Technology
OWASP	Open Worldwide Application Security Project

JULY 2026 © MarketsandMarkets™

RAG	Retrieval-Augmented Generation
RBI	Reserve Bank of India
SaaS	Software-as-a-Service
SCU	Security Compute Unit
SIEM	Security Information and Event Management
SLA	Service-level Agreement
SMEs	Small and Medium-sized Enterprises
SOAR	Security Orchestration, Automation, And Response
SOC	Security Operations Center
SOCaaS	SOC-as-a-Service
TTPs	Tactics, Techniques, And Procedures
UAE	United Arab Emirates
UEBA	User and Entity Behavior Analytics
VARs	Value-Added Resellers
VP	Vice President
XDR	Extended Detection and Response

JULY 2026 © MarketsandMarkets™

1 INTRODUCTION

1.1 STUDY OBJECTIVES

- To define, describe, and forecast the AI security operations center (SOC) market based on offering, organization size, application, vertical, and region
- To provide detailed information about the major factors (drivers, opportunities, restraints, and challenges) influencing the growth of the market
- To analyze opportunities for stakeholders by identifying the high-growth segments of the market
- To forecast the size of the market segments with respect to five main regions: North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America
- To analyze subsegments of the market with respect to individual growth trends, prospects, and contributions to the overall market
- To profile the key players and comprehensively analyze their market sizes and core competencies
- To track and analyze competitive developments such as product enhancements, new product launches, acquisitions, and partnerships & collaborations in the global market

1.2 MARKET DEFINITION

The AI security operations center (SOC) market comprises software platforms and security services that leverage artificial intelligence (AI), machine learning (ML), generative AI (GenAI), large language models (LLMs), and agentic AI to augment, automate, or autonomously perform SOC functions throughout the cyber threat lifecycle.

1.3 STUDY SCOPE AND SEGMENTATION

The study provides an in-depth analysis of the global AI SOC market from 2022 based on contemporary market trends and developments, as well as its potential growth from 2026 to 2031. It provides detailed market trends, competitive landscape, market size, forecasts, and analysis of the key players in the AI SOC market.

JULY 2026 © MarketsandMarkets™

1.3.1 MARKET SEGMMENTATION & REGION COVERAGE

FIGURE 1 MARKET SEGMENTATION AND REGIONS COVERED



Notes:

Other verticals include transportation & logistics, travel & hospitality, real estate & construction, professional and business services, legal services, agriculture, and nonprofit organizations.

Rest of Europe includes the Netherlands, Spain, Sweden, and other countries.

Rest of Asia Pacific includes Australia, South Korea, Singapore, and other countries.

Rest of GCC countries include Bahrain, Kuwait, Oman, and Qatar

Rest of Middle East includes Israel, Egypt, Jordan, Turkey, and other countries.

Rest of Latin America includes Colombia, Chile, Costa Rica, Peru, and other countries.

Source: MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

1.3.2 INCLUSIONS AND EXCLUSIONS

CATEGORY	INCLUSION	EXCLUSION
Market Boundary	Includes commercially available software solutions/platforms and services that materially apply artificial intelligence, machine learning, generative AI, behavioral analytics, or autonomous agents to SOC activities Covered activities include security monitoring, threat detection, alert triage, investigation, threat hunting, incident response, security-data analysis, threat intelligence, and SOC-focused compliance operations	Excludes conventional SOC tools without material AI functionality, internal security-team expenditure, internally developed SOC tools, general cybersecurity products, physical security operations, fraud operations, IT operations, and technologies used primarily to protect AI models, applications, or training data
Offering: Solutions	Includes commercially licensed AI SOC software, platforms, modules, and agent-based solutions used to support or automate detection, analysis, investigation, threat hunting, response, security-data management, threat intelligence, and SOC-focused governance activities	Excludes hardware-only products, conventional security software without material AI functionality, general-purpose analytics platforms, internal software development, and standalone cybersecurity products that do not support centralized SOC workflows
Solution: AI-enabled detection and analytics platforms	Includes AI-enabled SIEM platforms, security analytics platforms, UEBA solutions, anomaly-detection platforms, and the investigation and correlation components of XDR platforms Also includes AI-based malware, phishing, and behavioral analysis used within SOC workflows	Excludes endpoint protection and prevention, standalone EDR, NDR, email security, network security, cloud workload protection, vulnerability management, and other point-security products For bundled XDR offerings, only the detection, correlation, investigation, and SOC-workflow portion is included
Solution: AI-orchestrated response and automation platforms	Includes AI-enabled SOAR, security hyperautomation, playbook automation, case-management automation, detection-engineering automation, workflow orchestration, and automated response platforms used by SOC teams	Excludes general IT workflow automation, robotic process automation, business-process automation, vulnerability-remediation platforms, general GRC automation, and autonomous analyst agents classified under AI SOC agent solutions
Solution: AI-native SOC platforms	Includes converged AI-native platforms commercially positioned as unified replacements for multiple SOC tools, such as SIEM, SOAR, security analytics, XDR investigation, case management, and automated response systems	Excludes individual SIEM, SOAR, XDR, UEBA, or security analytics products that are not sold as converged SOC platforms Standalone AI copilots and agents are classified under AI SOC agent solutions rather than this segment
Solution: AI SOC agent solutions	Includes SOC-focused AI copilots, generative AI assistants, autonomous SOC analysts, multi-agent security systems, and agentic threat-hunting solutions that support or independently conduct alert triage, evidence collection, investigation, incident summarization, query generation, response recommendation, or approved remediation	Excludes general-purpose enterprise copilots, foundation-model platforms, internally developed chatbots, conventional SOAR platforms, customer-service AI agents, and AI security products designed primarily to protect AI models and applications

JULY 2026 © MarketsandMarkets™

Solution: Security data platforms	Includes separately licensed security data lakes, telemetry pipelines, security-data routing platforms, data-federation layers, normalization engines, and security-specific data platforms used to collect, prepare, route, and retain telemetry for AI SOC operations	Excludes generic cloud storage, data warehouses, lakehouses, database platforms, observability-data platforms, and storage functionality bundled within SIEM or AI-native SOC contracts without separate commercial value
Solution: Threat intelligence platforms	Includes standalone threat intelligence platforms, intelligence-enrichment systems, malware intelligence platforms, adversary intelligence tools, threat investigation platforms, and AI-enabled systems used to collect, correlate, prioritize, and operationalize threat intelligence within SOC workflows	Excludes raw threat feeds embedded within firewalls, email-security products, endpoint-security products, and other point solutions Standalone digital-risk protection, brand monitoring, executive monitoring, and external attack-surface monitoring are excluded unless directly integrated with SOC threat-intelligence operations
Solution: AI governance, risk, and compliance solutions	Includes AI-enabled compliance monitoring, control mapping, evidence collection, reporting, regulatory-impact analysis, and governance capabilities purchased and used within an SOC or security-operations context	Excludes general-purpose enterprise GRC suites, audit-management platforms, third-party risk management, privacy-management software, ESG reporting, policy-management systems, and compliance products not directly associated with security operations
Offering: Services	Includes externally delivered services that materially use AI-enabled platforms, analytics, automation, or agents to provide managed detection, outsourced SOC operations, incident response, digital forensics, threat intelligence, and SOC advisory support	Excludes general IT outsourcing, non-AI security monitoring, standalone implementation of out-of-scope cybersecurity tools, physical security services, security staffing without managed outcomes, and consulting engagements unrelated to AI-enabled security operations
Service: AI-augmented managed detection and response (MDR)	Includes vendor-delivered monitoring, AI-assisted detection, alert triage, investigation, managed threat hunting, and response support using the service provider's security platform, telemetry stack, or managed detection technology	Excludes endpoint-protection license revenue embedded in MDR bundles, unmanaged EDR, standalone incident-response retainers, basic alert forwarding, and conventional managed security services without material AI-enabled detection or investigation
Service: AI SOC-as-a-Service (SOCaaS)	Includes fully or substantially outsourced SOC operations delivered across the customer's existing security technology environment Covered activities may include continuous monitoring, alert management, investigation, threat hunting, case management, reporting, and response coordination	Excludes staff augmentation, temporary SOC staffing, basic managed SIEM administration, help-desk services, general IT outsourcing, and vendor-telemetry-led MDR services classified separately under AI-augmented MDR

JULY 2026 © MarketsandMarkets™

Service: Incident response and forensics services	Includes AI-assisted incident-response retainers, breach investigation, digital forensics, malware analysis, compromise assessment, root-cause analysis, evidence reconstruction, and remediation support delivered through or alongside AI SOC platforms	Excludes crisis public relations, cyber-insurance services, legal representation, litigation support, insurance claims management, physical investigations, and conventional forensics work without a direct cybersecurity incident-response component
Service: Threat intelligence and advisory services	Includes human-delivered threat intelligence, adversary analysis, intelligence reporting, managed intelligence, SOC transformation consulting, AI SOC implementation, operating-model design, threat-hunting advisory, and security-operations optimization services	Excludes standalone threat-intelligence software subscriptions, general cybersecurity strategy, generic IT consulting, audit-only engagements, security-awareness training, and advisory work not directly related to AI SOC implementation or operation
Application: Threat detection and monitoring	Includes continuous analysis of endpoint, identity, network, cloud, application, email, and other security telemetry to identify malicious activity, anomalous behavior, indicators of compromise, and emerging attack patterns	Excludes preventive security controls, infrastructure availability monitoring, application-performance monitoring, physical surveillance, fraud monitoring, and detection performed solely within standalone point-security products
Application: Alert triage and prioritization	Includes AI-based alert deduplication, clustering, suppression, enrichment, classification, severity scoring, risk prioritization, false-positive reduction, and assignment of alerts for analyst review	Excludes alert generation without prioritization, generic IT ticket routing, customer-service case classification, and manual triage activities not delivered through an AI-enabled SOC product or service
Application: Incident investigation and analysis	Includes AI-assisted evidence gathering, event correlation, attack-chain reconstruction, root-cause analysis, timeline generation, query generation, case summarization, entity analysis, and investigation of affected users, assets, or workloads	Excludes legal e-discovery, non-cyber forensic investigations, general data analytics, fraud investigations, and incident analysis performed outside cybersecurity operations
Application: Threat hunting	Includes proactive AI-assisted or agentic searching for hidden threats, suspicious behaviors, compromised identities, malicious persistence, lateral movement, and previously undetected attack activity across security telemetry	Excludes penetration testing, red teaming, breach and attack simulation, vulnerability scanning, bug-bounty programs, and standalone offensive-security services
Application: Incident response and remediation	Includes AI-generated response recommendations, automated or analyst-approved containment, account suspension, endpoint isolation, malicious-process termination, blocking actions, case escalation, and remediation workflow orchestration	Excludes disaster recovery, business-continuity management, general IT remediation, patch-management platforms, backup restoration, and response actions performed solely by out-of-scope point-security products

JULY 2026 © MarketsandMarkets™

Application: Insider threat detection	Includes AI-enabled analysis of user and entity behavior to identify compromised accounts, malicious insiders, abnormal access, unusual data activity, privilege misuse, and suspicious employee or contractor behavior within SOC workflows	Excludes employee productivity monitoring, workplace surveillance, human-resource investigations, standalone DLP, general insider-risk management, and physical access monitoring not integrated with cybersecurity operations
Application: Cloud security monitoring	Includes SOC monitoring and analysis of cloud logs, workload telemetry, cloud identities, configuration events, API activity, containers, serverless environments, and cloud-based security alerts	Excludes standalone CNAPP, CSPM, CWPP, CIEM, cloud vulnerability management, cloud infrastructure management, and posture-management revenue not directly attributable to SOC monitoring and investigation
Application: Identity and access monitoring	Includes monitoring of authentication events, account activity, privilege use, access anomalies, credential compromise, impossible travel, session risks, and identity-based attacks within SOC detection and investigation workflows	Excludes standalone IAM, IGA, PAM, access provisioning, single sign-on, multifactor authentication, password management, and identity administration platforms
Application: Compliance monitoring and reporting	Includes continuous security-control monitoring, automated evidence collection, SOC reporting, incident documentation, audit-support reporting, regulatory mapping, and AI-assisted compliance analysis performed within security operations	Excludes enterprise-wide GRC, financial audit, privacy compliance, ESG reporting, policy administration, third-party risk management, and regulatory consulting unrelated to SOC activities
Application: Security analytics and visualization	Includes AI-enabled SOC dashboards, security-data exploration, attack timelines, relationship graphs, risk visualization, incident trends, analyst workbenches, and visualization of correlated security events	Excludes generic business intelligence, enterprise reporting, data-science platforms, observability dashboards, application analytics, and visualization tools not designed for cybersecurity operations
Geographic Revenue Attribution	Revenue is assigned according to the location of the end-user customer or the primary location where the AI SOC solution or service is consumed. Cross-border contracts are allocated across regions where a defensible customer or consumption split is available	Excludes allocation based solely on the vendor's headquarters, incorporation country, development center, cloud region, or service-delivery location Unallocated global revenue must not be assigned entirely to a single region
Market Sizing and Revenue Attribution	Includes only the portion of product, subscription, license, usage, professional-service, and managed-service revenue directly attributable to in-scope AI SOC functionality Products are assigned to one primary offering category to prevent double counting	Excludes total company revenue, total cybersecurity revenue, unrelated platform revenue, internal SOC expenditure, channel markups already included in vendor revenue, and the endpoint, network, identity, email, cloud-posture, vulnerability, or other out-of-scope portions of bundled contracts

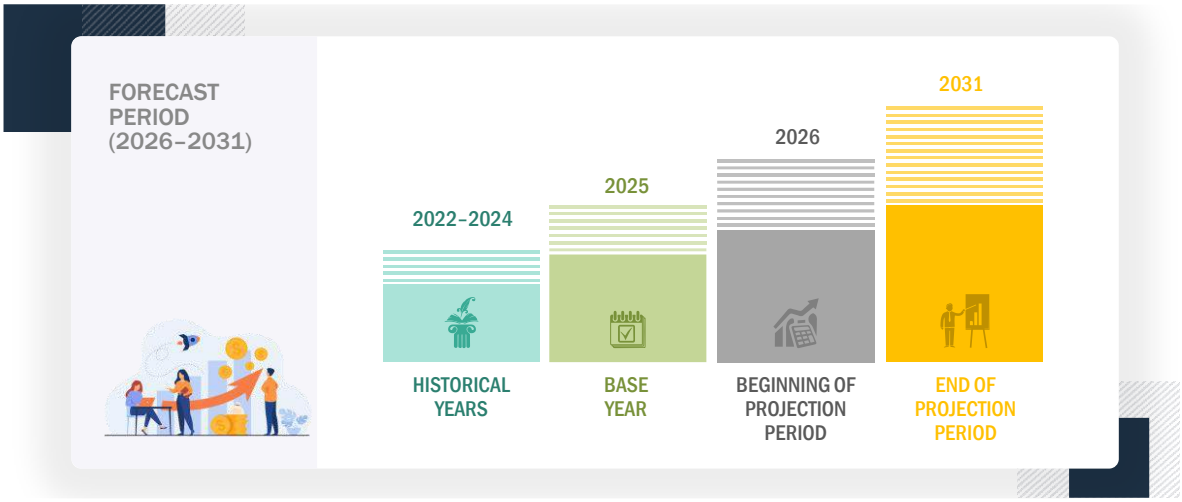
JULY 2026 © MarketsandMarkets™

Company Profile	Includes vendors offering commercially available AI SOC software, platforms, agents, managed services, incident-response services, threat-intelligence services, or advisory services with identifiable market participation and attributable revenue Both diversified cybersecurity vendors and specialist AI SOC providers are covered	Excludes distributors, resellers without proprietary offerings, non-commercial research projects, open-source communities without commercial monetization, staffing-only firms, pure hardware suppliers, general IT consultants, and companies offering only out-of-scope cybersecurity products

Source: Secondary Literature and MarketsandMarkets Analysis

1.3.3 YEARS CONSIDERED

FIGURE 2 STUDY YEARS CONSIDERED



Source: MarketsandMarkets Analysis and Secondary Research

- The projection period considered for this study is 2026–2031.
- The financial year considered for all company profiles is 2025.
- The period considered for the study of the competitive landscape spans from January 2024 to July 2026.

1.4 CURRENCY CONSIDERED

The currency used in the report is the US dollar, with the market size indicated in USD million/billion.

- ISO 4217 codes depict currency names; the market size is represented using USD.
- The market has been studied in terms of USD million, with specific values provided in USD billion. The denomination is based on the size of the values, enabling uniform accommodation of these values within the tables, figures, or segments.
- The data has been taken from companies' annual reports reporting their revenues in USD.
- For companies that reported their revenue in a currency other than USD, the average annual currency conversion rate used for that particular year has been taken from the US IRS to convert into USD values.

JULY 2026 © MarketsandMarkets™

TABLE 1 USD EXCHANGE RATES, 2022–2025

Currency	2022	2023	2024	2025
Euro (EUR)	1.06	1.10	1.09	1.17
Indian Rupee (INR)	0.012	0.012	0.012	0.012
Great British Pound (GBP)	1.20	1.27	1.25	1.34
Canadian Dollar (CAD)	0.73	0.75	0.75	0.73
Japanese Yen (JPY)	0.007	0.007	0.007	0.007

Source: Oanda.com

1.5 STAKEHOLDERS

- Chief Information Security Officers (CISOs) & Security Leaders
- Security Operations Center (SOC) Teams & Security Analysts
- Information Technology (IT) & Cybersecurity Professionals
- Government Agencies & Critical Infrastructure Operators
- Small and Medium-sized Enterprises (SMEs) and Large Enterprises
- Managed Security Service Providers (MSSPs)
- Managed Detection and Response (MDR) Providers
- AI SOC Platform Vendors
- SIEM, SOAR, XDR & EDR Solution Providers
- Threat Intelligence Platform Providers
- Cloud Service Providers (AWS, Microsoft Azure, Google Cloud)
- AI Infrastructure & GPU Providers
- System Integrators & Cybersecurity Consulting Firms
- Technology Channel Partners & Value-Added Resellers (VARs)
- Compliance, Risk & Governance Professionals
- Investors & Venture Capital Firms
- Industry Analysts & Research Organizations
- Telecommunications & Digital Infrastructure Providers
- Third-Party Security Service Providers
- Enterprise Software & Identity Security Vendors (IAM/PAM) table of contents

JULY 2026 © MarketsandMarkets™

2 EXECUTIVE SUMMARY

2.1 MARKET HIGHLIGHTS AND KEY INSIGHTS

Artificial intelligence security operations center (AI SOC) solutions enable organizations to transform traditional security operations by integrating artificial intelligence, machine learning, generative AI, automation, and advanced analytics into cybersecurity monitoring and response processes. These solutions provide organizations with intelligent capabilities for continuous threat detection, security alert prioritization, automated investigation, threat intelligence analysis, incident response orchestration, and proactive threat hunting across complex digital environments. By combining AI-driven analytics, behavioral monitoring, security automation, and real-time decision support, AI SOC platforms help organizations improve threat visibility, reduce analyst workload, accelerate incident response, and strengthen overall cyber resilience against evolving security threats.

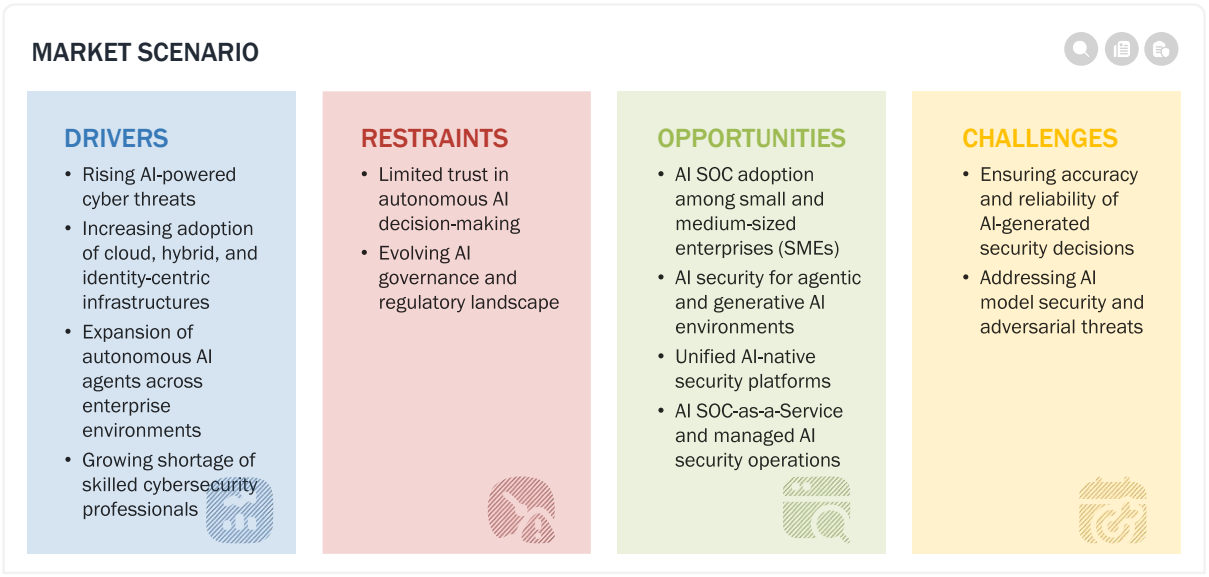
The AI SOC market is experiencing significant growth, driven by increasing sophistication of cyberattacks, rising security alert volumes, growing adoption of cloud and hybrid infrastructures, expansion of digital transformation initiatives, and increasing demand for automated cybersecurity operations. Organizations across industries are increasingly adopting AI-enabled SOC capabilities to address challenges associated with traditional security operations, including alert fatigue, shortage of skilled cybersecurity professionals, delayed threat investigation, and the inability to analyze large-scale security telemetry in real time. Furthermore, the growing use of generative AI, autonomous AI agents, and machine learning technologies in cybersecurity is accelerating the transition toward intelligent and autonomous security operations models.

Modern AI SOC platforms are evolving beyond conventional SOC automation tools by enabling autonomous investigation, AI-assisted decision-making, security workflow orchestration, and adaptive threat response capabilities. Advancements in large language models (LLMs), generative AI security assistants, agentic AI, behavioral analytics, and extended security intelligence are allowing organizations to build more proactive and efficient security operations environments. These technologies enable security teams to correlate diverse data sources, identify emerging threats, automate repetitive tasks, and improve response accuracy while maintaining human oversight for complex security decisions.

Key adoption of AI SOC solutions spans large enterprises, small and medium-sized enterprises (SMEs), government agencies, and managed security service providers (MSSPs) across industries including banking and financial services, healthcare and life sciences, manufacturing, retail and e-commerce, energy and utilities, telecommunications, transportation, and public sector organizations. As organizations continue expanding cloud environments, connected digital ecosystems, and AI-driven business applications, AI SOC solutions are becoming a critical component of next-generation cybersecurity strategies. They play an essential role in enabling proactive threat detection, automated response, operational efficiency, regulatory compliance, and improved cyber resilience within an increasingly complex and AI-driven threat landscape.

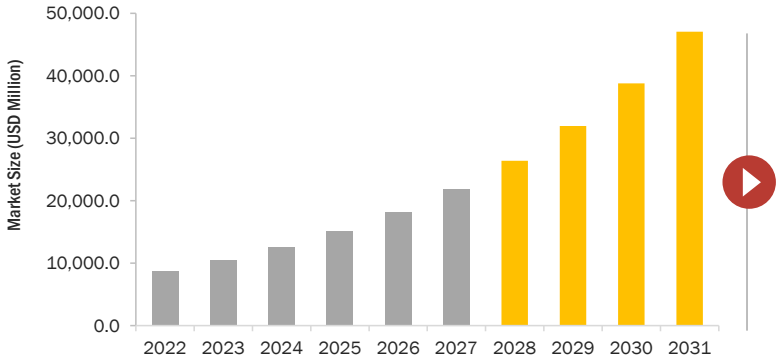
JULY 2026 © MarketsandMarkets™

FIGURE 3 MARKET SCENARIO



Source: Interviews with Experts, Secondary Research, and MarketsandMarkets Analysis

FIGURE 4 GLOBAL AI SOC MARKET, 2022–2031 (USD MILLION)



21.1%

Demand in the AI SOC market is driven by the growing need to detect and respond to advanced cyber threats in real time, automate security operations with AI, reduce analyst workload, strengthen cyber resilience, and secure hybrid, multi-cloud, and AI-powered enterprise environments across BFSI, healthcare & life sciences, manufacturing, government & defense, and other critical industries.

According to MarketsandMarkets, the global AI SOC market is projected to reach USD 47,066.1 million by 2031, registering a CAGR of 21.1% during the forecast period.

The AI SOC market growth is driven by the increasing demand for intelligent, automated, and scalable cybersecurity operations across enterprises, governments, and managed security service providers. Organizations are increasingly adopting AI SOC solutions to improve threat detection accuracy, automate security investigations, prioritize alerts, enhance incident response capabilities, and reduce the operational burden on security teams. The growing volume and sophistication of cyber threats, including ransomware, advanced persistent threats (APTs), phishing attacks, and AI-powered cyberattacks, are further accelerating demand for AI-driven security operations platforms, threat intelligence solutions, security analytics, and automated response capabilities. Additionally, rapid digital transformation initiatives and expanding adoption of cloud computing, hybrid infrastructure, Internet of Things (IoT), and connected digital ecosystems are creating significant opportunities for AI SOC deployment across banking and financial services, healthcare, manufacturing, retail and e-commerce, telecommunications, government, energy, and critical infrastructure sectors.

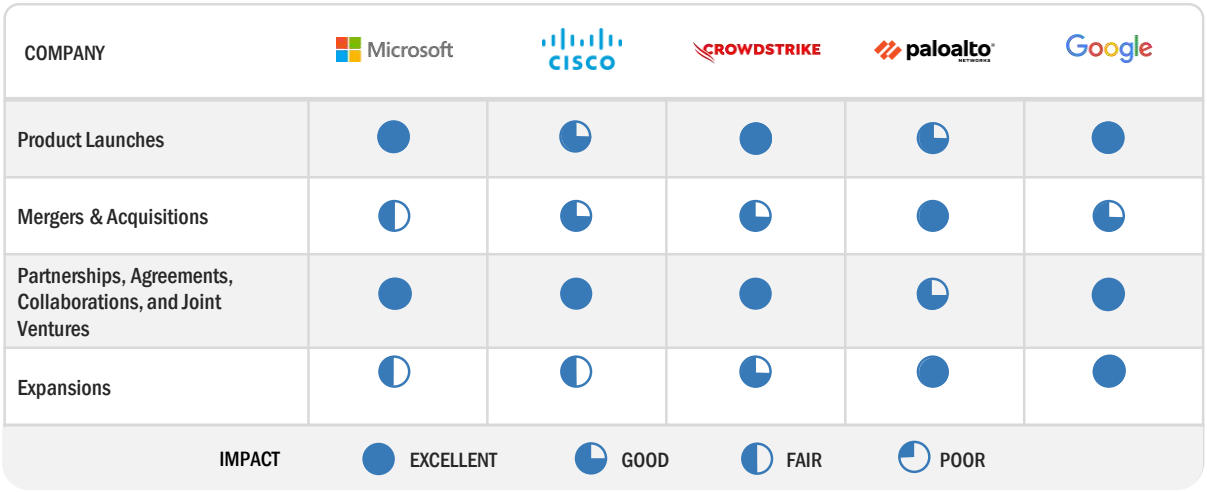
The integration of AI SOC platforms with emerging technologies such as generative AI, large language models (LLMs), autonomous AI agents, extended detection and response (XDR), security information and event management (SIEM), and security orchestration, automation, and response (SOAR) is enabling

JULY 2026 © MarketsandMarkets™

organizations to develop more proactive, adaptive, and autonomous cybersecurity environments. Advancements in AI-driven threat hunting, behavioral analytics, natural language processing, automated investigation workflows, and autonomous remediation capabilities are improving security operations efficiency and supporting broader enterprise adoption. Growing investments in cybersecurity modernization, increasing regulatory requirements for cyber resilience, and rising demand for continuous monitoring and automated defense mechanisms are also contributing to market growth. While North America and Europe continue to dominate the market due to mature cybersecurity ecosystems, strong presence of AI security vendors, advanced cloud adoption, and stringent cybersecurity regulations, Asia Pacific is expected to witness significant growth driven by rapid digitalization, expanding enterprise AI adoption, increasing cyber threat exposure, and government-led cybersecurity modernization initiatives across emerging economies.

2.2 KEY MARKET PARTICIPANTS: MAPPING OF STRATEGIC DEVELOPMENTS

FIGURE 5 MAJOR STRATEGIES ADOPTED BY KEY PLAYERS IN AI SOC MARKET, 2022–2026



Source: Interviews with Experts, Secondary Research, and MarketsandMarkets Analysis

Major participants in the AI SOC market include Microsoft, Cisco, CrowdStrike, Palo Alto Networks, Google, Sophos, IBM, Fortinet, Arctic Wolf, Elastic, Rapid7, SentinelOne, Lumu Technologies, ReliaQuest, Exabeam, eSentire, Expel, Huntress, UnderDefense, Swimlane, Stellar Cyber, Radiant Security, Torq, Intezer, Conifers.AI, Dropzone AI, Simbian, Prophet Security, Legion Security, CyberSilo, Bricklayer AI, Augur, BlinkOps, Gruve, CyberNX, Anvilogic, AIStrike, D3 Security, Exaforce, RiverSafe, SOC Jedi.AI, Vulnuris among others. The AI SOC market is characterized by a moderate level of market concentration, with established cybersecurity vendors, cloud security providers, SIEM/XDR platform providers, and AI-native security companies accounting for a significant share of the market. Their competitive strength is driven by advanced artificial intelligence capabilities, extensive security telemetry, threat intelligence ecosystems, enterprise customer bases, and the ability to integrate AI-driven automation across security operations workflows. Market differentiation is based on offerings such as AI-powered threat detection, automated alert triage, security investigation copilots, autonomous response capabilities, generative AI assistants, threat intelligence integration, and AI-native SOC platforms. Vendors with scalable architectures, broad security integrations, strong automation frameworks, and proven enterprise deployments are better positioned to expand their market presence.

Barriers to entry remain relatively high due to significant investments required in artificial intelligence development, cybersecurity expertise, large-scale security data processing capabilities, integration with existing security ecosystems, regulatory compliance requirements, and the need to ensure accuracy and reliability of automated security decisions. As enterprise adoption of AI-driven security operations

JULY 2026 © MarketsandMarkets™

accelerates, leading companies continue to invest in generative AI security assistants, autonomous SOC capabilities, AI-powered threat intelligence, security orchestration and automation, and strategic partnerships to enhance innovation, improve operational efficiency, and strengthen their competitive position in the global AI SOC market.

The figure highlights the strategic developments of leading AI SOC market participants, with Microsoft, CrowdStrike, and Google demonstrating particularly strong momentum in product launches and strategic partnerships, reflecting their continued investments in AI-native security operations, agentic AI, and autonomous SOC platforms. Cisco and Palo Alto Networks also maintain balanced innovation strategies, supported by continuous platform enhancements, ecosystem collaborations, and targeted acquisitions that strengthen their AI-powered security portfolios. Overall, the AI SOC market is characterized by a combination of continuous product innovation, strategic partnerships, mergers and acquisitions, and geographic expansion. Vendors are increasingly focusing on integrating generative AI, AI agents, security automation, and cloud-native security operations while expanding technology alliances to accelerate enterprise adoption, enhance platform interoperability, and strengthen their competitive positioning in the rapidly evolving AI SOC landscape.

2.3 DISRUPTIVE TRENDS SHAPING MARKET

FIGURE 6 DISRUPTIVE TRENDS IMPACTING GROWTH OF AI SOC MARKET



Source: Interviews with Experts, Secondary Research, and MarketsandMarkets Analysis

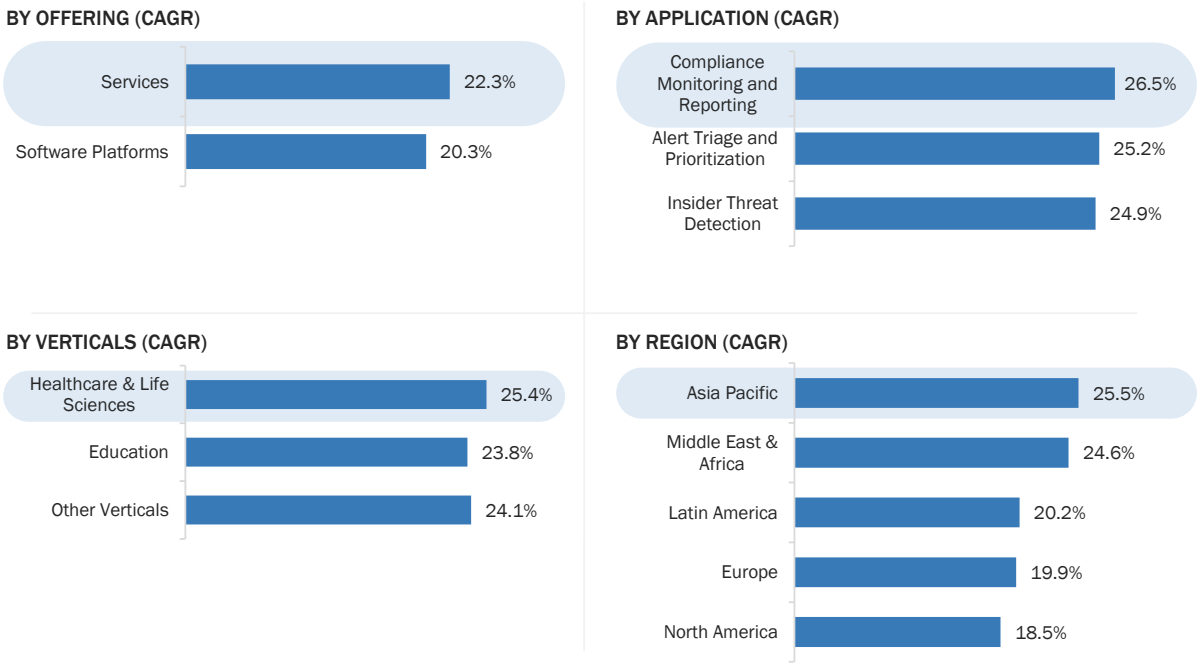
Technological advancements such as autonomous AI agents, generative AI-powered security copilots, AI-native SOC platforms, automated threat hunting, predictive analytics, and AI-driven SOC-as-a-Service offerings are significantly reshaping the AI SOC market. As organizations accelerate digital transformation initiatives through cloud adoption, hybrid infrastructures, identity-centric security models, and expanding digital ecosystems, demand for intelligent, automated, and scalable security operations capabilities continues to increase. Modern AI SOC platforms are leveraging artificial intelligence (AI), machine learning (ML), large language models (LLMs), behavioral analytics, and security automation frameworks to improve threat detection accuracy, accelerate investigation workflows, automate incident response, and enhance analyst productivity. These innovations enable organizations to strengthen cyber resilience while improving operational efficiency, reducing alert fatigue, enhancing threat visibility, and enabling proactive defense against increasingly sophisticated cyber threats.

JULY 2026 © MarketsandMarkets™

At the same time, the rapid expansion of AI-powered cyberattacks, ransomware campaigns, cloud-native environments, generative AI applications, and complex multi-vector attack surfaces is intensifying demand for advanced AI-driven security operations solutions. Growing requirements for real-time threat monitoring, autonomous investigation, continuous compromise assessment, compliance management, and proactive threat hunting are compelling organizations to adopt next-generation AI SOC platforms. Additionally, increasing investments in AI-enabled SIEM, SOAR, XDR, managed detection and response (MDR), security orchestration platforms, and threat intelligence solutions are accelerating market expansion across industries such as banking and financial services, healthcare, government, manufacturing, retail and e-commerce, telecommunications, and energy. As leading providers such as Microsoft, Google, CrowdStrike, Palo Alto Networks, and Lumu Technologies continue to innovate through autonomous SOC capabilities, AI-driven threat detection, security automation, and integrated cyber defense platforms, the competitive landscape is intensifying—creating significant growth opportunities while encouraging organizations to modernize their security operations and transition toward proactive, AI-powered cybersecurity frameworks.

2.4 HIGH-GROWTH SEGMENTS & EMERGING FRONTIERS

FIGURE 7 HIGH-GROWTH SEGMENTS & EMERGING FRONTIERS IN THE AI SOC MARKET, 2026



Source: Interviews with Experts, Secondary Research, and MarketsandMarkets Analysis

The infographic highlights the fastest-growing segments in the AI SOC market during the forecast period, categorized by offering, application, vertical, and region. By offering, the services segment is projected to register the highest CAGR of 22.3%, driven by the growing demand for AI-augmented managed detection and response (MDR), AI SOC-as-a-Service (SOCaaS), incident response, and threat intelligence services as organizations seek expert support to strengthen cyber resilience and address cybersecurity talent shortages. Meanwhile, the software platforms segment continues to witness strong growth as enterprises invest in AI-enabled detection, security automation, AI SOC agents, and AI-native security operations to modernize Security Operations Centers.

By application, compliance monitoring & reporting is expected to record the highest CAGR of 26.5%, fueled by evolving AI governance frameworks, stricter cybersecurity regulations, and the increasing need for continuous compliance monitoring across highly regulated industries. Alert triage & prioritization (25.2%) is

JULY 2026 © MarketsandMarkets™

also witnessing rapid adoption as organizations leverage AI to reduce alert fatigue, improve analyst productivity, and accelerate incident investigations. Additionally, insider threat detection (24.9%) continues to gain traction as enterprises strengthen identity-centric security strategies and deploy behavioral analytics to detect anomalous user activities and mitigate internal security risks.

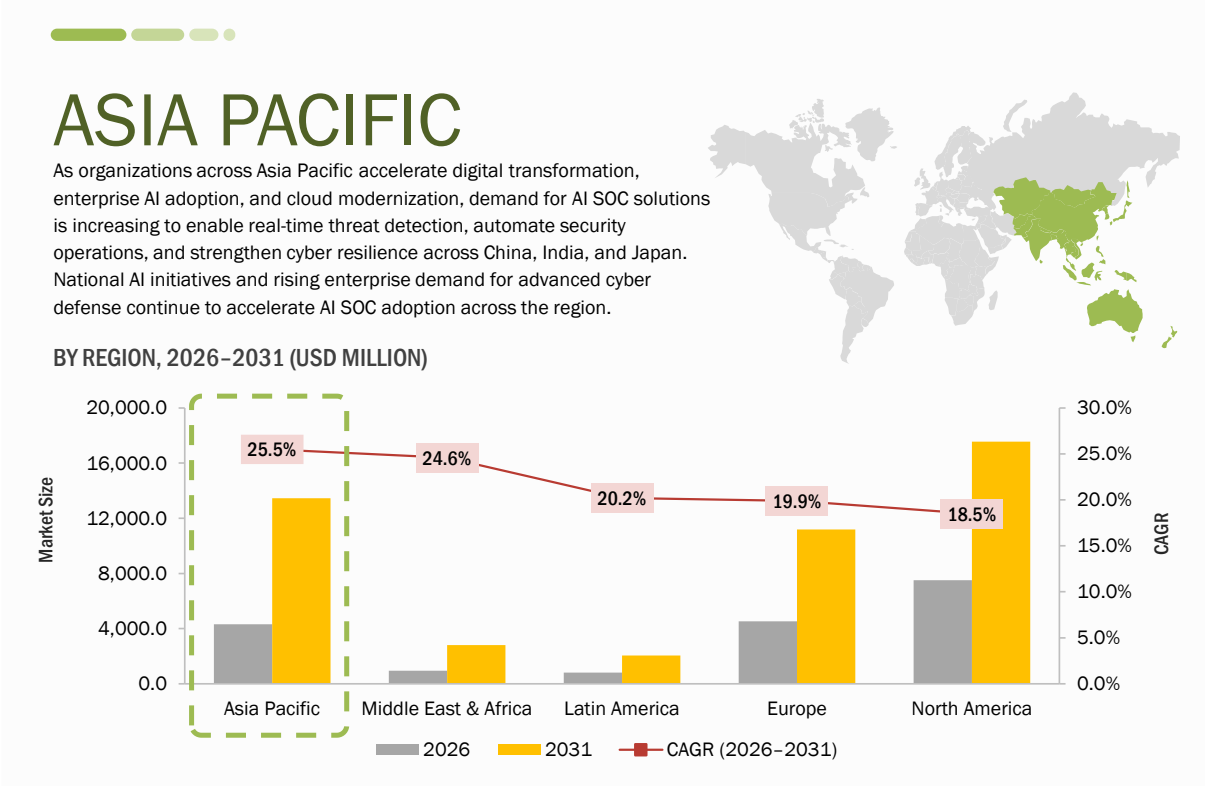
Across industry verticals, the healthcare & life sciences segment is projected to grow at the highest CAGR of 25.4%, driven by the increasing frequency of ransomware attacks, stringent data privacy requirements, and the growing adoption of AI-powered security operations to protect sensitive patient data and connected healthcare environments. Other verticals (24.1%) are also expected to witness strong growth as organizations across diverse industries accelerate AI-driven SOC modernization to address evolving cyber threats. Meanwhile, the education sector (23.8%) is increasingly adopting AI SOC solutions to strengthen cyber resilience, secure digital learning environments, and protect institutional networks from phishing, ransomware, and identity-based attacks.

Regionally, Asia Pacific is projected to register the highest CAGR of 25.5%, supported by rapid digital transformation, expanding enterprise AI adoption, increasing cybersecurity investments, and government-led AI initiatives across major economies. The Middle East & Africa (24.6%) is also witnessing significant growth due to national AI strategies, smart city initiatives, and increasing investments in protecting critical infrastructure. Latin America (20.2%) and Europe (19.9%) continue to demonstrate robust market expansion driven by digital transformation, strengthening AI governance, and rising enterprise cybersecurity investments, while North America (18.5%) maintains steady growth supported by its mature cybersecurity ecosystem, continued innovation in AI-native security operations, and the strong presence of leading AI SOC technology providers. Collectively, these trends underscore the accelerating adoption of AI-driven security operations as organizations worldwide modernize SOCs to combat increasingly sophisticated cyber threats.

JULY 2026 © MarketsandMarkets™

2.5 SNAPSHOT: GLOBAL MARKET SIZE, GROWTH RATE, AND FORECAST

FIGURE 8 ASIA PACIFIC TO REGISTER HIGHEST GROWTH DURING FORECAST PERIOD



Source: Interviews with Experts, Secondary Research, and MarketsandMarkets Analysis

The AI SOC market is witnessing robust global growth, driven by the rapid adoption of AI-native security operations, escalating AI-powered cyber threats, increasing cloud and hybrid infrastructure deployments, and rising enterprise investments in autonomous cybersecurity. Organizations across industries are modernizing Security Operations Centers by integrating generative AI, agentic AI, security automation, and intelligent threat detection to improve cyber resilience and reduce response times. Asia Pacific is projected to register the highest CAGR, supported by rapid digital transformation, expanding AI adoption, increasing cybersecurity investments, and government-led AI initiatives across China, India, Japan, and other Asia Pacific countries. The region's growing technology ecosystem, cloud adoption, and rising cyberattack sophistication are accelerating demand for AI-driven security operations.

North America is expected to account for the largest share of the AI SOC market, owing to its mature cybersecurity ecosystem, early adoption of AI-native security platforms, strong presence of leading vendors such as Microsoft, Google, Cisco, CrowdStrike, Palo Alto Networks, IBM, and SentinelOne, and supportive government initiatives promoting secure AI adoption and cyber resilience. Europe continues to experience strong market growth, driven by stringent cybersecurity regulations, increasing enterprise investments in AI-powered SOC modernization, and growing adoption of Zero Trust and AI governance frameworks. The Middle East & Africa is witnessing significant momentum through national AI strategies, smart city initiatives, and increasing investments in critical infrastructure protection, while Latin America is steadily expanding as organizations accelerate digital transformation and strengthen cyber defenses across financial services, government, healthcare, and critical infrastructure. Together, these regional trends underscore the growing importance of AI SOC platforms in enabling autonomous, intelligent, and resilient security operations across the global enterprise landscape.

JULY 2026 © MarketsandMarkets™

3 PREMIUM INSIGHTS

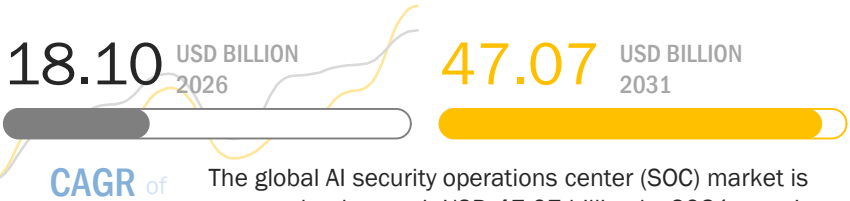
3.1 ATTRACTIVE OPPORTUNITIES FOR PLAYERS IN AI SOC MARKET

FIGURE 9 RISING AI-POWERED CYBER THREATS, AUTONOMOUS SECURITY OPERATIONS, AND ENTERPRISE AI ADOPTION CONTINUE TO DRIVE AI SOC MARKET



North America is estimated to hold the largest market share in 2026, and the Asia Pacific market is projected to register the highest CAGR during the forecast period.





CAGR of 21.1%

The global AI security operations center (SOC) market is expected to be worth USD 47.07 billion by 2031, growing at a CAGR of 21.1% during the forecast period.

The adoption of AI SOC platforms is accelerating due to the growing need for real-time threat detection, intelligent security operations, automated incident response, and cyber resilience, supported by expanding enterprise digital transformation and increasingly sophisticated AI-powered cyber threats.

The growing need to reduce analyst workload, improve threat visibility, accelerate investigations, and automate security workflows is encouraging organizations to deploy AI SOC platforms across BFSI, healthcare & life sciences, manufacturing, government & defense, and other critical industries.

Increasing investments in agentic AI, AI-native security platforms, security automation, AI SOC agents, and cloud-native security operations are driving AI SOC market growth globally, supported by expanding enterprise adoption and continuous SOC modernization initiatives.

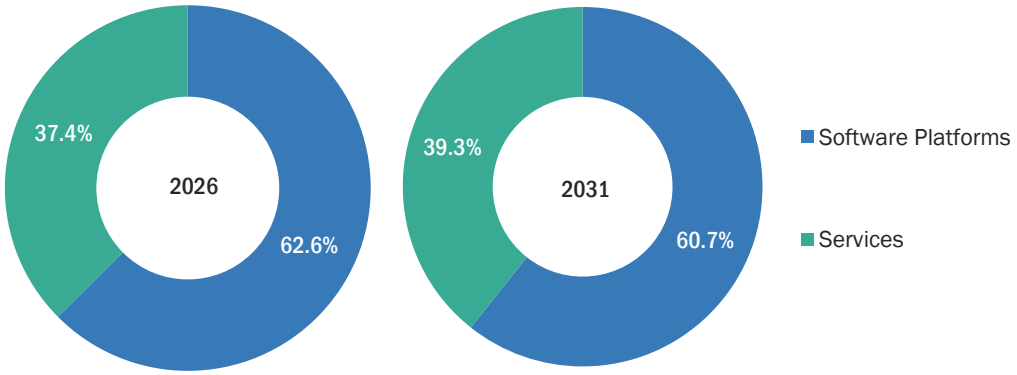
High demand for AI-native security operations, autonomous threat detection, intelligent investigations, unified security platforms, and compliance-driven cyber resilience is driving significant AI SOC market growth, particularly across North America, Europe, and Asia Pacific.

Source: Interviews with Experts, Company Presentations, Associations, Secondary Analysis, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

3.2 AI SOC MARKET, BY OFFERING

FIGURE 10 SOFTWARE PLATFORMS TO ACCOUNT FOR LARGER MARKET SHARE DURING FORECAST PERIOD

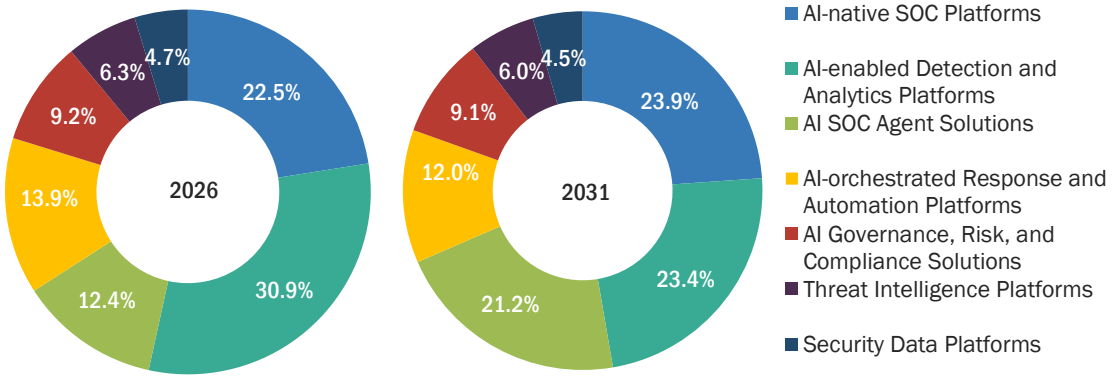


Note: Percentage values indicate the market share of segments in 2026 and 2031

Source: Secondary Literature, Interviews with Experts, and MarketsandMarkets Analysis

3.3 AI SOC MARKET, BY SOFTWARE PLATFORM

FIGURE 11 AI-ENABLED DETECTION & ANALYTICS PLATFORMS TO HOLD HIGHEST MARKET SHARE DURING FORECAST PERIOD



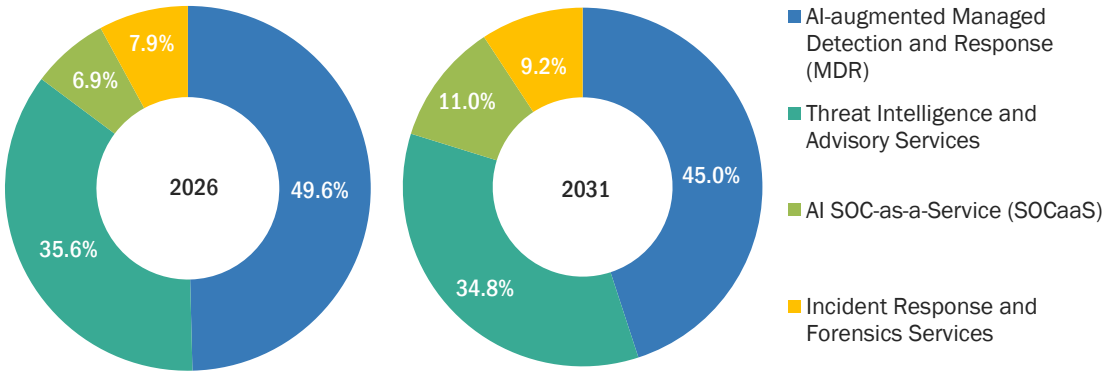
Note: Percentage values indicate the market share of segments in 2026 and 2031

Source: Secondary Literature, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

3.4 AI SOC MARKET, BY SERVICE

FIGURE 12 AI-AUGMENTED MANAGED DETECTION AND RESPONSE (MDR) SEGMENT TO HOLD HIGHEST MARKET SHARE DURING FORECAST PERIOD

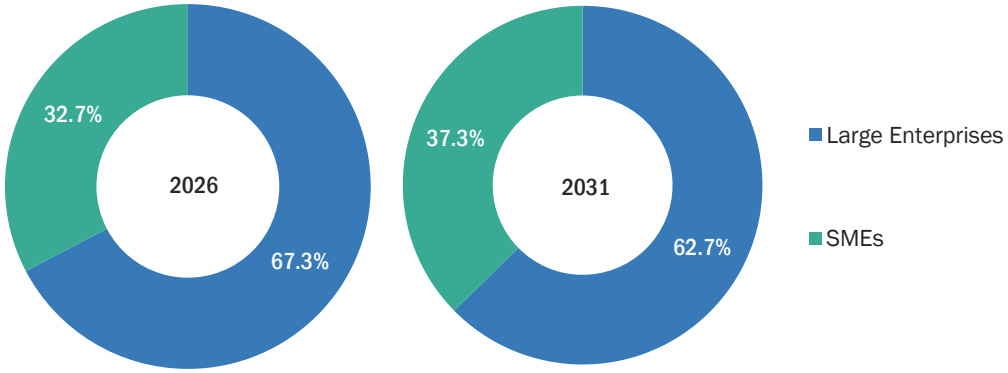


Note: Percentage values indicate the market share of segments in 2026 and 2031

Source: Secondary Literature, Interviews with Experts, and MarketsandMarkets Analysis

3.5 AI SOC MARKET, BY ORGANIZATION SIZE

FIGURE 13 LARGE ENTERPRISES SEGMENT TO HOLD HIGHEST MARKET SHARE DURING FORECAST PERIOD



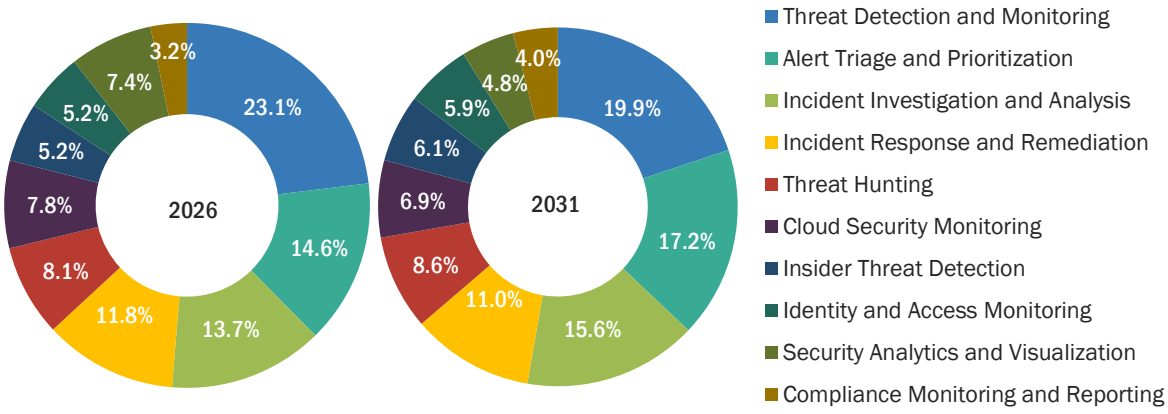
Note: Percentage values indicate the market share of segments in 2026 and 2031

Source: Secondary Literature, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

3.6 AI SOC MARKET, BY APPLICATION

FIGURE 14 THREAT DETECTION & MONITORING SEGMENT TO HOLD HIGHEST MARKET SHARE DURING FORECAST PERIOD

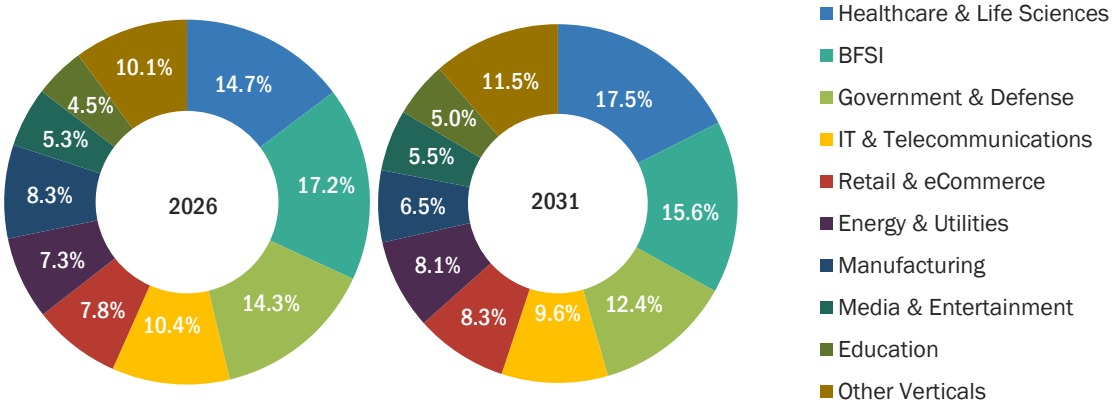


Note: Percentage values indicate the market share of segments in 2026 and 2031

Source: Secondary Literature, Interviews with Experts, and MarketsandMarkets Analysis

3.7 AI SOC MARKET, BY VERTICAL

FIGURE 15 BFSI SEGMENT TO HOLD LARGEST SHARE DURING FORECAST PERIOD



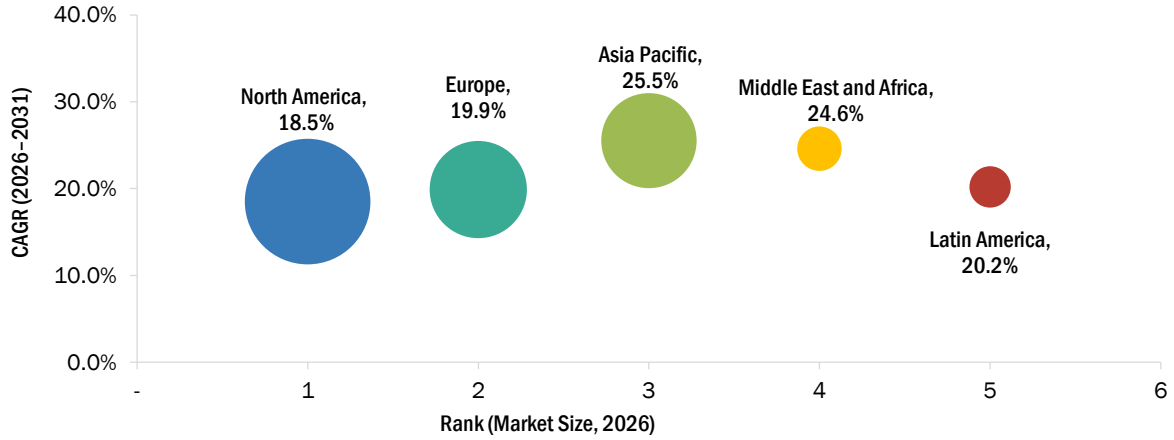
Note: Percentage values indicate the market share of segments in 2026 and 2031

Source: Secondary Literature, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

3.8 AI SOC MARKET, BY REGION

FIGURE 16 NORTH AMERICA TO EMERGE AS MOST SIGNIFICANT MARKET FOR NEXT FIVE YEARS



Note: The bubble size represents the market share of the regions.

Source: Secondary Literature, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

4 MARKET OVERVIEW

4.1 INTRODUCTION

The AI SOC market refers to the global ecosystem of AI-powered security operations platforms and technologies that leverage artificial intelligence, machine learning (ML), generative AI (GenAI), and autonomous agents to enhance cybersecurity monitoring, threat detection, investigation, and incident response. AI SOC solutions combine capabilities such as Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Extended Detection and Response (XDR), Network Detection and Response (NDR), threat intelligence, and AI-driven analytics to help organizations identify, prioritize, and remediate cyber threats with greater speed, accuracy, and operational efficiency. These platforms are increasingly being adopted across industries including BFSI, healthcare, government, manufacturing, retail, energy & utilities, and IT & telecommunications, where continuous security monitoring and rapid incident response are critical.

The market is witnessing rapid evolution as organizations modernize security operations to address increasingly sophisticated cyber threats and expanding digital environments. Key technology trends include the integration of generative AI and agentic AI into SOC workflows, AI-assisted threat hunting, intelligent incident investigation, automated response orchestration, and unified security operations platforms. At the same time, the growing adoption of cloud computing, hybrid IT environments, Zero Trust architectures, and identity-centric security models is increasing the volume and complexity of security telemetry, driving demand for AI-powered platforms capable of correlating data across multiple security domains. These advancements enable organizations to improve analyst productivity, reduce response times, and strengthen overall cyber resilience.

Enterprises are increasingly adopting AI-powered security copilots, autonomous security agents, and AI-native SecOps platforms to improve operational efficiency while addressing evolving cybersecurity challenges. Growing investment in AI-driven security operations, increasing adoption of managed AI SOC services, and the convergence of AI with cloud-native cybersecurity platforms are expected to further accelerate market growth. However, concerns related to AI governance, explainability, integration complexity, and trust in autonomous security decisions continue to influence adoption strategies. Overall, the AI SOC market is poised for significant growth as organizations increasingly embrace intelligent, data-driven, and automated security operations to strengthen cyber defense capabilities.

This chapter discusses the key drivers, opportunities, restraints, and challenges shaping the AI SOC market and highlights their impact. It also provides insights into use cases, value chain analysis, pricing trends, Porter's Five Forces analysis, the impact of 2025 US tariffs, the impact of generative AI, and detailed information on the ecosystem related to the AI SOC market.

4.2 MARKET DYNAMICS

The AI SOC market is expected to witness strong growth during the forecast period, driven by the increasing sophistication of AI-powered cyberattacks, rising security alert volumes, and the growing need for intelligent threat prioritization and response automation. The rapid adoption of cloud, hybrid, and identity-centric infrastructures, along with the expansion of autonomous AI agents across enterprise environments, is further accelerating demand for AI-native security operations platforms.

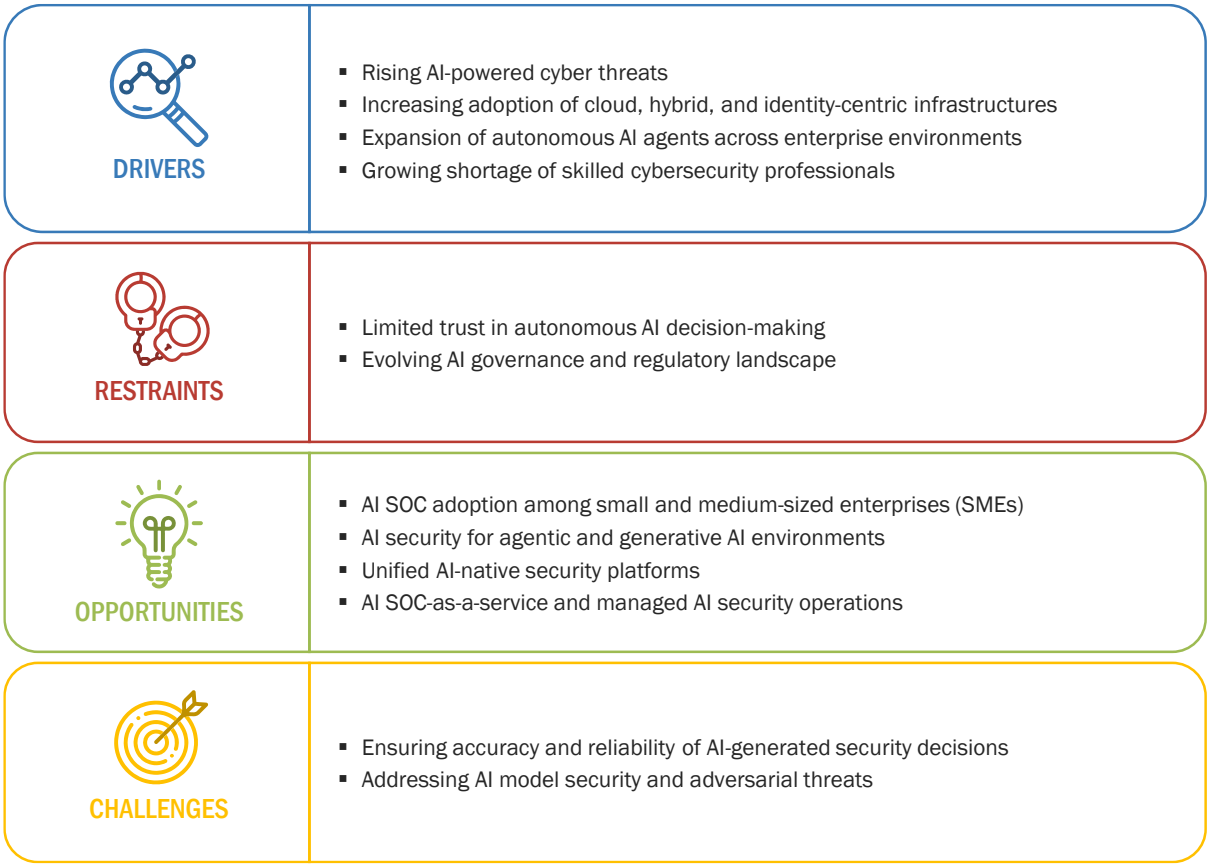
Limited trust in autonomous AI decision-making and the evolving AI governance and regulatory landscape may restrain market growth. Organizations continue to seek greater transparency, explainability, and human oversight before deploying AI for critical security operations, particularly in highly regulated industries.

JULY 2026 © MarketsandMarkets™

At the same time, increasing AI SOC adoption among small and medium-sized enterprises (SMEs), the need to secure agentic and generative AI environments, growing demand for unified AI-native security platforms, and the expansion of AI SOC-as-a-Service are expected to create significant growth opportunities. Despite these opportunities, challenges related to AI model accuracy, integration across heterogeneous security environments, protection of sensitive security data, adversarial attacks targeting AI systems, and balancing autonomous operations with human expertise may affect the pace of market adoption.

The following section highlights the drivers, restraints, opportunities, and challenges in the AI SOC market.

FIGURE 17 AI SOC MARKET: DRIVERS, RESTRAINTS, OPPORTUNITIES, AND CHALLENGES



Source: Secondary Literature, Interviews with Experts, and MarketsandMarkets Analysis

4.2.1 DRIVERS

4.2.1.1 Rising AI-powered cyber threats

The rapid evolution of artificial intelligence is fundamentally changing the cyber threat landscape, driving organizations to modernize security operations through AI-enabled SOCs. Threat actors are increasingly using generative AI and machine learning to automate phishing campaigns, develop sophisticated malware, accelerate reconnaissance, and evade traditional security controls. According to the CrowdStrike 2026 Global Threat Report, AI-enabled adversaries increased their operations by 89% year-over-year, while the average eCrime breakout time dropped to 29 minutes, with the fastest observed breakout occurring in 27 seconds. The report also highlights that attackers are exploiting legitimate generative AI tools and AI development platforms, significantly reducing defenders' response window and increasing the need for autonomous threat detection and response capabilities.

JULY 2026 © MarketsandMarkets™

These evolving threats are accelerating enterprise investment in AI-driven SOC platforms capable of continuously detecting, investigating, and responding to attacks with minimal human intervention. Leading cybersecurity vendors including CrowdStrike, Microsoft, Google Cloud, Palo Alto Networks, and Lumu Technologies have introduced AI-powered security assistants, autonomous investigation capabilities, and agentic SOC solutions to reduce response times and improve operational efficiency. Lumu's Autopilot functions as an autonomous execution layer for security operations, while Microsoft's Security Copilot and CrowdStrike's Charlotte AI automate investigation and remediation workflows. As cyberattacks become increasingly AI-enabled and machine-speed, organizations are transitioning from conventional SOC models to AI-native security operations that deliver continuous monitoring, intelligent decision-making, and automated response at scale.

4.2.1.2 Increasing adoption of cloud, hybrid, and identity-centric infrastructures

The continued expansion of cloud computing, hybrid infrastructure, and identity-based access models is transforming enterprise security requirements and creating demand for AI-native SOC platforms. Organizations increasingly operate across multiple environments, including public clouds, private data centers, SaaS applications, remote endpoints, and distributed workforce ecosystems. This transition has shifted the traditional security perimeter from network boundaries toward identities, applications, and data access patterns. As a result, SOC teams must analyze security signals across multiple technology domains while maintaining visibility into user behavior, privileged access, workload activity, and potential attack paths. AI-powered SOC platforms are gaining importance by enabling organizations to correlate diverse security data sources and generate contextual insights across complex digital environments.

Cybersecurity vendors are responding to this shift by developing integrated AI security platforms that combine identity protection, cloud security, endpoint monitoring, and threat intelligence capabilities. Microsoft has emphasized identity as a central component of modern cybersecurity through integrations between Microsoft Entra, Defender, Sentinel, and Security Copilot. Google Security Operations applies cloud-scale analytics and AI capabilities to improve threat investigation across enterprise environments, while vendors such as Palo Alto Networks, CrowdStrike, Cisco Splunk, and Lumu are expanding platforms that unify security telemetry across multiple domains. The growing complexity of hybrid environments is therefore creating demand for AI SOC solutions capable of connecting fragmented security information and providing a consolidated operational view of enterprise risk.

4.2.1.3 Expansion of autonomous AI agents across enterprise environments

The growing deployment of autonomous AI agents across enterprise functions is creating a new requirement for security operations platforms capable of monitoring and protecting AI-driven workflows. Organizations are increasingly adopting AI agents to perform business activities such as data analysis, software development, customer interactions, and operational decision-making. Unlike traditional software applications, AI agents can independently interpret information, interact with systems, and execute actions based on contextual inputs. This evolution introduces new security considerations involving AI identities, access permissions, autonomous decision-making, and interactions between multiple AI systems. As enterprises expand the use of agentic technologies, AI SOC platforms are expected to become critical for securing these emerging digital ecosystems.

The cybersecurity industry is moving toward agent-based security operations models that extend beyond traditional AI assistance. Microsoft has introduced security agents within Security Copilot that automate specific security tasks, including threat intelligence analysis, phishing investigation, and vulnerability-related workflows. The company has highlighted that Microsoft Threat Intelligence processes 100 trillion signals daily, demonstrating the scale of security data requiring AI-supported analysis. Similarly, Lumu has advanced Autopilot toward an Agentic SOC model focused on autonomous investigation and remediation workflows. As organizations continue adopting AI agents across business operations, demand is expected

JULY 2026 © MarketsandMarkets™

to increase for AI SOC platforms that can provide governance, monitoring, risk assessment, and protection for autonomous systems operating within enterprise environments.

4.2.1.4 Growing shortage of skilled cybersecurity professionals

The persistent shortage of skilled cybersecurity professionals is accelerating the adoption of AI-powered SOCs as organizations seek to maintain effective security operations with limited human resources. Modern SOCs must continuously monitor increasingly complex IT environments, investigate sophisticated attacks, and respond rapidly to evolving threats. However, recruiting and retaining professionals with expertise in cloud security, AI, threat hunting, incident response, and security engineering remains a major challenge. According to the 2025 ISC2 Cybersecurity Workforce Study, cybersecurity organizations are shifting their focus from simply increasing headcount to acquiring specialized skills, with AI (41%) and cloud security (36%) identified as the most pressing capability gaps. These workforce constraints are encouraging enterprises to adopt AI technologies that augment analyst capabilities and improve operational efficiency.

Rather than replacing security professionals, AI SOC platforms are increasingly being deployed to enhance productivity by automating repetitive investigations, accelerating incident analysis, and providing contextual recommendations that allow analysts to focus on high-value security activities. As cybersecurity teams increasingly prioritize advanced technical skills over workforce expansion, AI-powered SOC solutions are emerging as strategic tools for improving operational resilience, reducing manual workloads, and enabling organizations to scale security operations despite ongoing talent constraints.

4.2.2 RESTRAINTS

4.2.2.1 Limited trust in autonomous AI decision-making

The increasing autonomy of AI SOC platforms introduces concerns regarding the reliability, accuracy, and accountability of AI-generated security decisions. Unlike traditional security tools that primarily provide alerts or recommendations, modern AI SOC solutions are evolving toward autonomous investigation, prioritization, and remediation capabilities. Organizations remain cautious about allowing AI systems to independently execute actions such as isolating assets, blocking access, or modifying security configurations, particularly in critical infrastructure, financial services, healthcare, and government environments where incorrect decisions can have significant operational consequences. The requirement for human validation and approval of high-impact actions continues to influence enterprise adoption strategies and limits the immediate transition toward fully autonomous security operations.

Trust and transparency are becoming critical evaluation factors as organizations assess AI-driven security technologies. Security teams require visibility into how AI models generate recommendations, what data influences decisions, and whether automated actions can be audited after execution. NIST's AI Risk Management Framework emphasizes the importance of trustworthy AI characteristics, including validity, reliability, transparency, explainability, accountability, security, and resilience throughout the AI lifecycle. As AI SOC vendors introduce more advanced capabilities, enterprises are expected to establish governance controls, testing procedures, and human oversight mechanisms before granting broader autonomy to security systems. These trust requirements may slow the adoption of fully autonomous AI SOC platforms, especially among organizations with strict risk management and compliance obligations.

4.2.2.2 Evolving AI governance and regulatory landscape

The rapidly developing regulatory environment surrounding artificial intelligence represents a challenge for organizations deploying AI-powered SOC solutions. AI SOC platforms increasingly rely on generative AI models and autonomous agents to analyze security data, recommend actions, and execute operational workflows, creating new requirements around transparency, accountability, data protection, and auditability. However, global AI regulations and governance frameworks are still evolving, creating uncertainty for enterprises regarding compliance obligations, documentation requirements, and acceptable

JULY 2026 © MarketsandMarkets™

levels of AI autonomy in cybersecurity operations. Organizations must balance the benefits of AI-driven security capabilities with the need to align deployments with emerging regulatory expectations across different jurisdictions.

Government agencies and standards organizations are actively developing frameworks to support responsible AI adoption, but the absence of universally adopted AI governance standards creates complexity for multinational organizations. NIST's AI Risk Management Framework and its Generative AI Profile provide guidance for managing AI risks through functions such as governance, measurement, and risk management; however, these frameworks remain voluntary and require organizations to develop their own implementation approaches. Additionally, emerging regulations such as the European Union AI Act introduce additional compliance considerations for organizations using advanced AI systems. As AI SOC platforms become more autonomous and integrated into critical security processes, evolving governance requirements may increase implementation complexity, extend deployment timelines, and create additional operational responsibilities for enterprises.

4.2.3 OPPORTUNITIES

4.2.3.1 AI SOC adoption among small and medium-sized enterprises (SMEs)

Small and medium-sized enterprises (SMEs) are emerging as a significant growth opportunity for the AI SOC market as they face increasingly sophisticated cyber threats but often lack dedicated security teams and large cybersecurity budgets. Traditionally, enterprise-grade SOCs were accessible primarily to large organizations due to the high cost of infrastructure, specialized personnel, and continuous monitoring. However, the availability of cloud-native AI SOC platforms is democratizing advanced security operations by delivering automated threat detection, investigation, and response through subscription-based models. This shift enables SMEs to strengthen cyber resilience without making substantial investments in on-premises SOC infrastructure or expanding internal security teams.

Leading cybersecurity vendors are actively expanding AI-powered security offerings tailored to organizations with limited operational resources. Microsoft has broadened access to Security Copilot by making it available to eligible Microsoft 365 E5 & E7 customers with included monthly Security Compute Unit (SCU) capacity, while continuing to offer consumption-based licensing for other organizations. Similarly, cloud-delivered platforms from CrowdStrike, Google Cloud, Cisco Splunk, and Lumu provide scalable security operations that reduce deployment complexity and operational overhead. As SMEs continue accelerating digital transformation and cloud adoption, demand for affordable, AI-enabled SOC capabilities is expected to create substantial opportunities for vendors offering flexible, subscription-based security operations platforms.

4.2.3.2 AI security for agentic and generative AI environments

The rapid deployment of generative AI applications and autonomous AI agents across enterprises is creating a new opportunity for AI SOC vendors to provide specialized security capabilities for AI-driven environments. Organizations are increasingly integrating AI systems into business processes, software development, customer engagement, and decision-making workflows, resulting in new security requirements around AI models, data access, application behavior, and autonomous actions. Unlike traditional applications, AI agents can interact with multiple systems, access enterprise information, and execute tasks independently, creating new risks related to unauthorized actions, data exposure, and AI-driven attacks. This shift is creating demand for security platforms capable of monitoring AI workloads, protecting AI identities, and detecting abnormal behavior across AI ecosystems.

Industry organizations and technology vendors are developing frameworks and solutions to address emerging AI security requirements. NIST's Generative AI Risk Management Profile highlights risks associated with generative AI systems, including data security, privacy, model reliability, and malicious use, encouraging organizations to adopt structured AI risk management practices. Security providers are

JULY 2026 © MarketsandMarkets™

increasingly expanding their platforms to support AI governance, AI workload protection, and monitoring of autonomous systems. Microsoft, Google Cloud, and other technology providers are introducing security controls for AI applications and agents, while cybersecurity companies are exploring AI-specific detection and response capabilities. As enterprises continue scaling AI adoption, securing AI-powered environments is expected to become an important growth opportunity within the AI SOC market.

4.2.3.3 Unified AI-native security platforms

The increasing complexity of cybersecurity environments is creating opportunities for unified AI-native security platforms that consolidate multiple security capabilities into integrated operational ecosystems. Enterprises traditionally manage separate solutions for SIEM, SOAR, endpoint protection, network security, identity security, and threat intelligence, often resulting in fragmented visibility and operational inefficiencies. AI-native security platforms address this challenge by combining security data, analytics, automation, and intelligence into a centralized architecture capable of analyzing diverse signals and generating contextual insights. This platform consolidation approach enables organizations to simplify security operations, improve visibility across environments, and enhance the effectiveness of existing cybersecurity investments.

Leading cybersecurity vendors are increasingly shifting toward integrated AI-powered security platforms rather than standalone solutions. Microsoft has combined capabilities across Defender, Sentinel, Entra, Purview, and Security Copilot to create a unified security operations experience, while Google Security Operations integrates cloud-scale analytics with generative AI capabilities for investigation and detection workflows. Similarly, Palo Alto Networks Cortex, CrowdStrike Falcon, Cisco Splunk, and Lumu SecOps Platform are expanding integrated approaches that combine detection, intelligence, automation, and response capabilities. The growing preference for consolidated security architectures is expected to create opportunities for vendors that can deliver AI-native platforms capable of supporting end-to-end security operations across enterprise environments.

4.2.3.4 AI SOC-as-a-service and managed AI security operations

The evolution of managed security services is creating significant opportunities for AI SOC-as-a-Service models that combine artificial intelligence with outsourced security operations. Many organizations are shifting from internally operated SOC models toward flexible service-based approaches that provide continuous monitoring, investigation support, and security expertise without requiring large capital investments. AI capabilities are enhancing this model by enabling service providers to improve operational scalability, standardize security workflows, and support multiple customers through intelligent automation. For managed security service providers (MSSPs), AI SOC capabilities create opportunities to increase service efficiency, expand customer coverage, and deliver advanced security operations to organizations that may not have mature internal security teams.

The adoption of AI within managed security operations is encouraging MSSPs to transform traditional SOC delivery models into AI-enhanced security services. Service providers are increasingly incorporating AI-based analytics, automated case enrichment, investigation assistance, and response orchestration into their offerings to improve service consistency and operational scalability. Microsoft, through Security Copilot and its partner ecosystem, is enabling security providers to extend AI-assisted security capabilities to customers, while cybersecurity vendors such as CrowdStrike, Google Cloud, Cisco Splunk, and Lumu are supporting managed detection and response models with AI-driven technologies. As enterprises increasingly prefer outcome-based cybersecurity services, AI SOC-as-a-Service is expected to become a key opportunity area by enabling scalable, intelligent, and partner-driven security operations.

JULY 2026 © MarketsandMarkets™

4.2.4 CHALLENGES

4.2.4.1 Ensuring accuracy and reliability of AI-generated security decisions

AI SOC platforms depend on machine learning models, large language models (LLMs), and behavioral analytics to analyze security events and recommend or execute actions. However, ensuring consistent accuracy across diverse enterprise environments remains a significant challenge. Security data varies significantly across organizations due to differences in infrastructure, applications, user behavior, and threat exposure. As a result, AI models may face difficulties in interpreting new attack patterns, distinguishing legitimate activities from malicious behavior, or reducing false positives without continuous tuning and contextual learning. Maintaining reliable AI-driven decision-making is particularly challenging in security operations, where incorrect recommendations can impact business continuity and incident response effectiveness.

The challenge becomes more complex as AI SOC platforms evolve toward autonomous investigation and remediation capabilities. Organizations require continuous evaluation mechanisms to verify AI outputs, monitor model performance, and detect potential degradation over time. NIST highlights that deployed AI systems require ongoing monitoring due to challenges related to performance changes, operational reliability, security risks, and compliance requirements. For AI SOC vendors, improving model accuracy, explainability, and adaptability across different customer environments remains essential for building confidence and achieving widespread enterprise adoption.

4.2.4.2 Addressing AI model security and adversarial threats

As organizations increasingly depend on AI-driven security operations, protecting the AI models themselves becomes an emerging challenge. Cyber attackers may attempt to manipulate AI systems through techniques such as data poisoning, adversarial inputs, prompt injection, or exploitation of vulnerabilities in AI workflows. Since AI SOC platforms are designed to analyze threats and potentially execute security actions, compromising the underlying AI capabilities could impact detection accuracy, investigation outcomes, or automated response decisions.

The increasing adoption of autonomous AI agents further expands this risk landscape by introducing additional attack surfaces involving model interactions, tool usage, and decision execution. NIST identifies adversarial machine learning and AI system security as important areas requiring dedicated risk management approaches. As AI SOC solutions become more autonomous, vendors will need to continuously improve model protection, validation processes, threat testing, and security controls to ensure that AI capabilities enhance cybersecurity operations without introducing new vulnerabilities.

4.3 UNMET NEEDS AND WHITE SPACES

The AI SOC market is experiencing rapid growth as organizations adopt artificial intelligence to improve threat detection, investigation, and incident response. However, several critical unmet needs continue to limit the effectiveness and large-scale adoption of AI-powered security operations. One of the most significant gaps is the lack of unified visibility across increasingly distributed enterprise environments comprising cloud, on-premises, endpoints, identities, SaaS applications, and network infrastructure. Fragmented security tools and disconnected telemetry reduce the quality of AI-driven analysis and make it difficult to generate accurate, context-rich investigations. In addition, many AI SOC platforms continue to face challenges related to AI explainability, model transparency, integration with heterogeneous security ecosystems, and maintaining human oversight over autonomous security decisions.

These challenges create significant white space opportunities for innovation across the AI SOC ecosystem. There is growing demand for unified AI-native security platforms capable of consolidating SIEM, SOAR, XDR, NDR, identity security, and threat intelligence into a single operational environment. Organizations are also seeking explainable and trustworthy AI that provides transparent reasoning, confidence scoring, and

JULY 2026 © MarketsandMarkets™

human-in-the-loop governance for critical security decisions. Additional opportunities exist for AI-native protection of generative AI applications and autonomous agents, industry-specific AI SOC solutions tailored to regulated sectors, and AI SOC-as-a-Service offerings that enable organizations to access advanced security operations without building dedicated SOC infrastructure.

TABLE 2 UNMET NEEDS AND WHITE SPACES IN AI SOC MARKET

UNMET NEED/WHITE SPACE	DESCRIPTION
Unified Security Visibility Across Multi-Domain Environments	▪ Many organizations continue to operate fragmented security environments consisting of separate SIEM, XDR, cloud security, identity security, endpoint protection, and network monitoring platforms. These disconnected data sources limit AI's ability to correlate threats, reconstruct attack paths, and generate high-confidence investigations. Organizations require unified AI SOC platforms that provide centralized visibility and contextual threat intelligence across hybrid, multi-cloud, SaaS, endpoint, identity, and network environments.
Explainable and Trustworthy AI for Security Operations	▪ While AI is increasingly capable of investigating incidents and recommending remediation actions, many organizations require greater transparency before allowing autonomous execution of security decisions. Security teams need AI systems that provide explainable reasoning, confidence levels, audit trails, and human approval workflows to satisfy operational, regulatory, and governance requirements. Improving AI trust remains essential for broader enterprise adoption of autonomous SOC technologies.
Protection of Enterprise AI and Agentic AI Environments	▪ The rapid deployment of generative AI applications and autonomous AI agents has created a new security domain that existing SOC architectures were not originally designed to protect. Organizations require AI SOC platforms capable of monitoring AI identities, model interactions, prompt-based attacks, agent behavior, and AI-specific attack surfaces while maintaining governance across enterprise AI deployments.
Interoperability Across Heterogeneous Security Ecosystems	▪ Enterprises typically operate multi-vendor cybersecurity environments containing legacy infrastructure alongside modern cloud-native security platforms. AI SOC solutions often require extensive customization to integrate diverse security products, normalize telemetry, and orchestrate automated workflows. There remains a strong need for open, interoperable AI SOC platforms with standardized APIs, pre-built integrations, and vendor-agnostic security orchestration capabilities.
White Space Opportunities	▪ Development of unified AI-native security operations platforms integrating SIEM, SOAR, XDR, NDR, identity security, and threat intelligence into a single operational environment ▪ Expansion of explainable and trustworthy AI security platforms featuring transparent reasoning, confidence scoring, auditability, and human-in-the-loop governance for autonomous security operations ▪ Growth of AI security solutions for generative AI and agentic AI environments, including protection for AI agents, AI identities, LLM applications, and AI runtime environments ▪ Scaling of AI SOC-as-a-Service and managed AI security operations, enabling MSSPs to deliver AI-driven detection, investigation, and response capabilities through cloud-based subscription models ▪ Innovation in industry-specific AI SOC platforms tailored for highly regulated sectors such as BFSI, healthcare, government, and critical infrastructure, with built-in compliance, governance, and sector-specific threat intelligence

Source: Company Website and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

4.4 INTERCONNECTED MARKETS AND CROSS-SECTOR OPPORTUNITIES

The AI SOC market is increasingly interconnected with multiple cybersecurity and enterprise technology ecosystems, enabling organizations to build intelligent, automated, and unified security operations. As cyber threats become more sophisticated and enterprise environments expand across cloud, hybrid, multi-cloud, and edge infrastructures, AI SOC platforms are integrating with technologies such as generative AI, cloud computing, identity and access management (IAM), extended detection and response (XDR), threat intelligence, and Security Information and Event Management (SIEM). These interconnected technologies enhance real-time threat detection, contextual investigation, automated response, and security decision-making while improving operational efficiency across modern digital environments.

This convergence is accelerating the development of AI-native security platforms that unify security telemetry, automate workflows, and strengthen cyber resilience across industries. Strategic collaboration among cybersecurity vendors, cloud service providers, identity security providers, AI platform developers, and managed security service providers (MSSPs) is driving innovation in autonomous security operations, AI-assisted threat hunting, intelligent incident response, and continuous security monitoring. As a result, AI SOC is evolving beyond traditional security monitoring into a foundational platform for protecting cloud-native enterprises, digital businesses, and AI-enabled environments.

4.4.1 INTERCONNECTED MARKETS

INTERCONNECTED MARKET	APPLICATION
Generative AI & Large Language Models (LLMs)	Enables AI-assisted threat investigation, natural language security analysis, incident summarization, security copilots, and autonomous workflow orchestration, improving SOC analyst productivity and accelerating incident response
Cloud Computing Platforms	Supports cloud-native AI SOC platforms by enabling centralized security monitoring, scalable analytics, and unified visibility across hybrid, multi-cloud, and SaaS environments through cloud-delivered security operations
Identity and Access Management (IAM)	Strengthens AI SOC capabilities by providing identity-centric threat detection, privileged access monitoring, identity risk analytics, and Zero Trust enforcement to protect users, workloads, and AI agents
Extended Detection and Response (XDR) & SIEM	Provides unified telemetry from endpoints, networks, cloud workloads, email, and identities, enabling AI SOC platforms to correlate security events, prioritize threats, and automate investigations from a centralized security operations environment
Threat Intelligence Platforms	Enhances AI SOC with real-time indicators of compromise (IoCs), attacker intelligence, malware analysis, and threat context, enabling faster detection, improved risk prioritization, and proactive security operations
Managed Security Services (MSSPs & MDR)	Expands AI SOC adoption through AI-powered Security Operations Center-as-a-Service, enabling continuous monitoring, automated investigations, and managed detection and response for organizations with limited internal security resources

Source: Secondary Research and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

4.4.2 CROSS-SECTOR OPPORTUNITIES

- Generative AI and Agentic Security Operations: The convergence of AI SOC platforms with generative AI and autonomous AI agents is transforming modern security operations. AI-powered security copilots and agentic SOC capabilities automate alert triage, incident investigation, threat hunting, and response orchestration while maintaining human oversight for critical decisions. This integration enables security teams to improve productivity, reduce investigation time, and respond to AI-enabled cyber threats more effectively across enterprise environments.
- Cloud-Native Security Operations and Multi-Cloud Protection: The rapid adoption of cloud computing is creating opportunities for AI SOC platforms to deliver centralized security monitoring across hybrid and multi-cloud environments. By integrating with cloud-native security services, AI SOC solutions provide unified visibility, scalable analytics, and automated threat detection across cloud workloads, SaaS applications, containers, and virtual infrastructure. This convergence supports organizations pursuing cloud-first and digital transformation strategies.
- Identity-Centric Security and Zero Trust: The integration of AI SOC with Identity and Access Management (IAM), Identity Threat Detection and Response (ITDR), and Zero Trust architectures is strengthening enterprise cyber resilience. AI SOC platforms continuously analyze user identities, privileged accounts, authentication events, and access behavior to detect identity-based attacks, insider threats, and compromised credentials. This convergence is becoming increasingly important as identities emerge as one of the primary attack vectors in modern enterprises.
- Unified Detection, Threat Intelligence, and Security Automation: AI SOC platforms are increasingly converging with SIEM, XDR, SOAR, Network Detection and Response (NDR), and threat intelligence platforms to create unified security operations. This integration enables automated correlation of telemetry from endpoints, networks, cloud environments, email, and identities, providing contextual threat intelligence and orchestrated incident response. Organizations benefit from reduced tool sprawl, improved operational efficiency, and faster threat containment through centralized AI-driven security operations.
- Managed AI Security Operations and MSSP Ecosystems: The growing adoption of AI SOC technologies is creating new opportunities for Managed Security Service Providers (MSSPs) and Managed Detection and Response (MDR) providers. AI-powered investigation, automated response, and continuous threat monitoring enable service providers to deliver scalable Security Operations Center-as-a-Service (SOCaaS) offerings to organizations lacking dedicated security teams. This convergence is expanding enterprise access to advanced AI-driven security capabilities while improving service efficiency and operational scalability.

4.5 STRATEGIC MOVES BY TIER -1/2/3 PLAYERS

The AI SOC market is characterized by rapid innovation as cybersecurity vendors transition from conventional, analyst-driven Security Operations Centers toward AI-native, autonomous security operations. Vendors are increasingly integrating generative AI, machine learning, agentic AI, and security automation into their platforms to automate threat detection, investigation, prioritization, and response. Rather than offering standalone SIEM or SOAR capabilities, vendors are developing unified AI SOC platforms that combine security analytics, threat intelligence, workflow automation, identity security, cloud security, and autonomous decision support to improve operational efficiency and cyber resilience. This evolution enables enterprises to reduce alert fatigue, accelerate incident response, and operate scalable security operations despite the growing cybersecurity talent shortage.

The competitive landscape of the AI SOC market can be categorized into three tiers based on platform breadth, AI maturity, and operational specialization. Tier-1 vendors focus on comprehensive AI-native cybersecurity platforms that integrate SIEM, XDR, cloud security, identity protection, and AI copilots into

JULY 2026 © MarketsandMarkets™

enterprise-scale security operations. Tier-2 vendors emphasize specialized AI SOC capabilities including MDR, autonomous investigations, threat intelligence, workflow automation, and AI-assisted detection and response. Tier-3 vendors primarily develop agentic AI, autonomous SOC analysts, AI copilots, and niche security automation platforms that address specific operational challenges such as alert triage, threat hunting, and autonomous incident investigation. Together, these vendors are driving the evolution of Security Operations Centers toward intelligent, autonomous, and continuously adaptive cyber defense.

TABLE 3 STRATEGIC MOVES BY PLAYERS IN AI SOC MARKET

TIER	FOCUS AREAS	EXAMPLES	STRATEGIC INITIATIVES/DESCRIPTION
Tier 1 – Market Leaders	Unified AI-native cybersecurity platforms, SIEM/XDR integration, cloud security, identity security, AI copilots, enterprise-scale SecOps	Microsoft, Google, IBM, Cisco (Splunk), Palo Alto Networks, Fortinet, CrowdStrike, SentinelOne, Elastic	Tier-1 vendors are expanding unified AI-native cybersecurity platforms by integrating SIEM, XDR, identity security, cloud security, threat intelligence, and generative AI assistants. Vendors emphasize platform consolidation, enterprise automation, AI copilots, and agentic security capabilities to deliver end-to-end security operations across hybrid and multi-cloud environments.
Tier 2 – Established & Specialized Players	Managed Detection and Response (MDR), AI-assisted SOC, security analytics, SOAR, autonomous investigation, threat intelligence	Rapid7, Arctic Wolf, eSentire, Expel, Huntress, Stellar Cyber, UnderDefense, Anvilogic, Gruve, D3 Security	Tier-2 vendors are strengthening AI-driven security operations through managed detection and response, AI-assisted investigations, workflow automation, threat intelligence integration, and cloud-native SOC services. Vendors focus on improving analyst productivity, reducing mean time to detect (MTTD), and accelerating incident response through intelligent automation.
Tier 3 – Niche & Emerging Players	Agentic AI SOC, autonomous security agents, GenAI analysts, AI copilots, autonomous triage, workflow automation	Radiant Security, Conifers.ai, Dropzone AI, Simbian, Prophet Security, Legion Security, CyberSilo, Bricklayer AI, BlinkOps, Torq, Exaforce, Vulnuris, AIStrike, SOC Jedi.AI	Tier-3 vendors are introducing AI-native autonomous SOC platforms that leverage multi-agent AI architectures, large language models, and intelligent workflow automation to perform alert triage, investigation, threat hunting, evidence collection, and autonomous remediation. These vendors emphasize rapid deployment, modular AI agents, and seamless integration with existing enterprise security stacks.

Source: Company Website and MarketsandMarkets Analysis

4.5.1 CROSS-TIER STRATEGIC PATTERNS

The cross-tier strategic patterns in the AI SOC market reflect the industry's transition from security automation toward autonomous, AI-native security operations. Organizations are increasingly adopting unified security platforms capable of correlating telemetry from cloud environments, endpoints, identities, applications, and networks while embedding generative AI and agentic AI throughout the security operations lifecycle. Growing demand for faster threat detection, reduced analyst workload, and improved operational resilience is encouraging vendors across all tiers to strengthen AI capabilities, platform interoperability, and automation-driven security operations.

Strategic differentiation among vendor tiers is increasingly driven by AI maturity, platform integration, autonomous decision-making capabilities, and ecosystem partnerships. Tier-1 vendors continue expanding comprehensive cybersecurity platforms through AI copilots, cloud-native security, and platform

JULY 2026 © MarketsandMarkets™

consolidation. Tier-2 vendors differentiate through managed AI SOC services, AI-assisted detection, and specialized security operations, while Tier-3 innovators focus on agentic AI, autonomous SOC analysts, and intelligent workflow orchestration. These cross-tier developments are accelerating innovation, strategic acquisitions, and enterprise adoption of AI-driven security operations worldwide.

TABLE 4 CROSS-TIER STRATEGIC PATTERNS OF VENDORS

STRATEGIC THEME	KEY INSIGHTS
Unified AI-Native Security Platforms	Tier-1 vendors are consolidating SIEM, XDR, SOAR, identity security, cloud security, and generative AI into unified AI-native security platforms. Tier-2 and Tier-3 vendors increasingly integrate with these ecosystems through APIs and specialized AI capabilities.
Agentic AI & Autonomous Security Operations	Vendors across all tiers are investing in agentic AI to automate alert triage, threat investigation, evidence collection, response orchestration, and autonomous remediation. Emerging vendors are leading innovation, while Tier-1 vendors embed these capabilities into enterprise platforms.
Human-AI Collaborative Security Operations	AI copilots and intelligent assistants are becoming standard across enterprise SOCs. Vendors focus on augmenting analyst productivity through explainable AI, guided investigations, contextual recommendations, and human-in-the-loop decision-making.
Platform Consolidation & Security Ecosystem Integration	Organizations increasingly prefer integrated cybersecurity platforms instead of fragmented tools. Vendors are expanding partnerships, acquisitions, and native integrations to provide centralized visibility, unified telemetry, and end-to-end security operations.
Managed AI SOC & SOC-as-a-Service Expansion	Managed security providers are embedding AI across MDR and SOC-as-a-Service offerings to improve operational scalability, accelerate response, and deliver enterprise-grade security operations to organizations lacking dedicated SOC resources.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

4.5.2 STRATEGIC TRENDS

The AI SOC market is undergoing a significant transformation as organizations increasingly adopt artificial intelligence to modernize security operations and address the growing complexity of cyber threats. Key strategic trends include the emergence of agentic AI for autonomous security operations, the adoption of human-AI collaborative workflows, and the integration of AI with Continuous Threat Exposure Management (CTEM) to enable proactive cyber risk reduction. At the same time, cybersecurity vendors are embedding generative AI, intelligent automation, and unified security analytics into their platforms to improve detection accuracy, accelerate incident response, and enhance analyst productivity. These developments are reshaping SOCs into intelligent, data-driven, and highly automated environments, positioning AI SOC as a foundational capability for next-generation enterprise cybersecurity.

4.5.2.1 Rise of Agentic AI in security operations

Agentic AI is redefining the way SOCs detect, investigate, and respond to cyber threats by moving beyond AI-assisted recommendations toward autonomous execution. Unlike traditional automation, agentic AI systems can independently triage alerts, correlate evidence across identities, endpoints, cloud workloads, and networks, investigate incidents, and execute approved remediation actions with minimal human intervention. Leading vendors including Microsoft, Google Cloud, Lumu, Cisco, and Elastic are embedding autonomous AI agents into their security platforms to accelerate response times and reduce analyst workload. As cyberattacks continue to increase in speed and sophistication, organizations are increasingly adopting agentic AI to improve operational scalability while allowing analysts to focus on strategic

JULY 2026 © MarketsandMarkets™

investigations, threat hunting, and cyber resilience. The evolution toward autonomous yet human-governed SOC operations is expected to become one of the defining trends shaping next-generation security operations.

4.5.2.2 Human-AI collaborative security

Rather than replacing cybersecurity professionals, AI is increasingly being deployed as a collaborative partner that augments human expertise throughout the security operations lifecycle. Modern AI SOC platforms automate repetitive activities such as alert triage, case enrichment, malware analysis, log correlation, and incident summarization, enabling analysts to dedicate more time to complex investigations, threat hunting, and strategic decision-making. This collaborative operating model combines machine speed with human judgment, improving both efficiency and accuracy while reducing analyst fatigue. Leading cybersecurity vendors are emphasizing explainable AI, human-in-the-loop approval mechanisms, and transparent decision-making to ensure responsible adoption of autonomous capabilities. As organizations seek to maximize analyst productivity without compromising governance or accountability, human-AI collaboration is becoming a foundational operating principle for future SOCs.

4.5.2.3 AI-Powered Continuous Threat Exposure Management (CTEM)

Organizations are increasingly integrating AI-powered SOCs with Continuous Threat Exposure Management (CTEM) to shift cybersecurity from reactive incident response toward proactive risk reduction. Instead of treating vulnerabilities, misconfigurations, and attack paths independently, AI-enabled CTEM continuously identifies, validates, prioritizes, and remediates exposures based on exploitability and business impact. Artificial intelligence enhances this process by correlating threat intelligence, asset criticality, identity risks, cloud configurations, and attacker behavior to recommend the most effective remediation actions. Major cybersecurity vendors are incorporating CTEM capabilities into AI-driven security platforms to help organizations reduce attack surfaces and strengthen cyber resilience before compromises occur. As enterprises prioritize exposure management alongside threat detection, AI-powered CTEM is emerging as a strategic capability that complements modern AI SOC platforms and enables continuous, intelligence-driven security operations.

JULY 2026 © MarketsandMarkets™

5 INDUSTRY TRENDS

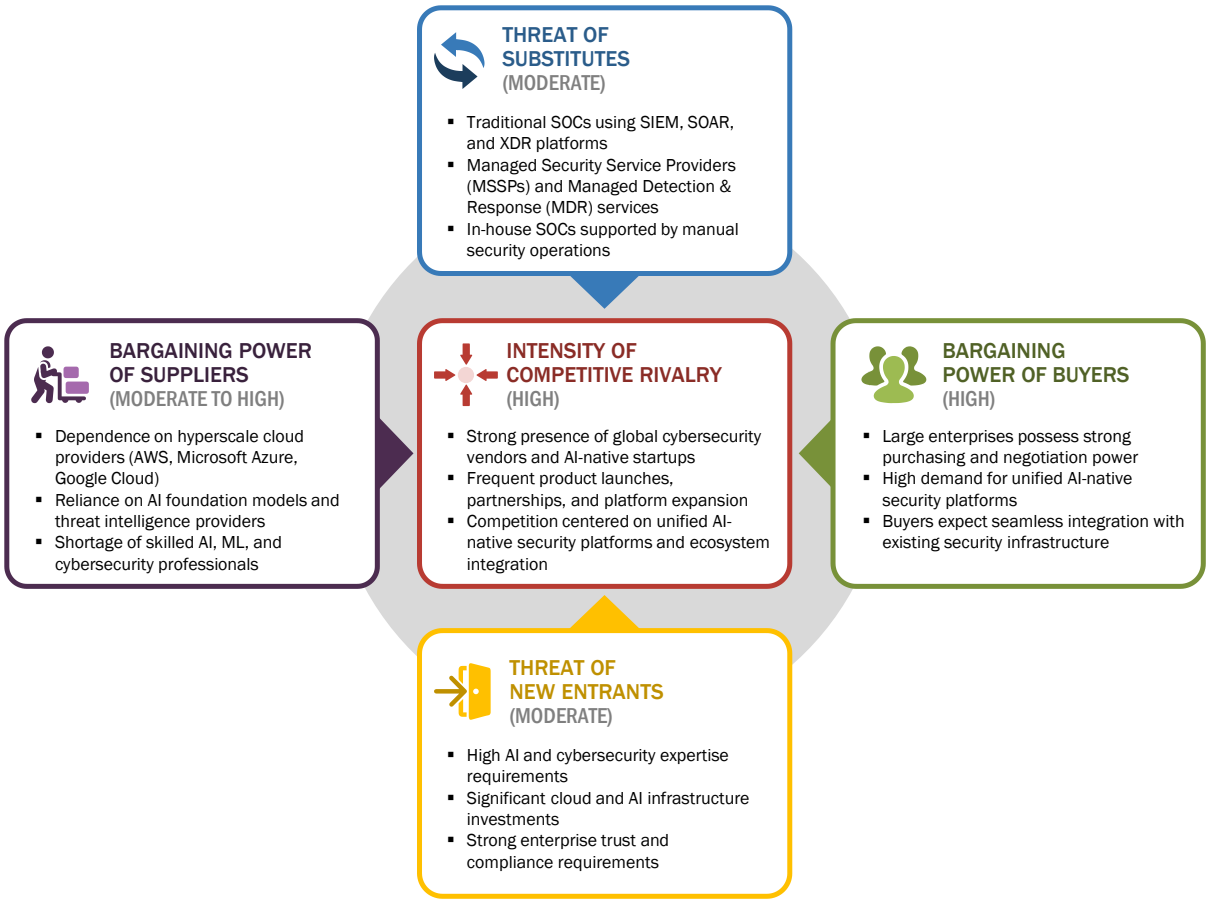
5.1 PORTER'S FIVE FORCES ANALYSIS

Porter's Five Forces analysis is a strategic framework used to evaluate the competitive intensity and overall attractiveness of an industry by examining the influence of five key competitive forces: competitive rivalry, the threat of new entrants, the bargaining power of suppliers, the bargaining power of buyers, and the threat of substitutes. The framework helps organizations understand how industry structure influences competition, innovation, pricing, and long-term profitability.

In the AI SOC market, Porter's Five Forces analysis highlights the impact of rapid advancements in artificial intelligence, increasing cybersecurity investments, evolving enterprise security requirements, and the growing demand for autonomous security operations. The analysis demonstrates how factors such as AI innovation, cloud ecosystem partnerships, platform consolidation, regulatory requirements, and competitive differentiation are shaping vendor strategies and accelerating the adoption of AI-native security operations across enterprises.

The following figure illustrates Porter's Five Forces analysis for the global AI SOC market.

FIGURE 18 AI SOC MARKET: PORTER'S FIVE FORCES ANALYSIS



Source: Secondary Literature, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 5 PORTER'S FIVE FORCES' IMPACT ON AI SOC MARKET

PORTER'S FIVE FORCES	IMPACT
Threat of New Entrants	Moderate
Bargaining Power of Suppliers	Moderate to High
Bargaining Power of Buyers	High
Threat of Substitutes	Moderate
Intensity of Competitive Rivalry	High

Source: MarketsandMarkets Analysis

5.1.1 THREAT OF NEW ENTRANTS

The threat of new entrants in the AI SOC market is considered **moderate** due to the high technological and operational barriers associated with developing enterprise-grade AI security platforms. Vendors must invest significantly in artificial intelligence, threat intelligence, cloud infrastructure, cybersecurity research, and skilled security professionals to deliver reliable AI-powered detection and response capabilities. In addition, enterprises increasingly expect AI SOC solutions to provide explainability, regulatory compliance, and seamless integration with existing security ecosystems, making market entry more challenging.

Furthermore, established cybersecurity vendors such as Microsoft, Google Cloud, Cisco (Splunk), Palo Alto Networks, CrowdStrike, and IBM possess strong competitive advantages through extensive customer relationships, mature security portfolios, large threat intelligence datasets, and robust partner ecosystems. These incumbents continuously invest in generative AI, agentic AI, and unified security operations, raising the benchmark for innovation and customer trust. While AI-native startups continue to enter the market with specialized capabilities, scaling globally and competing with established vendors requires substantial financial resources, technological expertise, and ecosystem partnerships.

5.1.2 BARGAINING POWER OF SUPPLIERS

The bargaining power of suppliers in the AI SOC market is considered **moderate** to **high** because vendors depend on a limited number of cloud infrastructure providers, AI model developers, cybersecurity data providers, and highly skilled cybersecurity professionals. Hyperscale cloud platforms such as Microsoft Azure, Amazon Web Services (AWS), and Google Cloud provide the computing infrastructure required to train and deploy AI-driven security solutions. Additionally, the global shortage of AI engineers, cybersecurity analysts, and threat intelligence experts increases dependence on specialized talent and technology providers.

However, supplier influence is partially offset by the growing availability of multi-cloud deployment models, open-source AI frameworks, and diversified threat intelligence sources. Many AI SOC vendors also develop proprietary AI models, establish strategic partnerships, and adopt hybrid cloud architectures to reduce dependence on individual suppliers. As competition among cloud providers and AI technology vendors continues to increase, AI SOC companies are expected to gain greater flexibility in sourcing infrastructure and AI capabilities while maintaining innovation and scalability.

JULY 2026 © MarketsandMarkets™

5.1.3 BARGAINING POWER OF BUYERS

The bargaining power of buyers in the AI SOC market is considered **high** because enterprises have access to numerous cybersecurity vendors offering AI-powered security operations, SIEM, XDR, SOAR, and managed detection and response solutions. Buyers increasingly evaluate vendors based on AI accuracy, automation capabilities, interoperability, regulatory compliance, scalability, and total cost of ownership. Large organizations often conduct proof-of-concept evaluations and negotiate customized pricing, deployment models, and service-level agreements before making purchasing decisions.

The availability of multiple competing platforms enables organizations to switch vendors more easily if solutions fail to meet operational or business requirements. In addition, enterprises increasingly prefer integrated security platforms that reduce tool sprawl and improve operational efficiency, encouraging vendors to continuously enhance AI capabilities and customer support. As AI SOC adoption expands, vendors will need to differentiate through innovation, ecosystem integration, measurable security outcomes, and customer experience to maintain competitive positioning.

5.1.4 THREAT OF SUBSTITUTES

The threat of substitutes in the AI SOC market is considered **moderate** because organizations can continue relying on conventional Security Operations Centers supported by traditional SIEM, SOAR, XDR, Managed Detection and Response (MDR), and Managed Security Service Providers (MSSPs). Some enterprises also utilize in-house security teams combined with standalone security tools instead of deploying fully integrated AI SOC platforms. These alternatives continue to provide effective security monitoring for organizations with established cybersecurity operations.

However, the increasing speed, sophistication, and volume of cyberattacks are reducing the effectiveness of manual and rule-based security operations. AI-powered investigation, intelligent threat prioritization, autonomous response, and continuous learning capabilities provide significant operational advantages that traditional SOC models struggle to match. As organizations pursue faster detection, reduced analyst workload, and scalable security operations, AI SOC platforms are expected to increasingly replace conventional security operations approaches rather than simply complement them.

5.1.5 INTENSITY OF COMPETITIVE RIVALRY

The intensity of competitive rivalry in the AI SOC market is considered **high** due to the presence of numerous global cybersecurity vendors continuously expanding their AI-powered security capabilities. Companies including Microsoft, Google Cloud, Cisco (Splunk), Palo Alto Networks, CrowdStrike, IBM, SentinelOne, Fortinet, and Lumu compete through rapid innovation in generative AI, agentic AI, threat intelligence, unified security platforms, and automated incident response. Frequent product launches, acquisitions, strategic partnerships, and AI feature enhancements continue to intensify market competition.

Competition is increasingly centered on delivering unified AI-native security operations that combine SIEM, SOAR, XDR, cloud security, identity security, and threat intelligence within integrated platforms. Vendors are also differentiating through autonomous investigation capabilities, AI copilots, industry-specific security solutions, and open technology ecosystems. As enterprises prioritize platform consolidation and AI-driven automation, vendors must continuously invest in research, product innovation, and ecosystem expansion to strengthen market position and sustain long-term competitive advantage.

JULY 2026 © MarketsandMarkets™

5.2 MACROECONOMIC INDICATORS

5.2.1 INTRODUCTION

This section highlights the key macroeconomic factors influencing the AI security operations center (AI SOC) market, including the rapid adoption of artificial intelligence, increasing enterprise cybersecurity investments, expansion of cloud and hybrid IT environments, and accelerating digital transformation initiatives. As organizations generate larger volumes of security data and face increasingly sophisticated AI-powered cyber threats, the demand for intelligent and automated security operations continues to grow. AI SOC platforms are becoming an essential component of enterprise cyber resilience by enabling real-time threat detection, automated investigation, and faster incident response across increasingly complex digital infrastructures.

Enterprises across industries such as BFSI, healthcare, government, manufacturing, retail, telecommunications, and energy are investing in AI SOC solutions to secure cloud workloads, endpoints, identities, applications, and hybrid infrastructures. The growing adoption of generative AI, Software-as-a-Service (SaaS), remote work, and multi-cloud architectures has significantly expanded enterprise attack surfaces, driving demand for AI-native security operations. In addition, organizations are increasingly integrating AI with SIEM, SOAR, XDR, threat intelligence, and identity security platforms to improve operational efficiency and reduce response times.

Furthermore, increasing government focus on cybersecurity resilience, responsible AI adoption, and critical infrastructure protection is playing a significant role in shaping the AI SOC market. North America, Europe, and Asia Pacific continue to strengthen cybersecurity regulations, AI governance frameworks, and digital security initiatives, encouraging enterprises to modernize Security Operations Centers through AI-driven automation. Simultaneously, the growing frequency of ransomware attacks, identity-based threats, and AI-enabled cyberattacks is positioning AI SOC platforms as a strategic investment for organizations seeking continuous security monitoring and cyber resilience.

5.2.2 GDP TRENDS AND FORECAST

Gross domestic product (GDP) is an important macroeconomic indicator influencing enterprise spending on digital transformation, artificial intelligence, cloud computing, and cybersecurity technologies, including AI SOCs. Countries with higher GDP and mature digital economies generally invest more heavily in AI infrastructure, cloud platforms, cybersecurity modernization, and enterprise security operations. As AI adoption accelerates across industries, GDP growth continues to support higher capital expenditure on intelligent security technologies that strengthen cyber resilience and operational efficiency.

Major economies such as the US, China, Germany, the UK, Japan, India, South Korea, and Singapore are expected to remain key contributors to AI SOC market growth due to strong AI investments, expanding cloud adoption, and increasing cybersecurity expenditure. These countries are witnessing rapid enterprise adoption of generative AI, intelligent automation, and cloud-native technologies, creating sustained demand for AI-powered security operations. Emerging economies are also accelerating digital transformation initiatives, expanding opportunities for AI SOC deployment across both public and private sectors.

JULY 2026 © MarketsandMarkets™

TABLE 6 GDP PERCENTAGE CHANGE, BY KEY COUNTRY, 2021–2030

Country	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Argentina	10.7%	5%	-1.6%	-2.8%	5.0%	4.5%	3.9%	3.1%	2.3%	3.2%
Australia	5.6%	3.8%	2.1%	1.5%	2.0%	2.1%	2.2%	2.2%	2.3%	2.3%
Austria	4.2%	4.8%	-0.7%	0.4%	1.6%	1.4%	1.0%	0.9%	0.9%	0.7%
Belgium	6.9%	3%	1.5%	1.2%	1.2%	1.2%	1.2%	1.3%	1.3%	1.3%
Brazil	4.8%	3%	2.9%	2.2%	2.1%	2.1%	2.0%	2.0%	2.0%	2.5%
Chile	11.3%	2.1%	0.2%	2.0%	2.5%	2.4%	2.3%	2.3%	2.3%	2.2%
China	8.4%	3%	5.2%	4.6%	4.1%	3.8%	3.6%	3.4%	3.3%	3.4%
Colombia	10.8%	7.3%	0.6%	1.1%	2.5%	3.0%	3.0%	3.0%	3.0%	2.8%
Denmark	6.8%	2.7%	1.8%	2.1%	1.5%	1.5%	1.4%	1.4%	1.4%	1.5%
Egypt	3.3%	6.7%	3.8%	3.0%	4.4%	4.7%	5.1%	5.5%	5.6%	5.3%
Finland	2.8%	1.3%	-1.0%	0.4%	1.9%	1.9%	1.7%	1.6%	1.5%	1.2%
France	6.3%	2.5%	0.9%	0.7%	1.4%	1.6%	1.5%	1.4%	1.3%	1.2%
Germany	3.2%	1.8%	-0.3%	0.2%	1.3%	1.5%	1.1%	0.8%	0.7%	0.7%
India	9.7%	7%	7.8%	6.8%	6.5%	6.5%	6.5%	6.5%	6.5%	6.5%
Indonesia	3.7%	5.3%	5.0%	5.0%	5.1%	5.1%	5.1%	5.1%	5.1%	5.1%
Iran	4.7%	3.8%	4.7%	3.3%	3.1%	2.7%	2.3%	2.0%	2.0%	2%
Iraq	1.6%	7.0%	-2.2%	1.4%	5.3%	3.8%	3.6%	3.6%	3.6%	4.1%
Italy	8.3%	4.0%	0.9%	0.7%	0.7%	0.2%	0.3%	0.8%	0.8%	0.7%
Japan	2.6%	1.0%	1.9%	0.9%	1.0%	0.8%	0.6%	0.6%	0.4%	0.5%
South Korea	4.3%	2.6%	1.4%	2.3%	2.3%	2.2%	2.1%	2.1%	2.0%	1.9%
Kuwait	1.7%	6.1%	-2.2%	-1.4%	3.8%	2.5%	2.6%	2.6%	2.6%	2.3%
Malaysia	3.3%	8.7%	3.7%	4.4%	4.4%	4.4%	4.0%	4.0%	4.0%	4%
Mexico	5.7%	3.9%	3.2%	2.4%	1.4%	1.9%	2.1%	2.1%	2.1%	2.1%
Netherlands	6.2%	4.3%	0.1%	0.6%	1.3%	1.9%	1.9%	1.8%	1.6%	1.2%
New Zealand	5.6%	2.4%	0.6%	1.0%	2.0%	2.4%	2.4%	2.4%	2.4%	2.2%
Philippines	5.7%	7.6%	5.6%	6.2%	6.2%	6.2%	6.3%	6.3%	6.4%	6%
Poland	6.9%	5.3%	0.2%	3.1%	3.5%	3.3%	3.0%	3.0%	3.0%	2.6%
Qatar	1.6%	4.2%	1.6%	2.0%	2.0%	5.9%	7.6%	3.4%	1.6%	3.4%
Saudi Arabia	5.1%	7.5%	-0.8%	2.6%	6.0%	4.0%	3.5%	3.0%	3.5%	3.3%
Singapore	9.7%	3.8%	1.1%	2.1%	2.3%	2.5%	2.5%	2.5%	2.5%	2.5%
South Africa	4.7%	1.9%	0.6%	0.9%	1.2%	1.4%	1.4%	1.4%	1.4%	1.8%
Spain	6.4%	5.8%	2.5%	1.9%	2.1%	1.8%	1.6%	1.6%	1.6%	1.6%
Sweden	6.1%	2.7%	-0.2%	0.2%	2.2%	2.2%	2.2%	2.1%	2.1%	1.7%
Switzerland	5.4%	2.7%	0.8%	1.3%	1.4%	1.8%	1.2%	1.8%	1.2%	1.8%
Thailand	1.5%	2.5%	1.9%	2.7%	2.9%	3.0%	3.0%	3.0%	3.0%	2.5%
Türkiye	11.4%	5.5%	4.5%	3.1%	3.2%	3.3%	3.4%	3.5%	3.5%	3.8%
UAE	4.4%	7.9%	3.4%	3.5%	4.2%	4.3%	4.4%	4.5%	4.5%	3.9%

JULY 2026 © MarketsandMarkets™

UK	8.7%	4.3%	0.1%	0.5%	1.5%	1.7%	1.7%	1.6%	1.4%	1.4%
US	5.8%	1.9%	2.5%	2.7%	1.9%	2.0%	2.1%	2.1%	2.1%	1.8%
Vietnam	2.6%	8.1%	5.0%	5.8%	6.5%	6.5%	6.5%	6.5%	6.5%	5.3%

Source: International Monetary Fund (IMF)

According to recent global economic outlooks published by the International Monetary Fund (IMF), the global economy is expected to maintain moderate but resilient growth during 2025–2026, supported by continued expansion in major economies and sustained investments in digital technologies despite geopolitical and macroeconomic uncertainties. At the same time, enterprise spending on artificial intelligence and information technology is accelerating rapidly, creating a strong foundation for AI-enabled cybersecurity solutions. As organizations increasingly adopt cloud computing, generative AI, hybrid work environments, and digital business models, the demand for AI SOCs is rising to protect expanding digital assets, identities, applications, and cloud infrastructure from increasingly sophisticated cyber threats.

Simultaneously, global investments in artificial intelligence and cybersecurity are growing at an unprecedented pace. Organizations are increasingly investing in AI SOC platforms, autonomous security operations, generative AI assistants, threat intelligence, identity security, and cloud-native security analytics to improve operational efficiency and cyber resilience. These investments are being driven by the increasing frequency of ransomware attacks, AI-enabled cyber threats, expanding cloud adoption, and the growing complexity of hybrid enterprise environments.

Emerging economies such as India, Southeast Asian countries, and the Middle East are rapidly expanding investments in AI, cloud infrastructure, and enterprise digital transformation, creating significant opportunities for AI SOC adoption across public and private sectors. Meanwhile, developed markets including North America and Europe continue to lead AI SOC deployment due to mature cloud ecosystems, higher cybersecurity spending, and strong regulatory initiatives supporting AI governance and cyber resilience. Overall, stable global economic growth, accelerating AI investments, and increasing enterprise dependence on digital infrastructure are expected to sustain strong long-term growth in the AI SOC market throughout the forecast period.

5.2.3 TRENDS IN GLOBAL ICT INDUSTRY

The global cybersecurity industry is undergoing a structural transformation as cyber risks evolve from isolated IT incidents to enterprise-wide business risks. The rapid expansion of cloud computing, digital services, Internet of Things (IoT), operational technology (OT), and AI-powered applications has significantly broadened the enterprise attack surface. Consequently, organizations are shifting from traditional prevention-centric security models toward cyber resilience strategies that emphasize continuous monitoring, rapid recovery, and business continuity. Governments and regulators worldwide are also strengthening cybersecurity requirements, making cyber resilience a board-level priority rather than solely an IT responsibility.

Another major trend is the growing convergence of cybersecurity with enterprise risk management and governance. Organizations are increasingly investing in Zero Trust architectures, identity-first security, cloud-native application protection, software supply chain security, and cyber resilience programs to safeguard distributed digital environments. Identity has become the new security perimeter as enterprises protect users, devices, workloads, APIs, and machine identities across hybrid environments. Simultaneously, geopolitical tensions, ransomware, and AI-enabled attacks are accelerating investments in advanced security technologies and critical infrastructure protection across both public and private sectors.

JULY 2026 © MarketsandMarkets™

The cybersecurity vendor landscape is also evolving through platform consolidation, strategic acquisitions, and ecosystem partnerships. Organizations increasingly prefer integrated cybersecurity platforms that combine endpoint security, cloud security, identity protection, threat intelligence, and security analytics rather than managing numerous standalone tools. This trend is driving significant M&A activity as vendors acquire AI capabilities and expand platform portfolios to deliver unified cyber defense. As digital transformation accelerates globally, cybersecurity is becoming a foundational enabler of enterprise innovation, regulatory compliance, and operational resilience.

5.2.4 TRENDS IN GLOBAL AI SOC INDUSTRY

The global AI SOC industry is rapidly evolving from AI-assisted security monitoring to autonomous, intelligence-driven security operations. Organizations are increasingly deploying generative AI, large language models (LLMs), and agentic AI to automate alert triage, incident investigation, threat hunting, malware analysis, and response orchestration. Rather than functioning as standalone automation tools, modern AI SOC platforms are becoming decision-support and execution engines that continuously learn from enterprise telemetry and threat intelligence. This shift is fundamentally redefining how SOCs operate and scale.

A defining trend within the AI SOC market is the adoption of human-AI collaborative security operations. Security teams are increasingly integrating AI copilots and autonomous agents into analyst workflows while maintaining human oversight for governance, compliance, and high-risk decisions. Explainable AI, policy-driven automation, and human-in-the-loop frameworks are becoming essential components of enterprise AI SOC deployments to improve analyst productivity without compromising transparency or accountability. Gartner identifies AI-driven SOC solutions and AI governance among the most influential cybersecurity trends shaping enterprise security operations.

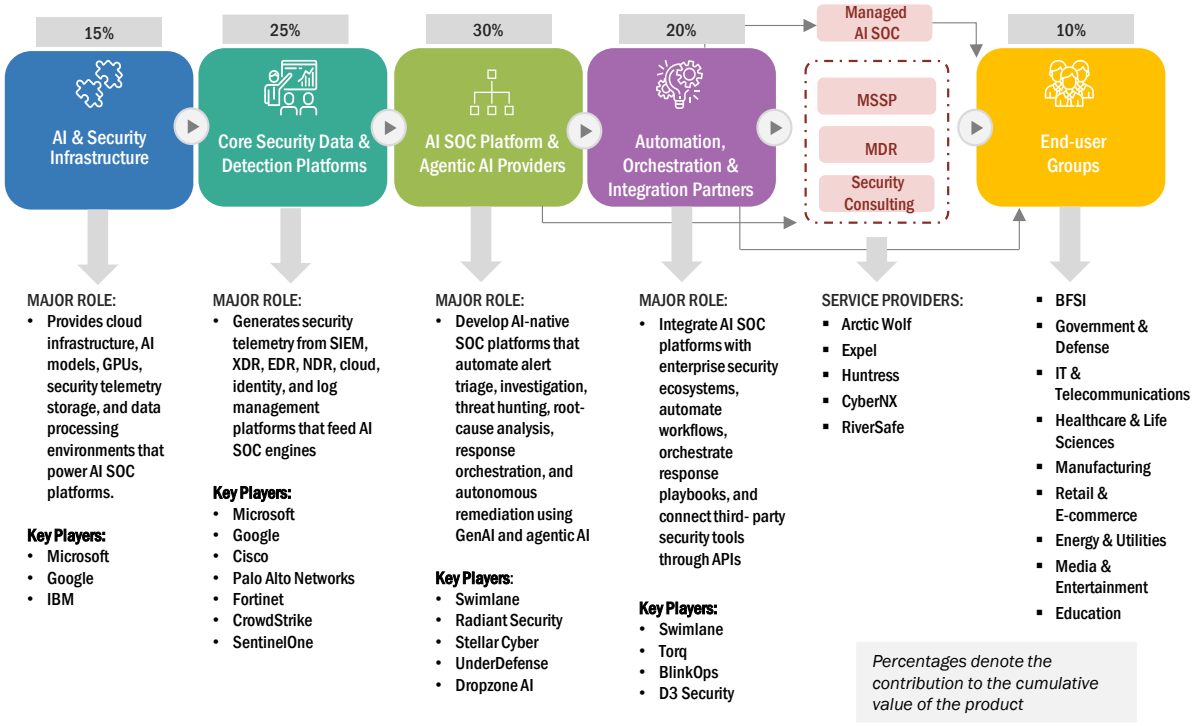
Another significant trend is the emergence of AI-native SecOps platforms that unify SIEM, SOAR, XDR, NDR, identity security, cloud security, exposure management, and threat intelligence into a single operational platform. Vendors are increasingly embedding AI into every stage of the security operations lifecycle, enabling predictive analytics, continuous threat exposure management (CTEM), automated investigations, and autonomous remediation. As organizations seek to reduce operational complexity and improve security outcomes, AI SOC platforms are evolving into intelligent, cloud-native security ecosystems capable of delivering scalable, proactive, and continuously adaptive cyber defense.

5.3 VALUE CHAIN ANALYSIS

The AI SOC market comprises cloud infrastructure providers, cybersecurity platform vendors, AI SOC technology providers, security automation companies, managed security service providers (MSSPs), and enterprise end users that collectively deliver intelligent, AI-driven security operations. These stakeholders work together to provide continuous threat detection, automated investigation, response orchestration, and cyber resilience across modern enterprise environments. As organizations increasingly adopt cloud computing, hybrid infrastructures, identity-centric security, and artificial intelligence, collaboration across the AI SOC ecosystem has become essential for enabling scalable, autonomous, and real-time security operations.

JULY 2026 © MarketsandMarkets™

FIGURE 19 AI SOC MARKET: VALUE CHAIN ANALYSIS



Source: Articles, White Papers, Interviews with Experts, and MarketsandMarkets Analysis

The AI SOC value chain highlights the integration of cloud and AI infrastructure providers, security telemetry platforms, AI-native SOC vendors, automation and orchestration providers, and managed security service organizations to deliver end-to-end intelligent security operations. Unlike traditional SOCs that rely heavily on manual investigations and siloed security tools, AI SOC ecosystems leverage artificial intelligence, machine learning, agentic AI, and workflow automation to continuously analyze security data, prioritize threats, investigate incidents, and orchestrate response actions across enterprise environments. The value chain can be divided into the following stages:

The breakdown of each stage can be described as:

5.3.1 AI & SECURITY INFRASTRUCTURE

This stage provides the foundational computing environment required to power AI SOC platforms. It includes cloud infrastructure, AI model hosting, GPU computing, large-scale data storage, identity services, and security analytics platforms that enable organizations to ingest, process, and analyze massive volumes of security telemetry. These infrastructure providers deliver the scalability, performance, and availability required for real-time AI-driven threat detection, investigation, and response across cloud, hybrid, and multi-cloud environments.

Key Players: Microsoft, Google, IBM

JULY 2026 © MarketsandMarkets™

5.3.2 CORE SECURITY DATA & DETECTION PLATFORMS

This stage focuses on collecting, correlating, and normalizing security telemetry from enterprise environments. Security platforms including SIEM, XDR, EDR, NDR, identity security, cloud security, and log management solutions continuously generate security events that serve as the primary data source for AI SOC platforms. These platforms provide comprehensive visibility across endpoints, networks, identities, applications, and cloud workloads, enabling AI engines to perform accurate threat detection, correlation, and contextual analysis.

Key Players: Microsoft, Google, Cisco (Splunk), Palo Alto Networks, Fortinet, CrowdStrike, SentinelOne, Elastic, Rapid7

5.3.3 AI SOC PLATFORM & AGENTIC AI PROVIDERS

This stage represents the core intelligence layer of the value chain, where AI-native security operations platforms leverage generative AI, machine learning, and agentic AI to automate security workflows. These platforms perform alert prioritization, threat correlation, incident investigation, malware analysis, threat hunting, response recommendations, and increasingly autonomous remediation. By reducing analyst workload and accelerating response times, AI SOC vendors enable organizations to operate more efficient and scalable Security Operations Centers while improving overall cyber resilience.

Key Players: Swimlane, Radiant Security, Stellar Cyber, UnderDefense, Conifers.ai, Dropzone AI, Simbian, Prophet Security, Legion Security, CyberSilo, Bricklayer AI, Exaforce, AIStrike, Vulnuris, SOC Jedi.AI

5.3.4 AUTOMATION, ORCHESTRATION & INTEGRATION PARTNERS

This stage enables seamless integration between AI SOC platforms and enterprise security ecosystems. Automation and orchestration providers develop workflow automation, API integrations, playbooks, case management, and response orchestration capabilities that connect AI SOC platforms with SIEM, SOAR, XDR, identity, cloud, ticketing, and IT service management systems. These solutions help organizations automate repetitive security processes while ensuring coordinated response across heterogeneous security environments.

Key Players: Swimlane, Torq, BlinkOps, D3 Security, Gruve, Anvilogic

5.3.5 MANAGED AI SOC SERVICES (CROSS-STAGE LAYER)

This cross-functional stage supports organizations throughout the AI SOC lifecycle by delivering managed detection and response (MDR), Security Operations Center as a Service (SOCaaS), security consulting, deployment, monitoring, incident response, compliance support, and continuous optimization services. Managed security providers help enterprises accelerate AI SOC adoption while supplementing in-house security teams with specialized expertise, continuous monitoring, and operational best practices.

Key Players: Arctic Wolf, eSentire, Expel, Huntress, CyberNX, RiverSafe

5.3.6 END USER GROUPS

End users include organizations across industries such as Banking, Financial Services & Insurance (BFSI), government and defense, IT & telecommunications, healthcare, manufacturing, retail & e-commerce, energy & utilities, transportation & logistics, education, and critical infrastructure. These organizations deploy AI SOC platforms to strengthen cyber resilience, automate threat detection and response, reduce analyst fatigue, improve compliance, and secure increasingly complex cloud, hybrid, and AI-enabled enterprise environments.

JULY 2026 © MarketsandMarkets™

5.4 ECOSYSTEM ANALYSIS

The AI SOC market ecosystem comprises a diverse mix of software platform providers and security service providers that collectively enable organizations to modernize security operations through AI-driven detection, investigation, response, and continuous threat monitoring. Software platform vendors develop AI-native technologies that automate core SOC functions, including threat detection and analytics, security orchestration, autonomous investigations, AI SOC agents, security data management, and threat intelligence. At the same time, service providers complement these capabilities with managed detection and response (MDR), AI SOC-as-a-Service (SOCaaS), incident response and digital forensics, and threat intelligence advisory, helping organizations strengthen cyber resilience while addressing cybersecurity talent shortages and increasingly sophisticated cyber threats.

The software platform landscape is led by established cybersecurity vendors such as Microsoft, Google, IBM, Cisco, Swimlane, CrowdStrike, Palo Alto Networks, SentinelOne, Fortinet, Elastic, Rapid7, Sophos, Arctic Wolf, Lumu Technologies, and Exabeam, alongside a rapidly expanding group of AI-native innovators including Radiant Security, Conifers.ai, Dropzone AI, Prophet Security, Simbian, Exaforce, Anvilogic, Legion Security, Bricklayer AI, Augur, BlinkOps, SOC Jedi.AI, AIStrike, Torq, Intezer, CyberSilo, and D3 Security. These companies are advancing agentic AI, autonomous investigations, AI-powered SIEM, XDR, and security automation to improve alert prioritization, reduce analyst workload, and accelerate incident response. The service ecosystem includes vendors such as Google (Mandiant), CrowdStrike, Sophos, Arctic Wolf, eSentire, Expel, Huntress, UnderDefense, Stellar Cyber, ReliaQuest, CyberNX, Gruve, RiverSafe, Vulnuris, and Exabeam, which combine AI-native platforms with expert-led managed services to deliver continuous monitoring, proactive threat hunting, incident response, and cyber resilience.

The market is increasingly characterized by the convergence of AI-native software platforms and managed security services, with vendors integrating generative AI, agentic AI, security data platforms, and open ecosystem partnerships into unified security operations. Organizations are also adopting hybrid deployment models that combine AI-powered automation with human expertise to improve detection accuracy, accelerate response, and maintain governance across complex hybrid and multi-cloud environments. As enterprises seek to consolidate fragmented security tools while enhancing operational efficiency, collaboration between software providers, MDR vendors, cloud hyperscalers, system integrators, and technology partners is expected to remain a defining characteristic of the evolving AI SOC ecosystem.

JULY 2026 © MarketsandMarkets™

FIGURE 20 AI SOC MARKET: ECOSYSTEM ANALYSIS



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 7 AI SOC MARKET: ECOSYSTEM

ROLE IN ECOSYSTEM	COMPANY
Software Platforms	▪ Swimlane ▪ Elastic ▪ Torq ▪ Legion Security ▪ D3 Security ▪ SOC Jedi.AI
Software Platforms, Services	▪ Microsoft ▪ Cisco ▪ CrowdStrike ▪ Palo Alto Networks ▪ Google ▪ Sophos ▪ IBM ▪ Fortinet ▪ Arctic Wolf ▪ Rapid7 ▪ SentinelOne

JULY 2026 © MarketsandMarkets™

- Expel
- ReliaQuest
- Exabeam
- eSentire
- Lumu Technologies
- Huntress
- UnderDefense
- Stellar Cyber
- Radiant Security
- Intezer
- Conifers.ai
- Dropzone AI
- Simbian
- Prophet Security
- CyberSilo
- Bricklayer AI
- Augur
- BlinkOps
- Gruve
- CyberNX
- Anvilogic
- AIStrike
- Exaforce
- RiverSafe
- Vulnuris

Source: Company Websites and MarketsandMarkets Analysis

5.5 PRICING ANALYSIS

The pricing of AI SOC solutions varies considerably depending on deployment model, organization size, number of monitored assets or users, data ingestion volume, AI capabilities, and the scope of managed security services. Unlike traditional SOC platforms that rely primarily on SIEM licensing and analyst-intensive operations, AI SOC solutions increasingly combine AI-native software, autonomous investigation engines, security copilots, XDR, SOAR, and MDR services into integrated subscription offerings. As enterprises migrate toward cloud-native security operations, vendors are increasingly adopting flexible SaaS-based and consumption-driven pricing models that reduce upfront capital expenditure while allowing organizations to scale security operations based on business requirements. AI compute costs and autonomous AI workflows are also driving the emergence of hybrid pricing models that combine fixed platform subscriptions with usage-based billing for advanced AI capabilities.

JULY 2026 © MarketsandMarkets™

Pricing Models in AI SOC Market:

With the rapid evolution of AI-native security operations, vendors increasingly offer multiple commercial pricing models to address diverse enterprise requirements:

- **Subscription-Based (SaaS) Pricing:** The most widely adopted model for AI SOC platforms. Customers pay a monthly or annual subscription for access to AI-powered SOC capabilities, including AI-assisted investigations, autonomous threat detection, security copilots, XDR, SOAR, and continuous monitoring. Pricing generally varies according to the selected feature tier, deployment scale, and service-level agreement (SLA).
- **Per Endpoint / Asset Pricing:** Common among AI SOC, MDR, and XDR providers. Organizations are charged based on the number of protected endpoints, servers, cloud workloads, network devices, or other monitored assets. This model provides predictable costs while allowing security coverage to scale as enterprise infrastructure expands.
- **Usage-Based / Consumption Pricing:** Pricing is determined by operational metrics such as security events processed, AI investigations performed, log ingestion volume, API calls, AI compute consumption, or autonomous workflows executed. This model is increasingly adopted for AI-native platforms where infrastructure usage directly influences operating costs.
- **Per User/Identity Pricing:** Frequently used for identity-centric AI SOC deployments, particularly where monitoring focuses on user identities, privileged accounts, SaaS applications, or Zero Trust environments. Charges are based on the number of monitored users or identities rather than physical devices.
- **Tiered Enterprise Licensing:** Large enterprises purchase predefined Standard, Professional, Enterprise, or Premium packages offering different levels of AI automation, threat hunting, compliance reporting, autonomous response, integrations, and support services. This model simplifies procurement while enabling customers to upgrade capabilities as security maturity increases.
- **Managed AI SOC/MDR Service Pricing:** Managed Security Service Providers (MSSPs) and MDR vendors offer AI SOC capabilities through recurring managed service contracts. Pricing is typically based on service scope, number of monitored assets, coverage hours (8×5 or 24×7), incident response requirements, and SLA commitments, allowing organizations to outsource AI-driven security operations without building an in-house SOC.
- **Custom/Project-Based Pricing:** Large enterprises with complex hybrid, multi-cloud, or regulated environments often procure AI SOC platforms through customized commercial agreements. Pricing depends on deployment complexity, integrations, migration services, compliance requirements, AI customization, training, and long-term support contracts.

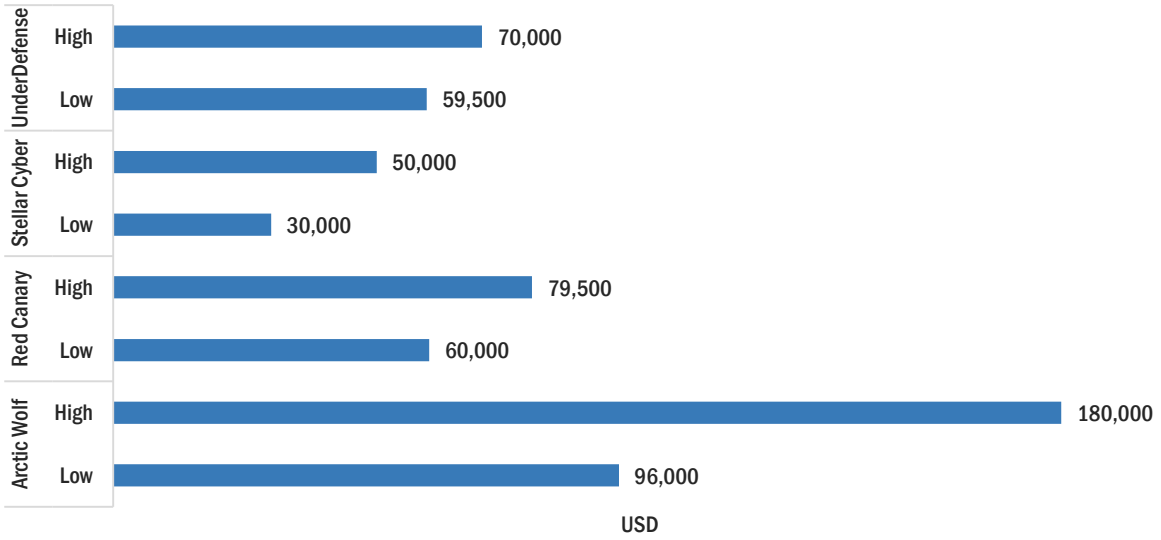
5.5.1 AVERAGE ANNUAL SELLING PRICE OF KEY AI SOC VENDORS FOR A 500-ENDPOINT DEPLOYMENT

The annual cost of AI SOC solutions varies depending on the scope of services, level of automation, deployment model, endpoint coverage, and integration requirements. AI SOC offerings are typically delivered through subscription-based Software-as-a-Service (SaaS), Managed Detection and Response (MDR), or SOC-as-a-Service (SOCaaS) models, with pricing influenced by the number of protected endpoints, cloud workloads, identities, data retention requirements, and response service levels. Vendors offering advanced AI capabilities such as autonomous investigations, automated response, behavioral analytics, and threat intelligence generally command higher annual contract values.

JULY 2026 © MarketsandMarkets™

For a standard deployment supporting approximately 500 endpoints, annual pricing typically reflects the breadth of AI-driven detection, investigation, response, and managed security services included within the subscription. Organizations also incur additional costs for implementation, onboarding, integration with SIEM, XDR, cloud, and identity platforms, as well as premium incident response, compliance reporting, and extended log retention services. As enterprises increasingly adopt cloud-native AI SOC platforms, vendors are offering scalable, consumption-based pricing that enables predictable operational expenditure while reducing upfront infrastructure investments.

FIGURE 21 AVERAGE ANNUAL SELLING PRICE OF KEY AI SOC VENDORS, FOR 500-ENDPOINT DEPLOYMENT, 2025 (USD)



Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 8 AVERAGE ANNUAL SELLING PRICE OF KEY AI SOC VENDORS, FOR 500-ENDPOINT DEPLOYMENT, 2025 (USD)

KEY PLAYERS	AI SOC ANNUAL COST AT 500 ENDPOINTS
Arctic Wolf	▪ Low: USD 96,000 per year ▪ High: USD 180,000 per year
Red Canary	▪ Low: USD 60,000 per year ▪ High: USD 79,500 per year
Stellar Cyber	▪ Low: USD 30,000 per year ▪ High: USD 50,000 per year
UnderDefense	▪ Low: USD 59,500 per year ▪ High: USD 70,000 per year

Note 1: The pricing has been given for reference. It is not the final price of the products.

Note 2: Pricing represents indicative annual subscription costs for a deployment protecting approximately 500 endpoints. Actual pricing varies depending on deployment scope, number of users and endpoints, cloud workloads, log ingestion volume, AI automation capabilities, service-level agreements (SLAs), incident response coverage, compliance requirements, contract duration, and negotiated enterprise discounts.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

5.5.2 INDICATIVE PRICING ANALYSIS FOR KEY PLAYERS

AI SOC vendors employ diverse commercial models, including subscription-based, consumption-based, per-endpoint, per-user, and AI compute-based pricing. While most enterprise AI SOC platforms are sold through customized commercial agreements, several vendors publicly disclose indicative pricing for AI assistants, cloud-native SIEM platforms, AI-powered security services, and endpoint protection offerings. The pricing presented below represents publicly available list prices or starting prices for selected AI SOC-related offerings and provides a benchmark for comparing commercial positioning across leading vendors. Actual enterprise pricing varies depending on deployment scale, number of protected endpoints, data ingestion volumes, AI compute consumption, integration requirements, managed services, and contractual commitments.

TABLE 9 INDICATIVE PRICING OF AI SOC OFFERINGS, BY KEY PLAYER, 2025 (USD)

OFFERING	COMPANY NAME	PRICE
Microsoft Security Copilot	Microsoft	▪ Security Compute Unit (SCU): USD 4 per provisioned SCU/hour ▪ Overage capacity: USD 6 per SCU/hour ▪ Eligible Microsoft 365 E5 and E7 customers receive monthly included SCU capacity
Microsoft Sentinel (Cloud-Native AI SIEM)	Microsoft	▪ Pay-As-You-Go pricing based on GB of data ingested/day ▪ Capacity Reservation pricing available for predictable workloads ▪ Storage billed separately
CrowdStrike Falcon Platform (Charlotte AI-enabled)	CrowdStrike	▪ Falcon Go: USD 59.99/device/year ▪ Falcon Pro: USD 99.99/device/year ▪ Falcon Enterprise: USD 184.99/device/year ▪ Falcon Complete & Charlotte AI: Custom enterprise quotation
Google Security Operations (Chronicle SecOps)	Google Cloud	▪ Standard edition pricing starts at approximately USD 30 per employee/year (public starting price); enterprise deployments priced according to data volume and features
Splunk Enterprise Security	Cisco (Splunk)	▪ Enterprise Security licensing generally starts around USD 20–40 per GB/day of indexed data, depending on deployment model and enterprise agreement. Custom quotations for large environments
Cortex XSIAM	Palo Alto Networks	▪ Enterprise subscription pricing available through custom quotation based on data ingestion, users, and automation requirements
Stellar Cyber Open XDR + AI SOC	Stellar Cyber	▪ Subscription pricing based on protected assets and data volume; custom quotation for enterprise deployments
Dropzone AI	Dropzone AI	▪ Public pricing starts at approximately USD 36,000/year for AI SOC analyst platform; enterprise pricing varies by investigation volume

JULY 2026 © MarketsandMarkets™

Prophet Security AI SOC Platform	Prophet Security	▪ Public pricing starts at approximately USD 50,000 for 5,000 AI investigations; enterprise pricing available via quotation

Note: Pricing shown is based on publicly available information published by vendors and reflects indicative list pricing or starting prices. Actual enterprise pricing varies depending on deployment size, number of endpoints/users, data ingestion volume, cloud consumption, AI compute requirements, service-level agreements (SLAs), contract duration, and negotiated commercial agreements. Most enterprise AI SOC platforms are sold through customized annual subscription or consumption-based licensing models.

Source: Secondary Literature and MarketsandMarkets Analysis

5.6 KEY CONFERENCES & EVENTS, 2026

This section includes upcoming key conferences and events related to the AI SOC market in 2026.

TABLE 10 AI SOC MARKET: DETAILED LIST OF CONFERENCES & EVENTS, 2026

YEAR/ QUARTER	NORTH AMERICA	EUROPE	ASIA PACIFIC	REST OF THE WORLD
Q3 2026	[September] 17th Annual Billington CyberSecurity Summit	[September] Secure AI Summit	-	-
Q4 2026	[October] SecTor 2026 – Black Hat Event [November] SANS AI Cybersecurity Summit Fall 2026	[December] Black Hat Europe 2026 [December] Global AI Security Summit 2026 (GASS 2026)	-	-
Q1 2027	-	-	-	-

Source: Secondary Research

5.7 TRENDS AND DISRUPTIONS IMPACTING CUSTOMER BUSINESS

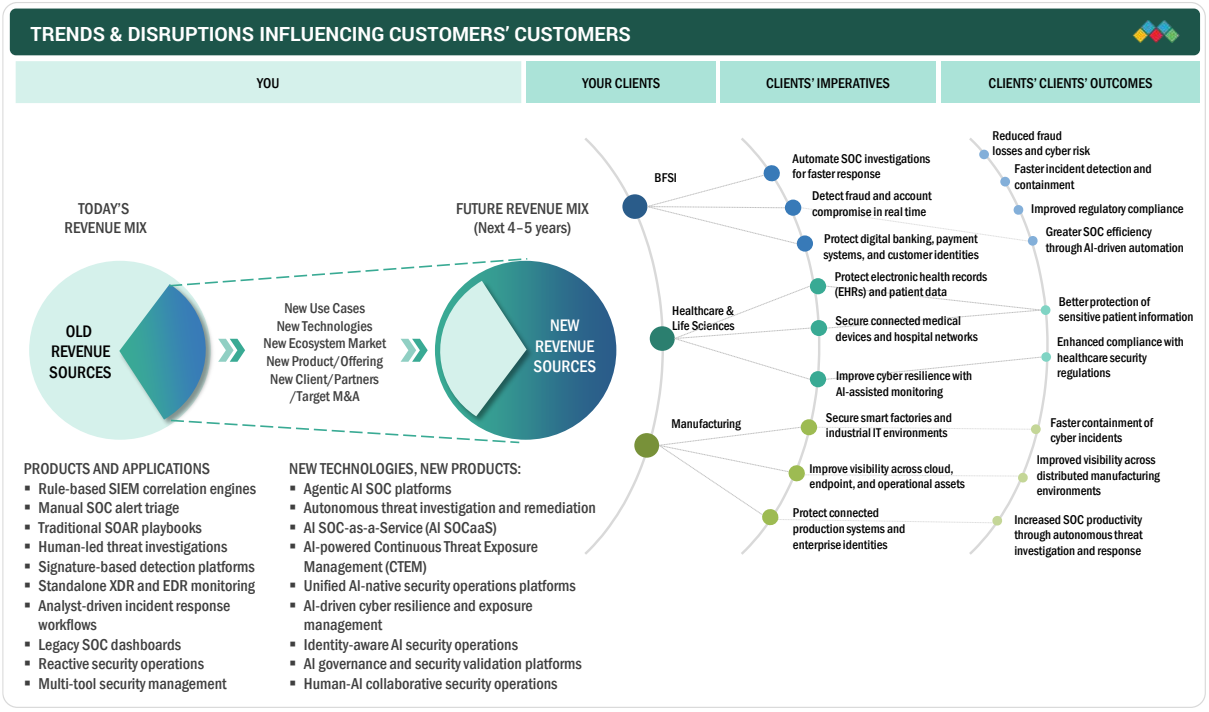
The AI SOC market is undergoing a fundamental transformation as organizations increasingly adopt artificial intelligence to address the growing complexity, speed, and scale of modern cyber threats. Enterprises are moving beyond traditional, analyst-centric SOCs toward AI-native security operations that leverage generative AI, agentic AI, machine learning, and autonomous workflow automation to enhance threat detection, investigation, and incident response. Rising attack sophistication, expanding hybrid cloud environments, identity-centric security challenges, and persistent shortages of skilled cybersecurity professionals are accelerating demand for intelligent security operations platforms. This transition is further supported by the convergence of SIEM, SOAR, XDR, threat intelligence, and AI copilots into unified security platforms that enable continuous monitoring, contextual decision-making, and faster remediation. Recent industry developments, including Microsoft's vision for the Agentic SOC, Gartner's recognition of AI SOC agents, and AI-native security platforms from leading vendors, reinforce the market's shift toward autonomous security operations.

This evolution is enabling AI SOC providers to address mission-critical security priorities across industries such as BFSI, healthcare & life sciences, and manufacturing. Financial institutions are deploying AI SOC platforms to automate fraud detection, identity threat response, and regulatory compliance while protecting digital banking ecosystems. Healthcare organizations are leveraging AI-driven security operations to safeguard electronic health records, connected medical devices, and clinical networks against ransomware and data breaches. Manufacturing enterprises are adopting AI SOC solutions to

JULY 2026 © MarketsandMarkets™

secure hybrid IT environments, cloud-connected production systems, and industrial identities while minimizing operational disruption. These capabilities enable organizations to improve analyst productivity, accelerate threat investigation, reduce incident response times, and strengthen cyber resilience in increasingly complex digital environments.

FIGURE 22 TRENDS/DISRUPTIONS INFLUENCING CUSTOMER BUSINESS



Source: MarketsandMarkets Analysis

The AI SOC market is rapidly progressing from AI-assisted security operations toward fully autonomous, agentic security execution models that can independently investigate, correlate, and respond to cyber threats. Traditional revenue streams centered on SIEM platforms, rule-based automation, and managed monitoring services are gradually expanding toward AI-native offerings such as autonomous investigation engines, AI security agents, continuous threat exposure management (CTEM), and AI SOC-as-a-Service. Vendors are also converging security analytics, threat intelligence, identity protection, and workflow orchestration into unified AI-native platforms capable of delivering continuous, contextual, and machine-speed security operations. This evolution is reshaping the AI SOC from a reactive monitoring function into an intelligent cyber defense platform that continuously adapts to evolving attack techniques.

The technology shift is creating measurable business value across enterprise security operations. Organizations are increasingly deploying AI SOC platforms to automate repetitive analyst tasks, reduce investigation complexity, improve security workflow orchestration, and optimize resource utilization without proportionally increasing SOC staffing. Emerging capabilities including agentic AI, multi-agent security architectures, human-AI collaborative workflows, and AI-driven exposure management are enabling scalable security operations while supporting enterprise expansion across cloud, hybrid, and identity-centric environments. As AI maturity advances, future market growth is expected to be driven by autonomous security execution, adaptive AI governance, and intelligent security platforms that continuously learn from organizational telemetry to improve operational efficiency and cyber resilience.

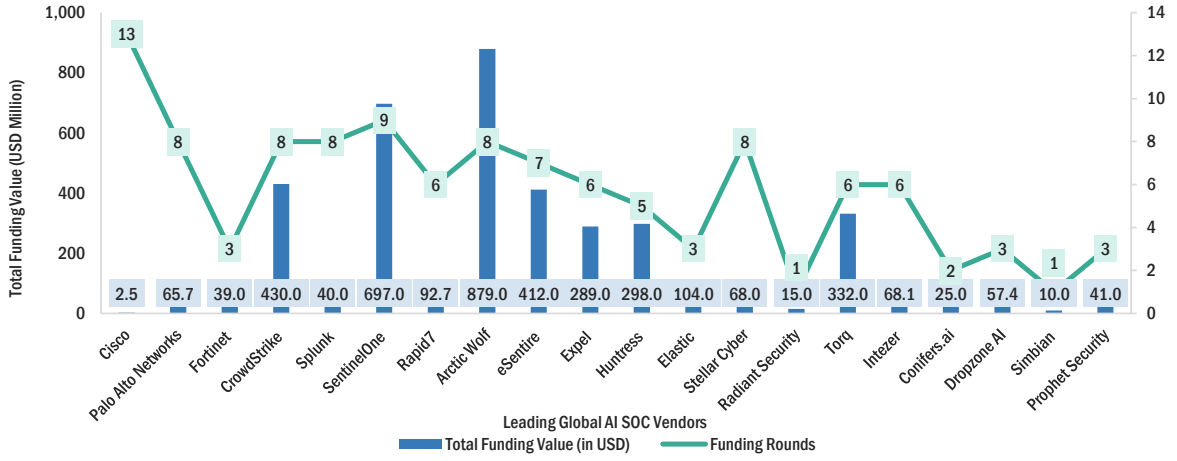
JULY 2026 © MarketsandMarkets™

5.8 INVESTMENT AND FUNDING SCENARIO

The AI SOC market continues to attract substantial venture capital and strategic investment as enterprises accelerate adoption of AI-native cybersecurity platforms, agentic security operations, autonomous threat detection, and security automation. Investment activity has been particularly strong among vendors developing AI-driven SOC platforms, autonomous investigation engines, security copilots, extended detection and response (XDR), and security orchestration technologies. Companies such as Arctic Wolf, SentinelOne, CrowdStrike, and eSentire have secured significant funding, reflecting strong investor confidence in AI-powered security operations, cloud-native SOC architectures, and autonomous cyber defense capabilities. Recent funding rounds for emerging AI SOC vendors such as Torq further demonstrate growing investor interest in agentic AI platforms capable of transforming traditional SOC operations.

At the same time, emerging and high-growth vendors including Expel, Huntress, Stellar Cyber, Intezer, Radiant Security, Prophet Security, Simbian, and Dropzone AI continue to attract investment to expand autonomous SOC capabilities, AI-assisted investigations, MDR, and cloud-native security operations. The funding landscape indicates increasing confidence in technologies that reduce analyst workload, automate incident response, and improve enterprise cyber resilience amid growing alert volumes and increasingly sophisticated cyber threats. As organizations continue modernizing security operations through generative AI, security copilots, and autonomous AI agents, investment momentum is expected to remain strong, particularly for vendors advancing explainable AI, agentic SOC platforms, unified security operations, and AI-native cyber defense ecosystems capable of supporting next-generation enterprise security operations.

FIGURE 23 LEADING GLOBAL AI SOC VENDORS, BY TOTAL FUNDING VALUE AND NUMBER OF FUNDING ROUNDS (USD MILLION)



Source: Secondary Research and MarketsandMarkets Analysis

5.9 CASE STUDY ANALYSIS

This section presents case studies from leading AI SOC vendors, highlighting real-world deployments across industries including financial services, healthcare, manufacturing, energy, and managed security services. These implementations demonstrate how AI-powered SOCs are enabling organizations to automate alert triage, accelerate threat investigation, strengthen incident response, and improve security analyst productivity. By integrating technologies such as generative AI, agentic AI, extended detection and response (XDR), security information and event management (SIEM), and security orchestration, automation and response (SOAR), enterprises are transforming traditional SOCs into intelligent, AI-native security operations platforms capable of managing increasingly sophisticated cyber threats.

JULY 2026 © MarketsandMarkets™

The featured case studies also illustrate the strategic value of AI SOC platforms in addressing persistent security challenges such as alert fatigue, analyst shortages, fragmented security tools, and growing attack complexity. Organizations are leveraging AI-driven security operations to unify telemetry across cloud, endpoint, network, identity, and email environments while enabling autonomous investigations, contextual threat correlation, and guided or automated response workflows. These deployments demonstrate measurable improvements in operational efficiency, investigation speed, threat visibility, and cyber resilience, reinforcing the role of AI SOC as a foundational capability for modern enterprise security operations and next-generation cyber defense strategies.

5.9.1 KEY ENTERPRISE USE CASES OF AI SOC

5.9.1.1 AI-Driven Phishing and Business Email Compromise (BEC) Response

Phishing and Business Email Compromise (BEC) attacks continue to be among the most common initial attack vectors targeting enterprises, making automated email security a critical application of AI-powered Security Operations Centers (SOCs). Modern AI SOC platforms leverage generative AI, behavioral analytics, and large language models (LLMs) to analyze email content, sender reputation, communication patterns, user behavior, and threat intelligence in real time. Unlike traditional rule-based filtering, AI-powered systems identify sophisticated phishing campaigns and impersonation attempts by understanding contextual anomalies rather than relying solely on known indicators of compromise.

Leading AI SOC vendors are increasingly deploying autonomous investigation capabilities that automatically validate suspicious emails, correlate related endpoint, identity, and network activities, determine the attack scope, and recommend or execute predefined response actions such as quarantining emails, disabling compromised accounts, or blocking malicious domains. This significantly reduces analyst workload, accelerates incident response, minimizes successful phishing attacks, and improves organizational resilience against evolving social engineering threats.

5.9.1.2 Autonomous Alert Triage and Threat Investigation

Security Operations Centers receive thousands of security alerts daily, many of which are false positives or low-risk events that consume valuable analyst time. AI SOC platforms are transforming this process by autonomously triaging alerts, correlating telemetry across endpoints, identities, cloud environments, networks, and security tools, and prioritizing only high-confidence incidents requiring human attention. Agentic AI systems dynamically generate investigation plans, collect evidence, enrich alerts with contextual intelligence, and determine the likelihood of malicious activity without relying on predefined playbooks.

This autonomous investigation capability enables organizations to dramatically reduce alert fatigue while improving the consistency and quality of threat investigations. Rather than manually switching between multiple security consoles, analysts receive fully contextualized incidents with investigation summaries, root cause analysis, confidence scores, and recommended remediation actions. As AI reasoning capabilities continue to mature, autonomous alert investigation is becoming one of the defining use cases of next-generation AI-native Security Operations Centers.

5.9.1.3 Identity and Insider Threat Detection

As enterprise environments become increasingly identity-centric, compromised credentials, privilege misuse, and insider threats have emerged as major cybersecurity risks. AI SOC platforms continuously monitor authentication patterns, user behavior, endpoint activity, cloud access, and privileged account usage to establish behavioral baselines and detect anomalous activities that may indicate credential compromise or malicious insider behavior. Machine learning models correlate identity signals with endpoint, network, and cloud telemetry to uncover multi-stage attacks that traditional security tools often fail to detect.

JULY 2026 © MarketsandMarkets™

AI-powered Security Operations Centers also automate investigations by linking identity events with lateral movement, abnormal privilege escalation, unusual data access, and suspicious login behaviors across hybrid environments. Analysts receive prioritized investigations with contextual evidence and recommended containment actions, enabling faster detection of account takeover attempts, insider threats, and identity-based attacks while strengthening enterprise Zero Trust security strategies and reducing business risk.

5.9.1.4 Cloud Security Investigation and Response

The rapid adoption of cloud-native applications, SaaS platforms, containers, and multi-cloud environments has significantly expanded the enterprise attack surface, making cloud security a critical use case for AI-powered SOCs. Modern AI SOC platforms continuously monitor cloud workloads, identities, APIs, storage services, and network activity to detect anomalies such as unauthorized access, privilege escalation, suspicious API calls, and lateral movement across hybrid cloud environments. By correlating cloud telemetry with endpoint, identity, and network data, AI enables security teams to identify complex attack chains that would otherwise remain undetected.

AI-powered investigation engines automatically gather contextual evidence from multiple cloud services, enrich alerts with threat intelligence, and generate comprehensive incident summaries for analysts. Many platforms also recommend or execute predefined remediation actions such as disabling compromised identities, revoking excessive permissions, isolating affected workloads, and blocking malicious sessions. These capabilities improve visibility across distributed cloud environments, reduce investigation time, strengthen cloud resilience, and enable organizations to secure increasingly dynamic enterprise infrastructures.

5.9.1.5 AI-driven Data Loss Prevention (DLP) and Sensitive Data Protection

Protecting sensitive enterprise data has become increasingly complex as organizations adopt cloud collaboration platforms, hybrid work models, and AI-enabled applications. AI-powered Security Operations Centers enhance Data Loss Prevention (DLP) by continuously analyzing user behavior, file access patterns, data movement, and communication channels to identify abnormal activities that may indicate accidental data exposure, insider threats, or malicious exfiltration attempts. Unlike traditional DLP solutions that rely primarily on static policies, AI-driven platforms incorporate behavioral analytics and contextual intelligence to distinguish legitimate business activities from high-risk actions.

When suspicious data movement is detected, AI SOC platforms automatically investigate related endpoint, identity, cloud, and network events to determine the scope and intent of the incident. Security analysts receive prioritized investigations supported by evidence, risk assessments, and recommended containment actions, enabling faster and more accurate decision-making. This approach reduces false positives, strengthens data governance, improves regulatory compliance, and helps organizations safeguard critical intellectual property and sensitive customer information across modern enterprise environments.

JULY 2026 © MarketsandMarkets™

5.9.2 CASE STUDIES

5.9.2.1 St. Luke's University Health Network Enhances Healthcare Cyber Defense with Microsoft Security Copilot and AI-Driven SOC Operations

CLIENT	ST. LUKE'S UNIVERSITY HEALTH NETWORK (PENNSYLVANIA, US)
Vendor	Microsoft (US)
Description	St. Luke's implemented Microsoft Security Copilot to unify security operations across endpoints, identities, cloud workloads, and email security while improving analyst productivity through AI-powered security workflows.
Challenge	Security teams struggled with fragmented visibility across multiple security platforms, time-consuming phishing investigations, and increasing alert volumes requiring manual correlation.
Solution	Microsoft integrated Security Copilot with Defender XDR and Sentinel, enabling AI-assisted investigation, phishing alert triage, incident reporting, and centralized threat visibility across the SOC.
Benefit	The organization saves nearly 200 hours per month on phishing alert triage, creates incident reports in minutes instead of hours, and significantly improves SOC efficiency.

Source: Company Website and Press Release

5.9.2.2 Mondelēz International Modernizes Global Security Operations Through CrowdStrike's AI-Native Falcon Platform

CLIENT	MONDELĒZ INTERNATIONAL
Vendor	CrowdStrike (US)
Description	Mondelēz International partnered with CrowdStrike to modernize its global Security Operations Center (SOC) using the AI-native Falcon platform. The company consolidated endpoint, identity, cloud, and SIEM security into a unified platform, enabling AI-assisted threat detection, investigation, and response across its global enterprise.
Challenge	Mondelēz relied on fragmented security tools, manual investigation processes, and reactive incident response workflows. The organization lacked centralized SOC metrics, standardized detection procedures, and integrated visibility across endpoint, identity, and cloud environments, making rapid threat investigation and remediation difficult.
Solution	CrowdStrike deployed its AI-native Falcon platform, including Falcon Next-Gen SIEM, Falcon Insight XDR, Falcon Identity Protection, Falcon Cloud Security, and Charlotte AI. The integrated platform centralized security telemetry, automated log parsing, enriched investigations with AI, and enabled faster, intelligence-driven security operations.
Benefit	Mondelēz reduced mean time to detect threats to less than 15 minutes and mean time to mitigate incidents to approximately two hours. The company also achieved annual savings of about USD 800,000 in SIEM storage costs and USD 379,000 through improved identity security operations while significantly improving SOC efficiency.

Source: Company Website and Press Release

JULY 2026 © MarketsandMarkets™

5.9.2.3 Fortune 500 Oil & Gas Company Transforms Legacy SOC into an AI-Driven Security Operations Center with Palo Alto Networks Cortex XSIAM

CLIENT	OIL & GAS COMPANY
Vendor	Palo Alto Networks (US)
Description	A Fortune 500 US oil and gas company transformed its legacy Security Operations Center (SOC) by deploying Palo Alto Networks Cortex XSIAM, an AI-driven security operations platform. The organization modernized threat detection, investigation, and response while building a highly automated, best-in-class SOC with unified visibility across security operations.
Challenge	The organization's legacy SIEM generated nearly 90% false-positive alerts, required manual investigations across multiple disconnected security tools, and supported limited data ingestion. These constraints reduced threat visibility, delayed investigations, increased analyst workload, and contributed to significant SOC inefficiencies and analyst fatigue.
Solution	Palo Alto Networks deployed Cortex XSIAM to consolidate SIEM, XDR, SOAR, identity threat detection, attack surface management, and threat intelligence into a single AI-driven platform. Machine learning automated data normalization, incident correlation, behavioral analytics, and response workflows, enabling intelligent, automation-first security operations.
Benefit	The deployment reduced false positives from approximately 90% to virtually zero, cut daily investigations from around 1,000 incidents to 250, reduced median resolution time to 59 minutes, doubled data sources, and significantly improved analyst productivity while creating a mature AI-driven SOC.

Source: Company Website and Press Release

5.9.2.4 US Financial Services Firm Unifies Enterprise Security Operations with Stellar Cyber's AI-Native SecOps Platform

CLIENT	FINANCIAL SERVICES FIRM
Vendor	Stellar Cyber (US)
Description	A financial services firm in the Central United States modernized its Security Operations Center (SOC) using Stellar Cyber's AI-Native SecOps Platform. The organization established a unified AI-powered SOC to correlate alerts across the entire attack surface, automate anomaly detection, and improve analyst productivity through Open XDR capabilities.
Challenge	The firm operated numerous disconnected security tools, including firewalls, SIEM, IDS, IPS, and identity management platforms. Security analysts struggled with overwhelming alert volumes, multiple management consoles, and limited visibility, making it difficult to distinguish genuine threats from false positives and respond efficiently.
Solution	Stellar Cyber deployed its AI-Native SecOps Platform (Open XDR) to unify telemetry from existing security tools into a centralized SOC. Built-in AI and machine learning automated alert correlation, anomaly detection, investigation, and response while providing a single operational console for security analysts.

Benefit	The organization significantly improved analyst productivity, accelerated threat detection and incident response, reduced alert fatigue through automated correlation, and gained unified visibility across its attack surface. The AI-powered SOC enabled faster, more accurate investigations while lowering operational complexity and improving overall security effectiveness.

Source: Company Website and Press Release

5.9.2.5 CarbonHelix Accelerates MSSP Growth Through Intezer's AI-Powered Autonomous Security Operations Center

CLIENT	CARBONHELIX
Vendor	Intezer (US)
Description	CarbonHelix, a managed security services provider (MSSP), adopted Intezer's AI SOC platform to modernize its 24/7 Security Operations Center. The AI-powered platform automated alert triage and threat investigations, enabling the company to efficiently scale SOC operations while delivering faster and more consistent security services to customers.
Challenge	CarbonHelix's analysts manually investigated every security alert, with each incident requiring up to 45 minutes of analysis. The labor-intensive process created operational bottlenecks, limited scalability, increased analyst workload, and made it difficult to deliver rapid, around-the-clock incident response across its growing customer base.
Solution	Intezer deployed its AI SOC platform to automate alert triage, forensic investigation, and threat analysis across CarbonHelix's security operations. The platform required only about 15 minutes for onboarding, enabling rapid deployment with minimal configuration while providing AI-driven investigation and intelligent escalation of high-risk alerts.
Benefit	During the first month, Intezer analyzed more than 78,000 security alerts, while only about 1% required escalation to analysts. Investigation time decreased from 45 minutes to less than five minutes, significantly improving SOC efficiency, accelerating incident response, and supporting scalable business growth.

Source: Company Website and Press Release

5.10 IMPACT OF 2025 US TARIFFS – AI SOC MARKET

5.10.1 INTRODUCTION

The implementation of elevated US tariff measures during 2025 has had a low to moderate impact on the AI SOC market. Unlike hardware-centric cybersecurity segments, AI SOC solutions are primarily delivered through software, cloud-native platforms, Software-as-a-Service (SaaS), and managed security services. Consequently, AI SOC vendors are not directly exposed to tariffs on imported goods to the same extent as manufacturers of networking equipment, industrial hardware, or semiconductor-based security appliances. However, because AI SOC platforms rely heavily on hyperscale cloud infrastructure, AI accelerators, servers, networking equipment, and advanced semiconductors for model training and inference, tariff-related increases in infrastructure costs have indirectly influenced operating expenses across the market.

The indirect impact is most evident in the increasing cost of AI infrastructure supporting modern SOCs. Rising prices of GPUs, AI servers, storage systems, and networking hardware have contributed to higher cloud infrastructure expenditures for hyperscale providers and AI platform operators. These cost pressures may marginally increase subscription pricing or delay infrastructure expansion for some vendors. Nevertheless, enterprise demand for AI-powered threat detection, autonomous investigations, and security automation continues to remain strong, supported by escalating cyber threats, growing SOC analyst

JULY 2026 © MarketsandMarkets™

shortages, and increasing adoption of AI-native cybersecurity platforms. As a result, market growth fundamentals remain significantly stronger than the tariff-related headwinds.

Across 2025 and into 2026, AI SOC vendors are increasingly optimizing infrastructure utilization through cloud-native architectures, AI model optimization, and agentic AI workflows that reduce computational overhead while improving operational efficiency. Organizations are also expanding partnerships with hyperscale cloud providers and adopting subscription-based deployment models that minimize upfront infrastructure investments. These strategies, combined with continued enterprise cybersecurity spending and rapid innovation in generative AI and autonomous security operations, have helped limit the overall impact of tariffs on the AI SOC market. Consequently, the 2025 US tariff environment is expected to influence deployment economics rather than materially slowing AI SOC adoption or long-term market expansion.

Key implications include:

- Overall market impact remains low to moderate because AI SOC solutions are predominantly software-, cloud-, and SaaS-based rather than hardware-centric.
- Rising costs of GPUs, AI servers, semiconductors, and networking equipment are indirectly increasing AI infrastructure and cloud operating expenses.
- AI SOC vendors are accelerating adoption of cloud-native, subscription-based, and managed AI SOC platforms to reduce dependence on customer-owned infrastructure.
- Higher AI infrastructure costs are encouraging greater focus on efficient AI models, autonomous AI agents, and infrastructure optimization.
- Enterprise investments in AI-driven cybersecurity continue to outweigh tariff-related cost pressures due to escalating cyber threats and workforce shortages.
- Partnerships with hyperscale cloud providers and regional infrastructure expansion are helping vendors maintain scalability despite higher infrastructure costs.

Overall, the 2025 US tariff measures have had only a limited indirect impact on the AI SOC market. While tariffs have increased the cost of AI infrastructure components that support cloud-based security operations, the market's software-centric delivery model, subscription-based business models, and sustained enterprise demand for AI-powered cybersecurity have largely mitigated these effects. As AI SOC platforms continue to evolve toward autonomous, cloud-native, and agentic security operations, tariff-related challenges are expected to remain secondary to the market's primary growth drivers.

JULY 2026 © MarketsandMarkets™

5.10.2 KEY TARIFF RATES

TABLE 11 KEY TARIFF RATES

SR. NO.	COUNTRY	KEY AI SOC-RELEVANT COMPONENTS AFFECTED	ESTIMATED TARIFF	EFFECTIVE DATE	AI SOC IMPACT LEVEL	REMARKS/CONFIDENCE LEVEL
1	China	AI servers, networking equipment, semiconductor components, GPUs, data center hardware	~10–25% (selected technology categories)	2025–2026	Moderate	China remains an important supplier of AI infrastructure components. Higher infrastructure costs indirectly increase cloud operating expenses for AI SOC vendors, although software demand remains resilient.
2	United States	Imported AI chips, GPUs, AI servers, cloud infrastructure components	~5–15% (import-dependent segments)	2025–2026	Low–Moderate	AI SOC vendors primarily deliver SaaS solutions. Tariffs mainly influence infrastructure costs rather than demand for AI SOC platforms.
3	Taiwan	Advanced AI chips, GPUs, server motherboards, semiconductor manufacturing	Tariff exposure through semiconductor trade actions	2025–2026	Moderate	Taiwan is the world's leading supplier of advanced AI semiconductors. Any tariff or trade restriction affecting chip supply can indirectly influence AI SOC infrastructure economics.
4	South Korea	AI memory (HBM), DRAM, enterprise storage, semiconductor components	~8–20% (technology products)	2025–2026	Moderate	South Korea plays a critical role in supplying high-bandwidth memory and semiconductor components used in AI servers supporting AI SOC platforms.
5	Japan	High-performance servers, semiconductor manufacturing equipment, networking systems	~5–10%	2025–2026	Low	Japan's contribution lies mainly in semiconductor equipment and precision technologies. Effects on AI SOC remain indirect through infrastructure costs.
6	European Union	Enterprise servers, cloud infrastructure equipment, networking hardware	~6–12%	2025–2026	Low	AI SOC adoption in Europe continues to be driven primarily by cybersecurity demand. Tariffs have only a limited influence on deployment economics.

JULY 2026 © MarketsandMarkets™

7	India	Imported AI servers, GPUs, networking equipment, enterprise data center hardware	~7–18%	2025–2026	Low	India's AI SOC market remains software- and cloud-led. Import costs may increase infrastructure investments, but demand continues to be driven by rapid enterprise digitalization and cybersecurity modernization.

**Tariff rates listed are effective as of July 17, 2026, and are subject to change based on ongoing trade negotiations and regulatory updates.*

Source: WITS, World Bank, White House Press Release, and Desk Research

5.10.3 PRICE IMPACT ANALYSIS

The 2025 US tariff measures on semiconductors, AI servers, networking equipment, and data center infrastructure have had a low to moderate indirect impact on the AI SOC market. Since AI SOC solutions are primarily delivered through cloud-native software, SaaS platforms, and managed security services, tariffs do not directly increase the cost of AI SOC software. Instead, they raise the cost of AI infrastructure, including GPUs, high-performance servers, networking equipment, and hyperscale data centers that support AI model training, inference, and large-scale security analytics. This has increased infrastructure-related operating costs for cloud providers and AI SOC vendors but has had only a limited effect on overall platform pricing.

To mitigate these cost pressures, AI SOC vendors are accelerating the adoption of cloud-first architectures, AI model optimization, and subscription-based delivery models that reduce dependence on customer-owned infrastructure. Enterprises are increasingly adopting SaaS-based AI SOC platforms, managed AI SOC services, and agentic AI capabilities to improve scalability while minimizing upfront capital investments. As demand for AI-driven threat detection, autonomous investigations, and SOC automation continues to grow, vendors are largely absorbing infrastructure cost increases through operational efficiencies rather than significantly increasing prices, ensuring continued market expansion despite tariff-related headwinds.

Strategic responses adopted in the AI SOC market:

- Greater adoption of cloud-native AI SOC platforms to minimize customer infrastructure investments
- Expansion of AI SOC-as-a-Service and managed detection and response (MDR) offerings
- AI model optimization and efficient inference techniques to reduce GPU and compute costs
- Strategic partnerships with hyperscale cloud providers to optimize infrastructure utilization
- Subscription- and usage-based pricing models that distribute infrastructure costs across customers
- Increased investment in autonomous AI agents to improve analyst productivity while controlling operational expenses

JULY 2026 © MarketsandMarkets™

Strategic shift & emerging trends:

- Accelerating migration toward AI-native, cloud-first Security Operations Centers
- Growing deployment of agentic AI for autonomous investigation and response
- Consolidation of SIEM, SOAR, XDR, threat intelligence, and AI copilots into unified security platforms
- Greater emphasis on compute-efficient generative AI models to improve cost efficiency
- Expansion of managed AI SOC services enabling predictable operational expenditure and faster deployment

Overall, while the 2025 US tariff measures have increased the cost of AI infrastructure supporting cloud-based security operations, their impact on AI SOC pricing remains low to moderate because the market is fundamentally software- and SaaS-driven. Rather than significantly increasing platform prices, tariffs are encouraging vendors to optimize AI infrastructure, strengthen cloud partnerships, and expand managed AI SOC delivery models, thereby preserving scalability, pricing stability, and long-term market growth.

5.10.4 IMPACT ON COUNTRY/REGION

5.10.4.1 North America

North America is expected to experience the lowest direct but highest strategic impact from the 2025 US tariff measures within the AI SOC market. Unlike other regions, North America hosts the world's largest concentration of hyperscale cloud providers, AI model developers, cybersecurity software vendors, and managed security service providers. Since AI SOC platforms are predominantly delivered through SaaS and cloud-native architectures, tariffs have not significantly increased software prices. Instead, they have primarily affected investments in AI compute infrastructure, including GPUs, AI servers, networking equipment, and data centers required to support large-scale security analytics and autonomous SOC operations. Despite higher infrastructure costs, strong enterprise cybersecurity spending, continued AI investments by hyperscalers, and federal initiatives supporting AI-enabled cyber defense continue to sustain market growth across the region.

US

The US remains the global innovation hub for AI SOC technologies, hosting leading vendors including Microsoft, Google, CrowdStrike, Palo Alto Networks, Cisco (Splunk), SentinelOne, Arctic Wolf, and numerous AI-native cybersecurity startups. The primary impact of tariffs is visible in AI infrastructure expansion rather than enterprise AI SOC adoption. Higher costs for imported AI chips, networking hardware, and data-center equipment have increased capital expenditure for hyperscalers and AI security vendors building next-generation AI SOC platforms. However, enterprises continue accelerating adoption of autonomous SOCs, AI copilots, and agentic security operations as analyst shortages and sophisticated cyber threats outweigh infrastructure cost pressures. Recent federal initiatives promoting AI-enabled cyber defense are further accelerating investment in AI-assisted security operations across critical infrastructure sectors.

Canada

Canada's AI SOC market is being shaped less by tariffs and more by the country's growing focus on critical infrastructure resilience and AI governance. Financial institutions, utilities, telecommunications providers, and public-sector organizations are increasing investments in AI-assisted security operations following repeated warnings from the Canadian Centre for Cyber Security regarding AI-enabled cyber threats. Rather than developing large domestic AI compute infrastructure, Canadian enterprises increasingly consume AI SOC capabilities through regional cloud providers and managed security partners. This limits direct tariff

JULY 2026 © MarketsandMarkets™

exposure while accelerating demand for cloud-delivered AI SOC platforms, threat intelligence, and AI-powered incident response services.

Mexico

Mexico's AI SOC market is evolving alongside the country's rapid expansion as a North American manufacturing and nearshoring destination. Growth in automotive, electronics, logistics, and manufacturing sectors is increasing demand for AI-driven security operations capable of protecting hybrid IT, cloud, and operational technology environments. While tariffs have moderately increased costs for imported AI infrastructure used by service providers, most Mexican enterprises continue adopting subscription-based AI SOC and MDR services instead of investing in dedicated AI infrastructure. Cross-border business operations with US enterprises are also encouraging greater adoption of AI-powered SOC platforms to meet cybersecurity requirements across regional supply chains.

Market Challenges:

- Higher capital expenditure for AI data centers, GPUs, and hyperscale cloud infrastructure supporting AI SOC platforms
- Continued dependence on imported AI chips, advanced networking equipment, and high-performance computing infrastructure
- Increasing AI-driven cyber threats targeting financial services, healthcare, energy, and critical infrastructure
- Shortage of experienced AI security engineers and SOC analysts despite increasing automation
- Rising compliance requirements for AI governance, cybersecurity, and critical infrastructure protection across North America

Mitigation Measures:

- Expansion of hyperscale AI cloud infrastructure across the US and Canada to reduce long-term infrastructure constraints
- Greater adoption of SaaS-based AI SOC, MDR, and Security Operations-as-a-Service models that minimize customer infrastructure investment
- Increased optimization of AI models to improve inference efficiency and reduce GPU utilization
- Strengthening public-private collaboration on AI-enabled cyber defense through federal cybersecurity initiatives
- Diversification of semiconductor sourcing and continued investment in regional AI infrastructure to improve long-term supply-chain resilience

5.10.4.2 Europe

The European AI SOC market is experiencing a moderate but primarily compliance-driven impact from the 2025 US tariff measures. Unlike North America, where AI infrastructure expansion dominates market dynamics, Europe's response is shaped by its emphasis on digital sovereignty, trusted AI, and regulatory compliance. Higher costs for imported AI servers, GPUs, networking equipment, and cloud infrastructure are encouraging organizations to optimize AI investments while accelerating the adoption of sovereign cloud environments and AI platforms that comply with European cybersecurity and privacy requirements. At the same time, the phased implementation of the EU AI Act, alongside NIS2 and the Cyber Resilience Act, is increasing demand for AI SOC platforms capable of delivering explainable AI, continuous monitoring, automated compliance reporting, and secure AI governance. These regulatory and technological developments continue to support AI SOC adoption despite infrastructure cost pressures.

JULY 2026 © MarketsandMarkets™

Germany

Germany represents Europe's largest enterprise AI SOC market, supported by its advanced manufacturing sector, automotive industry, industrial software ecosystem, and strong cybersecurity investments. The primary tariff impact is being felt through higher costs for AI computing infrastructure supporting enterprise AI deployments rather than AI SOC software itself. German organizations are increasingly integrating AI SOC platforms with Industry 4.0 environments, industrial cybersecurity operations, and Security Operations Centers that monitor both IT and OT. Simultaneously, enterprises are prioritizing AI solutions that align with the EU AI Act and Germany's focus on secure industrial digitalization, creating strong demand for transparent and auditable AI-driven security operations.

France

France's AI SOC market is being shaped by the country's strategic investments in sovereign AI infrastructure, national cloud capabilities, and cybersecurity modernization. Rather than relying extensively on foreign AI ecosystems, French enterprises and public-sector organizations are increasingly investing in trusted AI platforms that support data sovereignty and regulatory compliance. Although tariff-related increases in AI infrastructure costs have affected hyperscale computing investments, organizations continue expanding AI-powered SOC capabilities across banking, defense, healthcare, and public administration. Government initiatives promoting domestic AI innovation are further strengthening demand for AI-native security operations designed around European governance principles and trusted AI frameworks.

UK

The UK follows a distinct AI strategy compared with the European Union, emphasizing innovation-led AI governance while strengthening AI cybersecurity standards through initiatives such as the AI Cyber Security Code of Practice. Rising costs for AI infrastructure have encouraged UK enterprises to increase adoption of cloud-delivered AI SOC platforms, managed detection and response (MDR), and AI-assisted security operations instead of expanding dedicated on-premises AI infrastructure. Financial services, healthcare, telecommunications, and government organizations continue investing heavily in AI-driven SOC automation to improve cyber resilience while balancing operational efficiency with evolving AI security requirements.

Market Challenges:

- Rising costs for imported AI compute infrastructure, GPUs, and advanced networking equipment supporting AI SOC platforms
- Complex compliance requirements arising from the EU AI Act, NIS2, GDPR, and Cyber Resilience Act
- Dependence on non-European cloud infrastructure and AI foundation models for enterprise AI workloads
- Balancing AI innovation with explainability, transparency, and regulatory accountability
- Limited availability of highly specialized AI security professionals with expertise in both cybersecurity and AI governance

Mitigation Measures:

- Expansion of sovereign cloud initiatives and trusted European AI infrastructure
- Adoption of AI SOC platforms incorporating explainable AI, governance, and automated compliance capabilities
- Increased investment in regional AI data centers and secure cloud computing capacity

JULY 2026 © MarketsandMarkets™

- Greater collaboration between governments, cybersecurity vendors, and research institutions to strengthen AI resilience
- Diversification of AI technology partnerships while reducing dependence on imported AI infrastructure and external cloud ecosystems

5.10.4.3 Asia Pacific

The Asia Pacific AI SOC market is witnessing a low-to-moderate indirect impact from the 2025 US tariff measures, although the implications vary significantly across countries due to the region's role in global AI infrastructure and semiconductor supply chains. Unlike Europe, where regulatory compliance drives adoption, or North America, where hyperscale cloud providers dominate, Asia Pacific's AI SOC ecosystem is closely linked to AI hardware manufacturing, sovereign AI initiatives, and government-backed digital transformation programs. Rising prices for GPUs, AI accelerators, advanced servers, and networking equipment have marginally increased infrastructure costs for AI-powered security platforms. However, sustained investments in domestic AI capabilities, regional cloud infrastructure, and cybersecurity modernization continue to support strong demand for AI-native SOC solutions across enterprises and public-sector organizations.

China

China remains one of the world's largest AI markets, supported by extensive investments in domestic AI models, cloud infrastructure, and cybersecurity technologies. Export controls and semiconductor-related trade restrictions have accelerated the country's emphasis on indigenous AI innovation and locally developed computing infrastructure. Consequently, Chinese enterprises are increasingly deploying AI SOC platforms built on domestic AI models, regional cloud ecosystems, and locally developed cybersecurity technologies. Rather than slowing AI SOC adoption, geopolitical pressures are reinforcing investments in autonomous security operations, AI-assisted threat intelligence, and intelligent SOC automation as part of China's broader AI self-reliance strategy.

India

India is emerging as one of the fastest-growing AI SOC markets, driven by rapid enterprise digitalization, expanding cybersecurity investments, and the Government's IndiaAI Mission. Rather than being constrained by tariff-related cost pressures, organizations are increasingly leveraging cloud-based AI SOC platforms and managed AI security services that reduce upfront infrastructure investment. Financial institutions, IT services providers, telecom operators, and government agencies are accelerating adoption of AI-powered threat detection, SOC automation, and AI-assisted incident response. Simultaneously, public investments in GPU infrastructure, indigenous AI models, and AI governance frameworks are strengthening the country's long-term AI cybersecurity ecosystem.

Japan

Japan's AI SOC market is being shaped by national investments in trusted AI infrastructure, high-performance computing, and secure enterprise AI adoption. Large enterprises across financial services, manufacturing, and telecommunications are expanding AI-driven security operations while emphasizing reliability, explainability, and operational resilience. Although higher AI infrastructure costs have influenced capital expenditure planning, organizations continue investing in AI SOC platforms to address workforce shortages and increasingly sophisticated cyber threats. Government-backed initiatives to strengthen domestic AI compute capacity are expected to improve long-term availability of AI infrastructure supporting enterprise security operations.

JULY 2026 © MarketsandMarkets™

Market Challenges:

- Rising costs of GPUs, AI accelerators, and advanced computing infrastructure supporting AI SOC workloads
- Continued dependence on imported high-performance AI chips in several regional markets
- Diverse AI governance and cybersecurity regulations across APAC economies
- Shortage of experienced AI security engineers and SOC automation specialists
- Balancing rapid AI innovation with data localization, cybersecurity, and national security requirements

Mitigation Measures:

- Expansion of sovereign AI initiatives and government-supported AI compute infrastructure
- Increased adoption of cloud-native AI SOC platforms and AI-powered managed security services
- Greater investment in indigenous AI models, cybersecurity innovation, and regional AI ecosystems
- Diversification of AI hardware supply chains and regional semiconductor manufacturing capabilities
- Workforce development programs focused on AI, cybersecurity, and autonomous security operations

5.10.5 IMPACT ON END-USE INDUSTRIES

BFSI:

- Banking and financial institutions are witnessing ~5–12% increases in AI SOC operating costs due to higher cloud AI infrastructure, GPU compute, and cybersecurity platform expenses, while software subscription pricing remains largely stable.
- Rapid adoption of AI-powered fraud detection, automated alert triage, identity threat detection, and autonomous SOC investigations is improving detection speed and reducing analyst workload as cyberattacks become increasingly sophisticated.
- Financial institutions are expanding investments in AI-native SIEM, SOAR, XDR, and continuous threat exposure management (CTEM) platforms to strengthen cyber resilience, regulatory compliance, and operational efficiency.
- Growing reliance on managed AI SOC services and AI-assisted security operations is helping address cybersecurity talent shortages while enabling 24×7 threat monitoring and faster incident response.

Healthcare & Life Sciences:

- Healthcare organizations are experiencing ~4–10% increases in AI infrastructure and cloud computing costs supporting AI-driven security operations, while demand for AI SOC platforms continues to rise because of increasing ransomware attacks and stricter data protection requirements.
- Hospitals, pharmaceutical companies, and healthcare providers are increasingly deploying AI-powered threat detection, medical IoT security monitoring, identity protection, and automated incident response to safeguard sensitive patient information and connected clinical systems.

JULY 2026 © MarketsandMarkets™

- Organizations are integrating AI SOC platforms with Zero Trust security, cloud security, and threat intelligence to secure hybrid healthcare environments spanning on-premises infrastructure, cloud workloads, and medical devices.
- Growing adoption of SaaS-based AI SOC and managed detection and response (MDR) services enables healthcare organizations to strengthen cyber resilience without major investments in dedicated AI infrastructure.

Manufacturing:

- Manufacturing enterprises are experiencing low-to-moderate (6–15%) increases in AI infrastructure costs supporting AI-powered security operations due to higher prices for GPUs, AI servers, and cloud computing resources required for large-scale security analytics. However, SaaS-based AI SOC platforms and hyperscale cloud deployments continue to reduce overall cost pressures for manufacturers.
- Manufacturers are rapidly adopting AI SOC platforms to detect ransomware, supply chain compromises, insider threats, identity-based attacks, and anomalies across converged IT, OT, IoT, and Industry 4.0 environments. The increasing digitalization of production facilities and connected factories is accelerating investment in AI-driven security operations.
- Growing deployment of AI-powered XDR, behavioral analytics, agentic investigations, and autonomous threat correlation is improving protection of industrial networks, connected production systems, and smart manufacturing environments. These capabilities enable faster identification of sophisticated cyber threats while enhancing cyber resilience across distributed manufacturing operations.
- Enterprises are expanding investments in cloud-native AI SOC platforms, MDR, unified IT-OT security operations, and AI-assisted SOC automation to improve operational resilience, simplify security management, and address persistent shortages of skilled cybersecurity professionals supporting manufacturing environments.

JULY 2026 © MarketsandMarkets™

6 TECHNOLOGICAL ADVANCEMENTS, AI-DRIVEN IMPACT, PATENTS, INNOVATIONS, AND FUTURE APPLICATIONS

6.1 TECHNOLOGY ANALYSIS

The AI SOC market is evolving rapidly as organizations modernize security operations to address the increasing volume, sophistication, and speed of cyber threats. The widespread adoption of cloud computing, hybrid work, SaaS applications, AI-enabled attacks, and distributed IT environments has significantly expanded the enterprise attack surface, making traditional SOCs increasingly difficult to scale. As a result, organizations across industries such as BFSI, healthcare, manufacturing, government, and technology are adopting AI-native security operations platforms that leverage generative AI, large language models (LLMs), machine learning, and autonomous AI agents to automate alert triage, threat detection, investigation, and incident response. These capabilities enable security teams to reduce analyst fatigue, improve operational efficiency, and accelerate response to increasingly complex cyberattacks.

Advancements in agentic AI, extended detection and response (XDR), security information and event management (SIEM), security orchestration, automation and response (SOAR), and AI-powered threat intelligence are fundamentally transforming modern SOC architectures. Rather than operating as isolated security tools, AI SOC platforms are evolving into unified security operations ecosystems that continuously correlate telemetry across endpoints, identities, networks, cloud workloads, applications, and external threat intelligence sources. By combining real-time analytics, contextual reasoning, automated investigations, and intelligent response orchestration, these platforms enable proactive threat detection, predictive risk management, and continuous security operations while improving overall cyber resilience.

In this rapidly evolving landscape, technological innovation has become a key differentiator for AI SOC vendors seeking to deliver autonomous, scalable, and intelligence-driven security operations. Enterprises increasingly prioritize AI SOC solutions that integrate seamlessly with existing cybersecurity ecosystems, support multi-cloud and hybrid environments, provide explainable AI-driven decision-making, and enable secure human-AI collaboration under Zero Trust principles. This technology analysis categorizes the AI SOC ecosystem into key, complementary, and adjacent technologies, each contributing to intelligent threat detection, automated response, continuous exposure management, and enterprise-wide cyber resilience.

6.1.1 KEY EMERGING TECHNOLOGIES

6.1.1.1 Agentic AI for Autonomous Security Operations

Agentic AI is rapidly emerging as the defining technology for next-generation AI SOCs, enabling security platforms to move beyond rule-based automation toward autonomous decision-making. Unlike traditional SOAR workflows or AI copilots that assist analysts, agentic AI deploys multiple intelligent agents capable of independently triaging alerts, correlating telemetry from SIEM, XDR, identity, cloud, and threat intelligence platforms, conducting investigations, and recommending or executing response actions under human oversight. Leading vendors such as Google Cloud (Agentic SOC), Microsoft, Palo Alto Networks, Cisco, SentinelOne, and CrowdStrike are embedding agentic capabilities into their security platforms to reduce analyst workload and accelerate incident response.

The technology is particularly valuable in addressing cybersecurity talent shortages, alert fatigue, and increasingly sophisticated AI-enabled cyberattacks. Modern agentic AI platforms perform multi-step reasoning, maintain contextual memory, collaborate across specialized AI agents, and continuously learn from analyst feedback to improve future investigations. Enterprises are using these capabilities for autonomous alert enrichment, threat hunting, malware investigation, detection engineering, and policy-driven response orchestration. While organizations continue to maintain human approval for high-risk

JULY 2026 © MarketsandMarkets™

actions, agentic AI is significantly reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), positioning autonomous SOCs as the future operating model for enterprise security operations.

6.1.1.2 AI-Powered Continuous Threat Exposure Management (CTEM)

AI-powered Continuous Threat Exposure Management (CTEM) is transforming cybersecurity from reactive incident response to proactive risk reduction. Rather than relying on periodic vulnerability scans or isolated penetration tests, AI-enabled CTEM platforms continuously discover assets, analyze attack paths, correlate vulnerabilities with business context, and prioritize remediation based on exploitability and organizational risk. Machine learning models continuously evaluate changes across cloud, identity, endpoint, network, and application environments, enabling security teams to identify the most critical exposures before adversaries can exploit them. CTEM is increasingly integrated with vulnerability management, attack surface management, threat intelligence, and security validation platforms.

Within AI SOC environments, CTEM provides continuous prioritization of security risks while automating remediation workflows and improving analyst decision-making. Organizations are leveraging AI-driven exposure analytics to reduce false positives, optimize patch management, validate security controls, and strengthen cyber resilience. The technology supports strategic initiatives such as Zero Trust, cyber resilience, and continuous compliance by shifting SOC operations from alert-centric workflows toward risk-centric security management. As attack surfaces expand across hybrid cloud, SaaS, AI workloads, and distributed enterprises, AI-powered CTEM is becoming a foundational capability for modern AI-native security operations.

6.1.1.3 Large Language Model (LLM)-Driven Security Copilots

Large Language Models (LLMs) are fundamentally reshaping how SOC analysts interact with cybersecurity platforms through AI-powered security copilots. Modern AI SOC solutions increasingly embed enterprise-grade LLMs to summarize alerts, explain attack chains, generate investigation hypotheses, perform natural-language threat hunting, create detection rules, automate incident documentation, and assist with malware analysis. Vendors including Microsoft Security Copilot, Google Gemini Security, CrowdStrike Charlotte AI, Palo Alto Networks Cortex, and SentinelOne Purple AI are integrating generative AI directly into security operations, allowing analysts to interact with complex security data using conversational interfaces rather than manual queries.

Beyond productivity improvements, LLM-driven copilots enable organizations to preserve institutional knowledge, standardize investigations, and accelerate analyst onboarding. By combining enterprise telemetry, threat intelligence, MITRE ATT&CK mappings, and historical incidents, these copilots deliver contextual recommendations while maintaining human oversight for critical decisions. They reduce alert fatigue, improve reporting quality, and significantly shorten investigation cycles. As organizations adopt Retrieval-Augmented Generation (RAG), domain-specific security models, and secure enterprise AI architectures, LLM-powered copilots are evolving into intelligent analyst assistants that enhance both operational efficiency and security decision-making without replacing human expertise.

6.1.1.4 AI-Native Extended Detection and Response (XDR)

AI-native Extended Detection and Response (XDR) is redefining enterprise threat detection by unifying telemetry across endpoints, identities, cloud workloads, email, networks, applications, and operational technology into a single intelligent security platform. Unlike conventional SIEM or standalone detection tools, AI-native XDR applies machine learning, behavioral analytics, and real-time correlation to identify sophisticated multi-stage attacks that span multiple security domains. AI continuously prioritizes incidents based on business risk, enriches investigations using global threat intelligence, and recommends or automates containment actions, significantly improving SOC efficiency and threat visibility.

The technology has become a central intelligence layer within modern AI SOC architectures, enabling security teams to reduce false positives while improving detection accuracy across increasingly distributed enterprise environments. Organizations are deploying AI-native XDR to strengthen ransomware defense,

JULY 2026 © MarketsandMarkets™

insider threat detection, identity protection, cloud workload security, and hybrid infrastructure monitoring. Integration with generative AI, automated response playbooks, and agentic investigation capabilities further enables autonomous incident analysis and response orchestration. As enterprises consolidate multiple security products into unified AI-driven platforms, AI-native XDR is becoming a strategic foundation for scalable, cloud-native, and intelligent security operations.

6.1.1.5 Multi-Agent Security Orchestration and Autonomous Incident Response

Multi-agent security orchestration represents the next evolution of AI SOC automation, where multiple specialized AI agents collaborate to perform complex cybersecurity workflows simultaneously. Instead of relying on a single AI model, specialized agents independently conduct threat hunting, alert triage, malware analysis, digital forensics, vulnerability assessment, compliance validation, and response orchestration while exchanging contextual information through secure orchestration frameworks. This distributed AI architecture enables parallel investigations, adaptive reasoning, and dynamic task delegation across enterprise security environments, significantly improving operational scalability and response speed.

Real-world enterprise deployments increasingly combine multi-agent orchestration with Model Context Protocol (MCP), Retrieval-Augmented Generation (RAG), and secure workflow governance to ensure explainability, policy enforcement, and human oversight. These architectures enable AI SOC platforms to coordinate investigations across SIEM, SOAR, XDR, cloud security, identity systems, and threat intelligence platforms while minimizing analyst intervention. As organizations pursue autonomous security operations, multi-agent orchestration is expected to become a core enabling technology for intelligent, resilient, and highly scalable AI SOC ecosystems capable of responding to machine-speed cyber threats while maintaining governance, transparency, and regulatory compliance.

6.1.2 COMPLEMENTARY TECHNOLOGIES

6.1.2.1 Cloud-Native Application Protection Platform (CNAPP)

Cloud-Native Application Protection Platforms (CNAPPs) have become one of the most important complementary technologies for AI SOCs as enterprises increasingly operate applications across hybrid and multi-cloud environments. CNAPP unifies cloud security posture management (CSPM), cloud workload protection (CWPP), cloud infrastructure entitlement management (CIEM), Kubernetes security, API protection, and software supply chain security into a single platform. Rather than generating isolated security findings, modern CNAPP solutions continuously assess cloud assets, identify attack paths, prioritize risks based on business context, and provide actionable telemetry to AI SOC platforms. Gartner identifies deep integration with SIEM, SOAR, XDR, and SOC platforms as a defining capability of mature CNAPP offerings, reflecting the industry's shift toward unified cloud and security operations.

Within AI SOC environments, CNAPP provides valuable cloud context that significantly improves AI-driven threat detection, investigation, and response. AI models combine CNAPP telemetry with endpoint, identity, and network signals to detect sophisticated cloud attacks such as privilege escalation, container compromise, lateral movement, exposed APIs, and workload misconfigurations. Leading vendors including Microsoft, Palo Alto Networks, Wiz, CrowdStrike, and Google Cloud are increasingly integrating CNAPP with AI-powered SOC workflows to deliver unified visibility across code, cloud, and runtime environments. This convergence enables faster attack-path analysis, automated risk prioritization, and cloud-native incident response while reducing alert fatigue and improving overall cyber resilience in modern enterprise environments.

JULY 2026 © MarketsandMarkets™

6.1.2.2 Identity Threat Detection and Response (ITDR)

Identity Threat Detection and Response (ITDR) has emerged as a critical complementary technology for AI SOCs as identity-based attacks continue to dominate modern cyber intrusions. Since compromised credentials, privilege escalation, session hijacking, and identity misuse are frequently involved in ransomware campaigns and advanced persistent threats, organizations are increasingly deploying ITDR solutions to continuously monitor authentication events, privileged accounts, Active Directory, cloud identities, and identity infrastructure. ITDR combines behavioral analytics, identity intelligence, and threat detection to identify suspicious user activity, detect compromised credentials, and prevent unauthorized access before attackers can establish persistence or move laterally across enterprise environments.

When integrated with AI SOC platforms, ITDR provides essential identity context that enables AI engines to correlate identity signals with endpoint, network, cloud, and application telemetry for more accurate investigations. AI-powered SOCs leverage ITDR to automate identity risk scoring, detect abnormal authentication behavior, investigate insider threats, and recommend or initiate response actions such as session termination, credential resets, privilege revocation, or adaptive access controls. As Zero Trust architectures become standard across enterprises, ITDR is increasingly serving as the intelligence layer that enables identity-centric security operations, helping organizations reduce false positives, accelerate investigations, and strengthen protection against credential-based attacks across hybrid and cloud-native environments.

6.1.2.3 Threat Intelligence Platforms (TIPs)

Threat Intelligence Platforms (TIPs) have become an essential complementary technology for AI SOCs by providing continuously updated cyber threat intelligence from internal telemetry, commercial feeds, open-source intelligence, industry sharing communities, and government advisories. Modern TIPs aggregate indicators of compromise (IOCs), attacker tactics, techniques, and procedures (TTPs), malware intelligence, vulnerability intelligence, exploit activity, and adversary profiles into a centralized knowledge base. By normalizing and enriching threat data using frameworks such as MITRE ATT&CK, TIPs enable AI SOC platforms to better understand evolving attack campaigns, prioritize high-risk alerts, and improve contextual decision-making during security investigations.

AI SOC platforms increasingly integrate TIPs with SIEM, XDR, SOAR, EDR, and cloud security solutions to automate threat enrichment, correlate alerts with global threat campaigns, and support proactive threat hunting. Artificial intelligence further enhances TIP capabilities by identifying emerging attack patterns, filtering irrelevant intelligence, summarizing adversary behavior, and recommending mitigation actions based on organizational risk. Leading cybersecurity vendors integrate threat intelligence directly into AI-driven security operations to improve detection accuracy, accelerate incident response, and strengthen cyber resilience. As cyber threats continue to evolve rapidly, TIPs are becoming indispensable for enabling predictive, intelligence-driven, and highly automated AI SOC operations across enterprise environments.

6.1.3 ADJACENT TECHNOLOGIES

6.1.3.1 Cyber Asset Attack Surface Management (CAASM)

Cyber Asset Attack Surface Management (CAASM) has emerged as a critical adjacent technology for AI SOCs by providing a unified inventory of enterprise cyber assets across endpoints, cloud environments, identities, applications, IoT devices, and security tools. Rather than discovering assets independently, CAASM aggregates information through API integrations with existing security and IT platforms to eliminate visibility gaps and identify unmanaged or unprotected assets. Gartner increasingly positions CAASM as a foundational capability within Continuous Threat Exposure Management (CTEM), enabling organizations to understand their complete attack surface and continuously assess cyber exposure across hybrid enterprise environments.

JULY 2026 © MarketsandMarkets™

When integrated with AI SOC platforms, CAASM significantly improves AI-driven detection, investigation, and response by providing complete asset context for every security alert. AI models leverage CAASM data to correlate vulnerabilities with asset criticality, identify missing security controls, prioritize incidents based on business impact, and automate remediation workflows. Organizations across BFSI, healthcare, manufacturing, and government sectors increasingly use CAASM to validate security coverage, support Zero Trust initiatives, improve regulatory compliance, and accelerate threat hunting. As enterprises adopt AI-native SOC architectures, CAASM is becoming an essential intelligence layer that enables more accurate risk prioritization, reduces analyst workload, and strengthens overall cyber resilience through continuous asset visibility.

6.1.3.2 Breach and Attack Simulation (BAS)

Breach and attack simulation (BAS) has become an important adjacent technology for AI SOCs by continuously validating an organization's cybersecurity posture through automated simulation of real-world cyberattacks. Instead of waiting for actual incidents, BAS platforms emulate adversary techniques such as ransomware deployment, phishing, privilege escalation, lateral movement, and data exfiltration using frameworks like MITRE ATT&CK. These simulations help organizations evaluate the effectiveness of security controls, detection rules, incident response playbooks, and SOC workflows without disrupting production environments. As cyber threats evolve rapidly, BAS enables continuous security validation rather than relying solely on periodic penetration testing.

AI SOC platforms increasingly integrate BAS outputs to improve detection engineering, optimize AI models, and continuously refine automated response workflows. Simulation results provide valuable feedback that helps AI engines identify detection gaps, reduce false positives, prioritize remediation, and recommend improvements to security policies. Large enterprises in financial services, healthcare, telecommunications, and critical infrastructure use BAS to measure cyber resilience, validate compliance requirements, and strengthen SOC readiness against emerging attack techniques. As autonomous security operations mature, BAS is becoming a key mechanism for continuously training and validating AI SOC capabilities, ensuring that AI-driven detections remain effective against evolving threat landscapes.

6.1.3.3 Secure Access Service Edge (SASE)

Secure Access Service Edge (SASE) has emerged as a major adjacent technology for AI SOCs by converging networking and cloud-delivered security into a unified architecture. SASE integrates Software-Defined WAN (SD-WAN), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall-as-a-Service (FWaaS), and Zero Trust Network Access (ZTNA) to provide secure connectivity for distributed users, branch offices, cloud applications, and remote workforces. As enterprises increasingly adopt hybrid work models and cloud-first strategies, SASE generates rich telemetry on users, devices, applications, and network behavior that significantly enhances AI-driven security operations.

Within AI SOC environments, SASE provides real-time network and identity intelligence that enables AI models to detect anomalous user behavior, compromised credentials, insider threats, and policy violations across distributed environments. AI-powered SOC platforms correlate SASE telemetry with endpoint, cloud, email, and identity signals to accelerate investigations, automate incident response, and improve risk-based decision-making. Organizations across banking, healthcare, retail, and global enterprises increasingly integrate SASE with AI-native SOC platforms to support Zero Trust architectures, reduce alert fatigue, and secure hybrid digital ecosystems. This convergence is enabling security teams to deliver unified visibility, faster threat containment, and more adaptive cyber defense across increasingly complex enterprise environments.

JULY 2026 © MarketsandMarkets™

6.2 TECHNOLOGY/PRODUCT ROADMAP

The AI SOC market is entering a transformative phase driven by rapid advancements in generative AI, agentic AI, large language models (LLMs), and autonomous security operations. Traditional SOCs built around manual investigations, rule-based workflows, and fragmented security tools are evolving into AI-native security operations platforms capable of continuously detecting, investigating, prioritizing, and responding to threats with minimal human intervention. As enterprises expand hybrid cloud environments, SaaS adoption, remote workforces, and digital ecosystems, organizations are prioritizing intelligent SOC architectures that integrate SIEM, XDR, SOAR, threat intelligence, identity security, and AI-powered analytics into a unified operational platform. This shift is enabling security teams to improve detection accuracy, reduce analyst fatigue, accelerate incident response, and strengthen cyber resilience against increasingly sophisticated cyber threats.

The rapid evolution of AI-powered cyberattacks, identity-based threats, cloud-native attacks, and ransomware campaigns is accelerating investments in autonomous SOC technologies and AI-driven security operations. Vendors are increasingly embedding agentic AI, security copilots, automated reasoning engines, and continuous exposure management capabilities into their platforms to support end-to-end SOC automation. At the same time, enterprises are emphasizing explainable AI, governance frameworks, and human-AI collaboration to ensure trustworthy adoption of autonomous security operations. The roadmap below outlines the key technology, product, and adoption milestones expected to shape the AI SOC market as it evolves from AI-assisted security operations toward autonomous, self-optimizing cyber defense platforms.

6.2.1 SHORT-TERM (2026–2027) | FOUNDATION & EARLY COMMERCIALIZATION

Focus Areas:

Core Technology Development

- Expansion of AI-powered alert triage and investigation engines using generative AI and large language models (LLMs)
- Integration of SIEM, XDR, SOAR, identity security, and threat intelligence into unified AI-native SOC platforms
- Development of AI security copilots that assist analysts with incident summarization, root cause analysis, and remediation recommendations
- Growing adoption of cloud-native AI SOC architectures supporting hybrid and multi-cloud security operations

Product Innovations

- Launch of AI SOC platforms with automated alert prioritization, investigation workflows, and contextual threat correlation
- Introduction of security copilots capable of generating investigation reports, attack timelines, and remediation guidance
- Development of subscription-based AI SOC platforms integrating endpoint, cloud, identity, and network telemetry
- Expansion of AI-assisted threat hunting and workflow automation capabilities to reduce SOC analyst workload

JULY 2026 © MarketsandMarkets™

Market Adoption

- Strong enterprise adoption across BFSI, healthcare & life sciences, manufacturing, government, and technology sectors
- Increasing deployment of AI-enabled SIEM modernization and cloud-native SOC transformation initiatives
- Strategic partnerships between cybersecurity vendors, hyperscale cloud providers, and AI foundation model providers
- Rising adoption of managed AI SOC services among mid-sized enterprises addressing cybersecurity talent shortages

6.2.2 MID-TERM (2027–2030) SCALING, AUTONOMY & ECOSYSTEM EXPANSION

Focus Areas:

Core Technology Development

- Maturation of agentic AI systems capable of autonomous investigations, reasoning, and policy-driven response orchestration
- Expansion of Continuous Threat Exposure Management (CTEM) integrated with AI SOC platforms for proactive risk reduction
- Development of multi-agent AI architectures coordinating threat hunting, malware analysis, identity security, and cloud security operations
- Increased adoption of explainable AI, AI governance, and trust frameworks supporting enterprise-scale autonomous SOC deployments

Product Innovations

- Commercial deployment of autonomous AI SOC platforms capable of executing end-to-end investigation and response workflows
- Introduction of industry-specific AI SOC solutions tailored for BFSI, healthcare, manufacturing, public sector, and critical infrastructure
- Expansion of unified AI-native security operations platforms integrating CNAPP, ITDR, DSPM, SASE, and exposure management
- Development of AI-driven security knowledge graphs enabling advanced contextual reasoning and attack path analysis

Market Adoption

- Broad enterprise adoption of AI SOC platforms replacing legacy SOC workflows and fragmented security operations
- Rapid deployment of AI SOC-as-a-Service and autonomous Managed Detection and Response (MDR) offerings
- Accelerated growth across North America, Europe, and Asia Pacific driven by AI adoption, cloud transformation, and cybersecurity regulations
- Expansion of strategic ecosystems among cybersecurity vendors, hyperscale cloud providers, telecom operators, and enterprise software vendors

JULY 2026 © MarketsandMarkets™

6.2.3 LONG-TERM (2030–2035+) | AUTONOMOUS, PREDICTIVE & SELF-OPTIMIZING SECURITY OPERATIONS

Focus Areas:

Core Technology Development

- Emergence of fully autonomous AI SOC platforms capable of self-learning threat detection, autonomous reasoning, and adaptive response
- Integration of predictive cyber risk forecasting using foundation models, digital twins, and advanced behavioral analytics
- Development of self-optimizing security operations powered by collaborative multi-agent AI ecosystems
- Adoption of enterprise-wide AI governance frameworks integrating cybersecurity, compliance, privacy, and AI risk management

Product Innovations

- Launch of self-governing AI SOC platforms capable of orchestrating detection, investigation, containment, remediation, and post-incident learning with minimal analyst intervention
- Expansion of autonomous cyber defense platforms capable of continuously adapting security controls based on evolving attack patterns
- Development of intelligent cyber resilience platforms integrating business risk, identity security, cloud security, and enterprise exposure management
- Integration of quantum-resilient cryptography, confidential AI computing, and secure AI agent governance into next-generation SOC architectures

Market Adoption

- AI SOC platforms become foundational security infrastructure across digital enterprises, cloud-first organizations, and critical infrastructure operators.
- Widespread adoption of autonomous security operations supported by human-AI collaborative governance models
- Global standardization of AI security governance, agent security frameworks, and cross-industry threat intelligence collaboration
- AI SOC evolves into a strategic cyber resilience platform supporting predictive, adaptive, and continuously optimized enterprise security operations

JULY 2026 © MarketsandMarkets™

6.3 PATENT ANALYSIS

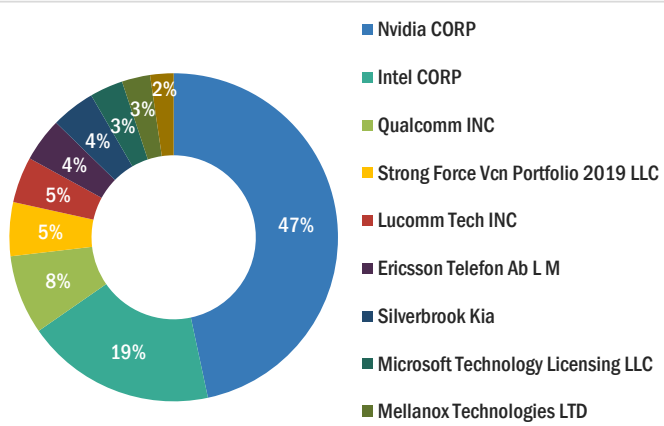
Patent analysis provides insights into innovation trends and technological advancements within the AI SOC market. This study examines patents related to AI-driven security operations, including generative AI and agentic AI for cybersecurity, machine learning-based threat detection, security information and event management (SIEM), endpoint detection and response (EDR), automated incident response, threat intelligence, behavioral analytics, and SOC automation. Patents were systematically categorized and evaluated based on their relevance to enhancing threat detection accuracy, alert prioritization, incident investigation, response automation, and overall SOC efficiency.

The analysis highlights global patenting trends, emerging AI cybersecurity innovations, and the evolution of intelligent security operations across enterprise, cloud, hybrid, and operational technology (OT) environments. Patent data were collected and assessed using patent intelligence platforms such as The Lens and WIPO. Over the past decade, the AI SOC market has witnessed growing patent activity, driven by increasing investments in generative AI, autonomous security agents, predictive threat analytics, and AI-powered security operations that enable faster, more proactive cyber defense.

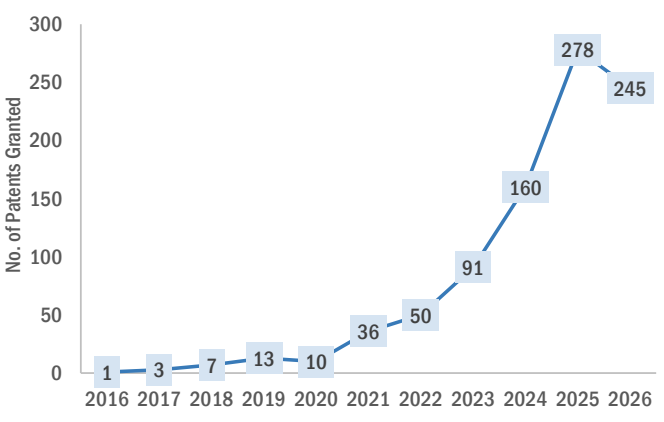
Some of the granted and applied patents are listed below:

FIGURE 24 PATENTS GRANTED IN AI SOC MARKET, 2016–2026

TOP 10 COMPANIES WITH HIGHEST NO. OF PATENT APPLICATIONS IN LAST 10 YEARS



NO. OF PATENTS GRANTED IN A YEAR OVER THE LAST 10 YEARS



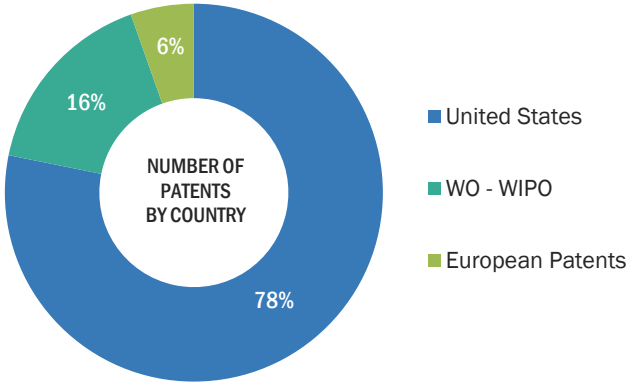
TOP 20 PATENT OWNERS IN THE LAST 10 YEARS	NO. OF PATENTS
Nvidia Corp	826
Intel Corp	367
Qualcomm Inc	134
Strong Force VCN Portfolio 2019 LLC	111
Lucomm Tech Inc	108
Ericsson Telefon Ab L M	76
Microsoft Technology Licensing LLC	65
Silverbrook Kia	60
McAfee LLC	48
Mellanox Technologies Ltd	47
Dell Products LP	41
AT&T LP	39
Samsung Electronics CO Ltd	35
Unifabrix Ltd	34
Huawei Tech Co Ltd	31
Quantum Digital Solutions CORP	26
Digital Global Systems Inc	25
Meta Platforms Inc	23
Guim Bernat Francesc	20
Kia Silverbrook	19

Note: The patent granted count is as of July 17, 2026.

Source: Lens.Org-Patent and Scholarly Search and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

FIGURE 25 REGIONAL ANALYSIS OF PATENTS GRANTED IN AI SOC MARKET



Note: Patents have been considered from January 2016 to July 2026

Source: Lens.org and MarketsandMarkets Analysis

TABLE 12 LIST OF TOP PATENTS IN AI SOC MARKET, 2024–2026

APPLICANT	PUBLICATION NUMBER	PUBLISHED YEAR	PATENT DESCRIPTION
Panik Button Holding BV	EP 4365742 B1	April 2026	This patent describes an automated cyber recovery system that securely validates backup data within a sandbox environment before restoring enterprise operations following a network failure or cyberattack. While primarily focused on cyber resilience and disaster recovery, it complements AI-driven security operations by enabling secure post-incident recovery and business continuity.
Orange	EP 3957045 B1	May 2025	This patent describes an AI-enabled alert processing framework that analyzes anomaly reports from network-connected devices and dynamically selects cyberattack detection algorithms based on device resource constraints. By optimizing threat analysis and automated response recommendations, it enhances AI-driven security operations, intelligent alert validation, and incident response across distributed network environments.
Musarubra Us LLC	US 12231443 B2	February 2025	This patent describes an AI-driven security operations approach that uses machine learning to analyze endpoint detection and response (EDR) metadata, establish behavioral baselines, and identify anomalous activities. By prioritizing uncommon endpoint events and reducing alert volume, it enables SOC analysts to focus on high-risk threats, improving detection accuracy and operational efficiency.

JULY 2026 © MarketsandMarkets™

Mccarson Brian	US 12088599 B1	September 2024	This patent introduces a Generative AI and Agentic AI framework that autonomously analyzes cybersecurity data, generates and validates predictive threat hypotheses, and recommends prevention, detection, mitigation, and remediation actions. By combining contextual intelligence with adaptive machine learning, it enables AI-driven SOC automation, threat hunting, incident response, and continuous cybersecurity decision support.

Note: The data given for 2024–2026 is dated as of July 17, 2026.

Source: Lens.Org-Patent and Scholarly Search and MarketsandMarkets Analysis

6.4 FUTURE APPLICATIONS

This comprehensive analysis examines five critical future applications through a standardized framework examining technical breakthroughs, implementation scalability, market impact, and commercial development.

FIGURE 26 FUTURE APPLICATIONS: AI SOC MARKET



Source: Secondary Research and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

6.4.1 PREDICTIVE CYBER DEFENSE AND CYBER RESILIENCE

Technical Breakthroughs	Advances in predictive AI, attack path analysis, behavioral analytics, digital twins, and threat intelligence fusion are enabling AI SOC platforms to forecast cyber risks and anticipate adversary movements before attacks occur.
Implementation Scalability	AI-powered predictive defense can be deployed across hybrid cloud, multi-cloud, on-premises, SaaS, endpoint, identity, and OT environments, enabling organizations to proactively manage enterprise-wide cyber risk from a centralized AI SOC.
Market Impact	Predictive cyber defense reduces incident frequency, minimizes business disruption, improves cyber resilience, and enables organizations to transition from reactive incident response to continuous risk anticipation and prevention.
Commercial Development	Vendors including Microsoft, Palo Alto Networks, Google Cloud, CrowdStrike, Cisco, and IBM are integrating predictive analytics, attack path modeling, exposure management, and AI-driven risk prioritization into next-generation AI SOC platforms.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

6.4.2 AI-NATIVE REGULATORY COMPLIANCE AND CONTINUOUS AUDIT OPERATIONS

Technical Breakthroughs	Generative AI, policy intelligence, automated evidence collection, and continuous control monitoring are transforming compliance management by mapping security events directly to regulatory frameworks and governance requirements.
Implementation Scalability	AI-native compliance engines continuously monitor cloud, endpoint, identity, SaaS, and network environments, enabling organizations to automate compliance across global regulations including NIS2, DORA, PCI DSS, HIPAA, ISO 27001, and GDPR.
Market Impact	Continuous compliance reduces audit preparation time, minimizes regulatory risks, improves governance maturity, and lowers operational costs through automated reporting, policy validation, and evidence generation.
Commercial Development	Microsoft, Google Cloud, IBM, Palo Alto Networks, Cisco, and ServiceNow are expanding AI-powered governance, compliance automation, policy management, and continuous audit capabilities across enterprise security platforms.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

6.4.3 CYBER FUSION CENTERS FOR ENTERPRISE RISK INTELLIGENCE

Technical Breakthroughs	AI-driven data correlation, knowledge graphs, contextual analytics, and multi-source intelligence fusion enable security operations to integrate cyber, operational, fraud, identity, cloud, and business risk information into unified decision-making platforms.
Implementation Scalability	AI-enabled Cyber Fusion Centers consolidate telemetry from SIEM, XDR, SOAR, cloud security, identity platforms, fraud detection systems, and IT operations, supporting enterprise-wide security operations across distributed environments.
Market Impact	Enterprise-wide risk visibility enables faster executive decision-making, better threat prioritization, stronger collaboration across security teams, and improved organizational resilience against increasingly complex cyber threats.
Commercial Development	Vendors such as Microsoft, Cisco (Splunk), IBM, Google Cloud, and Palo Alto Networks are expanding unified security operations platforms that combine AI-driven analytics with enterprise risk intelligence and operational visibility.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

6.4.4 AUTONOMOUS THIRD-PARTY AND SUPPLY CHAIN RISK MONITORING

Technical Breakthroughs	AI-powered external attack surface monitoring, software supply chain analytics, threat intelligence integration, and continuous vendor risk assessment enable AI SOCs to detect third-party cyber risks in real time.
Implementation Scalability	Autonomous monitoring platforms continuously assess suppliers, cloud services, SaaS applications, APIs, software dependencies, and external digital assets across complex global enterprise ecosystems.
Market Impact	Continuous supply chain monitoring strengthens cyber resilience, reduces third-party exposure, improves vendor risk management, and enables earlier detection of vulnerabilities before they affect enterprise operations.
Commercial Development	Companies including Microsoft, CrowdStrike, Palo Alto Networks, Rapid7, Google Cloud, and IBM are strengthening third-party risk intelligence, external attack surface management, and software supply chain security capabilities within AI SOC platforms.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

6.4.5 EXECUTIVE CYBER DECISION INTELLIGENCE AND BUSINESS RISK FORECASTING

Technical Breakthroughs	AI-powered business risk modeling, cyber exposure quantification, predictive analytics, and executive dashboards enable AI SOC platforms to translate technical security events into measurable business impact and strategic insights.
Implementation Scalability	Decision intelligence platforms aggregate cybersecurity, financial, operational, cloud, identity, and compliance data to provide real-time enterprise risk visibility for CISOs, executives, and board members.
Market Impact	AI-driven business risk forecasting improves cybersecurity investment decisions, enhances enterprise resilience, supports board-level governance, and enables proactive prioritization of cyber risks aligned with business objectives.
Commercial Development	Microsoft, IBM, Google Cloud, Cisco, Palo Alto Networks, and ServiceNow are integrating AI-driven cyber risk quantification, executive reporting, and business resilience capabilities into enterprise security operations platforms.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

6.5 IMPACT OF AI/GEN AI ON AI SOC MARKET

Artificial Intelligence (AI) and Generative AI (GenAI) are fundamentally transforming the AI SOC market by automating threat detection, accelerating incident investigation, and enabling intelligent security decision-making across increasingly complex enterprise environments. Modern organizations generate vast amounts of telemetry from endpoints, cloud workloads, identities, applications, networks, and SaaS platforms, making traditional manual SOC operations insufficient. AI-powered SOC platforms leverage machine learning, behavioral analytics, and threat intelligence to correlate security events, prioritize high-risk incidents, detect sophisticated attack patterns, and significantly reduce alert fatigue. Generative AI further enhances analyst productivity by automatically summarizing incidents, generating investigation timelines, recommending remediation actions, translating natural language queries into security workflows, and assisting security teams with contextual threat analysis. These capabilities are enabling organizations to improve detection accuracy, reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), and operate more efficient, scalable security operations.

JULY 2026 © MarketsandMarkets™

AI and GenAI are also driving the evolution of security operations from analyst-assisted automation toward autonomous and agentic SOCs capable of independently performing investigation, triage, threat hunting, containment, and response while maintaining human oversight for critical decisions. AI agents are increasingly collaborating across multiple security functions to orchestrate end-to-end workflows, allowing SOC analysts to focus on strategic investigations and proactive cyber resilience. However, the growing adoption of AI also introduces new security challenges, including prompt injection attacks, AI model manipulation, AI agent abuse, hallucinations, and governance risks. As a result, organizations are investing in responsible AI frameworks, model validation, identity-centric controls, explainable AI, and robust governance mechanisms to ensure secure, transparent, and trustworthy AI-driven security operations.

TABLE 13 TOP USE CASES AND MARKET POTENTIAL

TOP USE CASES	MARKET POTENTIAL
AI-Powered Threat Detection & Intelligent Alert Prioritization	Strong growth driven by increasing cyberattack volume and alert overload—AI enables real-time anomaly detection, contextual risk scoring, and intelligent prioritization of high-risk incidents across hybrid enterprise environments.
GenAI-Assisted Security Investigation & Incident Response	High adoption potential as organizations automate alert correlation, incident summarization, threat investigation, and remediation recommendations, significantly improving SOC analyst productivity and reducing response times
Autonomous SOC Operations & Agentic Security Workflows	Rapidly emerging opportunity driven by cybersecurity workforce shortages—AI agents autonomously perform investigation, threat hunting, containment, remediation, and workflow orchestration with human oversight for complex decisions.
AI-Driven Threat Hunting & Predictive Risk Analytics	Growing demand for proactive security operations—AI continuously analyzes attacker behavior, threat intelligence, and exposure data to identify hidden threats, predict attack paths, and strengthen cyber resilience before compromise occurs.
Security Copilots & Natural Language SOC Operations	Expanding enterprise adoption as GenAI enables analysts to interact with security platforms using natural language, automate playbook creation, generate executive reports, and simplify complex investigations without requiring advanced scripting expertise

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

6.5.1 BEST PRACTICES IN AI SOC MARKET

TABLE 14 BEST PRACTICES: COMPANIES IMPLEMENTING USE CASES

OEM	USE CASE	VALUE CHAIN
Palo Alto Networks	Cortex XSIAM and Cortex AgentiX deliver an AI-driven SOC platform that autonomously performs alert triage, investigation, threat hunting, and response using agentic AI, helping enterprises reduce analyst workload and accelerate security operations.	Autonomous SOC, AI Investigation, XSIAM, Threat Detection, SOAR, Incident Response
CrowdStrike	Falcon Next-Gen SIEM, Charlotte AI, and Agentic SOAR provide AI-powered detection, investigation, threat hunting, and automated response while securing enterprise, cloud, identity, and AI environments through an AI-native SOC platform.	Next-Gen SIEM, AI Investigation, Threat Hunting, Agentic SOAR, Incident Response, AI Security

JULY 2026 © MarketsandMarkets™

SentinelOne	SentinelOne Singularity Platform with Purple AI delivers autonomous threat hunting, AI-assisted investigations, XDR, and security automation, enabling analysts to rapidly identify, investigate, and remediate advanced cyber threats across enterprise environments.	Autonomous Threat Hunting, XDR, AI Investigation, Security Automation, Incident Response, Threat Intelligence
Cisco Splunk	Cisco Splunk Enterprise Security integrates AI-assisted investigations, SIEM analytics, SOAR automation, and threat intelligence to provide centralized visibility, rapid incident response, and operational efficiency across modern enterprise SOCs.	AI SIEM, Security Analytics, SOAR, Threat Intelligence, Incident Investigation, Security Operations
Stellar Cyber	Stellar Cyber's AI-native Open XDR platform provides autonomous SOC capabilities through multi-layer AI, agentic auto-triage, AI-powered investigations, continuous threat hunting, and automated incident response across hybrid enterprise environments.	Open XDR, AI Auto-Triage, Threat Hunting, AI Investigation, Incident Response, Autonomous SOC

Source: Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

6.5.2 CASE STUDIES OF AI IMPLEMENTATION IN AI SOC MARKET

TABLE 15 AI SOC MARKET: CASE STUDIES RELATED TO GEN AI IMPLEMENTATION

CASE STUDY	DETAILS
Microsoft Advances AI-Powered Security Operations with Security Copilot	Microsoft integrates Generative AI through Security Copilot with Microsoft Sentinel and Defender XDR to enhance SOCs. The platform automates alert triage, incident investigation, threat hunting, and remediation recommendations using natural language interactions. AI-assisted workflows help analysts reduce investigation time, improve detection accuracy, and strengthen cyber resilience across hybrid, multi-cloud, identity, endpoint, and SaaS environments while maintaining human oversight for critical security decisions.
Google Cloud Enables AI-Native Security Operations with Gemini	Google Security Operations integrates Gemini AI to automate threat detection, investigation, malware analysis, threat hunting, and case management across enterprise environments. By combining AI reasoning with Google's threat intelligence and cloud-scale analytics, the platform accelerates incident response, reduces analyst workload, and enables unified security operations across cloud, network, endpoint, and identity infrastructures.
CrowdStrike Delivers Agentic AI for Autonomous SOC Operations	CrowdStrike's Charlotte AI transforms modern SOCs by autonomously triaging alerts, conducting investigations, generating threat-hunting queries, and recommending response actions. Embedded within the Falcon platform, Charlotte AI enables organizations to reduce manual investigations, improve analyst productivity, accelerate incident response, and operate AI-native, agentic SOCs capable of responding to evolving cyber threats at machine speed.
Palo Alto Networks Accelerates AI-Driven Security Operations with Cortex XSIAM	Palo Alto Networks integrates AI, machine learning, and automation within Cortex XSIAM to transform enterprise security operations. The platform correlates telemetry across security tools, automates alert triage, orchestrates investigations, and enables autonomous threat detection and response. Organizations benefit from reduced false positives, faster incident resolution, and highly efficient AI-driven SOC operations across hybrid enterprise environments.

JULY 2026 © MarketsandMarkets™

Stellar Cyber Delivers Autonomous AI SOC through Open XDR	Stellar Cyber combines Open XDR, autonomous AI, and intelligent automation to streamline security operations. The platform automatically correlates alerts, prioritizes threats, performs AI-assisted investigations, and orchestrates response workflows across cloud, network, endpoint, and identity environments. This enables security teams to improve SOC efficiency, reduce alert fatigue, and strengthen enterprise cyber resilience through unified AI-native security operations.

Source: Press Releases, Company Websites, and MarketsandMarkets Analysis

6.5.3 INTERCONNECTED ADJACENT ECOSYSTEM AND IMPACT ON MARKET PLAYERS

TABLE 16 INTERCONNECTED ADJACENT ECOSYSTEM AND IMPACT ON MARKET PLAYERS

ECOSYSTEM	INTEGRATION	IMPACT
Cloud Computing & Hyperscaler Ecosystems	AI SOC platforms integrate with public, private, and hybrid cloud environments through hyperscalers such as Microsoft Azure, AWS, and Google Cloud to collect telemetry, perform AI-driven analytics, and secure multi-cloud workloads, identities, applications, and cloud infrastructure from a unified security operations platform.	Enables centralized security operations, improves scalability across distributed cloud environments, and accelerates adoption of cloud-native AI SOC platforms with unified visibility and automated threat response
XDR, SIEM & SOAR Security Platforms	AI SOC solutions integrate with Extended Detection and Response (XDR), SIEM, SOAR, endpoint security, email security, network security, and threat intelligence platforms to correlate multi-domain telemetry, automate investigations, orchestrate response workflows, and enable autonomous security operations.	Strengthens cross-domain threat detection, reduces alert fatigue, improves incident response speed, and enables AI-native SOCs capable of autonomous investigation and remediation
Identity Security & Zero Trust Ecosystem	Integration with Identity and Access Management (IAM), Identity Threat Detection and Response (ITDR), Privileged Access Management (PAM), and Zero Trust architectures enables AI SOCs to continuously analyze user behavior, detect identity-based attacks, and enforce adaptive access controls across enterprise environments.	Enhances identity-centric threat detection, limits lateral movement, strengthens Zero Trust implementation, and improves enterprise cyber resilience against credential-based attacks
Cloud-Native Application Protection (CNAPP) & Application Security	AI SOC platforms integrate with CNAPP, CSPM, CWPP, CIEM, Kubernetes security, DevSecOps, and application security solutions to correlate cloud posture, runtime activity, vulnerabilities, and attack paths within unified security operations workflows.	Provides end-to-end code-to-cloud visibility, improves cloud risk prioritization, accelerates cloud incident investigations, and enables unified protection across modern application environments
Generative AI, Threat Intelligence & AI Security Ecosystem	AI SOC platforms combine Generative AI, large language models (LLMs), AI agents, threat intelligence feeds, malware intelligence, and security knowledge graphs to automate investigations, perform contextual reasoning, generate incident summaries, and support autonomous SOC workflows.	Improves analyst productivity, accelerates threat hunting and incident response, reduces manual investigation effort, and drives the evolution toward fully autonomous and agentic AI SOC operations.

Source: Press Releases, Investor Presentations, Journals, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

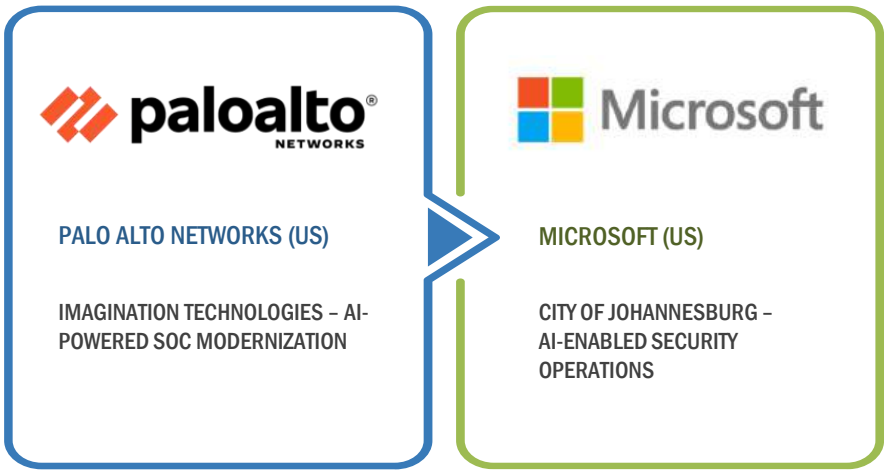
6.5.4 CLIENTS' READINESS TO ADOPT GENERATIVE AI IN AI SOC MARKET

Organizations are demonstrating high readiness to adopt Generative AI within SOCs as cybersecurity operations become increasingly data-intensive and difficult to manage through conventional workflows. Rather than viewing GenAI as a standalone productivity tool, enterprises are integrating it into broader cyber resilience, governance, and security transformation initiatives. Buyers are prioritizing AI SOC platforms capable of interpreting complex security telemetry, generating contextual recommendations, supporting policy validation, and simplifying interactions with security systems through natural language. The growing maturity of enterprise AI platforms from Microsoft, Google Cloud, IBM, CrowdStrike, and Palo Alto Networks has further increased buyer confidence in deploying AI across mission-critical security operations.

Enterprise adoption is also being driven by the need to standardize security operations across geographically distributed environments, support multi-cloud infrastructures, and strengthen governance over expanding AI usage within organizations. Buyers increasingly evaluate AI SOC solutions based on explainability, model transparency, regulatory compliance, data privacy controls, and seamless interoperability with existing security ecosystems instead of automation capabilities alone. At the same time, organizations are establishing AI governance frameworks, security validation processes, and human oversight mechanisms to ensure responsible AI deployment while addressing emerging risks such as prompt injection, model misuse, and shadow AI. As governance maturity improves and enterprise AI strategies evolve, Generative AI is becoming a foundational capability for next-generation AI-native SOCs rather than an experimental technology.

6.6 SUCCESS STORIES AND REAL-WORLD APPLICATIONS

FIGURE 27 SUCCESS STORIES AND REAL-WORLD APPLICATIONS



Source: Press Releases and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

6.6.1 PALO ALTO NETWORKS: IMAGINATION TECHNOLOGIES – AI-POWERED SOC MODERNIZATION

Imagination Technologies modernized its security operations center (SOC) using Palo Alto Networks' Cortex XSIAM, replacing manual, fragmented security operations with an AI-driven, automation-first platform. By consolidating endpoint, network, cloud, and identity telemetry into a unified security data layer, the organization significantly improved visibility, accelerated threat investigations, and strengthened its overall cybersecurity posture across a rapidly expanding enterprise environment.

The deployment enabled a 10× improvement in incident closure rates, increasing from below 10% to 100%, while reducing median investigation time from months to approximately five hours. AI-powered analytics, automated incident correlation, and intelligent prioritization allowed the lean SOC team to respond proactively, improve operational efficiency, and focus on high-risk threats instead of repetitive manual investigations.

6.6.2 MICROSOFT: CITY OF JOHANNESBURG – AI-ENABLED SECURITY OPERATIONS

The City of Johannesburg strengthened its cyber defense capabilities by deploying Microsoft Security Copilot across its security operations center. Integrated with Microsoft Defender and the broader Microsoft Security platform, AI agents automate alert triage, threat correlation, investigation, reporting, and incident response, helping security analysts protect a complex hybrid IT and operational technology environment supporting critical public services.

Within months of deployment, the city reduced false positives by up to 95%, achieved productivity improvements of 23–46.7%, and accelerated analyst task completion by 26%. The AI-enabled SOC also enhanced executive visibility, reduced operational costs, and improved protection for critical infrastructure and sensitive citizen data while enabling secure digital services for millions of residents.

JULY 2026 © MarketsandMarkets™

7 REGULATORY LANDSCAPE

7.1 REGIONAL REGULATIONS AND COMPLIANCE

The AI SOC market operates within an increasingly stringent global regulatory environment shaped by cybersecurity, artificial intelligence governance, data privacy, and operational resilience requirements. Unlike traditional SOC platforms, AI SOC solutions leverage generative AI, large language models (LLMs), autonomous agents, and machine learning for threat detection, investigation, and response, making compliance with both cybersecurity and AI-specific regulations increasingly important. Frameworks such as the EU AI Act, NIS2 Directive, Digital Operational Resilience Act (DORA), GDPR, and the NIST AI Risk Management Framework (AI RMF) are establishing requirements for trustworthy AI, risk management, transparency, human oversight, and secure AI deployment. These regulations are driving AI SOC vendors to incorporate explainable AI, governance controls, audit logging, model validation, and continuous monitoring into their platforms.

Across North America, organizations increasingly align AI SOC deployments with the NIST Cybersecurity Framework (CSF), NIST AI RMF, and guidance from CISA, while highly regulated industries such as financial services and healthcare must also comply with sector-specific requirements. In Europe, the AI Act, NIS2, DORA, GDPR, and the Cyber Resilience Act collectively establish one of the world's most comprehensive governance environments for AI-enabled cybersecurity platforms. Meanwhile, Asia Pacific countries including Singapore, Japan, Australia, India, and South Korea are strengthening AI governance frameworks, cybersecurity legislation, national CERT capabilities, and digital trust initiatives to support secure enterprise AI adoption while encouraging innovation. Middle East governments such as the UAE and Saudi Arabia are embedding AI governance into national digital transformation programs, whereas Latin American countries continue strengthening cybersecurity maturity through national cyber strategies, privacy regulations, and regional collaboration initiatives.

Regulatory compliance has become a strategic differentiator within the AI SOC market, influencing platform architecture, AI model governance, data handling, incident response workflows, and third-party risk management. Enterprises increasingly expect AI SOC platforms to provide explainable decision-making, secure model lifecycle management, audit-ready evidence, continuous compliance monitoring, and integration with governance, risk, and compliance (GRC) frameworks. As regulations governing AI continue to mature across jurisdictions, vendors are embedding policy enforcement, AI risk assessment, model monitoring, human-in-the-loop controls, and automated compliance reporting into AI SOC platforms. Although regulatory fragmentation remains a challenge for multinational deployments, increasing convergence around risk-based AI governance and cybersecurity best practices is expected to accelerate enterprise adoption of trusted, compliant, and resilient AI-native security operations platforms.

JULY 2026 © MarketsandMarkets™

7.1.1 REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

This section includes a region-wise list of key regulatory bodies, government agencies, industry associations, and non-profit organizations relevant to the market.

TABLE 17 NORTH AMERICA: REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	SHORT DESCRIPTION
United States	National Institute of Standards and Technology (NIST)	Government Agency	Develops globally recognized cybersecurity and AI frameworks, including the Cybersecurity Framework (CSF) and AI Risk Management Framework (AI RMF), widely adopted for AI-enabled SOC governance and cyber resilience
United States	Cybersecurity and Infrastructure Security Agency (CISA)	Government Agency	Leads national cybersecurity and critical infrastructure protection through threat advisories, incident response, vulnerability management, and secure AI guidance supporting enterprise SOC modernization
United States	Center for AI Standards and Innovation (CAISI), NIST	Government Agency	Develops voluntary standards, evaluation methodologies, and best practices for secure, trustworthy, and interoperable AI systems, supporting safe deployment of AI technologies within enterprise security operations
United States	Cloud Security Alliance (CSA)	Non-profit Organization	Global nonprofit developing cloud security best practices, Zero Trust guidance, AI security research, and certification programs that help organizations securely deploy AI-native SOC and cloud security platforms
United States	ISACA	Professional Association / Non-profit	Develops governance, audit, cybersecurity, AI risk management, and digital trust frameworks while providing globally recognized certifications supporting AI-enabled security operations and cyber governance
United States	Information Systems Security Association (ISSA)	Industry Association	Professional cybersecurity association promoting security education, knowledge sharing, SOC best practices, workforce development, and collaboration among cybersecurity practitioners and technology leaders
United States	Center for Internet Security (CIS)	Non-profit Organization	Develops CIS Controls, secure configuration benchmarks, and cyber defense best practices widely adopted by SOC teams for vulnerability management, detection engineering, and security operations
United States	SANS Institute	Non-profit Research & Training Organization	Global cybersecurity research and training organization providing SOC methodologies, threat hunting techniques, incident response education, AI security research, and widely adopted GIAC certifications

JULY 2026 © MarketsandMarkets™

Canada	Canadian Centre for Cyber Security	Government Agency	Canada's national technical authority for cybersecurity, providing threat intelligence, incident response guidance, AI security recommendations, and cyber resilience support for government and private organizations
Canada	Public Safety Canada	Government Agency	Leads national cybersecurity policy, critical infrastructure resilience, emergency preparedness, and public-private collaboration to strengthen Canada's cyber defense and digital security ecosystem
Canada	Information and Communications Technology Council (ICTC)	Non-profit Organization	Supports Canada's digital economy through cybersecurity workforce development, AI skills initiatives, industry research, and programs addressing talent shortages affecting modern Security Operations Centers

Source: Secondary Literature and MarketsandMarkets Analysis

TABLE 18 EUROPE: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	DESCRIPTION
Europe (EU)	European Commission (Directorate-General for Communications Networks, Content and Technology – DG CONNECT)	Government Body	Leads the EU's digital strategy, cybersecurity legislation, AI policy, and implementation of the AI Act, supporting secure adoption of AI-powered cybersecurity and enterprise security operations
Europe (EU)	European Union Agency for Cybersecurity (ENISA)	EU Agency	The EU's cybersecurity agency responsible for cyber resilience, certification frameworks, incident preparedness, threat intelligence cooperation, and guidance supporting AI-enabled SOC operations across Member States
Europe (EU)	European Artificial Intelligence Office (AI Office)	EU Government Body	Oversees implementation and enforcement of the EU AI Act, coordinates AI governance, supervises general-purpose AI models, and promotes trustworthy AI deployment across European industries
Europe (EU)	European Cyber Security Organization (ECSO)	Industry Association	Public-private partnership bringing together cybersecurity vendors, research institutions, governments, and end users to accelerate innovation, investment, policy development, and cybersecurity adoption across Europe
Europe (EU)	European Data Protection Board (EDPB)	Regulatory Body	Ensures consistent application of GDPR across the EU, guiding privacy, AI governance, cross-border data protection, and secure processing of personal information within AI-driven security platforms

JULY 2026 © MarketsandMarkets™

France	National Cybersecurity Agency of France (ANSSI)	Government Agency	France's national cybersecurity authority responsible for protecting government systems, critical infrastructure, cyber incident response, cybersecurity policy, and operational guidance for public and private organizations
UK	National Cyber Security Centre (NCSC)	Government Agency	The UK's national technical authority for cybersecurity, providing threat intelligence, incident response guidance, AI security recommendations, and cyber resilience support for government and enterprise organizations
UK	Department for Science, Innovation and Technology (DSIT)	Government Department	Leads the UK's AI, digital technology, and cybersecurity strategy, supporting secure AI innovation, cyber resilience, digital regulation, and responsible deployment of AI across public and private sectors
UK	Chartered Institute of Information Security (CIISec)	Professional Membership Organization	Professional body promoting cybersecurity excellence through certifications, workforce development, professional standards, and knowledge sharing for security practitioners, SOC analysts, and cyber leaders
Europe	ISACA Europe	Professional Association	Supports cybersecurity governance, AI risk management, digital trust, auditing, and enterprise security through globally recognized certifications, research, and professional education across European markets

Source: Secondary Literature and MarketsandMarkets Analysis

TABLE 19 ASIA PACIFIC: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	DESCRIPTION
Asia Pacific	Asia Pacific Computer Emergency Response Team (APCERT)	Regional Cybersecurity Organization	APCERT strengthens cybersecurity cooperation among national CERTs across Asia Pacific by promoting cyber threat intelligence sharing, incident response coordination, capacity building, and regional cyber resilience initiatives
China	Cyberspace Administration of China (CAC)	Government Agency	China's primary cybersecurity and internet regulator overseeing cybersecurity governance, AI regulations, data security, generative AI compliance, critical infrastructure protection, and enterprise security requirements
China	China Academy of Information and Communications Technology (CAICT)	Government Research Institute	Government-affiliated research institute supporting AI standards, cybersecurity research, digital infrastructure development, AI governance, and technology evaluation for China's digital economy and enterprise innovation

JULY 2026 © MarketsandMarkets™

Japan	National Center of Incident Readiness and Strategy for Cybersecurity (NISC)	Government Agency	Japan's central cybersecurity authority responsible for national cyber policy, incident readiness, critical infrastructure protection, and international collaboration on cybersecurity frameworks including SIEM and SOAR guidance
Japan	Information-technology Promotion Agency (IPA)	Government Agency	Promotes cybersecurity awareness, digital transformation, workforce development, vulnerability management, AI security research, and secure software development across Japan's public and private sectors
Japan	Japan Network Security Association (JNSA)	Industry Association	Industry association promoting cybersecurity standards, information sharing, workforce development, security awareness, and collaboration among technology vendors, enterprises, researchers, and government agencies
India	Indian Computer Emergency Response Team (CERT-In)	Government Agency	India's national incident response organization responsible for cyber incident management, threat advisories, cybersecurity coordination, vulnerability disclosures, and protection of national digital infrastructure
India	Ministry of Electronics and Information Technology (MeitY)	Government Ministry	Leads India's digital governance, AI strategy, cybersecurity policy, trusted AI initiatives, and implementation of frameworks supporting responsible AI adoption and cyber resilience
India	Data Security Council of India (DSCI)	Industry Association / Non-profit	Industry body under NASSCOM promoting cybersecurity best practices, AI governance, privacy, workforce development, cyber resilience, and collaboration between government and industry
Singapore	Cyber Security Agency of Singapore (CSA)	Government Agency	Singapore's national cybersecurity agency responsible for protecting critical information infrastructure, cyber resilience, national cyber defense, AI security guidance, and enterprise cybersecurity capability development
Singapore	Infocomm Media Development Authority (IMDA)	Government Agency	Develops Singapore's AI governance frameworks, including AI Verify and the Model AI Governance Framework for Agentic AI, supporting trustworthy enterprise AI deployment and secure digital innovation
Singapore	AI Verify Foundation	Non-profit Organization	Global open-source initiative supporting AI testing, governance, transparency, and interoperability through technical assurance tools that help organizations deploy trustworthy and secure AI systems
Australia	Australian Cyber Security Centre (ACSC)	Government Agency	Australia's national cybersecurity authority providing threat intelligence, incident response guidance, cyber resilience strategies, essential security controls, and best practices for enterprise security operations

JULY 2026 © MarketsandMarkets™

South Korea	Korea Internet & Security Agency (KISA)	Government Agency	National cybersecurity agency responsible for cyber incident response, information security standards, AI security research, privacy protection, and strengthening cybersecurity across public and private sectors

Source: Secondary Literature and MarketsandMarkets Analysis

TABLE 20 MIDDLE EAST & AFRICA: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	DESCRIPTION
Saudi Arabia	National Cybersecurity Authority (NCA)	Government Agency	Saudi Arabia's national cybersecurity regulator responsible for cybersecurity governance, national frameworks, AI cybersecurity guidelines, SOC licensing, critical infrastructure protection, and cybersecurity policy implementation
Saudi Arabia	Saudi Data & Artificial Intelligence Authority (SDAIA)	Government Agency	Leads Saudi Arabia's national AI strategy, responsible AI adoption, data governance, AI innovation, and regulatory initiatives supporting secure enterprise AI deployment and digital transformation
Saudi Arabia	Saudi CERT	Government Agency	National Computer Emergency Response Team providing cyber incident response, vulnerability coordination, threat intelligence sharing, and operational cybersecurity support for government and critical infrastructure sectors
United Arab Emirates	UAE Cyber Security Council	Government Agency	Leads national cybersecurity strategy, cyber resilience initiatives, AI security policies, and public-private collaboration to strengthen digital infrastructure and enterprise cyber defense across the UAE
United Arab Emirates	Dubai Electronic Security Center (DESC)	Government Agency	Develops cybersecurity policies, governance frameworks, and security standards for Dubai government entities while promoting secure digital transformation and resilient Security Operations Centers
Qatar	National Cyber Security Agency (NCSA)	Government Agency	Leads Qatar's national cybersecurity strategy, cyber resilience, incident response coordination, and protection of government systems and critical national infrastructure against evolving cyber threats
Qatar	Ministry of Communications and Information Technology (MCIT)	Government Ministry	Develops Qatar's digital transformation, AI adoption, cybersecurity strategy, cloud policy, and regulatory initiatives supporting secure digital services and enterprise cyber resilience

JULY 2026 © MarketsandMarkets™

Israel	Israel National Cyber Directorate (INCD)	Government Agency	National authority responsible for cyber defense, critical infrastructure protection, incident response coordination, cyber innovation, and strengthening Israel's national cybersecurity ecosystem
South Africa	Department of Communications and Digital Technologies (DCDT)	Government Department	Leads South Africa's national digital transformation, cybersecurity policy, AI development initiatives, and ICT governance supporting secure adoption of emerging digital technologies
South Africa	Cyber Security Hub	Government Initiative	National cybersecurity collaboration platform facilitating cyber awareness, threat information sharing, incident reporting, and cybersecurity guidance for businesses and public sector organizations
South Africa	Information Regulator	Independent Regulatory Authority	Oversees implementation of the Protection of Personal Information Act (POPIA), ensuring data privacy, information governance, and regulatory compliance for AI-enabled security platforms
Africa (Regional)	Smart Africa Alliance	Intergovernmental Organization	Pan-African alliance promoting digital transformation, cybersecurity cooperation, AI adoption, secure digital infrastructure, and cross-border collaboration among African member states

TABLE 21 LATIN AMERICA: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	DESCRIPTION
Latin America	CiberLAC	Regional Cybersecurity Initiative	Regional cybersecurity collaboration platform supported by the Inter-American Development Bank (IDB) and OAS that strengthens cyber resilience, capacity building, incident response, and policy coordination across Latin America
Latin America	Organization of American States (OAS) – Cybersecurity Program	Intergovernmental Organization	Supports member states through cybersecurity policy development, CSIRT maturity, cyber resilience programs, critical infrastructure protection, and regional cooperation against evolving cyber threats
Brazil	Brazilian Internet Steering Committee (CGI.br)	Multi-stakeholder Organization	Coordinates internet governance, cybersecurity best practices, digital trust initiatives, and policy recommendations supporting secure AI adoption and enterprise cybersecurity across Brazil
Brazil	CERT.br (Brazilian National CSIRT)	Government-supported Incident Response Organization	Brazil's national Computer Security Incident Response Team responsible for cyber incident coordination, vulnerability response, threat intelligence dissemination, and cybersecurity awareness

JULY 2026 © MarketsandMarkets™

Mexico	CERT-MX	Government Incident Response Team	Mexico's national Computer Emergency Response Team coordinates cyber incident handling, vulnerability reporting, threat intelligence sharing, and protection of national digital infrastructure
Argentina	CERT.ar	Government Agency	Argentina's national Computer Emergency Response Team provides incident response, cyber threat monitoring, vulnerability management, and cybersecurity guidance for government and enterprise organizations
Argentina	Agency for Access to Public Information (AAIP)	Government Regulatory Authority	Enforces Argentina's personal data protection framework, promotes privacy governance, and supports responsible handling of digital information in AI-enabled environments
Chile	National Cybersecurity Agency (ANCI)	Government Agency	Chile's national cybersecurity authority responsible for cyber resilience, national cyber strategy implementation, incident coordination, and protection of critical infrastructure and public services
Chile	CSIRT Government of Chile	Government Agency	Coordinates cyber incident response, threat intelligence sharing, vulnerability notifications, and cybersecurity support for public institutions and critical national infrastructure

Source: Secondary Literature and MarketsandMarkets Analysis

7.1.2 INDUSTRY STANDARDS

The AI SOC market is increasingly being shaped by globally recognized technical standards and operational frameworks that promote consistency, interoperability, and trusted AI-driven security operations across enterprise environments. Unlike regulatory frameworks, which establish mandatory legal obligations, industry standards provide common engineering practices for designing, deploying, and operating AI-enabled SOC platforms. These standards help vendors normalize security telemetry, improve interoperability between SIEM, XDR, EDR, cloud security, identity platforms, and threat intelligence systems, while ensuring AI models are transparent, explainable, auditable, and operationally reliable. As organizations transition toward AI-native and agentic SOC architectures, standardized operational practices are becoming essential for maintaining detection quality, reducing integration complexity, and supporting multi-vendor security ecosystems.

Industry adoption is increasingly centered around frameworks such as MITRE ATT&CK and MITRE D3FEND for detection engineering and defensive strategy mapping, MITRE ATLAS for securing AI and machine learning systems, Open Cybersecurity Schema Framework (OCSF) for standardized security data models, and STIX/TAXII for automated cyber threat intelligence exchange. At the AI governance layer, organizations are implementing ISO/IEC 42001 and the NIST AI Risk Management Framework (AI RMF) to establish consistent AI lifecycle management, model governance, and operational assurance, while ISO/IEC 27001 continues to underpin enterprise information security management. Together, these standards provide a common technical foundation that enables AI SOC platforms to deliver interoperable analytics, reliable automation, high-quality threat intelligence, and scalable autonomous security operations across increasingly complex hybrid and multi-cloud environments.

TABLE 22 GLOBAL INDUSTRY STANDARDS IN AI SOC MARKET

STANDARD/GUIDELINE	ISSUING BODY	DESCRIPTION
NIST AI Risk Management Framework (AI RMF)	National Institute of Standards and Technology (NIST), USA	The NIST AI Risk Management Framework (AI RMF) provides the world's leading framework for trustworthy AI governance, risk management, model lifecycle management, explainability, human oversight, and continuous monitoring. It is increasingly adopted by AI SOC vendors to manage risks associated with AI-driven threat detection and autonomous security operations.
NIST Cybersecurity Framework (CSF) 2.0	National Institute of Standards and Technology (NIST), USA	The NIST Cybersecurity Framework (CSF) 2.0 is a risk-based cybersecurity framework covering Govern, Identify, Protect, Detect, Respond, and Recover functions. It forms the foundational cybersecurity framework for modern Security Operations Centers (SOCs), AI SOC platforms, and enterprise cyber resilience programs.
MITRE ATT&CK Framework	MITRE Corporation	The MITRE ATT&CK Framework is a globally recognized knowledge base of adversary tactics, techniques, and procedures (TTPs). It is widely used by AI SOC platforms for threat detection, attack mapping, automated investigations, threat hunting, and detection engineering.
MITRE D3FEND	MITRE Corporation	MITRE D3FEND is a defensive cybersecurity knowledge graph that maps security countermeasures to attacker behaviors. It supports AI-assisted security operations, automated response orchestration, defensive playbooks, and SOC detection engineering.
MITRE ATLAS (Adversarial Threat Landscape for Artificial Intelligence Systems)	MITRE Corporation	MITRE ATLAS is a framework focused on AI-specific attack techniques targeting machine learning and generative AI systems. It helps AI SOC teams detect, assess, and defend against model poisoning, prompt injection, adversarial ML attacks, and AI supply-chain threats.
Open Cybersecurity Schema Framework (OCSF)	Linux Foundation (OpenSSF contributors including AWS, IBM, Microsoft, Palo Alto Networks, CrowdStrike and others)	The Open Cybersecurity Schema Framework (OCSF) is an open standard that normalizes cybersecurity telemetry across security products. It enables AI SOC platforms to correlate events consistently across SIEM, XDR, EDR, cloud security, and identity security solutions.
ISO/IEC 27001 Information Security Management Systems (ISMS)	ISO / IEC	ISO/IEC 27001 is the international standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It provides governance, risk management, and security controls widely adopted across AI SOC deployments.
ISO/IEC 42001 Artificial Intelligence Management System (AIMS)	ISO / IEC	ISO/IEC 42001 is the first international management system standard specifically for AI. It defines governance, risk management, lifecycle controls, accountability, and responsible AI practices for organizations developing or deploying AI-enabled security platforms.
STIX 2.x & TAXII 2.x	OASIS Open	STIX 2.x and TAXII 2.x are global standards for structured cyber threat intelligence representation and automated threat intelligence sharing, and are extensively used by AI SOC platforms for integrating external intelligence feeds, threat correlation, and automated investigations.

JULY 2026 © MarketsandMarkets™

OWASP Top 10 for Large Language Model (LLM) Applications/GenAI Security Guidance	Open Worldwide Application Security Project (OWASP)	The OWASP Top 10 for LLM Applications provides best practices for securing LLM-based and generative AI applications against prompt injection, model manipulation, sensitive data exposure, insecure plugins, and AI supply-chain vulnerabilities. It is increasingly incorporated into AI SOC governance and secure AI operations.

Source: Secondary Research, Company Websites, Regional Government Bodies, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

8 CONSUMER LANDSCAPE & BUYER BEHAVIOR

8.1 DECISION-MAKING PROCESS

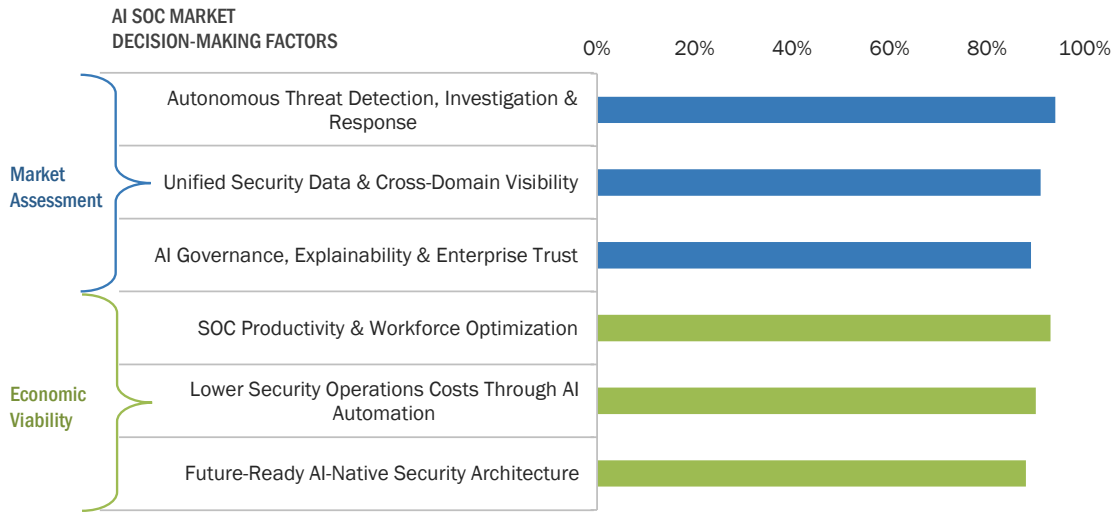
The decision-making process for investing in artificial intelligence security operations center (AI SOC) solutions begins with assessing an organization's ability to modernize security operations against increasingly sophisticated cyber threats, expanding attack surfaces, and persistent shortages of skilled cybersecurity professionals. Enterprises across BFSI, healthcare, manufacturing, government, technology, and critical infrastructure sectors prioritize AI SOC platforms that deliver autonomous threat detection, intelligent alert prioritization, AI-assisted investigations, automated response orchestration, and continuous monitoring across hybrid, multi-cloud, SaaS, endpoint, identity, and network environments. Market assessment typically involves evaluating AI-native SOC vendors, SIEM and XDR providers, managed detection and response (MDR) providers, and AI security platform vendors offering capabilities such as agentic AI, security copilots, behavioral analytics, threat intelligence integration, and security workflow automation. Customer readiness depends on the maturity of existing security operations, telemetry quality, cloud adoption, integration with identity, endpoint, network, and cloud security tools, as well as organizational preparedness to operationalize trustworthy AI within security workflows.

Organizations benchmark AI SOC platforms based on autonomous investigation capabilities, detection accuracy, cross-domain visibility, scalability, explainability of AI decisions, interoperability with existing security ecosystems, and support for human-in-the-loop operations. Key decision-making factors include seamless integration with SIEM, XDR, EDR, CNAPP, identity security, threat intelligence platforms, and SOAR, together with support for generative AI assistants, autonomous security agents, AI governance, model transparency, and compliance with emerging cybersecurity and AI governance frameworks. Strategic alignment increasingly focuses on how AI SOC solutions improve analyst productivity, accelerate incident investigation, strengthen cyber resilience, reduce alert fatigue, and enable proactive risk management while supporting enterprise-wide digital transformation and cloud-first security strategies. As enterprises continue adopting agentic AI and AI-native security operations, buyers increasingly prioritize platforms capable of continuously learning from evolving attack patterns and adapting security workflows with minimal manual intervention.

Risk assessment further considers AI hallucinations, model drift, adversarial AI attacks, governance complexity, data privacy, vendor transparency, integration effort, and operational dependence on autonomous decision-making. Organizations evaluate vendor maturity, AI model governance, deployment flexibility across cloud and hybrid environments, explainability, auditability, and the ability to maintain human oversight for high-impact security decisions. Economic viability is validated through reduced analyst workload, faster security investigations, lower operational costs, improved threat detection efficiency, stronger cyber resilience, optimized security tool utilization, and enhanced protection against advanced threats. As security operations continue evolving toward AI-native and agentic architectures, enterprises increasingly view AI SOC investments as strategic enablers of scalable, intelligent, and resilient cyber defense capable of supporting long-term business growth and digital resilience.

JULY 2026 © MarketsandMarkets™

FIGURE 28 AI SOC MARKET: DECISION-MAKING FACTORS



Source: Secondary Research

The chart highlights the key decision-making factors influencing enterprise investment in the AI SOC market, where Autonomous Threat Detection, Investigation & Response (94%) emerges as the strongest purchasing criterion. Organizations are rapidly moving beyond AI-assisted alert triage toward agentic security operations capable of autonomously investigating incidents, correlating security events, and executing response actions at machine speed. This shift is driven by increasingly sophisticated cyber threats, expanding attack surfaces, and persistent shortages of experienced cybersecurity professionals.

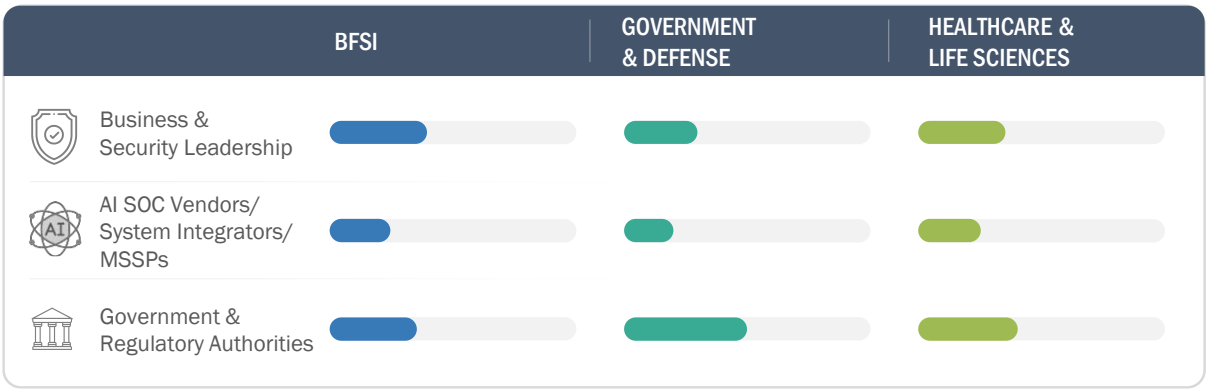
SOC Productivity & Workforce Optimization (93%) follows closely, reflecting growing demand for AI that automates repetitive analyst tasks, accelerates investigations, and improves overall security operations efficiency. Unified Security Data & Cross-Domain Visibility (91%) emphasizes the need to correlate endpoint, cloud, identity, network, and threat intelligence data within a single operational platform, improving investigation accuracy and contextual decision-making. Meanwhile, Lower Security Operations Costs Through AI Automation (90%) demonstrates enterprises' focus on reducing operational expenditure through intelligent automation and platform consolidation. Finally, AI Governance, Explainability & Enterprise Trust (89%) and Future-Ready AI-Native Security Architecture (88%) illustrate that organizations increasingly view transparent AI governance, auditability, and scalable AI-native platforms as essential requirements for deploying autonomous security operations while maintaining resilience against evolving cyber threats.

JULY 2026 © MarketsandMarkets™

8.2 KEY STAKEHOLDERS & BUYING CRITERIA

8.2.1 KEY STAKEHOLDERS IN BUYING PROCESS

FIGURE 29 INFLUENCE OF STAKEHOLDERS ON BUYING PROCESS FOR TOP THREE VERTICALS



Source: Secondary Research and MarketsandMarkets Analysis

TABLE 23 INFLUENCE OF STAKEHOLDERS ON BUYING PROCESS FOR TOP THREE VERTICALS

Key Stakeholder	BFSI	Government & Defense	Healthcare & Life Sciences
Business & Security Leadership	40%	30%	35%
AI SOC Vendors / System Integrators / MSSPs	25%	20%	25%
Government & Regulatory Authorities	35%	50%	40%
Total	**100%**	**100%**	**100%**

Source: MarketsandMarkets Analysis

8.2.2 BUYING CRITERIA

This sub-section outlines the key buying criteria users consider when purchasing AI SOC software platforms and services, including cost, quality, and performance.

FIGURE 30 KEY BUYING CRITERIA FOR TOP THREE VERTICALS



Source: MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 24 KEY BUYING CRITERIA FOR TOP THREE VERTICALS

Buying Criteria	BFSI	Healthcare & Life sciences	Government & Defense
Ownership Costs	5	4	4
Product Quality	5	4	5
Product Features	5	4	5
Brand Recognition/Reputation	4	3	4
Services	5	5	4
Relationship with Suppliers/Vendors	4	4	4
Regulatory Compliance	5	3	5

Note: Respondents have rated each criterion on a scale of 1–5, where 1 indicates "Least Important" and 5 indicates "Most Important or Critical."

Source: MarketsandMarkets Analysis

8.3 ADOPTION BARRIERS & INTERNAL CHALLENGES

Although AI SOCs are rapidly emerging as the next generation of cybersecurity operations, enterprise adoption remains in the early stages due to several technological, organizational, and governance challenges. Growing cyber threats, expanding hybrid and multi-cloud environments, and the need for autonomous security operations are driving demand for AI SOC platforms. However, organizations continue to face barriers related to fragmented security ecosystems, inconsistent security telemetry, legacy SOC infrastructures, and the complexity of integrating AI SOC solutions with existing SIEM, XDR, EDR, identity security, cloud security, and threat intelligence platforms. In addition, enterprises remain cautious about allowing autonomous AI agents to execute security actions without adequate explainability, governance, and human oversight.

While advancements in generative AI, agentic AI, security copilots, and autonomous investigation technologies are significantly improving SOC efficiency, challenges associated with AI governance, model transparency, data quality, regulatory compliance, and enterprise trust continue to influence adoption decisions. Organizations must also address shortages of cybersecurity professionals with AI expertise, internal resistance to AI-driven workflow transformation, and growing concerns surrounding AI hallucinations, adversarial attacks, privacy, and responsible AI deployment. Consequently, the long-term growth of the AI SOC market increasingly depends on collaboration among cybersecurity vendors, cloud providers, AI infrastructure providers, industry standards organizations, and regulators to develop secure, explainable, interoperable, and enterprise-ready AI SOC platforms capable of supporting trusted autonomous security operations.

JULY 2026 © MarketsandMarkets™

FIGURE 31 ADOPTION BARRIERS AND INTERNAL CHALLENGES



Source: Secondary Research

JULY 2026 © MarketsandMarkets™

8.4 UNMET NEEDS IN VARIOUS END-USE INDUSTRIES

Despite rapid advancements in autonomous security operations, generative AI, and agentic SOC platforms, the AI SOC market continues to face several unmet needs that limit large-scale enterprise adoption and operational maturity. Organizations increasingly require AI SOC platforms capable of delivering explainable AI, trustworthy autonomous decision-making, and seamless interoperability across fragmented security ecosystems. However, many enterprises still struggle with siloed security telemetry, inconsistent data quality, legacy security infrastructures, and complex integrations across SIEM, XDR, EDR, IAM, cloud security, and threat intelligence platforms. These challenges reduce the effectiveness of AI-driven investigations, autonomous response, and enterprise-wide cyber resilience. Additionally, concerns surrounding AI governance, data privacy, regulatory compliance, adversarial AI attacks, and model transparency continue to influence enterprise adoption strategies.

Unmet requirements also vary significantly across end-use industries due to differences in regulatory obligations, operational priorities, cyber-risk exposure, and digital maturity. Financial institutions require AI SOC platforms capable of detecting AI-enabled fraud, securing digital payments, and managing third-party cyber risks, while healthcare organizations demand AI-assisted protection for clinical systems, connected medical devices, and sensitive patient data. IT & telecommunications providers require autonomous detection across large-scale hybrid and cloud-native infrastructures, whereas manufacturing organizations need AI SOC platforms that correlate IT, OT, and IoT threats without disrupting operations. Government and defense agencies increasingly require sovereign AI SOC capabilities with high-assurance security, explainable AI, and mission-critical cyber resilience. Addressing these industry-specific gaps will be essential for accelerating enterprise adoption of trusted, scalable, and AI-native security operations.

TABLE 25 UNMET NEEDS AI SOC MARKET, BY END-USE INDUSTRY

END-USE INDUSTRY	UNMET NEEDS
BFSI	▪ AI SOC platforms capable of detecting AI-enabled financial fraud, account takeover, and deepfake-driven attacks in real time ▪ Explainable AI and automated compliance reporting aligned with financial regulations and audit requirements ▪ Unified visibility across digital banking, payment systems, cloud workloads, third-party ecosystems, and identity infrastructure
Healthcare & Life Sciences	▪ AI SOC capabilities for protecting connected medical devices, hospital networks, EHR systems, and clinical applications ▪ Privacy-preserving AI investigations that maintain compliance with healthcare data protection regulations ▪ Continuous monitoring across hybrid clinical, cloud, and biomedical research environments with minimal operational disruption
IT & Telecommunications	▪ Autonomous AI SOC platforms capable of securing large-scale cloud-native, multi-tenant, and 5G environments ▪ AI-driven correlation across network, endpoint, identity, application, and cloud telemetry at telecom scale ▪ Real-time protection against AI-powered attacks targeting telecom infrastructure and digital services

JULY 2026 © MarketsandMarkets™

Manufacturing	▪ Unified AI SOC platforms integrating IT, OT, IoT, industrial edge, and IIoT security telemetry ▪ Autonomous detection of cyber-physical threats without affecting production continuity ▪ AI-assisted security operations supporting smart factories, Industry 4.0 environments, and connected supply chains
Government & Defense	▪ Sovereign AI SOC platforms supporting classified environments and national cybersecurity operations ▪ Trusted AI with explainability, human oversight, and secure autonomous response for mission-critical systems ▪ Advanced AI-driven cyber defense against nation-state attacks across government, defense, and critical infrastructure networks

Source: Secondary Research

Addressing these unmet needs presents significant opportunities for AI SOC vendors, hyperscale cloud providers, cybersecurity platform vendors, MSSPs, and AI infrastructure companies. Organizations delivering explainable AI, agentic security operations, autonomous investigation capabilities, and interoperable AI-native security platforms will be well positioned to lead the next generation of security operations. Solutions that combine generative AI, autonomous security agents, unified telemetry, behavioral analytics, and real-time threat intelligence can enable faster detection, automated response, continuous risk assessment, and highly scalable cyber defense across increasingly complex hybrid enterprise environments.

Furthermore, alignment with emerging AI governance frameworks, cybersecurity regulations, and industry-specific compliance requirements will accelerate AI SOC adoption across BFSI, healthcare & life sciences, IT & telecommunications, manufacturing, and government & defense sectors. Strategic collaboration among AI SOC vendors, cloud service providers, cybersecurity technology vendors, standards organizations, and enterprise software providers will be essential to develop secure, interoperable, and enterprise-ready AI SOC ecosystems. Such collaboration will help organizations deploy trusted autonomous security operations while improving cyber resilience, operational efficiency, regulatory compliance, and long-term business continuity.

JULY 2026 © MarketsandMarkets™

9 AI SOC MARKET, BY OFFERING

KEY FINDINGS

- By offering, the software platforms segment is projected to have the largest market size, and it will grow from USD 11,323.8 million in 2026 to USD 28,552.6 million by 2031, at a CAGR of 20.3% during the forecast period.
- This significant growth is due to increasing enterprise adoption of unified AI-native SOC platforms that integrate threat detection, investigation, response, security analytics, and AI agents into a single operational environment, reducing security complexity and improving analyst productivity.
- Growing investments in agentic AI, security data lakes, AI-powered analytics, and autonomous SOC technologies by vendors such as Microsoft, Google, Cisco, CrowdStrike, and Palo Alto Networks are accelerating software platform adoption across hybrid, multi-cloud, and identity-centric enterprise infrastructures.
- The services segment is estimated to register the highest CAGR of 22.3%, growing from USD 6,777.5 million in 2026 to USD 18,513.6 million by 2031, as organizations increasingly outsource AI-enabled security operations through MDR, AI SOC-as-a-Service (SOCaaS), incident response, and threat intelligence services to address cybersecurity talent shortages and rapidly evolving threats.
- Rising adoption of cloud-native infrastructure, AI applications, and increasingly stringent cybersecurity and AI governance requirements is driving demand for consulting, deployment, managed operations, continuous optimization, and lifecycle security services that help enterprises maximize the value of AI SOC investments while reducing operational overhead.

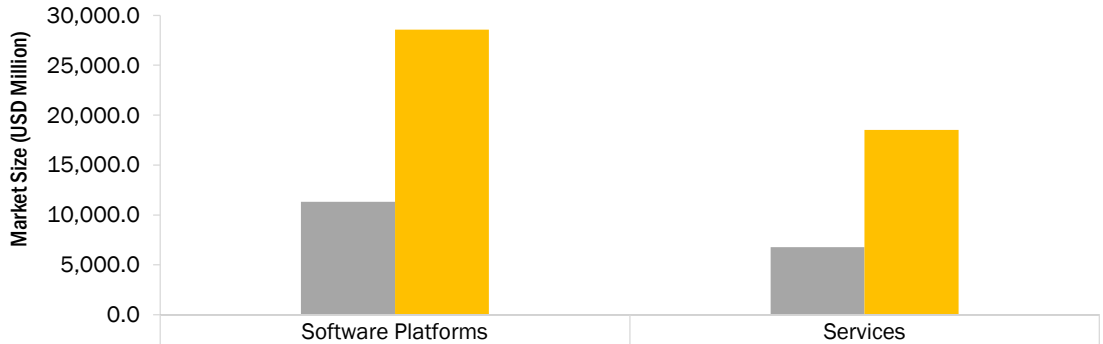
JULY 2026 © MarketsandMarkets™

9.1 INTRODUCTION

The AI SOC market by offering comprises Software Platforms and Services, which together enable organizations to modernize security operations through artificial intelligence, automation, and human expertise. Software platforms form the technological foundation of AI-driven Security Operations Centers by integrating capabilities such as AI-powered threat detection, security analytics, autonomous response, agentic AI, threat intelligence, security data management, and governance into unified platforms. Leading vendors including Microsoft, Palo Alto Networks, CrowdStrike, Google, Cisco, SentinelOne, Sophos, ReliaQuest, Exabeam, and Anvilogic are continuously expanding these platforms with generative AI and autonomous security agents that reduce analyst workload while improving detection accuracy and response speed. At the same time, government initiatives promoting secure AI adoption and cybersecurity resilience are encouraging organizations to invest in AI-enabled security operations and trustworthy AI governance frameworks.

Complementing software platforms, AI-driven security services help organizations operationalize advanced security capabilities without maintaining large in-house SOC teams. AI-augmented MDR, SOC-as-a-Service (SOCaaS), incident response and forensics, and threat intelligence services combine machine-speed analytics with expert oversight to deliver continuous monitoring, rapid investigations, and guided remediation. Vendors such as Arctic Wolf, eSentire, Expel, Huntress, Sophos, Rapid7, UnderDefense, RiverSafe, CyberNX, and Vulnuris are increasingly embedding AI into managed security offerings to improve operational efficiency, accelerate incident response, and address the growing shortage of skilled cybersecurity professionals. Together, software platforms and services are driving the transition from reactive SOC operations toward intelligent, adaptive, and highly automated security operations capable of defending increasingly complex hybrid, cloud-native, and AI-enabled enterprise environments.

FIGURE 32 SERVICES SEGMENT TO GROW AT HIGHER CAGR DURING FORECAST PERIOD



	Software Platforms	Services
2026	11,323.8	6,777.5
2031	28,552.6	18,513.6
CAGR (2026–2031)	20.3%	22.3%

Source: Expert Interviews and MarketsandMarkets Analysis

9.1.1 OFFERING: AI SOC MARKET DRIVERS

- Rapid adoption of agentic AI across enterprise security operations is accelerating investments in AI-native software platforms and AI-powered security services that autonomously investigate alerts, orchestrate response actions, and reduce dependence on manual SOC workflows.
- Escalating cyberattack sophistication and exponentially increasing security telemetry are driving organizations toward AI-enabled detection, analytics, and managed security offerings capable of correlating multi-source data and identifying advanced threats with greater speed and accuracy.

JULY 2026 © MarketsandMarkets™

- Persistent shortages of experienced cybersecurity professionals are increasing enterprise reliance on AI-augmented MDR, SOC-as-a-Service, and intelligent automation platforms that improve analyst productivity while enabling 24×7 security operations without proportionally expanding SOC teams.
- Growing adoption of hybrid cloud, SaaS applications, digital identities, and distributed enterprise infrastructures is fueling demand for unified AI security platforms that consolidate telemetry, automate investigations, and provide centralized visibility across diverse IT environments.
- Increasing regulatory focus on trustworthy AI, secure AI agents, and operational governance is encouraging enterprises to invest in AI governance, risk, compliance, and advisory offerings alongside AI SOC platforms to strengthen resilience and ensure responsible AI adoption.
- Continuous innovation by leading vendors including Microsoft, Google, Palo Alto Networks, Cisco, CrowdStrike, Sophos, SentinelOne, and emerging AI SOC specialists is expanding the availability of integrated AI platforms and managed services that simplify enterprise AI SOC adoption.
- Government initiatives promoting secure AI deployment, AI agent standards, and cybersecurity modernization are encouraging public- and private-sector organizations to accelerate investments in AI-powered security platforms and specialized AI SOC service offerings.

TABLE 26 AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	5,619.7	6,673.3	7,943.1	9,471.8	19.0%
Services	3,158.5	3,809.8	4,606.4	5,580.1	20.9%
Total	**8,778.2**	**10,483.1**	**12,549.5**	**15,051.9**	**19.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 27 AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	11,323.8	13,573.4	16,308.3	19,632.6	23,669.1	28,552.6	20.3%
Services	6,777.5	8,253.9	10,076.4	12,326.0	15,101.2	18,513.6	22.3%
Total	**18,101.3**	**21,827.3**	**26,384.6**	**31,958.6**	**38,770.3**	**47,066.1**	**21.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

9.2 SOFTWARE PLATFORMS

9.2.1 RISING ENTERPRISE DEMAND FOR UNIFIED AI SECURITY PLATFORMS TO DRIVE SOFTWARE PLATFORM ADOPTION

Software platforms represent the technological foundation of the AI SOC market, enabling organizations to transform conventional Security Operations Centers into intelligent, data-driven, and increasingly autonomous cyber defense environments. Unlike traditional security tools that operate independently, AI SOC software platforms unify telemetry from endpoints, networks, cloud workloads, identities, applications, email, and third-party security solutions to provide centralized visibility and real-time threat analysis. The rapid increase in AI-assisted cyberattacks, expanding digital infrastructures, and growing volumes of security data have accelerated enterprise demand for integrated platforms capable of continuously detecting, correlating, prioritizing, investigating, and responding to threats at machine speed. Vendors including Microsoft, Palo Alto Networks, Google, Cisco, CrowdStrike, SentinelOne, Sophos, IBM, Elastic, and Rapid7 are evolving their platforms by embedding generative AI, agentic AI, behavioral analytics, and autonomous reasoning directly into core security operations.

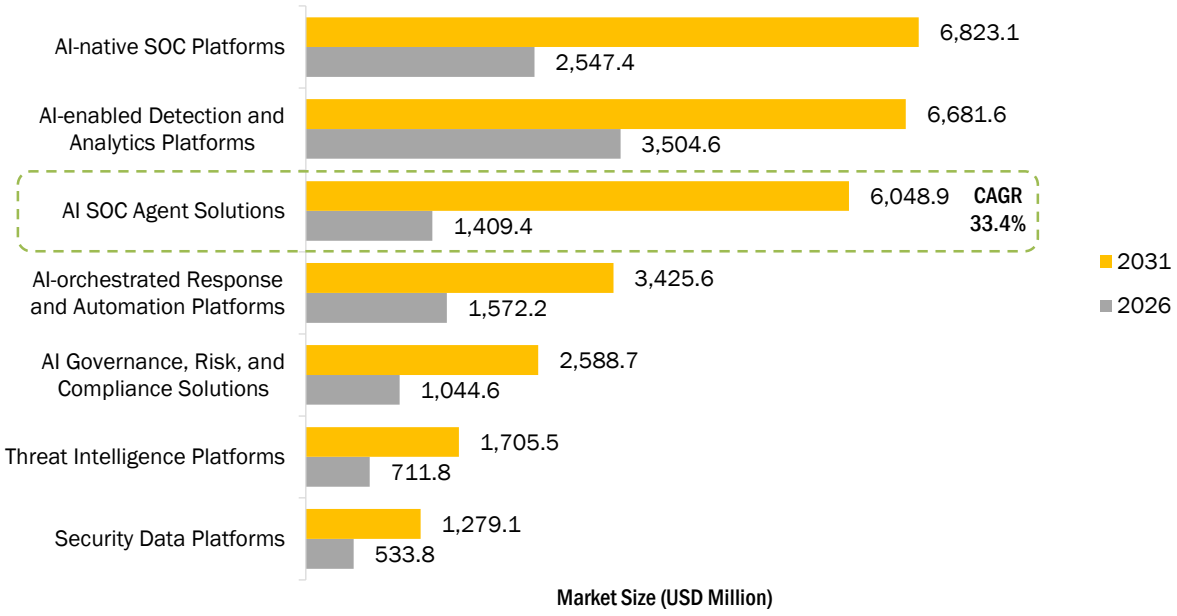
The software platform landscape has evolved beyond traditional SIEM and SOAR architectures toward unified AI-native security operations platforms that combine detection engineering, AI-powered analytics, automation, security data management, threat intelligence, and governance within a single operational framework. Recent innovations including Microsoft's expansion of Security Copilot agents, Palo Alto Networks' autonomous Cortex XSIAM capabilities, Google's Gemini-powered Security Operations, Cisco's integration of Splunk into its AI-driven Security Cloud, and emerging agentic SOC platforms from ReliaQuest, Exaforce, Radiant Security, Prophet Security, Dropzone AI, Simbian, Torq, and Intezer demonstrate an industry-wide transition from assistive AI to autonomous AI agents capable of independently executing Tier-1 and increasingly complex security workflows under human supervision. This evolution is reducing alert fatigue, improving investigation consistency, and allowing analysts to focus on advanced threat hunting and strategic decision-making rather than repetitive operational tasks.

Government agencies and regulatory bodies are also influencing the growth of AI SOC software platforms by emphasizing trustworthy AI, secure AI deployment, cyber resilience, and responsible automation. Organizations such as NIST, CISA, ENISA, and the UK National Cyber Security Centre are promoting guidance for secure AI adoption, AI risk management, Zero Trust architectures, and resilient security operations, encouraging enterprises to deploy AI platforms with explainability, governance, human oversight, and policy-driven automation. These initiatives are driving demand for software platforms that incorporate AI governance, compliance monitoring, security analytics, and auditability alongside autonomous detection and response capabilities. As organizations increasingly adopt hybrid cloud, multi-cloud, SaaS, operational technology (OT), and AI-enabled business applications, software platforms capable of securing highly distributed digital ecosystems are becoming strategic cybersecurity investments rather than standalone operational tools.

Looking toward 2031, software platforms are expected to remain the largest offering segment within the AI SOC market as enterprises pursue greater platform consolidation, operational efficiency, and cyber resilience. Future innovation will increasingly focus on multi-agent AI collaboration, predictive threat reasoning, self-learning detection models, autonomous investigation pipelines, and continuous security optimization across enterprise environments. Rather than replacing human analysts, next-generation AI SOC platforms will augment security teams by combining autonomous execution with human governance, enabling organizations to build adaptive, scalable, and continuously improving security operations capable of responding to increasingly sophisticated AI-powered cyber threats. Continuous investments from established cybersecurity leaders and emerging AI SOC specialists are expected to further accelerate platform maturity, enterprise adoption, and market expansion throughout the forecast period.

JULY 2026 © MarketsandMarkets™

FIGURE 33 AI SOC AGENT SOLUTIONS SEGMENT TO GROW AT HIGHER CAGR DURING FORECAST PERIOD



Source: Expert Interviews and MarketsandMarkets Analysis

TABLE 28 AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platform	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	2,086.5	2,374.5	2,703.7	3,093.7	14.0%
AI-orchestrated Response and Automation Platforms	866.0	1,002.9	1,163.4	1,353.1	16.0%
AI-native SOC Platforms	1,201.5	1,445.3	1,742.5	2,104.8	20.6%
AI SOC Agent Solutions	358.0	523.9	742.9	1,060.5	43.6%
Security Data Platforms	275.5	324.0	381.9	451.0	17.9%
Threat Intelligence Platforms	367.3	432.0	509.2	601.4	17.9%
AI Governance, Risk, and Compliance Solutions	465.0	570.6	699.5	807.3	20.2%
Total	**5,619.7**	**6,673.3**	**7,943.1**	**9,471.8**	**19.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 29 AI SOC MARKET, BY SOFTWARE PLATFORMS, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	3,504.6	3,978.4	4,523.9	5,150.5	5,867.4	6,681.6	13.8%
AI-orchestrated Response and Automation Platforms	1,572.2	1,831.2	2,137.4	2,499.0	2,925.4	3,425.6	16.9%
AI-native SOC Platforms	2,547.4	3,090.8	3,758.9	4,580.2	5,588.7	6,823.1	21.8%
AI SOC Agent Solutions	1,409.4	1,878.5	2,509.9	3,360.5	4,506.9	6,048.9	33.8%
Security Data Platforms	533.8	633.4	753.4	897.7	1,071.3	1,279.1	19.1%
Threat Intelligence Platforms	711.8	844.6	1,004.5	1,197.0	1,428.4	1,705.5	19.1%
AI Governance, Risk, and Compliance Solutions	1,044.6	1,316.6	1,620.3	1,947.6	2,281.0	2,588.7	19.9%
Total	**11,323.8**	**13,573.4**	**16,308.3**	**19,632.6**	**23,669.1**	**28,552.6**	**20.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 30 AI SOC SOFTWARE PLATFORMS MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	2,541.9	2,955.2	3,443.9	4,020.7	16.5%
Europe	1,468.6	1,728.2	2,038.4	2,409.0	17.9%
Asia Pacific	1,149.8	1,415.8	1,747.4	2,160.6	23.4%
Middle East & Africa	253.0	311.0	382.6	472.2	23.1%
Latin America	206.3	263.1	330.8	409.3	25.7%
Total	**5,619.7**	**6,673.3**	**7,943.1**	**9,471.8**	**19.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 31 AI SOC SOFTWARE PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	4,706.2	5,523.0	6,497.0	7,657.8	9,039.3	10,676.5	17.8%
Europe	2,852.8	3,387.3	4,031.4	4,807.6	5,741.7	6,861.5	19.2%
Asia Pacific	2,678.3	3,328.8	4,146.9	5,176.2	6,470.4	8,092.9	24.8%
Middle East & Africa	581.1	717.0	886.6	1,098.6	1,363.2	1,692.5	23.8%
Latin America	505.4	617.3	746.2	892.3	1,054.5	1,229.1	19.5%
Total	**11,323.8**	**13,573.4**	**16,308.3**	**19,632.6**	**23,669.1**	**28,552.6**	**20.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

9.2.2 AI-ENABLED DETECTION AND ANALYTICS PLATFORMS

9.2.2.1 AI-driven threat detection and contextual security analytics are redefining modern security operations

AI-enabled detection and analytics platforms form the analytical foundation of modern AI-powered Security Operations Centers by transforming vast volumes of security telemetry into actionable intelligence. Unlike traditional rule-based detection systems that rely heavily on manually created signatures and static correlation rules, these platforms continuously analyze endpoint, network, identity, cloud, application, and threat intelligence data to identify subtle behavioral deviations, emerging attack patterns, and previously unknown threats. Leveraging machine learning, behavioral analytics, graph intelligence, and generative AI, provide dynamic risk scoring, anomaly detection, and contextual prioritization that significantly improve detection accuracy while reducing false positives. Vendors such as Microsoft (Microsoft Defender XDR and Security Copilot), Google Security Operations, CrowdStrike Falcon, Palo Alto Networks Cortex XSIAM, Cisco XDR, SentinelOne, Elastic, Exabeam, and Stellar Cyber continue expanding AI-driven analytics capabilities that enable analysts to detect increasingly sophisticated identity-based attacks, insider threats, cloud compromises, and AI-assisted cyber intrusions. Recent innovations—including Microsoft's specialized cybersecurity AI models, CrowdStrike's Falcon Next-Gen SIEM enhancements, and Google Security Operations' Gemini-powered analytics—illustrate the industry's shift toward AI-native detection architectures capable of continuously learning from evolving attack behaviors.

The strategic importance of AI-enabled detection platforms continues to grow as enterprises deploy generative AI, autonomous AI agents, hybrid cloud infrastructures, and increasingly distributed digital ecosystems. Government organizations and standards bodies are simultaneously emphasizing continuous monitoring, trustworthy AI, and post-deployment AI oversight through initiatives such as NIST's Center for AI Standards and Innovation (CAISI), reinforcing the need for intelligent monitoring technologies capable of adapting to dynamic threat environments. AI-enabled analytics platforms are therefore evolving beyond event correlation into predictive security intelligence engines that combine telemetry fusion, automated reasoning, explainable AI, and continuous risk assessment. As the market evolves, these platforms are expected to become the primary decision engines within AI-native SOCs, supporting autonomous detection, adaptive threat modeling, and proactive cyber defense across enterprise, cloud, operational technology (OT), and AI-enabled environments while enabling security teams to respond to increasingly machine-speed cyber threats.

TABLE 32 AI-ENABLED DETECTION AND ANALYTICS PLATFORMS MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	944.7	1,052.1	1,172.2	1,313.2	11.6%
Europe	544.0	614.2	693.8	786.8	13.1%
Asia Pacific	428.0	504.5	594.8	705.7	18.1%
Middle East & Africa	93.5	110.4	130.2	154.2	18.2%
Latin America	76.2	93.3	112.6	133.7	20.6%
Total	**2,086.5**	**2,374.5**	**2,703.7**	**3,093.7**	**14.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 33 AI-ENABLED DETECTION AND ANALYTICS PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,454.9	1,615.6	1,797.5	2,002.8	2,233.4	2,490.2	11.3%
Europe	885.3	997.9	1,126.3	1,272.4	1,437.7	1,623.2	12.9%
Asia Pacific	826.2	969.7	1,140.6	1,343.8	1,585.1	1,870.2	17.7%
Middle East & Africa	180.8	212.1	249.2	292.8	343.9	403.5	17.4%
Latin America	157.4	183.1	210.4	238.8	267.3	294.5	13.3%
Total	**3,504.6**	**3,978.4**	**4,523.9**	**5,150.5**	**5,867.4**	**6,681.6**	**13.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

9.2.3 AI-ORCHESTRATED RESPONSE AND AUTOMATION PLATFORMS

9.2.3.1 Intelligent security orchestration and agentic automation are transforming incident response operations

AI-orchestrated response and automation platforms are becoming the operational backbone of next-generation Security Operations Centers by enabling organizations to move beyond rule-based workflows toward intelligent, adaptive response mechanisms. Unlike traditional SOAR platforms that execute predefined playbooks, modern AI-orchestrated platforms leverage generative AI, agentic AI, reasoning engines, and contextual decision-making to dynamically coordinate investigations, validate attack hypotheses, enrich alerts, recommend remediation actions, and execute response workflows across multiple security technologies. These platforms integrate endpoint protection, identity security, cloud security, threat intelligence, ticketing systems, and network controls into unified operational workflows that substantially reduce analyst intervention while improving response consistency. Vendors including Palo Alto Networks (Cortex XSIAM and Cortex XSOAR), Microsoft Security Copilot, Google Security Operations, Cisco XDR, CrowdStrike Charlotte AI, Torq AI SOC Platform, Swimlane, BlinkOps, and D3 Security are rapidly expanding AI-driven orchestration capabilities to support autonomous security operations. Recent innovations—including CrowdStrike's Charlotte AI Agentic Response and Charlotte Agentic SOAR, together with Palo Alto Networks' continued expansion of Cortex XSIAM's autonomous SOC capabilities—demonstrate the industry's transition from workflow automation to coordinated AI-driven security execution.

The evolution of AI orchestration is also being shaped by increasing enterprise demand for machine-speed cyber defense as adversaries adopt AI to accelerate attacks. Rather than automating isolated security tasks, organizations are deploying AI-orchestrated platforms that coordinate multiple AI agents, security tools, and human analysts within a single operational framework while maintaining governance, policy enforcement, and analyst oversight. Government guidance promoting trustworthy AI, explainability, and human accountability, including NIST's AI Risk Management Framework, further reinforces the importance of controlled autonomous decision-making within enterprise security operations. As AI-native security ecosystems mature, orchestration platforms are expected to become central coordination layers capable of continuously optimizing detection, investigation, containment, and recovery activities across hybrid cloud, multi-cloud, operational technology (OT), and AI-enabled enterprise environments. In the years ahead, AI-orchestrated response and automation platforms are expected to evolve into fully adaptive operational control planes that intelligently synchronize security actions across distributed infrastructures, enabling resilient, policy-driven, and autonomous SOC operations at enterprise scale.

JULY 2026 © MarketsandMarkets™

TABLE 34 AI-ORCHESTRATED RESPONSE AND AUTOMATION PLATFORMS MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	391.8	444.2	504.4	574.4	13.6%
Europe	226.2	259.6	298.6	344.1	15.0%
Asia Pacific	177.3	212.9	255.9	308.7	20.3%
Middle East & Africa	38.9	46.7	56.0	67.5	20.1%
Latin America	31.7	39.5	48.5	58.5	22.6%
Total	**866.0**	**1,002.9**	**1,163.4**	**1,353.1**	**16.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 35 AI-ORCHESTRATED RESPONSE AND AUTOMATION PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	653.2	744.7	850.9	974.0	1,116.3	1,279.9	14.4%
Europe	396.4	457.6	529.3	613.3	711.4	825.3	15.8%
Asia Pacific	371.5	448.4	542.3	657.2	797.4	968.1	21.1%
Middle East & Africa	80.8	97.0	116.6	140.4	169.2	204.0	20.3%
Latin America	70.3	83.5	98.2	114.2	131.0	148.3	16.1%
Total	**1,572.2**	**1,831.2**	**2,137.4**	**2,499.0**	**2,925.4**	**3,425.6**	**16.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

9.2.4 AI-NATIVE SOC PLATFORMS

9.2.4.1 Unified AI-native security operations platforms are driving the transition toward autonomous cyber defense

AI-native SOC platforms are fundamentally reshaping security operations by converging detection, investigation, response, threat intelligence, security analytics, and automation into a single intelligence-driven operating environment. Unlike conventional SOC architectures built around multiple standalone SIEM, SOAR, XDR, and analytics solutions, AI-native platforms are designed with artificial intelligence as the core operational layer rather than an additional capability. These platforms continuously ingest and correlate telemetry from endpoints, identities, networks, cloud environments, applications, operational technology (OT), and external threat intelligence sources to provide unified situational awareness, contextual reasoning, and autonomous decision support. By eliminating fragmented security workflows and data silos, AI-native SOC platforms enable analysts to investigate complete attack chains from a centralized interface while significantly improving operational efficiency. Industry leaders including Microsoft (Unified Security Operations Platform), Google Security Operations, Palo Alto Networks Cortex XSIAM, Cisco XDR, CrowdStrike Falcon, Elastic Security, Arctic Wolf Aurora Platform, ReliaQuest GreyMatter, and Stellar Cyber Open XDR continue investing in unified AI-native architectures that integrate generative AI, agentic AI, behavioral analytics, and autonomous investigations into end-to-end security operations. Recent platform enhancements, including Cortex XSIAM's expanded Agentic AI capabilities and Microsoft's AI-powered unified security platform, demonstrate the industry's strategic shift toward consolidated AI-native SOC ecosystems.

JULY 2026 © MarketsandMarkets™

The rapid evolution of enterprise AI adoption, increasingly complex hybrid infrastructures, and growing regulatory emphasis on trustworthy AI are accelerating demand for integrated AI-native security operations. Organizations are seeking platforms capable of simultaneously protecting traditional IT assets, cloud-native workloads, AI applications, and autonomous AI agents while maintaining governance, explainability, and policy-based oversight. Government initiatives such as NIST's AI Risk Management Framework (AI RMF) and ongoing work on AI security guidance for critical infrastructure are reinforcing the importance of secure, accountable, and continuously monitored AI-enabled security operations. Rather than functioning solely as security monitoring tools, AI-native SOC platforms are evolving into enterprise cyber resilience platforms that coordinate detection, investigation, response, exposure management, and AI governance through a common data foundation. Going forward, these platforms are expected to become the primary operating model for modern Security Operations Centers, enabling organizations to transition from reactive incident management toward predictive, self-optimizing, and increasingly autonomous cyber defense capable of protecting highly distributed digital and AI-driven enterprise environments.

TABLE 36 AI-NATIVE SOC PLATFORMS MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	543.5	640.1	755.5	893.5	18.0%
Europe	313.9	374.3	447.2	535.3	19.5%
Asia Pacific	245.9	306.7	383.3	480.1	25.0%
Middle East & Africa	54.1	67.3	83.9	104.9	24.7%
Latin America	44.1	57.0	72.6	91.0	27.3%
Total	**1,201.5**	**1,445.3**	**1,742.5**	**2,104.8**	**20.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 37 AI-NATIVE SOC PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,058.6	1,257.6	1,497.4	1,786.3	2,134.1	2,551.1	19.2%
Europe	641.8	771.5	929.5	1,122.0	1,356.2	1,640.2	20.6%
Asia Pacific	602.4	757.8	955.5	1,207.1	1,527.1	1,933.1	26.3%
Middle East & Africa	130.8	163.3	204.5	256.4	322.1	404.7	25.4%
Latin America	113.7	140.7	172.1	208.3	249.2	293.9	20.9%
Total	**2,547.4**	**3,090.8**	**3,758.9**	**4,580.2**	**5,588.7**	**6,823.1**	**21.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

9.2.5 AI SOC AGENT SOLUTIONS

9.2.5.1 Agentic AI is enabling autonomous security operations through intelligent AI SOC agents

AI SOC agent solutions represent the next evolution of security operations by introducing autonomous software agents capable of independently performing investigation, reasoning, decision support, and response activities that traditionally required human analysts. Unlike AI copilots that primarily assist users through recommendations or conversational interfaces, AI SOC agents execute multi-step investigative workflows by gathering evidence, correlating alerts, querying security tools, validating attack hypotheses, recommending remediation actions, and, where authorized, initiating response actions under human-defined governance policies. These solutions leverage large language models (LLMs), retrieval-augmented generation (RAG), behavioral intelligence, memory frameworks, and reasoning engines to continuously adapt investigations based on contextual information rather than static playbooks. Leading vendors including Microsoft (Security Copilot Agents), Google Security Operations, CrowdStrike Charlotte AI, Palo Alto Networks Cortex Agentic AI, Prophet Security, Dropzone AI, Radiant Security, Simbian, Legion Security, Intezer, Exaforce, Conifers.AI, and Lumu Technologies are actively developing agentic AI capabilities that enable Security Operations Centers to automate complex analyst workflows while maintaining explainability and human oversight. The rapid emergence of purpose-built AI SOC agent platforms demonstrates the industry's transition from AI-assisted security operations toward autonomous SOC execution.

The rapid expansion of enterprise AI adoption has simultaneously increased the need for secure, governed deployment of autonomous AI agents. Governments and standards organizations are responding by developing frameworks specifically addressing AI agent security, identity, authorization, and interoperability. In 2026, NIST's Center for AI Standards and Innovation (CAISI) launched the AI Agent Standards Initiative and published guidance on securing AI agent systems, highlighting the importance of trustworthy, interoperable, and securely governed autonomous agents across enterprise environments. These initiatives reinforce enterprise demand for AI SOC agent solutions that combine autonomous execution with robust governance, auditability, policy enforcement, and human-in-the-loop controls. Rather than replacing security professionals, AI SOC agents are increasingly functioning as specialized digital teammates capable of operating continuously across detection, investigation, threat hunting, malware analysis, and incident response workflows. In the upcoming years, AI SOC agent solutions are expected to become foundational components of AI-native Security Operations Centers, enabling organizations to deploy collaborative teams of specialized AI agents that significantly improve operational efficiency, accelerate cyber defense, and strengthen resilience against increasingly machine-speed attacks while maintaining accountable and secure AI operations.

TABLE 38 AI SOC AGENT SOLUTIONS MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	163.7	236.7	330.2	463.7	41.5%
Europe	91.2	129.5	179.6	250.6	40.1%
Asia Pacific	75.4	117.2	174.9	262.7	51.6%
Middle East & Africa	15.3	22.1	31.6	45.5	43.9%
Latin America	12.3	18.3	26.5	38.0	45.5%
Total	**358.0**	**523.9**	**742.9**	**1,060.5**	**43.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 39 AI SOC AGENT SOLUTIONS MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	602.6	785.3	1,025.7	1,342.5	1,759.7	2,308.1	30.8%
Europe	330.2	436.1	577.6	766.3	1,018.3	1,354.2	32.6%
Asia Pacific	361.7	499.3	690.9	958.0	1,330.2	1,848.2	38.6%
Middle East & Africa	62.6	86.3	119.2	164.9	228.5	316.8	38.3%
Latin America	52.4	71.5	96.5	128.9	170.2	221.6	33.4%
Total	**1,409.4**	**1,878.5**	**2,509.9**	**3,360.5**	**4,506.9**	**6,048.9**	**33.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

9.2.6 SECURITY DATA PLATFORMS

9.2.6.1 Unified security data foundations are enabling AI-ready security operations at enterprise scale

Security data platforms are emerging as a critical component of AI-native security operations centers by providing a unified, scalable foundation for collecting, storing, normalizing, and analyzing massive volumes of security telemetry across hybrid enterprise environments. Modern organizations generate petabytes of security data from endpoints, cloud workloads, identities, networks, applications, operational technology (OT), SaaS platforms, and third-party security tools, making fragmented data architectures increasingly ineffective for AI-driven security operations. Security data platforms consolidate these heterogeneous datasets into centralized repositories or security data lakes, enabling advanced analytics, AI model training, long-term retention, and cross-domain threat correlation from a single operational environment. Vendors including Microsoft (Microsoft Sentinel Data Lake), Google Security Operations, Elastic Search AI Lake, Cisco Splunk Platform, Palo Alto Networks, IBM, CrowdStrike, and Anvilogic continue investing in AI-ready data architectures that eliminate telemetry silos while supporting high-performance analytics and autonomous investigations. Recent developments such as Microsoft's Sentinel Data Lake and Elastic's Search AI Lake demonstrate the industry's transition toward cloud-native security data platforms designed to power AI-driven detection, agentic security operations, and large-scale security analytics. These platforms increasingly support open data architectures that simplify integration across diverse security ecosystems while reducing operational complexity.

The strategic importance of security data platforms continues to increase as organizations deploy generative AI, autonomous AI agents, and enterprise-wide security analytics that depend on complete, high-quality, and contextualized telemetry. Rather than functioning solely as centralized log repositories, these platforms are evolving into enterprise security intelligence layers that provide unified data access for AI models, threat hunting, forensic investigations, compliance reporting, and automated response workflows. Government initiatives promoting trustworthy AI, stronger cyber resilience, and continuous security monitoring, including NIST's guidance on AI governance and cybersecurity, further reinforce the need for secure, scalable, and interoperable security data infrastructures capable of supporting AI-powered security operations. As enterprises continue their cybersecurity transformation, security data platforms are expected to become the foundational data layer for AI-native SOCs, enabling organizations to securely manage exponentially growing security telemetry while supporting predictive analytics, autonomous cyber defense, and cross-platform AI collaboration across increasingly distributed digital ecosystems.

JULY 2026 © MarketsandMarkets™

TABLE 40 AI SECURITY DATA PLATFORMS MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	124.6	143.5	165.6	191.5	15.4%
Europe	72.0	83.9	98.0	114.7	16.8%
Asia Pacific	56.4	68.7	84.0	102.9	22.2%
Middle East & Africa	12.4	15.1	18.4	22.5	21.9%
Latin America	10.1	12.8	15.9	19.5	24.4%
Total	**275.5**	**324.0**	**381.9**	**451.0**	**17.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 41 AI SECURITY DATA PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	221.8	257.7	300.1	350.1	409.1	478.3	16.6%
Europe	134.5	158.1	186.3	219.9	260.0	307.5	18.0%
Asia Pacific	126.2	155.3	191.5	236.6	292.8	362.4	23.5%
Middle East & Africa	27.4	33.5	41.0	50.3	61.7	75.9	22.6%
Latin America	23.8	28.8	34.5	40.8	47.8	55.1	18.3%
Total	**533.8**	**633.4**	**753.4**	**897.7**	**1,071.3**	**1,279.1**	**19.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

9.2.7 THREAT INTELLIGENCE PLATFORMS

9.2.7.1 Real-time threat intelligence to enable proactive and context-aware AI security operations

Threat intelligence platforms are becoming indispensable components of AI-native security operations centers by providing continuously updated intelligence on adversaries, attack techniques, malware campaigns, vulnerabilities, indicators of compromise (IoCs), and emerging AI-enabled threats. Unlike conventional threat feeds that primarily distribute static indicators, modern AI-powered threat intelligence platforms aggregate data from global telemetry networks, open-source intelligence (OSINT), dark web monitoring, malware sandboxes, vulnerability databases, and proprietary research teams to generate contextual intelligence that enhances every stage of the security lifecycle. Artificial intelligence further enriches this intelligence by automatically correlating attacker behavior, mapping adversary tactics to frameworks such as MITRE ATT&CK, identifying attack trends, and prioritizing threats based on organizational risk. Vendors including Microsoft, Google, CrowdStrike, Cisco, Palo Alto Networks, IBM, Fortinet, ReliaQuest, Rapid7, and Intezer continue strengthening AI-driven threat intelligence capabilities that improve proactive defense and decision-making. Recent innovations such as CrowdStrike Threat AI, the industry's first agentic threat intelligence system, and Microsoft's collaboration with CrowdStrike to harmonize threat actor attribution demonstrate how AI is transforming threat intelligence into an operational decision engine rather than a passive information source.

As cyber adversaries increasingly weaponize generative AI and autonomous attack techniques, enterprises require continuously evolving intelligence capable of anticipating emerging threats before they impact operations. Government agencies and international cybersecurity organizations are simultaneously emphasizing intelligence sharing and coordinated cyber defense to strengthen national cyber resilience. AI-

JULY 2026 © MarketsandMarkets™

powered threat intelligence platforms are therefore evolving beyond external threat feeds into collaborative intelligence ecosystems that continuously support threat hunting, detection engineering, incident response, exposure management, and AI agent decision-making. As AI SOC adoption continues to accelerate, these platforms are expected to function as the strategic intelligence layer of AI-native SOCs, continuously learning from global cyber activity, autonomously updating defensive models, and enabling predictive security operations that identify emerging attack campaigns before they escalate into enterprise-wide incidents.

TABLE 42 AI THREAT INTELLIGENCE PLATFORMS MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	166.1	191.3	220.8	255.3	15.4%
Europe	96.0	111.9	130.7	153.0	16.8%
Asia Pacific	75.2	91.7	112.0	137.2	22.2%
Middle East & Africa	16.5	20.1	24.5	30.0	21.9%
Latin America	13.5	17.0	21.2	26.0	24.4%
Total	**367.3**	**432.0**	**509.2**	**601.4**	**17.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 43 AI THREAT INTELLIGENCE PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	295.8	343.6	400.1	466.8	545.5	637.7	16.6%
Europe	179.3	210.8	248.4	293.2	346.6	410.0	18.0%
Asia Pacific	168.3	207.1	255.4	315.5	390.4	483.3	23.5%
Middle East & Africa	36.5	44.6	54.6	67.0	82.3	101.1	22.6%
Latin America	31.8	38.4	46.0	54.4	63.7	73.5	18.3%
Total	**711.8**	**844.6**	**1,004.5**	**1,197.0**	**1,428.4**	**1,705.5**	**19.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

9.2.8 AI GOVERNANCE, RISK, AND COMPLIANCE SOLUTIONS

9.2.8.1 Responsible AI governance and continuous compliance are emerging as core components of AI-native security operations

AI governance, risk, and compliance (GRC) solutions are rapidly becoming a strategic element of AI SOC architectures as enterprises seek to securely deploy, monitor, and govern artificial intelligence across increasingly complex business environments. The rapid adoption of generative AI, large language models (LLMs), AI agents, and autonomous business applications has introduced new risks related to model misuse, prompt injection, sensitive data exposure, regulatory compliance, AI transparency, and policy enforcement. Consequently, organizations are integrating AI GRC solutions into security operations centers to continuously assess AI risk posture, monitor AI asset inventories, identify shadow AI usage, validate policy compliance, and support secure AI lifecycle management. Rather than functioning solely as compliance tools, these platforms provide continuous visibility into AI deployments while enabling security teams to govern AI systems alongside traditional enterprise infrastructure. Vendors including Microsoft, Google, IBM, Cisco, Palo Alto Networks, CrowdStrike, and emerging AI governance providers continue expanding capabilities for AI security posture management, AI asset discovery, runtime monitoring, and

JULY 2026 © MarketsandMarkets™

policy-driven AI governance. Microsoft's expansion of AI Security Posture Management across multicloud and multimodel environments exemplifies the industry's growing emphasis on integrated AI governance within enterprise security operations.

Regulatory momentum is further accelerating adoption of AI GRC solutions as governments and standards bodies establish frameworks for trustworthy and secure AI deployment. The NIST AI Risk Management Framework (AI RMF), together with emerging AI governance initiatives worldwide, encourages organizations to implement continuous monitoring, explainability, accountability, and lifecycle risk management for AI systems. These evolving expectations are driving enterprises to integrate governance directly into AI SOC workflows so that AI security, compliance, and operational resilience are managed through a unified security platform. In the coming years, AI GRC solutions are expected to evolve from compliance-focused technologies into continuous AI assurance platforms capable of autonomously monitoring AI models, AI agents, data usage, and regulatory obligations while supporting secure, transparent, and responsible enterprise AI adoption across increasingly AI-driven digital ecosystems.

TABLE 44 AI GOVERNANCE, RISK, AND COMPLIANCE SOLUTIONS MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	207.4	247.4	295.1	329.1	16.6%
Europe	125.2	154.8	190.6	224.4	21.5%
Asia Pacific	91.6	114.2	142.4	163.4	21.3%
Middle East & Africa	22.3	29.2	37.9	47.6	28.8%
Latin America	18.4	25.2	33.6	42.8	32.5%
Total	**465.0**	**570.6**	**699.5**	**807.3**	**20.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 45 AI GOVERNANCE, RISK, AND COMPLIANCE SOLUTIONS MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	419.2	518.6	625.3	735.3	841.2	931.2	17.3%
Europe	285.3	355.3	434.1	520.6	611.5	701.1	19.7%
Asia Pacific	221.9	291.2	370.8	458.1	547.4	627.5	23.1%
Middle East & Africa	62.3	80.2	101.6	126.8	155.5	186.7	24.6%
Latin America	56.0	71.3	88.5	106.9	125.4	142.2	20.5%
Total	**1,044.6**	**1,316.6**	**1,620.3**	**1,947.6**	**2,281.0**	**2,588.7**	**19.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

9.3 SERVICES

9.3.1 AI-DRIVEN MANAGED SECURITY SERVICES ARE ENABLING ENTERPRISES TO SCALE SECURITY OPERATIONS WITHOUT EXPANDING INTERNAL SOC TEAMS

AI-powered services have become an essential component of the AI SOC market as organizations increasingly seek operational expertise alongside advanced security technologies. While software platforms provide the technological foundation for intelligent security operations, AI-driven services help enterprises operationalize these capabilities through continuous monitoring, threat investigation, incident response, and strategic cyber advisory. Rising cyberattack complexity, persistent cybersecurity workforce shortages, and the need for 24×7 security coverage are driving organizations to outsource critical security operations to specialized service providers. Vendors such as Arctic Wolf, Sophos, eSentire, Expel, Huntress, ReliaQuest, UnderDefense, CyberNX, RiverSafe, and Vulnuris are embedding generative AI, agentic AI, behavioral analytics, and automated workflows into managed services, enabling customers to achieve enterprise-grade security operations without building large in-house SOC teams. At the same time, government agencies continue to promote stronger cyber resilience and AI security practices, encouraging organizations to adopt managed security capabilities that align with evolving cybersecurity frameworks and secure AI guidance.

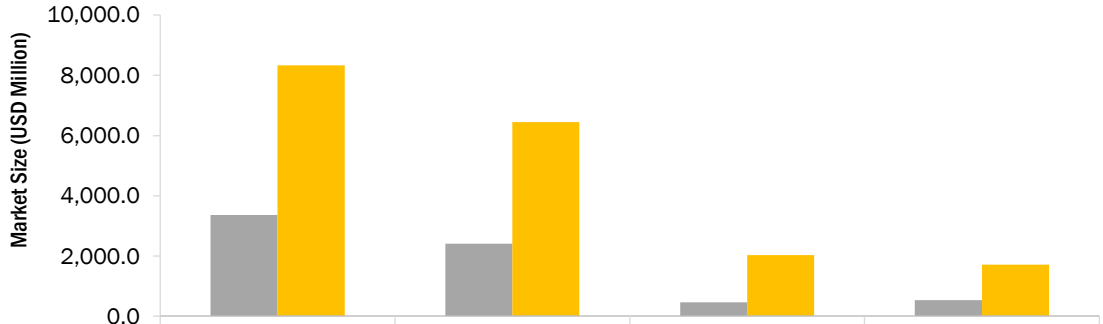
Among service offerings, AI-augmented managed detection and response (MDR) is experiencing significant adoption as organizations require continuous monitoring supported by both AI and human expertise. Modern MDR providers combine AI-driven detection, automated investigation, threat hunting, and analyst validation to identify sophisticated attacks while minimizing false positives. AI SOC-as-a-Service (SOCaaS) extends these capabilities further by delivering fully managed cloud-based security operations, including SIEM, SOAR, AI-powered analytics, continuous monitoring, compliance reporting, and automated response through subscription-based delivery models. This approach allows organizations, particularly SMEs and mid-sized enterprises, to rapidly deploy advanced security operations while reducing infrastructure investments, accelerating implementation, and improving operational scalability. Real-world adoption increasingly demonstrates that AI augments security analysts rather than replacing them, with AI performing repetitive investigations while experts retain decision authority for high-impact incidents.

The growing sophistication of ransomware, supply chain attacks, cloud compromises, and identity-based threats has also expanded demand for Incident Response and Forensics Services. AI is increasingly used to accelerate evidence collection, attack reconstruction, malware analysis, root-cause identification, and recovery planning, significantly reducing investigation timelines during active cyber incidents. Complementing these capabilities, Threat Intelligence and Advisory Services provide organizations with continuously updated intelligence on adversary tactics, emerging vulnerabilities, geopolitical cyber risks, and AI-enabled attack techniques. Leading providers combine global threat telemetry, proprietary research, and AI-assisted analytics to deliver actionable recommendations, proactive threat hunting, exposure assessments, and strategic guidance that strengthen enterprise cyber resilience and improve security decision-making across increasingly complex digital environments.

In the coming years, AI-driven security services are expected to evolve from traditional outsourced monitoring toward highly autonomous, intelligence-led security partnerships. Future service models will increasingly incorporate multi-agent AI systems capable of independently performing Tier-1 and Tier-2 investigations, continuously validating security controls, prioritizing organizational risks, and supporting compliance with emerging AI governance requirements. Human expertise will remain central for strategic decision-making, complex incident response, digital forensics, and executive cyber advisory. As enterprises continue adopting hybrid cloud, AI-enabled applications, operational technology, and distributed digital ecosystems, AI-powered services will become a strategic enabler for organizations seeking resilient, scalable, and continuously adaptive security operations without the operational burden of managing increasingly sophisticated SOC environments internally.

JULY 2026 © MarketsandMarkets™

FIGURE 34 AI SOC-AS-A-SERVICE (SOCAAS) SEGMENT TO GROW AT HIGHER CAGR DURING FORECAST PERIOD



	AI-augmented Managed Detection and Response (MDR)	Threat Intelligence and Advisory Services	AI SOC-as-a-Service (SOCaaS)	Incident Response and Forensics Services
2026	3,361.7	2,414.6	464.5	536.7
2031	8,327.2	6,447.1	2,029.5	1,709.8
CAGR (2026–2031)	19.9%	21.7%	34.3%	26.1%

Source: Expert Interviews and MarketsandMarkets Analysis

TABLE 46 AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Service	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented managed detection and response (MDR)	1,684.6	1,996.3	2,370.8	2,821.8	18.8%
AI SOC-as-a-Service (SOCaaS)	117.0	171.0	243.0	347.2	43.7%
Incident response and forensics services	217.3	272.0	340.8	428.3	25.4%
Threat intelligence and advisory services	1,139.7	1,370.4	1,651.8	1,982.8	20.3%
Total	**3,158.5**	**3,809.8**	**4,606.4**	**5,580.1**	**20.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 47 AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented managed detection and response (MDR)	3,361.7	4,015.4	4,807.4	5,766.7	6,927.7	8,327.2	19.9%
AI SOC-as-a-Service (SOCaaS)	464.5	622.3	834.9	1,121.6	1,508.5	2,029.5	34.3%
Incident response and forensics services	536.7	674.2	848.9	1,070.9	1,352.8	1,709.8	26.1%
Threat intelligence and advisory services	2,414.6	2,942.0	3,585.2	4,366.8	5,312.3	6,447.1	21.7%
Total	**6,777.5**	**8,253.9**	**10,076.4**	**12,326.0**	**15,101.2**	**18,513.6**	**22.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 48 AI SOC SERVICES MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	1,428.2	1,685.8	1,994.7	2,364.7	18.3%
Europe	806.6	964.0	1,154.7	1,385.9	19.8%
Asia Pacific	660.0	825.3	1,034.5	1,299.3	25.3%
Middle East & Africa	145.3	181.3	226.6	284.0	25.0%
Latin America	118.4	153.4	195.9	246.2	27.6%
Total	**3,158.5**	**3,809.8**	**4,606.4**	**5,580.1**	**20.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 49 AI SOC SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	2,810.6	3,349.7	4,001.7	4,790.4	5,743.2	6,890.2	19.6%
Europe	1,666.9	2,010.2	2,430.1	2,943.4	3,570.7	4,334.4	21.1%
Asia Pacific	1,636.2	2,065.9	2,614.9	3,316.6	4,213.1	5,355.5	26.8%
Middle East & Africa	355.0	445.0	559.1	703.9	887.6	1,120.0	25.8%
Latin America	308.8	383.1	470.5	571.7	686.6	813.4	21.4%
Total	**6,777.5**	**8,253.9**	**10,076.4**	**12,326.0**	**15,101.2**	**18,513.6**	**22.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

9.3.2 AI-AUGMENTED MANAGED DETECTION AND RESPONSE (MDR)

9.3.2.1 AI-augmented MDR services are enabling continuous threat defense through expert-led and AI-powered security operations

AI-augmented managed detection and response (MDR) services are redefining outsourced cybersecurity by combining human expertise with artificial intelligence to deliver continuous threat monitoring, investigation, and response across increasingly complex enterprise environments. Unlike traditional managed security services that primarily focus on alert monitoring, AI-augmented MDR providers leverage machine learning, behavioral analytics, large language models (LLMs), and automated investigation capabilities to identify sophisticated attacks, validate malicious activity, prioritize incidents, and rapidly contain threats before they escalate into business disruptions. The service model enables organizations to benefit from around-the-clock security operations without maintaining large in-house SOC teams, making it particularly valuable for enterprises facing cybersecurity talent shortages and expanding digital infrastructures. Leading providers including CrowdStrike (Falcon Complete Next-Gen MDR), Microsoft Defender Experts, Google Mandiant Managed Defense, Arctic Wolf, eSentire, Expel, Huntress, ReliaQuest, UnderDefense, Sophos, and Lumu Technologies continue enhancing MDR offerings with AI-assisted investigations, autonomous threat hunting, and proactive attack disruption capabilities. Recent platform innovations, including CrowdStrike's Charlotte AI integration into MDR workflows and eSentire's Atlas platform with expert AI, demonstrate how providers are embedding AI across managed security operations to improve both response quality and operational efficiency.

JULY 2026 © MarketsandMarkets™

The growing sophistication of ransomware, identity-based attacks, cloud compromises, and AI-enabled cyber threats is accelerating enterprise demand for MDR services capable of delivering expert-led security outcomes with AI-driven speed and scalability. Governments and cybersecurity agencies, including CISA, continue emphasizing continuous monitoring, rapid incident detection, and coordinated response as essential components of cyber resilience, encouraging organizations to strengthen operational security capabilities regardless of internal resource constraints. AI-augmented MDR services are therefore evolving beyond outsourced detection into proactive cyber resilience partnerships that combine continuous telemetry analysis, threat intelligence, automated containment, digital forensics, and strategic security guidance. In the coming years, AI is expected to automate much of the routine investigation and triage performed within MDR environments, allowing security experts to focus on advanced threat hunting, incident containment, and strategic cyber risk management while delivering highly adaptive, intelligence-driven protection across hybrid, multi-cloud, and AI-enabled enterprise infrastructures.

TABLE 50 AI-AUGMENTED MANAGED DETECTION AND RESPONSE (MDR) MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	761.6	883.0	1,025.9	1,194.6	16.2%
Europe	424.9	498.6	586.2	690.7	17.6%
Asia Pacific	355.9	437.4	538.7	665.1	23.2%
Middle East & Africa	78.3	96.1	118.0	145.4	22.9%
Latin America	63.9	81.3	102.0	126.0	25.4%
Total	**1,684.6**	**1,996.3**	**2,370.8**	**2,821.8**	**18.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 51 AI-AUGMENTED MANAGED DETECTION AND RESPONSE (MDR) MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,392.3	1,626.8	1,905.3	2,235.7	2,627.1	3,088.7	17.3%
Europe	814.5	962.8	1,140.7	1,353.7	1,608.8	1,912.7	18.6%
Asia Pacific	821.6	1,017.8	1,263.8	1,572.4	1,959.6	2,443.7	24.4%
Middle East & Africa	178.3	219.2	270.2	333.7	412.8	511.1	23.4%
Latin America	155.0	188.8	227.4	271.1	319.3	371.1	19.1%
Total	**3,361.7**	**4,015.4**	**4,807.4**	**5,766.7**	**6,927.7**	**8,327.2**	**19.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

9.3.3 AI SOC-AS-A-SERVICE (SOCAAS)

9.3.3.1 Cloud-delivered AI security operations are expanding access to enterprise-grade cyber defense

AI SOC-as-a-Service (SOCaaS) is transforming how organizations consume security operations by delivering fully managed, cloud-based SOC capabilities through a subscription model. Unlike AI-augmented MDR, which primarily focuses on managed threat detection and response, AI SOCaaS provides a comprehensive outsourced Security Operations Center that includes continuous monitoring, AI-driven alert triage, security analytics, investigation, incident response, detection engineering, threat hunting, reporting, and platform management without requiring organizations to build or operate an internal SOC. This delivery model enables enterprises to rapidly deploy advanced security operations while reducing infrastructure investments, operational complexity, and cybersecurity staffing requirements. Leading providers including Microsoft, Google, Cisco, Arctic Wolf, ReliaQuest, eSentire, Expel, Huntress, CyberNX, RiverSafe, Gruve, UnderDefense, and emerging AI-native vendors are increasingly integrating generative AI, autonomous investigations, AI SOC agents, and cloud-native analytics into SOCaaS offerings to improve service quality and response efficiency. The growing convergence of AI, XDR, SIEM, SOAR, and managed security services is enabling SOCaaS providers to deliver scalable security operations that continuously adapt to evolving enterprise environments while supporting organizations with diverse security maturity levels.

Growing adoption of hybrid work, multi-cloud infrastructure, SaaS applications, and AI-enabled business operations is accelerating demand for flexible security services that can scale alongside rapidly changing digital environments. Rather than functioning as outsourced monitoring centers, AI SOCaaS providers are evolving into strategic cybersecurity partners capable of delivering continuous cyber resilience through AI-assisted decision-making, expert analyst oversight, compliance reporting, and proactive risk reduction. Government guidance from agencies such as CISA continues emphasizing continuous security monitoring, ongoing risk assessments, and operational resilience for public and private sector organizations, reinforcing the value of externally managed security operations that align with recognized cybersecurity frameworks. Through 2031, AI SOCaaS is expected to become one of the fastest-growing service models within the AI SOC market as organizations increasingly prioritize operational flexibility, predictable security expenditures, faster deployment, and access to advanced AI-powered security capabilities without the cost and complexity of establishing dedicated in-house Security Operations Centers.

TABLE 52 AI SOC-AS-A-SERVICE (SOCAAS) MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	53.0	76.0	105.8	147.9	40.8%
Europe	35.1	49.2	67.5	92.8	38.3%
Asia Pacific	20.6	32.6	49.5	75.6	54.2%
Middle East & Africa	4.5	7.2	10.8	16.5	53.9%
Latin America	3.7	6.1	9.4	14.3	57.1%
Total	**117.0**	**171.0**	**243.0**	**347.2**	**43.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 53 AI SOC-AS-A-SERVICE (SOCAAS) MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	193.8	254.2	333.8	438.5	576.5	757.6	31.3%
Europe	122.3	161.0	212.0	279.1	367.4	483.3	31.6%
Asia Pacific	105.6	147.8	207.5	291.8	411.0	579.4	40.6%
Middle East & Africa	22.9	31.8	44.4	61.9	86.6	121.2	39.5%
Latin America	19.9	27.4	37.3	50.3	67.0	88.0	34.6%
Total	**464.5**	**622.3**	**834.9**	**1,121.6**	**1,508.5**	**2,029.5**	**34.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

9.3.4 INCIDENT RESPONSE AND FORENSICS SERVICES

9.3.4.1 AI-powered incident response and digital forensics are accelerating cyber recovery and operational resilience

Incident response and forensics services are evolving rapidly as organizations face increasingly sophisticated cyberattacks that demand faster investigation, evidence preservation, and coordinated recovery. Modern incident response extends well beyond breach containment, encompassing attack reconstruction, root-cause analysis, malware reverse engineering, cloud and endpoint forensics, identity compromise investigations, legal evidence collection, and post-incident remediation. Artificial intelligence is significantly enhancing these services by automating evidence correlation, attack timeline reconstruction, log analysis, malware classification, and hypothesis generation, enabling responders to investigate complex incidents with greater speed and accuracy. Leading providers including Microsoft Incident Response, Google Cloud Mandiant Incident Response, CrowdStrike Incident Response Services, Cisco Talos Incident Response, IBM X-Force Incident Response, Palo Alto Networks Unit 42, Secureworks, Expel, and UnderDefense are integrating AI-assisted investigation, behavioral analytics, and threat intelligence into forensic workflows to reduce attacker dwell time and accelerate recovery. Recent developments, including Microsoft's integration of AI-guided investigation capabilities into Defender XDR, Google's continued expansion of Mandiant's incident response portfolio, and CrowdStrike's AI-native forensic investigation capabilities, highlight the industry's transition toward intelligent, AI-assisted cyber response services.

As ransomware, cloud intrusions, supply-chain attacks, and AI-enabled cyber threats continue to increase in scale and complexity, organizations are prioritizing incident readiness alongside rapid post-breach recovery. Governments and cybersecurity agencies worldwide, including CISA and NIST, continue emphasizing incident preparedness, forensic readiness, and coordinated cyber response as essential components of organizational resilience, encouraging enterprises to establish mature incident response capabilities aligned with recognized cybersecurity frameworks. AI is consequently transforming digital forensics from a reactive investigative process into a continuously adaptive capability that supports proactive threat validation, automated evidence analysis, and accelerated remediation while maintaining evidentiary integrity. Through 2031, Incident Response and Forensics services are expected to increasingly leverage agentic AI, automated reasoning, cloud-native forensic analytics, and AI-assisted evidence reconstruction to deliver faster breach containment, improve legal and regulatory reporting, and strengthen enterprise cyber resilience against increasingly machine-speed attacks.

JULY 2026 © MarketsandMarkets™

TABLE 54 INCIDENT RESPONSE AND FORENSICS SERVICES MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	98.3	120.5	147.8	181.8	22.8%
Europe	57.1	70.7	87.6	108.9	24.0%
Asia Pacific	44.2	57.5	74.8	97.7	30.2%
Middle East & Africa	9.7	12.6	16.4	21.4	29.9%
Latin America	7.9	10.7	14.2	18.5	32.6%
Total	**217.3**	**272.0**	**340.8**	**428.3**	**25.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 55 INCIDENT RESPONSE AND FORENSICS SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	223.0	274.3	338.1	417.4	516.1	638.3	23.4%
Europe	135.1	167.9	209.2	261.0	326.0	407.4	24.7%
Asia Pacific	127.0	165.6	216.4	283.4	371.8	487.9	30.9%
Middle East & Africa	27.6	35.7	46.3	60.2	78.3	102.0	29.9%
Latin America	24.0	30.7	38.9	48.9	60.6	74.1	25.3%
Total	**536.7**	**674.2**	**848.9**	**1,070.9**	**1,352.8**	**1,709.8**	**26.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

9.3.5 THREAT INTELLIGENCE AND ADVISORY SERVICES

9.3.5.1 Intelligence-led cyber advisory services are strengthening proactive risk management in AI-enabled security operations

Threat intelligence and advisory services are evolving into strategic cybersecurity capabilities that help organizations anticipate emerging threats, strengthen cyber resilience, and make informed security decisions beyond day-to-day incident response. Unlike threat intelligence platforms that primarily deliver technology-driven intelligence feeds, these services combine expert-led threat analysis, adversary profiling, geopolitical risk assessment, vulnerability intelligence, cyber risk consulting, executive advisory, detection engineering guidance, and security maturity assessments tailored to an organization's business and threat landscape. Artificial intelligence is significantly enhancing these services by rapidly processing global threat data, identifying attack trends, mapping adversary tactics, and generating contextual intelligence that enables security teams to prioritize defensive actions based on business risk. Leading providers including Google Mandiant, Microsoft Defender Experts, Cisco Talos, CrowdStrike Services, Palo Alto Networks Unit 42, IBM X-Force, Rapid7, ReliaQuest, and eSentire continue integrating AI-assisted intelligence analysis with human expertise to deliver actionable strategic guidance, proactive threat hunting recommendations, executive reporting, and cyber resilience planning. Recent industry developments, including Microsoft's convergence of Defender Threat Intelligence into Microsoft Sentinel and Defender XDR, together with AI-powered threat intelligence enhancements across major security platforms, demonstrate the industry's shift toward embedding real-time intelligence directly into enterprise security operations.

JULY 2026 © MarketsandMarkets™

As cyber threats become increasingly driven by artificial intelligence, supply-chain attacks, geopolitical conflicts, and sophisticated ransomware campaigns, organizations require advisory services that extend beyond technical detection to support strategic cyber risk management. Governments and cybersecurity agencies, including CISA, NIST, and international cyber defense organizations, continue promoting threat intelligence sharing, continuous cyber risk assessment, and collaborative defense as essential pillars of national cyber resilience. AI is enabling advisory teams to analyze significantly larger volumes of threat intelligence, rapidly identify emerging attack campaigns, and deliver highly contextual recommendations that improve executive decision-making and long-term security planning. Through 2031, Threat Intelligence and Advisory Services are expected to evolve into continuous cyber risk advisory functions that combine AI-powered intelligence, industry-specific expertise, geopolitical awareness, and strategic consulting to help organizations proactively adapt security strategies, optimize AI SOC operations, and strengthen resilience against an increasingly dynamic global threat landscape.

TABLE 56 THREAT INTELLIGENCE AND ADVISORY SERVICES MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	515.3	606.4	715.2	840.4	17.7%
Europe	289.5	345.5	413.3	493.4	19.4%
Asia Pacific	239.3	297.8	371.5	460.9	24.4%
Middle East & Africa	52.7	65.4	81.4	100.7	24.1%
Latin America	42.9	55.3	70.3	87.3	26.7%
Total	**1,139.7**	**1,370.4**	**1,651.8**	**1,982.8**	**20.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 57 THREAT INTELLIGENCE AND ADVISORY SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,001.5	1,194.3	1,424.6	1,698.7	2,023.6	2,405.6	19.2%
Europe	595.0	718.5	868.2	1,049.6	1,268.5	1,531.1	20.8%
Asia Pacific	581.9	734.7	927.3	1,168.9	1,470.7	1,844.5	26.0%
Middle East & Africa	126.3	158.3	198.3	248.1	309.8	385.8	25.0%
Latin America	109.8	136.3	166.9	201.5	239.7	280.1	20.6%
Total	**2,414.6**	**2,942.0**	**3,585.2**	**4,366.8**	**5,312.3**	**6,447.1**	**21.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

10 AI SOC MARKET, BY ORGANIZATION SIZE

KEY FINDINGS

- Based on organization size, the large enterprises segment is estimated to account for the larger market of USD 12,187.7 million in 2026. It is projected to reach USD 29,498.4 million by 2031, growing at a CAGR of 19.3% during the forecast period.
- Increasing deployment of agentic AI, unified SecOps platforms, and AI-driven XDR, SIEM, and security data platforms by organizations across BFSI, healthcare, manufacturing, government, and telecommunications is accelerating AI SOC adoption among large enterprises seeking greater operational efficiency and cyber resilience.
- SMEs segment is projected to reach USD 17,567.8 million by 2031, growing from USD 5,913.6 million in 2026.
- The SMEs segment is expected to achieve the highest CAGR of 24.3% during the forecast period, driven by the growing availability of cloud-delivered AI SOC platforms, AI SOC-as-a-Service (SOCaaS), and AI-augmented MDR services that significantly reduce deployment costs and operational complexity.
- Growing accessibility of subscription-based AI security solutions, simplified deployment models, and managed AI SOC services is enabling SMEs to strengthen cybersecurity operations without building dedicated Security Operations Centers or expanding in-house security teams, supporting faster adoption across resource-constrained organizations.

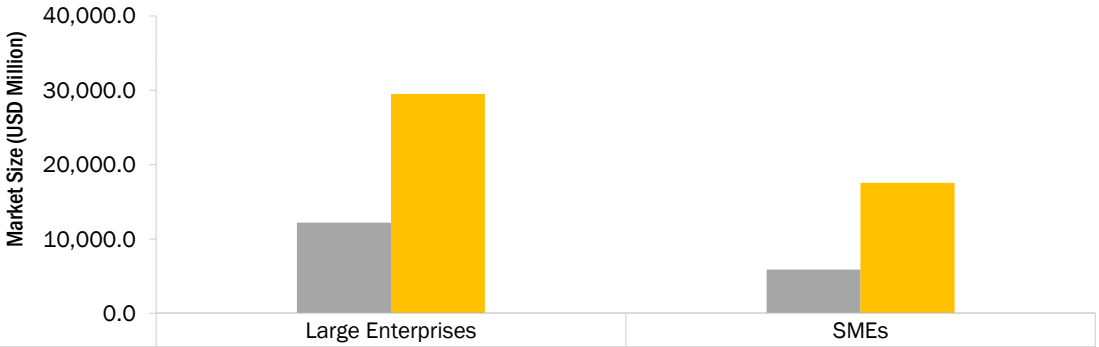
JULY 2026 © MarketsandMarkets™

10.1 INTRODUCTION

The AI SOC market, by organization size, is segmented into large enterprises and small & medium-sized enterprises (SMEs), both of which are increasingly adopting artificial intelligence to modernize security operations and strengthen cyber resilience. Large enterprises have emerged as the primary adopters of AI SOC solutions due to their extensive digital infrastructures, large-scale security operations, and ability to invest in advanced AI-native platforms, autonomous security agents, and managed security services. These organizations are integrating AI across Security Operations Centers to improve threat detection, automate investigations, optimize incident response, and secure increasingly complex hybrid cloud, multi-cloud, operational technology (OT), and AI-enabled environments. Vendors including Microsoft, Palo Alto Networks, Google, Cisco, CrowdStrike, IBM, Sophos, Fortinet, SentinelOne, and Elastic continue to expand enterprise-focused AI SOC capabilities through unified security platforms, autonomous AI agents, and cloud-native security operations.

SMEs are emerging as one of the fastest-growing customer segments as cloud-native AI SOC platforms, AI-Augmented MDR, and SOC-as-a-Service (SOCaaS) significantly reduce the cost and operational complexity of deploying enterprise-grade security operations. Instead of building dedicated in-house SOCs, SMEs increasingly rely on managed AI security services that combine continuous monitoring, AI-driven threat detection, automated investigations, and expert analyst oversight through subscription-based delivery models. Vendors such as Arctic Wolf, Huntress, eSentire, Expel, ReliaQuest, Sophos, CyberNX, RiverSafe, and Vulnuris are expanding AI-powered managed security offerings specifically to address SME requirements for affordability, rapid deployment, and operational simplicity. At the same time, government-led digital transformation initiatives, AI adoption programs, and cybersecurity resilience strategies are encouraging organizations of all sizes to strengthen cyber defenses through responsible AI adoption, further accelerating AI SOC implementation across both enterprise and SME segments.

FIGURE 35 LARGE ENTERPRISES SEGMENT TO ACCOUNT FOR LARGER MARKET DURING FORECAST PERIOD



	Large Enterprises	SMEs
2026	12,187.7	5,913.6
2031	29,498.4	17,567.8
CAGR (2026–2031)	19.3%	24.3%

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

10.1.1 ORGANIZATION SIZE: AI SOC MARKET DRIVERS

- Rapid expansion of hybrid workforces, multi-cloud infrastructures, and AI-enabled business applications is driving both large enterprises and SMEs to adopt AI SOC solutions that provide scalable, centralized, and intelligent security operations across distributed environments.
- Persistent shortages of skilled cybersecurity professionals are encouraging organizations of all sizes to invest in AI-powered security operations that automate alert triage, investigations, and incident response while allowing analysts to focus on high-priority threats.

JULY 2026 © MarketsandMarkets™

- Growing availability of cloud-native AI SOC platforms, AI-Augmented MDR, and SOC-as-a-Service offerings is reducing deployment costs and enabling SMEs to access enterprise-grade security capabilities without establishing dedicated in-house security operations centers.
- Large enterprises are accelerating investments in unified AI-native security platforms to consolidate fragmented security tools, improve operational efficiency, and strengthen cyber resilience across global, highly regulated, and increasingly complex digital ecosystems.
- Increasing ransomware attacks, AI-assisted cyber threats, and identity-centric attacks are compelling organizations of every size to adopt AI SOC capabilities that deliver faster threat detection, automated investigations, and continuous security monitoring while improving overall operational resilience.
- Large enterprises are accelerating AI SOC adoption to secure geographically distributed operations, complex hybrid IT-OT environments, and global compliance requirements through centralized, AI-driven security operations and standardized governance across business units.
- Increasing availability of subscription-based AI SOC platforms and consumption-based pricing models is enabling SMEs to deploy enterprise-grade security operations with lower upfront investments, faster implementation, and greater operational flexibility.

TABLE 58 AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	6,254.6	7,364.6	8,692.9	10,279.5	18.0%
SMEs	2,523.6	3,118.4	3,856.6	4,772.4	23.7%
Total	**8,778.2**	**10,483.1**	**12,549.5**	**15,051.9**	**19.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 59 AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	12,187.7	14,488.6	17,265.2	20,615.0	24,651.9	29,498.4	19.3%
SMEs	5,913.6	7,338.7	9,119.4	11,343.6	14,118.4	17,567.8	24.3%
Total	**18,101.3**	**21,827.3**	**26,384.6**	**31,958.6**	**38,770.3**	**47,066.1**	**21.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

10.2 LARGE ENTERPRISES

10.2.1 COMPLEX DIGITAL ECOSYSTEMS AND LARGE-SCALE SECURITY OPERATIONS ARE ACCELERATING AI SOC ADOPTION ACROSS LARGE ENTERPRISES

Large enterprises account for the largest share of the AI SOC market due to their expansive digital infrastructures, geographically distributed operations, and growing exposure to sophisticated cyber threats targeting cloud environments, operational technology (OT), supply chains, and AI-enabled business applications. These organizations generate massive volumes of security telemetry from endpoints, networks, identities, cloud workloads, SaaS platforms, and connected assets, making manual security operations increasingly unsustainable. Consequently, enterprises are investing in AI-native Security Operations Centers that combine machine learning, generative AI, agentic AI, behavioral analytics, and automation to continuously detect, prioritize, investigate, and respond to threats across highly complex environments. Leading vendors including Microsoft, Palo Alto Networks, Cisco, CrowdStrike, Google, IBM, Sophos, SentinelOne, and Elastic are expanding enterprise-focused AI SOC platforms with autonomous security agents, unified security operations, and integrated AI governance capabilities to address these evolving operational requirements.

The rapid evolution of enterprise AI adoption is further strengthening demand for AI SOC solutions. As organizations deploy generative AI, autonomous AI agents, and AI-powered business workflows across finance, manufacturing, healthcare, telecommunications, retail, and government operations, security teams must simultaneously secure both traditional IT assets and emerging AI ecosystems. Modern AI SOC platforms are therefore evolving beyond conventional SIEM and SOAR architectures by integrating identity protection, cloud security, exposure management, threat intelligence, AI workload monitoring, and automated response into unified operational environments. Large enterprises are increasingly adopting phased AI maturity strategies that begin with analyst augmentation and progressively advance toward supervised autonomous security operations, enabling security teams to improve operational efficiency while maintaining governance and human oversight.

Enterprise cybersecurity strategies are also being shaped by increasingly stringent regulatory and governance requirements surrounding artificial intelligence, critical infrastructure protection, data privacy, and cyber resilience. Organizations operating across multiple jurisdictions must comply with evolving frameworks while maintaining consistent security visibility across global business units. AI SOC platforms support these objectives by centralizing security operations, standardizing investigation workflows, automating compliance reporting, and improving audit readiness through policy-driven security orchestration. Simultaneously, many multinational enterprises are consolidating fragmented security technologies into unified AI-native platforms to simplify operations, reduce total cost of ownership, and improve security effectiveness. This platform consolidation trend is becoming a strategic priority as enterprises seek greater operational resilience while securing rapidly expanding digital ecosystems.

As enterprises continue their cybersecurity transformation, large enterprises are expected to remain the primary adopters of advanced AI SOC capabilities as security operations evolve toward intelligent, collaborative human-AI operating models. Future enterprise deployments will increasingly leverage multi-agent AI systems capable of autonomously conducting investigations, validating attack hypotheses, orchestrating remediation workflows, and continuously optimizing security operations across hybrid and multi-cloud environments. Rather than replacing experienced analysts, these platforms will enable security teams to manage significantly larger attack surfaces with improved speed, consistency, and operational scalability, positioning AI SOC as a core component of enterprise cyber resilience strategies throughout the forecast period.

JULY 2026 © MarketsandMarkets™

TABLE 60 AI SOC MARKET FOR LARGE ENTERPRISES, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	2,828.2	3,259.0	3,764.5	4,356.3	15.5%
Europe	1,598.9	1,865.1	2,180.7	2,554.6	16.9%
Asia Pacific	1,305.8	1,594.2	1,951.1	2,392.4	22.4%
Middle East & Africa	287.4	350.2	427.3	522.9	22.1%
Latin America	234.3	296.2	369.4	453.3	24.6%
Total	**6,254.6**	**7,364.6**	**8,692.9**	**10,279.5**	**18.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 61 AI SOC MARKET FOR LARGE ENTERPRISES, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	5,054.5	5,879.9	6,856.6	8,011.3	9,374.3	10,976.0	16.8%
Europe	2,998.6	3,529.1	4,163.1	4,920.5	5,824.1	6,897.7	18.1%
Asia Pacific	2,941.4	3,626.1	4,481.1	5,549.0	6,882.0	8,541.2	23.8%
Middle East & Africa	638.2	781.0	958.1	1,177.7	1,449.9	1,786.3	22.9%
Latin America	555.1	672.5	806.4	956.6	1,121.6	1,297.2	18.5%
Total	**12,187.7**	**14,488.6**	**17,265.2**	**20,615.0**	**24,651.9**	**29,498.4**	**19.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

10.3 SMES

10.3.1 CLOUD-NATIVE AI SOC SERVICES ARE ENABLING SMES TO ACCESS ENTERPRISE-GRADE CYBERSECURITY CAPABILITIES

Small and medium-sized enterprises (SMEs) are emerging as one of the fastest-growing customer segments within the AI SOC market as cyber threats increasingly target resource-constrained organizations with limited security personnel and budgets. Unlike large enterprises that often operate dedicated Security Operations Centers, SMEs typically rely on lean IT teams that must simultaneously manage infrastructure, compliance, and cybersecurity responsibilities. This operational reality is accelerating demand for AI-powered security operations that automate repetitive SOC activities while minimizing deployment complexity. Cloud-native AI SOC platforms, AI-augmented managed detection and response (MDR), and AI SOC-as-a-Service (SOCaaS) have significantly lowered adoption barriers by allowing SMEs to consume enterprise-grade security capabilities through subscription-based models rather than investing in expensive infrastructure or specialized security teams. Vendors such as Sophos, Huntress, Arctic Wolf, eSentire, Expel, CyberNX, RiverSafe, and Vulnuris are increasingly tailoring AI-driven managed security offerings specifically for small and mid-sized organizations seeking continuous protection with predictable operational costs.

SMEs are increasingly prioritizing AI SOC investments as ransomware groups, identity-based attacks, phishing campaigns, and supply-chain compromises continue to target organizations that often lack mature security operations. Modern AI SOC solutions enable smaller businesses to automate alert prioritization, investigation, threat correlation, and guided incident response without requiring deep cybersecurity expertise; rather than replacing security personnel, artificial intelligence functions as a force

JULY 2026 © MarketsandMarkets™

multiplier by reducing false positives, accelerating investigations, and enabling limited security staff to focus on higher-priority risks. This combination of automation and expert oversight allows SMEs to improve cyber resilience while maintaining operational agility and supporting ongoing digital transformation initiatives, including cloud migration and AI adoption.

Government initiatives promoting SME digitalization and cybersecurity resilience are also supporting broader adoption of AI-enabled security operations. Organizations such as the OECD and national AI programs are encouraging small businesses to adopt secure AI technologies while addressing persistent barriers related to cybersecurity skills, implementation costs, and operational maturity. At the same time, evolving cybersecurity guidance from standards bodies is encouraging organizations to embed secure operational practices and AI governance into everyday business processes. These developments are creating a favorable environment for managed AI SOC offerings that combine continuous monitoring, compliance support, threat intelligence, and automated security operations without imposing significant administrative or technical burdens on SMEs.

Over the forecast period, SMEs are expected to represent the fastest-growing organization-size segment as AI SOC solutions become increasingly modular, affordable, and consumption-based. Future offerings will continue incorporating autonomous AI agents, natural-language security assistants, predictive threat analytics, and managed AI operations designed specifically for organizations with limited internal cybersecurity resources. As AI-native security platforms mature and managed service providers expand their AI capabilities, SMEs will be able to achieve security outcomes previously attainable only by large enterprises, enabling them to strengthen cyber resilience, satisfy regulatory expectations, and confidently support increasingly digital business operations.

TABLE 62 AI SOC MARKET FOR SMES, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	1,141.9	1,382.1	1,674.1	2,029.0	21.1%
Europe	676.3	827.2	1,012.4	1,240.4	22.4%
Asia Pacific	504.0	646.9	830.8	1,067.4	28.4%
Middle East & Africa	110.9	142.1	181.9	233.3	28.1%
Latin America	90.4	120.2	157.3	202.2	30.8%
Total	**2,523.6**	**3,118.4**	**3,856.6**	**4,772.4**	**23.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 63 AI SOC MARKET FOR SMES, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	2,462.4	2,992.7	3,642.2	4,436.9	5,408.3	6,590.8	21.8%
Europe	1,521.1	1,868.4	2,298.4	2,830.6	3,488.3	4,298.2	23.1%
Asia Pacific	1,373.1	1,768.6	2,280.8	2,943.9	3,801.4	4,907.2	29.0%
Middle East & Africa	297.9	380.9	487.6	624.8	800.9	1,026.3	28.1%
Latin America	259.1	328.0	410.4	507.5	619.5	745.3	23.5%
Total	**5,913.6**	**7,338.7**	**9,119.4**	**11,343.6**	**14,118.4**	**17,567.8**	**24.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

11 AI SOC MARKET, BY APPLICATION

KEY FINDINGS

- Threat detection and monitoring segment is estimated to account for the largest market size of USD 4,176.0 million in 2026, reaching USD 9,350.4 million in 2031, at a CAGR of 17.5% during the forecast period.
- This growth is driven by organizations' need for continuous visibility across hybrid, multi-cloud, identity-centric, and AI-enabled environments to identify sophisticated cyber threats before they disrupt business operations.
- Compliance monitoring and reporting is expected to register the highest CAGR of 26.5% during the forecast period.
- This fast growth is due to expanding cybersecurity regulations, AI governance frameworks, and continuous compliance requirements that require organizations to automate evidence collection, policy validation, and audit reporting across enterprise environments.
- Alert triage and prioritization is projected to be the second-largest application with a market size of USD 2,635.6 million in 2026, as enterprises increasingly deploy AI to reduce alert fatigue, prioritize high-risk incidents based on business context, and improve SOC analyst productivity amid rapidly growing security event volumes.

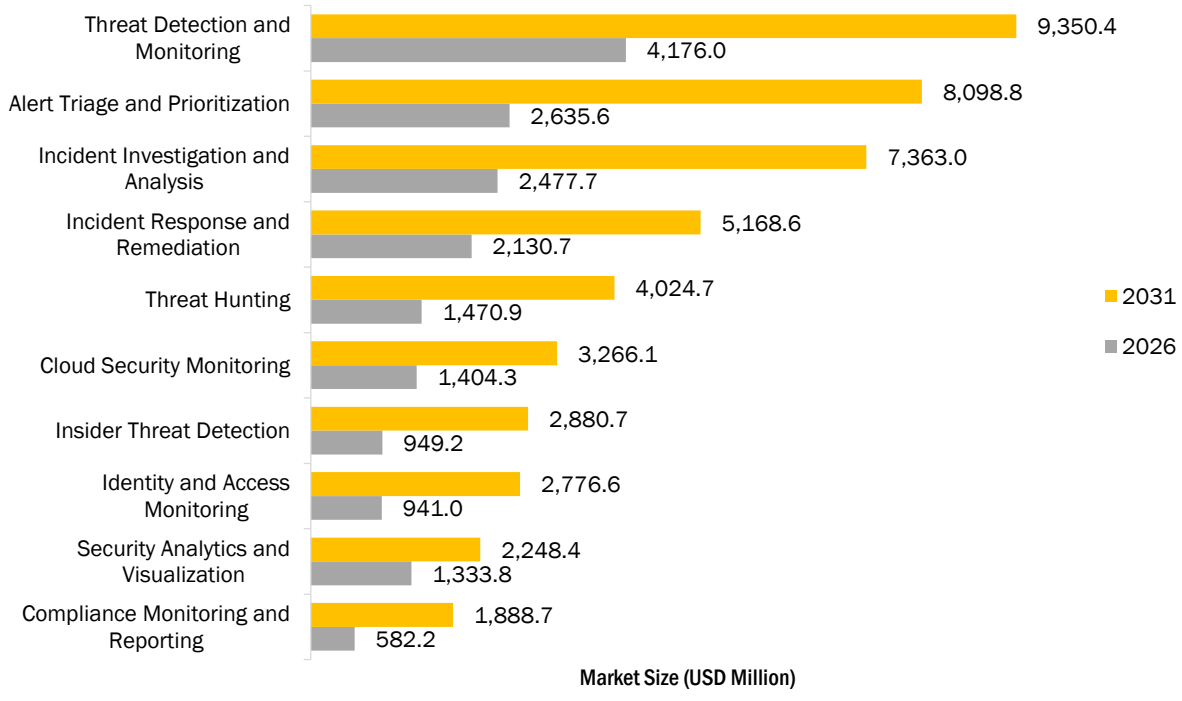
JULY 2026 © MarketsandMarkets™

11.1 INTRODUCTION

The AI SOC market, by application, encompasses a broad range of security operations use cases where artificial intelligence enhances the speed, accuracy, and efficiency of cyber defense. These applications span the complete incident lifecycle from threat detection and monitoring, alert triage and prioritization, incident investigation and analysis, and threat hunting to incident response and remediation, insider threat detection, cloud security monitoring, identity and access monitoring, compliance monitoring and reporting, and security analytics and visualization. As enterprises continue expanding hybrid cloud infrastructures, AI-enabled business applications, and distributed workforces, AI is increasingly embedded across every stage of security operations to reduce manual workloads, improve decision-making, and accelerate response to sophisticated cyber threats. Vendors including Microsoft, Google, Palo Alto Networks, Cisco, CrowdStrike, SentinelOne, Sophos, IBM, Elastic, Exabeam, ReliaQuest, and emerging AI SOC providers are continuously extending AI capabilities across these operational workflows through generative AI, agentic AI, behavioral analytics, and autonomous reasoning engines.

The evolution of AI SOC applications reflects the industry's transition from isolated automation toward intelligent, end-to-end security operations. Rather than supporting only individual security tasks, modern AI platforms correlate telemetry from endpoints, networks, cloud environments, identities, applications, and threat intelligence sources to deliver contextual, risk-driven insights across the entire security lifecycle. At the same time, regulatory emphasis on trustworthy AI, continuous monitoring, cyber resilience, and secure AI deployment is encouraging organizations to adopt AI SOC applications that combine operational automation with governance, explainability, and human oversight. As AI capabilities continue to mature, organizations are increasingly deploying application-specific AI across detection engineering, investigation, cloud security, identity protection, compliance monitoring, and security analytics, enabling Security Operations Centers to become more proactive, adaptive, and resilient against evolving cyber threats throughout the forecast period.

FIGURE 36 THREAT DETECTION AND MONITORING SEGMENT TO ACCOUNT FOR LARGEST MARKET BY 2031



Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

11.1.1 APPLICATION: AI SOC MARKET DRIVERS

- Escalating volumes of sophisticated cyberattacks are driving organizations to deploy AI across threat detection, investigation, hunting, and response workflows to identify malicious activity earlier and reduce attacker dwell time.
- Growing alert fatigue and increasing false-positive rates are accelerating adoption of AI-powered alert triage and prioritization applications that intelligently correlate events, suppress benign alerts, and enable analysts to focus on high-risk incidents.
- Rapid migration to hybrid cloud, multi-cloud, SaaS, and containerized environments is fueling demand for AI-driven cloud security monitoring applications capable of continuously analyzing distributed workloads, identities, and cloud-native attack paths from a unified operational view.
- The rapid expansion of digital identities, machine identities, privileged accounts, and AI agents is increasing the need for intelligent identity and access monitoring applications that continuously detect anomalous authentication behavior, privilege misuse, and identity-based attacks.
- Increasing regulatory expectations for continuous security validation, audit readiness, and responsible AI governance are driving adoption of AI-enabled compliance monitoring and reporting applications that automate evidence collection, policy validation, and security documentation.
- Organizations are increasingly adopting AI-powered security analytics and visualization applications to transform large volumes of heterogeneous security telemetry into contextual, risk-based insights that improve executive decision-making and SOC situational awareness.
- Growing enterprise adoption of AI-assisted investigation, autonomous threat hunting, and guided incident response is expanding the use of application-specific AI capabilities that automate repetitive analyst tasks while maintaining human oversight for high-impact security decisions.

TABLE 64 AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	2,252.6	2,623.3	3,057.6	3,575.9	16.7%
Alert Triage and Prioritization	1,094.2	1,362.6	1,695.6	2,118.0	24.6%
Incident Investigation and Analysis	1,065.4	1,313.5	1,620.3	2,005.0	23.5%
Threat Hunting	683.6	825.3	998.5	1,210.6	21.0%
Incident Response and Remediation	1,089.0	1,283.9	1,517.0	1,796.3	18.2%
Insider Threat Detection	399.4	495.4	614.4	764.8	24.2%
Cloud Security Monitoring	739.0	865.4	1,015.0	1,193.7	17.3%
Identity and Access Monitoring	407.5	501.4	617.4	762.6	23.2%
Compliance Monitoring and Reporting	227.2	288.1	364.1	462.5	26.7%
Security Analytics and Visualization	820.4	924.1	1,049.6	1,162.6	12.3%
Total	**8,778.2**	**10,483.1**	**12,549.5**	**15,051.9**	**19.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 65 AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	4,176.0	4,889.2	5,737.1	6,744.4	7,939.3	9,350.4	17.5%
Alert Triage and Prioritization	2,635.6	3,287.5	4,109.8	5,147.1	6,454.8	8,098.8	25.2%
Incident Investigation and Analysis	2,477.7	3,069.5	3,811.4	4,741.5	5,907.0	7,363.0	24.3%
Threat Hunting	1,470.9	1,792.0	2,188.3	2,677.8	3,281.8	4,024.7	22.3%
Incident Response and Remediation	2,130.7	2,534.0	3,021.0	3,608.8	4,317.5	5,168.6	19.4%
Insider Threat Detection	949.2	1,181.0	1,472.7	1,839.8	2,301.6	2,880.7	24.9%
Cloud Security Monitoring	1,404.3	1,656.3	1,958.2	2,319.6	2,751.7	3,266.1	18.4%
Identity and Access Monitoring	941.0	1,164.0	1,443.3	1,793.0	2,230.6	2,776.6	24.2%
Compliance Monitoring and Reporting	582.2	734.4	928.2	1,175.1	1,489.5	1,888.7	26.5%
Security Analytics and Visualization	1,333.8	1,519.3	1,714.6	1,911.4	2,096.5	2,248.4	11.0%
Total	**18,101.3**	**21,827.3**	**26,384.6**	**31,958.6**	**38,770.3**	**47,066.1**	**21.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

11.2 THREAT DETECTION AND MONITORING

11.2.1 SHIFT FROM ALERT-CENTRIC SECURITY TO CONTINUOUS RISK OBSERVABILITY IS ACCELERATING AI-DRIVEN THREAT DETECTION

Threat detection is rapidly evolving from identifying isolated security events to continuously understanding organizational risk across interconnected digital environments. Modern enterprises no longer operate within clearly defined network perimeters; instead, users, applications, cloud workloads, identities, APIs, SaaS platforms, and AI agents continuously generate security-relevant activity that changes every second. As attack campaigns increasingly unfold across multiple stages rather than through a single malicious event, organizations require persistent monitoring capable of recognizing subtle behavioral shifts before business disruption occurs. Consequently, enterprises are prioritizing AI SOC capabilities that maintain continuous operational visibility rather than depending on periodic alert reviews. This evolution is particularly evident across highly regulated sectors such as financial services, healthcare, manufacturing, and government, where uninterrupted monitoring has become central to cyber resilience strategies. Recent enhancements across Microsoft Security Copilot, Google Security Operations, CrowdStrike Falcon, Cisco XDR, and Palo Alto Networks Cortex demonstrate how vendors are redesigning security monitoring around continuous operational awareness instead of isolated event management.

The application is also expanding because enterprise leadership increasingly views continuous threat monitoring as an operational resilience function rather than purely a cybersecurity capability. Executive teams require real-time visibility into cyber risk that supports business continuity, regulatory reporting, and protection of AI-enabled operations. Recent guidance from NIST on continuous monitoring of deployed AI systems further reinforces that security monitoring must evolve alongside rapidly changing AI environments instead of relying on static security controls. As organizations deploy autonomous AI agents, machine identities, and highly distributed digital infrastructures, threat detection is expected to become a continuously adaptive operational discipline that provides business-wide cyber situational awareness. Looking ahead, AI SOC deployments will increasingly measure success through continuous risk visibility, earlier attack discovery, and operational resilience rather than simply increasing the number of alerts detected.

JULY 2026 © MarketsandMarkets™

TABLE 66 AI SOC MARKET FOR THREAT DETECTION AND MONITORING, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	1,018.6	1,160.9	1,324.1	1,515.4	14.2%
Europe	576.6	665.3	767.5	888.6	15.5%
Asia Pacific	469.7	567.1	685.9	832.2	21.0%
Middle East & Africa	103.4	124.6	150.2	181.9	20.7%
Latin America	84.3	105.4	129.9	157.7	23.2%
Total	**2,252.6**	**2,623.3**	**3,057.6**	**3,575.9**	**16.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 67 AI SOC MARKET FOR THREAT DETECTION AND MONITORING, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,731.9	1,984.3	2,278.5	2,621.0	3,018.8	3,478.4	15.0%
Europe	1,027.7	1,191.3	1,383.7	1,609.7	1,874.6	2,183.6	16.3%
Asia Pacific	1,007.6	1,223.3	1,488.7	1,815.5	2,217.4	2,710.1	21.9%
Middle East & Africa	218.6	263.5	318.3	385.3	467.2	566.8	21.0%
Latin America	190.1	226.9	267.9	313.0	361.4	411.6	16.7%
Total	**4,176.0**	**4,889.2**	**5,737.1**	**6,744.4**	**7,939.3**	**9,350.4**	**17.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

11.3 ALERT TRIAGE AND PRIORITIZATION

11.3.1 BUSINESS-CONTEXT–DRIVEN ALERT PRIORITIZATION IS IMPROVING SOC DECISION QUALITY AND REDUCING ANALYST FATIGUE

Alert triage and prioritization have become one of the most critical operational applications within AI-powered Security Operations Centers as enterprises struggle to distinguish genuine cyber threats from the overwhelming volume of routine security notifications. Modern SOCs generate thousands of alerts every day from endpoint, cloud, identity, email, network, and application security tools, yet only a small proportion require immediate analyst intervention. The challenge is no longer detecting security events—it is determining which events present the greatest operational or business risk. Consequently, organizations are increasingly deploying AI SOC capabilities that evaluate alerts in the context of asset criticality, user behavior, attack progression, business impact, and historical incident patterns rather than relying solely on predefined severity scores. This shift enables security teams to allocate analyst attention where it delivers the highest value, reducing investigation delays while improving operational efficiency. Recent developments such as Microsoft's Security Alert Triage Agent and Phishing Triage Agent, together with agentic capabilities introduced by leading AI SOC vendors, demonstrate how intelligent prioritization is becoming a fundamental component of modern security operations rather than a supplementary automation feature.

JULY 2026 © MarketsandMarkets™

The application is also evolving because organizations increasingly measure SOC performance by investigation quality and response effectiveness rather than the number of alerts processed. Executive leadership expects security teams to rapidly identify incidents capable of disrupting critical business operations, regulatory compliance, or customer trust, making intelligent prioritization a strategic business capability. Recent academic research and enterprise deployments demonstrate that adaptive AI-based prioritization significantly improves analyst productivity by continuously ranking incidents according to changing organizational risk instead of static alert queues. Simultaneously, AI-driven prioritization supports analyst wellbeing by mitigating alert fatigue, one of the most persistent operational challenges facing modern SOCs. Alert triage is expected to transition from rule-based queue management toward continuously adaptive risk orchestration, where AI dynamically reprioritizes investigations based on evolving threats, business context, and real-time operational impact, enabling SOCs to operate with significantly greater precision and resilience.

TABLE 68 AI SOC MARKET FOR ALERT TRIAGE AND PRIORITIZATION, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	495.0	603.7	735.6	899.7	22.0%
Europe	289.5	357.3	439.9	543.9	23.4%
Asia Pacific	221.3	285.8	369.3	479.0	29.4%
Middle East & Africa	48.7	62.8	80.9	104.7	29.1%
Latin America	39.7	53.1	69.9	90.7	31.7%
Total	**1,094.2**	**1,362.6**	**1,695.6**	**2,118.0**	**24.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 69 AI SOC MARKET FOR ALERT TRIAGE AND PRIORITIZATION, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,096.3	1,339.1	1,639.2	2,010.1	2,468.0	3,031.6	22.6%
Europe	670.5	828.3	1,025.2	1,270.9	1,577.2	1,957.6	23.9%
Asia Pacific	618.0	799.6	1,037.0	1,347.7	1,754.1	2,284.8	29.9%
Middle East & Africa	134.1	172.2	221.7	286.0	369.6	477.8	28.9%
Latin America	116.6	148.3	186.6	232.3	285.9	347.0	24.4%
Total	**2,635.6**	**3,287.5**	**4,109.8**	**5,147.1**	**6,454.8**	**8,098.8**	**25.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

11.4 INCIDENT INVESTIGATION AND ANALYSIS

11.4.1 AI-ASSISTED INVESTIGATIONS ARE SHIFTING SECURITY OPERATIONS FROM EVIDENCE COLLECTION TO RAPID DECISION-MAKING

Incident investigation and analysis has become a high-value application of AI SOC as security teams increasingly prioritize understanding the complete scope, origin, and business impact of an attack rather than simply confirming whether an alert is malicious. Modern cyber incidents frequently span multiple environments including cloud workloads, endpoints, identities, collaboration platforms, SaaS applications, and AI systems, making manual investigation both time-consuming and operationally expensive. Consequently, organizations are adopting AI SOC capabilities that rapidly reconstruct attack narratives, correlate related activities, identify affected assets, and generate contextual insights that enable analysts to reach informed decisions significantly faster. Instead of spending valuable time gathering evidence from multiple consoles, investigators can concentrate on validating attack intent, assessing organizational exposure, and determining the most effective containment strategy. This transition is reflected in recent vendor innovations such as Microsoft Purview Data Security Investigations, Google's Mandiant AI-assisted investigation capabilities, and expanding investigation workflows across Microsoft Security Copilot and enterprise AI SOC platforms, where AI assists analysts by organizing complex evidence into actionable investigative findings.

Incident investigation and analysis is also becoming increasingly important as organizations seek to reduce incident resolution time while improving the quality and consistency of investigative outcomes. Executive leadership, regulators, legal teams, and cyber insurance providers increasingly expect organizations to produce well-documented incident assessments that clearly explain attack progression, affected business processes, and remediation actions. AI-assisted investigation supports these objectives by enabling faster evidence review, structured incident documentation, and more comprehensive post-incident analysis without compromising investigative rigor. As adversaries increasingly operationalize AI to accelerate attacks, security teams are similarly leveraging AI to strengthen analytical reasoning and improve investigative accuracy. Going forward, incident investigation and analysis is expected to evolve into an intelligence-driven application where AI continuously develops investigative hypotheses, reconstructs complex attack chains, and delivers contextual recommendations that enable security professionals to focus on strategic judgment, business risk evaluation, and coordinated cyber response rather than manual evidence processing.

TABLE 70 AI SOC MARKET FOR INCIDENT INVESTIGATION AND ANALYSIS, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	481.9	581.8	702.7	851.5	20.9%
Europe	280.5	342.7	418.5	512.9	22.3%
Asia Pacific	216.5	276.7	354.3	455.0	28.1%
Middle East & Africa	47.6	60.8	77.6	99.5	27.8%
Latin America	38.8	51.4	67.1	86.2	30.4%
Total	**1,065.4**	**1,313.5**	**1,620.3**	**2,005.0**	**23.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 71 AI SOC MARKET FOR INCIDENT INVESTIGATION AND ANALYSIS, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,030.3	1,249.8	1,519.4	1,850.7	2,257.4	2,754.7	21.7%
Europe	627.8	770.3	947.2	1,166.6	1,438.6	1,774.6	23.1%
Asia Pacific	583.1	749.1	964.9	1,245.2	1,609.6	2,082.0	29.0%
Middle East & Africa	126.5	161.3	206.3	264.3	339.1	435.4	28.0%
Latin America	110.0	138.9	173.6	214.7	262.3	316.2	23.5%
Total	**2,477.7**	**3,069.5**	**3,811.4**	**4,741.5**	**5,907.0**	**7,363.0**	**24.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

11.5 THREAT HUNTING

11.5.1 PROACTIVE ADVERSARY HUNTING IS SHIFTING SECURITY OPERATIONS FROM REACTIVE DEFENSE TO CONTINUOUS CYBER RESILIENCE

Threat hunting has emerged as one of the fastest-evolving applications within AI SOC as organizations recognize that sophisticated adversaries increasingly evade traditional security controls and remain undetected for extended periods. Rather than waiting for security alerts to trigger investigations, threat hunting enables security teams to proactively search enterprise environments for hidden attacker activity, lateral movement, credential abuse, persistence mechanisms, and early indicators of compromise before operational disruption occurs. As cybercriminals increasingly leverage artificial intelligence, malware-free techniques, and identity-centric attacks, organizations are integrating AI into hunting workflows to generate investigative hypotheses, identify abnormal attack patterns, correlate weak signals across diverse data sources, and accelerate analyst decision-making. Vendors including Microsoft, CrowdStrike, Google, Palo Alto Networks, Cisco, SentinelOne, and Intezer continue enhancing AI-assisted hunting capabilities through natural language search, AI-guided query generation, automated evidence discovery, and contextual threat exploration. Recent innovations such as Microsoft Security Copilot Threat Hunting Agent and CrowdStrike's AI-powered Counter Adversary Operations demonstrate how AI is transforming threat hunting into a continuously adaptive capability that augments analyst expertise rather than replacing it.

The business value of threat hunting is increasingly measured by an organization's ability to identify attacker activity before conventional detection mechanisms generate high-confidence alerts. Security leaders are therefore expanding dedicated hunting programs to strengthen cyber resilience, improve detection engineering, validate defensive controls, and uncover emerging attack techniques targeting cloud infrastructure, AI workloads, operational technology, and machine identities. Enterprise security strategies are also becoming increasingly intelligence-led, where threat hunting directly influences incident response planning, detection rule development, and long-term security architecture improvements. As organizations adopt autonomous AI agents and increasingly dynamic digital ecosystems, proactive hunting is evolving into a continuous operational discipline rather than a periodic security exercise. Over the coming years, AI-powered threat hunting is expected to become an always-on capability that continuously formulates investigative hypotheses, validates adversary behaviors, and uncovers previously unknown attack paths, enabling organizations to identify and disrupt sophisticated threats well before they develop into large-scale security incidents.

JULY 2026 © MarketsandMarkets™

TABLE 72 AI SOC MARKET FOR THREAT HUNTING, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	309.2	365.4	432.8	513.8	18.4%
Europe	178.1	213.1	255.4	306.9	19.9%
Asia Pacific	140.2	175.6	220.3	277.0	25.5%
Middle East & Africa	30.9	38.6	48.2	60.5	25.2%
Latin America	25.2	32.6	41.7	52.5	27.8%
Total	**683.6**	**825.3**	**998.5**	**1,210.6**	**21.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 73 AI SOC MARKET FOR THREAT HUNTING, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	611.1	728.9	871.4	1,043.9	1,252.4	1,503.6	19.7%
Europe	369.3	445.5	538.9	653.0	792.6	962.5	21.1%
Asia Pacific	349.0	440.8	558.3	708.4	900.4	1,145.1	26.8%
Middle East & Africa	75.7	95.0	119.4	150.4	189.7	239.5	25.9%
Latin America	65.9	81.8	100.5	122.1	146.7	173.9	21.4%
Total	**1,470.9**	**1,792.0**	**2,188.3**	**2,677.8**	**3,281.8**	**4,024.7**	**22.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

11.6 INCIDENT RESPONSE AND REMEDIATION

11.6.1 RAPID BUSINESS RECOVERY IS DRIVING AI-ENABLED INCIDENT RESPONSE AND REMEDIATION CAPABILITIES

Incident response and remediation has evolved into a business continuity function, where the primary objective extends beyond stopping an attack to restoring normal operations with minimal disruption. As enterprises increasingly depend on cloud-native applications, digital services, AI workloads, and interconnected business processes, prolonged cyber incidents can directly affect revenue generation, customer trust, regulatory compliance, and operational resilience. Consequently, organizations are adopting AI SOC capabilities that accelerate decision-making during active incidents by recommending containment strategies, identifying the most effective remediation path, coordinating recovery actions, and documenting response activities. Instead of requiring analysts to manually determine every containment measure, AI increasingly supports response teams by evaluating attack progression, recommending response priorities, and orchestrating coordinated actions across endpoint, identity, network, and cloud security controls. Recent innovations such as Microsoft Security Copilot Guided Response, AI-assisted remediation within Microsoft Defender XDR, Palo Alto Networks Cortex XSIAM, Google Security Operations, Cisco XDR, and CrowdStrike Falcon demonstrate how response activities are becoming more coordinated, contextual, and operationally efficient.

The application is gaining strategic importance because organizations are increasingly evaluated not only on their ability to detect cyber incidents, but also on how quickly they recover critical business functions. Cyber resilience frameworks promoted by CISA and industry collaboration initiatives emphasize structured response planning, coordinated information sharing, and repeatable recovery processes that reduce

JULY 2026 © MarketsandMarkets™

operational and systemic cyber risk. AI SOC platforms therefore support response teams by standardizing remediation workflows, preserving decision consistency during high-pressure situations, and reducing recovery timelines without eliminating human oversight. Looking ahead, incident response is expected to become increasingly adaptive as AI continuously evaluates changing attack conditions, recommends alternative containment strategies, and dynamically adjusts recovery priorities based on business impact rather than technical severity alone. Incident Response and Remediation will increasingly function as an intelligent business resilience capability that enables organizations to restore critical operations faster, strengthen organizational preparedness, and minimize the financial and operational consequences of sophisticated cyberattacks.

TABLE 74 AI SOC MARKET FOR INCIDENT RESPONSE AND REMEDIATION, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	492.5	568.3	657.2	761.6	15.6%
Europe	280.5	327.6	383.4	449.8	17.0%
Asia Pacific	225.8	276.1	338.3	415.4	22.5%
Middle East & Africa	49.7	60.6	74.1	90.8	22.2%
Latin America	40.5	51.3	64.0	78.7	24.8%
Total	**1,089.0**	**1,283.9**	**1,517.0**	**1,796.3**	**18.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 75 AI SOC MARKET FOR INCIDENT RESPONSE AND REMEDIATION, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	884.2	1,029.3	1,201.0	1,404.2	1,644.1	1,926.3	16.9%
Europe	528.3	622.2	734.5	868.8	1,029.1	1,219.7	18.2%
Asia Pacific	510.9	630.0	778.8	964.8	1,197.0	1,486.1	23.8%
Middle East & Africa	110.8	135.7	166.5	204.8	252.2	310.8	22.9%
Latin America	96.4	116.8	140.2	166.3	195.1	225.7	18.5%
Total	**2,130.7**	**2,534.0**	**3,021.0**	**3,608.8**	**4,317.5**	**5,168.6**	**19.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

11.7 INSIDER THREAT DETECTION

11.7.1 HUMAN RISK INTELLIGENCE IS EMERGING AS A STRATEGIC APPLICATION OF AI SOC PLATFORMS

Insider threat detection is becoming an increasingly important application within AI SOC as organizations recognize that cyber risk is no longer limited to external attackers. Modern enterprises must address risks arising from employees, contractors, privileged administrators, third-party partners, and even AI-enabled digital identities that possess legitimate access to business-critical systems. Unlike external attacks, insider incidents often involve valid credentials and authorized system access, making them significantly more difficult to identify using conventional security controls. Consequently, organizations are deploying AI SOC capabilities that continuously assess behavioral changes, unusual data access patterns, privilege misuse, abnormal collaboration activities, and deviations from established user baselines to identify potentially harmful activity before sensitive information is compromised. Rather than treating insider risk solely as a compliance function, enterprises increasingly view it as a continuous business risk management capability spanning cybersecurity, identity, legal, HR, and governance teams. Vendors including Microsoft Purview Insider Risk Management, Google Cloud, Cisco, CrowdStrike, Exabeam, IBM, Palo Alto Networks, and Fortinet continue strengthening AI-powered insider risk capabilities that combine behavioral intelligence with contextual business information to improve decision quality while reducing unnecessary investigations. Microsoft's recent expansion of AI-powered Alert Triage Agents for Insider Risk Management further illustrates how AI is streamlining insider risk investigations and prioritization.

The nature of insider threats is also changing as enterprises adopt generative AI, autonomous AI agents, hybrid work models, and extensive third-party collaboration. Organizations are increasingly concerned about accidental data exposure through AI assistants, misuse of sensitive information, compromised employee accounts, and unauthorized interactions between AI systems and enterprise data. NIST continues emphasizing insider threat programs as coordinated organizational capabilities for detecting and mitigating risks associated with authorized access, reinforcing the need for continuous behavioral monitoring rather than isolated policy enforcement. Simultaneously, growing concern around "synthetic insiders" and AI-assisted identity fraud is encouraging enterprises to integrate insider risk intelligence directly into Security Operations Centers instead of managing it as an independent compliance activity. Insider Threat Detection is expected to evolve into a predictive human risk intelligence function where AI continuously evaluates organizational behavior, digital trust relationships, and identity risks to help organizations proactively prevent data loss, intellectual property theft, and business disruption while preserving employee privacy and regulatory compliance.

TABLE 76 AI SOC MARKET FOR INSIDER THREAT DETECTION, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	180.7	219.5	266.5	324.8	21.6%
Europe	105.5	129.7	159.1	196.1	23.0%
Asia Pacific	80.9	104.1	134.0	173.2	28.9%
Middle East & Africa	17.8	22.9	29.4	37.9	28.6%
Latin America	14.5	19.3	25.4	32.8	31.2%
Total	**399.4**	**495.4**	**614.4**	**764.8**	**24.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 77 AI SOC MARKET FOR INSIDER THREAT DETECTION, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	394.8	481.0	587.3	718.4	879.8	1,078.1	22.3%
Europe	241.1	297.1	366.9	453.7	561.7	695.6	23.6%
Asia Pacific	222.9	287.6	372.1	482.3	626.1	813.4	29.6%
Middle East & Africa	48.4	61.9	79.5	102.4	131.9	170.1	28.6%
Latin America	42.1	53.3	66.9	83.1	102.0	123.5	24.0%
Total	**949.2**	**1,181.0**	**1,472.7**	**1,839.8**	**2,301.6**	**2,880.7**	**24.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

11.8 CLOUD SECURITY MONITORING

11.8.1 CONTINUOUS MULTICLOUD VISIBILITY IS EMERGING AS A STRATEGIC REQUIREMENT FOR AI-DRIVEN SECURITY OPERATIONS

Cloud Security Monitoring has become a mission-critical application of AI SOC as enterprises transition from centralized data centers to highly distributed hybrid and multicloud architectures. Modern organizations operate workloads across public clouds, private clouds, Kubernetes clusters, SaaS platforms, serverless environments, and AI services, creating dynamic infrastructures where assets are continuously provisioned, modified, and decommissioned. In such environments, security teams require persistent visibility into cloud configurations, workload behavior, identity activity, API interactions, and AI resources to identify risks before they disrupt business operations. Consequently, AI SOC platforms are increasingly being deployed to provide unified cloud monitoring that enables security teams to continuously assess operational exposure, prioritize high-risk cloud assets, and detect emerging threats across heterogeneous cloud ecosystems. Vendors including Microsoft Defender for Cloud, Google Security Operations, CrowdStrike, Palo Alto Networks, Cisco, and IBM continue expanding AI-driven cloud monitoring capabilities that integrate cloud posture management, runtime threat detection, AI workload protection, and multicloud visibility into unified security operations.

Cloud monitoring is also evolving from infrastructure oversight into continuous operational assurance as organizations increasingly rely on cloud-native business services, AI platforms, and digital ecosystems for mission-critical operations. Rather than focusing solely on identifying cloud misconfigurations, enterprises are using AI SOC capabilities to understand how cloud risks evolve, how identities interact across cloud services, and how business-critical workloads can be protected against increasingly sophisticated cyber threats. Continuous cloud monitoring is further reinforced by industry best practices promoting ongoing security posture assessment across multicloud environments. As enterprises expand AI-enabled applications and cloud-hosted autonomous agents, cloud security monitoring is expected to become an operational intelligence function that continuously evaluates cloud resilience, business exposure, and evolving attack paths. Over the next several years, Cloud Security Monitoring will increasingly support autonomous cloud defense by providing real-time operational visibility, adaptive risk assessment, and AI-assisted protection across highly distributed enterprise cloud environments.

JULY 2026 © MarketsandMarkets™

TABLE 78 AI SOC MARKET FOR CLOUD SECURITY MONITORING, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	334.2	383.0	439.6	506.0	14.8%
Europe	189.7	220.1	255.6	297.7	16.2%
Asia Pacific	153.7	186.6	227.1	277.0	21.7%
Middle East & Africa	33.8	41.0	49.7	60.5	21.4%
Latin America	27.6	34.7	43.0	52.5	23.9%
Total	**739.0**	**865.4**	**1,015.0**	**1,193.7**	**17.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 79 AI SOC MARKET FOR CLOUD SECURITY MONITORING, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	582.6	672.5	778.1	902.0	1,047.0	1,216.1	15.9%
Europe	346.8	405.0	474.1	555.9	652.7	766.6	17.2%
Asia Pacific	337.8	413.2	506.6	622.4	765.8	942.9	22.8%
Middle East & Africa	73.3	89.0	108.3	132.1	161.3	197.2	21.9%
Latin America	63.8	76.6	91.2	107.3	124.8	143.2	17.6%
Total	**1,404.3**	**1,656.3**	**1,958.2**	**2,319.6**	**2,751.7**	**3,266.1**	**18.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

11.9 IDENTITY AND ACCESS MONITORING

11.9.1 CONTINUOUS IDENTITY VISIBILITY IS BECOMING CENTRAL TO AI-DRIVEN SECURITY OPERATIONS

Identity and access monitoring has emerged as one of the fastest-growing AI SOC applications as identities increasingly replace endpoints as the primary target of modern cyberattacks. Enterprises today manage millions of human, machine, application, service, API, and AI-agent identities that continuously request access across hybrid cloud environments. Consequently, security teams are shifting their operational focus from monitoring infrastructure alone to continuously validating who is accessing enterprise resources, what privileges are being exercised, and whether those activities align with expected business behavior. Rather than functioning solely as an Identity and Access Management (IAM) capability, identity monitoring has become an operational intelligence function within AI SOCs that enables organizations to detect privilege misuse, anomalous authentication patterns, identity-based lateral movement, compromised workload identities, and unauthorized AI agent activities before they evolve into large-scale security incidents. Recent innovations, including Microsoft Entra Agent ID, Conditional Access Optimization Agent, Microsoft's Identity Threat Detection and Response (ITDR), and Google Cloud Identity enhancements, illustrate how leading vendors are embedding AI directly into identity security operations to continuously monitor both human and non-human identities.

JULY 2026 © MarketsandMarkets™

The rapid growth of autonomous AI agents, cloud-native applications, and machine identities is fundamentally expanding the scope of identity monitoring beyond traditional employee authentication. Governments and standards organizations are responding by strengthening digital identity guidance, with NIST SP 800-63-4 establishing updated digital identity and authentication recommendations, while organizations increasingly adopt Zero Trust architectures that require continuous verification rather than one-time authentication. Simultaneously, enterprises are extending AI SOC monitoring to privileged accounts, workload identities, AI agents, and cross-cloud identity relationships to reduce identity sprawl and strengthen cyber resilience. Identity monitoring is expected to evolve from detecting suspicious login events into continuously evaluating identity trust, delegated permissions, AI-agent behavior, and access governance across highly dynamic enterprise ecosystems. Looking ahead, Identity and Access Monitoring is anticipated to become a strategic AI SOC application that continuously validates digital trust relationships, enabling organizations to securely govern human and non-human identities while reducing identity-driven cyber risk across increasingly autonomous enterprise environments.

TABLE 80 AI SOC MARKET FOR IDENTITY AND ACCESS MONITORING, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	184.3	222.1	267.8	323.8	20.7%
Europe	107.2	130.7	159.3	194.9	22.1%
Asia Pacific	82.9	105.7	135.1	173.2	27.9%
Middle East & Africa	18.2	23.2	29.6	37.9	27.6%
Latin America	14.9	19.6	25.6	32.8	30.2%
Total	**407.5**	**501.4**	**617.4**	**762.6**	**23.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 81 AI SOC MARKET FOR IDENTITY AND ACCESS MONITORING, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	391.2	473.9	575.3	699.8	852.3	1,038.7	21.6%
Europe	238.2	291.9	358.4	440.8	542.9	668.8	22.9%
Asia Pacific	221.6	284.3	365.6	471.2	608.2	785.5	28.8%
Middle East & Africa	48.1	61.2	78.2	100.0	128.1	164.3	27.9%
Latin America	41.8	52.7	65.8	81.2	99.1	119.3	23.3%
Total	**941.0**	**1,164.0**	**1,443.3**	**1,793.0**	**2,230.6**	**2,776.6**	**24.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

11.10 COMPLIANCE MONITORING AND REPORTING

11.10.1 CONTINUOUS COMPLIANCE ASSURANCE IS BECOMING A STRATEGIC FUNCTION OF AI-POWERED SECURITY OPERATIONS

Compliance monitoring and reporting is evolving from a periodic audit exercise into a continuous operational capability as organizations navigate an increasingly complex landscape of cybersecurity, privacy, and AI governance regulations. Enterprises today must demonstrate ongoing compliance with frameworks such as NIS2, DORA, ISO/IEC 42001, NIST AI RMF, GDPR, HIPAA, PCI DSS, and sector-specific cybersecurity mandates, while simultaneously governing rapidly expanding AI deployments. This has significantly increased demand for AI SOC capabilities that continuously validate security controls, monitor policy adherence, generate audit-ready evidence, and provide executives with real-time compliance visibility instead of relying on manual assessments conducted weeks or months before regulatory reviews. Rather than treating compliance reporting as a separate governance activity, organizations are integrating it directly into security operations so that every investigation, policy update, security event, and remediation action contributes to an auditable record of cyber resilience. Vendors including Microsoft Purview, Google Cloud, IBM, Cisco, Palo Alto Networks, and CrowdStrike are expanding AI-driven governance capabilities that automate evidence collection, policy validation, AI usage monitoring, and compliance reporting across multicloud environments. Microsoft's recent enhancements to Purview Compliance Manager and Data Security Posture Management (DSPM) for AI illustrate how compliance monitoring is becoming tightly integrated with AI security operations.

The application is becoming increasingly strategic as regulators shift their focus from documenting compliance to demonstrating continuous operational assurance. Organizations are expected to show not only that security controls exist, but also that they remain effective as infrastructure, AI models, and business processes evolve. Recent work by NIST's Center for AI Standards and Innovation (CAISI) highlights post-deployment monitoring, operational oversight, and continuous reporting as essential elements of trustworthy AI governance, reinforcing the need for ongoing compliance monitoring rather than periodic certification exercises. As enterprises expand the use of AI agents, generative AI applications, and autonomous business processes, AI SOC platforms are expected to automate regulatory reporting, continuously evaluate control effectiveness, and provide real-time compliance intelligence for executive leadership and auditors. Over the coming years, Compliance Monitoring and Reporting will increasingly function as a continuous assurance capability that enables organizations to maintain regulatory readiness, strengthen governance transparency, and reduce the operational burden associated with cybersecurity and AI compliance obligations.

TABLE 82 AI SOC MARKET FOR COMPLIANCE MONITORING AND REPORTING, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	102.8	127.7	158.0	196.6	24.1%
Europe	60.6	76.2	95.2	119.6	25.4%
Asia Pacific	45.6	59.9	78.8	104.0	31.7%
Middle East & Africa	10.0	13.2	17.2	22.7	31.4%
Latin America	8.2	11.1	14.9	19.7	34.1%
Total	**227.2**	**288.1**	**364.1**	**462.5**	**26.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 83 AI SOC MARKET FOR COMPLIANCE MONITORING AND REPORTING, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	242.3	299.3	370.5	459.3	570.0	707.6	23.9%
Europe	149.1	186.3	233.0	291.9	365.8	458.5	25.2%
Asia Pacific	135.7	177.6	232.9	306.2	403.1	531.0	31.4%
Middle East & Africa	29.4	38.2	49.8	65.0	84.9	111.0	30.4%
Latin America	25.6	32.9	41.9	52.8	65.7	80.6	25.8%
Total	**582.2**	**734.4**	**928.2**	**1,175.1**	**1,489.5**	**1,888.7**	**26.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

11.11 SECURITY ANALYTICS AND VISUALIZATION

11.11.1 VISUAL SECURITY INTELLIGENCE IS ENABLING FASTER CYBER RISK DECISIONS ACROSS MODERN SECURITY OPERATIONS

Security analytics and visualization has evolved beyond dashboard reporting into a strategic decision-support application that enables organizations to understand complex cyber risks through contextual, business-oriented intelligence. Modern Security Operations Centers are required to analyze enormous volumes of security telemetry originating from cloud platforms, endpoints, identities, AI applications, OT systems, SaaS environments, and threat intelligence sources. However, the true challenge lies not in collecting this information, but in transforming it into actionable operational insight that analysts, executives, and incident responders can interpret quickly. Consequently, AI SOC platforms increasingly employ interactive visual analytics, attack-path mapping, relationship graphs, risk heatmaps, executive dashboards, and AI-generated summaries that allow security teams to rapidly understand attacker behavior, identify systemic exposure, and evaluate organizational cyber posture. Vendors including Microsoft, Google, Cisco, CrowdStrike, Palo Alto Networks, Elastic, IBM, and Exabeam continue expanding advanced visualization capabilities that combine AI-generated insights with graph-based security analytics. Microsoft's introduction of Microsoft Sentinel Graph represents this industry transition by enabling defenders to visualize relationships among identities, assets, activities, and threat intelligence, allowing analysts and AI agents to investigate complex attack paths that are difficult to identify through traditional tabular analysis.

The application is becoming increasingly valuable because executive leadership, security analysts, and risk managers require a common operational view of enterprise cyber risk rather than isolated technical alerts. Interactive visualization enables security teams to communicate investigation findings, demonstrate business impact, support compliance reporting, prioritize remediation investments, and accelerate executive decision-making during active cyber incidents. As AI-generated security insights become more prevalent, visual context is also improving explainability by allowing analysts to validate AI reasoning instead of treating recommendations as opaque outputs. The continued evolution of AI-ready security data platforms and graph-based analytics is further strengthening this capability by connecting previously isolated security information into unified operational views. As the industry moves toward intelligent, autonomous security operations, Security Analytics and Visualization is expected to evolve into an immersive cyber decision intelligence capability where AI continuously generates dynamic visual representations of organizational risk, attack progression, business exposure, and defensive effectiveness, enabling faster, more informed, and collaborative cybersecurity decisions across the enterprise.

JULY 2026 © MarketsandMarkets™

TABLE 84 AI SOC MARKET FOR SECURITY ANALYTICS AND VISUALIZATION, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	370.9	408.7	454.2	492.2	9.9%
Europe	207.1	229.6	259.1	284.7	11.2%
Asia Pacific	173.2	203.4	238.8	273.9	16.5%
Middle East & Africa	38.1	44.7	52.3	59.9	16.2%
Latin America	31.1	37.8	45.2	51.9	18.6%
Total	**820.4**	**924.1**	**1,049.6**	**1,162.6**	**12.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 85 AI SOC MARKET FOR SECURITY ANALYTICS AND VISUALIZATION, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	552.1	614.7	678.1	739.0	792.6	831.7	8.5%
Europe	320.9	359.5	399.7	439.7	477.3	508.4	9.6%
Asia Pacific	327.9	389.1	456.9	529.2	601.8	667.4	15.3%
Middle East & Africa	71.1	83.8	97.7	112.3	126.8	139.6	14.4%
Latin America	61.9	72.2	82.2	91.2	98.1	101.4	10.4%
Total	**1,333.8**	**1,519.3**	**1,714.6**	**1,911.4**	**2,096.5**	**2,248.4**	**11.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

12 AI SOC MARKET, BY VERTICAL

KEY FINDINGS

- The BFSI vertical is estimated to account for the largest market of USD 3,111.8 million in 2026. It is projected to reach USD 7,323.9 million by 2031, at a CAGR of 18.7%, during the forecast period.
- This significant market growth is due to the sector's high exposure to ransomware, payment fraud, identity-based attacks, and increasingly sophisticated AI-enabled cyber threats targeting critical financial infrastructure. Financial institutions are accelerating investments in AI-driven security operations to ensure continuous monitoring, rapid incident response, and operational resilience.
- The healthcare & life sciences vertical is projected to grow at the highest CAGR of 25.4% during the forecast period. The market is estimated to reach USD 8,259.9 million by 2031.
- This fastest growth is due to the rapid digitization of healthcare delivery, widespread adoption of electronic health records (EHRs), connected medical devices, telehealth platforms, and cloud-hosted clinical applications, all of which require continuous AI-driven security monitoring and incident response.
- Escalating ransomware attacks against hospitals, growing protection requirements for sensitive patient data, and increasingly stringent healthcare cybersecurity and privacy regulations are accelerating investments in AI SOC solutions that provide real-time threat detection, automated investigations, and continuous compliance monitoring across healthcare ecosystems.

JULY 2026 © MarketsandMarkets™

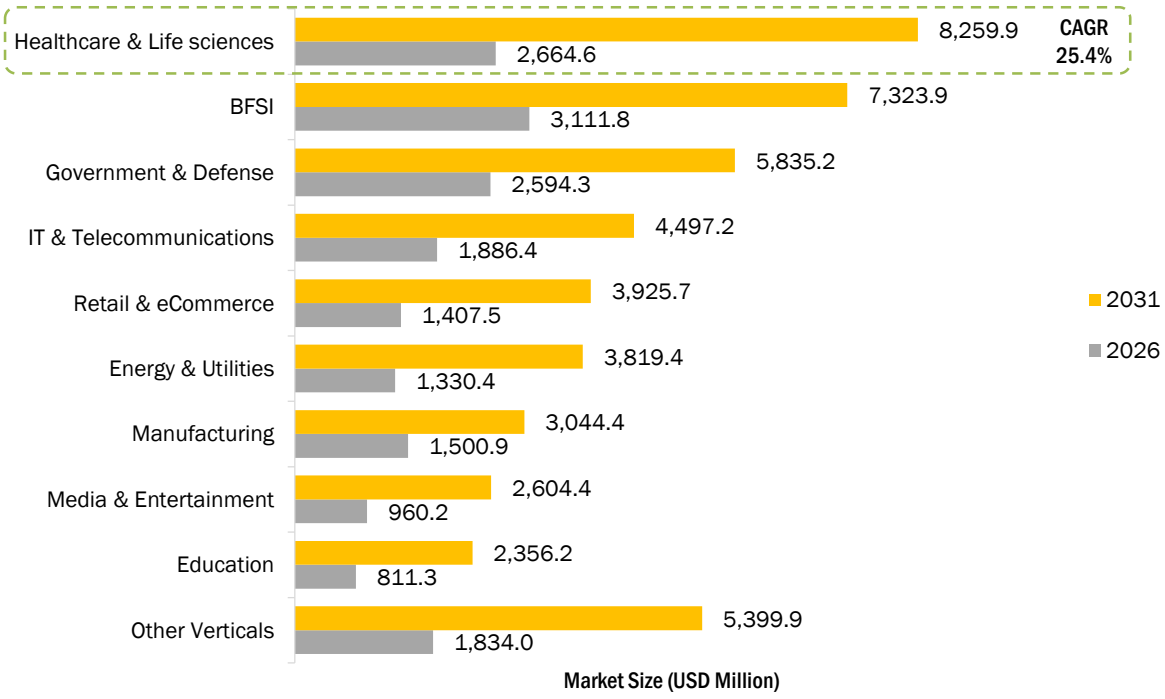
12.1 INTRODUCTION

The AI SOC market, by vertical, is witnessing widespread adoption as organizations across diverse industries integrate artificial intelligence into security operations to address sector-specific cyber risks, regulatory requirements, and operational complexities. Industries including banking, financial services, and insurance (BFSI), government and defense, healthcare and life sciences, IT and telecommunications, manufacturing, retail and ecommerce, energy and utilities, media and entertainment, education, and others are increasingly deploying AI SOC solutions to strengthen threat detection, automate incident response, improve cyber resilience, and secure rapidly expanding digital ecosystems. As organizations accelerate cloud adoption, AI-enabled business processes, operational technology (OT) connectivity, and digital transformation initiatives, traditional Security Operations Centers are evolving into intelligent, AI-driven environments capable of protecting highly distributed infrastructures against increasingly sophisticated cyber threats. Vendors such as Microsoft, Palo Alto Networks, Google, Cisco, CrowdStrike, IBM, Sophos, Fortinet, SentinelOne, and numerous AI-native security providers continue to develop industry-specific AI SOC capabilities that address the unique operational and regulatory needs of different verticals.

AI SOC adoption patterns vary significantly across industry verticals based on risk exposure, digital maturity, compliance obligations, and criticality of operations. Highly regulated sectors such as BFSI, healthcare, and government prioritize AI-powered security operations to protect sensitive information, detect advanced attacks, and comply with evolving cybersecurity and AI governance requirements. Meanwhile, manufacturing, energy and utilities, retail, telecommunications, and media organizations are increasingly leveraging AI SOC platforms to secure hybrid IT-OT environments, cloud-native applications, connected devices, and digital customer services while minimizing operational disruptions. Government initiatives promoting trustworthy AI, critical infrastructure protection, and cyber resilience, together with industry-specific security frameworks, are further accelerating AI SOC adoption across both public and private sectors. As AI technologies mature, vertical-specific AI SOC solutions are expected to evolve beyond generalized threat detection toward context-aware security operations that incorporate industry workflows, regulatory intelligence, and sector-specific risk models, enabling organizations to proactively defend increasingly complex digital environments throughout the forecast period.

JULY 2026 © MarketsandMarkets™

FIGURE 37 HEALTHCARE & LIFE SCIENCES VERTICAL TO ACHIEVE FOR HIGHEST CAGR DURING FORECAST PERIOD



Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

12.1.1 VERTICAL: AI SOC MARKET DRIVERS

- Increasing cyberattacks targeting highly regulated industries such as BFSI, healthcare, government, and critical infrastructure are accelerating adoption of AI SOC solutions that provide continuous monitoring, intelligent threat detection, and rapid incident response tailored to sector-specific risk profiles.
- Rapid digital transformation across industries—including cloud migration, AI-enabled business processes, IoT adoption, and operational technology (OT) connectivity—is driving demand for AI-powered security operations capable of protecting increasingly distributed and heterogeneous enterprise environments.
- Growing cybersecurity regulations and sector-specific compliance mandates, including NIS2, DORA, healthcare security requirements, and financial cyber resilience frameworks, are encouraging organizations to deploy AI SOC capabilities that automate continuous monitoring, compliance validation, and security reporting.
- Expanding adoption of AI across mission-critical industries is creating new attack surfaces that require vertical-specific AI SOC capabilities to secure AI workloads, autonomous systems, connected devices, and industry-specific digital assets throughout their operational lifecycle.
- Critical infrastructure modernization initiatives across manufacturing, energy, utilities, transportation, and public-sector organizations are increasing investments in AI-driven security operations that strengthen cyber resilience against sophisticated nation-state and ransomware attacks.
- Industry-specific security operations are increasingly adopting AI-powered behavioral analytics, contextual threat intelligence, and automated investigations to improve detection accuracy while reducing operational disruptions across financial services, healthcare, telecommunications, retail, and education environments.

JULY 2026 © MarketsandMarkets™

- Organizations across all verticals are prioritizing AI SOC adoption as cybersecurity becomes a strategic business enabler, supporting operational resilience, customer trust, regulatory compliance, and secure digital innovation in increasingly AI-driven enterprise ecosystems.

TABLE 86 AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

End-User Sector	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	1,624.6	1,905.5	2,240.0	2,638.8	17.6%
Government & Defense	1,395.6	1,625.4	1,896.9	2,219.1	16.7%
Healthcare & Lifesciences	1,117.5	1,384.3	1,719.1	2,137.7	24.1%
IT & Telecommunications	976.1	1,147.3	1,351.6	1,595.6	17.8%
Manufacturing	858.2	985.8	1,133.8	1,308.3	15.1%
Retail & eCommerce	643.0	779.7	947.6	1,153.8	21.5%
Energy & Utilities	595.1	725.2	886.0	1,084.3	22.1%
Media & Entertainment	449.6	541.7	654.2	791.7	20.8%
Education	356.8	437.1	536.3	659.5	22.7%
Other Verticals	761.8	951.0	1,184.1	1,463.1	24.3%
Total	**8,778.2**	**10,483.1**	**12,549.5**	**15,051.9**	**19.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 87 AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	3,111.8	3,679.1	4,360.0	5,176.9	6,155.7	7,323.9	18.7%
Government & Defense	2,594.3	3,040.4	3,571.1	4,201.9	4,950.6	5,835.2	17.6%
Healthcare & Lifesciences	2,664.6	3,329.4	4,169.4	5,230.9	6,571.5	8,259.9	25.4%
IT & Telecommunications	1,886.4	2,235.9	2,656.5	3,162.4	3,770.1	4,497.2	19.0%
Manufacturing	1,500.9	1,725.1	1,986.1	2,289.3	2,640.4	3,044.4	15.2%
Retail & eCommerce	1,407.5	1,721.4	2,110.4	2,592.3	3,189.1	3,925.7	22.8%
Energy & Utilities	1,330.4	1,636.6	2,018.0	2,493.2	3,084.9	3,819.4	23.5%
Media & Entertainment	960.2	1,167.7	1,423.6	1,738.9	2,127.4	2,604.4	22.1%
Education	811.3	1,000.5	1,236.7	1,531.5	1,899.1	2,356.2	23.8%
Other Verticals	1,834.0	2,291.0	2,852.9	3,541.3	4,381.5	5,399.9	24.1%
Total	**18,101.3**	**21,827.3**	**26,384.6**	**31,958.6**	**38,770.3**	**47,066.1**	**21.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

12.2 BFSI

12.2.1 RISING AI-ENABLED FINANCIAL FRAUD AND REGULATORY REQUIREMENTS ARE ACCELERATING AI SOC ADOPTION ACROSS THE BFSI SECTOR

The BFSI sector represents one of the largest adopters of AI SOC solutions due to its continuous exposure to financially motivated cyberattacks, stringent regulatory obligations, and rapidly expanding digital banking ecosystems. Financial institutions process billions of transactions daily across online banking, mobile applications, payment platforms, open banking APIs, and digital asset infrastructures, creating an extensive attack surface for ransomware, account takeover, insider threats, AI-generated phishing, deepfake-enabled fraud, and credential compromise. To address these risks, banks and financial institutions are increasingly deploying AI-powered Security Operations Centers capable of continuously monitoring user behavior, correlating fraud indicators, detecting anomalous transactions, and automating incident investigations. Leading vendors including Microsoft, Google, IBM, Cisco, Palo Alto Networks, CrowdStrike, Sophos, and Exabeam are expanding AI-driven security operations capabilities tailored to financial institutions through AI-assisted threat detection, behavioral analytics, identity intelligence, and autonomous investigation technologies. At the same time, regulatory bodies such as the U.S. Department of the Treasury, Bank for International Settlements (BIS), and Federal Reserve are encouraging secure and resilient AI adoption within financial services while emphasizing AI risk management, cybersecurity governance, and operational resilience.

The sector's growing reliance on AI is also transforming security operations beyond traditional fraud prevention. AI SOC platforms are increasingly being deployed to secure generative AI applications, detect AI-assisted attacks, monitor privileged identities, and strengthen cyber resilience across cloud-native banking infrastructures. Recent initiatives including the U.S. Treasury's public-private AI cybersecurity program, the BIS Innovation Hub's work on explainable AI for financial supervision, and evolving financial-sector AI governance frameworks highlight the increasing importance of AI-enabled security operations in maintaining trust, resilience, and regulatory compliance across the global financial system. Similarly, regulators such as the New York Department of Financial Services (NYDFS) have issued AI cybersecurity guidance, while central banks including the Reserve Bank of India (RBI) have identified AI-enabled cyberattacks as one of the most significant emerging risks to financial stability. As digital banking, embedded finance, instant payments, and AI-driven financial services continue expanding, BFSI organizations are expected to increase investments in AI SOC platforms capable of autonomous threat detection, continuous fraud monitoring, intelligent investigations, and real-time incident response, positioning AI-powered security operations as a critical pillar of financial sector resilience through the forecast period.

TABLE 88 AI SOC MARKET IN BFSI, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	734.6	843.1	969.8	1,117.9	15.0%
Europe	413.7	480.5	559.2	652.2	16.4%
Asia Pacific	340.3	414.1	504.8	617.0	21.9%
Middle East & Africa	74.9	91.0	110.5	134.9	21.7%
Latin America	61.1	76.9	95.6	116.9	24.2%
Total	**1,624.6**	**1,905.5**	**2,240.0**	**2,638.8**	**17.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 89 AI SOC MARKET IN BFSI, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,289.9	1,492.2	1,730.2	2,010.0	2,338.2	2,721.5	16.1%
Europe	761.3	890.9	1,044.9	1,227.6	1,444.3	1,699.9	17.4%
Asia Pacific	754.5	925.2	1,137.2	1,400.6	1,727.7	2,132.5	23.1%
Middle East & Africa	163.7	199.3	243.1	297.3	364.0	446.0	22.2%
Latin America	142.4	171.6	204.6	241.4	281.6	323.9	17.9%
Total	**3,111.8**	**3,679.1**	**4,360.0**	**5,176.9**	**6,155.7**	**7,323.9**	**18.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

12.3 GOVERNMENT AND DEFENSE

12.3.1 NATIONAL CYBER RESILIENCE INITIATIVES AND DEFENSE AI MODERNIZATION ARE ACCELERATING AI SOC ADOPTION

Government and defense organizations are rapidly modernizing Security Operations Centers to counter increasingly sophisticated cyber campaigns targeting national infrastructure, defense networks, public services, and classified information systems. Nation-state actors, ransomware groups, and advanced persistent threats (APTs) are increasingly leveraging artificial intelligence to automate reconnaissance, phishing, malware development, and cyber espionage, compelling governments to strengthen cyber defense capabilities with AI-powered security operations. Consequently, ministries of defense, intelligence agencies, civilian government departments, and critical infrastructure operators are investing in AI SOC platforms capable of continuous monitoring, large-scale threat correlation, automated investigations, and rapid incident response. Technology providers including Microsoft, Google, Palo Alto Networks, Cisco, CrowdStrike, IBM, Fortinet, SentinelOne, and Sophos continue expanding AI-driven security capabilities for government environments through sovereign cloud security, Zero Trust architectures, AI-assisted threat intelligence, and autonomous SOC technologies. Simultaneously, agencies such as CISA, NSA, and NIST are strengthening guidance for secure AI deployment, AI governance, and cyber resilience, encouraging government organizations to modernize security operations while maintaining human oversight and mission assurance.

Governments worldwide are also integrating AI into broader national security and defense modernization strategies, significantly expanding demand for intelligent security operations. The US Department of Defense has accelerated AI adoption across defense operations, emphasizing AI-enabled decision support, cyber defense, and secure operational deployment, while recent legislation requires department-wide policies governing the cybersecurity of AI and machine learning systems used in national defense. Similarly, government-led AI security initiatives, including NIST's Center for AI Standards and Innovation (CAISI) and cross-agency collaboration on AI risk evaluation, are promoting standardized approaches for securing AI systems and defending against AI-enabled cyber threats. These developments are encouraging defense organizations to transition from reactive SOC operations toward intelligence-driven, AI-assisted cyber defense capable of protecting complex military, intelligence, and civilian digital infrastructures. Through 2031, continued geopolitical tensions, increasing cyber warfare activity, and expanding AI adoption across government services are expected to accelerate investments in AI-native SOC platforms that combine autonomous threat detection, human-in-the-loop decision-making, and mission-critical cyber resilience to safeguard national security assets.

JULY 2026 © MarketsandMarkets™

TABLE 90 AI SOC MARKET IN GOVERNMENT AND DEFENSE, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	630.9	719.0	820.9	939.5	14.2%
Europe	353.0	406.8	469.9	543.8	15.5%
Asia Pacific	294.1	355.5	430.4	522.6	21.1%
Middle East & Africa	64.7	78.1	94.2	114.2	20.8%
Latin America	52.8	66.1	81.5	99.0	23.3%
Total	**1,395.6**	**1,625.4**	**1,896.9**	**2,219.1**	**16.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 91 AI SOC MARKET IN GOVERNMENT AND DEFENSE, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,074.5	1,231.9	1,415.3	1,628.9	1,876.9	2,163.4	15.0%
Europe	629.0	729.3	847.2	985.5	1,147.7	1,336.8	16.3%
Asia Pacific	633.7	770.4	938.9	1,146.5	1,402.1	1,715.7	22.0%
Middle East & Africa	137.5	165.9	200.7	243.3	295.4	358.8	21.1%
Latin America	119.6	142.9	169.0	197.6	228.5	260.6	16.9%
Total	**2,594.3**	**3,040.4**	**3,571.1**	**4,201.9**	**4,950.6**	**5,835.2**	**17.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

12.4 HEALTHCARE & LIFE SCIENCES

12.4.1 EXPANDING DIGITAL HEALTH ECOSYSTEMS AND PROTECTION OF SENSITIVE PATIENT DATA ARE DRIVING AI SOC ADOPTION

Healthcare and life sciences organizations are rapidly adopting AI SOC solutions as they become increasingly dependent on interconnected digital health ecosystems, cloud-based clinical applications, Internet of Medical Things (IoMT) devices, telehealth platforms, electronic health records (EHRs), genomic research environments, and AI-assisted clinical workflows. These advancements have significantly expanded the cyberattack surface, making hospitals, pharmaceutical companies, biotechnology firms, and research institutions prime targets for ransomware, medical data theft, supply-chain compromises, and attacks on connected medical devices. Consequently, healthcare organizations are deploying AI-powered Security Operations Centers to continuously monitor clinical systems, detect abnormal user and device behavior, automate threat investigations, and accelerate incident response while ensuring uninterrupted patient care. Vendors including Microsoft, Google, Palo Alto Networks, Cisco, IBM, CrowdStrike, SentinelOne, Sophos, and Fortinet continue expanding healthcare-focused cybersecurity capabilities that combine AI-driven threat detection, cloud security, identity protection, and Zero Trust architectures to secure both traditional healthcare IT systems and emerging AI-enabled clinical environments. Simultaneously, the National Institute of Standards and Technology (NIST) continues publishing cybersecurity guidance for telehealth, connected healthcare devices, and AI systems, reinforcing the need for resilient AI-enabled security operations across healthcare organizations.

JULY 2026 © MarketsandMarkets™

Beyond protecting patient records, AI SOC adoption is increasingly becoming a strategic enabler for secure healthcare innovation. Governments and healthcare regulators are actively promoting responsible AI adoption while strengthening cybersecurity governance for medical AI applications. For example, the U.S. Department of Health and Human Services (HHS) introduced a department-wide AI strategy to strengthen AI governance, improve operational resilience, and enhance cybersecurity across federal healthcare agencies, while the UK Medicines and Healthcare products Regulatory Agency (MHRA) is advancing regulatory frameworks for AI-enabled healthcare technologies. These initiatives are encouraging healthcare organizations to integrate AI SOC capabilities that support continuous monitoring of AI applications, medical devices, clinical data, and cloud-native healthcare services while maintaining compliance with evolving cybersecurity and privacy requirements. Through 2031, increasing adoption of precision medicine, digital therapeutics, remote patient monitoring, AI-assisted diagnostics, and connected healthcare infrastructure is expected to further accelerate investments in AI-native security operations centers capable of autonomously securing highly sensitive healthcare environments without disrupting clinical operations.

TABLE 92 AI SOC MARKET IN HEALTHCARE & LIFE SCIENCES, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	505.7	613.6	746.5	909.3	21.6%
Europe	300.5	369.1	454.3	559.7	23.0%
Asia Pacific	222.4	285.7	368.0	474.8	28.8%
Middle East & Africa	48.9	62.8	80.6	103.8	28.5%
Latin America	39.9	53.1	69.7	90.0	31.1%
Total	**1,117.5**	**1,384.3**	**1,719.1**	**2,137.7**	**24.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 93 AI SOC MARKET IN HEALTHCARE & LIFE SCIENCES, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,110.3	1,358.9	1,666.7	2,047.8	2,519.2	3,100.3	22.8%
Europe	690.7	854.1	1,058.2	1,313.0	1,630.9	2,026.3	24.0%
Asia Pacific	614.3	797.0	1,036.4	1,350.6	1,762.7	2,302.2	30.2%
Middle East & Africa	133.3	171.7	221.6	286.6	371.4	481.5	29.3%
Latin America	115.9	147.8	186.5	232.8	287.3	349.6	24.7%
Total	**2,664.6**	**3,329.4**	**4,169.4**	**5,230.9**	**6,571.5**	**8,259.9**	**25.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

12.5 IT & TELECOMMUNICATIONS

12.5.1 EXPANDING AI-NATIVE NETWORKS AND HYPERSCALE DIGITAL INFRASTRUCTURES ARE ACCELERATING AI SOC DEPLOYMENTS ACROSS THE IT AND TELECOMMUNICATIONS SECTOR

The IT and telecommunications sector is at the forefront of AI SOC adoption as organizations manage some of the world's largest and most dynamic digital infrastructures. Cloud service providers, software companies, managed service providers (MSPs), telecommunications operators, internet exchanges, and hyperscale data center operators process enormous volumes of network traffic, user identities, application telemetry, and security events every second. The rapid deployment of 5G, edge computing, cloud-native applications, software-defined networking (SDN), and AI-enabled network operations has significantly expanded the attack surface while increasing the operational complexity of modern Security Operations Centers. Consequently, organizations are adopting AI SOC platforms capable of continuously correlating network, endpoint, identity, and cloud telemetry to detect sophisticated attacks in real time while automating investigation and response workflows. Technology leaders including Microsoft, Google, Cisco, IBM, Palo Alto Networks, CrowdStrike, Fortinet, SentinelOne, Elastic, and Rapid7 continue enhancing AI-native security platforms with autonomous SOC capabilities, AI assistants, and advanced security analytics designed specifically for large-scale IT and telecom environments. At the same time, telecom providers are strengthening cybersecurity programs to secure increasingly interconnected digital ecosystems supporting governments, enterprises, and consumers.

The convergence of artificial intelligence and next-generation communications is further reshaping security operations across the sector. NIST's Communications Technology Laboratory (CTL) is actively advancing research on secure AI-enabled 6G, Zero Trust architectures, and Open RAN technologies to ensure future communication networks are intelligent, interoperable, and secure by design. In parallel, international standards activities within the International Telecommunication Union (ITU-T) are addressing AI system supply chain security for telecommunications organizations, reflecting the growing importance of AI governance within critical communications infrastructure. These initiatives complement enterprise investments in AI SOC platforms that secure AI-powered network management systems, cloud services, customer-facing applications, and critical telecom infrastructure against increasingly sophisticated cyber threats. Through 2031, continued expansion of hyperscale cloud computing, AI-native telecommunications networks, edge infrastructure, and autonomous network operations is expected to accelerate demand for AI SOC solutions capable of delivering predictive threat intelligence, automated network defense, and resilient security operations across highly distributed digital environments.

TABLE 94 AI SOC MARKET IN IT & TELECOMMUNICATIONS, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	441.3	507.7	585.2	676.1	15.3%
Europe	249.1	289.9	338.2	395.4	16.7%
Asia Pacific	204.1	248.8	304.0	372.3	22.2%
Middle East & Africa	44.9	54.7	66.6	81.4	21.9%
Latin America	36.6	46.2	57.6	70.5	24.4%
Total	**976.1**	**1,147.3**	**1,351.6**	**1,595.6**	**17.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 95 AI SOC MARKET IN IT & TELECOMMUNICATIONS, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	782.1	907.1	1,054.6	1,228.3	1,432.8	1,672.2	16.4%
Europe	462.7	542.9	638.5	752.2	887.4	1,047.5	17.8%
Asia Pacific	456.4	561.0	691.3	853.5	1,055.5	1,306.0	23.4%
Middle East & Africa	99.0	120.8	147.8	181.2	222.4	273.1	22.5%
Latin America	86.1	104.0	124.4	147.1	172.0	198.4	18.2%
Total	**1,886.4**	**2,235.9**	**2,656.5**	**3,162.4**	**3,770.1**	**4,497.2**	**19.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

12.6 MANUFACTURING

12.6.1 INDUSTRY 4.0 AND IT-OT CONVERGENCE ARE ACCELERATING AI SOC ADOPTION ACROSS THE MANUFACTURING SECTOR

Manufacturing organizations are increasingly deploying AI SOC solutions as Industry 4.0 initiatives connect industrial control systems (ICS), operational technology (OT), industrial Internet of Things (IIoT) devices, robotics, edge computing platforms, and cloud-based manufacturing applications. While these technologies improve operational efficiency and production visibility, they also significantly expand the cyberattack surface by increasing connectivity between traditionally isolated OT environments and enterprise IT networks. Ransomware attacks targeting production facilities, supply-chain compromises, and nation-state attacks against industrial infrastructure have made continuous cyber monitoring a business-critical requirement rather than solely an IT function. As a result, manufacturers are investing in AI-powered Security Operations Centers capable of correlating telemetry across IT and OT environments, identifying abnormal industrial behavior, automating threat investigations, and minimizing operational downtime. Vendors including Microsoft, Palo Alto Networks, Cisco, Google, CrowdStrike, Fortinet, IBM, SentinelOne, Nozomi Networks (through integrations), and Stellar Cyber are increasingly enhancing AI-driven security capabilities that protect converged manufacturing environments while supporting operational continuity. NIST's Manufacturing Cybersecurity Program also continues to advance guidance for securing industrial environments through behavioral anomaly detection and integrated IT-OT cybersecurity practices.

The manufacturing sector is also benefiting from government-led initiatives that combine artificial intelligence with industrial cybersecurity to strengthen national manufacturing resilience. In 2025, NIST announced new Centers for AI in Manufacturing and Critical Infrastructure, supporting the development of AI technologies that improve both manufacturing competitiveness and cybersecurity resilience. Simultaneously, the NCCoE released guidance for responding to and recovering from cyberattacks in manufacturing environments, reflecting growing emphasis on resilient industrial security operations as OT and IT systems become increasingly interconnected. These initiatives align with manufacturers' growing investments in AI SOC platforms capable of continuously monitoring production networks, detecting process anomalies, securing industrial AI applications, and accelerating incident response without disrupting factory operations. Continued adoption of smart factories, autonomous production systems, digital twins, and AI-enabled industrial automation is expected to significantly increase demand for AI-native SOC platforms that deliver predictive threat detection, IT-OT security convergence, and autonomous cyber defense across modern manufacturing ecosystems.

JULY 2026 © MarketsandMarkets™

TABLE 96 AI SOC MARKET IN MANUFACTURING, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	387.9	435.9	490.3	553.2	12.6%
Europe	214.2	243.1	276.3	314.7	13.7%
Asia Pacific	183.0	218.3	260.7	312.8	19.6%
Middle East & Africa	40.3	48.0	57.1	68.4	19.3%
Latin America	32.8	40.6	49.4	59.3	21.7%
Total	**858.2**	**985.8**	**1,133.8**	**1,308.3**	**15.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 97 AI SOC MARKET IN MANUFACTURING, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	620.6	697.4	784.9	884.2	996.3	1,122.0	12.6%
Europe	356.8	405.0	460.1	522.9	594.0	673.9	13.6%
Asia Pacific	372.4	444.5	531.7	637.2	764.4	917.3	19.8%
Middle East & Africa	80.8	95.7	113.7	135.2	161.0	191.9	18.9%
Latin America	70.3	82.4	95.7	109.8	124.6	139.3	14.7%
Total	**1,500.9**	**1,725.1**	**1,986.1**	**2,289.3**	**2,640.4**	**3,044.4**	**15.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

12.7 RETAIL & ECOMMERCE

12.7.1 EXPANDING DIGITAL COMMERCE AND AI-DRIVEN CUSTOMER ENGAGEMENT ARE DRIVING AI SOC ADOPTION ACROSS THE RETAIL AND ECOMMERCE SECTOR

Retail and eCommerce organizations are increasingly investing in AI-powered Security Operations Centers as digital commerce ecosystems become more interconnected, data-intensive, and attractive to cybercriminals. Online marketplaces, omnichannel retail platforms, digital payment systems, loyalty programs, mobile commerce applications, and AI-powered customer engagement tools collectively process enormous volumes of sensitive customer and financial information, making retailers prime targets for account takeover, payment fraud, ransomware, bot attacks, API exploitation, and supply-chain compromises. The rapid adoption of generative AI for personalized shopping experiences, pricing optimization, inventory management, and customer service has further expanded the cyberattack surface, requiring security operations to monitor both conventional IT assets and AI-enabled business applications. Consequently, retailers are deploying AI SOC platforms that combine behavioral analytics, AI-driven threat detection, identity intelligence, and automated incident response to continuously secure customer-facing digital environments without disrupting shopping experiences. Technology providers including Microsoft, Google, Palo Alto Networks, Cisco, CrowdStrike, IBM, Sophos, and Fortinet continue enhancing AI-native security capabilities that help retailers protect omnichannel operations, digital payment infrastructures, and cloud-native commerce platforms. Additionally, the NIST National Cybersecurity Center of Excellence (NCCoE) continues promoting stronger authentication and risk-based security controls for ecommerce environments to combat increasingly sophisticated online fraud.

JULY 2026 © MarketsandMarkets™

The increasing use of artificial intelligence by cybercriminals is further accelerating AI SOC adoption across the retail sector. AI-enabled bots are now capable of automating credential stuffing, account takeover, fraudulent purchases, price manipulation, promotional abuse, and distributed attacks that closely mimic legitimate customer behavior, making traditional rule-based security monitoring significantly less effective. Industry reports indicate that retailers continue to experience substantial volumes of AI-driven attacks, particularly during peak shopping seasons when transaction volumes increase dramatically. As a result, retail organizations are adopting AI-powered security operations that continuously analyze customer behavior, correlate fraud indicators, prioritize high-risk incidents, and automate investigation workflows in real time. Through 2031, continued expansion of digital commerce, embedded payments, AI-powered customer experiences, and omnichannel retail ecosystems is expected to further strengthen demand for AI-native SOC platforms capable of protecting complex retail infrastructures while maintaining seamless customer experiences, safeguarding consumer trust, and supporting secure digital business growth.

TABLE 98 AI SOC MARKET IN RETAIL & ECOMMERCE, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	290.9	345.4	411.0	490.0	19.0%
Europe	169.2	203.3	244.7	295.2	20.4%
Asia Pacific	130.7	164.4	207.2	261.8	26.1%
Middle East & Africa	28.8	36.1	45.4	57.2	25.8%
Latin America	23.5	30.5	39.2	49.6	28.3%
Total	**643.0**	**779.7**	**947.6**	**1,153.8**	**21.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 99 AI SOC MARKET IN RETAIL & ECOMMERCE, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	585.3	700.9	841.3	1,011.9	1,218.8	1,469.0	20.2%
Europe	356.7	432.0	524.5	638.0	777.1	947.2	21.6%
Asia Pacific	331.2	420.1	534.2	680.7	868.6	1,109.1	27.3%
Middle East & Africa	71.9	90.5	114.2	144.5	183.0	232.0	26.4%
Latin America	62.5	77.9	96.1	117.3	141.6	168.5	21.9%
Total	**1,407.5**	**1,721.4**	**2,110.4**	**2,592.3**	**3,189.1**	**3,925.7**	**22.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

12.8 ENERGY & UTILITIES

12.8.1 MODERNIZATION OF CRITICAL ENERGY INFRASTRUCTURE AND IT-OT CONVERGENCE ARE DRIVING AI SOC ADOPTION ACROSS THE ENERGY AND UTILITIES SECTOR

The energy and utilities sector is rapidly adopting AI-powered Security Operations Centers (SOCs) as utilities modernize electricity grids, renewable energy assets, oil and gas operations, substations, and industrial control systems (ICS). The increasing convergence of operational technology (OT) with enterprise IT, coupled with the deployment of smart grids, distributed energy resources, advanced metering infrastructure (AMI), and cloud-based energy management platforms, has significantly expanded the cyberattack surface for critical infrastructure operators. Nation-state attacks, ransomware campaigns, and supply chain compromises targeting power generation, transmission, and distribution networks have made continuous cyber monitoring a strategic priority. Consequently, utilities are deploying AI SOC platforms capable of correlating telemetry from IT, OT, cloud, and field devices to detect anomalies, automate investigations, and accelerate incident response while maintaining uninterrupted energy delivery. Technology providers including Microsoft, Palo Alto Networks, Google, Cisco, IBM, CrowdStrike, Fortinet, and SentinelOne continue strengthening AI-driven cybersecurity capabilities for critical infrastructure through AI-assisted threat detection, Zero Trust architectures, industrial security, and cloud-native security operations. Simultaneously, the U.S. Department of Energy (DOE) continues expanding cybersecurity initiatives that integrate artificial intelligence to strengthen operational resilience across the energy sector.

Artificial intelligence is becoming a strategic component of both energy operations and cyber defense. The DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER) recently launched initiatives such as AI-FORTS and the Stormbreaker testbed to evaluate large language models and agentic AI within power systems and OT environments, enabling utilities to assess AI performance and cyber resilience before operational deployment. These initiatives complement broader government efforts focused on protecting critical infrastructure and promoting secure AI adoption for essential services. At the enterprise level, utilities are increasingly implementing AI SOC platforms to secure renewable energy assets, transmission networks, AI-enabled grid management systems, and connected industrial environments while supporting compliance with evolving critical infrastructure cybersecurity requirements. Through 2031, continued investment in smart grids, decentralized energy systems, electric vehicle charging infrastructure, and AI-enabled utility operations is expected to significantly increase demand for AI-native SOC platforms capable of delivering predictive threat detection, autonomous incident investigation, and continuous protection of mission-critical energy infrastructure against increasingly sophisticated cyber threats.

TABLE 100 AI SOC MARKET IN ENERGY & UTILITIES, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	269.2	321.3	384.4	460.7	19.6%
Europe	157.4	190.1	230.2	279.2	21.0%
Asia Pacific	120.4	152.1	192.7	244.6	26.7%
Middle East & Africa	26.5	33.4	42.2	53.5	26.4%
Latin America	21.6	28.3	36.5	46.4	29.0%
Total	**595.1**	**725.2**	**886.0**	**1,084.3**	**22.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 101 AI SOC MARKET IN ENERGY & UTILITIES, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	553.5	666.8	805.1	974.0	1,180.1	1,430.5	20.9%
Europe	339.2	413.2	504.4	617.0	755.7	926.1	22.2%
Asia Pacific	311.4	397.3	508.3	651.6	836.5	1,074.7	28.1%
Middle East & Africa	67.6	85.6	108.7	138.3	176.2	224.8	27.2%
Latin America	58.8	73.7	91.5	112.3	136.3	163.2	22.7%
Total	**1,330.4**	**1,636.6**	**2,018.0**	**2,493.2**	**3,084.9**	**3,819.4**	**23.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

12.9 MEDIA & ENTERTAINMENT

12.9.1 PROTECTING DIGITAL CONTENT, STREAMING PLATFORMS, AND AI-DRIVEN MEDIA ECOSYSTEMS IS ACCELERATING AI SOC ADOPTION ACROSS THE MEDIA AND ENTERTAINMENT INDUSTRY

The media and entertainment industry is increasingly adopting AI-powered security operations centers (SOCs) as digital content production, streaming platforms, cloud-based post-production, gaming ecosystems, and direct-to-consumer services become central to business operations. Media companies manage vast repositories of high-value intellectual property, subscriber data, digital rights, advertising platforms, and cloud-native production environments, making them attractive targets for ransomware, data breaches, credential theft, API attacks, and content piracy. The rapid integration of generative AI into video production, recommendation engines, advertising, and content creation has further expanded the cyberattack surface, requiring continuous monitoring of AI models, cloud workloads, and digital assets. Consequently, broadcasters, streaming providers, gaming companies, and content studios are implementing AI SOC platforms that leverage behavioral analytics, AI-assisted threat detection, automated investigations, and identity intelligence to safeguard creative assets while maintaining uninterrupted digital services. Technology providers including Microsoft, Google, Palo Alto Networks, Cisco, CrowdStrike, IBM, and Elastic continue strengthening AI-native security platforms that help media organizations secure cloud-first production workflows, streaming infrastructure, and AI-enabled content ecosystems. Simultaneously, industry organizations such as the Society of Motion Picture and Television Engineers (SMPTE) and the European Broadcasting Union (EBU) are advancing guidance on secure AI adoption and governance across media workflows.

Government initiatives are also encouraging secure digital transformation across the media sector. In 2026, India's Ministry of Information and Broadcasting launched a National AI Skilling Initiative in partnership with Google and YouTube to strengthen AI capabilities across the media ecosystem, alongside establishing AI academies and creator-focused programs to promote responsible AI adoption. These initiatives reflect the growing convergence of artificial intelligence, digital content creation, and cybersecurity across the global media landscape. At the same time, entertainment companies are strengthening cyber resilience to combat AI-generated deepfakes, intellectual property theft, synthetic identity fraud, and attacks targeting streaming and content distribution platforms. Through 2031, continued expansion of AI-assisted production, immersive media, cloud broadcasting, digital advertising, and creator economy platforms is expected to significantly increase demand for AI-native SOC solutions capable of protecting high-value digital content, securing AI-enabled creative workflows, and preserving consumer trust across increasingly interconnected media ecosystems.

JULY 2026 © MarketsandMarkets™

TABLE 102 AI SOC MARKET IN MEDIA & ENTERTAINMENT, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	203.4	239.9	283.7	336.0	18.2%
Europe	117.6	140.4	167.9	201.4	19.6%
Asia Pacific	91.9	114.9	143.9	180.6	25.2%
Middle East & Africa	20.2	25.2	31.5	39.5	24.9%
Latin America	16.5	21.3	27.2	34.2	27.5%
Total	**449.6**	**541.7**	**654.2**	**791.7**	**20.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 103 AI SOC MARKET IN MEDIA & ENTERTAINMENT, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	399.1	475.1	567.1	678.2	812.3	973.6	19.5%
Europe	241.9	291.3	351.7	425.5	515.5	625.0	20.9%
Asia Pacific	227.1	286.4	362.1	458.8	582.1	739.0	26.6%
Middle East & Africa	49.3	61.7	77.4	97.4	122.6	154.6	25.7%
Latin America	42.9	53.1	65.2	79.1	94.9	112.2	21.2%
Total	**960.2**	**1,167.7**	**1,423.6**	**1,738.9**	**2,127.4**	**2,604.4**	**22.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

12.10 EDUCATION

12.10.1 DIGITAL LEARNING EXPANSION AND RISING CYBER THREATS ARE ACCELERATING AI SOC ADOPTION ACROSS EDUCATIONAL INSTITUTIONS

Educational institutions are increasingly investing in AI-powered security operations centers (SOCs) as schools, universities, and research organizations undergo large-scale digital transformation. Learning management systems (LMS), cloud-based collaboration platforms, student information systems, online examinations, research networks, and AI-enabled educational applications have become integral to modern education, significantly expanding the sector's cyberattack surface. At the same time, educational institutions have become frequent targets of ransomware, phishing campaigns, identity theft, and data breaches due to the large volumes of sensitive student, faculty, research, and financial information they manage. Limited cybersecurity budgets and shortages of skilled security personnel have further increased reliance on AI-enabled security operations capable of automating threat detection, alert prioritization, and incident response. Consequently, universities and educational institutions are adopting AI SOC platforms that provide continuous monitoring, behavioral analytics, automated investigations, and cloud security while reducing the operational burden on internal IT teams. Technology providers including Microsoft, Google, Cisco, IBM, Palo Alto Networks, CrowdStrike, Sophos, and Fortinet continue expanding AI-driven cybersecurity capabilities that help educational institutions secure increasingly cloud-first learning environments. Meanwhile, NIST's NICE program continues supporting cybersecurity education, workforce development, and partnerships that strengthen cyber resilience across the education sector.

JULY 2026 © MarketsandMarkets™

AI is simultaneously transforming both education delivery and cybersecurity operations, requiring institutions to balance innovation with responsible risk management. UNESCO continues promoting a human-centered approach to AI adoption through guidance on AI governance, learner protection, privacy, and digital rights, encouraging educational institutions to deploy AI securely while protecting sensitive academic and personal data. In parallel, governments are expanding cybersecurity workforce development initiatives to address growing shortages of cybersecurity professionals, with programs such as NIST NICE, cybersecurity education partnerships, and AI literacy initiatives strengthening institutional cyber readiness. As universities increasingly adopt generative AI, virtual learning environments, digital research platforms, and AI-assisted academic services, AI SOC platforms are becoming essential for securing academic infrastructure, protecting intellectual property, and ensuring uninterrupted learning operations. Through 2031, continued growth in digital education, cloud-native campuses, AI-enabled learning ecosystems, and collaborative international research is expected to accelerate demand for AI-native SOC platforms capable of delivering autonomous threat detection, intelligent investigations, and resilient cybersecurity across increasingly connected educational environments.

TABLE 104 AI SOC MARKET IN EDUCATION, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	161.4	193.7	232.7	280.2	20.2%
Europe	94.8	115.0	139.8	170.2	21.5%
Asia Pacific	71.8	91.3	116.3	148.4	27.4%
Middle East & Africa	15.8	20.1	25.5	32.4	27.1%
Latin America	12.9	17.0	22.0	28.1	29.7%
Total	**356.8**	**437.1**	**536.3**	**659.5**	**22.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 105 AI SOC MARKET IN EDUCATION, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	337.6	407.7	493.6	598.5	726.7	882.9	21.2%
Europe	207.4	253.2	309.9	379.9	466.3	572.6	22.5%
Asia Pacific	189.4	242.4	310.8	399.4	514.0	661.8	28.4%
Middle East & Africa	41.1	52.2	66.5	84.8	108.3	138.4	27.5%
Latin America	35.7	44.9	55.9	68.9	83.8	100.5	23.0%
Total	**811.3**	**1,000.5**	**1,236.7**	**1,531.5**	**1,899.1**	**2,356.2**	**23.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

12.11 OTHER VERTICALS

Other verticals include transportation & logistics, travel & hospitality, real estate & construction, professional services, legal services, agriculture, and nonprofit organizations. These verticals represent industries that operate increasingly digital and distributed environments but do not fit within the major vertical categories covered separately in the segmentation. Their security requirements are driven by growing cloud adoption, remote workforces, connected operational assets, third-party access, expanding digital service channels, and limited availability of skilled cybersecurity personnel. AI-enabled SOC platforms and services help organizations in these verticals automate security monitoring, correlate alerts across multiple systems, identify anomalous behavior, accelerate threat investigation, and improve incident-response consistency.

Transportation & logistics includes airlines, airports, rail operators, shipping companies, ports, fleet operators, freight forwarders, courier companies, and logistics service providers. These organizations manage geographically distributed IT and operational technology environments, including fleet-management systems, warehouse platforms, cargo-tracking applications, industrial control systems, telematics devices, and customer-facing booking or shipment portals. AI SOC solutions support continuous monitoring of these environments, detection of credential compromise, ransomware, supply-chain attacks, GPS or telematics manipulation, and unauthorized access to operational systems.

Travel & hospitality includes hotels, resorts, travel agencies, online travel platforms, cruise operators, and tourism service providers. These organizations process large volumes of payment information, customer identities, loyalty-program data, and reservation records. Their dependence on online booking systems, point-of-sale infrastructure, property-management platforms, mobile applications, and third-party service providers creates a broad attack surface. AI SOC capabilities help identify account takeover, payment fraud, phishing, suspicious login activity, malware, insider threats, and abnormal access to guest information.

Real estate & construction includes property developers, construction companies, engineering contractors, commercial property owners, facility-management companies, and real estate service providers. Their digital environments may include building information modeling platforms, project collaboration tools, connected building systems, access-control systems, surveillance networks, IoT devices, and contractor-managed endpoints. AI SOC platforms can correlate security events across corporate IT, construction sites, smart-building infrastructure, and third-party systems to detect unauthorized access, compromised contractor accounts, data theft, and attacks on building-management systems.

Professional services include consulting, accounting, engineering, staffing, market research, and other business advisory organizations, excluding legal services classified separately. These companies hold confidential client information, financial records, intellectual property, project documentation, and employee data. They frequently depend on cloud-based collaboration platforms, remote access, email, and client-facing digital systems. AI SOC solutions help detect business email compromise, credential theft, malicious file activity, insider risk, data exfiltration, and misuse of privileged accounts.

Legal services include law firms, legal process outsourcing providers, litigation-support companies, and corporate legal service organizations. These entities manage highly confidential legal documents, privileged communications, intellectual property, merger and acquisition information, and litigation records. They are attractive targets for ransomware, espionage, extortion, and account compromise. AI-driven SOC capabilities support behavioral analytics, sensitive-data monitoring, rapid investigation of suspicious access, and automated response to compromised identities or endpoints.

Agriculture includes commercial farms, agribusiness companies, agricultural cooperatives, food-production support providers, and operators of precision-agriculture technologies. Their environments increasingly combine enterprise IT with connected machinery, farm-management platforms, drones, sensors, satellite systems, irrigation controls, and supply-chain applications. AI SOC solutions can help identify attacks

JULY 2026 © MarketsandMarkets™

against connected equipment, unauthorized remote access, ransomware, disruption of agricultural operations, and manipulation of sensor or production data.

Nonprofit organizations include charities, foundations, associations, humanitarian organizations, and nongovernmental organizations. These entities often manage donor information, beneficiary records, payment data, employee information, and sensitive program-related data while operating with constrained cybersecurity budgets and small internal security teams. AI SOC platforms and managed AI SOC services can reduce the operational burden by automating alert prioritization, threat detection, investigation, reporting, and response activities.

TABLE 106 AI SOC MARKET IN OTHER VERTICALS, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	344.7	421.6	514.2	622.4	21.8%
Europe	205.7	254.0	312.5	383.1	23.0%
Asia Pacific	151.0	195.9	253.9	325.0	29.1%
Middle East & Africa	33.2	43.0	55.6	71.0	28.8%
Latin America	27.1	36.4	48.1	61.6	31.5%
Total	**761.8**	**951.0**	**1,184.1**	**1,463.1**	**24.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 107 AI SOC MARKET IN OTHER VERTICALS, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	764.0	934.7	1,140.1	1,386.5	1,681.2	2,031.3	21.6%
Europe	474.1	585.6	722.2	889.4	1,093.2	1,340.6	23.1%
Asia Pacific	424.0	550.2	710.7	914.0	1,170.0	1,490.1	28.6%
Middle East & Africa	92.0	118.5	152.0	194.0	246.5	311.6	27.6%
Latin America	80.0	102.0	127.9	157.6	190.7	226.3	23.1%
Total	**1,834.0**	**2,291.0**	**2,852.9**	**3,541.3**	**4,381.5**	**5,399.9**	**24.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13 AI SOC MARKET, BY REGION

KEY FINDINGS

- North America is estimated to lead the AI SOC market from 2026 to 2031. The market in this region is projected to grow from USD 7,516.8 million in 2026 to USD 17,566.7 million by 2031, at a CAGR of 18.5% during the forecast period.
- The strong presence of global AI SOC vendors, mature enterprise cybersecurity ecosystems, and federal initiatives promoting secure AI adoption are accelerating AI-native SOC deployment. Rising AI-powered cyber threats, widespread cloud adoption, and large-scale investments in autonomous security operations continue to reinforce North America's market leadership.
- The Asia Pacific market is projected to register the highest CAGR of 25.5% during the forecast period. The AI SOC market in Asia Pacific will grow up to USD 13,448.4 million by 2031.
- Rapid digital transformation, expanding enterprise AI adoption, and government-backed AI and cybersecurity initiatives across China, India, Japan, and other Asia Pacific countries are accelerating AI SOC adoption. Growing cloud deployments, sovereign AI investments, and increasing cyberattacks on critical infrastructure are driving the region's fastest market growth.
- The EU AI Act, NIS2 Directive, DORA, and the EU Action Plan on Cybersecurity and Artificial Intelligence are accelerating AI SOC adoption across regulated industries in the European region. Rising AI-enabled cyber threats targeting critical infrastructure, combined with increasing enterprise investments in AI-powered cyber resilience, continue to strengthen regional market growth.
- National AI strategies, critical infrastructure protection initiatives, and smart city programs are accelerating AI SOC adoption across the Middle East & Africa.
- Rapid digital transformation, expanding AI governance initiatives, and rising cybersecurity investments are driving steady AI SOC adoption across Latin America.

JULY 2026 © MarketsandMarkets™

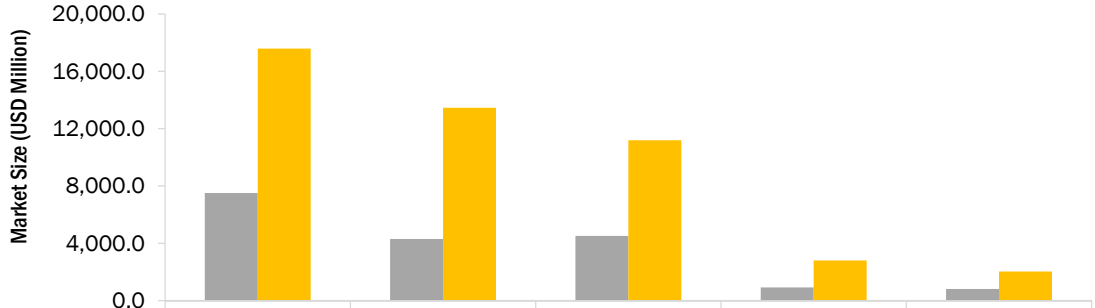
13.1 INTRODUCTION

The AI SOC market is expanding globally as organizations across industries accelerate cybersecurity modernization to address increasingly sophisticated cyber threats, rising security data volumes, and growing operational complexity. Increasing adoption of artificial intelligence, cloud computing, hybrid infrastructure, and automation technologies is transforming traditional Security Operations Centers (SOCs) into intelligent, AI-driven platforms capable of real-time threat detection, automated investigation, threat prioritization, and autonomous incident response. Enterprises across BFSI, healthcare, telecommunications, manufacturing, government, and critical infrastructure sectors are increasingly investing in AI SOC solutions to improve security resilience, reduce analyst workload, and enhance cyber defense capabilities against ransomware, advanced persistent threats, and AI-enabled attacks.

Regionally, North America dominates the AI SOC market due to its mature cybersecurity ecosystem, strong presence of leading security technology providers, advanced cloud adoption, and increasing investments in AI-powered security automation. Asia Pacific is expected to witness the fastest growth, driven by rapid digital transformation, expanding enterprise AI adoption, increasing cyber threat exposure, and growing demand for scalable security operations across emerging economies. Europe represents a significant market, supported by stringent cybersecurity regulations, digital sovereignty initiatives, and increasing adoption of AI-driven security platforms across regulated industries. Meanwhile, Latin America and the Middle East & Africa are emerging markets, driven by digital government initiatives, cloud migration, critical infrastructure modernization, and growing cybersecurity investments aimed at strengthening cyber resilience.

The increasing deployment of AI-native SOC platforms, generative AI-based security assistants, autonomous response technologies, and managed AI security operations services is expected to reshape the global cybersecurity landscape throughout the forecast period. However, challenges related to AI governance, data privacy, integration with legacy security infrastructure, and shortage of skilled cybersecurity professionals may influence adoption across certain regions.

FIGURE 38 ASIA PACIFIC TO REGISTER HIGHEST CAGR DURING FORECAST PERIOD



	North America	Asia Pacific	Europe	Middle East and Africa	Latin America
2026	7,516.8	4,314.5	4,519.7	936.1	814.2
2031	17,566.7	13,448.4	11,195.9	2,812.6	2,042.5
CAGR (2026–2031)	18.5%	25.5%	19.9%	24.6%	20.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 108 AI SOC MARKET, BY REGION, 2022–2025 (USD MILLION)

Region	2022	2023	2024	2025	CAGR (2022–2025)
North America	3,970.1	4,641.1	5,438.6	6,385.3	17.2%
Europe	2,275.2	2,692.2	3,193.1	3,794.9	18.6%
Asia Pacific	1,809.8	2,241.1	2,781.9	3,459.9	24.1%
Middle East and Africa	398.3	492.3	609.2	756.2	23.8%
Latin America	324.8	416.4	526.7	655.5	26.4%
Total	**8,778.2**	**10,483.1**	**12,549.5**	**15,051.9**	**19.7%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 109 AI SOC MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	7,516.8	8,872.7	10,498.8	12,448.2	14,782.6	17,566.7	18.5%
Europe	4,519.7	5,397.5	6,461.5	7,751.0	9,312.4	11,195.9	19.9%
Asia Pacific	4,314.5	5,394.7	6,761.9	8,492.8	10,683.5	13,448.4	25.5%
Middle East and Africa	936.1	1,161.9	1,445.7	1,802.5	2,250.8	2,812.6	24.6%
Latin America	814.2	1,000.5	1,216.8	1,464.0	1,741.1	2,042.5	20.2%
Total	**18,101.3**	**21,827.3**	**26,384.6**	**31,958.6**	**38,770.3**	**47,066.1**	**21.1%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

13.2 NORTH AMERICA

North America remains the global innovation hub for the AI SOC market owing to its highly mature cybersecurity ecosystem, strong AI research capabilities, and concentration of leading cybersecurity vendors, hyperscale cloud providers, and venture-backed startups. Organizations across the US and Canada are rapidly transitioning from traditional security operations centers (SOCs) to AI-driven and autonomous SOC models to address escalating cyberattacks, increasing alert volumes, and persistent cybersecurity workforce shortages. The region benefits from high enterprise cybersecurity spending, widespread cloud adoption, and rapid deployment of XDR, SIEM, SOAR, and MDR platforms, enabling organizations to modernize security operations and reduce response times. Continuous investments by Microsoft, Google, AWS, Cisco, IBM, Palo Alto Networks, CrowdStrike, SentinelOne, and other technology leaders are further strengthening the regional AI SOC ecosystem.

Another distinguishing characteristic of North America is its strong cybersecurity innovation ecosystem, supported by close collaboration among cloud providers, AI developers, cybersecurity vendors, venture capital firms, research institutions, and enterprise customers. The region continues to witness increasing investment in AI-focused cybersecurity startups, expansion of managed security services, and commercialization of agentic AI technologies for security operations. Financial services, healthcare, energy, manufacturing, and critical infrastructure organizations are among the earliest adopters of AI-enabled SOC capabilities, creating a favorable environment for technology validation and large-scale deployment. This collaborative innovation ecosystem is expected to accelerate commercialization of next-generation autonomous SOC technologies across the region.

JULY 2026 © MarketsandMarkets™

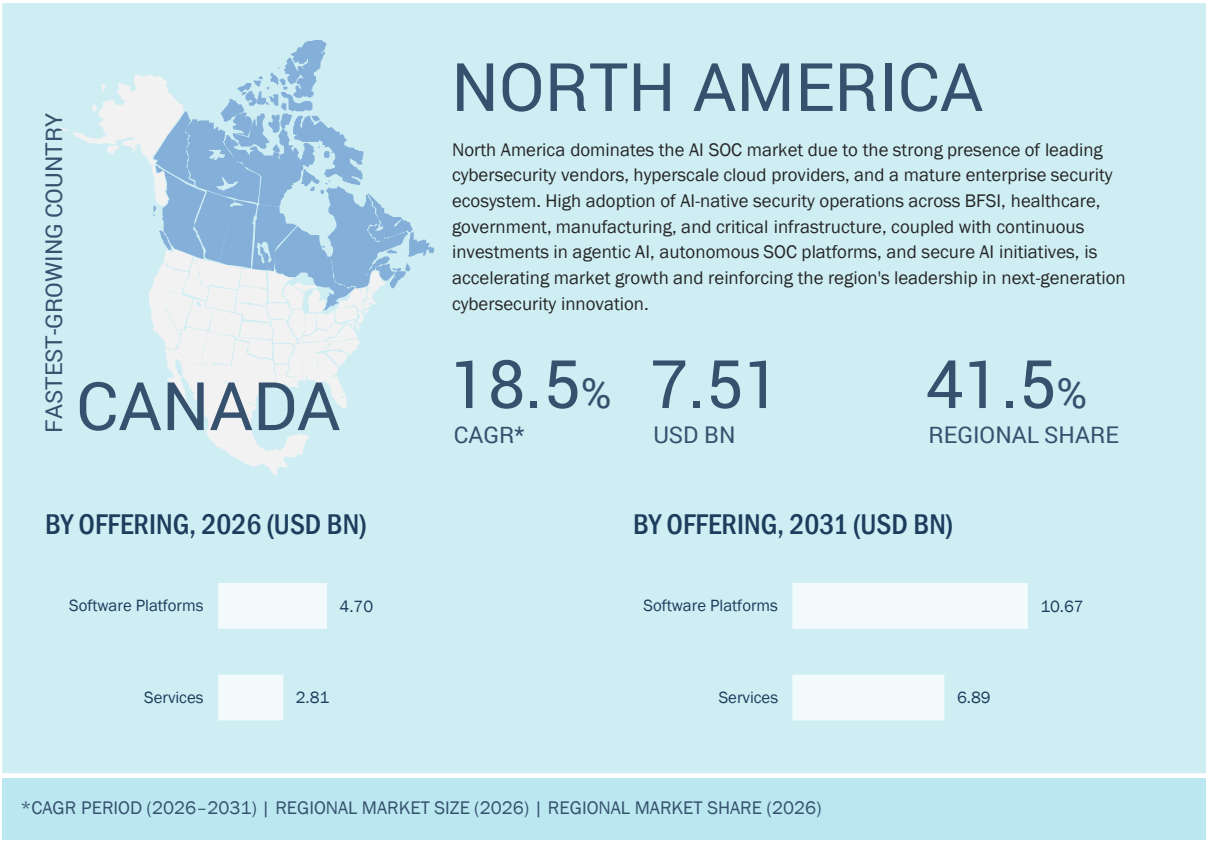
Looking ahead, North America is expected to maintain its leadership position through continuous investment in AI infrastructure, cybersecurity R&D, and advanced security operations. The growing convergence of AI, cloud computing, identity security, and threat intelligence is expected to drive demand for unified AI-native security platforms capable of providing real-time visibility and automated cyber defense across complex enterprise environments. Continued innovation from established vendors and emerging cybersecurity startups is expected to create significant growth opportunities for AI SOC providers throughout the forecast period.

13.2.1 NORTH AMERICA: AI SOC MARKET DRIVERS

- North America benefits from one of the world's most mature cybersecurity innovation ecosystems, supported by leading cloud providers, AI developers, cybersecurity vendors, venture capital investments, and research institutions. This collaborative environment accelerates the commercialization and adoption of AI-native SOC platforms, autonomous security agents, and next-generation threat detection technologies across enterprises.
- Organizations are increasing cybersecurity budgets to strengthen resilience against increasingly sophisticated AI-enabled threats. Enterprises are prioritizing investments in AI-driven security operations, cloud security, and security automation, creating sustained demand for AI SOC platforms capable of improving threat detection accuracy and operational efficiency.
- The growing adoption of autonomous AI agents across enterprises is transforming security operations throughout the region. Organizations are increasingly deploying AI agents to automate alert triage, investigations, and response workflows while simultaneously investing in platforms capable of securing both human and machine identities within increasingly autonomous enterprise environments.
- The widespread adoption of hybrid and multi-cloud infrastructures has significantly increased organizational attack surfaces. This is driving demand for AI SOC platforms that provide centralized visibility, continuous monitoring, and automated threat detection across cloud, on-premises, SaaS, and edge environments while improving security operations efficiency.
- Enterprises are increasingly partnering with Managed Security Service Providers (MSSPs) and Managed Detection and Response (MDR) providers to augment internal security teams. AI-powered SOC capabilities enable service providers to automate investigations, improve response times, and deliver scalable security operations, particularly for organizations facing cybersecurity talent shortages.
- North American enterprises are increasingly integrating AI SOC platforms with identity security, Zero Trust architectures, and threat intelligence platforms to strengthen cyber resilience. This convergence enables continuous risk assessment, contextual threat analysis, and adaptive security policies capable of protecting increasingly dynamic enterprise environments and autonomous AI workloads.

JULY 2026 © MarketsandMarkets™

FIGURE 39 NORTH AMERICA: AI SOC MARKET SNAPSHOT



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 110 NORTH AMERICA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	2,541.9	2,955.2	3,443.9	4,020.7	16.5%
Services	1,428.2	1,685.8	1,994.7	2,364.7	18.3%
Total	**3,970.1**	**4,641.1**	**5,438.6**	**6,385.3**	**17.2%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 111 NORTH AMERICA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	4,706.2	5,523.0	6,497.0	7,657.8	9,039.3	10,676.5	17.8%
Services	2,810.6	3,349.7	4,001.7	4,790.4	5,743.2	6,890.2	19.6%
Total	**7,516.8**	**8,872.7**	**10,498.8**	**12,448.2**	**14,782.6**	**17,566.7**	**18.5%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 112 NORTH AMERICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	944.7	1,052.1	1,172.2	1,313.2	11.6%
AI-orchestrated Response and Automation Platforms	391.8	444.2	504.4	574.4	13.6%
AI-native SOC Platforms	543.5	640.1	755.5	893.5	18.0%
AI SOC Agent Solutions	163.7	236.7	330.2	463.7	41.5%
Security Data Platforms	124.6	143.5	165.6	191.5	15.4%
Threat Intelligence Platforms	166.1	191.3	220.8	255.3	15.4%
AI Governance, Risk, and Compliance Solutions	207.4	247.4	295.1	329.1	16.6%
Total	**2,541.9**	**2,955.2**	**3,443.9**	**4,020.7**	**16.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 113 NORTH AMERICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	1,454.9	1,615.6	1,797.5	2,002.8	2,233.4	2,490.2	11.3%
AI-orchestrated Response and Automation Platforms	653.2	744.7	850.9	974.0	1,116.3	1,279.9	14.4%
AI-native SOC Platforms	1,058.6	1,257.6	1,497.4	1,786.3	2,134.1	2,551.1	19.2%
AI SOC Agent Solutions	602.6	785.3	1,025.7	1,342.5	1,759.7	2,308.1	30.8%
Security Data Platforms	221.8	257.7	300.1	350.1	409.1	478.3	16.6%
Threat Intelligence Platforms	295.8	343.6	400.1	466.8	545.5	637.7	16.6%
AI Governance, Risk, and Compliance Solutions	419.2	518.6	625.3	735.3	841.2	931.2	17.3%
Total	**4,706.2**	**5,523.0**	**6,497.0**	**7,657.8**	**9,039.3**	**10,676.5**	**17.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 114 NORTH AMERICA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	761.6	883.0	1,025.9	1,194.6	16.2%
AI SOC-as-a-Service (SOCaaS)	53.0	76.0	105.8	147.9	40.8%
Incident Response and Forensics Services	98.3	120.5	147.8	181.8	22.8%
Threat Intelligence and Advisory Services	515.3	606.4	715.2	840.4	17.7%
Total	**1,428.2**	**1,685.8**	**1,994.7**	**2,364.7**	**18.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 115 NORTH AMERICA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	1,392.3	1,626.8	1,905.3	2,235.7	2,627.1	3,088.7	17.3%
AI SOC-as-a-Service (SOCaaS)	193.8	254.2	333.8	438.5	576.5	757.6	31.3%
Incident Response and Forensics Services	223.0	274.3	338.1	417.4	516.1	638.3	23.4%
Threat Intelligence and Advisory Services	1,001.5	1,194.3	1,424.6	1,698.7	2,023.6	2,405.6	19.2%
Total	**2,810.6**	**3,349.7**	**4,001.7**	**4,790.4**	**5,743.2**	**6,890.2**	**19.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 116 NORTH AMERICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	2,828.2	3,259.0	3,764.5	4,356.3	15.5%
SMEs	1,141.9	1,382.1	1,674.1	2,029.0	21.1%
Total	**3,970.1**	**4,641.1**	**5,438.6**	**6,385.3**	**17.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 117 NORTH AMERICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	5,054.5	5,879.9	6,856.6	8,011.3	9,374.3	10,976.0	16.8%
SMEs	2,462.4	2,992.7	3,642.2	4,436.9	5,408.3	6,590.8	21.8%
Total	**7,516.8**	**8,872.7**	**10,498.8**	**12,448.2**	**14,782.6**	**17,566.7**	**18.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 118 NORTH AMERICA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	1,018.6	1,160.9	1,324.1	1,515.4	14.2%
Alert Triage and Prioritization	495.0	603.7	735.6	899.7	22.0%
Incident Investigation and Analysis	481.9	581.8	702.7	851.5	20.9%
Threat Hunting	309.2	365.4	432.8	513.8	18.4%
Incident Response and Remediation	492.5	568.3	657.2	761.6	15.6%
Insider Threat Detection	180.7	219.5	266.5	324.8	21.6%
Cloud Security Monitoring	334.2	383.0	439.6	506.0	14.8%
Identity and Access Monitoring	184.3	222.1	267.8	323.8	20.7%
Compliance Monitoring and Reporting	102.8	127.7	158.0	196.6	24.1%
Security Analytics and Visualization	370.9	408.7	454.2	492.2	9.9%
Total	**3,970.1**	**4,641.1**	**5,438.6**	**6,385.3**	**17.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 119 NORTH AMERICA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	1,731.9	1,984.3	2,278.5	2,621.0	3,018.8	3,478.4	15.0%
Alert Triage and Prioritization	1,096.3	1,339.1	1,639.2	2,010.1	2,468.0	3,031.6	22.6%
Incident Investigation and Analysis	1,030.3	1,249.8	1,519.4	1,850.7	2,257.4	2,754.7	21.7%
Threat Hunting	611.1	728.9	871.4	1,043.9	1,252.4	1,503.6	19.7%
Incident Response and Remediation	884.2	1,029.3	1,201.0	1,404.2	1,644.1	1,926.3	16.9%
Insider Threat Detection	394.8	481.0	587.3	718.4	879.8	1,078.1	22.3%
Cloud Security Monitoring	582.6	672.5	778.1	902.0	1,047.0	1,216.1	15.9%
Identity and Access Monitoring	391.2	473.9	575.3	699.8	852.3	1,038.7	21.6%
Compliance Monitoring and Reporting	242.3	299.3	370.5	459.3	570.0	707.6	23.9%
Security Analytics and Visualization	552.1	614.7	678.1	739.0	792.6	831.7	8.5%
Total	**7,516.8**	**8,872.7**	**10,498.8**	**12,448.2**	**14,782.6**	**17,566.7**	**18.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 120 NORTH AMERICA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	734.6	843.1	969.8	1,117.9	15.0%
Government & Defense	630.9	719.0	820.9	939.5	14.2%
Healthcare & Life sciences	505.7	613.6	746.5	909.3	21.6%
IT & Telecommunications	441.3	507.7	585.2	676.1	15.3%
Manufacturing	387.9	435.9	490.3	553.2	12.6%
Retail & eCommerce	290.9	345.4	411.0	490.0	19.0%
Energy & Utilities	269.2	321.3	384.4	460.7	19.6%
Media & Entertainment	203.4	239.9	283.7	336.0	18.2%
Education	161.4	193.7	232.7	280.2	20.2%
Other Verticals	344.7	421.6	514.2	622.4	21.8%
Total	**3,970.1**	**4,641.1**	**5,438.6**	**6,385.3**	**17.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 121 NORTH AMERICA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	1,289.9	1,492.2	1,730.2	2,010.0	2,338.2	2,721.5	16.1%
Government & Defense	1,074.5	1,231.9	1,415.3	1,628.9	1,876.9	2,163.4	15.0%
Healthcare & Life sciences	1,110.3	1,358.9	1,666.7	2,047.8	2,519.2	3,100.3	22.8%
IT & Telecommunications	782.1	907.1	1,054.6	1,228.3	1,432.8	1,672.2	16.4%
Manufacturing	620.6	697.4	784.9	884.2	996.3	1,122.0	12.6%
Retail & eCommerce	585.3	700.9	841.3	1,011.9	1,218.8	1,469.0	20.2%
Energy & Utilities	553.5	666.8	805.1	974.0	1,180.1	1,430.5	20.9%
Media & Entertainment	399.1	475.1	567.1	678.2	812.3	973.6	19.5%
Education	337.6	407.7	493.6	598.5	726.7	882.9	21.2%
Other Verticals	764.0	934.7	1,140.1	1,386.5	1,681.2	2,031.3	21.6%
Total	**7,516.8**	**8,872.7**	**10,498.8**	**12,448.2**	**14,782.6**	**17,566.7**	**18.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 122 NORTH AMERICA: AI SOC MARKET, BY COUNTRY, 2022–2025 (USD MILLION)

Country	2022	2023	2024	2025	CAGR (2022–2025)
US	3,057.3	3,556.9	4,148.0	4,846.6	16.6%
Canada	912.8	1,084.2	1,290.6	1,538.8	19.0%
Total	**3,970.1**	**4,641.1**	**5,438.6**	**6,385.3**	**17.2%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 123 NORTH AMERICA: AI SOC MARKET, BY COUNTRY, 2026–2031 (USD MILLION)

Country	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
US	5,677.7	6,669.1	7,852.6	9,264.7	10,947.6	12,944.7	17.9%
Canada	1,839.2	2,203.6	2,646.2	3,183.5	3,835.0	4,622.1	20.2%
Total	**7,516.8**	**8,872.7**	**10,498.8**	**12,448.2**	**14,782.6**	**17,566.7**	**18.5%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

13.2.2 US

13.2.2.1 Federal AI cybersecurity modernization accelerating autonomous SOC adoption

The US is at the forefront of AI SOC adoption, supported by a robust cybersecurity ecosystem, significant enterprise security investments, and the presence of global technology and cybersecurity leaders such as Microsoft, Google, Palo Alto Networks, CrowdStrike, Cisco, IBM, SentinelOne, Fortinet, and Trellix. Enterprises across critical infrastructure, financial services, healthcare, defense, and technology sectors are rapidly transitioning from conventional security operations centers to AI-native SOCs to combat increasingly sophisticated AI-powered cyberattacks, ransomware, and identity-based threats. The country's mature cloud infrastructure, thriving cybersecurity startup ecosystem, and continuous investments in generative AI, autonomous security agents, and AI copilots are accelerating the commercialization and deployment of next-generation security operations platforms.

The AI SOC landscape in the US is further strengthened by an evolving federal policy framework that positions AI as a strategic pillar of national cybersecurity. In July 2025, the White House introduced America's AI Action Plan, outlining more than 90 federal actions to accelerate AI innovation, strengthen AI infrastructure, and enhance national security while directing agencies to expand the secure adoption of AI technologies. Building on this strategy, the administration launched the Gold Eagle initiative in July 2026, a national cybersecurity clearinghouse that enables AI developers, federal agencies, software vendors, and critical infrastructure operators to collaboratively identify, prioritize, and remediate software vulnerabilities discovered using advanced AI models. The initiative, established under the Executive Order on Promoting Advanced Artificial Intelligence Innovation and Security, reflects the United States' shift toward collaborative, AI-enabled cyber defense and reinforces its leadership in autonomous security operations. These policy initiatives, combined with continuous innovation from domestic technology leaders and strong public-private collaboration, are expected to sustain the country's position as the largest and most influential AI SOC market throughout the forecast period.

TABLE 124 US: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	1,942.4	2,247.0	2,605.5	3,026.5	15.9%
Services	1,114.9	1,309.9	1,542.6	1,820.1	17.7%
Total	**3,057.3**	**3,556.9**	**4,148.0**	**4,846.6**	**16.6%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 125 US: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	3,524.5	4,115.1	4,815.9	5,646.7	6,630.4	7,789.8	17.2%
Services	2,153.1	2,553.9	3,036.7	3,618.0	4,317.2	5,154.9	19.1%
Total	**5,677.7**	**6,669.1**	**7,852.6**	**9,264.7**	**10,947.6**	**12,944.7**	**17.9%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 126 US: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	724.1	801.3	886.9	988.5	10.9%
AI-orchestrated Response and Automation Platforms	299.7	337.9	381.6	432.4	13.0%
AI-native SOC Platforms	415.4	486.7	571.6	672.6	17.4%
AI SOC Agent Solutions	129.4	191.4	270.3	384.3	43.7%
Security Data Platforms	95.2	109.1	125.3	144.1	14.8%
Threat Intelligence Platforms	127.0	145.5	167.0	192.2	14.8%
AI Governance, Risk, and Compliance Solutions	151.6	175.1	202.8	212.5	11.9%
Total	**1,942.4**	**2,247.0**	**2,605.5**	**3,026.5**	**15.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 127 US: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	1,085.2	1,194.5	1,317.8	1,456.6	1,612.4	1,785.8	10.5%
AI-orchestrated Response and Automation Platforms	488.7	553.8	629.0	715.8	815.7	930.1	13.7%
AI-native SOC Platforms	792.7	936.7	1,109.4	1,316.5	1,564.5	1,860.2	18.6%
AI SOC Agent Solutions	497.2	645.0	838.6	1,092.5	1,425.2	1,860.2	30.2%
Security Data Platforms	166.1	192.0	222.4	258.1	299.9	348.8	16.0%
Threat Intelligence Platforms	221.5	256.0	296.5	344.1	399.9	465.1	16.0%
AI Governance, Risk, and Compliance Solutions	273.1	337.3	402.2	463.2	512.8	539.5	14.6%
Total	**3,524.5**	**4,115.1**	**4,815.9**	**5,646.7**	**6,630.4**	**7,789.8**	**17.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 128 US: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	601.2	694.2	803.2	931.7	15.7%
AI SOC-as-a-Service (SOCaaS)	34.8	51.8	73.8	105.9	44.9%
Incident Response and Forensics Services	74.7	91.3	111.6	136.8	22.3%
Threat Intelligence and Advisory Services	404.2	472.6	554.0	645.6	16.9%
Total	**1,114.9**	**1,309.9**	**1,542.6**	**1,820.1**	**17.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 129 US: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	1,081.2	1,258.2	1,467.6	1,715.4	2,008.0	2,352.1	16.8%
AI SOC-as-a-Service (SOCaaS)	138.9	182.7	240.9	318.3	421.2	557.7	32.0%
Incident Response and Forensics Services	167.2	204.7	251.3	309.2	381.0	469.7	23.0%
Threat Intelligence and Advisory Services	765.8	908.3	1,076.8	1,275.1	1,507.0	1,775.4	18.3%
Total	**2,153.1**	**2,553.9**	**3,036.7**	**3,618.0**	**4,317.2**	**5,154.9**	**19.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 130 US: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	2,205.9	2,530.2	2,909.2	3,351.3	15.0%
SMEs	851.4	1,026.6	1,238.8	1,495.3	20.6%
Total	**3,057.3**	**3,556.9**	**4,148.0**	**4,846.6**	**16.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 131 US: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	3,870.7	4,482.6	5,203.9	6,053.3	7,052.2	8,221.3	16.3%
SMEs	1,806.9	2,186.4	2,648.7	3,211.4	3,895.4	4,723.4	21.2%
Total	**5,677.7**	**6,669.1**	**7,852.6**	**9,264.7**	**10,947.6**	**12,944.7**	**17.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 132 US: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	793.6	900.1	1,022.7	1,165.8	13.7%
Alert Triage and Prioritization	373.9	453.6	550.7	671.0	21.5%
Incident Investigation and Analysis	365.7	439.2	528.3	637.4	20.3%
Threat Hunting	236.9	278.6	328.5	388.0	17.9%
Incident Response and Remediation	381.5	438.1	504.4	581.9	15.1%
Insider Threat Detection	136.7	165.2	199.9	242.6	21.1%
Cloud Security Monitoring	259.7	296.2	338.6	388.0	14.3%
Identity and Access Monitoring	140.0	167.8	201.5	242.6	20.1%
Compliance Monitoring and Reporting	77.0	95.1	117.4	145.7	23.7%
Security Analytics and Visualization	292.6	322.9	356.1	383.7	9.5%
Total	**3,057.3**	**3,556.9**	**4,148.0**	**4,846.6**	**16.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 133 US: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	1,326.0	1,512.3	1,728.9	1,980.5	2,272.2	2,608.6	14.5%
Alert Triage and Prioritization	813.3	988.5	1,204.3	1,470.2	1,797.5	2,199.2	22.0%
Incident Investigation and Analysis	767.3	926.1	1,120.5	1,358.4	1,649.4	2,004.0	21.2%
Threat Hunting	459.2	545.0	648.3	772.8	922.7	1,102.3	19.1%
Incident Response and Remediation	672.3	778.8	904.5	1,052.5	1,226.6	1,430.5	16.3%
Insider Threat Detection	293.3	355.6	432.1	526.1	641.6	782.9	21.7%
Cloud Security Monitoring	444.6	510.8	588.3	678.9	784.7	907.6	15.3%
Identity and Access Monitoring	291.6	351.4	424.6	514.0	623.2	756.1	21.0%
Compliance Monitoring and Reporting	178.6	219.5	270.5	334.0	413.0	511.1	23.4%
Security Analytics and Visualization	431.5	481.1	530.6	577.3	616.7	642.4	8.3%
Total	**5,677.7**	**6,669.1**	**7,852.6**	**9,264.7**	**10,947.6**	**12,944.7**	**17.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 134 US: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	574.9	657.2	752.7	864.3	14.6%
Government & Defense	496.9	564.2	641.7	732.0	13.8%
Healthcare & Life sciences	375.7	453.5	548.7	665.1	21.0%
IT & Telecommunications	344.8	394.9	453.3	521.5	14.8%
Manufacturing	309.1	346.5	388.8	438.2	12.3%
Retail & eCommerce	220.8	260.9	309.0	366.7	18.4%
Energy & Utilities	203.3	241.4	287.4	342.7	19.0%
Media & Entertainment	155.3	182.3	214.5	252.9	17.7%
Education	121.4	144.9	173.4	207.9	19.7%
Other Verticals	255.0	311.0	378.5	455.2	21.3%
Total	**3,057.3**	**3,556.9**	**4,148.0**	**4,846.6**	**16.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 135 US: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	992.9	1,143.7	1,320.6	1,527.9	1,770.4	2,052.7	15.6%
Government & Defense	833.9	952.4	1,090.4	1,250.7	1,436.7	1,651.4	14.6%
Healthcare & Life sciences	808.4	985.2	1,203.6	1,473.3	1,806.3	2,215.9	22.3%
IT & Telecommunications	600.6	693.6	802.8	931.1	1,081.6	1,257.1	15.9%
Manufacturing	490.1	549.6	617.5	695.1	783.3	883.0	12.5%
Retail & eCommerce	435.8	519.4	620.4	742.5	890.1	1,067.6	19.6%
Energy & Utilities	409.7	491.2	590.3	710.8	857.2	1,034.5	20.3%
Media & Entertainment	298.9	354.1	420.6	500.5	596.5	711.3	18.9%
Education	249.3	299.6	361.0	435.7	526.7	637.0	20.6%
Other Verticals	557.9	680.2	825.4	997.0	1,198.9	1,434.2	20.8%
Total	**5,677.7**	**6,669.1**	**7,852.6**	**9,264.7**	**10,947.6**	**12,944.7**	**17.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.2.3 CANADA

13.2.3.1 National cybersecurity strategy and trusted AI governance strengthening AI SOC growth

Canada's AI SOC market is evolving through a strong emphasis on cyber resilience, trusted AI adoption, and collaborative security operations. Unlike the United States, where innovation is largely driven by federal cyber defense programs, Canada is focusing on strengthening cybersecurity through national governance frameworks and public-private collaboration. In February 2025, the Government of Canada launched its new National Cyber Security Strategy (NCSS), built around a whole-of-society approach that brings together government agencies, critical infrastructure operators, academia, Indigenous communities, and the private sector. As part of the strategy, the government established the Canadian Cyber Defence Collective to enhance threat intelligence sharing, improve coordinated cyber response, and strengthen national cyber resilience. The strategy also supports initiatives such as the Cyber Security Innovation Network, Digital Technology Supercluster, and Cyber Security Cooperation Program to expand cybersecurity innovation and develop a skilled cyber workforce.

Canada is also positioning itself as a global leader in responsible AI by integrating AI governance with cybersecurity modernization. In June 2026, the federal government introduced AI for All, Canada's new national AI strategy, aimed at accelerating enterprise AI adoption while prioritizing trustworthy AI, digital sovereignty, and secure AI infrastructure. Complementing this initiative, the Canadian Centre for Cyber Security (Cyber Centre) has issued new guidance on securing AI deployments and has urged organizations operating critical infrastructure to strengthen defenses against risks associated with frontier AI models. Canada's financial sector is already responding to these developments, with regulators encouraging banks and insurers to enhance AI-driven cyber risk management as advanced AI systems reduce the time available to detect and respond to sophisticated attacks. These initiatives are expected to accelerate the adoption of AI-enabled SOC platforms across banking, government, healthcare, energy, and other critical sectors while reinforcing Canada's position as a trusted market for AI-driven cybersecurity solutions.

TABLE 136 CANADA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	599.6	708.2	838.4	994.2	18.4%
Services	313.3	376.0	452.1	544.6	20.2%
Total	**912.8**	**1,084.2**	**1,290.6**	**1,538.8**	**19.0%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 137 CANADA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	1,181.6	1,407.9	1,681.2	2,011.1	2,409.0	2,886.8	19.6%
Services	657.5	795.7	965.0	1,172.4	1,426.0	1,735.3	21.4%
Total	**1,839.2**	**2,203.6**	**2,646.2**	**3,183.5**	**3,835.0**	**4,622.1**	**20.2%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 138 CANADA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	220.6	250.8	285.4	324.7	13.8%
AI-orchestrated Response and Automation Platforms	92.1	106.3	122.8	142.0	15.5%
AI-native SOC Platforms	128.1	153.4	183.9	220.9	19.9%
AI SOC Agent Solutions	34.3	45.3	59.9	79.4	32.2%
Security Data Platforms	29.4	34.4	40.3	47.3	17.2%
Threat Intelligence Platforms	39.2	45.8	53.7	63.1	17.2%
AI Governance, Risk, and Compliance Solutions	55.8	72.2	92.3	116.7	27.9%
Total	**599.6**	**708.2**	**838.4**	**994.2**	**18.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 139 CANADA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	369.7	421.1	479.7	546.1	621.0	704.5	13.8%
AI-orchestrated Response and Automation Platforms	164.5	191.0	222.0	258.2	300.6	349.8	16.3%
AI-native SOC Platforms	265.9	320.9	388.0	469.8	569.6	690.8	21.0%
AI SOC Agent Solutions	105.4	140.3	187.1	250.0	334.6	447.9	33.6%
Security Data Platforms	55.7	65.7	77.7	92.1	109.2	129.5	18.4%
Threat Intelligence Platforms	74.3	87.7	103.6	122.7	145.5	172.6	18.4%
AI Governance, Risk, and Compliance Solutions	146.1	181.3	223.1	272.1	328.4	391.7	21.8%
Total	**1,181.6**	**1,407.9**	**1,681.2**	**2,011.1**	**2,409.0**	**2,886.8**	**19.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 140 CANADA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	160.4	188.8	222.7	262.9	17.9%
AI SOC-as-a-Service (SOCaaS)	18.2	24.3	32.0	42.0	32.1%
Incident Response and Forensics Services	23.6	29.2	36.2	44.9	24.0%
Threat Intelligence and Advisory Services	111.1	133.7	161.2	194.7	20.6%
Total	**313.3**	**376.0**	**452.1**	**544.6**	**20.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 141 CANADA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	311.0	368.7	437.7	520.4	619.1	736.5	18.8%
AI SOC-as-a-Service (SOCaaS)	54.9	71.5	92.8	120.2	155.3	199.9	29.5%
Incident Response and Forensics Services	55.9	69.6	86.7	108.2	135.1	168.7	24.7%
Threat Intelligence and Advisory Services	235.7	286.0	347.7	423.5	516.5	630.1	21.7%
Total	**657.5**	**795.7**	**965.0**	**1,172.4**	**1,426.0**	**1,735.3**	**21.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 142 CANADA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	622.3	728.7	855.3	1,005.0	17.3%
SMEs	290.5	355.4	435.3	533.7	22.5%
Total	**912.8**	**1,084.2**	**1,290.6**	**1,538.8**	**19.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 143 CANADA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	1,183.7	1,397.3	1,652.7	1,958.0	2,322.1	2,754.7	18.4%
SMEs	655.4	806.3	993.5	1,225.5	1,512.8	1,867.4	23.3%
Total	**1,839.2**	**2,203.6**	**2,646.2**	**3,183.5**	**3,835.0**	**4,622.1**	**20.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 144 CANADA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	225.1	260.8	301.4	349.6	15.8%
Alert Triage and Prioritization	121.2	150.1	184.9	228.7	23.6%
Incident Investigation and Analysis	116.3	142.6	174.4	214.1	22.6%
Threat Hunting	72.3	86.8	104.4	125.8	20.3%
Incident Response and Remediation	111.0	130.2	152.8	179.8	17.4%
Insider Threat Detection	44.0	54.3	66.7	82.2	23.2%
Cloud Security Monitoring	74.5	86.8	101.1	118.0	16.6%
Identity and Access Monitoring	44.3	54.3	66.3	81.2	22.4%
Compliance Monitoring and Reporting	25.8	32.6	40.6	50.9	25.4%
Security Analytics and Visualization	78.4	85.8	98.1	108.5	11.4%
Total	**912.8**	**1,084.2**	**1,290.6**	**1,538.8**	**19.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 145 CANADA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	405.9	472.0	549.6	640.5	746.6	869.8	16.5%
Alert Triage and Prioritization	283.0	350.6	434.9	539.9	670.5	832.4	24.1%
Incident Investigation and Analysis	263.0	323.7	398.9	492.3	608.0	750.7	23.3%
Threat Hunting	151.9	183.9	223.0	271.0	329.8	401.4	21.5%
Incident Response and Remediation	212.0	250.4	296.5	351.7	417.5	495.9	18.5%
Insider Threat Detection	101.5	125.4	155.2	192.3	238.3	295.2	23.8%
Cloud Security Monitoring	138.0	161.7	189.8	223.0	262.3	308.5	17.5%
Identity and Access Monitoring	99.6	122.5	150.7	185.8	229.1	282.6	23.2%
Compliance Monitoring and Reporting	63.7	79.8	100.0	125.3	157.0	196.5	25.3%
Security Analytics and Visualization	120.6	133.6	147.4	161.7	175.9	189.2	9.4%
Total	**1,839.2**	**2,203.6**	**2,646.2**	**3,183.5**	**3,835.0**	**4,622.1**	**20.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 146 CANADA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	159.6	185.9	217.0	253.6	16.7%
Government & Defense	134.1	154.8	179.2	207.5	15.7%
Healthcare & Life sciences	130.0	160.2	197.8	244.2	23.4%
IT & Telecommunications	96.6	112.8	131.9	154.6	17.0%
Manufacturing	78.8	89.3	101.5	115.1	13.4%
Retail & eCommerce	70.1	84.4	102.0	123.3	20.7%
Energy & Utilities	65.9	79.9	97.0	118.0	21.4%
Media & Entertainment	48.1	57.6	69.1	83.1	20.0%
Education	40.1	48.7	59.3	72.3	21.7%
Other Verticals	89.7	110.6	135.7	167.2	23.1%
Total	**912.8**	**1,084.2**	**1,290.6**	**1,538.8**	**19.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 147 CANADA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	297.0	348.4	409.5	482.0	567.8	668.9	17.6%
Government & Defense	240.6	279.4	324.9	378.2	440.2	512.0	16.3%
Healthcare & Life sciences	301.9	373.7	463.1	574.5	712.9	884.4	24.0%
IT & Telecommunications	181.5	213.6	251.7	297.2	351.2	415.1	18.0%
Manufacturing	130.4	147.8	167.4	189.1	213.1	239.0	12.9%
Retail & eCommerce	149.4	181.5	220.9	269.3	328.8	401.4	21.9%
Energy & Utilities	143.8	175.6	214.8	263.2	322.8	396.0	22.5%
Media & Entertainment	100.2	121.0	146.5	177.7	215.9	262.3	21.2%
Education	88.3	108.1	132.6	162.8	200.0	245.9	22.7%
Other Verticals	206.1	254.5	314.7	389.4	482.3	597.1	23.7%
Total	**1,839.2**	**2,203.6**	**2,646.2**	**3,183.5**	**3,835.0**	**4,622.1**	**20.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.3 EUROPE

Europe is emerging as a regulation-led market for AI SOCs, where cybersecurity modernization is being shaped by harmonized digital legislation and a strong emphasis on operational resilience. Unlike other regions that primarily focus on technology adoption, the European market is increasingly driven by compliance requirements that encourage organizations to modernize security operations using AI-enabled monitoring, threat detection, and automated incident response. The implementation of the NIS2 Directive, the Digital Operational Resilience Act (DORA) for the financial sector, and the phased rollout of the EU AI Act are accelerating investments in intelligent SOC capabilities across critical sectors, including energy, transportation, healthcare, manufacturing, telecommunications, and public administration. Together, these regulations are encouraging organizations to deploy AI SOC platforms capable of continuous monitoring, faster incident reporting, and enhanced cyber resilience.

Europe is also strengthening its regional cybersecurity capabilities through coordinated initiatives led by the European Commission and the European Union Agency for Cybersecurity (ENISA). During 2025-2026, ENISA expanded its threat landscape assessments to address the growing use of AI by both defenders and adversaries, highlighting the increasing sophistication of AI-enabled phishing, malware, and social engineering attacks across the region. In July 2026, the European Commission introduced the EU Action Plan on Cybersecurity and Artificial Intelligence, promoting the secure adoption of AI for vulnerability detection, cyber defense, and incident response while reinforcing implementation of existing legislation such as NIS2 and the Cyber Resilience Act. These initiatives are fostering greater collaboration among Member States and encouraging enterprises to integrate AI into security operations without compromising governance, transparency, or resilience.

Looking ahead, Europe is expected to witness significant demand for AI-native SOC platforms as organizations seek unified solutions that combine threat intelligence, security analytics, automation, and regulatory compliance. The region's focus on digital sovereignty, trusted AI, cybersecurity certification, and secure digital infrastructure is creating opportunities for both established cybersecurity vendors and emerging European AI security companies. As enterprises continue to align cybersecurity strategies with evolving EU regulations and cross-border resilience objectives, Europe is expected to remain one of the prominent markets for AI SOC solutions.

13.3.1 EUROPE: AI SOC MARKET DRIVERS

- The implementation of the NIS2 Directive, Digital Operational Resilience Act (DORA), Cyber Resilience Act (CRA), and EU AI Act is compelling organizations across Europe to modernize security operations with AI-driven monitoring, automated incident response, and continuous cyber resilience capabilities to meet increasingly stringent regulatory obligations.
- European governments are investing in sovereign AI capabilities, secure digital infrastructure, and trusted AI ecosystems to reduce strategic technology dependencies while strengthening cybersecurity resilience. These initiatives are creating favorable conditions for the deployment of AI-native SOC platforms that align with the region's governance and security objectives.
- Critical sectors including energy, transportation, healthcare, finance, telecommunications, and public administration are strengthening cyber resilience against increasingly sophisticated threats. This is driving demand for AI-enabled security operations that provide continuous monitoring, rapid threat detection, and automated response across complex and distributed digital environments.
- Europe continues to expand investments in AI Factories, future AI Gigafactories, cybersecurity research, and collaborative innovation programs. These initiatives are accelerating the development of indigenous AI-powered cybersecurity technologies while creating new opportunities for regional AI SOC vendors, research institutions, and technology providers.

JULY 2026 © MarketsandMarkets™

- European enterprises are modernizing legacy IT environments through secure cloud transformation and resilience-focused cybersecurity strategies. The convergence of hybrid cloud, Zero Trust architectures, AI-driven security analytics, and automated security operations is increasing enterprise demand for intelligent SOC platforms capable of protecting highly regulated digital ecosystems.
- Cross-border collaboration among the European Commission, ENISA, Member States, industry, and research organizations is accelerating the adoption of AI for cyber defense. Regional initiatives focused on AI model evaluation, secure AI testing, threat intelligence sharing, and coordinated incident response are strengthening Europe's collective cybersecurity capabilities and driving investments in AI SOC solutions.

TABLE 148 EUROPE: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	1,468.6	1,728.2	2,038.4	2,409.0	17.9%
Services	806.6	964.0	1,154.7	1,385.9	19.8%
Total	**2,275.2**	**2,692.2**	**3,193.1**	**3,794.9**	**18.6%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 149 EUROPE: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	2,852.8	3,387.3	4,031.4	4,807.6	5,741.7	6,861.5	19.2%
Services	1,666.9	2,010.2	2,430.1	2,943.4	3,570.7	4,334.4	21.1%
Total	**4,519.7**	**5,397.5**	**6,461.5**	**7,751.0**	**9,312.4**	**11,195.9**	**19.9%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 150 EUROPE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	544.0	614.2	693.8	786.8	13.1%
AI-orchestrated Response and Automation Platforms	226.2	259.6	298.6	344.1	15.0%
AI-native SOC Platforms	313.9	374.3	447.2	535.3	19.5%
AI SOC Agent Solutions	91.2	129.5	179.6	250.6	40.1%
Security Data Platforms	72.0	83.9	98.0	114.7	16.8%
Threat Intelligence Platforms	96.0	111.9	130.7	153.0	16.8%
AI Governance, Risk, and Compliance Solutions	125.2	154.8	190.6	224.4	21.5%
Total	**1,468.6**	**1,728.2**	**2,038.4**	**2,409.0**	**17.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 151 EUROPE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	885.3	997.9	1,126.3	1,272.4	1,437.7	1,623.2	12.9%
AI-orchestrated Response and Automation Platforms	396.4	457.6	529.3	613.3	711.4	825.3	15.8%
AI-native SOC Platforms	641.8	771.5	929.5	1,122.0	1,356.2	1,640.2	20.6%
AI SOC Agent Solutions	330.2	436.1	577.6	766.3	1,018.3	1,354.2	32.6%
Security Data Platforms	134.5	158.1	186.3	219.9	260.0	307.5	18.0%
Threat Intelligence Platforms	179.3	210.8	248.4	293.2	346.6	410.0	18.0%
AI Governance, Risk, and Compliance Solutions	285.3	355.3	434.1	520.6	611.5	701.1	19.7%
Total	**2,852.8**	**3,387.3**	**4,031.4**	**4,807.6**	**5,741.7**	**6,861.5**	**19.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 152 EUROPE: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	424.9	498.6	586.2	690.7	17.6%
AI SOC-as-a-Service (SOCaaS)	35.1	49.2	67.5	92.8	38.3%
Incident Response and Forensics Services	57.1	70.7	87.6	108.9	24.0%
Threat Intelligence and Advisory Services	289.5	345.5	413.3	493.4	19.4%
Total	**806.6**	**964.0**	**1,154.7**	**1,385.9**	**19.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 153 EUROPE: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	814.5	962.8	1,140.7	1,353.7	1,608.8	1,912.7	18.6%
AI SOC-as-a-Service (SOCaaS)	122.3	161.0	212.0	279.1	367.4	483.3	31.6%
Incident Response and Forensics Services	135.1	167.9	209.2	261.0	326.0	407.4	24.7%
Threat Intelligence and Advisory Services	595.0	718.5	868.2	1,049.6	1,268.5	1,531.1	20.8%
Total	**1,666.9**	**2,010.2**	**2,430.1**	**2,943.4**	**3,570.7**	**4,334.4**	**21.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 154 EUROPE: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	1,598.9	1,865.1	2,180.7	2,554.6	16.9%
SMEs	676.3	827.2	1,012.4	1,240.4	22.4%
Total	**2,275.2**	**2,692.2**	**3,193.1**	**3,794.9**	**18.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 155 EUROPE: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	2,998.6	3,529.1	4,163.1	4,920.5	5,824.1	6,897.7	18.1%
SMEs	1,521.1	1,868.4	2,298.4	2,830.6	3,488.3	4,298.2	23.1%
Total	**4,519.7**	**5,397.5**	**6,461.5**	**7,751.0**	**9,312.4**	**11,195.9**	**19.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 156 EUROPE: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	576.6	665.3	767.5	888.6	15.5%
Alert Triage and Prioritization	289.5	357.3	439.9	543.9	23.4%
Incident Investigation and Analysis	280.5	342.7	418.5	512.9	22.3%
Threat Hunting	178.1	213.1	255.4	306.9	19.9%
Incident Response and Remediation	280.5	327.6	383.4	449.8	17.0%
Insider Threat Detection	105.5	129.7	159.1	196.1	23.0%
Cloud Security Monitoring	189.7	220.1	255.6	297.7	16.2%
Identity and Access Monitoring	107.2	130.7	159.3	194.9	22.1%
Compliance Monitoring and Reporting	60.6	76.2	95.2	119.6	25.4%
Security Analytics and Visualization	207.1	229.6	259.1	284.7	11.2%
Total	**2,275.2**	**2,692.2**	**3,193.1**	**3,794.9**	**18.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 157 EUROPE: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	1,027.7	1,191.3	1,383.7	1,609.7	1,874.6	2,183.6	16.3%
Alert Triage and Prioritization	670.5	828.3	1,025.2	1,270.9	1,577.2	1,957.6	23.9%
Incident Investigation and Analysis	627.8	770.3	947.2	1,166.6	1,438.6	1,774.6	23.1%
Threat Hunting	369.3	445.5	538.9	653.0	792.6	962.5	21.1%
Incident Response and Remediation	528.3	622.2	734.5	868.8	1,029.1	1,219.7	18.2%
Insider Threat Detection	241.1	297.1	366.9	453.7	561.7	695.6	23.6%
Cloud Security Monitoring	346.8	405.0	474.1	555.9	652.7	766.6	17.2%
Identity and Access Monitoring	238.2	291.9	358.4	440.8	542.9	668.8	22.9%
Compliance Monitoring and Reporting	149.1	186.3	233.0	291.9	365.8	458.5	25.2%
Security Analytics and Visualization	320.9	359.5	399.7	439.7	477.3	508.4	9.6%
Total	**4,519.7**	**5,397.5**	**6,461.5**	**7,751.0**	**9,312.4**	**11,195.9**	**19.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 158 EUROPE: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	413.7	480.5	559.2	652.2	16.4%
Government & Defense	353.0	406.8	469.9	543.8	15.5%
Healthcare & Life sciences	300.5	369.1	454.3	559.7	23.0%
IT & Telecommunications	249.1	289.9	338.2	395.4	16.7%
Manufacturing	214.2	243.1	276.3	314.7	13.7%
Retail & eCommerce	169.2	203.3	244.7	295.2	20.4%
Energy & Utilities	157.4	190.1	230.2	279.2	21.0%
Media & Entertainment	117.6	140.4	167.9	201.4	19.6%
Education	94.8	115.0	139.8	170.2	21.5%
Other Verticals	205.7	254.0	312.5	383.1	23.0%
Total	**2,275.2**	**2,692.2**	**3,193.1**	**3,794.9**	**18.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 159 EUROPE: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	761.3	890.9	1,044.9	1,227.6	1,444.3	1,699.9	17.4%
Government & Defense	629.0	729.3	847.2	985.5	1,147.7	1,336.8	16.3%
Healthcare & Life sciences	690.7	854.1	1,058.2	1,313.0	1,630.9	2,026.3	24.0%
IT & Telecommunications	462.7	542.9	638.5	752.2	887.4	1,047.5	17.8%
Manufacturing	356.8	405.0	460.1	522.9	594.0	673.9	13.6%
Retail & eCommerce	356.7	432.0	524.5	638.0	777.1	947.2	21.6%
Energy & Utilities	339.2	413.2	504.4	617.0	755.7	926.1	22.2%
Media & Entertainment	241.9	291.3	351.7	425.5	515.5	625.0	20.9%
Education	207.4	253.2	309.9	379.9	466.3	572.6	22.5%
Other Verticals	474.1	585.6	722.2	889.4	1,093.2	1,340.6	23.1%
Total	**4,519.7**	**5,397.5**	**6,461.5**	**7,751.0**	**9,312.4**	**11,195.9**	**19.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 160 EUROPE: AI SOC MARKET, BY COUNTRY, 2022–2025 (USD MILLION)

Country	2022	2023	2024	2025	CAGR (2022–2025)
UK	542.3	636.4	748.4	882.0	17.6%
Germany	678.3	786.2	913.5	1,063.4	16.2%
France	387.3	466.0	561.9	678.9	20.6%
Italy	135.0	162.6	196.4	237.7	20.8%
Rest of Europe	532.3	641.0	772.9	932.9	20.6%
Total	**2,275.2**	**2,692.2**	**3,193.1**	**3,794.9**	**18.6%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 161 EUROPE: AI SOC MARKET, BY COUNTRY, 2026–2031 (USD MILLION)

Country	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
UK	1,041.5	1,233.1	1,463.4	1,740.0	2,072.1	2,469.3	18.8%
Germany	1,240.7	1,451.3	1,701.9	1,999.9	2,353.6	2,771.8	17.4%
France	822.1	998.1	1,214.8	1,477.3	1,801.8	2,199.4	21.8%
Italy	288.2	350.4	427.2	521.7	638.3	781.3	22.1%
Rest of Europe	1,127.3	1,364.6	1,654.2	2,012.1	2,446.6	2,974.1	21.4%
Total	**4,519.7**	**5,397.5**	**6,461.5**	**7,751.0**	**9,312.4**	**11,195.9**	**19.9%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.3.2 UK

13.3.2.1 Trusted AI governance and financial sector digitalization advancing intelligent security operations

The UK is positioning itself as a leading market for AI-powered security operations through its distinctive pro-innovation approach to AI regulation and strong focus on securing advanced AI systems. Unlike the European Union's comprehensive AI Act, the UK has adopted a principles-based regulatory framework that enables faster AI deployment while emphasizing cybersecurity, resilience, and responsible innovation. In February 2025, the government rebranded the AI Safety Institute as the AI Security Institute (AISI), expanding its mandate to evaluate frontier AI models against cybersecurity risks, including autonomous cyber capabilities and AI-enabled attacks. Complementing this initiative, the UK also published the Code of Practice for the Cyber Security of AI in January 2025, providing guidance for organizations to securely design, develop, deploy, and maintain AI systems throughout their lifecycle. These developments are encouraging enterprises to integrate AI securely into security operations while strengthening trust in AI-driven cybersecurity solutions.

The UK's AI SOC market is further supported by a well-established cybersecurity ecosystem, a highly digital financial sector, and increasing investments in sovereign AI infrastructure. Financial institutions, insurers, and other regulated enterprises are accelerating the adoption of AI-driven security operations to strengthen fraud detection, identity protection, and operational resilience against increasingly sophisticated cyber threats. To reinforce the country's AI capabilities, the UK government introduced the AI Opportunities Action Plan in 2025 and the UK Compute Roadmap, which outlines investments in sovereign compute infrastructure, AI Growth Zones, national supercomputing capabilities, and secure AI deployment across public and private sectors. Alongside established cybersecurity leaders such as Darktrace, Sophos, NCC Group, and BAE Systems Digital Intelligence, emerging AI SOC providers including Riversafe and SOC Jedi.AI are expanding AI-powered SOC, security monitoring, and threat detection capabilities for UK enterprises. This combination of government-backed AI infrastructure, a mature cybersecurity industry, and a growing ecosystem of AI-focused security providers is expected to strengthen the UK's position as one of Europe's leading markets for AI SOC solutions during the forecast period.

TABLE 162 UK: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	356.2	415.7	486.2	569.8	17.0%
Services	186.1	220.7	262.2	312.2	18.8%
Total	**542.3**	**636.4**	**748.4**	**882.0**	**17.6%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 163 UK: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	669.2	787.8	929.8	1,099.2	1,301.6	1,542.2	18.2%
Services	372.4	445.3	533.7	640.8	770.5	927.0	20.0%
Total	**1,041.5**	**1,233.1**	**1,463.4**	**1,740.0**	**2,072.1**	**2,469.3**	**18.8%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 164 UK: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	131.0	147.2	165.5	186.1	12.4%
AI-orchestrated Response and Automation Platforms	54.7	62.4	71.2	81.4	14.1%
AI-native SOC Platforms	76.1	90.0	106.7	126.6	18.5%
AI SOC Agent Solutions	20.4	26.6	34.8	45.5	30.6%
Security Data Platforms	17.5	20.2	23.4	27.1	15.8%
Threat Intelligence Platforms	23.3	26.9	31.2	36.2	15.8%
AI Governance, Risk, and Compliance Solutions	33.2	42.4	53.5	66.9	26.3%
Total	**356.2**	**415.7**	**486.2**	**569.8**	**17.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 165 UK: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	209.3	235.6	265.3	298.5	335.5	376.3	12.4%
AI-orchestrated Response and Automation Platforms	93.2	106.9	122.7	141.2	162.4	186.9	14.9%
AI-native SOC Platforms	150.6	179.6	214.6	256.8	307.8	369.1	19.6%
AI SOC Agent Solutions	59.7	78.5	103.5	136.7	180.8	239.3	32.0%
Security Data Platforms	31.6	36.8	43.0	50.3	59.0	69.2	17.0%
Threat Intelligence Platforms	42.1	49.1	57.3	67.1	78.6	92.2	17.0%
AI Governance, Risk, and Compliance Solutions	82.7	101.5	123.4	148.7	177.5	209.3	20.4%
Total	**669.2**	**787.8**	**929.8**	**1,099.2**	**1,301.6**	**1,542.2**	**18.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 166 UK: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	95.3	110.8	129.1	150.7	16.5%
AI SOC-as-a-Service (SOCaaS)	10.8	14.2	18.6	24.1	30.6%
Incident Response and Forensics Services	14.0	17.1	21.0	25.8	22.6%
Threat Intelligence and Advisory Services	66.0	78.5	93.5	111.6	19.1%
Total	**186.1**	**220.7**	**262.2**	**312.2**	**18.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 167 UK: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	176.1	206.3	242.1	284.4	334.5	393.5	17.4%
AI SOC-as-a-Service (SOCaaS)	31.1	40.0	51.3	65.7	83.9	106.8	28.0%
Incident Response and Forensics Services	31.6	38.9	48.0	59.2	73.0	90.1	23.3%
Threat Intelligence and Advisory Services	133.5	160.0	192.3	231.5	279.1	336.6	20.3%
Total	**372.4**	**445.3**	**533.7**	**640.8**	**770.5**	**927.0**	**20.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 168 UK: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	369.7	427.7	496.0	576.1	15.9%
SMEs	172.6	208.6	252.5	305.9	21.0%
Total	**542.3**	**636.4**	**748.4**	**882.0**	**17.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 169 UK: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	670.3	781.9	914.0	1,070.2	1,254.7	1,471.6	17.0%
SMEs	371.2	451.2	549.4	669.8	817.4	997.6	21.9%
Total	**1,041.5**	**1,233.1**	**1,463.4**	**1,740.0**	**2,072.1**	**2,469.3**	**18.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 170 UK: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	133.7	153.1	174.8	200.4	14.4%
Alert Triage and Prioritization	72.0	88.1	107.2	131.1	22.1%
Incident Investigation and Analysis	69.1	83.7	101.1	122.7	21.1%
Threat Hunting	42.9	50.9	60.5	72.1	18.9%
Incident Response and Remediation	65.9	76.4	88.6	103.0	16.0%
Insider Threat Detection	26.1	31.9	38.7	47.1	21.7%
Cloud Security Monitoring	44.3	50.9	58.6	67.6	15.2%
Identity and Access Monitoring	26.3	31.9	38.4	46.6	20.9%
Compliance Monitoring and Reporting	15.4	19.1	23.5	29.2	23.9%
Security Analytics and Visualization	46.6	50.4	56.9	62.2	10.1%
Total	**542.3**	**636.4**	**748.4**	**882.0**	**17.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 171 UK: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	229.9	264.1	303.9	350.1	403.4	464.7	15.1%
Alert Triage and Prioritization	160.3	196.2	240.5	295.1	362.3	444.7	22.6%
Incident Investigation and Analysis	148.9	181.1	220.6	269.1	328.5	401.0	21.9%
Threat Hunting	86.0	102.9	123.3	148.1	178.2	214.4	20.0%
Incident Response and Remediation	120.0	140.1	164.0	192.2	225.6	264.9	17.2%
Insider Threat Detection	57.5	70.2	85.8	105.1	128.7	157.7	22.4%
Cloud Security Monitoring	78.1	90.5	104.9	121.9	141.7	164.8	16.1%
Identity and Access Monitoring	56.4	68.5	83.4	101.5	123.8	151.0	21.8%
Compliance Monitoring and Reporting	36.1	44.7	55.3	68.5	84.8	105.0	23.8%
Security Analytics and Visualization	68.3	74.8	81.5	88.4	95.0	101.1	8.2%
Total	**1,041.5**	**1,233.1**	**1,463.4**	**1,740.0**	**2,072.1**	**2,469.3**	**18.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 172 UK: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	94.8	109.1	125.9	145.4	15.3%
Government & Defense	79.7	90.9	103.9	118.9	14.3%
Healthcare & Life sciences	77.2	94.0	114.7	140.0	21.9%
IT & Telecommunications	57.4	66.2	76.5	88.6	15.6%
Manufacturing	46.8	52.4	58.9	65.9	12.1%
Retail & eCommerce	41.6	49.6	59.1	70.7	19.3%
Energy & Utilities	39.1	46.9	56.3	67.6	20.0%
Media & Entertainment	28.5	33.8	40.1	47.6	18.6%
Education	23.8	28.6	34.4	41.5	20.3%
Other Verticals	53.3	64.9	78.7	95.8	21.6%
Total	**542.3**	**636.4**	**748.4**	**882.0**	**17.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 173 UK: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	168.2	195.0	226.5	263.5	306.8	357.3	16.3%
Government & Defense	136.2	156.4	179.7	206.7	237.8	273.5	15.0%
Healthcare & Life sciences	170.9	209.1	256.1	314.0	385.2	472.5	22.5%
IT & Telecommunications	102.8	119.5	139.2	162.5	189.8	221.8	16.6%
Manufacturing	73.9	82.7	92.6	103.4	115.1	127.7	11.6%
Retail & eCommerce	84.6	101.6	122.2	147.2	177.6	214.4	20.4%
Energy & Utilities	81.4	98.2	118.8	143.9	174.4	211.6	21.0%
Media & Entertainment	56.7	67.7	81.0	97.1	116.6	140.1	19.8%
Education	50.0	60.5	73.3	89.0	108.1	131.4	21.3%
Other Verticals	116.7	142.4	174.0	212.9	260.6	319.0	22.3%
Total	**1,041.5**	**1,233.1**	**1,463.4**	**1,740.0**	**2,072.1**	**2,469.3**	**18.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.3.3 GERMANY

13.3.3.1 Industrial digitalization and smart manufacturing increasing demand for autonomous cyber defense

Germany's AI SOC market is being shaped by the country's advanced industrial base and strong focus on securing digital manufacturing environments. As Europe's largest manufacturing economy, Germany is increasingly integrating AI-powered security operations into Industry 4.0 ecosystems to protect connected factories, industrial control systems (ICS), operational technology (OT), and critical infrastructure from increasingly sophisticated cyber threats. The Federal Office for Information Security (BSI) continues to strengthen the country's cyber resilience by promoting secure AI adoption and advancing guidance on AI security, while emphasizing that cybersecurity and digital transformation must evolve together. In parallel, Germany is implementing the EU's NIS2 Directive and Cyber Resilience Act requirements, prompting manufacturers, utilities, automotive companies, and industrial enterprises to modernize security operations with AI-driven monitoring, anomaly detection, and automated incident response capabilities.

Germany is also strengthening its AI ecosystem through large-scale industrial AI investments aimed at enhancing Europe's technological competitiveness. In 2025, the Federal Ministry for Economic Affairs launched the IPCEI on Artificial Intelligence, enabling collaborative investments in industry-specific AI technologies across Europe, while projects such as KIbSIS (AI-based Security for Industrial Systems) focus on AI-driven anomaly detection, cyber-physical system protection, and secure industrial automation. The German government's AI Offensive further targets increasing AI's contribution to the national economy by expanding AI infrastructure, industrial AI applications, and high-performance computing capabilities. These initiatives are creating significant opportunities for AI-enabled SOC platforms capable of protecting complex IT-OT environments. Germany's growing cybersecurity ecosystem, including Elastic, together with domestic industrial cybersecurity providers and research institutions such as Fraunhofer, continues to accelerate innovation in AI-driven threat analytics, industrial security monitoring, and autonomous cyber defense, positioning the country as one of Europe's leading markets for AI-powered security operations.

TABLE 174 GERMANY: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	430.9	496.7	573.8	664.1	15.5%
Services	247.4	289.5	339.7	399.4	17.3%
Total	**678.3**	**786.2**	**913.5**	**1,063.4**	**16.2%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 175 GERMANY: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	770.2	895.5	1,043.8	1,218.9	1,425.5	1,668.0	16.7%
Services	470.5	555.8	658.2	781.0	928.2	1,103.8	18.6%
Total	**1,240.7**	**1,451.3**	**1,701.9**	**1,999.9**	**2,353.6**	**2,771.8**	**17.4%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 176 GERMANY: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	160.7	177.1	195.3	216.9	10.5%
AI-orchestrated Response and Automation Platforms	66.5	74.7	84.0	94.9	12.6%
AI-native SOC Platforms	92.2	107.6	125.9	147.6	17.0%
AI SOC Agent Solutions	28.7	42.3	59.5	84.3	43.2%
Security Data Platforms	21.1	24.1	27.6	31.6	14.4%
Threat Intelligence Platforms	28.2	32.2	36.8	42.2	14.4%
AI Governance, Risk, and Compliance Solutions	33.6	38.7	44.7	46.6	11.5%
Total	**430.9**	**496.7**	**573.8**	**664.1**	**15.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 177 GERMANY: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	237.1	259.9	285.6	314.4	346.6	382.4	10.0%
AI-orchestrated Response and Automation Platforms	106.8	120.5	136.3	154.5	175.4	199.2	13.3%
AI-native SOC Platforms	173.2	203.8	240.4	284.2	336.3	398.3	18.1%
AI SOC Agent Solutions	108.7	140.4	181.8	235.8	306.4	398.3	29.7%
Security Data Platforms	36.3	41.8	48.2	55.7	64.5	74.7	15.5%
Threat Intelligence Platforms	48.4	55.7	64.3	74.3	86.0	99.6	15.5%
AI Governance, Risk, and Compliance Solutions	59.7	73.4	87.2	100.0	110.2	115.5	14.1%
Total	**770.2**	**895.5**	**1,043.8**	**1,218.9**	**1,425.5**	**1,668.0**	**16.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 178 GERMANY: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	133.4	153.4	176.9	204.4	15.3%
AI SOC-as-a-Service (SOCaaS)	7.7	11.4	16.2	23.2	44.4%
Incident Response and Forensics Services	16.6	20.2	24.6	30.0	21.9%
Threat Intelligence and Advisory Services	89.7	104.5	122.0	141.7	16.5%
Total	**247.4**	**289.5**	**339.7**	**399.4**	**17.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 179 GERMANY: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	236.3	273.8	318.1	370.3	431.7	503.7	16.3%
AI SOC-as-a-Service (SOCaaS)	30.4	39.8	52.2	68.7	90.6	119.4	31.5%
Incident Response and Forensics Services	36.5	44.6	54.5	66.7	81.9	100.6	22.5%
Threat Intelligence and Advisory Services	167.3	197.7	233.4	275.2	324.0	380.2	17.8%
Total	**470.5**	**555.8**	**658.2**	**781.0**	**928.2**	**1,103.8**	**18.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 180 GERMANY: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	489.4	559.3	640.7	735.3	14.5%
SMEs	188.9	226.9	272.8	328.1	20.2%
Total	**678.3**	**786.2**	**913.5**	**1,063.4**	**16.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 181 GERMANY: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	845.8	975.5	1,127.9	1,306.6	1,516.1	1,760.4	15.8%
SMEs	394.8	475.8	574.1	693.2	837.5	1,011.4	20.7%
Total	**1,240.7**	**1,451.3**	**1,701.9**	**1,999.9**	**2,353.6**	**2,771.8**	**17.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 182 GERMANY: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	176.1	199.0	225.2	255.8	13.3%
Alert Triage and Prioritization	82.9	100.3	121.3	147.2	21.1%
Incident Investigation and Analysis	81.1	97.1	116.3	139.9	19.9%
Threat Hunting	52.6	61.6	72.3	85.1	17.4%
Incident Response and Remediation	84.6	96.9	111.1	127.7	14.7%
Insider Threat Detection	30.3	36.5	44.0	53.2	20.6%
Cloud Security Monitoring	57.6	65.5	74.6	85.1	13.9%
Identity and Access Monitoring	31.1	37.1	44.4	53.2	19.7%
Compliance Monitoring and Reporting	17.1	21.0	25.9	32.0	23.2%
Security Analytics and Visualization	64.9	71.4	78.4	84.2	9.1%
Total	**678.3**	**786.2**	**913.5**	**1,063.4**	**16.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 183 GERMANY: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	289.8	329.1	374.7	427.5	488.5	558.6	14.0%
Alert Triage and Prioritization	177.7	215.1	261.0	317.3	386.4	470.9	21.5%
Incident Investigation and Analysis	167.7	201.5	242.8	293.2	354.6	429.1	20.7%
Threat Hunting	100.3	118.6	140.5	166.8	198.4	236.0	18.7%
Incident Response and Remediation	146.9	169.5	196.0	227.2	263.7	306.3	15.8%
Insider Threat Detection	64.1	77.4	93.6	113.6	137.9	167.6	21.2%
Cloud Security Monitoring	97.2	111.2	127.5	146.6	168.7	194.3	14.9%
Identity and Access Monitoring	63.7	76.5	92.0	111.0	134.0	161.9	20.5%
Compliance Monitoring and Reporting	39.0	47.8	58.6	72.1	88.8	109.4	22.9%
Security Analytics and Visualization	94.3	104.7	115.0	124.6	132.6	137.6	7.8%
Total	**1,240.7**	**1,451.3**	**1,701.9**	**1,999.9**	**2,353.6**	**2,771.8**	**17.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 184 GERMANY: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	127.6	145.3	165.8	189.6	14.1%
Government & Defense	110.2	124.7	141.3	160.6	13.4%
Healthcare & Life sciences	83.4	100.2	120.8	145.9	20.5%
IT & Telecommunications	76.5	87.3	99.8	114.4	14.4%
Manufacturing	68.6	76.6	85.6	96.1	11.9%
Retail & eCommerce	49.0	57.7	68.0	80.5	18.0%
Energy & Utilities	45.1	53.4	63.3	75.2	18.6%
Media & Entertainment	34.5	40.3	47.2	55.5	17.2%
Education	26.9	32.0	38.2	45.6	19.2%
Other Verticals	56.6	68.7	83.4	99.9	20.9%
Total	**678.3**	**786.2**	**913.5**	**1,063.4**	**16.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 185 GERMANY: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	217.0	248.9	286.2	329.8	380.6	439.5	15.2%
Government & Defense	182.2	207.3	236.3	270.0	308.9	353.6	14.2%
Healthcare & Life sciences	176.7	214.4	260.9	318.0	388.3	474.5	21.8%
IT & Telecommunications	131.2	150.9	174.0	201.0	232.5	269.2	15.4%
Manufacturing	107.1	119.6	133.8	150.0	168.4	189.1	12.0%
Retail & eCommerce	95.2	113.0	134.5	160.3	191.4	228.6	19.1%
Energy & Utilities	89.5	106.9	127.9	153.4	184.3	221.5	19.9%
Media & Entertainment	65.3	77.1	91.1	108.0	128.2	152.3	18.5%
Education	54.5	65.2	78.2	94.1	113.2	136.4	20.2%
Other Verticals	121.9	148.0	178.9	215.2	257.7	307.1	20.3%
Total	**1,240.7**	**1,451.3**	**1,701.9**	**1,999.9**	**2,353.6**	**2,771.8**	**17.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.3.4 FRANCE

13.3.4.1 Cyber sovereignty initiatives and trusted AI governance reinforcing national digital resilience

France is strengthening its AI SOC market through a national strategy centered on cyber sovereignty, trusted artificial intelligence, and the protection of critical digital infrastructure. The country has adopted a risk-based approach to AI cybersecurity, led by the French National Cybersecurity Agency (ANSSI), which focuses on three strategic priorities: securing AI systems, leveraging AI to strengthen cyber defense, and mitigating cyber risks introduced by AI-enabled attacks. As part of France's renewed National AI Strategy announced in 2025, ANSSI has expanded its technical guidance for secure AI deployment, including recommendations for generative AI security, AI evaluation methodologies, and trusted AI governance. These initiatives are encouraging enterprises to integrate AI into security operations while ensuring transparency, resilience, and compliance across regulated industries.

France is also reinforcing its long-term cybersecurity capabilities through investments in sovereign technologies and national cyber resilience. The government's National Cybersecurity Strategy 2026–2030 prioritizes technological innovation, cybersecurity talent development, protection of critical infrastructure, and the expansion of France's domestic cyber industry. At the same time, ANSSI continues to strengthen security requirements for emerging technologies, including announcing a transition toward quantum-resistant cryptography for government-certified security products beginning in 2027, reflecting France's proactive approach to future cyber risks. The country's cybersecurity ecosystem, supported by global technology leaders such as Thales, Capgemini, Orange Cyberdefense, Atos/Eviden, and Airbus CyberSecurity, alongside growing AI cybersecurity startups, is accelerating innovation in AI-driven threat detection, cyber analytics, and security automation. These developments position France as one of Europe's leading markets for trusted AI-enabled security operations and resilient digital infrastructure.

TABLE 186 FRANCE: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	246.1	294.4	352.9	424.0	19.9%
Services	141.3	171.6	209.0	255.0	21.8%
Total	**387.3**	**466.0**	**561.9**	**678.9**	**20.6%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 187 FRANCE: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	510.3	615.9	745.0	900.4	1,091.3	1,323.5	21.0%
Services	311.7	382.2	469.8	576.9	710.6	875.8	22.9%
Total	**822.1**	**998.1**	**1,214.8**	**1,477.3**	**1,801.8**	**2,199.4**	**21.8%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 188 FRANCE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	91.7	105.0	120.1	138.5	14.7%
AI-orchestrated Response and Automation Platforms	38.0	44.3	51.7	60.6	16.8%
AI-native SOC Platforms	52.6	63.8	77.4	94.2	21.4%
AI SOC Agent Solutions	16.4	25.1	36.6	53.8	48.6%
Security Data Platforms	12.1	14.3	17.0	20.2	18.7%
Threat Intelligence Platforms	16.1	19.1	22.6	26.9	18.7%
AI Governance, Risk, and Compliance Solutions	19.2	22.9	27.5	29.8	15.7%
Total	**246.1**	**294.4**	**352.9**	**424.0**	**19.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 189 FRANCE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	157.1	178.8	203.9	232.3	265.4	303.4	14.1%
AI-orchestrated Response and Automation Platforms	70.8	82.9	97.3	114.1	134.3	158.0	17.4%
AI-native SOC Platforms	114.8	140.2	171.6	209.9	257.5	316.1	22.5%
AI SOC Agent Solutions	72.0	96.5	129.7	174.2	234.6	316.1	34.4%
Security Data Platforms	24.1	28.7	34.4	41.2	49.4	59.3	19.8%
Threat Intelligence Platforms	32.1	38.3	45.9	54.9	65.8	79.0	19.8%
AI Governance, Risk, and Compliance Solutions	39.5	50.5	62.2	73.9	84.4	91.7	18.3%
Total	**510.3**	**615.9**	**745.0**	**900.4**	**1,091.3**	**1,323.5**	**21.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 190 FRANCE: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	76.2	90.9	108.8	130.5	19.7%
AI SOC-as-a-Service (SOCaaS)	4.4	6.8	10.0	14.8	49.8%
Incident Response and Forensics Services	9.5	12.0	15.1	19.2	26.5%
Threat Intelligence and Advisory Services	51.2	61.9	75.0	90.4	20.9%
Total	**141.3**	**171.6**	**209.0**	**255.0**	**21.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 191 FRANCE: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	156.6	188.3	227.0	273.5	330.5	399.6	20.6%
AI SOC-as-a-Service (SOCaaS)	20.1	27.3	37.3	50.8	69.3	94.8	36.3%
Incident Response and Forensics Services	24.2	30.6	38.9	49.3	62.7	79.8	26.9%
Threat Intelligence and Advisory Services	110.9	135.9	166.6	203.3	248.0	301.7	22.2%
Total	**311.7**	**382.2**	**469.8**	**576.9**	**710.6**	**875.8**	**22.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 192 FRANCE: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	279.5	331.5	394.1	469.5	18.9%
SMEs	107.9	134.5	167.8	209.5	24.8%
Total	**387.3**	**466.0**	**561.9**	**678.9**	**20.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 193 FRANCE: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	560.4	670.9	805.0	965.2	1,160.7	1,396.8	20.0%
SMEs	261.6	327.2	409.7	512.1	641.1	802.5	25.1%
Total	**822.1**	**998.1**	**1,214.8**	**1,477.3**	**1,801.8**	**2,199.4**	**21.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 194 FRANCE: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	100.5	117.9	138.5	163.3	17.6%
Alert Triage and Prioritization	47.4	59.4	74.6	94.0	25.7%
Incident Investigation and Analysis	46.3	57.5	71.6	89.3	24.4%
Threat Hunting	30.0	36.5	44.5	54.4	21.9%
Incident Response and Remediation	48.3	57.4	68.3	81.5	19.0%
Insider Threat Detection	17.3	21.6	27.1	34.0	25.2%
Cloud Security Monitoring	32.9	38.8	45.9	54.4	18.2%
Identity and Access Monitoring	17.7	22.0	27.3	34.0	24.2%
Compliance Monitoring and Reporting	9.7	12.5	15.9	20.4	27.9%
Security Analytics and Visualization	37.1	42.3	48.2	53.8	13.2%
Total	**387.3**	**466.0**	**561.9**	**678.9**	**20.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 195 FRANCE: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	192.0	226.3	267.5	315.8	374.0	443.2	18.2%
Alert Triage and Prioritization	117.8	147.9	186.3	234.4	295.8	373.7	26.0%
Incident Investigation and Analysis	111.1	138.6	173.3	216.6	271.5	340.5	25.1%
Threat Hunting	66.5	81.6	100.3	123.2	151.9	187.3	23.0%
Incident Response and Remediation	97.3	116.6	139.9	167.8	201.9	243.0	20.1%
Insider Threat Detection	42.5	53.2	66.8	83.9	105.6	133.0	25.7%
Cloud Security Monitoring	64.4	76.4	91.0	108.3	129.2	154.2	19.1%
Identity and Access Monitoring	42.2	52.6	65.7	82.0	102.6	128.5	24.9%
Compliance Monitoring and Reporting	25.9	32.9	41.8	53.3	68.0	86.8	27.4%
Security Analytics and Visualization	62.5	72.0	82.1	92.1	101.5	109.2	11.8%
Total	**822.1**	**998.1**	**1,214.8**	**1,477.3**	**1,801.8**	**2,199.4**	**21.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 196 FRANCE: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	72.8	86.1	102.0	121.1	18.5%
Government & Defense	63.0	73.9	86.9	102.5	17.7%
Healthcare & Life sciences	47.6	59.4	74.3	93.2	25.1%
IT & Telecommunications	43.7	51.7	61.4	73.1	18.7%
Manufacturing	39.2	45.4	52.7	61.4	16.2%
Retail & eCommerce	28.0	34.2	41.9	51.4	22.5%
Energy & Utilities	25.8	31.6	38.9	48.0	23.1%
Media & Entertainment	19.7	23.9	29.1	35.4	21.7%
Education	15.4	19.0	23.5	29.1	23.7%
Other Verticals	32.3	40.7	51.3	63.8	25.4%
Total	**387.3**	**466.0**	**561.9**	**678.9**	**20.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 197 FRANCE: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	143.8	171.2	204.3	243.6	291.4	348.8	19.4%
Government & Defense	120.7	142.5	168.7	199.4	236.5	280.6	18.4%
Healthcare & Life sciences	117.1	147.4	186.2	234.9	297.3	376.5	26.3%
IT & Telecommunications	87.0	103.8	124.2	148.5	178.0	213.6	19.7%
Manufacturing	71.0	82.2	95.5	110.8	128.9	150.0	16.2%
Retail & eCommerce	63.1	77.7	96.0	118.4	146.5	181.4	23.5%
Energy & Utilities	59.3	73.5	91.3	113.3	141.1	175.8	24.3%
Media & Entertainment	43.3	53.0	65.1	79.8	98.2	120.9	22.8%
Education	36.1	44.8	55.8	69.5	86.7	108.2	24.6%
Other Verticals	80.8	101.8	127.7	159.0	197.3	243.7	24.7%
Total	**822.1**	**998.1**	**1,214.8**	**1,477.3**	**1,801.8**	**2,199.4**	**21.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.3.5 ITALY

13.3.5.1 AI strategy and public sector digitalization accelerating cyber modernization

Italy is strengthening its AI SOC market by aligning its national AI strategy with cybersecurity modernization and digital resilience objectives. The Italian Strategy for Artificial Intelligence 2024-2026, led by the Department for Digital Transformation in collaboration with the Agency for Digital Italy (AgID) and the National Cybersecurity Agency (ACN), prioritizes AI adoption across public administration, enterprises, research, and workforce development while emphasizing secure, transparent, and human-centric AI deployment. Under Italy's AI governance framework, AgID and ACN have been designated as the national authorities responsible for AI oversight, compliance, and cybersecurity, encouraging organizations to integrate AI securely into security operations and enterprise risk management. This coordinated governance model is fostering greater confidence in AI-enabled cybersecurity solutions across both public and private sectors.

Italy is also reinforcing its cyber resilience through sustained investments in cybersecurity research, digital infrastructure, and critical infrastructure protection. In 2026, ACN and the Ministry of University and Research (MUR) published the updated National Cybersecurity Research and Innovation Agenda, identifying artificial intelligence, cyber defense, and quantum technologies as strategic priorities for future research and innovation. At the same time, Italy continues to strengthen national preparedness for high-profile events such as the Milano Cortina 2026 Winter Olympics, where ACN has deployed AI-assisted cyber monitoring and threat intelligence capabilities to protect critical digital infrastructure from increasingly sophisticated cyberattacks. These initiatives, together with the country's expanding digital transformation programs and growing adoption of AI across regulated industries, are expected to create significant opportunities for AI SOC platforms that support continuous monitoring, automated threat detection, and cyber resilience across government, financial services, manufacturing, and critical infrastructure sectors.

TABLE 198 ITALY: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	85.8	102.7	123.4	148.4	20.1%
Services	49.2	59.9	73.0	89.2	21.9%
Total	**135.0**	**162.6**	**196.4**	**237.7**	**20.8%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 199 ITALY: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	178.9	216.2	262.0	318.0	386.6	470.2	21.3%
Services	109.3	134.2	165.2	203.8	251.7	311.1	23.3%
Total	**288.2**	**350.4**	**427.2**	**521.7**	**638.3**	**781.3**	**22.1%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 200 ITALY: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	32.0	36.6	42.0	48.5	14.9%
AI-orchestrated Response and Automation Platforms	13.2	15.4	18.1	21.2	17.0%
AI-native SOC Platforms	18.3	22.3	27.1	33.0	21.6%
AI SOC Agent Solutions	5.7	8.8	12.8	18.8	48.9%
Security Data Platforms	4.2	5.0	5.9	7.1	18.9%
Threat Intelligence Platforms	5.6	6.7	7.9	9.4	18.9%
AI Governance, Risk, and Compliance Solutions	6.7	8.0	9.6	10.4	15.9%
Total	**85.8**	**102.7**	**123.4**	**148.4**	**20.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 201 ITALY: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	55.1	62.8	71.7	82.0	94.0	107.8	14.4%
AI-orchestrated Response and Automation Platforms	24.8	29.1	34.2	40.3	47.6	56.1	17.7%
AI-native SOC Platforms	40.2	49.2	60.3	74.1	91.2	112.3	22.8%
AI SOC Agent Solutions	25.2	33.9	45.6	61.5	83.1	112.3	34.8%
Security Data Platforms	8.4	10.1	12.1	14.5	17.5	21.1	20.1%
Threat Intelligence Platforms	11.2	13.5	16.1	19.4	23.3	28.1	20.1%
AI Governance, Risk, and Compliance Solutions	13.9	17.7	21.9	26.1	29.9	32.6	18.6%
Total	**178.9**	**216.2**	**262.0**	**318.0**	**386.6**	**470.2**	**21.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 202 ITALY: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	26.5	31.7	38.0	45.7	19.8%
AI SOC-as-a-Service (SOCaaS)	1.5	2.4	3.5	5.2	50.1%
Incident Response and Forensics Services	3.3	4.2	5.3	6.7	26.7%
Threat Intelligence and Advisory Services	17.8	21.6	26.2	31.7	21.1%
Total	**49.2**	**59.9**	**73.0**	**89.2**	**21.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 203 ITALY: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	54.9	66.1	79.8	96.6	117.1	142.0	20.9%
AI SOC-as-a-Service (SOCaaS)	7.1	9.6	13.1	17.9	24.6	33.7	36.7%
Incident Response and Forensics Services	8.5	10.8	13.7	17.4	22.2	28.3	27.3%
Threat Intelligence and Advisory Services	38.9	47.7	58.6	71.8	87.9	107.2	22.5%
Total	**109.3**	**134.2**	**165.2**	**203.8**	**251.7**	**311.1**	**23.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 204 ITALY: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	97.4	115.7	137.7	164.3	19.1%
SMEs	37.6	46.9	58.7	73.3	24.9%
Total	**135.0**	**162.6**	**196.4**	**237.7**	**20.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 205 ITALY: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	196.5	235.6	283.1	340.9	411.2	496.2	20.4%
SMEs	91.7	114.9	144.1	180.9	227.1	285.1	25.5%
Total	**288.2**	**350.4**	**427.2**	**521.7**	**638.3**	**781.3**	**22.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 206 ITALY: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	35.0	41.2	48.4	57.2	17.7%
Alert Triage and Prioritization	16.5	20.7	26.1	32.9	25.9%
Incident Investigation and Analysis	16.1	20.1	25.0	31.3	24.6%
Threat Hunting	10.5	12.7	15.6	19.0	22.1%
Incident Response and Remediation	16.8	20.0	23.9	28.5	19.2%
Insider Threat Detection	6.0	7.6	9.5	11.9	25.4%
Cloud Security Monitoring	11.5	13.5	16.0	19.0	18.4%
Identity and Access Monitoring	6.2	7.7	9.5	11.9	24.4%
Compliance Monitoring and Reporting	3.4	4.3	5.6	7.1	28.1%
Security Analytics and Visualization	12.9	14.8	16.9	18.8	13.4%
Total	**135.0**	**162.6**	**196.4**	**237.7**	**20.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 207 ITALY: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	67.3	79.5	94.0	111.5	132.5	157.5	18.5%
Alert Triage and Prioritization	41.3	51.9	65.5	82.8	104.8	132.7	26.3%
Incident Investigation and Analysis	38.9	48.7	61.0	76.5	96.2	121.0	25.4%
Threat Hunting	23.3	28.6	35.3	43.5	53.8	66.5	23.3%
Incident Response and Remediation	34.1	40.9	49.2	59.3	71.5	86.3	20.4%
Insider Threat Detection	14.9	18.7	23.5	29.6	37.4	47.3	26.0%
Cloud Security Monitoring	22.6	26.8	32.0	38.2	45.8	54.8	19.4%
Identity and Access Monitoring	14.8	18.5	23.1	28.9	36.3	45.6	25.3%
Compliance Monitoring and Reporting	9.1	11.5	14.7	18.8	24.1	30.8	27.8%
Security Analytics and Visualization	21.9	25.3	28.9	32.5	36.0	38.8	12.1%
Total	**288.2**	**350.4**	**427.2**	**521.7**	**638.3**	**781.3**	**22.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 208 ITALY: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	25.4	30.0	35.6	42.4	18.6%
Government & Defense	21.9	25.8	30.4	35.9	17.8%
Healthcare & Life sciences	16.6	20.7	26.0	32.6	25.3%
IT & Telecommunications	15.2	18.1	21.5	25.6	18.9%
Manufacturing	13.6	15.8	18.4	21.5	16.3%
Retail & eCommerce	9.7	11.9	14.6	18.0	22.6%
Energy & Utilities	9.0	11.0	13.6	16.8	23.2%
Media & Entertainment	6.9	8.3	10.2	12.4	21.8%
Education	5.4	6.6	8.2	10.2	23.9%
Other Verticals	11.3	14.2	17.9	22.3	25.6%
Total	**135.0**	**162.6**	**196.4**	**237.7**	**20.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 209 ITALY: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	50.4	60.1	71.8	86.0	103.2	123.9	19.7%
Government & Defense	42.3	50.0	59.3	70.4	83.8	99.7	18.7%
Healthcare & Life sciences	41.0	51.8	65.5	83.0	105.3	133.8	26.7%
IT & Telecommunications	30.5	36.4	43.7	52.4	63.1	75.9	20.0%
Manufacturing	24.9	28.9	33.6	39.1	45.7	53.3	16.5%
Retail & eCommerce	22.1	27.3	33.7	41.8	51.9	64.4	23.8%
Energy & Utilities	20.8	25.8	32.1	40.0	50.0	62.4	24.6%
Media & Entertainment	15.2	18.6	22.9	28.2	34.8	42.9	23.1%
Education	12.7	15.7	19.6	24.5	30.7	38.4	24.9%
Other Verticals	28.3	35.7	44.9	56.1	69.9	86.6	25.0%
Total	**288.2**	**350.4**	**427.2**	**521.7**	**638.3**	**781.3**	**22.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.3.6 REST OF EUROPE

The Rest of Europe, comprising countries such as the Netherlands, Spain, Switzerland, Belgium, the Nordic countries, Austria, Ireland, Portugal, Poland, and other Central and Eastern European nations, is witnessing steady growth in AI-powered security operations as governments and enterprises accelerate digital transformation and cyber resilience initiatives. Unlike major Western European economies that emphasize AI governance or industrial cybersecurity, many countries in this region are prioritizing the modernization of critical infrastructure, cloud security, digital public services, and national cyber defense capabilities. The implementation of EU-wide regulations, including the NIS2 Directive, Cyber Resilience Act, and Digital Operational Resilience Act (DORA), is encouraging organizations to adopt AI-enabled threat detection, security analytics, and automated incident response to strengthen operational resilience across public and private sectors.

Several countries across the region are also expanding investments in sovereign AI capabilities, cybersecurity innovation, and digital infrastructure. The Netherlands and the Nordic countries continue to strengthen AI research and cybersecurity collaboration, while Spain and Poland are investing in AI innovation hubs and cloud infrastructure to support secure digital transformation. In July 2026, the European Commission's EU Action Plan on Cybersecurity and Artificial Intelligence introduced new initiatives, including the EU Grand Challenge on AI for Cybersecurity, expanded AI Factories, and future AI Gigafactories, creating opportunities for organizations across smaller European economies to accelerate the development and deployment of AI-enabled cybersecurity solutions. These initiatives are expected to improve regional cybersecurity preparedness while supporting collaboration among governments, academia, and industry.

The region also benefits from a growing ecosystem of cybersecurity vendors and AI innovators. Companies such as Elastic (Netherlands) and Vulnuris (Spain), together with regional cybersecurity startups, managed security providers, and research organizations, are contributing to the development of AI-driven threat detection, security analytics, and SOC automation capabilities. As enterprises continue to modernize digital infrastructure, migrate to cloud-native environments, and strengthen cyber resilience against increasingly sophisticated AI-enabled threats, the Rest of Europe is expected to present significant growth opportunities for AI SOC platforms and managed AI security services throughout the forecast period.

TABLE 210 REST OF EUROPE: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	349.6	418.7	502.1	602.7	19.9%
Services	182.7	222.3	270.8	330.2	21.8%
Total	**532.3**	**641.0**	**772.9**	**932.9**	**20.6%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 211 REST OF EUROPE: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	724.3	871.8	1,051.0	1,271.1	1,536.8	1,857.5	20.7%
Services	403.0	492.7	603.3	741.0	909.8	1,116.6	22.6%
Total	**1,127.3**	**1,364.6**	**1,654.2**	**2,012.1**	**2,446.6**	**2,974.1**	**21.4%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 212 REST OF EUROPE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	128.6	148.3	170.9	196.9	15.2%
AI-orchestrated Response and Automation Platforms	53.7	62.8	73.5	86.1	17.0%
AI-native SOC Platforms	74.7	90.7	110.2	133.9	21.5%
AI SOC Agent Solutions	20.0	26.8	35.9	48.1	33.9%
Security Data Platforms	17.1	20.3	24.1	28.7	18.8%
Threat Intelligence Platforms	22.8	27.1	32.2	38.3	18.8%
AI Governance, Risk, and Compliance Solutions	32.5	42.7	55.3	70.7	29.5%
Total	**349.6**	**418.7**	**502.1**	**602.7**	**19.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 213 REST OF EUROPE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	226.6	260.7	299.9	345.2	396.2	453.3	14.9%
AI-orchestrated Response and Automation Platforms	100.9	118.2	138.7	163.2	191.8	225.1	17.4%
AI-native SOC Platforms	163.0	198.7	242.5	296.9	363.4	444.5	22.2%
AI SOC Agent Solutions	64.6	86.9	117.0	158.0	213.4	288.2	34.9%
Security Data Platforms	34.2	40.7	48.6	58.2	69.6	83.3	19.5%
Threat Intelligence Platforms	45.5	54.3	64.8	77.6	92.8	111.1	19.5%
AI Governance, Risk, and Compliance Solutions	89.5	112.3	139.5	172.0	209.5	252.0	23.0%
Total	**724.3**	**871.8**	**1,051.0**	**1,271.1**	**1,536.8**	**1,857.5**	**20.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 214 REST OF EUROPE: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	93.5	111.6	133.4	159.4	19.5%
AI SOC-as-a-Service (SOCaaS)	10.6	14.3	19.2	25.5	33.9%
Incident Response and Forensics Services	13.7	17.3	21.7	27.2	25.7%
Threat Intelligence and Advisory Services	64.8	79.1	96.6	118.1	22.1%
Total	**182.7**	**222.3**	**270.8**	**330.2**	**21.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 215 REST OF EUROPE: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	190.6	228.3	273.6	328.9	395.0	473.9	20.0%
AI SOC-as-a-Service (SOCaaS)	33.7	44.3	58.0	76.0	99.1	128.6	30.8%
Incident Response and Forensics Services	34.2	43.1	54.2	68.4	86.2	108.5	25.9%
Threat Intelligence and Advisory Services	144.5	177.1	217.4	267.7	329.5	405.5	22.9%
Total	**403.0**	**492.7**	**603.3**	**741.0**	**909.8**	**1,116.6**	**22.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 216 REST OF EUROPE: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	362.9	430.9	512.2	609.3	18.9%
SMEs	169.4	210.2	260.7	323.6	24.1%
Total	**532.3**	**641.0**	**772.9**	**932.9**	**20.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 217 REST OF EUROPE: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	725.6	865.3	1,033.2	1,237.5	1,481.4	1,772.5	19.6%
SMEs	401.7	499.3	621.0	774.6	965.1	1,201.6	24.5%
Total	**1,127.3**	**1,364.6**	**1,654.2**	**2,012.1**	**2,446.6**	**2,974.1**	**21.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 218 REST OF EUROPE: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	131.2	154.2	180.5	212.0	17.3%
Alert Triage and Prioritization	70.7	88.7	110.7	138.7	25.2%
Incident Investigation and Analysis	67.8	84.3	104.5	129.8	24.2%
Threat Hunting	42.1	51.3	62.5	76.3	21.9%
Incident Response and Remediation	64.7	77.0	91.5	109.0	19.0%
Insider Threat Detection	25.6	32.1	39.9	49.9	24.8%
Cloud Security Monitoring	43.4	51.3	60.5	71.5	18.1%
Identity and Access Monitoring	25.9	32.1	39.7	49.2	24.0%
Compliance Monitoring and Reporting	15.1	19.3	24.3	30.9	27.0%
Security Analytics and Visualization	45.7	50.8	58.7	65.8	12.9%
Total	**532.3**	**641.0**	**772.9**	**932.9**	**20.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 219 REST OF EUROPE: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	248.8	292.3	343.6	404.8	476.3	559.7	17.6%
Alert Triage and Prioritization	173.5	217.1	271.9	341.3	427.8	535.6	25.3%
Incident Investigation and Analysis	161.2	200.4	249.4	311.2	387.9	483.0	24.5%
Threat Hunting	93.1	113.9	139.4	171.3	210.4	258.3	22.6%
Incident Response and Remediation	129.9	155.1	185.4	222.3	266.4	319.1	19.7%
Insider Threat Detection	62.2	77.7	97.0	121.5	152.0	190.0	25.0%
Cloud Security Monitoring	84.6	100.1	118.6	141.0	167.3	198.5	18.6%
Identity and Access Monitoring	61.1	75.8	94.2	117.4	146.2	181.8	24.4%
Compliance Monitoring and Reporting	39.1	49.4	62.5	79.2	100.2	126.4	26.5%
Security Analytics and Visualization	73.9	82.7	92.2	102.2	112.2	121.8	10.5%
Total	**1,127.3**	**1,364.6**	**1,654.2**	**2,012.1**	**2,446.6**	**2,974.1**	**21.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 220 REST OF EUROPE: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	93.1	109.9	130.0	153.8	18.2%
Government & Defense	78.2	91.5	107.3	125.8	17.2%
Healthcare & Life sciences	75.8	94.7	118.5	148.0	25.0%
IT & Telecommunications	56.3	66.7	79.0	93.7	18.5%
Manufacturing	46.0	52.8	60.8	69.8	14.9%
Retail & eCommerce	40.9	49.9	61.1	74.8	22.3%
Energy & Utilities	38.4	47.2	58.1	71.5	23.0%
Media & Entertainment	28.0	34.0	41.4	50.4	21.6%
Education	23.4	28.8	35.5	43.8	23.3%
Other Verticals	52.3	65.4	81.2	101.4	24.7%
Total	**532.3**	**641.0**	**772.9**	**932.9**	**20.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 221 REST OF EUROPE: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	182.0	215.8	256.0	304.7	362.2	430.4	18.8%
Government & Defense	147.5	173.0	203.1	239.0	280.8	329.4	17.4%
Healthcare & Life sciences	185.0	231.4	289.5	363.1	454.8	569.1	25.2%
IT & Telecommunications	111.2	132.2	157.4	187.8	224.1	267.1	19.1%
Manufacturing	80.0	91.5	104.6	119.5	135.9	153.8	14.0%
Retail & eCommerce	91.6	112.4	138.1	170.2	209.7	258.3	23.0%
Energy & Utilities	88.1	108.7	134.3	166.4	206.0	254.8	23.7%
Media & Entertainment	61.4	74.9	91.6	112.3	137.7	168.8	22.4%
Education	54.1	67.0	82.9	102.9	127.6	158.2	23.9%
Other Verticals	126.3	157.6	196.7	246.1	307.7	384.2	24.9%
Total	**1,127.3**	**1,364.6**	**1,654.2**	**2,012.1**	**2,446.6**	**2,974.1**	**21.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.4 ASIA PACIFIC

Asia Pacific is emerging as the fastest-growing region in the AI SOC market, fueled by rapid digital transformation, expanding cloud adoption, and increasing investments in artificial intelligence across both developed and emerging economies. Unlike North America, where AI SOC innovation is led by technology providers, or Europe, where regulatory compliance is the primary catalyst, Asia Pacific is characterized by large-scale digital economy initiatives, accelerated enterprise AI adoption, and rising cybersecurity investments to secure increasingly connected digital ecosystems. The rapid expansion of digital banking, e-commerce, smart manufacturing, telecommunications, and smart city programs has significantly increased the regional cyberattack surface, prompting enterprises to modernize security operations with AI-powered threat detection, automation, and real-time security analytics. The growing frequency of AI-enabled phishing, ransomware, and identity-based attacks across Asia and the Pacific is further accelerating investments in intelligent SOC platforms and managed security services.

Regional collaboration is also strengthening AI-enabled cybersecurity capabilities. During the AI Seoul Summit (2024), several Asia-Pacific economies including Japan, Singapore, South Korea, and Australia joined the international AI Safety Institutes Network, reinforcing cooperation on frontier AI evaluation, AI security testing, and safe AI deployment. In parallel, APEC has expanded regional dialogue on artificial intelligence, cybersecurity, trusted data flows, and digital resilience through its Digital Economy Steering Group, while ASEAN released the Responsible AI Roadmap (2025-2030) to support interoperable AI governance and responsible AI adoption across Southeast Asia. These regional initiatives are encouraging governments and enterprises to integrate AI securely into cybersecurity strategies while strengthening cross-border cyber resilience and digital trust.

Looking ahead, Asia Pacific is expected to become a major growth hub for AI-native security operations as enterprises increasingly deploy autonomous security technologies to address cybersecurity talent shortages, protect critical infrastructure, and secure rapidly expanding cloud environments. The region is also witnessing the emergence of a vibrant cybersecurity innovation ecosystem supported by global and regional vendors, including Trend Micro (Japan), AhnLab (South Korea), ManageEngine (India), Seqrite (India), and Cyfirma (Singapore), alongside increasing investments from international cybersecurity providers. As governments continue investing in AI infrastructure, digital public services, sovereign AI capabilities, and cyber resilience programs, Asia Pacific is expected to offer significant opportunities for AI SOC platform providers, managed security service providers, and AI-driven cybersecurity innovators throughout the forecast period.

13.4.1 ASIA PACIFIC: AI SOC MARKET DRIVERS

- Asia Pacific's rapid digital transformation across banking, e-commerce, telecommunications, manufacturing, and government services is significantly expanding the cyberattack surface. As enterprises migrate to hybrid and multi-cloud environments, organizations are increasingly investing in AI SOC platforms to enhance threat visibility, automate incident response, and strengthen cyber resilience.
- The growing sophistication of AI-powered phishing, ransomware, deepfakes, and identity-based attacks is compelling enterprises to modernize conventional SOCs with AI-assisted threat detection, behavioral analytics, and autonomous response capabilities. Organizations across the region are prioritizing intelligent security operations to counter increasingly automated and large-scale cyber threats.
- Governments across Asia Pacific are strengthening AI and cybersecurity ecosystems through investments in sovereign AI infrastructure, trusted AI research, secure digital public services, and national cyber resilience programs. These initiatives are encouraging enterprises to adopt AI-native security operations while accelerating innovation in intelligent cyber defense across critical sectors.

JULY 2026 © MarketsandMarkets™

- Organizations in financial services, manufacturing, healthcare, telecommunications, and public administration are rapidly integrating AI into business operations, creating demand for intelligent SOC platforms capable of securing AI workloads, cloud-native applications, and complex digital environments. The increasing use of generative AI is further driving investments in AI-assisted security monitoring and automated incident response.
- Regional innovation led by technology providers, research institutions, and cybersecurity companies across China, Japan, India, South Korea, Singapore, and Australia is accelerating the development of AI-powered threat detection, autonomous SOC platforms, and advanced security analytics. Growing public-private collaboration is further strengthening the commercialization of AI-driven cybersecurity solutions across the region.
- The shortage of skilled cybersecurity professionals, combined with increasing alert volumes and operational complexity, is encouraging enterprises to deploy AI-enabled SOC platforms that automate alert triage, threat investigation, and remediation. AI-assisted security operations are enabling organizations to improve operational efficiency while addressing the scalability challenges of modern cybersecurity environments.

FIGURE 40 ASIA PACIFIC: AI SOC MARKET SNAPSHOT



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 222 ASIA PACIFIC: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	1,149.8	1,415.8	1,747.4	2,160.6	23.4%
Services	660.0	825.3	1,034.5	1,299.3	25.3%
Total	**1,809.8**	**2,241.1**	**2,781.9**	**3,459.9**	**24.1%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 223 ASIA PACIFIC: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	2,678.3	3,328.8	4,146.9	5,176.2	6,470.4	8,092.9	24.8%
Services	1,636.2	2,065.9	2,614.9	3,316.6	4,213.1	5,355.5	26.8%
Total	**4,314.5**	**5,394.7**	**6,761.9**	**8,492.8**	**10,683.5**	**13,448.4**	**25.5%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 224 ASIA PACIFIC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	428.0	504.5	594.8	705.7	18.1%
AI-orchestrated Response and Automation Platforms	177.3	212.9	255.9	308.7	20.3%
AI-native SOC Platforms	245.9	306.7	383.3	480.1	25.0%
AI SOC Agent Solutions	75.4	117.2	174.9	262.7	51.6%
Security Data Platforms	56.4	68.7	84.0	102.9	22.2%
Threat Intelligence Platforms	75.2	91.7	112.0	137.2	22.2%
AI Governance, Risk, and Compliance Solutions	91.6	114.2	142.4	163.4	21.3%
Total	**1,149.8**	**1,415.8**	**1,747.4**	**2,160.6**	**23.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 225 ASIA PACIFIC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	826.2	969.7	1,140.6	1,343.8	1,585.1	1,870.2	17.7%
AI-orchestrated Response and Automation Platforms	371.5	448.4	542.3	657.2	797.4	968.1	21.1%
AI-native SOC Platforms	602.4	757.8	955.5	1,207.1	1,527.1	1,933.1	26.3%
AI SOC Agent Solutions	361.7	499.3	690.9	958.0	1,330.2	1,848.2	38.6%
Security Data Platforms	126.2	155.3	191.5	236.6	292.8	362.4	23.5%
Threat Intelligence Platforms	168.3	207.1	255.4	315.5	390.4	483.3	23.5%
AI Governance, Risk, and Compliance Solutions	221.9	291.2	370.8	458.1	547.4	627.5	23.1%
Total	**2,678.3**	**3,328.8**	**4,146.9**	**5,176.2**	**6,470.4**	**8,092.9**	**24.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 226 ASIA PACIFIC: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	355.9	437.4	538.7	665.1	23.2%
AI SOC-as-a-Service (SOCaaS)	20.6	32.6	49.5	75.6	54.2%
Incident Response and Forensics Services	44.2	57.5	74.8	97.7	30.2%
Threat Intelligence and Advisory Services	239.3	297.8	371.5	460.9	24.4%
Total	**660.0**	**825.3**	**1,034.5**	**1,299.3**	**25.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 227 ASIA PACIFIC: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	821.6	1,017.8	1,263.8	1,572.4	1,959.6	2,443.7	24.4%
AI SOC-as-a-Service (SOCaaS)	105.6	147.8	207.5	291.8	411.0	579.4	40.6%
Incident Response and Forensics Services	127.0	165.6	216.4	283.4	371.8	487.9	30.9%
Threat Intelligence and Advisory Services	581.9	734.7	927.3	1,168.9	1,470.7	1,844.5	26.0%
Total	**1,636.2**	**2,065.9**	**2,614.9**	**3,316.6**	**4,213.1**	**5,355.5**	**26.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 228 ASIA PACIFIC: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	1,305.8	1,594.2	1,951.1	2,392.4	22.4%
SMEs	504.0	646.9	830.8	1,067.4	28.4%
Total	**1,809.8**	**2,241.1**	**2,781.9**	**3,459.9**	**24.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 229 ASIA PACIFIC: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	2,941.4	3,626.1	4,481.1	5,549.0	6,882.0	8,541.2	23.8%
SMEs	1,373.1	1,768.6	2,280.8	2,943.9	3,801.4	4,907.2	29.0%
Total	**4,314.5**	**5,394.7**	**6,761.9**	**8,492.8**	**10,683.5**	**13,448.4**	**25.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 230 ASIA PACIFIC: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	469.7	567.1	685.9	832.2	21.0%
Alert Triage and Prioritization	221.3	285.8	369.3	479.0	29.4%
Incident Investigation and Analysis	216.5	276.7	354.3	455.0	28.1%
Threat Hunting	140.2	175.6	220.3	277.0	25.5%
Incident Response and Remediation	225.8	276.1	338.3	415.4	22.5%
Insider Threat Detection	80.9	104.1	134.0	173.2	28.9%
Cloud Security Monitoring	153.7	186.6	227.1	277.0	21.7%
Identity and Access Monitoring	82.9	105.7	135.1	173.2	27.9%
Compliance Monitoring and Reporting	45.6	59.9	78.8	104.0	31.7%
Security Analytics and Visualization	173.2	203.4	238.8	273.9	16.5%
Total	**1,809.8**	**2,241.1**	**2,781.9**	**3,459.9**	**24.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 231 ASIA PACIFIC: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	1,007.6	1,223.3	1,488.7	1,815.5	2,217.4	2,710.1	21.9%
Alert Triage and Prioritization	618.0	799.6	1,037.0	1,347.7	1,754.1	2,284.8	29.9%
Incident Investigation and Analysis	583.1	749.1	964.9	1,245.2	1,609.6	2,082.0	29.0%
Threat Hunting	349.0	440.8	558.3	708.4	900.4	1,145.1	26.8%
Incident Response and Remediation	510.9	630.0	778.8	964.8	1,197.0	1,486.1	23.8%
Insider Threat Detection	222.9	287.6	372.1	482.3	626.1	813.4	29.6%
Cloud Security Monitoring	337.8	413.2	506.6	622.4	765.8	942.9	22.8%
Identity and Access Monitoring	221.6	284.3	365.6	471.2	608.2	785.5	28.8%
Compliance Monitoring and Reporting	135.7	177.6	232.9	306.2	403.1	531.0	31.4%
Security Analytics and Visualization	327.9	389.1	456.9	529.2	601.8	667.4	15.3%
Total	**4,314.5**	**5,394.7**	**6,761.9**	**8,492.8**	**10,683.5**	**13,448.4**	**25.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 232 ASIA PACIFIC: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	340.3	414.1	504.8	617.0	21.9%
Government & Defense	294.1	355.5	430.4	522.6	21.1%
Healthcare & Life sciences	222.4	285.7	368.0	474.8	28.8%
IT & Telecommunications	204.1	248.8	304.0	372.3	22.2%
Manufacturing	183.0	218.3	260.7	312.8	19.6%
Retail & eCommerce	130.7	164.4	207.2	261.8	26.1%
Energy & Utilities	120.4	152.1	192.7	244.6	26.7%
Media & Entertainment	91.9	114.9	143.9	180.6	25.2%
Education	71.8	91.3	116.3	148.4	27.4%
Other Verticals	151.0	195.9	253.9	325.0	29.1%
Total	**1,809.8**	**2,241.1**	**2,781.9**	**3,459.9**	**24.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 233 ASIA PACIFIC: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	754.5	925.2	1,137.2	1,400.6	1,727.7	2,132.5	23.1%
Government & Defense	633.7	770.4	938.9	1,146.5	1,402.1	1,715.7	22.0%
Healthcare & Life sciences	614.3	797.0	1,036.4	1,350.6	1,762.7	2,302.2	30.2%
IT & Telecommunications	456.4	561.0	691.3	853.5	1,055.5	1,306.0	23.4%
Manufacturing	372.4	444.5	531.7	637.2	764.4	917.3	19.8%
Retail & eCommerce	331.2	420.1	534.2	680.7	868.6	1,109.1	27.3%
Energy & Utilities	311.4	397.3	508.3	651.6	836.5	1,074.7	28.1%
Media & Entertainment	227.1	286.4	362.1	458.8	582.1	739.0	26.6%
Education	189.4	242.4	310.8	399.4	514.0	661.8	28.4%
Other Verticals	424.0	550.2	710.7	914.0	1,170.0	1,490.1	28.6%
Total	**4,314.5**	**5,394.7**	**6,761.9**	**8,492.8**	**10,683.5**	**13,448.4**	**25.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 234 ASIA PACIFIC: AI SOC MARKET, BY COUNTRY, 2022–2025 (USD MILLION)

Country	2022	2023	2024	2025	CAGR (2022–2025)
China	641.5	784.4	961.3	1,180.5	22.5%
Japan	323.2	393.9	481.1	588.8	22.1%
India	199.1	250.1	314.9	397.2	25.9%
Rest of Asia Pacific	645.9	812.7	1,024.5	1,293.3	26.0%
Total	**1,809.8**	**2,241.1**	**2,781.9**	**3,459.9**	**24.1%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 235 ASIA PACIFIC: AI SOC MARKET, BY COUNTRY, 2026–2031 (USD MILLION)

Country	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
China	1,453.4	1,794.3	2,220.6	2,748.5	3,410.2	4,234.2	23.8%
Japan	722.5	889.0	1,096.4	1,355.1	1,677.4	2,077.8	23.5%
India	502.4	637.2	810.0	1,031.7	1,316.2	1,676.7	27.3%
Rest of Asia Pacific	1,636.1	2,074.2	2,634.8	3,357.4	4,279.7	5,459.8	27.3%
Total	**4,314.5**	**5,394.7**	**6,761.9**	**8,492.8**	**10,683.5**	**13,448.4**	**25.5%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.4.2 CHINA

13.4.2.1 Indigenous AI innovation and cloud security leadership transforming intelligent cyber resilience

China is rapidly advancing its AI SOC market by integrating artificial intelligence into national digital infrastructure, cloud security, and enterprise cybersecurity. As organizations accelerate AI adoption across manufacturing, telecommunications, finance, and public services under the country's digital transformation agenda, demand is growing for intelligent security operations capable of protecting increasingly complex and large-scale digital environments. Domestic technology providers are embedding AI agents, large language models (LLMs), and automated response capabilities into security platforms to improve threat detection, incident investigation, and cyber resilience. This momentum is reinforced by China's emphasis on developing indigenous AI technologies, expanding cloud infrastructure, and strengthening cybersecurity capabilities across critical sectors.

China's AI SOC ecosystem is being shaped by rapid innovation from domestic cloud and cybersecurity providers. In 2026, Alibaba Cloud introduced its Agentic SOC platform, upgrading its Cloud Threat Detection and Response (CTDR) service into an AI agent-driven security operations platform capable of autonomous threat detection, multi-agent investigation, attack chain reconstruction, and automated incident response across hybrid and multi-cloud environments. The platform leverages Alibaba's Qwen large language model, graph computing, and SOAR capabilities to reduce investigation times from hours to minutes while automating end-to-end security workflows. In parallel, China Telecom Global has expanded its AI and Security Innovation Centres to accelerate AI-enabled cybersecurity research and enterprise security services, further strengthening the country's AI security ecosystem. Alongside leading domestic cybersecurity companies such as VenusTech, Qi-Anxin, Sangfor Technologies, and 360 Digital Security, these developments are fostering indigenous innovation in AI-powered security analytics, intelligent SOC automation, and cloud-native cyber defense. Supported by continuous investments in AI infrastructure and enterprise AI adoption, China is expected to remain one of the most innovative and dominating markets for autonomous security operations in the Asia Pacific region.

TABLE 236 CHINA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	407.6	495.5	603.8	737.2	21.8%
Services	234.0	288.9	357.5	443.3	23.7%
Total	**641.5**	**784.4**	**961.3**	**1,180.5**	**22.5%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 237 CHINA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	902.3	1,107.2	1,361.9	1,675.2	2,065.4	2,548.0	23.1%
Services	551.2	687.1	858.7	1,073.4	1,344.8	1,686.2	25.1%
Total	**1,453.4**	**1,794.3**	**2,220.6**	**2,748.5**	**3,410.2**	**4,234.2**	**23.8%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 238 CHINA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	151.9	176.7	205.5	240.8	16.6%
AI-orchestrated Response and Automation Platforms	62.9	74.5	88.4	105.3	18.8%
AI-native SOC Platforms	87.2	107.3	132.5	163.8	23.4%
AI SOC Agent Solutions	27.1	42.2	62.6	93.6	51.1%
Security Data Platforms	20.0	24.1	29.0	35.1	20.7%
Threat Intelligence Platforms	26.6	32.1	38.7	46.8	20.7%
AI Governance, Risk, and Compliance Solutions	31.8	38.6	47.0	51.8	17.6%
Total	**407.6**	**495.5**	**603.8**	**737.2**	**21.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 239 CHINA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	277.8	321.4	372.7	432.1	502.3	584.1	16.0%
AI-orchestrated Response and Automation Platforms	125.1	149.0	177.9	212.3	254.1	304.2	19.5%
AI-native SOC Platforms	202.9	252.0	313.7	390.6	487.3	608.5	24.6%
AI SOC Agent Solutions	127.3	173.5	237.2	324.1	443.9	608.5	36.7%
Security Data Platforms	42.5	51.7	62.9	76.6	93.4	114.1	21.8%
Threat Intelligence Platforms	56.7	68.9	83.8	102.1	124.6	152.1	21.8%
AI Governance, Risk, and Compliance Solutions	69.9	90.7	113.7	137.4	159.7	176.5	20.3%
Total	**902.3**	**1,107.2**	**1,361.9**	**1,675.2**	**2,065.4**	**2,548.0**	**23.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 240 CHINA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	126.2	153.1	186.2	226.9	21.6%
AI SOC-as-a-Service (SOCaaS)	7.3	11.4	17.1	25.8	52.3%
Incident Response and Forensics Services	15.7	20.1	25.9	33.3	28.6%
Threat Intelligence and Advisory Services	84.8	104.2	128.4	157.3	22.9%
Total	**234.0**	**288.9**	**357.5**	**443.3**	**23.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 241 CHINA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	276.8	338.5	415.0	508.9	625.5	769.4	22.7%
AI SOC-as-a-Service (SOCaaS)	35.6	49.2	68.1	94.4	131.2	182.4	38.7%
Incident Response and Forensics Services	42.8	55.1	71.1	91.7	118.7	153.6	29.1%
Threat Intelligence and Advisory Services	196.0	244.4	304.5	378.3	469.4	580.7	24.3%
Total	**551.2**	**687.1**	**858.7**	**1,073.4**	**1,344.8**	**1,686.2**	**25.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 242 CHINA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	462.9	558.0	674.2	816.3	20.8%
SMEs	178.7	226.4	287.1	364.2	26.8%
Total	**641.5**	**784.4**	**961.3**	**1,180.5**	**22.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 243 CHINA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	990.9	1,206.1	1,471.6	1,795.8	2,196.7	2,689.2	22.1%
SMEs	462.6	588.3	749.0	952.7	1,213.4	1,545.0	27.3%
Total	**1,453.4**	**1,794.3**	**2,220.6**	**2,748.5**	**3,410.2**	**4,234.2**	**23.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 244 CHINA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	166.5	198.5	237.0	284.0	19.5%
Alert Triage and Prioritization	78.4	100.0	127.6	163.4	27.7%
Incident Investigation and Analysis	76.7	96.9	122.4	155.3	26.5%
Threat Hunting	49.7	61.4	76.1	94.5	23.9%
Incident Response and Remediation	80.0	96.6	116.9	141.7	21.0%
Insider Threat Detection	28.7	36.4	46.3	59.1	27.2%
Cloud Security Monitoring	54.5	65.3	78.5	94.5	20.1%
Identity and Access Monitoring	29.4	37.0	46.7	59.1	26.2%
Compliance Monitoring and Reporting	16.1	21.0	27.2	35.5	30.0%
Security Analytics and Visualization	61.4	71.2	82.5	93.5	15.0%
Total	**641.5**	**784.4**	**961.3**	**1,180.5**	**22.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 245 CHINA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	339.4	406.9	488.9	587.5	707.8	853.3	20.2%
Alert Triage and Prioritization	208.2	266.0	340.6	436.2	559.9	719.3	28.1%
Incident Investigation and Analysis	196.4	249.2	316.9	403.0	513.8	655.5	27.3%
Threat Hunting	117.6	146.6	183.3	229.3	287.4	360.5	25.1%
Incident Response and Remediation	172.1	209.5	255.8	312.2	382.1	467.9	22.1%
Insider Threat Detection	75.1	95.7	122.2	156.1	199.8	256.1	27.8%
Cloud Security Monitoring	113.8	137.4	166.4	201.4	244.4	296.9	21.1%
Identity and Access Monitoring	74.6	94.6	120.1	152.5	194.1	247.3	27.1%
Compliance Monitoring and Reporting	45.7	59.1	76.5	99.1	128.7	167.2	29.6%
Security Analytics and Visualization	110.5	129.4	150.1	171.3	192.1	210.1	13.7%
Total	**1,453.4**	**1,794.3**	**2,220.6**	**2,748.5**	**3,410.2**	**4,234.2**	**23.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 246 CHINA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	120.6	144.9	174.5	210.5	20.4%
Government & Defense	104.3	124.4	148.7	178.3	19.6%
Healthcare & Life sciences	78.8	100.0	127.2	162.0	27.1%
IT & Telecommunications	72.4	87.1	105.1	127.0	20.6%
Manufacturing	64.9	76.4	90.1	106.7	18.1%
Retail & eCommerce	46.3	57.5	71.6	89.3	24.5%
Energy & Utilities	42.7	53.2	66.6	83.5	25.1%
Media & Entertainment	32.6	40.2	49.7	61.6	23.6%
Education	25.5	32.0	40.2	50.6	25.7%
Other Verticals	53.5	68.6	87.7	110.9	27.5%
Total	**641.5**	**784.4**	**961.3**	**1,180.5**	**22.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 247 CHINA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	254.2	307.7	373.5	453.3	551.5	671.4	21.4%
Government & Defense	213.5	256.3	308.3	371.0	447.5	540.2	20.4%
Healthcare & Life sciences	207.0	265.1	340.4	437.1	562.7	724.8	28.5%
IT & Telecommunications	153.8	186.6	227.0	276.2	336.9	411.2	21.7%
Manufacturing	125.5	147.9	174.6	206.2	244.0	288.8	18.1%
Retail & eCommerce	111.6	139.7	175.4	220.3	277.3	349.2	25.6%
Energy & Utilities	104.9	132.2	166.9	210.9	267.0	338.4	26.4%
Media & Entertainment	76.5	95.3	118.9	148.5	185.8	232.7	24.9%
Education	63.8	80.6	102.1	129.3	164.1	208.4	26.7%
Other Verticals	142.8	183.0	233.4	295.8	373.5	469.1	26.9%
Total	**1,453.4**	**1,794.3**	**2,220.6**	**2,748.5**	**3,410.2**	**4,234.2**	**23.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.4.3 JAPAN

13.4.3.1 AI-security research and resilient digital infrastructure advancing next-generation cyber defense

Japan's AI SOC market is evolving through a strong emphasis on AI security research, resilient digital infrastructure, and the protection of mission-critical industries. As enterprises accelerate the adoption of generative AI, cloud computing, and connected manufacturing technologies, organizations are increasingly modernizing security operations to defend against sophisticated cyber threats targeting industrial systems, financial institutions, telecommunications networks, and public services. To strengthen national capabilities, Japan's National Institute of Information and Communications Technology (NICT) established the Center for Research on AI Security and Technology Evolution (CREATE) in February 2025. CREATE serves as Japan's national hub for advancing "Security for AI," "AI for Security," and "Trustworthy AI," focusing on AI security evaluation, AI-driven threat detection, explainable AI, automated alert triage, and secure deployment of large language models. The center also promotes international collaboration with academia and industry to build secure AI-native digital infrastructure.

Japan is also strengthening its AI-enabled cybersecurity ecosystem through collaboration between government, academia, and industry. In 2026, NICT and SB Intuitions launched joint research to develop secure, high-performance Japanese large language models with enhanced AI safety capabilities, supporting the country's objective of deploying trustworthy AI across critical sectors. At the enterprise level, organizations are increasingly embedding AI into security operations. NEC has expanded its AI-driven cybersecurity capabilities by integrating generative AI into threat analysis and security operations, while NTT Security, LAC (JSOC), and SoftBank continue to strengthen AI-assisted SOC services for enterprise customers. International collaborations are also accelerating innovation, including Deloitte Japan's adoption of Cisco Foundation AI to enhance SOC operations and OpenAI's collaboration with SoftBank to expand secure enterprise AI deployment. Supported by sustained investments in AI infrastructure, cybersecurity research, and trusted AI development, Japan is expected to remain one of Asia Pacific's leading markets for intelligent security operations and autonomous cyber resilience.

TABLE 248 JAPAN: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	205.4	248.8	302.2	367.7	21.4%
Services	117.9	145.1	178.9	221.1	23.3%
Total	**323.2**	**393.9**	**481.1**	**588.8**	**22.1%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 249 JAPAN: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	448.5	548.5	672.4	825.9	1,015.9	1,250.4	22.8%
Services	274.0	340.4	424.0	529.2	661.5	827.4	24.7%
Total	**722.5**	**889.0**	**1,096.4**	**1,355.1**	**1,677.4**	**2,077.8**	**23.5%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 250 JAPAN: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	76.6	88.7	102.9	120.1	16.2%
AI-orchestrated Response and Automation Platforms	31.7	37.4	44.3	52.5	18.4%
AI-native SOC Platforms	43.9	53.9	66.3	81.7	23.0%
AI SOC Agent Solutions	13.7	21.2	31.4	46.7	50.6%
Security Data Platforms	10.1	12.1	14.5	17.5	20.3%
Threat Intelligence Platforms	13.4	16.1	19.4	23.3	20.3%
AI Governance, Risk, and Compliance Solutions	16.0	19.4	23.5	25.8	17.2%
Total	**205.4**	**248.8**	**302.2**	**367.7**	**21.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 251 JAPAN: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	138.1	159.2	184.0	213.1	247.1	286.6	15.7%
AI-orchestrated Response and Automation Platforms	62.2	73.8	87.8	104.7	125.0	149.3	19.1%
AI-native SOC Platforms	100.9	124.9	154.9	192.6	239.7	298.6	24.2%
AI SOC Agent Solutions	63.3	86.0	117.1	159.8	218.4	298.6	36.4%
Security Data Platforms	21.1	25.6	31.1	37.7	46.0	56.0	21.5%
Threat Intelligence Platforms	28.2	34.1	41.4	50.3	61.3	74.6	21.5%
AI Governance, Risk, and Compliance Solutions	34.8	45.0	56.2	67.7	78.6	86.6	20.0%
Total	**448.5**	**548.5**	**672.4**	**825.9**	**1,015.9**	**1,250.4**	**22.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 252 JAPAN: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	63.6	76.9	93.2	113.2	21.2%
AI SOC-as-a-Service (SOCaaS)	3.7	5.7	8.6	12.9	51.8%
Incident Response and Forensics Services	7.9	10.1	12.9	16.6	28.1%
Threat Intelligence and Advisory Services	42.7	52.3	64.3	78.4	22.4%
Total	**117.9**	**145.1**	**178.9**	**221.1**	**23.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 253 JAPAN: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	137.6	167.7	204.9	250.9	307.7	377.5	22.4%
AI SOC-as-a-Service (SOCaaS)	17.7	24.4	33.6	46.6	64.5	89.5	38.3%
Incident Response and Forensics Services	21.3	27.3	35.1	45.2	58.4	75.4	28.8%
Threat Intelligence and Advisory Services	97.5	121.1	150.4	186.5	230.9	285.0	23.9%
Total	**274.0**	**340.4**	**424.0**	**529.2**	**661.5**	**827.4**	**24.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 254 JAPAN: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	233.2	280.2	337.4	407.1	20.4%
SMEs	90.0	113.7	143.7	181.7	26.4%
Total	**323.2**	**393.9**	**481.1**	**588.8**	**22.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 255 JAPAN: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	492.6	597.5	726.6	885.4	1,080.5	1,319.6	21.8%
SMEs	229.9	291.4	369.8	469.7	596.9	758.2	26.9%
Total	**722.5**	**889.0**	**1,096.4**	**1,355.1**	**1,677.4**	**2,077.8**	**23.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 256 JAPAN: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	83.9	99.7	118.6	141.6	19.1%
Alert Triage and Prioritization	39.5	50.2	63.9	81.5	27.3%
Incident Investigation and Analysis	38.7	48.6	61.3	77.4	26.1%
Threat Hunting	25.0	30.9	38.1	47.1	23.5%
Incident Response and Remediation	40.3	48.5	58.5	70.7	20.6%
Insider Threat Detection	14.5	18.3	23.2	29.5	26.8%
Cloud Security Monitoring	27.5	32.8	39.3	47.1	19.7%
Identity and Access Monitoring	14.8	18.6	23.4	29.5	25.8%
Compliance Monitoring and Reporting	8.1	10.5	13.6	17.7	29.6%
Security Analytics and Visualization	30.9	35.8	41.3	46.6	14.7%
Total	**323.2**	**393.9**	**481.1**	**588.8**	**22.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 257 JAPAN: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	168.7	201.6	241.4	289.7	348.1	418.7	19.9%
Alert Triage and Prioritization	103.5	131.8	168.2	215.0	275.4	353.0	27.8%
Incident Investigation and Analysis	97.6	123.4	156.5	198.7	252.7	321.7	26.9%
Threat Hunting	58.4	72.6	90.5	113.0	141.4	176.9	24.8%
Incident Response and Remediation	85.6	103.8	126.3	153.9	187.9	229.6	21.8%
Insider Threat Detection	37.3	47.4	60.3	76.9	98.3	125.7	27.5%
Cloud Security Monitoring	56.6	68.1	82.1	99.3	120.2	145.7	20.8%
Identity and Access Monitoring	37.1	46.8	59.3	75.2	95.5	121.4	26.7%
Compliance Monitoring and Reporting	22.7	29.3	37.8	48.9	63.3	82.0	29.3%
Security Analytics and Visualization	54.9	64.1	74.1	84.4	94.5	103.1	13.4%
Total	**722.5**	**889.0**	**1,096.4**	**1,355.1**	**1,677.4**	**2,077.8**	**23.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 258 JAPAN: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	60.8	72.8	87.3	105.0	20.0%
Government & Defense	52.5	62.5	74.4	88.9	19.2%
Healthcare & Life sciences	39.7	50.2	63.6	80.8	26.7%
IT & Telecommunications	36.5	43.7	52.6	63.4	20.2%
Manufacturing	32.7	38.4	45.1	53.2	17.7%
Retail & eCommerce	23.3	28.9	35.8	44.6	24.0%
Energy & Utilities	21.5	26.7	33.3	41.6	24.6%
Media & Entertainment	16.4	20.2	24.9	30.7	23.2%
Education	12.8	16.1	20.1	25.3	25.3%
Other Verticals	27.0	34.4	43.9	55.3	27.1%
Total	**323.2**	**393.9**	**481.1**	**588.8**	**22.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 259 JAPAN: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	126.4	152.5	184.4	223.5	271.3	329.5	21.1%
Government & Defense	106.1	127.0	152.2	182.9	220.1	265.1	20.1%
Healthcare & Life sciences	102.9	131.3	168.1	215.5	276.8	355.7	28.2%
IT & Telecommunications	76.4	92.4	112.1	136.2	165.7	201.8	21.4%
Manufacturing	62.4	73.3	86.2	101.7	120.0	141.7	17.8%
Retail & eCommerce	55.5	69.2	86.6	108.6	136.4	171.4	25.3%
Energy & Utilities	52.1	65.5	82.4	104.0	131.3	166.0	26.1%
Media & Entertainment	38.0	47.2	58.7	73.2	91.4	114.2	24.6%
Education	31.7	39.9	50.4	63.7	80.7	102.2	26.4%
Other Verticals	71.0	90.7	115.2	145.8	183.7	230.2	26.5%
Total	**722.5**	**889.0**	**1,096.4**	**1,355.1**	**1,677.4**	**2,077.8**	**23.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.4.4 INDIA

13.4.4.1 AI-native security operations and cybersecurity services ecosystem accelerating cyber modernization

India's AI SOC market is gaining momentum as enterprises modernize security operations to secure one of the world's fastest-growing digital economies. The rapid expansion of digital public infrastructure, cloud adoption, digital payments, e-commerce, and AI-enabled enterprise applications is driving organizations to adopt intelligent security operations capable of managing increasingly complex cyber threats. At the same time, the convergence of AI with Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), and User and Entity Behavior Analytics (UEBA) is transforming conventional SOCs into AI-assisted command centers that automate alert triage, threat correlation, and incident response. According to an IDC study commissioned by Fortinet, 94% of Indian organizations are already using AI across their cybersecurity environments, reflecting one of the highest enterprise AI adoption rates globally. This shift is particularly evident across banking, financial services, telecommunications, healthcare, and digital commerce, where organizations are leveraging AI to improve operational resilience while addressing persistent cybersecurity talent shortages.

India is also emerging as a major innovation hub for AI-driven cybersecurity services. Leading IT service providers such as Infosys, TCS, Wipro, and HCLTech are integrating generative AI, automation, and advanced analytics into managed security operations, while domestic cybersecurity companies are introducing AI-native SOC platforms tailored for enterprise environments. In 2026, ProTechmanize launched an AI-Driven Security Operations Center (AISOC) in Mumbai powered by its Aquila I platform, combining AI, Continuous Threat Exposure Management (CTEM), threat intelligence, and human expertise to deliver predictive cyber defense. At the same time, specialized providers such as CyberNX are expanding AI-enabled SOC and MDR services across regulated industries, reflecting growing demand for autonomous and cloud-native security operations. Supported by India's expanding AI ecosystem, digital infrastructure investments, and strong cybersecurity services industry, the country is expected to emerge as one of the fastest-growing markets for AI SOC solutions in the Asia Pacific region.

TABLE 260 INDIA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	126.5	158.0	197.8	248.1	25.2%
Services	72.6	92.1	117.1	149.2	27.1%
Total	**199.1**	**250.1**	**314.9**	**397.2**	**25.9%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 261 INDIA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	311.9	393.2	496.7	628.8	797.2	1,009.0	26.5%
Services	190.5	244.0	313.2	402.9	519.0	667.7	28.5%
Total	**502.4**	**637.2**	**810.0**	**1,031.7**	**1,316.2**	**1,676.7**	**27.3%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 262 INDIA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	46.5	56.0	67.3	81.0	20.3%
AI-orchestrated Response and Automation Platforms	19.4	23.7	29.0	35.4	22.2%
AI-native SOC Platforms	27.0	34.2	43.4	55.1	26.8%
AI SOC Agent Solutions	7.2	10.1	14.1	19.8	39.8%
Security Data Platforms	6.2	7.7	9.5	11.8	24.0%
Threat Intelligence Platforms	8.3	10.2	12.7	15.8	24.0%
AI Governance, Risk, and Compliance Solutions	11.8	16.1	21.8	29.1	35.2%
Total	**126.5**	**158.0**	**197.8**	**248.1**	**25.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 263 INDIA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	97.6	117.6	141.7	170.8	205.5	246.2	20.3%
AI-orchestrated Response and Automation Platforms	43.4	53.3	65.6	80.7	99.5	122.3	23.0%
AI-native SOC Platforms	70.2	89.6	114.6	146.9	188.5	241.5	28.0%
AI SOC Agent Solutions	27.8	39.2	55.3	78.2	110.7	156.5	41.3%
Security Data Platforms	14.7	18.4	23.0	28.8	36.1	45.3	25.2%
Threat Intelligence Platforms	19.6	24.5	30.6	38.4	48.2	60.3	25.2%
AI Governance, Risk, and Compliance Solutions	38.6	50.6	65.9	85.1	108.7	136.9	28.8%
Total	**311.9**	**393.2**	**496.7**	**628.8**	**797.2**	**1,009.0**	**26.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 264 INDIA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	39.2	48.8	61.0	76.4	24.9%
AI SOC-as-a-Service (SOCaaS)	2.3	3.6	5.6	8.7	56.4%
Incident Response and Forensics Services	4.9	6.4	8.5	11.2	32.1%
Threat Intelligence and Advisory Services	26.3	33.2	42.1	52.9	26.2%
Total	**72.6**	**92.1**	**117.1**	**149.2**	**27.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 265 INDIA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	95.7	120.2	151.4	191.0	241.4	304.7	26.1%
AI SOC-as-a-Service (SOCaaS)	12.3	17.5	24.9	35.4	50.6	72.2	42.5%
Incident Response and Forensics Services	14.8	19.6	25.9	34.4	45.8	60.8	32.7%
Threat Intelligence and Advisory Services	67.8	86.8	111.1	142.0	181.2	230.0	27.7%
Total	**190.5**	**244.0**	**313.2**	**402.9**	**519.0**	**667.7**	**28.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 266 INDIA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	143.7	177.9	220.9	274.7	24.1%
SMEs	55.5	72.2	94.0	122.6	30.3%
Total	**199.1**	**250.1**	**314.9**	**397.2**	**25.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 267 INDIA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	342.5	428.3	536.8	674.1	847.9	1,064.9	25.5%
SMEs	159.9	208.9	273.2	357.6	468.3	611.8	30.8%
Total	**502.4**	**637.2**	**810.0**	**1,031.7**	**1,316.2**	**1,676.7**	**27.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 268 INDIA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	51.7	63.3	77.6	95.6	22.7%
Alert Triage and Prioritization	24.3	31.9	41.8	55.0	31.2%
Incident Investigation and Analysis	23.8	30.9	40.1	52.2	29.9%
Threat Hunting	15.4	19.6	24.9	31.8	27.3%
Incident Response and Remediation	24.8	30.8	38.3	47.7	24.3%
Insider Threat Detection	8.9	11.6	15.2	19.9	30.7%
Cloud Security Monitoring	16.9	20.8	25.7	31.8	23.4%
Identity and Access Monitoring	9.1	11.8	15.3	19.9	29.7%
Compliance Monitoring and Reporting	5.0	6.7	8.9	11.9	33.6%
Security Analytics and Visualization	19.1	22.7	27.0	31.5	18.2%
Total	**199.1**	**250.1**	**314.9**	**397.2**	**25.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 269 INDIA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	117.3	144.5	178.3	220.5	273.2	337.9	23.6%
Alert Triage and Prioritization	72.0	94.4	124.2	163.7	216.1	284.9	31.7%
Incident Investigation and Analysis	67.9	88.5	115.6	151.3	198.3	259.6	30.8%
Threat Hunting	40.6	52.1	66.9	86.1	110.9	142.8	28.6%
Incident Response and Remediation	59.5	74.4	93.3	117.2	147.5	185.3	25.5%
Insider Threat Detection	26.0	34.0	44.6	58.6	77.1	101.4	31.3%
Cloud Security Monitoring	39.3	48.8	60.7	75.6	94.3	117.6	24.5%
Identity and Access Monitoring	25.8	33.6	43.8	57.2	74.9	97.9	30.6%
Compliance Monitoring and Reporting	15.8	21.0	27.9	37.2	49.7	66.2	33.2%
Security Analytics and Visualization	38.2	46.0	54.7	64.3	74.1	83.2	16.9%
Total	**502.4**	**637.2**	**810.0**	**1,031.7**	**1,316.2**	**1,676.7**	**27.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 270 INDIA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	37.4	46.2	57.1	70.8	23.7%
Government & Defense	32.4	39.7	48.7	60.0	22.9%
Healthcare & Life sciences	24.5	31.9	41.7	54.5	30.6%
IT & Telecommunications	22.5	27.8	34.4	42.7	23.9%
Manufacturing	20.1	24.4	29.5	35.9	21.3%
Retail & eCommerce	14.4	18.3	23.5	30.1	27.9%
Energy & Utilities	13.2	17.0	21.8	28.1	28.5%
Media & Entertainment	10.1	12.8	16.3	20.7	27.0%
Education	7.9	10.2	13.2	17.0	29.2%
Other Verticals	16.6	21.9	28.7	37.3	31.0%
Total	**199.1**	**250.1**	**314.9**	**397.2**	**25.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 271 INDIA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	87.9	109.3	136.2	170.2	212.9	265.9	24.8%
Government & Defense	73.8	91.0	112.5	139.3	172.7	213.9	23.7%
Healthcare & Life sciences	71.5	94.1	124.1	164.1	217.2	287.0	32.0%
IT & Telecommunications	53.1	66.3	82.8	103.7	130.0	162.8	25.1%
Manufacturing	43.4	52.5	63.7	77.4	94.2	114.4	21.4%
Retail & eCommerce	38.6	49.6	64.0	82.7	107.0	138.3	29.1%
Energy & Utilities	36.3	46.9	60.9	79.2	103.1	134.0	29.9%
Media & Entertainment	26.4	33.8	43.4	55.7	71.7	92.1	28.4%
Education	22.1	28.6	37.2	48.5	63.3	82.5	30.2%
Other Verticals	49.4	65.0	85.1	111.0	144.1	185.8	30.3%
Total	**502.4**	**637.2**	**810.0**	**1,031.7**	**1,316.2**	**1,676.7**	**27.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.4.5 REST OF ASIA PACIFIC

The Rest of Asia Pacific, comprising Singapore, South Korea, Australia, New Zealand, Indonesia, Malaysia, Thailand, Vietnam, the Philippines, and other ASEAN economies, is witnessing robust growth in AI SOC adoption as organizations accelerate digital modernization while strengthening cyber resilience across increasingly interconnected economies. Unlike China, Japan, and India, where domestic AI innovation and national AI strategies are the primary growth catalysts, these markets are emphasizing secure digital transformation, operational resilience, and enterprise cybersecurity modernization. Rapid expansion of digital banking, cloud-based business applications, critical infrastructure digitization, and connected supply chains is increasing the need for AI-driven security operations capable of delivering continuous threat monitoring, intelligent alert prioritization, and automated incident response across distributed enterprise environments. Regional enterprises are also increasing investments in AI-enabled cybersecurity to secure hybrid work environments, cloud-native applications, and expanding digital ecosystems.

Governments across the region are complementing enterprise investments by strengthening national cyber resilience and critical infrastructure protection. Australia continues implementing its 2023-2030 Cyber Security Strategy, focusing on resilient digital infrastructure, cyber preparedness, and stronger public-private collaboration, while Singapore's Digital Enterprise Blueprint (DEB) and the AI for Enterprise Impact Playbook, introduced in 2026, provide structured guidance for enterprises to adopt AI while strengthening cyber resilience and digital trust. Across Southeast Asia, governments are expanding national cybersecurity capabilities, digital trust initiatives, and cyber capacity-building programs to improve preparedness against increasingly sophisticated AI-enabled cyber threats targeting financial services, healthcare, telecommunications, transportation, and government services. These efforts are creating favorable conditions for enterprises to modernize legacy SOC environments with AI-assisted detection, automated investigation, and response capabilities.

The region is also emerging as a strategic destination for cybersecurity investment and managed security services as organizations increasingly seek scalable security operations to address growing cyber complexity. Enterprises are partnering with cloud service providers, MSSPs, and systems integrators to integrate AI into existing SOC environments without significant in-house resource expansion. Growing investments in hyperscale cloud infrastructure, regional data centers, digital commerce, and secure cross-border digital services are further driving demand for AI-native SOC platforms capable of protecting complex hybrid and multi-cloud environments. As cyber threats continue to evolve alongside rapid digitalization, the Rest of Asia Pacific is expected to offer significant growth opportunities for AI SOC platform providers and managed AI security service vendors throughout the forecast period.

TABLE 272 REST OF ASIA PACIFIC: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	410.3	513.4	643.5	807.6	25.3%
Services	235.5	299.3	381.0	485.7	27.3%
Total	**645.9**	**812.7**	**1,024.5**	**1,293.3**	**26.0%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 273 REST OF ASIA PACIFIC: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	1,015.6	1,279.9	1,615.9	2,046.3	2,592.0	3,285.5	26.5%
Services	620.4	794.3	1,018.9	1,311.1	1,687.7	2,174.2	28.5%
Total	**1,636.1**	**2,074.2**	**2,634.8**	**3,357.4**	**4,279.7**	**5,459.8**	**27.3%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 274 REST OF ASIA PACIFIC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	153.0	183.1	219.0	263.8	19.9%
AI-orchestrated Response and Automation Platforms	63.3	77.2	94.3	115.4	22.1%
AI-native SOC Platforms	87.7	111.2	141.2	179.5	26.9%
AI SOC Agent Solutions	27.3	43.7	66.8	102.6	55.4%
Security Data Platforms	20.1	24.9	30.9	38.5	24.1%
Threat Intelligence Platforms	26.8	33.2	41.3	51.3	24.1%
AI Governance, Risk, and Compliance Solutions	32.0	40.0	50.1	56.7	21.0%
Total	**410.3**	**513.4**	**643.5**	**807.6**	**25.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 275 REST OF ASIA PACIFIC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	312.7	371.5	442.2	527.9	630.3	753.2	19.2%
AI-orchestrated Response and Automation Platforms	140.8	172.2	211.0	259.4	318.9	392.3	22.7%
AI-native SOC Platforms	228.4	291.3	372.2	477.1	611.6	784.6	28.0%
AI SOC Agent Solutions	143.3	200.6	281.4	395.9	557.1	784.6	40.5%
Security Data Platforms	47.9	59.7	74.6	93.5	117.3	147.1	25.2%
Threat Intelligence Platforms	63.8	79.6	99.5	124.7	156.3	196.2	25.2%
AI Governance, Risk, and Compliance Solutions	78.7	104.9	134.9	167.8	200.5	227.6	23.7%
Total	**1,015.6**	**1,279.9**	**1,615.9**	**2,046.3**	**2,592.0**	**3,285.5**	**26.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 276 REST OF ASIA PACIFIC: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	127.0	158.6	198.4	248.6	25.1%
AI SOC-as-a-Service (SOCaaS)	7.4	11.8	18.2	28.3	56.6%
Incident Response and Forensics Services	15.8	20.9	27.6	36.5	32.3%
Threat Intelligence and Advisory Services	85.4	108.0	136.8	172.3	26.4%
Total	**235.5**	**299.3**	**381.0**	**485.7**	**27.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 277 REST OF ASIA PACIFIC: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	311.6	391.3	492.4	621.6	785.0	992.1	26.1%
AI SOC-as-a-Service (SOCaaS)	40.0	56.8	80.8	115.4	164.7	235.2	42.5%
Incident Response and Forensics Services	48.2	63.7	84.3	112.1	148.9	198.1	32.7%
Threat Intelligence and Advisory Services	220.7	282.5	361.3	462.1	589.1	748.8	27.7%
Total	**620.4**	**794.3**	**1,018.9**	**1,311.1**	**1,687.7**	**2,174.2**	**28.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 278 REST OF ASIA PACIFIC: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	466.0	578.1	718.6	894.3	24.3%
SMEs	179.9	234.6	306.0	399.0	30.4%
Total	**645.9**	**812.7**	**1,024.5**	**1,293.3**	**26.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 279 REST OF ASIA PACIFIC: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	1,115.4	1,394.2	1,746.1	2,193.6	2,756.9	3,467.6	25.5%
SMEs	520.7	680.0	888.7	1,163.8	1,522.8	1,992.2	30.8%
Total	**1,636.1**	**2,074.2**	**2,634.8**	**3,357.4**	**4,279.7**	**5,459.8**	**27.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 280 REST OF ASIA PACIFIC: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	167.6	205.7	252.6	311.1	22.9%
Alert Triage and Prioritization	79.0	103.6	136.0	179.0	31.4%
Incident Investigation and Analysis	77.3	100.4	130.5	170.1	30.1%
Threat Hunting	50.0	63.7	81.1	103.5	27.4%
Incident Response and Remediation	80.6	100.1	124.6	155.3	24.4%
Insider Threat Detection	28.9	37.7	49.4	64.7	30.9%
Cloud Security Monitoring	54.9	67.7	83.6	103.5	23.6%
Identity and Access Monitoring	29.6	38.3	49.8	64.7	29.8%
Compliance Monitoring and Reporting	16.3	21.7	29.0	38.9	33.7%
Security Analytics and Visualization	61.8	73.8	88.0	102.4	18.3%
Total	**645.9**	**812.7**	**1,024.5**	**1,293.3**	**26.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 281 REST OF ASIA PACIFIC: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	382.1	470.3	580.1	717.7	888.3	1,100.2	23.6%
Alert Triage and Prioritization	234.4	307.4	404.1	532.8	702.7	927.6	31.7%
Incident Investigation and Analysis	221.1	288.0	376.0	492.3	644.8	845.3	30.8%
Threat Hunting	132.3	169.5	217.5	280.1	360.7	464.9	28.6%
Incident Response and Remediation	193.7	242.2	303.5	381.4	479.5	603.3	25.5%
Insider Threat Detection	84.5	110.6	145.0	190.7	250.8	330.2	31.3%
Cloud Security Monitoring	128.1	158.9	197.4	246.0	306.8	382.8	24.5%
Identity and Access Monitoring	84.0	109.3	142.5	186.3	243.6	318.9	30.6%
Compliance Monitoring and Reporting	51.5	68.3	90.8	121.0	161.5	215.6	33.2%
Security Analytics and Visualization	124.3	149.6	178.0	209.2	241.1	271.0	16.9%
Total	**1,636.1**	**2,074.2**	**2,634.8**	**3,357.4**	**4,279.7**	**5,459.8**	**27.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 282 REST OF ASIA PACIFIC: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	121.5	150.2	185.9	230.6	23.8%
Government & Defense	105.0	128.9	158.5	195.3	23.0%
Healthcare & Life sciences	79.4	103.6	135.5	177.5	30.8%
IT & Telecommunications	72.8	90.2	112.0	139.2	24.1%
Manufacturing	65.3	79.2	96.0	116.9	21.4%
Retail & eCommerce	46.6	59.6	76.3	97.9	28.0%
Energy & Utilities	43.0	55.2	71.0	91.4	28.6%
Media & Entertainment	32.8	41.7	53.0	67.5	27.2%
Education	25.6	33.1	42.8	55.5	29.3%
Other Verticals	53.9	71.1	93.5	121.5	31.1%
Total	**645.9**	**812.7**	**1,024.5**	**1,293.3**	**26.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 283 REST OF ASIA PACIFIC: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	286.1	355.7	443.1	553.7	692.1	865.8	24.8%
Government & Defense	240.3	296.2	365.9	453.2	561.7	696.5	23.7%
Healthcare & Life sciences	233.0	306.4	403.9	533.9	706.1	934.6	32.0%
IT & Telecommunications	173.1	215.7	269.4	337.4	422.8	530.2	25.1%
Manufacturing	141.2	170.9	207.2	251.9	306.2	372.4	21.4%
Retail & eCommerce	125.6	161.5	208.2	269.1	348.0	450.3	29.1%
Energy & Utilities	118.1	152.8	198.1	257.6	335.1	436.3	29.9%
Media & Entertainment	86.1	110.1	141.1	181.4	233.2	300.0	28.4%
Education	71.8	93.2	121.1	157.9	205.9	268.7	30.2%
Other Verticals	160.8	211.6	277.0	361.3	468.7	604.9	30.3%
Total	**1,636.1**	**2,074.2**	**2,634.8**	**3,357.4**	**4,279.7**	**5,459.8**	**27.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.5 MIDDLE EAST & AFRICA

The Middle East & Africa (MEA) is emerging as a strategically important market for AI SOCs, driven by large-scale investments in sovereign artificial intelligence, national cybersecurity programs, and digital economy transformation. Unlike North America, where innovation is led by technology providers, or Europe, where regulatory compliance is the primary catalyst, the MEA region is characterized by government-led digital transformation agendas and increasing investments in resilient digital infrastructure. Across the Gulf Cooperation Council (GCC), organizations are accelerating the adoption of AI-driven security operations to secure smart cities, energy infrastructure, financial services, telecommunications, and public sector digital services. At the same time, African economies are strengthening cybersecurity capabilities to support expanding digital economies, cloud adoption, and critical infrastructure modernization, creating growing demand for AI-enabled threat detection, security analytics, and automated incident response.

Regional governments are increasingly integrating AI into national cybersecurity strategies while strengthening cyber resilience through new governance frameworks and cross-sector collaboration. During 2025-2026, Saudi Arabia's National Cybersecurity Authority (NCA) introduced AI Cybersecurity Guidelines to establish governance, defense, resilience, and third-party security requirements for AI systems deployed across public and private organizations. In parallel, the African Union continues to advance implementation of its Continental AI Strategy, encouraging member states to develop national AI policies, strengthen cybersecurity governance, and expand secure digital infrastructure. The region is also witnessing increasing collaboration between governments, regulators, academia, and technology providers to improve AI governance, cyber resilience, and critical infrastructure protection while enabling the secure adoption of AI across strategic sectors.

Looking ahead, the Middle East & Africa is expected to present significant opportunities for AI SOC providers as organizations transition from conventional security operations to intelligent, automated cyber defense. Rapid investments in hyperscale data centers, sovereign cloud platforms, digital government initiatives, and critical infrastructure modernization are increasing demand for AI-native SOC platforms capable of delivering continuous monitoring, autonomous threat investigation, and predictive security analytics. As governments continue prioritizing digital resilience, AI innovation, and cyber capacity building, the region is expected to become an increasingly attractive market for AI-driven security operations and managed cybersecurity services throughout the forecast period.

13.5.1 MIDDLE EAST & AFRICA: AI SOC MARKET DRIVERS

- Governments across the Middle East & Africa are embedding artificial intelligence into national cybersecurity strategies, sovereign AI programs, and digital transformation agendas. Initiatives such as Saudi Arabia's Vision 2030, the UAE's AI-native government strategy, GCC AI programs, and the African Union's Continental AI Strategy are accelerating enterprise investments in AI-enabled security operations.
- Large-scale modernization of energy, utilities, transportation, telecommunications, financial services, and government infrastructure is increasing the need for AI-powered threat detection and automated incident response. Organizations are adopting AI SOC platforms to secure operational technology (OT), cloud environments, and mission-critical digital assets against increasingly sophisticated cyber threats.
- Rapid deployment of sovereign cloud platforms, hyperscale data centers, and AI computing infrastructure across the GCC and other MEA countries is transforming enterprise security requirements. As organizations migrate critical workloads to hybrid and cloud-native environments, demand is growing for AI SOC platforms capable of delivering continuous monitoring, AI-driven analytics, and autonomous threat response.

JULY 2026 © MarketsandMarkets™

- Governments are introducing AI governance frameworks, cybersecurity guidelines, and national security policies to promote secure AI adoption and protect critical digital infrastructure. These evolving regulatory requirements are encouraging enterprises to modernize conventional SOC environments with AI-assisted threat intelligence, automated investigation, and continuous compliance monitoring.
- The expansion of AI-enabled public services, smart cities, digital identity platforms, and e-government ecosystems across the Middle East and Africa is creating new cybersecurity requirements. Public-sector organizations are increasingly deploying AI SOC solutions to improve cyber situational awareness, accelerate incident response, and secure interconnected digital services supporting citizens and critical infrastructure.
- As organizations across Africa and emerging Middle Eastern economies accelerate digital transformation, many are adopting managed AI security operations to overcome resource constraints and strengthen cyber resilience. Increasing reliance on managed SOCs, AI-assisted threat intelligence, and automated security operations is creating significant opportunities for AI SOC platforms and managed security service providers across the region.

TABLE 284 MIDDLE EAST & AFRICA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	253.0	311.0	382.6	472.2	23.1%
Services	145.3	181.3	226.6	284.0	25.0%
Total	**398.3**	**492.3**	**609.2**	**756.2**	**23.8%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 285 MIDDLE EAST & AFRICA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	581.1	717.0	886.6	1,098.6	1,363.2	1,692.5	23.8%
Services	355.0	445.0	559.1	703.9	887.6	1,120.0	25.8%
Total	**936.1**	**1,161.9**	**1,445.7**	**1,802.5**	**2,250.8**	**2,812.6**	**24.6%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 286 MIDDLE EAST & AFRICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	93.5	110.4	130.2	154.2	18.2%
AI-orchestrated Response and Automation Platforms	38.9	46.7	56.0	67.5	20.1%
AI-native SOC Platforms	54.1	67.3	83.9	104.9	24.7%
AI SOC Agent Solutions	15.3	22.1	31.6	45.5	43.9%
Security Data Platforms	12.4	15.1	18.4	22.5	21.9%
Threat Intelligence Platforms	16.5	20.1	24.5	30.0	21.9%
AI Governance, Risk, and Compliance Solutions	22.3	29.2	37.9	47.6	28.8%
Total	**253.0**	**311.0**	**382.6**	**472.2**	**23.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 287 MIDDLE EAST & AFRICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	180.8	212.1	249.2	292.8	343.9	403.5	17.4%
AI-orchestrated Response and Automation Platforms	80.8	97.0	116.6	140.4	169.2	204.0	20.3%
AI-native SOC Platforms	130.8	163.3	204.5	256.4	322.1	404.7	25.4%
AI SOC Agent Solutions	62.6	86.3	119.2	164.9	228.5	316.8	38.3%
Security Data Platforms	27.4	33.5	41.0	50.3	61.7	75.9	22.6%
Threat Intelligence Platforms	36.5	44.6	54.6	67.0	82.3	101.1	22.6%
AI Governance, Risk, and Compliance Solutions	62.3	80.2	101.6	126.8	155.5	186.7	24.6%
Total	**581.1**	**717.0**	**886.6**	**1,098.6**	**1,363.2**	**1,692.5**	**23.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 288 MIDDLE EAST & AFRICA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	78.3	96.1	118.0	145.4	22.9%
AI SOC-as-a-Service (SOCaaS)	4.5	7.2	10.8	16.5	53.9%
Incident Response and Forensics Services	9.7	12.6	16.4	21.4	29.9%
Threat Intelligence and Advisory Services	52.7	65.4	81.4	100.7	24.1%
Total	**145.3**	**181.3**	**226.6**	**284.0**	**25.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 289 MIDDLE EAST & AFRICA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	178.3	219.2	270.2	333.7	412.8	511.1	23.4%
AI SOC-as-a-Service (SOCaaS)	22.9	31.8	44.4	61.9	86.6	121.2	39.5%
Incident Response and Forensics Services	27.6	35.7	46.3	60.2	78.3	102.0	29.9%
Threat Intelligence and Advisory Services	126.3	158.3	198.3	248.1	309.8	385.8	25.0%
Total	**355.0**	**445.0**	**559.1**	**703.9**	**887.6**	**1,120.0**	**25.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 290 MIDDLE EAST & AFRICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	287.4	350.2	427.3	522.9	22.1%
SMEs	110.9	142.1	181.9	233.3	28.1%
Total	**398.3**	**492.3**	**609.2**	**756.2**	**23.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 291 MIDDLE EAST & AFRICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	638.2	781.0	958.1	1,177.7	1,449.9	1,786.3	22.9%
SMEs	297.9	380.9	487.6	624.8	800.9	1,026.3	28.1%
Total	**936.1**	**1,161.9**	**1,445.7**	**1,802.5**	**2,250.8**	**2,812.6**	**24.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 292 MIDDLE EAST & AFRICA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	103.4	124.6	150.2	181.9	20.7%
Alert Triage and Prioritization	48.7	62.8	80.9	104.7	29.1%
Incident Investigation and Analysis	47.6	60.8	77.6	99.5	27.8%
Threat Hunting	30.9	38.6	48.2	60.5	25.2%
Incident Response and Remediation	49.7	60.6	74.1	90.8	22.2%
Insider Threat Detection	17.8	22.9	29.4	37.9	28.6%
Cloud Security Monitoring	33.8	41.0	49.7	60.5	21.4%
Identity and Access Monitoring	18.2	23.2	29.6	37.9	27.6%
Compliance Monitoring and Reporting	10.0	13.2	17.2	22.7	31.4%
Security Analytics and Visualization	38.1	44.7	52.3	59.9	16.2%
Total	**398.3**	**492.3**	**609.2**	**756.2**	**23.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 293 MIDDLE EAST & AFRICA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	218.6	263.5	318.3	385.3	467.2	566.8	21.0%
Alert Triage and Prioritization	134.1	172.2	221.7	286.0	369.6	477.8	28.9%
Incident Investigation and Analysis	126.5	161.3	206.3	264.3	339.1	435.4	28.0%
Threat Hunting	75.7	95.0	119.4	150.4	189.7	239.5	25.9%
Incident Response and Remediation	110.8	135.7	166.5	204.8	252.2	310.8	22.9%
Insider Threat Detection	48.4	61.9	79.5	102.4	131.9	170.1	28.6%
Cloud Security Monitoring	73.3	89.0	108.3	132.1	161.3	197.2	21.9%
Identity and Access Monitoring	48.1	61.2	78.2	100.0	128.1	164.3	27.9%
Compliance Monitoring and Reporting	29.4	38.2	49.8	65.0	84.9	111.0	30.4%
Security Analytics and Visualization	71.1	83.8	97.7	112.3	126.8	139.6	14.4%
Total	**936.1**	**1,161.9**	**1,445.7**	**1,802.5**	**2,250.8**	**2,812.6**	**24.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 294 MIDDLE EAST & AFRICA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	74.9	91.0	110.5	134.9	21.7%
Government & Defense	64.7	78.1	94.2	114.2	20.8%
Healthcare & Life sciences	48.9	62.8	80.6	103.8	28.5%
IT & Telecommunications	44.9	54.7	66.6	81.4	21.9%
Manufacturing	40.3	48.0	57.1	68.4	19.3%
Retail & eCommerce	28.8	36.1	45.4	57.2	25.8%
Energy & Utilities	26.5	33.4	42.2	53.5	26.4%
Media & Entertainment	20.2	25.2	31.5	39.5	24.9%
Education	15.8	20.1	25.5	32.4	27.1%
Other Verticals	33.2	43.0	55.6	71.0	28.8%
Total	**398.3**	**492.3**	**609.2**	**756.2**	**23.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 295 MIDDLE EAST & AFRICA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	163.7	199.3	243.1	297.3	364.0	446.0	22.2%
Government & Defense	137.5	165.9	200.7	243.3	295.4	358.8	21.1%
Healthcare & Life sciences	133.3	171.7	221.6	286.6	371.4	481.5	29.3%
IT & Telecommunications	99.0	120.8	147.8	181.2	222.4	273.1	22.5%
Manufacturing	80.8	95.7	113.7	135.2	161.0	191.9	18.9%
Retail & eCommerce	71.9	90.5	114.2	144.5	183.0	232.0	26.4%
Energy & Utilities	67.6	85.6	108.7	138.3	176.2	224.8	27.2%
Media & Entertainment	49.3	61.7	77.4	97.4	122.6	154.6	25.7%
Education	41.1	52.2	66.5	84.8	108.3	138.4	27.5%
Other Verticals	92.0	118.5	152.0	194.0	246.5	311.6	27.6%
Total	**936.1**	**1,161.9**	**1,445.7**	**1,802.5**	**2,250.8**	**2,812.6**	**24.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 296 MIDDLE EAST & AFRICA: AI SOC MARKET, BY COUNTRY, 2022–2025 (USD MILLION)

Country	2022	2023	2024	2025	CAGR (2022–2025)
GCC	302.8	372.3	458.3	565.9	23.2%
Rest of Middle East	60.3	76.3	96.5	122.4	26.6%
Africa	35.1	43.7	54.4	67.9	24.6%
Total	**398.3**	**492.3**	**609.2**	**756.2**	**23.8%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 297 MIDDLE EAST & AFRICA: AI SOC MARKET, BY COUNTRY, 2026–2031 (USD MILLION)

Country	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
GCC	696.6	859.6	1,063.3	1,317.7	1,635.2	2,030.4	23.9%
Rest of Middle East	154.9	196.6	250.1	318.8	407.0	519.9	27.4%
Africa	84.6	105.7	132.3	166.0	208.6	262.3	25.4%
Total	**936.1**	**1,161.9**	**1,445.7**	**1,802.5**	**2,250.8**	**2,812.6**	**24.6%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

13.5.2 GULF COOPERATION COUNCIL (GCC)

13.5.2.1 Sovereign AI investments and regional cybersecurity cooperation strengthening intelligent cyber resilience

The Gulf Cooperation Council (GCC) countries, including the Kingdom of Saudi Arabia (KSA) and the United Arab Emirates (UAE), are emerging as one of the fastest-growing markets for AI SOCs, driven by sovereign AI investments, digital economy diversification, and large-scale cybersecurity modernization. The GCC is characterized by coordinated government-led initiatives that integrate artificial intelligence into national cybersecurity, cloud infrastructure, smart cities, energy, financial services, and digital government programs. The region's rapid deployment of hyperscale data centers, sovereign cloud platforms, and AI-enabled digital services is significantly expanding demand for intelligent security operations capable of protecting increasingly interconnected critical infrastructure and digital assets. These developments are encouraging enterprises to transition from conventional SOCs to AI-driven platforms that deliver real-time threat detection, automated investigation, and autonomous response capabilities.

Cybersecurity cooperation has also become a defining characteristic of the GCC market. During 2025, the GCC Ministerial Committee for Cybersecurity approved the Executive Plan for the Gulf Cybersecurity Strategy (2024-2028), alongside a regional framework for international cybersecurity cooperation and a governance mechanism for the GCC Cyber Threat Information Sharing Platform. The initiative aims to strengthen cross-border cyber resilience through coordinated threat intelligence sharing, joint cyber exercises, harmonized cybersecurity policies, and collaborative incident response among member states. Simultaneously, GCC governments continue to position artificial intelligence as a strategic pillar of economic diversification by aligning national AI strategies with cybersecurity, digital infrastructure, and critical infrastructure protection, creating a favorable environment for enterprise adoption of AI-enabled security operations.

Looking ahead, the GCC is expected to remain a strategic growth market for AI SOC solutions as governments continue investing in AI infrastructure, secure cloud ecosystems, and resilient digital economies. The region is witnessing increasing collaboration between hyperscale cloud providers, telecommunications operators, cybersecurity firms, and public-sector organizations to develop AI-ready security architectures capable of supporting next-generation digital services. As national visions focused on economic diversification and digital competitiveness continue to mature, enterprises across the GCC are expected to accelerate investments in AI-native SOC platforms, autonomous threat detection, and intelligent cyber defense to enhance operational resilience and protect rapidly expanding digital ecosystems.

JULY 2026 © MarketsandMarkets™

TABLE 298 GCC: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	192.4	235.2	287.9	353.4	22.5%
Services	110.4	137.1	170.5	212.5	24.4%
Total	**302.8**	**372.3**	**458.3**	**565.9**	**23.2%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 299 GCC: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	432.4	530.4	652.1	803.1	990.4	1,221.8	23.1%
Services	264.2	329.2	411.2	514.6	644.9	808.5	25.1%
Total	**696.6**	**859.6**	**1,063.3**	**1,317.7**	**1,635.2**	**2,030.4**	**23.9%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 300 GCC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	71.0	83.4	98.0	115.4	17.6%
AI-orchestrated Response and Automation Platforms	29.6	35.3	42.2	50.5	19.5%
AI-native SOC Platforms	41.1	50.9	63.2	78.5	24.1%
AI SOC Agent Solutions	11.5	16.3	22.9	32.4	41.5%
Security Data Platforms	9.4	11.4	13.8	16.8	21.3%
Threat Intelligence Platforms	12.6	15.2	18.5	22.4	21.3%
AI Governance, Risk, and Compliance Solutions	17.2	22.6	29.4	37.2	29.3%
Total	**192.4**	**235.2**	**287.9**	**353.4**	**22.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 301 GCC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	134.7	157.4	184.0	215.2	251.4	293.2	16.8%
AI-orchestrated Response and Automation Platforms	60.1	71.8	85.8	102.8	123.1	147.5	19.6%
AI-native SOC Platforms	97.3	120.9	150.4	187.5	234.0	292.2	24.6%
AI SOC Agent Solutions	44.3	60.8	83.4	114.7	158.0	217.6	37.5%
Security Data Platforms	20.4	24.8	30.1	36.7	44.9	54.8	21.9%
Threat Intelligence Platforms	27.2	33.0	40.2	49.0	59.8	73.0	21.9%
AI Governance, Risk, and Compliance Solutions	48.3	61.8	78.1	97.2	119.2	143.6	24.3%
Total	**432.4**	**530.4**	**652.1**	**803.1**	**990.4**	**1,221.8**	**23.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 302 GCC: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	59.6	72.7	88.8	108.8	22.2%
AI SOC-as-a-Service (SOCaaS)	3.4	5.4	8.2	12.4	53.1%
Incident Response and Forensics Services	7.4	9.6	12.3	16.0	29.2%
Threat Intelligence and Advisory Services	40.0	49.5	61.2	75.4	23.5%
Total	**110.4**	**137.1**	**170.5**	**212.5**	**24.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 303 GCC: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	132.7	162.2	198.7	244.0	299.9	368.9	22.7%
AI SOC-as-a-Service (SOCaaS)	17.0	23.6	32.6	45.3	62.9	87.5	38.7%
Incident Response and Forensics Services	20.5	26.4	34.0	44.0	56.9	73.7	29.1%
Threat Intelligence and Advisory Services	94.0	117.1	145.8	181.4	225.1	278.5	24.3%
Total	**264.2**	**329.2**	**411.2**	**514.6**	**644.9**	**808.5**	**25.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 304 GCC: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	218.5	264.9	321.5	391.3	21.4%
SMEs	84.3	107.5	136.9	174.6	27.4%
Total	**302.8**	**372.3**	**458.3**	**565.9**	**23.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 305 GCC: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	474.9	577.8	704.6	860.9	1,053.4	1,289.5	22.1%
SMEs	221.7	281.8	358.7	456.8	581.9	740.9	27.3%
Total	**696.6**	**859.6**	**1,063.3**	**1,317.7**	**1,635.2**	**2,030.4**	**23.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 306 GCC: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	78.6	94.2	113.0	136.1	20.1%
Alert Triage and Prioritization	37.0	47.5	60.9	78.3	28.4%
Incident Investigation and Analysis	36.2	46.0	58.4	74.4	27.1%
Threat Hunting	23.5	29.2	36.3	45.3	24.5%
Incident Response and Remediation	37.8	45.9	55.7	67.9	21.6%
Insider Threat Detection	13.5	17.3	22.1	28.3	27.9%
Cloud Security Monitoring	25.7	31.0	37.4	45.3	20.8%
Identity and Access Monitoring	13.9	17.6	22.3	28.3	26.9%
Compliance Monitoring and Reporting	7.6	10.0	13.0	17.0	30.7%
Security Analytics and Visualization	29.0	33.8	39.3	44.8	15.6%
Total	**302.8**	**372.3**	**458.3**	**565.9**	**23.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 307 GCC: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	162.7	194.9	234.1	281.7	339.4	409.2	20.3%
Alert Triage and Prioritization	99.8	127.4	163.1	209.1	268.5	344.9	28.2%
Incident Investigation and Analysis	94.1	119.4	151.7	193.2	246.4	314.3	27.3%
Threat Hunting	56.3	70.2	87.8	109.9	137.8	172.9	25.1%
Incident Response and Remediation	82.5	100.4	122.5	149.7	183.2	224.4	22.2%
Insider Threat Detection	36.0	45.8	58.5	74.8	95.8	122.8	27.8%
Cloud Security Monitoring	54.5	65.8	79.7	96.6	117.2	142.4	21.2%
Identity and Access Monitoring	35.8	45.3	57.5	73.1	93.1	118.6	27.1%
Compliance Monitoring and Reporting	21.9	28.3	36.6	47.5	61.7	80.2	29.6%
Security Analytics and Visualization	52.9	62.0	71.9	82.1	92.1	100.8	13.7%
Total	**696.6**	**859.6**	**1,063.3**	**1,317.7**	**1,635.2**	**2,030.4**	**23.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 308 GCC: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	56.9	68.8	83.2	100.9	21.0%
Government & Defense	49.2	59.1	70.9	85.5	20.2%
Healthcare & Life sciences	37.2	47.5	60.6	77.7	27.8%
IT & Telecommunications	34.2	41.3	50.1	60.9	21.3%
Manufacturing	30.6	36.3	43.0	51.2	18.7%
Retail & eCommerce	21.9	27.3	34.1	42.8	25.1%
Energy & Utilities	20.1	25.3	31.8	40.0	25.7%
Media & Entertainment	15.4	19.1	23.7	29.5	24.3%
Education	12.0	15.2	19.2	24.3	26.4%
Other Verticals	25.3	32.6	41.8	53.1	28.1%
Total	**302.8**	**372.3**	**458.3**	**565.9**	**23.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 309 GCC: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	121.8	147.4	178.8	217.3	264.4	322.0	21.5%
Government & Defense	102.3	122.8	147.6	177.9	214.6	259.0	20.4%
Healthcare & Life sciences	99.2	127.0	163.0	209.5	269.8	347.6	28.5%
IT & Telecommunications	73.7	89.4	108.7	132.4	161.6	197.2	21.8%
Manufacturing	60.1	70.8	83.6	98.9	117.0	138.5	18.2%
Retail & eCommerce	53.5	66.9	84.0	105.6	132.9	167.5	25.6%
Energy & Utilities	50.3	63.3	79.9	101.1	128.0	162.3	26.4%
Media & Entertainment	36.7	45.6	56.9	71.2	89.1	111.6	24.9%
Education	30.6	38.6	48.9	62.0	78.7	99.9	26.7%
Other Verticals	68.4	87.7	111.8	141.8	179.1	225.0	26.9%
Total	**696.6**	**859.6**	**1,063.3**	**1,317.7**	**1,635.2**	**2,030.4**	**23.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 310 GCC: AI SOC MARKET, BY COUNTRY, 2022–2025 (USD MILLION)

Country	2022	2023	2024	2025	CAGR (2022–2025)
KSA	134.4	162.5	196.7	238.7	21.1%
UAE	95.1	118.2	147.1	183.6	24.5%
Rest of GCC	73.3	91.6	114.6	143.6	25.1%
Total	**302.8**	**372.3**	**458.3**	**565.9**	**23.2%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 311 GCC: AI SOC MARKET, BY COUNTRY, 2026–2031 (USD MILLION)

Country	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
KSA	288.8	350.4	426.0	518.9	632.8	772.2	21.7%
UAE	228.4	284.9	356.2	446.2	559.6	702.3	25.2%
Rest of GCC	179.3	224.3	281.1	352.7	442.8	555.9	25.4%
Total	**696.6**	**859.6**	**1,063.3**	**1,317.7**	**1,635.2**	**2,030.4**	**23.9%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.5.2.2 KSA

13.5.2.2.1 Vision 2030 and national AI governance accelerating intelligent cybersecurity transformation

KSA is at the forefront of AI SOC adoption in the GCC, driven by Vision 2030, large-scale investments in artificial intelligence, and one of the region's most mature national cybersecurity ecosystems. Rather than focusing solely on enterprise digitalization, the Kingdom is integrating AI into national cyber resilience, critical infrastructure protection, and digital government transformation. The Saudi Data and Artificial Intelligence Authority (SDAIA) continues to lead the country's AI strategy by accelerating AI adoption across government and industry, while the National Cybersecurity Authority (NCA) is strengthening governance through comprehensive cybersecurity frameworks and standards. In July 2026, the NCA introduced the AI Cybersecurity Guidelines, providing organizations with a dedicated framework for securing AI systems throughout their lifecycle, including AI governance, model protection, data security, resilience, and third-party risk management. These initiatives are creating a strong regulatory foundation for organizations deploying AI-enabled security operations across energy, finance, telecommunications, healthcare, and public sector environments.

KSA is also rapidly expanding its AI and cybersecurity ecosystem through strategic investments in cloud infrastructure, hyperscale data centers, and advanced digital services. Under Vision 2030, the Kingdom continues to position itself as a regional AI hub by attracting global cloud providers while simultaneously strengthening domestic cyber capabilities through initiatives led by SDAIA, the NCA, and the Global Cybersecurity Forum. The country's expanding digital economy, coupled with increasing investments in smart cities, industrial digitalization, and critical infrastructure modernization, is accelerating demand for AI-driven SOC platforms capable of autonomous threat detection, intelligent security analytics, and automated incident response. As enterprises continue to modernize security operations to protect increasingly connected digital ecosystems, KSA is expected to remain the largest and most advanced AI SOC market within the GCC throughout the forecast period.

TABLE 312 KSA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	85.4	102.7	123.5	149.1	20.4%
Services	49.0	59.8	73.1	89.6	22.3%
Total	**134.4**	**162.5**	**196.7**	**238.7**	**21.1%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 313 KSA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	179.3	216.2	261.3	316.2	383.3	464.7	21.0%
Services	109.5	134.2	164.7	202.6	249.6	307.5	22.9%
Total	**288.8**	**350.4**	**426.0**	**518.9**	**632.8**	**772.2**	**21.7%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 314 KSA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	31.4	36.4	42.0	48.7	15.7%
AI-orchestrated Response and Automation Platforms	13.1	15.4	18.1	21.3	17.5%
AI-native SOC Platforms	18.2	22.2	27.1	33.1	22.0%
AI SOC Agent Solutions	4.9	6.6	8.8	11.9	34.5%
Security Data Platforms	4.2	5.0	5.9	7.1	19.3%
Threat Intelligence Platforms	5.6	6.6	7.9	9.5	19.3%
AI Governance, Risk, and Compliance Solutions	8.0	10.5	13.6	17.5	30.1%
Total	**85.4**	**102.7**	**123.5**	**149.1**	**20.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 315 KSA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	56.1	64.7	74.5	85.9	98.8	113.4	15.1%
AI-orchestrated Response and Automation Platforms	25.0	29.3	34.5	40.6	47.8	56.3	17.7%
AI-native SOC Platforms	40.4	49.3	60.3	73.9	90.6	111.2	22.5%
AI SOC Agent Solutions	16.0	21.5	29.1	39.3	53.2	72.1	35.1%
Security Data Platforms	8.5	10.1	12.1	14.5	17.4	20.8	19.8%
Threat Intelligence Platforms	11.3	13.5	16.1	19.3	23.2	27.8	19.8%
AI Governance, Risk, and Compliance Solutions	22.2	27.8	34.7	42.8	52.3	63.0	23.3%
Total	**179.3**	**216.2**	**261.3**	**316.2**	**383.3**	**464.7**	**21.0%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 316 KSA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	26.4	31.7	38.1	45.9	20.2%
AI SOC-as-a-Service (SOCaaS)	1.5	2.4	3.5	5.2	50.5%
Incident Response and Forensics Services	3.3	4.2	5.3	6.7	27.1%
Threat Intelligence and Advisory Services	17.8	21.6	26.3	31.8	21.4%
Total	**49.0**	**59.8**	**73.1**	**89.6**	**22.3%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 317 KSA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	55.0	66.1	79.6	96.1	116.1	140.3	20.6%
AI SOC-as-a-Service (SOCaaS)	7.1	9.6	13.1	17.8	24.3	33.3	36.3%
Incident Response and Forensics Services	8.5	10.8	13.6	17.3	22.0	28.0	26.9%
Threat Intelligence and Advisory Services	39.0	47.7	58.4	71.4	87.1	105.9	22.1%
Total	**109.5**	**134.2**	**164.7**	**202.6**	**249.6**	**307.5**	**22.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 318 KSA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	97.0	115.6	137.9	165.1	19.4%
SMEs	37.4	46.9	58.7	73.6	25.3%
Total	**134.4**	**162.5**	**196.7**	**238.7**	**21.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 319 KSA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	196.9	235.5	282.3	339.0	407.6	490.4	20.0%
SMEs	91.9	114.9	143.7	179.9	225.2	281.8	25.1%
Total	**288.8**	**350.4**	**426.0**	**518.9**	**632.8**	**772.2**	**21.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 320 KSA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	34.9	41.1	48.5	57.4	18.1%
Alert Triage and Prioritization	16.4	20.7	26.1	33.0	26.2%
Incident Investigation and Analysis	16.1	20.1	25.0	31.4	25.0%
Threat Hunting	10.4	12.7	15.6	19.1	22.4%
Incident Response and Remediation	16.8	20.0	23.9	28.7	19.5%
Insider Threat Detection	6.0	7.5	9.5	11.9	25.7%
Cloud Security Monitoring	11.4	13.5	16.1	19.1	18.7%
Identity and Access Monitoring	6.2	7.7	9.6	11.9	24.7%
Compliance Monitoring and Reporting	3.4	4.3	5.6	7.2	28.5%
Security Analytics and Visualization	12.9	14.8	16.9	18.9	13.7%
Total	**134.4**	**162.5**	**196.7**	**238.7**	**21.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 321 KSA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	67.5	79.5	93.8	110.9	131.3	155.6	18.2%
Alert Triage and Prioritization	41.4	51.9	65.3	82.3	103.9	131.2	26.0%
Incident Investigation and Analysis	39.0	48.7	60.8	76.1	95.3	119.5	25.1%
Threat Hunting	23.4	28.6	35.2	43.3	53.3	65.7	23.0%
Incident Response and Remediation	34.2	40.9	49.1	58.9	70.9	85.3	20.1%
Insider Threat Detection	14.9	18.7	23.4	29.5	37.1	46.7	25.6%
Cloud Security Monitoring	22.6	26.8	31.9	38.0	45.4	54.1	19.1%
Identity and Access Monitoring	14.8	18.5	23.0	28.8	36.0	45.1	24.9%
Compliance Monitoring and Reporting	9.1	11.5	14.7	18.7	23.9	30.5	27.4%
Security Analytics and Visualization	22.0	25.3	28.8	32.3	35.6	38.3	11.8%
Total	**288.8**	**350.4**	**426.0**	**518.9**	**632.8**	**772.2**	**21.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 322 KSA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	25.3	30.0	35.7	42.6	19.0%
Government & Defense	21.8	25.8	30.4	36.1	18.2%
Healthcare & Life sciences	16.5	20.7	26.0	32.8	25.6%
IT & Telecommunications	15.2	18.0	21.5	25.7	19.2%
Manufacturing	13.6	15.8	18.4	21.6	16.7%
Retail & eCommerce	9.7	11.9	14.7	18.1	23.0%
Energy & Utilities	8.9	11.0	13.6	16.9	23.6%
Media & Entertainment	6.8	8.3	10.2	12.5	22.2%
Education	5.3	6.6	8.2	10.2	24.3%
Other Verticals	11.2	14.2	17.9	22.4	26.0%
Total	**134.4**	**162.5**	**196.7**	**238.7**	**21.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 323 KSA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	50.5	60.1	71.6	85.6	102.3	122.4	19.4%
Government & Defense	42.4	50.0	59.2	70.0	83.0	98.5	18.4%
Healthcare & Life sciences	41.1	51.8	65.3	82.5	104.4	132.2	26.3%
IT & Telecommunications	30.6	36.4	43.6	52.1	62.5	75.0	19.7%
Manufacturing	24.9	28.9	33.5	38.9	45.3	52.7	16.1%
Retail & eCommerce	22.2	27.3	33.7	41.6	51.4	63.7	23.5%
Energy & Utilities	20.8	25.8	32.0	39.8	49.6	61.7	24.2%
Media & Entertainment	15.2	18.6	22.8	28.0	34.5	42.4	22.8%
Education	12.7	15.7	19.6	24.4	30.4	38.0	24.5%
Other Verticals	28.4	35.7	44.8	55.8	69.3	85.6	24.7%
Total	**288.8**	**350.4**	**426.0**	**518.9**	**632.8**	**772.2**	**21.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.5.2.3 UAE

13.5.2.3.1 AI-native government and sovereign AI ecosystem transforming digital security

The UAE is positioning itself as a prominent leader in AI-enabled cybersecurity by embedding artificial intelligence into government operations, digital infrastructure, and national cyber resilience. Unlike other GCC countries that primarily focus on AI governance frameworks, the UAE is advancing an AI-native government model, integrating AI into public services, critical infrastructure, and enterprise digital ecosystems. In 2026, the UAE established the Artificial Intelligence and Data Authority to unify national AI, data, and digital government capabilities under a single governance framework. The government also announced a landmark initiative to transform 50% of federal government operations into Agentic AI-driven services within two years, accelerating the adoption of autonomous AI across cybersecurity, governance, and public administration. These initiatives are creating strong demand for AI-powered security operations capable of protecting increasingly autonomous and interconnected digital environments.

The UAE is simultaneously strengthening its cybersecurity ecosystem through sovereign AI platforms, AI security standards, and strategic public-private partnerships. In 2026, the UAE Cyber Security Council introduced the National Cyber Security Policy for Artificial Intelligence, establishing comprehensive requirements for AI governance, model security, adversarial AI protection, AI monitoring, automated incident response, and AI-specific digital forensics. The country has also partnered with leading technology providers to develop AI-driven cybersecurity capabilities, including a strategic collaboration between the UAE Cyber Security Council and Palo Alto Networks to build an AI-driven, data-centric cybersecurity ecosystem, along with the launch of the UAE Sovereign AI Platform by the Cyber Security Council, e&, and Open Innovation AI to support secure deployment of AI across critical infrastructure and government environments. These developments, combined with sustained investments in hyperscale AI infrastructure and secure digital transformation, are expected to position the UAE as one of the GCC's leading markets for AI-native SOC platforms and intelligent cyber defense.

TABLE 324 UAE: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	60.4	74.7	92.4	114.6	23.8%
Services	34.7	43.5	54.7	68.9	25.7%
Total	**95.1**	**118.2**	**147.1**	**183.6**	**24.5%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 325 UAE: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	141.8	175.8	218.4	271.9	338.9	422.6	24.4%
Services	86.6	109.1	137.7	174.2	220.7	279.7	26.4%
Total	**228.4**	**284.9**	**356.2**	**446.2**	**559.6**	**702.3**	**25.2%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 326 UAE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	22.2	26.5	31.5	37.4	19.0%
AI-orchestrated Response and Automation Platforms	9.3	11.2	13.5	16.4	20.8%
AI-native SOC Platforms	12.9	16.2	20.3	25.5	25.4%
AI SOC Agent Solutions	3.5	4.8	6.6	9.2	38.3%
Security Data Platforms	3.0	3.6	4.4	5.5	22.6%
Threat Intelligence Platforms	3.9	4.8	5.9	7.3	22.6%
AI Governance, Risk, and Compliance Solutions	5.6	7.6	10.2	13.5	33.7%
Total	**60.4**	**74.7**	**92.4**	**114.6**	**23.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 327 UAE: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	44.4	52.6	62.3	73.8	87.4	103.1	18.4%
AI-orchestrated Response and Automation Platforms	19.7	23.8	28.8	34.9	42.3	51.2	21.0%
AI-native SOC Platforms	31.9	40.1	50.4	63.5	80.1	101.1	25.9%
AI SOC Agent Solutions	12.6	17.5	24.3	33.8	47.1	65.6	39.0%
Security Data Platforms	6.7	8.2	10.1	12.4	15.4	19.0	23.2%
Threat Intelligence Platforms	8.9	10.9	13.5	16.6	20.5	25.3	23.2%
AI Governance, Risk, and Compliance Solutions	17.5	22.6	29.0	36.8	46.2	57.3	26.8%
Total	**141.8**	**175.8**	**218.4**	**271.9**	**338.9**	**422.6**	**24.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 328 UAE: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	18.7	23.1	28.5	35.3	23.6%
AI SOC-as-a-Service (SOCaaS)	1.1	1.7	2.6	4.0	54.7%
Incident Response and Forensics Services	2.3	3.0	4.0	5.2	30.6%
Threat Intelligence and Advisory Services	12.6	15.7	19.6	24.5	24.8%
Total	**34.7**	**43.5**	**54.7**	**68.9**	**25.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 329 UAE: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	43.5	53.7	66.6	82.6	102.6	127.6	24.0%
AI SOC-as-a-Service (SOCaaS)	5.6	7.8	10.9	15.3	21.5	30.3	40.2%
Incident Response and Forensics Services	6.7	8.7	11.4	14.9	19.5	25.5	30.5%
Threat Intelligence and Advisory Services	30.8	38.8	48.8	61.4	77.0	96.3	25.6%
Total	**86.6**	**109.1**	**137.7**	**174.2**	**220.7**	**279.7**	**26.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 330 UAE: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	68.7	84.1	103.2	126.9	22.7%
SMEs	26.5	34.1	43.9	56.6	28.8%
Total	**95.1**	**118.2**	**147.1**	**183.6**	**24.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 331 UAE: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	155.7	191.5	236.0	291.5	360.5	446.0	23.4%
SMEs	72.7	93.4	120.1	154.7	199.1	256.3	28.7%
Total	**228.4**	**284.9**	**356.2**	**446.2**	**559.6**	**702.3**	**25.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 332 UAE: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	24.7	29.9	36.3	44.2	21.4%
Alert Triage and Prioritization	11.6	15.1	19.5	25.4	29.8%
Incident Investigation and Analysis	11.4	14.6	18.7	24.1	28.5%
Threat Hunting	7.4	9.3	11.6	14.7	25.9%
Incident Response and Remediation	11.9	14.6	17.9	22.0	22.9%
Insider Threat Detection	4.3	5.5	7.1	9.2	29.3%
Cloud Security Monitoring	8.1	9.8	12.0	14.7	22.1%
Identity and Access Monitoring	4.4	5.6	7.1	9.2	28.2%
Compliance Monitoring and Reporting	2.4	3.2	4.2	5.5	32.1%
Security Analytics and Visualization	9.1	10.7	12.6	14.5	16.9%
Total	**95.1**	**118.2**	**147.1**	**183.6**	**24.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 333 UAE: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	53.3	64.6	78.4	95.4	116.1	141.5	21.5%
Alert Triage and Prioritization	32.7	42.2	54.6	70.8	91.9	119.3	29.5%
Incident Investigation and Analysis	30.9	39.6	50.8	65.4	84.3	108.7	28.6%
Threat Hunting	18.5	23.3	29.4	37.2	47.2	59.8	26.5%
Incident Response and Remediation	27.0	33.3	41.0	50.7	62.7	77.6	23.5%
Insider Threat Detection	11.8	15.2	19.6	25.3	32.8	42.5	29.2%
Cloud Security Monitoring	17.9	21.8	26.7	32.7	40.1	49.2	22.5%
Identity and Access Monitoring	11.7	15.0	19.3	24.8	31.9	41.0	28.5%
Compliance Monitoring and Reporting	7.2	9.4	12.3	16.1	21.1	27.7	31.0%
Security Analytics and Visualization	17.4	20.6	24.1	27.8	31.5	34.9	15.0%
Total	**228.4**	**284.9**	**356.2**	**446.2**	**559.6**	**702.3**	**25.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 334 UAE: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	17.9	21.8	26.7	32.7	22.3%
Government & Defense	15.5	18.8	22.8	27.7	21.5%
Healthcare & Life sciences	11.7	15.1	19.5	25.2	29.2%
IT & Telecommunications	10.7	13.1	16.1	19.8	22.6%
Manufacturing	9.6	11.5	13.8	16.6	19.9%
Retail & eCommerce	6.9	8.7	11.0	13.9	26.4%
Energy & Utilities	6.3	8.0	10.2	13.0	27.1%
Media & Entertainment	4.8	6.1	7.6	9.6	25.6%
Education	3.8	4.8	6.1	7.9	27.8%
Other Verticals	7.9	10.3	13.4	17.2	29.5%
Total	**95.1**	**118.2**	**147.1**	**183.6**	**24.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 335 UAE: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	39.9	48.9	59.9	73.6	90.5	111.4	22.8%
Government & Defense	33.5	40.7	49.5	60.2	73.4	89.6	21.7%
Healthcare & Life sciences	32.5	42.1	54.6	71.0	92.3	120.2	29.9%
IT & Telecommunications	24.2	29.6	36.4	44.8	55.3	68.2	23.1%
Manufacturing	19.7	23.5	28.0	33.5	40.0	47.9	19.4%
Retail & eCommerce	17.5	22.2	28.1	35.8	45.5	57.9	27.0%
Energy & Utilities	16.5	21.0	26.8	34.2	43.8	56.1	27.8%
Media & Entertainment	12.0	15.1	19.1	24.1	30.5	38.6	26.3%
Education	10.0	12.8	16.4	21.0	26.9	34.6	28.1%
Other Verticals	22.4	29.1	37.4	48.0	61.3	77.8	28.2%
Total	**228.4**	**284.9**	**356.2**	**446.2**	**559.6**	**702.3**	**25.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.5.2.4 Rest of GCC

The Rest of GCC Countries, comprising Qatar, Kuwait, Bahrain, and Oman, are steadily expanding their AI SOC capabilities by integrating artificial intelligence into national digital transformation, cybersecurity modernization, and critical infrastructure protection. Unlike Saudi Arabia's Vision 2030-led AI ecosystem and the UAE's AI-native government strategy, these countries are focusing on strengthening sector-specific AI adoption, secure digital government services, and resilient cyber infrastructure. Rapid digitalization across the energy, financial services, telecommunications, logistics, and public sectors is increasing demand for AI-driven security operations capable of improving threat detection, security visibility, and incident response across increasingly connected digital environments. Governments are also prioritizing trusted AI deployment and cybersecurity readiness to safeguard national digital assets while supporting long-term economic diversification strategies.

Each country is advancing AI-enabled cybersecurity through distinct national initiatives. Qatar is implementing its National Cybersecurity Strategy (2024-2030) while establishing the National Centre for Artificial Intelligence and expanding the GovAI program to accelerate AI adoption across government services. Bahrain launched its National Policy for the Use of Artificial Intelligence in 2025 and adopted the GCC's AI Ethics Manual to promote secure and responsible AI deployment across the public sector. Kuwait is advancing the National AI Strategy (2025-2028) as part of its New Kuwait 2035 vision, while Oman continues implementing Vision 2040 and its National Programme for AI and Advanced Technologies to strengthen digital innovation and cybersecurity capabilities. Together, these initiatives are creating favorable conditions for enterprises to modernize conventional SOC environments with AI-assisted security analytics, automated investigation, and intelligent threat response, positioning the Rest of GCC Countries as an emerging growth market for AI SOC solutions during the forecast period.

TABLE 336 REST OF GCC: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	46.5	57.9	72.0	89.7	24.4%
Services	26.7	33.7	42.6	53.9	26.4%
Total	**73.3**	**91.6**	**114.6**	**143.6**	**25.1%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 337 REST OF GCC: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	111.3	138.4	172.4	215.0	268.2	334.5	24.6%
Services	68.0	85.9	108.7	137.7	174.6	221.4	26.6%
Total	**179.3**	**224.3**	**281.1**	**352.7**	**442.8**	**555.9**	**25.4%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 338 REST OF GCC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	17.4	20.6	24.5	29.3	19.1%
AI-orchestrated Response and Automation Platforms	7.2	8.7	10.5	12.8	21.3%
AI-native SOC Platforms	10.0	12.5	15.8	19.9	26.0%
AI SOC Agent Solutions	3.1	4.9	7.5	11.4	54.3%
Security Data Platforms	2.3	2.8	3.5	4.3	23.2%
Threat Intelligence Platforms	3.0	3.7	4.6	5.7	23.2%
AI Governance, Risk, and Compliance Solutions	3.6	4.5	5.6	6.3	20.1%
Total	**46.5**	**57.9**	**72.0**	**89.7**	**24.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 339 REST OF GCC: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	34.3	40.2	47.2	55.4	65.2	76.7	17.5%
AI-orchestrated Response and Automation Platforms	15.4	18.6	22.5	27.2	33.0	39.9	20.9%
AI-native SOC Platforms	25.0	31.5	39.7	50.1	63.3	79.9	26.1%
AI SOC Agent Solutions	15.7	21.7	30.0	41.6	57.6	79.9	38.4%
Security Data Platforms	5.2	6.5	8.0	9.8	12.1	15.0	23.3%
Threat Intelligence Platforms	7.0	8.6	10.6	13.1	16.2	20.0	23.3%
AI Governance, Risk, and Compliance Solutions	8.6	11.3	14.4	17.6	20.7	23.2	21.9%
Total	**111.3**	**138.4**	**172.4**	**215.0**	**268.2**	**334.5**	**24.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 340 REST OF GCC: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	14.4	17.9	22.2	27.6	24.2%
AI SOC-as-a-Service (SOCaaS)	0.8	1.3	2.0	3.1	55.5%
Incident Response and Forensics Services	1.8	2.4	3.1	4.1	31.3%
Threat Intelligence and Advisory Services	9.7	12.2	15.3	19.1	25.5%
Total	**26.7**	**33.7**	**42.6**	**53.9**	**26.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 341 REST OF GCC: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	34.1	42.3	52.5	65.3	81.2	101.0	24.2%
AI SOC-as-a-Service (SOCaaS)	4.4	6.1	8.6	12.1	17.0	24.0	40.4%
Incident Response and Forensics Services	5.3	6.9	9.0	11.8	15.4	20.2	30.7%
Threat Intelligence and Advisory Services	24.2	30.6	38.5	48.5	61.0	76.2	25.8%
Total	**68.0**	**85.9**	**108.7**	**137.7**	**174.6**	**221.4**	**26.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 342 REST OF GCC: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	52.9	65.2	80.4	99.3	23.4%
SMEs	20.4	26.4	34.2	44.3	29.5%
Total	**73.3**	**91.6**	**114.6**	**143.6**	**25.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 343 REST OF GCC: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	122.3	150.8	186.3	230.4	285.2	353.1	23.6%
SMEs	57.1	73.5	94.8	122.3	157.6	202.8	28.9%
Total	**179.3**	**224.3**	**281.1**	**352.7**	**442.8**	**555.9**	**25.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 344 REST OF GCC: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	19.0	23.2	28.2	34.5	22.0%
Alert Triage and Prioritization	9.0	11.7	15.2	19.9	30.4%
Incident Investigation and Analysis	8.8	11.3	14.6	18.9	29.2%
Threat Hunting	5.7	7.2	9.1	11.5	26.5%
Incident Response and Remediation	9.1	11.3	13.9	17.2	23.6%
Insider Threat Detection	3.3	4.3	5.5	7.2	30.0%
Cloud Security Monitoring	6.2	7.6	9.4	11.5	22.7%
Identity and Access Monitoring	3.4	4.3	5.6	7.2	28.9%
Compliance Monitoring and Reporting	1.8	2.4	3.2	4.3	32.8%
Security Analytics and Visualization	7.0	8.3	9.8	11.4	17.5%
Total	**73.3**	**91.6**	**114.6**	**143.6**	**25.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 345 REST OF GCC: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	41.9	50.9	61.9	75.4	91.9	112.0	21.7%
Alert Triage and Prioritization	25.7	33.3	43.1	56.0	72.7	94.4	29.7%
Incident Investigation and Analysis	24.2	31.2	40.1	51.7	66.7	86.1	28.8%
Threat Hunting	14.5	18.3	23.2	29.4	37.3	47.3	26.7%
Incident Response and Remediation	21.2	26.2	32.4	40.1	49.6	61.4	23.7%
Insider Threat Detection	9.3	12.0	15.5	20.0	26.0	33.6	29.4%
Cloud Security Monitoring	14.0	17.2	21.1	25.8	31.7	39.0	22.7%
Identity and Access Monitoring	9.2	11.8	15.2	19.6	25.2	32.5	28.7%
Compliance Monitoring and Reporting	5.6	7.4	9.7	12.7	16.7	21.9	31.2%
Security Analytics and Visualization	13.6	16.2	19.0	22.0	24.9	27.6	15.1%
Total	**179.3**	**224.3**	**281.1**	**352.7**	**442.8**	**555.9**	**25.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 346 REST OF GCC: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	13.8	16.9	20.8	25.6	23.0%
Government & Defense	11.9	14.5	17.7	21.7	22.1%
Healthcare & Life sciences	9.0	11.7	15.2	19.7	29.8%
IT & Telecommunications	8.3	10.2	12.5	15.5	23.2%
Manufacturing	7.4	8.9	10.7	13.0	20.6%
Retail & eCommerce	5.3	6.7	8.5	10.9	27.1%
Energy & Utilities	4.9	6.2	7.9	10.2	27.7%
Media & Entertainment	3.7	4.7	5.9	7.5	26.3%
Education	2.9	3.7	4.8	6.2	28.4%
Other Verticals	6.1	8.0	10.5	13.5	30.2%
Total	**73.3**	**91.6**	**114.6**	**143.6**	**25.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 347 REST OF GCC: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	31.4	38.5	47.3	58.2	71.6	88.2	23.0%
Government & Defense	26.3	32.0	39.0	47.6	58.1	70.9	21.9%
Healthcare & Life sciences	25.5	33.1	43.1	56.1	73.1	95.2	30.1%
IT & Telecommunications	19.0	23.3	28.7	35.4	43.7	54.0	23.3%
Manufacturing	15.5	18.5	22.1	26.5	31.7	37.9	19.6%
Retail & eCommerce	13.8	17.5	22.2	28.3	36.0	45.8	27.2%
Energy & Utilities	12.9	16.5	21.1	27.1	34.7	44.4	28.0%
Media & Entertainment	9.4	11.9	15.1	19.1	24.1	30.5	26.5%
Education	7.9	10.1	12.9	16.6	21.3	27.4	28.3%
Other Verticals	17.6	22.9	29.5	38.0	48.5	61.6	28.4%
Total	**179.3**	**224.3**	**281.1**	**352.7**	**442.8**	**555.9**	**25.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.5.3 REST OF MIDDLE EAST

The Rest of Middle East, comprising countries such as Israel, Egypt, Jordan, Türkiye, and other regional economies, is steadily strengthening its AI SOC landscape through investments in cybersecurity modernization, national AI strategies, and resilient digital infrastructure. Unlike the GCC, where sovereign AI investments and national visions are the primary growth catalysts, these countries are leveraging AI to enhance cyber defense capabilities across government, financial services, telecommunications, defense, healthcare, and critical infrastructure. Rapid digitalization, expanding cloud adoption, and increasing cyber threats targeting public and private organizations are encouraging enterprises to modernize conventional Security Operations Centers (SOCs) with AI-assisted threat detection, behavioral analytics, and automated incident response. These developments are creating sustained demand for intelligent security operations that improve cyber resilience while reducing operational complexity.

Governments across the region are reinforcing cybersecurity through country-specific initiatives. Jordan is implementing its National Cybersecurity Strategy 2025–2028, supported by a national cybersecurity framework that is being deployed across government institutions and critical infrastructure entities, alongside expanded cyber workforce development and AI readiness programs. Egypt is advancing the second phase of its National AI Strategy, strengthening cooperation with global technology companies to expand AI capabilities, cybersecurity skills, and digital infrastructure while positioning itself as a regional AI innovation hub. Meanwhile, Israel continues to strengthen its globally recognized cybersecurity ecosystem through significant investments in AI-focused cyber startups and venture capital, reinforcing its leadership in AI-powered cyber defense technologies. These complementary initiatives are accelerating enterprise adoption of AI-driven security operations while fostering innovation across the broader Middle East cybersecurity ecosystem.

TABLE 348 REST OF MIDDLE EAST: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	38.3	48.2	60.6	76.5	25.9%
Services	22.0	28.1	35.9	46.0	27.8%
Total	**60.3**	**76.3**	**96.5**	**122.4**	**26.6%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 349 REST OF MIDDLE EAST: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	96.2	121.3	153.4	194.3	246.5	312.9	26.6%
Services	58.8	75.3	96.7	124.5	160.5	207.0	28.6%
Total	**154.9**	**196.6**	**250.1**	**318.8**	**407.0**	**519.9**	**27.4%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 350 REST OF MIDDLE EAST: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	14.3	17.2	20.6	25.0	20.4%
AI-orchestrated Response and Automation Platforms	5.9	7.2	8.9	10.9	22.7%
AI-native SOC Platforms	8.2	10.4	13.3	17.0	27.5%
AI SOC Agent Solutions	2.6	4.1	6.3	9.7	56.1%
Security Data Platforms	1.9	2.3	2.9	3.6	24.7%
Threat Intelligence Platforms	2.5	3.1	3.9	4.9	24.7%
AI Governance, Risk, and Compliance Solutions	3.0	3.8	4.7	5.4	21.5%
Total	**38.3**	**48.2**	**60.6**	**76.5**	**25.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 351 REST OF MIDDLE EAST: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	29.6	35.2	42.0	50.1	59.9	71.7	19.4%
AI-orchestrated Response and Automation Platforms	13.3	16.3	20.0	24.6	30.3	37.4	22.9%
AI-native SOC Platforms	21.6	27.6	35.3	45.3	58.2	74.7	28.1%
AI SOC Agent Solutions	13.6	19.0	26.7	37.6	53.0	74.7	40.7%
Security Data Platforms	4.5	5.7	7.1	8.9	11.2	14.0	25.3%
Threat Intelligence Platforms	6.0	7.5	9.4	11.8	14.9	18.7	25.3%
AI Governance, Risk, and Compliance Solutions	7.5	9.9	12.8	15.9	19.1	21.7	23.8%
Total	**96.2**	**121.3**	**153.4**	**194.3**	**246.5**	**312.9**	**26.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 352 REST OF MIDDLE EAST: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	11.9	14.9	18.7	23.5	25.6%
AI SOC-as-a-Service (SOCaaS)	0.7	1.1	1.7	2.7	57.3%
Incident Response and Forensics Services	1.5	2.0	2.6	3.5	32.8%
Threat Intelligence and Advisory Services	8.0	10.1	12.9	16.3	26.9%
Total	**22.0**	**28.1**	**35.9**	**46.0**	**27.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 353 REST OF MIDDLE EAST: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	29.5	37.1	46.7	59.0	74.6	94.5	26.2%
AI SOC-as-a-Service (SOCaaS)	3.8	5.4	7.7	11.0	15.7	22.4	42.7%
Incident Response and Forensics Services	4.6	6.0	8.0	10.6	14.2	18.9	32.8%
Threat Intelligence and Advisory Services	20.9	26.8	34.3	43.9	56.0	71.3	27.8%
Total	**58.8**	**75.3**	**96.7**	**124.5**	**160.5**	**207.0**	**28.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 354 REST OF MIDDLE EAST: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	43.5	54.2	67.7	84.7	24.8%
SMEs	16.8	22.0	28.8	37.8	31.0%
Total	**60.3**	**76.3**	**96.5**	**122.4**	**26.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 355 REST OF MIDDLE EAST: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	105.6	132.2	165.7	208.3	262.2	330.2	25.6%
SMEs	49.3	64.5	84.4	110.5	144.8	189.7	30.9%
Total	**154.9**	**196.6**	**250.1**	**318.8**	**407.0**	**519.9**	**27.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 356 REST OF MIDDLE EAST: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	15.7	19.3	23.8	29.5	23.4%
Alert Triage and Prioritization	7.4	9.7	12.8	17.0	31.9%
Incident Investigation and Analysis	7.2	9.4	12.3	16.1	30.7%
Threat Hunting	4.7	6.0	7.6	9.8	28.0%
Incident Response and Remediation	7.5	9.4	11.7	14.7	25.0%
Insider Threat Detection	2.7	3.5	4.6	6.1	31.5%
Cloud Security Monitoring	5.1	6.3	7.9	9.8	24.1%
Identity and Access Monitoring	2.8	3.6	4.7	6.1	30.4%
Compliance Monitoring and Reporting	1.5	2.0	2.7	3.7	34.3%
Security Analytics and Visualization	5.8	6.9	8.3	9.7	18.8%
Total	**60.3**	**76.3**	**96.5**	**122.4**	**26.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 357 REST OF MIDDLE EAST: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	36.2	44.6	55.1	68.1	84.5	104.8	23.7%
Alert Triage and Prioritization	22.2	29.1	38.4	50.6	66.8	88.3	31.8%
Incident Investigation and Analysis	20.9	27.3	35.7	46.7	61.3	80.5	30.9%
Threat Hunting	12.5	16.1	20.6	26.6	34.3	44.3	28.7%
Incident Response and Remediation	18.3	23.0	28.8	36.2	45.6	57.5	25.6%
Insider Threat Detection	8.0	10.5	13.8	18.1	23.9	31.4	31.5%
Cloud Security Monitoring	12.1	15.1	18.7	23.4	29.2	36.5	24.6%
Identity and Access Monitoring	8.0	10.4	13.5	17.7	23.2	30.4	30.7%
Compliance Monitoring and Reporting	4.9	6.5	8.6	11.5	15.4	20.5	33.3%
Security Analytics and Visualization	11.8	14.2	16.9	19.9	22.9	25.8	17.0%
Total	**154.9**	**196.6**	**250.1**	**318.8**	**407.0**	**519.9**	**27.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 358 REST OF MIDDLE EAST: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	11.3	14.1	17.5	21.8	24.4%
Government & Defense	9.8	12.1	14.9	18.5	23.5%
Healthcare & Life sciences	7.4	9.7	12.8	16.8	31.3%
IT & Telecommunications	6.8	8.5	10.5	13.2	24.6%
Manufacturing	6.1	7.4	9.0	11.1	22.0%
Retail & eCommerce	4.4	5.6	7.2	9.3	28.6%
Energy & Utilities	4.0	5.2	6.7	8.7	29.2%
Media & Entertainment	3.1	3.9	5.0	6.4	27.7%
Education	2.4	3.1	4.0	5.3	29.9%
Other Verticals	5.0	6.7	8.8	11.5	31.7%
Total	**60.3**	**76.3**	**96.5**	**122.4**	**26.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 359 REST OF MIDDLE EAST: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	27.1	33.7	42.1	52.6	65.8	82.4	24.9%
Government & Defense	22.8	28.1	34.7	43.0	53.4	66.3	23.9%
Healthcare & Life sciences	22.1	29.0	38.3	50.7	67.1	89.0	32.2%
IT & Telecommunications	16.4	20.4	25.6	32.0	40.2	50.5	25.2%
Manufacturing	13.4	16.2	19.7	23.9	29.1	35.5	21.5%
Retail & eCommerce	11.9	15.3	19.8	25.5	33.1	42.9	29.2%
Energy & Utilities	11.2	14.5	18.8	24.5	31.9	41.5	30.0%
Media & Entertainment	8.2	10.4	13.4	17.2	22.2	28.6	28.5%
Education	6.8	8.8	11.5	15.0	19.6	25.6	30.3%
Other Verticals	15.2	20.1	26.3	34.3	44.6	57.6	30.5%
Total	**154.9**	**196.6**	**250.1**	**318.8**	**407.0**	**519.9**	**27.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.5.4 AFRICA

13.5.4.1 Expanding AI-enabled security operations strengthening cyber resilience across digital economies

Africa is steadily emerging as a promising market for AI SOCs, supported by expanding digital economies, national AI strategies, and growing investments in cybersecurity capacity building. Africa's growth is centered on strengthening digital resilience, improving cyber readiness, and building foundational AI capabilities across public and private sectors. Rapid digitalization of financial services, mobile payments, e-government platforms, telecommunications, and critical infrastructure is increasing exposure to sophisticated cyber threats, prompting organizations to modernize security operations through AI-assisted threat detection, automated security monitoring, and intelligent incident response. As cloud adoption and enterprise digitization continue to accelerate across the continent, demand is rising for scalable AI SOC platforms that can enhance cyber resilience while addressing resource and operational constraints.

Continental collaboration is playing a pivotal role in shaping Africa's AI cybersecurity landscape. In 2024, the African Union (AU) adopted the Continental Artificial Intelligence Strategy, providing a unified framework for responsible AI development, digital sovereignty, cybersecurity, and regional cooperation under Agenda 2063. Building on this momentum, the AU convened a High-Level Policy Dialogue on AI in 2025, reaffirming its commitment to developing continent-wide AI governance frameworks, strengthening secure AI deployment, and promoting cross-border collaboration among governments, industry, academia, and international partners. At the national level, countries including Egypt, Kenya, Nigeria, Rwanda, Ghana, Ethiopia, and South Africa are advancing AI policies, digital transformation initiatives, and cybersecurity programs to strengthen trusted digital ecosystems and support secure enterprise AI adoption.

Looking ahead, Africa is expected to witness increasing adoption of AI-enabled security operations as governments and enterprises invest in digital infrastructure, AI talent development, cloud computing, and cybersecurity modernization. International technology providers, regional innovation hubs, and public-private partnerships are supporting the expansion of AI skills, cyber workforce development, and secure digital ecosystems across the continent. As organizations increasingly prioritize cyber resilience to protect expanding digital services and critical infrastructure, Africa is expected to present significant long-term opportunities for AI SOC platforms, managed security service providers, and AI-driven cybersecurity solutions throughout the forecast period.

TABLE 360 AFRICA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	22.3	27.6	34.2	42.4	23.9%
Services	12.8	16.1	20.2	25.5	25.8%
Total	**35.1**	**43.7**	**54.4**	**67.9**	**24.6%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 361 AFRICA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	52.5	65.2	81.1	101.2	126.3	157.8	24.6%
Services	32.1	40.5	51.2	64.8	82.3	104.5	26.6%
Total	**84.6**	**105.7**	**132.3**	**166.0**	**208.6**	**262.3**	**25.4%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 362 AFRICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	8.2	9.8	11.6	13.9	19.1%
AI-orchestrated Response and Automation Platforms	3.4	4.1	5.0	6.1	20.9%
AI-native SOC Platforms	4.8	6.0	7.5	9.4	25.5%
AI SOC Agent Solutions	1.3	1.8	2.4	3.4	38.4%
Security Data Platforms	1.1	1.3	1.6	2.0	22.7%
Threat Intelligence Platforms	1.5	1.8	2.2	2.7	22.7%
AI Governance, Risk, and Compliance Solutions	2.1	2.8	3.8	5.0	33.8%
Total	**22.3**	**27.6**	**34.2**	**42.4**	**23.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 363 AFRICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	16.4	19.5	23.2	27.5	32.6	38.5	18.6%
AI-orchestrated Response and Automation Platforms	7.3	8.8	10.7	13.0	15.8	19.1	21.2%
AI-native SOC Platforms	11.8	14.9	18.7	23.6	29.9	37.8	26.2%
AI SOC Agent Solutions	4.7	6.5	9.0	12.6	17.5	24.5	39.2%
Security Data Platforms	2.5	3.0	3.8	4.6	5.7	7.1	23.4%
Threat Intelligence Platforms	3.3	4.1	5.0	6.2	7.6	9.4	23.4%
AI Governance, Risk, and Compliance Solutions	6.5	8.4	10.8	13.7	17.2	21.4	27.0%
Total	**52.5**	**65.2**	**81.1**	**101.2**	**126.3**	**157.8**	**24.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 364 AFRICA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	6.9	8.5	10.5	13.1	23.7%
AI SOC-as-a-Service (SOCaaS)	0.4	0.6	1.0	1.5	54.9%
Incident Response and Forensics Services	0.9	1.1	1.5	1.9	30.7%
Threat Intelligence and Advisory Services	4.6	5.8	7.3	9.0	24.9%
Total	**12.8**	**16.1**	**20.2**	**25.5**	**25.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 365 AFRICA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	16.1	19.9	24.7	30.7	38.3	47.7	24.2%
AI SOC-as-a-Service (SOCaaS)	2.1	2.9	4.1	5.7	8.0	11.3	40.4%
Incident Response and Forensics Services	2.5	3.2	4.2	5.5	7.3	9.5	30.7%
Threat Intelligence and Advisory Services	11.4	14.4	18.1	22.8	28.7	36.0	25.8%
Total	**32.1**	**40.5**	**51.2**	**64.8**	**82.3**	**104.5**	**26.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 366 AFRICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	25.3	31.1	38.1	47.0	22.9%
SMEs	9.8	12.6	16.2	21.0	28.9%
Total	**35.1**	**43.7**	**54.4**	**67.9**	**24.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 367 AFRICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	57.7	71.0	87.7	108.5	134.4	166.6	23.6%
SMEs	26.9	34.6	44.6	57.5	74.2	95.7	28.9%
Total	**84.6**	**105.7**	**132.3**	**166.0**	**208.6**	**262.3**	**25.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 368 AFRICA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	9.1	11.1	13.4	16.3	21.5%
Alert Triage and Prioritization	4.3	5.6	7.2	9.4	29.9%
Incident Investigation and Analysis	4.2	5.4	6.9	8.9	28.6%
Threat Hunting	2.7	3.4	4.3	5.4	26.0%
Incident Response and Remediation	4.4	5.4	6.6	8.2	23.0%
Insider Threat Detection	1.6	2.0	2.6	3.4	29.4%
Cloud Security Monitoring	3.0	3.6	4.4	5.4	22.2%
Identity and Access Monitoring	1.6	2.1	2.6	3.4	28.4%
Compliance Monitoring and Reporting	0.9	1.2	1.5	2.0	32.2%
Security Analytics and Visualization	3.4	4.0	4.7	5.4	17.0%
Total	**35.1**	**43.7**	**54.4**	**67.9**	**24.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 369 AFRICA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	19.8	24.0	29.1	35.5	43.3	52.9	21.7%
Alert Triage and Prioritization	12.1	15.7	20.3	26.3	34.2	44.6	29.7%
Incident Investigation and Analysis	11.4	14.7	18.9	24.3	31.4	40.6	28.8%
Threat Hunting	6.8	8.6	10.9	13.8	17.6	22.3	26.7%
Incident Response and Remediation	10.0	12.3	15.2	18.9	23.4	29.0	23.7%
Insider Threat Detection	4.4	5.6	7.3	9.4	12.2	15.9	29.4%
Cloud Security Monitoring	6.6	8.1	9.9	12.2	15.0	18.4	22.7%
Identity and Access Monitoring	4.3	5.6	7.2	9.2	11.9	15.3	28.7%
Compliance Monitoring and Reporting	2.7	3.5	4.6	6.0	7.9	10.4	31.2%
Security Analytics and Visualization	6.4	7.6	8.9	10.3	11.8	13.0	15.1%
Total	**84.6**	**105.7**	**132.3**	**166.0**	**208.6**	**262.3**	**25.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 370 AFRICA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	6.6	8.1	9.9	12.1	22.4%
Government & Defense	5.7	6.9	8.4	10.3	21.6%
Healthcare & Life sciences	4.3	5.6	7.2	9.3	29.3%
IT & Telecommunications	4.0	4.8	5.9	7.3	22.7%
Manufacturing	3.6	4.3	5.1	6.1	20.0%
Retail & eCommerce	2.5	3.2	4.1	5.1	26.6%
Energy & Utilities	2.3	3.0	3.8	4.8	27.2%
Media & Entertainment	1.8	2.2	2.8	3.5	25.7%
Education	1.4	1.8	2.3	2.9	27.9%
Other Verticals	2.9	3.8	5.0	6.4	29.6%
Total	**35.1**	**43.7**	**54.4**	**67.9**	**24.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 371 AFRICA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	14.8	18.1	22.3	27.4	33.7	41.6	23.0%
Government & Defense	12.4	15.1	18.4	22.4	27.4	33.5	21.9%
Healthcare & Life sciences	12.0	15.6	20.3	26.4	34.4	44.9	30.1%
IT & Telecommunications	9.0	11.0	13.5	16.7	20.6	25.5	23.3%
Manufacturing	7.3	8.7	10.4	12.5	14.9	17.9	19.6%
Retail & eCommerce	6.5	8.2	10.5	13.3	17.0	21.6	27.2%
Energy & Utilities	6.1	7.8	9.9	12.7	16.3	21.0	28.0%
Media & Entertainment	4.5	5.6	7.1	9.0	11.4	14.4	26.5%
Education	3.7	4.7	6.1	7.8	10.0	12.9	28.3%
Other Verticals	8.3	10.8	13.9	17.9	22.8	29.1	28.4%
Total	**84.6**	**105.7**	**132.3**	**166.0**	**208.6**	**262.3**	**25.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.6 LATIN AMERICA

Latin America is steadily emerging as a high-potential market for AI SOCs, driven by accelerating digital transformation, expanding cloud adoption, and increasing government focus on artificial intelligence and cybersecurity resilience. Latin America is characterized by the rapid maturation of its digital economy and growing investments in national AI capabilities. The increasing digitalization of banking, e-commerce, manufacturing, telecommunications, healthcare, and public services has significantly expanded the regional cyberattack surface, prompting enterprises to modernize conventional Security Operations Centers through AI-assisted threat detection, intelligent security analytics, and automated incident response. Organizations are increasingly adopting AI-enabled security operations to improve operational efficiency while addressing evolving ransomware, phishing, and identity-based cyber threats.

Regional cooperation is also strengthening the foundation for secure AI adoption across Latin America. In 2025, the Economic Commission for Latin America and the Caribbean (ECLAC) and Chile's National Center for Artificial Intelligence (CENIA) released the Latin American Artificial Intelligence Index (ILIA 2025), providing a comprehensive framework to assess AI readiness, governance, research, adoption, and enabling infrastructure across 19 countries. The Index is helping governments identify investment priorities and accelerate national AI strategies while fostering greater regional collaboration. In parallel, the Organization of American States (OAS), through its Inter-American Committee against Terrorism (CICTE), continues to work with governments and international organizations to strengthen AI-enabled cybersecurity policies, cyber capacity building, and resilience against emerging AI-driven cyber threats across the region.

Looking ahead, Latin America is expected to witness increasing adoption of AI-native security operations as enterprises modernize cybersecurity architectures to support cloud-native applications, digital financial services, and connected critical infrastructure. The region is also experiencing growing investments in AI research, digital innovation, and high-performance computing, supported by collaboration among governments, academia, technology providers, and multilateral organizations. As organizations increasingly prioritize proactive cyber defense, intelligent threat hunting, and automated security operations, Latin America is expected to present significant opportunities for AI SOC platform providers, managed security service providers, and AI-driven cybersecurity innovators throughout the forecast period.

13.6.1 LATIN AMERICA: AI SOC MARKET DRIVERS

- Governments across Latin America are prioritizing AI development, digital transformation, and cybersecurity resilience through national strategies and policy frameworks. These initiatives are encouraging organizations to modernize traditional SOC environments with AI-powered threat detection, automated investigation, and intelligent incident response capabilities.
- Increasing ransomware, phishing, identity-based attacks, and advanced cyber threats across Latin America are compelling enterprises to adopt AI-enabled SOC platforms. Organizations are leveraging AI-driven analytics, automated threat hunting, and real-time response capabilities to improve cyber resilience and manage evolving attack complexities.
- Rapid adoption of cloud services, hybrid infrastructure, and digital platforms across industries is expanding enterprise attack surfaces in Latin America. Organizations are increasingly deploying AI SOC solutions to analyze large security data volumes, detect anomalies, and secure complex multi-cloud environments.
- Rising enterprise adoption of artificial intelligence across banking, manufacturing, telecommunications, healthcare, and government sectors is increasing the need for AI-driven cybersecurity operations. Organizations are implementing AI SOC platforms to automate security workflows, enhance threat intelligence, and improve incident response efficiency.

JULY 2026 © MarketsandMarkets™

- Limited availability of skilled cybersecurity professionals across Latin America is encouraging enterprises to adopt AI-powered SOC platforms. Automated alert prioritization, investigation assistance, and response orchestration enable organizations to overcome analyst shortages while improving operational efficiency and maintaining continuous security monitoring.
- Growing digitalization of critical infrastructure sectors, including energy, utilities, mining, transportation, and telecommunications, is increasing cybersecurity requirements across Latin America. AI SOC solutions enable continuous monitoring, behavioral analysis, and automated response capabilities to protect interconnected operational and digital environments.

TABLE 372 LATIN AMERICA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	206.3	263.1	330.8	409.3	25.7%
Services	118.4	153.4	195.9	246.2	27.6%
Total	**324.8**	**416.4**	**526.7**	**655.5**	**26.4%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 373 LATIN AMERICA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	505.4	617.3	746.2	892.3	1,054.5	1,229.1	19.5%
Services	308.8	383.1	470.5	571.7	686.6	813.4	21.4%
Total	**814.2**	**1,000.5**	**1,216.8**	**1,464.0**	**1,741.1**	**2,042.5**	**20.2%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 374 LATIN AMERICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	76.2	93.3	112.6	133.7	20.6%
AI-orchestrated Response and Automation Platforms	31.7	39.5	48.5	58.5	22.6%
AI-native SOC Platforms	44.1	57.0	72.6	91.0	27.3%
AI SOC Agent Solutions	12.3	18.3	26.5	38.0	45.5%
Security Data Platforms	10.1	12.8	15.9	19.5	24.4%
Threat Intelligence Platforms	13.5	17.0	21.2	26.0	24.4%
AI Governance, Risk, and Compliance Solutions	18.4	25.2	33.6	42.8	32.5%
Total	**206.3**	**263.1**	**330.8**	**409.3**	**25.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 375 LATIN AMERICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	157.4	183.1	210.4	238.8	267.3	294.5	13.3%
AI-orchestrated Response and Automation Platforms	70.3	83.5	98.2	114.2	131.0	148.3	16.1%
AI-native SOC Platforms	113.7	140.7	172.1	208.3	249.2	293.9	20.9%
AI SOC Agent Solutions	52.4	71.5	96.5	128.9	170.2	221.6	33.4%
Security Data Platforms	23.8	28.8	34.5	40.8	47.8	55.1	18.3%
Threat Intelligence Platforms	31.8	38.4	46.0	54.4	63.7	73.5	18.3%
AI Governance, Risk, and Compliance Solutions	56.0	71.3	88.5	106.9	125.4	142.2	20.5%
Total	**505.4**	**617.3**	**746.2**	**892.3**	**1,054.5**	**1,229.1**	**19.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 376 LATIN AMERICA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	63.9	81.3	102.0	126.0	25.4%
AI SOC-as-a-Service (SOCaaS)	3.7	6.1	9.4	14.3	57.1%
Incident Response and Forensics Services	7.9	10.7	14.2	18.5	32.6%
Threat Intelligence and Advisory Services	42.9	55.3	70.3	87.3	26.7%
Total	**118.4**	**153.4**	**195.9**	**246.2**	**27.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 377 LATIN AMERICA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	155.0	188.8	227.4	271.1	319.3	371.1	19.1%
AI SOC-as-a-Service (SOCaaS)	19.9	27.4	37.3	50.3	67.0	88.0	34.6%
Incident Response and Forensics Services	24.0	30.7	38.9	48.9	60.6	74.1	25.3%
Threat Intelligence and Advisory Services	109.8	136.3	166.9	201.5	239.7	280.1	20.6%
Total	**308.8**	**383.1**	**470.5**	**571.7**	**686.6**	**813.4**	**21.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 378 LATIN AMERICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	234.3	296.2	369.4	453.3	24.6%
SMEs	90.4	120.2	157.3	202.2	30.8%
Total	**324.8**	**416.4**	**526.7**	**655.5**	**26.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 379 LATIN AMERICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	555.1	672.5	806.4	956.6	1,121.6	1,297.2	18.5%
SMEs	259.1	328.0	410.4	507.5	619.5	745.3	23.5%
Total	**814.2**	**1,000.5**	**1,216.8**	**1,464.0**	**1,741.1**	**2,042.5**	**20.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 380 LATIN AMERICA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	84.3	105.4	129.9	157.7	23.2%
Alert Triage and Prioritization	39.7	53.1	69.9	90.7	31.7%
Incident Investigation and Analysis	38.8	51.4	67.1	86.2	30.4%
Threat Hunting	25.2	32.6	41.7	52.5	27.8%
Incident Response and Remediation	40.5	51.3	64.0	78.7	24.8%
Insider Threat Detection	14.5	19.3	25.4	32.8	31.2%
Cloud Security Monitoring	27.6	34.7	43.0	52.5	23.9%
Identity and Access Monitoring	14.9	19.6	25.6	32.8	30.2%
Compliance Monitoring and Reporting	8.2	11.1	14.9	19.7	34.1%
Security Analytics and Visualization	31.1	37.8	45.2	51.9	18.6%
Total	**324.8**	**416.4**	**526.7**	**655.5**	**26.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 381 LATIN AMERICA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	190.1	226.9	267.9	313.0	361.4	411.6	16.7%
Alert Triage and Prioritization	116.6	148.3	186.6	232.3	285.9	347.0	24.4%
Incident Investigation and Analysis	110.0	138.9	173.6	214.7	262.3	316.2	23.5%
Threat Hunting	65.9	81.8	100.5	122.1	146.7	173.9	21.4%
Incident Response and Remediation	96.4	116.8	140.2	166.3	195.1	225.7	18.5%
Insider Threat Detection	42.1	53.3	66.9	83.1	102.0	123.5	24.0%
Cloud Security Monitoring	63.8	76.6	91.2	107.3	124.8	143.2	17.6%
Identity and Access Monitoring	41.8	52.7	65.8	81.2	99.1	119.3	23.3%
Compliance Monitoring and Reporting	25.6	32.9	41.9	52.8	65.7	80.6	25.8%
Security Analytics and Visualization	61.9	72.2	82.2	91.2	98.1	101.4	10.4%
Total	**814.2**	**1,000.5**	**1,216.8**	**1,464.0**	**1,741.1**	**2,042.5**	**20.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 382 LATIN AMERICA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	61.1	76.9	95.6	116.9	24.2%
Government & Defense	52.8	66.1	81.5	99.0	23.3%
Healthcare & Life sciences	39.9	53.1	69.7	90.0	31.1%
IT & Telecommunications	36.6	46.2	57.6	70.5	24.4%
Manufacturing	32.8	40.6	49.4	59.3	21.7%
Retail & eCommerce	23.5	30.5	39.2	49.6	28.3%
Energy & Utilities	21.6	28.3	36.5	46.4	29.0%
Media & Entertainment	16.5	21.3	27.2	34.2	27.5%
Education	12.9	17.0	22.0	28.1	29.7%
Other Verticals	27.1	36.4	48.1	61.6	31.5%
Total	**324.8**	**416.4**	**526.7**	**655.5**	**26.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 383 LATIN AMERICA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	142.4	171.6	204.6	241.4	281.6	323.9	17.9%
Government & Defense	119.6	142.9	169.0	197.6	228.5	260.6	16.9%
Healthcare & Life sciences	115.9	147.8	186.5	232.8	287.3	349.6	24.7%
IT & Telecommunications	86.1	104.0	124.4	147.1	172.0	198.4	18.2%
Manufacturing	70.3	82.4	95.7	109.8	124.6	139.3	14.7%
Retail & eCommerce	62.5	77.9	96.1	117.3	141.6	168.5	21.9%
Energy & Utilities	58.8	73.7	91.5	112.3	136.3	163.2	22.7%
Media & Entertainment	42.9	53.1	65.2	79.1	94.9	112.2	21.2%
Education	35.7	44.9	55.9	68.9	83.8	100.5	23.0%
Other Verticals	80.0	102.0	127.9	157.6	190.7	226.3	23.1%
Total	**814.2**	**1,000.5**	**1,216.8**	**1,464.0**	**1,741.1**	**2,042.5**	**20.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 384 LATIN AMERICA: AI SOC MARKET, BY COUNTRY, 2022–2025 (USD MILLION)

Country	2022	2023	2024	2025	CAGR (2022–2025)
Brazil	240.3	306.3	385.0	476.2	25.6%
Mexico	55.0	72.0	93.1	118.5	29.2%
Rest of Latin America	29.5	38.1	48.5	60.7	27.2%
Total	**324.8**	**416.4**	**526.7**	**655.5**	**26.4%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 385 LATIN AMERICA: AI SOC MARKET, BY COUNTRY, 2026–2031 (USD MILLION)

Country	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Brazil	587.7	717.8	867.6	1,037.3	1,225.8	1,428.9	19.4%
Mexico	150.5	188.8	234.3	287.7	348.9	417.3	22.6%
Rest of Latin America	75.9	93.9	114.9	139.1	166.4	196.4	20.9%
Total	**814.2**	**1,000.5**	**1,216.8**	**1,464.0**	**1,741.1**	**2,042.5**	**20.2%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.6.2 BRAZIL

13.6.2.1 National AI investments and regulatory modernization accelerating AI-driven security operations

Brazil is the largest AI SOC market in Latin America, supported by its mature digital economy, expanding cloud infrastructure, and strong government commitment to artificial intelligence and cybersecurity modernization. Unlike Mexico, where AI SOC adoption is closely linked to nearshoring and industrial manufacturing, Brazil is building a broad AI ecosystem through national AI investments, regulatory advancements, and enterprise digital transformation. In 2024, the federal government launched the Brazilian Artificial Intelligence Plan (Plano Brasileiro de IA 2024-2028), allocating approximately BRL 23 billion (USD 4 billion) to strengthen AI infrastructure, develop sovereign AI capabilities, expand high-performance computing, and accelerate AI adoption across strategic sectors. Combined with Brazil's General Data Protection Law (LGPD) and ongoing discussions surrounding the national AI regulatory framework, these initiatives are encouraging enterprises to adopt AI-powered security operations capable of improving threat detection, security analytics, and automated incident response across increasingly digital business environments.

Brazil's enterprise cybersecurity landscape is also creating strong demand for AI-native SOC platforms. Financial institutions, healthcare providers, retailers, telecommunications companies, and public-sector organizations are increasingly deploying AI-enabled security operations to address escalating ransomware, phishing, and identity-based attacks while securing hybrid and multi-cloud environments. The country's rapidly expanding cloud ecosystem, coupled with increasing adoption of managed security services and Security Information and Event Management (SIEM) platforms, is accelerating investments in intelligent SOC modernization. Supported by continued AI investments, digital infrastructure expansion, and a strong domestic technology ecosystem, Brazil is expected to remain Latin America's leading market for AI SOC platforms throughout the forecast period.

TABLE 386 BRAZIL: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	152.7	193.5	241.8	297.4	24.9%
Services	87.6	112.8	143.2	178.8	26.8%
Total	**240.3**	**306.3**	**385.0**	**476.2**	**25.6%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 387 BRAZIL: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	364.8	442.9	532.1	632.2	742.4	859.8	18.7%
Services	222.9	274.9	335.5	405.1	483.4	569.0	20.6%
Total	**587.7**	**717.8**	**867.6**	**1,037.3**	**1,225.8**	**1,428.9**	**19.4%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 388 BRAZIL: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	56.2	68.5	82.3	97.1	20.0%
AI-orchestrated Response and Automation Platforms	23.5	29.0	35.4	42.5	21.9%
AI-native SOC Platforms	32.6	41.9	53.1	66.1	26.5%
AI SOC Agent Solutions	8.7	12.4	17.3	23.7	39.5%
Security Data Platforms	7.5	9.4	11.6	14.2	23.7%
Threat Intelligence Platforms	10.0	12.5	15.5	18.9	23.7%
AI Governance, Risk, and Compliance Solutions	14.2	19.7	26.6	34.9	34.9%
Total	**152.7**	**193.5**	**241.8**	**297.4**	**24.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 389 BRAZIL: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	114.1	132.5	151.8	171.7	191.4	209.8	12.9%
AI-orchestrated Response and Automation Platforms	50.8	60.1	70.2	81.2	92.6	104.2	15.4%
AI-native SOC Platforms	82.1	101.0	122.8	147.7	175.5	205.8	20.2%
AI SOC Agent Solutions	32.5	44.1	59.2	78.6	103.1	133.4	32.6%
Security Data Platforms	17.2	20.7	24.6	28.9	33.6	38.6	17.5%
Threat Intelligence Platforms	22.9	27.6	32.8	38.6	44.9	51.4	17.5%
AI Governance, Risk, and Compliance Solutions	45.1	57.0	70.6	85.5	101.2	116.7	20.9%
Total	**364.8**	**442.9**	**532.1**	**632.2**	**742.4**	**859.8**	**18.7%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 390 BRAZIL: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	47.3	59.8	74.6	91.5	24.7%
AI SOC-as-a-Service (SOCaaS)	2.7	4.5	6.8	10.4	56.1%
Incident Response and Forensics Services	5.9	7.9	10.4	13.4	31.8%
Threat Intelligence and Advisory Services	31.8	40.7	51.4	63.4	25.9%
Total	**87.6**	**112.8**	**143.2**	**178.8**	**26.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 391 BRAZIL: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	111.9	135.4	162.1	192.1	224.8	259.6	18.3%
AI SOC-as-a-Service (SOCaaS)	14.4	19.7	26.6	35.6	47.2	61.6	33.8%
Incident Response and Forensics Services	17.3	22.0	27.8	34.6	42.7	51.8	24.5%
Threat Intelligence and Advisory Services	79.3	97.8	119.0	142.8	168.7	196.0	19.8%
Total	**222.9**	**274.9**	**335.5**	**405.1**	**483.4**	**569.0**	**20.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 392 BRAZIL: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	173.4	217.9	270.0	329.3	23.8%
SMEs	66.9	88.4	115.0	146.9	30.0%
Total	**240.3**	**306.3**	**385.0**	**476.2**	**25.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 393 BRAZIL: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	400.7	482.5	574.9	677.7	789.6	907.5	17.8%
SMEs	187.0	235.3	292.6	359.6	436.2	521.4	22.8%
Total	**587.7**	**717.8**	**867.6**	**1,037.3**	**1,225.8**	**1,428.9**	**19.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 394 BRAZIL: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	62.4	77.5	94.9	114.6	22.5%
Alert Triage and Prioritization	29.4	39.1	51.1	65.9	30.9%
Incident Investigation and Analysis	28.7	37.8	49.0	62.6	29.6%
Threat Hunting	18.6	24.0	30.5	38.1	27.0%
Incident Response and Remediation	30.0	37.7	46.8	57.2	24.0%
Insider Threat Detection	10.7	14.2	18.6	23.8	30.4%
Cloud Security Monitoring	20.4	25.5	31.4	38.1	23.2%
Identity and Access Monitoring	11.0	14.5	18.7	23.8	29.4%
Compliance Monitoring and Reporting	6.0	8.2	10.9	14.3	33.3%
Security Analytics and Visualization	23.0	27.8	33.1	37.7	17.9%
Total	**240.3**	**306.3**	**385.0**	**476.2**	**25.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 395 BRAZIL: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	137.3	162.8	191.0	221.7	254.4	287.9	16.0%
Alert Triage and Prioritization	84.2	106.4	133.1	164.6	201.3	242.7	23.6%
Incident Investigation and Analysis	79.4	99.7	123.8	152.1	184.7	221.2	22.7%
Threat Hunting	47.5	58.7	71.6	86.5	103.3	121.7	20.7%
Incident Response and Remediation	69.6	83.8	99.9	117.8	137.3	157.9	17.8%
Insider Threat Detection	30.4	38.3	47.7	58.9	71.8	86.4	23.3%
Cloud Security Monitoring	46.0	55.0	65.0	76.0	87.9	100.2	16.8%
Identity and Access Monitoring	30.2	37.8	46.9	57.6	69.8	83.5	22.6%
Compliance Monitoring and Reporting	18.5	23.6	29.9	37.4	46.2	56.4	25.0%
Security Analytics and Visualization	44.7	51.8	58.6	64.6	69.0	70.9	9.7%
Total	**587.7**	**717.8**	**867.6**	**1,037.3**	**1,225.8**	**1,428.9**	**19.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 396 BRAZIL: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	45.2	56.6	69.9	84.9	23.4%
Government & Defense	39.1	48.6	59.6	71.9	22.6%
Healthcare & Life sciences	29.5	39.0	50.9	65.4	30.3%
IT & Telecommunications	27.1	34.0	42.1	51.2	23.7%
Manufacturing	24.3	29.8	36.1	43.1	21.0%
Retail & eCommerce	17.4	22.5	28.7	36.0	27.6%
Energy & Utilities	16.0	20.8	26.7	33.7	28.2%
Media & Entertainment	12.2	15.7	19.9	24.9	26.7%
Education	9.5	12.5	16.1	20.4	28.9%
Other Verticals	20.0	26.8	35.1	44.7	30.7%
Total	**240.3**	**306.3**	**385.0**	**476.2**	**25.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 397 BRAZIL: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	102.8	123.1	145.9	171.1	198.2	226.6	17.1%
Government & Defense	86.3	102.5	120.5	140.0	160.9	182.3	16.1%
Healthcare & Life sciences	83.7	106.0	133.0	165.0	202.2	244.6	23.9%
IT & Telecommunications	62.2	74.7	88.7	104.3	121.1	138.8	17.4%
Manufacturing	50.7	59.2	68.2	77.8	87.7	97.5	13.9%
Retail & eCommerce	45.1	55.9	68.5	83.1	99.7	117.8	21.2%
Energy & Utilities	42.4	52.9	65.2	79.6	96.0	114.2	21.9%
Media & Entertainment	30.9	38.1	46.5	56.0	66.8	78.5	20.5%
Education	25.8	32.3	39.9	48.8	59.0	70.3	22.2%
Other Verticals	57.8	73.2	91.2	111.6	134.2	158.3	22.3%
Total	**587.7**	**717.8**	**867.6**	**1,037.3**	**1,225.8**	**1,428.9**	**19.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.6.3 MEXICO

13.6.3.1 Nearshoring-driven industrial digitalization and national cybersecurity modernization accelerating AI-enabled security operations

Mexico is emerging as one of Latin America's fastest-growing markets for AI SOCs, supported by rapid industrial digitalization, expanding cloud adoption, and increasing cybersecurity investments across manufacturing, automotive, financial services, logistics, and telecommunications. Unlike Brazil, where AI innovation is largely driven by a broad national AI ecosystem, Mexico's AI SOC market is closely tied to its nearshoring boom and deep integration with North American supply chains. As multinational manufacturers continue relocating operations to Mexico, organizations are modernizing cybersecurity capabilities to protect increasingly connected factories, industrial control systems, and digital supply chains from sophisticated cyber threats. In 2025, the Mexican government launched the National Cybersecurity Plan, introducing a comprehensive roadmap that includes the establishment of a National Cybersecurity Operations Center, continuous vulnerability management, AI-assisted cyber defense, and coordinated protection of critical infrastructure across the federal government.

Mexico is also strengthening the foundation for AI-enabled cybersecurity through national digital transformation initiatives and growing enterprise security investments. The National AI Agenda (IA2030Mx) identifies cybersecurity, digital infrastructure, and trusted AI as strategic priorities for accelerating responsible AI adoption across government and industry. Meanwhile, the country's expanding digital economy and increasing ransomware and AI-enabled cyberattacks are driving enterprises to adopt AI-native SOC platforms capable of intelligent threat detection, automated investigation, and rapid incident response. According to Fortinet, Mexico accounted for more than half of all cyberattack attempts reported across Latin America during the first half of 2024, highlighting the growing need for advanced AI-driven security operations. Supported by continued government modernization efforts, industrial digitalization, and rising enterprise demand for intelligent cyber defense, Mexico is expected to remain one of the region's most attractive markets for AI SOC solutions throughout the forecast period.

TABLE 398 MEXICO: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	34.9	45.5	58.5	74.0	28.5%
Services	20.0	26.5	34.6	44.5	30.5%
Total	**55.0**	**72.0**	**93.1**	**118.5**	**29.2%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 399 MEXICO: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	93.4	116.5	143.7	175.3	211.3	251.1	21.9%
Services	57.1	72.3	90.6	112.3	137.6	166.2	23.8%
Total	**150.5**	**188.8**	**234.3**	**287.7**	**348.9**	**417.3**	**22.6%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 400 MEXICO: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platform	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	13.0	16.2	19.9	24.2	22.9%
AI-orchestrated Response and Automation Platforms	5.4	6.8	8.6	10.6	25.2%
AI-native SOC Platforms	7.5	9.9	12.8	16.4	30.1%
AI SOC Agent Solutions	2.3	3.9	6.1	9.4	59.3%
Security Data Platforms	1.7	2.2	2.8	3.5	27.2%
Threat Intelligence Platforms	2.3	2.9	3.8	4.7	27.2%
AI Governance, Risk, and Compliance Solutions	2.7	3.5	4.6	5.2	24.0%
Total	**34.9**	**45.5**	**58.5**	**74.0**	**28.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 401 MEXICO: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platform	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	28.8	33.8	39.3	45.2	51.4	57.6	14.9%
AI-orchestrated Response and Automation Platforms	13.0	15.7	18.8	22.2	26.0	30.0	18.3%
AI-native SOC Platforms	21.0	26.5	33.1	40.9	49.9	60.0	23.3%
AI SOC Agent Solutions	13.2	18.3	25.0	33.9	45.4	60.0	35.4%
Security Data Platforms	4.4	5.4	6.6	8.0	9.6	11.2	20.6%
Threat Intelligence Platforms	5.9	7.2	8.8	10.7	12.7	15.0	20.6%
AI Governance, Risk, and Compliance Solutions	7.2	9.5	12.0	14.4	16.3	17.4	19.2%
Total	**93.4**	**116.5**	**143.7**	**175.3**	**211.3**	**251.1**	**21.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 402 MEXICO: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Service	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	10.8	14.1	18.0	22.8	28.2%
AI SOC-as-a-Service (SOCaaS)	0.6	1.0	1.7	2.6	60.6%
Incident Response and Forensics Services	1.3	1.8	2.5	3.3	35.6%
Threat Intelligence and Advisory Services	7.3	9.6	12.4	15.8	29.5%
Total	**20.0**	**26.5**	**34.6**	**44.5**	**30.5%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 403 MEXICO: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	28.7	35.6	43.8	53.3	64.0	75.8	21.5%
AI SOC-as-a-Service (SOCaaS)	3.7	5.2	7.2	9.9	13.4	18.0	37.3%
Incident Response and Forensics Services	4.4	5.8	7.5	9.6	12.1	15.1	27.9%
Threat Intelligence and Advisory Services	20.3	25.7	32.1	39.6	48.0	57.2	23.0%
Total	**57.1**	**72.3**	**90.6**	**112.3**	**137.6**	**166.2**	**23.8%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 404 MEXICO: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	39.7	51.2	65.3	82.0	27.4%
SMEs	15.3	20.8	27.8	36.6	33.7%
Total	**55.0**	**72.0**	**93.1**	**118.5**	**29.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 405 MEXICO: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	102.6	126.9	155.3	188.0	224.8	265.0	20.9%
SMEs	47.9	61.9	79.0	99.7	124.2	152.3	26.0%
Total	**150.5**	**188.8**	**234.3**	**287.7**	**348.9**	**417.3**	**22.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 406 MEXICO: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	14.3	18.2	23.0	28.5	26.0%
Alert Triage and Prioritization	6.7	9.2	12.4	16.4	34.7%
Incident Investigation and Analysis	6.6	8.9	11.9	15.6	33.4%
Threat Hunting	4.3	5.6	7.4	9.5	30.6%
Incident Response and Remediation	6.9	8.9	11.3	14.2	27.5%
Insider Threat Detection	2.5	3.3	4.5	5.9	34.2%
Cloud Security Monitoring	4.7	6.0	7.6	9.5	26.7%
Identity and Access Monitoring	2.5	3.4	4.5	5.9	33.1%
Compliance Monitoring and Reporting	1.4	1.9	2.6	3.6	37.1%
Security Analytics and Visualization	5.3	6.5	8.0	9.4	21.3%
Total	**55.0**	**72.0**	**93.1**	**118.5**	**29.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 407 MEXICO: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	35.1	42.8	51.6	61.5	72.4	84.1	19.1%
Alert Triage and Prioritization	21.6	28.0	35.9	45.6	57.3	70.9	26.9%
Incident Investigation and Analysis	20.3	26.2	33.4	42.2	52.6	64.6	26.0%
Threat Hunting	12.2	15.4	19.3	24.0	29.4	35.5	23.9%
Incident Response and Remediation	17.8	22.0	27.0	32.7	39.1	46.1	20.9%
Insider Threat Detection	7.8	10.1	12.9	16.3	20.4	25.2	26.6%
Cloud Security Monitoring	11.8	14.5	17.6	21.1	25.0	29.3	19.9%
Identity and Access Monitoring	7.7	9.9	12.7	16.0	19.9	24.4	25.8%
Compliance Monitoring and Reporting	4.7	6.2	8.1	10.4	13.2	16.5	28.3%
Security Analytics and Visualization	11.4	13.6	15.8	17.9	19.7	20.7	12.6%
Total	**150.5**	**188.8**	**234.3**	**287.7**	**348.9**	**417.3**	**22.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 408 MEXICO: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	10.3	13.3	16.9	21.1	26.9%
Government & Defense	8.9	11.4	14.4	17.9	26.1%
Healthcare & Life sciences	6.8	9.2	12.3	16.3	34.0%
IT & Telecommunications	6.2	8.0	10.2	12.8	27.2%
Manufacturing	5.6	7.0	8.7	10.7	24.5%
Retail & eCommerce	4.0	5.3	6.9	9.0	31.2%
Energy & Utilities	3.7	4.9	6.5	8.4	31.9%
Media & Entertainment	2.8	3.7	4.8	6.2	30.4%
Education	2.2	2.9	3.9	5.1	32.6%
Other Verticals	4.6	6.3	8.5	11.1	34.4%
Total	**55.0**	**72.0**	**93.1**	**118.5**	**29.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 409 MEXICO: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	26.3	32.4	39.4	47.4	56.4	66.2	20.2%
Government & Defense	22.1	27.0	32.5	38.8	45.8	53.2	19.2%
Healthcare & Life sciences	21.4	27.9	35.9	45.7	57.6	71.4	27.2%
IT & Telecommunications	15.9	19.6	24.0	28.9	34.5	40.5	20.5%
Manufacturing	13.0	15.6	18.4	21.6	25.0	28.5	17.0%
Retail & eCommerce	11.6	14.7	18.5	23.1	28.4	34.4	24.4%
Energy & Utilities	10.9	13.9	17.6	22.1	27.3	33.3	25.2%
Media & Entertainment	7.9	10.0	12.5	15.5	19.0	22.9	23.7%
Education	6.6	8.5	10.8	13.5	16.8	20.5	25.5%
Other Verticals	14.8	19.3	24.6	31.0	38.2	46.2	25.6%
Total	**150.5**	**188.8**	**234.3**	**287.7**	**348.9**	**417.3**	**22.6%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

13.6.4 REST OF LATIN AMERICA

The Rest of Latin America, comprising Argentina, Chile, Colombia, Peru, Costa Rica, Ecuador, Uruguay, the Dominican Republic, and other regional economies, is steadily expanding its AI SOC market through digital government modernization, enterprise cloud adoption, and growing investments in cybersecurity resilience. Unlike Brazil, where AI development is supported by large-scale national investments, or Mexico, where industrial digitalization and nearshoring are key growth drivers, these countries are strengthening AI-enabled security operations by modernizing public digital infrastructure, expanding cloud-based services, and improving cyber readiness across critical sectors. Rapid digitalization of financial services, healthcare, telecommunications, mining, utilities, and public administration is increasing the demand for AI-powered threat detection, automated security analytics, and intelligent incident response solutions capable of protecting increasingly connected digital environments.

Regional collaboration is further accelerating AI and cybersecurity maturity across these markets. During 2025, Chile and the European Union launched the EU–LAC Digital Alliance Cybersecurity Capacity Building Program, bringing together multiple Latin American countries to strengthen cybersecurity regulations, develop common policy frameworks, and enhance regional cyber resilience. In parallel, Peru and Chile signed a bilateral agreement to jointly advance AI research and the Latam-GPT initiative, reinforcing regional cooperation on sovereign AI development and trusted AI ecosystems. Countries including Chile, Colombia, Argentina, Peru, and Uruguay are also expanding national AI strategies, digital innovation programs, and cybersecurity capabilities to support secure AI deployment across government and enterprise sectors. These collaborative initiatives are creating favorable conditions for organizations to modernize conventional SOCs with AI-assisted threat detection, automated investigation, and intelligent security operations, positioning the Rest of Latin America as an emerging growth market for AI SOC solutions throughout the forecast period.

TABLE 410 REST OF LATIN AMERICA: AI SOC MARKET, BY OFFERING, 2022–2025 (USD MILLION)

Offering	2022	2023	2024	2025	CAGR (2022–2025)
Software Platforms	18.8	24.1	30.5	37.9	26.4%
Services	10.8	14.0	18.0	22.8	28.4%
Total	**29.5**	**38.1**	**48.5**	**60.7**	**27.2%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 411 REST OF LATIN AMERICA: AI SOC MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Software Platforms	47.1	57.9	70.4	84.8	100.8	118.2	20.2%
Services	28.8	35.9	44.4	54.3	65.6	78.2	22.1%
Total	**75.9**	**93.9**	**114.9**	**139.1**	**166.4**	**196.4**	**20.9%**

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 412 REST OF LATIN AMERICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2022–2025 (USD MILLION)

Software Platforms	2022	2023	2024	2025	CAGR (2022–2025)
AI-enabled Detection and Analytics Platforms	7.0	8.6	10.4	12.4	21.0%
AI-orchestrated Response and Automation Platforms	2.9	3.6	4.5	5.4	23.2%
AI-native SOC Platforms	4.0	5.2	6.7	8.4	28.1%
AI SOC Agent Solutions	1.3	2.1	3.2	4.8	56.8%
Security Data Platforms	0.9	1.2	1.5	1.8	25.2%
Threat Intelligence Platforms	1.2	1.6	2.0	2.4	25.2%
AI Governance, Risk, and Compliance Solutions	1.5	1.9	2.4	2.7	22.1%
Total	**18.8**	**24.1**	**30.5**	**37.9**	**26.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 413 REST OF LATIN AMERICA: AI SOC MARKET, BY SOFTWARE PLATFORM, 2026–2031 (USD MILLION)

Software Platforms	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-enabled Detection and Analytics Platforms	14.5	16.8	19.3	21.9	24.5	27.1	13.3%
AI-orchestrated Response and Automation Platforms	6.5	7.8	9.2	10.7	12.4	14.1	16.6%
AI-native SOC Platforms	10.6	13.2	16.2	19.8	23.8	28.2	21.6%
AI SOC Agent Solutions	6.6	9.1	12.3	16.4	21.7	28.2	33.5%
Security Data Platforms	2.2	2.7	3.3	3.9	4.6	5.3	19.0%
Threat Intelligence Platforms	3.0	3.6	4.3	5.2	6.1	7.1	19.0%
AI Governance, Risk, and Compliance Solutions	3.7	4.7	5.9	7.0	7.8	8.2	17.5%
Total	**47.1**	**57.9**	**70.4**	**84.8**	**100.8**	**118.2**	**20.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 414 REST OF LATIN AMERICA: AI SOC MARKET, BY SERVICE, 2022–2025 (USD MILLION)

Services	2022	2023	2024	2025	CAGR (2022–2025)
AI-augmented Managed Detection and Response (MDR)	5.8	7.4	9.4	11.7	26.2%
AI SOC-as-a-Service (SOCaaS)	0.3	0.6	0.9	1.3	58.0%
Incident Response and Forensics Services	0.7	1.0	1.3	1.7	33.4%
Threat Intelligence and Advisory Services	3.9	5.1	6.5	8.1	27.5%
Total	**10.8**	**14.0**	**18.0**	**22.8**	**28.4%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 415 REST OF LATIN AMERICA: AI SOC MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Services	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
AI-augmented Managed Detection and Response (MDR)	14.5	17.7	21.5	25.7	30.5	35.7	19.8%
AI SOC-as-a-Service (SOCaaS)	1.9	2.6	3.5	4.8	6.4	8.5	35.4%
Incident Response and Forensics Services	2.2	2.9	3.7	4.6	5.8	7.1	26.1%
Threat Intelligence and Advisory Services	10.2	12.8	15.8	19.1	22.9	26.9	21.3%
Total	**28.8**	**35.9**	**44.4**	**54.3**	**65.6**	**78.2**	**22.1%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 416 REST OF LATIN AMERICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2022–2025 (USD MILLION)

Organization Size	2022	2023	2024	2025	CAGR (2022–2025)
Large Enterprises	21.3	27.1	34.0	42.0	25.4%
SMEs	8.2	11.0	14.5	18.7	31.6%
Total	**29.5**	**38.1**	**48.5**	**60.7**	**27.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 417 REST OF LATIN AMERICA: AI SOC MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	51.8	63.1	76.1	90.9	107.2	124.7	19.2%
SMEs	24.2	30.8	38.7	48.2	59.2	71.6	24.3%
Total	**75.9**	**93.9**	**114.9**	**139.1**	**166.4**	**196.4**	**20.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 418 REST OF LATIN AMERICA: AI SOC MARKET, BY APPLICATION, 2022–2025 (USD MILLION)

Application	2022	2023	2024	2025	CAGR (2022–2025)
Threat Detection and Monitoring	7.7	9.6	12.0	14.6	24.0%
Alert Triage and Prioritization	3.6	4.9	6.4	8.4	32.5%
Incident Investigation and Analysis	3.5	4.7	6.2	8.0	31.3%
Threat Hunting	2.3	3.0	3.8	4.9	28.6%
Incident Response and Remediation	3.7	4.7	5.9	7.3	25.5%
Insider Threat Detection	1.3	1.8	2.3	3.0	32.0%
Cloud Security Monitoring	2.5	3.2	4.0	4.9	24.7%
Identity and Access Monitoring	1.4	1.8	2.4	3.0	31.0%
Compliance Monitoring and Reporting	0.7	1.0	1.4	1.8	34.9%
Security Analytics and Visualization	2.8	3.5	4.2	4.8	19.4%
Total	**29.5**	**38.1**	**48.5**	**60.7**	**27.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 419 REST OF LATIN AMERICA: AI SOC MARKET, BY APPLICATION, 2026–2031 (USD MILLION)

Application	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Threat Detection and Monitoring	17.7	21.3	25.3	29.7	34.5	39.6	17.4%
Alert Triage and Prioritization	10.9	13.9	17.6	22.1	27.3	33.4	25.1%
Incident Investigation and Analysis	10.3	13.0	16.4	20.4	25.1	30.4	24.3%
Threat Hunting	6.1	7.7	9.5	11.6	14.0	16.7	22.2%
Incident Response and Remediation	9.0	11.0	13.2	15.8	18.6	21.7	19.3%
Insider Threat Detection	3.9	5.0	6.3	7.9	9.8	11.9	24.8%
Cloud Security Monitoring	5.9	7.2	8.6	10.2	11.9	13.8	18.3%
Identity and Access Monitoring	3.9	4.9	6.2	7.7	9.5	11.5	24.1%
Compliance Monitoring and Reporting	2.4	3.1	4.0	5.0	6.3	7.8	26.6%
Security Analytics and Visualization	5.8	6.8	7.8	8.7	9.4	9.7	11.1%
Total	**75.9**	**93.9**	**114.9**	**139.1**	**166.4**	**196.4**	**20.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

TABLE 420 REST OF LATIN AMERICA: AI SOC MARKET, BY VERTICAL, 2022–2025 (USD MILLION)

Vertical	2022	2023	2024	2025	CAGR (2022–2025)
BFSI	5.6	7.0	8.8	10.8	24.9%
Government & Defense	4.8	6.0	7.5	9.2	24.1%
Healthcare & Life sciences	3.6	4.9	6.4	8.3	31.9%
IT & Telecommunications	3.3	4.2	5.3	6.5	25.2%
Manufacturing	3.0	3.7	4.5	5.5	22.5%
Retail & eCommerce	2.1	2.8	3.6	4.6	29.2%
Energy & Utilities	2.0	2.6	3.4	4.3	29.8%
Media & Entertainment	1.5	2.0	2.5	3.2	28.3%
Education	1.2	1.6	2.0	2.6	30.5%
Other Verticals	2.5	3.3	4.4	5.7	32.3%
Total	**29.5**	**38.1**	**48.5**	**60.7**	**27.2%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 421 REST OF LATIN AMERICA: AI SOC MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	13.3	16.1	19.3	22.9	26.9	31.1	18.6%
Government & Defense	11.2	13.4	16.0	18.8	21.8	25.0	17.6%
Healthcare & Life sciences	10.8	13.9	17.6	22.1	27.5	33.6	25.5%
IT & Telecommunications	8.0	9.8	11.7	14.0	16.4	19.1	18.9%
Manufacturing	6.6	7.7	9.0	10.4	11.9	13.4	15.4%
Retail & eCommerce	5.8	7.3	9.1	11.1	13.5	16.2	22.7%
Energy & Utilities	5.5	6.9	8.6	10.7	13.0	15.7	23.4%
Media & Entertainment	4.0	5.0	6.2	7.5	9.1	10.8	22.0%
Education	3.3	4.2	5.3	6.5	8.0	9.7	23.7%
Other Verticals	7.5	9.6	12.1	15.0	18.2	21.8	23.9%
Total	**75.9**	**93.9**	**114.9**	**139.1**	**166.4**	**196.4**	**20.9%**

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

14 COMPETITIVE LANDSCAPE

This chapter provides a broad understanding of the competitive leadership mapping of key vendors and startups/SMEs in the AI SOC market. These players have adopted organic and inorganic growth strategies to expand their global presence, which has helped them increase their market share. The competitive landscape section analyzes the growth strategies various major players implement in the global AI SOC market.

14.1 KEY PLAYER STRATEGIES/RIGHT TO WIN

Key players in the market have adopted organic and inorganic growth strategies to expand their global presence, which has supported them in increasing their market share. Major market players generate significant revenue from North America, followed by Europe and Asia Pacific. The strategies adopted by key players are given below.

TABLE 422 OVERVIEW OF STRATEGIES ADOPTED BY KEY AI SOC VENDORS, 2024–2026

KEY PLAYER	PRODUCT TYPE	STRATEGIC DEVELOPMENTS/ PARTNERSHIPS	MERGERS & ACQUISITIONS/PRODUCT LAUNCHES	REGION
Microsoft	AI-Powered Unified SecOps Platform, Microsoft Security Copilot, Microsoft Defender XDR, Microsoft Sentinel, Microsoft Security Exposure Management, Microsoft Defender for Cloud, and Microsoft Defender Experts for XDR	Microsoft collaborated with CP Group, True, and True IDC to accelerate Thailand's AI and cloud ecosystem, including exploration of an AI-powered Cloud Security Operations Center (SOC) for real-time threat detection, predictive analytics, and automated incident response.	Microsoft launched Copilot for Security, a generative AI-powered security solution that assists SOC analysts with incident investigation, threat hunting, response recommendations, and security intelligence analysis to accelerate cybersecurity operations and improve analyst productivity.	Strong global presence across North America, Europe, Asia Pacific, Middle East & Africa, and Latin America
Cisco	Cisco XDR, Splunk Enterprise Security, Splunk SOAR, Cisco AI Assistant for Security, Cisco AI Canvas, Cisco Security Cloud Control, Cisco Managed Detection and Response (MDR), and Cisco Incident Response Services	Cisco partnered with Indosat Ooredoo Hutchison to launch Indonesia's Sovereign Security Operations Centre, combining Splunk Enterprise Security, AI-powered threat detection, real-time security monitoring, and localized data residency to strengthen AI-driven security operations and cyber resilience.	Cisco announced the acquisition of WideField Security to strengthen Splunk's Agentic SOC capabilities by enriching identity intelligence, correlating AI-agent activity, and improving autonomous threat detection and investigation across enterprise environments.	Strong global presence with significant revenue contribution from North America, Europe, Asia Pacific, and Latin America

JULY 2026 © MarketsandMarkets™

CrowdStrike	CrowdStrike Falcon Next-Gen SIEM, Charlotte AI, Charlotte Agentic SOAR, Charlotte AI AgentWorks, Falcon Complete Next-Gen MDR, AI Security Readiness Services, and Falcon Onum	CrowdStrike partnered with IBM to integrate Charlotte AI with IBM's Autonomous Threat Operations Machine (ATOM), combining AI-driven investigation, coordinated machine-speed response, managed Threat Detection and Response services, and Cyber Range validation to accelerate enterprise Agentic SOC transformation.	CrowdStrike launched Agentic MDR and SOC Transformation Services to help organizations operationalize the Agentic SOC by combining AI agents, Falcon Complete expertise, automated investigations, machine-speed response, and modernization of SIEM, data pipelines, governance, and security workflows.	Strong enterprise presence across North America, Europe, Asia Pacific, and Middle East & Africa
Palo Alto Networks	Cortex XSIAM, Cortex XDR, Cortex XSOAR, Unit 42 Managed XSIAM, Unit 42 Managed Detection and Response (MDR), and Unit 42 Managed Threat Hunting	Palo Alto Networks partnered with Wipro to combine Cortex XSIAM with Wipro CyberShield, delivering AI-powered managed security operations, automated threat detection, and machine-learning-driven SOC services for enterprise customers worldwide.	Palo Alto Networks completed the acquisition of CyberArk, integrating privileged access management and identity security into its AI-driven cybersecurity platform to secure human and machine identities within autonomous security operations and AI-enabled enterprise environments.	Strong presence across North America, Europe, and Asia Pacific with growing enterprise adoption
Google	Google Security Operations – Agentic SOC Platform, Gemini in Google Security Operations, Triage and Investigation Agent, Detection Engineering Agent, Threat Hunting Agent, Google Security Operations SIEM, Google Security Operations SOAR, Google Threat Intelligence, Google Cloud Cybershield, Mandiant Threat Defense, and Mandiant Incident Response (IR)	Google partnered with Tata Consultancy Services (TCS) to expand their strategic collaboration by launching TCS AI SOC enabled by Google SecOps, combining Google SecOps, Gemini, and Google Threat Intelligence to deliver AI-driven threat detection, autonomous investigations, and faster incident response.	Google launched the Triage and Investigation Agent within Security Operations, enabling autonomous alert analysis, evidence collection, investigation summaries, and threat validation to reduce analyst workload and significantly accelerate security incident investigation processes.	Strong global presence with major revenue contribution from North America, Europe, and Asia Pacific

Source: Company Website, Press Releases, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

Strategies of various AI SOC vendors have been assessed based on the following:

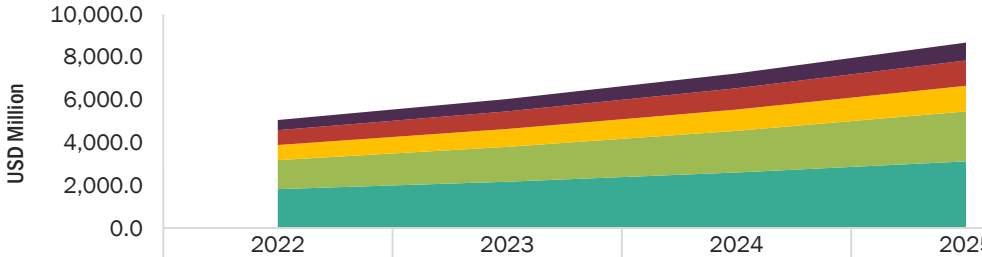
- **Product type:** Assessed to check if the product portfolio is comprehensive, covering most solutions, or focused on a handful of solutions
- **Regional focus:** Assessed to understand if the company's strategies are well-diversified globally or focused on a few key regions. This has been assessed based on where they source their revenues and where their primary client base exists
- **Strategic development/partnerships:** Assessed to see if the companies are deploying organic means to grow or leveraging partnerships (technology-based or go-to-market-based) to increase revenues
- **Mergers and acquisition/New product launch:** Assessed to check if the companies have been active on the M&A front or investing in startups

14.2 REVENUE ANALYSIS

Players in the AI SOC market were identified through secondary research, and their market share was inferred from their annual reports, presentations, and secondary research sources. Primary research interviews were conducted with key opinion leaders in the industry, such as chief executive officers (CEOs), directors, industry experts, and other executives, to validate revenues and market shares.

The first step in preparing this report was to define the approach and methodology to estimate the market size. This was followed by primary interviews and feature mapping on a regional basis from the MarketsandMarkets repository. The bottom-up approach was followed to derive the market size in terms of value. In-depth interviews with industry experts and secondary research validated the market size. The excerpts of these interviews are available in the discussion guide section of the appendix chapter.

FIGURE 41 SEGMENTAL REVENUE ANALYSIS OF KEY PLAYERS, 2022–2025 (USD MILLION)



	2022	2023	2024	2025
Google	482.9	576.7	690.3	828.0
Palo Alto Networks	692.3	826.7	989.7	1,187.0
CrowdStrike	700.5	836.5	1,001.4	1,201.1
Cisco Systems	1,359.3	1,623.3	1,943.3	2,330.8
Microsoft	1,821.6	2,175.3	2,604.1	3,123.4

Note 1: The market share of key players is estimated based on their product offerings and business strategies. Secondary research and in-depth primary interviews conducted with key industry leaders have also contributed to the analysis.

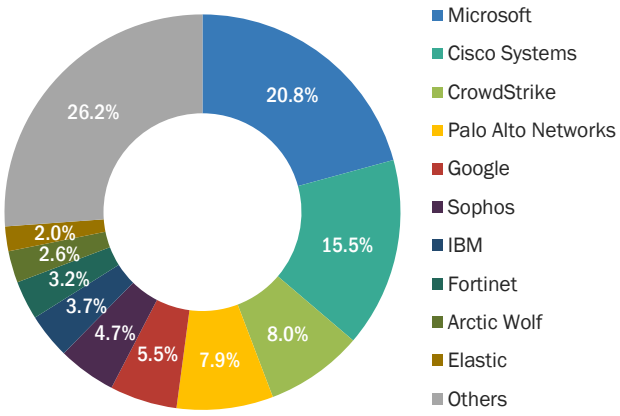
Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

14.3 MARKET SHARE ANALYSIS

The market share and ranking of key players are arrived at based on various parameters, including product offerings, regional reach, segmental revenue, and organic and inorganic growth strategies, such as product launches, partnerships, and collaborations.

FIGURE 42 SHARE OF LEADING COMPANIES IN AI SOC MARKET, 2025



Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 423 AI SOC MARKET: DEGREE OF COMPETITION

DEGREE OF COMPETITION	CONSOLIDATED
Total Market Share of Top 10 Players	73.85%
Microsoft	20.75%
Cisco Systems	15.48%
CrowdStrike	7.98%
Palo Alto Networks	7.89%
Google	5.50%
Sophos	4.75%
IBM	3.70%
Fortinet	3.18%
Arctic Wolf	2.60%
Elastic	2.02%

Source: Press Releases, Investor Presentations, Interviews with Experts, and MarketsandMarkets Analysis

THE DEGREE OF COMPETITION IS DEFINED BELOW:

- Fragmented: When the top ten players have a total market share of < 25%
- Competitive: When the top ten players have a total of 25–50% market share
- Consolidated: When the top ten players have a total market share of > 50%

JULY 2026 © MarketsandMarkets™

The market is highly consolidated, and below are a few strategies adopted by the top five vendors and their right to win:

Microsoft:

- Strategy: Microsoft strengthens its leadership in the AI SOC market by integrating generative AI, agentic AI, threat intelligence, and autonomous security operations across its unified security ecosystem. Through Microsoft Security Copilot, Microsoft Defender XDR, Microsoft Sentinel, Entra, and Purview, the company is transforming traditional SOCs into agentic security operations capable of automating investigations, triaging alerts, and orchestrating responses across identity, endpoint, cloud, email, and data environments. Microsoft further reinforces this strategy through its global threat intelligence, extensive partner ecosystem, and continuous investment in autonomous security agents.
- Right to Win: Microsoft's competitive advantage stems from its ability to combine cloud infrastructure, productivity applications, identity security, XDR, SIEM, threat intelligence, and AI within a single integrated platform. With Security Copilot, autonomous security agents, Microsoft Defender XDR, and Sentinel operating on Microsoft's global telemetry, the company enables enterprises to unify security operations, automate high-volume analyst tasks, and progressively evolve toward an agentic SOC while leveraging the scale of Azure and Microsoft 365 ecosystems.

Cisco:

- Strategy: Cisco is positioning AI SOC as a core pillar of its Security Cloud by combining networking, observability, identity, Splunk's security analytics, and AI-powered security operations into a unified architecture. Following the acquisition of Splunk, Cisco is integrating AI-driven detection, security analytics, automation, and threat intelligence to help enterprises modernize SOC operations while simultaneously securing emerging AI applications, AI agents, and hybrid infrastructures.
- Right to Win: Cisco's primary advantage lies in combining enterprise networking, cloud security, identity, Splunk SIEM, observability, and AI security capabilities under one ecosystem. The integration of Splunk significantly expands Cisco's AI SOC capabilities by enabling unified telemetry, AI-powered analytics, automated investigations, and security operations across network, cloud, endpoint, and application environments, making Cisco a strategic platform provider for large global enterprises.

CrowdStrike:

- Strategy: CrowdStrike continues to expand its AI SOC strategy around the Falcon platform by embedding agentic AI, autonomous detection, cloud-native security analytics, and real-time threat intelligence across modern security operations. Through Charlotte AI, Falcon Next-Gen SIEM, Falcon Fusion, Falcon Complete Next-Gen MDR, and Falcon Adversary OverWatch, the company is enabling enterprises to automate investigations, accelerate incident response, and improve analyst productivity while protecting hybrid and AI-enabled environments.
- Right to Win: CrowdStrike differentiates itself through its cloud-native Falcon platform, industry-leading threat intelligence, and extensive endpoint telemetry collected from millions of protected assets worldwide. By combining Charlotte AI, Falcon Next-Gen SIEM, MDR, identity protection, cloud security, and automation within a unified platform, CrowdStrike enables organizations to rapidly investigate threats, reduce alert fatigue, and operate AI-assisted security operations at enterprise scale.

JULY 2026 © MarketsandMarkets™

Palo Alto Networks:

- Strategy: Palo Alto Networks is driving AI SOC transformation through its AI-powered Cortex Security Operations Platform, combining Cortex XSIAM, Cortex XDR, Cortex Cloud, Precision AI, and agentic AI capabilities into a unified autonomous security architecture. The company is increasingly positioning AI SOC as the operational foundation for modern cyber defense by integrating endpoint, network, cloud, identity, and AI security into a single platform capable of continuously detecting, investigating, and responding to threats.
- Right to Win: Palo Alto Networks' competitive strength lies in its ability to unify massive volumes of security telemetry with AI-driven analytics, automation, and autonomous response across the entire enterprise environment. Through Cortex XSIAM, Precision AI, and Frontier AI support, the company enables enterprises to consolidate fragmented security tools, automate complex SOC workflows, reduce analyst workload, and transition toward intelligent, autonomous security operations while leveraging one of the industry's largest cybersecurity data ecosystems.

Google:

- Strategy: Google continues to strengthen its AI SOC strategy by combining Google Security Operations, Gemini, Google Threat Intelligence, Mandiant expertise, and Google Cloud's AI infrastructure into a unified, cloud-native security platform. The company is increasingly embedding generative and agentic AI across threat detection, investigation, threat hunting, malware analysis, and incident response while leveraging Google's global-scale cloud, AI, and internet intelligence to modernize enterprise SOC operations.
- Right to Win: Google's key advantage lies in combining industry-leading AI innovation, hyperscale cloud infrastructure, Mandiant threat intelligence, VirusTotal intelligence, and Google Security Operations within a single platform. By integrating Gemini-powered investigations, cloud-scale analytics, and AI-assisted SOC workflows, Google enables enterprises to improve detection accuracy, accelerate investigations, automate repetitive analyst tasks, and securely protect increasingly AI-driven enterprise environments.

JULY 2026 © MarketsandMarkets™

14.4 BRAND/PRODUCT COMPARISON

FIGURE 43 AI SOC MARKET: COMPARISON OF VENDORS' BRANDS/PRODUCTS

PARAMETERS	Microsoft	Cisco	CrowdStrike	paloalto NETWORKS	Google
PRODUCT PORTFOLIO	●	●	●	●	●
INNOVATION READINESS	●	◔	●	◔	●
CUSTOMER FEEDBACK/ RATING	●	●	◔	●	◔
STRENGTHS	Unified AI security ecosystem with unmatched cloud, identity, threat intelligence, and enterprise adoption.	Strong networking expertise combined with Splunk analytics enables comprehensive AI-driven security operations.	Industry-leading cloud-native Falcon platform with advanced threat intelligence and AI-driven detection.	Broad AI-powered cybersecurity portfolio with strong automation and autonomous SOC capabilities.	Combines Gemini AI, Mandiant intelligence, and hyperscale cloud for advanced AI SOC.
WEAKNESSES	Highest value achieved within Microsoft ecosystem; licensing and multi-vendor integration remain complex.	Splunk integration transition may increase deployment complexity and operational learning curve.	Less comprehensive networking portfolio than competitors offering broader infrastructure security capabilities.	Extensive product portfolio increases implementation complexity and overall deployment costs.	Greater dependence on Google Cloud ecosystem for maximizing AI SOC capabilities.

IMPACT: ● EXCELLENT | ◔ GOOD | ◑ FAIR | ◔ POOR

Source: Annual Reports, Press Releases, and MarketsandMarkets Analysis

Microsoft

Microsoft remains a leading AI SOC provider through its integrated security ecosystem comprising Microsoft Security Copilot, Microsoft Defender XDR, Microsoft Sentinel, Microsoft Entra, and Defender for Cloud. The company combines generative AI, autonomous security agents, XDR, SIEM, and global threat intelligence to automate threat detection, investigation, and response across hybrid, multi-cloud, endpoint, identity, email, and data environments. Leveraging Azure's hyperscale infrastructure and an extensive partner ecosystem, Microsoft enables enterprises to build unified, AI-driven security operations while securing emerging AI workloads and digital assets.

Cisco

Cisco continues to strengthen its AI SOC portfolio by integrating Splunk Enterprise Security, Splunk SOAR, Cisco XDR, Cisco AI Defense, and Security Cloud into a unified AI-powered security operations platform. Following the Splunk acquisition, Cisco has expanded its capabilities across AI-driven threat detection, observability, automation, and incident response. The company leverages its leadership in networking, cloud security, identity, and enterprise infrastructure to deliver AI SOC capabilities across complex hybrid and multi-cloud environments.

JULY 2026 © MarketsandMarkets™

CrowdStrike

CrowdStrike is a leading AI-native security vendor built around the Falcon platform, integrating Charlotte AI, Falcon Next-Gen SIEM, Falcon Fusion SOAR, Falcon Complete Next-Gen MDR, and Falcon Adversary OverWatch. The company leverages cloud-native architecture, real-time threat intelligence, and AI-powered automation to help organizations detect, investigate, and remediate cyber threats at machine speed. Continuous innovation in agentic AI, identity protection, cloud security, and managed detection and response has strengthened CrowdStrike's position in modern AI SOC deployments.

Palo Alto Networks

Palo Alto Networks continues to be a prominent AI SOC provider through its Cortex Security Operations Platform, including Cortex XSIAM, Cortex XDR, Cortex XSOAR, Precision AI, and Cortex Cloud. The company helps enterprises consolidate fragmented security operations into an autonomous, AI-driven platform capable of correlating telemetry across network, endpoint, cloud, identity, and application environments. By combining advanced automation, AI-powered analytics, and extensive cybersecurity expertise, Palo Alto Networks enables organizations to modernize SOC operations while improving detection accuracy and response efficiency.

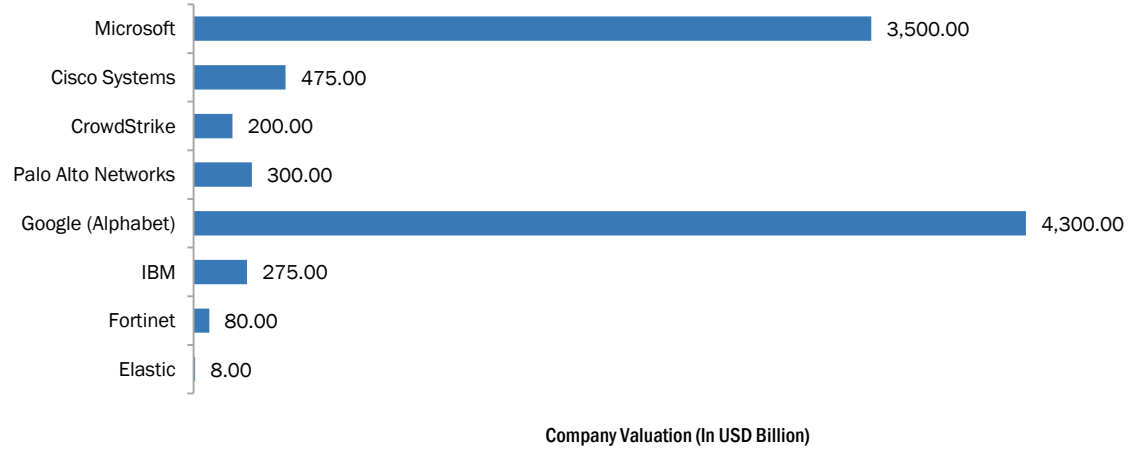
Google

Google has established a strong position in the AI SOC market through Google Security Operations, Gemini in Security Operations, Google Threat Intelligence, Mandiant, VirusTotal, and Chronicle SIEM. The company combines hyperscale cloud infrastructure, generative AI, threat intelligence, and security analytics to help organizations automate investigations, threat hunting, malware analysis, and incident response. Google's AI SOC strategy is further strengthened by continuous innovation in Gemini-powered security workflows and strategic investments in cloud-native cybersecurity capabilities.

14.5 COMPANY VALUATION AND FINANCIAL METRICS

14.5.1 COMPANY VALUATION

FIGURE 44 COMPANY VALUATION, 2025 (USD BILLION)

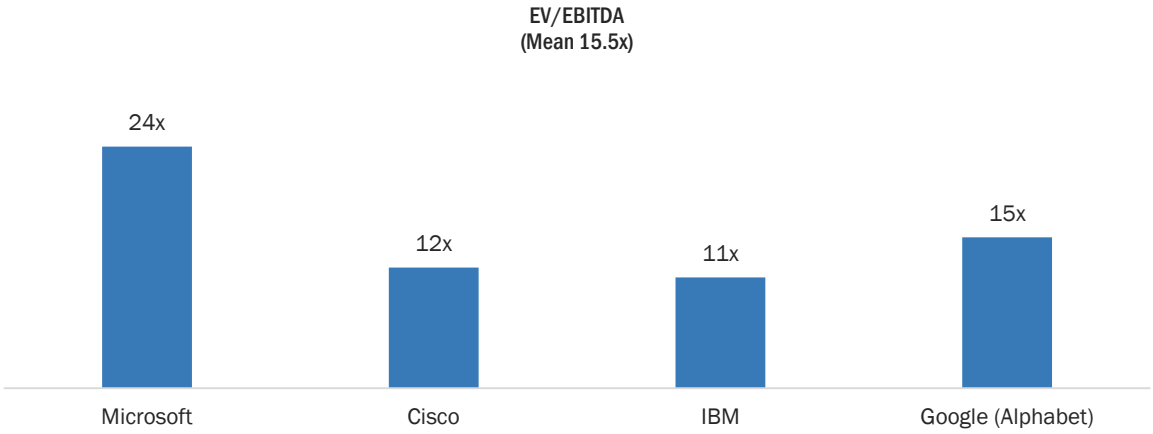


Source: dealroom.co

JULY 2026 © MarketsandMarkets™

14.5.2 FINANCIAL METRICS USING EV/EBIDTA

FIGURE 45 EV/EBIDTA, 2025



Note: EV/EBITDA for all the mentioned companies is as of July 28, 2026.

Source: Finbox.com

14.6 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2025

The company evaluation matrix provides information about the major players offering AI SOC software platforms and services. It also outlines the findings and analysis of how well each market vendor performs within the predefined competitive leadership mapping criteria. The vendor evaluations are based on two broad categories: product footprint and market share/rank. Each category carries various criteria based on which vendors have been evaluated. The evaluation criteria considered under the product footprint include the breadth and depth of product offerings, product features and functionality, and estimated product revenue.

Based on a questionnaire, extensive secondary and primary research was conducted to gather critical information about the vendor's strength of product portfolio and market share/rank. A scale of 0–10 was formulated for each question, after which each criterion for every vendor was scored based on the collected information. After data gathering and verification, the scores and weightage for shortlisted vendors against each parameter were finalized. A comparison scorecard was prepared after evaluating all vendors, and they were then placed into four categories based on their performance in each criterion. These are Stars, Emerging Leaders, Pervasive Players, and Participants.

- Stars (companies with large market share, wider application, and geographical use cases and footprint)
- Emerging leaders (companies with large market share, low application, and geographical penetration)
- Pervasive players are companies with small market share, high application, and regional availability; these players' products are available for multiple application/end-use industries and in most regions worldwide
- Participants have a small footprint in the market at a global level but may have a strong presence in one or more regions and/or customer segments

JULY 2026 © MarketsandMarkets™

14.6.1 STARS

Microsoft, Cisco, CrowdStrike, Palo Alto Networks, Google, Sophos, and IBM are considered the leaders in the AI SOC market and are recognized as star players. They offer robust software platforms and service portfolios in the AI SOC market. These vendors have been marking their presence in the market by providing customized solutions as per the requirements of end use verticals and adopting growth strategies to achieve technological consistency in the AI SOC market.

14.6.2 EMERGING LEADERS

Fortinet, Arctic Wolf, Elastic, and Exabeam are recognized as emerging leaders in the AI SOC market. They possess innovative solutions to cater to future AI SOC demands. These companies are concerned about their product portfolio and have a robust potential to build strong business strategies to expand their business and stay on par with the stars. These vendors have been offering their customers AI SOC solutions to fulfill their demands. Emerging leaders have been at the forefront of the deployment of solutions.

14.6.3 PERVASIVE PLAYERS

Rapid7, ReliaQuest, SentinelOne, Expel, and eSentire are recognized as pervasive players in the AI SOC market. They offer innovative software platforms and services portfolios and have an extensive network of channel partners and resellers to increase the deployment of their solutions across many vertical markets. Pervasive companies have consistently generated positive revenue growth in the AI SOC market. Their market position is boosted by the organic and inorganic ventures they undertake.

14.6.4 PARTICIPANTS

Most participant companies have been adopting multiple organic and inorganic strategies to boost their sales capabilities across regions and offer clients integrated AI SOC solutions and services. These companies have the scope to grow their market share by expanding their product offering. No companies have been identified under this category for this market.

JULY 2026 © MarketsandMarkets™

FIGURE 46 AI SOC MARKET: COMPANY EVALUATION MATRIX (KEY PLAYERS), 2025



Source: Press Releases, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

14.6.5 COMPANY FOOTPRINT: KEY PLAYERS

14.6.5.1 Company footprint

FIGURE 47 AI SOC MARKET: COMPANY FOOTPRINT, 2025

COMPANY NAME	OFFERING FOOTPRINT	ORGANIZATION SIZE FOOTPRINT	VERTICAL FOOTPRINT	REGIONAL FOOTPRINT	OVERALL FOOTPRINT
Microsoft	○○○○	○○○○	○○○○	○○○○	○○○○
Cisco	○○○○	○○○○	○○○	○○○○	○○○
CrowdStrike	○○○○	○○○○	○○○	○○○○	○○○
Palo Alto Networks	○○○○	○○○○	○○○	○○○○	○○○
Google	○○○○	○○○○	○○○○	○○○○	○○○○
Sophos	○○○○	○○○○	○○○	○○○○	○○○
IBM	○○○○	○○○○	○○○	○○○○	○○○
Fortinet	○○○○	○○○○	○○○○	○○○○	○○○○
Arctic Wolf	○○○○	○○○○	○○○	○○○○	○○○
Elastic	○○○	○○○○	○○○	○○○○	○○○
Rapid7	○○○○	○○○○	○○○	○○○○	○○
SentinelOne	○○○○	○○○○	○○○	○○○○	○○
Expel	○○○○	○○○○	○○	○○○○	○○
ReliaQuest	○○○○	○○○○	○○	○○○○	○○
Exabeam	○○○○	○○○○	○○	○○○○	○○
eSentire	○○○○	○○○○	○○	○○○	○○

RATING : ○○○○ EXCELLENT ○○○ GOOD ○○ AVERAGE ○ BELOW AVERAGE NOT APPLICABLE

Source: Press Releases, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

14.6.5.2 Offering footprint

TABLE 424 AI SOC MARKET: OFFERING FOOTPRINT, 2025

COMPANY	SOFTWARE PLATFORMS	SERVICES	OVERALL OFFERING FOOTPRINT
Microsoft	Y	Y	4.00
Cisco	Y	Y	4.00
CrowdStrike	Y	Y	4.00
Palo Alto Networks	Y	Y	4.00
Google	Y	Y	4.00
Sophos	Y	Y	4.00
IBM	Y	Y	4.00
Fortinet	Y	Y	4.00
Arctic Wolf	Y	Y	4.00
Elastic	Y	N	2.00
Rapid7	Y	Y	4.00
SentinelOne	Y	Y	4.00
Expel	Y	Y	4.00
ReliaQuest	Y	Y	4.00
Exabeam	Y	Y	4.00
eSentire	Y	Y	4.00

Source: Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

14.6.5.3 Organization Size footprint

TABLE 425 AI SOC MARKET: ORGANIZATION SIZE FOOTPRINT, 2025

COMPANY	LARGE ENTERPRISES	SMES	OVERALL ORGANIZATION SIZE FOOTPRINT
Microsoft	Y	Y	4.00
Cisco	Y	Y	4.00
CrowdStrike	Y	Y	4.00
Palo Alto Networks	Y	Y	4.00
Google	Y	Y	4.00
Sophos	Y	Y	4.00
IBM	Y	Y	4.00
Fortinet	Y	Y	4.00

JULY 2026 © MarketsandMarkets™

Arctic Wolf	Y	Y	4.00
Elastic	Y	Y	4.00
Rapid7	Y	Y	4.00
SentinelOne	Y	Y	4.00
Expel	Y	Y	4.00
ReliaQuest	Y	Y	4.00
Exabeam	Y	Y	4.00
eSentire	Y	Y	4.00

Source: Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

14.6.5.4 Vertical footprint

TABLE 426 AI SOC MARKET: VERTICAL FOOTPRINT, 2025

COMPANY	BFSI	GOVERNMENT AND DEFENSE	GOVERNMENT AND DEFENSE	IT & TELECOMMUNICATIONS	MANUFACTURING	RETAIL & ECOMMERCE	ENERGY & UTILITIES	MEDIA & ENTERTAINMENT	EDUCATION	OTHER VERTICALS	OVERALL VERTICAL FOOTPRINT
Microsoft	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
Cisco	Y	Y	Y	N	Y	Y	Y	Y	Y	N	3.20
CrowdStrike	Y	Y	Y	N	Y	Y	N	N	Y	Y	2.80
Palo Alto Networks	Y	Y	Y	N	Y	Y	Y	N	N	N	2.40
Google	Y	Y	Y	Y	Y	Y	N	Y	Y	N	3.20
Sophos	Y	Y	Y	N	Y	Y	N	N	Y	N	2.40
IBM	Y	Y	Y	Y	N	Y	Y	N	N	N	2.40
Fortinet	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
Arctic Wolf	Y	Y	Y	N	Y	Y	N	Y	Y	N	2.80
Elastic	Y	Y	Y	Y	Y	Y	N	Y	N	N	2.80
Rapid7	Y	Y	Y	N	N	Y	Y	N	Y	N	2.40
SentinelOne	Y	Y	Y	N	Y	Y	Y	N	Y	Y	3.20
Expel	Y	N	N	Y	N	Y	N	N	N	N	1.20
ReliaQuest	Y	N	Y	Y	Y	Y	N	N	N	N	2.00
Exabeam	Y	Y	Y	N	Y	N	N	N	Y	N	2.00

JULY 2026 © MarketsandMarkets™

eSentire	Y	Y	Y	N	Y	Y	N	N	N	Y	2.40

Source: Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

14.6.5.5 Regional footprint

TABLE 427 AI SOC MARKET: REGIONAL FOOTPRINT, 2025

COMPANY	NORTH AMERICA	EUROPE	ASIA PACIFIC	MIDDLE EAST & AFRICA	LATIN AMERICA	OVERALL REGIONAL FOOTPRINT
Microsoft	Y	Y	Y	Y	Y	4.00
Cisco	Y	Y	Y	Y	Y	4.00
CrowdStrike	Y	Y	Y	Y	Y	4.00
Palo Alto Networks	Y	Y	Y	Y	Y	4.00
Google	Y	Y	Y	Y	Y	4.00
Sophos	Y	Y	Y	Y	Y	4.00
IBM	Y	Y	Y	Y	Y	4.00
Fortinet	Y	Y	Y	Y	Y	4.00
Arctic Wolf	Y	Y	Y	Y	Y	4.00
Elastic	Y	Y	Y	Y	Y	4.00
Rapid7	Y	Y	Y	Y	Y	4.00
SentinelOne	Y	Y	Y	Y	Y	4.00
Expel	Y	Y	Y	Y	Y	4.00
ReliaQuest	Y	Y	Y	Y	Y	4.00
Exabeam	Y	Y	Y	Y	Y	4.00
eSentire	Y	Y	Y	Y	N	3.20

Source: Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

14.7 COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2025

The company evaluation matrix for startups and SMEs identifies and profiles companies with commercial AI SOC offerings globally, regardless of their development stage (seed, early-stage, and mid-stage). Companies are classified into startups and SMEs based on defined parameters:

SMEs (Small & Medium-sized Enterprises):

- Companies with an annual revenue of less than USD 500 Million

Startups:

- The annual revenue is less than USD 50 million
- The employee count is less than 100
- Company valuation is less than USD 500 million
- The age of the company is less than 10 years, and any of the above conditions is met

The startups/SMEs evaluation matrix features emerging and innovative AI SOC market companies. The startups selected for the matrix were chosen based on their founding years, revenues, and employee count. Overall vendor evaluations are based on the strength of the product portfolio and market shares/rank:

- Progressive Companies: Vendors that have been marking their presence in the market by offering innovative solutions as per customer requirements and adopting various strategies to achieve growth in the market
- Responsive Companies: These companies have a robust potential to build strong business strategies to expand their product footprint and stay on par with progressive companies
- Dynamic Companies: Dynamic companies offer innovative solution portfolios and have competent distribution to increase their market presence
- Starting Blocks: Most starting blocks have been undertaking multiple product developments and launches to cater to a broader range of clients

The competitive evaluation matrix includes the company evaluation matrix of startups operating in the market to understand each player's performance. It features the analysis of startups in the AI SOC market based on their offerings.

14.7.1 PROGRESSIVE COMPANIES

Swimlane, Stellar Cyber, Exaforce, Torq, Lumu, Huntress, D3 (Morpheus), Anvilogic, BlinkOps, and Prophet Security are some of the progressive companies in the AI SOC market. They offer strong solution portfolios and have been marking their presence in the market by offering customized solutions as per requirements and adopting growth strategies to achieve technological consistency in the market.

14.7.2 RESPONSIVE COMPANIES

Dropzone AI, Intezer, and Gruve are recognized as responsive companies in the AI SOC market. They possess innovative solutions to cater to future AI SOC demands. These companies are concerned about their product portfolios and have robust potential to build strong business strategies to expand their business and stay on par with progressive companies. These vendors have been offering their customers AI SOC solutions to fulfill their demands. Responsive companies have been at the forefront of the deployment of their solutions.

JULY 2026 © MarketsandMarkets™

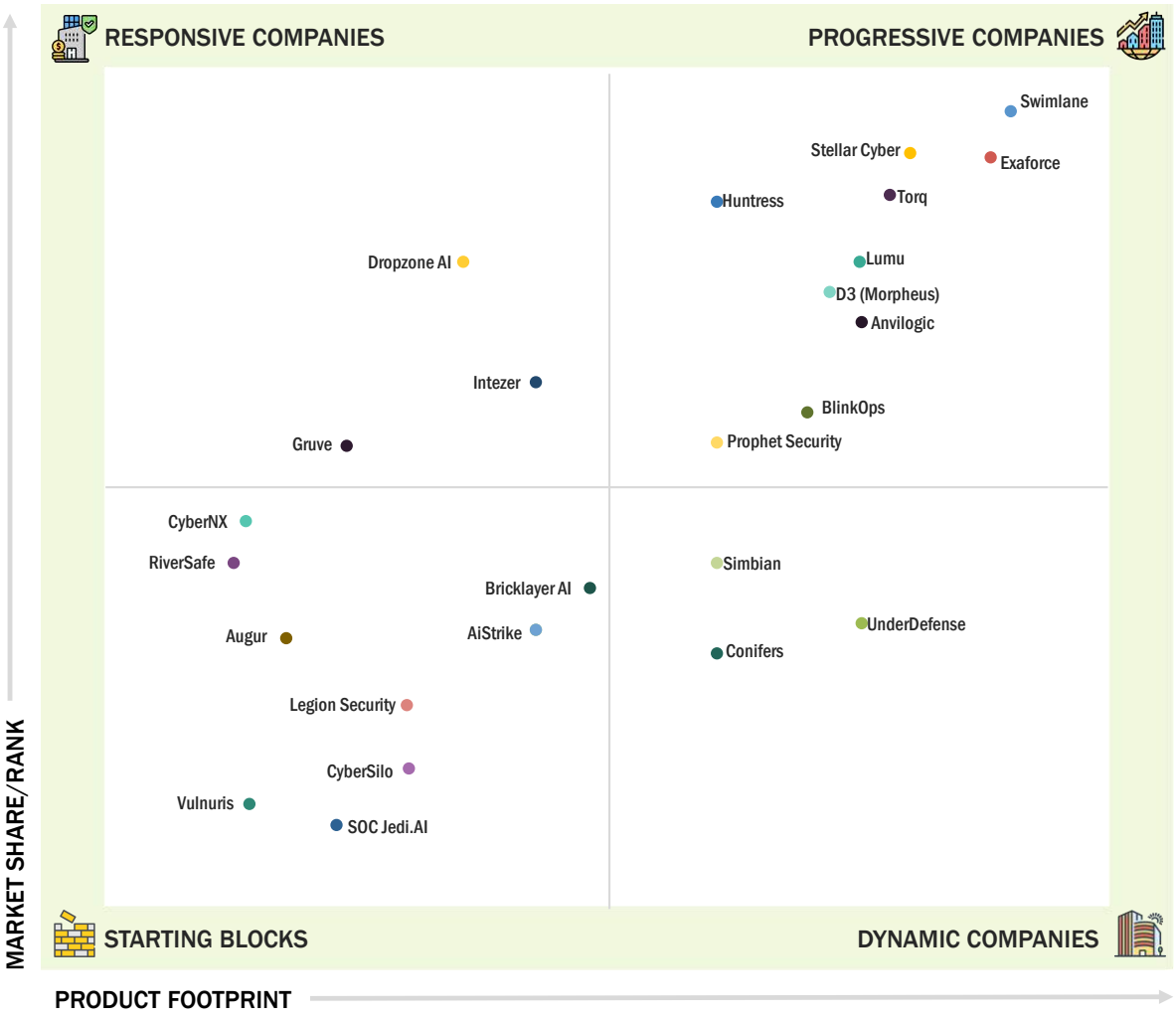
14.7.3 DYNAMIC COMPANIES

Simbian, Conifers, and UnderDefense are recognized as dynamic companies in the AI SOC market. Dynamic companies offer innovative solution portfolios and have an extensive network of channel partners and resellers to increase the deployment of their solutions across many vertical markets. Dynamic companies have consistently generated positive revenue growth in the AI SOC market, and organic and inorganic ventures have boosted their market position.

14.7.4 STARTING BLOCKS

Bricklayer AI, CyberNX, RiverSafe, AiStrike, Augur, Legion Security, CyberSilo, Vulnuris, and SOC Jedi.AI are some of the companies recognized as starting blocks in the AI SOC market. Most of the starting blocks have been undertaking multiple growth strategies to boost their sales capabilities across regions and offer solutions and services to clients.

FIGURE 48 AI SOC MARKET: COMPANY EVALUATION MATRIX (STARTUPS/SMES), 2025



Source: Press Releases, Expert Interviews, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

14.7.5 COMPETITIVE BENCHMARKING: STARTUPS/SMES

14.7.5.1 Detailed list of key startups/SMEs

TABLE 428 DETAILED LIST OF KEY STARTUPS/SMES, 2025

COMPANY NAME	CATEGORY	OWNERSHIP STATUS	HQ LOCATION	YEAR FOUNDED	EMPLOYEES	FINANCING ROUND	LATEST FUNDING ROUND (USD MILLION)	TOTAL FUNDING/TOTAL CAPITAL (USD MILLION)
Lumu Technologies	Computer and Network Security	Private	US	2019	51–200	Conventional Debt	NA	USD 39.5 million
Huntress	Computer and Network Security	Private	US	2015	501–1000	Series D	USD 180 million	USD 298 million
UnderDefense	Computer and Network Security	Private	US	2017	51–200	NA	NA	NA
Swimlane	Computer and Network Security	Private	US	2014	201–500	Series D	USD 45 million	USD 302 million
Stellar Cyber	Computer and Network Security	Private	US	2015	51–200	Conventional Debt	NA	USD 68 million
Radiant Security	Computer and Network Security	Private	US	2021	51–200	Series A	NA	USD 15 million
Torq	Computer and Network Security	Private	US/ Israel	2020	201–500	Series D	USD 140 million	USD 332 million
Intezer	Computer and Network Security	Private	US	2016	51–200	Series C	NA	USD 68.1 million
Conifers.AI	Computer and Network Security	Private	US	2024	11–50	Series A	NA	USD 25 million
Dropzone AI	Computer and Network Security	Private	US	2023	51–200	Series B	NA	USD 57.4 million
Simbian	Computer and Network Security	Private	US	2023	51–200	Seed	NA	USD 10 million
Prophet Security	Computer and Network Security	Private	US	2023	51–200	Series A	NA	USD 41 million

JULY 2026 © MarketsandMarkets™

Legion Security	Technology, Information and Internet	Private	US	2024	51–200	Series A	NA	USD 38 million
CyberSilo	Computer and Network Security	Private	US	2022	11–50	NA	NA	NA
Bricklayer AI	Software Development	Private	US	2023	11–50	Seed	NA	USD 7.5 million
Augur	Computer and Network Security	Private	US	2014	11–50	Series A	NA	USD 5.1 million
BlinkOps	Software Development	Private	US	2021	51–200	Series B	NA	USD 100 million
Gruve	IT Services and IT Consulting	Private	US	2024	501–1,000	Series A	NA	USD 87.5 million
CyberNX	Information Technology & Services	Private	India	2019	51–200	NA	NA	NA
Anvilogic	Computer and Network Security	Private	US	2019	51–200	Series C	NA	USD 85 million
AiStrike	Computer and Network Security	Private	US	2024	11–50	Seed	NA	USD 7 million
D3 Security	Software Development	Private	Canada	2012	51–200	Seed	NA	USD 10 million
Exaforce	Computer and Network Security	Private	US	2023	51–200	Series B	USD 125 Million	USD 200 million +
RiverSafe	Computer and Network Security	Private	UK	2010	11–50	NA	NA	NA
SOC Jedi.AI	Computer and Network Security	Private	US	2024	2–10	NA	NA	NA
Vulnuris	Computer and Network Security	Private	India	2018	11–50	NA	NA	NA

Source: Press Releases and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

14.7.5.2 Competitive benchmarking of key startups/SMEs

14.7.5.2.1 Offering footprint

TABLE 429 AI SOC MARKET: OFFERING FOOTPRINT OF STARTUPS/SMES, 2025

COMPANY NAME	SOFTWARE PLATFORMS	SERVICES	OVERALL OFFERING FOOTPRINT
Lumu Technologies	Y	Y	4.00
Huntress	Y	Y	4.00
UnderDefense	Y	Y	4.00
Stellar Cyber	Y	Y	4.00
Radiant Security	Y	Y	4.00
Torq	Y	N	2.00
Intezer	Y	Y	4.00
Conifers.AI	Y	Y	4.00
Dropzone AI	Y	Y	4.00
Simbian	Y	Y	4.00
Prophet Security	Y	Y	4.00
Legion Security	Y	N	2.00
CyberSilo	Y	Y	4.00
Bricklayer AI	Y	Y	4.00
Augur	Y	Y	4.00
BlinkOps	Y	Y	4.00
Gruve	Y	Y	4.00
Swimlane	Y	Y	4.00
CyberNX	Y	Y	4.00
Anvilogic	Y	Y	4.00
AIStrike	Y	Y	4.00
D3 Security	Y	N	2.00
Exaforce	Y	Y	4.00
RiverSafe	N	Y	2.00
SOC Jedi.AI	Y	N	2.00
Vulnuris	Y	Y	4.00

Source: Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

14.7.5.2.2 Organization size footprint

TABLE 430 AI SOC MARKET: ORGANIZATION SIZE FOOTPRINT OF STARTUPS/SMES, 2025

COMPANY	LARGE ENTERPRISES	SMES	OVERALL ORGANIZATION SIZE FOOTPRINT
Lumu Technologies	Y	Y	4.00
Huntress	N	Y	2.00
UnderDefense	Y	Y	4.00
Stellar Cyber	Y	Y	4.00
Radiant Security	Y	Y	4.00
Torq	Y	Y	4.00
Intezer	Y	Y	4.00
Conifers.AI	Y	N	2.00
Dropzone AI	Y	Y	4.00
Simbian	Y	Y	4.00
Prophet Security	Y	Y	4.00
Legion Security	Y	N	2.00
CyberSilo	Y	Y	4.00
Bricklayer AI	Y	Y	4.00
Augur	Y	Y	4.00
BlinkOps	Y	Y	4.00
Gruve	Y	Y	4.00
Swimlane	Y	Y	4.00
CyberNX	Y	Y	4.00
Anvilogic	Y	Y	4.00
AIStrike	Y	Y	4.00
D3 Security	Y	Y	4.00
Exaforce	Y	Y	4.00
RiverSafe	Y	Y	4.00
SOC Jedi.AI	Y	Y	4.00
Vulnuris	Y	Y	4.00

Source: Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

14.7.5.2.3 Vertical footprint

TABLE 431 AI SOC MARKET: VERTICAL FOOTPRINT OF STARTUPS/SMES, 2025

COMPANY	BFSI	GOVERNMENT AND DEFENSE	GOVERNMENT AND DEFENSE	IT & TELECOMMUNICATIONS	MANUFACTURING	RETAIL & ECOMMERCE	ENERGY & UTILITIES	MEDIA & ENTERTAINMENT	EDUCATION	OTHER VERTICALS	OVERALL VERTICAL FOOTPRINT
Lumu Technologies	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
Huntress	Y	Y	Y	N	Y	Y	Y	N	Y	N	2.80
UnderDefense	Y	N	Y	Y	N	N	N	N	N	N	1.20
Stellar Cyber	Y	Y	N	N	Y	N	N	N	Y	N	1.60
Radiant Security	Y	N	Y	N	Y	N	N	N	N	N	1.20
Torq	Y	N	N	Y	N	Y	N	N	N	N	1.20
Intezer	Y	N	N	Y	Y	N	N	N	N	N	1.20
Conifers.AI	Y	N	N	Y	N	N	N	N	N	Y	1.20
Dropzone AI	Y	Y	N	Y	Y	N	Y	Y	N	Y	2.80
Simbian	Y	N	N	Y	N	N	N	N	N	N	0.80
Prophet Security	Y	N	N	Y	N	N	N	N	N	Y	1.20
Legion Security	Y	N	N	Y	N	N	N	N	N	N	0.80
CyberSilo	Y	N	N	Y	N	N	N	N	N	N	0.80
Bricklayer AI	N	N	N	Y	N	N	N	N	N	N	0.40
Augur	Y	N	N	Y	N	N	N	N	N	N	0.80
BlinkOps	Y	Y	Y	Y	Y	Y	Y	N	Y	N	3.20
Gruve	Y	Y	Y	Y	Y	Y	Y	N	Y	N	3.20
Swimlane	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
CyberNX	Y	Y	Y	Y	Y	Y	Y	N	N	N	2.80
Anvilogic	Y	N	Y	Y	Y	N	N	N	N	N	1.60
AIStrike	N	N	N	Y	N	N	N	N	N	N	0.40
D3 Security	Y	Y	Y	N	N	N	N	N	N	N	1.20
Exaforce	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	4.00
Riversafe	Y	Y	Y	Y	Y	N	Y	N	N	N	2.40

JULY 2026 © MarketsandMarkets™

SOC Jedi.AI	N	N	N	Y	N	N	N	N	N	N	0.40
Vulnuris	Y	N	N	Y	N	N	N	N	N	N	0.80

Source: Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

14.7.5.2.4 Regional footprint

TABLE 432 AI SOC MARKET: REGIONAL FOOTPRINT OF STARTUPS/SMES, 2025

COMPANY NAME	NORTH AMERICA	EUROPE	ASIA PACIFIC	MIDDLE EAST AND AFRICA	LATIN AMERICA	OVERALL REGION FOOTPRINT
Lumu Technologies	Y	Y	N	Y	Y	3.20
Huntress	Y	Y	Y	Y	Y	4.00
UnderDefense	Y	Y	N	N	N	1.60
Stellar Cyber	Y	Y	Y	Y	Y	4.00
Radiant Security	Y	Y	N	N	Y	2.40
Torq	Y	Y	N	N	Y	2.40
Intezer	Y	Y	N	Y	N	2.40
Conifers.AI	Y	Y	Y	Y	N	3.20
Dropzone AI	Y	Y	N	Y	N	2.40
Simbian	Y	Y	Y	N	N	2.40
Prophet Security	Y	N	N	N	N	0.80
Legion Security	Y	N	N	Y	N	1.60
CyberSilo	Y	N	Y	Y	N	2.40
Bricklayer AI	Y	N	N	N	N	0.80
Augur	Y	Y	Y	Y	N	3.20
BlinkOps	Y	N	N	Y	N	1.60
Gruve	Y	N	Y	Y	N	2.40
Swimlane	Y	Y	Y	Y	Y	4.00
CyberNX	N	N	Y	Y	N	1.60
Anvilogic	Y	N	Y	N	N	1.60
AIStrike	Y	N	Y	N	N	1.60
D3 Security	Y	Y	Y	Y	Y	4.00
Exaforce	Y	Y	Y	N	N	2.40
RiverSafe	Y	Y	N	Y	N	2.40

JULY 2026 © MarketsandMarkets™

SOC Jedi.AI	Y	Y	Y	Y	Y	4.00
Vulnuris	Y	N	Y	Y	N	2.40

Source: Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

14.8 COMPETITIVE SCENARIO AND TRENDS

This section studies the growth strategies adopted by top 5 players between January 2024–July 2026. Major players are adopting strategies to increase market share, such as product/solution launches, product enhancements, partnerships, collaborations, and acquisitions.

14.8.1 PRODUCT LAUNCHES

TABLE 433 AI SOC MARKET: PRODUCT LAUNCHES, JANUARY 2024–JULY 2026

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
July 2026	Product Enhancement	Microsoft (US)	Microsoft Defender XDR (Solution)	Microsoft enhanced Defender XDR with AI agent posture risk assessment capabilities, enabling security teams to identify, prioritize, and remediate risks associated with enterprise and local AI agents through configuration, access, runtime activity, and threat intelligence analysis.
April 2026	Product Enhancement	Google (US)	Agentic SOC – Threat Hunting Agent (Solution)	Google enhanced its Agentic SOC capabilities by introducing AI-powered Threat Hunting Agent functionality, enabling autonomous discovery of emerging threats through security telemetry analysis, threat intelligence integration, and machine-scale investigation workflows.
April 2026	Product Enhancement	Google (US)	Agentic SOC – Detection Engineering Agent (Solution)	Google enhanced its Agentic SOC platform with Detection Engineering Agent capabilities that identify security coverage gaps, generate detection rules, validate detection effectiveness, and assist SOC teams in improving proactive threat detection capabilities.
March 2026	Product Enhancement	Cisco (US)	Splunk Enterprise Security (Solution)	Cisco enhanced Splunk Enterprise Security with Exposure Analytics, Detection Studio, Federated Search, and a new suite of specialized AI agents that automate detection engineering, alert triage, malware analysis, guided response, and SOC automation.

JULY 2026 © MarketsandMarkets™

March 2026	Product Launch	CrowdStrike (US)	Agentic MDR & SOC Transformation Services (Service)	CrowdStrike launched Agentic MDR and SOC Transformation Services to help organizations operationalize the Agentic SOC by combining AI agents, Falcon Complete expertise, automated investigations, machine-speed response, and modernization of SIEM, data pipelines, governance, and security workflows.
January 2026	Product Enhancement	Microsoft (US)	Microsoft Sentinel (Solution)	Microsoft enhanced Sentinel availability within the Defender portal, enabling broader adoption of unified security operations by allowing organizations to access SIEM capabilities alongside Defender XDR and AI-powered security workflows.
January 2026	Product Enhancement	Google (US)	Gemini in Google Security Operations (Solution)	Google enhanced Gemini in Security Operations by expanding assistant capabilities beyond security-specific queries, enabling broader knowledge access, coding assistance, and data analysis support directly within SOC workflows.
December 2025	Product Enhancement	Microsoft (US)	Microsoft Defender XDR (Solution)	Microsoft enhanced Security Copilot in Defender by introducing the Dynamic Threat Detection Agent, an adaptive AI capability designed to continuously analyze security signals and identify hidden threats across Defender and Sentinel environments.
November 2025	Product Launch	Google (US)	Triage and Investigation Agent (Solution)	Google launched the Triage and Investigation Agent within Security Operations, enabling autonomous alert analysis, evidence collection, investigation summaries, and threat validation to reduce analyst workload and significantly accelerate security incident investigation processes.
September 2025	Product Enhancement	Microsoft (US)	Microsoft Defender XDR (Solution)	Microsoft enhanced Defender XDR with AI-assisted investigation features, including security investigation tasks, guided workflows, and advanced analytics capabilities that help SOC teams streamline incident management and improve response efficiency.
September 2025	Product Enhancement	Cisco (US)	Splunk Enterprise Security 8.2 (Solution)	Cisco enhanced Splunk Enterprise Security by introducing Enterprise Security Premier Edition and Essentials Edition, delivering agentic AI-powered SecOps capabilities that unify threat detection, investigation, and response within an AI-native SOC platform.

JULY 2026 © MarketsandMarkets™

September 2025	Product Enhancement	Cisco (US)	Agentic AI for Splunk Security (Solution)	Cisco enhanced Splunk Security with AI-powered Triage Agent, Malware Reversal Agent, AI Playbook Authoring, Response Importer, AI-Enhanced Detection Library, and Detection SPL Generator to automate SOC investigations and response workflows.
September 2025	Product Launch	CrowdStrike (US)	Charlotte AI AgentWorks (Solution)	CrowdStrike launched Charlotte AI AgentWorks, a no-code platform that enables organizations and partners to build, orchestrate, govern, and deploy custom AI security agents, accelerating AI-native SOC transformation through secure agent orchestration and automation.
August 2025	Product Launch	CrowdStrike (US)	AI for SecOps Readiness (Service)	CrowdStrike launched AI for SecOps Readiness, a professional service that helps organizations securely operationalize AI within security operations by assessing SOC workflows, identifying automation opportunities, implementing governance, and accelerating AI-driven detection, investigation, and response capabilities.
June 2025	Product Enhancement	Microsoft (US)	Microsoft Sentinel (Solution)	Microsoft enhanced Sentinel capabilities within the unified security operations experience by improving integration with Defender XDR, enabling centralized visibility, AI-assisted analytics, threat investigation, and automated response across enterprise security environments.
April 2025	Product Enhancement	Cisco (US)	Cisco XDR (Solution)	Cisco enhanced Cisco XDR by integrating Instant Attack Verification, enabling security teams to automatically validate threats, prioritize high-risk incidents, and accelerate AI-assisted investigations and response across enterprise security environments.
April 2025	Product Enhancement	CrowdStrike (US)	Charlotte AI (Solution)	CrowdStrike enhanced Charlotte AI with AI innovations including Detection Triage, improved investigation capabilities, Falcon Fusion integration, and expanded generative AI workflows, enabling SOC analysts to automate alert prioritization, investigations, and incident response across the Falcon platform.

JULY 2026 © MarketsandMarkets™

April 2025	Product Enhancement	CrowdStrike (US)	Charlotte AI Agentic Response & Agentic Workflows (Solution)	CrowdStrike enhanced Charlotte AI by introducing Agentic Response and Agentic Workflows, enabling autonomous investigation, AI-guided reasoning, root-cause analysis, automated response orchestration, and intelligent decision-making to accelerate operations across AI-native security operations centers.
April 2025	Product Enhancement	Palo Alto Networks (US)	Cortex XSIAM 3.0 (Solution)	Palo Alto Networks enhanced Cortex XSIAM 3.0 by adding AI-driven Exposure Management, Advanced Email Security, and a unified Cloud & SOC Command Center, extending the platform from reactive incident response to proactive security operations.
April 2025	Product Launch	Google (US)	Google Security Operations Agentic SOC Platform (Solution)	Google launched its Agentic SOC platform, introducing Gemini-native AI agents that autonomously perform alert triage, threat investigation, threat hunting, and detection engineering workflows to reduce manual SOC effort and accelerate cyber incident response.
March 2025	Product Enhancement	Microsoft (US)	Microsoft Security Copilot Agents (Solution)	Microsoft enhanced Security Copilot with AI agent capabilities, introducing specialized security agents that autonomously handle high-volume SOC tasks, support incident investigation, automate workflows, and integrate with Microsoft Security solutions to improve operational efficiency.
March 2025	Product Enhancement	Microsoft (US)	Microsoft Defender XDR (Solution)	Microsoft enhanced Defender XDR with AI-powered SOC capabilities, introducing Security Copilot agents including the Phishing Triage Agent to autonomously analyze alerts, prioritize threats, reduce false positives, and improve incident investigation efficiency for security teams.
January 2025	Product Launch	Cisco (US)	AI Assistant for Security (Solution)	Cisco launched AI Assistant for Security, later integrated AI Canvas (in June 2025), enabling SOC analysts to collaborate with AI agents, investigate threats, summarize incidents, and streamline security operations through a unified AI-powered workspace.

JULY 2026 © MarketsandMarkets™

May 2024	Product Enhancement	Palo Alto Networks (US)	Cortex XSIAM (Solution)	Palo Alto Networks enhanced Cortex XSIAM with Bring Your Own ML (BYOML), third-party EDR data ingestion, expanded Cloud Detection and Response capabilities, and Precision AI-powered customization to improve autonomous security operations and detection accuracy.
May 2024	Product Enhancement	Google (US)	Google Security Operations (Solution)	Google enhanced Security Operations by introducing AI-powered SecOps capabilities with Gemini integration, enabling SOC teams to accelerate investigations, generate detection rules, analyze threats, summarize intelligence, and improve analyst productivity through generative AI assistance.
May 2024	Product Launch	Google (US)	Gemini in Google Security Operations (Solution)	Google launched Gemini in Security Operations to provide generative AI assistance for SOC analysts, enabling natural language investigations, threat intelligence analysis, search summarization, YARA-L rule generation, and automated security workflow support.
May 2024	Product Enhancement	Google (US)	Google Threat Intelligence (Solution)	Google enhanced Google Threat Intelligence by integrating Gemini capabilities with Mandiant intelligence and VirusTotal data, enabling security teams to accelerate threat research, analyze adversary behavior, summarize intelligence, and improve proactive threat detection
April 2024	Product Launch	Microsoft (US)	Microsoft Copilot for Security (Solution)	Microsoft launched Copilot for Security, a generative AI-powered security solution that assists SOC analysts with incident investigation, threat hunting, response recommendations, and security intelligence analysis to accelerate cybersecurity operations and improve analyst productivity.
April 2024	Product Enhancement	Palo Alto Networks (US)	Cortex XSIAM for Cloud (Solution)	Palo Alto Networks enhanced Cortex XSIAM by introducing Cloud Detection and Response (CDR), Cloud Command Center, and unified cloud-native SOC capabilities, enabling AI-driven threat detection, investigation, and remediation across enterprise and multi-cloud environments.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

14.8.2 DEALS

TABLE 434 AI SOC MARKET: DEALS, JANUARY 2024–JULY 2026

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION	DEAL SIZE
June 2026	Acquisition	Cisco (US)	WideField Security (US)	Cisco announced the acquisition of WideField Security to strengthen Splunk's Agentic SOC capabilities by enriching identity intelligence, correlating AI-agent activity, and improving autonomous threat detection and investigation across enterprise environments.	NA
June 2026	Partnership	Palo Alto Networks (US)	Wipro (India)	Palo Alto Networks partnered with Wipro to combine Cortex XSIAM with Wipro CyberShield, delivering AI-powered managed security operations, automated threat detection, and machine-learning-driven SOC services for enterprise customers worldwide.	NA
May 2026	Collaboration	Google (US)	Information Services (Bulgaria)	Google collaborated with Information Services to launch Bulgaria's AI-powered National Cybershield, deploying Google Security Operations, Google Threat Intelligence, and Mandiant intelligence to establish a federated SOC that strengthens AI-driven threat detection and incident response across 54 government entities.	NA
April 2026	Partnership	Google (US)	Tata Consultancy Services (TCS) (India)	Google partnered with Tata Consultancy Services (TCS) to expand their strategic collaboration by launching TCS AI SOC enabled by Google SecOps, combining Google SecOps, Gemini, and Google Threat Intelligence to deliver AI-driven threat detection, autonomous investigations, and faster incident response.	NA
March 2026	Integration	Microsoft (US)	Commvault (US)	Microsoft integrated Commvault Cloud with Microsoft Sentinel and Security Copilot, enabling AI-driven threat detection, investigation, and automated recovery workflows by combining security telemetry, backup intelligence, and SOC operations capabilities.	NA

JULY 2026 © MarketsandMarkets™

March 2026	Collaboration	CrowdStrike (US)	Accenture (Ireland), Amazon Web Services (US), Anthropic (US), Deloitte (UK), Kroll (US), NVIDIA (US), OpenAI (US), Salesforce (US), Telefónica Tech (Spain)	CrowdStrike collaborated with Accenture, AWS, Anthropic, Deloitte, Kroll, NVIDIA, OpenAI, Salesforce, and Telefónica Tech to launch the Charlotte AI AgentWorks Ecosystem, enabling organizations to build, orchestrate, govern, and scale secure AI agents that accelerate agentic SOC transformation and AI-native security operations.	NA
March 2026	Partnership	CrowdStrike (US)	IBM (US)	CrowdStrike partnered with IBM to integrate Charlotte AI with IBM's Autonomous Threat Operations Machine (ATOM), combining AI-driven investigation, coordinated machine-speed response, managed Threat Detection and Response services, and Cyber Range validation to accelerate enterprise Agentic SOC transformation.	NA
March 2026	Partnership	CrowdStrike (US)	Ernst & Young (EY) (UK)	EY selected the CrowdStrike Falcon platform to power its Agentic Security Operations Center (SOC) services, leveraging NVIDIA AI infrastructure and NVIDIA AI Enterprise software to deliver AI-driven threat detection, investigation, and autonomous security operations for enterprise customers.	NA
March 2026	Acquisition	Google (US)	Wiz (US)	Google completed its acquisition of Wiz, integrating its cloud and AI security platform with Google Security Operations and Google Threat Intelligence to enhance AI-powered threat prevention, detection, investigation, and response across hybrid and multicloud environments.	USD 32 billion

JULY 2026 © MarketsandMarkets™

March 2026	Collaboration	Google (US)	SentinelOne (US)	Google collaborated with SentinelOne through a multi-year strategic agreement to deliver autonomous AI-powered security by integrating Google Security Operations, Google Threat Intelligence, and Google Cloud infrastructure with SentinelOne's AI-native security platform, strengthening enterprise threat detection and incident response.	NA
February 2026	Acquisition	Palo Alto Networks (US)	CyberArk (Israel)	Palo Alto Networks completed the acquisition of CyberArk, integrating privileged access management and identity security into its AI-driven cybersecurity platform to secure human and machine identities within autonomous security operations and AI-enabled enterprise environments.	NA
January 2026	Collaboration	Google (US)	PwC (US)	Google collaborated with PwC through a three-year strategic alliance to modernize AI-powered security operations by combining Google Security Operations, Google Threat Intelligence, and agentic AI capabilities with PwC's managed security services to accelerate threat detection, investigation, and response.	USD 400 million
December 2025	Partnership	Google (US)	Deloitte India (India)	Google partnered with Deloitte India to deliver AI-powered security operations by combining Google Security Operations, Google Threat Intelligence, and Google Cloud Cybershield with Deloitte's managed security services to modernize SOCs, strengthen threat detection, and accelerate AI-driven incident response.	NA
November 2025	Integration	Microsoft (US)	Illumio (US)	Microsoft integrated Illumio's AI-powered breach containment capabilities with Microsoft Sentinel and Security Copilot, enabling SOC teams to correlate security telemetry, analyze attack paths, detect lateral movement risks, and accelerate AI-driven threat investigation and containment workflows.	NA

JULY 2026 © MarketsandMarkets™

November 2025	Partnership	Microsoft (US)	Rapid7 (US)	Microsoft partnered with Rapid7 to advance modern detection and response capabilities by integrating Rapid7's AI-native security operations platform and MDR expertise with Microsoft Defender, enabling 24/7 threat monitoring, investigation, and automated response workflows.	NA
October 2025	Collaboration	Microsoft (US)	Charoen Pokphand Group (CP Group) (Thailand); True Corporation (Thailand); True Internet Data Center (True IDC) (Thailand)	Microsoft collaborated with CP Group, True, and True IDC to accelerate Thailand's AI and cloud ecosystem, including exploration of an AI-powered Cloud Security Operations Center (SOC) for real-time threat detection, predictive analytics, and automated incident response.	NA
August 2025	Partnership	Cisco (US)	Indosat Ooredoo Hutchison (Indonesia)	Cisco partnered with Indosat Ooredoo Hutchison to launch Indonesia's Sovereign Security Operations Centre, combining Splunk Enterprise Security, AI-powered threat detection, real-time security monitoring, and localized data residency to strengthen AI-driven security operations and cyber resilience.	NA
August 2025	Partnership	CrowdStrike (US)	Zscaler (US)	CrowdStrike partnered with Zscaler to expand AI-driven security operations by integrating the Falcon platform with Zscaler Zero Trust Exchange and Red Canary's agentic AI-driven MDR capabilities, enabling unified visibility, accelerated threat detection, automated response, and modernized enterprise SOC operations.	NA
August 2025	Acquisition	CrowdStrike (US)	Onum (Spain)	CrowdStrike acquired Onum, a real-time security data pipeline company, to strengthen Falcon Next-Gen SIEM with intelligent telemetry management, high-fidelity data processing, and AI-ready security data that improves agentic detection, investigation, and autonomous SOC operations.	USD 290 million

JULY 2026 © MarketsandMarkets™

July 2025	Collaboration	Microsoft (US)	Accenture (Ireland)	Microsoft collaborated with Accenture to develop generative AI-powered cybersecurity solutions focused on SOC modernization, leveraging Microsoft Sentinel, Defender, Security Copilot, and Accenture's cybersecurity expertise to enhance threat detection, investigation, and automated response capabilities.	NA
July 2025	Acquisition	Palo Alto Networks (US)	Protect AI (US)	Palo Alto Networks acquired Protect AI to strengthen AI security capabilities across the software development lifecycle, expanding protection for AI models, applications, and agentic AI environments while complementing its Cortex AI-driven security operations portfolio.	NA
March 2025	Collaboration	Microsoft (US)	OneTrust (US); Aviatrix (US); BlueVoyant (US); Tanium (US); Fletch (US)	Microsoft collaborated with cybersecurity partners to expand Security Copilot AI agent capabilities, enabling automated privacy breach response, SOC optimization, alert triage, network analysis, and threat prioritization workflows for improved AI-driven security operations.	NA
October 2024	Partnership	CrowdStrike (US)	Fortinet (US)	CrowdStrike partnered with Fortinet to integrate the Falcon platform with FortiGate Next-Generation Firewalls, enabling unified AI-powered endpoint and network visibility, accelerated threat detection, automated investigations, and faster SOC response across enterprise environments.	NA
September 2024	Acquisition	Palo Alto Networks (US)	IBM (US)	Palo Alto Networks completed the acquisition of IBM's QRadar Software-as-a-Service (SaaS) assets, strengthening its AI-powered security operations portfolio by accelerating customer migration to Cortex XSIAM and expanding autonomous SOC capabilities through Precision AI and automation.	Approximately USD 500 million

JULY 2026 © MarketsandMarkets™

July 2024	Partnership	Google (US)	PwC India (India)	Google partnered with PwC India to deliver Google Security Operations, an AI-powered SecOps platform, combining Gemini, Google Threat Intelligence, and PwC India's managed security expertise to accelerate threat detection, investigation, and incident response for organizations across India.	NA
June 2024	Partnership	Google (US)	Thales (France)	Google partnered with Thales to develop a global Security Operations Center (SOC) platform combining Google Security Operations, Google Threat Intelligence, VirusTotal, Mandiant intelligence, and generative AI capabilities to strengthen AI-driven cyber detection, investigation, and incident response services.	NA
May 2024	Collaboration	Microsoft (US)	ServiceNow (US)	Microsoft collaborated with ServiceNow to integrate Security Copilot capabilities with ServiceNow workflows, enabling security teams to combine generative AI assistance, incident management, and automated response processes for improved SOC efficiency and faster threat resolution.	NA
May 2024	Collaboration	Microsoft (US)	Jamf (US)	Microsoft collaborated with Jamf to integrate Security Copilot capabilities with third-party security ecosystems, enabling SOC teams to leverage AI-assisted investigation and response workflows across diverse endpoint and device management environments.	NA
May 2024	Partnership	Palo Alto Networks (US)	IBM (US)	Palo Alto Networks partnered with IBM to deliver AI-powered security operations by combining Cortex XSIAM with IBM Consulting services and watsonx capabilities, while enabling migration of IBM QRadar SaaS customers to an AI-native SOC platform.	NA

JULY 2026 © MarketsandMarkets™

April 2024	Partnership	Palo Alto Networks (US)	Google Cloud (US)	Palo Alto Networks partnered with Google Cloud to expand AI-powered cybersecurity by integrating Cortex and Prisma Cloud with Google Cloud services, helping enterprises strengthen cloud security, threat detection, and AI-driven SOC operations.	NA
April 2024	Partnership	Google (US)	Palo Alto Networks (US)	Google partnered with Palo Alto Networks to expand their strategic alliance by integrating Google Cloud AI, Google Security Operations, and Google Threat Intelligence with Palo Alto Networks' AI-powered security platforms, enabling enhanced threat detection, automated security operations, and protection for AI applications.	NA
March 2024	Acquisition	Cisco (US)	Splunk (US)	Cisco completed the acquisition of Splunk to combine Cisco's security portfolio with Splunk's SIEM, SOAR, and observability capabilities, creating an AI-powered security operations platform that accelerates threat detection, investigation, and autonomous SOC operations.	USD 28 million

Source: Company Website and Press Releases

14.8.3 EXPANSIONS

TABLE 435 AI SOC MARKET: EXPANSIONS, JANUARY 2024–JULY 2026

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY	COMPANY	DESCRIPTION
June 2026	Expansion	Regional AI SOC Expansion (Sovereign Security Platform)	Europe	Palo Alto Networks (US)	Palo Alto Networks expanded its AI-driven security operations footprint across Europe by introducing Sovereign Cortex with T Security in collaboration with Deutsche Telekom, enabling regulated organizations to adopt Cortex AI-powered SecOps while meeting European data sovereignty and compliance requirements.

JULY 2026 © MarketsandMarkets™

June 2026	Expansion	Regional Expansion	South Korea	Google (US)	Google strengthened its regional AI security operations capabilities by introducing Google Security Operations in the Seoul Region, enabling local data residency and providing AI-driven threat detection, automated response workflows, and Google Threat Intelligence for regulated industries.
January 2026	Expansion	Regional Cloud Expansion (Data Sovereignty)	Saudi Arabia, India & United Arab Emirates	CrowdStrike (US)	CrowdStrike expanded its Global Data Sovereignty initiative by launching new in-country regional cloud deployments in Saudi Arabia, India, and the UAE. The expansion enables organizations to deploy the Falcon platform with local data residency while retaining access to CrowdStrike's global threat intelligence, AI-powered security operations, and Falcon Next-Gen SIEM capabilities, supporting AI-native SOC adoption in regulated industries.
July 2024	Expansion	Regional Cloud Infrastructure Expansion	Indonesia	Palo Alto Networks (US)	Palo Alto Networks expanded its regional cloud infrastructure by launching a new cloud location in Indonesia, enabling Cortex XSIAM, Cortex XSOAR, and Cortex XDR customers to meet local data residency requirements while delivering AI-powered security operations and automated threat response capabilities.
May 2024	Expansion	Regional Expansion	India	Google (US)	Google expanded its AI-powered Security Operations footprint by launching a dedicated Google Security Operations region in Mumbai, enabling organizations to store SecOps data locally while leveraging Gemini-powered investigations, AI-driven threat detection, Google Threat Intelligence, and automated incident response capabilities.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15 COMPANY PROFILES

15.1 KEY PLAYERS

15.1.1 MICROSOFT

15.1.1.1 Business overview

Microsoft Corporation is one of the world's leading technology companies, providing a broad portfolio of cloud computing, artificial intelligence (AI), cybersecurity, productivity, and enterprise software solutions. Through Microsoft Azure and its security ecosystem, the company enables organizations, governments, and enterprises to modernize digital operations, protect critical assets, and improve operational efficiency. Microsoft offers cybersecurity capabilities spanning threat intelligence, identity protection, endpoint security, cloud security, security information and event management (SIEM), extended detection and response (XDR), and AI-powered security operations.

In the AI SOC market, Microsoft provides an integrated AI-driven security operations ecosystem through Microsoft Security Copilot, Microsoft Defender XDR, Microsoft Sentinel, and the AI-powered Unified SecOps Platform. Security Copilot leverages generative AI to assist SOC analysts with incident investigation, threat hunting, intelligence analysis, security posture management, and automated response workflows. Microsoft Sentinel provides an AI-ready cloud-native SIEM platform with capabilities for threat detection, investigation, proactive hunting, and automated response across multi-cloud and multi-platform environments, while Defender XDR delivers unified visibility and response across endpoints, identities, email, applications, and cloud workloads.

Microsoft serves customers across diverse industries, including banking, financial services and insurance (BFSI), government and defense, healthcare and life sciences, IT and telecommunications, manufacturing, retail and e-commerce, energy and utilities, education, and media and entertainment. The company has established a strong global presence through its cloud infrastructure, cybersecurity partner ecosystem, and enterprise technology footprint, enabling organizations worldwide to adopt AI-powered security operations capabilities.

Microsoft continues to strengthen its AI SOC ecosystem through advancements in agentic AI, autonomous security operations, and AI-powered threat response. The company has expanded Security Copilot with AI agents that automate SOC workflows, including alert triage, threat investigation, vulnerability prioritization, and incident response. By integrating AI capabilities across Defender XDR and Sentinel, Microsoft delivers a unified security operations platform combining SIEM, XDR, threat intelligence, automation, and generative AI. These capabilities, along with extensive ecosystem integrations, enable organizations to improve detection accuracy, reduce analyst workload, and accelerate the transition toward autonomous and AI-native SOC environments.

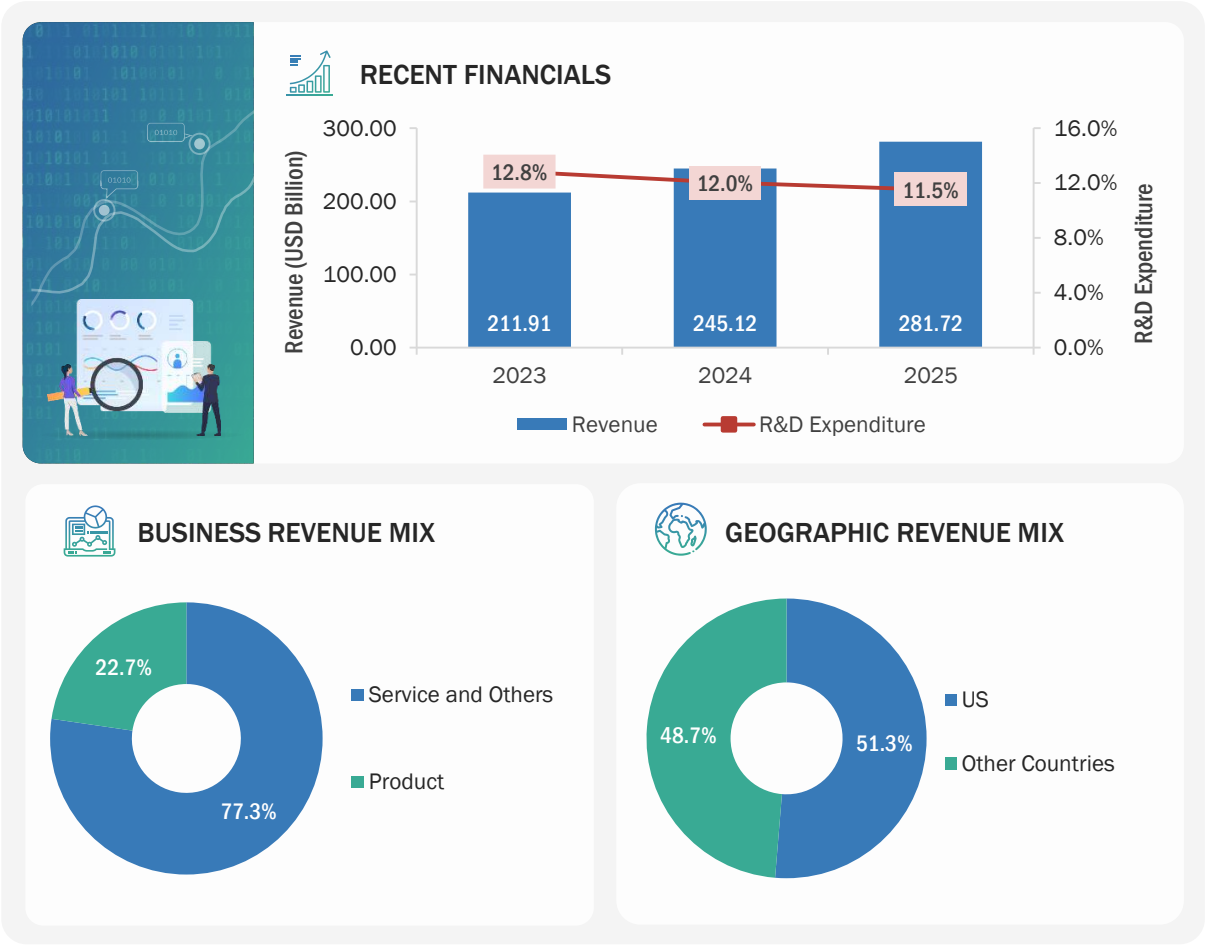
TABLE 436 MICROSOFT: COMPANY OVERVIEW

Founding Year	1975
Headquarters Country	US
Headquarters City/State	Redmond, Washington
Ownership Type	Public (NASDAQ: MSFT)

Source: Company Website, Annual Reports, and SEC Filings

JULY 2026 © MarketsandMarkets™

FIGURE 49 MICROSOFT: COMPANY SNAPSHOT



Source: Company Website and Annual Reports.

15.1.1.2 Products/Solutions/Services offered

TABLE 437 MICROSOFT: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/SERVICE	DESCRIPTION	VERTICAL
Solution	AI-Powered Unified SecOps Platform	Microsoft's AI-powered Unified SecOps Platform integrates prevention, detection, investigation, and response capabilities into a centralized security operations environment, combining AI, threat intelligence, XDR, SIEM, and automation to improve SOC efficiency and cyber resilience.	▪ Education ▪ Financial services ▪ Healthcare & life sciences ▪ Manufacturing ▪ Retail & e-commerce ▪ Energy and utilities ▪ Government ▪ IT and telecommunications ▪ Media and entertainment

JULY 2026 © MarketsandMarkets™

Solution	Microsoft Security Copilot	Microsoft Security Copilot is a generative AI-powered security assistant that enables SOC analysts to investigate incidents, perform threat hunting, analyze security risks, generate insights, and accelerate response workflows using natural language-based AI capabilities.	▪ Education ▪ Financial services ▪ Healthcare & life sciences ▪ Manufacturing ▪ Retail & e-commerce ▪ Energy and utilities ▪ Government ▪ IT and telecommunications ▪ Media and entertainment
Solution	Microsoft Defender XDR	Microsoft Defender XDR provides AI-driven extended detection and response capabilities by correlating signals across endpoints, identities, email, applications, and cloud environments to automatically detect, disrupt, investigate, and respond to sophisticated cyber threats.	▪ Education ▪ Financial services ▪ Healthcare & life sciences ▪ Manufacturing ▪ Retail & e-commerce ▪ Energy and utilities ▪ Government ▪ IT and telecommunications ▪ Media and entertainment
Solution	Microsoft Sentinel	Microsoft Sentinel is a cloud-native SIEM platform that leverages AI, analytics, automation, and threat intelligence to provide centralized security monitoring, intelligent threat detection, incident investigation, and automated response across enterprise digital environments.	▪ Education ▪ Financial services ▪ Healthcare & life sciences ▪ Manufacturing ▪ Retail & e-commerce ▪ Energy and utilities ▪ Government ▪ IT and telecommunications ▪ Media and entertainment
Solution	Microsoft Security Exposure Management	Microsoft Security Exposure Management uses AI-powered risk analysis and exposure management capabilities to identify attack paths, prioritize vulnerabilities, assess security posture, and help organizations proactively reduce cyber risks across hybrid environments.	▪ Education ▪ Financial services ▪ Healthcare & life sciences ▪ Manufacturing ▪ Retail & e-commerce ▪ Energy and utilities ▪ Government ▪ IT and telecommunications ▪ Media and entertainment

JULY 2026 © MarketsandMarkets™

Solution	Microsoft Defender for Cloud	Microsoft Defender for Cloud delivers AI-enabled cloud security capabilities by continuously monitoring cloud workloads, identifying threats, managing security posture, and protecting applications across multi-cloud and hybrid environments through integrated security controls.	▪ Education ▪ Financial services ▪ Healthcare & life sciences ▪ Manufacturing ▪ Retail & e-commerce ▪ Energy and utilities ▪ Government ▪ IT and telecommunications ▪ Media and entertainment
Solution	Microsoft Defender Experts for XDR	Microsoft Defender Experts for XDR is a managed security service that augments SOC teams with Microsoft security expertise, threat hunting, investigation support, and response assistance to improve detection accuracy and accelerate incident resolution.	▪ Education ▪ Financial services ▪ Healthcare & life sciences ▪ Manufacturing ▪ Retail & e-commerce ▪ Energy and utilities ▪ Government ▪ IT and telecommunications ▪ Media and entertainment

Source: Company Website

15.1.1.3 Recent developments

15.1.1.3.1 Product launches/enhancements

TABLE 438 MICROSOFT: PRODUCT LAUNCHES/ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
July 2026	Product Enhancement	Microsoft (US)	Microsoft Defender XDR (Solution)	Microsoft enhanced Defender XDR with AI agent posture risk assessment capabilities, enabling security teams to identify, prioritize, and remediate risks associated with enterprise and local AI agents through configuration, access, runtime activity, and threat intelligence analysis.
January 2026	Product Enhancement	Microsoft (US)	Microsoft Sentinel (Solution)	Microsoft enhanced Sentinel availability within the Defender portal, enabling broader adoption of unified security operations by allowing organizations to access SIEM capabilities alongside Defender XDR and AI-powered security workflows.

JULY 2026 © MarketsandMarkets™

December 2025	Product Enhancement	Microsoft (US)	Microsoft Defender XDR (Solution)	Microsoft enhanced Security Copilot in Defender by introducing the Dynamic Threat Detection Agent, an adaptive AI capability designed to continuously analyze security signals and identify hidden threats across Defender and Sentinel environments.
September 2025	Product Enhancement	Microsoft (US)	Microsoft Defender XDR (Solution)	Microsoft enhanced Defender XDR with AI-assisted investigation features, including security investigation tasks, guided workflows, and advanced analytics capabilities that help SOC teams streamline incident management and improve response efficiency.
June 2025	Product Enhancement	Microsoft (US)	Microsoft Sentinel (Solution)	Microsoft enhanced Sentinel capabilities within the unified security operations experience by improving integration with Defender XDR, enabling centralized visibility, AI-assisted analytics, threat investigation, and automated response across enterprise security environments.
March 2025	Product Enhancement	Microsoft (US)	Microsoft Security Copilot Agents (Solution)	Microsoft enhanced Security Copilot with AI agent capabilities, introducing specialized security agents that autonomously handle high-volume SOC tasks, support incident investigation, automate workflows, and integrate with Microsoft Security solutions to improve operational efficiency.
March 2025	Product Enhancement	Microsoft (US)	Microsoft Defender XDR (Solution)	Microsoft enhanced Defender XDR with AI-powered SOC capabilities, introducing Security Copilot agents including the Phishing Triage Agent to autonomously analyze alerts, prioritize threats, reduce false positives, and improve incident investigation efficiency for security teams.
April 2024	Product Launch	Microsoft (US)	Microsoft Copilot for Security (Solution)	Microsoft launched Copilot for Security, a generative AI-powered security solution that assists SOC analysts with incident investigation, threat hunting, response recommendations, and security intelligence analysis to accelerate cybersecurity operations and improve analyst productivity.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.1.3.2 Deals

TABLE 439 MICROSOFT: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
March 2026	Integration	Microsoft (US)	Commvault (US)	Microsoft integrated Commvault Cloud with Microsoft Sentinel and Security Copilot, enabling AI-driven threat detection, investigation, and automated recovery workflows by combining security telemetry, backup intelligence, and SOC operations capabilities.
November 2025	Integration	Microsoft (US)	Illumio (US)	Microsoft integrated Illumio's AI-powered breach containment capabilities with Microsoft Sentinel and Security Copilot, enabling SOC teams to correlate security telemetry, analyze attack paths, detect lateral movement risks, and accelerate AI-driven threat investigation and containment workflows.
November 2025	Partnership	Microsoft (US)	Rapid7 (US)	Microsoft partnered with Rapid7 to advance modern detection and response capabilities by integrating Rapid7's AI-native security operations platform and MDR expertise with Microsoft Defender, enabling 24/7 threat monitoring, investigation, and automated response workflows.
October 2025	Collaboration	Microsoft (US)	Charoen Pokphand Group (CP Group) (Thailand); True Corporation (Thailand); True Internet Data Center (True IDC) (Thailand)	Microsoft collaborated with CP Group, True, and True IDC to accelerate Thailand's AI and cloud ecosystem, including exploration of an AI-powered Cloud Security Operations Center (SOC) for real-time threat detection, predictive analytics, and automated incident response.
July 2025	Collaboration	Microsoft (US)	Accenture (Ireland)	Microsoft collaborated with Accenture to develop generative AI-powered cybersecurity solutions focused on SOC modernization, leveraging Microsoft Sentinel, Defender, Security Copilot, and Accenture's cybersecurity expertise to enhance threat detection, investigation, and automated response capabilities.

JULY 2026 © MarketsandMarkets™

March 2025	Collaboration	Microsoft (US)	OneTrust (US); Aviatrix (US); BlueVoyant (US); Tanium (US); Fletch (US)	Microsoft collaborated with cybersecurity partners to expand Security Copilot AI agent capabilities, enabling automated privacy breach response, SOC optimization, alert triage, network analysis, and threat prioritization workflows for improved AI-driven security operations.
May 2024	Collaboration	Microsoft (US)	ServiceNow (US)	Microsoft collaborated with ServiceNow to integrate Security Copilot capabilities with ServiceNow workflows, enabling security teams to combine generative AI assistance, incident management, and automated response processes for improved SOC efficiency and faster threat resolution.
May 2024	Collaboration	Microsoft (US)	Jamf (US)	Microsoft collaborated with Jamf to integrate Security Copilot capabilities with third-party security ecosystems, enabling SOC teams to leverage AI-assisted investigation and response workflows across diverse endpoint and device management environments.

Source: Company Website and Press Releases

15.1.1.4 MnM view

15.1.1.4.1 Key strengths

Microsoft maintains a strong position in the global AI SOC market through its integrated security ecosystem, combining AI-powered Security Copilot, Microsoft Sentinel, Microsoft Defender XDR, threat intelligence, and automation capabilities. The company's AI-powered Unified SecOps Platform enables organizations to consolidate prevention, detection, investigation, and response workflows into a unified security operations environment. Microsoft Security Copilot strengthens SOC analyst productivity by providing generative AI-powered incident summaries, threat investigation guidance, natural language queries, and automated security insights, while Defender XDR and Sentinel provide cross-domain visibility across endpoints, identities, cloud workloads, applications, and networks.

Microsoft further differentiates its AI SOC capabilities through extensive security telemetry, global cloud infrastructure, threat intelligence capabilities, and deep integration across its security portfolio. The company's embedded AI agents enable SOC teams to automate repetitive security tasks, perform continuous threat hunting, prioritize alerts, and orchestrate response actions at machine speed. Additionally, Microsoft's broad enterprise customer base, partner ecosystem, and managed security capabilities through Defender Experts for XDR strengthen its ability to support organizations across BFSI, government, healthcare, telecommunications, manufacturing, and other industries.

JULY 2026 © MarketsandMarkets™

15.1.1.4.2 Strategic choices

Microsoft continues to focus on transforming traditional security operations into AI-native SOC environments by embedding generative AI, autonomous agents, and automation across its security portfolio. Rather than offering standalone AI security tools, Microsoft is strategically integrating AI capabilities into existing SOC platforms such as Microsoft Sentinel and Defender XDR, enabling unified security operations with centralized data visibility, intelligent detection, automated investigation, and accelerated incident response.

The company is increasingly emphasizing agentic AI capabilities to automate complex SOC workflows, including threat investigation, alert triage, security posture assessment, and response orchestration. Through Security Copilot and AI-powered security agents, Microsoft aims to reduce analyst workload, address cybersecurity talent shortages, and enable organizations to operate security teams more efficiently. Furthermore, Microsoft is expanding its AI SOC ecosystem through third-party integrations, partner-developed Security Copilot agents, and interoperability with security platforms such as ServiceNow and Jamf, strengthening its position as an AI-driven security operations platform provider.

15.1.1.4.3 Weaknesses & competitive threats

Microsoft faces increasing competition in the AI SOC market from established cybersecurity vendors such as Palo Alto Networks, CrowdStrike, Google Cloud, IBM, and Cisco, which are also accelerating investments in AI-powered detection, autonomous response, and security operations platforms. While Microsoft benefits from its broad security ecosystem and cloud advantage, its AI SOC strategy is closely tied to the adoption of Microsoft security products, creating potential challenges among organizations operating heterogeneous multi-vendor security environments.

The company also faces challenges related to trust, governance, and security risks associated with autonomous AI capabilities. As enterprises increasingly deploy AI agents within SOC workflows, concerns around AI decision accuracy, explainability, data privacy, regulatory compliance, and potential adversarial manipulation may influence adoption. Additionally, rapid innovation from specialized AI security vendors and emerging agentic SOC platforms could intensify competitive pressure, requiring Microsoft to continuously enhance AI model reliability, threat intelligence capabilities, and security automation features.

JULY 2026 © MarketsandMarkets™

15.1.2 CISCO

15.1.2.1 Business overview

Cisco is transforming from a networking leader into a data-driven cybersecurity and AI company, leveraging its expertise in secure networking, threat intelligence, software, and observability to redefine enterprise security operations. The acquisition of Splunk significantly strengthened this transformation by expanding Cisco's capabilities in security analytics, SIEM, SOAR, and observability, enabling the company to unify network intelligence with AI-powered threat detection, investigation, and response across hybrid and multi-cloud environments. This strategic integration positions Cisco to deliver data-driven cyber resilience by correlating telemetry across networks, endpoints, cloud workloads, identities, applications, and security tools through a unified security platform. Complementing these capabilities, Cisco's cybersecurity portfolio encompasses Cisco Talos, Cisco XDR, Zero Trust, cloud security, AI-powered security operations, Security Cloud Control, and managed security services, helping enterprises strengthen cyber resilience against increasingly sophisticated and distributed cyber threats.

Building on this integrated cybersecurity foundation, Cisco is reshaping modern security operations through its Agentic SOC vision. The company's AI SOC portfolio combines Cisco XDR, Splunk Enterprise Security, Splunk SOAR, AI Assistant for Security, AI Canvas, and Cisco Talos into a unified security operations ecosystem designed to streamline the entire threat lifecycle. Rather than limiting AI to analyst assistance, Cisco embeds specialized AI agents across investigation, alert validation, detection engineering, malware analysis, and incident response workflows, enabling higher levels of automation and operational consistency. By combining Cisco Talos' global threat intelligence with Splunk's advanced security analytics and automation platform, the company helps organizations convert massive volumes of security telemetry into actionable intelligence, improve analyst productivity, and accelerate response across increasingly complex hybrid and multi-cloud environments.

Cisco supports customers across BFSI, government and public sector, healthcare, manufacturing, telecommunications, retail, energy and utilities, education, and other critical infrastructure industries. Through its global presence spanning North America, Europe, Asia Pacific, Latin America, and the Middle East & Africa, together with an extensive channel ecosystem, managed security capabilities, and Cisco Talos research organization, the company enables enterprises worldwide to modernize security operations while protecting hybrid, multi-cloud, and AI-driven environments.

Cisco's recent cybersecurity strategy reflects a shift from delivering individual security products to building a unified AI-native security platform. The integration of Splunk has expanded the company's security analytics and automation capabilities, while continuous investments in agentic AI, AI Assistant for Security, AI Canvas, Security Cloud Control, and AI-driven SOC workflows reinforce its long-term vision for autonomous security operations. By combining network intelligence, observability, AI-powered automation, and one of the industry's largest commercial threat intelligence organizations, Cisco is strengthening its position as a provider of next-generation AI-driven security operations platforms.

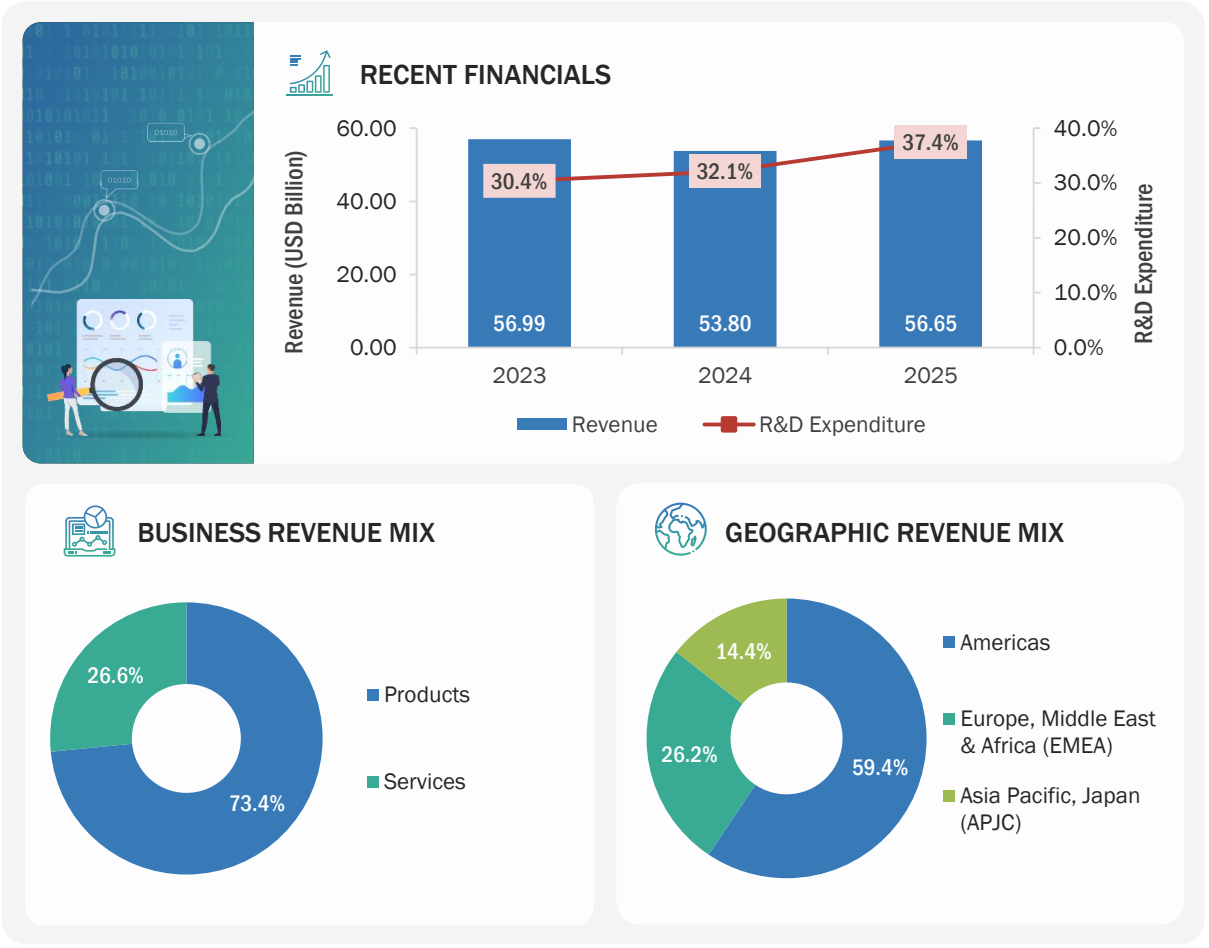
TABLE 440 CISCO: COMPANY OVERVIEW

Founding Year	1984
Headquarters Country	US
Headquarters City/State	San Jose, California
Ownership Type	Public (NASDAQ: CSCO)

Source: Company Website, Annual Reports, and SEC Filings

JULY 2026 © MarketsandMarkets™

FIGURE 50 CISCO: COMPANY SNAPSHOT



Source: Company Website and Annual Reports.

15.1.2.2 Products/Solutions/Services offered

TABLE 441 CISCO: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/SERVICE	DESCRIPTION	VERTICAL
Solution	Cisco XDR	Cisco XDR is an AI-powered extended detection and response platform that correlates telemetry across endpoints, networks, cloud, identities, email, and third-party tools to automate threat detection, investigation, prioritization, and incident response across modern SOC environments.	▪ Cities and communities ▪ Education ▪ Financial services ▪ Government ▪ Healthcare ▪ Manufacturing ▪ Mining ▪ Oil and gas ▪ Retail ▪ Smart buildings ▪ Sports, media, and entertainment ▪ Transportation ▪ Utilities

JULY 2026 © MarketsandMarkets™

Solution	Splunk Enterprise Security	Splunk Enterprise Security provides an AI-enhanced SIEM platform that combines security analytics, risk-based alerting, correlation searches, threat intelligence, and automation to help SOC teams detect, investigate, and respond to cyber threats more efficiently.	▪ Cities and communities ▪ Education ▪ Financial services ▪ Government ▪ Healthcare ▪ Manufacturing ▪ Mining ▪ Oil and gas ▪ Retail ▪ Smart buildings ▪ Sports, media, and entertainment ▪ Transportation ▪ Utilities
Solution	Splunk SOAR	Splunk SOAR automates security operations by orchestrating incident response workflows, case management, threat intelligence enrichment, and remediation across multi-vendor security environments, enabling faster and more consistent SOC operations.	▪ Cities and communities ▪ Education ▪ Financial services ▪ Government ▪ Healthcare ▪ Manufacturing ▪ Mining ▪ Oil and gas ▪ Retail ▪ Smart buildings ▪ Sports, media, and entertainment ▪ Transportation ▪ Utilities
Solution	Cisco AI Assistant for Security	Cisco AI Assistant for Security leverages generative AI to assist SOC analysts with alert investigation, incident summarization, threat analysis, remediation guidance, and natural language interactions, improving analyst productivity and accelerating security operations.	▪ Cities and communities ▪ Education ▪ Financial services ▪ Government ▪ Healthcare ▪ Manufacturing ▪ Mining ▪ Oil and gas ▪ Retail ▪ Smart buildings ▪ Sports, media, and entertainment ▪ Transportation ▪ Utilities

JULY 2026 © MarketsandMarkets™

Solution	Cisco AI Canvas	Cisco AI Canvas provides a collaborative AI-powered workspace that enables SOC analysts and AI agents to share investigation context, coordinate threat analysis, automate workflows, and accelerate incident response within unified security operations.	▪ Cities and communities ▪ Education ▪ Financial services ▪ Government ▪ Healthcare ▪ Manufacturing ▪ Mining ▪ Oil and gas ▪ Retail ▪ Smart buildings ▪ Sports, media, and entertainment ▪ Transportation ▪ Utilities
Solution	Cisco Security Cloud Control	Cisco Security Cloud Control provides a unified AI-powered security management platform that centralizes policy administration, security analytics, threat visibility, and operational workflows across Cisco and third-party security technologies to improve SOC efficiency.	▪ Cities and communities ▪ Education ▪ Financial services ▪ Government ▪ Healthcare ▪ Manufacturing ▪ Mining ▪ Oil and gas ▪ Retail ▪ Smart buildings ▪ Sports, media, and entertainment ▪ Transportation ▪ Utilities
Service	Cisco Managed Detection and Response (MDR)	Cisco Managed Detection and Response delivers 24×7 AI-assisted threat monitoring, proactive threat hunting, investigation, and response by combining Cisco XDR, Splunk Security, Cisco Talos intelligence, and expert security analysts.	▪ Cities and communities ▪ Education ▪ Financial services ▪ Government ▪ Healthcare ▪ Manufacturing ▪ Mining ▪ Oil and gas ▪ Retail ▪ Smart buildings ▪ Sports, media, and entertainment ▪ Transportation ▪ Utilities

JULY 2026 © MarketsandMarkets™

Service	Cisco Incident Response Services	Cisco Incident Response Services provide expert-led investigation, containment, eradication, and recovery from cyberattacks by combining AI-driven analytics, Cisco Talos threat intelligence, digital forensics, and incident response expertise.	▪ Cities and communities ▪ Education ▪ Financial services ▪ Government ▪ Healthcare ▪ Manufacturing ▪ Mining ▪ Oil and gas ▪ Retail ▪ Smart buildings ▪ Sports, media, and entertainment ▪ Transportation ▪ Utilities

Source: Company Website

15.1.2.3 Recent developments

15.1.2.3.1 Product launches/enhancements

TABLE 442 CISCO: PRODUCT LAUNCHES/ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
March 2026	Product Enhancement	Cisco (US)	Splunk Enterprise Security (Solution)	Cisco enhanced Splunk Enterprise Security with Exposure Analytics, Detection Studio, Federated Search, and a new suite of specialized AI agents that automate detection engineering, alert triage, malware analysis, guided response, and SOC automation.
September 2025	Product Enhancement	Cisco (US)	Splunk Enterprise Security 8.2 (Solution)	Cisco enhanced Splunk Enterprise Security by introducing Enterprise Security Premier Edition and Essentials Edition, delivering agentic AI-powered SecOps capabilities that unify threat detection, investigation, and response within an AI-native SOC platform.
September 2025	Product Enhancement	Cisco (US)	Agentic AI for Splunk Security (Solution)	Cisco enhanced Splunk Security with AI-powered Triage Agent, Malware Reversal Agent, AI Playbook Authoring, Response Importer, AI-Enhanced Detection Library, and Detection SPL Generator to automate SOC investigations and response workflows.

JULY 2026 © MarketsandMarkets™

April 2025	Product Enhancement	Cisco (US)	Cisco XDR (Solution)	Cisco enhanced Cisco XDR by integrating Instant Attack Verification, enabling security teams to automatically validate threats, prioritize high-risk incidents, and accelerate AI-assisted investigations and response across enterprise security environments.
January 2025	Product Launch	Cisco (US)	AI Assistant for Security (Solution)	Cisco launched AI Assistant for Security, later integrated AI Canvas (in June 2025), enabling SOC analysts to collaborate with AI agents, investigate threats, summarize incidents, and streamline security operations through a unified AI-powered workspace.

Source: Company Website and Press Releases

15.1.2.3.2 Deals

TABLE 443 CISCO: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION	DEAL SIZE
June 2026	Acquisition	Cisco (US)	WideField Security (US)	Cisco announced the acquisition of WideField Security to strengthen Splunk's Agentic SOC capabilities by enriching identity intelligence, correlating AI-agent activity, and improving autonomous threat detection and investigation across enterprise environments.	NA
August 2025	Partnership	Cisco (US)	Indosat Ooredoo Hutchison (Indonesia)	Cisco partnered with Indosat Ooredoo Hutchison to launch Indonesia's Sovereign Security Operations Centre, combining Splunk Enterprise Security, AI-powered threat detection, real-time security monitoring, and localized data residency to strengthen AI-driven security operations and cyber resilience.	NA
March 2024	Acquisition	Cisco (US)	Splunk (US)	Cisco completed the acquisition of Splunk to combine Cisco's security portfolio with Splunk's SIEM, SOAR, and observability capabilities, creating an AI-powered security operations platform that accelerates threat detection, investigation, and autonomous SOC operations.	USD 28 million

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.2.4 MnM view

15.1.2.4.1 Key strengths

Cisco has established a differentiated position in the AI SOC market by combining its networking, cybersecurity, and observability capabilities into a unified security operations ecosystem following the acquisition of Splunk. The company's AI SOC portfolio integrates Cisco XDR, Splunk Enterprise Security, Splunk SOAR, AI Assistant for Security, and AI Canvas, enabling security teams to consolidate telemetry, automate investigations, prioritize high-risk alerts, and accelerate incident response through agentic AI. Cisco's AI-driven SOC innovations also include specialized AI agents for detection engineering, malware analysis, guided response, and workflow automation, allowing organizations to transition from reactive security monitoring to machine-speed security operations.

Cisco strengthens its AI SOC capabilities through the integration of Cisco Talos threat intelligence, its extensive enterprise networking footprint, and the Splunk data platform, providing broad visibility across network, endpoint, cloud, identity, and application environments. Its large installed customer base, global partner ecosystem, and managed security expertise enable enterprises across BFSI, government, healthcare, manufacturing, telecommunications, retail, and critical infrastructure sectors to deploy AI-native security operations while leveraging existing Cisco and Splunk investments.

15.1.2.4.2 Strategic choices

Cisco's AI SOC strategy centers on building an Agentic SOC, where autonomous AI agents collaborate with security analysts to execute investigation, detection engineering, threat validation, and response activities at machine speed. Rather than positioning AI as a standalone assistant, Cisco is embedding agentic capabilities throughout its security portfolio including Cisco XDR, Splunk Enterprise Security, AI Assistant for Security, and AI Canvas to create an integrated platform for end-to-end security operations.

A key pillar of Cisco's strategy is leveraging the Splunk acquisition to unify security operations with observability and enterprise data analytics. The company continues to expand its ecosystem through AI-focused partnerships, technology integrations, and innovations that combine Cisco Talos intelligence, AI-powered automation, and Zero Trust security. This approach enables organizations to modernize SOC operations, improve operational resilience, and secure increasingly complex hybrid, multi-cloud, and AI-driven enterprise environments.

15.1.2.4.3 Weaknesses & competitive threats

Cisco's AI SOC portfolio has expanded significantly following the integration of Splunk; however, organizations may face integration complexity and operational adjustments when consolidating Cisco Security, Splunk, and existing third-party security platforms into a unified security operations architecture. Enterprises with established multi-vendor SOC environments may require substantial migration, data integration, and workflow optimization efforts to fully realize the platform's AI-driven capabilities.

The company also competes against cybersecurity vendors that have mature AI-native SOC platforms, including Microsoft, Palo Alto Networks, Google, CrowdStrike, and IBM, all of which continue to invest aggressively in autonomous security operations and agentic AI. Maintaining competitive differentiation will require Cisco to further strengthen AI orchestration, interoperability, autonomous decision-making, and measurable security outcomes while accelerating enterprise adoption of its Agentic SOC vision.

JULY 2026 © MarketsandMarkets™

15.1.3 CROWDSTRIKE

15.1.3.1 Business overview

CrowdStrike Holdings, Inc. is a global cybersecurity company focused on protecting modern enterprises through its AI-native, cloud-delivered cybersecurity platform. Built around the CrowdStrike Falcon® platform, the company unifies endpoint, identity, cloud, data, and next-generation SIEM capabilities within a single cloud-native architecture. Powered by the CrowdStrike Security Cloud, the platform combines artificial intelligence, real-time threat intelligence, behavioral analytics, and high-fidelity telemetry to deliver accurate threat detection, automated protection, proactive threat hunting, and rapid incident response across complex enterprise environments. CrowdStrike's cybersecurity portfolio spans endpoint security, cloud security, identity protection, exposure management, managed detection and response (MDR), threat intelligence, next-generation SIEM, AI security, and security services, enabling organizations to strengthen cyber resilience while reducing operational complexity.

Within the AI SOC market, CrowdStrike is advancing an Agentic SOC strategy through the Falcon platform by integrating Falcon Next-Gen SIEM, Falcon Onum, Charlotte AI, Charlotte AI AgentWorks, Charlotte Agentic SOAR, Falcon Complete Next-Gen MDR, and AI Security Readiness Services into a unified security operations ecosystem. Rather than positioning AI as a standalone assistant, CrowdStrike embeds mission-ready AI agents throughout the SOC lifecycle to automate alert triage, threat hunting, investigation, detection engineering, malware analysis, and incident response. Falcon Onum strengthens this architecture by providing AI-ready security data pipelines, while Charlotte AI AgentWorks enables organizations and partners to build, orchestrate, and govern custom AI agents that accelerate autonomous security operations.

CrowdStrike serves organizations across BFSI, government and public sector, healthcare and life sciences, manufacturing, retail, energy and utilities, telecommunications, education, and technology through its global cloud infrastructure and regional cloud deployments spanning North America, Europe, Asia Pacific, Latin America, the Middle East, and Africa. The company's ecosystem-driven strategy is reinforced through collaborations with global consulting firms, cloud providers, AI companies, and cybersecurity vendors, enabling enterprises to modernize SOC operations while meeting regional data residency and regulatory requirements. Strategic relationships with IBM, EY, Zscaler, Fortinet, and the Charlotte AI AgentWorks Ecosystem partners further expand the adoption of AI-native security operations across heterogeneous enterprise environments.

Recent initiatives demonstrate CrowdStrike's long-term vision of building a fully autonomous security platform. The company has expanded the Falcon platform with mission-ready AI agents, introduced Charlotte AI AgentWorks, launched AI Security Readiness and Agentic MDR services, and strengthened Falcon Next-Gen SIEM through the acquisition of Onum, enhancing AI-ready telemetry and real-time security data management. These investments, together with continuous advancements in agentic AI, unified security data, and open ecosystem integrations, position CrowdStrike as one of the leading providers driving the transition from analyst-assisted SOCs to AI-native, agentic security operations.

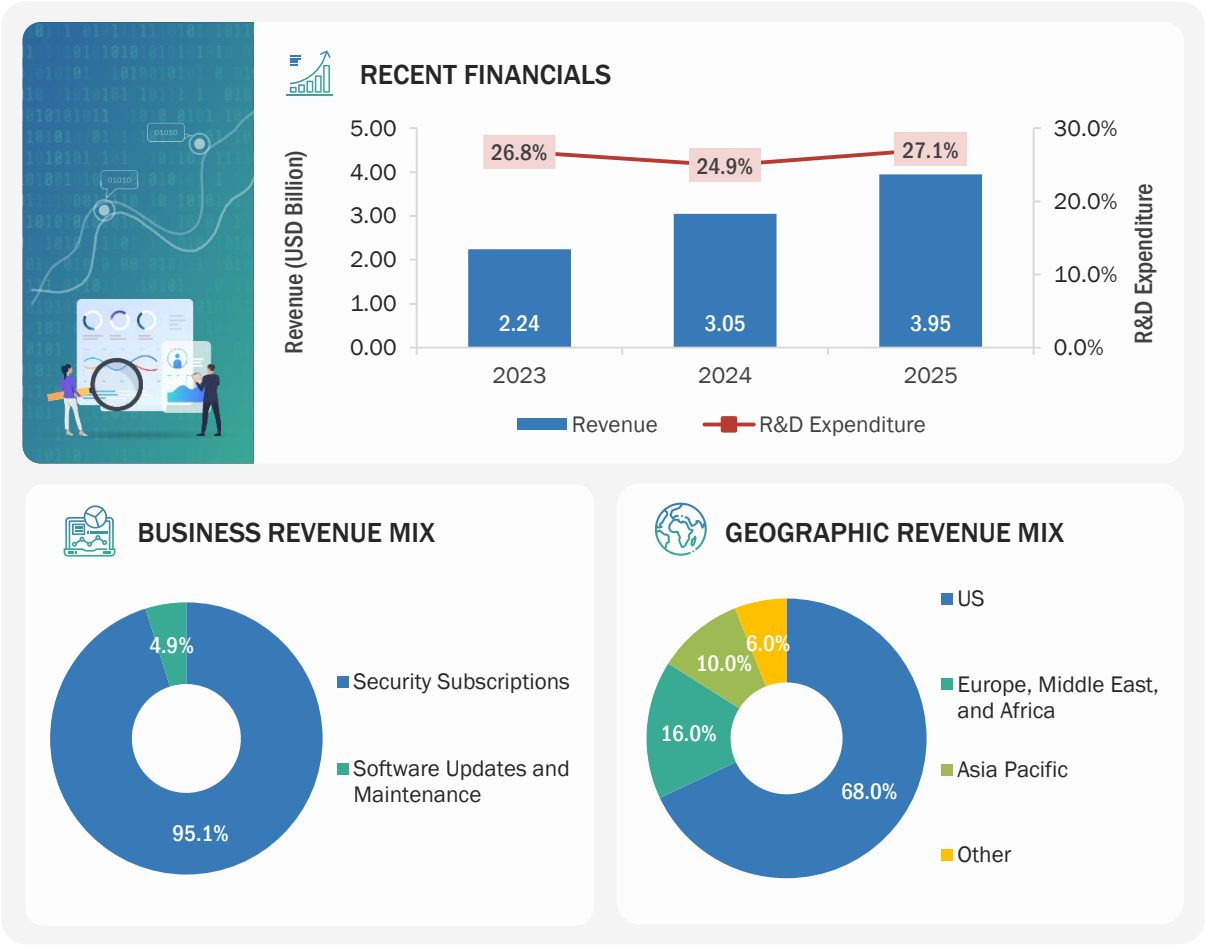
TABLE 444 CROWDSTRIKE: COMPANY OVERVIEW

Founding Year	2011
Headquarters Country	US
Headquarters City/State	Austin, Texas
Ownership Type	Public (NASDAQ: CRWD)

Source: Company Website, Annual Reports, and SEC Filings

JULY 2026 © MarketsandMarkets™

FIGURE 51 CROWDSTRIKE: COMPANY SNAPSHOT



Source: Company Website and Annual Reports.

15.1.3.2 Products/Solutions/Services offered

TABLE 445 CROWDSTRIKE: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/SERVICE	DESCRIPTION	VERTICAL
Solution	CrowdStrike Falcon Next-Gen SIEM	Falcon Next-Gen SIEM is an AI-native cloud security information and event management platform that unifies first- and third-party telemetry, correlates threats in real time, and accelerates AI-driven detection, investigation, and response across modern SOC environments.	▪ Federal government ▪ Department of War ▪ State & local government ▪ Financial services ▪ Healthcare ▪ Election security ▪ Education ▪ Retail ▪ Manufacturing

JULY 2026 © MarketsandMarkets™

Solution	Charlotte AI	Charlotte AI is CrowdStrike's generative AI security assistant that automates alert triage, threat investigation, malware analysis, incident summarization, and response recommendations using intelligence trained on millions of real-world SOC decisions.	▪ Federal government ▪ Department of War ▪ State & local government ▪ Financial services ▪ Healthcare ▪ Election security ▪ Education ▪ Retail ▪ Manufacturing
Solution	Charlotte Agentic SOAR	Charlotte Agentic SOAR orchestrates autonomous security workflows by coordinating multiple AI agents to investigate threats, execute response actions, and automate incident remediation while maintaining human oversight and governance.	▪ Federal government ▪ Department of War ▪ State & local government ▪ Financial services ▪ Healthcare ▪ Election security ▪ Education ▪ Retail ▪ Manufacturing
Solution	Charlotte AI AgentWorks	Charlotte AI AgentWorks is a no-code platform that enables organizations to build, customize, orchestrate, and deploy secure AI security agents for SOC operations using CrowdStrike Falcon data, enterprise workflows, and frontier AI models.	▪ Federal government ▪ Department of War ▪ State & local government ▪ Financial services ▪ Healthcare ▪ Election security ▪ Education ▪ Retail ▪ Manufacturing
Service	Falcon Complete Next-Gen MDR	Falcon Complete Next-Gen MDR combines managed detection and response with Charlotte AI to deliver 24×7 threat hunting, AI-assisted investigations, automated response, and expert-led security operations for enterprise SOC teams.	▪ Federal government ▪ Department of War ▪ State & local government ▪ Financial services ▪ Healthcare ▪ Election security ▪ Education ▪ Retail ▪ Manufacturing

JULY 2026 © MarketsandMarkets™

Service	AI Security Readiness Services	AI Security Readiness Services help organizations assess SOC readiness for AI adoption by evaluating governance, operational processes, security controls, and AI risk management while preparing security teams for agentic SOC transformation	▪ Federal government ▪ Department of War ▪ State & local government ▪ Financial services ▪ Healthcare ▪ Election security ▪ Education ▪ Retail ▪ Manufacturing
Solution	Falcon Onum	Falcon Onum is a real-time security data control platform that collects, enriches, filters, and routes security telemetry, providing high-fidelity AI-ready data for Falcon Next-Gen SIEM and enabling faster, agentic threat detection, investigation, and response across modern SOC environments.	▪ Federal government ▪ Department of War ▪ State & local government ▪ Financial services ▪ Healthcare ▪ Election security ▪ Education ▪ Retail ▪ Manufacturing

Source: Company Website

15.1.3.3 Recent developments

15.1.3.3.1 Product launches/enhancements

TABLE 446 CROWDSTRIKE: PRODUCT LAUNCHES/ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
March 2026	Product Launch	CrowdStrike (US)	Agentic MDR & SOC Transformation Services (Service)	CrowdStrike launched Agentic MDR and SOC Transformation Services to help organizations operationalize the Agentic SOC by combining AI agents, Falcon Complete expertise, automated investigations, machine-speed response, and modernization of SIEM, data pipelines, governance, and security workflows.
September 2025	Product Launch	CrowdStrike (US)	Charlotte AI AgentWorks (Solution)	CrowdStrike launched Charlotte AI AgentWorks, a no-code platform that enables organizations and partners to build, orchestrate, govern, and deploy custom AI security agents, accelerating AI-native SOC transformation through secure agent orchestration and automation.

JULY 2026 © MarketsandMarkets™

August 2025	Product Launch	CrowdStrike (US)	AI for SecOps Readiness (Service)	CrowdStrike launched AI for SecOps Readiness, a professional service that helps organizations securely operationalize AI within security operations by assessing SOC workflows, identifying automation opportunities, implementing governance, and accelerating AI-driven detection, investigation, and response capabilities.
April 2025	Product Enhancement	CrowdStrike (US)	Charlotte AI (Solution)	CrowdStrike enhanced Charlotte AI with AI innovations including Detection Triage, improved investigation capabilities, Falcon Fusion integration, and expanded generative AI workflows, enabling SOC analysts to automate alert prioritization, investigations, and incident response across the Falcon platform.
April 2025	Product Enhancement	CrowdStrike (US)	Charlotte AI Agentic Response & Agentic Workflows (Solution)	CrowdStrike enhanced Charlotte AI by introducing Agentic Response and Agentic Workflows, enabling autonomous investigation, AI-guided reasoning, root-cause analysis, automated response orchestration, and intelligent decision-making to accelerate operations across AI-native security operations centers.

Source: Company Website and Press Releases

15.1.3.3.2 Deals

TABLE 447 CROWDSTRIKE: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION	DEAL SIZE
March 2026	Collaboration	CrowdStrike (US)	Accenture (Ireland), Amazon Web Services (US), Anthropic (US), Deloitte (UK), Kroll (US), NVIDIA (US), OpenAI (US), Salesforce (US), Telefónica Tech (Spain)	CrowdStrike collaborated with Accenture, AWS, Anthropic, Deloitte, Kroll, NVIDIA, OpenAI, Salesforce, and Telefónica Tech to launch the Charlotte AI AgentWorks Ecosystem, enabling organizations to build, orchestrate, govern, and scale secure AI agents that accelerate agentic SOC transformation and AI-native security operations.	NA

JULY 2026 © MarketsandMarkets™

March 2026	Partnership	CrowdStrike (US)	IBM (US)	CrowdStrike partnered with IBM to integrate Charlotte AI with IBM's Autonomous Threat Operations Machine (ATOM), combining AI-driven investigation, coordinated machine-speed response, managed Threat Detection and Response services, and Cyber Range validation to accelerate enterprise Agentic SOC transformation.	NA
March 2026	Partnership	CrowdStrike (US)	Ernst & Young (EY) (UK)	EY selected the CrowdStrike Falcon platform to power its Agentic Security Operations Center (SOC) services, leveraging NVIDIA AI infrastructure and NVIDIA AI Enterprise software to deliver AI-driven threat detection, investigation, and autonomous security operations for enterprise customers.	NA
August 2025	Partnership	CrowdStrike (US)	Zscaler (US)	CrowdStrike partnered with Zscaler to expand AI-driven security operations by integrating the Falcon platform with Zscaler Zero Trust Exchange and Red Canary's agentic AI-driven MDR capabilities, enabling unified visibility, accelerated threat detection, automated response, and modernized enterprise SOC operations.	NA
August 2025	Acquisition	CrowdStrike (US)	Onum (Spain)	CrowdStrike acquired Onum, a real-time security data pipeline company, to strengthen Falcon Next-Gen SIEM with intelligent telemetry management, high-fidelity data processing, and AI-ready security data that improves agentic detection, investigation, and autonomous SOC operations.	USD 290 million
October 2024	Partnership	CrowdStrike (US)	Fortinet (US)	CrowdStrike partnered with Fortinet to integrate the Falcon platform with FortiGate Next-Generation Firewalls, enabling unified AI-powered endpoint and network visibility, accelerated threat detection, automated investigations, and faster SOC response across enterprise environments.	NA

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.3.3.3 Expansions

TABLE 448 CROWDSTRIKE: EXPANSIONS

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY	COMPANY	DESCRIPTION
January 2026	Expansion	Regional Cloud Expansion (Data Sovereignty)	Saudi Arabia, India & United Arab Emirates	CrowdStrike (US)	CrowdStrike expanded its Global Data Sovereignty initiative by launching new in-country regional cloud deployments in Saudi Arabia, India, and the UAE. The expansion enables organizations to deploy the Falcon platform with local data residency while retaining access to CrowdStrike's global threat intelligence, AI-powered security operations, and Falcon Next-Gen SIEM capabilities, supporting AI-native SOC adoption in regulated industries.

Source: Company Website and Press Releases

15.1.3.4 MnM view

15.1.3.4.1 Key strengths

CrowdStrike has established a leading position in the AI SOC market through its Falcon platform, which integrates Falcon Next-Gen SIEM, Falcon Fusion SOAR, Charlotte AI, Falcon Onum, Falcon LogScale, Falcon Foundry, and Falcon Complete Next-Gen MDR into a unified AI-native security operations platform. Designed to power the agentic SOC, the platform combines AI-driven detection, investigation, workflow automation, and threat intelligence to accelerate security operations, reduce analyst fatigue, and enable machine-speed response across hybrid enterprise environments.

CrowdStrike further strengthens its AI SOC capabilities through its single-agent, cloud-native Falcon architecture, which unifies endpoint, identity, cloud, and third-party telemetry within a common data model. The company's continuous innovation in Charlotte AI, agentic SOAR, AI-powered SIEM, and workflow automation, supported by industry-leading threat intelligence and a broad partner ecosystem, enables organizations across BFSI, healthcare, manufacturing, government, retail, and critical infrastructure to modernize SOC operations and improve cyber resilience.

15.1.3.4.2 Strategic choices

CrowdStrike is specializing as an AI-native security platform provider focused on delivering autonomous and intelligence-driven security operations through a unified cloud platform. Its strategy centers on embedding Charlotte AI and agentic AI workflows across the Falcon platform, enabling organizations to automate investigations, accelerate response, and improve SOC productivity without relying on fragmented security tools.

A key element of CrowdStrike's strategy is expanding the Falcon platform into the central AI-native SOC by combining AI-powered SIEM, XDR, SOAR, security data management, and threat intelligence within a single architecture. The company continues to invest in agentic AI, workflow automation, open integrations, and

JULY 2026 © MarketsandMarkets™

ecosystem partnerships, helping enterprises consolidate security operations while improving operational efficiency and reducing complexity.

15.1.3.4.3 Weaknesses & competitive threats

CrowdStrike's AI SOC is built around the Falcon platform, which may present adoption challenges for organizations seeking vendor-neutral or multi-platform security operations. Enterprises with significant investments in legacy SIEMs or heterogeneous security environments may require additional integration and migration efforts to fully leverage the platform's AI-native capabilities.

The company also faces intense competition from hyperscale cloud providers and cybersecurity vendors such as Microsoft, Google, Palo Alto Networks, Cisco, SentinelOne, and IBM, all of which are investing aggressively in agentic AI, autonomous SOC platforms, AI-powered SIEM, and unified security operations. Sustaining its leadership will require CrowdStrike to continuously enhance Charlotte AI, expand ecosystem interoperability, and demonstrate measurable improvements in automation, scalability, and return on security investments.

JULY 2026 © MarketsandMarkets™

15.1.4 PALO ALTO NETWORKS

15.1.4.1 Business overview

Palo Alto Networks, Inc. is a prominent cybersecurity company built around delivering AI-driven security platforms that protect enterprises across network, cloud, endpoint, identity, and security operations environments. The company's platform-based strategy integrates prevention, detection, response, and security management into a unified architecture, enabling organizations to simplify cybersecurity operations while improving resilience against increasingly sophisticated cyber threats. Its portfolio spans network security, cloud security, security operations, threat intelligence, and AI-powered security services, supported by the Unit 42 incident response and threat intelligence organization.

Within the AI SOC market landscape, Palo Alto Networks differentiates itself from competitors through the Cortex portfolio, led by Cortex XSIAM, an AI-native security operations platform that converges SIEM, SOAR, XDR, threat intelligence, and automation into a single operating environment. Complementing XSIAM are Cortex XDR, Cortex XSOAR, Cortex AgentiX, and Cortex Frontier AI, which collectively enable autonomous alert triage, AI-assisted investigations, threat hunting, detection engineering, and automated response. The company further extends these capabilities through Unit 42 Managed XSIAM, Managed Detection and Response (MDR), and Managed Threat Hunting services, providing organizations with expert-led, AI-powered security operations.

Palo Alto Networks serves organizations across banking, financial services and insurance (BFSI), government and defense, healthcare and life sciences, IT and telecommunications, manufacturing, retail and e-commerce, energy and utilities, education, and other critical infrastructure sectors. The company maintains a strong presence across North America, Europe, Asia Pacific, Latin America, and the Middle East & Africa, supported by a global channel ecosystem, cloud-delivered security platforms, and Unit 42's worldwide incident response and consulting capabilities.

Palo Alto Networks is driving the industry's transition toward the Autonomous SOC through continuous investments in Precision AI, agentic AI, and unified security operations. Recent initiatives including the evolution of Cortex XSIAM, introduction of Cortex Frontier AI and Cortex AgentiX, strategic acquisitions such as IBM QRadar SaaS assets and Protect AI, and expanded partnerships with global technology providers reinforce the company's vision of delivering machine-speed detection, investigation, and response through a consolidated AI-native security platform.

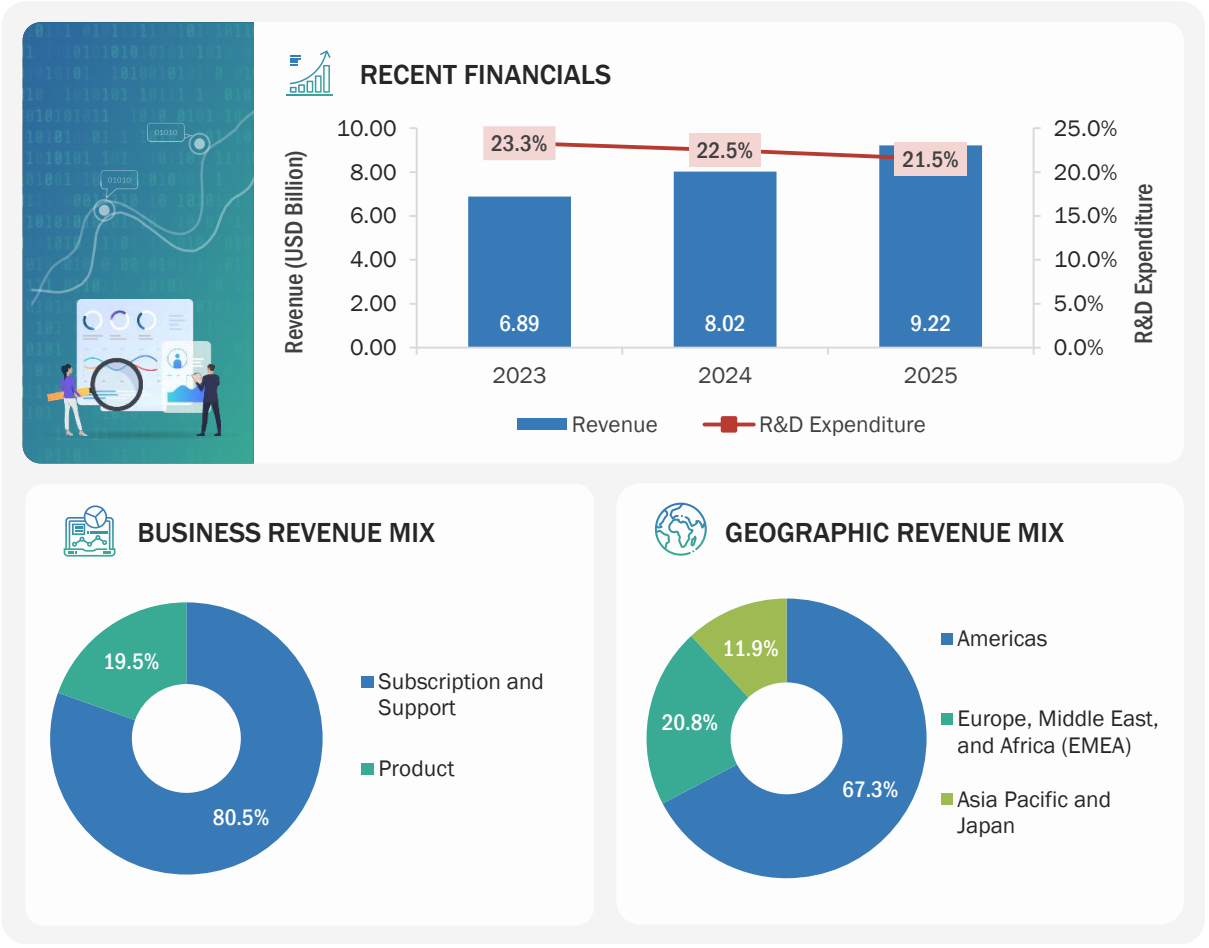
TABLE 449 PALO ALTO NETWORKS: COMPANY OVERVIEW

Founding Year	2005
Headquarters Country	US
Headquarters City/State	Santa Clara, California
Ownership Type	Public (NYSE: PANW)

Source: Company Website, Annual Reports, and SEC Filings

JULY 2026 © MarketsandMarkets™

FIGURE 52 PALO ALTO NETWORKS: COMPANY SNAPSHOT



Source: Company Website and Annual Reports.

15.1.4.2 Products/Solutions/Services offered

TABLE 450 PALO ALTO NETWORKS: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/SERVICE	DESCRIPTION	VERTICAL
Solution	Cortex XSIAM	Cortex XSIAM is Palo Alto Networks' AI-powered security operations platform that unifies SIEM, XDR, SOAR, threat intelligence, and automation to deliver autonomous threat detection, investigation, and response through Precision AI and agentic SOC capabilities.	▪ Financial services ▪ Healthcare ▪ ICS/SCADA ▪ Manufacturing ▪ Oil and gas ▪ Public sector ▪ Retail ▪ Utilities

JULY 2026 © MarketsandMarkets™

Solution	Cortex XDR	Cortex XDR leverages AI and behavioral analytics to correlate telemetry across endpoints, networks, cloud workloads, identities, and third-party sources, enabling high-fidelity threat detection, automated investigations, and accelerated incident response within modern SOC environments.	▪ Financial services ▪ Healthcare ▪ ICS/SCADA ▪ Manufacturing ▪ Oil and gas ▪ Public sector ▪ Retail ▪ Utilities
Solution	Cortex XSOAR	Cortex XSOAR automates security operations by orchestrating incident response workflows, threat intelligence management, case management, and security playbooks across hundreds of integrated security products, improving SOC productivity and response consistency.	▪ Financial services ▪ Healthcare ▪ ICS/SCADA ▪ Manufacturing ▪ Oil and gas ▪ Public sector ▪ Retail ▪ Utilities
Service	Unit 42 Managed XSIAM	Unit 42 Managed XSIAM delivers fully managed, AI-driven security operations by combining Cortex XSIAM with 24×7 expert monitoring, continuous SOC engineering, proactive threat hunting, automated response, and end-to-end incident remediation across enterprise environments.	▪ Financial services ▪ Healthcare ▪ ICS/SCADA ▪ Manufacturing ▪ Oil and gas ▪ Public sector ▪ Retail ▪ Utilities
Service	Unit 42 Managed Detection and Response (MDR)	Unit 42 Managed Detection and Response provides 24×7 AI-assisted monitoring, threat detection, investigation, proactive hunting, and guided remediation, leveraging Cortex XDR, global threat intelligence, and expert analysts to strengthen enterprise cyber resilience.	▪ Financial services ▪ Healthcare ▪ ICS/SCADA ▪ Manufacturing ▪ Oil and gas ▪ Public sector ▪ Retail ▪ Utilities
Service	Unit 42 Managed Threat Hunting	Unit 42 Managed Threat Hunting provides continuous proactive threat hunting performed by experienced threat researchers who leverage AI, attacker behavior analytics, and global intelligence to identify hidden threats before they escalate into security incidents.	▪ Financial services ▪ Healthcare ▪ ICS/SCADA ▪ Manufacturing ▪ Oil and gas ▪ Public sector ▪ Retail ▪ Utilities

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.1.4.3 Recent developments

15.1.4.3.1 Product launches/enhancements

TABLE 451 PALO ALTO NETWORKS: PRODUCT LAUNCHES/ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
April 2025	Product Enhancement	Palo Alto Networks (US)	Cortex XSIAM 3.0 (Solution)	Palo Alto Networks enhanced Cortex XSIAM 3.0 by adding AI-driven Exposure Management, Advanced Email Security, and a unified Cloud & SOC Command Center, extending the platform from reactive incident response to proactive security operations.
May 2024	Product Enhancement	Palo Alto Networks (US)	Cortex XSIAM (Solution)	Palo Alto Networks enhanced Cortex XSIAM with Bring Your Own ML (BYOML), third-party EDR data ingestion, expanded Cloud Detection and Response capabilities, and Precision AI-powered customization to improve autonomous security operations and detection accuracy.
April 2024	Product Enhancement	Palo Alto Networks (US)	Cortex XSIAM for Cloud (Solution)	Palo Alto Networks enhanced Cortex XSIAM by introducing Cloud Detection and Response (CDR), Cloud Command Center, and unified cloud-native SOC capabilities, enabling AI-driven threat detection, investigation, and remediation across enterprise and multi-cloud environments.

Source: Company Website and Press Releases

15.1.4.3.2 Deals

TABLE 452 PALO ALTO NETWORKS: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION	DEAL SIZE
June 2026	Partnership	Palo Alto Networks (US)	Wipro (India)	Palo Alto Networks partnered with Wipro to combine Cortex XSIAM with Wipro CyberShield, delivering AI-powered managed security operations, automated threat detection, and machine-learning-driven SOC services for enterprise customers worldwide.	NA

JULY 2026 © MarketsandMarkets™

February 2026	Acquisition	Palo Alto Networks (US)	CyberArk (Israel)	Palo Alto Networks completed the acquisition of CyberArk, integrating privileged access management and identity security into its AI-driven cybersecurity platform to secure human and machine identities within autonomous security operations and AI-enabled enterprise environments.	NA
July 2025	Acquisition	Palo Alto Networks (US)	Protect AI (US)	Palo Alto Networks acquired Protect AI to strengthen AI security capabilities across the software development lifecycle, expanding protection for AI models, applications, and agentic AI environments while complementing its Cortex AI-driven security operations portfolio.	NA
September 2024	Acquisition	Palo Alto Networks (US)	IBM's QRadar Software-as-a-Service (SaaS) assets	Palo Alto Networks completed the acquisition of IBM's QRadar Software-as-a-Service (SaaS) assets, strengthening its AI-powered security operations portfolio by accelerating customer migration to Cortex XSIAM and expanding autonomous SOC capabilities through Precision AI and automation.	Approximately USD 500 million
May 2024	Partnership	Palo Alto Networks (US)	IBM (US)	Palo Alto Networks partnered with IBM to deliver AI-powered security operations by combining Cortex XSIAM with IBM Consulting services and watsonx capabilities, while enabling migration of IBM QRadar SaaS customers to an AI-native SOC platform.	NA
April 2024	Partnership	Palo Alto Networks (US)	Google Cloud (US)	Palo Alto Networks partnered with Google Cloud to expand AI-powered cybersecurity by integrating Cortex and Prisma Cloud with Google Cloud services, helping enterprises strengthen cloud security, threat detection, and AI-driven SOC operations.	NA

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.4.3.3 Expansions

TABLE 453 PALO ALTO NETWORKS: EXPANSIONS

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY	COMPANY	DESCRIPTION
June 2026	Expansion	Regional AI SOC Expansion (Sovereign Security Platform)	Europe	Palo Alto Networks (US)	Palo Alto Networks expanded its AI-driven security operations footprint across Europe by introducing Sovereign Cortex with T Security in collaboration with Deutsche Telekom, enabling regulated organizations to adopt Cortex AI-powered SecOps while meeting European data sovereignty and compliance requirements.
July 2024	Expansion	Regional Cloud Infrastructure Expansion	Indonesia	Palo Alto Networks (US)	Palo Alto Networks expanded its regional cloud infrastructure by launching a new cloud location in Indonesia, enabling Cortex XSIAM, Cortex XSOAR, and Cortex XDR customers to meet local data residency requirements while delivering AI-powered security operations and automated threat response capabilities.

Source: Company Website and Press Releases

15.1.4.4 MnM view

15.1.4.4.1 Key strengths

Palo Alto Networks has emerged as one of the pioneers of the autonomous AI SOC by building its security operations strategy around a single, AI-native platform rather than disconnected SIEM, SOAR, and XDR products. Its Cortex XSIAM platform consolidates security telemetry, analytics, automation, threat intelligence, and response into a unified data architecture powered by Precision AI, enabling organizations to significantly reduce alert noise, accelerate investigations, and automate response workflows at scale. The platform further integrates Cortex XDR, XSOAR, Extended Data Lake (XDL), and Cortex AgentiX, allowing SOC teams to transition from reactive operations to autonomous, AI-driven security operations.

Another key differentiator is Palo Alto Networks' emphasis on AI-first SOC transformation supported by one of the industry's largest security data ecosystems. Precision AI leverages extensive real-world security telemetry, while Cortex Frontier AI incorporates leading frontier AI models to improve reasoning, investigation accuracy, and autonomous decision-making. Combined with Unit 42 managed security expertise and an extensive technology partner ecosystem, the company enables enterprises across BFSI, government, healthcare, manufacturing, telecommunications, retail, and other regulated industries to modernize security operations while reducing operational complexity.

JULY 2026 © MarketsandMarkets™

15.1.4.4.2 Strategic choices

Palo Alto Networks is pursuing a strategy centered on platform consolidation, replacing fragmented SOC architectures with an integrated security operations platform built around Cortex. Instead of expanding individual SIEM or SOAR capabilities independently, the company continues to unify data management, detection engineering, threat intelligence, automation, exposure management, and AI reasoning within Cortex XSIAM, simplifying security operations while improving automation and operational efficiency.

The company is also investing aggressively in frontier AI and agentic security operations to prepare SOCs for machine-speed cyber threats. Through innovations such as Cortex Frontier AI, Cortex AgentiX, and Precision AI, Palo Alto Networks is enabling AI agents to perform complex investigations, automate remediation, and continuously improve security workflows. Strategic acquisitions and ecosystem partnerships further strengthen its ability to deliver scalable AI-native security operations across hybrid, multi-cloud, and enterprise environments.

15.1.4.4.3 Weaknesses & competitive threats

Palo Alto Networks' AI SOC platform delivers maximum value when organizations adopt a broader Cortex-centric security architecture, which may require significant platform consolidation and migration from legacy SIEM or multi-vendor SOC environments. Enterprises with deeply entrenched third-party security ecosystems may face higher implementation complexity, operational change management requirements, and investment costs during large-scale modernization initiatives.

The company also competes in an increasingly crowded AI SOC market where Microsoft, Google, Cisco, CrowdStrike, SentinelOne, and IBM are embedding generative AI and autonomous capabilities into their security platforms. As AI-driven cyber threats continue to evolve rapidly, Palo Alto Networks must sustain its leadership in autonomous reasoning, AI governance, interoperability, and large-scale automation while demonstrating measurable operational outcomes to enterprises adopting next-generation AI SOC platforms.

JULY 2026 © MarketsandMarkets™

15.1.5 GOOGLE

15.1.5.1 Business overview

Google LLC, a subsidiary of Alphabet Inc., is a global technology company with extensive capabilities in cloud computing, AI, cybersecurity, data analytics, and enterprise software through Google Cloud. Leveraging its cloud-native architecture, large-scale data infrastructure, and advanced AI technologies, the company enables organizations to modernize digital operations, secure hybrid and multi-cloud environments, and accelerate enterprise AI adoption. Its cybersecurity portfolio encompasses cloud security, threat intelligence, security analytics, identity protection, and AI-powered security operations.

At the core of Google's AI SOC strategy is an integrated security operations portfolio comprising Google Security Operations (SecOps), Gemini in Google Security Operations, Google Threat Intelligence, Security Operations SIEM, SOAR, and Agentic SOC capabilities. The platform combines cloud-native SIEM, SOAR, Mandiant frontline intelligence, VirusTotal intelligence, and Gemini-powered AI agents to automate alert triage, threat investigation, threat hunting, detection engineering, and incident response across enterprise environments.

Serving organizations across banking, financial services and insurance (BFSI), government and public sector, healthcare and life sciences, IT and telecommunications, manufacturing, retail and e-commerce, energy and utilities, media and entertainment, and education, Google leverages its global cloud infrastructure, regional Google Security Operations deployments, and extensive partner ecosystem to help customers implement AI-driven security operations while meeting regulatory, compliance, and data sovereignty requirements. The company maintains a strong global presence across North America, Europe, Asia Pacific, Latin America, the Middle East, and Africa, enabling enterprises worldwide to modernize security operations through cloud-native and AI-powered cybersecurity capabilities.

Recent strategic initiatives reflect Google's long-term vision for autonomous security operations. By advancing Agentic SOC capabilities, the company has introduced AI agents for alert triage, threat hunting, and detection engineering while embedding Gemini across its security platform to improve analyst productivity and accelerate incident response. Google further strengthened its cloud and AI security portfolio through the acquisition of Wiz, expanding its capabilities in multicloud security, cloud-native application protection, and AI-driven threat prevention, detection, and response. Strategic partnerships with global system integrators, managed security service providers, and cybersecurity vendors, together with regional Google Security Operations deployments, further reinforce Google's AI SOC ecosystem and support enterprise security modernization worldwide.

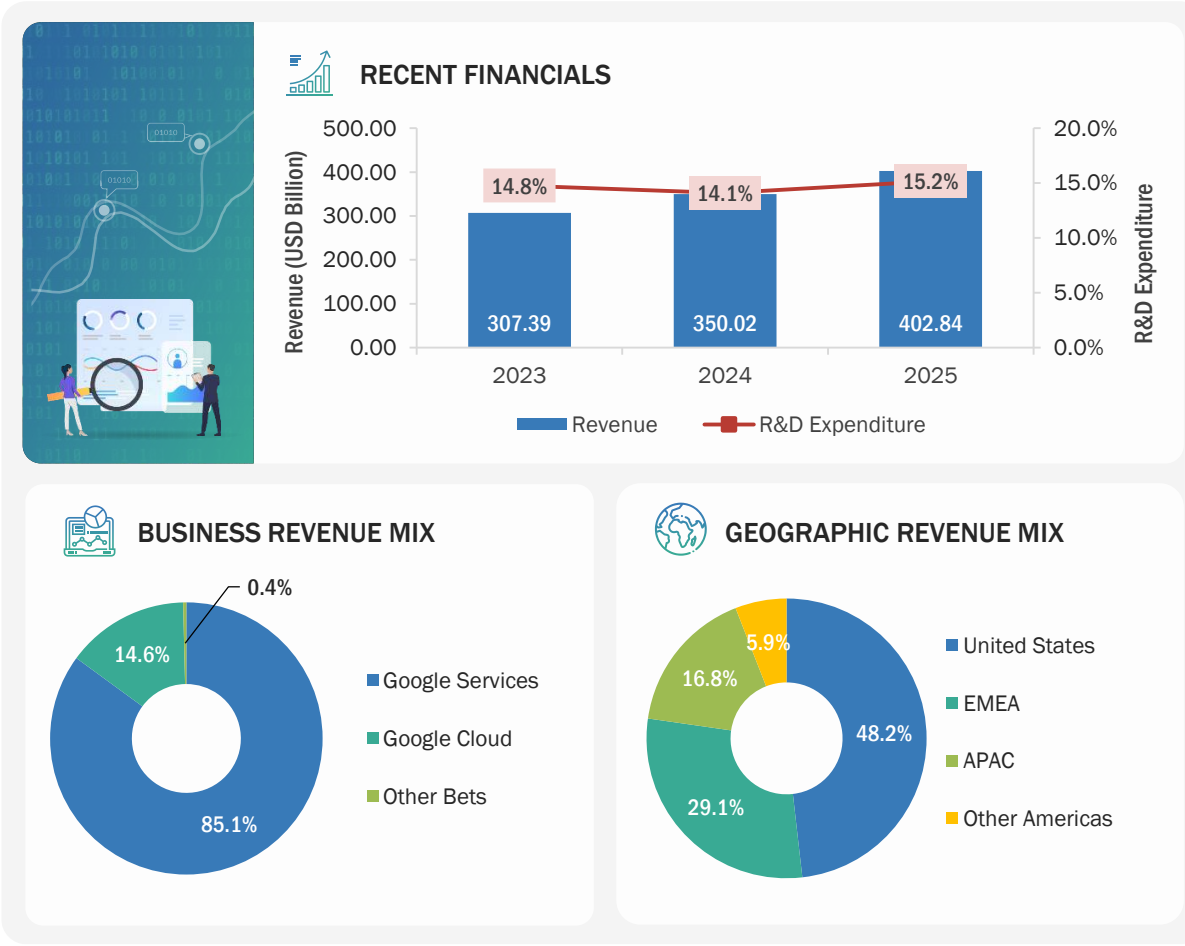
TABLE 454 GOOGLE: COMPANY OVERVIEW

Founding Year	1998
Headquarters Country	US
Headquarters City/State	Mountain View, California
Ownership Type	Public (NASDAQ: GOOG)

Source: Company Website, Annual Reports, and SEC Filings

JULY 2026 © MarketsandMarkets™

FIGURE 53 GOOGLE: COMPANY SNAPSHOT



Source: Company Website and Annual Reports.

15.1.5.2 Products/Solutions/Services offered

TABLE 455 GOOGLE: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/SERVICE	DESCRIPTION	VERTICAL
Solution	Google Security Operations – Agentic SOC Platform	Google Security Operations Agentic SOC platform leverages Gemini-powered AI agents to automate SOC workflows including alert triage, threat investigation, threat hunting, and detection engineering, enabling organizations to achieve faster response, improved productivity, and autonomous security operations.	▪ Retail ▪ BFSI ▪ Telecommunications ▪ Media and entertainment ▪ Healthcare and life sciences ▪ Manufacturing ▪ Government ▪ Education

JULY 2026 © MarketsandMarkets™

Solution	Gemini in Google Security Operations	Gemini in Google Security Operations provides generative AI capabilities that assist SOC analysts with security investigations, natural language-based queries, threat analysis, incident summarization, and workflow automation, helping reduce manual effort and accelerate cybersecurity decision-making processes.	▪ Retail ▪ BFSI ▪ Telecommunications ▪ Media and entertainment ▪ Healthcare and life sciences ▪ Manufacturing ▪ Government ▪ Education
Solution	Triage and Investigation Agent	Google's Triage and Investigation Agent is an AI-powered SOC assistant embedded within Google Security Operations that autonomously analyzes alerts, gathers evidence, determines true or false positives, and provides investigation summaries to accelerate incident response.	▪ Retail ▪ BFSI ▪ Telecommunications ▪ Media and entertainment ▪ Healthcare and life sciences ▪ Manufacturing ▪ Government ▪ Education
Solution	Detection Engineering Agent	Google's Detection Engineering Agent uses AI to analyze threat profiles, identify security coverage gaps, generate detection rules, and validate detection effectiveness, enabling SOC teams to proactively improve threat detection capabilities and reduce manual engineering efforts.	▪ Retail ▪ BFSI ▪ Telecommunications ▪ Media and entertainment ▪ Healthcare and life sciences ▪ Manufacturing ▪ Government ▪ Education
Solution	Threat Hunting Agent	Google's Threat Hunting Agent enables proactive threat discovery by analyzing security telemetry, identifying emerging attack patterns, and investigating adversary behaviors that bypass traditional defenses, helping SOC teams improve proactive detection and threat response capabilities.	▪ Retail ▪ BFSI ▪ Telecommunications ▪ Media and entertainment ▪ Healthcare and life sciences ▪ Manufacturing ▪ Government ▪ Education

JULY 2026 © MarketsandMarkets™

Solution	Google Security Operations SIEM	Google Security Operations SIEM provides cloud-native security analytics, centralized telemetry management, threat detection, investigation, and response capabilities, enhanced with AI-driven analytics and threat intelligence to support modern AI-powered SOC operations.	▪ Retail ▪ BFSI ▪ Telecommunications ▪ Media and entertainment ▪ Healthcare and life sciences ▪ Manufacturing ▪ Government ▪ Education
Solution	Google Security Operations SOAR	Google Security Operations SOAR enables automated security response workflows by orchestrating actions across security tools and integrating AI agents into playbooks, helping SOC teams automate repetitive tasks, improve incident response efficiency, and reduce operational workload.	▪ Retail ▪ BFSI ▪ Telecommunications ▪ Media and entertainment ▪ Healthcare and life sciences ▪ Manufacturing ▪ Government ▪ Education
Solution	Google Threat Intelligence	Google Threat Intelligence combines Mandiant expertise, VirusTotal intelligence, and Google-scale analytics to provide contextual threat insights, adversary intelligence, and enrichment capabilities that support AI-driven detection, investigation, and threat hunting within SOC environments	▪ Retail ▪ BFSI ▪ Telecommunications ▪ Media and entertainment ▪ Healthcare and life sciences ▪ Manufacturing ▪ Government ▪ Education
Solution	Google Cloud Cybershield	Google Cloud Cybershield™ provides AI-powered cyber defense capabilities for governments by combining Google Security Operations, threat intelligence, Gemini capabilities, and Mandiant expertise to modernize SOC operations, improve threat detection, automate response workflows, and enhance national cyber resilience.	▪ Retail ▪ BFSI ▪ Telecommunications ▪ Media and entertainment ▪ Healthcare and life sciences ▪ Manufacturing ▪ Government ▪ Education

JULY 2026 © MarketsandMarkets™

Service	Mandiant Threat Defense	Mandiant Threat Defense delivers AI-assisted managed threat detection, continuous threat hunting, expert-led investigations, and rapid incident response through Google SecOps, combining Google Threat Intelligence, Gemini, and automated response playbooks to strengthen enterprise AI-driven security operations.	▪ Retail ▪ BFSI ▪ Telecommunications ▪ Media and entertainment ▪ Healthcare and life sciences ▪ Manufacturing ▪ Government ▪ Education
Service	Mandiant Incident Response (IR)	Mandiant Incident Response provides expert-led incident investigation, digital forensics, malware analysis, containment, recovery, and crisis management. Leveraging Google Threat Intelligence and frontline expertise, it helps organizations rapidly contain sophisticated cyberattacks and strengthen overall security operations resilience.	▪ Retail ▪ BFSI ▪ Telecommunications ▪ Media and entertainment ▪ Healthcare and life sciences ▪ Manufacturing ▪ Government ▪ Education

Source: Company Website

15.1.5.3 Recent developments

15.1.5.3.1 Product launches/enhancements

TABLE 456 GOOGLE: PRODUCT LAUNCHES/ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
April 2026	Product Enhancement	Google (US)	Agentic SOC – Threat Hunting Agent (Solution)	Google enhanced its Agentic SOC capabilities by introducing AI-powered Threat Hunting Agent functionality, enabling autonomous discovery of emerging threats through security telemetry analysis, threat intelligence integration, and machine-scale investigation workflows.
April 2026	Product Enhancement	Google (US)	Agentic SOC – Detection Engineering Agent (Solution)	Google enhanced its Agentic SOC platform with Detection Engineering Agent capabilities that identify security coverage gaps, generate detection rules, validate detection effectiveness, and assist SOC teams in improving proactive threat detection capabilities.

JULY 2026 © MarketsandMarkets™

January 2026	Product Enhancement	Google (US)	Gemini in Google Security Operations (Solution)	Google enhanced Gemini in Security Operations by expanding assistant capabilities beyond security-specific queries, enabling broader knowledge access, coding assistance, and data analysis support directly within SOC workflows.
November 2025	Product Launch	Google (US)	Triage and Investigation Agent (Solution)	Google launched the Triage and Investigation Agent within Security Operations, enabling autonomous alert analysis, evidence collection, investigation summaries, and threat validation to reduce analyst workload and significantly accelerate security incident investigation processes.
April 2025	Product Launch	Google (US)	Google Security Operations Agentic SOC Platform (Solution)	Google launched its Agentic SOC platform, introducing Gemini-native AI agents that autonomously perform alert triage, threat investigation, threat hunting, and detection engineering workflows to reduce manual SOC effort and accelerate cyber incident response.
May 2024	Product Enhancement	Google (US)	Google Security Operations (Solution)	Google enhanced Security Operations by introducing AI-powered SecOps capabilities with Gemini integration, enabling SOC teams to accelerate investigations, generate detection rules, analyze threats, summarize intelligence, and improve analyst productivity through generative AI assistance.
May 2024	Product Launch	Google (US)	Gemini in Google Security Operations (Solution)	Google launched Gemini in Security Operations to provide generative AI assistance for SOC analysts, enabling natural language investigations, threat intelligence analysis, search summarization, YARA-L rule generation, and automated security workflow support.
May 2024	Product Enhancement	Google (US)	Google Threat Intelligence (Solution)	Google enhanced Google Threat Intelligence by integrating Gemini capabilities with Mandiant intelligence and VirusTotal data, enabling security teams to accelerate threat research, analyze adversary behavior, summarize intelligence, and improve proactive threat detection

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.5.3.2 Deals

TABLE 457 GOOGLE: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION	DEAL SIZE
May 2026	Collaboration	Google (US)	Information Services (Bulgaria)	Google collaborated with Information Services to launch Bulgaria's AI-powered National Cybershield, deploying Google Security Operations, Google Threat Intelligence, and Mandiant intelligence to establish a federated SOC that strengthens AI-driven threat detection and incident response across 54 government entities.	NA
April 2026	Partnership	Google (US)	Tata Consultancy Services (TCS) (India)	Google partnered with Tata Consultancy Services (TCS) to expand their strategic collaboration by launching TCS AI SOC enabled by Google SecOps, combining Google SecOps, Gemini, and Google Threat Intelligence to deliver AI-driven threat detection, autonomous investigations, and faster incident response.	NA
March 2026	Acquisition	Google (US)	Wiz (US)	Google completed its acquisition of Wiz, integrating its cloud and AI security platform with Google Security Operations and Google Threat Intelligence to enhance AI-powered threat prevention, detection, investigation, and response across hybrid and multicloud environments.	USD 32 billion
March 2026	Collaboration	Google (US)	SentinelOne (US)	Google collaborated with SentinelOne through a multi-year strategic agreement to deliver autonomous AI-powered security by integrating Google Security Operations, Google Threat Intelligence, and Google Cloud infrastructure with SentinelOne's AI-native security platform, strengthening enterprise threat detection and incident response.	NA

JULY 2026 © MarketsandMarkets™

January 2026	Collaboration	Google (US)	PwC (US)	Google collaborated with PwC through a three-year strategic alliance to modernize AI-powered security operations by combining Google Security Operations, Google Threat Intelligence, and agentic AI capabilities with PwC's managed security services to accelerate threat detection, investigation, and response.	USD 400 million
December 2025	Partnership	Google (US)	Deloitte India (India)	Google partnered with Deloitte India to deliver AI-powered security operations by combining Google Security Operations, Google Threat Intelligence, and Google Cloud Cybershield with Deloitte's managed security services to modernize SOCs, strengthen threat detection, and accelerate AI-driven incident response.	NA
July 2024	Partnership	Google (US)	PwC India (India)	Google partnered with PwC India to deliver Google Security Operations, an AI-powered SecOps platform, combining Gemini, Google Threat Intelligence, and PwC India's managed security expertise to accelerate threat detection, investigation, and incident response for organizations across India.	NA
June 2024	Partnership	Google (US)	Thales (France)	Google partnered with Thales to develop a global Security Operations Center (SOC) platform combining Google Security Operations, Google Threat Intelligence, VirusTotal, Mandiant intelligence, and generative AI capabilities to strengthen AI-driven cyber detection, investigation, and incident response services.	NA
April 2024	Partnership	Google (US)	Palo Alto Networks (US)	Google partnered with Palo Alto Networks to expand their strategic alliance by integrating Google Cloud AI, Google Security Operations, and Google Threat Intelligence with Palo Alto Networks' AI-powered security platforms, enabling enhanced threat detection, automated security operations, and protection for AI applications.	NA

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.5.3.3 Expansions

TABLE 458 GOOGLE: EXPANSIONS

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY	COMPANY	DESCRIPTION
June 2026	Expansion	Regional Expansion	South Korea	Google (US)	Google strengthened its regional AI security operations capabilities by introducing Google Security Operations in the Seoul Region, enabling local data residency and providing AI-driven threat detection, automated response workflows, and Google Threat Intelligence for regulated industries.
May 2024	Expansion	Regional Expansion	India	Google (US)	Google expanded its AI-powered Security Operations footprint by launching a dedicated Google Security Operations region in Mumbai, enabling organizations to store SecOps data locally while leveraging Gemini-powered investigations, AI-driven threat detection, Google Threat Intelligence, and automated incident response capabilities.

Source: Company Website and Press Releases

15.1.5.4 MnM view

15.1.5.4.1 Key strengths

Google has established a strong position in the AI SOC market through its Google Security Operations (SecOps) platform, which integrates cloud-native SIEM, SOAR, Google Threat Intelligence, Mandiant expertise, VirusTotal intelligence, and Gemini-powered AI into a unified security operations environment. Its Agentic SOC architecture enables organizations to automate alert triage, threat investigation, detection engineering, and threat hunting, helping security teams accelerate incident response, reduce analyst workload, and improve operational efficiency across hybrid and multi-cloud environments.

Google differentiates its AI SOC capabilities through its hyperscale cloud infrastructure, extensive global threat intelligence, and leadership in generative AI. Gemini-powered security agents leverage real-time intelligence from Google and Mandiant to autonomously investigate alerts, enrich security context, and generate detections while keeping analysts in the decision loop. Additionally, Google's expanding ecosystem of global consulting, MSSP, and technology partners strengthens enterprise adoption across BFSI, government, healthcare, manufacturing, telecommunications, and other regulated industries.

JULY 2026 © MarketsandMarkets™

15.1.5.4.2 Strategic choices

Google is strategically evolving security operations from AI-assisted workflows toward agentic and autonomous SOC environments by embedding Gemini-native AI agents across Google Security Operations. Rather than delivering standalone AI security tools, the company integrates AI-driven detection, investigation, threat intelligence, and response orchestration into a unified SecOps platform. This approach enables organizations to modernize SOC operations while reducing manual intervention and improving cyber resilience against increasingly sophisticated threats.

The company is also expanding its AI SOC ecosystem through strategic partnerships with global system integrators, managed security service providers, and cybersecurity vendors, alongside regional deployments of Google Security Operations to support data residency and regulatory compliance. Google continues to invest in agentic AI capabilities, enabling autonomous workflows, human-in-the-loop governance, and interoperability across enterprise security tools, positioning the company as a key provider of AI-native security operations platforms.

15.1.5.4.3 Weaknesses & competitive threats

Google faces strong competition from Microsoft, Palo Alto Networks, CrowdStrike, Cisco, IBM, and other cybersecurity vendors that continue to expand AI-powered SOC, XDR, and autonomous security platforms. Although Google benefits from advanced AI capabilities and industry-leading threat intelligence, enterprise adoption of Google Security Operations remains comparatively lower than some incumbent enterprise security ecosystems. Furthermore, organizations with heterogeneous, multi-vendor security environments may encounter integration and migration challenges when adopting Google-centric security operations solutions.

The company also faces challenges associated with the rapid adoption of autonomous AI in cybersecurity, including concerns around AI governance, explainability, regulatory compliance, and trust in AI-driven decision-making. As specialized AI security vendors continue to innovate in autonomous detection and response, Google must continuously strengthen its interoperability, AI model reliability, and security automation capabilities to maintain competitive differentiation in the evolving AI SOC market.

JULY 2026 © MarketsandMarkets™

15.1.6 SWIMLANE

15.1.6.1 Business overview

Swimlane is a US-based agentic AI automation company headquartered in Denver, Colorado. The company started as a security automation provider and has since evolved into an agentic AI automation company that helps enterprises and managed security service providers (MSSPs) address alert overload, staffing constraints, operational complexity, and the growing cognitive burden on security analysts. Its strategy combines artificial intelligence with deterministic automation to deliver faster, more scalable, and better-governed security operations. Swimlane takes a practitioner-led approach, building a platform that unifies security teams, tools, telemetry, workflows, and AI-driven decision-making in a single operating environment.

The company's flagship Swimlane Turbine platform provides the technological foundation for its AI SOC offering. Turbine combines agentic and generative AI, low-code playbooks, case management, cloud-native architecture, dashboards, reporting, and extensive API-based integrations. Hero AI is Turbine's suite of agentic AI capabilities, which is key to extending the platform beyond conventional SOC automation by pairing deterministic automation for predictable tasks with AI agents that can reason across complex security workflows.

In January 2026, the company introduced an AI Agent Workforce built on Hero AI expert agents and an agent-builder integrated into Turbine, letting organizations build and deploy specialized agents across security workflows. Swimlane reports that its AI agents and automation now perform work equivalent to more than 60,000 SOC analysts each day across its customer base. Swimlane brought these capabilities together in its Swimlane AI SOC product, first introduced in February 2026. AI SOC gives SOC teams an approachable way to harness automation and agents for investigations, remediation planning, and playbook development, all while maintaining explainability, auditability, governance, and human oversight.

Swimlane's AI SOC strategy is expanding beyond individual analyst assistance toward a full AI-enabled security workforce, supporting model selection across specific AWS Bedrock models and letting customers bring their own model (BYOM). In July 2026, the company extended its AI SOC offering to MSSPs, letting managed security providers build AI SOC services on Turbine while retaining ownership of their customer relationships, data, and services. This positions Swimlane to address both enterprise SOC modernization and the scaling needs of managed security operations.

Swimlane continues to strengthen its AI SOC market position through product innovation, strategic investment, global expansion, and ecosystem development. In 2025, the company secured USD 45 million in additional capital to fund its growth and agentic AI roadmap, developed more than 100 expert agents, and achieved 110% net revenue retention. Swimlane operates across North America, Europe, Asia Pacific, and other international markets, supported by a strategic R&D center in Hyderabad focused on advancing Turbine and AI-enabled security automation. The company serves customers in banking, finance & insurance, healthcare, energy & utilities, federal government, education, state & local government, and retail. Swimlane has also strengthened its enterprise and government positioning with FedRAMP High certification for Turbine, enabling deployment of its AI SOC capabilities in sensitive federal environments. Together, these milestones mark Swimlane's transition from traditional security automation toward a scalable, agentic AI operating model spanning SOC, vulnerability management, compliance, and other security functions.

JULY 2026 © MarketsandMarkets™

TABLE 459 SWIMLANE: BUSINESS OVERVIEW

Founded	2014
Headquarters Country	US
Headquarters City/State	Denver, Colorado
Ownership	Private

Source: Company Website

15.1.6.2 Products/Solutions/Services offered

TABLE 460 SWIMLANE: PRODUCTS/SOLUTIONS/SERVICES OFFERINGS

PRODUCT TYPE	PRODUCT/SOLUTION/ SERVICE	DESCRIPTION	VERTICAL
Platform	Swimlane Turbine	Swimlane Turbine is an agentic AI automation platform for security operations that provides the foundation for AI SOC deployments, enabling organizations to automate security workflows and orchestrate AI-driven operations across enterprise environments.	▪ Banking, Finance & Insurance ▪ Healthcare ▪ Energy & Utilities ▪ Federal Government ▪ Education, State & Local ▪ Government ▪ Retail
Solution	Swimlane AI SOC	Swimlane AI SOC is an AI-powered security operations solution that automates threat detection, alert triage, investigation, and response, enabling security teams to improve analyst productivity, accelerate incident resolution, and scale SOC operations.	▪ Banking, Finance & Insurance ▪ Healthcare ▪ Energy & Utilities ▪ Federal Government ▪ Education, State & Local ▪ Government ▪ Retail
Services	Swimlane Professional Services	Swimlane Professional Services support the deployment and implementation of Turbine and SOC automation solutions, including integration with existing security tools, workflow automation, alert triage, phishing response, threat intelligence, and incident management.	▪ Banking, Finance & Insurance ▪ Healthcare ▪ Energy & Utilities ▪ Federal Government ▪ Education, State & Local ▪ Government ▪ Retail

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.1.6.3 Recent developments

15.1.6.3.1 Product launches and enhancements

TABLE 461 SWIMLANE: PRODUCT LAUNCHES AND ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	PRODUCT DESCRIPTION
July 2026	Product Launch	Swimlane (US)	Swimlane AI SOC – for MSSPs (Solution)	Swimlane launched AI SOC for MSSPs, extending its agentic AI automation approach to managed security providers with centralized command, cross-tenant threat intelligence, AI-driven triage and investigation, and portfolio analytics to enable scalable security operations.
February 2026	Product Launch	Swimlane (US)	Swimlane AI SOC (Solution)	Swimlane launched AI SOC, an autonomous security operations solution built on Turbine that combines deep and expert AI agents to automate investigation and response, reducing analysts' cognitive workload while maintaining explainability, governance, auditability, and human control.
January 2026	Product Launch	Swimlane (US)	Swimlane Turbine – AI Agent Workforce (Platform)	Swimlane launched an AI Agent Workforce within the Turbine platform, introducing Hero AI expert agents that autonomously perform specialized security tasks while integrating with playbooks for orchestration, governance, guardrails, and human oversight across SOC operations.
November 2025	Product Launch	Swimlane (US)	Swimlane Turbine - incident response AI agents (Platform)	Swimlane launched AI agents for case management through Hero AI, enabling automated evidence gathering, correlation, triage, and explainable decision-making across security data sources to accelerate investigations and support AI-driven incident response.
September 2025	Product Enhancement	Swimlane (US)	Swimlane Turbine – Hero AI (Platform)	Swimlane enhanced Hero AI within Turbine with natural-language playbook execution, dynamic playbook discovery, and pre-execution confirmations, enabling analysts to trigger automated security responses conversationally while maintaining governance, auditability, and human oversight.
January 2025	Product Launch	Swimlane (US)	Swimlane Turbine – Hero (Platform)	Swimlane launched Hero, the industry's first private agentic AI security operations (SecOps) companion, fully integrated into the Swimlane Turbine platform. Hero provides context-aware decision support, incident summarization, recommendations, and conversational assistance to accelerate investigations and security operations.
January 2024	Product Launch	Swimlane (US)	Swimlane Turbine – Hero AI & Turbine Canvas (Platform)	Swimlane launched Hero AI and Turbine Canvas within Turbine, introducing AI-enhanced security automation, a private LLM, AI-assisted workflows, and a low-code visual automation studio designed to accelerate SOC playbook development and analyst productivity.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.6.3.2 Deals

TABLE 462 SWIMLANE: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1 NAME	COMPANY 2 NAME	DESCRIPTION	DEAL SIZE
June 2026	Partnership	Swimlane (US)	Knox Systems (US)	Swimlane achieved Federal Risk and Authorization Management Program (FedRAMP) High Authorization for its Swimlane Turbine agentic AI platform in partnership with Knox Systems, enabling federal agencies to deploy explainable, auditable AI SOC capabilities across demanding security environments.	NA
January 2026	Partnership	Swimlane (US)	Wiz (US)	Swimlane partnered with Wiz by joining the Wiz Integration Network, combining Wiz's real-time cloud risk visibility with Turbine's agentic AI automation to accelerate cloud vulnerability response and risk remediation for mutual customers.	NA
August 2024	Partnership	Swimlane (US)	Macnica (Japan)	Swimlane partnered with Macnica through an exclusive global agreement to expand Turbine adoption across APJ and META, enabling distributors and resellers to deliver AI-enhanced security automation and establish regional automation practices.	NA
May 2024	Partnership & Distribution Agreement	Swimlane (US)	Wavelink (Australia)	Swimlane partnered with Wavelink to distribute its AI-enhanced security automation platform across Australia and New Zealand, expanding regional access to Turbine while providing channel partners with implementation support and cybersecurity services.	NA
February 2024	Partnership	Swimlane (US)	NTT DATA (Japan)	Swimlane partnered with NTT DATA as a global security automation partner, combining Turbine's AI-enabled automation with NTT DATA's global services to deliver scalable security operations and automation capabilities for clients worldwide.	NA

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.7 LUMU TECHNOLOGIES

15.1.7.1 Business overview

Lumu Technologies is a US-based cybersecurity company founded in 2020 and headquartered in Doral, Florida, US. The company specializes in AI-driven security operations and Continuous Compromise Assessment (CCA), a patented cybersecurity model that enables organizations to continuously measure, detect, and respond to confirmed cyber compromises in real time. Leveraging network metadata, proprietary artificial intelligence, advanced analytics, and threat intelligence, Lumu provides continuous visibility into malicious activities, helping organizations strengthen cyber resilience and improve security operations.

The company's cybersecurity portfolio comprises the Lumu SecOps Platform, which includes Lumu Defender, Lumu Autopilot, Lumu Discover, Lumu Archive, and Maltiverse. The company's flagship Lumu SecOps Platform unifies Network Detection and Response (NDR), AI-powered security automation, autonomous incident response, threat intelligence, attack surface visibility, and compliance capabilities within a single platform. Its core portfolio includes Lumu Defender for network detection and response, Lumu Autopilot for AI-powered autonomous incident investigation and response, CCA for real-time compromise measurement, Lumu Discover for external attack surface visibility, Maltiverse by Lumu for threat intelligence, and Lumu Archive for long-term network log retention and retrospective threat hunting. These capabilities enable security teams to streamline security operations, reduce alert fatigue, accelerate incident response, and improve overall SOC efficiency.

Lumu serves organizations of all sizes across industries, including financial services, healthcare, education, government, technology, telecommunications, and managed security service providers (MSSPs). Its platform is designed to protect hybrid IT environments spanning on-premises infrastructure, public and private clouds, remote users, and distributed enterprise networks. Through an extensive ecosystem of integrations with SIEM, XDR, EDR, SOAR, firewalls, identity security, and other cybersecurity technologies, Lumu enables organizations to maximize existing security investments while enhancing operational effectiveness.

Lumu continues to strengthen its position in the AI SOC market through continuous product innovation, AI-powered automation, and strategic ecosystem expansion. Recent developments include the launch of the Lumu SecOps Platform, the introduction of Lumu Autopilot for autonomous security operations, the acquisition of Maltiverse to enhance threat intelligence capabilities, and technology integrations with vendors such as CrowdStrike to accelerate AI-driven threat detection, investigation, and response. These initiatives reinforce the company's focus on delivering intelligent, automated, and scalable security operations for modern enterprises.

TABLE 463 LUMU TECHNOLOGIES: COMPANY OVERVIEW

Founding Year	2020
Headquarters Country	US
Headquarters City/State	Doral, Florida
Ownership Type	Private

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.1.7.2 Products/Solutions/Services offered

TABLE 464 LUMU TECHNOLOGIES: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/ SERVICE	DESCRIPTION	VERTICAL
Platform	Lumu SecOps Platform	Lumu SecOps Platform is an AI-powered cloud-native Security Operations (SecOps) platform that unifies continuous threat detection, investigation, response, automation, and security operations using network metadata, advanced analytics, and threat intelligence to accelerate cyber incident detection and remediation.	▪ Enterprise ▪ State and local government ▪ Financial services ▪ K-12 & education ▪ Healthcare
Solution	Lumu Autopilot	Lumu Autopilot is an AI-powered autonomous security operations solution that leverages AI-driven playbooks to prioritize, investigate, respond to, and escalate security incidents automatically, enabling 24×7 virtual SOC operations while reducing analyst workload and accelerating incident resolution.	▪ Enterprise ▪ State and local government ▪ Financial services ▪ K-12 & education ▪ Healthcare
Solution	Lumu Defender	Lumu Defender is the unified visibility and orchestration engine powering Lumu's Agentic AI SOC. It continuously ingests network, endpoint, and cloud telemetry, leveraging Lumu AI to deliver autonomous threat detection, context, and cross-stack mitigation.	▪ Enterprise ▪ State and local government ▪ Financial services ▪ K-12 & education ▪ Healthcare

Source: Company Website

15.1.7.3 Recent developments

15.1.7.3.1 Product launches/enhancements

TABLE 465 LUMU TECHNOLOGIES: PRODUCT LAUNCHES/ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
May 2026	Product Enhancement	Lumu Technologies (US)	Lumu Autopilot (Solution)	Lumu Technologies enhanced Lumu Autopilot by introducing the industry's first proven Agentic SOC, enabling autonomous investigation and remediation of confirmed compromises through AI-driven workflows, significantly reducing manual triage and accelerating security operations.

JULY 2026 © MarketsandMarkets™

April 2026	Product Enhancement	Lumu Technologies (US)	Lumu Defender (Solution)	Lumu enhanced Lumu Defender by extending Continuous Compromise Assessment beyond the network to include endpoint, cloud, and identity visibility, providing unified threat detection across enterprise environments.
April 2025	Product Launch	Lumu Technologies (US)	Lumu SecOps Platform (Solution)	Lumu Technologies launched the Lumu SecOps Platform, a unified security operations solution integrating network detection and response, AI-driven automation, threat intelligence, compliance, and attack surface visibility to streamline threat detection, investigation, and response.
April 2024	Product Launch	Lumu Technologies (US)	Lumu Autopilot (Solution)	Lumu Technologies launched Lumu Autopilot, a patented, AI-powered autonomous cybersecurity incident response and management solution (recognized under U.S. Patent No. 12,712,891) that acts as a virtual security operations team by automatically investigating, prioritizing, and responding to security incidents while enabling continuous 24×7 SOC operations.

Source: Company Website and Press Releases

15.1.7.3.2 Deals

TABLE 466 LUMU TECHNOLOGIES: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
March 2025	Acquisition	Lumu Technologies (US)	Maltiverse (Spain)	Lumu Technologies acquired Maltiverse, a Spain-based cyber threat intelligence company, to strengthen its AI-driven security operations by integrating curated threat intelligence, enriched indicators of compromise, and advanced threat context into its SecOps Platform and Continuous Compromise Assessment capabilities.
May 2024	Integration	Lumu Technologies (US)	CrowdStrike (US)	Lumu Technologies integrated its CCA platform with the CrowdStrike Falcon XDR platform to automate threat detection, investigation, and response, enabling organizations to accelerate security operations through AI-driven workflows and network-centric threat intelligence.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.7.3.3 Expansions

TABLE 467 LUMU TECHNOLOGIES: EXPANSIONS

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY	COMPANY	DESCRIPTION
January 2026	Expansion	Global Leadership Expansion	Global	Lumu Technologies (US)	Lumu Technologies expanded its global leadership team by appointing senior executives across sales, marketing, customer success, and engineering to support growing worldwide demand for AI-driven security operations and accelerate adoption of its AI-powered SecOps platform.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.8 EXAFORCE

15.1.8.1 Business overview

Exaforce is a US-based AI-native cybersecurity company specializing in agentic security operations and real-time security reasoning. The company focuses on transforming Security Operations Centers (SOCs) through a combination of multi-model AI, autonomous AI agents, and a unified real-time security data platform. Exaforce is positioned around reducing the operational burden associated with alert volumes, fragmented security telemetry, and manual investigation workflows. Its approach moves beyond conventional SIEM, SOAR, and UEBA architectures by bringing core security operations together within an integrated agentic SOC environment. Exaforce's platform provides security teams with continuous visibility across cloud, SaaS, identity, endpoint, and other enterprise environments while enabling AI-driven reasoning and automated security operations.

The company's flagship Exaforce Agentic AI SOC Platform provides the foundation for its AI SOC proposition, combining a unified real-time security data platform, multi-model AI engine, and four specialized autonomous AI agents known as Exabots - Exabot Detect, Exabot Triage, Exabot Investigate, and Exabot Respond. These agents support detection, alert triage, investigation, threat hunting, and response, enabling security teams to operate on a unified view of security activity and context. Its multi-model AI architecture combines Semantic, Behavioral, and Knowledge Models to establish relationships between identities, resources, and activities, identify behavioral anomalies, and apply contextual reasoning using business rules, historical outcomes, and large language models. This architecture is designed to produce more deterministic, explainable, and auditable security decisions than approaches relying solely on large language models. Exaforce also provides conversational and visual investigation capabilities that allow analysts to explore security data without extensive reliance on complex queries or manual data correlation.

Within the AI SOC market, Exaforce extends security operations from conventional analyst-led workflows toward autonomous, full-lifecycle SOC operations. Its agentic approach automatically filters false positives, correlates related findings, enriches alerts with identity and behavioral context, and supports deeper investigations, threat hunting, and response. This allows security teams to reduce manual investigation effort, improve response speed, and scale SOC operations without proportionally increasing analyst workload. Exaforce's AI SOC approach also addresses the shortage of skilled security personnel by enabling AI agents to perform activities traditionally distributed across multiple SOC analyst tiers. The company complements its platform with Exaforce MDR, an AI-native managed detection and response service that combines Exabots with expert security analysts to provide 24/7 monitoring, threat hunting, investigation, and response.

Exaforce serves organizations across technology, financial services, healthcare, manufacturing, energy, fintech, and other high-target industries, supporting security operations across cloud, identity, endpoint, SaaS, and code environments. The company also has a growing global presence across North America, Europe, and Asia Pacific, with operations and/or teams in the US, Europe, India, and Japan, supporting regional deployments and data-sovereignty requirements.

Exaforce continues to strengthen its position in the AI SOC market through product innovation, investment, and international expansion. In August 2025, the company formally introduced its full-lifecycle Agentic AI SOC proposition, bringing AI across detection, triage, investigation, and response. In May 2026, Exaforce raised USD 125 million in Series B funding, following its USD 75 million Series A in 2025, bringing total funding to USD 200 million and supporting expansion of its AI-native security operations platform and real-time reasoning capabilities. The company subsequently launched ExaGo, an AI voice-powered mobile AI SOC application, in July 2026, extending AI-driven security investigation and response to mobile workflows. Exaforce has also expanded internationally, including establishing a Tokyo presence with local engineering and MDR teams to support Japanese customers. These initiatives reinforce its strategy of building an AI-

JULY 2026 © MarketsandMarkets™

native SOC that combines autonomous agents, contextual security data, multi-model reasoning, and human expertise to improve the speed, scale, and effectiveness of modern security operations.

TABLE 468 EXAFORCE: BUSINESS OVERVIEW

Founded	2023
Headquarters Country	US
Headquarters City/State	San Jose, California
Ownership	Private

Source: Company Website

15.1.8.2 Products/Solutions/Services offered

TABLE 469 EXAFORCE: PRODUCTS/SOLUTIONS/SERVICES OFFERINGS

PRODUCT TYPE	PRODUCT/SOLUTION/ SERVICE	DESCRIPTION	VERTICAL
Platform	Exaforce Agentic AI SOC	Exaforce Agentic AI SOC Platform is an AI-native security operations platform that combines a unified, real-time security data layer with four specialized Exabots to automate detection, triage, investigation, and response across cloud, SaaS, identity, and endpoint environments.	▪ Healthcare ▪ Technology ▪ Financial Services ▪ Energy ▪ Manufacturing
Solution	Exaforce AI for SOC	Exaforce AI for SOC applies agentic AI across the security operations lifecycle, enabling autonomous alert triage, investigation, threat hunting, and incident response while reducing alert fatigue and extending analyst capabilities without proportional headcount increases.	▪ Healthcare ▪ Technology ▪ Financial Services ▪ Energy ▪ Manufacturing
Service	Exaforce MDR	Exaforce MDR combines expert security analysts with Exaforce's agentic AI platform to provide 24/7 managed detection and response, covering threat detection, triage, investigation, and response on behalf of customers.	▪ Healthcare ▪ Technology ▪ Financial Services ▪ Energy ▪ Manufacturing

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.1.8.3 Recent developments

15.1.8.3.1 Product launches and enhancements

TABLE 470 EXAFORCE: PRODUCT LAUNCHES AND ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	PRODUCT DESCRIPTION
July 2026	Product Launch	Exaforce (US)	ExaGo (AI SOC Mobile Application)	Exaforce launched ExaGo, an AI voice-powered mobile SOC application that enables analysts to investigate threats, receive spoken security insights, approve response actions, generate reports, and manage incidents through natural-language conversations.
June 2026	Product Enhancement	Exaforce (US)	Exaforce Agentic AI SOC (Platform)	Exaforce enhanced its AI SOC platform to monitor Claude activity with identity-graph context, sensitive-chat labeling, and behavioral threat detection, helping security teams identify risks associated with enterprise use of AI applications.
August 2025	Product Launch	Exaforce (US)	Exaforce Agentic AI SOC (Platform)	Exaforce launched its agentic AI SOC platform, combining a unified real-time security data layer with four specialized Exabots to automate detection, triage, investigation, and response across cloud, SaaS, identity, and endpoint environments.
August 2025	Product Launch	Exaforce (US)	Exaforce MDR (Service)	Exaforce launched its MDR service, combining its agentic AI capabilities with expert security analysts to deliver 24/7 managed monitoring, proactive threat hunting, contextual investigation, and rapid containment and response for organizations without sufficient in-house SOC resources.

Source: Company Website and Press Releases

15.1.8.3.2 Deals

TABLE 471 EXAFORCE: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1 NAME	COMPANY 2 NAME	DESCRIPTION
July 2026	Collaboration	Exaforce (US)	ExtraHop (US)	Exaforce collaborated with ExtraHop through the Agentic SOC Alliance to combine Exabots with ExtraHop RevealX 360 network intelligence, providing high-fidelity network context for autonomous detection, investigation, and response.
May 2026	Partnership	Exaforce (US)	KDDI America (US)	Exaforce partnered with KDDI America to expand its agentic AI security operations capabilities in the US market, leveraging KDDI's enterprise presence and security expertise to extend Exaforce's AI-native SOC platform to customers.

JULY 2026 © MarketsandMarkets™

May 2026	Partnership	Exaforce (US)	KDDI Europe (UK)	Exaforce partnered with KDDI Europe to accelerate its global expansion and extend agentic AI security capabilities across European markets, leveraging KDDI's regional enterprise network to support adoption of Exaforce's AI-native SOC platform.
April 2026	Partnership	Exaforce (US)	Wiz (US)	Exaforce partnered with Wiz through the Wiz Integration Network to connect cloud security findings with SOC workflows, enabling automated correlation, investigation, triage, and response using Exaforce's agentic AI.
October 2025	Partnership	Exaforce (US)	Fuze (UAE)	Exaforce partnered with Fuze to provide AI-powered managed detection and response for its digital-asset and stablecoin infrastructure, enabling continuous monitoring, automated alert triage, investigation, and incident response across critical environments.

Source: Company Website and Press Releases

15.1.8.3.3 Expansions

TABLE 472 EXAFORCE: EXPANSIONS

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY/ REGION	COMPANY	DESCRIPTION
March 2026	Expansion	Regional Expansion	Japan	Exaforce (US)	Exaforce expanded into Japan by opening a new Tokyo office with dedicated engineering and MDR teams, strengthening its agentic SOC presence through localized deployments, Japanese-language support, data-sovereign operations, and 24/7 AI-driven detection and response for Japanese customers.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.9 SOPHOS

15.1.9.1 Business overview

Sophos is a global cybersecurity company specializing in AI-native cyber defense and managed security operations, helping organizations combat increasingly sophisticated cyber threats through a unified, intelligence-driven security architecture. Since becoming a privately held company following its acquisition by Thoma Bravo in 2020, Sophos has accelerated investments in AI, cloud-native security, and managed security services to strengthen its cybersecurity portfolio. The company protects more than 625,000 organizations worldwide with an extensive portfolio spanning endpoint, network, cloud, email, identity, XDR, SIEM, and Managed Detection and Response (MDR). Supported by one of the industry's largest ecosystems of managed service providers (MSPs), managed security service providers (MSSPs), resellers, and technology partners, Sophos delivers integrated cybersecurity solutions that combine AI, automation, and human expertise to improve cyber resilience across organizations of all sizes.

Within the AI SOC market, Sophos has significantly strengthened its position with the launch of Sophos Fusion, its AI-native cybersecurity defense system designed to unify security operations, endpoint, network, identity, cloud, email, XDR, MDR, and next-generation SIEM within a single open architecture. Built on agentic AI and synchronized security principles, Sophos Fusion enables coordinated prevention, detection, investigation, and response across native and third-party security controls. The platform leverages AI to automate routine SOC tasks while enabling human analysts to focus on complex investigations, allowing organizations to accelerate incident response, improve operational efficiency, and defend against AI-enabled cyberattacks at machine speed.

A major milestone in Sophos' AI SOC strategy was its USD 859 million acquisition of Secureworks, which substantially expanded its managed security services, threat intelligence, and cloud-native security operations capabilities. The integration of Secureworks Taegis analytics, the Counter Threat Unit (CTU), and advanced XDR technologies into the Sophos ecosystem has strengthened Sophos' AI-driven MDR, Next-Gen SIEM, and XDR offerings while significantly increasing telemetry, threat intelligence, and AI training data. This combination enables Sophos to deliver an open security operations platform with hundreds of integrations, identity threat detection and response (ITDR), AI-powered analytics, and richer threat intelligence for enterprises operating heterogeneous IT environments.

Sophos continues to strengthen its AI SOC strategy through investments in agentic AI, autonomous security operations, and an open security ecosystem. The company has enhanced its MDR, XDR, and Next-Gen SIEM capabilities, introduced Sophos Fusion, and expanded AI-driven cyber governance through the acquisition of Arco Cyber. Together with AI-native security operations, human-led MDR expertise, and an expanding partner ecosystem, these initiatives enable organizations to modernize SOCs, improve operational efficiency, and accelerate threat detection and response while strengthening overall cyber resilience.

TABLE 473 SOPHOS: COMPANY OVERVIEW

Founding Year	1985
Headquarters Country	UK
Headquarters City/State	Abingdon, Oxfordshire
Ownership Type	Private (Acquired by the private equity firm Thoma Bravo)

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.1.9.2 Products/Solutions/Services offered

TABLE 474 SOPHOS: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/ SERVICE	DESCRIPTION	VERTICAL
Solution	Sophos Fusion	Sophos Fusion is an AI-native cybersecurity defense system that unifies endpoint, network, identity, email, cloud, SIEM, XDR, MDR, and threat intelligence into a single architecture, enabling coordinated AI-driven prevention, detection, investigation, and response across enterprise security operations.	▪ Education ▪ Finance and banking ▪ Government ▪ Healthcare ▪ Manufacturing ▪ Retail
Service	Sophos Managed Detection and Response (MDR)	Sophos Managed Detection and Response (MDR) is a fully managed detection and response service combining agentic AI with 24×7 human-led monitoring, threat hunting, investigation, containment, and remediation across Sophos and third-party security environments through an AI-native SOC.	▪ Education ▪ Finance and banking ▪ Government ▪ Healthcare ▪ Manufacturing ▪ Retail
Solution	Sophos XDR	Sophos XDR is an extended detection and response platform that correlates endpoint, network, cloud, identity, and email telemetry, leveraging AI-powered analytics and threat intelligence to accelerate investigations, threat hunting, and incident response within modern SOCs.	▪ Education ▪ Finance and banking ▪ Government ▪ Healthcare ▪ Manufacturing ▪ Retail
Solution	Sophos Next-Gen SIEM	Sophos Next-Gen SIEM is a cloud-native AI-powered SIEM providing centralized security analytics, AI-assisted investigations, threat correlation, behavioral detection, and integrated SOAR capabilities to improve SOC visibility, detection fidelity, and response efficiency.	▪ Education ▪ Finance and banking ▪ Government ▪ Healthcare ▪ Manufacturing ▪ Retail

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.1.9.3 Recent developments

15.1.9.3.1 Product launches/enhancements

TABLE 475 SOPHOS: PRODUCT LAUNCHES/ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
July 2026	Product Launch	Sophos (UK)	Sophos Fusion (Solution)	Sophos launched Sophos Fusion, an AI-native cybersecurity defense system that unifies XDR, MDR, SIEM, endpoint, identity, cloud, email, network security, and threat intelligence into a coordinated AI-driven security operations platform.
July 2026	Product Launch	Sophos (UK)	Sophos Next-Gen SIEM (Solution)	Sophos launched Next-Gen SIEM as an integrated extension of Sophos Fusion, XDR, and MDR, providing AI-assisted data ingestion, long-term log retention, compliance reporting, centralized analytics, and enhanced threat investigations.
July 2026	Product Enhancement	Sophos (UK)	Sophos XDR (Solution)	Sophos enhanced Sophos XDR by integrating Secureworks Taegis analytics, adding thousands of new detection rules, built-in SOAR playbooks, improved analyst workflows, and higher-fidelity AI-powered threat detection and response capabilities.
July 2026	Product Enhancement	Sophos (UK)	Sophos Managed Detection and Response (MDR) (Service)	Sophos enhanced MDR with continuous AI-enabled threat hunting, expanded response across endpoint, firewall, cloud, email, and identity environments, and deeper integration with Sophos Fusion to strengthen AI-driven security operations
February 2026	Product Enhancement	Sophos (UK)	Sophos Managed Detection and Response (MDR) (Service)	Sophos enhanced its MDR service by deploying specialized AI agents that automate alert triage, evidence correlation, malware analysis, investigation workflows, and response recommendations, enabling its Agentic SOC to resolve threats significantly faster.
February 2025	Product Enhancement	Sophos (UK)	Sophos XDR – AI Assistant (Solution)	Sophos enhanced Sophos XDR by introducing the AI Assistant, a generative AI capability that accelerates investigations through natural-language queries, case summarization, threat intelligence enrichment, and AI-guided incident analysis for SOC analysts.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.9.3.2 Deals

TABLE 476 SOPHOS: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION	DEAL SIZE
February 2025	Acquisition	Sophos (UK)	Secureworks (US)	Sophos completed the acquisition of Secureworks, enabling integration of the Taegis cloud-native XDR platform, AI-powered analytics, detection engineering, and managed detection and response capabilities into Sophos' unified AI SOC portfolio.	USD 859 million
February 2025	Partnership	Sophos (UK)	Stellar Cyber (US)	Sophos partnered with Stellar Cyber to integrate Sophos MDR with the Stellar Cyber Open XDR platform, delivering unified AI-driven threat detection, investigation, and response across hybrid security environments while improving SOC visibility and operational efficiency.	NA

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.10 IBM

15.1.10.1 Business overview

IBM Corporation is a leading global cybersecurity and consulting company committed to hybrid cloud, AI, enterprise software, and cybersecurity solutions. Through IBM Consulting, IBM Software, and IBM X-Force, the company helps enterprises strengthen cyber resilience, modernize security operations, and secure increasingly complex hybrid and multi-cloud environments. Its cybersecurity portfolio spans threat detection and response, threat intelligence, incident response, AI security, security automation, governance, and managed security services, supported by watsonx AI and IBM's global consulting expertise.

Within the AI SOC market, IBM delivers an AI-native security operations portfolio centered on the Autonomous Threat Operations Machine (ATOM), an agentic AI orchestration engine that powers autonomous Security Operations Centers. The company's AI SOC offerings include Threat Detection and Response (TDR) Services, X-Force Predictive Threat Intelligence, IBM Consulting Autonomous Security, and AI-powered investigation capabilities that automate threat hunting, alert triage, investigation planning, detection optimization, and remediation across heterogeneous security environments. Unlike product-centric security vendors, IBM combines AI-driven automation with managed security services, consulting, and an open integration model to help enterprises modernize existing SOC infrastructures.

IBM serves organizations across financial services, government, healthcare and life sciences, IT and telecommunications, retail, energy and resources, education, automotive and other highly regulated industries. The company maintains a significant global presence across North America, Europe, Asia Pacific, Latin America, the Middle East, and Africa, supported by IBM Consulting, X-Force cybersecurity teams, global delivery centers, and an extensive partner ecosystem that enables enterprise-scale deployment of AI-driven security operations.

IBM is accelerating the evolution of autonomous security operations through continued investments in agentic AI, predictive cyber intelligence, and interoperable security architectures. Recent advancements include the introduction of the ATOM, enhanced AI-powered TDR capabilities, and strategic collaborations with CrowdStrike, Palo Alto Networks, Microsoft, and Google Cloud to extend autonomous threat detection, investigation, and response across heterogeneous enterprise environments. By combining AI orchestration, X-Force threat intelligence, industry-specific AI models, and consulting-led cybersecurity expertise, IBM is reinforcing its position as a trusted provider of autonomous, AI-driven security operations for global enterprises.

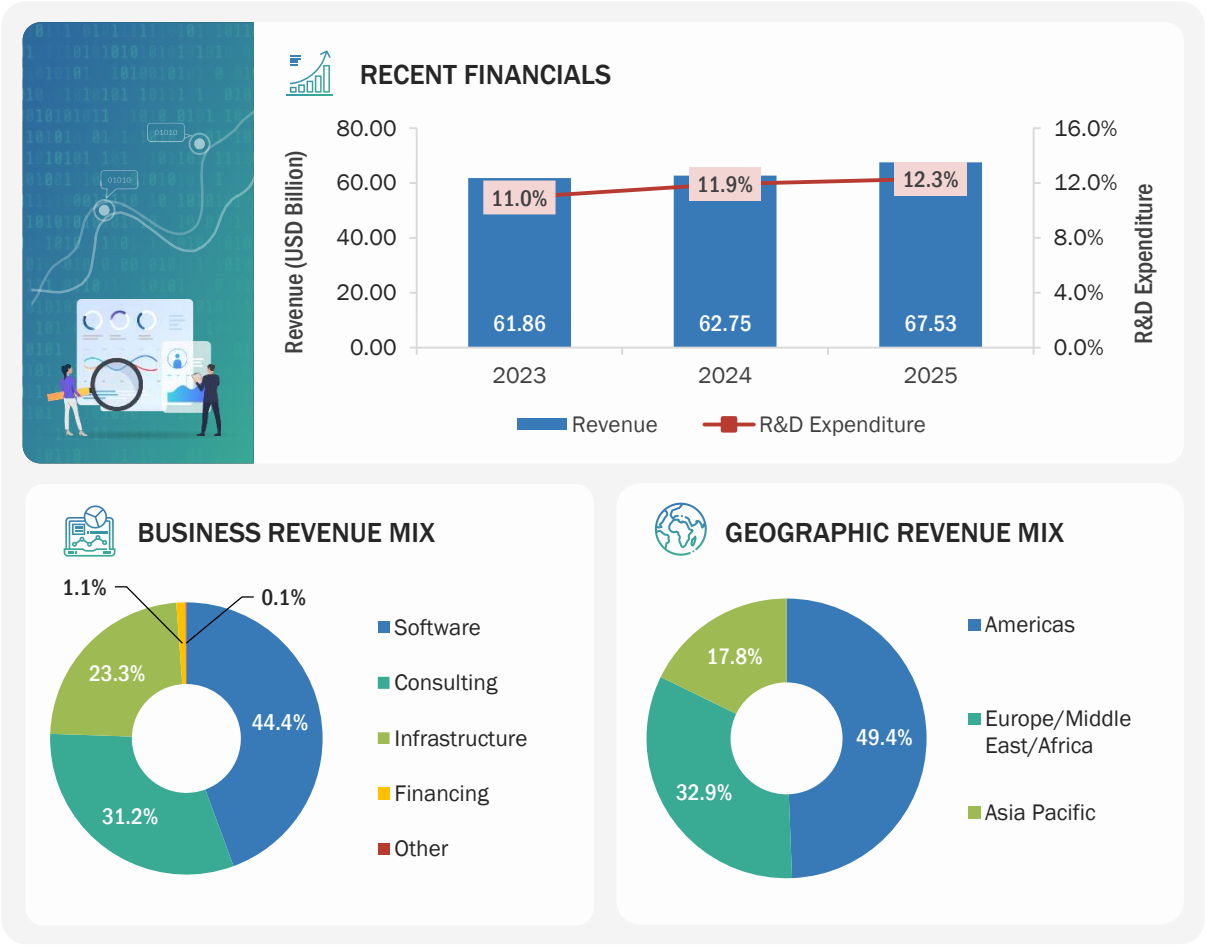
TABLE 477 IBM: COMPANY OVERVIEW

Founding Year	1911
Headquarters Country	US
Headquarters City/State	Armonk, New York
Ownership Type	Public (NYSE: IBM)

Source: Company Website, Annual Reports, and SEC Filings

JULY 2026 © MarketsandMarkets™

FIGURE 54 IBM: COMPANY SNAPSHOT



Source: Company Website and Annual Reports.

15.1.10.2 Products/Solutions/Services offered

TABLE 478 IBM: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/ SERVICE	DESCRIPTION	VERTICAL
Solution	Autonomous Threat Operations Machine (ATOM)	IBM's Autonomous Threat Operations Machine (ATOM) is an agentic AI-powered security operations solution that orchestrates multiple AI agents to automate threat hunting, alert triage, investigation planning, predictive threat intelligence, and remediation across the entire SOC lifecycle.	▪ Automotive ▪ Energy & resources ▪ Financial services ▪ Government ▪ Healthcare & life sciences ▪ Private equity ▪ Retail ▪ Telecommunications

JULY 2026 © MarketsandMarkets™

Service	Threat Detection and Response (TDR) Services	IBM Threat Detection and Response Services provide AI-driven, 24×7 managed security operations that combine continuous monitoring, threat detection, investigation, incident response, and automated remediation through the ATOM orchestration engine and IBM X-Force expertise	▪ Automotive ▪ Energy & resources ▪ Financial services ▪ Government ▪ Healthcare & life sciences ▪ Private equity ▪ Retail ▪ Telecommunications
Service	X-Force Predictive Threat Intelligence (PTI)	IBM X-Force Predictive Threat Intelligence is an AI-powered threat intelligence service that leverages industry-specific foundation models to predict adversary activity, automate threat hunting, prioritize emerging risks, and strengthen proactive security operations within autonomous SOC environments.	▪ Automotive ▪ Energy & resources ▪ Financial services ▪ Government ▪ Healthcare & life sciences ▪ Private equity ▪ Retail ▪ Telecommunications
Service	IBM Consulting Cybersecurity Assistant	The IBM Consulting Cybersecurity Assistant is a generative AI-powered tool built into the IBM Consulting Advantage platform. It accelerates threat investigations, automates operational tasks, and streamlines the resolution and escalation of critical security alerts.	▪ Automotive ▪ Energy & resources ▪ Financial services ▪ Government ▪ Healthcare & life sciences ▪ Private equity ▪ Retail ▪ Telecommunications
Service	IBM Consulting Cybersecurity Services – Autonomous Security	IBM Consulting Autonomous Security Services combine Autonomous Threat Operations Machine (ATOM), Autonomous Defense Agents (ADA), and Autonomous Risk Governance Orchestrator (ARGO) to deliver AI-native security operations, continuous risk management, automated defense, and autonomous incident response.	▪ Automotive ▪ Energy & resources ▪ Financial services ▪ Government ▪ Healthcare & life sciences ▪ Private equity ▪ Retail ▪ Telecommunications

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.1.10.3 Recent developments

15.1.10.3.1 Product launches/enhancements

TABLE 479 IBM: PRODUCT LAUNCHES/ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
May 2025	Product Launch	IBM (US)	QRadar Investigation Assistant (Solution)	IBM launched QRadar Investigation Assistant, a watsonx.ai-powered solution that generates AI-driven incident summaries, automates threat enrichment, recommends response actions, and accelerates investigations using natural language interactions within QRadar SIEM.
April 2025	Product Launch	IBM (US)	Autonomous Threat Operations Machine (ATOM) (Solution)	IBM launched Autonomous Threat Operations Machine (ATOM), an agentic AI-powered security operations solution that automates threat hunting, alert triage, investigation planning, predictive threat intelligence, and remediation through coordinated AI agents across the SOC lifecycle.
April 2025	Product Launch	IBM (US)	X-Force Predictive Threat Intelligence (Service)	IBM launched X-Force Predictive Threat Intelligence, an AI-powered service that uses industry-specific foundation models to predict adversary activity, prioritize emerging cyber risks, automate threat hunting, and strengthen proactive security operations.
August 2024	Product Launch	IBM (US)	IBM Consulting Cybersecurity Assistant (Service)	IBM launched the IBM Consulting Cybersecurity Assistant, a generative AI-powered capability for Threat Detection and Response Services that accelerates alert identification, threat investigation, incident response, and security operations by leveraging watsonx AI and existing automation technologies.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.10.3.2 Deals

TABLE 480 IBM: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
June 2026	Partnership	IBM (US)	OpenAI (US)	IBM partnered with OpenAI by joining the OpenAI Daybreak Cyber Partner Program to integrate frontier AI into enterprise security operations. The collaboration enables AI-powered vulnerability validation, application security, and advanced cyber defense workflows through IBM Consulting services.
March 2026	Partnership	IBM (US)	CrowdStrike (US)	IBM partnered with CrowdStrike to expand their AI security collaboration by integrating CrowdStrike Charlotte AI with IBM's Autonomous Threat Operations Machine (ATOM), enabling coordinated threat investigations, machine-speed containment, and managed Agentic SOC transformation across enterprise environments.
July 2024	Partnership	IBM (US)	Microsoft (US)	IBM collaborated with Microsoft to modernize security operations by combining IBM Threat Detection and Response Cloud Native services with Microsoft Sentinel, Defender XDR, and Defender for Cloud, enhancing AI-driven threat detection and automated incident response.
May 2024	Partnership	IBM (US)	Palo Alto Networks (US)	IBM partnered with Palo Alto Networks to deliver AI-powered security offerings by integrating watsonx AI with Cortex XSIAM, expanding IBM Consulting security services, and enabling seamless migration of QRadar SaaS customers to next-generation AI-powered SOC platforms.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.10.3.3 Expansions

TABLE 481 IBM: EXPANSIONS

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY	COMPANY	DESCRIPTION
July 2025	Expansion	Innovation Center Launch	India	IBM (US)	IBM launched the Agentic AI Innovation Center in Bengaluru to help enterprises, developers, and partners co-create, test, and deploy autonomous AI agents. The center supports enterprise AI innovation, including AI-powered cybersecurity, autonomous operations, governance, and intelligent workflow automation.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.11 FORTINET

15.1.11.1 Business overview

Fortinet is a distinguished cybersecurity company, built around the convergence of networking and security, delivering an integrated platform that enables organizations to secure users, devices, applications, and data through a unified Security Fabric architecture. Rather than relying on disconnected point products, the company emphasizes tightly integrated security capabilities that span network security, cloud security, endpoint protection, Zero Trust access, security operations, AI security, and managed security services. Supported by FortiGuard Labs, one of the industry's largest threat intelligence organizations, and a portfolio of more than 50 enterprise-grade products, Fortinet combines AI, machine learning, and real-time threat intelligence to help organizations strengthen cyber resilience across increasingly distributed IT environments.

In the AI SOC market, Fortinet is advancing a platform-centric approach to security operations through FortiSOC, FortiSIEM, FortiSOAR, FortiAnalyzer, FortiAI, and FortiGuard SOC-as-a-Service. These solutions unify SIEM, SOAR, threat intelligence, identity threat detection, security analytics, and agentic AI into a cloud-native security operations platform that enables organizations to automate alert triage, threat investigation, detection engineering, and incident response. Built on the Fortinet Security Fabric, the platform consolidates telemetry across networks, endpoints, cloud, email, and operational technology (OT) environments, enabling SOC teams to improve visibility, accelerate response, and reduce operational complexity.

Fortinet serves organizations across BFSI, government and public sector, healthcare, manufacturing, retail, telecommunications, energy and utilities, education, and other critical infrastructure sectors. The company maintains a strong global footprint across North America, Europe, Asia Pacific, Latin America, and the Middle East & Africa. It is supported by an extensive channel ecosystem, global security operations expertise, FortiGuard Labs research, and cybersecurity training initiatives that help enterprises modernize security operations while addressing evolving regulatory and cyber risk requirements.

Fortinet's recent strategic direction reflects its vision of simplifying modern SecOps through AI-driven automation and unified platform operations. At the Fortinet SecOps Summit 2025, the company showcased how AI, agentic automation, and integrated security operations are reshaping the future of SOCs, emphasizing faster threat detection, autonomous investigations, and streamlined response workflows. This vision culminated in the introduction of FortiSOC, a unified cloud-native SOC platform powered by agentic AI, reinforcing Fortinet's long-term strategy of enabling predictive, AI-native, and highly automated security operations through a single integrated platform.

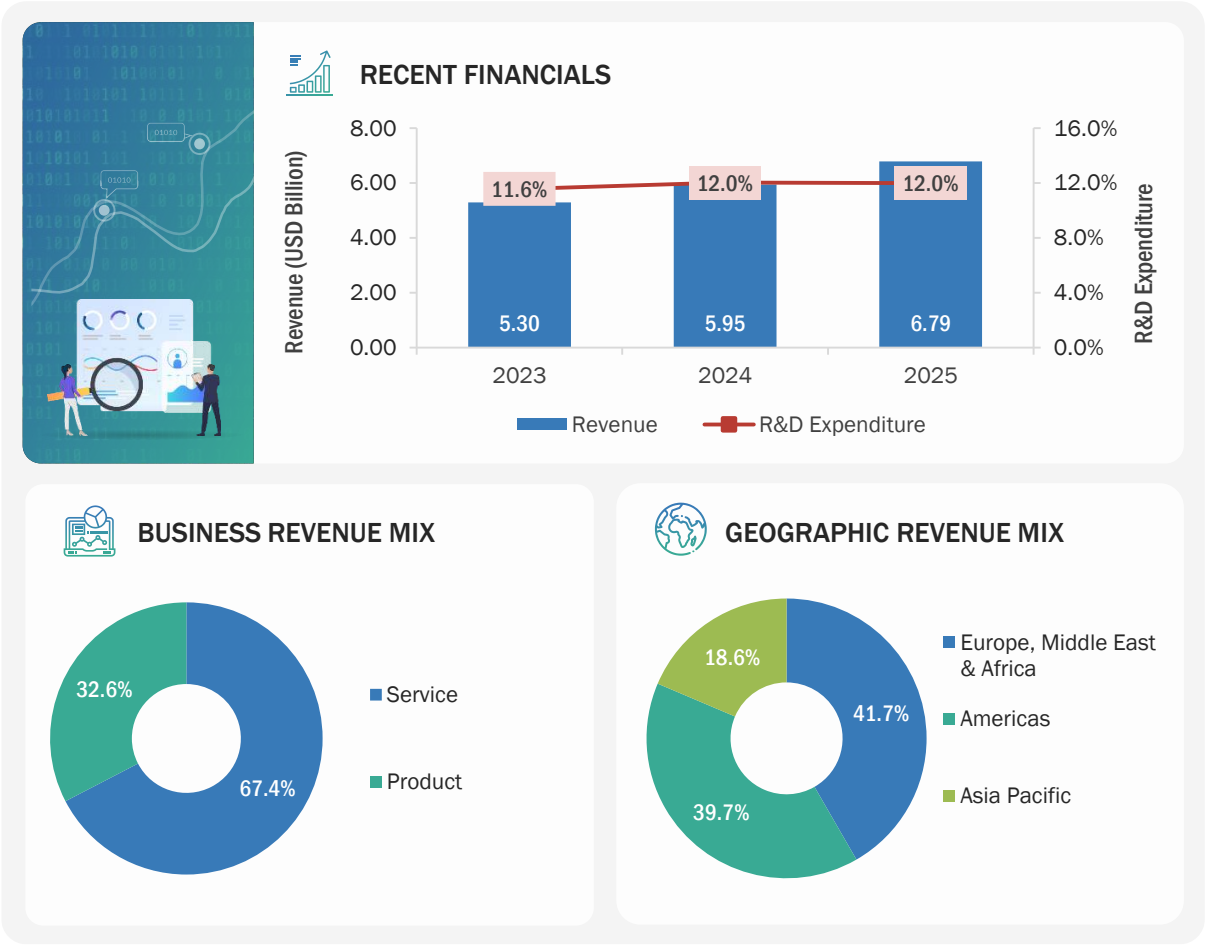
TABLE 482 FORTINET: COMPANY OVERVIEW

Founding Year	2000
Headquarters Country	US
Headquarters City/State	Sunnyvale, California
Ownership Type	Public (NASDAQ: FTNT)

Source: Company Website, Annual Reports, and SEC Filings

JULY 2026 © MarketsandMarkets™

FIGURE 55 FORTINET: COMPANY SNAPSHOT



Source: Company Website and Annual Reports.

15.1.11.2 Products/Solutions/Services offered

TABLE 483 FORTINET: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/ SERVICE	DESCRIPTION	VERTICAL
Solution	FortiSOC	FortiSOC is Fortinet's unified, cloud-delivered AI SOC platform that combines SIEM, SOAR, threat intelligence, identity threat detection, case management, and agentic AI to automate threat detection, investigation, and response through a single SaaS experience.	▪ Federal government ▪ State and local government ▪ Media and entertainment ▪ Technology ▪ Education ▪ Operational technology ▪ Manufacturing ▪ SCADA/ICS ▪ Oil & gas ▪ Power utilities ▪ Healthcare ▪ Pharmaceutical ▪ Financial services ▪ Retail

JULY 2026 © MarketsandMarkets™

			▪ Hospitality ▪ Transportation
Solution	FortiSIEM	FortiSIEM delivers AI-assisted security information and event management with enterprise-wide visibility, behavioral analytics, IT/OT threat detection, event correlation, and automated incident response across hybrid and multi-cloud environments.	▪ Federal government ▪ State and local government ▪ Media and entertainment ▪ Technology ▪ Education ▪ Operational technology ▪ Manufacturing ▪ SCADA/ICS ▪ Oil & gas ▪ Power utilities ▪ Healthcare ▪ Pharmaceutical ▪ Financial services ▪ Retail ▪ Hospitality ▪ Transportation
Solution	FortiSOAR	FortiSOAR enables AI-driven security orchestration, automation, and response by automating investigations, incident management, threat intelligence enrichment, and remediation workflows across Fortinet and third-party security environments.	▪ Federal government ▪ State and local government ▪ Media and entertainment ▪ Technology ▪ Education ▪ Operational technology ▪ Manufacturing ▪ SCADA/ICS ▪ Oil & gas ▪ Power utilities ▪ Healthcare ▪ Pharmaceutical ▪ Financial services ▪ Retail ▪ Hospitality ▪ Transportation
Solution	FortiAnalyzer	FortiAnalyzer provides a centralized security data lake with AI-assisted analytics, log management, threat detection, automated investigations, and reporting, enabling security teams to improve visibility and accelerate SOC operations.	▪ Federal government ▪ State and local government ▪ Media and entertainment ▪ Technology ▪ Education ▪ Operational technology ▪ Manufacturing ▪ SCADA/ICS

JULY 2026 © MarketsandMarkets™

			▪ Oil & gas ▪ Power utilities ▪ Healthcare ▪ Pharmaceutical ▪ Financial services ▪ Retail ▪ Hospitality ▪ Transportation
Service	FortiGuard SOC-as-a-Service (SOCaaS)	FortiGuard SOCaaS delivers 24×7 managed security operations, continuous monitoring, threat detection, investigation, and remediation guidance by combining Fortinet technologies, FortiGuard Labs intelligence, and expert SOC analysts.	▪ Federal government ▪ State and local government ▪ Media and entertainment ▪ Technology ▪ Education ▪ Operational technology ▪ Manufacturing ▪ SCADA/ICS ▪ Oil & gas ▪ Power utilities ▪ Healthcare ▪ Pharmaceutical ▪ Financial services ▪ Retail ▪ Hospitality ▪ Transportation
Solution	FortiAI-Assist	FortiAI-Assist embeds generative AI across Fortinet's SOC platform to automate investigations, guide analysts, summarize incidents, recommend remediation actions, and improve security operations productivity using natural language interactions.	▪ Federal government ▪ State and local government ▪ Media and entertainment ▪ Technology ▪ Education ▪ Operational technology ▪ Manufacturing ▪ SCADA/ICS ▪ Oil & gas ▪ Power utilities ▪ Healthcare ▪ Pharmaceutical ▪ Financial services ▪ Retail ▪ Hospitality ▪ Transportation

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.1.11.3 Recent developments

15.1.11.3.1 Product launches/enhancements

TABLE 484 FORTINET: PRODUCT LAUNCHES/ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
June 2026	Product Launch	Fortinet (US)	FortiSOC (Solution)	Fortinet launched FortiSOC, a unified cloud-native AI SOC platform that integrates SIEM, SOAR, threat intelligence, identity threat detection, and agentic AI to automate threat detection, investigation, and response through a single SaaS-based security operations experience.
March 2026	Product Enhancement	Fortinet (US)	Fortinet Security Operations Platform (Solution)	Fortinet enhanced its Security Operations Platform with expanded agentic AI capabilities, previewing FortiSOC, advancing FortiAI, strengthening FortiGuard SOC-as-a-Service, and unifying SIEM, SOAR, endpoint security, and automated threat response within a single Security Fabric architecture.
March 2024	Product Enhancement	Fortinet (US)	FortiGuard SOC-as-a-Service (Service)	Fortinet enhanced FortiGuard SOC-as-a-Service by expanding integrations with FortiSIEM, FortiSOAR, FortiAnalyzer, FortiEDR, FortiNDR, and FortiGuard Labs, enabling unified AI-driven threat detection, investigation, response orchestration, and 24×7 managed security operations across hybrid environments.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.11.3.2 Deals

TABLE 485 FORTINET: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
October 2024	Partnership	Fortinet (US)	CrowdStrike (US)	Fortinet partnered with CrowdStrike to integrate FortiGate Next-Generation Firewalls with the Falcon platform, delivering AI-powered endpoint and network protection, unified telemetry, accelerated threat detection, and streamlined SOC investigations and incident response across enterprise environments.
August 2024	Acquisition	Fortinet (US)	Lacework (US)	Fortinet completed the acquisition of Lacework to strengthen its AI-driven cloud security capabilities by integrating CNAPP, AI-powered threat detection, and cloud telemetry into the Fortinet Security Fabric, enhancing visibility and security operations across hybrid and multi-cloud environments.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.12 ARCTIC WOLF

15.1.12.1 Business overview

Arctic Wolf is a leading AI-native security operations provider specializing in autonomous threat detection, investigation, response, and cyber resilience through its cloud-native Aurora Platform. Unlike traditional cybersecurity vendors that build broad portfolios of point security products, Arctic Wolf has centered its strategy on operationalizing security by combining AI, large-scale telemetry, threat intelligence, and human expertise into a unified security operations model. The company serves more than 10,000 organizations worldwide, processing over 10 trillion security events each week through one of the world's largest commercial security operations environments, supported by an extensive ecosystem of technology, cyber insurance, and channel partners.

Within the AI SOC market, Arctic Wolf has significantly advanced its strategy through the Aurora Superintelligence Platform and the Aurora Agentic SOC, which transform traditional analyst-centric security operations into an AI-driven, agent-led operating model. Built on the company's Swarm of Experts™ framework, the platform combines agentic AI, generative AI, machine learning, open XDR architecture, and human oversight to automate threat detection, investigation, prioritization, and response while maintaining transparency and operational trust. Complementing these capabilities are Aurora Managed Detection and Response (MDR) and Aurora Endpoint Security, providing organizations with continuous AI-powered protection across endpoint, identity, cloud, network, and third-party security environments.

Arctic Wolf has further strengthened its AI SOC capabilities through strategic investments and partnerships that expand both platform intelligence and operational scale. The acquisition of BlackBerry's Cylance business integrated AI-driven endpoint prevention and detection into the Aurora Platform, while strategic collaborations with Anthropic are advancing research and development for next-generation autonomous SOCs using frontier AI models. In addition, the company's Strategic Collaboration Agreement with Amazon Web Services (AWS) is enabling global scaling of the Aurora Platform and AI-powered SOC, enhancing cloud-native telemetry processing, AI-driven threat detection, and security operations performance.

Arctic Wolf differentiates itself by positioning security operations—not individual security products—at the center of its business strategy. Through continuous innovation in agentic AI, an open integration ecosystem, and the evolution of the Aurora Platform into a large-scale AI-native security operations architecture, the company is enabling enterprises to reduce alert fatigue, automate complex SOC workflows, and improve cyber resilience. Its focus on combining trusted AI with human expertise positions Arctic Wolf as one of the emerging pioneers in the transition from managed detection and response to autonomous, AI-driven security operations.

TABLE 486 ARCTIC WOLF: COMPANY OVERVIEW

Founding Year	2012
Headquarters Country	US
Headquarters City/State	Eden Prairie, Minnesota
Ownership Type	Private

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.1.12.2 Products/Solutions/Services offered

TABLE 487 ARCTIC WOLF: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/ SERVICE	DESCRIPTION	VERTICAL
Solution	Aurora Agentic SOC	Aurora Agentic SOC is an AI-led security operations platform that combines a Swarm of Experts framework with human oversight to automate threat detection, investigation, response, and SOC workflows, delivering trusted agentic security operations at enterprise scale.	▪ Financial services ▪ State & local government ▪ Legal ▪ Education ▪ Healthcare ▪ Manufacturing ▪ Retail ▪ Transportation ▪ Credit unions ▪ Aviation ▪ Auto dealers ▪ Sports & entertainment
Solution	Aurora Superintelligence Platform	Aurora Superintelligence Platform is an AI-native security operations platform integrating agentic AI, generative AI, machine learning, threat intelligence, and customer-specific context to power trusted, context-aware detection, investigation, response, and security decision-making across modern SOC environments.	▪ Financial services ▪ State & local government ▪ Legal ▪ Education ▪ Healthcare ▪ Manufacturing ▪ Retail ▪ Transportation ▪ Credit unions ▪ Aviation ▪ Auto dealers ▪ Sports & entertainment
Service	Aurora Managed Detection and Response (MDR)	Aurora Managed Detection and Response (MDR) is a fully managed detection and response service powered by the Aurora Agentic SOC, combining AI-driven threat detection, proactive threat hunting, automated investigations, and expert validation to accelerate incident response across hybrid environments.	▪ Financial services ▪ State & local government ▪ Legal ▪ Education ▪ Healthcare ▪ Manufacturing ▪ Retail ▪ Transportation ▪ Credit unions ▪ Aviation ▪ Auto dealers ▪ Sports & entertainment

JULY 2026 © MarketsandMarkets™

Solution	Aurora Endpoint Security	Aurora Endpoint Security is an AI-driven endpoint prevention, detection, and response solution powered by the Aurora Agentic SOC, delivering continuous endpoint monitoring, automated threat investigation, and coordinated response to strengthen enterprise security operations.	▪ Financial services ▪ State & local government ▪ Legal ▪ Education ▪ Healthcare ▪ Manufacturing ▪ Retail ▪ Transportation ▪ Credit unions ▪ Aviation ▪ Auto dealers ▪ Sports & entertainment

Source: Company Website

15.1.12.3 Recent developments

15.1.12.3.1 Product launches/enhancements

TABLE 488 ARCTIC WOLF: PRODUCT LAUNCHES/ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
March 2026	Product Launch	Arctic Wolf (US)	Aurora Agentic SOC (Solution)	Arctic Wolf launched Aurora Agentic SOC, introducing the world's largest commercial agentic security operations platform that combines AI agents, the Aurora Superintelligence Platform, and expert human oversight to automate threat detection, investigation, and response.
March 2026	Product Launch	Arctic Wolf (US)	Aurora Superintelligence Platform (Solution)	Arctic Wolf launched the Aurora Superintelligence Platform, an AI-native platform that powers the Aurora Agentic SOC by combining generative AI, machine learning, threat intelligence, and customer-specific context for autonomous security operations.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.12.3.2 Deals

TABLE 489 ARCTIC WOLF: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
May 2026	Partnership	Arctic Wolf (US)	Securecom (New Zealand)	Arctic Wolf partnered with Securecom to deliver AI-led security operations powered by the Aurora Superintelligence Platform and Aurora Agentic SOC, enabling organizations to accelerate threat detection, investigation, response, and cyber resilience through a unified AI-native security operations model.
April 2026	Partnership	Arctic Wolf (US)	Datalink Networks (US)	Arctic Wolf partnered with Datalink Networks to deliver AI-led security operations through the Aurora Platform, Managed Detection and Response (MDR), Managed Risk, and Aurora Endpoint Security, enabling organizations to modernize security operations with AI-driven threat detection and response.
March 2026	Partnership	Arctic Wolf (US)	Wiz (US)	Arctic Wolf partnered with Wiz to integrate cloud security posture and cloud detection with the Aurora Platform, enabling unified AI-driven cloud threat detection, investigation, and response while strengthening end-to-end security operations.
October 2025	Partnership	Arctic Wolf (US)	Amazon Web Services (AWS) (US)	Arctic Wolf collaborated with Amazon Web Services (AWS) under a Strategic Collaboration Agreement to scale the Aurora Platform and its AI-powered Security Operations Center (SOC), advancing AI-driven threat detection, response, and cloud-native security operations for more than 10,000 customers worldwide.
April 2025	Partnership	Arctic Wolf (US)	Anthropic (US)	Arctic Wolf collaborated with Anthropic to advance research and development for next-generation autonomous SOCs by combining the Aurora Platform with Claude AI models, accelerating trusted agentic AI, AI Security Assistant capabilities, and autonomous security operations.
February 2025	Acquisition (Completed)	Arctic Wolf (US)	BlackBerry – Cylance (Canada)	Arctic Wolf completed the acquisition of Cylance and launched Aurora Endpoint Security, combining Cylance's AI-driven endpoint protection with the Aurora Platform to enhance AI-native detection, investigation, and response across security operations.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.13 ELASTIC

15.1.13.1 Business overview

Elastic is a well-established Search AI company that has evolved its search and analytics expertise into an AI-powered security platform, enabling organizations to transform vast volumes of enterprise and security telemetry into actionable intelligence. Built on the Elastic Search AI Platform, the company delivers integrated solutions for search, observability, and security that are used by thousands of organizations, including more than half of the Fortune 500. With an open, model-agnostic architecture and strong open-source heritage, Elastic enables enterprises to leverage their preferred AI models while maintaining transparency, explainability, and control over security operations.

Within the AI SOC market, Elastic differentiates itself by embedding agentic AI, retrieval-augmented generation (RAG), semantic search, and large language models (LLMs) directly into the security operations workflow rather than treating AI as a standalone assistant. Its AI security portfolio—including Elastic AI SOC Engine (EASE), Elastic AI Assistant for Security, Attack Discovery, and Elastic Security—helps SOC teams automatically correlate alerts, uncover hidden attack chains, generate investigation queries, recommend remediation actions, and automate repetitive security tasks. The platform is designed to augment existing SIEM and EDR/XDR investments, enabling organizations to modernize security operations without replacing their existing security infrastructure.

Elastic has further strengthened its AI SOC strategy through strategic collaborations with leading cloud and AI providers, including Amazon Web Services (AWS), Microsoft, Google Cloud, and Kyndryl, enabling deeper integration of AI-powered security analytics across cloud-native and hybrid environments. These collaborations expand Elastic's AI-driven security capabilities through integrations with Microsoft Sentinel, Azure AI, Google Gemini, Vertex AI, and managed security services, while supporting scalable deployment of AI-powered SOC capabilities across enterprise and public-sector environments. The company's open AI ecosystem also enables customers to use leading foundation models from providers such as Anthropic, OpenAI, and Google while maintaining flexibility and avoiding vendor lock-in.

Elastic positions itself at the forefront of agentic security operations by combining AI reasoning, vector search, contextual data retrieval, and explainable AI into every stage of the SOC lifecycle. Rather than relying on closed AI workflows, Elastic emphasizes an open, auditable, and model-agnostic AI framework that allows organizations to build trusted AI-driven security operations tailored to their environments. This strategy enables security analysts, threat hunters, and detection engineers to reduce alert fatigue, accelerate investigations, improve detection accuracy, and build intelligent, AI-native SOCs capable of addressing increasingly sophisticated cyber threats.

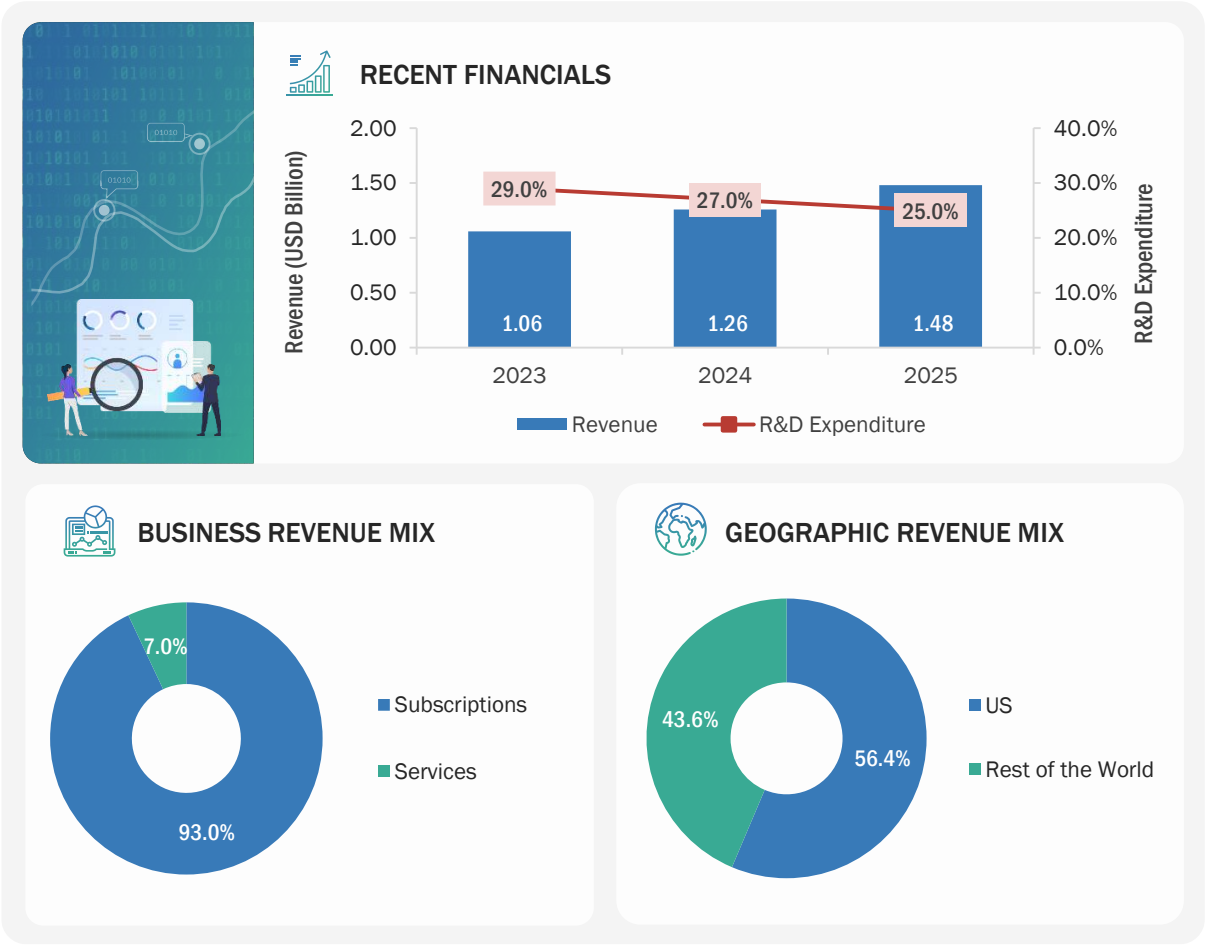
TABLE 490 ELASTIC: COMPANY OVERVIEW

Founding Year	2012
Headquarters Country	Netherlands
Headquarters City/State	Amsterdam
Ownership Type	Public (NYSE: ESTC)

Source: Company Website

JULY 2026 © MarketsandMarkets™

FIGURE 56 ELASTIC: COMPANY SNAPSHOT



Source: Company Website and Annual Reports.

15.1.13.2 Products/Solutions/Services offered

TABLE 491 ELASTIC: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/ SERVICE	DESCRIPTION	VERTICAL
Solution	Elastic AI SOC Engine (EASE)	Elastic AI SOC Engine (EASE) is an AI-powered serverless security operations solution that augments existing SIEM and EDR/XDR platforms with AI-driven attack discovery, alert correlation, investigation, workflow automation, and threat prioritization to accelerate modern SOC operations.	▪ Financial services ▪ Public sector ▪ Telecommunications ▪ Retail ▪ Manufacturing and automotive ▪ Healthcare ▪ Technology ▪ Media and entertainment

JULY 2026 © MarketsandMarkets™

Platform	Elastic Security	Elastic Security is an AI-enabled security analytics platform combining SIEM, XDR, threat hunting, case management, detection engineering, and AI-powered investigation capabilities to help organizations detect, investigate, and respond to sophisticated cyber threats.	▪ Financial services ▪ Public sector ▪ Telecommunications ▪ Retail ▪ Manufacturing and automotive ▪ Healthcare ▪ Technology ▪ Media and entertainment
Solution	Elastic AI Assistant for Security	Elastic AI Assistant for Security is a generative AI-powered security assistant that enables SOC analysts to investigate alerts, generate ES|QL queries, summarize incidents, recommend remediation, and accelerate threat investigations through natural-language interactions with security telemetry.	▪ Financial services ▪ Public sector ▪ Telecommunications ▪ Retail ▪ Manufacturing and automotive ▪ Healthcare ▪ Technology ▪ Media and entertainment
Solution	Attack Discovery	Attack Discovery is an AI-driven threat detection capability that automatically correlates multiple alerts, identifies attack campaigns, maps activity to the MITRE ATT&CK framework, prioritizes incidents, and provides contextual intelligence for faster SOC investigations.	▪ Financial services ▪ Public sector ▪ Telecommunications ▪ Retail ▪ Manufacturing and automotive ▪ Healthcare ▪ Technology ▪ Media and entertainment

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.1.13.3 Recent developments

15.1.13.3.1 Product launches/enhancements

TABLE 492 ELASTIC: PRODUCT LAUNCHES/ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
August 2025	Product Launch	Elastic (Netherlands)	Elastic AI SOC Engine (EASE) (Solution)	Elastic launched the Elastic AI SOC Engine (EASE), a serverless AI-powered security operations solution that augments existing SIEM and EDR/XDR platforms with AI-driven attack discovery, investigation, workflow automation, and threat prioritization.
August 2025	Product Enhancement	Elastic (Netherlands)	Attack Discovery (Solution)	Elastic enhanced Attack Discovery with advanced AI correlation and reasoning capabilities that automatically consolidate related alerts into attack stories, prioritize high-risk incidents, map adversary behavior, and reduce analyst investigation time.
August 2025	Product Enhancement	Elastic (Netherlands)	Elastic Security (Solution)	Elastic enhanced Elastic Security by integrating EASE, AI-powered Attack Discovery, generative AI workflows, and intelligent investigation capabilities, enabling faster detection, triage, and response across modern security operations centers
November 2024	Product Enhancement	Elastic (Netherlands)	Elastic AI Assistant for Security (Solution)	Elastic enhanced the AI Assistant with custom knowledge sources, support for locally hosted LLMs, and contextual cloud detection and response integrations, enabling richer AI-assisted investigations and faster security operations
June 2024	Product Enhancement	Elastic (Netherlands)	Elastic AI Assistant for Security (Solution)	Elastic enhanced the AI Assistant for Security in Elastic Security 8.14 with expanded investigation workflows, ES|QL support, streaming responses, centralized management, Claude 3 integration, and improved analyst productivity for modern SOC operations.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.13.3.2 Deals

TABLE 493 ELASTIC: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
April 2026	Partnership	Elastic (Netherlands)	Google Cloud (US)	Elastic collaborated with Google Cloud to embed its agentic security operations platform into Google Distributed Cloud air-gapped environments, delivering AI-powered security analytics, XDR, automation, and Attack Discovery for highly regulated organizations.
December 2025	Partnership	Elastic (Netherlands)	Microsoft (US)	Elastic partnered with Microsoft to expand AI-powered security operations by integrating Elastic AI SOC Engine (EASE), Attack Discovery, AI Assistant, Microsoft Sentinel, Azure AI Foundry, and Microsoft Security technologies for accelerated SOC investigations.
December 2025	Partnership	Elastic (Netherlands)	Google Cloud (US)	Elastic partnered with Google Cloud to strengthen AI-driven security operations by integrating Gemini, Vertex AI, Elastic AI Assistant, Attack Discovery, Security Command Center, and Google Threat Intelligence for enhanced SOC detection and response.
October 2025	Partnership	Elastic (Netherlands)	Kyndryl (US)	Elastic partnered with Kyndryl to integrate Elastic Security with Kyndryl's Security Operations as a Platform, combining AI-powered detection, investigation, analytics, and SOAR capabilities to improve managed SOC efficiency and incident response.

Source: Company Website and Press Releases

15.1.14 RAPID7

15.1.14.1 Business overview

Rapid7, Inc. is a major cybersecurity vendor specializing in AI-powered managed security operations and threat exposure management, enabling organizations to proactively identify, prioritize, and respond to cyber risks through an open, intelligence-driven security platform. At the core of its portfolio is the Rapid7 Command Platform, which unifies exposure management, threat detection, vulnerability management, AI-powered security analytics, threat intelligence, and managed detection and response (MDR) into a single operational environment. Built on an open and extensible architecture, the platform integrates first- and third-party security data to provide organizations with contextual visibility and accelerate security outcomes across hybrid and multi-cloud environments.

Within the AI SOC market landscape, Rapid7 is advancing a vision of AI-assisted and agentic security operations through Incident Command, its AI-native next-generation SIEM, alongside InsightConnect, Managed Detection and Response (MDR), and its proprietary Rapid7 AI Engine. Rather than replacing security analysts, Rapid7 embeds SOC-trained AI models throughout the investigation lifecycle to automate alert triage, correlate security evidence, generate contextual investigations, recommend response actions, and streamline incident remediation. The platform further differentiates itself by combining attack surface context, embedded threat intelligence, SOAR automation, and AI-assisted decision support within a unified analyst experience.

Rapid7 serves organizations across financial services, healthcare, government, manufacturing, retail, technology, education, telecommunications, and other critical infrastructure sectors, supporting more than 11,500 customers worldwide through a global presence spanning North America, Europe, Asia Pacific, and Latin America. The company continues to strengthen its AI SOC ecosystem through strategic initiatives, including the acquisition of Kenzo Security to accelerate autonomous investigations, expansion of its Global Capability Center in India to support AI-driven security operations, and deeper integration of AI across the Command Platform. These investments reinforce Rapid7's strategy of combining AI innovation with managed security expertise to help organizations modernize SOC operations while reducing operational complexity.

Rapid7 has evolved its security operations strategy by combining AI, automation, threat intelligence, and exposure management into an integrated security operations platform. Recent innovations including Incident Command, agentic AI investigation workflows, Unified Threat-Informed Remediation, and the incorporation of Kenzo Security's autonomous AI capabilities reflect the company's focus on enabling faster, context-rich, and increasingly autonomous security operations. By leveraging decades of MDR expertise, an open integration ecosystem, and AI trained on real-world SOC workflows, Rapid7 is strengthening its position as a provider of AI-native security operations that help enterprises reduce alert fatigue, improve analyst productivity, and respond to cyber threats with greater speed and precision.

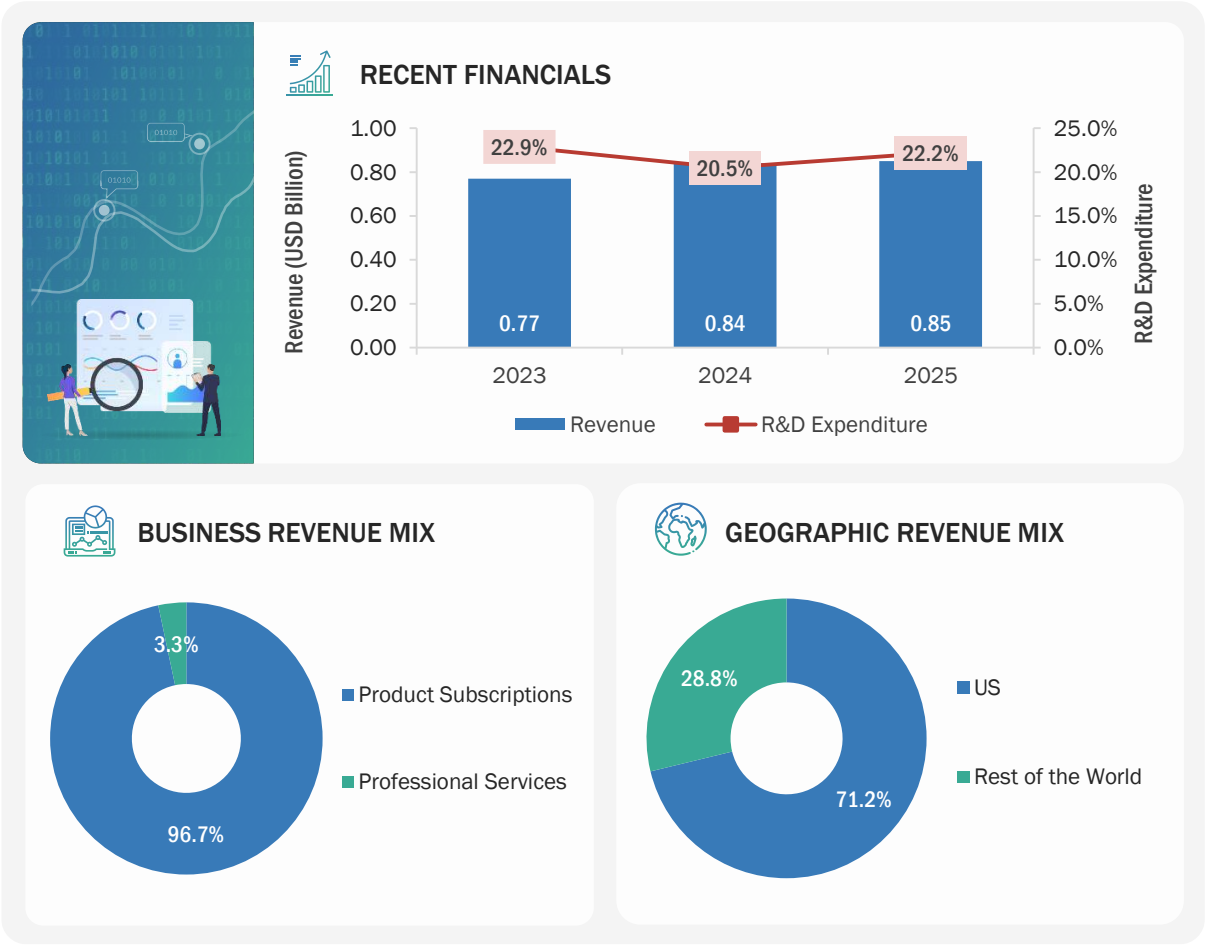
TABLE 494 RAPID7: COMPANY OVERVIEW

Founding Year	2000
Headquarters Country	US
Headquarters City/State	Boston, Massachusetts
Ownership Type	Public (NASDAQ: RPD)

Source: Company Website, Annual Reports, and SEC Filings

JULY 2026 © MarketsandMarkets™

FIGURE 57 RAPID7: COMPANY SNAPSHOT



Source: Company Website and Annual Reports.

15.1.14.2 Products/Solutions/Services offered

TABLE 495 RAPID7: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/ SERVICE	DESCRIPTION	VERTICAL
Platform	Rapid7 Command Platform	Rapid7 Command Platform is a unified AI-driven security operations platform that integrates exposure management, AI-powered detection, next-generation SIEM, XDR, automation, and managed security services, enabling organizations to modernize and streamline enterprise SOC operations.	▪ Federal government ▪ State and local government ▪ Healthcare ▪ Energy ▪ Financial services ▪ Education ▪ Retail

JULY 2026 © MarketsandMarkets™

Solution	Rapid7 Incident Command (AI-Powered Next-Gen SIEM)	Rapid7's AI-powered next-generation SIEM unifies security telemetry, AI-driven behavioral analytics, threat intelligence, and contextual investigations to accelerate threat detection, threat hunting, and incident response across hybrid and multi-cloud security operations.	▪ Federal government ▪ State and local government ▪ Healthcare ▪ Energy ▪ Financial services ▪ Education ▪ Retail
Solution	Rapid7 AI Engine	Rapid7's proprietary AI engine powers AI-assisted alert triage, behavioral analytics, exposure prioritization, contextual investigations, and intelligent SOC workflows, improving detection accuracy while reducing analyst workload and false positives.	▪ Federal government ▪ State and local government ▪ Healthcare ▪ Energy ▪ Financial services ▪ Education ▪ Retail
Service	Managed Detection and Response (MDR)	Rapid7's MDR service combines AI-assisted threat detection, agentic AI investigations, expert SOC analysts, continuous monitoring, threat hunting, and incident response to rapidly identify, investigate, and contain sophisticated cyber threats.	▪ Federal government ▪ State and local government ▪ Healthcare ▪ Energy ▪ Financial services ▪ Education ▪ Retail

Source: Company Website

15.1.14.3 Recent developments

15.1.14.3.1 Product launches/enhancements

TABLE 496 RAPID7: PRODUCT LAUNCHES/ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
July 2025	Product Launch	Rapid7 (US)	Incident Command (AI-Native Next-Generation SIEM) (Solution)	Rapid7 launched Incident Command, an AI-native next-generation SIEM that combines threat detection, exposure management, threat intelligence, automation, and agentic AI workflows into a unified SOC platform, enabling faster investigations, AI-assisted triage, and streamlined incident response.

JULY 2026 © MarketsandMarkets™

June 2025	Product Enhancement	Rapid7 (US)	Rapid7 Managed Detection and Response (MDR) (Service)	Rapid7 enhanced its Managed Detection and Response (MDR) service by embedding agentic AI workflows powered by the Rapid7 AI Engine, automating investigations, accelerating analyst decision-making, and improving transparency, speed, and efficiency across security operations.
April 2025	Product Enhancement	Rapid7 (US)	Command Platform (Platform)	Rapid7 enhanced its Command Platform with unified threat-informed remediation, AI-powered alert triage, automated remediation workflows, and Active Remediation capabilities, enabling faster threat prioritization, investigation, and response across enterprise security operations.
April 2025	Product Launch	Rapid7 (US)	Intelligence Hub (Solution)	Rapid7 launched Intelligence Hub within the Command Platform, delivering curated threat intelligence, AI-assisted prioritization, and contextual insights that strengthen threat detection, investigation, and response for modern security operations teams.
June 2024	Product Enhancement	Rapid7 (US)	Rapid7 AI Engine (Solution)	Rapid7 enhanced its AI Engine by incorporating generative AI capabilities to improve Managed Detection and Response (MDR) services, enabling AI-powered alert validation, investigation assistance, automated incident reporting, and faster analyst-driven security operations.

Source: Company Website and Press Releases

15.1.14.3.2 Deals

TABLE 497 RAPID7: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
March 2026	Acquisition	Rapid7 (US)	Kenzo Security (US)	Rapid7 acquired Kenzo Security, an agentic AI security platform, to strengthen the Rapid7 Command Platform with autonomous investigations, AI-driven threat hunting, and machine-speed detection and response capabilities for modern AI-powered security operations.
November 2025	Partnership	Rapid7 (US)	Microsoft (US)	Rapid7 partnered with Microsoft to expand modern detection and response by integrating Rapid7 MDR with Microsoft Defender, combining AI-driven insights, Microsoft telemetry, and SOC expertise to improve detection, investigation, and response across hybrid environments.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.14.3.3 Expansions

TABLE 498 RAPID7: EXPANSIONS

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY	COMPANY	DESCRIPTION
March 2025	Expansion	Global Capability Center (Innovation Hub & Security Operations Center)	India	Rapid7 (US)	Rapid7 expanded its global operations by establishing a Global Capability Center (GCC) in Pune, India, serving as an innovation hub and Security Operations Center (SOC). The facility supports AI innovation, cyber operations, product development, customer support, and 24×7 managed detection and response (MDR) services while strengthening regional cybersecurity talent and AI collaborations.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.1.15 SENTINELONE

15.1.15.1 Business overview

SentinelOne, Inc. is an AI-native cybersecurity company focused on delivering autonomous, data-driven cyber defense through its Singularity Platform, which unifies endpoint, identity, cloud, AI, and security data into a single intelligent security architecture. Powered by Autonomous Security Intelligence, the platform combines machine learning, behavioral AI, real-time telemetry, and automation to detect, investigate, and respond to cyber threats at machine speed. SentinelOne's portfolio spans endpoint security, AI SIEM, cloud security, identity security, AI security, hyperautomation, threat intelligence, managed detection and response (MDR), and incident response services, enabling organizations to simplify security operations while improving cyber resilience.

Within the AI SOC market, SentinelOne has positioned itself as a pioneer of the Autonomous SOC by integrating Purple AI, Singularity AI SIEM, Hyperautomation, AI Data Pipelines, Data Lake, Prompt Security, and Wayfinder Threat Detection and Response into a unified security operations ecosystem. Rather than using AI solely as an analyst assistant, the company embeds agentic AI across the entire SOC lifecycle to automate alert triage, threat hunting, investigations, malware analysis, detection engineering, and response orchestration. Recent innovations, including Purple AI Agentic Investigation, AI Security for AI agents, and enhanced AI-native security capabilities, further strengthen its ability to help organizations secure both enterprise infrastructure and emerging AI environments.

SentinelOne serves customers across financial services, government, healthcare, manufacturing, retail, telecommunications, technology, education, and critical infrastructure, protecting nearly one-fifth of the Fortune 500 and hundreds of Global 2000 organizations through its global operations headquartered in Mountain View, California. The company continues to expand its international footprint through regional cloud deployments and data sovereignty initiatives while strengthening its AI SOC ecosystem through strategic collaborations with Google Cloud, Amazon Web Services (AWS), Cloudflare, LevelBlue, Silverfort, Anthropic, and other technology partners. These partnerships enhance interoperability across AI security, AI SIEM, managed security operations, threat intelligence, and autonomous response capabilities.

SentinelOne continues to advance its long-term vision of autonomous security operations through sustained investments in agentic AI, AI security, and open security ecosystems. Recent initiatives include expanding Purple AI with agentic investigation capabilities, introducing Prompt Security for AI applications and agents, extending AI-powered security to sovereign and air-gapped environments, and deepening strategic alliances with Google Cloud and leading managed security providers. By combining AI-native analytics, autonomous decision-making, and an open integration ecosystem, SentinelOne is strengthening its position as a leading provider of AI-driven and autonomous security operations for modern enterprises.

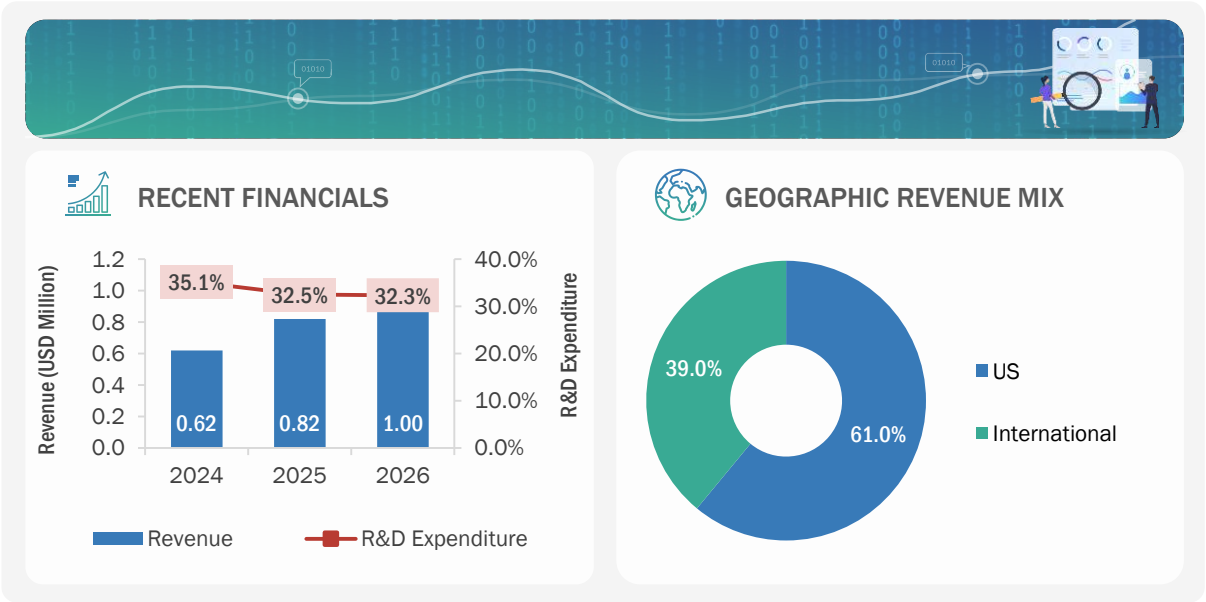
TABLE 499 SENTINELONE: COMPANY OVERVIEW

Founding Year	2013
Headquarters Country	US
Headquarters City/State	Mountain View, California
Ownership Type	Public (NYSE: S)

Source: Company Website, Annual Reports, and SEC Filings

JULY 2026 © MarketsandMarkets™

FIGURE 58 SENTINELONE: COMPANY SNAPSHOT



Source: Company Website and Annual Reports.

15.1.15.2 Products/Solutions/Services offered

TABLE 500 SENTINELONE: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT TYPE	PRODUCT/SOLUTION/ SERVICE	DESCRIPTION	VERTICAL
Solution	Singularity Platform	SentinelOne's unified AI-native security platform integrates endpoint, cloud, identity, AI security, AI SIEM, hyperautomation, and a common data architecture to provide centralized visibility, autonomous threat detection, investigation, and response across modern enterprise security operations.	▪ Healthcare ▪ Financial services ▪ Federal government ▪ State and local government ▪ Manufacturing ▪ Energy ▪ Transportation and logistics ▪ Higher education ▪ K-12 education ▪ Retail and hospitality
Solution	Autonomous SOC	SentinelOne's Autonomous SOC unifies AI Data Pipelines, AI SIEM, Purple AI, and Hyperautomation to deliver machine-speed threat detection, agentic investigation, and autonomous response, reducing operational complexity while improving visibility, analyst productivity, and response efficiency.	▪ Healthcare ▪ Financial services ▪ Federal government ▪ State and local government ▪ Manufacturing ▪ Energy ▪ Transportation and logistics ▪ Higher education ▪ K-12 education ▪ Retail and hospitality

JULY 2026 © MarketsandMarkets™

Solution	Singularity AI SIEM	Singularity AI SIEM is a cloud-native AI-powered SIEM that consolidates endpoint, identity, cloud, and third-party telemetry into a unified platform, providing AI-driven detection, contextual investigations, threat hunting, and integrated response from a single security operations console.	▪ Healthcare ▪ Financial services ▪ Federal government ▪ State and local government ▪ Manufacturing ▪ Energy ▪ Transportation and logistics ▪ Higher education ▪ K-12 education ▪ Retail and hospitality
Solution	Purple AI	SentinelOne's AI-powered security analyst automates alert triage, threat hunting, investigations, and decision support using natural language, agentic reasoning, and real-time security context to accelerate SOC operations and improve analyst productivity.	▪ Healthcare ▪ Financial services ▪ Federal government ▪ State and local government ▪ Manufacturing ▪ Energy ▪ Transportation and logistics ▪ Higher education ▪ K-12 education ▪ Retail and hospitality
Solution	Singularity Hyperautomation	Singularity Hyperautomation is a no-code security orchestration and automation solution that enables organizations to build automated response workflows, orchestrate actions across native and third-party security tools, and accelerate incident containment throughout the SOC lifecycle.	▪ Healthcare ▪ Financial services ▪ Federal government ▪ State and local government ▪ Manufacturing ▪ Energy ▪ Transportation and logistics ▪ Higher education ▪ K-12 education ▪ Retail and hospitality
Service	Singularity Managed Detection and Response (MDR)	SentinelOne's managed detection and response service combines AI-powered analytics, Purple AI insights, expert threat hunters, and continuous monitoring to detect, investigate, contain, and remediate advanced cyber threats across enterprise environments.	▪ Healthcare ▪ Financial services ▪ Federal government ▪ State and local government ▪ Manufacturing ▪ Energy ▪ Transportation and logistics ▪ Higher education ▪ K-12 education ▪ Retail and hospitality

JULY 2026 © MarketsandMarkets™

Service	Wayfinder Threat Detection and Response (Wayfinder TDR)	Wayfinder Threat Detection and Response (Wayfinder TDR) is an AI-assisted threat detection and response service that combines SentinelOne's autonomous detection capabilities with expert analyst expertise to deliver continuous threat monitoring, investigation, incident response, and proactive threat hunting.	▪ Healthcare ▪ Financial services ▪ Federal government ▪ State and local government ▪ Manufacturing ▪ Energy ▪ Transportation and logistics ▪ Higher education ▪ K-12 education ▪ Retail and hospitality
Solution	Singularity AI Data Pipelines	SentinelOne's AI-powered data pipeline solution filters, normalizes, enriches, and optimizes security telemetry before SIEM ingestion, reducing data volume by up to 80% while improving detection accuracy, investigation quality, and AI-driven SOC efficiency.	▪ Healthcare ▪ Financial services ▪ Federal government ▪ State and local government ▪ Manufacturing ▪ Energy ▪ Transportation and logistics ▪ Higher education ▪ K-12 education ▪ Retail and hospitality
Solution	Singularity Data Lake	SentinelOne's cloud-native security data lake unifies endpoint, cloud, identity, and third-party telemetry into a single always-hot data foundation, enabling AI SIEM, Purple AI, and Hyperautomation to perform faster investigations, long-term threat hunting, and AI-powered security operations.	▪ Healthcare ▪ Financial services ▪ Federal government ▪ State and local government ▪ Manufacturing ▪ Energy ▪ Transportation and logistics ▪ Higher education ▪ K-12 education ▪ Retail and hospitality

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.1.15.3 Recent developments

15.1.15.3.1 Product launches/enhancements

TABLE 501 SENTINELONE: PRODUCT LAUNCHES/ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY	PRODUCT NAME (TYPE)	DESCRIPTION
June 2026	Product Enhancement	SentinelOne (US)	Purple AI Agentic Investigation (Solution)	SentinelOne enhanced Purple AI by making Agentic Investigation generally available, enabling zero-click autonomous investigations that detect, investigate, validate, and respond to threats using frontier AI reasoning integrated across the Singularity Platform.
March 2026	Product Launch	SentinelOne (US)	Prompt AI Agent Security (Solution)	SentinelOne launched Prompt AI Agent Security, providing real-time discovery, governance, monitoring, and policy enforcement for AI agents and agentic workflows, extending autonomous protection across enterprise AI environments and AI-powered SOC operations.
March 2026	Product Enhancement	SentinelOne (US)	Purple AI Auto Investigation (Solution)	SentinelOne enhanced Purple AI with general availability of Auto Investigation, enabling one-click agentic investigations that autonomously collect evidence, construct attack timelines, generate explainable verdicts, and trigger Hyperautomation-based remediation within Singularity AI SIEM.
November 2025	Product Launch	SentinelOne (US)	AI Security Portfolio (Solution)	SentinelOne launched an expanded AI Security portfolio featuring AI-ready Data Pipelines, AI agent security, enhanced Purple AI capabilities, and Wayfinder AI-powered threat detection services to help organizations secure AI systems and automate modern security operations.
November 2025	Product Enhancement	SentinelOne (US)	Purple AI (Solution)	SentinelOne enhanced Purple AI with agentic auto-investigations, dynamic reasoning, advanced triage, orchestration workflows, and autonomous response capabilities, reducing investigation times while improving analyst productivity within AI-native security operations centers.

JULY 2026 © MarketsandMarkets™

April 2025	Product Enhancement	SentinelOne (US)	Purple AI Athena (Solution)	SentinelOne enhanced Purple AI with the Athena release, introducing deep security reasoning, agentic detection and response, Hyperautomation workflows, and support for third-party SIEMs and data lakes to accelerate AI-driven SOC investigations and response.

Source: Company Website and Press Releases

15.1.15.3.2 Deals

TABLE 502 SENTINELONE: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
June 2026	Integration Partnership	SentinelOne (US)	Amazon Web Services (AWS) (US)	SentinelOne integrated Prompt Security with Amazon Bedrock AgentCore to provide runtime guardrails for AI agents, enabling enterprises to secure agentic workflows, enforce AI policies, and extend autonomous security controls across AI-powered environments.
June 2026	Integration Partnership	SentinelOne (US)	Anthropic (US)	SentinelOne integrated Anthropic's Claude capabilities through Claude Compliance API integrations with Prompt Security and Singularity AI SIEM, enabling organizations to monitor AI activity, enforce governance policies, investigate AI usage, and strengthen AI-driven SOC operations.
April 2026	Strategic Partnership	SentinelOne (US)	Silverfort (US)	SentinelOne partnered with Silverfort to secure human, AI agent, and non-human identities by combining identity protection with endpoint, cloud, and AI application security capabilities, enabling autonomous detection and response against identity-based threats in AI-driven environments.
March 2026	Partnership	SentinelOne (US)	Cloudflare (US)	SentinelOne expanded its partnership with Cloudflare by integrating Cloudflare Logpush telemetry with Singularity AI SIEM, enabling AI-driven correlation across endpoint, cloud, identity, and network data to improve real-time threat detection, investigation, and automated response.
March 2026	Strategic Collaboration	SentinelOne (US)	Google Cloud (US)	SentinelOne has expanded its strategic collaboration with Google Cloud to develop integrated AI-powered security solutions combining SentinelOne's EDR, AI security capabilities, and autonomous platform with Google Security Operations and Google Threat Intelligence to strengthen AI-driven cyber defense at global scale.

JULY 2026 © MarketsandMarkets™

March 2026	Strategic Partnership	SentinelOne (US)	LevelBlue (US)	SentinelOne partnered with LevelBlue to deliver AI-powered managed security operations and incident response services by combining Purple AI, Singularity Platform, AI SIEM analytics, and LevelBlue's managed security expertise to accelerate detection, investigation, and response.
October 2024	Collaboration	SentinelOne (US)	Amazon Web Services (AWS) (US)	SentinelOne collaborated with AWS to expand its strategic alliance by integrating Purple AI with Amazon Bedrock, enabling generative AI-powered security analysis, AI-driven investigations, and enhanced access to SentinelOne's Singularity Platform through AWS Marketplace for enterprise SOC modernization.
August 2024	Strategic Partnership	SentinelOne (US)	Google Cloud (US)	SentinelOne partnered with Google Cloud to strengthen AI-powered cyber defense by integrating autonomous endpoint protection with Google Threat Intelligence, shared security telemetry, and Gemini AI models, enhancing Purple AI and the Singularity Platform for AI-driven security operations.

Source: Company Website and Press Releases

15.1.15.3.3 Expansions

TABLE 503 SENTINELONE: EXPANSIONS

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY	COMPANY	DESCRIPTION
March 2026	Expansion	Regional Cloud Expansion (Data Sovereignty)	North America, Germany (Frankfurt), Saudi Arabia	SentinelOne (US)	SentinelOne expanded the regional availability of its Singularity Platform through Google Cloud infrastructure across North America, Frankfurt, and Saudi Arabia. The expansion supports AI-powered security operations with in-country data residency, regulatory compliance, and autonomous SOC capabilities for global enterprises.

Source: Company Website and Press Releases

JULY 2026 © MarketsandMarkets™

15.2 OTHER KEY PLAYERS

15.2.1 RELIAQUEST

Founding Year	2007
Headquarters – Country	US
Headquarters – City/State	Tampa, Florida
Ownership Type	Private
Business Overview	ReliaQuest is a private AI cybersecurity company focused on transforming enterprise security operations through an open, vendor-agnostic security operations platform. The company enables organizations to maximize the value of existing cybersecurity investments rather than replacing them with proprietary technologies. Its flagship GreyMatter platform ingests, normalizes, and analyzes telemetry from hundreds of security technologies using its patented Universal Translator, allowing enterprises to detect, investigate, contain, and respond to cyber threats from a unified operating environment. The company serves more than 1,000 enterprise customers globally and operates from Tampa, Las Vegas, Salt Lake City, Dublin, London, and Pune. Within the AI SOC market, ReliaQuest has positioned GreyMatter Agentic AI at the center of its security operations strategy, introducing specialized AI Teammates for investigation and response, threat hunting, detection engineering, threat intelligence, IT, and OT security operations. The platform combines agentic AI, automation, proprietary incident response knowledge, and human oversight to execute investigations, optimize detections, and accelerate incident response across multi-cloud, hybrid, and multi-SIEM environments. Recent innovations include expanded Agentic AI capabilities that enable organizations to build AI-driven SOCs while preserving existing security investments. ReliaQuest primarily serves industries including financial services, healthcare, manufacturing, retail, energy & utilities, telecommunications, transportation, government, and other large enterprise sectors.
Products/Platforms/Solutions Offered	▪ GreyMatter Security Operations Platform ▪ GreyMatter Agentic AI ▪ GreyMatter Agentic Teammates
Geographic Presence	North America, Europe, Asia Pacific, and the Middle East & Africa

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.2 EXABEAM

Founding Year	2013
Headquarters – Country	US
Headquarters – City/State	Broomfield, Colorado
Ownership Type	Private
Business Overview	Exabeam is a behavior intelligence company focused on transforming security operations through AI-driven analytics, behavioral intelligence, and automation. Following its merger with LogRhythm in 2024, the company established a unified security operations portfolio that brings together cloud-native SIEM, user and entity behavior analytics (UEBA), threat detection, and automated response capabilities within a single platform. By consolidating these technologies, Exabeam enables organizations to improve threat visibility, accelerate incident response, and simplify security operations across hybrid and multi-cloud environments. The company serves a broad customer base spanning financial services, healthcare, manufacturing, government, retail, technology, telecommunications, and critical infrastructure, helping enterprises strengthen cyber resilience against increasingly sophisticated threats. Within the AI SOC market, Exabeam is driving the evolution of agentic security operations through its New-Scale Security Operations Platform, New-Scale Fusion, and Exabeam Nova. These offerings leverage behavioral intelligence, generative AI, natural-language interactions, and intelligent automation to streamline threat detection, investigation, and response while reducing analyst workload and alert fatigue. Recent innovations, including Agent Behavior Analytics (ABA), extend visibility beyond human users to monitor autonomous AI agents and machine identities, enabling organizations to secure emerging AI-powered environments. By embedding AI across investigation, threat hunting, detection engineering, and response workflows, Exabeam is helping security teams transition from reactive SOC operations to proactive, intelligence-led security operations that deliver faster decision-making, greater operational efficiency, and improved cyber resilience.
Products/Platforms/Solutions Offered	▪ New-Scale Fusion Security Operations Platform ▪ Exabeam Nova ▪ New-Scale SIEM ▪ New-Scale Analytics ▪ Exabeam Professional Services
Geographic Presence	North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.3 ESENTIRE

Founding Year	2001
Headquarters – Country	Canada
Headquarters – City/State	Waterloo, Ontario
Ownership Type	Private
Business Overview	eSentire is a Managed Detection and Response (MDR) company that has evolved its business around Controlled Autonomy SecOps, combining agentic AI with continuous human oversight to deliver enterprise-grade security operations. Rather than replacing security teams with autonomous automation, the company emphasizes a "human-on-the-loop" operating model that balances machine-speed decision-making with expert validation and accountability. Serving more than 2,000 organizations across 35+ industries worldwide, eSentire protects enterprises through its cloud-native security operations platform, proprietary threat intelligence, and 24×7 Security Operations Centers. The company supports organizations across financial services, healthcare, manufacturing, legal, technology, government, education, retail, and other highly regulated sectors that require resilient, always-on cyber defense. In the AI SOC market landscape, eSentire has positioned the Atlas Platform as the foundation of its next-generation security operations strategy. Powered by Atlas AI, the platform combines agentic AI operatives, real-time telemetry correlation, autonomous investigation, offensive security validation, and expert-led MDR services to preempt, detect, and neutralize cyber threats across heterogeneous security environments. Recent developments, including the launch of a Technology Innovation Center in India to accelerate generative AI and automation development, underscore the company's commitment to advancing AI-assisted security operations. Through an open integration architecture that connects with existing security tools rather than replacing them, eSentire enables organizations to modernize SOC operations while improving analyst efficiency, reducing alert fatigue, and strengthening cyber resilience.
Products/Platforms/Solutions Offered	▪ Atlas Platform (Atlas Security Operations Platform) ▪ Managed Detection and Response (MDR) ▪ eSentire Atlas SIEM and Log Management
Geographic Presence	North America, Europe, Asia Pacific, and the Middle East & Africa

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.4 EXPEL

Founding Year	2016
Headquarters – Country	US
Headquarters – City/State	Herndon, Virginia
Ownership Type	Private
Business Overview	Expel is a global provider of MDR, focused on making security operations faster, more transparent, and easier to manage through the combined expertise of security practitioners and AI-driven automation. Founded by former Mandiant and FireEye security leaders, the company has built its business around an open, customer-centric operating model that integrates with existing security investments instead of requiring organizations to replace their security stack. Its cloud-native security operations platform provides continuous monitoring, investigation, response, and operational visibility across cloud, identity, email, endpoint, SIEM, SaaS, and on-premises environments. Expel serves organizations across financial services, healthcare, retail, manufacturing, technology, education, legal, and other highly regulated industries, helping them strengthen cyber resilience while reducing operational complexity. In the AI SOC market, Expel differentiates itself through its agentic MDR approach, where AI accelerates investigations while human analysts retain decision-making authority over critical security actions. The company's Expel Workbench security operations platform and MDR service leverage Ruxie AI to automate repetitive tasks, correlate alerts, prioritize threats, and assist analysts throughout the entire threat lifecycle from detection to remediation. Rather than pursuing fully autonomous security operations, Expel emphasizes AI-augmented decision-making that combines automation with practitioner expertise, enabling organizations to improve response speed, reduce alert fatigue, and modernize SOC operations without sacrificing transparency, flexibility, or operational control. Recent innovations have expanded AI capabilities across the full threat lifecycle, reinforcing Expel's position as a leader in agentic MDR and AI-assisted security operations.
Products/Platforms/Solutions Offered	▪ Expel Workbench ▪ Managed Detection and Response (MDR) ▪ Managed SIEM ▪ Ruxie AI
Geographic Presence	North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.5 HUNTRESS

Founding Year	2015
Headquarters – Country	US
Headquarters – City/State	Columbia, Maryland
Ownership Type	Private
Business Overview	Huntress is a managed cybersecurity company dedicated to making enterprise-grade security operations accessible to organizations of all sizes through a unified, AI-centric managed security platform. Founded by former US National Security Agency (NSA) cyber operators, the company has built its business around the philosophy that AI should enhance rather than replace human expertise in defending against modern cyber threats. Its platform delivers managed endpoint, identity, and security operations capabilities supported by a global 24×7 Security Operations Center (SOC) that continuously monitors, investigates, and responds to threats. Huntress serves businesses ranging from small and medium-sized organizations to large enterprises, as well as managed service providers (MSPs), across industries including healthcare, financial services, education, manufacturing, legal, retail, and government. Within the AI SOC market, Huntress has positioned its Agentic Security Platform around an AI-Centric, Human-Led SOC model, where AI agents accelerate telemetry correlation, investigation, timeline creation, and incident summarization while experienced SOC analysts retain responsibility for validation and response decisions. The company's portfolio combines Managed EDR, Managed ITDR, and Managed SIEM with continuous threat hunting to deliver proactive security outcomes and reduce alert fatigue. Rather than pursuing fully autonomous SOC operations, Huntress emphasizes trusted human-AI collaboration that improves investigation speed, maintains decision transparency, and delivers high-confidence incident response. This approach enables organizations to modernize security operations while preserving expert oversight for complex cyber incidents.
Products/Platforms/Solutions Offered	▪ Huntress Agentic Security Platform ▪ Managed EDR ▪ Managed ITDR ▪ Managed SIEM
Geographic Presence	North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.6 UNDERDEFENSE

Founding Year	2017
Headquarters – Country	US
Headquarters – City/State	New York City, New York
Ownership Type	Private
Business Overview	UnderDefense is a prominent cybersecurity company focused on delivering AI-driven security operations and compliance automation through a unified, open security architecture. Since its establishment, the company has evolved from a cybersecurity services provider into a platform-led business centered around UnderDefense MAXI, enabling organizations to automate security operations while preserving full control over their existing technology stack. Rather than replacing deployed security tools, UnderDefense integrates with leading SIEM, EDR, cloud, identity, and network security solutions to orchestrate detection, investigation, response, and compliance from a single operating environment. The company supports enterprises across financial services, healthcare, manufacturing, technology, energy, retail, and other regulated industries with managed detection and response, managed SIEM, managed SOC, incident response, and compliance services. Within the AI SOC market, UnderDefense is positioning itself around agentic security operations through its MAXI Agentic AI SOC Platform, which combines autonomous multi-agent investigations, AI-powered alert correlation, response orchestration, and expert validation to accelerate incident response. In 2026, the company introduced the industry's first on-premises Agentic AI SOC designed for sovereign, closed, and air-gapped environments, enabling organizations with strict data residency requirements to deploy autonomous AI investigations entirely within their own infrastructure. By combining AI-driven automation with 24×7 cybersecurity expertise, UnderDefense enables enterprises to reduce alert fatigue, improve investigation accuracy, and modernize SOC operations while maintaining transparency, regulatory compliance, and human oversight over critical security decisions.
Products/Platforms/Solutions Offered	▪ UnderDefense MAXI Platform ▪ MAXI AI SOC ▪ Managed Detection and Response (MDR) ▪ Managed SIEM ▪ Managed SOC (SOCaaS) ▪ Incident Response Management
Geographic Presence	North America and Europe

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.7 STELLAR CYBER

Founding Year	2015
Headquarters – Country	US
Headquarters – City/State	San Jose, California
Ownership Type	Private
Business Overview	Stellar Cyber is an AI-native security operations company focused on helping enterprises and managed security service providers (MSSPs) build a human-augmented autonomous SOC through an open, unified security operations platform. Established with the mission of transforming security operations using artificial intelligence, the company addresses the challenges of fragmented security stacks, excessive alert volumes, and manual investigations by consolidating security telemetry into a single operational environment. Its platform integrates AI-driven SIEM, Open XDR, network detection and response (NDR), identity threat detection and response (ITDR), and automated response capabilities, enabling organizations to maximize existing security investments without replacing their deployed technologies. Serving more than 15,000 customers across over 50 countries, Stellar Cyber supports enterprises and MSSPs across financial services, healthcare, manufacturing, government, retail, education, telecommunications, and other critical sectors. In the AI SOC market, Stellar Cyber has positioned its Open XDR Platform as the foundation for autonomous security operations powered by its Multi-Layer AI™ architecture. The platform applies agentic AI, automated triage, AI-assisted investigations, intelligent threat hunting, and contextual incident response to accelerate the complete security operations lifecycle while maintaining human oversight for critical decisions. Recent advancements, including the introduction of the Human-Augmented Autonomous SOC at RSAC 2025, further strengthen the company's strategy of combining explainable AI with analyst expertise to improve detection accuracy, reduce alert fatigue, and streamline incident response. By delivering an open architecture that unifies security tools, data, and workflows, Stellar Cyber enables organizations to modernize SOC operations while improving operational efficiency and cyber resilience.
Products/Platforms/Solutions Offered	▪ Security Operations Platform ▪ Multi-Layer AI ▪ AI-Native Next-Gen SIEM ▪ Open XDR
Geographic Presence	North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.8 RADIANT SECURITY

Founding Year	2021
Headquarters – Country	US
Headquarters – City/State	Pleasanton, California
Ownership Type	Private
Business Overview	Radiant Security is an AI SOC company focused exclusively on automating security operations through adaptive artificial intelligence that investigates every security alert, regardless of its source, complexity, or vendor. Founded by cybersecurity veterans with extensive experience in enterprise security operations, the company was established to eliminate the operational inefficiencies created by alert overload, fragmented security tools, and static automation playbooks. Radiant dynamically builds investigation logic for each alert, enabling organizations to centralize alert triage, incident investigation, response, and log management within a single cloud-native platform. Its solutions are designed for enterprise security teams across financial services, healthcare, technology, manufacturing, retail, energy, and other industries seeking to modernize SOC operations while maximizing existing security investments. Within the AI SOC market, Radiant Security delivers the Adaptive AI SOC Platform as the core of its technology strategy, enabling autonomous alert triage, AI-driven investigations, integrated response orchestration, and built-in log management through adaptive AI agents. Unlike conventional AI SOC solutions that support only predefined security use cases, Radiant's platform dynamically adapts to 100% of alert types across cloud, endpoint, identity, email, network, SIEM, OT, and other environments without requiring playbooks or manual rule creation. Recent platform enhancements have further expanded adaptive AI capabilities, allowing security teams to investigate novel threats, reduce false positives, accelerate incident response, and improve analyst productivity while maintaining full transparency into every AI-generated decision.
Products/Platforms/Solutions Offered	▪ AI SOC Platform ▪ Log Management
Geographic Presence	North America, Europe, and Latin America

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.9 TORQ

Founding Year	2020
Headquarters – Country	Dual HQ: US/Israel
Headquarters – City/State	New York/Tel Aviv
Ownership Type	Private
Business Overview	Torq is an AI security operations company specializing in autonomous and agentic SOC technologies that enable enterprises to automate the complete threat management lifecycle from alert triage through investigation, containment, remediation, and case closure. Founded by cybersecurity entrepreneurs Ofer Smadari, Leonid Belkind, and Eldad Livni, the company initially pioneered security hyperautomation before expanding into AI-native security operations. Today, Torq combines large-scale automation, multi-agent AI, and orchestration to help organizations modernize SOC workflows while leveraging existing security investments rather than replacing them. Its platform is adopted by Fortune 500 enterprises across industries including financial services, healthcare, manufacturing, retail, telecommunications, hospitality, and technology, enabling security teams to improve operational efficiency while addressing growing cyber risks and analyst shortages. Torq's AI SOC strategy is built around its Torq AI SOC Platform, which integrates Hyperautomation and HyperAgents to deliver autonomous threat triage, AI-assisted investigations, contextual risk analysis, workflow orchestration, and response automation from a single operating environment. Unlike conventional SOAR platforms that primarily automate predefined workflows, Torq applies coordinated multi-agent reasoning across the entire security operations lifecycle while maintaining configurable human oversight. Recent innovations, including native Multi-Agent System capabilities and Model Context Protocol (MCP) support, have further strengthened the platform's ability to investigate, prioritize, and remediate threats at enterprise scale. Through continuous investment in agentic AI and security automation, Torq is positioning itself as one of the key innovators driving the evolution of autonomous SOC operations.
Products/Platforms/Solutions Offered	▪ Torq AI SOC Platform ▪ Torq Hyperautomation ▪ Torq HyperAgents ▪ Torq Professional Services
Geographic Presence	North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.10 INTEZER

Founding Year	2016
Headquarters – Country	US
Headquarters – City/State	New York City, New York
Ownership Type	Private
Business Overview	Intezer is a prominent AI SOC company, focused on transforming enterprise security operations through forensic-grade artificial intelligence that investigates every security alert with evidence-based accuracy. Founded by former Israeli cyber defense experts and cybersecurity entrepreneurs, the company was established to eliminate one of the industry's largest operational challenges—the inability of SOC teams to investigate every alert because of limited analyst capacity. Intezer enables enterprises to retain control of their security operations by automating alert triage, investigation, and response across endpoint, identity, cloud, email, network, and SIEM environments. Its platform combines proprietary forensic analysis, reverse engineering, memory analysis, and threat intelligence with agentic AI to help organizations improve detection quality while reducing operational overhead. Today, Intezer is trusted by more than 150 global enterprises, including numerous Fortune 500 organizations, across industries such as financial services, healthcare, manufacturing, technology, telecommunications, energy, and retail. Within the AI SOC market, Intezer has built its strategy around the Intezer AI SOC platform, which autonomously investigates 100% of security alerts at forensic depth while escalating fewer than 2% for analyst review. The platform combines ForensicAI, agentic AI, automated detection engineering, and continuous learning to help organizations shift analysts from manual alert triage to supervising AI-generated outcomes. Recent innovations, including the introduction of the SOC Operating Layer and Org Brain, a self-learning organizational memory that continuously improves investigations based on historical analyst decisions and live organizational context, further strengthen Intezer's vision of an adaptive AI SOC capable of improving accuracy over time. By integrating explainable AI with deterministic forensic analysis, Intezer enables enterprises to modernize security operations while improving investigation speed, operational efficiency, and cyber resilience.
Products/Platforms/Solutions Offered	Intezer AI SOC
Geographic Presence	North America, Europe, and the Middle East & Africa

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.11 CONIFERS

Founding Year	2024
Headquarters – Country	US
Headquarters – City/State	Dallas, Texas
Ownership Type	Private
Business Overview	Conifers is an agentic AI security operations company dedicated to transforming enterprise Security Operations Centers (SOCs) through autonomous AI that executes the complete security operations lifecycle. The company has developed an end-to-end agentic architecture that unifies threat intelligence, threat hunting, detection engineering, investigation, and remediation into a single coordinated AI system. Built for enterprise SOCs as well as managed security service providers (MSSPs) and managed detection and response (MDR) providers, Conifers enables organizations to modernize security operations without replacing their existing SIEM, SOAR, XDR, or other security technologies. Its semantic integration layer allows organizations to preserve existing security investments while introducing AI-driven investigations, transparent reasoning, and governed automation across complex hybrid environments. Backed by cybersecurity-focused investors including SYN Ventures, PICUS Capital, and Washington Harbour Partners, the company has rapidly expanded its presence in the AI SOC market. Within the AI SOC market, Conifers offers the CognitiveSOC platform, an end-to-end agentic AI platform designed to investigate every alert with contextual reasoning rather than static automation or predefined playbooks. The platform employs a coordinated fabric of AI agents that continuously exchange organizational knowledge while executing the five core SOC functions—threat intelligence, threat hunting, detection engineering, investigation, and response. Recent platform advancements have introduced transparent AI reasoning, governed investigations, customer-specific institutional knowledge, and configurable autonomy that allows organizations to progressively transition from human-in-the-loop to human-on-the-loop operations. By combining explainable AI, enterprise governance, and machine-speed investigations, Conifers enables security teams to improve investigation quality, accelerate incident response, and scale SOC performance while maintaining full analyst oversight and accountability.
Products/Platforms/Solutions Offered	CognitiveSOC (Agentic AI SOC Platform)
Geographic Presence	North America, Europe, Asia Pacific, and the Middle East & Africa

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.12 DROPZONE AI

Founding Year	2023
Headquarters – Country	US
Headquarters – City/State	Seattle, Washington
Ownership Type	Private
Business Overview	Dropzone AI is an agentic AI cybersecurity company focused on transforming security operations by deploying autonomous AI analysts that investigate, hunt, and respond to cyber threats alongside human defenders. Dropzone AI integrates with customers' SIEM, EDR, SOAR, XDR, identity, cloud, and case management platforms, enabling organizations to automate repetitive Tier-1 investigation tasks while preserving their current security investments. Today, the company supports more than 300 enterprise and MSSP deployments worldwide across industries including financial services, healthcare, technology, manufacturing, government, telecommunications, and energy. Within the AI SOC market, Dropzone AI has built its portfolio around autonomous AI SOC Analysts that replicate the investigation techniques of experienced security analysts using coordinated AI agents. The platform autonomously investigates every security alert, enriches findings with contextual intelligence, generates decision-ready reports, and escalates only verified threats for human review, significantly reducing analyst workload and response times. Recent innovations, including the introduction of AI Threat Hunter, AI Threat Intelligence Analyst, and the company's broader Agentic SOC architecture, expand automation beyond alert triage into continuous threat hunting, threat intelligence, and detection engineering. By combining explainable AI reasoning with seamless integration into existing security ecosystems, Dropzone AI enables organizations to scale security operations without proportionally increasing analyst headcount, helping enterprises transition toward fully agentic security operations.
Products/Platforms/Solutions Offered	▪ AI SOC Analyst ▪ AI Threat Hunter ▪ AI Threat Intelligence Analyst
Geographic Presence	North America, Europe, and the Middle East & Africa

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.13 SIMBIAN

Founding Year	2023
Headquarters – Country	US
Headquarters – City/State	Mountain View, California
Ownership Type	Private
Business Overview	Simbian is a US-based autonomous security operations company focused on building a self-improving SecOps platform capable of defending organizations against AI-driven cyberattacks through reasoning-based autonomous AI. Unlike conventional SOAR or AI copilots that depend on static playbooks and manual intervention, Simbian applies enterprise-aware reasoning, contextual learning, and coordinated AI agents to automate complex security workflows across heterogeneous environments. Its platform integrates with existing SIEM, XDR, EDR, cloud, network, and threat intelligence solutions, enabling enterprises and managed security providers to modernize security operations without replacing their existing technology investments. Simbian primarily serves large enterprises, MSSPs, and MDR providers across financial services, healthcare, technology, manufacturing, telecommunications, government, and other highly regulated sectors. Within the AI SOC market, Simbian has positioned its Self-Improving SecOps Platform around a shared Context Lake and Reasoning Engine, enabling multiple AI agents to continuously learn from enterprise telemetry, analyst feedback, organizational knowledge, and threat intelligence. The platform unifies offensive and defensive security through specialized AI agents including the AI SOC Agent and AI Threat Hunt Agent that collaborate to investigate alerts, proactively identify threats, validate exposures, and automate response with minimal human intervention. Recent platform innovations have strengthened Simbian's vision of fully autonomous security operations by introducing reasoning-based investigations, continuous reinforcement learning, and coordinated multi-agent decision-making.
Products/Platforms/Solutions Offered	AI SOC Agent
Geographic Presence	North America, Europe, and Asia Pacific

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.14 PROPHET SECURITY

Founding Year	2023
Headquarters – Country	US
Headquarters – City/State	Palo Alto, California
Ownership Type	Private
Business Overview	Prophet Security is an agentic AI security operations company dedicated to transforming enterprise SOCs through reasoning-driven AI that automates investigations, threat hunting, detection engineering, and incident response. Built by former StackRox executives and cybersecurity practitioners, the company was founded to address the operational burden caused by alert overload, fragmented security tools, and increasing analyst shortages. Instead of replacing existing SIEM, EDR, XDR, SOAR, cloud, or identity security investments, Prophet Security integrates with customers' security ecosystem to deliver contextual investigations and autonomous workflows through a unified AI-powered platform. Designed for enterprise SOCs across financial services, healthcare, technology, manufacturing, retail, and other regulated industries, the platform enables organizations to modernize security operations while preserving existing security architectures. Since launching publicly in 2024, Prophet Security has rapidly expanded its market presence through significant venture funding and strategic investments that support the advancement of agentic AI for security operations. Within the AI SOC market, Prophet Security has built its portfolio around the Prophet Agentic AI SOC Platform, which combines specialized AI agents to automate the complete security operations lifecycle. The platform includes AI SOC Analyst and AI Threat Hunter, enabling organizations to investigate alerts, proactively hunt threats, strengthen detection coverage, and orchestrate response using explainable reasoning and organizational context. Prophet's AI continuously adapts through analyst feedback, internal documentation, and enterprise-specific knowledge to improve investigation quality over time. Recent investments from Accel, Amex Ventures, and Citi Ventures further reinforce the company's strategy of accelerating enterprise adoption of agentic AI SOC technologies that improve analyst productivity, reduce investigation time, and enable human analysts to focus on high-value security decisions.
Products/Platforms/Solutions Offered	▪ Agentic AI SOC Platform ▪ AI SOC Analyst ▪ AI Threat Hunter
Geographic Presence	North America

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.15 LEGION SECURITY

Founding Year	2024
Headquarters – Country	US
Headquarters – City/State	New York City, New York
Ownership Type	Private
Business Overview	Legion Security is an enterprise AI security company focused on redefining Security Operations Centers through browser-native agentic AI that learns directly from analysts rather than relying on static playbooks or predefined workflows. Legion observes how analysts investigate incidents, documents real-world workflows, and transforms that operational expertise into trusted AI agents capable of executing investigations while preserving enterprise governance and transparency. Instead of requiring APIs, custom integrations, or major infrastructure changes, the platform operates directly within analysts' existing browser-based workflows, enabling rapid deployment across complex enterprise security environments. The company primarily serves large enterprises in highly regulated industries seeking to modernize SOC operations without disrupting existing security investments. Within the AI SOC market, Legion has built its strategy around the Agentic Security Operations Platform, which progresses through Learning Mode, Companion Mode, and Autonomous Mode to gradually introduce trusted AI into security operations. Unlike conventional AI SOC platforms trained on generic datasets, Legion continuously learns analyst behavior, organizational context, historical investigations, runbooks, and playbooks before recommending or automating actions. This human-centric learning approach enables organizations to deploy AI agents that accurately reflect internal security processes while maintaining complete analyst oversight, explainability, and auditability. Built on Google Cloud infrastructure and powered by Google Gemini models, the platform helps enterprises reduce repetitive investigation tasks, improve response consistency, accelerate analyst productivity, and safely transition toward autonomous security operations through configurable, trust-based automation.
Products/Platforms/Solutions Offered	Agentic Security Operations Platform
Geographic Presence	North America and the Middle East & Africa

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.16 CYBERSILO

Founding Year	2022
Headquarters – Country	US
Headquarters – City/State	Aldie, Virginia
Ownership Type	Private
Business Overview	CyberSilo is a cybersecurity product company focused on building an AI-first security platform that unifies security operations, threat intelligence, compliance, and attack surface visibility within a single ecosystem. The company develops cloud-native security technologies that combine artificial intelligence with expert-led security operations to help organizations detect, investigate, and respond to cyber threats more efficiently. Its portfolio spans SIEM, threat intelligence, governance, risk and compliance (GRC), SAP security, exposure monitoring, and AI-powered SOC automation, enabling organizations to consolidate multiple security capabilities into an integrated platform. CyberSilo serves enterprises, managed security service providers (MSSPs), cloud service providers, telecommunications companies, financial institutions, healthcare organizations, manufacturers, educational institutions, government agencies, and other highly regulated industries requiring continuous cyber resilience. Within the AI SOC market, CyberSilo positions Agentic SOC AI as the centerpiece of its autonomous security operations strategy. The platform automates Level 1 and Level 2 SOC functions through AI-driven threat detection, alert triage, contextual investigation, MITRE ATT&CK-aligned analytics, and automated incident response while allowing analysts to focus on advanced investigations. Complementing this capability are ThreatHawk SIEM and ThreatHawk MSSP SIEM, which provide centralized telemetry collection, multi-tenant SOC management, and real-time threat intelligence. By combining AI-powered analytics with expert SOC oversight, CyberSilo enables organizations to reduce false positives, accelerate incident response, improve analyst productivity, and modernize security operations through an integrated AI-native cybersecurity platform.
Products/Platforms/Solutions Offered	▪ Agentic SOC AI ▪ ThreatHawk SIEM ▪ ThreatHawk MSSP SIEM
Geographic Presence	North America, Asia Pacific, and the Middle East & Africa

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.17 BRICKLAYER AI

Founding Year	2023
Headquarters – Country	US
Headquarters – City/State	Arlington, Virginia
Ownership Type	Private
Business Overview	Bricklayer AI is an agentic cybersecurity company focused on enabling enterprises to build a governed AI workforce for modern Security Operations Centers (SOCs). Rather than replacing analysts with isolated AI assistants, the company orchestrates teams of specialized AI agents that collaborate across security workflows while operating under enterprise-defined policies, human oversight, and full auditability. Built specifically for enterprise SOCs and managed security service providers (MSSPs), the platform integrates with existing SIEM, EDR, SOAR, threat intelligence, vulnerability management, and cloud security solutions, allowing organizations to modernize security operations without replacing their established security stack. By emphasizing context sharing, coordinated execution, institutional memory, and governance, Bricklayer AI helps organizations improve operational efficiency while maintaining transparency and compliance across security investigations. Within the AI SOC market, Bricklayer AI centers its innovation on the Agentic Cybersecurity Platform, which dynamically assembles specialized AI agents to execute investigation procedures, correlate evidence, perform threat intelligence analysis, orchestrate response actions, and document every decision with complete audit trails. Unlike traditional SOAR platforms that depend on static playbooks, Bricklayer's coordinated AI workforce continuously shares context, collaborates across multiple workflows, and executes organization-specific procedures under policy-based governance. The platform also provides shared workbenches where analysts and AI agents collaborate in real time, enabling security teams to reduce investigation time, accelerate incident response, and scale SOC operations while preserving human control over every security decision.
Products/Platforms/Solutions Offered	Bricklayer Agentic Cybersecurity Platform
Geographic Presence	North America

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.18 AUGUR

Founding Year	2014
Headquarters – Country	US
Headquarters – City/State	San Diego, California
Ownership Type	Private
Business Overview	Augur is an AI-driven cybersecurity company focused on shifting enterprise security from reactive detection to predictive threat prevention. The company applies machine learning, behavioral modeling, and large-scale internet telemetry to detect malicious infrastructure during its earliest stages—often weeks or months before attacks are launched. By continuously analyzing global routing activity, DNS changes, domain registrations, hosting behavior, spam traps, malware telemetry, and other infrastructure signals, Augur enables security teams to proactively disrupt adversary operations before weaponization. The platform is designed for enterprises operating in highly targeted sectors such as financial services, energy, telecommunications, critical infrastructure, healthcare, and government, where minimizing attack exposure and operational disruption is essential. Within the AI SOC market, Augur extends traditional threat intelligence by providing predictive intelligence that integrates directly with enterprise SIEM, SOAR, EDR, firewall, proxy, and cloud security environments. Its Augur Preemptive Cybersecurity Platform enables SOC analysts to enrich investigations with AI-driven infrastructure attribution, predictive threat intelligence, automated enforcement, and proactive threat hunting before attacks materialize. Complementary offerings such as Augur Investigate, Augur Brand Protection, and Augur Leaked Credentials further strengthen security operations by enabling infrastructure investigations, phishing prevention, and credential exposure monitoring from a unified intelligence platform. Through AI-powered behavioral analysis and automation, Augur helps organizations reduce alert fatigue, prioritize emerging threats, and transition toward proactive, intelligence-led security operations.
Products/Platforms/Solutions Offered	Augur Preemptive Cybersecurity Platform
Geographic Presence	North America, Europe, Asia Pacific, and the Middle East & Africa

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.19 BLINKOPS

Founding Year	2021
Headquarters – Country	US
Headquarters – City/State	Austin, Texas
Ownership Type	Private
Business Overview	BlinkOps is an agentic security operations company focused on transforming enterprise SOCs through AI-powered automation and autonomous security workflows. Founded by security and IT operations experts, the company helps organizations replace manual, playbook-driven security operations with intelligent AI agents capable of reasoning, collaborating, and executing security tasks at machine speed. BlinkOps integrates with more than 30,000 security, cloud, identity, IT, and DevOps applications, enabling enterprises to automate security operations across heterogeneous environments. The platform is designed for enterprise SOCs, MSSPs, and highly regulated industries including financial services, healthcare, technology, retail, manufacturing, telecommunications, and government. Within the AI SOC market, BlinkOps has built its strategy around the Blink Agentic Security Operations Platform, which combines AI reasoning, deterministic automation, and governed execution to automate the complete security operations lifecycle. The platform enables organizations to deploy specialized security micro-agents that autonomously perform alert triage, investigation, enrichment, case management, and response while maintaining human oversight through configurable guardrails. Complementing the platform are Agentic Studio for building enterprise AI agents and Workflow Studio for orchestrating security automation using natural language, low-code, or code-based workflows. By combining AI agents with trusted automation and an embedded AI-as-a-Service delivery model, BlinkOps enables enterprises to accelerate investigations, reduce analyst fatigue, and modernize SOC operations with explainable, enterprise-grade autonomous security.
Products/Platforms/Solutions Offered	▪ Blink Agentic Security Operations Platform ▪ Blink AI as a Service
Geographic Presence	North America and the Middle East & Africa

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.20 GRUVE

Founding Year	2024
Headquarters – Country	US
Headquarters – City/State	Redwood City, California
Ownership Type	Private
Business Overview	Gruve is a US-based AI-native enterprise services company specializing in secure AI transformation, helping organizations deploy AI infrastructure, intelligent agents, and cybersecurity solutions at enterprise scale. Built around a "chip-to-agent" operating model, the company combines expertise in AI infrastructure, data engineering, cloud platforms, cybersecurity, and AI agent development to help enterprises accelerate AI adoption while maintaining governance, compliance, and measurable business outcomes. Rather than delivering isolated consulting engagements, Gruve provides an integrated portfolio spanning AI infrastructure, data foundations, AI security, and managed AI operations. Its services support organizations across financial services, healthcare, government, manufacturing, telecommunications, retail, and other highly regulated industries seeking to modernize enterprise technology through AI-native architectures. Within the AI SOC market, Gruve delivers AI SOC as a managed transformation and operations service that embeds AI agents throughout the security operations lifecycle. The company combines autonomous AI with experienced SOC analysts to automate alert triage, threat investigation, enrichment, detection engineering, SOAR-driven response, compliance reporting, and continuous monitoring while preserving human oversight for critical security decisions. By integrating AI-native security operations with governance and operational expertise, Gruve enables organizations to reduce analyst workload, improve detection accuracy, accelerate incident response, and modernize SOC operations without replacing their existing security ecosystem.
Products/Platforms/Solutions Offered	▪ Gruve AI SOC Service ▪ Gruve Managed AI Security and DFIR
Geographic Presence	North America, Asia Pacific, and the Middle East & Africa

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.21 CYBERNX

Founding Year	2019
Headquarters – Country	India
Headquarters – City/State	Mumbai, Maharashtra
Ownership Type	Private
Business Overview	CyberNX is an India-based cybersecurity company delivering managed cyber defense, cloud security, governance, risk and compliance (GRC), and security operations services through an AI-driven operating model. Built around its cloud-native cybersecurity practice, the company helps organizations strengthen cyber resilience by combining managed detection and response, cloud security, digital risk monitoring, threat intelligence, incident response, and compliance services. As a CERT-In impaneled and ISO 27001:2022-certified cybersecurity provider, CyberNX serves organizations across banking, financial services, insurance, manufacturing, healthcare, retail, technology, and public sector industries. The company has expanded its global footprint with operations in the Middle East and the United States while continuously investing in its Cyber Defence Centres, managed security capabilities, and AI-powered security technologies. Within the AI SOC market, CyberNX delivers AI Managed SOC as a Service, which combines generative AI, machine learning, commercial threat intelligence, automation, and expert SOC analysts to improve threat detection, investigation, and response. Rather than replacing existing security investments, the service integrates with SIEM, SOAR, UEBA, EDR, cloud-native security platforms, and threat intelligence feeds to provide continuous monitoring, AI-assisted investigations, and proactive threat hunting. Complementing its AI SOC capabilities is the Peregrine managed security platform, which unifies MDR, threat hunting, threat intelligence, digital forensics, and brand risk monitoring under a single managed security ecosystem. Through AI-driven automation and 24×7 security operations, CyberNX helps enterprises reduce alert fatigue, accelerate response times, and strengthen operational resilience against evolving cyber threats.
Products/Platforms/Solutions Offered	▪ Peregrine ▪ CyberNX AI Managed SOC as a Service ▪ CyberNX Managed Detection and Response ▪ CyberNX Digital Forensics and Incident Response
Geographic Presence	Asia Pacific and the Middle East & Africa

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.22 ANVILOGIC

Founding Year	2019
Headquarters – Country	US
Headquarters – City/State	Palo Alto, California
Ownership Type	Private
Business Overview	Anvilogic is an AI-native security operations company focused on enabling enterprise SOCs to transition from legacy, manually operated security workflows to agentic, AI-driven security operations. Founded by former security leaders from Splunk, Symantec, and Proofpoint, the company was established to eliminate SIEM lock-in while allowing organizations to modernize detection engineering, threat hunting, investigation, and incident response without replacing their existing security infrastructure. Its platform operates across traditional SIEMs, modern security data lakes, and cloud storage environments, enabling security teams to search, analyze, and operationalize security data wherever it resides. Serving large enterprises across financial services, healthcare, telecommunications, manufacturing, retail, and critical infrastructure, Anvilogic helps organizations improve SOC efficiency while significantly reducing operational complexity and security data costs. Within the AI SOC market, Anvilogic has evolved into an Agentic SecOps Platform that applies AI across every stage of security operations through an integrated AI Operating System, specialized AI agents, and reusable Blueprints. Rather than limiting AI to investigation or alert triage, the platform automates data onboarding, federated search, detection engineering, threat investigations, and end-to-end SOC workflows while keeping analysts in control through governed approvals and transparent reasoning. Built on its Enterprise Security Graph, the platform continuously learns organizational context and enables enterprises to create custom AI workflows across heterogeneous environments. By combining agentic automation with open integration across SIEMs, data lakes, and cloud platforms, Anvilogic enables organizations to improve detection coverage, reduce manual effort, accelerate investigations, and scale modern security operations without increasing analyst headcount.
Products/Platforms/Solutions Offered	▪ Agentic SecOps Platform ▪ Agentic SOC
Geographic Presence	North America and Asia Pacific

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.23 AISTRIKE

Founding Year	2024
Headquarters – Country	US
Headquarters – City/State	Pleasanton, California
Ownership Type	Private
Business Overview	AiStrike is an AI-native cybersecurity company focused on reinventing enterprise security operations through a preemptive, autonomous cyber defense model. Founded by former Securonix executives with deep expertise in SIEM, threat detection, and security analytics, the company was established to help organizations move beyond reactive, alert-centric SOC operations toward continuous AI-driven cyber defense. Rather than relying solely on SIEM alerts, AiStrike correlates telemetry across cloud, identity, endpoints, networks, and security workflows to proactively identify exposures, strengthen detections, and stop threats before they become incidents. Built for large enterprises, MSSPs, and highly regulated industries, the platform integrates seamlessly with existing SIEM, XDR, SOAR, cloud, and identity security ecosystems, enabling customers to modernize security operations without replacing their existing infrastructure. In 2026, the company secured USD 7 million in seed funding to accelerate development of its AI-native security operations platform and expand global go-to-market activities. Within the AI SOC market, AiStrike delivers a Composite AI architecture that combines machine learning, knowledge graphs, threat intelligence, and autonomous AI agents to automate the complete security operations lifecycle. Its AiStrike for Security Operations platform continuously improves detection quality, eliminates security blind spots, automates investigations, and orchestrates response actions while learning from every investigation to enhance future detections. The company further expanded its AI SOC portfolio with the launch of AiStrike MDR, an AI-powered Managed Detection and Response service that combines AI-led investigations with expert-guided oversight to deliver scalable, autonomous security operations. By integrating detection engineering, threat hunting, investigation, response, and cloud security automation into a unified platform, AiStrike enables organizations to reduce analyst workload, maximize SIEM effectiveness, and transition from reactive SOC operations to continuously self-improving AI-driven cyber defense.
Products/Platforms/Solutions Offered	▪ AiStrike for Security Operations ▪ AiStrike Managed MDR ▪ AiStrike for MDR Providers
Geographic Presence	North America and Asia Pacific

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.24 D3 SECURITY

Founding Year	2012
Headquarters – Country	Canada
Headquarters – City/State	Vancouver, British Columbia
Ownership Type	Private
Business Overview	D3 Security is a cybersecurity company specializing in AI-driven security operations, incident response, and security orchestration for enterprise SOCs and MSSPs. Recognized as one of the pioneers of the SOAR market, the company has continuously evolved its platform from traditional incident response automation into an autonomous, AI-native security operations architecture. D3 integrates with more than 800 security technologies, enabling organizations to orchestrate investigations, automate workflows, manage cases, and reduce alert fatigue across complex hybrid environments. Its solutions are widely deployed by Fortune 500 enterprises, government agencies, financial institutions, healthcare providers, critical infrastructure organizations, and global MSSPs that require scalable, high-fidelity security operations. Over a decade of continuous innovation has positioned D3 as a leading provider of enterprise-grade security automation and autonomous SOC technologies. Within the AI SOC market, D3 has expanded beyond conventional SOAR with Morpheus, an accountable agentic AI SOC platform that autonomously performs investigation, triage, attack path discovery, and governed response across the complete alert lifecycle. Complementing Morpheus is Smart SOAR, which provides enterprise orchestration, codeless automation, case management, and extensive third-party integrations to streamline security operations. Unlike conventional AI copilots, Morpheus employs a purpose-built Cybersecurity Triage Reasoning Graph to conduct Level-2 investigations, dynamically generate response playbooks, and maintain transparent reasoning with configurable autonomy levels that preserve analyst oversight. By combining agentic AI with mature SOAR capabilities, D3 enables organizations to achieve continuous alert coverage, reduce analyst workload, accelerate incident response, and modernize security operations while maintaining governance, auditability, and regulatory compliance.
Products/Platforms/Solutions Offered	▪ D3 Morpheus ▪ D3 Smart SOAR
Geographic Presence	North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.25 RIVERSAFE

Founding Year	2010
Headquarters – Country	UK
Headquarters – City/State	London
Ownership Type	Private
Business Overview	RiverSafe is a UK-based cybersecurity consultancy and managed security services provider specializing in Security Operations Centre (SOC) transformation, AI-enabled cyber defense, DevSecOps, and application security. Founded by cybersecurity professionals Oseloka Obiora and Suid Adeyanju, the company has evolved from a specialist cybersecurity consultancy into a broader security engineering and digital resilience partner serving complex enterprise environments. RiverSafe works with many of the world's leading organizations, including Vodafone, BP, Tesco, Deliveroo, Sky, Virgin Media O2, Safaricom, and SMBC, to modernize security architectures, optimize SIEM deployments, strengthen cloud security, and improve operational resilience. Rather than delivering standalone security products, the company combines consulting expertise, managed services, and strategic technology partnerships with vendors such as Splunk, Exabeam, Microsoft Sentinel, Cribl, and Google SecOps to maximize customers' existing security investments. Within the AI SOC market, RiverSafe focuses on helping enterprises build next-generation AI-enabled Security Operations Centers through AI-Driven SOC Services and SOC Modernisation Services. Its approach integrates artificial intelligence into threat detection, SIEM optimization, vulnerability management, SOAR automation, and security analytics while maintaining expert human oversight throughout the security lifecycle. Rather than promoting autonomous AI platforms, RiverSafe emphasizes practical AI adoption by helping organizations deploy intelligent threat detection, AI-assisted investigations, automated incident response playbooks, and adaptive SOC workflows that improve detection accuracy while reducing analyst workload. Through advisory, implementation, optimization, and managed security engagements, RiverSafe enables enterprises to transition from legacy SOC architectures toward scalable, AI-driven security operations aligned with evolving cyber threats and business objectives.
Products/Platforms/Solutions Offered	▪ RiverSafe AI-Driven SOC Services ▪ RiverSafe SOC Modernisation Services
Geographic Presence	North America, Europe, and the Middle East & Africa

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.26 SOC JEDI.AI

Founding Year	2024
Headquarters – Country	US
Headquarters – City/State	San Francisco, California
Ownership Type	Private
Business Overview	SOC Jedi.AI is an AI-native cybersecurity company focused exclusively on automating Security Operations Center (SOC) investigations through autonomous AI analysts. The company delivers an AI-driven investigation platform capable of handling alert triage, contextual enrichment, hypothesis generation, malware analysis, and incident reporting without disrupting existing SOC infrastructure. Available as both SaaS and fully on-premises deployments, the platform integrates with SIEM, EDR, XDR, IRP, data lakes, and threat intelligence platforms to help enterprises modernize security operations while maintaining complete control over sensitive security data. The solution is designed for enterprise SOCs, MSSPs, government agencies, financial institutions, healthcare organizations, and other security-conscious industries seeking to reduce analyst fatigue and improve operational efficiency. Within the AI SOC market, SOC Jedi.AI has developed an AI SOC Automation Platform centered around its AI SOC Analyst, which orchestrates multiple specialized AI agents to automate end-to-end security investigations. Supporting agents, including ML Pre-Scoring, Reverse Engineer, External IT Auditor, and Darknet Monitoring, work together to reduce false positives, enrich investigations, identify zero-day threats, assess attack paths, and monitor external cyber risks. The platform leverages historical incident data, machine learning, threat intelligence, and hypothesis modeling to generate SOC-grade investigation reports while enabling analysts to focus on high-priority threats. By combining explainable AI with continuous automation, SOC Jedi.AI enables organizations to reduce investigation time, improve detection accuracy, and accelerate incident response across modern enterprise SOC environments.
Products/Platforms/Solutions Offered	▪ AI SOC Automation Platform ▪ AI SOC Platform Agents ▪ SOC Jedi.AI for MSSPs
Geographic Presence	North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America

Source: Company Website

JULY 2026 © MarketsandMarkets™

15.2.27 VULNURIS

Founding Year	2018
Headquarters – Country	India
Headquarters – City/State	Pune, Maharashtra
Ownership Type	Private
Business Overview	Vulnuris is an India-based cybersecurity company delivering AI-powered cyber defense, managed security services, governance, cloud security, application security, and enterprise risk management through a unified security portfolio. Originally established as Newtons Apple Security Solutions, the company rebranded to Vulnuris to reflect its broader vision of providing end-to-end cyber resilience. Built around its "Find, Fix, Fortify" framework, Vulnuris combines offensive security, continuous monitoring, AI-driven threat intelligence, and strategic advisory services to help organizations proactively strengthen their cybersecurity posture. The company serves enterprises across IT, manufacturing, healthcare, BFSI, fintech, education, government, and critical infrastructure while maintaining operations in India, the United States, the UAE, and Kuwait. Its portfolio spans cloud security, GRC, managed services, industrial security, privacy, vulnerability management, and enterprise cyber defense. Within the AI SOC market, Vulnuris delivers an AI Security Operations Center (AI SOC) designed to automate modern security operations through autonomous threat detection, intelligent event correlation, behavioral analytics, risk prioritization, and automated incident response. The platform ingests telemetry from cloud, endpoint, identity, email, applications, and network environments to provide centralized visibility while significantly reducing false positives and accelerating response times. Complementing AI SOC are the company's managed detection, threat intelligence, and cyber risk services that enable enterprises to modernize security operations without expanding analyst teams. By combining agentic AI with expert SOC oversight, Vulnuris enables organizations to improve detection accuracy, reduce operational costs, strengthen compliance readiness, and transition from reactive monitoring to intelligent, AI-driven cyber defense.
Products/Platforms/Solutions Offered	AI Security Operations Center
Geographic Presence	North America, Asia Pacific, and the Middle East & Africa

Source: Company Website

JULY 2026 © MarketsandMarkets™

16 RESEARCH METHODOLOGY

16.1 RESEARCH DATA

The research study was developed through a structured combination of extensive secondary research and targeted primary research to establish a reliable, market-specific view of the AI Security Operations Center market. Secondary research included company annual reports, investor presentations, product documentation, regulatory publications, technical papers, industry databases, cybersecurity standards, and credible third-party sources. Information from organizations such as the MITRE Corporation, the National Institute of Standards and Technology, the Cybersecurity and Infrastructure Security Agency, the European Union Agency for Cybersecurity, and other recognized cybersecurity bodies was used to define the market, identify relevant technologies, assess adoption trends, and validate the evolving role of artificial intelligence in security operations.

The primary research program involved participants across the AI SOC ecosystem, including cybersecurity technology vendors, AI SOC platform providers, managed security service providers, system integrators, cloud service providers, security consultants, government and regulatory organizations, and enterprise security teams. In-depth interviews and structured discussions were conducted with chief information security officers, SOC leaders, security architects, detection and response specialists, AI and cybersecurity professionals, product executives, and senior decision-makers. These interactions were used to validate market assumptions, technology adoption patterns, vendor positioning, customer priorities, deployment challenges, purchasing criteria, and revenue estimates.

The study also examined the convergence of SIEM, XDR, SOAR, security analytics, threat intelligence, automated investigation, generative AI, and agentic security operations. Particular emphasis was placed on distinguishing currently deployed and revenue-generating capabilities from announced roadmaps, early-stage pilots, and unverified marketing claims. Vendor participation in the market was assessed using product availability, breadth of AI SOC functionality, customer adoption, geographic reach, partner ecosystem, market-specific revenue, and evidence of commercial deployment.

Key market participants were initially identified through secondary research and subsequently evaluated through primary interviews, company disclosures, product reviews, customer references, funding and growth activity, and other market evidence. The resulting market size, competitive landscape, and company positioning were triangulated across multiple sources to improve consistency, minimize estimation bias, and provide a current and contextual assessment of the global AI SOC market.

JULY 2026 © MarketsandMarkets™

The following illustrative figure highlights the market research methodology applied in making the report on the global AI SOC market:

FIGURE 59 AI SOC MARKET: RESEARCH DESIGN



Source: Secondary Research, Industry Experts, and MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

16.1.1 SECONDARY DATA

Market sizes of companies offering AI SOC software platforms and services were arrived at based on secondary data available through paid and unpaid sources. These were also arrived at by analyzing the product portfolios of major companies and rating them based on the performance and quality of products offered. Secondary research was mainly used to obtain key information about the industry's supply chain, country-wise technology spending, total pool of key players, market classification and segmentation, key developments from both market and technology-oriented perspectives, economic trends, and currency exchange rates. For instance, the market sizes of companies offering AI SOC software platforms & services were based on secondary data available through paid databases and publicly available information.

In the secondary research process, various sources were referred to for identifying and collecting information for this study. The secondary sources included annual reports, press releases, investor presentations of companies; white papers, journals, certified publications; and articles from recognized authors, directories, and databases.

FACTORS CONSIDERED FOR ESTIMATING MARKET SIZE ARE AS FOLLOWS:

- Technological initiatives undertaken by governments of different countries
- Gross domestic product (GDP) growth
- Information and communications technology (ICT) spending
- Recent market developments
- Market ranking analysis of major AI SOC solution providers

16.1.2 PRIMARY DATA

Various primary sources from the supply and demand sides were interviewed to obtain qualitative and quantitative information for this report in the primary research process. The primary sources from the supply side included various industry experts, including Chief Executive Officers (CEOs), Vice Presidents (VPs), marketing directors, technology and innovation directors, and related key executives from various key companies and organizations operating in the AI SOC market.

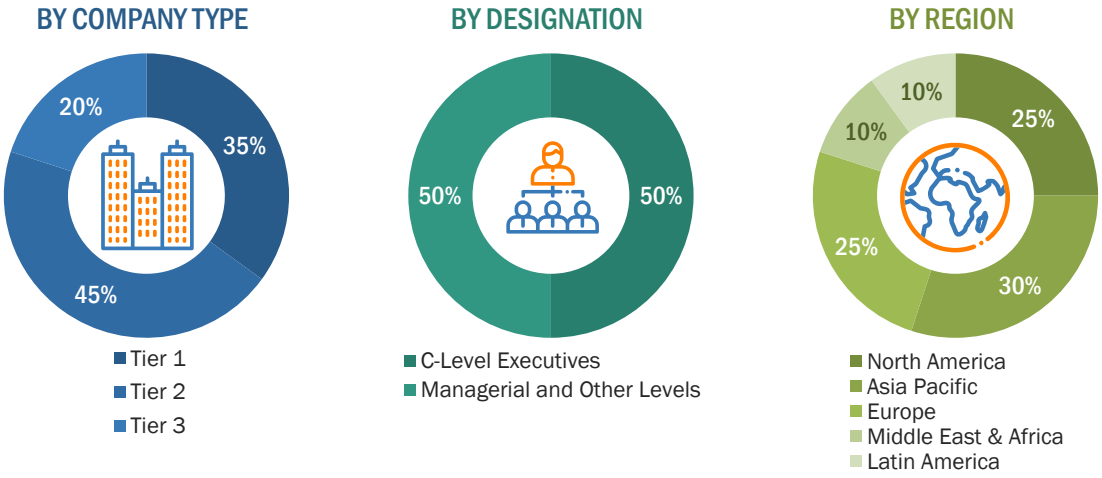
In the market engineering process, top-down and bottom-up approaches and several data triangulation methods were extensively used to perform market estimation and market forecasting for the overall market segments and subsegments listed in this report. The complete market engineering process involved extensive qualitative and quantitative analysis to list key information/insights throughout the report.

After the complete market engineering process (calculations for market statistics, market breakups, market size estimations, market forecasts, and data triangulation), extensive primary research was conducted to gather information and verify and validate the critical numbers arrived at. The primary research was also conducted to identify the segmentation types; industry trends; the competitive landscape of the AI SOC market players; and the key market dynamics, such as drivers, restraints, opportunities, challenges, and key strategies.

JULY 2026 © MarketsandMarkets™

16.1.2.1 Breakup of primary profiles

FIGURE 60 BREAKUP OF PRIMARY PROFILES, BY COMPANY TYPE, DESIGNATION, AND REGION



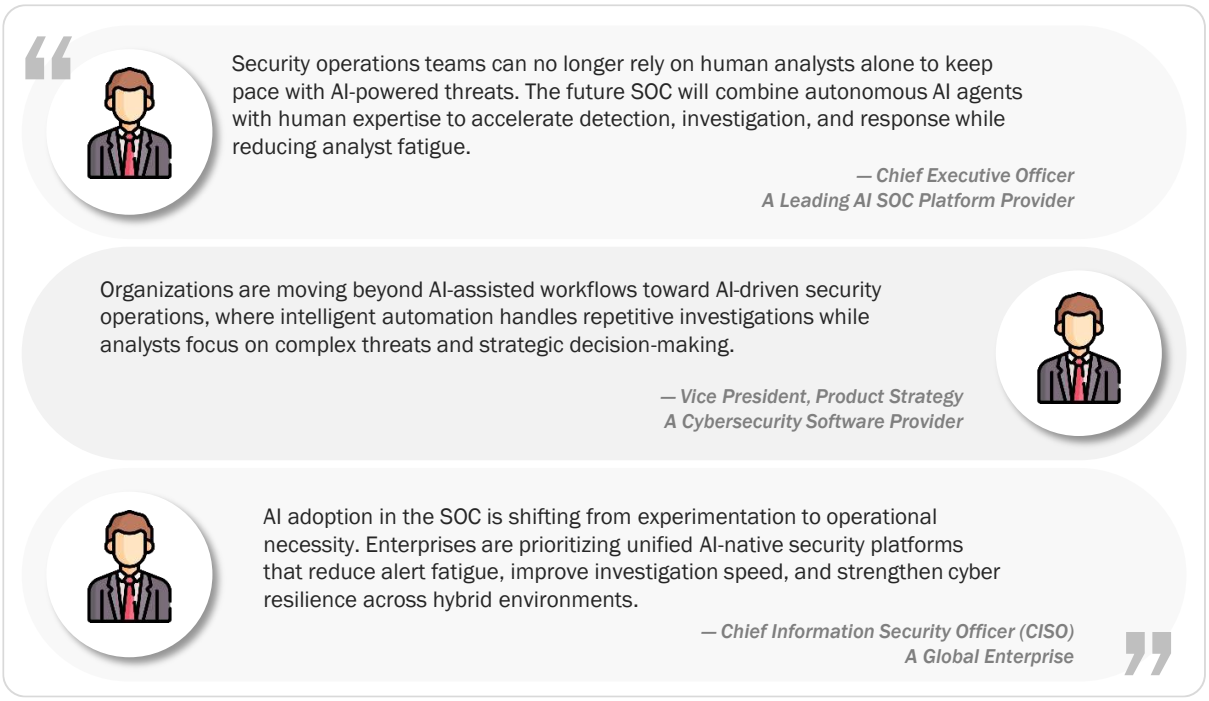
Note: Others include sales managers, marketing managers, and product managers.

The annual revenue of tier I companies is greater than USD 5 billion; the annual revenue of tier II companies is between USD 1 billion and 5 billion; and the annual revenue of tier III companies is below USD 500 million.

Source: Industry Experts, MarketsandMarkets Analysis

16.1.2.2 Key industry insights

FIGURE 61 KEY INSIGHTS FROM INDUSTRY

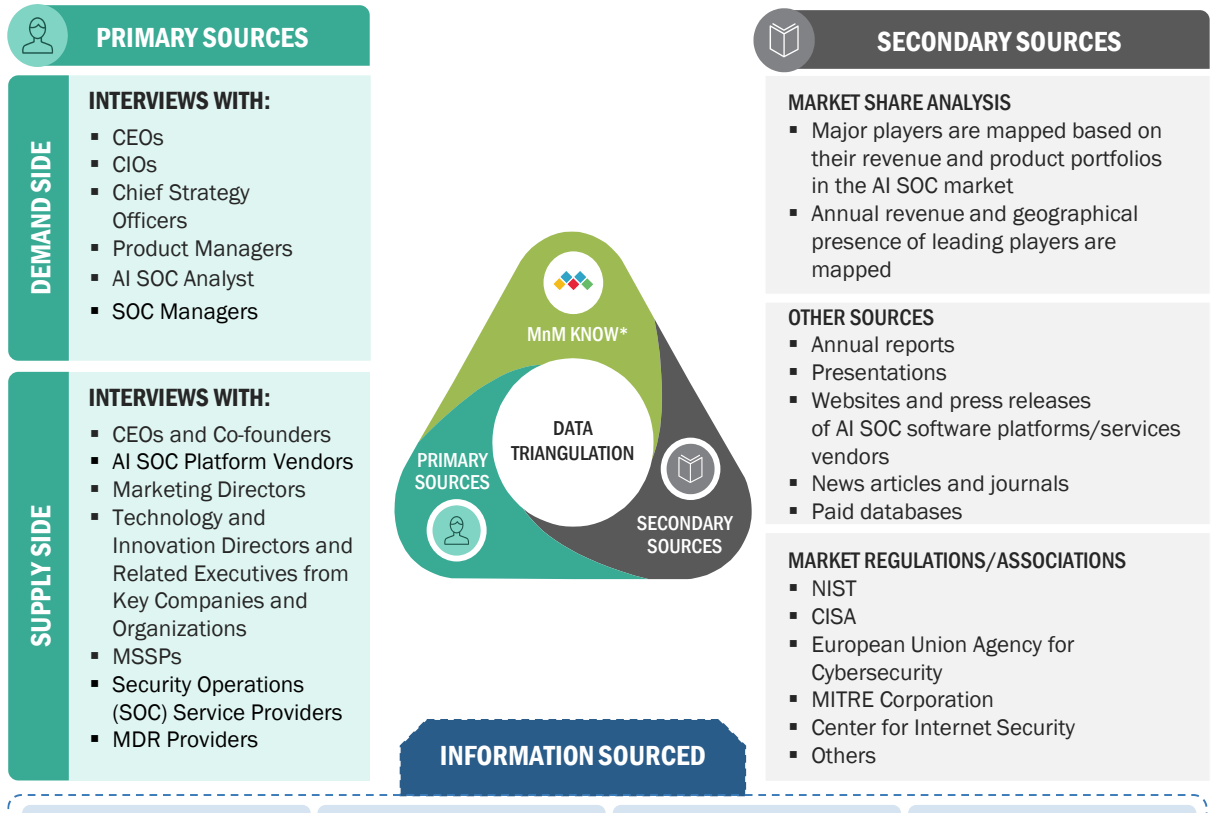


Source: Industry Experts

JULY 2026 © MarketsandMarkets™

16.2 DATA TRIANGULATION

FIGURE 62 DATA TRIANGULATION

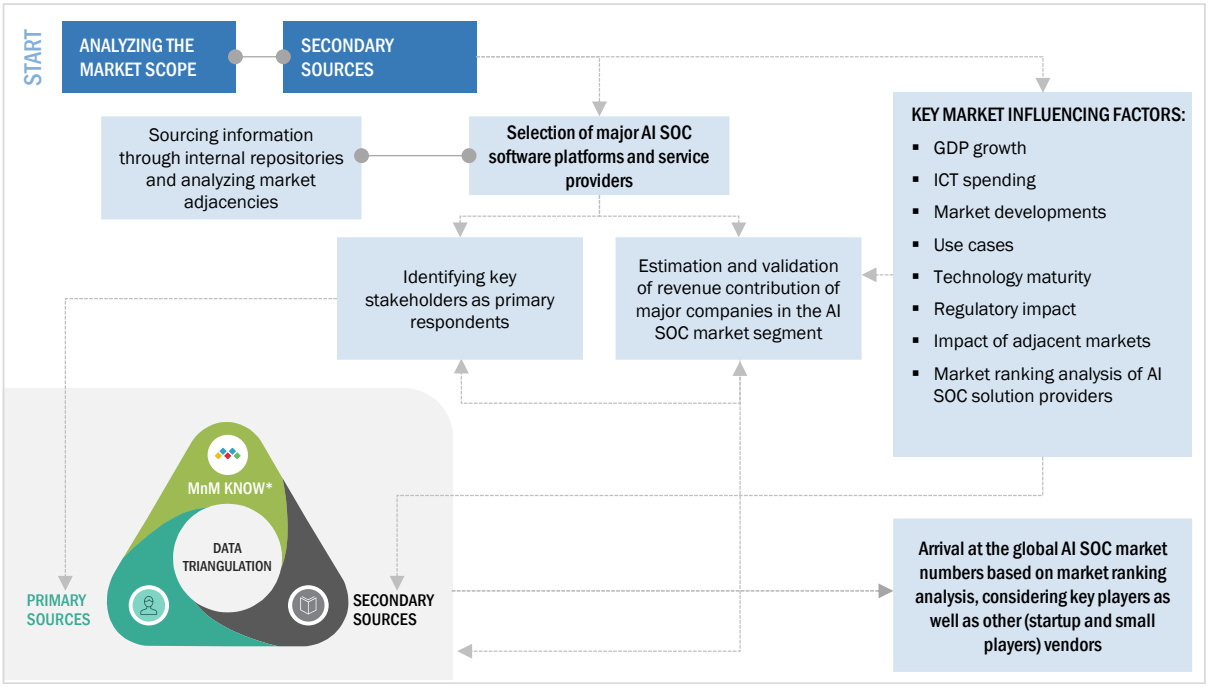


*MnM KNOW stands for MarketsandMarkets' "Knowledge Asset Management" framework. It refers to the existing market research knowledge repository of over 5,000 granular markets, our flagship competitive intelligence and market research platform "KnowledgeStore," subject matter experts, and independent consultants. MnM KNOW acts as an independent source that helps us validate information gathered from primary and secondary sources.

Source: MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

FIGURE 63 AI SOC MARKET: RESEARCH FLOW



Source: MarketsandMarkets Analysis

16.3 MARKET SIZE ESTIMATION

Multiple approaches were adopted to estimate and forecast the AI SOC market size. In the market engineering process, top-down and bottom-up approaches and several data triangulation methods were extensively used to perform market estimation and market forecasting for the overall market segments and sub-segments listed in this report. Extensive qualitative and quantitative analysis was performed on the complete market engineering process to list key information/insights throughout the report.

This procedure included studying top market players' annual and financial reports and extensive interviews for key insights from industry leaders, such as CEOs, VPs, directors, and marketing executives. All percentage splits and breakups were determined using secondary sources and verified through primary sources. All possible parameters that affect the market covered in this research study have been accounted for, viewed in extensive detail, verified through primary research, and analyzed to get the final quantitative and qualitative data. This data is consolidated and added to detailed inputs and analysis from MarketsandMarkets.

Top-down and bottom-up approaches were used to estimate and validate the size of the global AI SOC market and the size of various dependent subsegments. The research methodology used to estimate the market size included the following details:

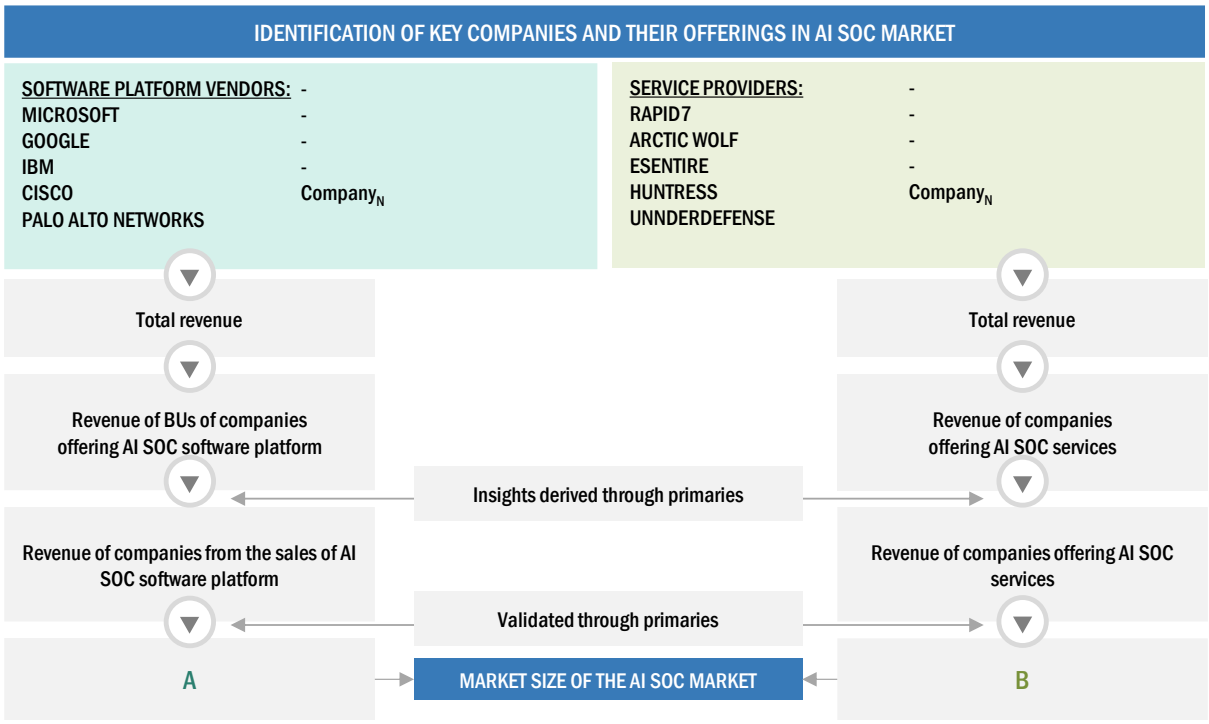
- The key players in the market were identified through secondary research, and their revenue contributions in respective regions were determined through primary and secondary research.
- This procedure included studying top market players' annual and financial reports and extensive interviews for key insights from industry leaders, such as CEOs, VPs, directors, and marketing executives.
- All percentage splits and breakups were determined using secondary sources and verified through primary sources.

JULY 2026 © MarketsandMarkets™

All possible parameters that affect the market and have been covered in this research study have been accounted for, viewed in extensive detail, verified through primary research, and analyzed to get the final quantitative and qualitative data. This data is consolidated and added to detailed inputs and analysis from MarketsandMarkets.

The first approach involves the estimation of the market size by the summation of companies' revenue generated through the sale of software platforms and services.

FIGURE 64 APPROACH 1 (SUPPLY-SIDE ANALYSIS): REVENUE OF SOFTWARE PLATFORMS/SERVICES IN AI SOC MARKET



**Key companies contribute to more than 70–75% of the total market*

Source: MarketsandMarkets Analysis

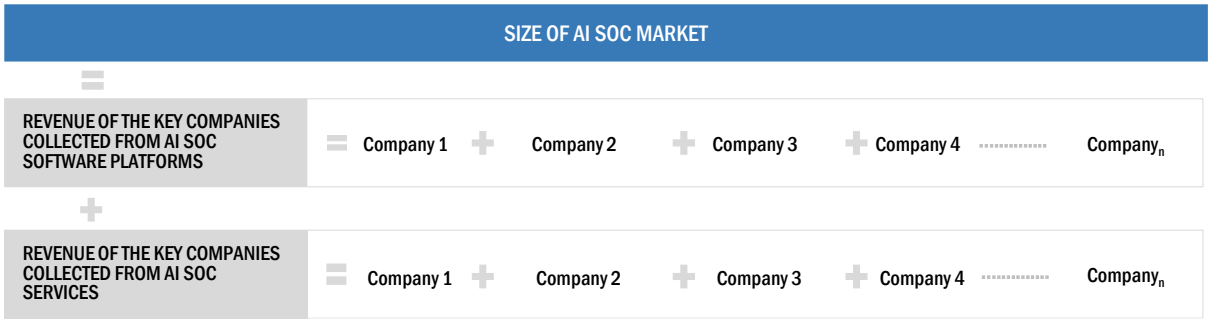
JULY 2026 © MarketsandMarkets™

FIGURE 65 MARKET SIZE ESTIMATION METHODOLOGY: APPROACH 1, SUPPLY-SIDE ANALYSIS

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
Identification of top companies operating in the AI SOC market	A. Identification of AI SOC software platforms and services offered by each vendor B. Identification of key use cases in the AI SOC market	Calculation of the cumulative market size of companies in the AI SOC market	Calculation of the market share of the top companies in the AI SOC market using the calculated market size	Revalidation of the total market size and market share estimations through primary respondents
KEY SOURCE OF INFORMATION:				
Secondary sources such as company financials, press releases, paid databases (Factiva), and primary research	Secondary sources such as company financials, press releases, paid databases (Factiva), and primary research	Company financials, annual reports, paid databases, and MarketsandMarkets analysis	MarketsandMarkets calculations	Primary research with stakeholders such as CXOs, VPs, marketing directors, and technology and innovation directors

Source: MarketsandMarkets Analysis

FIGURE 66 APPROACH 2, BOTTOM-UP (SUPPLY SIDE): COLLECTIVE REVENUE FROM ALL OFFERINGS IN AI SOC MARKET



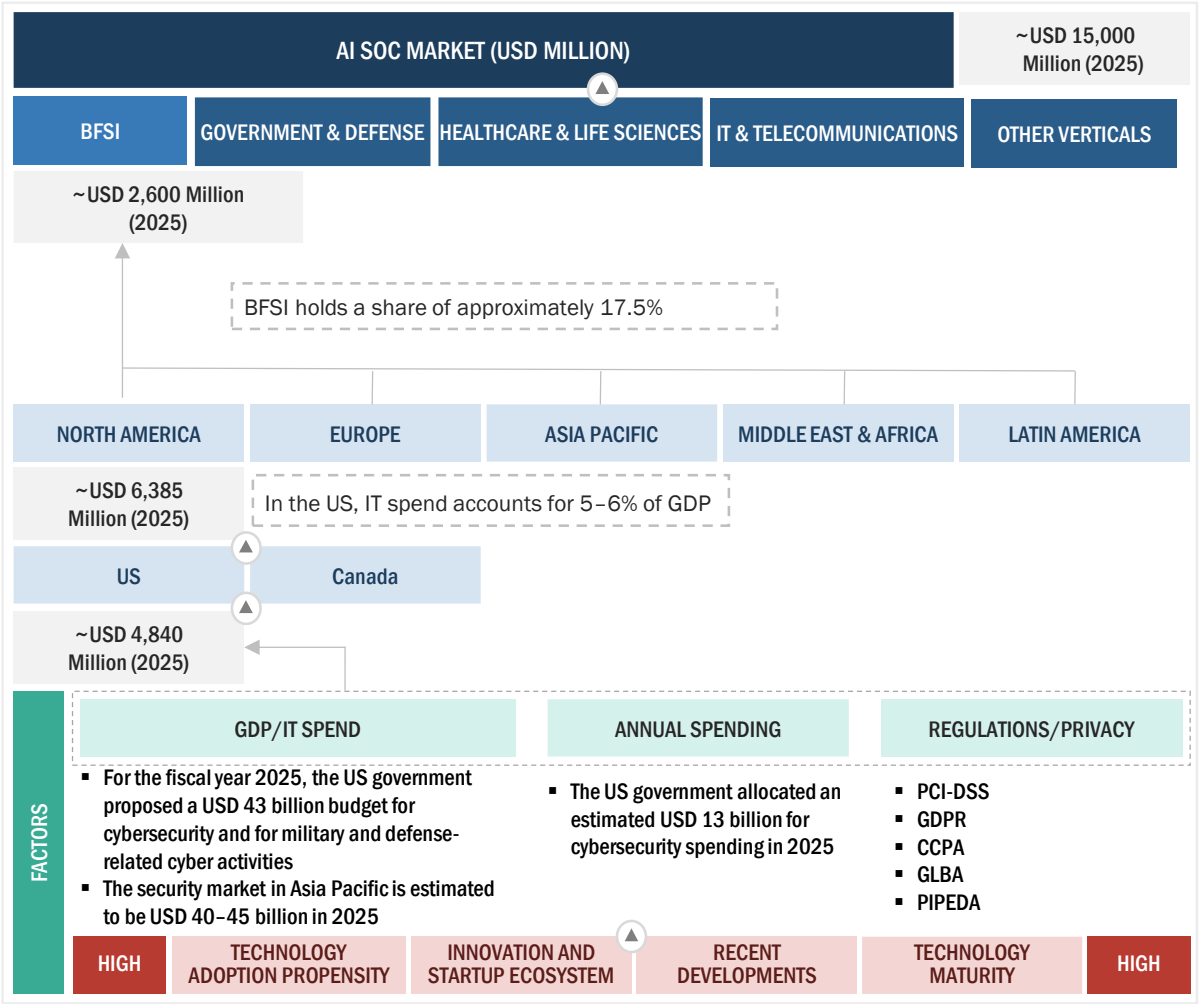
Source: MarketsandMarkets Analysis

The market sizes of companies offering AI SOC were arrived at based on the secondary data available through paid and unpaid sources. These were also arrived at by analyzing the product portfolios of major companies and rating them based on the performance and quality of the products offered.

After confirming these companies through primary interviews with industry experts, MarketsandMarkets estimated their total revenue through annual reports, SEC filings, and paid databases. These companies' revenue pertaining to the business units (BUs) that offer AI SOC software platforms was identified through similar sources. Then, through primaries, MarketsandMarkets collected data for the revenue generated through specific AI SOC software platforms and services. The collective revenue of key companies offering the AI SOC software platforms comprised 65–70% of the market, while AI SOC services comprised 30–35% of the market, again confirmed through primary interviews with industry experts. With the assumption that the rest of the market is contributed to by smaller players (part of the unorganized market), we arrived at the global size of the AI SOC market.

JULY 2026 © MarketsandMarkets™

FIGURE 67 MARKET SIZE ESTIMATION METHODOLOGY (TOP-DOWN APPROACH): DEMAND-SIDE ANALYSIS



Source: MarketsandMarkets Analysis

The top-down approach segmented the overall AI SOC market into software platforms and services. The software segment includes AI-enabled SIEM, XDR, SOAR, security analytics, threat detection, automated investigation, incident response, and agentic SOC solutions. The services segment includes managed SOC and MDR services, advisory and consulting, implementation and integration, training, and support and maintenance. Revenue generated from both technology solutions and associated services was considered to estimate the total AI SOC market, valued at approximately USD 15.0 billion in 2025.

JULY 2026 © MarketsandMarkets™

16.4 MARKET FORECAST

Factors that directly or indirectly impact the market were analyzed to estimate the market's overall trend during the forecast period. Each factor was analyzed on a scale of 1–3, with 1 being the lowest and 3 being the highest. After analyzing each factor and its impact on the market, various forecasting techniques were used to arrive at the market size.

TABLE 504 FACTOR ANALYSIS

FACTOR	INFERENCE	IMPACT
Increasing AI-Powered Cyberattacks	The rapid growth in AI-assisted phishing, malware, ransomware, and automated attack campaigns is increasing the need for AI-native security operations capable of detecting and responding to threats at machine speed. Organizations are accelerating investments in AI SOC platforms to improve resilience against sophisticated cyber threats.	High
Enterprise AI & Cloud Adoption	Enterprises are increasingly adopting cloud-native, hybrid, and AI-enabled environments, expanding the attack surface and creating demand for AI-driven SOC platforms that provide continuous monitoring, threat detection, and automated response across distributed infrastructures.	High
SOC Analyst Shortage & Alert Fatigue	Organizations continue to face a shortage of skilled cybersecurity professionals while managing overwhelming alert volumes. AI SOC solutions help automate alert triage, investigation, and prioritization, improving operational efficiency and reducing analyst workload.	High
Agentic AI & Autonomous Security Operations	The emergence of autonomous AI agents capable of investigating and responding to cyber incidents is transforming traditional SOC operations. Enterprises are gradually shifting from AI-assisted workflows toward autonomous security operations with appropriate human oversight.	High
Technology Maturity & AI Innovation	Advances in generative AI, large language models (LLMs), machine learning, behavioral analytics, and AI copilots are improving threat detection accuracy, investigation speed, and response automation, strengthening enterprise confidence in AI SOC platforms.	High
Cybersecurity Regulations & AI Governance	Governments and regulatory bodies are strengthening cybersecurity, AI governance, and critical infrastructure protection requirements. These developments are encouraging organizations to adopt AI-enabled security operations while maintaining transparency, explainability, and human oversight.	Medium–High
Growth of Managed Security Services	Increasing adoption of Managed Detection and Response (MDR), SOC-as-a-Service, and managed security services is expanding opportunities for AI-powered SOC platforms that enable scalable, automated security operations for enterprises and SMEs.	Medium–High
Enterprise Digital Transformation	Continued investments in digital transformation, cloud modernization, IoT, SaaS applications, and remote work environments are increasing the need for intelligent SOC platforms capable of securing complex enterprise ecosystems through AI-driven monitoring and response.	Medium–High
Unified Security Platform Adoption	Organizations are increasingly consolidating SIEM, SOAR, XDR, threat intelligence, identity security, and cloud security capabilities into unified AI-native security platforms to improve operational visibility, simplify management, and reduce tool sprawl.	High

JULY 2026 © MarketsandMarkets™

Human-AI Collaboration & Trust	Enterprises continue to adopt AI within SOC environments while maintaining human oversight for critical decision-making. Improving explainability, trust, governance, and collaboration between AI systems and security analysts remains essential for broader adoption of autonomous SOC capabilities.	Medium–High

Source: MarketsandMarkets Analysis

16.5 RESEARCH ASSUMPTIONS

The following assumptions were taken into consideration to complete the overall market engineering for the AI SOC market:

TABLE 505 RESEARCH ASSUMPTIONS

PARAMETER	ASSUMPTION
Global AI SOC Market Size	Market size estimates are conservative/realistic as opposed to pessimistic/aggressive.
Exchange Rate	Dollar fluctuations are not expected to be serious enough to affect the forecasts to a significant extent. A fall in the dollar value is expected to enhance revenue growth opportunities for US multinationals. In contrast, stability in the dollar value is expected to stabilize the price of imports and exports.
Quantitative Assumption	The market size may not add up to the total, as it has been rounded off. A quantitative analysis of the adjacent markets, including SIEM, SOAR, XDR, MDR, threat intelligence, and AI in cybersecurity, is considered to evaluate the AI SOC market.
Global Economic Condition	The global economy is assumed to remain largely stable despite macroeconomic uncertainties such as inflation, geopolitical tensions, regulatory changes, and fluctuations in enterprise IT budgets. However, increasing cyber threats are expected to sustain cybersecurity investments.
Geographic Analysis	Major and emerging economies have been studied to analyze the market regarding value and size. Major countries in North America, Europe, Asia Pacific, the Middle East and Africa, and Latin America have been studied and analyzed. However, similar trends have been assumed for the rest of the countries, as observed in the major economies.
Software	Enterprise spending on AI-powered cybersecurity software is expected to increase as organizations modernize security operations, automate threat detection and response, and secure cloud and hybrid environments against increasingly sophisticated AI-enabled cyber threats.
Service	The managed security services, MDR, SOC-as-a-Service, consulting, and incident response segments are expected to witness steady growth as organizations increasingly outsource security operations to address talent shortages, reduce operational complexity, and improve cyber resilience.
Financial Statistics	All the revenue and financial insights were extracted from company websites or annual reports, which are true to the best of MarketsandMarkets' knowledge.

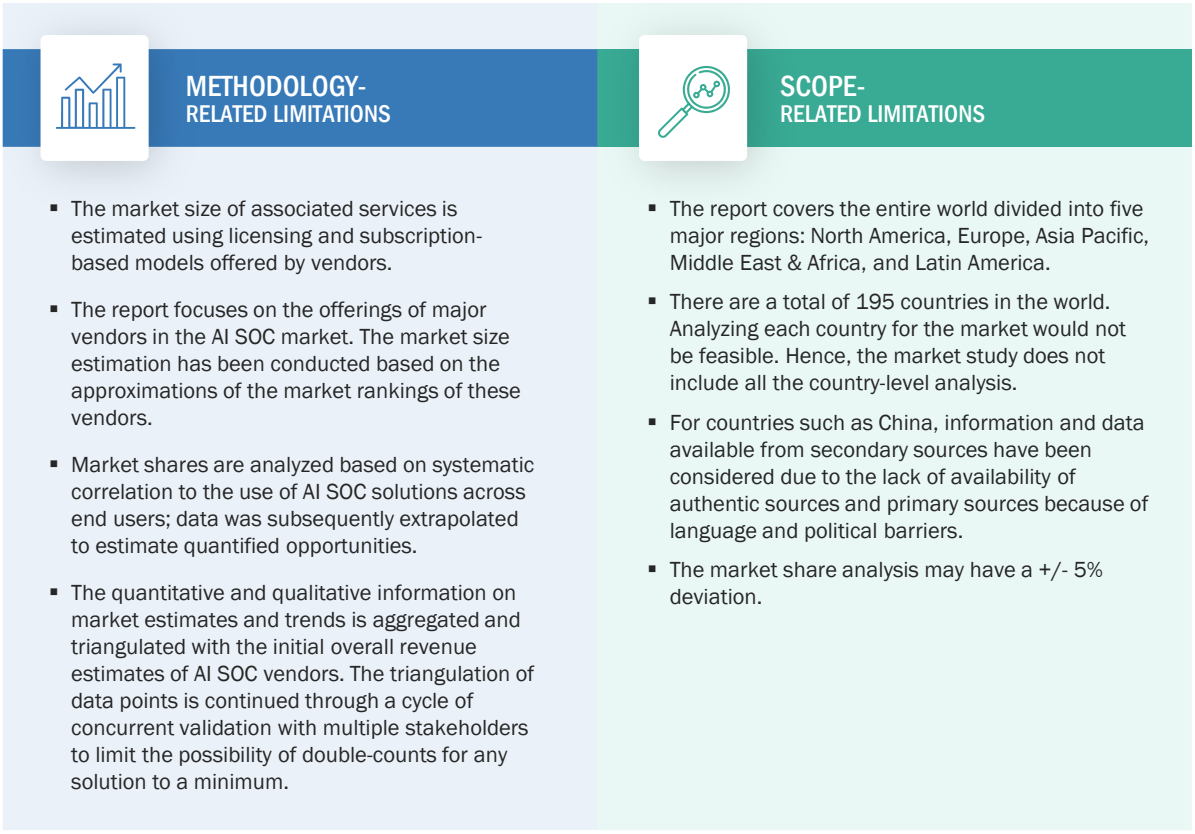
Source: MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

16.6 LIMITATIONS & RISK ASSESSMENT

The following limitations were taken into consideration to complete the overall market engineering process of the AI SOC market.

FIGURE 68 LIMITATIONS & RISK ASSESSMENT



Source: MarketsandMarkets Analysis

JULY 2026 © MarketsandMarkets™

17 APPENDIX

17.1 DISCUSSION GUIDE

A discussion guide is a set of questions and pain points for which an analyst wants to gain insights from industry and subject matter experts.

We are conducting a global AI security operations center (SOC) market study focusing on current trends and opportunities. The report provides comprehensive details and forecast analysis of the overall market and its submarkets. It also features a detailed analysis of the opportunities, market drivers, restraints, roadmaps, competitive landscape, and profiles of key industry players.

NAME
Designation
Company Name
Phone No
Email ID

Q. 1. Could you provide a brief on your offerings related to the AI SOC market?

Primary's Viewpoint: _____

Q. 2. How do you see the growth of the AI SOC market globally, now, and in the next five years? What would be the projected market size and growth rate of the market between 2026 and 2031, respectively?

Primary's Viewpoint: _____

Q. 3. What are the AI SOC market's top three drivers, restraints, opportunities, and challenges?

SR. NO.	DRIVERS	RESTRAINTS	OPPORTUNITIES	CHALLENGES
1				
2				
3				

Q. 4. We have segmented the AI SOC market based on offering, as given below. According to you, which offering is the most attractive in terms of market opportunities now and in the future? Please rate on a scale of 1–2, with 2 being the most lucrative.

SR. NO.	OFFERING	ATTRACTIVENESS OF OPPORTUNITY, 2026	ATTRACTIVENESS OF OPPORTUNITY, 2031
1	Solutions		
2	Services		

JULY 2026 © MarketsandMarkets™

Q. 5. We have segmented the AI SOC market based on software platforms, as given below. According to you, which is the most attractive in terms of market opportunities now and in the future? Please rate on a scale of 1–7, with 7 being the most lucrative.

SR. NO.	SOFTWARE PLATFORMS	ATTRACTIVENESS OF OPPORTUNITY, 2026	ATTRACTIVENESS OF OPPORTUNITY, 2031
1	AI-enabled Detection and Analytics Platforms		
2	AI-orchestrated Response and Automation Platforms		
3	AI-native SOC Platforms		
4	AI SOC Agent Solutions		
5	Security Data Platforms		
6	Threat Intelligence Platforms		
7	AI Governance, Risk, and Compliance Solutions		

Q. 6. We have segmented the AI SOC market based on services, as given below. According to you, which is the most attractive in terms of market opportunities now and in the future? Please rate on a scale of 1–4, with 4 being the most lucrative.

SR. NO.	SERVICES	ATTRACTIVENESS OF OPPORTUNITY, 2026	ATTRACTIVENESS OF OPPORTUNITY, 2031
1	AI-augmented Managed Detection and Response (MDR)		
2	AI SOC-as-a-Service (SOCaaS)		
3	Incident Response and Forensics Services		
4	Threat Intelligence and Advisory Services		

Q. 7. We have segmented the AI SOC market based on organization size, as given below. According to you, which is the most attractive in terms of market opportunities now and in the future? Please rate on a scale of 1–2, with 2 being the most lucrative.

SR. NO.	ORGANIZATION SIZE	ATTRACTIVENESS OF OPPORTUNITY, 2026	ATTRACTIVENESS OF OPPORTUNITY, 2031
1	Large Enterprises		
2	Small and Medium-Sized Enterprises (SMEs)		

JULY 2026 © MarketsandMarkets™

Q. 8. We have segmented the AI SOC market based on application, as given below. According to you, which is the most attractive in terms of market opportunities now and in the future? Please rate on a scale of 1–10, with 10 being the most lucrative.

SR. NO.	APPLICATION	ATTRACTIVENESS OF OPPORTUNITY, 2026	ATTRACTIVENESS OF OPPORTUNITY, 2031
1	Threat Detection and Monitoring		
2	Alert Triage and Prioritization		
3	Incident Investigation and Analysis		
4	Threat Hunting		
5	Incident Response and Remediation		
6	Insider Threat Detection		
7	Cloud Security Monitoring		
8	Identity And Access Monitoring		
9	Compliance Monitoring and Reporting		
10	Security Analytics and Visualization		

Q. 9. We have segmented the AI SOC market based on vertical. Which vertical, in your opinion, is the most attractive in terms of market opportunities now and in the future? Please rate on a scale of 1-11, with 11 being the most lucrative.

SR. NO.	VERTICAL	ATTRACTIVENESS OF OPPORTUNITY, 2026	ATTRACTIVENESS OF OPPORTUNITY, 2031
1	Banking, Financial Services, and Insurance (BFSI)		
2	Government and Defense		
3	Healthcare and Life Sciences		
4	IT and Telecommunications		
5	Manufacturing		
6	Retail and Ecommerce		
7	Energy and Utilities		
8	Media and Entertainment		
9	Education		
10	Other Verticals		

JULY 2026 © MarketsandMarkets™

Q. 10. In your opinion, which region contributes the highest (1) and lowest (5) revenue now (2026) and in the future (2031) to the AI SOC market? Please rank on a scale of 1-5, with 1 being the highest.

SR. NO.	REGION	REVENUE SHARE, 2026	REVENUE SHARE, 2031
1	North America		
2	Europe		
3	Latin America		
4	Asia Pacific		
5	Middle East & Africa		

Q. 11. What are the various regulations and standards impacting the AI SOC market?

Primary's Viewpoint: _____

Q. 12. What innovations are you expecting in the AI SOC market that would have a high impact on the market?

Primary's Viewpoint: _____

Q. 13. Please name and rank your three main competitors.

Primary's Viewpoint: _____

Q. 14. What would you like to see covered additionally in the report besides the market segmentation mentioned?

Primary's Viewpoint: _____

JULY 2026 © MarketsandMarkets™

17.2 KNOWLEDGESTORE: MARKETSANDMARKETS' SUBSCRIPTION PORTAL

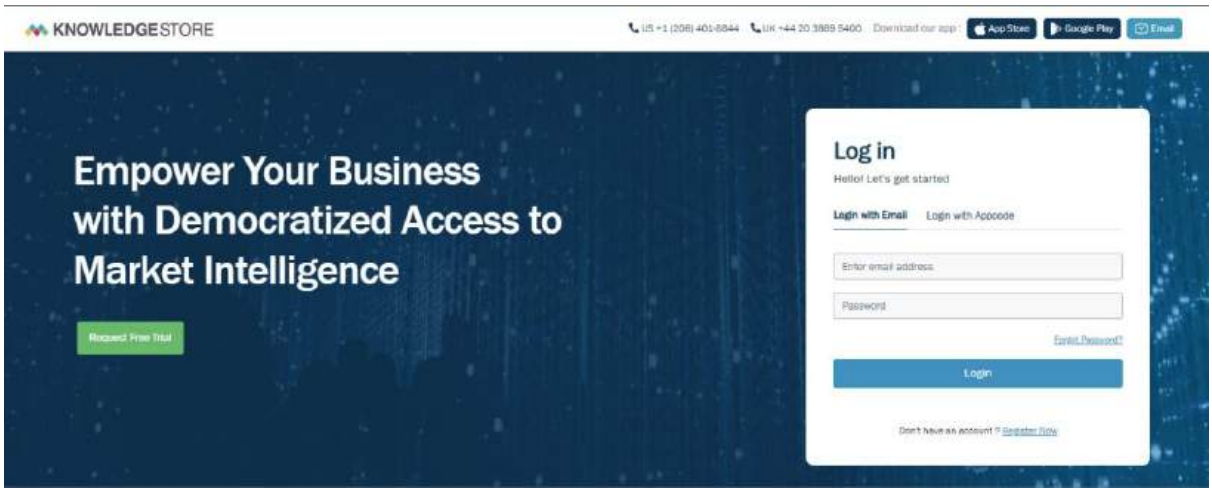
KnowledgeStore contains unique market insights of MarketsandMarkets. As a subscriber, you have access to all of the published titles and any new ones added over the course of the subscription period. You can subscribe to a specific number of reports or domains of your interest.

KNOWLEDGESTORE ENABLES YOU TO:

- View & download all subscribed reports from a single, online platform
- Contact our analysts to answer any questions related to our reports or request a custom research
- Share comments on specific reports with the other users of your organization
- Suggest titles/topics to our research teams that you would like us to cover in our future reports
- Identify reports published on the high growth markets within your industry

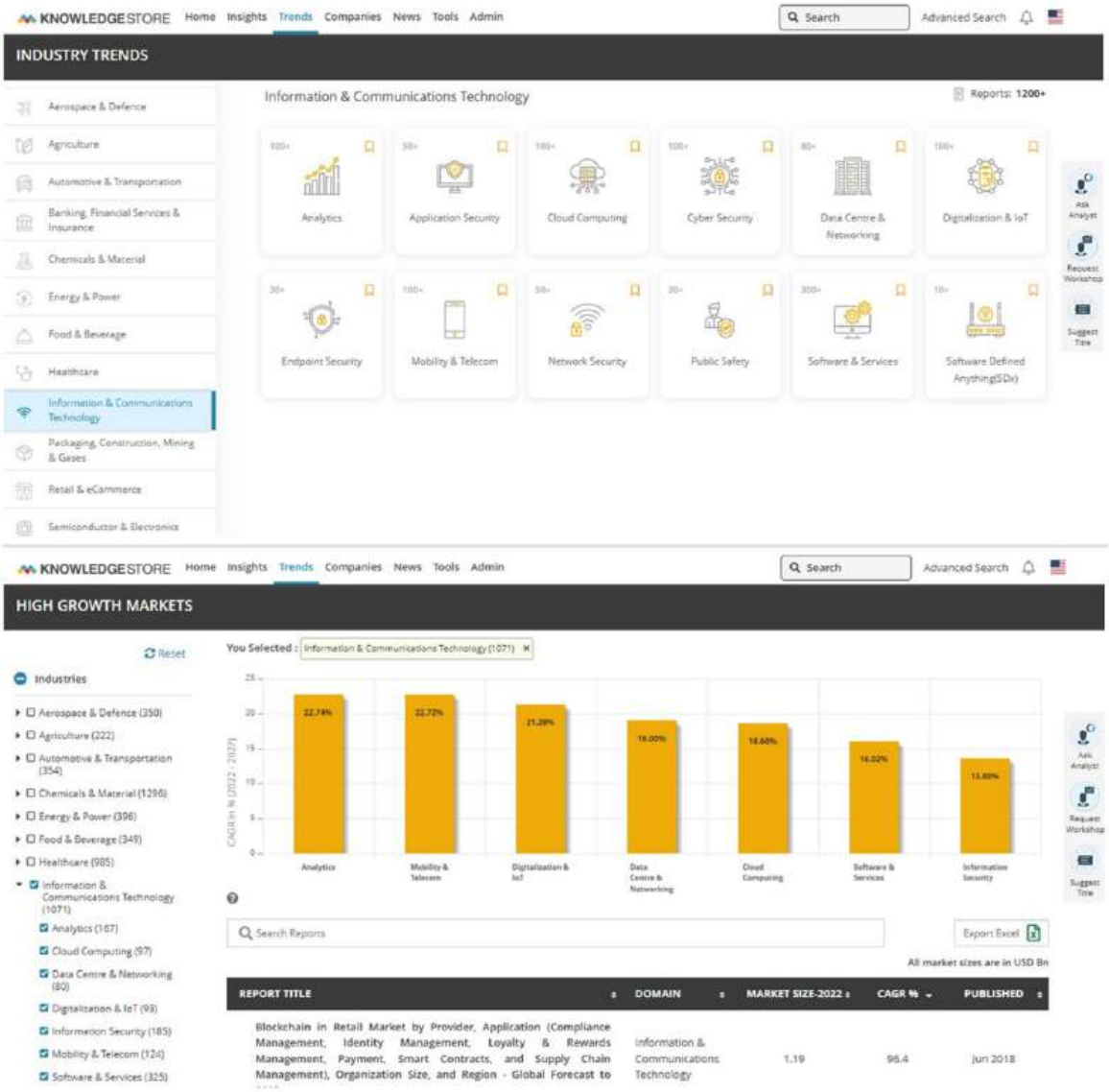
Get started now by requesting a demo and learning more about KnowledgeStore www.mnmks.com

MARKETSANDMARKETS KNOWLEDGESTORE SNAPSHOT



JULY 2026 © MarketsandMarkets™

MARKETSANDMARKETS KNOWLEDGESTORE: INFORMATION & COMMUNICATION TECHNOLOGY SNAPSHOT



JULY 2026 © MarketsandMarkets™

17.3 CUSTOMIZATION OPTIONS

With the given market data, MarketsandMarkets offers customizations per company-specific needs. The following customization options are available for the report:

COMPANY INFORMATION

- Detailed analysis and profiling of additional market players (up to five)

GEOGRAPHIC ANALYSIS

- Further breakdown of the geographies into respective countries

17.4 RELATED REPORTS

SR. NO	REPORT TITLE	PUBLISHED DATE
1	**SOC AS A SERVICE (SOCAAS) MARKET - GLOBAL FORECAST TO 2030** By Service Type (Managed SIEM & Log Management, Vulnerability Scanning & Assessment, Threat Detection & Remediation), Security Type (Endpoint Security, Network Security, Cloud Security) https://www.marketsandmarkets.com/Market-Reports/soc-as-a-service-market-31262563.html	January 2025

JULY 2026 © MarketsandMarkets™

17.5 AUTHOR DETAILS

Harminder Singh Bhatia
Assistant Vice President, Information and Communications Technology

Strategic Market Intelligence Leader with 17+ years of expertise in Research, Sales Enablement, Client Engagement, and Business Advisory. Demonstrated success in establishing and scaling research functions, delivering actionable market insights, optimizing sales processes, and shaping business strategies for clients across North America and Europe. Career experience spans leadership roles with PwC, Innova Solutions, Cognizant, Copal Amba (Moody's), and GlobalData.

Proficient in account and client management, competitive intelligence, emerging technology trends, vendor evaluations, and strategic consulting engagements. Recognized for driving market entry and expansion strategies, growth advisory initiatives, stakeholder analysis, and large-scale project execution. Experienced in leading technology integration and consulting programs within the ICT domain, covering multiple industry verticals.

Holds a Master of Business Administration (Finance & Marketing) and a Bachelor of Commerce, complemented by a professional certification from the National University of Singapore.

Vivek Ravichandran
Senior Research Manager, Information and Communications Technology

17 years of experience in Business Advisory, Strategy & Growth Consulting, and Best Practices Benchmarking.

In his current role, Vivek focuses on revenue impact for clients through new revenue opportunities driven by the everchanging revenue mix, uses cases driving the change, and how clients can tap new revenue streams while leveraging the current revenue streams (cash cows).

Before MarketsandMarkets, he worked with Ramco Systems, Zinnov (deputed), Infiniti Research (TechNavio), and Cognizant, where he played the role of a strategic partner for Mobility and CIS teams to penetrate key accounts from core pillars and strengthen revenue streams.

Vivek holds a Master's in Business Administration with a dual specialization in Finance & Marketing from NMIMS and a Bachelor of Engineering in Electronics and Communication from Anna University.

Contributors

Sayali Saste
Manager

Vidhu Rawat
Assistant Manager

Shivam Jethwa
Team Lead

Pratiksha Sonawane
Research Associate

JULY 2026 © MarketsandMarkets™

Disclaimer: MarketsandMarkets™ provides strategic analysis services to a select group of customers in response to orders. Our customers acknowledge when ordering that these strategic analysis services are solely for internal use and not for general publication or disclosure to any third party. MarketsandMarkets™ does not endorse any vendor, product, or service profiled in its publications. MarketsandMarkets'™ strategic analysis constitutes estimations and projections based on secondary and primary research and are therefore subject to variations. MarketsandMarkets™ disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness, for any particular purpose. MarketsandMarkets™ takes no responsibility for incorrect information supplied to it by manufacturers or users.

Trademarks, copyrights, and other forms of intellectual property belong to MarketsandMarkets™ or their respective owners and are protected by law. Under no circumstance may any of these be reproduced, copied, or circulated in any form, without the prior written approval of MarketsandMarkets™ or its owner—as the case may be. No part of this strategic analysis service may be given, lent, resold, or disclosed to any third party, without express permission from MarketsandMarkets™.

Reproduction and/or transmission in any form and by any means, including photocopying, mechanical, electronic, recording, or otherwise, without the permission of MarketsandMarkets™, is prohibited.

For information regarding permission, contact:
Tel: +1-888-600-6441