CATO NETWORKS

Cato Networks + Stellar Cyber SecOps Integration

The Challenge: SecOps Without Network Context

Security teams are struggling to operate in an environment where users, applications, data, and infrastructure are no longer centralized. Visibility is split across tools, signals arrive without context, and investigations are slowed by disconnected logging systems that were never designed for cloud-scale, identity-driven, and edge-routed traffic patterns. Many organizations have made progress consolidating networking and security through SASE, but their unifying SecOps platforms remain siloed and blind to the network layer where lateral movement and behavioral anomalies are first observable.

Modern security operations require a model where the edge and the SOC are not separate worlds. Instead, network and identity context needs to flow natively into investigation and response so analysts can understand what is happening and why — without reconstructing evidence manually or pivoting across multiple systems.

A Unified SASE SecOps Platform

This integration brings together Cato's converged SASE platform and Stellar Cyber's unified Security Operations platform into a single operational flow. Cato provides an SLA-backed global private backbone, Zero Trust policy enforcement, and full-fidelity flow and security telemetry from every connected user, branch, and cloud workload. Stellar Cyber ingests this telemetry and applies data transformation, AI-driven detection and correlation, and investigation logic that includes SIEM, NDR/OT visibility, ITDR, and UEBA— all within one AI-native platform.

The result is a SecOps operating model that eliminates blind spots and accelerates investigations because network evidence arrives already contextualized, not as an additional data source analysts must query,normalize and analyze on their own.

Primary Joint Use Cases

Lateral Movement and Post-Compromise Activity

Once an attacker gains a foothold, internal traffic patterns and identity misuses are often the earliest signals of escalation. By combining Cato session telemetry and policy with Stellar Cyber's behavioral analytics and entity tracking, analysts can confirm threats earlier and prioritize cases with higher confidence.

Account Misuse and Identity-Based Threats

Authentication alone does not confirm legitimacy. The joint integration correlates identity signals, Zero Trust policy outcomes, and network interactions to surface identity misuse that would not be visible from cloud or endpoint signals alone.

Hybrid Workforce and Application Access Visibility

Because Cato routes and inspects traffic globally, via its private backbone, remote users and branch locations produce the same standardized telemetry as datacenter or cloud-hosted resources. Stellar Cyber transforms this uniform visibility into streamlined investigations regardless of where the user or workload sits.

How the Integration Works

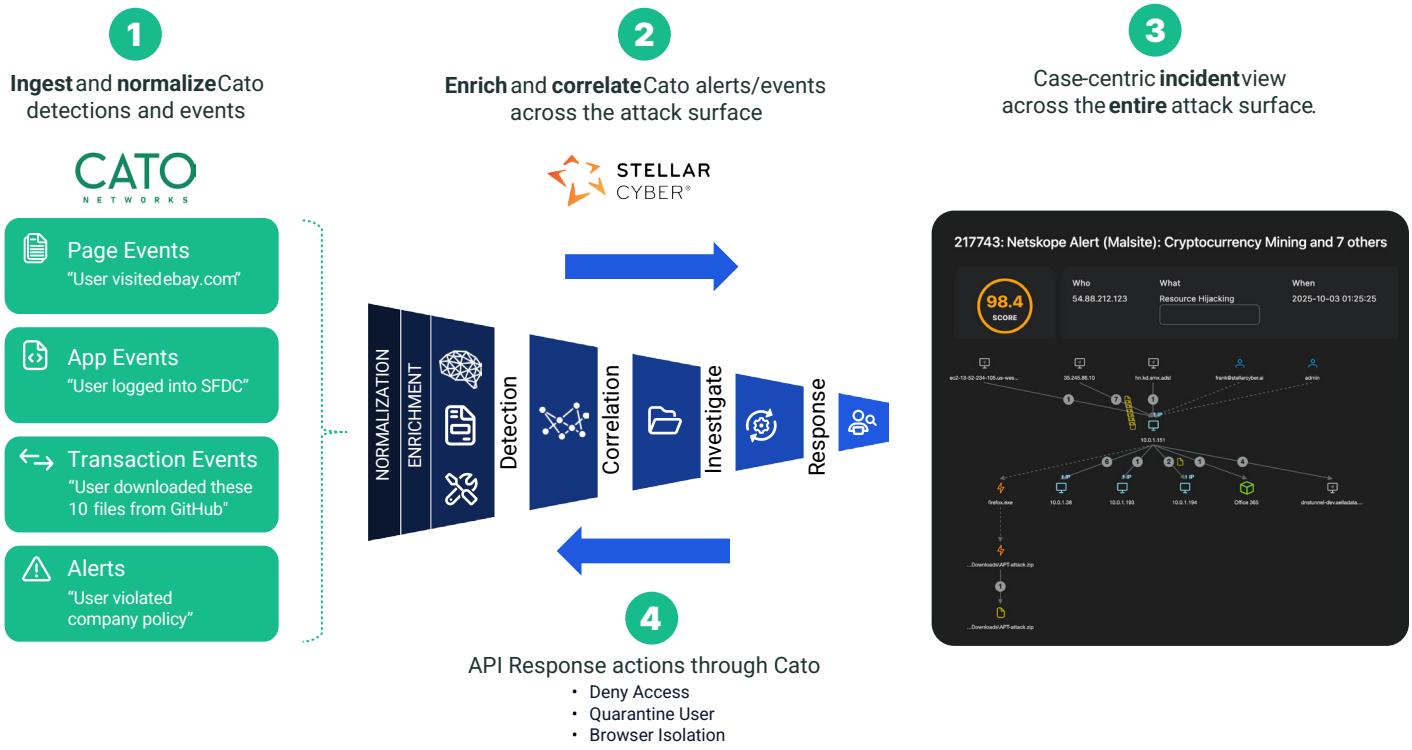
The Cato SASE Platform delivers converged networking and security as a single global cloud service, built on a global private backbone. That telemetry includes real-time flow records, session metadata, access decisions, security policy outcomes, and infrastructure context. This telemetry is streamed into Stellar Cyber's open Security Operations platform through secure integration channels for analysis and investigation.

Inside Stellar Cyber, the data is normalized, enriched, and correlated across other sources such as identity, cloud, infrastructure, endpoint, OT, and user behavior. The outcome is a case-ready narrative rather than an isolated event. Analysts do not need to pivot into separate network tools to verify what actually happened — the investigation begins with network context already in place.

This approach removes one of the most time-consuming components of incident triage: reconstructing the path between identity, traffic, and infrastructure. With Cato as the network and access control layer, and Stellar Cyber as the SecOps layer, the investigation immediately includes who was involved, what they attempted, and how the environment responded.

Better Together

Turn-key Integration, with **Visibility** Across the Attack Surface



Benefits for MSSPs

For MSSPs, delivering a managed SASE or MDR service typically requires multiple platforms, custom integrations, and dedicated infrastructure to ingest, process, and analyze data. This joint solution significantly simplifies that model. Cato delivers secure connectivity and full security enforcement as a single global service, while Stellar Cyber provides multi-tenant SecOps operations that unify investigation and response across all tenants.

This allows MSSPs to onboard customers faster, deliver consistent outcomes, and scale services without re-engineering toolchains or expanding staff to manage data pipelines. The architecture is built for recurring service delivery rather than one-off integrations, which improves margin and lowers operational burden.

Benefits for Enterprise Security Teams

Many resource-constrained security teams cannot build or maintain a SIEM-centric architecture capable of ingesting and normalizing the volume of data required for modern threat detection. This integration gives them a path to enterprise-grade SecOps without building custom infrastructure or correlating network data manually.

The unified platform approach enables a shift from reactive investigation to proactive detection because evidence arrives already structured for analysis. It also simplifies adoption of Zero Trust principles by aligning identity, network, and behavioral context inside a single operational view.

Why Cato and Stellar Cyber Together

The strength of this collaboration is that each platform reinforces the other: Cato secures connectivity and enforces policy at the edge, and Stellar Cyber transforms that context into SOC-ready intelligence. Rather than attempting to replicate network visibility inside SIEM pipelines or retrofit SSE feeds into SecOps tooling, the two platforms interlock cleanly—one as the distributed enforcement layer, the other as the operational decision layer.

This design makes SecOps more effective without requiring a change in workflow or the addition of more analyst effort. The network edge and the SOC are finally aligned as parts of a single system rather than adjacent systems with separate data paths.

Summary

Cato Networks delivers the Cato SASE Platform for converged networking and security, and Stellar Cyber provides a unified Security Operations platform built to operationalize that context through AI-driven SIEM, NDR/OT visibility, ITDR, and UEBA in one workflow. Together they deliver an edge-to-SOC model that improves threat detection fidelity, reduces investigation time, and simplifies service delivery for both MSSPs and enterprise security teams.

By shining a bright light on the darkest corners of security operations, Stellar Cyber empowers organizations to see incoming attacks, know how to fight them, and act decisively – protecting what matters most. Stellar Cyber's award-winning open security operations platform includes NG SIEM, NDR, Open XDR, and Multi-Layer AI™ under one license. With almost ⅓ of the top 250 MSSPs and over 14,000 customers worldwide, Stellar Cyber is one of the most trusted leaders in security operations. Learn more at https://stellarcyber.ai