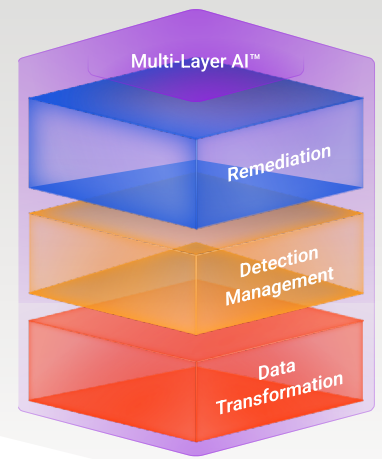


Managed Identity Security for MSSPs



Turn identity signals customers already generate into a recurring managed service that detects risky behavior, validates what matters, and moves to response.

Most customers already have IAM, MFA, Active Directory, Microsoft Entra ID, Okta, and access policies. The service opportunity is not to replace those controls - it is to continuously answer a more valuable question: what are your identities doing now, and which ones should we worry about?

A Managed Service Built Around Better Answers

Detect Meaningful Identity Behavior

Monitor for impossible travel, unusual login locations and times, abnormal asset access, privilege misuse, and other identity-linked anomalies.

Investigate with Full Attack-Chain Context

Correlate the identity with endpoint, network, cloud, SaaS, and other telemetry to determine whether suspicious behavior became an active attack.

Respond and Prove Value

Use approved response actions and playbooks, then show customers what was investigated, what mattered, and what was done about it.

What the MSSP Delivers

Identity Monitoring and Insights	Detect and report on meaningful identity anomalies and behavioral changes across each customer environment.
Managed Identity Investigation	Add analyst validation, automated triage, and full attack-chain context so customers receive an answer - not another alert.
Managed Identity Response	Add customer-approved actions such as session revocation, account disabling, endpoint isolation, and supported response playbooks.

The Service Promise

Detect suspicious identity behavior. Determine whether it matters.

Act before trusted access becomes an active attack.

Built to scale across your customer base

A new service only works if the MSSP can deliver it repeatedly without adding analysts at the same rate it adds customers. Stellar Cyber combines identity telemetry, behavioral detection, automated investigation, response, reporting, and multi-tenant operations in one platform

Use the identity data customers already generate

- Ingest identity-related data from Active Directory, Microsoft Entra ID, Okta, LDAP, and other supported sources.
- Combine identity context with endpoint, network, cloud, SaaS, and security telemetry.
- Avoid forcing customers to build or standardize on a new identity stack.

Make automation support the service economics

- Automated triage handles repetitive enrichment and first-pass investigation.
- Analysts focus on identity activity that deserves attention rather than manually correlating every alert.
- Repeatable playbooks help move from investigation to approved response actions.

Make the customer value visible

- Provide tenant-specific reporting on high-risk identity anomalies, users investigated, cases, and response actions.
- Show changes in identity behavior and trends over time.
- Turn invisible SOC work into visible evidence of service value.

Operate securely across tenants

- Multi-tenant architecture and role-based governance help keep security data controlled and separated as AI use expands.
- Tenant-level dashboards and centralized operational views support managed service delivery.
- Build the service once and deliver it consistently across the customer base.

Why Customers Will Buy It

Know which identities deserve attention

Move beyond authentication events to behavioral insight and full attack-chain context.

Get an answer, not another alert

Give customers analyst-validated findings supported by automated triage and evidence.

Know which identities deserve attention

Move beyond authentication events to behavioral insight and full attack-chain context.

Get an answer, not another alert

Give customers analyst-validated findings supported by automated triage and evidence.

Turn identity signals into insight. Turn the insight into a new service.

Create new recurring revenue while giving customers another reason to stay.

Learn more at <https://stellarcyber.ai>.