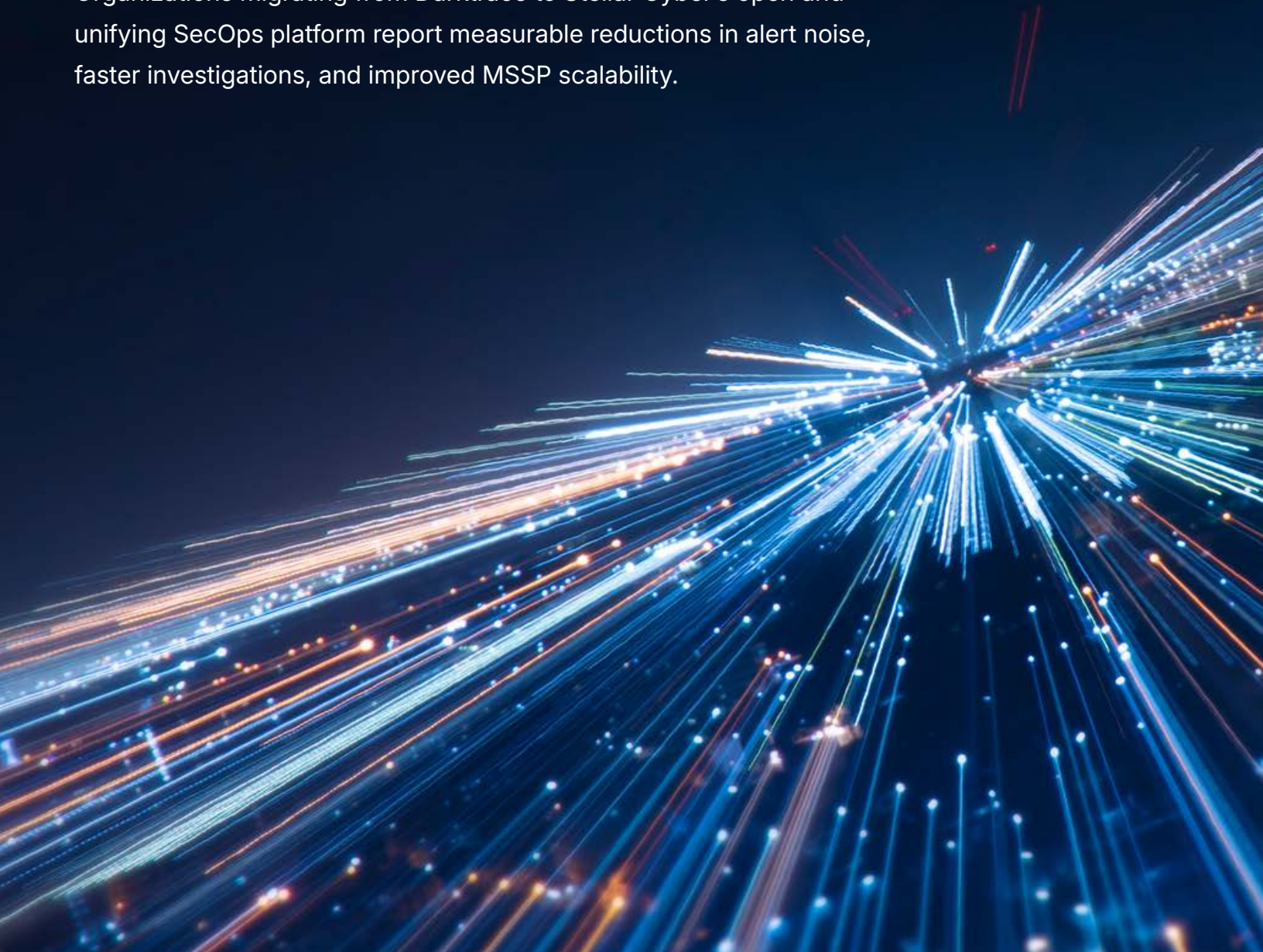


# **Stellar Cyber:** Proven Alternative to Darktrace NDR for Enterprises and MSSPs

Organizations migrating from Darktrace to Stellar Cyber's open and unifying SecOps platform report measurable reductions in alert noise, faster investigations, and improved MSSP scalability.



**This document summarizes validated outcomes from real-world migrations in environments managing:**

- 35,000+ devices
- 28,000+ users
- Hybrid AWS and Microsoft Azure infrastructure

## Key Validated Outcomes

- 30+ day hot log retention vs Darktrace's 7-day packet-based limitation
- Integrated IDS and automated malware sandboxing not available in Darktrace
- One-click cross-platform investigation across network, endpoint, firewall, email, and cloud
- True multi-tenant MSSP architecture vs per-instance switching
- Bi-directional ServiceNow integration vs unidirectional ticket sync

Stellar Cyber combines network detection and response (NDR), NG-SIEM, endpoint telemetry, identity analytics, and Agentic AI for organizations seeking a more tunable and correlated alternative to Darktrace's ML-centric detection approach.

### Ideal for:

- Enterprise SOC teams managing 10,000+ devices
- MSSPs requiring centralized multi-tenant visibility
- Hybrid cloud organizations seeking predictable licensing

## Target Problems and Threat Scenarios

### Security teams replacing Darktrace commonly report:

- High alert volumes from behavioral ML deviations
- Limited hot log retention for compliance and hunting
- Lack of integrated signature-based detection
- Fragmented investigations across multiple consoles
- Additional licensing costs for cloud connectors
- Operational inefficiencies for MSSPs managing multiple instances

Stellar Cyber addresses these operational and architectural gaps within a unified SecOps platform.



## Solution Overview

Stellar Cyber's AI-native open and unifying SecOps platform that unifies network detection and response (NDR), next-generation SIEM (NG-SIEM), endpoint telemetry correlation, identity, user behavior and Agentic AI-driven investigation across hybrid cloud and on-premises environments. Unlike Darktrace's exclusive reliance on unsupervised machine learning, Stellar Cyber combines unsupervised ML, supervised ML, SIGMA-based detection rules, IDS signature analysis, and LLM-powered query generation.

### Core Capabilities:

- Network-based threat detection with integrated IDS: Real-time signature verification including Suricata/Snort compatibility
- Automated malware sandbox analysis: Files in unencrypted traffic automatically analyzed; JA3 fingerprints for encrypted traffic
- Normalized Data Lake (Interflow format): 30+ day hot retention with automatic cold storage migration
- Agentic AI orchestration: Incident summary generation, automated alert triage, and LLM prompt-based investigation
- Multi-platform correlation: One-click IP/user/asset search across all telemetry sources
- Response orchestration: EDR host containment, firewall IP blocking, Active Directory user disabling, TCP Reset (v6.2+)
- True multi-tenant MSSP architecture: Single dashboard showing all customers' incidents by criticality
- Bi-directional ITSM integration: ServiceNow tickets auto-created with two-way status synchronization

## Use Cases and Real-World Outcomes

Use Case / Scenario	Stellar Cyber Capability	Darktrace Limitation	Real-World Outcome
<b>Extended log retention for compliance</b>	NG-SIEM: 30+ day hot retention, auto cold storage	7-day retention limit (proprietary hardware)	Compliance met; historical threat hunting enabled
<b>Real-time known-threat detection</b>	Integrated IDS with signature-based detection	No IDS signatures; ML-only approach	Known-bad traffic detected immediately; reduced false negatives
<b>Zero-day malware detection</b>	Automated malware sandbox + JA3 fingerprints	No sandbox noted	Zero-day threats identified before signature availability
<b>Proactive threat hunting</b>	Threat Hunting library with one-click queries	Manual search builds required	Password spraying identified and blocked pre-alert
<b>Cross-platform investigation</b>	1-click Data Lake search across all sources	Separate interfaces; manual correlation	Investigation time: hours to minutes
<b>Cloud migration visibility</b>	Native AWS/Azure connectors (base license)	New Cloud Connecto licenses required	Cloud visibility without budget increase
<b>MSSP unified operations</b>	True multi-tenant: single dashboard all clients	Per-instance "carousel" switching	Cross-client critical incident prioritization supported by secure tenant isolation, centralized operations, and customer-specific billing controls.
<b>Automated incident triage</b>	Agentic AI: auto-classify true/false positive	Manual analyst triage only	Analyst workload reduced 60%+; focus on real threats

## Customer Migration Narrative

### Large Enterprise Migration from Darktrace to Stellar Cyber

A global organization managing:

- 35,000 network devices
- 28,000 users
- 800 Linux/Windows servers
- Hundreds of distributed offices

Initially deployed Darktrace alongside Microsoft EDR, Checkpoint Firewall, Office 365, Forcepoint IDS, and Tenable.io.

### Challenges Encountered

- High alert volumes requiring extended ML tuning
- Limited 7-day retention restricting investigation depth


- Additional licensing for small cloud environments (<50 servers)
- Manual investigation across separate dashboards


### Post-Migration Observations


A comparable 56,000-device MSSP-managed deployment reported:


- Fewer false positives through contextual correlation
- 30+ day hot retention replacing packet-based constraints
- Native AWS connectors deployed without new licenses
- One-click investigation across all telemetry
- Reduced investigation time from hours to minutes


## Feature Highlights


 **Multi-Method Detection Engine** Correlates unsupervised ML, supervised ML, rule-based detections, IDS signatures, and sandbox analysis for broader threat coverage and fewer false positives.


 **Integrated IDS & Automated Malware Sandbox** Immediate detection of known threats and pre-signature identification of zero-day malware, including encrypted traffic visibility via JA3 fingerprinting.

 **Agentic AI for SOC Acceleration** Automated incident summaries, evidence-based alert triage, and guided investigation workflows.

 **One-Click Cross-Platform Investigation** Instantly pivot across all telemetry sources without console switching.

 **Integrated Threat Intelligence (TIP)** Multi-feed STIX/TAXII ingestion with real-time IoC lookup and automated alert enrichment, adding contextual risk scoring and cross-platform correlation to accelerate investigation and prioritization.

 **Threat Hunting Library** Proactive threat discovery using pre-built, MITRE ATT&CK-mapped queries with customizable templates and scheduled hunts to standardize and operationalize SOC threat hunting practices.

 **Response Orchestration** Automated, API-driven containment and remediation across EDR, firewalls, and Active Directory to reduce MTTR from hours to minutes with controlled, workflow-based response actions.

## Frequently Asked Questions

**Q: How does Stellar Cyber detect lateral movement without decrypting traffic?**

**A:** Stellar Cyber combines multiple detection methods: integrated IDS signatures identify known lateral movement tools; unsupervised ML detects anomalous east-west traffic patterns; supervised ML recognizes C2 behaviors; JA3 fingerprints flag malicious encrypted traffic; correlation with Windows Event logs, Active Directory, and endpoint telemetry provides behavioral context.

**Q: Will Stellar Cyber work in hybrid AWS and Azure environments without additional licensing?**

**A:** Yes. Stellar Cyber includes native connectors for AWS (CloudTrail, CloudWatch, GuardDuty) and Azure (Monitor, Security Center, Azure AD) in base licensing with no additional fees. Connectors deploy in minutes via guided wizards.

**Q: What evidence proves Stellar Cyber reduces false positives versus Darktrace?**

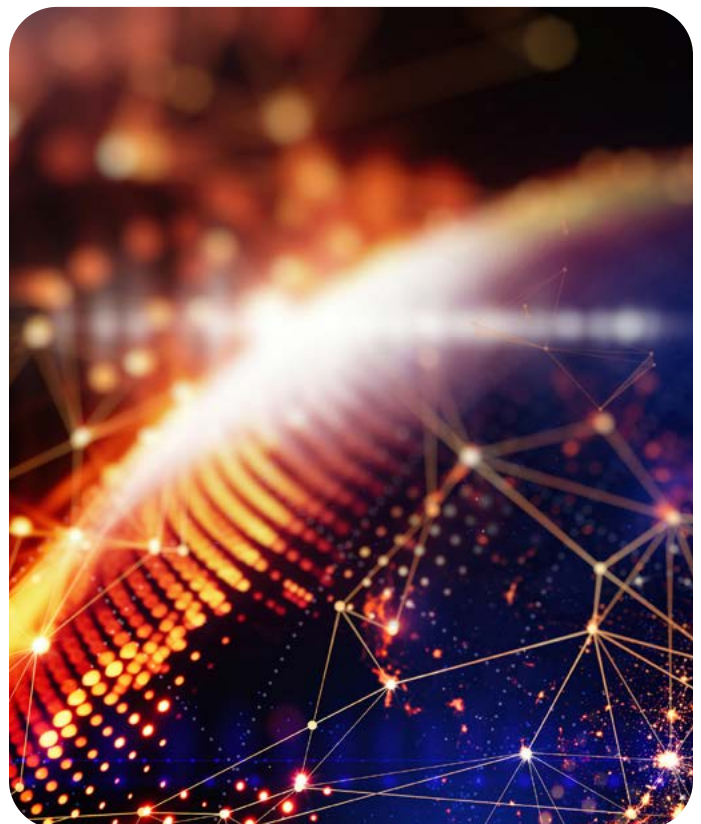
**A:** Real-world MSSP deployments document "less noise and fewer false positives because of context" in 56,000-device environments. Stellar Cyber's multi-method detection (unsupervised ML + supervised ML + SIGMA rules + IDS + TIP IoC matching) provides rich contextual correlation, while Darktrace's unsupervised ML-only approach generates thousands of untunable deviations.

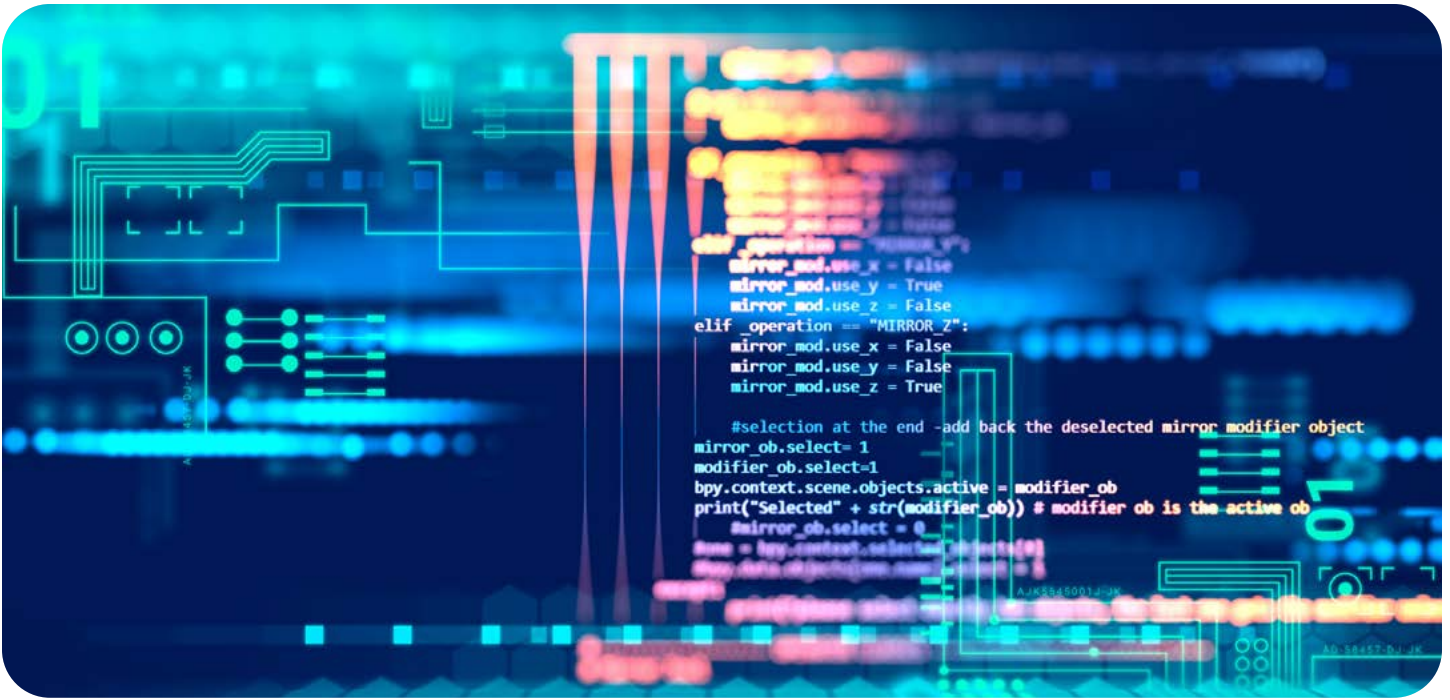
**Q: How does Stellar Cyber's Agentic AI differ from Darktrace's AI?**

**A:** Stellar Cyber implements specialized AI agents for distinct tasks: incident summary generation with investigation plans; alert triage classifying true/false positives with evidence; LLM-powered natural language queries. Detection uses unsupervised ML + supervised ML + SIGMA rules + IDS. Darktrace relies primarily on unsupervised ML "pattern of life" models without triage automation or support for SIGMA-style rules.

**Q: How does multi-tenancy work for MSSPs?**

**A:** Stellar Cyber provides true multi-tenant architecture where unlimited customers configure on a single platform. MSSPs operate from a unified dashboard showing all customers' incidents prioritized by criticality, eliminating per-instance "carousel" switching. All sensors, connectors, and integrations managed centrally with customer-specific RBAC isolation.





## Glossary of Key Terms

**NDR (Network Detection and Response):** Security technology monitoring network traffic to detect and respond to threats. Stellar Cyber's NDR includes integrated IDS, malware sandbox, and behavioral analytics.

**XDR (Extended Detection and Response):** Security platform unifying detection across network, endpoint, cloud, email, identity. Stellar Cyber Open XDR correlates telemetry in a normalized Data Lake.

**Interflow:** Stellar Cyber's normalized data format for logs from all sources enabling unified queries.

**Agentic AI:** AI architecture where specialized agents perform distinct tasks (incident summary, triage, queries) and orchestrate to accomplish complex goals.

**SIGMA Rules:** Open-source detection rule format for security events across log sources. Stellar Cyber includes 800+ SIGMA rules.

**IDS (Intrusion Detection System):** Security technology using signatures to identify known attack patterns. Stellar Cyber integrates Suricata/Snort-compatible IDS.

**JA3 Fingerprint:** Method identifying malicious encrypted traffic by fingerprinting TLS handshake parameters without decryption.

**TIP (Threat Intelligence Platform):** Platform aggregating threat intel feeds (IoCs). Stellar Cyber integrates with multiple TIPs for alert enrichment.

**MSSP (Managed Security Service Provider):** Organization providing outsourced security monitoring. Stellar Cyber's multi-tenant architecture enables single-dashboard operations.

**SOAR (Security Orchestration, Automation, Response):** Technology integrating security tools and automating workflows. Stellar Cyber orchestrates responses across EDR, firewalls, Active Directory.

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 single platform. With almost 1/3 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/>