securonix

Securonix Threat Analytics for Microsoft Sentinel

Help customers improve detection coverage, accelerate detection and response, and maximize Sentinel ROI with behavior-driven analytics, continuously maintained detections, cross-source correlation, and risk-based prioritization—without replacing Sentinel or changing how their analysts work.

For MSSPs and MDR providers, Securonix provides a repeatable way to standardize behavior-driven detection across customer environments, accelerate detection and response, reduce tenant-by-tenant engineering, protect service margins, and deliver differentiated managed detection services .Microsoft Sentinel remains each customer's system of record, investigation console, and primary analyst workflow.

Scale stronger detection across Microsoft Sentinel tenants—without multiplying engineering work or disrupting customer workflows.

OUTCOMES FOR MSSPS AND MDR PROVIDERS

IMPROVE DETECTION ACROSS TENANTS. Standardize behavior-driven analytics, enrichment, correlation, and risk scoring across diverse customer environments without building one-off detection logic for every tenant.

IMPROVE DETECTION COVERAGE ACROSS TENANTS. Standardize behavior-driven analytics, continuously maintained detection content, cross-source correlation, and dynamic risk scoring across customer environments. Expand real-time detection beyond Sentinel's native NRT rule constraints without building and maintaining one-off logic for every tenant.

PROTECT SERVICE MARGINS. Reduce custom KQL development, manual tuning, false-positive triage, detection-content maintenance, and onboarding effort so analysts can support more customers without proportional increases in headcount.

DIFFERENTIATE MANAGED SENTINEL SERVICES. Create premium Microsoft Sentinel services built around insider threat detection, UEBA, identity security, MITRE-aligned coverage optimization, and risk-prioritized investigation.

ACCELERATE DETECTION AND RESPONSE. Turn fragmented signals into enriched, risk-prioritized incidents with behavioral evidence, entity context, MITRE ATT&CK mapping, and risk scores—so analysts can move from alert to informed action faster in their existing Sentinel workflows.

MAXIMIZE SENTINEL ROI FOR CUSTOMERS. Increase the fidelity, context, and prioritization of the detections analysts receive while preserving customer data architectures, investigation processes, playbooks, and response workflows. No SIEM migration, duplicate data, additional agents, new customer-side pipelines, or disconnected analyst experience.

Build a stronger Sentinel service. Deliver better customer outcomes. Protect service margins.

Why MSSPs Choose Securonix Threat Analytics

Sentinel-centered operations. Microsoft Sentinel remains the customer's data platform, investigation console, incident-management environment, and response workflow. Enriched, risk-prioritized detections return directly to Sentinel, where analysts already investigate and respond.

Detection expansion without rule-limit tradeoffs. Extend Microsoft Sentinel with immediate detection coverage beyond native near-real-time rule constraints, helping providers deliver broader protection without building and maintaining every analytic from scratch.

Behavior-driven detection across the attack surface. Apply UEBA, ITDR, anomaly detection, entity profiling, peer-group analysis, advanced correlation, and continuously maintained detection content to identify subtle and multi-stage threats that static rules can miss.

Faster onboarding with lower friction. Extend customer environments without agents, duplicate data, new customer-side pipelines, SIEM migration, or disruption to established workflows. Supported environments can typically begin realizing value in approximately two to three weeks.

Broad Microsoft and non-Microsoft coverage. Apply consistent analytics across identity, cloud, SaaS, endpoint, network, infrastructure, and third-party security telemetry through more than 600 supported integrations.

How It Works

Microsoft Sentinel collects and stores - Sentinel continues to ingest and store customer telemetry and remains the system of record, primary investigation console, incident management environment, and response workflow.

Securonix enriches, correlates, and prioritizes - Securonix applies behavior-driven analytics, entity context, MITRE ATT&CK mapping, cross-source correlation, and dynamic risk scoring. Real-time detection expands beyond Sentinel's native NRT constraints without requiring custom logic for every customer.

Analysts investigate and respond in Sentinel - Enriched alerts, behavioral anomalies, chained activity, entity context, and risk-prioritized incidents return directly to Sentinel, giving analysts stronger signal and investigation-ready context without changing their workflow.

Sentinel collects and orchestrates. Securonix enriches, correlates, and prioritizes. Analysts investigate and respond in Sentinel.

Proof Points That Support Service Growth

- 2,400+ continuously maintained detections backed by Securonix Threat Labs
- 600+ integrations across cloud, identity, SaaS, endpoint, network, infrastructure and security ecosystems
- Unlimited real-time detection expansion beyond Sentinel's native NRT rule limit
- Typical value realization in approximately two to three weeks for supported environments

The Bottom Line

Securonix Threat Analytics helps MSSPs and MDR providers build differentiated Microsoft Sentinel services that improve detection coverage, accelerate detection and response, and maximize customer Sentinel ROI. Standardize behavior-driven analytics across tenants, reduce alert noise and engineering work, protect service margins, and return enriched, risk-prioritized incidents directly to Sentinel—without changing how customers store data, investigate incidents, or respond to threats.

Improve detection coverage, accelerate investigation and response, and maximize Microsoft Sentinel ROI—in weeks, not months.