securonix

Securonix Threat Analytics for Microsoft Sentinel

Help customers improve detection coverage, accelerate detection and response, and maximize Microsoft Sentinel ROI without replacing their SIEM. MSSPs and MDR providers are under pressure to deliver stronger detection outcomes across increasingly complex customer environments. Microsoft Sentinel provides a powerful cloud-native SIEM foundation, but visibility alone is not enough. Coverage can vary by tenant, and alert quality can vary by data source. Sentinel's 50 near-real-time rule limit can constrain detection strategies. Analysts spend too much time tuning rules, triaging false positives, writing custom KQL, and stitching together context across identity, cloud, SaaS, endpoint, and third-party tools. Securonix Threat Analytics for Microsoft Sentinel gives providers a scalable way to turn Sentinel into a higher-fidelity managed detection service. Sentinel remains the customer's data lake, investigation console, and response workflow. Securonix enriches existing telemetry, applies behavior-driven analytics, expands real-time detection coverage beyond native NRT constraints, and returns high-confidence findings to Sentinel. **Extend Microsoft Sentinel with Behavior-Driven Analytics for Managed Detection Services.**

OUTCOMES FOR MSSPS AND MDR PROVIDERS

SCALE HIGH-FIDELITY 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 BEYOND NATIVE LIMITS. Help customers overcome Sentinel's 50 NRT rule limit with Securonix-powered real-time detections that improve coverage without forcing providers to create and maintain custom rules at scale.

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

DIFFERENTIATE MANAGED SENTINEL SERVICES. Package behavior-driven analytics, MITRE-aligned coverage visibility, threat intelligence enrichment, and risk-based prioritization into premium Microsoft Sentinel service tiers.

ACCELERATE DETECTION AND RESPONSE. Help customers detect insider threats, identity misuse, ransomware, cloud compromise, and advanced threats earlier and respond faster while preserving their existing Microsoft investment.

MAXIMIZE SENTINEL ROI FOR CUSTOMERS. Increase the value of existing Sentinel deployments without platform migration, duplicate data, new customer-side pipelines, or workflow disruption.

Why MSSPs Choose Securonix Threat Analytics

High-fidelity detections without SIEM replacement. Enhance Microsoft Sentinel instead of replacing it. Customers keep their existing data lake, workflows, playbooks, and analyst experience.

Detection expansion without rule-limit tradeoffs. Extend Microsoft Sentinel with real-time detection coverage that goes beyond native NRT rule constraints, helping providers deliver broader protection without adding operational complexity.

Behavior-driven analytics beyond static rules. Apply UEBA, anomaly detection, entity profiling, peer-group analysis, ITDR, curated threat intelligence, and advanced correlation to identify threats that rule-based detections can miss.

Faster onboarding with lower operational burden. Use a lightweight integration with no agents, no new customer-side pipelines, no data duplication, and no workflow disruption.

Coverage across hybrid and multi-cloud environments. Extend detection across Microsoft and non-Microsoft ecosystems, including identity, endpoint, SaaS, cloud, infrastructure, and third-party security tools.

How It Works

Microsoft Sentinel remains the system of record - Sentinel continues to ingest and store customer telemetry and remains the primary investigation and response workflow.

Securonix enriches, correlates, and prioritizes telemetry - Securonix applies behavioral analytics, curated threat intelligence, correlation, entity context, MITRE mapping, and dynamic risk scoring to identify high-risk behavior and prioritize the threats that matter most.

Real-time detection coverage expands - Securonix extends detection coverage beyond Sentinel's 50 NRT rule limit, helping providers improve real-time threat detection without building and maintaining custom detection logic for every customer.

High-confidence detections return to Sentinel - Risk-prioritized alerts and anomalies flow back into Sentinel so analysts can investigate and respond in the tools they already use.

Proof Points That Support Service Growth

- 2,400+ continuously maintained detections backed by Securonix Threat Labs
- 600+ integrations across cloud, SaaS, identity, endpoint, and infrastructure ecosystems

The Bottom Line

Securonix Threat Analytics helps MSSPs turn Microsoft Sentinel into a higher-fidelity managed detection service. Providers can improve detection coverage beyond native real-time constraints, reduce alert noise, accelerate detection and response, and deliver measurable customer value without forcing customers to migrate platforms, duplicate data, or change how their SOC operates. **Build a differentiated Sentinel detection service and deliver stronger outcomes in weeks, not months.**