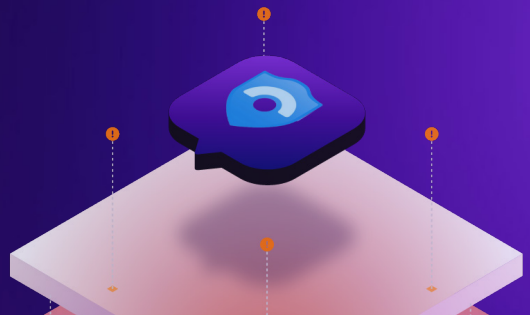
securonix DATASHEET

Threat Analytics for Microsoft Sentinel

Improve Detection Coverage. Accelerate Investigation and Response. Maximize Sentinel ROI.



Extend Microsoft Sentinel with behavior-driven analytics and risk-based prioritization.

Microsoft Sentinel provides a powerful cloud-native foundation for security operations, but many organizations continue to struggle with alert fatigue, limited detection fidelity, and increasing sophisticated attacks. Static rules and threshold-based detections often generate excessive noise while missing the subtle behaviors associated with insider threats, identity compromise, ransomware, cloud attacks, and advanced persistent threats.

Securonix Threat Analytics for Microsoft Sentinel extends your existing Sentinel deployment with AI-driven behavioral analytics, advanced correlation, risk-based prioritization, and continuously curated threat intelligence—without replacing your SIEM, duplicating data, or disrupting existing workflows.

Using lightweight API-based integration, Microsoft Sentinel continues to collect and store security telemetry while Securonix analyzes activity across users, identities, endpoints, cloud platforms, and SaaS applications, and returns enriched, high-confidence detections directly into native Sentinel workflows for investigation and response.

Together, Microsoft Sentinel and Securonix help organizations improve detection coverage,accelerate detection and response, increase analyst productivity, and achieve greater value from their existing Sentinel investment.

Customer Outcomes

Organizations using Securonix Threat Analytics have achieve:

- Up to 875 behavioral detections using adaptive threat modeling and UEBA
- Approximately 60% greater detection coverage
- Approximately 60% fewer false positives
- Up to 3x greater ROI from Microsoft Sentinel investments.

Business Outcomes

DETECT MORE ADVANCED THREATS

Identify sophisticated attacks that traditional rule-based detections often miss, including insider threats, credential abuse, ransomware, cloud attacks, identity misuse, and advanced persistent threats. Behavioral analytics continuously identify abnormal activity before attackers reach critical assets.

IMPROVE SOC EFFICIENCY

Reduce alert fatigue by correlating low-fidelity events into prioritized, high-confidence incidents enriched with business context, risk scores, entity information, threat intelligence, and MITRE ATT&CK mappings. Analysts spend less time investigating noise and more time responding to genuine threats.

MAXIMIZE MICROSOFT SENTINEL ROI

Extend the value of your existing Microsoft Sentinel deployment without additional data pipelines, platform migration, duplicate storage, or operational disruption. Securonix enhances the investments you have already made while accelerating time to value.

How Securonix Enhances Microsoft Sentinel

Securonix operates as a cloud-native analytics layer that integrates seamlessly with Microsoft Sentinel.

1. Microsoft Sentinel collects and stores security telemetry.
2. Securonix applies behavioral analytics, AI-driven correlation, entity context, and dynamic risk scoring.
3. High-confidence detections are returned directly into Microsoft Sentinel for investigation and response.

No agents. No data duplication. No disruption to existing SOC workflows.

Core Capabilities

DETECT SOPHISTICATED ATTACKS WITH BEHAVIORAL ANALYTICS

Move beyond static rules and thresholds with patented User and Entity Behavior Analytics, Identity Threat Detection and Response, anomaly detection, peer group analysis, event rarity, and behavioral profiling. Identify subtle indicators of compromise across hybrid and multi-cloud environments before they escalate into security incidents.

PRIORITIZE THE THREATS THAT MATTER MOST

Dynamic risk scoring combines behavioral analytics, threat intelligence, entity context, business impact, and MITRE ATT&CK mapping to prioritize alerts. Security teams can quickly focus on the highest-risk threats without manually sorting through thousands of disconnected events.

REDUCE ALERT FATIGUE THROUGH INTELLIGENT CORRELATION

Automatically correlate related security events into high-confidence incidents that give analysts with the context needed for rapid investigation. Behavioral profiling, entity-based correlation, and risk-based prioritization reduce false positives while improving detection fidelity.

KEEP DETECTION COVERAGE CURRENT

Apply continuously maintained detection content backed by Securonix Threat Labs research to address evolving attacker behavior, emerging techniques, and new risks. Customers benefit from updated analytics without having to continually build, tune, test, and maintain detection logic themselves.

EXPAND DETECTION COVERAGE

Leverage more than 2,400 prebuilt detections backed by Securonix Threat Labs to extend coverage across Microsoft, cloud, identity, SaaS, endpoint, network, and third-party security platforms. The Threat Coverage Analyzer continuously identifies detection gaps and recommends improvements aligned with the MITRE ATT&CK framework.

Key Benefits

DETECT MORE WHILE INVESTIGATING LESS

AI-driven behavioral analytics surface high-confidence threats while dramatically reducing alert noise.

ACCELERATE INVESTIGATION AND RESPONSE

Risk scoring, contextual enrichment, entity profiling, and automated correlation provide analysts with immediate insight into attacker behavior, enabling faster triage and response.

STRENGTHEN DETECTION COVERAGE

Expand beyond Microsoft-native telemetry to monitor users, identities, cloud platforms, SaaS applications, endpoints, network activity, and third-party security technologies through more than 600 supported integrations.

REDUCE DETECTION ENGINEERING BURDEN

Deploy more than 2,400 continuously maintained detections without forcing internal teams to build, tune, validate, and update every analytic themselves.

REDUCE OPERATIONAL COMPLEXITY

Deploy rapidly through a lightweight integration without replatforming, additional infrastructure, or duplicate data pipelines, or changes to established analyst workflows.

SCALE WITH YOUR BUSINESS

Support enterprise SOCs, MSSPs, and MDR providers through centralized policy management, multi-tenant architecture, and consistent behavioral analytics across diverse customer environments.

Common Use Cases

INSIDER THREAT DETECTION

Identify privilege misuse, abnormal access, risky peer-group deviations, potential data exfiltration, and abnormal user behavior before sensitive information is compromised.

IDENTITY THREAT DETECTION AND RESPONSE

Detect account compromise, credential abuse, impossible travel, suspicious authentication activity, privilege escalation, lateral movement, and identity-based attacks across hybrid identity environments.

RANSOMWARE DETECTION

Identify early-stage ransomware behaviors, lateral movement, privilege escalation, abnormal data activity, persistence, and command-and-control communications before encryption or widespread disruption occurs.

CLOUD THREAT DETECTION

Monitor suspicious activity across Microsoft Azure, AWS, Google Cloud Platform, and SaaS applications, and cloud workloads using behavioral analytics rather than relying only on static detection rules.

ADVANCED THREAT DETECTION

Correlate activity across users, identities, endpoints, cloud services, SaaS applications, and network telemetry to identify low-and-slow attacks and multi-stage threat patterns.

SOC OPTIMIZATION

Improve analyst productivity by reducing false positives, prioritizing high-risk incidents, automating correlation, and accelerating investigation workflows.

DETECTION COVERAGE OPTIMIZATION

Map detections to MITRE ATT&CK, identify meaningful coverage gaps, and prioritize improvements based on organizational risk.

Why Organizations Choose Securonix

Unlike traditional detection approaches that rely primarily on static rules and thresholds, Securonix continuously learns normal behavior across users and entities to identify sophisticated attacks that might otherwise remain hidden.

Organizations choose Securonix because it delivers:

- AI-driven behavioral analytics
- Industry-leading User and Entity Behavior Analytics
- Identity Threat Detection and Response
- Dynamic risk-based prioritization
- Advanced event and entity correlation
- Continuously maintained Threat Labs detection content

Platform Overview

Securonix Threat Analytics is delivered as a cloud-native SaaS solution designed specifically to extend Microsoft Sentinel.

DEPLOYMENT Rapid onboarding using lightweight integration.

ARCHITECTURE No agents, no duplicate data ingestion, no new customer-side pipelines, and no disruption to existing Sentinel workflows.

DETECTION ENGINE Behavioral analytics, AI-driven correlation, anomaly detection, entity profiling, and risk scoring operate continuously across identity, cloud, SaaS, endpoints, and network telemetry.

COVERAGE ANALYSIS Threat Coverage Analyzer maps detection content to MITRE ATT&CK, identifies gaps, and helps security teams prioritize coverage improvements.

OUTPUT Enriched, high-confidence incidents are automatically returned to Microsoft Sentinel for Investigation and response

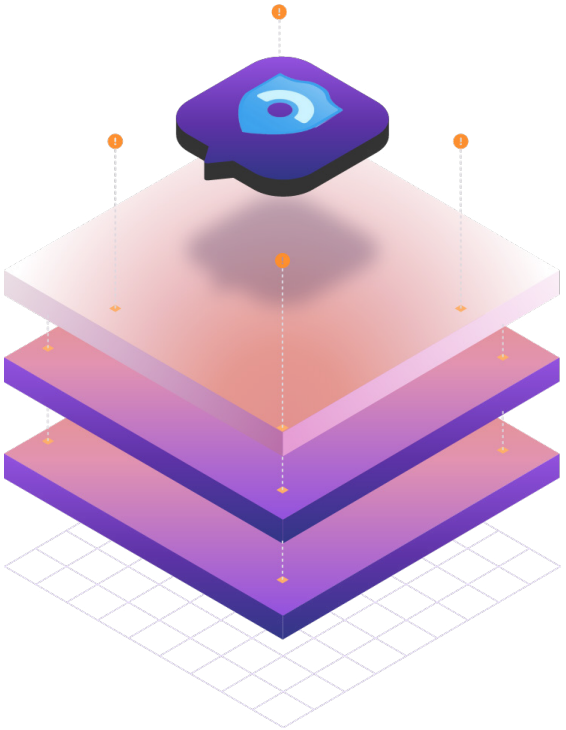
Flexible Deployment

Whether you operate a single enterprise SOC or manage multiple customer environments as an MSSP or MDR provider, Securonix scales to meet your operational requirements.

Available deployment options include:

- Enterprise Security Operations Centers
- Managed Detection and Response providers
- Managed Security Service Providers
- Hybrid and multi-cloud environments
- Multi-tenant deployments

Flexible SaaS pricing aligns with Microsoft Sentinel deployments, organizational scale, and business requirements while eliminating unnecessary infrastructure costs.



Breach Ready. Board Ready.

Securonix Threat Analytics transforms Microsoft Sentinel into a behavior-driven detection platform that helps organizations detect sophisticated threats earlier, reduce alert fatigue, improve analyst productivity, and maximize existing SIEM investments without changing how security teams already work.

Improve Detection Coverage. Accelerate Investigation and Response. Maximize Microsoft Sentinel ROI.

Schedule a demo to see Securonix Threat Analytics in action.
Visit securonix.com or contact sales@securonix.com.