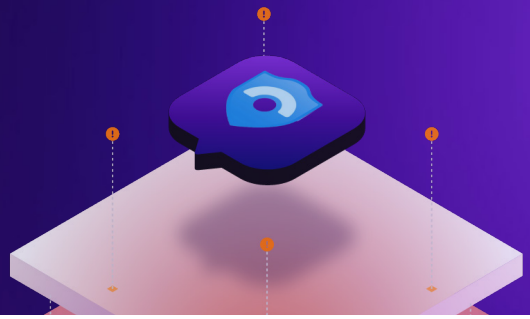
securonix DATASHEET

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—and turn more of your security data into decisive action.

Microsoft Sentinel provides a powerful cloud-native foundation for security operations. But as attacks become more sophisticated and span identities, endpoints, cloud platforms, SaaS applications, and third-party environments, many security teams still struggle with detection gaps, alert fatigue, and slow investigations.

Static rules and threshold-based detections can generate excessive noise while missing the subtle behaviors associated with insider threats, identity compromise, ransomware, cloud attacks, and advanced persistent threats.

Securonix Threat Analytics strengthens Microsoft Sentinel with AI-driven behavioral analytics, continuously maintained detection content, advanced correlation, and dynamic risk scoring. It helps teams detect sophisticated threats earlier and focus on the activity that presents the greatest risk—without replacing Sentinel, duplicating data, or disrupting existing workflows. Enriched, risk-prioritized detections return directly to Sentinel, giving analysts the context to triage faster, investigate with confidence, and respond sooner.

Together, Microsoft Sentinel and Securonix help organizations improve detection coverage, accelerate detection and response, increase analyst productivity, and maximize the value of their existing Sentinel investment.

The result: broader detection coverage, faster detection and response, greater analyst productivity, and more value from your existing Sentinel investment.

Customer Outcomes

Organizations using Securonix Threat Analytics have achieved:

- Up to 875 behavioral detections using behavior-based detections powered by 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

IMPROVE DETECTION COVERAGE

Detect sophisticated threats earlier across insider risk, credential abuse, ransomware, cloud compromise, identity misuse, and advanced persistent threats. Behavior-driven analytics surface abnormal activity that static rules can miss—before attackers reach critical assets.

ACCELERATE DETECTION AND RESPONSE

Turn noisy, disconnected events into risk-prioritized incidents enriched with business context, entity insight, threat intelligence, and MITRE ATT&CK mapping. Analysts spend less time triaging low-value alerts and more time containing meaningful threats.

MAXIMIZE MICROSOFT SENTINEL ROI

Get more value from your existing Microsoft Sentinel deployment without platform migration, duplicate storage, new customer-side pipelines, or operational disruption. Preserve the workflows and investments already in place while accelerating time to value.

How Microsoft Sentinel and Securonix Work Together

Microsoft Sentinel remains the system of record and primary analyst workflow. Securonix adds a cloud-native analytics and enrichment layer that strengthens detection without changing how your SOC operates.

1. Microsoft Sentinel collects and stores security telemetry.
2. Securonix enriches and analyzes that telemetry using behavioral-driven analytics, cross-source correlation, entity context, and dynamic risk scoring.
3. Enriched, high-confidence detections return directly to Microsoft Sentinel for triage, investigation, and response.

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 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.

CONTINUOUSLY IMPROVE DETECTION COVERAGE

Put more than 2,400 prebuilt, Threat Labs-backed detections to work across Microsoft and non-Microsoft cloud, identity, SaaS, endpoint, network, and security platforms. Threat Coverage Analyzer maps coverage to MITRE ATT&CK, reveals meaningful gaps, and helps teams prioritize the improvements that matter most.

Key Benefits

REDUCE ALERT FATIGUE

Behavior-driven analytics and risk-based prioritization help surface the threats most likely to matter while dramatically reducing alert noise.

ACCELERATE DETECTION AND RESPONSE

Risk scoring, entity context, threat intelligence, and automated correlation give analysts immediate insight into attacker behavior—accelerating triage, investigation, and response.

EXTEND VISIBILITY ACROSS YOUR ENVIRONMENT

Apply consistent analytics across users, identities, clouds, SaaS applications, endpoints, networks, and third-party security technologies through more than 600 supported integrations.

REDUCE DETECTION ENGINEERING BURDEN

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

REDUCE OPERATIONAL COMPLEXITY

Deploy rapidly through a lightweight integration—without replatforming, adding agents or customer-side infrastructure, duplicating data pipelines, or changing established analyst workflows.

SCALE WITH YOUR BUSINESS

Standardize behavioral analytics and policy management across enterprise SOCs, MSSPs, MDR providers, and diverse multi-tenant environments.

Common Use Cases

INSIDER THREAT DETECTION

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

IDENTITY THREAT DETECTION AND RESPONSE

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

RANSOMWARE DETECTION

Detect early-stage ransomware behavior—including abnormal data activity, privilege escalation, lateral movement, persistence, and command-and-control communications—before encryption or widespread disruption.

CLOUD THREAT DETECTION

Identify suspicious activity across Microsoft Azure, AWS, Google Cloud Platform, SaaS applications, and cloud workloads with behavior-driven analytics that go beyond static rules.

ADVANCED THREAT DETECTION

Correlate user, identity, endpoint, cloud, SaaS, and network activity to expose low-and-slow and multi-stage attacks..

SOC OPTIMIZATION

Reduce false positives, prioritize high-risk incidents, automate correlation, and accelerate investigations directly within Microsoft Sentinel workflows.

DETECTION COVERAGE OPTIMIZATION

Map detections to MITRE ATT&CK, reveal meaningful coverage gaps, and prioritize improvements according to 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:

- Behavior-driven analytics and 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 a cloud-native SaaS solution designed specifically to extend Microsoft Sentinel.

DEPLOYMENT Rapid onboarding through a lightweight integration.

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

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

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

OUTPUT Enriched, high-confidence incidents return automatically to Microsoft Sentinel for Investigation and response.

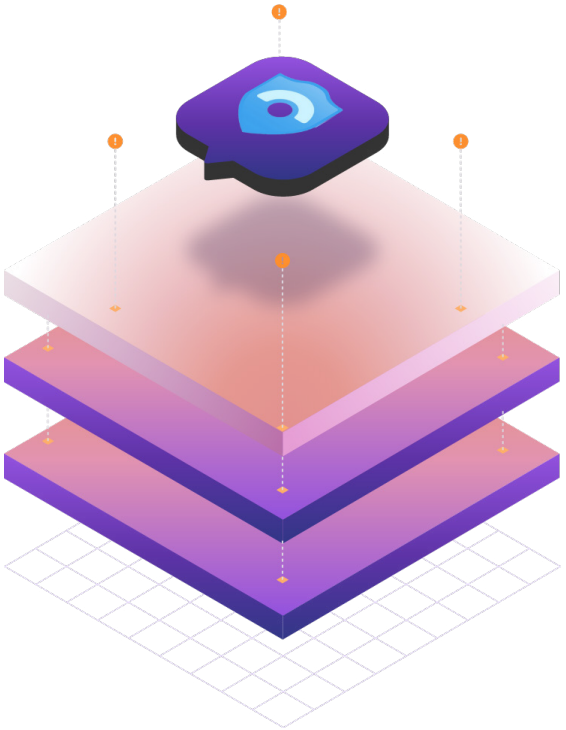
Flexible Deployment

Securonix scales from a single enterprise SOC to complex multi-tenant MSSP and MDR environments.

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 deployment scale, analytics needs, and business requirements—helping organizations avoid unnecessary infrastructure costs.



Breach Ready. Board Ready.

Securonix Threat Analytics extends Microsoft Sentinel with behavior-driven analytics, and risk-based prioritization—helping teams detect sophisticated threats earlier, reduce alert fatigue, accelerate response, and get more value from the SIEM they already use.

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

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