securonix

SOLUTION BRIEF

7 Ways to Improve Microsoft Sentinel Detection Outcomes

Improve Detection Coverage.
Reduce SOC Engineering Work.
Maximize Sentinel ROI.

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

Microsoft Sentinel gives security teams a strong cloud-native foundation for collecting telemetry, investigating incidents, and orchestrating response. But growing data volumes, expanding attack surfaces, and increasingly subtle adversary behavior make it difficult to turn every relevant signal into a high-confidence detection.

Security teams often respond by building more KQL queries, adding static rules, tuning thresholds, and creating custom enrichment and correlation pipelines. This can improve coverage, but it also increases engineering work, content maintenance, alert noise, and operational complexity.

Securonix Threat Analytics provides a more scalable approach.

Securonix extends Microsoft Sentinel with a lightweight, cloud-native analytics and enrichment layer. It applies behavior-driven analytics, industry-leading user and entity behavior analytics, advanced correlation, continuously maintained Threat Labs content, entity context, and dynamic risk scoring to telemetry already collected by Sentinel.

The Detection Challenge Is Not a Lack of Data

It Is the Work Required to Turn Data into Meaningful Security Outcomes

Microsoft Sentinel can collect telemetry across identities, endpoints, cloud infrastructure, SaaS applications, networks, workloads, and third-party security platforms.

The challenge is determining which activity represents meaningful risk.

Modern attacks rarely generate one obvious, high-severity alert. They often unfold gradually across multiple users, systems, and environments. Attackers use legitimate credentials, trusted applications, native tools, and low-volume actions to avoid triggering static rules and fixed thresholds.

A valid login may be followed by an unusual privilege change. A permitted cloud action may be followed by access to an unfamiliar data repository. A series of low-severity authentication failures may represent a distributed credential attack when viewed across thousands of accounts.

Each event may appear routine in isolation. The risk becomes visible only when activity is connected across entities, sources, and time.

For many Sentinel customers, closing these gaps requires substantial operational effort:

- Developing and maintaining custom KQL
- Tuning static thresholds and exceptions
- Testing and validating new detection logic
- Correlating Microsoft and non-Microsoft telemetry
- Maintaining custom enrichment workflows
- Managing low-fidelity, disconnected alerts
- Prioritizing which analytics can run in real time
- Continuously updating content as attacker techniques evolve

The problem is not a lack of telemetry. It is the engineering and analyst effort required to transform that telemetry into high-confidence, risk-prioritized detections.

Strengthen Sentinel Across Three Critical Priorities

Improve Detection Coverage

Extend Sentinel beyond isolated rules and thresholds with behavior-driven analytics, advanced correlation, and continuously maintained detection content.

Securonix analyzes behavior across users, identities, accounts, devices, workloads, applications, and peer groups. It identifies subtle changes that may indicate credential abuse, privilege misuse, insider risk, lateral movement, persistence, ransomware preparation, or data exfiltration. More than 2,400 continuously maintained Threat Labs–backed detections help organizations address high-value use cases without having to build and maintain every analytic from scratch. Threat Coverage Analyzer maps detections to MITRE ATT&CK, identifies coverage gaps, and helps teams prioritize improvements.

The result is broader coverage, earlier detection, and greater confidence across hybrid and multi-cloud environments.

Accelerate Detection and Response

Turn fragmented signals into enriched, risk-prioritized incidents so analysts can investigate and respond faster.

Securonix applies behavioral analytics, adaptive baselines, peer-group analysis, cross-source correlation, threat intelligence enrichment, and dynamic risk scoring. Continuously maintained Threat Labs content evolves with attacker behaviors and techniques. Rather than manually connecting related events or building separate enrichment workflows for each alert type, analysts receive higher-confidence incidents with entity context, threat intelligence, MITRE ATT&CK mapping, and risk scores included. This helps reduce custom KQL development, static-threshold tuning, tenant-by-tenant content maintenance, and reliance on custom correlation pipelines. Analysts spend less time assembling context and triaging noise—and more time validating, containing, and responding to meaningful threats.

The result is faster triage, more efficient investigations, and quicker response within existing Sentinel workflows.

Maximize Sentinel ROI

Keep Microsoft Sentinel at the center of security operations while improving the quality, context, and prioritization of detections analysts receive.

Sentinel remains the system of record, primary investigation console, incident-management environment, and response workflow. Analysts continue working in Sentinel, using the processes and tools they already know. Securonix returns enriched alerts, behavioral anomalies, entity context, risk scores, and high-confidence incidents directly to Sentinel. Organizations preserve their existing incident-management, SOAR, and response processes without SIEM migration, duplicate customer data storage, additional agents, new customer-side ingestion pipelines, or a disconnected analyst console

The result is greater value from the existing Microsoft investment without replatforming the SOC or disrupting

How Securonix Threat Analytics Works

1. **Microsoft Sentinel Collects and Stores**
   Microsoft Sentinel continues to collect security telemetry across identity, cloud, SaaS, endpoint, network, application, infrastructure, and third-party environments.

   It remains the customers:

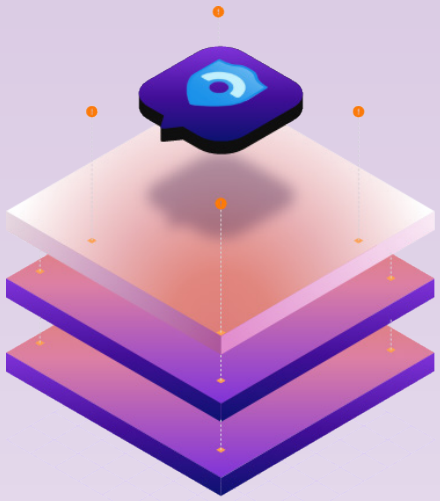
   - Security data platform
   - System of record
   - Investigation console
   - Incident-management environment
   - Automation and response workflow

   Organizations retain their existing Sentinel architecture, data strategy, operational processes, and analyst experience.

2. **Securonix Enriches, Correlates, and Prioritizes**
   Securonix applies a behavior-driven analytics and enrichment layer to the telemetry already collected by Sentinel.

   Capabilities include:

   - Behavior-driven analytics and UEBA
   - Identity Threat Detection and Response
   - Anomaly detection and entity profiling
   - Behavioral baselines and peer-group analysis
   - Cross-source and entity-based correlation



   - MITRE ATT&CK context
   - Dynamic risk scoring
   - Continuously maintained Threat Labs detection content

   Securonix connects related activity across users, entities, sources, and time. Fragmented signals become contextualized, risk-prioritized detections that analysts can evaluate more quickly and confidently.

3. **Analysts Investigate and Respond in Sentinel**
   Enriched alerts, behavioral anomalies, chained activity, entity context, risk scores, and high-confidence incidents are returned directly to Microsoft Sentinel.

   Analysts continue to triage, investigate, orchestrate, and respond using existing Sentinel workflows.

   No agents. No data duplication. No new customer-side pipelines. No SIEM migration. No workflow disruption.

7 Ways Securonix Improves Microsoft Sentinel Performance

Detect Insider Risk Before Sensitive Data Is Lost

Legitimate Access Can Still Represent Material Risk

An employee begins accessing sensitive applications outside normal working hours. The user downloads more confidential data than usual and interacts with systems that are uncommon for the role. The credentials are valid. Access is technically permitted. No individual event exceeds a fixed threshold Viewed together, however, the activity represents a significant departure from established behavior.

How Securonix Strengthens Sentinel

Securonix applies behavioral analytics across users, identities, devices, applications, data sources, and peer groups. It evaluates indicators such as:

- Unusual access times
- Changes in data-access patterns
- Increased interaction with sensitive information
- Activity inconsistent with the user's role
- Deviations from historical behavior
- Differences from peer-group activity
- Abnormal movement across applications or repositories
- Related identity, endpoint, or cloud risk indicators

Rather than presenting each event as a separate alert, Securonix correlates the activity into a risk-scored narrative. Analysts can see which behavior changed, how it differs from normal activity, and why the cumulative risk matters.

Detection Outcome

Security teams can identify potential insider risk and data exfiltration earlier, before suspicious activity results in material loss.

Engineering Outcome

Adaptive user and peer-group baselines reduce the need to create and maintain separate static thresholds for every role, department, or access pattern.

Identify Credential Abuse and Distributed Identity Attacks

Low-Frequency Activity Can Hide a Coordinated Campaign

A threat actor launches a password-spraying or account-enumeration campaign across thousands of users. Each account receives only a small number of attempts, helping the attacker remain below lockout limits and brute-force thresholds.

Microsoft Sentinel records the authentication activity, but each individual event appears low risk. Detecting the campaign requires correlation across users, applications, locations, devices, infrastructure, and time.

How Securonix Strengthens Sentinel

Securonix applies identity analytics, behavioral aggregation, clustering, entity profiling, and cross-source correlation to identify:

- Distributed login attempts across many accounts
- Similar authentication patterns from shared infrastructure
- Enumeration across applications and systems
- Abnormal relationships between users, devices, and locations
- Unusual authentication timing or frequency
- Activity that remains below per-account thresholds
- Successful access following earlier low-severity failures

Dynamic risk scoring increases the priority of the incident as related identity indicators accumulate.

Detection Outcome

Security teams can identify password spraying, account enumeration, credential abuse, and account compromise earlier and with fewer low-value alerts.

Engineering Outcome

Prebuilt identity analytics reduce the need to develop complex KQL correlation logic for every authentication source, attack pattern, and threshold variation.

Expose Low-and-Slow, Multi-Stage Attacks

See the Attack Path, Not a Series of Unrelated Events

An attacker compromises a legitimate account without triggering an obvious malware or brute-force alert. Over several days, the attacker performs reconnaissance, accesses additional resources, changes privileges, and moves laterally.

Each action resembles normal administrative or user activity when evaluated independently.

The threat becomes clear only when the events are connected as stages in the same attack.

How Securonix Strengthens Sentinel

Securonix correlates behavior across identities, accounts, hosts, workloads, applications, cloud services, and time periods.

It connects activity such as:

- Unusual discovery behavior
- Access to unfamiliar systems
- Privilege or group membership changes
- Credential use from new devices or locations
- Lateral movement between systems
- Persistence-related activity
- Changes in data-access behavior
- Related anomalies across multiple sources

Behavioral chaining turns low-severity signals into a unified attack narrative. Dynamic risk scores increase as additional stages of the attack emerge.

Detection Outcome

SOC teams gain earlier visibility into advanced persistent threats, account compromise, privilege escalation, persistence, and lateral movement.

Engineering Outcome

Advanced correlation reduces the need for detection engineers to predict every possible attack sequence and encode each sequence as a custom multi-stage rule.

Identify Ransomware Precursors Before Encryption Begins

The Best Time to Detect Ransomware Is Before the Final Payload Executes

Ransomware incidents often begin with identity compromise, discovery, credential access, privilege escalation, defensive evasion, and lateral movement.

Encryption may be the most visible stage, but it is rarely the first.

Static rules focused on known malware or high-volume file changes may detect the attack only after it has reached a damaging phase.

How Securonix Strengthens Sentinel

Securonix correlates early-stage behavioral indicators across identity, endpoint, cloud, network, and application telemetry.

These may include:

- Unusual administrative activity
- Rapid privilege changes
- Abnormal access to multiple systems
- Credential use across unfamiliar hosts
- Security-control tampering
- Discovery of high-value assets
- Lateral movement patterns
- Suspicious access to backup or recovery systems
- Unusual file and data activity

Securonix connects these precursor behaviors, enriches them with entity and threat context, and increases risk as the attack progresses.

Detection Outcome

Security teams can identify ransomware activity earlier in the attack chain, creating more time to contain compromised identities and systems before widespread disruption occurs.

Engineering Outcome

Continuously maintained detections and cross-source correlation reduce the effort required to build and update separate rules for every ransomware family and attack variation.

Detect Unknown Command-and-Control and Beaconing Activity

Suspicious Infrastructure Is Not Always Known in Advance

A compromised endpoint begins communicating with a newly registered domain. The destination does not appear on a known blocklist, and no malware signature is available.

The traffic is low volume and occurs at regular intervals. There are no significant bandwidth spikes or obvious threshold violations.

Traditional detections that depend on known malicious indicators may not respond until the infrastructure has already been classified.

How Securonix Strengthens Sentinel

Securonix evaluates behavioral, temporal, and contextual indicators such as:

- Domain age and rarity
- First-seen communication
- Abnormal DNS behavior
- Repeated time-based communication patterns
- Frequency and interval consistency
- Destination rarity
- Long-term persistence
- Deviations from normal traffic profiles
- Similar activity across other users or entities

The combination of anomaly detection, behavioral analysis, and curated threat intelligence helps identify suspicious communication even when the destination was not previously known to be malicious.

Detection Outcome

Teams can identify emerging command-and-control infrastructure, beaconing, and persistent outbound communication earlier, reducing attacker dwell time and exposure.

Engineering Outcome

Behavior-driven detection reduces dependence on manually maintained indicator lists and fixed timing or traffic-volume thresholds.

Detect Cloud and SaaS Compromise Across Complex Environments

Attackers Move Across Platforms, Not Product Boundaries

Modern organizations operate across Microsoft services, other cloud platforms, SaaS applications, identity providers, endpoints, networks, and third-party security tools.

An attacker may compromise an identity in one environment, change permissions in another, and access sensitive data through a third. Platform-specific alerts may identify individual actions without showing the broader attack path.

How Securonix Strengthens Sentinel

Securonix supports more than 600 integrations across cloud, identity, SaaS, endpoint, network, infrastructure, and security ecosystems.

It applies behavioral analytics and cross-source correlation to activity such as:

- Unusual cloud-console access
- New or abnormal permission assignments
- Suspicious administrative actions
- Changes in SaaS application behavior
- Access from unfamiliar identities, devices, or locations
- Workload and service-account anomalies
- Cross-platform privilege misuse
- Data access inconsistent with role or peer behavior

Securonix connects Microsoft and non-Microsoft activity and returns the resulting high-confidence detection to Sentinel.

Detection Outcome

Security teams gain broader visibility and more consistent detection across hybrid and multi-cloud environments.

Engineering Outcome

Prebuilt integrations and maintained detection content reduce the need to build a separate analytics and correlation strategy for each platform.

Accelerate Investigations with Context and Risk-Based Prioritization

Analysts Need Complete Incidents, Not More Raw Signals

When an alert is triggered, analysts often need to gather information from multiple tools before determining whether the activity is malicious.

They may need to:

- Review identity and authentication history
- Check IP and domain reputation
- Investigate related user and entity activity
- Search for connected alerts
- Determine asset or application criticality
- Map behavior to MITRE ATT&CK
- Assess the potential business impact
- Build an attack timeline

This work consumes time and can lead to inconsistent investigations, particularly when analysts have different experience levels or face high alert volumes.

How Securonix Strengthens Sentinel

Securonix automatically enriches and correlates detections with:

- Curated, out-of-the-box threat intelligence that adds context about emerging indicators, attacker infrastructure, tactics, techniques, and procedures—helping analysts understand the significance of suspicious activity without manually researching every alert.
- User, identity, device, workload, and entity context
- Historical behavioral activity
- Peer-group comparisons
- Related security signals
- MITRE ATT&CK mapping
- Cross-source correlation
- Dynamic risk scoring
- Business-relevant context

Instead of receiving a disconnected alert, the analyst receives a higher-confidence incident with the context needed to begin triage and investigation.

The incident is returned directly to Sentinel, where the analyst continues working within the existing investigation and response process.

Detection Outcome

Analysts can focus first on the activity most likely to affect the business, improving triage speed, investigative consistency, and response confidence.

Engineering Outcome

Automated enrichment and correlation reduce reliance on custom lookup scripts, point-to-point integrations, manual investigation procedures, and customer-built enrichment pipelines.

Continuously Improve Detection Coverage

See What Your Current Detections May Be Missing

Detection content can grow over time without providing a clear picture of which attacker techniques are covered, where controls overlap, or where meaningful gaps remain.

Manual mapping and coverage assessment can be time-consuming, particularly across large hybrid environments.

Threat Coverage Analyzer maps detections to the MITRE ATT&CK framework, identifies meaningful gaps, and helps teams prioritize improvements.

This enables security and detection-engineering leaders to make more informed decisions about where new content is needed and where existing analytics already provide sufficient coverage.

Customer Outcome

Organizations gain a measurable, continuously improving detection posture across identity, endpoint, cloud, SaaS, hybrid, and multi-cloud environments.

Stop Building Every Detection from Scratch

Continuously Maintained Content Reduces the Detection-Engineering Burden

Custom detection development requires more than writing an initial query.

Each analytic must be:

- Designed
- Tested
- Validated
- Tuned
- Documented
- Mapped to relevant techniques
- Updated as environments change
- Maintained as attacker behavior evolves

Securonix provides more than 2,400 continuously maintained Threat Labs–backed detections. Behavioral analytics, adaptive baselines, advanced correlation, and risk scoring help teams operationalize high-value use cases without manually engineering every component.

This does not eliminate the need for customer-specific detection strategy. It reduces the repetitive engineering work required to maintain broad, effective coverage. **Better Detection. Less Engineering. Same Sentinel Workflow.**

Extend Real-Time Detection Capacity

Apply More High-Value Analytics Without Restricting Coverage to a Small Set of Rules

Real-time detection constraints can force security teams to choose which analytics run immediately and which operate on a delayed schedule.

Securonix expands real-time detection capacity beyond Sentinel's native near-real-time rule constraints, enabling organizations to apply more high-value analytics without relying exclusively on customer-maintained NRT rules.

This helps teams prioritize detection based on security value rather than available native rule capacity.

Customer Outcome

Security teams can expand time-sensitive detection coverage across more behaviors and use cases while reducing the effort required to maintain the underlying analytic content.

Built to Strengthen Sentinel, Not Replace It

Keep the Microsoft Operating Model Your Team Already Uses

Securonix Threat Analytics is designed as an augmentation layer for Microsoft Sentinel.

Sentinel Remains the System of Record

Microsoft Sentinel continues to store customer telemetry and serve as the primary security operations platform.

Analysts Remain in Sentinel

High-confidence detections and supporting context return directly to Sentinel. Analysts do not need to adopt a second SIEM investigation workflow.

Existing Processes Remain in Place

Organizations preserve existing incident management, automation, orchestration, investigation, and response processes.

No Data Duplication

The solution is designed to extend analytics without requiring a duplicate customer data store or separate customer-side ingestion architecture.

No Additional Agents

Organizations do not need to deploy a new set of endpoint agents to gain the analytics capabilities.

No New Customer-Side Pipelines

The lightweight integration model reduces reliance on custom data and enrichment pipelines.

No SIEM Migration

Customers retain their Microsoft Sentinel investment, operating model, and analyst experience.

Enterprise and Service Provider Scale

A cloud-native, multi-tenant architecture supports enterprise SOCs, MSSPs, MDR providers, hybrid environments, and multi-tenant operating models.

Potential Business and Security Impact

Improve Coverage, Efficiency, and the Value of Sentinel

Depending on the customer environment, implementation scope, and operational model, potential or observed results may include:

60%
Approximate Greater Detection Coverage

60%
Approximate Fewer False Positives

85%
Up To 85% Faster Deployment

3X
Up To 3x Greater Sentinel ROI

- Value realization in approximately two to three weeks for supported environments
- Faster triage and investigation
- Less custom KQL development and threshold tuning
- Reduced detection-content maintenance
- Lower reliance on custom enrichment pipelines
- Greater analyst productivity
- Broader behavioral visibility across Microsoft and non-Microsoft telemetry

These figures represent potential or observed results, not guaranteed outcomes. Actual results vary based on environment, use cases, data availability, deployment scope, and operational maturity.

A Stronger Sentinel-Centered Security Operation

Microsoft Sentinel provides the SIEM foundation.

Securonix extends that foundation with behavior-driven analytics, continuously maintained detections, advanced correlation, curated threat intelligence, entity context, and dynamic risk scoring.

Together, they help organizations:

- Improve detection coverage across identity, insider risk, ransomware, cloud compromise, SaaS applications, and advanced threats
- Detect subtle and multi-stage attacks that isolated rules may miss
- Turn fragmented signals into high-confidence incidents
- Reduce custom KQL development and static-threshold tuning
- Apply maintained detection content as threats evolve
- Provide analysts with context at the beginning of an investigation
- Preserve existing Sentinel investigation and response workflows
- Increase the value of telemetry already being collected
- Improve Sentinel outcomes without replatforming the SOC

Microsoft Sentinel is the foundation. Securonix makes its detections stronger.

Improve Your Microsoft Sentinel Detection Coverage

Better Detection. Less Engineering. Same Sentinel Workflow.

See how Securonix Threat Analytics can help your organization extend Sentinel beyond static rules and thresholds, reduce custom detection engineering, and turn existing telemetry into higher-confidence security outcomes.

See What Your Current Detections May Be Missing

Evaluate coverage across priority identity, insider risk, ransomware, cloud, SaaS, and advanced-threat use cases.

Reduce Custom Detection Engineering

Explore how continuously maintained analytics, automated correlation, and behavioral baselines can reduce KQL development, tuning, testing, and content maintenance.

Start Improving Detection Outcomes in Weeks

Assess how Securonix can strengthen detection while Sentinel remains the system of record and analysts continue to investigate and respond using their existing workflows.

Schedule a Personalized Demonstration

Discover how Securonix Threat Analytics can improve detection coverage, reduce SOC engineering work, and maximize the value of your Microsoft Sentinel investment. **Request a demo.**

That is what it means to be **Breach Ready. Board Ready. AI Powered.**

About Securonix

Securonix is transforming security operations with Unified Defense SIEM powered by Agentic AI. Our cloud-native platform unifies detection, investigation, and response to help security teams move faster, operate at scale, and reduce risk with greater precision. With human oversight, measurable governance, and a focus on analyst productivity, Securonix helps organizations save time, control costs, and strengthen trust across the enterprise. Learn more at securonix.com. For more information visit **securonix.com**

securonix