

Securonix UEBA

DETECT BEHAVIORAL CHANGE. UNDERSTAND INTENT. ACT BEFORE IMPACT.



Turn behavior, identity, context, and intent into prioritized action

Risk rarely arrives as one obvious alert.

Insider misuse, compromised identities, and AI-assisted data leakage often develop through small changes in access, data movement, communication, and usage patterns. Static rules can identify known conditions. They struggle to connect weak signals across users, entities, systems, and time.

Securonix UEBA, embedded within Unified Defense SIEM, learns normal behavior across users and entities, detects meaningful deviations, and correlates low-signal activity into prioritized threat chains. Identity, asset sensitivity, geolocation, threat intelligence, business context, entity relationships, and behavioral history add the context analysts need to understand what matters—and why.

The Insider Intent Agent extends that visibility with behavioral, linguistic, sentiment, and AI-interaction signals that can surface emerging insider risk earlier. Agentic Mesh provides the governed orchestration layer for AI-assisted triage, investigation, and approved response, with explainability, auditability, policy controls, and human oversight.

Together, these capabilities help security teams identify risk earlier, reduce investigation drag, and act with greater confidence.



See risk earlier

Identify behavioral drift, peer-group deviations, suspicious sequences, emerging intent signals, and AI misuse before traditional indicators appear.



Prioritize what matters

Turn fragmented anomalies into a contextual risk story around the users and entities that warrant investigation first.



Act faster-with control

Give analysts explainable findings and clearer next steps while preserving human oversight and an auditable decision trail.

How Securonix UEBA Works

Move from raw activity to explainable, prioritized risk.



STEP 1

Establish behavioral baselines

Learn normal activity across users, service accounts, devices, applications, systems, IP addresses, and other relevant entities.



STEP 2

Detect meaningful behavioral change

Identify event rarity, volume and frequency anomalies, peer-group deviations, behavioral drift, and suspicious sequences.



STEP 3

Build an explainable risk story

Correlate related activity into threat chains, enrich it with context, apply dynamic risk scoring, and generate analyst-ready findings and next steps.

Core Capabilities

Behavioral baselining and peer analysis

Model normal activity and compare users and entities with relevant peers to identify deviations that deserve attention.

Threat-chain correlation

Connect low-signal, multi-entity, and multi-stage activity across identity, endpoint, network, cloud, SaaS, applications, and data security systems.

Contextual enrichment and dynamic risk scoring

Prioritize risk using identity, asset sensitivity, geolocation, threat intelligence, business context, entity relationships, and behavioral history.

Extended Detection Beyond Traditional Signals

Retrospective detection

Scan historical activity to uncover latent insider and identity risk, low-and-slow misuse, and patterns that were not visible when they first occurred.

AI-interaction intelligence

Use supported prompt, metadata, sentiment, and interaction telemetry to identify risky data use, policy evasion, and unusual AI-assisted activity.

Governed agentic mesh workflows

Coordinate AI-assisted triage, enrichment, investigation, and approved response through a governed orchestration layer with shared context, explainability, auditability, policy controls, and human oversight.

Analyst Outcomes

More signal. Less investigation drag. Faster, more defensible decisions.

Reduce alert fragmentation, accelerate context gathering, understand why investigation is warranted, and expose AI-assisted risk before material impact.

FROM ANOMALY TO ACTION

Detect → Correlate → Enrich → Prioritize → Act

Common Use Cases

Built for security operations, insider-risk, and identity teams operating across complex cloud, SaaS, hybrid, on-premises, and AI-enabled environments.

Insider threat and risk

Identify malicious, negligent, or compromised insider behavior before it creates material impact.

Identity threat detection and response

Detect credential abuse, abnormal access, suspicious authentication, privilege escalation, lateral movement, and account misuse across human and non-human identities.

AI risk and data leakage

Identify risky prompts, sensitive-data use, policy evasion, and unusual behavior across supported AI-assisted workflows.

Privilege and data misuse

Surface unusual access, privilege abuse, suspicious data movement, and potential exfiltration.

Low-and-slow and multi-stage threats

Correlate activity across systems and time to expose developing risk that isolated alerts and static rules can miss.

Governance and audit readiness

Use explainable detections, governed workflows, masking, audit trails, and approval controls to support defensible investigation and decision making.

Why Organizations Choose Securonix

Standalone UEBA and rule-only approaches can leave analysts assembling context across disconnected alerts and tools. Securonix embeds behavior-first analytics inside Unified Defense SIEM, carrying the risk story from behavioral change to investigation and action.

- ✓ **Behavior-first analytics across users and entities** reveal risk that known-condition rules can miss.
- ✓ **Threat chain correlation** connects activity across identity, endpoint, network, cloud, SaaS, applications, and data.
- ✓ **Contextual enrichment and dynamic risk scoring** help analysts understand which users and entities matter most.
- ✓ **Insider Intent Agent** adds behavioral, linguistic, sentiment, and AI-interaction intelligence for earlier insider-risk prioritization.
- ✓ **Agentic Mesh** brings policy-governed, explainable, auditable, human-supervised orchestration to AI-assisted workflows.
- ✓ **Unified Defense SIEM** keeps detection, investigation, and response in a connected operating workflow.

Platform Overview

Delivery options

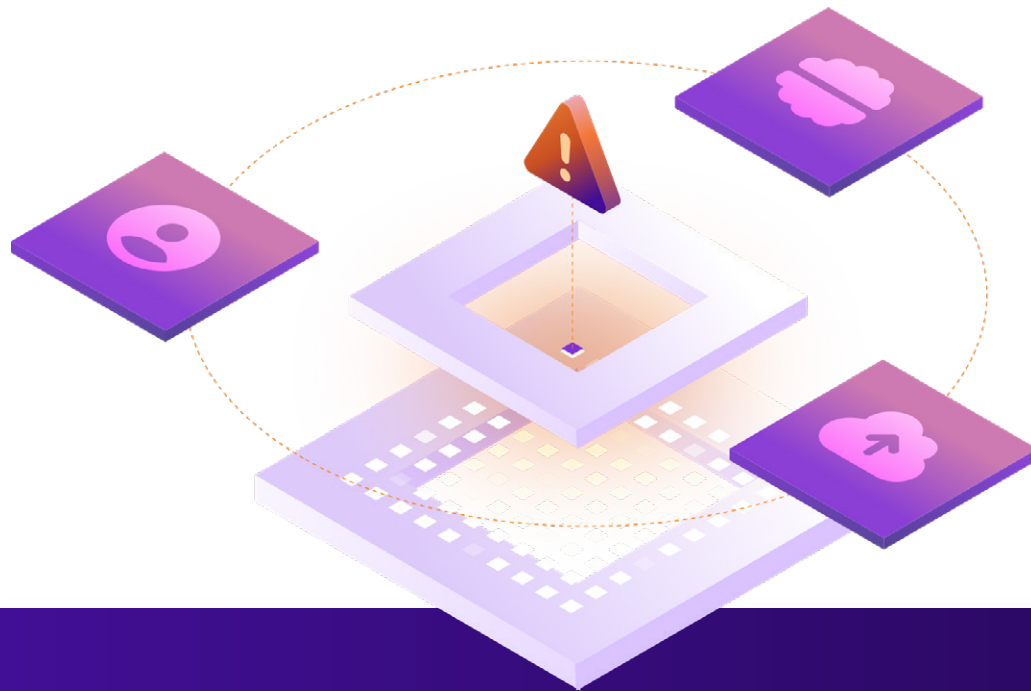
SaaS, hosted, or hybrid deployment with cloud-native analytics across distributed environments.

Entity and data coverage

Users, service accounts, devices, applications, systems, IP addresses, and telemetry spanning identity, endpoint, cloud, SaaS, applications, data, infrastructure, and supported HR sources.

Integrations and governance

APIs, connectors, prebuilt use cases, role-based access, masking, approval-based unmasking, audit trails, escalation policies, and human oversight.



Flexible Deployment and Integration

Operationalize Securonix UEBA across complex enterprise environments without limiting analysis to a single technology domain.

- Broad telemetry coverage across identity, endpoint, cloud, SaaS, applications, data, infrastructure, and supported HR sources
- Users, service accounts, devices, applications, systems, IP addresses, and other relevant entities
- APIs, connectors, prebuilt use cases, and out-of-the-box content for faster time to value
- Role-based access, masking, approval controls, audit trails, escalation policies, and human oversight, backed by onboarding assistance and global support

60%

Fewer false positives and less alert noise

50%

Faster investigations

3x

Greater analyst productivity

Up to figures cited in Securonix source materials. Results vary by environment and implementation.

Breach Ready. Board Ready.

Securonix UEBA turns behavior, context, and intent into prioritized action so teams can find insider and identity risk earlier, investigate faster, and act with confidence.

See risk before the rule breaks.

See Securonix UEBA in action. Visit securonix.com or contact sales@securonix.com.

