

Securonix Advanced Behavioral Analytics

UEBA AND AEBA REVEAL RISK DEVELOPING ACROSS USERS, ENTITIES, AND AI AGENTS

TURN BEHAVIORAL CHANGE INTO PRIORITIZED ACTION.

UEBA + AEBA: See developing risk across users, entities, and AI agents.

Trusted access creates ambiguity. Insider misuse, compromised identities, and unusual AI-agent activity often emerge through small changes in access, authority, data movement, tool use, and time. Static rules see isolated conditions; Securonix connects the weak signals that reveal developing risk.

UEBA finds meaningful change; AEBA extends the behavioral model to AI agents. Embedded in Unified Defense SIEM, Securonix evaluates user, entity, and agent activity—including expected purpose, own or inherited authority, tools, APIs, data access, and interaction patterns—to show what changed, why it matters, and what merits investigation.

Move from evidence to governed action. Insider Intent Agent adds permitted potential-intent context to authorized human-risk investigations. Agentic Mesh accelerates AI-assisted triage, investigation, and approved response with explainability, policy controls, auditability, and human oversight.



See risk earlier across users entities and AI agents

Identify behavioral drift, peer-group deviations, suspicious sequences, changes in AI-agent purpose or authority, potential-intent signals, and AI misuse before traditional indicators appear.



Prioritize what matters

Turn fragmented anomalies into contextual risk stories around the users, entities, and AI agents that warrant investigation first.



Act faster with control

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

How Securonix UEBA and AEBA Work

Move from raw activity to explainable, prioritized risk.



STEP 1

Establish expected behavior

Learn expected activity across users, service accounts, devices, applications, systems, IP addresses, and other entities. For enterprise AI agents, baseline purpose, authority, tools, data, volume, velocity, operating time, and interactions.



STEP 2

Detect meaningful behavioral change

Identify event rarity, volume and frequency anomalies, peer-group deviations, behavioral drift, suspicious sequences, and AI-agent activity that moves outside expected purpose or operating patterns. activity that moves outside expected purpose or operating patterns.



STEP 3

Build an explainable risk story

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

Core Capabilities

Behavioral baselining and peer analysis

Model expected activity across users, entities, and enterprise AI agents. Compare behavior with relevant peers or historical patterns to identify deviations that deserve attention.

Threat-chain correlation

Connect low-signal and multi-stage activity across users, entities, and AI agents using identity, endpoint, network, cloud, SaaS, applications, data security, and supported AI-agent telemetry.

Contextual enrichment and dynamic risk scoring

Prioritize risk using identity, authority, asset sensitivity, geolocation, threat intelligence, business context, entity relationships, agent purpose, tool use, and behavioral history.

Agent and Entity Behavior Analytics

Extend UEBA to enterprise AI agents and identify technically permitted but operationally abnormal behavior without creating a separate investigation silo.

Retrospective detection

Scan historical activity to uncover latent insider, identity, and AI-agent 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, unusual AI-assisted activity, and human-to-agent interaction patterns where telemetry is available.

Governed Agentic Mesh workflows

Coordinate Securonix security agents across AI-assisted triage, enrichment, investigation, and approved response with shared context, explainability, auditability, policy controls, and human oversight.

Analyst Outcomes

More connected evidence. Less investigation drag. Faster, more defensible decisions. Reduce alert fragmentation, accelerate context gathering, understand why investigation is warranted, and surface developing risk across users, entities, and AI agents before material impact.

Common Use Cases

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

Insider threat and risk

Identify malicious, negligent, inadvertent, or compromised insider activity 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 agent behavior and authority risk

Identify enterprise AI agents operating outside expected purpose, invoking unusual tools or APIs, accessing unexpected data, or acting through excessive or inherited authority.

AI interaction and data leakage

Identify risky prompts, sensitive-data use, policy evasion, and unusual human-to-agent interactions where supported telemetry is available.

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 analytics and rule-only approaches can leave analysts assembling context across disconnected alerts and tools. Securonix embeds UEBA and AEBA inside Unified Defense SIEM, carrying the risk story across users, entities, and enterprise AI agents from behavioral change to investigation and governed action.

- ✓ **One behavioral model across users, entities, and enterprise AI agents** reveals risk that known-condition rules can miss.
- ✓ **Threat-chain correlation** connects activity across identity, endpoint, network, cloud, SaaS, applications, data, and supported AI-agent telemetry.
- ✓ **Contextual enrichment and dynamic risk scoring** help analysts understand which users, entities, and AI agents matter most as evidence changes.
- ✓ **AEBA** evaluates expected agent purpose, own or inherited authority, tools, data access, volume, velocity, and interactions in the established SOC workflow.
- ✓ **Insider Intent Agent** adds permitted potential-intent context and supported AI-interaction signals to authorized human-risk investigations.
- ✓ **Agentic Mesh** coordinates Securonix security agents through policy-bound, explainable, auditable, human-supervised workflows.
- ✓ **Unified Defense SIEM** keeps behavioral evidence, investigation, and response in one 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, enterprise AI agents, and telemetry spanning identity, endpoint, cloud, SaaS, applications, data, infrastructure, supported HR sources, and supported AI-agent activity.

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 and AEBA across complex enterprise environments without limiting analysis to a single technology domain or creating a separate AI-agent security silo.

- Broad telemetry coverage across identity, endpoint, cloud, SaaS, applications, data, infrastructure, supported HR sources, and supported AI-agent telemetry
- Users, service accounts, devices, applications, systems, IP addresses, enterprise AI agents, 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

Securonix Results

60%

Fewer false positives and less alert noise

50%

Faster investigations

3x

Greater analyst productivity

Results vary by environment and implementation.

Breach Ready. Board Ready.

Securonix UEBA and AEBA connect behavior, authority, context, and permitted potential-intent signals to prioritized action.

Teams find developing risk across users, entities, and enterprise AI agents earlier, investigate faster, and act with confidence.

See risk developing before impact.

See Securonix Advanced Behavioral Analytics in action. Visit **securonix.com** or contact **sales@securonix.com**.

