securonix

OVERVIEW

The Securonix Advantage

Built for the Agentic SOC

Security operations teams face a widening gap between the risk they must reduce and the people, time, and budget available to do it.

Securonix closes that gap with a Unified Defense SIEM, bringing governed autonomy, behavioral analytics, operationalized threat intelligence, and value-based data economics together to reduce risk faster, multiply analyst impact, maintain control over AI and prove measurable business value.

Move Beyond Assistance. Complete the Work.

Most security AI stops at assistance: finding information generating summaries or recommending next steps. Securonix operationalizes governed autonomy so the SOC can complete more work with the same team. Sam, the Securonix AI SOC Analyst, automates and accelerates Tier 1 and Tier 2 work across triage, investigation, correlation, and response preparation.

Sam operates through Agentic Mesh, the governed orchestration layer that coordinates specialized AI agents, data, and workflows within defined policies and human oversight. Actions remain explainable, auditable, policy-bound, and human-supervised. Analysts stay in control while repetitive work is completed faster and more consistently.

Unify Security Operations Around Outcomes

Securonix brings SIEM, UEBA, SOAR, governed AI, and threat intelligence together in a cloud-native platform, so detection, investigation, response, and reporting operate as one connected system instead of a collection of separate tools. Teams gain faster decisions, more consistent execution, and reporting provides a clearer view of risk across the cybersecurity lifecycle.

Align Telemetry Cost to Security Value

Traditional SIEM economics often force teams to choose between broader visibility and budget control. Data Pipeline Manager and the Data Pipeline Agent align ingest cost to data value. The agent classifies, filters, routes and governs telemetry in real time, while one flexible entitlement applies across Analytics, Investigation, and Basic tiers. High-value data supports real-time detection and investigation; lower-priority data remains available for compliance, forensics, and long-term analysis.

> **30% to 70% greater effective data capacity for the same ingest commitment.**

This value-based model expands visibility, retention, and investigation depth without paying premium analytics rates for every data source. Teams gain predictable security economics and trusted data for effective investigations and AI-driven operations.

securonix

Detect What Static Rules Miss

Modern attacks rarely reveal themselves through a single alert or static rule.

Securonix applies behavioral analytics and entity-centric context across data environments and historical activity to connect subtle signals into attack patterns, improving detection coverage and investigative confidence. Securonix Threat Labs continuously translates emerging attacker techniques into practical detection of content and behavioral models, and hunting intelligence, helping security coverage keep pace with an evolving threat landscape.

Turn Threat Intelligence into Action

Threat intelligence creates business value only when it improves security decisions and operational response. ThreatQ operationalizes threat intelligence by connecting data sources, tools and teams around prioritized context for detection, investigation, and response. Analysts gain a shared source of truth that reduces investigative friction, strengthens collaboration, and accelerates better-informed decisions.

Put Continuous Research to Work

Securonix Threat Labs turns continuous research into practical detection content, behavioral models, and hunting intelligence.

ThreatWatch extends that research into each customer environment, evaluating exposure to emerging threats and delivering human-verified, executive-ready findings. Security leaders gain clearer evidence of risk to guide operational priorities and board-level communication.

Prove Operational Performance in Business Terms

Securonix helps security leaders connect SOC performance to measurable outcomes the business and board can understand.

BUSINESS OUTCOME	PROOF POINT
Return on Investment *Forrester TEI*	**193%**
Reduction in false positives	**Up to 60%**
Increase in analyst productivity	**3×**

Trusted by Security Leaders

Independent analyst recognition and customer validation reinforce Securonix as a trusted choice for modern security operations.

6X

Six-Time Gartner Magic Quadrant Leader for SIEM

Gartner Peer Insights Customer Choice for SIEM

Leader in the 2026 SPARK Matrix for Insider Risk Management

Five-time Leader in the 2026 SPARK Matrix for Digital Threat Intelligence Management

Breach Ready. Board Ready. AI-Powered.

Bring governed autonomy, behavioral analytics, operationalized threat intelligence, and value-based data economics together in Unified Defense SIEM. Reduce risks faster. Multiply analyst impacts. Keep AI explainable and under human control. Prove measurable value to the business and the board.

Book a demo and see how Unified Defense SIEM turns insight into action. Reduce risk faster. Multiply analyst impact. Powered by Agentic AI.

Visit **securonix.com** or contact sales@securonix.com.