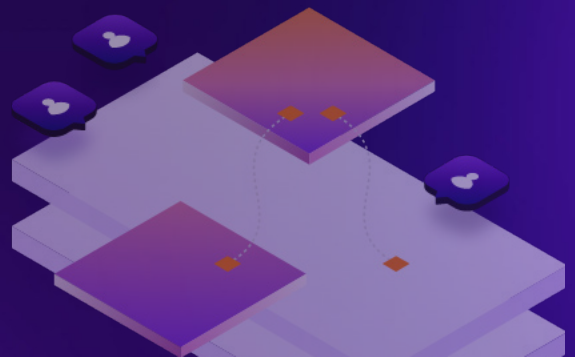
securonix DATASHEET

Unified Defense SIEM

BREACH READY. BOARD READY. AI POWERED.



Modern security operations demand more than alerts and dashboards. CISOs are now expected to reduce risk, improve operational efficiency, prove measurable ROI, and demonstrate resilience at the board level.

Legacy SOC architectures were not built for those outcomes.

Securonix Unified Defense SIEM delivers a new operating model for security operations: AI-powered, cloud-native, and outcome-driven.

By unifying advanced analytics, governed Agentic AI, automated response, and executive-ready reporting into a single platform, Securonix enables organizations to reduce operational complexity, accelerate detection and response, and align security performance directly to business outcomes.

The result is a modern SOC that is faster, more resilient, and built to keep organizations breach ready and board ready.

Why Change?

Legacy SOC Economics and Architecture Are Failing

Legacy SOCs are not failing because security teams lack effort or expertise. They are failing because traditional security architectures can no longer deliver the operational speed, visibility, and measurable outcomes modern organizations require.

Disconnected SIEM, SOAR, UEBA, and threat intelligence platforms create operational friction that slows detection, delays response, and increases total cost of ownership. Analysts spend too much time navigating fragmented tools, manually correlating alerts, and managing infrastructure instead of stopping threats.

As telemetry expands across cloud, SaaS, identity, and hybrid environments, operational complexity compounds:

- Alert fatigue overwhelms analysts
- MTTR remains unacceptably high
- Tool sprawl drives operational and infrastructure costs upward
- High-confidence threats become buried in noise

At the same time, expectations have fundamentally changed. Boards, regulators, and executive leaders now demand measurable proof of resilience, faster breach disclosure, and clear alignment between cybersecurity operations and business risk. Security leaders are expected to demonstrate outcomes, not activity.

©2026 Securonix

The Shift is Clear:
Security operations must evolve from managing alerts to delivering measurable business results.

Securonix enables this transformation with a unified, AI-powered operating model built for modern SOC outcomes:

- Faster detection and response that reduces operational and business impact
- Higher analyst productivity through Agentic AI, automation, and intelligent noise reduction
- Predictable security economics aligned to value, not raw data volume
- Board-ready visibility that translates security performance into measurable business risk and resilience

The result is a modern SOC that is not only operationally efficient, but measurably effective, delivering stronger resilience, lower operational drag, optimized cost control, and greater executive confidence.

Key Benefits

Consolidate and Simplify

Unify SIEM, UEBA, SOAR, and threat intelligence into a single governed platform that eliminates tool sprawl, streamlines workflows, and reduces total cost of ownership.

Accelerate Detection and Response

Leverage Agentic AI, behavioral analytics, and unified workflows to reduce investigation time, accelerate triage, and improve response speed by up to 3x.

Drive Measurable Business Outcomes

Align security operations to measurable outcomes including analyst productivity, operational efficiency, risk reduction, and board-ready ROI metrics.

Embed Compliance by Design

Generate audit-ready, explainable reporting mapped directly to regulatory, governance, and compliance frameworks with full visibility into AI-driven decisions and workflows.

Scale with Confidence

Adopt an open, cloud-native architecture built for elastic scale, flexible data economics, and seamless integration without vendor lock-in or pricing volatility.

©2026 Securonix

True SIEM. Built for Analysts. Powered by AI.

Agentic AI, Built for Analysts

Specialized AI agents accelerate detection, investigation, and response while maintaining transparency, explainability, and full analyst control.

Open by Design

Ingest and correlate data from 750+ sources across cloud, endpoint, identity, SaaS, AI, network, and hybrid environments for complete visibility without vendor lock-in.

Cloud-Native Core

Built on Snowflake and AWS for elastic scale, real-time analytics, and cost-effective storage with no rehydration delays, infrastructure overhead, or performance bottlenecks.

Transparent, Predictable Pricing

Outcome-aligned pricing models and flexible hot/cold data tiers eliminate hidden charges for SOAR, UEBA, analytics, or AI-driven workflows while giving organizations predictable security economics at scale.

Unified Platform

Unify SIEM, UEBA, SOAR, TIP, and threat intelligence into a single cloud-native platform that eliminates tool sprawl, streamlines operations, and enables full-spectrum threat detection, investigation, and response.

Curated Intelligence. Proactive Defense.

Security teams do not need more alerts. They need intelligence that delivers context, confidence, and actionability. Through integrated threat intelligence, automated threat sweeps, and behavioral analytics, Securonix enriches detections and investigations with real-time context across cloud, identity, endpoint, SaaS, and network environments.

By combining internal telemetry with curated external intelligence, Securonix enables organizations to:

- ✓ Prioritize high-confidence threats faster
- ✓ Reduce false positives and analyst fatigue
- ✓ Accelerate investigations with AI-driven enrichment and correlation
- ✓ Detect subtle behavioral anomalies and insider risk earlier

Agentic AI continuously correlates signals across users, assets, sessions, and behaviors to surface risk before impact. The result is a SOC that shifts from reactive triage to proactive defense with greater speed, precision, and operational confidence.

Securonix enriches detections and investigations with real-time context across cloud, identity, endpoint, SaaS, and network environments.

©2026 Securonix

Scale Without Limits. Operate Without Friction.

As telemetry volumes grow, many SIEM platforms introduce rising costs, operational complexity, and performance bottlenecks. Securonix removes those constraints with a cloud-native architecture built on Snowflake and AWS, delivering elastic scale, real-time analytics, and predictable economics.

Organizations gain:

- ✓ A unified data layer that powers detection, investigation, and response
- ✓ Real-time analytics with no rehydration delays or storage bottlenecks
- ✓ Flexible data routing and tiered storage through Data Pipeline Manager Flex
- ✓ Open architecture that eliminates vendor lock-in and preserves ecosystem flexibility
- ✓ 365 days of searchable, always-hot telemetry for investigations and compliance

With outcome-driven data economics and intelligent pipeline management, organizations can expand visibility, improve detection coverage, and optimize storage costs without sacrificing security outcomes.

Agentic AI Built for Analysts.

Securonix Agentic AI is designed to augment analysts, not replace them. Through the Securonix Agentic Mesh and SAM, the AI SOC Analyst, security teams automate repetitive tasks while maintaining full human oversight, explainability, and policy-driven governance.

Modular AI agents accelerate:

- ✓ Alert triage and noise reduction
- ✓ Investigation enrichment and contextual analysis
- ✓ Natural-language threat hunting and search
- ✓ Detection rule creation and policy tuning
- ✓ Automated response orchestration
- ✓ Executive and compliance reporting

Every AI-driven action remains transparent, auditable, and governed through human-in-the-loop controls. The outcome is measurable analyst productivity, faster response times, and AI that security leaders, regulators, and boards can trust.

©2026 Securonix

Turn Compliance Into Confidence.

Compliance is no longer just an audit requirement. It is now a board-level expectation tied directly to resilience, governance, and operational accountability. Securonix transforms compliance from a manual reporting exercise into continuous, automated assurance by delivering:

- Executive-ready reporting aligned to SEC, GDPR, DORA, and global frameworks
- Full transparency into AI-driven decisions and workflows
- Audit-ready investigations with explainable analytics and complete traceability
- Long-term searchable retention without operational overhead

Security leaders gain the visibility, governance, and measurable outcomes needed to demonstrate resilience and communicate cyber risk in business terms.

Operate Faster. Strengthen Defense.

Securonix eliminates the operational drag of legacy SIEM architectures. Security teams gain:

- ✓ Real-time search across all data without delays
- ✓ A unified data layer that eliminates duplication and rework
- ✓ 365 days of instantly accessible telemetry to support faster investigations
- ✓ Continuously evolving detection content without added operational burden

The result is a simpler, faster, and more effective SOC that allows analysts to focus on stopping threats, not managing systems Securonix transforms security operations into a measurable business function by delivering speed, visibility, and outcomes that matter to both the SOC and the board.

Security That Delivers Measurable Business Outcomes.

Securonix is built to align security performance with business impact. Organizations leveraging the platform have achieved:

UP TO **70%** faster detection and response times	UP TO **90%** reduction in false positives	**2-3x** analyst productivity improvements	UP TO **50%** lower data and storage costs	**193%** ROI with measurable operational efficiencies

This is more than SIEM modernization. It is a new operating model for security operations: AI-powered, outcome-driven, and designed to help organizations stay breach ready and board ready every day. With productivity-based AI and value-aligned data economics, SOC investments scale with outcomes, not data volume.

©2026 Securonix

Securonix Solves Tool Sprawl

Rapid Time-to-Value

Deploy within your cloud environment with minimal disruption and begin delivering measurable security outcomes in less than 30 days.

Unified Analyst Experience

Work within a single, continuous investigation workflow that eliminates swivel-chair operations, reduces context switching, and accelerates detection and response.

Reduced Alert Noise

Reduce false positives by up to 60%, allowing analysts to focus on high-confidence threats instead of repetitive triage and alert fatigue.

AI-Driven Operations with Governance

Automate triage, enrichment, investigation, and response workflows with Agentic AI while maintaining full human oversight, explainability, and policy-based governance.

Optimized Data Economics

Route telemetry based on analytical value, not raw volume, to expand visibility, improve detection coverage, and control ingestion and storage costs without sacrificing security outcomes.

Modular AI Agents

Leverage specialized AI agents for detection, investigation, response, threat intelligence, and executive reporting, all operating within a governed and explainable framework.

Lower Total Cost of Ownership

Reduce SIEM costs by 30–50% through outcome-aligned pricing, intelligent data management, and unified operations that eliminate unnecessary platform complexity.

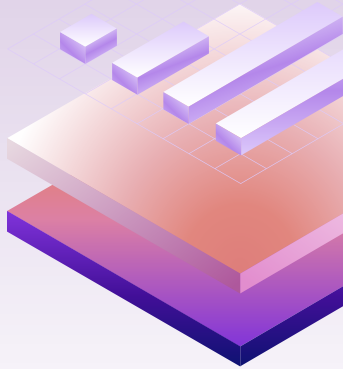
Measurable Business Impact

Translate security operations into measurable business outcomes with improved analyst productivity, faster response, reduced risk, and lower operating costs.

Unified Architecture

SIEM. UEBA. SOAR. TIP. One governed, AI-powered platform.

Securonix gives organizations the speed, scale, governance, and economics required to modernize the SOC and prove value at every level of the business.



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

©2026 Securonix