securonix DATASHEET

Unified Defense SIEM

Breach Ready. Board Ready. Powered by Agentic AI.

Why Change? Legacy SOCs Can't Keep Up

Let's be honest—most legacy SOCs are stuck. Disconnected SIEM, SOAR, UEBA, and TIP tools don't work well together. They create silos, drive up costs, and slow everything down. That means longer investigations and missed threats buried in fragmented context.

And it's not just about detection anymore. Regulations like SEC, GDPR, and DORA are raising the bar. Faster breach disclosure, tighter third-party oversight, continuous proof of resilience—it's all on the table. Meanwhile, boards aren't satisfied with static dashboards. They want results they can measure.

The Securonix Difference

That's where Securonix comes in. We deliver the industry's first **Unified Defense SIEM powered by Agentic AI**—purpose-built to reduce MTTR, stop threats faster, and deliver ROI your board can actually see.

For Analysts: Faster, Simpler Operations

Your analysts shouldn't waste time babysitting tools. With Securonix, they can focus on stopping threats:

✓ **One Unified Data Layer** – Store telemetry once and use it everywhere: detection, investigation, and response.

✓ **Always Fast** – Our single-tier, cloud-native architecture eliminates delays and bottlenecks.

✓ **Noise Cancelation** – AI filters out false positives and redundant alerts so analysts get their time back.

✓ **Continuously Updated Threat Content** – Delivered as-a-service, so defenses evolve without piling more work on your team.

For Leaders: ROI, Compliance & Assurance

✓ Security should show its value, not just its activity. With Securonix, you get:

✓ Executive-Ready Reporting – Automated insights that map directly to compliance standards.

✓ 177% ROI – Lower costs, reduced risk, and faster time-to-value.

✓ 365 Days of Always-Hot Data – Investigations and audits that don't stall out.

✓ Scalable by Design – An open, cloud-native platform that grows with your business and avoids vendor lock-in.

True SIEM. Built for Analysts. Powered by AI.

Agentic AI, Built for Analysts
Modular AI agents accelerate detection and response-while maintaining transparency and analyst control

Open by Design
Ingest data from 750+ sources-cloud, endpoint, Identity, SaaS, and more-for full visibility across hybrid environments

Cloud-Native Core
Built on Snowflake and AWS for elastic scale, real-time analytics, and cost-effective storage-without rehydration delays

Transparent, Predictable Pricing
Ingestion-based pricing with flexible hot/cold tiers-no hidden charges for SOAR, UEBA, or advanced analytics

Unified Platform
SIEM, UEBA, SOAR, and TIP in a single platform-removing tool sprawl and enabling full-spectrum threat response

Securonix Unified Defense SIEM

Powered by Agentic AI

Securonix brings together advanced analytics, autonomous response, and ROl-driven reporting to do what legacy SIEMs can't-**reduce MTTR, stop threats faster, and keep your organization breach ready and board ready every single day.**

Open by Design. Built for Scale.

Most SIEMs slow down as your data grows. Not Securonix. Our cloud-native, single-tier architecture— powered by Snowflake and AWS-handles massive volumes without breaking a sweat. No tiers, no delays. Just fast, scalable performance. And because we're built to integrate, not isolate, you avoid vendor lock-in while gaining the flexibility to scale and adapt as threats evolve.

Curated Intelligence. Proactive Defense.

You don't just need alerts-you need actionable intelligence. With automated threat sweeps, curated content from Threat Labs, and real-time intelligence sharing, Securonix helps your team collaborate smarter and respond faster-staying one step ahead of attackers.

Board-Ready Compliance, Built In.

Meeting regulations doesn't have to be a headache. Securonix delivers **automated, executive-ready reporting** that maps directly to board and compliance requirements-turning what used to be manual work into streamlined, auditable insight.

Security as a Business Driver.

Security isn't just about defense anymore-it's about value. Securonix delivers 177% ROl by reducing risk, cutting operational costs, and giving leaders the visibility they need. The result: a SOC that runs faster, smarter, and proves its worth at every board meeting.

Faster Searches. Simpler Operations. Stronger Defense.

Traditional SIEMs rely on complex, multi-tiered storage that slows investigations and drives up costs. Securonix changes the game with a single-tier, unified data layer designed for speed and simplicity:

- ✓ **Always Fast** - Optimized for large-scale searches with no delays or bottlenecks.
- ✓ **One Data Layer** - Store telemetry once to power detection, investigation, and response—no duplication, no re-correlation.
- ✓ **Streamlined Operations** - Analysts spend more time stopping threats, less time managing storage and tools.
- ✓ **Real-Time, Always-Hot Data** - A full year of searchable, high-fidelity telemetry means you catch threats in hours, not months.
- ✓ **Continuously Updated Threat Content** - Delivered as-a-service, keeping defenses current without overwhelming your team.

Securonix gives you the speed, scale, and intelligence you need to **modernize your SOC and prove value at every level of the business.**

Securonix Solves Tool Sprawl

Rapid Time-to-Value

Deploys in your cloud with minimal disruption- showing measurable outcomes in <30 days

Single Console, Shared Timeline

Analysts work within an continuous investigation flow- no more swivel-chair analysis

Noise Cancelation

Filters false positives and redundant alerts, reclaiming analyst hours

Agentic Al

Automates investigantion and triage while keeping humans in control

Data Pipeline Manager

Streamiines ingestion-cutting noise, reducing cost, and delivering the right data to analysts when they need it

Modular Al Agents

Automate triage, enrichment, and response in one workflow- boosting productivity without adding tools

Lower TCO

Outcome-based pricing and smart ingestion reduce licensing and storage costs by 30-50%

Cyber ROI

Outcomes expressedrd in board-ready language, risk reduced, costs lowered, efficiency gained

UNIFIED ARCHITECTURE

SIEM, UEBA, SOAR, and TIP in one cloud-native platform

See how Securonix can modernize your SOC, schedule a demo at:

WWW.SECURONIX.COM/REQUEST-A-DEMO