

The logo for Securonix, featuring the word "securonix" in a lowercase, sans-serif font. The letter "i" is replaced by a small orange square with a white dot in the center, resembling an eye or a data point. The background of the entire page is a dark purple and blue gradient with abstract, glowing particle effects and a wireframe structure on the right side.

securonix

# Healthcare Leader Boosts Threat Detection and Response Through Cloud-native SIEM



# Healthcare Leader Boosts Threat Detection and Response Through Cloud-native SIEM

## CASE STUDY

### The Challenge: On-premises SIEM Lacks Visibility & Actionable Insight

A leading Midwestern healthcare provider found themselves lagging with outdated, on-premises SIEM technology lacking the visibility, scalability, and convenience of an analytics-fueled, cloud-based SIEM solution. The current application showed its age and wasn't delivering the actionable outputs the team needed to manage threats effectively. The healthcare provider's CISO decided it was time to look for another solution, and the idea of switching to a cloud-native next-generation SIEM gained traction.

The healthcare provider's original plan was to migrate to the current provider's SaaS solution, but the team was discouraged by its high price. Disappointment and understandable skepticism mounted as the team prepared to explore other market options.

The search was on for a analytics-driven, cloud-native SIEM solution capable of collecting data at scale, increasing threat visibility, and expediting detection and response while making security operations simpler. Four vendors rose above the rest, including Securonix, based on its leader status in the Gartner Magic Quadrant for SIEMs report and favorable industry peer reviews.

### The Solution: Securonix for Security Analytics at Cloud Scale

The healthcare provider's team prioritized state-of-the-art analytics combined with the flexibility of a cloud architecture. Unlike many competitors, Securonix's platform is cloud-native, built in the cloud and for the cloud with efficient and straightforward on-demand scaling and architecture resiliency. These qualities resonated with the team, and in April 2021, the healthcare provider began a partnership with Securonix.

Lack of actionable output was no longer a problem with the Securonix solution on the job, and it didn't take long for the advantages of this Next-Gen SIEM to become apparent. Out of the box, the security team appreciated the open, modular architecture for flexible and convenient deployment. The Securonix platform then provided real-time data collection and viewing at scale with added perks like customizable alerts. Gaining industry-leading analytics fueled by machine learning, context enrichment, and playbooks for automated response, the healthcare provider felt more confident that their cyber risk was reduced.

Securonix continued to impress the healthcare provider with more than just the ease and efficiency of a cloud-native, analytics-based SIEM built for the modern enterprise. From top to bottom, the team was pleasantly surprised by the superior follow-up service and support delivered by Securonix. In the words of pleased CISO, "Securonix's response on any issue was far superior to what we experienced with the previous provider."



## Business Impact: Superior Data Security with Single-Pane-of-Glass Simplicity

The team now accesses real-time, actionable data with rapid response capability, all from the convenience of a single collaborated platform. Threats can be detected and eliminated faster—shrinking dwell times and potential harm to the organization. Now risk can be managed with fewer false positives, and the challenge of maintaining regulatory compliance becomes less daunting.

Even beyond these many apparent advantages, the most significant business benefit of all may be the user-friendly simplicity of Securonix's Next-Gen SIEM. Superior user interfaces boost ease, allowing users a more intuitive experience. Unparalleled threat visibility combines with cloud convenience, all from a collaborated, "single-pane-of-glass" platform. The CISO sums up this critical benefit, "Securonix provided a better integrated solution, not one I had to jump into three different systems to use."

### Company Profile

This healthcare system has evolved from a local community medical center to its regional tertiary healthcare leader in a five-state region. They have engaged Securonix to provide Next-Gen SIEM.

### About Securonix + AWS

Securonix is leading the transformation of cybersecurity with the industry's first Unified Defense SIEM powered by agentic AI and built natively on Snowflake and AWS. By leveraging Amazon Bedrock (including Anthropic's Claude 3) for advanced AI agents and a split-data architecture, Securonix delivers elastic, privacy-preserving analytics that keep telemetry where customers want it while cutting storage costs and accelerating detection. Our platform collects and correlates logs across AWS services — including ECS, CloudTrail, CloudWatch, and S3 — applies behavioral analytics and AI-driven threat models, and automates response with built-in SOAR to provide end-to-end visibility for containerized workloads and hybrid environments. Recognized as a Leader in the Gartner® Magic Quadrant™ for SIEM and a Customers' Choice by Gartner Peer Insights™, Securonix empowers organizations to move from reactive security to proactive, autonomous operations. Learn more at [www.securonix.com](http://www.securonix.com).

Securonix is built on and powered exclusively by Amazon Web Services (AWS), ensuring scalability, resilience, and enterprise-grade security. Securonix utilizes AWS Services including Bedrock, S3, EC2, RDS, and many others.