securonix

INDUSTRY:
**HEALTHCARE SERVICES**

LOCATION:
**MIDDLE EAST**

CUSTOMER CASE STUDY

# Securing a Fragmented Network: How A Leading Healthcare Provider Strengthened Its Security Program with Securonix

**Challenge:** A major healthcare organization in the Middle East, operating across multiple locations with thousands of employees, sought to modernize its security infrastructure to meet evolving regulatory requirements. Their objectives included enhancing visibility, streamlining audit processes, strengthening insider threat detection, and improving overall security to protect sensitive patient data across their extensive network.

**Solution:** To address these challenges, the organization deployed Securonix's SIEM and UEBA solutions, ensuring centralized monitoring, advanced analytics, and improved threat detection. These tools provided a comprehensive view of security activities across the entire environment. With scalable event processing capabilities, the organization was able to expand its security operations efficiently as it continued to grow.

For more information, visit securonix.com.

## Benefits

- **Enhanced Visibility:** Complete monitoring of user behavior and system activities across all departments.
- **Operational Efficiency:** Streamlined security incident management and audit preparation, reducing compliance workload by 33%.
- **Improved Threat Detection:** Strengthened ability to identify and mitigate insider threats.
- **Scalability:** Flexible log ingestion capabilities supported organizational growth without compromising security.

## Results

Securonix transformed a major healthcare organization's security, ensuring compliance, efficiency, and data protection with a scalable framework for growth.

- **33%** Faster Audits
- **Improved Visibility** Across All Locations
- **Scalable Security** With Flexible EPS

> “Our organization underwent around 10 audits annually, each of which was labor-intensive and time-consuming. The audits required the manual collection of logs from multiple fragmented systems and the involvement of a dedicated compliance officer to manage the workload. Securonix’s advanced compliance reporting capabilities made the audit process significantly more efficient. This streamlined approach drastically reduced the time required for audit completion and greatly improved the overall efficiency of the information security compliance team.”
>
> – Associate Vice President Information Security,
> A Major Healthcare Organization in the Middle East

## The Challenge

A major healthcare organization in the Middle East, operating across multiple locations, faced significant information security challenges due to its complex IT infrastructure. Over the years, various acquisitions had resulted in a fragmented network with disparate systems, making visibility, centralized monitoring, and regulatory compliance difficult. The organization struggled with a lack of visibility across multiple IT environments, no centralized log repository for effective threat detection, and increased insider threats due to limited user behavior analysis. Additionally, regulatory audits were time-consuming and complex, and the absence of forensic capabilities hindered the organization’s ability to investigate security breaches.

To address these challenges, the organization prioritized integrating its IT environments, implementing centralized monitoring systems, and enhancing its security posture through advanced threat detection, user analytics, and enhanced forensic capabilities. These initiatives were crucial to safeguarding patient data, streamlining operations, and meeting stringent regulatory requirements.

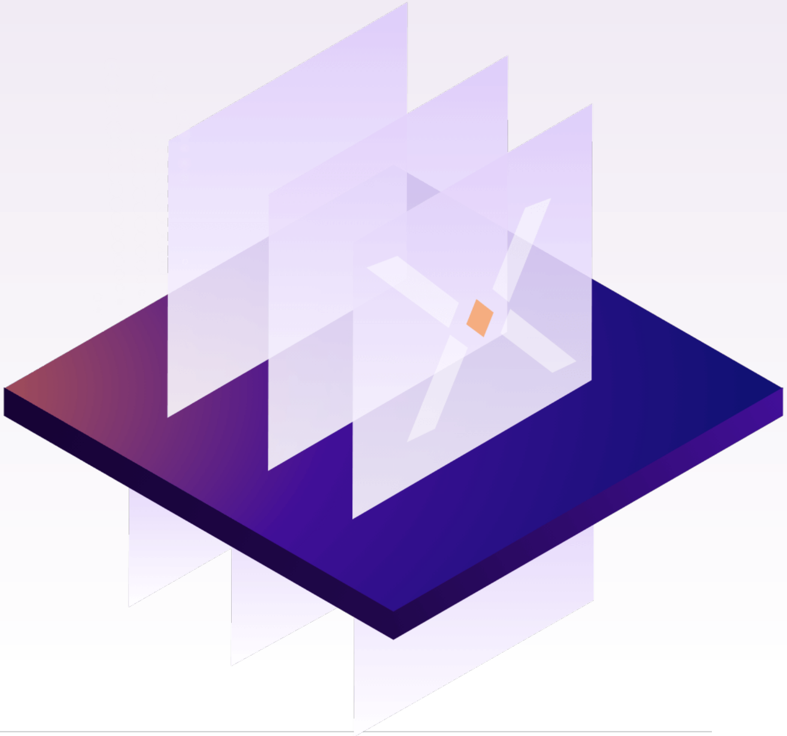
## Solution

The organization embarked on a major security transformation initiative. A key step was deploying Securonix's SIEM and UEBA solutions, which provided enhanced visibility, centralized security monitoring, and improved forensic capabilities. The flexible scaling of Securonix's EPS ingestion allowed the organization to expand seamlessly, ensuring security operations remained robust even as new facilities were added. With these enhancements, the security team could monitor user behavior across all locations, correlate logs efficiently across different systems, detect and mitigate insider threats, and reduce the compliance workload through automated audit capabilities.

## Results

The implementation of Securonix's solutions significantly improved security operations, compliance management, and insider threat detection. The organization reduced regulatory audit preparation time by 33%, enhanced security visibility across its vast network, and created a scalable security framework that could grow with its expansion.

> **"By deploying Securonix's Unified Defense SIEM solution with natively integrated UEBA capabilities, our customer has dramatically enhanced visibility, operational efficiency, and audit compliance reporting via seamless monitoring across all department monitoring. This partnership has provided a scalable security solution to support their continued growth."**
>
> – Sheik Abideen, Regional Sales Director, Securonix



## Key Challenges

- **Limited information security Tools:** Before implementing Securonix, the organization heavily relied on manual processes to correlate and collect logs for forensic and audit purposes. This prompted them to recognize the need for more advanced tools to enhance operational efficiency. They embarked on a journey to transform their information security operation program, by implementing a SIEM and UEBA tool as the first critical step in this initiative.
- **Fragmented Infrastructure:** Over time, the organization has grown to become a combination of multiple business entities. It faced challenges in achieving visibility and managing security across siloed departments, each with different technical solutions. It needed a security solution that would help it gain visibility across its entire environment.
- **Varying User Behaviors:** User behavior across different entities varied due to cultural and technological differences, complicating efforts to detect and respond to security incidents, such as phishing or insider threats. They needed a UEBA solution that would help them restrict or allow certain behaviors across different departments.
- **Audit Management:** The organization faced significant challenges with regulatory audits, requiring extensive manual efforts to collect logs from disparate systems for compliance reporting. The lack of centralized log management capabilities put them at risk of financial penalties from regulators.

## Key Features Utilized

- **SIEM and UEBA Integration:** The seamless integration of Securonix's SIEM and UEBA solutions provided comprehensive visibility across the organization's fragmented infrastructure.
- **Flexible EPS Scaling:** Securonix's ability to scale EPS ingestion allowed for seamless expansion as the organization onboarded new clinics and business entities, ensuring they could manage their growing data needs.
- **Compliance Reporting:** Securonix's compliance reporting feature streamlined auditing efforts by offering automated log collection, retrieval, and reporting, significantly reducing the time and labor required to meet regulatory requirements.

## Benefits

- **Enhanced Visibility:** Securonix provided complete visibility across the organization's IT infrastructure, allowing the security team to make sense of logs, monitor user behavior, and respond swiftly to incidents across different departments.
- **Operational Efficiency:** Integrating SIEM and UEBA reduced time spent managing security incidents, saving time and money and making day-to-day operations more efficient.
- **Audit Compliance Simplified:** Securonix's compliance reporting capabilities provided easy access to logs going back as far as 3-12 months, reducing audit log preparation time by 33% and effectively reducing the workload of the information security compliance officer. This allowed the organization to redirect resources to higher-value projects.
- **Scalable Security for Growth:** The flexible EPS capability allowed the organization to expand its security operations log collection and monitoring efforts seamlessly as it opened new clinics across the Middle East.

## Conclusion:

A major healthcare organization successfully transformed its fragmented information security posture by partnering with Securonix. The platform enhanced visibility, streamlined audits, and strengthened threat detection, enabling the organization to effectively address internal risks and compliance challenges. This strategic move has significantly bolstered the organization's information security posture and operational efficiency.

### 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.

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.