securonix

RAKBANK

INDUSTRY: **FINANCIAL SERVICES (BANKING)**

LOCATION: **UNITED ARAB EMIRATES (UAE)**

CASE STUDY

# RAKBANK Replaces ArcSight with Securonix, Accelerates Threat Detection and Data Retrieval with Snowflake Integration

**Challenge:** RAKBANK, a leading UAE financial institution, faced escalating cyber threats, operational inefficiencies, and delayed threat detection due to a fragmented legacy SIEM environment (ArcSight). Their on-premises setup caused hour-long delays for historical searches, lacked scalable storage, and failed to provide advanced behavioral analytics, making it challenging to meet high-volume, high-compliance requirements.

**Solution:** After evaluating next-gen SIEM options, RAKBANK selected Securonix Unified Defense SIEM with integrated Snowflake for cloud-native scalability, extended hot storage, and advanced behavioral analytics. The transition consolidated multiple SIEM systems, improved search speed dramatically, enriched 85% of data sources with context, and enabled real-time threat detection and response. Customized integrations with in-house SOAR further streamlined operations.

### Benefits

- **Consolidated Multiple SIEMs into a Single Unified Platform:** Enhancing SOC efficiency.
- **85% Data Sources Contextually Enriched:** Improving alert fidelity and investigations.
- **35% Increase in Detection Coverage:** Surfacing threats previously missed.
- **Extended Hot Storage Access to 1 Year:** Enabling faster, deeper investigations.

### Results

- **15% reduction** in false positives
- **30% increase** in cloud/cyber threat detection
- **Investigation times reduced** from hours to minutes

**"RAKBANK's journey is a perfect example of how a forward-thinking organizations can elevate its security posture with the right technology. Our partnership with RAKBANK has been focused on empowering their team with advanced threat detection, scalable analytics, and a seamless user experience. We're proud to help drive their success."**

**– Ajay Biyani, Vice President, Sales – APMEA, Securonix**

## The Challenge

RAKBANK, a leading national bank in the UAE with over 3,000 employees, serves both retail and corporate clients. Operating in a region frequently targeted by cyber threats such as phishing and credit card fraud, the bank needed to strengthen its security operations. Despite having a robust security stack, their multi-legacy SIEM environment, consisting of ArcSight, was unable to provide a consolidated perspective which added complexity to cyber defense operations.

Their legacy on-premises SIEM infrastructure experienced performance issues, which significantly hindered log ingestion, data retrieval, and threat detection. Searching through historical logs, critical for investigations, could take nearly an hour, severely delaying response times. The system offered only limited "hot" storage, making it difficult to quickly access older data – a critical capability for a high-volume, high-compliance environment like banking.

The lack of behavioral analytics, scalability, and storage flexibility of the legacy SIEM infrastructure constrained operations. RAKBANK recognized that to stay ahead of sophisticated cyberattacks, it required a next-generation Security Information and Event Management (SIEM) solution with built-in User and Entity Behavior Analytics (UEBA), seamless cloud scalability, extended hot storage and streamlined log management.

After evaluating several next-generation SIEM options, RAKBANK selected Securonix for its cloud-native architecture, industry-leading UEBA capabilities and deep integration with Snowflake.

Initially deployed as a standalone UEBA solution, Securonix has since become RAKBANK's unified SIEM and UEBA platform—providing advanced threat detection, real-time behavioral analytics and scalable event ingestion to meet growing operational demands.

With Snowflake, RAKBANK now benefits from extended hot storage for up to one year of data, enabling faster searches and investigations while reducing infrastructure complexity and cost. This marks a significant improvement from the previous SIEM, which offered only 1-2 months of searchable data. This change now allows for 1 year of hot-searchable data availability, enabling deep investigations, historical searches, and threat hunting.

**"Moving to Securonix has transformed our security operations. We went from sluggish, manual processes to a modern, behavioral-driven approach that helps us detect threats faster and respond more efficiently. Their support team is always ready to help—and they actually listen to customer feedback. The integration with Snowflake has been a game-changer for us. Having up to a year of hot storage means we can access historical data instantly, without the delays we previously faced. It's improved our investigation speed, reduced operational friction, and made our analysts' jobs much easier."**

**– Jayakumar Ramasamy, Vice President - Information and Cybersecurity Operations, RAKBANK**

The bank also leverages Securonix's flexible integration capability to integrate Securonix's Incident Management to their in-house SOAR to automate response actions, and customized use cases have been developed to meet their unique business requirements.

Advanced data enrichment capabilities have also been implemented—85% of RAKBANK's data sources are now enriched with contextual information such as user identity, geo-location, and customer lookup tables.

This flexible and intelligent security foundation has significantly enhanced RAKBANK's ability to detect and respond to threats in real time.

## Key Challenges

- **Multiple SIEM Infrastructure:** RAKBANK had deployed different solutions to cover On premise and Cloud Solutions.
- **Inefficient Historical Log Search:** ArcSight's on-prem infrastructure made historical data retrieval extremely slow, taking up to an hour to search just three months of logs, delaying investigations and response.
- **Limited Behavioral Threat Detection:** ArcSight lacked UEBA capabilities, preventing the security team from detecting insider threats and anomalous user activity across the environment.
- **Log Ingestion and Correlation Issues:** The previous SIEM struggled with log ingestion at scale and offered limited correlation across diverse log sources, reducing detection coverage.
- **Scalability Constraints:** The legacy on-prem deployment was unable to meet increasing EPS demands and could not scale to support the bank's evolving security and operational needs.
- **Minimal Vendor Support and Innovation:** ArcSight provided little ongoing support or product evolution and lacked responsiveness to customer feedback or new threat detection requirements.

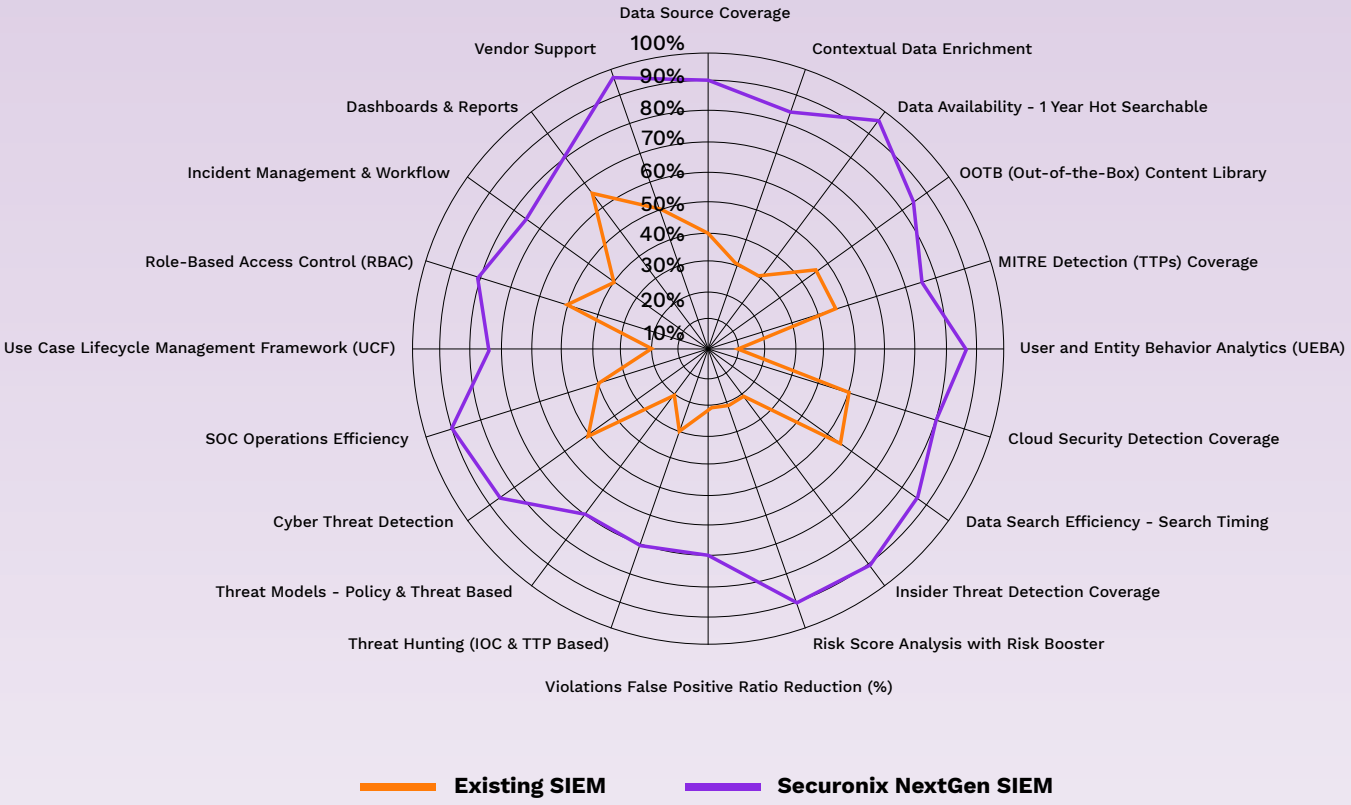
## Key Features Utilized

- **Cloud-Native SIEM Platform:** Securonix's scalable, cloud-native architecture enabled RAKBANK to ingest and analyze large volumes of security data without the limitations of on-prem infrastructure.
- **Securonix's pre-built Connector Library:** Securonix's extended connector library enabled RAKBANK to onboard and monitor a wide variety of on-premise as well as AWS and Azure cloud applications without the need for customized development.
- **Advanced Behavioral Analytics and Monitoring:** Built-in UEBA capabilities and continuous behavioral monitoring enabled RAKBANK to detect anomalous activity, improve detection accuracy, and expand visibility across users, endpoints, and infrastructure.
- **Snowflake Integration for Extended Hot Storage:** Native integration with Snowflake provided up to one year of fast-access hot storage, improving historical investigations and reducing costs.
- **Customizable Detection and Policy Management:** Flexible rule and policy creation allowed RAKBANK to tailor threat detection and response use cases to meet business-specific needs.
- **Proactive Support and Enablement:** The Securonix team delivered hands-on implementation, ongoing support, and early access to product enhancements with fast feedback turnaround.

# Benefits

- **Consolidation:** RAKBANK were able to consolidate their multi-SIEM environments into one comprehensive feature rich platform, enhancing SOC efficiency from the onset itself.
- **Deep Contextual Enrichment:** 85% of RAKBANK's data sources are now enriched with contextual metadata, including user identity, geo-location, and customer lookup tables —enhancing alert fidelity and investigation depth.
- **Enhanced Insider Threat Detection:** The implementation of UEBA and insider threats detection contributed to a 35% increase in detection coverage, surfacing threats that the previous SIEM was unable to identify.
- **Cloud and Cyber Threat Visibility:** RAKBANK experienced a 30% increase in detection coverage for cloud-based and emerging cyber threats, further strengthening its security posture.
- **Improved Accuracy with Fewer False Positives:** Behavioral analytics and machine learning models helped reduce false positives by 15%, allowing analysts to focus on real actionable alerts.
- **Faster Detection and Response Times:** Integrated automation, enriched data, and accelerated queries significantly reduced investigation and containment delays—cutting investigation times from hours to minutes in some workflows. Securonix significantly reduced investigation delays, enabling the security team to identify and respond to threats in a fraction of the time compared to the legacy system.
- **Instant Access to Historical Search & Threat Hunting Data:** The legacy system offered very limited period searchable data. With Securonix and Snowflake, RAKBANK now benefits from a full integration provided up to one year of hot-searchable storage. Historical and threat hunting queries that once took hours can now be completed in minutes., allowing analysts to retrieve and analyze historical logs quickly for faster investigations.
- **Improved Detection Accuracy:** Behavioral analytics and advanced threat models enhanced visibility across the environment and enabled earlier, more accurate detection of complex and evolving threats.
- **Reduced Operational Overhead:** The cloud-native platform eliminated infrastructure management burdens and enabled easier scaling to handle increasing event volume.
- **Stronger Vendor Partnership:** Ongoing support, proactive enablement, and rapid product updates ensured continuous value and alignment with evolving security needs.

# RAKBANK SIEM Efficiency - Before & After




**Consolidation** of multiple SIEM solutions

**Searchable Data** Availability Increased from days to a **year**

**UEBA AND Insider Threat Detection** newly added contributing to **35%** more coverage

**15% Reduction** in False positive violations

**Historical and Hunting** Query time reduce from hours to single digit **minutes**

Threat Hunting Based on **IOCs AND TTPs** is accelerating SOC maturity & a valuable in-built capability of the platform

**30% Increase** in Cloud and Cyber Threat Detection Coverage

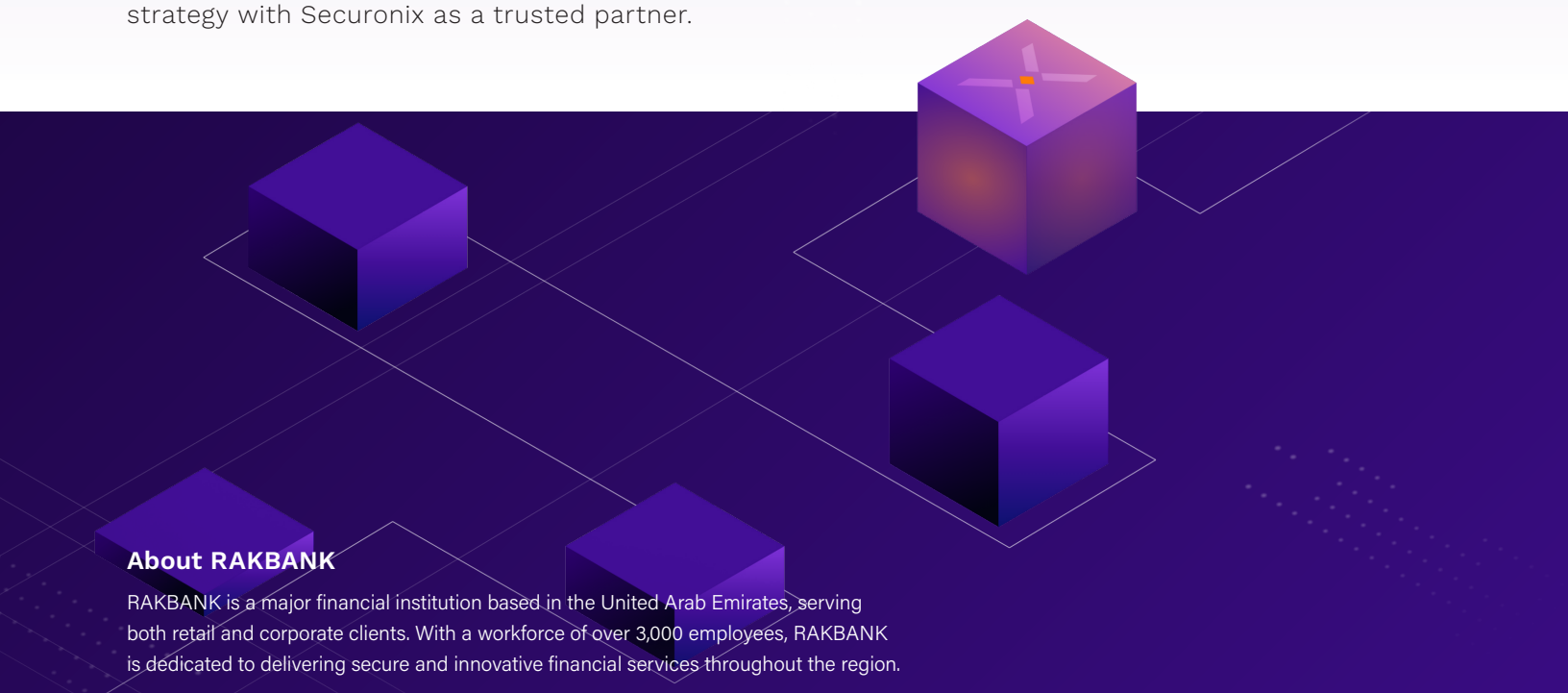
Cloud-native SaaS solutions for seamless **auto-scalability and reduced operational costs** compared to on-premise solutions

## Conclusion:

By transitioning from ArcSight to Securonix, RAKBANK successfully modernized its security operations and laid the foundation for long-term resilience against evolving cyber threats. The unified SIEM and UEBA platform, combined with Snowflake's extended hot storage, is providing the speed, scalability and intelligence needed to stay ahead of attackers.

With measurable improvements including 90% data source coverage, 85% contextual enrichment, a 15% reduction in false positives, and accelerated investigation times, RAKBANK has not only strengthened its cyber defense, but also dramatically improved analyst efficiency.

With faster threat detection, enhanced visibility and proactive vendor support, RAKBANK has not only improved operational efficiency but also empowered its security team to respond to threats with confidence. Looking forward, the bank is well-positioned to continue strengthening its cyber defense strategy with Securonix as a trusted partner.



### About RAKBANK

RAKBANK is a major financial institution based in the United Arab Emirates, serving both retail and corporate clients. With a workforce of over 3,000 employees, RAKBANK is dedicated to delivering secure and innovative financial services throughout the region.

### 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.

securonix