



Industry:
Financial Services

Location:
India, Middle East, Europe and USA

CASE STUDY

Maveric Strengthens Banking Security with Securonix Unified Defense SIEM

Challenge: Maveric Systems is a domain-led banking and financial services technology specialist offering end-to-end transformation across data, AI, and automation. Serving top-tier banking clients across India, the Middle East, Europe, UK, and the US, the company needed a robust security solution to meet the stringent compliance demands of the banking and financial services sector. With multiple fragmented tools and policies, like email security and standalone anti-phishing platforms slowing down threat response, Maveric was keen to invest in a Security Information and Event Management (SIEM) solution to bring all the data together into one single repository. Initially it considered on-premises SIEM but was keen to better optimize budget. After evaluating the market, the company chose Securonix’s Unified Defense SIEM platform engineered for modern threat detection, investigation and response, to bring together its security framework, scale efficiently, and deliver actionable insights without the burden of heavy legacy infrastructure.

Solution: After evaluating several SIEM vendors, Maveric chose Securonix for its cloud-native architecture, flexible deployment, predictable pricing and cultural alignment. By opting for a dedicated, isolated cloud tenant solution, Maveric ensured secure data segregation, which is of utmost importance for its banking clients, while avoiding costly infrastructure such as servers and dual data centers. The Unified Defense SIEM model significantly reduced false alerts, rapidly improved investigation times, while reducing operational overhead. This meant the Maveric team could shift focus from maintenance to strategic improvements.

Benefits

- **Budget optimization:** Maveric managed its budget more efficiently by selecting a cloud-native model over on-premises infrastructure.
- **Rapid deployment:** Fully operational within one month of signing the agreement
- **Scalability:** Ability to handle a larger volume of data
- **Time decreases:** With automated data collection and centralized logging compliance-oriented tasks have been considerably reduced
- **Continuous improvement:** Established a foundation for future AI-driven enhancements and optimization

Results

- **70% reduction** in false positives
- **MTTD/MTTR Reduction:**
 - ◊ Average time from detection to incident report is now 30 minutes
 - ◊ Average time from detection to resolution is now 48 hours
- **Automation:** 50% reduction in time spent on manual data correlation and threat analysis
- **Collaborative support:** Cross-functional Securonix teams, sales, post-sales, marketing, and partner support, worked seamlessly to deliver value



The Challenge

Maveric Systems is a domain-led banking and financial services technology specialist offering end-to-end transformation across data, AI, and automation. Serving top-tier banking clients across India, the Middle East, Europe, the UK, and the US, the company needed a robust security solution to meet the stringent compliance demands of the banking and financial services sector.

In the BFSI sector, information security, cybersecurity, and data privacy are treated seriously with utmost importance. Any breach can trigger intense scrutiny and regulatory action from central authorities like the Saudi Arabian Monetary Agency, often leading to rigorous investigations. Given this environment, banks enforce strict zero-tolerance policies toward cybersecurity incidents.

To meet these expectations, Maveric aligns closely with each banking client's unique security requirements. It ensures secure connectivity, whether via VDI or RDP, from

its delivery centers in India to client-hosted data centers, backed by stringent controls to prevent data leakage, unauthorized transfers, or privacy violations.

Maveric's infrastructure emphasizes encrypted connections, secure gateways, and robust endpoint protection through EDR, anti-malware, threat hunting, and continuous monitoring. The company has evolved from managing fragmented point solutions to building a unified, enterprise-grade security framework.

However, managing disparate platforms, like email security and standalone anti-phishing tools, required manual data aggregation and correlation, which slowed threat detection and response. This prompted Maveric to evaluate SIEM tools to streamline and centralize threat visibility.

Initially, Maveric considered an on-premises SIEM deployment due to the sensitivity of data processed. But quickly realised that a cloud-native approach was more

“Securonix didn't just sell us a solution, they worked closely with us through every step of the journey. From proof of concept to deployment, they aligned with our culture, understood our needs, and helped us build a security foundation that's scalable, cost-effective, and audit-ready. We've had zero escalations and smooth statutory audits ever since and we've managed to reduce costs by 50% on any manual data correlation or threat analysis.”

– **Sunil Peter**
VP & Gopal Head - IT, Maveric Systems



“Maveric’s commitment to security excellence in the BFSI sector made them an ideal partner for us. By leveraging our Unified Defense SIEM, they’ve transformed their operations with agility and precision. We’re proud to support their journey toward continuous improvement and AI-driven threat detection.”

— Ajay Biyani, Vice President - APMEA, Securonix

scalable and manageable from a budget perspective. After assessing multiple vendors, Maveric shortlisted Securonix for its cloud-native architecture, flexible deployment model, predictive pricing and strong cultural and operational alignment.

Following detailed use case evaluations, consultations with banking clients, and successful pilot implementations, Maveric selected Securonix Unified Defense SIEM due to its cloud native architecture and deployed on a dedicated, isolated cloud tenant. Positive reference feedback further reinforced the decision.

Beyond commercial viability, Securonix met Maveric’s highly specific and demanding use cases. On-premises deployment was ruled out due to the complexity and the need to maintain infrastructure such as servers, dual data centers, and the need for 24/7 monitoring. Internal hosting would have required increased headcount and constant uptime management, an operational burden Maveric wanted to avoid and therefore opted for a managed service option delivered by IT services provider, Valuepoint, a Securonix partner.

Before Securonix, Maveric had not implemented a SIEM solution. Instead, it built its security framework gradually, layering controls across endpoints like laptops and mobile devices, and extending protection to network components such as switches, server farms, and firewalls. The company also secured its servers, cloud environments, proxy solutions, and DLP tools. This foundational approach allowed Maveric to mature its security posture before integrating SIEM for centralized visibility and data correlation. The next phase of its journey includes exploring AI-driven enhancements, with agent-based intelligence to accelerate triage detection and response.

Securonix’s Unified Defense SIEM platform stood out for its technical capabilities and its cost-effectiveness compared to other SIEM alternatives. Coverage has been enhanced, as all security solutions and critical server logs are captured in the SIEM and Maveric has recently added secure web gateway logs, which enhance visibility of internet traffic and any threats. Average time from detection to resolution of threats is now down to just

48 hours, with the time from detection to reporting an incident now just 30 minutes. Maveric is now able to handle a large volume of data. Overall, false positives have reduced by 70% for level 1 analysis which enables SOC team analysts to focus on genuine threats and improve overall incident responses.

One of the most notable aspects of the engagement was the cultural alignment between the two organizations. The Securonix team demonstrated a deep understanding of Maveric’s requirements and worked collaboratively from proof of concept through full deployment. Their willingness to support Maveric at every step fostered a strong sense of trust and partnership. Only two companies have stood out for Maveric as true partners: Cisco and Securonix.

While many SIEM vendors offer similar features, it was Securonix’s ability to communicate its breach-ready value powered by AI and help Maveric articulate its use cases that made the difference. The collaborative sales journey built a foundation of mutual respect and understanding.

From an investment standpoint, choosing Securonix eliminated the need for significant CapEx in servers and maintenance. Maveric was fully productive within a month of signing, avoiding the delays and complexity of setting up physical infrastructure.

The implementation was smooth, with cross-functional teams from Securonix, including marketing, sales, post-sales, and partner support, working in sync to deliver results. Since deployment, Maveric has experienced zero escalation calls. Previously, taking backups from individual security applications and storing them in multiple locations was time-consuming and added to workload. With the implementation of Securonix, where all security systems are integrated using Syslog and APIs for real-time log transmission, the process has been significantly streamlined. Statutory audits have been seamless, and the solution has become a trusted part of Maveric’s sales narrative. When banks request detailed security documentation, Maveric simply states: “We use Securonix.”

The cost savings from choosing the Unified Defense SIEM platform over on-premises have been



substantial. Operationally, everything remains within SLA, and the team has shifted its focus from issue resolution to continuous improvement.

Maveric is now exploring ways to further reduce operational time by emphasizing optimization rather than firefighting. Ultimately, the implementation of Securonix has been a strategic success. Maveric's primary concern remains ensuring that client-site assets are properly patched and secure, with no credential leaks or unauthorized access. In this context, features like User and Entity Behavior Analytics (UEBA) have proven invaluable. Maveric has enhanced its ability to protect highly sensitive data, ensure regulatory compliance and provide its banking clients with a more resilient cybersecurity framework.

Key Challenges

- ◆ Fragmented security tools requiring manual correlation
- ◆ High regulatory scrutiny from banking authorities
- ◆ Need for secure, compliant connectivity across geographies
- ◆ Need for robust budget management and optimization
- ◆ Lack of centralized visibility into threats and user behavior

Key Features Utilized

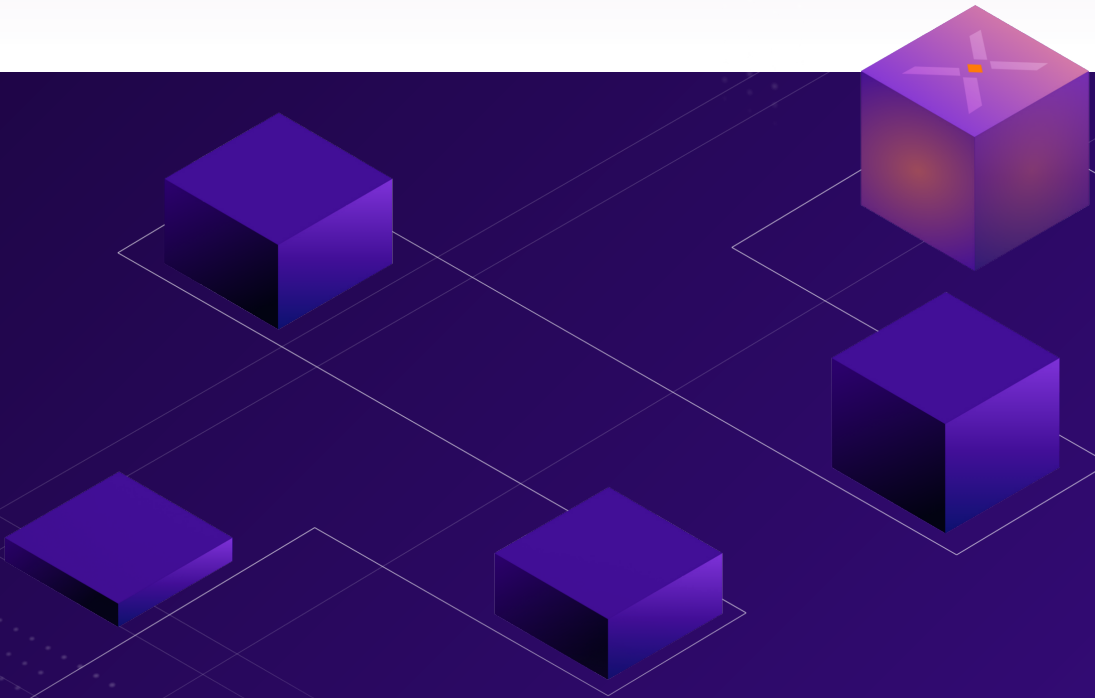
- ◆ Cloud-native SIEM with isolated tenant deployment
- ◆ User and Entity Behavior Analytics (UEBA) for proactive threat detection
- ◆ Curated threat intel, modular AI agents and workflow
- ◆ All security solutions and critical server logs are captured in the SIEM
- ◆ Security systems are integrated using Syslog and APIs for real time log transmission with logs now centrally managed.

Benefits

- ◆ Automation: 50% reduction in time spent on manual correlation
- ◆ Reduction in False Alerts: 70% fewer false positives, allowing for the team to focus on genuine threats
- ◆ Faster Containment: Average time to resolve issues is now down to 48 hours with time from detection to incident report down to 30 minutes.
- ◆ Continuous Improvement: Foundation laid for future AI-driven enhancements.

Conclusion:

By adopting Securonix's Unified Defense SIEM, Maveric has automated its security operations, drastically reduced false positives, improved visibility and detection and response times and aligned with the rigorous compliance standards of its banking clients. The partnership delivered not just technical value but cultural synergy, enabling Maveric to focus on optimization and innovation. With a solid foundation in place, Maveric is now exploring AI-driven security enhancements to further elevate its security posture.



About the Customer

Maveric Systems is a domain-led banking and financial services technology specialist offering end-to-end transformation across data, AI, and automation. With over 25 years of experience and a global footprint, Maveric delivers digital transformation, AI, data, and quality engineering solutions to leading banks across the Middle East, Europe, UK, and the US.

About Securonix

Securonix is leading the transformation of cybersecurity with the industry's first Unified Defense SIEM powered by agentic AI, purpose built to decide and act across the threat lifecycle with a human-in-the-loop philosophy. Built for scale, precision and speed, our cloud-native platform empowers global enterprises to shift from reactive security to proactive autonomous operations. Recognized as a leader in the Gartner® Magic Quadrant™ for SIEM and a Customer's Choice by Gartner Peer Insights™, Securonix is driving the next era of intelligent autonomous security operations. Learn more at www.securonix.com.

securonix