splunk> a CISCO company

CUSTOMER STORY

M Bank Reinforces Digital Banking Security with Proactive Real-Time Visibility

Key Challenges

Due to the lack of real-time visibility across its distributed, multi-platform computing environment, M bank faced difficulties in maintaining a robust security posture to stay ahead of cyber threats.

Key Results

The Splunk SIEM platform offers centralized security visibility, enabling proactive threat detection and response, reducing risks, and strengthening digital resilience and customer confidence.

From zero to hero: unlocking cybersecurity with proactive threat hunting

Mongolia-based M bank is a fully digital neobank aiming to reinvent financial experience with mobile-first services. It is branchless, queueless, and does not even close, allowing customers to manage finances solely through smartphone apps and web platforms from anywhere.

While M bank always makes cybersecurity a top priority, its security operations center (SOC) had a hard time monitoring its highly distributed and heterogeneous computing infrastructure which consisted of more than 100 siloed hosts, on-premises and cloud-based, operation system, and applications logs. Many of those platforms were self-developed with their own programming languages and strategies by different departments, which made log correlation and information sharing impossible.

Anomaly investigation needed to be performed manually, with the SOC team checking logs one by one, system by system. This required a substantial amount of manual effort, and worse still, the SOC was often unaware of critical incidents and where they occurred. To address this, M bank decided to implement a Security Information and Event Management (SIEM) platform to improve security visibility. The bank selected Splunk through its technology partner Unity Data Technology. Splunk Enterprise Security (ES) stood out for its performance and ease of use. Most importantly, it enabled M bank to move from zero to visibility in real time, making proactive threat hunting a reality.

M bank

Industry: Financial Services

Solutions: Security

Products: Splunk Enterprise Security

Capabilities: SIEM / Security Analytics, Unified Security Operations, Security Incident Response, Infrastructure Monitoring and Troubleshooting, Incident Response and Automation, Logs for Observability

Outcomes

- **Reduced** security management time from hours to seconds
- **50%** faster incident detection and response
- **Enhanced** business continuity and digital resilience

From “not knowing” to “seeing the whole picture”

Splunk Enterprise Security, a Leader in the 2025 Gartner Magic Quadrant for SIEM for the eleventh consecutive time, provides M bank with a unified SIEM platform that centralizes data from diverse sources and generates real-time operational visibility. It also offers pre-built dashboards, such as Security Posture, Incident Review, and Threat Activity, helping streamline SOC operations. The team is now able to monitor overall security posture and view key security data and correlations in real time.

Splunk also allows the SOC to develop custom dashboards which are tailored to accommodate special use cases like fraud detection, anomalous access, and infrastructure security monitoring. The team can also package those dashboards into custom Splunk apps for reuse, role-based access, and better lifecycle management.

Splunk Enterprise Security, together with these custom dashboards, offer a single interface for real-time log analysis, security monitoring, and troubleshooting. Splunk’s Predictive Analytics enable early detection of anomalies and threats through behavioral data analysis.

> **Splunk helps us maintain a robust security posture and creates a more proactive and efficient means of defending against cyber threats.**
>
> Nyamdorj Miya, Head of Information Security Department, M bank

“With Splunk, we connect all the pieces, fully understand every security risk, and get to the bottom of it quickly,” says Nyamdorj Miya, Head of Information Security Department of M bank. “From failing to know what happened in our IT environment to having a clear view of our cybersecurity posture, we have for the first time moved from reactive security management to proactive threat hunting.”

“It is not only about feasibility but also efficiency”, Miya emphasizes. “Previously our SOC team had to check every log in every system and application manually to uncover the root cause of incidents, usually spending at least one hour — and sometimes a day. Now, anomaly checking and incident review become seconds of automatic operation on the Splunk Dashboard.” Regarding the exact efficiency gain in threat detection and response, Miya thinks it is case by case. But on average, the bank has experienced a 50 percent decrease in “mean time to detect (MTTD)” and “mean time to respond (MTTR)”.

Smarter operations and enhanced digital resilience

Besides enabling real-time, proactive threat hunting, Splunk also allows M bank to work more efficiently. “Splunk offers us unprecedented simplicity and convenience,” says Miya. Running Splunk is rather straight forward without the need to learn complex search language syntax.

Miya also appreciates that with Splunk, they can manage multiple security needs within a single tool from a single vendor. Splunk’s risk-based alert capability enables the SOC to assign risk scores to assets and users according to their importance, helping the team prioritize security investigations more effectively.

The bank’s management also gained a level of visibility it previously did not have. “By transforming complex security data into actionable insights, Splunk gives our board members new visibility for making more informed decisions. It helps optimize our security strategies to swiftly recover from and even proactively prevent security incidents. This results in stronger digital resilience, further minimizing operational risks and ensuring business continuity,” Miya adds.

Fostering peaceful minds in the digital age

While peace of mind is a critical driver for customer satisfaction and loyalty, Splunk has empowered M bank to translate technology advancement into real customer value.

For example, the big leap the bank has made in security management with Splunk enables it to comply with international regulations such as ISO/IEC 27001, an international standard for information security management systems, and data security standard PCI DSS. “This boosts customer confidence about our ability to safeguard their financial information and sensitive data against evolving cyber threats,” Miya explains.

With Splunk, M bank has become a pioneer in using data-driven security analytics to enhance digital banking. The bank is also exploring the potential of the Splunk AI Toolkit aiming to further “see the unseen” in its data for faster and smarter decision making in future. This aligns with M bank’s mission to enable financial well-being, cultivate healthy financial habits, and reinvent financial experience for customers as a digital bank of the next generation.