splunk> a CISCO company

CUSTOMER STORY

Boost Bank Builds a Secure, Resilient Digital Bank with Unified Security and Observability

Key Challenges

As Malaysia's first homegrown digital bank with a pioneering embedded banking feature, Boost Bank required monitoring high-velocity hybrid cloud transactions, maintaining compliance, audit-ready logging, and building trust in a competitive market.

Key Results

Boost Bank leveraged real-time visibility and advanced analytics to transition to a proactive security posture and observability, accelerating decision-making and enhancing overall customer experience.

Industry: Financial Services

Solutions: Platform, Observability

Products: Splunk Enterprise, Splunk Observability Cloud

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

Building security and compliance into a digital-first bank

Boost Bank was built with a clear mandate to deliver seamless, inclusive financial services to underserved communities while meeting the highest standards of security, resilience, and regulatory compliance.

From day one, Boost Bank recognized that trust is the foundation of digital banking. Operating in a highly regulated environment and serving always-on consumers and small and medium-sized enterprises, it required a technology platform that could provide real-time visibility, proactive threat detection, and audit-ready controls across its hybrid cloud environment.

Moreover, launching a digital bank is fundamentally different from transforming a legacy institution. Boost Bank needed to monitor complex, high-velocity digital transactions across hybrid cloud environments, while detecting and responding to cyber and operational risks in real time. It also needed to meet stringent regulatory expectations including Bank Negara Malaysia's Risk Management in Technology (RMiT) requirements, while ensuring audit-ready logging, traceability, and operational resilience from launch.

Rather than adopting reactive tools after launch, Boost Bank made a deliberate decision to embed security, observability, and resilience upfront.

Outcomes

- **Proactive** security management and observability
- **Enhanced** efficiency through automation
- **Accelerated** decision-making driven by holistic visibility

"We needed a robust platform that integrates data from disparate sources and provides a unified, real-time view of our IT and security operations," says Fozia Amanulla, CEO of Boost Bank. "Equally important, it had to scale with us and support regulatory expectations as customer adoption and ecosystem integrations grow."

To meet these demands, Boost Bank selected Splunk Enterprise and Splunk Observability Cloud as the backbone of its security and observability strategy.

Unified security and observability with Splunk

Ahead of its Alpha launch in 2024, Boost Bank deployed Splunk Enterprise and Splunk Observability Cloud. This early deployment ensures its infrastructure is resilient, secure, and fully observable before opening services to a wider customer base.

Splunk Enterprise, together with Splunk Observability Cloud, enables Boost Bank to achieve centralised, immutable log management across applications, infrastructure, and security systems, with dashboards delivering real-time, full-stack visibility across hybrid environments. Boost Bank is also able to reduce manual monitoring through automated anomaly detection and intelligent alerts, and accelerate investigation and resolution of incidents through advanced analytics and drill-down capabilities.

This unified approach allows Boost Bank to move beyond reactive troubleshooting to proactive operational awareness.

"With Splunk, we transitioned from ad-hoc incident response to structured, proactive monitoring," Fozia explains. "We can identify unusual patterns, system degradation, and potential risks before they impact our customers."

> **With Splunk, we have strengthened our security, improved operational resilience, and built a proactive approach to incident detection and investigation — essential foundations for a digital bank.**
>
> Fozia Amanulla, CEO of Boost Bank

Strong security, faster response, better outcomes

With Splunk, Boost Bank continuously monitors application performance as well as application programming interface behavior, transaction flows, and infrastructure health in real time. This results in faster detection and resolution of security and operational incidents, lesser manual intervention through automation, and improved mean time to detect (MTTD) and mean time to resolve (MTTR), resulting in greater confidence during peak transaction periods.

Beyond security, Splunk provides deep operational insights — from high-traffic services and user behaviour to early indicators of performance bottlenecks.

Regulatory compliance and audit readiness are core to Boost Bank's operating model

Splunk also enables Boost Bank to demonstrate strong governance, transparency, and accountability to support compliance to Bank Negara Malaysia's RMiT security policy.

With Splunk, Boost Bank can easily get immutable, searchable log trails; clear traceability for system access, transactions and events; verifiable data retention and access controls, and audit-ready evidence for regulatory reviews and internal assurance.

This enables Boost Bank to demonstrate strong governance, transparency, and accountability — not only during audits, but as part of everyday operations.

Moreover, for Boost Bank, security and observability are not just risk controls — they directly support customer experience. With holistic visibility that Splunk offers, Boost Bank rapidly detects and resolves issues that could affect customer touchpoints.

This also ensures higher service reliability, reduces disruption to digital journeys, and improve customer trust and retention. "Our improved visibility enhances customer experience, which is our top priority," says Fozia. "That is critical in digital banking, where trust is built through consistency and reliability."

A strategic partnership for long-term growth

Boost Bank values the responsiveness and expertise of the Splunk team, whose support and best-practice guidance help maximize its investment in the platform. Looking ahead, Boost Bank is expanding Splunk dashboards beyond technology teams to include executives and senior management, to enable faster, data-driven decision-making across the organization.

Splunk will continue to play a role in Boost Bank's technology roadmap, supporting digital resilience, strong security posture, and advanced analytics for fraud detection and customer insights.

"Splunk positions us as a forward-thinking institution," Fozia adds. "It supports our growth, strengthens our security foundation, and enables us to meet evolving regulatory and customer expectations with confidence."