splunk>

CASE STUDY

BEA Ensures Global Security Management for Digital Resilience With Splunk

Key Challenges

Lack of visibility into The Bank of East Asia, Limited (BEA)'s distributed environment made it difficult to achieve digital resilience, a key aspect of the bank's fintech initiative. Manual troubleshooting was also time-consuming since each global team had to run its own SIEM.

Key Results

As a first adopter of cloud SIEM in the local banking industry, BEA now has a centralized SIEM internationally with Splunk Cloud Platform, helping the bank gain full network visibility and saving valuable staff time.

BEA東亞銀行

Industry: Financial Services

Solutions: Security, Platform

Technology is best when it brings people together.

A leading Hong Kong-based and listed financial services group for over 100 years, BEA provides a comprehensive range of banking services through more than 130 outlets across the world. The bank actively works to foster technological innovation, launching the **BEA**ST initiative to spark collaboration with local startups and to nurture a vibrant fintech ecosystem in the area.

BEA strives to be on the cutting edge of technology, and had been relying on Splunk Enterprise Security for over a decade to monitor its on-premises infrastructure. When it then sought to standardize security information and event management (SIEM) across all its international branches, BEA partnered with Splunk again. Now with Splunk Cloud Platform, BEA is one of the first banking institutions in Hong Kong to pioneer the use of cloud-based SIEM — gaining full visibility into its environment in the process.

Centralization boosts efficiency and productivity

"An in-country SIEM system is now up and running within a month," says Stephen Leung, head of the information technology and fintech development department at BEA. "It would previously take months just to set up the infrastructure."

With global visibility at its fingertips, BEA's Hong Kong IT team can now pull security data from anywhere in real time. Before, the in-country teams needed to build their own SIEM system for security monitoring and analytics, then ping the Hong Kong headquarters with security-related inquiries. Now the head office easily shares a Splunk dashboard with every subsidiary. This gives each team full visibility into its security posture, keeps up with the dynamic threat landscape and proactively resolves issues before they become major problems.

Outcomes

1
month to set up an in-country SIEM, down from months previously

Full
visibility across distributed international environment

0
manual effort needed for issue investigation and response

"The move to Splunk Cloud Platform allows us to achieve group alignment by aggregating all security-relevant events from either cloud or on-premises sources anywhere in the world," says Leung. "Starting with Hong Kong, we are gradually expanding the use of Splunk Cloud Platform to other offices in Macau, Taiwan, Singapore, the United Kingdom, the United States and other locations in the world."

BEA's own centralization strategy, together with the software-as-a-service approach of Splunk Cloud Platform, helped the bank's IT team increase efficiency and productivity. "Splunk Cloud Platform is easy to deploy without the need for regular maintenance. It is also scalable enough to meet our evolving data needs," says Leung. This not only reduces implementation times and simplifies configurations, but also eliminates manual effort when installing and upgrading an on-premises solution.

> Splunk enables us to stay ahead of the trends shaping digital transformation – not just keep up with them"
>
> Stephen Leung, Head of Information Technology and Fintech Development Department, The Bank of East Asia, Limited

Automation eases the burden and improves agility

They say an ounce of prevention is worth a pound of cure — and that's certainly true in security. Splunk SOAR, which orchestrates and automates incident investigation and response, helps BEA's security analysts address every alert easily and proactively avoid potential issues with real-time situational awareness and timely threat intelligence. They are also freed up from repetitive, manual workflows so they can focus on more strategic initiatives and mission-critical objectives.

"On one hand, the actionable insights generated with Splunk help us make smarter security-related decisions. On the other hand, they allow us to maintain a stable operation across geographical boundaries and around the clock," says Leung. On a practical level, Splunk helps BEA become more resilient in three ways: troubleshooting in real time, evolving with the threat environment and staying agile in the cloud environment — all creating better banking experiences for BEA's customers.

Pushing forward the frontiers of digital resilience

Through the years, BEA has been dedicated to driving fintech innovation. Splunk has helped the company set a good example, becoming one of the first financial institutions in Hong Kong to take its SIEM to the cloud.

"Digital resilience is an integral part of our fintech strategy," says Leung. "We strive to strengthen cybersecurity while fostering an innovative culture to thrive in the ever-changing digital world. With Splunk, we manage to enhance automation for effective monitoring and patch deployment, while continuing to optimize security orchestration — streamlining threat detection and responses."

Looking forward, Splunk Cloud Platform also offers BEA the flexibility to drive future growth. Because Splunk's SIEM solution is built with cloud-native technologies in mind, it is constantly kept up to date with the latest features and can scale on demand to match BEA's usage patterns. For BEA, the journey has just begun — and Splunk will continue supporting them every step of the way.

24-127487-Splunk-APAC BEA-CS-SS-106-Follow up-101