

HKIX Proactively Monitors Its Network Management System to Achieve Compliance

Key Challenges

Reactive troubleshooting from disparate devices consumed time and created efficiency challenges for HKIX.

Key Results

Thanks to Splunk Cloud, laborious issue management has been replaced with real-time visualizations, proactive information security and holistic system visibility for better operations and ISO 27001 compliance.



Industry: Communications

Solutions: Security

In today's world, proactive security is critical to success.

That's why Hong Kong Internet eXchange (HKIX) — one of Asia-Pacific's largest internet exchange points supporting fast and easy interconnections among local and international networks — prioritizes security incident investigation.

"When we were preparing to get ISO 27001 certified, consultants and auditors suggested that we bring in a security information and event management (SIEM) tool for security management," says Kenneth Chan, chief operations officer of HKIX. Impressed by its reputation for turning data into action, Chan chose Splunk as the best solution for building predictive and preventative analytics to ensure secure operation of the company's network management system, which is responsible for hosting its management tools.

Proactive incident response reduces team's burden

With Splunk, the HKIX team now proactively investigates incidents. Splunk Cloud analyzes system behaviors and monitors logs in real time to track anomalous trends, offering instant visibility into system operations and stopping issues before they turn into outages or crises.

Chan and his team no longer need to reactively write scripts to sift through gigabytes of logs or painstakingly search keywords and match records just to identify vulnerabilities and potential risks in its network management system. "We now seize the initiative to avoid problems," Chan says. Splunk Security Cloud's rule-based approach to flagging anomalous behaviors also helps HKIX address compliance needs, transforming security event investigation into a hassle-free operation.

With its SaaS operating model, Splunk Cloud has freed up time for the HKIX team while eliminating the challenges that accompany on-premises products — beginning with a seamless rollout. "We received the portal within a week after purchase," says Chan. "After we logged into the system, everything was up and running smoothly with a simple data onboarding workflow." Having offloaded everything from system monitoring and troubleshooting to maintenance and updates, the HKIX team can now focus more on high-value tasks.

Turning Data Into Outcomes

- Accelerated MTTI and MTTR from hours to minutes
- Gained instant access to real-time insights at the team's fingertips
- Moved from reactive to proactive information security management

From hours of calculations to real-time analytics

Since turning to Splunk Cloud, HKIX visualizes its network management system in a unified view. “Previously my team had to bury themselves in program scripts for hours to generate charts and graphs to complete the system status report,” Chan says. But now, pressing a single button instantaneously yields a wealth of metrics about the company’s security environment on the highly interactive, graphic-rich Splunk dashboard, which also gives the team flexibility to customize how visualizations are displayed.

While the HKIX network management environment includes logs from many different servers, end points, firewalls and Windows and Linux operating systems, the Splunk platform centrally manages all logs on a single pane of glass. This simplified method of collecting, searching and analyzing session logs allows the team to enhance the company’s security environment.

With Splunk, HKIX has significantly improved its security management, reducing mean time to identify (MTTI) and mean time to respond (MTTR) from hours to minutes. Moreover, Splunk Cloud allows users to act on data with the tap of a finger while also giving the HKIX team access to a vast repository of best practices and insightful use cases.

“We are particularly excited about the good amount of security analytics content we can easily download from the Splunk knowledge base, which broadens our horizon on information security,” Chan says. “What’s more, the SaaS model of Splunk Cloud not only brings a whole new level of data protection in the form of geographic redundancy and off-site disaster recovery, but also minimizes our effort in managing the hardware platform, which empowers us to run multiple data centers in a cost-effective way.”

Scaling to manage growth and fuel cloud transformation

After using Splunk Cloud, HKIX successfully complied with the requirements outlined in ISO 27001, making it one of the earliest security-aware internet exchange organizations to achieve this information security management standard. HKIX also plans to scale Splunk Cloud to cover more data and further optimize its information security lifecycle. “At the end of the day, ISO is all about driving continuous improvement,” says Chan. “Splunk is helping us constantly improve what we do.”

Meanwhile HKIX is supporting nearly 340 participants from different sectors — including local and regional internet service providers, content providers, data centers and anti-DDos providers. “Our operation is growing day by day with network traffic increasing about 30% per year,” Chan says. With Splunk, HKIX is well positioned to seamlessly manage the growth in logs, systems and security tools, allowing the organization to continue thriving throughout its cloud journey.



We need convenience, precision and efficiency to succeed, and the Splunk solution has lived up to our expectations.”

Kenneth Chan, Chief Operations Officer, HKIX

[Download Splunk for free](#) or get started with the [free cloud trial](#). Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.



Learn more: www.splunk.com/asksales

www.splunk.com