

ACE Meets Security Standard and Cuts Costs 10% While Boosting Performance

Key Challenges

Before Splunk, ACE couldn't centrally correlate security data from multiple devices, thus reducing multicloud visibility, slowing event response and driving up labor costs.

Key Results

Splunk helped ACE enhance security monitoring with faster threat hunting and real-time event response, cut costs by 10 percent, simplify system maintenance, raise efficiency and secure user assets.



Industry: Financial Services

Solutions: Security, Platform

A lot can go wrong when you don't have the right security platform.

Founded in 2018, ACE Exchange is Taiwan's first legal cryptocurrency exchange that lets users buy and sell Bitcoin (BTC), Ethereum (ETH) and Tether (USDT) with New Taiwan Dollar. It offers the largest number of financial tools to date, aiming to facilitate the migration from DeFi to CeFi, and the most comprehensive range of cross-chain services. To support its extensive blockchain transaction and incubation ecosystem, ACE needed an effective security monitoring platform. The platform needed to fuel the steady growth of ACE while protecting the security of user assets and ensuring legal compliance and business continuity.

However, the open-source analytics platform that ACE used wasn't up to par. It couldn't centralize data, correlate logs for detecting anomalous transactions or oversee resource usage and allocation across its growing multicloud environment. This meant ACE's security team had to log into different consoles just to investigate a single issue, which delayed MTTD while making it tough to predict advanced threats. The platform was also difficult to maintain, requiring human intervention for data onboarding and dashboard customization, putting pressure on the team and limiting hardware functionality.

For granular visibility into its complex environment, ACE turned to Splunk to make its security posture stronger, threat hunting more robust and operations more efficient.

Centralized security monitoring, greater productivity

"With Splunk, we finally got the security analytics platform of our dreams," says Fngi Hsu, chief information security officer of ACE Exchange. Splunk was perfect for managing the complexity of the organization's multicloud environment, automatically collecting log data from all public cloud computing platforms ACE uses — including Google Cloud, Amazon Web Services and Microsoft Azure — then generating a complete picture of the company's security posture for quicker threat hunting, real-time

Outcomes

70%
less human
intervention required
for security monitoring

10%
cost savings from idle
cloud resources

24/7
availability, thanks to
real-time visibility
into operations

event response and more reliable monitoring. ACE's security teams also benefited from Splunk's intuitive dashboards, relying on them to predict, detect and respond to different types of threats.

Adopting Splunk has massively reduced security teams' workloads. "The simple, easy-to-learn Splunk Search Processing Language not only solves the slow search problem of the old platform, but also enables us to flexibly adjust the dashboard and alert settings to meet our security needs, especially the new 'A.8.16 Monitoring Activities' control item of the ISO27001:2022 practice," Hsu explains. "Credit also goes to the Splunk Mobile app, which gives us access to dashboards, reports and alerts from a single interface on the go. Instead of working night shifts in the office, the team can now stay connected with the Splunk platform anytime, anywhere."

ACE has also used Splunk to develop machine learning models that predict cyber threats and alert on security incidents. This reduces repetitive, manual tasks, meaning that jobs that once took seven days to complete now only take two. These productivity savings allow team members to focus on what matters most while enabling ACE to reallocate its resources for other strategic security initiatives.

Maximizing ROI with real-time resource management

For ACE, greater visibility into its multicloud operations has also improved resource management. After using Splunk, ACE gained greater insights into spending across its cloud services, identifying unnecessary services and reallocating resources in real time to boost overall ROI. According to Hsu, ACE has cut costs by more than 10% through identifying and conserving idle cloud resources.

Across the board, ACE's teams have found Splunk easy to use. "There are many out-of-the-box apps from Splunk supporting different brands of products in both cloud and on-premises deployments, and they streamline our data onboarding and integration," Hsu says. "Ongoing maintenance is as simple as upgrading the apps, while a single source of truth can extend to different use cases — such as information security, IT operation and business analysis — without installing multiple monitoring software."

The journey continues

While Splunk has advanced cybersecurity for ACE, it's just the beginning. "In the future, we will certainly go further and achieve more with Splunk," Hsu predicts. "The next step is to increase the level of security automation." To achieve this, ACE is looking to Splunk SOAR to further improve efficiency for its security operations and accelerate incident detection and recovery. ACE also has plans to use Splunk to detect fraud and reduce the number of unusual internal transactions, helping ACE stay resilient while supporting new avenues for the trading of the future.



Splunk optimizes our hybrid multicloud journey and maximizes ROI for us."

Fngi Hsu, Chief Information Security Officer, ACE Exchange

[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