

Seven Bank Fights Financial Crimes With Real-Time Log Correlation and Analytics



Executive summary

Seven Bank, Ltd., a Japanese bank offering a variety of cutting-edge financial services to a broad base of customers, opens approximately 17,000 new user accounts monthly and operates more than 24,000 automatic teller machines in Japan. With a growing focus on online transactions, the company has stringent security and risk management requirements. Since deploying Splunk Cloud, Seven Bank has seen benefits including:

- Integrated real-time visibility into anomalies and threats
- Streamlined operations and fraud analysis
- Improved risk assessment and management

Why Splunk

Seven Bank had been striving to mitigate financial fraud and unauthorized use of bank accounts by using siloed, manual solutions to monitor cash transactions and internet access. Although this process was able to safeguard individual points of operation, the lack of log correlation across organizational barriers restricted the bank's capability in capturing cross section data, responding to anomalies quickly, protecting its overall business and making effective business decisions. The bank also spent a considerable amount of time manually operating the applications.

Facing the challenge of fast business growth and an increasing number of user accounts, Seven Bank needed an effective approach to unauthorized access control and a flexible platform for operational analysis. After evaluating a few solutions, its financial crime countermeasures department decided to adopt Splunk Cloud. Splunk's market reputation and comprehensive product training meet the bank's needs. The bank is also impressed by the rich array of Splunk apps available that enable the company to bring in new functions whenever needed.

Detecting anomalies and preventing crimes in real time

Splunk Cloud enables Seven Bank to integrate a broad range of data from multiple sources including internet banking access logs, cash transaction information, account information, phone call records and services data onto a central platform, and automatically collect, search,

Industry

- Financial Services

Splunk Use Cases

- Security
- Fraud

Challenges

- Needed advanced analytics and log correlation to identify anomalies
- Manual online fraud tracking was time-consuming
- Inefficiency in managing siloed applications and inflexibility in capturing cross-section data

Business Impact

- Enhanced crime prevention, thanks to the integrated real-time visibility into anomalies and threats
- Improved efficiency and staff morale due to streamlined operations and fraud analysis
- Business automation with improved risk assessment and management

Data Sources

- Internet banking access logs
- Bank account and cash transaction data
- Unauthorized access detection data
- Call detail records

Splunk Products

- Splunk Cloud

monitor, report and analyze all real-time and historical data using a cloud service. It then generates useful insights for spotting customer churn and patterns that indicate severe business impacts, as well as signs of unauthorized access through behavioral analysis, and notifies administrators of potential risks through a score-based alert system. This predictive analysis helps prevent unauthorized use of bank accounts, illegal money transfers and other financial crimes.

Seven Bank can also detect system outages before they occur and proactively keep its services up and running to meet business needs. Gigabytes of data in various formats are processed and correlated every day to produce operational insights for the bank to maintain a safe and healthy operation.

Boosting efficiency by eliminating human intervention

Splunk Cloud offers a single point of access and a holistic view across the organization that can support a wide range of analytics. More importantly, it standardizes and automates analysis tasks previously handled manually. The streamlined operation allows Seven Bank to keep pace with its business growth and retain talent while facilitating workflows and cutting human resources training time by one-half.

Moreover, the intuitive Splunk dashboard offers a painless operating experience by visualizing all information related to the detected account on a single monitor. Administrators can also predefine rules to track incidents and potential issues, perform analytics on historical and new real-time data, and derive meaningful, actionable insights to speed up decision-making processes.

“The Splunk analytics solution not only helps us master financial crime challenges and facilitate our operations, but also acts as a major catalyst for our business growth and success, keeping us in pace with the ever-changing business world.”

Takanori Yasuda
Seven Bank, Ltd.

Gone are the days when the system operators continually kept an eye on the monitor to trace anomalous behaviors and predict failures. Now, whenever unusual activities and events are detected, the operator will immediately receive an email alert. The improved consistency removes stresses from and boosts the staff morale. There is also no need for the bank to increase staff despite the increasing workload.

Improved risk management opens up new opportunities for business automation

With Splunk Cloud in place, Seven Bank can eliminate time-consuming manual procedures and stay focused on the core business. It can also analyze a larger variety of external data in a broader context and greater depth, generating unprecedented real-time insights and perspectives for better business planning and crime prevention.

In the future, Seven Bank plans to use the new risk scoring-based alert system to automate other business processes, such as freezing illegal accounts and blocking abnormal money transfers. It is also considering using the Splunk solution to detect hardware failure and track inventory while supporting other possible areas of business operations.

[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