

Japan's Online Banking Pioneer Gains Real-Time Visibility Into Cybersecurity Risks



Executive summary

The Japan Net Bank, Ltd. (JNB), Japan's first internet-only bank, offers convenient, around-the-clock online banking services. To follow the common practice in Japan's financial services industry, JNB has joined the Financial Services Information Sharing and Analysis Center Japan (Financials ISAC Japan), a global financial industry resource for cyber and physical threat intelligence analysis and sharing. Since adopting Splunk Enterprise to derive real-time, actionable cybersecurity intelligence from operational data, JNB has seen the following benefits:

- Cyberattack management decreased from hours to minutes
- Prevention of illegal money transfers
- Identified opportunities for new security measures

Why Splunk

Unlike bricks-and-mortar banks, JNB runs a unique banking model that is conducted entirely online. Therefore, cybersecurity is absolutely critical for its business. Previously, the bank's IT Supervision Department found it challenging to manage security risks. The department spent many hours digging out firewall and proxy logs from the office automation environment and analyzing web access logs to spot unauthorized accesses. The bank also required high accuracy in monitoring transaction logs to safeguard against spoofing and illegal fund transfers, and it needed to share information with Financials ISAC Japan.

JNB decided to establish an intelligent platform to collect, analyze and deliver real-time insights from machine-generated big data to improve its cyber defense strategies. Among all of the alternatives considered, JNB found that Splunk Enterprise was the best option.

Hours of manual processing reduced to minutes

Splunk Enterprise makes it easy to capture, analyze and act upon the untapped value of the big data generated from JNB's daily operations. Previously taking one-half day or a full day to complete a search or security investigation, the bank now has real-time access to data and

Industry

- Financial services

Splunk Use Cases

- Security and Fraud

Challenges

- Inefficient log management in the office automation environment
- Labor-intensive and time-consuming risk management processes
- Ineffective analysis of web access logs in detecting unauthorized accesses

Business Impact

- Accelerated analysis of cyberattacks from one-half to one day to a few minutes
- Prevented illegal money transfers
- Gained new opportunities for enhancing cybersecurity

Data Sources

- In-house office automation environment
 - Firewall
 - Access logs
 - Next-generation firewall
 - Filtering logs
 - Proxy
- Internet banking
 - Customer transaction logs
 - Request header
 - Response header
 - Geographical IP address information
 - Response time
 - WAF detection information

Splunk Products

- Splunk Enterprise

completing an investigation is a multi-minute exercise. Captured logs can be searched on demand with only a few keyboard clicks, and with the cybersecurity information shared from Financials ISAC Japan, IT supervisors can easily investigate every case to spot security vulnerabilities in the online banking system before they adversely impact the bottom line.

Splunk Enterprise provides an analytics-driven security solution that enables real-time security monitoring, advanced threat detection, forensics and incident management. It enables JNB to access operational and security intelligence in different views to accommodate specific needs. JNB can easily create consolidated reports and dashboards to view enterprise-wide security risk in a single pane of glass.

Prevention of illegal money transfers

With the Splunk analytics platform in place, JNB was able to implement a new cybersecurity measure that provides all online bank users with a free-of-charge, one-time password. In addition, Splunk Enterprise automatically sends real-time alert emails to JNB's Computer Security Incident Response Team upon detection of any signs of phishing attacks. This has improved the team's capabilities and enabled them to successfully identify more than 20 spoof websites in a single year, achieving a new level of security. JNB has also set up the Security Operations Center to go the extra mile in combatting cyberattacks.

“Visibility is critical to boosting cybersecurity. Splunk Enterprise eases our life in managing various types of logs and reports and allows us to acquire different viewpoints of our online banking business. It has created a brand-new chapter in the cybersecurity history of JNB.”

Kenji Ninomiya

Senior Manager, IT Planning Department / JNB-CSIRT,
The Japan Net Bank, Ltd.

“The Splunk solution enables JNB to lead the way in cybersecurity and become a role model in Japan's banking industry.”

Kaz Ozawa

Assistant Manager, IT Planning Department, Cyber Security Office / JNB-CSIRT, The Japan Net Bank, Ltd.

Opening up new cybersecurity possibilities

“The Splunk solution enables JNB to lead the way in cybersecurity and become a role model in Japan's banking industry,” says Kaz Ozawa, assistant manager, IT Planning Department, Cyber Security Office / JNB-CSIRT, The Japan Net Bank, Ltd. The company is also planning to extend powerful Splunk analytics to a broader range of applications, including the detection of unauthorized accounts and financial crimes, monitoring of illegal deposits and withdrawals, as well as machine learning-based detection of illegal money transfers.

“Visibility is critical to boosting cybersecurity,” says Kenji Ninomiya, senior manager, IT Planning Department / JNB-CSIRT, The Japan Net Bank, Ltd. “Splunk Enterprise eases our life in managing various types of logs and reports and allows us to acquire different viewpoints of our online banking business. It has created a brand-new chapter in the cybersecurity history of JNB.”

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