NXLog

NXLOG HELPS LA BANQUE POSTALE TO ENABLE AUTONOMOUS LOG COLLECTION AND MEET NATIONAL REGULATIONS.

CUSTOMER CASE STUDY

NXLOG HELPS LA BANQUE POSTALE TO ENABLE AUTONOMOUS LOG COLLECTION AND MEET NATIONAL REGULATIONS.

A multi-partner and international bancassurance group, serving 64 million customers in 19 countries across Europe and Latin America, and with net banking income €9,516m as of 2022.

It was established as a universal bank in 2006, as a subsidiary of the national postal service of France (La Poste). It now supports over 20 million customers with a full range of financial products and services, via a unique network of local branches (17,000 points of contact, including 7,600 post offices, community branches and relay shops).

RELATED INDUSTRIES

- Retail banking
- Life and Non-life insurance
- Consumer finance
- Digital banking and loans

BUSINESS DEMAND

Centralize log collection to improve security posture and meet various domestic and international regulations.

CHALLENGE

Establish a unified log collection pipeline to gather events from various sources, including Windows, Linux, AIX, and network appliances. Overcome native Splunk forwarder limitations.

SOLUTIONS

- NXLog Enterprise Edition
- NXLog Agent Manager

BUSINESS RESULTS

- Built a unified and autonomous log collection pipeline
- Simplified on-going event source integration
- Improved security posture with broader log collection coverage
- Achieved compliance goals

BACKGROUND

Finance institutions, such as banks, insurance, and investment firms operate with complex IT systems that are constantly being enhanced and updated. With the increase in digital transactions and remote access, these organizations face a heightened risk of cyber threats and the potential for substantial financial losses.

It is crucial for them to adhere to different cybersecurity regulations (**GDPR, PCI DSS, SOX, GLBA,** etc.) and implement rigorous defense-in-depth strategies to safeguard their systems and data from internal and external threats. This includes continuous log collection and ongoing threat analysis as recommended by industry standards - like the **ISO** and **NIST** frameworks - and national regulations. By integrating security best practices into their operations, financial institutions can better protect themselves against potential cyberattacks and preserve the trust and confidence of their customers.

As a critical infrastructure operator, La Banque Postale is subject to security requirements, imposed by various domestic and international regulations, that aim to ensure every critical system is resilient. Log collection and centralization is a key requirement of this compliance, enabling La Banque Postale's security team to detect, prevent, and remediate threats across their vital banking systems in time.

CHALLENGES & SOLUTION

The main goal of the project was to collect and centralize logs from all data center systems into a Splunk data store for operational and threat analysis. The first stage involved migration from native Splunk forwarders to NXLog Enterprise Edition-powered collectors designed to ingest logs from various computer endpoints (Windows, Linux, and AIX).

(!) As a dedicated log collection tool NXLog has a lot of advantages when compared to native Splunk forwarders, including ingestion speed, integration abilities, powerful filtration capabilities, and more.

One of the reasons for the migration was a helpful embedded log rotation feature of NXLog Enterprise Edition that allows effective log file management without having to leverage a system's log rotation functionality. Migration to NXLog Enterprise Edition helped to avoid different limitations and allowed the team to be autonomous and effective with the ongoing integration of log sources.

To stay compliant with multiple regulations, it is required to collect logs not only from computer endpoints, but also from key network, security, and storage services across a data center. So, the next challenge was to collect logs from various appliances, including those from Bluecoat, Cisco, CyberArk, F5, IBM, Hitachi, and others. These services and appliances often provide a way to transmit events by syslog; thus, to accumulate the logs, it was decided to set up a cluster of NXLog Enterprise Edition collectors with load balancing.

(!) NXLog Enterprise Edition allows different configurations for high availability, including fail-over and load balancing.

After being centrally collected, events are filtrated, processed, and forwarded from the NXLog Enterprise Edition cluster to an Apache Kafka broker cluster, and then on to a Splunk SIEM instance for security engineers to monitor, detect, and remediate threats.
As a result of this project, a robust and autonomous log collection pipeline - powered by NXLog - was designed and successfully implemented. It complies with government regulations and allows La Bank Postale to integrate various data sources quickly and proactively respond to emerging threats based on the events collected.

> *"We really appreciate versatility of NXLog. It's ultimately lightweight in regard to CPU/RAM consumption, while still extremely powerful to process a solid event stream flawlessly. Also, as NXLog provides a lot of integration options, it allows us to collect a wide variety of assets' logs and be flexible with log collection architecture"*
>
> ***- Yann Chanel, Systems and Networks***

SOLUTIONS

NXLog Enterprise Edition

NXLog Manager

NXLog Add-Ons

REQUEST A FREE TRIAL

*Visit our **website** to learn more about our products or get in touch with one of our dedicated representatives. should just say 'get in touch'.*