NXLog

Enhancing Log Management and Security for a Major U.S. Bank

Enhancing Log Management and Security for a Major U.S. Bank

CUSTOMER PROFILE

One of the Top 10 largest banks in the United States, providing a comprehensive range of retail, commercial, and investment banking services.

RELATED INDUSTRIES

Banking & Financial Services

BUSINESS DEMANDS

- Regulatory compliance
- Security posture improvement

CHALLENGES

- Heterogeneous infrastructure (Windows, Linux, macOS)
- Diversity of log types
- Log collection performance
- Integration with SIEM and long-term storages

SOLUTION

NXLog Platform

BUSINESS RESULTS

The creation of a unified log collection pipeline, built across the infrastructure to ensure both efficient security analysis and regulatory compliance.

BACKGROUND

One of the USA's largest banks, the client offers its customers a full range of retail, commercial, and investment banking services. The institution handles millions of customer accounts and facilitates billions of dollars in transactions every single day. With a vast and complex IT infrastructure spread across numerous data centers and cloud environments, maintaining compliance, protecting customer data, and detecting threats in real-time are critical to its operations. Furthermore, the bank's IT environment comprises thousands of devices, requiring a robust and efficient log management solution.

CHALLENGES

Managing logs across such an IT environment presented a series of significant challenges for the client:

• Diverse Infrastructure

The IT environment included around 500,000 log sources across a mix of operating systems, such as Windows, Amazon Linux, Red Hat (8 & 9), Ubuntu (20.04 / 22.04), and macOS. Aggregating and standardizing logs from these heterogeneous platforms was a daunting task.

• Diversity of log types

To ensure complete visibility, the client needed to collect different log types – including application (plain text) logs, Windows Event Logs, and Linux system logs.

• Performance

The client's existing log management tools created bottlenecks, generating excessive noise in its Security Information and Event Management (SIEM) system and reducing performance across critical endpoints.

• Regulatory compliance

In order to adhere to strict financial regulations, the bank needed a reliable log collection solution that could meet stringent audit and reporting requirements.

• SIEM integration

The client used Elastic SIEM for centralized monitoring and analytics and needed a seamless solution for forwarding logs to the SIEM while also storing them locally for redundancy and auditing.

SOLUTION

To tackle these multifaceted challenges, the bank chose NXLog to devise a solution for handling its log collection and management needs.

NXLog agents were deployed across a variety of systems to collect data from application log files, Windows Event Logs, and Linux system logs. This agent-based approach ensured reliable log capture from all 500,000 data sources – providing full visibility into the bank's infrastructure.

With native support for a variety of operating systems – including Microsoft Windows, Linux (Red Hat, Ubuntu in the case) and macOS – NXLog agents provided a unified log collection solution that worked seamlessly across the bank's entire IT infrastructure.

The lightweight design and configurability of NXLog agents minimized the performance impact on critical endpoints in comparison to the client's previous solution. Furthermore, NXLog agent's ability to pre-filter logs reduced the amount of data sent to the SIEM, optimizing resource usage and SIEM performance.

The NXLog agents were also seamlessly integrated with Elastic SIEM using a native NXLog HTTP output module. This enabled real-time threat detection and analytics while facilitating logs routing to local log storage for the sake of enhanced redundancy and compliance audits.

DEPLOYMENT

Phase 1

Installation of NXLog agents on Windows, Linux, and macOS endpoints to enable comprehensive security and application logs collection.

Phase 2

Configuration of log forwarding to Elastic SIEM via the HTTP output module, enabling real-time analytics and threat detection.

Phase 3

Configuration of logs routing to a local storage to ensure data redundancy in case of SIEM outages while supporting audit requirements.

Phase 4

Testing and performance fine-tuning to confirm that all logs were efficiently captured, stored, and analyzed – with minimal resource consumption.

RESULTS

Following the deployment of NXLog, the client has seen significant improvements in its log management capabilities.

In capturing logs from all 500,000 sources, the bank has achieved full visibility across its diverse infrastructure, while integration with Elastic SIEM has improved threat detection and incident response – enabling the Security Operations Center (SOC) to swiftly address potential threats. NXLog has also helped to reduce the volume of data forwarded to the Elastic SIEM, alleviating system bottlenecks and preventing SOC downtime.

Moreover, by enabling robust local log retention, NXLog agents have given the client enhanced event traceability and audibility to ensure compliance with stringent financial regulations.

By implementing NXLog, the bank has transformed its log management approach, achieving a unified, scalable, and compliant solution that supports real-time security monitoring and regulatory requirements. With full visibility into its infrastructure and optimized system performance, the client is well-equipped to handle future business challenges while maintaining a robust security posture.

This successful deployment underscores the value of NXLog as a versatile, high-performance log collection solution for large-scale and heterogeneous environments.

For more information on NXLog visit our website, checkout our integrations page or schedule a meeting with one of our representatives.

Request a free trial for our solutions:
NXLog Enterprise Edition
NXLog Manager
NXLog Add-Ons