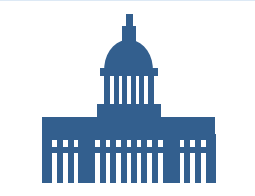
NXLog

TOP-TIER PUBLIC SECTOR CHOSE NXLOG FOR BETTER SECURITY OPERATIONS

TOP-TIER PUBLIC SECTOR CHOSE NXLOG FOR BETTER SECURITY OPERATIONS



CUSTOMER PROFILE

Government institution for the Top 10 largest economy in the World.

RELATED INDUSTRIES

- Federal government
- Public sector

BUSINESS DEMAND

Improve security posture of internal infrastructure, SOC performance, and reliability.

CHALLENGE

Establish unified log collection pipeline to get events from various network sources. Implement pre-filtering of events on agents and forwarders to decrease EPS volume.

SOLUTIONS

- NXLog Enterprise Edition
- NXLog Agent Manager

BUSINESS RESULTS

- Unified log collection pipeline
- Security tools performance improved
- Security posture improved

BACKGROUND

The public sector and various federal agencies are responsible for a wide range of sensitive data, varying from personal to classified information. The public sector remains at the top of the most frequently attacked industries, along with healthcare and education. According to recent security research, it was ranked second with an average of 1745 attacks weekly during H1 2023.

Government institutions have been a high-value target for motivated attackers for many years, as any breach opens a door for a threat actor into the national security data lake. Potentially, it also allows access to many third-party contractors and organizations employed by the government to support its operation. It's worth mentioning that public government resources are trusted by users and have a wide audience, so a breach can also be leveraged to distribute malware to many instantly.

Protecting government systems is a challenging task in itself. While having a complex infrastructure in place and housing large volumes of sensitive data, public organizations are less funded compared to commercial sectors, so they have small security teams and employ a mixture of outdated software, posing a challenge for modern security tools to be integrated with.

PROJECT & SOLUTION

Since the start of the IT era, logs have been at the core of cybersecurity operations. It helps the security team detect and remediate threats, meet regulatory compliance, and discover application errors and other security-related issues.

With the increased complexity of cyber defense strategy, the following issues and challenges have been identified by the security team regarding the log collection agenda:

- Multi-vendor environments expose incompatible logging mechanisms
- Boosted volumes of log data make security tools slow and inefficient
- Hybrid infrastructure (cloud/on-prem) requires a new approach to log collection

All this yielded the following business requirements for a new log collection system, including:

- Support for various input sources (text files, Windows event logs, DNS, SQL, etc.)
- Support for various output formats required to ingest data into security tools (syslog, json, etc.)
- Support for multiple log destinations as needed to feed each of the security services
- Raw data processing capabilities (e.g., logs re-normalization, formatting, filtration, etc.)
- Centralized management capability to achieve consistent configurations across infrastructure
- Centralized monitoring for log collection health checks

Based on the requirements, the security team did a PoC (proof of concept) round with several leading vendors from the log collection industry. NXLog stood out as the only product able to fulfill all the business demands.

"In our environment, several cybersecurity areas would not be functioning without logging strategy and architecture: Forensics, Monitoring, Threat Hunting, Investigations, and Incident Response. Each of these areas employs distinct tools which bring unique requirements when it comes to log collection."

- Senior IT Security Analyst, The Customer's Office of the Chief Technology Officer

"Now, with so many data sources, it's difficult to know if one or more data sourcesare having issues."

– Senior IT Security Analyst continues –

"For instance if data is not being sent/ received due to changes introduced by operation teams."

"Some of the most notable features of NXLog for us are support for MS DNS (ETL trace), ability to integrate via uncommon channels (like Kafka and RabbitMQ),"

– Senior IT Security Analyst concludes –

"and powerful logs processing that helps to reduce logs traffic and save costs on security tools, licensed by EPS."

SOLUTIONS

NXLog Enterprise Edition

NXLog Manager

NXLog Add-Ons

REQUEST A FREE TRIAL

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