NXLog

NXLOG HELPS TOP-3 AUTOMOTIVE FINANCIAL SERVICES COMPANY TO STRENGTHEN CYBERSECURITY AND ACHIEVE COMPLIANCE

CUSTOMER CASE STUDY

NXLOG HELPS TOP-3 AUTOMOTIVE FINANCIAL SERVICES COMPANY TO STRENGTHEN CYBERSECURITY AND ACHIEVE COMPLIANCE

FINANCIAL SERVICES COMPANY —

a business division of world's Top-3 tier automotive group of companies with thousands employees working at dozens of branches across the globe.

RELATED INDUSTRIES

- Automotive Financial and Services
- Direct Banking
- Financing, Leasing & Insurance
- Fleet Management
- Payment and Rental

BUSINESS DEMAND

Increase infrastructure protection, Meet SEC, SOX, PCI, GLBA compliance, national and corporate regulations for log retention & analysis

CHALLENGE

Establish a secured and time/cost effective log collection pipeline for events retention and ongoing threat analysis.

SOLUTIONS

- NXLog Enterprise Edition
- NXLog Agent Manager

BUSINESS RESULTS

- Unified and autonomous logcollection pipeline has been built.
- On-going event source integrationsimplified.
- Security posture increased withbroader log collection coverage.
- Compliance achieved.

BACKGROUND

Financial services sector is subject to various global and local regulations (GDPR, PCI DSS, SOX, GLBA, etc.) that mandate safeguarding infrastructure and customer financial data. Cybercriminals may reap substantial profits from successful attacks on financial services companies, hence obtaining a detailed, precise, and upto-date perspective of all network activities is essential to fortify defenses against such threats.

Full-scale log collection and on-going analysis are essential components of well defined defense-in-depth strategy according to security standards and guidelines like from ISO, NIST or similar.

Financial Services companies depend on complex IT infrastructure and applications to manage financial data, fulfill customer requests, and carry out other essential business operations. Through analyzing and connecting log, metric, and trace data, engineering teams can achieve comprehensive insight into the wellbeing and effectiveness of IT-services, allowing for expedited resolution of production and security issues. Furthermore, filtering out extraneous data can decrease expenses for data retention.

CHALLENGES & SOLUTION

In order to improve security posture and meet compliance regulations the Customer made a decision to replace old log collection solution that has been considered as obsolete, ineffective and difficult to manage.

A solid log management process requires a robust logging pipeline first to be established across all the network infrastructure, including air-gaped nodes. The main challenge here is a variety of target systems from different vendors with assorted logging capabilities and technologies. Solving that challenge the Customer was looking to implement vendor-agnostic log collection pipeline that allows fast and easy integration for old and new network endpoints and applications.

Why NXLog Enterprise Edition has been chosen over competitors
NXLog Enterprise Edition agent supports a huge variety of log sources including Windows event logs and can process logs with volumes over 100,000 events per second. It can accept event logs over TCP, TLS/SSL, and UDP; from files and databases; and in Syslog, Windows Event Log, and JSON formats.

> *"We are very pleased working with NXLog and really appreciate all the advanced features of the product. We were looking for a lightweight log collection tool, that allows to flexibly filter and transform events, while keeping it easy to deploy agents across Microsoft infrastructure. We considered NXLog as the most versatile product that completely fulfill all the needs for us."*
>
> ***- CISO, Top-3 Automotive Financial Services Company***

Log management is not a one-time task, but an on-going process where all the collecting agents and forwarders have to be monitored and managed while new network endpoints are to be seamlessly integrated into the pipeline. For the Customer it was crucial to have an ability to easily deploy collecting agents across all the Microsoft Windows infrastructure.

Why NXLog Enterprise Edition has been chosen over competitors
NXLog Enterprise Edition agent supports many operating systems and provides a flexible deployment scenarios including one via Windows Group Policy with a signed package.

Another feature demand from the Customer was a reach data filtration and transformation features. With log collection it's always a task to pick only those events that matter for analysis and skip a huge volume of diagnostics that doesn't help for a specific task, like security, for instance. Message transformation is also often required to a the central store requirements, for example, a specific SIEM or APM type of the system.

Why NXLog Enterprise Edition has been chosen over competitors
NXLog Enterprise Edition agent can perform advanced processing on log messages, such as rewriting, correlating, alerting, pattern matching, scheduling, and log file rotation. It supports prioritized processing ofcertain log messages, and can buffer messages on disk or in memory to work around problems with input latency or network congestion. After processing, NXLog can store or forward event logs in any of manysupported formats including popular SIEM, like IBM QRadar, MicroFocus ArcSight, Google Chronicle,Microsoft Sentinel and others.

Finally, a new unified log collection pipeline powered by NXLog has been deployed that helped to meetboth corporate and national regulations.

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*

Contact us: **nxlog.co** YouTube LinkedIn Twitter