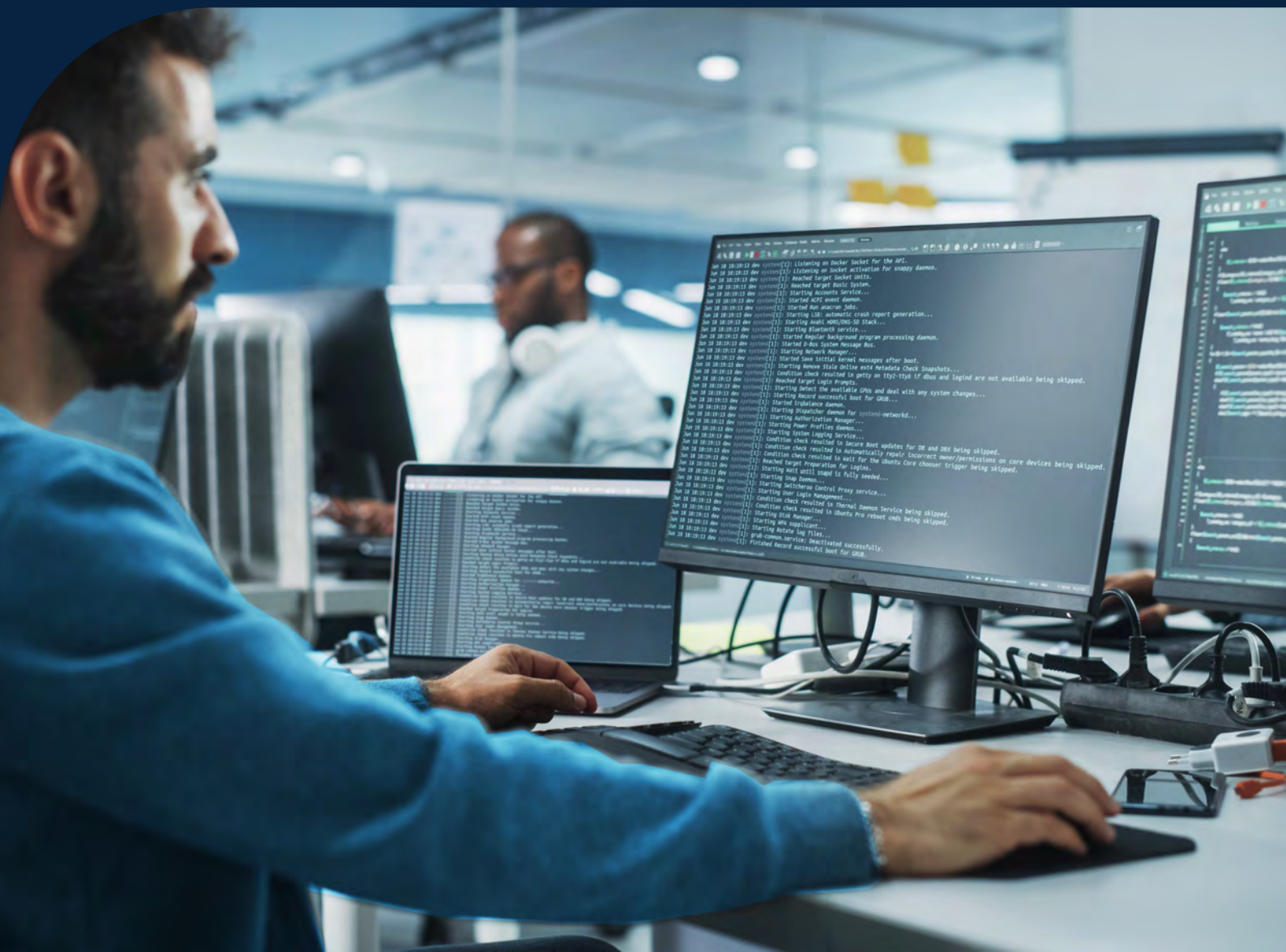
NXLog

NXLog Helps Top Automotive Financial Services Company To Strengthen Cybersecurity And Achieve Compliance



NXLog Helps Top Automotive Financial Services Company To Strengthen Cybersecurity And Achieve Compliance

Financial Services Company

A business division of the world's top-tier automotive group of companies with thousands of 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

Improve security posture, Meet SEC, SOX, PCI, GLBA compliance, national and corporate regulations for log retention & analysis.

CHALLENGE

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

SOLUTION

- NXLog Enterprise Edition
- NXLog Agent Manager

BUSINESS RESULTS

- A unified and autonomous log collection pipeline has been built.
- Ongoing event source integration simplified.
- Security posture improved with broader log collection coverage.
- Compliance achieved.

NXLog

BACKGROUND

The 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 up-to-date perspective of all network activities is essential to fortify defenses against such threats.

Full-scale log collection and ongoing analysis are essential components of a well-defined defense-in-depth strategy according to security standards and guidelines like 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. By analyzing and connecting logs, metrics, and trace data, engineering teams can achieve a comprehensive insight into the well-being and effectiveness of their IT services, allowing for expedited resolution of production and security issues. Furthermore, filtering out extraneous data can decrease expenses for data retention.

CHALLENGES & SOLUTION

To improve security posture and meet compliance regulations, the Customer decided to replace the old log collection solution considered obsolete, ineffective, and difficult to manage. A solid log management process must establish a robust pipeline 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. To solve the challenge, the Customer wanted to implement a vendor-agnostic log collection pipeline that allows fast and easy integration for old and new network endpoints and applications.

WHY NXLOG ENTERPRISE EDITION IS FAVORED OVER ITS COMPETITORS:

NXLog Enterprise Edition agent supports various log sources, including Windows event logs, and can process logs with volumes over 100,000 events per second. It supports all standard network protocols, can collect logs from files and databases, and is compatible with many log formats by default.

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

NXLog Enterprise Edition agent supports many operating systems and provides flexible deployment scenarios, including one via Windows Group Policy with a signed package.

Another feature demanded by the Customer was reach data filtration and transformation capabilities.

With log collection, it's always a task to pick only those events that matter for analysis and skip a vast volume of diagnostics that don't help for a specific job, such as security. Message transformation is also often required to meet the central store requirements, for example, a particular SIEM or APM type of the system.

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 of specific 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 many supported formats, including popular SIEM solutions like IBM QRadar, MicroFocus ArcSight, Google Chronicle, and Microsoft Sentinel.

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

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,
Automotive Financial
Services Company

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