NXLog

Transforming Security for a U.S. Government Agency

Customer Profile

A U.S. government state, managing a robust and diverse economy, driven by key sectors such as energy, agriculture, and aerospace. The state is a long-standing leader in oil and natural gas production, accelerating its growth in renewable energy and advanced manufacturing.

Related Industries

- Government

Business Demands

- Security posture improvement
- Regulatory compliance
- SIEM cost reduction

Challenges

- Heterogeneous infrastructure (Windows, Linux, network devices)
- Diverse log types
- Migration from Splunk to Anomali SIEM

Solution

NXLog Platform

Business Results

Enabled reliable log collection across a disparate, multi-vendor environment – both cloud and on-prem.

Ensured efficient security monitoring under heavy log stream conditions.

Reduced SIEM costs

Background

Faced with growing cyber threats, a major U.S. government institution needed to overhaul its security monitoring. For years, it relied on Splunk as its SIEM. But explosive growth in log volumes pushed the system beyond its limits. Costs soared under a licensing model tied to data ingestion, and performance lagged as data pipelines choked, leading to delays and missed alerts.

The client's diverse IT environment, spanning legacy systems, cloud infrastructure, and a wide array of security tools, produced inconsistent logs that were difficult to aggregate and normalize.

Managing thousands of agents added further complexity. It diverted the security team from its core job while compliance pressures mounted. The inevitable gaps in log collection ultimately threatened the organization's audit readiness.

Recognizing these challenges, the client made a strategic shift. It migrated to Anomaly SIEM while rethinking its entire telemetry infrastructure. It needed a solution that could efficiently collect, process, and deliver clean, structured logs — laying the foundation for scalable, real-time security operations.

Solution

After a rigorous evaluation of commercial and open-source solutions, the institution selected NXLog as the core of its new security data pipeline. Chosen for its lightweight design, high performance, and flexibility, NXLog was the best-fit solution to aggregate and forward logs across a vast, complex IT environment to the new Anomaly SIEM.

Deployment was carefully orchestrated to integrate NXLog into the entire IT landscape, collecting logs from all necessary sources, including the network infrastructure (Juniper, Palo Alto, F5, Zscaler, Cisco), Windows environments (collecting event logs, Sysmon, Active Directory logs), and PRTG, as well as various custom systems. However unique or complex the source, each data stream was seamlessly incorporated into a centralized, unified logging pipeline.

A key driver of this transformation was NXLog's advanced edge processing capabilities. This helped the client's security team enrich and normalize log data before transmission, parsing and filtering raw messages and converting them into clean, structured JSON.

This significantly improved data quality and reduced unnecessary noise. With built-in dynamic routing, NXLog could intelligently forward logs to appropriate destinations. For example, sending exhaustive raw firewall logs to Amazon S3 and endpoint data to Anomaly SIEM. This optimized both storage efficiency and SIEM ingestion performance.

To handle scale, the team leveraged NXLog's batching and compression capabilites, while minimizing network overheads and storage costs. All transmissions were encrypted, and Amazon S3 served as a secure, compliant staging area, supporting strict federal audit requirements.

Results

The government team saw immediate impact. Overall security operation costs dropped significantly thanks to smarter log processing and reduced SIEM ingestion volumes. Scalability was drastically improved, and real-time security visibility was guaranteed – even under heavy load.

Operational efficiency also soared as automation replaced manual log wrangling, freeing analysts to focus on threat detection and response. And finally, the Anomaly SIEM benefited from clean, context-rich logs, enabling faster correlation and fewer false positives.

For more information about NXLog products and services, visit our website, contact us via the web form, or schedule a meeting.

Start free with the NXLog Platform now!