NXLog

How we Boosted a Biotech S&P100 Company's Security Operations and Compliance

How we Boosted a Biotech S&P100 Company's Security Operations and Compliance

CUSTOMER PROFILE

Global biotech company (S&P100) with a longstanding history of discovering, developing, and delivering innovative medicines.

RELATED INDUSTRIES

- Biotechnology
- Biopharmaceutical

BUSINESS DEMANDS

- Regulatory compliance (HIPAA, FDA, GDPR)
- Security posture improvement

CHALLENGES

- Heterogeneous infrastructure (Windows, Linux, network devices)
- Diversity of log types
- Unified integration with SIEM

SOLUTION

NXLog Platform

BUSINESS RESULTS

Delivered a unified log collection pipeline, built across the client's IT infrastructure, to streamline and optimize security analysis and regulatory compliance.

NXLog

BACKGROUND

Our client, a prominent global biotech company, handles sensitive data ranging from proprietary research outputs and how-tos to personal health information. As such, the client is subject to strict regulatory standards, including the Health Insurance Portability and Accountability Act (HIPAA, mandating the protection of patient health information), Food and Drug Administration (FDA) Regulations (requiring meticulous record-keeping around research and development processes) and General Data Protection Regulation (GDPR, governing the handling of personal data for international operations), amongst others. Failure to comply could result in severe legal penalties, while a data leak could seriously impact the company's reputation and credibility.

A key factor in any successful risk management and regulatory compliance strategy is a well-established log management process. Comprehensive log management is critical for consistent, continual incident detection and response. It's also a must-have when it comes to demonstrating data compliance for audit purposes.

Our client's IT infrastructure is a heterogeneous mix of operating systems and devices, including thousands of Microsoft endpoints (Windows 10 and 11 workstations and Windows Server 2016 and 2019), Linux-based systems (Red Hat Enterprise Linux (RHEL) versions 8 and 9, CentOS, and Amazon Linux), network devices (e.g. Cisco routers and switches), and various firewall appliances from different vendors.

Collecting logs from a hybrid environment like this poses a significant technical challenge. Each system and device generates logs in different formats, requiring different means and protocols to capture them. This makes centralized collection very difficult.

The client's ultimate goal was to enhance security, ensure compliance, and streamline operations by integrating log sources with its existing Security Information and Event Management (SIEM) platform, IBM QRadar.

Like every other general-purpose SIEM solution on the market, IBM QRadar has limited technical capabilities in terms of integration with log sources. Tools for only the most basic use cases are provided. So, for our client's security team, it became obvious that an autonomous log collection pipeline was needed to enable compliance-ready log acquisition from its disparate data sources, which it could then feed to its SIEM in compatible formats.

To add to this, with the rapid expansion of ongoing R&D projects, the volume of log data is increasing exponentially. Transmitting large volumes of log data across the network to an SIEM requires significant bandwidth and storage resources and impacts SIEM performance and related costs. The client needed a solution that could scale seamlessly without affecting its SIEM and SecOps budget.

SOLUTION

After evaluating several potential vendors, the client chose NXLog Platform – successor of the NXLog Enterprise Edition log management solution – for its versatility, scalability, and robust feature set. The log collection architecture was planned, and then deployment began.

Among the solutions provided by NXLog Platform, the following were implemented to overcome challenges posed by the heterogeneous nature of the client's IT infrastructure, as well as the strict regulatory technical requirements:

- **A centralized interface** to manage thousands of agents and collectors installed across the client's environment.
- **A unified pipeline** to collect logs from all systems and devices, including:
    - **Windows Systems:** using the im_msvistalog module, NXLog Agent collects Windows Event Logs from desktops and servers. The module gathers logs related to security events, system errors, application issues, and more.
    - **Linux Systems:** with the im_file module, NXLog Agent captures data from various log files on Linux systems, such as /var/log/messages, /var/log/secure, and application-specific logs, required for regulatory compliance.
    - **Network Devices:** with the im_udp and im_tcp modules, NXLog Agent captures syslog messages from network devices such as Cisco routers and firewalls sent over UDP and TCP protocol.

We addressed integration, bandwidth and storage concerns with the following NXLog Platform components:

- **Batch Compression:** with the im_batchcompress module, NXLog Agent can handle archived log files and data transmitted in a compressed format. This significantly reduced the size of data sent over the network, easing the burden on bandwidth.

- **Data Parsing:** with regular expressions and embedded parsing options, NXLog Agent can extract meaningful information from unstructured log messages. This functionality allowed our client to pre-filter logs and save only the necessary data volume, which could then be forwarded to the SIEM – optimizing its performance and storage.
- **Data Normalization:** NXLog ensures data structure (fields) align across different log sources so that similar events are consistently represented, regardless of their origin.
- **Data Transformation:** NXLog Agent can transform logs into common structured formats like JSON, XML, or CSV for seamless integration with up-stream systems like SIEM.
- **SIEM Integration:** NXLog Agent sends logs directly to QRadar, requiring no intermediate steps. And with custom parsing/mapping rules, NXLog Agent automatically matches the log format expected by IBM QRadar.

RESULTS

Since deploying NXLog Platform, our client has optimized its security monitoring, balanced its SIEM performance and leveraged alerts for close to real-time threat detection. With its security team able to gain immediate access to comprehensive, centralized log data – accelerating investigation and remediation efforts – the client's incident response has significantly improved.

Additionally, by providing a transparent audit trail and ensuring that all necessary logs were collected, stored, easily retrievable, and properly disposed of, NXLog Platform has enabled the client to meet its compliance requirements. Plus, with log pre-filtering reducing the volume of data collected, the client was able to boost its efficiency while retaining its current SIEM licensing tier, thereby avoiding additional costs.

Finally, the autonomous log collection pipeline powered by NXLog Platform has streamlined the client's operations by centralizing log data and unifying reporting across different teams and departments.

> *The investment into building a security observability pipeline with NXLog not only fortified our existing IT infrastructure but also made room for us to grow securely. As we continue to innovate in biotech, we can rely on NXLog Platform to scale with us, making sure security and compliance risks are managed properly*
>
> Chief Information Security Officer,
> S&P100 Biotech Company

NXLog

For more information on NXLog visit our website or schedule a meeting.

Start free with NXLog Platform now.