NXLog

SIMPLIFYING MANAGED SECURITY SERVICES LOG COLLECTION STRATEGY WITH A SINGLE TOOL

CUSTOMER CASE STUDY

atmosera

With 20+ years of experience managing complex IT environments, offering public, private, and hybrid cloud solutions, Atmosera works closely with organizations across all industries to architect, operate, and optimize cloud infrastructures with their advanced services. As a Gold-level, Managed Microsoft Partner, Atmosera is a leading certified Azure Expert MSP offering InfoSec services, compliance (HIPAA/HITECH, PCI-DSS, IRS1075, SOC 1, and SOC 2 Type II), data protection, DevOps as a service.

INDUSTRY

Managed Service Provider

HEADQUATER

Beaverton, Oregon, United States

EMPLOYEE

Byron Anderson, Infosec Engineer

CHALLENGES

- Collecting all the logs generated at clients' heterogeneous log sources
- Transmitting these logs to a centralized SIEM and additional targets securely, adds further complexity to implementing a compliant log collection strategy
- Simplifying processes with automated solutions that can be deployed easily and standardized across all operating systems

BUSINESS SOLUTIONS

- NXLog Enterprise Edition
- NXLog Support Services

SIMPLIFYING MANAGED SECURITY SERVICES LOG COLLECTION STRATEGY WITH A SINGLE TOOL

BACKGROUND

A couple of years ago Atmosera began to establish their security division to provide Managing Security Solutions to help their clients in an evolving world of cybersecurity threats. This division was meant to anticipate and lead technology innovation to help the company's clients benefit from everything that cybersecurity technologies can offer. They started to create a platform of solutions that later would became their security platform. Their goal was to look for powerful tools and solutions with diverse functionalities, so they would only need to use a handful of them.

THE CHALLENGE

As the business expanded to include managed security services, they moved ahead helping businesses of all sizes to be secure against cyberattacks by offering Managed InfoSec services, compliance, data protection, DevOps as a service, and more. Therefore, Atmosera needed a way to **collect the large amount of log data generated at all their clients' endpoints** and then have it forwarded into their Securonix SIEM platform, while **maintaining security and compliance** to various regulations. They wanted a solution that was simple to work with and especially one that can be **standardized across all systems.**

Automating every process in their organization is one of their main goals, so they were seeking solutions that could be configured and easily deployed, where their DevOps team would be able to take full advantage of its capabilities.

Besides, for Atmosera, having **reliable vendor-support** is key, considering their compliance services, so if any problem arises, they want to **ensure they can support their clients' diverse needs**. They needed a supported tool that can comply with any industry's requirements allowing them to store log data that can be processed or reviewed in the future to detect changes that occurred at any given moment in files and directorie

SOLUTION

Backed with their **previous experience of using NXLog Community Edition** and experience with different trials of other solutions like **Snare**, they ultimately decided that the **NXLog Enterprise Edition** would make the most sense for them, as it did a **better job and had more capabilities**.

The NXLog Enterprise Edition and its Support Services enabled Atmosera to implement a **scalable logging system** by making sure that all their log data is collected in an efficient, secure, and reliable way, at the same time allowing them to structure, format, and filter the data so it can be forwarded in a unified format to their SIEM to ingest.

Atmosera, a US-based company partnered with NXLog to deliver log collection and centralization solutions along with their Security Information and Event Management platform. As an NXLog MSSP Partner, Atmosera continues to build customer trust with solutions that provide tangible results maximizing their security and ensuring compliance.

For Atmosera having **NXLog Support Services** is very important, considering that part of their security business involves compliance and they also wanted a way to provide a light **File Integrity Monitoring (FIM)** capability in their services, along with **encryption** to conceal sensitive information, a security measure that may be required by **compliance mandates.**

> *"Some other solutions that we looked at; their capabilities were minimal. Since we work with so many different clients, we never know what request the client is going to throw at you and we want to know that we can support those requests no matter what they are, and* ***with NXLog it's sort of like the swiss army knife of logging tools****."*
>
> *-Byron Anderson, Infosec Engineer*

BUSINESS OUTCOME

NXLog Enterprise Edition became **one of their core applications within their Managed Detection and Response (MDR)**, platform, designed to support environments with advanced security and compliance requirements. NXLog Enterprise enhances their SIEM platform ingestion capabilities by forwarding their log data for threat analytics. In addition to the flexibility of log ingestion, the integrated **File Integrity Monitoring (FIM) also became one of the main features in their Premium Service** helping their clients to respond quickly and effectively to unexpected changes to files which is a standard requirement for many regulatory compliance objectives.

All the **plain text configuration files helped the organization to automate their deployments** and having a **solution that is simple to configure** through standard text-based config files, made their DevOps team's work much easier.

"There is nothing at this point that I wanted to do with NXLog that I haven't been able to do, and its support has always been very responsive and really good."

NXLog Enterprise Editions' flexibility and shared scope of capabilities have given them the ability to feel comfortable and work with any client no matter what the requirements are regarding log collection processing or forwarding. NXLog, being so easy to troubleshoot, has significantly reduced Atmosera's troubleshooting time in dealing with those types of issues.

"I worked with a lot of log management solutions in the past, and a lot of them use their proprietary agent technology those agents are very difficult, they either work or they don't, and when they don't work, they are very difficult to troubleshoot. With NXLog, logging is clear and easy to understand, so it drops our troubleshooting time on our log forwarding agent."

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.*