Improving Security Monitoring & Speeding Response Time

Logz.io log management and alerts modernized local health organization

The Challenge

U.S.-based healthcare network provider, Westbrook Health Services, needed to filter through large volumes of log data to identify and respond to potential security threats, while ensuring compliance with complex mandates such as HIPAA. The organization was in need of a solution to increase visibility to protect against potential threats.

> *"By the time I was done with the evaluation, Logz.io was already implemented"*

Shawn Reaser
Director of IT

With a network of eight main sites and 40 residential homes overseen by an IT team of five, Westbrook Health Services determined that it needed a more streamlined approach to log management and security event alerting across their wide network of facilities.

Most importantly, whatever solution implemented would need to protect confidential patient information and comply with industry regulations like those mandated by HIPAA.

Another core goal of the project was to ensure that the entire Westbrook Health network was securely updated to meet changing security requirements while improving team productivity, and streamlining related processes.

With a firm understanding of key objectives, Director of IT Shawn Reaser began researching solutions with a focus on improving security alerting and investigation practices while addressing the organization's varied compliance requirements.

Additionally, the desired solution needed to integrate directly with Westbrook's existing tools including its widely deployed SonicWall firewall systems. Moreover, the organization sought to markedly reduce monitoring time frames and mean time to response (MTTR), while increasing productivity—all within a set budget.

CUSTOMER
Westbrook Health Services

INDUSTRY
Healthcare

LOGZ.IO CUSTOMER SINCE
September 2021

PRODUCTS

Log Management

Cloud SIEM

HEADQUARTERS
Parkersburg, West Virginia

The Logz.io Solution

Given Westbrook's urgency for implementation, the IT team immediately began looking at roughly 60 different log management solutions including Logz.io. From the start, Reaser said he knew the Logz.io platform was not only going to meet the company's strict compliance requirements, but also enable his team to meet their efficiency and productivity goals.

Reaser noted that time to value for Logz.io also quickly proved itself as a strength once it had been chosen as a solution, with the Westbrook IT team fully up and running in only two weeks, including the creation of numerous dashboards and graphs. Additionally, based on Logz.io's open source foundation, the solution enabled the lean IT team to confidently implement and seamlessly integrate Logz.io with their existing open source tech stack.

With the move to cloud-based log management this also allowed the Westbrook team to securely store their network data offsite, with no concern of service interruption. Long term, Reaser said the ability to extend monitoring and alerts to its email security systems was another key advantage of utilizing Logz.io.

Results

Using Logz.io, Westbrook Health now relies heavily on the platform's numerous dashboards and graphs to perform the heavy lifting of its monitoring activities. Instead of manually monitoring logs each day, accounting for many hours of his available time, Reaser and his team utilize Logz.io to monitor logs from web servers, emails, as well as their cloud-based HR system. The platform's team alerts have been instrumental for the group, Reaser said, allowing him to assign various tasks directly from Logz.io to other members of the Westbrook staff.

Using Logz.io, Reaser estimates that the amount of time necessary to perform targeted security analysis has been reduced significantly, from many hours each day to less than an hour per day, allowing more time to focus on building security systems and fine tuning the healthcare network's management processes.

> *"Before [Logz.io] we were being reactive and now we're actually proactive."*
>
> **Shawn Reaser**
> Director of IT

Building a Better Future with Logz.io

By partnering with Logz.io, Westbrook Health Services has been able to future proof their trusted healthcare network and make a major impact on the IT department's overall productivity, freeing up time to build new security systems and support future expansion of its operations, Reaser said.

Just four months since its initial implementation of the Logz.io Log Management and SIEM solution, the Westbrook IT team has seen significant improvement to their security monitoring processes and compliance auditing, with plans to explore expanded use of the Logz.io observability platform to address adjacent monitoring and security requirements.

> *"Logz.io solution was faster and cheaper to implement than all the other solutions. That's why I picked Logz.io over everything else"*
>
> **Shawn Reaser**
> Director of IT

logz.io