sumologic

CASE STUDY

medidata

Medidata

Medidata Finds the Cure for Security Analytics with Sumo Logic

Overview

Company

- Medidata

Industry

- Life Sciences

Region

- North America

Size

- 1,400 employees

Use Case

- Security and Compliance

Business

Medidata needed insight into the security posture of its systems and be able to spot potential indicators of attacks from within its on-premises systems and cloud services, so that it could stop attacks as quickly as possible and be able to substantiate its high level of security to its clients.

Challenges

Medidata chose Sumo Logic's cloud-native data analytics platform to gain full stack visibility and real-time insights into the security status of their on-premises and cloud-based data centers.

Results

- Ability to demonstrate to customers the same level of security visibility into cloud systems as on-premise systems.
- Proactive resolution of security incidents that may have otherwise gone undetected.
- The ability to identify only the events that matter in more than 2 terabytes of system event data generated monthly.

Introduction

Medidata helps clinical trials and studies run better. Today, more than two million patients participate in about 9,000 studies that depend on Medidata's cloud platform, the Medidata Clinical Cloud. The Medidata Clinical Cloud improves productivity and quality in the clinical testing process of new medical treatments, from study design and planning through study execution, management, and reporting.

> "Sumo Logic has helped us effectively manage our hybrid infrastructure and accelerate innovation. Now we can collect logs from both our on-premise data center as well as our cloud applications, make sense of it and take action in real-time, and that's really the golden nugget."
>
> Glenn Watt, CISO, Medidata

In this way, the Medidata Clinical Cloud helps life science organizations reduce their risks associated with clinical trials and improve outcomes, all while lowering their costs and the amount of time to completion. Medidata's customer base spans biopharmaceutical companies, medical device and diagnostic companies, academic and government institutions, contract research organizations, and other research organizations, 24 of the top 25 global pharmaceutical companies that are developing life-enhancing medical treatments and diagnostics.

Founded in 1999 in New York, with offices now throughout the United States, the United Kingdom, and Japan, Medidata relies heavily on technology to run its business and provides its services. That business technology includes a combination of on-premise data centers and public cloud systems. Today, Medidata's traditional data center in Houston, Texas, runs a number of on-premises applications that are core to its business such as its platform host Electronic Data Capture, and Safety Gateway which identifies potentially serious adverse effects in a clinical trial and contains the largest storehouse of Medidata's information. "That data center is very important and it's very large, but the rest of the applications Medidata relies on run within Amazon Web Services (AWS)," says Glenn Watt, CISO at Medidata.

The need for transparency and insight

To protect its systems and data, Medidata had put into place a mature security program with numerous security controls and processes within its physical data center, as well as utilizing the security features provided by AWS, such as AWS security groups. In addition to those existing efforts to secure its on-premises and cloud systems, Medidata needed to improve its level of transparency into security events on its systems, help substantiate its high level of security diligence to clients, prevent data leakage, and be able to analyze attacks in near real-time.

What Watt needed to achieve was the ability to analyze Medidata's log and system files for events that would indicate something could be going awry or an attack was underway. The team needed to do so without having to depend upon outdated signature-based or intrusion detection systems that issue countless false positives when tuned too tightly, or miss incidents altogether when tuned too loosely. "We're generating just under two terabytes a month of log files. No one can realistically go through all of that data and identify the correlations necessary to spot attacks, and that's why we needed a strong security data analytics capability," Watt says.

Additionally, that capability would go a long way to help alleviate the concerns of some of Medidata's customers about so much of their business operating within the cloud. Because of the nature of the data and the increased amount of third-party vetting and due diligence today, a number of Medidata's clients question Medidata when it comes to how they secure their cloud-based systems. "From our customers' perspective, the first thing they see is that we have considerable operations in the cloud. Some are very skeptical that as there's an inherent fear of the cloud and the fact that it may not be secure. And that data may be vulnerable and at worst, perhaps manipulation of the data," Watt says.

To find the right solution, Watt originally evaluated the top SIEMs and a number of security data analytics tools available on the market. Unfortunately, very few would work both on-premises and within AWS and many even required equipment to be on-premises. "My first question to all of the vendors we evaluated was whether or not the system ran within AWS. If it didn't, it was a five-minute discussion," Watt says. "But the solution had to do more than work within AWS; it had to also work in our data center, and I wanted a solution that did not require any additional hardware or software."

The move to Sumo Logic

After careful evaluation, Medidata realized they could accomplish this with a cloud-native data analytics solution and chose Sumo Logic. Sumo Logic delivers real-time, continuous intelligence across Medidata's entire infrastructure and application stack, and provided Medidata with a solution that helps it to automatically generate audit-ready compliance reports from both its on-premises and AWS event logs. Sumo Logic also provides Medidata a way to simplify cloud and on-premises audits and strengthen its security posture with a composite view across the network, server, and application stack.

Additionally, predictive analytics powered by machine learning algorithms uncovers unknown security events without relying on rules or predefined schemas to ward off impending threats.
Watt was pleased with the smooth Sumo Logic implementation. "It took literally minutes to get up and running," he says. "Our engineers worked with the Sumo Logic engineering team and within 20 minutes it was done, and it's remained that easy. From our first report, we were able to get actionable information that has been extremely valuable on a daily basis."

Seeing only what matters

With nearly two terabytes of log data being generated a month, Watt needed a way to rapidly separate what mattered from what didn't. "Sumo Logic does that exceptionally well; no question about that. Before Sumo Logic, we didn't even know what we didn't know, so things were going on and there were threats that were presenting themselves at our front door that we were unaware of. With Sumo Logic, it's like somebody took the blindfold off, and we could see what was potentially impacting our business," Watt says.

Sumo Logic also has helped Watt to demonstrate Medidata's high level of data security and its ability to respond to incidents. "We have customers who have to know what we are doing when it comes to our security efforts. They need proof, and with the reports that Sumo Logic provides, that is made possible. With Sumo Logic, Medidata can now more easily substantiate its security efforts and have visibility into events on AWS as well as the ability to identify any potential suspicious traffic that may arise. Also, that same reporting helps Medidata comply with CFR Part 11 from the Food and Drug Administration, which mandates numerous cybersecurity regulatory requirements that Medidata must meet.

Spotting attacks in real time

It's not just about regulatory compliance and monitoring for the sake of monitoring and compliance and customer assertions; Sumo Logic also provides actionable security information and has successfully blocked attacks that were underway. "Late one night, Sumo Logic triggered an alert on what appeared to be an attack coming in against our servers. We were notified and within minutes and concluded that it looked like an attack and we blocked the source," recalls Watt.

Sumo Logic provided Medidata the insight it needed to identify the root source of that apparent attack within minutes. The apparent attack was coming from a client's server. Watt reached out to the client over the phone, thinking that what was being observed could have been an attack underway, or a false positive. Either way, it was crucial that the client be informed. However, the client informed Watt that it had been conducting a penetration test that weekend.

"Somebody entered something incorrectly during the penetration test, so not only did they attack their own servers during the attack, but also a server that Medidata was using with the client. I told them that we picked up an attack, and that we stopped it within minutes, and that's what we're going to do every time we see something," Watt says. "They were knocked off their socks. They couldn't believe that we were able to react that swiftly, and that we were protecting them at that level. And we could not have done it without Sumo Logic," he says.

"Our move to Sumo Logic has been a great success in every aspect. We can see what we need to see in both our physical data center and within Amazon Web Services. Sumo Logic helps us to substantiate what our customers need to know about our security program; there are potentially a lot of attacks and activities that are unknown to us and Sumo Logic helps us to now see that activity," Watt says.

> "Our move to Sumo Logic has been a great success in every aspect. We can see what we need to see in both our physical data center and within Amazon Web Services. Sumo Logic helps us to substantiate what our customers need to know about our security program; there are potentially a lot of attacks and activities that are unknown to us and Sumo Logic helps us to now see that activity."
>
> Glenn Watt, CISO, Medidata

About Sumo Logic

Sumo Logic is a secure, cloud-native, data analytics service, delivering real-time, continuous intelligence across an organization's entire infrastructure and application stack. More than 700 customers around the globe experience real-time operational, business and customer insights using Sumo Logic for their DevOps, IT ops and security and compliance use cases. With Sumo Logic, customers gain a service-model advantage to accelerate their shift to continuous innovation, increasing competitive advantage, business value and growth. Founded in 2010, Sumo Logic is a privately held company based in Redwood City, CA and is backed by Greylock Partners, DFJ, IVP, Sutter Hill Ventures, Accel Partners and Sequoia Capital. For more information, visit www.sumologic.com.