splunk>

CASE STUDY

Biopharma Leader Gets Ahead of Security Threats With Analytics-Driven SIEM in the Cloud

Healthcare

Executive summary

One company, a fast-growing global leader in the biopharmaceutical space, is highly regarded for the effective drugs it develops to help customers. But, with data silos located across the globe, the company needed a security information and event management (SIEM) solution that would better protect its customers and intellectual property against cyberthreats and breaches, particularly given today's ever-changing security threat landscape. Since adopting Splunk Cloud with Splunk Enterprise Security (ES) for security and compliance, the company has seen benefits including:

- An estimated 30 percent lower cost of ownership compared to on-premises alternatives
- A dramatic reduction in security investigation and resolution times
- Protection against threats, breaches and malware; ensuring regulatory compliance

Why Splunk

Prior to adopting the Splunk platform, the company used an antiquated security tool that had fallen off of the Gartner SIEM Magic Quadrant. The company's security team had tried to revitalize its legacy SIEM, but found it very difficult to get data into it and to derive necessary insights from it. The company has datacenters located in multiple locations, and due to the limitations of its legacy SIEM, it was very difficult for the security team to bring in data from the various silos together to get the much-needed visibility and stay ahead of threats.

Previously, with its legacy SIEM, security investigation and resolution times at the company were slow—typically stretching to days, weeks or even months. What's more, without preemptive security insight, the company was concerned that it might face regulatory and compliance penalties that could damage its reputation and stock price. The organization needed a security solution that was flexible and scalable enough to ingest all of its data ubiquitously and that would enable the security team to draw conclusions from its data in near real time.

Industry

- Healthcare

Splunk Use Cases

- Security
- Compliance
- IT operations

Challenges

- Concerned about protecting customer and intellectual property data
- Legacy SIEM lacked the ability to perform analytics across many different data sets
- Needed insights to stay ahead of the cyberthreats
- Needed to meet regulatory and compliance mandates to avoid penalties and damage to the company's reputation or stock price

Business Impact

- Estimated 30 percent lower cost of ownership compared to alternative on-premises solutions
- Fast time to value
- Protection against threats, breaches, malware and ensuring regulatory compliance
- Security investigation and resolution times reduced from up to months to minutes

Data Sources

- Server
- Network
- Endpoint
- Firewall
- Database
- Application
- Amazon Web Services

Splunk Products

- Splunk Cloud
- Splunk Enterprise Security

The company issued an RFP and looked at several traditional SIEM tools including IBM QRadar and a few others that are typically adequate for asking specific questions of data. But, with security threats changing daily, the security team members needed a solution designed to help ask questions of their data that they had not yet considered, which prompted them to adopt the Splunk platform.

Instant cloud availability

Given that the company manages highly sensitive consumer and proprietary intellectual property data, it needed a solution that would provide visibility into any possible threats in its IT environment as soon as possible. The company was satisfied with the immediate availability of Splunk Cloud with Splunk Enterprise Security as its SIEM, and the security team began asking questions and getting answers from its data right away.

Today, the company's chief information security officer and global head of cybersecurity, along with a team of 20 people in the company's security operations center, provide security service globally. The Splunk analytics-driven SIEM takes in log information from all areas of the company—including infrastructure, applications and devices—to detect security incidents and manage those events, which simply could not be done adequately with its legacy SIEM.

The company's security team feels confident that the Splunk analytics-driven SIEM is helping it to avoid facing a serious situation like the one that another industry player faced recently when it was hit by a malware event and experienced data exfiltration. Now, with the Splunk platform, the company has a solution for monitoring threats and a process to triage those threats. Overall, security investigation and resolution times have been reduced from up to months to hours or even minutes.

Meeting FDA and GDPR compliance

In the pharmaceutical industry, companies must retain all data for a certain period of time to comply with U.S. Food and Drug Administration regulations and the E.U. General Data Protection Regulation (GDPR). Prior to adopting the Splunk platform, the company had no way to prove that it was meeting data retention requirements. Now, the company can be proactive with these requirements, demonstrating that it is in compliance, avoiding penalties and the deterioration of its brand reputation.

Currently, the company primarily relies on Splunk Cloud for security and compliance, and is being thoughtful about bringing in new data sources, whether they are traditional data sources or through acquisition of other entities, to proactively plan for future potential threats. The company is also beginning to use Splunk Cloud to monitor the company's IT operations, and plans are underway to identify additional ways to leverage insights from the data and help the business moving forward.