splunk>

CASE STUDY

Luxury Retailer Replaces Legacy SIEM With Analytics-Driven SIEM

Retail

Executive summary

Retail companies face many challenges when it comes to protecting their businesses and their customers—from securing online accounts and point-of-sale (POS) systems, to eliminating malware and other vulnerabilities. When one luxury retailer grew concerned about security breaches negatively affecting its customers and brand reputation, it replaced its security information and event management (SIEM) solution with an advanced and reputable alternative—Splunk Enterprise Security (ES). Since deploying Splunk ES, the retailer has seen benefits including:

- Fast implementation: replaced underperforming SIEM in only six weeks
- Added capabilities to prevent security breaches, mitigate fraud and ensure Payment Card Industry (PCI) compliance
- Gained ability to protect customer data and company reputation

Why Splunk

For many years, the luxury retailer had outsourced its security monitoring responsibilities to a managed service provider running HP ArcSight. In-house security staff assumed the implementation was solid and that they would be alerted to issues requiring further triage, but when the company experienced a serious security breach it realized its SIEM was not very useful in detecting and exposing what was occurring inside of the company's IT environment. The company had a bloated security operations center (SOC), yet it lacked a strategic solution for security. Moreover, it was very cumbersome to get data into the outdated SIEM or extract data out of it, and it was impossible to search the data.

What's more, the company's data was not being parsed correctly and because staff lacked visibility into the environment, they did not know there were issues that needed to be addressed to achieve full PCI and security compliance. The company realized that it needed a more robust platform and it adopted Splunk ES as its go-to solution for alerting on and searching all security-related events in the organization. In only six weeks, the company migrated off of HP ArcSight, the solution it had relied on for 10 years and implemented Splunk ES under a tight deadline.

Industry

- Retail

Splunk Use Cases

- Security
- Compliance
- Fraud
- IT operations
- Application delivery

Challenges

- Antiquated SIEM left company vulnerable to data breaches and bad publicity
- Lacked PCI and security compliance
- Cumbersome to ingest and extract data with previous SIEM
- Data was static, difficult to search and impossible to analyze
- Required bloated SOC team plus managed service provider
- SIEM platform was limited to security data

Business Impact

- Six-week implementation and rapid time to value
- Protecting customer data and company reputation
- Achieving PCI and security compliance
- Interactive solution for alerting, searching, reporting and visualization
- Managing security operations with lean, nimble team
- Expanding scalable big data analytics platform to be leveraged beyond security

Data Sources

- POS application logs
- Firewall syslogs
- Microsoft Windows events
- UNIX/Linux logs
- Juniper VPN syslogs
- F5 BigIP Load Balancer and F5 ASM syslogs
- SourceFire eStreamer syslogs
- Aruba switches syslogs
- CISCO ACS and IOS syslogs
- Web server logs

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security

Analytics-driven security platform

Soon after adopting Splunk ES, the company cleaned up its legacy data misconfigurations and captured the data necessary for PCI and security compliance. In addition to its legacy data, the company now has brought more useful and valuable data into Splunk ES to deliver an analytics-driven SOC, which is providing better protection than was possible with its previous SIEM.

Now, armed with Splunk ES and a new managed service provider, the company has a leaner, more nimble team to manage its security operations. Not only do the managed service provider and in-house team members monitor alerts from the enterprise data infrastructure, but they also have an interactive platform for active hunting, gathering and reporting. Rich Splunk ES visualizations enable the team to understand attack details and the sequential relationships between events for rapid incident response and management.

All data is security-relevant

The company relies on dozens of reports and searches, such as daily device status, daily event count summary, detailed firewall traffic for geolocation, malware callback, infected alerts reports and many more. Because all data is security relevant, the company has indexed nearly 200 data sources, including firewall logs, syslogs and POS application logs, to name a few.

> **"There is no other vendor that would have come into our enterprise and helped us to the degree that Splunk did. Most of the others would have just waited around for us to fix our issues, twiddling their thumbs and doing nothing. Splunk was fantastic, a partner, not just a vendor."**
>
> Security Manager at Luxury Retailer

With Splunk ES, the customer has invested in a big data platform. The retailer is repurposing its data and building out important new capabilities such as monitoring the company's POS systems to protect customer data. The company also is adding more fraud data sources for loss prevention and exploring many other use cases including IT operations, application delivery and business analytics to support omnichannel marketing. What's more, plans are underway to empower the company's CIO with machine learning made possible with Splunk ES.

"There is no other vendor that would have come into our enterprise and helped us to the degree that Splunk did," says the company's security manager. "Most of the others would have just waited around for us to fix our issues, twiddling their thumbs and doing nothing. Splunk was fantastic, a partner, not just a vendor."

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com