splunk>

CASE STUDY

# Global Fashion Accessories Retailer Speeds Threat Identification, Prevents Attacks With Splunk SIEM in the Cloud

## Fashion Retailer

### Executive summary

A strong security posture for retail companies is more critical than ever, with ransomware, distributed denial-of-service (DDoS) attacks and security breaches affecting major companies—and their customers across the globe—with growing frequency. When one leading global fashion accessories retailer was bogged down with an inefficient alerting system and unable to proactively prevent security incidents, it turned to Splunk Cloud with Splunk Enterprise Security (ES). Since deploying the Splunk platform, the company has seen benefits including:

- Drastically reduced security incident investigation times
- Prevention of ransomware attacks by identifying threats faster
- Freeing up of analysts' time to proactively prevent issues before they arise

### Why Splunk

The retailer manufactures and sells fashion accessories to consumers and acts as a wholesaler to more than 90 locations worldwide. With online and brick-and-mortar stores serving a global customer base, the company generates massive amounts of sensitive data daily. Its information security team was growing increasingly concerned about protecting customer data and wanted to avoid a headline-grabbing security breach.

Lacking a security information and event management (SIEM) system, email alerts served as an inefficient system to monitor the company's security posture. Analysts manually investigated every security event, but correlations were not done. This was both a time drain and not scalable as the company grew. To ensure the company was protected, the team needed to equip itself with the right tools.

When the company was deciding on a SIEM, Splunk Cloud with Splunk ES stood out above the competition for its high performance, functionality and value. "The value for the money spent has been tremendous—along with the ease of deployment, the capability of the tool and the amount of data we're able to send to it," says the company's senior security operations center (SOC) analyst.

Another important consideration for the team was speed. "With our old system, it could take anywhere from a couple of hours to a couple

### Industry

- Retail
- Online Services

### Splunk Use Cases

- Security
- Compliance
- IT Operations
- Business Analytics

### Challenges

- Lacked SIEM for alerting, searching, reporting and visualizations
- Inefficient alert monitoring system was slow and left company vulnerable to data breaches
- Unable to dedicate necessary time to preventative security measures
- System in place could not provide visibility into the company's many global locations
- Lost revenue as a result of avoidable downtime

### Business Impact

- Drastically reduced security incident investigation time
- Prevented ransomware attacks by identifying threats quickly
- Freed up analysts' time to proactively prevent issues before they arise
- Gained ability to prevent lost revenue from unnecessary e-commerce and point-of-sale downtime
- Achieved cost savings by shutting down unnecessary Amazon Web Services (AWS) instances

### Data Sources

- Windows event logs
- E-commerce logs
- Web proxy logs
- DNS queries

### Splunk Products

- Splunk Cloud
- Splunk Enterprise Security
- Splunk App for AWS
- Windows App for Splunk
- DNS Analytics for Splunk
- Hurricane Labs Search Add-on for Shodan

of days for a typical investigation. Now, with Splunk, it's only about 20 minutes," says the senior manager of information security.

## Easy deployment and immediate results

Implementing Splunk Cloud was quick and easy for the team. In fact, the senior manager of information security explains that the majority of the initial deployment period wasn't spent implementing Splunk, but instead involved getting other servers configured. "We were able to investigate before the deployment was done—we saw the results immediately," says the senior manager of information security.

The senior SOC analyst contrasts the process of deploying the Splunk platform to that of a different SIEM, HP ArcSight, which he used at a prior company. "ArcSight took an extremely high degree of technical knowledge to get it up and running. For ease of deployment, it was nothing like Splunk—Splunk was extremely easy to implement." What's more, in terms of cost compared to the other SIEM, "I would estimate Splunk is about 60 percent less," he adds.

## End-to-end visibility for quick intervention

With Splunk software in place, the company is now able to properly address growing security concerns, like potential ransomware or DDoS attacks. Having seen an uptick in security attacks against large businesses and the high-profile media attention that surrounds these breaches, it was critical for the company to prevent situations where customer data could be exposed. The team now has global visibility, so it can effectively monitor security events, point-of-sale systems and firewalls to detect and prevent any malicious activity.

**"With our old system, it could take anywhere from a couple of hours to a couple of days for a typical investigation. Now, with Splunk Cloud, it's only about 20 minutes."**

**Senior Manager, Information Security**

**"ArcSight took an extremely high degree of technical knowledge to get it up and running. For ease of deployment, it was nothing like Splunk—Splunk was extremely easy to implement."**

**Senior SOC Analyst**

"We implemented Splunk right after the ransomware trend started happening. Previously, our biggest issue was identifying who was logged into what system or which system was infected. We couldn't investigate without a lot of manual effort," says the senior SOC analyst. With knowledge of the typical words and file extensions tied to ransomware attacks, the team is now able to set up a Splunk search to identify and prevent potential ransomware threats.

## Taking full advantage of resources

The team is taking advantage of the Splunk user resource known as the Splunk Community, which includes Splunk Answers, Splunk Documentation, and more, all of which provide information and support to get the most out of Splunk deployments. What's more, Splunkbase Apps and Add-ons have helped the team solve additional challenges. For instance, the Splunk App for AWS has provided visibility that enabled the company to identify and shut down two unused private cloud networks. Meanwhile, the DNS Analytics for Splunk App helps the team identify compromised hosts, and even pinpoint unusual activity, including one instance where individuals were mining Bitcoins.

Since deploying the Splunk platform, feedback from people in the organization has been extremely positive. The team is leveraging Splunk more broadly, to assist network teams on outages, and to monitor disk space on point-of-sale systems and on systems running low on memory or high on CPU utilization, to ensure action can be taken before unnecessary downtime results in lost company revenue.