CASE STUDY

Online Content Specialist Boosts Security With Splunk Cloud

BRIGHTEDGE

Executive summary

As a search engine optimization and content marketing performance company, BrightEdge needs to ensure its 1,500-plus global customers trust its award-winning software as a service (SaaS) platform, so maintaining a secure environment is paramount. That's why BrightEdge uses Splunk Cloud running on Amazon Web Services (AWS) for security information and event management (SIEM). Since deploying Splunk solutions for analytics-driven security, the company has seen benefits including:

- Correlation with multiple data sources and no need to build multiple apps
- Seamless integration with Salesforce.com and other cloud applications
- Helps compliance with ISO 27001 and other security standards

Why Splunk

"In this age of cybersecurity threats, you don't know what vulnerabilities you may have," explains Jae An, BrightEdge head of information security. In addition to a mix of vulnerability scanning and anti-malware tools as well as its own software, the firm relies on an incident response process to monitor operations, detect problems and respond quickly. Rather than waiting until a customer encounters a website problem or a denial-of-service attack threatens, BrightEdge has Splunk Cloud, a companywide solution for log management and real-time security investigation.

"As a cloud-first company without a large IT department, we use pretty much all of the best-of-breed SaaS products, from NetSuite as a financial system to BambooHR for human resources," An says. After evaluating tools including Loggly and Sumo Logic, An says, BrightEdge realized that Splunk Cloud, "is not just a SIEM system; it's a platform with an app for almost everything that I need."

After purchase, Splunk Cloud was up and running within a day, giving visibility into logs and correlation with multiple data sources that BrightEdge's previous solution couldn't offer: "If I had to use Graylog to do what I'm doing with Splunk Cloud, I would probably have to build at least five different applications on my own and hire another two headcounts," says An.

Industry

- Online services

Splunk Use Cases

- Cloud solutions
- Security and fraud
- Log management
- IT operations management

Challenges

- Limited visibility into logs
- No correlation with multiple data sources
- Need to maintain security with lean IT resources

Business Impact

- Immediate impact, time and headcount savings compared to generic log management
- Discovered unauthorized access attempts and malware
- Smorgasbord of apps and add-ons for integration with other workflows

Data Sources

- Server logs
- AWS CloudTrail
- VPC Flow Logs
- Amazon Inspector
- OSIDS (Open Source Intrusion Detection Systems)
- Rapid7
- Salesforce
- Dropbox

Splunk Products

- Splunk Cloud
- Splunk App for AWS
- Splunk App for Salesforce
- Splunk Add-on for Symantec Endpoint Protection

Protecting customer data in the cloud

Like many other midsized businesses, BrightEdge relies on Salesforce.com for customer relationship management, and the Splunk App for Salesforce to gain insight into the CRM platform's adoption, usage and security.

"We recently had one of our employees compromise her access," An recalls. "She didn't know that she had an issue until an (unnamed) organization tried to use her credentials to access our Salesforce application. Splunk Cloud detected that immediately, and we were able to respond quickly so we didn't lose any data."

Similarly, Splunk Cloud detected that two end-user computing devices in the office were vulnerable to threats, after talking to hostile websites outside of the organization. Initially, security team members suspected that two employees might have been browsing inappropriate websites, but not only was that not the case, they weren't even using their computers at the time of the breach. It turned out that it was only when the PCs were idle that they were talking to malicious websites in a UDP channel. An and team realized that, "The endpoint security software we had at the time didn't detect the malware, so we immediately replaced it. Without Splunk Cloud we probably wouldn't have known."

"They asked about its cost in the beginning, but a few months ago, Splunk Cloud helped us stop a data breach. When that happened our execs, our CFO and everybody, said, 'Oh, I get it.' So yes, our Splunk investment has definitely paid off."

Jae An Head of Information Security, BrightEdge

"Now I can do a security investigation in less than an hour. I can't believe what Splunk Cloud can do; it's achieving the impossible."

Jae An Head of Information Security, BrightEdge

Bringing SIEM within reach

SIEMs can take a long time to get up and running. According to An, "Implementing a security incident response and threat monitoring system can take months, or sometimes in large organizations, even up to a year."

However, midsized and smaller organizations are generally more agile and need to deploy a system right away. Combining Splunk Cloud with available apps is the most direct path to a quick solution. "It can be customized as needed, without having to reinvent the wheel."

When using a prior homegrown tool in the past, a typical security investigation involving large logs and text files would take days. "Now I can do a security investigation in less than an hour. I can't believe what Splunk Cloud can do; it's achieving the impossible," comments An.

A security Swiss army knife

Looking ahead, An anticipates bringing online the Splunk Add-on for Symantec Endpoint Protection, fine-tuning its use of the Splunk App for AWS and refining the automated monitoring and intelligent alerts that help the company keep its ISO 27001 compliance.

"A resource like Splunk Cloud helps me do my job and enables our organization to be compliant. Without it, I could not be responsible or accountable for security within BrightEdge," An concludes.

About AWS: For 10 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud service. AWS offers over 70 fully featured services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 35 Availability Zones (AZs) across 13 geographic regions in the U.S., Australia, Brazil, China, Germany, Ireland, Japan, Korea, Singapore, and India. AWS services are trusted by more than a million active customers around the world – including the fastest growing startups, largest enterprises, and leading government agencies – to power their infrastructure, make them more agile, and lower costs. To learn more about AWS, visit http://aws.amazon.com.

About Splunk: Splunk Inc. provides the leading software platform for real-time Operational Intelligence. Splunk software and cloud services enable organizations to search, monitor, analyze and visualize machine-generated big data coming from websites, applications, servers, networks, sensors and mobile devices. More than 13,000 enterprises, government agencies, universities and service providers in over 110 countries use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, prevent fraud, improve service performance and reduce costs. Splunk products include Splunk® Enterprise, Splunk Cloud™, Splunk Light and premium solutions. To learn more, please visit http://www.splunk.com/company.

aws | splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

CS-Splunk-BrightEdge-AWS-Cobrand-102