CASE STUDY

EnerNOC Gains Visibility into AWS Environment, Turns Data into Real-Time Security Insights

Executive summary

EnerNOC is a Boston-based provider of energy intelligence software for the largest consumers of energy on the electrical grid, with customers in locations spanning the globe. EnerNOC is fully deployed on Amazon Web Services (AWS) and requires single-pane-of-glass visibility into all of its AWS accounts, activity and usage at a precise level in order to ensure strict adherence to security best practices. Since deploying the Splunk App for AWS, EnerNOC has seen benefits including:

- Increased visibility into its AWS environment including data from AWS CloudTrail & AWS Config
- Real-time security insights
- Streamlined implementation of security best practices

Why Splunk

EnerNOC helps its customers make better decisions around energy usage and spend. A critical element of EnerNOC's ability to do this is processing and analyzing large amounts of data. In addition to deploying Splunk Enterprise, EnerNOC also chose the Splunk App for AWS for its ability to provide real-time visibility across all of its AWS environments.

EnerNOC initially began using the Splunk App for AWS to view AWS CloudTrail data to perform user analytics and look at web access logs. As its architecture evolved, EnerNOC began analyzing data from additional services such as Amazon Simple Storage Service (Amazon S3) and Elastic Load Balancing. After seeing how easy it was to bring this data into Splunk, EnerNOC extended the Splunk App for AWS into all of its accounts, pulling in Amazon CloudTrail data from all regions as well as Amazon CloudWatch data for specific accounts.

In addition to using the Splunk App for AWS to improve the security posture of workloads on AWS, EnerNOC also uses it to monitor its service billing data. This helps the company keep an eye on costs, and supports budgeting and cost planning for its customers.

Industry

- Energy and Utilities

Splunk Use Cases

- Security and fraud
- Log management
- Cloud solutions

Challenges

- Wanted an aggregate view of large-scale AWS deployment as well as individual user and resource activity on AWS
- Needed to strengthen security posture for itself and its customers
- Required a scalable cloud solution for log analysis

Business Impact

- Able to implement and automate security best practices for itself and its customers
- Gained full operational visibility into AWS accounts, activity and usage to improve overall security posture
- Able to triage and resolve security issues in real time
- Mitigate risk of production outages
- Saving its customers tens of thousands of dollars through real-time monitoring of billing data

Data Sources

- AWS CloudTrail, AWS Config, VPC Flow Logs
- Amazon CloudWatch data
- Elastic Load Balancing logs
- Sensor data
- Web server logs
- Billing data

Splunk Products

- Splunk Enterprise
- Splunk App for AWS

Promoting real world security best practices

Through access to a pre-built suite of dashboards and reports, and with real-time visibility into its AWS environment with the Splunk App for AWS, EnerNOC is able to internally promote security best practices across the organization as well as to its customers, and maintain its part of the AWS Shared Responsibility Model for security. EnerNOC has strengthened its security posture by setting up alerts based on specific user activities that increase security risk, such as using API keys instead of instance roles. This is especially powerful in a situation where API access keys accidentally end up in the wrong hands, or are checked into an open-source project. In this situation, EnerNOC can identify and respond within minutes to deactivate the key in question, potentially saving tens of thousands of dollars, as well as limiting the impact of a potential breach. Without the Splunk App for AWS, EnerNOC would have no way of knowing the API key was compromised until seeing an increase in costs on a bill, up to 30 days later. At that point, the team would need to manually sift through thousands of events to find the source of the issue. In addition, the Splunk App for AWS has enabled EnerNOC to create a baseline for normal vs. abnormal activity usage patterns. Whenever EnerNOC notices spikes in certain types of API usage or error rates, the company can use the Splunk App for AWS to determine the cause of the error and proactively notify its customers.

Helping ensure a secure AWS deployment

Security and visibility are critical considerations in any AWS deployment. The Shared Responsibility model at AWS means that AWS manages security of the cloud, while security on the cloud is the responsibility of the customer. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks, just as they would for applications in an on-site datacenter. The Splunk App for AWS makes it easier for EnerNOC to properly manage its responsibility in the AWS Shared Responsibility model.

"Having all of our Amazon CloudTrail data loaded into Splunk software makes it easy to quickly dig down into the raw data to detect and alert on any kind of abnormal access. Operational visibility into our environment with the Splunk App for AWS has really helped us with problem detection and mitigation."

Jim Nichols, Principal Engineer
EnerNOC

EnerNOC uses the Splunk App for AWS to achieve real-time visibility into its thousands of Amazon Elastic Compute Cloud (Amazon EC2) instances across many regions. EnerNOC also uses services such as Amazon S3, Elastic Load Balancing, AWS Lambda, Amazon Kinesis, and Amazon DynamoDB. With the Splunk App for AWS, EnerNOC is able to gain information from data that was previously opaque or disjointed.

About AWS: For 10 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 70 fully featured services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 33 Availability Zones (AZs) across 12 geographic regions in the U.S., Australia, Brazil, China, Germany, Ireland, Japan, Korea, and Singapore. 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.

CS-Splunk-EnerNOC-AWS-Cobranded-107