CASE STUDY

REI, Inc. Gains Edge Protection with Splunk Cloud and AWS

Executive summary

National speciality outdoor retailer, Recreational Equipment, Inc. (REI) believes a life outdoors is a life well lived. And, as an organization known for its customer service and brand reputation it comes as no surprise that REI wanted to extend its security posture to include edge protection of its Amazon Virtual Private Clouds (VPCs) as it migrated applications to Amazon Web Services (AWS). REI deployed Splunk Cloud and Amazon GuardDuty managed threat detection service across its hybrid environment and has seen benefits including:

- Gaining end-to-end security visibility during AWS cloud migration
- Real-time insight into potential threats
- Enabling a security-oriented mindset through DevSecOps transformation

Why Splunk

At REI, the technology organization comprises approximately 400 people across security, application, core infrastructure and DevOps. Previously, the organization lacked a solid investigation workflow that included its AWS deployment, so teams underwent a time-consuming process — up to a week — to log into multiple accounts used by various departments, export data into files, and aggregate and analyze spreadsheets with many tools and no formal process. What's more, REI lacked a secure ingress path for migrating applications to AWS, and the company needed to solve this security challenge. Furthermore, REI is undergoing an organizational transformation by implementing a DevSecOps practice across the enterprise that centralizes and standardizes the security solutions across all REI accounts and VPCs. This allows REI developers to not focus on foundational security within AWS and instead focus on shipping business capabilities.

REI underwent a proof of concept (POC), centralizing log management and edge protection services from across the digital community and security teams. "We quickly demonstrated the standalone capabilities of Splunk, AWS Shield, and Amazon GuardDuty, but also the benefit of using Amazon GuardDuty in conjunction with Splunk for fast, insightful security intelligence," says David Bell, who manages infrastructure and cloud services at REI.

Now, security, application, core infrastructure and DevOps teams have access to Splunk Cloud to enable them to make decisions driven by analytics, and with enough context to minimize risk while ensuring availability for customers.

"We want to protect REI data — that's where we put our resources and invest time," Bell continues. "Procuring Splunk Cloud has been a really good investment, not just for the capabilities it offers but also for the time savings."

Industry

- Retail

Splunk Use Cases

- Security monitoring
- Advanced threat detection

Challenges

- Needed to close a security gap during cloud migration

Business Impact

- Gaining real-time visibility across applications, services, and security infrastructure
- Providing threat intelligence, alerting, security monitoring and troubleshooting
- Enhancing edge security as applications migrate to AWS
- Fast time to value and ease of use reduces staffing challenges

Data Sources

- Amazon Virtual Private Cloud
- AWS Application Load Balancer (ALB)
- Amazon GuardDuty
- AWS Config
- Amazon CloudWatch

Splunk Products

- Splunk Cloud
- Splunk Enterprise Security
- Amazon GuardDuty Add-on for Splunk
- Splunk App for AWS
- Splunk Add-on for Amazon Web Services

End-to-end security visibility

As REI undergoes its cloud migration, it has met the requirements for using native-AWS security solutions at the edge, which helps the development community to attach a security solution to public endpoints programmatically. With Splunk Cloud, Splunk Add-on for Amazon Web Services, Amazon GuardDuty Add-on for Splunk, and Splunk App for AWS, REI has security visibility and alerting across the environment.

As REI aggregates all security-relevant machine data in Splunk Cloud, the technology organization is getting answers. "The largest gain was through securing at the edge," Bell says. "This removed the need for individual dev teams to come up with edge protection models for public-facing endpoints. Splunk is helping us aggregate the Amazon VPC flow logs, AWS Application Load Balancer logs and Amazon GuardDuty logs for easy correlation, visualization and alerting."

With Amazon GuardDuty, AWS Shield managed Distributed Denial of Service (DDoS) protection service and AWS Web Application Firewall (AWS WAF), REI has met its intrusion detection system (IDS) and security requirements for blocking common exploits.

An evolving and maturing security model

According to Rick Adams, senior systems engineer at REI, GuardDuty Add-on for Splunk is a welcome addition because the security team does not have to log into different AWS accounts to monitor GuardDuty alerts. Instead, GuardDuty Add-on for Splunk dashboards enable the security team to filter through alerts for all accounts and get to critical information in real time. Additionally, Splunk integration streamlines ingestion of GuardDuty security findings from across regions and accounts, which provides security teams with additional context for early detection, rapid investigations and remediation of potential threats.

"The largest gain was through securing at the edge. This removed the need for individual dev teams to come up with edge protection models for public-facing endpoints. Splunk is helping us aggregate the Amazon VPC flow logs, AWS Application Load Balancer logs and Amazon GuardDuty logs for easy correlation, visualization and alerting."

David Bell
Manager, Infrastructure and Cloud Services, REI

By adopting Splunk Cloud and AWS services, REI can gather events and aggregate them for DevSecOps assessment and response. "As we developed our DevSecOps practice within REI, we've ensured that all centralized security and other standard capabilities were built into our infra code pipeline using Terraform and Jenkins. This has guaranteed that as we stand up a new account or VPC, they are all fitting the same standards and being added into our Splunk Cloud solution through a pipeline-based deployment model," Adams says.

Ease of use reduces staffing challenges

According to the REI team, another added benefit of the Splunk platform is that the Splunk Search Processing Language (SPL) is well-known, and it's easy to get staff up to speed — even for those that lack familiarity. "We don't need to take somebody who's new and train them up on Splunk," Bell concludes. "It's this generic capability that's specific now to AWS security, and that's powerful for us. It's all about that time to market."

"We want to protect REI data — that's where we put our resources and invest time. Procuring Splunk Cloud has been a really good investment, not just for the capabilities it offers but also for the time savings."

David Bell
Manager, Infrastructure and Cloud Services, REI

About AWS: For over 12 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 125 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management from 55 Availability Zones (AZs) within 18 geographic regions and one Local Region around the world, spanning the U.S., Australia, Brazil, Canada, China, France, Germany, India, Ireland, Japan, Korea, Singapore, and the UK. AWS services are trusted by millions of 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 https://aws.amazon.com.

About Splunk: Splunk Inc. (NASDAQ: SPLK) turns machine data into answers. Organizations use market-leading Splunk solutions with machine learning to discover their "aha" moments with machine data and solve their toughest IT, Internet of Things and security challenges. Use Splunk software in the cloud and on-premises to improve service levels, reduce operations costs, mitigate security risks, enable compliance, enhance DevOps collaboration and create new product and service offerings. Join millions of passionate users by trying Splunk software for free: www.splunk.com/free-trials.

CS-Splunk-REI-AWS-Cobrand-102