TrueCar Drives Log Management, Application Delivery and Security Success With Splunk Cloud and Amazon Web Services

TRUECar

Executive summary

TrueCar, a digital automotive marketplace, provides comprehensive automotive pricing transparency. While migrating its technology infrastructure to the cloud, the company required a log management and infrastructure monitoring solution that could scale and support cross-functional searching and reporting to manage and troubleshoot its complex IT environment. TrueCar discovered additional uses for the Splunk platform, including application delivery and security. Since deploying Splunk Cloud running on Amazon Web Services (AWS), TrueCar has seen benefits including:

- Immediate value from deploying Splunk Cloud in one day and gaining real-time insights
- Accelerating software and product development
- Providing additional visibility into AWS billing
- Security insights and threat detection

Why Splunk

According to David Giffin, senior vice president of the technology platform at TrueCar, the company's technology platform encompasses everything that sits on top of AWS. His team is responsible for all of the infrastructure, deploying the code out to that infrastructure and ensuring that all daily operations run smoothly. "My teams include the infrastructure team, the team that manages our internal deployment tool that we call Spacepods, the team responsible for our data warehouse and data movement and the business intelligence team."

TrueCar had set up ELK (Elastic Stack) "because it was an open-source tool we could run in our environment," Giffin says. "Our infrastructure team spent many hours maintaining ELK. By moving to Splunk Cloud, we were able to free up our infrastructure team's time to tackle other problems."

Initially, the infrastructure team completed a proof of concept to evaluate log management solutions, including side-by-side comparisons of searches conducted on Splunk Cloud and ELK. "We wanted to not manage any of it and Splunk Cloud allowed us to do that," Giffin says. "Once that was done we told everybody, 'We're shutting down ELK and the dashboards need to migrate.'"

Industry
- Online services

Splunk Use Cases
- Log management
- IT operations
- Application delivery
- Security

Challenges
- Open-source log management tool that was time-consuming to maintain
- Wanted to improve security posture
- Wanted additional business insights, including AWS billing and application delivery

Business Impact
- Deploying Splunk Cloud into production in one day
- Speeding software development
- Providing security insights, improving threat detection
- Repurposing data across teams for better business insights
- Providing visibility into AWS billing

Data Sources
- AWS Kinesis, CloudWatch, CloudTrail, CloudFront, Config and AWS billing data
- New Relic
- Jenkins
- Salesforce
- Okta

Splunk Products
- Splunk Cloud

Repurposing data for business insights

The Spacepods team integrated Splunk Cloud into its tool set, quickly relying on it for monitoring all core infrastructure and application delivery across the organization. From there, a lot of reporting moved into Splunk Cloud. The infrastructure team created dashboards to provide visibility into AWS billing. This enabled the team to better control costs and allocate resources effectively throughout TrueCar's cloud migration without needing to manage the infrastructure. "Given the fact that we already had all of our logs flowing through the (AWS) Kinesis stream, we just pulled those same log messages off the stream and put them into Splunk. We were able to deploy Splunk into production in one day," Giffin says.

Giffin explains that Splunk Cloud adoption happened very rapidly, with TrueCar's security team creating several valuable dashboards that enabled them to monitor and prevent malicious exploits. Soon after, other teams began to repurpose the same data sources for important business insights.

Today, having Splunk Cloud across various teams means that everyone has the same data sources at their fingertips, enabling collaboration on dashboards that shed light on how the business operates. People across all technology teams rely on Splunk Cloud. Key

"Having Splunk Cloud enables our developers to get insights into what their applications are doing, and that's invaluable."

David Giffin
Senior Vice President, Technology Platform, TrueCar

"Splunk Cloud just works, and it's one of the things that people rely on day to day."

David Giffin
Senior Vice President, Technology Platform, TrueCar

areas for usage include the infrastructure team, which is responsible for shipping the logs out to Splunk, and the Spacepods team. "Through the creation and deployment of Pods, we surface up Splunk links that allow you to filter the logs specific to a given environment or a given Pod," Giffin explains.

Built to scale

Every new application that TrueCar developers build has logs, and they all end up in Splunk Cloud. Currently, more logs are indexed in Splunk Cloud than previously with ELK, and the solution handles the traffic with ease. "Splunk Cloud just works, and it's one of the things that people rely on day to day,"Giffin says.

As the company makes the migration to the cloud, Giffin says, "having Splunk Cloud as a platform enables our developers to get insights into what their applications are doing, and that's invaluable. Having ready access to logs, a longer retention period than we had with ELK and not having to maintain our logging infrastructure makes Splunk Cloud a big win."

"Compared with ELK, Splunk has more search and visualization capabilities."

David Giffin
Senior Vice President, Technology Platform, TrueCar

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.