Running workloads in any cloud environment is not a “set it and forget it” endeavor. You need to monitor the performance, usage, security and availability of your cloud infrastructure continuously. And with the right solutions, it’s possible to manage your IT systems and derive actionable insights from all of your data in one place, even if you’re running workloads in hybrid environments.

In addition to running your business smoothly, you also need to protect against threats and anticipate the unknown. With a rapidly changing security landscape, every organization needs to safeguard customer and employee information, protect intellectual property, innovations—and your competitive advantage. With an analytics-driven security approach, you can gain end-to-end security visibility with the added capabilities of data science and machine learning to detect and respond to threats at machine speed.

At Splunk, we make it easy for our customers to turn mountains of machine data in their AWS and hybrid environments into valuable business, operational and security insights that improve their businesses. And we trust AWS to run our own cloud service—Splunk Cloud. Read this e-book to see some great customer examples—and get inspiration for what you can do for your organization.
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.

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
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.”

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.

“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

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.

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.”
FINRA Protects American Investors With Splunk Cloud and AWS

Executive summary
FINRA — the Financial Industry Regulatory Authority — regulates one critical part of the securities industry — brokerage firms doing business with the public in the United States. FINRA processes and analyzes massive amounts of data, and one challenge is to protect that data against new and unexpected threats. FINRA’s security information and event management (SIEM) solution, despite high costs, was providing limited functionality. Migrating to Splunk Cloud, Splunk Enterprise Security (ES) and Amazon Web Services (AWS) has provided FINRA with benefits including:

- The ability to ingest data from 170 different applications and run ad hoc queries
- Flexible scaling in a pay-per-use model matching cost to demand
- Unprecedented transparency into every aspect of the computing environment

Why Splunk
Every day in the United States, as many as 100 billion securities market financial transactions take place, involving billions of investors’ dollars. A Congressionally authorized not-for-profit organization, FINRA oversees market integrity.

“We bring in tons of data, every order, quote and transaction in almost every equities and options market in the United States, and we look for abnormalities,” says Gary Mikula, senior director of cyber and information security at FINRA. “There were so many other logs we wanted, like badge information and different access logs, and our SIEM couldn’t ingest that data. Secondly, it didn’t provide a flexible user interface allowing us to query the data how we wanted.”

Industry
- Financial Services

Splunk Use Cases
- IT Operations
- Security
- Log Management

Challenges
- Needed central logging and ad hoc querying capabilities for massive amounts of data from many different types of logs

Business Impact
- Ingest massive amounts of data from diverse access logs
- Run ad hoc queries with central logging, dashboard access
- Visibility into most U.S. stock and options market transactions
- Gain cost and operational efficiencies with Splunk on AWS
- Protect investors from fraud, foster market transparency

Data Sources
- Amazon Kinesis Data Firehose
- Amazon CloudWatch
- AWS CloudTrail
- AWS IAM
- AWS RDS
- AWS Config
- Amazon Simple Storage Service (S3)
- Amazon Elastic MapReduce (EMR)
- Windows and Linux Syslog data
- Firewalls
- VPN
- Proxies
- 170 enterprise applications

Splunk Products
- Splunk Cloud
- Splunk Enterprise Security
- Splunk App for AWS
Searching for a better solution, FINRA considered several SIEMs. The products could generate alerts, but they didn’t significantly improve data ingestion or analysis. Then Mikula attended SplunkLive! in Washington, D.C., and found what he was looking for — a means to capture, index and correlate big data from all of FINRA’s desired sources in real time, and customize queries through flexible dashboards.

“The competitors were playing catch-up to the capabilities that were already in Splunk,” Mikula says. “We didn’t want to play that game.”

**All-in on cloud**

Already impressed by the capabilities of Splunk Enterprise and Splunk Enterprise Security (ES), FINRA learned that Splunk Cloud had just come on the market and decided to become its first big customer. The pay-per-use cloud model lets FINRA match its computing costs to demand fluctuations. And instead of spending months building out an environment, FINRA leveraged the mature data-collection agents within Splunk to start consuming data within days of signing the contract. Today, Splunk ingests logs from 170 different applications and AWS Services, including Amazon Simple Storage Service (S3), Amazon CloudWatch, AWS Config and AWS CloudTrail. “No SIEM could match this,” Mikula says.

**Powerhouse design**

Magnifying the power of FINRA’s Splunk Cloud solution is integration with Amazon Web Services. AWS Lambda lets FINRA run code without provisioning or managing servers, paying only for the compute time consumed. Amazon Kinesis Data Firehose, a fully managed service, delivers real-time streaming data to Splunk. Mikula calls Amazon Kinesis Data Firehose an ideal solution for creating subscriptions filters to reliably, securely, quickly and cost-efficiently move AWS logs into the Splunk solution for analysis. This capability benefits developers and network staff as well as security specialists, bridging silos.

“It’s made a partnership between our security and operations teams,” Mikula says. “We have a common goal of wanting the same logs. Now we have a single place to ingest and consume them.”

“**We are putting our crown jewels — our ability to take every transaction every day on almost every U.S. stock and options market and analyze that data in the cloud — and we are using Splunk to assure that it is secure. Splunk and AWS together give us an unparalleled ability to protect investors.**”

Gary Mikula
Senior Director, Cyber and Information Security, FINRA

Such efficiencies keep FINRA ahead of evolving threats by enabling teams to analyze data flexibly. FINRA is one of the biggest users of Amazon’s EMR Hadoop framework; deploying the Splunk agent onto this platform-as-a-service provides information that allows FINRA to optimize resource allocations. What’s more, FINRA sunset a dedicated third-party billing tool and replaced it with its own process for ingesting the data into Splunk. With Splunk Cloud, FINRA has better analytics and reporting, which has led to better project tracking of AWS Services and reduced costs. “We are more effectively managing our cloud costs using our Splunk solution and at less than five percent of the dedicated tools price tag,” Mikula adds.

In addition to its commitment to cloud computing, FINRA embraces open source software development, sponsoring multiple open source projects in big data, DevOps and quality assurance. Mikula’s team even built a tool to collect AWS CloudTrail logs and ingest them into Splunk.

Pursuing such innovations as serverless computing in the cloud, FINRA finds that it must track logs more than ever. “You can never know what the next threat will be and what questions we’ll want to ask our data. Splunk allows us to easily collect all the data we want and query it ad hoc,” Mikula says. “What’s more, the insights from Splunk allow us to use more AWS services. We are putting our crown jewels — our ability to take every transaction every day on almost every U.S. stock and options market and analyze that data in the cloud — and we are using Splunk to assure that it is secure. Splunk and AWS together give us an unparalleled ability to protect investors.”
Autodesk Saves Time and CapEx Costs With Splunk on AWS

Executive summary
Customers across the manufacturing, architecture, building, construction and media and entertainment industries use Autodesk software to design, visualize and simulate their ideas. Given its large global footprint, Autodesk faced two distinct challenges: the need to gain business, operational and security insights worldwide across multiple internal groups, and the need to choose the right infrastructure to deploy Operational Intelligence software. Since deploying the Splunk platform, the company has seen benefits including:

• Savings of hundreds of thousands of dollars
• Critical operational and security-related insights
• Real-time visibility into product performance

Why Splunk
Splunk first found a home at Autodesk in 2007 as a way to harness machine data for operational troubleshooting. Today, that usage has expanded to include real-time monitoring, detailed security insights and executive-relevant business analytics across three Autodesk divisions, including:

Enterprise Information Services (EIS)—responsible for global corporate IT management, including information security and information management.

Autodesk Consumer Group (ACG)—responsible for all of Autodesk’s consumer-facing products.

Industry
• Technology

Splunk Use Cases
• Business analytics
• Cloud solutions
• IT operations
• Security

Challenges
• Needed to support large global footprint
• Wanted to gain in-depth business, operational and security visibility
• Avoid capital and labor costs required for on-premises infrastructure upgrade
• Ensure security and compliance across cloud environment
• Reduce time required to isolate and resolve security issues

Business Impact
• Save hundreds of thousands of dollars in capital costs, time and labor expenses
• Reduce operational effort by leveraging AWS CloudFormation templates and Ansible playbooks
• Deep insight into product performance, user preferences and usage metrics
• Resolve security issues and avoid the expense of a dedicated SIEM solution
• Gain visibility into AWS accounts and ensure security and compliance

Data Sources
• Thousands of global end points
• AWS CloudTrail
• Apache Kafka messaging broker
• Windows, Linux, Solaris servers
• Oracle, SAP, Siebel, TIBCO applications

Splunk Products
• Splunk Enterprise
• Splunk Enterprise Security
• Splunk App for AWS
Information Modeling & Platform Products (IPG)—responsible for Autodesk’s solutions for commercial customers, including designers and engineers across all industries.

Autodesk is using Splunk Enterprise Security (Splunk ES) to reduce the time to identify and resolve security issues. The company also uses the Splunk App for AWS to deliver and manage flexible resources for Splunk Enterprise and other critical applications.

**Splunk on AWS keeps the focus on service**

Given the global nature of its operations, an on-premises refresh of Autodesk’s Splunk environment would have required a team of eight, cost hundreds of thousands of dollars and taken months to complete. Instead, it took the Autodesk cloud architect just a few weeks to deploy Splunk Enterprise on AWS, saving more than half the capital costs and almost all the labor costs.

The Autodesk cloud architect created AWS CloudFormation templates and Ansible playbooks to provision Splunk on AWS. These services have reduced the total time to provision new end-to-end environments from hours or days to less than 30 minutes. As a result, Autodesk’s total operational effort to manage a global 1TB+ a day Splunk deployment across multiple divisions is less than 0.1 FTE.

AWS account visibility is required for each of the hundreds of AWS enterprise customers that are active at any given moment. To meet this challenge and ensure security and compliance, Autodesk leverages the Splunk App for AWS, integrated with AWS CloudTrail and AWS Config. The Splunk App for AWS is used to monitor account activity in real time and audit accounts regularly, delivering a centralized view into Autodesk’s AWS environment that enables rapid response and resolution of operational and security-related issues.

**“We need to move fast and develop products quickly. Deploying Splunk Enterprise on AWS meets that need in every way. From fast provisioning to quick deployment of new features, we don’t have to wait for anything.”**

Alan Williams  
Autodesk Consumer Group (ACG), Autodesk, Inc.

**Diverse divisions gain deep insight into operations and security**

Autodesk’s EIS group relies on Splunk Enterprise to help find, correlate and resolve errors occurring across critical applications. EIS uses Splunk ES to reduce the time needed to isolate and resolve security issues by up to 80 percent and to correlate system performance with security data. Splunk ES has also enabled Autodesk to avoid the cost of a more expensive, dedicated security information and event management (SIEM) solution.

The Autodesk ACG group depends on Splunk-derived business insights to provide executive-level visibility. The business development team, for instance, uses Splunk dashboards to understand the number of active users per project per month, where users are coming from and how the number trends month-to-month.

The IPG group uses Splunk analytics to understand product usage, including Autodesk A360. More than 300 IPG members use Splunk Enterprise to conduct product analytics for Autodesk’s Big Data Platform.
FamilySearch Moves to Continuous Delivery and Gains Real-Time Visibility for AWS Migration

Executive summary
Founded over 100 years ago, FamilySearch International is the largest genealogy organization in the world, hosting, maintaining and sharing genealogical records at FamilySearch.org and through over 4,600 family history centers in 132 countries. FamilySearch needed a way to move to a continuous delivery model, manage its all-in migration to Amazon Web Services (AWS) and immediately troubleshoot website errors. Since beginning its effort, the organization has seen benefits including:

- Successful migration from monthly releases to over 900 deployments per day
- Ability to re-allocate 12 developers to more value-added tasks
- Visibility into the AWS environment to support AWS migration strategy

Why Splunk
FamilySearch planned to move to a continuous delivery model on AWS to increase business agility and more rapidly deliver features to its customers. To do so, the company needed a monitoring service that could immediately detect changes across its website properties following the push of a new release. This service needed to support the cultural change to a DevOps deployment model. To meet this need, FamilySearch chose Splunk Cloud to help analyze logs from all components of its IT infrastructure.

Industry
- Online services
- Nonprofit

Splunk Use Cases
- Application delivery
  - DevOps
  - Cloud solution
  - IT operations management
  - Log management
  - Security

Challenges
- Wanted to increase update release frequency
- Needed to monitor and immediately detect changes to website to move to a DevOps model
- Issues with troubleshooting and keeping website stable

Business Impact
- Successful migration from monthly releases to 900 deployments per day
- Enables developers to easily see whether components are healthy
- Moved to a DevOps model and achieved continuous delivery
- Gained back 12 developers who were previously focused on implementing releases and keeping website running

Data Sources
- Amazon EC2
- AWS Elastic Load Balancing (ELB)
- AWS CloudTrail
- Amazon CloudWatch
- AWS Billing
- Routers
- Applications
- On-premises servers

Splunk Products
- Splunk Cloud
- Splunk App for AWS
- Splunk Enterprise
environment in real time, without additional developer effort. Leveraging Splunk Cloud, FamilySearch is now able to identify errors in real time and has successfully moved to continuous delivery with over 900 deployments per day.

FamilySearch pushes all of its log data through Splunk Cloud, including data from load balancers, routers, APM tools and the applications themselves. Then, a JIRA ticket is automatically created for bug tracking policies following any error. FamilySearch now ingests 3.5–4TB of data per day into Splunk Cloud. The organization is able to give all developers access to all production data—without necessarily granting access to the application servers—enabling staff to build dashboards to monitor the health of the site following a release and move from code check-in to deployment in under 20 minutes.

By deploying Splunk Cloud, FamilySearch gains the inherent benefits of a cloud service: elasticity, security and scalability, without the operational effort.

Improving developer speed, efficiency

Splunk Cloud is critical to FamilySearch’s shift to a DevOps model and enables developers to troubleshoot errors in real time. “Previously, we were doing monthly releases and struggling to get them built. Splunk Cloud has enabled us to see whether apps are running once we drop them into production—we now have immediate operational visibility whenever there’s any deployment issue. Without Splunk Cloud, we wouldn’t have been able to go to continuous delivery,” says Gary Stokes, director of Engineering, FamilySearch.

FamilySearch now leverages Splunk Cloud in all stages of its Software Development Life Cycle (SDLC). After pushing to production, developers leverage Splunk Cloud to assess the health of a component. This allows FamilySearch developers to rapidly resolve detected issues and iterate new application releases.

“Splunk Cloud has been more stable than our internal implementation and has freed up two resources to work on software development instead of managing infrastructure. It has clearly proven to be cost-effective compared to managing infrastructure ourselves.”

Gary Stokes
Director of Engineering, FamilySearch

After integrating Splunk Cloud into its workloads, FamilySearch was able to gain back 12 developers. With the easy-to-learn, yet powerful, Splunk search processing language (SPL), FamilySearch developers have been able to easily create dashboards.

Expanding use of Splunk solutions

FamilySearch is in the midst of migrating 100% of its applications to AWS. FamilySearch uses the Splunk App for AWS to gain real-time visibility into user operational and security-related activity in its AWS account, allowing the company to migrate to AWS with full visibility. The Splunk App for AWS provides this visibility by analyzing all AWS CloudTrail, AWS CloudWatch, and AWS Billing data in Splunk Cloud. In the future, FamilySearch plans to expand its usage of Splunk solutions to gain business analytics on patron behavior as well as real-time AWS cost management.

“Splunk Cloud has enabled us to gain immediate operational visibility whenever we deploy code. Without Splunk Cloud, we wouldn’t have been able to move to continuous delivery on AWS with over 900 deploys per day.”

Gary Stokes
Director of Engineering, FamilySearch
TrueCar Drives Log Management, Application Delivery and Security Success With Splunk Cloud and Amazon Web Services

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

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
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.’”

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 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... 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
New York Regional Education Agencies Unify Data to Improve Operations and Accelerate Student Learning

Executive summary
Technology is a key component of K-12 educational instruction and school district operations, but the challenge is how to use technology effectively while ensuring the privacy of sensitive student data. In New York state, a project called RIC One offers a family of services that provide end-to-end, fully automated data integration and single sign-on for applications that students, teachers and administrators use within school districts to improve school operations and classroom instruction. Since deploying Splunk Cloud and Splunk Enterprise for central log management and application monitoring, RIC One has seen benefits, including:

• Supporting districts statewide while ensuring student data privacy
• Eliminating time-consuming manual data entry processes
• Saving costs with easy-to-use and provision cloud solution
• Enabling small, distributed statewide team to work efficiently

Why Splunk
In New York, Boards of Cooperative Educational Services (BOCES) partner with school districts to provide shared educational programs and services that help meet the evolving educational needs of students. Currently, 12 Regional Information Centers (RICs) across the state, organized under BOCES, are collaborating on the RIC One project.

As the project got underway, the team responsible for infrastructure and operations needed to collect log data to monitor the many components that make up the RIC One

Industry
• Education

Splunk Use Cases
• Log management
• Application delivery
• IT operations
• Cloud solutions

Challenges
• Manual application administration and login was time-consuming for teachers
• Required centralized log management solution to monitor application performance
• Needed to ensure secure student data management

Business Impact
• Enhances overall educational experience with simplified access to relevant applications at any time
• Easier user and application management reduces IT burden
• Promotes efficiencies and enables districts to implement new IT solutions with ease
• Ensures security of student and teacher data across districts
• Cloud solution is easy to use, provision and is cost-effective

Splunk Products
• Splunk Cloud
• Splunk Enterprise
• Splunk App for AWS
• Splunk for OpenAM App
technology stack. The team relies on several open-source tools and initially considered various options for log aggregation and data visualization. The team selected Splunk Cloud because of its need for a central logging solution, since the components of the stack are deployed, in part, to both Amazon Web Services (AWS) and local infrastructures in all of the RICs throughout New York state. A key benefit of Splunk Cloud was that it required fewer servers for the team to maintain and administer.

Centralized application monitoring
RIC One has developed an Application Programming Interface (API) that provides education application developers with an easy and consistent way to access data, including class roster data, while enabling school districts to retain complete control of privacy and security for their students and staff. Data is partitioned into 12 regional data providers hosted within the private cloud of the RICs. The RIC One team also developed RIC One LOGIN, which gives students and staff single sign-on capability for logging in to instructional and administrative apps and significantly saves time versus older processes that required teachers to enter student information manually.

The RIC One infrastructure team builds technology stacks for VMware and Microsoft Hyper-V, and also uses Docker and several other solutions. Once a RIC deploys a stack into its infrastructure, the RIC One infrastructure team no longer has visibility into it. Therefore, the only way the RIC One team can get visibility into its applications to see how they are performing and to troubleshoot is to have centralized application management.

“We don’t have access to these sites where our applications are running. So when normalization of student data is encountering errors, or when the API isn’t responding as we thought, having those applications log centrally and having those alerts and dashboards right in front of us has been huge. We’re such a small team, so it would be more expensive if I had to dedicate a guy to manage, run and build visualizations, whereas with Splunk Cloud it was ‘set it, forget it and it works.’”

Staff Member, RIC One

“We don’t have access to these sites where our applications are running. So when normalization of student data is encountering errors, or when the API isn’t responding as we thought, having those applications log centrally and having those alerts and dashboards right in front of us has been huge.” says a RIC One staff member. “We’re such a small team, so it would be more expensive if I had to dedicate a guy to manage, run and build visualizations, whereas with Splunk Cloud it was ‘set it, forget it and it works.’”

Staff Member, RIC One

Proactive monitoring, alerts and visualizations add value
RIC One relies on Splunk Cloud for proactive log monitoring and ensuring that processes are running and succeeding every day. Splunk Cloud alerts the team if one of the processes fails, enabling them to resolve issues quickly. In addition to Splunk Cloud, the RIC One infrastructure team relies on Splunk Apps, including the Splunk App for AWS, which offers critical insights into its AWS account. In addition to Splunk Cloud and Splunk Apps, the RIC One project is also running Splunk Enterprise on-premises to safeguard students’ personally identifiable information.

According to the RIC One team, the ability to demonstrate the project’s successes to a superintendent or a director of technology has been gratifying. For example, when the team created a graph to show that they have authenticated 12,000 people and connected them to 36 different applications in the last 30 days, they received extremely positive feedback.

“I don’t think we could be operating without Splunk. If we had to manually go to these different places to find this information and do data correlations without the notifications, we wouldn’t be where we are,” says the RIC One staff member. “Splunk is so powerful that if you have all that information there, what you can do with it is just endless.”
Innovative Cloud-Based SIEM Deployment Delivers Actionable Security Intelligence for Equinix

Executive summary
Equinix, Inc. (Nasdaq: EQIX) connects the world’s leading businesses to their customers, employees and partners in 33 markets across five continents. Security is of paramount importance at Equinix as thousands of companies worldwide rely on Equinix datacenters and interconnection services. To gain a unified view across its security infrastructure, Equinix needed a cloud solution with centralized visibility and SIEM functionality that could be implemented easily, quickly and without significant operational effort. Since deploying Splunk Cloud and Splunk Enterprise Security (ES), Equinix has seen benefits including:

• Full operational visibility
• Enhanced security posture
• Time and cost savings

Why Splunk
To deliver the highest levels of security and data protection to its customers, Equinix implemented a multi-faceted global security infrastructure. However, the company lacked a unified view across this infrastructure and had to rely on alerts and reports from each individual system. To gain insight into security events, Equinix had to extract and correlate the data manually—a very time-intensive process that made sub-optimal use of limited security personnel and resources. It was essential for Equinix to gain centralized visibility and that its SIEM solution be deployed as a cloud service.

Industry
• Technology

Splunk Use Cases
• Security

Challenges
• Lacked unified view into multi-faceted global security infrastructure
• Manual process for extraction and correlation of data was time and resource intensive
• Wanted centralized visibility and SIEM functionality
• Needed to accelerate time-to-value with cloud SIEM solution

Business Impact
• Gained operational visibility across infrastructure
• Full SIEM functionality to aggregate and correlate data from all security systems
• Innovative cloud SIEM deployment provides cost-and time-savings over traditional SIEM solutions
• 30 billion raw security events reduced down to about 24,000 indicators of compromise, to 20 actionable alerts
• 50 percent TCO savings compared to an on-premises based legacy SIEM deployment
• Achieved 30 percent faster response to security incidents
• Enhanced security posture
• Provide the foundation for planned SOC

Data Sources
• Firewalls, VPNs and other security systems
• Intrusion Prevention and Detection Systems
• F5 load balancers
• Host-based intrusion management platform
• Microsoft Active Directory
• Salesforce.com
• UNIX and Windows servers

Splunk Products
• Splunk Cloud
• Splunk Enterprise Security (ES)
Splunk Cloud met all of Equinix’ requirements for a cloud service that could aggregate the information from all of its security technologies and easily handle multiple types of data, speeds and feeds. “Splunk Cloud’s 100 percent uptime SLA and its SOC2 Type 2 certification gave us the confidence to forward our critical data offsite,” says George Do, CISO, Equinix. “With Splunk Cloud we had value immediately.”

Equinix also utilized Splunk ES with Splunk Cloud as its SIEM solution. According to Do, “For years, we have been very vocal about the benefits of adopting a ‘SIEM in the cloud’ strategy. With Splunk Enterprise Security, we now have a secure, cost-effective SIEM with the functionality and scalability to underpin our planned SOC. Having it in the cloud means we have also eliminated the numerous hassles involved with deploying and then maintaining an onsite SIEM implementation.”

**Overarching visibility into infrastructure with Splunk Cloud and Splunk Enterprise Security**

Before Splunk Cloud, Equinix was overwhelmed by more than 30 billion raw security events generated every month. With Splunk Enterprise Security and Splunk Cloud, the security team can now reduce the 30 billion raw security events down to about 24,000 indicators of compromise, and then to 20 actionable alerts, thus providing actionable security intelligence and the foundation for a dedicated SOC.

With all the data aggregated within the Splunk platform, the security team can cross-reference data between systems, enabling them to research, investigate and respond to incidents 30 percent faster than before. “Our ultimate goal is to protect our customers, employees and data. With ES and Splunk Cloud as our SIEM platform, the information we want is always at our fingertips,” says Do.

“Whenever we need to investigate an incident, we simply display the relevant data in Splunk dashboards, so the information can be accessed by everyone on our security team as well as our C-level executives. The savings in time and effort are huge, as is the savings of 50 percent in total cost of ownership (TCO) compared to deploying a traditional on-premises based SIEM.”

“From day one, Splunk Cloud has given us actionable, data-driven intelligence. With Splunk Enterprise Security in the cloud, we’re getting comprehensive SIEM functionality, the economics and simplicity of software as a service, and outstanding availability and security. As more employees use the Splunk platform, we’re sure to find important new use cases beyond securing our infrastructure.”

George Do
CISO, Equinix

Thanks to Splunk Enterprise Security, Equinix is now armed with comprehensive security analytics. For example, whenever a user account shows signs of suspicious activity, such as a local employee unexpectedly logging in from another continent, high priority alerts are immediately triggered and sent to the security team. Also, using Splunk Cloud with ES enables Equinix to prevent the leakage of sensitive business information. In particular, administrators use correlations to determine whether a departing employee might be seeking to steal confidential data.

**Expanding value across the enterprise**

The usefulness of Splunk Cloud at Equinix extends far beyond the security team. Upper management, including the CIO, uses Splunk dashboards and analytics to monitor the firm’s security posture. Additionally, the company’s infrastructure team is looking to deploy the Splunk platform to monitor the health of its applications, and the DevOps team is considering Splunk Cloud to optimize application performance, track key performance indicators (KPIs) and receive critical alerts.

“From day one, Splunk Cloud has given us actionable, data-driven intelligence,” concludes Do. “With Splunk Enterprise Security in the cloud, we’re getting compelling SIEM functionality, the economics and simplicity of software as a service, and outstanding availability and security. As more employees use the Splunk platform, we’re sure to find important new use cases beyond securing our infrastructure.”
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 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

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
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.

**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 can internally promote security best practices across the organization and 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.

“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

**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.

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.
City of Los Angeles Integrates Real-Time Security Intelligence Sharing Across 40+ City Agencies

Executive summary
To protect its digital infrastructure, the City of Los Angeles requires situational awareness of its security posture and threat intelligence for its departments and stakeholders. In the past, the city’s more than 40 agencies had disparate security measures, complicating the consolidation and analysis of data. Los Angeles sought a scalable SaaS security information and event management (SIEM) solution to identify, prioritize and mitigate threats, gain visibility into suspicious activities and assess citywide risks. Since deploying Splunk Cloud and Splunk Enterprise Security (ES), the city has seen benefits including:
- Creation of citywide security operations center (SOC)
- Real-time threat intelligence
- Reduced operational costs

Why Splunk
Los Angeles is a vast metropolis with critical infrastructure like airports, seaports, and water and power, as well as 35,000 employees and over 100,000 endpoints generating 14 million security events daily. Its departments had their own security tools, requiring the city to gather and manually correlate logs from each agency for broad views of its network security. This process was cumbersome, imprecise and slow to address threats.

“Our mayor issued an executive directive to improve cybersecurity,” says Timothy Lee, chief information security officer for Los Angeles. “This meant collecting and evaluating all of our logs in real time. We needed a scalable SIEM to drive an integrated, citywide SOC.”

Industry
- City government

Splunk Use Cases
- Security

Challenges
- Disparate logs from over 40 departments were difficult to aggregate
- Inadequate situational awareness of security events
- Limited threat intelligence
- Slow responses to security incidents
- Modest IT resources

Business Impact
- Real-time, citywide, 24/7 network surveillance
- Stronger protection of digital assets and infrastructure
- Proactive network safeguards
- Shared threat intelligence with federal agencies
- Reduced headcount and lower operational costs
- Preservation of public trust

Data Sources
- Firewall logs
- FireEye Threat Prevention Platform
- Intrusion prevention/detection systems
- External threat intelligence feeds
- Switches and routers

Splunk Products
- Splunk Cloud
- Splunk Enterprise Security
Mindful of the city’s budget, Lee wanted a cloud-based SIEM to avoid the administrative burdens of onsite platforms. After considering available solutions, Los Angeles chose Splunk Cloud and Splunk Enterprise Security. Splunk Cloud offers extraordinary scalability and a 100 percent uptime SLA. According to Lee, “Splunk Cloud was fast to deploy and easy to tailor, whereas customizing competing products required two full-time employees.”

Splunk Cloud also resolved two concerns: data security and bandwidth consumption. Splunk forwarders encrypt and compress all data before it leaves the enterprise, rendering information secure in transit and bandwidth consumption negligible.

**Real-time situational awareness**

Splunk Cloud provides Los Angeles with holistic views of its security posture. Splunk forwarders send raw logs and other data from the city’s departments to Splunk Cloud, where they are normalized and returned to the integrated SOC, and then analyzed and visualized in Splunk dashboards.

Using pre-built, easily customizable dashboards in Splunk ES, executives and analysts have always-available, real-time situational awareness of security events across the city’s networking infrastructure. With all security data in one continuously updated database, Lee’s team views and compares any machine-generated data, including disparate logs and both structured and unstructured data, to extract all-inclusive, actionable security intelligence.

Analysts can monitor for malware and identify the top attackers and their targets within the infrastructure. Splunk dashboards alert for security events, enabling prompt responses to intrusions that threaten public services or assets. Analysts conduct searches and forensic investigations, drilling down to track hazards anywhere in the enterprise.

“By using the Splunk platform to gain visibility into questionable network activities, we assess risks, prioritize and mitigate threats, and proactively address vulnerabilities,” says Lee. “Our Splunk SIEM is like having video cameras on every block; it provides visibility into what’s happening on the network, which is foundational to safety.”

“By deploying the Splunk SIEM solution, we enhance our detection and response capabilities to protect the City’s critical assets from all manner of cyberthreats and intrusions. By utilizing a cloud solution, our security team can focus on security events rather than deploying and maintaining infrastructure.”

Timothy Lee
Chief Information Security Officer, City of Los Angeles

**Timely threat intelligence**

The city’s integrated SOC does more than collect information; it also provides information. It translates data from Splunk Cloud into timely threat intelligence. The city shares its findings with its agencies as well as external stakeholders like the FBI, the Department of Homeland Security, the Secret Service and other law enforcement agencies. With this information, the city collaborates with federal agencies to identify risks and develop strategies for deterring future network intrusions.

“With situational awareness, we know ourselves,” says Lee. “But with threat intelligence, we know our enemy. We’re now operating an integrated threat intelligence program and our Splunk SIEM is one of the key solutions for a centralized information management platform that we deploy at our Integrated Security Operations Center (ISOC).”

**Locking down the city’s digital assets**

By anchoring its integrated SOC with the rich SIEM functionalities of Splunk Cloud and ES, Los Angeles met its mayor’s directive by transforming its patchwork of security measures into a cohesive, all-encompassing cybersecurity strategy. “As the number and sophistication of risks increase, our cloud-based Splunk solution levels the playing field by making our security team more effective,” concludes Lee. “With both holistic and granular views of our digital assets, we have the awareness and knowledge to counter the threats that imperil Los Angeles and other cities. For municipalities that are decentralized into many departments, the Splunk platform is a comprehensive yet cost-effective security solution.”
Executive summary

With more than $1.2 billion in assets, Orrstown Financial Services, Inc. and its wholly-owned subsidiary, Orrstown Bank, provide a full range of financial services through 22 locations throughout Pennsylvania and Maryland. With a need to comply with demanding security regulations, Orrstown Bank wanted a security solution that could provide visibility into its complex hybrid IT infrastructure, identify and resolve threats, and provide required uptime and compliance. Since deploying Splunk Cloud, the bank has seen benefits including:

- Improved operational efficiency and customer satisfaction
- Estimated 50 percent reduction in fraud losses
- Enhanced security posture

Why Splunk

Initially, Orrstown Bank relied on a security services provider that delivered basic security information and event management (SIEM) functionality around the bank’s security devices. Unfortunately, the security service could not offer enough intelligence for the bank’s security team to rapidly identify incidents or respond to requests from regulators.

“Our security provider is a one-size-fits-all solution designed for community banks, which did not give us long-term trending and analytics,” says Andrew Linn, SVP, chief information security officer, Orrstown Bank. “We needed to augment its monitoring to properly defend the bank against threats and fraud. We wanted greater visibility to detect both internal and external threats and...”
to collect forensic evidence to understand and neutralize them. But our business is banking, not running a datacenter, so we want as little on-premises infrastructure as possible.

Prior to Orrstown, Linn and his colleagues had worked for some of the world’s largest financial institutions and were familiar with Splunk Enterprise. Splunk Cloud, which delivers all the functionality of Splunk Enterprise as a cloud service, eliminated the need for an onsite deployment. Another important factor was Splunk Cloud’s 100 percent uptime SLA and its SOC2 Type II certification.

“Rather than buy a dedicated SIEM solution and numerous monitoring solutions, we deployed the Splunk Cloud platform, which slashed our administrative overhead,” says Linn. “We’re aggregating data from over 60 sources, mostly on-premises servers and security systems, and are constantly discovering new use cases for Splunk software.”

Centralized visibility into security and business processes

Splunk Cloud took just two weeks to deploy at Orrstown Bank and is providing the bank with real-time, centralized visibility into its security, network and business operations. Administrators and security specialists now use the platform to establish baseline performance metrics to assess the health of systems, proactively monitor and receive alerts, and quickly investigate and resolve any issues. “Rather than pore over thousands of lines of transactions, we use Splunk Cloud dashboards to visualize patterns and trends,” says Linn. “We can observe login anomalies, detect questionable activities and behaviors, and promptly take measures to remediate them.”

Fraud reduction yields far-reaching benefits

Orrstown has experienced an increase of more than 400 percent in debit card fraud over the past three years. To combat this, the bank integrates an anomaly detection solution in its Splunk Cloud deployment. This joint solution rapidly identifies the first instance of fraud and then prevents subsequent fraudulent transactions. The solution uses statistical modeling to discover abnormal activities, incorporating transaction characteristics such as the location, amount, time of transaction, as well as the risk profile of the vendor.

The combination of these dimensions determines a risk score for each transaction. Based on the severity of the score, Orrstown is able to take appropriate action, such as disabling the debit card or issuing a proactive customer notification. By incorporating anomaly detection into Splunk Cloud, the bank estimates it cut debit card fraud losses by over 50 percent.

Security intelligence improves ATM operations

With Splunk Cloud, Orrstown gains real-time fraud and business analytics across its network of ATMs. The bank indexes data from the ATMs and displays the information in Splunk dashboards, providing near real-time insight into potentially fraudulent activities.

Thanks to Splunk Cloud, the bank also derives business intelligence from its ATMs. By baselining the flow of money in and out of each ATM, for instance, it ensures the devices are neither under nor over-provisioned, efficiently making funds available to customers.

Linn concludes, “These innovative Splunk use cases allow us to further monetize our ATM system. We initially applied Splunk Cloud for security use cases, but we’re developing more and more business-focused use cases where we use the visibility and analytics provided by the Splunk platform to improve our operations and customer satisfaction. We’re enjoying security, IT and business value from a single, cost-effective solution.”
Online Content Specialist Boosts Security With Splunk Cloud

Executive summary
BrightEdge provides search engine optimization and content marketing performance to 1,500-plus global customers through an award-winning software as a service (SaaS) platform that runs on Amazon Web Services (AWS). To ensure performance and customer confidence, maintaining a secure environment is paramount, and that’s why BrightEdge uses Splunk Cloud running on AWS as its security intelligence platform. Since deploying Splunk solutions for analytics-driven security, the company has seen benefits including:

• Correlation of multiple data sources without the need to build multiple connectors or apps
• Seamless integration with Salesforce.com and other cloud applications
• Monitoring for compliance with ISO 27001 and other security standards
• Keeps security information and event management (SIEM) data completely isolated from the rest of the internal technical infrastructure, to protect the integrity of log data

Why Splunk
“In this age of cybersecurity threats, you don’t know what vulnerabilities you may have,” explains Jae An, BrightEdge’s 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 uses Splunk Cloud, a companywide solution for log management and real-time security investigation. Splunk

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 head count 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
• AWS Config
• OSSEC
• Rapid7
• Salesforce
• Dropbox

Splunk Products
• Splunk Cloud
• Splunk App for AWS
• Splunk App for Salesforce
• Splunk Add-on for Symantec Endpoint Protection
Cloud works with AWS core services and infrastructure to provide the flexibility and powerful security tools BrightEdge needs.

“As a cloud-first company without a large IT department, we use pretty much all of the best-of-breed SaaS products,” An says. “After evaluating the available tools, 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 providing correlations across multiple data sources that BrightEdge’s previous solution couldn’t offer. “If I had to use our previous solution 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 head count,” says An.

Protecting business in the cloud

Like many other SaaS businesses, BrightEdge relies on AWS infrastructure to keep its software products available online. “Splunk Cloud monitors all logs from servers and IDS in near real time, and alerts our security team as soon as it detects threats from hostile sources,” An says. “Splunk Cloud also monitors the API calls and IAM activities in AWS using the Splunk App for AWS. Since its adoption, Splunk Cloud has helped us stop cyberattacks numerous times, and it has also helped us monitor internal DevOps activities for compliance as well. Basically, it helps our business run in the cloud.”

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

“Salesforce contains highly confidential internal sales and opportunity information. Splunk monitors all security events and data export activities within Salesforce, and it provides a very critical data loss prevention function for us,” An says.

Splunk Cloud also detected a malware-compromised workstation in the corporate network that was attacking one of the company’s corporate business applications. This helped the IT team prevent a data breach and the spread of malware to other computers in the network.

“Now I can do a security investigation in less than an hour. It is amazing to see what Splunk Cloud can do; it’s achieving the impossible.”

Jae An
Head of Information Security, Brightedge

An and team realized that, “The endpoint security software we had at that time didn’t detect the unknown malware, and instead it was disabled by the malware and other computers were being attacked. So, we had to manually quarantine and replace the infected machine. Without Splunk Cloud we probably wouldn’t have known about the malware.”

Bringing analytics-driven security within reach

Delivering end-to-end security visibility can take a long time to implement. According to An, “Implementing a security incident response and threat monitoring system can take months, or sometimes years, in large organizations.”

However, midsized and smaller organizations are generally more agile and need to deploy a solution 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,” An says.

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 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, it would be almost impossible to protect the organization from ever-evolving security threats,” An concludes.
End-to-End Cloud and Hybrid Visibility Are Within Reach

Whether hosting apps in IaaS, PaaS or serverless infrastructures, Splunk can ingest any format of AWS event logs and other mission-critical data. With the Splunk App for AWS, you can monitor the scale-up and scale-down of instances and workloads that are constantly changing and connect data with application metrics for holistic monitoring. With Splunk optimized for AWS, you gain a complete picture of the health of your entire cloud and hybrid infrastructures—including all of your nodes, transactions and users in one platform.

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.

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.