aws | splunk>

CASE STUDY

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."

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

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

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."

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.

"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

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."

"When we looked at what other companies were providing, they were playing catch-up to the capabilities that were already in Splunk."

Gary Mikula
Senior Director, Cyber and Information Security, FINRA

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-FINRA-AWS-Cobrand-A4-102