

Raymond James Gains Fast Time to Value With Splunk Cloud

RAYMOND JAMES®

Executive summary

Raymond James is a full-service financial services company and trusted advisor to individuals and institutions throughout the U.S., and through its subsidiaries in Canada and Europe. The company adopted Splunk Cloud for security information and event management (SIEM) and has since expanded to additional use cases including application monitoring. Since deploying Splunk Cloud, Raymond James has seen benefits including:

- Fast time to value, with initial deployment completed in one weekend
- Decreased hardware requirements
- Reduced certain queries from 48 hours to 30 minutes

Why Splunk

At Raymond James, the security, engineering and operations department is responsible for network security, infrastructure security, and reporting and monitoring. According to Kevin Lane, a Raymond James security engineer, “With our previous platform, we wanted more consistent data, to correlate events across multiple systems and log types, and to decrease our time to resolve IT and security investigations.”

A proof of concept (POC) enabled the team to determine that Splunk Cloud met its requirements, including increased query speed. “When you’re doing investigative work for security reasons, you want to resolve incidents quickly,” Lane says. “Certain queries over a month used to take about 48 hours to return, and then we ran the same query in Splunk Cloud, and it took approximately 30 minutes.”

“In the financial services industry, getting the right information, being able to correlate and search through data quickly is very beneficial to us,” says Lauren Deren, security engineering and operations manager at Raymond James.

With Splunk Cloud, Raymond James would not have to purchase additional on-premises hardware and keep it up to date. It was also very important to the team that they would not have to set up an entirely new business continuity management and disaster recovery (BCP-DR) infrastructure. “With Splunk Cloud, our infrastructure is dynamic. We can lean on those resources and save manpower and a lot of time,” shares Deren.

Industry

- Financial services

Splunk Use Cases

- Security
- IT operations

Challenges

- Correlate events across multiple systems and log types
- Needed a solution for fast IT and security investigations
- Wanted a cloud solution to reduce hardware maintenance time and spend

Business Impact

- Reduced certain queries from 48 hours to 30 minutes
- Improved user experience
- Saving costs by using far less hardware
- Rededicated people from maintaining its previous complex SIEM solution to higher-value tasks
- Enabled disaster recovery

Data Sources

- Firewall
- VPN
- Syslog
- Microsoft Windows
- Linux

Splunk Products

- Splunk Cloud
- Splunk Machine Learning Toolkit

Ease of use

The initial Splunk Cloud deployment took place over a weekend. With fast time to value, Deren and team have opened Splunk Cloud up to more users, and many are taking advantage of the platform. “Running searches in Splunk is a lot easier for people outside of our specific area,” Deren says. “With other SIEMs you have to learn about five different programming languages to manage it. Splunk uses one, so that helps from a user perspective.”

“The cloud platform reduces administrative workload so that users can focus on company-specific information, such as alerting, monitoring and increasing visibility,” says Deren. “Our team is maximizing efficiency, using their time for high-value projects.”

Improved self-service

Another big benefit of Splunk Cloud is that the team has been able to offer self-service to its internal customers, such as other IT and HR teams. For example, the IT help desk can avoid escalating issues to multiple teams by using self-service Splunk Cloud dashboards to increase their call resolution.

Splunk Cloud dashboards help the HR teams perform basic self-service investigations without having to involve the security team. Even system administrators and other internal back office teams have begun using Splunk Cloud dashboards because of the overall positive user experience.

“Certain queries over a month used to take about 48 hours to return, and then we ran the same query in Splunk Cloud, and it took approximately 30 minutes.”

Kevin Lane, Security Engineer
Security, Engineering and Operations, Raymond James

“With other SIEMs you have to learn about five different programming languages to manage it. Splunk uses one, so that helps from a user perspective.”

Kevin Lane, Security Engineer
Security, Engineering and Operations, Raymond James

Expanded use cases

While security monitoring was the main reason why Raymond James selected Splunk Cloud, the team has discovered other use cases for it as well. “As we moved to Splunk, we identified several of the operational use cases that were well-suited for the platform and have taken a prominent role with our user base,” Lane says.

“Since we’ve done the Splunk Cloud implementation, we’ve expanded our IT monitoring significantly,” says Deren. “We’re able to monitor many applications and look at application health. We’re able to see if there’s any performance degradation before a user calls in.”

The team at Raymond James is looking at other premium Splunk solutions to complement the platform, such as Splunk User Behavior Analytics (UBA) and Splunk IT Service Intelligence (ITSI). “Our DevOps team is already using the Splunk Machine Learning Toolkit for monitoring standard deviations and website traffic,” explains Lane.

“Our DevOps team is using the Splunk Machine Learning Toolkit for monitoring standard deviations and website traffic.”

Lauren Deren, Manager
Security, Engineering and Operations, Raymond James

[Download Splunk for free](#) or get started with the [free cloud trial](#). Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.



Learn more: www.splunk.com/asksales

www.splunk.com