splunk> turn data into doing™

CASE STUDY

Raymond James Gains Fast Time to Value With Splunk Cloud

Key Challenges

Financial services organization Raymond James needed a new cloud solution that could quickly correlate critical security events across multiple systems and log types while saving money.

Key Results

With Splunk Cloud™, Raymond James has improved its user experience, saved money and accelerated response times while freeing employees to focus on high-value tasks, not SIEM maintenance.

RAYMOND JAMES®

Industry: Financial Services

Solutions/Use Cases: Security, IT Operations

Turning Data Into Outcomes

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

Could a move to the cloud save time and money?

That's what Raymond James would soon find out. This full-service financial services company is a 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.

From Daily Workflows to Disaster Recovery

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.

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."

> With Splunk Cloud, our infrastructure is dynamic. We can lean on those resources and save manpower and a lot of time."
>
> **Lauren Deren,** Security, Engineering and Operations Manager, Raymond James

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.

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

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.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2020 Splunk Inc. All rights reserved.

20-15406-SPLK-RaymondJamesGainsFastTimetoValue-103-CS-tier2