splunk>

CASE STUDY

Fairfax County Protects Citizen Data Using Splunk Enterprise Security in the Cloud

Executive summary

Fairfax County, Virginia, located in the heart of the nation's capital, employs 12,000 people across more than 50 agencies and serves more than 1.1 million citizens. Its government is regarded as a leader in many areas when it comes to cybersecurity and IT, enabling it to serve the needs and protect the data of its IT-savvy and high profile citizens. Since deploying Splunk Enterprise Security (ES) with Splunk Cloud as its security information and event management (SIEM) platform, Fairfax County has seen benefits including:

- Proactively supporting more than 50 county agencies and protecting citizens' data
- Reducing security reporting from two weeks to real time
- Increasing focus on strategic initiatives by leveraging cloud services

Why Splunk

According to Mike Dent, chief information security officer (CISO) for Fairfax County, 210 IT professionals support more than 50 county agencies, each with unique business and security requirements. Some agencies, such as the Health Department, are governed by regulations like HIPAA, while others must comply with payment card industry (PCI) regulations. Ultimately, the county requires reliable and secure access to data so it can make the best decisions to support county citizens.

In the past, one of the major challenges Dent and his team faced was centered around the numerous disparate systems from which it had to pull event logs. What's more, its previous SIEM tool could not keep up with the more than 3.9 petabytes of data the county must control, access and secure. Dent explains that after comparing the Splunk data analytics platform to several other products, the county partnered with Splunk's professional services team to conduct a successful proof of concept, and then moved forward with an implementation that was easy on his staff.

"Previously, reporting to leadership was difficult because everything was manual. My staff would spend countless hours, probably two weeks' worth of work, to get me a summary report of our cybersecurity stance," Dent says. "Now, with the Splunk platform, I have real-time access and can give an overall security posture to my leadership to let them know when we have issues."

Industry

- Public sector

Splunk Use Cases

- Security
- Compliance

Challenges

- Unable to access data residing in disparate systems
- Time-consuming security and IT reporting
- On-premises software required additional personnel and large, costly data center footprint
- Inability to access, secure and manage large amount of data (3.9 petabytes)

Business Impact

- Proactively protecting citizens' data and supporting more than 50 county agencies
- Replacing time-consuming, two-week security reporting with real-time reporting to leadership
- Achieving significant cost savings by reducing data center hardware footprint
- Reducing impact by monitoring employee email phishing and millions of daily threats on endpoint systems
- Protecting against dangerous malware and defending critical infrastructure systems
- Repurposing full-time equivalents (FTEs) away from managing infrastructure and towards more value-added tasks

Data Sources

- Next Generation Firewalls
- Network Infrastructure (routers, switches, load balancers)
- End Point Protection Infrastructure

Splunk Products

- Splunk Enterprise Security
- Splunk Cloud

Security visibility and operations using the cloud

Initially, some of Dent's security counterparts questioned the county's decision to go with a cloud platform due to security concerns. "With Splunk Cloud and Amazon Web Services (AWS) it's an easier win for me to explain to leadership that I have a secure connection to the cloud," Dent says. "My staff can get to it. The data is there, it's ours. We manage and control it. No one else has access to it. I don't have to worry about hardware failing. All of that is taken care of through my agreement with the cloud services that we're using. It's 24/7 access."

Fairfax County is benefitting from its cloud service for Operational Intelligence in several ways including elasticity, security and scalability, without the operational effort. Dent says that the county is also enjoying cost savings from a hardware perspective because there is a smaller data center footprint. What's more, only one individual is required to manage the Splunk implementation, which enables the county to maximize its resources.

Today, Fairfax County relies on the Splunk platform and Splunk ES as its SIEM to monitor employee emails for phishing attempts and millions of daily threats on its endpoint systems. In addition to known threats, the county monitors and protects against dangerous malware while also defending its critical infrastructure including supervisory control and data acquisition (SCADA) systems. Moving forward, the county intends to use the Splunk platform to ingest PCI-relevant data to ensure compliance.

"My top priority is to protect the citizens' data. Making sure that these citizens can trust the government they have with the data that they have entrusted us with is our mission."

Mike Dent, CISO
Fairfax County, Virginia

Beyond security

Dent and his colleagues appreciate having an analytics platform offering broad capabilities beyond security reporting, such as the ability to report on IT usage, including hardware, software, internet use and bandwidth utilization. With the Splunk platform, internet reports and bandwidth utilization get correlated into an event that Dent uses to communicate to the leadership visually. The platform also enables reporting on application performance and citizen access. These capabilities have helped Dent to secure more budget, and the county leadership now has a platform to help make better decisions.

Fairfax County's security strategy is defense in depth. As a CISO, Dent says this starts with making sure you have the right solutions, in combination with the right people, processes and policies. When you put all of that together it becomes a good strategy and a great security program.

"My top priority is to protect the citizens' data," Dent concludes. "Making sure that these citizens can trust the government they have with the data that they have entrusted us with is our mission."

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