Maryland's Prince George's County Mission-Ready With Splunk Platform

Executive summary

Home to NASA's Goddard Space Flight Center, the University of Maryland and nearly one million citizens, Prince George's County, Maryland, located outside of Washington, D.C., spans almost 500 square miles. The county's centralized Office of Information Technology (OIT), which supports all branches, agencies and government employees, faces many challenges when it comes to fulfilling its mission with limited resources and funding. Since deploying Splunk Enterprise, the county has seen benefits including:

- Improved government efficiency and transparency to better serve constituents
- Helped small IT team reduce time to identify and resolve IT issues from days or weeks to hours
- Transformed county operations by replacing data silos with a platform for IT operations, application monitoring and security

Why Splunk

OIT provides infrastructure and core IT services to support the goals of diverse countywide agencies, from Public Safety to the Health and Human Services and the Social Services Departments. Prior to implementing Splunk Enterprise, the county had siloed data sets, which made it challenging for its small IT team to get visibility into issues that were occurring and resolve them quickly to ensure uninterrupted services. For example, when county staff experienced frequent user account lockouts and password resets it was difficult for the OIT team to troubleshoot where issues were occurring and which devices were causing problems. The team resorted to working together via email, by phone or in person. By implementing Splunk Enterprise, the team gained visibility across functional teams to get a broader understanding of issues and solve them more quickly.

"Splunk Enterprise has allowed us to save a tremendous amount of time when working with password and account lockout issues," says Jayson Loveless, the OIT enterprise architect who also oversees the network infrastructure teams. "In the past it took days, if not weeks, to clearly identify the source of the problem. With Splunk, we're able to identify and resolve that issue within a matter of hours."

Industry
- Public Sector

Splunk Use Cases
- IT operations
- Application delivery
- Security

Challenges
- Deliver reliable services to agencies and constituents with limited resources
- Data siloed across functional areas
- Time-consuming IT troubleshooting and resolution
- Ensure reliable citizen access to applications
- Provide data transparency to agencies
- Increase in number of cyberthreats

Business Impact
- Improving government efficiency and transparency to better serve constituents
- Ensuring citizens have reliable access to online services
- Helping agencies solve IT challenges and support their missions
- Reducing time to identify and resolve IT issues from days or weeks to hours
- Enhancing security posture
- Supporting compliance with ISO 27001 standards

Data Sources
- Palo Alto firewall data
- ForeScout network data
- Mircrosoft Windows event data
- Nessus vulnerability scan data
- Public Safety Crime Incident data
- Health data
- 311 non-emergency data

Splunk Products
- Splunk Enterprise
- Palo Alto Networks App for Splunk
- ForeScout App for Splunk
- Splunk Add-on for Tenable
- Splunk App for Windows Infrastructure
- CIS Critical Security Controls App

According to Loveless, the county CIO's top priorities include big data, data analytics, cybersecurity and building a workforce for the future. "OIT is limited in its resources, and we feel it's important to engage the business community and our partners to understand and maintain current trends in emergent technology," Loveless says. "We look at Splunk Enterprise as a solution to get a better understanding of all data including system health, public safety and transportation, to solve problems, help our agencies fulfill their missions and make government more efficient."

"We look at Splunk Enterprise as a solution to get a better understanding of all data including system health, public safety and transportation data, to solve problems, help our agencies fulfill their missions and make government more efficient."

Jayson Loveless

Enterprise Architect, Prince George's County OIT

Improving customer service

Loveless and his colleagues rely on Splunk Enterprise to monitor the network, consisting of approximately 100 sites and 500 network devices, to ensure that services are available and agencies can serve county citizens. In addition, OIT manages 300 virtualized servers in the data center to support the agencies. OIT provides infrastructure that supports the majority of the county's data, including public safety dispatch, public safety records management systems, 311 non-emergency services, the SAP ERP system and more. One of the department's missions is to be more transparent with the agencies, and Loveless notes that Splunk Enterprise dashboards and data visualizations are enabling OIT to do so.

The county also relies on Splunk Enterprise for application monitoring, including an application that enables citizens and contractors to apply for and complete permits online. Moreover, the county has started to leverage some Splunk apps including the Palo Alto Networks App for Splunk, the ForeScout App for Splunk and Splunk Add-on for Tenable, to integrate with other platforms the county uses.

Today, in addition to providing some of the county's senior managers and engineers with IT operations visibility, OIT staff also rely on Splunk Enterprise to help with cybersecurity. "Today, we're pulling in the Nessus vulnerability scans to assist not only with vulnerability identification and historical information, but also to support the ISO 27001 framework," Loveless says. "To support that, we're using Splunk Enterprise with Nessus to ensure we have continuous vulnerability scanning."

Countywide data platform improves operational efficiency

Moving forward, the county plans to grow its use of the Splunk platform to improve its security posture and quickly investigate potential threats or vulnerabilities to take action on those events proactively. Loveless explains that the OIT has faced recent cyberthreats and needs to ensure data integrity, availability of service and that the service is being used as intended.

"Splunk is a platform for Operational Intelligence for Prince George's County," Loveless concludes. "With Splunk, we're able to have greater visibility across functional teams, to identify trends and potential problems in advance and to resolve issues more quickly by seeing a broader view of the problem."

"With Splunk, we're able to have greater visibility across functional teams, to identify trends and potential problems in advance and to solve issues more quickly by seeing a broader view of the problem."

Jayson Loveless

Enterprise Architect, Prince George's County OIT

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