A Clearer View of IT Operations

Government IT Modernization Depends on Efficient Enterprise Operations Enabled by Visibility and Integration.

By **Kevin Davis**
Vice President, Public Sector
Splunk

Digital transformation is a priority for government organizations, in part because the continued upkeep of aging legacy infrastructure consumes as much as 75 percent of IT operating budgets. This hefty investment in traditional computing architectures prohibits the introduction of new, more efficient technologies that meet current and evolving agency requirements.

How can agencies, encumbered with legacy systems and constrained budgets, implement new technologies and streamline processes to improve how they perform the business of government? What government organization would not want a more integrated, efficient, and responsive IT infrastructure, supported by thoughtful processes that result in consistent and timely customer experiences?

This scenario motivated passage of the *Modernizing Government Technology Act of 2017*, intended to provide funding and incentives to help government agencies break from long-standing IT procurement strategies and drive them to consider more cloud-based technologies to fuel and expedite their digital transformations.

To move in this direction, agency professionals need a complete understanding of their current enterprise IT operations. They must evaluate traditional tools, systems, and governing policies to determine where opportunities for improvement will have the most impact on budget, staff, and future operations. By employing an analytical, data-driven approach, they can be equipped to create the vision and introduce new methods and technologies to enable sustainable, secure, and optimized IT operations.

> Integrate data from independent systems into searchable repositories for visibility across the entire computing environment.

Managing agency IT operations is a challenge. Federal CIO organizations are responsible for monitoring, managing, and troubleshooting rapidly evolving and increasingly complex environments. Introduction of the latest technologies, pressure to migrate workloads to the cloud, compliance mandates and expanding cyber threats combine to limit agency capabilities to deliver services, fulfill service level agreements (SLAs), meet citizen expectations, and accomplish their missions.

Despite the headwinds, many agencies have launched digital transformation programs and the transition has begun, as evidenced by IT budgets shifting from traditional on-premises investments to more cloud-based solutions and agile development models. Unfortunately, the transition is not pain-free. A recent survey conducted by the Ponemon Institute polled more than 1,200 decision-makers and operations staff supporting public sector programs, including government, education, and contractor professionals. The Splunk-sponsored research revealed that while a handful of new approaches are advancing IT operations, including adoption of DevOps, there is an overall loss of confidence among public sector organizations in the shifting IT environments they manage.

Operating in Silos

Government agencies have diverse mandates and their technology infrastructures have been driven by individual department requirements. The result is that agency technologists are attempting to manage a heterogeneous landfill of intertwined components to deliver mission-critical services. Yet they lack the real-time, end-to-end visibility into their IT operations and are unable to quickly identify root causes of outages given the lack of integration between systems that often are supported by ad hoc mitigation processes.

The Ponemon study reported more than half of public sector IT respondents cannot, or were unsure, if they could pinpoint problems because their systems were managed in silos. This inability to resolve failures quickly is significant--the survey found that system recovery following an outage can take an average of 44 hours and as many as 12 full-time resources to resolve. Most also expect near-term spending for cloud and DevOps to grow by nearly 50%, a shift that has shaken the confidence of many who question their abilities to meet SLAs and manage data center upgrades and cloud migration programs.

Overcoming Complexity

Improving IT operations management is essential so agencies can invest their financial, personnel and technical resources where they are needed most. While government professionals are looking to data and monitoring tools to advance this cause, they must resist a "silo mentality" where monitoring tools are technology- or application-specific.

How can government professionals manage hundreds (or thousands) of applications, servers, and virtual machines generating an unprecedented volume of disparate data streams? Clearly not by relying on existing tools that monitor segments of the infrastructure but fail to evaluate overall enterprise IT operations. Traditional approaches no longer support the complexity, volume, and speed that the modern agency needs to support mobile applications, cloud-based resources, virtual machines and software-defined everything.

To overcome the encumbrance of legacy systems, government organizations need to ingest and integrate data from independent systems and resources into easily searchable repositories for visibility across their entire computing environment. Modern enterprise IT operations rely on highly-scalable platforms that aggregate machine data, including all tiers of applications and hardware infrastructure, into a single, secure, and centralized location. Only with a comprehensive view of enterprise IT operations can agency professionals glean the trusted operational intelligence needed for more data-driven decision-making.

Realizing Digital Transformation

The promise of digital transformation is increasing operational efficiency through eliminating stove-piped systems, reducing system complexity, strengthening cybersecurity, improving incident response, and employing DevOps practices. Transformation begins with a complete understanding of current enterprise systems, workloads, and processes. This can most effectively be derived from an analytical, data-driven approach that supports the evaluation of modernization tools and methods. By embracing new tools and methods, agencies are more than twice as likely to deliver higher quality products and services, realize better operating efficiency, and ensure increased customer satisfaction. ■

SOLUTION FOCUS

Splunk Software Streamlines IT Operations

The key to optimizing Federal IT operations is greater end-to-end visibility into systems performance, availability, and usage with trusted capabilities to identify, troubleshoot, and resolve problems quickly. What is needed is a data collection and analytics capability that delivers a comprehensive operational view into enterprise systems and applications, from the data center to the cloud, which combine to deliver an automated framework for achieving maximum efficiency.

Splunk software delivers this enterprise-wide view built on granular system information by ingesting data from any source, in any format, and presenting it in a single interface that can be used to discern usage patterns, trouble spots, and risk areas. With automation and machine learning, Splunk helps simplify operations, prioritize issue resolution, and provide continuous monitoring capabilities to enable threat detection and mitigation.

Importantly, the Splunk approach to data management — collect-once, aggregate, and use-many-times — delivers multiple IT operational benefits, including comprehensive risk assessment, resource management, and reliable service delivery. Powerful and integrated Splunk solutions allow agencies to eliminate multiple, stove-piped tools, applications and their associated costs, further streamlining IT operations.

Federal IT modernization programs rely on Splunk to aggregate data, understand current asset inventories and usage, and to accelerate cloud migration with targeted issue resolution and insights for performance improvement. Using Splunk to monitor workloads facilitates data center consolidation by tracking managed space, power loads, and servers. In the security domain, Splunk's data-driven analytics enable informed incident management and forensics capabilities and improved self-reporting and compliance audits.

Splunk software capabilities allow Federal IT professionals to harness data from multiple sources and present system-wide visibility in a single interface that enables rapid decision-making to continually improve operational efficiency. The results are compelling: less downtime, faster incident response, more robust cybersecurity, and increased user satisfaction.

Learn more at: https://www.splunk.com/en_us/form/digging-out-of-the-silos.html.