Splunk and Government IT Modernization

Citing that the Federal Government spends nearly three-fourth of its annual IT budget on maintaining and operating legacy IT systems, Congress recently passed and the President signed the Modernizing Government Technology Act of 2017.

The MGT Act also strikes a chord with the Security Executive Order that preceded it and the resulting Report to the President on IT Modernization. The report envisions modernization as a state where agencies can (a) maximize secure use of cloud computing, (b) modernize government-based applications and (c) shift towards a consolidated IT model by adopting centralized offerings for commodity IT (shared services).

Modernization in Government

Modernization attempts have been in earnest in government but sluggish. Aside from budget shortfalls, resource constraints and skills gap, a fundamental source of stagnation lies in heterogeneous systems and applications operated in silos across agencies. At times, it is hard to identify assets that are of high value (HVAs), and how they are interconnected. Any attempt to modernize systems agency-wide is either impossible or short-lived since IT staff neither have the insights to confidently develop a strategy for migrating applications and systems nor monitor their progress effectively. An outage or interruption during the process of transformation can lead to mission impediment or failure and constituent dissatisfaction.

A recent survey on the state of IT Operations conducted by the Ponemon Institute, revealed a decline in confidence among respondents, specifically calling out the inability to manage data center upgrades, and move workloads to the cloud. Two of the biggest concerns that respondents pointed out with cloud migrations were the inability to monitor and troubleshoot applications and lack of visibility across workloads. Clearly the diversity and management of systems and applications in silos has created a non-collaborative environment and the lack of holistic visibility is an impediment to insights to influence a successful migration strategy.

Shared Services

Shared services enable agencies to overcome not only constraints in budgets but overcome resource and skills gap. Modernization inherently involves innovation and lack of training or expertise cannot always be the barrier for adoption. With shared services, agencies or departments pay only for what they use and do not have to invest, manage and maintain individual systems and applications. This can contribute valuable funds to other important agency initiatives and focus staff on the mission of the agency rather than IT maintenance and management. A common service delivery model also ensures consistency across the recipients, promoting a healthy and uniform cybersecurity posture.

To effect migration to new technologies and embrace shared services, agencies need end-to-end granular visibility into systems and applications in real-time so they can understand the dependencies and relationships between them. During migrations, they not only need to continuously monitor progress but be able to foresee issues so they can course correct appropriately on time, lest the mission or service delivery is adversely impacted. Shared services need the ability to monitor usage at a detailed level so agencies have the transparency and are billed appropriately.

Splunk

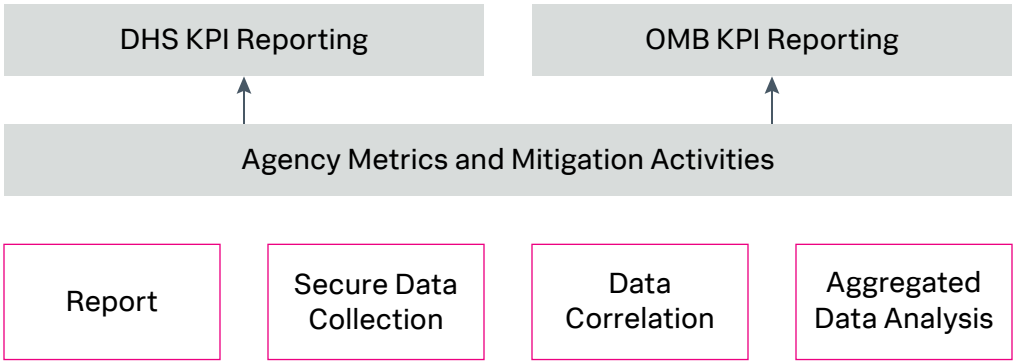
For government agency officials, CIOs and CISOs who seek to modernize and transform their agencies legacy infrastructures, Splunk helps them overcome their biggest hurdle in embracing modernization initiatives and consolidating legacy systems by providing granular visibility and insights into migrations and performance and availability of applications and systems. It enables discovery of powerful insights during and after migrations to overcome challenges, drive successful modernization initiatives, address exceptions, improve efficiencies and deliver superior citizen experiences.

IT Modernization Requirement	How Splunk Delivers
Visibility into activities at the application, network and data levels.	End-to-end granular visibility into all activities in real-time, regardless of source, format or type.
Identify and address risks in High Valued Assets (HVAs).	Collect and aggregate data to develop an asset inventory and track usage, monitor and deliver risk profiles of identified high values assets fast.
Maximize use of secure cloud computing	Accelerate cloud initiatives confidently with granular insights into migrations and address issues before they adversely impact the initiative.
Drive shared services initiatives, eliminate duplication efforts and reduce costs.	Monitor and provide granular visibility into resource workloads, performance and pinpoint issues before they impact migrations.
Expedite the modernization and adoption of CDM to identify, detect, and respond to threats in the Federal Government's increasing move to cloud environments and mobile devices.	Simplify the collection of data from disparate security tools, vendors, and service providers. Extensive add-ons to collect configuration snapshots, Inspector services, and more. Monitor AWS CloudTrail, Kinesis and cloud billing reports.
The establishment of a SOC as a service (SOCaaS) capability is essential to ensure appropriate enterprise-wide visibility, incident discovery, and information sharing among Federal agencies.	Provide a highly scalable platform with data driven analytics and tools to build out a SOC. Out of the box incident response, forensics and security investigation capabilities and ability to apply consistent policies across agencies.
Deliver on initiatives such as data center consolidations and accelerate green initiatives by tracking capacity utilization, availability of managed space and energy efficiencies.	Track capacity utilization and availability of managed space including but not limited to floor space, rack space, PDU power capacity, circuit breaker load, cooling capacity, patch panel ports and physical servers. Predict future capacity needs. Track energy efficiency information such as power usage effectiveness (PUE), including any supplementary tools and instruments.
Meet any compliance mandates.	Enable assessment of implementation and effectiveness of controls against RMF, CSF and any other mandates. Ensure a passing scorecard with easier audits and self-reporting.

A key capability of the Splunk® platform is the ability to collect data once and use it across many use cases that support diverse government initiatives: security and risk management, compliance, IT consolidation and optimization efforts, citizen services delivery, compliance and smart infrastructure initiatives, are a few. This ability to derive value from the same data across disparate initiatives extends returns on investments and lowers overall costs.

Splunk offers government agencies the critical ability to harness data from any source and gain organization-wide visibility so they can make fast and confident decisions. Using the Splunk platform, agencies strengthen their future and ensure success by extending citizen and cyber safety, delivering service excellence and embracing innovations responsibly. The platform can ingest large amounts of data from any source and is available in on-premise, cloud and hybrid models.

Automated Continuous Diagnostics and Mitigation (CDM) Data Driven Activities



splunk>

Contact a Splunk Expert to **discuss** your environment and assess your requirements or contact a sales representative.

20-15508-SPLK-Splunk and Government IT Modernization-102-TB