Leveraging Splunk for U.S. DoD IL5

Cloud computing and technology allow the U.S. Department of Defense (DoD) to consolidate infrastructure, leverage commodity IT functions and eliminate functional redundancies while improving operations. Given the gravity of security concerns when it comes to the U.S. DoD, the Defense Information Systems Agency (DISA) has developed a DoD Cloud Computing Security Requirements Guide (SRG) to dictate levels of authorization for cloud service providers.

This guide categorizes information and information systems into four impact levels based on 1) the sensitivity of the information to be stored and/or processed in the cloud, and 2) the potential impact of a security event that would compromise the integrity, confidentiality or availability of that information. The four impact levels (ILs) that require authorization are IL2, IL4, IL5 and IL6. The lowest of these, IL2, applies to data cleared for public release, while the highest, IL6, applies to classified, top-secret data. IL5 allows access to national security systems and higher-sensitivity, controlled unclassified information (CUI).

According to the SRG, IL5-protection includes information categories such as critical infrastructure, defense, export controls, budget/financial, intelligence, law enforcement, nuclear energy and individual privacy data. It also includes the requirements in NIST SP 800-171, intended for use by federal agencies in contracts or other agreements established with non-federal organizations.

IL5 authorization also applies to information systems that are identified as national security systems (NSS). An NSS, according to NIST SP 800-59, is any information system used by an agency that involves activities related to intelligence, national security cryptologic, command and control of military forces, equipment integral to weapons systems, and any other functions critical to direct fulfillment of military or intelligence missions.

Splunk Cloud Platform, a SaaS cloud service offering hosted in AWS GovCloud(US), has achieved U.S. DoD authorization at IL5. The service is designated as a U.S. government community cloud, and is initially available to U.S. federal agencies who can access the service via the Defense network (NIPRnet). For this offering, service delivery and support is performed by U.S. Citizens, on U.S. soil. Splunk Cloud Platform with DoD IL5 authorization is now available for sale. Federal agencies can now use Splunk to meet the specific challenges they face when using cloud computing to address a variety of data analytics and AI use cases — with confidence, and at mission speeds.

Compliance

Federal agencies must be sure the cloud products and providers they use are fully compliant with regulatory mandates. Agencies are mandated to procure and use only U.S. DoD authorized cloud service providers. They must also follow a mandate under the Defense Federal Acquisition Regulation Supplement (DFARS) to only use systems that comply with NIST SP 800-171, which protects controlled unclassified information in non-federal systems.

The NIST SP 800-53 controls that comprise FedRAMP Moderate Impact Level baseline are a superset of NIST SP 800-171 referenced controls. Splunk Cloud Platform with FedRAMP Moderate baseline is compliant with applicable requirements specified under DFARS section 252.204-7012(b)(2) (ii)(D) and NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations). Splunk Cloud Platform also adheres to some of the most rigorous security and compliance standards. Its “single tenant” deployment model offers extra protection and data isolation so that each customer has their own dedicated instance of the Splunk Cloud service. Splunk Cloud Platform is also encrypted, meeting both FedRAMP and IL5 cryptographic requirements for data protection at rest and in transit. FIPS 140-2 validated cryptographic modules are employed for data encryption.

Time and resources

USG agencies have limited time and resources, and must often manage and maintain their own infrastructures. Data ingestion, normalization, modeling and curation take a lot of time and resources, and don't always deliver optimal results. Agencies need fast, flexible cloud solutions to save time and accelerate time-to-value, and keep the total cost of ownership low.

Splunk Cloud Platform allows users to ingest any data, in any format, in near real time, providing automatic correlation and saving the time it takes to manually curate data models. With Splunk Cloud Platform, agencies can go live fast, accelerating time-to-value in as quickly as two days. As a subscription service, agencies don't need to provision or manage infrastructure and can focus their scarce and valuable resources on strategic initiatives instead.

There are 700+ Splunkbase apps validated for Splunk Cloud Platform that provide analytics, alerts, dashboards and visualizations, ready to use.

Data analytics

In addition to being time and resource intensive, data ingestion, normalization, modeling and curation can also be very complex activities requiring multiple analytics tools and products. A single organization-wide solution will help agencies to scale and provide holistic visibility and analytics.

Splunk Cloud Platform is a single solution that provides end-to-end visibility, tools for auditing and complete analytics. By ingesting data from any source regardless of format and type, in real time, Splunk Cloud Platform helps agencies streamline processes and eliminate many of the manual tasks that can overcomplicate data analytics. It also provides granular, real-time situational awareness and insight across hybrid environments, eliminating any blind spots and providing an accurate picture of uptime, availability and any other relevant metrics. Splunk Cloud Platform is also scalable, architected to facilitate sudden or unexpected bursts in data volume, quickly expand deployment (with multiple terabytes of incremental capacity available within two days), and provide flexible time periods for data retention.

Service and billing

USG agencies require adequate visibility into cloud providers' service availability and other resources needed to troubleshoot potential issues. Predictable cost at the end of each billing cycle is also an important consideration for agency budget management.

Splunk Cloud Platform is operated by Splunk experts and relieves agencies of the people, processes and systems required to run Splunk on-premises. The platform offers a resilient infrastructure and services with a 24/7 NOC/SOC support team as well as independent service delivery. Splunk Cloud Platform handles upgrades and updates and can also help monitor cloud usage so that agencies have a real-time understanding of resources consumed. This way, there are no surprises at the end of the billing period.

Splunk Cloud Platform enables USG agencies to ingest data once and bring that data to every question, action and decision across multiple use cases. Splunk Cloud Platform meets the FedRAMP security standards, has the additional IL5 authorization, and helps U.S. federal agencies and their partners drive confident decisions and decisive actions at mission speeds.

Learn more about Splunk Cloud Platform, or contact us to discuss your needs and requirements.

splunk>

Learn more: www.splunk.com/asksales www.splunk.com/publicsector

21-14963-Splunk-Leveraging Splunk for US DoD IL5-TB-102