Splunk Cloud Platform: Shared Responsibility Model

The Splunk Cloud Platform SaaS operates on a shared responsibility model to ensure the optimum customer experience. This shared model can help relieve the customer's operational burden as Splunk operates, manages and controls the Splunk Cloud Platform service components, which includes services from our cloud service provider partners, as needed. The nature of this shared responsibility provides customers flexibility and control of their Splunk Cloud Platform environment. Splunk Cloud Platform provides a complete suite of self-service capabilities to simplify actions customers can take as part of the shared responsibility model.

The following table helps customers better understand the distribution of responsibility for their Splunk Cloud Platform service. Customer responsibility varies based on many factors, including use case, subscription type, and the laws and regulations applicable to their organization. Therefore, the following table is for illustrative purposes only and is not exhaustive. Please see Splunk Documentation for additional detail.

Area	Category	Splunk Responsibility	Customer Responsibility
Application Lifecycle	**Splunk Supported Apps and Add-Ons:** These are apps and add-ons that are available through Splunkbase and marked as Splunk-supported.	Splunk publishes the list of Splunk-supported apps and add-ons on Splunkbase. In addition, you are informed of any incompatible apps that need to be upgraded prior to a service update. Splunk reserves the right to change app data models and data structures to optimize usage of the apps. Splunk may deprecate Splunk-supported apps.	You ensure the latest compatible version of the app available on Splunkbase is installed so service updates are unblocked. Be prepared for the possibility that the data structures of Splunk-supported apps and add-ons may change. If app data models and data structures do change, you can adapt your use case to the updated models and structures.
	Private Apps: These are apps and add-ons that you build.	Splunk allows you to build, vet and install your private apps or add-ons on Splunk Cloud Platform. Splunk maintains our cloud app vetting service to vet your private apps and add-ons prior to installation. Splunk may make platform changes for compliance and security-related changes.	When you build your own private apps or add-ons, you are responsible for all aspects of the app's or add-on's lifecycle, including planning, development, release and maintenance. Follow the app lifecycle best practices as described in the Developer Guide for Splunk Cloud Platform and Splunk Enterprise. Please be sure to follow policies specific to Splunk Cloud Platform.

Area	Category	Splunk Responsibility	Customer Responsibility
Data Collection	**Agent-based:** Splunk Forwarder (Splunk to Splunk). **Pull-based:** Data Manager and add-ons with modular inputs, with scripted inputs and with apps.	Splunk makes available binaries and licenses required for Splunk-to-Splunk data collection, such as for Splunk forwarders and deployment server licenses, to help ensure compatibility and ease of management at scale. Splunk provides documentation on best practices and example configurations for data collection. In addition, optional instructor-led education courses and Splunk Professional Services are also available. Splunk maintains Splunk Cloud Platform endpoints as well as polling-based data collection mechanisms. Splunk provides license usage information.	You manage the full lifecycle of Splunk agents deployed in your environment. You select which data is collected using the appropriate mechanism. You configure this data collection mechanism based on your use case and Splunk-recommended best practices. You perform timely updates of agent certificates and keep all configurations up-to-date to ensure accurate collection of data. You monitor this data collection mechanism to ensure successful forwarding of your data. As applicable for your subscription type, you ensure your data collection usage is in accordance with your subscription entitlement.
	REST-based API: Splunk HTTP Event Collector (HEC) data collection mechanisms, including supported push-based data collection from data buses and streaming solutions.	Splunk maintains HEC data collection mechanisms, including supported push-based data collection from data buses and streaming solutions.	You select which data is collected using this mechanism. You configure and monitor this data forwarding mechanism based on your use case and Splunk-recommended best practices.
Data Retention	Index Management	Splunk enforces retention policies as defined by you on a per-index basis.	You manage the lifecycle of data through index management settings, as well as the creation, management and removal of data indexes, summaries and other acceleration mechanisms.

Area	Category	Splunk Responsibility	Customer Responsibility
Data Retention (cont.)	Storage Management	Splunk applies data resiliency and backup policies in accordance with our Splunk Cloud Platform Service Details. Splunk Cloud Platform elastically expands to retain your data per your retention settings. In addition, we provide data retention and storage usage telemetry to help you manage your Splunk Cloud Platform subscription entitlement.	You select the best storage option available for your Splunk Cloud Platform subscription, and you manage these settings in Splunk Web or REST-based API. You ensure storage usage in accordance with your subscription entitlement. If your Splunk Cloud Platform storage usage exceeds your storage entitlement, you may incur a true-up charge.
Network Connectivity		Splunk maintains ingest, login and search endpoints so they are reachable from the public internet, or on a case-by-case basis, through a private network. This includes monitoring the availability of these endpoints. Splunk will provide you with advanced notice in the rare occurrence of a network address change that impacts the ingest, login and search endpoints.	You ensure the public or private internet connectivity between all of your users (such as admins and end users) and the Splunk Cloud Platform ingest, login and search endpoints. In addition, ensure your IP allow list configuration is updated to manage access to your Splunk Cloud Platform environment. You ensure your outbound firewall rules are promptly updated in the rare occurrence of a network address change that impacts the ingest, login and search endpoints.
Search		Splunk maintains the search endpoints per the Splunk Cloud Platform SLA. In addition, we provide documentation and best practices for composing efficient Splunk Search Processing Language (SPL) queries and creating dashboards. Splunk documents service limits related to search, such as the maximum number of concurrent searches. Splunk provides pre-defined workload management pools to assist with search priority in the event of search congestion.	You create your searches using SPL, or using alternative ways to display and analyze data graphically without composing SPL queries. You ensure your search load is in accordance with the documented service limits. You apply workload management rules to prioritize your search workloads appropriately.

Area	Category	Splunk Responsibility	Customer Responsibility
Search (cont.)		Splunk provides information regarding search performance which may include information on long-running searches, skipped scheduled searches and average search runtime.	You review the health and performance of your searches using information provided through Cloud Monitoring Console (CMC). As needed, you take action to improve the performance of your searches.
Security		The Splunk Cloud Platform Security Addendum (CSA) sets forth the administrative, technical and physical safeguards Splunk takes to protect confidential information, including customer content, in Splunk Cloud Platform (Security Program). Splunk updates and publishes the FedRAMP, HIPAA and PCI attestations.	You configure your user accounts to be authenticated using supported identity providers (IdP), including single sign-on (SSO). If required for compliance, configure your IP allow list rules to ensure permitted access to your Splunk Cloud Platform environment. Finally, you assign the appropriate team members to the sc_admin role, which has the permissions to perform self-service tasks. The above is a minimal list and not intended to be exhaustive. You contact your Splunk account representative to review relevant compliance documentation.
Service Lifecycle		Splunk provides notification of changes in the service description plus advanced 14-day notice for service updates and Splunk-initiated routine maintenance. For more information, see the Splunk Cloud Service Maintenance Policy. In the event of a service-impacting incident, Splunk will review service level credit requests when Service Level Agreement (SLA) incidents are submitted by you within the time constraints.	You ensure your operational contacts are kept up-to-date in order for them to receive service updates and Splunk-initiated routine maintenance notifications. In addition, you ensure your assigned maintenance window is kept up-to-date to match your business needs. If you encounter a service-impacting incident, you submit an SLA incident and credit required per SLA guidelines.

22-22220-Splunk-Cloud Platform Shared Responsibility Model-SG-101