Splunk Offerings

Published: February 2024

Splunk Offerings Purchase Capacity and Limitation

Below is the Splunk Offerings Purchase Capacity and Limitations as of the Effective Date. The most current terms are available at: https://www.splunk.com/en_us/legal/licensed-capacity.html

Offering	Capacity	Limitations
Splunk Enterprise	Daily Indexing Volume or number of vCPUs as set forth in the Order "***Daily Indexing Volume***" means the daily aggregate volume of uncompressed data for indexing as set forth in the Order "***vCPUs***" refers to the virtual CPUs to which Software has access. Each virtual CPU is equivalent to a distinct hardware thread of execution in a physical CPU core. Note: For metrics indexing, the Daily Indexing Volume will be calculated by converting each measurement into GB of daily ingestion using a fixed ratio as described in the software documentation.	
Splunk Cloud Platform	Daily Indexing Volume or number of Splunk Virtual Compute ("SVC") ***"Splunk Virtual Compute (SVC)"*** means a unit of capabilities in Splunk Cloud Platform that includes the following resources: compute, memory and I/O as further explained in the service documentation.	
Splunk Enterprise Rapid Adoption Packages	Number of Use Cases identified in the Order "***Use Cases***" are defined and listed here: https://www.splunk.com/en_us/legal/use-case-definitions.html Note: The Rapid Adoption Packages can be purchased in connection with Splunk Cloud Platform as well.	Maximum Daily Index Volume permitted: 25GB (regardless of number of Use Cases) Deployment type: Limited to a single instance deployment Not stackable with other Splunk licenses
Splunk Enterprise for DNS & Netflow Data	Daily Indexing Volume Note: This limited source-type license is also available for Splunk Enterprise Security and Splunk IT Service Intelligence.	Limited Source Types: This license will allow Customers to index the specified Daily Indexing Volume of DNS, Netflow, and/or public cloud access data in any combination of the following data source types: ● aws:vpc:flowlogs ● aws:cloudwatchlogs:vpcflow ● mscs:nsg:flow

		● zeek_conn and/or bro_conn ● zeek:conn:json and/or bro:conn:json ● zeek_dns and/or bro_dns ● zeek:dns:json and/or bro:dns:json ● *dns* and/or *DNS* (i.e. any source type containing the string dns) ● corelight_conn ● corelight_conn_red ● flowintegrator ● *netflow* ● *sflow* ● *jflow* ● Extrahop:flow ● Vectra:congnito:stream This license can be combined with other daily indexing volume-based Splunk Enterprise licenses. Any ingest of these specific source types in excess of the Daily Indexing Volume of this license will be counted against the general ingest license capacity of Splunk Enterprise.
Splunk Enterprise for Cisco AnyConnect NVM	Number of Endpoints	Limited Source Types: This license will allow users to index only Cisco AnyConnect Network Visibility Module (NVM) source type data. This source type restricted license can be stacked on other non-source type restricted licenses. This license is available exclusively from Cisco Systems. Each Endpoint allows indexing of 10MB/day.
Splunk Analytics for Hadoop	Maximum number of Nodes or Fractional Use of Nodes from which data can be sourced to be analyzed and visualized, as identified in the applicable Order (Note: Data in a Node that has already been indexed by Splunk Enterprise (or Splunk Cloud Platform) will not be counted toward the paid volume.) "***Node***" means a 64 bit Linux operating system or any other operating system identified in the documentation that runs Hadoop TaskTracker or Node Manager to execute Splunk jobs on Hadoop nodes. "***Fractional Use of Nodes***" means the greater of compute load or applicable storage of the number of Nodes in Cluster(s) for a specific use case or business unit, as identified in an Order. "***Cluster***" means a group of Nodes administered by one Hadoop JobTracker or Hadoop Resource Manager.	Maximum of five (5) Nodes from which data can be sourced to be analyzed and visualized

Splunk Data Stream Processor (Splunk DSP)	Number of vCPUs as set forth in the Order Note: For the avoidance of doubt, data ingested into Splunk Enterprise through Splunk DSP counts against the license capacity of Splunk Enterprise.	
Splunk Enterprise Security	Daily Indexing Volume or number of vCPUs as set forth in the Order Note: When consumed within Splunk Cloud Platform, SVC is also available.	
Splunk User Behavior Analytics (Splunk UBA)	Number of User Behavior Analytics Monitored Accounts. "***Number of User Behavior Analytics Monitored Accounts***" means the number of user and service accounts in Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP) or any similar service that is used to authenticate users inside the network; or Daily Indexing Volume. This option is restricted to UBA licenses purchased as an add-on license to Splunk Enterprise Security.	For the latter option, the maximum Daily Indexing Volume is limited to the same data being indexed into Splunk Enterprise Security or a subset thereof and the maximum Number of User Behavior Analytics Monitored Accounts is limited to 250,000.
Splunk Phantom	Number of Events. "***Event***" means a single event or grouping of discrete information regarding an event sent to the Software to act on; or Number of User Seats. "***User Seats***" means the user accounts created for the Software	Maximum Number of Events per 24-hour period measured using Coordinated Universal Time Each distinct user account may be used only by a single user at a time (i.e., simultaneous logins by multiple users leveraging the same user account is disallowed). Limited Use Case: For an end user's internal security purposes only
Splunk SOAR Cloud	Number of User Seats (as defined above for Splunk SOAR on-prem	Each distinct user account may be used only by a single user (i.e., simultaneous logins by multiple users leveraging the same user account is disallowed).
Splunk Mission Control		Only available to customers of Splunk Enterprise Security (either as a stand-alone product or part of a suite).
Splunk Attack Analyzer (formerly, "TwinWave")	Number of User Seats. "***User Seats***" (including the corresponding per User Seat allotment of (10) Daily Submissions as defined below) means the user accounts that are licensed, created, or authorized by a customer for accessing the Splunk Attack Analyzer service. Number of Daily Submissions. "***Daily Submissions***" means the total aggregate number of reported or suspected threat or attack chain analysis requests uploaded under a single User Seat to the Splunk Attack Analyzer service in a given day.	Each User Seat includes a licensed allotment limit of (10) Daily Submissions per User Seat. Additional supplemental Daily Submissions licensed capacity can be optionally purchased. The maximum licensed Submissions capacity limit is equal to the total aggregate per User Seat Daily Submission allotment plus and, if any, the number of additionally purchased supplemental capacity.
Splunk Asset and Risk Intelligence App	Per Asset. "Asset" means all devices, components or subcomponents utilized by Customer that are	One license of ARI means a single instance deployment of the ARI app

	identified by a network address or unique identifier and is subject to, used in connection with, monitored by, discovered by or otherwise serviced by the ARI app. Any asset that appears in the network asset inventory with a last detect date within the previous 30 days is counted against the license limit.	
Splunk App for PCI Compliance	Daily Indexing Volume Note: When consumed within Splunk Cloud Platform, SVC is also available.	
Splunk Insights for Ransomware	Number of Ransomware Monitored Accounts. "***Number of Ransomware Monitored Accounts***" means the number of user and service accounts in Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP) or any similar service that is used to authenticate users inside the network.	Limited Use Case: To detect if any ransomware is present, attempting to be present or attempting to be disseminated in the designated end user's environment. Not stackable with other Splunk licenses.
Splunk IT Service Intelligence (Splunk ITSI)	Daily Indexing Volume or number of vCPUs as set forth in the Order Note: When consumed within Splunk Cloud Platform, SVC is also available.	
Splunk Insights for Infrastructure	Volume of data stored	Storage Limits: Once storage limit is reached, any new data stored will replace the earliest stored data in amounts needed to place total storage at or below the storage limit (First In, First Out). Not stackable with other Splunk licenses.
Splunk On-Call	Number of Users (as defined as the number of unique email addresses)	
Splunk Infrastructure Monitoring ("Splunk IM")	For host-based pricing: Number of Hosts and associated entitlements of Containers and Custom Metrics as indicated in the Order For usage-based pricing: MTS (Metric Time Series) as measured by the unique combination of a metric and a set of associated dimensions as indicated in the Order Note: See Specific Offering Terms at **www.splunk.com/SpecificTerms** for definitions.	Usage and subscription limit enforcement are described **here**.
Splunk APM	For host-based pricing: Number of Hosts and associated entitlements of Containers, Profiled Containers, Monitoring MetricSets, Troubleshooting MetricSets, Trace Volume, and Profiling Volume as indicated in the Order For usage-based pricing: Number of TAPM (Trace Analyzed Per Minute) and associated entitlements of Monitoring MetricSets, Troubleshooting MetricSets, Trace Volume, and Profiling Volume as indicated in the Order	Usage and subscription limit enforcement are described **here**.

	Note: See Specific Offering Terms at **www.splunk.com/SpecificTerms** for definitions	
Splunk Synthetic Monitoring	Number of Browser Test Runs per month A "***Browser Test Run***" refers to each simulation of a full business transaction or user journey using a full web browser. For example, a test run every 5 minutes (12 times per hour) from 3 locations per test will count as 36 Browser Test Runs per hour. Number of API Test Runs per month An "***API Test Run***" refers to a request of a single API endpoint. For multistep API Tests, each request counts as an individual API Test Run. For example, a three request API Test running once a minute consumes 180 API Test Runs per hour. Number of Uptime Test Runs per month An "***Uptime Test Run***" refers to a request of a single URL to check for availability of a website or application. For example, an Uptime Test running once a minute consumes 60 Uptime Test Runs per hour. Number of Web Optimization Scans per month A *"Web Optimization Scan"* refers to a single performance evaluation of a single webpage.	Usage and subscription limit enforcement are described **here**.
Splunk Log Observer	For host-based pricing: Number of Hosts For usage-based pricing: Volume of Indexed Data or Ingested Data "***Indexed Data***" means logs that are parsed, extracted and indexed for fast querying "***Ingested Data***" means logs that are stored in Customer's object store and not queried Note: See Specific Offering Terms at **www.splunk.com/SpecificTerms** for definitions	Usage and subscription limit enforcement are described **here**. Available only to customers of Splunk IM, Splunk APM or Splunk Observability Cloud 30-day retention for Indexed Data. Options to expand to 60-day or 90-day retention for Indexed Data.
Splunk Real User Monitoring ("**Splunk RUM**")	Sessions per month A "***Session***" refers to a group of user interactions on an application (for a maximum of 4 hours). A Session begins when a user loads the front-end application and ends when the application is terminated or expires. Sessions will also expire after 15 minutes of inactivity.	Usage and subscription limit enforcement are described **here**.
Splunk Observability Cloud	Number of Hosts Note: See Specific Offering Terms at **www.splunk.com/SpecificTerms** for additional definitions	Per Host entitlements are described **here**.

Splunk Security for SAP® solutions	Monitored Users Monitored Users are employees, contract workers or other individuals whose credentials, permissions, privileges and/or other user information will be monitored, protected or evaluated by the software, or are authorized to use the reporting console. Monitored Users must be assigned to specific individuals with limited transferability to other individuals. Note: See Specific Offering Terms at www.splunk.com/SpecificTerms for additional details.	SAP software bundled in the Splunk Security for SAP solutions can only be used with the Splunk Security for SAP solution for the duration of the subscription term of the license. Such software may only be used with Splunk Security for SAP solutions to enable its performance, with data access limited to data created or processed by Splunk Security for SAP solutions. The Splunk Security for SAP solution may only be used with Splunk Enterprise and/or Splunk Cloud Platform. Not stackable with SAP licenses or Splunk licenses. Total monitored users will be aggregated across all uses by Third Party Providers and separate use of Enhancements made available to you.
Splunk Federated Search for 3rd party cloud object stores	Data Scan Unit(s) (“DSU(s)”) A DSU is a unit of 10TB of data scanning capabilities using Splunk Federated Search on customer-managed cloud data storage, as further explained in the **service documentation**.	This offering is sold in units of 10 TB (each, a "Data Scan Unit") for scanning external customer-managed cloud object stores using Splunk Federated Search. This offering is subject to overages after depleting all pre-purchased units. Overages will be billed in units of 1TB, rounded up to the nearest terabyte, at one-tenth of the list price of a 10 TB - Data Scan Unit.

Prior versions of SPLUNK OFFERINGS

- Published October 2023
- Published June 2023
- Published April 2023
- Published February 2023
- Published September 2022