Splunk Offerings

Published: Aug 2026

Splunk Offerings Purchase Capacity and Limitation

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

Offering	Capacity	Limitations
Cisco Data Fabric (CDF) -included capacity package	Splunk Cloud Customers on AWS commercial and Victoria Experience may utilize CDF with no additional charge, subject to the following limitations. Any capacity in excess of the stated limitations is subject to the purchase of add-on capacity.	Fixed capacity included in CDF is as follows: • Machine Data Lake - Ingest & Retain: Land and retain but to 10 TB of machine data in Machine Data Lake. • Machine Data Lake – Promote to Analytics Table: 10 GB/day • Federated Search: 100 federated searches/day
Splunk OT Intelligence (Splunk OTI)	**Splunk OTI (Essentials)**: Maximum of two OTI Edge Installations on one Site. One Site only. **Splunk OTI (Advantage)**: No limit on OTI Edge Installations per Site. "**Edge Installation**" means any device that can run or host OTI Edge software as part of a Splunk platform subscription or license. For recommended devices, see here. "**Site**" means a single physical or mobile facility, location, or vessel/vehicle under Customer's ownership or operational control, identified by a distinct and contiguous operational boundary within which the Splunk OTI is deployed, accessed, or used to process or monitor assets.	Splunk OTI (Essentials) Customers may opt to upgrade to Splunk OTI (Advantage) when exceeding the permitted OTI Edge Installations capacity, as further explained in the service document. Customers may refer to the subscription pricing information if an additional Site is required. Note: A Site remains the same regardless of temporary changes in staffing, connectivity, or geographic position. If Customer expands the physical footprint, capacity, or equipment monitored or managed by Splunk OTI such that the operational scope of the Site materially increases beyond its original scale or configuration at the time of license issuance, the materially expanded portion may be deemed a new Site and require an additional license.

PURCHASE CAPACITY AND LIMITATIONS

Splunk Ingest Processor (Essentials tier)	Maximum Daily Processing Volume permitted: 500GB/day "***Daily Processing Volume***" means daily aggregate processing volume through Ingest Processor pipelines	Maximum Daily Processing Volume permitted: 500GB/day. Any volume in excess of this capacity may be subject to limitations in performance. Customers may opt to upgrade to Ingest Processor (Premier tier), as further explained in the service documentation.
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 Enterprise is purchased either as volume licenses (Daily Indexing Volume) or infrastructure licenses (vCPU). Customers cannot stack volume licenses and infrastructure licenses. Premium licenses (such as Enterprise Security and IT Service Intelligence) must match the license type of the core Splunk Enterprise license.
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:cognito: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 Essentials	See "*Splunk Enterprise Security Editions*" below	
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.	UBA Capacity Limitations are set forth here.
Splunk SOAR for on-prem	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 for cloud	Number of User Seats (as defined above in Splunk SOAR for 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 Enterprise Security Premier (ES Premier)	See "*Splunk Enterprise Security Editions*" below	
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 any additionally purchased supplemental capacity.
Splunk Asset and Risk Intelligence App	Per Asset. "Asset" means all devices, components or subcomponents utilized by Customer that are 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.	One license of ARI means a single instance deployment of the ARI app
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.	Limited Use Case: To detect if any ransomware is present, attempting

	"***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.	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 Application Monitoring ("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 Run 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 Database Monitoring	Number of Database Instance(s), as indicated in the Order "**Database Instance**" means a unique, running installation or operational service of a Database Management System (DBMS) software that is monitored by Splunk Database Monitoring.	Usage and subscription limit enforcement are described here
Splunk Secure Application	Note: Splunk Secure Application – Vulnerabilities Detection is currently available as an add-on to Splunk APM. Number of Hosts and associated entitlements of an Events ingestion volume limited to an aggregate of 8GB per day. (Vulnerabilities events 1 GB per day and Attacks events 7 GB per day) "**Event**" means a single runtime application security event detected by Splunk Secure Application – Vulnerabilities Detection (e.g., a 3rd party library detected in Customer's application service that may have runtime vulnerability). See Specific	Usage and subscription limit enforcement are described here

	Offering Terms at www.splunk.com/SpecificTerms for additional definitions	
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 additional details.	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 Agent Observability	30 million Spans/year 48 billion Luna Tokens/year A "**Span**" means a single action in an AI workflow within Agent Observability. A "**Luna Token**" means a data unit used to interpret text chunk (including words, punction and spaces).	Sold as part of package. Add-ons sold in units of 10K Spans or 200B Luna Tokens.
Splunk AppDynamics	Splunk AppDynamics license entitlements, restrictions, and definitions are available at these links: **Splunk AppDynamics Hosted Service**: https://docs.appdynamics.com/appd/24.x/24.6/en/cisco-appdynamics-licensing/license-entitlements-and-restrictions **Splunk AppDynamics On-Premise Product**: https://docs.appdynamics.com/appd/on	

	prem/24.x/24.4/en/cisco-appdynamics-licensing/on-premises-licensing/on-premises-license-entitlements-and-restrictions		
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.
Splunk Enterprise Security Editions	**Essentials**	**Premier**	
Ingest	**measurement**: Daily Indexing Volume (volume) and SVCs or vCPUs, as set forth in the order	**measurement**: Daily Indexing Volume (volume) and SVCs or vCPUs, as set forth in the order	volume: Splunk Cloud Platform or Splunk Enterprise vCPU: Splunk Enterprise SVC: Splunk Cloud Platform
Automated Threat Analysis (ATA)	N/A	**measurement**: Per submission	volume: max 2K ATA submissions per day vCPU: max 2K ATA submissions per day SVC: max 2K ATA submissions per day
Exposure Analytics (EA)	N/A	**measurement**: Per asset	volume: max 1M EA assets per tiered license vCPU: max 1M EA assets per tiered license SVC: max 1M EA assets per tiered license
SOAR	**measurement**: Per playbook run	**measurement**: Per playbook run	volume: max 250k SOAR playbook runs per day vCPU: max 250k SOAR playbook runs per day SVC: max 250k SOAR playbook runs per day

Triage Agent (TA)	N/A	**measurement**: Per finding	volume: max 200 TA findings per day vCPU: max 200 TA findings per day SVC: max 200 TA findings per day
UEBA	N/A	**measurement**: Daily Indexing Volume (volume) and SVCs or vCPUs, as set forth in the order	volume: max 0.5 UEBA GB per ingested GB vCPU: max 2.5 UEBA GB per vCPU GB SVC: mad 5.0 UEBA GB per SVC GB