# Splunk Offerings

Published: April 2021

| Offering | Capacity | Limitations |
|---|---|---|
| Splunk Enterprise | Daily Indexing Volume or number of vCPUs as set for the in the Order<br>"**Daily Indexing Volume**" means the daily aggregate volume of uncompressed data for indexing as set forth in the Order<br>"**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.<br>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 | Daily Indexing Volume or number of Splunk Virtual Compute ("SVC")<br>"**Splunk Virtual Compute**" means a unit of capabilities in Splunk Cloud that includes the following resources: compute, memory and I/O as further explained in the service documentation.<br>NOTE: Splunk Cloud is also available as part of Splunk Cloud Foundations, which can be purchased only based on the number of SVCs. Please learn more here. | |
| Splunk Enterprise Rapid Adoption Packages | Number of Use Cases identified in the Order<br>"**Use Cases**" are defined and listed here: https://www.splunk.com/en_us/legal/use-case-definitions.html<br>Note: The Rapid Adoption Packages can be purchased in connection with Splunk Cloud as well. | Maximum Daily Index Volume permitted: 25GB (regardless of number of Use Cases)<br>Deployment type: Limited to a single instance deployment<br>Not stackable with other Splunk licenses |
| Splunk Enterprise for DNS & Netflow Data | Daily Indexing Volume<br>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:<br>• aws:vpc:flowlogs<br>• Aws:cloudwatchlogs:vpcflow<br>• mscs:nsg:flow<br>• zeek_conn and/or bro_conn<br>• zeek:conn:json and/or bro:conn:json<br>• zeek_dns and/or bro_dns<br>• zeek:dns:json and/or bro:dns:json<br>• *dns* and/or *DNS* (i.e. any source type containing the string dns)<br>• flowintegrator<br>• *netflow*<br>• *sflow*<br>• *jflow* |

| Offering | Capacity | Limitations |
|---|---|---|
| Splunk Enterprise for DNS & Netflow Data (cont.) | | This license can be combined with other daily indexing volume-based Splunk Enterprise licenses.<br>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.<br>This license is available exclusively from Cisco Systems.<br>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) will not be counted toward the paid volume.)<br>"**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.<br>"**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.<br>**"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<br>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 Protected Devices or vCPUs as set forth in the Order<br>"**Protected Device**" means any device or asset with an IP address (e.g., VoIP systems, LDAP Directory, switches, router, desktops, tablets, phones, etc.) visible in data sent to Splunk platform. It is not just the devices sending logs to Splunk but also the devices that are mentioned in the logs. For example, a firewall supporting 1,000 desktop PC's connecting to the Web would be 1,001 devices total, as each desktop PC will be referenced in the firewall events, even though all those events are being sent from the single firewall device to Splunk.<br>Note: Existing customers can increase their license capacity based on the number of SVCs they have purchased. | NOTE: Customers may purchase subscription under the Protected Devices metric with Splunk Cloud Foundations only. |

| Offering | Capacity | Limitations |
|---|---|---|
| Splunk User Behavior Analytics (Splunk UBA) | Number of User Behavior Analytics Monitored Accounts.<br>**"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<br>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<br>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<br>Each distinct user account may be used only by a single user at a time.<br>Limited Use Case: For an end user's internal security purposes only |
| Splunk Mission Control | Number of User Seats<br>Note: A certain number of User Seats of Splunk Mission Control will be entitled to customers of Splunk Enterprise Security based on their current license entitlement of Splunk Enterprise Security. Learn more at Seat Entitlement. | Available on a limited basis to customers of Splunk Enterprise Security (either as a stand-alone product or part of a suite)<br>To be used for security use cases only. |
| Splunk App for PCI Compliance | Daily Indexing Volume<br>Note: When consumed within Splunk Cloud, SVC is also available. | |
| Splunk Insights for Ransomware | Number of Ransomware Monitored Accounts.<br>"**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.<br>Not stackable with other Splunk licenses. |
| Splunk IT Service Intelligence (Splunk ITSI) | Daily Indexing Volume or number of Managed Entities or vCPUs as set forth in the Order<br>Number of "**Managed Entities**" refers to the total number of Hosts (as defined in IT Cloud) and Assets. An "**Asset**" refers to any Protected Device or API endpoints (e.g., serverless functions, ActiveDirectories, M365 service, or Twitter feed) sending data directly to Splunk but that is not already counted as a Host.<br>Note: Existing customers can increase their license capacity based on the number of SVCs they have purchased. | |
| 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).<br>Not stackable with other Splunk licenses. |

| Offering | Capacity | Limitations |
|---|---|---|
| Splunk On-Call | Number of Users | https://www.splunk.com/en_us/software/pricing/devops.html#splunk-on-call |
| Splunk Infrastructure Monitoring ("Splunk IM") | For host-based pricing: Number of Hosts and associated entitlements of Containers, Custom Metrics, and High Resolution Metrics as indicated in the Order<br>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<br>Note: See Specific Offering Terms at www.splunk.com/SpecificTerms for definitions. | https://www.splunk.com/en_us/software/pricing/faqs/devops.html#Splunk-Infrastructure-Monitoring |
| Splunk APM | For host-based pricing: Number of Hosts and associated entitlements of Containers, Monitoring MetricSets, Troubleshooting MetricSets, and Trace Volume as indicated in the Order<br>For usage-based pricing: Number of TAPM (Trace Analyzed Per Minute) and associated entitlements of Monitoring MetricSets, Troubleshooting MetricSets, and Trace Volume as indicated in the Order<br>Note: See Specific Offering Terms at www.splunk.com/SpecificTerms for definitions | https://www.splunk.com/en_us/software/pricing/faqs/devops.html#Splunk-APM |
| Splunk Synthetic Monitoring | Number of Browser Test Runs per month<br>A "**Browser Test Run**" refers to each simulation of a full business transaction or user journey (up to a maximum of 25 steps). For example, a test with 26 steps that is run every 5 minutes (12 times per hour) from 3 locations per test will count as 72 Browser Test Runs per hour.<br>Number of API Test Runs per month<br>An "**API Test Run**" refers to a request of a single endpoint or URL using uptime tests or API tests. 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. | |
| Splunk Log Observer | For host-based pricing: Number of Hosts<br>For usage-based pricing: Volume of Indexed Data or Ingested Data<br>"**Indexed Data**" means logs that are parsed, extracted and indexed for fast querying<br>"**Ingested Data**" means logs that are stored in Customer's object store and not queried<br>Note: See Specific Offering Terms at www.splunk.com/SpecificTerms for definitions | Available only to customers of Splunk IM, Splunk APM or Splunk Observability Cloud<br>30-day retention for Indexed Data |

| Offering | Capacity | Limitations |
|---|---|---|
| Splunk Real User Monitoring ("Splunk RUM") | Sessions per month<br>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. | |
| Splunk IT Cloud | Number of Hosts<br>"**Host**" means a virtual machine or physical server with a dedicated operating system up to 64 GB of memory<br>Note: See Specific Offering Terms at www.splunk.com/SpecificTerms for additional definitions | Per Host entitlements are described here |
| Splunk Security Cloud | Number of Protected Devices (as defined in Splunk Enterprise Security above) | Per Protected Device entitlements are described here. |
| Splunk Observability Cloud | Number of Hosts (as defined above)<br>Note: See Specific Offering Terms at www.splunk.com/SpecificTerms for additional definitions | Per Host entitlements are described here |

Updated on April 15, 2021