Splunk Terms for Splunk Offerings

Published: March 2024

Splunk Cloud Platform

1. **Service Description**
   https://docs.splunk.com/Documentation/SplunkCloud/latest/Service/SplunkCloudservice

2. **Security and Protection of Customer Content on Splunk Cloud Platform.**
   Splunk maintains administrative, physical and technical safeguards to protect the security of Customer Content on Splunk Cloud Platform as set forth in the Splunk Cloud Security Addendum located at https://www.splunk.com/en_us/legal/splunk-cloud-security-addendum.html ("**Cloud Security Addendum**").

   Splunk's security safeguards include, without limitation, employee (and contractor, as applicable) security training, background testing and confidentiality obligations. Splunk's security controls adhere to generally accepted industry standards, are subject to audit by third-parties (as described in the Cloud Security Addendum), and are designed to (a) ensure the security and integrity of Customer Content; (b) detect and protect against threats or hazards to the security or integrity of Customer Content; and (c) prevent unauthorized access to Customer Content.

3. **Service Level Schedule – Splunk Cloud Platform**
   Splunk's Splunk Cloud Service Level Schedule, set forth at https://www.splunk.com/en_us/legal/splunk-cloud-service-level-schedule.html, will apply to the availability and uptime of the Splunk Cloud Platform, subject to planned downtime and any unscheduled emergency maintenance according to Splunk's Maintenance Policy referenced in the Splunk Service Level Schedule. Customer will be entitled to service credits for downtime in accordance with the applicable Service Level Schedule.

4. **Data Usage Policy for Splunk Cloud Platform**
   For Subscriptions based on Maximum Daily Indexing Volume, Customer is entitled to periodically exceed the daily volume purchased by Customer in accordance with Splunk's data ingestion and daily license usage policy set forth at http://docs.splunk.com/Documentation/SplunkCloud/latest/User/DataPolicies#Data_ingestion_and_daily_license_usage

5. **FedRAMP or StateRAMP for Splunk Cloud Platform**
   If you access or use any Hosted Services in the specially isolated Amazon Web Services ("**AWS**") GovCloud (US) region that are provisioned in a FedRAMP or StateRAMP authorized environment ("Government Cloud"), you acknowledge the Government Cloud is a more restricted environment. As a more restricted environment, Administrative Access to the Government Cloud must be restricted to individuals that are US Persons, as defined under 22 CFR part 120.62 ("Approved Personnel"). Administrative Access is defined as Customer's users in roles with capabilities that are exclusive to the "Admin" and/or "Sc admin" roles set forth in the "Table of Splunk platform capabilities" page here: https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/Rolesandcapabilities#Table_of_Splunk_platform_capabilities.

   Customer acknowledges that FedRAMP or StateRAMP authorized offerings will only meet the standards of an authorized FedRAMP or StateRAMP Hosted Service, respectively, if Customer performs its obligations as set forth in both the "FedRAMP Low or Moderate Control Implementation Summary (CIS) Worksheet" and the "FedRAMP Low or Moderate Customer Responsibility Matrix (CRM) Worksheet" available from Splunk upon request. To maintain the security of the FedRAMP or StateRAMP authorized offerings, Customer agrees to cooperate with Splunk to remediate any security vulnerabilities upon Splunk's request.

Splunk On-Call

1. **Service Description**
   https://help.victorops.com

2. **Additional Users**
   If Customer wants to add additional permitted users, Customer can do so through the Offering administrative portal, and either (i) Splunk will immediately charge Customer's credit card for the prorated amount for the current term, or (ii) if Customer does not have a credit card on file, then Splunk will invoice Customer for the additional permitted users in accordance with the Terms.

3. **Support**
   Splunk On-Call support is provided via the following portal: https://help.victorops.com/knowledge-base/how-to-contact-splunk-on-call-support.

4. **Security of Customer Content**
   Splunk maintains administrative, physical and technical safeguards to protect the security of Customer Content on Splunk On-Call as set forth in the Splunk On-Call Security Addendum located at https://www.splunk.com/en_us/legal/splunk-on-call-security-addendum.html ("Splunk On-Call Security Addendum").
   Customer acknowledges and agrees that Splunk On-Call has not yet undergone a security audit by an independent third party and therefore does not have SOC2 or ISO27001 certification.

5. **Service Level Schedule**
   Splunk's Splunk On-Call Service Level Schedule, set forth at https://www.splunk.com/en_us/legal/splunk-on-call-service-level-schedule.html, will apply to the availability and uptime of the Splunk On-Call service.

Splunk Observability Cloud

Splunk Observability Cloud includes the following services (as part of a suite or as individual services): Splunk Infrastructure Monitoring, Splunk Application Performance Monitoring (Splunk APM), Splunk Real User Monitoring (Splunk RUM), and Splunk Log Observer, and Splunk Synthetic Monitoring.

1. **Service Descriptions**
   https://docs.splunk.com/Observability

2. **Usage, Subscription Limits Enforcement, and Entitlements**
   https://www.splunk.com/en_us/legal/usage-subscription-limits-enforcement-and-entitlements.html

3. **Security and Protection of Customer Content**
   a. Splunk maintains administrative, physical and technical safeguards to protect the security of Customer Content as set forth in the Security Addendum located at https://www.splunk.com/en_us/legal/splunk-observability-security-addendum.html ("**Observability Security Addendum**"). Splunk's security safeguards include, without limitation, employee (and contractor, as applicable) security training, background testing and confidentiality obligations.
   b. Splunk's security controls adhere to generally accepted industry standards, are subject to audit by third-parties (as described in the Observability Security Addendum), and are designed to (a) ensure the security and integrity of Customer Content; (b) detect and protect against threats or hazards to the security or integrity of Customer Content; and (c) prevent unauthorized access to Customer Content.

4. **Service Level Schedule – Splunk Observability Cloud**
   Splunk's Splunk Observability Cloud Service Level Schedule, set forth at https://www.splunk.com/en_us/legal/observability-service-level-schedule.html, will apply to the availability and uptime of the Splunk Observability Cloud. Customer will be entitled to service credits for downtime in accordance with the applicable Service Level Schedule.

5. **Definitions.** The following definitions are applicable to Orders for Splunk Observability Cloud services.

   "Analyzed Trace" means a trace that was sent to and processed by Splunk APM.

   "APM Identities" means the count of all unique spans and initiating operations across all service endpoints for metricization. Additional dimensions on these, specified as select span tags, create further APM Identities based on the count of values of those tags.

   "Container" means a stand-alone, executable package of software that includes application software and sufficient operating system libraries to run in isolation but shares the underlying operating system with other Containers.

   "Custom Metric" means any Metric that is not automatically collected and reported as part of Splunk's standard Host-

based integrations.

"Host" means a virtual machine or physical server being monitored.

"Metric" means any unique combination of a metric name and dimension value reporting data to Splunk within the last hour.

"Monitoring MetricSet" means a set of metrics created by default for certain components in a monitored distributed application and designed to alert on changes in application performance. A Monitoring MetricSet includes metrics such as request rate, error rate, and latency percentiles.

"MTS" means Metric Time Series.

"**Profiled Container**" means a Container that is instrumented to send Profiling data to Splunk APM.

"**Profiling**" means automated collection and analysis of code behavior data from runtime environments.

"**Profiling Volume**" means the amount of Profiling data that customers pay for to be ingested by Splunk APM.

"**Serverless Function**" means a stand-alone, executable package of single-purpose software that runs in serverless environments and is triggered by an event or message.

"**Session Volume**" means the amount of Session data that customers pay for to be ingested by Splunk RUM.

"Span" means an area of code instrumented to be captured as part of a recorded transaction (eg. rpc, function). Each service can have many spans. At a minimum, there will be 2 spans - inbound and outbound to the service.

"TAPM" means Trace Analyzed Per Minute.

"Trace" means an array of spans represented as a Directed Acyclic Graph.

"Trace Volume" means amount of trace data per minute that customers pay for to be ingested by Splunk APM.

"Troubleshooting MetricSet" means a set of metrics created by default for certain components in a monitored distributed application and designed to enable detailed analysis and troubleshooting of an application. A Troubleshooting MetricSet includes metrics such as the request rate, error rate, root-cause error rate and latency percentiles.

Splunk Synthetic Monitoring

1. **Service Description**
   https://help.rigor.com/hc/en-us

2. **Security**
   Customer hereby acknowledges and agrees that Splunk Synthetic Monitoring has not yet undergone a security audit by an independent third party and therefore does not have SOC2 or ISO27001 certification. **The security terms in Splunk's Cloud Security Addendum and the Observability Security Addendum do NOT apply.** Customer may not upload or transmit to this environment any regulated data, such as financial information (including PCI-DSS data), protected health information, ITAR data or classified information.

3. **Usage and Subscription Limits Enforcement, and Entitlements**
   https://www.splunk.com/en_us/legal/usage-subscription-limits-enforcement-and-entitlements.htm

Splunk Secure Gateway

Splunk Secure Gateway app facilitates communication between mobile devices and Splunk instances with an end-to-end encrypted free cloud service called Spacebridge. Spacebridge cloud service environment, and the service itself, is separate from the Splunk Enterprise and Splunk Cloud offering. Spacebridge is a free Hosted Service and use is subject to Splunk General Terms available at: https://www.splunk.com/en_us/legal/splunk-general-terms.html. See here to learn more about the Spacebridge offering. Learn more

You may not transmit regulated data, including PHI data of PCI data, to Spacebridge unless you are using Spacebridge with a managed Splunk Cloud deployment and have specifically purchased the applicable regulated environment for that managed Splunk Cloud deployment. Spacebridge does not leverage the FIPS 140-2 validated Splunk Cryptographic Module and may not be used in environments that require this standard.

You must agree to use Spacebridge to use Splunk Secure Gateway. If you want to permanently disable the use of

Spacebridge, you must disable Splunk Secure Gateway. Disable Splunk Secure Gateway in **Apps > Manage Apps.** If you're using a managed Splunk Cloud deployment, file a support ticket to disable Splunk Secure Gateway.

Splunk Security Offerings

Splunk Intelligence Management (TruSTAR legacy service)

1. **Service Description**
   https://docs.splunk.com/Documentation/SIM/current/User/Intelligenceoverview

2. **Security**
   Customer hereby acknowledges and agrees that Splunk Intelligence Management no longer has SOC2 attestation as audited by an independent third party.

Splunk Security for SAP® solutions

1. Service Description

https://docs.splunk.com/Documentation/SAPSecurity

2. General Availability

License to use Splunk Security for SAP solutions is subject to general availability. In the event this Purchased Offering is no longer generally available, Splunk may terminate the Purchased Offering and refund to you any prepaid fees covering the unexpired Term.

3. Monitored Users

A "Monitored User" cannot be assigned to more than one (1) individual. However, a Monitored User assignment may be transferred from one (1) individual to another, but only if the individual to which the Monitored User was assigned is:

a. is on vacation;
b. is absent due to sickness;
c. has their employment terminated;
d. is moved into a new job function which no longer requires them to use Splunk Security for SAP solutions; or
e. is subject to a condition that is otherwise agreed by Splunk.

4. Additional License Restrictions

SAP software bundled in the Splunk Security for SAP solution ("SAP Software") can only be used with the Splunk Security for SAP solution for the duration of the subscription term of the license to Splunk Security for SAP solutions. The SAP 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.

5. Restricted Activity

You may not distribute or publish keycodes or otherwise endanger the security or operation of Splunk Security for SAP solutions, including the SAP Software, or other materials provided in connection therewith.

Notwithstanding the General Terms, You do not have the right to make additional copies of Splunk Security for SAP solutions for archival and back-up purposes.

SAP Software and related material is Confidential Information. With respect to your use of Splunk Security for SAP solutions, you agree not disclose or reveal any such Confidential Information to any person other than your Affiliates, employees, contractors, legal representatives, accountants, or other professional advisors whose access is necessary to enable you to exercise your rights or perform your obligations under the General Terms and who are under obligations of confidentiality substantially similar to those in the General Terms, including these Specific Terms for Splunk Offerings.

6. Your responsibilities

You are responsible for (i) setting up, installing, configuring and managing the Splunk for SAP solution on any SAP software, and (ii) obtaining internet connectivity. Splunk will not be responsible for loss due to your failure to comply

with your responsibilities in this section or for activities that take place in your SAP environment (which shall be governed by your applicable agreement with SAP).

7. Not for Resale and Evaluation Licenses

If Splunk makes available the Splunk Security for SAP solution pursuant to Section 1.D of the General Terms, the Splunk Security for SAP solution must not be used in production and must be destroyed or deleted when the license terminates**.** Licenses to Splunk Security for SAP solutions made available under Section 1.D of the General Terms may be terminated at any time upon written notice from Splunk.

8. SAP Open Source

Applicable specific conditions related to certain open source products made available in SAP Software are part of the applicable product documentation and apply to your use of any such open source products. The SAP Software open source components and their related licenses are documented at https://docs.splunk.com/Documentation/SAPSecAddOn/1.0.0/User/Credits.

9. SAP Software License Specific Terms

Splunk Security for SAP solutions includes SAP Enterprise Threat Detection - OEM and SAP HANA, RTed Appl&BW-new/subsq partial ("SAP Products"). Subject to the license restrictions under the General Terms, including these Specific Terms for Splunk Offerings, SAP products come with additional software usage rights. Such rights can be found in the SAP Software Usage Rights available at https://assets.cdn.sap.com/agreements/oem-agreements/sur/sap-partneredge-build-formerly-oem-software-use-rights-english-v7-2022.pdf. Exercise of any of such additional rights shall be subject to the SAP Software Usage Rights.

Splunk Asset Risk Intelligence

1. Security Industry Certifications

Customer acknowledges and agrees that Splunk Asset Risk Intelligence has not yet undergone a security audit by an independent third party and therefore does not have SOC2 or ISO27001 certification.

Splunk Attack Analyzer (TwinWave legacy service)

1. Service Level Schedule

The Service Level Schedule for the Splunk Attack Analyzer, set forth at https://www.splunk.com/en_us/legal/attack-analyzer-service-level-schedule.html, will apply to service availability of the Splunk Attack Analyzer Hosted Service. Customer will be entitled to service credits for downtime in accordance with the Service Level Schedule.

2. Security of Customer Content

Splunk maintains administrative, physical and technical safeguards to protect the security of Customer Content on Splunk Attack Analyzer as set forth in the Splunk Attack Analyzer Security Addendum located at https://www.splunk.com/en_us/legal/splunk-attack-analyzer-security-addendum.html ("SAA Security Addendum").

Customer acknowledges and agrees that Splunk Attack Analyzer has not yet undergone a security audit by an independent third party and therefore does not have SOC2 or ISO27001 certification.

3. Use of Customer Content

The operation and functionality of Splunk Attack Analyzer depends on the continuous improvement of detection capabilities through the application of threat intelligence information that is derived from the data our customers submit to the Splunk Attack Analyzer service. Accordingly, Customer agrees that Splunk may use Customer Content submitted to Splunk Attack Analyzer for purposes of analyzing threat trends, enhancing detection capabilities, and otherwise testing, improving and operating Splunk's products and services, provided that Customer Content will not be disclosed to any third party except in aggregated format and in a manner that does not identify Customer as the source of the Customer Content and could not otherwise be attributable to Customer or any individual.

Hosted Services Environment Terms

FedRAMP or StateRAMP for Splunk Cloud Platform

If you access or use any Hosted Services in the specially isolated Amazon Web Services ("AWS") GovCloud (US) region that are provisioned in a FedRAMP or StateRAMP authorized environment ("Government Cloud"), you acknowledge the Government Cloud is a more restricted environment. As a more restricted environment, Administrative Access to the Government Cloud must be restricted to individuals that are US Persons, as defined under 22 CFR part 120.62 ("Approved Personnel"). Administrative Access is defined as Customer's users in roles with capabilities that are exclusive to the "Admin" and/or "Sc admin" roles set forth in the "Table of Splunk platform

capabilities” page here: https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/Roles andcapabilities#Table_of_Splunk_platform_capabilities.

Customer acknowledges that FedRAMP or StateRAMP authorized offerings will only meet the standards of an authorized FedRAMP or StateRAMP Hosted Service, respectively, if Customer performs its obligations as set forth in both the “FedRAMP Low or Moderate Control Implementation Summary (CIS) Worksheet” and the “FedRAMP Low or Moderate Customer Responsibility Matrix (CRM) Worksheet” available from Splunk upon request. To maintain the security of the FedRAMP or StateRAMP authorized offerings, Customer agrees to cooperate with Splunk to remediate any security vulnerabilities upon Splunk’s request.

Prior Versions of SPLUNK TERMS FOR OFFERINGS

- Published January 2024
- Published October 2023
- Published August 2023
- Published June 2023
- Published February 2023