SPECIFIC TERMS FOR SPLUNK OFFERINGS

Last updated: June 2026

Additional terms apply to certain Splunk Offerings as well as to certain Hosted Services environments. The below terms apply to your Offerings and Hosted Services as applicable and are incorporated into the Splunk General Terms.

Splunk Offerings Terms

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 out in the Splunk Cloud Security Exhibit located at https://www.splunk.com/en_us/legal/splunk-cloud-security-addendum.html ("**Cloud Security Exhibit**").

   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 Exhibit), 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 out 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 out at https://docs.splunk.com/Documentation/SplunkCloud/latest/Service/SplunkCloudservice# Data_policies

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 General 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 out in the Splunk On-Call Security Exhibit located at https://www.splunk.com/en_us/legal/splunk-on-call-security-exhibit.html ("Splunk On-Call Security Exhibit").

   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 out 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), Splunk Log Observer Connect, 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 out in the Security Exhibit located at https://www.splunk.com/en_us/legal/splunk-observability-security-addendum.html ("**Observability Security Exhibit**"). 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 Exhibit), 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.

Page Sections

Splunk Offerings Terms

Splunk Cloud Platform

Splunk On-Call

Splunk Observability Cloud

Splunk Observability Free Edition

Splunk AppDynamics

Splunk Synthetic Monitoring (Legacy Rigor Platform)

Splunk Secure Gateway

Splunk Security Offerings Terms

Splunk Asset and Risk Intelligence and Exposure Analytics

Splunk Attack Analyzer and Automated Threat Analysis

Splunk Enterprise Security

Splunk Intelligence Management (TruSTAR legacy service)

Splunk SOAR

Hosted Services Environments Terms

FedRAMP or StateRAMP for Splunk Cloud Platform

Business Associate Agreement

Splunk AI Offerings Terms

Splunk AI Offerings

Cisco Firewall Promotional Splunk Capacity Offer

Promotional Capacity Terms

c. Customer is responsible for using Splunk Observability Cloud in compliance with applicable laws, including but not limited to providing notice to and obtaining any necessary consent from individuals whose data will be collected by Customer's use of the services.

4. **Service Level Schedule – Splunk Observability Cloud**
Splunk's Splunk Observability Cloud Service Level Schedule, set out 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. **Integration with PCI-DSS-Certified Environments**
Customer hereby acknowledges that Splunk Observability Cloud is not PCI-DSS-certified. Integrating PCI-DSS-certified platforms with Splunk Observability Cloud may result in exposure of PCI data to non-PCI-certified environments.

6. **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 Observability Free Edition

Terms are available at https://www.splunk.com/en_us/legal/splunk-observability-free-edition-terms.html

Splunk AppDynamics

1. **Service Description and Documentation**
Splunk AppDynamics is offered as a Hosted Service and an On-Premise Product, as indicated in the relevant Order and described more fully in the Documentation available at http://docs.appdynamics.com (The Hosted Service and On-Premise Product versions are collectively referred here to as the "Product"). The Product provides performance monitoring and analysis of applications, websites, databases and IT infrastructure.

2. **License Entitlements and Restrictions**

Splunk AppDynamics Hosted Service: https://help.splunk.com/en/appdynamics-saas

Splunk AppDynamics On-Premise Product:
https://docs.appdynamics.com/appd/onprem/24.x/24.4/en/cisco-appdynamics-licensing/on-premises-licensing/on-premises-license-entitlements-and-restrictions

3. **Security, and Protection of Customer Data**

a. The administrative, physical and technical safeguards applicable to the delivery, provisioning, support, and maintenance of the Product are set forth in the Cisco Information Security Exhibit located at https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/1604543381171981 (“Cisco ISE”).

b. These security safeguards adhere to generally accepted industry standards, are subject to audit by third parties as described in the Cisco ISE 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.

c. Customer is responsible for using the Product in compliance with applicable laws, including but not limited to providing notice to and obtaining any necessary consent from individuals whose data will be collected by Customer’s use of the services.

4. **Service Level Agreement and Enterprise Support**

a. The Service Level Agreement exhibit applies to your use of the Splunk AppDynamics Hosted Service. The Service Level Agreement exhibit does not apply to the Splunk AppDynamics On-Premise Product.

b. Enterprise Support, as defined and detailed in the Splunk AppDynamics Enterprise Support exhibit, apply to your use of the Splunk AppDynamics Product

The term "Offer Description" in the exhibits referenced in this Section 4 refers to these Specific Terms for Splunk Offerings, including this Splunk AppDynamics section. Support pursuant to the Service Level Agreement and Enterprise Support exhibits is delivered by Cisco Systems Inc. (or its designated Affiliate) (“Cisco”).

5. **Systems Information**
The Product collects Systems Information to assist with understanding product usage and enabling product improvements. For more information on Systems Information, please see https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/1604543672547988

6. **Data Deletion and Retention**
Notwithstanding anything in the General Terms to the contrary, the Splunk AppDynamics Hosted Service retains personal data in registration information and email delivery information for no more than one (1) year after expiration or termination of the Splunk AppDynamics Hosted Service Term. Personal data in support information will be deleted upon request.

7. **Additional Limits on Usage**
In addition to any usage limits described in the General Terms and Documentation, you will not (and will not authorize any third party to) configure the Product to intentionally collect any: (1) social security numbers or other government-issued identification numbers, (2) unencrypted passwords or other authentication credentials, (3) health information, biometric data, generic data, or any other similar data, (4) payment, financial, insurance or similar information, (5) data relating to a person under the age of 13 years old, or (6) data that is classified as sensitive data, or special category data, under applicable laws. A breach of this paragraph is considered a misuse of our intellectual property rights.

8. **Additional Obligations for the Splunk AppDynamics On-Premise Product**

a. If you purchase the Splunk AppDynamics On-Premise Product, you must download, install, and host it in your environment, where you will exercise exclusive control over it and ensure appropriate back-ups of your data are done.

b. You will maintain the Splunk AppDynamics On-Premise Product software in a secured environment accessible only to you and your Third-Party Providers.

c. You will replace or patch the Splunk AppDynamics On-Premise Product software when new releases become available.

d. You will not (and will not authorize any third party to) publish the result of any benchmarking tests run on the Splunk AppDynamics On-Premise Product.

e. You will implement and maintain appropriate technical and organizational measures designed to protect the Splunk AppDynamics On-Premise Product software against accidental loss, destruction or alteration, unauthorized access, or unlawful destruction.

f. Oracle Corporation is a third-party beneficiary under the General Terms solely with respect to the MySQL database included with the Splunk AppDynamics On-Premise Product software.

9. **Open Source Technology**
Separate licenses terms apply to third party open-source technology used in the Product. Open-source terms are found at Cisco’s Open Source webpage, available at: https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html

10. **End of Life Policy**
Splunk may end of life the Product in accordance with the Cisco End of Life policy, available at: https://www.cisco.com/c/en/us/products/eos-eol-policy.html

11. The following products and support, which may be included with your purchase of the Product, are governed by the terms and conditions located at https://www.snpgroup.com/en/eula/ or any superseding agreement between You and Datavard AG, Germany and/or SNP Deutschland GmbH (collectively “SNP”): SNP CrystalBridge Monitoring (formerly known as Datavard Insights) licensed under the “SAP Peak Bundle,” “Enterprise Edition for SAP Solutions Bundle,” or “SAP Peak or Enterprise Edition for SAP Solutions Bundle” software suites; and support for such software suites from SNP.

Splunk Synthetic Monitoring (Legacy Rigor Platform)

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

2. **Security**
Customer hereby acknowledges and agrees that Splunk Synthetic Monitoring (Legacy Rigor Platform) 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 Exhibit and the Observability Security Exhibit 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, Subscription Limits Enforcement, and Entitlements**
   https://www.splunk.com/en_us/legal/usage-subscription-limits-enforcement-and-entitlements.html

Splunk Secure Gateway

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 or 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 Terms

Splunk Asset and Risk Intelligence and Exposure Analytics feature of ES Premier

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

2. **Support**
   Support for Splunk Asset and Risk Intelligence is set out at https://www.splunk.com/en_us/pdfs/data-sheets/asset-risk-intelligence.pdf

Splunk Attack Analyzer and Automated Threat Analysis feature of ES Premier

1. **Service Level Schedule**
   The Service Level Schedule for the Splunk Attack Analyzer, set out 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. **Support**
   Support for Splunk Attack Analyzer is set out at https://www.splunk.com/en_us/pdfs/data-sheets/attack-analyzer.pdf

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

4. **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.

5. **Use of Customer Content by Cisco Talos**
   Cisco's Talos Threat Hunting Service may be deployed as part of the Splunk Attack Analyzer service in which case the Cisco Talos team may access Customer Content if such data triggers or is related to a security event. Talos Threat Hunting will process data as set forth in the Threat Hunting Offer Disclosure.

Splunk Enterprise Security

1. **Threat Data Usage**
   The operation and functionality of Splunk security Offerings depends on continuously updating and improving detection capabilities through the application of threat intelligence, threat detection, and security event information that is derived from the data our customers submit to Splunk's Enterprise Security Hosted Service ("Threat Data"). Accordingly, Customer instructs and grants Splunk the right to extract a copy of Threat Data and use Threat Data in connection with providing, creating, and improving our Offerings, which includes training and improving algorithms, detections, and models, and using artificial intelligence, machine learning, and other techniques with Threat Data to gain insights, and to make the Offerings more responsive and predictive to the needs of you and our customers, and to grant to others rights to do any of the foregoing, provided that in all cases Splunk's use of Threat Data is subject to Splunk's obligations under the General Terms with respect to Customer Content and Confidential Information. More information about this use is set out in our Documentation at https://help.splunk.com/en/?resourceId=ES_User_ShareThreatData

2. **Use of Customer Content by Cisco Talos**
   Cisco's Talos Threat Hunting may be deployed as part of the Splunk Enterprise Security service. The Cisco Talos team may access Customer Content if such data triggers or is related to a security event. Talos Threat Hunting will process data as set forth in the Threat Hunting Offer Disclosure.

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 SOAR

Use of Customer Content by Cisco Talos
Cisco's Talos Threat Hunting may be deployed as part of the Splunk SOAR service. The Cisco Talos team may access Customer Content if such data triggers or is related to a security event. Talos Threat Hunting will process data as set forth in the Threat Hunting Offer Disclosure.

Hosted Services Environments 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.

Customer acknowledges that FedRAMP Moderate or StateRAMP Moderate authorized offerings will only meet the standards of an authorized FedRAMP Moderate or StateRAMP Moderate Hosted Service, respectively, if Customer performs its obligations as set out 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. Customer acknowledges that FedRAMP High authorized offerings will only meet the standards of an authorized FedRAMP High Hosted Service if Customer performs its obligations as set out in the "SSP Appendix J Control Implementation Summary (CIS) and Customer Responsibility Matrix (CRM) Workbook" 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.

Business Associate Agreement

Splunk will comply with the requirements and obligations in the Splunk Business Associate Agreement set out at https://www.splunk.com/en_us/legal/splunk-baa.html for (i) Hosted Services provisioned in Splunk Cloud Platform's Premium HIPAA environment, as specified in an Order; and (ii) Splunk Observability Cloud.

Splunk AI Offerings Terms

Splunk AI Offerings

1. **TERMS.**
   Your use of a Splunk® AI Offering ("AI Offering") is governed by the Splunk General Terms ("SGT") and these Specific Terms for Splunk Offerings, including those set forth in this Splunk AI Offerings section ("Specific Offering Terms," and the SGT and Specific Terms, "Terms"). By using an AI Offering, you agree to be bound by the Terms. If you are entering into these Terms on behalf of Customer, you represent that you have the authority to bind Customer. If you do not agree to the Terms, or do not have the authority to bind Customer, do not use Splunk's AI Offerings. For clarity, these Specific Terms hereby incorporate the SGT terms by reference.

2. **SERVICE DESCRIPTION.**
   AI Offerings are elements of the respective Offerings through which they are made available. The functionality and details relevant to specific AI Offerings are set forth in the Documentation pertinent to such underlying Offerings, or, in the case of AI Assistants, in the respective Assistant Documentation. Your use of each AI Offering is subject to the conditions, limitations, and requirements set forth in the Documentation and/or Assistant Documentation, together with the Terms. AI Offerings may include features and functionality that include, but are not limited to, generative artificial intelligence ("genAI") and Agentic AI Features.

3. **PURPOSE AND USE.**
   When you interact with an AI Offering, Splunk will use your Inputs, Context Data, and Outputs (collectively, "AI Service Data") to provide, operate, maintain, and Modify the AI Offerings, to comply with applicable law, and to enforce these Terms. For clarity, as used in this Section, "Modify" does not include Training and Fine-Tuning. By using an AI Offering, you hereby grant Splunk a perpetual, irrevocable, worldwide, royalty-free, non-exclusive, sub-licensable, fully paid-up license to access and use the AI Service Data for such purposes.

4. **TRAINING AND FINE-TUNING.**
   If you do not expressly withhold consent to Splunk's use of your AI Service Data for Training and Fine-Tuning by deactivating the "opt-in" setting in the AI Offering settings, then in addition to the uses described in Section 3 above, Splunk may use your AI Service Data for the purpose of Training and Fine-Tuning AI Models. You may opt out of this use of your AI Service Data in the user interface settings. By using an AI Offering and not toggling off the collection of AI Service Data for Training and Fine-Tuning, you agree that, in addition to the rights granted to Splunk in Section 3 above, you also hereby grant Splunk a perpetual, irrevocable, worldwide, royalty-free, non-exclusive, transferrable, sublicensable (through multiple tiers), fully paid-up license to use and transform your AI Service Data for the purpose of Training and Fine-Tuning AI Models in any form, medium or technology now known or later developed and to commercialize such AI models and make derivatives thereof. You acknowledge and agree that some AI Service Data may be replicated in outputs for third parties who use the AI Offering that has been Trained or Fine-Tuned with your AI Service Data and may therefore be disclosed; you consent to such disclosure and use.

5. **FEEDBACK.**
   "Feedback" has the meaning ascribed to it in the SGT and includes in-product Feedback. Notwithstanding any election to opt-out of the use of your AI Service Data for Training and Fine-Tuning as described above, any Feedback you provide may be used by Splunk for any legal purpose, including without limitation, Training and Fine-Tuning.

6. **OWNERSHIP OF INPUTS.**
   As between you and Splunk, Inputs, except any Pre-existing Splunk Content, are owned by you. For each Input, you represent and warrant that you have all rights necessary for you to grant the licenses granted in these Terms, and that such Input, and your provision thereof to and through an AI Offering, comply with all applicable laws, rules and regulations, and these Terms.

7. **OWNERSHIP OF OUTPUTS.**
   Except with respect to Pre-existing Splunk Content, as between you and Splunk, Outputs are owned by you. You will have the right to access and use the Pre-existing Splunk Content in connection with your applicable Offerings, and those rights will be of the same scope and duration as your rights to the underlying Offering.

8. **RESTRICTIONS AND ACCEPTABLE USE**
In using an AI Offering, you must comply with the acceptable use policy set forth in the Policy. In addition, you may not, and may not allow any user or third party to: (i) use an AI Offering in a way that violates any person's rights; (ii) use an AI Offering or any Output from an AI Offering to develop or improve models (or other product or service) that are similar to or compete with Splunk or LLM service providers, or to benchmark or to Train any other model; (iii) work around any technical limitations in an AI Offering or restrictions in Documentation; (iv) install or use any third-party software or technology in a way that would subject an AI Offering or any portion thereof to any other license; (v) use an AI Offering or Outputs for any activity for which applicable regulations would require licensure by a local, state, or federal agency or regulatory body if performed by a human (vi) use any Output relating to a person for any purpose that could have a legal or material impact on that person, such as making credit, educational, employment, housing, insurance, legal, medical, or other important decisions about them (including, but not limited to, the uses described in Section 9 below). Your access to and use of an AI Offering is subject to temporary throttling in Splunk's reasonable discretion in accordance with relevant Documentation.

9. **NO HAZARDOUS OR MEDICAL USE.**
You acknowledge and agree that an AI Offering is not designed or intended: (i) to support any use in which a service interruption, defect, error, or other failure of an AI Offering could result in the death or serious bodily injury of any person or in physical or environmental damage (collectively, "Hazardous Use"); or (ii) for use as a medical device(s), to be a substitute for professional medical advice, diagnosis, treatment, or judgment ("Medical Use"). You shall not, and shall not permit anyone to, make Hazardous Use or Medical Use of an AI Offering or Output. You will defend, indemnify and hold Splunk and its affiliates harmless from and against all damages, costs and attorneys' fees in connection with any claims arising from a Hazardous Use or Medical Use in connection with an AI Offering, including any claims based in strict liability or that Splunk (or any of Splunk's suppliers) was negligent in designing or providing the AI Offering (or any part thereof) to you.

10. **THIRD-PARTY SERVICE PROVIDERS.**
The AI Offering may integrate with a third-party AI service as outlined herein or in the applicable AI Offering Documentation. In cases where such third-party integration is embedded in the AI Offering as provided to you by Splunk, and Splunk transmits your AI Service Data to the third party, Splunk will bind the third party to contractual obligations to afford confidentiality and security safeguards to such AI Service Data that are consistent with those by which Splunk is bound. You consent to Splunk sending your AI Service Data to such third-party AI service to provide the AI Offering services and for the purposes agreed herein.

11. **TERM.**
The terms applicable to AI Offerings as set forth herein take effect when you gain access to each respective AI Offering and remain in effect for the duration of your subscription term of the applicable AI Offering or, if there is no specific subscription term for the applicable AI Offering, for the subscription term of the underlying Offering in which the AI Offering runs unless terminated earlier. You may terminate the terms applicable to any AI Offering at any time for any reason by discontinuing the use of the respective AI Offering and providing written notice of termination to Splunk; termination of your subscription to the underlying Offering in which an AI Offering runs will automatically terminate the terms specific to your use of the AI Offering. If Splunk, in its sole discretion, believes your use of an AI Offering or Agentic AI Features may be in breach of the applicable terms or could result in a potential harm to Splunk, Splunk customers, Splunk vendors, or the general public, Splunk may immediately suspend your use of the AI Offering or Agentic AI Features.

12. **DISCLAIMER OF WARRANTIES.**
Splunk does not offer any representation or warranties, express or implied, that Outputs are accurate or free from error or bias. You should independently evaluate the Outputs through human review, including to make sure that such Outputs are accurate, lawful, and otherwise appropriate and permissible under these Terms and that you have adequate rights to use such Outputs, before relying on them. You will ensure that your Inputs and use of any Outputs does not violate the intellectual property or proprietary rights of Splunk or any third party. Splunk makes no warranties or representations, express or implied, that the Output is protectable under any law. With respect to any separately downloaded and installed AI Offering, you agree that Splunk is not responsible for any impact on your experience of any Splunk Offering with which you use the AI Offering, and that your sole remedy for any negative impact will be to discontinue use of the AI Offering.

YOUR USE OF AN AI OFFERING IS AT YOUR OWN RISK. IT IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS WITHOUT WARRANTY OF ANY KIND. SPLUNK AND/OR ITS SUPPLIERS AND LICENSORS HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO AI OFFERINGS OR ANY OUTPUTS, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. SPECIFICALLY, SPLUNK MAKES NO WARRANTY THAT (I) AN AI OFFERING OR ITS OUTPUTS WILL MEET YOUR REQUIREMENTS, (II) YOUR ACCESS TO AN AI OFFERING OR ITS OUTPUTS WILL BE UNINTERRUPTED, TIMELY, SECURE OR ERROR-FREE, (III) THE QUALITY OF ANY CONTENT, PRODUCTS, SERVICES, INFORMATION OR OTHER MATERIAL OBTAINED THROUGH AN AI OFFERING WILL MEET YOUR EXPECTATIONS, AND (IV) ANY ERRORS IN THE SOFTWARE WILL BE CORRECTED. AN AI OFFERING AND OUTPUTS COULD INCLUDE TECHNICAL INACCURACIES, ERRORS, OR OMISSIONS. THE DISCLAIMERS OF WARRANTY AND LIMITATIONS OF LIABILITY APPLY, WITHOUT LIMITATION, TO ANY DAMAGES OR INJURY CAUSED BY THE FAILURE OF PERFORMANCE, ERROR, OMISSION, INTERRUPTION, DELETION, DEFECT, DELAY IN OPERATION OR TRANSMISSION, COMPUTER VIRUS, COMMUNICATION LINE FAILURE, THEFT OR DESTRUCTION OR UNAUTHORIZED ACCESS TO, ALTERATION OF OR USE OF ANY ASSET, WHETHER ARISING OUT OF BREACH OF CONTRACT, TORTIOUS BEHAVIOR, NEGLIGENCE OR ANY OTHER COURSE OF ACTION BY SPLUNK.

As genAI systems, AI Offerings may hallucinate, provide inaccurate, incomplete or irrelevant information, generate Outputs that are harmful or that are not fit for use (including from a legal and/or business perspective). As between you and Splunk, you are responsible for evaluating the accuracy of any Output as appropriate for your use case, including by using human review of the Output.

13. **INDEMNIFICATION.**
To the extent that any Customer Claim arises from your AI Service Data, the "Our Indemnification to You" subpart of Section 21 (Indemnity) of the SGT will not apply with regard to an AI Offering. By using an AI Offering, and without limiting the "Your Indemnification to Us" subpart of Section 21 (Indemnity) of the SGT (which applies to your use of an AI Offering), you agree to defend, indemnify and hold harmless Splunk, our affiliates and our personnel from and against any claims, causes of action, demands, recoveries, losses, damages, fines, penalties or other costs or expenses arising from or in connection with your use of an AI Offering in any manner inconsistent with the requirements herein. You may not settle or compromise any claim that requires any action or forbearance on Splunk's part without first obtaining Splunk's written consent.

14. **AGENTIC AI FEATURES.**

If an Offering or AI Offering includes Agentic AI Features, Splunk will identify such features within the Offering or AI Offering. The terms in this Section 14 apply to your use of Agentic AI Features:

a. **Customer Responsibility and Risk Acceptance for Agentic AI Features.** You acknowledge and agree that Agentic AI Features are designed to operate with at least a degree of autonomy. You are responsible for (i) configuring, validating, and monitoring the Agentic AI Features; (ii) carrying out any AI impact assessments required by law; (iii) reviewing and approving any proposed or executed actions by or results from Agentic AI Features; and (iv) ensuring that your use of Agentic AI Features complies with all applicable laws. You understand that Agentic AI Features may generate erroneous, unintended, or unwanted actions, results, configurations, or modifications. By using Agentic AI Features, you acknowledge and accept that there are inherent risks associated with their autonomous operation. Splunk will use commercially reasonable efforts to ensure the Agentic AI Features function as described in the applicable documentation. Splunk will be liable for errors, damages, or losses arising directly from (v) a material defect in the Agentic AI Features as provided by Splunk, (vi) Splunk's gross negligence or willful misconduct, or (vii) Splunk's breach of its express obligations under this Agreement. Except as set forth above, and to the extent permitted by law, Splunk disclaims all liability for any actions taken or not taken by Agentic AI Features, or for any consequences arising from such actions or inactions.

b. **Human-in-the-Loop Controls.** Where Splunk provides Human-in-the-Loop Controls, you are responsible for configuring and actively using these controls to review, approve, modify, or reject results or actions proposed or taken by the Agentic AI Features. Your failure to properly vet results or configure or use such controls, or your decision to override or disable them, will not diminish your responsibility or acceptance of risk as outlined herein. You acknowledge that the effectiveness of Agentic AI Features is contingent upon your proper implementation and oversight of these controls.

c. **Indemnification for Agentic AI Features.** In addition to your indemnification obligations set forth in the General Terms and Section 13 above, you agree to defend, indemnify, and hold harmless Splunk, its affiliates, and its personnel from and against any claims, causes of action, demands, recoveries, losses, damages, fines, penalties, or other costs or expenses arising from or in connection with (i) your use of any Agentic AI Features in a manner inconsistent with these Terms; (ii) your failure to properly configure any Agentic AI Feature; or (iii) your failure to use or configure Human-in-the-Loop controls provided for Agentic AI Features. This indemnification obligation will not apply to the extent such claims arise directly from a material defect in the Agentic AI Features as provided by Splunk, or from Splunk's gross negligence or willful misconduct. For clarity, issues relating to the uptime, accuracy, or inherent biases of third-party AI Model providers shall not be considered a material defect.

15. **ORDER OF PRECEDENCE.**
Despite Section 22 of the SGT (Updates to Offerings), in the event of any conflict between these Specific Terms and the SGT, these Specific Terms will control.

16. **DEFINITIONS**

"Agentic AI Features" means features or functionality that are (1) designed to autonomously initiate or execute actions, configurations, or modification within your environment or other systems; and (2) identified as an Agentic AI Feature within the Splunk Offering user interface or relevant Documentation.

"Assistant Documentation" means the descriptive, instructional, and other supporting documentation published by Splunk pertinent to a Specific Assistant found using *"Splunk AI Assistant"* keywords search here: https://help.splunk.com/en

"AI Model" means a computational system, algorithm, or framework that has been trained on data to learn patterns, relationships, or representations and is designed to process inputs (e.g., prompts or data) and generate relevant and responsive outputs. This term encompasses the underlying architecture, parameters, and weights, and any associated algorithms necessary for its functionality. For clarity, "AI Model" expressly excludes (i) the data used to train the AI Model, (ii) specific inputs provided by a user to the AI Model, and (iii) the outputs generated by the AI Model.

"AI Offering" means a feature, function, or add-on module of a Splunk product or service that uses artificial intelligence in processing information or producing a response to an end-user provided prompt.

"AI Offering Documentation" means the descriptive, instructional, and other supporting documentation published by Splunk pertinent to a Specific AI Offering found using *"Splunk AI"* keywords search here: https://help.splunk.com/en

"Context Data" means data stored in your instance of the Splunk Offering that underlies your use of the AI Offering (e.g. your Splunk Cloud environment) provided by the Splunk system to an AI Model, together with end-user provided Input that provides relevant reference data used by the AI Model to meaningfully respond to Input.

"Human-in-the-Loop Control" means a process in which AI-generated outputs or actions allow for human review, approval, or intervention before or during execution.

"Input" means the raw data or content that you upload or submit to an AI Offering or that is used as input context from your Offering environment to power an AI Offering.

"Modify" means to evolve and improve the AI Offering, including without limitation by correcting errors, resolving interoperability issues, patching security vulnerabilities, making feature modifications; improvements; and additions, and by improving services associated with the AI Offering.

"Output" means the data or content generated by an AI Offering and displayed to the end-user as the response or final result of the end-user's interaction with the AI Offering.

"Policy" means the Cisco Acceptable Use Policy as set forth here: https://www.cisco.com/c/dam/en_us/about/legal/cisco-acceptable-use-policy.pdf

"Pre-existing Splunk Content" means any materials in which Splunk has pre-existing intellectual property ownership or rights.

"Training and Fine-Tuning" means teaching or conditioning AI Models to learn patterns and perform specific tasks by supplying the AI Models with datasets and optimizing their relevant parameters; it includes adapting pre-trained AI Models to improve performance through methods such as adjusting relevant weights.

Cisco Firewall Promotional Splunk Capacity Offer

Promotional Capacity Terms

1. Splunk Cloud Platform or Splunk Enterprise Capacity provided free-of-charge pursuant to the Cisco Firewall Promotional Splunk Capacity offering (“Promotional Capacity”) is subject to the Splunk General Terms and the following additional terms and conditions:

    a. In addition to your purchase of eligible Cisco products as described in the promotional materials, you must purchase and maintain at least as much paid-for Capacity of an eligible Splunk product as you receive in Promotional Capacity, and Promotional Capacity will be co-termed with your current license or subscription term for the eligible Splunk product(s), excluding any renewal periods. Splunk makes no guarantee that the Promotional Capacity will be offered at the time of renewal. Upon expiration of the free offering, if you wish to continue utilizing any previously offered Promotional Capacity, you will be required to pay for such Capacity at then-current rates.

    b. Promotional Capacity is additive to your paid-for Capacity and not intended to offset or substitute any paid-for Capacity for any Splunk Offering.

    c. Promotional Capacity may not be transferred from the legal entity associated with the eligible Cisco Secure Firewall licenses and cannot be combined or split between Splunk instances.

    d. Promotional Capacity is provided at the same Support service level as the paid capacity, e.g. if the paid capacity has premium support, the Promotional Capacity will be delivered as premium support.

    e. The Promotional Capacity does not apply for determining eligibility for OnDemand Services and Education credits (outlined here: https://www.splunk.com/en_us/customer-success/success-plans.html).

    f. Promotional Capacity must be ingested via the Cisco Security Cloud App (https://splunkbase.splunk.com/app/7404) and either of the sourcetype methods, *cisco:sfw:estreamer* or *cisco:ftd:syslog*. Promotional Capacity may only be used for ingesting/processing data from qualifying Firewall licenses.

2. Splunk reserves the right to reduce or immediately terminate any Promotional Capacity if you fail to maintain any eligibility criterion during the course of the promotional period, including but not limited to

    a. You fail to maintain an eligible Cisco Secure Firewall Threat Defense license subscription and applicable Cisco Support contract for each such license;

    b. You reduce your paid Capacity of eligible Splunk products;

    c. Your underlying contract with Splunk is terminated;

    d. You deactivate threat data sharing or other required telemetry.

Prior Versions of SPLUNK TERMS FOR OFFERINGS AND HOSTED SERVICES

- **Published February 2025**
- **Published January 2025**

- **Published October 2024**
- **Published September 2024**
- **Published March 2024**
- **Published February 2024**
- **Published January 2024**