Offer Description – Product

Splunk Observability Cloud

This Offer Description is part of the General Terms or similar terms existing between You and Cisco (e.g., the End User License Agreement) (the "**Agreement**"). Capitalized terms, unless defined in this Offer Description, have the meaning in the Agreement. In addition, any reference to the "Agreement" or "Splunk General Terms" in the Documentation or policies linked from this Offer Description mean the Agreement, as defined above.

1. Summary

1.1 This Offer Description is for the Splunk Observability Cloud that includes the following Cloud Services (as part of a suite or as individual services): Splunk Infrastructure Monitoring (Splunk IM), Splunk Application Performance Monitoring (Splunk APM), Splunk Real User Monitoring (Splunk RUM), Splunk Log Observer Connect, and Splunk Synthetic Monitoring, as described more fully in the Splunk Documentation (collectively the "**Product**").

1.2 To the extent applicable to the Product, any reference to the "Hosted Services" or "Offerings" in the Documentation, and other materials in this Offer Description (including linked content), mean the Product, as applicable.

2. Support and Other Services

2.1 **Support.** Your purchase of the Product includes the support services described at Splunk Support Terms.

2.2 **Splunk Extensions**. You may use Splunk Extensions solely in connection with the Product subject to the same terms and conditions for the Product and payment of the fees associated with the Splunk Extensions. Some Splunk Extensions may be provided under terms that provide broader rights than the rights You have to the underlying Product.

2.3 **Third Party Extensions on Splunkbase.** Cisco may make third party Extensions available from Splunkbase ("**Third Party Extension**"). Cisco does not represent, warrant or guarantee the accuracy, integrity, quality, or security of any Third Party Extension, even if that Third Party Extension is identified as "certified" or "validated" for use with the Product. Your use of a Third Party Extension may be subject to additional terms, conditions or policies. Cisco may block or disable access to a Third Party Extension at any time.

2.4 **Success Plans.** If You qualify for and have purchased a Success Plan, Your Product includes the relevant services described at Splunk Success Plans. All Success Plan credits must be consumed within the time period specified. At the end of the applicable period, any remaining credits will expire, and no refunds will be provided for unused credits.

3. Performance Standards

The Splunk Observability Cloud Service Level Schedule applies to Your use of the Product.

4. Data Protection and Security

4.1 **Privacy Data Sheet**. The Splunk Cloud Privacy Data Sheet describes the Personal Data that Cisco collects and processes as part of delivering the Product.

4.2 **Data Processing Terms**. The Data Processing Terms apply as defined in the Agreement except as set forth below.

(A) **Information Security Exhibit.** The Information Security Exhibit, as defined in the Agreement and as referenced within the Data Processing Terms, is replaced with the Splunk Observability Security Addendum.

(B) **Notification Obligations**. The notification obligations contained in the Incident Response and Breach Notification section of the Splunk Observability Security Addendum will apply instead of any notification terms contained in the Data Processing Terms.

(C) **Return, deletion and/or retrieval of Personal Data.** Any provisions in the Data Processing Terms concerning the return, deletion and/or retrieval of Personal Data following termination of the Data Processing Terms is deleted and the following shall apply instead: "On termination of the Order and at Your expense, You can delete or retrieve Customer Content, including any Personal Data contained in Customer Content, from the Product as provided in the Agreement. If Cisco is required under applicable law to retain Personal Data in its possession after termination of the Agreement, Cisco will protect the Personal Data as set forth in the Splunk Observability Security Addendum. At Your written request, Cisco will give You confirmation in writing that it has fully complied with this section or provide a justification as to why such compliance is not feasible.

4.3 **Privacy and Security.** The Privacy and Security section in the Agreement applies to the Product, except that the reference to the Information Security Exhibit is replaced with Splunk Observability Security Addendum, and references to the Customer Content Data Brief and the Systems Information Data Brief do not apply.

4.4 **Your Responsibility for Data Protection**. You are responsible for: (a) selecting from the security configurations and security options Cisco makes available for the Product; (b) taking additional measures outside of the Product to the extent the Product does not provide the controls that may be required or desired by You; and (c) routine archiving and backing up of Customer Content. You agree to notify Cisco promptly if You believe that an unauthorized third party may be using Your accounts or if Your account information is lost or stolen.

5. Special Terms

5.1 **Right to Use**. The Use Rights under this Offer Description for the Use Term are limited to Your own internal business operations based on the analysis, monitoring or processing of Your data from Your systems, networks, and devices and does not include monitoring or servicing the systems, networks and devices of any third parties.

5.2 **Additional Limits on Usage**. In addition to the limits on usage described in the Agreement and Documentation, You will not: (a) use the Product to ingest or analyze the machine, system or application data of any third party; (b) access the Product to monitor its availability, performance, or functionality for competitive purposes; (c) separately use any of the Product features and functionalities with external applications or code not furnished by Cisco or with any data not processed by the Product; or (d) exceed the purchased Capacity.

5.3 **Policy Application**. Cisco's Software License Portability Policy and Software License Transfer and Re-Use Policy do not apply to this Product.

5.4 **Acceptable Use**. You will abide by the Splunk Acceptable Use Policy for Cloud Offerings which will be an additional acceptable use provision as referenced in the Agreement.

5.5 **Data Usage, Subscription Limits Enforcement and Entitlements.** The additional data usage, subscription limits enforcement and entitlements that apply to the Product are described at Splunk Observability Usage, Subscription Limits and Entitlements.

5.6 **Developer Tools and Customer Extensions**. Cisco may make Developer Tools available so You can develop Extensions for use with the Product (Extensions that You develop, "**Customer Extensions**"). You have a Use Right, subject to the Agreement, to use those Developer Tools to develop Your Customer Extensions. This Use Right includes supporting interoperability between the Product and Your system or environment. You may not remove or alter any proprietary legends or notices contained in Splunk Developer Tools. You retain title to Your Customer Extensions, subject to Cisco's ownership in the Product and any materials and technology provided by Cisco in connection with the Developer Tools. You agree to assume full responsibility for the performance and distribution of Customer Extensions.

5.7 **Third Party Content**. The Product may contain features that enable interoperation with Third Party Content that You choose to add to the Product. You may be required to: (a) separately obtain access to Third Party Content from its provider; and (b) grant Cisco access to Your accounts with those providers. By choosing to enable such interoperation by allowing Cisco to enable access to Third Party Content, You: (i) certify that You are authorized to do so; and (ii) authorize Cisco to allow that provider to access Customer Content as necessary for the interoperation. Cisco is not responsible or liable for disclosure, modification or deletion of Customer Content resulting from this interoperation, nor is Cisco liable for damages or downtime or other impacts on the Product, resulting from Your use of or reliance on Third Party Content, sites or resources.

5.8 **Open-source Technology.** The Product may contain Open Source Software. Open Source Software that is delivered as part of the Product and which may not be removed or used separately from the Product is covered by the warranty, support and indemnification provisions applicable to the Product. Open Source Software may have additional terms that apply to the use of the Product as set out in the Documentation. However, those terms will not: (a) impose additional restrictions on Your Use Rights during Use Term; or (b) negate or amend Your responsibilities with respect to the Product. The Open Source provisions in the Agreement do not apply to the Product.

5.9 **End of Life Notifications.** Cisco may end the life of the Product in accordance with the Splunk Support Policy.

5.10 **Usage Data**. Cisco collects and processes Usage Data as set out in the Splunk Privacy Policy. Usage Data does not include Customer Content.

5.11 **Ownership of Intellectual Property**

(A) **Product.** As between You and Cisco, Cisco owns and reserves all right, title, and interest in and to Cisco Content, Splunk Developer Tools and other materials, including all intellectual property rights. Cisco retains rights in anything delivered or developed by Cisco or on our behalf under the Agreement. No rights are granted to You other than as set out in this Agreement.

(B) **Customer Content.** You own and reserve all right, title and interest in Customer Content, including all intellectual property rights. By sending the Customer Content to the Product, You grant Cisco a worldwide, royalty free, non-exclusive license to access and use the Customer Content for purposes of providing You the Product. Subject to 5.11(A), You own any reporting results that You or Your Authorized Users may derive from Customer Content through the use of the Product.

5.12 **Return of Customer Content**. You may retrieve and remove Customer Content from the Product at any time during Your Use Term. Cisco will also make the Customer Content available for Your retrieval for 30 days after termination of Your subscription. After those 30 days, Cisco will delete all remaining Customer Content, unless legally prohibited.

5.13 **Overages.** If a Use Record verification report reveals that You have exceeded the purchased Capacity or Use Rights, Cisco will have the right to invoice You at the then current list price, which will be payable by You within 30 days.

5.14 **Compliance with laws**. In addition to Your obligations under the Agreement, You are responsible for Your Customer Content and users, their compliance with the Agreement, and the accuracy, lawful use of, and how You acquired Your Customer Content. This includes Your responsibility to ensure that You provide any required notice to Your end users and obtain any required consents.

5.15 **PHI, PCI Data and ITAR Data**. You may not transmit or store PHI Data, PCI Data or ITAR Data within the Product unless You have specifically purchased the compliant version of the Product for the applicable regulated environment.

5.16 **Registration**. You agree to provide accurate and complete information when You register for and use the Product and agree to keep this information current. Each person who uses the Product must have a separate username and password. You must provide a valid email address for each person authorized to use the Product. Cisco may require additional information in connection with the Product, and You will provide this information as Cisco reasonably requests. You are responsible for securing, protecting, and maintaining the confidentiality of Your account usernames, passwords and access tokens.

5.17 **Trade compliance**. Export information regarding the Product, including export control classifications, is at https://www.splunk.com/en_us/legal/export-controls.html.

5.18 **Governing law and venue**. For purposes of this Offer Description, the laws of the People's Republic of China will not apply to the Agreement and the jurisdiction of the Hong Kong International Arbitration Center is excluded. If Your primary place of business is mainland China, the laws and courts of California will be the governing law and exclusive jurisdiction for any disputes arising from these terms.

5.19 **US Government end users**. If You are a US Federal Government End User, the following additional clauses apply to the Product: FAR 12.212 (Computer Software) and, for Department of Defense transactions, DFARS 252.227-7015 (Technical Data – Commercial Items).

5.20 **Managed Service Provider Terms**. The following additional terms apply only if You are an authorized Cisco channels partner, authorized to provide managed services:

(A) You may provide managed services to a single, named End User (as described in Your applicable partner agreement). Therefore, You may not use a single instance of the Product to simultaneously provide managed services to unrelated End Users unless Cisco specifically approves it in writing.

(B) You will ensure that any End User's use of the managed Services is subject to the General Terms and this Offer Description by passing these terms through to Your End Users before provisioning the managed services.

5.21 **No Future Functionality**. You agree that Your purchase of the Product is not contingent on the delivery of any future functionality or features, or dependent on any oral or written statements made by us regarding future functionality or features.

5.22 **Automatic Renewal.** Unless indicated otherwise in an Order, the Product Use Term will automatically renew for the same period as the previous Use Term, unless either party writes to the other party that it does not want to renew the subscription at least 1 day before the applicable Use Term ends.

5.23 **Use by Third Parties.** Your Affiliates may not access or use the Products, unless agreed in writing.

5.24 **Definitions**

Term	Meaning
Analyzed Trace	A trace that was sent to and processed by Splunk APM.

Term	Meaning
APM Identities	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.
Capacity	The measurement of usage of the Product (e.g., aggregate daily volume of data indexed, specific source type rights, number of search and compute units, number of monitored accounts, virtual CPUs, user seats, use cases, storage capacity, etc.) that is purchased for the Product, as stated in the Order. The Capacities are at https://www.splunk.com/en_us/legal/licensed-capacity.html.
Container	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	Any Metric that is not automatically collected and reported as part of Cisco's standard Host-based integrations.
Customer Content	Data in the Product that has been ingested by or on behalf of You from Your internal data sources.
Customer Extension	As defined in Section 5.6.
Developer Tool	The standard application programming interface, configurations, software development kits, libraries, command line interface tools, other tooling (including scaffolding and data generation tools), integrated development environment plug-ins or extensions, code examples, tutorials, reference guides and other related materials identified and provided by us to facilitate or enable the creation of Extensions or otherwise support interoperability between the software and Your system or environment.
Extension	Any separately downloadable or accessible suite, configuration file, add-on, technical add-on, plug-in, example module, command, function, playbook, content or application that extends the features or functionality of the Product.
HIPAA	The Health Insurance Portability and Accountability Act of 1996, as amended, and supplemented by the Health Information Technology for Economic and Clinical Health Act.
Host	A virtual machine or physical server being monitored.
ITAR Data	Information protected by the International Traffic in Arms Regulations.
Metric	Any unique combination of a metric name and dimension value reporting data to Cisco within the last hour.
Monitoring MetricSet	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	Metric Time Series.
PCI Data	Credit card information within the scope of the Payment Card Industry Data Security Standard.
PHI Data	Any protected health data, as defined under HIPAA.
Profiled Container	A Container that is instrumented to send Profiling data to Splunk APM.
Profiling	Automated collection and analysis of code behavior data from runtime environments.
Profiling Volume	The amount of Profiling data that customers pay for to be ingested by Splunk APM.
Session Volume	The amount of Session data that customers pay for to be ingested by Splunk RUM.

Term	Meaning
Span	An area of code instrumented to be captured as part of a recorded transaction (e.g., rpc, function). Each service can have many spans. At a minimum, there will be 2 spans - inbound and outbound to the service.
Splunkbase	Online directory of, or platform for, Extensions at https://splunkbase.splunk.com and any and all successors, replacements, new versions, derivatives, updates and upgrades and any other similar platforms owned and/or controlled by us.
Splunk Extensions	Extensions made available through Splunkbase that are identified on Splunkbase as built by us (and not by any third party).
TAPM	Trace Analyzed Per Minute.
Trace	An array of spans represented as a Directed Acyclic Graph.
Trace Volume	Amount of trace data per minute that customers pay for to be ingested by Splunk APM.
Third Party Content	Information, data, technology, or materials made available to You by any third party that You license and add to the Product or direct us to install in connection with the Product. Third Party Content includes but is not limited to, Third Party Extensions, web-based or offline software applications, data service or content that are provided by third parties.
Third Party Extension	As defined in Section 2.3.
Troubleshooting MetricSet	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.
Usage Data	Data generated from the usage, configuration, deployment, access, and performance of the Product. For example, this may include such things as information about Your operating environment, such as Your network and systems architecture, or sessions, such as page loads and session views, duration, or interactions, errors, number of searches, source types and format (e.g., json, xml, csv), ingest volume, number of active and licensed users, or search concurrency. Usage Data does not include Customer Content.