Offer Description for Cisco Cloudlock

Overview

This Offer Description sets forth a description of Cisco Cloudlock, a Cisco Software-as-a-Service offering. Please see the applicable Order for the specific Cisco Cloudlock Services covered by Your subscription.

The Cisco Universal Cloud Agreement ("**Agreement**"), in addition to the terms and conditions contained in this Offer Description, shall govern Your use of Cisco Cloudlock. A current copy of the Agreement is located at: http://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html.

Capitalized terms used in this Offer Description are defined in **Appendix A**; capitalized terms used and not defined herein shall have the meanings given to them in the Agreement.

If You are purchasing Cisco Cloudlock directly from Cisco, this Offer Description and the Agreement are both incorporated into Your applicable master agreement with Cisco. If You are purchasing through an Approved Source, then the Agreement and this Offer Description govern Your use of Cisco Cloudlock. All non-conflicting and additional terms and conditions in Your purchase agreement with an Approved Source remain applicable to Your purchase, and are between You and Your Approved Source.

If you are using Cisco Cloudlock with other Cisco products or services, You are also responsible for complying with the terms for such other Cisco products and services, as applicable. The terms set forth herein apply to Cisco Cloudlock whether purchased for use on a standalone basis, or purchased for use with such other Cisco products or offerings.

Description and Terms

Description.
Cisco Cloudlock is a cloud-based Cloud Access Security Broker (CASB) and cloud cybersecurity platform that helps organizations securely leverage use of applications in the cloud. Cisco Cloudlock delivers visibility and control for Software-as-a-Service ("SaaS"), Platform-as-a-Service ("PaaS"), and Infrastructure-as-a-Service ("IaaS") environments across users, data, and applications. The core functionality of Cisco Cloudlock covers the following three use cases:

- Data Loss Prevention ("**DLP**"): Cisco Cloudlock provides DLP functionality that monitors cloud environments to detect and secure sensitive information through out-of-the-box policies as well as highly-tunable custom policies. Automated response actions can remediate risk in the instance of policy violation, including, but not limited to, end-user notifications, file-level encryption, transfer of ownership, and quarantines.

- User and Entity Behavior Analytics ("**UEBA**"): Cisco Cloudlock provides cross-platform UEBA functionality for SaaS, IaaS, PaaS, and Identity-as-a-Service ("**IDaaS**") environments. Cisco Cloudlock leverages advanced machine learning algorithms to detect anomalies based on factors such as activities outside of whitelisted countries and actions across distances at impossible speeds.

- Apps Firewall ("**Apps**"): Cisco Cloudlock Apps discovers cloud apps connected to Your corporate environment, and provides a crowd-sourced Community Trust Rating for individual applications, as well as the ability to ban or whitelist them based on risk profile and access scope, increase employee awareness with email alerts, and revoke apps in bulk across the entire user base.

Cisco Cloudlock also includes access to actionable cybersecurity intelligence through its data scientist-led CyberLab and crowd-sourced security analytics. The CyberLab provides analytics to identify, research, and investigate, and advises customers and others regarding, security trends, and threats.

Please consult the Documentation for further information regarding Cisco Cloudlock technical specifications, features and functionalities.

Service Availability Commitment.
Cisco shall use commercially reasonable efforts to maintain Cisco Cloudlock availability of 99.9% of each calendar month. Availability will be calculated by dividing the total number of minutes of Uptime (defined below) during the applicable calendar month by the total number of minutes in such month, minus minutes of Cisco Cloudlock Outages (defined below) occurring due to scheduled maintenance or attributable to Third Party Actions (defined below), and multiplying that amount by 100. The formula for this calculation is as follows:

$$\text{Availability} = (X \div Y) \times 100$$

X= Total # of minutes of Uptime during calendar month

Y= (Total # of minutes in such calendar month) - (Total # of minutes of Outages from scheduled maintenance and Third Party Actions)

For the purposes of this calculation, (i) An **"Outage"** means Cisco Cloudlock is completely unreachable when Your Internet connection is working correctly, (ii) "**Uptime**" means the number of minutes where there were no Cisco Cloudlock Outages, excluding Outages for scheduled maintenance and Third Party Actions, and (iii) "**Third Party Action**" means any action beyond Cisco's reasonable control including, without limitation, the performance of Internet networks controlled by other companies or traffic exchange points that are controlled by other companies, labor strikes or shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, earthquakes and material shortages. If a dispute arises about whether or not an Outage occurred, Cisco shall make a determination in good faith based on its system logs, monitoring reports and configuration records, and as between customer records and Cisco records, Cisco records shall control. Cisco shall not be responsible for any Cisco Cloudlock Outages arising out of Third Party Actions.

Usage Limits.
You may not deploy or use Cisco Cloudlock in a manner that (i) extends beyond the duration of the applicable subscription term (e.g. 1, 3 or 5 years), or (ii) exceeds any use limitations or other

metrics related to Your license, including the limits set forth below and as otherwise set forth in an Order, SKU, product identifier (PID) or Documentation.

Metric	Limit
Number of Users	Subscription limited to applicable quantity of Users set forth on the Order.
Number of Covered Cloud Services Domains	Unless the Order specifies otherwise, Your subscription is limited to a single Domain for each of the Covered Cloud Services.
Number of Active Policies	Up to 30
Enterprise API Limits	Up to 100 Enterprise API requests per User license for the Core Cloudlock Services per day (measured in the aggregate: 100 x number of Users for the Core Cisco Cloudlock Services covered under the subscription), but not to exceed 10,000 Enterprise API requests per day in the aggregate. An Enterprise API request is a request to Cisco Cloudlock from an external system. This limit does not apply to API calls between Cisco Cloudlock and the Covered Cloud Service.
Retroactive Monitoring Scans	Up to 1 Retroactive Monitoring scan per month, except for Student Licenses. For Student Licenses, You are limited to 1 Retroactive Monitoring scan per year.
Number of Data Assets	Up to 1,000 Data Assets per User license for the Core Cisco Cloudlock Services (measured in the aggregate: 1000 x the number of Users for the Core Cisco Cloudlock Services covered under the subscription).
Test/Development Environment	Unless the Order specifies otherwise, each Cisco Cloudlock subscription includes 1 Test/Development Environment.

Security.

Cisco conducts an annual SOC II Type II or higher security audit on Cisco Cloudlock and will not materially reduce the administrative, physical and technical safeguards reviewed in connection with such audit. Cisco will maintain administrative, physical and technical safeguards consistent with industry standards and the Documentation, which are designed to provide security, confidentiality and integrity of Customer Data used by Cisco.

Customer Data.
As between You and Cisco, You own all right, title and interest in all Customer Data, including the content on the Covered Cloud Service and Cisco Cloudlock Metadata, but excluding Non-Identifiable Aggregated Data as described below. Nothing in the Agreement or this Offer Description shall be construed to grant Cisco any rights in Customer Data beyond those expressly provided in the Agreement and this Offer Description. Notwithstanding any other restrictions on use of data in this or any other agreement, You hereby grant Cisco (i) a limited, non-exclusive right to perform automated content scans of Customer Data stored on the Covered Cloud Service for the purpose of delivering Cisco Cloudlock, (ii) a limited, non-exclusive right to view, modify, collect, create, store, and use Cisco Cloudlock Meta-Data for the purpose of delivering Cisco Cloudlock, and (iii) the right to use Customer Data (including Cisco Cloudlock Metadata) to create Non-Identifiable Aggregated Data and use such Non-Identifiable Aggregated Data as provided below.

As between You and Cisco, (i) You retain control of the Customer Data at all times (except for Cisco Cloudlock Metadata as described below) and are responsible for backing up the Customer Data, (ii) You are responsible for the content, quality and accuracy of Customer Data, for securing any necessary approvals and license rights for Cisco's use of the Customer Data as provided for herein, and for ensuring that the Customer Data as made available by You complies with applicable laws and regulations, and (iii) You are responsible for ensuring You have the appropriate agreement in place with the applicable third party system vendor(s) to protect Customer Data in the event that You elect to leverage a Cisco supplied integration to any such third party system. **Cisco Cloudlock will not store any Customer Data, except to the extent that it constitutes Cisco Cloudlock Metadata.**

You agree that Cisco shall own all right, title and interest in and to Non-Identifiable Aggregated Data and may use such Non-Identifiable Aggregated Data for Cisco's business purposes in any manner in its sole discretion, including without limitation for analyzing trends and customer needs and for improving its services.

Software.
You and Your Users are granted a limited, non-exclusive, non-sublicensable and non-transferable license to use any downloadable Software made available with Cisco Cloudlock solely in connection with your authorized use thereof and only for the term that You are entitled to use Cisco Cloudlock. You further agree to promptly implement any updates, modifications and/or changes to the Software as requested by Cisco. In Your use of the Software, You may be granted access to certain third party open source code software ("**OSS**") that is provided for free for use in combination with the Software. Such OSS is made available to You for use pursuant to their respective third party license agreements. A listing of the OSS is available in the Documentation, as applicable. You may obtain the source code to the OSS in accordance with the directions set forth in the Documentation.

Cisco Threat Content.
If Your subscription to Cisco Cloudlock requires or permits You to use any Cisco Threat Content, then You (and Your agents acting on your behalf) may only use such Cisco Threat Content for use with Cisco Cloudlock and You may not license, sublicense or otherwise distribute the Cisco Threat Content to any third party.

Warranties.
In addition to the warranties and disclaimers set forth in the Agreement, Cisco warrants that it will provide Cisco Cloudlock in a manner consistent with general industry standards reasonably

applicable to the provision thereof. CISCO DOES NOT REPRESENT OR WARRANT THAT CISCO CLOUDLOCK WILL GUARANTEE ABSOLUTE SECURITY DUE TO THE CONTINUAL DEVELOPMENT OF NEW TECHNIQUES FOR INTRUDING UPON AND ATTACKING FILES, NETWORKS AND ENDPOINTS. CISCO DOES NOT REPRESENT OR WARRANT THAT CISCO CLOUDLOCK WILL PROTECT ALL YOUR FILES, NETWORK, OR ENDPOINTS FROM ALL MALWARE, VIRUSES OR THIRD PARTY MALICIOUS ATTACKS. CISCO DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES REGARDING ANY THIRD PARTY SYSTEM OR SERVICE TO WHICH CISCO CLOUDLOCK INTEGRATES OR TO ANY ONGOING INTEGRATION SUPPORT. INTEGRATIONS MADE ACCESSIBLE TO YOU THAT ARE NOT A GENERALLY AVAILABLE PRODUCT INCLUDED ON YOUR ORDER ARE PROVIDED ON AN "AS IS" BASIS. API'S SUPPLIED OR MADE ACCESSIBLE THROUGH CISCO CLOUDLOCK ARE SUBJECT TO CHANGE AND YOU ASSUME THE ASSOCIATED RISKS OF USING API'S FOR DEVELOPMENT PURPOSES IF YOU ELECT TO DO SO. ALL SUCH APIs ARE PROVIDED ON AN AS-IS BASIS.

Technical Support

Support Coverage.
Cisco will provide You with technical support in accordance with the following applicable Technical Support Level and Priority/Response:

Technical Support Level	Description
Basic	• Email Access Only • Access to online tools (e.g. knowledgebase, forums, Documentation, case portal, and notifications)
Gold	• Email Access • 24x7 phone support for P1 requests • 24x5 phone support for P2 – P3 requests (Sunday 4pm PST – Friday 5pm PST)

Support Priority	Response Target	Description
P1: Outage (as defined above)	-30 Minutes for phone requests (Gold Support) -2 Hours for Basic Support	Cisco will work on the resolution on a 24×7 basis to either resolve the issue, or develop a reasonable workaround.
P2: Technical Issue	1 Business Day	An issue occurs if Cisco Cloudlock is available but response times are slow while Your Internet connection is working correctly. Issues include technical questions or configuration issues related to Customer's account that moderately impact

Support Priority	Response Target	Description
		Your ability to use Cisco Cloudlock. Cisco will work on the resolution continuously during business hours until either the issue has been resolved, or a plan has been developed and mutually agreed upon between You and Cisco.
P3: Information Request	2 Business Days	Information requests include account questions, password resets, and feature questions. Cisco personnel will be assigned to work on the resolution at the time of response or as soon as practicable thereafter.

Cisco may have user access to view Your Cisco Cloudlock user interface for the purposes of providing technical support and in order to continually improve the operation, security efficacy and functionality of Cisco Cloudlock.

Scheduled Maintenance.
In all cases where scheduled maintenance for Cisco Cloudlock will be performed, Cisco will make reasonable attempts to ensure that scheduled maintenance that affects the availability of Cisco Cloudlock for more than thirty (30) minutes is performed between 12:00 AM and 5:00 AM Eastern Time, Monday through Friday (excluding U.S. holidays), or between 12:00 PM and 5:00 AM Eastern Time on Saturday, Sunday and U.S. holidays.

From time to time, Cisco performs scheduled maintenance to update the servers and software that are used to provide Cisco Cloudlock. Cisco agrees to use reasonable efforts to provide You with prior notice of any scheduled maintenance in advance of any planned downtimes that would impact Your use of Cisco Cloudlock. Notwithstanding the foregoing, You acknowledge that Cisco may, in certain situations, need to perform emergency maintenance of Cisco Cloudlock without providing advance notice.

Feedback.
Cisco has the right, but not the obligation, to incorporate Feedback into Cisco Cloudlock in its sole discretion. You hereby grant Cisco a non-exclusive, irrevocable, worldwide, perpetual, royalty-free, transferable (in whole or in part) and fully paid-up license to use the Feedback for any purpose whatsoever, including, without limitation, for purposes of enhancing, developing, marketing, and/or promoting Cisco products and services, including Cisco Cloudlock.

[Appendix A Follows]

Appendix A

Definitions

"Active Policy" means a predefined policy that comes with Cisco Cloudlock or a policy You create to the extent any such policy is flagged as active within Cisco Cloudlock.

"Cisco Cloudlock Metadata" is information and data generated or collected through use of Cisco Cloudlock and stored within Cisco Cloud Lock including, but not limited to information about the use of a Covered Cloud Service, such as user accounts, usernames, organizational structure (groups, OUs, etc.), permissions (e.g. Alice may access files in folder "Wonderland"); file, record or other asset information such asset names, identifiers, sizes, types, and owners; file or record creation and modification dates; folder structure; login /logout information including IP addresses and location; asset access information (e.g. Alice has downloaded file X at date and time Y); configuration changes made by users to the Covered Cloud Service or their accounts; Cisco Cloud Lock configuration information; security settings; information about 3rd party applications installed or connected to the Covered Cloud Service (e.g. identifiers, date and time installed, permissions, and activity); policies (including regular expressions) implemented or configured by You for use with Cisco Cloudlock; incidents and alerts raised by Cisco Cloudlock; audit logs and files; and access keys and authentication tokens provided by You to allow access to the target Covered Cloud Service.

"Cisco Threat Content" means any Cisco provided content or data including, but not limited to, rules, signatures, threat data feeds or suspicious IP address data feeds for use with any Cisco product or service.

"Core Cisco Cloudlock Services" means, as of the publication date of this Offer Description, the following: Cloudlock for Google, Cloudlock for Salesforce, Cloudlock for Dropbox, Cloudlock for Box, Cloudlock for Microsoft Office365, Cloudlock for ServiceNow, and Cloudlock App Connector for Slack. Additional core services may be made available for Cisco Cloudlock from time to time.

"Covered Cloud Services" means the applicable SaaS, PaaS, or IaaS environments for which You will use Cisco Cloudlock (e.g. Your Salesforce, Box or Dropbox environment).

"Customer Data" means all information and materials that You or Your users or anyone acting on Your behalf provide or make accessible to Cisco and/or Cisco Cloudlock in connection with Your use of Cisco Cloudlock.

"Data Asset" means a single discrete file, record, document or other object within the applicable Covered Cloud Services.

"**Documentation**" means Cisco's release notes, technical guides and user documentation in hard copy or machine-readable form that describe the functionality of the applicable Cloud Service and/or the Software.

"Domain" means a single installation, instance, or domain of the applicable Covered Cloud Service. For example, one Domain is one Google Apps installation or one Salesforce Org or installation.

"Feedback" means any suggested changes, clarifications, additions, modifications or recommended product improvements to Cisco Cloudlock that You or Your users provide to Cisco as part of technical support or otherwise whether by direct entry into a product user interface, phone conversation, e-mail or otherwise.

"Non-Identifiable Aggregated Data" means any information or data that Cisco derived from Customer Data and/or Cisco Cloudlock Metadata provided that such information or data is aggregated and/or anonymized such that it cannot reasonably be used to identify an individual or entity and cannot otherwise be used to identify Your network.

"Retroactive Monitoring" is the ability to assess Your entire data set at-rest for policy violations including all historic available data objects in the applicable cloud application.

"Salesforce Communities Log-In User" is a User of Salesforce Communities with a login-based license that consumes a login each time he or she logs in to the community.

"Salesforce Communities Named User" is a User of Salesforce Communities with a member-based license allowing such User to log in to communities as often as he or she wants.

"**Software**" means any Cisco proprietary security software products or any third party software provided by Cisco via download, if any, and any patches, updates, improvements, additions and other modifications or revised versions thereof that are made available by Cisco from time to time for use with Cisco Cloudlock.

"Student License for Higher Ed" covers a User that is a student for a higher education institution. Student Licenses for Higher Ed include the UEBA and Apps use cases.

"Student License for K-12" covers a User that is a student in a K-12 institution. Student Licenses for K-12 include the DLP and Apps use cases.

"Test/Development Environment" means an environment on Cisco Cloudlock that is authorized to You for test and development purposes and is authorized for up to the lesser of 1,000 Users in the aggregate or the number of User licenses purchased for the Core Cisco Cloudlock Services.

"Users" means the individual users (active, suspended or otherwise) on the applicable Covered Cloud Service being monitored and scanned by Cisco Cloudlock.

*****