Offer Description: Cisco Cloudlock

This Offer Description (the **"Offer Description"**) describes Cisco Cloudlock (the **"Cloud Service"**). Your subscription is governed by this Offer Description and the Cisco Universal Cloud Agreement located at www.cisco.com/go/uca (or similar terms existing between you and Cisco) (the **"Agreement"**). Capitalized terms used in this Offer Description and/or the Order not otherwise defined herein have the meaning given to them in the Agreement.

Table of Contents

1. Offer 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 cloud application environments across users, data, and applications. The core functionality of Cisco Cloudlock covers the following four 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, transfer of ownership, and quarantines.

User and Entity Behavior Analytics ("UEBA"): Cisco Cloudlock provides cross-platform UEBA functionality for cloud application 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.

Apps Firewall ("Apps Firewall"): Certain Cisco Cloudlock applications enable discovery of cloud applications connected to Your corporate environment via an Oauth connection, and provide 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 application use in bulk across the entire user base.

App Discovery ("App Discovery"): App Discovery is an optional add-on service that provides visibility into cloud applications (SaaS, PaaS, Iaas) used or visited by individuals through a

customer's network (applications accessed outside of an OAuth connection) via the then current supported data sources.

2. Supplemental Terms and Conditions

2.1. Cisco Threat Content.

If Your use of a Cloud Service 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 Your use with such Cloud Service and with those third party products or services offerings that Cisco has identified as being compatible. You agree not to provide Cisco Threat Content to a third party.

2.2. Integration with Third Party Products.

The Cloud Service may allow you to integrate with third-party products. Cisco does not support or warrant third-party products and disclaims all responsibility and liability for third-party products used with the Cloud Service, including any responsibility for customer data transferred to such third-party product through Your use of the applicable integration. If You use a third-party product, the terms of use for that third-party product are between You and the provider. Some third-party products may contain tracking technology. Accordingly, it is Your responsibility to read the third party's disclosures, terms of use, and privacy policy before using such third-party products with the Cloud Service.

2.3. Disclaimers.

CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICES 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 THE CLOUD SERVICES 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 A CLOUD SERVICE 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.

2.4. 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 and 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.

2.5. Users and Usage.

Please see https://www.cloudlock.com/usage/ for information on how to count users for your Cisco Cloudlock subscription and for other applicable usage based limitations.

2.6. Application Programming Interfaces ("APIs").

Application Programming Interfaces (APIs). APIs 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.

3. Data Protection

Cisco's data protection obligations are set forth in the Agreement. Additionally, the Cisco Cisco Cloudlock Privacy Data Sheet(s) (available here) supplement the Cisco Privacy Statement and describe the Personal Data that Cisco collects and processes as part of the delivery of the Cloud Services.

If You use the Cloud Service in China, You (1) acknowledge that You are the entity causing data to be transferred outside of China in connection with your use of the Cloud Service, and (2) acknowledge Your obligation to comply with China's cybersecurity requirements and other requirements related to the cross border transfer of data.

If You use the Cloud Service in Russia, You acknowledge that You are the data operator as defined under Russian law for purposes of Your users' personal data that is collected and processed in connection with the Cloud Service.

4. Support & Maintenance.

Technical support for Cisco Cloudlock will be provided in accordance with the applicable Technical Support Level and Priority/Response Targets set forth below, unless You are receiving support directly from the applicable Approved Source. The embedded support option for Cisco Cloudlock is the Basic level described below.

Cisco may adjust assigned case severity or priority to align with the definitions herein.

Technical Support Level	Description
Basic	• Email Access Only

Technical Support Level	Description
	• Access to online tools (e.g. knowledgebase, forums, Documentation, case portal, and notifications)
Gold	• Email Access • Access to online tools (e.g. knowledgebase, forums, Documentation, case portal, and notifications) • 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 in Availability SLA)	--30 minutes for phone request --2 hours for email request	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 the Cloud Service is available but response times are slow while Your Internet connection is working correctly. Issues include technical questions or configuration issues related to Your account that moderately impact Your ability to use the Cloud Service. 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.

From time to time, Cisco performs scheduled maintenance, to update the servers and software that are used to provide the Cloud Service. Cisco will make all notifications for such scheduled maintenance solely via email and status web portals. Notwithstanding the foregoing, You acknowledge that Cisco may need to perform emergency maintenance without providing advance notice.

Cisco reserves the right to modify and update the features and functionality of the Cloud Services. Cisco will make good faith efforts to provide notice of any material modification or updates to the Cloud Services and will use commercially reasonable efforts to implement modifications or updates in a manner that minimizes the impact on your use of and the performance of the Cloud Services.

You will also have access to Cisco.com, which provides helpful technical and general information about Cisco products, as well as access to Cisco's on-line knowledge base and forums. Please note that access restrictions identified by Cisco from time to time may apply.

Definitions.

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

Telemetry Data means Telemetry Data as defined in the Agreement and for the avoidance of doubt, includes without limitation: netflow data; origin and nature of malware; network security policies; the types of software or applications installed on a network or an endpoint; information related to the usage, origin of use, traffic patterns and behavior of the users of a network or cloud service; any geolocation data; or network traffic data such as cookies, web logs, web beacons, and other similar applications.