Offer Description: Cisco Umbrella

This Offer Description (the **"Offer Description"**) describes Cisco Umbrella (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 Umbrella is a cloud-based security platform at the DNS (domain name system) layer that provides the first line of defense against threats on the Internet by blocking requests to malicious destinations (domains, IPs, URLs) before a connection is established. It provides protection against threats over all ports and protocols, and can protect Internet access across all devices on Your network, all office locations, and roaming users. Cisco Umbrella Investigate provides access to certain Cisco Threat Content about malicious domains, IPs, networks, and file hashes. Using a diverse dataset of billions of daily DNS requests and live views of the connections between different networks on the Internet, Cisco Umbrella Investigate applies statistical models and human intelligence to identify attackers' infrastructures. Cisco Umbrella Investigate's data can be accessed via a web-based console or an API.

Your Cisco Umbrella subscription includes access to Cisco Threat Response. Cisco Threat Response is a cloud based aggregator of threat intelligence collected or generated by Cisco security products as well as other third party security products. Cisco Threat Response allows You to pull together critical threat intelligence and add context from Your organization so You know which systems and devices are infected.

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. Restrictions.

If You are an authorized Cisco service provider whose contract with Cisco authorizes You to utilize Cisco cloud services on behalf of end customers, You may use the Cloud Service for the benefit of such end customers.

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. Cisco Umbrella Cloud Delivered Firewall ("CDFW").

In connection with Your use of CDFW (to the extent applicable), You will not (and will not allow any third party to): (i) use the Cloud Service to run automated queries to external websites; (ii) use the Cloud Service to access websites or blocked services in violation of applicable law and/or regulation; or (iii) use the Cloud Service for the purpose of intentionally masking Your identity in connection with the commission of unlawful activities or to otherwise avoid legal process. Additionally, by using CDFW, you acknowledge that in the event that Cisco receives a third party request for information, demand letter, or other similar inquiry with regards to alleged unlawful activity on Your network, Cisco may disclose Your name to such third party as necessary to comply with legal process or meet national security requirements; protect the rights, property, or safety of Cisco, its business partners, You, or others; or as otherwise required by applicable law.

CDFW Bandwidth: CDFW is licensed by mega bits per second ("Mbps") and the total amount of Mbps that You are licensed to use is your "Subscribed Bandwidth." Cisco will continuously measure Your usage of CDFW throughout a given month by analyzing the previous thirty (30) day period for peaks in Mbps on Your network. If at any time, Cisco determines that Your 95th Percentile Bandwidth (defined below) has exceeded Your Subscribed Bandwidth, Cisco reserves the right, in its sole discretion and at any point during the thirty (30) day monitoring period, to throttle Your bandwidth or require You to increase Your Subscribed Bandwidth at Your cost.

Your 95th Percentile Bandwidth is calculated by observing Your Mbps peaks over the course of thirty (30) days, with the first thirty (30) day period beginning upon activation of the Cloud Service, and discarding the top five (5) Mbps peaks observed in that time frame. The next highest peak value after discarding the top five (5) Mbps peaks is Your “95th Percentile Bandwidth.” For example, if Your six (6) highest Mbps peaks were measured as 22Mbps,

25Mbps, 28Mbps, 35Mbps, 27Mbps, and 24Mpbs for that thirty (30) day period, Your 95th Percentile Bandwidth would be 22Mbps.

2.5. 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.

3. Service Level Agreement

For purposes of this Service Availability Commitment, "Service" shall be defined as Cisco's recursive DNS service and does not include web-based user interfaces, configuration systems or other data access or manipulation methods. Cisco shall use commercially reasonable efforts to maintain Cisco Umbrella Service availability of 99.999% 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 Umbrella Service 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 Umbrella is completely unreachable when Your Internet connection is working correctly, (ii) "Uptime" means the number of minutes where there were no Cisco Umbrella Service 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 Umbrella Outages arising out of Third Party Actions.

4. Data Protection

Cisco's data protection obligations are set forth in the Agreement. Additionally, the Cisco Umbrella 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.

5. Support & Maintenance.

Technical support for Cisco Umbrella 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 Umbrella 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 • 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)
Platinum	• Dedicated technical account manager (TAM) • 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.

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.