Offer Description: Cisco Umbrella

This Offer Description (the "Offer Description") describes Cisco Umbrella ("Umbrella" or "Cisco Technology"). Your subscription is governed by this Offer Description and the Cisco End User License Agreement located at www.cisco.com/go/eula (or similar terms existing between you and Cisco) (the "Agreement"). If capitalized terms are not defined in this Offer Description, then they have the meaning given to them in the Agreement or order(s).

1. Description

Umbrella is a cloud security platform that unifies multiple security services in a single cloud-delivered platform to secure internet access and control cloud app usage from your network, branch offices, and roaming users. Your Umbrella subscription includes access to Cisco SecureX, Cisco's integrated security platform that aggregates threat intelligence, unifies visibility across various Cisco and third-party security products, enables automated workflows, and more. The Package Comparison provides information about the various Umbrella packages.

2. Supplemental Terms and Conditions

2.1. Covered Users

For packages with user-based pricing, You must purchase one user license for each Covered User unless a published Umbrella data sheet states otherwise.

2.2. Usage and Range Limits

Umbrella is subject to limitations and range limits set forth in the SIG Documentation and the DNS Documentation.

Umbrella SIG packages are subject to an average bandwidth limit of up to 50 kilobits per second ("kbps") per Covered User, based on a 95th Percentile Calculation (whether such traffic is generated by individuals, devices, or servers). The 95th Percentile Calculation allows peaks in usage that exceed the limit for brief periods of time. "95th Percentile Calculation" means Cisco: (a) takes traffic samples over the course of 30 days at each Cisco Umbrella data center handling Your traffic, (b) discards the top 5% of the traffic samples at each such data center and takes the next highest traffic sample value (this next highest traffic sample value is called the "Peak Value"), and (3) adds together the Peak Value for each data center. This limit is further described in the SIG Documentation referenced above.

Umbrella DNS Security packages are also subject to a monthly DNS query limit average (whether such queries are generated by individuals, devices, or servers). This limit is further described in the DNS Documentation referenced above.

You and Cisco agree to work together in good faith to resolve any excessive usage.

2.3. Cisco Umbrella Reserved IP

If You have purchased a subscription to Cisco Umbrella Reserved IP, please see Reserved IP Supplemental Terms for additional terms and conditions applicable to Your subscription.

2.4. Cisco-Managed S3 Log Storage

Certain Umbrella packages include the ability to select Cisco-managed S3 storage or Your own storage for DNS, proxy, and event logs. Cisco-managed S3 log storage is available with 7-day, 14-day or 30-day retention options.

Please see the Cisco-managed S3 Bucket documentation for related requirements and best practices.

2.5. Data Centers

Your Cisco Umbrella subscription includes access to Cisco Umbrella global data centers found here: Global Data Centers. Data centers not included at this link may require a separate subscription. And any data center(s) located in mainland China, when and if available, require a separate subscription purchased directly through the applicable service operator in China.

2.6. Acceptable Use

You will not (and will not allow any third party to): (i) establish regular and frequent automated queries to an external site, such as port scanning of a third-party entity not in Your control, or use offensive security technologies against a third party through the use of Umbrella (because these actions could reasonably be viewed by the external site as a denial of service attack or a violation of the third party's terms and could lead to Cisco being blacklisted); (ii) use Umbrella to access websites or blocked services in violation of applicable law and/or regulation; or (iii) use Umbrella for the purpose of intentionally masking Your identity in connection with the commission of unlawful activities or to otherwise avoid legal process. If Cisco receives a third-party request for information, demand letter, or other similar inquiry in connection with Your use of Umbrella relating 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.

2.7. Disclaimers

WHILE CISCO HAS USED COMMERCIALLY REASONABLE EFFORTS TO CREATE EFFECTIVE SECURITY TECHNOLOGIES, DUE TO THE CONTINUAL DEVELOPMENT OF NEW TECHNIQUES FOR INTRUDING UPON AND ATTACKING FILES, NETWORKS, AND ENDPOINTS, CISCO DOES NOT REPRESENT OR WARRANT THAT UMBRELLA WILL GUARANTEE ABSOLUTE SECURITY OR THAT IT WILL PROTECT ALL YOUR FILES, NETWORK, OR ENDPOINTS FROM ALL MALWARE, VIRUSES, OR THIRD-PARTY MALICIOUS ATTACKS.

3. Service Levels Agreements

3.1. DNS Service

Cisco will use commercially reasonable efforts to maintain DNS Service availability of 99.999% of each calendar month. "DNS Service" means the Umbrella recursive DNS service, excluding web-based user interfaces, dashboards, reporting or other services available to Your Umbrella administrators. Availability will be calculated by dividing the total number of minutes of Uptime during the applicable calendar month by the total number of minutes in such month less minutes of Outages occurring due to scheduled maintenance and/or Third-party Actions and multiplying the result by 100. The formula for this calculation is as follows:

Availability = (X ÷ Y) x 100, where:

X= Total # of minutes of Uptime during calendar month; and

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

3.2. SIG Service

Cisco will use commercially reasonable efforts to maintain SIG Service availability of 99.99% of each calendar month. "SIG Service" means the Umbrella SIG service, excluding web-based user interfaces, dashboards, add-ons, reporting or other services available to Your Umbrella administrators. Availability for the SIG Service means the service is available to accept end user Internet traffic from You when properly configured to allow You to leverage the Umbrella redundant global infrastructure. If You are using IPSec tunnels(s), proper configuration means the SIG Service is configured with a primary and secondary tunnel with failover behavior.

Availability will be calculated by dividing the total number of minutes of Uptime during the applicable calendar month by the total number of minutes in such month less minutes of Outages occurring due to scheduled

maintenance and/or Third-Party Actions and multiplying the result by 100. The formula for this calculation is as follows:

Availability = (X ÷ Y) x 100, where:

X= Total # of minutes of Uptime during calendar month; and

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

4. Data Protection

The Cisco Umbrella and Cisco SecureX Privacy Data Sheets describe the Personal Data that Cisco collects and processes as part of the delivery of Umbrella. Additionally, some Umbrella packages leverage Cisco Secure Malware Analytics analysis features (formerly, AMP Ecosystem and Threat Grid). Please see the applicable Privacy Data Sheets available on the Trust Portal. For further details on how Cisco processes, uses and protects all categories of data, please visit Cisco's Security and Trust Center.

5. Support & Maintenance

Cisco Umbrella support packages are referenced below. Unless You receive support directly from Your Cisco partner, Cisco will respond as set forth in the table below and may require information from You to resolve service issues. You agree to provide the information requested and understand that a delay in providing the information to Cisco may delay resolution and response time.

Phone Support provides Cisco Technical Assistance Center (TAC) access 24 hours per day, 7 days per week to assist by telephone. Support also includes access to online tools to assist with usage and troubleshooting issues. You also have access to Cisco.com, which provides helpful technical and general information about Cisco products, and to Cisco's online knowledge base and forums. Please note that access restrictions identified by Cisco from time to time may apply. Your access to and use of Umbrella may be suspended for the duration of unanticipated or unscheduled downtime, including as a result of catastrophic events, external denial of service or other security breach, or operational incidents.

The below table outlines Cisco's response objectives based on case severity. Cisco may adjust assigned case severity to align with the severity definitions below.

Software Support Service	Technical Support Coverage	Response Time Objective for Case Severity 1 or 2	Response Time Objective for Case Severity 3 or 4
Basic	Email access only for Severity 3 or 4 Email and phone for Severity 1 and 2 Access to online tools (e.g., knowledgebase, forums, Documentation, case portal, and notifications)	Response within 1 hour of receipt of phone call	Response next Business Day
Enhanced (previously "Gold")	24x7 via Phone & Web	Response within 30 minutes	Response next Business Day
Premium	24x7 via Phone & Web	Response within 15 minutes	Response next Business Day

6. Definitions

"**Business Day**" means the generally accepted days of operation per week within the relevant region where the Cloud Service will be performed, excluding local holidays as observed by Cisco.

"**Local Time**" means Central European Time for support provided in Europe, Middle East and Africa, Australia's Eastern Standard Time for support provided in Australia, Japan's Standard Time for support provided in Japan and Pacific Standard Time for support provided in all other locations.

"**Response time**" means the time between case submission in the case management system to support engineer contact.

"**Severity 1**" means Umbrella is unavailable or down or there is a critical impact to Your business operation. You and Cisco both will commit full-time resources to resolve the situation.

"**Severity 2**" means Cisco Umbrella is severely degraded or significant aspects of Your business operation are negatively impacted by unacceptable performance. You and Cisco both will commit full-time resources during Standard Business Hours to resolve the situation.

"**Severity 3**" means Umbrella is impaired, although most business operations remain functional. You and Cisco are both willing to commit resources during Standard Business Hours to resolve the situation.

"**Severity 4**" means a minor intermittent functionality or performance issue with, or information is required about Umbrella. There is little or no impact to Your business operation. You and Cisco are both willing to provide resources during Standard Business Hours to provide assistance or information as requested

"**Standard Business Hours**" means 8am to 5pm Local Time at the location of the respective Cisco TAC, on Business Days, for the handling of TAC calls.

"**Covered User**" means each Internet-connected employee, subcontractor, and any other authorized individual covered (i.e., protected) by Your deployment of Umbrella.

"**Outage**" means (i) the DNS Service is completely unreachable when Your Internet connection is working correctly; or (ii) the SIG Service is not available to accept end user Internet traffic from You when properly configured; excluding Outages due to scheduled maintenance and/or Third-Party Actions.

"**Uptime**" means the number of minutes where there were no Outages, excluding Outages for scheduled maintenance and/or Third-Party Actions.

"**Third-Party Action**" means any action beyond Cisco's reasonable control including, without limitation, the failure of Your network to forward Internet traffic to Cisco, the performance of Internet networks controlled by other companies (e.g., ISP) or traffic exchange points that are controlled by other companies, local regulations or practices that prevent or limit Cisco from processing Internet traffic in certain regions, events of force majeure (e.g., labor strikes or shortages, riots, insurrection, fires, flood, storm, explosions, war, terrorism, governmental action, labor conditions, earthquakes, global pandemics and material shortages), and Your failure to purchase adequate licenses to meet the volume or capacity at which You use Umbrella, if the service level objective would have been met if not for such failure.