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 End User License Agreement located at www.cisco.com/go/eula (or similar terms existing between you and Cisco) (the “Agreement”). Capitalized terms used in this Offer Description and not otherwise defined herein have the meaning given to them in the Agreement.

Table of Contents

1. Description ....................................................................... 1
2. Supplemental Terms and Conditions ................................. 1
   2.1. Restrictions .............................................................. 1
   2.2. Disclaimers ............................................................... 1
   2.4. Cisco Umbrella Secure Internet Gateway Essentials (“SIG Essentials”)........................................................ 2
   2.5. Cloud Delivered Firewall and SIG Essentials .............. 3
   2.6. DNS Security Essentials and DNS Security Advantage (“DNS Security”).........................................................3
   2.7. Cisco Umbrella Investigate for MSSP .......................... 3
   2.8. Cisco-Managed S3 Log Storage .................................. 3
3. Service Level Agreement .................................................... 3
4. Data Protection .................................................................... 4
5. Support & Maintenance .................................................... 4
   5.1. Cisco Umbrella Technical Support.............................. 4
   5.2. SIG Essentials and DNS Security Technical Support ... 5

1. Description

Cisco 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. Depending on the package and deployment, Cisco Umbrella integrates secure web gateway, cloud-delivered firewall (“CDFW”), DNS-layer security, cloud malware protection and cloud access security broker (CASB) functionality for effective protection anywhere users go. Before users connect to any online destination, Cisco Umbrella acts as a secure onramp to the internet and delivers deep inspection and control to support compliance and block threats. Cisco Umbrella is backed by one of the largest threat intelligence teams in the world, Cisco Talos, and it provides interactive access to threat intelligence through Cisco Umbrella Investigate to aid in incident response and threat research. Cisco Umbrella Investigate provides access to certain Cisco threat intelligence 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 applies statistical models and human intelligence to identify attackers’ infrastructures. Cisco Umbrella Investigate data can be accessed via a web-based console or an API. Please consult the Umbrella Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

Your Cisco Umbrella subscription includes access to Cisco SecureX, Cisco’s integrated security platform that aggregates threat intelligence (through SecureX threat response, also known as Cisco Threat Response), unifies visibility across various Cisco and third party security products, enables automated workflows, and more. For more information on SecureX, please see the SecureX Offer Description at https://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html.

2. Supplemental Terms and Conditions

2.1. 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 only for the benefit of such end customers.

2.2. 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.

2.3. Cisco Umbrella Cloud Delivered Firewall – DNS Security Add-On for Layers 3 and 4 (“CDFW L3/4”)

CDFW L3/4 Bandwidth: CDFW L3/4 is licensed by megabits 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 L3/4 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 5% of the Mbps peaks observed in that time frame. The next highest Mbps peak value after discarding the top 5% Mbps peaks is Your “95th Percentile Bandwidth.” For example, if there are one hundred (100) Mbps peaks observed, Cisco would discard the top five (5) Mbps peaks and the next highest Mbps peak is Your 95th Percentile Bandwidth. So, if the highest six (6) 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.

2.4. Cisco Umbrella Secure Internet Gateway Essentials (“SIG Essentials”)

The following use limitations apply in connection with Your use of Cisco Umbrella Secure Internet Gateway Essentials and Cisco Umbrella Secure Internet Gateway SIG Essentials Add-On (collectively, “SIG Essentials”).

SIG Essentials is licensed based on the quantity of Covered Users and is subject to an Average Bandwidth (as defined below) limit of 50 kilobits per second (“kbps”). “Covered Users” means the total number of your internet-connected employees, subcontractors and other authorized individuals covered by your deployment of the applicable Software or Cloud Service.

Cisco will continuously measure Your usage of SIG Essentials throughout a rolling thirty (30) day period to determine Your Average Bandwidth. If at any time Cisco determines that Your Average Bandwidth has exceeded 50 kbps, Cisco reserves the right to require You to purchase additional licenses as required to reduce Your Average Bandwidth to 50 kbps. The formula for Average Bandwidth is:

\[
\text{Average Bandwidth} = \frac{95^{th} \text{ Percentile Bandwidth}}{\text{Number of Covered Users}}
\]

The 95th Percentile Bandwidth is calculated by: (i) observing Your traffic samples over the course of thirty (30) days at each Cisco Umbrella data center Your traffic is sent to, (ii) discarding the top 5% of the traffic samples at each such data center and taking the next highest traffic sample value (“Peak Value”), and (iii) adding together the Peak Value for each data center. Traffic samples for purposes of this calculation include DNS traffic, secure web gateway (proxy) traffic and CDFW traffic (Layer 3, Layer 4 and if applicable, Layer 7).

For example, if the Peak Value at one data center is 1,000,000 kbps and the Peak Value at a second data center Your traffic is sent to is 10,000 kbps, the 95th Percentile Bandwidth is 1,000,000 + 10,000 = 1,010,000 kbps. The Average Bandwidth would be 1,010,000 kbps divided by the number of Covered Users licensed under Your subscription. If You have 25,000 users covered by Your subscription. Your Average per user Bandwidth for the monitored period is 1,010,000 / 25,000 = 40.4 kbps.
2.5. **Cloud Delivered Firewall and SIG Essentials**

In connection with Your use of Cisco Umbrella Cloud Delivered Firewall and/or SIG Essentials, 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 either of these Cloud Services, 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.

2.6. **DNS Security Essentials and DNS Security Advantage (“DNS Security”)**

The following use limitations apply in connection with Your use of Cisco Umbrella DNS Security Essentials and DNS Security Advantage (collectively, “DNS Security”).

DNS Security is licensed based on the quantity of Covered Users and is subject to a Monthly DNS Query Average (as defined below) limit of three thousand (3,000) DNS queries per User per day. Cisco will continuously monitor Your usage of DNS Security on a monthly basis to determine Your Monthly DNS Query Average. If at any time Cisco determines that Your Monthly DNS Query Average has exceeded three thousand (3,000) DNS queries per Covered User per day, Cisco reserves the right to require You to purchase additional licenses as required.

Monthly DNS Query Average = \[(\frac{\text{number of DNS queries in applicable month}}{\text{number of days in applicable month}}) / \text{number of licensed Covered Users}\]

For example, if You purchased licenses for 1,000 Covered Users and Your Covered Users submitted a total of 3,000,000 DNS queries in the prior 30-day month, Your Monthly DNS Query Average is as follows:

\[
\frac{3,000,000}{30} / 1,000 = 100
\]

2.7. **Cisco Umbrella Investigate for MSSP**

Notwithstanding anything to the contrary in the Agreement, if You purchased a Cisco Umbrella Investigate for MSSP SKU labeled UMB-INV-CONSOLE-SP and/or UMB-INV-INT-API-SP (collectively, “Investigate for MSSP”), You may use Investigate for MSSP as a tool to perform research and generate reports for the benefit of Your third party customers solely as part of connectivity, management, and/or administrative services You provide to Your third party customers.

Any co-branding of Investigate for MSSP by You shall be subject to the guidelines located here: https://www.cisco.com/c/dam/en/us/products/collateral/security/umbrella/umbrella-sps-co-branding-guidelines.pdf and any additional intellectual property and trademark guidelines set forth in the Agreement. For clarity, if You provide any research, data, or results generated from Your use of Investigate for MSSP to Your third party customers, You must at all times credit Cisco as the source of such information following the above guidelines.

2.8. **Cisco-Managed S3 Log Storage**

Certain Cisco Umbrella packages include the ability to select Cisco-managed S3 storage or Company-managed storage (i.e. Your own storage) for DNS, proxy and event logs. Cisco-managed S3 log storage is available with 7, 14 or 30 day retention options. If You require more than 30 days retention, You should select Company-managed storage or export the data from the Cisco-managed storage to Your Company-managed storage prior to the expiration of the retention period.

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:

\[
\text{Availability} = \left( \frac{X}{Y} \right) \times 100
\]

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

The Cisco Umbrella, Cisco Threat Response, and Cisco SecureX Privacy Data Sheets (available [here](#)) describe the Personal Data that Cisco collects and processes as part of the delivery of the Cloud Services. Additionally, Cisco Umbrella Insights, Cisco Umbrella Platform, Cisco Umbrella Secure Internet Gateway (SIG) Essentials, Cisco Umbrella DNS Security Advantage, and Cisco Umbrella Secure Internet Gateway (SIG) Essentials Add-on package(s) leverage(s) the Cisco Advanced Malware Protection (AMP) Ecosystem. Please see the AMP Ecosystem Privacy Data Sheet (available [here](#)). 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

5.1. Cisco Umbrella Technical Support

Except for SIG Essentials and DNS Security, 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.

<table>
<thead>
<tr>
<th>Technical Support Level</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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) |
### Technical Support Level

<table>
<thead>
<tr>
<th>Technical Support Level</th>
<th>Description</th>
</tr>
</thead>
</table>
|                         | • 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

<table>
<thead>
<tr>
<th>Support Priority</th>
<th>Response Target</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.

#### 5.2. SIG Essentials and DNS Security Technical Support

SIG Essentials and DNS Security include online support and phone support. 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, or web case submission and online tools with use and troubleshooting issues.

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.
The below table outlines Cisco’s response objectives based on case severity. Customers have the option of selecting Enhanced or Premium support for DNS Security and SIG Essentials. Cisco may adjust assigned case severity to align with the Severity definitions below.

<table>
<thead>
<tr>
<th>Software Support Service</th>
<th>Technical Support Coverage</th>
<th>Response Time Objective for Case Severity 1 or 2</th>
<th>Response Time Objective for Case Severity 3 or 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced</td>
<td>24x7 via Phone &amp; Web</td>
<td>Response within 30 minutes</td>
<td>Response within 2 hours</td>
</tr>
<tr>
<td>Premium</td>
<td>24x7 via Phone &amp; Web</td>
<td>Response within 15 minutes</td>
<td>Response within 1 hour</td>
</tr>
</tbody>
</table>

The following definitions apply to this Section.

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

**Severity 1** means SIG Essentials or DNS Security, as applicable, is unavailable or down or there is a critical impact to a significant impact to Case Submitter’s business operation. Case Submitter and Cisco both will commit full-time resources to resolve the situation.

**Severity 2** means SIG Essentials or DNS Security, as applicable, is degraded or significant aspects of Case Submitter’s business operation are negatively impacted by unacceptable software performance. Case Submitter and Cisco both will commit full-time resources during Standard Business Hours to resolve the situation.

**Severity 3** means SIG Essentials or DNS Security, as applicable, is impaired, although most business operations remain functional. Case Submitter and Cisco both are willing to commit resources during Standard Business Hours to resolve the situation.

**Severity 4** means minor intermittent functionality or performance issue, or information is required on SIG Essentials or DNS Security, as applicable. There is little or no impact to Case Submitter’s business operation. Case Submitter and Cisco both are willing to provide resources during Standard Business Hours to provide assistance or information as requested.

**Business Day** means the generally accepted days of operation per week within the relevant region where the Cloud Services 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.