Offer Description
for
AMP, Threat Grid, Clarity, CTA, Stealthwatch Cloud, CES, CRES, CDO, Umbrella, and Cloudlock

OVERVIEW

This Offer Description describes the following security Cloud Services:

- Cisco Advanced Malware Protection (AMP)
- Cisco AMP Threat Grid
- Cisco Clarity
- Cisco Cognitive Threat Analytics (CTA)
- Cisco Stealthwatch Cloud
- Cisco Cloud Email Security (CES) and Cisco Registered Envelope Service (CRES)
- Cisco Defense Orchestrator (CDO)
- Cisco Umbrella
- Cisco Cloudlock

The Cisco Universal Cloud Agreement ("**Agreement**") and the terms herein govern Your use of each Cloud Service referenced herein. A current copy of the Agreement is located at: http://www.cisco.com/c/en/us/about/legal/cloud-and-software.html.

Unless defined within the text herein, capitalized terms used in this Offer Description are defined in **Appendix A**, **Appendix B** (for Cloudlock) or the Agreement.

If a Cloud Service listed in this Offer Description is compatible for use with other Cisco products or service offerings not referenced herein, such other products and/or offerings may have additional license terms that apply to Your use of such products and offerings. You are also responsible for complying with the terms for such other Cisco products and offerings, as applicable. The terms set forth herein apply to the Cloud Services listed in this Offer Description whether purchased for use on a standalone basis, or purchased for use with such other Cisco products or offerings.

GENERAL TERMS AND CONDITIONS

The following general terms and conditions apply to *all* Cloud Services referenced in this Offer Description:

A. Technical Support. Cisco will provide You with 24x7 Cisco Software Subscription Support Services for each Cloud Service, the current terms of which are located at: http://www.cisco.com/c/dam/en_us/about/doing_business/docs/cisco-software-support-service.pdf; however, the terms of support for the Cloudlock and Umbrella Cloud Services are set forth below.

B. Scheduled Maintenance. From time to time, Cisco performs scheduled maintenance to update the servers and software that are used to provide the Cloud Services. 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 a Cloud Service. Notwithstanding the foregoing, You acknowledge that Cisco may, in certain situations, need to perform emergency maintenance of a Cloud Service without providing advance notice.

C. 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.

D. Use Limitations. You may not deploy or use a Cloud Service in a manner that (i) extends beyond the duration of the applicable subscription term (e.g. 1 month, or 1, 3 or 5 years), or (ii) exceeds any use limitations or other metrics related to Your license (e.g. number of Seats, Effective Megaflows, Endpoints, maximum queries, device limits, sites, access points, users, hosts, file submissions, scans, assets, etc.) as set forth in this Offer Description, an Order, SKU, product identifier (PID) or Documentation for the applicable Cloud Service.

E. Use of Software. If the Cloud Service You use analyzes malware and files that function on Microsoft or other third party operating systems and/or applications, then it is Your obligation to obtain and comply with all applicable Microsoft and other third party product licenses for every end-user device running such Microsoft and third party products.

F. Cisco Use of Data. As part of Your use of the Cloud Services You will be providing, making accessible to Cisco and/or generating through your use of the Cloud Service(s) (i) Customer Data, (ii) Network Data, and (iii) Cisco Cloudlock Metadata (if You are using Cisco Cloudlock) (all of the foregoing collectively shall be referred to herein as "**Data**"). You acknowledge and consent that Cisco may use Data for the purposes of (a) delivering, enhancing, maintaining, customizing and/or supporting the Cloud Services; and (b) creating Statistical Data. Cisco may share Data (x) within Cisco and any of our worldwide subsidiaries and with our authorized contractors only for the above authorized purposes; (y) as necessary to comply with law and subject to Cisco's policy on law enforcement requests at http://www.cisco.com/c/en/us/about/trust-transparency-center/validation/report.html; and (z) otherwise with Your written consent. Any Personal Data included in Data is defined in, and subject to, the terms set forth in the Agreement.

Some Data that Cisco collects from a Cloud Service, or that You provide or make accessible to Cisco as part of Your use of a Cloud Service, is necessary for the essential use and functionality of such Cloud Service. Data is also used by Cisco to provide associated services such as technical support and to continually improve the operation, security efficacy and functionality of the Cloud Services. For those reasons, You may not be able to opt out from some of the Data collection other than by uninstalling or disabling the applicable Cloud Service. You may have the ability, however, to configure the Cloud Service to limit some of the Data that can be collected, as further described in the applicable Documentation. Certain Cloud Services allow Data to be modified based on Your desired configurations (for example, setting a rule to set publicly accessible data to a private setting).

Please consult the applicable Documentation for more information on how You can configure Data collection.

G. Use of Statistical Data. You hereby grant Cisco a non-exclusive, transferable, irrevocable, worldwide, perpetual, royalty-free and fully paid-up license to use Statistical Data for any purpose whatsoever, including, without limitation, for purposes of enhancing, developing, marketing, and/or promoting Cisco products and services including the Cloud Services.

H. Data Security. 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 the Data used by Cisco.

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

OFFER DESCRIPTIONS AND SUPPLEMENTAL TERMS

Set forth below is a description of each Cloud Service, plus the supplemental terms and conditions that are applicable to each Cloud Service, if any. If You have not purchased a subscription or license to use any of the Cloud Services referenced below, then the description and supplemental terms below for such Cloud Service are not applicable to You.

Cisco Advanced Malware Protection ("AMP")

Description. AMP is a cloud-based advanced malware analysis and protection solution that allows You to conduct metadata File analysis to detect malware and cyber threats. Cryptographic hashes of Files are collected and transmitted to a Cisco-managed cloud server where File reputation analysis is performed and a disposition is made as to whether the File is good, bad or unknown. If a disposition is unable to be made after analysis of the hash of a File, then You have the option (depending on the license(s) purchased) to submit the File to AMP Threat Grid (described below) for further sandboxing analysis up to Your licensed daily submission limit. After the File analysis is completed, AMP will act on the disposition (e.g. by deleting the File and putting it into quarantine if it is determined to be malicious). AMP is available in various form factors including AMP for Endpoints, AMP for Email, AMP for Web, AMP Private Cloud, AMP on NGIPS (AMP for Networks), AMP on NGFW, and AMP for Meraki MX. Please consult the AMP Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

Supplemental Terms.

AMP Private Cloud. AMP Private Cloud offers You a private cloud instance that remains on Your premises (the "Private Cloud") and may be configured to pull updates from the Cisco managed public cloud server ("Public Cloud"). You can choose to run AMP Private Cloud in either "proxy" or "air gap" mode. If You choose "proxy" mode, Your cryptographic hashes of Files will be transmitted from your Private Cloud to the Public Cloud for file reputation analysis. If You choose "air gap" mode, no data is transmitted to the Public Cloud; Your data will remain in the Private Cloud.

Cisco AMP Threat Grid

Description. AMP Threat Grid is a cloud-based malware analysis and threat intelligence sandbox solution to which You can submit malware samples for additional analysis. AMP Threat Grid analyzes each File in order to record its behavior and determine whether it is malicious. AMP Threat Grid will search and correlate data elements of a single malware sample against millions of samples collected and sourced from around the world to give You a global view of malware attacks and its associations. Please consult the AMP Threat Grid Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

Supplemental Terms.

File Submissions. When You submit a File to the AMP Threat Grid cloud, it is possible that due to the comparative analysis functionality included with AMP Threat Grid that another user could examine and determine the contents of such File because AMP Threat Grid crowd-sources malware from its user community. If You elect to submit a File to AMP Threat Grid as a Private File, then that File is not made available to other users for analysis. If You do not designate a File as a Private File upon submission to the AMP Threat Grid cloud, then such File is a Non-Confidential File that can be examined by other users of AMP Threat Grid and will not be considered Confidential Information. Other AMP Threat Grid users have access to Non-Confidential Files and thus have the ability to review the content of Non-Confidential Files. The ability to submit a File to AMP Threat Grid as a Private File may require additional licenses and/or subscriptions.

If a File contains sensitive or Confidential Information that You do not want other users of AMP Threat Grid to have the ability to analyze, then You must either (i) not submit the File to AMP Threat Grid, (ii) submit the File as a Private File, or (iii) submit the File to a local appliance version of AMP Threat Grid for maximum enforcement of confidentiality. Regarding the Non-Confidential Files that Cisco collects in Your use of AMP Threat Grid, You grant to Cisco and its authorized service providers a non-exclusive, perpetual, irrevocable, transferable, worldwide, royalty-free and fully paid-up license, with the right to sublicense, to use all Non-Confidential Files to provide AMP Threat Grid to You and other users and for any other purpose.

Malware samples and Files submitted to the AMP Threat Grid cloud are automatically deleted after twenty-four (24) months. At any time, You may delete these samples or Files via the Threat Grid portal if You have a valid portal account or You may contact customer support to request the deletion of specific samples or Files.

Cisco Clarity ("Clarity")

Description. Clarity is a cloud-based security solution deployable on iOS devices that provides You with visibility and protection against advanced malicious threats. Application and network connectivity details (i.e. domains, IPs, ports, URLs) from Your iOS devices are identified and transmitted to a Cisco-managed cloud server where Your information is correlated against other Cisco Advanced Malware Protection (AMP) Connector details. Using Your correlated data, Clarity and the AMP for Endpoints Console (the "Console") provide You with visibility on non-standard behavior to highlight those iOS devices that may be experiencing suspicious activity. The Console and reporting capabilities can be used to investigate suspicious activity across Your Endpoints. Please consult the Clarity Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

Cisco Cognitive Threat Analytics ("CTA")

Description. CTA is a cloud-based malware behavioral analysis solution that leverages web proxy logs from either Cisco web gateway solutions such as Cisco Web Security Appliance ("WSA") and Cloud Web Security ("CWS") or other supported third-party platforms and/or NetFlow from Cisco Stealthwatch as a way to identify malware present within Your environment and to research related active malicious activities. CTA is available for use as part of AMP for

Endpoints and AMP for Web on WSA licenses or as standalone and/or add-on licenses to other supported AMP products, where applicable. Please consult the CTA Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

Supplemental Terms.

Proxy Log and NetFlow Submissions. To use CTA, You are required to submit web proxy logs from a supported platform and/or NetFlow from Cisco Stealthwatch as described in the Documentation. Such logs may contain identifiable data such as user name, machine name, IP address, and browsing information. CTA may use this data to perform analysis to identify the presence of malware on Your systems and relate communications to and from such systems affected to and from suspected malicious machines or sites. If You do not want to provide Your web proxy logs and/or NetFlow and related information to the CTA cloud to have the ability to analyze for active malware inside Your environment, then You must not enable CTA.

Cisco Stealthwatch Cloud ("Stealthwatch Cloud")

Description. Stealthwatch Cloud technology provides cloud-based dynamic behavioral modeling of entities on the network; it provides You with the ability to gain real-time situational awareness of users, IP connected assets and traffic on the network, in the data center or the cloud. Its cloud-native, machine learning techniques help You to identify insider and external threats through modeling algorithms that detect changes in behavior. Stealthwatch Cloud is available as Private Network Monitoring and Public Cloud Monitoring. Please consult the Stealthwatch Cloud Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

Supplemental Terms.

Scheduled Maintenance. In all cases where scheduled maintenance for Stealthwatch Cloud will be performed, Cisco will make reasonable attempts to ensure that scheduled maintenance that affects the availability of Stealthwatch Cloud for more than thirty (30) minutes is performed between 12:00 AM and 5:00 AM Central Time, Monday through Friday (excluding U.S. holidays), or between 12:00 PM and 5:00 AM Central Time on Saturday, Sunday and U.S. holidays, or on Tuesday between 14:00 and15:00 UTC.

Trials. Free trials for Stealthwatch Cloud are offered for a maximum of sixty (60) days and may include technical support at Cisco's sole discretion.

Cisco Cloud Email Security ("CES") Cisco Registered Envelope Service ("CRES")

Description. CES is a cloud-based email security service that blocks spam and security threats from the Internet and, depending on the features licensed, prevents the accidental or intentional leakage of the Your data. CES includes the option to license Cisco Registered Envelope Service ("CRES"). CRES helps companies secure their email communications and allows businesses to send encrypted messages via registered envelopes. Please consult the CES Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

Supplemental Terms.

CES offers inbound protection and outbound control of Your email traffic. The following feature functionalities are available as part of CES depending on the licensed features purchased:

- Anti-spam
- Intelligent Multi-Scan Anti-spam
- Anti-virus
- Outbreak Filters
- Advanced Malware Protection
- Safe Unsubscribe
- Image Analysis
- Email Encryption (CRES)
- Data Loss Prevention

Your Responsibilities**.** You must supply Cisco with all technical data and other information Cisco may reasonably request to allow Cisco to supply CES to You. Cisco cannot make CES available unless we receive all required information.

CES is delivered on a co-managed model. You are responsible for configuring CES for Your desired use case such as setting the applicable domains, safelists, blocklists, and policy configurations. You are granted administrative access to the application software.

Cisco Responsibilities**.** Cisco is responsible for the maintenance of the back-end hardware, network infrastructure, virtual infrastructure, and application software required for Cisco to make CES available for Your use.

Use Limitations**.** Cisco may audit Your usage of CES and if Cisco determines in good faith that You are using CES as an outbound bulk email delivery service, Cisco may require You to purchase additional services or require You to re-architect the email flow to exclude CES from the outbound bulk email flow.

Capacity Assurance**.** Cisco may, in its sole and reasonable discretion and solely to the extent Your account is in good standing, provide additional capacity to handle an increase in spam volumes and inbound email for the number of users specified on the Order. In such case, Cisco will use commercially reasonable efforts to provide capacity for unforeseen events. Any such additional capacity made available will not exceed 50% of the initial deployed capacity.

The above assurance does not apply to:

1. Capacity requirements placed on CES due to misconfigured, ill-formed or performance intensive activities that include but are not limited to body-scanning, or content dictionaries.
2. Capacity needs placed on CES resulting from a change in applicable regulatory schemes or business environment.
3. Capacity needs placed on CES from non-users including, but not limited to, marketing communications, Your customers, or an email generating program or entity.
4. An increase in email volume from marketing campaigns and other application-generated emails.

Service Level Agreements ("SLAs").

The following defined terms apply to the CES and CRES Service Level Agreements:

- "**Caught Spam**" is Spam either quarantined or categorized as a "threat message" in the user interface.

- **"Infraction"** is a single instance of unavailability in accordance with the specific calculation set forth in the applicable Service Level Agreement. Separate downtime occurrences cannot be aggregated for purposes of determining an Infraction has occurred.
- "**Known Virus**" is defined solely by the provider of anti-virus software that is used for a specific message or file.
- "**Missed Spam**" is Spam delivered to an end user's email inbox.
- **"Service Credits"** are the amounts set forth in the applicable table in each Service Level Agreement and are Your sole and exclusive remedy for an Infraction. Service Credits earned will be applied to either (1) the subscription fee for the next subscription term if You have prepaid for the then-current subscription in full, or (2) the next installment payment amount owed if You are paying for the subscription on a monthly, quarterly or annual installment basis.
- "**Spam**" is unsolicited or unauthorized bulk electronic mail (SMTP only), and excludes unwanted marketing messages that include opt-out provisions.
- "**Virus**" is a binary or executable code whose purpose is to gather information from the infected host, change or destroy data on the infected host, use inordinate system resources in the form of memory, disk space, CPU cycles or network bandwidth on the infected host, use the infected host to replicate itself to other hosts, or provide control or access to any of the infected host's system resources. A Virus does not include: (1) text messages that use fraudulent claims to deceive the customer, and/or prompt the customer to action, (2) a binary or executable code installed or run by the end user that gathers information for sales or marketing purposes, (3) a virus that may be detected and cleaned by other virus scanning products, or (4) an ineffective or inactive virus fragment.

Uptime Service Level Agreement**.** CES will accept connections on Port 25 and process email at least 99.999% of the time during each calendar month, excluding maintenance windows. Uptime is determined by dividing the total number of minutes CES was processing email divided by the number of minutes in that calendar month. A CES downtime must exceed 26 seconds per occurrence for it to be considered an Infraction.

Remedy

If You experience a downtime Infraction, then subject to the General Exceptions (defined below), You will be entitled to the applicable Service Credit set forth in the table below.

Monthly Service Availability	Service Credit as a % of Monthly Fee
< 99.999%	20%
< 99.0%	40%
< 98.0%	100%

Delivery Time Service Level Agreement**.** CES will process email messages such that the monthly Average Time in the Work Queue of CES (as shown in the administrator console) will be less than one (1) minute based on a calendar month, provided, that the quantity of email messages above 10MB sent to CES does not exceed 0.01% of all email traffic. "**Average Time in the Work Queue**" is the amount of time spent processing a message from the point at which the message is accepted via SMTP to the first SMTP delivery attempt from CES.

Remedy

If You experience a delivery time Infraction, then subject to the General Exceptions, You will be entitled to the applicable Service Credit set forth in the table below.

Monthly Average Delivery Time	Service Credit as a % of Monthly Fee
> 1 minute	20%

> 5 minutes	40%
> 10 minutes	100%

Anti-Spam Service Level Agreement**.** CES will detect and stop at least 99% of all inbound Spam that is routed through CES. This "Spam Catch Rate" is determined by dividing Caught Spam by the sum of the Caught Spam and the number of Missed Spam, during a calendar month.

Exception
Marketing emails with opt-out provisions will not be counted as a Missed Spam.

Remedy
If You experience a Spam Catch Rate Infraction, and subject to the exception above and the General Exceptions, then You will be entitled to the applicable Service Credit set forth in the table below.

Spam Catch Rate During Month	Service Credit as a % of Monthly Fee
< 99%	20%
< 98%	40%
< 95%	100%

False Positive Rate Service Level Agreement**.** CES will not categorize legitimate inbound email as Spam more than one (1) time per one million (1,000,000) messages processed. This "***False Positive Rate***" is determined by dividing the number of non-Spam messages misclassified as Spam by the total attempted messages processed during that calendar month.

Exceptions and Conditions
Email messages from legitimate senders whose IP addresses may be compromised due to an unforeseen event will not be counted towards the False Positive Rate. Cisco will make a determination in good faith based on its system logs, monitoring reports and configuration records for such email senders. In addition, marketing emails with opt-out provisions will not be counted towards the False Positive Rate.

The following conditions also apply:

- SenderBase reputation filters must be enabled at default levels or more conservatively,
- You must have the reputation messages per connection multiplier set to the default value;
- You must have IronPort Anti-Spam (IPAS) block settings at the default value or more conservatively;
- You must have IronPort Anti-Spam quarantine enabled with settings at default or more conservatively;
- You must have SenderBase Network Participation enabled;
- You must provide copies of false positive messages to Cisco;
- You must provide the domains covered by CES, the number of mailboxes and the incoming mail report for the last thirty (30) days; and
- You must only enable IPAS for spam scanning to qualify.

Failure to comply with any of the above conditions will eliminate Your right to receive a Service Credit.

Remedy
If You experience a False Positive Rate Infraction, and subject to the exceptions set forth above and the General Exceptions, then You will be entitled to the applicable Service

Credit set forth in the table below.

False Positives During a Month	Service Credit as a % of Monthly Fee
> 1 in 1 Million	20%
> 1 in 100 Thousand	40%
> 1 in 1 Thousand	100%

Virus Catch Rate Service Level Agreement**.** CES will detect and stop one hundred percent (100%) of all Known Viruses that are routed through CES within thirty (30) minutes of when the applicable anti-virus provider releases a signature for the platform (the "***Virus Catch Rate***").

Exceptions and Conditions
Messages that contain a URL to a website hosting malware and Virus attachments that are password protected are not included in the Virus Catch Rate.
The following conditions also apply:

- You must have SenderBase reputation filters enabled at a default level or more aggressively;
- SenderBase Network Participation must be enabled;
- You must provide all samples of missed Viruses to Cisco,
- You must ensure that the message was scanned by the anti-virus engine (e.g. message did not exceed the maximum scanning size limit); and
- You must provide the domains covered by CES, the number of mailboxes and the incoming mail report for the last thirty (30) days.

Failure to comply with any of the above conditions will eliminate Your right to receive a Service Credit.

Remedy
If You experience a Virus Catch Rate Infraction, and subject the exception set forth above and the General Exceptions, then You will be entitled to the applicable Service Credit set forth in the table below.

Virus Catch Rate During a Month	Service Credit as a % of Monthly Fee
< 100%	20%
< 99%	40%
< 95%	100%

CRES Uptime Service Level Agreement**.** CRES will be Operational at least 99.999% of the time during each calendar month, excluding maintenance windows. For the purposes of this section, "***Operational***" means that You will have access to CRES for the purposes of: (1) encrypting emails; (2) enabling secure envelope recipient actions (e.g. opening, secure reply, secure forward, and/or forwarding to mobile@res.cisco.com); and (3) CRES user account access. CRES uptime is determined by dividing the total number of minutes CRES was Operational divided by the number of minutes in that calendar month. Consequently, an Infraction is a minimum of thirty (30) seconds of CRES downtime. CRES uptime is determined and validated by an industry-recognized third-party monitoring service that performs service-level checks from various locations on the Internet.

Exceptions
This Service Level Agreement excludes any downtime resulting from Your administrator account access.

Remedy

If You experiences a downtime Infraction, and subject to the exception above and the General Exceptions, You will be entitled to the applicable Service Credit set forth in the table below.

Monthly Service Availability	**Service Credit as a % of Monthly Fee**
< 99.999%	20%
< 99.0%	40%
< 98.0%	100%

General Service Level Agreement Conditions**.** All remedies for Service Credits referred to above are conditioned upon Your (1) payment of all applicable fees, (2) fulfillment all of Your obligations under this Offer Description, and (3) Your submission of a claim in accordance with the SLA Claim Procedure below. If You have earned a Service Credit but have prepaid for a subscription in full and You do not renew such subscription, then all such earned Service Credits will be forfeited and no refund will be provided.

Service Credits do not apply as a result of CES not meeting a particular SLA due to any of the following ("**General Exceptions**"):

- Hardware or software upgrades, facility upgrades, or other similar Customer-led network interruptions requested by You;
- A scheduled maintenance period that was announced at least 24 hours in advance;
- Hardware, software or other data center equipment or services not in the control of Cisco or within the scope of CES;
- Hardware or software configuration changes made by You;
- Denial of CES attacks on the installed email security infrastructure or ancillary services such as SenderBase; or
- Events outside of Cisco's reasonable control, including without limitation acts of God, earthquake, labor disputes, industry wide shortages of supplies, actions of governmental entities, riots, war, terrorism, fire, epidemics, or delays of common carriers.

SLA Claim Procedure**.** You must submit a claim for a Service Credit within thirty (30) calendar days of the claimed Infraction. Each claim must be supported with evidence from message logs, sample messages, support ticket numbers, ping or trace route data, reporting data or other applicable method for documenting the occurrence and duration of the claimed Infraction. You must certify that (1) no changes or actions initiated by You were responsible for the occurrence resulting in the claimed Infraction, and (2) You did not ignore warnings by Cisco of certain behavior that is responsible for such occurrence—including but not limited to, the presence of a mail loop due to configuration within or external to CES; creating a policy bypass around anti-spam policies in the policy configuration; creating a policy bypass around anti-virus filtering in the configuration; or misconfiguration of an encryption profile or failure to permit upgrade of the PXE-SDK or software version of CES. You must submit all claims for Service Credits via a support ticket. Cisco will evaluate the claim, respond within forty-eight (48) regarding the validity of the claim, and, if applicable, provide Service Credits under the applicable remedy section within thirty (30) days following such response.

Cisco Defense Orchestrator ("CDO")

Description. CDO is a cloud-based security policy management application that allows the user to manage multiple Cisco security products with the following functionalities: policy change management, policy analysis and optimization, policy monitoring and reporting, and orchestration

of policy changes. Please consult the CDO Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

Cisco Umbrella

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 data can be accessed via a web-based console or an API. Cisco Umbrella includes various license options including Roaming, Branch, Professional, Insights, Platform and Investigate and WLAN. Please consult the Umbrella Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

Supplemental Terms.

Service Availability Commitment. 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 Service 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.

Umbrella Scheduled Maintenance. In all cases where scheduled maintenance for Cisco Umbrella Service will be performed, Cisco will make reasonable attempts to ensure that scheduled maintenance that affects the availability of Cisco Umbrella Service for more than thirty (30) minutes is performed between 12:00 AM and 5:00 AM Pacific Time, Monday through Friday

(excluding U.S. holidays), or between 12:00 PM and 5:00 AM Pacific Time on Saturday, Sunday and U.S. holidays.

Technical Support Level Descriptions. Technical support for Cisco Umbrella will be provided in accordance with the applicable Technical Support Level and Priority/Response Targets set forth below:

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)

Priority Levels and Response Targets.

Support Priority	**Response Target**	**Description**
P1: Outage (as defined above)	--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 Cisco Umbrella 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 Your ability to use Cisco Umbrella. 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 Cloudlock

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 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 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**"): Certain Cisco Cloudlock applications enable discovery of cloud applications connected to Your corporate environment, 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.

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 Cloudlock Documentation for further information on its technical specifications, features and functionalities.

Supplemental Terms.

Definitions. Additional Cisco Cloudlock defined terms are set forth in **Appendix B**.

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.

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.

Usage Limits. The following limitations apply to Your use of Cisco Cloudlock:

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 Cloudlock conducts an annual SOC II Type II or higher security audit 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.

Cloudlock Use of Customer Data. 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. In addition, use of Cisco Cloudlock requires automated scans of Customer Data as part of its functionality; you acknowledge and consent to such scans of Customer Data as part of Your use of Cisco Cloudlock.

Data Storage. Except for Cisco Cloudlock Metadata, You retain control of the Customer Data and are responsible for backing up the Customer Data. **Cisco Cloudlock will not store any Customer Data except to the extent that it constitutes Cisco Cloudlock Metadata.**

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.

Technical Level Descriptions. Technical support for Cisco Cloudlock will be provided in accordance with the following Technical Support Level and Priority/Response Targets:

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)

Priority Levels and Response Targets.

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 Your ability to use Cisco Cloudlock. Cisco will work on the

Support Priority	Response Target	Description
		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.

[Appendices Follow]

Appendix A

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.

"**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.

"Effective Megaflows" means the lines of flow log data generated by the Stealthwatch Cloud monitored environment and processed by Cisco.

"**Endpoint**" means any device capable of processing data and that can access a network, including but not limited to personal computers, mobile devices, iOS devices and network computer workstations.

"**Files**" mean those types of files identified in the applicable Documentation, such as an executable, Portable Document Format (PDF), Microsoft Office Documents (MS Word, MS Excel, MS PowerPoint), and those files in a ZIP file (.ZIP).

"**Network Data**" means Telemetry Data (as defined in the Agreement), plus any technical data and related information about Your computer network generated as part of Your usage of a Cloud Service including, but not limited to the operating system type and version; file metadata and identifiers such as SHA-256 values; network host data; origin and nature of malware; Endpoint GUIDs (globally unique identifiers); Internet Protocol (IP) addresses; MAC addresses; log files; web proxy logs; configuration files; network configurations; 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; and any aggregate, demographic or network traffic data such as cookies, web logs, web beacons, and other similar applications.

"**Non-Confidential File(s)**" a File submitted to AMP Threat Grid that You do not elect to maintain as "private" and thus can be viewed by other users of AMP Threat Grid.

"**Private File(s)**" a File submitted to AMP Threat Grid that You elect to maintain as "private" so that it can't be viewed by other users of AMP Threat Grid.

"**Statistical Data**" means any information/data that Cisco derives from Customer Data, Network Data and/or Cisco Cloudlock Metadata provided that such information/data is aggregated and/or de-identified such that it cannot reasonably be used to identify an individual or Your entity.

*****

Appendix B

Cloudlock Definitions

The following definitions apply only to Cisco Cloudlock and Your Cisco Cloudlock Order and govern in the event of a conflict with the Agreement or **Appendix A** to this Offer Description:

"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 Cloudlock 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 Cloudlock 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.

"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(s)).

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

"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.

"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.

"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. For purposes of the Cisco Cloudlock for AWS Console service, "User" refers to the administrative user who is authorized to access the AWS

Console, including root, IAM and federated users (i.e. users external to AWS who are authorized to access the AWS Console). Such AWS Users have a unique identity recognized by the AWS services and applications, and may be an individual, system or application.

*****