Offer Description
for
AMP, Threat Grid, Clarity, Cognitive Intelligence, CTR, Stealthwatch Cloud, CDO, Umbrella, Cloudlock, CES, CRES, DMP, and APP

OVERVIEW

This Offer Description describes the following security Cloud Services:

- Cisco Advanced Malware Protection (AMP)
- Cisco AMP Threat Grid
- Cisco Clarity
- Cisco Cognitive Intelligence (f/k/a Cognitive Threat Analytics)
- Cisco Threat Response (CTR)
- Cisco Stealthwatch Cloud
- Cisco Defense Orchestrator (CDO)
- Cisco Umbrella
- Cisco Cloudlock
- Cisco Cloud Email Security (CES) and Cisco Registered Envelope Service (CRES)
- Cisco Domain Protection (DMP) and Cisco Advanced Phishing Protection (APP)

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** 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 and Maintenance and Updates. Please see **Appendix B** for information regarding Technical Support, Maintenance and Updates.

B. 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.

C. 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.

D. 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.

E. Privacy. Cisco's data privacy obligations related to data processed to deliver the Cloud Services are governed by the Agreement which includes the Cisco Privacy Statement available at https://www.cisco.com/c/en/us/about/legal/privacy-full.html Additionally, the applicable Privacy Data Sheet available https://www.cisco.com/c/en/us/about/trust-center/solutions-privacy-data-sheets.html supplements the Cisco Privacy Statement and describes the personal data that Cisco collects and processes as part of the delivery of a Cloud Service to You (the "Data Sheets"). We may update the Data Sheets from time to time. If we modify our Data Sheets, we will post the revised version Privacy Data Sheet link above, with an updated revision date. You agree to visit these pages periodically to be aware of and review any such revisions. If we make material changes to our Data Sheets, we may also notify you by other means prior to the changes taking effect, such as by posting a notice on our websites or sending you a notification.

F. Restrictions. (a)You may use the Cloud Service for Your own internal business purposes and shall not outsource, sublicense, resell, lease, transfer or otherwise allow use of the Cloud Service for the benefit of any third party; except to the extent You are an authorized Cisco service provider whose contract with Cisco authorizes You to utilize Cisco cloud services on behalf of end customers (in which case You may use the Cloud Service only for the benefit of such end customers); and (b) You shall not (i) create derivative works based on the Cloud Service, or cause or permit others to; (ii) modify, reverse engineer, translate, disassemble, or decompile the Cloud Service, or cause or permit others to; (iii) access the Cloud Service in order to build a competitive product or service; or (iv) access the Cloud Service in order to infringe or misappropriate any intellectual property included in the Cloud Service. You will promptly notify Cisco of any unauthorized access or use of the Cloud Service.

G. 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.

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.

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

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

Description. Clarity is a cloud-based security solution that provides visibility and protection against advanced malicious threats on iOS devices. 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 Intelligence

Description. Cognitive Intelligence 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. Cognitive Intelligence 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 Cognitive IntelligenceDocumentation for further information on its technical specifications, configuration requirements, features and functionalities.

Supplemental Terms.

Proxy Log and NetFlow Submissions. To use Cognitive Intelligence, You are required to submit web proxy logs from a supported platform and/or NetFlow from Cisco Stealthwatch. Such logs may contain identifiable data such as user name, machine name, IP address, and browsing information. Cognitive Intelligence 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 Cognitive Intelligence cloud to have the ability to analyze for active malware inside Your environment, then You must not enable Cognitive Intelligence.

Cisco Threat Response ("CTR")

CTR is a cloud based aggregator of threat intelligence available from certain Cisco security products, as well as other third party security products. CTR allows You to pull together critical threat intelligence and add context from Your organization so You know which systems and devices are infected. Please consult the CTR Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

Cisco Stealthwatch Cloud

Description. Stealthwatch Cloud is a cloud security service that performs behavior anomaly detection on network connected devices and users in the data center and/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 and identify policy violations, misconfigured cloud assets and user error and misuse. 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.

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's 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 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.

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 four use cases:

- Data Loss Prevention ("**DLP**"): Cisco Cloudlock provides DLP functionality that monitors cloud environments to detect and secure sensitive information through out-of-the-box policies as well as highly-tunable custom policies. Automated response actions can remediate risk in the instance of policy violation, including but not limited to, end-user notifications, transfer of ownership, and quarantines.

- User and Entity Behavior Analytics ("**UEBA**"): Cisco Cloudlock provides cross-platform UEBA functionality for cloud application environments. Cisco Cloudlock leverages advanced machine learning algorithms to detect anomalies based on factors such as activities outside of whitelisted countries and actions across distances.

- Apps Firewall ("**Apps Firewall**"): Certain Cisco Cloudlock applications enable discovery of cloud applications connected to Your corporate environment via an Oauth connection, and provide a crowd-sourced Community Trust Rating for individual applications, as well as the ability to ban or whitelist them based on risk profile and access scope, increase employee awareness with email alerts, and revoke application use in bulk across the entire user base.

- App Discovery ("**App Discovery**"): App Discovery is an optional add-on service that provides visibility into cloud applications (SaaS, PaaS, Iaas) used or visited by individuals through a customer's network (applications accessed outside of an OAuth connection) via the then current supported data sources.

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

Supplemental Terms.

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.

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

Application Programming Interfaces (APIs). APIs supplied or made accessible through Cisco Cloudlock are subject to change and You assume the associated risks of using API's for development purposes if You elect to do so. All such APIs are provided on an AS-IS basis.

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.

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. CES is licensed based on the quantity of Users. Users means the employees, contractors and other agents authorized by You to use email services via Your email and Internet services.

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 capacity 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 a virus 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.

The Service Credits available to You under the CES and/or CRES SLA's are Your sole and exclusive remedy for Cisco's failure to meet the applicable SLA.

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) hours 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 Domain Protection ("DMP") and Cisco Advanced Phishing Protection ("APP")

Descriptions.

Cisco Domain Protection for external email helps prevent phishing emails from being sent using a customer domain(s). The Cisco Domain Protection service automates the process of implementing the email authentication standard Domain Message Authentication Reporting & Conformance (DMARC) to better protect employees, customers and suppliers from phishing attacks using a customer domain(s). This protects the customers' brand identity as well as increases email marketing effectiveness by reducing phishing messages from reaching inboxes. Please consult the Cisco Domain Protection Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

Cisco Advanced Phishing Protection stops identity deception based attacks such as social engineering, impostors and business email compromise (BEC) and provides local email intelligence and advanced machine learning techniques to model trusted email behavior on the internet, within organizations and between individuals. Cisco Advanced Phishing protection integrates Machine Learning techniques to drive daily model updates, maintaining a real-time understanding of email behavior to stop identity deception. Please consult the Cisco Advance Phishing Protection Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

Supplemental Terms:

Your Responsibilities**.**
You must supply Cisco with all technical data and other information Cisco may reasonably request to allow Cisco to supply DMP and APP to You. Cisco cannot make DMP or APP available unless we receive all required information. DMP and APP are delivered on a co-managed model. You are responsible for configuring the Cloud Service 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.

Use Limitations.
DMP and APP are licensed based on the quantity of Users. Users means the employees, contractors and other agents authorized by You to access the Internet or use email services via Your email and Internet services.

Additional Data Usage Acknowledgement for Cisco Domain Protection.
In connection with Your use of DMP, You can, at your discretion, publish a DMARC policy via your own DNS infrastructure. This policy instructs email service providers ("ESPs") to send numerical summaries to the Cloud Service about messages which have been processed and which appear to come from Your domains. You may also request that these ESPs send examples of messages failing email authentication to the Cloud Service. Some ESPs provide only redacted message samples containing the sender's email address, the message subject, URLs, and SMTP headers. Other ESPs may send the full content of the messages failing authentication in the failure sample feed, but in such cases the Cloud Service retains only the header information referenced in the preceding sentence above. In most cases, these failure examples originate from fraudulent senders and the URLs and attachments contain malware or link to fraudulent web sites. The details from these failure examples are shared only with You and are retained by the Cloud Service for no more than 14 days, at which time they are deleted following the then current Amazon Web Services best practices. Cisco and/or its applicable subprocessors and subcontractor(s) may use this Customer Data relating to emails that fail authentication ("Authentication Failure Data") in order to provide the Cloud Service and as otherwise authorized under the Agreement and this Offer Description. Without limiting rights otherwise set forth in the Agreement and this Offer Description, Cisco (and its subprocessor(s)) may compile, aggregate, publish, use and share anonymized summaries of such Authentication Failure Data both during and after the subscription term to determine and report Cloud Service usage patterns, to analyze and report security related issues and trends, and to improve upon and create new products and service offerings. You further acknowledge that, notwithstanding anything to the contrary herein or in the Agreement, Cisco (and its subprocessors and subcontractors involved in the delivery of the Cloud Service) may license and provide such aggregated and anonymized summary data (excluding Your Confidential Information and any personally identifiable information (if any is actually received)) to its or their licensees for their internal use in doing the same, both during and after the term of this Agreement. For clarity, no customer Confidential Information will be disclosed, published or shared with any third party. To the extent You may have any rights in or to any Authentication Failure Data, You hereby provide Cisco (and its subprocessors and subcontractors involved in the delivery of the Cloud Service) a perpetual, royalty-free, transferable license to do all of the foregoing. This paragraph will survive the expiration or termination of the Agreement.

Service Availability Commitment ("Availability SLA"):

1.0 Service Availability Definitions and Process

1.1 Definitions.

1.1.1 "Emergency Maintenance" means any time outside of the Scheduled Maintenance Window that Cisco is required to apply urgent patches or fixes, or undertake other urgent maintenance activities.

1.1.2 "Infraction" is a single instance of unavailability in accordance with the specific calculation set forth in this Availability SLA. Separate downtime occurrences cannot be aggregated for purposes of determining an Infraction has occurred.

1.1.3 “Scheduled Maintenance Window" means the window during which weekly scheduled maintenance (“Scheduled Maintenance”) of the Cloud Service may be. The Scheduled Maintenance Window is between the hours of Friday 9:00 p.m. to Saturday 5:00 a.m. Pacific time.

1.1.4 "Service Availability" means the percentage of total time during which the Cloud Service (including but not limited to the Cloud Service portal) is available to You and operating properly without material degradation of service, excluding up to thirty minutes per month for Scheduled Maintenance and Emergency Maintenance. “Available” in this context means You may log in, view data, create reports, modify settings and similar, and substantially all licensed components, including but not limited to hosted sensors (if applicable) and the Cloud Service portal, are functioning properly.

1.2 Service Credits

1.2.1 “Service Credit” means the percentage of the Calculated Monthly Fees paid that is awarded You for validated claim(s) associated with that portion of the Cloud Service related to breach of this Service Availability SLA during that month (see below for applicable percentages). The “Calculated Monthly Fee” is defined as fees received for Your annual subscription for the Cloud Service divided by 12. “Service Credits*”* are Your sole and exclusive remedy for any failure to achieve the Availability SLA. 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.

1.2.2 In any given month You shall in no event be entitled to receive a credit that exceeds 100% of the Calculated Monthly Fee for the nonconforming service.

1.2.3 Any Service Credits earned by You hereunder will be applied to the royalty fees owed by Cisco for the next royalty payment period.

1.3 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. You must submit all claims for Service Credits via a support ticket. Cisco will evaluate the claim, respond as soon as reasonably possible regarding the validity of the claim, and, if applicable, provide Service Credits under the applicable remedy section within thirty (30) days following such response.

1.4 Exclusions. Service Credits do not apply as a result of not meeting the Availability SLA due to any of the following (“**General Exceptions**”):

- Use of the Cloud Service outside the scope described in the Agreement or this Offer Description.

- 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 the Cloud Service;
- Hardware or software configuration changes made by You or Your failure to meet the configuration requirements set forth in the Documentation for this Cloud Service;
- Denial of service 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.

2.0 Availability SLA Percentage and Credits. The following SLA applies to the Cloud Service:

2.1 Cisco will provide at least 99.999% Service Availability for the Cloud Service (including but not limited to the portal, hosted sensors (if applicable) and other licensed components) during each calendar month, excluding up to thirty (30) minutes per month for Scheduled Maintenance and Emergency Maintenance. Service Availability is calculated as follows:

Availability = (X/Y) x 100, where

X = the total number of minutes of Service Availability (as defined above), and

Y = (the Total number of minutes in the calendar month) – (the Total # of minutes of downtime from Scheduled Maintenance and Emergency Maintenance which shall not exceed thirty (30) minutes).

2.2 If the Service Availability is less than 99.999%, Cisco will provide You with a Service Credit for the month in which the failure to meet the Availability SLA has occurred. The Service Credit will be calculated in accordance with the table below.

% of Service Availability per Calendar Month	Service Credit
< 99.999%	20%
< 99.0%	40%
< 98.0%	100%

[Appendix Follows]

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 one million optimized log lines 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).

“NetFlow” means IP network traffic data (e.g. IP source address, IP destination address, source port, and destination port).

“**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 and Telemetry Data provided that such information/data is aggregated, anonymized and/or de-identified such that it cannot reasonably be used to identify an individual or Your entity.

“Telemetry Data” means information generated by instrumentation and logging systems created through the use and operation of the Cloud Service and/or Cisco products and, for purposes of this Offer Description, includes, by way of example: 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.

Appendix B

Technical Support, Maintenance and Updates

Technical Support

Technical Support.

Cisco will provide You with technical support for the Cloud Services. For each Cloud Service, a specific support option is embedded but other levels of support may also be available. See Table 1 for the potential support options and applicable targeted response times. The Basic Option with Phone Support is the default support level unless a different support option is identified on the Order or below. You may purchase any additional support option to the extent available for the applicable Cloud Service. Support options for Cisco Cloudlock and Cisco Umbrella are separate and are listed and described in Tables 2 and 3 below.

Response time is defined as the time between case submission in the case management system to support engineer contact. The table below outlines Cisco's response objectives based on case severity with respect to submitted cases. Cisco may adjust assigned case severity to align with the Severity as defined herein.

Table 1

Support Service	Technical Support Coverage	Response Time Objective for Case Severity 1 or 2	Response Time Objective for Case Severity 3 or 4
Premium	24x7 via Phone & Web	Response within 15 minutes	Response within 1 hour
Enhanced	24x7 via Phone & Web	Response within 30 minutes	Response within 2 hours
Basic with Phone Support	24x7 via Phone & Web	Response with 1 hour	Response within one Business Day
Basic with Online Support*	Web only	Severity is not required to be specified. Response to all cases within next Business Day during local Standard Business Hours.	

*Stealthwatch Cloud embedded support is Basic with web only.

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.

Severity 1 means the Cloud Service 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 the Cloud Service 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 the Cloud Service 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 Cloud Service. 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.

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**.**

Technical Support for Cisco Umbrella and Cisco Cloudlock.

Technical support for Cisco Umbrella and Cisco Cloudlock will be provided in accordance with the applicable Technical Support Level and Priority/Response Targets set forth below. The embedded support option for these two Cloud Services is the Basic level described below:

Table 2

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)

*Not available for Cisco Cloudlock

Table 3

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.

Support Priority	Response Target	Description
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.

Maintenance and Updates

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.

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

Your access to and use of the Cloud Services 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.

*****