Service Description: Cisco Cloud Web Security Service

This document sets out the features and functionality of the Cisco Cloud Web Security Service (the "Service"). Depending on whether you have purchased the Essentials version or the Premium version of the Service, not all features may be available (as indicated in Section 3 below).

If you have purchased the Service via an authorized Cisco partner, this document is for description purposes only; and the contract, if any, governing the provision of the Service will be the one between you and your authorized Cisco partner. Your authorized Cisco partner should provide this document to you, or you can obtain a copy of this service description at: www.cisco.com/legal/services.html

Capitalized terms are defined in the Glossary of Terms at the end of this document.

1. Overview

1.1 Cisco Cloud Web Security is delivered through hardware and software deployed in Cisco managed data centers. Cisco will retain ownership, as applicable, of all hardware infrastructure used in its data centers as part of providing the Service.

1.2 The Service does not include Customer's access connection to the Internet or any equipment necessary for Customer to make such connection, which are Customer's sole responsibility.

1.3 Services that are not expressly set forth in this Service Description are not covered, including, without limitation, the following:

a) Any customization of, or labor to install, Software and Hardware.

b) Any expenses incurred to visit Customer's location, except as required during escalation of problems by Cisco.

c) Services or software to resolve Software or Hardware problems resulting from third party product or causes beyond Cisco's control or failure by Customer to perform its responsibilities set out in this Service Description.

d) Services for non-Cisco products used in connection with the Service.

1.4 Certain deployment options may involve the Customer downloading and installing Cisco Software (e.g. the Connector or AnyConnect Software as described below). The use of such Software is governed by separate end user license agreements which will be made available at the time of Software download. Except as provided in such agreements, Software entitlement, including media, documentation, binary code, source code or access in electronic or other form is not provided.

2. Cisco Responsibilities

2.1 As long as Customer has paid all applicable fees, Cisco will:

a) Provide the Service as ordered by the Customer;

b) Provide all Updates and Releases commercially released by Cisco; and

c) Use its reasonable commercial endeavors to resolve technical problems identified within the Service. Cisco does not provide technical support for any third-party hardware or software not purchased and/or authorized by Cisco.

3. Functionality

3.1 The Essentials version of the Service comprises Web Malware Scanning and Web Filtering. The Premium version of the Service also includes Advanced Malware Protection and Cognitive Threat Analytics. The functionality of the Service is described below.

3.2 The Customer's external HTTP, HTTPS and FTP over HTTP requests (including all attachments, macros or executables) are directed through the Service. The configuration settings required to direct this external traffic via the Service are made and maintained by the Customer (with assistance and support from Cisco as reasonably required) and are dependent on the Customer's technical infrastructure. The Customer should ensure that internal HTTP/HTTPS/FTP over HTTP traffic (e.g. to the corporate intranet) is not directed via the Service.

Web Malware Scanning ("MS")

3.3 Once the relevant configuration changes are made, unencrypted Web pages and attachments will be scanned by Outbreak Intelligence™, a proprietary security platform that detects malware threats by using a combination of multiple, correlated detection technologies, including industry leading anti-malware engines.

3.4 MS will scan as much of the Web page and its attachments as possible. It may not be possible to scan certain Web pages or attachments (for example, password protected). Unscannable attachments will be blocked. Encrypted traffic (i.e. HTTPS/SSL) cannot be scanned and will be passed through MS unscanned (unless HTTPS Inspection is enabled as described in paragraph 3 below).

3.5 If a requested Web page or attachment is found to contain malware (or deemed unscannable in accordance with paragraph 3.4, except for SSL traffic), then access to that Web page or attachment is denied and the user will be displayed an automatic alert Web page. Notification may also be sent by email to a customer administrator.

Web Filtering ("WF")

3.6 Once the relevant configuration changes are made, Web pages and attachments will be filtered using industry leading URL categorization and content analysis. URLs are categorized by reference to a number of predefined categories as specified in the Portal (see below).

3.7 The Customer can configure WF to create access restriction policies (based both on categories and types of content) and deploy these at specific times to specific Internet users or groups. A number of additional features (for example, 'blocked' and 'allowed' list functionality) are also available.

3.8 WF will filter as much of the Web page and its attachments as possible. It may not be possible to filter certain Web pages or attachments (for example, password protected). The Customer may also configure specific exceptions for web sites that should not be filtered. Encrypted traffic (i.e. HTTPS/SSL) cannot be filtered and will be passed through WF unless otherwise specified by the Customer in relation to specific categories of content. WF will only filter Web pages that are categorized by WF in accordance with the category that the Customer has chosen to filter.

3.9 The Customer can use individual and/or group administration and reporting capabilities by utilizing the optional Connector software described below.

3.10 If a user requests a Web page or attachment where an access restriction policy applies, then access to that Web page or attachment is denied and the user will be displayed an automatic alert Web page. Notification may also be sent by email to a customer administrator.

HTTPS Inspection

3.11 Where enabled, HTTPS Inspection allows the administrator to set a policy determining which domains and categories of HTTPS traffic are decrypted and inspected on the scanning infrastructure. Data is encrypted from the Web server to the scanning tower in the normal way; however, for sites which the customer wishes to be inspected, the scanning tower will terminate the SSL-based connection, inspect the data in the same way as for HTTP traffic, and then re-encrypt the traffic from the scanning towers to the end user using a different certificate. The corresponding certificate authority will need to be rolled out to the Customer's Web browsers as a trusted certificate authority to prevent domain mismatch warnings appearing to end users. HTTPS Inspection can be used for both malware detection and enhanced Web filtering actions such as Outbound Content Control.

Outbound Content Control

3.12 Outbound Content Control gives Web filtering Customers the flexibility to define rules based on the HTTP protocol's POST function. These filters look for specific files with certain characteristics (e.g. MD5 or SHA1 checksums), keyword analysis, outbound file types, preconfigured IDs (e.g. credit card numbers or social security numbers) and DFA-based regular expressions.

Block Alert Pages

3.13 Block alert pages are dynamically generated HTML pages displayed to end users when they are prevented from accessing prohibited Web content. The Customer can choose a standard block alert page or customized content which can be uploaded via the Portal (see below). Cisco will host the blocked pages.

Connector

3.14 If ordered by the Customer, Cisco will provide the Connector software for the Customer to install in its network in accordance with Cisco's installation guidelines. The Connector does not support all potential customer systems and set-ups.

3.15 The Connector enables users to connect to the Service even without a static IP address by using an authentication key. If users have other services that rely on a fixed IP address for identification, they can configure direct connections for specific websites, domains, hosts or networks.

3.16 Administrators can create, revoke, activate, and deactivate authentication keys for Connectors per group or per users.

Cisco AnyConnect (Secure Mobility)

3.17 If ordered by the Customer, Cisco will provide the AnyConnect software for the Customer to install on its end users' PCs or laptops in accordance with Cisco's installation guidelines. AnyConnect does not support all potential customer setups.

3.18 AnyConnect allows the end user's PC or laptop to connect to the Service from a remote location outside the customer's internal network. It does not rely on provisioned IP addresses.

Advanced Malware Protection (AMP)

3.19 Advanced Malware Protection (AMP) is included with the Premium Service and may be ordered separately by Customers of the Essentials Service. If ordered by the Customer, Cisco will provide AMP technology to the Customer for performing file analysis at the gateway to detect malware threats. This functionality augments the anti-malware detection and blocking capabilities offered by Web Malware Scanning.

3.20 Cryptographic hashes of files are collected and transmitted to a Cisco-managed cloud server where analysis is performed and a disposition is made whether the file is malicious, neutral or unknown.

3.21 If a disposition is unable to be made after the analysis of the hash of a file, the Customer has the additional ability to submit the file to a separate cloud-based sandbox managed by Cisco for further analysis. The Customer can configure AMP to limit the type of files sent to the sandbox.

3.22 After the file analysis is completed, reputation reporting, file behavior reporting and retrospective verdict alerting are accessible from the Portal.

Cognitive Threat Analytics

3.23 Cognitive Threat Analytics (CTA) is included with the Premium Service and may be ordered by Customers, together with AMP, as an upgrade to the Essentials Service. If included in the Service ordered by the Customer, CTA performs a behavioral analysis of the web logs generated by the Service and identifies anomalous traffic that indicates possible malware infections, malicious activity, or policy violations on the Customer network ("Incidents"). CTA generates Incident reports for the Customer on the Portal. The CTA Incident report lists Incidents that indicate possibly infected hosts on the Customer network that communicate through the Service.

3.24 Cisco does not guarantee the availability of Portal reports or that CTA will accurately identify or report Incidents. Detection and reporting of Incidents is subject to the Customer's network environment and many other factors outside Cisco's control.

3.25 The Customer is responsible for investigating and/or mitigating Incidents reported by CTA to Customer, and Cisco is not responsible for any investigation and/or mitigation of Incidents.

3.26 To effectively enable CTA, the Customer is responsible for configuring its network traffic so each individual end user is identifiable by a separate and unique user identity. The Customer should ensure that multiple users are not represented under the same user identity. If separate and unique user identities are not available, CTA behavioral analysis will be based on client IP address and may not generate accurate Incident reports.

Portal

3.27 The Customer will be provided access to a Web-based portal, hosted by Cisco, to administer and report on the Service. Access to the Portal is via a secure (HTTPS) website and is password-protected.

3.28 The Customer may have multiple administrators for a single account. The Customer can give each administrator a unique login and provide full access or read only privileges specific to each user. This functionality allows a unique, single "Super User" account that can create multiple administrators.

3.29 The Portal enables the customer administrator to:

a) review statistics of all malware stopped and other Web content blocked;

b) generate reports in relation to the AMP and CTA elements of the Service (if applicable);

c) create access restrictions and apply these to specific users or groups (if the Connector software has been installed);

d) customize browser alert pages seen by users when access to a particular website or file is denied;

e) update administration details for real-time email alerts; and

f) configure and schedule automated system auditing and reporting.

3.30 Automated reports are available on overall traffic, bandwidth, blocked URLs, malicious files and Web malware stopped. The Portal also offers a comprehensive selection of additional reports, generated daily, which provide in-depth analysis in the form of graphs, tables, and exportable data files. The Customer can

schedule regular reports for different service functionality and specify users, times, and email it to certain users or groups.

3.31 Audit Logging functionality records administration, configuration, filtering, and policy changes made for the Service, and can be configured by full access administrators or the Super User. Auditing includes who made the change, what was changed, and when it was changed. Audit logs can be searched by specifying a time period, category or type of logs, and type of action taken.

3.32 Privacy Logging functionality, when enabled, will log when web pages are blocked according to web filtering policy, but will obfuscate private details such as source username and IP address. This feature is for customers who must comply with local privacy policies or regulations.

3.33 The Log Extraction API allows Customers to automatically pull web usage data quickly and securely for analysis using an S3 compatible HTTPS API. The log data is compiled in W3C text format that can be correlated with existing data using a variety of reporting and analysis tools such as SIEM.

4. Maintenance and updates

4.1 From time to time, Cisco performs scheduled maintenance, to update the servers and software that are used to provide the Service. Cisco will make all reasonable attempts to notify Customer at least five business days in advance of any planned downtime or scheduled maintenance. Notwithstanding the foregoing, Customer acknowledges that Cisco may, in certain situations, need to perform emergency maintenance without providing advance notice.

4.2 Cisco reserves the right to modify and update the features and functionality of the Services, at no additional cost to Customer, with the objective of providing Customer with equal or enhanced Services. These updates shall include any subsequent release or version of the Services containing functional enhancements, extensions, error corrections or fixes which are generally made available free of charge to customers who have contracted for the appropriate level of Services. Updates shall not include any release, option or future product which Cisco licenses separately or which is not included under the applicable level of support.

4.3 Cisco will give Customer prior written notice of any material modification or update. Cisco will use reasonable efforts to ensure that any modifications or updates do not materially degrade the performance of the Services or Customer's use of the Services. Cisco will ensure that any modifications or updates do not require Customer to incur any material additional cost to continue its use of the Services.

4.4 Cisco will use reasonable efforts to implement modifications or updates in a manner that minimizes the impact on Customer's use of the Services. Cisco will give Customer at least seven days' notice of planned maintenance. Wherever possible, planned maintenance is carried out at weekends or between 8 p.m. and 8 a.m. (customer local time). Cisco may need to carry out emergency maintenance at other times in the event of an emergency (without prejudice to Section 10).

5. Pricing Conditions

5.1 The Customer must notify Cisco within 14 days if the number of Seats increases by more than 5% of the then declared number of Seats. Cisco reserves the right to require the Customer to purchase additional Seats if the number of actual distinct users (as shown by Cisco's Web traffic logs) exceeds the number of licensed Seats from time to time.

5.2 Pricing is subject to the Customer's peak bandwidth per seat (the higher of inbound and outbound, measured on a 95th percentile basis) not exceeding an average of 15 kb/s in any calendar month. Charges will be increased pro rata if this level is exceeded for two or more calendar months. Cisco will notify the Customer if this level is exceeded in any one calendar month, such notification to be given within 10 business days after the end of such month.

5.3 Where the Customer has ordered the Service for wi-fi hotspots and pricing is thus based on the level of bandwidth rather than the number of Seats, the following provisions will apply:

a) The level of bandwidth utilized by the Customer will be determined using the following methodology:

b) Cisco will generate a monthly report (using the WIRe reporting tool) showing the average volume of data transmitted per second during each 5 minute interval within that month to or from the Customer's end users for each datacenter utilized by the Customer ('Traffic Sample').

c) Cisco will rank the Traffic Samples by size for each datacenter separately.

d) Cisco will disregard the highest 5% of all the Traffic Samples for each datacenter.

e) The level of traffic for each datacenter will be deemed to be the average rate of data transmitted during the next highest (i.e. 95th percentile) Traffic Sample divided by 300 (i.e. the number of seconds in 5 minutes).

f) The aggregate level of traffic will be deemed to be the sum of the 95th percentile figures for each datacenter.

g) Cisco will provide the Customer with details of the above reports and calculations in any calendar month, such notification to be given within 20 business days after the end of such month.

Based on such notification from Cisco, if during any calendar month the Customer's peak bandwidth exceeds the level of bandwidth previously ordered, the Customer must place a further order (at the same price per Mb/s) so that the total level of bandwidth ordered continues to be higher than the Customer's peak bandwidth (rounded up to the nearest 10 Mb/s).

6. Customer Responsibilities

6.1 Customer shall supply Cisco with all technical data and all other information Cisco may reasonably request from time to time to allow Cisco to supply the Service to the Customer, including a completed deployment questionnaire and site matrix.

6.2 Customer recognises that information sent to and from Customer will pass through Cisco's systems and accordingly Customer undertakes to comply with all relevant legislation applicable to its use of the Internet.

6.3 Customer is responsible for implementing and using strong passwords for accessing Cisco dedicated infrastructure and the associated support portal.

The following are common guidelines for choosing strong passwords. These are designed to make passwords less easily discovered by intelligent guessing:

- *Include numbers, symbols, upper and lowercase letters in passwords*
- *Password length should be around 12 to 14 characters*
- *Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, or biographical information (e.g., dates, ID numbers, ancestors' names or dates...)*

6.4 In providing the Service, Cisco may instruct the Customer to perform certain tasks or checks relating to Customer's network. Customer shall, at its expense, perform all such checks and tests. Customer will also provide Cisco, or its authorized representative, reasonable and free access to Customer's networking equipment. Customer shall not be required to furnish specialized equipment or know-how. Customer agrees to pay Cisco, at Cisco's then-current rates, plus any reasonable actual out-of-pocket expenses, for any rework or additional work resulting from modification of the Service requested by Customer (and accepted by Cisco) or any act or omission of Customer, including providing inaccurate information to Cisco. Cisco shall seek Customer's approval in advance of incurring such costs if it knows costs will be incurred as a result of such act or omission of Customer.

6.5 Customer is responsible for obtaining all approvals required by any third parties in order for Cisco to provide the Service. Cisco shall not be in default of its obligations to the extent it cannot provide the Service either because such approvals have not been obtained or any third party otherwise prevents Cisco from providing the Service.

6.6 Customer agrees that it shall not resell the Service or create or offer derivative versions of the Service either directly or through a third party.

6.7 Customer assumes full responsibility for the control and use of the data contained in any reports provided by Cisco hereunder. Customer acknowledges the potential privacy and other issues associated with the collection and use of this data.

6.8 Customer assumes full responsibility to back-up and/or otherwise protect all data against loss, damage, or destruction. Customer acknowledges that it has been advised to back-up and/or otherwise protect all data against loss, damage or destruction.

6.9 Customer shall comply with such laws and regulations governing use, export, re-export, and transfer of Cisco technology and will obtain all required U.S. and local authorizations, permits, or licenses.

6.10 The failure of Customer to comply with this Section may be deemed a material breach.

7. Data Privacy

7.1 Subject to the Cisco Privacy Statement at http://www.cisco.com/web/siteassets/legal/privacy_full.html or a successor site location, as the same may be amended from time to time by Cisco. Customer hereby consents and grants to Cisco a license to collect and use the data from the Customer as described in the Documentation, as the same may be updated from time to time by Cisco ("Data"). To the extent that reports or statistics are generated using the Data, they shall be disclosed to third parties only in the aggregate on an anonymized basis and no end user identifying information will be included with the Data, including without limitation user names, phone numbers, unobfuscated file names, email addresses, physical addresses and file content.

8. Licenses and Ownership

8.1 Subject to Customer's compliance with the terms of this Service Description, Cisco grants to Customer a worldwide, non-exclusive and non-transferable license to use, for Customer's internal business use only

and for the duration of the relevant purchase order: (i) the Service; (ii) other Deliverables specified in an applicable SOW, if any, and (iii) Data Collection Tools, if any (collectively and individually, the ***"Licensed Materials"***). These license grants do not include the right to sublicense; provided that Customer may permit its suppliers, subcontractors and other related third parties to use the Licensed Materials solely on Customer's behalf for Customer's benefit, provided that Customer ensures that any such use is subject to license restrictions and confidentiality obligations at least as protective of Cisco's rights in such Licensed Materials as are specified in this Service Description.

8.2 Except as otherwise expressly set forth in this Service Description, Customer shall not (and shall not permit a third party to): make error corrections or derivative works of, or otherwise modify, decompile, decrypt, reverse engineer, disassemble or otherwise reduce all or any portion of any Deliverable, Data Collection Tool or the Service to human-readable form; or transfer, sublicense, rent, lease, distribute, or sell, any Service, Deliverables or Data Collection Tools. Customer agrees that it receives no implied licenses under this Service Description, and all rights not expressly granted herein are reserved to Cisco.

8.3 Each party will retain the exclusive ownership of all its Pre-Existing Technology.

8.4 Except as otherwise expressly set forth in this Service Description, Cisco owns and will continue to own all right, title and interest in and to the Hardware, Service, Deliverables, Data Collection Tools, Reports, sketches, diagrams, text, know-how, concepts, proofs of concepts, artwork, software, algorithms, methods, processes, identifier codes or other technology provided or developed by Cisco (or a third party acting on Cisco's behalf) pursuant to this Service Description, including modifications, enhancements, improvements or derivative works of any of the foregoing, regardless of who first conceives or reduces to practice, and all Intellectual Property in any of the foregoing (collectively, "***Cisco Intellectual Property***").

8.5 As between Customer and Cisco, Customer shall at all times retain all right, title and interest in and to all of Customer's Pre-Existing Technology and all Intellectual Property that is developed by Customer or by a third party on Customer's behalf thereafter, other than Cisco Intellectual Property. Products supplied to Customer by any third party shall at all times be owned by the applicable third party, and will be subject to any applicable third party license terms.

8.6 Customer hereby grants to Cisco a perpetual, irrevocable, royalty free, worldwide right and license to all Intellectual Property in the Customer Feedback (as defined below) to use and incorporate Customer Feedback into any Service, Products, Deliverables, Data Collection Tools, Reports or Cisco Pre-Existing Technology, and to use, make, have made, offer to sell, sell, copy, distribute and create derivative works of such Customer Feedback for any and all purposes whatsoever, and Customer acknowledges and agrees that it will obtain no rights in or to any Service, Products, Deliverables, Data Collection Tools, Reports or Cisco Pre-Existing Technology as a result of Cisco's use of any such Customer Feedback. For purposes of this Service Description, "Customer Feedback" means all oral or written communications regarding improvements or changes to any Service, Products, Deliverables, Data Collection Tools, Reports or Cisco Pre-Existing Technology that Customer provides to Cisco.

9. Acceptable Use Policy

9.1 The Customer is responsible for ensuring that all users of the Service are aware of this policy. The Customer is also responsible for ensuring that these regulations are complied with at all times, and shall indemnify Cisco against liability, whether civil or criminal, for any violation by such users as the Customer permit to use the Service.

9.2 Users must not under any circumstances whatsoever commit, or attempt to commit, nor aid or abet any action that may threaten the Service – this shall include but is not limited to:

- Using the Service for any unlawful, invasive, infringing, defamatory, or fraudulent purpose;
- Intentionally sending any virus, worm, Trojan horse or harmful code or attachment with the Service;
- Interfering with the use of the Service by other authorized users;
- Altering, tampering with or circumventing any aspect of the Service;
- Any attempt to crash a Service host or network;
- "Denial of service" attacks, or "flooding" attacks;
- Reselling, passing-through, renting, leasing, timesharing or branding the Service or otherwise providing the Service to any party which is not contractually authorized by Cisco to receive the Service;
- Testing or reverse-engineering the Service in order to find limitations, vulnerabilities or evade filtering capabilities;
- Supplying proprietary information about the Service, including but not limited to screen shots, product documentation, demonstrations, service descriptions, announcements, or feature roadmaps to unauthorized third parties;
- Any attempt to circumvent the user authentication or security of a Service host or network;

- The creation, transmission, storage, or publication of any kind of virus or corrupting program or corrupted data;
- Any other action that may adversely affect the Service.

9.3 Cisco shall have the right to suspend or terminate the Service, and to take such defensive action as may at its sole discretion be deemed necessary in the event of any attack upon the Service or network. Furthermore, Cisco may instigate civil and/or criminal proceedings as appropriate against the perpetrators of such prohibited action.

10. Service Level Agreements

Service Availability

10.1 Cisco warrants that its network will process and deliver Customer's Web requests at least 99.999% of the total hours during every month Customer uses the Service ("Availability"). Availability will be determined on an aggregate basis across all Customer sites. Cisco provides both primary and secondary proxy addresses for each site from which Web traffic may be directed. As a result, non-Availability occurs only where Web content sent from a site to both proxy addresses is not being received or transmitted to end users at the affected Customer site.

10.2 If Cisco breaches the Availability warranty, Cisco shall provide service credits of a portion of Customer's monthly Service fees on the following basis:

Monthly Service Availability	% reimbursement of monthly Service fee
99.999 - 99.5 %	10
99.49 - 99.0 %	20
98.99 - 98.5 %	30
98.49 - 98.0 %	40
97.99 - 97.5 %	50
97.49 - 97.0 %	60
96.99 - 96.5 %	70
96.49 - 96.0 %	80
95.99 - 95.5 %	90
Below 95.5%	100

Web Filtering Latency

10.3 Web Filtering Latency refers to the additional Web page load time attributable to the Service. Web Filtering Latency is assessed by reference to the average elapsed time between:

- a Web page request being sent to Cisco at the datacenter where the applicable scanning towers are located; and
- receipt of the requested Web-page data by the requesting party.

10.4 Web Filtering Latency shall be assessed solely by reference to the time taken to download a discrete resource from a selection of popular websites. For the avoidance of doubt the Web Filtering Latency SLA does not apply to the AnyConnect service.

10.5 To calculate the average Web Filtering Latency, Cisco shall measure the average elapsed time taken to download a discrete resource from each of the websites referred to above ("Filtered Response Time") and compare this time to the average elapsed time taken for identical Web page requests by the same requesting party during the same testing period which are not processed through the Service ("Unfiltered Response Time"). Each such sample of the Filtered Response Time and Unfiltered Response Time is referred to as a "Sampled Pair". Such samples shall be taken every 60 minutes.

10.6 Cisco warrants that the Filtered Response Time (averaged over all of the Sampled Pairs) in any one calendar month will not exceed the greater of:

- one second more than the Unfiltered Response Time; and
- three times the Unfiltered Response Time.

10.7 If Cisco breaches the above warranty, Cisco will provide service credits of an amount equal to 10% of the Customer's monthly Service fees for the Service provided for that month.

False-Positive Web Filtering Rate

10.8 The "False-Positive Filtering Rate" Service Level measures the percentage of URLs and domains that were blocked by the Service but, based on the Customer's chosen categorization policies, should not have been blocked ("Bad Blocks"). For the avoidance of doubt, if a URL is in the 'unclassified' category it shall be required to be blocked if the Customer has elected to block all unclassified URLs.

False-Positive Filtering Rate =

100

x total number of Bad Blocks in a calendar month at all Sites

÷ total number of URLs scanned by the Web Filtering Service at all Sites during the same calendar month

where the Bad Blocks are determined by Cisco acting reasonably.

10.9 If the False-Positive Filtering Rate is greater than or equal to 0.0004%, Cisco will provide service credits of an amount equal to 10% of the Customer's monthly fees for the Web Filtering Service. Cisco shall respond within seven days of receipt of notification that the Customer believes there to have been a Bad Block, and shall give reasons for its decision as to whether there has been a Bad Block or not.

False-Negative Web Filtering Rate

10.10 The False-Negative Filtering Rate Service Level measures the percentage of URLs and domains that were not blocked by the Service but, based on the Customer's chosen categorization policies, should have been blocked ("Missed Blocks"). For the avoidance of doubt, if a URL is in the 'unclassified' category it shall only be required to be blocked if the Customer has elected to block all unclassified URLs.

False-Negative Filtering Rate =

100

x total number of Missed Blocks in a calendar month at all Sites

÷ total number of URLs scanned by the Web Filtering Service at all Sites during the same calendar month

where the Missed Block are determined by Cisco acting reasonably.

10.11 If the False-Negative Filtering Rate is greater than or equal to 0.0004%, Cisco will provide service credits of an amount equal to 10% of the Customer's monthly fees for the Web Filtering Service. Cisco shall respond within seven days of receipt of notification that the Customer believes there to have been a Missed Block, and shall give reasons for its decision as to whether there has been a Missed Block or not.

General

10.12 If Customer believes that Cisco has not met any of the above warranties, Customer must contact Cisco in writing within 15 business days of the end of the month in which Customer believes the relevant warranty was not met.

10.13 Cisco will implement, maintain and use appropriate processes, procedures and tools to monitor, calculate and report on the performance of the Service against the service levels set forth in this Section. If a dispute arises about this Section, Cisco will make a determination in good faith based on its system logs, monitoring reports and configuration records.

10.14 All remedies referred to in this Section are subject to the Customer having paid all applicable fees and fulfilled all of its obligations under this Service Description.

10.15 The remedies in this Section do not apply to any matters arising due to any of the following:

- Customer-requested hardware or software upgrades, moves, facility upgrades, etc.
- 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 Service
- hardware or software configuration changes made by the Customer without the prior written consent of Cisco
- Denial of Service attacks on the installed email security infrastructure or ancillary services
- events outside 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.

10.16 The remedies set out in this Section shall be Customer's sole and exclusive remedy in contract, tort or otherwise in respect of the relevant events. No more than one category of credit may be claimed in respect of any one issue.

10.17 For the avoidance of doubt, while Cisco will use its reasonable efforts to detect malware, Cisco does not guarantee that the Service (including AMP and CTA) will detect or block any specific malicious threat.

11. Support and Escalation Matrix

11.1 Cisco operates a 24/7 helpdesk. If engineers are unable to resolve the issue they will escalate the issue internally for resolution.

11.2 Customer is responsible for using reasonable efforts to resolve internally any support questions prior to contacting Cisco. Customer is responsible for reporting any and all errors promptly in writing in English and for providing sufficient information to Cisco to enable Cisco to duplicate the circumstances indicating a reported Software defect or error. Customer shall provide technical information as may be required by Cisco systems engineers or security analysts, including but not limited to IP addresses for Customer's existing solution.

11.3 A TAC Service Request can be opened in multiple way, via: 1) an online Service Request Tool, 2) email or 3) phone.

a) The online Service Request Tool via "Cisco.com" allows Customer to enter information pertaining to the issue.

b) Customer can send an email to tac@cisco.com including the problem description and contact details.

c) Customer can use the phone. When Customer calls the 1-800 number, the call gets transferred to a Customer Interaction Network (CIN) Agent who captures the initial information about Customer's Service Request and routes the call to the appropriate engineering resource. The CIN team handles all incoming telephone and e-mail messages. The CIN agent completes the following functions for each Service Request: a) open a case, b) verify Customer's entitlement, c) discuss and set priority (Customer sets the severity 1-4) and d) dispatch to the appropriate TAC team.

Help Desk Numbers

	Telephone	Email	Web
EMEA	+44 (0)20 7034 9400	tac@cisco.com	http://www.cisco.com/cisco/web/support/index.html
US	+1 877 472 2680	tac@cisco.com	http://www.cisco.com/cisco/web/support/index.html
APAC	+64 800 513 572	tac@cisco.com	http://www.cisco.com/cisco/web/support/index.html

Severity Definitions

11.4 Cisco helpdesks shall assign a severity to all problems submitted by Customer.

- Severity 1: An existing network is down or there is a critical impact to the Customer's business operation. Cisco and Customer will commit full-time resources to resolve the situation.
- Severity 2: Operation of an existing network is severely degraded, or significant aspects of the Customer's business operation are being negatively impacted by unacceptable network performance. Cisco and Customer will commit full-time resources during Standard Business Hours to resolve the situation.
- Severity 3: Operational performance of the network is impaired while most business operations remain functional. Cisco and Customer are willing to commit reasonable resources during Standard Business Hours to restore service to satisfactory levels.
- Severity 4: Information or assistance is required on product capabilities, installation, or configuration. There is clearly little or no impact to Customer's business operation. Cisco and Customer is willing to provide resources during Standard Business Hours to provide information or assistance as requested.

11.5 For the purposes of this document:

a) "Business Days" means the generally accepted days of operation per week within the relevant region where the Service shall be provided, excluding local holidays.

b) "Local Time" means Central European Time where the Service is provided in Europe-Middle-East and Africa, Australia's Eastern Standard Time where the Service is provided in Australia, Japan's Standard Time where the Service is provided in Japan, and Pacific Standard Time for all other locations.

c) "Standard Business Hours" means 8:00 AM to 5:00 PM, Local Time at location, on Business Days.

Escalation process

11.6 Customers should engage the below contacts when an issue requires escalation.

11.7 Severity 1 escalation times are measured in calendar hours - 24 hours per day, 7 days per week. Severity 2, 3, and 4 escalation times correspond with Standard Business Hours.

Elapsed Time	Severity 1	Severity 2	Severity 3	Severity 4
1 hour	Senior Customer Service Technician			
4 hours	Service Level Manager	Senior Customer Service Technician		
24 hours	Technical Support Manager	Service Level Manager		
48 hours	Director, Technical Support	Technical Support Manager		
72 hours		Director, Technical Support	Service Level Manager	
96 hours			Technical Support Manager	Service Level Manager

GLOSSARY OF TERMS

Cisco means Cisco Systems, Inc. and where appropriate includes its group companies (Cisco International Limited, Cisco Systems International B.V., Cisco Systems G.K., Cisco Systems Australia Pty. Ltd., Cisco Systems Canada Co., Cisco Systems (Italy) s.r.l., ScanSafe Limited and ScanSafe Services LLC).

Data Collection Tools means Hardware and/or Software tools that support Cisco's ability to provide troubleshooting on cases, data analysis, and report generation capabilities.

Documentation means user manuals, training materials, Service descriptions and specifications, technical manuals, license agreements, supporting materials and other information relating to services offered by Cisco, whether distributed in print, electronic, CD-ROM or video format.

Hardware means any tangible Cisco equipment, devices, or components made available to Customers.

Intellectual Property means any and all tangible and intangible: (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Pre-Existing Technology in relation to either party means all of such party's pre-existing Intellectual Property, confidential information and materials, including, without limitation, proprietary ideas, sketches, diagrams, text, know-how, concepts, proofs of concepts, artwork, software, algorithms, methods, processes, identifier codes or other technology that are owned by a party prior to commencement of any part of the Service hereunder, or that are otherwise developed by or for such party outside the scope of this Service Description.

Release means an incremental Software release that provides maintenance fixes and/or provides additional functionality.

Reports means reports, recommendations, network configuration diagrams, and any related items provided by Cisco to Customer.

Service means the Cloud Web Security Service described in this document.

Software means the software programs provided to Customer by Cisco, including any copies, Updates, upgrades, modifications, enhancements, and any derivative works thereof.

Update means Cisco Releases containing the same configuration or feature set as originally acquired, unless the Customer has upgraded the applicable Service to a configuration or feature set other than what was originally acquired, and the applicable license fee for that upgrade has been paid. Updates do not include any separately licensed and priced Software release that contains an enhanced configuration or feature set.