IronPort Email and Web Security

Service Description: Cisco IronPort Hybrid Email Security Service

Direct Sale from Cisco IronPort. If you have purchased these services directly from Cisco IronPort, this document is incorporated into your purchase agreement with Cisco IronPort.

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

This Service Description should be read in conjunction with the other applicable documents found 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 Hybrid Email Security is delivered through hardware and software deployed in IronPort managed data centers. IronPort and/or its parent company will retain ownership, as applicable, of all hardware infrastructure used in IronPort data centers as part of providing the Hybrid Email Security service.

The Hybrid Email Security component includes the following two components

- Cloud Email Security - delivered through hardware and software deployed in IronPort data centers
- On-Premise Email Security – delivered through IronPort appliances and software deployed onsite at Customer's premises or in Customer's data center

The Cloud Email Security component includes hardware infrastructure powered by IronPort technology together with 24x7 monitoring, management and support. The On-Premise Email Security component includes IronPort email security appliances together with 24x7 support.

1.2 The Services do 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 IronPort.

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

d) Services for non-IronPort products used in connection with IronPort Services.

1.4 Except as otherwise agreed, Software entitlement, including media, documentation, binary code, source code or access in electronic or other form is not provided.

2. IronPort Responsibilities

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

a) Provide the Services set forth in the Service Description as ordered by the Customer;

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

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

d) Back-up the Customer's configuration.

e) Provide 24 x 7 access to all of its Documentation and its Knowledge Base; and

f) Provide 24 x 7 access to Remote Management Services for the Hybrid Email Security Service.

3. Functionality

3.1 The Cisco Hybrid Email Security Services provides comprehensive inbound protection and outbound control our Customer's email traffic as described below. Customers have the option of purchasing and enabling the following list of available capabilities with the Service:

- IronPort Anti-Spam
- Intelligent Multi-Scan
- Sophos Anti-Virus
- McAfee Anti-Virus
- Outbreak Filters
- Image Analysis
- Email Encryption
- Data Loss Protection
- Cloudmark Anti-Spam

3.2 The Customer's inbound and outbound SMTP email traffic is directed through the Services. The configuration settings required to direct this email traffic via the Services are made and maintained by the Customer (with assistance and support from IronPort or partner as reasonably required) and are dependent on the Customer's technical infrastructure.

Inbound Spam Protection

3.3 Once the relevant configuration changes are made, inbound email will be directed to the Service where all types of undesirable email messages will be blocked using a multi-scanning architecture.

3.4 Inbound email traffic will first pass through the **IronPort Reputation Filters** where a real-time traffic threat assessment will be performed to identify suspicious email senders.

3.5 Next, inbound email traffic will be analyzed by IronPort's proprietary **Content Adaptive Scanning Engine (CASE).** CASE combines leading conventional techniques with IronPort's context-sensitive detection technology to eliminate the broadest range of known and emerging email threats. Any message deemed undesirable will be tagged for action as defined in the configuration. All actions taken by the system will be logged for review and analysis.

Inbound Virus Defense

3.6 Once the relevant configuration changes are made, inbound email will be directed to the Service where all types of email messages with malicious content or attachments will be blocked using a multi-layer, multi-vendor approach.

3.7 Inbound email traffic will pass through the IronPort **Virus Outbreak Filters** as critical first layer of preventive defense stopping viruses before they enter the network by identifying and quarantining suspicious email – hours before traditional virus signatures are available.

3.8 Next, inbound email traffic will be analyzed by multiple traditional virus detection engines – Sophos and/or McAfee -- to ensure maximum protection against even the most complex virus attacks.

Email Encryption

3.9 IronPort Email Encryption protects confidential data, using IronPort PXE™ technology to enable simple, secure two-way communication with any email recipient. The capability is an optional element of the Service available to all customers.

Data Loss Prevention

3.10 Integrated Content Scanning technology enables easy-to-manage enforcement of regulatory and acceptable use policies and protection of intellectual property, based on the content of messages and attachments. Turnkey PCI, HIPAA, SOX and GLB solutions are available with this feature.

Web Based Interface

3.11 The Customer will be provided access by IronPort to a Web-based interface to administer and report on the Services. Access to the interface is via a secure (HTTPS) website and is password-protected.

3.12 The Customer may have multiple administrators for a single account. The Customer can request a unique login for each administrator and provide full access or read only privileges specific to each user.

3.13 The interface enables the customer administrator to:

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

b) create access restrictions and apply these to specific users or groups;

c) configure and schedule automated system reporting; and

d) track email messages.

3.14 Customers also can access a comprehensive support portal with an extensive knowledge base of subject matter expertise to assist with their needs. Using this support portal, customers can view all current and historical events/tickets, reports as well as the status of their Hybrid service infrastructure.

4. Maintenance

4.1 From time to time, IronPort performs scheduled maintenance, to update the servers (IronPort and third-party servers at the datacenter(s)) and software that are part of the Hybrid Email Security service. IronPort 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 IronPort may, in certain situations, need to perform emergency maintenance on less than 48 hours advance notice.

5. Customer Responsibilities

5.1 Customer shall supply IronPort with all technical data and all other information IronPort may reasonably request from time to time to allow IronPort to supply the Services to the Customer, including a completed deployment questionnaire.

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

5.3 Customer is responsible for implementing and using strong passwords for accessing IronPort 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...)*

5.4 Customer or its designated personnel must not change the password for IronPort support services or delete the support user ID.

5.5 In performing the Services, IronPort 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 IronPort, 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 IronPort, at IronPort's then-current rates, plus any reasonable actual out-of-pocket expenses, for any rework or additional work resulting from modification of the Services requested by Customer (and accepted by IronPort) or any act or omission of Customer, including providing inaccurate information to IronPort. IronPort 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.

5.6 Customer is responsible for obtaining all approvals required by any third parties in order for IronPort to perform any Service under this Service Description. IronPort shall not be in default of its obligations to the extent it cannot perform the Services either because such approvals have not been obtained or any third party otherwise prevents IronPort from performing such Services.

5.7 Customer agrees that it shall not resell the Product and/or Services or create or offer derivative versions of the Services either directly or through a third party.

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

5.9 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.

5.10 Customer must not use the Services to send spam, viruses or malware.

5.11 Customer is responsible for any catastrophic security events that result from any unauthorized configuration of the Hybrid Email Security Service components by Customer's personnel. These include, but are not limited to, configuring the Hybrid Email Security service components in a manner not prescribed in the Documentation, creating an open relay, changing the network configuration set by IronPort, shutting down the IronPort infrastructure, etc.

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

5.13 From time to time, IronPort may perform an inventory review of Customer's infrastructure. IronPort will charge a Service fee if it finds that unauthorized Services are being provided. This Service fee includes amounts that should have been paid, interest, attorneys' and audit fees. IronPort requires that Customer take all necessary action (for example, disabling passwords) to ensure that any former employees and contractors do not access or use the Service.

5.14 IronPort reserves the right to require Customer to purchase additional seats if the number of actual distinct users (as shown by IronPort's traffic logs) exceeds the number of licensed seats from time to time.

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

6. Data Privacy

6.1 Subject to the IronPort Privacy Statement at www.ironport.com/privacy.html or a successor site location, as the same may be amended from time to time by IronPort with notice to Customer, Customer hereby consents and grants to IronPort 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 IronPort ("Data"). To the extent that reports or statistics are generated using the Data, they shall be disclosed only in the aggregate and no End User identifying information may be surmised from the Data, including without limitation, user names, phone numbers, unobfuscated file names, email addresses, physical addresses and file content.

7. Licenses and Ownership

7.1 Subject to Customer's compliance with the terms of this Service Description, IronPort 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 Services; (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 IronPort's rights in such Licensed Materials as are specified in this Service Description.

7.2 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 Services to human-readable form; or transfer, sublicense, rent, lease, distribute, or sell, any Services, 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 IronPort.

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

7.4 Except as otherwise expressly set forth in this Service Description, IronPort owns and will continue to own all right, title and interest in and to the Hardware, Services, 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 IronPort

(or a third party acting on IronPort'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, "***IronPort Intellectual Property***"). Without limiting the foregoing, IronPort owns and will continue to own all right, title and interest in and to:

- Hardware infrastructure used in the IronPort data center as part of the Cloud Email Security component of the Hybrid Email Security Service.
- IronPort appliances provided as part of the On-Premise Security component of the Cisco Hybrid Email Security Service..

7.5 If Customer already possesses title to IronPort appliances, then it shall retain title to such existing appliances.

7.6 If Customer is requesting shipments outside of the United States, then Customer will own title to IronPort appliances provided as part of the On-Premise Security component.

7.7 As between Customer and IronPort, 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 IronPort 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.

7.8 Customer hereby grants to IronPort 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 Services, Products, Deliverables, Data Collection Tools, Reports or IronPort 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 Services, Products, Deliverables, Data Collection Tools, Reports or IronPort Pre-Existing Technology as a result of IronPort'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 Services, Products, Deliverables, Data Collection Tools, Reports or IronPort Pre-Existing Technology that Customer provides to IronPort.

8. Capacity Assurance

8.1 As long as Customer has paid all applicable fees, IronPort will, in its sole and reasonable discretion, provide additional capacity to handle an increase in spam volumes and inbound email for the number of users specified on the Purchase Order. The capacity assurance spans both the Cloud Email Security component and on-premise component of the IronPort Hybrid Email Security Services:

- Capacity assurance for the Cloud component will include capacity to handle an increase in spam volumes and inbound email.
- Capacity assurance for the on-premise component will include capacity required to handle an increase in user generated outbound mail volume as well as legitimate inbound email volumes.

8.2 IronPort will use its commercially reasonable efforts to provide capacity for events that were unforeseen by the Customer. The additional capacity will not exceed 50% of the Initial Deployed Capacity.

8.3 The above assurance does not apply to:

a) Capacity requirements placed on the system due to misconfigured, ill-formed or performance intensive activities that include but are not limited to body-scanning, content dictionaries, , etc.

b) Capacity needs placed on the system due to new requirements placed on the system due to a changing regulatory scheme or business environment.

c) Capacity needs placed on the system from non-users. This includes but is not limited to marketing communications, customer's customers, email generating program or entity, etc.

d) An increase in email volume from marketing campaigns and other events that are not part of the Customer's day-to-day operations.

9. Acceptable Use Policy

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

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

- Using the Services for any unlawful, invasive, infringing, defamatory, or fraudulent purpose;
- Intentionally sending any virus, worm, Trojan horse or harmful code or attachment with the Services;
- Interfering with the use of the Services by other authorized users;
- Altering, tampering with or circumventing any aspect of the Services;
- Any attempt to crash a Services host or network;
- "Denial of service" attacks, or "flooding" attacks;
- Reselling, passing-through, renting, leasing, timesharing or branding the Services or otherwise providing the Services to any party which is not contractually authorized by us to receive the Services;
- Testing or reverse-engineering the Services in order to find limitations, vulnerabilities or evade filtering capabilities;

- Supplying proprietary information about the Services, 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 Services 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 Services or their operation.

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

10. Service Level Agreements (applicable only to the Cloud Email Security component)

For the purposes of this Section:

"Spam" is unsolicited or unauthorized bulk email (SMTP only) as mutually agreed upon by Customer and IronPort, and excludes unwanted marketing messages that include opt-out provisions.

"Caught Spam" is Spam either quarantined; or categorized as a "threat message" in the User Interface.

"Missed Spam" is Spam delivered to an end user's inbox.

"Virus" is a binary or executable code whose purpose is to gather information from the infected host, change or destroy data on the infected host, use inordinate system resources in the form of memory, disk space, CPU cycles or network bandwidth on the infected host, use the infected host to replicate itself to other hosts, or provide control or access to any of the infected host's system resources. A virus does not include: (1) text messages that use fraudulent claims to deceive the customer, and/or prompt the customer to action, (2) a binary or executable code installed or run by the end user that gathers information for sales or marketing purposes, (3) a virus that may be detected and cleaned by other virus scanning products, or (4) an ineffective or inactive virus fragment.

Uptime Service Level Agreement

A. The Hybrid Email Security Service will accept connections on Port 25 and process email at least 99.999% over a trailing one-year period. Uptime is determined by dividing the total number of minutes the Service was processing email divided by the number of minutes in a one year period or 525,600 minutes. Downtime must exceed 30 seconds per occurrence before it is an infraction. An infraction is limited to a single incident, whereby separate downtime occurrences cannot be aggregated. Uptime is determined and validated by an industry-recognized 3rd party monitoring service that performs service-level checks from various locations on the global internet.

B. Remedy

If Customer experiences a downtime infraction and subject to the General Exceptions (as defined below), then the Customer will be entitled to the applicable service credit (as set forth in the table below) as its sole and exclusive remedy:

Mailbox Count:	**250+**	**2,000+**	**5,000+**	**10,000+**	**20,000+**
Actual Uptime < 99.999%	$100	$200	$500	$1,000	$2,000

Customer may only make a total of two (2) claims of a downtime occurrence within a rolling three hundred sixty-five (365) day period. If Customer experiences three (3) or more downtime occurrences within a rolling three hundred sixty-five (365) day period, IronPort and Customer will come to a written agreement, within thirty (30) days of Customer providing notice of such occurrence, on the next course of action. If Customer experiences a downtime infraction more than five (5) within a rolling three hundred sixty-five (365) day period and IronPort fails to provide a reasonable written plan of permanent corrective action to customer within a 30 day time frame after the fifth occurrence, then Customer shall have the right to cancel the Services at no cost or obligation and no financial responsibility for any future payments.

C. Customer responsibilities

- Customer must provide notice within thirty (30) days of the downtime occurrence
- Customer must provide timeframe details of the downtime occurrence, any correlated support ticket numbers, and, if available, pings and trace routes showing that the device was not available on the network
- Customer must provide confirmation, if possible, that there were:
  1. No network failures at the customer site either internal or external at the time of the occurrence
  2. No Customer implemented changes that adversely affected the system availability or made the system to cause delays (excepting any changes requested by IronPort)
  3. No material delay in responding to warnings raised by IronPort generally, or specifically related to the incidence of downtime

Failure to comply with this Section C will result in a forfeit of Customer's right to the remedy set forth in Section C above.

Anti-Spam Service Level Agreement

A. The Hybrid Email Security Service will detect and stop at least 99% of all inbound Spam that is routed through the Service. The ***"Spam Catch Rate"*** is determined by dividing Caught Spam by the sum of the Caught Spam and the number of Missed Spam, during a trailing thirty (30) day period.

B. Exceptions

- Marketing emails with opt-out provisions will not be counted in the missed spam calculation.

C. Remedy

If Customer experiences a Spam Catch Rate equal to less than the amount set forth in Section A and subject to the General Exceptions (as defined below) and the exceptions set forth in Section B, then the Customer will be entitled to the applicable service credit (as set forth in the table below) as its sole and exclusive remedy:

Mailbox Count:	**250+**	**2,000+**	**5,000+**	**10,000+**	**20,000+**
Anti-Spam	$100	$200	$500	$1,000	$2,000

Within any given three hundred sixty-five (365) day period, Customer may only make a total of two (2) claims that the Anti-Spam Service Level Agreement is not being met. If Customer experiences three (3) or more occurrences within a rolling three hundred sixty-five (365) day period, that the Anti-Spam Service Level Agreement is not being met, IronPort and Customer will come to a written agreement, within thirty (30) days of Customer providing notice of such occurrence, on the next course of action.

D. Customer Responsibilities

- Customer must provide notice within thirty (30) days of the date the claim arises.
- Customer must have SenderBase reputation filters enabled at default levels (blocking from -10 to -3) or more aggressive.
- Customer must have the reputation messages per connection multiplier set to the default value (3).
- Customer must have IronPort Anti-Spam block settings at the default value (90) or more aggressive.
- Customer must have IronPort Anti-Spam quarantine enabled with settings at default (50) or more aggressive.
- Customer must have SenderBase Network Participation enabled.
- Customer must be able to provide copies of missed spam to IronPort upon request.
- Customer must provide the domains covered by the service, the number of mailboxes and the incoming mail report for the last 30 days.

Failure to comply with this Section D will result in a forfeit of Customer's right to the remedy set forth in Section C above.

False Positive Rate Service Level Agreement

A. The Hybrid Email Security Service will not categorize legitimate inbound email as Spam more than one time per one million messages processed. The ***"False Positive Rate"*** is determined by counting the number of non-Spam messages misclassified as Spam relative to the total attempted messages processed over a trailing thirty (30) day period, as set forth in the User Interface.

B. Exceptions

- 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. IronPort will make a determination in good faith based on its system logs, monitoring reports and configuration records for such email senders.
- Marketing emails with opt-out provisions will not be counted towards the false positive rate.

C. Remedy

If Customer experiences a False Positive Rate greater than the rate set forth in Section A above and subject to the General Exceptions (as defined below) and the exceptions set forth in Section B above, then the Customer will be entitled to the applicable service credit (as set forth in the table below) as its sole and exclusive remedy:

Mailbox Count:	**250+**	**2,000+**	**5,000+**	**10,000+**	**20,000+**
False Positive	$100	$200	$500	$1,000	$2,000

Within any given three hundred sixty-five (365) day period, Customer may only make a total of two (2) claims that the False Positive Rate Service Level Agreement is not being met. If Customer experiences three (3) or more occurrences within a rolling three hundred sixty-five (365) day period, that the False Positive Rate Service Level Agreement is not being met, IronPort and Customer will come to a written agreement, within thirty (30) days of Customer providing notice of such occurrence, on the next course of action.

D. Customer Responsibilities

- Customer must provide notice within thirty (30) days of the date the claim arises.
- Customer must have SenderBase reputation filters enabled at default levels (blocking from -10 to -3) or more conservative.
- Customer must have the reputation messages per connection multiplier set to the default value (3).
- Customer must have IronPort Anti-Spam block settings at the default value (90) or more conservative.
- Customer must have IronPort Anti-Spam quarantine enabled with settings at default (50) or more conservative. Non-Spam that is quarantined counts as a false positive
- Customer must have SenderBase Network Participation enabled.
- Customer must provide copies of false positive messages to IronPort.
- Customer must provide the domains covered by the service, the number of mailboxes and the incoming mail report for the last 30 days. Hybrid customers must enable IronPort Anti-Spam at a minimum in the cloud layer and not on-premise.
- Customers must only enable IronPort Anti-Spam for spam scanning to qualify.

Failure to comply with this Section D will result in a forfeit of Customer's right to the remedy set forth in Section C above.

Virus Catch Rate Service Level Agreement

A. The Hybrid Email Security Service will detect and stop 100% of all Known Viruses that are routed through the Service. A ***"Known Virus"*** is defined solely by the provider of anti-virus software that is used for a specific message. Known

Viruses will be detected and stopped within 30 minutes of when the anti-virus provider releases a signature for the platform.

B. Exceptions

- Messages that contain a URL to a website hosting malware are not included.

C. Remedy

If Customer experiences a Virus Catch Rate less than the rate set forth in Section A above and subject to the General Exceptions (as defined below) and the exceptions set forth in Section B above, then the Customer will be entitled to the applicable service credit (as set forth in the table below) as its sole and exclusive remedy:

Mailbox Count:	**250+**	**2,000+**	**5,000+**	**10,000+**	**20,000+**
Anti-Virus	$100	$200	$500	$1,000	$2,000

Within any given three hundred sixty-five (365) day period, Customer may only make a total of two (2) claims that this Virus Catch Rate Service Level Agreement is not being met. If Customer experiences three (3) or more occurrences within a rolling three hundred sixty-five (365) day period, that this Virus Catch Rate Service Level Agreement is not being met, IronPort and Customer will come to a written agreement, within thirty (30) days of Customer providing notice of such occurrence, on the next course of action.

D. Customer Responsibilities

- Customer must provide notice within thirty (30) days of the date the claim arises.
- Customer must have SenderBase reputation filters enabled at default levels (blocking from -10 to -3) or more aggressive.
- Customer must have SenderBase Network Participation enabled.
- Customer must provide copies of all missed Virus-positive messages to IronPort in a password-protected attachment.
- Customer must ensure that the message was scanned by the anti-virus engine (e.g. message did not exceed the maximum scanning size limit).
- Customer must provide the domains covered by the service, the number of mailboxes and the incoming mail report for the last 30 days.

Failure to comply with this Section D will result in a forfeit of Customer's right to the remedy set forth in Section C above.

CRES Uptime for PXE Service Level Agreement ("CRES SLA")

A. The installed Cisco Registered Envelope Service (***"CRES"***) will be Operational at least 99.999% of the time, over a trailing one-year period. For the purposes of this Section D, ***"Operational"*** means that Customer 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 the service was Operational divided by the number of minutes in a one year period or 525,600 minutes. This results in an infraction constituting a minimum of 30 seconds of downtime. An infraction is limited to a single incident, whereby separate downtime occurrences cannot be aggregated. CRES Uptime is determined and validated by an industry-recognized 3rd party monitoring service that performs service-level checks from various locations on the global internet.

B. Exceptions

- This CRES SLA does not include uptime of other Services including CASE updates, AV updates from IronPort partners and the SenderBase service.
- This CRES SLA excludes Customer's Administrator account access.

C. Remedy

If Customer's CRES is not Operational for more than 99.999% of the time, subject to the General Exceptions (as defined below) and the provisions set forth in Section (B) above, then the Customer will be entitled to the applicable service credit (as set forth in the table below) as its sole and exclusive remedy:

Mailbox Count:	**up to 199**	**200+**	**500+**	**1,000+**	**2,000+**	**5,000+**	**10,000+**	**20,000+**
Actual Uptime < 99.999%	$30	$40	$60	$100	$200	$500	$1,000	$2,000

Within any given three hundred sixty-five (365) day period, Customer may only make a total of two (2) claims that the CRES Uptime Service Level Agreement is not being met. If Customer experiences three (3) or more occurrences within a rolling three hundred sixty-five (365) day period, that the CRES Uptime Service Level Agreement is not being met, Cisco IronPort and Customer will come to a written agreement, within thirty (30) days of Customer providing notice of such occurrence, on the next course of action.

D. Customer Responsibilities

- Customer must provide notice within thirty (30) days of the date the claim arises.
- Customer must provide timeframe details of the downtime occurrence, any correlated support ticket numbers, and, if available, pings and trace routes showing that the device was not available on the network
- Customer must provide confirmation, if possible, that there were:

1. No network failures at the customer site either internal or external at the time of the occurrence
2. No Customer implemented changes that adversely affected the system availability or made the system to cause delays (excepting any changes requested by Cisco IronPort)
3. No material delay in responding to warnings raised by Cisco IronPort generally, or specifically related to the incidence of downtime

Failure to comply with this Section D will result in a forfeit of Customer's right to the remedy set forth in Section C above.

General Conditions

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.

The remedies in this Section do not apply to any matters arising due to any of the following ("General Exceptions"):

- 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 IronPort or within the scope of the Hybrid Email Security Service
- hardware or software configuration changes made by the Customer
- Denial of Service attacks on the installed email security infrastructure or ancillary services such as SenderBase
- .Events outside IronPort'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.

11. Support and Escalation Matrix

11.1 IronPort operates a 24/7 helpdesk which comprises both Tier 1 and Tier 2 engineers. All issues must be logged with Tier 1 engineers in the first instance. If an issue is not resolved by Tier 1 engineers, the issue will be escalated to Tier 2 engineers for resolution. If Tier 2 engineers are unable to resolve the issue they will escalate the issue internally to Operations Engineers for resolution.

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

Help Desk Numbers

	Email	**Telephone**
EMEA	Support@opmanager.com	+44 (0)20 8824 1000
US / APAC	Support@opmanager.com	+1 800 553 2447

Severity Definitions

11.3 IronPort 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 End User's business operation. End User and IronPort will commit full-time resources to resolve the situation.
- Severity 2: Operation of an existing network is severely degraded, or significant aspects of the End User's business operation are being negatively impacted by unacceptable network performance. IronPort and End User 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. IronPort and End User are willing to commit reasonable resources during Standard Business Hours to restore service to satisfactory levels.
- Severity 4: Information or assistance is required on a Supplier's product capabilities, installation, or configuration. There is clearly little or no impact to the End User's business operation. IronPort and End User are willing to provide resources during Standard Business Hours to provide information or assistance as requested.

11.4 For the purposes of this document:

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

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

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

Escalation process

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

11.6 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	Customer Engineering Manager			
4 hours	Technical Support Director	Customer Engineering Manager		
24 hours	Vice President, Customer Advocacy	Technical Support Director		
48 hours	President Customer Advocacy	Vice President, Customer Advocacy		
72 hours		President Customer Advocacy	Customer Engineering Manager	
96 hours			Technical Support Director	Customer Engineering Manager

GLOSSARY OF TERMS

Data Collection Tools means Hardware and/or Software tools that support IronPort'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 IronPort, whether distributed in print, electronic, CD-ROM or video format.

Hardware means any tangible IronPort 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 Services 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 IronPort to Customer.

Services means one or more of the services options selected by the Customer and described at: www.cisco.com/legal/services.html.

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

Update means IronPort Releases containing the same configuration or feature set as originally acquired, unless the Customer has upgraded the applicable Services 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.