Symantec™ Email Security.cloud

Service Description

September 2018

This Service Description describes Symantec's Email Security.cloud ("Service"). All capitalized terms in this description have the meaning ascribed to them in the Agreement (defined below) or in the Definitions section.

This Service Description, with any attachments included by reference, is part of and incorporated into Customer's manually or digitally-signed agreement with Symantec which governs the use of the Service, or if no such signed agreement exists, the Symantec Online Services Terms and Condition (hereinafter referred to as the "Agreement").

Table of Contents

1: Technical/Business Functionality and Capabilities

Service Overview

Symantec™ Email Security.cloud is a hosted service that filters Email messages and helps protect organizations from Malware (including targeted attacks and phishing), Spam, and unwanted bulk Email. The Service offers encryption and Data Protection options to help control sensitive information sent by Email. The Service supports multiple mailbox types from multiple vendors.

Service Features

- Customer Administrators can access the Service management console by using a secure password-protected login. The management console provides the ability for Customer to configure and manage the Service, access reports, and view data and statistics when available as part of the Service.
- The Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for hardware availability, service capacity and network resource utilization. The Service is regularly monitored for service level compliance and adjustments are made as needed.
- Reporting for the Service is available through the management console. Reporting may include activity logs and/or statistics. Using the management console, Customer may choose to generate reports, which can be configured to be sent by Email on a scheduled basis, or downloaded from the management console.
- The Service is intended to enable Customer to implement a valid and enforceable computer use policy, or its equivalent.
- Suggested word lists and template rules or policies supplied by Symantec contain words which may be considered offensive.
- Should the Service be suspended or terminated for any reason whatsoever, Symantec may reverse all configuration changes made upon provisioning the Service, and it is the responsibility of Customer to undertake all other necessary configuration changes when the Service is reinstated.

Service Options and Features

The Service is offered in two (2) options: Email Protect or Email Safeguard. The Service must be purchased for each User of the selected option or add-on (subject to any restrictions described in this Service Description).

Features by Service Option

	Email Protect	Email Safeguard
Email Antimalware: Malware protection including Phishing and Targeted Attack protection	✓	✓
Email Antispam: Spam and Phishing (with real-time link following), and Bulk Mail Protection	✓	✓
Email Data Protection: Customizable Content Filtering Policy Controls		✓
Email Image Control: Offensive Image Detection		✓
Outbound Filtering	✓	✓
Enforced TLS Encryption		✓

Opportunistic TLS Encryption	✓	✓
Address Registration: Invalid recipient handling	✓	✓
Users and Groups LDAP Synchronization tool	✓	✓
Message Tracing	✓	✓
Reporting Dashboard	✓	✓
Summary (PDF) and Detailed (CSV) Reporting	✓	✓
End User Spam Quarantine Portal and Notifications	✓	✓
Disclaimer Management	✓	✓
Policy Based Encryption Essentials		✓
Email Impersonation Controls		✓

Additional information on individual Service features is available in the online help at http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=EN_US.

Service Add-Ons

	Email Protect	Email Safeguard
Advanced Threat Protection: Email	Available	Available
Policy Based Encryption Advanced	_	Available
Email Fraud Protection	Available	Available
Email Threat Isolation	Available	Available

Additional information on individual Service Add-Ons is available in the online help at http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=EN_US. The Service Description for Email Fraud Protection can be found at: https://www.symantec.com/about/legal/repository.

Advanced Threat Protection: Email detects advanced threats sent by Email using the Symantec Cynic™ sandbox, identifies targeted Email attacks against the recipient organization or user, and identifies URLs that turn malicious after the delivery of the Emails with Symantec Click-time™ URL Protection. It can pull back emails that are determined to be malicious post-delivery by our Cynic™ sandbox for O365 customers. It provides detailed malware reporting, including URL information, malware category, detection method, and file hashes. A Data Feed API is included to enable malware reporting via an authenticated URL without file imports or emailing data. Advanced Threat Protection: Email also provides access to the Phishing Readiness service, a phishing attack simulator used to determine the susceptibility of personnel to such attacks. Use of the Phishing Readiness service is governed by the terms and conditions located at (https://www.symantec.com/about/legal/repository).

Policy Based Encryption Advanced provides: (i) a pull Web pickup portal; (ii) PGP and S/MIME delivery support; (iii) the ability to attempt TLS encryption before falling back to less transparent encryption technologies; and (iv) an encrypted .pdf push delivery (the only encryption method provided as part of the Policy Based Encryption Essentials feature of the Email Safeguard plan). Policy Based Encryption Advanced is licensed per sending User, which may be a subset of the overall User count for the Email Safeguard option. If a Customer requires use of the Policy Based Encryption Advanced option for secure statement delivery, Symantec may enable the Customer to purchase additional User licenses based on the number of statements to be delivered, per a formula to be defined by Symantec.

Symantec™ Email Fraud Protection is a cloud service that automates enforcing DMARC (Domain-based Message Authentication, Reporting, and Conformance). Symantec Email Fraud Protection makes every step to DMARC enforcement simpler and more seamless compared with the manual method. Enforcement reduces the risk of inbound impersonation attacks, as all emails that originate from unauthenticated sources get quarantined or rejected. Once at enforcement, email recipients or Mail Transfer Agents know they can trust the customer's domain, in turn increasing email deliverability rates.

Symantec™ Email Threat Isolation strengthens protection against spear phishing, credential theft, and advanced email attacks by isolating malicious links and by safely rendering risky webpages. Email Threat Isolation enables Symantec to offer the strongest protection against sophisticated email threats that leverage malicious links, such as advanced spear phishing or credential theft attacks.

Email Threat Isolation creates a secure execution environment between users and their email links, rendering suspicious links remotely and showing only inoculated web content to users. As a result, Symantec stops any threats that contain malicious links from reaching users, as every link it receives is treated as malicious and executed remotely, away from users and their devices. Email Threat Isolation also stops credential phishing attacks by rendering phishing websites in read-only mode, which prevents users from entering corporate credentials and other sensitive information.

Service Level Agreement

- Symantec provides the applicable service level agreement ("SLA") for the Service as specified in Exhibit-A.

Supported Platforms and Technical Requirements

- Supported platforms and technical requirements for the Service are provided at http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=EN_US.

Hosted Service Software Components

- The Service includes the software Service Components available in the management console, which may be accessed upon payment of any applicable fee.

2: Customer Responsibilities

Symantec can only perform the Service if Customer provides required information or performs required actions, otherwise Symantec's performance of the Service may be delayed, impaired or prevented, and/or eligibility for Service Level Agreement benefits may be voided as noted below.

- Setup Enablement: Customer must provide information required for Symantec to begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist Symantec in delivery of the Service, upon reasonable request by Symantec.
- Customer is responsible for its account information, password, or other login credentials.
- Customer agrees to use reasonable means to protect the credentials and will notify Symantec immediately of any known unauthorized use of Customer account.
- Renewal Credentials: If applicable, Customer must apply renewal credential(s) provided in the applicable Subscription Instrument or Order Confirmation within its account administration, to continue to receive the Service, or to maintain account information and Customer data which is available during the Service Term.
- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the management console, if applicable, or default settings will apply. In some cases, default settings do not exist and no Service will be provided until Customer chooses

a setting. Configuration and use of the Service(s) are entirely in Customer's control, therefore, Symantec is not liable for Customer's use of the Service, nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.

Acceptable Use Policy

- Customer is responsible for complying with the Symantec Online Services Acceptable Use Policy.

3: Entitlement and Subscription Information

Charge Metrics

The Service is available under the following Meter as specified in the Order Confirmation:

- "**User**" means an individual person and/or device authorized to use and/or benefits from the use of the Service, or that actually uses any portion of the Service.

Changes to Subscription

If Customer has received Customer's Subscription or Entitlement directly from Symantec, communication regarding permitted changes of Customer's Subscription or Entitlement must be sent to the following address (or replacement address as published by Symantec): CLD_cancellations_MLABS@symantec.com, unless otherwise noted in Customer's agreement with Symantec. Any notice given according to this procedure will be deemed to have been given when received. If Customer has received Customer's Subscription or Entitlement through a Symantec reseller, please contact Customer's reseller.

4: Assistance and Technical Support

Note: This section only applies if Customer is entitled to receive Customer Assistance and Support directly from Symantec ("Support"). If a Customer is entitled to receive Assistance and Support from a Symantec reseller, refer to Customer's agreement with that reseller for details regarding such Support, and the Support described here will not apply to Customer.

Customer Assistance

Symantec will provide the following assistance as part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service;
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions.

Technical Support

Entry-level Support is included as part of the Service as specified below.

- Support is available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Customer with configuration of the Service features and to resolve reported problems with the Service. Support for Services will be performed in accordance with the published terms and conditions and technical support policies published at https://support.symantec.com/en_US/article.TECH236428.html.
- Once a severity level is assigned to a Customer submission for Support, Symantec will make every reasonable effort to respond per the response targets defined in the table below. Faults originating from Customer's actions or requiring the actions of other service providers are beyond the control of Symantec and as such are specifically excluded from this Support commitment.

Problem Severity	Support (24x7) Response Targets*
Severity 1: A problem has occurred where no workaround is immediately available in one of the following situations: (i) Customer's production server or other mission critical system is down or has had a	Within 30 minutes

substantial loss of service; or (ii) a substantial portion of Customer's mission critical data is at a significant risk of loss or corruption.	
Severity 2: A problem has occurred where a major functionality is severely impaired. Customer's operations can continue in a restricted fashion, however long-term productivity might be adversely affected.	Within 2 hours
Severity 3: A problem has occurred with a limited adverse effect on Customer's business operations.	By same time next business day**
Severity 4: A problem has occurred where Customer's business operations have not been adversely affected.	Within the next business day; Symantec further recommends that Customer submit Customer's suggestion for new features or enhancements to Symantec's forums

The above Support Response Targets are attainable during normal service operations and do not apply during Maintenance to the Service and/or supporting infrastructure as described in the Maintenance section below.

** Target response times pertain to the time to respond to the request, and not resolution time (the time it takes to close the request).*

*** A "business day" means standard regional business hours and days of the week in Customer's local time zone, excluding weekends and local public holidays. In most cases, "business hours" mean 9:00 a.m. to 5:00 p.m. in Customer's local time zone.*

Maintenance to the Service and/or supporting Service Infrastructure

Symantec must perform maintenance from time to time. Symantec will use commercially reasonable efforts to perform routine maintenance at times when collective Customer activity is low to minimize disruption. Customer will not receive prior notification for these routine maintenance activities. For all other types of maintenance and as listed below, Symantec will endeavor to inform the affected parties in advance by posting an alert to the Symantec Status Page (https://status.symantec.com/). For information on Service status, planned maintenance and known issues, visit the Symantec Status Page, and subscribe to Symantec Email Security.cloud Page to receive the latest updates. **Core service features such as Security Scanning and Email Delivery remain uninterrupted during all maintenance activities.**

- ***Planned Maintenance:*** Planned Maintenance means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. Symantec will endeavor to perform Planned Maintenance at times when collective customer activity is low, in the time zone in which the affected Infrastructure is located, and only on part, not all, of the network. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. For Planned Maintenance, Symantec will use commercially reasonable efforts to give Customer seven (7) calendar days' notification posted on Symantec Status Page. Customers can also receive notifications via SMS, email or Twitter by subscribing to Symantec Status Page.
- ***Unplanned Maintenance:*** Unplanned Maintenance means scheduled maintenance periods that do not allow for the standard seven (7) days notification and during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. Symantec will use commercially reasonable efforts to give Customer a minimum of one (1) calendar day notification posted on Symantec Status Page. During Unplanned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. At times Symantec will perform Emergency Maintenance. Emergency Maintenance is defined as maintenance that *must be implemented as quickly as possible to resolve or prevent a major incident*. Symantec will endeavor to inform the affected parties in advance by posting an alert to Symantec Status Page no less than one (1) hour prior to the start of the maintenance.
- ***Management Console Maintenance:*** For Management Console Maintenance, Symantec will use commercially reasonable efforts to give Customer fourteen (14) calendar days' notification posted on Symantec Status Page.   Symantec will endeavor to perform maintenance on the management console at times when collective customer activity is low to minimize disruption to the availability of the management console. On occasion, Symantec may perform minor updates to the Management Console, Customers will not receive prior notification for these routine maintenance activities.

5: Additional Terms

- The Service may be accessed and used globally, subject to applicable export compliance limitations and technical limitations in accordance with the then-current Symantec standards.
- Symantec reserves the right to modify and update the features and functionality of the Service, with the objective of providing equal or enhanced Service (as long as Symantec does not materially reduce the core functionality of the Service). Customer acknowledges and agrees that Symantec reserves the right to update this Service Description at any time during the Subscription Term to accurately reflect the Service being provided, and the updated Service Description will become effective upon posting.
- The use of any Service Component in the form of software shall be governed by the license agreement accompanying the software. If no EULA accompanies the Service Component, it shall be governed by the terms and conditions located at (http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf). Any additional rights and obligations with respect to the use of such Service Component shall be as set forth in this Service Description.
- Except as otherwise specified in the Service Description, the Service (including any Hosted Service Software Component provided therewith) may use open source and other third party materials that are subject to a separate license.
- Symantec may update the Service at any time to maintain the effectiveness of the Service.

- Any templates supplied by Symantec are for use solely as a guide to enable Customer to create its own customized policies and other templates.
- The following limits apply to the Service:
  - Inbound and outbound messages, per User per calendar month = ten thousand (10,000). This limit is not inclusive of Spam and Malware directed at Customer.
  - Symantec reserves the right to invoice Customer for additional Users, upon notification, for the remaining months on the Service contract where usage exceeds the message limit.
  - Inbound and outbound mail retry schedule = seven (7) calendar days.
  - Default maximum email size = fifty megabytes (50MB). Customer can specify any maximum Email size up to one thousand megabytes (1000MB). Any Emails that are received by the Service that exceed the specified limit will be blocked and deleted, and a notification alert Email will be sent to the sender, intended recipient, and an Administrator.
  - Message Tracing = data is available for troubleshooting searches for 30 days; additional limits apply to the number of results that can be returned by a single search.
  - Malware Quarantine = Emails are automatically deleted after thirty (30) days.
  - Spam Quarantine = Emails are automatically deleted after fourteen (14) days, unless otherwise configured.
  - Dashboard reporting data availability = forty (40) days for detailed information; twelve (12) months for summary information.
  - Summary (PDF) reporting data availability = twelve (12) months.
  - Detailed (CSV) reporting data availability = forty (40) days.

- The following limitations apply to Policy Based Encryption:
  - Policy Based Encryption (Z) outbound Emails per User per month = three hundred (300).
  - Policy Based Encryption Essentials/Advanced outbound Emails per User per month = four hundred and eighty (480).
  - When sending to multiple recipients, each unique address will be counted as a secure Email. In the event that Customer exceeds the number of permitted secure Emails in any calendar month, Symantec reserves the right to invoice Customer for actual usage.
  - Emails routed through the Policy Based Encryption Service are limited to a maximum size of fifty megabytes (50 MB).
  - If using Pull encryption with Policy Based Encryption (Z) service, by default, Emails will be stored for 90 days in the secure pickup portal before expiring.
  - If using Pull encryption with Policy Based Encryption Advanced service, by default, Emails will be stored for 30 days in the secure pickup portal before expiring.
  - The Availability and Latency Service Levels do not apply to this Service.

- To ensure that messages are secured at all points during transmission, Symantec recommends that Customer configure domains, that will be used for Policy Based Encryption, such that TLS encryption is enforced on all outbound and inbound messages to and from the Service Infrastructure.
- Customers must route their inbound Email through Symantec using the routing information provided by Symantec and must not route Email to a specific Tower or IP address.

- The Service is only available to a Customer who has its own Email domain name and has the ability to configure the MX records and/or DNS for that domain name.
- Customer must accept inbound Email from all required IP ranges to ensure continuity of service in the event that a portion of the Infrastructure is not available.
- Customer must specify the mail server IP address(es) or hostname(s) for the delivery of inbound Emails to their organization.
- Customer must ensure that all domains (including sub-domains) requiring the Service are provisioned. Customer accepts that Service features may not function correctly and Email delivery may be unavailable for domains that are not provisioned. Customer agrees to provide and maintain a list of valid Email addresses to receive the Service (the “Validation List”). It is Customer’s responsibility to verify the Validation List prior to the Service being made available and throughout the Term. Emails sent to Email addresses not on the Validation List, or incorrectly entered, will be rejected by the Service. Customer accepts that SLAs will not apply to Emails sent to invalid addresses. For the avoidance of doubt, Customers using the Spam Quarantine system must maintain a Validation List and have the Address Registration capability enabled. If Customer is unable to provide such Validation List and requests that the Address Registration capability is disabled, Symantec will review each such request on a case-by-case basis and reserves the right to decline requests, in Symantec’s sole and absolute discretion.
- Customer may release Emails that have been categorized as containing a Malware, or Spam, or request that Symantec release such Email, within Customer’s domain. CUSTOMER AGREES THAT SYMANTEC CANNOT ACCEPT ANY LIABILITY DUE TO THE RELEASE OF SUCH EMAILS ON CUSTOMER’S REQUEST.
- Symantec is not liable for any damage or loss resulting directly or indirectly from any failure of the Service to identify Spam or for wrongly identifying an Email as being Malware or Spam. Symantec reserves the right to scan all outbound Emails.
- A default disclaimer message will be applied to Emails that are scanned by the Service from the time of provisioning the Service, the text of which may be edited by Customer via the management console. Symantec reserves the right to update the default disclaimer message at any time.
- Customer shall comply with all applicable laws with respect to use of the Service. In certain countries, it may be necessary to obtain the consent of individual personnel. Configuration and use of the Service(s) is entirely in Customer’s control; therefore, Symantec is not liable for Customer’s use of the Service(s), nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.
- In the event that continued provision of the Service to Customer would compromise the security of the Service, including but not limited to hacking attempts, denial of Service attacks, mail bombs or other malicious activities either directed at or originating from Customer’s domains, Customer agrees that Symantec may temporarily suspend Service to Customer. In such an event, Symantec will promptly inform Customer and will work with Customer to resolve such issues. Symantec will reinstate the Service upon removal of the security threat.
- Should a Service be suspended for any reason whatsoever, the Service will not be applied to Customer’s Emails, and Emails will not be routed through Symantec’s Infrastructure. Customer is responsible for redirecting their Email during suspension and confirming that all configurations are accurate if the Service is reinstated.
- Should a Service be terminated for any reason whatsoever, Customer’s account will be deleted, and Customer will not have access to the Service.
- Customer shall not allow its systems to: (i) act as an Open Relay or Open Proxy; or (ii) send Spam. Symantec reserves the right at any time to review Customer’s compliance with this section. For the avoidance of doubt, any breach of this Clause will constitute a material breach of the Agreement and Symantec reserves the right to suspend all or part of the Service immediately and until the breach is remedied, or terminate the Agreement with respect to the affected Service.
- If at any time (i) Customer’s Email systems are blacklisted, or (ii) Customer causes the Symantec systems to become blacklisted due to the sending of Spam, or (iii) Customer fails to meet any of the obligations set out in this Service Description, Symantec shall inform Customer and reserves the right at its sole discretion to immediately withhold provision of, suspend or terminate all or part of the Service.
- Customer is permitted to use the Service solely for Customer's own business purposes. Customer agrees not to resell, sublicense, lease, or otherwise make the Service and associated documentation available to any third party. Customer agrees not to use the Service for the purposes of building a competitive product or service or copying its features or user interface, performing Service evaluations, benchmarking or other comparative analysis intended for publication outside Customer organization without Symantec’s prior written consent.

6: Definitions

"**Address Registration**" is a mandatory feature of the Service that rejects inbound Emails sent to Email addresses that are not included in Customer's list of valid Email addresses (the "Validation List").

"**Administrator**" means a Customer User with authorization to manage the Service on behalf of Customer. Administrators may have the ability to manage all or part of a Service as designated by Customer.

"**AntiSpam Best Practice Settings**" means Symantec's recommended configuration guidelines for the Service as provided to Customer during the provisioning process or as published in the online help resource.

"**Connection Manager**" means the detection methods which sit at the SMTP handshake stage.

"**Credit Request**" means the notification which Customer must submit to Symantec by Email to support.cloud@symantec.com with the subject line "Credit Request" (unless otherwise notified by Symantec).

"**Designated Tower Cluster**" means two (2) or more Towers designated to provide Email Security Services to Customer.

"**Domain Level Settings**" means domain settings that are customizable for a particular domain within the management console for the Email Security Services.

"**Email**" means any inbound or outbound SMTP message passing through the Service.

"**Email Security Services**" are the Email Safeguard and Email Protect options and any available add-on services.

"**Email Malware False Positive**" means a legitimate Email incorrectly identified as containing Malware.

"**End User License Agreement (EULA)**" means the terms and conditions accompanying Software (defined below).

"**Global Settings**" means the actions within the management console which are applied to all domains and group levels for the Services.

"**Group Level Settings**" means group settings that are customizable for a particular group within the management console for applicable features of the Service.

"**Infrastructure**" means any Symantec or licensor technology and intellectual property used to provide the Services.

"**Known Malware**" means Malware for which at the time of receipt of the content by Symantec, a signature has already been made available for a minimum of one (1) hour for use by antivirus technologies deployed by Symantec.

"**Malware**" or "**malicious software**" means any software used to disrupt computer or mobile operations, or without proper authorization, used to gather sensitive information and/or to gain access to private computer systems.

"**Malware False Positive**" means a legitimate Email incorrectly identified as containing a Malware.

"**Member**" means Customer and third parties with whom Customer creates an encrypted network by utilizing the legacy Email Boundary Encryption add-on Service.

"**Monthly Charge**" means the monthly charge for the affected Service(s) as defined in the Agreement.

"**Online Help**" means the additional information available at http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=EN_US.

"**Open Proxy**" means a proxy server configured to allow unknown or unauthorized third parties to access, store, or forward DNS, web pages or other data for the Service.

"**Open Relay**" means an Email server configured to receive Email from an unknown or unauthorized third party and forward the Email to one or more recipients that are not users of the Email system to which that Email server is connected. Open Relay may also be referred to as "Spam relay" or "public relay."

"**Order Confirmation**" has the meaning given in the Symantec Online Services Terms and Conditions, if applicable. If there are no such terms and conditions applicable to the Service, then "Order Confirmation" shall mean the Subscription Instrument, as defined herein.

"**Service**" means the Protect or Safeguard option of Symantec Email Security.cloud, purchased by Customer.

"**Service Component**" means certain enabling software, hardware peripherals and associated documentation which may be separately provided by Symantec as an incidental part of a Service.

"**Service Credit**" means the amount of money that will be credited to Customer's next invoice after submission of a Credit Request and validation by Symantec that a credit is due to Customer.

"**Service Software**" means Software (defined below), as may be required by a Service, which must be installed on each Customer computer, in order to receive the Service. Service Software includes the Software and associated documentation that may be separately provided by Symantec as part of the Service.

"**Software**" means each Symantec or licensor software program, in object code format, licensed to Customer by Symantec and governed by the terms of the accompanying EULA, including without limitation new releases or updates as provided hereunder.

"**Spam**" means unsolicited commercial Email.

"**Spam False Negative**" means a Spam Email that is not identified as Spam by the Service.

"**Spam False Positive**" means an Email incorrectly identified as Spam by the Service.

"**Spam Recommended Settings**" means Symantec's recommended configuration guidelines for the Service as provided to Customer during the provisioning process or as published in the online help resource.

"**Subscription Instrument**" means one or more of the following applicable documents which further defines Customer's rights and obligation related to the Service: a Symantec certificate or a similar document issued by Symantec, or a written agreement between Customer and Symantec, that accompanies, precedes, or follows the Service.

"**Symantec Hosted Service Terms**" means the Symantec Hosted Services Terms located at or accessed through https://www.symantec.com/about/legal/service-agreements.jsp.

"**Symantec Online Service Terms and Conditions**" means the Online Services Terms and Conditions located at or accessed through https://www.symantec.com/about/legal/service-agreements.jsp.

"**Symantec Tracker**" means a Symantec tool by which Service Availability and Latency are measured for the Service.

"**Tower**" means a cluster of load balanced Email servers.

"**User**" means an individual person sending and receiving email, and is protected by any portion of the Service.

Exhibit-A

Service Level Agreement

General

- Customer may be entitled to a Service Credit if Symantec does not meet the defined service level. If Customer believes it is entitled to a Service Credit, Customer must submit a Credit Request within ten (10) business days of the end of the calendar month in which the suspected service level non-compliance occurred. Customer recognizes that logs are only kept for a limited number of calendar days and therefore any Credit Request submitted outside of the provided timeframe will be deemed invalid.
- A Credit Request is made by contacting Symantec Technical Support. Please access the product support landing page for detailed instructions found here: https://support.symantec.com/en_US/email-security-cloud..html.
- All Credit Requests will be subject to verification by Symantec in accordance with the applicable provisions of this Service Level Agreement. Symantec may request additional information from Customer to validate the Credit Request.
- This Service Level Agreement will not operate: (i) during periods of Planned Maintenance or Emergency maintenance, periods of non-availability due to force majeure or acts or omissions of either Customer or a third party; (ii) during any period of suspension of service by Symantec in accordance with the terms of the Agreement; (iii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); (iv) where Customer has not configured the Service in accordance with the Agreement; or (v) during trial service periods.
- The remedies set out in this Service Level Agreement shall be Customer's sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise, with respect to this Service Level Agreement.
- The maximum accumulative liability of Symantec under this Service Level Agreement in any calendar month shall be a credit equal to the lower of 100% of the Monthly Charge or ten thousand dollars/five thousand pounds sterling/ten thousand euro ($10,000/£5,000/€10,000) (depending on the currency in which Customer is invoiced).
- If the affected Service is purchased as part of a Services bundle, then the Service Credit will be calculated based on the affected Service and not on the entire Services bundle.

Exceptions to Service Level Agreement for Email Security Services

This Service Level Agreement will not operate: (i) in respect of any Emails that have not passed through the Service (including without limitation if Customer has not taken appropriate steps to ensure that it will only accept inbound Email from the Symantec Infrastructure); (ii) in respect of any inbound or outbound Emails that were initially sent to Symantec containing more than 500 recipients per SMTP session, (iii) for any Customers provisioned on any Tower designated as a Bulk Cluster Tower, or (iv) in respect of any inbound or outbound Emails for Customer domains that are not provisioned for the Service.

Service Availability

The Service Availability Service Level is defined by the ability to establish an SMTP session on port 25 from the Customer MTA to the Symantec Infrastructure, in compliance with RFC5321. The Service Availability Service Level does not apply to the management portal or spam quarantine system. This service level shall not apply if the Customer has incorrectly configured the Service or due to unforeseen circumstances or causes beyond Symantec's reasonable control, including but not limited to natural disaster, war, terrorism, riot, government action, or a network or device failure external to Symantec's data centers, including at Customer's site or between Customer's site and Symantec's data center.

If Service Availability is below one hundred percent (100%) in any calendar month, Customer may submit a Credit Request and may receive a Service Credit for the following percentage credit equal to the lower of 100% of the Monthly Charge or ten thousand dollars/five thousand pounds sterling/ten thousand euro ($10,000/£5,000/€10,000) (depending on the currency in which Customer is invoiced):

Percentage Available Per Calendar Month	Percentage Credit Of Monthly Charge
below 100% and above or equal 99%	25%

below 99% and above or equal 98%	50%
below 98%	100%

If Service Availability falls below ninety-eight percent (98%) in any calendar month, as confirmed by Symantec, Customer shall be entitled to terminate the affected Service and receive a pro-rata refund of fees paid in advance for the portion of the term after such termination is effective.

Email Delivery

The Email Delivery Service Level is defined by Symantec's ability to deliver 100% of all Email sent to or from Customer subject to the following conditions:

a) The Email must have been received by Symantec; and

b) The Email must not contain a Malware, Spam or other content which has caused it to be intercepted by the Service.

Subject to the conditions above, in the event Symantec fails to deliver an Email to or from Customer, and Customer is not in breach of the terms of the Agreement, Customer is entitled to terminate the Service upon thirty (30) calendar days prior written notice.

Email Latency

The Email Latency Service Level is defined by whether the average round trip time, as measured by the Symantec Tracker, for Emails sent every five (5) minutes to and from every tower within Customer's Designated Tower Cluster exceeds the delays stated in the table below, in a calendar month. If Customer believes that the Latency Service Level has not been met, Customer may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Average Round Trip Time (seconds)	Percentage Credit Of Monthly Charge
above 60 and below or equal 90	25%
above 90 and below or equal 120	50%
above 120 and below or equal 180	75%
above 180	100%

This Latency Service Level will not apply if:

a) Customer has not supplied Symantec with a Validation List and Customer suffers a denial of service attack;

b) Periods of delay are caused by a mail loop from/to Customer systems; or

c) Customer's primary Email server is unable to accept Email on the initial attempted delivery.

Spam False Positives

The Spam False Positive Service Level defines the maximum Spam False Positive Capture Rate. The Spam False Positive Service Level will only apply if Customer implements the AntiSpam Best Practice Settings as provided in the Online Help resource. If the average Spam False Positive capture rate rises above 0.0003% of Customer's inbound Email traffic in any calendar month, Customer may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Spam False Positive Capture Rate %	Percentage Credit Of Monthly Charge
above 0.0003 and below or equal 0.003	25%
above 0.003 and below or equal 0.03	50%

above 0.03 and below or equal 0.3	75%
above 0.3	100%

The following Emails do not constitute Spam False Positive Emails for the purposes of this service level:
a) Emails that are not legitimate business Email;
b) Emails containing more than 20 recipients;
c) Emails where the sender of the Email is on Customer's blocked senders list, including without limitation, those defined by the individual user if Customer has enabled user-level settings;
d) Emails that are sent from a compromised machine;
e) Emails that are sent from a machine which is on a third party block-list;
f) Emails intercepted by outbound Spam scanning.

In order to be eligible for a Service Credit, Customer must report suspected false positive Emails to Symantec Technical Support within five (5) calendar days of receipt of the Email. Symantec will investigate and confirm whether or not the Email is a Spam False Positive and will record the finding.

Spam Capture Rate

The Spam Capture Rate Service Level defines the minimum Spam Capture Rate. This service level will only apply if Customer implements the AntiSpam Best Practice Settings as provided in the Online Help resource. The service level corresponds to the number of Spam False Negatives measured in a calendar month. Customer may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Spam Capture Rate %	Percentage Credit Of Monthly Charge
above 98 and below or equal 99	25%
above 97 and below or equal 98	50%
above 96 and below or equal 97	75%
below 96	100%

This Spam Capture Rate Service Level will not apply if the Email was not sent to a valid Email address. A lower Spam Capture Rate of ninety-five percent (95%) shall apply to Emails containing more than fifty percent (50%) Double Byte character sets. In the event that such Spam Capture Rate falls below ninety-five percent (95%), Customer shall be entitled to a twenty-five percent (25%) Service Credit of the monthly charge. In the event that the Spam Capture Rate falls below ninety percent (90%), Customer may be entitled to a Service Credit equal to one hundred percent (100%) of the monthly charge.

In order to be eligible for a Service Credit, Customer must report suspected false negative Emails to Symantec Technical Support within five (5) calendar days of receipt of the Email. Symantec will investigate and confirm whether or not the Email is a Spam False Negative and will record the finding.

Malware Protection

If Customer systems are infected by known or unknown Malware that propagates via Email(s) passed through the cloud scanning service, Customer may be entitled to a Service Credit in the amount defined below. Customer must notify Symantec within five (5) days of learning of such Malware and such notification must be logged, investigated, and validated by Symantec. Customer must submit a Credit Request, and if validated, will receive a Service Credit equal to the lower of one hundred percent (100%) of the Monthly Charge or ten thousand dollars/five thousand pounds sterling/ten thousand euro ($10,000/£5,000/€10,000) (depending on the currency in which Customer is invoiced). The remedy set out in this section shall be the sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise in respect of any infection by a Malware passed to

Customer or a third party through the Service. For the avoidance of doubt, the remedy set out in this section shall not apply in cases of deliberate self-infection.

Customer systems are deemed to be infected if a Malware attached to an Email was received through the Service and the Malware has been activated within Customer's system(s) either automatically or with manual intervention. In the event that Symantec detects, but does not stop an Email with a Malware attachment, and publishes an update on the Symantec Status Page or otherwise notifies Customers, providing sufficient information to enable Customer to identify and delete the infected Email, the remedy set out above shall not apply.

The Service will scan as much of the Email and its attachments as possible. It may not be possible to scan attachments with content that is under the direct control of the sender (*e.g.*, password protected and/or encrypted attachments and/or the password is sent separately from the Email). Such Email and/or attachments are excluded from the service level, and the remedy set out above shall not apply.

This Malware Protection Service Level shall not operate in relation to Malware that have been intentionally released by Customer or by Symantec at Customer's request.

This Malware Protection Service Level shall only apply to Malware as defined in this Service Description, and will not apply to the following: spyware, adware, URL links to websites hosting malicious content, or unknown trojans.

Malware False Positive

The Malware False Positive Service Level defines the maximum Malware False Positive Capture Rate. If the Email Malware False Positive capture rate rises above 0.0001% of Customer's Email traffic in any calendar month Customer may submit a Credit Request and may receive a Service Credit in accordance with the table below:

Malware False Positive Capture Rate %	Percentage Credit Of Monthly Charge
above 0.0001 and below or equal 0.001	25%
above 0.001 and below or equal 0.01	50%
above 0.01 and below or equal 0.1	75%
above 0.1	100%

24x7 Technical Support and Fault Response

Technical Support is available twenty-four (24) hours/day, seven (7) days/week to:
a) provide technical support to Customer for problems with the Service; and
b) communicate with Customer to resolve such problems.