Symantec Email Security.cloud

Saas Listing

The definitions set out in the Agreement will apply to this SaaS Listing document.

The CA software program(s) ("CA Software") listed below is provided under the following terms and conditions in addition to any terms and conditions referenced on the CA quote or other transaction document entered into by you and the CA entity ("CA") through which you obtained a license for the CA Software (hereinafter referred to as the "Agreement"). These terms shall be effective from the effective date of such ordering document.

This SaaS Listing describes Email Security.cloud ("Service"). All capitalized terms in this Listing have the meaning ascribed to them in the Agreement (defined above) or in the Definitions section

Table of Contents

Symantec Email Security.cloud

Saas Listing

1: Technical/Business Functionality and Capabilities

Service Overview

Symantec Email Security.cloud ("Service") 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. The Service receives, processes and delivers Email from a common, shared, multi-tenanted infrastructure.

Service Features

- Customer can access the Service through a self-service online portal ("Portal"). Customer may configure and manage the Service, access reports, and view data and statistics, through the Portal, 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 Portal.. Reporting may include activity logs and/or statistics. Customer may choose to generate reports, which can be configured to be sent by email on a scheduled basis, or downloaded from the Portal. 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 CA may contain words which may be considered offensive.
- Should a Service be suspended or terminated for any reason whatsoever, CA will 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.
- The Service must be purchased for each User of the selected option or add-on (subject to any restrictions described in this SaaS Listing).
- The Service is for use with normal external business messaging traffic only, and Customer shall not use the Service for machine-generated message delivery of bulk or unsolicited emails or emails sent from an account not assigned to an individual User.

Features included with the Email Safeguard solution include:

- 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, API and Notifications
- Disclaimer Management
- Policy Based Encryption Essentials
- Email Impersonation Controls

Symantec Email Security.cloud

Saas Listing

Additional information on individual Service features is available in the online help at https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/email-security-cloud/1-0.html.

Service Add-Ons

- **Email Threat Detection and Response:**
    - Email Threat Detection and Response (ETDR) 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.
    - ETDR can pull back emails that are determined to be malicious post-delivery by our Cynic™ sandbox for O365 customers. Additionally, ETDR can help customers remediate email attacks by blacklisting emails based on indicators of compromise.
    - ETDR 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.
    - ETDR includes Email Threat Isolation which strengthens protection against spear phishing, credential theft, and advanced email attacks by isolating malicious links and by safely rendering risky webpages. Email Threat Isolation creates a secure execution environment between users and their email links or attachments, by executing web sessions remotely and only sending safe rendering information to users' browsers. As a result, CA helps stop threats that contain malicious links and attachments from reaching users.
    - Email Threat Detection and Response also provides access to the Phishing Readiness service, a phishing attack simulator used to determine the susceptibility of personnel to such attacks. The Service includes simulated phishing assessments and templates which address the most common attack types:
        - Open/Click Assessment: This test will measure which of the targeted Users will open, load remote content, and subsequently click any links in messages.
        - Data Exposure Assessment: This test aims to convince Users to enter additional sensitive data into a form or application on a malicious website.
        - Attachment Assessment: This test aims to entice Users to open a malicious attachment.

      The Service includes pre-loaded templates for each assessment type that can be further customized by Customer to match specific organizational branding, messaging, or culture. In addition, Customer may create its own original templates. The Service provides a private portal to view reports, data, and metrics for each simulated phishing assessment. This data may be used in demonstrating the effectiveness of personnel awareness training and/or susceptibility to real-world phishing attacks. It also can identify persons and groups who are unintentionally exposing the Customer to the risk of compromise through the phishing attack type.
- **Policy Based Encryption Advanced:** 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, CA 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 CA.
- **PGP Encryption Service for Email Security:** PGP Encryption Service for Email Security 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). PGP Encryption Service for Email Security 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 PGP Encryption Service for Email Security option for secure statement delivery, CA 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 CA.
- **Email Fraud Protection:** 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. Email Fraud Protection is also available as a stand-alone service. This add-on Service has a separate SaaS Listing located https://www.broadcom.com/company/legal/licensing and use of this add-on Service is governed by that SaaS Listing.

Symantec Email Security.cloud

Saas Listing

- **Email Threat Isolation Stand-alone Service:** 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 creates a secure execution environment between users and their email links or attachments, by executing web sessions remotely and only sending safe rendering information to users' browsers. As a result, CA helps stop threats that contain malicious links and attachments from reaching users. Email Threat Isolation is included in the Email Threat Detection and Response (ETDR) add-on offering and is also available as a stand-alone service. This add-on Service has a separate SaaS Listing located https://www.broadcom.com/company/legal/licensing and use of this add-on Service is governed by that SaaS Listing.

Supported Platforms and Technical Requirements

- Supported platforms for the Service are defined at https://techdocs.broadcom.com/us/en/symantec-security-software/email-security.htm.

Service Software Components

- The Service includes the following software components:
    - Synchronization tool
- The use of any software component is governed by the Agreement and, if applicable, any additional terms published with this SaaS Listing on https://www.broadcom.com/company/legal/licensing.

2: Customer Responsibilities

CA can only perform the Service if Customer provides required information or performs required actions, otherwise CA's performance of the Service may be delayed, impaired or prevented, and Customer may lose eligibility for any Service Level Agreement.

- Setup Enablement: Customer must provide information required for CA to begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist CA in delivery of the Service.
- Renewal Credentials: If applicable, Customer must apply renewal credential(s) provided in the applicable 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 Subscription 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, CA 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.

3: Entitlement and Subscription Information

Charge Metrics

The Service is available under one of the following Meters as specified in the Order Confirmation:

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

4: Customer Assistance and Technical Support

Customer Assistance

CA 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

If CA is providing Technical Support to Customer, Technical Support is included as part of the Service as specified below. If Technical Support is being

Symantec Email Security.cloud

Saas Listing

provided by a reseller, this section does not apply.

- Support for Services will be performed in accordance with the published terms and conditions and technical support policies published in the "Broadcom Software Maintenance Policy Handbook" at https://support.broadcom.com/external/content/release- announcements/CA-Support-Policies/6933.

Maintenance to the Service and/or supporting Service Infrastructure

CA must perform maintenance from time to time. For information on Service status, planned maintenance and known issues, visit https://status.broadcom.com/. The following applies to such maintenance:

- **Planned Maintenance:** Planned Maintenance means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. 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, CA will provide seven (7) calendar days' notification.
- **Unplanned Maintenance**: Unplanned Maintenance means scheduled maintenance periods that do not allow for seven (7) days notification and during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. CA will provide a minimum of one (1) calendar day notification. 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 CA 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. Notification of Emergency Maintenance will be provided as soon as practicable.
- **Note:** For Management Console Maintenance, CA will provide fourteen (14) calendar days' notification. CA may perform minor updates or routine maintenance to the Management Console with no prior notification as these activities do not result in Service disruption.

5: Additional Terms

CA may modify the Online Services and/or the corresponding SaaS Listings at any time: (a) due to changes in applicable laws or industry standards; and (b) for any other reason, if the modification does not materially reduce the level of performance, functionality, security or availability of the Online Services during the Subscription Term.

- Any templates supplied by CA 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.
    - CA 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.
    - If at any time the Customer's email systems are being used for bulk email or spam, CA reserves the right to suspend all or part of the Service immediately and until such use is terminated.
    - 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:

Symantec Email Security.cloud

Saas Listing

- 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, CA 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 (50MB).
- 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.
- The Availability and Latency Service Levels do not apply to this Service.

- The following limitations apply to PGP Encryption Service for Email Security:
  - PGP Encryption Service for Email Security 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, CA reserves the right to invoice Customer for actual usage.
  - Emails routed through the PGP Encryption Service for Email Security Service are limited to a maximum size of fifty megabytes (50MB).
  - If using Pull encryption with PGP Encryption Service for Email Security, by default, Emails will be stored for 90 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, CA 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 CA using the routing information provided by CA 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 has the option 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, CA will review each such request on a case-by-case basis and reserves the right to decline requests, in CA’s sole and absolute discretion.
- Customer may release Emails that have been categorized as containing a Malware, or Spam, or request that CA release such Email, within Customer’s domain. CUSTOMER AGREES THAT CA CANNOT ACCEPT ANY LIABILITY DUE TO THE RELEASE OF SUCH EMAILS ON CUSTOMER’S REQUEST.
- CA is not liable for any damage or loss resulting directly or indirectly from any failure of the Service to identify Spam or Malware for wrongly identifying an Email as being Malware or Spam. CA 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. CA 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, CA 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 CA's ability to deliver service to other customers, including but not limited to hacking attempts, denial of Service attacks, mail bombs or other malicious activities originating from Customer's domains, Customer agrees that CA may, as a final resort, temporarily suspend Service to Customer. Whenever possible, any suspension above will be limited to the single user email account(s) causing the compromise. CA will promptly inform Customer and will work with Customer to resolve such issues.
- In the event that malicious activities, including but not limited hacking attempts, denial of Service attacks, or mail bombs are directed at Customer's domains, CA will promptly inform Customer and will work with Customer to resolve such issues.
- 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 CA's infrastructure. CA is responsible for the full backup and restoration of the Customer configuration. CA will restore the Customer configuration to same state it was in prior to such interruption. Notwithstanding the foregoing, when the Service is restored, Customer is responsible for redirecting Customer's Email back to the Service (example: update MX record changes on their infrastructure).
- Should a Service be terminated for any reason whatsoever, Customer's account will be suspended and/or deleted, and Customer will not have access to the Service.
- If Customer relays outbound email through the Service, Customer shall not allow its systems to: (i) act as an Open Relay or Open Proxy; or (ii) send Spam. CA 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 CA 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 CA systems to become blacklisted due to the sending of Spam, or (iii) Customer fails to meet any of the obligations set out in this SaaS Listing, CA 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 CA's prior written consent.
- CA is free to provide the Service from any data center forming part of the Service anywhere in the world and may, at any time and without further notice, transfer the provision of the Service from one installation to another. CA generally endeavours to provide i) Customers in the United States from a data center within the United States, including any data center used for purposes of system failover and ii) Customers based in the European Union (EU) or European Economic Area (EEA) from a data center in a country within the EU or EEA, including any data center used for purposes of system failover.
- The following limitations apply to Phishing Readiness:
    - Administrator Roles: There are three (3) levels of administrator access: Full Admin, Manager, and Platform User. Customer determines which personnel resources are assigned to each type of role.
    - There is no limit to the number of phishing campaigns that Customer can run during the Subscription Term.
    - Templates are provided in English. Customer is permitted to translate the templates and content into other languages for use during Subscription Term.
    - Training Message: For each assessment, a specific training message and schedule can be created according to Customer policies. Users that do not complete the training immediately after clicking on a phishing link will be reminded via email to return to complete the training.
    - Customer must take action to authorize the Symantec Phishing Readiness mail servers to send Email to Customer personnel. This may require "white-listing" by IP address, creating exceptions in Email filtering gateways, or bypassing other protection or inspection mechanisms that may block suspicious, malicious or suspect Email. The IP addresses of the Service's Email servers are available in the Symantec Phishing Readiness Help Center (accessible from the Platform). Other key filtering attributes such as Email headers and content tokens that can be used for Email filter bypass are also available in the Symantec Phishing Readiness Help Center.
    - Customer must not undertake to perform any phishing campaigns that contain any third party trademarks, copyrighted content or other protected items or material ("Intellectual Property") without prior express written permission from the owners of the

Intellectual Property. If a third party submits a complaint alleging infringement upon their Intellectual Property rights, CA will direct them to Customer for resolution of the matter. Customer will reply to any third party abuse complaints in a timely manner.

6: Data Export

Customer can export a wide variety of data from the Portal. Data is available as comma-separated value (CSV) files for greater interoperability. Some summary reports are also available as PDF files for higher-level review. Customer can export data using the following reports:

Email Data

- Email Summary Report
- Email Detailed Report
- Email Configuration Report

Portal Audit Data

- Audit Detailed Report: contains detailed information about Customer's domains.

Core Email Reports

- Service Summary: includes Portal login and service subscription reports.
- Service Details: includes reports that cover Scan-time policy incidents and Portal login details.
- Service Statistics: includes reports on mail queue lengths, Threat Isolation incidents, and spam and malware sample submissions.
- Configuration Snapshot Reports: includes details about Customer's current service configurations, including custom domains, anti-spam, anti-malware, image control, data protection, threat detection and isolation, protection policies, encryption, email platform specifics, email address registration, Portal users and permissions, and third-party domains.
- Audit Reports: includes anti-spam and anti-malware basic configuration, blocked and approved senders, data protection configuration, policy details, and custom lists and groups. Also includes Portal users, user permissions, and IP address usage audit.

Non-exportable Data

Broadcom does not export secret materials that are related to credentials or tokens.

7: 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.

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

"Assessment" means a simulated phishing campaign sent to a group or list of targets.

"Bulk Mail Cluster" is a designated tower cluster intended for use only by bulk mail applications (non-user traffic).

"**CA Online Service Terms and Conditions**" means the terms and conditions located at or accessed through https://www.broadcom.com/company/legal/licensing.

"Designated Tower Cluster" means two (2) or more Towers designated to provide the Service to Customer.

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

Symantec Email Security.cloud

Saas Listing

“Email Malware False Positive” means a legitimate Email incorrectly identified as containing Malware.

“Infrastructure” means any CA or licensor technology and intellectual property used to provide the Services.

“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.

“Online Help” means the additional information available at: https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/email-security-cloud/1-0.html.

“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 CA Online Services Terms and Conditions.

“Phishing Readiness Help Center” means the online Support and Knowledge Base available from within the Platform.

“Service Credit” means the number of days that are added to Customer’s current Subscription Term.

“Service Infrastructure” means any CA or licensor technology and intellectual property used to provide the Services.

“Spam” means unsolicited bulk Email.

“Spam False Positive” means an Email incorrectly identified as Spam by the Service.

“Symantec Tracker” means a CA tool by which Service Availability and Latency are measured for the Service.

“Target” means an email address that will be sent a phishing assessment message**.**

“Tower” means a cluster of load balanced Email servers.

“User” means an individual person sending and receiving email, and that is protected by any portion of the Service.

Symantec Email Security.cloud

Saas Listing

Exhibit-A

Service Level Agreement(s)

1.0 GENERAL

These Service Level Agreements ("SLA(s)") apply to the Online Service that is the subject matter of this SaaS Listing only. If CA does not achieve these SLA(s), then Customer may be eligible to receive a Service Credit. Service Credits are Customer's sole and exclusive remedy and are CA's sole and exclusive liability for breach of the SLA.

2.0 SERVICE LEVEL AGREEMENT(S)

a. **Availability.** This SLA applies to the following: Email Safeguard, Email Threat Detection and Response. Availability is the amount of time that the Service is operational in minutes, expressed as a percentage per calendar month, excluding Excused Outages. Availability SLAs may exist for i) Inline (Data Plane) Service, and ii) Non-Inline (Control Plane) Service, separately:

- **Inline Service Availability** means access to the core features of the Service that impact the data in transit to and from Customer to the Internet. Inline features of the Service means the availability of Service Infrastructure for Customer's Mail Transfer Agent (MTA) to establish a SMTP session on port 25, in compliance with RFC5321. This SLA does not apply to the management console or spam quarantine system.

Inline Service Availability	**99.999%**

- **Non-inline Service Availability** is access to the controls that govern the features of the Service that do not impact data in transit to and from the end-user to the Internet (e.g., reporting tools used by the administrator).

Non-Inline Service Availability	**N/A**

b. **Other SLAs:** All Other SLAs only apply to Emails received by the Service.

- **Email Latency**: Customer may request a Service Credit if the time from an Email is accepted by the Service to the time the Email is sent from the Service Infrastructure to the intended recipient(s) exceeds the average round trip time stated below, as measured by the Symantec Tracker. Latency SLA will not apply if: a) Customer has not supplied CA 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 unreachable or unable to accept Email on the initial attempted delivery. Email Latency is measured as a percentage of all emails sent to or from Customer handled by the Service in a calendar month.

Average Round Trip Time	**60 Seconds**

- **Email Delivery**: Customer may request a Service Credit if CA fails to deliver Email sent to or from Customer subject to the following conditions: a) The Email must have been received by CA; and b) The Email must not contain a Malware, Spam or other content which has caused it to be intercepted by the Service. Email Delivery SLA will not apply if recipient's email server(s) as configured in the service or DNS is/are unreachable or unable to accept the Email according to the configured retry schedule, or if the recipient's email server rejects the email. Email Delivery is measured as a percentage of all emails sent to or from Customer handled by the Service in a calendar month.

Email Delivery	**100%**

- **Spam False Positive**: This SLA applies to the following: Email Protect and Email Safeguard. Customer may request a Service Credit when the number of legitimate business emails misidentified by the Service as Spam exceeds the Spam False Positive capture rate below, subject to Customer implementing the Anti Spam Best Practice Settings as provided in the Online Help resource. Spam False Positive is measured as a percentage of all emails sent to Customer handled by the Service in a calendar month. The following Emails do not constitute Spam False Positive Emails for the purposes of this SLA: 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 CA within five (5) calendar days of receipt of the Email. CA will investigate and confirm whether or not the Email is a Spam False Positive and will record the finding.

Spam False Positive Capture Rate	No more than 0.0003%

- **Spam Capture Rate**: This SLA applies to the following: Email Protect and Email Safeguard. Customer may request a Service Credit if the Service fails to identify the minimum percentage stated below of Emails containing Spam sent to Customer, subject to Customer implementing the AntiSpam Best Practice Settings as provided in the Online Help resource. Spam Capture Rate is measured as a percentage of all Emails sent to Customer handled by the Service in a calendar month. This Spam Capture Rate SLA will not apply if the Email was not sent to a valid Email address. In order to be eligible for a Service Credit, Customer must report suspected false negative Emails to CA within five (5) calendar days of receipt of the Email. CA will investigate and confirm whether or not the Email is a Spam False Negative and will record the finding.

Spam Capture Rate	99%
Spam Capture Rate SLA where Emails contain more than 50% Double Byte character sets	**95%**

- **Malware Protection**: This SLA applies to the following: Email Protect and Email Safeguard. Customer may request a Service Credit if Customer's system is infected by known or unknown Malware that propagates via Email(s) passed through the Service. 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. The following are excluded from the Malware Protection SLA: (a) Malware that CA detects, but does not stop, in an Email attachment, where CA publishes an update on the or otherwise notifies Customers, providing sufficient information to enable Customer to identify and delete the infected Email; (b) 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); or (c) Malware that has been intentionally released by Customer or by CA at Customer's request. This Malware Protection SLA shall only apply to Malware as defined in this SaaS Listing, and will not apply to the following: spyware, adware, URL links to websites hosting malicious content, or unknown trojans. Malware Protection is measured as a percentage of all email sent to or from the Customer handled by the Service in a calendar month. Customer must notify CA within five (5) days of learning of such Malware and such notification must be logged, investigated, and validated by CA.

Malware Protection SLA	100%

- **Malware False Positive**: This SLA applies to the following: Email Protect and Email Safeguard. Customer may request a Service Credit if the number of legitimate business Emails incorrectly identified as containing Malware exceeds the maximum Malware False Positive capture rate stated below. The Maximum False Positive capture rate is measured as a percentage of all Emails sent to or from Customer handled by the Service in a calendar month.

Malware False Positive Capture Rate	No more than 0.0001%

3.0 AVAILABILITY CALCULATION

Availability is calculated as a percentage of 100% total minutes per calendar month as follows:

$$\frac{\text{Total Minutes in Calendar Month} - \text{Excused Outages} - \text{Non-Excused Outages*}}{\text{Total} - \text{Excused Outages}} \times 100 > \text{Availability Target}$$

**Non-Excused Outages = Minutes of Service disruption that are not an Excused Outage*

Note: The availability calculation is based on the entire calendar month regardless of the Service start date.

4.0 SERVICE CREDIT

If a claim is made and validated, a Service Credit will be applied to Customer's account.

CA will provide a Service Credit equal to two (2) days of additional service for each 1 hour or part thereof (aggregated) that the service is not available in a single 24-hour period, subject to a maximum of seven (7) calendar days for all incidents occurring during that 24 hour period. A Customer may only receive up to twenty-eight (28) days maximum, for up to four (4) Service Credits, over twelve (12) months. The maximum is a total for all claims made in that twelve (12) month period.

Symantec Email Security.cloud

Saas Listing

Service Credits:

- May not be transferred or applied to any other CA Online Service, even if within the same account.
- Are the only remedy available, even if Customer is not renewing for a subsequent term. A Service Credit is added to the end of Customer's current Subscription Term.
- May not be a financial refund or credit of any kind.
- Do not apply to failure of other service level SLAs if such failure relates to non-availability of the Service. In such cases Customer may only submit a claim for the Availability SLA.

5.0 CLAIMS PROCESS

Customer must submit the claim in writing via email to CA Customer Support. Each claim must be submitted within ten (10) days of the end of the calendar month in which the alleged missed SLA occurred for CA to review the claim. Each claim must include the following information:

(i) The words "Service Credit Request" in the subject line.
(ii) The dates and time periods for each instance of claimed outage or other missed SLA, as applicable, during the relevant month.
(iii) An explanation of the claim made under this SaaS Listing, including any relevant calculations.

All claims will be verified against CA's system records. Should any claim be disputed, CA will make a determination in good faith based on its system logs, monitoring reports and configuration records and will provide a record of service availability for the time period in question to Customer.

6.0 EXCUSED OUTAGES AND EXCLUSIONS TO CLAIMS

The following are minutes of downtime that are defined as Excused Outages:

- Planned Maintenance and Unplanned Maintenance as defined in the SaaS Listing.
- Force Majeure as defined in the Agreement.
- Any downtime that results from any of the below listed exclusions to a claim.

If any of the following exclusions apply, a claim will not be accepted:

- Any Service provided on a provisional basis, including but not limited to: trialware, evaluation, Proof of Concept, Not for Resale, pre-release, beta versions.
- Customer has not paid for the Service.
- Third party, non-CA branded products or services resold with the Service.
- Hardware, software or other data center equipment or services not in the control of CA or within the scope of the Service.
- Any item that is not a Service Component that is provided for use with the Service.
- Technical support provided with the service.
- Failure of Customer to correctly configure the Service in accordance with this SaaS Listing.
- Hardware or software configuration changes made by the Customer without the prior written consent of CA.
- Unavailability of a specific web page or a third party's cloud application(s).
- Unavailability of one or more specific features, functions, or equipment hosting locations within the service, while other key features remain available.
- Failure of Customer's internet access connections.
- Suspension and termination of Customer's right to use the Service.
- Alterations or modifications to the Service, unless altered or modified by CA (or at the direction of or as approved by CA
- Defects in the Service due to abuse or use other than in accordance with CA's published Documentation unless caused by CA or its agents.
- Customer-requested hardware or software upgrades, moves, facility upgrades, etc.

Service-specific exclusions: For Email Security.cloud, SLAs will not apply: (i) to 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 Service Infrastructure); (ii) to 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) to any inbound or outbound Emails for Customer domains that are not provisioned for the Service.

END OF EXHIBIT A