Web Security Service

Service Description

June 2019

This Service Description describes Symantec's Web Security Service("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 Online Services Terms and Conditions published with the Service Description at www.symantec.com/about/legal/repository (hereinafter referred to as the "Agreement").

Table of Contents

Web Security Service

Service Description

June 2019

1: Technical/Business Functionality and Capabilities

Service Overview

Web Security Service ("Service") enforces granular access and security policies that manage web internet usage by application, device, user, or location.

Service Features

- The Service helps to protect web traffic, users and devices via cloud-delivered security service.
- 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.
- The Service is intended to enable Customer to implement a valid and enforceable computer use policy, or its equivalent.
- Reporting for the Service is available through the Portal. Reporting may include activity logs and/or statistics. Customer may choose to generate reports through the Portal, which can be configured to be sent by email on a scheduled basis, or downloaded from the Portal.
- The Service includes one hundred (100) days of reporting. Longer log retention options are available for a fee.

Service Level Agreement

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

Service Software Components

- The Service includes the following software components:
    - Auth Connector: This software is required to import users, groups information to the Service
    - WSS Agent (Optional): If purchased, can be deployed on endpoints to connect to the Service.
- The use of any software component is governed by the Agreement and, if applicable, any additional terms published with this Service Description on www.symantec.com/about/legal/repository.

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 Customer may lose eligibility for any Service Level Agreement.

- 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.
- 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 Portal, 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.
- Customer must provide accurate and complete information regarding usage for calculating the Meter and/or applicable Fees.

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 authorized to use and/or benefit from the use of the Service, or that actually uses any portion of the Service. A User may have up to two (2) devices under the Web Security Subscription, and two (2) additional devices under the Mobile Device Security Subscription. In addition, a "User" may be calculated by Symantec at its sole discretion through counting the number of devices or measuring equivalent activity/expected data consumption for an individual person where usage by individuals cannot be determined.
- "**Unit**" means the number of instances of Cloud-HSM that are integrated with WSS and are managed by Customer. This Unit meter is available for the Self-Managed Certificate Service as an add-on feature (separate purchase required).

4: Customer Assistance and Technical Support

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

If Symantec is providing Technical Support to Customer, Technical Support is included as part of the Service as specified below. If Technical Support is being provided by a reseller, this section does not apply.

- 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 substantial loss of service; or (ii) a substantial portion of Customer's mission critical data is at a significant risk of loss or corruption.	Within 30 minutes
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. For information on Service status, planned maintenance and known issues, visit https://status.symantec.com/ and subscribe to Symantec Status email service to receive the latest updates. 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, Symantec will provide 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 seven (7) days notification and during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. Symantec will provide a minimum of one (1) calendar day notification posted on the 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. Notification of Emergency Maintenance will be provided as soon as practicable.
- **Note:** For Management Console Maintenance, Symantec will provide fourteen (14) calendar days' notification posted on Symantec Status Page. Symantec 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

- *Additional terms and conditions that may apply to the Service are available at: https://www.symantec.com/content/dam/symantec/docs/eulas/third-party-notice/blue-coat-products-third-party-en.pdf.*
- *Excessive Consumption. If Symantec determines that Customer's aggregate activity on the Service imposes an unreasonable load (Customer's average per User usage is greater than the average per User usage generated by 95% of inline Users of the Service on a monthly basis) on bandwidth, infrastructure, or otherwise, Symantec may impose controls to keep the usage below excessive levels. Upon receiving Service notification (e.g., email) of excessive (vs. expected) usage, Customer agrees to remediate their usage within ten (10) days, or to work with its reseller to enter into a separate fee agreement for the remainder of the Subscription Term. Symantec reserves the right to manage bandwidth and route traffic in a commercially optimal way, including without limitations, diverting traffic from well-known media streaming, trusted software update sites and cloud-based backup sites to the extent not posing any material security threat to Users, and providing guidance to Customer on ways that Customer can control bandwidth usage by bypassing such sites.*
- *User Count. In the event that Customer exceeds its authorized Users (as measured in Symantec's reporting system or as otherwise calculated by Symantec), Customer agrees to promptly pay the amounts invoiced for the excess usage and/or submit a new order for the excess use. In addition, the parties agree to meet in good faith to determine the number of new User subscriptions required by Customer for the remainder of the Subscription Term.*

- *Optional add-on services may be available with the Service and will be provided in accordance with their documentation.*

- *Symantec Endpoint Protection. Customers that have both a Symantec Endpoint Protection ("SEP") subscription and Service subscription are given access to use the WSS Traffic Redirection ("WTR") feature. If Customer enables the WTR feature, Symantec will install a TLS root certificate authority ("CA") on each authorized Device (as defined in the SEP Product Use Rights Supplement). The CA permits the Service to intercept and inspect encrypted traffic, and is necessary for the Service to operate with encrypted (HTTPS) traffic. If the CA was installed by SEP, the CA will be removed when the WTR feature is disabled. Symantec will use intercepted traffic to authenticate traffic as originating from a valid User of the Service, carry out processing of traffic as configured within the Service and for delivery of error responses. Use of the WTR feature is intended only for Customers who have valid subscriptions for both SEP and the Service. Symantec makes no claim of support or viability for the WTR feature to be used for any other purpose.*

6: Definitions

"**Administrator**" means Customer's designated personnel to manage the Service on behalf of Customer.

"Mobile Device Security Subscription" *means the add-on entitlement which adds iOS and Android VPN connectivity support to WSS, and that requires purchase of the Web Security Subscription.*

"**Service Credit**" means the number of days that are added to Customer's current Subscription Term.

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

"**Symantec Online Services Terms and Conditions**" means the terms and conditions located at or accessed through https://www.symantec.com/about/legal/repository.

"Web Security Subscription" *means the base entitlement required for all services sold under the WSS umbrella.*

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 Service Description only. If Symantec 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 Symantec's sole and exclusive liability for breach of the SLA.

2.0 SERVICE LEVEL AGREEMENT(S)

a. **Availability.** 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. *Web Security Service is an Inline Service that includes Content-Filtering and Anti-Malware scanning.*

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). Examples of Non-Inline Service for this Service include*: Reporting and Advanced Malware sandboxing*

Non-Inline Service Availability	**99.5%**

b. **Other SLAs**:

a. **Average Latency**: Average latency for transactions passing through the Service is based on the processing time attributed to the WSS infrastructure. Average latency for the Service is defined as the average time it takes for the service to scan, process and apply the Customer's policy to the web content data, assuming a 1MB web page, and does not include the time for communications outside the service data center. Average Latency is 100 milliseconds or less and is determined by the monthly average among samples taken by Symantec in a given month.

Latency SLA: Average Round Trip	**100 Milliseconds or less**

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.

Availability SLA: Symantec 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.

All other SLA types: Symantec will provide a Service Credit equal to two (2) days of additional service per individual missed SLA in a single 24-hour period, subject to a maximum of seven (7) calendar days for all incidents related to that SLA occurring during that 24 hour period. The number of Service Credits available are based on the relevant unit of measure for that individual SLA.

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.

Service Credits:

- May not be transferred or applied to any other Symantec 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 Symantec Customer Support at ServiceCredit_Request@symantec.com. Each claim must be submitted within ten (10) days of the end of the calendar month in which the alleged missed SLA occurred for Symantec 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 Service Description, including any relevant calculations.

All claims will be verified against Symantec's system records. Should any claim be disputed, Symantec 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 Service Description.
- 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-Symantec branded products or services resold with the Service.
- Hardware, software or other data center equipment or services not in the control of Symantec 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 Service Description.
- Hardware or software configuration changes made by the Customer without the prior written consent of Symantec.
- Unavailability of a specific web page or a third party's cloud application(s).
- Individual data center outage.
- 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 Symantec (or at the direction of or as approved by Symantec
- Defects in the Service due to abuse or use other than in accordance with Symantec's published Documentation unless caused by Symantec or its agents.
- Customer-requested hardware or software upgrades, moves, facility upgrades, etc.

END OF EXHIBIT A