Web Security Service

Service Description

May 2018

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 Symantec Online Services Terms and Conditions (hereinafter referred to as the "Agreement").

Table of Contents

Web Security Service

Service Description

May 2018

1. TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Overview

The Symantec Web Security Service (WSS) ("Service") enforces granular access and security policies that manage web internet usage by application, device, user, or location. The Service will be provided in accordance with the terms of the Agreement and the documentation available at the Portal.

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 includes one hundred (100) days of reporting. Longer log retention options are available for a fee.

Service Level Agreement

- Symantec provides the service level agreement ("SLA") for the Service as specified in Exhibit A. The SLA in Exhibit A does not apply to or govern any other purchased Symantec services that integrate with the Symantec Web-Security License, even if Customer accesses such integrated services through the Symantec Web Security Service. For availability and latency associated with separately purchased Symantec services, Customer may refer to the service description and/or service level agreement applicable to the service.

Service Enabling Software

- This Service may include enabling software, which should be used only in connection with Customer's use of the Service during the Subscription Term. Use of the enabling software is subject to the license agreement accompanying such software ("Software License Agreement"). If no Software License Agreement accompanies the software, it is governed by the terms and conditions located at (http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf). In the event of conflict, the terms of this Service Description prevail over any such Software License Agreement. Customer must remove enabling software upon expiration or termination of the Service.

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.
- 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 comply with all applicable laws with respect to use of the Service.
- Customer must use the Service in accordance with the documentation available at the Portal.
- Customer is responsible for obtaining all approvals and consents required by any third parties in order for Symantec to provide the Service. Symantec is not in default of its obligations to the extent it cannot provide the Service either because such approvals or consents have not been obtained or any third party otherwise prevents Symantec from providing the Service.
- Customer is responsible for its data, and Symantec does not endorse and has no control over what users submit through the Service. Customer assumes full responsibility to back-up and/or otherwise protect all data against loss, damage, or destruction. Customer acknowledges that it has been advised to back-up and/or otherwise protect all data against loss, damage or destruction.
- 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's account.

Acceptable Use Policy

- Customer is responsible for complying with the Symantec Online Services Acceptable Use Policy available at: https://www.symantec.com/content/dam/symantec/docs/eulas/policy/online-services-acceptable-use-policy-v6-en.pdf

Customer Service-Specific Warranties

- Customer warrants that all information it provides related to usage for calculating the Meter and/or applicable Fees is accurate and complete.

3. SUBSCRIPTION INFORMATION

Customer may use the Service only in accordance with the use meter or model under which Customer has obtained use of the Service: (i) as indicated in the applicable Order Confirmation; and (ii) as defined in this Service Description or the Agreement.

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 License, and two (2) additional devices under the Mobile Device Security License. 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.

Changes to Subscription

If Customer has received Customer's Subscription directly from Symantec, communication regarding permitted changes of Customer's Subscription must be sent to the following address (or replacement address as published by Symantec): NP_CustomerCare@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 through a Symantec reseller, please contact the reseller.

4. ASSISTANCE AND TECHNICAL SUPPORT

Technical Support

If Customer is entitled to receive technical support ("Support") from Symantec, the Support as specified in Exhibit B is included with the Service. If Customer is entitled to receive Support from a Symantec reseller, please refer to Customer's agreement with that reseller for details regarding such Support, and the Support described in Exhibit B will not apply to Customer.

5. ADDITIONAL TERMS

- Customer may not disclose the results of any benchmark tests or other tests connected with the Service to any third party without Symantec's prior written consent.
- The Service may be accessed and used globally unless otherwise set forth in Customer's signed agreement with Symantec, subject to applicable export compliance limitations and technical limitations in accordance with the then-current Symantec standards.
- Any templates supplied by Symantec are for use solely as a guide to enable Customer to create its own customized policies and other templates.
- 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.
- 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 licensed 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") license 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 licensed 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 licenses 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

"Web Security License" means the base license required for all services sold under the WSS umbrella.

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

"Symantec Online Services Terms and Conditions" means the terms and conditions located at or accessed through https://www.symantec.com/content/dam/symantec/docs/eulas/service-agreement/symantec-online-services-agreement-2016-12-en.pdf or https://www.symantec.com/about/legal/service-agreements.jsp.

EXHIBIT A

SERVICE LEVEL AGREEMENT

The following service levels are applicable to the Service during the Subscription Term.

1. Availability of the Service.

a. Availability. Availability of the Service is distinguished between Inline Service and Non-Inline Service. Inline Service is defined as the processing or effecting data in transit to and from the end-user to the internet. Non-inline Service is any service that does not process or effect data in transit to and from the end-user to the internet (e.g., reporting tools used by the administrator). Examples of Inline Service include: Content-Filtering and Anti-Malware scanning. Examples of Non-inline Service include: Reporting and Advanced Malware sandboxing. Inline Service will be generally available 99.999% of the time. Non-inline Service will be available 99.5% of the time. Availability is calculated per calendar month as follows:

$$\frac{\text{Total – Non-excluded}}{\text{Total – Excused Outages}} \text{ X 100 > availability target}$$

• Service unavailability will not be assessed due to: (i) a failure of Customer to correctly configure the service in accordance with applicable service documentation or adherence to the Agreement; (ii) the unavailability of a specific web page or a third party's cloud application(s); (iii) individual data center outage; or (iv) unavailability of one or more specific features, functions, or equipment hosting locations within the service, while other key features remain available.
• "Total" means the number of minutes for the calendar month.
• "Non-excluded" means unplanned downtime.
• "Excused Outages" include:
o Planned downtime. With respect to planned downtime, Symantec shall provide Customer with as much notice as practical under the circumstances and strives for a minimum of 72 hours or more of advance notice. Symantec shall make commercially reasonable efforts to schedule planned downtime in off peak hours (local data center time).
o Emergency maintenance. Customer acknowledges that Symantec may, in certain situations, need to perform emergency maintenance (unplanned downtime) on less than 24 hours advance notice.
o Any unavailability caused by circumstances beyond Symantec's reasonable control, including, without limitation, acts of God, acts of government, flood, fires, earthquakes, civil unrest, acts of terror, strikes or other labor problems (excluding those involving Symantec employees), failures or delays involving hardware, software, network intrusions or denial of service attacks not within Symantec's possession or reasonable control.

For any partial calendar month during which Customer subscribes to the Service, general availability will be calculated based on the entire calendar month, not just the portion for which Customer subscribed.

b. Remedies. In the event that any particular feature within the Service is not Available for reasons other than an Excused Outage and subject to the requirements of Section 4 below, Symantec will provide an extension of the current term of the subscribed service at no charge to Customer in an amount equal to two (2) days of additional service for each 1 hour or part thereof that the service is not available, subject to a maximum of a one (1) additional week of service per incident of un-availability and subject to the maximum of four (4) service extensions for any one year of subscribed service.

c. Chronic Failure. Subject to the requirements of Section 4 below, if the subscribed service is not Available, for reasons other than an Excused Outage, and such non-availability is attributable solely to Symantec and not to Customer, in whole or in part, for more than thirty-six (36) non-consecutive hours in any calendar quarter or where Symantec has provided three (3) or more service extensions for any one year of subscribed service, Customer may terminate the effected service upon thirty (30) days' written notice to Symantec. In the event that Symantec validates the conditions of the termination under this Section, Symantec shall refund to

Customer directly or through the reseller, where applicable, a pro-rata portion of the service fees paid in advance and not yet used within forty-five (45) days from termination, or, upon Customer's request and at Symantec's sole option, offer a credit of the pro-rata refund amount toward a new Symantec product purchase to be used within a set period of time.

2. Average Latency Specific to Services.

a. Web Security Service. 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.

b. Remedies. Subject to the requirements of Section 4 below, in the event that a particular average latency is not met in any month for reasons other than an Excused Outage (as defined in Section 1a above) or any actions attributable to Customer, Symantec will provide an extension of the current term of the specific subscribed service at no charge to Customer in an amount equal to an additional one (1) week of such service per commitment failure incident, subject to the maximum of four (4) weeks of additional service for any one year term of the subscribed service.

3. Exclusions.

Notwithstanding any other clause herein, no commitment is made under this policy with respect to: (i) the Service being used in conjunction with hardware or software other than as specified in Symantec's published Documentation; (ii) alterations or modifications to the Service, unless altered or modified by Symantec (or at the direction of or as approved by Symantec); (iii) 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); (iv) an evaluation of the Service or other trial provided to Customer at no charge; and (v) any problems or issues of connectivity due to the network or internet connection of Customer.

4. Reporting and Claims.

a. To file a claim or termination notice with refund claim, as applicable, Customer must include in a written notice the following details:
• Downtime information detailing the dates and time periods for each instance of claimed downtime or Average Latency failure, as applicable, during the relevant month (or calendar quarter for termination with a refund claim).
• An explanation of the claim made under this Service Level Agreement, including any relevant calculations.

b. Claims may only be made on a calendar month basis and only for the previous calendar month or part thereof. All claims must be made within 10 days of the end of each calendar month. A termination notice with a refund claim must be made within 10 days of the end of a calendar quarter.

c. All claims will be verified against Symantec's system records. Should any claim submitted by Customer be disputed, Symantec will make a determination in good faith based on its system logs, monitoring reports and configuration records and will provide to Customer a record of service availability for the period in question. The record provided by Symantec shall be definitive. Symantec will provide records of service availability in response to valid Customer claims upon Customer's request. Symantec shall respond to a Customer claim within 10 days of claim submission.

d. All remedies referred to in this Service Level Agreement are subject to Customer having paid all applicable fees and fulfilled all of its obligations under the Agreement.

e. Notwithstanding any other clause herein, the remedies in this Service Level Agreement do not apply to any matters arising due to any of the following:
(i) Customer-requested hardware or software upgrades, moves, facility upgrades, etc.
(ii) Excused Outages.
(iii) Hardware, software or other data center equipment or services not in the control of Symantec or within the scope of the Service.
(iv) Hardware or software configuration changes made by the Customer without the prior written consent of Symantec.

5. Exclusive Remedies.

Notwithstanding any other clause in the Agreement, the remedies set out in this Service Level Agreement shall be Customer's sole and exclusive remedy in contract, tort or otherwise in respect of service affecting events.

END OF EXHIBIT A

EXHIBIT B

TECHNICAL SUPPORT

Technical Support for the Service is provided in accordance with the following terms and conditions.

DEFINITIONS

"BlueTouch Support Provider" or "Secure One Services Provider" means a Symantec partner authorized by Symantec to provide Technical Support for the Service.

"Customer Support Portal" or "Support Portal" means that portion of Symantec's website URL where Customer may access Service Documentation, software downloads, active tracking of service requests and such other information as Symantec may provide to Customer as part of the Technical Support.

"Error" means a failure of the Service to conform to the applicable Service Description.

"Service Request" means the specific case number assigned to the Customer by Symantec at the time Customer makes a verified request under a valid Support Contract or Warranty.

"Service Software Update" means a formal or informal software release for a Service which incorporates functionality changes to the Software, but is not treated as a new Service by Symantec. Symantec shall make Software Updates available to Customer via electronic download from the Customer Support Portal for so long as the Service is in effect. The content of all Software Updates shall be determined by Symantec in its sole discretion.

1. TECHNICAL SUPPORT SERVICES

1.1 Coverage Generally. Symantec will use commercially reasonable efforts to provide assistance with the diagnosis of, and resolution of, basic Service configuration issues and failures specific to Services in production. All Technical Support will be provided "as is" and in accordance with the processes set forth on the Customer Portal, including, without limitation, the proper initiation of Service Requests, priority rules, information and assistance required, escalation paths, and work arounds. Symantec does not offer support for any software provided by application vendors and will not provide software fixes, patches, maintenance releases, updates or new feature releases for any third party applications, and such support is expressly excluded from Technical Support.

1.2 Service Software Support. In the event that Customer demonstrates a non-conformance with Service Software specifications that can be duplicated by Symantec and that is not addressed by an Update, Symantec will use commercially reasonable efforts to remedy such non-conformance. Such remedy may include a work around or other temporary or permanent fix. Symantec does not represent or warrant that all non-conformities of the Service Software will be corrected. Symantec reserves the right to incorporate any remedies provided to Customer into future software revisions, in its sole discretion.

2. CUSTOMER OBLIGATIONS

Technical Data. Customer shall provide reasonable assistance to Symantec when providing Technical Support, which may include the Customer providing required data from the Service to implement a work around to minimize Customer impact, or such other information as may be required by Symantec in order to perform the Technical Support.

3. SERVICE EXCLUSIONS

Technical Support covered by a Service Level Agreement will include only those items expressly defined in the Service Level Agreement, and no other services shall be implied. Without limiting the foregoing, the following services are specifically excluded from Technical Support, but may be provided by Symantec at the request of Customer for an additional charge under a Professional Services Agreement:

(a) Any work at Customer's site, other than as mutually agreed as necessary to perform a specific Service Request;
(c) Support for any modifications of the Services by anyone other than Symantec;
(d) Services purchased through a non-authorized source; or maintenance or repair by anyone other than Symantec personnel or authorized Symantec representatives;
(e) Support for any software provided by application vendors; Symantec does not provide software fixes, patches, maintenance releases, updates or new feature releases for any third party applications;
(f) Support for any non-Symantec equipment, including, without limitation, electrical or network cabling external to the Services; accessories, attachments or any other devices not furnished by Symantec;
(g) Failure to notify Symantec of the Service defect during the term of Service; and
(h) Any Services to the extent Customer ordered such Service through a BlueTouch Support Provider, in which case Customer shall obtain Support Services from that BlueTouch Support Provider.

4. EXCLUSIVE REMEDIES

Notwithstanding any other clause in the Agreement, the remedies set out in the Service Level Agreement shall be Customer's sole and exclusive remedy in contract, tort or otherwise for claims arising under these Technical Support terms and conditions.

END OF EXHIBIT B