Symantec™ Endpoint Protection Hardening

Service Description

December, 2017

This Service Description describes Symantec's Endpoint Protection Hardening 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 Condition (hereinafter referred to as the "Agreement").

Table of Contents

1. **Technical/Business Functionality and Capabilities**
    - Service Overview
    - Service Features
    - Supported Platforms and Technical Requirements
2. **Customer Responsibilities**
    - Acceptable Use Policy
3. **Entitlement and Subscription Information**
    - Charge Metrics
    - Changes to Subscription
4. **Assistance and Technical Support**
    - Customer Assistance
    - Technical Support
5. **Additional Terms**
6. **Definitions**

Exhibit A: Technical Support

1. TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Overview

Symantec Endpoint Protection Hardening is a an advanced application defense service that provides protection for applications by isolating suspicious apps and shielding trusted ones. This Service is only available to Customers who are also using the Symantec Endpoint Protection software product with a current maintenance or subscription entitlement ("SEP").

Service Features The Service allows Customers to

- Auto-classify risk levels of all endpoint applications, whether or not they're in use
- Use application isolation to limit exploits
- Implement hardening with an intuitive workflow on the cloud console

- The Service enables comprehensive application security by minimizing the attack surface
  - Mitigate the risk of vulnerable applications being exploited by applying isolation policies
  - Protect applications from zero-day exploits by using enhanced memory exploit mitigation
- The Service provides visibility by assisting in the discovery and categorization of all endpoint applications
  - Customer may obtain a complete inventory of all endpoint applications and respective vulnerabilities
  - Customer may gain actionable insight with recommendations to track suspicious apps and shield trusted apps
- The Service enables quick time to value (TTV) by leveraging SEP's single agent architecture
  - Maximize efficacy with application isolation in combination with SEP protections
- Customer can access the Symantec Security Cloud Console ("SSCC") by using a secure password protected login. The 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. Reporting may include activity logs and/or statistics. Customer may choose to generate reports through the console.
- 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.
- Should a Service be suspended or terminated for any reason whatsoever, Symantec 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.

Supported Platforms and Technical Requirements

- Supported platforms and Hardware requirements for the Service are defined at https://www.symantec.com/products/endpoint-protection/requirements.

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.

- 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 and manage the features of the Service through the SSCC, 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 make any required firewall changes to allow the agent to communicate and operate with the Service.
- 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 account.

Acceptable Use Policy

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

3. ENTITLEMENT AND 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:

Meter is per "**Device**"

Licensable Devices only include: desktop computers, laptop computers, workstations or virtual desktops instance in an operating system environment running VDI

Changes to Subscription

If a Customer has received Customer's Subscription directly from Symantec, communication regarding permitted changes of Customer's Subscription must be sent to (AMS) order-admin@symantec.com, (APJ) order-admin-apac@symantec.com, (EMEA) order-admin-emea@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

Customer Assistance.

Symantec will provide the following assistance a 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 Customer is entitled to receive technical support ("Support") from Symantec, the Support as specified in Exhibit-A 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-A 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, 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.
- 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.

6. DEFINITIONS

"**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.

"**Emergency Maintenance**" means unscheduled maintenance periods which during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure or any maintenance for which Symantec could not have reasonably prepared for the need for such maintenance, and failure to perform the maintenance would adversely impact Customer.

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

"**Planned Maintenance**" means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure.

"**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 Online Service Terms and Conditions" means the 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, as described in Schedule 3, Service Level Agreement, are measured for the Email Security Services.

EXHIBIT-A

TECHNICAL SUPPORT

- 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.
- Whenever a Customer raises a problem, fault or request for Service information via telephone or web or portal submission with Symantec, its priority level is determined and it is responded to 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 FOLLOWING ACKNOWLEDGEMENT
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, although 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: One of the following: a problem where Customer's business operations have not been adversely affected or a suggestion for new features or an enhancement regarding the Service or Service Software	within the next business day; Symantec further recommends that Customer submit Customer's suggestion for new features or enhancements to Symantec's forums

Maintenance. Symantec must perform maintenance from time to time. The following applies to such maintenance:

- *Planned Maintenance*. For Planned Maintenance, Symantec will use commercially reasonable efforts to give Customer seven (7) calendar days' notification, via email, SMS, or as posted on the Portal. Symantec will use commercially reasonable efforts 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. If possible, Planned Maintenance will be carried out without affecting the Service. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance in order to minimize disruption of the Service.
- *Emergency Maintenance.* Where Emergency Maintenance is necessary and is likely to affect the Service, Symantec will endeavor to inform the affected parties in advance by posting an alert on the applicable Portal no less than one (1) hour prior to the start of the Emergency Maintenance.
- *Routine Maintenance.* Symantec will use commercially reasonable efforts to perform routine maintenance of Portals at times when collective Customer activity is low to minimize disruption to the availability of the Portal. Customer will not receive prior notification for these routine maintenance activities.