Symantec Endpoint Security

Service Description

October 2019

Symantec Endpoint Security ("SES") allows Customers to choose deployment on-premises or in the cloud. The Online Services Terms and Conditions and Service Description apply to a Customer's use of Symantec Endpoint Security as a cloud-based service. The End User License Agreement and Product Use Rights Supplement apply to a Customer's use of Symantec Endpoint Security as an on-premises solution. This Service Description describes Symantec Endpoint Security ("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 at www.symantec.com/about/legal/repository (hereinafter referred to as the "Agreement").

Table of Contents

1: Technical/Business Functionality and Capabilities

Service Overview

Symantec Endpoint Security ("Service") is a cloud solution to protect traditional and modern endpoints from a wide variety of threats and is automatically updated using data from Symantec's Global Intelligence Network. It uses a combination of technologies to provide automated attack surface reduction, attack prevention, breach prevention, and remediation for comprehensive threat protection.

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.
- The Service comes with default policies that can be customized by the Customer. These policies govern the behavior of technologies, including: Antimalware with Advanced Machine Learning and Behavior Analysis, Intrusion Prevention (IPS), Firewall, Memory Exploit Mitigation, Device Control, and agent communication.
- The Service is automatically updated on a schedule determined by Symantec. The Service can automatically upgrade Windows agents on a schedule defined by the Customer.
- 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.
- Content updates to protect endpoints against emerging threats are automatically provided to agents on a regular basis.
- Content updates may be restricted if the Customer does not have a license under active maintenance or exceeds the number of endpoints covered by the license.
- The Service is used to detect and help mitigate mobile cyber attacks across multiple attack vectors such as physical, malware, network and vulnerability exploits (Mobile).*
- The Service offers the Customer the ability to define rules and configurations that are applied to mobile devices that access Customer's network or data (Mobile).*
- In case of a detected network attack, Internet traffic is rerouted from the mobile device, to allow it to pass through a secured connection (Mobile)*
- The Service works in conjunction with most third-party Mobile Device Management Systems (MDM). For organizations with no third-party MDM, an option is available to optimize functionality and security using Symantec's own systems (Mobile).*
- The Service offers Attack Surface Reduction policies and workflows that include these features:
    - Auto-classify risk levels of all endpoint applications, whether or not they're in use**
    - Generate smart 'allow' and 'block' lists that operate without impacting user productivity**
    - Simplify policy updates by auto-managing drift with smart recommendations for handling new applications**
    - Designate trusted updaters to allow trusted software updates to run smoothly**
    - Customize 'allow' or 'block' rules based on various attributes of files and applications such as Reputation, Publisher, Hash, Path etc.**
    - Apply controls gradually by using different enforcement modes: monitor only, allow with user over-rides or strict enforcement**
    - Define user over-ride options based on application reputation and whether it is signed or not**
    - Default policies that can be customized by the Customer. These policies govern the behavior of the application control technology to 'allow,' 'block' or make an application trusted updater**
    - Use application isolation to mitigate exploits**

  - Implement hardening with an intuitive workflow on the cloud console**
  - Mitigate the risk of vulnerable applications being exploited by applying isolation policies**
  - Protect applications from zero-day exploits by using enhanced memory exploit mitigation**
  - Default policies that can be customized by the Customer. These policies govern the behavior of isolation technologies to defend good applications such as browsers, office and PDF Renderer as well as isolating suspicious applications to run in low, medium or high isolation sandboxes**

- Suggested word lists and template rules or policies supplied by Symantec contain words which may be considered offensive.**
- 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.**
- The Service provides visibility of endpoint behavior and activity
  - Actively records endpoint behavior
  - Identifies malicious/suspicious files/activity as well as suspicious/malicious behavior
- The Service provides the ability to hunt for IOCs/IOAs.
- The Service provides the ability to remediate endpoints.
  - Easily pivot to retrieve/delete files, isolate/rejoin endpoints, blacklist/whitelist files and submit to sandbox
- The Service provides the ability to identify suspicious files and automatically have them sent to sandboxing for analysis.
- The Service provides the ability to generate custom behavior alerting.
- Symantec, as part of the Service, may direct the Administrator to DNS configuration as provided by certain third parties as a free public service. Symantec disclaims all responsibility and liability associated with any of these separately provided services. Nothing in this Service Description or Customer's Agreement applies to, governs, or covers any process or service as provided by these 3rd party DNS configuration services.
- In some cases, when an indication of compromise is detected on the Device, internet traffic may be tunneled from it via a secure connection to allow the investigation and mitigation of such threats.
- Symantec Endpoint Security has a built-in feature to enable Customer to query the www.haveibeenpwned.com service to check Customer's enrolled user email address(es). Customer should note that this convenience is simply made available to Customer by Symantec Endpoint Security, but the use of this service provided by www.haveibeenpwned.com is at Customer's sole discretion and entirely subject to the terms of that third-party provider.

*** Indicates a Service Feature that is not available to "SES for Servers" Customers.**

**** Indicates a Service Feature that is only available to "SES Complete" Customers.**

Service Level Agreement

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

Supported Platforms and Technical Requirements

- Supported Platforms for the Service are defined here:
  - Symantec Endpoint Security
  - Rogue Wi-Fi Protection, Network Integrity and Smart VPN capabilities
  - Mobile Security
  - Threat Defense for Active Directory

Service Software Components

- The Service includes the following software components:
    - Symantec Agent
    - iOS app
    - Android app
    - App for Rogue Wi-Fi Protection, Network Integrity and Smart VPN capabilities
    - Endpoint Detection and Response (EDR)
    - SEP Client 14 RU1 and above deployed on endpoint (App Control and App Isolation)

  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 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.

3: Entitlement and Subscription Information

Charge Metrics

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

- **"Device(s)"** means a single physical or virtual desktop, laptop computer, thin client, workstation, mobile device, or server,* or other virtual operating system environment, on which a single instance of the Software, or portion thereof, is installed, executed, or performing services.

  ***Customer may only use the Service on a server if Customer has purchased *SES for Servers* or *SES Complete* which is sold separately from *SES*.**

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 via email, SMS, or Twitter 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.
- **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 Symantec Status. 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. 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

- If Customer elects, and Symantec has provided Customer access, to download a file which has been detected and indicated by the Service to be malicious, the act of downloading the file is not subject to and does not derive any benefit from any support or service obligations provided herein.
- Any templates supplied by Symantec are for use solely as a guide to enable Customer to create its own customized policies and other templates.

6: Definitions

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

"**App Control and App Isolation"** mean component services Endpoint Application Control and Endpoint Application Isolation.

"CCD" means component service Endpoint Cloud Connect Defense.

"**EDR"** means component service Endpoint Detection and Response.

"**Mobile"** means component service Endpoint Protection Mobile

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

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.

Inline Service Availability	**N/A**

- **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*:*
  - *Accessing the Management Console and APIs*
  - *Managing policies and configuration*
  - *Generating reports*
  - *Viewing data, statistics, security and audit events*
  - *Viewing information about Devices*
  - *Sending commands to Devices*
  - *Data Analytics/Forensic Analysis with alerting (EDR)*
  - *Retrieval /Deletion of malicious files and associated artifacts on all impacted endpoints (EDR)*
  - *Reporting (EDR)*

Non-Inline Service Availability	**99.5%**

3.0 AVAILABILITY CALCULATION

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

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

**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.

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. 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.
- 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 changes such as domain deletion or account termination.

END OF EXHIBIT A