Symantec Endpoint Protection Mobile (SEP Mobile)

Service Description

February 2018

This Service Description describes Symantec Endpoint Protection Mobile (SEP Mobile) (the "*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 refered to as the "Agreement").

Table of Contents

Symantec Endpoint Protection Mobile (SEP Mobile)

Service Description

February 2018

1. TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Overview

The Symantec Endpoint Protection Mobile (SEP Mobile) ("*Service*") protects mobile Devices used by anyone that has access to Customer's computer network or data through that device, for which Customer has activated the Service.

Service Features

- The Service is used to detect and help mitigate mobile cyber attacks across multiple attack vectors such as physical, malware, network and vulnerability exploits
- 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.
- In case of a detected network attack, Internet traffic is rerouted from the Device, to allow it to pass through a secured connection.
- 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.
- Customer can access the Service through a self-service Skycure Management Console ("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. For access to certain features, the Portal may require additional user validation information in addition to any user name and password supplied by Symantec.
- 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 information about security incidents and/or compliance and threat 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.
- 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.

Service Level Agreement

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

Service Enabling Software

- This Service includes 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 of the "Endpoint Protection Mobile Apple App" License Agreement or the Endpoint Protection Mobile Android App" License Agreement 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 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:

- "**Device**" means any mobile communication device, that is connected to the Customer's mobile communication network, on which Customer can install and use the software.

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-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, 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.

"Credit Request" means the notification which Customer must submit to Symantec by Email to support.cloud@symantec.com with the subject line "Credit Request" (unless otherwise notified by Symantec).

"**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.

"**Service Credit**" means the amount of money that will be credited to Customer's next invoice after submission of a Credit Request and validation by Symantec that a credit is due to Customer.

"**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.

EXHIBIT-A

SERVICE LEVEL AGREEMENT

General

- Customer must submit a Credit Request within ten (10) business days of the end of the calendar month in which the suspected service level non-compliance occurred, and any Credit Request submitted outside of the provided timeframe will be deemed invalid.
- All Credit Requests will be subject to verification by Symantec in accordance with the applicable provisions of this Service Level Agreement.
- This Service Level Agreement will not operate: (i) during periods of Planned Maintenance or Emergency maintenance, periods of non-availability due to force majeure or acts or omissions of either Customer or a third party; (ii) during any period of suspension of service by Symantec in accordance with the terms of the Agreement or (iii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); or (iv) Customer has not configured the Service in accordance with the Agreement.
- The remedies set out in this Service Level Agreement are Customer's sole and exclusive remedies in contract, tort (including without limitation negligence) or otherwise, with respect to this Service Level Agreement.
- The maximum accumulative liability of Symantec under this Service Level Agreement in any calendar month is no more than one hundred percent (100%) of the Monthly Charge payable by Customer for the affected Service(s).

99% Service Availability

- In relation to the Services, this Service Availability Service Level means the availability of the Portal, and only applies if Customer's Devices are correctly configured on a 24x7 basis.
- If in any calendar month Service Availability is below ninety-nine percent (99%), Customer may submit a Credit Request and may receive a Service Credit for the following percentage credit:

Percentage Service Availability Per Calendar Month	**Percentage credit of Monthly Charge**
< 99% but >= 98%	10
< 98% but >= 95.0%	25
< 95.0%	50

EXHIBIT-B

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.

Severity	Description	Initial Response	Action
Critical (Severity 1)	Service interruption for at least 25% of the devices of a account running Skycure in a way that affects regular device usage (i.e., email access, network connectivity) and no workaround is immediately available.	1 business hour* or less	Work continuously until issue is fixed
High (Severity 2)	A major service functionality is impacted by an issue that is persistent and affects many users and/or major functionality —and no reasonable workaround is available. Examples: Management console goes down, or integration between Skycure and other business systems goes down, or device activation issues impact a large number of devices.	8 business hours* or less	Work through normal business day
Medium (Severity 3)	Service is operational, although partially degraded for some or all users, and an acceptable workaround or solution exists. Examples: Issues concern a non-critical feature or functionality such as issues with the activation process of a specific device or activating security detection on a specific device.	2 business days	Reasonable – as resources are available
Low (Severity 4)	Minor issue not impacting service functionality. Enhancement requests, missing or erroneous manuals.	10 business days	Reasonable – as resources are available

- The Customer is required to notify Symantec Support about Critical and/or High severity issues via phone support. Should the Customer decide to use a different channel for the initial communication in such scenarios, Symantec cannot guarantee it will be handled according to the defined SLAs.

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 thePortal. 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.