Symantec Cloud Workload Protection for Storage

Service Description

May 2019

This Service Description describes *Symantec Cloud Workload Protection for Storage* ("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 Conditions (hereinafter referred to as the "Agreement").

Table of Contents

Symantec Cloud Workload Protection for Storage

Service Description

May 2019

1: Technical/Business Functionality and Capabilities

Service Overview

Symantec Cloud Workload Protection for Storage ("*Service*") is a service that secures data in Amazon Simple Storage Service ("Amazon S3") and Azure Blob storage (Block-Blob).

Service Features

Symantec Cloud Workload Protection for Storage (CWP for Storage)

- The Symantec Cloud Workload Protection for Storage Service scans the Amazon S3 buckets and Azure Blob Storage Accounts (General-purpose v2 accounts and Block blob storage accounts) for security threats by using antivirus features and other technologies like file reputation and advanced machine learning.
- This Anti-Malware Service provides protection at all times by scanning any file which gets uploaded, downloaded, updated or data at rest within Amazon S3 and Azure Blob Storage Accounts.
- Near real-time scan (NRTS) feature scans files as soon as they get created or modified in the Amazon S3 buckets and in Azure Blob Storage Accounts. Scheduled scan periodically scans the Amazon S3 buckets and Azure Blob Storage Accounts with latest virus definitions and as per the defined scope & schedule.

Symantec Cloud Workload Protection for Storage DLP (CWP for Storage DLP)

- Symantec Cloud Workload Protection for Storage DLP (CWP for Storage DLP) service identifies sensitive data and content violation in AWS S3 Storage.
- The service provides in-tenant single-pass multi-scan of content for access permissions, antimalware and information protection (DLP). Scans happen in 'Near Real-Time' and 'Scheduled' scanning modes enabling identification of content on uploads/edits etc.
- Violations show up in CWP-Storage console as well as the DLP enforce console. Based on these sensitive content identification AWS Tags, IAM policies prevent data loss.

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: 1. Management Console, 2. Agent
- 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.

Service Hardware Components

- If the Customer chooses to configure two-factor authentication, Customer may purchase such two-factor authentication token from Symantec.
- The use of any hardware 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.

- 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.

- Customer must provide appropriate access to its Amazon (or Amazon Web Services) and Azure deloyments to the Service as defined in the Documentation to enable all the capabilities 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. Some of the features are configured at the time of deployment of Enabling Software through AWS CFT inputs and through Azure solution template inputs.
- Some configurations can also be done through the Command Gateway (Command-line utility) provided along with the Enabling Software.

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:

- "**Gigabyte (GB)**"refers to the amount of digital information (i) that uses and/or benefits from the use of the Service, or (ii) that actually uses any portion of the Service. Usage is tracked and billed in Gigabytes of digital information scanned by the Service.

Pay for Use

The Pay for Use meter is available only for Symantec Cloud Workload Protection for Storage (CWP for Storage) and NOT for Symantec Cloud Workload Protection for Storage DLP (CWP for Storage DLP)

- Customer pays in arrears for the Service based on the number of Gigabytes of digital information scanned by the Service in the prior month rounded up to the nearest whole Gigabyte.
- Billing increments are computed by the Gigabytes with a minimum of one (1)Gigabyte.
- Customer can run the Service without a predetermined limit.

Annual Subscription

- Customers can reduce the monthly bill by purchasing annual Subscriptions and prepaying for a pre-determined quantity of Gigabytes of digital information scanned.
- An annual Subscription entitles Customer to protect one (1) Gigabyte of digital information scanned per month.
- An annual Subscription with monthly billing plans entitles Customer to protect one (1) Gigabyte of digital information scanned per month.
- With monthly billing plans, customer cannot purchase annual Subscription alone. In order to cover any potential overage, Customer must maintain an active account for Pay for Use at the same time.

4: Customer Assistance and Technical Support [This Section 4 may not be edited. It must remain with this exact text.]

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 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: Definitions

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

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

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

"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. *N/A*

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*:* Management and the administration of the service via management console which includes features such as deployment, reporting, asset representation, alerting and notification

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:

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

**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.

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.
- 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