Symantec Workload Assurance Service

Service Description

October 2018

This Service Description describes Symantec's Cloud Workload Assurance ("**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

Symantec Workload Assurance Service

Service Description

October 2018

1: Technical/Business Functionality and Capabilities

Service Overview

The Symantec™ Cloud Workload Assurance ("**Service**") is a new, cloud-based scanning service that allows Customer to configure its own policy-based security assessment strategy for validating security across their public cloud management plane.

Service Features

The Service enables Customer to implement security controls for the public cloud infrastructure.

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.

Customer subscribing to the Service can define and run assessments to be implemented on their AWS and Azure management plane accounts, services and resources.

Customer will be subscribed to the Service with a password-based authentication to the Management Console. Optionally, Customer can request and enforce two-factor authentication to access the Service via the management console. Customer using Symantec's Validation & ID Protection (VIP) Service[1] can easily integrate with VIP to authenticate Administrator's access.

The Service with out-of-box policies, based on continuous monitoring or scheduled scans, allows for quick insight into identifying and remediating misconfigurations in the public-cloud services and resources that may impact the security posture of Customer's.

The Service allows Customer to view alerts and events generated as a result of the monitoring / assessment of the policies. The Service further allows the Administrator (or the DevOps individual) to tune the policies in response while reviewing the alerts and events.

Service Level Agreement

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

Service Enabling Software

This Service requires the use of software, which should be used only in connection with Customer's use of the Service during the Subscription Term ("**Service Software**"). If no terms of use accompanies the Service Software, then it is governed by the terms of use located at http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf.

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.

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.

[1] Separate purchase required.

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.

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.

Should the Service be suspended or terminated for any reason whatsoever, Symantec will reverse all configuration changes made upon provisioning the Service and it is Customer's responsibility to undertake all necessary configuration changes when the Service is reinstated.

Acceptable Use Policy

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

3: Entitlement and Subscription Information

Charge Metrics

The Service is available using the following Meter as specified in the Order Confirmation:

"**User**" means an individual account on the public cloud that monitors and assesses a maximum of 500 Resources from a secure configuration or compliance perspective. Assessment of more than 500 Resources will result in additional fees. See more details in "**Service Buying Model and Metering"** below.

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): 3S_Orders@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 to request any permitted change.

4: Assistance and Technical Support

Note: This section only applies if Customer is entitled to receive Customer Assistance and Support directly from Symantec ("Support"). If Customer is entitled to receive Assistance and Support from a Symantec reseller, refer to Customer's agreement with that reseller for details regarding such Support, and the Support described here will not apply to Customer.

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

Entry-level Support is included as part of the Service as specified below.

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 email service to receive the latest updates. 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. As used herein, "**Planned Maintenance**" means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure.

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. As used herein, "**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.

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.

5: Additional Terms

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.

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.

SERVICE-SPECIFIC TERMS

Service Buying Model and Metering

Pay for Use

- Customer pays in arrears for the Service based on what was consumed in the prior month.
    - The consumption is calculated based on the number of Users (that is public cloud accounts) that have been assessed at least once during the duration of the month minus the number of active annual prepaid accounts assessed during the billing month
        - Note: if an individual User assesses more than 500 Resources during the billing period, each additional 500 Resources or fraction thereof assessed will be counted as an additional User for billing purposes. For example, if a User assesses 750 Resources during the month, the count for that User will be two.
    - Billing increments are calculated by number of accounts assessed and number of Resources.
    - Customer can run the Service on any number of accounts and Resources without a predetermined limit.
- Symantec will invoice Customer monthly, based on the calculation described above. Customer acknowledges that the Agreement constitutes a legally binding obligation to pay the applicable fees for all committed items as specified herein.
- Pay for Use continues until Customer terminates the Service.
- Customer can terminate the Service by sending a written request to 3S_Orders@symantec.com at least thirty (30) days before the desired termination date. A notice of termination takes effect upon the later of: (a) at the end of the month after the 30-day notice period is over; or (b) if applicable, the termination of annual subscription. Any notice given according to this procedure will be deemed to have been given when received.

Annual Subscription

- Customers can reduce the monthly bill by purchasing annual subscriptions and prepaying for a pre-determined capacity.

- One (1) annual subscription entitles one (1) User account to monitor or access a maximum of 500 Resources throughout the one (1)-year Subscription Term. If the User account assesses more than 500 Resources, Customer must purchase an additional subscription for each additional increment of 500 Resources or fraction thereof.
- Annual subscriptions fees must be prepaid.
- Customer cannot purchase annual subscriptions alone. In order to cover any potential overage, Customer must maintain an active account for Pay for Use at the same time.
- No credit or refund will be due to the Customer for any expired or unused services.

Changes to Subscription or Entitlement

If Customer has received Subscription or Entitlement directly from Symantec, communication regarding permitted changes of the applicable Subscription or Entitlement must be sent to the following address: 3S_Orders@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 you have received your Subscription or Entitlement through a Symantec reseller, please contact your reseller.

Service Conditions

- Except as otherwise specified in the Service Description, the Service (including any Service Software provided therewith) may use open source and other third-party materials that are subject to a separate license. Please see the applicable Third Party Notice, if applicable, at https://www.symantec.com/about/legal/repository.
- Customer shall comply with all applicable laws with respect to use of the Service. In certain countries it may be necessary to obtain the consent of individual personnel. Configuration and use of the Service is 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. Further, Customer shall at all times remain responsible for its implementation of a policy, and Symantec shall not be responsible or liable for Customer's implementation of any such policy.
- 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 a Customer User with authorization to manage the Service on behalf of Customer. Administrators may have the ability to manage all or part of the Service as designated by Customer.

"Resource" is a cloud-service object whose configuration is assessed by the Service.

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. Cloud Workload Assurance (CWA) is a non-Inline Service. 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). 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:

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

- Service unavailability for Non-inline services is assessed if the CWA portal or UI pages are unavailable.
- 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; provided that Customer is serviced by one of Symantec's other data centers and does not experience a service interruption; or (iv) unavailability of one or more specific features, functions, or equipment hosting locations within the Service; provided that the Service is accessible and the key features of the Service remain available. For clarity, "**key features**" refers to the core functionality of the Service.
- "**Total**" means the number of minutes for the calendar month.
- "**Non-excluded**" means unplanned downtime.
- "**Excused Outages**" include:
    - Planned downtime. With respect to planned downtime, Symantec shall provide Customer with 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 datacenter time).
    - Emergency maintenance. Customer acknowledges that Symantec may, in certain situations, need to perform emergency maintenance on less than 24 hours' notice.
    - 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 (1) 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 (1) 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. 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.

3. 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.

4. 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 with respect to default of the applicable service level. Notwithstanding the foregoing, to the extent that, concurrent with or as part of a failure to meet a service level, Symantec has failed to meet some other obligation of the Agreement, Customer shall be entitled to exercise any other rights and remedies Customer may have as a result of such other failure under the Agreement.

END OF EXHIBIT A

END OF SERVICE DESCRIPTION