Symantec™ Cloud Workload Protection

SaaS Listing

The definitions set out in the Agreement will apply to this SaaS Listing document.

The CA software program(s) ("CA Software") listed below is provided under the following terms and conditions in addition to any terms and conditions referenced on the CA quote or other transaction document entered into by you and the CA entity ("CA") through which you obtained a license for the CA Software (hereinafter referred to as the "Agreement"). These terms shall be effective from the effective date of such ordering document.

This SaaS Listing describes Symantec Cloud Workload Protection and Cloud workload Protection Antimalware Service ("Service"). All capitalized terms in this Listing have the meaning ascribed to them in the Agreement (defined below) or in the Definitions section.

Table of Contents

1: Technical/Business Functionality and Capabilities

- Service Overview
- Service Features
- Service Level Agreement
- Supported Platforms and Technical Requirements
- Service Software Components
- Service Hardware Components

2: Customer Responsibilities

3: Entitlement and Subscription Information

- Charge Metrics

4: Customer Assistance and Technical Support

- Customer Assistance
- Technical Support
- Maintenance to the Service and/or supporting Service Infrastructure

5: Definitions

Exhibit-A Service Level Agreement(s)

1: Technical/Business Functionality and Capabilities

Service Overview

The Symantec™ Cloud Workload Protection and Cloud Workload Protection Antimalware Service ("Service") provides infrastructure security as a service for workloads on Amazon Web Services ("AWS"), Microsoft Azure ("Azure"), Google Cloud Platform ("GCP"), Oracle Cloud Infrastructure (OCI) and other cloud platforms. The Service allows businesses to take control of their public cloud infrastructure by providing visibility, workload, application and container security, threat and vulnerability insight from a single console. The Service is designed to eliminate blind spots in public cloud deployment while allowing security organizations to control the behavior of applications and detecting changes to any configuration or application control data in real time.

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 enables Customer to implement security controls for the public cloud infrastructure.
- Customer can access the Service Management Console (SMC) by using a secure password protected login. The SMC 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.
- 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 has a single pane of glass to define security policies to define host-based controls to manage security risks across their AWS, Azure, and GCP deployments. Customer will be subscribed to the Service with a secure password-based authentication to SMC. Optionally, Customer can request and enforce two-factor authentication to the Service. Customer interested in two-factor authentication to access the Service via SMC has a choice to use Symantec VIP (VIP tokens for Administrator).
- Customer must delegate appropriate access to its AWS, Azure, and GCP, OCI deployments to the Service as defined in the Documentation to enable all the capabilities of the Service.
- The Service gathers appropriate context and metadata about the AWS/Azure/GCP/OCI instances deployed as seen by the delegated role. This provides instant visibility into the instances.
- On an instance with the Service Software deployed, the system discovers the deployed applications. This information and the metadata information collected from the cloud platform provide the context to auto recommend appropriate HIPS and HIDS policies.
- The Service, with native integrations into AWS, Azure, GCP, and OCI delivers scale out security for public cloud infrastructure. For example, an instance that belongs to an autoscaling group will be automatically protected at the same level as the other instances in the same autoscaling group. The threat and vulnerability overview allow for quick insight into identifying and managing exploits across the public cloud deployments managed by the Service.
- The Service collects the Symantec Global Intelligence Network (GIN) threat and vulnerability feeds to correlate with the discovered software in order to provide an accurate picture of the threat and vulnerability exposure to the AWS/Azure/GCP/OCI deployments. Appropriate remediation tasks are suggested to take an appropriate action as a means of providing compensating controls for detected threats.
- The Service allows Customer to view the alerts and events generated as a result of the monitoring/enforcement of the policies. The Service further allows the Administrator (or the DevOps individual) to tune the policies in response while reviewing the events.
- The Service allows for the policy groups defined via the SMC to be automatically available to the instances that are available.
- Suggested word lists and template rules or policies supplied by CA contain words which may be considered offensive.
- In the event that continued provision of the Service to Customer would compromise the security of the Service, including, but not limited to, hacking attempts, denial of service attacks, mail bombs or other malicious activities either directed at or originating from Customer's domains, Customer agrees that CA may temporarily suspend Service to Customer. In such an event, CA will promptly inform Customer and will work with Customer to resolve such issues. CA will reinstate the Service upon removal of the security threat.

- Should a Service be suspended or terminated for any reason whatsoever, CA shall reverse all configuration changes made upon provisioning the Service and it shall be the responsibility of Customer to undertake all other necessary configuration changes when the Service is reinstated.
- Customers shall have access to the Service to download Events and Alerts information for up to 30 days after termination of the Service.

Service Level Agreement

- CA 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 at https://www.symantec.com/products/cloud-workload-protection

Service Software Components

- The Service includes the following software components: Symantec Cloud Workload Protection Agent
- The use of any software component is governed by the Agreement and, if applicable, any additional terms published with this SaaS Listing on www.symantec.com/about/legal/repository.

Service Hardware Components

- The Service includes the following hardware components: Optional two-factor authentication token.
- The use of any hardware is governed by the Agreement, and if applicable, any additional terms published with this SaaS Listing on www.symantec.com/about/legal/repository.

2: Customer Responsibilities

CA can only perform the Service if Customer provides required information or performs required actions, otherwise CA'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 CA to begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist CA in delivery of the Service.
- It is the Customer's responsibility to update the AWS settings and/or Azure or GCP subscriptions with any changes in the Customer environment to get the right protections.
- 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, CA 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

3: Entitlement and Subscription Information

Charge Metrics

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

Pay for Use

- Customer pays in arrears for the Service based on what was consumed in the prior month.
  - The consumption for each instance is calculated based on the number of hours the applicable instance (with Service Software installed) is in "Running" status as indicated on the SMC.
  - Billing increments are computed by the hour with a minimum of one hour.

  - Customer can run the Service on any number of server instances or servers for any number of hours without a predetermined limit.
- CA will invoice Customer monthly, based on the calculation described above. Notwithstanding anything to the contrary in the Agreement, Customer acknowledges that the Agreement constitutes 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 annual subscription entitles Customer to protection of one (1) unnamed server for one (1) year.
  - Annual subscriptions fees must be prepaid.
  - Customers who license Cloud Workload Protection Large, Cloud Workload Protection Medium, or Cloud Workload Protection Small annual subscriptions cannot purchase such annual subscriptions alone. In order to cover any potential overage, Customer must maintain an active account for Pay for Use at the same time.
  - Customers who license Cloud Workload Protection AnyServer subscriptions may purchase such subscriptions without an active account for Pay for Use.
  - Customers who license Cloud Workload Protection Antimalware subscriptions may purchase such subscriptions without an active account for Pay for Use.
  - No credit or refund will be due to Customer for any expired or unused services.

4: Customer Assistance and Technical Support

Customer Assistance

CA 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 CA 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, CA 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 CA 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	Within 30 minutes

substantial loss of service; or (ii) a substantial portion of Customer's mission critical data is at a significant risk of loss or corruption.	
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; CA further recommends that Customer submit Customer's suggestion for new features or enhancements to CA'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

CA must perform maintenance from time to time. For information on Service status, planned maintenance and known issues, visit https://status.symantec.com/. 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, CA will provide seven (7) calendar days' notification.
- **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. CA will provide a minimum of one (1) calendar day notification. 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 CA 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, CA will provide fourteen (14) calendar days' notification. CA 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 Credit**" means the number of days that are added to Customer's current Subscription Term.

"**Service Infrastructure**" means any CA 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 SaaS Listing only. If CA 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 CA'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. Cloud Workload Protection is an Inline Service where the Agent communicates information to and from the customer environment to the server, including and not limited to commands, policies and events.

Inline Service Availability	**≥99.9%**

- **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*:* The management portal console and REST API access for the management of the service including visibility, configuration, orchestration, monitoring and notifications.

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:

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

**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.

CA 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 CA Customer Support. Each claim must be submitted within ten (10) days of the end of the calendar month in which the alleged missed SLA occurred for CA 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 SaaS Listing, including any relevant calculations.

All claims will be verified against CA's system records. Should any claim be disputed, CA 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 SaaS Listing.
- 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 CA 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 SaaS Listing.
- Hardware or software configuration changes made by the Customer without the prior written consent of CA.
- 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 CA (or at the direction of or as approved by CA
- Defects in the Service due to abuse or use other than in accordance with CA's published Documentation unless caused by CA or its agents.
- Customer-requested hardware or software upgrades, moves, facility upgrades, etc.

END OF EXHIBIT A