CloudSOC (Audit, CASB for SaaS, CASB for IaaS, CASB Gateway)

Service Description

June 2019

This Service Description describes Symantec's CloudSOC Audit, CloudSOC CASB for SaaS (formerly CloudSOC Security for SaaS), CloudSOC CASB for IaaS (formerly CloudSOC Security for IaaS), and CloudSOC CASB Gateway services (each, a "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 with the Service Description 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 CloudSOC is a Cloud Access Security Broker (CASB) platform that provides multiple services, including CloudSOC Audit, CloudSOC CASB for SaaS (formerly CloudSOC Security for SaaS), CloudSOC CASB for IaaS (formerly CloudSOC Security for IaaS), and CloudSOC CASB Gateway services (each, a "Service"). The Service will be provided in accordance with the terms of the Agreement and the documentation available at the Portal.

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.

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: Reach Agent and SpanVA.
- 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.

3: Entitlement and Subscription Information

Charge Metrics

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

- "**User**" has the meanings set forth in the descriptions for CloudSOC Audit, CloudSOC CASB for SaaS, CloudSOC CASB for IaaS, and CloudSOC CASB Gateway in the "Subscription Information" section of the Service Description.
- **"Usage"** means GB/day usage for processed data for IaaS applications as set forth in the description for CloudSOC CASB for IaaS in the Service Description

CloudSOC Audit

CloudSOC Audit is a cloud-based service that provides visibility into usage of cloud applications, and the security risk of the applications based on a business reading rating (BRR) model.

CloudSOC Audit may be used for no more than the number of licensed Users. A "User" is defined as a uniquely identifiable user in the proxy or firewall logs as identified by username or user ID. In the absence of either, client IP addresses are used for user identification.

• Subscription to CloudSOC Audit includes access to functionality within the SpanVA virtual appliance to collect, compress and/or tokenize proxy or firewall logs before transferring to CloudSOC Audit for processing.

• Customers can create up to twenty (20) unique log data sources from CloudSOC Audit app.

• Customers can define data retention for CloudSOC Audit results from a minimum of two (2) and up to twelve (12) months.

• A CloudSOC Audit subscription provides access to CloudSOC CASB Audit AppFeed that allows cloud application discovery and controls from the ProxySG, Secure Web Gateway VA, Advanced Secure Gateway, or Web Security Service.

CloudSOC CASB for SaaS (formerly CloudSOC Security for SaaS) and CloudSOC CASB for IaaS (formerly CloudSOC Security for IaaS)

CloudSOC CASB for SaaS and CloudSOC CASB for IaaS are cloud-based services that provide visibility and control over activities of Users in cloud applications, as well as monitoring and protection of data that is transferred, stored, and/or shared.

Available for SaaS or IaaS applications, a complete list of cloud applications supported by the CloudSOC CASB offerings can be found in the CloudSOC online store, and includes, but is not limited to:

- Microsoft Office365
- G Suite
- Box
- Dropbox
- Salesforce.com
- DocuSign
- Jive
- ServiceNow
- GitHub
- Amazon Web Services (AWS)
- Yammer
- Microsoft Azure
- Cisco Webex Teams
- Facebook Workplace
- Slack
- Workday

The licenses are available on a per User basis in multiple user bands for SaaS applications, and on a GB/day total aggregate usage basis in multiple processed-data-volume tiers for IaaS applications. A "User" is defined as a uniquely identifiable user in each cloud application that has a name and email address. Unless noted below, CloudSOC CASB may be used for no more than the number of licensed users for that cloud application or total across all cloud applications, as applicable. If supported, API connectivity and scanning content within cloud applications is limited to all documents and last thirty (30) days of messages, posts, emails and attachments. Retention of data for CloudSOC CASB offerings is limited to a maximum of three (3) full calendar months for use with the Service. During the first week of each calendar month, one (1) calendar month of older data will be archived and made available for download for one (1) calendar year after the date that the data was archived. For example, for a subscription term that begins on January 15, the data from January 15 through April 30 will be available for active use until the first week of May. During the first week of May, the data from January 15-31 will be archived for one (1) calendar year, and data from February, March and April will continue to be available for

active use during the month of May. During the first week of June, data for the calendar month of February will be archived for one (1) calendar year, and data from March, April and May will continue to be available for use during the month of June.

In the event that Symantec discontinues the Service for a cloud application before the end of the applicable Subscription Term, Symantec shall provide to Customer directly or through the reseller, where applicable, a refund for the pro-rata portion of the service fees paid in advance and not yet used in the form of a credit toward a new Symantec product purchase to be used within a set period of time.

CloudSOC CASB Gateway

CloudSOC CASB Gateway is a cloud-based transparent gateway service that provides visibility and control of user activities through inline inspection of traffic.

CloudSOC CASB Gateway is offered as a subscription license on a per User basis in multiple user bands. A "User" is defined as a uniquely identifiable user who has authenticated with the CloudSOC environment (either directly, via Single Sign On, or by other means) in order to access supported cloud applications. Retention of data for the CloudSOC CASB Gateway service is limited to a maximum of three (3) full calendar months for use with the Service. During the first week of each calendar month, one (1) calendar month of older data will be archived and made available for download for one (1) calendar year after the date that the data was archived. For example, for a subscription term that begins on January 15, the data from January 15 through April 30 will be available for active use until the first week of May. During the first week of May, the data from January 15-31 will be archived for one (1) calendar year, and data from February, March and April will continue to be available for active use during the month of May. During the first week of June, data for the calendar month of February will be archived for one (1) calendar year, and data from March, April and May will continue to be available for use during the month of June.

• Customers can deploy any number of CloudSOC Reach Agents for the express purpose of device management and traffic steering to CloudSOC CASB Gateways on Windows, Mac OS X, and Android endpoints and VPN profiles on iOS devices.

• Customers can forward traffic for supported cloud applications from other web gateways that support proxy chaining rules to the CloudSOC CASB Gateway.

• Access to Detect feature for User behavior analytics, Investigate feature for forensics, Protect feature for policies and content inspection.

CloudSOC SpanVA

Subscription to any CloudSOC product includes access to up to ten SpanVAs - a virtual appliance that can be installed and run by Customers inside their network for log collection, tokenization, and directory integration. SpanVA can be hosted on supported platforms including but not limited to VirtualBox, VMWare Fusion, VMware ESX/ESXi, VMWare Workstation, or VMPlayer.

CloudSOC Reach Agent

Subscription to CloudSOC CASB Gateway includes access to CloudSOC Reach Agents for Windows, Mac OS X, and Android endpoints and VPN profiles on iOS devices.

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

The Service may be accessed and used globally unless otherwise set forth in Customer's signed agreement with Symantec, subject to applicable export compliance limitations and technical limitations in accordance with the then-current Symantec standards.

Excessive Consumption. If Symantec determines that Customer's aggregate activity on the Service imposes an unreasonable load on bandwidth, infrastructure, or otherwise, Symantec may impose controls to keep the usage below excessive levels. For Inline Service, defined as the processing or effecting data in transit to and from the end-user to the internet, the expected average weekly usage is 6 kilobits per second per user (approximately 2GB per month per user). Upon receiving notification (e.g., email) of excessive (vs. expected) usage, Customer agrees to remediate their usage within ten (10) days, or to work with its reseller to enter into a separate fee agreement for the remainder of the Subscription Term. If the parties are not able to establish a resolution within ten (10) days after the initial notification, then Symantec may institute controls on the Service or terminate the Service and this Agreement, without liability. In addition, if Symantec determines that the excessive usage may present a risk to the Service, Symantec may implement technical and business measures to bring usage into compliance.

User/Usage Count. In the event that Customer exceeds its licensed Users or Usage amount (as measured in Symantec's reporting system or as otherwise calculated by Symantec), Customer agrees to promptly pay the amounts invoiced for the excess usage and/or submit a new order for the excess use. In addition, the parties agree to meet in good faith to determine the number of new User/Usage amount subscriptions required by Customer for the remainder of the Subscription Term.

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.

For the purposes of this Service, the definition of **"Network Data"** includes Cloud Application Data.

"Cloud Application Data" means cloud application data that Symantec may receive, store, and/or process to configure and provide the Online Service, and/or to provide any included support for the Online Service, including but not limited to time of transaction, User IP address, username, URL, URL category, status (success or error), file type, filter result (allowed or denied), virus ID, files, records, Customer selected account names and activity types, and other metadata (e.g. browser software used), and any other network traffic (and data related thereto) sent to or received from You through use of the Online Service, in detail and/or in an aggregated form.

"**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

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. CloudSOC Gateway is an Inline Service that is outlined in Section 3 above.

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*:* CloudSOC Audit and CloudSOC Securlet as outlined in Section 3 above.

Non-Inline Service Availability	**≥99.5%**

b. **Other service levels**:

- **Latency**:
  - **CloudSOC CASB Gateway**: Average latency for transactions passing through the CloudSOC CASB Gateway service is based on end-user performance and will not exceed one (1) second or twice the Direct Response Time (as defined below). The CloudSOC CASB Gateway average latency is assessed on the difference between: (a) The completion time for a cloud application transaction when its traffic is sent to a cloud service via an CloudSOC CASB Gateway; and (b) the completion time for an identical cloud application transaction from the same end-point device and location when its traffic is sent directly to the cloud service, without using an CloudSOC CASB Gateway ("Direct Response Time"). Average latency is determined by the monthly average among samples taken by Symantec in a given month. Average Latency excludes file transfer activities requiring content inspection and/or encryption.

  - **CloudSOC Audit**: The average latency for processed data to be available in CloudSOC Audit will be no later **six (6) hours** after periodic uncorrupted data batch in formats supported by Symantec is completely streamed/uploaded by the end device. Average latency is determined by the monthly average among samples taken by Symantec in a given month. Maximum daily streaming exceeding one day's worth of logs will be excluded from average latency calculations.

  - **CloudSOC CASB for SaaS and IaaS (Securlets).** The average latency to process an event and associated data within the CloudSOC CASB monitored SaaS or IaaS application will take no more than six (6) hours after the occurrence of that event. Average latency is determined by the monthly average among samples taken by Symantec in a given month. Initial processing of events and associated data triggered by the activation or re-activation of a Securlet and addition or migration of new users and their data to the application, is excluded from average latency calculations. Latency introduced by (i) the SaaS or IaaS application, either due to delayed availability of events and associated data from their

API or due to throttling of API calls made by CloudSOC , or (ii) in any way attributable to third party SaaS or IaaS providers, is excluded from average latency calculations.

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.

All other SLA types: Symantec will provide a Service Credit equal to two (2) days of additional service per individual missed SLA in a single 24-hour period, subject to a maximum of seven (7) calendar days for all incidents related to that SLA occurring during that 24-hour period. The number of Service Credits available are based on the relevant unit of measure for that individual SLA.

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