Symantec™ Data Loss Prevention Cloud Detection Service and Data Loss Prevention Cloud Service for Email

Service Description

April 2018

This Service Description describes Symantec's Data Loss Prevention Cloud Detection Service and Data Loss Prevention Cloud Service for Email (individually and collectively, the "Service"). All capitalized terms in this description have the meaning ascribed to them in the Agreement (defined below) or in the Definitions section.

This Service Description, with any attachments included by reference, is part of and incorporated into Customer's manually or digitally-signed agreement with Symantec which governs the use of the Service, or if no such signed agreement exists, the Symantec Online Services Terms and Condition (hereinafter referred to as the "Agreement").

Table of Contents

Symantec™ Data Loss Prevention Cloud Detection Service and Data Loss Prevention Cloud Service for Email

Service Description

April 2018

1. TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Overview

The Symantec Data Loss Prevention Cloud Detection Service and DLP Cloud Service for Email (the "Service") are hosted services that provide content inspection capabilities through the use of advanced content aware detection technologies. Application of user configured Data Loss Prevention ("DLP") policies to content submitted to the Service enables the identification of sensitive information contained within the submitted content.

Other Symantec or third party services integrating with the Service (each, an "Integrating Service") can send content for scanning of sensitive data to the Service. In return, the Integrating Service receives DLP policy violations and recommended remediation actions from the Service.

The Service is licensed for use in the following ways:

- **DLP Cloud Detection Service with Symantec CloudSOC™ CASB service**: The Service is used in conjunction with the Symantec CloudSOC™ CASB service to add Symantec DLP detection to cloud application data monitored by the CASB service. (Note: A separate subscription to CloudSOC™ CASB service is required. The Service Description for the Symantec CloudSOC™ CASB service is located at https://www.symantec.com/about/legal/repository.)
- **DLP Cloud Detection Service with Symantec Web Security Service**: The Service is used in conjunction with the Symantec Web Security Service (WSS) cloud-proxy to add Symantec DLP detection to outbound web traffic monitoring by the cloud-proxy. (Note: A separate subscription to WSS is required. The Service Description for the Symantec WSS service is located at https://www.symantec.com/about/legal/repository.)
- **DLP Cloud Detection Service** with a Symantec certified partner application (available under a separate license from Symantec) or with a Custom Integration (defined below). Customers may license a REST API of the DLP Cloud Detection Service from Symantec for purposes of adding DLP functionality to Customer's internally used application or service ("Custom Integration"), which DLP functionality can be invoked from such internally used application or service to perform DLP detection on data sent to the Service. Please contact your Symantec representative for more information about licensing Service's REST API for development of a Custom Integration.
- **DLP Cloud Service for Email**: The Service provides Symantec DLP detection to outbound email traffic by any of the following supported third party enterprise email service providers: Microsoft Office 365 Exchange Online, Microsoft Exchange Server, or Google G Suite Gmail. The Service can be used in conjunction with Microsoft Office 365 Exchange Online to perform DLP detection on outbound emails from Microsoft Office 365 Exchange Online, or can be used in conjunction with Symantec Email Security.cloud Safeguard to perform DLP detection on outbound emails from Microsoft Office 365 Exchange Online, Microsoft Exchange Server, or Google G Suite Gmail. (Note: A separate subscription to Email Security.cloud is required. The Service Description for Symantec Email Security.cloud service is located at https://www.symantec.com/about/legal/repository.)

Service Features

- Customer can create DLP policies, remediate incidents and access reports using Symantec's Enforce management console installed at Customer's premises ("Portal").
- The Service is intended to enable Customer to implement a valid and enforceable computer use policy, or its equivalent.
- The Service is monitored by Symantec for service availablity and service capacity on a twenty-four (24) hours/day by seven (7) days/week basis. The Service is also regularly monitored for service level compliance and adjustments may be made by Symantec as needed for maintaining service availability and service capacity.

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

Service Level Agreement

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

Supported Platforms and Technical Requirements

- Supported platforms and technical requirements are defined at: www.symantec.com/docs/DOC9414.

Service Enabling Software

- This Service includes Enabling Software (including the Symantec Enforce management console), which should be used only in connection with Customer's use of the Service during the Subscription Term. Use of the Enabling Software is subject to the license agreement accompanying such software ("Software License Agreement"). If no Software License Agreement accompanies the software, it is governed by the terms and conditions located at http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf. In the event of conflict, the terms of this Service Description prevail over any such Software License Agreement. Customer must remove Enabling Software upon expiration or termination of the Service.

2. CUSTOMER RESPONSIBILITIES

- Symantec can only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following responsibilities, 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.
    - *Service Activation*: Customer must follow required steps to activate the Service.
    - *On-premise installation and use of management console*: Customer must install and use an on-premise version of Enforce, the DLP Cloud Detection software management console.
    - *Customer Configurations*: Customer must configure features of the Service through the Enforce management console.
    - *Connecting Applications*: If the service is used by Customer with their Integrating Service, the Integrating Service must comply with the API specification for the REST API when calling the Service.
- Setup Enablement: Customer must provide information required for Symantec to begin providing the Service.
- Customers developing Custom Integrations must specify the name of the internally used application or service to be integrated with the Service using a Custom Integration request form provided by Symantec. Symantec reserves the right in its sole discretion to decline any proposed Custom Integration with the Service, and shall notify Customer promptly upon such determination.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist Symantec in delivery of the Service, upon reasonable request by Symantec.
- Renewal Credentials: If applicable, Customer must apply renewal credential(s) provided in the applicable Order Confirmation within its account administration to continue to receive the Service, or to maintain account information and Customer data which is available during the Subscription Term.

- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the Portal, if applicable, or default settings will apply. In some cases, default settings do not exist and no Service will be provided until Customer chooses a setting. Configuration and use of the Service(s) are entirely in Customer's control, therefore, Symantec is not liable for Customer's use of the Service, nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.
- Customer is responsible for obtaining all approvals and consents required by any third parties in order for Symantec to provide the Service. Symantec is not in default of its obligations to the extent it cannot provide the Service either because such approvals or consents have not been obtained or any third party otherwise prevents Symantec from providing the Service.
- Customer is responsible for its data, and Symantec does not endorse and has no control over what users submit through the Service. Customer assumes full responsibility to back-up and/or otherwise protect all data against loss, damage, or destruction. Customer acknowledges that it has been advised to back-up and/or otherwise protect all data against loss, damage or destruction.
- Customer is responsible for its account information, password, digital certificates, 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 may use a Sandbox subscription to the Service ("Sandbox") as follows:
    - A Sandbox subscription may be used solely on a non-production basis for purposes of testing the functionality of the Service.
    - Each Sandbox subscription is limited to use for up to one thousand (1000) Users.
- The foregoing restrictions apply whether Customer has purchased a Sandbox subscription in addition to a Service subscription, or a Sandbox-only subscription for testing.
- The following conditions apply to DLP Cloud Service for Email only:
    - Customer may choose to route emails scanned by the Service to Symantec Email Security.cloud or Microsoft Office 365 Exchange Online for delivery to recipients. Customer that chooses to route emails scanned by the Service to Symantec Email Security.cloud must have a concurrent subscription to the Symantec Email Security.cloud Safeguard service in order for Symantec to deliver the Service. Customer that chooses to route emails scanned by the Service to Microsoft Office 365 Exchange Online for delivery to recipients must have a concurrent subscription to the Microsoft Office 365 Exchange Online, maintain a valid certificate provided by Symantec for the Service, and designate the Symantec-provided certificate as trusted by Customer's Microsoft Office 365 Exchange Online service. Customer, and not Symantec, is solely responsible for any failure of the Service to function due to lack of valid certificate unless Symantec fails to provide such certificate.
    - Default maximum email size = thirty megabytes (30MB). Customer can specify any maximum email size up to fifty megabytes (50MB). Any emails that are received by the Service that exceed the specified limit will be scanned for the first fifty megabytes (50MB) of a received email against detection policy configured by Customer. If the first fifty megabytes (50MB) of a received email violates the policy, automated remediation actions will be applied to the entire email (including portions of the email beyond the 50MB threshold). Otherwise, if the first 50MB of a received email does not violate any policy, such email will be passed along to either Symantec Email Security.cloud or Microsoft O365 Exchange Online without application of any automated remediation action based on routing configurations chosen by Customer.
    - Customers must route their outbound email through the Service using the routing information provided by Symantec.
    - Customer must ensure that all domains (including sub-domains) requiring the Service are provisioned. Customer accepts that Service features may not function correctly and email delivery may be unavailable for domains that are not provisioned.

- 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 Symantec may temporarily suspend Service to Customer. In such an event, Symantec will promptly inform Customer and will work with Customer to resolve such issues. Symantec will reinstate the Service upon removal of the security threat.
- Should the Service be suspended for any reason whatsoever, the Service will not be applied to Customer's emails, and emails will not be routed through Symantec's Infrastructure. Customer is responsible for redirecting their email during suspension and confirming that all configurations are accurate if the Service is reinstated.
- Should a Service be terminated for any reason whatsoever, Customer's account will be deleted and Customer will not have access to the Service.
- Customer will not allow its systems to: (i) act as an Open Relay or Open Proxy or (ii) send Spam. Symantec reserves the right at any time to review Customer's compliance with this restriction. For the avoidance of doubt, any breach of this restriction will constitute a material breach of the Agreement and Symantec reserves the right to suspend all or part of the Service immediately and until the breach is remedied, or terminate the Agreement with respect to the affected Service.
- If at any time (i) Customer's email systems are blacklisted, or (ii) Customer causes the Symantec systems to become blacklisted due to the sending of Spam, or (iii) Customer fails to meet any of the obligations set out in this Service Description, Symantec shall inform Customer and reserves the right at its sole discretion to immediately withhold provision of, suspend or terminate all or part of the Service.
- The Service is only available to a Customer who has its own email domain name and has the ability to configure the MX records and/or DNS for that domain name.
- Customer must specify the mail server IP address(es) or hostname(s) for the delivery of inbound emails to their organization.
- Customer agrees to provide and maintain a list of valid email addresses (the "Validation List") to receive the Service. It is Customer's responsibility to verify the Validation List prior to the Service being made available and throughout the Term. Emails with email addresses not on the Validation List, or incorrectly entered, will be rejected by the Service. If Customer is unable to provide such Validation List and requests, Symantec will review each such request on a case-by-case basis and reserves the right to decline requests, in Symantec's sole and absolute discretion.

Acceptable Use Policy

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

3. ENTITLEMENT AND SUBSCRIPTION INFORMATION

Customer may use the Service only in accordance with the use meter or model under which Customer has obtained use of the Service: (i) as indicated in the applicable Order Confirmation; and (ii) as defined in this Service Description or the Agreement.

Charge Metrics

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

Per User License: "**User**" means an individual person (i) authorized to use the Service, (ii) benefitting from use of the Service, (iii) on behalf of whom Customer derives benefit from the use of the Service, or (iv) that actually uses any portion of the Service. Each subscription purchased for the Service may only be used by a single User in conjunction with a single Cloud Application. As used herein and for purposes of determining the applicable User count for the Service, "Cloud Application" means the target application or hosted service scanned by an Integrating Service. Where Symantec™ CloudSOC™ CASB service is the Integrating Service, each Securlet for a target application constitutes one Cloud Application and all Gatelets taken together constitute one Cloud Application. Where Symantec

Web Security Service (WSS) is the Integrating Service, WSS constitutes one Cloud Application that requires a DLP Cloud Detection Service subscription for each User licensed to WSS otherwise as a stand-alone service. In the case of AWS S3 as the Integrating Service, AWS S3 constitutes one Cloud Application whereby Customer must purchase a maximum User count of Service subscriptions (i.e., a Service subscription for each individual person within Customer's organization) for such Cloud Application.

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 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.

4. ASSISTANCE AND TECHNICAL SUPPORT

Customer Assistance.

Symantec will provide the following assistance a part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support.

If Customer is entitled to receive technical support ("Support") from Symantec, the Support as specified in Exhibit-B is included with the Service. If Customer is entitled to receive Support from a Symantec reseller, please refer to Customer's agreement with that reseller for details regarding such Support, and the Support described in Exhibit-B will not apply to Customer.

Maintenance

Symantec must perform maintenance from time to time. The following applies to such maintenance:

- *Planned Maintenance*. For Planned Maintenance, Symantec will use commercially reasonable efforts to give Customer seven (7) calendar days' notification, via email, SMS, or as posted on 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 Service 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 Service Infrastructure not undergoing maintenance in order to minimize disruption of the Service.
- *Emergency Maintenance.* Where Emergency Maintenance is necessary and is likely to affect the Service, Symantec will endeavor to inform the affected parties in advance via email or other written communications to customers no less than one (1) hour prior to the start of the Emergency Maintenance.
- *Routine Maintenance.* Symantec will use commercially reasonable efforts to perform routine maintenance at times when collective Customer activity is low to minimize disruption to the availability of the Service. Customer will not receive prior notification for these routine maintenance activities.

5. ADDITIONAL TERMS

- Customer may not disclose the results of any benchmark tests or other tests connected with the Service to any third party without Symantec's prior written consent.

- The Service may be accessed and used globally, subject to applicable export compliance limitations and technical limitations in accordance with the then-current Symantec standards.
- Any templates supplied by Symantec are for use solely as a guide to enable Customer to create its own customized policies and other templates.
- Symantec reserves the right to modify and update the features and functionality of the Service, with the objective of providing equal or enhanced Service (as long as Symantec does not materially reduce the core functionality of the Service). Customer acknowledges and agrees that Symantec reserves the right to update this Service Description at any time during the Subscription Term to accurately reflect the Service being provided, and the updated Service Description will become effective upon posting.

6. DEFINITIONS

"**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.

"Gatelets" means applications within the Symantec CloudSOC CASB that provide the ability to intercept traffic between Customer Users' devices and cloud applications.

"**Planned Maintenance**" means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure.

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

"**Enabling Software**" or "**Service Component**" means Software (defined below), as may be required by a Service, which must be installed on each Customer computer, in order to receive the Service. Enabling Software or Service Component includes the Software and associated documentation that may be separately provided by Symantec as part of the Service.

"**Software**" means each Symantec or licensor software program, in object code format, licensed to Customer by Symantec and governed by the terms of the accompanying EULA, including without limitation new releases or updates as provided hereunder.

"**Subscription Instrument**" means one or more of the following applicable documents which further defines Customer's rights and obligation related to the Service: a Symantec certificate or a similar document issued by Symantec, or a written agreement between Customer and Symantec, that accompanies, precedes or follows the Service.

"Subscription Term" means the period of time for which a Subscription is valid, as defined in each Subscription Instrument.

"Symantec Online Service Terms and Conditions" means the terms and conditions located at or accessed through https://www.symantec.com/about/legal/service-agreements.jsp.

EXHIBIT-A

SERVICE LEVEL AGREEMENT

General

- Customer must submit a claim for Service extension (each a "Claim") within ten (10) business days of the end of the calendar month in which the suspected Service level non-compliance occurred, and any Claim submitted outside of the provided timeframe will be deemed invalid.
- All Claims will be subject to verification by Symantec in accordance with the applicable provisions of this Service Level Agreement.
- This Service Level Agreement will not operate in the following instances (each, an "Excused Outage"): (i) during periods of Planned Maintenance or Emergency maintenance, periods of non-availability due to acts or omissions of either Customer or a third party; (ii) during any period of suspension of Service by Symantec in accordance with the terms of the Agreement; or (iii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); or (iv) if Customer has not configured the Service in accordance with the Agreement; or (v) during trial Service periods; or (vi) on the non-production Sandbox (test) instance of the Service; or (vii) during 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.
- The remedies set out in this Service Level Agreement are Customer's sole and exclusive remedies in contract, tort (including without limitation negligence) or otherwise, with respect to this Service Level Agreement.
- 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.
- 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. Hardware, software or other data center equipment or services not provided by Symantec as part of the Service under this Service Description.
  iii. Hardware or software configuration changes made by Customer without the prior written consent of Symantec.

Availability

- Service Availability for the DLP Cloud Detection Service for any month will be no less than ninety-nine and five-tenth percent (99.5%). Service Availability for the DLP Cloud Service for Email for any month will be no less than ninety-nine and nine-tenth percent (99.9%). "Service Availability" means the ability to send content for inspection to the Service as measured by the Symantec Availability Monitor that monitors the Service instance at Symantec. This Service Availability shall only apply if the Service configuration and associated policies are correctly configured in the Service through Customer's Enforce management console.

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 specified in Exhibit-A, 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) additional days of the Service for each one (1) hour or part thereof that the Service is not available, subject to a maximum of a one (1) additional week of the Service per incident of un-availability and subject to the maximum of four (4) service extensions for any one (1)-year period of the Service.

Chronic Failure

- In the event Service Availability falls below ninety eight percent (98%) in any calendar month, Customer is entitled to terminate the affected Service and receive a pro rata refund of charges paid in advance for the affected Service for the period after termination.

EXHIBIT-B

TECHNICAL SUPPORT

- Support is available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Customer with configuration of the Service features and to resolve reported problems with the Service.
- Whenever a Customer raises a problem, fault or request for Service information via telephone or web submission with Symantec, its priority level is determined and it is responded to per the response targets defined in the table below. Faults originating from Customer's actions or requiring the actions of other service providers are beyond the control of Symantec and as such are specifically excluded from this Support commitment.

PROBLEM SEVERITY	SUPPORT (24x7) RESPONSE TARGETS FOLLOWING ACKNOWLEDGEMENT
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, although 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: One of the following: a problem where Customer's business operations have not been adversely affected or a suggestion for new features or an enhancement regarding the Service or Enabling Software.	within the next business day; Symantec further recommends that Customer submit Customer's suggestion for new features or enhancements to Symantec's forums