Symantec™ Data Loss Prevention Cloud Detection Service

Service Description

September 2017

TABLE OF CONTENTS

A. SERVICE OVERVIEW

The Symantec Data Loss Prevention Cloud Detection Service (the "Service") is a hosted service that provides a REST–based API for detection of sensitive data by applying data loss prevention ("DLP") policies. Services integrating (each, an "Integrating Service") with the Service through this API can send content for scanning of sensitive data to the Service through the REST-based API. In return, the Integrating Service receives DLP policy violations and recommended remediation actions from the Service.

This Service Description, with any attachments included by reference, is part of (i) any signed agreement between Symantec and Customer that is intended to govern this Service Description; or (ii) if no such signed agreement exists, the Symantec Online Services Terms and Conditions or the Symantec Hosted Services Terms, as applicable to Customer's use of the Service (each, an "Agreement"). Capitalized terms shall have the meaning set forth in the Definitions section set forth below or the agreement which incorporates this Service Description.

B. TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

The Service is intended to enable Customer to implement a valid and enforceable computer use policy, or its equivalent. The Service is managed on a twenty-four (24) hour/day by seven (7) day/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 Features

The Service is comprised of the following features:

- A REST-based API that can be invoked by integrating applications to perform DLP detection on data sent to the Service in the API call.
- Advanced Content Detection including Exact Data Matching (EDM), Indexed Document Matching (IDM), Described Content Matching (DCM) with keywords, data identifiers or regular expressions, and Vector Machine Learning (VML) provides highly accurate detection of sensitive data in cloud data repositories.

- Flexible and granular scan and policy controls based on data owners, file sizes and file types as well as content such as customer personally identifiable information (PII), or intellectual property data.
- Incident generation with incident data that includes rich contextual information, sensitive content matches, policy violations, as well as applied remediation.
- Symantec's Enforce management console installed at Customer's premises provides policy creation, incident management, Service configuration and report generation functionality.

Supported Platforms and Technical Requirements

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

Hosted Service Software Components

The Service includes the following software Service Components available upon activation:

- The Enforce management console provides policy creation, incident management, Service configuration and report generation functionality for the Service.

Customer Use and Responsibilities

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 Subscription Instrument or Order Confirmation; and (ii) as defined in this Service Description or the Agreement. Each subscription purchased for the Service may be used by a single User in conjunction with a single Cloud Application. "Cloud Application" means the target application scanned by the Integrating Service. For instances where Elastica is the Integrating Service, each Elastica Securlet for a target application constitutes one Cloud Application and "All Elastica Gatelets" together constitute one "Cloud Application".

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.

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: Connecting applications must comply with the API specification for the REST API when calling the service.

Assistance and Technical Support

Customer Assistance Team**.** Symantec will provide the following assistance as part of the Service:

- Receive and process orders for implementation of the Service;
- Receive and process requests for permitted modifications to operational aspects of the Service; and

- Respond to billing and invoicing questions.

Technical Support Team**.** The following technical support is included with the Service:

- Support available on a twenty-four (24) hour/day by seven (7) day/week basis to:
  a) provide technical support to Customer for problems with the Service; and
  b) communicate with Customer to resolve such problems.

If a Customer contacts the Technical Support team via telephone or email, the severity level of the request is determined by, and response time defined by, the table below:

Severity Level	Definition	Response Target
1	Loss of Service	Except for Sandbox, calls responded to within 30 minutes For Sandbox, calls responded to within 8 hours
2	Partial loss of Service or Service impairment	Except for Sandbox, calls responded to within 2 hours For Sandbox, calls responded to within 8 hours
3	Potentially Service affecting or non-Service affecting information request	Calls responded to by same time Next Business Day

Maintenance

Symantec must perform maintenance on the Service Infrastructure in order to provide the Service. The following applies to such maintenance:

- *Planned Maintenance*. Symantec will use commercially reasonable efforts to give Customer seven (7) calendar days' notification via email for Planned Maintenance. 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 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 Customers in advance by posting an alert on the management console or by delivering an alert via email no less than one (1) hour prior to the start of the Emergency Maintenance.
- *Routine Maintenance.* Symantec will use commercially reasonable efforts to perform maintenance on the DLP Cloud Service when collective Customer activity is low, to minimize disruption to the availability of the Service and management console, respectively. Customer will not receive prior notification for these routine maintenance activities.

C. SERVICE CONDITIONS

- Should a Service be terminated for any reason whatsoever, Customer's account will be deleted and Customer will not have access to the Service. Symantec is not liable for any damage or loss resulting directly or indirectly from any failure of the Service or from any bug in the service when performing detection of sensitive data.

D. SERVICE LEVEL

Service Availability

- Service Availability for the Service for any month will be no less than ninety-nine and five-tenth percent (99.5%). Service Availability means the ability to invoke REST API calls 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 the customer's Enforce management console.
- The foregoing Service Availability will not apply: (i) during periods of Planned Maintenance, Emergency Maintenance, or of non-availability due to force majeure or 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; (iii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); (iv) if Customer has not configured the Service in accordance with the Agreement; (v) during trial service periods or (vi) on the non-production Sandbox (test) instance of the Service.

E. MISCELLANEOUS

Service Renewal

- Notwithstanding anything to the contrary in the Agreement, the Service does not renew automatically. To renew the Service, Customer must submit a renewal order at least sixty (60) days prior to expiration of the Service. To renew a Sandbox subscription, Customer must also purchase a Service subscription.
- Customer must provide reasonable assistance to Symantec to complete the processing of the Renewal Order and must apply required renewal credentials to renew the service and maintain account information and data available during the Service Term.

General

- Symantec may update the Service at any time in order to maintain the effectiveness of the Service. Symantec may update this Service Description from time to time to accurately reflect the Service being provided.
- 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.
- Customer is permitted to use the Service solely for Customer's own business purposes. Customer agrees not to resell, sublicense, lease, or otherwise make the Service and associated documentation available to any third party. Customer agrees not to use the Service for the purposes of building a competitive product or service or copying its features or user interface, performing Service evaluations, benchmarking or other comparative analysis intended for publication outside Customer organization without Symantec's prior written consent.
- 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, Customer is solely responsible for, and Symantec is not liable for, Customer's use of the Service(s), nor is Symantec liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.
- 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 use of any Service Component in the form of software shall be governed by the license agreement accompanying the software. If no EULA accompanies the Service Component, it shall be governed by the terms and conditions located at (http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf). Any additional rights and obligations with respect to the use of such Service Component shall be as set forth in this Service Description.

- Except as otherwise specified in the Service Description, the Service (including any Hosted Service Software Component 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 http://www.symantec.com/about/profile/policies/cloud-services-agreements.jsp.
- Any templates supplied by Symantec are for use solely as a guide to enable Customer to create its own customized policies and other templates.

F. DEFINITIONS

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement or this Services Description, have the meaning given below:

"**Email**" means any inbound or outbound SMTP message passing through the Service.

"**Emergency Maintenance**" means unscheduled maintenance periods 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.

"**End User License Agreement (EULA)**" means the terms and conditions accompanying Software (defined below).

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

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

"**Service Component**" means certain enabling software, hardware peripherals and associated documentation which may be separately provided by Symantec as an incidental part of a Service.

"**Service Software**" 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. Service Software 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.

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

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

"**User**" means an individual person and/or device authorized to use and/or benefits from the use of the Service, or that actually uses any portion of the Service.

"**Virus**" means a piece of program code, including a self-replicating element, usually disguised as something else, which is designed so that it may infect other computer systems.