Symantec™ Cyber Security: DeepSight™ Intelligence

Service Description

June 2019

This Service Description describes Symantec's Cyber Security: DeepSight™ Intelligence services comprising of either DeepSight™ Intelligence portal services ("**Intelligence Portal**") or DeepSight™ Intelligence datafeed services ("**Datafeeds**") (each a "**Service**" or collectively, "**Services**"). 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 Service 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™ Cyber Security: DeepSight™ Intelligence services are Symantec threat intelligence services comprising of either Intelligence Portal or Datafeeds, depending on the specific Service purchased by Customer. The Intelligence Portal Service is a threat intelligence service that allows Customer to view security information such as vulnerability data, malcode, cyber threats and adversary information. Datafeeds provide Customer access to one or more datafeeds containing various security data depending on the datafeed purchased.

Service Features

The following table illustrates the features associated with each Service:

Service Feature	Intelligence Portal – Standard	Intelligence Portal – Enterprise	Intelligence Portal – Advanced Enterprise	Datafeeds	Service Feature Description
Use Level	Up to two(2) Users	Per Managed User	Per Managed User	Per Managed User	Intelligence Portal – Standard is available on a per User basis up to a maximum of two (2) Users. Intelligence Portal – Enterprise and Advanced Enterprise and Data feeds Services are available on a per Managed User basis.
Managed Services Portal	●	●	●	●	Access to the Managed Services Portal is limited to Authorized Personnel. Certain features and functionality of the Managed Services Portal may vary based on the Service purchased by Customer.
Administrators	2	5	5	1	The number of Administrators that Customer may Register (as defined below) to access and use the applicable Service, including access and use of the Managed Services Portal and Symantec Materials. Administrators may additionally designate a reasonable number of non-Administrators to access and use the Services, subject to the limitations set forth in the Agreement.
Alert Creation	●	●	●		Authorized Personnel may configure Alerts to receive notifications on new/updated vulnerabilities, malcode, security risks, and other security data available in the Global Intelligence Network (GIN).
Email Delivery	●	●	●		Authorized Personnel may designate their email address as an electronic delivery method for Alert Information through the Managed Services Portal.
XML Delivery		●	●		Authorized Personnel may designate XML as an electronic delivery method for certain Alert Information through the Managed Services Portal.
MATI Reports			●		See service feature description below.
Custom Reports		●	●		Authorized Personnel may access certain custom reports that Symantec may make generally available to all customers through the Managed Services Portal.

Service Feature	Intelligence Portal – Standard	Intelligence Portal – Enterprise	Intelligence Portal – Advanced Enterprise	Datafeeds	Service Feature Description
API Calls		●	●	●*	Provides access to intelligence content through API calls (up to a certain number each 24-hour period) without manually logging onto the Managed Services Portal or downloading the Datafeed. The number of API calls included and the type of intelligence content accessible by API calls are determined by Customer's subscription to DeepSight Intelligence services.
DeepSight Security Risk Datafeed				●*	**Provides, in XML format, access to malicious code data and security risk data, including adware and spyware.**
DeepSight Vulnerability Datafeed				●*	**Provides, in XML format, access to vulnerability information, including mitigation guidance, impact analysis, SCAP related data, and links to security patches when available.**
DeepSight IP Reputation Datafeed				●*	**Provides, in XML, CSV or CEF format, access to reputation, hostility and confidence ratings of Internet protocol addresses, derived from threat analysis of data from the Symantec Sensor Network.**
DeepSight Advanced IP Reputation Datafeed				●*	**Provides, in XML, CSV or CEF format, access to reputation, hostility, confidence ratings, (as well as ownership, geolocation, and industry, where such data is available) and malicious behavior details of Internet protocol addresses, derived from threat analysis of data from the Symantec Sensor Network.**
DeepSight Domain Name & URL Reputation Datafeed				●*	**Provides, in XML, CSV or CEF format, access to reputation, hostility and confidence ratings of domains, Universal Resource Locators, derived from threat analysis of data from the Symantec Sensor Network.**
DeepSight Advanced Domain Name & URL Reputation Datafeed				●*	**Provides, in XML, CSV or CEF format, access to reputation, hostility, confidence ratings, (as well as ownership, geolocation, and industry, where such data is available) and malicious behavior details of domains and associated Universal Resource Locators, derived from threat analysis of data from the Symantec Sensor Network.**

*This Datafeed is only available to customers who have specifically purchased it, as indicated in the applicable Order Confirmation.

MATI Service Feature Description

Symantec's Managed Adversary and Threat Intelligence ("**MATI**") team of global researchers and analysts is dedicated to understanding the cyber threat ecosystem and providing context-rich intelligence reporting on adversaries so that customers can better respond to current and emerging threats. MATI is built upon Symantec's deep experience tracking the world's most prolific and sophisticated cyber threat actors, and utilizes a wide array of research methodologies and sources to identify and assess adversary behavior and attempt to provide a future outlook on that behavior.

Intelligence Portal – Advanced Enterprise customers can access periodic MATI reporting ("**MATI Reports**") on the latest developments in significant cyber threat campaigns. MATI Reports may include:

- Narrative analysis of the latest campaign activities, patterns, and trends;

- Actor attribution and identifiers (*e.g.*, email addresses, Internet Protocol addresses, and usernames/accounts);
- Actionable technical details of campaign tools and adversary tactics, techniques, and procedures (*e.g.*, vulnerabilities exploited, hash values of malware deployed, traits of portable executables, and other indicators of compromise);
- Characteristics of malicious infrastructure (*e.g.*, domains, uniform resource locators, IPs, autonomous system numbers, and geo-location); and
- Target identifiers (*e.g.*, industries, job functions, and other traits).

The MATI team harvests cyber threat insights from Symantec's proprietary Global Intelligence Network as well as from commercially available datasets and publicly available Internet resources, including limited-access marketplaces and forums. All MATI research activities are governed by Symantec's internal protocols and oversight mechanisms intended to ensure they are conducted ethically and in accordance with applicable laws and regulations.

Additionally Available Service (Optional)

For additional fees, Symantec offers the following options to complement DeepSight Intelligence services:

- **DeepSight Intelligence Directed Threat Research**

  Customers that purchase DeepSight™ Intelligence Directed Threat Research will receive Tokens for each purchase, which allows Authorized Personnel to request certain custom reports from Symantec.

  - Tokens are valid for twelve (12) months from the date of purchase. Unused Tokens will expire after the validity period is over.
  - For Customer to use unexpired Tokens, Customer must have a current and valid ***Intelligence Portal – Advanced Enterprise*** license. Customer must access the Managed Services Portal and submit requests for or view Directed Threat Research reports.
  - All costs (measured in Tokens) are per report. The exact cost of any requests will be determined when the request is received by the MATI team based on the scope of the request. Various factors affect the cost of a request. Please contact Symantec for details. Once the scope and cost have been confirmed, Tokens will be deducted from your account, and further changes will not be accepted.
  - Symantec reserves the right to decline all or any portion of a Directed Threat Research request.
  - Symantec will deliver Directed Threat Research reports when completed.
  - Directed Threat Research reports are subject to the same protocols as MATI Reports, as described above.

- **DeepSight Additional API Calls**

  Customers that purchase additional API calls can increase the number of daily API call capacity included in DeepSight™ Intelligence services.

  - Additional API calls are available for purchase in increments of 1,000 (per day).
  - Additional API calls are valid for twelve (12) months from the date of purchase. Unused API call capacity will expire after the validity period is over.
  - For Customer to use additional API calls, Customer must have a current and valid DeepSight Intelligence services. (The API call functionality is not available with *Intelligence Portal - Standard*).

- The number of daily API call capacity included in DeepSight Intelligence services are as follows:

Intelligence Portal	API Calls / Day			
	N/A	1,000	2,000	3,000
Standard	●			
Enterprise		●		
Advanced Enterprise				●
Datafeeds	**API Calls / Day**			
	N/A	1,000	2,000	3,000
Security Risk		●		
Vulnerability		●		
IP Reputation			●	
Domain & URL Reputation			●	
Adv. IP Reputation				●
Adv. Domain / URL Reputation				●

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.

- Customer must first register ("**Register**") the serial number(s) printed on the Order Confirmation in the licensing section of the MySymantec portal located at https://my.symantec.com/ and appoint the Administrators associated with the Services ("**Registration**").
- Customer is solely responsible for acquiring and maintaining the Internet or telecommunications services and devices required to receive, access or use the Services or Symantec Materials.
- Datafeeds, any datasets within the Datafeeds and APIs to access them are Symantec's proprietary and confidential information. Customer must promptly notify Symantec after becoming aware of any unauthorized access to, acquisition, disclosure, loss, or use of the Symantec Datafeeds (including datasets thereof) or APIs.

3: Entitlement and Subscription Information

Charge Metrics

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

- Intelligence Portal – Standard is available on a per User basis up to a maximum of two (2) Users. Intelligence Portal – Enterprise and Advanced Enterprise and Data feeds Services are available on a per Managed User basis.
- "**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.
- "**Managed Users**" means the total number of Customer's employees (excluding third party contractors), and is reflected in the banded amount in the SKU Description for Services set forth in the Order Confirmation.

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: Definitions

*"***Administrator**" means an employee or third-party contractor designated by Customer to have administrative access to and use of the Services, including the Managed Services Portal and Symantec Materials, and are identified upon Registration or thereafter within the Managed Services Portal. In the event of a conflict, those Administrators identified within the Managed Services Portal will control over Administrators identified at the time of Registration.

"**Alert Information**" means the alert messages, data and/or information that Symantec provides or makes available pursuant to the Services.

"**Authorized Personnel**" means, collectively, Administrators and any additional personnel Administrators have designated as non- Administrators to access and use the Services, subject to the limitations set forth in the Agreement.

"**Managed Services Portal**" means Symantec's password-protected intelligence portal website, currently located at deepsight.symantec.com, including any Symantec subsites accessible via the Managed Services Portal, and all content accessible on such sites.

"**Service Credit**" means the number of days that are added to Customer's current Subscription Term.

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

"**Symantec Online Services Terms and Conditions**" means the terms and conditions located at or accessed through https://www.symantec.com/about/legal/repository.

"**Tokens**" means the total number of units purchased and redeemable for Directed Threat Research reports.

"**User**" means a Customer employee or third-party contractor and is reflected in the SKU Description for Services set forth in the Subscription Instrument.