

# Symantec Threat Explorer

## 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 Threat Explorer (“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

#### **2: Customer Responsibilities**

#### **3: Entitlement and Subscription Information**

- Charge Metrics

#### **4: Assistance and Technical Support**

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

#### **5: Definitions**

#### **Exhibit-A Service Level Agreement**

# Symantec Threat Explorer

## SaaS Listing

---

### 1: Technical/Business Functionality and Capabilities

#### Service Overview

Symantec Threat Explorer is a stand-alone offering that compliments WebPulse enabled products. There are two different product offerings for Threat Explorer: Standard and Advanced (described below).

#### Symantec Threat Explorer Standard with Research Portal and Web Isolation

The Threat Explorer Standard offering features a research portal. Via the portal, subscribers can perform single or bulk queries of URLs and file hashes. Queries for URLs show the WebPulse URL: Category, Risk Level, rating history, as well as a multitude of other metadata such as server/IP information, WHOIS, SSL certificate, geo-location, and WebPulse community correlation. Queries for file hashes show the risk level of the file, along with associated CA metadata if the file is considered malicious. Finally, the Service includes the ability to manage users via Symantec Norton Secure Login. Administrators of the Service can create, delete and modify additional users and their privileges.

#### Symantec Threat Explorer Advanced with Research Portal, API, and Web Isolation

The Threat Explorer Advanced offering includes everything from Threat Explorer Standard but with more enhanced features. Customers of Threat Explorer Advanced have access to a suite of APIs that allow them to query Threat Explorer URL metadata programmatically.

#### Service Features

- The Service allows Customer to research URLs via a web portal and an API
- 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 is granted the right to use the Service only for the purposes of threat research in relation to supporting Symantec Network Protection Products' security processes and workflows.

#### Service Level Agreement

- CA provides the applicable service level agreement ("SLA") for the Service as specified in Exhibit-A

### 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 as noted below.

- Setup Enablement: Customer must provide information required for CA to begin providing 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. Customer's configuration cannot be saved if Customer's Subscription Term is terminated or otherwise interrupted.

### 3: Entitlement and Subscription Information

#### Charge Metrics

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

- **“Query”** means a single URL categorization inquiry performed by Customer using the SWAT URL lookup functionality, including any identical or duplicate inquiries.
- **“Submission”** means a single URL categorization suggestion performed by Customer using the SWAT URL category submission functionality, including any identical or duplicate suggestions.

SWAT is sold based on volume tiers and Customer’s Order Confirmation determines and limits the number of Queries and Submissions Customer may perform each day (UTC 00:00 to 24:00). Queries and Submissions are metered independently of each other, meaning a Customer’s daily limit for each is measured independently of the other.

### 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](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*
<b>Severity 1:</b> 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
<b>Severity 2:</b> 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

# Symantec Threat Explorer

## SaaS Listing

<b>Severity 3:</b> A problem has occurred with a limited adverse effect on Customer's business operations.	By same time next business day**
<b>Severity 4:</b> 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 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.

"**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:

- o **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.

<b>Inline Service Availability</b>	<b>N/A</b>
------------------------------------	------------

- o **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).

<b>Non-Inline Service Availability</b>	<b>99.5%</b>
--	--------------

### 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.

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