

# Symantec Intelligence Services

Blocking 99.99% of Emerging Threats with Advanced Threat Defense Solutions and Up-To-The-Minute Global Threat Intelligence

## At A Glance

### Global Intelligence

The Global Intelligence Network enables Intelligence Services to deliver global, fast content categorization to support enterprise security and compliance activities.

### Always Up-To-Date

Web and content intelligence feeds are updated in real-time, in the cloud, to address the latest threats; updates are propagated throughout the globe within minutes.

### Web Application Visibility & Control

Application intelligence provides visibility into sanctioned and un-sanctioned usage of key web applications to eliminate risks related to the inappropriate use of these applications. It enables control policies that extend governance and security beyond just URL-based controls.

### Blocks 99.99% of Threats

Comprehensive intelligence, with real-time updates, helps enterprises cost-effectively identify 99.99% of known and emerging threats.

The attacks of today's cybercriminals are increasingly ingenious and sophisticated in their efforts to target enterprise networks. The attacks employ various techniques to avoid detection as they carry out their malicious activities. While attackers are building their innovative arsenal, enterprises are playing catch up, trying to deploy technologies that will effectively protect them from these criminal attacks. What is needed are adaptive, up-to-date technologies and intelligence capable of defending enterprise networks against today's most advanced cybercriminals.

Powered by the Global Intelligence Network, Symantec Intelligence Services deliver fast, real-time global content categorization to empower advanced threat defenses and support ongoing enterprise compliance. Trusted by more than 15,000 enterprises globally, including over 70% of the Fortune 500, Symantec Intelligence Services allow businesses to implement risk control policies to extend web security to cloud applications. A strategic component of the Symantec Security Platform, Intelligence Services employ 200+ analytics engines to identify mass-market, targeted threats, blocking more than 99.99% of known and emerging threats.

## Advanced Global Intelligence Network Infrastructure

The Symantec Global Intelligence Network is a collaborative cloud infrastructure that collects, processes and distributes content and threat intelligence on a worldwide scale. As a web security partner to more than 15,000 of the world's largest enterprises, including over 70% of the Fortune Global 500 companies, Symantec has the ability to dynamically analyze and categorize new content, as soon as it is introduced. With more than 200 threat analytics engines, the Global Intelligence Network can process more than one billion web and file requests daily, in 55 languages. It is truly the most advanced real-time content and threat categorization network available today.

The Global Intelligence Network is also managed and backed by a team of the industry's most seasoned researchers and security experts from Symantec Labs. The team has developed effective algorithms for identifying, categorizing and blocking malicious content and malnet infrastructures before an attack can occur, making the Global Intelligence Network an integral

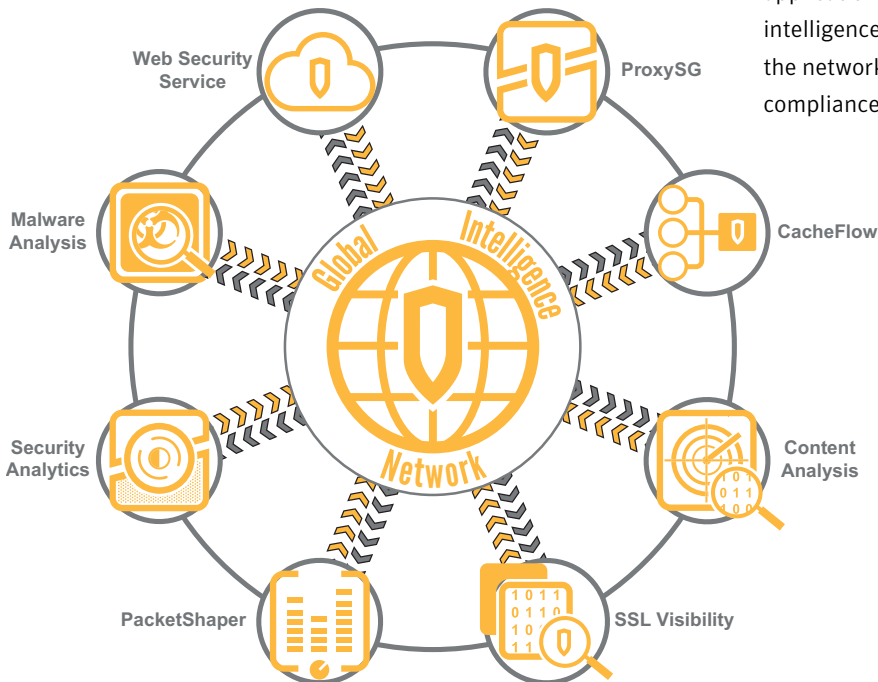


part of Symantec’s “negative-day” security capabilities. When a zero-day attack starts, the negative day defenses are already in place to eliminate the threat. Customers enjoy the confidence and peace of mind that their networks are well protected before those malicious attacks can even begin.

## Comprehensive Intelligence with Real-Time Updates

Like a chameleon that frequently changes its color to hide from predators looking for it, cybercriminals are constantly changing their identities and URLs trying to hide and avoid detection by your threat defense system. Recent research of “One Day Wonders” by Symantec Labs found that more than 71% of websites existed for only a very brief period of time (less than 24 hours). These “One-Day Wonder” websites are an ideal way for attackers to hide their malicious activities, using these new/unknown sites to launch or perpetrate their attacks.

With Intelligence Services, new applications and websites are analyzed by analytics engines in real time, and the intelligence is distributed throughout the network within minutes. As a result, enterprises always have the most comprehensive, up-to-the-minute threat intelligence to protect their networks from the web’s most advanced threats.



## Embrace the Web with Confidence

The world is becoming increasingly connected. The web not only is the central hub for people to get information and stay connected, it also helps businesses become more competitive by delivering scalability, efficiency and cost savings. This presents new challenges for IT, network and security professionals. Web traffic and web applications open up the door for potential malicious attacks and they make it easy for company data, including potentially sensitive enterprise information, to be accessed, distributed and altered outside of the protected corporate network. Special attention must be paid to policies that can help identify and protect web traffic and prevent sensitive data from going into these web applications.

The Symantec URL Threat Risk Levels and Geo IP intelligence delivered through the Intelligence Services, provide geo location information and assign risk ratings to millions of websites, to enable enterprises to implement granular and effective controls over their web traffic. With Symantec, enterprises can customize and deploy threat risk control policies based on their specific business needs and risk tolerance levels. They can eliminate high-risk web traffic, while allowing access to sanctioned websites and applications with acceptable risk levels. Through easy-to-use reports, administrators can quickly identify the top websites, applications and usage trends, understand their impact on the network bandwidth, and identify potential risky websites and applications introduced in the network. Equipped with this intelligence, administrators can make necessary adjustments to the network and security controls to ensure full corporate policy compliance without over-blocking.

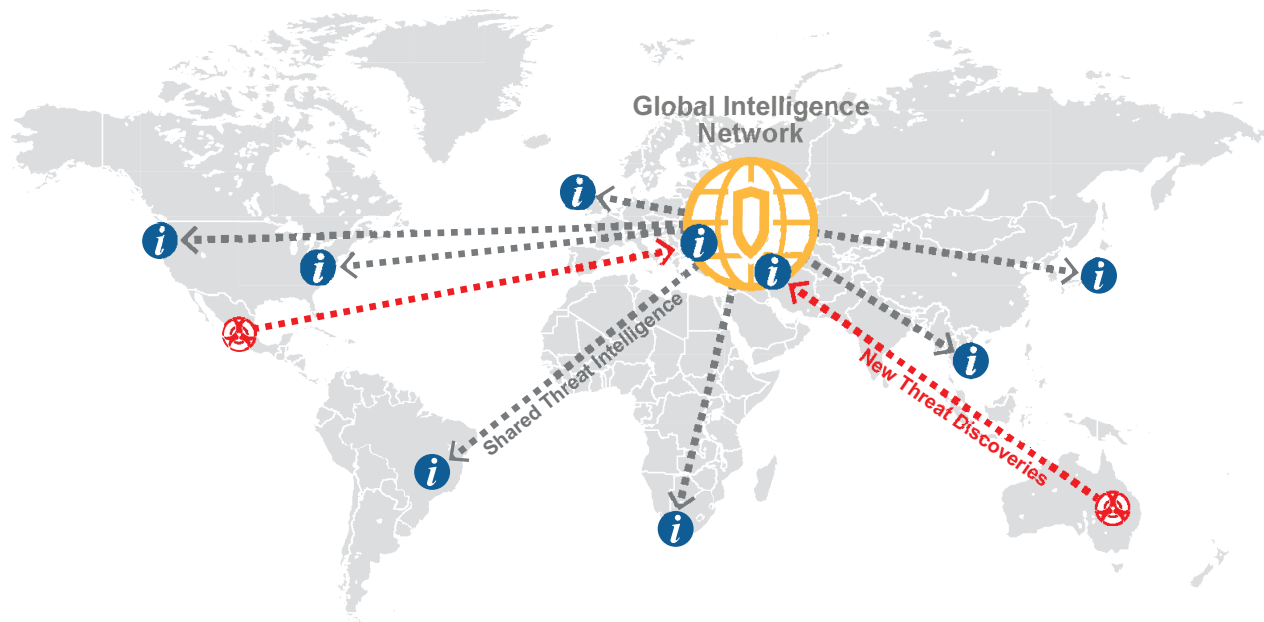
## Proven and Effective Threat Protection

Behind every successful security product, there is great threat intelligence. That statement certainly rings true for Symantec's Advanced Threat Defense solutions. Powered by expertise from Symantec Labs and over 200 threat analysis engines, the Global Intelligence Network processes more than one billion previously uncategorized new web requests and blocks over four million previously unseen or uncategorized threats every single day. The Intelligence Services, powered by the Global Intelligence Network, help enterprises stop attacks as they occur and keep malicious threats out of the network. Through the highly accurate intelligence feeds, enterprises are able to identify and stop 99.99% of threats at the gateway, so they never have a chance to enter the network. This reduces the resources and capital typically required to support locally deployed content analysis and sandboxing solutions – customers can eliminate much of the \$1.27M<sup>1</sup> operational costs due to false alarms.

<sup>1</sup> Ponemon Institute LLC, January 2015

## Intelligence Services Subscription

Intelligence Services are offered on supported Symantec products via a subscription license. Please consult the individual product datasheets for details on the subscriptions and release versions supported by that specific product. Intelligence Services subscription licenses are generally structured as bundles with various data feeds described in the Intelligence Services table below. There are two types of services; Web and Application services each containing different types of data feeds. Additional services and bundles may be introduced in the future, as new services become available and new product requirements emerge.



Global Intelligence Network Provides Real-time Intelligence Sharing Among Millions of Users Worldwide

## Data Feed Definitions

DATA FEED	DESCRIPTION
CONTENT CATEGORIES	The <i>Content Categories</i> data feed delivers a real-time, cost-effective approach for customers who are focused on acceptable use/compliance policies. These content-based categories can be used to classify websites for compliance with Internet access policies. Security categories are not included, but are available as separate data feeds.
SECURITY CATEGORIES	The <i>Security Categories</i> data feed is designed to deliver real-time threat intelligence for customers who have a need to implement security policies. It consists of unique security categories, including "Malicious Sources", "Suspicious" and "Proxy Avoidance" to help identify and stop malicious threats against enterprise networks and users.
URL THREAT RISK LEVELS	The <i>Threat Risk Levels</i> data feed is a composite URL risk index for threat analysis and security policy creation. It allows enterprises to eliminate the riskiest traffic in acceptable categories and simplify complex category-based policies, without over-blocking.
GEO LOCATION	<i>Geo Location</i> provides geo intelligence that allows enterprises to set country-specific or region-specific policies to manage network traffic flows. It is typically used for compliance or to limit/eliminate access to known high risk regions.
BASIC WEB APPLICATION CONTROLS	The <i>Basic Web Application Controls</i> is a data feed comparable to the data feed available in Symantec WebFilter which provides visibility for 180 web applications. It allows for classification of applications, and user operations for access logging and policy control.

DATA FEEDS	WEBFILTER COMPARISON	INTELLIGENCE SERVICES STANDARD WEB BUNDLE	INTELLIGENCE SERVICES ADVANCED WEB BUNDLE	
CONTENT CATEGORIES	✓	✓	✓	Establish compliance and enforcement policies for appropriate web access
SECURITY CATEGORIES	✓	✓	✓	Reduce and stop threat risks based on security categories
URL THREAT RISK LEVELS			✓	Fine-tune risk management without over-blocking with 10 risk levels
GEO LOCATION			✓	Geo intelligence and compliance with location-based policies
BASIC WEB APP CONTROL	✓	✓	✓	Visibility and metadata for 180 web applications

Note:  
Symantec Intelligence Services requires SGOS Version 6.6.3 or higher

## About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | [www.symantec.com](http://www.symantec.com)

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit [www.symantec.com](http://www.symantec.com) or connect with us on Facebook, Twitter, and LinkedIn.