SOLUTION BRIEF

Symantec® Intelligence Services

Block 99.99% of emerging threats with advanced threat defense solutions and up-to-the-minute global threat intelligence.

AT A GLANCE

- **Global Intelligence:** The GIN enables Symantec Intelligence Services to deliver global, fast content categorization and threat risk levels 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 and Control:** Application intelligence provides visibility into sanctioned and unsanctioned usage of over 45,000 key web applications to eliminate risks related to the inappropriate use of these applications.
- **Blocks 99.99% of Threats:** Comprehensive intelligence, with real-time updates, helps enterprises cost-effectively identify 99.99% of known and emerging threats.
- **Threat Explorer and Automation Toolkit:** Research detailed threat metadata with the Threat Explorer research portal and the available API. Automate daily administration tasks like category lookups with the Symantec Webpulse Automation Toolkit API.

Overview

The attacks of today's cyber criminals 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 cyber criminals.

Powered by the Symantec® Global Intelligence Network (GIN), Symantec Intelligence Services deliver fast, real-time global content categorization to empower advanced threat defenses and support ongoing enterprise compliance. Trusted by thousands of global enterprises, 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 to Symantec security solutions, Intelligence Services employ 200+ analytics engines to identify mass-market and targeted threats, blocking more than 99.99% of known and emerging threats.

Advanced Global Intelligence Network Infrastructure

The Symantec GIN is a collaborative cloud infrastructure that collects, processes, and distributes content and threat intelligence on a worldwide scale. As a web security partner to some of the world's largest enterprises, Symantec security solutions have the ability to dynamically analyze and categorize new content, as soon as it is introduced. With more than 200 threat analytics engines, the GIN can process more than one billion web and file requests daily, in over 60 languages. It is truly the most advanced real-time content and threat categorization network available today.

The GIN is also managed and backed by a team of the industry's most seasoned researchers and security experts from researchers and security experts. The team has developed effective algorithms for identifying, categorizing, and blocking malicious content and malnet infrastructures before an attack can occur, making the GIN an integral part of these "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, cyber criminals are constantly changing their identities and URLs to hide and avoid detection by your threat defense system. Research of One-Day Wonders by our security experts found that more than 71% of websites exist 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 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.

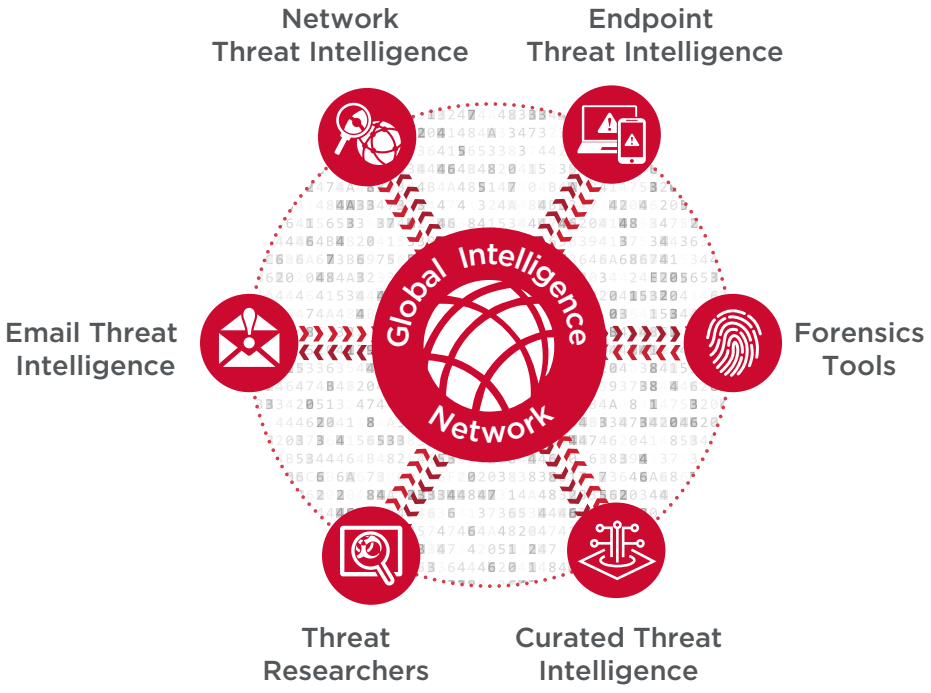
Embrace the Web with Confidence

The world is becoming increasingly connected. The web is not only the central hub for people to get information and stay connected, but 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 the door to potential malicious attacks and 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 URL Threat Risk Levels and Geo IP intelligence delivered through Intelligence Services assign risk ratings and provide geolocation to millions of websites to enable enterprises to implement granular and effective controls over their web traffic. With these tools, 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 overblocking.

Figure 1: The GIN



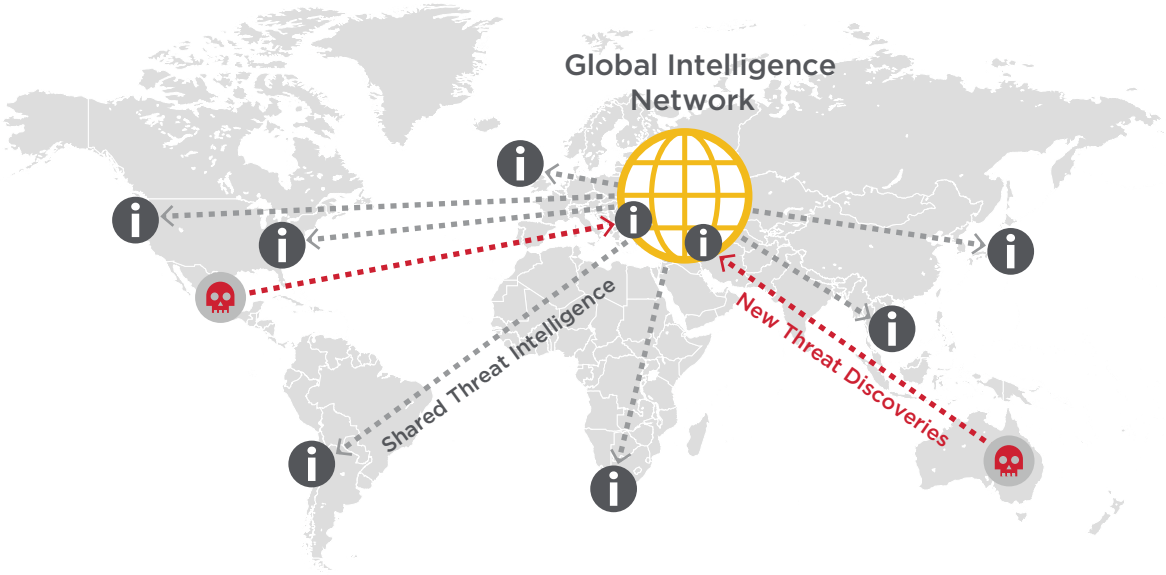
Proven and Effective Threat Protection

Behind every successful security product, there is great threat intelligence. That statement certainly rings true for Symantec Advanced Threat Defense solutions. Powered by expertise from Symantec researchers and over 200 threat analysis engines, the GIN processes more than one billion previously uncategorized new web requests and blocks over four million previously unseen or uncategorized threats every single day. Intelligence Services, powered by the GIN, 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.

Intelligence Services Subscription

Symantec Intelligence Services are offered on supported products via a subscription license. Consult the individual product data sheets or a Broadcom representative 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 as described in the Intelligence Services table on the next page.

Figure 2: GIN Threat Protection



Symantec Threat Explorer

Symantec Threat Explorer is an optional add-on subscription to augment Intelligence Services that provides access to an extensive research portal on URL reputation, risk scores, categorization, and classification data. Threat Explorer is a useful tool for Security Analysts and SOC teams.

Symantec WebPulse Automation Toolkit

Symantec Webpulse Automation Toolkit is an add-on optional subscription to Intelligence Services that provides access to an API to give administrators a way to automate URL lookups and requests for recategorization of URLs.

Data Feed	Description
Content Categories	*The Content Categories 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. For a full list of Content Categories visit Symantec Sitereview.*
Security Categories	*The Security Categories 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. For a full list of Security Categories visit Symantec Sitereview.*
URL Threat Risk Levels	*The Threat Risk Levels 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	*Geo Location 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.*
Data Feed: CloudSOC Audit Feed	*The Symantec CloudSOC data feed enables Intelligence Services to recognize over 45,000 cloud applications, enabling the proxy-based SWG to either allowed or deny access. More granular application access control can be provided by enabling full Symantec CloudSOC through separate licensing.*

Data Feed	Webfilter Comparison	Intelligence Services	Description
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 Controls	●	●	*Visibility and metadata for 180 web applications*

Note: Symantec Intelligence Services requires SGOS Version 6.6.3 or higher; customers should upgrade to SGOS version 7.3.XX or higher.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

SYM-Intelligence-Services-SB101 November 2, 2023