Symantec DeepSight™ DataFeeds

Real-time threat intelligence enables real-time security

Data Sheet: Security Intelligence

The Challenge

In today's enterprise, security threats are more dynamic and pervasive than ever. They are more sophisticated, and are doing more damage, increasingly with criminal intent. This, coupled with an increased ability to exploit vulnerabilities, is a growing worry for security professionals.

Traditional security solutions can only do so much; they can only attempt to identify and block threats as they attack the enterprise. By adding deep visibility into the global threat landscape, security policy can become more proactive.

For organizations trying to keep up with the threat landscape, trying to aggregate threat data from numerous sources, identifying which threats are relevant and then prioritizing mitigation actions is a full-time task. The time and effort spent on research also reduces the resources available for actually integrating this data into security systems and implementing solutions to enhance security.

Symantec DeepSight™ DataFeeds Overview

Symantec DeepSight™ DataFeeds provide actionable intelligence about malicious activity sources, emerging threats, and vulnerabilities. This intelligence can enable you to reduce your exposure to threats through automated integration with existing security solutions. This integration into existing processes and tools allows businesses to act appropriately and quickly, preventing security incidents before they happen. Proactively protecting systems from application vulnerabilities prior to exploits and vendors patches being released allows security operations staff to stay ahead of the curve.

DeepSight DataFeeds are derived from deep, proprietary analysis of billions of events from the Symantec™ Global Intelligence Network. The Global Intelligence Network provides global visibility into the threat landscape, including:

- More than 240,000 sensors monitoring networks in over 200 countries
- Over 133,000,000 Symantec products and services
- Visibility into all ports/protocols for threat analysis and collection
- More than 8 billion emails per day
- More than 1 billion web requests a day

DeepSight DataFeeds are delivered in an XML format to allow enterprise security teams to easily integrate this intelligence into their security applications and systems, enabling dynamic security policy refinement to protect against communication with a malicious source with no IT overhead required.

Many customers integrate DeepSight DataFeeds to harness Symantec's threat intelligence knowledge within their internal security programs and security intelligence dashboards. This enables customers to leverage a broad view of internet threats and apply this intelligence as a key element of identification and prevention within their internal environments.

Symantec Deepsight offers four datafeed options:

Symantec DeepSight™ Security Risk DataFeed

The Symantec DeepSight™ Security Risk DataFeed transports the intelligence garnered from the Global Intelligence Network directly to security and management systems offering real-time visibility into emerging threats, malicious code, and adware/spyware. This, combined with prevalence, risk, and urgency ratings as well as disinfection techniques and mitigation strategies, ensures that businesses can protect against both known and emerging threats in an accurate and timely manner.

Symantec DeepSight™ Security Content Automation Protocol (SCAP) Vulnerability DataFeed

By utilizing Symantec DeepSight™ Vulnerability DataFeeds, IT organizations receive automated, customized alerts for vulnerabilities and the associated security risks impacting nearly 105,000 technologies from more than 14,000 vendors. Based on company IT infrastructure and severity rating threshold, alerts can be customized to deliver those that carry the greatest urgency as defined by your own risk management strategy and threat posture.

Symantec DeepSight™ IP Reputation DataFeed

The Symantec DeepSight™ IP Reputation DataFeed provides up-to-date and actionable intelligence about malicious activity on the Internet, such as malware distribution and botnet command and control server communication. These datafeeds are derived from observed activity on the Internet.

Utilizing the Global Intelligence Network, IP address activity is analyzed to identify participation in the following:

- **Attacks**
- **Malware distribution**
- **Phishing scams**
- **Spam distribution**
- **Bots infections**
- **Botnet command and control server communication**

IP addresses and URLs are rated on a hostility score and/or confidence rating. A hostility score is calculated based on the frequency of activity and a confidence rating is assigned based on the number and types of sensors detecting the activity.

Each IP address is scored with one or more threat area, so that organizations can customize their alerts based on their individual needs and business concerns.

Symantec DeepSight™ Domain and URL Reputation DataFeed

The Symantec DeepSight™ Domain and URL Reputation DataFeed provides the same level of threat data as the DeepSight IP Reputation DataFeed, but focuses on domains and URLs, enabling the security team to define security policy for outbound traffic from internal source. The dynamic intelligence in both reuputation datafeeds can be used to prevent communication with compromised domains, preventing potential data loss, data theft, and blocking malware and Advanced Persistent Threat (APT) communication back to their command and control infrastructure.

Benefits

Unsurpassed accuracy and breadth of intelligence

Only Symantec has the breadth of visibility into real-world threat intelligence, combined with the expertise to analyze threat data to inform and protect our customers ahead of time.

Enable the transition from reactive to proactive security programs

Incorporating enhanced global threat and vulnerability visibility helps identify and block threats before they impact your network.

Improve IT security staff productivity

Delivered as an automated feed, there is no manual threat or vulnerability research required by IT, freeing up time that can be spent on additional tasks.

Adjust organization's response based on risk profile

The combination of threat, vulnerability, and reputation information allows businesses to customize which alerts to take action on based on their internal infrastructure and security posture.

System Requirements

Browser	Internet Explorer® 6 or higher, Firefox® 3.6.2 or higher, Safari® 4.0 or higher, Google Chrome™ 3.0 or higher
WebService	SOAP 1.1 or 1.2
DataFeed	XML version 1.0/Compression algorithm – zip – RFC 1950
SDK	Microsoft.NET framework 1.1 or higher

DeepSight DataFeeds licensing

All DataFeeds are licensed separately on a per datafeed basis for a 12, 24 or 36 month subscription.

Complementary Services

In addition to DeepSight DataFeeds, other services include:

- **Symantec DeepSight™ Early Warning Services**. Delivers global intelligence, analysis, and mitigation strategies for vulnerabilities and threats to critical infrastructure through a customizable alert service.
- **Symantec™ Managed Security Services.** Delivers 24x7 security monitoring and management services by expert security staff with a comprehensive "edge to endpoint" approach to provide broad visibilty of activity and potential threats across an enterprise's infrastructure.

More Information

Visit our website

http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

 21227149 02/12