Symantec™ DeepSight Early Warning Services

Real-time Intelligence on Threats and Vulnerabilities

Data Sheet: Security Intelligence

The Challenge

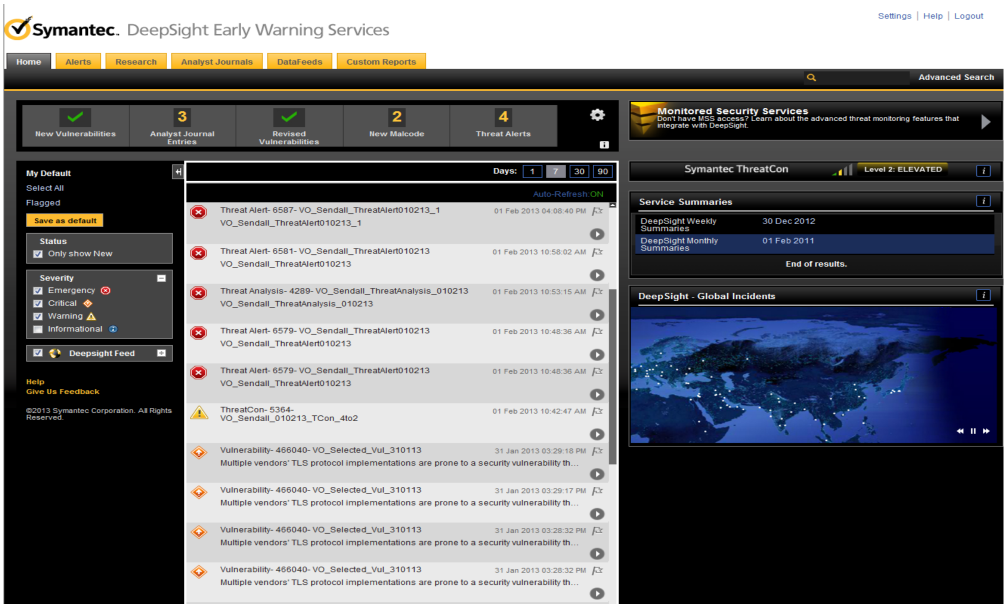
In today's enterprise, security threats are more dynamic and pervasive than ever. New threat vectors have emerged, such as hacktivists and nation-states, that are using malware to attack their victims, resulting in the threat landscape becoming more chaotic than ever before. Coupled with this, adversaries of all types and abilities have become more professional, with an accelerated ability to exploit vulnerabilities and launch sophisticated attacks through their ecosystems.

Traditional security solutions, although effective, are becoming more easily bypassed by attacks rapidly changing their appearance, and can only operate in a reactive mode once a known threat is detected. Adding visibility into the global threat landscape can provide and enable more proactive security policy to be implemented.

For organizations trying to keep pace with the threat landscape and trying to aggregate threat data from numerous sources, which might have unknown data quality, identifying which threats are relevant and then prioritizing mitigation actions is more than a full-time task. The time and effort spent on research and analysis also reduces the time available for utilizing this data to enhance security. Symantec, a leading provider of security intelligence services, offers an alternative to this costly approach through its DeepSight solutions.

Symantec™ DeepSight Early Warning Services Overview

Symantec™ DeepSight Early Warning Services provides organizations with timely, relevant threat and vulnerability exposure intelligence delivered through an intuitive web-based portal as well as through real-time alerts. Organizations can use this valuable global visibility and intelligence to help ensure that they adapt their security and risk profile to keep pace with the rapidly changing threat landscape.



☑ Only show New

☑ Emergency
☑ Critical
☑ Warning
☐ Informational

☑ Deepsight Feed

©2013 Symantec Corporation. All Rights Reserved.

Threat Alert- 6587- VO_Sendall_ThreatAlert010213_1 — 01 Feb 2013 04:08:40 PM
VO_Sendall_ThreatAlert010213_1

Threat Alert- 6581- VO_Sendall_ThreatAlert010213 — 01 Feb 2013 10:58:02 AM
VO_Sendall_ThreatAlert010213

Threat Analysis- 4289- VO_Sendall_ThreatAnalysis_010213 — 01 Feb 2013 10:53:15 AM
VO_Sendall_ThreatAnalysis_010213

Threat Alert- 6579- VO_Sendall_ThreatAlert010213 — 01 Feb 2013 10:48:36 AM
VO_Sendall_ThreatAlert010213

Threat Alert- 6579- VO_Sendall_ThreatAlert010213 — 01 Feb 2013 10:48:36 AM
VO_Sendall_ThreatAlert010213

ThreatCon- 5364- VO_Sendall_010213_TCon_4to2 — 01 Feb 2013 10:42:47 AM

Vulnerability- 466040- VO_Selected_Vul_310113 — 31 Jan 2013 03:29:18 PM
Multiple vendors' TLS protocol implementations are prone to a security vulnerability th...

Vulnerability- 466040- VO_Selected_Vul_310113 — 31 Jan 2013 03:29:17 PM
Multiple vendors' TLS protocol implementations are prone to a security vulnerability th...

Vulnerability- 466040- VO_Selected_Vul_310113 — 31 Jan 2013 03:28:32 PM
Multiple vendors' TLS protocol implementations are prone to a security vulnerability th...

Vulnerability- 466040- VO_Selected_Vul_310113 — 31 Jan 2013 03:28:32 PM
Multiple vendors' TLS protocol implementations are prone to a security vulnerability th...

Monitored Security Services
Don't have MSS access? Learn about the advanced threat monitoring features that integrate with DeepSight.

Symantec ThreatCon — Level 2: ELEVATED

Service Summaries

DeepSight Weekly Summaries	30 Dec 2012
DeepSight Monthly Summaries	01 Feb 2011

End of results.

DeepSight - Global Incidents

DeepSight Early Warning Services delivers security intelligence based on the deep, proprietary analysis of billions of events from the Symantec™ Global Intelligence Network (GIN). The Symantec GIN has global visibility into the threat landscape, including:

- More than 64.6 million attack sensors
- An extensive antifraud community of enterprises, security vendors, and more than 50 million consumers
- Visibility into all ports/protocols for threat analysis and collection
- More than 8 billion emails per day
- More than 1.4 billion web requests a day

IT organizations utilizing DeepSight Early Warning Services obtain direct visibility into malicious code, security risks and vulnerabilities covering over 40,000 products from more than 16,000 vendors in a single location. This greatly reduces the workload placed on IT security teams trying to stay ahead of the latest threats and vulnerabilities. Alerts can be customized by organizations based on industry, as well as internal IT infrastructure and security policy priorities, ensuring time is spent only on high priority events.

DeepSight Early Warning Services Features

DeepSight Early Warning Services portal offers insight into a wide range of real-time data designed to provide organizations with the information they need to proactively protect their infrastructure.

Truly global visibility

A customizable view into global threat data, including visibility into firewall, IDS and malware events, as well as detailed journals and analyst blogs can provide insight into threats and trends, often before they impact an organization.

In-depth threat analysis

Detailed analysis of emerging threats, vulnerabilities and malicious code, including targeted systems, symptoms, mitigation strategies and remediation steps enabling a rapid response to threat outbreaks.

Detailed research tools

Tools to simplify research related to security incidents including IP/URL reputation, malcode, port and suspicious file lookup.

Customized reporting

Reports can be scheduled and customized dependent on need, based on specific criteria relevant to your investigations, such as type of event, malcode, source/destination, target characteristics and ports.

Brand Protection

Organizations can be informed if use of their brand or IP address block is linked to any phishing or malicious code outbreaks.

DeepSight Early Warning Services are available at a number of different service levels; organizations can select the level that fits their needs and requirements.

Feature	Starter	Advanced	Silver	Gold	Platinum
Alerts:					
– Vulnerabilities	●	●	●	●	●
– Malicious Code	●	●	●	●	●
– Spyware & Adware	●	●	●	●	●
– Events & Threats		●	●	●	●
– Brand Protection		●	●	●	●
Search on Alerts	●	●	●	●	●
Event Notifications:					
– Email, RSS	●	●	●	●	●
– SMS	●	●	●	●	●
– XML				●	●
Extended Monitors (Port, Industry, Tech List)		●	●	●	●
Current & Historical Event Statistics		●	●	●	●
Analyst Journal		●	●	●	●
Unlimited Users			●	●	●
Content Redistribution			●	●	●
Tech List Sharing			●	●	●
Custom Reports				●	●
Remote Security Expert Service					●

Benefits

Unsurpassed accuracy and breadth of intelligence

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

Stay ahead of emerging threats and vulnerabilities

Access to the intelligence needed to stay ahead of new threats and emerging vulnerabilities through the intuitive Early Warning Services portal.

Reduce IT resources

A broad spectrum of intelligence from a single source, providing security professionals with the information they need to identify, block and mitigate new threats.

Adjust your organization’s response based on risk profile

The combination of customized threat and vulnerability information allows businesses to define alerts based on their individual IT infrastructure and security policies, enabling the adjustment of the security posture as needed.

Complementary Services

In addition to DeepSight Early Warning Services, other solutions include:

- **Symantec™ DeepSight DataFeeds** — Provide continuously updated intelligence that includes IP reputation, Domain/URL reputation, SCAP vulnerability information and security risk data. These datafeeds enhance security by enabling integration and automated response through existing security solutions such as SIEM, GRC and network security devices.
- **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 visibility of activity and potential threats across an enterprise’s infrastructure.

More Information

Visit our website

http://go.symantec.com/deepsight

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

Confidence in a connected world. Symantec.