

DeepSight™ Early Warning Services 8.0

The first line of defense for proactive enterprise security

Symantec™ Global Intelligence Network

Symantec has established some of the most comprehensive sources of Internet threat data in the world:

- 240,000 sensors monitor network attack activity in over 200 countries
- Malicious code data gathered from over 130 million systems
- Advanced honeypot network identifies new malicious code, zero day attacks, and new exploit vectors
- Over 2.5 million decoy mail accounts attract email messages globally, allowing Symantec to gauge worldwide spam and phishing activity

Keeping up with the rapid changes in today's threat landscape can be a daunting task. The increased volume and complexity of threats present significant challenges to organizations struggling to stay ahead of the risks posed by cyber crime. Protecting your Internet presence and brand name against malicious attacks continues to become more difficult.

In a recent survey, organizations identified that cyber risk and actual attacks have risen in the last two years. And that trend is expected to continue for the next two years. Actual losses, such as lost productivity and lost revenue, were felt by 98 percent of those surveyed. Exacerbating the problem, IT managers have found it increasingly difficult to provide effective IT security due to increased risk, increased regulatory pressures, lack of budget and the staffing challenge to find and retain qualified candidates.¹

So what is the answer? Access to a credible source for global intelligence, delivered through a customizable alerting service makes it possible for you to get the security intelligence you need to effectively do your job and protect your infrastructure efficiently.

Symantec DeepSight Early Warning Services

Symantec DeepSight Early Warning Services enable organizations to enhance security and take proactive control of the integrity of their information. DeepSight helps customers align risk profiles with the shifting threat landscape by delivering tailored information, analysis, mitigation strategies and recommended best practices for known and emerging threats and vulnerabilities.

DeepSight maintains comprehensive databases of vulnerabilities, malicious code, security risks, exposures, malicious IP addresses and other relevant information. Correlation engines map targeted ports to events, and continuously examine data streams from IDS and firewall sensors, antivirus submissions, and previously unidentified activity from proprietary honeypots. The statistical analysis engine flags unusual and potentially threatening activity. Symantec analyst teams use this information to develop alerts, analysis and remediation recommendations.

With personalized notification triggers and expert analysis, DeepSight enables organizations to prioritize IT resources, protect critical information assets against potential attacks, mitigate threats and remove security risks.

Key Benefits

- **Reliability of Intelligence.** The DeepSight alerts, analyses and reports have been thoroughly researched and prioritized by analysts with decades of practical hands-on security expertise.

1. *Managed Security in the Enterprise (U.S. Enterprise) March 2009*

DeepSight™ Early Warning Services 8.0

Symantec Global Intelligence Network, continued

- Process over 8 billion email messages daily
- Process over 1 billion web requests daily
- 4 Symantec Global Security Operations Centers
- 11 Symantec Security Response Centers
- 29 Symantec Global Support Centers
- More than 40,000 devices under management

- **Timely intelligence.** Detailed notifications provide timely intelligence on threats, vulnerabilities and security risks aggregated from thousands of exclusive sources and attack sensors worldwide. Detailed analysis of potential threats, actionable recommendations for mitigation and an easy to understand rating scale enables customers to make more informed decisions and respond quicker.
- **Prioritized incident response.** Enables efficient prioritization, allocation, and deployment of security staff by providing detailed threat mitigation strategies and customizable delivery options. Allows users to configure automated notifications based on the requirements of their unique IT infrastructure.
- **Comprehensive vulnerability intelligence.** Symantec maintains one of the world's most comprehensive vulnerability databases, consisting of more than 32,000 vulnerabilities. Vulnerability alerts on more than 72,000 technologies from more than 11,000 vendors provide actionable intelligence covering the complete threat lifecycle, from initial vulnerability identification to active attack.
- **Ability to demonstrate compliance.** The custom reports option provides powerful data mining, tracking, and reporting capabilities—including customization for specific source IP addresses or target ports. This can provide critical support for regulatory and auditing mandates, helping organizations meet compliance requirements and avoid potential penalties.
- **Saves Time and Money.** Symantec DeepSight analysts monitor potential threats across more than 18,000 distinct product versions. Detailed information based on specific enterprise platform configurations can be integrated into security operations. By eliminating hours spent searching Web sites and emails to gather security intelligence, DeepSight enables a proactive approach to security while saving time and money.

Key Features

- **Customized Technology Lists.** Technology Lists allow you to filter the malicious code and security risk databases based on specific products in your infrastructure.
- **Alerts.** Configurable monitors dispatch alerts whenever a newly released report type matches the criteria established within the corresponding monitor type. This includes vulnerabilities, malicious code, security risks, events, ports, industry and tech list activity.
- **Network infection.** DeepSight customers can be alerted when malicious activity has been recognized as originating from within their network. Customers can elect either High Priority Intelligence (tracking data sources considered high priority that should be acted upon with urgency using the mitigation strategies recommended in the alert) or Full Spectrum Intelligence for more extensive tracking against all available sources.
- **Brand protection.** DeepSight customers can be alerted when their brand is being adversely affected. Customers can monitor their domain and be alerted should it appear in the Symantec Phish Report Network as a targeted domain. Multiple domains can be entered, and inclusion of sub-domains is as easy as a checkbox within the interface.

DeepSight™ Early Warning Services 8.0

Symantec Security Intelligence Services*Symantec DeepSight DataFeeds*

Symantec DeepSight DataFeeds provides automated security intelligence data by enabling customers to integrate the DeepSight Vulnerabilities and Security Risks datafeeds with customer applications. This results in the ability to respond effectively to threats, address regulatory compliance requirements, and lower costs.

- **ThreatCon.** ThreatCon is a measurement of the global threat exposure, using a scale of 1 (low) to 4 (extreme) to rate conditions in the wild during the last 24 hour. The rating suggests an appropriate security posture based on network conditions.
- **Analysts Watch.** The Analyst Watch lists the ports being monitored over a 48 hour period. Sensors track activity for the number of events observed, origination IP address and cumulative IP addresses.
- **DeepSight Honeynet.** This is an extensive virtual network of systems designed to attract security risks, and provides a new data stream for tracking and analysis of threats in the wild. Users have access to analyst reports, honeynet statistics, journaling, compromised profile reporting and IP/URL address intelligence lists in XML format that provide insight of potential offenders.
- **Top Five Antivirus Threats.** Presents the top five threats in the previous 48 hours, providing a good indicator of malicious code propagation.

DeepSight Early Warning System Offerings

Symantec DeepSight Early Warning Services are offered in through a variety of packaging options that deliver the level of global security intelligence need to support an individual organization's risk mitigation profile.

DeepSight Starter Pack. This level of service provides customized alerting for vulnerabilities, malicious code and security risks, based on technologies within the organization's infrastructure. Delivery options include RSS or email based on user preference. Monitors can be configured for vulnerabilities, malicious code, security risks and domains.

DeepSight Silver. This level of service includes all of the capabilities of Starter Pack, plus:

- Configuration for extended monitor options (event, port, industry and tech list activity)
- Reports - daily/weekly/monthly reports, threat analysis and research reports
- Network infection alerting
- Brand protection
- Distribution of alerts using SMS
- Extended analysis for vulnerabilities, threat alerts, malicious code, research reports, summary reports, threat analysis, security risks and honeynet analysis
- Statistics – Analyst Watch of IDS, Firewall, antivirus, honeynet activities
- Analyst Journal
- Honeynet (compromise profiles, analysis, intelligence lists, analyst resources)

DeepSight Gold. This level of service includes all of the capabilities of Silver, plus:

- Distribution of alerts using XML
- Email integration of alerts
- Custom reports

DeepSight™ Early Warning Services 8.0

Symantec Security Intelligence Services

Symantec Cyber Threat Analysis Program

The Symantec Cyber Threat Analysis Program (CTAP) mitigates cyber risk with a comprehensive approach to threat identification, intelligence gathering and validation, and response to protect critical client information. The result is a highly customized solution that integrates multiple components to address the specific security requirements of customers.

- Content redistribution (within the company)

DeepSight Platinum. This level of service includes all of the capabilities of Gold, plus:

- Remote Expert Analyst Service. Direct access to a Symantec security analyst by phone or e-mail via the DeepSight portal to inquire about a specific report or customer issue.

About Symantec Global Services

Symantec Global Services offers tailored solutions that provide our customers with the expertise, product knowledge and process discipline to help them maximize their return on investment in Symantec products.

- Symantec Enterprise Consulting Services include: Advisory, Enablement, and Operational services for specific product and solution areas.
- Enterprise Support Services: include support and maintenance services for keeping Symantec products fully functional, up to date, and delivering maximum value.
- Education Services: include a comprehensive set of course offerings covering Symantec technical training and industry best practices, plus a full suite of learning services.
- Managed and Security Intelligence Services: 24x7 remote monitoring, management, reporting, and analysis delivered under strict service level agreements.

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.

Symantec World Headquarters

20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2009 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

09/09 20074679-1