



Symantec DeepSight™ Alert Services

Helping to proactively protect business through the timely delivery of actionable security information

With the increase in vulnerability discoveries, the fast spreading of blended threats, and the diversity of attack methods, having timely and credible security information is becoming critical for network and security management. Up-to-date, reliable security threat intelligence is the key to maintaining normal, secure business operations.

By delivering comprehensive and personalized notifications on the latest threats, Symantec DeepSight Alert Services enables organizations to proactively protect enterprise assets.

➤ **Timely and comprehensive information on new threats**

In 2003, an average of 51 new vulnerabilities were found every week, making it a time-consuming task to evaluate details to assess the urgency and analyze the impact. Symantec DeepSight Alert Services provides organizations with a view of their security risks that include vulnerabilities and malicious codes, in-depth technical analysis of new threats, recommendation on how to avoid breaches, and the confidence to prioritize and deploy resources on the most significant issues.

Symantec analysts review new vulnerabilities and research and monitor their exploits constantly. Currently Alert Services monitors 18,000 distinct technologies, operating systems, and application software product versions of 4,200 products from 2,200 vendors, by tracking information from over 150 authoritative sources. All the analysis and alerts are stored in the industry's leading vulnerability database where users can conduct queries by severity and impact rating for malicious codes and vulnerabilities.

DeepSight Alert Services saves time and money by eliminating the need to dedicate valuable staff resources to search for and evaluate the latest vulnerability and exploit information from multiple sources.

➤ **Actionable mitigation strategies and analysis**

The Symantec analysts research each vulnerability and provide the latest analysis regarding the potential threat and best-practices steps to keep systems protected.

For security professionals to make quick decisions for action, an analysis of every vulnerability and malicious code is provided along with:

- The severity of the vulnerability or malicious code, as well as its technical description
- The systems and specific versions that might be affected
- Impact and symptoms of the attack
- Mitigation strategies, including workarounds and available patches

The option to export alert contents via XML or to an internal Remedy® Help Desk format enables the integration of security risk management with IT service management. Personalized risk ratings of any threat, to any environment, can initiate and track remediation actions in security operation processes, including helpdesk solutions.

KEY POINTS

- Monitors vulnerabilities in more than 18,000 technologies, from 2,200 vendors and automatically delivers timely security notifications worldwide
- Optional XML output for integration into IT security processes and remediation solutions, such as help desk, enables tracking of actions by the security and IT team
- Alert status tracking streamlines task assignment and reporting by providing status and documenting resolutions
- Provides analysis and guidance on how to mitigate risks by using technologies such as IDS or firewall even before virus definition files are available
- Easily set up personalization enables security resources to receive only alerts relevant to their enterprise environment and their specific areas of responsibility
- Offers an industry leading range of delivery options, including email, voice, fax, and SMS
- Enables secure, Web-based queries to an industry-leading vulnerability database, and provides detailed patch and release information
- Prioritized alerts enable security and IT professionals to efficiently allocate time and resources based on the most pressing security issues
- Administrative user status gives control over subordinate users in order to share information, collaborate for early mitigation, and increase accountability

➤ **Enhanced administration capability**

Centralized administration helps mitigate risk at the earliest opportunity. Because all security resources can be centrally defined, controlled, monitored, and tracked the best synchronization between business strategy and risk reduction is possible. Central administration for alert status consolidation, coupled with detailed historical alert information, means that administrators can analyze and generate reports on successes and failures in the security process. It can be used to control alerts sent to third party processes enabling coordinated control over a wide-range of technologies.

➤ **Personalized for any environment**

Unlike other alert services which send all notifications to every user, Symantec DeepSight Alert Services can be configured so that the notification is filtered to administrators or users based on the exact system and network configuration of a given enterprise environment. For example, by personalizing technology lists and the risk factor monitor, alerts can be tailored by technology skill-set, geographical location, management hierarchy, and line-of-business responsibility. With alerts filtered to the appropriate personnel, the risk can be analyzed, decisions can be made, and security risk areas can be fixed before they can be exploited.

➤ **Symantec Early Warning Solutions – a proactive approach to security**

By providing notification of new potential threats as they're identified, with detailed, actionable information, Symantec DeepSight Alert Services helps organizations mitigate vulnerabilities before they can be exploited, and helps protect systems from malicious code before it strikes. For real-time proactive notification of potential attacks, Symantec DeepSight Threat Management System tracks global security events, providing early warning of active threats as they develop. Symantec DeepSight Threat Management System enables administrators to better prioritize and act upon information with a more detailed understanding of enterprise risk.

➤ **Symantec™ Enterprise Services**

Symantec Early Warning Solutions are part of a range of services from Symantec that provide security expertise, resources, and processes to effectively monitor, manage, and provide intelligence on security systems, as well as consulting and education services.

➤ **Backed by Symantec™ Security Response**

For even more security intelligence and timely, around-the-clock protection, Symantec DeepSight Alert Services is supported by Symantec Security Response, the world's leading Internet security research and support organization. At Symantec Security Response, a world-class team of experts works to identify and neutralize complex threats. Symantec Security Response provides swift, global responses to security events 24x7 and proactive research on future threats.

SYMANTEC ENTERPRISE SECURITY SERVICES ARE KEY COMPONENTS OF SYMANTEC ENTERPRISE SECURITY. SYMANTEC ENTERPRISE SECURITY COMBINES WORLD-CLASS TECHNOLOGIES, COMPREHENSIVE SERVICES, AND GLOBAL EMERGENCY RESPONSE TEAMS TO HELP BUSINESSES RUN SECURELY AND WITH CONFIDENCE.

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408 517 8000
800 721 3934

www.symantec.com

**For Product Information
In the U.S., call toll-free
800 745 6054**

**Symantec has worldwide
operations in 35 countries.
For specific country
offices and contact numbers
please visit our Web site.**