Symantec™ DeepSight™ Threat Management System

Helping to protect networks from active threats with an industry-leading Web-based early warning security system

In today’s networked environments, security technology alone is not sufficient to protect enterprise resources from constantly emerging vulnerabilities and threats. People, processes, intelligence, and technology must all work together to ensure a strong security posture. As an element of effective enterprise security preparedness, Symantec DeepSight Threat Management System enhances security by delivering proactive early notification of active attacks, potential threats and significant new vulnerabilities, enabling administrators to more accurately predict and quantify risk. With personalized warning alerts complemented by expert threat analysis, actionable assessments, and decision support, it is an industry-leading early warning system for global attacks.

- **Closes the gap between security awareness and action**
The Symantec DeepSight Threat Management System continuously aggregates and correlates attack data from the security systems of over 20,000 partners, plus other public and confidential sources, in over 180 countries around the world. Symantec human intelligence resources leverage their many industry relationships to keep track of the latest attack techniques. The experts at Symantec analyze the threat information to identify active attacks and deliver comprehensive analyses based on the specific network configuration of any given enterprise environment.

- **Up-to-the-minute intelligence enables attack prevention**
By delivering advanced warning of attacks before they can impact the enterprise, the system enables administrators to take proactive steps to protect their infrastructure and prevent network downtime, lost productivity, or damage to the company’s reputation. The system provides statistically reliable and highly detailed attack information, with the ability to track data by time, country, industry, and other parameters via automated, prioritized alerts, and through the Web. Patches, countermeasures, workarounds, and additional reference sources are also provided, enabling timely action.

- **Early warning protection optimizes security resources**
Leveraging proactive intelligence and response, companies can deploy specific countermeasures to help prevent threats from impacting their networks. By eliminating the hours spent searching through hundreds of Web sites and emails to gather information, the system maximizes IT resources while keeping operations running smoothly. At its core is the Symantec Event Database, which aggregates and correlates partner intrusion detection system (IDS) and firewall data, along with antivirus data from the Symantec Digital Immune System. Firewall data extends early warning capabilities by collecting data on new, unknown threats, while IDS data provides detailed attack information and antivirus data provides a measure of outbreak severity, enabling a global view of attack information throughout the system. Through a secure, Web-based console, the system provides personalized threat analyses, including alerts, reports, and triggers. The alerts are delivered directly to the administrator responsible for specific technologies via email, fax, SMS or voice.

**KEY POINTS**
- Detailed alerts provide timely intelligence on security incidents aggregated from thousands of exclusive sources and attack sensors worldwide
- Actionable intelligence enables more efficient prioritization, allocation and deployment of security staff and resources
- Customization enables administrators to receive automated alerts to reflect the requirements of their unique IT infrastructure
- The Custom Reports Add-on provides powerful data mining and reporting to deliver information on both specific attacks and trends, using criteria ranging from time period to industry type to attack specifics
- Backed by Symantec™ Security Response, the world’s leading Internet security research and support organization

Symantec DeepSight Threat Management System Architecture
Symantec DEEPSIGHT THREAT MANAGEMENT SYSTEM

> **Configurable alerts**
Malicious code and threat alerts are sent out within an hour of discovering any abnormal activity or hostile behavior. The alerts contain detailed technical explanations, as well as workarounds or patches. Alerts can quickly be personalized for specific configurations of networks, systems, and software in any enterprise environment. Plus, triggers can be set to react to spikes in activity on a technology, port, industry, or type of attack, and automatically generate alerts and reports upon seeing increased attacks.

> **Comprehensive analyst reports**
Threat analysis reports provide detailed explanations of attacks, their origin, spread, mitigating factors, and prevention. With invaluable intelligence for both security professionals and executive management, daily, weekly, and monthly summaries describe attacks, vulnerabilities, and trends over the reporting period.

> **Internet at a glance**
For a live summary on the state of the Internet, the Symantec DeepSight Threat Management System continuously generates a quick-view page for IDS, firewall and antivirus events. On one page, administrators can get detailed information on a variety of active enterprise attacks, including spikes, countries, ISPs, IP addresses, ports, products, and more. In addition, the Symantec Analyst Watch page provides the viewer with potential hot-spots that our analysts identify as most critical.

> **Custom Reports Add-on**
With the reporting module, which provides more than twenty different reports, administrators can conduct detailed analysis of global Internet activity. Customization options enable organizations to apply their own criteria, including industry, country and company size, as well as attack specifics, and templates allow custom reports to run automatically.

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

> **Backed by Symantec Security Response**
For even more security intelligence and timely, around-the-clock protection, Symantec DeepSight Threat Management System is supported by Symantec Security Response, the world’s leading Internet security research and support organization. Symantec Security Response provides swift, global responses to security events and proactive research on future threats. For more information visit http://enterprisesecurity.symantec.com.

EARLY WARNING SOLUTIONS 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.