Symantec™ Monitored and Managed IDS/IPS Services

Comprehensive security monitoring, management, and analysis to protect against intrusions

Reduce Security Risk

Today’s enterprise data networks enhance corporate communications and ensure business growth. However, these same networks are also vulnerable to attacks by hackers who constantly seek ways to compromise and exploit data and computing assets. Symantec™ Monitored and Managed Intrusion Detection and Prevention System (IDS/IPS) Services offer real-time protection from attack and enable companies to reduce their overall security risk. Symantec’s Security Operations Center technology platform combines real-time security alerts from a customer’s network with global intelligence information about security threat activity to support fast and accurate analysis of customer security data. This system enables Symantec security analysts to quickly identify activity from known and emerging security threats, notify customers, and provide recommendations for defense and protection before damage occurs.

Key Features

- NEW! Symantec™ Monitored and Managed IDS/IPS Services includes Vulnerability Data Correlation at no additional cost that enables organizations to:
  - Proactively manage and prevent the spread of security incidents by correlating attack data from IDS/IPS devices with vulnerability data
  - Meet regulatory control requirements by ensuring timely actions are taken to manage security risks
  - Increase staff productivity and operational efficiency by responding only to validated attacks
  - Minimize business impact and reduce overall risk from known emerging attacks
  - Tiered service levels allow businesses to build a managed security program to fit their individual risk management profile
  - Enhancements to the Secure Internet Interface allow customers to better view the impact of their security, emerging threats, and snapshots of security threats and posture
  - Provides support for major intrusion detection and intrusion prevention technologies from multiple security vendors
  - Offers organizations a real-time view of their enterprise security posture to help maintain security policy compliance
  - Enhances an organization’s information security posture through continuous monitoring and management, expert analysis of log data, and immediate response to potential security threats
  - Delivers 24x7, real-time monitoring and management of intrusion detection and intrusion prevention systems across the globe
  - Uses a state-of-the-art technology platform to aggregate and analyze data from heterogeneous security devices to quickly identify and defend against threats
Symantec Monitored and Managed IDS/IPS Services
Monitored network-based and host-based intrusion detection and intrusion prevention services:

• THE ADVANTAGES OF SYMANTEC REAL-TIME SECURITY MONITORING. Customers are provided with constant security monitoring, intelligence, and analysis of their intrusion detection technology while maintaining internal control over configuration and performance management of IDS/IPS and IDS/IPS management consoles.

Monitored and managed network-based intrusion detection and intrusion protection service:

• GAIN REAL-TIME SECURITY AND MAINTAIN CONTROL. Customers enjoy the advantages of constant security monitoring, analysis, and global intelligence in addition to configuration, performance, and fault management of IDS/IPS management consoles and IDS/IPS Sensors.
IPS services' customers have the flexibility to customize prevention baselines for each device when implementing IPS “blocking” policies. (Depending upon the service level purchased )

A Continuum of Service Offerings
Symantec Managed Security Services offers multiple tiers of service, allowing customers to choose the appropriate level of protection based on risk management and organizational need. These packages combine real-time security monitoring and continuous professional security analysis of IDS/IPS alerts with comprehensive management and monitoring of network – and host-based IDS and IPS.

• COMPLETE ANALYSIS OF SECURITY THREATS enables Symantec security experts to provide timely and insightful alerts and specific recommendations, to quickly and effectively improve each customer's security posture.

• DETECTION AND PROACTIVE RESPONSE to the most sophisticated hacker attacks.

• REAL-TIME SECURITY MONITORING and 24x7 expert security analysis of intrusion alerts.

• CORRELATION WITH VULNERABILITY DATA from supported scanning devices.

• COMPREHENSIVE MANAGEMENT SERVICES include complete remote configuration, rule changes, signature updates, system and software support, fault analysis, and performance management.
**Symantec Security Operations Center**

**Technology Platform**

The Symantec Security Operations Center (SOC) Technology Platform features advanced data mining and security event correlation capabilities that enable Symantec experts to actively monitor security devices in real-time.

- **SEPARATE ACTUAL THREATS FROM FALSE POSITIVES.**
  The SOC technology platform allows Symantec security experts to reliably separate actual security threats from false positives and deliverable actionable information, with reliable results. This process drastically reduces the amount of data a customer must consider to stay updated on the state of their security.

- **CONTROL THE SPREAD OF MALICIOUS ACTIVITY.**
  By correlating attack data generated by IDS/IPS devices with customer vulnerability data, Managed Security Services analysts can identify a compromised host, and then highlight other hosts with the same vulnerability that may not yet be compromised. This allows customers to take proactive steps to stop the spread of malicious activity to other vulnerable parts of the network.

- **ACCESS COMPREHENSIVE SECURITY INFORMATION.**
  Through the Secure Internet Interface Web portal, clients have access to comprehensive information from a wide variety of sources available to Symantec. This data is analyzed and presented in a way that makes the current security state of an enterprise understandable while allowing clients to maintain ultimate control of their security infrastructure.

- **GLOBAL EMERGING THREAT NOTIFICATION.**
  Monitoring thousands of devices on behalf of hundreds of customers and thousands of users in 69 countries around the world, Symantec Managed Security Services has unique insight into the emergence of security threats. Armed with emerging threat intelligence, Symantec provides proactive notification to customers regarding high-risk security events, such as worms and blended threats. The multi-source data that Symantec analyzes provides customers with a unique security perspective that no other managed security service provider can offer.

**Backed by Symantec—the leader in Internet security**

The breadth and depth of Symantec expertise enables customers to improve the security of their enterprise. In addition to global support from multiple SOCs that meet stringent industry certification and auditing best practice guidelines and standards, Symantec Managed Security Services is supported by Symantec™ Security Response, the world’s leading Internet security research and support organization. This team, in turn, leverages the data provided by the Symantec DeepSight™ Early Warning services, which provides notification of vulnerabilities and exploits as they are identified.
More information

Visit our Web site

www.symantec.com

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

Call toll-free 800 745 6054.

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

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

About Symantec

Symantec is the global leader in information security, providing a broad range of software, appliances, and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure. Symantec’s Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions. Headquartered in Cupertino, California, Symantec has operations in 35 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
408 517 8000
800 721 3934
www.symantec.com