Symantec™ Monitored and Managed IDS 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 System (IDS) 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.

Symantec Monitored and Managed IDS Services

MONITORED NETWORK-BASED AND HOST-BASED INTRUSION DETECTION 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 and IDS management consoles.

MONITORED AND MANAGED NETWORK-BASED INTRUSION DETECTION 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 management consoles and IDS Sensors.

A Continuum of Service Offerings

Symantec Managed Security Services now 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 alerts with comprehensive management and monitoring of network- and host-based IDSs.

- COMPLETE ANALYSIS OF SECURITY THREATS enables Symantec security experts to provide timely and insightful alerts and specific recommendations, to quickly and effectively improve customers’ security postures.
- DETECTION AND PROACTIVE RESPONSE to the most sophisticated hacker attacks.
- REAL-TIME SECURITY MONITORING and 24x7 expert security analysis of intrusion alerts.
- COMPREHENSIVE MANAGEMENT SERVICES include complete remote configuration, rule changes, signature updates, system and software support, fault analysis, and performance management.

KEY POINTS

- NEW! Tiered service levels allow businesses to build a managed security program to fit their individual risk management profile
- NEW! 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
- Helps minimize business impact and reduce overall security risk from known and emerging attacks
- Provides support for major intrusion detection 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 systems
- Provides rapid, cost-effective resolution of security problems from Security Operations Centers (SOCs) around the world
- 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 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 separate actual security threats from false positives, with reliable results. This process drastically reduces the amount of data a customer must consider to stay updated on the state of their security.

- **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 40 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’s 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.

**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.