Maximizing the Value of an Intrusion Protection Investment

INSIDE

▷ Network Intrusion Protection Systems and Technologies
▷ Value-add Managed Security Services
▷ Symantec ManHunt™ Network Intrusion Protection System
## Contents

- Executive Summary .......................................................... 3
- Introduction ........................................................................... 4
- Network Intrusion Protection Systems and Technologies .............. 5
  - Network-based intrusion protection technologies .................. 5
  - Signature-Based Detection .............................................. 5
  - Behavioral Anomaly Detection ......................................... 6
  - Protocol Anomaly Detection ............................................ 6
- Value-add Managed Security Services ....................................... 6
  - Security Monitoring ....................................................... 6
    - Data collection and normalization .................................. 7
    - Data mining ............................................................. 7
    - Automated security event correlation ............................. 7
    - Expert response to events ......................................... 7
    - Event reporting ...................................................... 7
  - Security Management ..................................................... 7
    - Fault management .................................................... 7
    - Configuration management ...................................... 8
    - Performance management ....................................... 8
    - Signature Maintenance ............................................ 8
- Symantec ManHunt™ Network Intrusion Protection System ........... 8
  - Complemented by Symantec Managed Security Services .......... 9
  - Monitored Services ...................................................... 10
  - Managed Services ....................................................... 11
  - Symantec Security Technology Platform ........................... 11
- Competitive Advantages of Partnering with Symantec .................. 12
Executive Summary

Organizations of all types are using the speed and flexibility of the Internet to drive their business strategies fast and far in terms of time-to-market and geographical reach. Public-facing Web sites, collaborative e-business applications, and advanced networking technology enhance business opportunities and help organizations link their customers, partners, and remote users. They also create new opportunities for potential intruders and malicious attacks.

Many organizations gain a basic level of security by deploying firewalls on the network perimeter and throughout the infrastructure. However, they are still vulnerable to attacks due to misconfigured products, interoperability problems, or incomplete analysis of the significant amount of data generated by these security and access control devices. While firewalls provide the first line of defense, they alone cannot prevent blended threats from penetrating the network. Blended threats (such as the Blaster worm) propagate through multiple points of attack, further complicating the challenges that organizations face in safeguarding networked assets. Intrusion protection systems add a layer of defense to help organizations detect internal attacks such as misuse of systems, as well as external attacks that have bypassed the firewall. But many of today's organizations lack sufficient staff and expertise to maintain and manage the variety of security products they have implemented from various vendors, never mind adding intrusion protection systems.

This paper presents an overview of network-based intrusion protection, including how it works, and the benefits of such a solution. It then articulates how, by partnering with a managed security service provider, organizations gain advanced network intrusion protection device and data management, monitoring, and analysis capabilities. These services help mitigate risk, control security costs, and provide a greater level of protection for business operations and data.

Next, the paper presents Symantec ManHunt™, a network-based intrusion protection solution that detects internal and external intrusion attempts and enables real-time response to attacks and threats. The paper also includes a description of the service offerings provided by Symantec Managed Security Services, which complement Symantec ManHunt and third-party security products. The conclusion summarizes the security benefits, cost savings, and competitive advantages of purchasing a combined product and service offering for advanced intrusion protection.
Introduction

Organizations increasingly rely on the Internet to conduct business, using data networks to support internal and external communication, transactions, and work processes. These networks link customers, partners, and remote users for greater speed and efficiency, and as a result, have become increasingly open in nature. With this higher level of accessibility comes greater information security risk.

Organizations of all sizes have implemented standalone security products such as firewalls and virus protection. Firewalls can be considered network gatekeepers, but most do not inspect the contents of all traffic packets they pass through to the network. As a result, blended threats, such as Blaster, Nimda and Code Red, can enter through the standard ports on a firewall at the network perimeter. Organizations recognize the added need for intrusion protection technology to inspect the contents of these packets.

Intrusion protection systems enhance the enterprise’s security profile and complement firewall technology by providing an added layer of security to detect, manage, and prevent malicious attacks. But many organizations are already constrained in their ability to adequately implement and maintain network security due to limited in-house resources and technical expertise. These same organizations are often hesitant to expand security infrastructure due to the costs associated with the training and staffing requirements. Yet the continued increase in the number and severity of attacks (worldwide attack activity rose 19% in the first half of 2003, compared to the same period in 2002)* heightens the need for expertise, vigilance, and rapid response to new threats in organizations of all sizes.

As an alternative to the cost and resource commitment required to implement and maintain advanced security systems in-house, managed security service providers (MSSPs) offer solutions for effective security monitoring and management that combine best-of-breed technology, security best practices and expertise. Enlisting the right service provider to manage network intrusion protection activities enables organizations of all sizes with resource-constrained IT departments to gain greater network protection and advanced security capabilities at a cost and level of service that matches their business needs.
Network Intrusion Protection Systems and Technologies

Intrusion protection solutions move beyond just detecting and preventing intrusions to managing attacks and providing security administrators with more time to respond and deploy mechanisms to prevent further occurrences.

NETWORK-BASED INTRUSION PROTECTION TECHNOLOGIES

Intrusion protection sensors are most effective at detecting intrusions when deployed on the network perimeter, such as on both sides of the firewall, near dial-up servers, and on links to partner networks. These sensors, known as network-based intrusion protection systems, detect attacks that firewalls are unable to see, can identify attacks as they occur, and protect against denial-of-service attacks and spoofing.

Network-based intrusion protection sensors are deployed as software installed on a dedicated, general purpose server, or are pre-loaded on a specialized network appliance, and then attached directly to a network segment. A network-based intrusion protection solution uses network cards in promiscuous mode to look at every packet that passes on the network. A typical network intrusion protection solution consists of one or more sensors and a console to aggregate and analyze data from the sensors. In pass-by mode, the sensor copies each packet and analyzes the copy for attack patterns by comparing it to attack signatures.

With sensors inside and outside the firewall, network-based systems use a number of different technologies to detect malicious activity and attacks. The three most widely used methods are signature detection, behavioral anomaly detection, and protocol anomaly detection. Organizations gain the greatest level of security from network-based intrusion protection systems that use an array of detection methodologies to effectively and accurately detect sophisticated attacks as they emerge.

Signature-Based Detection

This method of detection, on which most traditional network IDS systems are based, examines network traffic to identify specific patterns of attack. The security administrator codes a signature for every exploit and maintains a database of signatures to identify known threats. The effectiveness of this method of intrusion detection is based on the system’s ability to compare every packet of network traffic to every signature in the database. As network speeds increase, the resources that the intrusion detection sensor leverages to examine every packet decrease, causing some packets to be discarded and potentially leaving systems vulnerable to attack. In addition, attacks cannot be identified by signature-based systems until the signature is added to the database. As a result, the time required for administrators to identify a threat, create a signature, and release a security update creates another window of opportunity for malicious attacks.
Behavioral Anomaly Detection

Detecting statistical anomalies is a less widely used method of intrusion detection. This process continually tracks patterns of behavior to create a baseline of system statistics. Changes in these patterns are monitored to detect malicious activity. Examples of statistical anomalies include excessive use, use at unusual hours, and changes in system calls made by user processes. Security administrators can detect anomalies without having to understand their underlying cause. However, even legitimate use of the system can trigger anomalies, resulting in a high number of false positives.

Protocol Anomaly Detection

This method of detection focuses on the structure and content of communications. Protocol-based intrusion detection systems model the access rules of common application protocols directly in the intrusion protection sensor. The sensor identifies network traffic that contains unexpected data or invalid characters, or that uses an unusual request to post and execute malicious code on the victim server. While this type of attack bypasses signature-based detection, protocol anomaly detection easily recognizes it as a violation and alerts security administrators. The benefit is that protocol anomaly detection will spot a new type of attack – often called “zero-day” attacks – for which no signatures yet exist. Administrators then have hours, and in some cases days, to respond to the threat, develop a signature, and distribute a security update before the hacker can cause damage.

Value-add Managed Security Services

To successfully implement and maintain intrusion protection solutions, many organizations are turning to managed security services providers (MSSPs). Partnering with the right MSSP helps organizations gain access to advanced technology, experienced security personnel, continuous threat intelligence, and network-wide monitoring and management on a 24x7 basis. In order to provide effective and complete managed security services, an MSSP must offer advanced security monitoring capabilities, up-to-the-minute security threat intelligence, security device management. In addition, an MSSP must operate its services from a Security Operation Center (SOC). SOCs should be staffed with certified security specialists with knowledge that spans a broad range of security products from a variety of vendors. SOCs enable security analysts to monitor security devices in real time, reliably identify threats and suspicious activity, and rapidly respond to attacks.

Security Monitoring

Security monitoring refers to the analysis of security device data to detect and respond to signs of malicious activity. Many service providers that claim to offer security monitoring are, in fact, only reviewing the security devices to ensure that they are operational. In contrast to security device management, effective monitoring requires the use of a highly complex technical architecture that enables the service provider to analyze significant volumes of data generated by security devices distributed throughout the organization’s network. Despite frequent claims, few managed security service providers are adequately prepared to provide comprehensive security monitoring with the following capabilities:
**Data collection and normalization**

This process involves transforming security device data, such as firewall logs and intrusion alerts, into a consistent format so that a standard set of queries can be used to mine data and isolate signs of malicious activity.

**Data mining**

Data mining employs an automated system that continuously queries security data to detect signs of malicious activity and separate suspicious network traffic from legitimate network traffic. This technology is critical to the monitoring process and must be scalable to support an ever-increasing number of managed devices.

**Automated security event correlation**

Automated security event correlation groups individual signs of malicious activity by logical criteria, such as attack source, type, and destination. This enables security administrators to rapidly reconstruct and visualize an attack in its entirety. Without automated correlation, this is a manual process that is simply too time-consuming and complex to handle with any degree of scalability.

**Expert response to events**

Incident response is determined after security administrators review data generated by the correlation process. Actions may range from simple client notification to immediate involvement of law enforcement authorities. Review of security events on a 24x7 basis – and timely response to those incidents – is a critical element of advanced security monitoring.

**Event reporting**

Event reporting is the process by which customers are notified of security events that occur on their network. Notification may be completed by an immediate phone call, e-mail, postings to a real-time Web portal, periodic reports, or a combination of these methods.

**SECURITY MANAGEMENT**

Security device management refers to people and process issues that many security service providers address adequately in their basic services. The key to providing effective security device management is to engage security experts with the necessary experience and expertise. These experts should be able to implement best practices and standards for configuration and performance management, as well as processes and operating procedures to ensure that each security device conforms to these standards at all times. Effective security management requires skilled personnel who can perform the following services:

**Fault management**

This review ensures that devices function optimally at all times, and includes a regular “health check,” notification to customers, guidance if a device ceases to function for any reason, and periodic reports summarizing the operational status of devices.
Configuration management

Maintenance benefits offered by a managed security services provider include security device modifications, software support and upgrades, policy and rule changes, and daily, weekly or monthly reports summarizing all actions taken to maintain the configuration.

Performance management

This service involves the collection and presentation of performance statistics. These reports often include statistics that reveal the speed and efficiency of the network, help to identify bottlenecks that hinder network performance, and show consolidated log data from security devices.

Signature Maintenance

The managed security services provider should also maintain and update the signature database for the organization’s network-based intrusion protection system in order to shield the network from the latest exploits and threats.

Symantec ManHunt™ Network Intrusion Protection System

Symantec ManHunt is a cost-effective, real-time, intrusion detection, threat analysis, and policy-based response solution that protects networks of all sizes against intrusion and denial of service attacks. This effective intrusion protection system offers a unique hybrid architecture that includes the ability to analyze network traffic using protocol anomaly detection (i.e., zero-day detection), rather than solely relying on prior signatures. By providing layered protection against known and unknown attacks without overwhelming IT resources with false positives, Symantec ManHunt eliminates the window of vulnerability present in traditional signature-based intrusion detection products. Enabling a coordinated approach to enterprise security, Symantec ManHunt identifies threats, gathers actionable security intelligence, and delivers essential information based on incident type and location to help security administrators contain attacks in real time.

Symantec ManHunt supports throughput speeds ranging from 100 Mbps to two gigabits per second, depending on system configuration and organizations’ specific needs. The solution goes beyond passive incident identification and alerting to actively defend the network. It provides cross-node analysis to identify network traffic trends and quickly recognizes events as they occur. A scalable architecture enables a single Symantec ManHunt node to monitor and manage multiple network segments in a given geographic area, eliminating the need for additional hardware deployment. This reduction in hardware results in lower procurement and support costs, and increased rack space.
Symantec Managed Security Services help organizations enhance their security posture and defend against emerging threats, thereby minimizing the potential occurrence and impact of security attacks. In addition, Symantec Managed Security Services offerings provide flexibility to accommodate a variety of security environments, ensuring customers the freedom to select best-of-breed security devices.

Symantec offers the only true real-time monitoring services in the Managed Security Services industry. Symantec Monitored and Managed IDS Services provide complete security monitoring and management of intrusion protection systems, including 24x7 monitoring and advanced analysis of security log and alert data, advanced data mining to detect suspicious activity, and expert commentary on analyzed activity. Management functions include remote configuration, rule change, system and software support, signature maintenance, and system upgrades. The services use a next-generation technology platform to detect suspicious network activity, identify threats, and confine evolving attacks. In turn, this allows Symantec security experts to continuously analyze event data across multiple security devices. This level of vigilance helps prevent internal and external threats from causing harm.

For those organizations that leverage Symantec ManHunt along with Symantec Managed Security Services, the benefits increase. Symantec ManHunt’s zero-day protection features in particular, combined with the rapid and timely response of Symantec Managed Services, deliver a powerful level of protection and response. When the hybrid detection features within Symantec ManHunt detect a zero-day attack, the information is immediately sent to the Symantec Security Operation Center (SOC) analysts, who then correlate it with other incidents. A Symantec analyst then assesses these incidents to determine the nature and severity of the attack, notifies the affected customer, and recommends mitigation and/or remediation measures. The result is faster, more effective response to new attacks and outbreaks than can be achieved by monitoring and managing a signature-based intrusion protection system. Symantec ManHunt can monitor multiple network segments, allowing Symantec Managed Security experts to customize a threat response for each individual segment according to its specific hardware and software configuration.

Whether or not organizations choose Symantec ManHunt or an alternative third-party intrusion detection or prevention product, Symantec Managed Security Services provide organizations with dedicated expertise to improve enterprise protection and maximize their investment in information security. Through Symantec’s managed security services, organizations gain a real-time view of their enterprise security posture and the analysis and commentary needed to adjust defenses against emerging attacks, for optimal protection of mission-critical assets.

Symantec also offers managed security services to address a wide spectrum of security products and issues, including firewall, security appliances, vulnerability scanning, policy compliance, and antivirus at the gateway. Monitored and Managed Firewall Services often precede or are configured with IDS services to provide the comprehensive monitoring and management services that organizations require. These services help security administrators detect and respond to the most sophisticated and malicious hacker attacks with real-time, 24x7 security monitoring and expert analysis of firewall logs, including those generated by third-party firewall devices.
To further meet the varying needs of organizations, Symantec offers multiple tiers of its managed security services. These service level tiers are suited to a variety of security profiles and budgets, and allow the flexibility to mix levels of service depending on system criticality. Symantec maintains relationships with a variety of value-added resellers and other solution partners that can help organizations install security devices and activate these managed security services.

MONITORED SERVICES

All of Symantec’s monitored services offer comprehensive monitoring capabilities. Based on their needs, organizations can choose the level of incident commentary and recommendation they would like to receive. Access to Symantec SOC analysts varies based on the level of service chosen.

Standard Monitored:
This level of service includes human analysis of data to identify and separate real attacks from false positives. The Symantec Managed Security Services team leverages their global security intelligence to gather critical security data specific to the customer and to provide comprehensive analysis on severe security incidents. In addition, Symantec analysts provide commentary and recommendations on all severe security incidents. Should such an incident occur, customers receive automated notification from the Security Operations Center (SOC). Security analysts work with organizations to help them understand and respond to any severe security incident. Customers also have the option to receive consultation from a security analyst on the overall security landscape in order to strengthen their security posture.

Premium Monitored:
The Premium level of service includes human analysis of data to identify and separate real attacks from false positives. The Symantec Managed Security Services team leverages their global security intelligence to gather relevant security data specific to the customer and to provide comprehensive analysis on all types of security incidents. In addition, Symantec analysts provide commentary and recommendations on all levels of security incidents; recommendations range from informational to emergency (requiring immediate attention). Should a security incident occur, customers will receive notification of the incident directly from a SOC analyst. Security analysts work with the customer to help them understand and respond to any severe security incident. In addition, the security analyst will review the overall security landscape with the customer, and recommend how the organization can strengthen its security posture.
MANAGED SERVICES

Symantec offers three tiers of management capability to provide organizations with the flexibility they require to address their business needs. All three tiers include security device policy changes, device management for all supported security devices (including third-party solutions), and customer communications with the SOC.

**Standard Managed:**
With this level of managed service, customers are provided with multiple standard policy changes throughout the term of service. Standard maintenance for devices managed by Symantec will be completed within 24 hours of the request. In addition, any emergency maintenance for the devices will be done within one hours’ notice. Customers may make change requests through the Symantec Secure Internet Interface (SII) or may relay requests via phone to a Security Operations Center analyst.

**Enhanced Managed:**
The enhanced managed service level provides customers with multiple emergency policy changes and up to 15 standard policy changes throughout the term of service. Standard maintenance for devices managed by Symantec will be completed within 24 hours of the request. In addition, any emergency maintenance for the devices will be done within one hours’ notice. Customers may make change requests through the Symantec Secure Internet Interface (SII) or may relay requests via phone to a Security Operations Center analyst.

**Premium Managed:**
With this level of managed service, customers are allowed multiple emergency policy changes and an unlimited number of standard policy changes. Standard maintenance for devices managed by Symantec will be completed within 24 hours of the request with every attempt to schedule the maintenance during the customer’s off-peak hours. In addition, any emergency maintenance for the devices will be done within one hours’ notice. Customers may make change requests through the Symantec Secure Internet Interface (SII) or may relay requests via phone to a Security Operations Center analyst.

SYMANTEC SECURITY TECHNOLOGY PLATFORM

The Symantec Security Operations Center (SOC) next-generation platform enables real-time security monitoring and 24x7 expert security analysis of IDS, firewall, and other security device logs. The platform’s advanced data mining and automated security event correlation capabilities empower administrators in Symantec’s SOCs to monitor security devices in real time, reliably identify threats and suspicious activity, and rapidly respond to attacks. Security Operations Centers are staffed with security experts from a broad range of disciplines to complement organizations’ in-house IT security capabilities. Through the Secure Internet Interface customer portal, Symantec gives security managers an up-to-the-minute view of all threat detection activity on their network architecture.
Competitive Advantages of Partnering with Symantec

Symantec enables organizations to simply and cost-effectively employ industry-leading network-based intrusion protection and security expertise to mitigate threats at the network perimeter. A combined Symantec ManHunt-Symantec Managed Security Services offering delivers a powerful level of protection and response. Symantec ManHunt provides detection of zero-day attacks, which in turn strengthens the rapid response and analysis capabilities of the Symantec Managed and Monitored Services team. This combination of Symantec product and service enables organizations to add a critical layer of network protection and effectively manage it without incurring the added cost and burden of in-house device management and monitoring. Those organizations with a mix of security devices from multiple vendors can also leverage Symantec’s comprehensive firewall and intrusion protection management and monitoring capabilities to further protect information assets and mitigate security threats.

Partnering for intrusion protection activities in this way helps organizations manage the volatility associated with staffing for and responding to unpredictable network threats. By placing their ongoing security tasks and upgrades in the hands of Symantec’s knowledgeable experts, organizations can focus in-house resources on core business initiatives. Through a combination of advanced intrusion protection technology and expert managed security services, Symantec helps organizations protect critical networks, lower the total cost of security management, and realize the maximum return on their security infrastructure investments.

Symantec, the world leader in Internet security technology, provides a broad range of content and network security software and appliance solutions to individuals, enterprises and service providers. The company is a leading provider of virus protection, firewall and virtual private network, vulnerability assessment, intrusion prevention, Internet content and email filtering, and remote management technologies and security services to enterprises and service providers around the world. Symantec’s Norton brand of consumer security products is a leader in worldwide retail sales and industry awards. Headquartered in Cupertino, Calif., Symantec has worldwide operations in 38 countries.

For more information, please visit www.symantec.com