WHITE PAPER

symantec™

Demystifying the Managed Security Service Provider Market

INSIDE

- Effective security management and monitoring
- A closer look at management vs. monitoring
- How the right MSSP can make a difference
- Symantec Managed Security Services

Contents

Executive summary 3

The need for effective security management and monitoring 4

A closer look at management vs. monitoring 5

What is security management 5

What is security monitoring 6

Distinguishing security monitoring claims around from the reality 7

How the right MSSP can make a difference 8

Symantec Managed Security Services 10

Comprehensive management, monitoring, and response services 12

Benefits of choosing an MSSP that provides both security management and monitoring . . 13

Glossary 14

References 15

Executive summary

The value of data in today's information age has forced organizations to increase efforts to mitigate security risk and maintain the company's market standing. But providing an effective level of security requires a combination of state-of-the-art technology, experienced personnel, proven processes, and continuous threat intelligence that few organizations possess. Those organizations that choose to tackle these critical issues in-house invariably find themselves struggling to identify security events, provide security event alerts, respond to the threats, and manage the security risks that threaten their competitive advantage.

Managed Security Services Providers (MSSPs) remove the burden of managing and monitoring security devices and events, providing a level of technology and expertise that ensures rapid response to real threats. However, the wide range of MSSPs and their offerings can prove daunting to compare and understand.

This paper defines the key elements of a managed security service offering, with a focus on clarifying the differences between security management and monitoring. It also provides a set of criteria companies can reference when assessing an MSSP. It presents the features of the Symantec Managed Security Services offering, which is composed of a unique combination of technology, experience, processes, and human expertise. The paper concludes by summarizing the value of choosing an MSSP that provides both security management and monitoring.

By clarifying terms and types of services, the paper will help demystify the process of choosing an MSSP, so organizations can select the MSSP most likely to strengthen the company's security posture.

The need for effective security management and monitoring

It is essential that organizations weigh the risk of exposing their data to third parties against that of potentially losing intellectual property and productivity as a result of malicious activity. Only robust, round-the-clock security management and monitoring can mitigate the risk of these threats against an enterprise network. But effective security management and monitoring requires a combination of best-of-breed technology, security best practices and expertise not typically found in enterprise environments. According to Gartner, internal teams struggle to understand and combat the latest threats because they need to monitor systems constantly and remain up-to-date on all system vulnerabilities.[1] Maintaining the necessary level of vigilance requires significant investments in staff, IT systems, and training.

When companies choose to handle security management or monitoring in-house, they are often unsuccessful, for a variety of reasons. One reason for failure is that while the security staff commits to the tasks, they discover that they lack the time, expertise, and technical resources to provide effective, enterprise-wide monitoring and management on a 24x7 basis. Alternatively, enterprises may rely on security appliances alone. On their own, security appliances do not provide an adequate level of security protection, as evidenced by the 2002 CSI/FBI Computer Crime and Security Survey, which found that of the enterprises reporting security breaches, 90% had implemented firewalls and 60% had intrusion detection systems.[2]

True security monitoring can only be accomplished by combining advanced technology with expert human analysis. While enterprise security management vendors may provide correlation and data-mining products, the analysis of the data and corresponding response decisions produced by security experts are critical to preventing attacks. Some organizations use brute force methods, assigning security staff to manually review event logs. The reality is that it is impossible to manually examine millions of logs from disparate devices and locations, data-mine with specific queries to look for suspicious activity, and then cross-correlate the results to substantiate attack trends in real time.

Managed Security Service Providers (MSSPs) can address these issues and help organizations gain an effective security posture. Yet many organizations are not certain what to look for when choosing an MSSP. The issue is clouded by the fact that most MSSPs provide ad-hoc management or monitoring of security devices and the definition of the services they offer varies from vendor to vendor.

A closer look at management vs. monitoring

Early managed security services focused on security device management – that is, the management and maintenance of security devices, such as firewalls, intrusion detection systems, servers, and routers. Due to the increased sophistication, number, and type of threats to the corporate network, these services are now being supplemented with monitoring that provides expert, real-time analysis of the data generated by security devices, to enable timely response to intrusions.

What is security management?

Security management requires skilled personnel who can manage security devices in the following three ways:

- Fault management
- Configuration management
- Performance management

FAULT MANAGEMENT entails the management of customers' security devices to ensure that the devices function optimally at all times. This is usually, but not always, provided on a 24x7 basis. Fault management services typically include the following:

- A regular "health check" of security devices to detect problems.
- Notification to customers if a security device ceases to function for any reason, and guidance regarding appropriate measures to remediate the problem.
- Periodic reports to customers summarizing the operational status of security devices over a specified period of time.

CONFIGURATION MANAGEMENT assigns the configuration of a customer's security devices to an MSSP. Configuration management typically includes the following features:

- Security device application and operating system modifications and upgrades.
- Policy and signature changes to the security device.
- Daily, weekly, or monthly reports summarizing all new upgrades and modifications to customer security devices.

PERFORMANCE MANAGEMENT involves the collection and presentation of performance statistics for a customer's security devices. Content included in these reports often includes:

- Statistics describing the speed and efficiency of a customer's network.
- Identification of network bottlenecks that hinder performance.
- Consolidated performance reports that include all log data generated by a customer's security devices.

Most MSSPs provide one or more of these capabilities, but few address all three components.

What is security monitoring?

Security monitoring requires security expertise and a sophisticated architecture that helps analyze data across multiple devices across an entire global enterprise. Comprehensive monitoring services include the following capabilities:

DATA COLLECTION AND NORMALIZATION – This is a process in which security device data (e.g., firewall logs, IDS alerts, etc.) is collected and transformed into a standardized format, regardless of device type and brand. Data normalization is essential to effective security monitoring, as it enables MSSPs to use a standardized set of queries to mine security device data and isolate signs of malicious activity.

DATA MINING – In this process, an automated system continuously queries security data to detect signs of malicious activity and separates suspicious network traffic from legitimate network traffic. This is probably the most critical technological element in the monitoring process. A customer must ensure that an MSSP has the ability to scale their data mining abilities as more devices are plugged into the backend architecture. In other words, the MSSP must be able to build sophisticated queries as new devices are added. More queries does not necessarily equate to better data mining. The quality of the existing queries and their continuous refinement, as well as the timely creation of new queries to root out ever-evolving malicious activity, is of paramount importance. Only with highly sophisticated data mining can an MSSP provide the most effective cross-correlation of attack data.

AUTOMATED SECURITY EVENT CORRELATION – Another essential feature of an effective security monitoring service is correlation. This is the automated grouping of individual signs of malicious activity by logical criteria, such as attack source, type, and destination. The result of this process is the rapid reconstruction of attacks, enabling analysts to visualize an attack in its entirety. Without automated correlation, security analysts are forced to manually piece together attack sequences by manually scrolling through millions of lines of security device data. Even on networks experiencing low volume traffic, this task is simply too time-consuming and complex to handle with any degree of scalability.

EXPERT RESPONSE TO EVENTS – Response to security events is determined after security analysts review data generated by the correlation process. Depending upon the nature of the event, actions may range from simple client notification to immediate involvement of law enforcement. Having security experts review security events on a 24x7 basis is a critical element of every managed security service.

EVENT REPORTING – Event reporting is the process by which clients are notified about security events detected on their network. Depending upon the nature of the event, reporting can be handled through immediate voice notification, e-mail, postings to a real-time Web portal, periodic reports, or some combination of the above.

To provide effective, real-time security monitoring, an MSSP must incorporate all of the features listed above. Real-time protection, detection, and correction of network security risks are simply impossible if any of these components are missing.

The added human expertise and a complex technical architecture capable of analyzing data across multiple devices enterprise-wide is what separates security management from security monitoring. This was amplified in the article "Top Guns" that appeared in Information Security Magazine: "Security software has made great progress in its ability to consolidate, correlate and analyze event and log data from multiple devices –firewalls, IDSes, routers. But the people who sit in the cockpit of an MSSP SOC [security operations center] say old-fashioned intuition remains their most reliable tool when analyzing security events."[3] Despite their claims, few MSSPs have the necessary technical architecture and human expertise to provide effective security monitoring.

Distinguishing security monitoring claims from the reality

In marketing their monitoring capabilities, some managed security service providers mislead or confuse potential customers with their service descriptions. The following are common "security monitoring" offerings and their true definitions:

UP-TIME MONITORING – This simply means that the MSSP is ensuring that the security device is operating. Unfortunately, this does not help identify and prevent attacks, and at most, only provides customers of notification that a security device is not performing properly. A quality MSSP would perform this function as part of its management services.

LOG REDIRECTION – Typically, an MSSP offers this as an alternative to data mining and correlation because they lack the necessary technology and human expertise to perform these complex tasks. With log redirection, the MSSP simply extracts filtered security device data and presents it to the customer for analysis, putting the onus on the customer to identify and review suspicious data.

Some MSSPs claim to "correlate" security data from various devices, but in reality lack the architecture and technology to perform this task. Two examples are described below:

DATA CONSOLIDATION – Many MSSPs address correlation simply by collecting security data from disparate security devices and consolidating the data into a single view. Under this model, no automated processes connect pieces of data that logically relate to each other – the true definition of correlation. While this approach is useful in consolidating data for management purposes, it does not allow the MSSP to detect and respond to network attacks in a scalable fashion.

MANUAL CORRELATION – MSSPs that lack the technology to automate the correlation process will often claim to accomplish correlation by manually linking signs of malicious activity. Given the vast amount of information generated through the data mining process (even on a small scale), manual correlation is not a reliable or scalable method of reconstructing network attacks.

How the right MSSP can make a difference

An MSSP that provides the right combination of people, process, and technology coupled with continuous threat intelligence can maximize the value of an organization's investments in technology and internal resources while helping to smooth out security spending. Perhaps most importantly, by effectively solving security problems, these services enable enterprises to focus on their core business issues.

The following criteria should be considered when determining which MSSP can best provide secure, cost-effective, and flexible security services.

LONGEVITY. Enterprises should not take lightly the decision to entrust their sensitive security data to an MSSP. When organizations choose an MSSP, they are partnering with a company that will learn intimate details about the company's security measures and proprietary data. Both the MSSP and the customer will need to invest time and resources to ensure that the service is effectively addressing the organization's most critical needs. Because of this commitment, companies will want to partner with a stable vendor that has a proven track record of delivering quality services to a large number of customers over a long period of time. Organizations should also consider the ability of the MSSP to weather any economic downturns or industry shakeouts.

ANNUAL REVENUES. According to Gartner, for publicly traded companies, annual run rates of more than $10 million per year in managed security services contracts indicate a sufficient base of revenue to support growth and enhancement of services, if the vendor executes correctly.[4]

BREADTH OF CHANNEL PARTNERS. Companies will want an MSSP to invest its funds in security enhancements. If a company has a solid partnership program in place, it can increase its customer base without having to expand its direct sales channel, thus enabling it to direct more funds to Research and Development. These partnerships also allow the MSSP to serve customers in different industries, across all geographies, and supplement its own offerings with those of its partners. Because one strategic capability of an MSSP is to leverage the data across all of its customers' security devices to gain insight into new and emerging threats, its ability to expand its market reach can directly impact the quality of managed services it provides.

MANAGEMENT EXPERIENCE. A successful managed services provider staffs its security experts from a range of backgrounds, including those from military, government, and industrial sectors. Appropriate management experience is usually represented from a variety of applicable related services, such as online, financial, and service bureaus.

MINDSHARE. A company with higher market visibility is able to better leverage channel partnerships and is usually in a sound financial position. Some of the marketing vehicles that contribute to a strong mindshare include customer education programs, the dissemination of security advisories and alerts, press and trade publication exposure, and customer testimonials.

BREADTH OF SERVICES. The range of services offered indicates the MSSP's ability to meet the evolving security management needs of a wide variety of enterprises. Leading MSSPs will offer a complete set of managed and consulting security services, either organically or through partnerships. Services should include managed firewall, intrusion detection, antivirus, vulnerability assessment, and consulting services.[5] Ideally, the MSSP will offer customized services to meet the unique organizational requirements of each of its customers.

SECURITY MANAGEMENT PROCESSES. An MSSP should be able to provide documented standards and policies for handling typical and atypical operations and threats. Those MSSPs that have developed best practices based on industry standards are best able to provide effective security management and incident response services. The MSSP should offer a variety of attack alert notification methods to allow customers' security staff the ability to mitigate risk in real time.

AUDITING. Enterprises are being held to a higher standard of accountability with respect to audit requirements. As an extension of the enterprise, an MSSP must have facilities, processes, and procedures that are validated and certified by a third-party auditor in the form of a BS7799 and/or SAS70 Type II audit.

COMMITMENT TO TECHNOLOGY. The technology used to analyze and correlate data collected from multiple devices should support rapid response while ensuring the scalability to support an ever-increasing number of managed devices. The technology should be supported by security analysts who can separate real threats from false ones, so that customers can focus security staff on the most critical security issues.

REPORTING. Reporting can provide an enterprise-wide, real-time view into the customer's security posture and the effectiveness of the managed services. Thorough reports will include detailed information garnered from the managed devices, the related or recommended responses, any changes the MSSP made to the devices, and information about the latest threats. Ideally, the MSSP will provide options for viewing and managing reports, including access via e-mail, standard desktop programs, and a secure Web portal.

SECURITY OPERATIONS CENTER CAPABILITIES. An MSSP will need to operate multiple security operations centers (SOCs) from which it can globally monitor and manage security issues across its customer base. In today's business environment, these centers must be run 24x7x365, not only to remain abreast of the latest threats but also to ensure business continuity. These centers must follow predictable and proven processes and should be staffed with a range of security experts that extend the customer's in-house capabilities. Strict hiring guidelines must ensure that hackers are not entrusted with an enterprise's sensitive security data.

Symantec Managed Security Services

Symantec Managed Security Services, a division of Symantec Corporation, offers a unique combination of people, process, technology, expertise, and experience. This enables Symantec to provide managed security services that surpass standard security monitoring and management offerings. The following capabilities set Symantec's offering apart from others:

INDUSTRY LEADING SECURITY OPERATIONS CENTERS – Symantec has six security Operations Centers strategically located around the globe. Symantec Managed Security Services specialists offer more than 24x7 coverage by providing follow-the-sun support from these SOCs. This means our specialists provide around-the-clock vigilance combined with multi-lingual, localized capabilities, so customers experience no time delay in problem resolution. With full certification to meet international standards for information security management practices as set out in BS7799, Symantec's real-time Security Operations Center technology platform and best-practice methodologies ensure the highest level of protection and response for enterprise security.

SUPERIOR TRENDING CAPABILITIES – Symantec SOCs have superior data collection, normalization, data-mining, and cross-correlation capabilities. This enables Symantec to look across its entire customer base to elicit trends, gather intelligence, and validate attacks; this global trending analysis is based on a variety of monitored and managed security devices. By running thousands of queries every second against a massive 32 terabyte database and cross-correlating this information across multiple locations and times, and thousands of customer's security devices, the SOC Technology Platform is able to accurately identify signs of malicious activity.

REAL-TIME ANALYSIS AND INTERVENTION – Because the SOC technology applies vigorous, real-time analysis to genuine threats, Symantec security experts are able to supply timely and meaningful insights with alerts, specific recommendations, and response. Working closely with the customer, Symantec security analysts take action to defend against intrusions before a crippling loss of information can occur.

FLEXIBLE ESCALATION – Symantec works with its customers to develop customized escalation procedures that address each organization's unique requirements. Symantec security engineers initiate responses to security events in accordance with these customized procedures.

CUSTOMIZABLE REPORTS – Symantec provides the ability for customers to create customized reports and views via the Secure Internet Interface, Symantec's secure Web portal for Managed Security Services.

VENDOR NEUTRALITY – Symantec Managed Security Services provide the flexibility to accommodate a variety of security environments, allowing customers the freedom to select best-of-breed solutions. Symantec security specialists have certified expertise across a broad range of security products from a variety of security providers including Symantec technologies. Today, 80% of Symantec's monitored and managed devices are non-Symantec products. The ability to monitor and manage diverse security products in an integrated manner ensures effective analysis and threat detection, while protecting the value of customers' existing investments.

SOC CERTIFICATIONS – Symantec's UK and Alexandria SOCs are BS7799 certified. In addition, Symantec is renewing its Check Point Certified MSSP designation and is preparing to apply for SAS70 Type II certification for the Alexandria SOC. Symantec Managed Security Services is also a member of the AVVID technology affiliates program and the OPSEC partner program.

SECURITY BREADTH AND DEPTH – Symantec is a leading provider of client, gateway and server security solutions to enterprises and service providers around the world. Among the products available are virus protection, firewalls, virtual private network technology, vulnerability management, intrusion detection systems, content and e-mail filtering, and remote management technologies. Symantec's experience with this wide breadth of security technologies makes us an ideal partner with which enterprises can share the burden and responsibility of security management and incident response.

"Reputation, credibility, trust and confidence are fundamental customer commitments. We needed a partner that would provide an integrated solution–the products, consulting and proactive management necessary to protect ourselves and our customers."

The integrated security solution in which Citizens placed its trust came from the world's recognized Internet security leader: Symantec Corporation. "We looked to partner with a vendor that would take our business as seriously as its own."

- Elsa Zavala, senior vice president and director of Information Services, Citizens Business Bank

Comprehensive management, monitoring, and response services

Symantec Managed Security provides the following array of outsourced security management, monitoring, and response services that enables organizations to leverage the knowledge of Internet security experts in order to protect the value of their networked assets and infrastructure.

MONITORED AND MANAGED FIREWALL SERVICES. Flexible, remotely managed and monitored firewall and VPN solutions to help detect and respond to most sophisticated malicious hacker attacks.

MONITORED AND MANAGED INTRUSION DETECTION SERVICES (IDS). Provides 24/7 real-time security monitoring and expert analysis of IDS alerts.

MANAGED INTERNET VULNERABILITY ASSESSMENT SERVICE. Scans and evaluates the security of Internet-exposed systems such as firewalls, Web servers, and mail servers to detect unauthorized access and prevent tampering or theft.

MANAGED SECURITY POLICY COMPLIANCE SERVICE. Assesses security configurations against stated policies, helping to eliminate exploitable vulnerabilities that pose a threat to e-business initiatives.

MANAGED VIRUS PROTECTION SERVICE. Expert management of antivirus gateways from the leader in antivirus technology.

MONITORED AND MANAGED INTEGRATED SECURITY APPLIANCE SERVICE. Organizations can gain new levels of protection with a comprehensive gateway solution that delivers coordinated event monitoring, analysis and management for the Symantec Integrated Security Appliances, which combine firewall, intrusion detection, antivirus, and content filtering technology.

For more information about these Symantec service offerings, please visit
http://enterprisesecurity.symantec.com/SecurityServices/content.cfm?ArticleID=682&EID=0

"Intrusion happens all the time; it is not limited to the typical nine-to-five workday. Before the Nimda virus, security monitoring was a part-time activity for us. It was not receiving the appropriate focus. We did not have the proper resources in place, and it would have been too time-consuming and expensive to bring them on internally. Symantec provides a level of service that would not be cost-effective for us to do ourselves."

- Richard Diamond, chief information officer, The Doctors Company

Benefits of choosing an MSSP that provides both security management and monitoring

Organizations gain maximum efficiencies, effectiveness, and enterprise protection by leveraging the capabilities of a Managed Security Services Provider that offers an advanced technology platform and expertise across the ongoing management of security services. Comprehensive services that incorporate both security monitoring and management provide the ability to turn data into actionable information in real time, so that IT personnel can respond to genuine threats. This enables organizations to achieve a stronger security posture than they could on their own and frees security personnel to focus on higher-value strategic initiatives that are central to the business.

Managed security services also remove the volatility associated with staffing and responding to unpredictable network threats, allowing customers to better manage expertise requirements, resources, and cost. In addition, organizations benefit from a higher level of security while maximizing the value of existing security investments.

Unlike other MSSPs, Symantec Managed Security Services provide customers a unique opportunity to discover, through empirical expert monitoring and analysis, the frequency, severity, and source of Internet attacks against their business environment. With around-the-clock monitoring and response at the Symantec Security Operations Centers, security analysts deliver cost-effective, outsourced services that minimize an organization's investments in technology and internal resources while significantly mitigating its security risks.

"Outsourcing to an MSSP enables managers to receive timely updates on all aspects of the network, which often include recommendations tied to the company's

business objectives. These recommendations can be based on hardware faults, bottlenecks in the network and unusual behavior in traffic. They can also be new business initiatives. Companies are therefore able to get the best from the architecture they are running, and to alter it promptly for either technical or business reasons."

- Gartner, Managed Security Services Bring IT Value, 10 January 2003

"Most organizations, not just those with sophisticated Internet activities, can benefit from continuous management and monitoring of their security operations. Many IT security breaches still come from within companies. An MSSP can help managers develop an enterprise-wide security policy, and set appropriate access control rules governing all employees."

- Gartner, Managed Security Services Bring IT Value, 10 January 2003

Glossary

DATA CONSOLIDATION	combining data from multiple sources
DATA CORRELATION	the automated grouping of individual signs of malicious activity by logical criteria, such as attack source, type, and destination
DATA MINING	the automated extraction of predictive data from large databases
EVENT LOGS	records of security events detected by security products
NORMALIZATION	a process whereby data from a variety of sources is translated into a common format or language
SECURITY EVENT	potentially suspicious activity reported by one or more security device or sensor. May consist of multiple sub-events.
SECURITY INCIDENT	a set of one or more security events or conditions that requires action and closure
SECURITY SUB-EVENT	potentially suspicious activity reported by one security device or sensor.
SOC	Symantec Operations Center, which serves as home to security analysts and customer engineering groups. Designed for maximum redundancy, Symantec's multi-million dollar, state-of-the-art SOCs contain redundant, discrete power sources, fire suppression systems, three-factor biometric personnel screening, and VPN termination points that allow interoperability with nearly any client network.
SOC TECHNOLOGY PLATFORM SIGNATURE	A query that mines enterprise security data in search of specific patterns of malicious activity.

References

[1] Gartner Inc., "Managed Security Services Bringing IT Value and IT Excellence", 10 January 2003

[2] 2002 CSI/FBI Computer Crime and Security Survey, "Computer Security Issues & Trends", Vol. VIII, No. 1, Spring 2002, http://www.gocsi.com/press/20020407.html

[3] Information Security Magazine, "Top Guns", August 2002, http://www.infosecuritymag.com/2002/aug/topguns.shtml

[4] Gartner, Inc., "Choosing a Managed Security Services Provider", 31 August 2001

[5] Ibid

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

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