IBM Global Technology Services
Thought Leadership White Paper

May 2011

Selecting a Managed Security Services Provider: The 10 most important criteria to consider

IBM

Introduction

Enterprises today struggle with an ongoing battle to defend against online attackers that can strike at any moment. Whether it's viruses or denial-of-service attacks or unauthorized website access, if these offenders succeed, they can wreak havoc by impacting business operations and workforce productivity, damaging the infrastructure, and creating security breaches that can harm a company's reputation. Successful compromises or breaches are also expensive, in terms of operational impact, resources required to remedy the breach and potential loss of business.

The need for information security is broadly accepted. A successful security program demands deep insight into the current threat landscape. It also requires a strategic approach to managing the cost and complexity of the security technologies needed for security event and log management, vulnerability scanning, email security, and other activities. However, with the wide variety of current and emerging security threats, companies managing their own information security often lack the in-house resources required to protect online systems on a 24/7 basis. Advanced security practices require highly skilled personnel who can be expensive to recruit, hire, and retain—a challenge for firms with limited IT budgets. In addition, implementing and managing security solutions can divert IT resources from other critical initiatives, including preventing the next attack. Instead, IT teams are forced into a reactive posture that ignores the more important strategic role of an IT security function.

To ensure a cost-effective, comprehensive, proactive security posture, more and more companies are outsourcing portions or even all of their IT security programs. These companies typically:

- Lack the in-house capabilities required to keep pace with changing business demands, compliance mandates, and emerging threats for strategic implementation of new IT security solutions.
- Don't have the capabilities to effectively monitor and manage the security infrastructure to ensure optimal utilization of current assets.
- Have in-house IT staffs that spend too much time on day-to-day operational security issues versus new strategic projects.
- Depend on IT security tools and processes that provide a reactive, rather than proactive, approach to mitigating risk and minimizing data loss and downtime.

By outsourcing security operations to a managed security services provider (MSSP), companies can take advantage of the expert skills, tools, and processes provided, and significantly enhance the security of the enterprise, without making a large investment in technology and resources. The benefits of outsourcing security are clear, but selecting the right MSSP isn't as straightforward.

This white paper outlines a strategic approach to selecting an MSSP and establishes the 10 most important qualifications to consider in choosing a provider. The right MSSP can reduce the cost and complexity of information security while building a stronger security posture.

The 10 most important things to consider in selecting an MSSP

Companies that lack the resources and budget to build and operate security infrastructure on a 24/7 basis can outsource to a reliable MSSP. Allowing an MSSP to handle day-to-day security monitoring and management gives organizations an opportunity to allocate in-house IT resources to more strategic initiatives. MSSPs also facilitate business continuity by providing advanced intelligence to thwart attacks before they cause damage and disrupt business operations. This layer of proactive protection lends a competitive edge by ensuring that businesses will remain functional even when sophisticated malware is spreading rapidly across the Internet.

The potential benefits of outsourced security can only be achieved by selecting the right provider. To achieve the greatest advantage from outsourcing your security operations to an MSSP, be sure to first conduct an extensive evaluation of your security requirements. Understand which security measures you must comply with and establish a reliable governance model. Also understand which security requirements you expect the MSSP to have in place and be prepared to investigate whether they're equipped with relevant certifications that demonstrate their capabilities in these areas.

When ready to evaluate MSSPs, consider the following 10 criteria to ensure that the provider you select will best protect your vital IT assets while helping you meet compliance.

1) Broad portfolio of security services

Your security needs are continually evolving with the dynamic nature of your business environment, the influx of new threats, and changing regulatory requirements. Ensure that any managed security services partner offers a comprehensive suite of vulnerability assessment and management services that will keep you protected ahead of threats, regardless of your security challenges. To meet your budget and unique protection requirements, choose an MSSP that provides multiple service levels and the ability to mix and match services. Also consider a provider with offerings that are prepackaged and structured to ensure consistent delivery and performance. Through world-class services that address risk across each aspect of your business, you can build a strong security posture that will reduce costs, improve service, and manage risk.

2) Highly respected security intelligence and research experts

The MSSP you choose should have extensive, top-tier internal and external resources with ongoing insight into the latest attack strategies, network threats, and vulnerabilities, including up-to-the-minute information on emerging threats and remediation. Global operations groups, strong research and development teams, and proven vulnerability and threat analysis processes are crucial to keeping your company protected from evolving attack schemes and technologies. When MSSP providers focus on discovering and researching security vulnerabilities, while working with the affected vendors to get them fixed, your systems will be updated and protected before threats have a chance to impact them.

3) Reputation of the MSSP

You should also consider the reputation of an MSSP and their history of customer satisfaction. Look for a provider who has successfully retained customers for several years. Ask what their average customer churn rate is, looking for long-term customers in an industry and with network needs similar to yours. Ask to see results from current customer satisfaction research conducted either internally or by a third-party vendor. Leverage analyst reports that include the MSSP and compare them with competitors, for a non-biased evaluation of their services and expertise. Also ensure that their solid reputation stands beside a solid vision for the future. Make sure that the provider is investing in their portfolio of solutions and services, and has a clearly defined strategic roadmap that aligns with your security goals.

4) Robust web-based management tool

Though the MSSP will deliver a portion or all of your of your IT security program, your IT team will nonetheless need ready access to a comprehensive view of your entire security infrastructure. Look for an MSSP that provides a single management console, with the flexibility to mix and match by device type, vendor, and service level to meet your individual business needs. The best web-based management tools will allow your security resources to easily monitor both managed and unmanaged security devices.

5) Sophisticated back-end technology

Once you're certain that an MSSP is committed to ongoing global security intelligence, make sure they have the backend technology to align that intelligence with your IT infrastructure and security initiatives. The underlying protection system, accessed through a management portal, should perform far more than simple event monitoring and device management. The backend technology should also have the capabilities to perform advanced analysis, correlation, aggregation, categorization, and prioritization. Look for technology with incident escalation and remediation, and a sophisticated alert mechanism—all tied to an enormous database of known threats, provided by and continually updated by the MSSP. Ensure that your provider is leveraging a common platform across its customer base, rather than attempting to manage multiple distinct platforms simultaneously, which can increase opportunities for variance in service delivery.

6) One-stop solutions for federal, state, and industry regulations

Your MSSP should have a deep understanding of the compliance regulations that apply to your particular industry. Therefore, confirm that their work conforms to relevant industry-standard security and audit protocols. Consider seeking governance, risk, and compliance services from a single vendor that can help you evaluate your existing security practices in the context of your requirements and future objectives, including technical and business considerations, in addition to compliance. An MSSP with comprehensive services that will help you meet compliance will include capabilities for not only regulatory and standards compliance, but related functions such as security risk management, security program design and management, privacy, and security education and training.

7) Broad security infrastructure expertise

Check the provider's understanding, experience, and reputation in terms of providing the infrastructure and system integration that can support your managed security objectives. Ensure that the MSSP has extensive infrastructure expertise that includes hardware, software, and everything in the data center and across the network, and particularly as it relates to security best practices. MSSPs that offer integrated technology services such as business continuity, integrated communications, and storage and data services can extend the value of its managed security service offering. The MSSP should have the skills to allow you to grow beyond your managed security services implementation and expand into adjacent areas.

8) Multivendor support of security devices

In addition to managing and monitoring your security posture on a 24/7 basis, your MSSP must have the capability and necessary certification to protect your current equipment. Ensure that the MSSP can manage whatever equipment you are currently using, to avoid unnecessary changes and costs to implement new technologies. Look for an MSSP that has extensive experience in managing several technologies and platforms, in addition to their own suite of products. Ask for a list of platforms that the MSSP is certified to manage. If your current platform doesn't appear on the list, check with the provider to see if they can customize their services to suit your needs. However, beware of providers who insist they can support any IT environment and business needs, given the time and costs involved in ramping up a global set of resources to deliver expert, consistent, and reliable services.

9) Flexible, guaranteed performance-based service-level agreements

Any service provider can claim they respond rapidly and thoroughly. However, the MSSP you choose should offer more than just a rapid response guarantee, but also a guarantee of protection against emerging Internet threats. The provider must be willing to stand behind these commitments in the service-level agreement (SLA). Look for structured fixed-price, fixed-scope offerings that demonstrate the provider's ability to deliver services reliably and repeatedly. Also important, be sure the SLA they're offering serves your particular needs. After adopting the security service, validate and test the provider's capabilities and ensure performance against contracted agreements.

10) Financial stability

One of the most important criteria to consider when evaluating MSSPs is their financial stability. Managing security on an outsourced basis for large numbers of customers requires significant capital and resource outlays to operate a global network of security operations centers, develop new technologies, and attract and retain knowledgeable and motivated personnel. As with any business decision, look for selecting an MSSP that is financially stable, with deep resources and a sustainable business model.

IBM Managed Security Services

Many discerning organizations that take the time to thoroughly investigate MSSPs choose IBM Managed Security Services to protect their enterprises. In fact, IBM is recognized in the industry as a managed security services leader, receiving Frost & Sullivan's "2010 North American Managed Security Service Providers Market Leadership Award" for its ability to enhance and maintain the most market share among MSSPs.[1]

In a 2010 report on managed security services, independent research firm Forrester Research, Inc. concluded, "IBM has the broadest suite of MSS of all the providers assessed in this *Forrester Wave*."[2] Forrester also noted, "In addition to having the broadest set of services, IBM also leads in overall market share (by approximately 10 percent) and global reach (it operates in more than 150 countries)."

IBM Managed Security Services deliver advanced security solutions for real-time security management, including system and identity monitoring and management, emergency response, and 24/7/365 protection from the Internet's most critical threats. IBM's portfolio of security services help organizations minimize risk, reduce escalating security costs, reduce complexity, and demonstrate compliance. The broad portfolio of IBM Managed Security Services includes security device management and monitoring as well as Cloud Security Service offerings.

Security Device Management and Monitoring

IBM security device management services provide 24/7/365 monitoring and management of security technologies housed in an organization's IT environment. Through a single management console, companies can view the entire security infrastructure and remain actively involved with their information security programs in collaboration with IBM. IBM Security Device Management services include:

- ***Managed and monitored firewall service***—Providing real-time, 24/7 management of firewalls, this service delivers customized protection for less than the cost of many traditional solutions. It provides preemptive protection from known and emerging security threats, and multivendor support that helps maximize existing security investments. Companies stay informed with comprehensive and customizable reports, with executive and technical reporting options.
- ***Managed identity services***—This service-level-based identity lifecycle management solution helps protect information from unauthorized users by providing service authorizations only to individuals with a valid business need and removing such authorizations when access is no longer required. The solution features best practice identity lifecycle processes and preconfigured technology based on IBM Tivoli Identity Manager.
- ***Managed intrusion prevention and detection service***—A multivendor offering providing comprehensive protection for the network and servers, this service helps block threats and unauthorized access from internal and external sources. It provides expert, proactive intrusion detection, intrusion prevention, and incident response capabilities, along with real-time response and escalation of unauthorized activities that have the potential to threaten the business.
- ***Managed protection services***—These services help deliver expert monitoring, management, and incident escalation for the IT infrastructure 24/7/365. Managed Protection Services represent the most comprehensive managed security solution from IBM, and include IBM's unique protection guarantee service level agreements.
- ***Managed security services for unified threat management***—A comprehensive security solution designed to work ahead of the threat, this service provides 24/7/365 monitoring and support for unified threat management appliances from a variety of vendors, along with change management services and security policy design.
- ***Secure web gateway management***—This service is designed to provide around-the-clock management and monitoring for secure web gateway appliances, helping to deliver comprehensive web content control and protection.

Cloud Security Services

IBM Cloud Security Services leverage the power of the IBM Virtual Security Operations Center platform to deliver high-value services that require little or no security device investment or maintenance, making the total cost of ownership much lower than companies incur performing these security services in house. The cloud-based security services offerings from IBM are complemented by a comprehensive portfolio of traditional managed security and professional services solutions. Cloud-based security services from IBM Managed Security Services include:

- ***Hosted email security service***—This service is designed to act as a client's first line of defense by scanning email and eliminating threats before they reach the network. The solution is fully hosted by IBM and requires no hardware or software installation at client sites.
- ***Hosted web security service***—Designed to help clients protect their data from unintentional exposure resulting from malware, identity theft, and phishing scams, this service protects IT infrastructure and business continuity by virtually eliminating performance degradation and system crashes. It also reduces the need for additional hardware and software solutions. The service can help improve employee productivity by protecting desktop performance, helping prevent access to inappropriate websites, and helping clients streamline web security configuration and administration through a web interface.
- ***Security event and log management service***—This service enables IT teams to compile the event and log files from network applications and operating systems, as well as security technologies, into one seamless platform. It offers the ability to run queries on all of these logs using a single interface. This innovation dramatically improves the speed of conducting security investigations. In addition, IBM can archive forensically sound data, admissible as evidence in a court of law, for a period of up to seven years.
- ***Vulnerability management service***—Providing cloud-based internal and external infrastructure scanning through a single portal, this service streamlines compliance management requirements. It supports compliance initiatives by scanning for and classifying vulnerabilities, and provides the data and remediation steps for managing security risks and reducing threat exposure.
- ***X-Force threat analysis***—Delivering customized information about a wide array of threats that could affect network security, this security intelligence service helps companies proactively protect their networks with detailed analyses of global online threat conditions.

Why IBM Managed Security Services?

IBM has a long history as a trusted security expert for organizations and government organizations worldwide. IBM Managed Security Services—helping to set the standard for accountability,

reliability, and protection in managed security services since 1995—deliver the expertise, tools, and infrastructure companies need to secure their information assets from Internet attacks, often at a fraction of the cost of in-house security resources.

Industry-leading security expertise

At the core of IBM Managed Security Services, the IBM X-Force® research and development team provides the foundation for the proactive approach to Internet security that customers have grown to expect from IBM. In fact, the X-Force team is one of the best-known commercial security research groups in the world. In addition, the X-Force team serves as trusted security advisor to the U.S. Department of Homeland Security as well as many other federal, state, and local government organizations, helping create governmental security standards and initiatives.

The X-Force team is comprised of more than 15,000 researchers, developers, analysts, and experts on security initiatives, is responsible for 3,000 security and risk management patents, and has over 40 years of proven security success. This group of security experts researches and evaluates vulnerabilities and security issues, develops assessment and countermeasure technology for IBM products, and educates the public about emerging Internet threats through threat reports produced throughout the year, as well as critical alerts and advisories. The IBM X-Force team maintains the world's most comprehensive threats and vulnerabilities database—the result of tens of thousands of hours of research by the team, with much of the data used to power the preemptive protection delivered by IBM products.

IBM security analysts and experts are located in nine global security operations centers (SOCs), where they analyze more than nine billion security events daily. (See Figure 1)

Figure 1. IBM Security Operations Centers.

Innovative security technologies

IBM Managed Security Services, in addition to depending on SOC security experts, is supported and enabled by the IBM Virtual SOC, a secure web-based management tool. Leveraging the combined capabilities and intelligence of the global SOCs, the Virtual SOC provides a single interface (shown in Figure 2) for company security managers to easily monitor the security of the overall infrastructure of managed and unmanaged security devices. The Virtual SOC portal combines X-Force security research with service-level data from devices across company networks, helping IT teams manage vulnerabilities discovered in their systems.

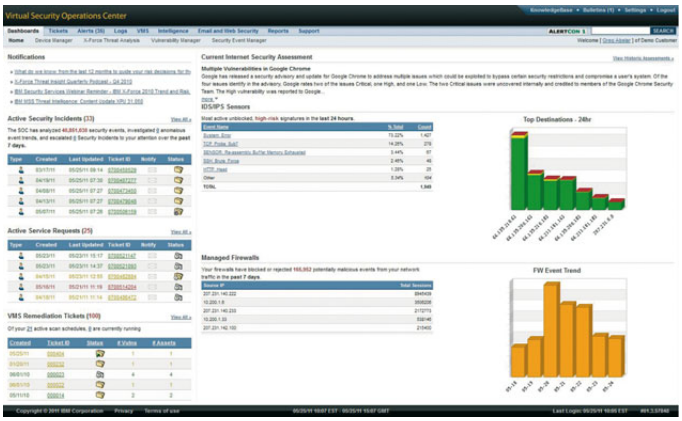

Figure 2: IBM Virtual Security Operations Center (SOC) portal.

IBM Managed Security Services clients use the Virtual SOC portal as their single command and control center for all of their IBM Cloud Security Services as well as security device management services. The secure web-based portal offers the intelligence, tools, and capabilities necessary to make real-time decisions to improve the security posture. Available anytime, anywhere, the Virtual SOC portal enables collaboration between organizations and their team of IBM security experts.

The IBM X-Force Protection System is the highly sophisticated backend system that delivers the ongoing security intelligence available through the Virtual SOC. IBM has invested more than $400 million over the last 10 years in the development of the Virtual SOC X-Force Protection System.

The X-Force Protection System sifts through the billions of security events and logs clients contend with on a daily basis to discover those that require additional attention or action. The system aggregates security information from multiple data sets, regardless of device type, vendor, or whether it is managed by IBM or in house. The system then normalizes that information, correlates it with other related data sets, and archives the raw data in a forensically sound manner for future compliance and security investigations. Further, it escalates priority events to alert an IBM security analyst or client to take action, and offers individualized remediation advice and capabilities such as ticketing and integrated workflow.

By giving clients a single management and operational view of their entire security infrastructure—regardless of vendor or device type—the X-Force Protection System allows organizations to more efficiently manage their security operations. The system is particularly beneficial for those clients dealing with multiple sites, such as multinational corporations or even those with branch offices or off-site data centers.

The benefits of choosing IBM Managed Security Services

IBM Managed Security Services enable companies to reduce the need for in-house security resources by outsourcing security operations or supplementing existing security teams. By choosing IBM to provide Cloud Security Services and security device management services, organizations can enhance their security posture while reducing costs. IBM offers the expertise to manage the complexity of the security landscape, provides the industry expertise needed to evaluate security risk posture, and delivers innovation through secure, end-to-end security solutions. IBM Managed Security Services enable organizations to:

- **Improve the security posture**—Ongoing insight into emerging Internet threats and remediation recommendations offers enhanced protection, ensures business continuity, helps unify policy management, and protects the company image. The IBM X-Force team delivers deep, continuous security intelligence. The IBM Virtual SOC portal offers the needed visibility, control, and automation, enabling proactive, real-time security management.
- **Reduce costs**—IBM Managed Security Services and the Virtual SOC can significantly reduce escalating security management costs. IBM lowers the total cost of ownership by saving up to 55 percent on information security management costs, allowing companies to reallocate resources to other business objectives. Companies can eliminate the cost of hiring and training additional resources to ensure proper network protection. Additional cost savings result from reduced downtime, infrastructure optimization, improved productivity, and preventing the loss of revenue that would result from security breaches and data loss.
- **Simplify management**—The IBM Virtual SOC offers a robust mechanism for end-to-end security management for IBM and other security solutions, as well as all domains of risk. IBM helps increase operational efficiencies by eliminating manual audit tasks, and reducing the number and complexity of required security controls. IBM security services also reduce redundant security expenses. Companies can consolidate multivendor environments for easier management, while efficiently managing global operational footprints.
- **Protect service investments**—Companies that choose IBM Managed Security Services benefit from guaranteed performance-based SLAs ensuring 100-percent accountable, reliable protection. Standardized, repeatable, predefined services and asset-based delivery, based on industry-recognized best practices, help optimize service investments. Additional protection results from simplified contracts, predictable pricing, and receiving a broad range of flexible services from one IT service provider.

- **Protect existing IT investments**—IBM Managed Security Services are based on a vendor-neutral approach to security management, supporting a variety of device types from many vendors such as IBM, CheckPoint, Cisco, Juniper, Symantec, McAfee, TrendMicro, 3com, and others. Integrated services delivery allows for the seamless integration of disparate security technologies, and together with built-in security intelligence, allows for improved decision-making and maximization of infrastructure investments. Enhanced security management helps organizations extend the value of security infrastructure investments by optimizing their performance.
- **Achieve and maintain compliance**—Through ongoing security monitoring and documented security policies and procedures, IBM Managed Security Services help companies maintain compliance with government and industry regulations. IBM holds certifications for some of the industry's most complex compliance regulations, with the expertise to assist companies in implementing internal and regulatory controls for SOX, PCI, GLBA, HIPAA, and other compliance mandates. IBM enables integrated delivery of security technologies required by many regulations, such as firewalls, intrusion protection systems, vulnerability management, and security event and log management.

IBM: Delivering confidence, simplicity, and value

Outsourcing security enables organizations to improve their security stature, lower operational costs, and focus key IT personnel on core business functions. Central to the success of a security outsourcing decision is choosing the right provider. Organizations should seek a provider with a history of reliable service and financial stability, along with bulletproof SLAs with guaranteed protection. A redundant global network of security operations centers staffed by experienced security experts and a comprehensive, continually evolving set of services will protect security investments and the enterprise.

With IBM Managed Security Services, companies benefit from improved operational, financial, and strategic efficiencies across the enterprise, and most importantly can advance their security management practices. As Forrester recognizes, "Security organizations that require global reach, a broad suite of security services, and good threat intelligence should look to IBM to deliver these services."[2]

Companies that choose IBM quickly gain *confidence* by working in collaboration with the world-class IBM X-Force security team. They also appreciate the *simplicity* offered by the IBM Managed Security Services Virtual SOC portal. Just as important, IBM's nine global security operations centers deliver consistent, premium levels of managed security services, offering maximum *value* for companies counting on IBM to support their risk management objectives.

For more information

To learn more about the IBM Managed Security Services please contact your IBM marketing representative or IBM Business Partner, or visit the following website: **ibm.com**/services/us/iss

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: **ibm.com**/financing

IBM
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
May 2011

[1] *Frost & Sullivan North American Managed Security Services Providers Market*, May 2010.

[2] *The Forrester Wave: Managed Security Services, Q3 2010*, Khalid Kark, for Security & Risk Professionals, August 4, 2010.

Please Recycle

SEW03026-USEN-00