Eight important criteria for selecting a managed security services provider

What you need to know to evaluate the marketplace

IBM

Introduction

Enterprises today continually struggle to defend against online attacks that can strike at any moment. Whether the threats are from viruses, denial-of-service attacks or unauthorized website access, these offenses can wreak tremendous havoc. Attacks can impact business operations and workforce productivity, damage infrastructures and create security breaches that can harm an organization's reputation. Such compromises or breaches can also be expensive in terms of operational impact, resources required to remedy the issue and potential loss of business.

A successful security program demands sophisticated, up-to-the-minute intelligence and 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 that exist, organizations that try to manage their own information security often lack the in-house resources required to adequately protect online systems around the clock.

In addition, implementing and managing security solutions can divert IT resources from other critical initiatives, including preventing the next attack. IT teams are forced into a reactive posture that ignores the more important strategic role of an IT security function.

To support a cost-effective, robust and proactive security posture, more and more organizations are outsourcing portions—or even all—of their IT security programs. These businesses typically:

- Lack the in-house capabilities required to properly manage changing business demands, compliance mandates and emerging threats for strategic implementation of new IT security solutions
- Do not have the capabilities to effectively monitor and manage the security infrastructure to help achieve optimal use of current assets
- Have in-house IT staff members who 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 a proactive, approach to mitigating risk and reducing data loss and downtime
- Lack the resources and expertise to gather and analyze security intelligence about current and emerging threats
- Are too overwhelmed by the magnitude and complexity of risks to confidently provide an integrated response.
- Need visibility into what the future holds in order to prepare for potential risk down the road

By outsourcing security operations to a managed security services provider (MSSP), organizations can take advantage of the expert skills, tools and processes that these service providers offer and significantly enhance security without making a large investment in technology and resources. But how do you select the right MSSP for your specific needs?

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

The eight most important things to consider in selecting an MSSP

Organizations that lack the resources and budget to build and operate their security infrastructure on an around-the-clock 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 helping your business to remain functional even when sophisticated threats continue to proliferate.

"The right MSSP can reduce the cost and complexity of information security while helping you build a stronger security posture."

To achieve the greatest advantage from outsourcing your security operations to an MSSP, you need to select a provider suited to your organization's specific needs. Before you do this, however, ask yourself the following questions:

- Have you conducted an extensive evaluation of your security requirements?
- Do you understand the security measures with which you must comply?
- Have you established a reliable governance model?
- Have you determined which security requirements you expect the MSSP to put in place?

Once you have addressed these questions, you are ready to begin evaluating MSSPs. The following eight criteria can help you select the right provider to protect your vital IT assets while better managing your compliance.

1. Broad portfolio of security services
As a result of the dynamic nature of your business environment, the influx of new threats and the changes in regulatory requirements, your security needs are continually evolving. Your managed security services partner should offer a robust suite of services that can help keep you protected ahead of threats, regardless of your security challenges and compliance requirements. 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 for more 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 can help you reduce costs, improve service and manage risk.

2. Sophisticated back-end technology
Once you are certain that an MSSP is committed to ongoing global security intelligence, make sure it has the back-end 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. It should also have the capability to handle vast amounts of unstructured data and go beyond the normal limits of IT security to perform advanced analysis to determine not just what happened, but who made it happen and why. Additionally, security intelligence should be integrated, enabling alerts from multiple service offerings to be chained together. This helps reduce the rate of false positives and streamline the identification of advanced threats, whether the threats target just your organization or a wide range of organizations.

Look for technology with incident escalation and remediation, as well as a sophisticated alert mechanism—all tied to an enormous database of known threats provided by and continually updated by the MSSP. Make sure that your provider is using 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.

3. Highly respected security intelligence and research professionals
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-date information on emerging threats and remediation. Global operations groups, strong research and development teams, and time-tested vulnerability and threat analysis processes are crucial to keeping your company protected from evolving attack schemes and technologies. In addition, the provider should be able to dedicate research resources to investigating vulnerabilities and threats, whether by assigning specific duties to each resource or by demonstrating a rotation of duties.

4. Excellent reputation
The reputation of an MSSP and its history of customer satisfaction are important factors to consider. Look for a provider that has successfully retained customers for several years. Review analyst reports that include the MSSP, and compare the provider with its competitors for an unbiased evaluation of its services and expertise. Also, consider whether or not their solid reputation stands beside a solid vision for the future. Make sure that the provider is investing in its portfolio of solutions and services and has a clearly defined strategic roadmap that aligns with your security goals.

5. 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 overall security strategy and objectives. The MSSP should have extensive infrastructure expertise that includes in-depth knowledge of hardware, software, data center and network requirements, particularly as they relate 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 their managed security services offerings. The MSSP should have the skills and analytics capabilities to help you understand how a security-rich infrastructure can support your growth beyond your managed security services implementation and facilitate your expansion into adjacent areas.

6. Multivendor support of security devices
In addition to managing and monitoring your security posture around the clock, your MSSP must have the capability and certification to protect your current equipment so you can avoid unnecessary and costly technology changes. Look for an MSSP that has extensive experience in managing a variety of technologies and platforms, in addition to its own suite of products. Ask for a list of platforms that the MSSP is certified to manage. If your current platform does not appear on the list, check with the provider to see if services can be customized to suit your needs. However, beware of providers who insist they can support any IT environment and business need, because the time and cost involved in ramping up a global set of resources to deliver expert, consistent and reliable services can be substantial.

7. Robust, web-based management tool to improve visibility and intelligence
Although the MSSP can deliver a portion or all of your IT security program, your IT team nevertheless needs ready access to a robust 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 that can meet your individual business needs. The best web-based management tools will allow your security resources to more easily monitor both managed and unmanaged security devices via the cloud and traditional approaches.

8. 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 an MSSP with deep resources and a sustainable business model.

IBM Security Services

IBM® Managed Security Services deliver advanced security solutions for near-real-time security management, including system and identity monitoring and management, emergency response and around-the-clock protection from the Internet's most critical threats. IBM's portfolio of security services helps organizations reduce risk, escalating security costs and complexity, while better managing compliance. The broad portfolio of IBM Managed Security Services solutions includes standard security management and monitoring as well as cloud-based security service offerings.

Managed Security Services (core offerings)

IBM Managed Security Services solutions combine industry-leading tools, facilities, expertise and industry-leading capabilities to help secure your information assets around the clock, often at a fraction of the cost of in-house security resources. Offerings include:

- ***Firewall management.*** Providing near-real-time security monitoring, management and analysis of firewall alerts and logs, this service delivers customized protection for less than the cost of many traditional solutions. It helps provide preemptive protection from known and emerging security threats, as well as vendor-neutral support that can help optimize your existing security investments. IBM's firewall management service keeps you informed with robust and customizable reports, along with executive and technical reporting options.
- ***Intrusion detection and prevention system (IDPS) management.*** This service is designed to improve your security posture by managing the intrusion detection and prevention devices that are being used to protect your networks and servers from internal and external threats and intrusions. Additionally, it delivers advanced attack detection by taking a multistep approach to event analysis and attack recognition. This service also provides configuration and customizable reporting, as well as increased visibility into your security events. Our solution combines around-the-clock threat monitoring and advanced policy management capabilities to help improve your security posture. In addition to supporting virtual private networks, our service also supports a wide range of IDPS devices.
- ***Server and workload protection.*** Using advanced security tools and technologies, this service offers around-the-clock monitoring, management and incident escalation to help protect your servers and workloads.

- ***Unified threat management.*** This service comprises two discreet security technologies—protection and content—which correspond to the capabilities available from market-leading unified threat management appliances. The protection component supports and manages intrusion prevention systems and firewalls designed to block traditional attacks like worms, Trojans and intruders. The content component provides management and support for web and email filtering and antispam and antivirus technology (where available).
- ***Secure web gateway management.*** Along with ongoing support to help protect critical web-based transactions, this service provides access to a web-based portal designed to optimize your security devices and give you an overall view of your security status. The service supports proxy or cache, content filtering, directory services and application control. In addition, it combines ongoing threat monitoring with advanced policy management capabilities to help improve your security posture.

"We help you better identify and respond to threats, manage compliance and optimize your infrastructure investment."

- ***Security intelligence analyst.*** With this service, you get a dedicated security specialist who works with you to analyze your current security posture, review trends in your environment and provide policy tuning and strategic recommendations to strengthen your overall security posture.
- ***Managed security information and event management (SIEM).*** This service provides around-the-clock security monitoring and reporting of activities across the enterprise and for specific users. We help you better identify and respond to threats, manage compliance and optimize your infrastructure investment. Our services, which can be delivered at a predictable monthly cost, support multivendor SIEM systems and can add value to your existing implementations.

Cloud security services

IBM Cloud Security Managed Services bring together integrated security technologies, global threat intelligence, vulnerability research—along with seasoned security professionals—to help separate "usual" or expected events from "unusual" attacks and incidents and deliver a more robust security solution for your cloud environment. Cloud-based security services from IBM Managed Security Services include:

- ***Hosted email and web security.*** Designed to help clients protect their email and data from unintentional exposure resulting from malware, identity theft and phishing scams, this service can protect 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.
- ***Managed web defense.*** This service offers a multi-layered approach to helping you plan for and respond to a DDoS attack and correlate data while it's happening. By combining IBM security expertise with cloud-based Kona Site Defender technology from Akamai, it can help you avoid potential attacks on your infrastructure and facilitate sustained performance and availability.
- ***Hosted 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.
- ***Intelligent log management.*** This cloud-based service is designed to provide around-the-clock monitoring that can help protect against threats and support your efforts to better manage compliance with those regulations requiring log monitoring for hybrid IT environments.
- ***IBM QRadar® Security Intelligence Platform.*** Next-generation architecture supports as-you-like-it security services with robust scalability and versatility—driven by IBM's global security team members and extensive threat intelligence. The platform provides security intelligence on a global scale and helps ensure support for a broad range of IT environments, in virtually any combination.
- ***Security use case library.*** A subscription-based access to a large repository of security use cases, rules and related implementation guidance.

What makes it work

There are several key elements that allow IBM Managed Security Services to provide you with the resources you need to help improve and advance your security management practices. These include:

- ***Best-in-class technology.*** We equip our analysts with the latest tools, including Watson for Cyber Security, which is currently incorporating 20 years of security research from IBM's comprehensive IBM X-Force® library to form a central part of its knowledge core. And as new information is published, Watson for Cyber Security will adapt that knowledge, providing new insights and patterns locked away in that information. Utilizing fully integrated, best-in-class technology lets IBM both produce answers and provide evidence-based reasoning and recommendations for improved decision making in real time. That means we can accelerate potential security strategies and help you reduce the cost and complexity of dealing with cyber security challenges.
- ***A 24x7 watch floor.*** With around-the-clock coverage, we can monitor and assess threats that are specifically relevant to your organization, so you can quickly and efficiently mitigate vulnerabilities and strengthen your cyber security posture.
- ***Continuous monitoring.*** Collaboration between our security experts and clients allows us to rapidly deploy efficient detection methods and take advantage of intelligence data to identify future attack indicators.
- ***Advanced intelligence.*** Our global facilities are capable of processing more than a trillion security events. In addition, the more than 35 billion events we typically see and analyze daily allow us to develop some 200,000 new pieces of threat intelligence each day, leveraging insights from the analysis of over 100 million web pages and images plus data collected from the 270 million endpoints we monitor. And that's in addition to the expansive library of threat research provided by the IBM X-Force threat intelligence team.

IBM X-Force Command Centers offer best-in-class security technology, tactics and expertise

IBM Security can help you prepare for and respond to today's most advanced threats with IBM X-Force Command Centers. With global expertise, advanced analytics tools and cyber simulation capabilities, IBM provides the industry's leading 24x7 security operation centers around the world.

Why IBM

When you team with IBM, you gain access to a security team of 8,000 people supporting more than 12,000 customers in 133 countries. As a proven leader in enterprise security, we hold more than 3,500 security patents. Our goal is to help companies like yours continue to innovate while reducing risk. That means you can continue to grow your business, while securing your most critical data and processes.

For more information

To learn more about the IBM Managed Security Services, please contact your IBM representative or IBM Business Partner, or visit the following website:.
ibm.com/security/services/managed-security-services

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2017

Please Recycle

SEW03026-USEN-04