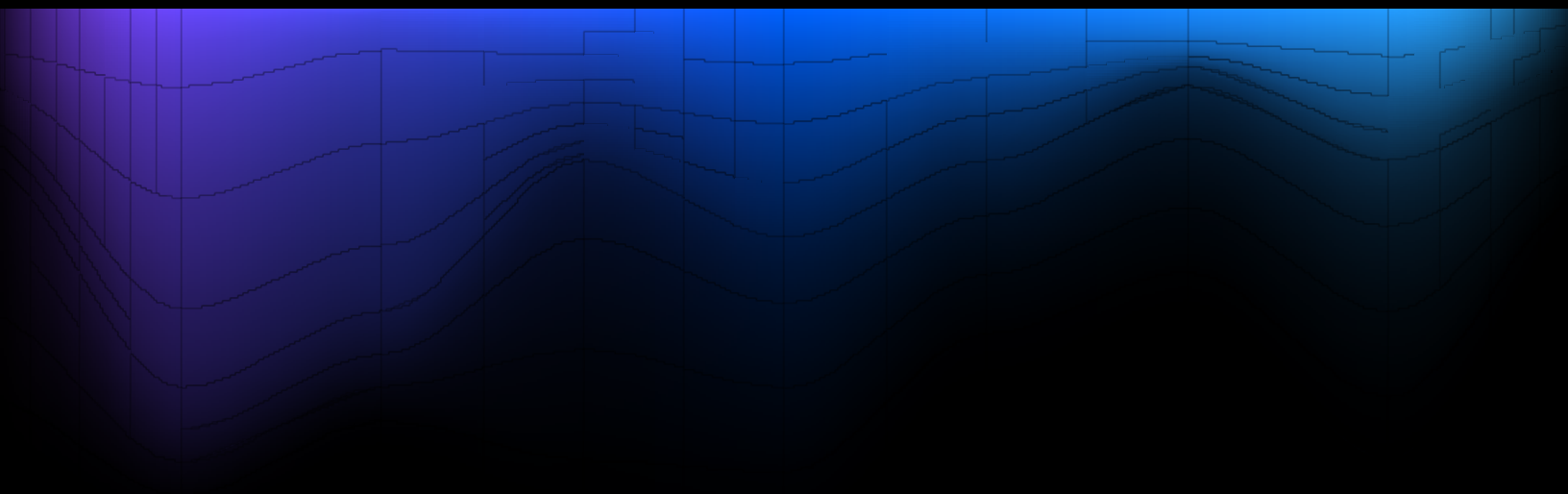
Buyers guide

Globally managed security services providers: A comparison

Does your vendor meet these eight criteria? What managed security services provider (MSSP) is your best choice? Evaluate your options with these questions.



IBM Security

IBM

Eight questions to consider for your MSSP vendor

To compete in the global economy, organizations must innovate quickly and operate efficiently. Cybersecurity tools and services are instrumental to advancing your business. An MSSP should provide expertise and leading technology and be able to justify the investment to your business leaders, stakeholders and customers. The MSSP should address the risk and compliance demands of chief regulatory officers and chief compliance officers and the security goals of chief information officers (CIOs) and chief information security officers (CISOs). When addressing these concerns and selecting a vendor, review the following eight questions and answers about available services that can apply to your operations.

1.

What meaningful metrics does the MSSP vendor offer that directly relate to your risk-based security strategy?

No analysis—it's security event monitoring only.
(1 point)

Incomplete solution
This MSSP vendor can tell you what security exposures exist for your enterprise. Beyond that information, the vendor provides no recommendations for you on the likelihood and impact of these and future risks.

Analysis occurs, but the customer must prioritize security events and determine policy enforcement and actions to be taken.
(2 points)

Knowledge lacking power
You'll get a better assessment of potential threats from your data as they develop. Still, the vendor won't offer recommendations to you to resolve your security events.

Customers get proactive prevention methods and responses to manage threats with the bottom line in mind.
(3 points)

Full service
This vendor provides you with system management that includes risks, recommendations, policies and rules. The MSSP detects, reacts to and reports threats and provides figures that reflect the costs to a business if risks are not addressed.

2.

How well does the solution integrate with your existing technology investments?

The solution is a standalone product.
(1 point)

Narrow functionality
MSSP vendors whose systems can't connect with any of your other services or best-in-class technology products hamper their offering's effectiveness. You'll have to take extra steps to install new equipment that can drain your resources prior to any security work.

You can deploy its managed security services with some of your technology.
(2 points)

Fragmentary collaboration
With these solutions, you can share services or best-in-class vendor products with the MSSP to an extent. The problem is that some incompatibilities between the vendor's products and your tools can fall on you to resolve elsewhere.

There's a tight partnership between product management, development, security operations centers and your technology.
(3 points)

Scalable and personable
The vendor designs security strategies that evolve at the same time as your enterprise undergoes digital transformation or cloud migration. Top MSSP vendors are product neutral and foster a culture of partnership designed to have their tools meet your needs.

3.

How advanced and comprehensive are the security event monitoring technology options?

Customers get only basic security event monitoring.
(1 point)

One size fits only some
A vendor with no tiers or add-ons for security protection seems unlikely to adapt to changes in your enterprise. You'll receive the same minimal customer service the MSSP uses on any other business regardless of size or scope. This MSSP has standard correlation rules independent of client environments and lack of tailored solutions.

There are a couple of options, but none offer a comprehensive solution including discovery, monitoring, recommendations and prevention of security events and threats.
(2 points)

Some items missing in action
With a provider lacking a flexible approach to offer comprehensive security monitoring and protection, leaders at your enterprise can easily find shortcomings. With no personalization, even this MSSP's top offering will fail to address some pressing and recurring security issues you may encounter.

Customers get a wide range of options, such as discovery, monitoring, analysis and protection including distributed denial of service (DDoS) protection, advanced threat intelligence (dark web monitoring) and identity and access management.
(3 points)

Extensive and expansive choices
The most thorough MSSPs provide comprehensive security management and monitoring with additional features such as threat intelligence, incident response and threat hunting. They can resolve your emergencies quickly 24/7 and have a full range of customizable services to address your risk, compliance and security needs.

4.

Does the vendor offer customized local geographical service delivery?

No such customization exists.
(1 point)

All or likely nothing
Some providers deliver the same managed security services throughout their global service zones. These vendors offer limited customization and standard services regardless of your business needs.

Local service delivery occurs in select areas.
(2 points)

Partial help available
These vendors have staff that can speak the dominant languages within a region or country. This setup can result in better engagement and higher customer satisfaction, but only to the extent of the number of nations served.

The vendor is both local in approach and global in scale.
(3 points)

A wide-ranging perspective
You want a vendor who shares an understanding of your business needs at all levels. The strongest MSSPs tailor your security solutions with considerations about the local and world cultures surrounding you. These MSSPs also understand regulatory, data and privacy requirements across the globe.

5.

Does the provider deliver a modern digital experience and put your Security Operations Center in the palm of your hand?

No mobile application is available from the provider.
(1 point)

A delay in access
CISOs or CIOs who get a security incident alert away from their offices face an unwieldy response process. Making them connect their laptops, log in to the MSSP portals and locate the case or ticket inconveniences them.

A mobile app exist, but it's slow to load, provides inadequate interactivity and visibility on results or both.
(2 points)

Uncertain availability
Time is of the essence in addressing your security threats. If a service's app hinders your ability to act quickly, lacks all necessary information to make a decision or both, you'll find its functionality fails to meet your needs.

Customers get an app available 24/7 that opens quickly with a convenient display of details.
(3 points)

Always connected to serve you
With a reliable mobile app, you can work without a laptop to respond expediently to security incidents. Get on a phone, open the app and start reviewing the incident's severity, criticality and context for rapid decision-making.

6.

How does the vendor respond to incidents?

Incidence response isn't part of the MSSP.
(1 point)

The burden is on you
This vendor essentially only records what security exposures you face and what damage they cause. You alone must decide how to handle an incident or engage other vendors. The only certainty will be that it will cost you additional time and resources.

The vendor offers a choice of either remote or on-site response.
(2 points)

Half an answer
You need flexibility in this area. Some complex security incidents will need remediation at your enterprises. Other events will need immediate assistance as they occur. This MSSP could be unable to respond sufficiently for your enterprise.

The vendor can respond both remote and on-site.
(3 points)

A defense ready to go
The provider is on guard for virtually any security attack on your enterprise and provides managed detection and response services. Top MSSPs with this add-on service also use system criticality scores to understand the vulnerability event's context with the aim of stopping similar incidents.

7.

Can the MSSP offer centralized policy and visibility across hybrid multicloud environments?

The vendor only offers services for on-premises environments.
(1 point)

Insufficient insights
Experts agree that the scope of security monitoring service requirements for most enterprises includes cloud-delivered services. A vendor unable to manage your security events in public or private clouds can't meet your current IT security demands.

The MSSP offers both on premises and Infrastructure as a Service (IaaS).
(2 points)

Some holes remain
You need security for Platform as a Service (PaaS) and Software as a Service (SaaS) as much as for IaaS, given their heavy usage. For example, this MSSP can't monitor and detect threats within your infrastructure or most of your apps from third-party sources.

You get coverage across hybrid multicloud environments, including IaaS, PaaS and SaaS.
(3 points)

Ready for the cloud
This MSSP has specialized skills and expertise to handle the complexity of all cloud environments. The vendor can monitor and respond to threats against cloud-native, modern applications enabled with microservices and containerization like Red Hat OpenShift, a popular open source container application platform.

8.

How much security analytics using machine learning does the vendor use to detect and prioritize events?

No machine learning occurs.
(1 point)

Falling behind the curve
Many security detection devices now use machine learning to improve efficiency in delivering service to customers. Vendors lacking this feature in their services can leave your enterprise responding to similar incidents frequently and slowly. This MSSP forwards high volume of noise and low-value information for you to process.

Machine learning occurs in limited uses.
(2 points)

Unfulfilled potential
This MSSP incorporates the process in only one or a couple of its security services. That approach can provide incomplete processing of data on security incidents, which can result in only spotty improvements of service.

Machine learning serves as a foundation for threat detection and prevention from the vendor.
(3 points)

Prepared for threat analysis
This approach provides enterprises with an automated security policy, automated alert handling and prioritization of threats. Analysis of data by devices can lead to timely fixes of vulnerabilities before they're exploited and enhance preventive actions against threats. This MSSP processes low-value alerts and noise through automation while handling high-value and high-impact alerts through analysts who have more time to focus on high-value analysis.

Tally your score

Does your MSSP vendor provide what you need?

Score: 8–15 A niche provider with inadequate capabilities

The MSSP vendor lacks many security provisions commonly expected by clients and likely can't scale to your needs. Its restricted functionality can complicate your efforts to comply with legal and industry regulations.

Score: 16–21 A niche provider that tries to adapt to enterprises

Although this vendor may have your best intentions in mind, its services have constraints that leave gaps in parts of its security offerings. There's a good chance you'll discover these missing elements and need a more thorough solution.

Score: 22–24 A trained vendor with breadth and depth of knowledge

This vendor has experience to tailor its solutions to fit your enterprise even if you're unsure what you require. You'll receive flexible security information and event management (SIEM) technology options ready to fulfill your demands as you grow globally. Top vendors empower organizations to recognize risks and pitfalls in their business plans before full implementation and serve as a trusted partner providing expertise and responsiveness, all on a global scale.

Remember these eight criteria for selecting a managed security services provider

Enterprises need to take proactive steps to defend themselves against malicious attacks. 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.

By outsourcing security operations to a 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? Remember the following eight criteria for selecting a managed security services provider:

1. Extensive vulnerability analysis connected to strategy
2. Multivendor support and product neutral
3. Advanced security event monitoring options
4. Local delivery and global scale
5. Mobile app
6. Incidence response service
7. Cloud security
8. Machine learning and automation

Take the next step

IBM® Managed Security Services fulfills all criteria for a top score for this criteria, delivering advanced security solutions for near-real-time security management. These solutions include 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, cost and complexity and also helps organizations better manage compliance. The portfolio of IBM Managed Security Services solutions includes on-premises security management and monitoring and cloud-based security service offerings. Additionally, IBM is in the Leader quadrant of the 2019 Gartner Magic Quadrant for Managed Security Services Worldwide, and the Forrester MSSP Wave 2018 report ranks IBM as a Leader. To learn more about IBM Managed Security Services and what it can do for you, visit **ibm.com/security/services/managed-security-services**