



# Top 10 tips for selecting an MSSP

Businesses often have trouble keeping up with today's constant barrage of cyber threats. Many are turning to **MSSPs (managed security services providers)** to help protect their networks cost-effectively and reliably. But choosing an MSSP requires thought and research. Not all offer the same levels of protection. You should focus your search on a provider with a solid track record and reputation.

## Here are 10 best practices to follow when selecting an MSSP.

**1 Getting to know you:**  
The first clue that you're talking to the right MSSP is that the provider asks about your business needs and strategic goals. A provider needs to learn your IT environment to properly help to protect it. If a provider doesn't ask enough questions about what's in place, how it's used, and which users need what levels of access, you probably should find another provider.



**2 Reputation matters:**  
Handing over IT security to a third party requires trust. Ask for references and get feedback from existing customers about the MSSP's reliability, expertise, and how responsive it is when clients need support. Find out if the MSSP has stopped any threats and, if remediation was required, how effective it was.



**3 Menu, please:**  
Security requires more than firewalls, patch updates, and antivirus. These days, you need functions such as asset discovery, vulnerability assessments, intrusion detection, log management, threat intelligence, and behavior monitoring. If an MSSP doesn't deliver these functions, it may not be able to fully protect you in a business environment where new malware threats are released every day.



**4 All covered:**  
With today's elevated threat levels, you can't take your eyes off the ball. That's why you'll want an MSSP that takes a holistic approach, preferably by implementing a Security Information and Event Management (SIEM) solution. SIEM provides virtually complete visibility into your environment. Your provider also should offer integrated threat intelligence to help accelerate detection of new threats and effective remediation.



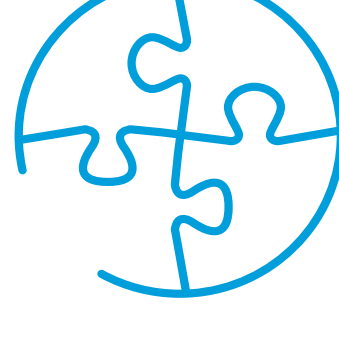
**5 Technical knowhow:**  
Some MSSPs focus on specific security areas or do little more than monitor your environment. That may not meet your needs. Be sure to check on the MSSP's levels of expertise and experience. Ask about its technical team – how much experience it has and what certifications its members hold. A well-rounded MSSP should have experts in multiple areas of IT security, and they should attend regular training to keep up with new and evolving threats.



**6 There for you:**  
It's one thing to have the best technology and a well-trained staff, but what happens when the customer needs support? An MSSP needs to be ready to respond to any inquiries you may have about their service or new threats. Considering what's at stake – your business data – you need a provider that answers your calls promptly, especially if you believe a breach is underway.



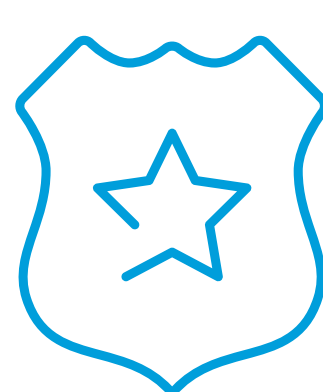
**7 Keeping it together:**  
An MSSP, like any other provider of remote and cloud-based services, functions better by using automation and being repeatable. All processes and procedures should be documented and understood. If the provider is unclear or unable to explain its services, take that as a sign it might struggle to deliver on promises.



**8 Human factor:**  
So, you've done your homework and have started working with an MSSP who is handling your data securely. But what about your users? Human action, malicious or otherwise, plays a major role in security incidents, which explains why cybercriminals rely so much on phishing to deliver malicious payloads. Find out if your MSSP offers training to teach users how to spot and avoid cyber threats and break risky practices that can result in a security incident. If your MSSP doesn't provide training, consider finding a third party that does.



**9 It's the law:**  
Aside from protecting your IT environment, your MSSP must have the tools and knowhow to help you comply with applicable privacy and security laws. The MSSP must know what laws apply to your particular business. The MSSP should also provide the ability to integrate data from legacy security tools to align with regulations.



**10 Value vs. cost:**  
When contracting with an MSSP, you'll want to know up front how much the provider charges and exactly what you're paying for. Try to get the best possible rates, but avoid basing decisions strictly on cost. Keep in mind the value of the security services, and how much it can cost a business to recover from a security incident, especially when valuable private records and business data are stolen.



CommSec helps reduce the complexity and cost of protecting your organisation from cybercrime.

### About CommSec

Founded in 2013, CommSec was established to address the growing numbers of cybercrime by offering affordable cyber security services to SMEs, NGOs, public and state funded organisations. CommSec provides managed cybersecurity services to identify, protect, prevent, detect, analyse cyber risks and threats. Using the latest leading-edge technologies, CommSec provides high-class cyber security management supported with expert analysis and action to reduce the risk that cybercrime costs.

We have partnered with the best of IT security software vendors to bring our clients proven and trusted solutions they can add to their security stacks. See a list of our security partners here.