6 Things To Look For In A Managed Security Service Provider (MSSP)

With over 300,000 new malware threats created daily, and the increasing complexity of cyber threats, businesses of all sizes are struggling to keep their IT environments safe. Inadequate security policies or poorly configured security controls could expose a company to security threats that lead to millions of dollars in damage.

For these reasons, businesses are turning to managed security service providers (MSSPs) for secure solutions to help protect their business assets and data.

An MSSP provides cybersecurity monitoring and management solutions to businesses to help them keep their networks and data safe from cybersecurity threats. Services often include managed firewalls, intrusion detection, vulnerability scanning, and antivirus protection services.

However, not all MSSPs offer the same level of protection. It's important to know what to look for when choosing a provider.

What To Look For In A Managed Security Service Provider

There are several things you need to look for when choosing an MSSP. Do they have a good reputation? Are they offering a level of service suitable to your business needs? Here are 6 things to consider when choosing your managed security service provider.

1. Do they ask about your business needs/goals?

To create the optimal security solution for your business, an MSSP needs to have a thorough understanding of the way your business works. Solutions provided should consider your business needs, strategic goals, IT environment, and any specific rules or regulations related to your business industry.

An MSSP provider should ask questions about the systems and solutions you currently have in place, how they are used, who has access to them, and the level of access of each user.

With a comprehensive view of the way your business works, an MSSP can help you create the best solution for the specific security issues you need to address in your business.

2. What is their reputation?

A certain level of trust is necessary when placing your IT security needs with a third-party provider. You want to choose a provider that has an excellent reputation and knows what they're doing.

Ask the important questions. How long have they been active in the industry? Are they reliable? What kind of track record do they have with quickly finding and fixing security issues? Find out what methods they use for remediating threat events and the success rate of those methods.

Also, ask for references, check reviews and get feedback from existing customers about their services. Granted, there is always someone with an issue but if too many people have complained about the same issue, it could be a red flag.

3. Do they take a holistic approach?

A cybersecurity solution shouldn't just focus on technology, it should also address security issues related to people, skills, processes, and governance within the business.

Everyone in the organization should understand their responsibilities related to the IT security of the company. An MSSP should be able to give you guidance on cybersecurity awareness training programs for your employees and creating security policies for device and data use.

On the technology side though, an MSSP should provide security mechanisms like SIEM to give you complete visibility of your IT environment, and to accelerate threat detection and remediation.

4. Ask what is included in their services to ensure your needs are covered.

It's important that you are clear on the services that the MSSP is offering. You don't want to be in the middle of a security event to find out that it's not covered by your MSSP.

Services provided by MSSPs can vary and not all will be suitable for your specific business needs. Some MSSPs focus solely on monitoring for intrusions while others offer comprehensive incident response solutions.

Common services include firewalls, antivirus, asset discovery, vulnerability assessments, intrusion detection, threat intelligence, and behavior monitoring. If you're in a heavily regulated industry, you'll also want to ensure that the MSSP meets any necessary compliance requirements.

Make sure that you both understand the level of service expected from the MSSP as well as your security responsibilities as a business.

5. Ask about their technical expertise & experience

If your security needs go beyond simply monitoring your IT environment for threats, confirm that the MSSP has the required technical expertise and experience to handle your needs.

Meet with the technical team to find out their level of experience. Are they certified in the latest security technologies? Does the MSSP provide regular training for technicians? Are the certifications in areas specific to your security needs?

The MSSP you choose should have experts in several IT security areas and ensure that its technicians are certified and always up to date with advanced security technologies related to new and evolving threats. Their experts should be constantly training and learning and demonstrating a high level of excellence in their work.

6. Understand cost vs. value

Make sure you know upfront how much you'll be paying for security services, exactly what's included in your package, and the payment structures offered. Some MSSPs offer services in tiers but costs can increase dramatically if you exceed your current tier. Others offer services at very low rates or one-size-fits-all solutions that may only include a limited number of services with additional services incurring extra costs.

While you'll want to get the best possible rates, try to avoid making decisions solely on cost. Remember that having strong security solutions in place could help you avoid millions of dollars in revenue lost to downtime, ransomware payments, or penalties due to breached regulations.

A good MSSP for your business will not only provide options to meet your security needs but work alongside you to create a complete security strategy that seeks to reduce costs and improve efficiency in the business.

Conclusion

At NewCloud Networks, we provide Security as a Service (SECaaS) solutions to small and medium-sized businesses. With services like our Security Information and Event Management (SIEM) solutions, we can help you maintain greater visibility of your cloud network. To find out more about our SECaaS solutions, contact us today.