7 Factors when Selecting an MSSP

From ransomware to DDoS attacks, companies are under siege. To effectively mitigate breach risk today requires enormous expertise, resources and budget. Many are turning to MSSPs (managed security services providers) to protect their networks cost-effectively and reliably. But choosing an MSSP requires thought and research. Not all offer the same levels of protection, so you should focus your search on a provider with a solid track record and reputation.

The Managed Security Services Provider Should:

1. Take time to understand your business

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 secure it. If a provider doesn't ask enough questions about what's in place, how it's used and which users need what level of access, you probably should find another provider.

2. Have a broad security portfolio

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 1 million new malware threats are released everyday.

3. Deliver 24/7 monitoring and notification

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 SIEM (Security Information and Event Management) solution. SIEM provides complete visibility into your environment. Your provider also should offer integrated threat intelligence to accelerate detection of new threats and – if ever needed – effective remediation and incident response.

4. Demonstrate expertise and experience in multiple areas of IT Security

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.

5. Possess mature processes that are documented and repeatable

An MSSP, like any other provider of remote and cloud-based services, functions better by leveraging automation and repeatable processes as much as possible. 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.

6. Be able to assess and ensure your compliance

Aside from protecting your IT environment, your MSSP must have the tools and knowhow to help you comply with all applicable privacy and security laws. The MSSP must know what laws apply to your particular business, and, from a technology standpoint, the provider should offer functionality such as asset discovery, vulnerability assessment, intrusion detection and log management. The MSSP should also provide the ability to integrate data from legacy security tools to ensure compliance.

7. Offer a predictable cost model aligned with your goals

When contracting an MSSP, you'll want to know upfront 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. In addition, be sure your MSSP shares the same goals as you and is incentivized to drive issues out of the environment.

1960 Zanker Road, Bldg. 10
San Jose, CA 95112

408.734.3339
800.969.4268

info@dataendure.com
www.dataendure.com

Strengthen Your Security Posture

It's a tremendous challenge to maintain the right security resources, tools and expertise to adequately defend corporate information systems. Gaps are inevitable, resulting in a reactive security posture that leaves your organization vulnerable. And without context on how best to defend against an attack, remediation efforts can be delayed, which amplifies the damage. Digital Defense SOCaaS helps put your security on the offensive, with dedicated expertise and technology that significantly reduces your risk.

Unified security management methodology

Reduce time-to-threat detection and accelerate incident response by combining extensive security capabilities tailored to your company's needs into a comprehensive, integrated service offering. Services include Network/Host IDS, file integrity monitoring, vulnerability assessment, and transparent log centralization and correlation.

Real-time threat monitoring and continuous security support

Without clarity on what's a viable threat and context on how best to defend against it, remediation efforts can be delayed, causing exponential damage while your infrastructure and your most valuable assets are infiltrated. During a critical event, our team of security analysts delivers actionable event information, including attack vectors, TTPs, triage and remediation stages, post-mortem analysis, and suggestions for ongoing improvement. Digital Defense SOCaaS can integrate with your existing security processes with escalation tiers and tailored incident-response workflows.

World-class specialists, best-in-class solutions

Security analysts are difficult to hire, train and retain because of their high demand. SOCaaS gives you 24/7 access to highly trained and experienced security team with the expertise to triage the flood of alerts for fast threat detection. Our enterprise-grade security platform is interoperable with your existing technology environment — for a fraction of what it would cost to build and maintain yourself.

Flexible design and deployment options

Our flexible deployment options are ideal for organizations that are only interested in meeting specific compliance goals, such as log retention or compliance-based reporting for their industry, e.g., ISO, SOX, PCI-DSS, HIPAA and GDPR.

Latest global threat intelligence

As DataEndure sees shifts in the global threat paradigm, we relay this information and update customers with proactive recommendations on how best to actively defend against new attack trends cybercriminals are using.

YOUR SECURITY ADVOCATE

With DataEndure's Digital Defense SOCaaS, your company has a dedicated security advocate, so you can focus more on running, not defending your company.

Learn how DataEndure can help protect your company and simplify compliance.
Contact us: sales@dataendure.com or 800-969-4268

DataEndure helps companies build digital resilience so that their critical information assets are protected and available to the right people, at the right time. We take a holistic approach in architecting and delivering a data management and protection strategy designed to simplify enterprise environments and accomplish specific customer goals.