



Why Your Mid-market Company Needs an MSSP



Why Your Mid-market Company Needs an MSSP

Keeping your business secure from cyber threats keeps getting more complicated. Even companies that previously thought they weren't targets due to their size or industry know they need to adjust their thinking — cybersecurity vigilance is today's reality.

Mid-market companies that need to update their security controls are particularly at risk. Cybercriminals know these companies lack the internal resources and expertise to maintain in-house security teams and are still struggling to secure the digital transformations they made during the pandemic.

Furthermore, if a company has a hybrid infrastructure, multiple locations, or people working from multiple locations but no centralized security management, it's exposed. And companies in regulated industries that aren't fully adhering to the latest requirements are inviting potentially catastrophic cyber loss.

What's a hacker's best-case scenario? Decision paralysis. The longer a company takes to secure its environment and processes, the more vulnerable it becomes.

Outsourced MSSP services are the fastest and most effective way for mid-market companies to get up to speed with cybersecurity and stay there.



What's the difference between an MSP and an MSSP?

The additional “S” in MSSP makes a big difference — MSPs focus on managing IT, while MSSPs focus on managing IT security. Here’s an overview of what each service typically provides:

MSP	MSSP
Goal: Meet business operation objectives	Goal: Meet modern security and compliance objectives
Manages and maintains infrastructure, systems, and applications, including cloud	Provides proactive and reactive cybersecurity services to protect a client's digital assets
Handles tasks like network monitoring, data backup, software updates, help desk support, and general IT management	Focuses on security monitoring, threat detection, incident response, vulnerability management, security consulting, and other proactive security services
Provides basic security measures, such as antivirus software or firewall management	Provides specialized expertise, including threat intelligence, ethical hacking, advanced security analytics
Has broad knowledge across various IT domains and has certifications in areas such as networking, cloud computing, or systems administration	Offers in-depth knowledge of security compliance frameworks and helps clients adhere to industry-specific standards and implement appropriate security controls
Manages a defined set of services that covers a specific inventory of assets	Manages vulnerabilities and event activities that cover a specific inventory of assets

Every MSSP has a dedicated Security Operations Center (SOC) that's the hub of all the action — it's the dark room where experts constantly monitor networks, systems, and applications to look for anomalies and security incidents.

But monitoring events is just a fraction of an MSSP's service. Security experts need to know how to track and manage vulnerabilities, interpret what they see, and act on them effectively.

“Incident response” activities involve investigating, containing, and remediating security incidents — it requires high-level expertise, as do the other activities listed in the table above. And proactivity is as vital as reactivity. MSSPs help companies prevent attacks from happening in the first place.

More sophisticated MSPs can identify some threats while they’re managing IT environments, but they need to call in security experts to handle incident response.

What is it like to work with an MSSP?

Your MSSP operates as a business partner. It follows standards, coordinates with your internal IT team and/or MSP, and takes responsibility for securing your digital assets according to your requirements.

The engagement typically starts with an assessment and gap analysis. The MSSP needs to understand your existing infrastructure to get a baseline for your security roadmap. The first step in executing your roadmap is integrating the MSSP's services and technologies with your existing systems — this could involve configuring monitoring agents, setting up secure connections, and ensuring compatibility between different platforms.

Training and knowledge transfer begin after the MSSP customizes and fine-tunes the integration. Your internal team and/or MSP must understand the services, processes, and tools the MSSP is using for the most effective collaboration.

The communication and coordination established during the MSSP onboarding process set the stage for a smooth transition and a successful long-term partnership


What kind of return on investment can you expect?

Companies that partner with an MSSP report think it's a wise investment.

Research shows MSSPs provide faster response times and more effective threat detection when compared to internal security management teams. Companies are also better positioned to stay ahead of emerging threats when they act on their MSSP's recommendations, which are included in regular reports on incidents, threat intelligence, and your overall security posture.

Scaling is also efficient and cost-effective. Companies can stay secure as they scale without making significant additional investments in their security function.

Your MSSP operates as a business partner. It follows standards, coordinates with your internal IT team and/or MSP, and takes responsibility for securing your digital assets according to your requirements.



You can expect MSSP services to be more expensive than MSP services. They require higher levels of expertise, sophisticated technologies, and dedicated resources. Costs vary, depending on the level and scope of the security services you want, infrastructure complexity, customization requirements, and your company's risk profile. Generally speaking, you can expect to spend about 30% of your IT budget on IT security-related expenses for a company using an MSSP.

Companies that offer both MSP and MSSP services provide a holistic approach that's the best value.


What's the best way to choose between two MSSPs?

There can be significant differences between the level of service you get from one MSSP versus another. It's best not to get sidetracked by the tools they use — instead, focus on the outcomes they deliver.

To make the best decision for your unique company, consider the following for each MSSP:

- 1. Track record and client references:** Look for evidence of successful engagements, long-term client relationships, and positive feedback from existing clients. You want to assess their ability to deliver on their promises and meet your expectations.
- 2. Number of managed environments:** When an MSSP is monitoring and managing cybersecurity for a multitude of different business environments, spotting trends and anomalies is second nature. Look for a partner with hundreds of client locations under management.
- 3. Performance and outcomes:** Consider the MSSP's performance in terms of incident response, threat detection, and resolution times. Ask about their success in mitigating security incidents and minimizing the impact of breaches, and about measurable outcomes and achievements in terms of reduced security risks and improved overall security posture.

Research shows MSSPs provide faster response times and more effective threat detection when compared to internal security management teams.




4. **Proactive approach:** Look for evidence of the MSSP's ability to identify vulnerabilities, recommend preventive measures, and provide ongoing security guidance. Ask if they provide thorough incident reports with actionable recommendations and how they stay up-to-date with emerging threats and technologies.

5. **Compliance and regulatory adherence:** If you must comply with regulations, assess the MSSP's ability to achieve and maintain compliance with relevant regulations and industry standards. Ask about their experience with the specific requirements you need to meet and how they help you meet the requirements.

6. **Long-term partnership:** Evaluate the MSSP's commitment to building long-term working relationships. Do they show a willingness to understand your organization's unique needs and customize their services? Consider their ability to provide ongoing support and how their company's goals and values align with yours.

7. **Industry reputation:** Research the reputation of each MSSP you're considering. Look for accolades, certifications, or recognition they've received, and gauge their involvement in their industry by looking at any participation in associations and thought leadership initiatives. A reputable MSSP often demonstrates a commitment to excellence and professionalism.

There can be significant differences between the level of service you get from one MSSP versus another. It's best not to get sidetracked by the tools they use — instead, focus on the outcomes they deliver.



Managing your cybersecurity is part of managing your business

Partnering with an MSSP is a mid-market company's best option to operate securely in today's complex cyber threat landscape.

Trying to manage and remediate threats in-house puts you in the position of running an in-house security operation. You need to hire and train your own security personnel, acquire and optimize the advanced tools yourself, stay up-to-date on the latest threat intelligence, and so on. It's a lot for a small internal team to manage, and it will only get more challenging as technology (and threats) continue to advance.

Some companies with robust resources can do it successfully, but most understand the advantages of outsourcing to professionals that already have the experience, tools, and know-how.

MSSP services are one of three sets of services Leapfrog offers — we are a security-focused managed IT services provider that offers traditional [MSP services](#), [MSSP services](#), and a [CyberRisk Program](#) for cybersecurity beyond IT. We have found that providing a holistic approach is the best way to simplify, streamline, and secure IT for our clients. It's easier and more cost-effective for them and allows us to deliver optimal, consistent results.

If you'd like to discuss how Leapfrog's MSSP services might resolve your cybersecurity concerns, please contact Reeves Smith at 404-229-5960.

