MSSPs

THE ULTIMATE GUIDE TO MAKING THE RIGHT CHOICE

Ascend TECHNOLOGIES

CONTENTS

Finding the right people to fill cybersecurity positions in your organization is getting harder and harder.

In 2018, according to the Information Systems Audit and Control Association (ISACA), *three in five organizations* have unfilled cybersecurity or IT security positions, with 54% of companies saying it took over three months to fill those positions.

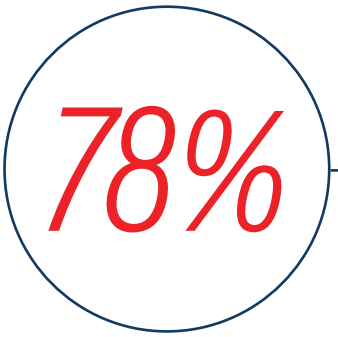
As the challenge to hire an in-house cybersecurity team continues to grow, so does the threat of a cyberattack, with *$1.1 million lost to cyberattacks every minute*.

Given this challenging landscape, what is the best way to protect your organization from these increasing cybersecurity threats and minimize costs, all while safeguarding company and customer information? Enter managed security service providers (MSSPs). MSSPs can provide an alternative to managing these challenges within your organization. But what are managed security service providers, what benefits do they offer, and how should you choose which MSSP to partner with?

WHAT IS AN MSSP?

A managed security service provider (MSSP) is a specific type of IT service provider that contracts with an organization to provide advanced security technology, backed by a team of experts. MSSPs partner with individual businesses or with managed service providers (MSP) to offer bundled security services to their customers.

MSSPs provide advanced technology and services for a variety of IT and cybersecurity challenges. Their security experts provide advanced insight into gaps in your security and help maintain updates to network systems and applications, ensuring that the correct patches and updates are made to secure the system. The services they offer can range from risk assessments, virus protection, firewalls, managed detection and response and more.



OF COMPANIES WITH SOME INTERNAL SECURITY RESOURCES STILL USE A THIRD PARTY FOR SOME OF THEIR SECURITY SERVICES

MSSP VS IN-HOUSE SOC

When considering an MSSP, it often boils down to whether security should be outsourced or managed internally with an in-house security operations center (SOC). However, in 2018, even among companies with some internal security resources, *78% of those companies still used third parties for some of their security services*.

There are many benefits that come from partnering with a managed security service provider (more on this in a minute) as well as some factors to consider if you do plan on working with an IT service provider. But as you look to weigh the options between an internal or an outsourced team, remember that there isn't a one-size-fits-all solution. Instead, there are a variety of factors that need to be considered to make the best decision for your organization.

BENEFITS OF AN MSSP

As you consider contracting security services rather than managing them all in-house (or doing nothing), it's important to note the specific ways that an MSSP can help your organization and build your security capabilities.

24/7 Security Monitoring

Working with an MSSP gives you confidence to know your organization and network are protected 24/7. Even if you have an extensive internal security team, it can be difficult to achieve 24/7 monitoring, especially when balancing that with other internal responsibilities. It can help your organization avoid costly breaches and maintain your reputation, building trust with your customers.

Best In-Class Intelligence

With an MSSP, not only do you have a security team that's intentionally monitoring and protecting your network, but, if you've chosen one wisely, you have the top intelligence in the field looking for vulnerabilities and keeping your system secure. For small businesses, that means that you have some of the best security protection, even with a smaller budget or smaller team. At the rate that cyberattacks and security breaches occur, it is risky to go without having security measures in place. A breach can be detrimental to a business of any size and affect their ability to keep the doors open.

WORKING WITH AN MSSP GIVES YOU CONFIDENCE TO KNOW YOUR ORGANIZATION AND NETWORK ARE PROTECTED 24/7

Extend Your Team

Even if you have an internal security team, partnering with an MSSP expands the knowledge and technology at your disposal. The MSSP will be able to offer advice on advanced technology to fight advancements in cyber threats or give you strategic direction as you look to improve your security in light of vulnerability assessments or penetration tests. Because they have worked with all types of companies, they've seen it all—and can share their insights with your organization.

This extends the reach and impact of your team, giving your internal IT team the consolidated information they need while allowing them to focus on other aspects of their role.

Risk Assessments and Security Testing

An MSSP can also provide you with an outside perspective on the gaps in your organization's security. Many offer everything from risk assessments to penetration tests that can give you an up-front look at where an attacker could make their way onto your network. This can be helpful information as you look to get started with an MSSP—or they can provide assessments throughout your partnership, like when there are major overhauls to your security technology or to maintain compliance.

AN MSSP CAN PROVIDE YOU WITH AN OUTSIDE PERSPECTIVE ON THE GAPS IN YOUR ORGANIZATION'S SECURITY

Lower Costs

Building a full-scale internal team and security operations center comes at a large cost. So does researching and implementing top-of-line security technology, not to mention the maintenance and updates, all while staying knowledgeable in the advances of cyberattacks.

EMPLOYEE COSTS

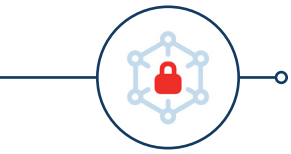
Because you don't have to maintain a fully-staffed IT security department, working with an MSSP can save hundreds of thousands of dollars per year on salaries alone, not to mention benefits, training, and other hiring costs.

STAFFING COSTS

Beyond basic employee costs, there is also the cost of staffing 24/7 to monitor alerts and respond to potential threats. This can also result in employee burnout, adding the cost of turnover and rehiring to the mix.

INFRASTRUCTURE COSTS

Rather than building a full infrastructure to support their security efforts, an organization can outsource the majority of those costs to the security provider. Working with an MSSP can reduce these costs dramatically.



BUNDLED SERVICES

Some of the top MSSPs offer bundled services, giving discounts to organizations who partner with them for a few different offerings. This gives an organization additional cost-savings for a full range of security protection.

Best Security Technology

Top MSSPs spend extensive time researching and vetting the security technology they offer to their customers. This allows you to be confident that the technology you implement will get the job done (and keep the threats out). Additionally, a managed security service provider is constantly on the lookout for more advanced solutions to offer to keep networks secure as attacks shift, new malware is created, or new tactics emerge.

Worry-Free Maintenance

Out-of-date systems, firewalls, or applications can leave the door open to potential attacks, but it can be an ongoing challenge for internal teams to manage all of the patches and updates. Working with a partner lets you rest securely, so you can know that your network is updated and maintained, keeping attackers from exploiting those holes in your system.

Compliance

No matter what the security standards or compliance regulations for your industry are, partnering with an MSSP can help you quickly move toward compliance, by identifying and addressing the gaps in your security. Qualified MSSPs will have experience handling various compliance mandates such as FFIEC, HIPAA, and PCI, which can save time and money as you look to become compliant (and stay that way). They will be able to partner with your team in conducting the proper tests, providing documentation, and finding tools to manage your security compliance in the future.

BE CONFIDENT THAT THE SECURITY EXPERTS & TECHNOLOGY YOU IMPLEMENT WILL GET THE JOB DONE AND KEEP THREATS OUT

CHOOSING AN MSSP

Not all MSSPs are created equal and as you select one to service your organization's security, it's important to do the research to find the best partner. There are a variety of factors to take into consideration.

The Security Team's Qualifications

While it's important to make note of the technology and services that an MSSP can offer, the biggest factor is the people managing and monitoring those tools. The best security experts understand the mindset of a hacker so that they can do whatever it takes to protect your network from such threats. It's best if they have experience with both the proactive and reactive sides of an attack, understanding the tools to manage threats at both stages.

The education and certifications of the team can display their qualifications, but the biggest factors are their experience and ability to stay in-the-know on the changes and advances in cybersecurity threats.

Questions to ask

- **What is the combined experience of your security team?**
- **How do the security engineers stay up-to-date on advances in cybersecurity?**
- **How do you hire or screen your security engineers?**
- **What variety of experience do your security engineers have?**
- **What are your response and resolution times?**
- **Is your support team located in the US?**
- **Are your engineers trained and certified cybersecurity engineers?**

Product and Service Offerings

Finding the right MSSP also means that they can offer the technology you need to protect your network at every point in the security lifecycle, everything from antivirus and malware protection to email security and endpoint detection & response (EDR). Their services can go further to include incident response, risk assessments, penetration tests, and even employee training services. Work with a partner that can offer the full scope of products and services you need to keep your organization secure.

Key products and services an MSSP should offer

- Real-time monitoring
- Incident response
- Risk assessments
- Penetration testing
- Next-generation antivirus
- SIEM and Log Analysis
- Managed detection and response (MDR)
- Behavioral analysis
- Auditing and reporting
- Advanced ticketing and traffic system
- Employee training and security awareness
- Strategic security direction
- Perimeter security
- Email security
- Vulnerability management

Questions to ask

- What services do you offer?
- How do you vet and select your technologies?
- What vendors do you use?
- Do you have an SOC that is monitored 24/7?

Their Policies and Standards

Review their standards, policies, and procedures carefully. This can be everything from the terms and length of a contract to the exit process if the partnership ends at some point in the future. Additionally, make sure you understand how the MSSP-client relationship is structured within a specific MSSP so that you know what the expectations are for both parties and can find the right fit for your organization. Their policies should also clearly define how they communicate with your team and handle your data. Ask questions about their communication methods when threats are detected or incidents need to be reported.

Questions to ask

- **What is the typical contract length?**
- **Are there any additional fees or costs to be aware of?**
- **What types of reports will you provide?**
- **How often will you communicate with our team?**
- **How do you secure the data in your own systems?**
- **What compliance standards do you support?**

Level of Trust

Ultimately, the decision to choose an MSSP boils down to trust—do you trust them to keep your organization safe and your network secure? Doing research and asking difficult questions can help you confidently select a partner who will give you strategic direction to proactively fight back against cyber threats.

Selecting the right partner shouldn't be an *act of faith*, but a decision based on their expertise, technology offerings, history of due diligence, and past success.

Questions to ask

- **Do you work with other companies in my industry? What success have they had?**
- **Can you provide any detailed references?**
- **What experience do you have with incident response?**
- **How long have you been in business?**
- **What makes you different from other MSSPs?**

Customization

Another benefit of partnering with a managed security service provider is their guidance as you look to find the best bundle of security tools for your organization. The best MSSPs will work with you, making recommendations on the necessary technology for the gaps in your security, based on their assessments of your network. They should be able to find the balance between offering strategic direction and incorporating your existing tools and systems.

Questions to ask

- **How do they customize their services and products specific to the organization's needs?**
- **How will the products be integrated with existing products?**

MSSP vs MDR

A common question that comes up in the process of choosing a security partner is the difference between an MSSP and a provider offering managed detection and response (MDR).

While the nature of an MSSP's offering varies based on the specific organization, managed detection and response focuses on threat hunting and detection—finding threats that have made their way past your defenses and onto your network. While some companies focus solely on providing MDR services, as the need continues to grow, many traditional MSSPs are also including managed detection and response services in order to provide a complete package for their customers—from risk assessments to antivirus protection to managed detection and response.

AS THE TACTICS USED BY ATTACKERS CONTINUE TO ADVANCE, IT'S CRITICAL TO MAKE USE OF THE ADVANCES IN DETECTION TECHNOLOGY AS WELL

As the tactics used by attackers continue to advance, it's critical to make use of the advances in detection technology as well. Endpoint detection and response is one such tool. It allows you to detect and fight back against attacks that make it past your first line of defense, giving you power to track the path of an attack as it moves throughout your network, receiving an alert when there is abnormal behavior, even from legitimate users.

This is especially significant as endpoints continue to be a organization's biggest vulnerability, due in part to the large number of endpoints on any given network and the large potential for human error when it comes to phishing attacks or other psychological tactics.

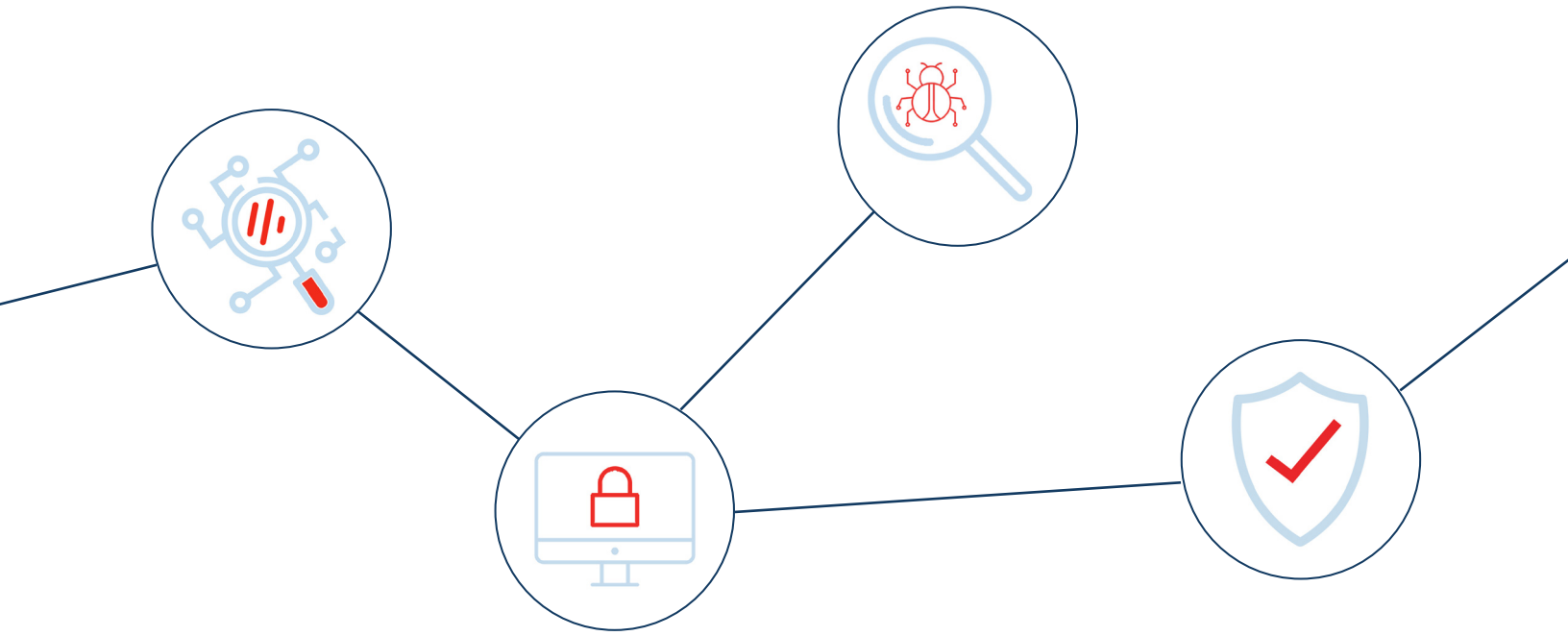
So, while there is a distinction between the technology offered by a traditional MSSP and a provider focused solely on MDR, it can be helpful to choose an MSSP that offers both the traditional IT services and newer, more advanced technology.

MSSP vs VALUE-ADDED RESELLER (VAR)

Another important distinction is between MSSPs and value-added resellers.

Value-added resellers are companies who resell hardware, software, and other technology services. They typically go beyond just selling the products and deploy them on the infrastructure, understanding the security needs and capabilities of the customer.

However this is often a short-term agreement, without providing additional support over time. MSSPs partner with an organization, *giving proactive support to the client* over an extended period of time, thinking through the entire cybersecurity lifecycle.



Working with an MSSP goes beyond finding the right tools and technologies—it's about working with a partner you trust to keep your organization, data, and network safe.

There might not be a one-size-fits-all option, but it starts by analyzing what your organization needs. Do you just need firewall technology? Or security training for your employees? Or do you want to go deeper and outsource your security to an MSSP you can trust, taking advantage of their team's security expertise and building a long-term partnership?

Ask the right questions, do the research, and you'll be on your way to finding a partner who can enhance the security of your organization.

SCHEDULE A CALL WITH A CYBERSECURITY EXPERT

BOOK YOUR FREE CONSULTATION

Ascend TECHNOLOGIES