

---

# How to Select a Managed Security Service Provider (MSSP)

**Mike Johnson**  
CTO



---

## Introduction

This whitepaper is the last of three in a series exploring MSSPs. In previous papers, we have defined what a Managed Security Service Provider (MSSP) does, and explored the benefits that can be experienced by partnering with one. But once you have decided that working with a MSSP makes sense for your company, how do you go about choosing the one that is right for you?

Selecting a MSSP can be a daunting task since services offered, terms used, and competence can vary widely across providers. Since the managed security market is still young there are numerous permutations of what each provider believes should be included with a managed security service. These differentiations aren't necessarily right or wrong but rather give the buyer more opportunity to seek the perfect fit for their situation.

With a dynamic market it is critical for a buyer to obtain all the necessary information to make the right decision. After reading this whitepaper you will have a greater understanding of Managed Security Service Providers and ideas to help you make the right choice when selecting a MSSP for your company.

## Reputation

Reputation in the marketplace should offer a good snapshot of the MSSP. Use it to give you an idea of how the MSSP works and what others think of the MSSP. Ask your technology providers if they know anything about a particular MSSP. Most importantly, talk to the MSSP's client references. They will provide you with the most insight into how happy you will be with that MSSP.

Questions to ask:

- Is the MSSP respected in the industry/area?
- Who are their customers?
- Do they already service customers in my industry?
- Do they service customers my size (small, medium, or large)?
- How long have their customers been with them?
- What is their cancellation/non-renew rate?

## Support for your systems

For a MSSP to be successful in supporting your infrastructure, naturally the MSSP must support the systems you use. If the MSSP only supports brand X firewall and you have brand Y, obviously the MSSP will not be a good fit for your organization.

Look for certifications or accreditations from the vendors of the products you own and on which you will need support. These may be in the form of company partner level certifications or at the individual engineer level or both.

Questions to ask:

- 
- Does the provider have deep experience with your systems similar to mine?
  - Are they certified/accredited with that technology?
  - Will they require me to put in new hardware or software, or change my network or processes in order to use their service?
  - Is technical support limited to certain systems or applications?
  - Am I limited to a certain number of support incidents per year?

## **Managed Security Specialization**

Many systems integrators and providers of other network services claim to be a MSSP as well. You will most likely find that these integrators are set up for project-based consulting and don't have the necessary infrastructure to support you in the role of a MSSP. An integrator's policies are created to provide service availability without respect to confidentiality or integrity. Response, reporting and monitoring will most likely be lacking from an integrator attempting to perform the role of a MSSP.

Questions to ask:

- Is the provider focused on managed security or is this an afterthought to their main line of business?
- What percentage of their revenue comes from managed services?
- Does the provider offer non-security services, such as desktop assistance or voice-over-IP deployments?

## **Personnel**

When you contract with an MSSP, the biggest value they bring to the relationship is in the expertise of their people. It is critical for a service company to maintain quality personnel. Abilities and attitudes of the MSSP's personnel can be easily ascertained. When selecting a MSSP, ask to speak with more than just the salesperson that is proposing you the service - ask to speak with one or more engineers.

Questions to ask:

- Is the engineer interested in me and my needs or blowing his/her own horn?
- Would I hire this person to manage my security?
- Does the company hire "reformed" hackers?
- Is a background check performed on new employees?
- Does the company use contractors for any of its services?
- Are personnel held to the same strict confidentiality agreements that I would initiate with the MSSP?
- What is the ratio of senior engineers to managed clients?
- What certifications are held by senior staff? Junior staff?
- What is the MSSP's employee turnover rate?

While it is important to evaluate the engineering staff, competence of sales personnel can also be a good gauge of corporate capability. Though it is often said that "the best service comes before the sale," if the sales staff has a good understanding of the products and services they are selling, it is a good indicator that the products are mature and well-defined, and that competency extends throughout the organization.

---

## Service Offering

A MSSP should provide you with a clear list of tasks that will be regularly performed. There should be no grey areas or potentially confusing conflicts. The point here is to insure that the lines of responsibility are clearly delineated. You should also make sure that the service offering covers all the tasks that you need performed.

Questions to ask:

- Is the service offering clear and well documented (no grey areas of responsibility)?
- Does the service offering include all items I would want done if I were hiring someone to perform the tasks in-house?

Look for a MSSP who is willing to fulfill your needs. For example, if you need a monthly or quarterly report on the state of your IT security make sure you can get it.

## Specialty

MSSPs specialize in specific client sizes. If your company has ten employees, you probably do not need a MSSP that specializes in companies with thousands of employees. The same holds true for MSSPs that specialize in small- and medium-sized business – these companies are not set up to work with a company with twenty thousand employees. Find a MSSP that specializes in companies of your size.

Some companies must comply with regulations related to their industry or financial status, such as Sarbanes Oxley, HIPAA, or Graham-Leach-Bliley. Companies that need to comply with regulations should look for a MSSP with experience in these areas. Different market segments have different needs. Finding a MSSP with experience in your segment will lighten your workload.

Questions to ask:

- How many employees does the MSSP's average client have?
- Does the MSSP specialize in any particular industries?
- Is the MSSP familiar with \_\_\_\_\_ (fill in the blank with an regulations applicable to your business)?

## Stability

Reasonable due diligence will often show how stable a company is: whether it is growing, stable, or near bankruptcy.

Examine the MSSP's stability. Make sure that the company has a viable business plan. Look for positive indicators like the number of years the MSSP has been in business. Look for signs of growth from the MSSP's major clients. Look for large account wins and growing revenue.

---

Client retention will also give an indication of company stability. If the MSSP has a history of losing clients it may be best to look elsewhere.

Questions to ask:

- How long has the MSSP been in business?
- What is the MSSP's client turnover rate?
- What are the MSSP's revenue numbers? (If the MSSP is private and unwilling to share this information, ask for the information in percentages rather than the actual numbers).

## **Response Time**

Many companies considering outsourcing are rightfully concerned about the response time they will receive from the MSSP. Sometimes in the event of a problem or a business need, changes need to be made immediately on security devices. MSSPs vary widely in their response time, so determining in advance what you can expect in common scenarios will help you gain a better understanding of the MSSP's customer service. A MSSP should have a sense of urgency when you have a problem or need quick action.

Questions to ask:

- What is the protocol for making firewall or IDS changes?
- How long will I have to wait for a firewall rule change or IDS rule change?
- Does the MSSP's response time change during off-hours?
- What sort of response can I expect when I have a question?
- How long can I expect to sit on hold when I call in with a question or problem?

## **Maturity**

Before signing with a MSSP, you should find out as much as you can about their background. How a MSSP is funded and their stage in their corporate lifecycle directly affects their capabilities, and how they will interact with clients.

Documentation of policies and procedures is a sign of a company with a solid foundation. Too often, technology companies grow quickly and don't take the time to document important information. If policies and procedures are not documented they will not support the company as it grows. Written policies and procedures also show that thought has been given to the details, which is a positive sign.

Questions to ask:

- How is the MSSP funded?
- What is the MSSP's 1-year plan? It's 5-year plan?
- Is the MSSP planning expansion, geographic or otherwise?
- What markets does the MSSP serve?
- Will the MSSP provide documentation on its internal security policies and procedures? (NDA probably needed to obtain this information)

---

## Escalation

Escalation is unavoidable when dealing with a support provider for any service. Security issues, though, often need top-level expertise quickly. Exploring the MSSP's escalation procedures in advance will insure that your provider shares your values. If you are not comfortable with how they handle problems, keep looking.

Questions to ask:

- What are the MSSP's escalation procedures? Ask to see these in writing.
- How long does a ticket wait until a senior engineer gets involved?
- Does the MSSP have a classification system to determine the priority of problems?
- Do I have any say in what is considered an emergency?
- Is the escalation procedure satisfactory to me?

## Location

In previous whitepapers, we've discussed the difference between national and regional MSSPs. Some companies prefer the comfort of choosing a MSSP with a nationally recognized name, while others prefer the more service-oriented nature of regional MSSPs. Each have pros and cons. Whatever your preference, make sure you understand what type of MSSP you are dealing with.

Questions to ask:

- Where are the technicians that are monitoring and managing my security devices located?
- If in a different time zone, whose business hours determine rates and services (if different during off-hours)?
- (If the MSSP support staff is not located in your country) Is there any potential for a language barrier?
- Are onsite visits, if necessary, included with service?

## Reporting

You may have the best MSSP in the world maintaining your security, however if there is not a reporting structure in place to inform you about the state of your security and important events you are missing out on a valuable asset.

A MSSP that acts as a true security partner will provide regular reports that contain details of security events, actions they took, and ways of limiting exposure in the future. Some reports may be computer generated, however you should expect a security expert to review and interpret critical data in the reports as well. Computers are valuable tools when it comes to sorting through vast amounts of information, but there is no replacement for human intelligence.

Along with reports you should expect real time access to data, events, and metrics. Many times this access is provided via a security portal. Find out what type of data you

---

can expect in this regard, and determine whether this information truly provides value to you. Sometimes we find that MSSPs place emphasis on presenting information that 'looks good' but doesn't actually provide the client with any real insight.

Questions to ask:

- ❑ What type of reports does the MSSP offer and in what intervals?
- ❑ Are the reports auto-generated or does a security expert create the report?
- ❑ Is there real-time reporting of information via a portal or some other process?
- ❑ What type of information is reported in real-time?
- ❑ Is the information actionable?

## Summary

Benefits of outsourcing security services are easy to see, but differentiating between MSSPs may not be as easy. By understanding what MSSPs offer and by thinking about how you might work with a MSSP on a day-to-day basis, selecting a MSSP becomes less daunting.

Since IT security is a specialized industry requiring extensive expertise, it is one that makes financial and business sense to outsource to a competent provider. Determining which provider suits your company best becomes the challenge. However, there are a number of characteristics that are shared between MSSPs that can be compared to differentiate one from another.

Carefully examine MSSPs to determine which will fulfill your requirements, has experience in your industry, and has the flexibility to do what you need rather than a prefabricated plan, and you will find engaging a MSSP for your IT security management to be a very effective partnership.

For more information on MSSPs, please reference Webfargo Data Security's previous whitepapers entitled "What is a Managed Security Service Provider," and "Why Outsource to a Managed Security Service Provider," which can be found at [www.webfargo.com/library](http://www.webfargo.com/library).

---

## Questions for MSSP Evaluation

### 1. Reputation

- 1.1. Is the MSSP respected in the industry/area?
- 1.2. Who are their customers?
- 1.3. Do they service customers in my industry?
- 1.4. Do they service customers my size?
- 1.5. How long have their customers been with them?
- 1.6. What is their cancellation/non-renew rate?

### 2. Support for your systems

- 2.1. Does the provider have deep experience with your systems similar to mine?
- 2.2. Are they certified/accredited with that technology?
- 2.3. Will they require me to put in new hardware or software, or change my network or processes in order to use their service?
- 2.4. Is technical support limited to certain systems or applications?
- 2.5. Am I limited to a certain number of support incidents per year?

### 3. Security Specialization

- 3.1. Is the provider focused on managed security or is this an afterthought to their main line of business?
- 3.2. What percentage of their revenue comes from managed services?
- 3.3. Does the provider offer non-security services, such as desktop assistance or voice-over-IP deployments?

### 4. Personnel

- 4.1. Is the engineer interested in me and my needs rather than blowing his own horn?
- 4.2. Would I hire this person to manage my security?
- 4.3. Does the company hire "reformed" hackers?
- 4.4. Is a background check performed on new employees?
- 4.5. Does the company use contractors for any of its services?
- 4.6. Are personnel held to the same strict confidentiality agreements that I would initiate with the MSSP?
- 4.7. What is the ratio of senior engineers to managed clients?
- 4.8. What certifications are held by senior staff? Junior staff?
- 4.9. What is the MSSP's turnover rate?

### 5. Service Offering

- 5.1. Is the service offering clear and well documented (no grey areas of responsibility)?
- 5.2. Does the service offering include all items I would want done if I were hiring someone to perform the tasks in-house?

### 6. Specialty

- 6.1. How many employees does the MSSP's average client have?
- 6.2. Does the MSSP specialize in any particular industries?
- 6.3. Is the MSSP familiar with \_\_\_\_\_? (fill in the blank with an regulations applicable to your business)

### 7. Stability

- 
- 7.1. How long has the MSSP been in business?
  - 7.2. What is the MSSP's client turnover rate?
  - 7.3. What are the MSSP's revenue numbers? (If the MSSP is private and unwilling to share this information, ask for the information in percentages rather than actual numbers).

## **8. Response Time**

- 8.1. What is the protocol for making firewall or IDS changes?
- 8.2. How long will I have to wait for a firewall rule change or IDS rule change?
- 8.3. Does the MSSP's response time change during off-hours?
- 8.4. What sort of response can I expect when I have a question?
- 8.5. How long can I expect to sit on hold when I call in with a question?

## **9. Maturity**

- 9.1. How is the MSSP funded?
- 9.2. What are the MSSP's 1-year plans? 5-year plans?
- 9.3. Is the MSSP planning expansion, geographic or otherwise?
- 9.4. What markets does the MSSP serve?
- 9.5. Will the MSSP provide documentation on its internal security policies and procedures? (NDA probably needed to obtain this information)

## **10. Escalation**

- 10.1. What are the MSSP's escalation procedures? Ask to see these in writing.
- 10.2. How long does a ticket wait until a senior engineer gets involved?
- 10.3. Does the MSSP have a system to determine the priority of a problem?
- 10.4. Do I have any say in what is considered an emergency?
- 10.5. Is the escalation procedure satisfactory to me?

## **11. Location**

- 11.1. Where are the technicians that are managing my security devices located?
- 11.2. If in another time zone, whose business hours determine rates and services?
- 11.3. Is there any potential for a language barrier?
- 11.4. Are onsite visits, if necessary, included with service?

## **12. Reporting**

- 12.1. What type of reports does the MSSP offer and in what intervals?
- 12.2. Are the reports auto-generated or does a security expert create the report?
- 12.3. Is there real-time reporting of information via a portal or some other process?
- 12.4. What type of information is reported in real-time?
- 12.5. Is the information actionable?