

---

# What is a Managed Security Service Provider (MSSP)?

**Mike Johnson**  
CTO



---

## Introduction

Security has always been a hot button in certain industries. You would expect that any organization that stores classified information, valuable intellectual property, or financial information would make IT Security a priority and devote resources and budget to creating a secure infrastructure. But what about the rest of the corporate world?

As threats emerge from hackers, corporate espionage, state sponsored terrorism, viruses, trojans, worms and spyware, security becomes a critical topic for every organization with a computer network. While risk varies from company to company based on the type of data that must be protected, any company that digitizes information and is connected to the Internet faces risk of a security incident.

Companies don't need to store national security secrets on their networks to be concerned about security either. Consider how you would answer the following questions:

- What would be the costs and repercussions if some or all of your company's computer infrastructure was disabled by a virus for a period of hours, days, or weeks?
- Would your company's reputation suffer if your web site was defaced?
- What would be the fallout if FDA or SEC regulated information was released to the public?
- What kind of hit would your business take if your customer data was leaked on the Internet?
- What would happen if your company's employee/HR records were accessed and distributed?
- Could your business continue to function if your main database was corrupted? Stolen?

Clearly, security needs to be a priority for every organization reasonably concerned with privacy of its information and integrity of its computer network.

## The Evolution of IT Security

As the concept of IT Security was developed decades ago, and further refined in the early 1990's, setting up a firewall, and even an antivirus solution, was traditionally all that was required to virtually eliminate risk of a security incident. Threats were relatively static, and untargeted malicious Internet activity was low.

Fast forward to the late 1990's, and threats are becoming more numerous and more malevolent. Hacking tools have been simplified so that non-techies can use them, and new worms and viruses are starting to spread without human intervention. Hackers are employing zombie networks of compromised computers to anonymously carry out their commands. Keeping computer networks secure from external and internal threats has

---

become a full time job – a job that few companies, especially in the small- to medium-sized business category, are able to staff full time.

Managed Security Service Providers (MSSPs) came along to fill this niche - to bridge the gap between IT Security need and corporate resources. By partnering with a MSSP, small and medium businesses can benefit from all the expertise and tools that a large enterprise might employ at a fraction of the cost. This is why managed security is one of the fastest-growing segments of the IT security market.

## **Exactly What is a MSSP?**

Put simply: MSSPs provide companies with some aspect of network security management. All or a portion of a company's security may be managed by a MSSP. Typical MSSP offerings include:

- ❑ Managed Firewall
- ❑ Managed VPN
- ❑ Managed Intrusion Detection
- ❑ Managed Intrusion Prevention
- ❑ Email Security
- ❑ Vulnerability Scanning
- ❑ Managed Authentication

In most every case, managed devices are monitored and anomalous behavior is detected and corrected. However, the similarities often end there as services can differ widely from MSSP to MSSP, with some providing mainly monitoring while others provide complete security management.

## **All MSSPs Are Not Created Equal**

MSSPs fall into two categories that can loosely be defined as National and Regional. National MSSPs are typically large companies with well-defined infrastructures who have a good deal of name recognition in the marketplace. Often the national MSSPs have sophisticated network operations centers and high-end tools. Regional MSSPs typically fill niches that the National MSSPs cannot adequately reach. While Regional MSSPs typically do not have the infrastructure of their National counterparts, they tend to make up for this by providing the customized service required by the small- to medium-sized business market, including onsite visits and participation in the creation and application of security policy. Regional MSSPs can often more effectively act as an outsourced security department to their clients.

Independent of the market that they serve, most MSSPs fall into one of three groups based on their lineage:

- 
- 1) The MSSP evolved from an ISP, hosting provider, or telecom that began to offer managed security services when they recognized the need for increased security from their clients, or
  - 2) The MSSP evolved from a network integration or consulting company that saw the same need in their clients, and formed a unit to address these needs, or
  - 3) The MSSP was formed solely to provide outsourced security management.

As you might expect, group 1 typically emphasizes infrastructure and reliability as their strengths while groups 2 and 3 play up their more consultative, solution-oriented approach to managing security. Group 3 is certainly the rarest.

In any case, it is important to note that competence and service among MSSPs can vary widely, and a thorough review of the service offering and client references is essential when seeking an IT security partner.

### **What is a MSSP *Not*?**

In the previous sections we've defined what a MSSP *is*, but what is a MSSP *not*? On the surface this may seem to be an unusual question, but since there are no standards governing the industry, it bears some scrutiny.

The following is a list of items that good MSSP should not do:

- ❑ A MSSP should NOT make you give up control of your security devices.
- ❑ A MSSP should NOT force you to make major network changes to accommodate their service (i.e., replace your firewall with their security appliance).
- ❑ A MSSP should NOT force you to make policy changes in order to work with them – they should fit into your policies rather than vice versa.
- ❑ A MSSP should NOT require any more network access than the minimum required to perform their contracted tasks.
- ❑ A MSSP should NOT be vague about their responsibilities.
- ❑ A MSSP should NOT provide your company with Internet service, web hosting service, phone service, network or desktop support. Keeping these services separate avoids potential conflicts of interest.

When considering a MSSP, it is important to not only understand what services they will be providing, but also to understand exactly what they will be requiring from you in order to use their service.

### **Who Should Choose to Partner With a MSSP?**

There are numerous reasons to partner with a MSSP, but we typically find the companies fit one of four different profiles:

---

Companies whose data is critical to their business. In this category are ecommerce companies, pharmaceutical companies, clinical research companies, financial companies, technology companies – any organization whose business would suffer if they were to lose intellectual property through a security incident. If your business revolves around data, making sure that data is appropriately protected could literally be the difference between corporate life and death.

Companies with big security needs but small budgets. Companies in this category may or may not have ultra-critical data, but regardless they understand the need to keep their network appropriately shielded from malicious users. These companies benefit from the advanced security services provided by a MSSP, which are delivered at the fraction of a cost of staffing a dedicated IT Security position.

Companies whose IT Staff is at capacity. Similar to the group above, these companies don't want to add additional demands to their IT staff. Since IT security is an area that requires significant and highly specialized expertise, outsourcing this task rather than constantly training and retraining existing IT employees makes economic sense.

Companies that need more insight into their network events. By using specialized tools and years of experience, a MSSP will typically provide much more actionable data than an in-house IT employee could be expected to provide. Whether it is round-the-clock monitoring, detailed firewall log review, or insight into suspicious IDS alerts, a MSSP can typically provide these services much more consistently than in-house staff, which appeals to those companies seeking more information about the state of their network security.

## **Summary**

There are a host of benefits to be realized by partnering with a security provider. Before looking outward for a MSSP, it makes sense to first look inward at your company's security requirements to better understand your needs, which will help you to determine what gaps need to be filled by a MSSP.

Though it may seem vexing that Managed Security Service Providers differ so widely in the marketplace, that is actually a benefit to the end user. The wide variation means that most any company or organization will be able to find a MSSP that shares their priorities and will integrate easily into their IT department.

MSSPs fill an important role in the IT security industry: providing high-end security services to business that otherwise could not afford a full time security staff. MSSPs level the playing field so that small- and medium-sized businesses can benefit from the same security infrastructure that was previously only found in large companies.

For more information on MSSPs, please reference Webfargo Data Security's 2<sup>nd</sup> whitepaper in this series entitled "Why Outsource to a Managed Security Service Provider," which can be found at [www.webfargo.com/library](http://www.webfargo.com/library).