

Choosing the Right Managed Security Services Provider

By Grant Geyer, Vice President, Global Managed Security Services, Symantec Corp.

Today's managed security services providers (MSSPs) bear little resemblance to the providers from earlier years. Several years ago, the MSS market was full of vendors providing remote security capabilities to enterprise customers looking to outsource. In the last several years, larger companies have set their acquisition sights on MSSPs to enter the market. Clearly, outsourced security is a service whose time has come.

The MSSPs in the market today are by and large stable, and can best be categorized as Strategic Outsourcers, Telecommunications Providers, Enterprise Pure Plays and Boutique Pure Plays. As the MSS market continues to consolidate, organizations must carefully consider the most appropriate MSSP for their needs. Is a pure-play MSSP the right choice, or is a strategic outsourcer or telecom carrier with security capabilities more suitable? And what happens if the chosen provider is acquired?

By understanding how the MSS market has evolved, understanding the different classes of providers, and identifying key considerations for making the right choice in a consolidated market, organizations can select the right MSSP in an increasingly challenging threat landscape.

A Maturing Customer Need

The MSS market was founded to help businesses improve their security posture by monitoring their infrastructure in real time against threats. The nature of the threats have changed over time, from hackers and viruses in the early days to stealthy fraud-based attacks aimed at stealing information for financial gain.

The combination of today's highly sophisticated threat landscape, together with a seemingly unending wave of government and industry regulations for data protection, has made information security a boardroom issue. Organizations that fail to protect information can be held liable for breaches and losses and be fined or sued. In addition to government-imposed fines and penalties, organizations may be subject to civil liabilities or class-action lawsuits on behalf of customers who have lost data.

Clearly, protecting information is now a high-profile business priority, which makes meeting regulatory requirements an important component of a risk management program. A growing number of organizations are discovering that outsourcing security monitoring to a capable MSSP enables them to do more than simply check a box to demonstrate compliance to an auditor. It enables them to better protect their information assets, reduce their vulnerability to threats and free IT to focus on core business issues.

Types of MSS Providers

Businesses must understand that selecting the right category of MSSP can make all the difference in solving their specific risk management business challenges. Currently, there are four classes of providers:

- **Strategic Outsourcers (SOs)** are in the business of providing complete outsourced IT solutions to their customers. The strategic outsourcers provide MSS as a natural extension of their IT outsourcing offerings.
- **Telecommunications Providers** can serve as full outsourcers to customers, but also provide "in the cloud" capabilities and include various built-in security elements such as firewalls and intrusion detection. This provider is typically attractive to customers seeking to streamline and minimize the number of vendors they have to manage.

- **Enterprise Pure Plays** are typically software or services companies offering MSS as part of their core portfolios. This segment is well-suited to customers looking for a full solution to meet a risk management need.
- **Boutique Pure Plays** tend to focus solely on MSS or might have a small complementary professional services component. They are experts in that one core area, but can lack the ability to scale to handle the full solutions customers desire.

Choosing a Provider

Today, organizations can select from a variety of providers that offer managed security services. However, just as outsourcing security may not be appropriate for every organization, every outsourcer may not be appropriate for each customer's needs.

One of the most fundamental differences among the four classes of providers is their delivery models. Telcos and SOs offer managed security services as a component of other outsourced services, while the pure plays tend to offer targeted security solutions to meet specific customer needs. Customers that work with a telco or outsourcer enjoy full turnkey solutions which minimizes the number of vendors a customer needs to work with to get a problem resolved. The other side of the argument is that while working with a pure vendor for your MSS and SO for IT outsourcing may create additional overhead, it provides checks and balances between the security and IT functions. For example, if the SO or telco is responsible for patching your systems, you might want an independent MSS pure play to provide validation.

The advantage of using pure plays rest with the independence they can offer customers from their IT teams, providing full checks and balances on typical IT operations. Also, these providers tend to have a specialized focus on security and have a critical mass of expertise that allows clients to gain leverage from the relationship. When deciding between an Enterprise and a Boutique Pure Play, clients should pay careful attention to the stability of the provider. Clients should look for vendors committed to the business and that focus on developing their offerings to keep pace with customer needs.

With the Boutique Pure Plays, the risks can be greater. Many boutiques have gone out of business, leaving their customers without protection and scrambling to find another provider. As Enterprise Pure Plays tend to be large organizations with broad relationships with each client, they have greater resources on hand to ensure their service delivery can be more effectively maintained over time.

Other Key Considerations

Regardless of which class of provider an organization considers, the details still, and always will, matter when choosing an MSSP. Nearly every large MSSP has an impressive security operations centers (SOCs), professionally staffed and outfitted with advanced technologies and systems. Yet, only by looking under the hood can the capabilities of the MSSP be understood.

For example, the most advanced MSSPs leverage vast global intelligence networks to provide real-time analysis of security data as attacks are detected in progress. The analysis of both firewall and intrusion detection data also raises the awareness of security threats exponentially.

Advanced MSSPs also correlate external threat activity with the unique requirements of an organization's environment to provide actionable, prioritized remediation recommendations. Customers should expect a full SOC tour, a detailed look at the provider's technology, interviews with the customer's security experts, and review the results of the providers SAS70 Type II and ISO27001 certifications.

With constantly evolving technologies and attack techniques making security a moving target, organizations are exposed to new risks nearly every day. By partnering with an MSSP that offers powerful technology along with accurate threat intelligence, proven processes, and experienced

professionals, organizations can significantly improve their protection while meeting complex compliance demands and maximizing their IT investments.