Avast Business

White paper

Top 5 reasons why savvy MSPs are adopting managed security services

16 November 2023

Avast Business

Introduction

It is no secret that the managed services industry, like many others, is undergoing a transformation. Because of new, more resilient technologies and new ways of working, installing hardware and maintaining the operational status of a network is no longer as valuable as it once was. As a result, managed services providers (MSPs) are looking for new revenue streams and new ways to deliver, and demonstrate, value to their clients.

One way to add value to clients is by offering managed security services. Small and medium-sized businesses (SMBs) are under attack by a variety of cyberthreats, but these organizations either do not realize how vulnerable they are or do not have the necessary time, resources, or skills to address the issues. By adding managed security services to their practice, MSPs can not only deliver real value to their customers and become their trusted security advisors, but they will also differentiate their business, making them very difficult to displace.

However, adding services to a practice is not easy, which means many MSPs are facing a very difficult decision. Stay with the status quo – and compete largely on price – or invest in evolving their practice so they do not become commoditized. The successful service providers are doing the latter. They are embracing innovative technologies and searching for new ways to add value to their clients while generating new, ongoing revenue.

The purpose of this white paper is to introduce managed security services as a key strategy for evolving your business. This paper will cover:

- How the threat landscape for SMBs is changing.
- What managed security services are.
- The top benefits that you – and your SMB clients – will realize from managed security services.
- Key components of a managed security service.

Contents

The New SMB Downtime – Cyberthreats 3

The Case for Managed Security Services 3

Key Components of a Managed Security Service 5

Summary 7

Avast Business

The New SMB Downtime – Cyberthreats

A common misunderstanding among SMBs is that they are too small to be a target for malware attacks and other cybercrime. While they understand that security is important, many business owners believe these attacks are merely focused on larger enterprises. Unfortunately, they are wrong.

According to the 2018 State of SMB Cybersecurity Report[1], published by Ponemon Institute, an independent research and education organization:

- Hackers breached 58% of SMBs over a 12-month period in the United States, derailing an SMB's "money making activities for up to a week"
- The most prevalent attacks against SMBs are web-based and phishing/social engineering
- 54% of SMBs have no visibility into employee password practices and hygiene
- 63% of SMBs that have a password policy do not strictly enforce it

The report called these and other statistics a national crisis while noting that, despite this known vulnerability, "many of America's 28 million small businesses are not thinking about cybersecurity."

The reality is that SMBs are often more vulnerable than their enterprise counterparts. Opportunistic hackers realize that many SMBs have weak cybersecurity protocols and lack specialized in-house IT professionals with security expertise. This makes them an appealing and easy target. As a result, cyberattacks now represent the most serious downtime threat to SMBs.

In addition, SMBs are increasingly dependent on interconnected systems, such as Cloud, SaaS, BYOD, and IoT. These technologies create opportunities for skilled hackers to unleash malware. Whether it is a virus, trojan, worm, bot, or other permutation, malware can inflict various degrees of damage, from simply being a minor annoyance to disabling entire businesses.

A ransomware scenario

Imagine that an employee at one of your SMB clients, accidentally let loose a virulent strain of ransomware. The infection has exploited a vulnerability in the clients' system and has spread rapidly across the network. As a result, critical files have been encrypted, paralyzing the entire business. The files remain inaccessible until the ransom is paid, typically in bitcoin or other difficult to trace cryptocurrency.

Cyberattacks now represent the most serious downtime threat to SMBs.

Malware can inflict various degrees of damage from simply being a minor annoyance to disabling entire businesses.

Avast Business

What most often occurs in these situations is that, even if the ransom has been paid, the attacker does not unlock the files or even destroys them, leaving the client with an irreparable damage. While this is a hypothetical scenario, the threat to your SMB clients is real. Threats are not only more prevalent, they are also increasingly complex. By the time a cyberattack has penetrated the network, it is almost impossible to repair the infected systems. As an MSP, you do not want to be in the situation where you are reacting to a successfully executed cyberattack, as the damage has already been done by that time. It is therefore better to prevent than to repair.

MSPs should put security at the core of their practice, but that doesn't mean completely overhauling their business and focusing exclusively on security, like MSSPs.

The Case for Managed Security Services

Many MSPs are dedicated to maintaining the operational status of an SMB network by aligning service priorities to availability, stability, and performance of critical SMB IT resources. While this role is clearly valuable, most SMBs have now adopted cloud services, mobile computing, and IT anywhere. Their networks have evolved to become more resilient and less susceptible to traditional downtime scenarios, such as hardware failures and incorrect application configurations.

Innovative MSPs recognize the importance of expanding their focus beyond availability, stability, and performance to include security services that protect data, devices, and people. Delivering comprehensive security services not only provides their customers with complete peace of mind, but allows them to grow their business. In addition to creating important new revenue streams, MSPs can position themselves as their customers' trusted security advisor, making them difficult to displace.

What are managed security services?

As an MSP, you are already familiar with the key principles of managed services. You proactively and remotely provide services. A managed security service is essentially the same.

For an additional fee, you extend your proactive monitoring and management to include network and cybersecurity services. The goal – and opportunity – is to take a proactive, systematic approach to assessing, securing, and monitoring your clients' day-to-day security needs.

By adding managed security services, you can not only deliver real value to your customers as trusted security advisors, but you can differentiate your business and create a strategic competitive advantage.

Avast Business

5 Benefits of Managed Security Services

1 **Stay ahead of new cyberthreats.**

If you are not prepared for a security incident as your client's IT advisor, you will lose their trust and their business. Adding security services to your MSP practice allows you to stay one step ahead of cybersecurity threats and keep your clients' businesses safe.

2 **Improve time to value.**

Today, customer churn is faster than ever before, so the sooner you can show value to your customers, the better. With the right security tools built into your offering, you can easily see all security services you've deployed, manage and change policies, check the status of devices, remediate device issues, and detect attacks before they've had a chance to do serious damage.

3 **Grow your bottom line — consistently.**

Offering a broader range of managed services, combined with minimal or no additional staffing costs, means that there is much more potential to grow annual recurring revenue without increasing costs, or changing your business processes.

4 **Strengthen client relationships.**

When you oversee a client's security infrastructure — in addition to other IT service — you gain the opportunity to strengthen your relationships with existing clients and become a true partner, making it much harder for your competitors to displace you.

5 **Differentiate your business.**

The services of a traditional MSP are becoming commoditized. A robust managed security services program, in addition to your existing services portfolio, makes you not only attractive to your existing clients, but new ones as well.

Key Components of a Managed Security Service

Effective cybersecurity rests on three pillars: products, processes, and people. However, most SMBs do not need the cumbersome, expensive protection that enterprises or businesses in highly regulated industries require. In fact, SMBs require the opposite: a flexible and dynamic approach that changes and adapts as the threatscape, tools, and techniques change.

For SMBs, a robust managed security service typically includes the following elements.

- Managed antivirus
- Web hardening
- Patch management
- Managed firewalls
- Secure web gateway
- Password management

- Multi-factor authentication
- User access controls
- Simple vulnerability scans
- Managed backup and disaster recovery
- Secure remote working (VPN)
- Data loss prevention
- Enforceable processes and policies
- Security awareness and training for employees

This last point is especially critical. Training employees and creating awareness play key roles in securing the network, as people are generally perceived as the weakest links in the digital security chain. A staggering 95 percent of all security breaches were caused by human error.

Creating a cybersecurity culture for your clients should include:

- Comprehensive cybersecurity policies that are part of business processes.
- Ongoing education, training, and security reviews that involve everybody.
- A focus on individual responsibility and awareness that everyone has a vital, ongoing role.

Summary

Managed security services are an important consideration for any MSP practice. SMB customers are under attack from increasingly complex malware that includes spyware, viruses, worms, trojans, and ransomware. As an MSP, you are the go-to-expert for your clients on a broad range of IT-related issues. Your clients will expect you to give appropriate recommendations and to take proactive measures to protect their business.

Adding a managed security service is a natural extension of your MSP business – enabling you to manage security solutions across all customer endpoints, servers, network, web, and email from a centralized remote monitoring and management platform.

In addition to protecting your SMB clients and deepening the relationship, a managed security service enables you to differentiate your practice, generate important new revenues – and ensure a successful MSP practice in a new climate of security concerns, privacy invasions, data breaches, and cybercrime.

1 2018 State of Cybersecurity in Small & Medium Sized Businesses (SMB), Ponemon Institute LLC, November, 2018

About Avast Business

Avast delivers easy-to-use, affordable, and award-winning cybersecurity solutions for small and growing businesses. Avast provides integrated security services to protect your devices, data, applications, and networks. Backed by 30 years of innovation, we have one of the largest, most globally dispersed threat detection networks in the world. Our cybersecurity solutions are built to provide maximum protection so that you can worry less about cyberthreats and focus more on growing your business. For more information about our cybersecurity solutions, visit **www.avast.com/business**.