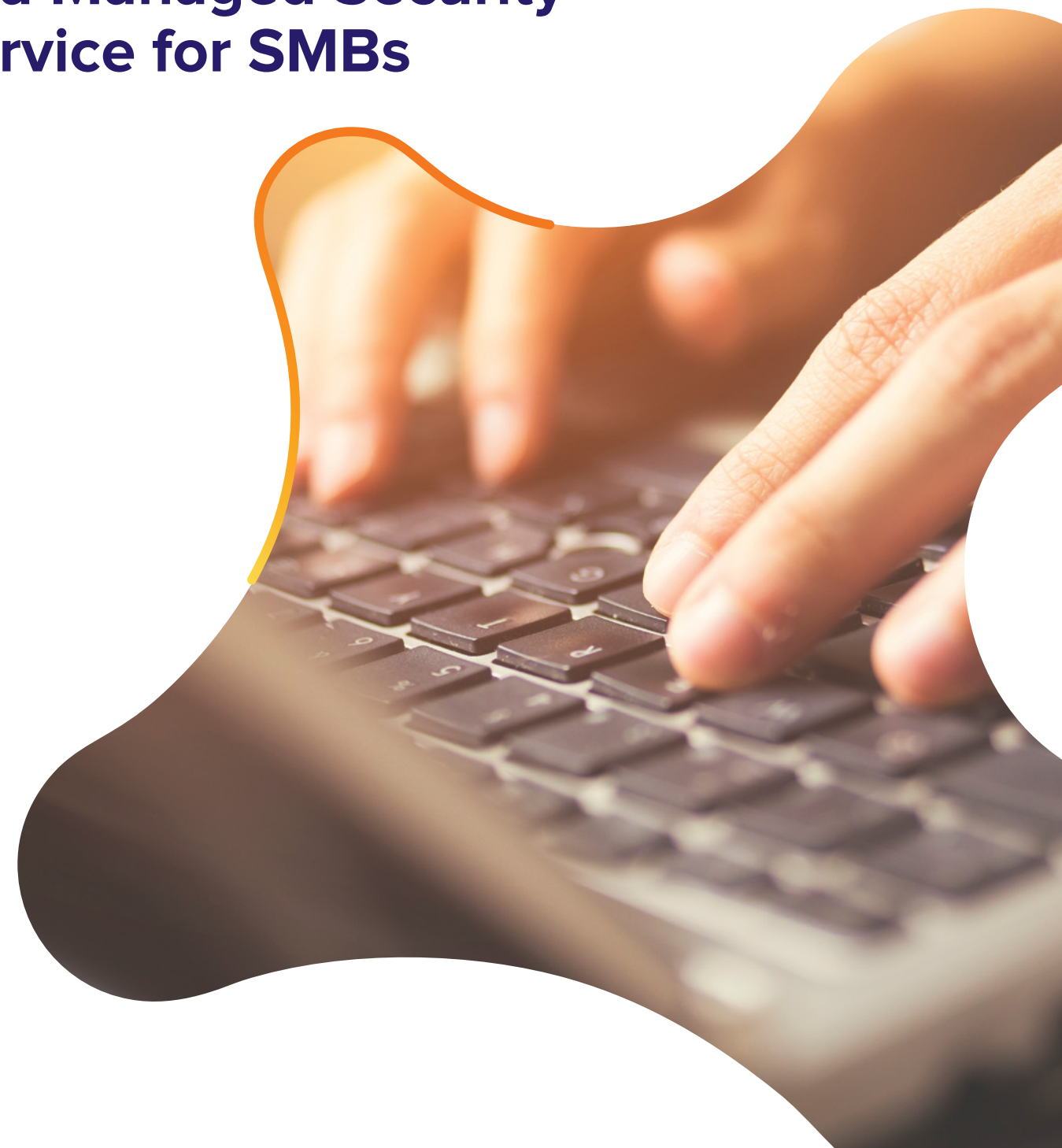
avast business

GUIDE

3 Essential Components of a Managed Security Service for SMBs



Introduction

Small- and medium-sized businesses have become increasingly attractive targets for cybercriminals because they lack the budget, resources, and security knowledge to put an effective defense in place and their data is just as valuable as an enterprise's. For IT service providers, this shift in focus to SMBs creates both an opportunity and a challenge.

The opportunity is managed security services. Managed security services are a great way for managed services providers (MSPs) to deliver the protection their customers are looking for while also growing their own business. Done right, managed security services can help SMBs mitigate the threat of downtime, lost revenue, and damage to their reputation. It can also help MSPs differentiate their business and build loyalty. However, the challenge for MSPs is knowing what security services their customers need and then determining how to effectively deliver these services on an SMB budget.

The first step in defining a security services portfolio is to look at your clients' attack surface. Once potential entry points have been identified, the next step is to apply the most appropriate tools and level of protection to stop these threats. Too much protection and the price tag quickly becomes too high or existing business processes break. Too little and your clients' vulnerability increases.

This white paper examines the current attack surface for SMBs and looks at the three essential components of a managed security service, which include protection for data, devices, and people. This combination ensures the right amount of proactive security for your customers without costing them too much. Specifically, this paper covers:

- What makes SMBs attractive targets
- Key vulnerabilities – devices and people
- Best practices for protecting your customers' data, devices, and people

Contents

What Makes SMBs Attractive Targets

Simply put, data is what cybercriminals are after. They can hold it hostage for a ransom, sell it on the black market, or use it to steal identities. They have lots of options. What makes SMBs attractive targets is their lack of defenses, especially when compared to enterprises.

Not too long ago, cybercriminals took a highly targeted approach and set their sites on enterprises because criminals thought enterprises had higher value data. But they have realized that SMBs have the same type of data — **customer contacts, health data, credit card data, or valuable intellectual property** — just less of it.

Now cybercriminals are taking an automated "spray and pray" approach which is easier and much more lucrative for them. In fact, fifty-eight percent of all American small and medium businesses experienced a data breach between October 2017 and November 2018[1].

Breaches and cyberattacks come at a considerable cost. These businesses spent an average of $1.43 million to pay for the damage or theft of their IT assets[2]. On top of that, most businesses were not able to conduct business as usual, which resulted in an average cost of $1.56 million, a 25 percent increase from $1.21 million in 2017.[3] The evolving threat landscape and these financial consequences are a great cause of concern for many SMBs.

> Fifty-eight percent of all American small and medium businesses experienced a data breach between October 2017 and November 2018.

What is keeping your clients awake at night?

- 60% of SMBs believe the consequences of cyberattacks are becoming more severe.
- 62% of SMBs believe cyberattacks are becoming more targeted.
- 59% of SMBs believe cyberattacks are becoming more sophisticated.[4]

Primary Attack Surfaces for SMBs

You've probably heard countless terms relating to cybersecurity, but here we are going to focus on just one: attack surface. An "attack surface" is simply the number of possible ways an attacker can get into a device or network and extract data. It's an especially important measure for SMBs because most think they are too small to be a target, but a quick look at their attack surface shows that it is often quite large, which increases their exposure to risk.

Like enterprises, SMBs have two primary attack surfaces: devices and people.

DEVICES

Because businesses are using more and more devices, there are more gateways for cybercriminals to carry out attacks. Predictions are that by 2020, businesses will account for six billion devices connected to the internet, ranging from laptops and phones to Internet of Things[5]. This inevitably means that the use of vulnerable operating systems and applications will increase as well.

> Cybercriminals want business data and there are two primary ways they can access it: devices and people. It is critical that your security services include security measures for all three areas to ensure proper protection.

The number one threat to devices is a hybrid ransomware attack. A ransomware attack on its own is bad enough. It allows hackers to take control of a device, after which they demand a ransom from the user before they can regain control. Today, ransomware is also spread in a hybrid form. By combining ransomware with the capabilities of a virus, it does not just infect one device, but easily spreads through the entire network.

PEOPLE

Sophisticated cyberattacks are mostly targeted at employees because they are the weakest link in the digital security chain. In fact **37% of security breaches** can be attributed to human error. Password policies and other safeguards designed to protect people, such as multi-factor authentication, are not standard practice within most SMB organizations. In fact, research by the Ponemon Institute showed that 57% of SMBs do not have a password policy in place[6].

The number one threat affecting people is targeted social engineering, which tricks people into handing over confidential company information. The hacker often contacts employees via e-mail, pretending to be a credible organization, such as FedEx, a bank, or even a colleague. Most employees do not have the knowledge to defend themselves against these advanced social engineering attacks.

> The number one threat to devices is a hybrid ransomware attack. For people, it's targeted social engineering.

Best Practices for Protecting Your Customers Devices, Data, and People

A managed security service for SMBs should include the ability to assess vulnerabilities, secure weak points, and monitor anomalies.

ASSESS

The first step in assessing your customers' potential vulnerabilities is to identify all the physical and virtual computing devices within the organization. Together with your client, make a list that includes all of the:

- Workstations and laptops
- Network file servers
- Network application servers
- Corporate firewalls and switches
- Multi-function printers
- Mobile devices

This infrastructure assessment should distinguish between cloud and on-premise systems and devices. This makes it easier for you to determine all possible storage locations for data.

Now, categorize all business data and divide it into three locations: cloud, on-premise systems, and devices. For example:

CLOUD	ON-PREMISE SYSTEMS	DEVICES
• Cloud email and applications • Cloud storage • Websites and social media	• Databases • Company-wide file sharing and storage • Intellectual property	• Presentations • Company memos • Statistics and reports

Next look at who has access and what kind of access they have. This third and final assessment is used to gain insight into the behaviors of each department or user within an organization, even if these users are unknown. These findings can be divided into the same three categories and should include the following aspects:

- Specific user access
- Multi-user access
- Unknown user access

SECURE

After conducting the assessment the next step is to determine what security you need. Below is an overview of the key security services an SMB needs.

DATA	DEVICES	PEOPLE
SECURE WEB GATEWAY Web threats are blocked from entering your network via malicious links, downloads, and more.	**ANTIVIRUS** Installing and monitoring antivirus on all devices – from PCs to mobile phones – is the best protection around.	**SECURE AUTHENTICATION** There are many ways to achieve this but defining password policies and using SSO and MFA are good first steps for an SMB.
EMAIL ENCRYPTION With end-to-end encryption, only the sender and receiver with a decryption key can view the contents of the email and any attachments.	**PATCH MANAGEMENT** All software systems come with vulnerabilities, but they can be resolved by installing patches and by keeping the software up to date.	**SECURE REMOTE WORKING** Remote workers need a VPN connection to their company network that encrypts all traffic to provide them with secure access to company data and applications.
DATA LOSS PREVENTION A DLP solution prevents end users from sharing sensitive data outside the company network by regulating what data they can transfer.	**REGULAR VULNERABILITY SCANS** Vulnerability scans should be done regularly and include the status of antivirus software, password policies, and software updates.	**DEFINE ENFORCEABLE PROCESSES AND POLICIES** With your clients, define what data needs protecting and how. Make this information available so everyone understands their role in keeping the business safe.
BACKUP AND DISASTER RECOVERY Even though you have taken every precaution, it is important to have a solid BDR solution in place that can restore operations quickly, at the push of a button.	**WEB SERVER HARDENING** Web servers usually sit at the edge of network making them more vulnerable to attacks. Proper hardening ensures default configurations are changed and that certain services and displays are disabled.	**PROVIDE SECURITY AWARENESS AND TRAINING** People cannot defend themselves against threats they are unaware of. Therefore, it is crucial to educate employees on ways to protect themselves, for example by creating strong passwords and recognizing phishing scams.

> By identifying and efficiently delivering the right combination of security services for small business budgets, you can differentiate your business, add new value and revenue, and most importantly, build lasting partnerships with your clients.

MONITOR

The third step in delivering security services is continuous monitoring. An attack can happen at any time, in any place. By implementing the best practices mentioned above, you will have built a solid foundation for a secure environment. However, these best practices are ongoing processes. Software vendors launch new patches and updates every day and new threats develop in a matter of seconds. You will constantly have to enforce security settings and monitor your client's devices to proactively secure their business.

That is a big task that becomes more manageable when using the right tools. One approach is to use a comprehensive solution with monitoring and management capabilities for better protection and significantly simplified service delivery.

Summary

SMBs face a threat landscape that is ever evolving. The sophisticated threats and lack of awareness among employees result in insufficient protection. Managed security services present an opportunity to provide the strong, cost-effective cybersecurity protection that SMBs require to reduce their exposure to risk in today's online business world. These services can be delivered as an extension of your existing portfolios and enable you to not only protect your customers' data, devices, and people but strengthen your role as a proactive, IT expert and trusted advisor to them. By identifying and efficiently delivering the right combination of security services for small business budgets, you can differentiate your business, add new value and revenue, and most importantly, build lasting partnerships with your clients.

1, 2, 3, 4 Ponemon Institute, 2018 State of Cybersecurity in Small & Medium Businesses (SMB), November 2018
5, 6 AV-test, Security Report 2016/17, 2017

About Avast Business

Avast Business provides integrated, enterprise-grade endpoint and network security solutions for SMBs and IT service providers Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. The result is superior protection that businesses can count on. For more information about our managed services and cybersecurity solutions, visit **www.avast.com/business**.