Avast Business

White paper

5 cybersecurity issues SMBs should tackle to stay safe and how MSPs can help

The case for SMBs adopting affordable, easy to deploy, enterprise-grade security measures and why it's a new opportunity for managed security service providers

16 September 2021

In association with

IDG CONNECT

Avast Business

About the author

Rob Krug,
Senior Security Architect,
Avast Business

Rob has been in the network engineering and security space for over 30 years. His background includes extensive work with telecommunications, network design and management, and most importantly, network security. Specializing in security vulnerabilities, Rob has extensive experience in cryptography, ethical hacking, and reverse engineering of malware. Rob served in the U.S. Navy and also worked as a Data Security Analyst and Director of Engineering for multiple international service providers and vendors. Rob has designed, implemented, and maintained some of the most complex and secure networks imaginable.

What's the problem?

Psychologists have a term for it. Optimism bias. It refers to people that believe they are less likely to experience a negative event. To some extent, small and midsize businesses (SMBs), organizations of up to 1,000 employees, are guilty of this, especially when it comes to cybersecurity.

Even for those that do understand the scale of the threat, a lack of security expertise and resources leave them vulnerable to hackers. Enterprises are typically protected because they have sophisticated cloud-based, real-time detection systems, whereas SMBs are often left exposed and it hasn't gone unnoticed.

According to the **Verizon 2019 Data Breach Investigations Report,** 43% of cyberattacks target small businesses because they have rudimentary protection. And their situation is only going to get worse. With the **rise in contractors and freelancers,** more mobile workers, and an increase in BYOD — all accessing corporate networks -- the threats and vulnerabilities increase significantly.

SMBs cannot afford to be vulnerable. As **research** this year revealed, the cost of a data breach has risen 12 percent over the past 5 years and it is particularly acute for SMBs. In the study, companies with fewer than 500 employees suffered losses of more than $2.5 million on average.

So, what can SMBs do about it?

Firstly, they should take threats seriously and dispel any notion that SMBs are not on the hackers' radar. Secondly, they should start adopting robust, scalable defensive capabilities that can manage the associated risks of changing working practices and ways of doing business.

Helping SMBs become more secure is a huge opportunity for managed service providers (MSPs) and managed security service providers (MSSPs) who can provide their expertise and gain regular income from enterprise grade security tailored for SMBs.

Avast Business

1 Forget what you learned yesterday

Security appliances are no longer relevant to modern working habits

Times have changed. The modern workforce is about mobility, remote working, and flexibility to get the job done. As organizations increasingly rely on business units, and not IT departments, that determine which devices and applications are best for their employees, so the potential for risk increases. This decentralization potentially comes at a cost, a loss of control, a lack of security oversight.

With policies such as **BYOD growing,** SMBs have to take into account how business data is now being accessed and used outside of the confines of the business walls. Like enterprise businesses, SMBs are having to come to terms with the idea that the network perimeter is broken and the security implications of this shift are severe.

Many SMBs are using security appliances to protect their networks, but we estimate that up to 73 percent of web traffic may now be bypassing these appliances because most UTMs are not using SSL inspection features. Unless SMBs inspect SSL, all other security features are worthless!

SSL/TLS encrypted traffic has grown to over 73% while in practice, most UTMs are not using SSL inspection features. Unless SMBs inspect SSL, all other security features are worthless.

2 Don’t lose your head in the cloud

SMB security is being made redundant by change

Applications, data, and infrastructure management are moving to the cloud, so on-premise security is quickly becoming less effective and relevant. While SMBs increasingly **allocate more budget** for cloud computing capabilities, traditional security becomes less and less effective.

At best, on-premise appliances will only protect a fraction of company data, leaving the business exposed. In fact, we would go as far as to say that UTMs are no longer safe. Today’s small businesses using office-based security appliances are one click away from disaster or financial bankruptcy.

Avast Business

3 Keeping on-premise security appliances up to date can be a headache for SMBs

The nature of evolving working habits and a multitude of devices have piled pressure on SMBs to keep their security up-to-date. Given that new threat variants appear at an astonishing rate of 125,000 per day, this becomes an almost impossible task with limited resources and tight budgets.

Most on-premise appliances do not download threat definition files immediately, as new threat variants break into the wild. This leaves appliances exposed, allowing these new variants into the network before the definition lists are updated, so how can SMBs cope? Then there is the issue of scalability. How do growing SMBs, opening new offices or even remote locations, ensure that all sites are fully secure and that the network is not going to be exposed to hackers?

4 SMBs need enterprise-level protection

It's not unusual for an SMB to have a mixed bag of security applications and appliances from different vendors. This has not always meant that these SMBs have been secure, even without the growth of mobility. As **Gartner discovered,** even those businesses that had SSL features in appliances, most were turned off.

It's not necessarily incompetence. It is most likely a lack of appropriate skills. The problem facing most SMBs is that there are significant skills shortages around the globe when it comes to cybersecurity. Recent **research** revealed that this shortage is now affecting 74 percent of organizations and SMBs are being hit the hardest.

SMBs need expertise. How can SMBs be sure they are covered in increasingly complex threat environments, without spending a fortune on security systems?

This is where partners step in. MSPs and MSSPs have an opportunity to evolve and become MSSPs by providing value-added security services to SMBs. Avast's new SIG product can be the backbone of this, providing hardware-free, cloud-based, scalable security that leading Fortune 500 companies have migrated to. **[see The Secure Internet Gateway (SIG) and why it matters].**

Avast Business

5 Cybercriminals target SMBs

As we have said before, cybercriminals rely on SMBs having optimism bias. They want SMBs to think nothing is going to happen to them because it makes for a less challenging target. So, doing nothing is not an option.

SMBs, with the help of MSPs, need to reevaluate their protection and align it with modern business practices. They need to re-evaluate their existing appliances and identify potential weaknesses in their network and workforce devices.

SMBs need a strategy that covers mobility and remote working trends, taking into account public Wi-Fi use in hotels, airports, and cafes. They're in need of a better understanding of the risks they face, along with help developing a security solution that fits their budget and working habits.

SMBs need a strategy that covers mobility and remote working trends, taking into account public Wi-Fi use in hotels, airports, and cafes.

The Secure Internet Gateway and why it matters

How do we help MSPs help their customers?

By providing a scalable, enterprise-grade, cloud-based solution tailored for SMBs that will protect a network from breaches, such as threats hiding in SSL, zero-day attacks, and botnets that may be easily bypassing traditional security perimeters.

Its main features are:

- SIG performs high-speed, intelligent analysis of hard-to-inspect encrypted SSL/TLS traffic, ensuring a high level of protection and better performance with minimal management.
- SIG provides cloud-based sandboxing for zero-day protection, automatically scanning .exe and . dll files from unknown sites for cyberthreats. In case a threat is detected, it will be placed in the sandbox and an automatic block will be deployed for that object in realtime, across the entire network. Cloud-based firewall control that allows granular rules to be set by IP, port, and protocol. SIG takes minutes to deploy and is easy to scale across multiple offices and locations.
- SIG places no limits on throughput, eliminating bottlenecks caused by traditional UTM appliance security.

- SIG provides easy-to-read reports.
- SIG is easy to deploy and configure, even if you would like to deploy the advanced threat protection settings that block suspicious content, phishing, cookie stealing, anonymizers, crosssite scripting, etc.
- In SIG, you are also able to configure bandwidth control to ensure apps like O365 are prioritized.

Conclusion: The SIGnificance of SMB security

With increased threats, less IT expertise, and smaller budgets, MSPs and MSSPs should consider enterprise-grade, cloud-based security services suitable for SMB customers. These security services should not just protect the office — but secure the whole organization.

Security experts agree that the internet has become the new office perimeter. It must be defended in a comprehensive way, so that MSPs and MSSPs have an opportunity to respond, with expertise and an enterprise-grade solution at SMB pricing.

Defense against advanced threats should be as good for an SMB as it is for an enterprise but it should also be less costly and less complicated to procure, use, deploy, and update. SMBs need the help and expertise of partners to make that possible. It's an opportunity to grow, to establish new security solutions for SMBs, that combine cloudbased gateways, such as secure gateways and advanced endpoint security. It's about thinking outside of the box, moving away from hardware sales and maintenance, moving from MSP to MSSP and embracing on-going revenue from cloud-based solutions – keeping threats at bay and customers happy.

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**.