avast business

GUIDE

Break the Link Between Users and Cyber Threats

Careless users, infected emails and unsafe or hijacked websites are a menace to SMBs. Learn how a secure web gateway can stop cyber threats at the source.

In association with

IDG CONNECT

What's the problem?

The cyberthreat to small and medium businesses (SMBs) is more financially damaging than the combined threat of fire, flood, and transport strikes, according to one report. It's an indication of how cyber criminals now view SMBs as an easy and lucrative target. While the vast majority of reported cybersecurity breaches over the past 18 months have concerned large and well-known companies across the globe, including Facebook, Equifax, and British Airways, it is SMBs that are increasingly the target.

According to a study by the Ponemon Institute, three in five SMBs have experienced a cyberattack in the last 12 months and one in three believe they are not capable of fending off an attack. Verizon's 2018 Data Breach Investigations Report claims that SMBs account for 58 percent of malware attack victims in the US. Not many SMBs have impenetrable cybersecurity measures in place and the implications of an attack can be devastating resulting in significant monetary and reputational losses.

According to Barclays Bank, cybercrime fraud against SMBs cost $45,000 on average per business and have resulted in over 50,000 job losses. The statistics make damning reading and the pressure on SMBs to mitigate against online threats is only increasing. Preventing cyber attacks has to be a priority but of growing concern is the proliferation of infected websites that use SEO tactics to lure unsuspecting employees. SEO poisoning campaigns are increasingly sophisticated in their methodology.

As SMBs migrate to cloud-based networks, use digital apps, social media sites for publicity and training, search engines for research, and live casting and communication, they open a potential door to the company network. An increasing reliance on the cloud to streamline operations and enable mobility also poses a number of security challenges related to BYOD and new social engineering tactics that trick people into clicking on malicious websites. Tackling this becomes a priority.

Unlike enterprises, SMBs rarely have the resources to build intricate solutions (appliances, software, firewalls, etc.) to check all bad traffic or requests from malicious websites. There is also the people issue. Educating and training staff takes time and resources. A paper last year claimed that staff awareness and vigilance are key issues in preventing attacks. Seven in ten businesses think SMB employees dealing with cybersecurity are capable of doing so, but few have cybersecurity training (20 percent of SMBs) or have cybersecurity policies (27 percent).

A US consultancy recently found that attitudes are a problem, claiming in its report that 51 percent of small business leaders and 35 percent of employees said they don't believe their company is a target for cybercriminals.

Interestingly in this last report, respondents also admitted to widespread use of public Wi-Fi and not changing passwords for well over a year. The perception that small businesses are anonymous to hackers is not just wrong, it is a threat to the future viability of those businesses, especially with data protection fines. This is what hackers rely on, complacency.

As data analytics firm Fico suggests; 2019 has been touted as "the Year of Cyber Insecurity: 52 weeks in which companies of all sizes and industries will experience a new level of fear – and in some cases panic – in realizing their vulnerability to data breaches, hacking, and other cybercrimes."

How can resellers and MSPs help SMB customers improve security, especially if so few provide adequate staff training? How can they help them implement policies, manage devices, and prepare for the unexpected?

We believe there is a big opportunity.

What are the main threats?

Ransomware

According to Europol's Internet Organised Crime Threat Assessment (IOCTA) ransomware from phishing activity in particular was a major problem in 2018 and will continue to be dominant in 2019.

Spear phishing

ENISA reports that the number of phishing/spear phishing attacks was instrumental in the new record in data breaches reported in 2018.

Cloud-based working

Remote access to the network from coffee shops, airports and even home can be a threat if devices are not managed.

The Secure Web Gateway (SWG)

Five reasons why it works for SMBs

Gartner predicts that half of malware campaigns in 2019 will use some type of encryption to conceal delivery, command and control activity, or data exfiltration. SMBs need multiple layers of security but by implementing a key layer, such as Secure Web Gateway (SWG), SMBs can safeguard the source, the internet. SWG will help SMBs tackle their most pressing web security issues. Here are some of the key benefits

1

Total protection at high speed

Protect all devices inside the network and roaming laptops at home, a hotel, an airport, or a coffee shop. SWG offers secure managed devices anywhere on the network and Windows laptops and desktops outside of the network. It scans for poisoned DNS, phishing links, downloads and infected websites before web traffic reaches the network. SWG uses DNS-based lookups that take less than 2 milliseconds, so they won't slow your network down like appliances and proxy servers. Network traffic from employees and remote users is automatically directed to the nearest DNS server, delivering the highest performance.

2

Easy to set-up

Cloud-based and easy to deploy and manage. It takes minutes to set up and configure.

3

Easy to use

A simple, centralized console providing complete visibility of assets. This means SMBs can have complete oversight of any device on the network, and alert to any potential threats.

Real-time learning

New malicious sites are emerging every day but the SWG is prepared for this by constantly scanning and learning, sandboxing any executables that need to be analyzed further.

Designed for SMBs

The SWG is especially built for SMBs, offering security from the endpoint to the network. Not all SMBs have had the resources to deploy sophisticated cyber defences, until now.

Key features at a glance

- **Integrated endpoint and web security** - Blocks malicious downloads and known malicious URLs from entering the network.
- **Intelligent SSL** - Performs high-speed, intelligent analysis of hard-to-inspect SS traffic with only a microsecond delay.
- **Cloud sandbox** - Analyzes suspicious files and URLs in a virtual environment to detect hidden malicious content for all EXE files and DLL traffic.
- **Intelligent proxying** - Inspects, categorizes, and classifies a suspicious unknown site into a known good or bad site. You can easily add URLs to customized block/allow lists.
- **Content filters** - Allows you to choose from over 90 categories, the level of content filtering you want to enforce for an organization's users.
- Single pane of glass for centralized, simple management

Adding value for IT Service Providers

The Secure Web Gateway (SWG) brings layered security to a new level in the CloudCare platform. From a single, cloud-based dashboard, partners can remotely secure multiple clients and deliver pay-as-you-go services that enhance their protection and boost margins and profits.

The SWG is a great opportunity for resellers and managed service providers to:

Add another layer of security

for customers to mitigate against the increasing risk of SMBs being targeted by cybercriminals. This means reduced numbers of security incidents to manage and increased trust with customers.

Move away from appliance management

and deliver tailored security solutions, enabling customers to benefit from sophisticated cyber security regardless of budget.

Easily scale to add/remove users

as a customer evolves, keeping customers happy and secure as their needs change.

Increase monthly recurring revenue (MRR)

with new securityas-a-service offering, boosting profitability but also customer relationships and retention.

Deliver managed security remotely

– less need to send expensive experts into the field.

We have endpoint security so why do customers need SWG?

On-premise security appliances are limited in their ability. SMBs need a layered approach to ensure protection, which means more opportunity for partners.

What's wrong with on-prem appliances?

The problem is that on-prem appliances are inadequate in isolation. Remote employees can bypass on-prem appliances and advanced threats will not be detected. They also slow everything down. Amazingly 90 percent of SMBs turn off SSL inspection because of severe latency.

The bottom line

Fully scalable, enterprise grade cybersecurity solution that delivers advanced protection against web threats without the complexity and overhead of proxy servers or on-premise appliances.

In association with

IDG CONNECT

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.