WEBROOT
Smarter Cybersecurity™

SMBs Are Vulnerable to Malware Attacks

10 reasons MSP clients need a layered security strategy to stay safe

They say recognizing a problem is the first step in solving it. But when it comes to cybersecurity, many small- and medium-sized businesses don't believe they have a problem. Many simply believe that hackers will focus their attention exclusively on large and well-heeled organizations, and aren't interested in smaller businesses. Unfortunately, this couldn't be further from the truth, and this "it won't happen to me" mentality leaves them highly susceptible to attacks.

While some attacks do target large corporations, most still do not discriminate based on the size of organization. Hackers just want to compromise the network and its devices to steal any and all data they can sell or use for their own ends. And once they've hacked a network server, they can use it to launch attacks on others.

This means that, in our current, constantly evolving threat landscape, simply deploying an antivirus solution isn't enough. Only a layered security strategy that includes multi-vector protection can successfully fend off advanced, zero-day threats like ransomware, malware, and more.

1 It's not a matter of if your clients will get hacked, but when.

Many small businesses don't invest sufficiently in IT security resources and protection. This may be due in part to the fact that they may not know they're being targeted. According to the Ponemon Institute 2016 State of SMB Cybersecurity Report, hackers have breached 50% of the 28 million small businesses in the United States.

2 The threat landscape evolves constantly.

Trying to keep pace with the changing nature of cyber threats is a full time job in and of itself. Many small- to medium-sized businesses cannot afford the cost of full-time IT security staff, which is why it's imperative that their MSP keep them protected from zero-day threats.

3 End users may not know security best-practices.

In the last year, phishing was involved in 90% of breaches, which makes end users both the weakest link and the first line of defense for SMBs. The best way to counter this threat is to continually train and educate users on the risks their behaviors. A well-trained user base can help prevent threats like ransomware, drive-by downloads, keyloggers, and many more.

4 Lack of effective security policies and protocols.

Ensuring all passwords are strong and regularly changed is a given, but it should be supplemented with strong, two-factor authentication. Access rights to network files, folders, and file shares need to be tightly controlled to avoid malware wreaking havoc on networks.

5 Exposure to multi-vector attacks.

All the ways your clients' users interact with the internet need to be considered, from emails, attachments, links, and browser, to web browsing and network activity. Effective endpoint security is vital to protecting all these vectors from cyberattacks. It should feature multi-vector protection to defend your clients from threats that use many different exploits to attack.

6 Complex security platforms create administration challenges.

Consider not only the costs of buying cybersecurity software, but also the operational expenses. Systems that integrate best-of-breed solutions and have a high degree of automation make security both more effective and more affordable. Plus, they make the administrator's job much easier.

7 Out-of-date systems create vulnerabilities.

By following a rigorous patching regime, your clients can avoid many of the application vulnerabilities used to compromise networks. Patching can be an onerous process, but many automated services are available to make it easier, more effective, and more affordable. News-making breaches like WannaCry could have been avoided by simply patching.

8 No network visibility.

Having accurate information about your network (and what is connected to it) is vital in protecting it from both internal and external threats. Effective network monitoring tools can identify network anomalies and counter threats before they do damage.

9 Poor data backup practices.

Faced with attacks like ransomware, SMBs must have an effective back-up regime. Sixty percent of small companies that suffer a cyberattack are out of business within six months. There are many on and off-premise cloud-based backup systems that will help you avoid such a fate, as even paying the ransom these days is no guarantee you will get your data back.

10 Compliance issues.

Regulations affect many industries, and effective endpoint security is a routine compliance requirement. It is vital to understand your clients' compliance obligations and ensure they have sufficient cybersecurity in place.

Many of the security issues raised in this list are solved by Webroot SecureAnywhere® Business Endpoint Protection, featuring multi-vector protection and our MSP-tailored Global Site Manager console. It gives SMBs the peace of mind to know they're protected from threats like the ones above, and it increases profitability and management capabilities for MSPs.

About Webroot

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.