WEBROOT
Smarter Cybersecurity™

Smarter Cybersecurity™ Solutions for Small and Medium-sized Businesses

Antivirus and Antimalware in One

Table of Contents

Background

Perhaps the most important software decision a small or medium-sized business (SMB) should concern itself with is endpoint cybersecurity, also known as antivirus or antimalware software. Endpoint cybersecurity solutions are still characterized by a huge gap between their relatively minimal purchase price and the enormous costs they can entail if they fail to work properly.

The typical cost of endpoint security for a single device and user varies according to functionality, but the price commonly ranges between $20 per year to $35 per year, per device. However, the potential financial and productivity losses suffered by small business which has chosen inadequate antivirus protection is extremely disproportionate. A single malware breach or other security failure easily dwarfs the upfront cost of endpoint protection. The cost of infection damage can range from paying a ransom demand, to system downtime and diminished user productivity, to lost sales revenues and even potential legal liability claims relating to compromised customer records or other private information.

Combating the alarming volume, velocity, and variance of today's security threats has become significantly more challenging as cybercriminals employ an extensive range of sophisticated new techniques, including polymorphism and spear phishing, to defeat traditional antivirus defenses. And, because small to medium sized businesses often lack skilled in-house IT security resources, they are ruthlessly targeted.

Despite the rapidly-evolving threat landscape—and the substantial financial hardships it can impose on small businesses—many SMBs still underestimate the importance of installing an optimum cybersecurity solution. By focusing solely on the modest acquisition expenses of new antivirus products, they overlook the significant business consequences and significant costs that choosing the wrong endpoint cybersecurity can entail.

"We heard about Webroot from one of our vendors who recommended it quite highly. We were planning on trialing Webroot for a month, but after 10 days, we signed up for 100 licenses, and then increased it further by 40 as more endpoints were added to the network. The level of efficacy, which was like night and day compared to our previous solution, was exactly what we were looking for. "

– Uzair Shah, Senior Network Engineer at Lennock Motors

The Drawbacks of Multi-Solution Cybersecurity Strategie

In an effort to overcome the risks posed by today's threat landscape, some SMBs have resorted to installing a combination of two separate and distinct cybersecurity products. They typically combine an antivirus with an antimalware, anti-exploit, or anti-ransomware solution. The motivation for this approach often stems from being infected at regular intervals because of new threats that well-established antivirus solutions are unable to stop.

For example, one of the most disruptive and prevalent security threats right now is ransomware. It's designed to extort money from businesses by denying them access to their PC and, in some cases, network files. Because of the complex encryption strategy it utilizes, such malware is nearly impossible to remediate once it has infected a system and spread into the network. The best protection against such infections requires a multi-layered preventive approach. Unfortunately, adding a second endpoint security layer, even if you have chosen your primary endpoint security carefully, is often a poor solution to the problem. Whatever endpoint solution you deploy will only be effective until the attacker has invented new ways to get around it; never mind the additional costs and complexity to providing adequate security.

"The multiple endpoint security solution approach entails several downsides, but higher cybersecurity purchase cost is not among them. That expense is still relatively trivial. Instead, it is the increased cost in time imposed on IT staff and the lack of any in-product automation that impedes any operational benefits. The man-hours needed to deploy and manage a typical signature-based antivirus can be substantial, and they become even more onerous when you use two separate products to ensure complete protection from the latest malware threats, such as ransomware."

Whenever a cybersecurity vendor releases signature updates, you must download those updates and schedule distribution from the dedicated server to every desktop and endpoint device in your IT environment. Best practices dictate testing any updates first, but using two cybersecurity solutions requires evaluating two sets of updates. Your IT staff may be tempted to push out both sets of untested signatures, which can result in crashed systems and significantly diminished user productivity.

Further productivity losses can also be traced to the use of multiple cybersecurity solutions. Traditional antivirus client software compares every file on the user's computer against the myriad definitions in the signature database within the client. These scans consume a huge amount of processing power, so much so that an end user's computer is rendered unusable during scans. These signature-based slowdowns are a leading source of user discontent, and they become far more disruptive and extensive when imposed by two separate cybersecurity solutions.

Additional drawbacks to the multiple-solution approach include the need to learn the different user interfaces and management dashboards for each of the separate solutions. This makes management far more time-consuming for IT staff. Also, the simultaneous use of multiple cybersecurity solutions introduces the potential for operational conflict, a particularly challenging problem as cybersecurity is not typically designed for concurrent duty with another endpoint security product.

Why a Single Cybersecurity Solution is Better

Webroot has applied modern technologies and methodologies to its endpoint security solutions, resulting in single offerings that deliver fundamentally superior protection, ease of use, and performance compared with any combination of conventional cybersecurity products. As a result, SMBs now have greater security and peace of mind by deploying just one security solution. In so doing, they will not only save money and simplify the deployment and management of endpoint protection, but also significantly strengthen their security and reduce their day to day costs.

The most obvious characteristic differentiating Webroot endpoint security solutions from competitors is their completely cloud-based architecture. This enables the use of a lightweight client (under 1 MB), because no signature database is stored within the client software. Instead Webroot maintains a massive signature database in the cloud. This approach combines far better protection, quicker installation, and faster scanning. Average scans complete in a matter of seconds, reducing IT overhead while improving productivity and uptime.

Smarter Cybersecurity™ solutions use cloud-predictive behavioral intelligence to discover malware as soon as it attempts to infect your devices. And, because Webroot endpoints collect over 200 gigabytes of behavioral execution data each day, Webroot solutions become more powerful every minute, strengthening their ability to automatically detect ransomware and other new infection variants before they can infiltrate and make changes to your endpoints.

Conclusion

Cobbling together multiple cybersecurity products to ensure you have adequate endpoint protection is clearly not a strategy most businesses favor. It is a costly and complex attempt to compensate for the inherent deficiencies of conventional signature-based cybersecurity. There is a better way.

Simply put, Webroot maximizes your security, cuts bandwidth utilization, reduces resource loads on PCs, and shrinks cybersecurity disk space use. All the while, its centralized console streamlines management, saving you time and money on administration of your endpoint devices; while the agent itself automatically remediates infections.

Equally important to its functionality, Webroot protection provides you with the enterprise-level security without requiring on-site enterprise-level security expertise. Small and medium sized businesses have reported not only significantly better infection statistics since deploying Webroot solutions, but also saving 50% or more money than with their previous solutions.

About Webroot

Webroot delivers next-generation network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions, BrightCloud® Threat Intelligence Services, and FlowScape® network behavioral analytics protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at www.webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900