WEBROOT®
Smarter Cybersecurity™

Smarter Cybersecurity™ Solutions

TABLE OF CONTENTS

BACKGROUND

Perhaps more than any other type of software solution a reseller can offer to its customers, endpoint security products are characterized by a huge gap between their minimal purchase prices and the enormous costs they can entail for clients if they fail to work properly. The financial benefits of retailing cybersecurity solutions are modest (typical direct purchase prices are $24/year per seat, with VAR cost roughly $12), while the potential losses suffered by a VAR's customer due to malware infections can be devastating.

Such costs can range from system downtime and diminished productivity to lost sales revenues and even potential legal liability for claims relating to any private information that may have been compromised. 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 (polymorphism, spear phishing, etc).

Despite the rapidly-evolving threat landscape—and the substantial financial hardships it can impose on resellers' customers—many VARs still underestimate the importance of offering the optimum cybersecurity solution. By focusing on the modest acquisition expenses of antivirus products, VARs may tend to overlook the significant business consequences and huge costs for its customers that choosing the wrong endpoint security solution can entail.

"What's more, the damage from virus and malware infections also affects VARs. Customer dissatisfaction and frustration arising from such incidents undermines trust in the VAR and with it the likelihood of long-term patronage (and thus its recurring, predictable revenue). It also jeopardizes a VAR's ability to cultivate a trusted advisor relationship with its customers that can open up a multitude of other business opportunities."

DRAWBACKS OF MULTI-SOLUTION CYBERSECURITY STRATEGIES

In an effort to deliver more comprehensive protection to their customers, some VARs have resorted to recommending a combination of two separate and distinct cybersecurity products. The motivation for this approach often stems from the presence of new threats that many well-established antivirus solutions are unable to address.

For example, CryptoLocker is a new and highly disruptive security threat, belonging to a family of malware called "ransomware." It's designed to extort money from victims by denying them access to their personal files. Because of the complex encryption strategy it utilizes, such malware is nearly impossible to remediate once it has infected a customer's computers. The best protection against such infections requires a preventive approach.

Unfortunately, VARs have found that a substantial number of high-profile cybersecurity solutions are ineffective in preventing such infections, and thus have been forced to add a second solution to their customer recommendations.

"This approach entails several downsides, but higher cybersecurity solution purchase costs for the VAR's customer is not among them. That expense is still relatively trivial. Instead, it is the increased cost in time imposed by multiple cybersecurity solutions that can frustrate and alienate customers. The man-hours needed to deploy and manage a typical signature-based antivirus can be substantial, and they become even more onerous when customers must use two separate products to ensure complete protection from the latest malware threats such as CryptoLocker."

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

Further productivity losses can also be traced to the use of multiple cybersecurity solutions. Traditional cybersecurity 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 customer 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 for customers to learn the different user interfaces and management dashboards for each of the separate solutions. This can make management far more time-consuming for the customer's IT staff. Also, the simultaneous use of multiple 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 cybersecurity solutions, resulting in single offerings that deliver fundamentally superior protection, ease of use, and performance to customers compared with any combination of conventional cybersecurity products. As a result, resellers can provide greater security and peace of mind to their customers with just one solution. In so doing, VARs will not only help their clients save money and simplify the purchase, deployment and management of endpoint protection, they'll also significantly strengthen their business relationships with those customers.

The most obvious characteristic differentiating Webroot endpoint cybersecurity 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 your customer's IT overhead while improving its productivity and uptime.

Smarter Cybersecurity™ solutions from Webroot use cloud-predictive behavioral intelligence to discover malware as soon as it attempts to infect your customer. 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 new infection variants before they can infect and make changes to the computer.

CONCLUSION

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

Simply put, Webroot maximizes your customers' security, cuts bandwidth utilization, reduces resource loads on PCs, and shrinks cybersecurity disk space use. All the while, its centralized online console streamlines management, saving your clients time—and money—on administration of their endpoint devices. Equally important, it cements your status as a trusted advisor to your customers by demonstrating an ability to deliver the best solutions available.

About Webroot

Webroot provides Smarter Cybersecurity™ solutions. We provide intelligent endpoint protection and threat intelligence services to secure the Internet of Everything. By leveraging our cloud-based collective threat intelligence platform, computers, tablets, smartphones, and more are protected from malware and other cyberattacks.Our award-winning SecureAnywhere™ intelligent endpoint protection and BrightCloud® threat intelligence services protect tens of millions of consumer, business, and enterprise devices. Webroot technology is trusted and integrated into market-leading companies including Cisco, F5 Networks, HP, Microsoft, Palo Alto Networks, RSA, Aruba and many more. Webroot is headquartered in Colorado and operates globally across North America, Europe, and the Asia Pacific region. Discover Smarter Cybersecurity solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
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