WEBROOT®

How Resellers Can Become the Trusted Advisors on Security Issues

Boosting Customer Satisfaction and Loyalty with Superior Antivirus Protection

MAY 2014

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Providing superior IT solutions to customers not only differentiates VARs from their competitors, it also establishes a foundation of trust upon which a VAR can build a lasting advisor relationship with its customers. Becoming a trusted advisor requires that VARs make a concerted, continuous effort to learn not only about their clients' business operations, but also about the optimum IT solutions for those customers – and that often means refusing to settle for the status quo.

It's not surprising that conventional antivirus (AV) solutions provide conventional (and unremarkable) results; nor is it surprising that many customers and VARs view AV products as necessary evils, offering some malware threat protection but at the cost of considerable customer frustration and dissatisfaction. VARs who settle for mediocre AV products ultimately encourage customers to view the VAR as equally undistinguished.

Delivering truly exceptional endpoint security – thus building credibility and trust with the VAR's customers – demands a fundamentally new approach... precisely what Webroot solutions employ. The cloud-based Webroot® architecture combines far better protection, quicker installation and faster scanning. Because Webroot provides unrivaled protection that imposes virtually no penalty on system performance, customer satisfaction (and with it, long-term patronage and recurring, predictable revenue for VARs) significantly increases.

ESTABLISHING A FOUNDATION OF TRUST

Introduction

While the specific issues VARs face vary widely, there is one universal challenge that every reseller should undertake—positioning itself as a trusted advisor to its customers. Achieving this goal can pay enormous dividends to customers and VARs alike; clients will benefit from solutions that more efficiently and cost-effectively meet their business needs, and VARs will cultivate long-term customer relationships that generate recurring, predictable revenue.

Of course, building such trust is an iterative process; it doesn't happen overnight. It requires that VARs make a concerted, continuous effort to learn not only about their customers' organizations and operations, but also about the IT solutions that will best meet the requirements those operations entail. Simply put, that means refusing to settle for the status quo.

Back in the 1980s, a widespread truism held that "Nobody ever got fired for buying IBM." Given the uncertainties that pervaded a then-nascent computer industry, the notion of playing it safe with a long-established vendor was very appealing. However, as both the diversity and sophistication of IT solutions have steadily grown, the impulse to reflexively choose solutions only from familiar "brand-name" vendors often proves counterproductive.

Solution Selection and VAR Accountability

Endpoint security and antivirus solutions are available from a wide variety of vendors, some with a marketplace presence that spans decades. This familiarity makes it relatively easy for VARs to sell these solutions to their customers.

"Unfortunately, by treating endpoint security solutions as commodities, VARs are actually encouraging their customers to see their VAR as a commodity too; just another reseller who provides the same choice of archaic, signature-based AV solutions from well-known vendors that countless other VARs offer."

Of course, customer satisfaction – and the trust in the VAR that it engenders – does not come from selling well-known AV solutions, it comes from consistently delivering superior results to customers. Unfortunately, some of the most longest-lived AV solutions on the market today rely (perhaps not surprisingly) on a fundamental approach to endpoint security that hasn't materially changed in over 25 years. Their archaic, signature-based architectures provide mediocre protection from malware threats, while imposing tedious management tasks and system slowdowns.

Obviously, such poor results will lead to significant customer dissatisfaction. While some customers may hold the AV solution vendor responsible, many will simply lay the blame at the feet of their VAR: "We paid you to deliver effective endpoint protection, and you let us down. We don't care that you selected a widely-known AV solution—we could have done that ourselves—all we care about are results." In such cases customer satisfaction, and trust in the VAR, are clearly undermined.

AV Solutions as Commodities

Given the relatively weak protection from malware threats that numerous endpoint security products provide, it comes as no surprise that many resellers regard AV solutions as a necessary evil: VARs must supply these products to satisfy their clients' demands, and grudgingly resign themselves to the inevitable infections, time-consuming remediation and consequent customer complaints and frustration that such solutions typically entail.

This sense of resignation towards AV solutions stems from a widespread belief that there is little to differentiate one AV product from another. As such, VARS often review the particular features of solutions from high-profile AV vendors such as Symantec, McAfee, Trend Micro or Kaspersky and then choose what seems to be the best match for their customer's needs. Beyond their specific feature sets, many VARs have come to see AV products as little more than interchangeable commodities.

Unfortunately, by treating endpoint security solutions as commodities, VARs are actually encouraging their customers to see them as a commodity too; just another reseller who provides the same choice of archaic, signature-based AV solutions from well-known vendors that countless other VARs offer.

Standing Apart from Other Resellers

To overcome this perception of VARs as commodities and differentiate themselves from their competition, VARs must establish greater credibility with their customers by demonstrating a fundamental understanding of the challenges and issues that conventional AV products pose. By clearly identifying the problems that customers experience, a VAR is far better positioned to resolve those problems – and thus build greater trust and loyalty with those clients:

» Traditional AV 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 CPU power, so much so that during such scans an end user's computer is essentially rendered useless. These signature-based slowdowns are a leading source of customer discontent, and signature files cause still more headaches.

» Whenever an AV vendor releases signature updates, a VAR's customer must download those updates and schedule when they can be pushed out from its dedicated server to every desktop and endpoint device in the customer's IT environment. Best practices dictate testing any updates first, but the sooner new signature definitions are distributed, the sooner end users are protected. Thus a customer's IT staff may be tempted to push out untested signatures, which can result in crashed systems and more dissatisfaction.

» By far the most damaging consequences for a VAR occur when its AV/endpoint security solution simply fails to prevent malware infections. These infections result in system downtime and lost productivity for its customers, while significantly diminishing satisfaction with their VAR. To repair the infected machine(s), IT departments (or the VAR, under a break-fix contract) may need hours of time to locate, diagnose and remediate the problem. In either case, client frustration and displeasure will follow.

» Malware threats are pervasive: according to survey results in a UBM TechWeb study , 80 percent of the respondents said their companies had been breached in the past 12 months.

BUILDING CUSTOMER TRUST WITH WEBROOT PROTECTION

Webroot: Modern Solution for Modern Threats

It's becoming increasingly clear that archaic, signature-based endpoint security solutions are incapable of effectively combating the alarming volume, velocity, and variance of today's threats. Cybercriminals are employing an extensive range of sophisticated new techniques (polymorphism, advanced persistent attacks, phishing, etc.), so it makes sense that modern endpoint protection solutions require a comparable commitment to innovative technologies.

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.

Webroot® security solutions 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 a CryptoLocker infection variant before it can infect and make changes to the computer.

The net result is that customers protected by Webroot security solutions can breathe a sigh of relief as they read more news articles about the havoc that CryptoLocker has wrought on other companies, and will remark on how their VAR's choice of Webroot SecureAnywhere® Business solutions has once again prevented their business operations from being disrupted.

Boosting Customer Productivity from Day One

The most obvious characteristic differentiating Webroot SecureAnywhere solutions from competitors is the completely cloud-based Webroot 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.

A recent PassMark Software study[2] compared Webroot SecureAnywhere Business Endpoint Protection with seven traditional endpoint security products and found Webroot delivers significant advantages in several areas, including:

» Installation size (see Figure 1)

» Memory Usage During System Idle (See Figure 2)

» Scheduled Scan Time (See Figure 3)

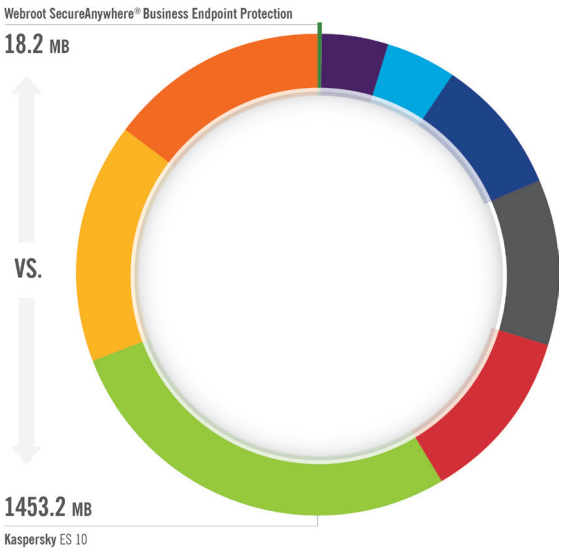
» Memory Usage During Intial Scan (See Figure 4)

» Installation Time (See Figure 5)

To ensure continuous client protection, Webroot solutions can be installed over existing AV solutions, which may then be removed later. In this way, a VAR can be assured there's no period of time in which its customers' machines might be exposed to infection.

FIGURE 1: Installation Size

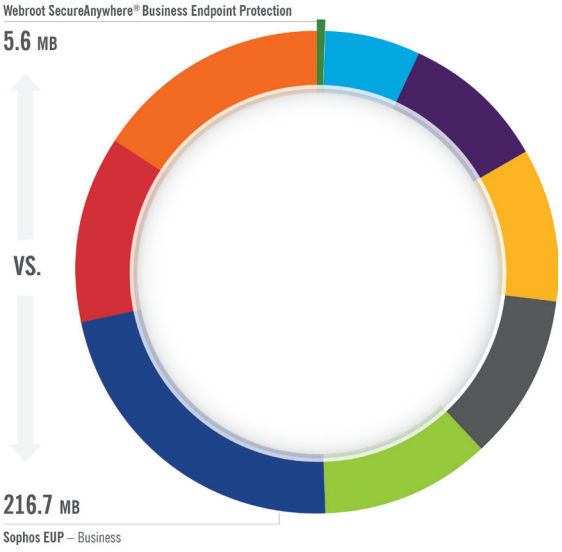
Webroot takes up 98% less space than Kaspersky™



This metric compares the total size of files added during the installation of endpoint security products. The test measures the minimum Installation Time a product requires to be fully functional and ready for use by the end user. Products with lower installation sizes are considered better performing products in this category.

FIGURE 2: Memory Usage During System Idle

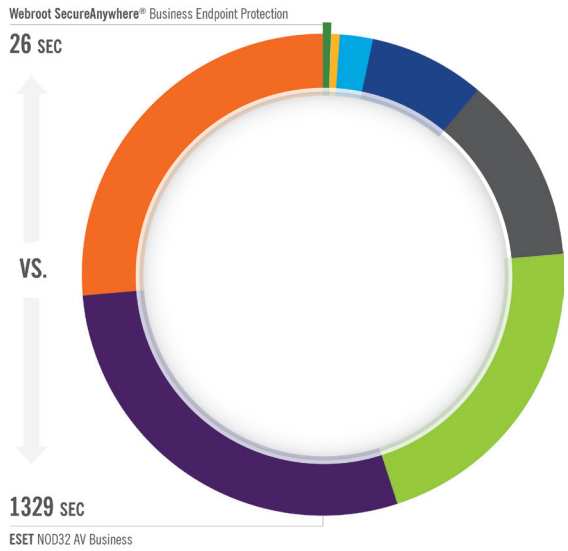
Webroot uses 97% less memory than Sophos®



This metric compares the average amount of RAM in use by an endpoint security product during a period of system idle. This average is taken from a sample of ten memory snapshots taken at roughly 60 seconds apart after reboot. Products with lower idle RAM usage are considered better performing products in this category.

FIGURE 3: Scheduled Scan Time

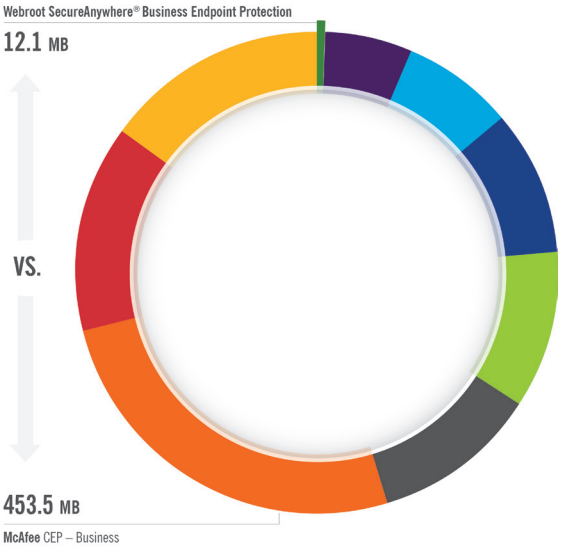
Webroot scans more than 51x faster than ESET®



This metric compares the average time taken to run a scheduled scan on the system. The scan is configured as a full system scheduled scan from the user interface. The default scheduled scan settings are kept (except for the start time) and the scan is scheduled to run at the next convenient time.

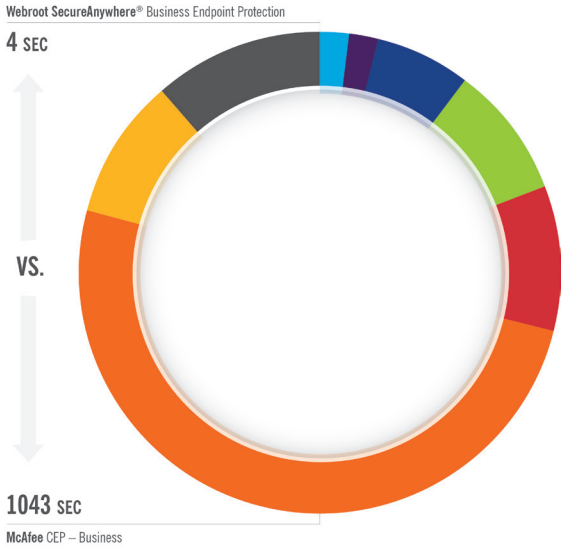
FIGURE 4: Memory Usage During Initial Scan

Webroot uses 97% less memory than McAfee®



This metric measures the average amount of RAM in use by an endpoint security product during an initial scan on the main drive. Products that use less memory during a scan are considered better performing products in this category.

FIGURE 5: Installation Time
Webroot installs 260x faster than McAfee®



This metric measured the minimum installation time it takes for endpoint security products to be fully functional and ready for use by the end user. Products with lower installation times are considered better performing products in this category.

From the end user's perspective, the most immediate benefit of cloud-based protection is the remarkable boost in system performance. By placing far less burden on a protected device's CPU and system resources than legacy AV solutions, Webroot solutions' background activity is virtually invisible to end users.

Maximizing Customer Security (and Satisfaction)

For a VAR, the single most important criterion when evaluating any endpoint security solution is its ability to keep customers protected. As noted earlier, Webroot solutions are always connected to an immense cloud-based signature database of malware threats (the Webroot® Intelligence Network) that is much more comprehensive, detailed and effective than any AV client-contained signature database could ever be.

"As today's VAR space becomes more competitive, the ability for any VAR to differentiate itself from other resellers becomes increasingly important. Providing a more effective AV solution is a sure way to increase customer satisfaction, and perhaps more importantly, cultivate a trusted advisor relationship for a VAR with its customers that can open up a multitude of other business opportunities."

But that's only one of the reasons Webroot SecureAnywhere® solutions deliver far greater protection from viruses and malware than conventionally-architected competitors. Webroot uses predictive intelligence to monitor the behaviors of applications and executables running on an end user's system. Should the Webroot client identify suspicious behavior, its first step is to immediately query the Webroot Intelligence Network to see if this suspicious behavior has been observed before. As every Webroot client around the world is continuously connected to the Webroot Intelligence Network, new info on emerging threats is constantly added.

If Webroot determines that the suspect file is indeed malicious, it captures the unique fingerprint, or hash value, for that file and uploads it to the Webroot Intelligence Network in real time. From that moment on, any other system in the world connected to the Webroot Intelligence Network is protected from this new threat. If it appears anywhere else, the Webroot software agent will instantly block it.

In the unlikely event that an infection does occur on a Webroot-protected machine, the process to remove the infection is much easier and far faster than on conventionally-protected systems. Using rollback remediation capability, Webroot SecureAnywhere® Business Endpoint Protection can undo every action that a malicious piece of software executed and return the machine to its state prior to the infection—in far less time than required by traditional AV solutions.

Conclusion

As today's IT landscape becomes more competitive, the ability for any VAR to differentiate itself from other resellers becomes increasingly important. Providing a more effective AV solution is a sure way for VARs to increase customer satisfaction, and perhaps more importantly, cultivate the trusted advisor relationship with its customers that can open up a multitude of other business opportunities.

Webroot has applied modern technologies and methodologies to its endpoint security solutions, resulting in AV products that deliver fundamentally superior protection, ease of use and performance compared with outdated competitors. Webroot AV solutions make it possible for resellers to provide greater security and peace of mind to their customers, but also to develop stronger and more collaborative connections with those customers.

About Webroot

Webroot is bringing the power of cloud-based software-as-a-service (SaaS) to internet security with its suite of Webroot SecureAnywhere® solutions for consumers and businesses. Founded in 1997 and headquartered in Colorado, Webroot is the largest privately held internet security organization based in the United States – operating globally across North America, Europe and the Asia Pacific region. For more information on our products, services and security visit www.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