WEBROOT
Smarter Cybersecurity

# Lowering MSP TCO for Endpoint Security Solutions

*Bottom-line Benefits of Cloud-based Antivirus Architecture*

## TABLE OF CONTENTS

## EXECUTIVE SUMMARY

The MSP business model reflects a more modern, efficient approach to IT infrastructure management that benefits MSPs and clients alike. Yet one aspect of MSP operations—the deployment and administration of endpoint security (antivirus) solutions—remains tied to outdated technologies and methodologies. The result is time-consuming, labor-intensive tasks for the MSP, and diminished system performance and more malware-related downtime for its clients.

Many MSPs have simply resigned themselves to the notion that endpoint security solutions are a loss leader, a source of little revenue, and require grossly disproportionate labor expenses. They accept the inflated TCO such solutions entail and hope to recover any losses with the other products and services they offer.

Reducing the MSP's TCO for endpoint security requires a fundamentally new approach. The cloud-based architecture from Webroot calls for less investment in associated infrastructure, enables faster deployment, and requires much less labor-intensive management. Most importantly, Webroot delivers dramatically better protection from malware threats, as well as timely remediation in the unlikely event an infection occurs.

Webroot significantly reduces the amount of time an MSP's technicians must devote to malware-related tasks, driving down Webroot's TCO and boosting an MSP's profitability. Because Webroot provides clients with unrivaled protection that imposes virtually no burden on system resources, MSP client satisfaction also grows.

## I. COSTS OF ARCHAIC ENDPOINT SECURITY

### A. Background: Emergence of MSPs

The growing power and sophistication of business IT solutions has yielded a commensurate increase in their complexity and difficulty of management, so much so that many small and medium-sized businesses (SMBs) are turning to outside companies for more comprehensive help. In the past, SMBs might have relied on a part-time IT person or one in-house employee to handle the day-to-day management of the IT infrastructure they purchased from their reseller, who merely provided break-fix services as needed.

Forward-thinking resellers realized such IT management responsibilities placed an onerous burden on smaller companies without dedicated IT departments, so these resellers began transitioning their businesses to a more service-oriented model. Aided by the advent of cloud technology, some resellers have evolved to the point that they classify themselves as managed service providers (MSPs). The result is that SMBs can now simply pay monthly service fees to an MSP who leases out and maintains the business' entire IT infrastructure.

This seemingly simple business model offers profound benefits for clients and MSPs alike. SMBs are no longer responsible for managing their IT environment, freeing them to focus on their core business. By converting their IT infrastructure from a capital expenditure to an operational expense, they streamline their financial profile, which eliminates the need to account for periodic cap-ex on equipment, such as purchasing new server hardware every three years.

Furthermore, outsourcing IT to MSPs significantly reduces costs. According to a CompTIA study, among the respondents who currently used managed services, 46 percent cut their annual IT expenditures by 25 percent or more by moving to managed services—including 13 percent that had decreased their annual IT expenditures by 50 percent or more. An additional 50 percent of organizations saved between one percent and 24 percent in IT costs annually.

These are compelling advantages to any client and explain why an increasing number of SMBs are outsourcing their IT needs to MSPs. In addition, the benefits to MSPs themselves are similarly striking. By establishing a recurring, predictable revenue stream from their clients, MSPs can significantly increase the valuation of their business (up to 3x-5x revenue vs. 1x for a typical reseller). The critical nature and customization of the services MSPs offer their clients combine to reduce churn, maximize long-term customer retention, and boost MSP profits.

With so many positive factors influencing the future of the MSP marketplace, it's important to remember that an MSP's success is still contingent on the quality of the solutions it offers. Unfortunately, there is one category of solutions that stubbornly continues to undermine MSP efficiency and profitability, as well as client productivity and satisfaction: endpoint security.

### B. Endpoint Security as Loss Leader

MSPs typically view endpoint antivirus security solutions as a necessary evil because they must be offered to satisfy client demand, but generate little or no revenue—the average cost of an antivirus solution is $24/year per seat, with MSP cost at approximately $12. These solutions frustrate clients with reduced system performance and bouts of virus-related downtime, as well as costly MSP tech hours to remediate. The source of these problems can be traced back to a traditional approach to endpoint security that hasn't truly changed in over 25 years.

This approach is still employed by many high-profile endpoint security solutions. First, it requires a dedicated server in the customer's environment on which to run the endpoint software and its administrative capabilities. Then it also demands that sizeable pieces of software be installed on every endpoint device to be protected. The need for these bulky software clients, whose install footprints often exceed 500 MB, can be attributed to reliance on an outdated technique called signature-based protection.

1 CompTIA, Trends in Managed Services, October 2011

*At best, a traditional antivirus solution protects an MSP's customers from infection but at the cost of sluggish performance. The software compares every file on the user's computer against the numerous definitions in the signature database within the client. These scans consume so much CPU power that the user's computer is rendered virtually useless until the scan completes.*

By nature, traditional endpoint security is reactive—it can only protect customers from an unknown piece of malware after that threat has caused an infection somewhere in the world. Once that infection has taken place and the malware is isolated and identified, security vendors can then write a new signature, or virus definition file, to protect all other customers from that same piece of malware.

Of course, such signatures need to be updated very frequently. With tens of millions of new pieces of malware appearing every month, security vendors must constantly add to already bloated signature files to incorporate the latest identified threats. And even that may not be enough. Cybercriminals are now using a technique called polymorphing, which enables malware to actually morph into a different form every time it infects a new system, requiring yet another unique signature. As more signatures are added to the client software on every protected machine, that client's footprint can easily exceed 1 GB.

## C. Slowdowns and System Crashes

Not surprisingly, many MSPs consider endpoint security products as a drain on their operations. At best, a traditional antivirus solution protects an MSP's customers from infection but at the cost of sluggish performance. The software compares every file on the user's computer against the numerous definitions in the signature database within the client. These scans consume so much CPU power that the user's computer is rendered virtually useless until the scan completes. Some MSPs try to work around this performance impediment by running scans during low usage times, but that leaves long windows during which clients may be more vulnerable to infection.

Signature-related slowdowns are a leading cause of customer dissatisfaction, as well as headaches for MSPs.

*The MSP suffers the opportunity cost of utilizing skilled, billable resources on unprofitable tasks, faces the potential loss of client fees due to triggered SLA payouts, and has jeopardized its ability to retain that client as a long-term customer (and a source of ongoing revenue) due to the MSP's clear failure to protect the client from a malware threat and consequent downtime.*

Whenever a security vendor releases signature updates, an MSP must download those updates and schedule deployment from the dedicated server to every desktop and other endpoint devices in the client's environment. This process is inherently labor-intensive and time-sensitive. Best practices dictate testing any updates first, but the sooner the latest signature definition packs are distributed, the sooner clients are protected. Thus MSPs may push out untested signatures, which can result in crashed systems—causing more work for the MSP, further fueling customer dissatisfaction.

However, the most damaging consequences for an MSP occur when its endpoint security solution simply fails to prevent malware infections. These infections result in system downtime and lost productivity for customers, while significantly diminishing their satisfaction with their MSP. To repair infected machines, the MSP typically sends a technician to the client's facility. Once there, the tech may need hours to locate, diagnose, and remediate the problem. As shown below, this can be a costly process for the MSP.

## D. MSP Costs of Ineffective Endpoint Security

To better appreciate the significant time and expense that an infected client machine can impose on an MSP, consider the following scenario that details the sequence of events following a typical malware breach:

| Malware Breach with Conventional Antivirus Solution | | |
|---|---|---|
| Step 1 | Client's computer crashes outright or ceases to operate normally. Client contacts MSP, who must first ascertain the nature of problem. At times this can be done remotely, but often requires the presence of an MSP technician onsite. | Non-billable MSP tech time begins |
| Step 2 | MSP tech examines affected machine to isolate root cause of problem, concludes that it has been infected by some type of malware. | Estimated MSP tech time used: 2 hours |
| Step 3 | Tech contacts support desk of endpoint security vendor, sends logs from infected system to vendor support for analysis and diagnosis. Depending on quality of support staff, process can be lengthy and convoluted to determine exact nature of breach. | Estimated MSP tech time used: 3 hours |
| Step 4 | Vendor support confirms that infection has occurred. If no definition file has been created, the MSP tech must wait until the vendor provides the definition. Tech can attempt to use one or more third-party tools in effort to clean machine, remove infection. Some MSP techs may elect to skip this process and proceed directly to step 5. | Estimated MSP tech time used: 4 hours |
| Step 5 | If MSP tech is not satisfied that infection has been completely removed, may elect to completely reimage the machine. Security software would be updated, then used to scan machine to verify infection is no longer present. Final testing by tech to ensure all functionality has been returned to normal. | Estimated MSP tech time used: 4 hours |
| Step 6 | The machine is returned to the user, who would then need to reconfigure the machine to state prior to infection (personalized settings, etc). Any client data on the infected machine that had not been backed up would be lost after reimaging. | |

Table 1. Sequence of events when typical antivirus solution identifies breach

This process may take hours and hours—and potentially cost an MSP thousands of dollars. At a typical bill rate of $150/hour, the 13 hours that the MSP tech spent in the above example amounts to almost $2000. Under common terms of an MSP SLA (for example, 99.95% availability equates to just under 4.4 hours of unplanned downtime per year), those technician's hours would not be billable to the client. The MSP could be liable to the client for an SLA payout of up to one month's fees or more.

### C. Time Is Money

What is the net result of processes described above? The MSP suffers the opportunity cost of utilizing skilled, billable resources on unprofitable tasks, faces the potential loss of client fees due to triggered SLA payouts, and jeopardizes its ability to retain that client as a long-term customer (and a source of ongoing revenue) due to the MSP's clear failure to protect the client from a malware threat and consequent downtime.

This latter point highlights the psychology underlying the MSP-client relationship. If an SMB with its own IT person experiences some downtime, it might accept it and shoulder part of the blame. But if that same SMB relies on an MSP to completely manage its IT environment—according to specific terms within an SLA—and pays the MSP significant fees to do so, that very same amount of downtime is far more distressing to the SMB.

The above issues are challenging enough when viewed in the context of a single infection on a single endpoint. They become far more daunting when extended to the dozens of clients that many MSPs have. Imagine an MSP with 50 clients, each employing the same antiquated endpoint security solutions noted earlier—and each vulnerable to malware infection. Even if the clients are smaller firms of approximately 25 employees each, the sheer number of potential targets for infection is distressing. What's more, such 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.

For an MSP, time is money. If even one technician spends an entire day remediating a customer's malware infection, that entails a significant loss to an MSP's business. Simply put, MSPs need a fundamentally different approach to endpoint security.

## II. THE WEBROOT DIFFERENCE

### A. Modern Solution for Modern Threats

It's clear that signature-based endpoint security solutions are incapable of effectively combating the alarming volume, velocity, and variety of today's threats. Modern cybercriminals employ an extensive range of sophisticated new techniques (polymorphism, advanced persistent threats, phishing, etc.), so it should come as no surprise that truly modern endpoint protection requires an analogous commitment to innovative technologies.

But such protection must not come at the expense of other key factors that an MSP should take into consideration. When evaluating the merits of an endpoint security solution (or indeed, any IT asset), there are three criteria that are particularly relevant to MSPs:

- **Profitability**
- **Manageability of the solution**
- **End user satisfaction**

Webroot understands the significance of these issues for MSPs, and has designed its SecureAnywhere™ endpoint security solutions to deliver superior results in all three areas.

### B. Getting Started with Cloud-based Architecture

The most obvious characteristic differentiating Webroot from competitors is its completely cloud-based architecture. This has immediate and powerful implications for the profitability of an MSP. Because Webroot solutions don't require dedicated infrastructure on the customer side, there is no server for the MSP to deploy and maintain (and no accompanying hardware to contract and maintenance agreement). Eliminating server hardware and maintenance costs significantly improves net MSP revenue.

Webroot's cloud-based approach also enables the use of a lightweight client (under one MB), because no signature database is stored within the client software. Instead, Webroot maintains a massive signature database in the cloud. Due to the cloud architecture, this approach combines far better protection, quicker installation, and faster scanning. Average scans complete in a matter of seconds, thereby reducing MSP labor cost and improving productivity and uptime.

For continuous client protection, Webroot solutions can be installed over existing security solutions, which may be removed at a later time. In this way, an MSP can ensure there's no vulnerability window. From the end user's perspective, the most immediate benefit of cloud-based protection is the remarkable increase in system performance. By placing far less burden on a protected device's CPU than old security solutions, Webroot solutions' background activity is virtually invisible to end users.

### C. Remote Management

Once deployed, Webroot endpoint solutions can be managed easily via a web-based console that's accessible by web browser. MSPs can log into this console from any location and see their entire IT environment. An MSP with many clients and a multitude of endpoints, perhaps spread across the globe, can access them all through this single console. By contrast, an MSP managing multiple clients—with each employing a dedicated infrastructure for their security—must suffer the inconvenience of logging into every client's administrator console separately.

Similarly, MSPs use a number of different solutions in the course of managing their clients' environments, and it's extremely inefficient for an

MSP to access every vendor's application individually. As a result, many MSPs utilize a tool called remote monitoring and management (RMM), which enables all of an MSP's applications to plug into a single RMM portal. There are different degrees of integration available depending on the specific applications and RMM tools involved, but at its most basic level, RMM gives MSPs one-stop access to high-level information about the status of their applications.

Webroot solutions integrate with LabTech and Kaseya, two of the most popular RMM platforms on the market today. This provides MSPs with a fast, convenient way to monitor the status of their Webroot solution. Should the RMM tool indicate that the Webroot software needs some attention, it's a simple matter for the MSP to then log into the Webroot portal.

### D. Security without Compromise

For an MSP, the most important criterion when evaluating any endpoint security solution is its ability to keep clients protected. As noted earlier, Webroot solutions are always connected to an immense cloud-based threat signature database (the Webroot BrightCloud® Threat Intelligence Platform) that is more powerful than any antivirus client-contained signature database could ever be.

But that's only one of the reasons Webroot delivers far greater protection from viruses and malware than conventionally-architected competitors. Webroot uses collective threat 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 BrightCloud® Threat Intelligence Platform to see if this suspicious behavior has been observed before (see figures 1 and 2, below). As every Webroot client around the world is continuously connected to the Webroot BrightCloud® Threat Intelligence Platform, new information on emerging threats is constantly added.

If the behavior has not been previously encountered, Webroot then uses a variety of heuristics that look for particular attributes that are characteristic of malicious activity. If Webroot still cannot determine if the suspect activity is malicious, it allows the software to run in a type of secure virtual machine known as a sandbox (i.e., isolated from infecting the system itself) in order to monitor the executable's behavior. 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 BrightCloud® Threat Intelligence Platform in real time.

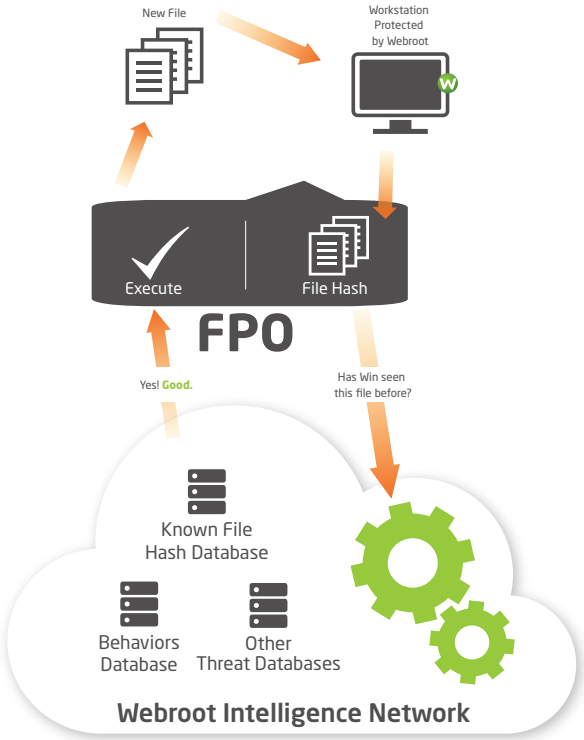


Figure 1. If the Webroot BrightCloud® Threat Intelligence Platform has seen file before and it is "known good," the file is allowed to execute.

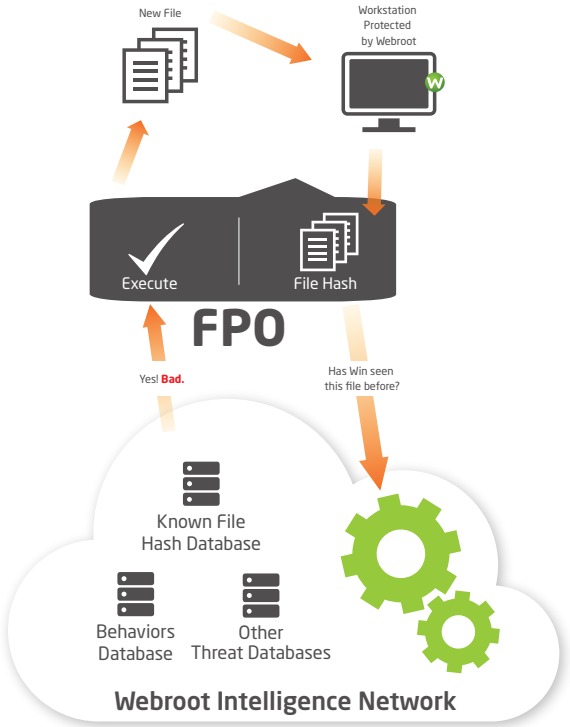


Figure 2. If Webroot BrightCloud® Threat Intelligence Platform has seen the file before and it is "known bad," the file is immediately quarantined and blocked from being able to execute.

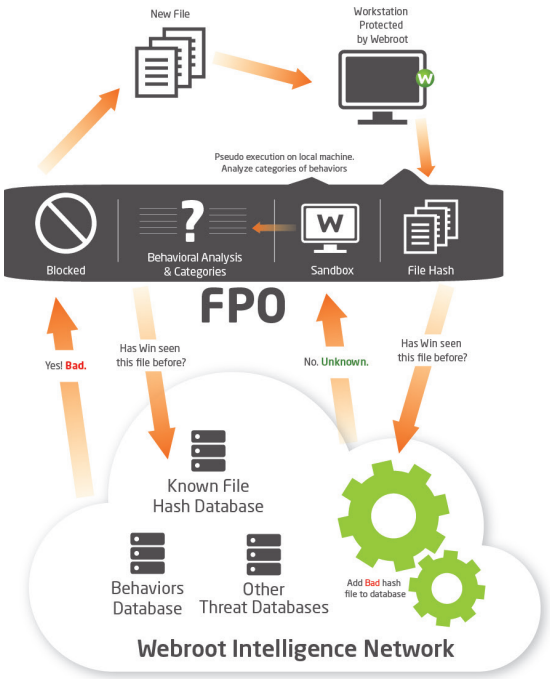


Figure 3. How the BrightCloud Threat Intelligence Platform makes file determinations.

From that moment on, any other system in the world connected to the Webroot BrightCloud® Threat Intelligence Platform 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 Business Endpoint Protection can undo every action that a malicious piece of software executed, even within the sandboxed environment, and return the machine to its state prior to the infection. To make this process even more cost-effective, the rollback can performed remotely, with no need to have a technician on site.

This is obviously a completely different, and far more efficient, remediation method than the traditional practice described earlier. The rollback remediation feature not only saves MSPs a significant amount of money and frees up technicians for more profitable endeavors, it also returns customers to work more quickly, improving customer satisfaction and long-term retention.

## E. Conclusion

Webroot significantly reduces the amount of time an MSP must devote to antivirus-related tasks, driving down Webroot TCO and boosting an MSP's profitability. Because Webroot provides clients with unrivaled malware protection that imposes virtually no burden on system performance, MSP client satisfaction also increases, as does long-term relationships and recurring, predictable revenue.

The MSP market is rapidly expanding, and growing more competitive. The ability to cost-effectively keep client IT environments protected and productive will play a significant role in determining how effectively MSPs can build, solidify, and broaden their client base. Webroot has applied modern technologies and methodologies to endpoint security solutions, making it possible for MSPs to finally see endpoint security solutions as fruitful assets rather than costly loss leaders.



**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