

August 3, 2012

## Building a Better Mousetrap in Anti-Malware

Stratecast Analysis by  
Michael Suby



Stratecast Perspectives & Insight  
for Executives

Volume 12, Number 28

## Building a Better Mousetrap in Anti-Malware

### Introduction<sup>1</sup>

This story is becoming frustratingly old. Cyber threats are continuously advancing in their adaptability speed, sophistication, and degree of stealthiness. At the same time, the exposed footprint is expanding. More business operations are moving online and end-user devices—corporate-issued and user-owned—are expanding in number and variety.

Furthermore, the means to turn the tide has been elusive. Businesses are routinely adding to their defensive arsenals in hopes of mitigating business continuity and productivity risk, and lowering the potential of data breaches. In economic terms, this has translated into increasing expenditures on security products and services.<sup>2</sup>

A reasonable question asked by executives responsible for making decisions on their organizations' security budgets is whether their money and resources are being spent wisely. Are their businesses buying and using the best mix of security technologies to meet their needs and obligations?

Beneficially, next generation security products do come to market that poke at the status quo and present genuine alternatives. Webroot<sup>®</sup> SecureAnywhere<sup>™</sup> Business - Endpoint Protection is one of those products. In this SPIE, Stratecast describes the deficiencies in traditional anti-malware products, outlines Webroot's fresh approach, and presents Stratecast's perspective.

### Deficiencies in Traditional Anti-Malware Products

The traditional approach of signature-based anti-malware software has been showing its age. When the number of unique strains of malware was relatively low and the time from infection to damage was measured in weeks and months rather than minutes, the general belief was that the malware threat could be kept at bay. The process of new malware discovery, analyzing its behaviors, preparing a malware signature, and then adding that signature to the malware file on the endpoint seemed like a reasonable approach. In time, however, reasonableness began to fade. As the cumulative volume of malware escalated and the pace of new malware introductions increased, malware signature files grew larger and larger. Consequently, the challenge of fighting malware was not just in finding and preparing

*The traditional approach of signature-based anti-malware software has been showing its age.*

---

<sup>1</sup> In preparing this report, Stratecast conducted interviews with representatives of the following company:

- Webroot – Mike Malloy - EVP, Products & Strategy; Patrick Kennedy - VP, Product Marketing; Andrew Bagnato - Sales Engineer; and Joe Jaroch - VP, Endpoint Solutions Engineering

Please note that the insights and opinions expressed in this assessment are those of Stratecast and have been developed through the Stratecast research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

<sup>2</sup> Frost & Sullivan's Network Security research consistently shows that expenditures on security products and managed security services are heading in one direction—upward. An ever-expanding list of research studies is available at: <http://www.frost.com/c/10402/sublib/category-index.do?category=industry&anchor=9519>. For more information on how to obtain any Frost & Sullivan or Stratecast report, contact your account executive or email [inquiries@stratecast.com](mailto:inquiries@stratecast.com).

malware signatures with speed and comprehensiveness, but also in effectively managing the distribution of the updated signature files and ensuring that malware scans were completed with each update.

All told, the tally for anti-malware protection is growing. The bandwidth associated with transporting the file updates to endpoints is increasing, as are individual endpoint requirements to receive and process the file updates and conduct scans. For end users, the fight against malware is no longer transparent. Their routines are subject to disruption.

***Structurally, the deficiency with traditional anti-malware is its lack of individuality.***

Structurally, the deficiency with traditional anti-malware is its lack of individuality. The inherent assumption with traditional anti-malware is that all endpoints are potential victims of any of the malware in the signature file. Therefore, all endpoints must be equally armed with the same burgeoning signature file.

In reality, endpoints are not uniform. They are a reflection of the individual user. For instance, malware is written to exploit application and process vulnerabilities and behaviors. Yet, the applications and processes present on user A's device are likely not an exact match with those on user B's device. Similarly, end users' online and computing activities vary. The activities of user A may be more "risky" than user B, resulting in user A "collecting" more malware than user B. Having an anti-malware signature file that includes signatures of all of vendor's known malware files is excessive; and, as previously outlined, this extra heavy blanket of a locally stored and processed malware signature file adds to the burden of anti-malware protection.

## Fresh Approach

Webroot makes the fight against malware more efficient by customizing the battle at each endpoint. Location is the difference maker. Rather than have a comprehensive malware signature file reside on each endpoint in order to conduct malware scans, malware intelligence resides and malware assessments are conducted in Webroot's cloud environment.

***Webroot makes the fight against malware more efficient by customizing the battle at each endpoint.***

Operationally in deep scan mode, the Webroot SecureAnywhere client locates file types and files in locations that have potential to infect the endpoint, and creates a hash, a small digital signature, for each of these files. This catalog of hashes are securely shared and compared with the Webroot's library of known malware files and known good files (i.e., whitelist). If there are malware matches, instructions are sent to the Webroot software client to remove the malware.

On a recurring basis (e.g., a daily scan), the endpoint's hash catalog is updated and shared with Webroot for malware assessments against Webroot's continuously expanding malware library and intelligence. Also, as new files are introduced onto the endpoint, or changes are made, unique hashes are created in real-time and shared with Webroot for malware assessment.

In this manner, it is the individuality of the endpoint and changes at the endpoint that are the principal impetus for malware assessments, not the expansion in the security vendor's malware library. This approach by Webroot contrasts with traditional anti-malware software where updates to the malware library are driven down to all endpoints in the form of an updated signature file, with no regard to individual endpoint relevance.

With Webroot's cloud-client architecture, there are performance gains which translate into end-user transparency in the battle against malware. Because the Webroot software client is not tasked with receiving and processing a signature file, the software client is significantly smaller in size than clients that conduct these tasks. As a result, the software installation time is shorter. Equally important in end-user transparency, and also attributable to the malware assessments being conducted in Webroot's cloud rather than on the end-user's device, the power of cloud computing accelerates scan times and limits the demand on endpoint computing and memory resources. Additionally, Webroot's focus on file types and file locations that have potential to infect further boosts overall performance run times without compromising efficacy.

To demonstrate that this transparency and high performance are concrete, Webroot commissioned a comparison of endpoint security software by PassMark Software in early 2012. Test results are available at: [http://www.webroot.com/En\\_US/resources-competitive.html](http://www.webroot.com/En_US/resources-competitive.html).

### ***Putting Webroot to a Personal Test***

As an end user, I too conducted my own tests on three Windows PCs I have in my possession—two that I own and the other owned and configured by my employer, Frost & Sullivan. Although I cannot replicate the laboratory rigor and comprehensiveness of a professional software testing firm, I, as an end user, can still measure certain comparative aspects of endpoint security software.

Each of my PCs is equipped with endpoint security software from a prominent security vendor. Prior to downloading and installing the Webroot SecureAnywhere client, and conducting an initial scan of these PCs, I updated the malware signature files for the current endpoint security software, ran a malware scan, and noted scan times, number of files scanned, and results. This was to ensure that I was starting with “malware-clean” PCs as determined by the existing security software.

In all three of my PCs, the total time to download and install the Webroot software, and run an initial scan (the scan automatically starts after installation) was less than five minutes. On one PC, a malware file was detected and automatically removed. Since the malware file was of a rootkit variety, a reboot was necessary and a rescan was automatically conducted. Webroot did not detect additional malware on the other two PCs. Incidentally, use of Webroot does not require the removal of existing endpoint security software. My experience confirmed this coexistence.

Scanning performance was significantly faster with Webroot. The Webroot scan rate ranged from a low of 8,300 file per minute to a high of 23,500 files per minute. The scan rates at the lower end of the range were associated with scheduled Webroot deep scans launched at PC booting and the higher rates occurred when I initiated a rescan, minutes to hours after booting. Retained knowledge of the previous scan on a “live” PC, and less contention for computing resources (i.e., not contending with the boot sequence), contributed to the higher scan rate. The scan rates with the existing security endpoint security products ranged from 700 files per minute to 1,700 files per minute. Based on my comparisons with two other endpoint security software products, Webroot's scan rate is approximately 12 times faster; a result similar to PassMark Software's test results.

***Based on my comparisons with two other endpoint security software products, Webroot's scan rate is approximately 12 times faster.***

On my two personally-owned PCs, I uninstalled and reinstalled the existing endpoint security software to have a comparative on download, install, and initial scan time. The online download and install time of the other vendor's software was completed in five minutes. Downloading the signature file added

another two minutes. Comparatively, the time required for Webroot software to be downloaded and installed, and to run an initial malware scan was approximately two minutes less than the time required by the other vendor’s software to be downloaded and installed and reach a “ready to scan” state.

**Protection from New Malware and Offline Vulnerabilities**

Since new malware is constantly being written, the need to detect and mitigate new malware in order to contain the damage of zero-day attacks is essential in anti-malware solutions. The diagram below illustrates Webroot’s real-time process flow when a new file, potentially harboring a zero-day threat, is detected on a Webroot-installed endpoint. In the first step, a file hash is created and passed to Webroot to compare with its library of known bad and good files. If not in the library, behavioral analysis of that file is conducted on the client with characteristics sent to the Webroot cloud to compare to its behaviors database. If determined to be bad, the file is placed in a sandbox on the client for isolated execution and deeper analysis of the file’s behaviors. Once completed, the file hash is added to the known file hash database in the Webroot cloud. Since the previously unknown file with suspicious behaviors only operated in a sandbox, damaging execution on the endpoint was blocked. Through this process Webroot protects the endpoint encountering the first instance of a zero-day threat and updates its bad file database so damage from occurrences of this same malware file on other Webroot-installed endpoints is automatically mitigated.

**Figure 1: Webroot SecureAnywhere Endpoint Protection Process Flow with New Files**



Source: Webroot

With Webroot’s cloud-client architecture, a logical question is how protection can continue when end-user devices are offline. In Webroot’s approach, the Webroot client enters surveillance mode. During this mode, offline heuristics tuned to the endpoint’s pre-offline software profile determine if threatening behaviors from a new software program introduced while the device is offline are

occurring. As warranted, the threatening behaviors are blocked from execution. The Webroot client also records changes to files, registry keys, and memory locations associated with new programs introduced while the device is offline. This process is beneficial if the heuristics did not trigger blocking but the new program is, in reality, malware. Once the endpoint is back online, a threat assessment is conducted in the Webroot cloud. If the program is determined to be malware, the program file is removed and Webroot returns the endpoint back to its previous known good state (i.e., reverses the changes).

## Stratecast Perspective

Stratecast has a bullish view on Webroot and its adoption of a cloud-client architecture in the endpoint fight against malware. Stratecast counts numerous competitive differentiation and strategic benefits associated with Webroot's cloud-client architecture:

- **Individuality** – As noted earlier in this SPIE, traditional anti-malware software follows a “one-size-fits-all” approach. While this traditional approach allows the anti-malware vendor to add new customers at minimal incremental cost, there are at least two drawbacks. The first is the consumption tax of an increasing size and update frequency of the malware signature file on end users and their devices. This situation places traditional approaches at risk of an “enough is enough” backlash, especially if efficacy is in question (i.e., infections still occurring). Second, the one-size-fits-all approach is incongruent with custom malware. As malware writers potentially advance their trade to become more tailored (e.g., writing malware specifically to attack the set of software applications common in a particular industry), an inability to support customization in malware assessments further widens the gap between what is needed in malware protection and what is delivered. Webroot is well positioned to demonstrate differentiation against traditional anti-malware products in both of these areas.
- **Lightweight and high performance** – The Webroot client is compact in size. Combined with the bulk of heavy lifting conducted in the Webroot cloud, end users gain transparency in malware protection, and malware assessments are bullet train fast. The low bandwidth usage between client and cloud is another plus. Finally, the ability to detect and react in real-time to new software introductions on the endpoint further adds to Webroot's high performance prowess. Like individuality, Stratecast sees two prominent benefits. First, all of these lightweight and high performance attributes represent the feature check boxes in anti-malware software for mobile devices. While there is market opportunity in desktops and laptops, anti-malware market saturation relegates Webroot's market opportunity to one of replacement. The greatest greenfield opportunities are in mobile devices—smartphones and tablets—where device growth is strongest and anti-malware penetration is the lowest. The company's anti-malware focus on Android devices and Android's open frontier application marketplace is a wise directional choice as it aligns well with Webroot's strengths in responding to device changes and individuality. Second, customer care is a profit margin penalty. Since the Webroot transitioned to a cloud-client architecture for anti-malware, the company states that customer care instances are dropping and the percentage of these being serviced online is increasing. These are trends any CFO would applaud.
- **Coexistence** – With market saturation of anti-malware on desktops and laptops, Webroot needs a highly scalable means to gain a toehold on its competitors' turf in order to increase

its market share. The ability to coexist with other anti-malware software plus fast and easy installation are key enablers for this type of invasion.

- **Turning back the clock** – As described in the offline use case, Webroot has the ability to track and reverse changes to files, key registries, and memory locations. This, Stratecast views, is a distinctive feature in helping end users stay on track in their device-dependent routines. Lacking insight on what changed, end users are at risk of a productivity hit if the malware damage is severe enough. Also, since no anti-malware vendor, including Webroot, can claim 100 percent malware detection, initially missed malware, whether it happens in online or offline mode, is a fact of life in cyber security. Being able to “turn back the clock” is an insurance policy-type capability Stratecast believes Webroot should trumpet louder.

### *Challenges to Overcome*

Even with the positive transition Webroot has made from being a provider of traditional anti-malware software to anti-malware built on a cloud-client architecture, market challenges and influences are nevertheless present.

- **Price ceiling** – The ubiquity and market maturity of anti-malware exerts downward pressure on pricing for all vendors, including Webroot. Despite the product and customer value differentiation in Webroot’s anti-malware software versus traditional anti-malware software, the ability to command a premium price differential will be difficult. Further, just maintaining price parity could be challenging if prominent market share leaders in endpoint security software make similar transitions in architecture with their anti-malware components, lower their prices, or do both.<sup>3</sup>
- **Cloud economics** – In the transition to a cloud-client architecture, a portion of computing also transitioned from devices owned by end users to the cloud platform owned or rented by the anti-malware software vendor. Essentially, a partial shift occurred on who pays for the computing resources needed to support anti-malware. With anti-malware software market prices per supported device stable to falling, covering the per device cost of cloud computing resources in a cloud-client architecture could be a material weight on Webroot’s profit margins.

---

<sup>3</sup> Market share and pricing analysis on endpoint security products can be found in *Global Endpoint Security Products Market: Protecting the Last Line of Defense from Emerging Threats* (N922-74) published by Frost & Sullivan in July 2011.

## Stratecast The Last Word

Change is a constant in security. Threats are constantly changing to evade security defenses and to reach their objectives, which is increasingly for financial gain. Oddly, some categories of security defenses have remained essentially unchanged in their operating principles. Anti-malware has been among the “unchanged.”

Webroot was also a member of the unchanged. The company’s anti-malware product followed the traditional approach of fighting malware at the endpoint with large and burdensome malware signature files. In late 2011, the company decided change was essential and the company changed in dramatic fashion. The company retired its traditional anti-malware product and introduced Webroot SecureAnywhere AntiVirus, founded on a highly efficient and adaptable cloud-client architecture. To that, Stratecast says congratulations! Change is good.

***Michael P. Suby***

VP of Research

Stratecast | Frost & Sullivan

[mike.suby@frost.com](mailto:mike.suby@frost.com)

### **About Stratecast**

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

### **About Frost & Sullivan**

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 40 offices on six continents. For more information about Frost & Sullivan's Growth Partnership Services, visit <http://www.frost.com>.

## **CONTACT US**

For more information, visit [www.stratecast.com](http://www.stratecast.com), dial 877-463-7678, or email [inquiries@stratecast.com](mailto:inquiries@stratecast.com).