



WEBROOT®

Secure *Anywhere. Business*
— *Endpoint Protection*

Technical Overview

George Anderson – *Senior Product Marketing Manager*
May 2012



Table of Contents

Introduction	3
Anti-Virus Testing Misconceptions	3
It was OK in 2006!	3
So it’s not working?.....	4
If I were you, I wouldn’t start from here.....	4
Starting from scratch	5
Webroot® SecureAnywhere™	5
Don’t waste my time or resources	6
Always up to date, on or offline	6
But we do that too.....well not really	7
Changing the ‘Game’	8
A Totally New Approach to Countering Malware	8
Webroot Starts Where Others Stop	9
Significant Offline Protection	10
Dealing With New Malware Offline.....	10
Better Protection Offline.....	11
Webroot Intelligence Network - Real-Time Protection	11
Protection From Infection, Not Protection Through Detection	13
Different From Other AV’s	13
Summary.....	14
System Requirements	14
About Webroot.....	14



Introduction

With the exponential growth and sophistication of malware today, the security industry can no longer afford to 'bury its head in the sand'. The bottom line is that traditional endpoint security protection is now ineffective due to the sheer volume, quality, and complexity of malware.

This paper looks at this problem and how Webroot, by going back to the drawing board on countering malware threats, is revolutionizing endpoint protection and solving the issues that hinder existing endpoint security solutions.

Anti-Virus Testing Misconceptions

The endpoint security market is one of the most competitive and largest security markets in existence, with well over 40 AV security vendors selling endpoint protection to consumers and enterprises in every corner of the globe. In an attempt to gain differentiation some solutions have resorted to 'proving' the efficacy of one solution against another. The irony is, that even with a 100% score from one of the independent testing labs, the results only show partial effectiveness; products scoring 100% are still letting malware through.

Testing assumes so much. Firstly, that the protection software is working (many malware compromises are pre-tested to ensure they bypass or knock-out the AV defenses.). Testing efficacy can only assess the 'known' temporary effectiveness of the test versus other vendors at that point in time. In addition, the testing itself is out of date before it's published, as during the test period a vast amount of new, unique and unknown malware is released each day.

Testing cannot account for the use of small volumes of highly targeted, unique, 'unknown' malware used to access defined targets with a specific set of objectives in mind, and that then continually attack until the objectives are reached. These types of sophisticated and persistent attack are often associated with professional state, government or industrial espionage, but today's organized criminal gangs seeking high value assets also have access to these resources and are just as likely, if not more so, to perform such advanced persistent threats.

When it comes to testing one should adopt the following viewpoint. Testing does provide some insight and a selective perspective on the capabilities of different endpoint AV vendors' over time. As such, testing delivers 'known' benchmarking, but given that 'unknown' malware is the real problem, a 100% result does not mean any endpoint is fully protected.

It was OK in 2006!

In 2006 the amount of totally new unique malware seen in that year was c.*1 million samples, in 2011 it was nearly *18 million samples!

Today much of the effort behind traditional AV products is still focused in creating detection signatures to recognize, block and remediate infections. So every day your AV program has to update itself to try to stay ahead in the malware 'arms race'. Signatures are of course not the only protection. They are now heavily supplemented with file



reputation, heuristics and other detection techniques that try to identify and stop malicious programs ‘owning’ endpoints such as desktops, laptops, tablets and mobile devices.

While this plethora of defenses helps sustain better protection efficacy, it also leads to very complex and bloated AV programs that use lots of RAM and CPU processing resources. To the extent that much of an endpoint’s computing power is hijacked by the security program and literally stops end-users from working productively - almost to the point in some cases where you could say that the cure is almost as bad as an infection.

The other drawbacks of continued organic AV development have been that with the addition of each ‘new’ component layer the ‘surface attack area’ for malware authors to stop the AV from working as designed has become even bigger. Now if an endpoint AV is not regularly updated it quickly becomes vulnerable, but the real problem is that the Internet is a real-time environment, and traditional AV is not.

(* Source: AV-TEST GmbH, www.av-test.org)

So it’s not working?

No matter what AV testing reveals we do return to the main endpoint issue – it’s simply not working. This was clearly illustrated in a global survey Webroot carried out just prior to the US RSA conference in February 2011. This research cast a lot of light on how enterprises are currently being affected by malware.

This research found †83% of enterprises with endpoint defenses in place still experiencing malware attacks from viruses; worms; spyware; phishing; hacking; Web site compromises; and infection via USB devices. Overall, three in ten (32%) of them had to deal with infections via USB devices, with the incidence rising the larger the company size - 39% of <2,500 and 47% of >2,500 seat companies). The consequences of malware infections were all very predictable too, with those who suffered one or more attacks reporting –

- Severe impacts on increased help desk time to repair damage.
- Declines in network performance.
- Reductions in employee productivity.
- Damage to the company’s reputation.

So not only is the AV model broken, the lack of efficacy is causing significant business problems too.

(† Source: Webroot RSA 2011 Global Research Survey)

If I were you, I wouldn’t start from here....

If you are designing a brand new way to counter malware and had a traditional signature AV as your core defense then I’m sure you’d think of the old Irish story about a tourist in Ireland who asks one of the locals for directions to Dublin. The Irishman replies: ‘Well sir, if I were you, I wouldn’t start from here’.



Right up until 2007 the signature based approach was ‘keeping up’ with defending endpoints. At that time malware volume was still running at well under *500K unique malware samples per month. The process used by traditional AV vendors of getting a sample, understanding how it works, developing a counter measure and creating a remediation signature takes at best a few hours, and for more complex malware days, weeks or more. However, today much of the malware is missed as there has to be some volume of malware for the AV vendors intelligence systems to even ‘see’ or ‘collect’ it.

Traditional AV also puts the emphasis on the endpoint being the defense point and downloading daily definition files to maintain defenses. These files are getting larger and because of other limitations can only address a small selection of all known malware.

Basically, traditional AV defenses are now too little, too late and only inform you when they ‘find’ an infection, rather than when the endpoint is ‘infected’. With the result that unknown malware achieves its objectives long before it is detected, if at all.

The real measure of protection is no longer ‘known’ malware but all the low volume targeted ‘unknown’ malware. How do you detect that? How can you possibly accurately test for it?

Starting from scratch

A new approach that efficiently counters malware is needed. AV has to move away from being a reactive and almost continually updated local protection model. It needs to move to a pro-active, always up to date, and always defending the endpoint in real-time model. And to achieve this it needs to use the ‘cloud’ to ensure it works at today’s Internet speed.

Given this change what would be the ‘optimum’ way to defend and protect endpoints? What improvements would you make to anti-malware prevention and remediation performance?

These were some of the questions that resulted in Webroot acquiring Prevx; BrightCloud and Usable Security in 2010. In this way Webroot was able to compliment the technology we already owned with more of the components needed to create a revolutionary new way of defending endpoints against all types of malware – both known and more importantly unknown. We were on the way to providing the best way to defend endpoints at Internet speed.

Webroot® SecureAnywhere™

Webroot SecureAnywhere is a radically new approach to endpoint security and malware detection. It’s a true cloud-based solution with a web-based management console for cloud configuration and management. Operationally it leverages the power of cloud computing and the Webroot Intelligence Network to analyze, identify, stop, remediate and protect all users endpoints in real-time.



The Webroot Intelligence Network consists of the world's largest database of unique extractable objects (over 250 million) and forms the foundation of our real-time threat detection capabilities. Our database also holds >50 terabytes of threat data that delivers protection against all known threats, and lets us guarantee 100% protection against them.

More key is that with real-time threat identification Webroot SecureAnywhere virtually eliminates the window of vulnerability between when a threat is released and when a remedy is identified. Using our unique file pattern and behavior recognition technology all file executions are intercepted and checked by the cloud intelligence. Any file that behaves in a similar way to an existing threat, or that has never been seen before, is quarantined in order to prevent execution. Information on new or potentially malicious files is also immediately available to help protect every customer. This 'network' or 'community' protection effect is greatly enhanced as the same core technology is used in both consumer and enterprise versions.

Don't waste my time or resources

High on the wish list for any brand new form of malware protection was a significant improvement in endpoint performance compared to the solutions out there today. Webroot SecureAnywhere was designed with that in mind too.

Independent testing by #PassMark Software published in February 2012 looked at the time and resources used by eight major AV vendors to perform 10 different tasks on a PC endpoint including - Initial Scan; Installation Size/Time; Boot Time; Memory Usage; etc. Webroot SecureAnywhere Business -Endpoint Protection scored 78 (97.5%) out of a maximum of 80 (100%), while the best top-selling traditional AV scored just 55 (68.8%).

With the complete installation and initial scan of a PC endpoint taking under a minute#, and subsequent scan time's averaging between 30 and 90 seconds our new anti-malware takes a fraction of the time of traditional solutions. Moreover, as a result of its small size and using 'cloud intelligence' (the complete installer is under 700KB and maximum disk space usage <4MB#) Webroot SecureAnywhere uses a fraction of the disk space, RAM and CPU of any endpoint security solution. The net result is that user and endpoint productivity is never compromised by its operation and users are freed to get on with whatever they want to do, without security software interrupting them. (*#PassMark Software - Webroot Secure Anywhere Cloud Antivirus vs. Six Traditional Antivirus Products – September 2011*)

Always up to date, on or offline

Another major advantage of using the cloud, rather than the endpoint, as the 'work horse' is that Webroot SecureAnywhere is always up-to-date. The majority of time an endpoint like a PC or Laptop is in use its online. So any necessary threat prevention is automatically available to the endpoint as the 'cloud' is being continually updated anytime a new or unknown file is identified from many source, including Webroot SecureAnywhere endpoint. Even if an endpoint is offline default policies are built-in to stop or lock-down devices like USB or CD/DVD and the use of new program files until an online connection is re-established. Built-in application white and black listing also ensures that only valid programs will be allowed to execute.



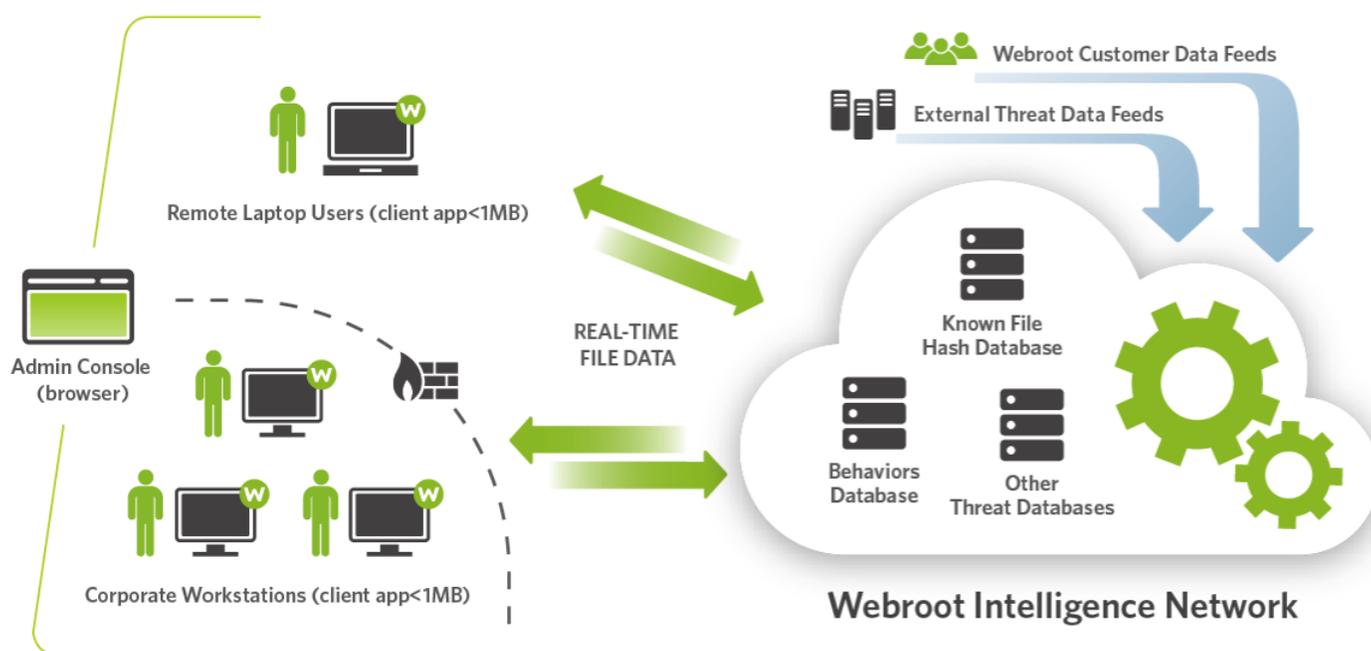
But we do that too.....well not really

Virtually all traditional AV vendors now have reputation based cloud lookup and some have been advertising being a cloud anti-virus for well over 2 years. Others have introduced similar 'cloud' platform claims to be able to beat their cloud drum too.

Francis deSouza, Group President of Enterprise products and services at Symantec recently said,^{*} "signature-based protection is insufficient and too slow". Symantec President and CEO Enrique Salem agreed that signature-based protection is insufficient and too slow when it comes to protecting against targeted attacks, zero-day threats and custom-made attacks. He also said: "In security, you have to drive efficiency without creating a false positive, as that is worse than the initial problem."

The bottom line is traditional AV vendors are using reputation and the 'cloud' in a very basic way to supplement their traditional defenses, and as a simple way of 'guessing' whether a file is good or bad, a purely reputational approach that can be wildly inaccurate. Webroot SecureAnywhere does use reputation with our file Age and Popularity heuristics and we are able to tune these parameters too. However, all reputation lookup achieves is better guesses at stopping zero-day threats, and whose heuristics are better than another's becomes highly debatable.

(^{*} Source: SC Magazine - Symantec: reputation-based protection is the future of anti-virus - October 05, 2011)



How Webroot SecureAnywhere Intelligence Network Works

What is not debatable is that Webroot SecureAnywhere does something far better than just reputation. We actually fully analyze the behavior of files and compare them against many different behavior patterns to accurately determine if a new and unknown file is potentially good or bad. This is investigating whether someone is actually



engaging in known criminal activity before determining that the person is good or bad. Traditional AV uses reputation and signatures, while Webroot SecureAnywhere does far more and goes much further to ensure the false positive issues that plague other behavior and reputations approaches do not occur.

Changing the 'Game'

Fundamentally, Webroot SecureAnywhere significantly changes the game versus traditional AV. It offers a superior cloud-based architecture and anti-malware prevention approach combined with an endpoint client that is the lightest[‡], fastest[‡] and most effective around.

It is extremely easy to deploy, install, and manage. It doesn't conflict with other endpoint applications, including other security solutions, meaning other software doesn't need to be uninstalled.

It leverages the world's most accurate cloud-based threat intelligence network – WIN - containing millions of files and associated file characteristics that results in endpoint scan times of typically less than 1 minute, improved endpoint performance, and through not getting in the way, user productivity increases too.

Its real-time monitoring of systems and files provides a far superior approach to malware threat identification. When unknown or suspicious files are discovered during a scan the instantaneous 'network effect' is able to block such files real-time - eliminating the window of vulnerability of traditional AV existing between the time a threat is introduced to when a signature is produced.

Add to this an intuitive online management web portal, and if you are a business, no need for an on-premise management or update server, and it's easy to see that Webroot SecureAnywhere immediately offers a lower total cost of ownership. It also frees-up both individuals and IT departments to focus on adding value, not managing or being delayed by security software updates and threat definitions.

The game changing approach taken by Webroot SecureAnywhere blocks all known threats, high probability threat variants, as well as zero-day attacks and provides the most effective and powerful endpoint security solution on the market today at stopping 'unknown' as well as 'known' malware.

A Totally New Approach to Countering Malware

Webroot® SecureAnywhere™ is the total opposite of a standard AV solution. It's small light and fast; needs no daily definition updates; uses minimal endpoint resources, and never slows a server application down - or gets in a user's way. Developed using Webroot's 15 year plus security experience, this 8th. generation solution re-thinks and re-architects malware protection to prevent infection in a completely different way from all other 'hybrid', 'cloud' and 'traditional' antivirus solutions.

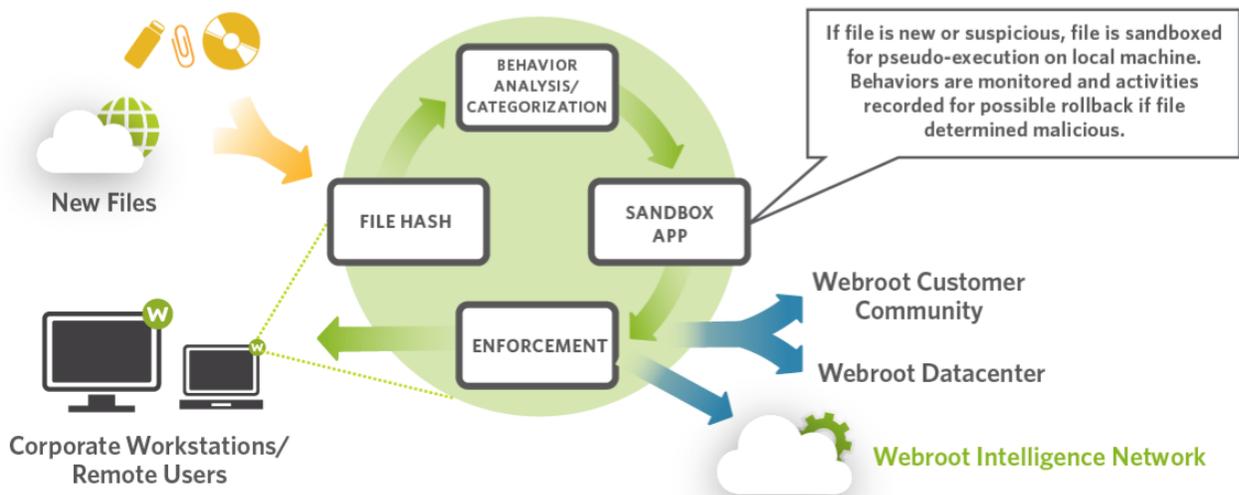
It's the first truly next generation approach to antimalware prevention for nearly 20 years, purpose designed to offer accurate, effective and instantaneous real-time threat determination and prevention within milliseconds.

Using the collective power of cloud computing and the Webroot Intelligence Network, with inputs from millions of endpoints, it optimizes prevention while minimizing the creation of false positives. And if it does categorize a good file as bad that's quickly and easily remedied using our unique override and rollback remediation controls.

Webroot Starts Where Others Stop

As Webroot SecureAnywhere first installs it analyzes all the applications and executable files on the endpoint and generates unique identification values to check the files in milliseconds with the Webroot Intelligence Network.

This whole 'learning' process takes only a couple of minutes and categorizes every file into good, bad or unknown. Unlike traditional AV, where if a file isn't bad it's 'assumed' to be good, only 'known good' files are allowed to execute and 'known bad' files are automatically blocked. Even at this early stage our approach to prevention is different, but major differences emerge when a file is unknown, or deemed suspicious.



Dealing with Zero-Day and 'Unknown' Malware

Then, the file is executed in a local sandbox and its behaviors checked against hundreds of thousands of behavioral patterns and rules using advanced logic systems to determine if it is malicious or not? If it is deemed malicious at this stage it is immediately blocked. (This level of checking dramatically reduces the risk of generating false positives.)

But there may still not be sufficient 'evidence' to categorize the file as bad (some malware is 'intelligent' enough to know it's in a sandbox and mask its true intentions) so the file is allowed to run on the endpoint.

However, the built-in monitoring and journaling of Webroot SecureAnywhere now comes into play, recording every change to the Registry and Files and monitoring other communications. Good copies of files and settings are created before any changes - so if the executions are now discovered to be malicious everything may be rolled back and remediated to a last 'good known' state.

This capability allows any errors either way to be easily reversed. It also removes the cost, time and lost productivity burdens that often occur in these circumstances as most endpoints need to be re-imaged due to the extensive file damage done by the malware.

Significant Offline Protection

Webroot SecureAnywhere Business is also designed to deliver significant offline endpoint protection. Webroot SecureAnywhere categorizes all the software on each endpoint and creates an inventory to ensure that it knows precisely what files exist and are active.

So if, for example, an infection compromised that endpoint two weeks before from a USB stick and you inserted that USB stick again when offline, Webroot SecureAnywhere would immediately block it.

In addition, if any similar infections (such as mutated versions of the original infection) try to compromise the endpoint, they would also be blocked, thanks to Webroot SecureAnywhere Business genetic signatures. These signatures look at the overall flow and layout of a program rather than a unique checksum.



How Webroot SecureAnywhere Works Offline

Dealing With New Malware Offline

Users are rarely offline these days, but when they are offline they cannot easily download and install any new programs, or get infected by drive-by, phishing, or other types of online compromise.

However, in the unlikely event that a brand-new piece of software is introduced when the endpoint is completely offline, and it has no relationship with any existing software on the endpoint, then Webroot SecureAnywhere Business automatically applies special offline heuristics. These heuristics are tuned to determine the origin of the software (such as a USB stick or a CD/DVD). After applying this local logic, Webroot SecureAnywhere blocks many threats automatically. Webroot SecureAnywhere also deals with threats that might get past the local logic heuristics

by using its behavior monitoring and rollback capabilities to ensure any threats that do execute cannot do lasting damage.

In this scenario, if a suspicious program has passed through several layers of local checks, it is monitored extremely closely to see precisely what files, registry keys, and memory locations are changed by the software program, while remembering the “before and after” picture of each change. If the software is then found to be malicious, Webroot SecureAnywhere proceeds to clean up the threat when it is online again.

Because the threat was active and changed or infected other files on the endpoint, Webroot SecureAnywhere doesn't just simply delete the main file—it removes every change that the threat made and returns the endpoint to its previously known good state. If at any point a suspicious program tries to modify the system in such a way that Webroot SecureAnywhere Business cannot automatically undo it, the user is notified and that change is automatically blocked.

Better Protection Offline

In offline mode, Webroot SecureAnywhere - Endpoint Protection provides an approach to countering malware infections that is far better and stronger than that provided by conventional antivirus products.

With conventional antivirus products, their signature bases are never completely up to date. When a brand-new infection emerges, and the antivirus software hasn't applied the latest update or there isn't a signature written for that specific threat, the infection simply roams freely across all endpoints, deleting, modifying, and moving files at will. As a result, it doesn't really matter if a device is online or offline - the malware infection has succeeded in compromising the endpoint.

When a traditional AV product comes back online, it applies any updates and typically runs a time-consuming scan - it might then be able to remove the infection. But it will not be able to completely reverse the changes the infection made, so the user or administrator will have to activate the System Restore function. More likely, the traditional AV-protected endpoint will need to be re-imaged because it's so unstable - a major further drain on time and productivity.

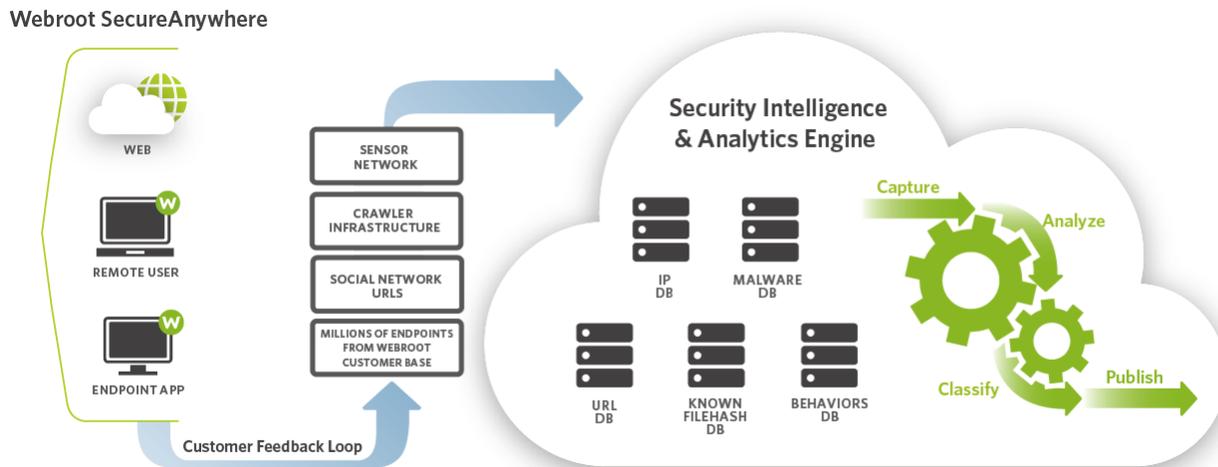
Conversely, Webroot SecureAnywhere leverages behavioral monitoring to pick up infections when the Internet is inactive or the endpoint is offline and it isn't sure whether a file is malicious or not. This process provides uniformly strong protection against the damaging effects of malware.

Webroot Intelligence Network - Real-Time Protection

Given the ever increasing volumes of malware protecting an endpoint with traditional signature definition anti-virus software is futile, but so is simply adding new detection features that simply drain more CPU and RAM resources, reducing performance and usability to even more unacceptable levels. There are now so many unknown infections being distributed by cyber-criminals that everyone is at constant risk.

Webroot Intelligence Network (WIN) is the key component of Webroot's malware prevention approach. When married to our ultra-efficient endpoint agent their combined power ensures known and unknown infections are stopped from doing harm.

The Webroot Intelligence Network integrates billions of pieces of information from multiple sources, including data from customers, test laboratories and intelligence shared between security vendors, to create probably the world's largest malware detection net.



The Webroot Intelligence Network (WIN) Engine

WIN incorporates Webroot's patented fourth generation 'Phileas' malicious code identification, plus ENZO our threat processing system for categorizing every software file and holding intimate knowledge of hundreds of millions of executable files including their behavioral characteristics.

WIN also uses systems that let us instantly categorize files and their interactions with other files and it uses our Webroot IP Reputation Service to track every malicious IP address on the Internet and provide accurate content classification; threat reputation and threat vector data. All this plus another 50+ terabytes of threat data ensures the Webroot Intelligence Network is always up to date and ready to detect any new malware infections.

WIN uses the Internet to connect with Webroot SecureAnywhere™ through a secure firewall connection and from the point when Webroot SecureAnywhere™ is installed all suspicious processes are closely monitored, analyzed and resolved real-time through WIN with its vast intelligence net keeping Webroot users' safe from both known and completely new and unknown infections.

Even when Webroot SecureAnywhere™ is not connected to the Internet it is able to function and detect infections, while taking the appropriate steps to stop them. No approach to stopping and protecting machines from infection is perfect, false positive mistakes are possible. Webroot SecureAnywhere™ - Endpoint Protection and WIN minimize these inaccuracies, and even allows a change to be reversed should files be incorrectly categorized.

Protection From Infection, Not Protection Through Detection

By combining the hugely powerful cloud interrogation of WIN with a completely new endpoint Webroot are able to stop infections without needing lots of signature updates. WIN harnesses the collective community of Webroot customers to continually refine file categorizations - even for the low-level and unique malware that normally remains undetected by traditional AV methods.

This ensures all Webroot endpoints are always protected against malware such as viruses, worms, Trojans, spyware, adware, bots, rootkits, and unique zero-day threats.

With advanced heuristics and behavior-based interception analyzing all files and potential threats in real-time, WIN ensures we minimize every user's window of vulnerability' between when a threat emerges and they are protected. And crucially, it is the high level of 'unknown' malware infection protection that makes Webroot SecureAnywhere™ - Endpoint Protection and WIN so powerful when compared to every other solution.

Different From Other AV's

While other vendors have invested in threat intelligence networks they are still used as bolt-on supplements to their traditional anti-virus solutions. None of these systems deliver or offer the breadth of in-depth capabilities of the Webroot SecureAnywhere™ that is purpose architected to integrate with WIN.

So, when comparing Webroot to other AV's, the differences and advantages of Webroot's approach to infection protection quickly become clear -

- WIN allows Webroot SecureAnywhere™ to be less than 700KB in size - the world's smallest endpoint security solution, almost unbelievably small. (The nearest traditional or 'cloud' antivirus solution installation file is over 128MB, and anti-virus solutions can easily use 750MB of hard disk space when fully installed.)
- Because of the installation size Webroot SecureAnywhere™ installs in seconds, and doesn't need traditional AV's to be uninstalled beforehand as it doesn't conflict with their detection processes.
- WIN allows ultra-fast scan times – typically a full PC scan will take less than 1 minute, so it never noticeably interrupts the user or unacceptably slows down their PC.
- WIN promotes low PC resource usage. Webroot SecureAnywhere™ - Endpoint Protection typically needs <12MB of RAM when scanning uses minimal CPU resources.
- WIN also allows Webroot SecureAnywhere™ - Endpoint Protection to be completely update-free with only ultra-low data exchanges between them needed. (All the updating happens in the 'Cloud', resulting in network traffic being c.150-250KB per day, a significant saving on normal anti-virus bandwidth usage.)

Webroot SecureAnywhere™ with WIN is a brand new way of protecting PCs.

It eliminates traditional signature based detection and fully exploits the benefits of 'cloud' computing through having a central intelligence network.

Summary

Webroot SecureAnywhere provides both consumers and enterprises with a brand new cloud-based security solution that is the lightest, fastest, and most effective endpoint security solution on the market. It offers a new, effective, efficient and superior way to protect endpoints.

By taking an entirely different approach to threat detection and prevention; eliminating traditional signature based detection at the endpoint; and leveraging the 'cloud' as its central intelligence network - Webroot SecureAnywhere now offers the best possible protection against unknown malware threats, improves PC performance and significantly reduces the pains of managing endpoint security.

System Requirements

Management Portal Access:

- Internet Explorer® version 7, 8, and 9
- Mozilla® Firefox® version 3.6, and upwards
- Chrome 11 and 12
- Safari 5
- Opera 11

Supported PC Platforms:

- Windows® XP Service Pack 2 and 3, 32- and 64-bit
- Windows Vista®, 32- and 64-bit
- Windows 7, 32- and 64-bit

Supported Server Platforms:

- Windows Server 2003 Standard, Enterprise, 32- and 64-bit
- Windows Server 2008 R2 Foundation, Standard, Enterprise
- Windows Small Business Server 2008 and 2011

Supported Virtual Server Platforms:

- VMware vSphere 4 (ESX/ESXi 3.0, 3.5, 4.0, 4.1, plus Workstation 6.5, 7.0, Server 1.0, 2.0
- Citrix XenDesktop 5 and XenServer 5.0, 5.5, 5.6
- Microsoft Hyper-V Server 2008, 2008 R2.6

About Webroot

Webroot is committed to taking the misery out of Internet security for businesses and consumers. Founded in 1997, privately held Webroot is headquartered in Colorado and employs approximately 400 people globally in operations across North America, Europe and the Asia Pacific region.

Webroot Headquarters: 385 Interlocken Crescent, Suite 800, Broomfield, Colorado 80021 USA