WEBROOT®
Smarter Cybersecurity™

FAQ | Webroot SecureAnywhere® Business Endpoint Protection

MALWARE EFFECTIVENESS

How can Webroot be so effective with an endpoint agent that's under 1MB and an 18[1] second scheduled scan time?

Webroot SecureAnywhere® Business Endpoint Protection works very differently from traditional and even so-called "next-gen" endpoint security. Backed by the Webroot® Threat Intelligence Platform—our advanced, fully cloud-based, machine learning threat intelligence architecture—Webroot solutions definitively identify all files and processes that execute on each endpoint as good, bad, or unknown in real time.

The SecureAnywhere agent was written very efficiently, almost at the machine code level, so it is capable, feature-rich, and needs minimal space on an endpoint's hard drive. Webroot real-time detection and protection uses a fully cloud-based architecture that places the processing burden of identifying malware in the cloud, not on endpoint resources. This keeps the installed agent lightweight, and extremely efficient.

Additionally, SecureAnywhere Business Endpoint Protection uses a RAW scanning approach that, when combined with other techniques, means it performs faster than many other antivirus approaches.

How does it protect offline endpoints?

Webroot SecureAnywhere Business Endpoint Protection is designed to provide protection even when a user is offline. All previously made categorizations are remembered on each endpoint. Should a user insert a USB and load a file that infected them previously, the agent would automatically block that threat.

If a never-before-seen threat infiltrated the endpoint while offline, then offline policy heuristics would protect the user. These heuristics account for the origin of a given file, such as a USB stick, or CD/DVD. If the file or process is unknown, the agent continuously monitors, journals, and limits the activities and changes the unknown file can make. Once the endpoint is back online, if any files introduced while offline are determined to be malicious, the agent automatically remediates the threat using its built-in rollback capabilities.

How does built-in auto-remediation work?

If no good/bad determination can be made on a given file, the SecureAnywhere agent monitors it extremely closely and records ("journals") its actions. If that file tries to modify the system in such a way that could not be reverted automatically, the administrator receives a notification and the change is blocked. This behavior monitoring engine also ensures that threats that bypass local offline protection cannot do lasting damage.

If the file in question is eventually determined to be malicious, then the agent will alert the administrator and/or user, then automatically quarantine and address the threat. It will then revert any journaled file and system changes as part of the remediation process.

Does Webroot SecureAnywhere Business Endpoint Protection include a firewall?

Yes, it includes an outbound only firewall to supplement the Microsoft Windows inbound-only firewall. It automatically monitors all TCP and UDP traffic for untrusted processes trying to connect to the network/internet, and blocks them from communicating to malware sites.

How can I protect remote/mobile off-network users?

The cloud-based Webroot management console lets admins set protection policies by individual or group to cover their on- and off-network protection. Additionally, Webroot offers more than 40 fully remote agent commands, application controls, and override settings that enable you to tailor protection, including application white and black listing.

MULTI-VECTOR PROTECTION

Does Webroot offer any other forms of prevention or protection?

SecureAnywhere Business Endpoint Protection offers a unique blend of layered, multi-vector protection to secure users and devices against today's attacks. It covers threats that come from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives, as well as other blended threats with the potential to deliver malicious payloads.

How does Webroot protect users when using the internet?

The Webroot Web Threat Shield protects users as they browse the internet. When using a search engine, the Web Threat Shield analyzes all the links on the search results page and uses Webroot BrightCloud Web Reputation intelligence to display real-time color-coded reputation scores in the Google, Bing, and Yahoo search engines. If the user attempts to navigate to a site with a malicious or suspicious reputation, they will receive a policy controlled block notice.

How does Webroot protect my organization against phishing and spear-phishing attacks?

Phishing accounted for 90% of successful breaches, according to the recent Verizon 2017 Data Breach Investigations Report. The level of social engineering information available makes it easy to trick anyone. For that reason, all Webroot SecureAnywhere solutions incorporate Webroot BrightCloud Real-Time Anti-Phishing intelligence. This protection layer kicks in when the Web Threat Shield cannot determine if a site is safe or not. The agent then performs numerous checks in milliseconds to determine with 99% accuracy if a website poses a phishing risk and blocks access accordingly.

How does Webroot secure USB and DVD/CD drives?

Webroot SecureAnywhere Business Endpoint Protection incorporates a USB Shield that blocks malicious activity from removable media drives, including USB, CD/DVD, etc.

How does Webroot protect the web browser and my users' login credentials?

Webroot solutions incorporate an Identity Shield to protect user information and transactional data that could be exposed during online transactions. By locking down the operating system and browser at the kernel level, the SecureAnywhere protection helps to neutralize phishing, DNS poisoning, keystroke logging, screen grabbing, cookie scraping, clipboard grabbing, man-in-the-middle and browser, and session hijacking by malicious software. In addition to a large number of browser and IP defenses, the Identity Shield also prevents programs from accessing users' protected credentials, such as usernames and passwords and website requests to remember credentials. Additionally, it automatically blocks untrusted programs from accessing protected data.

INFRASTRUCTURE IMPACT

Since Webroot SecureAnywhere Business Endpoint Protection is cloud-based, how much network bandwidth does it consume?

Very little, compared to the bandwidth consumed by traditional signature or definition updates. The endpoint agent only needs to communicate with the Webroot Threat Intelligence Platform when it finds a changed or new file, or to poll the management console for any policy changes. All exchanges are compressed and encrypted, and a typical endpoint will consume under 1 MB of network traffic per working day. During installation, a Webroot agent requires approximately 500 KB of network traffic bandwidth.

Does Webroot provide any assistance with uninstalling existing antivirus solutions?

Yes. However, Webroot SecureAnywhere solutions will run alongside existing security without conflict, so uninstalling previous antivirus is not inherently necessary. If you choose to do so, Webroot Sales Engineers are free to advise you on using the Webroot management console or other tools to uninstall existing antivirus software. The console offers powerful agent command scripting that lets you remotely download and run removal routines to uninstall applications remotely as needed.

MANAGEMENT & FUNCTIONALITY

Do I need to install a local administration/ management server on my network?

No. The Webroot SecureAnywhere agent and management console are completely cloud-based, so there's no on-premises management hardware or software.

How do you deploy the agent?

You can deploy the agent easily using any of the following methods: our packaged MSI installation file, Group Policy Objects (GPO), any existing deployment tool, or by emailing the agent executable to the desired recipient. Because the agent file size is under 1 MB, installation takes around 33[1] seconds.

Does Webroot offer device control capabilities?

Partially. Our customized heuristics allow admins to block the execution of newly introduced files from USB, CD, and DVD drives.

Does Webroot have Active Directory (AD) integration?

Partially. Webroot solutions do not integrate directly with Active Directory because that would require creating a communication port through your firewall. Many organizations view this as a security risk. For that reason, administrators will need to deploy users by Group, using the Group Management features built in to the management console. The Webroot management console offers AD mirroring via the agent. It is very easy to move users in and between Groups, and to view users in the console within your existing Active Directory tree. User views using IP ranges and Workgroups are also available from within the management console.

Do you have a NAC solution?

Yes. The SecureAnywhere agent supports the OPSWAT framework, which all top switches support.

What Data Loss Prevention (DLP) capabilities does Webroot offer?

The built-in Identity and Privacy shields and intelligent outbound firewall help prevent data exfiltration via malicious processes.

Does the Webroot management console have granular policy capabilities, e.g., setting up policies by group or individual?

Yes. The management console offers a fully customizable Group structure, with which admins can group endpoints based upon specific criteria. From there, they can apply specifically configured policies to those users' devices, as needed.

Since Webroot is cloud-based, what information does it capture, and how does it protect my organization and user data?

Webroot solutions operate on a highly distributed datacenter infrastructure architecture that uses Amazon Web Services globally to operate the Webroot Threat Intelligence Platform. These secure datacenters have highly restrictive access controls and are accredited under security standards such as SAS70 II and ISO27001. In the management console, you'll find your machine and group user information, administrator details, and system log files. Information such as installed software and infection data remains on the endpoint, not in the cloud. Webroot administrators must have specific permissions to access any data. All communications between our datacenters and the agent are bi-directionally encrypted.

Can admins override processes on specific endpoints, or across all endpoints globally?

Yes. Webroot offers override capabilities by individual agent, group policy, and account.

How often does the endpoint agent check in with the centralized management infrastructure?

The agent checks in to the cloud for threat data whenever activity on that system warrants it. In the Webroot management console, you can also set up automatic polling intervals for designated times. The intervals are 5 minutes; 30 minutes; or every 1, 2, 3, 4, 6, or 12 hours.

Do my deactivated Webroot agents count against my license device usage?

No. Any time you deactivate an agent in the console, it is automatically uninstalled from the endpoint and the license is immediately free for use on another endpoint device.

Can admins customize reports?

Yes. All reports allow different levels of customization so you can generate reports for targeted datasets. These are currently available in CSV format, but will eventually be available in PDF, SQL Database, as well as direct print from browser.

What happens when SecureAnywhere Business Endpoint Protection detects a false positive?

Webroot solutions have specific checks and balances to avoid false positives, so such detections occur very rarely. Should a file or process be blocked mistakenly, the administrator may immediately recategorize the file using the management console Override whitelisting function.

Do Webroot solutions protect mobile or remote users outside of the network?

Yes. Since Webroot uses a cloud-based architecture, the endpoint agent never needs to check in to any on-network service. It only requires an active internet connection to access Webroot Threat Intelligence Platform. This is also true for initial deployment. Users can deploy the agent directly by running specially named versions of the installation file. During installation, the license key is passed by the agent to the cloud. Webroot then registers that agent with the appropriate administration console via the license key, so the endpoint can be managed remotely.

Can I manage all endpoints through one management console?

Yes. Our centralized online management console offers full management over all endpoints from a single console, as well as different administration access permissions. Mobile devices, such as tablets and smartphones, can also be managed in the same console.

Do you offer file or disk encryption?

No. Windows-based machines already handle this very well with embedded tools like BitLocker.

Do you offer patch and vulnerability assessment?

No. Although we do not have specific patch and vulnerability assessment, if application vulnerabilities execute malicious code, the agent will monitor and block them as necessary.

Does Webroot offer spam filtering or mail scanning?

No. However, Webroot solutions scan all attachments when a user opens them in their email client.

COMPATIBILITY

Will Webroot SecureAnywhere Business Endpoint Protection run on Mac® or Linux-based machines?

We do support the Mac® operating system, but we do not plan to support Linux in the immediate future.

Is Webroot SecureAnywhere Business Endpoint Protection compatible with my existing antivirus?

Yes. Webroot solutions have no known conflicts with other antivirus solutions.

Is the endpoint agent the same for both workstations and servers?

Yes. The agent is the same for both workstations and servers. Mac® endpoints use a different agent.

Is the agent the same for Android™ and iOS® devices?

No. There are separate agents for these mobile operating systems.

SYSTEM REQUIREMENTS

Management Console Access:

» Google Chrome® 11 and newer

» Internet Explorer® version 7 and newer

» Mozilla® Firefox® version 3.6 and newer

» Safari® 5 and newer

» Opera 11 and newer

Note: Microsoft Edge® browser not currently supported

Supported Platforms:

» Windows® 10 32 and 64-bit

» Windows 8, 8.1, 32 and 64-bit

» Windows 7, 32 and 64-bit

» Windows Vista®, 32 and 64-bit

» Windows XP® SP 2 & 3, 32 and 64-bit

» Windows XP Embedded

» Mac OS® X v. 10.7.3 (OS X Lion™)

» Mac OS X v. 10.8 (OS X Mountain Lion®)

» Mac OS X v. 10.9 (OS X Mavericks®)

» Mac OS X v. 10.10 (OS X Yosemite®)

» Mac OS X v. 10.11 (OS X El Capitan®)

Supported Server/POS Platforms:

» Windows Server® 2012 R2 Standard, R2 Essentials

» Windows Server 2008 R2 Foundation, Standard, Enterprise

» Windows Server 2003 Standard, Enterprise, 32 and 64-bit

» Windows Small Business Server 2008, 2011, 2012

» Windows Server Core 2003, 2008, 2012

» Windows Server 2003 R2 for Embedded Systems

» Windows Embedded Standard 2009 SP2

» Windows XP Embedded SP1, Embedded Standard 2009 SP3

» Windows Embedded for POS Version 1.0

Supported Virtual Server Platforms:

» VMware vSphere® 5.5 and older (ESX/ESXi 5.5 and older),

» Workstation 9.0 and older, Server 2.0 and older

» Citrix® XenDesktop® 5; XenServer® 5.6 and older; XenApp® 6.5 and older

» Microsoft Hyper-V® Server 2008, 2008 R2

» Virtual Box®

Supported Mobile Operating Systems:

» Android™ operating system version 2.2 or higher

» Android-compatible phone or tablet device with 3MB of free storage space

» Apple® operating system iOS 6.1 or later

» Compatible with iPhone®, iPod touch®, and iPad® mobile digital devices

Supported Languages:

Webroot supports the following languages within the Management Console and our endpoint user agent:

» Chinese simplified, Chinese traditional, Dutch, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, Spanish, Turkish

Supported RMM and PSA Platforms:

Webroot has integrations with:

» Atera

» Autotask

» ConnectWise (LabTech)

» Continuum

» Kaseya

» Ninja

» And others

[1] Webroot SecureAnywhere® Business Endpoint Protection vs. Seven Competitors (April 2017)

About Webroot

Webroot delivers network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions, BrightCloud® Threat Intelligence Services, and FlowScape® network behavioral analytics protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 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