# FAQ

WEBROOT
SecureAnywhere® Business
Endpoint Protection

## INTRODUCTION

The following document contains answers to some of the questions partners commonly receive about Webroot SecureAnywhere® Business Endpoint Protection and how it combats malware.

## MALWARE EFFECTIVENESS

**Q: How can the software be effective with an agent of less than 750KB and only a 26 second1 scheduled scan time?**

**A:** Webroot SecureAnywhere Business Endpoint Protection works very differently from traditional antivirus solutions.

It accurately identifies files and categorizes them as good, bad, or unknown by using the immense power of the cloud-based Webroot® Intelligence Network (WIN). Although the installed agent is small, it's written very efficiently in C++ (at almost machine code level), so it's as capable as programs that are many times larger. Since much of the decision-making is performed in the cloud, it doesn't need a large amount of system resources, or a large local database of detection signatures. It's a new, more efficient method of identifying and addressing malware.

While the initial system scan is around two minutes, subsequent scans need only look for new or changed files, so not every file needs to be scanned each time. Additionally, the RAW scanning we perform is faster than traditional antivirus approaches.

**Q: How does it protect users who are offline?**

**A:** Webroot SecureAnywhere Business Endpoint Protection is designed to provide significant protection even when a user is offline, making the protection level significantly superior to that provided by competitive solutions.

When Endpoint Protection is first installed, all software on the endpoint is continuously monitored for change and a locally cached inventory is created to ensure the agent knows which files are active. If, for example, an infection had compromised an endpoint two weeks earlier via USB stick and you then inserted that USB stick again when offline, Webroot SecureAnywhere Business Endpoint Protection would still block it. Additionally, if similar infections, such as mutated variants of the same malware, attempted to compromise the endpoint, they would also be blocked using genetic signatures.

In the unlikely event that a never-before-seen threat infiltrated the endpoint while offline, then special offline policy heuristics would be applied automatically. These heuristics the origin of the software, such as a USB stick or a CD/DVD, enabling Webroot solutions to block many threats automatically. Any threats that might get past the local endpoint heuristics are remediated using the built-in journaling and rollback capabilities.

**Q: Is there any built-in remediation?**

**A:** If a suspicious program has bypassed the various layers of checks, it is monitored extremely closely. If no determination, good or bad, can be made, that program is automatically monitored any files, registry keys, and memory locations it changes are recorded.

This process is called 'journaling.' If the program is eventually determined to be malicious, then Webroot SecureAnywhere Business Endpoint Protection will alert the administrator/user and automatically quarantine and address the threat. Every change the threat made to files on the system is reverted as part of the remediation process. If, at any point, a suspicious program 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 off-line protection cannot do lasting damage.

**Q: Is there a firewall?**

**A:** Yes. The Webroot outbound firewall supplements the existing Windows inbound-traffic-only firewall by automatically monitoring all outbound traffic. It looks for untrusted processes that try to connect to the internet and blocks them from communicating to malware sites using Webroot threat intelligence.

**Q: How do I protect remote or mobile users who are off-network?**

**A:** You can apply usage policies by individual or user group through the online Webroot management console. Webroot also offers a wide range of remote commands, application controls and override policy settings that enable you to tailor protection to your needs, including application white- and blacklisting.

## INFRASTRUCTURE IMPACT

**Q: Since Endpoint Protection is primarily cloud-based, how much bandwidth does it consume?**

**A:** Compared with the daily signature/definition updates used by traditional antivirus products, measured in megabytes per day, Webroot SecureAnywhere Business Endpoint Protection consumes virtually no bandwidth. The agent only needs to communicate with the Webroot Intelligence Network when it finds a changed or new file, or to poll the management console for policy changes. All of these actions typically consume under 300 kilobytes of traffic per day. During installation, the agent requires approximately 500KB of network traffic.

**Q: Can you help with uninstalling my existing antivirus solution?**

**A:** Yes. Webroot Sales Engineers can advise you on uninstalling your existing software. However, it's not mandatory that you uninstall, as Webroot SecureAnywhere Business Endpoint Protection will run alongside your existing solution without conflict. Using the Webroot management console and application override controls, you can also stop existing security software from running. Powerful Agent Command scripting also lets you remotely download and run removal routines, as needed.

## MANAGEMENT/FUNCTIONALITY

**Q: Does a local administration/management server need to be installed on my network?**

**A:** No. The Webroot SecureAnywhere solution is completely cloud-based, including the management console, so no on premise hardware or software is needed.

**Q: How do you deploy the agent?**

**A:** 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 an email containing the <750KB executable. Because of the tiny file size, installation typically takes less than 51 seconds, which is faster than any other solution. Since Webroot SecureAnywhere Business Endpoint Protection doesn't conflict with other security, you don't need to worry about uninstalling existing solutions first.

**Q: Does Webroot offer device control capabilities?**

**A:** Partly. Our customized heuristics allow an administrator to block newly introduced files from USB, CD and DVD drives from executing.

**Q: Do you have Active Directory (AD) integration?**

**A:** Partly. We do not integrate directly with Active Directory because that would require creating an access port through your firewall, which many organizations view as a security risk. For that reason, administrators need to deploy users by Group, using the Group Management features built in to our console.

However, it is very easy to move users amongst Groups and also view users in your existing Active Directory tree within the management console. User views within IP ranges and according to Workgroups are also available.

**Q: Do you have a NAC solution**

**A:** Yes. The agent supports the OPSWAT framework, which all the top switches support.

**Q: What Data Loss Prevention (DLP) capabilities does your product have?**

**A:** The Identity Shield and outbound firewall prevent the extrusion of data via malicious processes.

**Q: Does the management console have granular policy capabilities, e.g., setting up a different policy by group or individual endpoint?**

**A:** Yes. The management console offers a customized group structure, which you can then use to group computers together based on your own criteria. Specifically configured policies can then be applied to those computers as needed.

**Q: Since this solution is cloud-based, what information does it capture and how does it protect my data?**

**A:** Webroot solutions operate on a highly distributed datacenter infrastructure architecture that uses Amazon Web Services globally to connect with the Webroot® Intelligence Network. These secure datacenters have highly restrictive access controls and are accredited under security standards such as SAS70 II and ISO27001. Within 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 permission to access any data.

**Q: Is there a way to overrides processes on specific, or globally across, endpoints?**

**A:** Yes. Webroot offers override capabilities that can be applied by individual agent, group policy, and account basis.

**Q: How often does the endpoint check in with the centralized management infrastructure?**

**A:** The endpoint checks in to the cloud for threat data whenever activity on that system warrants it. You can also set up the endpoint agent to automatically poll the management infrastructure at designated times. The intervals are 5 minutes; 30 minutes; 1, 2, 3, 4, 6, and 12 hours.

**Q: Do deactivated agents count against existing license usage?**

**A:** No. When you deactivate an agent in the console, it is automatically uninstalled from the endpoint and the license is immediately free for use on another system.

**Q: Are custom reports available?**

**A:** Yes. All reports have different levels of customization, allowing reports for targeted datasets. These are currently available in .CSV format, but will eventually be available in PDF, SQL Database, and direct print from browser. They will also offer scheduled delivery.

**Q: What happens when Webroot SecureAnywhere Business Endpoint Protection detects a false positive?**

**A:** 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 function and unquarantine right away.

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

**A:** Yes. Since Webroot uses a cloud-based architecture, the endpoint agents never need to check in to any service specifically on the network. They only require an active internet connection to access the Webroot® Intelligence Network. This includes the initial deployment as well. 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 customer administration console via the license key, so the endpoint can be managed remotely.

**Q: Can I manage all endpoints through one management console?**

**A:** 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 from here.

**Q: Do you offer file or disk encryption?**

**A:** No. Windows-based machines handle this very well with embedded tools like BitLocker.

**Q: Do you offer patch and vulnerability assessment?**

**A:** No. We do not have specific patch and vulnerability assessment, but should application vulnerabilities execute malicious code, the agent will monitor and block them as necessary.

**Q: Spam filtering and mail scanning?**

**A:** No. Webroot does not provide spam filtering, but it is important to note that we scan all attachments when they are opened via email client.

## INFRASTRUCTURE IMPACT

**Q: Does the Web Security Service use up more bandwidth?**

**A:** NO. In fact, the Webroot SecureAnywhere® Web Security Service will save bandwidth. The service automatically compresses user web page requests for optimum performance and minimal latency. Additionally, administrators can block pictures from web pages to reduce bandwidth even further, while Webroot automatically reformats the web page to remove resulting whitespace.

**Q: Does the Web Security Service require any network or firewall changes?**

**A:** SOMETIMES. Typically, no changes are needed. However, if your firewall is locked down, minor changes are necessary.

**Q: Does the Web Security Service require any changes to endpoint systems?**

**A:** YES. If you force users to always connect via your network, then no changes are required; however, this introduces latency and severely degrades web browsing performance. For most deployments, we recommend administrators install the Webroot DWP agent, which optimizes performance regardless of location and ensures that web policies enforcement.

**Q: Does the Web Security Service require any authentication?**

**A:** NO. Our DWP agent enforces seamless authentication and is automatically updated to the latest version, minimizing operational administration. Users may be asked for their Windows credentials if the agent is not installed.

## COMPATIBILITY

**Q: Will the Webroot SecureAnywhere Web Security Service work on Citrix or Terminal Server machines?**

**A:** YES. Webroot is one of the few cloud-based web security services to provide support for both Citrix and Terminal Services. All Citrix or Terminal Services users are individually authenticated. Unique policies may then be applied to separate users on a single Citrix or Terminal Services server and user activity logged individually.

**Q: Will the Webroot SecureAnywhere Web Security Service work on Mac® or Linux-based machines?**

**A:** NO. We currently don't support the Mac or Linux operating systems.

## SYSTEM REQUIREMENTS

### Management Console Access:

- Internet Explorer® version 7 and newer
- Mozilla® Firefox® version 3.6 and newer
- Chrome 11 and newer
- Safari 5 and newer
- Opera 11 and newer

### Supported Platforms:

- Windows 8, 8.1, 32 and 64-bit
- Windows 7, 32 and 64-bit
- Windows Vista®, 32 and 64-bit
- Windows® XP Service Pack 2 and 3, 32 and 64-bit
- Windows XP Embedded
- Mac OS X v.10.9 "Mavericks"
- Mac OS X v.10.8 "Mountain Lion"
- Mac OS® X v.10.7 "Lion"

### Supported Server/POS Platforms:

- Windows Server 2012 Standard, R2
- 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 4.2 or later
- Compatible with iPhone® and iPad® devices

### Supported Mobile Operating Systems:

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 and Turkish

### Supported RMM and PSA Platforms:

Webroot has integrations with:

- LabTech
- ConnectWise
- Spiceworks

### About Webroot

Webroot® is the market leader in cloud delivered security software as a service (SaaS) solutions for consumers, businesses and enterprises. We have revolutionized Internet security to protect all the ways you connect online. Webroot delivers real-time advanced internet threat protection to customers through its BrightCloud® security intelligence platform, and its SecureAnywhere™ suite of security products for endpoints, mobile devices and corporate networks. Over 7 million consumers, 1.5 million business users and 1.3 million mobile users are protected by Webroot. Founded in 1997 and headquartered in Colorado, Webroot is the largest privately held internet security company in the United States – operating globally across North America, Europe and the Asia Pacific region. For more information on our products and services, visit www.webroot.com


### Contact Us.

**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


1 Webroot SecureAnywhere® Business Endpoint Protection vs. Seven Endpoint Security Products PassMark Software Performance Benchmark Testing – February 2014