Webroot Frenquently Asked Questions

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

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?

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 SecureAnywhere Business 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 apply to 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 re-mediated using the built-in journaling and rollback capabilities.

Webroot Frenquently Asked Questions

Q. Is there any built-in remediation?

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?

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. With both the SecureAnywhere and Windows firewall turned on, your data has complete inbound and outbound protection. Please be aware of potential conflicts with other security applications running on your systems.

Q. Since SecureAnywhere Business is primarily cloud-based, how much bandwidth does it consume?

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 less than 300 kilobytes of traffic per day. During installation, the agent requires approximately 500KB of network traffic.

Webroot Frenquently Asked Questions

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

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

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.