Webroot SecureAnywhere® Business – Endpoint Protection

Significant Offline Protection

OVERVIEW

Webroot SecureAnywhere® Business – Endpoint Protection (WSAB-EP) is a true "cloud" antivirus solution providing the strongest protection when online by leveraging the real-time malware detection power of the Webroot Intelligence Network. In addition to its superb online protection WSAB-EP is also designed to deliver significant offline mode endpoint protection.

When WSAB-EP is first installed it continuously monitors and categorizes all the software on each endpoint and creates an inventory to ensure that it knows precisely what files are active. If, for example, an infection compromised that endpoint two weeks before from a USB stick and you inserted that USB stick again when offline, WSAB-EP would still 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 WSAB-EP genetic signatures. These signatures look at the overall flow and layout of a program rather than a unique checksum.

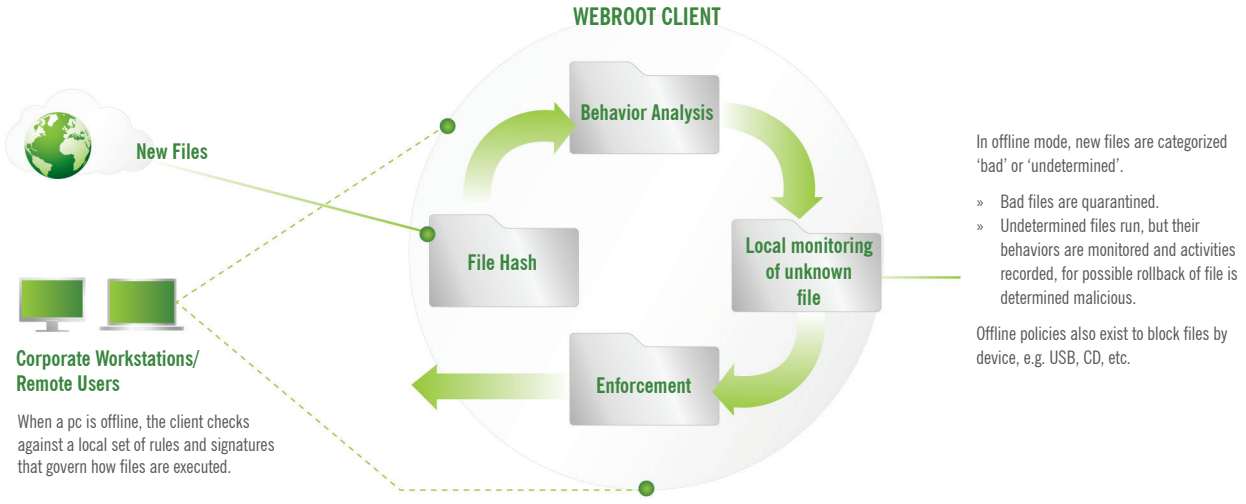
DEALING WITH NEW MALWARE OFFLINE

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.

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 WSAB-EP automatically applies special offline heuristics. These heuristics are tuned to determine the origin of the software (such as USB stick or a CD/DVD). After applying this local logic, WSAB-EP blocks many threats automatically. WSAB-EP 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, WSAB-EP proceeds to clean up the threat when it is online again.

Copyright © Webroot, Inc. > March 2014



How Endpoint Protection Works Offline

Because the threat was active and changed or infected other files on the endpoint, WSAB-EP 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 WSAB-EP cannot automatically undo, the user is notified and that change is automatically blocked.

BETTER THAN TRADITIONAL ANTIVIRUS SOLUTIONS

In offline mode, WSAB-EP provides an approach to countering malware infections that is far better and stronger than that provided by most 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, WSAB-EP 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.

PREMIUM IT DIGITAL SECURITY SOLUTIONS

PREMIUM IT is a leading distributor of High Quality IT security systems in Greece & Cyprus. Our solutions are designed, developed and manufactured in accordance with the highest quality standards.

Premium IT Ltd.
8 Timoxenous st.
11743, Athens - Greece
+302130087870
www.premiumit.gr

© 2014 Webroot Inc. All rights reserved. Webroot, SecureAnywhere, Webroot SecureAnywhere, Webroot Intelligence Network, and WIN are trademarks or registered trademarks of Webroot Inc. in the United States and/or other countries. All other trademarks are properties of their respective owners.