Webroot SecureAnywhere AntiVirus 2015

EDITOR RATING: EXCELLENT

- **PROS**
  Extremely small and light on resources. Fast install, super-fast scan. Top marks in two independent lab tests. Perfect score in hands-on malware blocking test. Very good malicious URL blocking. Can control protected computers from Web console. Good phishing protection.

- **CONS**
  Requires Internet connectivity for full protection.

- **BOTTOM LINE**
  Two independent testing labs have given Webroot SecureAnywhere AntiVirus (2015) their top ratings, and it earned a perfect score in our hands-on malware blocking test. Add the fact that it's the smallest antivirus around and you've got a definite Editors' Choice.

BY NEIL J. RUBENKING

How big is your antivirus? Would it fit on a diskette, if you could find one? Webroot SecureAnywhere AntiVirus (2015) manages to outperform most of the competition while remaining ridiculously tiny and light on resources. Both in independent lab tests and in my own hands-on testing, Webroot gets top marks.

The program's main window features a big button labeled Scan My Computer. It reports statistics, among them the time and duration of the latest scan. Simple switches let you turn the Real-time Shield, Web Shield, and Firewall on and off. Other links let you perform detailed configuration or get various views on the program's activities and system behaviors.

I should point out that the component called Firewall doesn't do what you might think. Rather, it tracks Internet and network connections and cranks up the heuristic detection level when it encounters suspicious activity. It doesn't attempt to stealth system ports, nor does it attempt the sort of program control that involves defining permissions for each program. It's meant to be used in conjunction with Windows Firewall, which does a fine job of stealthing your PC's ports and fending off external attacks.

Installation and Scanning

The Webroot installer is tiny, just 750KB. After installation, it takes a little over one megabyte on disk, and the installation takes just minutes. During the install process, it adjusts its configuration to your system, records a system baseline, and runs a scan. The scan takes just a few minutes, so the installation and scanning together take substantially less time than the installation and initial update for most antivirus programs.

One reason Webroot can be so small is that it doesn't maintain a local database of malware signatures. In fact, it doesn't use traditional signatures at all. Rather it examines a wide range of program attributes

and uses its cloud service to identify malware. The cloud service may identify a program as a named malware threat, or as a generic threat identified heuristically.

Some programs are suspicious, but not clearly malicious. Webroot monitors those and journals everything they do, including network and Internet activity. If the program's behavior pushes it over the line to malicious, it uses the stored information to roll back all the local changes made by the malware. The company claims this process will undo the encryption performed by CryptoLocker and other malware; I haven't been able to independently verify this claim.

Lab Results Scarce

I follow six independent antivirus testing labs that regularly release reports to the public. At the moment, Webroot participates with none of the six. In the past, when Webroot did participate, it frequently earned low scores, due, according to the company, to the fact that its detection methods are too different from the other products under test. There's no point in displaying my usual lab results roundup with a totally blank line for Webroot.

Fortunately I'm not entirely without lab report resources for Webroot. UK-based MRG-Effitas focuses on testing products for protecting online banking, but they also periodically release what they call "360 Assessment" reports. This type of assessment uses the full spectrum of malware types and includes a measurement of time-to-detect. That means the researchers start with brand-new malware, check whether the product defends against it, and give it additional opportunities for detection by rebooting three times, eight hours apart.

Webroot, Kaspersky, and Emsisoft were the only products to receive certification in this test. Four others, among them Trend Micro and Bitdefender, managed to clean the system after one or more reboots. Among the ten products that failed were some big names including Symantec, McAfee, and Panda.

Webroot commissioned a private test by Dennis Technology Labs earlier this year. Effectively, this was the public Q2 2014 report with Webroot added to the mix. With permission from Webroot and Dennis Labs, I can report that Webroot would have joined Kaspersky, Norton, and ESET at the tip-top AAA certification level. Starting in Q1 2015, Webroot will be a regular contender in tests by Dennis Labs.

Other Utilities

On the Tools page you'll find a variety of analytic and informational features. Tech experts will appreciate these tools; ordinary folks will most likely only use them under instruction from tech support.

It's not uncommon for malware to make system changes aimed at interfering with cleanup. Webroot includes tools to restore system policy defaults and also restore your desktop wallpaper and screensaver. You can use it to instantly reboot the system, or to reboot into Safe Mode. In addition, there's an option to manually remove malware, taking all of its Registry entries along with it. You're more likely to use the product's ability to run a cleanup script supplied by tech support.

On the Reports page you can generate logs of all scans and found threats, logs that you can submit to tech support. There's also a link to submit a suspect file. The Execution History log won't tell you much, but you might find the Statistics page interesting. Real-time numbers report all the various kinds of events Webroot has tracked. Across the bottom you can see how much CPU and disk space Webroot has used, and check your average scan time. On my test system, it reports 0.07 percent CPU usage, 0.012 percent of disk space, and 2.5 minutes for the average scan.

The System Control page includes an option to list all running processes. From the list you can tell Webroot to monitor or block any process, but most users should only do so if tech support so advises. Tech tinkerers may want to try the SafeStart Sandbox, which lets you control what system areas can be

changed by suspect programs. I tried launching all of the downloaded samples that got past the malicious URL blocking test. 62 percent simply wouldn't run with limited resources. Of the rest, only one actually managed to execute. This one was a dropper, an innocuous file that goes online to download its malicious components, and it was not permitted to download those components.

My Webroot Anywhere

The first time you click the My Account button, Webroot takes you through the process of setting up access to your online console. Webroot has some unusually stringent requirements for your master password, and won't accept anything not considered strong. You must also define a security code of at least six characters, and a security question and answer.

Each time you log in to the console, you first enter your email and password. Next it asks you for two characters from specific positions in your security code. The point is to foil any kind of keylogger or remote access Trojan that managed to get through other layers of defense. Remember, the computer you're logging in from doesn't necessarily have Webroot's protection.

Once you're logged in, you'll see five panels representing PC Security, Mobile Security, Backup & Sync, Passwords, and Community. If this is your only Webroot installation, PC Security and Community will be enabled, but the other three require an upgrade.

Clicking PC Security brings up a list of your protected PCs; clicking one of them brings up details. You can see things like the time and duration of the last scan, the keycode for this license, and how long your license is good for. Another tab lists results from the most recent scan along with details about any threats found.

The third tab, Commands, is perhaps the most interesting. You can remotely launch a scan, shut down the computer, or force a restart. You can also lock it remotely, so it keeps running ongoing tasks but nobody can access it without your Windows password. Finally, if this is a PC that you no longer own, you can deactivate protection, making that license available to protect a new PC.

A Tiny Dynamo

With top ratings from two independent labs and a perfect score in my own hands-on malware blocking test, Webroot SecureAnywhere AntiVirus (2015) looks pretty darn good. Add the fact that it's the smallest antivirus around, with the fastest scan, and you've got a definite winner. Webroot joins Bitdefender Antivirus Plus 2015 and Kaspersky Anti-Virus (2015) as Editors' Choice for commercial antivirus.

Impressive Malware Blocking

Webroot's real-time protection doesn't kick in based on the minimal file access that occurs when Windows Explorer checks a file's properties. Opening my folder of malware samples didn't get any reaction. However, it blocked 69 percent of the samples the instant I tried to launch them; the processes never actually executed at all.

Webroot blocked a few of the remaining samples after they started to install. It seemed to ignore the rest, at first. However, after a few minutes it reported finding malware. That's consistent with the concept of basing detection on actual process activity.

After removing the specific malware traces found, it launched a full scan. That wouldn't be reasonable for every antivirus, but Webroot's full scan takes just a few minutes. After any scan that finds additional malware traces, it scans again. After three scans, it came up green, and every single trace of every single sample was gone. With 10 of 10 possible points for malware blocking, Webroot clearly has the top score among products tested with my current sample set.

Very Good Malicious URL Blocking

Webroot's detection of the newest malware relies in part on monitoring behavior of a running program, so I wasn't sure how well it would do in my malicious URL blocking test. For this test, I start with a feed of very new malicious URLs supplied by MRG-Effitas. Using only those that actually point to a malicious executable, I launch each and note whether the antivirus blocks access to the URL, wipes out the downloaded file, or does nothing. Nowhere in this test does the malware get a chance to execute.

In fact, Webroot did quite well in this test. Out of about 100 valid malicious URLs, it prevented the browser from visiting 43 percent and wiped out another 30 percent at some point during the download process. Had I run this test a month ago, Webroot's 73 percent blocking would have put it in a tie for second place with F-Secure Internet Security 2015, bested only by avast! Free Antivirus 79 percent detection.

Identity Protection

Take a look at Webroot's Identity Protection settings page and you'll see that it promises to safeguard your private data in many ways. It protects against a variety of network and browser attacks, including man-in-the middle and man-in-the-browser. It isolates the browser from suspicious add-ins, and protects against keyloggers and screen-scraping attacks. It prevents external attacks on the browser, and more. You can add to the list of protected applications; the help suggests adding any financial apps you use.

Of course, all the protection in the world won't help if you're tricked into giving the bad guys your sensitive information. Webroot watches out for fraudulent websites (phishing sites) that attempt to steal your login credentials. It doesn't just check URLs against a list; it includes real-time analysis of page content.

Webroot did a good job detecting and blocking fraudulent sites, though not as good as consistent phishing champion Symantec Norton Security. Its detection rate lagged 14 percentage points behind Norton, and 7 percentage points behind Chrome's built-in phishing protection. On the plus side, it beat Firefox by 4 percentage points and out-detected Internet Explorer by 56 percentage points.