

## Prevx 3.0

Most modern anti-malware utilities or suites include a large database of signatures to help them identify known malware. Some can't scan at all after installation, until they perform a lengthy signature update. The database keeps growing as new malware appears at an ever-increasing rate. And, of course, zero-day malware may slip through before a signature becomes available. The better signature-based tools supplement their scanning with behavior-based detection of new threats. Prevx 3.0 (\$29.95/year direct) turns this concept on its head. It relies on behavior-based detection as its first line of defense, and it does a great job, too.

### The Prevx Process

When download Prevx you may think something's gone wrong with the browser. It couldn't have finished that fast, could it? But in truth the download is a mere 800 KB. MalwareBytes' Anti-Malware is a significantly smaller download than most anti-malware programs but it's still almost four times Prevx's size. You'd expect Panda Cloud Antivirus 0.9 to be a small download, since its intelligence lives in the cloud, but it weighs in at nearly 20 MB. Spyware Doctor with AntiVirus 6 is well over 20 MB and Webroot AntiVirus with AntiSpyware 6.0 just short of 40 MB. Prevx's minuscule download size is the first clue that we're looking at something really, really different.

Installation happens so fast you could miss it if you blink. A couple seconds after you accept the license agreement and click Next the installation is complete. Panda and

MalwareBytes both install in a little over a minute; I used to think that was fast. Eight minutes to install Webroot and 18 minutes to install Spyware Doctor on an identical test system now seem positively glacial.

Immediately upon installation Prevx launches directly into a required "learning scan." During this scan, it checks the installed programs and other executables on your system against the Prevx online database, identifying known good programs and flagging any malware it finds. The learning scan just takes a minute or so.

If the learning scan finds low-risk adware, Prevx offers to clean it up for free. If it finds anything more serious than that, you have to purchase and enter a license key before it will perform a cleanup. After you enter the license key, Prevx starts its standard full scan, which is more thorough than the learning scan. On a malware-infested system, this scan sometimes took four or five minutes. On a clean system, it ran in less than two minutes.

Prevx relies entirely on its online database for malware identification, so it simply won't scan if it can't contact the database. This is slightly different from Cloud Antivirus, which proceeds with the scan after warning the user that it won't be fully effective. On the other hand, Cloud Antivirus needed a full half-hour to scan my standard clean test system.

### Repeat As Necessary

Once the scan is complete, the next step is to download removal instructions for the found threats. Prevx doesn't maintain a huge set of local removal instructions

for every possible threat. It just downloads what it needs to know to get rid of the actual threats it found—a very smart approach. The instruction download is quick, and the removal process is quick. It's also potentially rough on other programs that are running. Prevx warns the

### Prevx 3.0

\$29.95 list



**BOTTOM LINE:** This forward-looking behavior-based anti-malware tool is incredibly small and fast because its intelligence lives in the cloud. It detected more threats than other products and overall scored better than its signature-based competition. One weak point—its cleanup leaves behind many traces. Even so, it's PCMag's new Editors' Choice for antispysware.

**PROS:** Minuscule download. Instant installation. Blazingly fast scan. Repeats scan until verified clean. Uses cloud-based behavioral malware detection. Replaces damaged system components. Detected the most malware in testing.

**CONS:** Cannot function without Internet connection. Cleanup left behind many file and Registry traces.

**COMPANY:** Prevx Ltd

### SPEC DATA

**PRICE:** \$29.95

**TYPE:** Business, Personal, Enterprise, Professional

**OS COMPATIBILITY:** Windows Vista, Windows XP

user to save all files, close all programs, disconnect from the Internet and be prepared to reboot.

Immediately on reboot, Prevx runs another scan. In testing, this repeated scan frequently found more threats and hence triggered another reboot and rescan. The product just won't rest until it has successfully run a full scan that detects no remaining threats. I like that, especially since each scan just takes a few minutes.

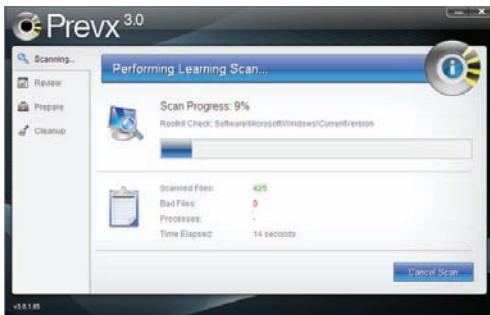
When malware damages or replaces essential system components, the cleanup process itself can cause system problems. For example, when Cloud Antivirus removed a threat that hooked into the TCP/IP stack, the system lost its ability to connect with the Internet. When Prevx detects this kind of problem, it checks its database to see if there's a copy of the undamaged component elsewhere on your computer. If so, Prevx simply restores the found good component. If not, the app prompts for the Windows install disk. And, indeed, it didn't lose connectivity on repairing the same system that gave Cloud Antivirus a problem.

If by some mischance Prevx can't fully clean the system, you can have a tech-support agent connect with your system remotely and perform a manual cleanup. The company is confident enough of success that they offer a money-back guarantee. In my testing Prevx always reached the green "Secure" status, so I didn't get to see this feature in action.

### Excellent Detection

I installed Prevx on a dozen test systems infested with a wide variety of malware samples including viruses, Trojans, worms, adware, spyware, and scareware (rogue security software). Prevx immediately went to work and quickly reported that each system was infected. I copy/pasted the license key to enable cleanup, after which it ran the deeper full scan.

In every case, Prevx required a reboot to finish cleaning up after the initial full scan. Five of the systems crashed with a blue screen error at this point. Blue screen errors during malware cleanup aren't uncommon, but I've never seen so many with one product. I asked Prevx about that and they explained that the program is designed to trigger a blue screen crash event if necessary to keep malware from re-infesting the system. Most users won't even see the crash because, by default, Windows restarts immediately. My vir-



tual machine test systems are configured to disable that automatic restart so I can view details of any crashes, or I would never have noticed.

In some cases, the program displayed a popup reporting detection of active malware and recommending removal. I always chose to remove the reported malware, which caused the current full scan to restart. That makes sense, because the product won't quit until it completes a full scan with no more detections. Some systems needed another reboot and rescan cycle. One had to go around five times before it was fully clean. I appreciate the Prevx's tenacity!

Under my current testing regimen, a product only gets the full ten points for removing a threat if it eliminates all of the threat's executable files and also removes 80 percent or more of the non-executable files and Registry debris. Removing 20 to 80 percent earns nine points, and if it leaves behind more than 80 percent of the junk it just gets eight points. Failing to remove executable files is more significant and knocks the score down to five. Leaving any of those executable files running means the product earns just three points.

Prevx detected 94 percent of the threats, more than any other product tested with this same collection. Norton 360 version 3 was next, with 92 percent, followed by Cloud Antivirus with 89 percent. But Norton did a more thorough job of cleaning up what it detected, so it scored 7.3 points for malware removal, compared to 7.0 for Prevx. None of the other apps tested scored as high.

In a parallel test using commercial keyloggers in place of actual malware, Prevx detected 90 percent of the threats, the same as Webroot and more than any other product. But Webroot cleaned up more thoroughly, scoring 6.8 in this test while Prevx got 6.0 points. Norton 360 edged out Prevx with 6.1 points. Fortunately for Cloud Antivirus (3.8 points) and MalwareBytes (0.5 points) I give much less weight to this test.

For the current round of testing, I've broken out a separate rootkit score, drawn from both malware and keyloggers that use rootkit technology. Prevx tied with Webroot for detection again: both got 89 percent. Webroot scored 7.1 overall against rootkits, while Prevx scored 6.7. None of the rest scored as high. In particular, Cloud Antivirus scored a measly 3.3 points and MalwareBytes just 3.6.

It's worth noting that Prevx successfully disabled the rootkit component of every such threat it detected.

Scareware (rogue security software) is a growing concern, so I've also started breaking out a scareware score. Prevx's 6.0 score is more or less in the middle, while MalwareBytes was the big winner with 7.3 points. Spyware Doctor had the lowest score, 3.3. It just didn't recognize most of these samples as threats.

Prevx detected a larger percentage of malware than any of the other products in this test, and it tied with Webroot for best detection of keyloggers and rootkits. Had it been as successful at cleanup as it was at detection it would have completely blown away the competition. That could still happen—Prevx CEO Mel Morris tells me that they're working on beefing up the product's cleanup ability.

### Powerful Protection

While Prevx is quite good at detecting malware on an infested system, it's even better at protecting a clean system. Some products scan every file on any kind of access, even the minimal access that occurs when Windows Explorer queries the file's details. Prevx, like Webroot and MalwareBytes, waits until the file tries to launch before scanning it.

Prevx's on-launch scan is extremely effective. In many cases, it immediately wiped out the malware installer, causing Windows to gripe that it "cannot access the specified device, path, or file." Others got caught during the install, or at the point when the installed malware

launched. In a few of those cases, it requested a full scan after detection.

As in the removal test, Prevx detected more malware than any of the competition—97 percent! And it was quite effective at preventing installation of those threats, coming up with a superb malware blocking score of 9.4 points. Webroot and Spyware Doctor detected 94 and 92 percent respectively. Norton 360 detected 89 percent but cleaned up what it found more effectively. So Norton 360 picked up 8.7 points while Webroot, Spyware Doctor, and Cloud Antivirus tied at 8.3. Malware-Bytes free edition doesn't include real-time blocking, and its Pro edition scored a dismal 4.3 points.

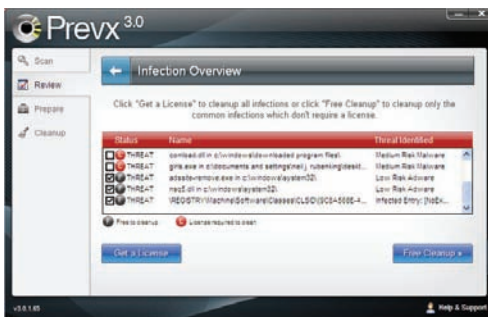
In a parallel test using commercial keyloggers in place of malware, Prevx detected every sample and completely prevented installation for most of them. None of the keyloggers could run, but some of the installers did manage to place executable files on the test system. Prevx's 8.9 points in this test is impressive, beaten only by 9.0 from Spyware Doctor.

Prevx and Spyware Doctor both detected all of the rootkit samples and both scored 8.9 points for rootkit blocking. But when I broke out a score specific to scareware, the results were quite different. Prevx and MalwareBytes scored 9.2 points, Webroot and Cloud Antivirus attained a perfect 10 points, and Spyware Doctor trailed the pack with a dismal 3.3.

Prevx had the highest detection percentage of any product tested in blocking or removal of malware, keyloggers, and rootkits (though it shared the top spot with others in some cases). Its overall malware blocking score is significantly higher than any of the others tested. And it does all this without needing to maintain and update a signature database. I'm very impressed.

### Detection and False Positives

As noted, Prevx doesn't rely on pre-defined signatures to identify malicious files. Rather, it looks at patterns of suspicious behavior. It also takes a file's age and distribution into account. A file seen by Prevx for the first time is naturally under more suspicion than a file that's been around for a year or two. And a widely-distributed file, one that's on thousands of computers, is less likely to be an emerging threat than one that's only found on a handful of Prevx-equipped systems.



The database quickly identifies most programs as known good or known bad. When it hits a suspicious unknown, it requests a copy of the sample and runs an automated analysis in an isolated sandbox environment. According to Prevx, this analysis takes from 30 seconds to five minutes. Of course, once the file is identified as good or bad, the same file needn't be analyzed again.

There's a chance any behavior-based system will mistakenly identify a valid program as malware. To test for such false positives, I installed a dozen-plus PCMag.com utilities that hook into Windows in ways that might be deemed suspicious. For example, KeyTick uses the same kind of keyboard hook as some keyloggers, and BHOCop changes the status of other Browser Helper Objects. Prevx didn't complain about any of these, which is a good sign.

It did identify one of my own hand-coded analysis tools as Medium Risk Malware, but I can hardly blame it. This is a tool that I use to check whether the product under testing has completely cleaned up known malware infestations. The program had never before been seen by Prevx and is found only on a handful of systems – strike one. It is only found on systems seriously infested with malware – strike two. And in order to check cleanup status it accesses tons of files and Registry keys associated with malware – strike three!

Rather than consider this a problem, I think it actually shows the effectiveness of Prevx's system. I had no trouble reporting the detection as a false positive and getting the tool re-categorized as a good program.

### Settings and Web Console

Prevx doesn't have quite the minimalist design of Cloud Antivirus, but there are still relatively few settings compared with most signature-based products. It allows

the user to set the sensitivity level for heuristic detection, age-based detection, and distribution-based detection. However, most users should leave these at their default settings. It's possible that tech support might advise raising the detection level in the face of frequent malware problems or lowering it if too many false positives arise.

The program's self-protection system is adjustable for similar reasons. At its default level, it prevents other programs from disabling its protection while maintaining compatibility with other security software. On a high risk computer with active malware, you crank it up (and risk interaction with other security products). On a system that uses multiple security products you may need to crank it down for compatibility. I had no trouble with the default protection level on my infested test systems.

By default, Prevx runs a scheduled scan at boot time and also once a day at 3 PM. You can turn off either scheduled scan, change the scan time, or choose a weekly scan rather than a daily one. But, given that the full scan runs so quickly, a daily scan seems good. Really, if you leave all the settings at their default values you won't go wrong.

While mostly aimed at Enterprise and high-volume users, the Web-based management console at [my.prevx.com](http://my.prevx.com) is available to any registered user of the program. From the console you can manage your licenses and Prevx-equipped PCs and also view infection events in the last hour, day, or week. The console sends a message to your registered e-mail account when a detection event occurs. By the end of my testing, I had received over a hundred of these! You might consider enabling this feature on a home computer, with the notifications sent to your work e-mail.

In the past I've evaluated non-signature anti-malware products separately from signature-based products and advised using them as a second line of defense against zero-day threats. Prevx 3.0 defies that second-string status. While designed to work comfortably with other security tools it proved more effective overall than the top signature-based products. Its cloud-based malware detection is outstanding, though cleanup could be more thorough. Prevx 3.0 is PCMag's new Editors Choice for antispyware.

—Neil J. Rubenking