



# RVS REVIEW

RETURNIL VIRTUAL SYSTEM  
Home Classic  
Review

Neil J. Rubenking from PC Magazine says RVS Home Classic is very good.  
“Reboot Really Restores” says Neil.

published May 19, 2010

You *know* you shouldn't wildly click links in e-mail messages, but you did it anyway. Now your computer has been totally pwned by a rogue security program that encrypted all your files and wants a ransom to decrypt them. Oh, if only you could go back in time to the instant before you clicked that fatal link! If you had installed Returnil Virtual System 2010 Home Classic (\$39.95 direct) you could do exactly that. Returnil virtualizes all changes to the file system and Registry. Just reboot and all evidence of the malware attack is gone, along with all other changes.

## Reboot to Restore

The Returnil concept is simple. When the System Safe virtualization mode is active, the real computer is unaffected by any changes to the file system or Registry. For the sake of system stability, it specifically omits the virtual memory page file and the hibernation file from virtualization. Programs don't know the difference—they happily use Returnil's virtualized versions of the file system and Registry. If malware hits your system, just reboot and it's gone. No, really—it's as simple as that!

If your system is already infected before you install Returnil, the malware infection will be restored on reboot just as your valid programs are. You'll definitely want to make sure there's no malware on the system before installing this product, perhaps by using one or more free Rescue CD products.

I was a bit thrown off by a couple aspects of the user interface. The System Safe area on the program's main page includes a link that says "Enable when I start Windows," but virtualization was not actually enabled when I restarted. It turns out you're meant to click that link and take the action it states... at which point the text changes to "Disable when I start Windows." A simple switch or pair of option buttons would have been clearer. I also found it odd that the floating toolbar uses a red icon to show that virtualization is on and a green icon to show it's off. But no matter; one can adjust to such minor eccentricities.

When you activate virtualization the program warns that a reboot removes *all* changes. Installed a new program? Gone. Edited a document? It's back to the unedited version. If you use your computer mostly for surfing the Internet, this seem like no big deal. Oh, but did you update Flash to play that spiffy new game? You'll have to update it again after your reboot. Any new bookmarks will also vanish. Clearly using virtualization-based protection requires a new kind of awareness.

There are some actions for which you just have to turn off virtualization. Among these are updating Windows, defragging the disk, creating a drive image backup, and scanning with another antivirus. But for day-to-day

computer use, Returnil includes a number of options for protecting particular files from being washed away by a reboot.

## Sidestepping Virtualization

Using Returnil's File Manager you can save new or changed files to the real disk. First you define a group of files and folders you want to protect. Then, at any time, you can save those files to the real disk. To avoid the possibility of having this feature manipulated by malware, Returnil specifically does not save all files in a folder; you must actively choose each file. And it's not automatic. If you edit a file and forget to save, the changes will be lost.

Returnil specifically virtualizes the system disk, the one from which Windows boots. If you have multiple partitions on your computer it's easy enough to store working files on one of the other partitions. They won't be wiped out by a reboot. Of course, the rare malware threat that installs on non-system partitions will also survive reboot, but it will be powerless because any file or Registry commands that would launch it at startup have vanished. Don't have that spare partition? Returnil can create a Virtual Disk that's accessible whether or not virtualization is active and that isn't affected by a reboot.

Advanced users can actually dig in and view the file structure of the real disk and the virtualized disk side by side, copying items from one to the other. A similar feature allows comparison of the real Registry and the virtual Registry. However, this isn't something you'd use under any normal circumstances.

It's bound to happen—eventually you'll install an important program while virtualization is turned on. It might not be safe to reboot into non-virtualized mode and reinstall, not if you've already activated the application's license. Fear not! There's an option to configure Returnil so that just this once it saves all changes to the real disk on reboot instead of discarding them.

On the flip side, the File Protection feature lets you extend a modicum of protection to files that are not found on the system disk and hence are not protected by virtualization. As with the file manager feature, you select a group of files and folders to be protected. Thereafter, any time File Protection is turned on all access to those files is blocked.

## Execution Limitation

Returnil's virtualization only affects your local system. Rebooting won't un-send e-mail messages you've sent, or call back Web forms you've filled out. It also won't recover personal information stolen and sent "home" by malware. Sure, on reboot the malware is gone, but the damage has been done.

To guard against this kind of problem, Returnil includes an option to prevent execution of any program that doesn't exist on the real disk. A drive-by download (or any newly-downloaded program) just won't run. Returnil suppresses such files quietly, but you'll find a note in its "Messages" log that says the file was blocked from executing.

Overall Returnil's, protection via virtualization is effective and well thought out. Without effort on your part any malware that may get onto the system will vanish at the next reboot. Yet Returnil also offers many different ways to ensure that specific files do get saved to the real disk. There's still a certain awkwardness involved in having to turn off protection for tasks like Windows Update, but that's the nature of this type of utility.

## Reboot Really Restores

This edition of Returnil doesn't attempt to recognize and block malicious software. I did launch my standard collection of malware samples, and as expected it didn't stop them in any way. However, in every case the malware installation was totally gone as soon as I rebooted. The flip side of that statement is that until I rebooted the malware was free to root around in my test system and steal any personal information it could find. If you're relying on Returnil's protection, you'll definitely want to shut down at the end of the day and boot fresh each morning rather than using standby or hibernate.

I'd strongly recommend using traditional antivirus alongside Returnil. For \$10 more, you could get Returnil Virtual System 2010 Home Lux, which has traditional antivirus built in—but in testing, it totally bombed. Instead I'd add a free antivirus to the Home Classic edition. Most of the Free Antivirus and Antispyware don't quite match the power of paid antivirus products, but, some, like Panda Cloud Antivirus Free Edition 1.0, come pretty close to the paid products even without help. Teamed up with Returnil, that'd be a quite effective security combination.

You will need to do a little work on the interaction between the antivirus and Returnil. Turn off automatic updates and scheduled scans, since these are pointless when the system is virtualized. Leave real-time protection active. And, once a week or so turn off virtualization, update the antivirus, and run a scan. Update Windows and any other programs while you're at it. Then re-enable virtualization.

Returnil also offers a totally free edition that omits the virus scanner but does include real-time antivirus protection. The free edition can create a virtual disk for storing files that won't be wiped out on reboot, but it omits the ability to access the real disk directly or save files to the real disk using the file manager. The free

edition doesn't include customer support, but with the simplicity of the virtualization system, many users won't need support.

The virtualization-based security at the heart of Returnil is totally effective in the sense that any malicious changes can be reversed by a reboot. It offers a number of options for handling files that shouldn't be wiped out on reboot, though you simply must turn it off during certain system tasks. Your system can still be pwned temporarily by malware, but only until the next reboot. It's definitely effective and especially useful for those who focus on Web surfing and don't install a lot of programs locally.

Read more from About.com at: <http://www.pcmag.com/article2/0,2817,2363909,00.asp>