The 120-day Microsoft security suite test drive

By Fred Langa

Frustration with most commercial antivirus suites launched a long-term, real-life test of Microsoft Security Essentials, Microsoft's free anti-malware application.

In one of the rare extended tests outside a lab, Microsoft's software has quietly kept two Windows 7 PCs free of infections, even in dangerous public environments.

I've tried many commercial security suites over the years and eventually grown unhappy with each of them. An anti-malware publisher would layer new features on top of old, and each new version would require more disk space and system resources — eventually making the software too big, too slow, or too hard to customize. Moving on to another publisher's suite only restarted the same pattern.

So four months ago, I decided to look into a new option: the recently released Microsoft Security Essentials (MSE) — the company's first antivirus and anti-malware application. (MSE is available as a free download from the product's info page.)

So far, my real-life test drive indicates that Microsoft may have finally got basic security right.

Three critical elements for basic security

I generally rely on three interlocking kinds of security protection: First, a firewall to protect against direct hack attacks. Next, various built-in filters and prescreens provided by online apps (browsers and e-mail, for example) to block malware downloads and prevent open doors to bad sites. Finally, an active anti-malware tool that monitors all file activity. The software screens out known or likely worms, viruses, Trojans, and other malicious code — either by identifying them directly or by watching their behavior.

For the first time, in Fall 2009 Microsoft provided all three pieces of the online security puzzle — and offered them free.

It's been a long time coming. Microsoft's first serious foray into online security was Internet Protocol Security (IPsec) — a primitive kind of firewall — bundled with Windows 2000. Improved and extended a bit in XP, IPsec became a fully functional firewall in Vista and was further refined in Windows 7.

Today, Win7's built-in firewall can protect as well as many third-party products can. (A WindowsSecurity.com article details what's in the Win7 firewall.)

Microsoft's anti-malware efforts began in earnest in 2005 when Microsoft bought out the modestly respected Giant AntiSpyware. Revamped and eventually renamed Windows Defender, Microsoft hoped this free antispyware application would bolster XP's aging and massively attacked infrastructure. Indeed, XP users can still download it from its product page. Later, Windows Defender was bundled into Vista and Windows 7.

But Windows Defender didn't specifically target viruses — a glaring omission. Microsoft Security Essentials finally corrects that.

MSE is a general anti-malware tool, protecting against viruses as well as the kinds of threats that Defender handled. In fact, MSE automatically disables any versions of Defender it finds on a PC. That's important because duplicated security services will ***often*** cause trouble. The rule of thumb is never to have different security tools performing the same job at the same time. MSE is smart enough not to compete with a sibling tool.

Running all-Microsoft protection — in the wild

With Microsoft now providing all the major pieces of a comprehensive security setup for free, the question arises: Do you really need any third-party security software?

To find out, I uninstalled all third-party security apps from two Windows 7 systems — one a portable, one a desktop — and created a basic security setup using only Windows' built-in firewall and Microsoft Security Essentials in their default state (no customizations).

Both machines included Mozilla's Thunderbird for e-mail and Firefox and IE8 for browsing (all fully updated and set to their default security states).

After four months of running those setups not just in my home office, but at public hotspots that are a potential gold mine for hackers — WiFi in coffee shops, hotels, and airport lounges — I have yet to see a successful attack on either system. (Later, I'll explain how I tested the systems to make sure the security tools were doing their job.)

One other note about testing MSE: Most of the lab tests of this security suite's AV capabilities are extremely dated — typically, completed when the product originally launched.

In my search of the Web, I could find only one recent lab test of MSE. A brief April 14 report by MaximumPC stated that the suite passed its synthetic testing "without so much as flinching and fared equally well at thwarting our attempts to inflict damage with genuine payloads."

Although that report backs up my findings, this review — as far as I can determine — is the only extended in-the-wild test published.

Security working quietly behind the curtains

In operation, Microsoft Security Essentials is nearly invisible — there's almost no user interaction needed. (Windows' firewall, likewise, has never needed much interaction.) MSE automatically scans files when they're created or accessed, and it monitors system activity for suspicious malware-like behavior. MSE also performs unattended scans of your entire system at a time you designate. MSE even updates itself silently in the background.

MSE calls for attention only when it finds trouble, as shown in Figure 1. But you can skip even this minor level of interaction if you direct MSE to automatically run recovery actions such as remove, clean, or quarantine.

Figure 1. Microsoft Security Essentials works quietly in the background until it discovers a potential attack. In this case, it intercepted malware in Firefox's cache.

You can't, however, ignore MSE's full scans — they can grind on for hours, as Figure 2 illustrates. The first few times I ran it, each full scan of my 1.5TB laptop took about a full day to complete. (See Figure 2.) Even running the scan mostly at night didn't let it finish in a reasonable time. Other MSE reviewers also noted long scan times.

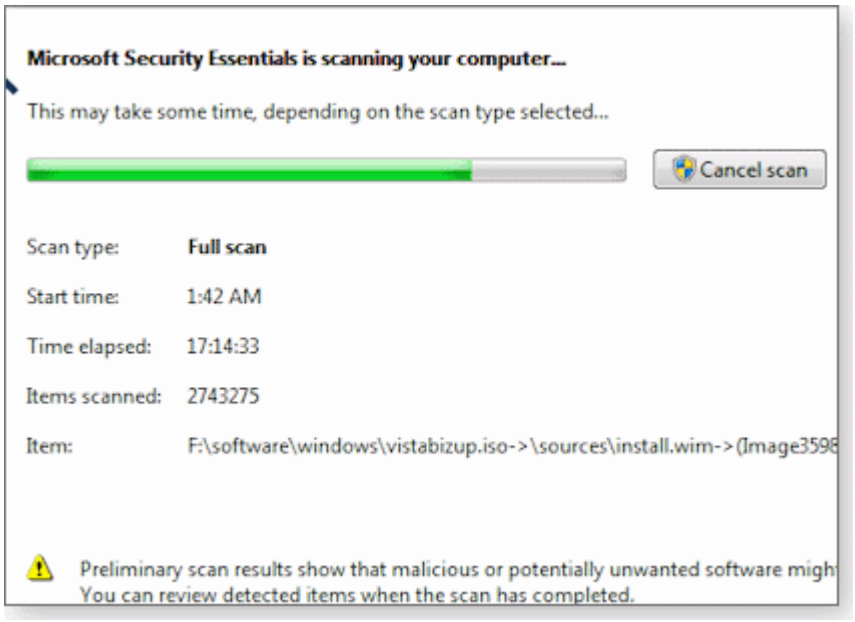

Figure 2. Though thorough, MSE's full, file-by-file scan is exceedingly slow. This dialog window displays the progress after 17 hours — in what turned out to be a 24-hour process.

Fortunately, once a system is completely checked, you reduce the need for full scans. After confirming that all of my files were clean, I reset MSE to focus only on the most-frequently used partitions. Now scans complete in a couple hours, at night, when the PC is otherwise idle.

Trust is good, but verification is better

Before giving MSE a thumbs-up, I had to know for sure that it was working. As Figure 2 shows, it did catch attempts to download malware onto my machines. But did it miss any?

To check, I periodically scanned my Win7 systems with standalone security tools that would not interfere with MSE. That way, I continually ensured that no new infections had taken up residence in my machines.

Typically, I ran a different scanner each night: Microsoft's Windows Live Safety Scanner, then ESET's Online Scanner, then either McAfee's FreeScan or Symantec's Security Check. (See Figure 3.)

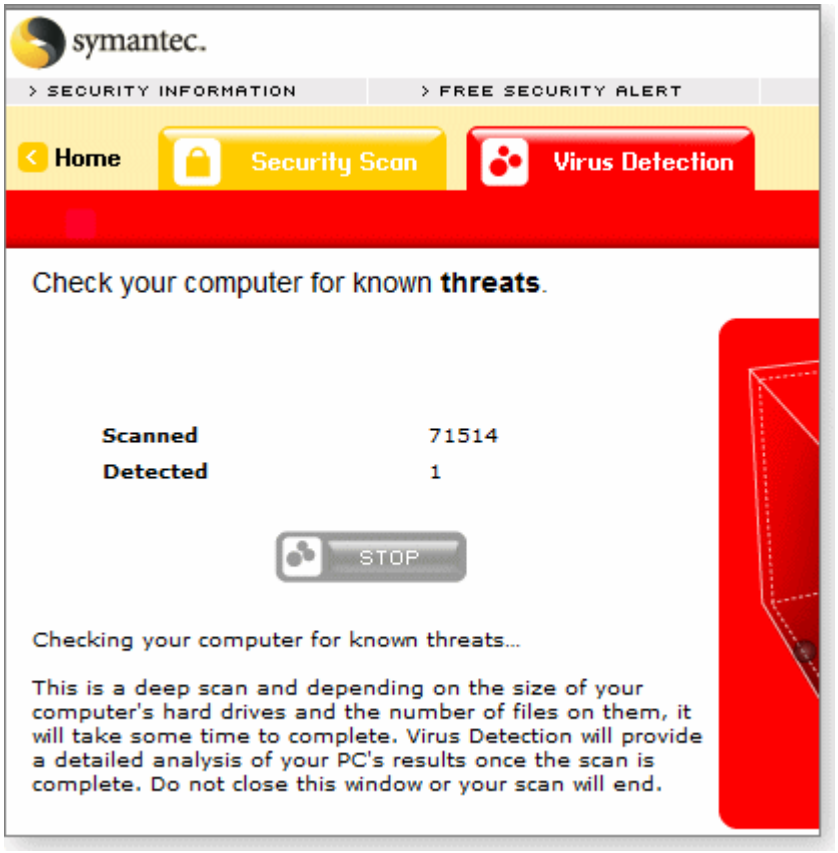

Figure 3. Using several standalone, third-party online AV scanners, I verify that my PCs remain uninfected. The one "infected" file detected in this scan was a known false positive.

These scanners do pick up dubious bits from time to time. For example, I have several password-recovery tools that all the scanners tag as malware (when obviously they're not.) So-called ***tracking cookies*** routinely show up in browser caches and are often tagged by the scanners as malicious. (These cookies are almost always harmless. I rarely bother to block them.)

MSE gets a thumbs-up, but with caveats

Four months in, and no malware has infected my Win7 systems. I've experienced no malware-like misbehavior on my machines, and to the best of my knowledge, my systems remain clean and unhacked.

So I'm comfortable saying that the combination of the Win7 firewall, Microsoft Security Essentials, and fully current

browsers and e-mail clients is proving to be a wholly acceptable security solution for routine use.

However, I'm not ready to recommend this combination to advanced users — especially those with demanding needs or who require the ability to easily customize their setup.

For example, MSE is harder to customize than competing software. Built to run mostly in full-automatic (for maximum ease of use), MSE lacks an advanced mode — where you can dig into the app and modify how it works. Maybe I have spent too many years tinkering with Windows, but I feel uneasy with a ***black box*** solution.

Other (mostly early) reviews of MSE echo my sentiments. Examples include:

- Ars Technica's September 29, 2009, article, "First Look: Microsoft Security Essentials Impresses"
- PC World's Oct. 2, 2009, security blog, "Microsoft's Free AV Looks Good in New Test Results"
- PC Mag.com's March 3, 2010, review, "Microsoft Security Essentials Probably Not for You"
- Washington Post's Sept. 30, 2009, report on AV-Test's MSE performance results.

MSE's poorest reviews come from synthetic lab tests that exercised MSE in isolation. While that's interesting information — it makes me go, "Hmmmmm" — security tools don't work in isolation in the real world.

As I've already stated, ***in combination*** with the Win7 firewall and up-to-date browsers and e-mail apps, MSE kept my PCs clean. Weigh the evidence for yourself.

I'll continue my tests — probably for another three months — and let you know what I find.