



[Click here](#)



[Login](#) | [Register](#)

Search GCN GCN

[Our Sites](#) | [Current Issue](#) | [White Papers](#) | [Subscribe](#) | [Blogs](#) | [eSeminars](#) | [Resource Center](#) | [Events](#) | [Jobs](#) | [FAQ](#)

GCN Hot Topics:

[Tech/Products Home](#) | [Authentication/ID Mgt.](#) | [Content/Record Mgt.](#) | [COOP/Telework](#) | [Data Mgt.](#) | [Defense IT](#) | [Enterprise Arc](#)
[Geospatial](#) | [Hardware](#) | [Homeland Security](#) | [IPv6](#) | [IT Mgt.](#) | [State & Local](#) | [Software Apps.](#) | [Web Strategies](#) | [Workflow/Collab](#)

[GCN Home](#) > 08/13/07 issue

You are naked without it

GCN Lab review | Antivirus programs seek and destroy malicious code waiting to pounce on remote systems

By John Breeden II

Story Tools: [Print this](#) | [Email this](#) | [Purchase a Reprint](#) | [Link to this page](#)

[Listen to this story](#)



More on this topic

The GCN Lab's unprotected laptop on the Web

16—Minutes to first infection

263—Viruses after one day

57—Pieces of spyware after one day

An antivirus program used to be like an insurance policy on your car: something that came in handy should you have an accident. But as the amount of malicious code has increased, antivirus has become more like oil in your engine. Your computer might run a little ways without it, but it won't get far.

The core of any good security system is antivirus, though anti-spyware and anti-spam protection are also important. During the past few years, the GCN Lab has reviewed appliances that sit at the gateway to a network and zap all kinds of malicious code before it even hits an agency e-mail server. But what about traveling employees or teleworkers? Sure, they can connect to the office via a virtual private network or other secure link, but that might not

always be available. Those mobile warriors need personal protection when away from their agency's digital fortress.

Thankfully, there are many security options for laptop PCs or stand-alone desktop PCs. The GCN Lab took a look at six programs designed to make the road a little bit safer. Specifically, we looked at antivirus programs and tested them for functionality — how well they were able to detect and zap all the stealth viruses we threw at them — ease of use, scan speeds and value.

To first prove the need for antivirus programs, we setup a honey-pot system on a laptop PC loaded with fake credit card numbers, a document we labeled top- secret and several MP3 files. The laptop was left outside the lab's firewalls and appliance-based protections, sitting powered and vulnerable like a goldfish swimming with sharks. The system was remotely monitored 24 hours a day, but otherwise no interference was given to any would-be hackers.

Surprisingly, it took 49 hours before the first intrusion occurred. That person took the MP3s and the fake credit card numbers, but had no interest in the top-secret document. For good measure, they dropped a P variant of the Netsky virus into the system on their way out. Nice guy. We traced the intruder's IP address to a server in the Far East.

After scrubbing the system, we repeated the experiment, but this time, we had the computer actively going to Web pages, checking e-mail and doing daily tasks. Of course, the infection occurred much more quickly and did not involve a hacker per se, but malicious code inserted by a Web page and several viruses that came in via e-mail, including the now-popular "A Classmate/friend/ family member/lover/school friend or your favorite pet has sent you a postcard, so please click here to get it" scam. Time to first infection: 16 minutes. Total number of viruses on the system after one day of running unprotected: 283, plus 57 pieces of spyware. Chance of working a normal day without any virus protection on your remote system: about equal to a paper dog catching an asbestos cat running through hell.



Latest News ■ **Washi**

■ **GCN.com**
The latest technology ne

- DHS bares upgrades to
- Certifiably geospatial
- OMB focuses on 'Core
- CompTIA floats printer
- CBP: Protecting our b

For our antivirus testing, we set up a fairly fast Pentium 4 laptop computer with 512M of RAM. After installing an antivirus program, we threw several known viruses at it from the GCN Lab's virus zoo in addition to some other forms of malicious code, such as tracking cookies from nefarious Web sites to see how the software worked.

We also planted a few viruses before adding the antivirus software, just to see how the software would handle it. We ran and timed a full scan, and recorded how long a typical update process took. At the end of each test, we uninstalled the software and replicated a plain-vanilla image to the system so that the next program would experience an identical situation.



NOD32 Version 2.7

Given a NOD: The interface for the NOD32 is clean.

Functionality: B+

Ease of use: A-

Speed: A

Value: A

Pros: Clean interface, very fast scanning.

Cons: Did not detect tracking cookies or other less dangerous threats.

The NOD32 software from ESET installed on our test system in just 2 minutes, 34 seconds. A reboot was then required.

It did not detect some tracking cookies we installed on the system before the virus protection came online, but it did find several viruses and even a rootkit once it was running. It does not attempt to scan a system as part of the install, something we found and liked about other programs in this review.

The interface for NOD32 is clean, although some of the terms used are not explained. Its main window is just a single window listing the various components of the NOD32 protection, though no effort is done to tell a user the difference between the AMON, DMON, EMON, IMON and NOD32 modules. If you click on them, you can probably figure out what each one means. AMON, for example, is the file system monitor, although we don't know what the acronym stands for. You would think that a file system monitor would be called FMON.

Clicking on any of the modules will open a second window that appears by default next to the main one. It tells you if the module is enabled and lets you configure how it should perform. For example, you can set the program to ignore, block or prompt a user for more information when a potentially bad program tries to access the Internet. This is all done easily once you figure out the main menu.

The first update took only 20 seconds and subsequent updates averaged only 8 seconds each. The scan time was also fast, finishing with the system in just 19 minutes, 40 seconds. However, NOD32 did encounter several locked files during the scan that it was unable to access. It let us know that these locked files were encountered by letting their names and locations scroll by in the scanner interface, but it gave us no option to fix the problem. This would leave a user to wonder if there was a problem with their system. It's bad form to show an error report in red letters during the scan and then not explain what it meant or how to fix it. In any case, NOD32 found all the viruses we implanted on the system and blocked all others from entering.

The government price of \$23 per seat with one year of service or \$35 per seat with two years of support is good.

ESET, (619) 876-5400, www.eset.com



AVG Antivirus 7.5 (build 476)

Systems Czech: Czech Republic-based Grisoft produces AVG Antivirus for \$38.

Functionality: B+

Ease of use: A+

Speed: B

Value: A

Pros: Extremely easy to use, good value.

Cons: Scan speed is slow, does not find some internet threats such as tracking cookies.

Many people might be familiar with Grisoft, a Czech Republic-based company — they also have an office in New Jersey — because of their revolutionary stance that the reason so many viruses exist is because people can't afford protection. As such, they released a free antivirus program that any nonbusiness home user can download to protect their computer. That free program is good, but there is also a version of the software you can pay for, which comes with support and help should anything go wrong.

The version of the software that you pay for, and which we tested, is reasonably priced at just \$38, which includes



TOP JOBS FROM LOCAL AREA

- [Information Security Associates, Inc.](#)
- [Applications Engineer](#)
- [Web Developer \(GU\)](#)

two full years of updates.

There are a few reasons why the AVG software is perfect for traveling employees. The most important one is the speed at which updates occur. Just about every time you log on to the Internet, the AVG software will query a server to see if it has the latest virus profiles. The update process happens by default as part of the boot-up process. In our testing, an update was ready for download almost every day and certainly every two days. But the updates were extremely small, mostly always less than a megabyte. Typically, it took only 11 seconds for the update process to complete. The first update process took 26 seconds.

AVG was a little slower than most when running a full-system scan. It took the program 45 minutes to complete the scan, and then it only reported scanning 95,824 files. By contrast, some of the other programs scanned more than 200,000 files. It could be argued that some of those extra files, such as text files, probably would not contain viruses. But still, given the stealth nature of viruses today, a full-system scan should look at everything just to be sure. You can change the slowness of the scan by setting the scan priority. But when we gave the scan top priority on the system, it only made the scan slower. One advantage is that you could do work while the scan was running. In any case, the quick nature of the updates was balanced a bit by the slow scan times.

In terms of ease of use, you won't find a better interface. Big, clickable icons lead to controls for all aspects of the program, and a big jail icon shows all the intercepted viruses and puts them into the virus vault for cleaning or destruction.

The AVG program did not detect any cookies or other less dangerous code that a user could pick up from the Web. Nevertheless, it zapped any actual viruses we threw at it, whether it was on the system before the scan or inserted after the protection curtain came up.

AVG Antivirus 7.5 is a good basic virus scanner that is easy to use and perfect for people who travel to places that lack broadband Internet connections. The tiny daily updates are fast even with a dial-up modem connection — at least quicker than any other program reviewed here.

Grisoft, (no phone number) www.grisoft.com



Panda Internet Security 2008

Vicious panda: The Panda software viciously tracks down viruses and cookies.

Functionality: A+

Ease of use: A

Speed: A-

Value: B+

Pros: Gives users a lot of info, deletes anything remotely suspicious.

Cons: Does a few things without asking.



When Panda software wanted to submit a beta of its 2008 antivirus software, we were a little skeptical; we put betas through the same rigorous testing as released software. But Panda representatives insisted. Panda Internet Security 2008 more than lived up to our expectations.

Installing the software was simple and easy, taking 4 minutes, 52 seconds, plus a reboot. It was the only program to find all 10 of the cookies we put on the test system, and it did it before it was even installed. During the install process, the program runs an anti-spyware scan. During this scan, it found all 10 cookies and automatically deleted them. The bad part about this was that seven of the cookies were not malicious, and we were given no choice as to their fate. The software just killed them without prompting and then finished the install.

Once installed, the Panda software was no less vicious in tracking down and eliminating all the viruses we had put on the system, in addition to others we tried to implant through various means. One nice feature is that the software constantly scans all active connections into or out of a system for anything suspicious. One screen shows you each and every port that is open on a system, what programs are using them and where the programs are located. This makes it impossible for any program that tries to get to the outside world to do so without detection. A separate screen monitors wireless access to a system, so you are protected from that angle, too.

The first update was a little long, at 2 minutes, 34 seconds, but a full scan took only 31 minutes, 7 seconds. And when we say a full scan, we mean it. The Panda software reported scanning 522,385 files, which is way more than any others in the review. Granted, most of these files might be unable to contain a virus, but given that a scan only takes 31 minutes, why not look at them? And it found every virus on the system, so it's both accurate and fast. And although this is mostly nonessential information, we like being told how many viruses the software is shielding us from. In this case, there are 533,079 in its database, according to what it told us at the end of an update.

In addition to antivirus, you also get anti-spam, anti-spyware, backup help and a program to optimize system performance.

The one thing we did not quite like was the price, which is \$69.95 with a year of system updates. That is a bit expensive, but considering Panda Internet Security 2008 works better than any other program in this review, has a good interface, is speedy and contains a lot of extras, that might not be so bad.

It earns our Reviewer's Choice designation for this review.



CA Threat Manager 8.1

idle Threat: Experts might appreciate the Threat Manager's customization, but most users will wonder how much longer they must wait for the updates to finish.

Functionality: A

Ease of use: C

Speed: C

Value: B+

Pros: Detailed virus-handling controls.

Cons: Unfriendly interface, slow speeds.

CA Threat Manager 8.1 seems to target users who are true experts on their systems. It offers a lot of ways to tweak the program to work exactly how you like in terms of viruses and malicious code, but getting things to work is not particularly easy or particularly fast.

Right from the start, you will be waiting a while for the CA program to follow your commands. The initial install took 5 minutes, 27 seconds and required a system reboot. And for the first 2 minutes, 12 seconds of the install, there is absolutely nothing on the screen to alert a user that the program is installing.

You simply click on the setup icon and the hard drive starts spinning like mad, but nothing moves on the screen.

We were getting ready to bring up the task manager to see if perhaps we did not click on the setup icon fast enough when a note finally came up to tell us that, yes, the program was installing.

The interface looks more like an old console command box than a modern graphical one. And it even talks like an old programming tool.

When you click the button that triggers an update, you see "Success, Update Initiated" for example, as if you just cracked the code to break into the Pentagon mainframe or something.

When we triggered the first update, other than the success note, nothing seemed to happen. A tiny icon did pop up in the taskbar, however, allowing you to open a new window showing the various files being checked and updated. But it's rather easy to miss. The first update process took 3 minutes, 2 seconds.

The scan time was also the slowest in the roundup, taking 68 minutes, 43 seconds to complete.

On the plus side, you can tightly configure how the program should react when a virus is found. For example, you can have the file cleaned, renamed, deleted or quarantined. And the software can automatically monitor both incoming and outgoing files.

It has a separate list of options for how to deal with word processing files with malicious macros. The macros can be stripped, the entire file quarantined or simply deleted, for example. The level of control is impressive.

At a cost of \$60 per seat, Threat Manager is a little expensive, although volume discounts do apply. However, the number of users in any given agency who could use and appreciate such a high-level antivirus program is probably pretty small. CA, (703) 708-3000, www.ca.com



Norton AntiVirus 2007

Slow and steady: Norton AntiVirus 2007 is no speed demon, but it's reliable and a good value.

Functionality: A

Ease of use: B+

Speed: B-

Value: A-

Pros: Found malicious code missed by other programs, easy to install.

Cons: Long update processes, slower scans.

The 2007 version of Norton AntiVirus is typical of what we have come to expect from Symantec products, especially Norton-branded ones.

You get excellent protection from viruses and other malicious code that surpasses most other programs. But you also get long scan times and terminally long update and install processes.

When we installed Norton AntiVirus 2007 on our test system, we were sitting around for a long time waiting for the process to complete. It took 12 minutes, 3 seconds in total, with a large part of that time devoted to a Folder Access Check. As part of the install process it runs a scan looking for any memory resident programs that might interfere

with the virus protection and even zapped one of our test viruses during this scan. However, this part of the install is extremely quick. It's checking the file access that takes so much time.

Once on your system, don't expect things to speed up much. The first update took 19 minutes, 11 seconds and required a system reboot when completed. This was the longest by far of any program we tested. Norton breaks down its protection into many different programs.

Our first update consisted of 17 different components. For example, the trusted-application list took more than five minutes to download and install, so that list must be huge.

By contrast, a full-system scan took 44 minutes, 5 seconds, which is about average.

Once installed, the program worked great, even finding three tracking cookies we had implanted on the system during our Web browsing, something that was resident but missed by almost every other program. We installed 10 of them, but the three found and zapped by Norton were the only ones that were slightly malicious because they tracked and recorded movement on sites other than the ones the cookies came from.

The interface for Norton AntiVirus 2007 is clean and functional. In a big window, you see different status checks, such as whether you have the latest updates or if you have run a system scan recently.

Oddly enough, clicking on the status text does nothing. You have to go down to the left of the menu to, say, trigger a full system scan if one has not yet occurred. This is not a big deal, but given the Web culture, where everything is clickable, we find it just a bit odd that you can't click directly on warning text to drill down and try to fix the problem.

The price of \$39 for the program plus a year of updates is good, especially given the protection it offers.

Symantec, (408) 517-8000, [ww.symantec.com](http://www.symantec.com)



McAfee VirusScan Enterprise 8.5i

Max out: Systems administrators will likely appreciate the VirusScan Enterprise 8.5i's features, especially the maximum-protection mode that puts a PC on lockdown.

Functionality: A

Ease of use: B

Speed: B

Value: A

Pros: Great price, good performance

Cons: Interface a little sparse

We were happy to see the improvements in the interface for the McAfee program. Previously, installing one McAfee program prompted a slew of advertisements trying to get you to buy others. But the company eliminated all that junk with VirusScan Enterprise 8.5i. They may have gone a little too far in the other direction, but it is still a huge improvement.

Installing the program took 3 minutes, 58 seconds. The first update took a rather long 57 seconds, but after that, the typical update was completed in just 15 seconds.

A full system scan took 39 minutes, 48 seconds, about the middle of the road in terms of speed. In addition to just antivirus, you also get an Alert Manager program to let you know about threats and a firewall to backup the standard Windows one.

The program is extremely inexpensive for government users. Assuming you have 2,001 or more users, you can get it for just \$15.82 per node. Renewing for a second year costs \$6.32 per seat more.

Once installed, you can set the level of protection from the default standard protection all the way to maximum protection.

The program warns you that in maximum-protection mode, some legitimate programs will not be able to install, which is certainly the case but might be a good option for agencies that want to lock down their desktops and allow only a small slate of programs to run.

The interface is a little sparse. You basically see a list of components in a window and click to further access that feature. The icons for each component are a little small but are easy enough to figure out.

It's not the best interface we have seen, but it is functional.

We get the feeling that the program is not designed for the user masses anyway but for the systems administrators who manage virus policy.

If you drill into the interface, you can find some interesting data, however. One window shows exactly what the program is doing, including the last file that was scanned, any file actions that were blocked, registry actions blocked and both incoming or outgoing port transmissions that were denied.

Sort of like a building's security monitoring room, this screen lets you see if any malicious programs — or any program — is trying to sneak around your system and what exactly it is attempting to do.

This makes Enterprise 8.5i worth the price of admission alone.

McAfee, (888) 847-8766, www.mcafee.com

More news on related topics: [IT Security](#), [Software Applications](#)

SAVE UP TO \$1475
on select Dell desktops, notebooks and servers.
Some offers end 9/30/07

SHOP NOW

intel
Core 2
Duo

DELL™

MARKETPLACE

Products and services from our sponsors

Virtualization and Recovery for COOP

Virtual servers provide government agencies with the ability to do more with less, enabling the consolidation of data and applications onto a single server. Double-Take delivers affordable enterprise class DR and HA for COOP in virtual environments.

Real-Time Intelligence for Operation Success

Discover how the U.S. Air Force has been able to reduce target acquisition time by 90% through a real-time, scalable data fusion repository. Access your copy of L-3/US Air Force's Network Centric Collaborative Targeting Systems case study today.

Moving your COBOL to SOA and Web Services

Micro Focus software solutions enable government agencies to assess, manage and modernize critical applications while reducing cost, gaining mission agility and flexibility. Download a white paper Extending COBOL to SOA, Web Services and Beyond

Quickly Analyze Labor Rates & Bid More Effectively

Compare your labor rates with other vendors your size. Find out how your GSA Schedule compares to your competitors. INPUT's Federal Labor Pricing service tracks over 2 million labor rates from more than 1,600 vendors and 425 different programs.

Sealed Mouse Alternative - Small footprint, Rugged

HAND-TRAK Input Devices - small footprint, light, no moving parts, works at any mounting angle, tolerates dust, muck & vibration. Much tougher than consumer mice. Small enough to fit in the space for a numeric keypad. Designed to be customized!

[View more products and services...](#)

[Buy a link now](#)

[Home](#) | [About GCN](#) | [Contact GCN](#) | [Customer Help](#) | [Privacy Policy](#) | [Editorial Info](#) | [Advertise](#) | [Link policy / Reprints](#) | [Site Map](#)



© 1996-2007 1105 Media, Inc. All Rights Reserved.