



“Selecting the best antivirus product wasn’t easy. Taking usability into account, however, my pick is Panda Software’s Panda Antivirus Platinum 6.0.”

Desktop Antivirus Software for Win2K Pro

Prevent viruses from slipping onto your system



Not many small office/home office (SOHO) environments have an IT department at their disposal. Although you have more direct control over your Windows 2000 Professional systems in a SOHO environment, you also have to maintain those systems, including their security. Fortunately, most traditional viruses choke under Win2K Pro’s protected architecture, making your systems immune to older viruses. However, the new breed of viruses (e.g., VBS.LoveLetter, Melissa) are more distributable and polymorphic than their predecessors and can wreak havoc on your Win2K-based systems. To add to this fatalistic scenario, the Internet is the primary distribution

vehicle for viruses, so the proliferation of broadband Internet connections that let you stay connected 24 × 7 means that viruses can slip onto your systems more easily than in the past.

The good news is that vendors have refined the latest generation of anti-virus software to catch viruses before they do serious damage. The products are easier to use, have better detection rates, and are cheaper than earlier virus scanners. So you have no excuse for failing to install a good virus scanner on your system.

However, the dozens of antivirus products on the market make selecting the right program a daunting task. What criteria should you consider when selecting a desktop virus scanner? Antivirus software vendors provide mas-

sive lists of every virus that their software can detect, but these lists are primarily for marketing purposes (when was the last time you ran across the Rasputin virus?). Whether a virus scanner can detect tens of thousands of nearly obsolete viruses that don’t affect Win2K Pro isn’t important. What matters is how well a virus scanner handles the viruses that your system will face daily. All the products in this review can detect and clean the latest viruses. Being able to download and install regular virus updates without user intervention is a bonus feature. Ultimately, your decision comes down to a product’s usability. (Table 1 compares the products’ features.)

If you don’t want to devote a lot of time to maintaining a virus scanner,

TABLE 1: Win2K Pro Desktop Antivirus Software Features

| | Intuitive UI | Automatic Virus Definition Updates | Flexible Scheduling Features | Flexible Notification Features | Active Web Content Monitoring |
|-------------------------------------|--------------|------------------------------------|------------------------------|--------------------------------|-------------------------------|
| Command AntiVirus 4.59.1 | Yes | No | Yes | No | No |
| F-Secure Anti-Virus 5.0 | No | Yes | No | No | No |
| Inoculate/IT 4.53 | No | No | Yes | Yes | No |
| Norton Antivirus 2000 | Yes | Yes | Yes | No | No |
| Panda Antivirus Platinum 6.0 | Yes | Yes | Yes | Yes | Yes |
| PC-cillin 2000 | No | Yes* | Yes | No | Yes |
| VirusScan 4.5 | No | Yes | Yes | No | Yes |

*PC-cillin 2000’s automatic update feature uses nonstandard ports to connect to Trend Micro’s servers. This setup can cause problems for systems that connect to the Internet through a proxy or IP routing server.

look for a program that doesn't require coddling to run efficiently. Some users consider a product's user interface (UI) to be a cosmetic feature, but a good UI lets you configure a program without frustration and hassle. In addition, a rich feature set lets you tailor a virus scanner to your system's design and needs. If you share Microsoft Word documents only internally, why waste CPU cycles on a realtime scanner that examines the documents every time you open them? If you're hardwired to the Internet, look for a product that embeds in your TCP/IP layer.

To test the seven desktop antivirus scanners that I reviewed, I pitted each product against the viruses that currently threaten Win2K Pro systems (i.e., macro and polymorphic viruses). I timed how long each product took to detect and clean 10MB of data contaminated with 17 live macro viruses. In addition, I compared the percentage of viruses that each product detected and cleaned from the infected 10MB, a test bed of 1200 macro viruses, and a boot volume directory that contained 5000 polymorphic viruses. I also tested the products' crucial usability features, such as scheduling flexibility. The test system was my Pentium III 600EB processor system with 256MB of RAM and one 66MHz 20GB 7200rpm IBM Ultra Direct Memory Access (UDMA) hard disk. The system runs Win2K Pro with all the current hotfixes applied. This machine is one of my primary workstations, and I used each virus scanner in a live environment rather than in a simulated and sterile lab environment. For additional testing, I used Pentium and Pentium II processor machines running Win2K Pro.

Results

Selecting the best antivirus product wasn't easy. Every product I tested detected and cleaned the viruses from my system. If your only concern is maintaining a virus-free environment, you can't go wrong with any of the products here.

Taking usability into account, however, my pick is Panda Software's Panda Antivirus Platinum 6.0. It provides a comprehensive feature set and a world

of customization options at a reasonable price. When I had this software installed on my system, I knew that the files I downloaded were clean and the documents I worked with weren't infected. In addition, Panda Antivirus updated virus definitions without intervention, and its well-crafted UI simplified reconfiguring the program to adapt to my ever-changing system configuration.

Panda Antivirus Platinum 6.0

A relative newcomer to the antivirus software market, Panda Software delivers a remarkably full-featured and polished product, Panda Antivirus, that holds its own against the competition. For compatibility, the company ships on one CD-ROM native versions of Panda Antivirus for Win2K, Windows NT, OS/2, Windows 9x, Windows 3.1, and MS-DOS. The CD-ROM also includes a tutorial that provides basic information about Panda Antivirus and virus scanners in general.

To ensure a painless installation process, the company used InstallShield to build the software's setup application. A full installation consumes 24MB of disk space. I selected the full installation option, and in a few moments the software was running.

After installation was complete, Panda Antivirus spoke to me. The program uses triggers that launch sound files when specific events occur. For example, the program plays a .wav file that says "virus detected" when the scanner runs across an infected file.

I found this feature annoying, so I disabled it in the program's configuration menu.

The software offers two UI modes that strike a balance between ease of use and program customizability. For newbies, Panda Antivirus provides a basic-mode UI, which uses simple icons and menus that ease the product's learning curve. By restricting your scanning options to one of several predefined templates, the basic mode lets you take a less-involved approach to virus scanning. The more adventurous or experienced user can select the Advanced mode, which Figure 1 shows. This mode offers more granular control and lets you create your own scanning templates.

I had partitioned my desktop's hard disk into two volumes, so, using the Advanced mode, I created a scan template that included only the volume that stores frequently accessed files. (I didn't anticipate any problems with the volume that houses Win2K.) In the scan template, I also included one mapped network drive that stores backup copies of my work. To add the drives to Panda Antivirus' scan list, I clicked the icon in the drive list that corresponded to the volume in question and moved it to the scan list.

The product's scanning engine is more like a grizzly than a panda. After I clicked the Scan icon to initiate the scan, the program took about 12 minutes to plow through the 10GB of contaminated data. The software detected

Panda Antivirus Platinum 6.0

CONTACT:

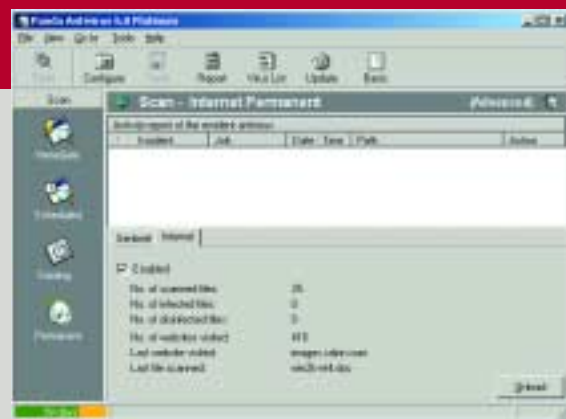
Panda Software • 818-553-0599
<http://www.pandasecurity.com/>

PRICE: \$29.95

DECISION SUMMARY:

Pros: Intuitive user interface; high detection rate; low-level TCP/IP scanning features that protect your network applications; excellent notification options

Cons: Annoying sound files



▲ FIGURE 1: Panda Antivirus' Advanced-mode UI

100 percent of the various Trojan horse and macro viruses that I had sprinkled on the volume. After it identified these viruses, Panda Antivirus quarantined the infected files on a directory that I specified and quickly disinfected them.

Not content with having the software detect the 17 live macro viruses on my system, I ran the scanner against my isolated test bed of 1200 macro viruses. The software detected 98 percent of the macro viruses.

Panda Antivirus uses a heuristic scanning engine, so the software can detect viruslike behavior. This functionality protects your system from polymorphic viruses. To test the scanning engine, I set up the product to scan a separate directory on my boot volume that contained 5000 polymorphic viruses. Panda Antivirus demonstrated an 84 percent detection rate.

The software also offers an internal scheduling service that lets you create automated scanning tasks. To do so, you simply use the scheduling configuration tool to tell the scheduler how often you want it to run the scans. You can specialize these scanning jobs depending on your system's topology. For example, I created a daily scanning task that scanned my data volume, a weekly scanning task that scanned my OS volume, and an hourly scanning task that scanned my system's mapped network drives. To be thorough, I also configured a weekly full-system scan.

The software triggered each scan as scheduled.

In addition to its on-demand scanner, Panda Antivirus includes Sentinel, a realtime scanning engine that proactively inspects your files. You can configure Sentinel to scan files according to the extension types that you specify. For example, if you work primarily with Word documents, you can set Sentinel to scan .doc files when you open them.

You can set up the software to broadcast an alert message to another computer on the network, send an alert message to an email address, and present a warning on the infected workstation when Panda Antivirus detects a virus. I opted to use all three notification options. When it detected a virus on my test system, the program displayed a pop-up warning-of-infection dialog box, sent a broadcast message to another system that I frequently work on, and fired off an email message over the Internet.

To test the notification system, I telephoned to a remote Linux-based system, attached the VBS.LoveLetter virus to an email message, and sent the message to my POP server. I had set the test system running Panda Antivirus to poll my mail server for new email messages every 5 minutes, so I waited for the software to download the contaminated message. The program detected the virus as soon as Outlook retrieved the email message.

Panda Antivirus immediately triggered all three alerts and prevented access to the file while the software disinfected the attachment.

You can use the software's internal FTP client to upgrade Panda Antivirus' virus-definition files. You can schedule the product to automatically search for definition file and product updates. You can also schedule automated updates as often as every hour and as infrequently as once a year.

Panda Antivirus works alongside Win2K's TCP/IP stack, so the software can monitor all your Internet file transfers, including files that you download from FTP sites and Web sites and files that you receive through instant-messaging applications. Combined with a good firewall and basic security settings, this product ensures that your system stays clean even when you connect to a potentially contaminated environment.

If you want a lot of functionality for a little money, Panda Antivirus is for you. The product's \$29.95 cost provides a lifetime license, which means you receive unlimited upgrades for the rest of the software's lifetime. ▲

Jonathan Chau is a contributing editor for *Windows 2000 Magazine*. He moonlights as a manager for CompuServe's Windows NT Workstation (NETWORK) and Windows NT Server (NTSERV) forums. You can reach him at jjc@win2000mag.com.



For More Information,
contact Sales at (800) 603-4922