

TECHNOLOGY ADVICE YOU CAN TRUST

**PC WORLD**[Topics](#) > [Software](#) > [Security Software](#) >

## Bigger Threats, Better Defense

**We test 16 security tools--firewalls, antivirus software, and anti-spyware programs--that aim to foil worms, viruses, spies, and hackers.**

**Mary Landesman**

From the June 2004 issue of PC World magazine

Today's malicious code does not just target your computer--it targets you. Criminals who traffic in stolen credit card numbers and identity information increasingly use viruses and worms to snare victims.

And viruses are only one of many threats. Some spam e-mail messages use so-called phishing schemes to trick recipients into revealing banking or credit card information. Miscreant advertisers use spurious pop-ups that exploit operating system weaknesses to hijack victims' browsers or install spying software.

As security threats have grown to encompass more than viruses, security experts have adopted the term malware to describe all malicious code. Combating this stew of invaders requires defense in depth--multiple barriers between the *malware* and your system. *PC World* evaluated 16 [firewalls](#), [virus scanners](#), [spyware removal tools](#), and [security suites](#) to find the best arsenal. (For our review of spam fighters, see "[Spam-Proof Your In-Box](#).")

Advertisement

### Tool Kit: Best Defenders

#### Software and Hardware Firewall Best Buys

- Trend Micro PC-cillin Internet Security 2004
- Zone Labs ZoneAlarm Pro 4.5

#### Antivirus Scanner Best Buy

- Trend Micro PC-cillin Internet Security 2004

#### Anti-Spyware Scanner Best Buys

- Lavasoft Ad-aware 6 Plus
- Spybot Search & Destroy

### Spam Filter Best Buy

- Cloudmark SpamNet

## Perimeter Defense: Firewalls

A firewall forms the first line of defense against hackers, worms, spyware, and other evils. *PC World* partnered with German security firm AV-Test to find the best.

Many homes and businesses use routers to share a broadband connection. To gauge the protection such devices provide, we tested two sample models of router and 802.11g wireless access point: Linksys's Wireless-G Broadband Router WRT54G and Microsoft's Wireless-G Base Station MN-700. Routers provide a basic firewall as a by-product of the way they handle Internet traffic. Using Network Address Translation (NAT) and Dynamic Host Control Protocol (DHCP), a router distributes private IP addresses to PCs on the network, thereby hiding them from outside computers, which see only the IP number of the router itself. Routers open ports to the Internet only if you set them to open or if the PCs on the network request data (in retrieving a Web page, for example).

The routers withstood assaults from port-scanning tools, which hackers use to find vulnerable targets. Since no system on the network had requested the data packets, the routers simply dropped them. Both products let us open select ports and assign them to the IP addresses of specific PCs. Known as *port forwarding*, this process lets you run servers for online games or Web sites without exposing other PCs on the network. One nice feature about Microsoft's unit: It enabled WEP encryption by default and generated a key to help protect wireless traffic. (For more on Wi-Fi security, see May's "[Beating the Wireless Blues](#).")

## Software Firewalls Watch Your PC

A router defends against outside attacks. But some types of malware--such as worms, Trojan horses, and spyware--work from within. You need a PC-based software firewall to stop them.

A purely permissions-based firewall alerts you when any application tries to communicate over the network, and enables you to block it. This will draw your attention to potential malware apps.

As a convenience, the firewalls in Panda Platinum Internet Security and in Symantec Norton Internet Security 2004 automatically granted permission to many Windows applications, but this measure can compromise protection. For example, Panda's provision to allow access for Windows services left open port 135--which the infamous Blaster worm uses to squirm into PCs. Panda fixed this vulnerability after we alerted the company.

Obviously, a security suite should permit its own components to run. McAfee Internet Security Suite 6, however, did not. Our attempts to send e-mail were thwarted by McAfee Privacy Service alerts reporting that MCSHIELD.EXE and MGHTML.EXE (two components of its own suite) were attempting to access a "guarded file,"--the e-mail client's application.dat file.

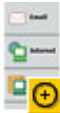
## Wrestling Worms

Programs	Access	
	Trusted	Internet
Generic Host Process...	✓	✓
Internet Explorer	✓	✓
Messenger	✗	✗
Microsoft Outlook	✓	✗

Sygate's Personal Firewall Pro 5.5 and Zone Labs' ZoneAlarm Pro 4.5 neither attacked themselves nor granted carte blanche to other applications. Consequently, they give you great power to monitor your system. But if you don't have the patience to ponder an alert before clicking 'OK', you may put yourself at greater risk.

Consider the Bagle worm, which hides its identity by injecting itself into the Windows Explorer application. When AV-Test infected a system with this worm, the McAfee, Norton, Sygate, and ZoneAlarm firewalls asked if Windows Explorer could access the Internet.

Attentive users might wonder why the app was spontaneously trying to access the Internet, but others might simply click the OK button without considering the implications.



To avoid such problems, you might opt for a port-filtering firewall of the type included in the Windows XP operating system or a port- and packet-filtering firewall like the one in Trend Micro's PC-cillin Internet Security 2004 suite. Packet-filtering firewalls monitor data passing to and from the computer and look for known vulnerabilities or suspicious behavior. For example, they can block attempts to access backdoor ports that e-mail worms may have opened to receive instructions from remote hackers.

Normally, you won't need a firewall to catch a worm or backdoor program; that's the job of an antivirus utility. But antivirus scanners work best when they can compare potential viruses against databases of previously identified viruses. New threats usually go undetected until specific updates can be created, released, and applied--a lapse in coverage that may range from a few hours to a few days, as AV-Test found in a separate, extensive survey of antivirus companies' outbreak response times.

For our review, AV-Test challenged the firewalls with common worm attacks. For example, testers installed a program that attempts to mass-mail several hundred copies of itself as an executable attachment. Both the McAfee and the ZoneAlarm firewalls stopped the action by using a throttling feature that warns of attempts to send messages to many recipients at once or to send a single message repeatedly. Panda thwarted the worm with a feature that blocks outgoing e-mail containing executable attachments.

In another test, Panda did not block an attempt by the Bagle worm to open a backdoor port on a system and receive instructions from a remote hacker. The two routers did block the action, and the software firewalls from McAfee, Norton, Sygate, and ZoneAlarm provided alerts about the attempt, but they identified Windows Explorer as the application using the port, and could not tell that a worm was piggybacking on Windows Explorer in order to evade detection. The port-filtering PC-cillin and Windows XP firewalls blocked attempts to access the worm through the port, thereby silently protecting the computer, without requiring users to interpret alerts as they would have to with the permission-based software firewalls from McAfee, Norton, Sygate, and ZoneAlarm.

In addition to opening backdoor ports, malware may try to expose a PC by disabling security software. Panda, Sygate, and ZoneAlarm Pro resisted such attacks. But invading code shut down the Windows XP firewall and McAfee, Norton, and Trend Micro suites, and deleted the program files of the latter three.

## Combine Forces



Routers like the Linksys and Microsoft models fend off externally launched attacks, while software firewalls protect systems from worms spread through shared drives, by e-mail, or via file-sharing applications such as Kazaa and Gnutella. Software firewalls are also a must for laptops that leave the protection of a home or office router and connect to public Wi-Fi hotspots or hotel networks.



We liked Sygate's performance and granular configuration options but found the program confusing. Consider this Sygate alert: "Internet Explorer (IEXPLORE.EXE) is trying to connect to www.microsoft.com (207.46.134.221) using remote port 80 (HTTP - World Wide Web)." ZoneAlarm asked, "Do you want to allow Internet Explorer to access the Internet?" ZoneAlarm Pro 4.5's usability and performance earned it our Best Buy. If you don't have the patience to configure a permission-based firewall, PC-cillin's port-filtering firewall is a worthy alternative Best Buy.

## Features Comparison: Combine Software and Hardware Firewalls (chart)

Software firewall	Product type	Street price when ranked	Ease of use	Performance	Protects against shutdown	Protects against deletion	Blocks Bagle worm backdoor	Blocks Bagle worm mass mailer	Blocks basic port scans	Blocks outside access to shared drives on network	Blocks Windows Messenger pop-ups	Comments
<a href="#">Microsoft Windows XP, SP1 Internet Firewall</a>	Port-filtering software firewall	Free with Windows XP Home and Professional operating systems (3/15/2004)	Very good	Good	No	Yes	Yes	No	Yes	Yes	Yes	Included as part of the Windows XP operating system, but not enabled by default. Its non-permission-based port filtering is a good free choice for people who run Windows XP.
<a href="#">Network Associates McAfee Internet Security Suite 6</a>	Permission-based software firewall	\$70 (3/15/2004)	Poor	Good	No	No	Yes	Yes	Yes	Yes	Yes	Bundled firewall offers good protection but conflicted with other components of the suite, resulting in testers' inability to send e-mail.
<a href="#">Panda Platinum Internet Security</a>	Permission-based software firewall	\$80 (3/15/2004)	Fair	Fair	Yes	Yes	No	Yes	Yes	Yes	Yes	Firewall's preconfigured permission list automatically gives access to installed apps and components of the Windows OS, lessening security. Only product to leave a port (number 135) open to our scan tests. Panda later issued a patch.
<a href="#">Sygate Personal Firewall Pro 5.5</a>	Permission-based software firewall	\$40 (3/15/2004)	Good	Good	Yes	Yes	Yes	No	Yes	Yes	No	High degree of granularity gives experienced users maximum control. Interface can be confusing to less experienced users, but default settings provide a high degree of security.
<a href="#">Symantec Norton Internet Security 2004</a>	Permission-based software firewall	\$69 (3/15/2004)	Fair	Fair	No	No	Yes	No	Yes	Yes	Yes	Preconfigured permission list automatically grants Internet access to certain programs; though convenient, it lessens the effectiveness of a permission-based firewall.
<a href="#">Best Buy Trend Micro PC-cillin Internet Security 2004</a>	Port- and packet-filtering software firewall	\$50 (3/15/2004)	Very good	Good	No	No	Yes	No	Yes	Yes	Yes	Includes privacy controls to prevent sending of sensitive information from the PC; port filtering approach makes it a good choice for novice users. Network worm awareness isolates infected systems.
<a href="#">Best Buy Zone Labs ZoneAlarm Pro 4.5</a>	Permission-based software firewall	\$50 (3/15/2004)	Outstanding	Very good	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Best-performing program is also easy to use, with simple configuration and meaningful alert messages. A free version lacks mass-mailer protection and extras such as privacy-guarding features.

Router firewall	Product type	Street price when ranked	Ease of use	Performance	Protects against shutdown	Protects against deletion	Blocks Bagle worm backdoor	Blocks Bagle worm mass mailer	Blocks basic port scans	Blocks outside access to shared drives on network	Blocks Windows Messenger pop-ups	Comments
<a href="#">Linksys Wireless-G Broadband Router WRT54G</a>	Router port-filtering firewall	\$90 (3/15/2004)	Very good	Very good	Yes	n/a	Yes	No	Yes	Yes	Yes	Management console is slow to load, but very easy to navigate for configuring the firewall and other features. Wireless encryption is disabled by default.
<a href="#">Microsoft Wireless-G Base Station MN-700</a>	Router port-filtering firewall	\$90 (3/15/2004)	Outstanding	Very good	Yes	n/a	Yes	No	Yes (but with standard settings, allows pings)	Yes	Yes	Provides a responsive, easy-to-use management console. Intuitive setup enabled WEP encryption by default and automatically generates encryption key.

## Inside Coverage: Antivirus Apps

Though firewalls do block some port-probing network worms and may hinder some mass-mailers, you need an antivirus scanner to stop many threats that arrive via e-mail or file downloads. And only an antivirus scanner can remove the infections. To find the best scanners, we first reviewed a fresh round of testing that AV-Test had performed on 31 antivirus products. We chose six of them for a closer look: the stand-alone programs Grisoft AVG Anti-Virus Professional and Eset NOD32, plus the scanners in the four security suites from our firewall tests.

Each product met our minimum requirement of catching all "in the wild" malware. Such viruses have been sighted by at least two members of the [WildList Organization](#), a cooperative effort of antivirus researchers and member companies worldwide. Though approximately 100,000 viruses exist, only about 250 are considered in-the-wild threats at any given time.

To further challenge the scanners, AV-Test pitted them against its zoo of approximately 60,000 malware samples. Whereas in-the-wild testing gauges whether a scanner can detect current threats, zoo tests indicate how it might handle a particular class of threats or family of viruses. For example, all of our chosen products performed well (ranging between 90.4 percent and 100 percent detection) against a collection of 12,341 viruses and worms that operate in a 32-bit Windows environment--the type of infectors most common on today's WildList. But some fared less well with the zoo collection of 14,288 Trojan horses, malware that can't spread on its own but can be carried by worms or viruses or be hidden within infected downloads. Despite accounting for a significant proportion of all malware, Trojan horses are not included on the WildList. And the antivirus scanners varied considerably more in their handling of these pests: AVG detected just 23.5 percent of the Trojan horses, while the McAfee and Norton scanners nabbed 99 percent and 97.5 percent, respectively.

AV-Test also scanned 20,000 clean files to determine whether the programs would mistakenly identify any as infected. PC-cillin excelled, with no false positives; at the other end of the scale, Eset's NOD32 misidentified 31 clean files. Even a small number of false positives can be a headache, as they may cause innocent and necessary files to be quarantined or even deleted.

## Dealing With New Threats

Antivirus scanners rely primarily on exact matches to identify malware, but they can sometimes catch infectors not included in their databases by using *heuristics*. Strictly speaking, heuristics refers to the ability to identify new malware based on telltale characteristics--for example, the presence of code that exploits a known vulnerability. In practice, however, heuristics also refers to the use of "fuzzy" pattern matching to identify a new variant of a known virus, using the generic definition of a virus such as Netsky.gen, for instance, to nab a particular brand-new variant such as Netsky.R.

AV-Test gauged heuristics by scanning files containing the newest malware with versions of each program that had last been updated three months prior. McAfee and AVG performed best, catching 70.1 percent and 65.6 percent, respectively, of infected files; NOD32 did worst, at 41.4 percent.

For each antivirus program, AV-Test used the highest possible settings to scan an infected hard drive, though NOD32 was a special case. Beyond the level of heuristics available for disk scans, NOD32 has a higher level called Advanced Heuristics for scanning incoming e-mail and Web traffic (the main routes of infection). AV-Test gauged NOD32's Advanced Heuristics using an undocumented command-line instruction (nod32.exe /AH) to turn the feature on for a disk scan. With its Advanced Heuristics enabled, NOD32's detection rate jumped to 53.5 percent.

In our tests, the antivirus scanners in our roundup succeeded only in detecting new members of known malware families. They did not catch any of the truly new viruses--a finding mirrored in AV-Test's separate outbreak response survey. (This additional survey covered 22 antivirus companies but did not include Eset's NOD32.) For example, none of the products tested in the outbreak survey could identify any of the infamous Netsky worms until the vendors issued detection signatures for them; but once McAfee wrote a generic signature, the scanner was able to detect several variants. Our conclusion: Heuristics offers only hit-and-miss protection. Your best defense lies in other security layers--including firewalls and your own common sense. For example, you should frequently update your antivirus scanner and patch your operating system. For more tips, see April's "[Lock Down Your PC](#)."

## The Smoothest Scanners

Had we based our Best Buy selection on scanning performance alone, McAfee's suite would have won. But McAfee had serious flaws. For example, we received multiple script errors during the update process, and the program erroneously reported that the virus scanner had been updated when it had not.

Though McAfee's suite was the most troublesome, it was not alone in having glitches. No program aced the infection-removal test, in which AV-Test ran each scanner on systems infected with the CTX virus, the Optix backdoor Trojan horse, and the MyDoom.A worm. PC-cillin handled cleanup best, fully removing two infections and never harming the system. McAfee, NOD32, and Panda left the system unusable after attempting (and failing) to remove the CTX virus.

Sluggishness was the biggest drawback to Norton's suite. In informal tests, system startups and shutdowns took about twice as long with Norton installed as with PC-cillin or NOD32, which had the least-discernible performance impact. Norton was the slowest at running a full disk scan, too, requiring about 12 minutes on a Windows XP Pro system equipped with an 800-MHz Pentium III processor, 256MB of RAM, and a 5400-rpm hard drive with 575MB of data. NOD32 was the fastest program, at only 52 seconds. (Norton had better detection rates than NOD32, however.) PC-cillin was the next fastest at just over 2.5 minutes.

We awarded our antivirus Best Buy to Trend Micro PC-cillin Internet Security 2004. Besides offering competent scanning at a moderate price, PC-cillin has an exceptionally clean and intuitive interface. Best of all, PC-cillin was the only software product in our review to provide no-cost telephone technical support--and via a toll-free number, too.

## Feature Comparison: PC-cillin Balances Performance and Usability (chart)

Antivirus scanner	Product type	Street price when ranked	Annual renewal	Ease of use	Scanning speed	Detection performance	Overall malware detection <sup>1</sup>	False positives (of 20,000 files checked)	32-bit Windows malware detection	Trojan horse detection	32-bit polymorphic virus detection	Backdoor channel detection	Visual Basic Script (.VBS) virus detection	Comments
<a href="#">Eset NOD32 2</a>	Stand-alone antivirus scanner	\$39 (3/15/2004)	\$27	Good	Outstanding	Very good	94%	31	100%	72%	98%	84%	100%	Fastest scan speed of all the products we tested. Its small footprint is suited for older PCs. Free online support via Web-based form. No phone support.

<a href="#">Grisoft AVG Anti-Virus Professional</a>	Stand-alone antivirus scanner	\$33 (3/15/2004)	License is for two years, after which users must purchase a new software package.	Fair	Very good	Fair	82%	16	90%	24%	67%	87%	100%	Lackluster detection of zoo viruses and cumbersome interface, but small footprint is ideal for older PCs. Free support via e-mail and fax. No phone support.
<a href="#">Network Associates McAfee Internet Security Suite 6</a>	Part of security suite	\$70 (3/15/2004)	\$30	Poor	Fair	Outstanding	99%	3	100%	99%	100%	96%	100%	Top scanning performance, but conflicts and errors make it difficult to use. Free online chat support, and \$39-per-incident (must be resolved in 48 hours) or \$3-per-minute phone support.
<a href="#">Panda Platinum Internet Security</a>	Part of security suite	\$80 (3/15/2004)	\$70	Very good	Fair	Very good	92%	23	99%	72%	89%	80%	100%	Provides relatively good detection and a nice interface. Free online support via Web-based form, \$20-per-incident phone support.
<a href="#">Symantec Norton Internet Security 2004</a>	Part of security suite	\$69 (3/15/2004)	\$30	Good	Poor	Outstanding	99%	2	100%	97%	100%	94%	100%	Very high detection rates, but slow scans. Had a noticeable negative impact on startup and shutdown times. \$29-per-incident phone support. Free online knowledge base.
<a href="#">Best Buy Trend Micro PC-cillin Internet Security 2004</a>	Part of security suite	\$49 (3/15/2004)	\$15	Outstanding	Good	Very good	92%	0	99%	76%	99%	66%	100%	Good infection removal and no false positives; includes Web mail protection. Free online knowledge base. Intuitive and easy to use. Free e-mail support.

<sup>1</sup>Percentages in this column differ from those reported in the June 2004 print issue *PC World*. Those earlier numbers were incorrect.

## Filling the Gaps: Anti-Spyware

Firewalls and antivirus scanners play valuable roles in protecting your system. But they may miss several types of marketing-driven parasites that fall under the general heading of spyware--though this category includes more than just spying applications. For example, browser hijackers, a form of adware, change Registry entries without your approval to redirect your Internet start page or to change the default search service that appears when you mistype a URL. Often called drive-by downloads, many hijackers take advantage of weak security settings, sometimes automatically installing themselves when you visit a Web site. The notorious Surfbar, for example, exploits a flaw in Internet Explorer that allows executable files to download to the user's PC. Also known as Junkbar or Pornbar, Surfbar changes Internet Explorer's start page to [www.surferbar.com](http://www.surferbar.com), drops hundreds of porn site shortcuts onto your desktop, and installs a toolbar pointing to dozens more. Other hijackers do ask for permission, but in a confusing way that may deceive you into consenting.

Genuine spyware monitors your Internet use, typically to determine what you do online and to deliver targeted advertising. Spyware usually comes packaged with shareware and freeware programs. Often, the end user licensing agreements for this "free" software disclose the real cost: You implicitly agree to allow remote monitoring by third parties that are interested in collecting marketing data or serving targeted ads. Utah recently enacted a state law banning spyware (see "[Next: Outlawing Spyware?](#)"). But this measure is unlikely to have much impact. For now, anti-spyware provides the best defense.

We evaluated five dedicated anti-spyware packages: Aluria Spyware Eliminator, InterMute SpySubtract Pro Version 2, Lavasoft Ad-aware 6 Plus, Network

Associates McAfee AntiSpyware, and Spybot Search & Destroy. (New editions of two other popular utilities--PestPatrol and Webroot Spy Sweeper--were not available in time for our review.) We also tested the spyware-hunting capabilities of the antivirus scanners and other utilities contained in the Internet security suites from Network Associates, Panda, Symantec, and Trend Micro. Unfortunately, even the best performers managed to capture only a little more than half of our spyware samples. For the time being, your best strategy is to use multiple anti-spyware scanners.



During informal tests, we infected a system with an array of spyware. Norton identified only two of the seven spyware infections as they were occurring; PC-cillin and Panda alerted only on one each. When we ran the antivirus suite scanners on a system that had already been infected, they detected the executable file that creates the nefarious Surfbar infection, but they did not remove the installed toolbar, porn site shortcuts, and hijacked home page. Though McAfee's Privacy Service accurately detected all attempts to modify the Registry and urged us to reject them, it didn't detect the underlying processes in memory that were responsible for the attempts at modification. So as soon as we rejected one set of changes, another assault occurred, resulting in an endless cycle of alert and rejection until we finally capitulated to the infection.

Unlike antivirus apps that match incoming files against malware signatures to determine whether they are infected, anti-spyware products rely heavily on Registry keys and values. Spybot Search & Destroy and Ad-aware had the most reliable detection in our tests, but Spybot Search & Destroy was best at removing bad files and restoring Registry values.

Although McAfee AntiSpyware detected three infectors--Gator, Huntbar, and MyFastAccess--it removed only the latter two completely. SpySubtract Pro 2 was the weakest of all, detecting only one spyware sample: the widely known Gator dashbar.

We liked the real-time protection that Ad-aware Plus's Ad-watch component provided. In our tests, Ad-watch foiled every hijacker that tried to change our Internet preferences. (Note that the basic, free version of Ad-aware does not include the Ad-watch component.)

None of the scanners we tested even approached 100 percent detection and removal, but Spybot Search & Destroy and Lavasoft Ad-aware Plus were the most capable. In general, Ad-aware does a better job of spotting pure adware, while Spybot is more adept at detecting pure spyware. They are also about tied in other features: We found Ad-aware 6 Plus much easier to use, and it came with Ad-watch; but Spybot Search & Destroy demonstrated superior cleaning ability.

## Features Comparison: Ad-aware and Spybot Protect Best (chart)

Anti-spyware scanner	Price/annual renewal (3/15/04)	Scans Registry/memory	Allows scan of select files/folders	Rate of detection and removal	Ease of use	Performance	Comments
<a href="#">Aluria Spyware Eliminator</a>	\$30/none	Yes/Yes	Yes	29%	Good	Poor	Consistently left Registry changes behind and failed to detect and remove some infected files. Prompts for registration during setup, but allows registration only from the Help menu (after the program is installed). ★★★★☆
<a href="#">InterMute SpySubtract Pro Version 2</a>	\$30/none	Yes/Yes	Yes (folders only)	29%	Outstanding	Poor	The spyware detection was poor, but the comprehensive Internet and file-use history cleaning will deny much of your personal data to spyware. ★★★★☆
<a href="#">Best Buy Lavasoft Ad-aware 6 Plus</a>	\$27/none	Yes/Yes <sup>1</sup>	Yes	57%	Outstanding	Good	Thorough in detecting spyware and easy to navigate, but it left some Registry keys behind after cleaning. Ad-watch performs real-time monitoring. ★★★★☆
<a href="#">Network Associates McAfee AntiSpyware</a>	\$40/ <sup>2</sup>	Yes/Yes	No	43%	Good	Fair	Achieved one of the higher rates of detection, cleanly removing any malware found, but the real-time monitor failed to prevent spyware infections from occurring. ★★★★☆

<a href="#">Network Associates McAfee Internet Security Suite 6</a> <sup>3</sup>	\$70/\$30	Yes/Yes	Yes	14%	Poor	Poor	Detected all Registry change attempts, but failed to catch changes made by spyware already on the system. Privacy Service failed to detect processes responsible for infection. ★★★☆☆
<a href="#">Panda Platinum Internet Security</a> <sup>3</sup>	\$80/\$70	No/Yes	Yes	0%	Very good	Unacceptable	Ineffective spyware removal; unable to identify most spyware program files during scan of test set. ★★☆☆☆
<b>Best Buy</b> Spybot Search & Destroy	Free <sup>4</sup>	Yes/Yes	No	57%	Good	Good	Free product has some of the best spyware detection and cleaning capabilities available, but memory-resident scanning ability is very limited. ★★★★☆
<a href="#">Symantec Norton Internet Security 2004</a> <sup>5</sup>	\$69/\$30	No/Yes	Yes	14%	Good	Poor	Identified nearly all spyware application files on disk but was ineffective at removing them. Does not scan the Registry, but does include an Internet privacy utility. ★★☆☆☆
<a href="#">Trend Micro PC-cillin Internet Security 2004</a> <sup>3</sup>	\$49/\$25	No/Yes	Yes	0%	Outstanding	Unacceptable	Able to detect spyware applications on disk but could not remove them. Does not scan for Registry changes. Firewall privacy controls block sending of personal information items that the user has predefined. ★★☆☆☆

<sup>1</sup> Ad-watch, Ad-aware's memory-resident component, is available only in the paid version.

<sup>2</sup> Network Associates has not yet determined a renewal policy.

<sup>3</sup> Spyware scanner is part of a suite that includes a firewall and other utilities.

<sup>4</sup> Software author requests donations.

<sup>5</sup> Spyware scanner is a component of the suite's antivirus utility, which is available separately for \$50.

## Strategy: Defense in Depth

Layers of protection block different kinds of threats and may provide backup if one layer fails.

### Hardware router

- Using NAT<sup>1</sup> masks IP address from port scans.
- Blocks unsolicited incoming communications.
- Does not protect against most malware, such as Trojan horses, viruses, e-mail worms, and spyware.

### Software firewall

- Prevents backdoor apps, Trojan horses, and unwanted applications from sending data from the PC.
- Protects a laptop on public wired and wireless networks.
- Can block some malware, but can't remove it.

### Antispam software

- Blocks deceptive e-mail scams (phishing schemes).
- Reduces e-mail sorting fatigue, so users are less likely to accidentally activate an e-mail-borne virus in haste.

### Antivirus software

- Protects against known worms, viruses, and Trojan horses but is less effective against new infectors.
- Systems are still vulnerable to infiltration from adware, spyware, and browser hijackers.

## Anti-spyware software

- Protects against adware, browser hijackers, spyware, tracking cookies, and other Internet parasites.

<sup>1</sup>The Network Address Translation Internet standard allows LANs to use different sets of IP addresses for internal and external traffic.

## Sour on the Suites

In a perfect world, we wouldn't need multiple layers of online protection. In an almost-perfect world, a single security suite of products from the same vendor would suffice. Unfortunately, none of the suites we tested vigilantly watched all vulnerable areas. For instance, none of them were proficient at recognizing and eradicating spyware.

Overall, though, Trend Micro's PC-cillin Internet Security 2004 was the best of the suites, with the top antivirus scanner and one of the best firewalls. Combining it with the free Spybot Search & Destroy provides a good measure of security for just \$50. For even stronger spyware protection, you can get Lavasoft's Ad-aware 6 Plus. (All three programs worked together without conflict in our tests.) PC-cillin's firewall is a good choice for most users. If you can spend more money and effort to bolster your support, disable PC-cillin's firewall and install ZoneAlarm Pro 4.5. (A basic, free version of ZoneAlarm is also available.)

Regrettably, none of the suites in this review had a top-notch antispam utility, but some stand-alone products performed quite well. To find out more, see "[Spam-Proof Your In-Box.](#)"

Related Topics: [Antivirus, Software](#), [System Suites](#), [Adware](#), [Firewalls](#), [Privacy & Security](#), [Online Security](#), [Network Security](#), [Spyware](#)