New anti-virus weapon

Current antivirus programs easily prevent known types of intrusions, but with unknown hazards it is unpredictable. Test results on 10 products give us information to choose the most valuable candidates to meet the actual needs effectively.

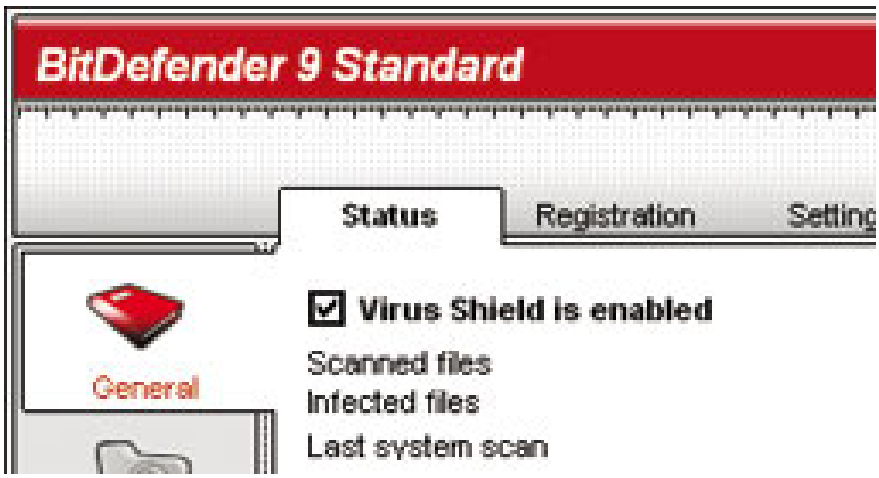
Current antivirus programs easily prevent known types of intrusions, but with unknown hazards it is unpredictable. Test results on 10 products give us information to choose the most valuable candidates to meet the actual needs effectively.

There is good news and bad news about the fight against computer viruses going on. Good news: all the products that PC World USA evaluated in this article discovered and isolated 100% of identified threats. Bad news: these tools cannot protect you completely from the emerging threats abounding on the Internet.

AV-Test (find.pcworld.com/51168), a German security software company, in collaboration with PC World USA, made this article, about 70-100 new threats appear each day. Although there are many variants of previously existing threats, in just a few hours waiting for publishers to release fixes is enough for them to attack your system. Moreover, the virus is not only a problem, there are also worms - one that doesn't need bait files to infect - and other destructive programs such as email attachments.

Because of these dangers, the antivirus program must be able to not only recognize, remove viruses, but also other types of threats.

Anti-virus tool countered



BitDefender main interface

Antivirus software companies have adapted and upgraded their products in different ways.The usual strategy is to include a traditional anti-virus program with other tools like anti-spyware (firewall), firewall (firewall) to protect users more comprehensively.The timing of the program update is shortened to deal with new hazards promptly.The heuristics of anti-virus tools are also improved, this technique can recognize new threats based on traces that are similar to known threats.

In addition, antivirus tools are equipped with behavior-based detection mechanisms to combat new threats. This technique monitors parts of the system that can be attacked, warning suspicious behavior and blocking. The drawback of this solution is that malicious programs must work on the system to be detected. For that reason, behavior-based detection mechanisms will be most effective when it is the additional protection layer behind the virus scanning mechanism before executing.

Free, independent tools and toolkits

PC-cillin aggregates lots of information in one screen
Testing the best 10 antivirus products can support both known and unknown threats, from free to $ 50.To be fair, the testing team (NTN) only checks the antivirus component of the toolkit.

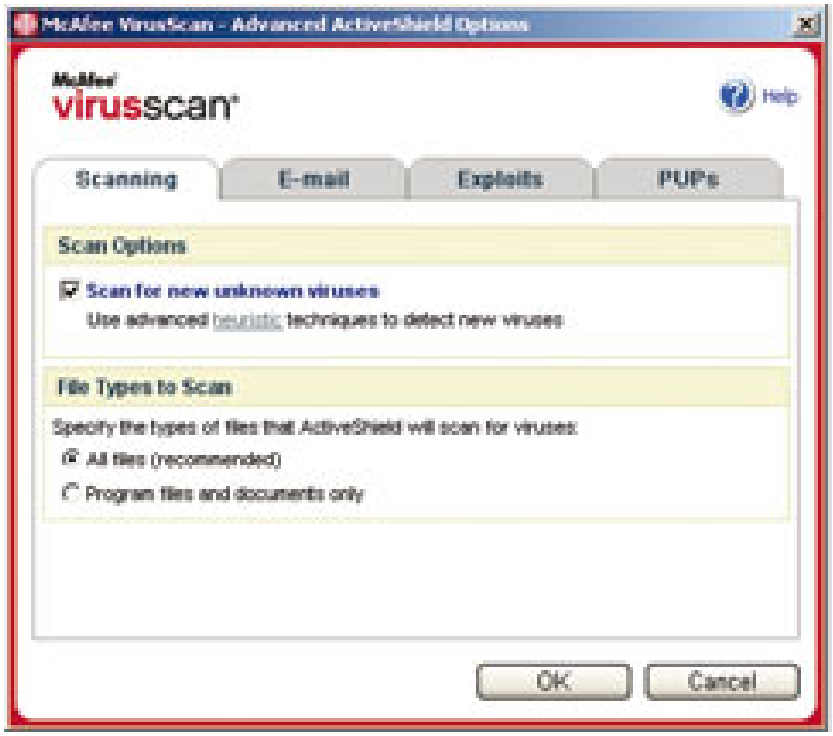
Among them, Alwil Software's Avast Home Edition 4.6, AntiVir PersonalEdition Classic 6.32 and Grisoft's AVG Free Edition 7.1 are free and standalone programs. F-Secure Anti-Virus 2006, Kaspersky Lab's Kasperky Anti-Virus Personal 5.0, McAfee VirusScan 2006 and BitDefender 9 are independent commercial applications. Panda Titaninum 2006 Antivirus + Symantec's Panda Software and Norton Antivirus 2006 all come with antispyware tools. Trend Micro sells antivirus products as part of PC-cilin Internet Security Suite 2006.

How to evaluate

In general, the test procedure consists of 5 steps.

Firstly, check the ability to detect 1,518 malicious codes identified by WildList.

Second, check the ability to detect 136,250 malicious code outside the WildList list, including Backdoor, Trojan and Bot (also called Zombie).This list is called the zoo, gathered from users, computer magazines and security research organizations.



McAfee VirusScan ranks second in heuristic testing
Third, assessing the ability of heuristics to detect new malware with programs that are not updated 1-2 months.

Fourth, check the possibility of eliminating 110 macro viruses that attack Microsoft Office applications.

On Thursday, comparing the response time of each software company "response" to 16 "outbreaks" took place in May 8, 2005.

To complete the test, we measured the virus scanning speed of each program, assessed the ease of use, features and technical support policies.

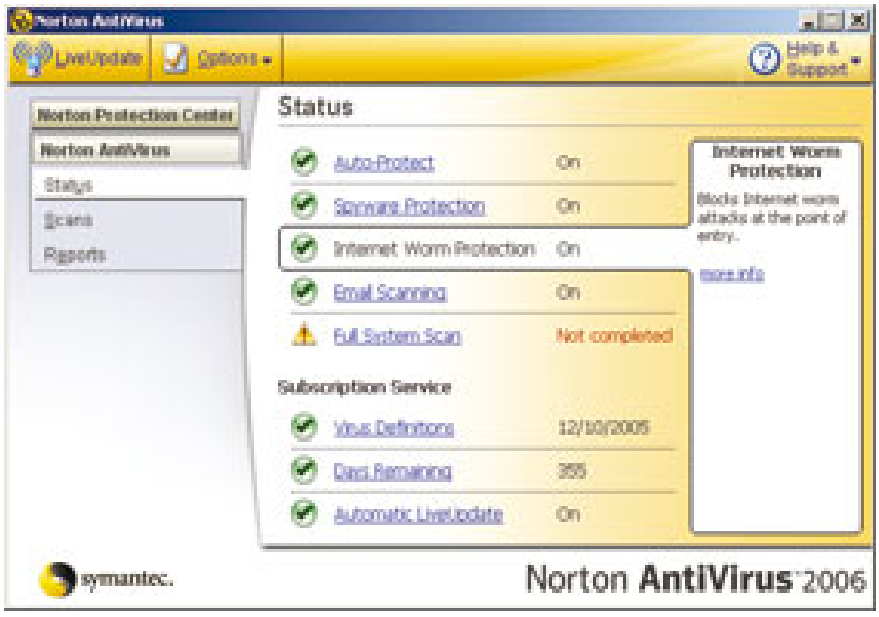
Winner

The most valuable BitDefender 9 Standard is one of the top 4 products for speed measurement and costs only $ 30. $ 40 McAfee VirusScan 2006 ranked second, the program has an intuitive interface and heuristics scanning capabilities are quite good.

PC-cillin Internet Security Suite 2006, a successor of a product that won Best Buy 2004 of PC World, ranked 9/10 because of the ineffectiveness in testing with zoo and heuristics, costing up to $ 50. However, this is a product with fast response time and excellent user interface.

Three adjacent ranking programs are AntiVir, Avast ranked 7, 8 and AVG, respectively, in the "window" position. Of course, for those who do not have the cost of antivirus software, these free products are acceptable.

Face to face



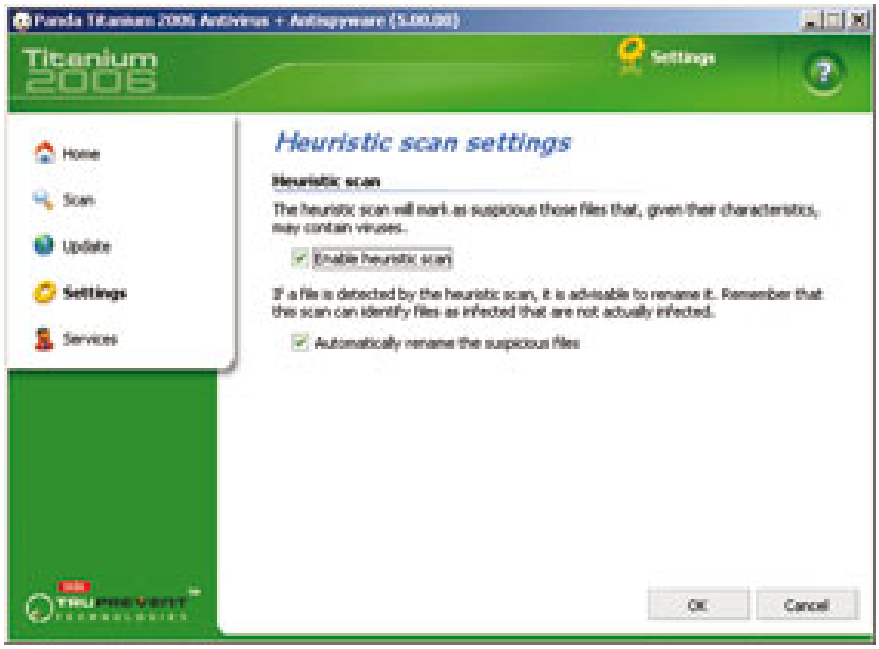
Norton Antivirus clearly explains the user interface and options
In the default configuration and the most fully updated status, all products detect 100% of the virus in the WildList list in real-time and on-demand protection mode.

All programs successfully detect and remove macro viruses, with only a few exceptions. Avast did not remove 10 viruses, including 2 viruses that attacked PowerPoint files from 97 to 2003 version and 4 viruses that attacked World 6 files. Panda did not completely clean up 2 PowerPoint viruses, but these files still working. AntiVir failed with 10 Word 6 viruses and BitDefender missed 2 viruses that attacked Word files version 97 to 2003. These viruses are not new, so programs must handle them correctly.

The ability to detect viruses in the WildList list is a basic requirement, since they are popular; but with the zoo list it is a little different.

Kaspersky Anti-Virus Personal 5.0 is the only program that successfully isolated 100% of all zoo categories. F-Secure and Symantec succeeded 97%, the score remained excellent. PC-cillin gave very disappointing results, only 76% (85% Bot, 82% Backdoor, and 69% Trojan). Explaining this, Trend Micro said that they did not focus on developing products to detect the entire zoo list because these threats had little impact on their customers.

Enemies in the dark



Heuristic feature of Panda is average

No one product is outstanding in the heuristics tests.All programs have not updated the virus identifier for 1 month, BitDefender is the most effective, detects 43% worms, 57% Backdoor.McAfee ranked second, detecting 41% worm, 55% Backdoor.F-Secure and Kaspersky followed closely behind with 32% worms, 53% Backdoor (50% detection rate was good).PC-cillin once again disappointed, scanning 5% of worms, 7% backdoor.

In the second trial, the time of not updating the new virus identification lasted 2 months, most of the programs gave "very modest" results.

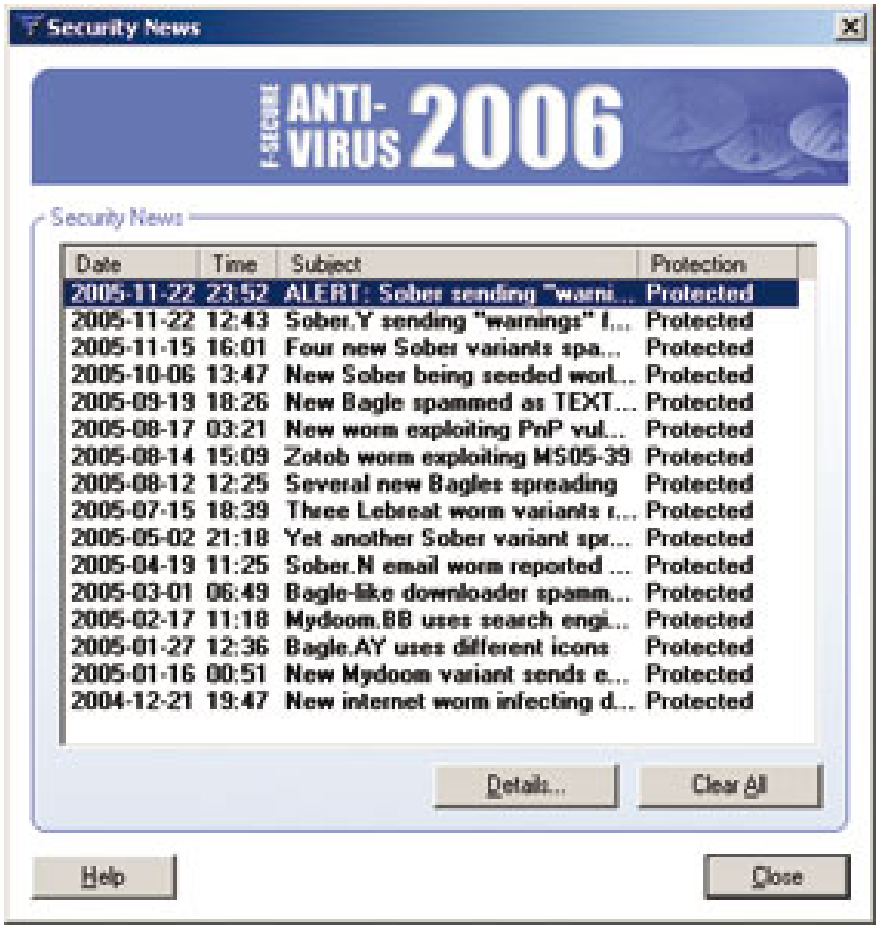
Speed

Avast has the same interface as the music player

The product is rated at two speeds: first, the virus scanning rate and the second are more important, the speed of giving updates when there is a new threat.Panda's software has been excellent in the virus scan race with an average time of 1 minute 43 seconds, 7 times faster than the slowest (Avast) product.

In terms of processing speed when the virus spreads, all the companies offer updates in about 12 hours, Kaspersky is the fastest, from 1-2 hours, BitDefender and F-Secure follow closely around 2-4 hours . AntiVir and PC-cillin are 4-6, Panda needs about 6-8 hours. All three products, AVG, Avast and McAfee, need 8-10 hours and after Symantec's end, it takes 10-12 hours.

Differences feature not much



F-Secure announces the latest security risks
Some products have additional good features.All have automatic updating capabilities, allowing you to configure your personal preferences or schedule scans.Some products are customizable, such as AVG only for scheduling scans on certain drives and file formats.Unlike other programs, Panda only allows scheduling in the full Panda Platinum 2006 Internet Security Suite.

Many programs have applied the same status screen as Windows XP SP2 Security Center, helping users know the current information of the computer. For example, Symantec's Norton Protection Center informs users about PC safety when surfing the web or using email. F-Secure and Panda provide security hotspots in the system tray. BitDefender displays a small File Zone window right on the desktop, indicating the number of files scanned a few minutes ago (users can disable this feature).

All products have technical support via email. BitDefender, F-Secure, Kaspersky, Panda and TrendMicro have 1 week of free phone support. Symantec charges US $ 30 for a one-time fix, McAfee charges US $ 3 per minute to answer the phone (telephone support is only valid in the US).

Easy to use

TrendMicro's PC-cillin is the easiest product to use, including lots of security information in a very convenient interface. The intuitive interface makes it easy for novices to control, but there are also settings for experienced users.

Alwil's Avast features a unique flashy main screen that can change the "skin" layer similar to music players.

The interface of other programs is quite simple. BitDefender turns on the notification screen only when auto-update and virus protection are enabled. The more important features are in the screens that are accessed on the left side of the window.

Grisoft AVG's main interface is disappointing, limited features and some essential functions are available only in the AVG Professional commercial version.

Although no one product can protect the PC absolutely from unknown threats, choosing one of the top 4 products will help you protect the best PC right now.

MICROSOFT ONECARE LIVE

Microsoft will soon join the list of companies that offer security software all in one.Let's take a look at the beta version of Windows OneCare Live, one of the many services offered online that can be downloaded at Windows Live Ideas (http://ideas.live.com/).
OneCare Live is a set of security tools and utilities that users can manage with just a single interface.The current antivirus component of this suite allows users to scan on demand, schedule scans, configure the file or folder to be scanned.Currently it has not yet scanned the received / sent emails and can only scan messages from MSN Messenger.Microsoft is planning to combine e-mail scanning capabilities and consider additional scanning capabilities of other pagers. A behavioral protection layer will track files with suspicious activity, for example. like changing the registry key.

Windows OneCare Live firewall has an easy-to-understand warning

The firewall in OneCare controls both the input and output network, which is an upgraded version of Windows Firewall.The first time you use OneCare will ask for software activities that are not recognized, such as updating iTunes software or Lotus Notes network activity.
Easy installation, although requires IE6. A web interface wizard checks to see if the system has minimum requirements and detects the risk of conflicts with other applications before continuing to install OneCare. Microsoft believes that OneCare will detect on the user's computer to ensure that it does not "clash" with running anti-virus programs, but in testing the product did not recognize the client version of the Symantec Norton Antivirus Corporate suite. Another experience shared on PC World's blog (find.pcworld.com/51360) is OneCare, which detects and suggests removing the version of Norton Antivirus.
Microsoft has not priced this product yet but the Purchase Now button (buy it now) shows that OneCare will not be free forever.

Hai Pham
PC World USA