

TECHNOLOGY

REVIEW

Protecting the homefront

Analyst Victor Garza tests four enterprise antivirus products

Are information technology managers paranoid? Or is someone really after them?

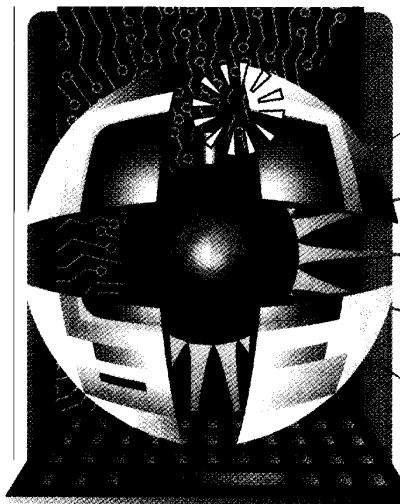
Every week, IT staff members wait for "The Next Big Virus." And for good reason. The recent rash of viruses, from SoBig.F to Blaster, is warning enough.

Microsoft Corp. officials have even resorted to an age-old tactic: the bounty. In early November, Microsoft officials announced that the company would pay successful bounty hunters up to \$250,000 for information leading to the arrest and conviction of those responsible for writing certain viruses. Their concern is understandable, because the majority of viruses target the Windows operating system.

Although it's not yet clear if Microsoft's bounty is going to have any significant impact, systems administrators at agencies and departments would be wise to forge ahead with implementing strong, multilayered antivirus strategies.

In this comparison, we look at the three biggest names in antivirus technology — Network Associates Technology Inc.'s McAfee Security Active Virus Defense Suite, Symantec Corp.'s Anti-Virus Corporate Edition and Trend Micro Inc.'s NeatSuite — along with a newcomer, Panda Software's EnterpriseSecure Antivirus. There are, of course, a number of other players we did not include.

Anyone implementing an antivirus security strategy must first recognize that server and desktop antivirus programs, such as those tested here, are not sufficient to ensure security. On the con-



**Every week,
information
technology staff
members wait for
'The Next Big Virus.'**

trary, they are the last line of defense.

In an enterprise setting, antivirus technologies should be employed at firewalls and gateways, preventing infected files and worms from getting into the network in the first place. And, to judge by what we hear from managers in the field, an even more frequently overlooked measure is a combination of policies and user education to guarantee that users do not unwittingly introduce malicious code via floppy disks and other media connected to the network.

When all else fails, it is up to the desktop antivirus solution to catch the little nasties.

All of the products we tested do a good job of

catching known viruses, with each snagging nearly all of the viruses we threw at them.

Several other concerns will be of far greater importance to most agency and departmental users when selecting the right antivirus solution. First, all the security precautions in the world are useless if they're not employed. Accordingly, we took a close look at how different solutions ensure that client systems are updated on a timely basis. It's also important that IT managers can prevent users from turning off the antivirus protection.

We put the four solutions through their paces at Federal Computer Week's test center and at analyst Victor Garza's lab. At FCW's test center, we installed the solutions on a Hewlett-Packard Co. Compaq ProLiant ML350 server with dual Intel Corp. Xeon 2.2 GHz processors and 256M of system memory running Windows Server 2003.

Among the highlights of his testing, Garza found that when it comes to client and server administration, Symantec and Network Associates add to solid Windows management technology while Panda and Trend Micro go their own ways. Trend Micro has a nice Web-based front end; Panda employs its own simple and effective interface.

Garza was surprised by the Symantec product's lackluster reporting and impressed with Trend Micro's and Network Associates' use of Crystal Decisions' Crystal Reports. Panda falls somewhere in between, lacking the ability to generate graphs or charts but still offering meaningful statistical reporting.

He found that all of the products, with the exception of Symantec's tool, offer multiplatform support, a big plus for many agencies and departments.

On the other hand, Symantec's product is the most affordable, so it's definitely worth considering if you don't need support for multiple platforms.

— Patrick Marshall

OntheWeb

For a list of other antivirus products, go to www.fcw.com.

ILLUSTRATION/AUGUST STEIN