3780

DOING THE SAFETY DANCE

Once a new exploit hits the streets, a single misstep can sink your network. We took six antivirus suites for a whirl. Trend Micro had the best moves BY JIM RYAN

Late summer brought a rude awakening for those network managers who felt secure in their virus-containment strategies. W32/Blaster, W32/Welchia and Sobig.F waltzed through the Internet in rapid succession, leaving billions of dollars in damage in their wake. These worms employed blended threats—combinations of attack mechanisms, such as social engineering and network communication strikes. The authors of these threats got around conventional antivirus (AV) defenses and left many security teams swamped by infections, patches and disinfections. At about the same time, the CCIA (Computer & Communications Industry Association) and Gartner declared that reliance on the Microsoft "monoculture" would make it far too easy for virus writers to cripple the Internet infrastructure, adding to enterprise unease (read the CCIA's report at *www.ccianet.org/press/03/0924.pdf*).

Given this sad state of affairs, we'll admit that we set out to test AV devices hoping to find a silver bullet. Alas, though many vendors have made progress, we didn't find anything that would prevent folks from getting hammered again next time a new attack comes down the pike. Why? Because the industry is still in a reactive rather than proactive mode. It would take a virus or worm with a particularly destructive payload putting thousands of companies out of business to motivate the industry to solve the root problem: anonymity (see "No Antivirus Silver Bullet in Your Lifetime," at *www.nwc.com/1424/1424rd5*).

Against this ominous backdrop, we set out to see which antivirus products could best fend off the new generation of network worm and virus attacks. Our two key questions: Have AV vendors been able to put together products and strategies that can defend against worms and blended threats as well as traditional viruses? And is there any way to defend networks during the window of vulnerability that exists for all

AV products because of their reliance on purely reactive signature-scanning technology?

Computer Associates, F-Secure, Network Associates, Sophos, Symantec and Trend Micro all responded to our invitation. Panda Software and Global Hauri both expressed an interest in participating, but were unable to get their products to us in time.

The first question is the easier of the two to answer—what's required is an integrated AV suite that covers all known infection vectors (paths into the network); a well-thought-out incident-response plan; 24x7 vendor support; thorough user training; and copious amounts of network staff time before, during and after an outbreak. This may sound like more work than we'd like, but it has proved an effective virus-containment strategy for many.

The second question, how to mitigate infection risk during the window of vulnerability, was more difficult to answer, but virtually all AV vendors are polishing "outbreak-management" systems that can minimize the damage if properly implemented. The basic AV signature-scanning technology employed by every product we tested is, at best, a double-edged sword. Although the technology works well to keep thousands of "in the wild" viruses from making an unwelcome comeback, it's purely reactive. There's always a significant delay from the time a virus is discovered until a defensive signature is installed at the user's desktop. This time lag creates a windows of vulnerability—an Achilles' heel in products that virus writers have learned how to exploit. For example, Sobig.F came with its own remarkably efficient SMTP server that let it propagate to millions of machines during the window of vulnerability.

What We Wanted

Some of the AV systems we tested came with lots of bells and whistles. But we didn't lose sight of the main reason you buy these products and used that premise to define our areas to test: installation, configuration and management consoles and features; e-mail system scanners; server file system scanners; client (desktop) scanners; perimeter scanners, where available; outbreak-management tools; and automated software and signature deployment, update, and policy management for all the aforementioned items.

We also scrutinized strategy versus product fit to see if the reality matches the marketing. For example, when it comes to outbreak management, the marketers are quick to say, "Sure! We do that!" But do vendors have the infrastructure in place to deploy useful policy recommendations within hours. Note also that the key to scalability is relational databases that keep track of the population. Computer Associates, Network Associates and Trend Micro all include relational databases as part of their product suites.

Although we found neither a silver bullet nor revolutionary technology, we did find considerable evolutionary improvements. You should expect to see some of these features showing up in new AV products:

» **Broader use of outbreak policies:** When a virus is first discovered, its basic attack mechanisms are understood long before signatures are available. Within hours of an outbreak, vendors can release policy-setting templates that deny a virus access to its propagation channel. For example, if a virus comes in a specific attachment form—say, .vbs encapsulated in a zip file—the Outbreak policy would recommend stripping all zipped .vbs files at the mail server or perimeter for the next several days, even if the company's normal policy doesn't require this. Expect robust outbreak management to be a standard offering from all AV vendors within a year.

» **Broader use of personal firewalls:** To control blended threats, some vendors may require personal firewalls, which can be managed en masse from a central AV policy-management console. However, such firewalls pose problems. For example, they must be locked down from user configuration; otherwise, every time an application wants to access the network, it will ask the user what to do, and the user invariably will say yes. We expect much debate over the widespread use of these firewalls in the months to come.

» **Hardware accelerators:** Just as hardware acceleration revolutionized firewall and intrusion-detection products a couple of years ago, it's now starting to show up in AV suites. For example, Trend Micro is shipping an

Executive Summary

ANTIVIRUS SUITES

After testing antivirus products from Computer Associates International, F-Secure Corp., Network Associates, Sophos, Symantec Corp. and Trend Micro, we've concluded that these suites have come a long way.

Indeed, the two key criteria we considered are antivirus strategic blueprints and outbreak management, and we were not disappointed. All the products have methods of combatting the rising tide of hostile exploits, with most relying heavily on desktop firewalls. And all six vendors are improving their outbreak-management policy distribution to the point where this technique should be standard fare in a matter of months.

However, the painful truth is that no matter which product you choose, technology can carry you only so far. Although Trend Micro's and Network Associates' products led the pack and would be a huge help to any organization, much of the burden for formulating a successful antivirus strategy—and communicating it to thousands of end users—still falls squarely on IT. Technical staff needs to get out in front of the user population in special AV education sessions to train internal customers in worm and virus avoidance. A little education goes long way.

HTTP AV proxy that employs an AV accelerator from Tarari to reduce latency dramatically—latency being a common problem in AV proxy servers.

» **Detection and containment of rogue machines:** McAfee is working with network vendors to test new machines coming onto the network for up-to-date AV software. Machines lacking such software will be denied a network connection. This forceful but necessary approach to closing the back door is likely to become common practice.

Some universities are already applying this technique. For example, Syracuse University requires users to run antivirus software. If McAfee AV is used, the university will keep it updated via McAfee's e-Policy Orchestrator. Users running other AV software must take responsibility and assume the risk of having their network ports shut off if their machines become infected.

» **Virtual-machine technology:** Norman Data Defense pioneered this for AV use. The theory is that you can let suspicious code execute in the VM to see if it exhibits dangerous behavior, then decide if it's something that should be allowed to run in the "real" machine.

What We Got

We scored each vendor's product suite with an eye to the following criteria:

» **Platform coverage.** Does the vendor cover all likely infection vectors for a broad range of OS platforms? This is a critical success factor. Although all the products we tested cover the requisite infection vectors, there were a few surprises in OS coverage. Most notable was a lack of Linux support, which hurt the scores of two very capable products, those from Network Associates and Symantec.

» **Management.** Another critical success factor was automated client installation, update and ongoing AV policy management. Sophos had the most intuitive management interface, while F-Secure and Trend Micro also had very usable management tools, if not as elegant.

Network Associates and Symantec scored quite well on raw management capability—if you have a huge network, you may need what they have. But both product suites were a bit of work to install and smacked of a bunch of point products glued together, with much of the "suite" integration happening at the marketing level.

» **Strategic plan:** Does the vendor have an effective blueprint to prevent outbreaks? Like it or not, AV defense is a sophisticated form of electronic warfare. No general would go into battle without a sound strategic plan. Fortunately, all the products we tested have solid strategic plans, though some, like Trend Micro, are better than others at mapping their products to support the plan directly. Equally important is your company's AV strategic plan—you do have one, right?

» **Outbreak management:** Does the vendor have an effective tactical plan to minimize damage during an outbreak? This may turn out to be the savior of fundamentally flawed signature-scanning technology. We weighted it heavily because we have seen 100,000 people idled for days as companies that use several of the products we tested were incapacitated during the window-of-vulnerability phase. Again, Trend Micro leads the pack with a very polished outbreak-management capability and, not surprisingly, earns our Editor's Choice award.

Rounding out our list were installation and documentation, as well as price. Although we weighted installation and documentation at only 10 percent of the overall score, it can rank high on the frustration scale when not done right. As for price, note that many of these products contain multiple components and convoluted pricing schemes (see our pricing chart online at *www.nwc.com/1424/1424rd3*).

Our analyses of the top three finishers follow. You'll find our takes on the other three products online at *www.nwc.com/showitem.jhtml?docid=1424f4*.

REAL-WORLD **REPORT CARD**

	Trend Micro NeaTSuite	Network Associates McAfee System Protection	Computer Associates eTrust Antivirus 7.0	F-Secure Anti-Virus Total Suite	Symantec AntiVirus Enterprise Edition	Sophos Anti-Virus; MailMonitor; SAV Interface; Enterprise Manager
OUTBREAK MANAGEMENT (25%)	4.4	4.7	3.8	3.8	3.8	1.6
COVERAGE (20%)	4.8	4.3	4.1	4	3.4	4.1
MANAGEMENT (20%)	3.6	4.8	4.1	4	3.3	3.8
STRATEGIC PLAN (20%)	5	4.3	4.8	4.5	4	4.5
INSTALLATION & DOCUMENTATION (10%)	4.8	4.2	4.8	4.8	4.2	5
PRICE (5%)	4.5	4	4.5	4	4	3
TOTAL SCORE (100%)	**4.49**	**4.48**	**4.26**	**4.13**	**3.71**	**3.53**
A≥4.3, B≥3.5, C≥2.5, D≥1.5, F<1.5 A-C GRADES INCLUDE + OR - IN THEIR RANGES. TOTAL SCORES AND WEIGHTED SCORES ARE BASED ON A SCALE OF 0-5.	A-	A-	B+	B+	B	B-

Customize the results of this report card using the Interactive Report Card™, a Java applet at www.nwc.com.

Trend Micro NeaTSuite **Trend Micro wins our Editor's Choice nod for hitting the target dead center** on both of our key questions. The starting point for its Enterprise Protection Strategy (EPA) is the premise that "antivirus focus is not sufficient." The company acknowledges the shortcomings of antivirus technology and has developed a set of products, services, prescribed operational tactics and management tools that minimize the cost and headaches of dealing with the inevitable virus outbreak. Trend Micro also provides the most robust outbreak-management capability of the products we tested. This well-conceived suite covers all the bases—perimeter, mail server, file server and desktop—while still being quite manageable via the intuitive, Web-based "Control Manager" console.

Although we had to install the individual products separately, accompanying Control Manager "agents" tied the point products together, providing us with handy centralized management. Installation on a half-dozen servers was wonderfully uneventful, as was the automated deployment of the desktop-scanning software to a half-dozen test PCs.

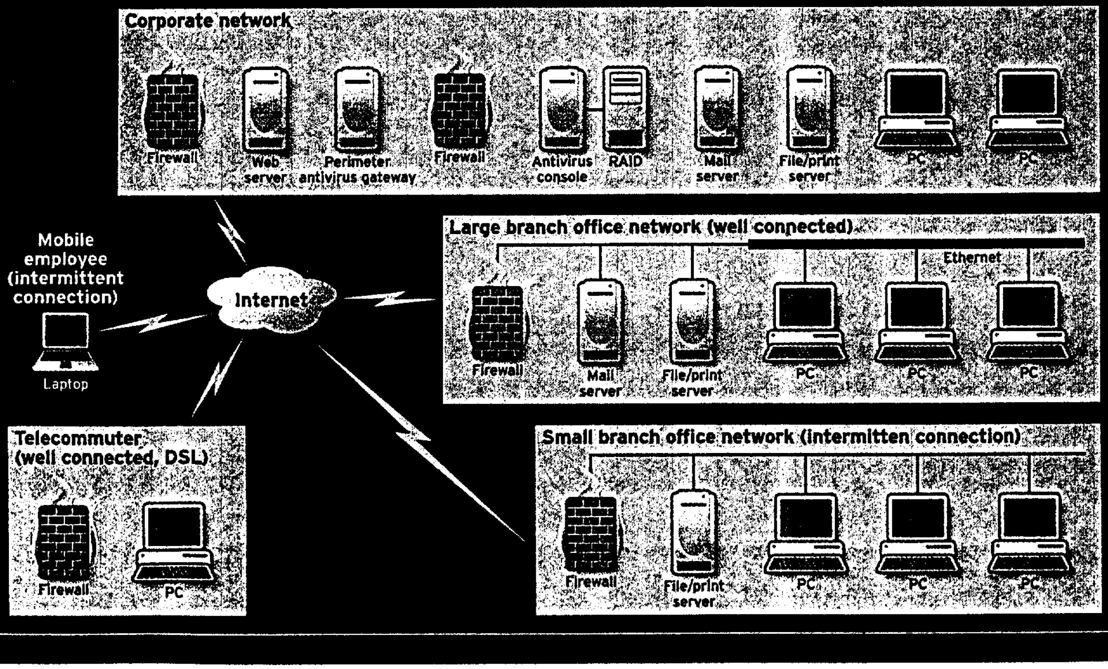
The capstone in the Trend Micro product suite is the outbreak-manager component of its Control Manager Console, designed to minimize damage during the window-of-vulnerability time frame inherent in signature-scanning technology. When a new virus surfaces, the outbreak manager automatically collects a set of policy-control templates from the Trend Micro support site. The policy templates are tailored to neutralize the virus du jour. We could set these templates to load to endpoint servers and workstations automatically or to queue up for our editing prior to distribution. Although most midsize to large organizations will pre-

HOW WE TESTED ANTIVIRUS SUITES

To test enterprise antivirus solutions, we first built the AV2004.net test bed (see diagram). The AV2004 is designed to be a microcosm of an enterprise-scale network that includes most of the tricky-to-manage elements that can complicate even a well-designed AV plan: mobile users and telecommuters; ornery users who refuse to run AV software because it "slows down their computers"; multiple points of entry, both physically and logically; wide-ranging geography; and multiple OS platforms. Then we asked the AV vendors to show us how to make this smorgasbord reasonably safe from viruses, yet manageable by mere mortals.

We tested several key points in the network:

» the perimeter, scanning inbound HTTP, FTP and SMTP traffic, as well as outbound SMTP traffic;
» mail-server scanners that ensure viruses entering through the back door—say, a laptop with out-of-date signatures—can't propagate rapidly in the internal mail system;
» file servers;
» desktop protection, sans personal firewalls;
» management consoles to assess both effectiveness and ease of use.



fer to edit and distribute the policy updates manually, it was nice to see someone take the lead in plugging this gaping hole in most AV product lines. And though, the other vendors also make policy templates available, we consider the Trend Micro implementation the most polished.

Trend Micro's rapid growth over the past several years is not an accident. The company is focused on antivirus, and its product road map covers all the bases with a nicely integrated toolset designed to support its strategic focus: managing virus outbreaks.

NeaTSuite. Trend Micro, (800) 228-5651, (408) 257-1500. *www.trendmicro.com*

Network Associates McAfee System Protection

Network Associates' years of experience shows through with a strategic architecture that not only covers all the requested bases, but also scales to very large configurations. McAfee Active Virus Defense Suite offers protection for all of the vectors we tested.

VirusScan Enterprise, the flagship product, provides AV protection for desktops and mobile users. Nicely integrated with ePolicy Orchestrator, it offers a "nag" feature we particularly liked: It lets you prompt laptop users to keep their AV protection up to date even if they don't fully update on any given connection attempt.

In keeping with the approach of other AV vendors, Network Associates is pushing the McAfee desktop firewall solution—again, integrated with ePolicy Orchestrator—to deal with blended threats.

We also tested the McAfee WebShield e500 perimeter appliance, which scans inbound and outbound SMTP, as well as inbound POP3 messages, HTTP and FTP traffic. The 1U box houses dual PIII, 1-GHz processors with 256 MB memory and dual 17.4-GB mirrored, hot-swappable SCSI hard disks. This hardware configuration was very close to that recommended by a couple of other vendors for hosting their perimeter gateway server software. The most notable feature with the WebShield e500 was ease of installation. We got the preloaded appliance up and running in a matter of minutes, and configuration via the Web interface was a snap. Controlling the e500 from the central ePolicy Orchestrator console was an intuitive process.

The McAfee line's only shortcoming was its challenging installation. The products tested were highly functional, but getting them to work together was a chore. The vendor seems to be missing a document describing the correct installation order for the full suite, and we had to restart the installation after hitting a dead end.

We were also surprised by McAfee's lack of Linux coverage. It and Symantec are the only vendors not supporting Linux at this time.

McAfee System Protection. Network Associates, (800) VIRUS-NO, (972) 963-8000. *www.mcafeesecurity.com*

Computer Associates International eTrust Antivirus 7

Computer Associates' eTrust product is the antivirus component of its larger, cross-platform "Threat Management" suite, which includes intrusion detection, secure content management (spam, URL and AV filtering) and a policy-compliance product that audits security policies. ETrust is an easy to manage, enterprise-class offering with one of the best coverage of any product we tested. If you have a platform that needs antivirus protection, CA has an answer: Windows 9X, Windows NT/2000/XP, Linux, Solaris, NetWare, MacOS, Palm OS and Pocket PC 2002 are all fully managed clients supported by eTrust Antivirus.

At the strategic level, CA understands the limitations of the technology; it has one of the most clearly espoused strategies and is working hard to communicate its belief that there are no halfway answers. Indeed, CA minced no words when telling us that in its view, the weak link in many corporate antivirus policies is the person sitting in front of the computer.

CA supports outbreak management with predefined policy plans that we could launch when required, policy-driven signature updates and a wide range of outbreak-alerting capabilities, including network broadcast, SNMP, SMTP, pager, trouble ticket and ties to CA's Unicenter network-management product.

ETrust employs two scanning engines to reduce the likelihood that a bug might slip through the net. The only other vendor with multiple engine support was F-Secure, with three engines. And eTrust is the only product we tested to offer free lifetime signature updates, regardless of maintenance contract status—unusual in an industry that regards signature-update subscriptions as a major revenue stream.

eTrust Antivirus 7.0. Computer Associates International, (800) 225-5224. *www.ca.com*

JIM RYAN is an infrastructure architect with Princeton Systems Consulting in Redmond, Wash. He has spent more than 10 years managing projects in the minicomputer industry, and for the past 15 years has been designing global networks and managing a wide range of infrastructure projects. Write to him at *jimryan@princeton-systems.com*. Post a comment or question on this story at *www.nwc.com/go/ask.html*.

WebLinks

Find this story in its entirety online at
www.nwc.com/showitem.jhtml?docid=1424f4

Our detailed features chart can be found at
www.nwc.com/1424/1424rd2.html

Our pricing chart can be found at
www.nwc.com/1424/1424rd3.html

Do you need a firewall on every desktop? See
www.nwc.com/1424/1424rd4.html

Virus writers have an advantage. Read what it is at
www.nwc.com/1424/1424rd5.html