

Network Computing

For IT By IT

11.25.2003 | WWW.NWC.COM

DOING THE SAFETY DANCE

BY JIM RYAN

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

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.cciainet.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.

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.

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.

Trend Micro NeaTSuite Trend Micro wins our Editor's Choice nod for hitting the target dead center on both of our

A- key questions. The starting point for its Enterprise Protection Strategy (EPS) 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 prefer 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



REAL-WORLD LABS REPORT CARD

Antivirus Suites

	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.