

INTERSCAN MESSAGING SECURITY APPLIANCE

ERADICATES SPAM

TREND MICRO'S INTERSCAN MESSAGING SECURITY APPLIANCE EARNS A NETWORK TESTING LABS WORLD CLASS AWARD. THE INTERSCAN MESSAGING SECURITY APPLIANCE GATEWAY IS A KEY PART OF TREND MICRO'S INTEGRATED AND LAYERED INTERNET MESSAGING SECURITY.

By Barry Nance

Network Security



Trend Micro's InterScan Messaging Security Appliance is pinpoint accurate, blazingly fast, easy to administer, scalable and robust. Cyber criminals – the bad guys – hate it, and with good reason.

Our tests show Trend Micro's InterScan Messaging Security Appliance provides unparalleled, effective email security at the gateway. The InterScan Messaging Security Appliance easily thwarted virtually all email threats in our tests, including spam, spyware, phishing, and viruses. InterScan Messaging Security Appliance earned Trend Micro top honors in our email security review.

The device also exhibits an intuitive user interface, well-designed reports, an easy plug and play installation process and an attractive price tag. Trend Micro wins a well-deserved Network Testing Labs World Class Award for the best integrated, layered Internet security gateway.

Email has become a predominant means of business communication. However, as email use has become more prevalent, so has its abuse. Businesses have to combat numerous email threats, including spam, spyware, phishing, and viruses, to be able to access critical business correspondence. These threats have also become more difficult to defend against, evolving into more sophisticated and blended attacks. Cyber criminals are combining threat types and using multiple protocols, such as email with embedded links to web-based threats, in one attack. Businesses need a solution that can defeat each of the email threats individually as well as the more advanced blended attacks.

Spam is flooding both the Internet and, unfortunately, your corporate network. Left unblocked, the torrent of spam uses up valuable resources and make it difficult to use email as an effective business tool. To add insult to injury, spam is also used to deliver other email threats such as phishing and malware.

Spam often includes links to dangerous web sites. Cyber criminals first create – or purchase – software that, for example, rifles the files on a PC for credit card numbers and other confidential data. The cyber criminals put the malware on a Web site, register the Web site and flood the Internet with spam containing a clickable link to the Web site. When an unsuspecting user clicks the link, even if only in the mail reader’s preview pane, the malware flows into the user’s PC and starts running.

Some malware authors have adopted a new approach to get their software onto your computers. These bad guys hijack one or more Web pages of an otherwise “clean,” innocuous Web site, and then send out a ton of spam referencing the site. Unaware that someone’s hacked it, a user visits the site. The user wants to get news, weather or sports information. Instead, the site downloads spyware or other malicious code onto your machine. To avoid these infected Web pages, it is important to block emails with links to dangerous sites before they even reach user Inboxes.

E-mail-borne spam, spyware, phishing attempts, viruses, Trojans, rootkits and links to malicious Web sites (collectively, “email threats) are no longer a problem you can ignore. Either you protect yourself now, or you’ll find that criminals have stolen your company and personal information quickly and silently from your computers – that is, if they haven’t already. Moreover, the malware authors have become extremely sophisticated. Because they build rootkit technology into their malicious code, removing the latest malware threats “by hand” is virtually impossible.

Network Testing Labs has created a special test environment (see the Testbed and Methodology section of this review) for evaluating email security products, and we’re on a quest for the best. The most important criterion in our evaluation is the ability to identify and thwart virtually all email threats. We also looked for quick performance, useful reports, ease of use and ease of deployment.

Trend Micro is a market leader in network security. To evaluate the vendor’s offerings in our lab environment, we invited Trend Micro to submit its InterScan Messaging Security Appliance (IMSA) to our Alabama lab. We note that Trend Micro’s expansive messaging security repertoire also includes a hosted security service, messaging security software for multiple platforms at both the gateway and the mail server, protection for SharePoint environments, and an Instant Messaging (IM) security tool.

Trend Micro's InterScan Messaging Security Appliance proved to be accurate, fast and easy to use. It turned aside virtually all email threats, and the appliance's impact on latency was virtually nil. Trend Micro wins the Network Testing Labs World Class Award for the best integrated Internet messaging security gateway.

InterScan Messaging Security Appliance

The InterScan Messaging Security Appliance (IMSA) foiled virtually all the email threats we subjected it to. The appliance also gave us great flexibility in how we could configure it to thwart email threats. InterScan Messaging Security Appliance performed so well that our users noticed no effect on the responsiveness of their email experience. It gave us rock-solid, reliable operation, and the appliance was intuitively easy to use. Impressively, the reputation services in InterScan Messaging Security Appliance blocked threats at the connection layer and kept spam and malware from even traversing our network, thus conserving bandwidth, storage and other computing resources. Best of all, we found the appliance saved our administrators from having to spend many long hours dealing with email threats.

Table 1 reveals, by type of email threat, the InterScan Messaging Security Appliance's impressive threat detection success rates. The gateway appliance kept at bay 98% of spyware, 99% of viruses and, most impressively, 99% of both spam and phishing attempts.

<i>Type of Email Threat</i>	<i>InterScan Messaging Security Appliance</i>
<i>Spyware</i>	98%
<i>Viruses</i>	99%
<i>Spam and phishing</i>	99%

Table 1. InterScan Messaging Security Appliance's ability to stop email threats.

We found the InterScan Messaging Security Appliance to be one of the quickest performing email security products on the market. It did its work quickly enough that client responsiveness (i.e., the impact on email latency) was virtually unaffected by the presence of the appliance (see Table 2). Even the most accurate email security tool is useless if it significantly slows down email and delays critical business communications.

<i>Latency</i>	<i>InterScan Messaging Security Appliance</i>
<i>Other than executable files</i>	12 ms
<i>Executables</i>	32 to 78 ms

Table 2. InterScan Messaging Security Appliance latency and throughput results.

The InterScan Messaging Security Appliance offers a Web-based user interface for setting configuration options, seeing real-time status and viewing reports. The appliance's interface is incredibly intuitive to use, and it's also easy to navigate. The InterScan Messaging Security Appliance's status screens and reports are comprehensive and highly informative.

Installation of the InterScan Messaging Security Appliance consists simply of cabling the box to the network, powering up and assigning an IP address. Trend Micro's documentation is clear, comprehensive and easy to follow.

The InterScan Messaging Security Appliance's designers obviously paid a great deal of attention to detail in their development of the appliance. Every aspect in operating the appliance revealed thoughtful, user-oriented features as well as innate quality and reliability. The appliance features hot-swappable, redundant hardware (including multi-channel RAID disk storage) as well as a fail-open mode to maximize uptime and reliability.

The unit itself is a powerful, well-built computer. It's a rack-mountable, 2U device that incorporates dual Xeon CPUs, 2 Gb of RAM, two 250 Gb SATA disk drives and 10/100/1000 Ethernet connectivity.

Control Manager – the Perfect InterScan Messaging Security Appliance Complement

For enterprises that need a central console for controlling multiple deployments of appliance as well as other Trend Micro security products, Control Manager is the key. Among its top features, Control Manager provides consolidated threat reporting and policy management across a large, distributed network. It also provides centralized key management, a significant value for customers running multiple Trend Micro products. Lastly, it allowed users to easily vary security policies by network segment, company division and company department, if we wished.

We particularly appreciated Control Manager's unified view of network security for the entire enterprise.

Control Manager is a snap to install, and it runs on Windows 2000 and 2003 (standard or enterprise). It can use the Microsoft Data Engine or SQL Server as a data repository.

Conclusion

The InterScan Messaging Security Appliance is a superior gateway-architecture security tool for keeping spam and malware off the network in the first place. It's accurate, fast, easy to administer, reliable and highly scalable. And Control Manager links and integrates Trend Micro's security tools across an entire enterprise.

We strongly recommend you look closely at Trend Micro's integrated line of layered security tools.

What's Bad About Spam

Spam now comprises approximately 94% of all email. This inundation of spam emails can bog down networks and deplete valuable resources—both in network infrastructure and IT and end-user time. Spam can also harbor other email threats. It is often used to send out malware or phishing. In addition, spam emails frequently include links to malicious websites, including phishing sites and sites with dangerous downloads, such as spyware, Trojans and viruses.

What's Bad About Malware

Malware is, collectively, damaging or annoying software and data files that you didn't knowingly install on your computers. Typically, malware deletes files, changes files, reveals file contents, throws pop-up advertisements onto your screen, slows down a computer, allows a remote attacker to control your computer, attempts to convince you to supply credit card and password data, tracks your keystrokes, threatens to blackmail you, sends e-mail to everyone in your address book and otherwise ruins your day (or perhaps your life). Malware typically also propagates itself and can install additional malware instances on your computers.

Malware can leverage both servers and clients in clever ways. Because virtually all users' logons are Administrator-privilege accounts, all the software that users run, even inadvertently, can fully control any aspect of the PC that the software (or malware) developer wishes.

With free rein over a PC's files and programs, including operating system files, a malware instance can configure a computer to run the malware perpetually and thwart attempts to remove the malware (i.e., a *rootkit*). The malware thus becomes part of the operating system itself.

The following table identifies five common types of spyware.

Category	Typical Action
Keystroke Logger (AKA Trackware)	Captures keystrokes (including personal information and passwords) or tracks the Web sites you visit.
Trojan	Enables remote control of your computer by a hacker, often for Distributed Denial of Service attacks.
Droneware	Sends spam or turns your PC into a host for offensive Web images.
Dialer	Auto-dials area code 900 or expensive long distance calls via your modem.
Adware	Pops up unsolicited and annoying advertisement-laden browser windows or hijacks your Internet search (Yahoo, Google, etc.) results.

Testbed and Methodology

We primarily looked for the ability to identify and block email threats (such as viruses, spam, phishing attempts, keystroke loggers, browser hijackers, bots, adware, rootkits, dialers, data miners and Trojans). We wanted InterScan Messaging Security Appliance to block spam, prevent malware from sending data from our network (i.e., “phoning home”), scan email traffic quickly, receive frequent malware definition updates, and produce helpful reports on infection attempts and traffic statistics.

We collected a suite of 18,000 messages comprised of spam, phishing attempts and normal e-mail (legitimate correspondence). We also used 200 malware samples from our lab’s library of spyware, adware, viruses, Trojans and the like.

The test network consisted of two subnets.

- Subnet 1 had 25 client machines with a variety of operating systems, including Windows 98, 2000, 2003, ME, XP and Vista as well as Red Hat Linux and Macintosh OS X.
- Subnet 2 contained three Web servers (Microsoft IIS, Netscape Enterprise Server and Apache), three e-mail servers (Exchange, Notes and Sendmail), two file servers (Windows 2003 Advanced Server and Netware) and two database servers (Oracle 8i and Microsoft SQL Server).

To measure performance, we used two time-synchronized protocol analyzers on the Internet and local network sides of the Internet connection and examined the resulting packet captures to determine the latency of the InterScan Messaging Security Appliance.

The InterScan Messaging Security Appliance connected the Internet to the other two subnets. Client and server machines started off in a pristine state for each test.

Our clients and servers attempted to download e-mail from the Internet. We noted how well the appliance identified spam, spyware, phishing attempts, viruses, Trojans, rootkits and links to malicious Web sites. For example, we gauged success or failure by examining each machine for malware after each test. We looked for running malware processes, new program files (EXE, DLL or OCX, possibly marked with the “Hidden” attribute) and directories as well as Registry and Start Menu changes.

Security Report Card

Grade scale is A through F, with F = Failing and A = Perfect

Category and weight (%)	Trend Micro InterScan Messaging Security Appliance
Identifying and thwarting malware (40%)	A
Performance (20%)	A
Ease of Use (10%)	A
Reports (10%)	A –
Deployment (10%)	A
Documentation (10%)	A
Overall score	A

Vendor Details

Products Reviewed:
InterScan Messaging Security Appliance (IMSA)
Trend Micro Control Manager

Price: Contact vendor for pricing information

Trend Micro, Inc.
10101 N. De Anza Blvd
Cupertino, CA 95014
(800) 228-5651
www.TrendMicro.com

About the Author

Barry Nance is a networking expert, magazine columnist, book author and application architect. He has more than 29 years experience with IT technologies, methodologies and products. Over the past dozen years, working on behalf of Network Testing Labs, he has evaluated thousands of hardware and software products for ComputerWorld, BYTE Magazine, Government Computer News, PC Magazine, Network Computing, Network World and many other publications. He's authored thousands of magazine articles as well as popular books such as *Introduction to Networking (4th Edition)*, *Network Programming in C* and *Client/Server LAN Programming*.

He's also designed successful e-commerce Web-based applications, created database and network benchmark tools, written a variety of network diagnostic software utilities and developed a number of special-purpose networking protocols.

You can e-mail him at barryn@erols.com.

About Network Testing Labs

Network Testing Labs performs independent technology research and product evaluations. Its network laboratory connects myriads of types of computers and virtually every kind of network device in an ever-changing variety of ways. Its authors are networking experts who write clearly and plainly about complex technologies and products.

Network Testing Labs' experts have written hardware and software product reviews, state-of-the-art analyses, feature articles, in-depth technology workshops, cover stories, buyer's guides and in-depth technology outlooks. Our experts have spoken on a number of topics at Comdex, PC Expo and other venues. In addition, they've created industry standard network benchmark software, database benchmark software and network diagnostic utilities.