

EVALUATION GUIDE



Trend Micro InterScan[®] eManager[™]

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014
Phone: 1-800-228-5651 / 1-408-257-1500
Fax: 1-408-257-2003
Web: www.trendmicro.com or www.antivirus.com



Table of Contents

THE THREAT OF PASSIVE CONTENT	3
INTERSCAN EMANAGER	5
<i>Spam filtering</i>	6
<i>Content filtering</i>	6
<i>Attachment filtering</i>	7
EMAIL MANAGEMENT	7
<i>Email Delivery Management</i>	7
<i>Performance Monitor</i>	8
<i>Scalability</i>	8
SYSTEM REQUIREMENTS	8
INSTALLATION.....	9
NOTE ABOUT VIRUS DETECTION TESTING	12
APPENDIX A: VIRUS TEST FILES.....	15
APPENDIX B: ABOUT TREND MICRO.....	16

Copyright © 2000-2001 by Trend Micro Inc. All rights reserved.

All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of the publisher. InterScan, eManager, Trend Virus Control System, ScanMail, ServerProtect, and OfficeScan are trademarks or registered trademarks of Trend Micro, Inc. All other company and product names are trademarks or registered trademarks of their respective owners.

The Threat of Passive Content

Given the current capabilities of the Internet, content security is no longer just a matter of viruses. Trojans, worms, malicious applets, and hacker agents are only half the problem. Passive content, such as unsolicited bulk email (spam), high email volume, and oversized files, can degrade system performance as much as any virus. Trend Micro eManager™ addresses the passive content security problem. An optional plug-in module for Trend Micro's highly successful InterScan® VirusWall®, eManager helps handle passive content threat.

On the face of it, spam doesn't appear to be a threat to a business, but deeper investigation explains why people are so upset. Spam can range from unsolicited advertisements for pornography to chain letters and promotions for pyramid schemes. Electronic junk mail has become so prevalent that many consumer groups are supporting legislation to outlaw spam, much as "junk faxes" were outlawed years ago. Not only does spam affect employee productivity, it can also bog down networks, even causing the system to crash under the burden of too much traffic.

Some Internet service providers are taking legal action against known spammers by employing lists of known offenders developed by consumer groups and others, such as the "Realtime Blackhole List" from the Mail Abuse Prevention System (<http://maps.vix.com/rbl/>). However, most of these lists are based on the IP source of the spam. Today, when many networks employ Dynamic Host Configuration Protocol, the result may be blocking many innocent users from sending email.

- Spam is the only form of advertising where the audience pays most of the bill.
- It is annoying to have your email box filled up with emails with no subject, or ambiguous subjects such as, "Check this out".
- Outbound spam, when sent through the corporate SMTP server by either an employee (advertising his/her own business, for example) or relayed by an unauthorized third-party user, puts your organization's interests at risk. Spam traced to your organization can hurt your reputation or even pose legal liabilities.
- Spam is an ideal mechanism for cyberterrorism. Modern email clients, such as Outlook 98 and Eudora and Netscape Communicator 4.5 can automatically run scripts written in Visual Basic or JavaScript embedded in an email. These scripts can be a harmless animation or sophisticated code designed to crash computers, steal data or steal passwords. One individual with a grudge could cause havoc by sending a malicious email.

Spam can be a very profitable proposition for marketers. For little cost, spammers can reach very targeted mailing lists. Many have their own spamming facilities, others use

outside services. The following is a price list for one bulk emailing service that was sent out, not surprisingly, via bulk email:

<u>Emails</u>		<u>Cost</u>
100,000	--	\$200
200,000	--	\$345
400,000	--	\$875
600,000	---	\$1,100
800,000	---	\$1,300
1,000,000	-	\$1,400
2,000,000	-	\$2,200

What isn't listed is the cost to the recipients; both in delivery fees paid to their ISPs for receiving mail and the cost of the time and bandwidth used.

Bandwidth Abuse

Internet connectivity comes with a price and many corporate IT managers have discovered this cost is often a slowing of network performance. This problem is akin to travelers carrying increasing amounts of luggage. Just as an airport baggage screening system can become overloaded with too many suitcases, so too can a network be bogged down with too many and too large emails.

Too many large attachments can bring the most robust email system to its knees, yet often there are good business reasons to send large files. Most corporations set a hard limit of between 2 and 5 megabytes per email. Exceptions can be made, but only on a case by case basis which can waste considerable time each day for the email administrators.

The Corporate Safe

Once the corporate safe was a large metal box hidden behind a picture in the CEO's office. Today a corporation's most precious assets are contained in its information. Since email is the main conduit of information throughout the company, it should come as no surprise that it is also the main pipe for information leaving the organization. There is probably no way to measure the value of unauthorized information leaked by email, but that the cost can be high.

Pre-release of information can blow product launches, result in lost market share, even lead to an investigation by the Security and Exchange Commission for insider trading. More and more legal authorities are expecting firms to make reasonable precautions to ensure email is not used inappropriately.

Content Filtering

Trend Micro's content filter provides a means for the administrator to evaluate and control the delivery of email on the basis of the message text itself, or policies can be created to check for use of the email system to distribute:

- Sensitive corporate information
- Sexually harassing language
- Racist language
- Offensive language (e.g. "four-letter" words)
- Resumes or other evidence of job seeking on company time
- Spamming or other unsanctioned commercial activities

InterScan eManager

eManager is a valuable addition to the network administrator's tool bag. When used in conjunction with other security tools and with well-designed email use policies, *eManager* will help reduce the threat posed by passive content.

Content filtering can block, copy or quarantine emails using keywords. This feature can be essential when the price of premature disclosure may be extraordinarily high. However, in most organizations, this feature would only be needed during exceptional circumstances like when a pattern of resource misuse has been previously established.

Unsolicited bulk email, known commonly as spam, has become a problem for everyone. Spam doesn't threaten your business, but it does waste time and bandwidth. Some users report that as much as 30% of their email is junk mail. Wasting five or ten minutes a day deleting junk mail may not sound like a big problem, yet multiplied by a thousand or ten thousand employees, the cost in terms of productivity and emotional distress becomes more clear.

The down time of the mail server becomes critical in the enterprise. During a virus outbreak such as the Melissa virus, many companies were forced to shut down their mail servers until a virus vaccine was available. The attachment filtering feature of *eManager* can be a proactive solution to block suspicious attachment files, thus reducing down time.

The *eManager* plug-in offers a powerful initial response against a virus outbreak. Before a virus pattern file is available, administrators can customize the filter to block potentially infected attachments. File blocking and stripping provides the tools you need to respond to virus threats quickly and eliminates the need to completely shut down your email system, allowing normal business activity to continue.

eManager helps manage the threat of passive content by blocking spam, scanning inbound and outbound email for keywords, blocking or stripping off attachment files by

attachment file name or MIME content-type, and helping to manage the delivery of large emails. *eManager* allows you to set up diverse rules for individual users and automatically updates its list of known sources of spam.

eManager runs on Windows NT, Solaris, HP-UX and RedHat Linux, and utilizes the COM/DCOM architecture for unparalleled scalability on the Windows NT platform. Each of *eManager*'s functions are objects that can be placed on one or more computers. *eManager* will automatically balance the load between multiple machines.

Spam filtering

eManager blocks the delivery of spam using a filter method. First, Trend Micro provides a list of known sources of spam based on email addresses. Second, Trend Micro supplies a list of phrases commonly found in email solicitations. These lists are automatically updated and can be easily customized to fit the needs of the user.

Unfortunately, spammers have gotten quite good at evading filtering strategies. It is a simple matter for a spammer to hide his or her email address and many spammers now avoid obvious phrases relied on by filtering products. To counter this, Trend Micro also filters spam based on the "landing structure" i.e. the Web site or 800 number the spammer includes in the email message. It is harder to change an 800 number than it is to change a solicitation. Trend Micro feels this is the most effective approach to counter spam strategies.

To ensure that Trend Micro's spam block lists are up-to-date and on target, Trend Micro employs a team of spam analysts who use a network of email boxes designed to collect the latest spam. Hundreds of spam messages are received each week in four languages: English, Japanese, Chinese and Spanish. Trend Micro also works with anti-spam activists to stay on top of current issues.

Development of anti-spam techniques is an ongoing process; the challenge is blocking spam without blocking legitimate email. Depending on the creativity of spammers, *eManager* may not be able to block 100% of spam, but typically can block 70-80% of spam.

Content filtering

eManager gives email administrators a useful tool for preventing abuse of the email system. It can block, quarantine or just archive emails with or without keywords or phrases. Different rules can be set for different users.

Some companies seek to prevent employees from sending confidential information by email. In some industries, financial securities for example, companies have a regulatory or fiduciary responsibility to archive emails. Firms may choose to use *eManager* for monitoring guest accounts or special accounts set up for temporary employees or

consultants. In many cases, content filtering is only used when an investigation is underway or where email misuse is already suspected.

The ability to send and receive emails via the Internet has become a regular business function, but reliance on email had opened doors to abuse. Email management cannot and should not be done by software alone. Each organization needs to create a set of expectations and policies that support those expectations. Such policies should be consistent with the corporate culture, put in writing and reviewed by both human resource departments and by legal staffs.

Attachment filtering

eManager's Attachment Filter provides the feature that removes attachments with a particular filename/MIME content-type from email messages and replaces them with a configurable notification text message. During a virus outbreak alert, suspicious attachment file types can be removed from the message before the virus vaccine is available, thereby averting the potential threat.

eManager can remove all the attachments in messages with the exact file name or specific extension name. This method prevents employees from receiving inappropriate material, such as pornography, by blocking all the attachments with file extension name *.jpg and *.gif. Additionally, this may be used to limit the number of employees that receive an executable program by email, thus reducing the opportunity of a computer being infected by unknown virus.

Email Management

Email Delivery Management

Of key concern to enterprise-wide productivity is the performance of the email system. Large quantities of email, both legitimate email with large attachments and spam mail, can cause delays and bog down the network for users throughout the enterprise.

Employees increasingly use email to share large data files such as spreadsheets, graphics, reports, database updates, and sales presentations. As these attachments flow in and out of the network, bottlenecks can arise during peak work hours. Size limits do effectively limit email congestion, but at the cost of prohibiting a useful business function.

The Email Management features of eManager provide load balancing for your Simple Mail Transfer Protocol (SMTP) servers by regulating the flow of traffic received by the SMTP server(s). eManager will delay the delivery of set types of email, such as email with large attachments to help optimize bandwidth use. This allows administrators to

shift delivery of large emails to off-peak hours, or shift delivery of international mail to coincide with business hours in other parts of the world, leveling the flow of messages and easing network bottlenecks. The product allows different rules to be set for different users so email policies can be tailored to meet the needs of different business groups.

To identify these "peaks and valleys," of SMTP server usage, Email Management includes a SMTP statistics gathering utility that allows you to generate reports viewable from either the Windows UI or a Web browser.

Performance Monitor

The performance monitoring options found in InterScan VirusWall gathers system statistics and helps fine tune program functions. Using a common interface, the performance monitor provides graphs, reports, and histogram representations of program data.

Scalability

eManager's scalability is a function of its advanced architecture. The NT version of eManager is built around Microsoft's COM/DCOM architecture allowing Trend Micro to distribute functions across multiple CPUs in the same NT domain. Task distribution is coordinated and controlled through InterScan VirusWall, versions 3.0 and later. eManager can be easily installed on additional servers on the network, critical for companies where email traffic is increasing each year.

System Requirements

To run InterScan eManager version 3.5, you need the following:

- A Pentium 266 or faster processor
- 64MB RAM (128 MB recommended)
- 100-500MB of free disk space for swap and temporary files
- InterScan® VirusWall 3.0 or above installed
- Windows NT 4.0 server with Service Pack 3 installed
- A monitor with 800x600 or higher resolution
- Internet Explorer version 3.02 or later, or Netscape Communicator 4.04 or later

Installation

InterScan eManager is a plug-in to InterScan VirusWall, which must be installed on the same machine as InterScan VirusWall. If you intend to employ load-balancing strategies by installing additional copies of eManager onto remote machines, install eManager on the InterScan VirusWall machine first, before installing the remote copies.

Installing InterScan eManager constitutes your acceptance of the terms and conditions of the license agreement that accompanies each evaluation copy of Trend Micro's software.

Please review the license agreement carefully before installing the software. In addition, please note that as a product reviewer, you may only install and use an evaluation copy of InterScan eManager for the purpose of preparing and publishing a product review. You may not use InterScan eManager in a production environment. Any use of an evaluation copy of the software in a production environment violates the terms and conditions of the license agreement.

Installing from the Trend Micro Enterprise Solution CD

Both InterScan VirusWall and eManager are available on the Trend Micro Enterprise Solution CD.

If you are installing from the **Trend Micro Enterprise Solution CD**, invoke GO.EXE by inserting the CD into the CD-ROM drive or by running the program from the **Start** menu. Select the language you want to use and then on the next screen click **Install**. Select **InterScan eManager** from the list at the right and then click **Install**. Alternatively, locate the directory containing the eManager files and double-click setup.exe

After accepting the License Agreement (required to proceed), specify where you want to install eManager. The default directory is \InterScan eManager.

Choose to install **InterScan eManager Email Management**, **InterScan eManager Content Management**, or both by checking the appropriate box and clicking **Next**.

If you are installing the free 30-day trial version, click **Next** without providing a serial number. The trial version is fully functional but will stop running after 30 days.

If you decide to purchase eManager, contact a Trend Micro sales representative about obtaining a serial number at the following email address: sales@trendmicro.com. The 30-day time-limit will be removed when you register InterScan eManager with Trend Micro. There is no need to reinstall or reconfigure the program.

1. Specify whether InterScan eManager is being installed on the InterScan VirusWall machine or a different one, and click **Next** to continue.

2. Choose **Local InterScan Server** to install the InterScan eManager on the same machine as InterScan VirusWall.
3. Choose **Remote InterScan Plug-In System** if InterScan eManager is already installed on the InterScan VirusWall machine and you are now installing a remote instance (you should be seated at that machine—the installation cannot be "pushed").
4. Choose the program folder where you want the InterScan eManager program icons located. The default is \InterScan VirusWall\InterScan eManager.
5. Enter the user name and password of an Administrative-level NT account on the machine where InterScan eManager is being installed.
6. Finally, choose one of the following four options:
 - **Run Email Management configuration program** to begin editing the Email Management configuration. This is necessary before the program will work. You will need to manually start Email VirusWall and the InterScan eManager services.
 - **Run Content Management configuration program** to begin editing the Content Management configuration. This is necessary before the program will work. You will need to manually start InterScan VirusWall and the InterScan eManager services.
 - **Start InterScan VirusWall and InterScan eManager** to start the services.
 - **Exit Setup** to quit Setup without starting InterScan VirusWall or configuring the programs. You will need to manually start InterScan VirusWall and the InterScan eManager services.

Starting eManager

1. The InterScan eManager services will only process messages while InterScan VirusWall is running. To start or restart the services, open Control Panel and click **Services**.
2. From the list of services that appears, select **InterScan VirusWall**, then click **Start**. Both **Content Management** and **Email Management** services will start along with InterScan VirusWall.
3. View the Activity Monitor.

Registering eManager

You can register InterScan eManager via Internet from the InterScan eManager program group. Step by step instructions follow:

1. Click the Windows NT **Start** button | **Programs** | **InterScan VirusWall** | **InterScan eManager**.

2. Click **InterScan eManager Registration Program** to bring up the serial number dialog box.
3. Type in your InterScan eManager serial number and click **OK**.

Serial numbers can be found on the front cover of the InterScan eManager Getting Started Guide and on the product registration card. Trial version users who want to remove the time limit can contact Trend Micro via email at **support@trendmicro.com** or **sales@trendmicro.com**

Remote Installation

Multiple instances of InterScan eManager Content Management can be installed on the network, provided that they are in the same NT domain as the InterScan VirusWall. Install Content Management onto multiple remote machines if:

- You expect to process a large number of email messages
 - You expect to employ a large number of anti-spam rules and content filter policies
 - The system resources on the InterScan VirusWall machine are nearly maximized
- All remote instances of Content Management must be installed on the same NT domain as InterScan VirusWall.

1. Install InterScan VirusWall. If you are going to filter outbound messages, be sure that **Enable outbound message processing** is checked in InterScan VirusWall.
2. Install InterScan eManager onto the InterScan VirusWall machine.
3. Relocate to each remote machine where you want to install the Content Management plug-in and run Setup again.
4. From any one of the InterScan eManager machines, define all of your spam and content filtering configurations.
5. Distribute the configuration files from this machine to the appropriate directory of each machine hosting an instance of Content Management.
6. In the InterScan Email Manager configuration page, add the remote Content Management servers to the InterScan Plug-in Manager tree.
7. Verify your setup by sending several test emails designed to trigger a spam mail or content filter match. You can observe the results in real-time by watching the Activity Monitor on the InterScan VirusWall server.

Outbound Filtering

The **Enable Outbound Mail Processing** option in InterScan VirusWall must be enabled for outbound content and spam filtering to occur.

Note: Outbound mail processing is a separate operation from outbound mail scanning. Be sure to also check **Enable outbound mail virus scanning** on the **Outbound SMTP Mail Processing** page to turn outbound virus scanning on.

To enable outbound mail processing using the Windows GUI:

1. Start the InterScan configuration program (Windows NT **Start button** | **Programs** | **InterScan VirusWall** | **InterScan VirusWall Windows Configuration**)
2. Make the **SMTP Configuration** tab active.
3. Click the Outbound Mail **Options** button.
4. Click **Enable outbound mail processing**.
5. Specify the outbound mail delivery servers and delivery method. (Required)
6. Click **Save**, then **Save** again on the **SMTP Configuration** tab.

Enabling Inbound Mail Processing

1. Click the Windows NT **Start** button, then choose **InterScan VirusWall** | **InterScan VirusWall Windows (or Web) Configuration** from the menu.
2. Click the **Enable Virus Scanning** check box.
3. Click **Save** to apply your changes.

Note About Virus Detection Testing

The antivirus marketplace is marred by a vast amount of hype and unsubstantiated claims, primarily in regard to virus detection rates. The following provides a guide for evaluating antivirus products:

1. The current hype persists due to the difficulty in testing detection rates. Depending on which variants are being defined as a "new virus," experts estimate there are between 8,000 and 50,000 known viruses. Perhaps 300 of those are "In-the-Wild", or known to be in the real world infecting computers. Testing antivirus software with a few dozen pet viruses is not statistically valid.
2. Many viruses infect boot sectors and master boot records and to run a valid test these need to be infected one at a time. Testing boot sector virus detection is a time-consuming, challenging process that doesn't begin to cover the full spectrum of in-the-wild viruses.
3. The best way to determine the quality of a product is to find out whether it has been certified by the International Computer Security Association (ICSA) and West Coast Labs (Checkmark). The ICSA creates test sets from the official published Wildlist compiled by the Wildlist Organization (www.wildlist.org). The resulting list inventories approximately 500 viruses which have shown up in the real world infecting computers. The ICSA and West Coast Lab also maintain a library of viruses known as the zoo which they use to test detection rates. Certification requires detection of 100% of in-the-wild viruses and at least 90% of viruses in the zoo.

4. Some vendors will distribute virus samples to reviewers which include rare samples they know their competitors will not detect. The best way to get a sample is to contact independent organizations like ICSA or West Coast Labs or have these independent organizations perform the testing for you.
5. Many vendors claim to have the ability to detect unknown viruses without backing up their claims. The ability to detect unknown viruses is important simply because viruses are coming out faster than software or pattern files can be updated.

Additional Factors to Consider

Defining the Virus Threat

Some vendors focus solely on the threat posed by programs that only meet the technical definition of computer virus. Obviously, a broader definition provides more protection. A complete antivirus solution should include protection from Trojans, malicious applets and related threats.

Cost of Ownership

Antivirus software is only as good as its last update. Approximately 500 new viruses appear in-the-wild and in the zoo each month, so products should be updated at least twice a month. If updates are not automated then they require the Administrator to take time from other business activities to verify that each desktop has been updated. There are tools which make this process faster and more efficient and these include centralized management.

Updates are only part of hidden costs associated with deployment and updating of antivirus software.

Consider the cost, in terms of time and resources, as well as how much training will be necessary and are end users required to participate. Non-technical end users should not be required to update or perform maintenance operations for the antivirus solution to be effective.

Central logs of virus events should be available not just from one server, but from all email servers so the administrator can work more efficiently. Centralized antivirus control offers the fastest response times and most effective defense against virus outbreaks.

Strength of Vision

Antivirus products require continued support and whether a vendor has its own true antivirus technology and virus research staff can become an issue when you really need support. Computer security is a highly dynamic market with new threats arising frequently. A company must have the vision to anticipate these threats and the technology

to respond to them. If a new class of threat appears, perhaps a hostile ActiveX applet or a new type of polymorphic virus, the product requires immediate updating to stop it.

Development of new technologies and problem solving scenarios is important to meeting the changing needs of business. A good antivirus product should be able to scan compressed files, but caution should be used when dealing with recursively-compressed files. One firm was sent an infected document, which had been zipped 2000 times over. Their email virus scanner attempted to recursively unzip the file 2000 layers deep. Not surprisingly, it ran out of memory and crashed the email server. The lesson here is the product should have been developed to scan a limited number of layers.

The product must also have the ability to expand with the enterprise as it grows. The Internet presents a number of new business opportunities and an antivirus solution should be able to fully protect the enterprise at every entry point. Protection should be about prevention and not rely solely on response.

Other Considerations

- Can the product manage multiple email servers simultaneously?
- Can the product tell you when a virus outbreak occurs?
- Can the product be installed and managed remotely without the need to set up complex trusted domains?
- Does the vendor provide a tool for managing all your antivirus products from a single console?
- Is there a way to scan both inbound and outbound mail?
- Can the product scan recursively-compressed files (zip files within zip files)?
- Can the product clean infections inside zipped attachments in real-time?
- Does the product scan public folders on access and on replication?
- Can the product scan nested attachment?
- Does the product detect malicious ActiveX and malicious Java code?
- Does the product's functionality match the needs of the market it was developed for?
- Is the product scalable to support the needs of the growing organization?
- Event tracking is very important as it allows companies to justify their efforts and budget to senior management.
- Does the product provide a central log of virus events?
- How comprehensive is the information in that log?

Appendix A: Virus Test Files

When you are testing antivirus software, you want to verify the product is working correctly. The problem is how to verify the product without introducing a real virus into your network. Testing virus detection using a real virus is a like catching the flu to see if the flu medicine works.

Since it is unacceptable to use a real virus to do testing, the European Institute of Computer Anti-virus Research (EICAR) has developed, along with antivirus vendors, a test file to assist users in testing their installations of antivirus software.

The EICAR file is not a virus. The file is a test file that may be used to test antivirus software. It is safe to pass around, because it is not a virus, and does not include any fragments of viral code. Most products react to it as if it was a virus, but in fact the file is a legitimate DOS program. The code is harmless and when detected properly the virus scanner will display the following message: EICAR-TEST-FILE

You can download the EICAR test script from the following URLs:

- <http://www.antivirus.com/vinfo/testfiles/>
- http://www.eicar.org/anti_virus_test_file.htm

Alternatively, you can create your own EICAR test script by copying the following into a text file and then naming the file "eicar.com":

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

If the installed software is working correctly, each of the following tests should result in a notification message and log entry that a virus was detected and the appropriate action performed.

Appendix B: About Trend Micro

Trend Micro provides centrally controlled server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and service providers worldwide to stop viruses and other malicious code from a central point before they ever reach the desktop.

Trend Micro's corporate headquarters is located in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia. Trend Micro's North American headquarters is located in Cupertino, CA. Trend Micro's products are sold directly and through a network of corporate, value-added resellers and service providers. Evaluation copies of all of Trend Micro's products may be downloaded from its award-winning Web site, <http://www.antivirus.com>.

