



Eliminating Viruses in the Microsoft Exchange Environment using Trend Micro ScanMail[®] for Exchange 5.5 (ESE Protocol)

***your* Internet VirusWall[®]**

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.antivirus.com or www.trendmicro.com



Table of Contents

ABSTRACT	3
The Microsoft Exchange Architecture	4
VIRUSES AND THE MICROSOFT EXCHANGE SERVER	5
Detecting and Cleaning Viruses in the Exchange Environment	6
HOW DOES THE TREND MICRO SCANMAIL ESE SOLUTION WORK?	7
TREND MICRO SCANMAIL® FOR MICROSOFT EXCHANGE.....	9
How ScanMail for Exchange ESE Works	9
Benefits of ScanMail for Exchange ESE API Solution	10
Spam Blocking and Content Filtering Management.....	12
Working with Microsoft Exchange Cluster Servers	13
ScanMail in Microsoft Exchange Cluster Environment	14
SUMMARY.....	16
APPENDIX A	17
ABOUT TREND MICRO	18

December 2001
Trend Micro, Inc.

©2001 by Trend Micro, Inc.

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 VCS, ScanMail, ServerProtect, OfficeScan, MacroTrap, Active Update, and SmartScan are trademarks of Trend Micro, Inc and registered in various jurisdictions worldwide. All other company and product names are trademarks or registered trademarks of their respective owners.

Abstract

Email and groupware systems require specialized antivirus software to prevent virus infections from spreading through shared server databases via attachments, data files, and executable programs. Such groupware formats render traditional virus protection ineffective because they lack the standardized formats and input/output activity queues traditional virus scanning engines rely on. As a result, network administrators are often forced to depend on desktop applications to combat viruses.

Unfortunately, desktop antivirus software only scans and disinfects local copies of attachments users save to their hard drives. This leaves the original file attachments, along with any viruses they are carrying, at the Exchange server where users may forward them, thereby spreading the virus. Since email file attachments are the single most common way that viruses spread today¹, effective email/groupware virus protection must address this primary threat to prevent viruses from spreading through information-sharing functions.

In November 1996, Trend Micro introduced ScanMail[®] for Microsoft Exchange, the first antivirus solution to effectively provide comprehensive protection under Exchange's proprietary communications environment. ScanMail for Microsoft Exchange is designed to detect infected files and eliminate viruses in real time at the server before they reach the desktop while protecting archived messages. Today ScanMail has a 31 percent market share in the antivirus groupware market².

This white paper outlines Microsoft Exchange's architecture, its vulnerability to viruses, and reviews how ScanMail works with Microsoft Exchange servers. The paper also describes the benefits of ScanMail for Microsoft Exchange in preventing virus proliferation.

¹ "Computer Virus Prevalence Survey 2000," September, 2000.

² September 2001 IDC Report

The Microsoft Exchange Server

A growing number of organizations rely on Microsoft Exchange for their communication needs. Every Exchange server has integrated email, group scheduling, electronic forms, groupware and Internet capabilities to create an environment where users can coordinate, discuss and collaborate on vital projects. Since Exchange servers support a wide variety of communications across a single platform, it has become one of the fastest growing email/groupware systems.

The Microsoft Exchange Architecture

The Mail Transport Agent (MTA) is at the heart of all information delivery, not only in the Microsoft Exchange Server, but also in most email and groupware systems (See figure 1). It is the logical place to intercept and scan for viruses and malicious code. Scanning at this point prevents infected files from reaching these systems' proprietary databases where they can spread, and also prevents infected information from being sent outside the network to prevent virus proliferation.

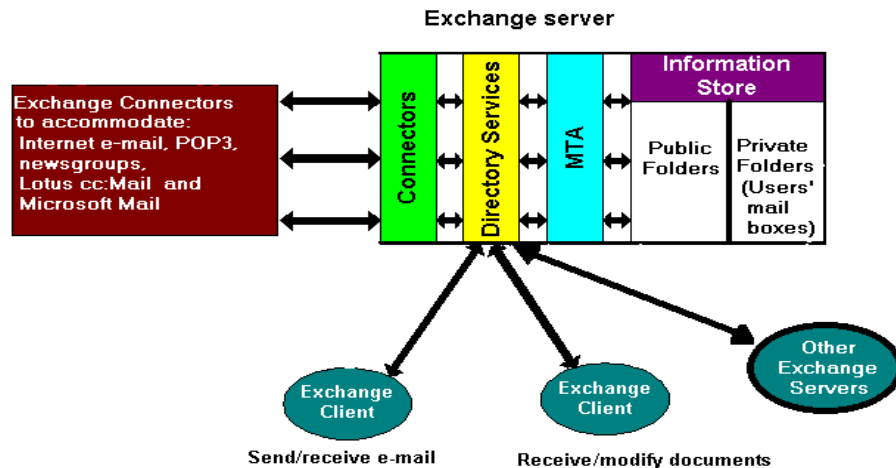


Figure 1. *The Microsoft Exchange Server, its Information Store where all information is scanned, and the Exchange “connectors” bridge for information to flow from and into the Exchange environment.*

Most messaging systems enable antivirus software to scan information at the MTA level with the exception of the Exchange Server. Microsoft has chosen to publish an MTA protocol to enable virus scanning Exchange at the MTA level. In the Exchange 5.5 environment, the most common scanning protocols are the Message API (MAPI) and the Microsoft virus scanning API (VS API). However, each of these scanning protocol has its weakness.

During a virus outbreak, there is a greater risk of the entire system becoming infected because MAPI hooks in at the inbox level. It is possible that the user might access a

message before ScanMail can scan it for viruses. This can be prevented by hooking at a lower level such as the Information Store of the Exchange server.

The Microsoft VS API provides scanning at the Information Store level, but it does not provide information such as the sender, recipient and the subject information for notification, reporting and logging.

Although Microsoft has improved the VS API in Service Pack 1 for the Exchange 2000 server, there is no plan to incorporate the fix in Exchange 5.5. Because Trend Micro is committed to offering customers an optional solution for the Exchange 5.5 environment, we have developed the Extensible Storage Engine (ESE) solution.

Connectors Extend Exchange's Communications Ability

Microsoft's March 1998 release of Exchange version 5.5 included additional connectors allowing more information to be traded outside its environment. Of the connectors listed in Figure 1, the ones listed below were new in the 1998 Exchange 5.5 release:

- SMTP Internet email service, to send Internet email
- X.400 Connector, IMC connector, to send and receive other mail message protocols
- A generic POP3 (Post Office Protocol 3) client allowing Internet email to be received

This simplifies sharing information between Exchange users and users located outside their environment. The new connectors translate electronic messages, files and documents from the Internet into Exchange's proprietary format.

Viruses and the Microsoft Exchange Server

Unfortunately Exchange's new, powerful information-sharing capability also creates new virus entry points which can lead to the infection of an organization's entire Exchange environment.

In the past, floppy disk-based viruses took weeks or months to travel around the world, but now it only takes a few seconds for a virus traveling via email to spread globally. The [W97M_MELISSA](#) virus was discovered on the morning of March 26, 1999 in the United States and by noon of that same day, this virus had traveled throughout the world, penetrating numerous enterprise networks.

Viruses spread from computer to computer when infected programs or data files are duplicated through server replication, Internet downloads, email attachments, floppy disks or any other means by which files are shared or exchanged. Viruses can be designed to carry a "payload" or undesirable action. These can be relatively harmless, like displaying an irreverent message on a user's screen, or be so damaging as to wipe out all data on the infected computer's hard drive.

In Exchange servers, viruses spread along with the files users share through email attachments and public folders, which are synchronized between servers through a replication process. While this replication process and Exchange 5.5's additional

connectors open servers to a broader range of Internet information sources, the process also greatly increases the risk of virus infestation.

Viruses in the Exchange Environment

Figure 2 demonstrates how a virus can proliferate throughout an organization via Microsoft Exchange server functions and then spread beyond that organization to users outside the network.

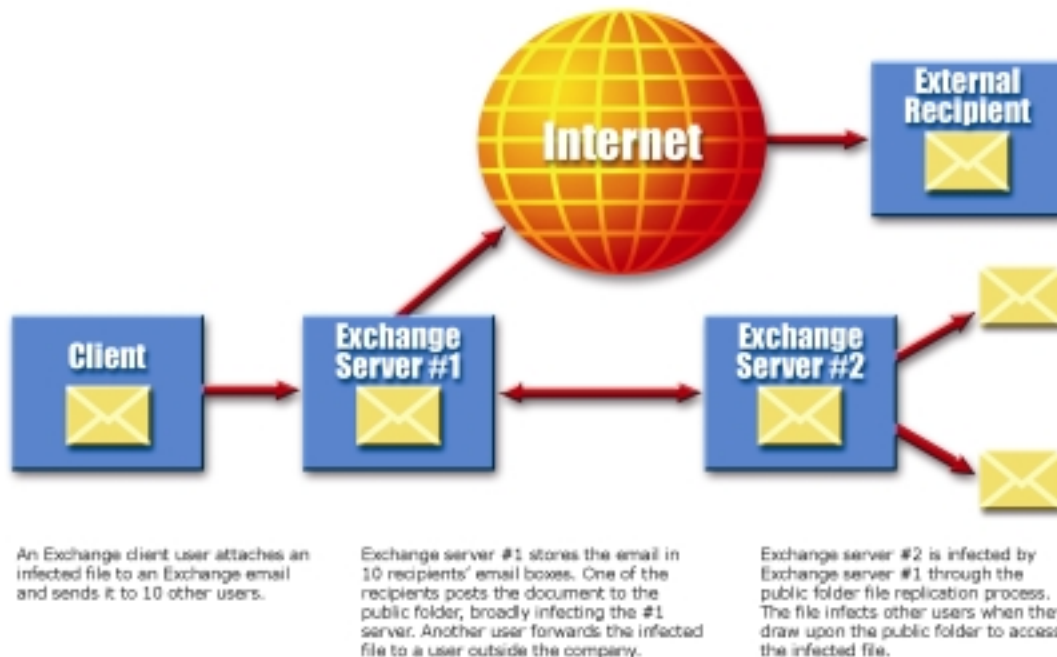


Figure 2. *One virus-infected file can quickly infect an entire organization and external users through Exchange's email and information-sharing functions*

Detecting and Cleaning Viruses in the Exchange Environment

Since messaging environments such as Microsoft Exchange have become important tools for business, any decline in performance of the Exchange server could negatively impact the company's daily operations and productivity. One approach to providing an effective antivirus solution for the Exchange environment involves providing real time protection at the Information Store level. In this approach, an on-demand or scheduled scan process would simultaneously scan and clean the archived folders residing in the Information Store database.

Once an antivirus solution cleans the Information Store, it must then prevent infected files from entering the server. Network administrators should be able to pinpoint and protect any possible virus entry points within the Exchange environment and enterprise network.

Exchange's external communication capabilities provide numerous network entry points that must be secured against viruses.

These include:

- User mailboxes
- Internet email attachments
- Newsgroup discussions that include posted file attachments
- Public folders where clients may store and access files
- Moving folders from one server to another
- Systems that transmit messages through connectors such as: Lotus cc:Mail, Microsoft Mail, SMTP, x.400 and other external email systems
- Remote access where Exchange Servers are being accessed through a Web browser

With the increase of new viruses and stealthy behaviors, antivirus products have to be more proactive when protecting the email environment besides scanning the message and attachment for virus. Recent viruses such as [NIMDA.A](#) reside in the memory and has the ability to infect many users in a very short period of time. During such virus attacks, every minute counts to avoid the virus from entering the network before an updated virus pattern is received from the antivirus companies. Under such conditions, ScanMail for Exchange with the support of ScanMail eManager has the capability of blocking any suspicious mail or attachments from entering the Exchange environment, by specifying the content of the message, content of attachments, subject line, and/or sender and recipients.

In addition to the virus entry points listed in Figure 2, Exchange Servers may be vulnerable to virus attacks due to uncoordinated virus protection elsewhere within the network.

How does the Trend Micro ScanMail ESE Solution Work?

Viruses such as the [VBS_LOVELETTER](#) have pushed the MAPI solution to the limit. Administrators around the world discovered that the MAPI method was not effectively protecting the network during a mass email attack on the server.

During that period, the Microsoft VS API was in the early stages of development and the method was lacking key message information for notification, logging and reporting on the Exchange 5.5 platform. Although this limitation was later addressed in the Exchange 2000 Service Pack 1, Microsoft has not announced plans to incorporate the fix in the Exchange 5.5 platform.

A series of mass email attacks in year 2000 alerted Trend Micro engineers who began looking into other possibilities for administrators who had concerns over the MAPI and VS API solutions. They developed a method of scanning at the Exchange store using the Microsoft Extensible Storage Engine API.

ESE API is a transacted database engine that stores all Microsoft Active Directory objects. When this scanning method was first introduced, Trend Micro engineers were reluctant the use the API because the solution was not supported by Microsoft.

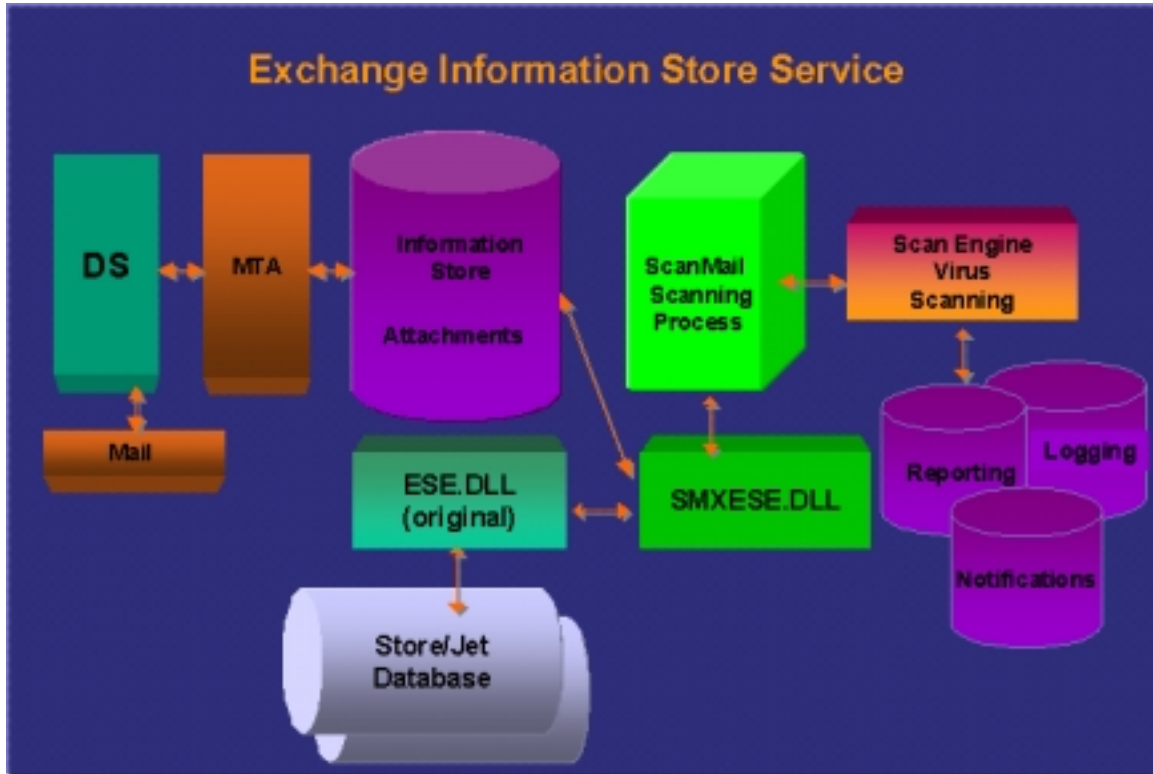


Figure 3 *ScanMail for Exchange v3.8 (ESE API) Architecture*

As research continued into the ESE solution, Trend Micro engineers discovered that ESE API provides all the message properties prior to being written to the Exchange Information Store database, thus provides an effective antivirus solution for Exchange 5.5 servers.

One of the challenges is redirecting the Information Store's call from the Microsoft ESE API to the ScanMail ESE API without affecting other software that is concurrently using the Microsoft ESE API. ScanMail for Exchange uses the NT Kernel hook method to direct all store.exe traffic to ScanMail for Exchange ESE. ScanMail for Exchange does not employ the renaming method, which might have effect on other software that uses the ESE API on the Exchange server. When the ScanMail services are stopped, the ScanMail for Exchange NT Kernel hook will redirect the store.exe traffic to the original Microsoft ESE API and does not require stop and restart of the Exchange services.

In addition, when implementing the ScanMail ESE solution, the Exchange services should not be dependent on the antivirus solution functioning in order to conduct normal activities. If ScanMail has any obstruction, users would still be able to perform their daily Exchange activities without the virus protection.

By routing all traffic through the ScanMail ESE API, ScanMail will scan for any virus in the message body and attachment. Once done, ScanMail writes all information to the database by calling the original Microsoft ESE DLL, thus ScanMail does not have direct contact with the Exchange Store database.

Trend Micro ScanMail® for Microsoft Exchange

Trend Micro was the first antivirus company to develop and market effective technology to detect and eliminate viruses inside the Microsoft Exchange environment. ScanMail for Microsoft Exchange performs real-time monitoring of incoming and outgoing email attachments, thereby eliminating viruses from the Exchange server before users can make copies of infected files.

ScanMail uses Trend Micro's award-winning 32-bit multi-threaded scanning scan engine with MacroTrap™ technology, which minimizes the performance impact on Exchange servers during scanning. This virus detection engine uses minimal server CPU resources while increasing its scanning speed and performance by more than 50 percent over Trend Micro's previous scan engine.

With the addition of the new ScanMail ESE API that hooks into the Exchange database, ScanMail will provide fast real-time scan of all attachments passing to and from the Exchange Server.

How ScanMail for Exchange ESE Works

ScanMail features:

- ❑ Easy navigation and configuration across the enterprise from a Windows Interface
- ❑ Easy selection of specific folders for scanning, including public folders and other mailbox items like Outbox and Sent Items
- ❑ Flexible configuration with multiple entries to invoke prescheduled scanning and pattern update downloads
- ❑ Easy look up of virus incident reports, update logs and virus information
- ❑ Easy, automatic updating of scan engines, virus pattern files and patch files through the Internet

ScanMail for Exchange v3.8 includes support for the Exchange Extensible Storage Engine (ESE) API for the scanning of both inbound and outbound traffic. The current implementation of the ESE solution will support the Exchange 5.5 service pack 2 and above environment.

Under the ESE protocol, ScanMail fully utilizes the ESE API capability of accessing the message before it is written to the information database. With this capability, ScanMail can scan and take action on the message and attachment before it hits the user inbox, thus provide a secure method of protection virus from infected by the user.

Real-time Scanning and Single Instance Scanning

In the implementation of the ESE API, all attachments of inbound and outbound messages will be scanned before they are written to the Information Store database. As email attachments arrive at the Information Store they are passed to ScanMail for automatic scanning and cleaning. Once this is completed, the attachments are written to the Information Store database using the original Microsoft ESE API and the email with its attachment will be sent to the recipient(s).

Since the ESE API scans before the message is written to the database instead of scanning at the individual user inbox, the message will be scanned once irrelevant of the number of recipients the message was intended for.

Active Message Filter™

Full access to the attachment and message is one of the limitation of ESE API, so when there is a virus outbreak, infected messages with zeroed out attachments will still be delivered to the end-user. For those end-users who are not familiar with the antivirus product might think they still have the infected email on their desktop and it can therefore create a lot of support calls to the IT helpdesk. To avoid this, Trend Micro has developed the Active Message Filter that will prevent the delivery of the zero byte messages to the end-user, when a virus is found or attachment blocked. When the message contains virus or has met the attachment blocking rules and the action is set to delete, the administrator now has a choice of deleting the entire message from being viewed by the end-user.

Support for Trend Micro ScanMail eManager™

In addition to real-time scanning for viruses, ScanMail constantly monitors all messages and content passing through Exchange servers using Trend Micro ScanMail eManager. eManager scans and blocks inappropriate content and unsolicited messages from entering Exchange servers. eManager is an optional plug-in available for ScanMail.

Blocking unsolicited, spurious and obscene content increases a server's overall performance by shortening email delivery time and freeing up valuable disk space on both servers and workstations. eManager's content filtering capabilities can be used to pass only work-related messages and attachments to users, helping to maintain employee productivity and work performance. eManager can also be used to stop sensitive information from leaving the confines of an organization via email.

Benefits of ScanMail for Exchange ESE API Solution

Administrators Determine Infected File Handling

ScanMail performs real-time scanning of information entering Exchange servers and provides manual or prescheduled scanning of existing email and public folder archives. Network administrators determine whether ScanMail will clean, delete, move or pass infected files found within the Information Store.

ADVANTAGES OF THE SCANMAIL ESE SOLUTION

- ❖ Enables the detection and elimination of viruses by scanning email attachments before an email is delivered or leaves the Information Store
- ❖ Improved real-time scanning performance and resource usage on the Exchange server with the support of memory scanning
- ❖ Does not use the rename method to the Microsoft ESE API, thus will not create potential problem for any software that uses the Microsoft ESE API
- ❖ By using the NT Kernel hooking method, ScanMail can ensure that only the Information Store's request to the ESE API is redirected to the ScanMail ESE
- ❖ Exchange service is not dependent on the antivirus software. Users will still be able to perform their daily Exchange routines, even if there is a problem with ScanMail
- ❖ Supports the ScanMail eManager™ plug-in for content filtering and anti-spam capabilities on the Exchange server
- ❖ Scans and blocks both inbound and outbound email attachments at the Information Store level with a low-level API hook
- ❖ Improved real-time, manual and scheduled scan performance and resource usage on Exchange servers with the ESE API
- ❖ ScanMail preserves the original email route to avoid information detours, preserve server performance and eliminate false delivery problems that can arise from additional routing
- ❖ Includes Active Message Filter™, which is responsible for preventing zero byte messages from being delivered to the end-user when a uncleanable virus is found or a file is blocked
- ❖ ScanMail only scans the email messages that have attachments or attachments that are capable of infection since they are the only ones capable of carrying viruses. Automatically bypassing email without attachments, unless configured to scan the message body for virus, reduces system overhead
- ❖ Scanning and file blocking by true file type, thus, ScanMail will still be able to detect the file type even if the file extension has been altered
- ❖ ScanMail's incremental scanning examines email attachments only once avoiding unnecessary repeated scanning of email archives to enhance overall scanning performance and shorten email delivery time
- ❖ ScanMail's attachment blocking capability allows administrators to delete or quarantine the specified file name and/or file extension
- ❖ Improved real-time, manual and schedule scan performance and resource utilization on the Exchange server by providing multi-threaded and thread pooling capabilities
- ❖ ScanMail's Performance Monitor generates real-time reports of regular and infected email traffic passing through Exchange servers for easy analysis and reporting

Simple Remote Deployment and Management

ScanMail's straightforward set-up procedures facilitate quick, easy installation across the entire Exchange environment. In order to be configured correctly to scan all mailboxes, ScanMail requires an NT account with full administrator-level privileges at the *site level* and *configuration levels*. It is not necessary to have administrator-level privileges at the *organization* to install or configure ScanMail. ScanMail prompts administrators through dialogue boxes to ensure that sufficient access rights are granted. The administrator then sets default actions for ScanMail to take when viruses are found and determines what notification message(s), if any, to send out to the sender, recipient or network administrators.

ScanMail for Microsoft Exchange was the first antivirus

product on the market that could be deployed and installed on remote Exchange servers across enterprise networks. This saves network administrators time in deploying duplicate virus protection to individual Exchange servers, making it unnecessary to travel to and from different geographical server locations.

On each Exchange installation server, ScanMail hosts a Web-based list to deploy virus protection to other Exchange servers. This list is automatically updated to reflect newly added or uninstalled Exchange servers. Each server entry on the list provides a link to ScanMail's Web-based control and configuration console for that server. Hence, administrators can now quickly and easily update ScanMail across their entire enterprise by downloading the latest virus pattern files from Trend Micro's Web site.

Furthermore, ScanMail's Web-based management console enables network administrators to configure and manage ScanMail throughout the enterprise via the Internet or an intranet environment.

Handling Scan Engine, Pattern and Patch Files

ScanMail includes ActiveUpdate™ technology that allows administrators to easily update the scan engine, pattern, and patch files across the enterprise — either on-demand or at pre-scheduled update times set by network administrators.

Spam Blocking and Content Filtering Management

The volume of unsolicited and inappropriate email continues to reach all-time highs. To address this problem, ScanMail for Exchange now includes email content filtering and spam blocking functions with the optional ScanMail eManager plug-in. ScanMail and eManager work together to monitor incoming and outgoing messages to ensure that emails received by end-users are safe, virus-free, and originate from legitimate sources.

Anti-Spam Filtering

The Anti-Spam filter defines which messages are to be blocked on the basis of the information appearing in the header. For example, messages may be blocked based on the domain from which email has been sent, or based on the contents of the "From," "To" and "Subject" fields.

Email Content Filtering

The Email Content Filter eliminates unsolicited commercial email (UCE, more commonly known as spam) before it reaches Exchange server(s). By employing a series of user-defined rules to evaluate the header and message text of incoming email, as well as the message attachments, ScanMail eManager's content filter reduces the number of solicited messages transported by the Exchange server, improving its efficiency and ensuring that the messages received by the end-user are valid. Content filtering provides a

means to evaluate and regulate incoming email traffic on the basis of the message text itself. Content filtering of inbound messages provides a more in-depth, sophisticated analysis of messages than anti-spam filtering. Content filters can be used to develop detailed, user-defined rules that address any number of specific content types. In addition, a synonym list extends the conceptual reach of the content filter through “fuzzy logic.”

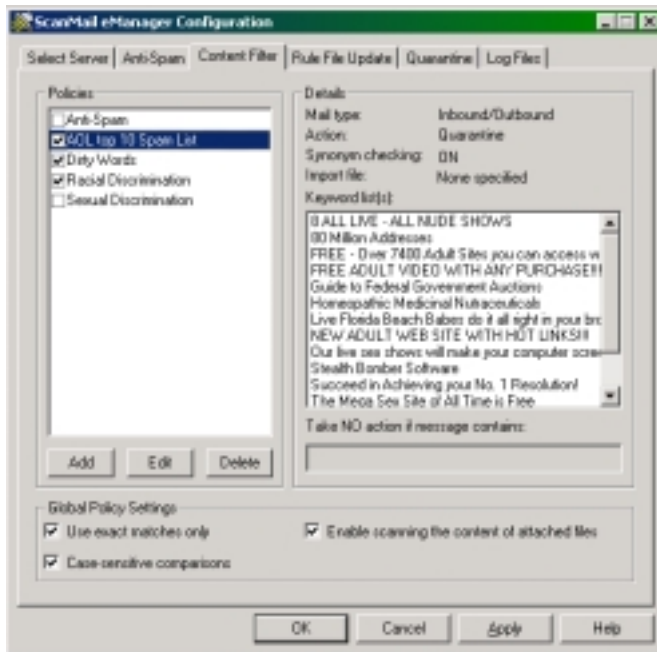


Figure 4. ScanMail's eManager filters email with sensitive content and blocks spam.

Working with Microsoft Exchange Cluster Servers

There are two basic methods for designing an antivirus product to work in the Microsoft Exchange Cluster Environment. One method is to customize an existing Exchange Server antivirus product to support the most common Exchange Server Cluster configurations. This method falls short because fail-over and disaster recovery are not initiated directly through the cluster server, but is triggered indirectly through monitoring of the Exchange Server on the product side.

The second is to design a product that takes full advantage of the Cluster API. This second process requires time and architecture changes on the part of the product and also requires written documentations of all the necessary processes and application components to be registered and installed as cluster resources.

Because it is the first antivirus product on the market that is fully compliant with Microsoft Exchange Cluster technology, ScanMail for Exchange installs as part of the Exchange Cluster resource and operates seamlessly to provide virus protection for clustered servers while preserving all fail-over and disaster recovery capabilities that can be initiated through cluster technology.

ScanMail must be installed on both the active and passive server nodes. During installation, the setup program automatically detects all cluster nodes and installs itself on the appropriate shared drive, selected by the user, on each node. It also adds ScanMail cluster resources automatically to the Exchange Cluster resource group. After ScanMail is installed, it automatically initiates all ScanMail services and begins protecting the active server mailboxes.

Trend Micro offers a better solution by completely restructuring the architecture of ScanMail to fully support all features of the Microsoft Cluster API. ScanMail's native cluster server architecture provides fail-over and disaster recovery automatically and directly through Microsoft's built-in clustering API. When installed, ScanMail will create its own cluster resources and install/register in the Cluster Administrator Console. Microsoft has approved this approach.

ScanMail in Microsoft Exchange Cluster Environment

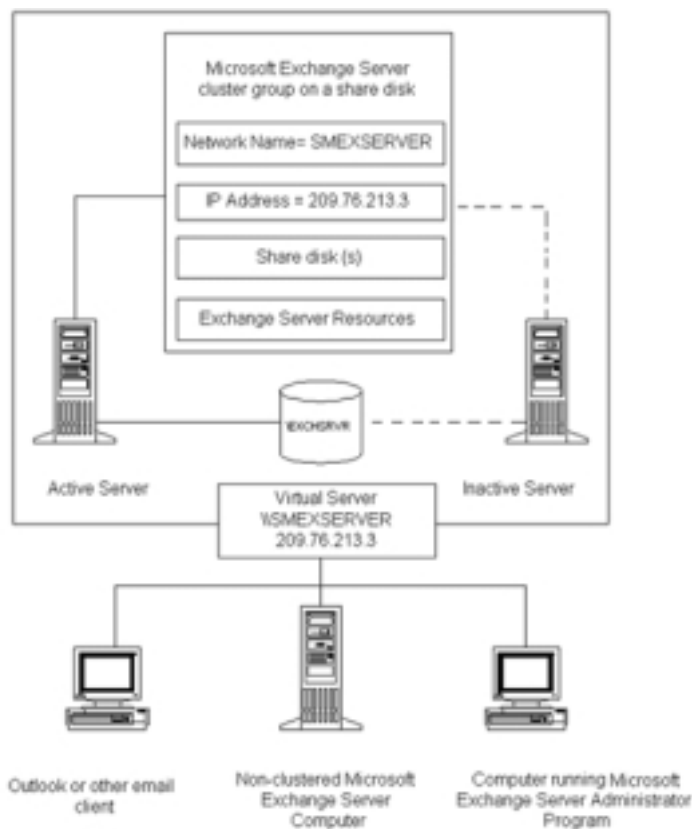


Figure 5. *The Microsoft Exchange Cluster*

one or more common physical disk drives, an IP address, a network name and Microsoft Exchange Server cluster resources.

Clustering two identical Microsoft Exchange Servers ensures that messaging services remain uninterrupted even if one of the nodes (servers) fails.

Sometimes referred to as “WolfPack,” the Microsoft Exchange Cluster is Microsoft’s version of fault tolerant server technology with disaster recovery/prevention capabilities designed for Windows[®] NT and Exchange environments. It is equivalent to Novell[®] NetWare[®]’s SFT III fault tolerance, except that under a NetWare environment, the administrator will only see one logical server. When cluster support is applied in a Windows NT environment, the administrator sees one logical server (cluster server) and two physical servers with their own static IP address.

A cluster consists of two Microsoft Exchange Servers, also called nodes, which share

For example, if the processor in a clustered Microsoft Exchange Server computer fails, the other server in the cluster is available to take its place. Users on the failed server do not see a change in their email service and continue to send and receive email without interruption.

Within a Microsoft Exchange Server cluster, only one node in the cluster can service network requests at any one time. The node that owns all clustered resources is called the active node. It owns the shared disk(s), the IP address and the network's name for the cluster while running Microsoft Exchange messaging services. If the active node in a cluster experiences a hardware failure, Microsoft Exchange services automatically migrate to the inactive node, which then becomes the active node.

As the following illustration of a Microsoft Exchange Server cluster shows, all network requests to the clustered Microsoft Exchange server are directed to the virtual server defined by the cluster, not to an individual node. Only the active node receives and processes these requests on behalf of the cluster. ScanMail should be installed into the two physical nodes, not the virtual node.

Note: When Microsoft Exchange Server is installed into a cluster environment, it is configured in a high-availability model, in contrast to a model that provides load balancing. As a result, Microsoft Exchange Servers assume the cluster is symmetrical. Consequently, both servers in a cluster must be identical in terms of performance and capacity so that one can host the other's clustered resources.

Clustering is also convenient if you need to upgrade a server or add new hardware without interrupting service to users. Exchange functions can *fail-over* to the cluster's other server, allowing it to take over the functions of the one being upgraded.

Summary

In Microsoft Exchange servers, viruses spread along with the files users share through email attachments and public folders, which are synchronized between servers through a replication process. Since messaging environments such as Microsoft Exchange have become one of the most widely used tools for businesses worldwide, any decline in performance of the Exchange server could negatively impact a company's daily operations and productivity.

Trend Micro engineers began looking into other possibilities for administrator who had concerns over the MAPI and VS API solutions. The engineers soon developed a method of scanning at the Exchange store using the Microsoft Extensible Storage Engine API. Trend Micro engineers discovered that ESE provides all message properties prior to being written to the Exchange Information Store database, thus provide an effective antivirus solution for Exchange 5.5 servers.

Appendix A

System Requirements

- Intel Pentium 200MHz or higher
- Windows NT server 4.0 with Service Packs 5 or above, Windows 2000 Server
- Microsoft Exchange server 5.5, with Service Pack 2 or above
- Microsoft Exchange Cluster Server Enterprise Edition, Windows 2000 Cluster Server
- 128MB RAM or higher
- 50MB free disk space for program files

Recent ScanMail Awards

- 2001, ScanMail for Microsoft Exchange and ScanMail eManager, *Editors' Choice*, PC Magazine
- 2000, ScanMail for Microsoft Exchange, **MEC 2000 Solutions Award: Best Tool/Utility**, Microsoft Exchange and Collaboration Solution Conference 2000
- 2000, **Secure Computing Millennium Award: Best Content Security**, SC Magazine
- 2000, ScanMail for Microsoft Exchange 2000, **Best Buy Award**, Secure Computing Magazine
- 1999, ScanMail for Exchange, **Solution of the Year**, PC Expert Magazine (France)

ScanMail Certifications

- International Computer Security Association, **ICSA Certified**, Detect 100% of viruses In-the-Wild
- West Coast Lab, **Check Mark Certified**, Detect 100% of viruses In-the-Wild

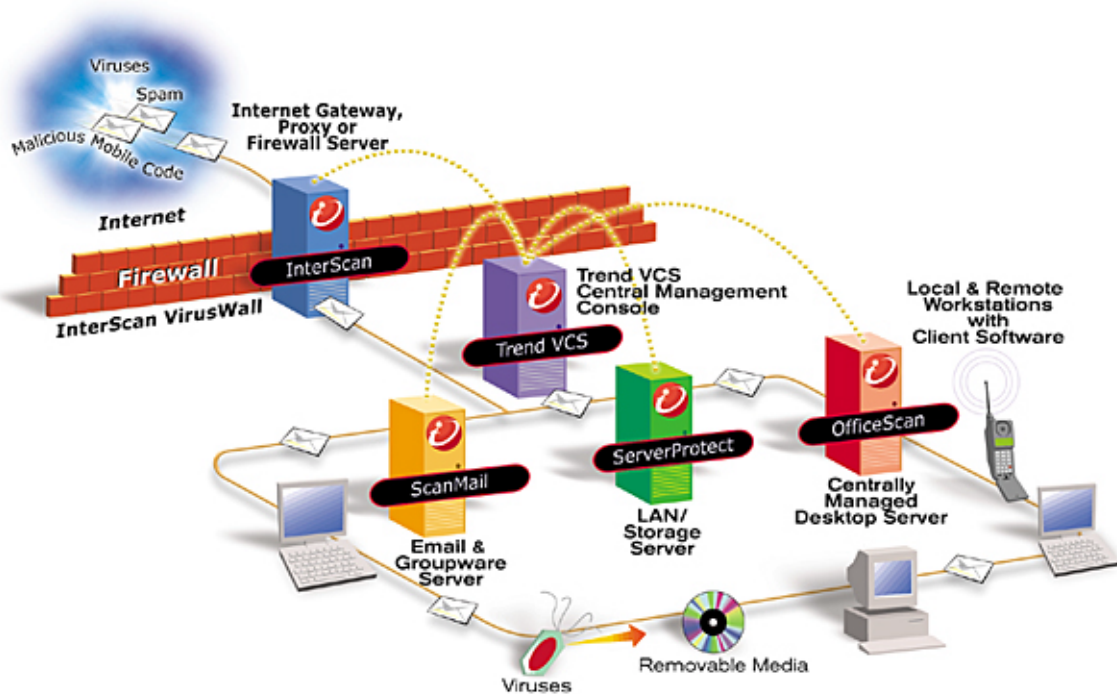
Bibliography

ICSA Labs (a Division of ICSA.net), "Computer Virus Prevalence Survey 2000," September, 2000. Available on the Web at: <http://www.icsa.net>

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>.



Trend Micro products working together to cover all enterprise virus entry points