



WHITE PAPER  
TREND MICRO™ SCANMAIL™  
FOR MICROSOFT® EXCHANGE

MAY 2002

TREND MICRO, INC.  
10101 N. DE ANZA BLVD.  
CUPERTINO, CA 95014  
T 800.228.5651 / 408.257.1500  
F 408.257.2003  
[WWW.TRENDMICRO.COM](http://WWW.TRENDMICRO.COM)

# Protecting the Microsoft® Exchange Environment

## TABLE OF CONTENTS

3	Abstract
4	Viruses and The Microsoft Exchange Server
5	Detecting and Cleaning Viruses in the Exchange Environment
6	Trend Micro ScanMail for Microsoft Exchange
9	Conclusion
10	About Trend Micro

May 2002  
Trend Micro, Inc.

©2002 by Trend Micro Incorporated. 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 Trend Micro Incorporated. Trend Micro, the t-ball logo, AppletTrap, Control Manager, eManager, GateLock, InterScan, HouseCall, InterScan VirusWall, MacroTrap, NeaTSuite, OfficeScan, PC-cillin, PortalProtect, ScanMail, ScriptClean, ScriptTrap, ServerProtect, SmartScan, TMCM, Trend Micro Content Scanning Protocol, Trend Micro Control Manager, Trend Micro CSP, Trend Micro Damage Cleanup Server, Trend Micro Damage Assessment and Cleanup Services, Trend Micro Outbreak Prevention Services, TrendLabs, Trend VCS, VirusWall, WebManager, WebProtect and WebTrap are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

## ABSTRACT

Email and groupware systems require specialized antivirus software to prevent viruses from spreading via attachments, data files, and executable programs shared through databases. While the proprietary formats of these databases ensure the security of the information they process, they also defy antivirus software's traditional scanning techniques. Proprietary email and groupware formats render traditional virus protection ineffective because they lack the standardized formats and API functions relied on by traditional virus scanning products. Hence, traditional antivirus software either bypasses or is unable to scan the email attachments and other information shared within these proprietary databases. Network administrators seeking email and groupware antivirus strategies are often forced to rely on desktop applications to combat viruses.

Unfortunately, desktop or server antivirus software only cleans local copies users save to their hard drives. This leaves the original files, along with any viruses they are carrying, sitting on the server ready to spread viruses. Since email file attachments continue to be responsible for 80% of virus outbreaks<sup>1</sup>, effective email/groupware virus protection must address this primary threat to prevent viruses from spreading through information-sharing functions.

This paper outlines the Microsoft® Exchange™ server architecture, identifies its vulnerability to viruses, and reviews how Trend Micro ScanMail for Microsoft Exchange and Trend Micro ScanMail for Microsoft Exchange 2000 functions in the Exchange environment.

<sup>1</sup> 2001 ICSA Labs 7<sup>th</sup> Annual Virus Prevalence Survey

## VIRUSES AND THE MICROSOFT EXCHANGE SERVER

From the smallest companies to the world's largest enterprises, a growing number of organizations are moving quickly to the new messaging and collaborations platform built for Microsoft Exchange. These companies rely on the Exchange server for mission-critical communications. Through integrated email, group scheduling, electronic forms, groupware and Internet capabilities users can coordinate, discuss and collaborate on vital projects. Exchange's support for a wide variety of communications on a single platform has made it one of today's fastest growing email/groupware systems.

### An Examination of Viruses

All messaging systems are vulnerable to virus attacks. Viruses spread when infected programs or data files are duplicated through server replication or any other means by which files are shared or exchanged. Viruses are usually designed to carry a "payload" or an undesirable action generated by a virus. While some of these viruses are relatively harmless, like displaying an irreverent message on a user's screen, they can also be damaging enough to wipe out all data on the infected computer's hard drive or completely shutdown the mail server through some form of denial of services.

In Exchange servers, viruses spread along with the files users share: through email attachments, public folders replication, database replication, installable file system and other Exchange compliance applications using the Web Store to store information and content. With the additional connectors and new protocols for the Exchange server, they are open to a broader range of Internet information sources, greatly expanding the number of opportunities for virus infestation.

Antivirus products have to be more proactive when protecting the email environment and should offer a strategy that goes beyond scanning the message and attachment for viruses. As Nimda and CodeRed proved, mixed-threat viruses can reside in the memory and infect a greater number of users in a much shorter period of time. During a mixed-threat virus attack, every minute counts, because the network is at its most vulnerable before an updated virus pattern is distributed by an antivirus vendor.

Under such conditions, ScanMail for Exchange, with the support of ScanMail eManager and Trend Micro Control Manager, has the capability of blocking any suspicious mail or attachments from entering the Exchange environment.

A virus in one client computer can proliferate throughout an organization via Exchange server functions and then spread beyond that organization to users outside the network. While the old style file and boot sector viruses remain a destructive threat which must be

addressed, most industry experts agree that mixed-threat viruses, like nimda, have eclipsed the former in terms of frequency of occurrence and has become the preferred method for virus writers to create successful viruses.

## **DETECTING AND CLEANING VIRUSES IN THE EXCHANGE ENVIRONMENT**

An effective antivirus solution for the Exchange environment provides real-time scanning on all Information Store databases for virus and other malicious content threats including inappropriate and unsolicited content. This includes both the EDB and STM database levels, while at the same time continually scanning and cleaning the archive folders residing in the Information Store database from using an on-demand or schedule scan process.

Once an antivirus application disinfects the Information Store database, 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.

Because many companies use an array of mismatched antivirus products, the server leak factor sometimes affects Exchange servers. The resulting overlap of functions, gaps in virus protection and different protocols used by competing antivirus packages, prevents them from working together to effectively protect Exchange servers and their client users. In such an environment, conventional viruses, malicious Java™, and ActiveX™ code can leak past gateways and file servers to infect Exchange servers and the enterprise at large.

The client leak factor is created by the reverse situation with desktop antivirus products being unable to scan Exchange email attachments, mailboxes or public folders, thereby allowing users to post or download infected files to Exchange servers.

Monitoring all potential points where viruses can enter enterprise-computing environments and leak into Exchange servers is CPU-resource intensive. Additionally, such monitoring can become extremely cumbersome for network administrators to manage. Fortunately, Trend Micro's family of integrated antivirus products includes an Exchange-specific application providing easy-to-manage, resource-efficient protection from viruses.

## **TREND MICRO SCANMAIL FOR MICROSOFT EXCHANGE**

Trend Micro was one of the first antivirus company to develop and market effective technology to detect and eliminate viruses inside the Exchange and Exchange 2000 environment. ScanMail for Exchange performs real-time monitoring of incoming and outgoing email attachments and message body, thereby eliminating viruses from the Exchange and Exchange 2000 server before users can make copies of infected files.

ScanMail uses Trend Micro's award-winning 32-bit multi-threaded VSAPI scanning engine with MacroTrap™ and Trend Micro™ ScripTrap technology. Trend Micro's patent-pending scanning engine minimizes the performance hits to servers during scanning. Furthermore, ScanMail cleans both known viruses in-the-wild as well as unknown macro viruses. Trend Micro's virus detection engine is designed to use minimal server CPU resources while increasing its scanning speed and performance by more than 50 percent over the previous scanning engine.

### **Spam Blocking and Content Filtering Management**

To address the problem of unsolicited and inappropriate email, ScanMail now includes email content filtering and spam blocking functions with its optional ScanMail eManager plug-in module. ScanMail and eManager are designed to 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 (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, content filtering offers a tool 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."

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.

### **Notification and Logging**

In a large enterprise environment it is important to receive notification when a virus is detected since it allows problem viruses to be effectively isolated and quarantined. ScanMail notifies network administrators, the sender and the recipient of any newly detected viruses

using email, SNMP trap notification, pager messaging, and Windows NT event log recording. Each of these notification methods can be configured to send a standard default message or a customized alert.

In addition to these standard notification methods, ScanMail offers the option of sending Outbreak Alert notifications whenever a high number of viruses attempt to pass through the Exchange server or if a pre-selected number of viruses have not been cleaned within a few hours.

Once properly configured, ScanMail creates logs of viruses attempting to pass through Exchange servers. These logs are later used to generate reports and analysis to better manage future virus threats. To help prevent future virus outbreaks, ScanMail's browser interface can remotely retrieve each server's virus logs to trace the source of infected files and isolate infested sites. This function can save administrators hours of valuable time and cuts the potential costs of a virus outbreak.

Administrators are provided with services both on-site and remotely through ScanMail's use of a Web browser. Depending upon the administrator's requirements, notification services can be configured to automatically alert administrators, the sender, recipients and selected Exchange users of infected email transmissions. The notification can be either by email, SNMP trap notification or pager. Administrators can elect to send a standard default notice or their own customized warning message.

A warning notification is sent to the sender and recipient in the attachment message and includes the infected attachment renamed with a customized message inserted inside. Administrators can customize this notification message or select not to send a notification if the attachment is successfully cleaned.

All automatic actions are performed on infected files in accordance with the administrator's configuration. Options include cleaning the file prior to sending it to original recipient, deleting the infected file, moving it into a quarantined folder, or letting it pass with a warning message to the user. In addition, ScanMail can be configured to backup infected attachments before any action is taken.

## **Centralized Management**

Threats from viruses and malicious code have become both more frequent and sophisticated, irrevocably changing the e-business environment. New threats are constantly appearing and as a result, point solutions of the past could be insufficient, compelling Trend Micro to develop a revolutionary approach to protect customers from these threats. Trend Micro Control Manager provides a comprehensive approach to protecting your corporate environment. Administrators are provided with an enterprise wide picture of the network and tools for keeping the environment protected.

Trend Micro Control Manager™ does more than just manage Trend Micro's antivirus products. It provides complete outbreak policy and content security management for the enterprise. Industry competitors often rely upon scheduled polling mechanisms that provide status to a management console or server at preset intervals. In reality, this method is not only slower than real-time notification but produces excessive strain on bandwidth when a large number of clients are periodically polling for virus activity.

Control Manager provides event driven notification. Control Manager utilizes real-time, event-triggered notification of outbreaks for the most up-to-date status of virus activity within the network. Control Manager can be configured to send out notifications of significant or unusual network events via email, pager, SNMP trap, and NT event log. This allows the administrator the option to remain informed of fluctuations in the network and to receive up-to-date information during a virus outbreak.

When a virus outbreak occurs, Outbreak Commander is designed to provide actions and policies to deploy and provides the administrator with recommended actions and policies to initiate, based on the virus classification. These options can be put into effect automatically, helping to reduce the administrator's burden, while providing more comprehensive protection.

## CONCLUSION

Traditional desktop antivirus software alone cannot provide complete virus protection for the enterprise, and it is unable to detect viruses embedded in email attachments inside Exchange servers. Desktop protection waits until users open attachments, leaving open the potential for infected files to be copied to the hard drive before scanning and cleaning is done.

Since traditional desktop antivirus applications cannot provide full protection within Microsoft Exchange proprietary email/groupware messaging format, enterprises must deploy email-specific scanning products, such as ScanMail for Microsoft Exchange and ScanMail for Microsoft Exchange 2000, for more complete virus protection.

Trend Micro recommends the deployment of four tiers of virus protection. This proactive approach includes complete SMTP scanning on the gateway, comprehensive virus protection of email and groupware servers, complete file server protection on all application/file sharing servers to help ensure they are free of virus, and a desktop antivirus software solution at the end-user level.

Trend Micro's approach to virus control provides complete desktop protection to aid in verifying all files copied from floppy or local hard drives are scanned and cleaned. These four layers of protection ensure the best virus protection in an organization.

## 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.trendmicro.com/>.