



WHITE PAPER
TREND MICRO™ SCANMAIL™
FOR MICROSOFT™ EXCHANGE

FALL 2003

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

Protecting the Microsoft™ Exchange 2000 and 2003 Environments

TABLE OF CONTENTS

4	Abstract
5	Microsoft Exchange 2000 and 2003 Server Architecture
7	The Microsoft Virus-Scanning API
7	The Trend Micro Implementation of the Microsoft Virus-Scanning API 2.0
8	The Trend Micro Implementation of the Microsoft Virus Scanning API 2.5
8	Virus Protection on the Microsoft Exchange 2003 Gateway/Bridgehead Server
9	Viruses and Microsoft Exchange 2000 and 2003 Servers
10	Detecting and Cleaning Viruses in the Exchange 2000 and 2003 Environment
10	Trend Micro™ ScanMail™ for Microsoft Exchange
11	Award-Winning Virus-Scanning Technology
11	Outbreak Prevention Services
12	Spam Blocking and Content Filtering Management
12	Anti-Spam Filtering
12	Email Content Filtering
13	Quarantine Management
13	Message Purging
13	Notification and Logging
14	Centralized Management
15	Virus Response Service Level Agreement
15	Trend Micro Control Manager™

Protecting the Microsoft® Exchange™ 2000 and 2003 Environment

16	Outbreak Commander
16	TrendLabs™: A Global Network of Security Expertise
17	How Trend Micro Enterprise Protection Strategy Responds to Security Threats
17	Conclusion

Fall 2003
Trend Micro, Inc.

©2003 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, eManager, MacroTrap, ScanMail, ScriptTrap, Trend Micro Control Manager, Outbreak Prevention Services and TrendLabs, 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 traditional virus scanning techniques. Proprietary email and groupware formats lack the standardized formats and API functions that traditional virus scanning products rely on. For proprietary formats, traditional antivirus software is ineffective and either bypasses or is unable to scan email attachments and other information shared within these proprietary databases. Network administrators seeking email and groupware antivirus strategies are often forced to install and support desktop applications to combat viruses.

Unfortunately, desktop or server antivirus software only cleans local copies of files saved to hard drives. This leaves the original files, along with any viruses they are carrying, available on the server for other users to access. Email file attachments continue to be responsible for 80% of virus outbreaks (ICSA Labs 7th Annual Virus Prevalence Survey, 2002), therefore, 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 2000 and 2003 server architecture, identifies its vulnerability to viruses, and reviews how Trend Micro™ ScanMail™ for Microsoft Exchange functions in the Exchange 2000 and 2003 environments.

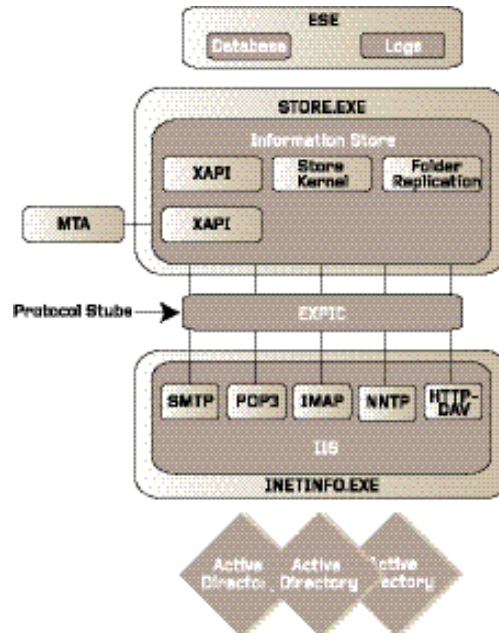
MICROSOFT EXCHANGE 2000 AND 2003 SERVER ARCHITECTURE

From the smallest companies to the world's largest enterprises, a growing number of organizations are quickly moving to the new messaging and collaborations platform built for Microsoft Exchange 2000 and Exchange 2003, Windows 2000 and Windows 2003. Support for a wide variety of communications on a single platform has made Exchange one of the fastest growing email/groupware systems. 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.

The Exchange server architecture provides users with a scalable messaging, data retrieval, and file sharing system. It allows greater flexibility for the administrator to design the network environment through integration with the Windows Active Directory, Microsoft Internet Information Service (IIS), and Web Storage System. Protocols such as Network News Transport Protocol (NNTP), Post Office Protocol version 3 (POP3), and Internet Message Access Protocol version 4 (IMAP4) run as part of the IIS process. The use of multiple databases and protocols expands the server's capabilities to reduce network traffic, expedite, and broaden data retrieval and usage, as well as to provide scalability, security, rapid recovery, and failover.

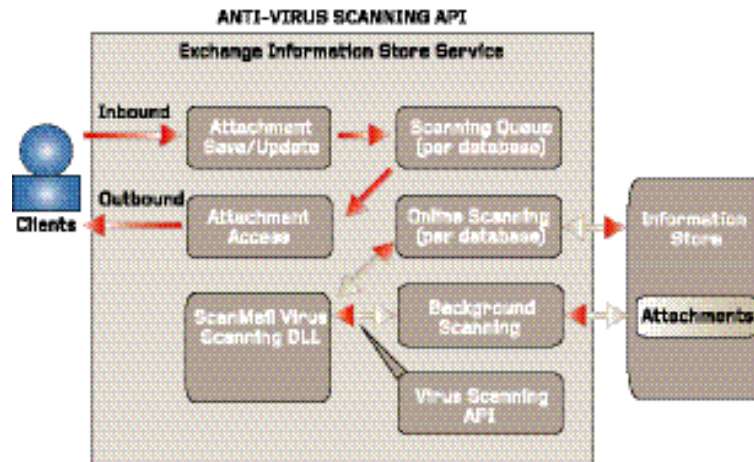
Exchange also supports multimedia formats, making information storage and retrieval fast and efficient. It stores native content, including Multipurpose Internet Mail Extensions (MIME) content, directly in a .stm file. Additionally, with the installable file system (IFS), Exchange can be used as a file repository for any application. IFS make it possible to map Exchange folders and mailboxes as shared network drives. Finally, Exchange supports multiple public folder hierarchies. Each hierarchy, or tree, is stored in a public folder store. The default server installation includes one public folder store containing one public folder hierarchy. Figure 1 shows a graphical representation of the Exchange architecture, including the Extensible Storage Engine, Web Storage System, Exchange Interprocess Communication Layer (ExIPC), the IIS, and the underlying components.

Figure 1. Microsoft Exchange 2000 and 2003 Server Architecture



With the architecture and capabilities of Exchange 2000 and 2003 come concerns over security issues such as viruses penetrating and damaging the Exchange database. For this reason, Microsoft included the Microsoft virus-scanning API (see Figure 2), which allows antivirus vendors to perform virus scanning before attachments and contents can be saved or retrieved from the storage systems.

Figure 2. Microsoft Virus-Scanning API



With the Microsoft virus-scanning API available to antivirus vendors, products such as Trend Micro ScanMail for Microsoft Exchange can be constructed to provide high-speed scanning, higher performance, and scalable virus protection while also ensuring the integrity of the Information Store, Web Store database, and its contents.

THE MICROSOFT VIRUS-SCANNING API

Since the Microsoft Exchange 2000 Service Pack 1, Microsoft has provided a virus-scanning interface implemented at a low level in the Information Store. This interface allows a virus-scanning implementation with high performance and helps ensure that the scanning dynamic link libraries are loaded and run before any client can access a message or attachment.

The Microsoft virus-scanning API reduces problems associated with recognizing when a new mailbox has been added to the system and addresses scalability issues arising when a particular server has a large number of users/mailboxes.

THE TREND MICRO IMPLEMENTATION OF THE MICROSOFT VIRUS-SCANNING API 2.0

Trend Micro ScanMail is fully compatible with the Microsoft virus-scanning API 2.0. The virus-scanning API allows messages to be scanned once before delivery, rather than multiple times, determined by the number of mailboxes to which the message is delivered. Single instance scanning helps prevent a message from being rescanned when it is copied or passed from server to server. The advantages of the Trend Micro ScanMail implementation are:

- Enables the detection and elimination of auto-executing viruses by scanning email attachments and the message body before the email enters/leaves the Information Store.
- Provides protection for email passing to and from the Exchange 2000 server, including SMTP, MAPI, HTTP, POP3, and IMAP4 traffic. It also provides protection for users who are using the Installable File System (IFS) and Network News Transport Protocol (NNTP).
- Scans and blocks both inbound and outbound infected messages and attachments traveling through the Exchange 2000 server, even under heavy traffic loads. The scan methodology, developed in close collaboration with Microsoft, guarantees the integrity of the Information Store database, messages, and attachments, resulting in improved reliability of virus detection and cleaning.
- Provides manual and scheduled scanning of all attachments residing in the Web Store database.
- Scans in background mode all attachments in the Web Store database to help ensure that known viruses residing in the database will be removed.
- Provides multi-threaded and thread pooling capabilities that result in improved real-time performance and resource utilization on the Exchange 2000 server.

- Features single instance scanning (smart scanning) so that messages and attachments are scanned only once, regardless of how many servers, recipients, or senders receive the message.
- Provides full access to message properties, allowing notification, logging, and reporting of recipient, sender, and administrator information.

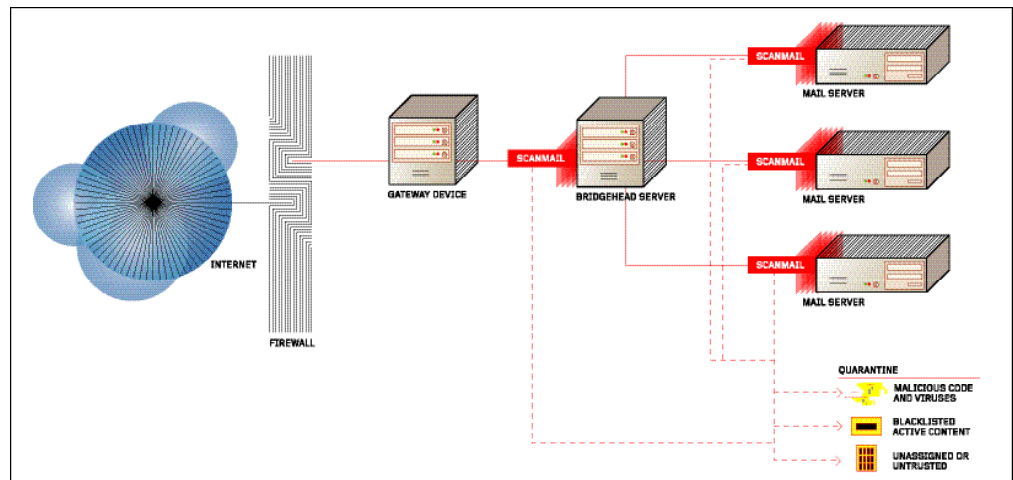
THE TREND MICRO IMPLEMENTATION OF THE MICROSOFT VIRUS SCANNING API 2.5

With Microsoft Exchange 2003, Microsoft provided an updated virus-scanning API version 2.5. This interface retains all existing functionalities provided by version 2.0. Trend Micro ScanMail is fully compatible with the Microsoft virus-scanning API 2.5 and offers the following additional features:

- Provides scanning of Multipurpose Internet Mail Extensions (MIME).
- Provides access to the message body.
- Implements new event log messages and performance monitoring counters for better administration.
- Includes sender and recipient addresses with the display names.
- Scans all outbound messages prior to sending them.
- Scans on an Exchange 2003 gateway machine because virus-scanning API is exposed on the transport level.

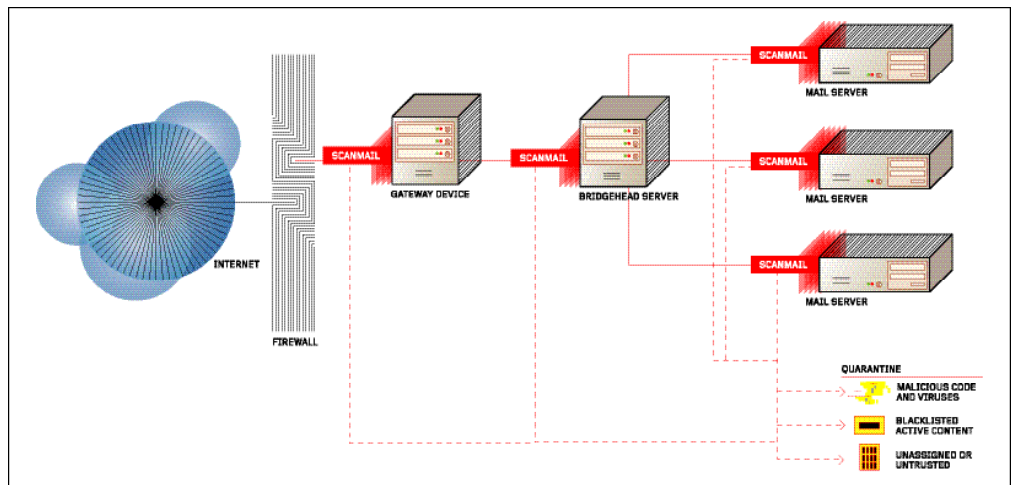
VIRUS PROTECTION ON THE MICROSOFT EXCHANGE 2003 GATEWAY/BRIDGEHEAD SERVER

Figure 3. Virus Protection on the Microsoft Exchange 2000/ Bridgehead Server



With Exchange 2000, virus scanning takes place on the mailbox server. (Figure 3). With Exchange 2003, and the Microsoft virus-scanning API 2.5, it is now possible to scan at the transport level (Figure 4). This allows antivirus companies to scan messages that will not be stored in the Information Store. It provides the capability of scanning messages that will be routed through the Exchange 2003 Gateway Server. This will prevent infected messages from entering into the network.

Figure 4. Virus Protection on the Microsoft Exchange Gateway/Bridgehead and Mailbox Servers



VIRUSES AND MICROSOFT EXCHANGE 2000 AND 2003 SERVERS

All messaging systems are vulnerable to virus attacks. Viruses spread when infected programs or data files are duplicated through server replication or by any other means in 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 irrelevant message, they can also be damaging enough to wipe out all data on the infected computer's hard drive or completely shut down the mail server through some form of denial of service.

In Exchange 2000 and 2003 Servers, viruses spread along with the files users share: through email attachments, public folders replication, database replication, installable file systems, and other Exchange compliant applications. With additional connectors and new protocols for Exchange servers, networks are open to a broader range of Internet information sources, greatly expanding the number of opportunities for viruses to enter the network.

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 the Nimda and CodeRed viruses proved, mixed-threat viruses can reside in the memory and infect a substantially greater number of users in a much shorter period of time. During a mixed-threat

virus attack, every minute counts. The network is at its most vulnerable before an antivirus vendor distributes an updated virus pattern.

Under such conditions, Trend Micro ScanMail for Microsoft Exchange, featuring Trend Micro™ Outbreak Prevention Services with Trend Micro Control Manager™, has the capability of blocking suspicious mail or attachments from entering the Exchange environment.

A virus in one client computer can proliferate throughout an organization via Exchange 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 that must be addressed, most industry experts agree that mixed-threat viruses have eclipsed the former in terms of frequency of occurrence and have become the preferred method for virus writers to create successful viruses.

DETECTING AND CLEANING VIRUSES IN THE EXCHANGE 2000 AND 2003 ENVIRONMENT

An effective antivirus strategy for the Exchange 2000 and 2003 environment should provide real-time scanning on all Information Store databases for viruses and other malicious content threats, including inappropriate and unsolicited content. This strategy should include scanning both the Exchange database (EDB) and Exchange streaming database (STM) levels, while at the same time continually scanning and cleaning the archive folders residing in the Information Store database by using either an on-demand or scheduled scan process.

Once an antivirus application disinfects the Information Store database, it must then prevent infected files from entering the server. Network administrators must pinpoint and protect all virus entry points within the Exchange 2000 and 2003 environment and enterprise network. Because many companies use an array of mismatched antivirus products, the “server leak” factor sometimes affects Exchange 2000 and 2003 servers. The resulting overlap of functions, gaps in virus protection, and different protocols used by competing antivirus packages prevent these products from working together to effectively protect Exchange 2000 and 2003 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 2000 and 2003 servers and the enterprise at large.

The “client leak” factor is created by the reverse situation in which desktop antivirus products are unable to scan Exchange email attachments, mailboxes or public folders, thereby allowing users to post or download infected files to Exchange 2000 and 2003 servers.

Monitoring all potential points where viruses can enter enterprise-computing environments and leak into Exchange servers is CPU-resource intensive. Additionally, such monitoring is extremely cumbersome for network administrators to manage. Fortunately, Trend Micro offers

an integrated antivirus strategy, including an Exchange 2000- and 2003-specific application, that provides easy-to-manage, resource-efficient protection from viruses.

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 and message bodies, helping eliminate viruses from Exchange 2000 and 2003 Servers before users can make copies of infected files.

AWARD-WINNING VIRUS-SCANNING TECHNOLOGY

Trend Micro ScanMail uses Trend Micro's award-winning 32-bit multi-threaded VSAPI scanning engine with Trend Micro MacroTrap™ and Trend Micro ScripTrap™ technology. ScanMail cleans both known viruses as well as unknown macro and script viruses. The patented Trend Micro scan engine minimizes the performance hits to servers during scanning, uses minimal server CPU resources, and enhances scanning speed and performance.

With the IntelliScan feature, ScanMail examines all files but scans only those file types that have the potential to be virus carriers. This helps reduce the burden on system resources. Using ActiveAction, ScanMail also identifies virus types and recommends actions to delete, clean, or quarantine them. The recommended actions are based on how each virus type infects a computer system or environment.

OUTBREAK PREVENTION SERVICES

The outbreak prevention phase is the critical time period after an outbreak has been identified and before a pattern file is available. During this crucial time, IT managers must endure a chaotic, time-consuming process of communication – often to global and decentralized groups within their organizations.

Prior to delivery of a pattern file, Trend Micro Outbreak Prevention Services provides attack specific information and outbreak prevention policies to help enterprises deflect, isolate and stem attacks. With Outbreak Prevention Services, policy recommendations can be centrally deployed to minimize coordination efforts and help ensure consistent application of policies throughout the network. This subscription-based service requires minimal up-front investment and provides enterprise-wide coordination and outbreak management via Trend Micro products that reside across critical points on the network including the Internet gateway, mail server, file server, caching server, client, remote and broadband user, and third-party enterprise firewalls. Policy recommendations delivered via Outbreak Prevention Services help IT managers

achieve accelerated response times for protecting against new viruses to contain outbreaks, minimize system damage, and prevent downtime.

Outbreak Prevention Services deliver notification of new threats as well as continuous and comprehensive updates on system status as an attack progresses. The timely delivery of detailed virus data, coupled with predefined, threat-specific action and scanning policies delivered immediately after a new threat is identified, allows enterprises to quickly contain viruses and prevent them from spreading.

Additionally, by centrally deploying and managing policy recommendations, Outbreak Prevention Services reduces the potential for miscommunication on application of policy. Instead, critical attack information is deployed consistently and as it is happening. By providing automatic or manual download and deployment of policies via Trend Micro Control Manager, Outbreak Prevention Services imports knowledge to critical access points on the network directly from experts at TrendLabs, Trend Micro's global security research and support network.

SPAM BLOCKING AND CONTENT FILTERING MANAGEMENT

The volume of unsolicited and inappropriate email that companies receive continues to reach new all-time highs. To address this problem, Trend Micro ScanMail includes email content filtering and spam blocking functions with its optional ScanMail eManager™ plug-in module. ScanMail and eManager integrate seamlessly 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 2000 and 2003 Servers. By employing a series of user-defined rules to evaluate the header and message text of incoming and outgoing email, as well as the message attachments, content filtering provides a means to evaluate and regulate email traffic on the basis of the message text itself.

Content filtering of inbound and outbound 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 innovative fuzzy logic. The eManager content filter reduces the number of unsolicited messages transported by the Exchange servers, improving its efficiency and ensuring that the messages received by the end user are valid.

QUARANTINE MANAGEMENT

Every organization has policies to quarantine suspicious messages and attachments. A tool to examine quarantined items to help avoid the accidental deletion of valid email is essential. Trend Micro ScanMail provides a user-friendly interface that allows administrators to easily view information in quarantined emails and attachments. Administrators can view or sort quarantined messages with details such as the "From" and "To" fields, quarantined attachment file name, file size, quarantine reasons, and whether the attachment has been resent or not. It also provides options to resend, forward, and delete the quarantined items or forward to an administrator mailbox.

In addition, ScanMail also allows administrators to configure scanning policies to quarantine and store attachments before a new pattern file is available. Once a new pattern file is released, administrators can scan quarantined messages with the new pattern.

MESSAGE PURGING

Mass-mailing viruses usually enter organizations via an infected email attachment. Most antivirus vendors can only remove the infected attachments and still deliver the empty messages to users' inboxes. This has the potential to increase help desk phone calls from panicked users who have received the empty messages. TrendMicro's Active Message Filter in Trend Micro ScanMail provides flexible configuration for inbound and outbound email to delete email with viruses, spam, and specified attachments before they are delivered to users. It can block mass-mailing viruses and remove all infected email and attachments, including zero byte attachments and email.

NOTIFICATION AND LOGGING

In a large enterprise environment it is important to receive notification when a virus is detected so that problem viruses can be effectively isolated and quarantined. Trend Micro 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 can send Outbreak Alert notifications whenever a high number of viruses attempt to pass through the Exchange 2000 and 2003 Servers or if a pre-selected number of viruses have not been cleaned within a few hours. ScanMail is designed to create logs of viruses attempting to pass through Exchange 2000 and

2003 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 helps cut the potential costs of a virus outbreak.

Administrators can access Trend Micro ScanMail services both on site and remotely through the 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 2000 and 2003 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. Administrators can customize the 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. 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, Trend Micro ScanMail can be configured to back up infected attachments before any action is taken.

CENTRALIZED MANAGEMENT

Threats from viruses and malicious code have become more frequent and sophisticated, irrevocably changing the e-business environment. New threats are constantly appearing and point solutions may prove insufficient. As a result, Trend Micro has developed a revolutionary approach to protecting customers from these threats. Trend Micro Control Manager offers a comprehensive approach to protecting the corporate environment. Administrators are provided with an enterprise wide picture of the network and the means of keeping the environment protected.

Trend Micro Control Manager does more than just manage Trend Micro's antivirus products. It can provide comprehensive outbreak policy and content security management for the enterprise. Industry competitors 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.

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

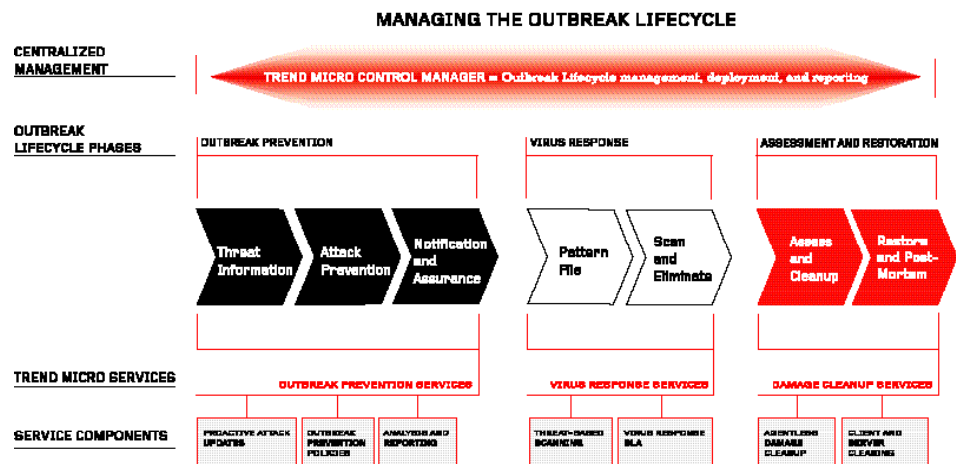
VIRUS RESPONSE SERVICE LEVEL AGREEMENT

Trend Micro’s Virus Response Service Level Agreement (SLA) also addresses the virus response phase of the outbreak lifecycle. A first for the antivirus industry, the Virus Response SLA provides customers with a penalty-backed guarantee that pattern files for detecting a new virus will be delivered within two hours from the time a virus case is submitted. Designed to deliver fast responses during the critical phases of an outbreak, the Virus Response SLA is further demonstration of Trend Micro’s strong commitment and high standards for service excellence.

TREND MICRO CONTROL MANAGER

Trend Micro Control Manager is the administration console that provides centralized management and enterprise-wide coordination for Trend Micro antivirus and content security products and services deployed throughout the network. A core component of the Enterprise Protection Strategy, Trend Micro Control Manager can help IT managers consistently enforce security policies throughout their organization, and respond quickly to the various stages of a virus outbreak— a key requirement for combating mixed-threat viruses that can appear in multiple areas of the network. Figure 4 illustrates the Enterprise Protection Strategy and the centralized management offered by the Trend Micro Control Manager.

Figure 5.
Trend Micro Enterprise
Protection Strategy



By managing antivirus and content security products and services through a single console, Trend Micro Control Manager can help IT managers consolidate information regarding virus events or unusual activity and create graphical reports for analysis and monitoring. Supported antivirus and content security products are organized into groups that can be remotely managed; servers can be configured simultaneously in groups or individually through replication. Product information and task functions are mirrored through Trend Micro Control Manager, making it fast to view and take control of newly installed products.

OUTBREAK COMMANDER

The Outbreak Commander console within Trend Micro Control Manager is designed to act as a central command center for deployment of services that deliver expertise and knowledge to specific points across the network. Outbreak Commander implements outbreak management-related tasks from a single interface, including the ability to automatically download and deploy policies set forth by Outbreak Prevention Services. Outbreak Commander organizes the vast capabilities included in the Trend Micro Enterprise Protection Strategy into three categories, as follows:

- Outbreak Prevention Services
- Virus Response Services
- Damage Cleanup Services

The Outbreak Commander console is centrally managed via the Trend Micro Control Manager and helps IT managers to convert into coherent and consistent global policies the extensive volume of discrete actions required when responding to potential threats.

TRENDLABS: A GLOBAL NETWORK OF SECURITY EXPERTISE

TrendLabs is Trend Micro's global network of security service centers. In addition to automatically notifying enterprises of new security threats, TrendLabs makes available a comprehensive body of security research, expertise, and knowledge that supplements Trend Micro antivirus software products. In addition to traditional support services offered by security vendors, TrendLabs delivers timely responses such as broadcasts of Medium and High Risk alert information to warn enterprises of newly identified security threats. TrendLabs also provides enterprise prevention and management of mixed-threat attacks and recommendations in advance of pattern file distribution, enabling enterprises to take immediate defensive action against threats. Once virus patterns are identified, TrendLabs delivers action policy templates for each Trend Micro product deployed on the network. Actions defined in these policy templates are threat-specific to help rapidly eliminate malicious code and repair damaged systems.

Among other benefits, IT managers can leverage the resource rich security knowledge and expertise of TrendLabs to avoid costly—and potentially disastrous—delays when seeking answers to urgent security questions. Through TrendLabs support services, IT managers have access to a vast global network of security experts 24x7, without hiring or developing such specialized skills in-house.

HOW TREND MICRO ENTERPRISE PROTECTION STRATEGY RESPONDS TO SECURITY THREATS

When a security threat is identified, TrendLabs automatically sends Medium and High Risk alert information and policy recommendations to the Trend Micro Control Manager, which resides on a central server at the enterprise. Trend Micro Control Manager can implement predefined activities (with the administrator's authorization) to contain the threat while minimizing the impact on non-threatened enterprise networking services. After installing the pattern files, the Trend Micro Control Manager can then rescan any suspect files and eliminate the virus before initiating damage assessment and cleanup procedures. After the incident, a comprehensive report is available to help assess enterprise-wide vulnerabilities as well as identify any systems where the cleanup efforts were not completed. In addition to providing enterprises with the industry's most thorough and up-to-date antivirus security protection, the Trend Micro Enterprise Protection Strategy is the first integrated security solution that completely eliminates the cost and complexity of software upgrades. All software is continuously upgraded as part of Trend Micro's online and real-time service program.

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 2000 and 2003 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.

Traditional desktop antivirus applications cannot provide full protection within the Microsoft Exchange 2000 and 2003 proprietary email/groupware messaging format. For more complete virus protection, enterprises must deploy email-specific scanning products such as Trend Micro ScanMail for Microsoft Exchange 2000 and 2003.

Trend Micro recommends the deployment of multiple tiers of virus protection. This multi-layer protection approach includes SMTP scanning on the gateway, virus protection for email and groupware servers, file server protection on all application/file sharing servers and a desktop antivirus software solution at the end-user level. These four layers of protection ensure the best virus protection in an organization.

ABOUT TREND MICRO

Trend Micro, Inc. is a leader in network antivirus and Internet content security software and services. The Tokyo-based corporation has business units worldwide. Trend Micro products are sold through corporate and value-added resellers, as well as managed service providers. For additional information and evaluation copies of all Trend Micro products, visit <http://www.trend-micro.com>.