


A background image showing a laptop on a desk with a speedometer overlay. The speedometer has a needle pointing towards the 40 mark, with numbers ranging from 10 to 70. The scene is set in a modern office environment with large windows in the background.

Layered Enterprise Messaging Security

Messaging Security 

 Protecting Business
Communications
throughout the Network

A Trend Micro White Paper | February 2007



CONTENT

I. EXECUTIVE SUMMARY.....	3
II. INTRODUCTION.....	3
III. MESSAGING THREATS.....	4
IV. LAYERED MESSAGING SECURITY.....	5
V. GATEWAY EMAIL SECURITY.....	7
VI. MAIL SERVER SECURITY.....	8
VII. EXTENDED MESSAGING SECURITY.....	9
VIII. TREND MICRO ADVANTAGE.....	10
IX. TREND MICRO MESSAGING SECURITY PRODUCTS.....	12
Gateway Security Products.....	12
Mail Server Security Products.....	12
Additional Messaging Security Products.....	13
Central Management.....	13
X. CONCLUSION.....	14

I. EXECUTIVE SUMMARY

While organizations are dependent on email as a primary communications channel, threats delivered by email are growing at an alarming rate. Not only are there a greater number of these threats than ever before, attacks and techniques are being combined to enhance their impact. In addition, enterprises are increasingly relying on other types of electronic communication, which further increase organizational risk. Savvy organizations are minimizing threats to their critical communications infrastructure by using interwoven layers of protection that spread throughout the network.

Layered protection strategies guard against combinations of internal and external threats, including spam, phishing, viruses, and other malware, as well as bulk mail attacks and threats to data security. However, the success of a layered strategy depends on its ability to leverage the most appropriate types of protection at the most effective points in the network. This paper briefly outlines the threats that imperil corporate email and then discusses the most effective ways of thwarting these malicious efforts at the email gateway and mail server. Given the increasingly blended nature of threats and growing use of additional electronic communication and collaboration tools, this paper also outlines complementary security that should be deployed beyond the email infrastructure. The paper concludes with a synopsis of the products that Trend Micro offers to provide a tightly interwoven network of protection.

Additional information about the threats introduced in this paper, as well as Trend Micro technologies and recommended offerings, can be found at the Trend Micro online messaging community at <http://messaging.security.trendmicro.com>

II. INTRODUCTION

Corporate email has become the primary means of business communication—making it crucial to protect this mission-critical electronic correspondence. At the same time, Instant Messaging and methods of collaboration, such as Microsoft SharePoint, are also expanding. Attacks can enter an organization through any of these methods of communication and at different points in the network. Confidential or inappropriate data can also leave the organization through the same channels. As a result, today's companies are increasingly looking for a tightly integrated solution that provides comprehensive messaging protection including compliance capabilities. They want this solution to be easy to deploy and manage, with support from a single, expert vendor.

An effective defense against both standalone and mixed-threat attacks utilizes multiple detection techniques and technologies in combination, which match or exceed threats in sophistication. Protection should also be deployed at different points within the network, reflective of the stage, nature, and characteristics of attacks that may be detected at each point.

Trend Micro recommends that most organizations begin with a layered approach to email security, combining gateway email security with mail server protection to provide a thorough defense against email threats. This layered email security can then be expanded through the addition of complementary security products to provide broader, comprehensive messaging security designed to encompass other methods of electronic communication.

III. MESSAGING THREATS

Today's increasingly interconnected organizations face more messaging threats than ever before—spam, viruses, phishing, spyware, bots, inappropriate content, and more. Not only are the number and types of threats increasing, but threats have become more sophisticated and often more targeted, insidious, and harmful to organizations. The unfortunate reality is that, with attacks primarily motivated by monetary gain, attackers are willing to invest more resources in their development.

Spammers, for example, continue to advance their techniques to bypass traditional anti-spam filters. Techniques such as randomization and embedded objects make the latest spam campaigns more difficult to detect than before. With the five-fold growth in spam over the last couple of years¹, companies continue to search for ways to improve spam detection. Effectively eliminating spam improves the overall efficiency of a company by enabling employees to quickly focus on the business-critical messages they receive and not waste time on spam.

Viruses have also shown dramatic evolution. Originally written by hackers seeking notoriety, today the main driver for virus writers is generally financial gain. For example, bot code is used to take over computers to later use them as zombies that send out spam and phishing emails with the intent to generate revenue. Viruses are also being used to disseminate code that captures confidential information and delivers it to the malicious party, often resulting in identity theft or loss of intellectual property. Inadvertently sending malicious content from within the infected company can be devastating to its reputation and erode its competitive advantage.

Phishing has traditionally been a consumer threat, where criminals pose as a legitimate company and use social engineering tricks to persuade recipients to divulge personal information. However, phishing has recently expanded into the corporate world with more targeted attacks called spear phishing. Using emails that appear to come from a source inside the company, such as the IT or accounting department, these attacks often seek to obtain confidential information that would provide access to the corporation's network, databases, or other protected resources.

Confidential information is also jeopardized by crimeware or spyware, such as key-logging Trojans and pharming code. Key-logging Trojans are inadvertently downloaded onto a victim's PC, where they record key strokes and other computer actions that can be sent back to the hacker. Pharming code is designed to misdirect the user to fraudulent Web sites where sensitive information can be captured, usually through DNS hijacking or poisoning.

Finally, bulk email attacks can also cause substantial damage to the organization. Distributed Denial of Service (DDoS) attacks bombard an organization with an extraordinarily large volume of emails designed to hog network resources. Bounce attacks spoof a legitimate company by inserting its domain as the sender of email, flooding that company's network when the receiving server bounces that email. In addition, these attacks can damage the reputation of the spoofed company, as it will appear as though it sent the email. Directory Harvest Attacks (DHA) attempt to glean lists of legitimate email addresses by sending high volumes of emails to randomly generated addresses with the company domain. These lists of valid email addresses can either be sold to other malicious parties or used by the harvesters themselves for any number of future targeted attacks.

¹ Ferris *The Global Economic Impact of Spam*, 2005. February 2005

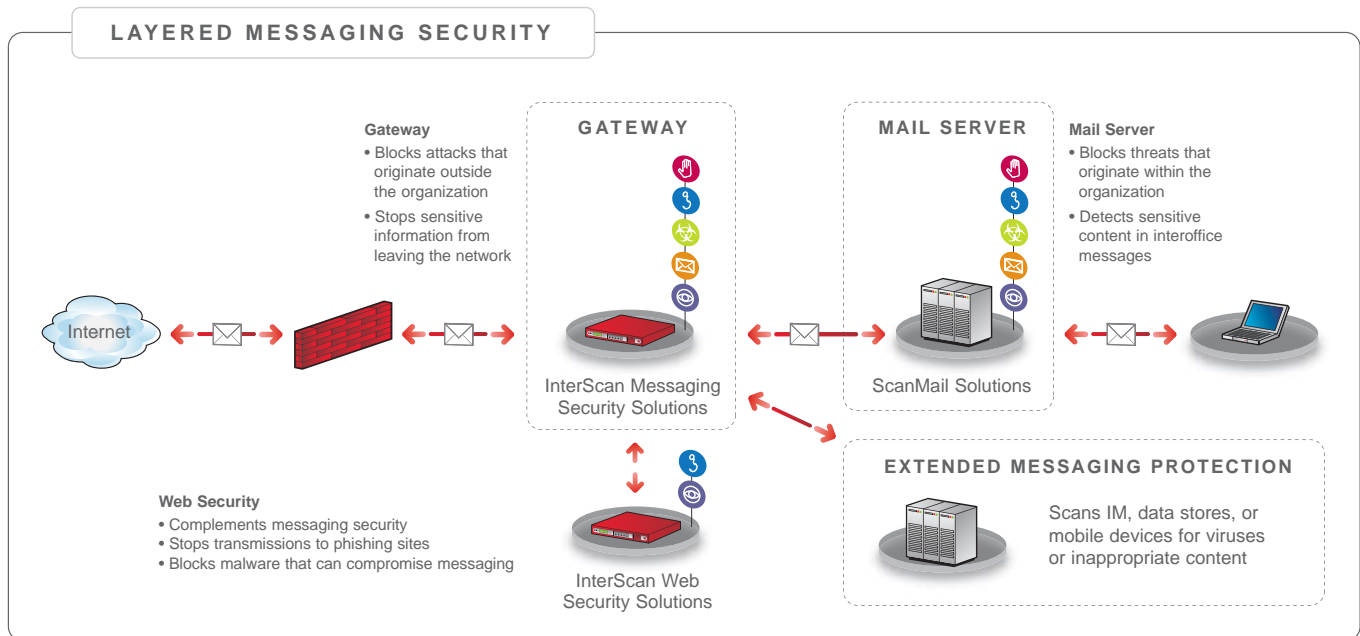
LAYERED ENTERPRISE MESSAGING SECURITY

While many organizations are primarily focused on preventing these inbound threats, there is also an increasing recognition of the need for messaging security to filter outbound messages to enforce regulatory compliance, implement corporate governance, and prevent the loss of confidential information.

Clearly, there are an increasing number of threats, often combining multiple tactics into more potent mixed-threat attacks. As one example, spam Trojans can spread through the network and embed malware to hijack PCs and create spam zombies which can initiate other email-based attacks. As another, spam campaigns can be used to broadly distribute spyware, often in the guise of trusted executables like news clips. Once distributed through spam, the spyware then reaches out to malicious Web sites to download additional malicious code. In light of this growing complexity of threats, an integrated, layered defense is required to provide comprehensive threat protection.

IV. LAYERED MESSAGING SECURITY

Given the wide range, varied nature, and enhanced sophistication of today's threats, point products are no longer an effective means of protecting an organization's critical business communications. Trend Micro has strategically placed its advanced messaging security technologies in products that address the unique needs of particular points in the network. Trend Micro helps organizations deploy the right mix of products and technologies, at the proper points of their IT infrastructure, to effectively and efficiently mitigate the business risks arising from various messaging threats.



TREND MICRO NETWORK SECURITY SOLUTIONS



LAYERED ENTERPRISE MESSAGING SECURITY

Trend Micro delivers two core layers of email protection, one at the gateway and the other at the mail server. Each provides specific advantages to protecting email. The gateway is the earliest and most efficient point to stop attacks that originate outside of the organization, and the only point at which incoming spam, phishing, and bulk email attacks can be completely blocked from entering the network. It is also the last opportunity to detect and stop sensitive information from leaving the network. Accordingly, Trend Micro has deployed specific external-facing technologies to best address threat prevention at the gateway, including reputation services, anti-spam and antivirus scanning engines, as well as content filtering.

At the same time, there are many threats that originate within the organization and are most appropriately addressed at the mail server level. This level is the only central inspection point for internal communications of most organizations, the first opportunity to look at outgoing email, and often the place at which storage, archiving, and regulatory requirements begin. Examples of email threats inside the organization include viruses that may have entered via mobile or remote PCs, spam generated by bots hosted by unsuspecting users, and sensitive or inappropriate content in messages from employees. Further, server-based protection uses the latest threat intelligence to inspect incoming messages as they flow through the email infrastructure as well as cleaning the mail store, where messages and their malicious code or content may reside for hours, days, weeks, or longer.

In addition to these two layers of email security, Trend Micro offers extended messaging protection through complementary products to provide comprehensive messaging security across the network. Notably, Web security products can be used to block access to, or malicious code from, hazardous websites whose URLs may have been delivered to unsuspecting users in email. Other products can be used to scan additional electronic communications such as IM or data stores—such as those in SharePoint™—for inbound viruses or outbound sensitive content. Mobile security products help protect increasingly vulnerable mobile devices, such as smartphones and wireless handhelds, from messaging threats.

This layered approach helps organizations safeguard the network while ensuring the availability of critical communications. The following sections will discuss the technologies recommended at each of these layers in greater detail, with a brief mention of the threats driving the need for these technologies.

V. GATEWAY EMAIL SECURITY

Protection at the messaging gateway is critical because it is the most common point of entry for Internet-based attacks, which tend to originate outside of the organization. Technologies to block spam, viruses, Trojans, worms, phishing, spyware, bounce mail attacks, DHA, and DDoS attacks are logically deployed at the gateway to stop the incursion of these threats throughout the network. At the same time, the gateway is the last point of protection for outbound email, which provides a final opportunity to prevent threats from leaving the organization, maintaining the reputation of the organization as a sender of safe and appropriate email.

➔ **Anti-spam**

Trend Micro's reputation services are a proven method of stopping large quantities of unwanted email sent by known sources of spam and other email threats and are only available in the gateway email security products. Network Reputation Services apply global and dynamic services and can stop up to 80% of spam and phishing emails before they enter the gateway. The dynamic service can even block zombies and botnets when they first emerge. Patent-pending IP Profiler technology provides customer-specific reputation services by letting organizations set threat thresholds that are applied to the organization's email traffic. The anti-spam composite engine provides content-based message inspection at the gateway to keep any remaining spam or phishing emails off of the mail server and out of the inbox.

➔ **Antivirus**

Deploying Trend Micro's award-winning antivirus scanning engine at the gateway is particularly effective because it is a central point to efficiently block viruses before they spread into and throughout the network. In addition, IntelliTrap, one of Trend Micro's approaches to zero-day protection can be deployed to catch new viruses and variants even faster. This technology focuses on the tools used to hide viruses and not the virus code itself, stopping viruses without having to wait until a pattern file is deployed. Anti-spyware is also applied at the gateway to stop targeted spyware attacks that are sent via email.

➔ **Anti-phishing**

Because phishing attacks originate from external senders seeking to ferret out confidential personal or corporate information from employees, anti-phishing protection is also most effectively applied at the gateway. Trend Micro protects against phishing attacks with reputation services to stop known senders of phishing emails and a composite engine that employs phishing signatures and anti-phishing heuristics. Further, antivirus scanning prevents the download of crimeware sent via email, which can steal confidential information. These types of email-based protections are complemented by Web security at the gateway, which stops the malicious transmission of data to known phishing-related sites and prevents the download of key-logging Trojans and pharming crimeware.

➔ **DHA and Bounce Mail Attack Safeguards**

By their very nature, volume based attacks target the connection-level operation of the email gateway, making the gateway the only place where these attacks can be blocked. Trend Micro IP Profiler creates a firewall against DHA and bounce mail attacks.

➔ **Data Privacy and Protection**

The gateway is the last point at which the content in emails and attachments can be inspected before leaving the company. Ensuring that confidential information remains within the corporation helps enforce compliance, meet internal standards, and prevent leakage of sensitive information. Trend Micro content filtering provides flexible policy implementation to meet these needs.

As shown, the email gateway is the only point at which many email threats can be blocked from even entering the network. It is the most efficient place to stop threats before they can spread to other points in the network, preventing potential damage. The gateway is also the last point of inspection for content filtering, which is critical for maintaining data privacy and protection.

VI. MAIL SERVER SECURITY

While gateway protection is particularly effective in stopping external threats at their primary entry point into the network, the mail server is also a crucial line of defense for companies. As the central routing point for internal communications, the mail server is the best place to stop viruses, spam and inappropriate content that may be sent between employees, especially remote users logging back into the network. As the first hop for outgoing email, the mail server is also the most efficient point for stopping threats and confidential information that may have been improperly destined for external recipients. At the same time, mail server security provides the only opportunity to continue inspecting incoming traffic for unwanted messages and malicious code as it passes through the email infrastructure or resides in the mail store.

➔ **Antivirus**

Deploying Trend Micro's segment-leading scan engine at the mail server not only ensures that internal email remains free of viruses, but it also prevents outgoing email containing malicious code from being inadvertently sent to customer or business partners. These risks often originate from mobile PCs that may become infected or hijacked when used outside of the corporate network log back into the network and resume email communications. Supplemental inspection of incoming email, using the latest threat intelligence, continues to protect against viruses, especially as they reside in the message store for an extended period of time. IntelliTrap may also be deployed at the mail server for zero-day protection.

➔ **Data Privacy and Protection**

Trend Micro's advanced content filtering is best deployed at the mail server to intercept sensitive information at the point where archiving, review, and other compliance obligations generally begin. Additionally, the mail server is generally the only place to detect offensive content sent between employees—a potential hazard that could lead to a hostile work environment and related legal costs, penalties, and settlements. Finally, mail server security can detect sensitive information within interoffice email, including data that is meant to be limited to particular departments or individuals within the organization, such as CEO memos within an executive team or financial information within a reporting group.

➔ **Anti-spam**

Anti-spam protection can also be valuable at the mail server, especially to detect zombie machines or other sources of spam originating within the organization. Appearing to come from an organization's employees, these outgoing spam emails can diminish a company's brand in the minds of customers, erode partner relationships, and even result in an organization being added to a DNS block list, impairing the delivery of legitimate mail. Trend Micro employs the anti-spam composite engine in its mail server security products to safeguard against these threats.

Even with highly effective protection at the email gateway, organizations must also implement security at the mail server to protect against threats that originate inside the organization and implement a layered defense against external attacks.

VII. EXTENDED MESSAGING SECURITY

While email is the primary means of communication for organizations today, there is growing awareness of the need to secure additional electronic communication and collaboration tools. This need for additional security mirrors the growth in use, attacks, and often compliance obligations associated with these tools. In particular, Instant Messaging is one of the fastest growing methods of communication today and collaboration solutions are also becoming more prevalent. Accordingly, for customers using a Microsoft network environment, Trend Micro has extended its proven security technologies to protect these additional messaging and collaboration tools, creating a “better together” approach to security. Trend Micro’s industry-leading antivirus engine and advanced content filtering protect Microsoft Office Live Communications Server and SharePoint Portal Server, stopping viruses and other malicious code as well as inappropriate content.

Data-centric mobile devices are also a major target for malware attacks as well as Short Message Service (SMS) text message spam. Trend Micro extends critical protection against viruses, worms, Trojans, and SMS spam to smartphones and wireless handhelds.

At the same time, gateway and mail server protection can be supplemented with scanning on the PC where messaging clients like Outlook reside, further ensuring comprehensive, layered protection.

➤ **Antivirus**

Deployment of leading antivirus scanning on IM servers secures this external-facing communication tool from viruses and other malware. Virus scanning on other collaboration servers and storage protects critical IT infrastructure and important business data from infection, corruption, and theft. Also, as the number of data-centric mobile devices grows, they become a more attractive target for malware, making it important to secure these devices with antivirus protection. Inspection of Outlook files on the client can provide a final level of protection from email-borne attacks.

➤ **Anti-spam**

With the prevalent use of mobile devices, flexible anti-spam technology is required to stop SMS text message spam sent directly to mobile devices such as smartphones and wireless handhelds. Trend Micro applies technologies such as an approved sender list, a blocked sender list, and the ability to block numberless SMS messages.

➤ **Data Privacy and Protection**

Data privacy and protection technologies can also be deployed on Microsoft-based enterprise IM and collaboration servers to minimize the risk of data loss and, in many cases, to comply with regulations. Further, preventing improper use of communications can reduce the potential costs of fines and settlements, lawsuits, negative public relations, loss of competitive advantage, and more.

VIII. TREND MICRO ADVANTAGE

WHY ONE VENDOR

The legacy approach to email security was to use separate vendor products, both at different points in the network and to combat different standalone threats. For example, a customer might purchase an antivirus product for the gateway from one vendor, purchase another antivirus product for the mail server from a separate vendor, and buy a gateway-based anti-spam solution from yet another vendor. Customers believed that by layering solutions from various vendors, they would increase the effectiveness of their protection.

This approach has since changed. The wide range of threats and their increasingly blended nature has resulted in a dramatic increase in the number of products required to work together as part of an integrated solution. As a result, more and more organizations are moving towards purchasing one solution from a single vendor that can provide best-of-breed, coordinated protection across multiple threats, layers, and communication channels. Today, buying protection from multiple vendors does not guarantee increased security. Unfortunately, it does require heavy management to configure, deploy, manage, and maintain as well as carrying a hefty price tag.

In an IDC Executive Brief, the IDC research firm recommended a single-vendor antivirus strategy as early as 2002. Some of the key benefits of the single-vendor approach include lower Total Cost of Ownership, simplified administration, ease of update, response to virus outbreaks (if an infection occurs, it is more easily traced and resolved in a single-vendor implementation), and support.

IDC continues to support this perspective. A 2006 IDC report states,

IDC believes that often point solutions are not an effective approach to building a secure enterprise infrastructure. If these point solutions and their accompanying support mechanisms are not completely compatible, the overall effectiveness and potential added cost of supporting and maintaining these independent systems are, to some extent, diverting valuable and limited IT resources...

When respondents in our survey were asked about the benefits of having an integrated security architecture with a single vendor supporting them, common responses were "It is much more efficient to be able to call a single number and discuss a complex critical security issue with someone you have developed a trusted relationship with and who understands your architecture and configuration" and "Generally we get the rapid support we need when it is crucial that we have all the answers."²

The key goal today is not to seek out emerging technologies from different vendors of point solutions, but rather to standardize on a single, proven vendor that provides effective protection across threats, layers, and protocols.

² IDC white paper sponsored by Trend Micro, *Secure Enterprise Threat Management through an Integrated Security Framework*. Doc. #203005 August 2006.

LAYERED ENTERPRISE MESSAGING SECURITY

WHY TREND MICRO

Trend Micro Incorporated is a global leader in network antivirus and Internet content security software, appliances, and services. Founded in 1988, Trend Micro focuses on providing organizations with a comprehensive approach to managing the threat lifecycle and minimizing the impact of network viruses, spam, spyware, inappropriate content, and other threats to productivity and information. With Trend Micro organizations can be assured that they are receiving mature, reliable solutions designed to protect their network environments.

Advantages to Trend Micro's layered messaging security

- Trend Micro offers trusted technologies to protect business-critical email, minimizing impact on systems and staff.
- Trend Micro's security is based on in-house technologies, ensuring timely and coordinated protection. The threat scanning engines receive timely updates, outbreak prevention policies are typically available within 15 minutes of virus confirmation, and reputation services reflect real-time activity. All of these technologies are backed by superior in-house support and information services.
- Trend Micro pioneered gateway antivirus security and continues to be the industry leader. According to IDC, Trend Micro has been the holder of the top global market share in Internet gateway antivirus for six consecutive years.³
- Trend Micro's is a market leader in mail server antivirus and ScanMail™ for Exchange™ is proven to introduce the lowest overhead to the system.⁴
- Trend Micro products are powered by TrendLabssm, a global network of research centers committed to constant threat surveillance and attack prevention. With accurate, real-time data, TrendLabs delivers more effective and timely security measures designed to detect, pre-empt, and eliminate attacks.
- Each of Trend Micro messaging products provides a single, centrally managed, Web-based administrative console to provide easy management.
- Trend Micro security expertise extends beyond messaging protection to offer broader, layered network security.

³ IDC, *Worldwide Antivirus 2006–2010 Forecast Update and 2005 Vendor Analysis*, Doc #204715, Dec 2006

⁴ Veritest report: *Performance Evaluation of Anti-Virus Solutions for Microsoft Exchange Server 2003 Final Report*, 07 September 2006

IX. TREND MICRO MESSAGING SECURITY PRODUCTS

GATEWAY SECURITY PRODUCTS

- ➔ **Trend Micro InterScan™ Messaging Security solutions** integrate antivirus, anti-spyware, anti-spam, anti-phishing, and content filtering for complete email protection. Offered on software, an appliance, or a hosted service, this protection is delivered on a single, centrally managed platform for easy, comprehensive email security at the gateway. The solutions offer the same complete protection, allowing customers to select the form factor that best fits their network environment.
 - **InterScan Messaging Security Suite** is a flexible software solution that allows enterprises to install the product on their own hardware and on multiple machines. The software is available on the leading operating systems: Windows™, Linux™, and Solaris™.
 - **InterScan Messaging Security Appliance** provides easy deployment with preconfigured software. This high-throughput, redundant appliance is optimized for security and performance.
 - **InterScan Messaging Host Security** is quickly deployed by simply redirecting the MX record. This hosted service keeps email threats off of the network, providing added security and bandwidth. No gateway email security hardware or software is needed, reducing infrastructure, costs, and administration.

Although Trend Micro strongly recommends comprehensive, layered messaging security, some gateway email security components are also available separately.

- ➔ **Spam Prevention Solution** blocks spam and phishing by combining global, dynamic, and customer-specific reputation services with an anti-spam composite engine. The solution efficiently filters SMTP/POP3 traffic to preserve network bandwidth, reduce infrastructure costs, and keep the network safe.
- ➔ **Network Reputation Services** verify IP addresses of incoming email against the world's largest, most trusted reputation database and use a dynamic reputation service to identify new spam and phishing sources as they first emerge. These services are offered either on-site through an MTA modification that conducts DNS queries or through a hosted service.

Trend Micro gateway Web security solutions supplement the protection provided at the messaging gateway.

InterScan™ Web Security solutions are offered on both software and an appliance. These products complement email security by scanning Web mail for malware and by providing additional protection against phishing and other threats to the loss of confidential information.

MAIL SERVER SECURITY PRODUCTS

- ➔ **Trend Micro ScanMail™ Suite solutions** run natively on either Microsoft™ Exchange™ or IBM™ Lotus™ Domino™, providing industry-leading antivirus and anti-spam scan engine technology as well as flexible content filtering. The solutions offer broad operating system support and a single, central management console that enable organizations to easily configure, deploy, and administer highly effective protection with minimal impact on email systems and staff. The solution's optimized performance, seamless integration with mail server products, and its superior platform support further differentiate ScanMail Suite from other established mail server security products.
 - **ScanMail™ Suite for Exchange** is optimized for multiple Exchange platforms (2000, 2003 and 2007) and is tightly integrated with an organization's Microsoft IT infrastructure—the solution leverages Microsoft SMS for remote silent install, integrates within Microsoft Operations Manager for simplified monitoring, and more. The suite offers full support for clustering and performance optimizations that have traditionally ensured in the lowest impact to systems among leading vendors.⁵

LAYERED ENTERPRISE MESSAGING SECURITY

- **ScanMail™ Suite for Lotus™ Domino™** runs natively on IBM Lotus Domino platforms and provides the broadest platform support, including Windows, Linux, Solaris and IBM zOS™. Specifically designed for use as a Domino server application and optimized for high performance, the solution also offers remote management as well as the choice to configure either servers or server groups.

ADDITIONAL MESSAGING SECURITY PRODUCTS

- ➔ **IM Security for Microsoft Live Communications Server** deploys the industry's leading antivirus engine directly on the IM server to prevent malicious code from utilizing instant messaging infrastructure as a vector of attack. Advanced content filtering also inspects communications to ensure content compliance.
- ➔ **PortalProtect™** further expands protection to the collaboration environment, ensuring the security and availability of business-critical information within Microsoft SharePoint. The solution stops malicious code from interrupting server operation or jeopardizing valuable company data. Advanced content filtering safeguards sensitive information.
- ➔ **Trend Micro Mobile Security** helps protect data-centric mobile devices, such as smartphones and wireless handhelds, from the evolving threats of viruses and SMS text message spam. Central management automates deployment of updates to handsets easing the administrative burden.
- ➔ **OfficeScan™** complements the layered messaging approach by scanning the desktop for viruses. This includes scanning Outlook—the final endpoint for emails.

CENTRAL MANAGEMENT

- ➔ **Trend Micro Control Manager™** acts as a central command center for deployment of Trend Micro's threat-specific expertise across the network. Centralized management capabilities are designed to provide a unified view of enterprise-wide security and enable administrators to configure, monitor, and maintain Trend Micro products and services installed on the network from a single console. By consistently and simultaneously deploying policies to Trend Micro products and services, Trend Micro Control Manager helps ensure the enforcement of proactive threat prevention policies.
- ➔ **Outbreak Prevention Services** applies outbreak policies within an average of 15 minutes. These policies prevent or contain an outbreak until a pattern file can be deployed. This technology serves as an “early warning” approach and protects companies while pattern files are being developed. These services can be used along with other Trend Micro products.

Trend Micro's layered messaging security approach safeguards enterprise email and other digital messaging throughout the network. However, Trend Micro goes beyond messaging protection to provide holistic network security through Trend Micro™ Enterprise Protection Strategy. The security framework provided through this strategy combines multiple layers of products and services for intelligent, comprehensive protection against known and unknown threats. The framework includes innovative new solutions that monitor customer-specific networks and accurately detect unknown threats in real time. Tightly-integrated, centrally-managed security enables seamless inter-product collaboration to guard every network endpoint.

⁵ Veritest report: Performance Evaluation of Anti-Virus Solutions for Microsoft Exchange Server 2003 Final Report, 07 September 2006

X. CONCLUSION

With Trend Micro, organizations can be assured that they are receiving comprehensive, industry-leading messaging security to reduce the very real and substantial business risks posed by today's messaging-related threats. TrendLabs provides a global network of experts that continually researches the evolution of messaging threats and creates innovative approaches to combating them. The resulting technologies are strategically placed in products to provide the best available threat prevention at the most appropriate place in the network. When messaging security products are combined, organizations achieve a highly effective layered defense that provides comprehensive protection for email and other electronic communications.

This layered approach helps enterprises maintain the security and availability of critical messaging and other IT infrastructure. This minimizes administration, improves employee productivity, and reduces infrastructure cost. At the same time, Trend Micro helps organizations mitigate the risk of data loss or misuse, reducing potentially adverse impacts. In particular, securing private data helps prevent legal or regulatory fines or settlements; erosion of customers, trust, or brand; negative public relations; and loss of competitive advantage.

Organizations may choose comprehensive messaging security from day one or simply start with targeted protection and expand over time as organizational needs grow. Trend Micro also goes beyond messaging security to offer broader, comprehensive network security through its Enterprise Protection Strategy. With this security framework, organizations can guard their networks from gateway-through-desktop against all types of threats to electronic data with minimal enterprise-wide cost.

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014
USA toll free: 1+800-228-5651
phone: 1+408-257-1500
fax: 1+408-257-2003
www.trendmicro.com

