

A background image showing a laptop on a desk with a speedometer overlay. The speedometer has numbers from 0 to 70 and a needle pointing towards 40. The scene is dimly lit, suggesting an office or laboratory environment.

Real-Time Communications and Real-World Threats

Driving the Need for Real-Time Protection

Trend Micro, Incorporated 



A closer look at today's deceptive threats targeting communication and collaboration systems and the security you need to stop them

A Trend Micro White Paper | September 2008

➔ TABLE OF CONTENTS

REAL-TIME COMMUNICATION AND COLLABORATION.....	3
REAL-TIME CONNECTIONS ENABLE REAL-TIME ATTACKS.....	4
REAL WORLD THREATS... AND THE SECURITY YOU NEED TO STOP THEM.....	4
EMAIL THREATS.....	4
SUBPOENA: TARGETED SOCIAL ENGINEERING LEVERAGING THE WEB.....	5
NUWAR: A MULTI-COMPONENT EMAIL THREAT.....	6
INSTANT MESSAGING THREATS.....	7
WORM_IRCBOT: MALWARE TARGETING SOCIAL NETWORKING.....	7
SKYPE LINKS: TAILORED MALWARE OVER THE WEB.....	8
COLLABORATION THREATS.....	9
MICROSOFT OFFICE EXPLOITS: MALWARE PROPAGATION VIA COMMON CONTENT.....	9
IFRAME: INSIDIOUS HIJACKING OF LEGITIMATE SITES.....	10
LESSONS TO LEARN FROM REAL-WORLD THREATS.....	11
THE WILD CARD: SOCIAL ENGINEERING.....	11
THE FIVE ESSENTIALS.....	12
THE POWER OF FOUR.....	13

Real-Time Communications and Real-World Threats Driving the Need for Real-Time Protections

REAL-TIME COMMUNICATION AND COLLABORATION

In the past, it was considered a sound business practice to keep partners and customers at an arms length. But companies today are reaping benefits by bringing everyone closer together. And the latest communication and collaboration solutions from Microsoft, IBM, and others empower organizations to do just that. Email, instant messaging, and collaboration systems connect employees, contractors, affiliates, partners, and existing customers. Together, these tools build stronger business ties, improve productivity, and increase innovation.

Of these systems, email is arguably the most indispensable, mission-critical business tool. But companies today are also adding instant messaging to the mix—for even faster real-time interactivity. Gartner predicts that 95% of all businesses will adopt an enterprise-wide IM solution by 2010.¹ Likewise, many organizations are deploying collaboration systems to connect people, processes, and information. Portals, wikis, blogs, and rich content repositories provide users with a wealth of resources at their fingertips.



¹ Source: Gartner Research. MarketScope for Instant Messaging, Document #G00147732, April 2007.

Real-Time Communications and Real-World Threats Driving the Need for Real-Time Protections

REAL-TIME CONNECTIONS ENABLE REAL-TIME ATTACKS

These instant connections are essential for your company to keep pace with the speed of business today, but they also increase your security risk by opening new pathways for cybercriminals to enter your network. In this real-time environment, attackers can spread malware, hijack your systems, and steal your data—in a split second. A single data loss incident can damage your reputation and customer trust, costing you millions. Just ask TJ Maxx. In 2007 when customer credit card records were stolen over the web, the company reported an initial \$5M charge to investigate and contain the breach², and more recently, settlement agreements of up to \$41M³ and \$24M with Visa and MasterCard customers alone.⁴

Email remains the most popular attack vector, with unwanted spam and malicious messages comprising roughly 90% of all email. Increasingly sophisticated, these threats often blend multiple types of malware and morphing techniques within multi-staged and serial attacks. Many leverage social engineering techniques designed to deceive even the most aware users. With the difficult challenge of constantly evolving threats, most organizations have reported that managing email security is their highest concern in regard to unified communications and messaging.⁵

At the same time, an increasing number of attacks are targeting collaboration portals and instant messaging, where activities like file sharing, chat, blog posting, and other Web 2.0 interactions elevate the risk of exposure. As Gartner Research warns, “The same Web 2.0 characteristics that enable productivity and collaboration also make the Web 2.0 ecosystem prone to successful attack and theft.”⁶ Many of the schemes exploit user behaviors and tendencies toward greater trust, more downloads, and the mix of business and personal communications. Worst of all, real-time connections enable these threats to strike faster than ever.

REAL WORLD THREATS... AND THE SECURITY YOU NEED TO STOP THEM

The average lifespan of a single piece of malware is just hours. But its impact can be felt for years. Let's take a look at general trends and some real-life attacks that offer valuable insight into the types of security needed to protect your communication and collaboration systems.

EMAIL THREATS

In the past few years, TrendLabs has seen exponential growth in the amount of spam, now accounting for as much as 80-90% of an organization's total email volume. More disturbingly, a growing percentage of that spam, now an estimated 15%, contains links to malicious websites that host malware. Following this same trend, email-borne malware is reaching out to malicious sites to execute additional malware or transmit stolen data. Such attacks fall into the category of “web threats,” a category that has grown more than 1,500% over the past two years.

In addition to leveraging the web, many attacks are becoming much more targeted, focusing on a single organization or even job title! The following examples, illustrate many of the latest techniques used in email threats.

² Source: The TJX Companies, Inc. Press Release: The TJX Companies, Inc. Reports Strong Fiscal Year 2007 Results; Fourth Quarter Results Above Expectations, February 21, 2007.

³ Source: The TJX Companies, Inc. Press Release: The TJX Companies, Inc. Announces Settlement Agreement with Visa U.S.A. Inc. and Visa Inc.; Estimated Costs Already Reflected in Previously Announced Charge, November 30, 2007.

⁴ Source: The TJX Companies, Inc. Press Release: The TJX Companies, Inc. Announces Settlement Agreement with MasterCard; Estimated Costs Already Reflected in Previously Announced Reserve, April 2, 2008.

⁵ Source: Osterman Research. Unified Communications/Messaging Trends, 2008-2011, June 2008.

⁶ Source: Gartner Research. Security Features Should be Built into Web 2.0 Applications, Document #G00153433. March 2008.

Real-Time Communications and Real-World Threats Driving the Need for Real-Time Protections

SUBPOENA: TARGETED SOCIAL ENGINEERING LEVERAGING THE WEB

Subpoena illustrates the hunger for valuable corporate information and highlights the sophistication of attacks targeting relatively small groups of users—in this case, North American CEOs. First, the cybercriminals obtained a targeted list of corporate executives, identified a compelling concern—a potential subpoena—and then created tailored websites mirroring those of the U.S. judicial systems in order to trick recipients into downloading a Trojan designed to steal information over time. More recently, a similar targeted attack duped victims under the guise of [tax petitions](#).

How Subpoena Works

Targeted CEOs receive an email message informing them they are wanted in court and that related court documents can be obtained by following the link provided. The message itself is compelling due to the following social engineering techniques:

- The sender uses an email address with the domain uscourts.com (the real domain is uscourts.org!)
- The email message accurately includes the target's name, company, and phone number
- When the link is clicked, the browser opens a site that closely mirrors the official U.S. Courts site
- The spoofed site offers a file download that uses the legitimate Adobe PDF icon, but it is actually TROJ_AGENT.AMAL



Once installed, the malware mines data from the infected PC and sends it to external IP addresses. Of note, a few days after the initial threat was identified, researchers found the same fake U.S. Courts site, using a different URL.

Defending against Subpoena

Because of its targeted nature, use of the web to host and deliver all malware, and its shifting site location, the following protections are needed above and beyond traditional antivirus scanning:

- Proactive protection like in-the-cloud email reputation
- Real-time embedded URL inspection at the email gateway and server
- Web threat protection on the endpoint to stop users from accessing the site, in the event emails reach the end user
- Strong antivirus on the endpoint to block downloads should recipients reach the bogus site and attempt to download the documents

Read the complete Trend Micro report on [Subpoena Attack](#). >>

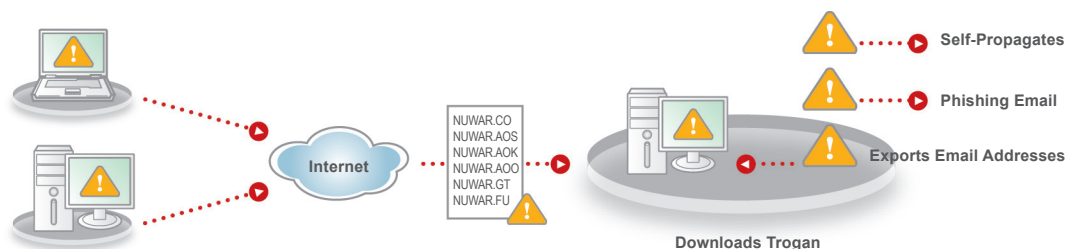
Real-Time Communications and Real-World Threats Driving the Need for Real-Time Protections

NUWAR: A MULTI-COMPONENT EMAIL THREAT

In various forms, NUWAR can be accurately called a worm, Trojan, rootkit, spyware, spam, and web threat. It infects machines to launch spam attacks for financial gain and/or mass-delivery of malicious code. More recent NUWAR attacks harvested email addresses from DHTML files on the infected PC to self-propagate via webmail. NUWAR also masqueraded as electronic greeting cards for Valentine's Day, to increase its chances of success. A particularly profitable use is the so-called "pump and dump" scheme, designed to artificially inflate a penny stock. This type of attack accounts for as much as 25% of all spam today.

How NUWAR Works

Spam emails sent by NUWAR also carry the NUWAR malware itself, so the number of infected machines can grow exponentially unless effective defenses are in place. Trend Micro detected more than 40 variants of NUWAR in a two-week period when it was first released. These variants present different digital signatures to defeat security programs that rely exclusively on signature-based defenses. In addition, the NUWAR Trojan downloader can install new variants—so in effect, NUWAR contains its own upgrade engine! While first seen in 2006, new versions of NUWAR continue to top the charts in terms of malware submission to TrendLabs—ranking 9th overall in April of 2008.



Defending against NUWAR

Due to NUWAR's complex, blended nature and many variants, an effective defense requires:

- Signature-independent zero-day protections to detect variants at the email gateway (for incoming attacks) and mail server (for internal propagation)
- Effective antispam, especially proactive email reputation to stop blended threats
- Dedicated spyware protection and a powerful antivirus scan engine to stop Trojan downloaders at every point starting with the email gateway on through to the endpoints
- Anti-bot technology to detect successful attacks that have hijacked endpoints

Read the complete Trend Micro report on **NUWAR** >>

Real-Time Communications and Real-World Threats Driving the Need for Real-Time Protections

INSTANT MESSAGING THREATS

While analysts predict that nearly all companies will adopt an enterprise-wide IM solution within the next few years,⁷ most of these systems, upon initial deployment, will have inadequate or zero protection. This of course, presents an alluring prospect for cybercriminals who are constantly seeking new ways to enter corporate networks. When targeting IM systems, attackers are often utilizing the same deceptive techniques that proved successful in email threats. Sophisticated, socially-engineered IM threats are either disseminating malware or links to malicious sites. And due to the instant nature of IM, these threats can strike in the blink of an eye.

WORM_IRCBOT: MALWARE TARGETING SOCIAL NETWORKING

IRCBOT, also known as the MSN Worm, exemplifies how cybercriminals are exploiting instant messaging as a new means for distributing malware. Using multiple social engineering techniques, it taps into the informal nature of IM chat, and tempts victims to execute malware by opening pictures that are supposedly on FaceBook, MySpace, and other popular sites. Variants have appeared with minor modifications, designed to help it pass reactive defenses and take more sophisticated and malicious action.

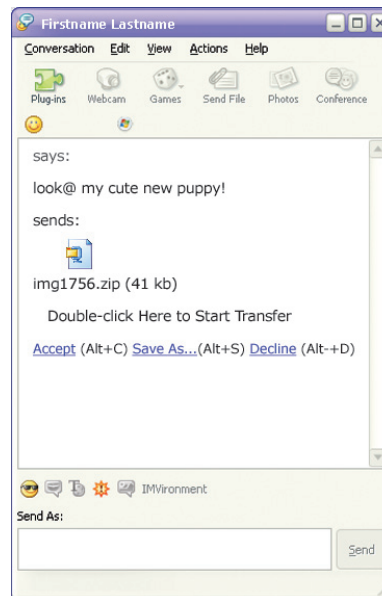
How IRCBOT Works

IRCBOT propagates via IM messages designed to bait recipients into opening pictures. Here are just a few of the tricks being used:

- Leveraging popularity of social networks: “can I throw this picture of us on my facebook.. please?”
- Playing to human nature: “This can’t be you, right?.”
- Utilizing chatty language: “OMG, i found ur pic on cuteornot.com! im not kidding either!!!”
- Creating deceptive details: links go to files titled something like “photos1_2008”

When the recipient clicks on an attachment, WORM_IRCBOT.SN is installed and executed. Its first task is to change the API SetLastError so the system does not display error messages. It then opens port 9103 to connect to the Internet Relay Chat (IRC) server, utilizing a dynamic user name that includes the computer name and operating system version of the affected system. This provides immediate information back to the attacker. Once connected over IRC, it waits for the following commands from the malware author:

- Act as an FTP and HTTP server
- Download and execute files
- Perform denial of service (DoS) attacks
- Perform propagation via IM



⁷ Gartner Research. Marketscope for Instant Messaging, 2007, Document # G00147732, April 2007.

Real-Time Communications and Real-World Threats Driving the Need for Real-Time Protections

Defending Against WORM_IRCBOT.SN

Due to IRCBOT's use of many different messages (all of which are short and easily changed), inspection must focus on the attachment itself rather than the message body. Effective protection requires the following:

- Signature-independent zero-day protections, as well as strong antivirus scanning, to detect the malware and its variants within IM
- Dedicated antivirus and antispymware protection to detect the downloader and subsequent spyware, in the event IRCBOT reaches the endpoint
- Web threat protection to stop communication back to the cybercriminal

Read the complete Trend Micro report on **Worm IRCBOT** >>

SKYPE LINKS: TAILORED MALWARE OVER THE WEB

This attack again highlights how insidious IM attacks can be: inspiring fear and tapping into prevalent security concerns about Microsoft Windows and its vulnerabilities. It also dupes victims by sending customized messages to mirror the IM application being used and selecting a sender name that gives the initial appearance of a system notification.

How the Attack Works

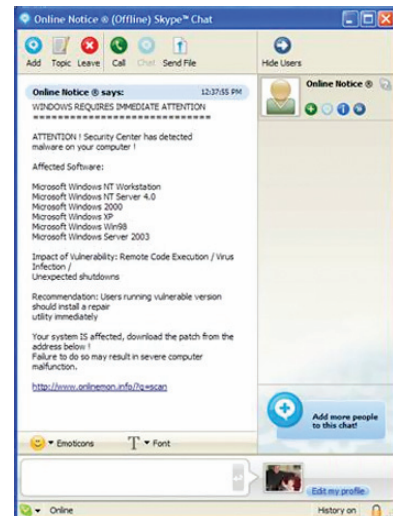
Targeted Skype users are identified through contact list mining and other nefarious methods. Attackers then send a message that appears to be a system notification about a specific Windows vulnerability that requires a patch. This alleged "patch" is offered via a link which actually goes to a malicious site where the user is invited to download a scanner which allegedly finds malware on the PC. Then the victim is asked to provide a host of personal information in order to download software that promises to remove the supposed malware.

Defending against This Attack

Because the IM message itself contains no malware, traditional antivirus scanning is of limited value. Instead, the following types of security are needed:

- Dynamic web reputation analysis that can identify malicious links within the IM based on source reputation and real-time threat intelligence
- Web threat protection on the endpoint, should it get that far, in order to prevent the recipient from following the URL
- Web security at the gateway in order to stop the transmission of sensitive information to the attacker

Read the complete Trend Micro report >>



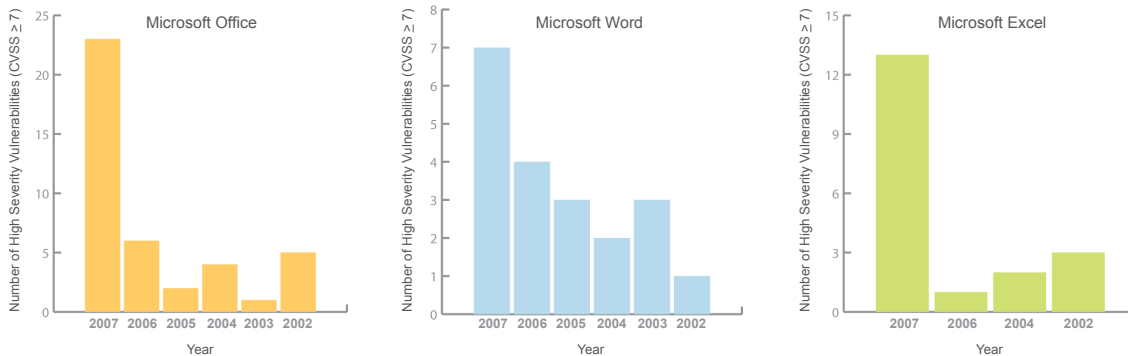
Real-Time Communications and Real-World Threats Driving the Need for Real-Time Protections

COLLABORATION THREATS

In the past, worms that spread among networked databases to bring down systems were the primary threat to SharePoint. However, a greater risk today is the malware that propagates via Microsoft Office files, the most common files stored within the repositories. On-demand access to these compromised files can pose a substantial security risk to you—and your affiliates, partners or customers. In addition, SharePoint is now much more than a content management system, encompassing a wide range of Web 2.0 capabilities. Team sites, personal portals, blogs, and wikis enable real-time interaction on the web, but they also present new vulnerabilities that allow attackers to infiltrate. The rise in web threats, specifically the compromise of legitimate sites, is perhaps the greatest risk that needs to be addressed.

MICROSOFT OFFICE EXPLOITS: MALWARE PROPAGATION VIA COMMON CONTENT

According to SANS Institute, vulnerabilities in Microsoft Office files, represented one of the top 20 security risks of 2007. In particular, high severity vulnerabilities within Microsoft Office tripled in one year from 2006 to 2007. Many attacks leverage these vulnerabilities to hide and then execute malicious code within otherwise innocuous files.



How These Attacks Work

Cybercriminals embed malware in a wide range of Microsoft Office documents, which are designed to seem legitimate. When unsuspecting end users open these files, malicious executables are automatically installed on their PCs. This automatic installation is made possible by various program vulnerabilities, such as [Microsoft Security Advisory 947563](#), which allows unauthorized remote code execution. Once installed, the malicious executables generally download additional malware (see TROJ_MDROPPER.GJ as one example) to establish a remote connection, giving the cybercriminal access to the infected system. From that point, anything can happen.

Real-Time Communications and Real-World Threats Driving the Need for Real-Time Protections

Defending against Compromised Microsoft Files

Keeping your SharePoint repository free of malicious files requires:

- Advanced anti-malware scanning within the content repository and on endpoints (those that can be controlled by the organization), especially the ability to detect malware embedded within files
- Zero-day protection to stop new versions of malware-infected files before signature updates are available
- Content filtering to remove malicious files from the repository if they slip past anti-malware scanning
- Vulnerability scanning and patching of endpoints to prevent embedded attacks that rely on vulnerability exploit
- Web security to detect subsequent malware downloads

Read the complete Trend Micro report >>

iFRAME: INSIDIOUS HIJACKING OF LEGITIMATE SITES

According to SANS, the number one cyber security menace for 2008 is, “increasingly sophisticated web site attacks that exploit browser vulnerabilities—especially on trusted web sites.” Likewise, TrendLabs reports that more than 40% of all web threats in 1Q08 involved legitimate sites hijacked by cybercriminals. In most cases, the hijackers create a redirect, called an iFrame, which sends web users unknowingly to malicious sites hosting malware.

How the Attack Works

Cybercriminals seek out websites with unpatched vulnerabilities that can be exploited to inject their own malicious code to prey on the sites' everyday visitors. News or retail sites are often targeted, as they offer broad exposure to a high volume of visitors and/or ready access to personal information. However, major brands, educational institutions, and government sites have also been compromised. And most recently, attacks have successfully compromised thousands of sites at one time.

The most common attack uses SQL injection to append a small snippet of code to text fields which commands the browser to redirect to a malicious website. When victims arrive at this unplanned destination, malware is automatically downloaded onto their machine. This is a rather insidious combination of vulnerability exploit combined with a drive-by download. As one example, malware known as JS_Dloader is installed, which then downloads spyware intended to steal login credentials.



Real-Time Communications and Real-World Threats Driving the Need for Real-Time Protections

Defending against the iFRAME Attack

Ultimately, the best way to avoid the compromise of your SharePoint site and infection of users is to:

- Conduct frequent vulnerability scanning and ensure that common vulnerabilities, especially SQL injection and cross-site scripting, are mitigated through patching
- Routinely scan your Intranet and Extranet sites for malicious code, files and links, using automated real-time inspection tools
- Deploy comprehensive endpoint security for your employees, including effective anti-malware, intrusion prevention, personal firewall technologies, as well as real-time web threat protection

“ Fool me once,
shame on you.
Fool me twice,
shame on me. ”

- English Idiom

Read the complete Trend Micro report >>

LESSONS TO LEARN FROM REAL-WORLD THREATS

Today's cybercriminals are designing stealthy, targeted, and fast-moving multi-stage attacks to first slip past traditional defenses and hijack PCs, then download additional malware to steal information and/or continue to morph and evade detection while awaiting further commands. In particular, the use of variants to change digital signatures, spam for quick dissemination, and URLs in place of attachments are all techniques designed to beat reactive signature-based defenses. As a result, the following proactive real-time protections and traditional defenses are critical:

- Real-time email reputation analysis to stop spam and blended threats based on the source, embedded links, and other characteristics rather than static signatures or heuristics which are quickly outdated
- Real-time web reputation analysis to detect and block links to malicious sites or legitimate compromised sites, which are often utilized in place of malware attachments
- Signature-independent zero-day protection to detect variants despite changing content or attachments
- Dedicated and proactive scan engines that take advantage of real-time threat intelligence to secure all avenues of attack

THE WILD CARD: SOCIAL ENGINEERING

For cybercriminals, beating defenses and reaching the end user is only half the battle. Convincing increasingly savvy end users to take the desired action is their next big challenge. To trick potential victims, they go to great lengths to create the illusion of authenticity, often customizing language, sender name, subject, attachment name, and file type to resonate with the recipient. And as we learned in the case of Subpoena, they are also spoofing sites that closely mirror the actual site, or in other instances, they are hiding within legitimate websites and then getting users to take action by tapping into real business concerns or fears. Unfortunately, these techniques are often successful, and end user education, while important, is not nearly enough to combat these threats.

This alarming trend of sophisticated social engineering drives the need for comprehensive security that can stop these attacks with as little reliance on end users as possible. In particular, it is important to deploy the right mix of protections at multiple layers: in-the-cloud, at the gateway, on the messaging servers, and at the endpoints. And while most organizations have mail server security, many are highly vulnerable when it comes to IM and collaboration. The key to protecting communication and collaboration systems and minimizing risk is to deploy unified security across email, instant messaging, and collaboration.

Real-Time Communications and Real-World Threats Driving the Need for Real-Time Protections

THE FIVE ESSENTIALS

Due to the risk of instant exposure, instant protection is critical. Organizations should look for solutions that meet 5 essential elements of enterprise security:

- Block threats fast with proactive protections
- Outsmart the threats using a combination of advanced techniques
- Stop all types of threats to combat sophisticated, blended attacks
- Secure every entry point across your communication and collaboration systems
- Reduce IT workload and costs with a highly-effective, centrally-managed solution

Why Trend Micro?

Trend Micro's real-time protections, powered by the unique cloud-client architecture of the [Smart Protection Network](#), work in concert with leading anti-malware, antispyware, and content filtering security to stop the wide range of threats—immediately and automatically. Together these technologies prevent data theft, infection, intrusion, reputation damage, and compliance violations.

1. Blocks threats fast

As we saw, many of the attacks propagate quickly—using spam, serial variants, instant messaging, and the web. Only real-time security can stop these threats before they cause damage. Trend Micro's Email and Web Reputation, powered by the Smart Protection Network, deliver up-to-the-minute correlated threat intelligence to automatically improve security and stop the latest threats—immediately.

2. Outsmarts the threats

Cybercrime attacks continue to grow more sophisticated, forcing defenses to become smarter. Who is the source, and can I trust them? What could be hidden in this message or file? How is it behaving? Trend Micro Communication & Collaboration Security identifies who, what and how with innovative reputation, content and behavior analysis. Together, this combination outsmarts threats before they can strike.

3. Stops all types of threats

Threats come in many forms and blended combinations of spam, phishing, viruses, worms, spyware, Trojans, and more. Trend Micro provides all-threat protection:

- Web threats
- Spam
- Trojans
- Phishing & pharming
- Data theft & loss
- Spyware
- Viruses
- Worms
- Bots
- Inappropriate content

4. Secures every entry point

Cybercriminals target every network entry point, and closing off only one vector of attack, such as email, or relying on protection at only one layer, makes your organization easy prey. To protect your network, data, employees, partners and customers, Trend Micro secures your Microsoft-based electronic communication & collaboration entry points—email, enterprise IM, and collaboration.

5. Reduces IT workload and costs

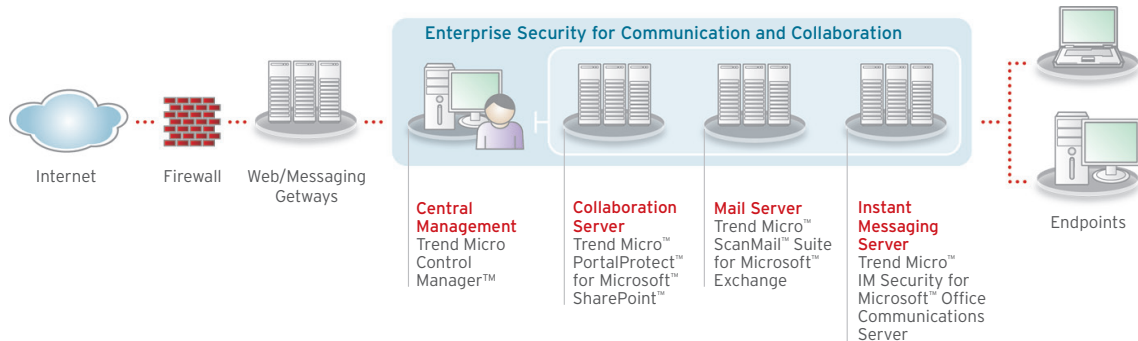
Deploying multiple point products can be cumbersome to manage and takes scarce resources away from strategic business-enabling projects. Given the complexity of today's threat landscape, organization's need to deploy a coordinated, proactive defense. Centralized management, optimized performance, tight integration, and powerful group management all contribute to low administration—giving you more time to be proactive and optimize security.

Real-Time Communications and Real-World Threats Driving the Need for Real-Time Protections

THE POWER OF FOUR

Trend Micro™ Enterprise Security for Communication and Collaboration

This 4-in-1 solution locks down all avenues of attack at the server level. And with centralized management, optimized performance, and tight platform integration, the suite reduces administration.



END-TO-END PROTECTION

For the most comprehensive protection against the many types of communication and collaboration threats described in this white paper, Trend Micro™ Enterprise Security for Communication and Collaboration can be deployed with Trend Micro™ InterScan™ Messaging Security Suite and Trend Micro™ InterScan™ Web Security Suite at the gateway, and Trend Micro™ OfficeScan™ Client/Server Edition at endpoints. Together, these solutions deliver the right combination of protections at all points of attack.

Enterprise Security for Communication and Collaboration	IM Security	ScanMail Suite	PortalProtect
Protection Point	IM Servers	Mail Servers	Collaboration Servers
Web Reputation	✓		
Email Reputation		✓	
Antivirus	✓	✓	✓
Antispyware	✓	✓	✓
Antispam		✓	
Antiphishing	✓	✓	
Content Filtering & Data Leak Prevention	✓	✓	✓

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

U.S. toll free: +1 800.228.5651

phone: +1 408.257.1500

fax: +1 408.257.2003

www.trendmicro.com

