Enterprise Prevention and Management of Mixed-Threat Attacks :

Why Current Antivirus and Content Security Approaches are Limited

TABLE OF CONTENTS

December 2002
Trend Micro, Inc.

EXECUTIVE SUMMARY

Today's corporations are highly dependent on global, distributed computing environments to streamline operations, increase efficiency and reduce costs. Deployment of multiple and new devices, operating systems, Web services, and online applications in these environments has enabled unprecedented capabilities and increased productivity. In addition, these technologies have also opened up remote access to the internal network, creating potential access points that can expose enterprises to crippling computer viruses.

Corporations are also burdened by the proliferation of mixed-threat attacks such as Nimda, which take advantage of multiple entry points and vulnerabilities in enterprise networks. These malicious programs use a variety of techniques to breach security at multiple entry points in the network, replicate and perform hostile acts against network resources. As a result of the increased complexity of these attacks and the distributed, global nature of corporate computing environments, IT managers face significant challenges associated with managing day-to-day operations and defining long-term security strategies.

While the reactive, pattern file-based approach to attack prevention is effective at detecting and cleaning known threats, it only solves a portion of an IT manager's problems. Many common issues IT managers and security staffs worldwide struggle to address include:

- Limited expertise to combat outbreak activity, apply best practices for prevention, and incorporate timely information as new threats become known
- A period of extreme vulnerability between the time a threat is known and the time a fix such as a pattern file is available
- Increased exposure to outbreaks due to administrative inefficiencies caused by inconsistent application of security policies throughout the network or the need to manually perform these tasks
- Significant assessment, restoration, and lost productivity costs associated with outbreaks
- Inability to measure the overall effectiveness of antivirus and content security investments

Trend Micro's vast experience with global, enterprise customers demonstrates that most businesses—regardless of size—have adopted a staged, seven-step process for responding to new security threats. Although some aspects of these procedures have been automated, they remain predominantly manual, time consuming, and inconsistent. For example, notifying personnel of a new security threat via telephone, fax, or email; individually configuring gateway-level antivirus and content security software settings to deter a specific threat; and consulting with management and security specialists to determine the most effective course of action are time-consuming, manual processes that delay action and increase an enterprise's chances of sustaining damage from an imminent attack.

Until now, IT managers have had limited antivirus and content security approaches to address the seven-step process for responding to new security threats. The Trend Micro Enterprise Protection Strategy is an industry-unique approach to antivirus and content security that addresses mixed-threat attacks through coordinated delivery of products, services and expertise to address customer needs throughout the outbreak lifecycle. The outbreak lifecycle, a seven-step process that customers undergo in response to new security threats or outbreaks, consists of three primary phases—outbreak prevention, virus response, and assessment and restoration. From attack-specific policy recommendations to cleanup and restoration templates, Enterprise Protection Strategy helps organizations continuously adapt as threats evolve. Designed to deliver timely updates and attack-specific policy recommendations, Enterprise Protection Strategy addresses all three phases of the outbreak lifecycle to help manage the explosive time, costs, and system damage associated with outbreaks.

THE PROLIFERATION AND ECONOMIC IMPACT OF MIXED-THREAT VIRUS ATTACKS

Customer View of Virus Outbreak Lifecycle
Due in part to a strategic gap between enterprise needs and industry solutions, successful virus infiltration of enterprise networks is steadily increasing. An ICSA Labs survey indicates that 99.67 percent of responding companies suffered at least one virus outbreak between 1996 and 2001, and that the rate of infection per thousand computers in surveyed companies rose from 1 percent in 1996 to 9.1 percent in 2001.

The emergence of new types of viruses during the summer and fall of 2001, such as CodeRed and Nimda, has caused many corporations to raise their barriers against malicious viruses at significantly higher levels. Unlike previous virus outbreaks, which typically executed a single hostile act (such as the Melissa virus, which overloaded and crashed a company's email system), mixed-threat attacks launch many diverse, parallel attacks. These mixed-threat attacks also replicate and proliferate much more rapidly than traditional viruses, exploiting multiple network pathways to slow traffic, deface Web sites, infiltrate other systems, and/or provide backdoor access to secure information. These new viruses can cause significant damage at a more rapid rate than previous and more rudimentary attacks. Existing antivirus and security technologies offer limited approaches for staving off or containing such accelerated and aggressive threats.

Security threats present more than headaches for the IT and security departments; they also significantly impact a company's financial health, as illustrated below.

Even viruses that do nothing but replicate themselves can inflict substantial havoc, as illustrated by Table 1. For example, the Melissa virus had no obviously malicious goal, or "payload," and did not destroy information or compromise network security. Yet the cost of scanning for

infected files, containing and eliminating the virus, and restoring the network services that crashed due to overloaded email servers was estimated at $1.1 billion[1]. Publicized incidents of virus outbreaks can also damage business reputations in ways that cannot always be quantified. For example, although the LoveBug and SirCam viruses negatively impacted network and email server performance, they also—more disturbingly—placed confidential enterprise information at risk. Damage from LoveBug could be mitigated by changing system passwords after clean up the infected files; SirCam, on the other hand, more actively compromised enterprises by emailing random files—including confidential ones—to address found on the network.
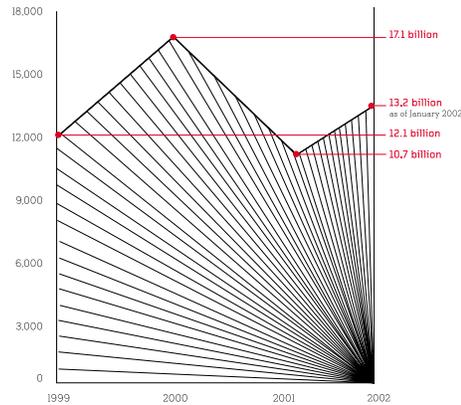
Note:
1. Computer Economics:
   Cyber attack Index,
   January 2002

Figure 1:
Estimated Economic Impact of Viruses

ESTIMATED ECONOMIC IMPACT OF VIRUSES

	17.1 billion	
	13.2 billion as of January 2002	
	12.1 billion	
	10.7 billion	

Virus	Details	Estimated Cost Worldwide
Melissa	Word 97 Macro virus that sends itself to first 50 names in Outlook address book.	$1.1 billion
LoveBug	Visual Basic script propagated through Outlook and IRC chat. Overwrites files with specific extensions with its code, modifies registry entries, and downloads a password-stealing Trojan into the infected system.	$8.75 billion
SirCam	Inserts malicious code into a random file and sends file as email attachment randomly to email addresses found on the system. Contains SMTP commands to propagate itself through mail servers.	$1.5 billion

THE LATEST CHALLENGE: A NEW TYPE OF ATTACK

When these new types of attacks, such as CodeRed and Nimda, burst onto the networked computing scene, enterprises were forced to re-evaluate the way they thought about computer viruses. Unlike previous attacks, these mixed-threat attacks deploy a variety of techniques to break into networks, replicate, and destroy, delete, or damage enterprise information assets.

First encounters: Nimda and CodeRed

Initially detected in the summer of 2001, the CodeRed virus was the first widespread, multiple threat attack to hit enterprise networks. Nimda followed just a few months later. Both viruses were immediately flagged by security experts as harbingers of future attacks.

CodeRed

After exploiting a security hole in Microsoft™ Internet Information Server (IIS), CodeRed rapidly replicated code designed to consume system resources like a worm, and then executed hostile code similar to a Trojan attack. CodeRed wreaks damage by defacing host Web sites and coordinating multiple distributed denial-of-service attacks that effectively shut down targeted servers. Because each CodeRed–infected server creates 99 simultaneous attempts to propagate the malicious code, CodeRed spread throughout the Internet at an alarming rate.

CodeRed infiltrated enterprise networks by first targeting a well-known security vulnerability on machines running Microsoft Internet IIS. This particular vulnerability was well chosen. Internet IIS is a broadly used, industry-standard package automatically installed on Windows machines by Microsoft operating systems. IIS is also installed by default on certain Cisco™ DSL routers.

Nimda

Nimda, which first appeared in September 2001, is an even more virulent attack that exploits multiple propagation methods to infect desktop and notebook PCs as well as Web servers. Some of the methods Nimda used are listed below:

- Transmit malicious email attachments. Nimda arrives as an attachment that exploits vulnerabilities in unpatched email client software, allowing the file to automatically launch and infect the computer when the message is read, regardless of whether the user opened the attachment.

- Exploit security holes on Web servers. Nimda can spreads among Web servers by exploiting a known vulnerability on IIS servers without up-to-date software patches or through a back door left by CodeRed II, a follow-up to the original CodeRed attack, that provides full access to infected systems

- Place hostile code on Web pages. Infected Web sites use JavaScript to pass Nimda to poorly configured Web browsers that automatically launch downloaded files

- Abuse network file-sharing privileges. Infected systems search the local network for computers with open file sharing and copy Nimda freely to these vulnerable systems

In addition to the problems caused by its ferocious propagation rate, Nimda compromised system security on infected machines by opening up access to PC hard drives and creating a password-free guest account with administrator privileges on Microsoft Windows NT™ and Windows™ 2000 systems.

Why Traditional Security Is Limited for Protecting Against Mixed-threat Attacks
As illustrated above, SirCam, Nimda, and CodeRed introduced a new type of attack, termed here as mixed-threat attack due to their variety of forms and propagation methods. Because mixed-threat viruses employ a range of attack techniques, traditional antivirus software can no longer reliably provide adequate protection. Even the most scrupulously maintained networks are at risk due to the inevitable security vulnerabilities in operating systems and server software (and for every vulnerability fixed through a vendor upgrade, several others are detected). Other kinds of security products are also largely ineffective because of their passive design. Most are incapable of proactively identifying and fending off these increasingly sophisticated threats.

Current Antivirus Solution Process
To better understand why a gap exists between today's security approaches and the core requirements needed to address the common issues IT managers and security staffs face, requires a brief review of the traditional approaches common to the antivirus industry. The traditional antivirus approach to protection concentrates on four major steps.

1. A virus is identified as a potential threat to the network

2. Because pattern files are not yet available, IT Managers must wait before initiating the appropriate security response. During this critical time of extreme vulnerability, an IT Manager is powerless to act except to take drastic actions, which can impede corporate productivity, such as shutting down network services

3.   Pattern files are automatically sent to an enterprise by the vendor. This critical step is cited by many customers as one which can take many hours or in some cases, days to achieve a final, fully-qualified pattern file solution depending upon the vendor, attack complexity, and quality of service

4.   The enterprise team tests pattern files and the central antivirus management program pushes the pattern files to client machines

Figure 2:
Current Antivirus Solution Process

1. Virus Discovered   2. System shutdown   3. Pattern File   4. Enterprise tests and pushes pattern
                          or await pattern file   received from vendor   files; then admin takes action

STOP

.xxx.vbs

PATTERN FILE
VIA VENDOR

ENTERPRISE

.xxx.vbs

AV POLICIES and
PATTERN FILES

DESKTOP

ADMINISTRATOR

ADMINISTRATOR

DESKTOP

FILE SERVER
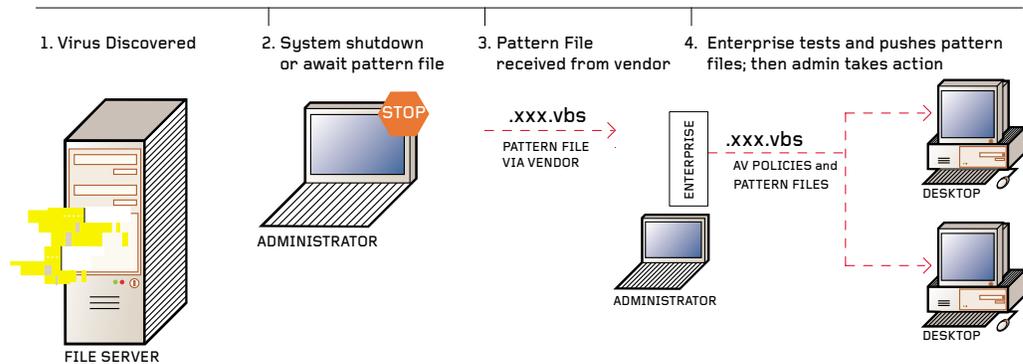
Although antivirus software vendors rush to create pattern files as soon as new viruses are identified, IT managers cannot always take proactive steps to minimize risk and disruptions— even if they suspect their systems are compromised—until the pattern files are available. During this critical time period, and after an attack, many enterprises remain vulnerable to attack and have minimal understanding of how to protect, prevent, and restore their networks from such malicious outbreaks.

It is because of this reactive, pattern file-based approach to security, that outbreaks continue to infect enterprises worldwide, even ones that have comprehensive solutions currently in place. When asked, many of those infected customers express dismay regarding the effectiveness of the technology approaches they currently implement.   Until the emergence of mixed-threat attacks, most IT managers were certain that their existing approaches to antivirus and content security were sufficient.

HOW CUSTOMERS DEAL WITH MIXED-THREAT ATTACKS: THE VIRUS OUTBREAK LIFECYCLE

Customer View of Virus Outbreak Lifecycle
In the wake of the virulent path of the Nimda and CodeRed viruses, Trend Micro, the global leader in network antivirus and Internet security software, launched a six-month research initiative to identify enterprise best practices for preventing or deflecting potentially damaging computer virus attacks. The results were illuminating. After in-depth interviews with more than 100 enterprise customers, Trend Micro found that most organizations—regardless of size— adhered to a remarkably similar set of staged procedures when responding to the various stages of what Trend Micro now refers to as "the outbreak lifecycle."

As illustrated in Figure 3, Trend Micro identified seven distinctive steps traditionally used by enterprises when responding to security threats.
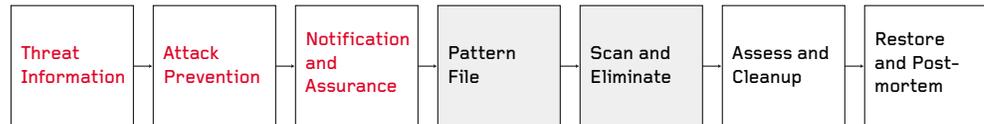
Figure 3:
Virus Outbreak Lifecycle

| Threat Information | Attack Prevention | Notification and Assurance | Pattern File | Scan and Eliminate | Assess and Cleanup | Restore and Post-mortem |

Note:
Most enterprises reported a remarkably similar multi-step procedure they followed when alerted to a potential attack.

Step 1: Threat Information
Upon learning of a potential threat—using information that can come from a variety of sources—the customer systematically searches for and collects all available information about the possible attack.

Customer Concern: Lack of Timely Knowledge of Threats
Many enterprises depend on subscription-based antivirus support services that notify them of pending threats, provide new virus pattern files, and otherwise provide timely knowledge and expertise as needed. While such services can be highly effective, they can vary in quality depending on the specific personnel assigned to an account. If staffed with minimally-trained or inexperienced people, a support service can be slow to react, possess limited knowledge, and incorrectly communicate complex, technical information. Although antivirus security services deliver real value and will always play a role in enterprise security strategies, such solutions work best when coupled with other, coordinated antivirus products and services which can leverage timely information to deliver automated policy recommendations throughout the outbreak lifecycle.

Regardless of their chosen intelligence method, upon learning of a potential threat the customer systematically searches for and collects all available information about the possible attack during this step in an attempt to be as proactive as possible in identifying and defending against potential attacks.

Real-world example: Nimda

In the case of Nimda, customers expressed concern that had they known that Nimda had multiple propagation capabilities and was capable of leaving virus remains that would keep systems vulnerable to attack, they would have taken much more drastic action in preventing and isolating the damage. As a result, many customers brought systems back online, unaware that the dangers of the virus had been further classified to include additional mailicious capabilities. Customers expressed a need during this step for consistent, proactive updates during this step of the outbreak lifecycle.

Step 2: Attack Prevention

In this step, the customer uses information obtained in Step 1 to assess operational vulnerability to the current threat and to adjust the configurations and settings of antivirus and content security products as necessary. If the threat is in the form of a new virus, the customer requests the latest "pattern file" from Trend Micro or other antivirus software vendors, and may suspend action until that file is available. If the potential attack is a known virus, system administrators can formulate an action policy for preventing or defending against the threat. This step is typically completed manually (e.g., requesting virus information from security experts and vendors, browsing the Internet for data, or downloading resources from the Web) and often involves comparing notes from various sources and coordinating with multiple departments to ensure that the action policy for protection is comprehensive enough to cover all know entry points and vulnerabilities. The primary customer concerns during this phase are:

Customer Concern: Lack of expertise concerning viruses activity and policy configuration

- Policy formulation: Few enterprises have the threat analysis experience, outbreak reproduction and testing capabilities, and policy creation expertise to accurately advise and assist in defining attack prevention strategies. While sources may provide descriptions of the impending attack, enterprises often need to conduct significant interpretation and investigation to determine how the attack information can be translated into an effective action policy. As a result, many IT managers and security staffs feel overwhelmed or under qualified to determine the appropriate policies to create and deploy

- Heterogeneous network implementation expertise: In addition to lacking the expertise to determine effective policy, enterprises also struggle with the technical expertise to determine the implementation plan required to deploy the policy recommendations to their environments in an efficient and effective manner. This step includes formulating a plan that configures and adjusts antivirus products, firewalls, caching devices, storage servers, and many other potential entry points. In addition, this step requires a coordinated effort from the technical implementation team, which often involves allocating and training global team members on the newest security needs. This process also involves keeping their technical expertise on the products up-to-date, which can be a very daunting task for even the largest of enterprises. To assist with this issue, customers have expressed a need for more information and potentially, automated policy generation to improve these administrative inefficiencies

Real-world example: Mixed-threat attacks penetrate multiple network entry points

The proliferation of new network protocols and access mechanisms also increases the complexity of responding effectively to potential attacks. For example, scanning messages at the email server level can intercept viruses sent as email file attachments or as embedded scripts in email messages. However, file attachments can also be downloaded through Web-accessible email systems such as AOL, Hotmail, or Yahoo, or transferred directly to a user's machine during an instant messaging session. In such cases, infected attachments take advantage of alternative network protocols and bypass the scanning technologies in question, allowing malicious code to be downloaded and executed on a local system without triggering security alarms or protective actions.

Firewalls, which control traffic between two networks, effectively defend against a number of common security threats if configured correctly. However, if a virus is embedded in an application, the firewall will allow it to enter the network as long as the file conforms to an approved protocol. CodeRed and Nimda both used this method to infiltrate firewall-protected systems. CodeRed's malicious code was included in an apparently acceptable HTTP communication. Nimda used a similar method to infect vulnerable servers and enter systems as seemingly acceptable email file attachments or as JavaScript code embedded on Web pages.

Proliferation of New Computing Devices

The increasing number and type of devices attached to the corporate network opens up additional security vulnerabilities. Enterprises must constantly monitor all systems—including user machines, email servers, Web servers, and storage devices, to ensure that local applications

do not impair antivirus software effectiveness and that users do not disable key antivirus mechanisms. As new information devices become available, this management burden grows. For example, virus protection is now needed for every desktop PC, notebook computer, network-enabled PDA, WAP-enabled mobile phone, or other device that accesses the network. Although enterprises require antivirus solutions that are platform-independent and easily scalable to a broad range of device footprints, most still fall back on traditional point security solutions that provide protection at the gateway, server, or even device-level.

Lack of Integrated Support for Distributed Networks

Enterprises can choose from a broad range of antivirus approaches that incorporate technologies which protect specific network access points and filter network traffic for viruses. These limited approaches require IT managers to possess vast knowledge of security vulnerabilities for a broad range of platforms and operating systems. These types of products also require extensive manual administration of configuration, deployment, and monitoring functions. Few IT managers have the time and resources to coordinate and implement these functions effectively.

Enterprise Concern: Inconsistent information and difficulty coordinating attack prevention efforts across departments

During this phase, as IT managers query multiple sources for current threat information, coordinate communication with many departments (e.g., firewall, security, HR departments) and incorporate the requirements of many devices in their formulation of prevention policies. Since this information is often inconsistently conveyed across multiple, global groups, policy recommendations are often created without proper information regarding the core requirements for specific prevention methods. Without an automated manner or single source of follow-up or policy adjustment, enterprises may determine or put in place an ineffective policy for potentially hours, days, or weeks, once again, leaving them vulnerable to attack.

IT managers often undergo this step to rapidly deliver a resolution or fix to stop or contain the threat. However, as a result of the concerns mentioned above, they often still have considerable concerns regarding the quality of decisions and policies that they created during this attack prevention stage due to the limited and often suspect information on which they base their decisions.

Step 3: Notification and Assurance

Once an action policy has been defined, the customer notifies all appropriate individuals and organizations within the enterprise of the pending threat and communicates the official policy recommendation. To assure compliance, the customer must closely monitor the status of at-risk networks and systems. The activities involved in this step—telephone calls and

email messages to check system status; device and software configuration using multiple consoles of antivirus point products—are typically completed manually.   As a result of these activities, customers have the following concerns during this step of the outbreak lifecycle:

- Chaos – This step is typically described as the most chaotic and unpredictable stage of the outbreak lifecycle (particularly by large and global enterprises)

- Inconsistent application of policy – by communicating application of policy recommendations internally via many manual and time-consuming methods such as email, fax, phone or pager, and relying on many globally-distributed resources (often with differing levels of expertise), IT managers complain that their ability to ensure that a policy was applied correctly is often suspect, time-consuming and costly

Step 4: Pattern File

If the current threat is from a new virus, customers wait for a new virus pattern file to be released from Trend Micro or other relevant vendors. Most businesses undergo a complete testing and quality assurance cycle prior to deploying the new pattern file.

Time Lag Between Threat Identification and Solution

In the past, enterprises were frequently placed in the frustrating position of knowing that a virus attack was imminent, yet not being able to take effective action against it because the new virus pattern file was not yet available. While antivirus vendors scramble to release new pattern files as rapidly as possible, timely release of such files is often delayed by testing or QA initiatives, or by the need to validate pattern file effectiveness across multiple platforms. There is usually a significant lag between the time a new virus is identified and the moment that a new and tested virus pattern file is available.

Even after a pattern file has been released, IT managers face the tedious administrative burden of first testing, disseminating the new code, and making sure that all at-risk systems throughout their organizations received and correctly implemented the updated software.

Previously, the only viable defense some enterprises could make, if compromised, was to shut down all or part of the network—a drastic move that resulted in costly business downtime and widespread productivity losses.

For the most part, businesses feel that the antivirus and content security industry has determined the technical aspects of this step successfully, to include centralized distribution and management of the pattern file and signature detection once the file is released. However, there still are some customer concerns with this phase:

- Enduring this phase is often a very painful experience as IT managers must wait for a pattern file while their networks are exposed to multiple vulnerabilities. Many customers have expressed interest in receiving an interim solution from their antivirus vendor, prior to the delivery of a pattern file
- Customers often have no idea how long this step may take, when they will hear from their antivirus vendor regarding the availability of a pattern file and how long they will remain vulnerable. As a result, many customers have expressed the need for some form of guarantee and measurement of performance in pattern file delivery that will help them track and evaluate their antivirus and content security vendors

While the technical aspects of the pattern file stage have been successfully addressed by the security industry, concerns regarding the more practical issues (proactive policy recommendations, timely responses) remain.

Step 5: Scan and Eliminate

Once the new virus pattern file has been tested and disseminated, customers can begin scanning for the virus. Any infected files are flagged and the virus is eliminated to prevent it from spreading.   This step has been technically mastered but many customers have remained concerned about the practicality and performance of this step. Specific customer requirements include:

- More flexibility in setting scanning parameters and defining scanning policies in their networks. Customer often complain that it is often "all or nothing" in regards to scanning policy flexibility

- There are elements of mixed-threat attacks, such as worms, Trojans, virus traps, back-doors, and remnants, that cannot be detected or successfully eliminated by the pattern file and scan engine alone. Customers would like other methods of detection and removal of elements of malicious behavior that the pattern file cannot address

Real-world example: CodeRed illustrated the limitations of pattern files
Because CodeRed resided within the infected system's memory, (i.e., not by executing a file stored on the disk drive) traditional file-based antivirus packages provided too little protection too late. For starters, systems were already infected by the time the virus was even noticed. Second, many virus software products scan files stored on disk drives or searches for traffic using a specific protocol. Such solutions would not identify any virus that is memory-resident. As a result, several pattern file methods to secure the enterprise had difficulty in defending against the CodeRed virus.

Step 6: Assess and Cleanup

Once the virus has been eliminated the customer determines which systems have been affected by the attack and evaluates the nature and extent of the damage. Infected systems are cleaned and/or restored to prevent a re-attack to the network. Customers' biggest concerns with this step are:

- Customers don't often know where they have been infected and where they remain vulnerable. They require some form of infection detection and assessment throughout their enterprise to help them assess the location, severity, and extent of the damage

- Current assessment and cleanup methods are typically manual and require system administrators to cleanup multiple systems on the network individually. In enterprises with thousands of desktops and servers that are globally distributed, this is often a very painful and time consuming step. To illustrate how true the customer perception of the insufficiencies of solutions in this stage is today, recent study by market research firm Computer Intelligence found that 80 percent of the costs of responding to the Goner virus outbreak involved manual "clean up " of infected systems

- Several customers have complained that after several days of cleaning thousands of systems worldwide day-and-night, their entire network operations were subsequently brought down because they missed one machine; which promptly re-infected the entire network when brought online

Not only do the current solutions deliver limited approaches for addressing the true threat, they are potentially costing corporations a great deal of operations costs and lost productivity.

Step 7: Restore and Post-Mortem

This crucial step allows customers to examine in retrospect what worked, what didn't, and what procedures they can implement differently when the next virus outbreak occurs. This step can include investigating various network and system performance metrics; conducting interviews with affected employees; initiating a formal review of current policies and procedures; and multiple forms of other analysis.

Additionally, if these enhancements were made to this step, customers would prefer them to be centrally administered and managed due to the complexities of tracking and evaluating scanning performance. Customers have requested one source of information that allows them

to track and manage attacks globally as they happen and helps them evaluate their performance in a consolidated and statistically significant manner. A common customer complaint is that the point product, system-based approach commonly employed today is insufficient for reviewing their operations holistically and evaluating their performance.

Intrusion Detection Systems

Unlike firewalls, intrusion detection systems bear no direct responsibility for controlling incoming and outgoing network traffic. Instead, they monitor key entrance points to a network, including firewalls, routers, and servers, for suspicious activities. These activities can include repeated logon failures, which may be attempts to gain unauthorized account access, or unauthorized scanning of port numbers, a common method for detecting system vulnerabilities.

However, intrusion detection systems rely on rule-based databases to determine whether any given behavior is suspicious. This provides an effective shield against known threats, but an intrusion detection system may not be able to detect new attacks. Also, most current intrusion detection systems are passive. They can report potential threats, but cannot perform defensive actions or initiate cleanup/repair of damaged systems.

Intrusion detection systems are further limited by the nature of mixed-threat attacks. Until recently, the majority of viruses were targeted at single, specific systems. The intrusion detection system identified the attack and warned the system administrator, who would then perform defensive activities such as closing the hacker's connection or installing a security patch. However, as demonstrated by recent distributed denial-of-service attacks, targeted systems can now be simultaneously attacked by multiple systems, or used as agents to attack other systems. In such cases, administrators must go beyond merely identifying threats. They must be able to rapidly define and implement enterprise-wide procedures on the fly that will stop attacks and begin repairing compromised systems immediately. Such rapid and complex responses are currently beyond the capabilities of intrusion detection systems.

A NEW APPROACH

The Trend Micro Enterprise Protection Strategy is an industry-unique approach to antivirus and content security that addresses mixed-threat attacks through coordinated delivery of products, services and expertise to address the entire outbreak lifecycle. The outbreak lifecycle, a customer-driven process of dealing with outbreaks, consists of three primary phases — outbreak prevention, virus response, and assessment and restoration.

Designed to deliver timely updates, and automated, attack-specific policy recommendations that incorporate knowledge and expertise from TrendLabs, Trend Micro's global network of security experts, the Enterprise Protection Strategy address each stage of the virus outbreak lifecycle, to help manage the explosive time, costs and system damage associated with outbreak Enhanced Capabilities of Trend Micro Enterprise Protection Strategy

Figure 4:

Trend Micro Enterprise Protection Strategy Manages the Outbreak Lifecycle
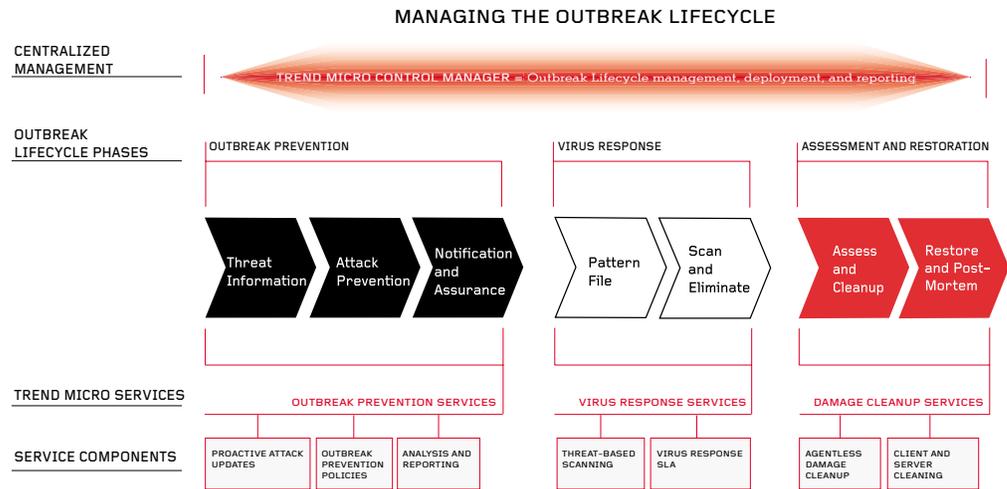
NOTE:

Trend Micro Enterprise Protection Strategy meets enterprise security needs at each stage of the virus outbreak lifecycle

MANAGING THE OUTBREAK LIFECYCLE

CENTRALIZED MANAGEMENT

TREND MICRO CONTROL MANAGER = Outbreak Lifecycle management, deployment, and reporting

OUTBREAK LIFECYCLE PHASES

OUTBREAK PREVENTION — Threat Information — Attack Prevention — Notification and Assurance

VIRUS RESPONSE — Pattern File — Scan and Eliminate

ASSESSMENT AND RESTORATION — Assess and Cleanup — Restore and Post-Mortem

TREND MICRO SERVICES — OUTBREAK PREVENTION SERVICES — VIRUS RESPONSE SERVICES — DAMAGE CLEANUP SERVICES

SERVICE COMPONENTS — PROACTIVE ATTACK UPDATES — OUTBREAK PREVENTION POLICIES — ANALYSIS AND REPORTING — THREAT-BASED SCANNING — VIRUS RESPONSE SLA — AGENTLESS DAMAGE CLEANUP — CLIENT AND SERVER CLEANING

The Enterprise Protection Strategy arms businesses with critical, industry-unique services, products and support to help businesses manage the explosive time, costs and system damage associated with outbreaks. Customer benefits include:

·   Coordinated delivery of industry-unique products, services and expertise to address the entire outbreak lifecycle

·   Timely updates and policy recommendations from TrendLabs, Trend Micro's global network of security experts

·   Robust centralized management for comprehensive visibility of network attack activity

·   Coordinated identification and deployment of policy recommendations across critical points of vulnerability throughout the enterprise

·   Enterprise-wide coordination through integration with best-of-breed third-party products, and heterogeneous platform support

INTEGRATED COMPONENTS OF TREND MICRO ENTERPRISE PROTECTION STRATEGY

The Enterprise Protection Strategy is comprised of the following integrated components:

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 which 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 undue downtime.

Outbreak Prevention Services deliver notification of new threats and 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 Service reduces the potential for miscommunication regarding application of policy, to deploy critical attack information consistently and as it is happening.

By providing automatic or manual download and deployment of policies via Trend Micro Control Manager™, Outbreak Prevention Service imports knowledge to critical access points on the network directly from experts at TrendLabs, Trend Micro's global security research and support network.

Threat-Based Scanning Services

During the virus response phase when a pattern file or fix is made available to address an outbreak, targeted, threat-based scanning allows enterprises to scan for specific types of viruses with attack-specific policy engines that scan based upon the identified threat for greater accuracy and detection.

Virus Response Service Level Agreement (SLA)

Trend Micro Virus Response 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.

Assessment and Restoration

The assessment and restoration phase is the period after a pattern file is deployed and the virus has been contained. To address this phase, Trend Micro provides attack-specific cleanup templates that help isolate and rid desktops and servers of virus remains such as hidden guest accounts, registry entries or memory-resident payloads. These cleanup templates are part of Trend Micro's damage cleanup services which are provided by Damage Cleanup Server, a server-based damage assessment and cleanup service and OfficeScan, a centrally-managed offering for the desktop.

These damage cleanup services help automate the enterprise-wide damage assessment and system cleanup functions, to accelerate recovery from attacks. With damage cleanup services, policy recommendations for cleanup and restoration are automatically delivered. Because these clean up templates are threat-specific, the previously time-consuming, manual task of damage assessment and system cleanup can be completed swiftly and precisely. Timely reports and analysis of the clean-up process allow system administrators to monitor the process and identify previously unknown network vulnerabilities.

The damage cleanup services include the following four steps:

1. Scanning for infected or altered files using a threat-specific profile of the virus footprint

2. Assessing actual damage incurred by analyzing changes made to files, system settings, network protocols, etc.

3.   The option of initiating automatic cleanup of infected files (recommended predefined clean up templates are available)

4.   Monitoring progress of clean-up process and generating reports

Components Supporting Trend Micro Enterprise Protection Strategy

Listed here are all other key components of the Trend Micro Enterprise Protection Strategy —including products, services, and other resources packaged or made available by Trend Micro.

Trend Micro Control Manager 2.5

Trend Micro Control Manager v2.5 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 helps 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.

By managing antivirus and content security products and services through a single console, Trend Micro Control Manager helps 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 acts 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. The Outbreak Commander console is centrally managed via Trend Micro Control Manager and helps IT managers to convert the extensive volume of discrete actions required when responding to potential threats into coherent and consistent global policies.

NOTE:
More information about Trend Micro Control Manager 2.5 can be found in the appendix.

Outbreak Commander organizes the vast capabilities included in the Trend Micro Enterprise Protection Strategy into three categories including:

Outbreak Prevention Stage

The products and services deployed during this response stage correspond with Steps 1, 2, and 3 in the staged, seven-step process for responding to new security threats. The aggregated capabilities include:

- Timely delivery of detailed threat information

- Threat-specific scanning and action policies available in advance of virus pattern files

- Notification of potential and new security threats to all appropriate individuals and groups

- Transparent, real-time monitoring of policy deployment

- Outbreak response reports and analysis delivered in real-time

Virus Response Stage

The capabilities delivered in this stage correspond to Step 4 of the original seven step process for responding to new security threats

- New virus pattern files are created and made available quickly
- Pattern files can be selectively or automatically deployed to system administrators for implementation
- Detailed reports on pattern file deployment are made available in real-time

Assessment and Restoration Stage

The capabilities delivered in this stage correspond to Step 5 of the original virus outbreak life-cycle model:

- New settings of scanning engines automatically configured in real-time
- Centralized management tools enable enterprise-wide virus scanning and elimination

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

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 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 eliminates 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.

KEY BENEFITS OF TREND MICRO ENTERPRISE PROTECTION STRATEGY

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 hassle of software upgrades. All software is continuously upgraded as part of Trend Micro's online and real-time service program.

Figure 5:

How Enterprise Security Strategy Responds to an Attack
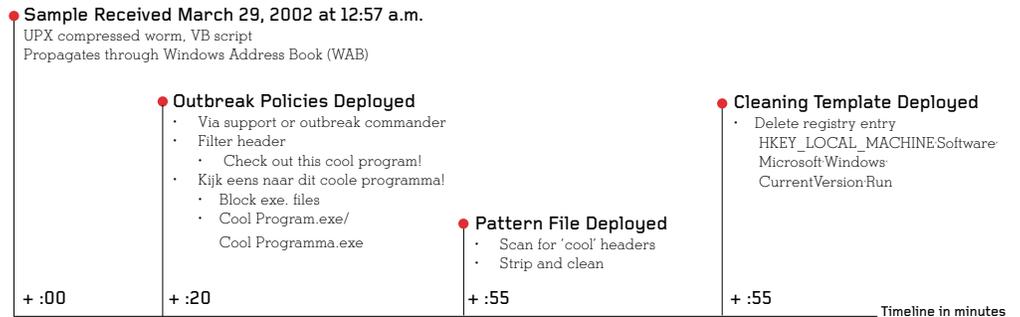
Fact:
This case study of Worm_Collo.C demonstrates how Enterprise Protection Strategy delivers proactive outbreak management of the entire lifecycle—from policy recom-mendations deployed via Outbreak Commander to cleanup templates provided by Damage Cleanup Services.

NOTE:
The response times shown above are actual numbers based upon a case study initiated and conducted internally by Trend Micro Inc. These numbers are not intended to guarantee specific response times, as these numbers will vary on a case-by-case basis.

Trend Micro Enterprise Protection Strategy in Action

● Sample Received March 29, 2002 at 12:57 a.m.
UPX compressed worm, VB script
Propagates through Windows Address Book (WAB)

● Outbreak Policies Deployed
· Via support or outbreak commander
· Filter header
  · Check out this cool program!
· Kijk eens naar dit coole programma!
· Block exe. files
· Cool Program.exe/
  Cool Programma.exe

● Cleaning Template Deployed
· Delete registry entry
  HKEY_LOCAL_MACHINE·Software·
  Microsoft·Windows·
  CurrentVersion·Run

● Pattern File Deployed
· Scan for 'cool' headers
· Strip and clean

| + :00 | + :20 | + :55 | + :55 |

Timeline in minutes

Threat Information → Attack Prevention → Notification and Assurance → Pattern File → Scan and Eliminate → Assess and Cleanup → Restore and Post-mortem

TREND MICRO ENTERPRISE PROTECTION STRATEGY IN ACTION

Among other benefits, Trend Micro Enterprise Protection Strategy delivers the following:

Centralized Management Tools

Trend Micro Control Manager 2.5 provides centralized management and enterprise-wide coordination for Trend Micro antivirus and content security products and services. Trend Micro Control Manager acts as the central command center for deployment of policies and cleaning templates to specific points throughout the network. Trend Micro Control Manager can receive Medium and High Risk alert warnings and disseminate outbreak prevention policies to diminish the threat of infection before pattern files are available. Administrators can then modify the policy templates as desired, and either automatically or manually deploy the solution throughout the enterprise.

Network Protection in Advance of Pattern Files

Outbreak Prevention Services enables enterprises to take immediate action against newly identified viruses. When a threat is identified, Trend Micro Control Manager receives descriptive information and can implement predefined activities to minimize the impact of the virus and maintain normal network functions as much as possible. For example, in the case of a hostile email attachment, Outbreak Prevention Services can help effectively secure the network from receiving or propagating malicious code by stripping the attachment from incoming and outgoing messages that match a particular profile. By the time the pattern files are distributed, Outbreak Prevention Services has already enabled the administrator to introduce safeguards against the new infection. When the pattern files are installed, the administrator can then rescan the previously suspect correspondence and forward safe messages to their intended destinations.

Flexible Deployment

Enterprise Protection Strategy allows enterprises to customize or otherwise selectively deploy specific features or components. For example, enterprises can decide to delegate virus scanning and cleanup activities to local administrators at the attack's point of origin —i.e., a virus outbreak in a geographically remote office. Alternatively, a business can automate select portions of products included in Trend Micro Enterprise Protection Strategy, and outsource all other antivirus activities to a service provider.

Comprehensive Reporting

Enterprise Protection Strategy monitors the enterprise from a single point of control (Trend Micro Control Manager) and automatically generates a consolidated incident and response report. This comprehensive enterprise-wide reporting enables administrators to improve response to future outbreaks by identifying network and system vulnerabilities.

Integrated Enterprise-Wide Protection

Effective defense against malicious code requires securing network entry points, propagation media, and productivity systems against potential hostile attacks uniquely targeted to those locations. Trend Micro Enterprise Protection Strategy enables administrators to choose the most effective defense and repair activities for the enterprise.

Real-Time Security Updates with Embedded Intelligence

TrendLabs, Trend Micro's ISO 9002-certified global network of antivirus research and product support centers, help ensure that all enterprise customers remain fully up to date on current security threats and are promptly provided with pattern files and cleanup templates as soon as they become available.

CONCLUSION

The proliferation of mixed-threat attacks and new communications protocols, services, and access devices has created fertile breeding grounds and effective distribution mechanisms for malicious code. Today's security threats exploit system and application vulnerabilities and spread too rapidly to be effectively stopped by traditional antivirus and security approaches. Addressing the antivirus and content security requirements of today's global, distributed enterprise requires a coordinated, comprehensive approach that enables IT managers to ensure a high level of protection while easing resource-intensive administration. The Trend Micro Enterprise Protection Strategy provides IT managers an industry-unique approach which incorporates coordinated delivery of products, services and expertise to address the damage caused by mixed-threat attacks and the need for a more efficient way of managing them enterprise-wide.

Business users today consider easy and transparent access to online business applications via intranets, extranets, and the Web indispensable. Mobile, offsite, and branch-office employees require remote access to critical business applications as well. Enterprise Protection Strategy supports the evolution of the enterprise by delivering timely updates and attack-specific policy recommendations at every stage of the outbreak lifecycle to help manage the explosive time, costs, and system damage associated with outbreaks.

APPENDIX: TREND MICRO ANTIVIRUS PRODUCTS

The following products and services help support Trend Micro Enterprise Protection Strategy.

Trend Micro Control Manager 2.5
Trend Micro Control Manager v.2.5 provides centralized management of Trend Micro antivirus and content security products and services throughout the network to address the entire outbreak lifecycle.

Issue	Trend Micro Enterprise Protection Strategy Solution
Networks are vulnerable before pattern files are available.	Medium and High Risk alerts provide early warning and detection services that address threats before new pattern files are distributed.
Administrators must decide how to handle malicious code and repair systems.	Cleanup templates and pattern files recommend actions to remove viruses and repair damage to infected systems. Administrators may accept or modify these recommendations to suit specific enterprise requirements.
Administrative control resides only at the central server, regardless of the location of the outbreak or the placement of other qualified personnel.	Flexible control features ensure that the most appropriate personnel address threats efficiently and effectively.

Policy recommendations provided by Trend Micro Control Manager during Medium and High Risk Alerts enable enterprises to take immediate defense precautions before virus pattern files are available to scan for the malicious code. These policy recommendations include the following:

- Stripping attachments by file type
- Deleting or quarantining email by subject or keyword
- Removing document macros
- Blocking certain HTTP commands to avoid denial-of-service attacks
- Blocking email altogether until virus pattern files are available (for particularly virulent threats)

Trend Micro Web Security Products

The following products provide security against malicious code that may enter the network through Web pages, applets, plug-ins, and other Web-based threats:

- InterScan VirusWall™ provides comprehensive virus detection and cleanup for all SMTP, HTTP and FTP traffic at the Internet gateway.
- InterScan VirusWall eManager™ is a plug-in for InterScan VirusWall that blocks spam, filters email content including embedded scripts and file attachments, and manages email deliveries for SMTP email servers.
- InterScan WebManager™ protects Web (HTTP) traffic from viruses and known malicious Java applets and Active X controls, and monitors and filters Web-browsing activity to address productivity and liability issues.
- InterScan WebProtect™ for ICAP (Internet Content Adaptation Protocol) provides virus protection at the Internet gateway for enterprises with Web caching solutions that support ICAP 1.0 from Network Appliance™ and BlueCoat Systems.

Trend Micro Messaging Security Products

The following products provide security against malicious code embedded in email messages or file attachments that enter through a traditional email server:

- InterScan™ Messaging Security Suite scans SMTP traffic as it enters the Internet gateway and provides content security policy mechanism to ensure the gateway is protected.
- ScanMail™ for Microsoft™ Exchange and ScanMail for Microsoft Exchange 2000 remove viruses from inbound and outbound email in real-time, performing file attachment blocking with no downtime, for Microsoft Exchange email servers.
- ScanMail eManager™ is a plug-in for ScanMail that provides spam blocking, message content filtering, and mail delivery management for Microsoft Exchange and Lotus Notes servers.

- ScanMail for Lotus Notes™ removes viruses from inbound and outbound email in real-time, performing file attachment blocking with no downtime, for the Lotus Notes environment.

Trend Micro File Server and Storage Security Products

The following products provide security against threats designed to harm data and application files residing on servers:

- ServerProtect™ for Windows NT™/NetWare offers centralized management and virus protection for Microsoft Windows NT and NetWare servers
- ServerProtect for Linux offers virus protection for Linux servers
- ServerProtect for Network Appliance™ offers centralized management and virus protection for Network Appliance storage devices.
- ServerProtect for EMC™ Celerra™ offers centralized management and virus protection for EMC storage devices.
- Trend Micro Damage Cleanup Server is a comprehensive service that helps clean and repair systems infected by Trojan viruses and worms without installing software on the client. It addresses the critical phase after a pattern file has been deployed, removing dangerous virus remnants that could re-attack the network.

Trend Micro Client Security Products

The following products provide client-based protection for user systems that connect to or otherwise access the enterprise network environment:

- OfficeScan™ Corporate Edition provides complete virus protection for servers, workstations, and email, including centralized, real-time virus infection reporting and notification and software configuration and updating.
- GateLock™ Corporate Edition (CE) combines antivirus, firewall, and intrusion detection capabilities into one, easy-to-use appliance to protect the remote workforce. Gatelock CE can be remotely deployed, monitored, and managed from a central location, making it easy for IT managers to maintain security for remote systems.

BIBLIOGRAPHY

Computer Economics, Computer Economics Malicious Code Attack Economic Impact Update – August 31, 2001, http://www.computereconomics.com/cei/news/codered.html.

Matt Curtin and Marcus J. Ranum, Firewalls FAQ, 1 December 2000,

ICSA Labs, ICSA Labs Computer Virus Prevalence Survey 2000

ICSA Labs, An Introduction to Intrusion Detection Assessment for System and Network Security Management, http://www.icsalabs.com/html/communities/ids/whitepaper/Intrusion1.pdf.

IDC, Antivirus Software: A Segmentation of the Market, August 2001.

ABOUT TREND MICRO

Trend Micro provides centrally controlled server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and managed service providers world-wide to stop viruses and other malicious code from a central point before these threats ever reach the desktop.

Trend Micro's corporate headquarters are located in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia. Trend Micro's North American headquarters are located in Cupertino, California. Trend Micro's products are sold directly and through a network of corporate, value-added resellers and managed service providers.

Evaluation copies of all Trend Micro products may be downloaded from Trend Micro's Web site, http://www.trendmicro.com.