



WHITE PAPER

FEBRUARY 2003

TREND MICRO, INC.
10101 N. DE ANZA BLVD.
CUPERTINO, CA 95014
T 800.228.5651 / 408.257.1500
F 408.257.2003
WWW.TRENDMICRO.COM

Trend Micro™ ServerProtect™ 5.5 For Microsoft™ Windows™

Managed Virus Protection for Enterprise-class Servers

TABLE OF CONTENTS

| | |
|----|--|
| 3 | Abstract |
| 4 | Trend Micro ServerProtect™ 5.5 |
| 4 | ServerProtect 5.5 Architecture |
| 5 | ServerProtect Virus Detection Technology |
| 7 | Central Deployment and Updates |
| 8 | Scalability |
| 8 | Trend Micro Enterprise Protection Strategy |
| 9 | Conclusion |
| 10 | About Trend Micro |

February, 2003
Trend Micro, Inc.

©2002 - 2003 by Trend Micro Incorporated.

All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of Trend Micro Incorporated. Trend Micro, the t-ball logo, ServerProtect, and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

ABSTRACT

Easy access to information is critical in today's fast-paced business environment. Corporations use servers to store, share, and distribute vast amounts of data. If one server becomes infected with a virus, it can quickly lead to a network-wide virus outbreak. A virus infestation on a server is a system administrator's worst nightmare. The cost of downtime and restoring networks is astronomical.

As the incidence of mixed-threat attacks continues to increase, the need arises for improved solutions to address these threats. Network administrators are confronted with the following questions:

- Is the antivirus software configured correctly on all servers?
- Can the status of all servers be viewed at any given time?
- Are there faster ways to eradicate viruses?
- How can the spread of a virus be contained?

This White Paper demonstrates how Trend Micro ServerProtect 5.5 addresses each of these ongoing IT management concerns.

ServerProtect 5.5 is an integral part of Trend Micro's Enterprise Protection Strategy; an approach for protecting resources across the enterprise through systematic prevention, detection, and cleanup of viruses and other malware.

TREND MICRO SERVERPROTECT 5.5

1. ICSA Labs Virus Prevalence Survey 2001, ICSA Labs, 2001

The virus problem facing corporations continues to worsen. ICSA¹ reported that in 2000, 36 percent of those reporting disasters estimated that servers were down one hour or less. By contrast, 65 percent of 2001's respondents reported downtime of one hour or less. The average server downtime was 14 hours.

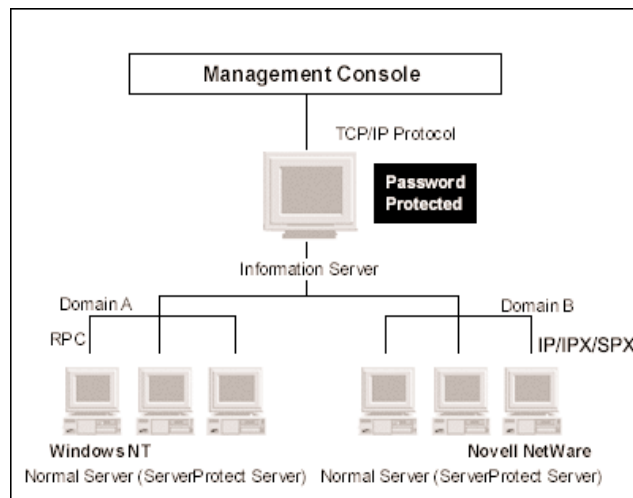
File servers are vulnerable; users can copy infected files to the server or run infected files on their workstations. The ideal antivirus program for file servers needs to feature centralized management capabilities to simplify the administrator's job, frequent automatic updates to detect the latest viruses, robust scanning options, and the ability to scale from a simple multisystem network to a large enterprise network.

ServerProtect delivers industry-certified virus protection. ServerProtect scans and detects viruses in real time and incorporates damage cleanup services to help remove malicious code and repair any system damage caused by them. Administrators can use one management console to centrally enforce, administer, and update the antivirus program on every server throughout an organization.

SERVER PROTECT 5.5 ARCHITECTURE

ServerProtect protects servers through a three-tier architecture: the Management Console, the Information Server, and the Normal Server. A normal server can be any server on the network on which ServerProtect is installed, for example, a file server or a FTP server. The Management Console is used to configure dedicated Information Servers, which then control the Normal Servers.

Figure 1. Three-tier Architecture



MANAGEMENT CONSOLE

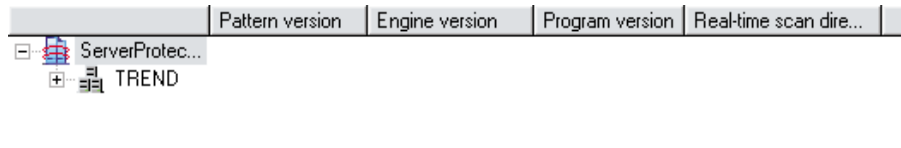
The ServerProtect Management Console provides network administrators with central control of multiple network servers and domains. The console enables administrators to simultaneously configure servers in the same domain and generate integrated virus incident reports for all servers. Options such as setting scans, tasks, updates, and reviewing logs, can be configured through the Management Console. This console provides access to every Normal Server on the network running ServerProtect.

Figure 2. ServerProtect Management Console



The browser tree displays the network components that the software protects, and includes a root (the ServerProtect product icon), branches (domains), and nodes (the ServerProtect Normal Servers). The header fields in the domain browser tree display useful information, such as the computer's operating system, virus pattern, scan engine, program versions, and real-time scan direction (Figure 3).

Figure 3. Domain Browser Tree Header Fields



INFORMATION SERVER

An Information Server is the main communication hub between the Management Console and the Normal Servers it manages. It simplifies control of Normal Servers by allowing administrators to send instructions and receive information from remote sites. Administrators configure the required information for each Normal Server on the Information Server, where all the configuration data can be shared and stored. Information Servers enable the Normal Servers to be configured according to the administrator's settings on the Management Console.

The Information Server also facilitates domain management. All servers in a domain can share both the same configurations and updates, thus minimizing bandwidth consumption.

NORMAL SERVER

The Normal Server is the first line of defense in ServerProtect. Normal Servers perform the actual antivirus functions of the system, and are managed by an Information Server.

SERVERPROTECT VIRUS DETECTION TECHNOLOGY

ServerProtect features the following virus detection technologies:

PATTERN MATCHING

ServerProtect draws upon an extensive database of virus patterns to identify known virus signatures using a process called pattern matching. Key areas of suspect files are examined for telltale signs of virus code and compared against thousands of virus signatures that Trend Micro has on record.

MACROTRAP

ServerProtect includes MacroTrap technology to guard against macro viruses in Microsoft Office files and templates. Macro viruses are harbored in files that are commonly passed around via email and therefore, these kinds of viruses spread easily. Macro virus code is typically contained as a part of the invisible template, for example, *.dot in Microsoft Word, that travels with the document. MacroTrap performs a rule-based examination of all Macro code that is saved in association with a document.

COMPRESSED FILES

Compressed files are sometimes used to "smuggle" viruses into protected networks or computers. The Trend Micro scan engine can scan files inside compressed archives. It can even scan compressed files that are composed of other compressed files - up to a maximum of five compression layers.

OLE LAYER SCAN

Microsoft Object Linking and Embedding (OLE) allows embedding of Microsoft Office files within themselves, for example a Microsoft Word document inside an Excel spreadsheet, which in turn is embedded in a PowerPoint presentation. Whilst OLE offers a large number of benefits, it can lead to potential infection. To address this issue, Trend Micro added a new scan feature, OLE Layer Scan.

INTELLISCAN

IntelliScan is new method of identifying which files to scan, that is both more secure and efficient than the standard "Scan all files" option. For executable files, for example, .zip, .exe, the true file type is determined by the file content. In the event that a file is not executable, for example, .txt, IntelliScan will use the file header to verify the true file type. One of the benefits of IntelliScan is that scan time is significantly less than that of other files scans. This is because only the files with a greater risk of being infected are scanned.

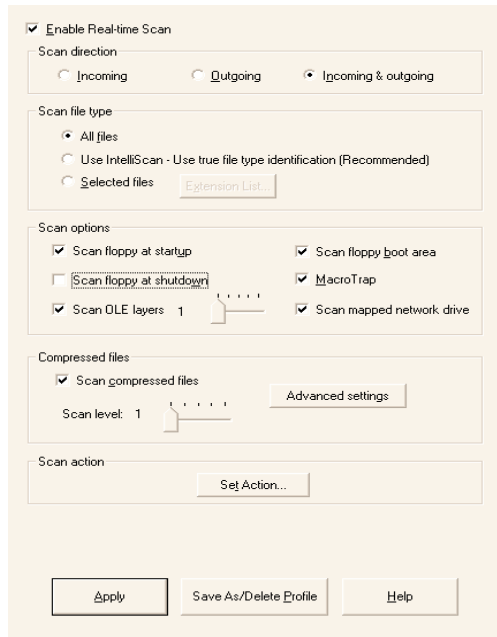
ACTIVEACTION

ActiveAction is a set of pre-configured scan actions that can be performed on viruses and other types of malware.

REAL-TIME SCAN AND ON-DEMAND SCAN

ServerProtect features two powerful scan functions: Real-time Scan and Scan Now.

Figure 4. Real-time Scan



Real-time Scan runs continuously on a server. All "open/close" file events on the server are monitored and infected files are prevented for being copied to or from the server (Figure 4).

Scan Now is a manual virus scan and can be used to check a machine that is suspected of being exposed to a virus, or about which, immediate information is required.

CENTRAL DEPLOYMENT AND UPDATES

A successful antivirus policy depends on the deployment of program files, scan engines, and pattern files that can deal with the latest virus threats. ServerProtect enables administrators to develop a deployment scheme based on their specific enterprise network topology. Administrators can also install ServerProtect software to new servers via the Management Console. This efficient approach simplifies the maintenance of Trend Micro software and reduces the total cost of a network's antivirus security.

SCALABILITY

If there are multiple ServerProtect Information Servers installed on a network, administrators can use Trend Micro Control Manager™ to collectively manage all servers. In keeping with other Trend Micro enterprise products, ServerProtect is designed for complete integration with Trend Micro Control Manager. In addition, other Trend Micro products, for example, OfficeScan and ScanMail for Microsoft Exchange can be jointly managed via Trend Micro Control Manager.

Figure 4. ServerProtect via the Trend Micro Control Manager Console



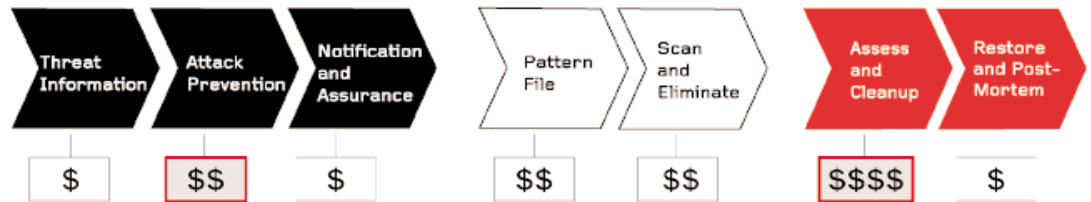
TREND MICRO ENTERPRISE PROTECTION STRATEGY

Most antivirus vendors focus solely on preventing attacks, and do not carefully consider how to manage virus outbreaks. The ability to manage viruses and prevent them from spreading greatly reduces the time and cost required to restore networks and repair systems.

ServerProtect is a key component of the Trend Micro Enterprise Protection Strategy, which delivers a coordinated, multi-layered defense against viruses and virus outbreaks during each phase of the outbreak life cycle. The outbreak prevention phase is the critical time when an outbreak has been identified and a pattern file is not yet available. When an outbreak occurs, the Outbreak Prevention Service enables administrators to receive policy recommendations from Trend Micro. These policy recommendations are designed to thwart new viruses and contain the spread of virus attacks until a fully tested pattern file is available. The Outbreak Prevention Service also provides administrators with information on new attacks as soon as they are identified; it sends a notice to every client machine, enabling the Outbreak Prevention mode. Systems in Outbreak Prevention mode can then be configured to block shared folders and specified ports, and/or deny writing certain file types to specified directories, further containing the virus threat.

Today the process of cleaning the network of virus remnants is incredibly time consuming and expensive, because most networks rely on a manual cleanup and restoration process. Trend Micro offers Damage Cleanup Services as part of the Enterprise Protection Strategy. Damage Cleanup Services terminates Trojan-related processes, and deletes files that the Trojan "drops" into the system, automating this part of the cleanup process.

Figure 6. Trend Micro offers services through ServerProtect that are designed to automate the cleanup process and reduce costs.



CROSS-PLATFORM PROTECTION

ServerProtect 5.5 provides broad coverage of server systems including Microsoft Windows™ .NET/2000/ NT servers. Additionally, ServerProtect is designed for the following storage platforms: Network Appliance filer, EMC™ NAS, IBM™ NAS, and Compaq™ NAS.

CERTIFICATIONS

ServerProtect has the following certifications: Microsoft Windows 2000 Server and .NET, IBM Server, Compaq Server, and Citrix MetaFrame™. In addition, VeriTest² has certified ServerProtect 5.31 with Windows 2000 Standard/Advanced Datacenter server qualifications.

CONCLUSION

ServerProtect 5.5 incorporates advanced virus detection technology designed to protect an enterprise's most precious assets; its information. ServerProtect enables network administrators to manage multiple Windows servers from a single, portable management console. ServerProtect simplifies the management process of antivirus software, allowing administrators to save time and focus on other network needs. Additionally, ServerProtect has been certified by several leading IT vendors.

Trend Micro Control Manager provides centralized administration of multiple Trend Micro products and with Outbreak Prevention Services, helps administrators manage virus outbreaks.

From attack-specific policy recommendations to cleanup and restoration templates, the Enterprise Protection Strategy helps organizations continuously adapt as threats evolve.

2.View full report at:
<http://cert.veritest.com>

ABOUT TREND MICRO INCORPORATED

Trend Micro Incorporated is a leader in network antivirus and Internet content security software and services. The Tokyo-based corporation has business units worldwide. Trend Micro products are sold in North America through corporate and value-added resellers. For additional information and evaluation copies of all Trend Micro products, visit our Web site, <http://www.trendmicro.com>