



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™ 1.1 Linux™ Edition

Protecting Files Where They Reside

TABLE OF CONTENTS

3	At Risk: Linux Servers for Windows Networks
4	Linux: A Mainstream Choice
4	ServerProtect Virus Detection Technology
6	Web-based Remote Management
6	Real-time and Scheduled Scanning
7	Automated and Manual Updates
7	Notification of Virus Outbreaks
8	Detailed and Easy-to-Maintain Logs
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.

AT RISK: LINUX SERVERS FOR WINDOWS NETWORKS

Many Linux systems are used as file servers in Microsoft™ Windows™-based networks. Without virus protection at the server level, Windows viruses can quickly spread across the network through shared files. In addition, viruses that specifically attack the Linux platform have increased in frequency and severity. Trojan viruses that infect ELF binaries can cause distributed denial of service (DDOS) attacks, resulting in havoc for administrators. Such viruses use the User Data Protocol (UDP) to execute the attack, and take advantage of a buffer overflow vulnerability in OpenSSL 0.9.6d, 0.9.7-beta2 and earlier versions.

Real-time antivirus software uses kernel-hooking methods to monitor for virus activities. However, with the frequent Linux kernel updates, the software needs to be recompiled each time in order to function correctly. Antivirus heuristic rules and signature files also need to be kept up-to-date to ensure comprehensive protection. The manual application of these tasks is both tedious and time consuming.

Trend Micro™ ServerProtect™ Linux Edition offers comprehensive virus protection for Linux-based systems, including file servers, workstations, FTP servers, and Web servers.

Its features include:

- Cross-platform compliancy; to help protect Windows systems from becoming infected via Linux servers.
- Automated updates for the most recent program and virus pattern files.
- Real-time scanning to prevent malicious code from executing before it is run.

LINUX: A MAINSTREAM CHOICE

1. Linux Operating Environments Market
to Reach \$280 Million by 2006....
www.idc.com

IDC¹ expects spending on Linux operating environments to increase over the next five years from \$80 million in 2001 to \$280 million in 2006, a 28 percent compound annual growth rate. IDC research shows this surge in client operating environment shipments was driven largely by growth in Asia and the Pacific, which contributed 34 percent of total new Linux client and server operating environments license shipments in 2001.

According to the same recent IDC press release, Linux has become a "mainstream choice for many infrastructure workloads" because the software is either freely available or can be deployed at low cost. Furthermore, Linux is often packaged with open source software such as Samba, Apache for Web services, and PostgreSQL for data management, making it a highly functional and cost-effective environment.

However, many IT administrators do not carefully consider the possibility of cross-platform virus infection. Work environments are often composed of a mix of Linux and non-Linux platforms - the risk of Linux boxes becoming virus-havens, serving as launch pads for outbreaks within networks, is a concern. If a network is composed of Windows machines operating behind Linux servers that are not protected, the file servers could be used to propagate Windows viruses throughout the network. In addition, standard FTP and Web servers often come under attack from malicious code and other viruses.

LINUX APPLICATIONS

SAMBA is typically used to share information between file-sharing server and Windows machines. SAMBA is a suite of programs that enables clients to access a server's file space and printers via the SMB (Session Message Block) protocol. ServerProtect is designed to protect both Linux file servers and other Windows systems using Linux servers for file sharing.

SERVER PROTECT VIRUS DETECTION TECHNOLOGY

Server Protect Linux Edition features ICSA certification for reliable scanning and uses the following technologies to detect different forms of malware:

PATTERN MATCHING

With Pattern Matching, key areas of suspect files are examined for telltale strings of malware code and compared with thousands of virus signatures that Trend Micro has on record. For polymorphic or mutation viruses, the ServerProtect scan engine permits suspicious files to execute in a protected area for decryption. ServerProtect then scans the entire file, and looks for strings of mutation-virus code.

MACROTRAP

Macro viruses are application specific, and are not confined to a particular operating system. If an operating system supports the macro's application, there is a chance of infection. Given the cross-platform interoperability, combined with the growing popularity of the Internet, and the increasing power of macro languages, the magnitude of the threat posed by these viruses is obvious.

MacroTrap performs a rule-based examination of all macro code that is saved in association with a document. Macro virus code is typically contained as part of an invisible template (for example, *.dot in Microsoft Word) that travels with the document. MacroTrap checks the template for signs of a macro virus by seeking out instructions that perform virus-like activity. Examples of this behavior include copying parts of the template to other templates (replication), and execution of harmful commands (destruction).

COMPRESSED FILE SCANNING

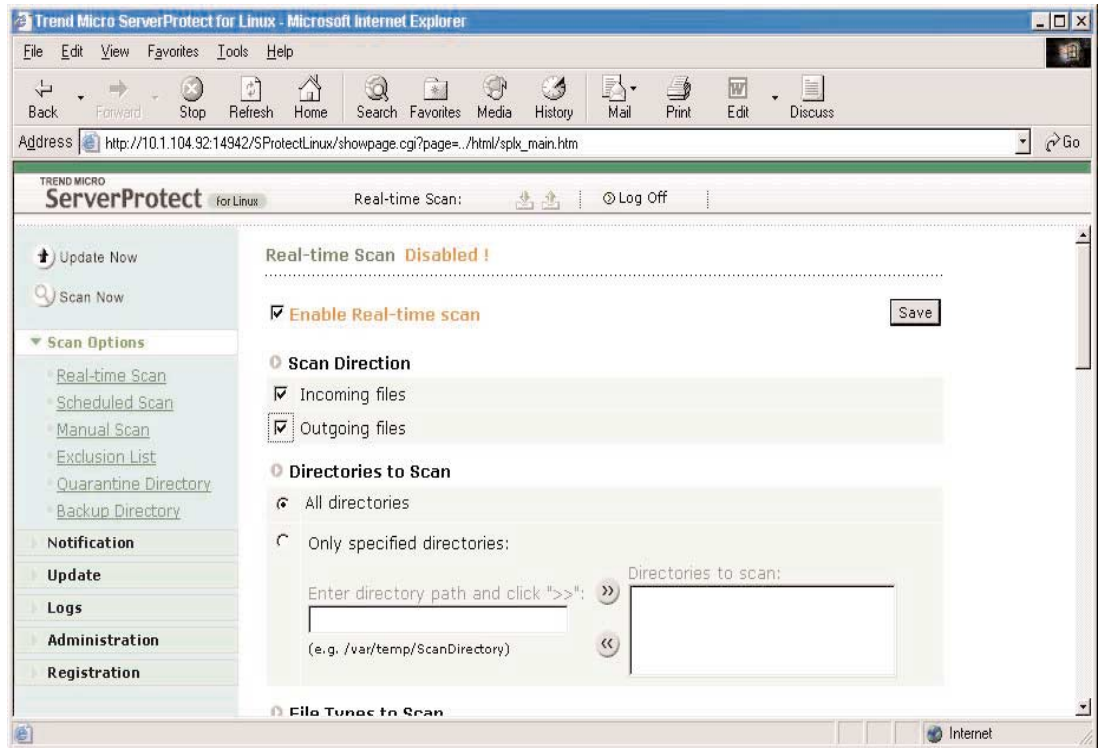
Compressed files are often the preferred file formats for distribution via email or the Internet. Unless an antivirus application is specially equipped to handle compressed files, there is a strong possibility that viruses and other malware may be "smuggled" into a network inside these files. The ServerProtect scan engine can scan inside archives and compressed files. It can even detect viruses in compressed files and archives composed of other compressed files - up to five compression layers deep.

In addition to the above features, ServerProtect incorporates ScriptTrap technology, which detects viruses written in script programming languages such as Visual Basic Script or JavaScript™. ServerProtect also performs kernel-level scanning for viruses and malicious code within the Linux operating system to minimize performance degradation. Trend Micro was one of the first vendors to provide this capability.

WEB-BASED REMOTE MANAGEMENT

ServerProtect is configured via a browser-based console. This allows administrators to control the application from any location with an Internet connection. The console can be accessed through both Microsoft Internet Explorer™ and Netscape Navigator™ (Figure1).

Figure 1. ServerProtect Linux Edition:
Web-based Management Console



REAL-TIME AND SCHEDULED SCANNING

Real-time scanning checks files or viruses whenever they are accessed, for example, when files are copied or read, and can detect viruses in both incoming and outgoing files. Incoming files are those that are being placed on your server, whereas outgoing files are copied or moved from your server to another location.

Scheduled scanning performs a thorough scan of your Linux machine at regular, user specified, intervals. Scans can be scheduled after office hours so as not to interfere with normal operations.

The following Scheduled scanning options are provided:

- **DIRECTORIES TO SCAN:** You can restrict scanning to specific directories.
- **FILE TYPES TO SCAN:** You can limit scanning to specific file types.
- **ACTION WHEN VIRUSES ARE FOUND:** You can select the appropriate action (clean, quarantine, rename, delete, or pass) to be taken when a virus, or other malware, is detected.

AUTOMATED AND MANUAL UPDATES

Administrators have a choice of automated or manual virus pattern and scan engine files updates. ServerProtect downloads the updates over the Internet from the Trend Micro ActiveUpdate servers.

VIRUS PATTERN FILE: This file contains hundreds of malware signatures, for example, viruses and Trojans. Trend Micro updates pattern files at least once a week to ensure protection against the latest threats.

SCAN ENGINE: This component performs the actual scanning and cleaning functions. It employs pattern-matching technology, using signatures in the pattern file to detect viruses, Trojans, and malicious programs. A new scan engine is issued to incorporate new technology, and is therefore only updated occasionally.

Manual Updates are a particularly useful feature during virus outbreaks, when updates do not arrive according to a definite schedule.

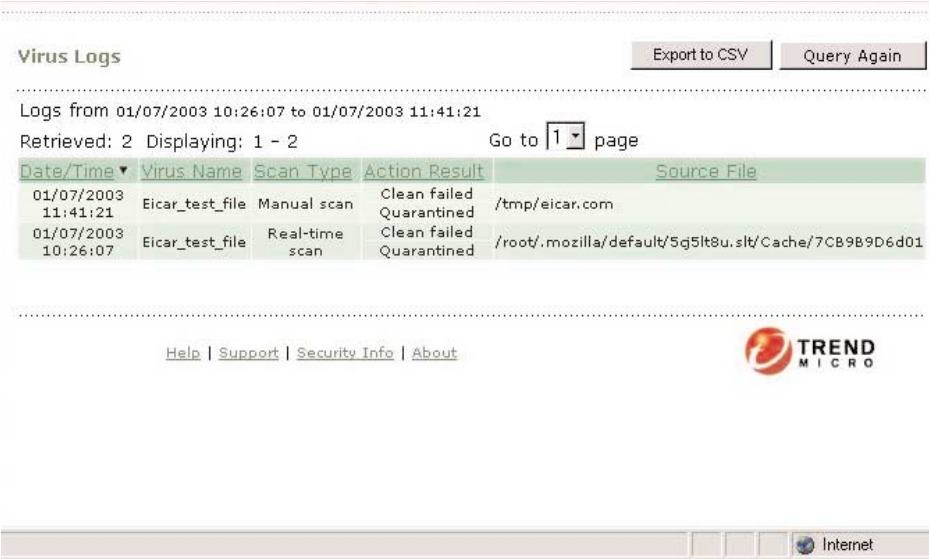
NOTIFICATION OF VIRUS OUTBREAKS

ServerProtect can alert administrators to virus outbreaks, infections, and system configuration changes, using a variety of notification methods, including email and/or Simple Network Management Protocol (SNMP). Notifications can be sent to several individuals at once. This allows administrators to stay on top of developing virus situations.

DETAILED AND EASY-TO-MAINTAIN LOGS

Administrators can view and export comprehensive logs about system and/or antivirus activities. Scan Logs record information about scans performed or attempted. Virus logs, on the other hand, keep track of viruses that were encountered and the measures taken. With ServerProtect, administrators have the options of deleting logs either manually or automatically, to avoid the log files becoming too large and unmanageable.

Figure 2. Virus Logs



The screenshot displays the 'Virus Logs' interface. At the top right, there are buttons for 'Export to CSV' and 'Query Again'. Below the title, it shows the log range: 'Logs from 01/07/2003 10:26:07 to 01/07/2003 11:41:21'. It also indicates 'Retrieved: 2 Displaying: 1 - 2' and a 'Go to 1 page' dropdown menu. The main content is a table with the following data:

Date/Time	Virus Name	Scan Type	Action Result	Source File
01/07/2003 11:41:21	Eicar_test_file	Manual scan	Clean failed Quarantined	/tmp/eicar.com
01/07/2003 10:26:07	Eicar_test_file	Real-time scan	Clean failed Quarantined	/root/.mozilla/default/5q5lt8u.slt/Cache/7CB9B9D6d01

At the bottom of the interface, there are links for 'Help | Support | Security Info | About' and the Trend Micro logo. A status bar at the very bottom shows 'Internet'.

Administrators can specify the query criteria for the logs that they want to view.

The parameters include:

- **LOGS FOR** - Select among commonly specified date ranges.
- **START DATE** - Specify the earliest log you want to view.
- **END DATE** - Specify the latest log you want to view.
- **SORT LOGS BY** - Specify the order and grouping of the logs.
- **LOGS PER PAGE** - Select the number of logs to be displayed at a time.

CONCLUSION

Trend Micro ServerProtect Linux Edition has been specifically engineered to protect Linux systems and reduce the threat of cross-platform contamination across a network. Simplifying the management process of antivirus software enables administrators to focus on other network needs. A Web-based management console allows remote control of the application from locations with Internet connections. The security and integrity of data on file servers is paramount to corporations. ServerProtect incorporates highly advanced virus detection technology designed to secure a corporation's information assets.

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>