



**WHITE PAPER**

# Ensuring Data Integrity with Trend Micro ServerProtect<sup>®</sup> for Network Appliance<sup>™</sup> filers

---

**Trend Micro, Inc.**

10101 N. De Anza Blvd.

Cupertino, CA 95014

Phone: 1(800) 228-5651 / 1 (408) 257-1500

Fax: 1(408) 257-2003

Web: [www.trendmicro.com](http://www.trendmicro.com) or [www.antivirus.com](http://www.antivirus.com)



## Table of Contents

<b>ABSTRACT.....</b>	<b>3</b>
<b>DATA INTEGRITY IN A STORAGE SYSTEM.....</b>	<b>4</b>
<b>SERVERPROTECT FOR NETWORK APPLIANCE FILER.....</b>	<b>4</b>
<b>ARCHITECTURE OF SERVERPROTECT FOR NETWORK APPLIANCE FILERS .....</b>	<b>5</b>
<b>BENEFITS FOR NETWORK APPLIANCE FILERS .....</b>	<b>7</b>
<b>SUMMARY .....</b>	<b>9</b>
<b>THE TREND MICRO FAMILY OF PRODUCTS .....</b>	<b>10</b>
<b>ABOUT TREND MICRO .....</b>	<b>12</b>

**August 2001**  
**Trend Micro, Inc.**

©2001 by Trend Micro, Inc.

*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 the publisher. InterScan, eManager, Trend VCS, ScanMail, ServerProtect, OfficeScan, MacroTrap, Active Update, and SmartScan are trademarks of Trend Micro, Inc and registered in various jurisdictions worldwide. All other company and product names are trademarks or registered trademarks of their respective owners.*

## Ensuring Data Integrity with Trend Micro ServerProtect® for Network Appliance™ filers

### **Abstract**

---

Most of the data storage industry has recognized the growing need for an antivirus solution for storage devices. Networked storage devices provide convenient data access, centralized file storage, and powerful data management solutions for the enterprise. Because a company's most precious assets are contained in its information, it is essential that data integrity is ensured and that data itself is kept virus-free.

Trend Micro ServerProtect® for Network Appliance™ filers provides a comprehensive antivirus solution for Network Appliance filers. Managed through an intuitive, portable Web-based console, the software provides centralized virus scanning, pattern updates, event reporting, and antivirus configuration. Virus scanning takes place on separate scan servers running Windows 2000/NT. In addition, multiple ServerProtect scan servers can be registered with one filer to provide better scan performance.

ServerProtect for Network Appliance filers works with Network Appliance filers running Network Appliance's proprietary operating system Data ONTAP 6.1 or above. Designed for easier virus management, ServerProtect for Network Appliance filers is equipped with centralized management tools. Using intelligent scanning technology, the software ensures the integrity of data stored in a Network Appliance filer.

This document provides an overview of ServerProtect 5.3 for Network Appliance filers, including a discussion of product architecture and product features.

## **Data Integrity in a Storage System**

---

Until recently most viruses spread primarily via floppy disk, but the Internet has provided a new virus distribution mechanism. Email is now an important business communication tool and viruses attached to email messages can infect an entire enterprise in a matter of minutes, costing companies millions of dollars annually in productivity loss and clean-up expenses. Viruses won't be going away any time soon. More than 500 new viruses are created every month, according to TruSecure, formerly the International Computer Security Association (ICSA). Most organizations deal regularly with virus outbreaks leaving no one who works with computers is immune.

Security and data integrity are very important for a storage system. A single virus-infected file in a storage system such as Network Appliance filers, can be responsible for infecting large amounts of data, which can result in a disastrous breakdown of storage services and data management. The infected file can be retrieved by any number of storage users and can eventually result in the virus spreading to client systems.

### **ServerProtect for Network Appliance filer**

---

According to IDC, revenue from disk storage systems is expected to grow to \$6.57 billion by 2003. Already there has been a significant increase from \$540 million in 1998, the predicted growth rate is almost 86% per year from 1999 to 2003. In addition, storage system customers are actively driving their requirements for an antivirus product for their storage devices. Trend Micro has been closely working with Network Appliance to provide virus protection for Network Appliance filers.

Trend Micro's ServerProtect for Network Appliance filers provides a comprehensive antivirus solution for Network Appliance filers. Managed through an intuitive, portable Web-based console, the software provides centralized virus scanning, pattern updates, event reporting and antivirus configuration. Virus scanning takes place on separate scan servers running Windows 2000/NT. Multiple ServerProtect scan servers can be registered with one filer to provide better scan performance.

Management of ServerProtect for Network Appliance filers can be done with limited resources and budget. Administrators can easily direct such virus maintenance tasks as configuring scanning, pattern and program file updates, compiling virus logs, and setting parameters for real-time scanning. ServerProtect for Network Appliance filers works with Network Appliance's proprietary operating system Data ONTAP 6.1 or above. The connection between ServerProtect scan servers and the filer is monitored and able to reconnect automatically.

## Architecture of ServerProtect for Network Appliance Filers

---

Virus scanning takes place in on-access mode and in one or more separate scan servers running Windows 2000 or NT4. For this purpose, the filer must have Network Appliance proprietary operating system Data ONTAP 6.1 or above, so the filer can interact with the scan servers of ServerProtect for Network Appliance filers. Figure 1 presents basic ideas on how data in the filers is protected from virus infections.

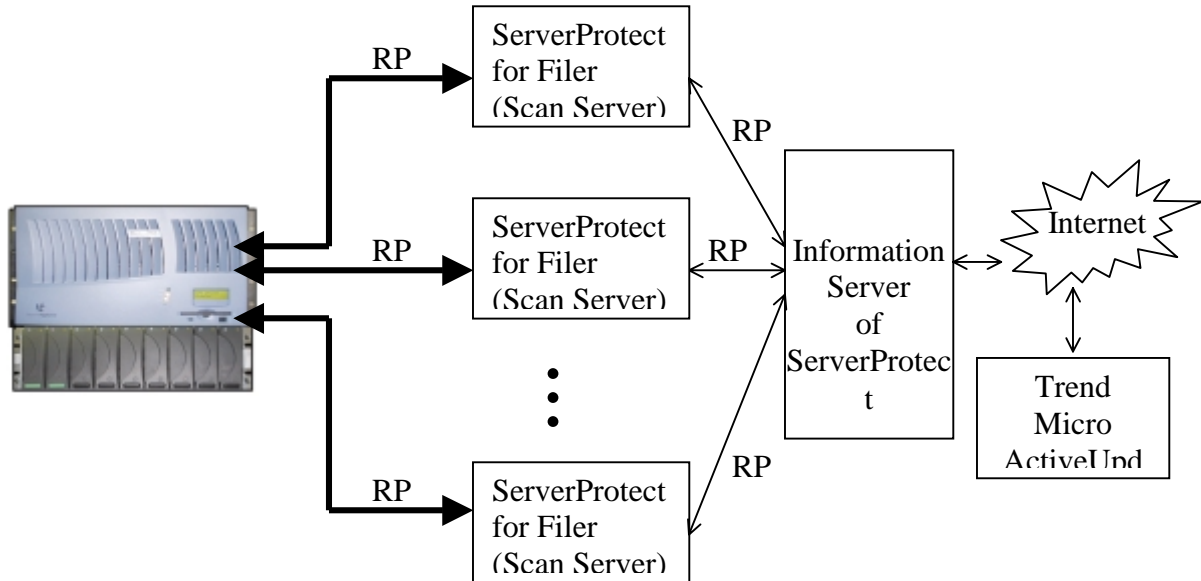


**Figure 1:** *The Work Flow of Virus Scanning*

When a client user attempts to access a file in the filers or store a new file to the filers, the filer will be triggered to perform virus checking. If a file's extension name appears on the list of file types predetermined by the Administrator, and the file has not been previously scanned, the filer will make a scan request to one of the registered scan servers. The result of the scan will then be passed back to the filer from the scan server and the user is, according to the scan result, either allowed to open/save the file or denied access to the file.

ServerProtect for Network Appliance filers communicates with the filers via Remote Procedure Call (RPC). The scan server performs the following functions:

- Register itself with the filers as a scan server to inform the filers of the availability
- Watch for the filers' requests of file scanning
- Return scan results to the filers
- Answer any queries from the filers
- Inform the filers of any pattern file or scan engine updates
- Communicate with the filers to check the connection between the scan server and the filers



**Figure 2.** Architecture of ServerProtect for Network Appliance filers

The Information Server is a communication hub for coordinating antivirus activities within its domains. It provides system administrators with a single point of management for the Scan Servers assigned to the filers thus relieving the administrators of the tedious task of directly communicating with every individual Scan Server. Note that each Scan Server is dedicated to a single filer. However, one filer can be registered with multiple scan servers.

Scanning is done on a separate scan server rather than on the filer, so that the filer's processing power will not be consumed for virus scanning. There is constant communication between the filer and the scan server to monitor the connection, handle scan requests, and return the scan results.

To optimize performance, the design works to minimize the traffic and increase scan performance with the following features:

- Administrators may configure the filer to send files of specified extensions to the scan server for virus checking to best use available bandwidth
- Files in the filer will be marked as *clean* if it has been scanned before and required no modification. Files marked as *clean* will not be sent to any scan server. A Gigabit connection between the filers and the scan server is recommended
- Adding and registering multiple scan servers with the filer evenly distributes the workload among the registered scan servers. Files to be scanned are sent to scan servers in a round-robin fashion, rotating in an orderly way which scan servers receives a file to be scanned.

- Clean files that have been scanned in the scan server will not be passed back to the filer. Only the scan results and files that have been disinfected will be returned to the filer.

---

**Note:** If a new virus pattern file becomes available on the scan servers, the administrator can reset the cached information on the filer to force it to scan all applicable files including those that were scanned with the old virus pattern file

---

## **Benefits for Network Appliance Filers**

---

### **Scalability and High Performance**

To increase scalability and increase performance levels, multiple ServerProtect scan servers can be registered with the filers at any time. An increased number of scan servers registered to a filer will increase the scan performance for the filer. Once a ServerProtect scan server is registered to a filer, connection and reconnection between the server and the filer is made automatically. Whenever the server detects any communication disconnection, it will send signals to the filer to reconnect.

### **Comprehensive Log Reports**

ServerProtect provides comprehensive log reports to enable the user to track and manage a large number of antivirus events including virus infection, pattern or program updates, virus alerts, running tasks, scan activity, and modifications from a single console. This simplifies the tasks of virus management and product configuration for administrators.

### **Centralized Management via Information Server**

ServerProtect Information Server provides simple management of multiple Windows NT scan servers from a single, portable management console. The multiple scan servers can be grouped into a logical domain. It is recommended to put scan servers for one filer into one domain.

The ServerProtect management console enables administrators to configure servers in the same domain simultaneously, and generate integrated virus incident reports from all scan servers. This consolidates status information if there are multiple filers and multiple scan servers for each filer.

### **Scan Engine and Virus Pattern Updates**

The Information Server of ServerProtect can be configured to download virus pattern file and scan engine updates automatically from Trend Micro's ActiveUpdate server and then distributes them to designated scan servers. The distribution of new virus pattern files

uses an incremental update mechanism, whereby a server only needs to download the new virus signatures that have been added since the last update. This highly efficient approach saves download time and preserves network bandwidth.

### **Virus Scanning to Ensure Data Integrity**

ServerProtect uses the latest Trend Micro proprietary scan engine. The engine uses both rule-based and pattern recognition technology to detect and remove both known and unknown viruses, including all “In-the-Wild” viruses. The engine recursively scans inside files compressed with the following compression algorithms: PKZIP, PKZIP\_SFX, LHA, LHA\_SFX, ARJ, ARJ\_SFX, CABANET, TAR, GUN ZIP, RAR, PKLITE, LZEXE, DIET, MSCOMPRESS, UNIX, PACKED, UNIX COMPACTED, UNIX LZW, UUENCODE, BINHEX, BASE64, and others.

### **Configurable Actions for Infected Files**

The Information Server provides GUIs for users to configure the action a scan server takes on an infected file.

Choices include:

- Quarantine the infected file
- Perform clean with a backup for cleanable viruses
- Perform clean without a backup
- Delete the infected file

### **Notification of Program Events**

ServerProtect for Network Appliance filers sends alerts to administrators with regard to potentially serious situations in their system. An alert will be issued in response to the following conditions: virus infections and an out-of-date virus pattern, or any problems with pattern/engine file distributions. Alerts can be sent via a message box, pager, printer, Internet email, SNMP trap, and written to the Windows NT event log.

### **Comprehensive Built-in Support**

ServerProtect provides intelligent help that recommends solutions to virus-related problems, and the on-line virus encyclopedia provides detailed descriptions of thousands of viruses.

## **Summary**

---

Security and data integrity for a storage system are very important. A storage system such as a Network Appliance filer will be vulnerable to virus attacks if the storage device is without virus protection. Moreover, a virus-infected filer can become a source of infection for other client systems as users retrieve the files.

Trend Micro proactively delivers comprehensive solutions to virus protection for storage devices. In addition, storage system customers are actively driving their requirements for an antivirus product for their storage devices. Trend Micro has been working closely with Network Appliance to provide virus protection for Network Appliance filers.

ServerProtect for Network Appliance filers provides a comprehensive antivirus solution for Network Appliance filers. Managed through an intuitive, portable Web-based console, the software provides centralized virus scanning, pattern updates, event reporting, and antivirus configuration. Virus scanning takes place on separate scan servers running Windows 2000/NT. Multiple ServerProtect scan servers can be registered with one filer to provide better scan performance.



### **File/Application Servers**

At the file/application server, Trend Micro ServerProtect™ for NT or NetWare prevents viruses from residing on general-purpose servers — preventing them from distributing viruses to workstations.

### **Desktop/mobile client workstations**

At desktop and mobile client workstations, Trend Micro OfficeScan™ Corporate Edition completes enterprise virus protection by guarding against infected floppy disks, remote dial-up modem, and other electronic access that can allow viruses to bypass network virus protection.

### **Trend VCS centralizes complete enterprise virus control**

Trend Micro antivirus products for the enterprise are integrated into the Trend Virus Control System (Trend VCS™) a Web-based console that may be used locally or remotely with equal ease. Through Trend VCS, network administrators can configure antivirus applications, update virus pattern files, monitor and receive virus alerts, and control most aspects of Trend Micro's server-based virus protection throughout the enterprise regardless of network complexity, server location, or platform, from a single interface.

### **Test drive the Trend Micro Enterprise Solution**

All Trend Micro products may also be easily downloaded for a 30-day evaluation at <http://www.antivirus.com/>.

## **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 service providers worldwide to stop viruses and other malicious code from a central point before they ever reach the desktop. Trend Micro's corporate headquarters is located in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia. Trend Micro's North American headquarters is located in Cupertino, CA. Trend Micro's products are sold directly and through a network of corporate, value-added resellers and service providers. Evaluation copies of all of Trend Micro's products may be downloaded from its award-winning Web site, <http://www.antivirus.com> or <http://www.trendmicro.com/>

