



WHITE PAPER

**Securing Data
in Network Attached Storage (NAS) Environments:
ServerProtect[®] for NAS**

Trend Micro, Inc.
10101 N. De Anza Blvd., 2nd Floor
Cupertino, CA 95014

Phone: 1-800-228-5651 / 408-257-1500
Fax: 408-257-2003
Web: www.antivirus.com or www.trendmicro.com

Table of Contents

ABSTRACT.....	3
THE STORAGE BOOM.....	3
VIRUSES AND MALICIOUS CODE AT LARGE.....	5
THREATS TO STORED DATA	6
TREND MICRO'S SOLUTION.....	6
SERVERPROTECT'S THREE-TIERED ARCHITECTURE.....	7
FEATURES AND BENEFITS FOR NAS SOLUTIONS	10
AUTOMATIC UPDATING.....	10
CURRENT VERSIONS OF SERVERPROTECT FOR NAS	12
SUMMARY.....	12
THE TREND MICRO FAMILY OF PRODUCTS	14
ABOUT TREND MICRO	15

**July 2001
Trend Micro, Inc.**

©2001 by Trend Micro, Inc., 10101 North De Anza Blvd., 2nd Floor, Cupertino, CA 95014

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 or registered trademarks of Trend Micro, Inc. All other company and product names are trademarks or registered trademarks of their respective owners.

Securing Data in Network Attached Storage Environments: ServerProtect® for NAS

Abstract

Data storage has become a vital, fast-growing part of the enterprise IT environment, as new business initiatives drive companies to accumulate vast amounts of information. To address the booming demand for greater shared storage capacity, leading vendors have developed increasingly robust data management solutions based on innovative new storage architectures, including network attached storage (NAS) and storage area network (SAN) technologies.

As enterprises make use of these advanced solutions to add scalable, high-performance storage systems, they must take care not to compromise network security standards. Network attached storage devices and the data they contain are vulnerable to attacks by viruses, worms and other forms of hostile code. Antivirus protection is an essential precaution, both to safeguard the integrity of stored data and to prevent hostile code from spreading to other parts of the network via the storage system. A responsible enterprise antivirus policy demands a dedicated antivirus solution for network attached storage.

Trend Micro, a long-standing leader in enterprise virus protection, provides a multi-layered defense for networks, covering all access points from the desktop to the Internet gateway. However, solutions at the firewall, email server or desktop are not ideal for protecting stored data, and relying on them could be risky. For this reason, Trend Micro has augmented its comprehensive range of solutions to include dedicated protection for the leading network attached storage solutions. By modifying and enhancing its award-winning ServerProtect® software to accommodate the NAS architecture and work with proprietary operating systems, Trend Micro currently offers antivirus solutions tailored to protect data on NAS appliances, including EMC's Celerra File Servers and Network Appliance's NetApp® filer storage appliances. These and other vendors have cooperated closely with Trend Micro to ensure the seamless interoperation of virus protection and the storage system.

The storage boom

Businesses now demand constant access to vast pools of shared data, such as inventory, customer records and employee databases. Critical applications, such as email, and critical resources, such as Web servers, also require increasing amounts of storage to serve the needs of the business. Moreover, as companies adopt new technologies to improve productivity, they are expanding high-speed Internet access, building intranets, implementing more complex software applications, and working with more media-rich forms of content. The result has been an explosion in the quantity of data being generated, stored and accessed.

Forrester Research recently looked at the storage requirements of fifty major corporations and found they were growing by an average of 52% in 2001. Other analysts project future corporate data storage requirements to grow by 80% to 100% per year until 2005. IDC projects that the total volume of stored electronic data, estimated at 180,000 terabytes in 1999, will rise more than tenfold to 2 million terabytes by 2003. This incredible demand has shaken up the storage market and spurred the rise of new, more powerful architectures.

What is Network Attached Storage (NAS)?

The traditional model for storage involves a hard disk drive and a disk array or a RAID system attached directly to a server or desktop machine. Known as Direct Attached Storage (DAS), this model is still in widespread use, but it will not be able to meet the needs of the future. Because it disperses data widely among many servers, the DAS model is inefficient and poorly-suited for managing mass storage in a network environment. Two new concepts which have begun to displace it are network attached storage (NAS) and the storage area network. (SAN).

NAS is system-independent, shareable storage that connects directly to the network and is accessible to heterogeneous servers and client computers (i.e. running Unix, Windows NT/2000, Netware, Linux etc.). NAS appliances are essentially specialized servers optimized for sharing files over networks and among different platforms. By simply attaching such devices to the network, IT departments can quickly and easily expand network storage capacity. Specialized designs help to improve efficiency and control IT expenses.

While integration with the network is one of the strengths of the NAS architecture, it also leads to a major limitation. Since the storage system shares the same network with clients and application servers, heavy data traffic can have undesirable effects, such as bottlenecks and reduced network performance. The Storage Area Network (SAN) model avoids this by creating a separate, dedicated network of storage devices, linked to the network by specialized software and hubs. The SAN framework allows centralized, highly-scalable data management solutions that maximize system performance by removing data traffic from the regular network. In general, most experts regard the two models as complementary more than exclusive. For example, NAS appliances can be highly effective components in a SAN.

Although NAS and SAN products combined represented less than 10% of the disk storage market in 2000, the IDC projects them to capture 38% of an estimated US\$46 billion storage market by 2003. More specifically, IDC projected that NAS appliance sales alone will top US\$5 billion by 2002, rising fivefold since 1998.

Viruses and Malicious Code at Large

A computer virus is a piece of executable code defined by its ability to replicate. Other features of a typical virus often include the ability to load onto computers without permission, run against the user's wishes, insert copies of itself into numerous files and carry a 'payload' of destructive commands. The simple boot sector and file viruses that were common a decade ago have evolved into a host of new breeds: such as polymorphic viruses, which alter their code to avoid detection, worms, which can replicate and spread through networks without infecting files. Trojans, which invade systems by posing as harmless applications, and many other malicious code threats are also part of this growing menace, while they may not, technically, be considered computer viruses.

Over the years, the number of known viruses has surpassed 50,000, and they have become faster, more versatile and harder to eradicate. They can attach themselves to more types of files and spread more efficiently, in more diverse ways. Recent global outbreaks like the Love Letter, Anna Kournikova and the Naked Wife Trojan have shown how effective malicious code can be.

As recently as 1998, computer viruses still spread primarily via floppy disk, a fairly slow, and predictable process. However, virus writers eventually hit on an effective method for hitching a ride on the Internet, a much faster and more effective distribution mechanism. Early in 1999, Melissa became the first virus to mass-mail itself all over the world as an email attachment, flooding networks and crashing hundreds of corporate mail servers in the process. Thanks to this stunning debut, along with the apparent eagerness of some users to click on any attached file they receive, however suspicious, email has remained the virus writer's infection vector of choice to this day. In 2000, email attachments were responsible for more than 90% of virus incidents reported by corporate users, according to the ICSA's latest virus prevalence survey. Each year since 1999, several email viruses have swept around the world, infecting entire enterprise networks in a matter of minutes. Each one of these major virus episodes costs companies millions of dollars in lost productivity and clean-up expenses.

With new viruses emerging daily to join the thousands in existence, it is evident that the virus issue will not go away any time soon. In fact, the ICSA's annual surveys since 1995 suggest that the problem has actually been getting worse. Over 99% of responding companies reported a virus incident in 2000, while nearly 67% experienced file problems and 40% suffered data losses from virus attacks. Most companies estimated annual losses from virus attacks at between \$100,000 and US\$1,000,000. The report's author concluded that corporations face a greater risk of "virus disasters" today than ever before.

Threats to Stored Data

Viruses can quickly compromise the security and integrity of data in a storage system. A new or unknown virus which slips past other defenses is likely to end up in the storage system. If it is a destructive virus, it may infect, corrupt or destroy large amounts of data before being detected. Even if these viruses fail to penetrate the storage system directly, they can cause infected or damaged files to be added to the NAS from the desktop or other system where the malicious code attacked..

Virus writers know that the most valuable part of any system is the data. The author of 'Love Letter,' for example, included forms of stored information in the file types it attacked, as well as applications and scripts. The author also chose to overwrite the data, rather than merely delete it, in an attempt to prevent its recovery. As NAS devices become more common, it is likely that virus writers will deliberately target the data they contain just as the 'Code Red' worm targeted specific Internet environments.

Viruses that are hidden away in stored data remain a serious threat to the network. Every time an infected file is accessed, the virus is likely to attack client systems or other parts of the network. An infection could even be transmitted to other systems or organizations through shared data including invaluable customers or business partners.

Virus protection intended for other parts of the network is an inadequate solution for the storage system. Consider the case of a mobile user who has rendered their client-based antivirus solution ineffective, either innocently or intentionally, which then allows a virus to infect their system while traveling. Upon their return to the office they could easily infect the shared storage of the organization. Or perhaps a new virus enters through the Internet gateway before the gateway can be updated to detect it. In either case, only an antivirus solution designed for NAS can both protect other users from accessing infected files while it also scans the entire NAS to remove the infection. Without storage-oriented virus protection, the network must rely upon the weakest link in its antivirus defense: the desktop solution. Since individual clients may include a variety of devices, such as notebook PCs and home PCs which periodically access the network, virus protection at this level is often the least uniform and the last to be updated.

In environments with poor security, the storage system could become a refuge for viruses and malicious code and a recurring source of infection. In a worst-case scenario, virus-ridden files in a storage system could result in a disastrous breakdown of storage services and data management, and irreplaceable data may be lost.

Trend Micro's Solution

Trend Micro's ServerProtect for Network Attached Storage (NAS) is designed to protect stored data from infection by virus code. It also protects network clients from infections that can occur through the storage system. ServerProtect for NAS scans stored data "on

access," i.e. whenever files on an NAS appliance are opened, created or changed by a user or application. Virus scanning takes place on separate Scan Servers running Windows NT or 2000 and is transparent to the end-user. Multiple scanners can balance loads and provide faster scan performance. Centrally managed through an intuitive, portable Windows-based console, ServerProtect for NAS provides fast, effective scanning, automatic pattern updates, event reporting, and remote antivirus configuration for administrators of network attached storage systems.

ServerProtect's Three-Tiered Architecture

ServerProtect solutions for NAS are tailored versions of the original ServerProtect for Windows NT/2000 and Novell Netware file servers. As the first commercial server-based antivirus solution, ServerProtect has a well developed, robust architecture designed to transparently provide the most effective protection. Thus it may be useful to review the architecture of the original ServerProtect.

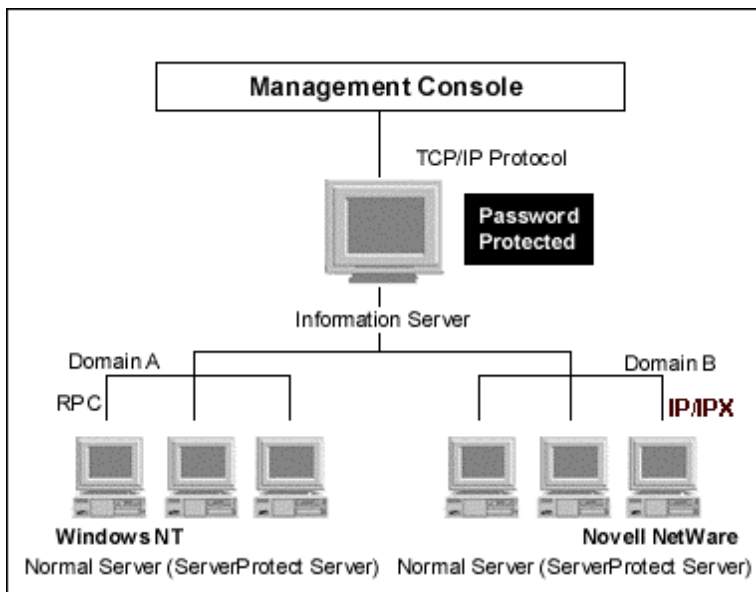


Figure 1. Original ServerProtect architecture

ServerProtect is designed to protect multiple servers and domains from viruses while installed and managed from a single, secure console. It operates through a three-tier architecture consisting of the Management Console, the Information Server, and the Normal Server. The administrator can use the Management Console to configure the Information Server (IS), which can in turn control the Normal Servers in the IS's domain. The three layers are independent from each other, and can be installed all on the same machine, on separate machines, or in a combination.

The **Management Console** is a portable console which permits the centralized control of multiple network servers and domains. It displays the status of all ServerProtect servers, enables the simultaneous configuration of servers in the same IS domain, and generates

integrated virus incident reports for all servers. The Console can be installed on any Win32 machine.

The **Information Server** is a communications hub for coordinating antivirus defense activities within its domains. An Information Server (IS) provides a single point of contact for all its assigned Normal Servers - saving time and reducing the workload on administrators by making it unnecessary to directly communicate with each individual Normal Server. In domains with many Normal Servers, administrators divide the number of Normal Servers among multiple IS servers to reduce the burden on each IS. The IS so collects log files.

The **Normal Server** is the first line of defense in the ServerProtect architecture, and where all scanning takes place. The Normal Servers are the machines in the organization which typically act as file servers, data servers, etc. Normal Servers can be scanned both manually and in real time.

Architecture of ServerProtect for NAS

ServerProtect for NAS uses the three-tiered architecture of ServerProtect to protect data stored on networked storage appliances. In ServerProtect for NAS, Normal Servers are known as Scan Servers. The antivirus scanner itself is installed on these Windows NT or Windows 2000 servers, and files stored in the NAS are scanned there upon access. Through the use of remote procedure calls (RPC), a simple application program interface (API) or a lightweight protocol, ServerProtect for NAS works with network attached storage appliances through the network, regardless of platform.

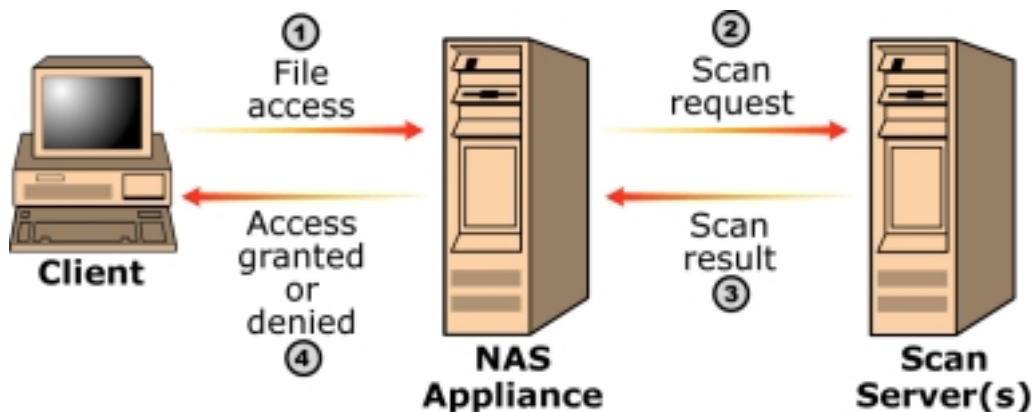


Figure 2. Virus Scanning Work Flow of ServerProtect for NAS

When a client user attempts to access a file on the storage appliance, or save a new or modified file to storage, a virus check is triggered. If the file name extension appears on a

predetermined list of file types, configurable by the Administrator, the NAS appliance notifies one of the registered Scan Servers and provides the path to the file to scan. ServerProtect then opens a connection to the file, scans it for known and unknown viruses, and notifies the NAS solution of the result. If no virus is found, the user is allowed to open the file. If a virus is discovered, ServerProtect takes action on the file in accordance with one of its settings, as configured by the administrator. Typically, ServerProtect will be set either to "Quarantine" or "Clean" an infected file. If the file is quarantined, the user is denied access and the administrator must take action. If the file is cleaned, the virus code is removed and the NAS application is notified, after which the user is allowed to access the now 'clean' file. If an attempt to clean a file is not possible or unsuccessful, ServerProtect will then quarantine the file and the user is denied access.

Table 1. Key Differences of ServerProtect Versions

	ServerProtect 5	ServerProtect 5 for NAS
Protection Focus:	Normal Servers (file servers, data servers, etc.).	Storage appliance (i.e. Network Appliance filer, EMC Celerra File Server)
Normal Server Role:	First line of defense: perform the actual antivirus functions of the system.	Acts as a "Scan Server" and scans files in the NAS appliance on access.

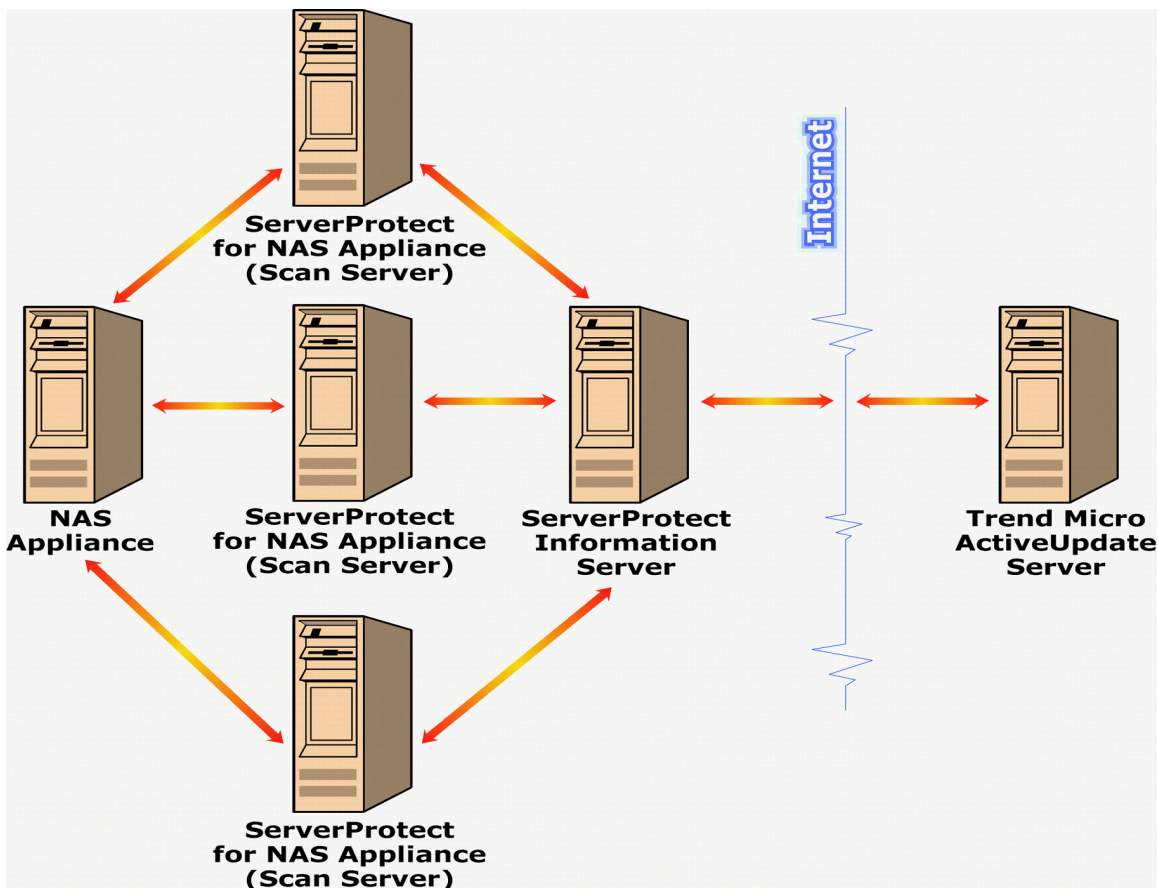


Figure 3. ServerProtect for NAS offers automatic updating and load balancing between multiple Scan Servers.

Features and Benefits for NAS Solutions

Virus Scanning Protects Data Integrity

ServerProtect for NAS uses the latest Trend Micro proprietary scan engine. It 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 all popular compression algorithms, including: PKZIP, PKZIP_SFX, LHA, LHA_SFX, ARJ, ARJ_SFX, CABINET, TAR, GUN ZIP, RAR, PKLITE, LZEXE, DIET, MSCOMPRESS, UNIX, PACKED, UNIX COMPACTED, UNIX LZW, UUENCODE, BINHEX, and BASE64.

Automatic Updating

A virus scanner is only as effective as its latest update. ServerProtect for NAS can be configured to automatically download the newest virus patterns and scan engine updates from Trend Micro’s ActiveUpdate server and distribute them to designated Scan Servers. To minimize download times and preserve network bandwidth, distribution to the

designated servers is done via an incremental update mechanism, which requires that ServerProtect for NAS downloads only the latest virus signatures to be added since the last update.

Centralized Management via Three-tiered Architecture

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 NAS appliance into one domain.

The ServerProtect management console enables administrators to configure all servers in the same domain simultaneously, and generate integrated virus incident reports from all Scan Servers. It thus consolidates status information from multiple NAS appliances and multiple Scan Servers for each NAS appliance.

Configurable Actions for Infected Files

The Information Server allows users to configure the action a Scan Server performs on an infected file. Possible choices include quarantining the infected file, cleaning the virus with or without a backup, or deleting the infected file.

Scalability and High Performance

To increase scalability and increase performance levels, multiple ServerProtect Scan Servers can be registered with the NAS appliances at any time. An increased number of Scan Servers registered to a NAS appliance will increase the scan performance. Once a ServerProtect Scan Server is registered to a NAS appliance, connection and reconnection between the server and the NAS appliance is made automatically. Whenever the server detects any communication disconnection, it will send signals to the NAS appliance to reconnect. This allows IT administrators to easily maintain effect security in a manner completely transparent to network users.

Comprehensive Log Reports

ServerProtect for NAS 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 while providing necessary audit and activity information.

Notification of Program Events

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

Current Versions of ServerProtect for NAS

Trend Micro currently offers versions of ServerProtect for NAS designed specifically to work with two leading NAS solutions: Network Appliance NetApp™ filers and EMC Celerra™ File Servers. Both vendors have worked closely with Trend Micro to ensure the seamless interoperation of virus protection and the storage system.

For a more detailed description and explanation of these products, consult the following Trend Micro white papers:

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

"Ensuring Data Integrity with Trend Micro ServerProtect® for EMC Celerra™ File Servers."

Summary

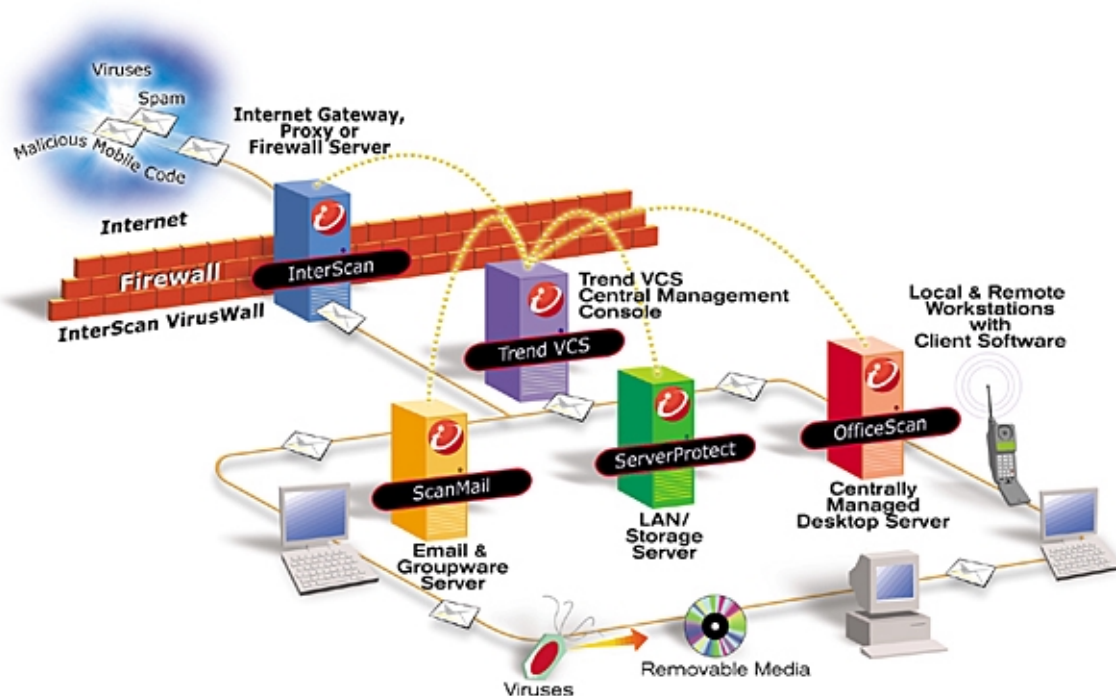
Security and data integrity are critical for stored data. A network-attached storage system such as an EMC Celerra file server or a Network Appliance filer will be vulnerable to virus attacks without dedicated virus protection for the storage device. Moreover, a virus-infected storage system can become a source of repeated 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 the requirements for an antivirus product for their storage devices. Trend Micro has been working closely with EMC and Network Appliance to provide virus protection for their network attached storage solutions.

ServerProtect for NAS provides a comprehensive antivirus solution for network attached storage systems. Managed through an intuitive, portable Windows-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 NAS appliance to provide better scan performance.

The Trend Micro Family of Products



The Trend Micro Enterprise Solution Stops Viruses at all Network Entry Points

Only when network administrators have secured all virus entry points mentioned below, can they be sure of complete virus protection for their enterprise's network.

Internet Gateway Servers:

On UNIX and Windows NT Internet gateway servers, Trend Micro InterScan VirusWall scans SMTP, HTTP, and FTP traffic to eliminate viruses attempting to enter through an enterprise's Internet gateway.

Email/groupware Servers

Trend Micro ScanMail protects email/groupware environments for Microsoft Exchange, Lotus Notes, and Hewlett-Packard OpenMail. ScanMail protects email-/groupware-messaging systems by scanning email, attachments and other shared information. By eliminating viruses in email/groupware servers, ScanMail prevents these systems from inadvertently distributing viruses to client PCs or to servers outside the enterprise.

File/Application Servers

At the file/application server, Trend Micro ServerProtect™ for NT/2000 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, and securing remote dial-up modems and other electronic access paths that can allow viruses to bypass network virus protection.

TVCS centralizes complete enterprise virus control

Trend Micro antivirus products for the enterprise are integrated into the Trend Virus Control System (Trend VCS™) a Windows-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 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>.