



Data Storage Security with Trend Micro ServerProtect[®] for EMC Celerra[™]

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 or www.antivirus.com



Table of Contents

ABSTRACT.....	3
DATA SECURITY IN A STORAGE SYSTEM	4
SERVERPROTECT FOR EMC CELERRA.....	4
ARCHITECTURE OF SERVERPROTECT FOR EMC CELERRA.....	5
BENEFITS FOR EMC CELERRA SERVERS	7
SUMMARY	9
THE TREND MICRO FAMILY OF PRODUCTS	10
ABOUT TREND MICRO	12

September 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.

Data Storage Security with Trend Micro ServerProtect® for EMC Celerra

Abstract

Most of the data storage industry has recognized the growing need for an effective 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 EMC Celerra provides an effective antivirus solution for data storage devices connected to EMC Celerra file servers, with minimal system overhead costs. Managed through an intuitive, portable Windows-based console, the software provides centralized virus scanning, pattern updates, event reporting, and antivirus configuration.

ServerProtect for EMC Celerra works with EMC Celerra file servers running EMC's proprietary NAS software v 2.2 or above, when installed with the Celerra Antivirus Agent (CAVA) v1.8.9 or above. Designed for easier virus management, ServerProtect for EMC Celerra is equipped with centralized management tools. Using intelligent scanning technology, the software ensures the integrity of data in a storage system device.

This document provides an overview of ServerProtect for EMC Celerra, including a discussion of product architecture and product features.

Data Security in a Storage System

Until recently most viruses spread primarily via floppy disk, but the Internet itself has become a virus distribution mechanism. Email is now an important business communication tool and viruses attached to email messages can infiltrate and 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 immune.

Security and data integrity are very important for storage systems. A single virus-infected file in a storage system such as EMC's Symmetrix™ Storage System, 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 EMC Celerra

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 requirements for an antivirus product for their storage devices.

EMC's Celerra File Server is dedicated to the function of serving files to clients over the network using industry-standard Common Internet File System (CIFS) protocols, and is designed for high performance, scalability, and high availability.

Trend Micro's ServerProtect for EMC Celerra provides a comprehensive antivirus solution for storage system devices connected to the Celerra File Server. 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 ServerProtect servers running Windows 2000/NT. Multiple ServerProtect servers can service a single Celerra server to provide better scan performance.

Management of ServerProtect for EMC Celerra can be done with limited resources and budget. Administrators can easily direct such virus maintenance tasks such as configuring scanning, pattern and program file updates, compiling virus logs, and setting parameters for real-time scanning. ServerProtect for EMC Celerra works with EMC's proprietary software, Celerra NAS v2.2 or above, when Celerra Antivirus Agent (CAVA) v1.8.9 or

above is installed. The connection between ServerProtect servers and the Celerra server is monitored so that in the event of a disruption it is able to reconnect automatically.

Architecture of ServerProtect for EMC Celerra

Virus scanning takes place in on-access mode and in one or more separate ServerProtect servers running Windows 2000 or NT (4.0). For this purpose, the Celerra server must be running Celerra NAS v2.2 or above and have the Celerra Antivirus Agent v1.87 or above installed, so the Celerra server can interact with the ServerProtect servers.

Figure 1 presents basic ideas on how data at the Celerra server is protected from virus infections.

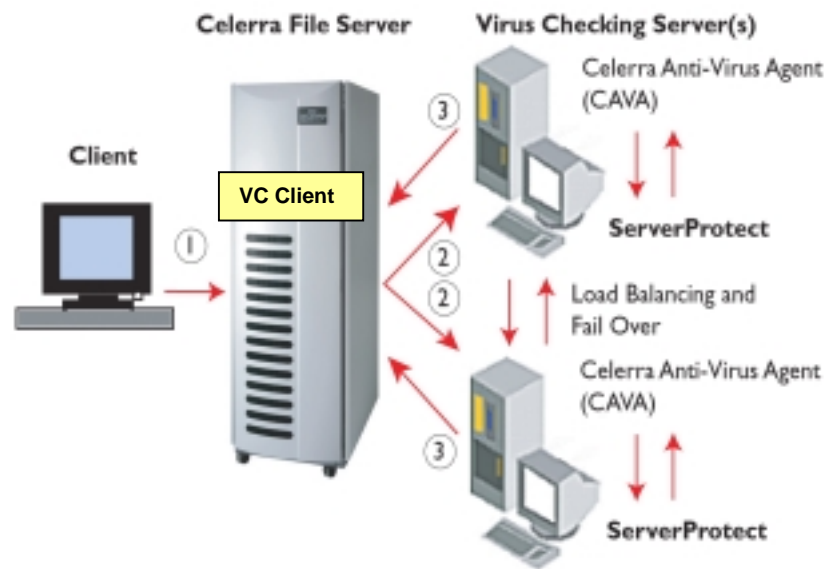


Figure 1: The Work Flow of Virus Scanning

When a client attempts to modify, close, or save a file to the Celerra file server, the Virus Checking (VC) Client on the Celerra server will request a virus check by sending the Universal Naming Convention (UNC) path name to the CAVA of ServerProtect machine. CAVA will have ServerProtect Scan Engine scan the file for viruses using Real-time Scan mode.

If the file is discovered to contain a virus, ServerProtect will perform the correct user-defined action on the file such as clean, delete, or remove before the CAVA returns the control of the file to the VC Client. If CAVA reports that the file has been successfully

cleaned, then the Celerra file server will allow the file to become available to the client or will save it to its attached data storage systems.

ServerProtect for EMC Celerra communicates with the Celerra server via Remote Procedure Call (RPC). The ServerProtect server performs the following functions:

- Designed for seamless compatibility with CAVA as AV server (antivirus server) for EMC Celerra File server
- Notifies VC Client of Celerra file server there is CAVA and AV engine installed as well as Real-Time Scan services running
- Monitors for requests for file scanning from the VC Client of Celerra File server
- Facilitates the exchange of scan results between the CAVA and the VC Client of Celerra file server
- Notifies the VC client of Celerra file server of any pattern file or scan engine updates
- Communicates with the VC client of Celerra File server to check the connection between the AV server and the Celerra File server
- Designed to provide load balancing across the Windows NT/2000 servers via a round robin method as long as there are several CAVA and AV engines for multiple AV servers .(Figure 2)

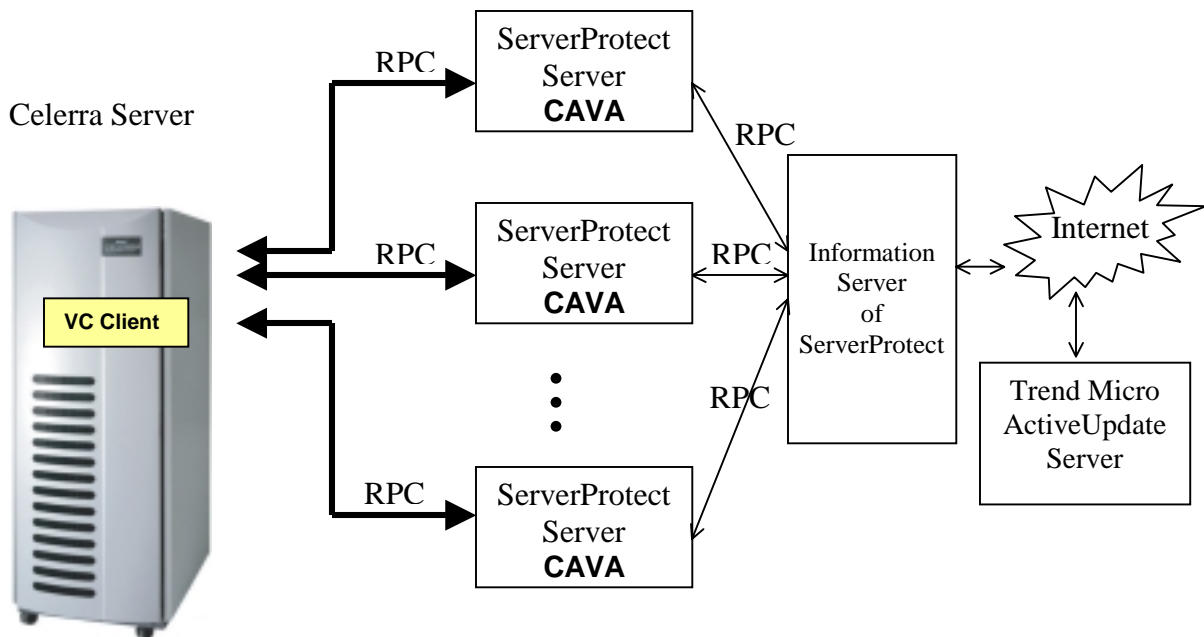


Figure 2. Architecture of ServerProtect for EMC Celerra

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 ServerProtect servers assigned to the filers, thus relieving administrators of the tedious task of directly communicating with every individual server. Each server is dedicated to a single Celerra server. However, one Celerra server can be registered with multiple ServerProtect servers.

Scanning is done on a separate ServerProtect server rather than on the Celerra server, so Celerra's processing power will not be impacted by the virus scanning. Connecting multiple ServerProtect servers with the Celerra server evenly distributes the scanning workload. Scan request or files to be scanned are sent to ServerProtect servers in a round-robin fashion, rotating in an orderly way which servers receives a file to be scanned. RPC connections maintain constant communication between the Celerra server and the ServerProtect Normal server(s) and the other Normal ServerProtect server(s) with the Information Server for round-the-clock insurance that only virus-free files are saved to the data storage system.

Benefits for EMC Celerra Servers

Scalability and High Performance

To increase scalability and performance levels, multiple ServerProtect servers can be connected to a single Celerra server at any time. An increased number of ServerProtect servers will increase the scan performance for the filer. Connections and reconnections between the servers are made automatically, and whenever ServerProtect detects any communication disconnection, it sends signals to the Celerra server to reconnect.

Comprehensive Log Reports

ServerProtect provides comprehensive log reports to enable the administrator 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's Information Server provides simple management of multiple Windows NT/2000 servers from a single, portable management console. Multiple ServerProtect servers can be grouped into a logical domain. Trend Micro recommends putting all ServerProtect servers for one Celerra server 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 ServerProtect servers. This consolidates status information if there are multiple Celerra servers and multiple ServerProtect servers for each Celerra.

Scan Engine and Virus Pattern Updates

The Information Server for ServerProtect can be configured to automatically download virus pattern file and scan engine updates from Trend Micro's ActiveUpdate server. It then efficiently distributes them to designated ServerProtect servers. The distribution of new virus pattern files uses an incremental update mechanism, whereby a server only needs to download the new virus signatures 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-Wild¹ 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 customize the action a ServerProtect 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 EMC Celerra sends alerts to administrators to notify them of potentially serious situations in their system. An alert is 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, or 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.

¹ Known to be in the real world infecting computers.

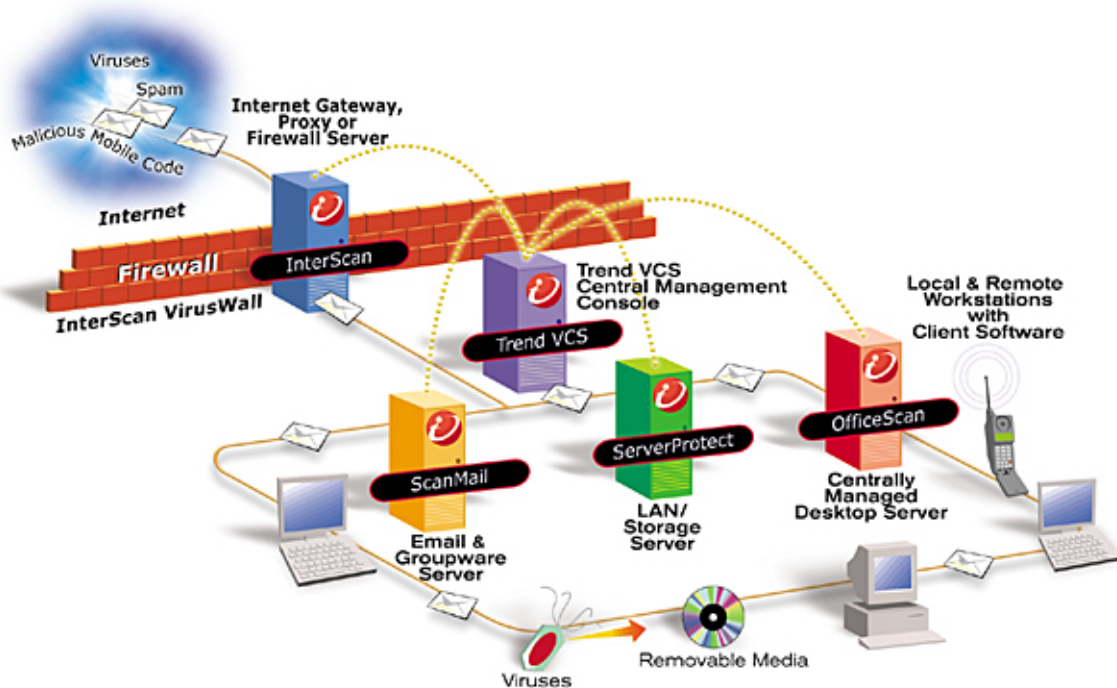
Summary

Security and data integrity for a storage system are very important. A storage system such as an EMC Symmetrix Storage System may 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.

ServerProtect for EMC Celerra delivers a comprehensive antivirus solution for storage devices that connect to an EMC Celerra File Server. With the development of the Celerra Antivirus Agent (CAVA) v1.8.9, EMC Celerra server users can now benefit from the award-winning protection of Trend Micro ServerProtect.

Trend Micro ServerProtect for EMC Celerra provides an effective antivirus solution for data storage devices connected to EMC Celerra file servers, with minimal system overhead.

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, Lotus cc:Mail, Microsoft Mail, or Hewlett-Packard OpenMail. ScanMail protects email-/groupware-messaging systems by scanning email attachments and 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 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/>

