

Trend Micro™

ServerProtect™ for Storage

Secures storage systems from EMC®, NetApp®, and Hitachi Data Systems

Comprehensive Data Protection for Storage Appliances

A single piece of malware can spread quickly in a networked environment because it is difficult to quarantine infected users. The more users share files by way of servers and storage systems, the greater the risk of network damage caused by infected files and of intellectual property theft by data-stealing malware. Also, the continuous expansion of data capacity can make the completion of scheduled scans a time-consuming task for administrators. To effectively protect file storage systems, enterprises need comprehensive, real-time scanning capabilities that take effect as users continuously access files from storage devices on the network.

Trend Micro™ ServerProtect™ is designed to provide network-wide, comprehensive anti-malware scanning for the EMC Celerra®, NetApp, and Hitachi Data Systems (HDS) lines of data storage systems. Managed through an intuitive, portable console, ServerProtect provides centralized malware scanning, cleanup, pattern file updates, and event reporting with enterprise-class performance and automation.

KEY FEATURES

Reliable Protection and Automatic Updates

- Features best-in-class scan engine technology with an extensive track record in protecting against viruses, worms, spyware, and Trojans
- Provides high-performance security scanning via load balancing multiple servers to service a single or multiple storage devices
- Allows automatic downloads and distribution of malware pattern files, scan engines, and program files

Flexible and Centralized Administration

- Enables administrators to manage security software from a single console
- Allows simultaneous configuration of scanning and notification options for multiple servers
- Provides server status through a single console, including pattern file and program versions, infection status, and connection status
- Provides fine-grained administrative controls for scan actions, CPU optimization, and log management

Automates Scanning to Optimize Protection

- Automates security maintenance tasks such as configuration scanning, pattern and program file updating, compiling virus logs, and setting parameters for real-time scanning
- Scans and remediates compressed archives for malware without requiring unnecessary decompression
- Breaks up scheduled scan tasks to scan high-usage directories on a different frequency than low-use directories
- Reduces resource impact by analyzing traffic and resources to create custom RTS policies for different times of the day

Comprehensive Log Report and Event Notifications

- Displays the infection history of servers in a central log file
- Provides preliminary statistics of antim malware events, exporting logs to other programs for further analysis
- Notifies pre-defined recipients of malware infections and program events
- Allows customization of multiple notification methods, including message box, pager, printer, Internet email, SNMP trap, or Windows event log

High Availability Architecture for NetApp and Hitachi

- Integrates tightly with NetApp Filers or Hitachi NAS Platform and enables multiple or single-scan server malware protection for multiple filers
- Employs a Cluster Failover Filer environment to enable other servers to take over scan requests if a server goes down
- Load balancing for scan request traffic with NetApp or Hitachi round-robin mechanism
- Enables automatic reconnection of the RPC bi-connection between the NetApp Filer/Hitachi NAS Platform and ServerProtect

SOFTWARE

Protection Points

- EMC Celerra storage servers
- NetApp ONTAP Filers
- Hitachi NAS Platform

Threat Protection

- Viruses
- Worms
- Spyware
- Trojans

KEY BENEFITS

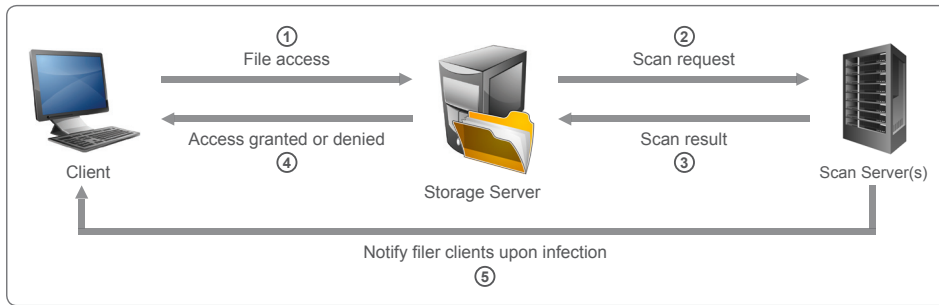
- Helps deliver real-time server protection against viruses, worms, spyware and Trojan attacks
- Permits multiple ServerProtect servers to storage or network appliances, increasing scalability and availability while lowering total cost of ownership
- Helps reduce administrative costs through management of remote installation, maintenance, and upgrades from a central console
- Minimizes manual tasks by automating routine antivirus maintenance and updates
- Granular policy management provides greater deployment flexibility and control
- Alerts administrators to virus outbreaks and emergencies to help reduce response time
- Provides comprehensive logs and reports to help identify dangerous activities before they become threats

“...having an integrated version of Trend Micro ServerProtect is an IT administrator's dream come true. We now get the benefits of reporting logs and real-time scanning without any major impact to system performance. This is perfect!”

Josh Gifford

Senior NT Administrator
Siemens Power Transmission & Distribution

Deployment Overview of ServerProtect for NetApp Filer and Hitachi NAS Platform



Trend Micro is a global leader in the overall server-based anti-malware software market, with anti-malware products and services designed to maximize server security while enhancing and complementing overall enterprise security. In addition, all these products and services are backed by TrendLabs, the global technical support and R&D center of Trend Micro that monitors potential security threats worldwide, developing the means to identify, detect, and eliminate new viruses, worms, spyware, Trojans, and data-stealing malware.

SOLUTION COMPONENTS

- ServerProtect for EMC Celerra
- ServerProtect for NetApp Filer and Hitachi NAS Platform

ADDITIONAL SERVERPROTECT PRODUCTS

- ServerProtect for Linux
- ServerProtect for Microsoft™ Windows™ and Novell™ NetWare™

COMPLEMENTARY PRODUCTS AND SERVICES

- Trend Micro Deep Security
- Trend Micro Core Protection for Virtual Machines
- OfficeScan™ Client-Server Suite
- Trend Micro Endpoint Security Platform
- InterScan™ Messaging Security Solutions
- InterScan™ Web Security Solutions
- Trend Micro Premium Support Services

MINIMUM SYSTEM REQUIREMENTS

Operating Systems
<ul style="list-style-type: none"> • Microsoft™ Windows™ 2003/2003 R2 Standard/Enterprise with SP2 or above (x86 or x64) • Microsoft Windows 2008/2008 R2 Standard/Enterprise (x86 or x64) • Microsoft Windows 2008/2008 R2 Hyper-V Standard/Enterprise (x64) • VMware ESX/ESXi 3.5/4.0
Normal Server
<ul style="list-style-type: none"> • 2.5-GHz Intel Pentium IV processor or 3.0-GHz EM64T Intel processor or 2.0-GHz AMD Athlon 64-bit processor (or equivalent) 1GB RAM; 1GB disk space
Information Server
<ul style="list-style-type: none"> • 3.0-GHz Intel Pentium IV processor or 3.0-GHz EM64T Intel processor or 2.0-GHz AMD Athlon 64-bit processor (or equivalent) 1GB RAM; 1GB disk space
Management Server
<ul style="list-style-type: none"> • 2.5-GHz Intel Pentium IV processor or 3.0-GHz EM64T Intel processor or 2.0-GHz AMD Athlon 64-bit processor (or equivalent) 1GB RAM; 1GB disk space (servers) or 512 MB RAM; 500MB disk space (clients)
EMC CELERRA STORAGE SERVER
<ul style="list-style-type: none"> • EMC Celerra file server Celerra Antivirus Agent (CAVA) 2.2.4 or above • CEE 4.0.5.4 or higher
NETAPP FILERS
<ul style="list-style-type: none"> • NetApp OS Data ONTAP 7.2 or above
HITACHI NAS PLATFORM
<ul style="list-style-type: none"> • BlueArc System Management Unit (SMU) 7.0



©2011 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, InterScan, OfficeScan, and TrendLabs 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. [DS01_SP_NetAppEMC_110913US] www.trendmicro.com