

Trend Micro™

SERVERPROTECT™ FOR STORAGE

Secures leading network-attached storage systems

A single piece of malware or ransomware, like WannaCry or Petya, can spread quickly in a networked environment because it is difficult to quarantine infected users. The more users who 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™ for Storage, powered by XGen™ security, leverages a blend of cross-generational threat protection techniques to safeguard a wide range of network attached storage systems by detecting and removing viruses and spyware in real time. This comprehensive storage security uses the industry-standard ICAP protocol to complement support for traditional RPC communication protocols. To simplify network protection for EMC, NetApp, and Hitachi Data Systems storage systems, ServerProtect for Storage provides automatic, incremental security updates and centralized management of servers via a web-based console.

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 one or more 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 and Optimizes 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 and ransomware 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 antimalware 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

Software

Protection Points

- EMC Celerra, Isilon, and VNX/VNXe storage servers
- NetApp ONTAP filers and IBM N Series running Data ONTAP
- Hitachi Data Systems NAS

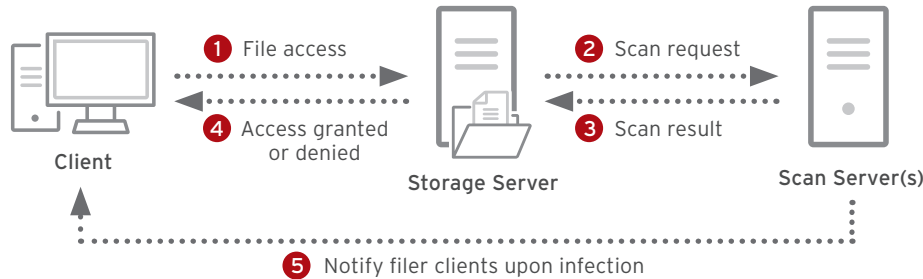
Threat Protection

- Ransomware
- Viruses
- Worms
- Spyware
- Trojans

Key Benefits

- Delivers real-time server protection against ransomware like WannaCary, viruses, worms, spyware, and Trojan attacks
- Lets multiple ServerProtect servers protect storage or network appliances, increasing scalability and availability while lowering total cost of ownership
- Reduces administrative costs with centralized management of remote installation, maintenance, and upgrades
- Minimizes manual tasks by automating routine antivirus maintenance and updates
- Provides granular policy management for greater deployment flexibility and control
- Alerts administrators to virus outbreaks and emergencies to help reduce response time
- Creates comprehensive logs and reports to help identify dangerous activities before they become threats

NETAPP AND HDS DEPLOYMENT OVERVIEW



Trend Micro™ ServerProtect™ for Storage, powered by XGen™ security, a smart, optimized, and connected security approach.



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 and ransomware attacks.

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) • Microsoft Windows Server 2012/2012 R2 Foundation, Essentials, Standard or Datacenter (x64) • Microsoft Windows Storage Server 2012/2012 R2 Standard or Workgroup (x64) • VMware ESX/ESXi 3.5/4.0/5.0
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 Storage Server	<ul style="list-style-type: none"> • EMC VNX/VNXe • EMC Celerra • EMC Isilon
NetApp ONTAP Filers	<ul style="list-style-type: none"> • NetApp Storage Devices running Data ONTAP 7.x and 8.x • IBM N Series running Data ONTAP
Hitachi Data Systems powered by BLUEARC	<ul style="list-style-type: none"> • Hitachi NAS
Protocols	<ul style="list-style-type: none"> • ICAP, EMC CAVA, and RPC



Securing Your Journey to the Cloud

©2017 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo 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. [DS02_ServerProtect_Storage_171016US]