

How to protect file servers from attacks and threats before they wreak havoc among users

Information is the most important asset in any organization as it is essential to all decision-making. When this information is shared in a server, to enable collaboration between members of a team, there is a serious risk factor: loss or theft of information or even inability to continue working if the server is attacked or infected.

Enforce security policies in your servers and prevent crashes due to malware

Panda Security for FileServers ensures the corporate information shared on the network is safe from attacks and other threats. This low-impact, high-performance antimalware solution for Windows file and print servers also detects vulnerabilities, hacking tools and other threats.

Panda for FileServers combines the fastest and most advanced technologies for detecting known malware with the new TruPrevent™ Technologies. These exclusive Panda Software technologies include network intelligence to detect denial of service (DoS) attacks and can seek out and analyze open communication ports, privilege-stealing processes and the malicious behavior of programs that cannot be detected by antivirus products.

This prevents the spread of massive virus attacks, spyware, adware, worms, Trojans... when computers access shared network resources.

Main benefits

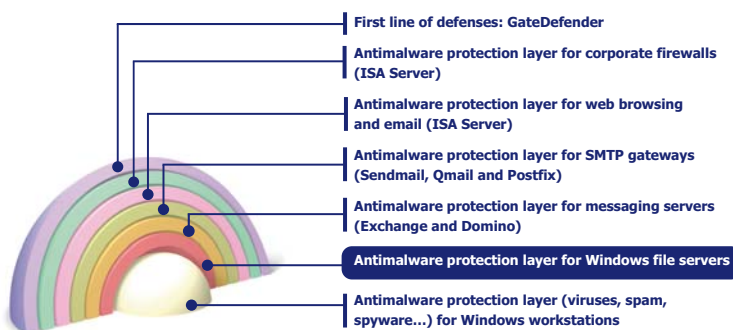
- Protects file servers at all levels and ensures the **integrity of corporate information**.
- It controls **user behavior** which could lead to network infections.
- **Boosts** administrator and end-user **productivity**.

Key features

- **Complete, latest generation antimalware engine** that detects server infections and scans for viruses, worms, spyware, rootkits and other threats.
- **Flexible policy management and secure communications** ensured through monitoring of main entry points.
- **Interception of unknown malware and intruders**, with the new **TruPrevent Technologies (HIPS)**.
- **Hourly automatic updates** of the malware signature file.
- **Optimum performance** of reactive and preventive protection to minimize system impact, thanks to specifically aimed server technology usage.
- **Centralized and remote administration** of networks with multiple server views and graphic reports to facilitate real-time decision making among administrators.

Layered preventive protection strategy

Panda Security for File Servers protects file servers from viruses and intruders.



Complete latest-generation antimalware engine

Panda Security for File Servers offers unrivalled protection against viruses, worms, Trojans, rootkits, spyware, tracking cookies, adware, hacking tools, dialers and security threats for file servers. Its features include resident HTTP protection and the ability to inspect files opened in exclusive mode. Its powerful *Genetic Heuristic Engine (GHE)* is also able to block the majority of unidentifiable new threats.

Flexible policy management and secure communications

To anticipate the actions of hackers and intruders, **Panda Security for File Servers** monitors the communications and the memory and prevents buffer overflows. It also exhaustively analyzes communication packets to detect practices such as attempts to identify the operating system, denial of service attacks, IP Spoofing, MAC Spoofing, network viruses...

To complement the **default security policies**, user and application access to system resources can be customized (files, registry entries, etc.) to reinforce security in the event of threats such as pharming. Finally, it prevents server infection and data leaks due to access by external personnel who do not have protection on their computers as well as employees without the necessary physical credentials -MAC address-.

Interception of unknown threats

In addition to its powerful antimalware engine, **Panda Security for File Servers** also includes **TruPrevent Technologies (HIPS)**, which monitor running processes to block malicious behavior of the new malware or intruders.

This system doesn't just detect unknown malware, it prevents it from running (leaving the file in quarantine), warns the other network computers of the attack, requests the antidote from Panda to disinfect it and thanks to the *SmartClean2* technology, repairs the system automatically. This mechanism reduces the risk window and prevents damage to your company reputation.

Hourly automatic updates

Panda Security for File Servers can be configured so that it checks for new signature files hourly without user intervention, and updates automatically. Incremental updates of malware signature files contribute to the reduction of total bandwidth usage and to mitigate communication peaks.

Optimum performance

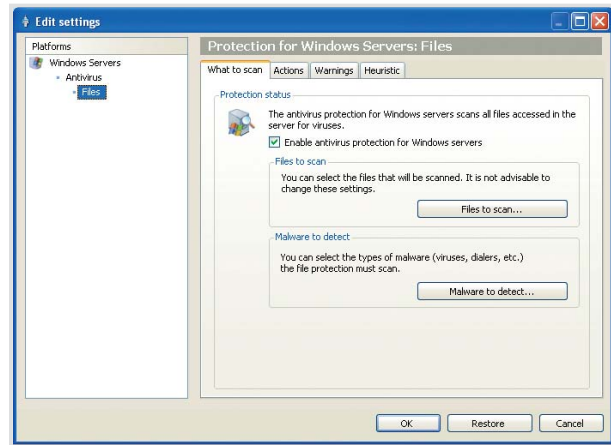
Panda Security for File Servers provides high-performance protection for the biggest companies' file and print servers. The antivirus kernel is multi-threaded for parallel scanning and, server hardware permitting, can distribute loads across various processors.

It includes a powerful cache and *AutoTuning* system to ensure smooth operation, both under independent and cluster server configurations or in 64-bit operating system versions.

Centralized and remote administration

Panda Security for File Servers is managed remotely and centrally through a single interface: **Panda AdminSecure**. Through this tool all protection is installed, and a security dashboard provides information on the server protection level.

Remember **Panda Security for File Servers** can be bought separately or as part of **Panda Security for Business** or **Panda Security for Enterprise**.



AdminSecure includes views, graphic reports, warnings, etc. The console lets you control the centralized quarantine so you can manage suspicious files awaiting disinfection. It also lets you identify the users that are the source of infection.

Technical requirements

Panda AdminSecure Console

Pentium II 266 MHz or above.
RAM: 140MB.
Hard disk free space: 140MB.
Internet Explorer 5.5.
Windows installer 2.0.

AdminSecure Operating systems: Windows 2000 / XP / XP 64 bits, Windows NT4 SP6 and Terminal Server, Windows 2000 Server SBS, Windows Server 2003 Enterprise Edition/SBS/R2, Windows Server 64-bit, Windows Vista 32 bits/64 bits, Windows Server 2008 (32 and 64 bits).

Panda Security for File Servers

Pentium 300 MHz or above.
RAM AV: 256 MB.
RAM AV+TP: 256MB. Recommended 512MB.
Hard disk free space: 160MB.
TruPrevent not supported in 64 bits.

Operating systems: Windows NT 4.0 with SP6 (Domain controller, SB Server, Terminal Server and cluster), Windows Server 2000 Domain Controller, StandAlone, Terminal Server, SB Server and cluster, Windows Server 2003 (32 and 64 bits)Enterprise Edition, SB Server, SP1, SP2 and cluster, Windows Server 2003 R2(32 and 64bits), Windows Server 2008 (32 and 64 bits), Windows SBS 2008 (32 and 64 bits).

"The signature update process provided with Panda Antivirus is making our department significant cost saving and improving our reputation with our users."

Mr. Vernon Warnen. IT Manager. Wrexham Maelor Hospital. UK.

