

Surefire preventive protection against malware and intruders for Windows and Novell servers

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

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

FileSecure combines the fastest and most advanced technology 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

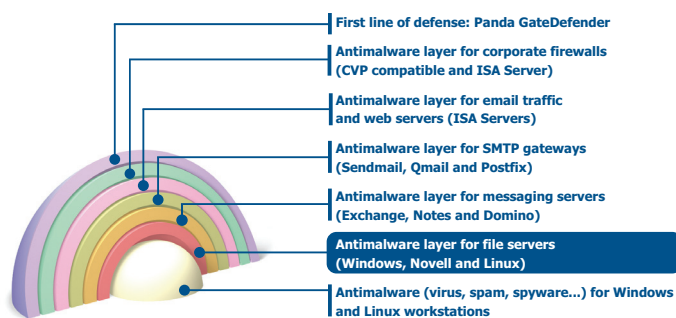
- **Integrated protection for your information** against all types of viruses and security threats.
- **Simple administration** and remote maintenance of the protection even in heterogeneous environments.
- **Maximum advantage** taken of hardware and software capabilities in high-performance platforms for scanning and disinfecting all file types.

Key features

- **Complete, latest generation antimalware engine** detects infections and scans for viruses, worms, spyware and other threats in servers.
- **Flexible policy management and secure communications** ensured through monitoring of main entry points.
- **Interception of unknown viruses and intruders**, with the new **TruPrevent™ Technologies**.
- **Completely automatic daily updates** of the Malware Signature File, as well as the rules for detecting the behavior of new malware.
- **High performance and low impact**, thanks to its server-based technologies.
- **Centralized and remote administration** of networks with multiple server views to facilitate administration tasks.

Layered preventive protection strategy

Panda FileSecure protects file servers from viruses and intruders.



Complete antimalware engine

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

Interception of unknown threats

In addition to its powerful antimalware engine, **FileSecure** also includes **TruPrevent™ Technologies**, which monitor running processes to search for the malicious behavior of any new malware which may have got past the signature-based scan and the GHE.

This system doesn't just detect unknown malware, it can block the process, preventing it from running (leaving the file in quarantine), **warn the other network computers of the attack**, and then request the antidote from Panda. Thanks to *SmartClean2* technology, it automatically disinfects and repairs the server, drastically reducing response time, and the risk of damage to your company or its reputation.

Communications safe from intruders

To anticipate the actions of hackers and intruders, **FileSecure** monitors communications and the memory: preventing buffer overflows and exhaustively analyzing 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 **security policies** included by Panda, user and application access to system resources can be customized: files, registry entries, COM components... to reinforce security in the event of pharming attacks, for example. Finally, **NetworkSecure** prevents infection of the server due to access by external personnel who do not have Panda protection in their computers as well as employees without the necessary physical access credentials -MAC address-, thereby preventing information leaks.

Automatic transparent updates

With no need for user intervention, **FileSecure** is updated automatically and transparently at least once a day. In each connection, only information relative to those threats that have appeared since the last update will be included, so as to avoid downloading the entire signature file. However in the event of an emergency, it is possible to distribute the identification of an exploit without waiting for the generation of a new signature file.

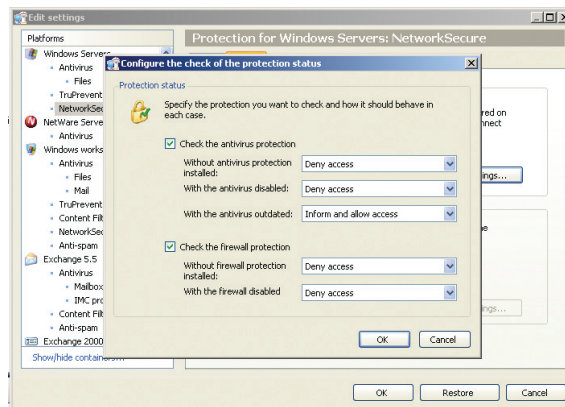
High performance, low impact

FileSecure provides high-performance antivirus services for even 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

FileSecure 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.



AdminSecure includes views, graphic reports, warnings, etc, as well as centralized quarantine so that files held pending disinfection can be managed from the console.

Technical requirements

Windows servers: Pentium Processor 300 MHz (or later version) with Windows NT 4.0 SP6, Windows Server 2000 and 2003 SBS/cluster/R2. 85 MB free space on the hard disk. 256 MB RAM.
Novell NetWare servers: 486 Processor or later version. Novell NetWare 4.11, 5.0, 5.1, 6.0 or 6.5. with 12 MB free space on the hard disk. 32 MB RAM.
Panda AdminSecure: Pentium III 800 MHz. 512 MB RAM. 500 MB hard disk. Operating systems: Windows NT4 SP6, 2000, XP and Server 2003/ SBS/ R2. AdminSecure Console also supports Windows 98 and Me.

"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. UNITED KINGDOM.

Panda Software Certifications



Remember **FileSecure** can be bought independently or as part of **BusinesSecure 2006** with **TruPrevent™ Technologies** or **EnterpriSecure 2006** with **TruPrevent™ Technologies**.

