

bitdefender® SECURITY FOR FILE SERVERS

FILE SERVERS - THE BACKBONE OF THE NETWORK

File servers are not just a network repository for the company's files. Unlike their name suggests, File Servers provide critical infrastructure services to ensure communication and interoperability between desktops, printers, and other resources found within the network. In smaller networks, critical services can be maintained by a single server configured for a multi-tasked role. In larger networks, services are often broken out and distributed amongst multiple, dedicated servers in order to ensure scalability, resiliency, redundancy, and improved response times to user requests.

Some of the critical services a File Server provides within a network include:

- Domain Controller (Active Directory) Server
- Application Servers (IIS, ASP.NET)
- File and Print Servers
- Remote Access/VPN Server
- Terminal Server
- DHCP Server
- WINS Server
- DNS Server
- Streaming Media Server

Critical servers should be deployed and maintained within a tightly controlled environment. Guidelines regarding system access to the Internet must be enforced to preserve system stability and minimize the risk of external compromise. However, these guidelines are inconvenient to the day-to-day running of the network. Over tasked administrators can sometimes disregard these guidelines when problems arise - surfing the Internet from a critical server looking for system utilities or security tools to fix an issue, invariably infecting the server with unwanted spyware, adware or a Trojan / virus. Worms can also propagate throughout the network and infect a Server without warning, and unless protected, the critical network services they provide will become unavailable to user community – greatly impacting the company's productivity.

SECURING FILE SERVERS WITH BITDEFENDER

Companies can protect their File Server deployments from attack by using BitDefender's ability to scan for malicious code in files, maintain system integrity, help ensure compliance to corporate security policies and prevent sensitive data from being distributed outside of the organization.

BitDefender Security for File Servers provides optimized protection of both the server operating system and data file structure for critical back-end systems. Easy to install, configure and maintain via the centralized management console, BitDefender for File Servers protects against viruses, spyware and rootkits to minimize the impact of malware propagation throughout the network.



KEY FEATURES AND BENEFITS

- **Award winning virus detection, cleaning and quarantine**
- **Minimize network downtime to increase operational efficiency**
- **Reduce resource costs and overhead**
- **Scans file traffic ensuring real-time antimalware protection to minimize the risk of malware propagation throughout the network**
- **Scans and fingerprints "read-only" files just once during the same session and only re-scans them if there is a new session, an update or an infection in the system**
- **Allows flexible scheduling of on-demand or immediate execution scans for possible infection assessment**
- **Quarantine's infected or suspected files, minimizing risk of propagation**
- **Integration with Microsoft's Virus Scanning API to optimize and accelerate the scanning process**
- **Allows remote configuration from any computer in the organization through a web configuration console**
- **Mail archive support for Dbx, Mbx, Pst, Mime, Mbox, Hqx, Uudecode, and Tnef file formats**

ADVANCED FEATURES

- Integration with BitDefender's Management Server
- Centralized dashboard providing deployment status overview with alert thresholds
- Custom antivirus scanning profiles (high, medium, low, create your own) to allow improved flexibility
- Safely quarantine suspicious files, with optional restore to original location feature

BITDEFENDER TECHNOLOGIES

b-have All BitDefender solutions include B-HAVE, a patent-pending technology which analyzes the behavior of potentially malicious codes inside a virtual computer, eliminating false positives and significantly increasing detection rates for new and unknown malware.

DEFENSE IN DEPTH

BitDefender Security for File Servers is just one element in a comprehensive suite of solutions providing end-to-end protection from the gateway to the desktop. BitDefender's proactive, multi-platform products detect and stop viruses, spyware, adware and Trojan threats that can compromise your network integrity.

SYSTEM REQUIREMENTS

Software

- Windows Server with SP4 and Update Rollup 1 v.2
- Windows Server 2003 with SP1, Windows Server 2003 R2
- Windows Server 2008, Windows Server 2008 R2, Windows Small Business Server (SBS) 2008
- Internet Explorer version 6.0 or higher



All trademarks, trade names, and products referenced herein are property of their respective owners. All Rights Reserved.
© 2010 BitDefender.

Proactive Server Protection

Antivirus
Antispyware
Rootkit Detection



Centralized Management

Auto Deploy
Auto Update
Enforce Policy
Reports & Alerts
License Mgmt

BitDefender's antimalware detection, management and reporting features ensures safe document sharing throughout the organization

ADVANCED, PROACTIVE DETECTION

Optimized for File Server environments, BitDefender's award-winning scan engines have been recognized by leading certification bodies, - including ICSA Labs, Virus Bulletin, and West Coast Labs - for their unmatched proactive antimalware protection. BitDefender provides multiple levels of advanced protection;

Antivirus – In addition to signature based detection, BitDefender provides heuristic detection that emulates a virtual computer-within-a-computer, checking all files and code for malicious behavior. This technique produces fewer false positives and significantly higher detection rates for zero-day and unknown threats.

Antispyware - BitDefender Client Security detects and prevents known spyware and adware by using five different filtering methods to monitor the registry for modifications, file scanning, cookie control, URL filtering and content inspection to prevent outbound data leakage.

Trojans and Root Kits are designed to allow remote access to a computer system. Once a Trojan or Root Kit has been installed, it is possible for an attacker to access the system remotely and often leads to data theft. Detecting and preventing these types of threats manually can be time consuming and often lead to a complete system reinstall if improperly removed.

OPTIMIZED SCANNING

The file scanning process is enhanced by BitDefender's new optimized scanning technology that significantly cuts on-demand scanning times. The optimized scanning maintains a database of already scanned and known to be safe to avoid scanning them again. Therefore the scanning speed is improved and also system load is reduced.

GRANULAR SCAN CONFIGURATION AND MANAGEMENT

BitDefender Security for File Servers provides On Access, On-Demand, Scheduled scanning methodologies to detect malicious code to safeguard the integrity of the file repositories. Suspected files are isolated in quarantine zones. The files can either be cleaned or kept in a quarantine zone for analysis, restored to its original location once validated, or sent directly to BitDefender's Antivirus Lab for assessment.



INTEGRATION WITH THE BITDEFENDER CENTRAL MANAGEMENT PLATFORM

BitDefender Security for File Servers provides integration with the Management Server's Security Dashboard, giving Administrators enterprise-wide visibility into their network resources and overall security posture. The BitDefender Management Server provides a centralized point for remote installation, configuration and reporting of all BitDefender Clients, Server and Gateway products deployed within the enterprise and notifies administrators of scan performance, infections and update tasks through its comprehensive alert module.