

# BITDEFENDER SECURITY FOR SAMBA



## PROTECTING CROSS PLATFORM NETWORK RESOURCES

Samba file servers are a common resource in many large, heterogeneous networks as they provide a cost effective suite of utilities and common interoperability between Linux/UNIX and Windows-based workstations and Servers. Samba provides secure, stable and fast file and print services for all many different platforms using the SMB/ CIFS protocol, including all versions of DOS, Windows, OS/2, and Linux.

Samba is also an important component that seamlessly integrates Linux/Unix workstations and Servers into Microsoft's Active Directory environments. Because of this integration into the Windows environment, Samba services can easily become a carrier for malicious code that target's the Windows platform.

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

- Web Servers (Apache)
- File and Print Servers (Samba)
- Remote Access/VPN Server
- DNS Server

Samba file servers are capable of spreading the following security threats;

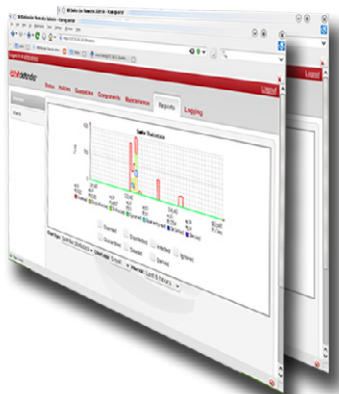
- Malicious code through shared files
- Compressed, infected archives
- Viruses, Trojans and Rootkits
- Worms and Spyware

Files stored on Samba shares can invariably infect other systems 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 SAMBA FILE SERVERS WITH BITDEFENDER

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

BitDefender Security for Samba enables organizations to deploy antivirus and antispyware protection for their Samba network shares running on Linux, FreeBSD and Solaris systems. Deployed and maintained centrally within the network, Security for Samba scans cross-platform data structures and file stores for malware, keeping network users safe from virus infection.



## KEY FEATURES AND BENEFITS

- Award winning virus detection, cleaning and quarantine
- Minimize network downtime and risk of malware propagation throughout the network by scanning shared files ensuring real-time antimalware protection
- Allows flexible scheduling of on-demand or immediate execution scans
- Quarantine's infected or suspected files, minimizing risk of propagation
- Allows remote configuration from any computer in the organization through a web-based Remote Administration interface
- Fully complies with FHS (Filesystem Hierarchy Standard), operating in a completely non-intrusive manner
- Works with any Samba build and can be easily compiled against all versions, thanks to its open-sourced vfs module
- Ensures compatibility with all major UNIX-based platforms due to its rpm, deb and generic .tar.run packages

## ADVANCED FEATURES

- Integration with BitDefender's Management Server
- Centralized dashboard providing deployment status overview with alert thresholds
- Safely quarantine suspicious files, with optional restore to original location feature
- Customizable e-mail notifications or SNMP alerts about its activity: number of scanned, disinfected, deleted, infected or filtered files

## 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 Samba 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

### Operating System:

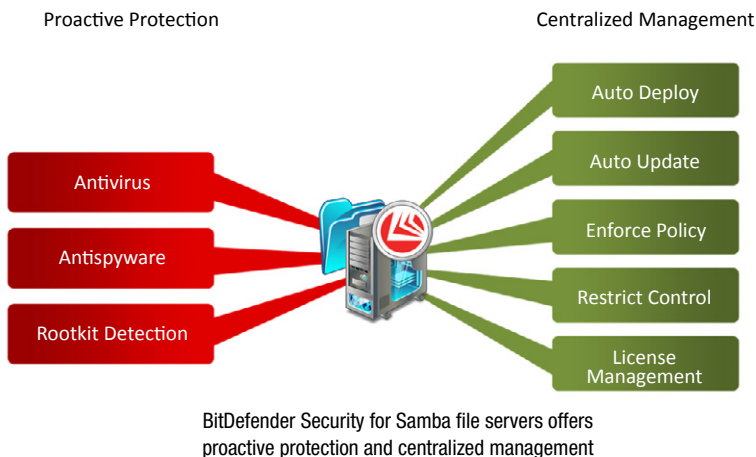
- Linux, FreeBSD, Solaris
- Linux Kernel 2.6.18 or newer
- glibc 2.3.1 or newer, and libstdc++ from gcc4 or newer

### Samba:

- Version 3.0 or newer

### Supported Distributions:

- Debian GNU/Linux 3.1 or newer
- Fedora Core 1 or newer
- FreeBSD: 5.4-RELEASE (or newer, with compat5x)
- Mandrake/Mandriva 9.1 or newer
- Novell SuSE Linux Enterprise Server 9, Linux 8.2 or newer
- OpenSolaris 2008 or 2009 (x86 platform)
- Oracle Linux 5 or newer
- RedHat Enterprise Linux 3, Linux 9 or newer
- Slackware 9.x or newer
- Solaris 9 or 10 (x86 platform)



## ADVANCED, PROACTIVE DETECTION

Optimized for Samba 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 detects and prevents known spyware and adware by using file scanning methods to prevent infections by spyware leading to 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.

## GRANULAR SCAN CONFIGURATION AND MANAGEMENT

BitDefender Security for Samba 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 Samba 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.

