BitDefender for File Servers

QUICK START

bitdefender
secure your every bit

How does it work?

BitDefender for File Servers is a solution implemented especially for servers running on the Windows platform. Its main features cover the security needs of a file-sharing server, while its purpose is to lower the burden implied by administrating a server software solution. Easy to install and easy to configure, but with a strong set of functionalities, it targets both small and large organizations.

Storing, sharing and distributing data are the main tasks of data management, but these would fail without easy access to information, data integrity and good system uptime. BitDefender for File Servers addresses the issues of data security and system availability with:

Advanced antivirus technologies

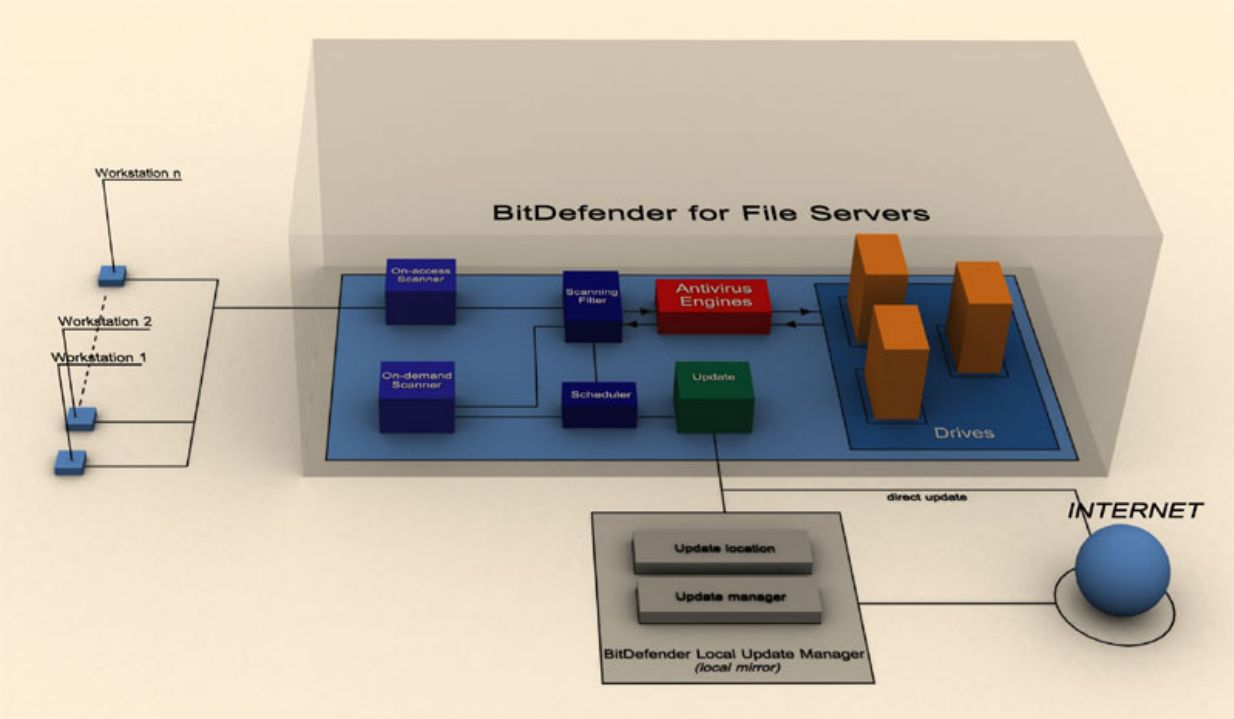
- HiVE technology and certified engines
- Optimized scanning and multithread scanning

Strong functionalities

- Both on-access and on-demand antivirus scanning
- Automatic update

Increased usability

- Scheduling system
- Logging, reporting and alerting system
- BitDefender Enterprise Manager integration



In the diagram above, the main processes, antivirus scanning and updating are described

To better serve its function as a security solution meant for servers, **BitDefender for File Servers** has been implemented based on a modular architecture. The main modules are:

- On-access Scanner
- On-demand Scanner
- Update
- Scheduler
- Scanning Filter
- Antivirus Engines

The real-time protection
As the files are being written on the disk or accessed the **On-access Scanner** module intercepts the event and starts the scanning process.

The following steps can describe the scanning process:

1. The scanning filter checks the file. The file extension, the file size, the file path are sequentially checked to match the administrator configurations. The result of the Scanning Filter is SCAN or NO SCAN.
2. If the result of the Scanning Filter is SCAN, the file is scanned by the Antivirus Engines. First the file is verified against the antivirus signatures database. If any part of the file matches a signature, the file is reported as infected. If none of the signatures is matched, the file is checked with the HiVE technology. In case the behavior of the file is similar to the behavior of a malware, the file is reported as suspect. The result of the Antivirus engines module can be INFECTED or CLEAN
3. If the result of the Antivirus Engines module is INFECTED one of the following actions can be taken: disinfect, delete, ignore, quarantine. If these actions fail to be applied "Deny access" is applied. In this way the user will not be able to execute infected code.

The on-demand protection
This type of protection is useful for usual maintenance purposes and for checking the server after a period of time when the on-access antivirus protection was disabled.

The **On-demand Scanner** module can be triggered by clicking "Scan now" from the user interface or by a scheduled on-demand scan task. The scanning process is the same, but it checks all the files that are submitted for scanning and not the files that are accessed.

The update process
The Update module performs the update process and its main function is to download the latest BitDefender files. Three types of files are available:

- **Antivirus signatures**. These files are updated constantly as the BitDefender Lab analyzes new viruses every day.
- **Antivirus engines**. These files are updated as frequent as the antivirus signatures as well. The HiVE, BitDefender proprietary technology has been implemented in the antivirus engines.
- **Product files**. The product files updates differ from the antivirus signatures updates and their function is to deliver bug fixes and performance improvements of the product. The product updates are downloaded, but they are not automatically installed. Please note that the installation of the product updates might request a system restart.

The update process is performed automatically every 3 hours, but the time interval can be configured as well as the update tasks be scheduled at any time.

The download of the latest BitDefender files requires an approved BitDefender update location. By default the product updates the files from the BitDefender sites, but local mirrors of the BitDefender update locations can be made by installing **BitDefender Local Update Manager**. The installation kit for the **BitDefender for File Servers** includes also the **BitDefender Local Update Manager**. In this way, the **BitDefender for File Servers** products can be updated from a location within the same network.

KEY FEATURES	BENEFITS
HiVE	HiVE stands for Heuristics in Virtual Environment; practically, it emulates a virtual computer-inside-a-computer where pieces of software are run in order to check potential malware behavior. This BitDefender proprietary technology represents a new security layer that keeps the operating system safe from unknown viruses by detecting potentially malignant pieces of code for which signatures have not been released yet. It thus supplements usual signature and behavior-based techniques, increasing the overall effectiveness of your antivirus solution. HiVE is a component of the BitDefender antivirus engines, which have been certified by **ICSA Labs**, **CheckMark**, **CheckVir**, **Virus Bulletin** and **TUV**.
Scan Optimization	The BitDefender antivirus scanner fingerprints, during each session, every “read-only” scanned file. The “read-only” permission assures that the file will not be modified or infected during the respective session. A database of recently scanned files that have been found safe is thus created. These files are not rescanned upon a new access. If an update is performed or if an infection is detected in the system, the database is reinitialized. This safety measure assures that all files are rescanned with the latest antivirus signatures.
Multithread Scanning	Multithread scanning implements a well-known method that simulates parallel execution of a program. Multiple instances of the engines are used in order to shorten the scanning process.
On-access Scanner	On-access scanning provides real time protection of the file server by scanning every file that is accessed or copied on the disk. This is the main feature of a server-oriented antivirus application and its function is to keep the file server free from malicious content.
On-demand Scanner	On-demand scanning is a powerful tool specially designed for administrators. Its purpose is to provide a second layer of defense against malicious software that might infect the file server. We recommend that you scan the file server periodically with the newest antivirus signatures by scheduling an on-demand antivirus scan or by performing a scan-now action.
Threat Mitigation	Automated signature and product updates, backed up by HiVE technology, minimize the window of vulnerability of your system. The updates are automatically downloaded from BitDefender servers or approved mirror sites hourly.
Scheduler	Scheduling capabilities have been added in BitDefender for File Servers. On-demand antivirus scans and update tasks can be scheduled from the product user interface. This system has been correlated with the Alerts module to provide notifications for administrators when an on-demand scan or an update has been performed.

Logging and Statistics

The monitoring system has been improved as well. Reports of the product activity can be created and a special module of statistics is provided. Also, the alert system includes new features as customizable alerts for several types of events: antivirus signature updates, product updates, on-demand scans, viruses detected.

Redesigned Interface

BitDefender for File Servers has an MMC-based user interface that offers a friendly working environment. The wizard system implemented in the interface enhances the usability of the product while the snap-in system provides the actual management functionality.

Centralized Management

BitDefender for File Servers is fully compatible with BitDefender Enterprise Manager, offering organizations a centralized-type of management for antivirus protection and security policies inside complex networks. Remote installation, remote configuration and status checks of BitDefender for File Servers can be performed in a centralized manner from an administrative console in your network.

SYSTEM REQUIREMENTS

Minimum Processor: Pentium II 300MHz
Minimum hard disk space: 75 MB
Minimum RAM Memory: 64 MB (128 MB recommended for superior performances)
Operating platform: Windows NT 4.0 SP6 + IE 5.5 +MMC v1.2
Windows 2000, Windows XP or Windows 2003 Server

Best practices

1. After the installation process is over, please register the product. You must access the **Register** section, select the product, type in the serial number and click the **Apply** button.
2. Activate your Support Account. To manage the feedback and feature requests/bugs you send to BitDefender, enter **Information\Register** section and click **Online Registration** from the BitDefender Help menu
3. Configure the update. Enter the **Update Settings** section and configure the update settings. By default, BitDefender will automatically update every 3 hours. Click **Update now!** to immediately update the scan engines.

   TIP: If **BitDefender for File Servers** was installed on a computer that doesn't have access to the Internet, configure the **BitDefender Local Update Manager** in order to keep the antivirus engine updated.
4. Apply available **Product Updates**. Enter the **Update\Product Updates** section and install the available product updates. The product updates differ from the antivirus signatures updates and their function is to deliver bug fixes and performance improvements of the product. The product updates are downloaded, but they are not automatically installed. Please note that the installation of the product updates might request a system restart. We advise you to install the latest version of product updates.
5. Select the action to be taken on infected files when scanning on-access. Enter the **Antivirus/On-access scanner** section and select the desired action: disinfect, delete, move to Quarantine or ignore (no action). For disinfect you can select a second action in case the disinfection fails.

   TIP: In case both actions fail, **BitDefender for File Servers** denies the access to the infected file in order to prevent the system from being infected.
6. Verify that BitDefender is working with the EICAR test. The test consists in creating a file using a text editor, provided the file is saved in standard MS-DOS ASCII format and is 68 bytes long. It might also be 70 bytes if the editor puts a CR/LF at the end. The file must contain the following single line: `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`. Save the file to any name with COM extension, for example EICAR.COM on the server protected by BitDefender. BitDefender must treat this file as an infected one.

   The string must be reproduced on a single line.
7. Perform a manual scan of the file server. Enter the **Antivirus\On-demand Scanner** section, configure the scan settings and click **Scan now**.
8. Exclude files/folders from on-access scanning. Enter the **Antivirus\On-access Scanner** section and select the desired files and/or folders. You can exclude from scanning as many folders as you want.

   TIP: For best performance, configure extensions scanning options by selecting the check box corresponding to **Application Extensions** to scan only the files, which can be executed.
9. Configure BitDefender alerts. If a virus is detected or an unexpected situation appears, there is the possibility of sending alarm messages by e-mail or by net send. Enter the **Mail Alerts** section or the **Net Send Alerts** section in order to configure BitDefender to send these notifications.