

VirusBuster for Windows Servers

▼ Corporate users:

▶ Servers – Windows NT/2000/2003 Server

In a network environment, the protection of servers is crucial as most of the data used for our everyday work is stored and transferred by servers. Therefore the effective protection of these servers does not only secure the stored data, but provides a secondary defense line for clients connected to them.

VirusBuster for Novell NetWare provides resident protection for data, systems and therefore for the everyday work, optimised to the increased data traffic of servers.

The task oriented operation, the flexible settings, the wizard style and advanced user interfaces provide ease of use with the highest level of security in the most flexible way.

- Effective resident protection for servers against viruses and other harmful codes
- Separate protection areas to handle servers' storage disks or their smaller areas individually
- Manual, automatic and scheduled virus scans
- Easy to use, wizard style user interface
- Advanced interface for advanced settings
- Task oriented operation, modular updates
- Intelligent quarantine for infected files
- Supports Windows Security Center
- Daily virus database updates

www.virusbuster.hu

mail@virusbuster.hu

H-1518 Budapest, Pf. 54.

Telefon: (+36 1) 382 7000

Fax: (+36 1) 382 7007

Minimum System requirements:

- Windows NT Server/2000 Server/2003 Server
- Intel Pentium (or compatible) 400 MHz
- 128 MB of available RAM
- 20 MB of available disk space

VirusBuster for Windows Servers

Easy to use

VirusBuster for Windows Servers' user interface was designed so that it is easy to use for beginner and experienced users alike. To modify the product's settings, the user can either use the wizard style interface, where settings can be modified step by step, or the advanced interface, where all settings can be overviewed and the user can switch modules with ease.

Using the wizard style interface is very easy, as every step has a detailed description and help, therefore every update or scan can be added or the settings of the resident protection can be modified by anyone in a couple of minutes. Every settings page contains help for using the page and advancing to the next page.

The advanced interface is a powerful tool for experienced users to overview settings and modify them easily in minutes

Task oriented operation

The product is based on tasks. Product and virus database updates, scheduled scans or any other function can be added as a task. Thanks to the built-in automatism, all tasks are executed at the needed time automatically with the desired settings, so it is not needed to run a virus scan or an update every time, as the product automatically executes these. VirusBuster for Windows Servers contains the most regularly used tasks by default (e.g. daily virus database updates), which can be modified to suit the user's needs.

Separate protection areas

The product provides comprehensive protection against every known virus and other harmful code, but in most

cases, administrator's need individual settings for each drive or other areas on the servers. The separate protection areas provide the opportunity of handling the servers disks or their smaller areas individually so that every data stored on these disks is protected at the needed level security.

Modular updates

With the help of the product's updater module, VirusBuster for Windows Servers is always up to date and ready to cope with the latest threats. The update can be performed from various sources (CD, FTP, HTTP, network path, Novell NetWare network path). Updates are modular, therefore only the needed update packages are downloaded to avoid useless network load.

Outstanding performance and effectiveness

VirusBuster for Windows Servers is based on VirusBuster's scan engine, which has an outstanding performance. The engine uses heuristic analysis to detect harmful programs. Thanks to its platform- and operating system independent scanning methods it effectively scans for all known viruses, worms, trojans, backdoors, scripts, macro viruses and other harmful code on any system. Depending on the available memory, it scans multiple compressions to any depth in numerous compression types and self-extractors. To improve scanning these files, the engine uses emulation techniques.