Dr.Backup™
online backup service

Dr.Backup Antivirus/Security Exclusions Explained

The Dr.Backup remote backup software client is designed to thoroughly scan your computer to monitor changes to critical data files.

Once identified, copies of new/changed files are created in a temporary working area on your hard disk where they are compressed, encrypted and transferred over the Internet to a secure storage vault for subsequent retrieval (if needed.)

While software components performing these operations are integral to Dr.Backup, they may be incorrectly characterized as invasive by anti-virus or malware detection applications installed on your system.

Once identified as a potential threat, parts of Dr.Backup may be disabled, quarantined or even improperly removed from your computer by security software. This will cause your online backups to fail and necessitate you call Dr.Backup customer support for assistance.

Vendors of security software generally provide a mechanism for you to manually identify "trusted" applications and folder structures which should NOT be monitored by security applications. The capability to specify exceptions to security software is known as "white-listing."

To ensure the proper operation of your Dr.Backup software, the following exclusions should be added to your security white list: (assumes backup software agent on C:\)

Processes to Exclude:

C:\Program Files (x86)\Remote Backup\rbclient.exe
C:\Program Files (x86)\Remote Backup\rclient.exe
C:\Program Files (x86)\Remote Backup\rbbackupprogress.exe
C:\Program Files (x86)\Remote Backup\rbtransfer.exe
C:\Program Files (x86)\Remote Backup\schwrap.exe
C:\Program Files (x86)\Remote Backup\exchangebackupservice.exe
C:\BMR\VHDBackup-64.exe (if you are using the Full Image Backup service)

Folders to Exclude:

C:\Drbackup\...
C:\Program Files (x86)\Remote Backup\...
C:\DrbKey\...
C:\BMR\...