

# BitDefender for MS Exchange 5.5

## QUICK START

# How does it work?

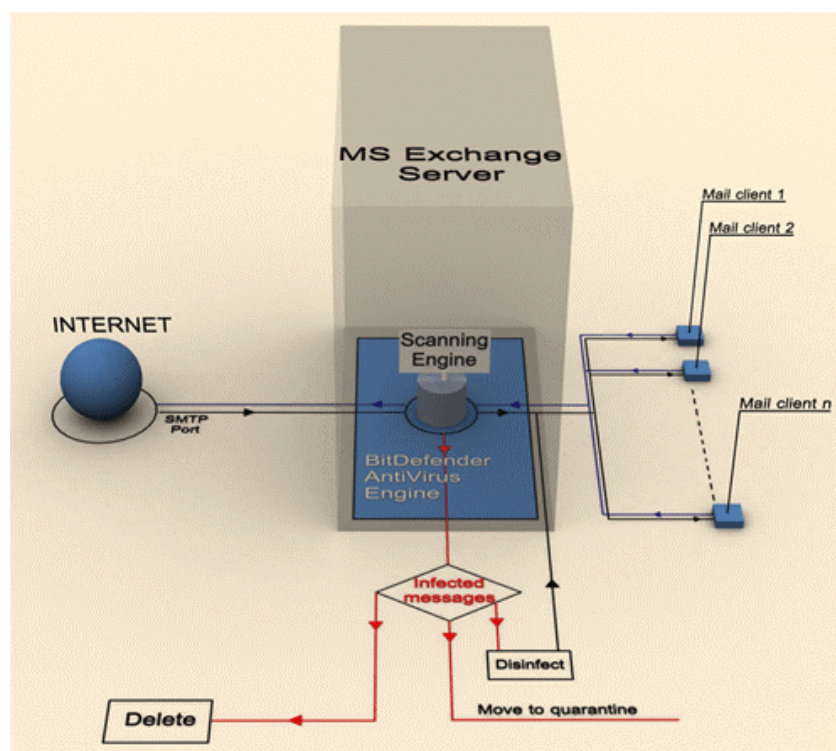
The acquisition and installation of an antivirus product for the company's mail server is the most efficient way of preventing the infection of a computer and the spreading of viruses inside the company, as well as outside the company through the most common way of communication - the e-mail.

**BitDefender for MS Exchange 5.5** is the solution SOFTWIN offers for the antivirus protection of the MS Exchange mail servers. The product is designed and implemented in a modular manner, thus it can easily adapt to any work environment.

BitDefender for MS Exchange deeply integrates with the Microsoft Exchange 5.5 SP3 through the Microsoft recommended scan interface. It uses the improved features of MS Exchange in order to minimize the waiting time of a mail message in the queue.

All the messages received by the server are scanned using the BitDefender scan engines. The scan engines identify the viruses presents in the attachments, including RAR, ZIP, ARJ, LZH, LHA, ACE, GZIP, TARGZ, JAR, UUE, MIME or CAB archives, no matter how they were created (self-extractable, multivolume, etc). If the message is clean, it will be sent forward to the mail recipient. In case an infection is found, it will be treated corresponding to the selected option (disinfection, deletion or isolation in the quarantine area) and alarm messages will be sent to the persons responsible with the administration and the protection of the network.

The schema below shows the way BitDefender works:



The message's HTML attachments will be verified in order to detect the infected files and the back doors/ trojans/ worm files and prevent their spreading into the system.

Following the scheme above, it can be observed that only the clean messages will be delivered to the mail clients from the workstations or will be sent further to the recipients outside the company.

The infected attachments are treated depending on the administrator's option, by disinfection, deletion or isolation in a certain location on the server, considered to be the quarantine zone.

## **BitDefender AntiVirus Engine**

The **BitDefender AntiVirus Engine** will check the e-mail for viruses with the BitDefender powerful scanning engines (**ICSA Labs-**, **Checkmark-** and **VB-**certified).

It will identify the viruses presents in the message body or attachment, including RAR, ZIP, ARJ, LZH, LHA, ACE, GZIP, TARGZ, JAR, UUE, MIME or CAB archives, no matter how they were created (self-extractable, multivolume, etc). Depending on the BitDefender actions, the infected messages can be disinfected, deleted or moved to quarantine and alarm messages (by e-mail or through NetSend ) can be sent to the persons in charge with the administration and the protection of the network.

## **SYSTEM REQUIREMENTS**


- ➔ Minimum 20 MB available hard disk space (50 MB Recommended)
- ➔ Microsoft Exchange 5.5 + SP3, Internet Explorer 4.0

# Best practices

1. After the installation process is over, please register the product.
2. Select the action to be taken on infected messages (**AntiVirus Engine** section).
3. Verify that BitDefender is working with the EICAR test.

The EICAR 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 and send it as attachment to an user that has the e-mail on the server protected by BitDefender. BitDefender must treat this message as an infected one.

 The string must be reproduced on a single line.

After sending those messages, access the **Statistics** section, where you can see if BitDefender is actually working.

4. If a virus is detected or an unexpected situation appears, there is the possibility of sending alarm messages by e-mail (**Mail Notification** section) or by net send (**NetSend Notification** section).
5. Configure the update. Enter the **BitDefender Update** section and if you are using a proxy check **Use Proxy** and type in the settings. You can change the update interval (the default interval is 8 hours).

Click **Update now** in order to update the BitDefender AntiSpam & AntiVirus engines.