

8.3 Antivirus

There are a number of antivirus packages available for individual computers and for network-wide virus scanning. It is important to consider the following factors when purchasing a virus scanning solution for your own organisation or for a client:

- **Budget:** Price is not the only factor that should be considered here, but if anything, widely examined.
- **Vulnerability:** A busy organization which frequently receives e-mails from outside the organisation and that downloads from the Internet will need higher antivirus protection than a smaller group that occasionally uses the Internet.
- **Skill:** Whoever will ultimately use the product must be able to understand how to use it. Are you getting a virus scanner for a group of tech-savvy engineers or a group of end users who are unlikely to be technically proficient?
- **Technical:** How does the virus scanner work? What methods does it use to scan? How often are the .dat files updated? How quickly does the vendor respond to new virus threats and release new .dat files?

All of these factors must be considered when selecting antivirus solutions. Security experts too often recommend a product they are familiar with, without conducting significant research.

8.3.1 McAfee

McAfee is a well-known antivirus vendor. This antivirus has been marketed under many names, including VirusScan, Endpoint Security, and Total Protection. This company offers solutions for home users and large organisations. All of McAfee's products share common features, including e-mail scanning and file scanning. They also scan instant messaging traffic.

McAfee scans e-mail, files, and instant messaging for known virus signatures. It also uses heuristic methods to locate new worms. Given the growing use of worms (in contrast with traditional viruses), this is an important benefit. McAfee offers a relatively easy download and installation process which offers a trial version on the company's website.

8.3.2 Norton Antivirus

Norton Antivirus is another widely known vendor of antivirus software. You can purchase Norton solutions for individual computers or for entire networks. Norton offers e-mail and file scanning, as well as instant messaging scanning. It also offers a heuristic approach to discovering worms and traditional signature scanning. Recent versions of Norton Antivirus have also added anti-spyware and anti-adware scanning, both being very useful features. An additional interesting feature of Norton Antivirus is the pre-install scan. During the installation, the install program scans the machine for any virus infections that might interfere with Norton. Because it is becoming more common to find virus attacks that actually seek to disable antivirus software, this feature is very helpful.

While Norton, like most antivirus vendors, offers versions for individual PCs and for entire networks, the individual version has a free trial version that you can download and experiment with for 15 days without any charge.

8.3.3 Avast Antivirus

This product is free for home and non-commercial use. You can download the product from the vendor's website: www.avast.com/. You can also find professional versions, versions for Unix or Linux, and versions specifically for servers. This product is also available in multiple languages including English, Dutch, Finnish, French, German, Spanish, Italian, and Hungarian.

Once downloaded, you can see that Avast opens up with a tutorial. This feature, combined with the fact that the home version is free, makes this a very attractive tool for the novice home user. The Multilanguage and multi operating system support makes it attractive professionals worldwide. When it finds a virus, a sound alarm is triggered with a voice stating: "Warning: There is a virus on your computer."

8.3.4 AVG

AVG antivirus has become quite popular. One reason for this is that there is a free version as well as a commercial version.

AVG is robust and a full-featured antivirus software. It integrates with e-mail clients such as Microsoft Outlook and it also filters web traffic and downloads.

8.3.5 Kaspersky

Kaspersky has been growing in popularity. It includes business and personal versions. Like most antivirus products, it also includes additional features not directly related to detecting viruses. For example, Kaspersky includes an encrypted password vault to keep your passwords in, upon request.

8.3.6 Panda

Panda is available for both commercial editions and free versions. The commercial version also comes with anti-spyware. Like Norton and McAfee, you can get a personal firewall bundled with the antivirus software. This product is available in English, French, and Spanish. Its wide range of features makes this product a robust and effective solution.

8.3.7 Malwarebytes

This product is available from <https://www.malwarebytes.com/>. There is a free version of the product and a paid premium version. Malwarebytes has a strong reputation in the industry. It is well regarded and fairly simple to use.

8.3.8 Antivirus Policies and Procedures

Antivirus scanners are not the only facet of protecting yourself against viruses. In fact, there are situations in which a virus scanner is simply not effective enough. You will need policies and procedures to complete your antivirus strategy. Policies and procedures are written rules that dictate certain actions that administrators and end users should take, alongside other activities they should avoid. Listed below are certain policies and procedures:

- Always use a virus scanner. It costs only about \$30 a year to keep your virus scanner updated. Failing to use a virus scanner could cost you more money in the long run.
- If you are weary about an attachment, do not open it. When you have specifically requested a file from someone, then

opening an attachment from that person is most probably safe. However, unexpected attachments are always cause for concern.

- Consider exchanging a code word with friends and colleagues. Notify them to put the code word in the title of the message if they wish to send you an attachment. Do not open any attachment without the code word.
- Be sceptical of any e-mail you are sent. Keeping e-mail to official traffic will help reduce danger. Jokes, flash movies, and so on should not be sent on a company e-mail system.
- Do not download files from the Internet. If you need a file downloaded, the IT department should do that. Carefully scan the file and then forward it to the user. If you feel compelled to download files you should follow two simple rules:
 - Only download from well-known, reputable sites.
 - Download to a machine that is off the network first. Then you can scan that system for viruses. In fact, if you do request your IT department to download something for you, this is the most likely process they will use.