

CHOOSING AN ANTIVIRUS SOLUTION FOR YOUR ORGANIZATION

In this age of weekly global virus outbreaks it goes without saying that every computer needs protection. The growth in the number of viruses and the speed with which they spread follows the trend in growth of the internet. Like a busy city, the internet is the perfect environment for infections to spread like wildfire. Community and voluntary organisations are in as much danger from viruses as businesses and individuals. For cash strapped organisations time and energy spent recovering from a virus outbreak is doubly expensive. Even more costly is the threat of leaking sensitive personal data to criminal gangs because of infection with malignant software. There are no ifs and buts about it – the level of threat and the potential cost of infection mean your organisation needs antivirus software *now!* It isn't only the threat to *your* organisation. You have a social responsibility to prevent viruses spreading on to others.

What to protect

Any way that files or programmes make their way into your office is a potential route for a computer virus. Viruses can arrive in emails, be downloaded with other software by unwitting members of staff, or be on a floppy disk you used to archive files five years ago.

Email Server

Most viruses these days are transmitted via email. Your first line of defence is therefore your email server. If you download your email from an external provider such as your ISP, check to see all email is checked on their server. If they say that you need to pay extra for this service, consider changing providers. Even free email providers such as Hotmail and Gmail provide this free as standard. If you are paying for email services and aren't being protected, ask yourself why not.

If you manage your own email server in-house, ensure antivirus software is installed on it that scans all arriving emails for viruses. The easiest way to obtain this software is as part of a corporate antivirus package (see below).

File Servers

Servers allow central storage and sharing of files, but you don't want to store or share viruses! Servers require different antivirus software to desktop PCs. Again, the easiest way to obtain this is through corporate antivirus packages.

Desktop PCs

The last line of defence is on the computers people work at each day. Every computer in the organisation should have antivirus software installed to protect against floppy disk borne viruses.

Different requirements

These three types of system each require a different kind of antivirus programme to protect them – desktop PCs need *on-access* scanning that checks each file as it is opened. File servers shouldn't be used to open files; so on-access scanning is not required and would slow the server down anyway. More important is the facility to run scheduled scans to find any infected files in shared and users folders. Mail servers need antivirus software which check messages as they arrive (and also for spam) and quarantine any infected ones somewhere they can be safely examined.

Choices

When choosing an antivirus solution for your organisation there are two main choices – *stand alone programmes* and *centrally managed programmes* (often referred to as *corporate* versions).

Corporate/Centralised Antivirus

Corporate versions of antivirus software allow one person in an organisation to manage all computers from a single location. You can see on a single screen which computers are up to date and protected and those which are not.

Corporate antivirus products are often the only way to obtain appropriate antivirus software for protecting a server, particularly Microsoft's Exchange email server. They often also include anti-spam filtering at no extra cost.

Corporate editions usually come with at least five *client licenses*, meaning you can run the software on this number of desktop computers. This can mean the total cost for corporate antivirus is less than buying standalone products for every computer in the organisation.

Additionally, you can often buy several years' updates up front at a reduced price. Some vendors allow you to spread this cost over the period signed up for.

Standalone

Standalone antivirus software is managed on the computer it runs on and does not affect other computers. Standalone antivirus is most appropriate for small organisations with less than five computers and no servers. It may also be the most appropriate option for laptops, or for individual staff members working at home.

Note that it is sometimes possible to buy several licenses for standalone antivirus software at once (e.g. 5 licenses) at a discount.

Online Scans

Many antivirus vendors provide online scanning tools on their websites, usually for free. Although these can detect and remove all the viruses the paid for programmes do, they cannot protect you from infection or viruses spreading to other computers.

Where infection is suspected, online antivirus can be the best method of recovery, but is a last resort.

Emergency disks

Emergency disks can be used to boot an infected computer, providing a safe environment from which to remove viruses.

Like online scans, emergency disks should be considered a last port of call for use on computers that may already be infected. For example, a donated computer should probably be scanned with an emergency disk before connecting it to your network.

Antivirus

Costs of bundled antivirus solutions

These days it is fairly common to find antivirus software preinstalled on new computers. This can initially seem like a perk – you normally get 90 days free antivirus updates. After this time you will need to pay for an annual license, or replace the software with a different one.

Of course, antivirus companies hope you will take the path of least resistance and stick with their system. In most cases this is not a problem, but remember that the antivirus software you get in this way represents the company that made the best deal with your computer's manufacturer, *not* which antivirus software is the best for *your* needs.

Bundled antivirus software cannot be centrally managed, and over time you will most likely find different computers in your organisation will be running different antivirus programmes. This makes it harder to manage your systems – the person supporting your ICT systems will need to be familiar with multiple programmes, and you will need to manage renewing several licenses with several companies over the course of a year.

Truly Free options

For those with no budget for anti virus, there are a couple of zero cost options – note these are only available as standalone versions.

AVG

Grisoft provide a free version of their AVG antivirus system. Although not licensed for organisational use, you might recommend this for staff to use on their home computers.

Open Source – ClamWin & WinPooch

On the open source front ClamAV has long been one of the anti virus products with the fastest response time to new viruses.

Originally designed for protecting UNIX servers, a version called ClamWin is available for Windows PCs. If installed with WinPooch, the two programmes will protect you against viruses and spyware. This is a relatively new programme, probably only for the adventurous.

The importance of firewalls

Recent experience has shown that a computer can be infected with a virus within *seconds* of connecting it to the internet. It is essential that any computer connecting to the internet have a firewall installed and activated first. The most recent versions of Windows XP have a firewall built in.

Staying updated

New viruses appear very regularly. Your antivirus is only as good as its last update. If you are serious about protecting your network, get serious about keeping antivirus software up to date. Your antivirus software should automatically update daily. Check these updates are working.

Do not ignore warnings telling you your antivirus is out of date. Do not scrimp on paying annual subscriptions.

Paying for AV – Charity Discounts

Most anti virus vendors provide significant charity discounts, usually between 40 and 50%. To find out about current discounts, contact the anti virus vendor directly.

Are Mac & Linux offices safe?

Many people believe that, because they are relatively rare, Mac and Linux systems are safe from viruses. In general, they are relatively safer, but viruses have appeared for these systems in recent years. You are advised to install anti virus programmes on Mac and Linux computers as it might still be possible for users to pass on infected files even if they themselves are immune. Most anti virus software vendors also produce products for Linux and Mac.

Evaluating Antivirus

Make sure it meets your needs

If you need file and email server protection, make sure you get it with the package you select.

Check it is Certified

Make sure any antivirus programme you choose is listed on the ICSA Labs list. This shows it has passed tests to find if it gives adequate protection.

Compare costs

Remember that you will usually need to subscribe to updates after the first year. Find out how much annual subscriptions cost, and factor that in when comparing prices. Check for any special offers that include extra annual subscription.

Check out options for laptops if you use them

If laptops will not be connected to a centrally managed system because they are used by roving workers, can they still get updates from the manufacturer?

Try out demos of two or three options

Free demo versions are usually available for 30 days. This gives you a chance to try out the features of the software. Check to see that updates work correctly. Also think about how easy the software is to use. If you find it tricky it may not be for you.

Be Careful not to run two antivirus programmes at same time

This will almost certainly cause problems. Make sure you uninstall any existing antivirus software or evaluation versions before installing a new one.

Other measures

Almost all viruses take advantage of flaws in operating systems such as Windows. As these flaws are discovered the manufacturers of operating systems release free updates to fix them. By regularly checking for, and installing security updates you reduce the risks of viruses affecting your systems.

Windows updates are available for free at www.windowsupdate.com. If you run Windows XP, activate automatic updates to make this a no-brainer.

Antivirus Products

Vendor	Standalone Product Name	Centralised Product Name	Charity Discount	Free Trial	Min Computers for Centralised	Notes
GFI	n/a	GFI Mail Security	50% discount on original purchase. 20% discount on subsequent annual subscriptions	Yes		Only provides virus and spam protection on mail server
Grisoft	AVG Pro	AVG SOHO Network	50% discount	30 Days		Subscriptions are for two years rather than one.
McAfee	Internet Security Suite		Up to 50%	30 Days		
Sophos	n/a	Sophos Antivirus	40 - 50%	30 Days	5 PCs + Server	Can spread cost of discounted multi year

Vendor	Standalone Product Name	Centralised Product Name	Charity Discount	Free Trial	Min Computers for Centralised	Notes
						license over several years
<u>Symantec</u>	Norton Antivirus	Symantec Antivirus	Yes - contact reseller for details	30 Days	10 PCs + Server	

Source : <http://www.ictknowledgebase.org.uk/choosingantivirus>