Viruses and Windows 95

Although almost all viruses are written for DOS, most still function under Windows 95. Windows 95 allows you to run DOS programs, and so a virus attached to a DOS program can also run. Even though the ability of many DOS based parasitic viruses to infect other programs, especially Windows 95 specific programs, is restricted, the side effects are still likely to function. In addition, most boot sector viruses are PC viruses, rather than DOS viruses, and as such will be able to infect PCs irrespective of the operating system they are running. Furthermore, macro viruses will infect documents on any operating system supported by the relevant application.

How SWEEP can help

Computer viruses often include side-effects, which can range from the relatively harmless to the decidedly malicious. Viruses can spread widely before these side-effects are seen, so it is vital to detect and eliminate them as soon as possible. This is SWEEP's main purpose.

SWEEP for Windows 95:

- Checks local hard disks, floppy disks and networks for the presence of all viruses known to Sophos at the time of SWEEP's release.
- Looks for both virus fragments (small fixed parts of the virus which can be used to recognise it) and virus identities (a set of known characteristics of a virus) which allows reliable detection of polymorphic viruses.
- Easily detects polymorphic viruses using Sophos' advanced Virus Description Language (VDL) and a built-in code emulator.
- Detects and disinfects Microsoft Word and Excel macro viruses.
- Is updated twelve times a year, and urgent updates can be distributed by fax or email or downloaded from the Sophos web site.
- Provides automatic updating for networked PCs.
- Offers two levels of security, allowing a 'quick sweep' which looks for virus identities in parts of executables likely to contain a virus, and a 'full sweep' which looks for virus fragments in every part of every file.
- Features an 'immediate mode' which allows checking on demand, along with a 'scheduled mode' which allows multiple scheduled jobs to be configured for automatic operation.
- Can notify network managers automatically, via Microsoft Exchange, if a virus is found.
- Includes an extensive on-line virus information database.
- Is a 32-bit application and is fully Windows 95 compliant.

SWEEP is also available for DOS/Windows, Windows NT (i386 & Alpha AXP), Novell NetWare, OpenVMS (VAX & Alpha AXP), OS/2 and Banyan VINES.

Updating SWEEP

Updating SWEEP

Registered users of SWEEP are sent an updated SWEEP disk in the first week of every month. SWEEP for Windows 95's 'auto-upgrade' facility makes installing these upgrades simple.

Urgent SWEEP updates

Viruses are detected using Sophos' proprietary Virus Description Language (VDL). VDL identities for the detection and disinfection of viruses can be encoded as IDE (identity) files which consist entirely of printable ASCII characters. New identities can be faxed, emailed or downloaded from Sophos' web site (http://www.sophos.com). Save the VDL update in an ASCII file with an 'IDE' extension (e.g. NEWVIRUS.IDE), and place this file in the SWEEP folder. SWEEP must be stopped and restarted for any changes to take effect.

Centralised distribution of IDE files

With a central installation of SWEEP with 'Auto-upgrade' enabled, the IDE file can be placed in the SWEEP destination folder on the file server. The local installations will receive the new IDE file the next time they are automatically upgraded.

IDE files and the InterCheck client

A new IDE file introduced to a local installation of the SWEEP for Windows 95 InterCheck client will not be recognised until InterCheck is restarted. When InterCheck is restarted, the virus check on start-up will behave as if SWEEP has been updated. The local checksum file will therefore normally be purged. See the 'What does InterCheck check?' section of the 'Configuring InterCheck clients' chapter for more information.

Using SWEEP

Overview of the SWEEP display

The menu and toolbar

The icons in the toolbar provide short-cuts to commonly used menu options.

The immediate and scheduled mode tabbed pages.

The immediate mode page is displayed on start-up. This contains the file list along with the progress indicator for immediate operation.

The immediate mode file list shows the drives, paths and files that can be swept on demand. An ‘active’ light indicates currently selected entries. The selection status of an entry can be toggled by clicking the selection indicator to the left of its icon.

The progress bar indicates the state of an active sweep. The scheduled mode progress bar also shows the name and time of the next scheduled job.

On-screen log

After a job is started for the first time, the SWEEP display expands to incorporate the on-screen log. This contains information about the current session including all log messages since SWEEP was started.

Immediate mode

Starting an immediate sweep

To sweep all the selected drives, paths and files, select *Sweep* from the *File* menu or click the associated ‘GO’ icon.

Any individual item in the immediate mode display can be swept by double-clicking on its icon in the file list.

Default immediate mode file list

All local drives are displayed on the immediate mode page and all local hard drives are marked as selected.

Adding new items for immediate sweep

To add new items for immediate sweep, press *Add* on the immediate mode page. This will display the new item details dialog.

- path name
- file types
- subfolders

Removing items from immediate sweep

Highlight the name of the path to be removed and click *Remove*. An entry in the file list is highlighted by clicking on the path name.

Editing an item for immediate sweep

To edit an entry in the file list, highlight the name of the path to be edited and click *Edit*. This will display the item selection dialog, as described in the ‘Adding new items for immediate sweep’ section above.

Scheduled mode

To view or edit scheduled options, click on the ‘scheduled’ tab.

Default scheduled mode job list

By default, a job named ‘Default’ is created. This will sweep the system at 13.00 every day, unless it is deselected or removed from the job list.

Adding a new scheduled job

To add a new scheduled job, press *Add* on the scheduled mode page. You will be prompted for a job name, and will then be presented with the scheduled mode configuration page as described in Configuring SWEEP.

Removing a scheduled job

Highlight the name of the job to be removed on the scheduled mode page and click *Remove*.

Editing a scheduled job

Highlight the name of the job to be edited and click *Edit*. This will display the scheduled mode configuration page as described in Configuring SWEEP.

Stand-alone and networked Windows 95 InterCheck clients

There are two types of InterCheck client for Windows 95: stand-alone and networked. See What is InterCheck? for an overview of InterCheck and the types of InterCheck client.

Installing Windows 95 InterCheck clients

Stand-alone clients are installed by the SWEEP installation program. Networked clients are installed from the server.

Using Windows 95 InterCheck clients

Starting InterCheck clients

Stand-alone Windows 95 InterCheck clients start automatically each time Windows 95 is started, before any network connections are made.

Networked Windows 95 InterCheck clients are started from the user's login script.

InterCheck clients in operation

Neither the stand-alone nor networked InterCheck clients require user input during normal operation.

InterCheck intercepts all access to program files. This includes accessing a program to extract its icon, as Explorer does the first time a program's icon is displayed. Thus, there may be a small delay browsing the network using Explorer while InterCheck is active.

The renaming of program files is not intercepted, so files can be renamed or moved within a logical drive without being checked.

The Windows 95 InterCheck clients disable access to floppy disks infected with a boot sector virus.

Stand-alone Windows 95 InterCheck clients do not display 'requesting authorisation' messages, thus speeding up the checking process.

Networked Windows 95 InterCheck clients display a 'requesting authorisation' message when communicating with an InterCheck server. There may sometimes be a delay before the InterCheck client can display this message because Windows 95 does not allow the display to be updated while certain system functions are being performed.

Configuring Windows 95 InterCheck clients

Both types of client are configured with the InterCheck configuration file.

Configuring SWEEP

About configuring SWEEP

Select *Configuration* from the *Options* menu or click the associated icon to call up the configuration page for the mode whose tabbed page is currently displayed.

Immediate and scheduled modes are configured independently.

Sweeping mode

- sweeping level
- priority
- compressed files

Action on virus detection

- disinfect boot sectors
- disinfect documents
- infected files
- request confirmation

Notification on virus detection

When SWEEP detects one or more viruses, it can send a notification message through Microsoft Exchange. If Microsoft Exchange is not installed, this option will not be available (see Mail profile).

- notify timing
- notification list

Reporting results

The report file contains information about individual immediate or scheduled jobs. It is generated in addition to the continuous log file.

- report mode
- report file

File list (scheduled mode only)

The scheduled mode file list is similar to the immediate mode file list, but specifies the files to be swept in a scheduled job. The default scheduled mode file list is the same as that for immediate mode, except that local floppy drives are not listed.

Time (scheduled mode only)

SWEEP can be configured to run at particular times on specific days of the week, for example, once a day on weekdays and twice a day at weekends.

The virus library

Starting the virus library

Select *Virus Library* from the *View* menu or click the associated icon to start the on-line virus library.

Information on a particular virus

Information about the highlighted virus can be displayed by clicking *Info* or by double-clicking its name. This information includes advice on disinfection.

Searching for a particular virus

The virus library can be searched for viruses with certain characteristics. Click the *Find* button to enter search criteria.

- infected objects
- memory resident
- disinfectable by SWEEP
- trigger conditions
- text in description

After a search, *Find Prev* and *Find Next* will find the previous (or the next) entry in the database which matches the search criteria.

SWEEP options

SWEEP command line qualifiers

-AUTO Auto start and exit

Starting SWEEP for Windows 95 from a command line in the following way

```
SWEEP95 –AUTO
```

will force SWEEP to perform an immediate sweep, with all user input, stop and unload options disabled. If no viruses or errors are detected, SWEEP will unload at the end of the job. If viruses or errors are detected SWEEP will display its normal messages and re-activate all controls.

-I Auto start

The -I command line qualifier causes SWEEP to perform an immediate sweep as soon as it is loaded. User input is not disabled, and SWEEP will not unload at the end of the immediate job.

SWEEP can also be set to start as soon as Windows 95 starts, by placing a shortcut to it in the Windows 95 StartUp folder.

-NI No interrupting

Suppresses all options to stop SWEEP. The STOP button and all internal unload mechanisms are disabled. When combined with the -I option, all these options will be disabled until the end of the immediate job, when they will be re-activated.

-NM No memory check

The -NM qualifier suppresses the sweeping of memory during SWEEP startup.

-NW No warning messages

The -NW qualifier suppresses any warning messages during SWEEP startup. This option is used when SWEEP is installed to start automatically.

Sweep memory

SWEEP will check memory automatically for memory resident viruses when it is first started. Memory can also be swept at other times by clicking *Sweep Memory* from the *File* menu.

Set log folder

SWEEP maintains a continuous log of all of its activity. This log file contains administrative messages along with the messages described in Virus detected messages and Error messages. The location of this log can be specified by the *Set Log Folder* option from the *File* menu.

By default the log file will be saved in the root folder of the first local hard drive, but this can be changed by clicking *Set Log Folder* from the *File* menu.

Executables

The list of file extensions to be treated as executables by SWEEP can be edited with this option. This list is only used if SWEEP is set to check ‘executable’ rather than ‘all’ file types.

Exclusion list

The exclusion list contains the specific files to be excluded from all SWEEP operations.

Mail profile

This option is only available if Microsoft Exchange is installed.

To send notification messages SWEEP must be able to log on to Microsoft Exchange without supplying a password. If your default profile requires a password to be entered, create a new profile with a preset password and use this option to select it.

Restore defaults

This option will set all SWEEP settings back to their defaults, after requesting confirmation. This will destroy all scheduled jobs as well as resetting other options.

Clear log

The on-screen log provides a record of activity in the current session, and reflects the information that is appended to the continuous log file. This option clears the on-screen log, but does not affect the continuous log file on disk.

Progress bar

In order to display the progress bar, SWEEP has to count all the items to be swept before starting the virus check. On large network drives this can take a significant length of time, which can be saved by disabling this option. This option will not affect any SWEEP jobs that are already running at the time the option is selected.

Treating viral infection

Establishing a clean environment for disinfection

A virus can be eliminated from the memory of an infected PC by switching the PC off and booting from an uninfected (and preferably write-protected) system disk. This is called performing a secure bootstrap or a clean boot, and is essential to providing a safe environment from which the disinfection process can begin.

Assuming the computer's memory is free from viruses, it is safe to move or copy infected files in the ways described below.

Treating infected floppy disks

If a virus is discovered on a floppy disk that has just been received, then it is relatively easy to deal with.

Infected files and documents can be automatically renamed, deleted, shredded, moved or copied if SWEEP has been configured to do so.

Floppy disks infected with boot sector viruses can normally be disinfected automatically by SWEEP. However, if SWEEP does not disinfect the boot sector, data can be safely copied off the disk and the disk reformatted. Formatting a floppy disk destroys all the data that is stored on it, including any viruses.

The source of the infected disk should then be established to locate any other infected disks.

Important! If just one infected floppy escapes disinfection other disks and PCs could be reinfected.

Note: It is advisable to preserve a clearly marked infected floppy for analysis and evidence.

Treating infected hard disks

If SWEEP discovers a virus on a hard disk, it is likely that the infection is widespread and considerably more work may be required to recover from the virus attack. The first step is to identify all infected PCs and disks.

The next step involves stopping the virus from spreading. Infected PCs should be disconnected from the network and all disk interchange between PCs suspended.

After the virus outbreak has been contained, the recovery process can begin. The virus has to be eliminated from all the infected floppy disks, as described above, as well as from infected hard disks.

If only files have been infected on the hard disk, these can be dealt with as described above.

However, if the boot sector of the hard disk is infected, then SWEEP for Windows 95 will not disinfect it. You should use the DOS version of SWEEP after a clean boot. See the DOS SWEEP user manual for more details, or contact Sophos' technical support.

After disinfection

There are a few other things worth bearing in mind after a virus attack:

- Uncover and close the loopholes which allowed the virus to enter the organisation.
- Inform any possible recipients of infected disks outside the organisation that they may be affected by the virus.
- In the UK, inform the *Computer Crime Unit* of *New Scotland Yard* in London about the attack (Tel 0171 230 1177, Fax 0171 230 1275).

Troubleshooting

SWEEP runs slowly

Full sweep

By default, SWEEP will perform a ‘quick sweep’ which checks only the parts of files which are likely to contain a virus. However, if ‘full sweep’ is set SWEEP will be much slower. The speed difference between ‘full sweep’ and ‘quick sweep’ depends on the configuration of the computer, but typically the ‘quick’ level is 5 to 10 times faster than the ‘full’.

Checking all files

By default, SWEEP will only check files defined as executables. If SWEEP is checking all files, it will take longer than if only executable files are being checked.

Network drives selected

Some network drives will be much larger than a local hard disk, and so will take significantly longer to check. Most network interfaces provide much slower access than a local hard disk, which can reduce the speed further still.

Progress bar selected

If the progress bar is selected then SWEEP will have to count all the items that are to be swept. This can take several minutes on large network drives.

Virus fragments

The report of a virus fragment indicates that a part of a file matches a part of a virus. There are three possible causes:

Variant of a known virus

Although new viruses appear all the time, many of them are based on existing ones, so that code fragments typical of a known virus may appear in files infected with a new one. SWEEP is able to take advantage of such similarities in its search for virus fragments. See New viruses.

Corrupted virus

Many viruses contain bugs in their replication routines so that they sometimes 'infect' target files incorrectly. A portion of the virus body (possibly a substantial part) may appear within the host file, but in such a way that it will never be actuated. In this case SWEEP will report 'Virus fragment' rather than 'Virus'. A corrupted virus cannot spread.

If a file contains a corrupted virus, remove the infected file and replace it with a clean copy.

False positive

On rare occasions, a virus fragment may be reported in an uninfected file. This may happen for a number of reasons. Swap files, for example, may contain fragments of real viral code on a computer on which infected files were recently used.

If in doubt, contact Sophos' technical support for advice or send us samples. It may be a new virus.

To decrease the chance of false positives:

- Only sweep executables.
- Perform a 'quick sweep' rather than a 'full sweep'.

False negatives

A false negative is the opposite of a false positive, i.e. the event in which SWEEP fails to report a virus in an infected file.

If a false negative is suspected:

- Ensure the latest version of SWEEP is being used.
- If a Word macro virus has been discovered, make sure that all file types are swept.

Virus not disinfected

If a virus was not disinfected:

- Check that ‘disinfect documents’ is selected.
- Make sure the disk is not write-protected.

New viruses

Any virus-specific software will discover only those viruses which were known to the manufacturer at the time of software release. If a virus unknown to SWEEP is suspected, please send Sophos a sample and a description of the symptoms, as soon as possible. There is a chance that the virus is ‘in the wild’ and the sooner that it gets incorporated into SWEEP, the better.

The infected sample can be emailed to support@sophos.com. Alternatively upload it onto our ftp site (ftp.sophos.com) or our secure bulletin board (+44 1235 559936) after contacting Sophos. When the virus has been analysed (which may take from 10 minutes to a few days), we will fax or email the IDE file which can be used to update SWEEP. The latest IDE files can also be downloaded from our web site (http://www.sophos.com).

On-screen log messages

Virus detected messages

Virus: '*virus name*' detected in *location*
No action taken

Virus: '*virus name*' detected in *location*
File deleted

Virus: '*virus name*' detected in *location*
File renamed to *filename*

Virus: '*virus name*' detected in *location*
File shredded

Virus: '*virus name*' detected in *location*
File moved to *new location*

Virus: '*virus name*' detected in *location*
File copied to *new location*

Virus: '*virus name*' detected in *location*
Error *action*

Virus: '*virus name*' detected in *location*
Has been disinfected

Virus: '*virus name*' detected in *location*
Error: Disinfection failed

Virus fragment: '*virus name*' detected in *location*
No action taken

Error messages

Error: Could not open *filename*

Error: Could not read *filename*

Error: Sector size of drive *drive* is too large

Error: Could not open report file *filename/directory*

Error: Log file *filename* could not be opened.
Log data will not be saved.

Error: Could not notify *user*

Error: Could not initialize mail system

Error: Could not login to mail system

Error: Could not allocate memory for *filename/directory*

On-screen log pop-up virus detected messages

Double-clicking on a line with a virus name will display more information about that virus. SWEEP's 'virus detected' message contains the name and location of the virus, followed by information about the action taken. This action will depend on the settings on the Action tab of the Configuration page.

The *location* will be one of either:

filename
Drive *drive name*: Sector *sector number*
Disk *disk* Cylinder *cylinder* Head *head* Sector *sector*
Memory block at address *8 digit hexadecimal address*

No action will be taken if SWEEP has been configured not to disinfect boot sectors or documents, and not to rename, delete, shred, move or copy any infected files.

The file in which the virus was found has been deleted.

The *filename* will be the old name with the file extender changed to a number. For example, if a virus was named VIRUS.EXE it would be renamed to VIRUS.000, or VIRUS.001 if there was already a file called VIRUS.000.

The infected file has been deleted and cannot be recovered.

The *new location* is the location specified in the Action tab of the Configuration option.

The *new location* is the location specified in the Action tab of the Configuration option.

The file could not be deleted/renamed/shredded/moved/ copied. If the infected file was found on a floppy disk, check that the disk is not write protected.

The *action* will be one of either:

```
deleting file
renaming to filename
shredding file
moving to location
copying to location
```

Important! The infected file will remain unchanged and may be able to infect other disks and files.

SWEEP for Windows 95 can automatically disinfect, or remove, certain boot-sector viruses on floppy disks if the ‘disinfect boot sector’ option has been selected. SWEEP for DOS will be required to disinfect a hard disk boot sector. SWEEP can also automatically remove the viral macros from documents infected with certain types of macro viruses.

SWEEP was unable to disinfect the boot-sector. See the ‘Treating viral infection’ chapter for advice on disinfecting a boot sector.

Important! The infected disk will remain unchanged and may be able to infect other disks and files.

Double-clicking on a line with a virus name will display more information about that virus. SWEEP's 'virus fragment detected' message contains the name and location of the virus fragment.

SWEEP does not remove virus fragments.

On-screen log pop-up error messages

The file called *filename* was on the list of files to be swept, but could not be opened for examination. Check that the file is not in use or already open.

The file called *filename* was on the list of files to be swept, but could not be read. This might indicate that the file or the disk is corrupt.

SWEEP will only currently sweep disk sectors of 2k or less. It is highly unlikely that it will ever encounter sectors larger than this.

The filename and folder of the report file are specified on the Report tab of the Configuration page. SWEEP will not be able to open the report file if its filename is not valid, or if it cannot access the file or folder.

The location of the log file is specified with the *Set Log Folder* option from the *File* menu. SWEEP will not be able to open the log file if it cannot access the file or folder.

The *user* was on the notification list but could not be notified. This could be because the *user* is no longer on the list of recognised Microsoft Exchange users, or because a profile requiring user entry of a password was used.

SWEEP checks to see if Microsoft Exchange is installed before allowing access to the notification options. However, there might be some situations in which SWEEP allows access even though Microsoft Mail is not setup correctly. For example, the MAPI mail interface might not be installed correctly.

If SWEEP cannot login to the mail system, then the profile name may be invalid.

SWEEP needs to allocate memory for the report if it is to send it to the users on the notification list. If the report is too big then SWEEP will not be able to load it into memory to send it. The report file can become very large if it is configured to list every file that it examines (see the ‘Report mode’ section of the ‘Configuration’ chapter).

Pop-ups

Specifies the drive, folder or filename to be swept. Both mapped and UNC path names can be entered. Wildcards can also be included. *Browse* can be used to select items.

Only those files defined as executables will be swept, unless the all file types option is selected.

Subfolders will be swept if this option is selected.

The ‘quick’ sweeping level only checks the parts of files likely to contain viruses, while the ‘full’ level examines the complete contents of each file. The ‘full’ level is more secure because it can discover viruses ‘buried’ underneath other code appended to a file, as well as minor virus mutations and corruptions. However, ‘full’ sweeping level is much slower, and for normal operation ‘quick’ sweeping is sufficient.

To minimise SWEEP's impact on system performance it can be set to run at 'low' priority. This will increase the time taken to sweep the system.

SWEEP is capable of looking for viruses inside files compressed with PKLite, LZEXE and Diet.
SWEEP does not currently look inside files which have been compressed using static compression utilities such as ARC, ZIP and ZOO. These files will need to be decompressed before sweeping. InterCheck provides automatic protection from viruses in files which have been compressed, because access to every unrecognised item (e.g. a newly decompressed file) is only granted after that item has been checked for viruses.

SWEEP can disinfect most boot sector viruses from floppy disks. Confirmation will be requested before a floppy disk is disinfected. Normally this option should only be used in immediate mode, because scheduled jobs will be suspended until confirmation is granted or refused by the user.
SWEEP for Windows 95 will not disinfect a hard disk's boot sector because some boot sector viruses are capable of performing stealth functions under Windows 95. To disinfect a hard disk boot sector, boot from a clean floppy disk and use the DOS version of SWEEP.

SWEEP can remove the viral macros from documents infected with certain types of macro viruses. If the document disinfection fails, the infected file will be dealt with in the same way as any other infected file.

If an infected file is found, there are several actions that can be taken to make that file safe. Renaming or moving an executable file should prevent it from being run, but deleting or shredding the file will ensure that it cannot be accidentally executed. Shredding is a more secure type of file deletion that overwrites the contents of the file.

If this option is selected, any action that involves changing infected items (i.e. disinfecting boot sectors, disinfecting documents, and renaming, deleting, shredding and moving infected files) will ask for confirmation before proceeding. This option is only available in immediate mode, where it is enabled by default.

The notification message can be the full report file sent at the end of each job, and/or a brief message for every infected file found.

The notification list defines the users who will be notified. Clicking *Add* will connect to Microsoft Exchange, and the list of possible users will be displayed.

Setting list filenames will cause SWEEP to record in the report file the names of every item examined. Otherwise only infected items will be recorded.

The report file will be saved to disk.

Viruses can attach themselves to COM and EXE files; they can infect the master boot sector or the DOS boot sector; companion viruses place the virus code in a COM file with the same name as the EXE file; link viruses subvert directory entries to point to the virus code; and Windows viruses affect Windows executables. Trojan horses are not viruses, but are programs which provide unanticipated and undesired side effects when executed.

Memory resident viruses stay in memory after they are executed and infect other objects when certain conditions are fulfilled.

A tick in these boxes will include in the search viruses which can be removed from floppy and hard disks.

Many viruses require specific conditions, such as a certain time or date, in order to exhibit side-effects.

The ‘text description’ option will search for a string which appears in the information about that virus.

What is InterCheck?

SWEEP with InterCheck technology offers on-access virus checking, while SWEEP alone offers on-demand checking. InterCheck ensures that unknown files (e.g. programs, documents, email attachments or Internet downloads) and disks cannot be used until checked for viruses.

InterCheck splits the task of virus detection between a client and a server. The **InterCheck client** determines whether items on the client workstation should be checked for viruses, while in a networked environment the **InterCheck server** performs the actual virus checks where necessary.

There are two main types of InterCheck client: networked and stand-alone. A **networked InterCheck client** exists on a separate machine from the InterCheck server, and communicates with it over the network. A **stand-alone InterCheck client** does not have to communicate with a remote InterCheck server, and uses a local installation of SWEEP to check for viruses.

A networked InterCheck client is easier to administer and uses fewer system resources on the client workstations. A stand-alone InterCheck client generally offers faster initial authorisation of files, and can also be used on machines not always connected to the network. Either way, InterCheck is the most efficient way of protecting users from viruses - each item is checked for viruses only once, unless it is modified in which case it is rechecked.

How does InterCheck work?

The InterCheck client software monitors all file and disk accesses. Whenever an item is accessed, it is compared with a list of authorised items. If a match is found the access is permitted. If a match is not found, the networked InterCheck client sends a copy of the item to the InterCheck server for checking, while the stand-alone InterCheck client checks with a local installation of SWEEP.

If the item is found to be clean, it is added to the list of authorised items and the access is allowed to continue. Any further accesses of this item are then completed without the need for further authorisation, unless it is modified, in which case authorisation is again automatically requested.

However, if a virus is found, InterCheck prevents access to the item, so the workstation cannot be infected.

Features

Complete cover

Of the network: InterCheck provides complete virus-protection for the entire network with minimal performance and memory overheads, and supports the widest range of client and server platforms.

Of the workstation: InterCheck monitors access to all programs, boot sectors, documents, email attachments, Internet downloads and CD-ROMs.

Performance

Once an item has been authorised, further virus-checking is not needed unless it changes or SWEEP is updated. The process of checking that an item has been authorised is much faster than performing a full virus check.

Automatic reporting

Many virus incidents are more serious than they need to be because users fail to report viruses to their managers. If an InterCheck client is connected to the network and a virus is found, a report can be sent to the network supervisor automatically.

Easy administration

InterCheck clients can be centrally controlled, configured and updated. Networked InterCheck clients can in many cases be installed automatically over the network.

Portable PCs

InterCheck clients can continue to provide the same levels of protection even when a PC is not connected to the network.

Overview of InterCheck installation and configuration

Networked InterCheck clients require a separate InterCheck server. This involves installing SWEEP and the InterCheck software on the file server, and running SWEEP in InterCheck server mode. Networked InterCheck clients are currently available for DOS, Windows 3.x, Windows for Workgroups, Windows 95 and Macintosh workstations.

Stand-alone InterCheck clients do not require an InterCheck server. In the case of Windows 95 and Windows NT, the stand-alone InterCheck clients are installed as part of the SWEEP installation process. Stand-alone InterCheck clients are currently available for Windows 3.x, Windows for Workgroups, Windows 95 and Windows NT workstations.

Native InterCheck server functionality is currently included in SWEEP for NetWare, Windows NT (Intel & Alpha), OpenVMS, DOS, OS/2 and Banyan VINES. SWEEP for DOS can also be used to provide InterCheck server functionality for other operating systems.

InterCheck server installation and configuration

Windows NT, NetWare, OpenVMS, OS/2 & Banyan VINES

See the SWEEP for Windows NT, NetWare, OpenVMS, OS/2 and Banyan VINES user manuals (i.e. the InterCheck server user manuals) respectively.

DOS

See the SWEEP for DOS InterCheck Supplement.

Stand-alone InterCheck client installation

Windows 3.x & Windows for Workgroups

See the ‘Installing InterCheck clients’ chapter of the InterCheck server user manuals.

Windows 95 & Windows NT

See the ‘Installing SWEEP’ chapters of the SWEEP for Windows 95 and SWEEP for Windows NT user manuals respectively.

Networked InterCheck client installation

DOS, Windows 3.x, Windows for Workgroups, Windows 95 & Macintosh

See the ‘Installing InterCheck clients’ chapter of the InterCheck server user manuals.

Stand-alone InterCheck client configuration

Windows 3.x, Windows for Workgroups & Windows 95

See the ‘Configuring InterCheck clients’ chapter in the InterCheck server user manuals, and also in the SWEEP for Windows 95 user manual.

Windows NT

See the ‘Configuring SWEEP’ chapter of the SWEEP for Windows NT user manual.

Networked InterCheck client configuration

DOS, Windows 3.x, Windows for Workgroups & Windows 95

See the ‘Configuring InterCheck clients’ chapter of the InterCheck server user manuals.

About Sophos Plc

Sophos Plc was founded in 1980, moved into data security in 1985, and is now a world leader in the development of software for data security and computer virus detection. At the centre of this success is a reputation for innovative and sophisticated products backed by quality support.

All Sophos products are designed, manufactured and supported by the company, which exports worldwide through a network of subsidiaries and international distributors. These products include:

- "Sophos Anti-Virus", comprising “SWEEP” for on-demand scanning and “InterCheck” for on-access scanning.
- "D-FENCE" disk authorisation software.
- "VACCINE" checksumming virus detection system.
- "E-DES" file encryption package for DOS and Windows.

Contacting Sophos

Email

General enquiries:
enquiries@sophos.com

Sales enquiries:
sales@sophos.com

Technical support:
support@sophos.com

Comments on manuals, on-line help, etc.:
publications@sophos.com

Sophos Plc, UK

Tel +44 1235 559933

Fax +44 1235 559935

Sophos Plc
The Pentagon
Abingdon Science Park
Abingdon
OX14 3YP
England

Sophos Inc, USA

Tel 781 932 0222

Fax 781 932 0251

Sophos Inc
18 Commerce Way
Woburn
MA 01801
USA

Sophos GmbH, Germany

Tel 06136 91193

Fax 06136 911940

Sophos GmbH
Am Hahnenbusch 21
D-55268 Nieder-Olm
Germany

Sophos Plc, France

Tel 01 46 92 24 42

Fax 01 46 92 24 00

Sophos Plc
2, Place de la Défense
BP 240
92053 Paris la Défense
France

WWW
http://www.sophos.com/

What is a computer virus?

A computer virus ‘infects’ programs and disks by attaching copies of itself to them:

- A boot-sector virus will infect the boot sector of disks.
- Parasitic, companion, link and macro viruses infect files.
- Multi-partite viruses can infect both files and boot sectors.

A PC or disk is said to be infected if it contains an infected boot sector and/or one or more infected files. A PC’s memory is said to be infected if it contains some form of memory resident virus.

There are three ways in which a PC and a PC’s memory can become infected:

- The PC is bootstrapped from a disk infected with a boot-sector or multi-partite virus.
- An infected program file is executed, e.g. by issuing its filename as a command at the command prompt, or by double-clicking its icon within Windows.
- A file infected with a macro virus is loaded into the application which ‘executes’ the relevant macro language.

See Sophos’ *Data Security Reference Guide* for more information on viruses.