Dr Solomon's WinGuard

Contents

CompuServe: GO DRSOLOMON

Introduction

Dr Solomon's WinGuard:

Protects your PC all the time you are running Windows
Intercepts every file and disk accessed, checking them for viruses
Uses the award-winning FindVirus scanning technology for complete accuracy
Includes Generic Decryption Engine to intercept polymorphic encrypted viruses
Provides transparent, background virus protection without inconveniencing PC users
Is fully compatible with 32-bit file and 32-bit disk access
Requires zero base memory in DOS boxes

What is a VxD?

A VxD is a Virtual Device Driver for the Windows operating system. It is comparable to TSRs or device drivers that run under DOS. In other words, a VxD is a device driver that runs constantly in the background during Windows sessions.

What is Dr Solomon's WinGuard?

Dr Solomon's WinGuard is a VxD: a full 32-bit device driver which runs constantly in the background of Windows sessions. WinGuard uses the award-winning FindVirus scanning technology to scan all executed or copied files. If a file is virus-infected, WinGuard will prevent access to it and can be configured to send an alert message to a system administrator. NB Network messaging is not currently available to users of the Windows 95 toolkit.

WinGuard components

WinGuard consists of two main components:

A VxD (WINGUARD.386) which runs as part of the Windows environment
A front end and control panel (WGFE.EXE) which enable the user to configure WinGuard's options, and to receive virus alerts

The front end also fetches information from the WinGuard VxD to assure you that it is working, and to tell you how it is configured

Because Dr Solomon's WinGuard is a VxD, it occupies Windows memory and not DOS memory. This allows it to contain substantially more functionality than a DOS-based TSR.

Installing Dr Solomon's WinGuard

WinGuard is installed by Dr Solomon's Anti-Virus Toolkit for Windows. The install process copies the files from the disks, and adds the necessary lines to the Windows system files. These are WIN.INI and SYSTEM.INI for the Windows 3.x version, and WIN.INI and the Registry for the Windows 95 version.

It is also possible to add the necessary lines to your system files from WinGuard's front end (see Configuring WinGuard's virus protection). WinGuard can also be uninstalled from the front end.

If you wish to install WinGuard on many machines at once, a command line program is provided for this purpose. In Windows 3.x, this program is called TKUTIL and in Windows 95 it is called WTKUTIL. Please note that WTKUTIL is a Win32 console program, which means that it can only be run in a DOS box under Windows 95.

These programs can be used in the following way:

<W>TKUTIL ADD WINGUARD <Installation directory> - where you must provide the directory containing the Anti-Virus Toolkit files. This will make the necessary modifications to the Windows system files to enable WinGuard.

<W>TKUTIL REMOVE WINGUARD. This will remove the modifications and thus disable WinGuard on that machine.

By putting these lines into your users' LOGIN scripts it is thus possible to install WinGuard easily across a network.

<W>TKUTIL WINGUARDCHECK. This checks if WinGuard is loaded, prints out a message to report its status, and returns errorlevel 0 if WinGuard is active, and 1 if WinGuard is not active.

You can also use <W>TKUTIL to configure WinGuard across a network. This is different for Windows 3.1 and Windows 95.

Windows 3.1:

Firstly, you must set up WinGuard on your own machine identically to how you wish WinGuard to be configured for your users. Then, using an editor, copy the sections [WinGuard] and [WinGuard Front End] from your SYSTEM.INI file to a text file called, for example, WGCONFIG.INI.

WGCONFIG.INI might then look like this:

```
[WinGuard]
allfiles=TRUE
drives=local

[WinGuard Front End]
FILEALERT=File <file> has the <virus> virus!!! Please phone Tech Support.
BOOTALERT=Disk <disk> has the <virus> virus!!! Please phone Tech Support.
NETWORKMSG=<user>'s machine has a virus!!!
USERID=Phil
SECURITY=1234
```

TKUTIL INIUPDATE <target> <updatefile> takes the section(s) in the update file and either adds them to the target file or replaces the section(s) in the target file if it already exists. So in this case, you would enter

```
TKUTIL INIUPDATE SYSTEM.INI O:\UPDATE\WGCONFIG.INI
```

if you put the WGCONFIG.INI file in the directory O:\UPDATE.

Windows 95:

Firstly, you must set up WinGuard on your own machine identically to how you wish WinGuard to be configured for your users. Then type:

```
WTKUTIL SAVESETTINGS WINGUARD MYSETTINGS.TXT
```

This saves your settings in text format into the file MYSETTINGS.TXT. If you then copy this file to a suitable network drive, and add the line:

```
WTKUTIL LOADSETTINGS WINGUARD O:\TOOLKIT\MYSETTINGS.TXT
```

to the user's LOGIN script, these settings will be added to the user's system files.

Configuring WinGuard's virus protection

The options configurable under *Configure/WinGuard...* allow you to install and uninstall the resident scanner and control what is to be scanned.

Select *Configure/WinGuard...* from the menu. If you have previously set a password, you will be prompted to enter the password. (To set and remove passwords see Configuring WinGuard's Front End.) A dialog will appear containing the following options:

WinGuard Enabled:
If this checkbox is enabled, WinGuard will be added to your Windows configuration files (WIN.INI and SYSTEM.INI), and will be active from the next time you start Windows.

If this checkbox is disabled, WinGuard will be removed from your Windows configuration files (WIN.INI and SYSTEM.INI), and will not be active next time you start Windows. The files needed to run WinGuard will NOT be deleted.

Scan all files:
If this checkbox is enabled, all files will be scanned for viruses, not only those with executable extensions. (The section on the 'Scan on writes' checkbox describes when they will be scanned.) This option is useful if you are concerned about viruses being copied after infected files have been renamed.

Scan on writes:
If this checkbox is enabled, files will be scanned after being written to the disk. The files which are scanned in this way are as described in the section on the 'Scan all files' checkbox. Infected files will launch an alert, but the file will not be deleted or renamed.

In its default state WinGuard scans files on copy attempts. Some writes to the disk, such as downloads from the Internet and those resulting from unarchiving, are not the results of 'copies' and would not trigger a scan. You can guard against this by selecting 'Scan on writes', when all files appearing on the disk will be scanned, whatever their source. (This results in copied non-infected files being scanned twice - one scan being triggered by the copy attempt, and the other scan being triggered by the write to disk.)

Close DOS box on virus:
If this checkbox is enabled, then if a virus is found in a program in a DOS box, the DOS box will be terminated next time DOS is idle (i.e. you are at the command prompt). This will prevent you from ignoring any warning you are getting from WinGuard.

Driver file:
This option allows you to select a different driver file for WinGuard, and may be useful if you wish to test a different driver file or store the driver file elsewhere (e.g. on the network). In general this is not recommended, but it may be useful occasionally.

☞ Note that if an invalid file is selected into this box, then WinGuard will not let you restart Windows. If you end up in this situation, you will have to uninstall WinGuard with <W>TKUTIL or by hand.

The default driver file is the same as that used by FindVirus, FINDVIRU.DRV. The Browse button allows you to search your directory structure for a different FindVirus driver file.

☞ Note that if you change the Driver File, you will be prompted twice for confirmation.   There will not normally be any need to change the driver file from the default, FINDVIRU.DRV.

Extra driver:
Data in the file specified in this box is used in addition to the data contained in the main driver file. If a file in the TOOLKIT directory has the name EXTRA.DRV, it will automatically be used as an extra driver, so it

need not be specified in this box. The Browse button allows you to search the directory structure and select a file.

Drives to scan:
This option allows you to select which drives WinGuard will check for viruses. The default, 'All', scans all drives. It is also possible to scan only removable drives, removable drives and your local hard drive, or removable drives and remote (network) drives. You can also supply WinGuard with your own list of drives to scan by selecting 'User defined' and filling in the drive letters in the edit box.

These options may be useful if your machine is very slow, or if you already have protection on some of your network drives, for example, and you wish to avoid the performance hit of scanning each file twice.

Any changes made in this dialog will not take effect until Windows has been restarted. When you click 'OK', you will be asked if you are sure you wish to change WinGuard's setup.   You will then be asked if you wish to restart Windows for the changes to take effect. You can choose to restart Windows or wait until you next start Windows.

See also: Configuring WinGuard's Front End

Configuring WinGuard's Front End

The options configurable under *Configure/Front End...* allow you to control the text that appears on the Alert dialog, the network message on a Novell Network and also to set a password to prevent others changing WinGuard's setup.

Select *Configure/Front End...* from the menu. ☞ Note that you can only do this if WinGuard has been enabled. If you have previously set a password, you will be prompted to enter the password. A dialog will then appear containing the following options:

File virus alarm message:
This string is displayed on the alert dialog when a file virus is discovered by WinGuard. The substring **<file>** is replaced by the name of the file, and the substring **<virus>** is replaced by the name of the virus.

Boot virus alarm message:
This string is displayed on the alert dialog when a boot sector virus is discovered by WinGuard. The substring **<disk>** is replaced by the drive letter of the infected diskette, and the substring **<virus>** is replaced by the name of the virus.

Network message:
This is the Novell NetWare message sent when WinGuard detects a virus. The substring **<user>** is replaced by the ID of the user who is logged on at the time of the alert. NB This option is not currently available to users of the Windows 95 toolkit.

Sent to (User ID):
This is the Novell NetWare user ID of the user to whom the above message is sent. If this box is empty, no message is sent. Typically this should be set up to send a message to the network supervisor or support department. NB This option is not currently available to users of the Windows 95 toolkit.

Password:
Enter a password into this box. If it matches the password in the 'Re-enter Password' box, a password will be set on the two configure dialogs. If they do not match, a warning will be issued.

Re-enter password:
This password must match the password in the 'Password' box.

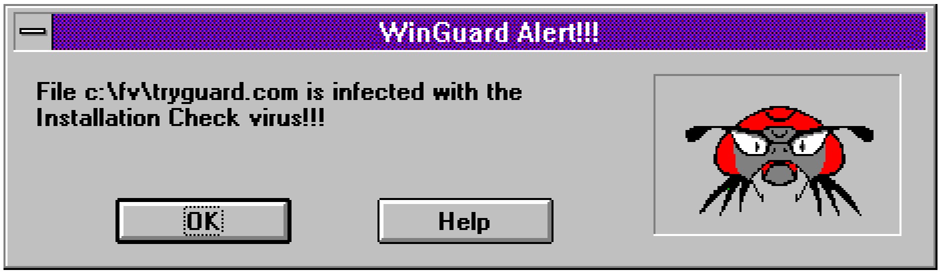
☞ Note that these changes take place immediately after you press 'OK'. It is not necessary to restart Windows for these changes to take effect.

See also: Configuring WinGuard's virus protection

WinGuard Virus Alert

Dr Solomon's WinGuard intercepts virus-infected files and disks as they are accessed. This means it can intercept a virus, before the virus has managed to execute.

If WinGuard intercepts a virus, an alert screen similar to the following will be displayed:



WinGuard Alert!!!

File c:\fv\tryguard.com is infected with the Installation Check virus!!!

If you find a virus...

1. Don't panic.
2. Don't be in a hurry.
3. Work systematically. Don't rush.
4. Inform your company, via the usual chain of reporting.

The company should then arrange to:

1. If appropriate, inform the Police Computer Crime Department.
2. Check all the surrounding computers.
3. Check all floppy diskettes that could have become infected.
4. Call Dr Solomon's, or the local distributor, for technical support, if needed.
5. Review anti-virus policy to try and prevent a recurrence.

Refer to your manual for details on how to use Dr Solomon's Anti-VirusToolkit to repair virus infections.