Contents

The following Help Topics are available:

Introduction

FindVirus is a program which you use to detect and remove viruses. Used manually, or scheduled to run automatically every day, it provides a good measure of protection.

However, FindVirus is only one of the modules of the Dr Solomon's Anti-Virus Toolkit, which is available as an upgrade from Dr Solomon's. The other modules of the Toolkit include WinGuard, which is a virus detector that works constantly in the background. It intercepts viruses automatically to prevent them spreading, and can optionally remove viruses.

Another advantage of upgrading to the full Toolkit is that it can be supported with update information, so that its detection capability covers the latest viruses (which are currently discovered at a rate of 300 to 350 a month).

Main screen

Button	What does it do?	Click for more
Scan	click to scan any disk(s) you have selected in the drive list above.	More
Disinfect	click to disinfect any disk(s) you have selected in the drive list above.	More

File menu

Option	What does it do?	Click for more
Exit	quits Dr Solomon's Anti-Virus	More

Exit

What does it do?

Quits Dr Solomon's Anti-Virus.
Any changes you have made in the scan options will be saved when you exit.

Exit is found under the File Menu

Click for more

Scan options

Scan menu

Select the required option. If you wish to change any scan settings select 'Options' before selecting a scan option.

Option	What does it do?	Click for more
Drive	this will scan a selected drive(s). In the dialog use Shift + Click to select more than one drive.	
Directory	this will scan a selected directory. Select a directory in the dialog. Only one directory at a time can be scanned.	
File	this will scan a selected file. Select a file in the dialog. Only one file at a time can be scanned.	
Options	this allows you to configure scan settings other than the default ones.	More

If a virus is found you will be notified immediately and given the option of disinfecting the file.

Scan options

Option	What does it do?	Click for more
Also scan	you can select to scan for unknown viruses, data (all) files and compressed files.	More
Reporting options	you can also scan for unknown viruses and have a report sent to printer or file.	More
If file cannot be disinfected	you can either rename or delete a file if it cannot be disinfected.	More

Scan menu Main Screen

Also Scan

Option	What does it do?	Click for more
For unknown viruses	will use the Advanced Heuristic Analyzer to search for new viruses not yet recorded in our database. This will, however, increase the scan time.	
Data files	will scan all files regardless of extension. This is usually only necessary if you are dealing with an outbreak of a virus. There is no need to do this in a routine scan. Macros are scanned by default.	
Scan compressed files	will scan inside compressed files which have the extensions listed next to this function. This will, however, increase the scan time.	Disinfecting compressed files

Reporting Options

Option	What does it do?
Report to printer	selecting this box causes FindVirus to output the report to a printer. **Ensure that your printer is switched on.**
Report to file	the file has a default name of FINDVIRU.REP and is stored in the 'C:\ Program files\ Dr Solomon's\Anti-Virus' folder. **You can change the folder and the file name by clicking 'Browse'.**

If file cannot be cleaned

Option	What does it do?
Rename infected files	this will change the first letter of the file extension to 'V' (e.g. .COM would change to .VOM) and is the default setting. If an unknown virus is found please send it to our Technical Support Department. **Delete the infected file as soon as possible.**
Delete infected files	use this to delete any files which cannot be disinfected. Dr Solomon's Anti-Virus deletes the file in such a way that it cannot be undeleted.

Deleting infected files Unknown virus

Disinfect menu

Option	What does it do?
Drive…	will perform a complete check and disinfect any files on the selected drive(s). This will check all files except for compressed files. Shift + Click to select more than one drive.
Directory…	will perform a complete check and disinfect any files on the selected directory. This will check all files except for compressed files. Only one directory at a time can be scanned.
File…	will perform a complete check and disinfect any file. This will check any file except for compressed files. Only one file at a time can be scanned.

How an infected file which cannot be disinfected is dealt with is decided in the scan options configuration.

More on Disinfecting

Info menu

This gives access to the Virus Encyclopedia for information on the various viruses.

Right-click scans

When in the Explorer you can start scans using the right hand mouse button. Right-click on the folder or file you wish to scan and select 'FindVirus...' from the menu. The scan now proceeds as normal.

Virus Encyclopedia

The Virus Encyclopedia holds explicit and offensive language which is contained within virus messages.

The Virus Encyclopedia is in a standard Windows help format. On starting the encyclopedia you see a list of virus names; click on a virus name to see its description. You can use the 'Search' button to find a specific virus in the list.

The description includes details such as whether the virus is polymorphic, and whether it uses stealth.

The Virus Encyclopedia is accessed from the Info menu.

If you find a new/unknown virus

There are two occasions when you could get a new or unknown virus message on your screen:

- a possible new variant of a known virus;
- a completely new virus (found by Advanced Heuristics Analyzer in a FindVirus scan).

By default the infected file is saved with a change to the extension. The first letter to the extension is changed to 'V', e.g. FILE.COM will change to FILE.VOM.

What to do

- Don't panic.
- Don't be in a hurry.
- Work systematically.

If the unknown virus is on a floppy disk:
We recommend that you send the disk to our Technical Support department.
The address is found in the 'Customer Support and Services' chapter in the manual.

If the unknown virus is on the hard disk:

1. Format a floppy disk in the infected computer.
2. Copy any infected files to that floppy disk.
3. Remove the floppy from the drive.
4. Send to Dr Solomon's Technical Support.
5. Disinfect the hard disk using the SOS disk.

If you include a letter, explaining any symptoms you have encountered, we can often tell you what the problem is, even if it is not a virus.

Note:

We cannot reply if we receive an anonymous diskette with no return address. If possible, include a fax and phone number as well as an address.

About viruses Deleting viruses

Cold Boot (Power-off)

How to do a Cold (Power-off) Boot:

1. Switch off the computer.
2. Wait 10 seconds for the power supply to reset.
3. Insert the SOS disk.
4. Switch the computer back on again.

Virus found

About Viruses

A virus is a program that copies itself without the knowledge of the computer user. Typically, a virus spreads from one computer to another by adding itself to an existing piece of executable code so that it is executed when its host code is run.

Viruses can be classified by their method of concealment. Some are called Stealth Viruses because of the way that they hide themselves, or Polymorphic because of the way they change themselves to avoid scanners.

The most common classification, however, relates to the sort of executable code which the virus attaches itself to. These are:

Types of viruses

Partition Viruses
Boot Sector Viruses
File Viruses
Overwriting Viruses
Macro Virus
Companion Viruses
Multipartite Viruses

There is also a set of programs that are **related to viruses** by virtue of their intentions, appearances, or users' likely reactions:
Droppers
Failed viruses
Packagers
Trojans
Jokes
Test files

Virus found Unknown virus

Stealth Viruses

If a stealth virus is in memory, any program attempting to read the file (or disk sector) containing the virus is fooled into believing that the virus is not there.

Memory-resident viruses will not normally function under Windows 95. However, they can be active in DOS sessions or if Windows 95 is running in real mode.

There are two ways to deal with this:

* Cold Boot from a clean DOS floppy, and make sure that nothing on the hard disk is executed. Run any anti-virus software from floppy diskette. Unfortunately, although this method is foolproof, relatively few people are willing to do it.

Search for known viruses in memory. All the programs in Dr Solomon's Anti-Virus do this when they are run.

About viruses

Polymorphic Viruses

A polymorphic virus is one that is encrypted, and the decryptor/loader for the rest of the virus is very variable. With a polymorphic virus, two instances of the virus have no sequence of bytes in common. This makes it more difficult for scanners to detect them.

Dr Solomon's Anti-Virus uses "Fuzzy Logic" techniques and the Generic Decryption Engine to detect these viruses.

About viruses

Partition Sector Viruses

The partition sector is the first sector on a hard disk. It contains information about the disk such as the number of sectors in each partition, where the bootable partition starts, plus a small program. The partition sector is also called the Master Boot Record (MBR).

Viruses can place all or part of their code in this location on a hard disk. The code in this location is the first to be executed when your computer starts up. Infecting this area allows a virus to install itself in memory before the operating system has loaded.

Since the partition sector is not part of the normal data storage area on the disk, utilities such as DEBUG will not allow access to it.

Floppy disks do not have a partition sector.

About viruses

Boot sector viruses

The boot sector is the first sector on a floppy diskette. On a hard disk it is the first sector of a partition It contains information about the disk or partition, such as the number of sectors, plus a small program.

When the computer starts it attempts to read the boot sector of a disk in drive A. If this fails because there is no disk in drive A it reads the boot sector of drive C. A boot sector virus replaces this sector with its own code and normally moves the original elsewhere on the disk.

Even a non-bootable floppy disk contains executable code in its boot sector. This displays the 'non-system' disk message when the computer attempts to boot from the disk. Therefore, a non-bootable floppy disk can still contain a virus and infect a computer if it is inserted in drive A when the computer starts.

About viruses

File viruses

File viruses append or insert themselves into executable files, typically .COM and .EXE programs, and macros.
A direct action file virus infects another executable file(s) on the disk when its 'host' executable file is run; but does not remain active in memory.

An indirect action (or TSR) file virus installs itself into memory when its 'host' is executed, and infects other files when they are subsequently accessed (most infect programs when they are run). This type of virus can also interfere, deliberately or accidentally, with the operation of other memory- resident programs. Some TSR viruses infect other programs when they are opened or copied as well as when they are run. These are known as 'fast infectors'.

On Windows 95 systems, a file virus can run whenever a DOS application is run. A handful of viruses have been written which are designed specifically to run under 32-bit operating systems like Windows 95.

Most file viruses try to go memory-resident when they run. This attempt to become memory-resident is likely to fail as memory is handled differently under Windows 95. This will severely hamper the ability of the virus to spread.

Note that under Windows 95, a virus may not have the same effect as it does under DOS. In particular, viruses will not be able to write to hard disk boot sectors and partition sectors from within the a DOS session.

About viruses

Overwriting viruses

Overwriting viruses overwrite all or part of the original program. As a result, the original program does not run. Overwriting viruses are not, therefore, a real problem - they are extremely obvious, and so cannot spread effectively. Overwriting viruses will run within a Windows 95 DOS session. Files infected by an overwriting virus cannot be disinfected.

About viruses

Macro viruses

Macro viruses are now common. They can be part of documents or spreadsheets created in applications which use macro languages. Any application which uses a sufficiently complex macro language could be a target for viruses; but to date we have only seen macro-viruses for Microsoft Word for Windows, Microsoft Excel for Windows and Lotus AmiPro for Windows.

Macro viruses generally function independently of the operating system. All the macro commands required for an infection, function on all platforms. A Macro virus created on an IBM compatible can infect a file on a Macintosh, or vice versa.

About viruses

Companion viruses

If you have a COM file and an EXE file of the same name, DOS always runs the COM file in preference to the EXE file, if no file extension is given. Companion viruses make use of this fact by creating COM files with the same name as the legitimate EXE files, thus, ensuring that they are executed. Then the viruses pass control to the original EXE file, which runs normally. Companion viruses will run in a Windows 95 DOS session and some may be effective under Windows 95.

A path companion virus creates an infected file with the same name as an executable file and places the infected file in a directory named earlier in the path. Therefore the infected file runs in preference to the original file.

About viruses

Multipartite viruses

Some viruses use a combination of techniques to spread and infect executable files, boot sectors and partition sectors. These will not generally be able to spread successfully under Windows 95.

About viruses

Droppers

Droppers are programs that have been written to perform some apparently useful job but, while doing so, write a virus out to the disk. In some cases, all that they do is install the virus (or viruses).

A typical example is a utility that formats a floppy diskette, complete with Stoned virus installed on the boot sector

Droppers that attempt to spread boot sector viruses will generally not work under Windows 95.

About viruses

Failed viruses

Sometimes a file is found that contains a 'failed virus'. This is the result of either a corrupted 'real' virus or simply a result of bad programming on the part of an aspiring virus writer. The virus does not work - it hangs when run, or fails to infect.

Many viruses have severe bugs that prevent their design goals - some will not reproduce successfully or will fail to perform their intended final actions (such as corrupt the hard disk).

Many virus authors are very poor programmers.

About viruses

Packagers

Packagers are programs that in some way wrap something around the original program. This could be as an anti-virus precaution, or for file compression. Packagers can mask the existence of a virus inside.

About viruses

Trojans and Jokes

A trojan is a program that deliberately does unpleasant things, as well as (or instead of) its declared function. They are not capable of spreading themselves and rely on users copying them.

A joke is a harmless program that does what its author thinks is amusing. We include the detection of a few jokes in Dr Solomon's Anti-Virus, where people have found particular jokes that give concern or offense.

About viruses

Test files

Test files, in the context of viruses, are used to test and demonstrate anti-virus software such as FindVirus. They are not viruses - simply small files that are recognized by the software and cause it to simulate what would happen if it had found a virus. This allows users to see what happens when it is triggered, without needing a live virus.

A test file for FindVirus can be made by creating a small text file, at least 50 characters long, which has the following sequence of characters at the very beginning:

ZQZXJVBVT

A FindVirus scan will report the file as a 'Test File', not a virus.

Note that the test file should have an executable extension (.COM or .EXE) for this to work correctly.

About viruses

If you find a virus

- Don't panic.
- Don't be in a hurry.
- Remove the virus using the Main Screen or the Disinfect Menu.
- If required call Dr Solomon's technical support.
- Review anti-virus policy to try and prevent a recurrence

Disinfect info Unknown virus Cannot disinfect

Deleting files that cannot be disinfected

The safest way to delete a file that cannot be disinfected is to use the 'Delete infected files' of Dr Solomon's Anti-Virus.

1. Start Dr Solomon's Anti-Virus.
2. Under the 'Scan' menu select 'Options'.
3. In the 'If file cannot be disinfected' section select 'Delete infected files'.
4. Click 'OK'.
5. Select Disinfect and then the relevant drive.
6. The infected file will be deleted and cannot be recovered.
7. To double check that your computer is now clean, click 'Scan' to re-check your computer.
8. If all is clear exit Dr Solomon's Anti-Virus.

Virus found

Help menu

Option	What does it do?	Click for more
Contents	will take you to the Contents of the main help menu	
Using Help	will explain how to move through a help file	More
Keyboard access	will explain how to use keyboard shortcuts instead of a mouse when using Dr Solomon's Anti-Virus.	More
About	will give you the current version of the Dr Solomon's Anti-Virus you are running. Dr Solomon's address and contact numbers are also given.	

Using Help

Some help topics will have a number of hotspots (cross-references) highlighted in green and underlined.

- To access a cross-referenced topic, select with a mouse click (the cursor changes to a hand when held over a) or use TAB (or Shift+TAB in reverse direction) to move to the highlighted text and then press ENTER.
- Use the scroll bar or up/down arrow keys to scroll through the text. PgUp and PgDn move through the text more rapidly.

Keyboard access

In Windows 95 shortcut keys are underlined. Most options can be selected by pressing shortcut key combinations.

Key	What does it do?
TAB	Move to next option or option group
Shift +TAB	Move to previous option or option group
Arrow keys	In an option group - move to next option in group Elsewhere - same as TAB, Shift + TAB
SPACE	Choose the active button or option
F1	Help
Alt or F10	Activate menu bar
Alt + Down arrow	Drop down a Combo Box
Alt + F4	Close program
Enter	Choose the active button
Esc	Cancel current dialog

Note:

Option groups are check boxes, radio buttons and anything with a scroll bar.

Detecting unknown viruses

Heuristic analysis is a technique used for scanning a file for suspicious code. However, it is very difficult to determine what code is suspicious. The code that might be innocent in one program (for example, FORMAT.COM) might be suspect in a virus infected file.

For this reason it is necessary for heuristic analyzers to calculate how suspicious a file appears. Typically, a scoring system is implemented, and any file which has enough suspicious elements (a high enough 'score') is flagged as being a possible virus. Suspicious elements could include: undocumented DOS functions, anti-debugging techniques to avoid disassembly, the existence of an executable file search mask (*.COM, *.EXE) etc.

Virus experts are typically seeing on average 200 to 250 new viruses every month. With the rising popularity of computers and the dramatically increased use of the Internet, new viruses are spreading faster and further than ever before.

There are two major problems with traditional heuristic analysis techniques.

- Firstly, unless great care is taken heuristic programs could give false alarms. A false alarm can be significantly more trouble and time-consuming than a genuine virus infection.
- Secondly, heuristics are unable to detect every existing virus.

Dr Solomon's Advanced Heuristic Analysis (AHA) answers the problems inherent in traditional heuristic analyzers. Through more detailed analysis of suspect files. AHA is able to virtually eliminate the possibility of false alarms. In tests, over gigabytes of software, it has succeeded in producing ZERO false alarms.

Traditional heuristic analyzers might confuse an innocent file for an infected file when scanning for suspicious code. Dr Solomon's Anti-Virus makes a more detailed analysis of suspect files. Polymorphic viruses, in particular, use techniques not used in most programs. Therefore, the more complicated the virus author makes a polymorphic virus, the more obvious it is to the analyzer.

Other scanners using traditional heuristic analysis have shown detection rates of only 60%, with a 1 in a 1,000 false alarm rate. (The computer on which this document has been written contains over 5,000 files). In laboratory tests AHA has been verified as detecting in excess of 80% of new and unknown viruses, with zero false alarms.

Unknown viruses

Disinfecting information

In the majority of cases Dr Solomon's Anti-Virus can reverse any damage, caused by a virus, to executable files. FindVirus removes the virus code from each infected file and restores the file to its original state. The virus code is then overwritten with zeroes to make sure that it is completely removed.

Where a virus has caused irreparable damage, FindVirus gives you the option to rename the file so that it cannot be run accidentally, or to delete the file. The file is overwritten with zeroes before it is deleted to make sure that it cannot be Undeleted.

Disinfect menu Cannot disinfect Virus found

What is FindVirus?

FindVirus is an extremely fast scanner and is, therefore, suitable for every day use. It looks for known viruses and provides comprehensive protection when working with up-to-date drivers. These are databases containing information on known viruses.

You must update regularly for FindVirus to be completely effective, you can only do this with the full version of the Toolkit.

A Test file can be prepared to simulate the effect of a virus on the programs.

Generic Decryption Engine

The dynamic nature of the virus world means that further advances must be made to cope with the latest viruses. The Generic Decryption Engine is one of the features which confirms Dr Solomon's position as the most technologically advanced anti-virus company in the world. Dr Solomon's were the first anti-virus company in the world to develop a generic decryption engine, first releasing it in September 1993.

The generic decryption engine followed the development of a series of virus engines, designed to produce polymorphic viruses. The Nuke Encryption Device (NED), for example, offers enormously high levels of polymorphism to the virus author. The engine is so polymorphic that using statistical analysis it resembles any fairly ordinary program. Statistical analysis is not enough to accurately detect (with no false alarms) viruses created with NED. Similarly, the Dark Angel's Multiple Encrypter (DAME) is impossible to detect reliably with conventional methods.

What was required was a method that would:

- detect polymorphic viruses, 100%;
- give zero false alarms;
- not slow down FindVirus

The research and development team at Dr Solomon's set out to write a program that could decrypt any encrypted program. The idea was to look at the code, work out the decryption algorithm from the code, and then decrypt the virus.

- 100% IDENTIFICATION:
  Once the code is decrypted, you have inside the encrypted part, a constant byte sequence which can be used for positive identification.
- FUTURE PROOF:
  If it is a truly general decryptor, it will work for MTE, TPE, NED, and other encryption methods.
- ZERO FALSE ALARMS:
  False alarms result because encrypted viruses are so variable. With a Generic Decryption Engine we are looking at something that is not variable, the decrypted bytes of the virus.
- PRECISE IDENTIFICATION:
  If we've decrypted the virus, we can then do an exact identification by checksumming it (in effect, taking a fingerprint).
- DISINFECT:
  Precise identification and complete decryption means disinfection of the virus is possible.
- SPEED:
  We have recorded speeds in excess of seven (7) megabytes/second. The Generic Decryption Engine will not slow down FindVirus in conventional operation. Of course, if a polymorphic virus is found during the scan there is a slight slowdown during the decryption process.

The Generic Decryption Engine produced in the Dr Solomon's virus laboratories does not need to know anything about how the NED works. The Generic Decryption Engine knows how to decrypt anything that is encrypted. Once decrypted a virus is relatively simple to identify by the constant sequence of bytes hidden by the encryption.

In its first test run the Generic Decryption Engine successfully decrypted, and detected almost every single file infected with the NED virus, Itshard. When run against a large collection of clean files it gave no false alarms.

In further tests we found that almost every encrypted virus in their collection could now be decrypted and removed. Furthermore, we found that our scanner could now perform exact repair (as the files were before infection) of viruses such as V2P6 which many other products cannot even detect reliably. Immensely Polymorphic viruses such as Bosnia, Trigger and Tremor can be detected with ease, and no false alarms.

Technical Support

	U.S.A and Canada
Telephone	617-273-7495
Fax	617-273-7474
e-mail	techhelp@us.drsolomon.com
Bulletin board	617-229-8804
Mailing Address	Technical Support Dr Solomon's Software, Inc. 1 New England Executive Park Burlington MA 01803 USA

Virus found

Unknown virus

File Allocation Table

The FAT is the area on the disk that contains the information about what part of the disk belongs to which file. If the FAT is zeroed or corrupted, then the hard disk is like the pages of a book, without any binding, in a random order, and no page numbers.

A number of viruses zero, overwrite, or (much worse) make small changes to the FAT.

About Dr Solomon's Anti-Virus

Programmers		Testers	Virus Group Team Leader
Graeme Bell	Duncan Lilly	Karobi Chaudhuri	Dr Paul Lawrence
Paul Carmichael	Andy Parr	Nigel Edwards	
Declan Eardly	Andy Ruddock	Adam Finch	**Virus Research Analysts**
Andy Glennister	Damian Wilson	Lee Jones	Dmitry Gryaznov
Robert Haynes	Kam Yeung	Adam Langford	Duncan Long
		Andrew Prevett	Peter Morley
		Mike Tucker	Dr Igor Muttik

Founder	Dr Alan Solomon		
Worldwide Product Marketing Director	Mike Hill	**R&D Director**	Bryn Taylor
Senior Vice President & General Manager, North America	Steve Orenberg	**Manager of Tech. Support**	John Althouse
Product Manager	Jolyon Jago	**Project Leader**	Joy Gregory
Director of Channel Sales	Kim Yandall	**Tech Writer**	Dafydd Ladd
Director of Marketing	Anne Beitel	**On-Line Systems Manager**	Paul J Evans
Director of Operations	Tom Lafleur		
Senior Technology Consultants	Graham Cluley Shane Coursen David Emm Glenn Jordan		

Disinfecting compressed files

Viruses within compressed and archived files cannot be disinfected without the file first being decompressed. To disinfect compressed files, decompress to a temporary directory and use the 'Disinfect' function to remove the virus.

Automatic Daily Scanning

There is a launch program - 'FVLAUNCH.EXE' - to implement daily virus scanning.

To activate FVLAUNCH, create a program item for it in the StartUp group (Windows 3.x), or create a short cut for it in the StartUp folder (Windows 95). To de-activate FVLAUNCH, remove its program item or short cut.

Each time you boot up the computer FVLAUNCH checks whether a virus scan has already been performed that day. If a scan has not been performed FVLAUNCH starts a scan, which checks the local drives.

Before the scan starts you may see the licence agreement prompt. If you do see this prompt you can check the 'Don't show again' box.

If you have previously checked the 'Don't show again' box the scan starts immediately.

You see an indication of the progress of the scan in the Task Bar. A report screen is displayed when the scan has completed.

Upgrade Order Form

To: _____ C/E056

_____

_____

_____

Name _____

Company _____

Department _____

Street _____

City, State, Zip/Country _____

Please complete the following:

Please send me the Dr Solomon's AntiVirus Toolkit
for (please check one operating system)

Windows 95 ___
Windows 3.x ___
Windows NT ___
Netware ___

1. Registration fee _____

   Please contact your local distributor
   for the current price

2. Shipping _____

3. Sales tax, if applicable _____

   TOTAL of 1, 2 and 3 _____

Please indicate payment method:

Check/M.O. ___ Credit card ___

Credit Card No _____ Expires _____

Signature _____ Date _____

Check here ____ if you require 5.25" media.

We accept corporate purchase orders--please call your local distributor for details.

In the USA, you can telephone your order to 800-310-9078 or fax this form to 617-238-0851.

Dr Solomon's Software can be contacted by e-mail

North America info@us.drsolomon.com
United Kingdom info@uk.drsolomon.com
Germany info@de.drsolomon.com

or on the World Wide Web http:/www.drsolomon.com/
or Compuserve Go Drsolomon

Distributors

Dr Solomon's Anit Virus is available from a number of sources. If your country does not appear on this list, or if you cannot contact your local distributor, please contact Dr Solomon's in the United Kingdom, in the USA or in Germany.

North America
Argentina
Australia
Austria
Bahrain
Baltic Republics
Bangladesh
Belgium
Belorussia
Bolivia
Brazil
Canada
Central America
Chile
China
Colombia
Cyprus
Czech Republic
Denmark
Egypt
Ecuador
Estonia
Ethiopia
Finland
France
Germany
Ghana
Greece
Guatamala
Honduras
Hong Kong
India
Indonesia
Iran
Ireland
Isreal
Italy
Ivory Coast
Japan
Kenya
Korea
Kuwait
Latvia
Luxembourg
Malaysia
Malta
Mexico
Nepal
Netherlands

New Zealand
Nicaragua
Nigeria
Norway
Oman
Peru
Poland
Portugal
Qatar
Russia
Saudi Arabia
Sierra Leone
Singapore
Slovakia
Soviet Block
Spain
Sri Lanka
Sweden
Switzerland
Taiwan
Thailand
Trinidad
Turkey
UAE
United Kingdom
USA
Venezuela
West Indies
Zimbabwe

Distribution in: United States of America

Dr Solomon's Software, Inc.
1 New England Executive Park
Burlington MA 01803
USA

Tel: +1 617 273-7495 (technical support)
      +1 617 273-7494 (customer service and sales)
Fax: +1 617 273-7474
BBS: +1 617 229-8804

Internet e-mail: techhelp@us.drsolomon.com (technical support)
                  custserv@us.drsolomon.com (customer service)

Back to Distributors

USA Head Office

Dr Solomon's Software, Inc.
1 New England Executive Park
Burlington MA 01803
USA

Tel: +1 617 273-7400
Fax: +1 617 273-7474
BBS: +1 617 229-8804

Internet e-mail: techhelp@us.drsolomon.com
CompuServe forum: GO DRSOLOMON

Back to Distributors

Distribution in: Argentina & Colombia

Economic Data S.L.
Ponzano, 39-5º I
28003 Madrid
Spain

Tel: +34 1 442 2800
Fax: +34 1 442 2294

Internet e-mail: edutaba@edata.es

Back to Distributors

Distribution in: Australia & New Zealand

Loadplan Australasia Pty Ltd
96-98 South Market Street
South Melbourne
Victoria 3205
Australia

Tel: +61 3 9690 0455
Fax: +61 3 9690 7349

Internet e-mail: loadplan@loadplan.com.au

Back to Distributors

Distribution in: Germany, Austria & Switzerland

Dr Solomon's Software GmbH
Luisenweg 40
20537 Hamburg
Germany

Tel: +49 40 25 19 54-0
Fax: +49 40 25 19 54-50

CompuServe: 75450,1326
Internet e-mail: support@de.drsolomon.com

Back to Distributors

Distribution in: Bahrain, Egypt, Kuwait, Oman, Qatar, Saudi Arabia & UAE

LBI International, Inc.
2 Torri Katur
Lourdes Lane
St Julians STJ 02
Malta GC

Tel: +356 344257
Fax: +356 340761

Back to Distributors

Distribution in: Belgium, Luxembourg & Netherlands

Data Alert International B V
Patrijsweg 80 E
2289 Ex Rijswijk
The Netherlands

Tel: +31 70 307 7111
Fax: +31 70 307 7886

Internet e-mail: 100627.2012@compuserve.com

Back to Distributors

Distribution in: Brazil

PC Software e Consultoria Ltda
R Voluntarios da Patria 45-13º
22270-000 Rio de Janeiro RJ
Brazil

Tel: +55 21 537 0405
Fax: +55 21 537 1411

Internet e-mail: pc.software@centroin.ax.apc.org

Back to Distributors

Distribution in: South East Asia

China, Hong Kong, Indonesia, Korea, Malaysia, Singapore, Taiwan & Thailand

Digitus Computer Systems
11 Dhoby Ghaut
#09-01 Cathay Building
Singapore 229233

Tel: +65 337 1945
Fax: +65 336 9672

Back to Distributors

Distribution in: Canada

Sensible Security Solutions
Golf Club Road
R.R. #1 Braeside
Ontario
KOA 1GO
Canada

Tel: +1 613-623-6966
Fax: +1 613-623-3992

Internet e-mail: secure-1@magi.com

Back to Distributors

Distribution in: Ecuaodor Chile, Guatamala, Honduras, Nicaragua,
Peru, Venezuela & Central America

Bysupport Computacion SA
Bernardo Vera y Pintado 2575
Providencia
Santiago
Chile

Tel: +56 2231 0300
+56 2231 0308
Fax: +56 2233 5917

Internet e-mail: bysup@reuna.cl

Back to Distributors

Distribution in: Cyprus & Greece

A E C Consultants Ltd
PO Box 906
1 G. Afxentiou Avenue
6023 Larnaca
Cyprus

Tel: +357 4 656108/650137/626422
Fax: +357 4 658972

Internet e-mail: aec@zenon.logos.hol.gr

Back to Distributors

Distribution in: Czech Republic

PCS Software spol. s.r.o.
Na Dvorcích 18
14000 Praha 4
Czech Republic

Tel: +42 2 42 3962
+42 2 42 1628
Fax: +42 2 42 0192

Back to Distributors

Distribution in: Denmark

Swanholm Distribution A/S
Transformervej 9 D
DK-2730 Herlev
Denmark

Tel: +45 44 92 9393
Fax: +45 44 92 7171

Internet e-mail: support@swanholm.dk

Back to Distributors

Distribution in: Estonia, Finland, Baltic Republics, Latvia,
Belorussia, Russia & Soviet Block.

LAN Vision Oy
Sinikalliontie 14
SF-02630 Espoo
Finland

Tel: +358 0 502 1947
Fax: +358 0 524 149

Back to Distributors

Distribution in: France

AB Soft
Parc Burospace 15
91572 Bièvres cedex
France

Tel: +33 1 69 33 70 00
Fax: +33 1 69 33 70 10

CompuServe: 72451,243
Internet e-mail: 72451.243@compuserve.com

Back to Distributors

Distribution in: Ghana, Nigeria, Ivory Coast and Sierra Leone

Software Marketing Consultancy
House No B26/28, New Achimota
PO Box 8592
Accra North
Ghana

Tel: +233 2755 7506
Fax: +233 2755 2718

Internet e-mail: ghemans@ug.gn.apc.org

Back to Distributors

Distribution in: India, Bangladesh, Nepal & Sri Lanka

IT Secure
52 Regency Chambers
Near Nandi Cinema
Bandra (West)
Bombay 400 050
India

Tel: +91 22 643 1233/1246
Fax: +91 22 642 2182
Internet e-mail: peter.quantum@axcess.net.in

N&N Systems and Software
105 Om Chambers
123 August Kranti Marg
Bombay 400 036
India

Tel: +91 22 368 0512/0517/0518
Fax: +91 22 368 0513
Internet e-mail: neville.bulsara@lwbom.nandanet.com

Back to Distributors

Distribution in: Iran

Shabakeh Gostar Corporation
Building Number 10
Palizi Square
North Sohrevardi Avenue
Tehran 15568
Iran

Tel: +98 21 876 7615
Fax: +98 21 876 7615

Back to Distributors

Distribution in: Ireland

Priority Data Systems Ltd
Priority House
63 Patrick St
Dun Laoghaire
Co Dublin
Ireland

Tel: +353 1 284 5600
Fax: +353 1 280 0311

CompuServe: 100143, 575
Internet e-mail: priority@iol.ie

Back to Distributors

Distribution in: Italy

Siosistemi srl
Via Cefalonia 58
25124 Brescia
Italy

Tel: +39 30 244 11
Fax: +39 30 222 249

Back to Distributors

Distribution in: Japan

Jade Corporation Ltd
3-6-11 Tokiwa-Cho
Shizuoka City
Shizuoka 420
Japan

Tel: +81 54 252 0085
Fax: +81 54 221 0282

CompuServe: 100225,3467
Internet e-mail: 100225.3467@compuserve.com

Back to Distributors

Distribution in: Kenya

Memory Masters
PO Box 70158
Nairobi
Kenya

Tel: +254 2 751916/743934
Fax: +254 2 751916

Internet e-mail: memorymasters@africaonline.co.ke

Back to Distributors

Distribution in: Malta

Panta Computer Co. Ltd
Panta House
Birkirkara Road
Msida MSD 03
Malta

Tel: +356 492 741
Fax: +356 492 744

Back to Distributors

Distribution in: Mexico

Grupo ASISA de Mexico, S.A. de C.V.
Darwin No. 32, Piso 6.
Col. Anzures.
Del. Miguel Hidalgo.
C.P. 11590 Mexico

Tel. +52 5 254-39-48
or +52 5 254-39-58

Internet e-mail: ventas@drsolomon.com.mx
World Wide Web: http://www.drsolomon.com.mx

Back to Distributors

Distribution in: Norway

Swanholm Distribution A/S
Wdm Thranesgt 77 (0715)
PO Box 9858, 1LA
0132 Oslo
Norway

Tel: +47 2 11 6828
Fax: +47 2 11 6363

Internet e-mail: swanholm@swanholm.no
World-Wide Web: http://www.swanholm.no/

Back to Distributors

Distribution in: Poland

Dagma sp. z o.o
UL Gen Jankego 15
40-615 Katowice
Poland

Tel: +48 32 102 11 22
Fax: +48 32 102 11 22

Internet e-mail: daggps@silter.silesia.ternet.pl

Back to Distributors

Distribution in: Portugal

RSVP Consultores Associados Lda
Rua Conde de Avranches, 659 - 2 Esq
4200 Porto
Portugal

Tel: +351 2830 0741
Fax: +351 2830 0740

Internet e-mail: rsvp.pt@tpone.telepac.pt

Back to Distributors

Distribution in: Slovakia

Lynx s.r.o.
Stefanikova 50a
Kosice
Slovakia
040 01

Tel: +42 95 62 27309
+42 95 62 27319
Fax: +42 95 62 26562

Back to Distributors

Distribution in: Spain

Economic Data S.L.
Ponzano, 39-5º I
28003 Madrid
Spain

Tel: +34 1 442 2800
Fax: +34 1 442 2294

Internet e-mail: edutaba@edata.es

Back to Distributors

Distribution in: Sweden

QA Information Security AB
Box 596
S-175 26 Järfälla
Sweden

Tel: +46 (0)8-580 100 02
Fax: +46 (0)8-580 100 05

Internet e-mail: support@qainfo.se

Back to Distributors

Distribution in: Turkey

Logosoft Yazilim San Tic Ltd
Albay Faik Sozener Cad.
Benson Is Merkezi
21/3 Kadikoy
81300 Istanbul
Turkey

Tel: +90 216 348 1399
+90 216 348 7309
Fax: +90 216 348 1754

Back to Distributors

Distribution in: United Kingdom

Dr Solomon's Software PLC
Alton House Business Park
Gatehouse Way
Aylesbury
Bucks HP19 3XU
England

Tel: +44 (0)1296 318700
Fax: +44 (0)1296 318777

Support tel: +44 (0)1296 318733
Support fax: +44 (0)1296 318734
Bulletin board: +44 (0)1296 318810

CompuServe forum: GO DRSOLOMON
Internet e-mail: support@uk.drsolomon.com
World-Wide Web: http://www.drsolomon.com/

Back to Distributors

Distribution in: Trinidad & West Indies

Global Traders Inc Ltd
First Floor Moller's Plaza
#18 Eastern Main Road
Tunapuna
Trinidad
West Indies

Tel: +1 809 662 6256
Fax: +1 809 662 6256

Back to Distributors

Distribution in: Zimbabwe

RyVal Computers (Private) Limited
PO Box AY 249
AMBY
Harare
Zimbabwe

Tel: +263 4 487 235
+263 4 487 239
Fax: +263 4 486 381
Internet e-mail: ryval@harare.iafrica.com

Ridgehill Investments
15 Lomagundi Road
Avondale
Harare
Zimbabwe

Tel: +263 4 304 822
Fax: +263 4 304 822

Back to Distributors