



Anti-Virus Toolkit Reference Guide

[What is a Virus?](#)

[Identifying the Threat](#)

[Minimising the risk of virus infection using Dr Solomon's](#)

[Dr Solomon's Anti-Virus Toolkit, Overview](#)

[What's in each version of Dr Solomon's Anti-Virus Toolkit](#)

[Network Protection](#)

[Scanning E-mail](#)

WHAT IS A VIRUS?

A virus is a piece of self-replicating code; in other words, it is software which is designed to copy itself.

Boot sector viruses infect the boot sector of floppy disks and the **partition sector** [or, in some cases, the boot sector] of hard disks, when the PC is booted from an infected floppy disk. **Executable file viruses** infect program files, on local drives or network drives. **Macro viruses** infect the macros within document and spreadsheet files.

In addition to the code necessary for the virus to copy itself, most successful **'in the wild'** viruses try to conceal themselves, from users and from anti-virus programs [if a virus quickly draws attention to itself, it is unlikely to spread very far]. Some viruses contain a **payload**; this may be anything from a screen display, or message, or damage to **data files**. However, not all viruses contain a payload. If the virus does contain a payload, there must be a trigger which causes the virus to deliver its payload. The **trigger** may be a particular system date, the number of re-boots, the number of floppy disks infected or something else which software can be designed to do.

It is worth noting that virus authors, unlike commercial software vendors, do not have to make their software compatible with other programs; they do not have to beta test their software or provide technical support on their products; for this reason, viruses may produce unintended consequences [they may make the system unstable, or prevent other software from working properly].

IDENTIFYING THE THREAT

Before implementing an anti-virus strategy, it is essential to identify the sources of any possible virus infection. The following provides an overview of the ways in which organisations can become infected by a virus.

1. Floppy disks and CDs brought into an organisation [including shrink-wrapped software from original manufactures, disks from other organisations [suppliers, marketing agencies, etc.]] bring with them the risk of virus infection. The movement of floppy disks and CDs between different sites within an organisation may also help to spread a virus. Boot sector viruses [which spread via floppy disks] are still common; and viruses have been found on CDs.
2. Desktop PCs used at home, and laptop PCs, are a potential source of virus infection. The use of laptop PCs, in particular, has become commonplace in the last few years. Floppy disks and CDs used in these PCs may not have been checked for viruses. And the employee may not be the only person using the PC. It is important to recognise that these PCs, which are not under the direct control of an organisation's IT Department, may be more exposed to virus infection than those which are under the direct control of the organisation.
3. The use of **e-mail** within corporate organisations provides an effective way for viruses to spread. It is not possible to become infected by a virus simply by reading a **text message** [in spite of the many virus hoaxes ['Good Times', 'Irina', 'Penpal Greetings', etc.] which supposedly spread via text messages]]. However, **e-mail attachments** are a potential threat. If a document or spreadsheet is infected, it can become widespread very quickly by being attached to an e-mail message. This is true even of an internal e-mail system, with no connection to the outside world. If users are able to send and receive e-mail to and from outside organisations, the threat becomes even greater.
4. Use of the **Internet** is a further potential source of infection. If any users within an organisation have access to the Internet [this includes access to **CompuServe**, **America Online**, the **World Wide Web**, etc.] they are able to download a vast range of material [including programs and documents] . . . all potentially infected.

MINIMISING THE RISK OF VIRUS INFECTION USING DR SOLOMON'S

So, what can be done to prevent a virus infection? Having identified the potential sources of infection within an organisation, it is essential to use effective anti-virus tools to ensure that (1) the risk of a virus entering the organisation is minimised; (2) if a virus does enter the organisation it is detected as soon as possible; (3) it can be removed easily. Dr Solomon's provides a range of tools designed to detect and remove viruses; and to prevent infection.

However, it is not possible simply to build a single defensive dyke around the organisation, in the hope that no virus will be able to breach the 'perimeter defences'. Often there is no 'perimeter', as such. The potential sources of infection [as outlined above] exist at different levels within the organisation. What is needed, therefore, is an anti-virus strategy which includes anti-virus protection at different levels within the organisation [a layered approach, so that a virus which is not detected at one level will be detected at another level]. Dr Solomon's offers anti-virus tools which are appropriate for different layers within an organisation [these anti-virus tools are outlined in later sections within the Reference Notes].

There is no universal model for deploying anti-virus tools; what is right for one organisation may not be right for another. However, the information below identifies the 'layers' of protection which are appropriate for most organisations. In addition, a few examples are given of how organisations of different sizes might use Dr Solomon's.

1. If a '**sheep-dip**' [or '**footbath**'] PC is used to check incoming floppy disks and CDs, this will provide early detection of a virus, before the infected floppy disk or CD is used within the organisation's main system. The 'sheep-dip' PC should be stand-alone [to avoid the risk of a virus infecting the network]. In a large organisation, it may be advisable to use several 'sheep-dip' PCs [one per building, one per department, etc.].
2. PCs [stand-alone or workstations] should be protected with an **on-access scanner** [VirusGuard and/or WinGuard], to provide the first layer of protection 'in-depth' [rather than at the perimeter]. The on-access scanner will scan disks and files before they are used. The on-access scanner runs in the background [requiring no action on the part of the user]. The user will be given a pop-up warning, to identify the virus; and the user will not be able to use the infected disk or file. VirusGuard and WinGuard provide protection for floppy disks, local hard disks and network drives. They are fully-configurable, to enable greater or lesser security [for example, checking files which are written to disk may be selected for those PCs which are downloading software, documents, etc. from a remote location [the Internet, **BBS**, etc.]]. WinGuard may be configured to auto-disinfect, so that disks and files may be cleaned automatically, on detection. This makes anti-virus management easier [virus removal is carried out automatically, rather than by a member of the IT Department]. WinGuard may be configured to log all virus incidents, allowing the IT Department to monitor all virus incidents.
3. Network servers should be effectively protected [programs and documents may be located on shared network drives; if they become infected, a virus will be able to spread via the network]. At the very least, network drives should be scanned regularly [see **Example 2** below]. However, Dr Solomon's offers server-based protection for Novell NetWare and Microsoft Windows NT servers; that is, anti-virus programs are designed to run directly from the server [see **Example 3** below; and the section **NETWORK PROTECTION**]. This adds a second layer of protection 'in-depth'. It also makes it easier to manage anti-virus protection, since scanning of network drives [and other functions, such as distribution and configuration of anti-virus programs, logging of virus incidents, virus alerts, etc.] can be automated.
4. The increased use of e-mail systems [and the threat from e-mail attachments [mainly infected Word for Windows documents]] means that a virus can spread very quickly throughout an organisation. If an organisation has an e-mail connection to the Internet, this threat increases dramatically. Although WinGuard will prevent access to infected e-mail attachments, this still leaves the logistical problem of removing the infected e-mail attachment from the mail-server [and the possibility of an unprotected workstation becoming infected]. This risk can be minimised by scanning e-mail as it enters [or leaves] the organisation. Dr Solomon's MailGuard is able to scan SMTP mail; Dr Solomon's Anti-Virus for Lotus Domino is able to scan Lotus Notes e-mail and databases. If e-mail is filtered in this way, it reduces the risk of a virus reaching any of the workstations. This adds an additional layer of protection, at the perimeter. However, it does not eliminate the need for VirusGuard and WinGuard on the workstations; remember that e-mail is not the only method by which viruses can enter an organisation.

Example 1 [single-user, home PC]

The home user is at threat from viruses from two sources. The first is floppy disks and CDs used to install software or to exchange data with others. The second is programs and documents downloaded from the Internet [this includes the World Wide Web, on-line services like CompuServe and America Online and any BBS accessed]. The home user should install Dr Solomon's Anti-Virus Toolkit for the operating system he or she uses. FindVirus should be used to scan incoming floppy disks and CDs [including **heuristic analysis** and checking of **compressed files**]; FindVirus should also be used to check files downloaded from the Internet. WinGuard should be loaded to provide background protection; it will check disks and files accessed in the PC. This will include files downloaded from the Internet, if the 'Scan on writes' option is selected. The 'Scan all OLE' option enables checking of OLE objects [including documents with extensions other than DOC and DOT]. The 'Auto-Disinfect' option enables automatic cleaning of infected disks and files.

Example 2 [small organisation]

The small [or medium-sized] organisation faces the same threat as the single-user. However, the threat is greater, for several reasons. (1) The threat is multiplied by the number of PCs involved. (2) The organisation is likely to have one, or more, networks; if one user becomes infected, the virus can spread across the network. (3) The organisation may have an e-mail system and may be connected to the Internet [or individual users may have a direct link to the Internet]; infected programs and documents may be downloaded and can spread throughout the organisation. FindVirus should be used to check all incoming floppy disks and CDs [preferably on a stand-alone 'sheep-dip' PC]. WinGuard should be installed on all PCs within the organisation, to check all disks and files used [the 'Scan on writes' option should be enabled for any user able to download files from the Internet; the 'Scan all OLE' option should be enabled if the organisation receives documents with extensions other than DOC and DOT; if the 'Auto-Disinfect' option is used, the 'Log' option should be enabled, so that all virus incidents are logged]. If the organisation uses NetWare or Windows NT, the server should be protected by installing Dr Solomon's Anti-Virus Toolkit for NetWare or Dr Solomon's Anti-Virus Toolkit for Windows NT. If this is not possible, the network supervisor, system administrator [or manager] should install Dr Solomon's Anti-Virus Toolkit for the operating system he or she uses; and set up a regular scheduled scan of network drives.

Example 3 [large organisation]

The large organisation faces the same threat as the small, or medium-sized, business; but the threat is greater because of the increased size of the organisation. (1) The organisation has many more users, PCs, networks, etc.. (2) The organisation may be divided into several [or many] geographical locations. (3) There is a much greater logistical problem involved in installing, distributing and updating anti-virus programs; in responding to virus incidents; in making sure that users are aware of the threat posed by viruses; and in ensuring that nothing 'slips through the net'. Each site, building or department should be equipped with a 'sheep-dip' PC, so that all incoming floppy disks and CDs are scanned with FindVirus. WinGuard should be installed on all PCs within the organisation, to check all disks and files used [the 'Scan on writes' option should be enabled for any user able to download files from the Internet; the 'Scan all OLE' option should be enabled if the organisation receives documents with extensions other than DOC and DOT; if the 'Auto-Disinfect' option is used, the 'Log' option should be enabled, so that all virus incidents are logged]. If the organisation uses NetWare or Windows NT, the servers should be protected by installing Dr Solomon's Anti-Virus Toolkit for NetWare or Dr Solomon's Anti-Virus Toolkit for Windows NT. If the organisation has an SMTP gateway for sending and receiving Internet e-mail, MailGuard should be installed to filter incoming and outgoing mail [see the section **SCANNING E-MAIL**]. If the organisation uses Lotus Notes, e-mail and databases should be checked using Dr Solomon's Anti-Virus for Lotus Domino [see the section **SCANNING E-MAIL**]. If the organisation's PCs are networked using Windows NT, Dr Solomon's Anti-Virus Toolkit for Windows NT Server [Management Edition] should be used to make anti-virus management easier [see the section **NETWORK PROTECTION**].

[Top of the page](#)

DR SOLOMON'S ANTI-VIRUS TOOLKIT, OVERVIEW

Dr Solomon's Anti-Virus Toolkit is a collection of programs designed to detect and remove viruses. It also contains a range of utilities designed to enable PC Support professionals to maintain and upgrade DSAV programs easily across networks. The different versions of DSAV [DOS, Windows 3.x, Windows 95, Windows NT, NetWare, OS/2, SCO UNIX and Macintosh] are designed to provide these functions for each specific operating system. In particular, each version of DSAV uses the same **virus database** [apart from the Macintosh version . . . there are Macintosh-specific viruses; and PC viruses [boot sector viruses and executable file viruses] do NOT infect the Macintosh]; for this reason, each version of DSAV will detect the same viruses, whether they are DOS, Windows, OS/2, etc.

Below is a list of the main DSAV programs. [NOTE: not every version of DSAV contains all of these programs; a list of programs for each specific operating system may be found in the section **WHAT'S IN EACH VERSION OF DR SOLOMON'S ANTI-VIRUS TOOLKIT**].

MAGIC BULLET Magic Bullet [supplied with every version of DSAV] is a clean boot disk, containing FindVirus. Magic Bullet is different to a standard DOS system disk . . . it does not contain the MS-DOS operating system files, or provide the user with an A:\> prompt. When a PC is booted with Magic Bullet, the user is provided with a simple user-interface, enabling them to detect and remove viruses. Magic Bullet scans and cleans files on any disks formatted under the FAT [File Allocation Table] system. This includes MS-DOS and Windows 95, including Windows 95 B [which uses a 32-bit FAT system]. Magic Bullet is unable to scan files in a non-FAT partition [for example, Windows NT's NTFS file system]; but it will scan the partition sector on a disk formatted under NTFS.]

USER-INTERFACE Each version of DSAV includes a user-interface, or menu, from which the other DSAV programs may be launched. The user-interface is used mainly by end-users, or anti-virus reviewers. Most corporate customers license individual DSAV programs [VirusGuard, WinGuard and FindVirus]

FINDVIRUS FindVirus is an **on-demand scanner** [it scans a disk only when the user chooses to run it, or may be scheduled to run at pre-defined times]. FindVirus is able to identify and remove viruses from partition sectors, boot sectors, executable files, documents and spreadsheets. FindVirus includes the Generic Decryption Engine [GDE], for detection and removal of **polymorphic** viruses. FindVirus may be configured to use Advanced Heuristic Analysis [AHA] to scan executable files for virus-like code, providing detection of unknown

viruses [from version 7.74, FindVirus will be able to scan documents and spreadsheets for unknown macro viruses]. FindVirus is able to check within compressed files.

VIRUSGUARD VirusGuard is an on-access scanner [it runs in the background and scans disks and files automatically when they are used]. VirusGuard is a **TSR** program, providing background protection in DOS. VirusGuard does not have the same detection capability as FindVirus and WinGuard: (1) it does not detect macro viruses [the user must be in Windows in order to access an infected document or spreadsheet]; (2) it detects programs infected with polymorphic viruses only after the virus has loaded into memory, not before the program is executed.

WINGUARD WinGuard is an on-access scanner [it runs in the background and scans disks and files automatically when they are used]. There are different versions of WinGuard for Windows 3.x [VxD], Windows 95 [VxD] and Windows NT [**kernel mode device driver**]. WinGuard has the same detection capability as FindVirus [from version 7.74, WinGuard will be able to scan documents and spreadsheets for unknown macro viruses].

VIVERIFY ViVerify is a **checksummer**, which checks for changes in partition sectors, boot sectors and executable files. It does this by creating 'fingerprints' for files on a clean hard disk and checking subsequently to see if these fingerprints change.

SCHEDULER The Scheduler allows users to run DSAV programs automatically at specified times. **VIRUS ENCYCLOPEDIA** This provides basic information on the viruses detected by each version of DSAV. This supplements the more detailed information in the printed Virus Encyclopedia [which is printed twice-yearly]. [The on-line Virus Encyclopedia is being re-designed, to include all the information provided in the printed version.]

TKUTIL TKUTIL contains a wide range of utilities designed to enable IT professionals to update and support DSAV programs within a corporate environment [updating WinGuard and FindVirus across a network, configuring PCs to run WinGuard and FindVirus, etc.]

[DSAV also includes a range of additional anti-virus utilities, designed to be used by advanced users, or by members of Technical Support. These includes Inspect Disk, which allows disks to be examined at low-level.]

[Top of the page](#)

WHAT'S IN EACH VERSION OF DR SOLOMON'S ANTI-VIRUS TOOLKIT

This section is designed to provide a quick check of the main programs included in each version of Dr Solomon's Anti-Virus Toolkit.

Dr Solomon's Anti-Virus Toolkit for DOS

Designed to run under DOS, programs may be run directly from the DOS **command line** or through the user-interface. The main programs in the DOS version of DSAV are:

- FindVirus
- VirusGuard
- ViVerify
- Scheduler
- Virus Encyclopedia
- TKUtil
- Magic Bullet

The DOS version of DSAV is also supplied with the program VGPOPUP, which provides a Windows **dialog** when VirusGuard produces a virus alert under Windows [NOTE: VGPOPUP simply provides a Windows dialog for VirusGuard; it does not check files itself and should not be confused with WinGuard].

The DOS version of DSAV may be used to check any DOS-accessible drive: this means that any network [for example Banyan Vines or DEC Pathworks] which can be accessed from a workstation, using DOS drive letter(s), may be checked for viruses.

Dr Solomon's Anti-Virus Toolkit for Windows 3.x

Designed to run under Windows 3.x, the programs are run by selecting the appropriate icon with the mouse. DSAV for Windows is also supplied with the DOS version, allowing programs to be run under DOS as well as Windows; and providing users with the advanced DOS utilities. The main programs in the Windows version of DSAV are:

- FindVirus
- VirusGuard
- WinGuard
- ViVerify
- Scheduler
- Virus Encyclopedia

TKUtil
Magic Bullet

VirusGuard is necessary to provide on-access scanning under DOS [WinGuard is able to provide protection ONLY when Windows is running].

Dr Solomon's Anti-Virus Toolkit for Windows 95

Designed to run under Windows 95, the programs are run by selecting the appropriate icon with the mouse. The Windows 95 version of DSAV is also supplied with the DOS version, to provide users with the advanced DOS utilities. The main programs in the Windows 95 version of DSAV are:

FindVirus
VirusGuard
WinGuard
ViVerify
Scheduler
Virus Encyclopedia
TKUtil
Magic Bullet

VirusGuard is necessary to provide protection under DOS [WinGuard is able to provide protection ONLY when Windows 95 is running].
[NOTE: although the Windows 95 and Windows 3.x versions of DSAV include the same programs, the Windows 3.x version will NOT run under Windows 95, since the two operating systems are significantly different.]

Dr Solomon's Anti-Virus Toolkit for Windows NT

Designed to run under Windows NT, programs are run by selecting the appropriate icon with the mouse. The Windows NT version of DSAV is also supplied with the DOS version, to provide users with the advanced DOS utilities. The main programs in the Windows NT version of DSAV are:

FindVirus
WinGuard
ViVerify
Scheduler
Virus Encyclopedia
TKUtil
Magic Bullet

The Windows NT version of DSAV will provide full protection for Windows NT workstations AND servers [the Windows NT Server & Management Edition provides easy management of Windows networks, rather than additional protection for the server].

Dr Solomon's Anti-Virus Toolkit for OS/2

Designed to run under OS/2, the programs are run by selecting the appropriate icon with the mouse. The OS/2 version of DSAV is also supplied with the DOS version, to provide users with the advanced DOS utilities. The main programs in the OS/2 version of DSAV are:

FindVirus
ViVerify
Virus Encyclopedia
TKUtil
Magic Bullet

Dr Solomon's Anti-Virus Toolkit for Macintosh

Designed to run on any Macintosh System 7 [or later], including Power Macintosh. Programs are run by selecting the appropriate icon with the mouse. The Macintosh version detects Macintosh viruses, macro viruses and PC boot sector viruses [PC boot sector viruses will not infect the Macintosh; however, it is possible for PC floppy disks to be accessed in a Power Macintosh]. Dr Solomon's Anti-Virus Toolkit for Macintosh includes the following programs:

FindVirus
Scheduler
MacGuard

Dr Solomon's Anti-Virus Toolkit for SCO UNIX

Designed to run under SCO UNIX, programs are run from the command line. The main programs in the SCO UNIX version of DSAV are:

FindVirus
Scheduler
Magic Bullet

The SCO UNIX version of DSAV is also supplied with the DOS version, to provide users with the advanced DOS utilities.

[For information on versions of Dr Solomon's designed to run on a network server, see the section **NETWORK PROTECTION**.]

[Top of the page](#)

NETWORK PROTECTION

It is possible to scan any DOS-compatible network drives from one of the workstations. If network drives can be seen from a workstation running DOS, Windows 95, Windows NT, etc., they can be scanned using the version of Dr Solomon's installed on the workstation. This should be done by a supervisor or system administrator, since they will have access to all network drives; and it should be a scheduled scan [to automate the scanning process]. This method should be used for scanning networks for which there is no specific server version of Dr Solomon's [for example, Banyan Vines, DEC Pathworks, LAN Server and LAN Manager].

However, versions of Dr Solomon's Anti-Virus Toolkit are available for Novell NetWare and Microsoft Windows NT. These are designed to run on the server itself. There are a number of advantages in running anti-virus programs directly from the server. In essence, server-based scanning provides centralised management. (1) The process is fully-automated. Scheduled scans of network drives can be set up, at specified times; this process requires no action from the supervisor or system administrator. An on-access scanner can be used to scan files before they are used, or before new files are written to the network. (2) All virus alerts [whether at the server or at one of the workstations] can be logged centrally; this allows the supervisor to track virus incidents. (3) If there is a virus alert, a message can be sent automatically to the supervisor. (4) Unprotected workstations can be denied access to the network.

The following is a list of the main programs in the server-based versions of Dr Solomon's Anti-Virus Toolkit.

Dr Solomon's Anti-Virus Toolkit for NetWare

FindVirus
File Access Monitor ['NetGuard']
Scheduler
Magic Bullet

The NetWare version of DSAV is also supplied with the DOS version, to provide users with the advanced DOS utilities.

Dr Solomon's Anti-Virus Toolkit for Windows NT

FindVirus
WinGuard
ViVerify
Scheduler
Virus Encyclopedia
Magic Bullet

The Windows NT version of DSAV is also supplied with the DOS version, to provide users with the advanced DOS utilities. The Windows NT version of DSAV will provide full protection for Windows NT workstations AND servers [the Windows NT Server & Management Edition provides easy management of Windows networks, rather than additional protection for the server].

Dr Solomon's Anti-Virus Toolkit for Windows NT Server [Management Edition]

Management Edition is designed to help system administrators manage anti-virus protection across Windows NT networks. (1) Management Edition provides centralised control, so that the entire network can be managed from a single location. (2) Management Edition allows simplified distribution of anti-virus programs [VirusGuard, WinGuard and FindVirus] to workstations running Windows NT, Windows 95 and Windows for Workgroups 3.11. The installation, configuration and updating of Dr Solomon's programs, on all PCs within the network, can be managed from a single location, using hierarchical domain management [on a Windows NT network, a domain is a group of PCs sharing the same security model; Management Edition allows the system administrator to manage anti-virus domains . . . a group of PCs sharing the same anti-virus policy]. (3) Management Edition's sophisticated alerting methods enable system administrators to keep track of all virus alerts across the network.

Management Edition is made up of a series of components, which are installed and configured via the Management Console [Management Edition's user-interface]. The Management Console is used to distribute anti-virus programs [and Management Edition components] to

PCs within the specified anti-virus domain(s). Management Console also keeps track of which versions of Dr Solomon's are being used within the network.

There are five essential components within Management Edition.

1. Scheduler enables anti-virus tasks [a FindVirus scan, for example] to be scheduled take place at specified times and locations [on a single workstation, a group of workstations or throughout the entire anti-virus domain].
2. Management Agent, which is resident on all workstations, receives instructions from the Scheduler [run FindVirus, for example] and carries them out. The Management Agent also looks out for alerts; if FindVirus or WinGuard detect a virus, Management Agent finds out the outcome.
3. Response Manager intercepts the results generated by tasks and alerts from the Management Agents. It has a user-configurable table to determine which alerting method to use. The system administrator is able to customise notification methods according to user, machine or workgroup; the possible notification methods are network broadcast, e-mail, pager, etc.
4. Messaging Agent carries out the alert notification, as instructed by the Response Manager.
5. Update Manager provides an easy way to distribute updated anti-virus programs to workstations in the domain. Enhanced management features include the ability to retry updates; and prevent the server from running out of connections or being flooded with file-copy requests when attempting to update a large number of PCs. If VirusGuard, WinGuard or FindVirus detect a virus, Response Manager alerts the administrator via network broadcast, e-mail, pager, logging, SNMP alerts, or printed trouble-tickets, ensuring that the system administrator is always informed about any virus incident within the domain [for e-mail alerts, Management Edition supports Lotus cc:Mail, Microsoft Exchange or any e-mail system accessible via an SMTP gateway.

Management Edition uses a Message Layer Interface [MLI] for internal communication between its components. The messaging and alerting is secured and authenticated. It runs transparently over IPX, TCP/IP and NETBIOS based networks; and interfaces directly with existing network management products such as OpenView, ManageWise and LanDesk by generating SNMP traps.

[Top of the page](#)

SCANNING E-MAIL

If WinGuard is installed on each PC within an organisation, users will be prevented from accessing infected documents and spreadsheets . . . from any source [including e-mail].

However, WinGuard is unable to clean infected mail attachments. Mail is likely to be stored on a mail-server, in a database format specific to each mail system [the formats used by Lotus cc:Mail, Lotus Notes, Microsoft Mail, Microsoft Exchange, etc. to store mail are all different]. This means that mail attachments can not be scanned using standard anti-virus tools; it is necessary to use a scanner which understands the specific format in which the mail is stored. In addition, it makes sense for larger organisations [with many users, many PCs, many sites, etc.] to scan mail attachments before they become items in a user's In-box. Dr Solomon's has a range of products designed to scan mail entering an organisation, providing an additional layer of anti-virus protection for large organisations.

Dr Solomon's MailGuard

There are a variety of different client mail systems available [Lotus cc:Mail, Lotus Notes, MS-mail, etc.]. **SMTP** [Simple Mail Transfer Protocol] is a standard protocol allowing mail to be delivered from one client mail system to another, across the Internet. Mail from a client mail system [including any attachments] must first be converted into **ASCII**; and it is **UUEncode** and **MIME** which provides the conversion of client mail into a format which can be delivered using SMTP. The SMTP gateway [which provides an interface with the Internet] handles the sending and receiving of all SMTP mail.

When data is sent via SMTP, it is converted into a format which can not be checked using normal anti-virus programs. And mail stored in a Post Office, within an organisation, is normally encrypted and / or compressed; again, making it impossible to scan the mail using standard anti-virus programs.

MailGuard is designed to allow the checking of all SMTP mail sent and received by an organisation. The PC running MailGuard [which must be running Windows NT] is 'plugged into' the link between the SMTP gateway and the client mail system's Post Office. In this way, all incoming and outgoing mail passes through MailGuard. MailGuard breaks the mail [including attachments] into its constituent parts, stripping away the encryption [UUEncode and MIME].

The files are then passed to FindVirus, which checks the files for viruses. If the files are clean, MailGuard re-assembles the mail message and forwards it to the Post Office. Infected files are quarantined, allowing the system administrator to deal with any infection [the system administrator is notified of the infected files; and the sender and receiver can also be sent an appropriate message].

Dr Solomon's Anti-Virus for Lotus Domino

Lotus Domino is a server-based application which allows client PCs running Lotus Notes to exchange mail, to access shared databases [stored on the server] and which provides a connection to other Lotus Domino servers.

Notes mail, like any other mail system, can be used to send files [including programs and documents] to any number of recipients. If any of these files are infected, the virus can spread rapidly.

Lotus Domino is designed to allow 'replication' of files and databases on other Lotus Domino servers. This provides a very effective mechanism for viruses to spread [copies of any infected files are sent automatically to every server within the system]. In addition, Lotus Domino is an ideal 'hiding-place' for viruses, since the files are stored in a database format which can not be scanned using standard anti-virus programs.

Dr Solomon's Anti-Virus for Lotus Domino provides the ability to scan Notes mail and Notes databases. DSAV for Lotus Domino scans every mail item as it is sent; and scans databases [since a Notes Post Office is a Notes database, it is possible to scan and clean the Post Office, to ensure that the entire domain is clean]. (1) Notes mail and databases are opened. (2) The attachments are removed and passed to FindVirus, for scanning. (3) Infected files are cleaned, or isolated. (4) Cleaned attachments are replaced in the mail or database.

Using DSAV for Lotus Domino, infected files can be cleaned or quarantined [so that they can be dealt with by the system administrator]. The system administrator [and users] can be informed using a comprehensive messaging system.

Messages [which are configurable by the system administrator] can be sent to (1) system administrators [or other groups], (2) the sender, (3) the addressees.

DSAV for Lotus Domino uses the messaging provided by Lotus Domino; messages can be sent via (1) pager, (2) e-mail, (3) fax, or (4) any other locally-implemented service.

DSAV for Lotus Domino runs on Windows NT 3.51 or 4.0; and Lotus Notes 4.0 [and above] and Lotus Domino 4.5 .

Dr Solomon's Anti-Virus for Microsoft Exchange

Microsoft Exchange is a client/server system which allows organisations to integrate e-mail, information sharing and the development of customised applications.

Microsoft Exchange allows information [contained in folders] to be copied automatically across an organisation [this is known as 'replication']. This provides a very effective mechanism for viruses to spread [copies of any infected files are sent automatically to every server within the system]. Since files are stored in a database format which can not be scanned using standard anti-virus programs, Microsoft Exchange's information stores form an ideal 'hiding-place' for viruses.

Dr Solomon's Anti-Virus for Microsoft Exchange [which operates transparently both on Exchange servers and client machines] is designed to ensure that Exchange's powerful features do not become the mechanism by which a virus is able to spread throughout an organisation.

Dr Solomon's Anti-Virus for Microsoft Exchange operates in the background, scanning new and existing files in Microsoft Exchange folders; files are scanned automatically when they are accessed, copied or replicated. In addition, Exchange administrators are able to schedule scans across the entire Microsoft Exchange information store.

E-mail messages [including attachments] are scanned automatically; and any infected files are immediately quarantined and disinfected. The Exchange administrator is notified automatically of any virus infection; and messages may be sent to the sender and receiver of the infected attachment. A central log file provides comprehensive event tracking.

Dr Solomon's Anti-Virus for Microsoft Exchange includes scanners for Microsoft Exchange, Microsoft Mail and Microsoft Outlook [the new Exchange client software].

[Top of the page](#)

Virus Central

- [Virus Analyses Main Menu](#)
- [Product Information Main Menu](#)
- [Search](#)

