

# Sophos Anti-Virus for Unix

Sophos Anti-Virus for Unix is virus detection and disinfection software which can be installed on Unix file servers and workstations. It operates in scheduled and on-demand modes, checking local and remote file systems and networks for the presence of viruses. It can provide on-access scanning of Internet downloads, email attachments and groupware for non-Unix workstations. Its unique architecture intelligently determines which files need to be virus checked, maximising user transparency and minimising performance overhead. Flexible configuration options mean that Sophos Anti-Virus can make the most efficient use of workstation and network resources.

## How it works

Sophos Anti-Virus for Unix has three components:

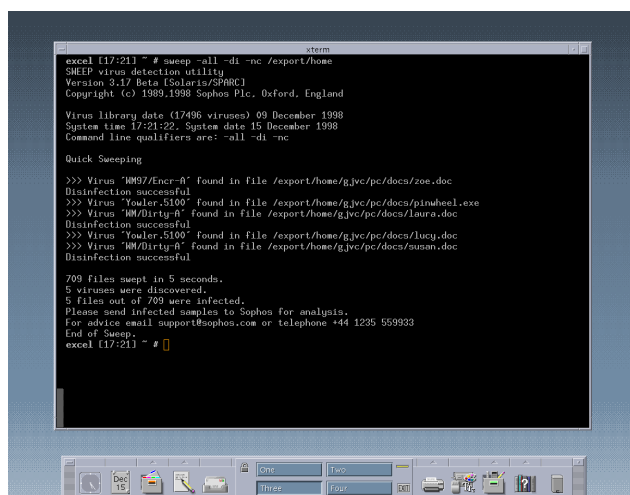
- **SWEEP** which provides on-demand checking of files on Unix file servers or workstations. Scheduled scans are also possible using SWEEP and standard Unix facilities.
- **InterCheck** which is placed on non-Unix workstations to allow on-access virus checking.
- **Sophos Anti-Virus Interface (SAVI)** which allows third-party software developers to integrate their firewall, gateway and similar applications with Sophos Anti-Virus.

**Infected** files can be removed.

**Infected** documents can be disinfected.

## Features

- Is updated twelve times a year, and urgent interim updates can be downloaded from the Sophos website or requested to be sent by fax or email.
- Easily detects polymorphic viruses using Sophos's advanced Virus Description Language (VDL) and a built-in code emulator.
- Detects and disinfects Microsoft Office macro viruses.
- Scans inside encoded and archive files.
- Features an 'immediate mode' which allows checking on demand.
- Ensures total security by providing automatic centralised reporting of every virus incident.
- Offers on-screen help as part of the CD on which the software is delivered.
- Allows third parties applications to integrate with the Sophos Anti-Virus detection engine via SAVI.
- Provides Sophos Anti-Virus for Unix servers and Sophos Anti-Virus for DOS/Windows 3.1x, Windows NT or 2000 and Windows 95/98/Me all as part of a single licence.



```
excel [17:21] ~ # sweep -all -di -nc /export/home
SHEEP virus detection utility
Version 3.17 Beta [Solaris/SPPRC]
Copyright (c) 1989,1998 Sophos Plc, Oxford, England

Virus library date (17486 viruses) 09 December 1998
System time 17:21:22, System date 15 December 1998
Command line qualifiers are: -all -di -nc

Quick Sweeping
>>> Virus "MM07/Encr-R" found in file /export/home/gjvc/pc/docs/zoe.doc
Disinfection successful
>>> Virus "Yowler.5100" found in file /export/home/gjvc/pc/docs/pinwheel.exe
Disinfection successful
>>> Virus "MM/Dirty-B" found in file /export/home/gjvc/pc/docs/laura.doc
Disinfection successful
>>> Virus "Yowler.5100" found in file /export/home/gjvc/pc/docs/lucy.doc
Disinfection successful
>>> Virus "MM/Dirty-B" found in file /export/home/gjvc/pc/docs/susan.doc
Disinfection successful

709 files swept in 5 seconds.
5 viruses were discovered.
5 files out of 709 were infected.
Please send infected samples to Sophos for analysis.
For advice email support@sophos.com or telephone +44 1235 559933
End of Sweep.
excel [17:21] ~ #
```

SAVI for Unix finding a virus



## Technical details

<b>Product name</b>	Sophos Anti-Virus for Unix.
<b>Function</b>	Scanning local and remote file systems for known viruses, and providing server-based scanning of individual non-Unix workstations.
<b>Mode of operation</b>	SWEEP: command line interface. InterCheck: daemon background process for InterCheck client workstations. SAVI: shared library.
<b>On-access scanning</b>	InterCheck Technology provides server-based scanning for non-Unix workstations.
<b>Updates</b>	12 per year, sent by post at the beginning of each month, or available for download via <a href="http://www.sophos.com">www.sophos.com</a> .
<b>Virus alerts</b>	System administrators (and optionally other users) can be automatically notified by SMTP email. In addition, logging is provided via syslog.
<b>Specification of items to be checked</b>	Individual files, recursive searching of subdirectories, individual disk subdirectories.
<b>Specification of identities</b>	Between monthly updates, interim virus identities (.IDEs) for new in-the-wild viruses can be downloaded from <a href="http://www.sophos.com">www.sophos.com</a> and added into SWEEP at run-time; they can also be sent as faxed ASCII text.
<b>Platforms</b>	AIX/PowerPC Digital Unix/Alpha (Compaq Tru64 Unix/Alpha) FreeBSD/Intel HP-UX/HP-PA Linux/Alpha Linux/Intel SCO OpenServer/Intel SCO UnixWare/Intel Solaris/Intel Solaris/SPARC

# SOPHOS

## ANTI-VIRUS



Sophos Anti-Virus (SAV) has been certified by the ICSA under Windows 95, Windows NT (Alpha), Windows NT (Intel) and NetWare; however, all SAV software shares the same virus data, virus engine and monthly concordance tests.

Sophos Plc • The Pentagon • Abingdon Science Park • Abingdon • OX14 3YP • England  
Tel 01235 559933 • Fax 01235 559935

Sophos Inc • 50-S Audubon Road • Wakefield • MA 01880 • USA  
Tel 781 213 3456 • Fax 781 213 5466

Sophos Pty Ltd • Level 4, 725 George Street • Sydney • NSW 2000 • Australia  
Tel 02 9212 1600 • Fax 02 9212 1788

Sophos Sarl • 1 Place Victor Hugo • 92411 Courbevoie Cedex • France  
Tel 01 41 99 94 20 • Fax 01 41 99 94 49

Sophos GmbH • IT-Park • Am Hahnenbusch • 55268 Nieder-Olm • Germany  
Tel 06136 91193 • Fax 06136 911940

Sophos KK • YBP W Tower (11F) • 134 Godo-cho Hodogaya-ku • Yokohama 240-0005 • Japan  
Tel 045 348 8400 • Fax 045 348 8989

[www.sophos.com](http://www.sophos.com)