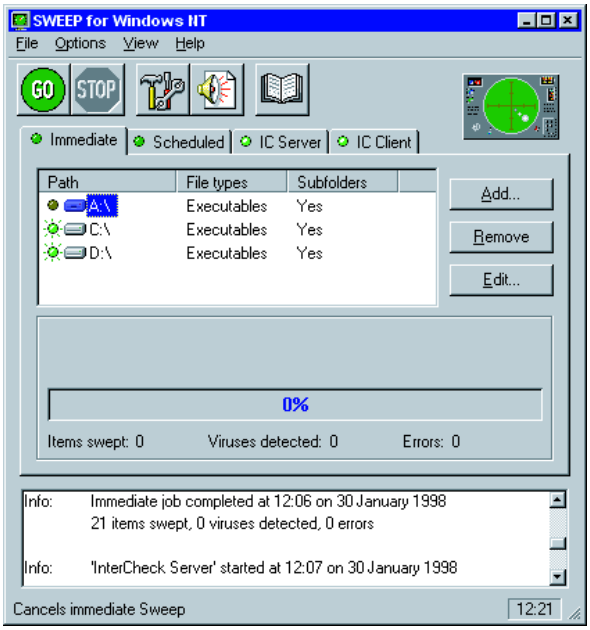
SOPHOS REVIEW
February 1998

Sophos Anti-Virus – easily the best for Windows NT



Centralisation and automation are at the core of Sophos Anti-Virus which provides a solid, enterprise-wide solution to gladden the heart of any Windows NT administrator.

Gimmick-free, the software speaks softly and carries a big stick. Its deceptively simple interface and range of easy-to-use management features belie the sophistication of its client-server operation. This innovative, corporate approach to the dynamically changing threats posed by computer viruses provides the maximum level of protection on Windows NT workstations, multiple servers and even portables that only occasionally connect to the network. Crucially, this is accomplished with no noticeable overhead.

With its robust combination of protection and automation, Sophos Anti-Virus far outstrips the offerings of its rivals. In the September 1997 *Virus Bulletin* comparative review of anti-virus products for Windows NT, Sophos Anti-Virus detected 100% of in-the-wild boot and file viruses, 100% of macro viruses and 100% of polymorphic viruses. Equally important, it found no false positives, not identifying as a virus anything that wasn't one.

The task of checking for viruses is split into two. The on-demand scanner, SWEEP, provides immediate and scheduled scanning (even when no-one is logged onto the system). The on-access scanner, InterCheck, performs real-time virus interception which prevents access to or automatically disinfects infected disks and files. Unlike most real-time scanners, InterCheck uses a database of authorisation checksums to ensure that files are scanned only if they are new or changed thus reducing the run-time overhead dramatically compared to conventional on-access scanners.

InterCheck scans all programs, documents, disks, Internet downloads, email attachments, CD-ROMs, ZIPped files and even Groupware systems – in short everything – at the point at which they are accessed by the end-user.

INTERCHECK™ TECHNOLOGY

Sophos Anti-Virus also provides heuristic recognition of macro viruses, a feature regarded as increasingly useful as the number of macro virus strains continues to grow. SWEEP's heuristic checking is switched on by default – a sure sign that Sophos is not worried about throwing up false positives.

There has been criticism that Sophos Anti-Virus does not scan inside compressed and encrypted files. This criticism is based on a myth – the fires of which are fanned by many anti-virus companies – that the only sure way of checking for viruses held in such files is to scan inside them. In fact, doing this could lead to dangerous complacency as compression and encryption techniques can conceal viruses. The only way to be certain you have trapped a virus is at the point of access; up until then, a virus cannot spread or cause any damage. By monitoring access at the point of use, InterCheck avoids data format issues. It doesn't rely on file extensions, but analyses the contents of every file accessed, irrespective of the filename.

Thanks to a friendly GUI complete with icons, drop-down menus, comprehensive on-line help, and a scrollable log of all virus incidents anywhere on the network, installation and administration are very straightforward – irrespective of the number of workstations connected to the server or the operating system they are using. This flexibility is matched by the configuration options available. On Windows 95 and other non-NT workstations, InterCheck is placed on the PC, but SWEEP can reside on the server to free up local resource. On the other hand, NT workstations take advantage of their greater power by having both SWEEP and InterCheck on the workstation. This provides quicker scanning and saves network traffic. Both configuration options can exist on the same NT network. In fact, although designed specifically for the corporate network, Sophos Anti-Virus can also be installed on a single PC, the software simply viewing the PC as a network of one.

From the CD-ROM on which it is supplied, the installation software is transferred into a central installation

directory (CID). From this single repository – and without having to configure individual workstations – the software can be installed onto a server (probably the same machine as the one holding the CID) and onto all workstations on the network.

The beauty of this centralised installation procedure is that it allows 'lights-out' updating. Every month when Sophos sends out its updates, the workstations automatically download the new software from the CID whenever they detect that a new version of Sophos Anti-Virus has been installed.

The basic setup options are enhanced by a range of management tools which further ease the task of securing the network. For instance, installation onto multiple servers from the central server can be carried out with the management tool SAVAdmin, and the administrator can create several central installations in order to balance the updating workload.

Extensive centralised messaging options, including SMTP email, mean that if Sophos Anti-Virus finds a virus anywhere on the network, an automatic report can be sent to the central administrator and/or others. The incident is also logged and a message appears on the screen of the relevant workstation.

Further security is possible in that unauthorised users can be prevented from removing Sophos Anti-Virus, and indeed the whole update process can be made non-interactive, requiring no user involvement. A neat extension to this latter feature, particularly helpful for those on remote dial-up modems, lets users postpone the update for a time determined by the administrator.

The software contains a comprehensive virus library currently detailing over 13,600 viruses – and growing by 200-300 with every monthly update. The library explains where and how each virus works, gives its aliases and advises on recovery measures. Incidentally, Sophos argues convincingly that infected program files should be replaced and not disinfected, as disinfection cannot ever guarantee that the 'cleaned' files are exactly the same as the original files.

The CD-ROM on which Sophos Anti-Virus is delivered also contains user manuals for all platforms and Sophos's Data Security Reference Guide. Creation of floppy disk versions of the software is made possible by the inclusion of the relevant images and the new open interface, SAVI, which lets third-party applications such as Integralis's MIMEsweeper integrate with Sophos Anti-Virus, is also included. The CD-ROM is accompanied by a useful Quick Start manual and the full Sophos Anti-Virus for Windows NT user manual.

Overall, it is clear that Sophos Anti-Virus has been designed for corporate networks. The software's ease-of-use, management support and centralised control make it the obvious choice for network administrators looking for extensive protection, flexibility and cross-platform support.

Management features

- centralised installation
- automatic update
- centralised multiple server installation/update
- 'lights-out' updating
- automatic virus reporting
- on-access scanning
- user transparency
- cross-platform support

Minimum requirements for Windows NT

An Intel or Alpha platform running Microsoft Windows NT 3.51 or later

Central NT installation:
– 4 Mb hard disk space (i386)
– 5.5 Mb hard disk space (AXP)

Full working installation:
– 12.5 Mb hard disk space (i386)
– 15.5 Mb hard disk space (AXP)

Sophos Anti-Virus provides comprehensive cross-platform protection: