

Technology Evaluation
and Comparison Report

February 2003

Network Security

The Benefits and Pitfalls of Contemporary
Network Security Technologies

Sophos Plc

Sophos Anti-Virus; MailMonitor; Enterprise Manager

Summary

Sophos Plc provides Anti-Virus (AV) solutions for businesses, and this Technology Audit covers three specific products: Sophos Anti-Virus, MailMonitor, and Enterprise Manager. Sophos Anti-Virus and MailMonitor are stand-alone products that can be deployed without other Sophos products, suiting customers looking for a multi-vendor approach to IT security. Enterprise Manager can be used to make the management of either or both of these products more simple, and is now bundled with Sophos Anti-Virus and MailMonitor.

Sophos Anti-Virus provides protection for the enterprise on desktop and server machines. Updates can be received automatically, up to 24 times per day, to ensure that maximum protection against virus infection can be achieved. These updates are propagated to all machines protected with Sophos Anti-Virus.

MailMonitor provides protection against e-mail-borne viruses, to ensure that incoming and outgoing mail is not carrying a recognised computer virus. Again, as with Sophos Anti-Virus, updates are provided automatically. Enterprise Manager is used to pull down virus updates from the Sophos Databank and push them into one (or more) Central Installation Libraries, from where protected machines can download the latest AV protection. This enables less human intervention than manually retrieving the latest updates and allows organisations the opportunity to be as up-to-date as possible in their fight against virus infection.

Sophos provides 24x7 support as standard, included in the annual licence fee, and this is a feature that Butler Group believes differentiates Sophos from its competitors. Certainly with AV protection time is of the essence, and the ability to contact Sophos front-line technical support (the only line of technical support) at any time of the day or night, irrespective of location, is something that we consider customers want.

► OPERATIONAL DEMANDS AND COSTS

As can be expected with most AV solutions, all three products can be used out-of-the-box, with no specific extras being required to make them work. Of course, regular updates of virus identities are required to ensure the solution remains as robust as possible.

Sophos Anti-Virus requires no dedicated server and is deployed directly on to the machines it is to protect. For 1,000 users the cost is £12 per user, offered on an annual licence basis. Support, updates, and software upgrades are included in the annual licence fee, and support is provided 24x7 as standard. Updates to the virus protection and upgrades of the software are provided automatically from the Sophos Databank using Enterprise Manager and, for remote users, Remote Update. These updates and upgrades can also be obtained manually from the Sophos Web site and a CD is shipped to customers at the beginning of each month.

Similarly to Sophos Anti-Virus, MailMonitor is provided as an out-of-the-box solution. The product is deployed directly on to the mail server, and the specification of this server is dependent upon the volume and profile of mail processed. The cost of a MailMonitor licence as a stand-alone product is £7,750 for a 1,000-user licence, again on an annual subscription basis. However, if the customer already has Sophos Anti-Virus or is purchasing it simultaneously, the cost is reduced to £2,500 on the same annual licence basis. In addition to receiving updates from the Sophos Databank, the only regular maintenance required is the management of a quarantine area where suspicious mails are placed following scanning.

As stated earlier, Enterprise Manager is now bundled with the other two Sophos products being discussed. The machine on which Enterprise Manager is installed requires a single Microsoft Windows NT SP6a, Windows 2000, or Windows XP workstation or server, running Internet Explorer 5 or above and Microsoft Management Console, or MMC, 1.2 or above to run the console software.

Enterprise Manager retrieves updates from the Sophos Databank, storing them on intermediate libraries, and then pushes them out to one (or more) Central Installation Directory (CID), from where the client computers can download the required updates. CIDs are best stored on a company server so that all clients can perform downloads simultaneously. Enterprise Manager can be used on a server used for other purposes; it does not need to be a dedicated machine. The licence supplied with Sophos Anti-Virus and/or MailMonitor incorporates one connection to the Sophos Databank per organisation. Further connection licences can be purchased but this is rarely required. Libraries can be cascaded to provide distribution across a large network.

► EASE OF USE AND MAINTENANCE

All products, because they can be deployed out-of-the-box, require only general IT administration skills to set up. For Sophos Anti-Virus it is expected that the IT administrator will alter aspects for a corporate network, for example, where to check on the network for updates. When configuring Sophos Anti-Virus, it is a matter of checking and unchecking boxes and adding the locations via a browse button (for example, locations of log files). MailMonitor uses a similar method for configuration. Enterprise Manager installation, configuration, and administration is done through the GUI and use is made of wizards and check boxes. Uninstallation of the libraries that it creates (these may be on remote computers) involves running a single command line.

The Sophos on-access filter InterCheck™ (real-time), runs in the background of Sophos Anti-Virus detecting file access and scanning new or modified files for viruses. If a virus is discovered it can be disinfected automatically, requiring no intervention by the end-user.

For both Sophos Anti-Virus and MailMonitor, updates and patches are provided in the same way, through Enterprise Manager. Additionally, Sophos Anti-Virus supplies a monthly CD to its customers, the contents of which can also be downloaded from the Sophos Web site. Enterprise Manager utilises pull technology to retrieve the latest update from the Sophos Databank, as does the Remote Update function for mobile users. Most users have Enterprise Manager set to automatically check for updates as often as possible, that is, every hour, 24x7. Butler Group believes this automated checking is a strength of the Sophos software.

Product upgrades are released by Sophos every month and these will be downloaded by all Enterprise Manager customers at a randomly allocated time within a window specified by Sophos each month, typically between six and 24 hours wide, depending on the amount of data to be transferred. It is important to note that administrators can subscribe to different versions of Sophos Anti-Virus simultaneously, to allow them to evaluate product upgrades before switching to the new version.

Once the updated virus identities have been received, administrators can choose to employ either push or pull technology to distribute the software to CIDs around the organisation. If left to pull down updates for themselves, workstations can be configured to check for updates from their CID server as frequently as every five minutes.

In terms of the security of the updates, files are signed (using Verisign) and checksummed before they are placed on the Sophos Databank. Thereafter, additional checksumming is used to guarantee that they are not corrupted during transmission to and around the organisation. Files that fail their checksums are resent. Client machines only install the software if the original checksums and signatures are correct.

► PRE-CONFIGURATION AND RULE CREATION

Sophos Anti-Virus is pre-configured for all known viruses and product updates. As a minimum, the CID needs to be specified, and configuration for a network of PCs can be done centrally by the administrator, who can include user authentication, proxy configuration, and update check frequency as required. On MailMonitor a series of default options are pre-configured, which are deemed suitable for most customers. Administrators can make changes to these default settings as required, using the MailMonitor user interface. Default settings are provided in Enterprise Manager for the location of the Sophos Databank and for the end-user configurations for Sophos Anti-Virus. The user is required to enter account credentials for accessing the Databank and other computers on the network, and network-specific settings to get through proxies.

Both MailMonitor and Sophos Anti-Virus allow an administrator to write their own rules.

► ALERTS AND REPORTING

Sophos Anti-Virus can differentiate between viruses, errors, a combination of the two, and all other activity, when alerting users to a threat. These include: desktop alerts; event log; SMTP e-mail; SNMP trap; network broadcast; and the proprietary InterCheck server already discussed. The alert options are: no message; viruses; errors; all messages; and on a per-scan-basis with alerts being sent to a list specified by the administrator. If an alert is ignored, an alert will continue to be generated every time the file is accessed.

For MailMonitor, users are alerted by e-mail messages that can be generated when a virus infection, an encrypted attachment, or an error is encountered. Alerts can be sent to recipients and senders of mail messages that are infected or encrypted, and a separate alert is also sent to the administrator. E-mail scanning will continue to take place regardless of whether an action is taken after an alert.

In terms of reporting, Sophos Anti-Virus can generate separate report files for each scan, both immediate and scheduled. Reports are displayed in text form, and can be detailed by on-access file-by-file detection of a virus, by each immediate and/or scheduled scan. It lists each virus found in each file, and each error.

MailMonitor reporting provides details of the activity of the product, including viruses detected. For a Lotus Notes environment the reports are produced using a Notes client and as such are viewed in the same environment that logs for the Domino server are viewed. Reports are also generated and stored appropriately for other platforms. The level of reporting is variable depending on what options the user selects. At a minimum, actions taken by the virus scanner are contained in the reports.

► MANAGEMENT ISSUES

Sophos Anti-Virus can optionally write information to the locally stored event log, and these logs are stored in real time. Enterprise Manager provides an event log on its own performance. The logs from any of the Enterprise Manager libraries around the organisation can be viewed at any time. They are stored in real-time on the remote library computer then transferred for viewing, periodically or on demand, to the console machine. MailMonitor does not deal with event logs itself.

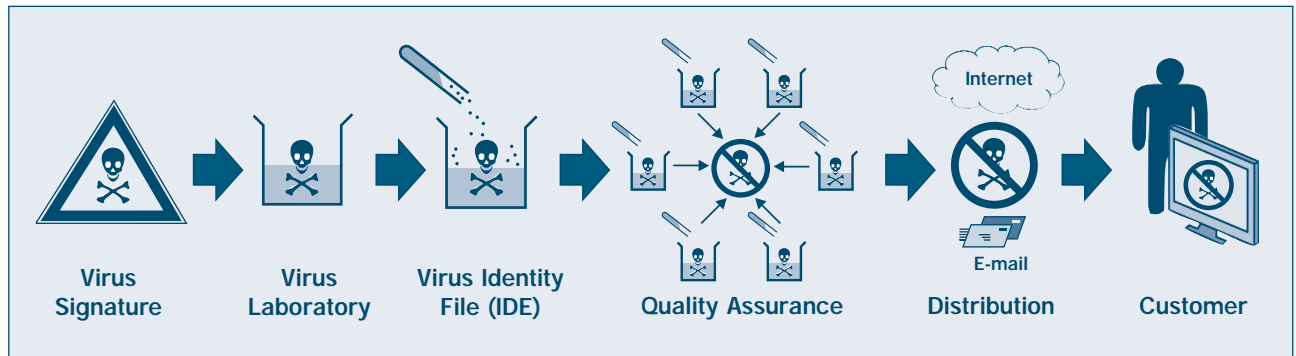
SAVAdmin, the software bundled with Sophos Anti-Virus and Enterprise Manager, administers AV protection across the network, and it includes its own console. Enterprise Manager administers product upgrades to Sophos Anti-Virus on Windows platforms as well as delivering the latest virus identities to both Sophos Anti-Virus and MailMonitor.

In Sophos Anti-Virus functions can be disabled at user level for immediate scanning, but not for on-access (real time) scanning, scheduled scanning, and virus alerts. The administrator can prevent alterations to the immediate scanning configuration. MailMonitor is a gateway product and thus all items, such as action on receipt of an infected mail, can be configured by the administrator. Overall, administrators can prevent users from disabling functions, and also from deferring a product update and removing the product. Administrators can also force non-interactive updates and prevent users from configuring the frequency with which the product checks for updates.

► RESPONSIVENESS TO NEW THREATS

In terms of self-propagating viruses, once a virus is added to the Sophos virus detection engine, the software will be able to protect against it, self-propagating or not. In addition, MailMonitor for SMTP includes threat reduction technology that can prevent infection from some new and unknown e-mail viruses by blocking common virus carriers at the gateway. All attachments and e-mail bodies passing through the server are checked for virus infection, and this includes any mass mailing e-mail viruses.

All new threats are identified in one of two categories: urgent and non-urgent. They all go through the same process, with the exception of the distribution method. The procedure for both types is shown in the following diagram:



New Threat Procedure

When a virus signature is identified it goes to the Sophos virus laboratory for a virus Identity file, or IDE, to be produced. There are likely to be a number of iterations in the virus lab of the IDE. The final IDE then goes for quality assurance testing, prior to distribution to the customer. The customer is generally configured to check for regular updates and often has already automatically retrieved the latest version before being notified by Sophos that an urgent update is available. For non-urgent updates the customer is not notified separately, but the updated virus identity will still be available for automatic retrieval and also sent out on the next CD update. Sophos claims to update CIDs within an average of 30 minutes of a new virus identity being published on its Web site, using Enterprise Manager. Approximately 20 such virus alerts are released each month, in addition to around 700 new identities released on the monthly CD.

Butler Group is satisfied that Sophos responds to new threats well, and is certainly maintaining pace with its AV competitors.

► DEPLOYMENT

Sophos Anti-Virus covers a significant number of platforms: Microsoft Windows 95/98/Me/NT/2000/XP; Linux Intel and Alpha; Netware 4,5,6; Macintosh OS8/9 and OS X; Solaris SPARC and Intel; FreeBSD/Intel; HP-UK and HP-PA; Compaq Tru64; IBM AIX; SCO OpenServer and Unixware; OpenVMS/VAX and Alpha; OS2; and DOS.

MailMonitor covers: SMTP (Microsoft Windows NT/2000; Linux; Solaris-Sparc); Notes Domino (Windows NT/2000); Exchange 2000 (Windows 2000). Enterprise Manager currently distributes Sophos Anti-Virus software for Microsoft Windows NT/2000/XP and Windows 95/98/Me clients. Sophos states that further Enterprise Manager platform support is planned for Netware, Macintosh OS, UNIX, and Linux, and Butler Group believes these will be important additions.

It is important to note that all Sophos software is backed up by 24x7 follow-the-sun support as standard. This is not something offered as standard by Sophos' competitors, and thus we feel it is a strong differentiator and a strength in Sophos' favour in the market place.

Sophos states that the installation procedure for MailMonitor requires only general IT administration skills and in most cases the customer will install the product. For Sophos Anti-Virus the administrator needs to set up a central repository and the deployment can be done via SAVAdmin, log-in scripts, or automatically via Remote Update. Currently the product cannot be deployed using a modular approach, although this is expected to change in the near future. When installing Enterprise Manager the administrator requires some knowledge of the network on which it is being installed. On larger networks more consideration has to be given to where libraries and CIDs need to be installed, to optimise the balance between WAN bandwidth usage, ease of configuration, and speed of deployment.

If required, Sophos can provide a training course for customers about the specific Sophos products they have purchased. As with most security vendors, this will be an additional cost for the customer.

► STRATEGY

The target market for Sophos security products is all-encompassing: all sizes of company in all industry sectors. Although Butler Group would often be critical of such a wide target market, in our opinion because Sophos is focusing solely on anti-virus technology, the niche it has forged makes it well positioned to attack a broad market. The route to market is mixed; a combination of a direct sales force and resellers. An extensive list of partners and certified partners can be found on the Sophos Web site, split by country and region.

In terms of what Sophos believes drives the market to its products, the rising threat of viruses is obvious, but also the transparency of AV solutions is important. Butler Group concurs with this opinion: customers want to know they are protected, but the solution they deploy must have no (or minimal) impact on performance, and end-users need to do very little to remain protected. In our opinion the standard 24x7 support is also a factor that many customers will be influenced by.

Sophos intends to enhance its Anti-Virus product for operating systems including Macintosh OS X and Microsoft Windows XP. The company is also working on streamlining installation and updating, whilst ensuring that the size of updates is kept to a minimum. This latter point is extremely important – the fix from Sophos for the recent Bugbear virus was only 571 bytes, compared to some fixes from other vendors that can run into megabytes. For MailMonitor, Sophos intends to incorporate threat reduction technology for MailMonitor for Exchange 2000 and MailMonitor for Lotus Notes. Enterprise Manager plans include increasing the languages it is available in (currently only English) and also improving on the platforms covered.

► STRENGTHS AND WEAKNESSES

STRENGTHS	WEAKNESSES
<ul style="list-style-type: none"> ● 24x7 support as standard. ● Frequent, automated checking available. ● Tight bandwidth management. 	<ul style="list-style-type: none"> ● Enterprise Manager currently limited by number of platforms available.

► VENDOR PROFILE

Sophos Plc was formed in 1980 and remains a privately held company. It made its first move into the security arena in 1985 when it produced software and hardware for data encryption, authentication, and secure erasure. It was one of the first companies to tackle the emerging virus problem when it produced anti-virus software in 1989. Sophos currently employs just over 430 people, a rapid growth from the 200 employees of 2000.

Sophos Plc is a global organisation, headquartered in Abingdon, UK. Other offices around the world include: US, Australia, France, Germany, Italy, Japan, and Singapore. In addition to the offices listed, the company also has a global network of subsidiaries and partners, enabling Sophos products to be sold and supported in over 150 countries.

As Sophos is a privately held company, financial data is limited. It has been announced that for the financial year ending 31 March 2002 turnover increased 40% to £31.6 million, and profit before tax grew 25% to £9.8 million. Also, company profits are on target for the current financial year, and since its inception Sophos has never made a financial loss. Anti-virus software accounts for 97% of Sophos' revenues, with the remainder made up from encryption software (historical product) and training. The company is fifth in terms of anti-virus vendor size, and third largest in terms of profit.

Customers include Bank of England, GlaxoSmithKline, KPMG, Marks & Spencer, and Xerox Corporation.

► CONTACT DETAILS

Sophos Plc
The Pentagon
Abingdon Science Park
Abingdon
OX14 3YP
UK

Tel: +44 (0)1235 559933

Fax: +44 (0)1235 559935

E-mail: sales@sophos.co.uk

www.sophos.co.uk

► BUTLER GROUP NETWORK SECURITY FEATURES MATRIX

Anti-Virus (AV) Features Table

		Computer Associates – eTrust Antivirus 6.0	Network Associates – McAfee Active Virus Defence	Sophos Plc – Sophos Anti-Virus, MailMonitor, and Enterprise Manager	Symantec Corporation – Symantec AntiVirus Enterprise Edition 8.5
Out-of-the-box		Yes	Yes (prefer tailored)	Yes (all 3 products)	Yes
Cost	Per 1,000 users	US\$35,000	£41,000 (1,001 seats)	£12,000	EU48,450
Administrative effort		Moderate	Moderate	Moderate/low	Moderate/high
Licence	Subscription	No	Yes	No	No
	Perpetual	Yes, volume discounts	Yes	No	Yes, volume discounts
	Annual	No	No	Yes	No
Support	Customisable by cost	Yes	Yes	No	Yes
	24x7 standard	No	No	Yes	No
Central management console		Yes	Yes	Yes	Yes
Hardware specification		Moderate	Moderate	Moderate/high	Moderate
Dedicated server		Recommended	Recommended (over 1,000)	No	Recommended
Bundling of additional products		Yes, management	Yes	Yes	Yes
Protection	Desktop	Yes	Yes	Yes	Yes
	File server	Yes	Yes	Yes	Yes
	Groupware server	Yes	Yes	Yes	Yes
	Gateway	Yes	Yes	Yes	Yes
Ease-of-use		Good	Good	Good	Good
Updates	Manual	No	Yes	Yes	Yes
	Automated	Yes	Yes	Yes	Yes
Download size control		Good	Good	Good	Average
Digitally signed updates		Yes	Yes	Yes	Yes
Own rules	Write own rules	No	No	Yes	No
	Rule wizardry	No	No	Yes	No
End-user interaction options		Controlled	Controlled	Controlled	Controlled
Reporting	Reporting media	Several	Adequate	Several	Several
	Reporting options	Detailed	Detailed	Average	Average, detailed for extra cost
Discrimination between threats	Configurable responses	Yes	Yes	Yes	Yes

		Computer Associates – eTrust Antivirus 6.0	Network Associates – McAfee Active Virus Defence	Sophos Plc – Sophos Anti-Virus, MailMonitor, & Enterprise Manager	Symantec Corporation – Symantec AntiVirus Enterprise Edition 8.5
Automated response		Yes, good	Yes, good	Yes, good	Yes, high quality
Escalation procedures		Yes	Yes	Yes	Yes
Potential number of users		Not specified	250,000	Not specified	Not specified
Integration with competing products		No	Yes	No	Yes
Platforms supported		Extensive	Microsoft flavours only	Extensive	Microsoft flavours only
Modular roll-out		Yes	Yes	Yes	Yes
Remote device compliance monitoring (i.e. remote users)		Yes	Yes	Yes	Yes
Configurable user alerts		Yes	Yes	Yes	Yes
Event log storage	Real-time	Yes	Yes	Yes	Yes
24x7 research facilities		Yes	Yes	Yes	Yes
Certification	ICSA	Yes	Yes	Yes	Yes

www.butlergroup.com

Headquarters:

Europa House, 184 Ferensway, Hull,
East Yorkshire, HU1 3UT, UK

Tel: +44 (0)1482 586149

Fax: +44 (0)1482 323577

Australian Sales Office:

Butler Direct Pty Limited, Level 6,
275 Alfred Street, North Sydney,
NSW, 2060, Australia

Tel: +61 (0)2 9955 6249

Fax: +61 (0)2 9955 5883

Butler Group ▶

ANALYSIS WITHOUT COMPROMISE