All anti-virus is not created equal

7 important factors to consider when evaluating virus protection

Chris Belthoff, Senior Security Analyst, Sophos Inc., USA

September 2003

EXECUTIVE SUMMARY

With the major anti-virus vendors offering products with uniformly high detection levels, there is a tendency to believe that anti-virus products are "all the same". However, this is a myth; the truth is that there is a great deal of difference between anti-virus products across a number of very important areas beyond detection rates. This paper provides a comprehensive summary of the seven factors that should be considered when evaluating current or new virus protection.

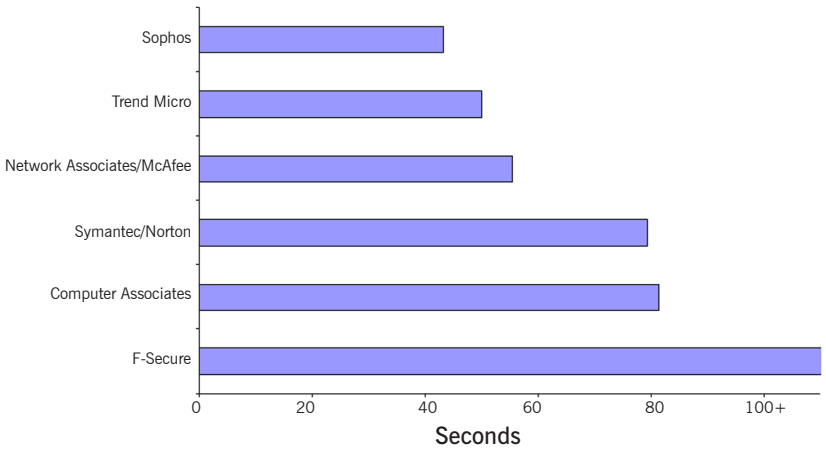
1 Performance

One of the most important aspects of virus protection is performance, particularly with respect to desktop protection. Virus engine performance at the desktop has a direct impact on end-user productivity. The faster that a virus product can perform the proper scanning, and the more efficiently the engine can be updated with the latest virus information, the less impact it will have on end-user productivity – the adage "faster is better" is hardly more relevant than when it comes to virus scanning. End users would prefer the virus software to run unobtrusively in the background and not bog down the system with exorbitant overhead.

One consequence of poor performance is the negative impact on security compliance. IT personnel are often surprised to realize that anti-virus applications are one of the biggest consumers of desktop system resource. Many IT staff whose companies use other virus vendor products are often dismayed by the fact that their end users, out of frustration, delay or cancel virus scanning at their desktops. This is due to the product consuming too much resource, taking excessive time to scan or update, and also impacting desktop stability. The end result is that this exposes a dangerous security hole and undermines the never-ending task of IT to keep the company, as a whole, in compliance with security policies.

InterCheck recognizes when files need to be scanned and scans for viruses only when necessary.

Independent testing proves Sophos Anti-Virus consistently outperforms all other major anti-virus products (see Figure 1). To optimize performance, Sophos's patented InterCheck technology intelligently recognizes when files need to be scanned for viruses and makes sure that scanning only occurs when necessary. This ensures your network and users are protected with minimal impact on system performance.



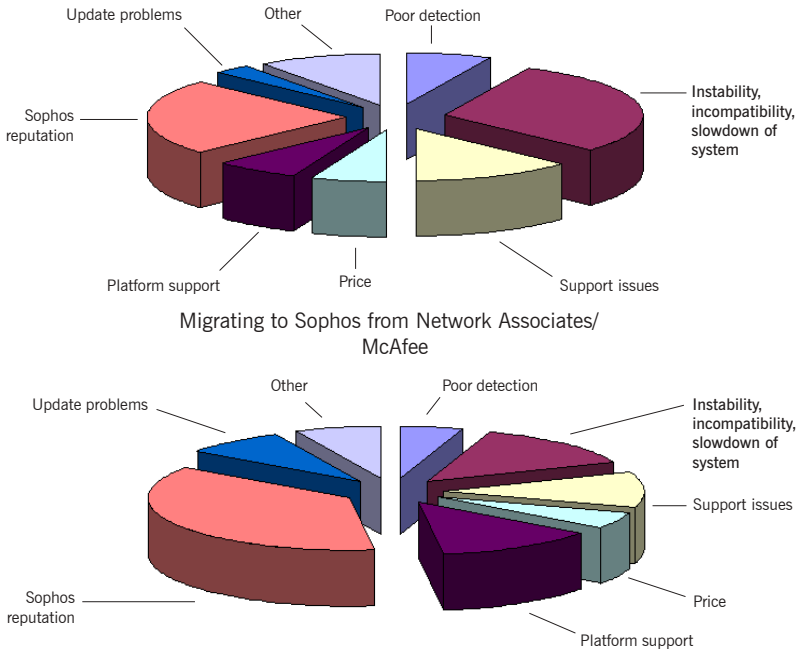
Source: Data taken from the last five tests conducted by Virus Bulletin *magazine* in which all the named companies participated (November 2001 to June 2003)*

Figure 1: Average speed of hard disk scan – anti-virus software compared

It is not that other anti-virus products are not good at *detection* – it is just that the products can be too difficult to keep properly deployed and running in the organization. Failure on this level results in a failure of the company to stay in compliance with security plans, possibly even failure to stay in compliance with regulations such as HIPAA healthcare regulations and securities/financial rules.

Customers switch to Sophos for a more stable, compatible product.

Customer surveys have verified that instability and system slowdown are two of the main reasons that companies have switched their anti-virus protection to Sophos:



Source: Data extracted from Sophos customer feedback, June 2003

Figure 2: Reasons for migration to Sophos from Network Associates and Symantec

Sophos offers an easier path to compliance, with high-performance desktop scanning that will not impact end-user productivity.

* To find out more about *Virus Bulletin*, visit www.virusbtn.com

2 Responsiveness

Responsiveness can be judged on two levels. First, how responsive is the *vendor* in identifying new virus threats and creating and making updates available for download? Second, how responsive is the *product architecture* at obtaining this update information and distributing it to the systems being protected as rapidly as possible? Both of these are important in terms of ensuring you have the latest virus protection in place. In the world of virus protection, you are only as good as your last update – without up-to-date protection an organization risks exposure to the latest virus threats.

A key aspect of vendor responsiveness is a focus on finding new viruses and creating appropriate updates to protect against them. With support teams and virus labs based around the world Sophos maintains a round-the-clock watch on new virus threats. This means Sophos can respond quickly to any new virus threat. In some documented cases Sophos is hours, even days, ahead of the competition in creating and providing virus updates.

This dedication to identifying new virus threats is supplemented by the Sophos Anti-Virus product architecture. Unlike other virus products, the Sophos architecture has been built from the ground up with networks in mind. Not only do Sophos's incremental virus updates have a minimal impact on networks, but they are also highly efficient and stable compared to other products. In fact, Sophos uses only text files for its incremental updates, not executable files that could disable a desktop configuration or interfere with other applications.

The impact of Sophos's incremental virus updates, in the order of 2KB, on a network is minimal.

Virus update sizes vary widely among the major virus vendors. With Sophos, incremental virus updates are in the order of 2KB in size. Deploying an update of this size throughout a large network (for example, 25,000 end-user desktops) typically takes 30 minutes or less. Figure 3 gives a comparison of the size and frequency of different vendors' updates.

	Sophos	Network Associates/ McAfee	Symantec/Norton	Trend Micro
Desktop installation size	12MB	25MB	45MB	30MB
Fileserver installation size (NT/2000)	10-20MB	22MB	140MB	60MB
Management console size	13MB (Enterprise Manager and SAVAdmin)	200-300MB (ePolicy Orchestrator)	155MB (Symantec System Center)	150MB (Control Manager) 100MB (OfficeScan Management)
Total (taking the largest figures)	45MB	347MB	340MB	240MB

	Sophos (IDEs)	Network Associates/ McAfee (DAT)	Symantec/Norton (LiveUpdate)	Trend Micro (Incremental)
April 2003	11	6	5	11
May 2003	23	7	8	13
June 2003	36	6	11	13
3 month total	70	19	24	37
Smallest update size	2KB	100KB	50KB	200KB
Total size of all virus updates released April-June 2003	140KB	1.9MB	1.2MB	2.37MB

Note: It is important to remember that all vendors have a number of different update methods. The methods used as examples are those most commonly used by system administrators.

Source: Data compiled by Sophos

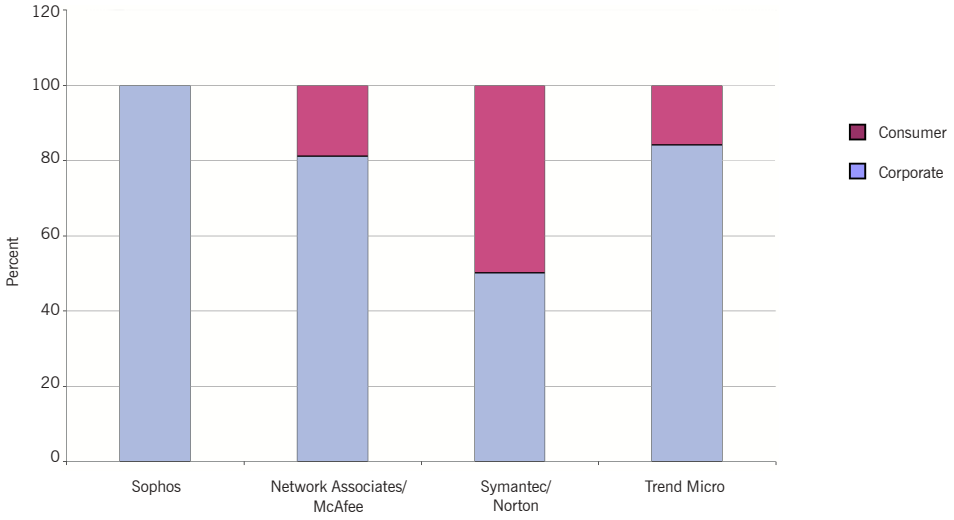
Figure 3: Update size and frequency compared

3 Enterprise/business focus

A business should choose an anti-virus vendor that focuses on the needs of the IT administrator.

In looking for an anti-virus solution for your business, it is important to choose an anti-virus vendor that focuses on the needs of an IT administrator managing business networks. These needs are very different, and much more demanding, than the needs of a home-use consumer. All other major anti-virus vendors have both business and consumer products. In fact, Symantec obtains a large proportion of its anti-virus revenue from consumer sales. This drives functionality, dilutes development resources, and impacts support efficiency.

Sophos product architecture has always focused on "top-down" network protection – very different from other vendors who have tried to take a "client-side" virus product and expand it to satisfy the needs of protecting large networks. The Sophos products are sold only to business customers and all development effort is aimed at providing the right set of features and enhancements for this market – not for the home-user market.



Source: IDC

Figure 4: Revenue by market sector, 2002

How is the Sophos architecture "network-centric"? One example is the technology employed for desktop updates, which is designed to allow desktop clients to "request" updates, instead of only being able to "push" updates down from a central point. This staggers the bandwidth requirements in a typical day and minimizes the impact on network performance.

The Sophos business focus also carries over into the area of technical support, described in more detail in section 5 below.

4 Platform coverage, including legacy systems

Cost-conscious companies need a vendor that offers consistent virus protection across a wide variety of platforms.

Many companies have made substantial investments in systems such as Windows 95/98, OpenVMS, and NetWare, as well as various Linux and Unix platforms, which are still providing benefit. With the increasing need to reduce IT budgets and contain costs, these companies are extremely reluctant to take their systems and "throw it all away" at high cost and risk to their business processes. What is needed is a virus vendor, such as Sophos, who can offer consistent protection across a wide variety of platforms.

Award-winner

"Sophos is the recipient of the customer satisfaction award. [It] has beaten tough competition from larger players in the market such as Trend Micro, Symantec and Network Associates... When ranked against other leading anti-virus vendors, Sophos came first in over half of the categories including reputation of the vendor, customer support, comprehensiveness and overall satisfaction. Sophos customers are the most satisfied of all anti-virus customers and so it has been reflected in this award.

Frost & Sullivan believes that Sophos has already gained a place on the top of the anti-virus market by having the most satisfied customers as a result of delivering on customers' expectations."

Sophos supports the investment you have already made. With an extensive list of supported platforms Sophos enables your company to leverage your existing hardware investment without the need for system upgrades. This upgrade requirement often originates from end users demanding better performance, when in all likelihood their current desktop or laptop is sufficient to run MS Office and other business applications.

Sophos supports a wide variety of platforms, as illustrated in Figure 5. This is critical both to organizations running heterogeneous networks (with non-Windows operating systems) and to those that rely on older platforms such as OpenVMS and NetWare. Platforms supported include Windows 95/98/Me, to Windows 2000/NT/XP, Mac, Linux, a wide variety of Unix flavors, NetWare, OpenVMS – even OS/2, MS-DOS and 16-bit Windows.

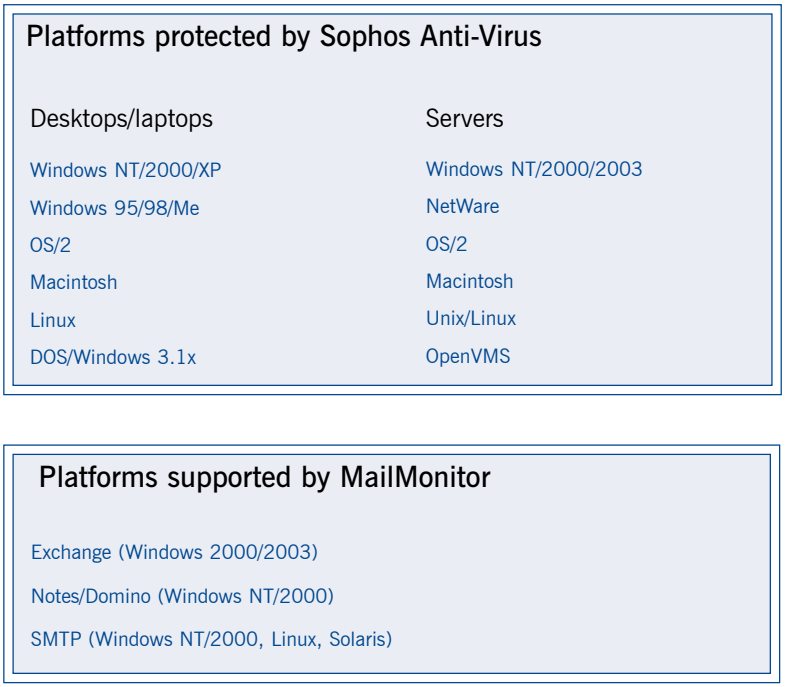


Figure 5: Platforms supported by Sophos

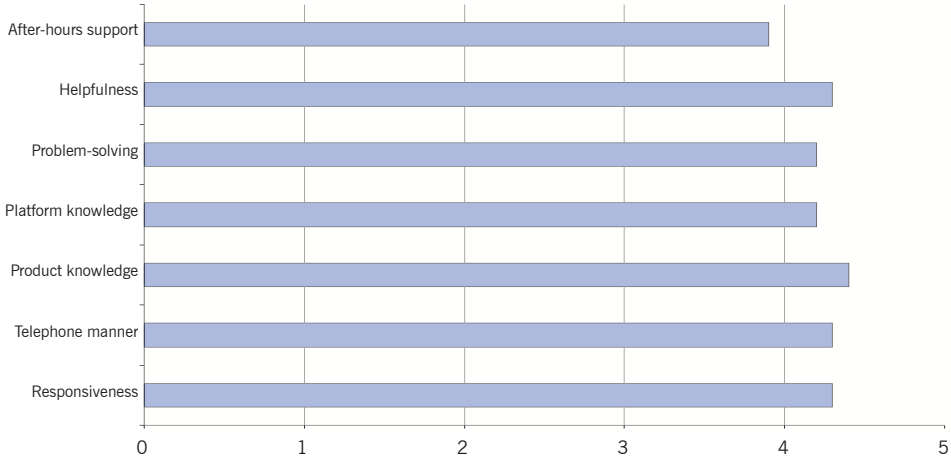
An important aspect of Sophos Anti-Virus is that the same underlying code base and engine is deployed across all supported platforms. The virus protection across all supported platforms is also updated simultaneously. This ensures consistency of coverage and product stability.

5 Technical support and customer satisfaction

One of the most important differentiators of anti-virus vendors is the way each company deals with technical support. Sophos's premium support is provided 24/7/365 to all customers at no additional cost above the license purchase, regardless of the license term. Most other virus vendors have a confusing set of support "levels" that they offer to customers, each at an additional cost.

Some vendors outsource their support, which means that the support personnel do not have direct access to the product development teams, often critical for the quick

resolution of support issues. Sophos support, on the other hand, comes from a dedicated, globally distributed, in-house team of experts who can offer practical detailed knowledge and experience. The success of this approach can be seen in the high ratings Sophos technical support receives from customers responding to its annual surveys.

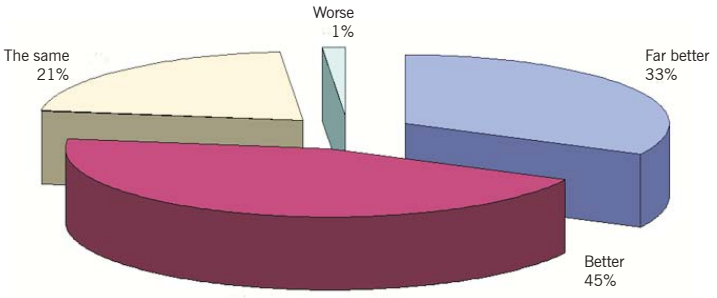


Source: Data extracted from annual Sophos 2003 customer survey;1=poor, 5= excellent

Figure 6: Average ratings for Sophos technical support

Sophos support is exclusively focused on providing help to business customers, not millions of consumer end users. This is important, particularly in times of a virus outbreak, when other vendors typically are overloaded with large numbers of non-business support calls and cannot effectively handle or respond to business customers' needs.

This business focus ensures that Sophos more than meets its goal of providing the highest level of customer satisfaction. In customer surveys conducted by Sophos, a large percentage of its customer base – 79% in the 2003 customer survey – consistently rates Sophos better or far better than other vendors' technical support.



Source: Data extracted from 2003 Sophos customer survey

Figure 7: Customer ratings for Sophos support compared with other vendors' support

6 Manageability

Superior virus protection requires a product that not only provides efficient and timely virus detection, but one that is also easy to set up and maintain. IT personnel typically desire security products that are as close to "set it and forget it" as possible. With anti-virus such a critical part of a company's overall security infrastructure, the time required for initial configuration needs to be low. More importantly, the time required for ongoing management and ensuring that updates are in place needs to be as low as possible.

Some vendors offer management tools that, although promoted by the vendor as "feature rich", often end up as expensive shelfware at the customer site. This is often due to the complexity of the management tool, and difficulties with initial configuration and ongoing management. As a result, customers abandon the product when they do not have the time and patience it demands.

With Sophos, even remote users are automatically protected and updated with minimal effort.

Sophos avoids this by providing intuitive management capabilities which deliver the necessary functionality with minimal time and effort. Sophos focuses exclusively on providing corporate anti-virus solutions that meet the needs of demanding network administrators, including an automated and easy hands-off approach to managing and updating network protection through the automatic distribution of virus updates. Even remote and mobile users are protected and automatically updated with minimal effort.

This is all available with Sophos's Enterprise Manager suite of applications. Enterprise Manager provides low-effort control over the installation and automatic updating of virus protection throughout the network – from the desktops to the servers to the gateway. Valuable virus activity information is also automatically gathered and available for review through straightforward and clear reporting capabilities.

7 Total cost of ownership

All of the six previous factors contribute, in various ways, to the essential factor that must be considered when evaluating virus protection – total cost of ownership (TCO). Measuring TCO for virus vendors and their products gives a clear understanding of the cost-effectiveness of each solution.

There are other contributors to the calculation of TCO, including the most obvious one of product license and support coverage costs. Organizations, however, are realizing that even sizable license and support costs can often be just a small proportion of anti-virus TCO. When examining TCO properly, taking into account aspects such as platform upgrades, bandwidth costs, ongoing administration time and effort, and outbreak management, it becomes very clear that there are major differences between virus vendors and between the products they offer, with resulting major differences in the cost-effectiveness of each particular product. The consequences of ignoring TCO when evaluating different anti-virus vendors can be substantial. With the current state of IT – attempting to address more security issues with tightly managed budgets and manpower – making the right choice for virus protection requires close examination of TCO. When judged by the various factors discussed in this paper, the excellence of Sophos anti-virus solutions prove the most cost-effective, with the lowest TCO.

"Sophos's simplicity makes it easy to get solid anti-virus protection."

InfoWorld

Further information

You can find out more about examining the TCO for anti-virus in the free independent report: *The hidden costs of virus protection*. More information is also available in the Sophos paper: *Total cost of ownership: a comparison of anti-virus software*, which highlights specific areas where comparisons between anti-virus vendors can be made.

Both documents can be downloaded from www.sophos.com/link/tcoinfo.

More information about Sophos products and details of how to contact your local office can also be found on the Sophos website, www.sophos.com.

Sophos, Inc.
6 Kimball Lane • 4th Floor • Lynnfield • MA 01940 • USA
Tel 1 781 973 0110 • Fax 1 781 245 8620 • Email salesus@sophos.com

SOPHOS PTY LTD
Sydney, Australia

SOPHOS SARL
Paris, France

SOPHOS GMBH
Mainz, Germany

SOPHOS SRL
Milan, Italy

SOPHOS KK
Yokohama, Japan

SOPHOS ASIA
Singapore

SOPHOS PLC
Oxford, UK

SOPHOS INC
Boston, MA, USA

SOPHOS
WWW.SOPHOS.COM