

Sophos anti-virus for business

Customer comments

“Unlike other products, you don’t know it’s there till you need it...low system overhead and high reliability make SAV the best product in the industry, period.”

“I like Sophos primarily because it releases new definitions earlier than its competitors, allowing me to protect my computers before the large virus wave hits.”

“While installing Sophos Anti-Virus, I found viruses that other anti-virus software has missed.”

“No one even comes close to the service and protection Sophos provides.”

The comments which appear throughout this briefing are taken from responses to a survey of over 1000 customers conducted by Sophos in 2002.

Summary

This executive briefing describes how Sophos products, support, and philosophy combine to deliver a complete anti-virus network solution for businesses, institutions and government organizations. Our company goal is to provide you with confidence, because you have a single anti-virus security solution that you can control across your entire network and all your operating platforms. Once you attain this sense of peace and control, your mind can relax “in the Sophos Zone”.

Who is Sophos?

Sophos is a world leader in developing anti-virus solutions for business. Since the late 1980s, Sophos products and research efforts have been exclusively focused on protecting corporate networks. Sophos’s user base is growing internationally and is currently well over 20 million protected users. Revenues are also growing, as illustrated by a nearly 50% increase in the year 2001-2002. Sophos products are sold and supported in over 150 countries through a global network of subsidiaries and partners.

Anti-virus protection from a business viewpoint

Today, computer viruses¹ have become a constant threat to the smooth operation of your networks and IT operations. Some virus attacks have become so well known and so threatening that they become the lead story of network television newscasts. The average person may not know how a virus actually works, but they do know that *Melissa* and *The Love Bug* were viruses that caused major damage to computer networks and the businesses that relied on those networks.

Computer viruses are real and preventing them from infecting computers is now an important issue in managing your corporate networks.

How do you protect your networks from virus infections? Well, obtaining an anti-virus protection product for a single computer is very easy. And in most cases, if you are diligent and download the latest anti-virus updates from the product vendor or let their automatic update feature kick-in and scan their website for the latest update, your computer will be well protected.

Protecting a single computer is simple, but what about all the computers attached to your network? The computers that connect to hundreds or thousands of other computers and are essential in helping you run your business? Ask yourself the following questions:

- Are all the computers on your network using the same anti-virus protection product?
- Can you receive and deploy the latest virus update file within minutes?
- Can you immediately respond to an alert from any computer on your network?
- If your network consists of several operating platforms, such as Windows, Linux, and Macintosh, are you able to deal effectively with multiple products and coordinate the support issues with multiple vendors?

¹ This paper uses the general term *computer virus* to refer to all types of malicious code, including Trojans and worms.

Customer comments

“Instant updates. Live technical support that is easy to reach! Not only easy to reach, but who are always pleasant and helpful on the RARE occasions I have needed them.”

“Release of IDE [virus identity file] updates is unmatched by anyone. (Fast!)”

If you have to say *No* to any of these questions, then your current anti-virus network solution may be a drain on your administrative and management resources and your protection may not be as thorough and responsive as it could be. Virus infections cost you time, money and the company trust you've worked so hard to build and maintain. The right solution is the one that gives you control over your entire network, and the peace of mind you deserve.

Corporate networks

Businesses run on networks. Corporate networks provide companies with the essential capability to efficiently share print, storage and communication resources. Each networked computer, and that could mean hundreds or thousands of nodes or stations, can communicate and share information across a local network, a private intranet, or the public internet. In today's business world, this ability to move and share information with internal departments, customers and vendors is essential to your business. Any threat to this ability is a threat to your success.

Your network exposure

Networks allow your end-users to communicate with business associates across the hall and around the globe. This powerful ability to reach out and make connections is a key element to most business transactions. However, the network architecture that supports these connections creates holes, or entry points, for viruses to enter your network.

A corporate network is typically built upon an infrastructure of four tiers:

1. Desktop and laptop computers for both local and remote users
2. Network file servers to provide network operating system services
3. Email servers to process incoming and outgoing email traffic
4. Managed services to connect beyond the local network to an intranet or the public internet

Each network tier represents potential entry points for a virus infection.

End-user desktop and laptop computers form the lowest tier group in the network structure and are very vulnerable to infection. Viruses can be introduced through physical media such as floppy disks, CDs, DVDs, or hidden in file downloads and email attachments. Even web-surfing may allow a virus to infect a computer. For any business, the number of workstations and computers across your network multiplies the difficulty in securing your network from a virus attack.

File servers are usually not as vulnerable as end-user computers. The number of servers on a network is relatively small compared to the number of users, and network administrators usually limit file server access. However, like an ordinary desktop, a file server can still be infected and since the server communicates with every networked station, a virus can spread across your network in a short amount of time.

Email servers, or gateways, touch the outside world and are responsible for routing billions of messages daily. Like a file server, the physical email server is not as vulnerable as an ordinary desktop. That's the good news. The bad news is that email has recently been acknowledged as the most common method of transmitting viruses. Since many businesses rely on email as an essential business communication tool, the potential for a virus to infect or pass through the email server and enter the network is very likely. For an email server, you need to protect both the physical server machine and the email traffic that passes through it.

Managed services, the highest tier in the network structure, are essentially the methods you choose to connect your network to the outside world. They can take the form of connecting to a third-party internet Security Provider (ISP) for email or internet

Customer comments

“I love the ease of administration with Sophos.”

“Have not had a single problem since implementation of the Sophos system.”

“From an administrator’s and user’s point of view, there is no better.”

“We have been saved a couple of times from nasty viruses due to SAV [Sophos Anti-Virus] and the automated downloading of IDEs [virus identity files]. The automated updating of the PCs via a network is one of the most important features of the software...doubt we’ll ever leave Sophos.”

connectivity, or leasing a dedicated server to control all the incoming and outgoing network traffic. In either case, the service is usually outsourced and you rely on the third party’s vigilance regarding virus protection.

Protecting your network

What should you do to protect your network and the business information that circulates across it?

Consider an anti-virus solution for every tier in your network architecture. That means providing an anti-virus solution for each desktop and remote end-user, your file and email servers, the email traffic itself, and whatever internet and email connection services you are using to connect your network to the outside world.

These initial steps will be more difficult if you are considering using multiple products from multiple vendors. If you are using products from a single vendor, the installations for each product are usually similar and the same vendor resolves any installation or interoperability issues.

Rather than physically installing an anti-virus solution on each machine, the most economical approach to installing software across your network is to automate the process from a central location. This saves a tremendous amount of time, allows you to set the configuration of each machine, and helps you establish central control procedures for later updating and reporting operations.

To begin implementing an anti-virus solution, you need to perform the following steps:

- Install anti-virus software on every desktop and workstation.
- Install anti-virus software on every remote user computer.
- Install anti-virus software on every file and email server on your network.
- Ensure that there is an anti-virus solution for the managed services you are using for your internet and email connections.

Once you have installed or ensured that there is an anti-virus solution for every tier, you now need to consider how you will effectively manage your anti-virus solution.

Managing and administering anti-virus protection

Installing an anti-virus solution across your network means you have placed a solution at your disposal. But how are you going to collect information from that solution? How are you going to make sure the latest virus update files are going to be placed on each machine in a timely manner? How will you know when an alert is generated on any network machine?

To ensure you are getting the full benefits of your anti-virus solution, you need to consider the following actions:

- Managing the process of providing timely virus update files for every computer on your network
- Identifying the procedures and reporting structure that must be followed when any station on your network acknowledges an alert for a potential virus
- Making sure all the anti-virus solutions you have deployed can report and help you monitor the virus activity across your network

Since most IT managers and administrators usually don’t have the extra hours to spend on these tasks, it is important to automate as many of these processes as you can. Automation allows you to execute a thorough administrative plan and maintain the consistency that is crucial to any security program.

Customer comments

“Support is critical in evaluating an anti-virus product, Sophos has always excelled here. Best of all, unlike some of the lesser industry leaders, it comes with the product at no extra charge, as it should be.”

“Vendors like [competitors] generally treat their customers like small children. Like many others who work in IT, I only call tech support when I have a real issue. The last thing I want is to be talked down to as if I was a child who knew nothing.”

“The automated updating of the PCs via a network is one of the most important features of the software...doubt we'll ever leave Sophos.”

Receiving support from your anti-virus vendor

Who can help you with the process of implementing and maintaining an anti-virus solution? You should be able to get a significant amount of support from your solution vendor or vendors. If you are using multiple products, your task will be more difficult because you will have more contacts and different procedures to follow.

Vendor support is an important consideration in choosing an anti-virus solution. If you have a critical situation, or if you just want to clarify an issue, you don't want to be placed on hold for long periods of time, especially if you are being charged for that support. Support should be available around the clock and not just during working hours.

The level of support can also be an issue. Unfortunately, many vendors hire support personnel to answer phones and elevate problems to a more limited number of experienced technical consultants. Getting a positive resolution on your first call is what you should expect from a solutions provider, so you can spend more time on other issues.

You also want a vendor that has anti-virus experience, whose products are certified by recognized independent certification bodies, such as ICISA and West Coast Labs, and who has invested money and resources in computer virus research.

Protecting your business and getting you in the Sophos Zone

Implementing an anti-virus solution across your network to protect your business assets is not a difficult task if you remember the following three points:

1. For total protection, make sure there is an anti-virus solution that protects each tier of your network architecture.
2. For management and control, make sure updating virus files, monitoring alerts, and collecting data is an easy, automated process.
3. For complete confidence in your anti-virus solution, make sure you select a vendor that has a tested and certified anti-virus solution for your network and that can provide you with experienced support coverage, 24 hours a day, 7 days a week, for 365 days a year (24x7x365).

These three principles are also the guidelines that we follow in designing Sophos anti-virus for business solutions. Our goal is to have our customers feel completely confident in choosing Sophos as their corporate-wide anti-virus solution. When someone mentions virus threats, our customers just smile and relax, knowing they are safely “in the Sophos Zone”.

Total protection

Sophos products are “engineered for business”. All Sophos products use the same award-winning Sophos virus detection engine and are designed to work together to catch viruses at every potential entry point across your network structure.

When you use the following Sophos products, each tier of your network is protected:

- *Sophos Anti-Virus* protects desktops, laptops and network servers.
- *MailMonitor* protects email gateways and servers.
- *SAV Interface* protects internet and other third-party connections that communicate beyond your local network.

Within each product the Sophos engine detects viruses at each potential entry point, including disks, programs, documents, hard drives, CD- and DVD-ROMs, email attachments and archived files. Using a combination of well-known and recognized anti-

Customer comments

“In our experience, just nothing comes close to the reliability and ease of distribution that Sophos can offer.”

“Sophos technical support is second-to-none, and makes a refreshing change from many other software vendors. Keep up the good work!”

“The Sophos tech support is by far the best I have used.”

“All staff that we have spoken to are helpful, friendly and excellent at their job. We would like you to pass our thanks on to them. Without them we are lost.”

virus detection technologies, including scanning, checksumming, and pattern matching, the Sophos engine detects 100% of the viruses that have been identified by virus research labs around the globe, including our own labs in the UK and Australia.

To keep you totally protected, Sophos also combines several anti-virus technologies when appropriate. For example, to help identify new virus variants and the encrypted polymorphic viruses that hide in application macros, Sophos added heuristics and virtual emulation components. Investigating and evaluating new technologies that can extend the detection capability of the Sophos engine is a continuing process at Sophos. Sophos is well recognized in the security industry and has the awards and certifications to prove it. We have been tested and certified by the following independent virus certification bodies:

- ICSA Labs
- Virus Bulletin
- West Coast Labs
- AV-Test.org

Sophos has also received numerous product awards, including:

- PC Pro Labs Winner for 2003, outperforming all nine competing products
- Network News' Recommended Product for 2002

Industry trade magazine reviews have also been positive.

- After evaluating a number of anti-virus products, InfoWorld recommended us with the following quote “...for the strongest security, best performance, technical support, and support for most desktop platforms, Sophos is the clear winner.”
- Federal Computer Week's commented, “The Sophos technology worked wonderfully in our test environments and trapped every single virus we threw in its way.”

Controls and automation

To execute an effective anti-virus solution across your network, automation is a necessity. Sophos allows you to completely automate your anti-virus solution using *Enterprise Manager* and *SAVAdmin* software. Together, this software allows you to install, administer and update the Sophos anti-virus solution anywhere on your network from a central location. This is a tremendous time saving, giving you the ability to deploy product and virus file updates within minutes of receiving them.

Enterprise Manager can also be used to automatically check the Sophos website for the latest updates and download the update packages you need at the times that are convenient for you and your company.

Monitoring virus activity from a central location is also a necessity for a good anti-virus solution. Sophos Anti-Virus incorporates a range of management features to support your network administrators. These features are installed during the initial setup and provide you with the capability of centrally logging and reporting on all virus incidents across your network.

Round-the-clock confidence

Sophos is dedicated to supporting you and your network, 24 hours a day, 7 days a week, 365 days a year. And our support is not simple phone coverage by someone who can only take a message or report an incident. Sophos technical support consultants are experienced anti-virus experts who know the industry, know your problems, and want you to feel confident about choosing Sophos as your anti-virus solution provider.

Customer comments

“On the rare occasion I have contacted Sophos for tech support, they have been brilliant.”

“Ease of management and administration definitely gives you the edge.”

“An excellent product from an excellent company. It is a pleasure to deal with you.”

By the way, Sophos support is included in your product license. You do not pay an extra fee, and we are always ready for your call.

To keep on top of the emerging viruses around the world, our virus labs are constantly analyzing new threats and sharing the information with other anti-virus vendors and certification labs. We consider your security important, and maintaining global alliances is a key part of our ongoing anti-virus development and support strategy.

Your opportunity to be in the Sophos Zone

You have your network and your business to protect. We recommend you choose a complete solution, one that allows you to feel confident and secure “in the Sophos Zone”.

To learn more about the Sophos anti-virus solution, you can:

- Visit our website, www.sophos.com, for more detailed information about our products, our company, our virus research and our customers.
- Download the trial product and evaluate it for 30 days, which includes free unlimited technical support.
- Or call our office and speak with a knowledgeable sales person.

Thank you for reading this brief introduction to our anti-virus solution for your business.

Sophos, Inc.

6 Kimball Lane • 4th Floor • Lynnfield • MA 01940 • USA

Toll Free 1 888 767 4679 • Tel 1 781 973 0110 • Fax 1 781 245 8620 • Email salesus@sophos.com • www.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

engineered for business