

SOPHOS

Reviewer's guide
Sophos Endpoint Security

 **enterprise console**

 **sophos anti-virus**

 **sophos client firewall**



WELCOME

Welcome to this reviewer's guide for Sophos Endpoint Security – Sophos's fully integrated, scalable endpoint security solution. This document introduces the elements of Sophos Endpoint Security: Sophos Enterprise Console, Sophos Anti-Virus, and Sophos Client Firewall.

The guide provides an overview of the powerful features of Sophos Endpoint Security. After reading it, you will have a deeper understanding of how Sophos Endpoint Security provides organizations with the most cost-effective and reliable protection available against known and unknown threats to computer security. It allows you to focus on other important tasks, enabling better business continuity and system efficiency.

For information on pricing and how to buy Sophos Endpoint Security, please contact your local Sophos representative. To find out who serves your area, please visit:

www.sophos.com/companyinfo/contacting

If you would like to request an evaluation of Sophos Enterprise Console, Sophos Anti-Virus and Sophos Client Firewall, please go to:

www.sophos.com/products/es/endpoint/eval

Note: Sophos supports over 25 platforms. Not all features are available on all platforms. The versions of our software described here are:



Enterprise Console: Windows XP/2000/2003 and Mac OS X



Sophos Anti-Virus: Windows XP/2000/2003 and Mac OS X



Sophos Client Firewall: Windows XP/2000

CONTENTS

1	REDUCING COST AND COMPLEXITY	4
	Overview of Sophos Endpoint Security	
2	SCALABLE, SIMPLIFIED POLICY-BASED MANAGEMENT	6
	Overview of Sophos Enterprise Console	
3	INTEGRATED THREAT PROTECTION	10
	Overview of Sophos Anti-Virus	
4	EXTENDING PROTECTION AGAINST THREATS	12
	Overview of Sophos Client Firewall	
5	SOPHOS ANTI-VIRUS IN ALL-MAC NETWORKS	15
	The need to protect all-Mac networks	
APPENDICES		
I	Evaluating Sophos Endpoint Security	17
II	The EICAR test “virus”	21
III	Other Sophos products and services	22

SOPHOS ENDPOINT SECURITY

1 REDUCING COST AND COMPLEXITY

OVERVIEW OF SOPHOS ENDPOINT SECURITY

Sophos Endpoint Security delivers a new level of enterprise security, protecting desktops, laptops, and servers against known and unknown threats. It delivers integrated protection against viruses, spyware, Trojans, worms, hackers, adware and potentially unwanted applications (PUAs) – applications that, while not malicious, are generally considered unsuitable for the majority of business networks.

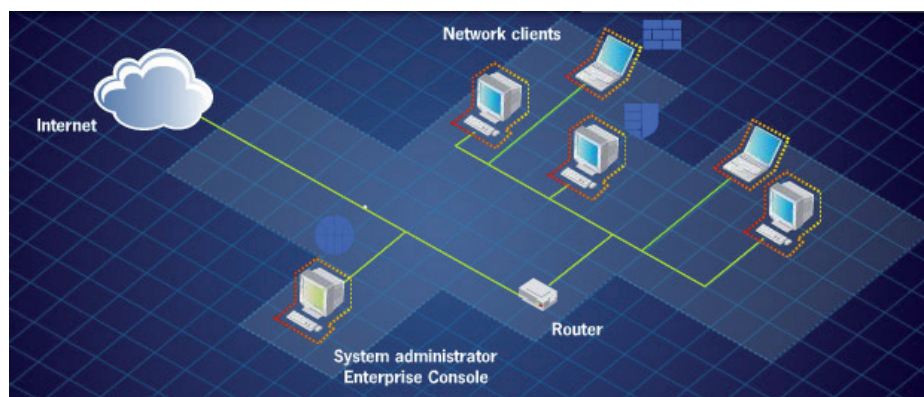


Figure 1: Integrated protection from Sophos

Sophos Endpoint Security is backed by SophosLabs™ – our global network of threat analysis centers – and brings together 20 years' experience and expertise in a single-client solution that is managed and monitored across the network from a central console. It consists of three integrated components:

- **Sophos Anti-Virus** prevents, detects and eliminates multiple known and unknown threats, including viruses, spyware, adware, and PUAs, in a single solution.
- **Sophos Client Firewall** monitors application behavior and proactively locks down computers, including remote laptops, protecting networks against internet worms, hackers and the risk of virus infection from unprotected computers.
- **Sophos Enterprise Console** centrally deploys, updates, configures, monitors, and manages both Sophos Anti-Virus and Sophos Client Firewall across tens of thousands of computers, including remote laptops, in complex networks.

With all management functions administered from a single console, and one supplier to provide support, Sophos Endpoint Security saves you and your business significant time and resources, and represents a truly low total cost of ownership. The following table shows some of the main reasons our customers choose Sophos solutions.



Reasons	Benefits of Sophos
Integrated threat management	20 years' experience means we respond rapidly to emerging threats, no matter how complex they are.
Ease of use	Enterprise Console ensures cost-effective, centralized, intuitive management that integrates the administration of Sophos Anti-Virus and Sophos Client Firewall, providing unrivaled control over network security all from a single console.
Rapid response	SophosLabs keeps a round-the-clock watch on new threats, with experts analyzing new malware across every time zone and delivering the fastest, smallest (about 5 KB) updates.
Support	Available 24/7 to all customers as part of the license, Sophos support comes from a dedicated, locally based team of experts offering practical and detailed experience, which has resulted in the highest levels of customer satisfaction levels in the industry
Business focus	Sophos sells only to corporate customers, ensuring all engineering, support, and research is focused on the needs of organizations, and is not diluted by the need to support consumers.

Table 1: Why customers trust Sophos

Unrivaled response speed

Of the four largest security vendors, Sophos regularly tops the rankings when tested for average speed in reacting to new threats.

Source: av-test.org

2 SCALABLE, SIMPLIFIED POLICY-BASED MANAGEMENT

OVERVIEW OF SOPHOS ENTERPRISE CONSOLE

Sophos Enterprise Console delivers a centralized, flexible and scalable enterprise-class management tool for endpoint security clients that reduces complexity and requires minimal administrative overhead. The console allows powerful, enforceable, policy-based management of Sophos Anti-Virus and Sophos Client Firewall on Windows and Mac computers, and lets you manage tens of thousands of users from a single console.

The console's straightforward management, effortless control over policies across the entire network, scalability and centralized targeted cleanup, significantly lower the total cost of ownership.

Many security solutions are over-engineered and burden administrators with increasingly complex systems. Enterprise Console has been engineered to give you a simple, integrated approach that allows you to take rapid action against emerging and potential problems.

Greater responsiveness and control – Sophos ActivePolicies

Sophos ActivePolicies™ is one of Enterprise Console's richest policy management features, giving you far greater insight and control when creating, deploying, and managing policies.

ActivePolicies is unique in allowing you to create a policy for Sophos Anti-Virus and Sophos Client Firewall once and then apply it to groups, or even to individual computers as required – i.e. a single default policy can be assigned to multiple groups centrally, from a single console.

This capability allows very large networks to be managed with ease from a single point, and lets you lockdown all your computers immediately in the event of a security incident.

Fast protection network-wide

ActivePolicies saves significant IT and management resources, since changes in security settings can be made to the entire network with just a few clicks.

Configuring ActivePolicies from a single console

You can quickly and intuitively configure policies in three main areas.

1 Updating policies

Enterprise Console enables you to configure the times at which different parts of the network update. This feature is particularly useful if your organization has large networks covering different time zones, or staff working at their computers at different times – particularly remote laptops connecting to the network.

Controlling automatic update settings also enables you to minimize the effect of updates on network performance.

As well as setting up automatic updating for the entire network according to your preferred schedule, you can force an update whenever a computer dials a

connection. You can also use bandwidth throttling, preventing computers from using all the bandwidth for updating when they need it for other purposes, e.g. downloading email.

2 Anti-malware and PUA policies

The “anti-virus” policy options in Enterprise Console, in fact allow you to protect your network from all known and unknown threats, including spyware, Trojans and worms, as well as adware and other PUAs that are a threat to productivity.

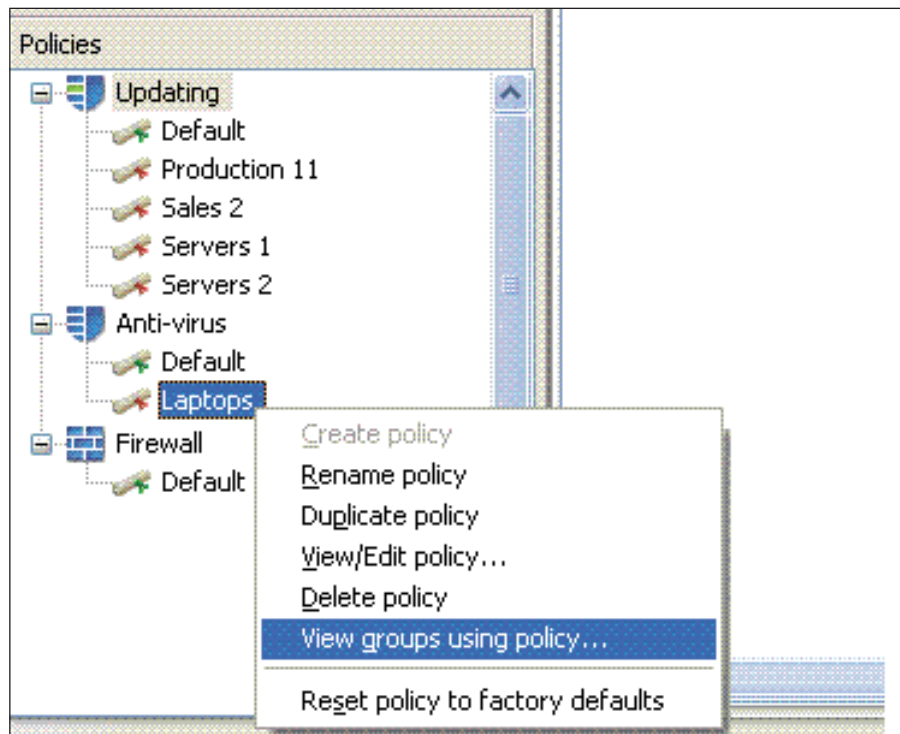


Figure 2: ActivePolicies – defining anti-malware policies

A wide range of scanning options can be configured for the entire network. You can specify requirements for on-access, scheduled and on-demand scanning and can opt to exclude particular file types where they are known to pose no threat. By default, computers will use the following standard policy:

- Scan all files that are vulnerable to malware.
- Deny access to any file that contains a virus, spyware, etc.
- Display an alert on the desktop of any computer where a virus or PUA is found.

3 Firewall policies

By default, Sophos Client Firewall is enabled for all computers in all groups and blocks all non-essential traffic. It is shipped with a set of secure default policies but these are easily changed by you to suit your particular business requirements. Every aspect of the firewall configuration can be centrally managed.

Immediate, network-wide visibility – Smart Views

Smart Views is a management feature unique to Sophos. It provides a complete, up-to-date view of the security status of all computers on the network from one console. At the click of a mouse, you can check the last known status of Sophos Anti-Virus and Sophos Client Firewall by individual computer or by group. You also have the option to view and fix only those computers that need attention, for example those with out-of-date protection or those not complying with policy.

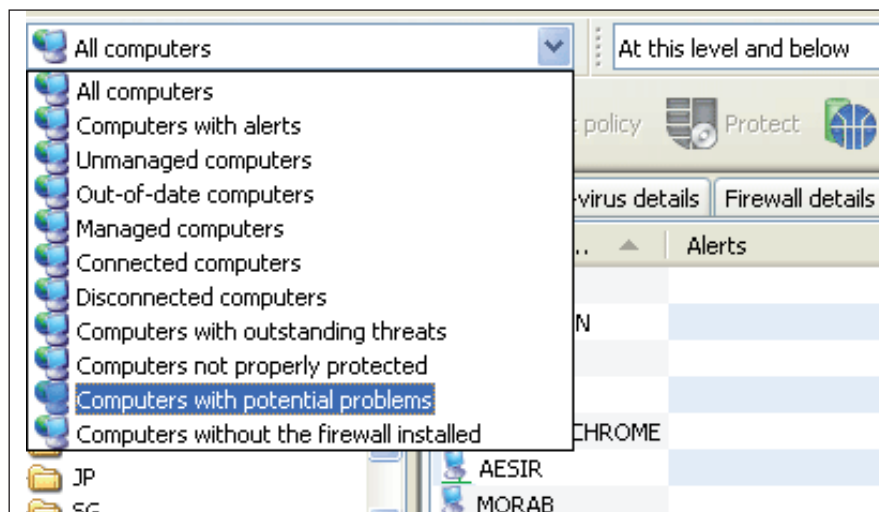


Figure 3: Smart Views – showing problems at a glance

Finding computers easily

Efficient computer discovery through the integration of Enterprise Console with Microsoft Active Directory®, network find, and IP/Subnet range search helps you to assign computers to groups more easily.

Real-time alerts

By default, alerts are displayed on the desktop of any computer on which malware or PUAs have been found. Email and SNMP alerts can also be sent to administrators or specific users if a virus, a PUA, or an error is found on any of the computers in a group. Any viruses detected on the computer will be displayed as hyperlinks, which lead to the relevant entry in the virus library on the Sophos website.

Significant scalability

Sophos Endpoint Security has been engineered to be highly scalable, enabling you to manage thousands of computers from a single console. Even greater scalability is achieved with message relays that allow computers on the network to act as relays to Enterprise Console. This reduces network traffic and load on the management server and lets very large organizations manage tens of thousands of computers.

At-a-glance visibility

With threats propagating between and within networks at ever-increasing speeds, the ability to view problem areas at a glance is a major advantage.

Message relays

By comparing and aggregating messages at the client side, Enterprise Console significantly reduces the number of messages that need to be sent between client and server, reducing the impact on the server and allowing a huge number of clients to be managed.

Centralized cleanup

Cleaning up a large network after a malware attack using standalone cleanup tools can be extremely expensive and time-consuming. Enterprise Console provides remote, centralized cleanup of files, registry entries, and running processes. Unprotected computers identified in smart Views can be cleaned in a couple of clicks.

This ability to identify and perform a targeted cleanup of threats on a remote system provides enhanced administrator productivity, significantly reducing the cost of an outbreak and its aftermath.

Integrated threat reporting

On-demand, integrated, network-wide reporting is pivotal to maintaining security in increasingly complex IT environments. Enterprise Console provides integrated reports covering computers across the entire network. With many customizable charts, graphs, and reports available, you can feel confident that you have full visibility of the status of your network.

Reports are created from virus alerts, which are processed and stored in a database on the server. Examples of the types of report available include:

- Alerts by threat
- Alerts per location
- Alerts by time
- Alert details.

Additional reporting enables you to view a wide range of information about any individual computer within the main console screen – double-clicking on the computer's name will bring up a dialog box showing a wealth of details, such as IP address, username and when the last scan was completed.

Integration with Microsoft SQL Server

Sophos Enterprise Console integrates with MSDE (Microsoft SQL Server Desktop Engine) as standard to store management information. If your organization is large, you might wish to use Microsoft SQL Server, which has enhanced functionality and greater scalability for large networks.

SOPHOS ANTI-VIRUS

3 INTEGRATED THREAT DETECTION

OVERVIEW OF SOPHOS ANTI-VIRUS

A powerful solution designed for corporate networks, Sophos Anti-Virus protects against multiple known and unknown threats in a single product, ensuring a reliable and integrated approach to threat management at the endpoint. It installs automatically throughout the network, and cannot be disabled by end users.

Sophos Anti-Virus is a key component of Sophos Endpoint Security, reducing the cost and complexity of securing your network, increasing your insight and control of security threats, and freeing up your time.

Sophos Anti-Virus supports English, French, German, Italian, Japanese, Spanish, Simplified Chinese and Traditional Chinese.

Elimination of known and unknown threats

Sophos Anti-Virus technology protects network endpoints from viruses, spyware, Trojans and worms on desktops, laptops, and servers. Genotype™ technology provides day zero protection, recognizing families and variants of known viruses, enabling them to be pre-emptively blocked even before specific detection becomes available.



Centralized detection and management of adware and PUAs

In addition to award-winning malware detection, Sophos Anti-Virus for Windows 2000/XP/2003 provides centrally managed detection and control of adware and potentially unwanted applications (PUAs). You can authorize or block PUAs selectively, at the desktop level or centrally.

Maximizing efficiency through high-performance scanning

Decision Caching™ – the high-performance on-access scanning technology in Sophos Anti-Virus for Windows 2000/XP/2003 – optimizes performance by ensuring that only new or changed files are scanned for threats. In addition, intelligent file recognition technology means that only those files which are capable of containing malware are scanned. Remote users can perform on-demand scans of individual files or the whole computer before reconnecting to the main network, providing an extra layer of security.

Freeing up time with the end-user quarantine manager

Administrators can free up time by giving end users permission to deal with any threats through a quarantine manager. They can move or delete infected files and selectively authorize PUAs, adding the applications to the approved list to stop them being blocked in future.

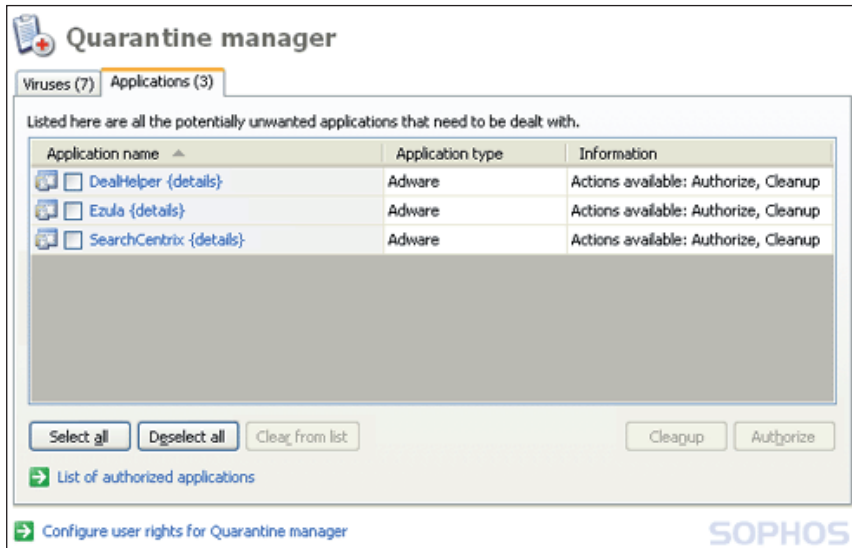


Figure 4: End-user quarantine manager

Cisco NAC integration

One of the most common causes of malware infection is from non-compliant or unprotected computers connecting to a network. Sophos Anti-Virus interfaces with the Cisco Trust Agent, allowing you to take advantage of the Cisco NAC (Network Admission Control) initiative. NAC gives you more control over computers that move on and off your networks, enabling you to ensure their anti-virus protection is up to date before they reconnect.

Support for 64-bit versions of Windows

64-bit processors let you to benefit from more memory, use larger data sets and more demanding applications, and generally run more capable operating systems. Sophos Anti-Virus's support for 64-bit versions of Windows 2000/XP/2003 ensures that any of your computers using these operating systems are protected from malware and PUAs.

SOPHOS CLIENT FIREWALL

4 EXTENDING PROTECTION AGAINST THREATS

OVERVIEW OF SOPHOS CLIENT FIREWALL

Sophos Client Firewall is a location-aware, centrally managed firewall designed for endpoint computers in an enterprise environment, and is a fully integrated component of Sophos Endpoint Security. It integrates with Sophos Anti-Virus to protect every vulnerable point of even the largest and most complex enterprise networks. It proactively locks down computers, protecting against known and unknown threats, such as internet worms, hackers, and unauthorized application communication.

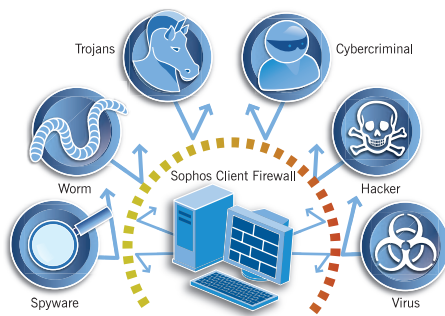


Figure 5: Day zero protection from Sophos Client Firewall

Sophos Client Firewall is centrally deployed, configured, updated, and managed by the same administration tool as Sophos Anti-Virus – Sophos Enterprise Console. It updates automatically with new versions and settings.

Day zero protection against known and unknown threats

Sophos Client Firewall works alongside Sophos Anti-Virus to provide day zero protection, i.e. it blocks the window of vulnerability that exists between a new threat emerging and protection being deployed. It defends all corporate computers from complex and rapidly spreading threats and prevents outbreaks before they can disrupt business continuity.

Proactive lockdown

Sophos Client Firewall protects against network and internet worms, hackers, and the risk of unprotected computers connecting to the network, by proactively locking down computers – both those in the office and laptops connecting via wireless hotspots and hotel broadband connections.

Port tracking and blocking to eliminate threats

Sophos Client Firewall stops known and unknown threats by tracking active ports and closing all inactive ports, ensuring that internet worms and hackers are blocked.

Stealth technology preventing intrusion by hackers

Cybercriminals, such as hackers, use port scanning to identify and target vulnerable computers with open ports. They do this by sending out connection requests across the internet. Sophos's stealth technology prevents computers from responding to these requests, hiding a computer and making it appear inactive to the outside world. This gives you an additional level of protection, ensuring privacy by eliminating the opportunity for hackers to identify and target vulnerable computers.

Preventing unauthorized access through location awareness

Sophos Client Firewall lets you configure trusted "safe zones" with different sets of rules for different network scenarios. The firewall applies the appropriate set of rules to a computer, depending on which network it is connected to. By enforcing these location-awareness rules, the firewall ensures that every computer is protected on and off its normal network.

Preventing information theft and application hijacking

Application-level filtering is used to monitor application behavior, allowing internet or network access only to applications that meet your specifications. Sophos Client Firewall prevents application hijacking by monitoring inappropriate application and system calls, and the launching of hidden processes. It also uses checksumming to foil attempts by spyware and other malware to masquerade as a legitimate application, thereby preventing the theft of confidential information over the internet.

Stateful inspection scans incoming and outgoing data packets

Sophos Client Firewall uses stateful inspection (invented by Check Point) to enhance security by keeping track of communications packets and ensuring only legitimate packets reach the network. Outgoing packets that request specific types of incoming packets are tracked; only those incoming packets constituting a proper response are allowed through the firewall.

Central reporting and logging

The firewall reports new and modified applications to Enterprise Console. You can set how long records are kept for and adjust the maximum amount of memory to be used for storage. In addition, the firewall's log viewer enables you to view, filter and save details of the connections that the firewall has allowed or blocked.

Stopping fast-moving threats

The fast-moving internet worm SQL Slammer infected hundreds of thousands of computers globally in a matter of minutes by spreading on port 1434. By blocking this port, affected organizations could have stopped the threat in the crucial early stages before the anti-virus signature file was deployed.

Interactive or non-interactive working

You can configure Sophos Client Firewall to allow end users to have control over which applications are or are not allowed, which offers the flexibility that some businesses require. Alternatively you can choose to set the firewall to operate non-interactively so that it automatically uses the rules you have set for the network.

Firewall policy control

If Enterprise Console is used to administer the network, it may override changes made by end users at individual desktops.

5 SOPHOS ANTI-VIRUS IN ALL-MAC NETWORKS

THE NEED TO PROTECT ALL-MAC NETWORKS

It has become increasingly important to protect Mac computers, even in an all-Mac environment. The ability of Macs to harbor and spread Windows viruses, the occasional appearance of Mac viruses, and legal demands that every computer be protected, all place increasing demands on IT administrators.

Like Sophos Anti-Virus for Windows 2000/XP/2003, Sophos Anti-Virus for Mac OS X offers a powerful and intuitive solution designed for corporate endpoint servers, desktops, and laptops. It is available in English, Japanese, French, German, and Spanish and supports both Intel and PowerPC.

Elimination of known and unknown threats

Sophos Anti-Virus for Mac OS X detects viruses, spyware, Trojans, and worms, in real time and on demand, and automatically cleans Windows as well as Mac malware. Sophos Anti-Virus for Mac OS X also detects viruses in compressed attachments, including recursive archives.

Centralized management through Sophos Update Manager

Designed for all-Mac networks, Sophos Update Manager allows updating and configuration from a single Mac computer. It enables you to set automatic updating and choose how you receive email notifications. It also allows you to determine how scanning will be implemented on desktops and laptops, and enables full centralized configuration of the desktop settings.

Note

Even where there is only one Windows computer, Sophos Enterprise Console is used to manage the Mac network, as described earlier.

This section refers to networks that are truly 100% Mac-based. In this case Sophos Anti-Virus is centrally configured, deployed and updated across the entire network using standard Mac tools and the Sophos Update Manager.

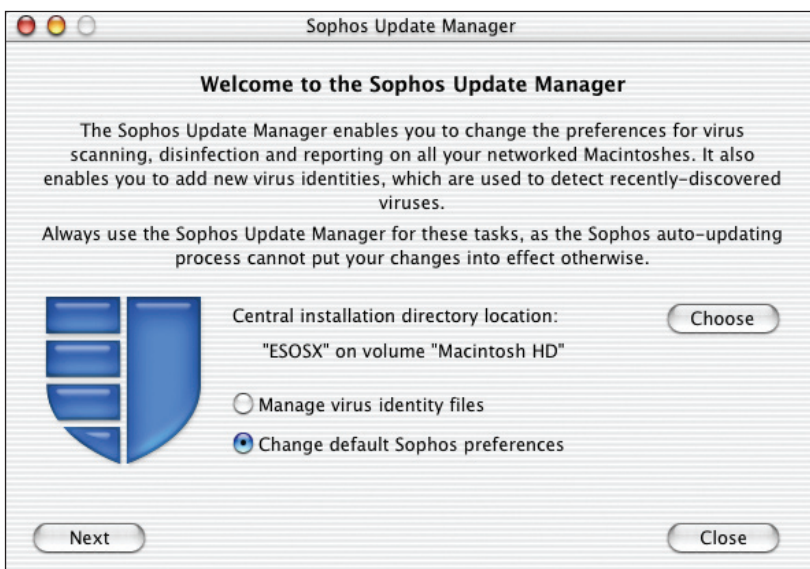


Figure 6: Sophos Update Manager



Automatic updating from SophosLabs

Through Sophos Update Manager you can specify the address, username, and password needed for computers to update themselves with the latest virus identity files (IDEs) from SophosLabs. Alternatively, you can set computers to update themselves from the CID (the central installation directory, which is set up on the network during the install process). If you choose this option, you will need to update your CID regularly by downloading the latest updates from the Sophos website manually.

You can also enable remote and mobile users to update from wherever they are via the network or internet, either from the main server, a backup, or directly from Sophos.

Automatic reporting of virus incidents

The flexible messaging options in Sophos Anti-Virus provide instant notification of any virus on the network, enabling administrators to take early action during a virus incident.

Using Sophos Update Manager, you can set alert options for immediate scanning and on-access scanning, and also select the recipient of the message. Alerts are stored if the sender is not connected, and are forwarded when the sender reconnects to the network, so that none are lost.

Minimized scanning overheads

Sophos Anti-Virus scans files on-access and on-demand, intelligently recognizing uninfected file types, thus saving system resources. You can set a number of scanning options in Sophos Update Manager, such as excluding certain files from scanning, and setting preferences for actions to take if a threat is found, e.g. disinfect or delete.

Includes end-user on-demand scanning for viruses

Sophos Anti-Virus automatically scans each file as you access it, granting access only if it is clean. End users can also carry out an on-demand scan by clicking on the Sophos Anti-Virus icon in the task bar.

Remote updating

The remote updating facility of Sophos Anti-Virus provides an extra layer of security to your network, ensuring that malware cannot be brought in via remote laptops.

APPENDIX I

EVALUATING SOPHOS ENDPOINT SECURITY

We want you to be absolutely convinced that Sophos Endpoint Security will protect your network and support you better than any other security vendor. This appendix gives you details of what documentation you will need to evaluate our software, suggests a test network and gives you a comprehensive checklist to help you consider every aspect of the software and support we offer.

Startup guide and user manuals

Before you evaluate Sophos Endpoint Security, you will need to download the Sophos Anti-Virus and Sophos Client Firewall network startup guide. To find this, go to:

www.sophos.com/support/docs

Note that Sophos Enterprise Console is covered as part of the installation and use of Sophos Anti-Virus and Sophos Client Firewall.

You might also like to click the **View all documents** tab to find:

- Sophos Anti-Virus and/or Sophos Client Firewall user manual.
- Sophos Anti-Virus and/or Sophos Client Firewall standalone startup guide. (You will only need these if you are evaluating on a single computer.)

If you want to set up and configure NAC settings, you will also need to download the Sophos Anti-Virus Cisco NAC integration guide, listed under **Supplements**.

Sophos Anti-Virus test network

Sophos Anti-Virus supports many platforms, including UNIX, Linux and NetWare. However, to evaluate the centralized management features of Enterprise Console you will need at least one Windows computer. We suggest you include the following in your test network:

- A management console, i.e. a computer running Windows 2000/XP/2003.
- At least one client – we recommend using a Windows 2000/XP/2003 desktop.

You will also need access to the internet. You might also like to include computers supporting Mac OS X platforms in your test network, as well as a remote standalone computer to evaluate remote updating and configuration capabilities.

Important

If you have any other anti-virus software installed on your test network, you should uninstall it first. If you have problems doing this, please contact Sophos technical support – contact details can be found at www.sophos.com/support/queries

Sophos Anti-Virus system requirements

Memory	
Windows 2000/XP/2003 and Enterprise Console	Recommended 256 MB
Windows NT4	Recommended 256 MB
Windows 95/98/Me	Recommended 64 MB
Disk space	
Windows 2000/XP/2003	120 MB
Windows NT4	256 MB
Platforms supported	
Windows 2000 Windows XP/2003, including 64-bit versions Windows 95/98/Me and NT4	

Sophos Client Firewall test network

To evaluate Sophos Client Firewall, you need to have Sophos Anti-Virus for Windows 2000/XP/2003 installed*.

Sophos Client Firewall system requirements

Disk space	Minimum 20 MB free
Memory	Recommended 256 MB RAM
Processor	Pentium class 300 MHz
Platforms supported	Windows 2000 Professional Windows XP Professional Windows XP Home

Sophos Anti-Virus for Mac OS X test network

You will need to set up a test network of computers running Mac OS X. You will also need to nominate one computer to act as a server containing the central installation directory (CID) – a folder used to download Sophos Anti-Virus and deploy it to the rest of the network. The CID will also house Sophos Update Manager, which keeps Mac OS X computers on the network up to date with the latest virus identity files (IDEs) and configuration settings.

Sophos Anti-Virus for Mac OS X system requirements

Disk space	Minimum 77 MB free
Memory	Recommended 128 MB RAM
Processor	Intel-based and PowerPC-based Macs
Platforms supported	Mac OS X 10.2 or higher

*Note that Sophos Client Firewall does not support Windows 2000/2003 Server

EVALUATION CHECKLIST

Installation

- Ability to integrate into the existing system architecture
- Scalability to meet the needs of larger networks (using message relays)
- Support for the operating systems in the organization
- Meeting hardware requirements – servers, laptops, and desktops
- Hardware upgrades required or not
- Installation method – local and remote
- Ability to check whether desktops are properly installed
- Overall ease of deployment, including management tools and computer discovery options*

Threat protection

- Detection rates
- Centralized control over unauthorized application communication* (hijacking and hidden processes behavior)
- Proactive ability to lock down vulnerable computers*
- Hacking and intrusion prevention*
- Centralized control over application filtering*
- Scanning efficiency
- Proactive protection from unknown and fast-moving threats (identifying families and variants of known viruses) and port tracking
- Ability to scan compressed files and archives
- Low CPU overhead and stability of the on-access scanner
- Centralized ability to update the entire network automatically
- Speed, frequency, and size of anti-virus and security updates
- Availability/speed of website for virus definition updates.
- Speed of scanning

Management

- Simplified, integrated, centralized, scalable management of Sophos Anti-Virus and Sophos Client Firewall
- Ability to check in a couple of clicks that every computer is protected and up to date*
- Mechanism used to deploy virus detection and security updates automatically across the network from a single location
- Ability to force an update
- Ability to simply create policies once, then edit, deploy, and manage them across the network from a single location*
- Ability to perform targeted cleanup of files, registry entries and running processes remotely from a central location*
- Centralized mechanism used to deploy engine and updates automatically
- Integrated reporting of threats*
- Administrator-assigned permission preventing end users disabling the software

- Centralized detection, cleanup and removal of malware (including registry entries) from a single location
- Centralized cleanup and removal of PUAs from a single location*
- Mechanism to add, update, and move software licenses
- End-user quarantine manager to ease virus infection and PUA cleanup, reducing administrative overheads*
- Ability to enforce security policy on computers connecting to the network (via integration with Cisco NAC)*
- Choice of MSDE and SQL Server databases for storing management information*
- Location awareness (Sophos Client Firewall)

Maintenance

- 24/7 local priority technical support, level of support and what, if any, additional cost is incurred
- Means used to address critical viruses from the first discovery
- Ease of access to product upgrades, patches and service packs and what, if any, additional cost is incurred
- Ability for employees to use the product at home at no extra cost
- License flexibility – per node, platform and country

* Applies only to Sophos Client Firewall and Sophos Anti-Virus for Windows 2000/XP/2003, v6.0

APPENDIX II

THE EICAR TEST “VIRUS”

ABOUT THE EICAR TEST FILE

The EICAR* Standard Anti-virus Test File is safe to use for test purposes because it is **not** a virus, and does not include any fragments of viral code. It is a legitimate DOS program that consists entirely of printable ASCII characters. The file lets you simulate safely what happens when Sophos Anti-Virus detects malicious code. When you attempt to run the file, it will be “detected” as though it were a real virus and (customizable) alert messages will be generated.

Using the EICAR file, you can also see the various kinds of report that can be generated.

Creating the EICAR test file

You can download a copy of the test file at www.eicar.org

Alternatively, to make your own EICAR test file, create a file entitled EICAR.COM in a text editor such as Notepad with the following characters as the only content:

```
X5O!P%@AP[4\PZX54(P^ )7CC7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Note that the file uses only upper case letters, digits and punctuation marks, and does not include spaces. You should also ensure that:

- the third character is the capital letter “O”, not the digit zero.
- all 68 characters are on one line.

We suggest that you make these 68 characters the only content but if you decide that you want to add other text, you must make sure that the EICAR characters are the very first line in the file.

Note

Because the EICAR file is not a real virus, it cannot be cleaned by Sophos Anti-Virus and you will need to delete the file manually.

*European Institute for Computer Anti-virus Research

APPENDIX III

OTHER SOPHOS PRODUCTS AND SERVICES

PRODUCTS

Gateway protection

Sophos Email Security Appliance

Sophos Email Security Appliance is a fully integrated hardware solution that provides effective, intelligent, and secure protection against viruses, spyware, Trojans, spam, and offensive content.

Sophos PureMessage®

Sophos PureMessage® is a flexible software solution integrating anti-virus, anti-spam, and powerful policy enforcement capabilities to protect against viruses, spyware, Trojans, spam, and email policy abuse at the UNIX gateway and on Windows®/Exchange email servers.

Sophos MailMonitor

Sophos MailMonitor™ provides anti-virus protection and threat reduction technology on SMTP servers and also protects networks where PureMessage is unsuitable, such as Notes/Domino™.

SAV Interface

SAV Interface™ enables software vendors, OEMs, ISPs, and ASPs to integrate Sophos malware detection into their own industry-standard firewalls, gateways, and similar solutions.

Sophos small business solutions

Sophos small business solutions provide award-winning virus, spyware, and spam protection to enterprises with little or no IT expertise.

SOPHOS ALERT SERVICES

Sophos ZombieAlert™ Service provides you with immediate warning if spammers have hijacked any of your organization's computers to send spam or launch denial-of-service attacks.

Sophos PhishAlert™ Service provides fast, near real-time alerts of phishing campaigns, so that you can take steps to shut down the imitation website and protect your organization's customers.

For more information on Sophos Alert Services, visit:

www.sophos.com/products/es/zombiealert
www.sophos.com/products/es/phishalert

Unlimited 24/7 support

The excellence of Sophos support services sets us apart from our competitors, allowing you to benefit from 24-hour support provided by a globally managed team every day of the year. You can contact our engineers for one-to-one support by email or telephone, or use our web-based support knowledgebase.

Our 24-hour support, included with every Sophos license, puts you in touch with support engineers who have the tools and resources to investigate any problems thoroughly – including access to a test network of machines running every supported operating system and network platform. Our experts can replicate, analyze, and resolve your problems, drawing on a wealth of experience and technology – backed by the multiple resources of SophosLabs and product development – to ensure the efficient resolution and tracking of all incidents. Premium and Platinum support packages are also available.

Our technical support operates from support centers in Australia, Canada, France, Germany, Japan, Italy, Singapore, UK and USA. Whichever center handles your problem, you can be assured of the highest level of expertise, professionalism and customer service. You can find full contact details for each center at:

www.sophos.com/support

SOPHOS

Sophos is the world leader in integrated threat management solutions purpose-built for business, education and government. With 20 years' experience SophosLabs protects even the most complex networks from known and unknown malware, spyware, intrusions, unwanted applications, spam and policy abuse. Our reliably engineered, easy-to-operate products are trusted by over 35 million users in more than 150 countries. Round-the-clock vigilance has resulted in our increasingly rapid international growth, expanding user base and continuous profitability. Our instant response to new threats is matched by business-focused, 24/7 technical support, and has led to the highest levels of customer satisfaction in the industry.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

esrg060506



integrated threat management