

# Cutting the cost and complexity of managing endpoint security

A Sophos positioning paper

July 2006

Managing the desktops, laptops and servers at the endpoints of corporate networks is an increasingly complex, time-consuming and expensive task. This paper examines the issues of managing security across the network, discusses the key criteria involved in choosing a solution, and looks at how Sophos Endpoint Security eases the administrative burden and provides an enviable total cost of ownership.

---

## The complexity of the challenge

Securing the business network is a constantly evolving, resource-consuming task. Not only has malware become increasingly complex – using blended techniques and spreading ever faster – but also the motivation behind it has changed.

Threats have become more targeted and surreptitious, written by cybercriminals for financial gain and with the intention of dropping beneath the radar of much detection software. The proportion of email which is virus infected has fallen considerably over the last year as hackers have turned from mass-mailing attacks to targeted Trojan horses containing spyware. In May 2005, one in every 38 emails was infected, now this number is just one in 141, as criminals look for new ways into the corporate network.<sup>1</sup> The relentless emergence of new threats, like spyware, adware and hackers, makes it harder than ever for organizations to keep themselves protected from intrusion and infection.

---

*In May 2006, only 12.3% of the new threats detected by Sophos were viruses and worms. The majority of the new threats (85.1%) were Trojan horses.<sup>1</sup>*

---

At the same time, IT requirements are changing, with end users demanding internet and email access outside the controlled environment of a local area network. Wireless networks, PDAs, laptops and USB storage devices are increasingly freeing employees to work remotely. While there are many business reasons that make this freedom desirable, it also carries significant risk. Mobile computers that are not effectively protected can carry unknown threats into the corporate network, compromising business continuity.

While it still remains vital to protect the email gateway to stop many threats before they even get to the network, today's

practice of anywhere, any time connection means that the traditional gateway defenses are often bypassed. Many threats can only be detected at an organization's endpoints – the laptops, desktops and servers.

## The challenge of the solution

Even with top priority being given to the creation and enforcement of robust security policies, the challenge of implementing and controlling multiple security technologies to protect every point on the network can take up an unnecessary amount of time, IT budget and resource. The effective management of security across all endpoints brings with it a particular set of problems, which can be complex and costly to implement. How do you know which computers are affected? How can you get them protected instantly? How can you isolate the ones that have a problem?

Security vendors have recognized the changing nature of the threat and many have responded with anti-malware software, appliances and firewalls laced with features that they hope will address those particular problems. Ironically, many of them fail because of these very features. Over-engineered and overly complex, these products often require separate management and do not allow you to respond and execute quickly to changing security threats. The question really is not how many features there are, or how many complicated things they can do, but how useful they are, how integrated they are, and how easy they are to use.

---

*Nearly 60 percent of US businesses believe that cybercrime is more costly to them than physical crime."<sup>2</sup>*

---

## Sophos Endpoint Security – lowering the TCO

The problem with managing security and policies across a large number of groups comes when the fragmented management tasks are replicated in fragmented solution – which is complex and costly to administer.

In order to lower the total cost of ownership (TCO) of managing endpoint security, you need to find a solution that offers, powerful, scalable management of all security endpoint computers but that is straightforward and simple to use, letting you manage your security software across your entire network from a single point.

An integrated solution – like Sophos Endpoint Security – can bring significant savings in time and resource, freeing you up to concentrate on other important tasks.

### Proactive protection against all threats

Clearly the starting point in choosing a solution is to establish that the underlying protection is totally reliable and able to protect against both known threats and unknown threats – not just traditional viruses and worms but also hackers, application hijackers, spyware, and potentially unwanted applications, such as adware.

Highly skilled analysts in SophosLabs™ – a worldwide network of threat analysis centers – combine expertise, technology, and a global visibility of emerging threats, to provide round-the-clock protection and the fastest smallest automatic updates. Sophos Anti-Virus™ provides protection against spyware, viruses, Trojans, and worms, and this is matched by application behavior monitoring and port blocking in Sophos Client Firewall™. However, even this high level of award-winning protection is not all that is required to constitute “the perfect solution”.

Protection on its own – however comprehensive – will not provide a good return on investment if you spend a long

time tracking down and visiting individual machines or if you have to recreate the same malware and firewall policies over and over again in order to deploy them to different groups of computers. The following paragraphs highlight the other key criteria above and beyond that of protection that you should look for in an effective management solution and demonstrate how Sophos Endpoint Security meets them.

---

*“With the rise of blended threats, there is an increasing need for integration between individual endpoint security components in order to reduce the cost and time associated with managing point products. Sophos Endpoint Security simplifies the complexity associated with managing multiple security solutions, while at the same time increasing the effectiveness of protection.”*

*Brian Burke, Research Manager, IDC*

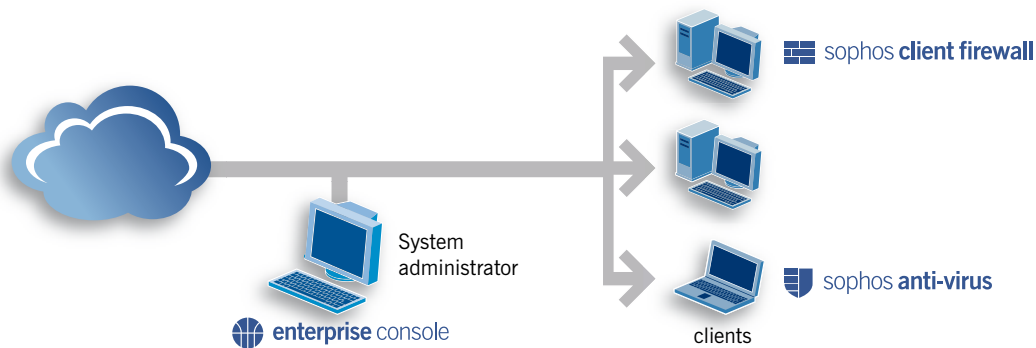
---

### Centralized management and control

One of the most resource-hungry tasks for IT is the need to visit multiple computers, whether to install software, to create and enforce policies, or to cleanup after any infection by malware.

#### Single-point installation and update

Sophos Enterprise Console™ – a major component of Sophos Endpoint Security – lets you deploy and update Sophos Anti-Virus and Sophos Client Firewall across the network, including remote computers, from a single console. You can easily find all the computers on the network by using built-in search or Microsoft Active Directory data, or searching by IP subnet ranges.



Sophos Endpoint Security – central management of endpoints from a single console

### *Rapid creation and enforcement of policies*

ActivePolicies, a key feature of Enterprise Console, lets you rapidly create and update security policies. You can deploy a single policy across multiple groups simultaneously, rather than having to create the same policy for each group that you want to apply it to.

### *Centralized clean up*

Cleaning up a large network after a malware attack using standalone cleanup tools can be extremely expensive and time-consuming. So being able to identify infected computers and perform a targeted cleanup of viruses, spyware, Trojans remotely can greatly enhance your productivity, and significantly reduce the cost of an outbreak and its aftermath.

---

*Respondents to an FBI survey spent nearly:*

*\$12m to deal with virus incidents*

*\$2.8m on financial fraud and*

*\$2.7m on network intrusions<sup>3</sup>*

---

### *Selective PUA authorization*

Potentially unwanted applications, like adware, are generally viewed by organizations as inappropriate for the business environment, even though they are not actually malicious. For this reason, Sophos Anti-Virus blocks these by default. However, because some organizations might want certain of these applications to be allowed, you can easily select and authorize them centrally from Enterprise Console. You can also centrally block any application.

### *Network access control*

One of the most common causes of infection is from non-compliant or unprotected computers connecting to the network. Sophos Anti-Virus's integration with Cisco NAC (Network Admission Control) gives you more control over computers that move on and off your network, enabling you to ensure their protection is up to date before they reconnect.

### *Network-wide 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. Smart Views lets you manage by exception, focusing straightaway on any vulnerable computers that are not complying with your security policies, that need updating policies, or that need cleaning up.

### *Real-time alerts*

If a virus or other incident does occur, you need to know instantly, in order to contain and deal with the infection. When any malware or PUA has been found, an alert is displayed on the computer and an alert is sent to the administrator.

### **Sophos Endpoint Security at a glance**

**Sophos Endpoint Security** builds on Sophos's 20 years' experience to deliver scalable, centralized, integrated protection against multiple known and unknown threats, backed up by 24/7 expert support:

- **Sophos Enterprise Console** is a single, scalable console that lets you manage and control protection on tens of thousands of computers with powerful but easy-to-use software.
- **Sophos Anti-Virus** provides complex networks with rapid integrated proactive protection against viruses, spyware, Trojans, adware and other PUAs and updates automatically with the latest protection from SophosLabs as frequently as every ten minutes.
- **Sophos Client Firewall** – stops day zero threats and hacker intrusion, locks down vulnerable computers, blocks worms, filters out unauthorized applications, and monitors application behavior.

### **Technology bytes**

**ActivePolicies™** lets you create a new security policy once and then deploy it across multiple groups simultaneously

**Centralized cleanup** lets you deal with malware and PUAs remotely from a central location, saving time and cost

**Checksumming** in Sophos Client Firewall prevents application hijacking and impersonation by spyware and other malware

**Cisco Network Admission Control (NAC)** integration helps deny access to network resources when anti-malware protection is not up to date

**Decision Caching™** provides performance-enhanced on-access scans by ensuring that only those files that have changed are scanned

**Genotype™ technology** provides proactive protection from new variants of virus and spam campaign families, even before specific, signature-based protection becomes available.

**Smart Views** enables you to instantly focus on vulnerable computers – including remote computers – so you can check compliance, update policies and clean up threats.

**Sophos AutoUpdate** technology offers failsafe updating and can throttle bandwidth when updating over low-speed network connections

**SQL** database support caters for the increased data storage requirements of even the largest network, while the built-in MSDE database will satisfy most organizations' requirements.

**Stealth mode** in the Sophos Client Firewall prevents computers responding and falling victim to hacker attacks.

### *Bandwidth control*

Having no control over when your anti-malware or firewall updates take place can place a significant burden on network – and therefore general IT – resource. Sophos Endpoint Security enables bandwidth throttling, giving you centralized management control of the timing of updating across the entire enterprise network.

### **Scalability**

While managing and controlling security software across small networks can be relatively simple, there can be significant problems in dealing with very large numbers of computers and groups of computers.

### *Managing very large networks*

Some solutions can, in theory, manage several thousand computers but in practice become unwieldy because of significant delays in communication between the management servers and the clients. By using intelligent rules to compare and aggregate messages at the client side, Enterprise Console significantly reduces the number of messages that need to be sent between client and server, letting you manage thousands of computers from a single console.

The use of message relays that allow computers on the network to act as relays to Enterprise Console, reduces the impact on the server even further and allows you to manage tens of thousands of computers, from a single console.

### *Managing stored information*

Sophos Endpoint Security also provides a choice of database solutions to help large organizations manage information effectively. It integrates with MSDE (Microsoft SQL Server Desktop Engine) as standard but you can also use SQL Server if you want to benefit from the enhanced functionality and greater scalability required for larger networks.

### **About Sophos**

Sophos is a world leader in integrated threat management solutions purpose-built for business, education and government. With 20 years' experience and consolidated anti-virus, anti-spyware and anti-spam expertise SophosLabs protects even the most complex networks from known and unknown threats. Our reliably engineered, easy-to-operate products protect over 35 million users in more than 150 countries from viruses, spyware, intrusions, unwanted applications, phishing, spam and email policy abuse. Round-the-clock vigilance has resulted in our increasingly rapid international growth, expanding user base and continuous profitability.

---

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

© Copyright 2006. Sophos Plc.

*All registered trademarks and copyrights are understood and recognized by Sophos.*

*No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.*

---

### **Integrated threat reporting**

On-demand, integrated, network-wide reporting is a key factor in helping you maintain security by letting you have full visibility of any infections and the status of protection across your network. Enterprise Console provides customizable, integrated charts, graphs and reports, created from virus alerts, which are processed, for instance, by threat, location and time.

### **Summary**

Managing security applications and enforcing policy across large and complex networks is a vital but expensive task. Many solutions designed to alleviate the problems often contribute to the complexity by burdening administrators with over-engineered products, heavy with features that will never be used. Sophos Endpoint Security has been designed expressly to reduce the complexity of managing security across the network desktops, laptops and servers, offering powerful, enforceable policy-based security management to give you comprehensive control and reduce your IT time, resource and cost.

### **Sources**

1 [www.sophos.com/pressoffice/news/articles/2006/06/toptenmay06.html](http://www.sophos.com/pressoffice/news/articles/2006/06/toptenmay06.html)

2 IBM press release, 14 Mar 2006, Armonk, NY. Quoted in [www.theregister.co.uk/2006/03/16/ibm\\_cybercrime\\_survey](http://www.theregister.co.uk/2006/03/16/ibm_cybercrime_survey)

3 2005 FBI Computer Crime Survey, quoted in [news.zdnet.co.uk/internet/security/0,39020375,39248195,00.htm](http://news.zdnet.co.uk/internet/security/0,39020375,39248195,00.htm)

*To find out more about Sophos and to evaluate our products, visit [www.sophos.com](http://www.sophos.com)*

**SOPHOS**  
WWW.SOPHOS.COM