

Security and control: The smarter approach to malware and compliance

The continuing evolution of malware threats combined with the demand for increasingly flexible working practices is a significant challenge to IT departments seeking to reduce help desk support and get better value for money from their investment in security. This paper looks at how organisations can benefit from a more integrated, policy-driven approach to protecting the network at all levels and controlling both user access and behaviour.

Security and control: The smarter approach to malware and compliance

The security challenge

IT departments are under continuous pressure to cut costs by reducing the load on the help desk, and to maximise their return on investment (ROI) in security and network management. At the same time, organisations and individuals alike expect greater flexibility in working practices – from mobile and remote connections to web access and instant messaging (IM). Now, however, it seems that productivity and network security are out of balance: the need to increase business productivity is driving greater network openness, which in turn is increasing the risk to network security.

The challenge for IT departments is to manage the demand for flexibility in a fast-changing environment. External pressures include the rapid growth in highly targeted threats and ever more stringent regulatory and audit compliance requirements; internally, help desk costs are escalating and the network is becoming increasingly heterogeneous, with multiple security layers, operating systems and device types.

Anti-virus and anti-spam solutions in particular have been seen as a drain on budgets and IT resources, particularly with the effort involved in troubleshooting and fixing the problems associated with implementing some solutions. To get better protection and improve ROI, the IT department needs to manage not only the obvious threats of malware and spam, but also users' access to the network – controlling how they connect, the computers and security they use, and what applications they run.

The continuing malware threat

Uncontrolled user behaviour is only one aspect of the threat landscape. The basic problem of rapid malware evolution has not gone away – it is getting faster and more complex, with more focused attacks. The need for multi-tier protection has never been greater, and organisations must safeguard the network from the gateway to the endpoint, including all points of access. Figure 1 shows the explosion of new threats detected by Sophos during 2006, totalling more than 40,000. The surge to over 7,600 in November – nearly four times as many as the same month in 2005 – can be attributed to the Stratio family of mass-mailing worms that had thousands of variants, increasing the chances of evading detection. Although this was a spike, the overall growth trend looks likely to continue.

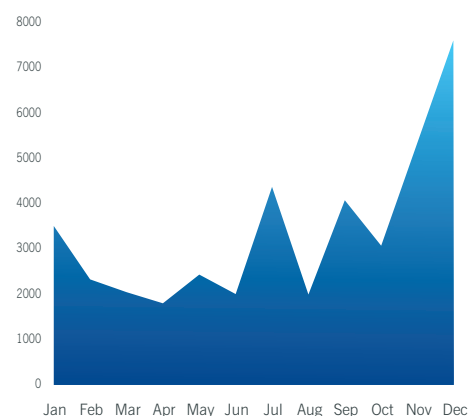


Figure 1: New malware threats each month in 2006

The threat from the web

The web is now perceived by administrators as the biggest threat to security and productivity.¹ Not only do some websites contain visibly undesirable content – many also harbour spyware and adware. There has been an explosive growth in web-based downloaders that deliver spyware: Figure 2 shows the percentage of email that contained spyware and the percentage of email that linked to websites from which spyware is downloaded, demonstrating a clear shift towards downloaders during 2006.

According to one survey, workers spend around 20% of their internet time on personal business or entertainment,² increasing the risk of inadvertently downloading malware – particularly spyware and Trojan downloaders. Unmanaged web browsing and personal web transactions in the workplace play into the hands of spammers and malware writers, exposing company email addresses to spam, harvesting and phishing. Analysis by SophosLabs in 2006 found that over 75% of all phishing emails targeted users of PayPal or eBay.³

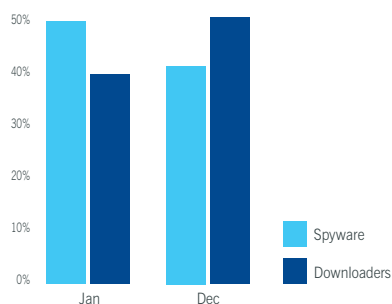


Figure 2: Spyware and downloaders in 2006

Organisations need an effective web security solution that must do more than just protect against all forms of malware – it must also eliminate potentially unwanted applications

(PUAs) and automatically prevent unauthorised web browsing by controlling access to known bad sites. Such a solution needs to be backed by continuous analysis of web traffic around the world, that evaluates the category, code and conduct of web pages.

The threat from email

Organisations should continue to be vigilant in order to safeguard their messaging systems by ensuring email gateway and groupware servers, and messaging databases such as Lotus Domino and Microsoft Exchange, are protected from email-borne threats. However, malicious code is being concealed and delivered in ever more devious ways, and the simple inclusion of malware in an email attachment is in decline – affecting just 1 in 337 emails in 2006, compared with 1 in 44 in 2005.

More spam now contains embedded images, increasing the chances of messages being read and reducing the detection rate by anti-spam filters that rely on the analysis of textual content. These larger files clog up mailboxes and can direct users to websites that deliver malware. For example, a spammed email in November 2006 that offered free explicit images and videos actually contained a weblink to the Psyme-DL Trojan, which has the potential to take control of the target computer. Modern spam can also mutate to avoid detection, and often uses zombie networks for mass delivery at almost no cost or risk of being blocklisted.

Truly effective protection is provided by solutions that can identify spam campaigns and malware families, rather than relying exclusively on specific spam and virus identities, and allow varied policies to be applied that meet the needs of different groups of users and compliance requirements.

The threat to endpoint computers

Specific protection against malware, hackers and unwanted applications at the desktop/laptop level is still essential, as highlighted by three high-profile email-aware worms that represented almost 40% of those circulating in November 2006: Stratio-Zip, Netsky-D, and MyDoom-O were all capable of running on Windows Vista. However, there is no longer a need to manage a variety of products to stop different threats. The best endpoint security products have moved way beyond simple protection from spyware, viruses, Trojans, worms, and PUAs. It is now possible to enforce policy from the same single central console to manage intrusion protection via a client firewall, block malicious code before it executes – giving the benefits of a Host Intrusion Protection System (HIPS) – and control access to unauthorised applications.

The enforcement of a broad-based endpoint security policy will itself provide significant protection against the worms and blended attacks that are among the most significant threats the enterprise faces today.

Scott Crawford, Enterprise Management Associates⁴

Unauthorised applications

Despite the potential business and productivity advantages of applications such as Voice over Internet Protocol (VoIP) and IM, they can be a distraction if used inappropriately. VoIP, which allows internet telephony, and distributed computing projects, such as SETI@Home that supports the search for extraterrestrial intelligence, also use up “spare” capacity – slowing the network and unnecessarily increasing the IT burden. Games and peer-to-peer (P2P) file sharing can also cause problems with legitimate corporate applications, adversely affecting both personal and IT productivity.

Emerging threats

To add to administrators’ woes, emerging threats include scareware and mobile malware. Scareware is software designed to dupe internet users into believing that their PC is infected or suffering from another security problem, and then encouraging them to purchase a “fully-working” version of the software that will disinfect their computer. Mobile malware that infects PDAs and smartphones remains a relatively small problem compared with the much larger amount of malware targeting Windows computers, but the threat is slowly becoming real and organisations should be prepared to implement an effective mobile security solution.

Controlling user behaviour

Both remote workers and guests on the network can compromise security if they connect devices that are not compliant with the organisation’s security policy for authorised applications, anti-virus software, and operating system patches. Security risks are substantially increased when employees connect remotely using wireless technology, or plug in PDAs and memory sticks to the network. Contractors and business partners can similarly threaten network security if they connect computers that do not comply with corporate policy, possibly running unauthorised applications and downloading files from the internet – all potentially without any intervention or control.

As users of all types continue to take advantage of new technology to work smarter and faster, organisations need to minimise the impact this can have on network security and IT resources by implementing policies that control not just which users have access to what parts of the network, but what they do while they are connected.

Network access control

Industry analysts are clear that implementing network access control (NAC) is essential to mitigate the potential risks posed by a more mobile and technology-driven workforce, and to

“It [Network Access Control] allows network managers to gain back control of their networks. Before this, it was like leaving the front door to the network wide open.”

Lawrence Orans, Gartner Inc⁵

combat regulatory pressures. True NAC includes reporting on the state of security compliance of computers connecting to the network, as well as enforcing policies that manage access at

various levels. NAC also allows organisations to enforce security policies that hitherto may have been enshrined only in company guidelines. By developing policies at a sufficiently granular level for different groups of users, productivity can be maintained and all points on the network protected automatically without increasing help desk load.

Furthermore, a software-based solution that retains and utilises existing security layers will not only minimise disruption to enterprise infrastructure and simplify implementation, it will also maximise effectiveness and ROI. Figure 3 demonstrates the ultimate benefit to network administrators of using integrated policies and a single agent to monitor and control both user behaviour and security.

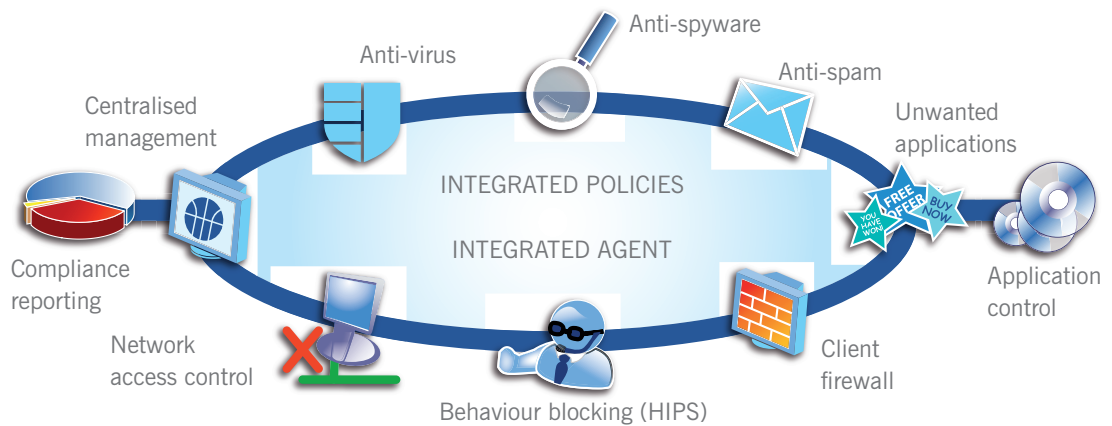


Figure 3: Integrated security and control

Summary

Conventional security tools offer protection from individual threat sources (e.g. anti-virus or web blocking), but do not cover unknown or non-compliant computers connecting to the network. As the network becomes increasingly open and threats increasingly diverse, security solutions have to change to control user access and behaviour, rather than just detecting and blocking threats. Organisations can maximise their

ROI in security and control by implementing a policy-driven solution that provides a simplified, integrated, and automated approach – with single agent, single control that protects against all threats and non-compliant behaviours. Application control, network access control and web access control will progressively become part of normal security management for organisations of all sizes – significantly reducing business risk and improving IT productivity at a lower overall cost.

The Sophos solution

Sophos protects at all levels – from gateway to endpoint.

Sophos Endpoint Security provides integrated protection against viruses, spyware, adware, PUAs and hackers, as well as preventing the use of unauthorised applications – all managed from a central console. It also protects against viruses and spyware on Windows Mobile devices.

Sophos NAC blocks unauthorised users, controls guest access, and ensures that legitimate users comply with the organisation's security policy – so administrators know who and what is connecting to the network.

Sophos gateway security integrates anti-virus, anti-spam, and policy enforcement at the email gateway, with a choice of highly flexible, scalable software solutions and managed email appliances. Sophos web appliances also protect the web gateway against malware and unwanted content – enabling safe and productive web browsing.

SophosLabs™ is a global network of threat research centres that analyses web and email traffic 24 hours a day to provide protection against known and unknown threats anywhere in the world, irrespective of origin.

To find out more about Sophos products and how to evaluate them, please visit www.sophos.com

Sources

- 1 Security threat report 2007. Sophos.
http://www.sophos.com/security/whitepapers/sophos-security-threats-2007_wsrus
- 2 Burstek releases 2005 internet usage study.
www.findarticles.com/p/articles/mi_m0EIN/is_2006_March_20/ai_n16109780
- 3 www.sophos.com/pressoffice/news/articles/2006/07/top-phishing-targets.html
- 4 Scott Crawford, Senior Analyst, Enterprise Management Associates, 2007
- 5 Lawrence Orans, Research Director, Gartner Inc

See also:

Instant Messaging, VoIP, P2P and games in the workplace: how to take back control
Sophos white paper. February 2007.

<http://www.sophos.com/security/whitepapers/sophos-app-control-wpus>

Maximizing security and performance for web browsing: the challenge for SMBs
Sophos white paper. October 2006.

<http://www.sophos.com/security/whitepapers/sophos-web-security-wpus>

About Sophos

Sophos is a world leader in IT security and control. We offer complete protection and control to business, education and government organisations – defending against known and unknown malware, spyware, intrusions, unwanted applications, spam, and policy abuse, and providing comprehensive network access control (NAC). Our reliably engineered, easy-to-operate products protect over 100 million users in more than 150 countries. With over 20 years' experience and a global network of threat analysis centres, the company responds rapidly to emerging threats and achieves the highest levels of customer satisfaction in the industry. Sophos is a global company with headquarters in Boston, MA., and Oxford, UK.

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

© Copyright 2007. 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.*

SOPHOS
WWW.SOPHOS.COM