

Maximizing security and performance for web browsing: the challenge for business

Spyware, viruses, worms, Trojans, adware, and other unwanted or unauthorized applications are not just an email problem. They also infiltrate networks via web browsing. This paper highlights the threats posed to organizations by malicious or inappropriate websites and the significant impact that employees' uncontrolled surfing of the web can have on productivity and network bandwidth. It defines the requirements for effective, manageable security that protects organizations from infection and legal risk, while also meeting end user demands for performance and accessibility.

Maximizing security and performance for web browsing: the challenge for business

The 21st century has seen a rapid acceleration in the evolution of new threats to organizations, both in the velocity of change and the increased malice of intent. Five years ago most threats were viruses and worms designed primarily to disrupt networks and crash computers. In the last year or so there has been a significant change in motivation – and therefore method – towards deliberate, focused attacks, designed specifically to make money for the perpetrators.

Workers spent around 20 percent of their internet time on personal business or for entertainment.²

Witness the recent escalation of spyware, which steals confidential information such as bank details and passwords, and can install programs that remotely control host computers. According to industry analyst IDC, spyware has climbed from fourth to second on a list of company security priorities, right behind email-borne viruses.¹ The impact of this is huge. Infected computers are used to channel corporate information outside the business, saturating the network with “phone home” traffic that reports back to the spyware’s author, and overwhelming the desktop infrastructure.

At the same time, productivity is being increasingly compromised by unmanaged web browsing. Employees are very often allowed to surf to wherever they want and download whatever they choose. According to internet management software firm Burstek, about 8 percent of the sites visited are assessed as posing potential legal liability to employers, such as sites that offer pornography or gambling.² Gartner Group has stated that, “over 70% of cyber attacks occur at the web (or website) application layer”³, and WhiteHat Security has found that 8 out of 10 websites currently have serious vulnerabilities.⁴

The exploitation of the web

Many organizations have no defenses beyond their network firewall for inspecting web traffic. Writers of malicious code capitalize on the often-overlooked and inadequate web security within corporate networks.

The objectives of malware writers are to steal confidential information or to establish botnets – networks of hijacked computers, or zombies, that are used to propagate spyware, viruses, spam and other threats. Infection is easy – malicious code can be downloaded and installed without any visible clue, simply by visiting a website. Potentially unwanted applications, such as adware and peer-to-peer programs, particularly popular and dangerous tools of the trade, are often used to install malware surreptitiously.

“Gartner estimates that fewer than “10-15 percent of enterprises have deployed web-based anti-virus scanning”.”³

By far the most exploited web protocol is HTTP – because it is the main protocol on the world wide web that enables web browsing, i.e. that enables computers to link to websites. HTTPS uses authentication certificates to validate web sites, erecting a considerable barrier to exploitation and greatly reducing the risk of infection. Similarly, the much less popular FTP protocol is a far less effective method of malware propagation, due in large part to its more limited use.

The diversity of threat

These web-based threats pose significant security and productivity challenges, including system infection, legal liability and breaches in corporate or regulatory compliance rules. Table 1 shows the different types of threat and how they can compromise an organization.

Threat vector	Threat type	Example	Risk
Conduct	Unwanted applications Malicious websites	Popup ads Browser toolbars Phishing	Productivity loss Information leakage
Category	Inappropriate content	Adult content	Legal liability
Code	Active content Spyware Viruses Worms Trojans	Malicious ActiveX Drive-by installers Browser helper objects	Client and network instability Information theft Bandwidth consumption

Table 1: Web-based threats

Theoretically, the threats can be classified into three types:

- **Conduct** – e.g. malicious websites and unwanted applications
- **Category** – inappropriate content
- **Code** – malicious code such as spyware and viruses

This expanding diversity and complexity make it increasingly difficult to enforce acceptable use of the internet without introducing significant administrative effort.

Inappropriate websites are readily identified through URL filtering services (see below). Malicious code, on the other hand, is much trickier to identify. Drive-by installers are clearly malicious, but programs such as browser help objects (BHOs) might have a legitimate purpose or might be malicious. Drive-by installers can secretly open a backdoor through the browser and install a keylogger that records confidential information, such as online banking account numbers and passwords, and transmits the information invisibly. Drive-by downloads may happen when a user visits a website, views an email message or clicks on a deceptive popup window in the mistaken belief that, for instance, it is an error report from his own PC or that it is an innocuous advertisement popup; in the case of popup ads, the “supplier” may claim that the user “consented” to the download though he was completely unaware to have initiated a malicious software download.

A secure web browsing solution should provide a unified policy framework for blocking dangerous content, scanning potentially dangerous content and optimizing the performance and availability of trusted content.

BHOs are plug-ins for the Microsoft Internet Explorer web browser and run automatically every time the browser is launched. Generally, a BHO is placed on the system by another software program and is typically installed as a toolbar accessory. It can track usage data and collect any information displayed on the internet. Malicious BHOs are mainly installed by browser hijackers (Trojans that alter the browser settings) using ActiveX controls. They can also redirect browsers to malicious websites, and share data with unknown third parties.

Similar confusion can be caused by conduct that might appear to be legitimate but might in fact be malicious. This is how phishing works. For example, a perfectly clean-looking email takes users to a website that looks just like a real banking site. However, the website is actually fake and is used to gather confidential details from the unsuspecting user.

Defense strategies for the expanding threat

The desktop is traditionally seen as the main battlefield in the fight against spyware, viruses and other malware. However, relying on desktop defenses puts a heavy load on local resources and ignores the impact that these threats can have on network bandwidth if desktop defenses fail. For optimal security, businesses should install defenses at both the gateway and the endpoint, stopping threats before they enter the network and scanning desktops for threats that enter via other means (visiting laptops, PDAs, USB drives, etc). This approach has proven highly effective for email-based threats, and is equally effective for threats circulating on the web.

Current web security technology at the gateway

To be effective, a web security solution must address both the threats that users will encounter, and the need for fast, efficient web browsing. Essentially, the solution should provide a unified policy framework for blocking dangerous content, scanning potentially dangerous and unwanted content and optimizing the performance and availability of trusted content. There are currently two predominant approaches to web security: URL filtering and anti-virus scanning.

URL filtering

URL filtering is carried out where productivity is the overriding concern. It relies on complex and resource-intensive categorizing of websites according to their content, and then providing black-and-white policy rules for each category, controlling where employees go on the web and blocking or limiting their access to undesirable content. While the solution itself is high-performance in terms of speed, there are considerable security risks since content from an allowed site would not get scanned. In an attempt to achieve tighter security, administrators either end up over-blocking content, generating high false positives and requiring constant, management-intensive tweaking of allow lists, or give up and take their chances with security. According to Gartner, incumbent URL filtering vendors “have considerable gaps to fill in their strategy and product road maps before they can meet enterprise requirements for broader gateway malicious code protection”.³

“Web security needs to achieve optimal protection without negatively impacting the end-user experience or significantly increasing administrative effort.”

Anti-virus scanning

The other approach, anti-virus scanning, is based on scanning of web content regardless of site category and is positioned as a better security solution than URL filtering. While this is undoubtedly true, anti-virus scanning solutions tend to lead to over-scanning of content, slowing network performance and negatively impacting the end-user experience. Like the URL filtering solutions, they require aggressive, time-consuming management.

The business challenge

Both solution types have merit, but for IT administrators, it means either trading off performance against security and leaving potential holes in their network defenses, or managing separate solutions in an attempt to achieve greater overall protection.

As a result of the inadequacies and complications outlined above, companies often do not deploy gateway solutions, leaving the endpoint to bear the brunt of protection. Unfortunately, this is an inadequate approach; IDC concludes that 75% of corporate desktops are infected with some type of spyware.¹ The results are higher infection rates, greater bandwidth consumption, more expensive clean-up efforts and a growing concern that the scale of the problem will rapidly overwhelm companies' existing web infrastructure.

A checklist for effective web security

What can businesses do to block this increasingly exploited vulnerability? And what should they be looking to implement?

As discussed above, a robust, useable web security solution should comprise:

- a URL filter to enforce an acceptable use policy
- a fast content scanner to protect against threats – like spyware, viruses, exploits, malicious code, and unwanted applications
- a policy framework that makes it easy to combine URL filtering and scanning for threats.

There is also a need for easy administrative tools for policy management and reporting, along with a confidence that the vendor will deploy up-to-date protection against any new threat instantly and reliably.

The current patchwork of solutions that is available has proven extremely difficult to implement and coordinate. Companies might have deployed a gateway anti-virus scanner or a URL filter, but, working independently of each other, neither is proving effective at meeting the range of requirements listed above.² Gateway anti-virus misses many of the new types of threats (e.g. browser helper objects and drive-by downloads), and URL filtering technology typically lacks adequate coverage of security-related threats.

Maintaining several separate solutions for web security not only introduces the need to tune multiple components; it also adds scanning latency and generally increases the total cost of ownership through an increase in acquisition and deployment costs and overall administrative burden.

Conclusion

Web traffic is being increasingly exploited for commercial gain, resulting in the loss of confidential information and the degradation of corporate

networks. As a core business enabler, web browsing requires as much security and protection as the email gateway and endpoint. Companies looking to protect themselves from this growing vulnerability need a solution that combines powerful URL filtering and scanning capabilities with low-impact, effective administration. At the same time end-user expectations and requirements for speed and efficiency have to be met. Any solution which fails to meet all these demands for security and performance will ultimately fail the organization. ◆

The Sophos solution

Sophos's broad visibility into the threat environment and our experience and expertise mean that our Web Security Appliances provide safe and efficient web browsing, with rapid, up-to-date protection and scanning for the full spectrum of web-based threats. Sophos Web Security Appliances offer integrated, enterprise-grade protection delivered on a managed hardware platform. Like all our products, they are powered by SophosLabs™ and backed by round-the-clock, global support. Scanning all HTTP and FTP via HTTP traffic, validating HTTPS certificates, blocking unwanted URLs and incorporating a built-in proxy and cache, Sophos Web Security Appliances provide a comprehensive solution that is easy to deploy and manage.

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

Sources

- 1 Worldwide Secure Content Management 2005-2009 forecast update and 2004 vendor shares: spyware, spam, and malicious code continue to wreak havoc. IDC. September 2005
- 2 Burstek releases 2005 internet usage study.
www.findarticles.com/p/articles/mi_m0EIN/is_2006_March_20/ai_n16109780
- 3 Marketscope for URL filtering 2006. Lawrence Orans and Arabella Hallawell. Gartner, Inc. March 2006
- 4 WhiteHat Security Risk report. April 2007.
<http://www.whitehatsec.com/home/resources/wp/whitepapers.html>

See also:

Spyware – the hidden threat to business security.
Sophos white paper. October 2006.
www.sophos.com/sophos/docs/eng/papers/sophos-spyware-wpus.pdf

About Sophos

Sophos is a world leader in IT security and control. We offer complete protection and control to business, education and government organizations – 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 centers, 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