

Astaro OrangePaper

An All-in-One Approach to Web Security Benefits for the Small-to Mid-sized Business

Authors:



Udo Kerst
Sr. Product Manager



Eric Bégoc
Product Manager

Date: 2008-04-10

Content	Page
Executive Summary	2
Introduction	2
Change: The One Indisputable Constant	3
Exploiting Server and Browser Vulnerabilities	3
The new threats of Skype, IM and P2P applications	5
Communication Issues for Staff Members	5
The Costs of Ineffective Web Security	7
Benefits of an Appliance Approach	8
Centralizing Security and Management Features	10
Security Costs and Resources	12
Benefits of an All-in-One Solution	13
Conclusion	14

Executive Summary

Granting web access to employees poses challenges to IT administrators in a number of ways and introduces unique security risks. Even as companies have perfected their security techniques to guard against network intrusion, hackers and data thieves have devised new ways to deliver payloads of malware—luring network users to pull in the infected packages during everyday web transactions. Unrestricted web access can also drain network resources and open unwanted communication channels through instant messaging and peer-to-peer software exchanges. To combat the problems associated with web access, many small- to mid-sized businesses (SMBs) are recognizing the advantages of an all-in-one solution as implemented in a secure web gateway.

Introduction

Nothing stands still in cyberspace. From the time the first packet made the transit from one lab to another, the infrastructure that fostered the Internet and gave birth to the World Wide Web has been undergoing steady, progressive change. Such is also the case for web security. IT administrators tasked with giving their organizations the communication benefits of a global network, while countering a steady succession of evolving threats, know that the phrase *eternal vigilance* is more than empty rhetoric. Threats are countered. New threats arise. Small- to mid-sized businesses in particular may lack the internal expertise to identify and cope with the latest concerns in the rapidly changing security landscape.

Adapting to the changing nature of security threats requires first identifying the paths of greatest risk, the types of transactions prone to theft or exposure and the potential mechanisms by which hackers or intruders might gain access to information. An equally relevant concern is identifying and preventing the activities by which insiders might abuse network resources, access information that is legally prohibited by age or policy, or inadvertently expose other network users to circulating viruses or malware. The effectiveness of a web security solution can be measured by success in accomplishing these goals in a manner that does not disrupt daily business operations or place an undue burden on the organization's staff members, partners, or customer base.

There is a wide range of approaches to web security, from strengthening end points using client-based software to fortifying the firewall by adding additional gateway functionality to seal out emerging risks. This paper describes the advantages of a centrally managed approach enabled by an all-in-one security gateway that can also enhance and complement existing measures. Using tools developed to counter today's most critical web access issues and applying them consistently across the organization offers many advantages over client-based solutions that may not be uniformly deployed or may be circumvented by users. This paper also discusses the benefits of consolidating web security mechanisms in an easily deployable hardware appliance or a convenient, self-contained virtual appliance (running under VMware). The deployment and maintenance of web security measures can in itself be a costly, resource-draining activity if implemented in a piecemeal, uncoordinated manner.

Change: The One Indisputable Constant

*Data thieves and hackers
are inventive*

The Internet has become vital to a broadening spectrum of business operations, but with the increased growth of worldwide networking, businesses face an expanding range of threats and vulnerabilities that, if left unchecked, can negate the advantages of an open business model. Anyone who has been involved in IT management or administration has undoubtedly noted that the technologies designed to counter network vulnerabilities are, by necessity, constantly changing to cope with the inventiveness of data thieves and hackers attempting to breach security measures. The viability of the network itself also faces internal risks, from the downloading of software that contains viruses or worms to the network slowdowns that result from excessive traffic associated with file-sharing sites and peer-to-peer exchanges.

Exploiting Server and Browser Vulnerabilities

One shift in hacker techniques that has been gaining more attention is "drive-by malware", a practice by which network users infect the network with their browsing activities. This tactic emerged when network security measures became more sophisticated at repelling denial-of-service attacks and similar techniques aimed at breaching a network through brute force. Now, hackers are increasingly focused on luring network users into performing activities, such as clicking on a link to access an e-card or simply navigating to a malicious web page that contains code designed to distribute worms, viruses, spyware, or malware.

"The magnitude of drive-by malware is significant"

Network World reported¹ on a 2007 Google survey, intended to identify the scope of the drive-by download threat, which revealed that many seemingly benign sites—including sites focusing on health care, the arts, entertainment, and social networking—had become the focus of malware distribution. Adult sites were also represented in a high percentage of instances, but the more chilling revelation was the high incidence of seemingly innocuous sites that had been subverted by hackers to become nodes for malware distribution. A method for accomplishing this is to exploit server security vulnerabilities, and the Google study also pointed out that 38.1 percent of Apache servers and 39.9 percent of servers incorporating PHP scripting support consisted of versions with known security flaws. The conclusion of this study noted that the magnitude of drive-by malware is *significant*.

Security analyst Mike Montecillo of the consulting firm Enterprise Management Associates (www.enterprisemanagement.com) also points a finger at the web browser as a primary vulnerability² in the security strategies of many organizations. Most companies, he believes, are more interested in providing employees the benefits of full browser functionality and do not pay enough attention to the corresponding risks that can be exploited through common applications, such as Flash, ActiveX, QuickTime, Java, and JavaScript. Each one of these browser components represents a channel that a hacker could potentially exploit to unleash malware on the network.

"Each and every Web site is a potential host for malicious code as hackers could potentially exploit even the most legitimate site as a means of hacking thousands of computers without the fear of reprisal," said Montecillo. "There is no end in sight to the number of malicious Web sites and browser-related vulnerabilities that can end up causing enterprise-wide breaches and incidents."

For this reason, Montecillo noted, many IT security professionals are increasingly relying on web browser protection through robust URL filtering solutions.

¹ "Google says the scope of drive-by malware is 'significant'"; <http://www.networkworld.com/newsletters/techexec/2008/0303techexec1.html>

² "EMA Points to Web Browsers as Emerging IT Security Threat"; <http://www.mywire.com/pubs/PRNewswire/2008/02/26/5764914>

By blocking sites that don't have any relation to everyday business operations, the chances of a browser-based security breach are diminished. Beyond filtering, Montecillo also recommends anti-malware software and automated code filtering to further strengthen security protections associated with browser activity.

The new threats of Skype, IM and P2P applications

Controlling Skype usage is a major headache for every administrator

Another emerging problem stems from the proliferation of instant messaging (IM) and peer-to-peer (P2P) software applications. Fraudsters using security holes in Voice-over-IP communication tools, such as Skype, sometimes create problems with phony chargebacks and compromised business practices. These kinds of communications among a company's employees can be difficult or impossible to regulate without some form of central control over web traffic.

Users often feel they have the right to install any applications they want on their work computers, regardless of company policies or practices. While some IM/P2P applications can provide useful business value to a company, IT administrators need a means to regulate and control user access in a centrally managed way. Applications that are deemed off limits should be blocked, and applications that offer business value and are used for legitimate purposes by staff members should be freely accessible.

For example, many companies take advantage of BitTorrent for exchange of large files or software downloads. In such a case, administrators need a mechanism to allow employees legitimate access to BitTorrent, while blocking out other applications that are deemed risky or inappropriate.

Communication Issues for Staff Members

Balanced use of available network bandwidth – not only an enterprise theme

Web access for staff members is a mixed blessing for small- to mid-sized companies. The same channel through which employees can perform market research, investigate trends, communicate globally with partners and customers, and generate sales leads can be a potential network-clogging traffic generator. Employees who engage in activities that result in large volumes of data being funneled through network resources can disrupt operations with higher priorities. While social and business networking, Voice-over-IP, streaming video access, peer-to-peer file sharing, and similar kinds of web access can have legitimate business applications, if unrestricted they can usurp network resources best devoted to other uses.

The popularity of these types of web applications has risen substantially, presenting one more challenge to IT administrators whose ultimate responsibility is the balanced use of available network bandwidth. In the past, central mechanisms for throttling back bandwidth for less-important applications was an area of functionality primarily available to enterprise-scale organizations. Newer solutions, however, appropriate to small- and mid-sized businesses, are addressing this requirement in response to the boosts in network traffic that can be directly attributed to certain kinds of web applications (which often have both business and personal uses).

An independent study conducted in 2007 by Dynamic Markets³ offered some indications of the extent to which employees contribute to security risks. The survey included 750 IT managers and employees in small- to mid-sized businesses across Europe:

- Despite the fact that employees admitted spending as much as two hours a day on web sites that were non-work related, only 47 percent of the IT managers had instigated web filtering to provide protection against web-based threats.
- Close to one-third of the employees also confessed to frequently accessing potential high-risk sites, including those that provide peer-to-peer file exchanges and offer free software downloads. These employees overwhelmingly (66 percent) believed that the company had provisions in place to guard against security threats arising from the Internet.
- Although a minority of IT managers at these companies (17 percent) believed that SMBs need less stringent security than large enterprises (because of minimal risk levels), a full 71 percent thought that the size of the company does not matter—SMBs need the same level of protection as large firms.

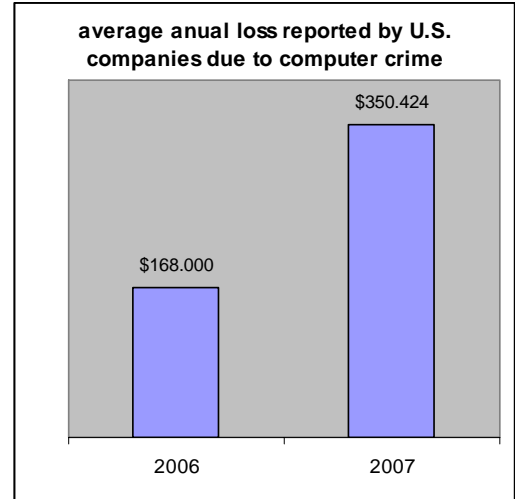
³ "European SMB Employees Surf for Two Hours a Day, Yet IT Managers Pass The Buck on Security"; <http://newsblaze.com/story/2007082301213200002.we/topstory.html>

The Costs of Ineffective Web Security

Viruses are no longer the source of the greatest financial loss

A 2007 survey by the Computer Security Institute⁴ quantified the financial losses of U.S. companies in the preceding year and determined that losses have risen sharply, from an average of \$168,000 per firm in 2006 to \$350,424 in 2007. One of the most significant causes of loss was system penetration by outsiders. Close to one-fifth of the survey respondents indicated that they had suffered a malware attack directed at

their organization. Another significant area of loss involved insider abuse of network access or e-mail. Incidents involving trafficking in pornography or downloading pirated software became more prevalent as a security issue (representing 59 percent of the reported problems) compared with virus problems (tallied at 52 percent).



In response to these results, Robert Richardson, the director of the Computer Security Institute said, "At a period when experts throughout the industry have been discussing with concern the growing sophistication and stealth of cyber attacks, here we have a couple hundred respondents saying they lost significantly more money last year. There's a strong suggestion in this year's results that mounting threats are beginning to materialize as mounting losses."

A full version of the report is available at: www.gocsi.com.

⁴ "2007 CSI Computer Crime and Security Survey Shows Average Cyber-Losses Jumping After Five-Year Decline"; <http://www.gocsi.com/press/20070913.jhtml>

Benefits of an Appliance Approach

Small- to mid-sized businesses gain the most efficiency in their processes when they are able to consolidate and streamline functionality in key areas—such as web security—in a manner that permits straightforward management, easy oversight, minimal day-to-day maintenance, and simple upgrading. The rising popularity of appliance-based approaches to network security is a testament to the fact that this model successfully meets the necessary criteria.

A security appliance can be constructed and deployed in any one of three possible packages:

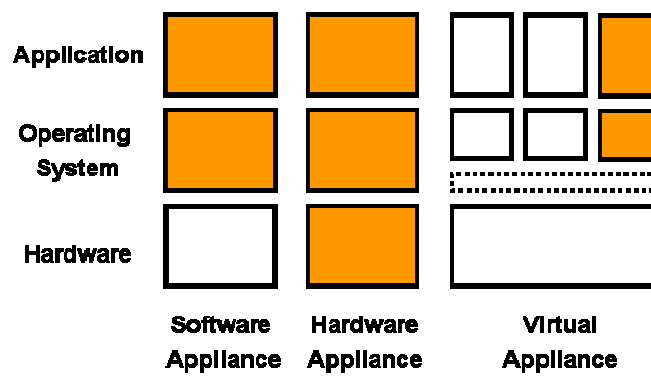


Fig. 1: *Security Appliance Deployment Models*

- **Software appliance:** The functionality of the security solution is obtained through a single software image, bundled with the operating system and all requisite applications, for quick installation on a dedicated server or PC. This results in a much faster and easier deployment than is typical for software applications, which require a separate pre-installed operating system.
- **Hardware appliance:** A hardware device with pre-installed operating system and application software is added to the network and quickly configured for operation. This often represents the quickest method to integrate the capabilities of a security solution onto a network with minimal instances of deployment problems or incompatibilities.
- **Virtual appliance:** A virtual appliance is a combination of all the required software applications, including the operating system, pre-installed, pre-configured, and designed to be run concurrently with other virtual appliances in a virtual environment, such as is provided by VMware.

This packaged approach to delivering security solutions benefits from the strength of consolidating the necessary protection at a key point of vulnerability. For example, Astaro Web Gateway provides a divide between the free-flowing information on the Internet and the network infrastructure inside the company's firewall. Working in combination with the firewall, this security gateway can filter content by URL, oversee and control the use of web applications, prioritize bandwidth use by application, and protect against malware reaching the internal network.

Benefits of Virtualization

Virtualization has become a popular way to take full advantage of available server resources, which are generally under-utilized in most companies. Because of the plug-in, packaged nature of a virtual appliance, installation and configuration issues are typically minimal and setup is often as easy as with a hardware appliance.

Another benefit of deploying a virtual appliance is the energy and cost savings associated with virtualization. Available server resources are used much more effectively—much closer to 100 percent than can be achieved when discrete servers running different operating systems and environments are used in the server room. This results in substantially reduced energy costs (since fewer servers are needed), allowing companies to reduce cooling requirements in the server room. As Green IT measures are more universally implemented to cut energy use and help combat global warming, products such as the Astaro Web Gateway virtual appliance contribute to reducing the carbon footprint associated with business computing⁵.

⁵ Astaro is also member of the Green Grid, a global consortium dedicated to advancing energy efficiency in data centers and business computing ecosystems.

Centralizing Security and Management Features

As illustrated by the examples and data points in this paper, IT administrators often lack the tools and technology to perform oversight of web access transactions throughout the organization—risking the opening of numerous additional threat scenarios and unwanted communication channels that breach normal firewall protection. While solutions that install on client computing devices can provide a measure of protection, these solutions are difficult to track and administer. Across an organization that may contain large numbers of individual computers, or even a relatively small number, an administrator trying to enforce installation of the latest patches or software updates to ensure current security coverage faces an almost impossible, ongoing struggle. Employees are known to sometimes circumvent existing protection by disabling security software or ignoring administrative requests to regularly download patches and updates.

The best way to counter the diverse range of threats associated with web access is to consolidate the necessary functionality in a gateway-based, all-in-one solution that works in concert with the existing firewall. The IT administrator immediately gains oversight and control of the web traffic, inbound and outbound, and can selectively install filters, monitors, and throttling controls to regulate traffic in a safe, orderly, system-wide manner.

The central, all-in-one web security solution by its nature also satisfies another concern of network administrators: providing a clear, comprehensive method for ensuring compliance with regulatory mandates that restrict access to certain types of content. For example, educational institutions may be required by law to block adult content from children who are using the web. A web security solution with filtering controls can comply with prevailing local and federal laws by effectively eliminating access to sites that are deemed inappropriate.

However, in order to prove the effectiveness of installed controls, web security solutions need to provide extensive logging and reporting capabilities as depicted in the following diagram.

Web Usage		Blocked Usage					
Top Blocked Categories		Results: 1-18 of 18					
Last 30 days		Update					
50							
Top	Category	Users	%	Domains	%	Requests	%
1	General News / Newspapers / Magazines	3	7.89	35	10.61	5 862	62.78
2	Newsgroups / Bulletin Boards / General Discussion Sites	2	5.26	42	12.73	867	9.29
3	Uncategorized	3	7.89	119	36.06	623	6.67
4	IT Security / IT Information	4	10.53	46	13.94	497	5.32
5	Online Shopping	3	7.89	21	6.36	468	5.01
6	Software / Hardware / Distributors	3	7.89	20	6.06	344	3.68
7	Financial Services / Investment / Insurance	1	2.63	8	2.42	286	3.06
8	Search Engines / Web Catalogs / Portals	4	10.53	10	3.03	120	1.29
9	Auctions / Classified Ads	3	7.89	13	3.94	120	1.29
10	Communication Services	3	7.89	6	1.82	117	1.25
11	Categorization Failed	1	2.63	2	0.61	10	0.11
12	Job Search	2	5.26	1	0.30	7	0.07
13	Gambling	1	2.63	2	0.61	4	0.04
14	Political Extreme / Hate / Discrimination	1	2.63	1	0.30	3	0.03
15	Computer Games	1	2.63	1	0.30	3	0.03
16	Warez / Hacking / Illegal Software	1	2.63	1	0.30	2	0.02
17	Chat	1	2.63	1	0.30	2	0.02
18	Erotic / Sex	1	2.63	1	0.30	2	0.02
		Totals				9 337	

Fig. 2: Astaro Web Gateway URL Filtering Report

The June 2007 Gartner research report, "Magic Quadrant for Secure Web Gateway 2007⁶", stated:

"A Secure Web Gateway (see "Introducing the Secure Web Gateway") is a solution that filters unwanted software/malware from user-initiated Web/Internet traffic and enforces corporate and regulatory policy compliance. To achieve this goal, SWGs must, at a minimum, include URL filtering, malicious-code detection and filtering, and application controls for popular Web-based applications, such as instant messaging (IM) and Skype."

According to Gartner:

"No product completely satisfies all functional categories in a single product, and buyers will definitely need to make some sacrifices."

⁶ Firstbrook, Peter, Lawrence Orans, and Araqbella Hallawell. "Magic Quadrant for Secure Web Gateway", Gartner, June 2007.

During product development, Astaro software engineers focused on designing a comprehensive, well-rounded solution to address the needs of the small- to mid-sized business. The design specifications for Astaro Web Gateway included these primary objectives:

- Include mechanisms to block malware from infecting the network.
- Regulate the use of applications that involve file-sharing or user communication.
- Restrict Internet access to approved uses for both business and legal reasons.
- Ensure that bandwidth for key business applications is given priority over more casual network usage.

This functionality, incorporated in the version of Astaro Web Gateway released in early 2008, ensures that companies can meet web security requirements effectively in a single, all-in-one solution.

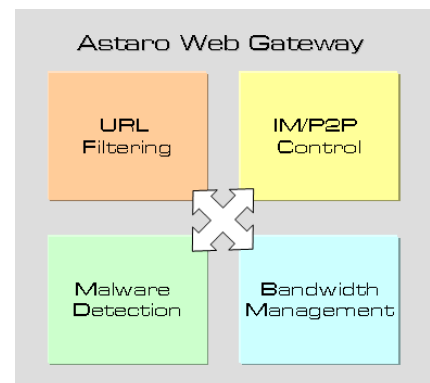


Fig.3: Astaro Web Gateway

Security Costs and Resources

Unlike their larger business brethren, small- to mid-sized businesses often lack an extensive internal staff devoted to security issues. The same personnel tasked with responding to support issues from end users often have to evaluate and deploy the security solutions used by the company, as well as maintain the security hardware and software in place. Complicated security measures that require individual monitoring of user configurations or determining whether current patches have been installed for browsers, anti-virus software, and personal firewalls are difficult to monitor and keep up to date. While these kinds of protections are useful, and in many cases necessary, it is equally important to have an effective first line of defense, a means of taking the traditional firewall protection and bolstering it through additional tools that provide comprehensive web security.

Astaro developed the Astaro Web Gateway with small- to mid-sized businesses in mind—companies that need comprehensive web security measures to enhance their existing protections but that may not have the expertise or staff resources to install and monitor a patchwork of individual point solutions. Even those companies that have sufficient IT personnel may find that an all-in-one package, deployed as a single-solution appliance, better meets their requirements and satisfies the need to strengthen security without compromising the benefits of transacting business across the Internet.

By concentrating much of the design effort on usability, the user interface of Astaro Web Gateway vastly simplifies the administrative functions and provides a clear, current view of the security status and traffic settings. Administrators can easily assess the security provisions in place, enable the settings that lock down or filter out the most dangerous web access threats, and oversee the entire web security situation from one central point.

Benefits of an All-in-One Solution

IT administrators who implement an all-in-one web security solution gain distinct advantages over more costly and complex single-function web-filtering solutions. Having a single point of control over web access and usage achieves a number of benefits:

- **Effective malware protection:** the threat vectors introduced by malware, spyware, viruses, worms, and other threats can be mitigated through a robust first line of defense.
- **Reduced costs:** a centrally managed appliance for web security reduces IT management tasks and simplifies routine maintenance and upgrades.
- **Legal compliance:** companies can block access to inappropriate or illegal web content to comply with internal policies and legal mandates.
- **Increased productivity:** employees won't be surfing non-business sites during business hours, which also lowers the risk of infection from malware obtained through questionable sites. Other non-productive activities, such as taxing the network with inappropriate bit streaming, can also be eliminated.

Astaro Web Gateway was designed with these tenets in mind to meet the requirements of IT administrators in small- to mid-sized organizations.

Conclusion

To cope with emerging categories of security threats—such as web-based attacks that exploit vulnerabilities at both the user and the server level—IT administrators need easily deployable solutions that offer comprehensive protection. Because the appropriate level of expertise and the IT security resources may not be available in a typical small- to mid-sized business, those organizations will be especially attracted to an appliance-based web security gateway that provides the means to implement cost-effective, easy-to-deploy protections and network-use controls in a centrally managed solution. This approach enhances traditional security measures while affording protection against contemporary and emerging threats.

An all-in-one approach to web security offers simplified management, more consistent security across the network, more opportunities for precisely controlling web application usage within a company, and a reduction in exposure to emerging web-based security threats.

Contact



Europe, Middle East, Africa

Astaro AG
Amalienbadstrasse 36
76227 Karlsruhe Germany
T: +49 721 255 16 0
F: +49 721 255 16 200
emea@astaro.com

www.astaro.com

The Americas

Astaro Corporation
3 New England Executive
Park
Burlington, MA 01803
USA
T: +1 781 345 5000
F: +1 781 345 5100
americas@astaro.com

Asia Pacific Region

Astaro K.K.
12/F Ark Mori Building
1-12-32 Akasaka Minato-ku
Tokio 107-6012, Japan
T: +81 3 4360 8350
apac@astaro.com

This document may not be copied or distributed by any means, electronically or mechanically, in whole or in part, for any reason, without the express written permission of Astaro AG.

© 2008 Astaro AG. All rights reserved. Astaro Security Gateway, Astaro Command Center and WebAdmin are trademarks of Astaro AG. All further trademarks are the property of their respective owners. No guarantee is given for the correctness of the information contained in this document.