



A Websense® White Paper

Security Appliance Market

Abstract: *The security appliance market, which includes everything from firewalls and virtual private networks (VPNs) to all-in-one security appliances, is expected to grow at a tremendous rate over the next three to five years. As the enterprise security market continues to mature, consolidation of traditional stand-alone products and services—including Internet content filtering—into various appliance forms is also expected to evolve in lockstep. This natural progression will enable companies to deploy Internet content filtering and other security products in a variety of ways, including stand-alone appliances, all-in-one appliances, and hardware “blades,” as well as straightforward software solutions. This paper examines recent industry trends and summarizes Websense, Inc.’s strategies for capitalizing on the emerging security appliance market. As the leading worldwide provider of employee Internet management (EIM) solutions, Websense is well positioned for continued growth and success in the security appliance market through its existing technology platforms, alliances, and channel partners.*



Table of Contents:

Executive Summary	3
The Security Appliance Market	3
• Evolving Customer Requirements.....	3
• Market Size and Growth Rate.....	5
• Platform Types and Key Players.....	6
• Looking Ahead.....	6
Websense EIM Solution.....	7
The Websense Appliance Strategy.....	8
• Stand-Alone Appliances.....	8
• Integrated/All-in-One Appliances.....	8
• Blade Appliances.....	8
• Software/ CD Appliances.....	8
Conclusion.....	8
About Websense, Inc.....	9
Appendix A: Websense Best of Breed Partners.....	9



Executive Summary

The enterprise security market continues to expand in response to new threats and customer demands. Companies are looking at evolving security solutions, as well as new, more secure platforms on which to leverage these solutions. The advent of the “security appliance” is rooted in organizations’ interest to benefit from a “hardened” appliance- implying it is less vulnerable to attacks- as well as realize additional benefits such as deploying multiple solutions on the same appliance, working with the same vendor across multiple solutions, or reducing total cost of ownership.

Websense, the world’s leading provider of Employee Internet Management (EIM) solutions, is well-poised to leverage the opportunities presented by the evolving security appliance market. Its award-winning EIM solution, Websense Enterprise®, is the *only* solution that provides multilayered filtering at multiple points within an enterprise, including on the network, gateway, and desktop to provide protection against emerging threats. Websense has earned its leadership position because of the superiority of its product offerings, the significant customer value offered through its solutions, and its unique alliances with a comprehensive network of technology partners.

With some 30 integrations available (see Appendix A), Websense has a proven track record of securing and cultivating technology partnerships with the industry’s leading networking and security platform vendors. Further, because of this breadth of integration options, Websense Enterprise can be successfully deployed on the widest range of networking and security infrastructure and edge devices found in enterprises around the world. Websense is addressing the security appliance market with exactly the same commitment to quality and technical expertise— extending existing relationships and building new ones to maintain a dominant integration position in appliances just as has been done with open platform servers.

As Websense’s technology partners move to introduce security appliances with EIM solutions, and as customers demand best of breed solutions, with its premier technology offering and key hardware platform partnerships, Websense is best positioned to become the EIM solution provider of choice in the security appliance market.

As the security appliance market evolves, customers will balance their own environment-specific requirements before deploying software-based, appliance-based, or even hybrid (both software and appliance) solutions in their enterprise. Whichever deployment options companies elect, Websense Enterprise will be included in all appliances offering best of breed EIM capabilities.

The Security Appliance Market

The enterprise security market has grown tremendously over the last several years and continues to evolve at a fast pace, in response to emerging threats and vulnerabilities as well as demanding customer requirements. The number of security offerings has expanded from the original perimeter security application—the firewall—to numerous others, including virtual private networks (VPNs), intrusion detection systems (IDS), anti-virus (AV) applications, e-mail/spam gateways, and employee Internet management (EIM) solutions. To date, most enterprises have deployed these applications as point solutions: standalone servers or appliances dedicated to individual security applications. However, the industry is already observing changes in the ways enterprises install and manage their security environments.

Evolving Customer Requirements

While many organizations continue to appreciate the flexibility of software-based solutions and the scalability of stand-alone devices, others are gravitating toward hardware-based solutions and all-in-one appliances. For example, large enterprises and data centers generally require more robust feature support for managing complex environments and higher performance due to greater network traffic. As a result, software or stand-alone solutions are more acceptable. On the other hand, distributed or remote enterprises (retail banks, fast-food chains, and corporate home offices, for example) are often willing to sacrifice sophisticated security policy enforcement for an easier, lower-cost, and more easily deployed option—making an all-in-one security appliance more desirable.



Evolving customer requirements that are driving the market towards more appliance-based solutions include:

Control Total Cost of Ownership (TCO)—Total cost of ownership is an important factor for many enterprises when considering whether to deploy appliances. For example, a single appliance purchase may eliminate the requirement to negotiate a separate operating system license agreement. Additionally an all-in-one appliance will reduce the total number of servers in the data center, thus reducing the overall TCO of ongoing support and maintenance.

Improve Ease of Installation, Configuration, and Administration—In many cases, appliance solutions offer pre-installed, pre-configured security applications, thereby creating more of a “plug and play” experience for customers. And, in addition to ease of installation and configuration, many appliance solutions offer remote administration capabilities that enable centralized management for distributed enterprises.

Use Standard Hardware—Many IT organizations have standardized application support on specific hardware platforms. For example, an IT department may standardize all server and/or appliance support on Hewlett-Packard hardware to take advantage of favorable volume purchasing and support contracts.

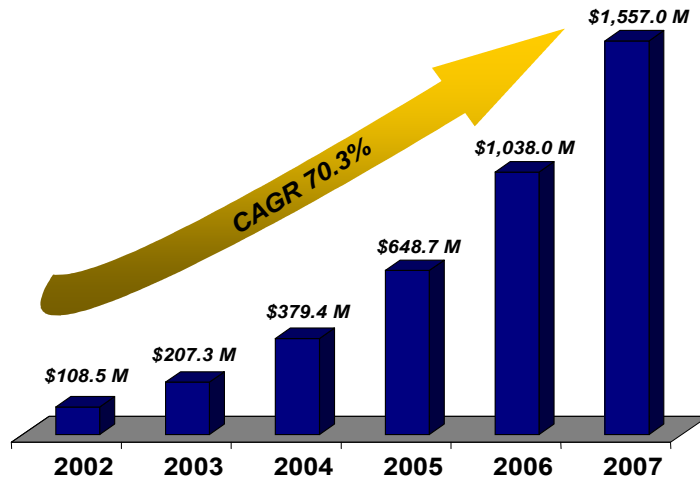
Guarantee a Secure Operating System—As security applications become more prevalent and a more integral part of the enterprise, it is becoming more important that the applications themselves are running on a secure operating system. Simply stated, IT departments don't want to be required to secure their own security applications. More and more customers consider it imperative that security applications are secured against “common” security vulnerabilities like buffer overflows, overloads, and format bugs.

Maximize the Use of Dedicated Resources—Customers requiring a high level of performance may opt for an appliance solution for two primary reasons: dedicated resources and application optimization. In the first scenario, in order to maximize performance, a large data center may choose to dedicate an appliance to a single security application. The one-to-one hardware-to-application relationship will ensure that performance will not be compromised by resource sharing conflicts. In the second scenario, the enterprise may prefer an application that has been optimized for its hardware environment.

Complement a Changing IT Organizational Structure—Some enterprises have transitioned security functions into the networking department of their IT organizations. Because many network administrators are familiar with appliance-based solutions for network-related functions (e.g., switches, routers, etc.) they are more willing to deploy security applications on an appliance. Additionally, since servers often fall under the domain of applications groups, network security professionals may decide on an appliance to eliminate possible political conflicts within their IT departments. Each organization will choose the deployment option that best fits its computing environment. Customers will balance their own environment-specific requirements before deploying software-based, appliance based, or even hybrid (both software and appliance) solutions in their enterprise.

Market Size and Growth Rate

According to IDC, the total worldwide market for security appliances is expected to exceed \$4.7 billion by 2007. The majority of this market comprises firewall/VPN appliances, which will contribute nearly \$2.8 billion. The rest of the market is divided between IDS appliances, at approximately \$345 million, and secure content management (SCM) appliances, which will reach a little over \$500 million. Of these submarkets, SCM appliances—which include EIM applications—are expected to grow the fastest at approximately 70.3% compound annual growth rate (CAGR).¹



Platform Types and Key Players

Different types of security appliances can be used to effectively deliver comprehensive security applications to enterprise customers. Each platform offers several benefits in varying ways and unique network environments. Appliance platform types that are most frequently used in conjunction with security applications include the following.

Stand-Alone Appliances—Stand-alone appliances are hardware platforms devoted to a single security application. Because stand-alone appliances devote hardware resources to a single application, enterprises benefit from higher performance and ease of upgrade.

Integrated/All-in-One Appliances—Integrated or “all-in-one” appliances, take a Swiss Army knife approach to security, often combining two or more security and networking applications in a single hardware device. Because applications are consolidated in a single device and policy engine, integrated/all-in-one appliance customers often realize lower TCO and improved ease of configuration.

Blade Appliances—Blade appliances typically include a chassis with one or more “blades” that run independent security applications inside the chassis. Each blade is equivalent to an independent server or appliance, and contains dedicated CPU, memory, and disk space resources for each security application. Blade appliances deliver built-in failover and load-balancing utilities into the chassis and act as a hybrid between stand-alone appliances and integrated/all-in-one appliances. Customers that deploy blade solutions benefit from higher overall system performance.

“Software” or “CD” Appliances—Software/CD appliances deliver security applications in software or compact disc format and typically run on multiple types of open systems. Security application software and hardware appliances typically “meet in the channel,” enabling resellers and customers to install these

¹IDC Market Analysis: Worldwide Security Appliance Forecast and Analysis, 2003-2007; December 2003
Figure 1. Growth Rate of Secure Content Management Security Appliances (Source: IDC)



solutions on various hardware devices and operating systems. Enterprises that use software/CD appliances experience the ease of installation of a hardware appliance alongside the flexibility and low cost of standardized and open systems (e.g., Intel-based servers, Linux operating systems, etc.). Strategies for Continued Growth and Success in the Employee Internet Management (EIM) Industry

The following table summarizes the various appliance platform types that are available to enterprises, as well as some of the key industry players.

Platform Types and Key Players

Platform Type	Customer Benefits	Key Players	
Stand-Alone	<ul style="list-style-type: none"> High Performance Ease of Installation/Upgrades Low Cost of Deployment 	Cisco Systems NetScreen Nokia WatchGuard	Dell Hewlett-Packard IBM Sun Microsystems
Integrated/ All-In-One	<ul style="list-style-type: none"> Lower Total Cost of Ownership Ease of Installation/Management 	Blue Coat Systems Cisco Systems Fortinet Internet Security Systems	Network Appliance Novell/Volera SonicWALL
Blade	<ul style="list-style-type: none"> High Performance Failover and Load Balancing Manageability 	Blade Fusion Cisco Systems	Crossbeam Systems OmniCluster
Software/CD	<ul style="list-style-type: none"> Flexibility Low Cost of Deployment Standardization 	Check Point Software (sw) Immunix (sw) Dell (hw)	Hewlett-Packard (hw) IBM (hw) Sun Microsystems (hw)

Looking Ahead

As the enterprise security market continues to evolve, security applications like IDS, AV, e-mail/spam gateways, and EIM will be deployed in varying ways to meet customer requirements. While some enterprises may continue to deploy stand-alone solutions, others will look for new ways to combine applications into integrated/all-in-one platforms, blade solutions, and software/CD appliances. Customers will deploy the security appliance solution that best suits their respective environments. Additionally, as the Gartner Group notes, existing security vendors (especially firewall vendors) will continue to add new functionality and deeper inspection capabilities (like AV and EIM) into their product lines. As the market has demonstrated with vendors like SonicWALL and Fortinet, this increasing trend could mean that many former stand-alone solutions may start to transition towards integrated/all-in-one appliances or event blade appliances.

“As the firewall market focuses more on deep packet inspection of application content, vendors could absorb HTTP and active content inspection functions.”

Bill Gassman and Arabella Hallawell, Gartner Group – August 5, 2003

WebSense's EIM Solution

Overview

WebSense Enterprise® (WSE) software enables organizations to manage the way employees use the Internet and corporate computing resources. WSE allows organizations to optimize their employees' use of the Internet via administrative options that enable control over what Internet-based content may be accessed, at what time of day and for how long. Other administrative management options include warning pages to notify employees that a requested Web site may include content that falls outside of their organization's defined policy and an option that enables employees to defer viewing of certain Web content until after work hours. The Websense solution includes an award-winning database of categorized Web sites, network protocols and desktop applications that is updated on a regular basis. Using this highly granular database, IT administrators can create employee-based policies to manage Internet use.

WSE is the *only* solution that filters at multiple points on the network, gateway, and desktop to ensure complete protection against emerging threats. The product allows organizations to easily assess risk areas, identify problem users, manage user and group privileges, and enforce corporate policies for appropriate use of the Internet and other computing resources.

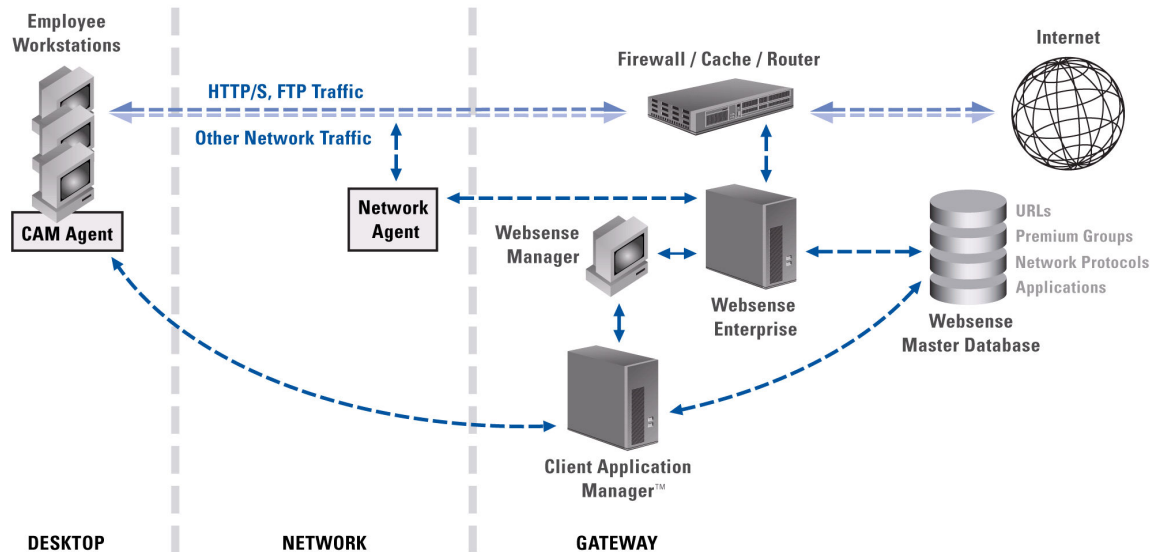


Figure 2. The Websense Enterprise EIM Solution

By enabling enterprises to manage the use of their employee computing resources, WSE provides customers with four key benefits to the enterprise:

- **Security**—Enhanced enterprise security through management of spyware and malicious mobile code, the prevention of employee use of hacking tools, as well as protection against zero day threats.
- **Productivity**—Increased productivity through the management of non-business activities.
- **Bandwidth**—Decreased bandwidth costs by limiting noncritical network traffic.
- **Legal Liability**—mitigated legal risk by blocking objectionable URLs and applications.



The Websense Appliance Strategy

More than any other EIM solution provider in the world, Websense has embraced the security appliance market opportunity. Websense has achieved its market leadership position for a number of reasons, including technology leadership, breadth of features, quality of product, and exceptional channel partners. Another fundamental reason for the industry success of Websense is its unique alliances with a comprehensive network of technology partners. Over the past several years, Websense has carefully chosen to develop relationships with only the industry's top networking and security vendors. Websense's deliberate focus on each of these "best-of-breed" networking and security vendors enables customers to flexibly deploy WSE software in their existing network infrastructure. For example, many customers deploy Websense in conjunction with one vendor's firewall at one office location and with another vendor's cache engine at another office. The same breadth of support and availability across multiple technology vendors and platforms that has enabled many enterprise-wide deployments of Websense software is the same strategy that Websense has invoked in the appliance market. Websense's proven track record of initiating, developing, and cultivating partnerships with the industry's leading technology vendors will facilitate Websense's continued market leadership in the EIM and security appliances markets.

This section describes how the Websense EIM can be deployed as part of different security appliance solutions.

Stand-Alone Appliances

Currently, the most popular appliance-based deployment of Websense is with the stand-alone platform. WSE software runs on the leading security and networking platforms including: Dell, Hewlett-Packard, IBM, Nokia, and Sun Microsystems. Additionally, Websense supports standardized operating systems (Linux, Solaris, and Windows) as well as Nokia's proprietary IPSO platform, thus making WSE compatible with nearly every available hardware environment.

Integrated/All-in-One Appliances

In addition to stand-alone appliances, Websense supports a number of integrated/all-in-one appliances, including embedded solutions that run together on Blue Coat Systems security appliances, Cisco Systems Content Engine, and Novell Volera Excelerator. These integrated/all-in-one appliances combine Websense EIM software with the leading security and networking applications of its partners. Websense continues to pursue best-of-breed and OEM relationships with the world's leading appliance vendors, in order to provide comprehensive EIM solutions for customers who choose to deploy integrated/all-in-one appliances.

Blade Appliances

Websense can work as part of blade appliance solutions. Websense's partnership with Crossbeam Systems makes Websense Enterprise available on a blade server alongside other security applications, including firewalls, VPN systems, IDS, and AV. Additionally, WSE software is embedded in the Cisco Content Engine Network Module—a blade that runs inside Cisco branch office routers. Each of these blade appliance solutions offers customers the flexibility for deploying WSE software within their existing network infrastructure.

Software/CD Appliances

One emerging segment of the security appliance market is the software/CD appliance. Software/CD appliance solutions are ideal for a "meet in the channel" approach where channel partners install and configure Websense Enterprise software with the hardware preferences of the customer. In this implementation, Websense Enterprise software is combined with the Immunix secure Linux operating system and installation/manageability toolsets.

Conclusion

Websense has achieved great success as the leading vendor of EIM software solutions, attracting over 20,600 customers worldwide, representing 16.4 million seats under subscription. This success is due primarily to Websense's commitment to delivering high-quality, feature-rich software, as well as its "best of breed" partnership strategy. As market dynamics change and customer requirements evolve, it is evident that the security appliance market—particularly SCM and EIM appliances—is on the verge of accelerated growth. Due to early and on-going significant investment in partnerships with the world's leading networking and security hardware providers, including both integrated and appliance-based solutions, Websense is already at the forefront of the appliance market for best of breed EIM solutions.



Websense has established partnerships with over 40 different networking and security vendors—including appliance-based solutions with Blue Coat Systems, Cisco Systems, Crossbeam Systems, Immunix, and Nokia. Each of these relationships provides enterprise customers with the flexibility to easily install, administer, and support Websense Enterprise within their existing IT infrastructure. The combination of Websense's technological superiority and its strategic partnerships with leading hardware vendors will enable Websense to continue its leadership in both software-based and appliance-based EIM solutions. Websense will continue to use these key advantages to leverage growth waves for EIM software as well as EIM security appliances—further extending Websense's position as the world's #1 EIM solution provider.

About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), protects more than 25 million employees from external and internal computer security threats. Using a combination of preemptive ThreatSeeker™ malicious content identification and categorization technology and information leak prevention technology, Websense helps make computing safe and productive. Distributed through its global network of channel partners, Websense software helps organizations block malicious code, prevent the loss of confidential information and manage Internet and wireless access. For more information, visit www.websense.com.



Appendix A: Websense Best of Breed Partners

Appliance Solutions

- Blue Coat Systems ProxySG Appliances Powered by Websense™
- Websense Enterprise Embedded In Cisco Content Engines
- Websense Enterprise Embedded In Crossbeam Appliances
- Websense Enterprise Embedded In Immunix Secure Servers
- Websense Enterprise Embedded In Nokia IPSO Appliances

Firewall Solutions

- Check Point Firewall-1
- Cisco Systems PIX Firewall
- CyberGuard
- Lightspeed Total Traffic Control
- NetScreen
- ServGate
- SLMsoft SecurIT
- SonicWALL

Cache/Proxy Server Solutions

- 3Com Webcache
- Blue Coat Systems SGProxy
- Cisco Systems Content Engine
- Dell PowerApp.cache
- F5 EDGE-FX
- Hewlett Packard Web Cache
- iMimic DataReactor
- InfoLibria DynaCache
- Inktomi Traffic Server
- Microsoft ISA Server
- Microsoft Proxy Server
- Network Appliance NetCache
- Squid Proxy
- Stratacache
- SunONE WebProxy Server
- Volera Excelerator

Switch/Router Solutions

- Cisco Systems Catalyst 6500 Switches
- Cisco Systems IOS Routers