

I D C V E N D O R S P O T L I G H T

Building a Web Security Ecosystem to Combat Emerging Internet Threats

September 2005

Adapted from: *Worldwide Secure Content Management 2005–2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam, and Malicious Code Continue to Wreak Havoc*, by Brian E. Burke; Doc # (forthcoming)

Sponsored by Websense

The Web filtering market continued to grow at a healthy pace in 2004, with 23% year-over-year growth reaching more than \$433 million in worldwide software revenue. The demand and interest in Web filtering solutions remains strong, with rising corporate concerns about Internet threats that reach beyond productivity, bandwidth, and liability issues and now into Web security. With the Internet becoming an increasingly complex threat vector for hackers, malicious applications, and vulnerability exploits, today's enterprises require a more holistic and integrated approach for Internet security — a Web security ecosystem — to combat emerging threats from the Internet. This report examines components of a comprehensive framework that enables organizations to enhance their threat-mitigation capabilities, while increasing the return on investment of existing information technology infrastructures. This paper also looks at the role of Websense in a multilayered approach to building and maintaining an effective security ecosystem for enterprises. As Internet threats have evolved to include security risks, Websense has adapted its product and technology partner strategy to provide interoperability with new security systems. Websense's Web Security Ecosystem has expanded to include partners from the following solution areas: Internet gateways, network access control, security event management, identity management, and appliance platforms.

Components of a Web Security Ecosystem

Secure Content Management Grows in Importance

Secure content management (SCM) is IDC's term for a superset of several security areas that address many — but not all — of an organization's needs. The SCM market reflects enterprise needs for policy-based Internet management tools that manage Web content, messaging security, virus protection, spyware, and malicious code. SCM vendors enjoyed another strong year of growth in 2004. IDC expects the worldwide revenue for SCM software to reach \$5.5 billion in 2005. The market is forecast to increase to \$10.5 billion in 2009 for a 18.7% compound annual growth rate (CAGR) for the period from 2004 through 2009.

Major virus and worm outbreaks, explosive growth in phishing, and corporate deadlines for compliance with government regulations fueled the need for Web and messaging security solutions. Additionally spyware is new on the scene and quickly moving up the priority list of corporate security issues. What concerns corporate security departments the most is that spyware can also be used to monitor keystrokes, scan files, install additional spyware, reconfigure Web browsers, and snoop email and other applications.

Additionally, phishing attacks continue to be a key driver for multilayered, integrated solutions. Phishing and other Web-based frauds are an excellent example of how malicious content may be

propagated through email and other messaging mediums, but must also be controlled by Web filtering and security solutions. Finally, government and industry regulations such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, and various SEC regulations continue to pressure corporations to secure the use of all electronic forms of communications.

The Imperative for Security Ecosystems

The evolution of Web-based threats has not only highlighted the importance of keeping security solutions up to date, but it has also put a spotlight on the growing need for more proactive, integrated security solutions in the IT environment. The rapid infection rates of malicious attacks means that slow responding systems will cripple most customer environments because of the inability to get ahead of initial infections and far more serious re-infections.

Moreover, malicious hackers are getting more sophisticated at exploiting application vulnerabilities, increasingly using blended malware from multiple threat vectors — and more specifically the Internet. Instead of reactive responses from point solutions, today's threat-based environment requires a more holistic, integrated, and multilayered approach to security infrastructure — a Web security ecosystem — that can enable more centralized policy management and compliance auditing.

Organizations of all sizes require various products and services to support their IT security needs. Inevitably, the evaluation process for security solutions often leads to “best-of-breed” or “best-in-class” purchases based on how well the product or service satisfies the specific requirements for each customer environment. Once these best-in-class solutions are selected, a key challenge for IT managers is to maximize their return on investment by seamlessly integrating security solutions into their existing environment. Seamless integration of security components is critical because it:

- lowers overall deployment costs
- improves overall strength of security systems
- increases the ROI of new and existing infrastructure investments

Web Filtering Expands Its Role

Web filtering software is an integral part of any enterprise security system and has accounted for the third-largest segment of the total SCM market in 2004. Recently, Web filtering has expanded its value proposition beyond objectionable and non-business related content to include malicious applications and Web sites. This increased demand for Web security in addition to traditional Web filtering has elevated the priority of Web filtering solutions within the IT security departments of enterprises of all sizes.

The recent focus on Web filtering as a critical security component of the IT security infrastructure has created more extensive integration and interoperability requirements for Web filtering and security solutions.

In 2004, the worldwide Web filtering software market reached \$433.5 million. IDC believes that Web filtering software will grow from \$433.5 million in 2004 to \$929 million in 2009, representing a compounded annual growth rate of 16.5%.

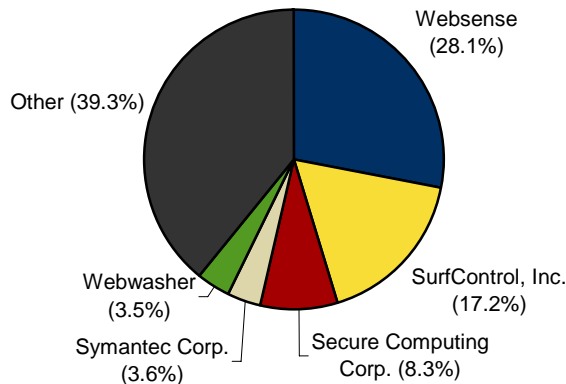
Websense: Leading the Web Filtering Software Market in 2004

According to IDC, Websense was the market leader in Web filtering software in 2004. As the largest Web filtering software vendor, Websense accounted for a 28.1% market share and more than \$111

million in revenue, as shown in Figure 1. From 2003 to 2004, Websense increased revenue 37% in the Web filtering market.

Figure 1

Worldwide Web Filtering Software Revenue by Vendor, 2004



Source: IDC, 2005

Strategic Direction

As the Internet has evolved from an abundant resource of information, content and online services to a legitimate attack vector with malicious websites that harbor harmful applications like viruses, worms, spyware, and keyloggers, Websense has responded by developing a sophisticated suite of products — the Websense Web Security Suite — that helps customers close the gaps of traditional firewall and anti-virus products. This expanded reach into Web filtering and security has led Websense to evolve its integrated technology approach to include several new value-added security solutions. Today, the Websense Web Security Ecosystem includes technology partnerships and integrations with five unique security solution areas (highlighted in Figure 2):

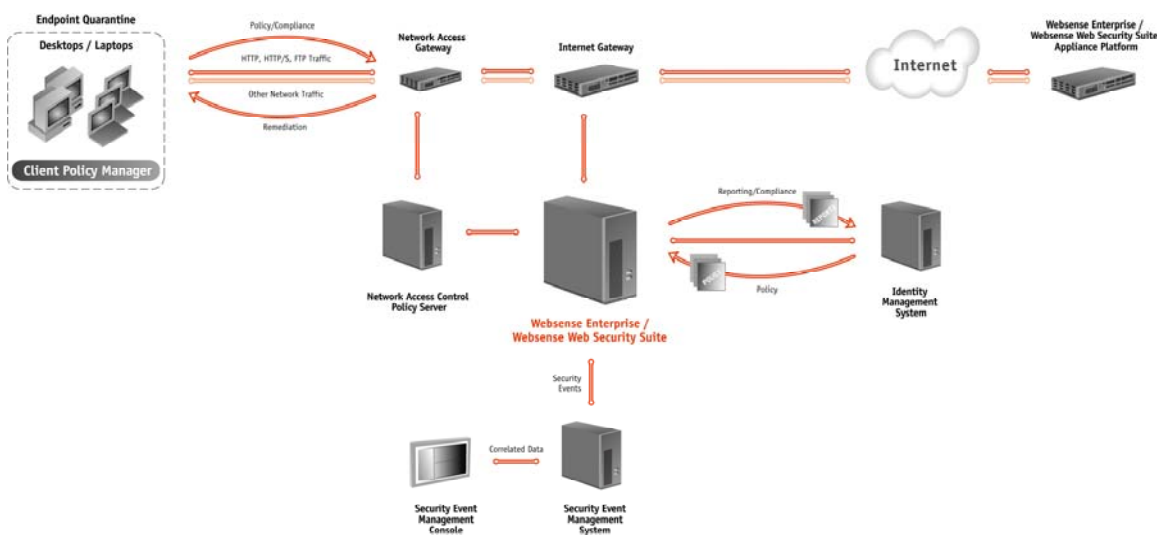
- **Internet Gateways:** Internet gateway integrations are a cornerstone of the Websense web filtering and security technology partner strategy. Since the inception of Websense's web filtering product implementations, Websense has sought and developed technology integrations and relationships with the leading security and networking solutions (like firewalls, proxies, switches and routers) to provide interoperability between internet gateways and Websense's web filtering and security solutions. These integrations have provided customers with key benefits that include scalability, accuracy, and stability of internet filtering technology. Today, the Websense Web Security Ecosystem includes more than 30 different internet gateways, assuring customers of seamless integration into almost any IT environment.
- **Network Access Control:** Network access control solutions offer customers with the ability to enforce endpoint policy compliance through network-based quarantining and streamlined remediation at network access gateways (routers, switches, authentication servers). Endpoint policy compliance includes confirmation that specified agents (AV, HIPS, etc.), application

versions and patches are up-to-date. If vulnerabilities exist, network access control gateways limit or quarantine network access until the identified problem is resolved. Websense's desktop security solution, Client Policy Manager, interoperates with leading network access control frameworks to provide integrated endpoint compliance.

- **Security Event Management:** These solutions consolidate and correlated security log and event data into real-time reports and dashboards that help IT security managers to prioritize and react to critical security events and vulnerabilities. Many organizations today deploy security event management systems not only to alleviate the problems associated with excessive alerts – but, also to add risk analysis to threat management. Websense integrates with Security Event Management systems by sending desktop security and Web filtering events related to spyware, keylogger, hacking, and malicious-code applications and Internet traffic. Websense's content categorization provides additional intelligence to enterprise security events that traditional security products often lack.
- **Identity Management:** These solutions enable enterprises to centrally configure and manage various IT applications and services including security policies. Today's identity management systems offer centralized configuration and management of several security devices and policies, as well as user access. Because Web filtering and security policies occur on both the user and group level, it's a natural extension to provide integration of policies with leading identity management systems. Additionally, Websense has extended this paradigm to include a complete feedback loop of policy compliance auditing to identity management systems. The seamless integration of Websense Internet access and desktop policies, and compliance reporting, offers IT administrators more streamlined Web security management.
- **Appliance Platforms:** These are a critical component of any SCM solution, including Web filtering. As a leading software provider, Websense continues to support best-of-breed security and unified threat management (UTM) appliances as a means of providing customers with pre-installed and embedded form factors of its Web filtering and security solutions.

Figure 2

The Websense Web Security Ecosystem



Source: Websense, 2005

Websense Products and Services

Websense offers the following web filtering and security products:

- **Websense Web Security Suite** provides an integrated web security solution that protects against spyware, blocks malicious mobile code (MMC), and other Web-based threats including spyware and keylogging transmissions back to their host sites. This offering also enables blocking of instant-messaging file attachments as well as real-time security updates that provide immediate protection from new security threats. Web Security Suite customers can also take advantage of Websense's SiteWatcher and BrandWatcher services, which monitor and alert customers to Web site intrusions and malicious use of their brands. *Websense Web Security Suite - Lockdown Edition* offers all these features plus enhanced endpoint security that blocks the execution of unauthorized applications such as spyware, peer-to-peer file sharing, hacking tools, and other malicious applications on the desktop.
- **Websense Enterprise** manages employee Web use at three network control points — the gateway, network, and desktop. Websense Enterprise enables management across Web pages, network protocols, and desktop applications to effectively combat growing security, legal, and productivity threats that infiltrate company networks.
- **Websense Client Policy Manager (CPM)** delivers desktop security protection against known and unknown security threats and prevents execution of unauthorized applications. CPM enforces employee application use policies with its unique and comprehensive database of categorized applications.

Other Websense Enterprise add-on modules include Bandwidth Optimizer, IM File Attachment Manager, Productivity PG and Bandwidth PG.

Websense also offers a Web security alerting service through its security research division — Websense Security Labs (www.websensesecuritylabs.com). In 2004, Websense formalized this program as an extension of its existing research group that has been classifying malicious websites since 2001. Today, Websense Security Labs mines more than 350 million websites per week for malicious code, phishing and frauds, spyware, keyloggers, and other threats. This research arm is a charter member of the Anti-Phishing Working Group and publishes daily security alerts and a semi-annual Web Security Trends Report that consolidates information and vital statistics of Web-based threats.

Challenges & Opportunities

While Websense is a leader in a robust market, the company does face challenges to its continued success. IDC believes that the biggest challenge in the SCM and threat management security market is product differentiation through improved performance, features, and interoperability. With the proliferation of so many products, customer confusion can and will occur. For Websense to win in such a hypercompetitive market, it must stand out, which can be accomplished in a number of ways: price, performance, the mix of security functions, improved manageability, security knowledge services, and/or security interoperability.

Because IDC believes that organizations need to develop and deploy integrated "security ecosystems," Websense is well-positioned as a revenue leader in the SCM market. To the extent that Websense can offer superior manageability with its products, as well as provide a multilayered approach to building and maintaining the security infrastructure, the company should be able to take advantage of the market trends to continue its market leadership.

Conclusion

Internet-borne threats to companies and organizations of all sizes continue to grow and become more complex. Although many security technologies have been deployed to protect these environments, hackers have increasingly focused on blended threats, a combination of malicious code keyed to exploit specific vulnerabilities. These blended attacks are specifically designed to circumvent point security mechanisms such as independent VPN, firewall, and antivirus products.

Blended threats work against point solutions, but they have a high probability of failure when the security solutions are unified. IDC believes that organizations need to develop and deploy holistic, integrated "security ecosystems" — systems that provide flexible best-practices security solutions for the future.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC visit www.idc.com. For more information on IDC GMS visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com