

EXCERPT

Worldwide Secure Content Management 2005–2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam, and Malicious Code Continue to Wreak Havoc

Brian E. Burke

Rose Ryan

IN THIS EXCERPT

This Excerpt is from *Worldwide Secure Content Management 2005–2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam, and Malicious Code Continue to Wreak Havoc* (IDC #34023, September 2005) by Brian E. Burke and Rose Ryan. It contains the Market Definition and Situation Overview sections as well as a Vendor Profile.

SECURE CONTENT MANAGEMENT MARKET DEFINITION

Secure content management (SCM) includes policy-based content security solutions designed to secure, monitor, filter, and block threats from messaging and Web traffic. SCM protects against inbound threats such as spam, fraudulent emails, viruses, worms, trojans, spyware, and offensive material. SCM solutions are also designed to protect against outbound threats such as confidential data, customer records, intellectual property, and offensive content leaving an organization. SCM solutions play a key role in complying with government and industry regulations as well as enforcing corporate policies. SCM is a superset of three specific product areas:

- ☒ **Antivirus** software identifies and/or eliminates harmful software and macros. Antivirus software scans hard drives, email attachments, floppy disks, Web pages, and other types of electronic traffic (e.g., instant messaging and short message service [SMS]) for any known or potential viruses, malicious code, trojans, or spyware.
- ☒ **Web filtering** software is used to screen and exclude from access or availability Web pages that are deemed objectionable or not business related. Web filtering is used by corporations to enforce corporate Internet use policies as well as by schools and universities and home computer owners (for parental controls).
- ☒ **Messaging security** software is used to monitor, filter, and/or block messages from different messaging applications (e.g., email, IM, SMS, and P2P) containing spam, company confidential information, and objectionable content. Messaging security is also used by certain industries to enforce compliance with privacy regulations (e.g., HIPAA, Gramm-Leach-Bliley [GLB], and SEC) by monitoring electronic messages for compliance violations. This market also includes secure (encrypted) email.

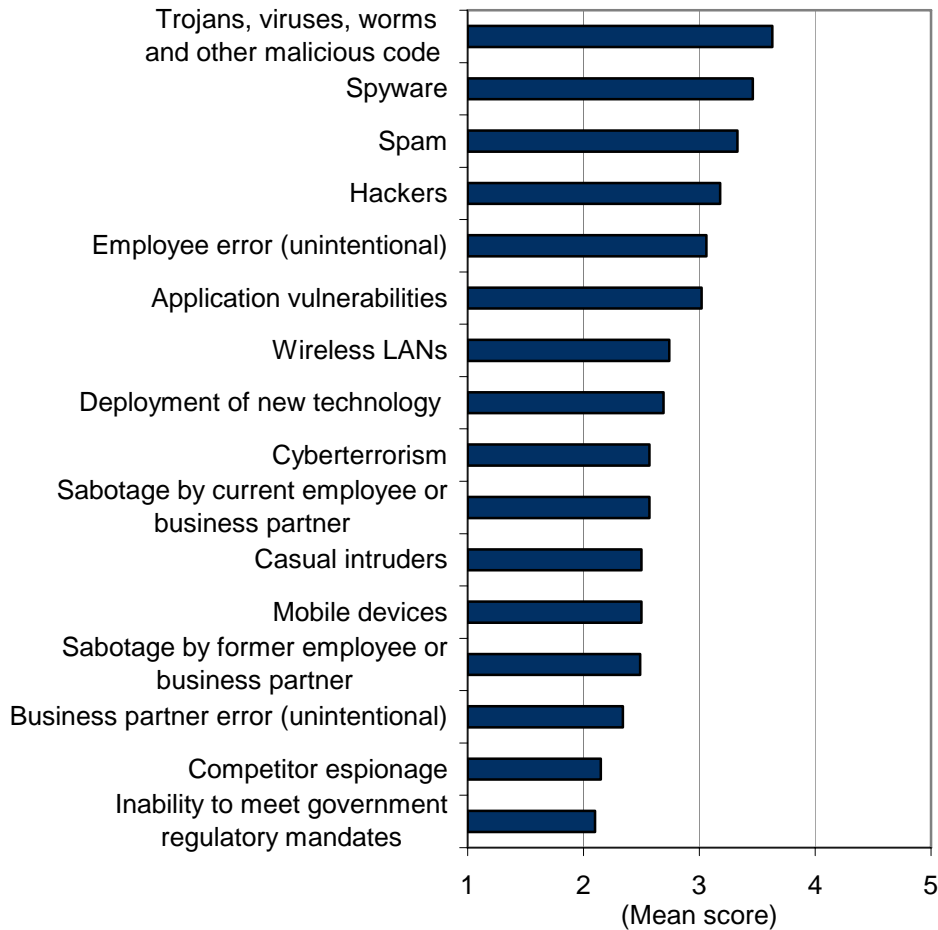
SITUATION OVERVIEW

Hot Trends in the Secure Content Management Market

Viruses and worms continue to be the most serious threat facing corporations today, but spyware has rapidly climbed the priority list of enterprise security threats and now ranks as the second most serious threat facing corporations today (as shown in Figure 1).

FIGURE 1

Threats to Enterprise Security



n = 435

Note: Scores are based on a scale from 1 to 5, with 1 being no threat and 5 being a significant threat.

Source: IDC's *Enterprise Security Survey*, 2005

Spyware: Motivated by Financial Gain

Spyware is now considered to be the second-greatest threat to enterprise network security, according to IDC's 2005 *Enterprise Security Survey*, up from fourth in 2004. Spyware has quickly become both a security and system management nightmare. IDC believes more than three-quarters of all corporate machines are infected with various forms of spyware. Theft of confidential information, loss of employee productivity, consumption of large amounts of bandwidth, damage to corporate desktops, and a spike in the number of help desk calls related to spyware are forcing corporations of all sizes to take action. Our survey results indicate that 84% of organizations have implemented antispymware.

Although the consequences of spyware may be as minor as annoying advertising pop-ups, spyware has the potential to do significant damage to the machine and also to the entire network. It has the ability to capture virtually all online activity. From monitoring all keystrokes, email snooping, and scanning files on the hard drive to changing system or registry settings, spyware is both a privacy and enterprise security threat. Such activities can lead to identity theft, data corruption, and, increasingly, theft of company trade secrets. Hackers are also using keyloggers to steal users' account information, log-in names, and passwords. With a user's account information, the hacker is then able to obtain a wealth of personal data, including bank information, additional passwords, and credit card numbers.

Spyware is far more sophisticated than traditional viruses, and the motivation of a spyware writer is drastically different from that of a virus writer. Spyware is not being created by the younger generation of script kiddies who create viruses, seeking personal pride or notoriety. Spyware writers, unlike virus writers, are motivated by profit and financial gain. The evolution from mischievous hobby to a money-making criminal venture has attracted a new breed of sophisticated hackers and organized crime. Hackers are now much less concerned with destroying systems and knocking out Web sites. They realize that they can generate money from stealing confidential personal information and corporate data and selling it to spammers or those involved in organized crime and fraud. IDC believes this profit-driven motivation will cause the number of attacks to increase in sophistication, frequency, and severity.

Outbound Content Compliance: Information Leakage and Data Protection

Historically, information security solutions have focused on addressing external threats to corporate networks and endpoints. Viruses, hackers, worms, trojans, spam, blended threats, and, most recently, spyware have wreaked havoc on corporate networks and users alike. In turn, enterprises have deployed an expanding array of security solutions such as firewall, antivirus, antispam, intrusion detection/prevention, and antispymware to protect the corporate perimeter from inbound threats. Today, an emerging threat to corporate security comes from inside the organization. The insider threat of trusted employees deliberately or inadvertently distributing sensitive information is quickly becoming a major concern in many organizations. This concern has created a new market, which IDC has termed outbound content compliance (OCC).

OCC includes solutions that monitor, secure/encrypt, filter, and block outbound content contained in email, instant messaging, P2P, file transfers, Web postings, and other types of messaging traffic. OCC solutions play a key role in enforcing corporate governance, which is defined by IDC as a combination of complying with both external regulatory requirements and internal corporate policies and best practices. These solutions help organizations protect against the following:

- Violations of government and industry regulations (HIPAA, Gramm-Leach-Bliley, Sarbanes-Oxley, and so on)
- Violations of corporate email policy and best practices
- Loss/leakage of intellectual property
- Loss/leakage of confidential or customer information
- Inappropriate content

The growing awareness of outbound content compliance was recently catalyzed by a series of corporate scandals in which customer records, confidential information, and intellectual property were leaked. As the vast majority of those cases demonstrate, such breaches are often not the result of malicious wrongdoing but rather employees who unknowingly put their companies at risk. This may occur as employees send out email messages that contain files or content they are not aware is confidential. Another example is employees delivering confidential files to their Web-based emailboxes, or copying files to mobile devices, and thus exposing them to untrusted environments. IDC believes enterprise rights management (ERM) solutions will also play a key role in preventing data leakage.

Web Filtering: No Longer Just a Productivity Tool

Web filtering has evolved from addressing a single class of employee distractions — access to inappropriate URLs — to more comprehensive Web security solutions that address a wide array of Web-based threats. Web security concerns are at an all-time high due to the rash of spyware, virus, phishing, and malicious mobile code attacks that have wreaked havoc on corporate networks. The number of Web sites distributing spyware has increased explosively as spyware creators continue to extend their distribution channels. As the number of Internet users continues to increase, the Web becomes an increasingly more attractive target for hackers, spyware, and virus writers. Moreover, attacks targeting Web browser vulnerabilities illustrate the sophisticated techniques hackers have developed to spoof, or fake, Web sites and how easily malicious code can steal usernames, passwords, and other vital information. IDC believes Web-based attacks will continue to become more malicious and sophisticated. Web filtering solutions will play a valuable role as a complementary enhancement to traditional antivirus and firewall deployments.

Vendor Performance by Market Segment

Web Filtering

Web filtering accounted for the third-largest segment of the SCM market in 2004, reaching \$433.5 million. From 2003 to 2004, the Web filtering market increased 22.9%.

TABLE 6

Worldwide Secure Content Management Product Revenue by Segment, 2003–2009 (\$M)

	2003	2004	2005	2006	2007	2008	2009	2004 Share (%)	2004–2009 CAGR (%)	2009 Share (%)
Antivirus	2,685.6	3,283.5	3,874.5	4,455.7	5,079.5	5,714.4	6,366.2	73.3	14.2	60.4
Antispyware	28.5	97.0	214.8	353.1	481.6	565.1	641.4	2.2	45.9	6.1
Web filtering	352.8	433.5	521.4	622.1	724.0	829.5	929.0	9.7	16.5	8.8
Messaging security	442.5	665.4	913.7	1,237.4	1,634.9	2,098.4	2,597.5	14.9	31.3	24.7
Total	3,509.4	4,479.4	5,524.4	6,668.2	7,920.0	9,207.5	10,534.1	100.0	18.7	100.0

Notes:

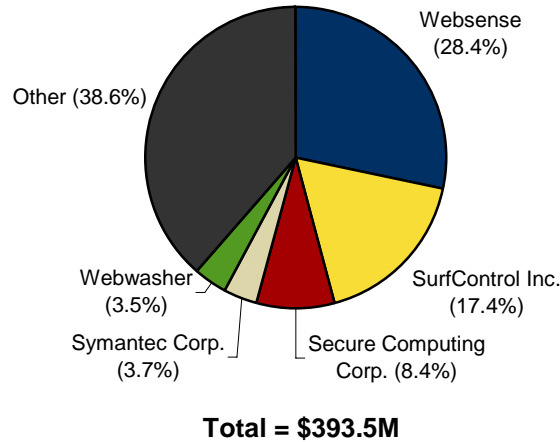
Vendor revenue includes hosted service-, software-, and appliance-based solutions.

See Table 10 for key forecast assumptions.

Source: IDC, 2005

FIGURE 5

Worldwide Web Filtering Software Revenue Share by Top 5 Vendor, 2004



Source: IDC, 2005

ESSENTIAL GUIDANCE

Vendor Profile

Websense

Overview

Websense was founded in 1994 and now has more than 24,000 customers. Headquartered in San Diego, California, with offices in China, Japan, and Australia and across Europe, Websense now employs approximately 530 people worldwide.

Secure Content Management Products

Websense Web Security Suite — Lockdown Edition is an integrated Web security solution that provides spyware protection and blocks access to malicious mobile code and other Web-based threats through the following:

- ☒ Websense Removable Media Lockdown allows system administrators to prevent devices such as flash drives, CD/DVD burners, floppy drives, and external hard drives from being used on client workstations. Organizations can also block writable media, depending on their policy.
- ☒ Websense Network Lockdown delivers protection against known and unknown security threats by blocking application network access to specific ports and protocols by application category.

- ☒ Websense Application Lockdown provides control over desktop environments by allowing only approved applications to run on corporate PCs and servers, thereby preventing potentially malicious applications from launching. It also detects and analyzes endpoint desktop security threats and application activity.
- ☒ Websense Express Lockdown allows system administrators to prevent the execution of new applications, thereby blocking attacks such as keyloggers, Trojan horses, worms, and other malicious code threats. Unlike Application Lockdown, Express Lockdown does not require a machine inventory.
- ☒ Websense Web-based Threat Mitigation provides protection from Web-based threats, including keyloggers, spyware, Trojan horses, botnets, scripts, and ActiveX controls, via a database of malicious Web-based applications.
- ☒ 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, such as P2P file sharing, IM, hacking tools, and spyware.
- ☒ Client Policy Manager (CPM) is an innovative endpoint security solution that delivers "zero day" threat protection from unknown security threats, including today's sophisticated malware. CPM policies also stop the execution of unauthorized applications such as spyware, P2P file sharing, and hacking tools while enabling flexible policy management of applications such as IM or remote control tools that only select users are allowed to launch. CPM also allows organizations to lock down removable media such as flash drives, CD/DVD burners, floppy drives, and external hard drives to avoid use on client workstations. Utilizing a unique application database with more than 50 categories, CPM enforces flexible-use policies for corporate desktops, mobile laptops, and servers.
- ☒ Bandwidth Optimizer improves overall network performance by reducing the use of non-work-related, high-bandwidth media based on real-time network conditions.
- ☒ IM Attachment Manager is an add-on module that enables IT managers to control the sending and receiving of files via IM clients. This module controls the security and legal risks posed by the unmanaged use of IM attachments, and it helps optimize IT resource allocation and employee productivity.

Strategic Direction

Websense was a leader in Web filtering revenue for 2004. Websense provides a layered solution to help organizations address Web security concerns by blocking access to spyware Web sites and spyware back-channel communication at the gateway and by preventing spyware applications from launching at the desktop. Websense secures organizations from emerging Internet threats by providing a Web security component that complements traditional security solutions.

Websense Web Security Suite provides an integrated Web security solution that offers spyware protection and blocks malicious mobile code and other Web-based threats as well as spyware and keylogging transmissions back to their host sites. It also protects employees from phishing and controls the sending and receiving of IM clients. The Websense Web Security Suite provides real-time Internet security updates for protection from new security threats and includes reporting and analysis tools that provide organizations with information on user access to fraudulent sites or vulnerability to malicious code.

Websense recently announced the general availability of Websense Enterprise CPM, a desktop security solution that fills critical endpoint gaps in today's multilayered enterprise defense systems. Complementing traditional firewall and antivirus tools, CPM closes the window of exposure to unknown security threats that often bring down networks before a virus signature or vulnerability patch is deployed.

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2005 IDC. Reproduction is forbidden unless authorized. All rights reserved.