

EXCERPT

Worldwide Web Security 2007 - 2011 Forecast and 2006 Vendor Shares (Excerpt from IDC #210034)

Brian E. Burke

IN THIS EXCERPT

This IDC excerpt is taken from the Worldwide Web Security 2007 - 2011 Forecast and 2006 Vendor Shares (IDC #210034, December 2007), by Brian Burke. All or part of the following sections are included in this excerpt: IDC Opinion, Situation Overview, The Web Security Market in 2006, Future Outlook, Essential Guidance, and Vendor Profiles. Also included is Table 1, Table 2, Figure 1 and Figure 2.

IDC OPINION

The demand and interest in Web security solutions is being fueled by rising corporate concerns about Internet threats that reach beyond productivity, bandwidth, and liability issues. 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. Key trends in the Web security market include:

- ☒ Web 2.0 has become a widely used term to describe second wave of the Internet', focusing on new collaboration technologies such as social-networking sites, wikis, and other types of Web applications designed to facilitate creativity, collaboration, and sharing between users. As Web 2.0 applications make their way into the enterprise, they bring with it new security concerns and attack vectors. A recent IDC study found that two-thirds of organizations are currently using at least one Web 2.0 application (source: IDC Doc #208944).
- ☒ Malicious hackers are getting more sophisticated at exploiting application vulnerabilities, increasingly using blended malware from multiple threat vectors — and more specifically the Web. Web-based threats such as spyware can be used to monitor keystrokes, scan files, install additional spyware, reconfigure Web browsers, and snoop email and other applications.
- ☒ Data loss prevention (DLP) is a growing concern in the Web 2.0 environment. 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, including the Web. Moreover, preventing leaks of intellectual property via web applications (web email, blogs, etc) has become an equally important concern in organizations of

- ☒ all sizes and vertical industries. This trend is driving the need for information protection and control (IPC) solutions that protect sensitive information and comply with privacy regulations for both Web and web applications.
-

SITUATION OVERVIEW

Web 2.0: Inbound and Outbound Threats

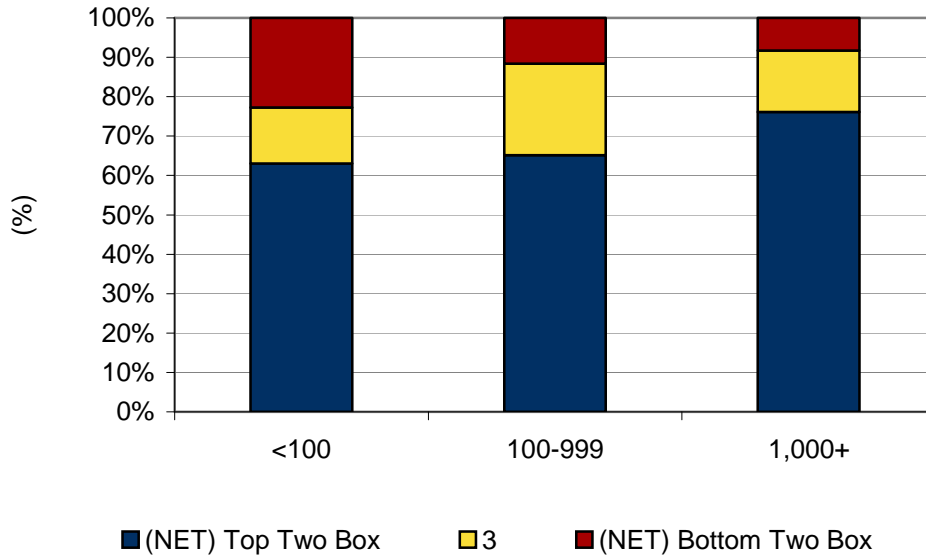
Recent years have seen a significant increase in the volume and sophistication of malware that uses the Web as an attack vector. These attacks are often carried out by professional hackers and criminals, who continuously look for weak spots in organizations' defenses. As most organizations are reasonably protected against traditional email-borne malware, the Web channel has become an alternative target for hackers that exploit the multiple vulnerabilities in Web browsers to launch various types of malware attacks, which in most cases are motivated by financial gain. Web-based threats can propagate automatically through drive-by downloads (an infected Web page can sometimes exploit a site visitor's computer remotely without the visitor even having to click on anything), an email message downloaded from a Web-based mailbox, and other techniques. The growing prevalence of Web-based threats that effectively apply these techniques is one of the main reasons for the recent surge in spyware, Trojans, worms, keyloggers, and other malware. In addition, Web-based attacks often employ sophisticated techniques to carry out targeted attacks in order to steal money, identities, or confidential information. Web-based attacks are constantly growing in sophistication. For example, one of the latest trends in Web-based threats is the use of encryption by hackers to hide malicious code in order to evade detection by traditional URL filtering and antivirus solutions that are unable to decode it. In addition, the use of Web-based attacks is one of the drivers for the recent surge in spyware, which is driven by the dramatic increase in the number of Web sites distributing spyware in recent times.

In addition to the inbound threats mentioned above, data loss prevention (DLP) is also becoming a major concern in the Web 2.0 environment for organizations of all sizes, as shown in Figure 1. Government and industry regulations such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, and various SEC regulations are forcing corporations to secure the use of all electronic forms of communications, including the Web. Moreover, preventing leaks of intellectual property via web applications (web email, blogs, etc) has become an equally important concern. This trend is driving the need for information protection and control (IPC) solutions that protect sensitive information and comply with privacy regulations for both Web and web applications.

FIGURE 1

Importance of Monitoring Employee Web 2.0 Use

Q: Using a 5-point scale where 5 is extremely important and 1 is not at all important, please rate the importance of monitoring employee use of Web 2.0 to prevent data leaks and compliance violations



N = 378

Source: IDC, 2007

The Web Security Market in 2006

Performance of Leading Vendors in 2006

Table 1 displays 2006 worldwide revenue and market share for Web security vendors. Worldwide revenue for Web security vendors reached \$1.2 billion in 2006. The top five Web security vendors in 2006 include:

- ☒ Websense led the Web security market in 2006 with \$247 million in revenue and an 22% share of the worldwide market. Websense revenue includes SurfControl acquisition.
- ☒ Trend Micro generated \$145 million in Web security revenue in 2006 and accounted for a 13% share of the worldwide market.
- ☒ Microsoft generated \$87 million in Web security revenue in 2006 and accounted for an 8% share of the worldwide market.
- ☒ Secure Computing generated \$46 million in Web security revenue in 2006 and accounted for a 4% share of the worldwide market.

☒ Check Point generated \$25 million in Web security revenue in 2006 and accounted for 2% share of the worldwide market.

TABLE 1

Worldwide Web Security Revenue by Vendor, 2006 (\$M)

Vendor	2006 Revenue	2006 Share
Websense	\$ 247.5	21.6%
Trend Micro	\$ 145.4	12.7%
Microsoft	\$ 86.9	7.6%
Secure Computing Corp.	\$ 45.8	4.0%
Check Point	\$ 25.0	2.2%
Panda Software	\$ 25.0	2.2%
IBM	\$ 20.7	1.8%
Finjan Software Ltd.	\$ 19.7	1.7%
Sophos	\$ 19.5	1.7%
Ahnlab Inc.	\$ 17.2	1.5%
St. Bernard Software	\$ 14.5	1.3%
8e6 Technologies	\$ 13.8	1.2%
ScanSafe	\$ 13.7	1.2%
Aladdin Knowledge Systems	\$ 12.3	1.1%
McAfee	\$ 10.6	0.9%
Citrix	\$ 8.5	0.7%
SonicWALL	\$ 8.2	0.7%
Norman ASA	\$ 7.0	0.6%
Clearswift Corp.	\$ 6.0	0.5%
Vontu	\$ 5.8	0.5%
Barracuda Networks Inc.	\$ 5.2	0.5%
Webroot	\$ 4.2	0.4%
IronPort Systems	\$ 4.0	0.3%

TABLE 1

Worldwide Web Security Revenue by Vendor, 2006 (\$M)

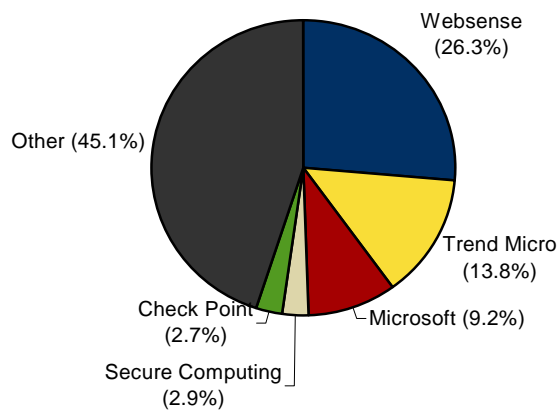
Vendor	2006 Revenue	2006 Share
CA	\$ 3.9	0.3%
Hauri Inc.	\$ 3.2	0.3%
MessageLabs	\$ 1.9	0.2%
Grisoft	\$ 1.9	0.2%
Kaspersky Lab	\$ 1.3	0.1%
Postini	\$ 1.2	0.1%
Subtotal	\$ 780.2	68.0%
Other	\$ 366.5	32.0%
Total	\$ 1,146.7	100.0%

Note: Websense revenue includes SurfControl acquisition

Source: IDC, 2007

FIGURE 2

Worldwide Web Security Software Revenue by Vendor, 2006 (\$M)



Source: IDC, 2007

FUTURE OUTLOOK

Forecast and Assumptions

Web Security Forecast, 2006–2011

Worldwide

IDC's estimate of the growth of the Web security market through 2011 is presented in Table 2 and figure 5. IDC forecasts the Web security market to grow from \$1.2 billion in 2006 to \$2.3 billion in 2011, representing a 15% compound annual growth rate (CAGR). Table 3 shows the key assumptions underlying this forecast.

TABLE 2

Worldwide Web Security Revenue, 2006-2011 (\$M)

	2006	2007	2008	2009	2010	2011	2006-2011 CAGR
Web Security Software	\$ 943.1	\$ 1,039.9	\$ 1,145.0	\$ 1,246.2	\$ 1,354.8	\$ 1,471.8	9.3%
Web Security Appliance	\$ 174.2	\$ 214.5	\$ 283.6	\$ 378.1	\$ 499.9	\$ 648.4	30.1%
Web Security Hosted Services	\$ 34.5	\$ 45.5	\$ 64.2	\$ 94.5	\$ 128.9	\$ 162.0	36.2%
Total Web Security	\$ 1,151.9	\$ 1,299.9	\$ 1,492.9	\$ 1,718.8	\$ 1,983.5	\$ 2,282.2	14.7%

Source: IDC, 2007

ESSENTIAL GUIDANCE

IDC believes the Web will increasingly be used as the threat vector of choice by hackers and cyber criminals to distribute malware and perpetrate identity theft, financial fraud, and corporate espionage. We expect hackers to target the growing number of non-secure Web 2.0 sites that are extremely vulnerable to compromises. Hackers will leverage the popularity of Web 2.0 in order to target the greatest number of Internet users. The practice of hackers planting malicious code on legitimate websites is quickly becoming the norm. Compromises of popular websites by hackers to install malicious code and steal personal or business confidential information will become increasingly more common. It will be no longer sufficient to

only block access to inappropriate websites that often contain malicious code. Web security vendors must also deal with detecting malware on legitimate websites.

Web 2.0 also presents a significant data loss prevention (DLP) challenge for many enterprises. Message boards, blogs, and social networking sites are becoming a pipeline for information leakage and corporate compliance violations. In fact, a recent IDC survey showed that 37% of confidential information leaks occurred via the Web. The same survey also showed that 67% of organizations believed that monitoring employee use of the Web to prevent data leaks and compliance violations was major concern. Given Web 2.0 exposes organizations to both inbound and outbound security threats, IDC believes effective Web Security solutions must analyze traffic bi-directionally.

VENDOR PROFILES

Profiles of Leading Web Security Vendors

Websense

Founded in 1994, Websense, Inc. (NASDAQ: WBSN) is the global leader of web security solutions and an emerging provider of messaging security, endpoint security, and information protection and control solutions. Websense products increase employee internet productivity and secure organizations from emerging internet threats by providing a proactive critical security component that complements traditional security solutions. Websense acquired SurfControl in 2007.

Web Security Solutions

- ☒ Websense Web Security Suite is a leading web security solution that protects organizations from known and new web-based threats. Based on Websense ThreatSeeker technology, Websense Web Security Suite protects against spyware, malicious mobile code, and phishing attacks, bots, and other threats. It also blocks spyware and keylogger backchannel communications from reaching their host servers. In addition, Websense Web Security Suite offers the Websense Web Protection Services that help protect organizations' websites, brands, and web servers.
- ☒ Websense Enterprise, an industry-leading web filtering solution, improves productivity, reduces legal liability, and optimizes the use of IT resources. Websense Enterprise integrates seamlessly with leading network infrastructure products to offer flexibility and control.
- ☒ Websense Express provides content filtering and Internet security capabilities in a simple and affordable solution. It allows organizations under 1000 users to quickly and easily protect their employees from Internet risks by controlling access to inappropriate content and proactively blocking security threats before they have a chance to infect their systems.
- ☒ Websense Content Protection Suite is a comprehensive solution to address the growing need for robust information leak prevention. The solutions helps prevent

internal and external data loss, improve business processes, protect competitive advantage, and manage risk management and compliance.

Strategic Direction

Websense is the worldwide leading vendor in the Web Security market. In recent years, Websense has rapidly enriched its portfolio to play an extended role in the security strategy of the enterprise, and to bring the level of conversation with its clients beyond IT to business issues, including regulation compliance, risk management, productivity, corporate governance, and business continuity. The SurfControl acquisition gives Websense a strong entry into the Web security and hosted services markets. Prior to this acquisition, Websense also acquired PortAuthority Technologies in January 2007, adding information protection and control to its Web security capabilities. Websense believes the acquisitions will create an organization with the scale to compete more effectively with large global security and software companies, and accelerate strategic initiatives with small and medium-sized business (SMB) customers.

LEARN MORE

Related Research

- ☒ *Worldwide Security and Vulnerability Management Software 2007–2011 Forecast and Analysis: Governing Security and Risk Management* (IDC #207658, August 2007)
 - ☒ *The Impact of Security Software Appliances on the Threat Management Security Appliance Marketplace* (IDC #207762, July 2007)
 - ☒ *Worldwide Secure Content and Threat Management 2007–2011 Forecast and 2006 Vendor Shares: 1 + 1 = 4* (IDC #207523, June 2007)
 - ☒ *Worldwide Information Protection and Control (IPC) 2007–2011 Forecast and Analysis: Securing the World's New Currency* (IDC #206750, May 2007)
 - ☒ *Worldwide Mobile Device Security 2007–2011 Forecast* (IDC #206072, March 2007)
 - ☒ *IDC's Software Taxonomy, 20076* (IDC #205437, February 2007)
 - ☒ *Enterprise Security Survey, 2006: The Rise of the Insider Threat* (IDC #204807, December 2006))
-

Methodology

The IDC software market sizing and forecasts are presented in terms of "packaged software revenue." IDC uses the term "packaged software" to distinguish commercially available software from "custom" software, not to imply that the software must be shrink-wrapped or otherwise provided via physical media. Packaged software is programs or codesets of any type commercially available

through sale, lease, rental, or as a service. Packaged software revenue typically includes fees for initial and continued right-to-use packaged software licenses. These fees may include, as part of the license contract, access to product support and/or other services that are inseparable from the right-to-use license fee structure, or this support may be priced separately. Upgrades may be included in the continuing right of use or may be priced separately. All of the above are counted by IDC as packaged software revenue.

Packaged software revenue *excludes* service revenue derived from training, consulting, and system integration that is separate (or unbundled) from the right-to-use license but does include the implicit value of software included in a service that offers software functionality by a different pricing scheme. It is the total packaged software revenue that is further allocated to markets, geographic areas, and operating environments.

The market forecast and analysis methodology incorporates information from five different but interrelated sources, as follows:

- ☒ **Reported and observed trends and financial activity.** This study incorporates reported and observed trends and financial activity in 2006 as of the end of April 2007, including reported revenue data for public companies trading on North American stock exchanges (CY 1Q06–4Q06 in nearly all cases).
- ☒ **IDC's *Software Census* interviews.** IDC interviews all significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.
- ☒ **Product briefings, press releases, and other publicly available information.** IDC's software analysts around the world meet with hundreds of software vendors each year. These briefings provide an opportunity to review current and future business and product strategies, revenue, shipments, customer bases, target markets, and other key product and competitive information.
- ☒ **Vendor financial statements and related filings.** Although many software vendors are privately held and choose to limit financial disclosures, information from publicly held companies provides a significant benchmark for assessing informal market estimates from private companies. IDC also builds detailed information related to private companies through in-depth analyst relationships and maintains an extensive library of financial and corporate information focused on the IT industry. We further maintain detailed revenue by product area models on more than 1,000 worldwide vendors.
- ☒ **IDC demand-side research.** This includes thousands of interviews with business users of software solutions annually and provides a powerful fifth perspective for assessing competitive performance and market dynamics. IDC's user strategy databases offer a compelling and consistent time-series view of industry trends and developments. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.

Ultimately, the data presented in this study represents IDC's best estimates based on the above data sources as well as reported and observed activity by vendors and further modeling of data that we believe to be true to fill in any information gaps.

The data in this study is derived from all the above sources and entered into the Software Market Forecaster (SMF) database, which is then updated on a continuous basis as new information regarding software vendor revenues becomes available. For this reason, the reader should note carefully the "as of" date in the Methodology discussion within the "In This Study" section, near the beginning of this study, whenever making comparisons between the data in this study and the data in any other software revenue study.

Synopsis

This study examines the Web Security market for the period from 2006 to 2011, with vendor revenue and market growth forecasts. Worldwide market sizing is provided for 2006 and a five-year growth forecast for this market is shown for 2007–2011. Revenue and market share of the leading vendors is provided for 2006.

"Web 2.0 exposes organizations to both inbound and outbound security threats" said Brian Burke, program director for IDC's Security Products program "IDC believes effective Web Security solutions must analyze traffic bi-directionally".

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 2007 IDC. Reproduction is forbidden unless authorized. All rights reserved.