

VENDOR PROFILE

WebSense Vendor Profile: Securing Web 2.0

Brian E. Burke

IDC OPINION

Social networking sites such as Facebook, which were once considered to be only consumer applications, are quickly moving into the enterprise environment. Many organizations are struggling with allowing their employees to use Web 2.0 tools responsibly without sacrificing security and regulatory compliance requirements. These environments have created a risk of both data leaks and new channels for malware. However, IDC believes Web 2.0 technologies, if used securely, can help organizations increase collaboration and productivity and drive revenue. This is especially important in today's tough economic climate. Organizations need to balance the business value of Web 2.0 technologies with the risks and security implications of many nonsecure and uncontrolled Web 2.0 environments. The advances in Web 2.0 technologies require a new generation of Web security tools that go well beyond traditional URL filtering. Key trends in the Web security market include:

- ☒ The high volume of user-generated content in the Web 2.0 environment requires that effective Web security solutions have real-time deep content analysis and classification.
- ☒ Web 2.0 presents a significant data loss prevention (DLP) challenge for many enterprises. Message boards, blogs, tweets, and other types of social networking sites are becoming a pipeline for information leakages and compliance violations.
- ☒ The boundaries between consumer and corporate Web 2.0 environments are blurring. IDC believes a growing number of consumer-oriented Web 2.0 technologies will continue to saturate the corporate environment.
- ☒ Many Web 2.0 applications leverage evasive techniques to communicate and share information. The challenge of identifying these applications and applying appropriate policies is a burden many organizations are facing today.
- ☒ The growing number of mobile and remote users is creating a complex distributed workplace. Many corporate applications are being moved to the Web 2.0 environment to allow remote employees to work more efficiently.

IN THIS VENDOR PROFILE

This IDC Vendor Profile features Websense Inc., the worldwide leader in the Web security market (see *Worldwide Web Security 2009–2013 Forecast and 2008 Vendor Shares: It's All About Web 2.0 YouTwitFace*, IDC #219502, August 2009). This Vendor Profile analyzes Websense's range of Web security services, company strategy, and developments in the market. Finally, this Vendor Profile discusses the challenges and opportunities that Websense will face in an increasingly competitive market.

SITUATION OVERVIEW

Company Overview

The Web Security Market in 2008

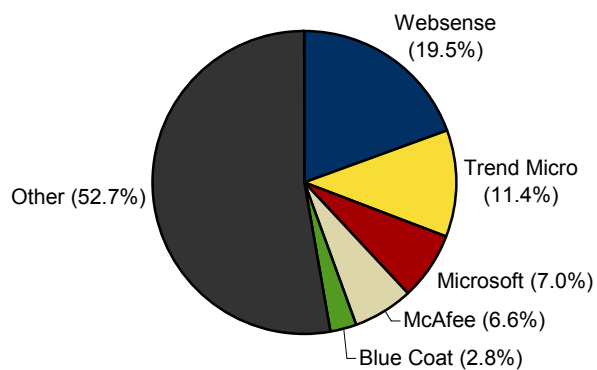
Performance of Leading Vendors in 2008

The worldwide Web security market reached \$1.4 billion in 2008, representing 16% growth over 2007. Figures 1 and 2 and Table 1 display the 2008 worldwide revenue share for Web security vendors. Websense was the worldwide Web security leader in 2007, and it once again leads the pack in 2008 in the total Web security market as well as the Web security software market. Websense is the second-largest vendor in the fast-growing Web security software-as-a-service (SaaS) market.

Websense was the worldwide Web security leader in 2007, and it once again leads the pack in 2008.

FIGURE 1

Worldwide Web Security Revenue Share by Vendor, 2008

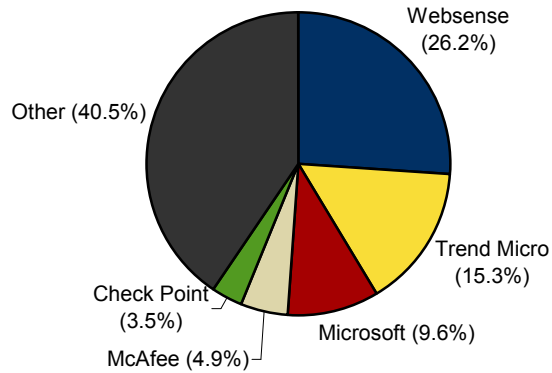


Total = \$1,409M

Source: IDC, 2009

FIGURE 2

Worldwide Web Security Software Revenue Share by Vendor, 2008



Total = \$1,032M

Source: IDC, 2009

TABLE 1

Worldwide Web Security SaaS Revenue by Vendor, 2007–2008 (\$M)

	2007	2008	2007 Share (%)	2007–2008 Growth (%)	2008 Share (%)
ScanSafe	17	23	34.5	35.3	30.3
Websense	3	5	5.5	96.3	7.0
Symantec	3	4	5.1	60.0	5.3
Trend Micro	2	3	4.5	36.4	3.9
Google	2	3	4.1	50.0	3.9
MX Logic	2	3	3.9	57.9	3.9
Webroot	1	3	2.0	150.0	3.3
Blue Coat	1	2	2.0	100.0	2.6
Purewire	–	1	–	NA	0.7
Zscaler	–	1	–	NA	0.7
Subtotal	30	47	61.5	54.5	61.6
Other	19	29	38.5	53.7	38.4
Total	49	76	100.0	54.2	100.0

Source: IDC, 2009

Company Strategy

Websense (Nasdaq: WBSN) is a global leader in integrated Web, data, and email security, providing Essential Information Protection for more than 42 million employees at more than 50,000 organizations worldwide. Headquartered in San Diego, California, Websense distributes its solutions through a global network of channel partners. Websense software and hosted security solutions help organizations block malicious code, prevent the loss of confidential information, and enforce Internet use and security policies. Websense has its roots in Web filtering and continues to develop its core strength in discovering and classifying content across all its product offerings. Websense provides visibility into the internal and external movement of information in the Web 2.0 world, with extensive management of who is authorized to access Web sites, content, or applications, as well as what data must be protected from leaks, where users and data can go online, and how data and online resources can be communicated and used.

Websense (Nasdaq: WBSN) is a global leader in integrated Web, data, and email security, providing Essential Information Protection for more than 42 million employees at more than 50,000 organizations worldwide.

Websense Web Security Gateway allows organizations to secure Web traffic effectively while still enabling the latest Web-based tools and applications. Through a multivector traffic-scanning engine, the Websense Web Security Gateway analyzes Web traffic in real time, instantly categorizing new sites and dynamic content and proactively discovering security risks and blocking dangerous malware.

Using the Websense ThreatSeeker Network, the Websense Web Security Gateway provides advanced analytics, including rules, signatures, heuristics, and application behaviors, to detect and block proxy avoidance, hacking sites, adult content, botnets, keyloggers, phishing attacks, spyware, and many other types of unsafe content. Websense Web Security Gateway also closes a common security gap: decrypting and analyzing SSL-encrypted content before it enters the network.

FUTURE OUTLOOK

The worldwide Web security market is forecast to grow from \$1.4 billion in 2008 to \$2.5 billion in 2013, representing a 12% compound annual growth rate (CAGR). Web security SaaS will be the fastest-growing segment of the Web security market. Web security SaaS will grow from \$76 million in 2008 to \$513 million in 2013, representing a 46.5% CAGR (see Table 2).

TABLE 2

Worldwide Web Security Revenue by Platform, 2008–2013 (\$M)

	2008	2009	2010	2011	2012	2013	2008 Share (%)	2008–2013 CAGR (%)	2013 Share (%)
Software	1,032	1,070	1,115	1,160	1,200	1,239	73.3	3.7	49.3
Appliance	301	360	449	559	670	760	21.3	20.4	30.3
SaaS	76	116	191	295	400	513	5.4	46.5	20.4
Total	1,409	1,545	1,755	2,014	2,270	2,512	100.0	12.3	100.0

Source: IDC, 2009

ESSENTIAL GUIDANCE

Advice for Websense

With Web 2.0 applications, the challenge is to imagine a threat where no perceived threats exist today. As organizations increasingly leverage Web 2.0 for large enterprise projects that involve sensitive data, security will need to be applied to this environment. The tolerance for simply smearing on security after a problem will be seen as increasingly poor, legally deficient, and ignorant of emerging threat environments.

Still, changing behaviors and perceptions require an incremental approach. The first step is monitoring so IT understands the issues and can prepare solutions. The next step is reporting on the findings in such a way that senior executives and business unit managers can understand the benefits of controlled collaboration where customer information and intellectual property (IP) are protected from mistaken, mischievous, and malicious exposure. This phased approach is slow and cumbersome to implement, but necessary. In concert, technologies must support gradual migration while also offering the flexibility to deal with monitoring, reporting, and enforcement. The policy enforcement aspect must be flexible enough to handle both draconian and laissez-faire attitudes toward these environments.

Instead of rolling up into a ball like an armadillo as an instinctive survival tactic or just adopting a laissez-faire process where "anything goes," IDC believes successful organizations should embrace Web 2.0 technologies. Web 2.0 dramatically changes the way solutions must classify content for data leakage, email, and Web threats. These applications and communities will become a major source of malware distribution, identity fraud, privacy violations, and corporate data loss. Organizations must address Web 2.0 technologies with the same security posture as any other business-critical application.

Web 2.0 dramatically changes the way solutions must classify content for data leakage, email, and Web threats.

LEARN MORE

Related Research

- ☒ *Worldwide Web Security 2009–2013 Forecast and 2008 Vendor Shares: It's All About Web 2.0 YouTwitFace* (IDC #219502, August 2009)
- ☒ *Worldwide Messaging Security 2009–2013 Forecast Update and 2008 Vendor Shares: Is Virtual a Reality?* (IDC #219270, July 2009)
- ☒ *IDC's Software Taxonomy, 2009* (IDC #216557, February 2009)
- ☒ *Worldwide IT Security Software, Hardware, and Services 2009–2012 Forecast and 2007 Vendor Shares: The Big Picture* (IDC #216224, January 2009)

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 2009 IDC. Reproduction is forbidden unless authorized. All rights reserved.