

EXCERPT

Worldwide Web Security 2011-2015 Forecast and 2010 Vendor Shares: From Surfing Police to Strategic Security Platform

Phil Hochmuth

IN THIS EXCERPT

The content for this excerpt was taken directly from the Worldwide Web Security 2011-2015 Forecast and 2010 Vendor Shares: From Surfing Police to Strategic Security Platform, by Phil Hochmuth (Doc # 229725). All or part of the following sections are included in this excerpt: IDC Opinion, In This Study, Situation Overview, Future Outlook, Essential Guidance, Learn More, Methodology, and Synopsis. Also included are tables 1 & 2 and figures 1, 2, & 3.

IDC OPINION

Web security technology is evolving from the blocking of bad Web sites to a more strategic security platform, responsible for securing a variety of advanced Web applications, communication channels, and even mobile devices. Some factors increasing the purview of Web security in the enterprise include increased usage of cloud computing (i.e., SaaS and other services, accessed via the Web), the need to protect Web activity on mobile devices (which are increasingly employee owned, but used for business purposes), and increased sophistication of Web-based attacks. All of these factors require more out of Web security software, gateways, and cloud services than basic filtering and blocking features. Enterprises want tighter control over the specific Web applications and services used by their employees (chat applications within a social networking site, the ability to view, but not post, online videos, etc.). This type of activity requires processor-intensive packet inspection and traffic-flow analysis to determine the identity of specific apps and what to do with such traffic streams when identified. Low latency, in order not to disrupt end-users' Web experience, is also a requirement for such Web security activities and is better delivered via hardware appliances (as opposed to server software or SaaS solutions). Such features can be process intensive and lend themselves to dedicated appliances. This is in contrast to the mainly software-based Web security deployments of two to three years ago, which provided basic URL filtering and Web activity monitoring. On the mobile front, Web security SaaS is emerging as a technology for securing mobile devices — such as smartphones and tablets — especially as more of these devices are employee owned and not controlled by corporate IT. Other trends in the current Web security market include:

- ☒ There was rapid growth as the Web security market grew 11.6% overall from 2009 to 2010, with hardware being the fastest-growing platform subsegment.

- ☒ SaaS also grew robustly in this market, with 47.7% year-over-year growth. Software was again the largest subsegment of Web security, but its overall share of the market shrank from 60.1% to 53.1% from 2009 to 2010.
 - ☒ Web security technology must still protect Web end users from embedded Web site malware, as well as online fraud and phishing.
 - ☒ Integrations of Web security with corporate SaaS applications and cloud identity solutions will be key in the near term and into the future.
-

IN THIS STUDY

Methodology

This IDC study examines the worldwide Web security market for the period from 2001 to 2015. Worldwide market size is provided for 2010, with trends from 2009. Revenue and market share of the leading vendors are provided for 2010. The vendor shares, competitive analysis, and forecast contained herein update those found in *Worldwide Web Security 2010–2014 Forecast and 2009 Vendor Shares: Web Security Takes to the Cloud* (IDC #224801, September 2010).

Note: All numbers in this document may not be exact due to rounding.

Web Security Market Definition

Web security includes URL filtering, Web antimalware, Web application firewall, and Web content filtering products. Web security products are deployed on software, appliances, and SaaS platforms. Web security products protect against both inbound (malware) threats and outbound (data leakage) threats.

SITUATION OVERVIEW

The Web Security Market in 2010

The worldwide Web security market reached \$1.7 billion in 2010, growing 11.6% over 2009. Table 1 displays 2009 and 2010 worldwide revenue and market share for Web security vendors. Figures 1–3 display 2010 vendor market share for software, appliances, and SaaS platforms.

TABLE 1

Worldwide Web Security Revenue by Vendor, 2009 and 2010 (\$M)

	2009	2010	2009 Share (%)	2010 Share (%)
Websense	290.7	305.8	19.2	18.1
Trend Micro	167.9	142.0	11.1	8.4
Cisco	89.8	113.2	5.9	6.7
Microsoft	101.3	99.9	6.7	5.9
McAfee	135.8	96.8	9.0	5.7
Barracuda	52.7	82.4	3.5	4.9
Imperva	47.0	67.2	3.1	4.0
IBM	29.2	47.7	1.9	2.8
Check Point	42.3	47.4	2.8	2.8
M86	58.4	36.0	3.9	2.1
AhnLab Inc.	31.4	32.4	2.1	1.9
Blue Coat	31.4	27.8	2.1	1.6
SafeNet	17.8	27.2	1.2	1.6
Citrix	11.6	26.9	0.8	1.6
Symantec	14.4	26.9	0.9	1.6
Kaspersky Lab	8.8	21.2	0.6	1.3
Panda Security	20.9	20.9	1.4	1.2
EdgeWave	24.9	17.3	1.6	1.0
Sophos	14.6	15.7	1.0	0.9
Clearswift Corp.	5.9	13.0	0.4	0.8
F-Secure	12.6	12.3	0.8	0.7
Norman ASA	9.7	10.0	0.6	0.6
F5 Networks	5.9	8.7	0.4	0.5
Webroot	4.2	8.4	0.3	0.5
Google	5.2	5.4	0.3	0.3

TABLE 1

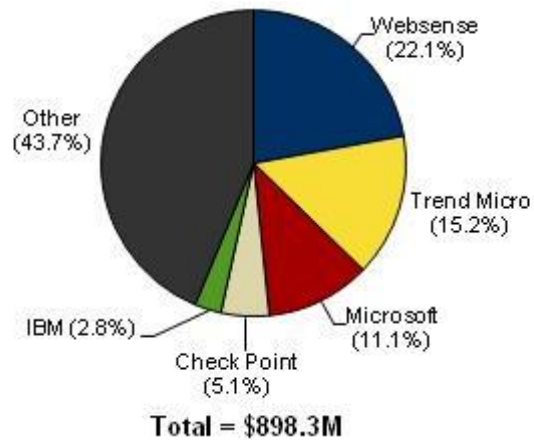
Worldwide Web Security Revenue by Vendor, 2009 and 2010 (\$M)

	2009	2010	2009 Share (%)	2010 Share (%)
WatchGuard (BorderWare)	6.1	4.7	0.4	0.3
CA Technologies	2.5	2.4	0.2	0.1
Subtotal	1,243.0	1,319.4	81.9	77.9
Other	273.8	373.4	18.1	22.1
Total	1,516.8	1,692.8	100.0	100.0

Source: IDC, 2011

FIGURE 1

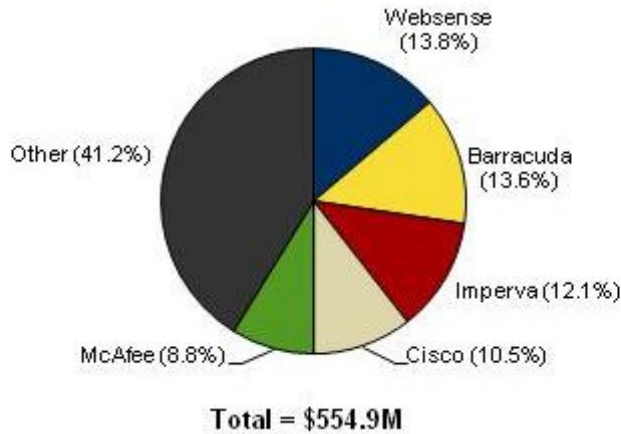
Worldwide Web Security Software Revenue Share by Vendor, 2010



Source: IDC, 2011

FIGURE 2

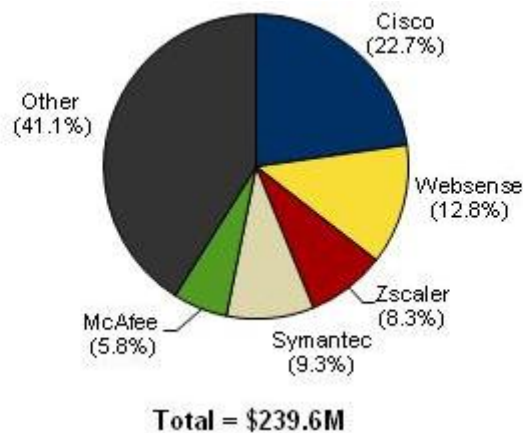
Worldwide Web Security Appliance Revenue Share by Vendor, 2010



Source: IDC, 2011

FIGURE 3

Worldwide Web Security SaaS Revenue Share by Vendor, 2010



Source: IDC, 2011

Performance of Leading Vendors in 2010

Websense was the overall market leader for Web security in 2010, with over \$305 million in product revenue, nearly 65% of this coming from the software category. Websense has shifted its marketing and focus on its V10000 and V5000 line of hardware appliances. The result has been significant revenue shift from software to appliances. Websense's plans here go beyond Web security, however, as it looks to integrate the three pillars of content security — Web, messaging, and DLP — with its TRITON platform, through which each respective content security feature can be

deployed and centrally managed. To that end, Websense saw huge growth in its Web security appliance business in 2010, while its software revenue shrank 7%.

FUTURE OUTLOOK

Forecast and Assumptions

The worldwide Web security market is forecast to grow from \$1.7 billion in 2010 to \$3.0 billion in 2015, representing a 12.1% 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 \$239.6 million in 2010 to \$660.2 million in 2015, representing a 22.5% compound annual growth rate.

Web security appliances will be the second-fastest-growing segment of the Web security market. Web security appliances will grow from \$554.9 million in 2010 to \$1.3 billion in 2015, representing a 17.8% CAGR. (see table 2)

TABLE 2

Worldwide Web Security Revenue by Platform, 2009–2015 (\$M)

	2009	2010	2011	2012	2013	2014	2015	2010 Share (%)	2015 Share (%)	2010–2015 CAGR (%)
Software on-premise	911.5	898.3	942.3	978.8	1,012.1	1,043.4	1,074.2	53.1	35.9	3.6
Appliance	443.1	554.9	677.0	812.4	958.6	1,112.0	1,256.5	32.8	42.0	17.8
Software as a service	162.2	239.6	297.5	384.1	473.3	563.2	660.2	14.2	22.1	22.5
Total	1,516.8	1,692.8	1,916.8	2,175.3	2,444.0	2,718.6	2,990.9	100.0	100.0	12.1

Note: See Table 3 for top 3 assumptions and Table 4 for key forecast assumptions.

Source: IDC, 2011

ESSENTIAL GUIDANCE

Web security will become more critical as applications, and IT services in general, move into the cloud. In an enterprise where a majority of critical applications and services are delivered as SaaS, Web security supplants network security as the most critical control point for enforcing policy, preventing breaches, and monitoring behavior and activity.

Web security will grow in prominence as enterprise applications jump the corporate firewall and move into hosted cloud and SaaS environments. Web security must now address a mix of traffic types with many shades of gray, from corporate SaaS applications, consumer-focused productivity Web apps, and questionable or distracting social media and entertainment apps to plain old Web surfing.

Also necessary is more granular policing of Web traffic; simply blocking access to sites like Facebook or LinkedIn via URLs is no longer an option for many enterprises. However, selective blocking of features, such as chat, video, or messaging apps embedded in such Web sites, is critical to maintain control over end-user activities while not stifling productivity or satisfaction with draconian Web access policies.

LEARN MORE

Related Research

- ☒ *Cisco's ISR/ScanSafe Integration Move Will Ripple Through the Web Security Market* (IDC #cUS22835811, May 2011)
- ☒ *IDC's Worldwide Security Products Taxonomy, 2011* (IDC #227247, March 2011)
- ☒ *Worldwide Web Security 2010–2014 Forecast and 2009 Vendor Shares: Web Security Takes to the Cloud* (IDC #224801, September 2010)

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 2008 as of the end of March 2009, including reported revenue data for public companies trading on North American stock exchanges (CY 1Q08–4Q08 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 interviews with business users of software solutions annually and provides a powerful fifth perspective for assessing competitive performance and market dynamics. 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 revenue 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 IDC study examines the Web security market for the period from 2009 to 2015, with vendor revenue and market growth forecasts. Worldwide market sizing is provided for 2009 and 2010, and a five-year growth forecast for this market is shown for 2011–2015. Revenue and market share of the leading vendors are provided for 2009 and 2010.

"Application control is the new cutting edge of Web security, as URL filtering and antimalware have become standard, basic features in the offerings of Web security product vendors. The ability to monitor and exert control over specific Web applications — from consumerized Web 2.0 apps to enterprise-class SaaS platforms — will be a critical task for Web security gateway technology going forward," says Phil Hochmuth, program director for IDC's Security Products program. "Meanwhile, platform choice for vendors, as well as enterprises, will also become critical, as hardware and SaaS offerings continue to offer complementary and integrated protection capabilities."

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 2011 IDC. Reproduction is forbidden unless authorized. All rights reserved.