

VENDOR PROFILE

WebSense Vendor Profile: At the Center of Content Security Convergence

Phil Hochmuth

IDC OPINION

The social Web phenomenon is now a top security concern among enterprise CIOs and CISOs. Many of the technologies powering social Web technology pose serious risks to enterprises and SMBs, as employees spend increasing amounts of time sharing data, accessing rich Web applications, and mixing consumer-based and enterprise technology. It has never been easier for enterprise employees to push data outside of an organization's perimeter or to access myriad, and potentially unauthorized, applications via the Web. As a result of this market climate, three distinct content security technologies — Web security, messaging security, and data loss prevention (DLP) — are currently on a collision course. And Websense, a provider of content security products and services, is right at the center of the content security market collision, as the company leads the market in Web security, with strong positions in messaging and DLP. The vendor's overall content security portfolio not only spans these three market areas but also has moved to a leadership position across the three security platforms defined by IDC: traditional software, hardware, and software as a service (SaaS). Websense has unified its content security product portfolio under its TRITON solution, providing customers with a common, underlying technology base for deploying, managing, and controlling enterprise content security. IDC finds:

- ☒ Websense has entered the hardware market and seen rapid initial growth. While its market share is small, it has grown rapidly, averaging nearly 40% quarter-over-quarter growth since the product line was introduced, according to IDC's Worldwide Quarterly Security Appliance Tracker. Websense's overall leading position in Web security software and SaaS should lead to more penetration for its hardware platforms — which provide flexible, multifunction capabilities and features.
- ☒ The vendor continues to push a tightly knit hybrid security architecture, where on-premise product capabilities are augmented by cloud-based or SaaS-based services, from traffic scrubbing and filtering done in the cloud to threat intelligence, correlation, and dynamic Web site reputation data, which can be fed down to customer-based products.
- ☒ Its Advanced Classification Engine (ACE) is the core engine behind its overall strategy. This technology provides real-time security and content classification, as well as reputation, antispam/malware, and filtering capabilities, which are both leveraged in on-premise devices and used to feed intelligence to Websense's ThreatSeeker cloud, which provides threat intelligence back to the vendor's installed base of security products.

IN THIS VENDOR PROFILE

This IDC Vendor Profile features Websense Inc., the worldwide leader in the Web security market (see *Worldwide Web Security 2010–2014 Forecast and 2009 Vendor Shares: Web Security Takes to the Cloud*, IDC #224801, September 2010). 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

Websense supplies enterprises with a well-integrated set of Web, messaging, and data protection technologies, delivered via a range of platforms, such as on-premise software and physical hardware appliances, as well as SaaS or "cloud" services. While the company has competed in these three content security markets for years, it introduced its TRITON unified content security solution and control platform in 2010, in an attempt to unify all of its enterprise content security technologies. The underlying engine of TRITON is the Advanced Classification Engine technology, which allows Websense nodes to identify threats dynamically and in real time, as opposed to relying on the traditional threat definitions/signatures updating method. ACE also acts as an intelligence feed into the vendor's worldwide database of URL reputation and content ratings, or ThreatSeeker Network, which is used widely by OEM partners as well as on Websense's own platforms. The Websense Security Labs also provide subscription customers with updates on new threats in addition to the ThreatSeeker data.

Websense has a fairly balanced geographical dispersion in terms of its customers and revenue sources, with its business split approximately in half between the United States and international; of the 50% that is international, about 30% is in EMEA and about 20% is throughout the rest of the world. Over the past three years, the company has successfully expanded more overseas, shifting from over 40% international in 2007.

Company Strategy

TRITON, Websense's unified Web, messaging, and data security platform, is the cornerstone of the company's content security strategy. The TRITON technology unifies the three content security areas, allowing Websense products to recognize and correlate threats across the three technology areas, as well as provide unified management, policy application, and visibility into all aspects of enterprise content security. With this architecture in mind, the next three sections of this document analyze Websense's technology-specific strategies and technology positioning for the three discrete areas of content security, respectively.

Web Security

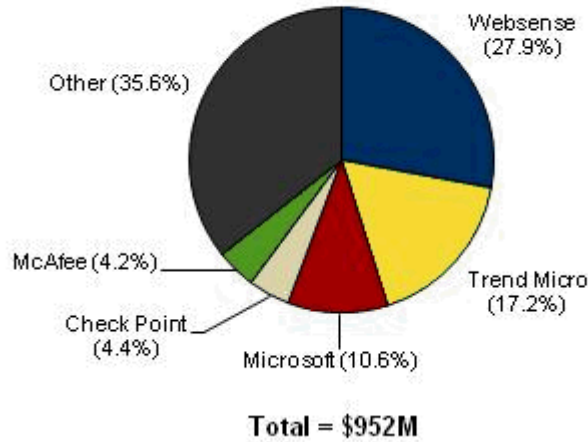
With the advent of social networking and rich Web applications, Websense's Web security products have evolved from simple filters and blocking technologies to more dynamic traffic inspection tools. Websense has been largely successful in this transformation, as the company's Web Security Gateway (WSG) now accounts for the majority of its Web security revenue, as opposed to its more legacy-oriented filtering technologies. WSG adds to basic Web security such features as antimalware, recognition of Web 2.0 applications and traffic flows, and the ability to control these types of activities at a finer level than block/allow. The vendor's strong position in on-premise and SaaS technologies also gives it a competitive hybrid Web security offering, where security can be applied in the cloud as well as on-premise, which is useful for defending against broad Web-based threats (via the cloud) across a distributed organization while providing more specific and localized policy enforcement on-premise.

In late 2009 and in 2010, Websense also introduced its hardware appliances, the V10000 and V5000 (enterprise- and SMB-focused boxes, respectively). While Websense is traditionally a software vendor, some of Websense's customers are beginning to show a preference for the appliance form factor, especially Websense's new WSG customers, which should further drive growth for this product line.

Websense revenue grew in its core market of Web security over the past three years, even during the recession period of 2008–2009, which reflects the importance of Web technology to enterprises. Over this period, Websense, and the market as a whole, also saw a dramatic shift in sales of on-premise Web security software to SaaS Web security. Among Web security software vendors, Websense has the strongest combination of premise-based and SaaS products, in terms of market share (see Figures 1 and 2). (Websense is the market leader in terms of combined on-premise/SaaS products.)

FIGURE 1

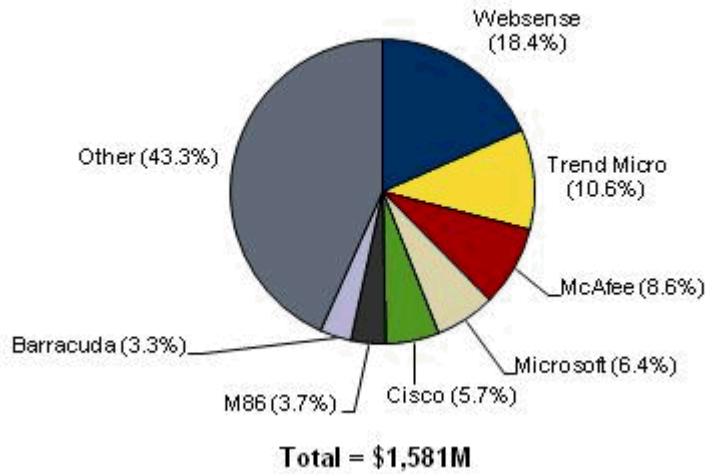
Worldwide Web Security Software Revenue by Vendor, 2009



Source: IDC, 2010

FIGURE 2

Worldwide Web Security Revenue by Vendor, 2009



Source: IDC, 2010

Data Loss Prevention

Websense gained traction in the DLP market in 2009 with its suite of network, endpoint, and discovery products, as well as integration of DLP features into its flagship Web Security Gateway and messaging security platforms. Its revenue surged 148% in 2009, reaching \$20.1 million (approaching its revenue in messaging security) and doubling its market share from 2008, giving it 8% of the total market.

Websense offers a unified Web/messaging product with deep integration of DLP and other information protection and control (IPC)-related features in the platform. This offering is complementary, not a competitive or cannibalistic threat, to Websense's current DLP product portfolio. The focus of a unified Web/messaging/DLP platform will bring additional data protection value to existing Web/messaging customers not currently using DLP. For customers using both WSG and DLP, the initiative promises to bring tighter integration and better security controls, as well as unified policy, reporting, and administration, among components of an enterprise's Websense-based DLP infrastructure and its Web and messaging security platforms.

Messaging Security

In 2009, Websense did just over \$30 million in messaging security; like Web security, the majority of messaging security was sold as on-premise software. SaaS was Websense's fastest-growing platform segment in messaging security, with 50% year-over-year growth. Like Web security, Websense provides a hybrid security option for messaging, with cloud- and premise-based email security tied together from a policy enforcement and filtering standpoint. More often, customers are using both Web and messaging security together to stop so-called "blended" threats of spam, which often deliver embedded malicious Web links. This plays into Websense's Web security strengths, as the majority of its messaging customer base is made up of its Web security customers.

FUTURE OUTLOOK

The greatest opportunity for Websense is to take advantage of its positions in the respective Web, messaging, and DLP as these three technologies rapidly converge. A leadership role in Web security and strong market share in DLP and messaging give Websense a powerful triumvirate of product offerings to take full advantage of this market convergence. The rollout of Websense's TRITON architecture in 2010 provided a good foundation (from both a technology and a marketing standpoint) for offering a unified content security requirement approach for enterprise customers.

The overall market shift to SaaS as a delivery platform for Web and messaging security also plays to the strengths of Websense, as it is among the top 5 vendors in the Web and the messaging SaaS categories. Additionally, the emergence of the hybrid security model gives Websense even more opportunity, as it is a leader in this combination of on-premise/cloud offerings.

The industry shift to Web-based applications, as well as Web 2.0 in general, presents one of the best opportunities for Websense to remain a must-have technology for enterprises. Wider adoption of SaaS in the enterprise — such as salesforce.com,

Oracle Platform for SaaS, and Google Apps — means more enterprise application traffic will flow externally over the Web, as opposed to internally over LANs and WANs. This shift overall puts Websense in a good position to be the security control point for myriad Web traffic types, beyond simply filtering unwanted end-user activities or policing employees' Web activities.

ESSENTIAL GUIDANCE

Advice for Websense

- ☒ Websense must continue to integrate its core Web, messaging, and data protection technologies and make these separate subfunctions into a seamless content security architecture. TRITON is the right platform and go-to-market strategy for this. More is expected to come in 2011, at least from a technical/product capability standpoint. This must also happen from a mindshare/perception standpoint in terms of customers and prospects.
- ☒ Regarding expected competition from IT vendor behemoths, with sights set on DLP/IPC, Websense should align itself with independent professional services or consulting firms in the governance, risk, and compliance (GRC) market, or with value-added security professional services firms servicing heavily regulated markets, such as financial, healthcare, and government. A level of partnering beyond traditional security technology channels (VARs and integrators) will be necessary for success as enterprises move beyond DLP to IPC.
- ☒ Websense must flesh out its IPC portfolio to complement its strong DLP offering. While the company already partners with vendors in the ERM, encryption, and data classification markets (e.g., Check Point, Microsoft, and Voltage), it will be important for Websense to own this technology going forward. Such technologies would greatly complement Websense's DLP enforcement and discovery capabilities, as well as its integrated protection technology in its Web/messaging gateways.

LEARN MORE

Related Research

- ☒ *Worldwide Data Loss Prevention 2010–2014 Forecast and 2009 Vendor Shares: DLP at Crossroads — Market or Feature?* (IDC #225752, December 2010)
- ☒ *Worldwide Messaging Security 2010–2014 Forecast and 2009 Vendor Shares: SaaS Is Here to Stay* (IDC #225194, October 2010)
- ☒ *Worldwide Web Security 2010–2014 Forecast and 2009 Vendor Shares: Web Security Takes to the Cloud* (IDC #224801, September 2010)

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 2010 IDC. Reproduction is forbidden unless authorized. All rights reserved.