



THE RADICATI GROUP, INC.

A TECHNOLOGY MARKET RESEARCH FIRM

1900 EMBARCADERO ROAD, SUITE 206 • PALO ALTO, CA 94303 • TEL. 650-322-8059 • FAX 650-352-2201

Corporate Web Security Market, 2011-2015

Editor: Sara Radicati, PhD; Principal Analyst: Masha Khmartseva

SCOPE

This study provides an analysis of the Corporate Web Security Market in 2011 and its potential growth over the next four years. It offers a detailed analysis of worldwide market trends, market size and growth forecasts, market share by vendor, vendor products and strategies, and more.

- The Web Security market is comprised of solutions that provide inbound and outbound security to organizations, protecting against the myriad of threats that exist on the Internet today. These threats can include viruses, various forms of spyware, phishing attacks, and other types of malware.
- Solutions in this market can be deployed in multiple form factors, including software, appliances, cloud services, as well as hybrid solutions.
- This report focuses exclusively on corporate deployments, which include government and educational organizations, but does not include service provider deployments.

All market numbers, such as market size, forecasts, installed base, and any financial information presented in this study represent worldwide figures, unless otherwise indicated. All pricing numbers are expressed in \$USD.

METHODOLOGY

The information and analysis in this report is based on primary research conducted by The Radicati Group, Inc. It consists of information collected from vendors, and users within global corporations via interviews and surveys.

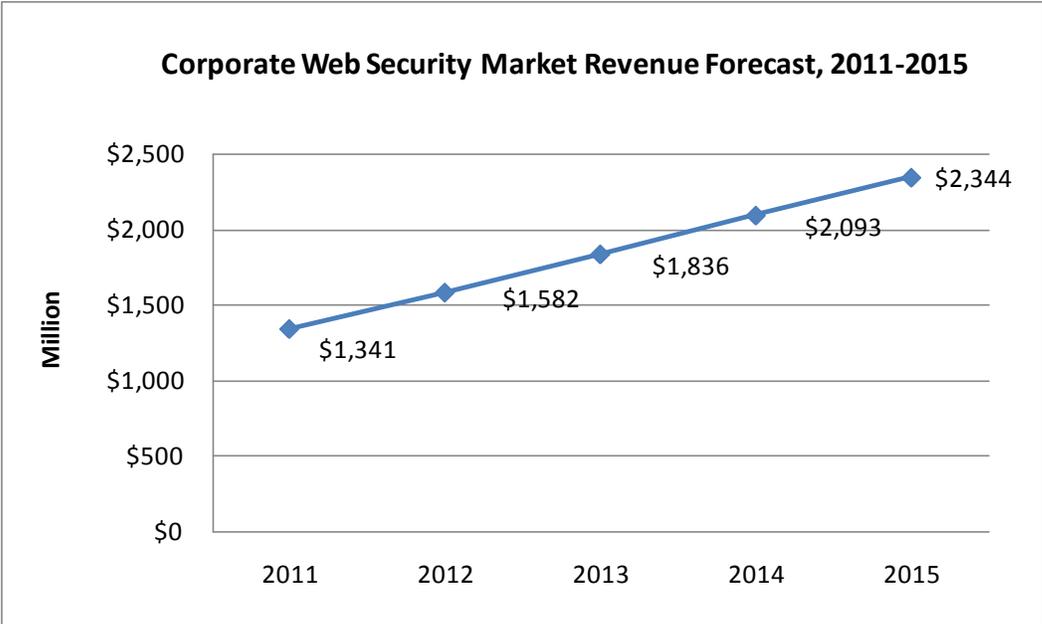
Secondary research sources have also been used, where appropriate, to cross-check the information collected. These include company annual reports and market size information from various market segments of the computer industry.

EXECUTIVE SUMMARY

- Web Security is defined as any software, appliance, or hosted service that protects corporate users and networks from Web-based malware, enables organizations to control employee behavior on the Internet (URL filtering), and helps prevent data loss.
- Most vendors and service providers offer a single solution for malware, URL filtering, and DLP protection. However, there are still a few vendors today that offer these capabilities to customers separately.
- Since many players in this market also offer e-mail security solutions, they often share a common anti-malware and reputation engine to enable vendors to gain a better insight into the malware outbreaks of e-mail and Web customers (especially those that occur via blended attacks).
- Malware attacks are on the rise, and they are expensive to clean up. According to our estimates, in 2011, a 1,000-user company spends over \$287,000 per year to defend against and clean up malware attacks, occurring across over all corporate channels.
- While many organizations, today, are still not convinced that social media sites (Facebook, Twitter, etc.) are important for their businesses, and prefer to simply block them, a growing number of customers are starting to see the benefits of allowing access to social media sites, while also being concerned about potential dangers. To create a safer dynamic site browsing environment, a number of Web security vendors are now offering monitored Facebook and Twitter access, enabling organizations to specify when, and how employees can access social

media web sites, what pages/applications they can see/use, what documents can and can't be downloaded/uploaded, as well as for how long users can stay there.

- To enable easier and more flexible deployment of their solutions, over the past 12 months many Web security vendors, who offer Web security solutions as appliances, have added a virtualization option. Today, VMware is the most popular virtualization platform in use by most Web security vendors.
- Data loss prevention is becoming a significant market driver, however most Web security vendors today do not really offer true DLP protection with deep content inspection, and hence their customers have to settle for simple keyword analysis combined with application blocking.
- The highly anticipated deployment of hybrid solutions is starting to happen, but their numbers are still not huge. Combining on-premises appliances with services in the cloud, hybrid deployments are most beneficial for larger organizations with multiple locations. We do believe though that the deployment of hybrid solutions will pick up, as soon as vendors will be able to demonstrate that these solutions are much more efficient in cleaning up traffic from malware, and offer more convenient user controls as opposed to regular appliances or pure services.
- In 2011, the majority of Corporate Web Security revenue is generated by large and very large organizations. By 2015, we expect small and medium businesses will make up a relatively larger portion of the market, as overall pricing decreases, as well as more solutions become available as services, which are easier to deploy and manage even for smaller organizations.
- The worldwide revenue for corporate Web security solutions is expected to grow from over \$1.3 billion in 2011, to over \$2.3 billion in 2014.



To view the complete Table of Contents for this report, visit our website at www.radicati.com.