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, 2013-2017

Editor: Sara Radicati, PhD; Principal Analyst: Thomas Buckley

SCOPE

This study provides an analysis of the Corporate Web Security market in 2013 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 Corporate Web Security market is comprised of solutions that provide inbound and outbound security to organizations, protecting against the many 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 are based on primary research conducted by The Radicati Group, Inc. Our proprietary methodology combines information derived from three principal sources:

a. Our Worldwide Database which tracks user population, seat count, enterprise adoption and IT use from 1993 onwards.
b. Surveys conducted on an on-going basis in all market areas which we cover.
c. Market share, revenue, sales and customer demand information derived from vendor briefings.

Forecasts are based on historical information as well as our in-depth knowledge of market conditions and how we believe markets will evolve over time.

Finally, secondary research sources have also been used, where appropriate, to cross-check all the information we collect. These include company annual reports and other financial disclosures, industry trade association material, published government statistics and other published sources.

Our research processes and methodologies are proprietary and confidential.

EXECUTIVE SUMMARY

- Web security is one of the most fundamental security solutions that an organization can deploy. Access to the Web is arguably the most important tool for workers in any organization. Providing safe Web access that encourages productivity is paramount in a successful organization.

- Corporate 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, and helps prevent data loss. Corporate Web Security solutions can be deployed on-premises, in the cloud, or as a hybrid solution. Regardless of deployment method, Corporate Web Security solutions are a cornerstone to IT security in the enterprise.

- Web threats continue to become more advanced and prevalent. Websites are becoming bloated with nested objects that most users pay little attention to. Each of these elements on a webpage can be pulled from a different domain, and one webpage can easily have dozens of domains that it pulls from. Furthermore, access to malware is becoming much easier with exploit kits. Anyone can buy an exploit kit with relative ease that gives the buyer access to tools that can exploit machines via software flaws. These kits are easy to use and do not require any technical know-how. The threats out there have usually been focused on financial gain, but sometimes cyber criminals are content with just being disruptive.

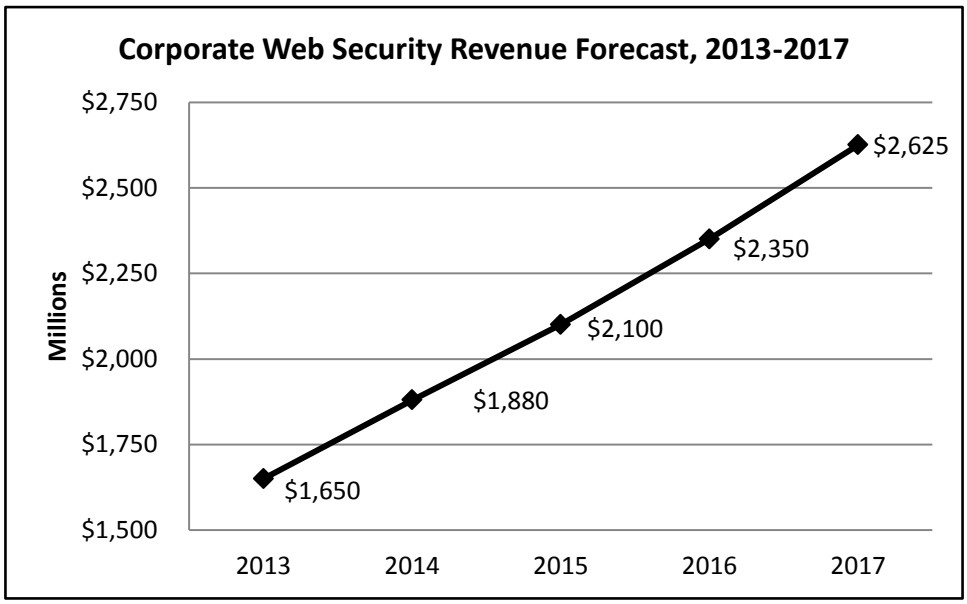
- The user, not merely the operating system, is also being attacked. Malware is becoming much more targeted through social engineering. Phishing attempts that used to be broadly targeted to anyone with an email address have now morphed into much more targeted attempts to trick users into giving up their passwords. This practice, called “spear phishing”, creates tailored traps for victims using publicly available information from social networks, such as Facebook. This has changed the threat landscape from random, mass targeting to specific, singled-out targeting. These types of attacks rely fully on deceiving the user, which makes it more difficult for a Corporate Web Security solution to intervene.

- Blended attacks are also a very common way in which malware infiltrates an organization. Web access, is usually one of the components in a blended attack. Organizations which deploy a Corporate Web Security solution can help eliminate or significantly reduce this type of attacks.

- Incoming malware is a huge risk, but outgoing risks (e.g. confidential data loss via webmail) can be just as worrisome. Productivity controls are also a key driver of growth.

- Hybrid solutions (i.e. a mix of on-premise and cloud-based solutions) are beginning to become more popular for Corporate Web Security deployments as organizations treat them as a stepping-stone in moving from an on-premises to a cloud-based deployment. Most hybrid solutions still have separate management interfaces for the cloud-based piece, which can make management of a hybrid solution more cumbersome. A few vendors, however, are now able to offer a unified interface for hybrid deployments, which is a key strength that allows their customers to easily transition and migrate their policies to an entirely cloud-based approach.

- The worldwide revenue for Corporate Web Security solutions is expected to grow from over $1.6 billion in 2013, to over $2.6 billion in 2017.



Corporate Web Security Market Revenue Forecast, 2013 – 2017

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