Cloud Security Services, 2011-2015

Editor: Sara Radicati, PhD; Principal Analyst: Daniel Oh

SCOPE

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

This report deals only with Cloud Security Services designed to protect business organizations (including government and educational institutions) rather than service providers or data centers.

While some providers in this market may offer suite solutions that include email archiving and other non-security features, the, installed base and revenue numbers in this study do not include these additional services.

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.
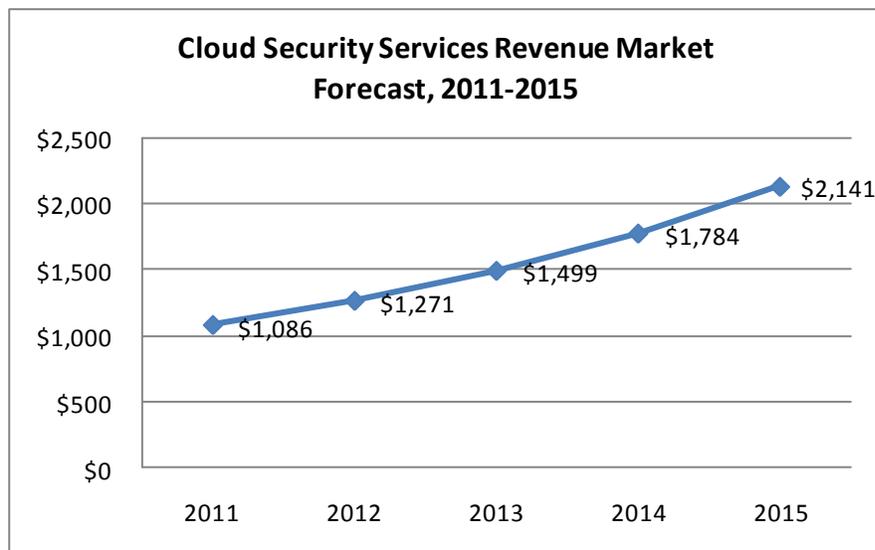
METHODOLOGY

The information and analysis in this report is based on primary research conducted by The Radicati Group, Inc. It consists of information collected from service providers and users 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

- Cloud Security Services are becoming increasingly popular in providing protection against web-based threats, email-based threats, and data leakage. These services help protect the corporate network from external threats, such as malware, phishing attacks, and hackers, as well as potential internal threats that may derive from data leakage.

- One of the major emerging security threats, today, is users connecting to the corporate network from remote locations. A key advantage of deploying cloud-based security services is that they are inherently designed to support remote users and offer them the same level of protection provided to on-site workers. As remote users connect through a Cloud Security Service, all of their web traffic and emails are sent through the same security filters, ensuring that potential threats are quickly identified and blocked.

- Social networking sites such as Twitter and Facebook are finding increasing adoption amongst businesses. While some companies prefer to block social networking usage outright, others are opting for a more light-handed approach by limiting social networking usage. Granular controls over social media and Web 2.0 sites provide businesses with flexibility in their web usage policies, which allows users to leverage social media and Web 2.0 for their work, while preventing use of these websites for non-work related purposes.

- Media rich content scanning is becoming an industry standard for both hosted email and web security vendors. Hosted email security providers are starting to implement attachment scanning that can process file archives, images, PDF files, and more to ensure that there is no malicious or inappropriate content in the message. Hosted web security providers are beginning to become sophisticated enough to scan through media-rich Web 2.0 websites and root out malicious code embedded within the site before it can threaten the user.

- Most Cloud Security Service vendors support endpoint protection, but few extend that protection to all mobile handsets and tablets. The increasing trend of "Bring Your Own Device (BYOD)" in the workplace has IT administrators worried over the different types of devices that they will have to secure. Workers have been pushing for corporate network access from their personal consumer devices, like smartphones and tablets. As a result, some Cloud Security Services are focusing on mobile endpoint support to help secure the wide range of personal mobile devices that are being brought into the workplace at an increasingly fast rate.

- Among the most prolific threats in the past 12 months, phishing and blended attacks have been a priority for both businesses and security vendors to suppress. A number of large companies have fallen victim to phishing attacks in the last 12 months (including security vendor RSA) and as a result, many Cloud Security Services have improved their protection against phishing and blended attacks. These attacks are becoming increasingly sophisticated, with some phishing attacks harvesting headers and footers from company emails to look more realistic, while others utilize a blended approach and insert a link into the message in order to bypass traditional filters.

- Revenue for Cloud Security Services is expected to increase steadily, growing from over $1 billion in 2011, to $2.1 billion in 2015. Average annual revenue growth is expected to be about 18%.

Cloud Security Services Revenue Market Forecast, 2011-2015

Year	Revenue
2011	$1,086
2012	$1,271
2013	$1,499
2014	$1,784
2015	$2,141

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