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

# *Endpoint Security Platforms Market, 2012-2016*

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

## SCOPE

This study provides an analysis of the Endpoint Security Platforms market in 2012 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 Endpoint Security Platforms market is comprised of solutions that provide security to all endpoints in organizations, protecting against the myriad of threats that exist in today's digital world. These threats can include viruses, malware, data loss, inbound network intrusion attempts, and much more.

- 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. It does not include consumer endpoint security platforms.

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

- An endpoint security platform offers organizations a solution to monitor, manage, and protect all the endpoints on an enterprise network. These endpoints can be secured through a variety of methods, such as a server on the network or in the cloud, software on an endpoint, or other means. The most common endpoints secured in the enterprise have traditionally been desktop computers. However, endpoints can also include a variety of other machines, such as virtual desktops, tablets, mobile devices, credit card readers, and more.

- One of the most fundamental elements of securing an endpoint starts with malware protection. Malware can surface in a variety of ways on an endpoint. It can enter through an email, on the Web, a downloaded file, or a plethora of other routes. The primary purpose of an endpoint security platform is to protect an organization from these threats, no matter how they enter the network. As a result, endpoint security platforms usually have all the necessary tools to block malware from entering the network. Email security, web security, antivirus security, and other malware prevention techniques are all common features in an endpoint security platform.

- Endpoint security platforms also include a broad range of other features to help secure endpoints. Device control, application blocking, locking down of ports, and more are a few of the features that can be found in most endpoint security platforms that aid in the managing, monitoring, and protecting of endpoints.

- Tablets and mobile devices are becoming a larger presence in the enterprise as employees are increasingly using one or more smartphones and tablets to work anywhere, anytime. These mobile

devices are still endpoints that are susceptible to malware, data loss, and more.

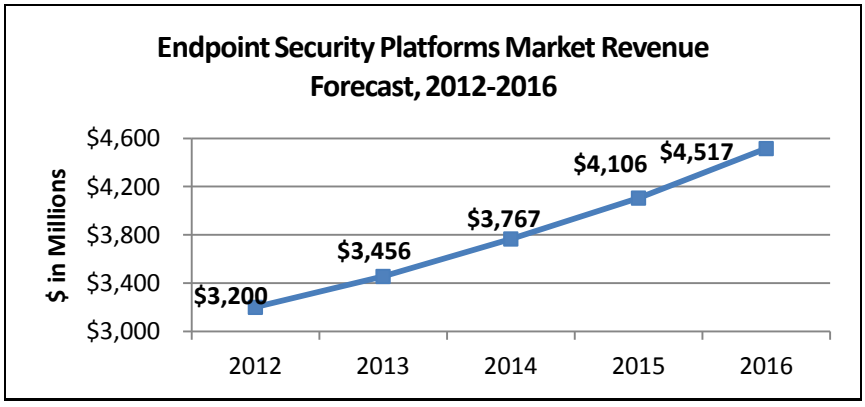
- Firewalls in endpoint security platforms are commonplace. Monitoring of outbound traffic is a key feature of firewall functionality. A powerful firewall will be able to block application access to the network and block or allow specific IP addresses. Firewalls are also commonly bundled with an intrusion prevention system or other similar system that blocks unwanted incoming traffic at the network layer.

- Vendors are increasingly offering a cloud-based option for endpoint security deployments. Cloud deployments are driven by the increased trend of borderless enterprises where the users work from home or while on the road and need quick, secure access to the business network.

- Endpoint security platforms continue to add increased functionality that are bringing them to the point of being the only security solution an organization needs to deploy. Soon, businesses may no longer need a separate solution for DLP or Web security since endpoint security platforms are increasingly including these capabilities.

- Malware attacks have been trending up dramatically as more attacks happen each year. A recent survey found that 46% of users surveyed had experienced malware attacks, averaging 5.2 attacks per user/year. According to the survey, it took organizations an average of 3.9 hours to clean up each infection.[1] These results show growth from a similar survey the previous year that revealed that 30% of users experienced malware attacks each year, averaging 2.1 attacks per user per year, and it took organizations an average of 2.8 hours to clean up each infection.[2]

- The worldwide revenue for enterprise endpoint security platforms is expected to grow from $3.2 billion in 2012 to over $4.5 billion in 2016.




[1] Survey - Security Archiving and Compliance Survey 2011 - 2012, The Radicati Group, Inc.
[2] Business User Survey, 2010-2014, The Radicati Group, Inc.

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