



THE RADICATI GROUP, INC.

A TECHNOLOGY MARKET RESEARCH FIRM

PALO ALTO, CA 94301

TEL. 650 322-8059

Endpoint Security Market, 2014-2018

SCOPE

This study provides an analysis of the business Endpoint Security market in 2014 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 market is comprised of solutions that secure 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 business endpoint security solutions. It does not include consumer endpoint security solutions.
- Government organizations are considered "corporate organizations" for the purposes of this report.

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.

EUROPE: LONDON NW3 5JY • TEL. +44 (0)207 794 4298

Email: admin@radicati.com

<http://www.radicati.com>

METHODOLOGY

The information and analysis in this report is 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

- Endpoint security solutions provide organizations with a way to monitor, manage, and protect all the endpoints on their networks. Traditional endpoints requiring protection have been desktop computers, and laptops. Endpoints today, however, include a myriad of other computing devices, such as servers on the network or in the cloud, virtual desktops and servers, credit card readers, removable disk drives or USB devices, mobile phones and tablets, and more.
- Endpoint protection begins with malware detection, however, endpoint security is much more than just malware detection. Endpoint security solutions will typically

also include device control, application blocking, locking down of ports, and more. All these features are provided to aid in managing, monitoring, and protecting all endpoints.

- Endpoint security solutions often include some form of Data Loss Prevention (DLP) functionality. While this is not a substitute for full content-aware DLP deployment, the availability of some DLP capabilities is nevertheless an important area of differentiation among vendors.
- Endpoint security vendors are increasingly offering cloud based options for their endpoint security deployments, some vendors offer exclusively cloud based solutions. The growing adoption of cloud based solutions for many applications, and in particular email, has led many organizations to feel more open to the adoption of cloud based solutions for security as well.
- Despite the growing importance of mobile devices in organizations of all sizes, endpoint security vendors, still have very different views on the right level of mobile protection that should be part of their endpoint security solutions. Some vendors do not include mobile protection at all, and choose to view it as a separate function that should be provided by a specialized Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) solution. These vendors may offer such an add-on of their own, or partner with a third party vendor. Other vendors view mobile device protection as an integral part of their endpoint security solutions and offer a rich set of features focused on mobile endpoint protection.
- Device control is also an increasingly common requirement for endpoint security solutions. Proper device controls can prevent most confidential data from leaving organizations. While there are also other avenues for stealing confidential information (e.g. printing, emailing, etc.) these tend to leave behind a digital footprint. Information loss from improper USB device use, on the other hand, is much more difficult to track.
- The Endpoint Security market was considered saturated and commoditized in recent years. However, it is now showing renewed growth as more organizations are re-evaluating their vendor relationships and investing in new, higher function Endpoint

Security solutions.

- Worldwide revenue for business Endpoint Security solutions is expected to grow from over \$4.1 billion in 2014, to more than \$7.1 billion in 2018. An annual growth rate of 15%.

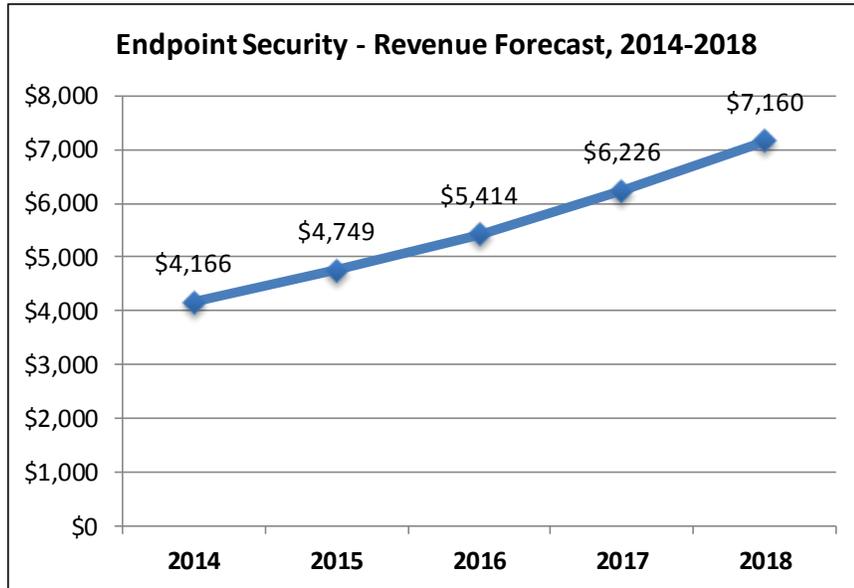


Figure 1: Endpoint Security Revenue Forecast, 2014 – 2018

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