



THE RADICATI GROUP, INC.

A TECHNOLOGY MARKET RESEARCH FIRM

WWW.RADICATI.COM

TEL. 650 322-8059

Advanced Persistent Threat (APT) Protection Market, 2017-2021

SCOPE

This study provides an analysis of the Advanced Persistent Threat (APT) Protection market in 2017 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 Advanced Persistent Threat (APT) Protection market consists of solutions that provide detection, prevention and possible remediation of zero-day threats and persistent malicious attacks. APT Protection solutions may include but are not limited to: sandboxing, reputation networks, threat intelligence management and reporting, forensic analysis and more.

This report focuses exclusively on corporate deployments, which include civilian government organizations and educational institutions. It 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.

EUROPE: LONDON, UK • TEL. +44 (0)20 7794 4298

Email: admin@radicati.com

<http://www.radicati.com>

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

- Advanced Persistent Threat (APT) Protection solutions are a set of integrated solutions for the detection, prevention and possible remediation of zero-day threats and persistent malicious attacks. APT solutions may include but are not limited to: sandboxing, reputation networks, threat intelligence management and reporting, forensic analysis and more.
- Web access and email continue to be the most prevalent methods through which APT attacks can enter an organization. While many security solutions focus on network level APT attacks, the most prevalent and successful attacks tend to come through applications, such as email and web access. Therefore, it is essential for vendors to

provide solutions that can intelligently identify and correlate information about a potential attack across multiple sources and channels.

- Threats are also becoming more targeted and personal. Blended attacks which present users with some information they recognize and request that they connect to a site to input more information are becoming more prevalent and highly successful. The user is typically totally unaware of the attack and can simply serve as a pass through allowing a threat to spread through an entire organization's network.
- APTs are very difficult to detect and remove as they will not obviously appear to be malware and may be planted very deeply into an organization's computing systems. In addition, the designers and initiators of the APT will consistently monitor and guide its activities by changing its code to evade detection and morph into an ever-changing set of behaviors. Typically, an organization that has been infiltrated will not even be aware of it and may only become aware at a much later time through monitoring of outbound communication activity, or through log analysis via Security Information and Event Management (SIEM) tools.
- Sandboxing is no longer enough and most vendors recognize that while sandboxing is a key element of an APT solution, it alone cannot be considered sufficient APT Protection. Sandboxing needs to fully integrate with a network-wide threat intelligence service in order to help collect, correlate and distribute threat information across all network and computing resources.
- The worldwide market for APT Protection solutions continues to show strong growth, as security concerns grow and organizations of all sizes decide to invest in more sophisticated protection solutions. The total market revenue for APT Protection solutions is expected to grow from over \$3.2 billion in 2017, to over \$7.5 billion by 2021.

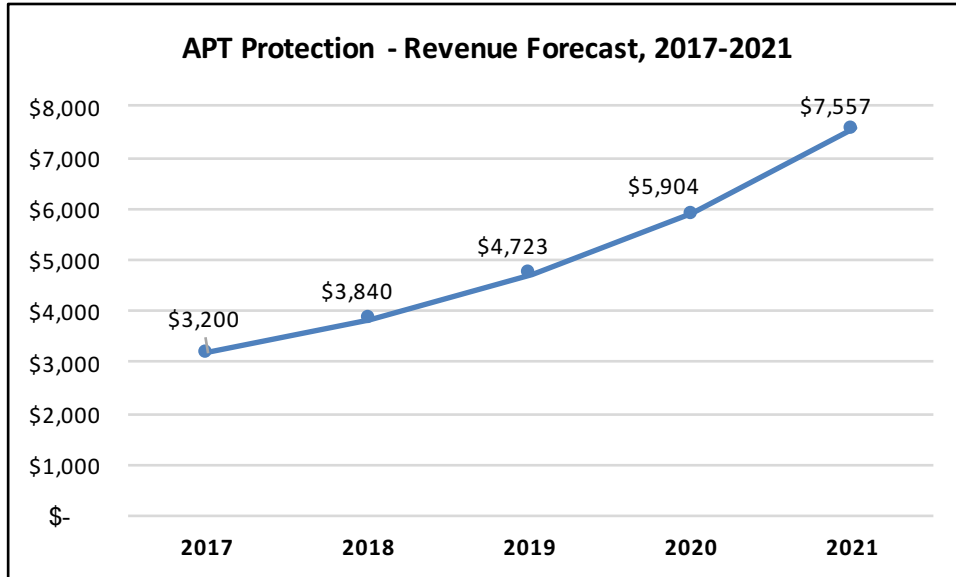


Figure 1: APT Protection Market Revenue Forecast, 2017 – 2021

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