



THE RADICATI GROUP, INC.

A TECHNOLOGY MARKET RESEARCH FIRM

WWW.RADICATI.COM

TEL. 650 322-8059

Advanced Persistent Threat (APT) Protection Market, 2020-2024

SCOPE

This study provides an analysis of the Advanced Persistent Threat (APT) Protection market in 2020 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 Protection Solutions offer detection, prevention and possible remediation of zero-day threats and persistent malicious attacks. APT solutions may include but are not limited to: sandboxing, EDR, CASB, reputation networks, threat intelligence management and reporting, forensic analysis and more.
- Advanced Persistent Threat (APT) refers to a set of malicious activities intended to penetrate an organization's computing resources with the objective to gain information illicitly and/or cause damage to the organization. Unlike traditional malware, APT's focus is on stealing information, rather than simply planting a virus or causing damage. Once a sufficient amount of information is extracted it may be used to cause further damage through ransom requests, open disclosure, sale of the

information to third parties, and active interference with the target organization's business.

- APTs will typically target business organizations or national government entities, and are initiated by an organized group of individuals, or a state run agent. APTs are designed to penetrate an organization's cyber defenses and install a backdoor or multiple backdoors through which to gain access to information. APTs may also sometimes masquerade as legitimate administrative actions, causing disruption and further gaining a foothold into the target organization.
- Organizations, which fall victim to APTs may not become aware of the attack until considerable damage has occurred. In addition, victim organizations will often be reluctant to disclose the attack and the extent of the damage they incurred. This makes it very difficult to identify and stop APTs on a wider scale.
- Web access and email are still the most prevalent methods through which attacks creep into organizations. 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.
- Market adoption of APT Protection solutions continues to see strong growth with organizations of all sizes. The worldwide market revenue for APT Protection solutions is expected to grow from over \$5.1 billion in 2020, to over \$10.5 billion by 2024.

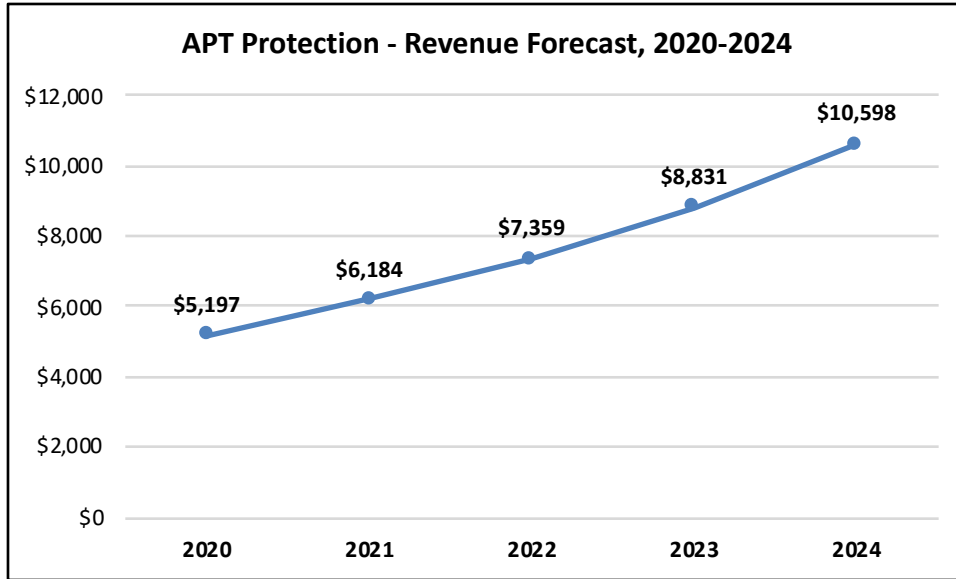


Figure 1: APT Protection Market Revenue Forecast, 2020 – 2024

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