

## **Penetration Testing - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029**

Market Report | 2024-02-17 | 100 pages | Mordor Intelligence

### **AVAILABLE LICENSES:**

- Single User License \$4750.00
- Team License (1-7 Users) \$5250.00
- Site License \$6500.00
- Corporate License \$8750.00

### **Report description:**

The Penetration Testing Market size is estimated at USD 4.25 billion in 2024, and is expected to reach USD 12.76 billion by 2029, growing at a CAGR of 24.59% during the forecast period (2024-2029).

#### Key Highlights

- The increasing number of cyber-attacks, coupled with the growing need to meet compliance measures, is anticipated to be a growth driver for the global penetration testing market during the forecast period.
- The increasing demand for the protection of software-based properties such as mobile and web applications is anticipated to boost the growth of the global penetration testing market. Additionally, the increasing use of cloud-based security solutions is expected to fuel the demand for penetration testing. This, in turn, is anticipated to foster the growth of the global penetration testing market. Moreover, the increasing digitization in developing countries is expected to increase the trend of Internet of Things (IoT)-based connected devices. This, in turn, drives the demand for penetration testing.
- The growing internet activities globally, coupled with the increased security compulsion, are driving the market growth of the global penetration testing market during the forecast period.
- Moreover, an increasing number of wireless networks and the growing number of connected devices are also generating demand for penetration testing across various industry verticals. However, the lack of skilled personnel and awareness in various developing and underdeveloped countries is likely to restrain the growth of the penetration testing market during the forecast period.
- Also, during Covid-19, businesses worldwide faced challenges in terms of carrying out operations due to the widespread closure of workplaces and other facilities. The danger of cyberattacks is growing as people use technology more and more to remain in touch and run their companies effectively, particularly during the pandemic. Due to this, the need for cutting-edge digital networks increased dramatically.

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scott's-international.com](mailto:support@scott's-international.com)

[www.scott's-international.com](http://www.scott's-international.com)

-Employees are accessing business networks and data using their devices that need to be adequately secure due to the growing trend of working from home (WFH), which exposes exploitable weaknesses to cyberattacks. Additionally, many companies have created and updated their current web- and mobile-based apps due to the increased adoption of digital transformation to meet the growing demand for customers to shop online, opening up possibilities for cyberattacks. The adoption of hybrid working methods by numerous sectors may increase the demand for vulnerability testing in the short term.

## Penetration Testing Market Trends

### Growing Requirement of Penetration Testing among Government and Defense

- The government and its agencies have the authority to access and manage large amounts of sensitive citizen information. Further, with the advent of the digital age, governments have leveraged online web portals and mobile applications to enhance government procedures and processes. For instance, the government of India has begun a digital movement, "Digital India," intending to digitize all government processes and payments.
- Infrastructure development is emerging as one of the priorities for governments, including deploying public Wi-Fi and connected public transport. As a result, there is a need for government organizations to secure the network and its applications to protect the integrity of citizen information on a large scale. This has created a greater vulnerability to sensitive data.
- Further, technologies, such as commercial off-the-shelf (COTS), are used by federal governments to enable broad functional capabilities for government applications. Since these solutions were developed for commercial purposes, government systems are vulnerable to certain unique risks that must be addressed.
- Thus, software vendors developing technology for the government have been pushed to ensure security for static and dynamic applications through compliance measures and mandates, such as the National Institute of Standards and Technology (NIST) risk management framework (RMF) and the Department of Defense Information Assurance Certification and Accreditation Process (DoD DIACAP). These mandates demand that vendors guarantee testing services and verification of their applications. The abovementioned factors are expected to propel the market's growth studied over the forecast period.

### North America to Hold Major Share

- The region is a technology hub. Therefore, the Federal government has made stringent rules regarding security testing services. Moreover, it is made compulsory for industries like BFSI to adhere to compliance testing.
- According to International Telecommunication Union (ITU), North America is the most proactive and committed region regarding cyber security-based initiatives. The GCI score given to the major countries (United States - 0.91 and Canada - 0.81) further reinforces their commitment to building a robust cybersecurity framework and enhanced security testing methodologies. Businesses in the region look forward to installing penetration testing, security, and vulnerability management solutions and have the best practices for regular business operations.
- Moreover, employees are accessing business networks and data using their devices that are not adequately secure due to the growing trend of working from home (WFH), which exposes exploitable weaknesses to cyberattacks. Additionally, many North American companies have created and updated their current web- and mobile-based apps due to the increased adoption of digital transformation to meet the growing demand for customers to shop online, opening up possibilities for cyberattacks.
- Companies across the region are anticipated to double down on necessary security arrangements such as a layered defense with firewall, filtered DNS, segmented networks, security clients, etc. However, employee awareness and training might be the investment that brings the highest ROI for companies.

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

## Penetration Testing Industry Overview

The penetration testing market is highly competitive and consists of several major players. In terms of market share, few of the major players currently dominate the market. These major players with a prominent market share are focusing on expanding their customer base across foreign countries. These companies are leveraging strategic innovations and collaborative initiatives to increase their market shares and increase their profitability. Security giants like Symantec and FireEye have offered pen testing for years, and other bug bounty players like Bugcrowd and Synack also conduct crowdsourced pen tests.

In May 2022, Cisco Inc. released a cybersecurity assessment tool to help small and medium-sized companies (SMBs) in the Asia Pacific area better understand their security posture.

### Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

### Table of Contents:

#### 1 INTRODUCTION

- 1.1 Study Deliverables
- 1.2 Study Assumptions
- 1.3 Scope of the Study

#### 2 RESEARCH METHODOLOGY

#### 3 EXECUTIVE SUMMARY

#### 4 MARKET DYNAMICS

- 4.1 Market Overview
- 4.2 Introduction to Market Drivers and Restraints
- 4.3 Market Drivers
  - 4.3.1 Increasing Security Threats
  - 4.3.2 Stringent Government Regulations Regarding Data Security
  - 4.3.3 Growing Requirement of Penetration Testing among Government and Defense
- 4.4 Market Restraints
  - 4.4.1 Lack of Awareness Regarding Penetration Testing
- 4.5 Industry Attractiveness - Porter's Five Force Analysis
  - 4.5.1 Threat of New Entrants
  - 4.5.2 Bargaining Power of Buyers/Consumers
  - 4.5.3 Bargaining Power of Suppliers
  - 4.5.4 Threat of Substitute Products
  - 4.5.5 Intensity of Competitive Rivalry

#### 5 MARKET SEGMENTATION

- 5.1 By Type
  - 5.1.1 Network Penetration Testing
  - 5.1.2 Web Application Penetration Testing

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

- 5.1.3 Mobile Application Penetration Testing
- 5.1.4 Social Engineering Penetration Testing
- 5.1.5 Wireless Network Penetration Testing Services
- 5.1.6 Other Type
- 5.2 By Deployment
  - 5.2.1 On-premise
  - 5.2.2 Cloud
- 5.3 By End-user Industry
  - 5.3.1 Government and Defense
  - 5.3.2 BFSI
  - 5.3.3 IT and Telecom
  - 5.3.4 Healthcare
  - 5.3.5 Retail
- 5.4 Geography
  - 5.4.1 North America
  - 5.4.2 Europe
  - 5.4.3 Asia Pacific
  - 5.4.4 Latin America
  - 5.4.5 Middle East and Africa

## 6 COMPETITIVE LANDSCAPE

- 6.1 Company Profiles
  - 6.1.1 Synopsys Inc.
  - 6.1.2 Acunetix Ltd.
  - 6.1.3 Checkmarx Ltd.
  - 6.1.4 IBM Corporation
  - 6.1.5 Rapid7, Inc.
  - 6.1.6 FireEye Inc.
  - 6.1.7 VERACODE Inc,
  - 6.1.8 BreachLock Inc.
  - 6.1.9 Broadcom Inc. (Symantec Corporation)
  - 6.1.10 Clavax Technologies LLC

## 7 INVESTMENT ANALYSIS

## 8 MARKET OPPORTUNITIES AND FUTURE TRENDS

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

**Penetration Testing - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029**

Market Report | 2024-02-17 | 100 pages | Mordor Intelligence

To place an Order with Scotts International:

- Print this form
- Complete the relevant blank fields and sign
- Send as a scanned email to support@scotts-international.com

**ORDER FORM:**

Select license	License	Price
	Single User License	\$4750.00
	Team License (1-7 Users)	\$5250.00
	Site License	\$6500.00
	Corporate License	\$8750.00
		VAT
		Total

\*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

\*\* VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>		
Company Name*	<input type="text"/>	EU Vat / Tax ID / NIP number*	<input type="text"/>
Address*	<input type="text"/>	City*	<input type="text"/>
Zip Code*	<input type="text"/>	Country*	<input type="text"/>
		Date	<input type="text" value="2026-03-03"/>
		Signature	

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

