Penetration Testing - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 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 5.30 billion in 2025, and is expected to reach USD 15.90 billion by 2030, at a CAGR of 24.59% during the forecast period (2025-2030).

The penetration testing market is witnessing rapid transformation, driven by increasing security needs across industries. The growing reliance on digital technologies and online platforms has escalated the risk of cyberattacks, making penetration testing services essential for identifying vulnerabilities. Various sectors, such as government, defense, healthcare, and BFSI (banking, financial services, and insurance), are adopting penetration testing solutions to mitigate risks associated with cyber threats. Penetration testing services offer companies the ability to assess their network, application, and cloud security, ensuring compliance with cybersecurity standards and regulations.

Penetration Testing Services: Rising Demand for Security Assessments

Key Highlights
- Penetration testing, also known as ethical hacking, focuses on identifying and mitigating security vulnerabilities in IT infrastructure. Organizations increasingly rely on penetration testing tools and services to safeguard data and ensure the robustness of their security systems. The demand for penetration testing services is fueled by the rise in sophisticated cyberattacks, regulatory requirements, and the shift toward cloud adoption.
- Key factors influencing this market include the increasing need for penetration testing automation and the evolution of testing methodologies tailored to various industries. The availability of cloud penetration testing solutions and advancements in cybersecurity compliance testing have expanded the market's scope, offering tailored services for different deployment environments, such as on-premise and cloud. Additionally, the rise of network penetration testing and application-specific testing

services, including web and mobile applications, continues to shape the market landscape.

Rising Cybersecurity Risks Across Sectors

Key Highlights
- Growing Cybersecurity Threats: The surge in security breaches has led to a significant demand for penetration testing services, especially in sectors handling sensitive data, such as finance, healthcare, and government. These industries require frequent vulnerability assessments to safeguard critical assets from increasingly sophisticated cyberattacks. With the escalation of cybercrime, the demand for cybersecurity compliance testing has grown, prompting organizations to enhance their defenses through comprehensive penetration testing tools and services.
- Ethical Hacking and Risk Assessment: Penetration testing companies offer a range of services, including ethical hacking, cyber risk assessments, and network security analysis. Cybercriminals are continually finding new ways to exploit vulnerabilities in digital ecosystems. The growing frequency and complexity of these attacks push businesses to invest in robust security measures, which has led to a steady rise in penetration testing demand.
- Cloud Security Concerns: As businesses digitize and embrace cloud technologies, they are exposed to a broader array of cyber risks. This has resulted in a surge in cloud penetration testing, where companies assess vulnerabilities in their cloud-based infrastructure. The healthcare sector, for instance, has seen a sharp rise in cyberattacks, driving a need for more rigorous penetration testing services to safeguard patient data and comply with stringent data protection regulations.

Government Regulations Driving Compliance Needs

Key Highlights
- Compliance Mandates: Strict government regulations regarding data security and privacy are forcing organizations to adopt more sophisticated security measures. Governments worldwide are implementing frameworks to ensure that businesses adhere to strict cybersecurity standards, often mandating regular penetration testing to ensure compliance. This has become particularly prominent in the BFSI sector, where the handling of sensitive financial data demands the highest levels of security and compliance with regulatory standards such as GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act).
- Government and Defense Sector Focus: Government and defense sectors, known for their sensitive data and critical infrastructure, are increasingly dependent on penetration testing services to protect against both domestic and international cyber threats. As the digital landscape evolves, government bodies are tightening their cybersecurity compliance standards, particularly in regions such as North America and Europe. This has driven the adoption of penetration testing tools to prevent breaches and ensure the integrity of national security systems.
- Rise of Penetration Testing Automation: The complexity of modern regulatory environments, coupled with the growing volume of cyber threats, has led to a surge in demand for penetration testing automation. Automation in penetration testing enables more frequent and comprehensive assessments, allowing businesses to identify security weaknesses efficiently and stay ahead of emerging threats.

Penetration Testing Market Trends

Growing Requirement of Penetration Testing among Government and Defense

- Increasing Demand for Cybersecurity Solutions: The penetration testing market has seen notable growth, driven by escalating

cybersecurity threats and the necessity for enhanced security measures across industries. As cyberattacks become more sophisticated, businesses are turning to penetration testing services to safeguard their systems. This surge in demand is most prominent in critical sectors like government and defense, where sensitive data and infrastructure require constant protection. Penetration testing tools and services have evolved, making them integral to modern cybersecurity frameworks.

- Government and Defense Sectors Drive Penetration Testing: The government and defense sectors are primary targets for cyberattacks, necessitating robust cybersecurity protocols, including penetration testing. With increasing cyber threats to national security and sensitive data, penetration testing helps identify vulnerabilities in critical infrastructure and secure these systems against potential breaches. Compliance with strict security standards such as NIST and the DoD's DIACAP mandates has made penetration testing a crucial component of government cybersecurity strategies. Automated penetration testing tools are gaining popularity in these sectors, allowing for efficient and continuous security assessments.
- Automation and Cloud Penetration Testing Trends: Automation in penetration testing has become a key trend, offering faster and more accurate results, particularly for large-scale networks in government systems. Automated tools enable continuous security evaluations, minimizing the need for manual intervention. Moreover, cloud penetration testing is gaining traction as governments and businesses increasingly adopt cloud-based infrastructures. This type of testing addresses the unique challenges posed by cloud environments, ensuring that sensitive information remains protected within dynamic infrastructures. The ethical hacking market is also expanding, with ethical hackers collaborating with government agencies to simulate attacks and identify weaknesses.
- Global Collaborations and Increasing Defense Budgets: The penetration testing market is further bolstered by rising defense budgets and global collaborations on cybersecurity initiatives. Governments worldwide are ramping up their investments in cybersecurity to safeguard national interests, driving the demand for penetration testing. These trends underscore the critical role penetration testing plays in fortifying security protocols across both government and defense sectors, ensuring preparedness against evolving cyber threats. The integration of advanced technologies into testing tools continues to enhance the efficiency and scope of security assessments in these industries.

North America to Hold Major Share

- North America Leads in Cybersecurity Infrastructure: North America is expected to dominate the penetration testing market, holding the largest share due to its advanced cybersecurity infrastructure and widespread adoption of security technologies. The region's focus on stringent cybersecurity regulations and its proactive response to sophisticated cyber threats has propelled it to the forefront of penetration testing services and tools. The United States, in particular, is leading the market, with its extensive government and defense networks and robust private sector creating a substantial demand for penetration testing solutions.
- Innovation and Compliance in the U.S. Market: The U.S. penetration testing market stands out for its innovation and adherence to regulatory frameworks such as NIST, which mandates regular penetration testing. This ensures that organizations meet stringent security standards and remain resilient against cyberattacks. Leading U.S. penetration testing companies are leveraging cutting-edge technologies to offer services such as network, application, and cloud penetration testing, further enhancing the country's cybersecurity posture. As cyberattacks grow more complex, U.S. businesses are relying on these advanced tools to stay ahead of emerging threats.
- Canada's Role in the Penetration Testing Market: Canada is also playing a crucial role in the North American penetration testing market. The country's growing investments in cybersecurity solutions are driving demand for penetration testing, especially in sectors like finance, healthcare, and government. Canadian organizations are increasingly adopting automated and continuous testing methods to enhance their cybersecurity defenses. As cyber threats continue to evolve, Canadian companies are focusing on improving security vulnerability assessments and adopting comprehensive testing solutions to secure sensitive data and infrastructure.
- Growth Driven by Regulatory Compliance: The growth of penetration testing in North America is strongly supported by the region's regulatory environment. Compliance with cybersecurity frameworks like the NIST in the U.S. and similar initiatives in

Canada has fueled demand for penetration testing services. Companies in North America are increasingly adopting these services to meet regulatory requirements, protect sensitive data, and strengthen their cybersecurity defenses. This focus on compliance, along with a strong emphasis on innovation, ensures that North America will continue to lead the global penetration testing market for the foreseeable future.

Penetration Testing Industry Overview

Market Characteristics: The penetration testing market is semi consolidated, with both global and regional players contributing to the overall landscape. Large multinational companies dominate the space, providing comprehensive cybersecurity solutions, including penetration testing as a part of broader security services. The market sees a balance between specialized cybersecurity firms and established tech conglomerates, leading to healthy competition. The moderately consolidated nature allows new players to enter, but they face significant competition from established companies with advanced capabilities.

Major Players: The leading companies in the penetration testing market include IBM Corporation, Rapid7, FireEye Inc., VERACODE, and Broadcom (Symantec). These players offer comprehensive penetration testing solutions as part of their larger cybersecurity portfolios, catering to enterprises across various industries. They have a global presence and are known for their strong research and development capabilities, enabling them to innovate and keep up with emerging threats.

Trends and Future Success Factors: The growing sophistication of cyberattacks is driving demand for advanced penetration testing services. To succeed in this market, companies must focus on improving their automation capabilities, integrating AI, and ensuring that their solutions address evolving security needs. Emphasizing cloud security and scalable solutions is also crucial as organizations continue to shift their operations to the cloud. Effective penetration testing companies will need to offer seamless, scalable services while maintaining a cutting-edge approach to threat detection.

Additional Benefits:

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

Table of Contents:

Penetration Testing - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 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*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-02
		Signature