Penetration Testing Market is projected to surpass US$4.351 billion by 2029 at a CAGR of 13.22%

The penetration testing market is anticipated to grow at a CAGR of 13.22% from US$1.781 billion in 2022 to US$4.351 billion by 2029.

NOIDA, UTTAR PARDESH, INDIA, June 25, 2024 /EINPresswire.com/ -- According to a new study published by Knowledge Sourcing Intelligence, the penetration testing market is projected to grow at a CAGR of 13.22% between 2022 and 2029 to reach US$4.351 billion by 2029.

Penetration testing, also called pen testing, is a reenacted cyberattack on a computer system, organization, or application to distinguish security vulnerabilities. It includes utilizing the same instruments and procedures as genuine attackers, with authorization from the system proprietor. The primary objective is to recognize weaknesses within the system's security posture, such as software, equipment, setup settings, or human methods. By recognizing vulnerabilities, organizations can take steps to settle them before they can be exploited, decreasing the risk of information breaches, money-related losses, and reputational harm.

> "
> The penetration testing market is anticipated to grow at a CAGR of 13.22% from US$1.781 billion in 2022 to US$4.351 billion by 2029."
>
> *Knowledge Sourcing Intelligence*

The penetration testing market is encountering significant expansion due to rising cyber dangers, expanding regulations, and developing mindfulness of potential money-related and reputational damage caused by data breaches. These variables are driving the need for strong security measures, as penetration testing helps organizations identify and address vulnerabilities before attackers exploit them. The market is additionally being driven by rigid information privacy directions and expanding mindfulness of the potential financial and reputational harm caused by information breaches.

The market of penetration testing is extending with the launch of new products and innovative advancements on a worldwide scale, for instance, in March 2024, F5 enhanced its Multicloud application security capabilities by including automated reconnaissance and penetration testing

capabilities, empowering clients to effectively scan for and discover vulnerabilities affecting their web applications, much obliged to the acquisition of Heyhack.

Access sample report or view details: https://www.knowledge-sourcing.com/report/penetration-testing-market

Based on the deployment, the penetration testing market is categorized into on-premise and cloud. The cloud-based penetration testing market is anticipated to develop quickly due to its focal points such as versatility, cost-effectiveness, availability, mechanization, compatibility with persistent integration and delivery (CI/CD) pipelines, and fast deployment and upgrades. These solutions eliminate the requirement for costly hardware and software foundation, making them cost-effective for organizations of all sizes.

Based on organization size, the global market of penetration testing is classified into large and small, and medium enterprises. Large enterprises are anticipated to stay the major supporters of the penetration testing market development due to stricter directions, bigger budgets, more complex IT foundations, and higher esteem of assets. These organizations confront more rigid compliance necessities, requiring normal and comprehensive entrance testing to guarantee information security and dodge fines.

Based on the component, the penetration testing industry is categorized into solution and service. The service section is anticipated to develop due to variables such as the need for in-house expertise, adaptability, and scalability, access to progressed devices and techniques, and cost-effectiveness. Organizations, especially SMEs, depend on external benefit suppliers for comprehensive entrance testing, which can be more cost-effective than hiring and training a dedicated security workforce.

Based on testing type, the worldwide market of penetration testing is classified into network penetration testing, application penetration testing, cloud penetration testing, and others. Network Penetration Testing may be a significant device for identifying network foundation vulnerabilities. Application Penetration Testing is anticipated to develop due to the expanding dependence on web and mobile applications. Cloud Penetration Testing is quickly increasing due to the endless attack surface for cloud-based foundations. Other testing types incorporate social design and emerging innovations like IoT and OT. The penetration testing market is likely to shift towards application and cloud penetration testing in the future.

Based on the industry vertical, the penetration testing market is categorized into healthcare, BFSI, government, and defence, retail and e-commerce, energy and utilities, and others. BFSI institutions, healthcare, government agencies, retail, and other sectors are all requiring regular penetration testing to ensure data security and compliance. Healthcare's increasing reliance on Electronic Health Records (EHR) creates a vast attack surface, while government agencies and defense sectors manage critical infrastructure and sensitive information. Retail and e-commerce are also vulnerable, as are energy and utilities, and manufacturing, as interconnected industrial

control systems create new attack vectors.

Based on Geography, North America is expected to have a major share of the worldwide market of penetration testing in the midst of the anticipated period owing to a number of major factors. North American organizations are progressively aware of cyber dangers and the potential monetary and reputational harm from information breaches, driving a better demand for penetration testing administrations. Strong regulatory bodies like HIPAA order customary penetration testing for organizations dealing with sensitive information. The advanced danger landscape, early adoption of modern technologies, and skilled workforce accessibility in North America encourage the improvement and execution of compelling penetration testing solutions and administrations.

As a part of the report, the major players operating in the penetration testing market that have been covered are Crowdstrike, Rapid7, Synopsys, Inc., IBM, Cigniti Technologies, Invicti, ASTRA IT, Inc., Secureworks, Inc., Indusface, and Vairav Technology Security Pvt. Ltd.

The market analytics report segments the penetration testing market on the following basis:

• BY DEPLOYMENT

o On-premise
o Cloud

• BY ORGANIZATION SIZE

o Large
o Small and Medium Enterprises

• BY COMPONENT

o Solution
o Service

• BY TESTING TYPE

o Network Penetration Testing
o Application Penetration Testing
o Cloud Penetration Testing
o Others

• BY INDUSTRY VERTICAL

o Healthcare

o BFSI
o Government and Defence
o Retail and E-commerce
o Energy and Utilities
o Others

• BY GEOGRAPHY

o North America

• United Kingdom
• Canada
• Mexico

o South America

• Brazil
• Argentina
• Others

o Europe

• United Kingdom
• Germany
• France
• Italy
• Spain
• Others

o Middle East and Africa

• Saudi Arabia
• UAE
• Others

o Asia Pacific

• Japan
• China
• India
• South Korea
• Taiwan
• Thailand

- Indonesia
- Others

Companies Profiled:

- Crowdstrike
- Rapid7
- Synopsys, Inc.
- IBM
- Cigniti Technologies
- Invicti
- ASTRA IT, Inc.
- Secureworks, Inc.
- Indusface
- Vairav Technology Security Pvt. Ltd

Explore More Reports:

- API Testing Market: https://www.knowledge-sourcing.com/report/api-testing-market

- Global Security Advisory Services Market: https://www.knowledge-sourcing.com/report/global-security-advisory-services-market

- Global Cyber Security Market: https://www.knowledge-sourcing.com/report/global-cybersecurity-market

Ankit Mishra
Knowledge Sourcing Intelligence LLP
+1 850-250-1698
email us here
Visit us on social media:
Facebook
X
LinkedIn