Security Testing Market is estimated to be US$ 52.71 billion by 2030 with a CAGR of 26.0% - By PMI

The report "Security Testing Market, By Deployment, By Type- Trends, Analysis and Forecast till 2030"

Security Testing Market -PMI

COVINA , CALIFORNIA, UNITED STATES, March 17, 2023 /EINPresswire.com/ -- According to the latest research study, the demand of "Security Testing Market accounted for US$ 5.34 billion in 2020 and is estimated to be US$ 52.71 billion by 2030 and is anticipated to register a CAGR of 26.0%"

Security testing is a testing technique that determines whether the IT infrastructure components such as networks, application, devices, and others are free from security vulnerabilities or not. It is about detecting security gaps present in the system, which might be exploited by attackers. It involves scanning of network and weak spot of the systems, and after determining the problems it itself provides solutions for the identified risks. It can be performed in both ways manual as well as automated scanning. For instance, a password stored in encrypted way, back button should not operate on financial websites etc. The aim of the security testing market is to provide a secured environment of browsing, to diagnose the system failures, solving the threats etc. are some of the common aims of this market. The organizations are rapidly growing due to the adoption of cutting-edge solutions to enhance productivity. In order to coordinate cross-business processes and facilitate the customers in the best possible way, the organizations are deploying third-party Types wherever necessary. These third-party types may be prone to cyber-attacks due to the variations in security policies of different organizations. The rising demand for protection of software bound valuable properties such as mobile and web application is the major driver for the growth of global security testing market.

Region Analysis:

North America holds the significant position in this market, and accounts largest share, owing to technological advancement in IT sector. This attributed to rise in adoption of Bring Your Own Device (BYOD) in different organizations in the region. Asia Pacific is anticipated to register high CAGR during the forecast period. The rising investment in the enhancing the security features across various industry verticals is expected to drive the growth of security testing market in the region.

Key Development:

- In April 2020, The Rapid7 uplifted its InsightIDR and also provided network traffic analysis capabilities.
- In Feb 2020, Rapid7 and Synk two well established company got merged and aims to deliver end-to-end application security to the organizations.

Request Sample Pages:
https://www.prophecymarketinsights.com/market_insight/Insight/request-sample/4155

Segmentation:

The Global Security Testing Market accounted for US$ 5.34 billion in 2020 and is estimated to be US$ 52.71 billion by 2030 and is anticipated to register a CAGR of 26.0%. The Global Security Testing Market is segmented by development, type, and region.

- By development, the Global Security Testing Market is segmented into On-Premise, Cloud, and Hybrid
- By Type, the Global Security Testing Market is classified into network security testing, and application security testing. The network security test is segmented into VPN testing, firewall testing, and other service types. The application security testing is bifurcated into application type and testing type. The application type is classified into mobile application security testing, web application security testing, cloud application security testing, and enterprise application security testing. The testing type is segmented into SAST, DAST, IAST, and RASP.
- By region, North America is expected to account for major revenue share in Global Tinplate Packaging Market, followed by other regions.

Key Benefits for Security Testing Market:

The security testing market has become increasingly important as more businesses and organizations rely on technology and digital systems to manage their operations. Here are some key benefits of the security testing market:

1. Improved Security: The primary benefit of the security testing market is improved security. Security testing helps identify vulnerabilities in software, applications, and systems before they can be exploited by cybercriminals. This proactive approach to security reduces the risk of data breaches, system downtime, and financial losses.

2. Compliance: Many industries, such as healthcare and finance, are required by law to comply with specific regulations and standards. Security testing helps organizations meet these compliance requirements by identifying and addressing any security issues that could prevent compliance.
3. Cost Savings: Identifying and addressing security issues early in the development cycle is less expensive than fixing them after a system or application has been deployed. Security testing can help businesses save money by reducing the likelihood of costly security breaches, system downtime, and legal fees.
4. Improved Reputation: A security breach can damage a company's reputation and lead to a loss of customers. By implementing security testing, businesses can demonstrate their commitment to security and build trust with their customers.
5. Competitive Advantage: In today's digital age, security is a critical differentiator. Businesses that invest in security testing can differentiate themselves from their competitors and attract customers who prioritize security.

Overall, the security testing market provides businesses with a proactive approach to security, compliance, cost savings, improved reputation, and competitive advantage.

Download PDF Brochure:
https://www.prophecymarketinsights.com/market_insight/Insight/request-pdf/4155

Company Profile:

• Cisco Systems, Inc.
o Company Overview
o Product Portfolio
o Key Highlights
o Financial Performance
o Business Strategies

• Hewlett Packard Enterprise
o Company Overview
o Product Portfolio
o Key Highlights
o Financial Performance
o Business Strategies

• IBM Corporation
o Company Overview
o Product Portfolio
o Key Highlights
o Financial Performance
o Business Strategies

- Qualys, Inc.
  - Company Overview
  - Product Portfolio
  - Key Highlights
  - Financial Performance
  - Business Strategies

- WhiteHat Security
  - Company Overview
  - Product Portfolio
  - Key Highlights
  - Financial Performance
  - Business Strategies

- Applause App Quality, Inc.
  - Company Overview
  - Product Portfolio
  - Key Highlights
  - Financial Performance
  - Business Strategies

- Veracode, Checkmarx
  - Company Overview
  - Product Portfolio
  - Key Highlights
  - Financial Performance
  - Business Strategies

- UL LLC
  - Company Overview
  - Product Portfolio
  - Key Highlights
  - Financial Performance
  - Business Strategies

- Intertek Group plc
  - Company Overview
  - Product Portfolio
  - Key Highlights
  - Financial Performance
  - Business Strategies

Frequently Asked Questions about Security Testing Market:

Here are some common FAQs (frequently asked questions) related to the security testing market:

1. What is security testing market, and why is it important?
Security testing market is the process of evaluating the security of a system, application, or network by identifying vulnerabilities and potential threats. It is essential for businesses to conduct security testing to proactively identify and address security issues before they can be exploited by cybercriminals.

2. What types of security testing market are there?
There are various types of security testing market, including vulnerability testing, penetration testing, compliance testing, security scanning, and security code review. Each type of testing focuses on different aspects of security, and the specific type of testing used depends on the needs and goals of the business.

3. What are the benefits of outsourcing security testing market?
Outsourcing security testing market can provide businesses with access to specialized expertise and resources, which may not be available in-house. Outsourcing security testing can also reduce the workload on internal staff, allowing them to focus on other critical tasks. Additionally, outsourcing security testing can be more cost-effective than building an in-house security testing team.

Key Reasons to Purchase Security Testing Market:

Here are some key reasons why you might consider investing in this market:

1. Growing Demand: With the increasing number of cyber-attacks and security breaches, the demand for security testing services is on the rise. Companies and organizations are investing heavily in cyber security solutions to protect their data and systems from potential threats.

2. Emerging Technologies: As new technologies continue to emerge, such as the Internet of Things (IoT) and cloud computing, the need for security testing is also increasing. These technologies bring new security challenges, and companies need to ensure that their systems are secure and protected.

3. Compliance Regulations: Many industries are subject to regulatory compliance requirements, such as PCI-DSS, HIPAA, and GDPR, which require companies to implement security testing measures. As these regulations become more stringent, the demand for security testing services is likely to increase.

4. Cost-Effective: Investing in security testing can be a cost-effective way for companies to mitigate security risks. By identifying vulnerabilities early, companies can avoid costly security breaches and the associated financial and reputational damages.

5. Competitive Advantage: Companies that invest in security testing can gain a competitive advantage by demonstrating to their customers that they take security seriously. This can be a valuable differentiator in industries where security is a top priority, such as finance and healthcare.

Overall, the security testing market is poised for continued growth as companies continue to prioritize cybersecurity and compliance. However, as with any investment, it is important to conduct your own research and consult with a financial advisor before making any decisions.

Check out more studies published by Prophecy Market Insights:

Cybersecurity Insurance Market - By Organization Size (Small and Medium Enterprises (SMEs), and Large Enterprises), By End-user Industry (Healthcare, Retail, BFSI, IT and Telecom, Manufacturing, Other End-user Industries), and By Region (North America, Europe, Asia Pacific, Latin America, and Middle East & Africa) - Trends, Analysis and Forecast till 2030

Hybrid Cloud Market - By Component (Solution and Services), By Service Model (Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service), By Organization Size (Large Enterprises, Small and medium-sized enterprises), By Industry Vertical (Banking, Financial Services, and Insurance (BFSI), Telecommunications and Information Technology (IT), Healthcare and Life sciences, and Others) and By Region (North America, Europe, Asia Pacific, Latin America, and Middle East & Africa) – Trends, Analysis and Forecast till 2030

Shweta Raskar
Prophecy Market Insights
+ 1 860-531-2701
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/622738842