+44 20 8123 2220
info@marketpublishers.com

Breach and Attack Simulation Market by Application (Configuration Management, Patch Management, Threat Intelligence), Vertical (BFSI, Healthcare, IT & ITeS, Education, Manufacturing) - Global Forecast to 2029

https://marketpublishers.com/r/BBA513116F04EN.html
Date: October 2024
Pages: 356
Price: US$ 4,950.00 (Single User License)
ID: BBA513116F04EN

Abstracts

The global Breach and Attack Simulation market size is projected to grow from USD 729.2 million in 2024 to USD 2,405.4 million by 2029 at a Compound Annual Growth Rate (CAGR) of 27.0% during the forecast period.

In the breach and attack simulation market, integration into the existing security solutions, which include SIEM and SOAR, drives the momentum of improving threat detection, response, and remediation. These have streamlined security processes, fastened response times, and vastly improved posture across industries. Finally, integrating AI and ML hardens the breach and attack simulation tools to predict specific vulnerabilities, simulate highly complex attacks, and give real-time feedback. Proactive cybersecurity strategies benefit from efficiency and reducing manual efforts in response to evolving cyber threats. The shift toward automation and AI-driven solutions allows organizations to meet compliance standards and build consumer trust.

'By Professional Services, the Security Posture Assessment will grow at a higher CAGR during the forecast period.'

The professional services segment is expected to have the highest CAGR of the breach and attack simulation market due to the absence of in-house capabilities in most organizations, primarily in SMEs. Professional service providers bridge this gap by providing scalable, cost-effective security assessments. Also, solid testing mechanisms among managed service providers would be required to ensure adequate security in

diverse client environments. It will thereby propel the use of breach and attack simulation services. Continuous security validation through training and on-demand services from analysts boost the proactive countering of organization vulnerabilities. The threat management segment had the most outstanding revenue share in 2023, reflecting the significant demand for specialty assessment to mitigate the growing cyber threats. Key industry players, including Rapid7, Cymulate, and AttackIQ, are leading in this market.

'By Deployment Mode, the On-Premises segment accounts for the largest market size during the forecast period. '

The on-premises segment of the breach and attack simulation market is a localized, customizable security testing approach with the software hosted in their data centers. Deployment of this type offers better control over sensitive data so that organizations can manage the testing process safely. On-premises breach and attack simulation solutions are also customizable and do not interfere with existing security structures. Hence, it is very suitable for industries to have rigid compliance. Most Vendors, such as Rapid7, Qualys, and Sophos, provide tailor-made on-premises solutions. However, the above solution requires high initial investments in hardware and software with an IT infrastructure. They pose scalability problems and require dedicated IT staff equipped with security-specific skills for maintenance and operation.

'By region, North America is expected to be the largest market during the forecast period.'

Higher expenditure on cybersecurity in North America owing to the rise in cyber threats and fraud is quite prolific for the growth of the breach and attack simulation market. The US, for one, increased its cybersecurity budget to USD 20 billion in 2023 and effectively enlisted all its broad adoption of breach and attack simulation tools for proactive security testing. The healthcare sector, susceptible to data breaches, has further pushed demand for breach and attack simulation solutions. For instance, regulatory pressures - such as the Cybersecurity and Infrastructure Security Agency and California Consumer Privacy Act - drive the adoption of breach and attack simulation platforms as a compliance source. The two major leaders, AttackIQ and Cymulate, will fortify their position in this emerging market with complete solutions composed of scenario-based simulations, continuous testing, and vulnerability assessment.

Breakdown of primaries:

In-depth interviews were conducted with Chief Executive Officers (CEOs), marketing directors, other innovation and technology directors, and executives from various key organizations operating in the breach and attack simulation market.

By Company Type: Tier 1: 55%, Tier 2: 25%, and Tier 3: 20%

By Designation: Directors: 50%, Managers: 30% and Other: 20%

By Region: North America: 40%, Europe: 35%, Asia Pacific: 20%, RoW: 5%

Cymulate (US), AttackIQ (US), XM Cyber (Israel), SafeBreach (US), Picus Security (US), Qualys (US), Rapid7 (US), IBM (US), Fortinet (US), Mandiant (US), Keysight Technologies (US), Aujas (US), Cytomate (Qatar), ReliaQuest (US), Detectify (Sweden), Scythe (US), BreachLock (US), CyCognito (US), Skybox Security (US), Aquila I (India), ImmuniWeb (Switzerland), ThreatGen (US), Strobes Security (US), NopSec (US), SimSpace (US), PurpleBox (US), and Kroll (US); are some of the key players in the breach and attack simulation solutions market.

The study includes an in-depth competitive analysis of these key players in the breach and attack simulation market, with their company profiles, recent developments, and key market strategies.

Research Coverage

The report comprehensively segments the breach and attack simulation Market. It provides forecasts regarding its size across various dimensions, including By Offering (Platform & Tools, services), By Deployment Mode (Cloud, On-Premises), By Organization Size (SMEs, Large Enterprises), By Application (Configuration Management, Patch Management, Threat Intelligence, Other Applications), By Vertical (BFSI, Healthcare, IT & ITES, Telecommunications, Retail & E-Commerce, Manufacturing, Education, Other Verticals), and Region (North America, Europe, Middle East & Africa, Asia Pacific, and Latin America). Additionally, the study encompasses a thorough competitive analysis of key market players, offering insights into their company profiles, product and business offerings, recent developments, and key market strategies.

Key benefits of buying report

The report offers valuable insights to market leaders and new entrants by closely approximating the breach and attack simulation market's revenue figures and subsegments. Stakeholders can leverage this report to better understand the competitive landscape, enabling them to position their businesses more effectively and develop tailored go-to-market strategies. Additionally, stakeholders can grasp the market dynamics and stay informed about key drivers, restraints, challenges, and opportunities shaping the industry landscape.

The report provides insights on the following pointers:

Analysis of critical drivers (Growing complexity and rising threats of cyberattacks in the digital age, Growing need to adhere to stringent regulations and data privacy laws, Rising Need for Continuous Security Testing, Integration of breach and attack simulation solutions tools with existing security tools), restraints (Lack of Skilled Professionals, High Implementation and Maintenance Costs), opportunities (Integration of breach and attack simulation solutions with Attack Surface Management(ASM), Rapid adoption of cloud-based services, integration of artificial intelligence (AI) and machine learning (ML) into breach and attack simulation solutions, Digital Transformation initiatives), and challenges (Resource allocation and integration complexity, Organizational Resistance and Misconceptions about breach and attack simulation.

Product Development/Innovation: Detailed insights on upcoming technologies, research development activities, new products, and service launches in the breach and attack simulation market.

Market Development: Comprehensive information about lucrative markets – the report analyses the breach and attack simulation solutions market across varied regions.

Market Diversification: Exhaustive information about new products and services, untapped geographies, recent developments, and investments.

Competitive Assessment: In-depth assessment of market shares, growth strategies, and service offerings of leading players Cymulate (India), AttackIQ (US), XM Cyber (Israel), SafeBreach (Israel), and Picus Security(US).

+44 20 8123 2220
info@marketpublishers.com

Contents

+44 20 8123 2220
info@marketpublishers.com

14 ADJACENT MARKETS

15 APPENDIX

+44 20 8123 2220
info@marketpublishers.com

I would like to order

Product name: Breach and Attack Simulation Market by Application (Configuration Management, Patch Management, Threat Intelligence), Vertical (BFSI, Healthcare, IT & ITeS, Education, Manufacturing) - Global Forecast to 2029

Product link: https://marketpublishers.com/r/BBA513116F04EN.html

Price: US$ 4,950.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/BBA513116F04EN.html

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:
Last name:
Email:
Company:
Address:
City:
Zip code:
Country:
Tel:
Fax:
Your message:

**All fields are required

Custumer signature _____

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms & Conditions at https://marketpublishers.com/docs/terms.html

To place an order via fax simply print this form, fill in the information below

+44 20 8123 2220
info@marketpublishers.com

and fax the completed form to +44 20 7900 3970