

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), Picos 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).

Contents

1 INTRODUCTION

- 1.1 STUDY OBJECTIVES
- 1.2 MARKET DEFINITION
 - 1.2.1 INCLUSIONS AND EXCLUSIONS
- 1.3 MARKET SCOPE
 - 1.3.1 MARKET SEGMENTATION
 - 1.3.2 YEARS CONSIDERED
- 1.4 CURRENCY CONSIDERED
- 1.5 STAKEHOLDERS
- 1.6 SUMMARY OF CHANGES

2 RESEARCH METHODOLOGY

- 2.1 RESEARCH DATA
 - 2.1.1 SECONDARY DATA
 - 2.1.2 PRIMARY DATA
 - 2.1.2.1 Breakup of primaries
 - 2.1.2.2 Key industry insights
- 2.2 MARKET BREAKUP AND DATA TRIANGULATION
- 2.3 MARKET SIZE ESTIMATION
 - 2.3.1 TOP-DOWN APPROACH
 - 2.3.2 BOTTOM-UP APPROACH
- 2.4 MARKET FORECAST
- 2.5 RESEARCH ASSUMPTIONS
- 2.6 STUDY LIMITATIONS

3 EXECUTIVE SUMMARY

4 PREMIUM INSIGHTS

- 4.1 ATTRACTIVE OPPORTUNITIES FOR KEY MARKET PLAYERS
- 4.2 AUTOMATED BREACH AND ATTACK SIMULATION MARKET, BY OFFERING
- 4.3 AUTOMATED BREACH AND ATTACK SIMULATION MARKET, BY DEPLOYMENT MODE
- 4.4 AUTOMATED BREACH AND ATTACK SIMULATION MARKET, BY ORGANIZATION SIZE

4.5 AUTOMATED BREACH AND ATTACK SIMULATION MARKET, BY KEY APPLICATION AND REGION

4.6 MARKET INVESTMENT SCENARIO

5 MARKET OVERVIEW AND INDUSTRY TRENDS

5.1 INTRODUCTION

5.2 MARKET DYNAMICS

5.2.1 DRIVERS

5.2.1.1 Growing complexity and rising threats of cyberattacks in digital age

5.2.1.2 Surging need for adherence to stringent regulations and data privacy laws

5.2.1.3 Rising need for continuous security testing

5.2.1.4 Integration of automated breach and attack simulation tools with existing security tools

5.2.2 RESTRAINTS

5.2.2.1 Lack of skilled professionals

5.2.2.2 High implementation and maintenance costs

5.2.3 OPPORTUNITIES

5.2.3.1 Integration of automated breach and attack simulation with attack surface management

5.2.3.2 Rapid adoption of cloud-based services

5.2.3.3 Integration of AI and ML into breach and attack simulation solutions

5.2.3.4 Digital transformation initiatives

5.2.4 CHALLENGES

5.2.4.1 Resource allocation and integration complexity

5.2.4.2 Organizational resistance and misconceptions about automated breach and attack simulation systems

5.3 IMPACT OF GENERATIVE AI (GENAI) ON AUTOMATED BREACH AND ATTACK SIMULATION MARKET

5.3.1 TOP USE CASES & MARKET POTENTIAL

5.3.1.1 Key use cases

5.3.2 TOP USE CASES AND MARKET POTENTIAL IN AUTOMATED BREACH AND ATTACK SIMULATION MARKET

5.3.3 IMPACT OF GEN AI ON INTERCONNECTED AND ADJACENT ECOSYSTEMS

5.3.3.1 Artificial intelligence and machine learning

5.3.3.2 Cloud computing

5.3.3.3 Big data analytics

5.3.3.4 Internet of Things (IoT)

5.3.3.5 Quantum computing

5.4 CASE STUDY ANALYSIS

5.4.1 CASE STUDY 1: CYMULATE HELPED GLOBAL BANK CORP. STRENGTHEN CYBERSECURITY DEFENSES USING AUTOMATED BREACH AND ATTACK SIMULATION PLATFORM

5.4.2 CASE STUDY 2: XM CYBER ASSISTED HEALTHCARE SYSTEMS BY PROVIDING CONTINUOUS VISIBILITY INTO POTENTIAL ATTACK PATHS

5.4.3 CASE STUDY 3: SAFE BREACH SUPPORTED RETAIL GIANT IN ENHANCING CYBERSECURITY AND PROTECTING CUSTOMERS USING AUTOMATED BREACH AND ATTACK SIMULATION TOOL

5.4.4 CASE STUDY 4: ATTACKIQ ASSISTED NATIONAL SECURITY AGENCY IN STRENGTHENING CYBERSECURITY MEASURES AGAINST EMERGING THREATS

5.4.5 CASE STUDY 5: PENTERA SUPPORTED GLOBAL MANUFACTURING CORP. IN BOLSTERING OPERATIONAL TECHNOLOGY SECURITY AND PREVENTING DISRUPTIONS

5.4.6 CASE STUDY 6: QUALYS ASSISTED GLOBAL BANK CORP. IN STRENGTHENING CYBERSECURITY AND SAFEGUARDING SENSITIVE DATA

5.5 VALUE CHAIN ANALYSIS

5.5.1 TECHNOLOGY INFRASTRUCTURE PROVIDERS

5.5.2 AUTOMATED BREACH AND ATTACK SIMULATION PROVIDERS

5.5.3 APPLICATION PROVIDERS

5.5.4 SYSTEM INTEGRATORS

5.5.5 END USERS

5.6 ECOSYSTEM ANALYSIS

5.7 PORTER'S FIVE FORCES ANALYSIS

5.7.1 THREAT OF NEW ENTRANTS

5.7.2 BARGAINING POWER OF SUPPLIERS

5.7.3 BARGAINING POWER OF BUYERS

5.7.4 THREAT OF SUBSTITUTES

5.7.5 INTENSITY OF COMPETITIVE RIVALRY

5.8 PRICING ANALYSIS

5.8.1 AVERAGE SELLING PRICE TREND OF KEY PLAYERS, BY SOLUTION

5.8.2 INDICATIVE PRICING ANALYSIS, BY OFFERING

5.9 TECHNOLOGY ANALYSIS

5.9.1 KEY TECHNOLOGIES

5.9.1.1 AI/ML

5.9.1.2 Graph-based simulation technology

5.9.1.3 Big data analytics

5.9.1.4 Zero trust

5.9.1.5 Behavioral analytics

5.9.2 COMPLEMENTARY TECHNOLOGIES

5.9.2.1 Cloud security

5.9.2.2 Virtual private networks

5.9.2.3 Behavioral biometrics

5.9.2.4 Natural language processing

5.9.3 ADJACENT TECHNOLOGIES

5.9.3.1 Quantum computing

5.9.3.2 IoT security

5.10 PATENT ANALYSIS

5.11 TRENDS AND DISRUPTIONS IMPACTING CUSTOMERS' BUSINESSES

5.12 KEY STAKEHOLDERS AND BUYING CRITERIA

5.12.1 KEY STAKEHOLDERS IN BUYING PROCESS

5.12.2 BUYING CRITERIA

5.13 REGULATORY LANDSCAPE

5.13.1 REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

5.14 KEY CONFERENCES & EVENTS, 2024–2025

5.15 INVESTMENT AND FUNDING SCENARIO

6 AUTOMATED BREACH AND ATTACK SIMULATION MARKET, BY OFFERING

6.1 INTRODUCTION

6.1.1 OFFERING: AUTOMATED BREACH AND ATTACK SIMULATION MARKET DRIVERS

6.2 PLATFORMS & TOOLS

6.2.1 INCREASING NEED FOR CONTINUOUS SECURITY AND SEAMLESS INTEGRATION TO DRIVE MARKET

6.2.2 STANDALONE PLATFORMS/SOFTWARE TOOLS

6.2.3 INTEGRATED SECURITY PLATFORMS/TOOLS

6.2.4 CLOUD-BASED SOLUTIONS

6.3 SERVICES

6.3.1 GROWING COMPLEXITY OF CYBER THREATS AND SURGING NEED FOR REGULATORY COMPLIANCE TO DRIVE MARKET

6.3.2 PROFESSIONAL SERVICES

6.3.2.1 Expertise and strategic guidance to propel demand for professional services

6.3.2.2 Implementation, Integration, and Consulting

6.3.2.3 Security Posture Assessment

6.3.2.4 Training, Compliance Reporting, and Auditing

6.3.2.5 Support & Maintenance

6.3.3 MANAGED SERVICES

6.3.3.1 Increasing need for focusing on core business operations while outsourcing complex security functions to accelerate market growth

7 AUTOMATED BREACH AND ATTACK SIMULATION MARKET,

BY DEPLOYMENT MODE

7.1 INTRODUCTION

7.1.1 DEPLOYMENT MODE: AUTOMATED BREACH AND ATTACK SIMULATION
MARKET DRIVERS

7.2 ON-PREMISES

7.2.1 PARAMOUNT NEED FOR STRICT REGULATORY COMPLIANCE AND DATA SECURITY TO DRIVE DEMAND FOR ON-PREMISES SOLUTIONS

7.3 CLOUD

7.3.1 SCALABILITY AND COST-EFFICIENCY TO DRIVE DEMAND FOR CLOUD-BASED BAS SOLUTIONS

8 AUTOMATED BREACH AND ATTACK SIMULATION MARKET,

BY ORGANIZATION SIZE

8.1 INTRODUCTION

8.1.1 ORGANIZATION SIZE: AUTOMATED BREACH AND ATTACK SIMULATION
MARKET DRIVERS

8.2 SMES

8.2.1 SCALABILITY AND AFFORDABILITY OF BAS SOLUTIONS TO DRIVE
MARKET

8.3 LARGE ENTERPRISES

8.3.1 SURGING NEED FOR PROTECTION OF VAST AMOUNTS OF SENSITIVE DATA TO FUEL MARKET GROWTH

9 AUTOMATED BREACH AND ATTACK SIMULATION MARKET, BY APPLICATION

9.1 INTRODUCTION

9.1.1 APPLICATION: AUTOMATED BREACH AND ATTACK SIMULATION MARKET
DRIVERS

9.2 CONFIGURATION MANAGEMENT

9.2.1 SPIKE IN DEMAND FOR REAL-TIME CONFIGURATION VALIDATION AND COMPLIANCE MANAGEMENT TO BOLSTER MARKET GROWTH

9.3 PATCH MANAGEMENT

9.3.1 GROWING COMPLEXITY OF IT INFRASTRUCTURES AND INCREASING VOLUME OF SOFTWARE VULNERABILITIES TO DRIVE MARKET

9.4 THREAT INTELLIGENCE

9.4.1 PROACTIVE RISK MANAGEMENT AND REAL-TIME THREAT DETECTION TO DRIVE DEMAND FOR BAS SOLUTIONS

9.5 OTHER APPLICATIONS

10 AUTOMATED BREACH AND ATTACK SIMULATION MARKET, BY VERTICAL

10.1 INTRODUCTION

10.1.1 VERTICAL: AUTOMATED BREACH AND ATTACK SIMULATION MARKET DRIVERS

10.2 BFSI

10.2.1 INCREASED NEED FOR ENHANCING CUSTOMER EXPERIENCES AND STREAMLINING OPERATIONS TO DRIVE MARKET

10.3 HEALTHCARE

10.3.1 SPIKE IN DEMAND FOR SECURING SENSITIVE HEALTH DATA FROM POTENTIAL BREACHES TO BOOST MARKET GROWTH

10.4 IT & ITES

10.4.1 SURGING NEED FOR ROBUST CYBERSECURITY MEASURES TO FOSTER MARKET GROWTH

10.5 TELECOMMUNICATIONS

10.5.1 SPIKE IN DEMAND FOR PROTECTION OF EXTENSIVE AND SENSITIVE COMMUNICATION INFRASTRUCTURES FROM RISING CYBER THREATS TO ACCELERATE MARKET GROWTH

10.6 RETAIL & ECOMMERCE

10.6.1 INCREASING DEMAND FOR IDENTIFICATION OF VULNERABILITIES AND TEST SECURITY CONTROLS IN REAL TIME TO FOSTER MARKET GROWTH

10.7 MANUFACTURING

10.7.1 INCREASED NEED FOR PROTECTION OF INTELLECTUAL PROPERTY AND COMBAT PIRACY TO DRIVE MARKET

10.8 EDUCATION

10.8.1 RISING NEED FOR REDUCTION OF OPERATIONAL DISRUPTIONS CAUSED

BY CYBER INCIDENTS TO PROPEL MARKET

10.9 OTHER VERTICALS

11 AUTOMATED BREACH AND ATTACK SIMULATION MARKET, BY REGION

11.1 INTRODUCTION

11.2 NORTH AMERICA

11.2.1 NORTH AMERICA: MARKET DRIVERS

11.2.2 NORTH AMERICA: MACROECONOMIC OUTLOOK

11.2.3 US

11.2.3.1 Rising complexity of cyber threats and need for continuous security to accelerate market growth

11.2.4 CANADA

11.2.4.1 Rising cybersecurity attacks and increasing data protection requirements across regulated industries to drive market

11.3 EUROPE

11.3.1 EUROPE: MARKET DRIVERS

11.3.2 EUROPE: MACROECONOMIC OUTLOOK

11.3.3 UK

11.3.3.1 Increasing cyber threats and need for robust security measures to accelerate market growth

11.3.4 GERMANY

11.3.4.1 Rising cyber threats, regulatory requirements, and increasing complexity of cyberattacks to bolster market growth

11.3.5 FRANCE

11.3.5.1 Burgeoning cybersecurity threats and digital transformation to boost market

11.3.6 ITALY

11.3.6.1 Rising significance of proactive security measures to foster market growth

11.3.7 REST OF EUROPE

11.4 ASIA PACIFIC

11.4.1 ASIA PACIFIC: MARKET DRIVERS

11.4.2 ASIA PACIFIC: MACROECONOMIC OUTLOOK

11.4.3 CHINA

11.4.3.1 Rapid digitalization and rising collaborations with managed service companies to drive market

11.4.4 JAPAN

11.4.4.1 Rising digital transformation and growing cybersecurity demands to foster market growth

11.4.5 INDIA

11.4.5.1 Substantial internet penetration, skilled IT workforce, and government support to aid market growth

11.4.6 REST OF ASIA PACIFIC

11.5 MIDDLE EAST & AFRICA

11.5.1 MIDDLE EAST & AFRICA: MARKET DRIVERS

11.5.2 MIDDLE EAST & AFRICA: MACROECONOMIC OUTLOOK

11.5.3 GCC

11.5.3.1 Cloud adoption and integration with other security tools to boost market

11.5.3.2 KSA

11.5.3.2.1 Fundamental digital transformation and rising need for robust data protection to boost market growth

11.5.3.3 UAE

11.5.3.3.1 Increasing cyber threats, regulatory demands, and growing cybersecurity awareness to promote market growth

11.5.3.4 Rest of GCC

11.5.4 SOUTH AFRICA

11.5.4.1 Dramatic increase in ransomware attacks to drive market

11.5.5 REST OF MIDDLE EAST & AFRICA

11.6 LATIN AMERICA

11.6.1 LATIN AMERICA: AUTOMATED BREACH AND ATTACK SIMULATION MARKET DRIVERS

11.6.2 LATIN AMERICA: MACROECONOMIC OUTLOOK

11.6.3 BRAZIL

11.6.3.1 Government initiatives and emergent technologies to propel market growth

11.6.4 MEXICO

11.6.4.1 Stringent regulatory compliance demands to drive market

11.6.5 REST OF LATIN AMERICA

12 COMPETITIVE LANDSCAPE

12.1 KEY PLAYER STRATEGIES/RIGHT TO WIN

12.2 REVENUE ANALYSIS

12.3 MARKET SHARE ANALYSIS, 2023

12.4 BRAND COMPARISON

12.5 COMPANY VALUATION AND FINANCIAL METRICS

12.5.1 COMPANY VALUATION

12.5.2 FINANCIAL METRICS USING EV/EBITDA

12.6 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2023

12.6.1 STARS

12.6.2 EMERGING LEADERS

12.6.3 PERVASIVE PLAYERS

12.6.4 PARTICIPANTS

12.6.5 COMPANY FOOTPRINT: KEY PLAYERS, 2023

12.6.5.1 Company footprint

- 12.6.5.2 Regional footprint
- 12.6.5.3 Deployment mode footprint
- 12.6.5.4 Vertical footprint

12.7 COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2023

- 12.7.1 PROGRESSIVE COMPANIES
- 12.7.2 RESPONSIVE COMPANIES
- 12.7.3 DYNAMIC COMPANIES
- 12.7.4 STARTING BLOCKS
- 12.7.5 COMPETITIVE BENCHMARKING: STARTUPS/SMES, 2023
 - 12.7.5.1 Detailed list of key startups/SMEs
 - 12.7.5.2 Competitive benchmarking of key startups/SMEs

12.8 COMPETITIVE SCENARIO

- 12.8.1 PRODUCT LAUNCHES & ENHANCEMENTS
- 12.8.2 DEALS

13 COMPANY PROFILES

13.1 KEY PLAYERS

- 13.1.1 CYMULATE
 - 13.1.1.1 Business overview
 - 13.1.1.2 Products/Solutions/Services offered
 - 13.1.1.3 Recent developments
 - 13.1.1.3.1 Product launches & enhancements
 - 13.1.1.3.2 Deals
 - 13.1.1.3.3 Other developments
 - 13.1.1.4 MnM view
 - 13.1.1.4.1 Key strengths
 - 13.1.1.4.2 Strategic choices
 - 13.1.1.4.3 Weaknesses and competitive threats
- 13.1.2 ATTACKIQ
 - 13.1.2.1 Business overview
 - 13.1.2.2 Products/Solutions/Services offered
 - 13.1.2.3 Recent developments
 - 13.1.2.3.1 Product launches & enhancements
 - 13.1.2.3.2 Deals
 - 13.1.2.4 MnM view
 - 13.1.2.4.1 Key strengths
 - 13.1.2.4.2 Strategic choices
 - 13.1.2.4.3 Weaknesses and competitive threats

13.1.3 XM CYBER

13.1.3.1 Business overview

13.1.3.2 Products/Solutions/Services offered

13.1.3.3 MnM view

13.1.3.3.1 Key strengths

13.1.3.3.2 Strategic choices

13.1.3.3.3 Weaknesses and competitive threats

13.1.4 SAFE BREACH

13.1.4.1 Business overview

13.1.4.2 Products/Solutions/Services offered

13.1.4.3 Recent developments

13.1.4.3.1 Product launches & enhancements

13.1.4.3.2 Deals

13.1.4.4 MnM view

13.1.4.4.1 Key strengths

13.1.4.4.2 Strategic choices

13.1.4.4.3 Weaknesses and competitive threats

13.1.5 PICUS SECURITY

13.1.5.1 Business overview

13.1.5.2 Products/Solutions/Services offered

13.1.5.3 Recent developments

13.1.5.3.1 Product launches & enhancements

13.1.5.4 MnM view

13.1.5.4.1 Key strengths

13.1.5.4.2 Strategic choices

13.1.5.4.3 Weaknesses and competitive threats

13.1.6 QUALYS

13.1.6.1 Business overview

13.1.6.2 Products/Solutions/Services offered

13.1.6.3 Recent developments

13.1.6.3.1 Product launches & enhancements

13.1.6.3.2 Deals

13.1.7 RAPID7

13.1.7.1 Business overview

13.1.7.2 Products/Solutions/Services offered

13.1.7.3 Recent developments

13.1.7.3.1 Product launches & enhancements

13.1.7.3.2 Deals

13.1.8 IBM

- 13.1.8.1 Business overview
- 13.1.8.2 Products/Solutions/Services offered
- 13.1.8.3 Recent developments
 - 13.1.8.3.1 Product launches & enhancements
 - 13.1.8.3.2 Deals
 - 13.1.8.3.3 Other developments
- 13.1.9 FORTINET
 - 13.1.9.1 Business overview
 - 13.1.9.2 Products/Solutions/Services offered
 - 13.1.9.3 Recent developments
 - 13.1.9.3.1 Product launches & enhancements
- 13.1.10 MANDIANT
 - 13.1.10.1 Business overview
 - 13.1.10.2 Products/Solutions/Services offered
- 13.1.11 KEYSIGHT TECHNOLOGIES
 - 13.1.11.1 Business overview
 - 13.1.11.2 Products/Solutions/Services offered
 - 13.1.11.3 Recent developments
 - 13.1.11.3.1 Product launches & enhancements
 - 13.1.11.3.2 Deals
- 13.1.12 AUJAS
 - 13.1.12.1 Business overview
 - 13.1.12.2 Products/Solutions/Services offered
- 13.2 OTHER PLAYERS
 - 13.2.1 CYTOMATE
 - 13.2.2 RELIAQUEST
 - 13.2.3 DETECTIFY
 - 13.2.4 SCYTHE
 - 13.2.5 BREACHLOCK
 - 13.2.6 CYCOGNITO
 - 13.2.7 SKYBOX SECURITY
 - 13.2.8 AQUILA I
 - 13.2.9 IMMUNIWEB
 - 13.2.10 THREATGEN
 - 13.2.11 STROBES SECURITY
 - 13.2.12 NOPSEC
 - 13.2.13 SIMSPACE
 - 13.2.14 PURPLEBOX
 - 13.2.15 KROLL

14 ADJACENT MARKETS

14.1 INTRODUCTION

14.2 LIMITATIONS

14.3 PENETRATION-TESTING-AS-A-SERVICE MARKET

14.4 SECURITY AND VULNERABILITY MARKET

15 APPENDIX

15.1 DISCUSSION GUIDE

15.2 KNOWLEDGESTORE: MARKETSANDMARKETS' SUBSCRIPTION PORTAL

15.3 CUSTOMIZATION OPTIONS

15.4 RELATED REPORTS

15.5 AUTHOR DETAILS

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**

Customer 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

and fax the completed form to +44 20 7900 3970