Generative AI Cybersecurity Market Size, Share, Growth Analysis, By Generative AI-native Tools (Threat Hunting, Remediation), Cybersecurity Tools for Generative AI (Model Security, Data Security), End-user and Region - Global Industry Forecast to 2030

https://marketpublishers.com/r/GA9F1AD0FC90EN.html
Date: July 2024
Pages: 484
Price: US$ 3,217.50 (Single User License)
ID: GA9F1AD0FC90EN

Abstracts

The Generative AI cybersecurity market is estimated to accrue a market value of USD 7.1 billion in 2024 and reach USD 40.1 billion by 2030, at a compound annual growth rate (CAGR) of 33.4% between 2024–2030. The generative AI cybersecurity market is rapidly expanding because of two considerations. On one hand, enterprises are increasingly implementing generative AI-powered security solutions to improve threat detection and response capabilities, resulting in a greatly improved overall security posture. The other major driving factor is booming use of generative AI in several industries which has resulted in the establishment of a unique market area devoted to safeguarding AI systems. These include protecting training data, preventing model tampering, and verifying the accuracy of AI-generated results.

“By offering, cybersecurity software for generative AI segment is expected to register the fastest market growth rate during the forecast period.”

Several significant factors have contributed to the continued adoption of cybersecurity software for generative AI. As generative AI technology gets more widely used, its potential flaws and the value of the data it handles make it an appealing target for cyber criminals. Enterprises are increasingly becoming dependent on generative AI for a variety of applications, ranging from content generation to decision-making processes, highlighting the necessity for strong security measures. The advanced nature of these generative models, specially LLMs, necessitates specialized security protocols that can efficiently reduce hazards. This growing reliance on generative AI, combined with increased awareness of cybersecurity vulnerabilities, is propelling the rapid growth of this section of the AI cybersecurity market.

“By security type, network security segment is expected to account for the largest market share during the forecast period.”

As more firms integrate generative AI into their networks, the complexity and volume of data processed has increased, making these networks excellent targets for cyber-attacks. This has led to a rapid rise of network security within the generative AI cybersecurity market, making it the largest segment by security type. The sensitive nature of the information handled by AI systems—ranging from personal data to confidential company insights—requires enhanced security measures. Furthermore, as remote work and cloud computing become the norm, protecting these interconnected systems from intrusions has never been more important. The increased awareness of possible risks, combined with the critical requirement to protect AI-driven processes, pulls the network security segment to the forefront of cybersecurity market.

“By Region, North America to have the largest market share in 2024, and Asia Pacific is slated to grow at the fastest rate during the forecast period.”

High frequency of cyber threats, substantial investment in AI research, and an established technical infrastructure has pushed North America as the regional leader in the deployment of generative AI in cybersecurity. The region's thriving tech scene, which includes centers like Silicon Valley, has encouraged creativity and attracted sizeable investments for firms in cybersecurity and artificial intelligence. US based vendors, such as IBM and AWS, are developing cybersecurity guardrails to protect generative AI infrastructure. On the other hand, companies such as Sophos and Palo Alto have infused generative AI into their cybersecurity products for increased threat protection. The US government has also recognized generative AI as an important tool for national security, initiating programs like the National AI Initiative Act.

Asia Pacific is the fastest growing regional market due to digital transformation and massive investments in integrating AI with cybersecurity. China, India and Australia are leading the charge, with China’s security spend expected to exceed USD 50 billion by 2026. The region is also experiencing a huge volume of attacks - over 1,800 cyberattacks per organization in early 2023. Government support and investment in innovation is helping organizations integrate generative AI into their cybersecurity frameworks. This combination of high threat, investment and regulation makes Asia Pacific the adopter of new cybersecurity technologies.

Breakdown of primaries

In-depth interviews were conducted with Chief Executive Officers (CEOs), innovation and technology directors, system integrators, and executives from various key organizations operating in the Generative AI cybersecurity market.

Research coverage

This research report categorizes the Generative AI cybersecurity Market by Offering (Software and Services), by Software Type (Generative AI-based Cybersecurity

Software, Cybersecurity Software for Generative AI), by Software Deployment Mode [Cloud and On-premises]), by Services (Professional Services [Training & Consulting, System Integration & Implementation, and Support & Maintenance] and Managed Services), by Generative AI-based Cybersecurity (Threat Detection & Intelligence Software, Risk Assessment Software, Exposure Management Software, Phishing Simulation & Prevention Software, Remediation Guidance Software, Threat Hunting Platforms, Code Analysis Software), by Cybersecurity for Generative AI (Generative AI Training Data Security, Generative AI Model Security, Generative AI Infrastructure Security, Generative AI Application Security), by Security Type (Database Security, Network Security, Endpoint Security, and Application Security), by End-user (enterprise end-users, cloud hyper scalers, generative AI providers, managed security service providers), and by Region (North America, Europe, Asia Pacific, Middle East & Africa, and Latin America). The scope of the report covers detailed information regarding the major factors, such as drivers, restraints, challenges, and opportunities, influencing the growth of the generative AI cybersecurity market. A detailed analysis of the key industry players has been done to provide insights into their business overview, solutions, and services; key strategies; contracts, partnerships, agreements, new product & service launches, mergers and acquisitions, and recent developments associated with the generative AI cybersecurity market. Competitive analysis of upcoming startups in the generative AI cybersecurity market ecosystem is covered in this report.

Key Benefits of Buying the Report

The report would provide the market leaders/new entrants in this market with information on the closest approximations of the revenue numbers for the overall generative AI cybersecurity market and its subsegments. It would help stakeholders understand the competitive landscape and gain more insights better to position their business and plan suitable go-to-market strategies. It also helps stakeholders understand the pulse of the market and provides them with information on key market drivers, restraints, challenges, and opportunities.

The report provides insights on the following pointers:

- Analysis of key drivers (increased adoption of generative AI driving demand for cybersecurity solutions, Pressing demand of AI-powered security driving the generative AI cybersecurity market, stricter data regulations and compliance laws fueling demand for secure AI systems, and rising cyber threats spurring demand for generative AI cybersecurity solutions), restraints (rising privacy concerns hindering generative AI cybersecurity adoption, lack of combined AI-cybersecurity expertise stifling generative AI cybersecurity market growth, and high deployment costs of advanced generative AI security solutions prohibiting smaller organizations), opportunities (advancing AI research fueling development of more powerful cybersecurity solutions, scalable and customizable generative AI cybersecurity solutions unlocking wider market adoption, AI-cybersecurity collaboration fostering innovation and market growth for generative AI security solutions), and challenges (ethical and legal concerns around misuse and accountability hindering AI adoption in cybersecurity, evolving cyber threats demanding continuous advancements in AI security solutions, and high-quality data scarcity limiting effectiveness of generative AI cybersecurity solutions).

Product Development/Innovation: Detailed insights on upcoming technologies, research & development activities, and new product & service launches in the Generative AI cybersecurity market.

Market Development: Comprehensive information about lucrative markets – the report analyses the Generative AI cybersecurity market across varied regions.

Market Diversification: Exhaustive information about new products & services, untapped geographies, recent developments, and investments in the Generative AI cybersecurity market.

Competitive Assessment: In-depth assessment of market shares, growth strategies and service offerings of leading players like Microsoft (US), IBM (US), Google (US), SentinelOne (US), AWS (US), NVIDIA (US), Cisco (US), CrowdStrike (US), Fortinet (US), Zscaler (US), Trend Micro (Japan), Palo Alto Networks (US), BlackBerry (Canada), Darktrace (UK), F5 (US), Okta (US), Sangfor (China), SecurityScorecard (US), Sophos (UK), Broadcom (US), and Trellix (US), among others in the Generative AI cybersecurity market. The report also helps stakeholders understand the pulse of the Generative AI cybersecurity market and provides them with information on key market drivers, restraints, challenges, and opportunities.

Contents

1 INTRODUCTION

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

2 RESEARCH METHODOLOGY

2.1 RESEARCH DATA
  2.1.1 SECONDARY DATA
  2.1.2 PRIMARY DATA
    2.1.2.1 Breakup of primary profiles
    2.1.2.2 Key insights from industry experts
2.2 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 RESEARCH LIMITATIONS

3 EXECUTIVE SUMMARY

4 PREMIUM INSIGHTS

4.1 ATTRACTIVE OPPORTUNITIES FOR KEY PLAYERS IN GENERATIVE AI CYBERSECURITY MARKET
4.2 GENERATIVE AI CYBERSECURITY MARKET: TOP THREE SECURITY TYPES
4.3 NORTH AMERICA: GENERATIVE AI CYBERSECURITY MARKET, BY OFFERING AND SECURITY TYPE
4.4 GENERATIVE AI CYBERSECURITY MARKET, BY REGION

5 MARKET OVERVIEW AND INDUSTRY TRENDS

5.1 INTRODUCTION
5.2 MARKET DYNAMICS
5.2.1 DRIVERS
5.2.1.1 Increased adoption of generative AI driving demand for cybersecurity solutions
5.2.1.2 Increased awareness of AI security needs
5.2.1.3 Stricter data regulations and compliance laws fueling demand for secure AI systems
5.2.1.4 Rising cyber threats spurring demand for generative AI cybersecurity solutions
5.2.2 RESTRAINTS
5.2.2.1 Rising privacy concerns hindering adoption of generative AI cybersecurity adoption
5.2.2.2 Lack of combined AI-cybersecurity expertise stifling market growth
5.2.3 OPPORTUNITIES
5.2.3.1 Rapid advancements in AI research fueling development of more powerful cybersecurity solutions
5.2.3.2 Increasing adoption of scalable and customizable generative AI cybersecurity solutions
5.2.3.3 Growing collaboration between AI and cybersecurity fostering innovation and market growth
5.2.4 CHALLENGES
5.2.4.1 Ethical and legal concerns around misuse and accountability
5.2.4.2 Evolving cyber threat landscape
5.3 TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS
5.4 PRICING ANALYSIS
5.4.1 AVERAGE SELLING PRICE TREND OF KEY PLAYERS, BY SOFTWARE TYPE
5.4.2 INDICATIVE PRICING ANALYSIS, BY OFFERING
5.5 SUPPLY CHAIN ANALYSIS
5.6 ECOSYSTEM ANALYSIS
5.6.1 GENERATIVE AI-BASED CYBERSECURITY TOOL PROVIDERS
5.6.2 CYBERSECURITY TOOL PROVIDERS FOR GENERATIVE AI
5.6.3 GENERATIVE AI CYBERSECURITY SERVICE PROVIDERS
5.6.4 CLOUD HYPERSCALERS
5.6.5 ENTERPRISE END USERS
5.6.6 GOVERNMENT AND REGULATORY BODIES

5.7 TECHNOLOGY ANALYSIS
5.7.1 KEY TECHNOLOGIES
5.7.1.1 Adversarial Machine Learning (AML)
5.7.1.2 Federated learning
5.7.1.3 Differential privacy
5.7.1.4 Homomorphic encryption
5.7.1.5 Secure Multi-Party Computation (SMPC)
5.7.2 COMPLEMENTARY TECHNOLOGIES
5.7.2.1 Blockchain
5.7.2.2 Zero-Trust Architecture (ZTA)
5.7.2.3 Endpoint Detection and Response (EDR)
5.7.2.4 Vulnerability management
5.7.3 ADJACENT TECHNOLOGIES
5.7.3.1 Quantum computing
5.7.3.2 DevSecOps
5.7.3.3 Forensics and incident response
5.7.3.4 Big data analytics
5.8 GENERATIVE AI CYBERSECURITY TECHNOLOGY ROADMAP
5.9 GENERATIVE AI CYBERSECURITY BUSINESS MODELS
5.9.1 BUSINESS MODELS: GENERATIVE AI-BASED CYBERSECURITY
5.9.1.1 Subscription-based model
5.9.1.2 AI licensing model
5.9.1.3 Consulting and implementation services model
5.9.2 BUSINESS MODELS: CYBERSECURITY FOR GENERATIVE AI
5.9.2.1 Subscription-based model
5.9.2.2 One-time license fee model
5.9.2.3 Pay-as-you-go model
5.9.2.4 Managed services model
5.10 PATENT ANALYSIS
5.10.1 METHODOLOGY
5.10.2 PATENTS FILED, BY DOCUMENT TYPE
5.10.3 INNOVATION AND PATENT APPLICATIONS
5.10.3.1 Top 10 applicants in generative AI cybersecurity market
5.11 KEY CONFERENCES AND EVENTS, 2024–2025
5.12 REGULATORY LANDSCAPE
5.12.1 REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS
5.12.2 REGULATIONS: GENERATIVE AI CYBERSECURITY
5.12.2.1 North America

5.12.2.1.1 US
5.12.2.1.1.1 Executive order on AI (US)
5.12.2.1.1.2 National Institute of Standards and Technology (NIST)
5.12.2.1.1.3 CISA’s AI roadmap
5.12.2.1.2 Canada
5.12.2.1.2.1 Artificial Intelligence and Data Act (AIDA)
5.12.2.1.2.2 Directive on automated decision-making
5.12.2.1.2.3 Canadian Centre for Cyber Security
5.12.2.1.2.4 Privacy guidelines
5.12.2.2 Europe
5.12.2.2.1 UK
5.12.2.2.1.1 Five cross-sectoral principles
5.12.2.2.1.2 AI cybersecurity code of practice
5.12.2.2.1.3 Generative AI Framework for HMG
5.12.2.2.2 Germany
5.12.2.2.2.1 General Data Protection Regulation (GDPR)
5.12.2.2.2.2 IT Security Act (IT-SiG 2.0)
5.12.2.2.2.3 AI strategy
5.12.2.2.3 France
5.12.2.2.3.1 AI for humanity strategy
5.12.2.2.3.2 National Commission for Informatics and Liberties (CNIL)
5.12.2.2.3.3 Cybersecurity framework
5.12.2.2.4 Italy
5.12.2.2.4.1 Italian Data Protection Code
5.12.2.2.4.2 National Cybersecurity Perimeter
5.12.2.2.4.3 AI strategy
5.12.2.2.5 Spain
5.12.2.2.5.1 Spanish Data Protection Agency (AEPD)
5.12.2.2.5.2 National Cybersecurity Strategy
5.12.2.2.5.3 AI strategy
5.12.2.2.6 Netherlands
5.12.2.2.6.1 Dutch Data Protection Authority (DPA)
5.12.2.2.6.2 National Cybersecurity Agenda (NCSA)
5.12.2.2.6.3 AI strategy
5.12.2.3 Asia Pacific
5.12.2.3.1 China
5.12.2.3.1.1 Interim Measures for Generative AI Services
5.12.2.3.1.2 Deep Synthesis and Algorithm Recommendation Measures
5.12.2.3.2 India

5.12.2.3.2.1 National Strategy on AI
5.12.2.3.2.2 Draft Personal Data Protection Bill
5.12.2.3.3 Japan
5.12.2.3.3.1 AI Strategy 2021
5.12.2.3.3.2 Act on Protection of Personal Information (APPI)
5.12.2.3.4 South Korea
5.12.2.3.4.1 AI National Strategy
5.12.2.3.4.2 Personal Information Protection Act (PIPA)
5.12.2.3.5 ASEAN
5.12.2.3.5.1 ASEAN framework on AI
5.12.2.3.5.2 National initiatives
5.12.2.3.6 Australia & New Zealand (ANZ)
5.12.2.3.6.1 Australia's AI ethics framework
5.12.2.3.6.2 New Zealand's AI principles
5.12.2.4 Middle East & Africa
5.12.2.4.1 United Arab Emirates (UAE)
5.12.2.4.1.1 UAE strategy for AI 2031
5.12.2.4.1.2 National AI programme
5.12.2.4.1.3 AI governance and regulatory frameworks
5.12.2.4.2 Kingdom of Saudi Arabia (KSA)
5.12.2.4.2.1 National Strategy for Data and AI (NSDAI)
5.12.2.4.2.2 Saudi Data and Artificial Intelligence Authority (SDAIA)
5.12.2.4.3 Kuwait
5.12.2.4.3.1 National AI and data strategy
5.12.2.4.3.2 Kuwait national cybersecurity strategy
5.12.2.4.4 Qatar
5.12.2.4.4.1 Qatar National Vision 2030
5.12.2.4.4.2 Qatar AI and cybersecurity initiatives
5.12.2.4.5 Turkey
5.12.2.4.5.1 National AI Strategy
5.12.2.4.5.2 Personal Data Protection Law (KVKK)
5.12.2.4.6 Egypt
5.12.2.4.6.1 National AI strategy
5.12.2.4.6.2 Egyptian cybersecurity regulations
5.12.2.4.7 Africa
5.12.2.4.7.1 African Union AI strategy
5.12.2.4.7.2 Country-specific initiatives
5.12.2.5 Latin America
5.12.2.5.1 Brazil

5.12.2.5.1.1 AI regulation framework
5.12.2.5.1.2 General Data Protection Law (LGPD)
5.12.2.5.1.3 National AI strategy
5.12.2.5.2 Mexico
5.12.2.5.2.1 Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP)
5.12.2.5.2.2 National digital strategy
5.12.2.5.2.3 AI governance initiatives
5.12.2.5.3 Argentina
5.12.2.5.3.1 Personal Data Protection Law
5.12.2.5.3.2 National AI Plan
5.12.2.5.3.3 Cybersecurity regulations
5.13 PORTER’S FIVE FORCES ANALYSIS
5.13.1 THREAT OF NEW ENTRANTS
5.13.2 THREAT OF SUBSTITUTES
5.13.3 BARGAINING POWER OF SUPPLIERS
5.13.4 BARGAINING POWER OF BUYERS
5.13.5 INTENSITY OF COMPETITIVE RIVALRY
5.14 KEY STAKEHOLDERS AND BUYING CRITERIA
5.14.1 KEY STAKEHOLDERS IN BUYING PROCESS
5.14.2 BUYING CRITERIA
5.15 EVOLUTION OF GENERATIVE AI CYBERSECURITY
5.16 INVESTMENT LANDSCAPE AND FUNDING SCENARIO
5.16.1 MOST VALUED CYBERSECURITY START-UPS, JULY 2024
5.16.2 GENERATIVE AI-BASED CYBERSECURITY START-UPS
5.16.3 START-UPS PROVIDING CYBERSECURITY FOR GENERATIVE AI
5.17 GUARDRAILS FOR LARGE LANGUAGE MODELS
5.17.1 NEED TO GUARDRAIL LLMS
5.17.2 THREE PILLARS OF LLM GUARDRAILS
5.17.2.1 Policy enforcement
5.17.2.2 Contextual understanding
5.17.2.3 Continous adaptability
5.17.3 TYPES OF LLM GUARDRAILS
5.17.3.1 Ethical guardrails
5.17.3.2 Compliance guardrails
5.17.3.3 Contextual guardrails
5.17.3.4 Security guardrails
5.17.3.5 Adaptive guardrails
5.17.4 IMPLEMENTING LLM GUARDRAILS

5.18 CASE STUDY ANALYSIS
5.18.1 BFSI
5.18.1.1 ZeroFox provided timely, actionable intelligence to shore up Simply Business's information security
5.18.1.2 Pomelo implemented several integrations to build end-to-end security program by deploying Snyk
5.18.2 TELECOMMUNICATIONS
5.18.2.1 Evocabank helped Nokia protect and engage with close to 28 million fans and followers online
5.18.2.2 Telenor reduced its vulnerability risk posture by integrating Snyk into its development process
5.18.3 HEALTHCARE
5.18.3.1 Sentara Healthcare determined most imminent threats by deploying Predictive Prioritization
5.18.4 CLOUD HYPERSCALERS
5.18.4.1 IBM enabled faster, more accurate threat detection and automated incident responses by using Palo Alto Networks' solutions
5.18.4.2 Oracle collaborated with Stellar Cyber and implemented Open Extended Detection and Response (XDR) platform on Oracle Cloud Infrastructure to detect and remediate threats early
5.18.5 GENERATIVE AI PROVIDERS
5.18.5.1 OpenAI partnered with Okta to contribute valuable insights and concentrate on creating groundbreaking AI technologies
5.18.5.2 NVIDIA partnered with Check Point to help secure cloud infrastructures at scale

6 GENERATIVE AI CYBERSECURITY MARKET, BY OFFERING

6.1 INTRODUCTION
6.1.1 OFFERINGS: GENERATIVE AI CYBERSECURITY MARKET DRIVERS
6.2 SOFTWARE, BY TYPE
6.2.1 GENERATIVE AI-BASED CYBERSECURITY SOFTWARE
6.2.1.1 Increasing sophistication of cyber threats and need for more adaptive and intelligent security measures to drive market
6.2.2 CYBERSECURITY SOFTWARE FOR GENERATIVE AI
6.2.2.1 Need for trustworthy and transparent AI systems and growing regulatory landscape around AI governance to propel market
6.3 SOFTWARE, BY DEPLOYMENT MODE
6.3.1 CLOUD

6.3.1.1 Increasing complexity and frequency of cyber threats, need for real-time security measures, and growing adoption of cloud computing and IoT technologies to foster market growth
6.3.2 ON-PREMISES
6.3.2.1 Growing complexity of cyber threats to drive on-premises deployment of generative AI cybersecurity solutions
6.4 SERVICES
6.4.1 PROFESSIONAL SERVICES
6.4.1.1 Increasing sophistication and frequency of cyber threats to fuel demand for professional services
6.4.1.1.1 Training & consulting services
6.4.1.1.2 System integration & implementation services
6.4.1.1.3 Support & maintenance services
6.4.2 MANAGED SERVICES
6.4.2.1 MSS to utilize generative AI to offer organizations proactive approach to cybersecurity

7 GENERATIVE AI CYBERSECURITY MARKET, BY GENERATIVE AI-BASED CYBERSECURITY SOFTWARE

7.1 INTRODUCTION
7.1.1 GENERATIVE AI-BASED CYBERSECURITY SOFTWARE: GENERATIVE AI CYBERSECURITY MARKET DRIVERS
7.2 THREAT DETECTION & INTELLIGENCE SOFTWARE
7.2.1 THREAT DETECTION AND INTELLIGENCE SOFTWARE TO SPOT UNUSUAL PATTERNS AND POTENTIAL THREATS IN REAL TIME AND KEEP DATA SAFE AND SECURE
7.2.1.1 Automated threat analysis
7.2.1.2 Security Information & Event Management (SIEM)
7.2.1.3 AI-native security analysis
7.2.1.4 Threat correlation
7.2.1.5 Threat intelligence
7.3 RISK ASSESSMENT SOFTWARE
7.3.1 RISK ASSESSMENT SOFTWARE TO ANALYZE DATA, IDENTIFY POTENTIAL RISKS, AND SUGGEST PREVENTIVE MEASURES
7.3.1.1 Automated risk insights
7.3.1.2 Impact analysis
7.3.1.3 Risk intelligence
7.3.1.4 Compliance automation

7.3.1.5 Other risk assessment software
7.4 EXPOSURE MANAGEMENT SOFTWARE
7.4.1 EXPOSURE MANAGEMENT SOFTWARE TO HELP ORGANIZATIONS KEEP TRACK OF THEIR DIGITAL ASSETS AND POTENTIAL VULNERABILITIES
7.4.1.1 Vulnerability analysis
7.4.1.2 Exposure prioritization
7.4.1.3 Automated exposure detection
7.4.1.4 Incident response
7.4.1.5 Other exponential management software
7.5 PHISHING SIMULATION & PREVENTION SOFTWARE
7.5.1 REALISTIC PHISHING SIMULATION AND PREVENTION SOFTWARE TO RECOGNIZE PHISHING ATTEMPTS AND PREVENT THEM
7.5.1.1 Phishing simulation campaigns
7.5.1.2 Phishing attack analysis
7.5.1.3 Deepfake detection
7.5.1.4 Fraud prevention
7.5.1.5 Social engineering detection
7.6 REMEDIATION GUIDANCE SOFTWARE
7.6.1 REMEDIATION GUIDANCE SOFTWARE TO HELP ORGANIZATIONS QUICKLY FIGURE OUT HOW TO FIX SECURITY PROBLEMS
7.6.1.1 Automated remediation
7.6.1.2 Interactive remediation support
7.6.1.3 Proactive threat management
7.6.1.4 Compliance remediation
7.6.1.5 Other remediation guidance software
7.7 THREAT HUNTING PLATFORMS
7.7.1 THREAT HUNTING PLATFORMS TO AUTOMATE ROUTINE TASKS AND ENABLE SECURITY EXPERTS TO FOCUS ON MORE COMPLEX ISSUES
7.7.1.1 Real-time threat analysis
7.7.1.2 Natural language query interface
7.7.1.3 Behavior analysis
7.7.1.4 Response automation
7.7.1.5 Other threat hunting platforms
7.8 CODE ANALYSIS SOFTWARE
7.8.1 CODE ANALYSIS SOFTWARE POWERED BY GENERATIVE AI TO DETECT AND MITIGATE THREATS
7.8.1.1 Code snippet analysis
7.8.1.2 Source code protection
7.8.1.3 Vulnerability detection

7.8.1.4 Automated code review
7.8.1.5 Compliance checks

8 GENERATIVE AI CYBERSECURITY MARKET, BY CYBERSECURITY SOFTWARE FOR GENERATIVE AI

8.1 INTRODUCTION
8.1.1 CYBERSECURITY SOFTWARE FOR GENERATIVE AI: GENERATIVE AI CYBERSECURITY MARKET DRIVERS
8.2 GENERATIVE AI TRAINING DATA SECURITY SOFTWARE
8.2.1 GENERATIVE AI TRAINING DATA SECURITY TO PROTECT DATA USED TO DEVELOP POWERFUL AI MODELS
8.2.1.1 Data integrity verification
8.2.1.2 Secure data augmentation
8.2.1.3 Automated data cleaning
8.2.1.4 Data quality monitoring
8.2.1.5 Data anonymization
8.3 GENERATIVE AI MODEL SECURITY SOFTWARE
8.3.1 GENERATIVE AI MODEL SECURITY SOFTWARE POISED TO MITIGATE RISKS ASSOCIATED WITH ITS ADOPTION
8.3.1.1 Model integrity
8.3.1.2 Adversarial training & testing
8.3.1.3 Secure model training environments
8.3.1.4 Model drift & bias detection
8.3.1.5 Robustness testing
8.4 GENERATIVE AI INFRASTRUCTURE SECURITY SOFTWARE
8.4.1 ORGANIZATIONS TO ENHANCE THEIR SECURITY POSTURE BY LEVERAGING GENERATIVE AI INFRASTRUCTURE SECURITY SOFTWARE
8.4.1.1 Continuous monitoring
8.4.1.2 Automated security patching
8.4.1.3 Secure API management
8.4.1.4 Real-time threat detection
8.4.1.5 Security audits
8.5 GENERATIVE AI APPLICATION SECURITY SOFTWARE
8.5.1 GENERATIVE AI APPLICATION SECURITY SOFTWARE TO PROVIDE BETTER ENCRYPTION TECHNIQUES TO PROTECT DATA WITHIN APPLICATIONS
8.5.1.1 Prompt injection security
8.5.1.2 Data leakage prevention
8.5.1.3 User authentication & access control

8.5.1.4 Monitoring & anomaly detection
8.5.1.5 Ethical AI governance

9 GENERATIVE AI CYBERSECURITY MARKET, BY SECURITY TYPE

9.1 INTRODUCTION
9.1.1 SECURITY TYPES: GENERATIVE AI CYBERSECURITY MARKET DRIVERS
9.2 DATABASE SECURITY
9.2.1 RISING DEMAND FOR DATABASE SECURITY DUE TO SURGE IN DATA BREACHES AND CYBERATTACKS TARGETING DATABASES TO FUEL MARKET GROWTH
9.2.1.1 Data Loss Prevention (DLP)
9.2.1.2 Data usage monitoring
9.2.1.3 Data compliance & governance
9.2.1.4 Data encryption
9.2.1.5 Data masking & tokenization
9.2.1.6 Access control
9.3 NETWORK SECURITY
9.3.1 RISE OF GENERATIVE AI TO ENHANCE NETWORK SECURITY MEASURES BY ENABLING MORE SOPHISTICATED THREAT DETECTION
9.3.1.1 Network Traffic Analysis (NTA)
9.3.1.2 Secure Access Service Edge (SASE)
9.3.1.3 Zero Trust Network Access (ZTNA)
9.3.1.4 Firewalls
9.3.1.5 Intrusion Detection/Prevention Systems (IDS/IPS)
9.3.1.6 VPNs & secure tunneling
9.4 ENDPOINT SECURITY
9.4.1 ENDPOINT SECURITY TO SAFEGUARD INDIVIDUAL DEVICES AND LEVERAGE ML ALGORITHMS TO PREDICT AND NEUTRALIZE THREATS IN REAL TIME
9.4.1.1 Endpoint Detection & Response (EDR)
9.4.1.2 Endpoint Protection Platforms (EPP)
9.5 APPLICATION SECURITY
9.5.1 DIFFUSION MODELS TO ENABLE GENERATION OF HIGHLY REALISTIC AND CONVINCING SYNTHETIC MEDIA
9.5.1.1 Static Application Security Testing (SAST)
9.5.1.2 Dynamic Application Security Testing (DAST)
9.5.1.3 LLM security
9.5.1.4 Runtime protection

9.5.1.5 Incident response & recovery
9.5.1.6 Governance, Risk, and Compliance (GRC)

10 GENERATIVE AI CYBERSECURITY MARKET, BY END USER

10.1 INTRODUCTION
10.1.1 END USERS: GENERATIVE AI CYBERSECURITY MARKET DRIVERS
10.2 END USERS: GENERATIVE AI-BASED CYBERSECURITY
10.2.1 GOVERNMENT & DEFENSE
10.2.1.1 Generative AI becoming an essential tool for government agencies and defense organizations
10.2.2 BFSI
10.2.2.1 Significant increase in cyber threats targeting financial institutions and compliance to regulations to drive market
10.2.3 IT/ITES
10.2.3.1 Generative AI to automate routine security tasks by reducing reliance on human intervention and improving response times
10.2.4 HEALTHCARE & LIFE SCIENCES
10.2.4.1 Rise in cyberattacks targeting healthcare systems and implementation of Internet of Medical Things (IoMT) to boost market growth
10.2.5 RETAIL & ECOMMERCE
10.2.5.1 Exponential increase in online transactions and rising incidents of cyber threats to foster market growth
10.2.6 MANUFACTURING
10.2.6.1 Need to implement sophisticated cybersecurity protocols that can detect and prevent unauthorized access to sensitive data to propel market
10.2.7 ENERGY & UTILITIES
10.2.7.1 Need to protect critical infrastructure from cyberattacks to drive demand for generative AI cybersecurity
10.2.8 TELECOMMUNICATIONS
10.2.8.1 Proliferation of connected devices to demand advanced security measures to manage and mitigate real-time risks
10.2.9 AUTOMOTIVE, TRANSPORTATION, AND LOGISTICS
10.2.9.1 Rapid technological advancements and need to secure vehicle communication systems and software to drive market
10.2.10 MEDIA & ENTERTAINMENT
10.2.10.1 Need for increasing digital content distribution and online streaming services to propel market
10.2.11 OTHER END USERS

10.3 END USERS: CYBERSECURITY FOR GENERATIVE AI
10.3.1 CLOUD HYPERSCALERS
10.3.1.1 Need for AI to help detect anomalies, assess risks, and respond to threats more efficiently to foster market growth
10.3.2 MANAGED SECURITY SERVICE PROVIDERS
10.3.2.1 Need for monitoring, threat detection, incident response, and compliance management to accelerate market growth
10.3.3 GENERATIVE AI PROVIDERS
10.3.3.1 Generative AI providers to offer advanced solutions to enhance detection, prevention, and response to cyber threats
10.3.3.1.1 Foundation model/LLM developers
10.3.3.1.2 Data annotators
10.3.3.1.3 Content creation platform providers
10.3.3.1.4 Generative AI-as-a-service provider

11 GENERATIVE AI CYBERSECURITY MARKET, BY REGION

11.1 INTRODUCTION
11.2 NORTH AMERICA
11.2.1 NORTH AMERICA: GENERATIVE AI CYBERSECURITY MARKET DRIVERS
11.2.2 NORTH AMERICA: MACROECONOMIC OUTLOOK
11.2.3 US
11.2.3.1 Robust technological infrastructure and culture of innovation to drive market
11.2.4 CANADA
11.2.4.1 Technological advancements and presence of leading companies to propel market
11.3 EUROPE
11.3.1 EUROPE: GENERATIVE AI CYBERSECURITY MARKET DRIVERS
11.3.2 EUROPE: MACROECONOMIC OUTLOOK
11.3.3 UK
11.3.3.1 UK's commitment to leveraging AI to stay ahead of evolving cyber threats to propel market
11.3.4 GERMANY
11.3.4.1 Rising incidents of cyberattacks and government initiatives to actively promote AI research to drive market
11.3.5 FRANCE
11.3.5.1 Strong focus on R&D and government initiatives to foster AI innovation to fuel market growth
11.3.6 ITALY

11.3.6.1 Increasing cyber threats, advancements in AI technology, and growing awareness of need for robust security measures to foster market growth
11.3.7 SPAIN
11.3.7.1 Rising focus on AI in cybersecurity to drive adoption of generative AI cybersecurity solutions
11.3.8 NETHERLANDS
11.3.8.1 Integration with advanced technologies and collaborative approach to foster innovation to accelerate market growth
11.3.9 REST OF EUROPE
11.4 ASIA PACIFIC
11.4.1 ASIA PACIFIC: GENERATIVE AI CYBERSECURITY MARKET DRIVERS
11.4.2 ASIA PACIFIC: MACROECONOMIC OUTLOOK
11.4.3 CHINA
11.4.3.1 Need for dynamic environment for developing sophisticated cybersecurity solutions to foster market growth
11.4.4 INDIA
11.4.4.1 Increasing cyber threats and urgent need for enhanced security measures to trigger market growth
11.4.5 JAPAN
11.4.5.1 Rising incidence of cyberattacks and need for advanced cybersecurity solutions to fuel market growth
11.4.6 SOUTH KOREA
11.4.6.1 Rising focus on synthetic media and AI technologies and investment in AI education and training programs to propel market
11.4.7 SINGAPORE
11.4.7.1 Robust digital infrastructure, supportive government policies, and emphasis on innovative technologies to drive market
11.4.8 AUSTRALIA & NEW ZEALAND
11.4.8.1 Changing regulatory landscape and increased emphasis on cybersecurity policies and frameworks to fuel market growth
11.4.9 REST OF ASIA PACIFIC
11.5 MIDDLE EAST & AFRICA
11.5.1 MIDDLE EAST & AFRICA: GENERATIVE AI CYBERSECURITY MARKET DRIVERS
11.5.2 MIDDLE EAST & AFRICA: MACROECONOMIC OUTLOOK
11.5.3 SAUDI ARABIA
11.5.3.1 Establishment of Center of Excellence (CoE) on Generative AI and R&D efforts on creating generative AI models to drive market
11.5.4 UAE

11.5.4.1 Major organizations to leverage generative AI for threat detection, risk assessment, and incident response
11.5.5 QATAR
11.5.5.1 QFC Data Protection Regulations to encourage organizations to invest in advanced cybersecurity measures
11.5.6 TURKEY
11.5.6.1 Turkish government's regulatory initiatives further enhancing country's readiness to tackle cybersecurity challenges effectively
11.5.7 REST OF MIDDLE EAST
11.5.8 AFRICA
11.5.8.1 Collaborative efforts between academia and industry to drive innovation and development of new AI models and surge in tech start-ups to foster market growth
11.6 LATIN AMERICA
11.6.1 LATIN AMERICA: GENERATIVE AI CYBERSECURITY MARKET DRIVERS
11.6.2 LATIN AMERICA: MACROECONOMIC OUTLOOK
11.6.3 BRAZIL
11.6.3.1 Rapid digital transformation and increasing awareness of cyber threats to accelerate market growth
11.6.4 MEXICO
11.6.4.1 Technological innovation, strategic regional initiatives, and technological advancements in AI to boost market growth
11.6.5 ARGENTINA
11.6.5.1 Rapid advancements in cybersecurity landscape and development of local start-ups focused on AI-driven security solutions to foster market growth
11.6.6 REST OF LATIN AMERICA

12 COMPETITIVE LANDSCAPE

12.1 OVERVIEW
12.2 KEY PLAYER STRATEGIES/RIGHT TO WIN
12.3 REVENUE ANALYSIS
12.4 MARKET SHARE ANALYSIS
12.4.1 MARKET SHARE OF KEY PLAYERS OFFERING GENERATIVE AI-BASED CYBERSECURITY
12.4.1.1 Degree of competition
12.4.2 MARKET SHARE OF KEY PLAYERS OFFERING CYBERSECURITY FOR GENERATIVE AI
12.4.2.1 Degree of competition
12.5 BRAND/PRODUCT COMPARISON

12.5.1 BRAND/PRODUCT COMPARISON: GENERATIVE AI-BASED CYBERSECURITY
12.5.1.1 Security Copilot (Microsoft)
12.5.1.2 Purple AI (SentinelOne)
12.5.1.3 Sec-PALM (Google)
12.5.1.4 Charlotte AI (CrowdStrike)
12.5.1.5 Prevent (DarkTrace)
12.5.1.6 ZDX Copilot (Zscaler)
12.5.1.7 FortiAI (Fortinet)
12.5.1.8 Precision AI (Palo Alto)
12.5.2 BRAND/PRODUCT COMPARISON: CYBERSECURITY FOR GENERATIVE AI
12.5.2.1 QRadar (IBM)
12.5.2.2 AI Runtime Security (Palo Alto)
12.5.2.3 Nitro Enclaves (AWS)
12.5.2.4 Zero Trust Exchange (Zscaler)
12.5.2.5 Defender Cloud (Microsoft)
12.5.2.6 Watsonx.governance (IBM)
12.5.2.7 Nemo LLM Guardrails (NVIDIA)
12.5.2.8 TruLens (True Era)
12.6 COMPANY VALUATION AND FINANCIAL METRICS
12.7 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2023
12.7.1 KEY PLAYERS OFFERING GENERATIVE AI-BASED CYBERSECURITY
12.7.1.1 Stars
12.7.1.2 Emerging leaders
12.7.1.3 Pervasive players
12.7.1.4 Participants
12.7.1.5 Company footprint: key players, 2023
12.7.1.5.1 Company footprint
12.7.1.5.2 Offering footprint
12.7.1.5.3 Security type footprint
12.7.1.5.4 End-user footprint
12.7.1.5.5 Regional footprint
12.7.2 KEY PLAYERS OFFERING CYBERSECURITY SOLUTIONS FOR GENERATIVE AI
12.7.2.1 Stars
12.7.2.2 Emerging leaders
12.7.2.3 Pervasive players
12.7.2.4 Participants
12.7.2.5 Company footprint: key players, 2023

12.7.2.5.1 Company footprint
12.7.2.5.2 Offering footprint
12.7.2.5.3 Security-type footprint
12.7.2.5.4 End-user footprint
12.7.2.5.5 Regional footprint
12.8 COMPANY EVALUATION MATRIX: START-UPS/SMES, 2023
12.8.1 PROGRESSIVE COMPANIES
12.8.2 RESPONSIVE COMPANIES
12.8.3 DYNAMIC COMPANIES
12.8.4 STARTING BLOCKS
12.8.5 COMPETITIVE BENCHMARKING: START-UPS/SMES, 2023
12.8.5.1 Detailed list of key start-ups/SMEs
12.8.5.2 Competitive benchmarking of key start-ups/SMEs
12.9 COMPETITIVE SCENARIO AND TRENDS
12.9.1 PRODUCT LAUNCHES AND ENHANCEMENTS
12.9.2 DEALS

13 COMPANY PROFILES

13.1 INTRODUCTION
13.2 KEY PLAYERS
13.2.1 MICROSOFT
13.2.1.1 Business overview
13.2.1.2 Products/Solutions/Services offered
13.2.1.3 Recent developments
13.2.1.4 MnM view
13.2.1.4.1 Right to win
13.2.1.4.2 Strategic choices made
13.2.1.4.3 Weaknesses and competitive threats
13.2.2 IBM
13.2.2.1 Business overview
13.2.2.2 Products/Solutions/Services offered
13.2.2.3 Recent developments
13.2.2.4 MnM view
13.2.2.4.1 Right to win
13.2.2.4.2 Strategic choices made
13.2.2.4.3 Weaknesses and competitive threats
13.2.3 AWS
13.2.3.1 Business overview

13.2.3.2 Products/Solutions/Services offered
13.2.3.3 Recent developments
13.2.3.4 MnM view
13.2.3.4.1 Right to win
13.2.3.4.2 Strategic choices made
13.2.3.4.3 Weaknesses and competitive threats
13.2.4 GOOGLE
13.2.4.1 Business overview
13.2.4.2 Products/Solutions/Services offered
13.2.4.3 Recent developments
13.2.4.4 MnM view
13.2.4.4.1 Right to win
13.2.4.4.2 Strategic choices made
13.2.4.4.3 Weaknesses and competitive threats
13.2.5 SENTITELONE
13.2.5.1 Business overview
13.2.5.2 Products/Solutions/Services offered
13.2.5.3 Recent developments
13.2.5.4 MnM view
13.2.5.4.1 Right to win
13.2.5.4.2 Strategic choices made
13.2.5.4.3 Weaknesses and competitive threats
13.2.6 NVIDIA
13.2.6.1 Business overview
13.2.6.2 Products/Solutions/Services offered
13.2.6.3 Recent developments
13.2.7 CISCO
13.2.7.1 Business overview
13.2.7.2 Products/Solutions/Services offered
13.2.7.3 Recent developments
13.2.8 CROWDSTRIKE
13.2.8.1 Business overview
13.2.8.2 Products/Solutions/Services offered
13.2.8.3 Recent developments
13.2.9 FORTINET
13.2.9.1 Business overview
13.2.9.2 Products/Products/Solutions/Services offered
13.2.9.3 Recent developments
13.2.10 ZSCALER

13.2.10.1 Business overview
13.2.10.2 Products/Products/Solutions/Services offered
13.2.10.3 Recent developments
13.2.11 TREND MICRO
13.2.12 PALO ALTO NETWORKS
13.2.13 BLACKBERRY
13.2.14 DARKTRACE
13.2.15 F5
13.2.16 OKTA
13.2.17 SANGFOR TECHNOLOGIES
13.2.18 VERACODE
13.2.19 LEXISNEXIS
13.2.20 SECURITYSCORECARD
13.2.21 SOPHOS
13.2.22 BROADCOM
13.2.23 TRELLIX
13.2.24 TENABLE
13.2.25 COHESITY
13.2.26 ELASTIC NV
13.2.27 SNYK
13.3 START-UPS/SMES
13.3.1 ABNORMAL SECURITY
13.3.2 ADVERSA AI
13.3.3 AQUASEC
13.3.4 BIGID
13.3.5 CHECKMARX
13.3.6 CREDO AI
13.3.7 CYBEREASON
13.3.8 DEEPKEEP
13.3.9 FLASHPOINT
13.3.10 LAKERA
13.3.11 MOSTLY AI
13.3.12 RECORDED FUTURE
13.3.13 SECUREFRAME
13.3.14 SKYFLOW
13.3.15 SLASHNEXT
13.3.16 TROJAI
13.3.17 VIRUSTOTAL
13.3.18 XENONSTACK

13.3.19 ZEROFOX

14 ADJACENT AND RELATED MARKETS

14.1 INTRODUCTION
14.2 GENERATIVE AI MARKET – GLOBAL FORECAST TO 2030
14.2.1 MARKET DEFINITION
14.2.2 MARKET OVERVIEW
14.2.2.1 Generative AI market, by offering
14.2.2.2 Generative AI market, by data modality
14.2.2.3 Generative AI market, by application
14.2.2.4 Generative AI market, by vertical
14.2.2.5 Generative AI market, by region
14.3 ARTIFICIAL INTELLIGENCE IN CYBERSECURITY MARKET – GLOBAL FORECAST TO 2028
14.3.1 MARKET DEFINITION
14.3.2 MARKET OVERVIEW
14.3.2.1 Artificial intelligence in cybersecurity market, by offering
14.3.2.2 Artificial intelligence in cybersecurity market, by security type
14.3.2.3 Artificial intelligence in cybersecurity market, by technology
14.3.2.4 Artificial intelligence in cybersecurity market, by application
14.3.2.5 Artificial intelligence in cybersecurity market, by vertical
14.3.2.6 Artificial intelligence in cybersecurity market, by region

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:	Generative AI Cybersecurity Market Size, Share, Growth Analysis, By Generative AI-native Tools (Threat Hunting, Remediation), Cybersecurity Tools for Generative AI (Model Security, Data Security), End-user and Region - Global Industry Forecast to 2030
Product link:	https://marketpublishers.com/r/GA9F1AD0FC90EN.html
Price:	US$ 3,217.50 (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/GA9F1AD0FC90EN.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 and fax the completed form to +44 20 7900 3970