+357 96 030922
info@marketpublishers.com

Generative AI Cybersecurity Market Forecasts to 2030 – Global Analysis By Type (Threat Detection & Analysis, Adversarial Defense, Insider Threat Detection, C Network Security and Other Types), Component, Technology, Application, End User and By Geography

https://marketpublishers.com/r/GE0A9B217469EN.html
Date: February 2025
Pages: 150
Price: US$ 4,150.00 (Single User License)
ID: GE0A9B217469EN

Abstracts

According to Stratistics MRC, the Global Generative AI Cybersecurity Market is accounted for $7.1 billion in 2024 and is expected to reach $43.7 billion by 2030 growing at a CAGR of 35.4% during the forecast period. Generative AI cybersecurity is a method that uses artificial intelligence to protect digital assets, networks, and systems from cyber threats. It involves using AI models that can generate solutions, strategies, or countermeasures to detect, analyze, and respond to cybersecurity risks. These models, often powered by deep learning and natural language processing, can identify patterns in vast amounts of data, simulate attack scenarios, and predict potential vulnerabilities in real time. Generative AI can automate tasks like anomaly detection, threat modeling, and risk assessment, enabling faster identification of potential breaches or attacks.

Market Dynamics:

Driver:

Increasing frequency and sophistication of cyber attacks

The cyber threat landscape is constantly evolving, with attacks becoming increasingly frequent, sophisticated, and impactful. Cybercriminals are employing advanced

+357 96 030922
info@marketpublishers.com

techniques like zero-day exploits, ransomware, and phishing attacks to infiltrate networks, steal data, and disrupt critical operations. Traditional security measures are often insufficient to detect and respond to these evolving threats. Generative AI offers a powerful solution by enabling organizations to proactively identify and mitigate these sophisticated attacks through advanced threat detection capabilities propelling the market growth.

Restraint:

Data privacy concerns

The use of generative AI in cybersecurity necessitates the collection and analysis of vast amounts of data, including sensitive information about individuals and organizations. This raises significant concerns about data privacy and security. Improper handling of sensitive data can lead to severe consequences, including reputational damage, legal liabilities, and financial losses. Organizations must carefully consider data privacy regulations and implement robust data protection measures to ensure the ethical and responsible use of AI in cybersecurity which hampers the market growth.

Opportunity:

Automated response & improved security posture

Generative AI empowers organizations to automate various aspects of cybersecurity operations, such as threat hunting, incident response, and vulnerability management. By automating these tasks, organizations can free up security teams to focus on more strategic initiatives, such as threat intelligence analysis and security strategy development. Furthermore, AI can continuously analyze vast amounts of data to identify patterns and anomalies, providing valuable insights into an organization's security posture. This allows organizations to proactively identify and address vulnerabilities, significantly reducing their overall risk exposure.

Threat:

Complexity of implementation

Implementing and maintaining AI-powered cybersecurity solutions can be complex and challenging. Organizations require skilled professionals with expertise in both AI and

+357 96 030922
info@marketpublishers.com

cybersecurity to effectively integrate and manage these solutions. Additionally, integrating AI-powered tools with existing security infrastructure can be complex and time-consuming. Furthermore, the rapid evolution of AI technology necessitates continuous learning and adaptation, requiring organizations to invest in ongoing training and development for their security teams impeding the market growth.

Covid-19 Impact

The Covid-19 pandemic significantly accelerated the shift towards remote work and digitalization, increasing the attack surface for cybercriminals. The sudden surge in remote work environments created new vulnerabilities and increased the risk of cyberattacks. This heightened the need for robust cybersecurity solutions, driving increased demand for AI-powered security technologies. Besides, the pandemic emphasized the importance of business continuity and resilience, leading organizations to invest more heavily in cybersecurity measures to ensure uninterrupted operations in the face of unforeseen disruptions.

The threat detection & analysis segment is expected to be the largest during the forecast period

The threat detection & analysis segment is expected to account for the largest market share during the forecast period due to enhanced proactive security measures by identifying patterns and anomalies that signal potential cyber threats. These models can also predict attacks, helping organizations anticipate them before they occur. This shift from reactive to proactive security strengthens defenses. Effective threat detection systems use AI to combat these AI-generated threats and can autonomously analyze malicious content and recommend or execute mitigation strategies in real-time.

The generative adversarial networks segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the generative adversarial networks segment is predicted to witness the highest growth rate owing to advanced threat simulation, improving cybersecurity measures, and enhancing anomaly detection. They can generate realistic but benign anomalies, enhancing intrusion detection systems. On the other hand, GANs can be used for sophisticated phishing and deepfake attacks, creating convincing phishing emails, voices, or videos. They can also generate malware that bypasses traditional detection methods boosting the markets growth.

+357 96 030922
info@marketpublishers.com

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share due to leading AI research institutions, tech companies, and cybersecurity startups, is a hub for innovation in generative AI applications. Businesses and government agencies often adopt advanced technologies like generative AI for threat detection and automated response. The region faces increased cyber threats like ransomware, phishing, and advanced persistent threats, necessitating the need for generative AI solutions encouraging the regions market.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR owing to China and South Korea investing heavily in AI research and development, particularly generative AI for cybersecurity. Governments and enterprises prioritize robust cyber defenses to safeguard critical data. Stricter data protection laws, such as China's Cybersecurity Law and India's Digital Personal Data Protection Act, are pushing businesses to adopt advanced security measures. The booming e-commerce and FinTech sectors in APAC, particularly India and Southeast Asia, require advanced AI-driven cybersecurity solutions to combat fraud and protect transactions.

Key players in the market

Some of the key players in Generative AI Cybersecurity market include Acalvio Technologies, Inc., Amazon Web Services, Inc., BlackBerry Limited, Capgemini S.A., Cisco Systems, Inc., CrowdStrike, Inc., Cylance Inc, Darktrace, FireEye, Inc., Fortinet, Inc., Google LLC, HCL Technologies Limited, IBM Corporation, Intel Corporation, LexisNexis, Micron Technology, Inc., Microsoft Corporate and NVIDIA Corporation.

Key Developments:

In January 2025, Walmart GoLocal, Walmart’s white-label delivery service for retailers, and IBM announced the integration of Walmart GoLocal into IBM Sterling Order Management, combining a leading order management platform with last-mile delivery.

In November 2024, Cisco, announced an expanded partnership to transform how global enterprises access wireless connectivity. As demand for flexible and cost-effective connectivity surges, Cisco and NTT DATA are responding with a unified solution backed by world-class support services from both companies.

+357 96 030922
info@marketpublishers.com

In September 2024, IBM announced its intent to acquire Accelalpha, a global Oracle services provider with deep expertise helping clients digitize core business operations and accelerate adoption of Oracle Cloud Applications.

Types Covered:

- Threat Detection & Analysis
- Adversarial Defense
- Insider Threat Detection
- Network Security
- Other Types

Components Covered:

- Hardware
- Software
- Services
- Other Components

Technologies Covered:

- Generative Adversarial Networks
- Variational Autoencoders
- Reinforcement Learning
- Deep Neural Networks

+357 96 030922
info@marketpublishers.com

- Natural Language Processing
- Other Technologies

Applications Covered:

- Zero-Day Threat Detection
- Traffic Analysis
- Sensitive Data Identification
- Phishing & Malware Detection
- Anomaly Detection
- Intrusion Detection & Prevention Systems
- Incident Analysis & Forensics
- Encrypted Traffic Analysis
- Behavioral Analytics & Privileged Access Monitoring
- Automated Threat Response
- Other Applications

End Users Covered:

- Banking, Financial Services, and Insurance
- Healthcare & Life Sciences
- Government & Defense
- Retail & E-Commerce

+357 96 030922
info@marketpublishers.com

- Information Technology (IT) & Telecommunications
- Energy & Utilities
- Other End Users

Regions Covered:

- North America
  - US
  - Canada
  - Mexico
- Europe
  - Germany
  - UK
  - Italy
  - France
  - Spain
  - Rest of Europe
- Asia Pacific
  - Japan
  - China
  - India

+357 96 030922
info@marketpublishers.com

- Australia
- New Zealand
- South Korea
- Rest of Asia Pacific

South America

- Argentina
- Brazil
- Chile
- Rest of South America

Middle East & Africa

- Saudi Arabia
- UAE
- Qatar
- South Africa
- Rest of Middle East & Africa

What our report offers:
- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2022, 2023, 2024, 2026, and 2030
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market

+357 96 030922
info@marketpublishers.com

estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

11 KEY DEVELOPMENTS

12 COMPANY PROFILING

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Generative AI Cybersecurity Market Forecasts to 2030 – Global Analysis By Type (Threat Detection & Analysis, Adversarial Defense, Insider Threat Detection, C Network Security and Other Types), Component, Technology, Application, End User and By Geography

Product link: https://marketpublishers.com/r/GE0A9B217469EN.html

Price: US$ 4,150.00 (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/GE0A9B217469EN.html