+357 96 030922
info@marketpublishers.com

AI in Cybersecurity Market Forecasts to 2032 - Global Analysis By Component (Solutions and Services), Security Type, Deployment Mode, Organization Size, End User and By Geography

https://marketpublishers.com/r/A63D101F8E25EN.html
Date: January 2026
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: A63D101F8E25EN

Abstracts

According to Stratistics MRC, the Global AI in Cybersecurity Market is accounted for $30.78 billion in 2025 and is expected to reach $145.17 billion by 2032 growing at a CAGR of 24.8% during the forecast period. Artificial Intelligence (AI) in cybersecurity refers to the application of machine learning, deep learning, and data analytics techniques to protect digital systems, networks, and data from cyber threats. AI enables security solutions to automatically detect anomalies, identify malware, predict potential attacks, and respond to incidents in real time. By analyzing large volumes of security data, AI improves threat intelligence, reduces false positives, and enhances decision-making accuracy. It supports proactive defense mechanisms such as behavioral analysis, automated threat hunting, and adaptive security controls, helping organizations strengthen their cyber resilience against evolving and sophisticated cyberattacks.

Market Dynamics:

Driver:

Rising sophistication of cyberattacks

Enterprises face increasingly complex threats such as advanced persistent attacks, ransomware, and AI-driven intrusions. Traditional defense mechanisms are insufficient, driving demand for intelligent, adaptive security solutions. AI-powered platforms enable real-time detection, predictive analytics, and automated response to evolving threats.

+357 96 030922
info@marketpublishers.com

Governments and enterprises are investing heavily in AI-driven defense frameworks to strengthen resilience. Rising sophistication of cyberattacks is propelling growth in the market.

Restraint:

Shortage of skilled cybersecurity professionals

The shortage of skilled cybersecurity professionals remains a significant restraint for AI in cybersecurity adoption. Enterprises struggle to recruit and retain talent capable of managing AI-driven defense systems. This skills gap increases reliance on external consultants and slows internal innovation. Training and certification programs require substantial investment, adding to operational costs. Smaller organizations face greater challenges in building dedicated AI security teams. Shortage of skilled professionals is restraining widespread adoption of AI in cybersecurity despite strong demand.

Opportunity:

Expansion of AI-driven automation tools

Expansion of AI-driven automation tools is creating strong opportunities for the cybersecurity market. Automated platforms reduce manual intervention and improve efficiency in detecting and mitigating threats. AI-driven tools enable predictive analytics, anomaly detection, and adaptive defense strategies. Enterprises are increasingly embedding automation into workflows to strengthen resilience and reduce costs. Integration with cloud ecosystems and IoT platforms further amplifies adoption. Expansion of AI-driven automation tools is fostering significant growth opportunities in the AI in cybersecurity market.

Threat:

Data privacy and regulatory compliance risks

Data privacy and regulatory compliance risks are slowing adoption of AI in cybersecurity. Governments are imposing stricter mandates on data handling, monitoring, and reporting. Enterprises face rising costs due to compliance audits and consumer protection requirements. Frequent policy changes create uncertainty for long-term investment planning. Smaller organizations struggle to adapt to complex regulatory frameworks compared to larger players. Data privacy and compliance risks are

+357 96 030922
info@marketpublishers.com

restraining confidence and threatening consistent growth in the market.

Covid-19 Impact:

The Covid-19 pandemic accelerated demand for AI in cybersecurity as enterprises shifted to remote work and digital-first strategies. On one hand, budget constraints delayed some large-scale deployments. On the other hand, surging cyberattacks targeting remote employees and cloud platforms boosted adoption. Enterprises leveraged AI-driven defense systems to manage phishing, ransomware, and insider threats during the pandemic. The crisis reinforced the importance of resilient digital ecosystems and automated defense frameworks. Overall, Covid-19 boosted awareness of AI in cybersecurity as a strategic enabler of enterprise resilience.

The network security segment is expected to be the largest during the forecast period

The network security segment is expected to account for the largest market share during the forecast period driven by demand for real-time monitoring, intrusion detection, and adaptive defense across enterprise networks. Network security platforms enable organizations to safeguard critical infrastructure and sensitive data. Enterprises rely on AI-driven systems to strengthen resilience against evolving cyber threats. Demand for scalable network security is rising as digital adoption expands globally. Integration with cloud and IoT ecosystems further strengthens adoption.

The healthcare & life sciences segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the healthcare & life sciences segment is predicted to witness the highest growth rate supported by rising demand for secure management of patient records and medical research data. Healthcare organizations require advanced AI-driven frameworks to comply with strict regulations such as HIPAA. Big data platforms in genomics, telemedicine, and clinical trials are driving adoption of AI security solutions. Rising investment in digital health initiatives is reinforcing demand for robust defense systems. Integration of AI-driven analytics in healthcare further amplifies the need for secure infrastructures. As healthcare and life sciences accelerate digital adoption AI in cybersecurity is propelling growth in the market.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest

+357 96 030922
info@marketpublishers.com

market share driven by advanced IT infrastructure strong regulatory frameworks and early adoption of AI-driven cybersecurity solutions. The presence of leading technology providers and mature digital ecosystems supports large-scale deployments. Regulatory emphasis on compliance and privacy drives investment in robust AI defense platforms. Enterprises in North America prioritize resilience and customer trust in data-driven operations. High demand for secure cloud and IoT ecosystems further strengthens adoption.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR fueled by rapid industrialization expanding digital ecosystems and government-led cybersecurity initiatives across emerging economies. Countries such as China, India, and Southeast Asia are investing heavily in AI-driven defense infrastructures. Rising demand for e-commerce, fintech, and healthcare innovation strengthens adoption of advanced AI security solutions. Local enterprises are deploying cost-effective platforms to meet growing digital needs. Expanding digital ecosystems are reinforcing the role of AI in enterprise modernization.

Key players in the market

Some of the key players in AI in Cybersecurity Market include IBM Corporation, Microsoft Corporation, Amazon Web Services, Inc., Google LLC, Cisco Systems, Inc., Palo Alto Networks, Inc., Fortinet, Inc., Check Point Software Technologies Ltd., CrowdStrike Holdings, Inc., Darktrace Holdings Limited, FireEye, Inc. (Trellix), Splunk Inc., Rapid7, Inc., SentinelOne, Inc. and Trend Micro Incorporated.

Key Developments:

In June 2024, Google announced a strategic partnership with Wiz to integrate its cloud security posture management (CSPM) technology directly into Google's security operations platform. This collaboration aims to provide customers with a unified view of risks and AI-powered remediation across their cloud environments.

In November 2023, AWS and Splunk announced a strategic partnership to co-develop AI and cybersecurity solutions, integrating Splunk's security analytics with AWS's AI services like Amazon Bedrock. This collaboration aims to help enterprises better detect and respond to threats using generative AI.

+357 96 030922
info@marketpublishers.com

Components Covered:

- Solutions
- Services

Security Types Covered:

- Network Security
- Application Security
- Endpoint Security
- Cloud Security
- Data & Identity Security
- Other Security Types

Deployment Modes Covered:

- On-Premise
- Cloud-Based

Organization Sizes Covered:

- Small & Medium Enterprises (SMEs)
- Large Enterprises

End Users Covered:

- Information Technology & Telecom

+357 96 030922
info@marketpublishers.com

- Banking, Financial Services & Insurance (BFSI)
- Healthcare & Life Sciences
- Retail & E-commerce
- Manufacturing & Industrial
- Government & Public Sector
- Energy & Utilities
- Other End Users

Regions Covered:

- North America
  - US
  - Canada
  - Mexico
- Europe
  - Germany
  - UK
  - Italy
  - France
  - Spain
  - Rest of Europe

+357 96 030922
info@marketpublishers.com

- Asia Pacific
  - Japan
  - China
  - India
  - 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

+357 96 030922
info@marketpublishers.com

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 2024, 2025, 2026, 2028, and 2032
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market 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

1 EXECUTIVE SUMMARY

2 PREFACE

2.1 Abstract
2.2 Stake Holders
2.3 Research Scope
2.4 Research Methodology
  2.4.1 Data Mining
  2.4.2 Data Analysis
  2.4.3 Data Validation
  2.4.4 Research Approach
2.5 Research Sources
  2.5.1 Primary Research Sources
  2.5.2 Secondary Research Sources
  2.5.3 Assumptions

3 MARKET TREND ANALYSIS

3.1 Introduction
3.2 Drivers
3.3 Restraints
3.4 Opportunities
3.5 Threats
3.6 End User Analysis
3.7 Emerging Markets
3.8 Impact of Covid-19

4 PORTERS FIVE FORCE ANALYSIS

4.1 Bargaining power of suppliers
4.2 Bargaining power of buyers
4.3 Threat of substitutes
4.4 Threat of new entrants
4.5 Competitive rivalry

5 GLOBAL AI IN CYBERSECURITY MARKET, BY COMPONENT

+357 96 030922
info@marketpublishers.com

5.1 Introduction
5.2 Solutions
5.2.1 Threat Intelligence & Analytics
5.2.2 Identity & Access Management (IAM)
5.2.3 Security Information & Event Management (SIEM)
5.2.4 Extended Detection & Response (XDR)
5.3 Services
5.3.1 Consulting & Advisory
5.3.2 Integration & Deployment
5.3.3 Managed Security Services
5.3.4 Training, Support & Maintenance

6 GLOBAL AI IN CYBERSECURITY MARKET, BY SECURITY TYPE

6.1 Introduction
6.2 Network Security
6.3 Application Security
6.4 Endpoint Security
6.5 Cloud Security
6.6 Data & Identity Security
6.7 Other Security Types

7 GLOBAL AI IN CYBERSECURITY MARKET, BY DEPLOYMENT MODE

7.1 Introduction
7.2 On-Premise
7.3 Cloud-Based

8 GLOBAL AI IN CYBERSECURITY MARKET, BY ORGANIZATION SIZE

8.1 Introduction
8.2 Small & Medium Enterprises (SMEs)
8.3 Large Enterprises

9 GLOBAL AI IN CYBERSECURITY MARKET, BY END USER

9.1 Introduction
9.2 Information Technology & Telecom

+357 96 030922
info@marketpublishers.com

9.3 Banking, Financial Services & Insurance (BFSI)
9.4 Healthcare & Life Sciences
9.5 Retail & E-commerce
9.6 Manufacturing & Industrial
9.7 Government & Public Sector
9.8 Energy & Utilities
9.9 Other End Users

10 GLOBAL AI IN CYBERSECURITY MARKET, BY GEOGRAPHY

10.1 Introduction
10.2 North America
  10.2.1 US
  10.2.2 Canada
  10.2.3 Mexico
10.3 Europe
  10.3.1 Germany
  10.3.2 UK
  10.3.3 Italy
  10.3.4 France
  10.3.5 Spain
  10.3.6 Rest of Europe
10.4 Asia Pacific
  10.4.1 Japan
  10.4.2 China
  10.4.3 India
  10.4.4 Australia
  10.4.5 New Zealand
  10.4.6 South Korea
  10.4.7 Rest of Asia Pacific
10.5 South America
  10.5.1 Argentina
  10.5.2 Brazil
  10.5.3 Chile
  10.5.4 Rest of South America
10.6 Middle East & Africa
  10.6.1 Saudi Arabia
  10.6.2 UAE
  10.6.3 Qatar

+357 96 030922
info@marketpublishers.com

10.6.4 South Africa
10.6.5 Rest of Middle East & Africa

11 KEY DEVELOPMENTS

11.1 Agreements, Partnerships, Collaborations and Joint Ventures
11.2 Acquisitions & Mergers
11.3 New Product Launch
11.4 Expansions
11.5 Other Key Strategies

12 COMPANY PROFILING

12.1 IBM Corporation
12.2 Microsoft Corporation
12.3 Amazon Web Services, Inc.
12.4 Google LLC
12.5 Cisco Systems, Inc.
12.6 Palo Alto Networks, Inc.
12.7 Fortinet, Inc.
12.8 Check Point Software Technologies Ltd.
12.9 CrowdStrike Holdings, Inc.
12.10 Darktrace Holdings Limited
12.11 FireEye, Inc. (Trellix)
12.12 Splunk Inc.
12.13 Rapid7, Inc.
12.14 SentinelOne, Inc.
12.15 Trend Micro Incorporated

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

Table 1 Global AI in Cybersecurity Market Outlook, By Region (2024-2032) ($MN)
Table 2 Global AI in Cybersecurity Market Outlook, By Component (2024-2032) ($MN)
Table 3 Global AI in Cybersecurity Market Outlook, By Solutions (2024-2032) ($MN)
Table 4 Global AI in Cybersecurity Market Outlook, By Threat Intelligence & Analytics (2024-2032) ($MN)
Table 5 Global AI in Cybersecurity Market Outlook, By Identity & Access Management (IAM) (2024-2032) ($MN)
Table 6 Global AI in Cybersecurity Market Outlook, By Security Information & Event Management (SIEM) (2024-2032) ($MN)
Table 7 Global AI in Cybersecurity Market Outlook, By Extended Detection & Response (XDR) (2024-2032) ($MN)
Table 8 Global AI in Cybersecurity Market Outlook, By Services (2024-2032) ($MN)
Table 9 Global AI in Cybersecurity Market Outlook, By Consulting & Advisory (2024-2032) ($MN)
Table 10 Global AI in Cybersecurity Market Outlook, By Integration & Deployment (2024-2032) ($MN)
Table 11 Global AI in Cybersecurity Market Outlook, By Managed Security Services (2024-2032) ($MN)
Table 12 Global AI in Cybersecurity Market Outlook, By Training, Support & Maintenance (2024-2032) ($MN)
Table 13 Global AI in Cybersecurity Market Outlook, By Security Type (2024-2032) ($MN)
Table 14 Global AI in Cybersecurity Market Outlook, By Network Security (2024-2032) ($MN)
Table 15 Global AI in Cybersecurity Market Outlook, By Application Security (2024-2032) ($MN)
Table 16 Global AI in Cybersecurity Market Outlook, By Endpoint Security (2024-2032) ($MN)
Table 17 Global AI in Cybersecurity Market Outlook, By Cloud Security (2024-2032) ($MN)
Table 18 Global AI in Cybersecurity Market Outlook, By Data & Identity Security (2024-2032) ($MN)
Table 19 Global AI in Cybersecurity Market Outlook, By Other Security Types (2024-2032) ($MN)
Table 20 Global AI in Cybersecurity Market Outlook, By Deployment Mode (2024-2032)

+357 96 030922
info@marketpublishers.com

($MN)
Table 21 Global AI in Cybersecurity Market Outlook, By On-Premise (2024-2032) ($MN)
Table 22 Global AI in Cybersecurity Market Outlook, By Cloud-Based (2024-2032) ($MN)
Table 23 Global AI in Cybersecurity Market Outlook, By Organization Size (2024-2032) ($MN)
Table 24 Global AI in Cybersecurity Market Outlook, By Small & Medium Enterprises (SMEs) (2024-2032) ($MN)
Table 25 Global AI in Cybersecurity Market Outlook, By Large Enterprises (2024-2032) ($MN)
Table 26 Global AI in Cybersecurity Market Outlook, By End User (2024-2032) ($MN)
Table 27 Global AI in Cybersecurity Market Outlook, By Information Technology & Telecom (2024-2032) ($MN)
Table 28 Global AI in Cybersecurity Market Outlook, By Banking, Financial Services & Insurance (BFSI) (2024-2032) ($MN)
Table 29 Global AI in Cybersecurity Market Outlook, By Healthcare & Life Sciences (2024-2032) ($MN)
Table 30 Global AI in Cybersecurity Market Outlook, By Retail & E-commerce (2024-2032) ($MN)
Table 31 Global AI in Cybersecurity Market Outlook, By Manufacturing & Industrial (2024-2032) ($MN)
Table 32 Global AI in Cybersecurity Market Outlook, By Government & Public Sector (2024-2032) ($MN)
Table 33 Global AI in Cybersecurity Market Outlook, By Energy & Utilities (2024-2032) ($MN)
Table 34 Global AI in Cybersecurity Market Outlook, By Other End Users (2024-2032) ($MN)
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: AI in Cybersecurity Market Forecasts to 2032 - Global Analysis By Component (Solutions and Services), Security Type, Deployment Mode, Organization Size, End User and By Geography

Product link: https://marketpublishers.com/r/A63D101F8E25EN.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/A63D101F8E25EN.html