+357 96 030922
info@marketpublishers.com

AI-Powered Cybersecurity Market Forecasts to 2032 – Global Analysis By Offering (Hardware, Software and Services), Security Type, Technology, Application, End User and By Geography

https://marketpublishers.com/r/A855E86238C6EN.html
Date: November 2025
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: A855E86238C6EN

Abstracts

According to Stratistics MRC, the Global AI-Powered Cybersecurity Market is accounted for $31.53 billion in 2025 and is expected to reach $145.39 billion by 2032 growing at a CAGR of 24.4% during the forecast period. AI-powered cybersecurity introduces an advanced approach to safeguarding digital environments through intelligent automation and predictive analytics. Leveraging machine learning models, neural networks, and pattern recognition, AI systems identify threats instantly and respond to suspicious activities before they escalate. These technologies evolve constantly, learning from historical and real-time data to uncover irregular behaviors and counter complex attacks, including malware, social engineering, and zero-day vulnerabilities. Automated security workflows improve precision and reduce manual intervention, empowering security teams to focus on critical challenges. By enabling adaptive, data-driven defense strategies, AI enhances overall cyber resilience and ensures robust, proactive protection for modern interconnected systems.

According to IDC data (commissioned by Fortinet, 2025), 94% of organizations in India are already deploying AI in cybersecurity operations to detect, respond to, and predict threats. The same survey found that 72% of organizations faced AI-powered cyberattacks in the past year, with attack volumes increasing two%- %to three-fold.

Market Dynamics:

Driver:

+357 96 030922
info@marketpublishers.com

Rising complexity of modern cyber threats

A key factor driving the AI-powered cybersecurity market is how cyber threats have become far more advanced and varied. Cybercriminals now use complex malware, shape-shifting ransomware, sophisticated phishing, and previously unknown exploits that evade older defenses. This transformation demands more intelligent protection, and AI meets that need with live threat monitoring, pattern recognition, and predictive threat forecasting. By constantly training on massive and evolving datasets, AI can forecast potential attack vectors before they emerge. Such an aggressive threat landscape compels companies to deploy AI-based security tools that evolve with attackers and offer scalable, proactive protection.

Restraint:

Rising cost burden of AI security deployment

High deployment and maintenance expenses act as a major barrier to the expansion of AI-powered cybersecurity solutions. Implementing these systems requires considerable investment in advanced hardware, cloud computing capacity, and sophisticated AI software tools. Beyond initial setup, companies must fund ongoing model training, data curation, system calibration, and experienced staff to operate and refine AI-enabled security infrastructures. For many small and mid-sized organizations, such costs are difficult to accommodate, reducing adoption rates. Integrating AI technologies into outdated networks also increases implementation challenges and financial strain. As a result, the substantial cost burden restricts broad adoption and slows overall market growth.

Opportunity:

Rise of predictive cyber risk forecasting

Predictive threat intelligence advancements represent a major opportunity within the AI-based cybersecurity market. Using AI, enterprises can examine vast, diverse datasets—ranging from threat reports to activity patterns—to detect subtle warning signs of upcoming attacks. This foresight allows security teams to address vulnerabilities early, deploy protective measures, and prevent breaches. With attackers constantly refining tactics, predictive capabilities help organizations stay ahead of evolving risks. The growing interest in anticipatory security fuels demand for AI platforms that offer predictive analytics, threat forecasting, and risk-ranking models. As proactive defense

+357 96 030922
info@marketpublishers.com

becomes crucial, vendors providing such next-generation capabilities are positioned for strong market growth.

Threat:

Dependence on reliable data pipelines

The reliance on robust, timely, and comprehensive data poses a substantial threat to AI-based cybersecurity. AI models can only perform accurately when reliable data is consistently available. If input data is limited, inconsistent, or outdated, detection capabilities weaken, increasing the likelihood of mistakes or overlooked threats. In industries with strict data-access rules, AI tools may struggle to gather enough information to operate fully. Additionally, interruptions in data flow—whether due to system failures, human error, or cyberattacks—can immediately reduce AI effectiveness. This strong dependence on data quality and continuity jeopardizes the stability and trustworthiness of AI-powered cybersecurity solutions.

Covid-19 Impact:

COVID-19 reshaped the AI-powered cybersecurity market by accelerating digital dependency and exposing new cyber risks as remote work surged worldwide. The sharp increase in ransomware, social-engineering scams, and cloud security breaches pushed organizations to adopt AI-driven defense systems capable of fast detection and automated mitigation. AI tools became essential for monitoring remote endpoints, supporting secure connectivity, and managing the heightened volume of security alerts. Although some companies initially delayed technology spending, the persistent threat environment strengthened long-term demand for intelligent, scalable cybersecurity platforms. Ultimately, the pandemic highlighted the necessity of AI in safeguarding dispersed digital infrastructures and ensuring uninterrupted, secure business operations.

The software segment is expected to be the largest during the forecast period

The software segment is expected to account for the largest market share during the forecast period because it forms the core of intelligent security automation and advanced threat analysis. AI-enhanced software solutions enable real-time monitoring, behavioral analytics, and predictive threat modeling across diverse digital environments. Their ability to integrate with enterprise systems, update rapidly, and scale effortlessly makes them indispensable to modern security frameworks. These tools evolve

+357 96 030922
info@marketpublishers.com

continuously by learning from new data, improving detection accuracy and response efficiency. With strong adaptability, remote manageability, and wide functional coverage, AI-driven software platforms deliver comprehensive protection, establishing them as the segment with the most prominent presence in the overall market.

The threat intelligence segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the threat intelligence segment is predicted to witness the highest growth rate because it enables organizations to understand evolving threats and act before attacks occur. AI-powered threat intelligence tools process vast, diverse data streams, detect unusual behaviors, and deliver actionable insights with high precision. Their predictive capabilities empower security teams to identify emerging vulnerabilities and build stronger preventive strategies. As cybercriminal tactics become more dynamic, enterprises increasingly adopt AI-based intelligence solutions to enhance situational awareness and automate complex analysis tasks. With rising demand across modern digital ecosystems—including cloud platforms and connected devices—AI-driven threat intelligence continues to expand rapidly, making it the fastest-growing segment.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, owing to its state-of-the-art digital infrastructure, broad cybersecurity awareness, and generous investment in innovation. The U.S. stands out with widespread enterprise adoption, governmental backing, and a high density of major AI and security companies. Its mature policies, regular exposure to cyber threats, and plentiful cybersecurity talent further fuel this lead. As businesses increasingly harness AI for real-time threat intelligence, cloud risk mitigation, and self-governing defenses, North America continues to set the pace in shaping global trends and driving demand across the AI-cybersecurity sector.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, powered by its extensive digitalization efforts, government-backed AI strategies, and escalating cyber threats. Major economies such as China, India, Japan, and South Korea are pushing aggressively into AI-enhanced security as they scale up cloud platforms, edge networks, and 5G/IoT infrastructure. The growing need for intelligent threat intelligence, automated responses, and predictive risk management is driving

+357 96 030922
info@marketpublishers.com

widespread regional adoption. This rapid trajectory highlights Asia-Pacific as the most dynamic and high-growth region in the global AI cybersecurity market.

Key players in the market

Some of the key players in AI-Powered Cybersecurity Market include CrowdStrike, Cybereason, SparkCognition, Tessian, Palo Alto Networks, Check Point Software Technologies, Darktrace, Fortinet, SentinelOne, Wiz, Varonis, IBM Corporation, Cisco SecureX, Microsoft Defender and Proofpoint.

Key Developments:

In September 2025, CrowdStrike and Redington announce new distribution agreement to accelerate cybersecurity transformation across India. This partnership strengthens Redington's channel reach, expands CrowdStrike's regional channel ecosystem, and enables Redington's partner base of leading resellers to drive vendor consolidation and stop breaches with cybersecurity's leading platform for the AI era.

In August 2025, SentinelOne® announced it has signed a definitive agreement to acquire Prompt Security, a pioneer in securing AI in runtime, preventing AI-related data leakage and protecting intelligent agents. The deal is part of SentinelOne's strategy to extend its AI-native Singularity™ Platform to secure the rapidly growing use of generative (GenAI) and agentic AI in the workplace.

In May 2025, Proofpoint, Inc announced it has entered into a definitive agreement to acquire Hornetsecurity Group, a leading pan-European provider of AI-powered Microsoft 365 (M365) security, data protection, compliance, and security awareness services. The acquisition significantly enhances Proofpoint's ability to provide human-centric security to small and mid-sized businesses (SMBs) globally through managed service providers (MSPs).

Offerings Covered:

- Hardware
- Software
- Services

+357 96 030922
info@marketpublishers.com

Security Types Covered:

- Network Security
- Endpoint Security
- Application Security
- Cloud Security
- Data Security

Technologies Covered:

- Machine Learning
- Deep Learning
- Natural Language Processing (NLP)
- Context-Aware Computing

Applications Covered:

- Identity & Access Management (IAM)
- Data Loss Prevention (DLP)
- Unified Threat Management (UTM)
- Risk & Compliance Management
- Threat Intelligence
- Intrusion Detection/Prevention Systems
- Fraud Detection & Anti-Fraud

+357 96 030922
info@marketpublishers.com

End Users Covered:

- BFSI
- Healthcare
- Government & Defense
- Retail & Manufacturing
- Automotive & Transportation
- IT & Telecom
- Energy & Utilities

Regions Covered:

- North America
  - US
  - Canada
  - Mexico
- Europe
  - Germany
  - UK
  - Italy
  - France

+357 96 030922
info@marketpublishers.com

- Spain
- Rest of Europe

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

+357 96 030922
info@marketpublishers.com

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 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

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

10 GLOBAL AI-POWERED CYBERSECURITY MARKET, BY GEOGRAPHY

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+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: AI-Powered Cybersecurity Market Forecasts to 2032 – Global Analysis By Offering (Hardware, Software and Services), Security Type, Technology, Application, End User and By Geography

Product link: https://marketpublishers.com/r/A855E86238C6EN.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/A855E86238C6EN.html