+357 96 030922
info@marketpublishers.com

AI-Powered Cyber Threat Intelligence Market Forecasts to 2032 – Global Analysis By Component (Solutions, and Services), Deployment Mode (On-premises, and Cloud-based), Organization Size (Small and Medium-sized Enterprises (SMEs), and Large Enterprises), Application, End User, and By Geography

https://marketpublishers.com/r/AB1FA2761A9FEN.html
Date: October 2025
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: AB1FA2761A9FEN

Abstracts

According to Stratistics MRC, the Global AI-Powered Cyber Threat Intelligence Market is accounted for $2.1 billion in 2025 and is expected to reach $7.6 billion by 2032 growing at a CAGR of 19.8% during the forecast period. AI-powered cyber threat intelligence focuses on platforms that use AI to collect, analyze, and contextualize vast amounts of data on cyber threats. It transforms raw data into actionable intelligence, predicting attack vectors and identifying novel malware. This enables proactive defense rather than reactive responses. As cyber threats grow in volume and sophistication, organizations rely on these AI-driven insights to prioritize risks, accelerate incident response, and fortify their security posture against evolving threats.

According to ENISA (EU Agency for Cybersecurity), real-time AI-powered cyber threat intelligence platforms helped decrease mean time to detection for malicious activity by 42% across critical sectors during 2024.

Market Dynamics:

Driver:

Increasing sophistication and frequency of cyber attacks

+357 96 030922
info@marketpublishers.com

The growing complexity and volume of cyber attacks are driving demand for AI-powered cyber threat intelligence solutions. Organizations face advanced persistent threats, ransomware, and phishing campaigns that traditional security tools struggle to detect in real time. AI-based platforms leverage machine learning, behavioral analytics, and threat correlation to proactively identify vulnerabilities and respond quickly. Furthermore, regulatory requirements and data protection mandates compel enterprises to adopt automated, predictive security solutions, positioning AI-powered threat intelligence as a critical investment for mitigating evolving cyber risks.

Restraint:

Shortage of skilled cybersecurity and AI professionals

Organizations often struggle to deploy, manage, and interpret AI-driven threat intelligence systems effectively, delaying adoption and reducing operational efficiency. Additionally, high recruitment costs and intensive training requirements limit smaller firms' ability to implement advanced solutions. This talent gap slows the scalability of AI-based security measures, making workforce development and partnerships with specialized service providers essential for market growth.

Opportunity:

Expansion into SME market through cloud-based solutions

Cloud-based and subscription-based models lower upfront investment barriers, providing SMEs access to advanced predictive security tools previously limited to large enterprises. Moreover, scalable solutions with automated threat detection and reporting cater to limited in-house IT teams, enabling rapid adoption. Strategic partnerships and education campaigns further enhance penetration, allowing vendors to expand their customer base while fostering long-term recurring revenue streams from a previously underrepresented segment.

Threat:

Competition from traditional security solutions

Despite advancements in AI-powered threat intelligence, traditional cybersecurity solutions such as firewalls, antivirus software, and intrusion detection systems continue

+357 96 030922
info@marketpublishers.com

to compete strongly. Many organizations rely on familiar tools due to existing contracts, perceived reliability, or lower upfront costs. Additionally, resistance to change, integration challenges, and limited awareness of AI capabilities may delay adoption. The presence of established vendors offering conventional products underscores the need for AI-based platforms to demonstrate measurable ROI, superior accuracy, and faster response times to secure market share.

Covid-19 Impact:

The Covid-19 pandemic accelerated digital transformation and remote working, increasing organizations' exposure to cyber threats. Demand for AI-powered cyber threat intelligence surged as enterprises sought real-time monitoring, automated threat detection, and incident response solutions. Supply chain vulnerabilities and increased phishing attacks highlighted the importance of predictive analytics. Furthermore, budget constraints and resource limitations during the pandemic led some organizations to prioritize scalable cloud-based AI solutions, driving accelerated adoption across industries. Overall, Covid-19 reinforced the critical role of intelligent cybersecurity tools globally.

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

The solutions segment is expected to account for the largest market share during the forecast period as they provide end-to-end capabilities, from threat identification to mitigation. Vendors offering modular and integrated platforms are preferred by enterprises seeking efficiency, cost savings, and advanced analytics. Additionally, solutions address the growing complexity of cyber threats by enabling predictive monitoring and automated response, reducing operational risk. The segment's dominance is reinforced by high adoption across industries, proven ROI, and the increasing necessity for compliance with evolving cybersecurity regulations worldwide.

The cloud-based segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the cloud-based segment is predicted to witness the highest growth rate due to lower upfront costs, ease of scalability, and rapid implementation. Cloud-based AI threat intelligence enables organizations to access advanced analytics, real-time updates, and global threat feeds without heavy on-premise infrastructure. Furthermore, subscription-based pricing reduces budget constraints, particularly for SMEs. Integration with cloud-native platforms and remote work requirements

+357 96 030922
info@marketpublishers.com

accelerates adoption, positioning the segment for the highest growth. Vendors benefit from recurring revenue and broad geographic reach through cloud delivery.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share due to a mature cybersecurity landscape, high adoption of AI technologies, and stringent regulatory compliance requirements. Enterprises invest heavily in predictive security solutions to protect critical infrastructure, data, and intellectual property. Established vendor ecosystems, strong R&D capabilities, and robust IT infrastructure further reinforce regional dominance. Additionally, increasing cyber threats, corporate awareness, and government initiatives drive large-scale deployment of AI-powered threat intelligence across industries in North America.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR due to increasing digitalization, expanding IT infrastructure, and rising awareness of cybersecurity risks. Government initiatives, growing SME adoption, and rising internet penetration encourage deployment of AI-powered solutions. Furthermore, international vendors and local startups are introducing cost-effective, cloud-based platforms tailored to regional requirements. The combination of economic growth, technology adoption, and rising cybersecurity incidents positions Asia Pacific as the fastest-growing market.

Key players in the market

Some of the key players in AI-Powered Cyber Threat Intelligence Market include Darktrace, CrowdStrike, Palo Alto Networks, Proofpoint, Vectra AI, Legit Security, Protect AI, SentinelOne, Anomali, Bitsight, Cyble, Hudson Rock, Digital Shadows, ReliaQuest, Fortinet, Safe Security, Nebulock, Dropla, Microsoft, and IBM.

Key Developments:

In September 2025, Darktrace unveiled its Cyber AI platform, which combines multiple AI models to deliver unified, intelligent, and proactive defense, transforming cybersecurity by augmenting security teams and stopping novel threats.

In September 2025, CrowdStrike introduced Threat AI, the industry's first agentic threat

+357 96 030922
info@marketpublishers.com

intelligence system. This system comprises autonomous agents designed to reason across data, hunt for threats, and act decisively to automate and accelerate complex workflows.

In September 2025, Palo Alto Networks launched Precision AI, utilizing data from cloud, endpoint, and network sources to scale and automate cyber defense, enabling real-time detection, prevention, and resolution of alerts.

In September 2025, Legit Security introduced its AI-native Application Security Posture Management (ASPM) platform, automating the discovery, prioritization, and remediation of application security issues, particularly focusing on AI-generated code and software supply chain risks.

Components Covered:

- Solutions
- Services

Deployment Modes Covered:

- On-premises
- Cloud-based

Organization Sizes Covered:

- Small and Medium-sized Enterprises (SMEs)
- Large Enterprises

Applications Covered:

- Security Analytics
- Security & Vulnerability Management

+357 96 030922
info@marketpublishers.com

- Incident Response & Forensics
- Risk & Compliance Management
- Fraud Detection
- Other Applications

End Users Covered:

- BFSI (Banking, Financial Services, and Insurance)
- IT & Telecommunications
- Government & Defense
- Healthcare & Life Sciences
- Retail & E-commerce
- Energy & Utilities
- Manufacturing
- Other End Users

Regions Covered:

- North America
  - US
  - Canada
  - Mexico

+357 96 030922
info@marketpublishers.com

- Europe
  - Germany
  - UK
  - Italy
  - France
  - 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

+357 96 030922
info@marketpublishers.com

- 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 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

+357 96 030922
info@marketpublishers.com

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 CYBER THREAT INTELLIGENCE MARKET, BY GEOGRAPHY

+357 96 030922
info@marketpublishers.com

11 KEY DEVELOPMENTS

12 COMPANY PROFILING

+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 Cyber Threat Intelligence Market Forecasts to 2032 – Global Analysis By Component (Solutions, and Services), Deployment Mode (On-premises, and Cloud-based), Organization Size (Small and Medium-sized Enterprises (SMEs), and Large Enterprises), Application, End User, and By Geography

Product link: https://marketpublishers.com/r/AB1FA2761A9FEN.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/AB1FA2761A9FEN.html