+357 96 030922
info@marketpublishers.com

AI in Cybersecurity – Threat Intelligence Market Forecasts to 2032 – Global Analysis By Component (Solutions, Services), Security Type (Network Security, Endpoint Security, Application Security, Cloud Security, Web Security and Other Security Types), Deployment Mode, Technology, Application, End User and By Geography

https://marketpublishers.com/r/A13AE72076E1EN.html
Date: July 2025
Pages: 150
Price: US$ 4,150.00 (Single User License)
ID: A13AE72076E1EN

Abstracts

According to Stratistics MRC, the Global AI in Cybersecurity – Threat Intelligence Market is accounted for $20.46 billion in 2025 and is expected to reach $92.22 billion by 2032 growing at a CAGR of 24% during the forecast period. Artificial Intelligence in Cybersecurity: Threat Intelligence is the use of AI to detect, evaluate, and neutralise online threats instantly. To identify irregularities, anticipate attacks, and automate reactions, it makes use of machine learning, natural language processing, and data analytics. AI improves situational awareness and decision-making by digesting massive volumes of threat data from various sources. By spotting trends in ransomware, phishing, and malware activity, it makes proactive defence tactics possible. This clever automation strengthens an organization's entire cybersecurity posture by greatly increasing threat detection speed, accuracy, and response time.

Market Dynamics:

Driver:

Rising sophistication of cyber-attacks

Advanced threats like as AI-driven malware and zero-day exploits necessitate quicker

+357 96 030922
info@marketpublishers.com

and more intelligent detection methods. Real-time detection of intricate attack patterns is frequently a challenge for traditional security solutions. By automating data processing and quickly identifying abnormalities, AI improves threat intelligence. It enables proactive defence by foreseeing and removing threats before damage is done. The industry is growing as a result of organisations depending more and more on AI-powered solutions to stay ahead of hackers.

Restraint:

Data privacy & regulatory risk

Access to the vast datasets required to train AI models is restricted by stringent data privacy regulations such as the CCPA and GDPR. When gathering or disseminating threat intelligence internationally, organisations frequently encounter compliance issues. These legal restrictions may hinder the uptake of AI and reduce its capacity to detect threats in real time. Investment in cutting-edge AI-driven cybersecurity tools is also deterred by regulatory uncertainty. Additionally, businesses are reluctant to fully utilise AI capabilities due to a concern of non-compliance penalties.

Opportunity:

Automation and predictive analytics

Real-time monitoring and quick analysis of massive amounts of data are made possible via automation and predictive analytics. Automated technologies simplify everyday security chores and minimise human mistake. By spotting trends and abnormalities before they become more serious, predictive analytics foresees possible hazards. Instead of only responding to breaches, this proactive strategy assists organisations in preventing them. Consequently, by lowering operating expenses and enhancing security results, these technologies propel market expansion.

Threat:

Rapid attacker evolution

Rapid attacker evolution refers to the real-time adaptability of AI models. Machine learning algorithms are less successful against novel, invisible dangers since they frequently rely on prior data. The use of AI by cybercriminals is growing, leading to increasingly complex and elusive attacks. This increases the complexity and operational

+357 96 030922
info@marketpublishers.com

expenses by necessitating frequent model upgrades and retraining. As a result, security firms have ongoing challenges in maintaining effective threat detection.

Covid-19 Impact

The COVID-19 pandemic significantly accelerated the adoption of AI in the cybersecurity – threat intelligence market. As remote work became the norm, organizations faced a surge in cyber threats and data breaches, prompting an urgent need for intelligent, automated security solutions. AI-powered threat detection systems helped companies quickly identify and respond to new and evolving cyber risks. Additionally, limited human intervention during lockdowns emphasized the value of machine learning in monitoring vast digital environments. Overall, the crisis reshaped cybersecurity strategies, positioning AI as a crucial component of defense mechanisms.

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 by enabling real-time threat detection across complex IT infrastructures. AI-powered tools analyze vast volumes of network traffic to identify anomalies and malicious patterns swiftly. This proactive approach helps organizations prevent breaches before they occur. The growing sophistication of cyberattacks has intensified the demand for AI-driven network defense solutions. As enterprises expand their digital presence, securing networks through intelligent automation becomes essential, boosting market growth.

The anomaly detection segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the anomaly detection segment is predicted to witness the highest growth rate by enabling early identification of suspicious patterns. It helps in detecting zero-day attacks and insider threats that traditional methods often miss. Real-time analysis of network traffic enhances proactive threat mitigation. AI-driven anomaly detection reduces false positives, improving incident response efficiency. Its continuous learning capability strengthens adaptive security frameworks across enterprises.

Region with largest share:

During the forecast period, the Asia Pacific region is expected to hold the largest market share due to the increasing digitization across sectors and rising cyberattacks on critical

+357 96 030922
info@marketpublishers.com

infrastructure. Countries like China, India, Japan, and South Korea are investing heavily in AI-based cybersecurity tools to protect financial services, government networks, and e-commerce platforms. This demand is further fuelled by rising cloud use and smartphone prevalence. Regional governments are also implementing stricter data protection laws, encouraging enterprises to deploy predictive threat detection and automated response systems, thereby fostering innovation in cybersecurity defense strategies.

Region with highest CAGR:

Over the forecast period, the North America region is anticipated to exhibit the highest CAGR, owing to advanced IT infrastructure and the presence of major tech companies. The U.S. leads in developing and deploying AI algorithms that identify, predict, and neutralize cyber threats in real-time. High cybercrime rates targeting banking, healthcare, and defense sectors push demand for AI-powered threat intelligence platforms. Additionally, rising investments in R&D and strategic partnerships among cybersecurity firms enhance threat detection capabilities. Strong regulatory frameworks like CISA and HIPAA further drive adoption of AI to secure digital ecosystems efficiently.

Key players in the market

Some of the key players profiled in the AI in Cybersecurity – Threat Intelligence Market include Palo Alto Networks, CrowdStrike, Fortinet, Darktrace, SentinelOne, Vectra AI, Wiz, Orca Security, Netskope, Check Point, Trellix, Tanium, Trend Micro, Splunk, Deep Instinct, Cybereason, SparkCognition and Armis.

Key Developments:

In April 2025, CrowdStrike entered a strategic partnership with Wipro to integrate its Falcon Next-Gen SIEM and threat intelligence into Wipro's cybersecurity services. This alliance aims to enhance global enterprise Security Operations Centers (SOCs) using AI-powered analytics and automation, streamlining threat detection, response workflows, and reducing operational complexity.

In March 2025, Palo Alto Networks signed a multiyear agreement with the NHL to be its Official Cybersecurity Partner. They'll deploy AI-powered next-gen firewalls, cloud and browser security to protect league operations and fan experiences across arenas ? boosting IoT threat blocking and reducing MTTR.

+357 96 030922
info@marketpublishers.com

In October 2024, Fortinet and CrowdStrike integrated Falcon’s AI-native endpoint detection with FortiGate firewalls, creating a unified AI-powered threat intelligence platform that enhances attack surface visibility, automates threat response, and streamlines detection-to-remediation across hybrid and cloud network environments.

Components Covered:

- Solutions
- Services

Security Types Covered:

- Network Security
- Endpoint Security
- Application Security
- Cloud Security
- Web Security
- Other Security Types

Deployment Modes Covered:

- Cloud-based
- On-premises

Technologies Covered:

- Machine Learning (ML)
- Natural Language Processing (NLP)

+357 96 030922
info@marketpublishers.com

- Context-Aware Computing
- Advanced Analytics
- Other Technologies

Applications Covered:

- Threat Intelligence
- Anomaly Detection
- Intrusion Detection and Prevention
- Identity and Access Management
- Risk and Compliance Management
- Other Applications

End Users Covered:

- Government and Defense
- IT and Telecom
- Healthcare
- Manufacturing
- Retail
- Energy and Utilities
- Education

+357 96 030922
info@marketpublishers.com

- Transportation and Logistics
- Other End Users

Regions Covered:

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

+357 96 030922
info@marketpublishers.com

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 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

+357 96 030922
info@marketpublishers.com

- 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

12 KEY DEVELOPMENTS

13 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: AI in Cybersecurity – Threat Intelligence Market Forecasts to 2032 – Global Analysis By Component (Solutions, Services), Security Type (Network Security, Endpoint Security, Application Security, Cloud Security, Web Security and Other Security Types), Deployment Mode, Technology, Application, End User and By Geography

Product link: https://marketpublishers.com/r/A13AE72076E1EN.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/A13AE72076E1EN.html