+357 96 030922
info@marketpublishers.com

AI in Cybersecurity – Threat Detection Systems Market Forecasts to 2032 – Global Analysis By Component (Solution, Service and Hardware), Deployment Mode (Cloud, On-Premise and Hybrid), Organization Size, Technology, End User and By Geography

https://marketpublishers.com/r/A8C2543B78A4EN.html
Date: July 2025
Pages: 150
Price: US$ 4,150.00 (Single User License)
ID: A8C2543B78A4EN

Abstracts

According to Stratistics MRC, the Global AI in Cybersecurity – Threat Detection Systems Market is accounted for $29.99 billion in 2025 and is expected to reach $123.42 billion by 2032 growing at a CAGR of 22.4% during the forecast period. Artificial Intelligence (AI) is revolutionizing cybersecurity, particularly in the area of threat detection systems. AI can examine enormous amounts of system logs and network traffic in real time by utilizing machine learning algorithms and data analytics to spot odd trends or anomalies that might point to a cyber threat. AI-driven detection tools, in contrast to conventional rule-based systems, are constantly learning from fresh data, which enhances their capacity to identify sophisticated malware, insider threats, and zero-day attacks. By automatically prioritizing alerts, these systems can lower false positives and facilitate quicker, more precise responses. Moreover, AI is becoming a crucial tool for proactive and adaptive cybersecurity defense as cyber threats become more sophisticated.

According to the European Union Agency for Cybersecurity (ENISA), there was a 30% increase in the adoption of AI-based security solutions in the past year, driven by the need for faster and more adaptive threat detection.

Market Dynamics:

+357 96 030922
info@marketpublishers.com

Driver:

Increasingly complex and advanced cyber threats

One of the main factors influencing the adoption of AI in cybersecurity is the growing frequency and complexity of cyber threats. Modern attackers use sophisticated tactics that frequently outperform conventional security tools, such as ransom ware-as-a-service, polymorphic malware, zero-day vulnerabilities, and AI-generated phishing attacks. Threat actors are now using AI to automate and customize their attacks, making them more elusive and challenging to identify. Organizations are responding by using AI-powered threat detection systems that are able to identify anomalies, analyze behavioral patterns, and adjust to changing attack tactics. Additionally, these systems greatly strengthen the defensive posture of businesses and governmental organizations alike by providing the speed and intelligence required to detect new threats in real time.

Restraint:

High operational and implementation costs

The high cost of implementation, integration, and maintenance is one of the biggest obstacles to the use of AI in threat detection systems. Significant expenditures in cutting-edge hardware infrastructure, software licenses, custom development, and cloud computing resources are frequently necessary for AI-driven cybersecurity solutions. Operational costs are further increased by the requirement for AI models to be continuously trained and updated using vast amounts of data. Small and medium-sized businesses (SMEs) may find these financial requirements to be impractical. Furthermore, decision-makers may be reluctant to make significant investments in such systems due to the lengthy ROI cycles and unclear benefits, particularly for businesses with no prior experience with AI.

Opportunity:

Combining AI, threat intelligence, and cyber risk assessment

The combination of AI with risk scoring tools and cyber threat intelligence platforms presents another new opportunity. AI systems can improve their situational awareness and identify new threats more quickly by combining real-time threat feeds from commercial databases, dark web monitoring, and open sources. This unstructured and dynamic data can be processed by machine learning models, which can then provide

+357 96 030922
info@marketpublishers.com

contextual relevance and produce useful insights. Moreover, using internal vulnerabilities and external threat landscapes, AI-based risk scoring systems assist organizations in determining the seriousness and business impact of threats. This makes it possible to prioritize resources and implement proactive cybersecurity strategies, particularly for industries like defense, healthcare, and finance.

Threat:

Insufficient interoperability and standardization

A disjointed ecosystem with a large number of proprietary tools, platforms, and protocols has resulted from the quick expansion of AI applications in cybersecurity. Organizations that depend on several vendors and technologies are seriously threatened by this lack of standardization and interoperability. Compatibility problems, uneven threat visibility, and communication breakdowns between security components can arise when various AI-based systems are integrated into a coherent cybersecurity framework. Furthermore, it is challenging to assess and contrast the efficacy of various AI solutions in the absence of standardized benchmarks. Widespread adoption may be hampered by organizations' inability to deploy AI securely and at scale in the absence of clear industry-wide standards and best practices.

Covid-19 Impact:

The COVID-19 pandemic significantly accelerated the adoption of AI in cybersecurity, particularly in threat detection systems, as organizations rapidly shifted to remote work, cloud services, and digital collaboration platforms. The demand for intelligent, automated security solutions that can monitor distributed networks and endpoints in real time has increased as a result of this abrupt digital transformation, which has increased the attack surface and revealed new vulnerabilities. The detection of phishing attempts, ransom ware attacks, and unusual behaviour that increased during the pandemic was made possible in large part by AI-powered threat detection tools. Additionally, cybersecurity remained a top priority, despite budgetary constraints affecting some IT investments. In the end, the crisis served as a catalyst for a deeper integration of AI into security operations across industries.

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

The cloud segment is expected to account for the largest market share during the forecast period. As enterprise environments become more dispersed—workloads moving

+357 96 030922
info@marketpublishers.com

across multiple clouds, remote endpoints, and hybrid configurations—cloud-native AI tools perform exceptionally well by providing automated analytics and real-time threat monitoring at scale. Because of their central management, ease of deployment, smooth updates, and quick access to new AI-driven features, cloud deployments are preferred by organizations. Furthermore, big data capabilities and advanced machine learning models are being integrated by top providers to improve detection accuracy and speed up incident response across geographically scattered assets.

The natural language processing (NLP) segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the natural language processing (NLP) segment is predicted to witness the highest growth rate. Systems can now analyze and interpret unstructured data, including emails, logs, alerts, and chat communications, to identify threats, sentiment shifts, insider risks, and compliance violations owing to the quick advancement of natural language processing (NLP) technologies. NLP improves context-aware analysis by integrating large language models and Transformer-based architectures, which can be used to automatically summarize security incidents, produce investigative insights, and even engage in conversational threat hunting. Moreover, NLP is the fastest-growing technology segment in threat detection systems, and this surge in adoption is due to its capacity to process natural-language inputs, close communication gaps between security analysts and AI systems, and scale intelligence across diverse data sources.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share. A strong digital ecosystem that makes significant investments in AI-driven cyber defense, including tech behemoths, governmental organizations, financial institutions, and operators of vital infrastructure, is the driving force behind this regional dominance. Additionally, advanced threat detection tools are also being adopted as a result of strict regulatory environments and compliance requirements. Leading North American cybersecurity companies are still at the forefront of innovation and setting the standard for AI-enhanced security solutions worldwide.

Region with highest CAGR:

Over the forecast period, the Asia-Pacific region is anticipated to exhibit the highest CAGR, driven by the quickening pace of digitalization, the expanding scope of cyber

+357 96 030922
info@marketpublishers.com

threats, and the growing use of AI technologies in industries like government, manufacturing, banking, and telecommunications. Advanced threat detection systems are being deployed more quickly as a result of significant investments made by nations like China, India, Japan, and South Korea in cloud-based security solutions, smart cities, and AI-enabled infrastructure. Furthermore, a favorable climate for rapid growth is also being produced by growing awareness of data privacy, an increase in cyberattacks on vital infrastructure, and government programs that encourage innovation in AI and cybersecurity.

Key players in the market

Some of the key players in AI in Cybersecurity – Threat Detection Systems Market include IBM Corporation, Palo Alto Networks, SentinelOne Inc, Fortinet Inc, Check Point Software Technologies (Infinity), Microsoft Corporation, Symantec (Broadcom), Vectra AI, CrowdStrike Inc, Darktrace Inc, Cisco Systems, Optiv, Cybereason Inc and UncommonX Inc.

Key Developments:

In June 2025, Palo Alto Networks is strengthening its presence across key markets in the Asia-Pacific and Japan (APJ) region through an expansion of its cloud infrastructure. This expansion of local cloud infrastructure within critical markets including Australia, India, Indonesia, Japan, and Singapore, is expected to change the way enterprises in the region secure web browsing while adhering to vital local data residency requirements.

In April 2025, IBM announced it has acquired Hakkoda Inc. Hakkoda will expand IBM Consulting's data transformation services portfolio, adding specialized data platform expertise to help clients get their data ready to fuel AI-powered business operations. Hakkoda has leading capabilities in migrating, modernizing, and monetizing data estates and is an award-winning Snowflake partner. This acquisition amplifies IBM's ability to meet the rapidly growing demand for data services and help clients build integrated enterprise data estates that are optimized for speed, cost and efficiency across multiple business use cases.

In October 2024, SentinelOne announced an extension of its strategic collaboration agreement (SCA) with Amazon Web Services (AWS), designed to deliver generative AI benefits. Under the terms of the agreement, SentinelOne’s Purple AI cybersecurity analyst will be powered by Amazon Bedrock, to provide AI-powered security and

+357 96 030922
info@marketpublishers.com

protection for customers. Additionally, the expanded SCA will increase investments in SentinelOne's AI-powered Singularity™ Platform within AWS Marketplace, empowering enterprises to quickly and easily access end-to-end protection from a unified, AI-powered platform.

Components Covered:

- Solution
- Service
- Hardware

Deployment Modes Covered:

- Cloud
- On-Premise
- Hybrid

Organization Sizes Covered:

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

Technologies Covered:

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

+357 96 030922
info@marketpublishers.com

- Computer Vision
- Behavioral Analytics
- Reinforcement Learning

End Users Covered:

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

Regions Covered:

- North America
  - US
  - Canada
  - Mexico
- Europe

+357 96 030922
info@marketpublishers.com

- 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

Middle East & Africa

+357 96 030922
info@marketpublishers.com

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

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

+357 96 030922
info@marketpublishers.com

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: AI in Cybersecurity – Threat Detection Systems Market Forecasts to 2032 – Global Analysis By Component (Solution, Service and Hardware), Deployment Mode (Cloud, On-Premise and Hybrid), Organization Size, Technology, End User and By Geography

Product link: https://marketpublishers.com/r/A8C2543B78A4EN.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/A8C2543B78A4EN.html