+357 96 030922
info@marketpublishers.com

AI-Powered Threat Intelligence Market Forecasts to 2034 – Global Analysis By Component (Solutions and Services), Security Type, Deployment Mode, Organization Size, End User and By Geography

https://marketpublishers.com/r/A74AB2C092F7EN.html
Date: June 2026
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: A74AB2C092F7EN

Abstracts

According to Stratistics MRC, the Global AI-Powered Threat Intelligence Market is accounted for $7.2 billion in 2026 and is expected to reach $30.1 billion by 2034 growing at a CAGR of 19.5% during the forecast period. AI-powered threat intelligence refers to the use of artificial intelligence and machine learning technologies to collect, analyze, and interpret cybersecurity threat data in real time. It enables organizations to identify malicious activities, detect emerging attack patterns, and predict potential security breaches with greater accuracy and speed. By automating large-scale data processing from networks, endpoints, cloud systems, and external threat feeds, AI-powered threat intelligence enhances proactive defense strategies, minimizes response times, and strengthens risk mitigation capabilities across enterprise IT infrastructures, critical industries, and digital ecosystems.

Market Dynamics:

Driver:

Ransomware and nation-state threat escalation

Dramatic escalation in ransomware attack frequency, sophistication, and financial impact combined with increasing nation-state sponsored cyber espionage and destructive attack campaigns targeting critical infrastructure, supply chains, and government networks is compelling organizations across all sectors to invest in AI-powered threat intelligence capabilities that can detect and respond to advanced

+357 96 030922
info@marketpublishers.com

persistent threats faster than human analyst teams working with traditional threat intelligence tools can manually process the volume of threat signals generated by modern enterprise security environments.

Restraint:

False positive alert fatigue burden

High false positive rates generated by AI threat detection models trained on incomplete or unrepresentative threat data create alert fatigue among security operations center analysts who must investigate and validate machine-generated threat alerts alongside genuine security incidents, paradoxically reducing the effective security value of AI threat intelligence deployments when false positive volumes overwhelm analyst capacity to process legitimate high-priority alerts. The difficulty of maintaining accurate threat detection model performance as enterprise network environments evolve, new cloud services are adopted, and legitimate user behavior patterns shift requires continuous model retraining and threshold calibration that imposes ongoing operational investment beyond initial platform deployment costs.

Opportunity:

Generative AI security operations automation

Integration of large language model capabilities into AI threat intelligence platforms is enabling natural language security incident investigation, automated threat report generation, AI-assisted malware reverse engineering, and intelligent security playbook execution that dramatically expands the analytical capacity of security operations teams without proportional headcount increases. Security operations centers deploying generative AI threat analysis capabilities report significant reductions in mean time to detect and respond to security incidents as AI systems autonomously perform initial triage, evidence collection, and contextual enrichment tasks that previously consumed analyst time before substantive investigation could begin.

Threat:

Adversarial AI evasion technique proliferation

Sophisticated threat actors, including nation-state hacking groups and advanced criminal organizations, are actively developing and deploying adversarial machine

+357 96 030922
info@marketpublishers.com

learning techniques, including generative adversarial network-powered malware mutation, polymorphic code generation, and AI-driven behavioral mimicry specifically engineered to evade AI-powered detection systems, creating an accelerating technological arms race where defensive AI capabilities must continuously evolve to counter offensive AI evasion innovation.

Covid-19 Impact:

Pandemic-driven remote work expansion dramatically increased enterprise attack surfaces through mass VPN deployment, personal device corporate access, and rapid cloud migration, creating surging cybersecurity incident volumes that overwhelmed traditional security operations capabilities and accelerated AI-powered threat detection adoption as a force multiplier for understaffed security teams. Healthcare and critical infrastructure cyber attacks exploiting pandemic disruptions demonstrated the national security consequences of inadequate threat intelligence capabilities, driving emergency government cybersecurity investment programs.

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

The services segment is expected to account for the largest market share during the forecast period, due to the strong and growing demand for managed detection and response services, combining AI-powered threat intelligence platforms with 24/7 expert security analyst coverage that provides small and medium enterprises with the security operations center capabilities they cannot build and staff internally at a viable cost. Managed security service provider subscriptions delivering AI threat intelligence, endpoint detection and response, and security information and event management as bundled managed services generate predictable high-retention recurring revenue from enterprise customers seeking comprehensive security coverage without internal security operations investment.

The network security segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the network security segment is predicted to witness the highest growth rate, driven by the expanding complexity and volume of network traffic requiring AI-powered analysis to detect sophisticated lateral movement, command-and-control communications, data exfiltration attempts, and zero-day exploit traffic that evade signature-based detection across hybrid enterprise networks spanning on-premises, multi-cloud, and operational technology environments simultaneously. AI

+357 96 030922
info@marketpublishers.com

network detection and response platforms providing behavioral analytics across encrypted network traffic are addressing the detection gap created by universal TLS encryption adoption that rendered traditional deep packet inspection less effective for threat detection without decryption overhead.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, due to the highest enterprise cybersecurity spending globally, driven by extensive regulatory compliance requirements, high cyber attack frequency targeting United States organizations, and concentration of leading AI-powered threat intelligence platform vendors, including Palo Alto Networks Inc., CrowdStrike Holdings Inc., and Darktrace plc, generating the largest aggregate commercial market revenue. United States federal government cybersecurity modernization programs under the Executive Order on Improving the Nation's Cybersecurity, mandating the deployment of advanced threat detection capabilities across civilian agency networks, represent significant public sector AI threat intelligence procurement.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, due to rapidly escalating cyber threat activity targeting Asia Pacific organizations, combined with growing enterprise cybersecurity investment driven by national cybersecurity strategy programs in Singapore, Australia, Japan, South Korea, and India, establishing mandatory security standards that are driving AI threat intelligence adoption across regulated industries. Australia's Security of Critical Infrastructure Act and Singapore's Cybersecurity Act, establishing enhanced security requirements for critical infrastructure operators, are driving mandatory threat intelligence capability procurement across telecommunications, energy, finance, and healthcare sectors.

Key players in the market

Some of the key players in AI-Powered Threat Intelligence Market include Palo Alto Networks Inc., CrowdStrike Holdings Inc., Fortinet Inc., Check Point Software Technologies Ltd., Cisco Systems Inc., IBM Corporation, Microsoft Corporation, Broadcom Inc. (Symantec), Trend Micro Incorporated, McAfee Corp., Darktrace plc, SentinelOne Inc., FireEye Inc. (Mandiant), Splunk Inc., Rapid7 Inc., Google LLC (Alphabet Inc.), Amazon Web Services Inc., and Oracle Corporation.

+357 96 030922
info@marketpublishers.com

Key Developments:

In April 2026, Microsoft Corporation announced enhanced Microsoft Sentinel AI threat intelligence integration with Security Copilot, providing automated threat actor attribution and campaign tracking for enterprise security operations teams managing hybrid cloud environments.

In March 2026, Darktrace plc expanded its Cyber AI Loop platform with proactive threat exposure management capabilities, enabling organizations to simulate adversary attack paths against their specific network topology before active exploitation occurs.

In February 2026, Palo Alto Networks Inc. released Cortex XSIAM 3.0 with autonomous AI-powered security operations center capabilities, reducing mean time to respond for critical incidents through automated investigation, containment, and remediation playbook execution.

Components Covered:

- Solutions
- Services

Security Types Covered:

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

+357 96 030922
info@marketpublishers.com

Deployment Modes Covered:

- On-Premises
- Cloud-Based
- Hybrid

Organization Sizes Covered:

- Large Enterprises
- Small & Medium Enterprises (SMEs)

End Users Covered:

- Banking, Financial Services & Insurance (BFSI)
- Government & Defense
- Healthcare & Life Sciences
- IT & Telecommunications
- Retail & E-Commerce
- Energy & Utilities
- Manufacturing
- Media & Entertainment

Regions Covered:

- North America

+357 96 030922
info@marketpublishers.com

United States

Canada

Mexico

Europe

United Kingdom

Germany

France

Italy

Spain

Netherlands

Belgium

Sweden

Switzerland

Poland

Rest of Europe

Asia Pacific

China

Japan

India

South Korea

+357 96 030922
info@marketpublishers.com

- Australia
- Indonesia
- Thailand
- Malaysia
- Singapore
- Vietnam
- Rest of Asia Pacific

South America

- Brazil
- Argentina
- Colombia
- Chile
- Peru
- Rest of South America

Rest of the World (RoW)

- Middle East
  - Saudi Arabia
  - United Arab Emirates
  - Qatar

+357 96 030922
info@marketpublishers.com

Israel

Rest of Middle East

Africa

South Africa

Egypt

Morocco

Rest of 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 2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032 and 2034
- 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)

+357 96 030922
info@marketpublishers.com

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 THREAT INTELLIGENCE MARKET, BY GEOGRAPHY

+357 96 030922
info@marketpublishers.com

11 STRATEGIC MARKET INTELLIGENCE

12 INDUSTRY DEVELOPMENTS AND STRATEGIC INITIATIVES

13 COMPANY PROFILES

+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 Rest of the World (RoW) 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 Threat Intelligence Market Forecasts to 2034 – Global Analysis By Component (Solutions and Services), Security Type, Deployment Mode, Organization Size, End User and By Geography

Product link: https://marketpublishers.com/r/A74AB2C092F7EN.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/A74AB2C092F7EN.html