EINPRESSWIRE

Artificial Intelligence in Cybersecurity Market Set to Transform Threat Detection and Risk Management

AI in cybersecurity enhances threat detection, automates defense, and empowers organizations to combat evolving digital risks.

Artificial Intelligence In Cybersecurity Market

NEWARK, DE, UNITED STATES, August 20, 2025 /EINPresswire.com/ -- The [Artificial Intelligence in Cybersecurity Market]() is on a remarkable growth trajectory, projected to surge from USD 32.0 billion in 2025 to USD 143.7 billion by 2035, registering a CAGR of 16.2%. This expansion underscores the vital role AI-driven cybersecurity solutions play in helping manufacturers and enterprises mitigate rapidly evolving digital threats.

Rising Threat Landscape Driving AI Adoption

Organizations worldwide face escalating cyber risks, ranging from ransomware and zero-day exploits to state-sponsored intrusions. For manufacturers operating in highly digitized and interconnected ecosystems, such attacks threaten both operational continuity and intellectual property.

Artificial Intelligence (AI) is transforming defensive strategies by enabling real-time threat detection, automated incident response, and predictive risk scoring. With adversaries themselves using AI to identify vulnerabilities, enterprises and government agencies are increasingly compelled to deploy intelligent, adaptive defenses.

The convergence of cloud-native environments, IoT-enabled manufacturing lines, and globally distributed supply chains has expanded attack surfaces. This makes AI-based cybersecurity not just a choice, but a strategic necessity for industrial and manufacturing firms looking to safeguard assets, ensure compliance, and maintain market trust.

Segmental Insights Highlighting Opportunities for Manufacturers

Hardware Segment (15% in 2025):
While smaller in share, hardware remains fundamental. AI accelerators, GPUs, and neural processors deliver the computational power needed for real-time anomaly detection and encryption. Manufacturers in regulated sectors such as defense, healthcare, and finance are investing in localized, hardware-based AI to meet sovereign data and compliance requirements.

Cloud Deployment (62.5% share in 2025):
Cloud-based AI platforms dominate, offering manufacturers scalable, cost-efficient, and agile security solutions. From centralized intelligence sharing to rapid deployment, cloud adoption aligns with manufacturers’ shift toward hybrid and multi-cloud operations. This model enables manufacturers to stay protected while expanding global operations and digital supply chains.

Network Security (28% share in 2025):
With IoT integration and connected production lines, network security remains the cornerstone of protection. AI-driven intrusion detection and zero-trust frameworks reduce dwell time and strengthen internal defenses. For manufacturers balancing Industry 4.0 adoption with cybersecurity, this segment provides immediate and measurable safeguards.

Historical Momentum and Future Growth

From 2020 to 2024, the market expanded at a 27.7% CAGR, fueled by surging malware attacks—averaging 419 threats per minute in Q2 2024. Remote workforce shifts compounded vulnerabilities, with 34% of organizations reporting breaches linked to telework.

Manufacturers, in particular, face unique risks with connected devices. Endpoint assaults exposed critical customer data in 68% of firms in 2020, highlighting the urgent need for decentralized and edge-based AI security solutions.

Regional Analysis: North America Leads, Asia-Pacific Rising

North America remains the nucleus of AI in cybersecurity, with 38.3% of 2024 revenue share, supported by industry leaders like IBM, Cisco, and Palo Alto Networks. Strategic government investments, such as Japan’s USD 230 million funding in 2024 for AI-driven defense, reinforce regional momentum.

The U.S. market alone is expected to generate over USD 16.1 billion in absolute dollar opportunities in the next decade, underscoring its pivotal role in shaping AI cybersecurity adoption.

Opportunities and Challenges for Manufacturers

Opportunities:

Protecting IoT-enabled smart factories, supply chains, and operational technologies.
Securing intellectual property with edge-based, decentralized AI defense systems.
Leveraging cloud-native AI tools for scalability and predictive threat management.

Challenges:

Severe global shortage of skilled cybersecurity professionals.
Growing sophistication of AI-driven attacks.
Need for continuous workforce training and cultural alignment with cybersecurity protocols.
Despite these hurdles, manufacturers stand to gain by embracing AI-powered cybersecurity as a cornerstone of digital transformation, enabling both operational resilience and competitive advantage.

Key Players Driving Market Evolution

Leading innovators include NVIDIA Corporation, IBM Corporation, Amazon Web Services, Intel Corporation, Samsung Electronics, Darktrace, Cylance, Vectra AI, and Micron Technology. These players are shaping the ecosystem through hardware innovation, AI-native platforms, and strategic acquisitions.

Notable developments include:

NVIDIA's Jetson Nano enabling AI applications with ultra-low power consumption.
Cylance's AI-native platform delivering automated forensic investigation.
BlackBerry's acquisition of Cylance, embedding AI into IoT security.
Palo Alto Networks' USD 420M acquisition of CloudGenix, bolstering secure cloud edge offerings.
Symantec's new DLP features enhancing protection against malicious applications.
Each innovation underscores the market's direction toward integrated, intelligent, and adaptive cyber defenses.

Outlook

As cybercriminals escalate their tactics, manufacturers and enterprises are aligning with AI-powered cybersecurity solutions to protect operations, customers, and reputation. With scalability across cloud and edge deployments, and proven efficacy in reducing dwell time, AI-based systems are set to define the next era of industrial cybersecurity resilience.

Request Artificial Intelligence In Cybersecurity Market Draft Report -
https://www.futuremarketinsights.com/reports/sample/rep-gb-15306

For more on their methodology and market coverage, visit https://www.futuremarketinsights.com/about-us.

Editor’s Notes

Manufacturers are urged to integrate AI-driven cybersecurity early to future-proof operations against next-gen threats.
Report highlights cover detailed segmentation by hardware, deployment type, and security applications, with regional insights for strategic decision-making.
Full market analysis, including investment trends and vendor strategies, is available in the extended report.

Rahul Singh
Future Market Insights Inc.
+1 347-918-3531
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/841473980