North America AI in Cybersecurity Market By Component (Solutions, Services), By Technology (Machine Learning, Natural Language Processing, Deep Learning, Robotic Process Automation), By Deployment Mode (On-premises, Cloud), By Application (Network Security, Endpoint Security, Application Security, Cloud Security), By End-User Industry (BFSI, Healthcare, Government, Retail, Telecommunications, Others), By Country, Competition, Forecast and Opportunities, 2019-2029F

Market Report | 2024-08-29 | 133 pages | TechSci Research

AVAILABLE LICENSES:

- Single User License $4400.00
- Multi-User License $5400.00
- Custom Research License $8400.00

Report description:

The North America AI in Cybersecurity Market was valued at USD 7.47 Billion in 2023 and is expected to reach USD 25.71 Billion by 2029 with a CAGR of 22.69% during the forecast period.
The North America AI in cybersecurity market is experiencing rapid growth, driven by escalating cyber threats and the increasing complexity of digital infrastructures. This dynamic market is characterized by the integration of artificial intelligence (AI) technologies to enhance traditional cybersecurity measures and address sophisticated cyber threats. AI's capability to analyze vast amounts of data in real time, recognize patterns, and predict potential vulnerabilities has revolutionized the cybersecurity landscape, making it a critical component for organizations across various sectors. One of the primary drivers of the market's expansion is the rising frequency and sophistication of cyberattacks. As cybercriminals employ more advanced tactics, including ransomware, phishing, and zero-day exploits, organizations are turning to AI to bolster their defenses. AI-driven cybersecurity solutions offer advanced threat detection, automated response, and predictive analytics, enabling organizations to stay ahead of emerging threats and mitigate risks more effectively. The growing complexity of IT environments, including the proliferation of

cloud computing, Internet of Things (IoT) devices, and remote work models, further fuels the demand for AI in cybersecurity. Traditional security measures often struggle to keep pace with the volume and variety of data generated in these environments. AI enhances the capability to monitor and analyze this data, providing real-time insights and actionable intelligence to safeguard against potential breaches.

Additionally, regulatory and compliance requirements are pushing organizations to adopt advanced security solutions. Increasingly stringent regulations regarding data protection and privacy, such as the GDPR and CCPA, necessitate robust cybersecurity measures to ensure compliance and avoid costly penalties. AI-driven solutions help organizations meet these requirements by providing detailed audit trails, real-time monitoring, and advanced threat detection capabilities. The North American market is also supported by a strong technology ecosystem, including leading cybersecurity firms and innovation hubs. The United States and Canada are home to numerous technology companies that are at the forefront of developing AI-powered security solutions, contributing to the market's growth and evolution.

Key Market Drivers

Increasing Frequency and Sophistication of Cyberattacks

The North America AI in cybersecurity market is significantly driven by the escalating frequency and sophistication of cyberattacks. Cyber threats are becoming increasingly advanced, with attackers employing complex techniques such as ransomware, advanced persistent threats (APTs), and zero-day exploits. Traditional security measures often struggle to keep up with these evolving threats, leading organizations to seek more advanced solutions. AI enhances cybersecurity by providing real-time threat detection and response capabilities, utilizing machine learning algorithms to identify unusual patterns and behaviors indicative of potential attacks. AI systems can analyze vast amounts of data at high speeds, allowing for the rapid identification and neutralization of threats before they cause significant damage. This capability is essential for mitigating the risks posed by modern cyber threats and ensuring robust protection for sensitive data and critical infrastructure. As the threat landscape continues to evolve, the demand for AI-driven cybersecurity solutions is expected to grow, driving market expansion.

Complexity of IT Environments

The increasing complexity of IT environments is another major driver of the North America AI in cybersecurity market. The rapid adoption of cloud computing, IoT devices, and remote work arrangements has expanded the attack surface for cyber threats. Traditional security solutions often struggle to manage and protect these diverse and dynamic environments effectively. AI-driven cybersecurity solutions offer enhanced capabilities for monitoring, analyzing, and securing complex IT infrastructures. AI technologies can handle large volumes of data, integrate with various systems, and provide a unified view of an organization's security posture. By leveraging AI, organizations can gain deeper insights into their security environments, detect anomalies across disparate systems, and respond more effectively to potential threats. The ability of AI to adapt to evolving IT landscapes and provide comprehensive protection drives its adoption in the market.

Regulatory and Compliance Requirements

Regulatory and compliance requirements are a significant driver for the North America AI in cybersecurity market. As data protection and privacy regulations become more stringent, organizations are required to implement robust security measures to avoid penalties and maintain compliance. Regulations such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and various industry-specific standards mandate comprehensive security practices to safeguard sensitive information. AI-driven cybersecurity solutions help organizations meet these regulatory requirements by providing advanced threat detection, real-time monitoring, and detailed audit trails. AI technologies enable organizations to ensure compliance with data protection laws, manage security risks effectively, and demonstrate adherence to regulatory standards. The increasing emphasis on compliance and the need to protect customer data drive the adoption of AI-powered security solutions in the market.

Digital Transformation and Adoption of Cloud Technologies

Digital transformation and the widespread adoption of cloud technologies are key drivers of the North America AI in cybersecurity market. Organizations are increasingly moving their operations to cloud environments to leverage the benefits of scalability, flexibility, and cost-efficiency. However, this shift also introduces new security challenges, including the need to protect cloud-based data and applications from cyber threats. AI-driven cybersecurity solutions offer advanced capabilities to secure cloud environments by providing real-time threat detection, automated response, and visibility across hybrid and multi-cloud

infrastructures. AI technologies can analyze cloud traffic, detect anomalies, and ensure the security of cloud-based assets. As more organizations embrace digital transformation and cloud computing, the demand for AI-powered cybersecurity solutions that can address the unique challenges of cloud security is expected to grow.

Key Market Challenges

High Implementation Costs

One of the primary challenges facing the North America AI in cybersecurity market is the high cost of implementing AI-driven solutions. Advanced AI technologies require substantial investment in both hardware and software, as well as ongoing maintenance and updates. For many organizations, particularly small and medium-sized enterprises (SMEs), the initial financial outlay for AI systems can be prohibitive. This includes costs associated with acquiring sophisticated AI tools, integrating them with existing systems, and training staff to effectively use these technologies. The substantial capital required can deter businesses from adopting AI solutions, impacting overall market growth. Additionally, the need for specialized skills to manage and optimize AI systems further adds to the expense, making it a significant barrier to widespread adoption.

Complex Integration with Existing Systems

Integrating AI-driven cybersecurity solutions with existing IT infrastructures presents another challenge. Many organizations operate with a mix of legacy systems and newer technologies, creating a complex environment for integrating advanced AI tools. The process of ensuring compatibility and seamless operation between new AI systems and older security frameworks can be both technically and operationally demanding. This complexity often requires substantial customization and additional resources, leading to longer deployment times and potential disruptions in security coverage. Organizations may face difficulties in achieving a unified security posture, which can impact the effectiveness of the AI solutions and hinder their overall return on investment.

Data Privacy and Security Concerns

The deployment of AI in cybersecurity involves handling large volumes of sensitive data, raising significant privacy and security concerns. AI systems often require access to extensive datasets to function effectively, including potentially sensitive information. This creates risks related to data breaches, misuse, and unauthorized access. Organizations must ensure that their AI solutions adhere to stringent data protection regulations and standards to avoid legal repercussions and maintain user trust. Balancing the need for comprehensive data access with robust privacy protections is a complex challenge that can impact the deployment and adoption of AI-driven security solutions.

Skill Shortages and Expertise

A shortage of skilled professionals with expertise in both AI and cybersecurity is a notable challenge for the market. The integration and management of AI technologies in cybersecurity require specialized knowledge that is in high demand but short supply. This skills gap can impede the effective implementation and optimization of AI solutions, leading to suboptimal performance and increased vulnerability. Organizations may struggle to recruit and retain qualified personnel, which can affect their ability to leverage AI technologies fully. The scarcity of skilled professionals also drives up the cost of talent, further exacerbating the challenges associated with AI adoption in cybersecurity.

Evolving Threat Landscape

The constantly evolving nature of cyber threats presents a significant challenge for AI-driven cybersecurity solutions. While AI can enhance threat detection and response, it is not immune to the dynamic and adaptive tactics employed by cybercriminals. Threat actors continuously develop new methods to bypass security measures, requiring AI systems to be regularly updated and refined to remain effective. The rapid pace of innovation in cyber threats means that AI solutions must continuously evolve to address emerging vulnerabilities and attack vectors. This ongoing need for adaptation can strain resources and complicate the management of AI systems, affecting their overall effectiveness and reliability in combating new and sophisticated threats.

Key Market Trends

Increased Adoption of AI-Driven Threat Detection and Response

One of the most significant trends in the North American AI in cybersecurity market is the widespread adoption of AI-driven threat detection and response solutions. As cyber threats become more sophisticated and frequent, traditional security measures often fall short. AI technologies, including machine learning and deep learning, offer advanced capabilities for identifying and mitigating these threats. These AI systems analyze vast amounts of data to detect unusual patterns, behaviors, and anomalies that may indicate a security breach. Real-time threat detection allows organizations to respond swiftly to potential attacks, minimizing

damage and reducing response times. The use of AI in automating threat responses also helps alleviate the burden on cybersecurity teams, enabling more efficient and effective management of security incidents.

Growth of AI-Powered Endpoint Security Solutions

AI-powered endpoint security solutions are experiencing significant growth in the North American market. With the increasing number of endpoints, such as laptops, mobile devices, and IoT devices, securing these endpoints has become a critical concern for organizations. AI enhances endpoint security by providing advanced protection against malware, ransomware, and other threats. AI-driven solutions offer capabilities like behavioral analysis, real-time threat detection, and automated responses to mitigate risks. The rise in remote work and the expansion of the digital workforce have further accelerated the demand for robust endpoint security solutions that can provide continuous monitoring and protection against evolving cyber threats.

Integration of AI with Cloud Security

The integration of AI with cloud security is a prominent trend in the North American market. As organizations increasingly adopt cloud services for their data storage and computing needs, ensuring the security of cloud environments has become essential. AI technologies are being leveraged to enhance cloud security by providing advanced threat detection, automated compliance monitoring, and data protection. AI systems can analyze large volumes of cloud data to identify potential vulnerabilities, detect suspicious activities, and ensure adherence to regulatory requirements. The ability of AI to scale with cloud environments and offer real-time insights makes it a valuable tool for protecting cloud-based assets and applications.

Segmental Insights

Technology Insights

Machine Learning segment dominates in the North America AI in Cybersecurity market in 2023 due to its advanced capabilities and effectiveness in addressing modern cyber threats. Several factors contribute to this dominance, reflecting the growing reliance on ML to enhance cybersecurity measures. ML's ability to process and analyze vast amounts of data in real-time is a significant advantage. Cybersecurity environments generate enormous volumes of data from network traffic, user behaviors, and system activities. ML algorithms excel at sifting through this data to identify patterns, anomalies, and potential threats that would be challenging for traditional security systems to detect. By continuously learning from new data and adapting to evolving threat landscapes, ML systems offer dynamic and responsive threat detection capabilities, making them highly effective in preventing cyberattacks. ML enhances threat detection through advanced pattern recognition. Unlike rule-based systems that rely on predefined signatures or patterns, ML algorithms can identify previously unknown threats by recognizing deviations from normal behavior. This capability is crucial for detecting sophisticated and novel attacks, such as zero-day exploits and advanced persistent threats, which traditional methods might miss. As cybercriminals employ more complex techniques, the ability of ML to adapt and learn in real-time provides a significant edge in maintaining security.

ML contributes to the automation of cybersecurity processes. By automating tasks such as incident response, threat intelligence, and vulnerability management, ML reduces the burden on human security teams. This automation not only enhances efficiency but also ensures faster and more accurate responses to security incidents, minimizing potential damage and reducing operational costs. Furthermore, the increasing complexity of IT environments, including the proliferation of IoT devices and cloud computing, drives the demand for ML solutions. ML□s scalability and adaptability make it well-suited to handle the diverse and dynamic nature of modern digital infrastructures.

Country Insights

United States dominated the North America AI in Cybersecurity market in 2023. The U.S. benefits from a robust technology ecosystem that fosters innovation in AI and cybersecurity. The country is home to numerous technology hubs and research institutions that drive advancements in AI technologies. Leading tech companies and startups based in Silicon Valley, Boston, and other major tech centers are at the forefront of developing cutting-edge AI solutions for cybersecurity. This innovation ecosystem fuels the growth of AI-driven cybersecurity tools and services, contributing to the U.S.'s market dominance.

The high level of cyber threats and attacks in the U.S. has spurred significant investment in advanced cybersecurity solutions. With the rise of sophisticated cyber threats targeting critical infrastructure, financial institutions, and government agencies, there is a strong demand for AI-powered security solutions that can provide advanced threat detection, real-time response, and predictive analytics. The urgency to protect sensitive data and maintain regulatory compliance drives the adoption of AI technologies in the cybersecurity sector. The U.S. has a favorable regulatory environment and substantial government support for

cybersecurity initiatives. Federal agencies, such as the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST), provide guidelines, funding, and research to advance cybersecurity practices. The federal government's emphasis on improving national security and the protection of critical infrastructure encourages organizations to invest in AI-driven cybersecurity solutions.

U.S. market benefits from a high level of technological adoption across various industries. Sectors such as finance, healthcare, and technology, which are prominent in the U.S., are early adopters of AI technologies. The need to safeguard digital assets and comply with stringent regulations drives the integration of AI into cybersecurity strategies within these sectors. The U.S. market is characterized by a high level of investment in cybersecurity research and development. Venture capital funding and corporate investments support the growth of innovative AI cybersecurity solutions, further solidifying the U.S.'s leading position in the market.

Key Market Players

- Darktrace Holdings Limited
- CrowdStrike, Inc.
- Palo Alto Networks, Inc.
- FireEye, Inc.
- Splunk Inc.
- IBM Corporation
- McAfee, LLC
- Cisco Systems, Inc.
- Fortinet, Inc.
- Check Point Software Technologies Ltd.
- Trend Micro Incorporated
- Sumo Logic, Inc.

Report Scope:

In this report, the North America AI in Cybersecurity Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

- North America AI in Cybersecurity Market, By Component:
  - Solutions
  - Services
- North America AI in Cybersecurity Market, By Technology:
  - Machine Learning
  - Natural Language Processing
  - Deep Learning
  - Robotic Process Automation
- North America AI in Cybersecurity Market, By Deployment Mode:
  - On-premises
  - Cloud
- North America AI in Cybersecurity Market, By Application:
  - Network Security
  - Endpoint Security
  - Application Security
  - Cloud Security
- North America AI in Cybersecurity Market, By End-User Industry:
  - BFSI
  - Healthcare
  - Government

- Retail
- Telecommunications
- Others

North America AI in Cybersecurity Market, By Country:

- United States
- Canada
- Mexico

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the North America AI in Cybersecurity Market.

Available Customizations:

North America AI in Cybersecurity Market report with the given market data, TechSci Research offers customizations according to a company's specific needs. The following customization options are available for the report:

Company Information

Detailed analysis and profiling of additional market players (up to five).

Table of Contents:

North America AI in Cybersecurity Market By Component (Solutions, Services), By Technology (Machine Learning, Natural Language Processing, Deep Learning, Robotic Process Automation), By Deployment Mode (On-premises, Cloud), By Application (Network Security, Endpoint Security, Application Security, Cloud Security), By End-User Industry (BFSI, Healthcare, Government, Retail, Telecommunications, Others), By Country, Competition, Forecast and Opportunities, 2019-2029F

Market Report | 2024-08-29 | 133 pages | TechSci Research

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4400.00
	Multi-User License	$5400.00
	Custom Research License	$8400.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email* Phone*

First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-02-08
		Signature	