AI In Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The AI In Security Market size is estimated at USD 25.22 billion in 2024, and is expected to reach USD 60.24 billion by 2029, growing at a CAGR of 19.02% during the forecast period (2024-2029).

Key Highlights
-With the rise in connected enterprises, devices, and applications, businesses are becoming more vulnerable as they are connected to a mass of independent endpoints. Therefore, AI in security provides an enticing proposition with its proactive threat mitigation capabilities, which are needed for constant supervision and adaptation to the multifaceted security vulnerabilities faced by the modern digitalized economy.
-AI and its applications allow users to protect any system by providing alerts to them in real-time to mitigate risk. The data available within the organizations are being used to train these systems. In February of the current year, DOD stood up the new position of the Office of the Chief Digital and AI Officer to serve as the department's senior official responsible for strengthening and integrating data, AI, and digital solutions and replacing the JAIC (Joint Artificial Intelligence Center) established in 2018.
-Implementing machine learning with AI enables threats and malware to be proactively prevented rather than only detected. This is expected to help create a huge market opportunity for artificial intelligence in the security market during the forecast period. In May 2022, the US Senate Armed Forces Committee's Subcommittee on Cyber held a congressional hearing on the importance of leveraging artificial intelligence and machine learning within cyberspace. This hearing included representatives from Google and the Center for Security and Emerging Technology at Georgetown University.
-The need for more skilled AI professionals and lack of awareness are expected to restrain the market during the forecast period. According to a report by IBM Security, artificial intelligence (AI), when fully deployed, provided the most significant cost mitigation, up to USD 3.05 million less at organizations with AI than organizations without AI. Data breach average cost increased by 2.6% from USD 4.24 million in the last year to USD 4.35 million in the current year.

Cloud segment is expected to grow at a higher pace

Antivirus/Anti-malware Offers Potential Growth

- Artificial intelligence and machine learning techniques are needed to counter-attack malicious software, with the malware getting more intelligent daily. Both antivirus and anti-malware fall under the broader term of cybersecurity. Cybersecurity is increasingly becoming a headache for everyone, from corporate executives to regular consumers, who are targeted by phishing scams and hackers attempting to access sensitive information.
- Modern cyber attackers' tactics, techniques, and procedures have become both rapid and abundant, while advanced threats such as ransomware, phishing, and software supply chain attacks are explosive. Further, to stand up to these challenges, businesses are developing, maintaining, and constantly updating their cybersecurity strategies and solutions. For instance, in August 2022, Prosegur Security, a leader in security technology, and Everseen, the leader in visual AI, partnered to reimagine physical security in retail and other industries using human-centric artificial intelligence solutions. The partnership will enhance security processes through a shared focus on innovation.
- According to the Consumer Technology Association, 44% of organizations across the globe are implementing AI applications to detect and deter security intrusions. Artificial intelligence in cybersecurity increases the efficiency and precision of the system to observe any potential threat in the organization's strategy. According to the Australian Signals Directorate, Andrew Hastie, assistant minister for defense, the Australian government is expected to spend USD 6.8 billion over the coming decade on measures to enhance the offensive and defensive cyber and intelligence capabilities of the Australian Signals Directorate (ASD).
- The gradual shift of enterprises toward adopting the internet to perform most tasks is compelling employees to remain online for a longer time and create a lot of data, thus increasing the risks for cyber-attacks and hacking. Thus with machine learning and AI, that peak of data could be carved down in a fraction of the time, helping the enterprise to identify and recover from the security threat.

Asia-Pacific to Witness the Highest Growth

- In Asia-pacific, great strides are being made in the digital economy. But it is also causing more threat-related opportunities. According to Cisco, companies receive six threats every minute in APAC, and 51% of all cyber-attacks result in a loss of more than USD 1 million.
- The growing penetration of the internet and the shift toward digitization of internal processes have been instrumental in driving the adoption of cloud-based services. Alongside the digital transformation in the region, owing to ineffective cyber laws and lack of cybersecurity awareness, companies in Asia-Pacific are 80% more likely to be targeted by hackers than in other regions. In July this year, Korea FSC (Financial Services Committee) and FSS (Financial Supervisory Service) announced AI Guidelines in Financial Services, which guide the industry on the responsibility, accuracy, safety, transparency, fairness, and consumer rights relating to AI security systems.
- Moreover, many countries have passed regulations and created independent programs to create a "single source of truth" and provide banks and retailers with verified digital customer identities. Malaysia's MyKad, Singapore's MyInfo, and Thailand's Digital ID are all designed to facilitate and speed up identity verification. This creates a huge scope for AI in the security market.
- All the above factors are expected to support the growth of artificial intelligence in the security market in this region during the forecast period. For instance, in February this year, IBM announced a multi-million dollar investment in its resources to help businesses prepare for and manage the growing threat of cyberattacks to organizations across the APAC region. The acquisition also includes a new Security Operation Center (SOC), part of IBM's vast network of existing global SOCs providing 24X7 security

response services to clients around the region.

Artificial Intelligence (AI) in Security Industry Overview

Artificial intelligence in the security market is highly competitive and fragmented as many new companies are developing innovative technologies due to the rise in cyber attacks over the years. Artificial intelligence (AI) is a rapidly growing field of technology that is capturing the attention of commercial investors, defense intellectuals, policymakers, and international competitors. This is making this market more competitive. A few players are IBM Corporation, Cisco Systems Inc., etc.

- In November 2023, Palo Alto Networks Inc. announced the addition of fresh features that are artificial intelligence-related to security. The features are added to its Cortex security automation and intelligence product line. The addition is made following the automation trend in finding and eliminating threats and exploits.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

AI In Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

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	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	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	2026-02-26
		Signature