AI In Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 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 30.02 billion in 2025, and is expected to reach USD 71.69 billion by 2030, at a CAGR of 19.02% during the forecast period (2025-2030).

Artificial intelligence plays a crucial role in the security market by enhancing threat detection, automating responses to cyberattacks, analyzing vast amounts of data for anomalies, and improving overall cybersecurity posture. AI-powered systems can identify patterns indicative of malicious activities, adapt to evolving threats, and provide real-time insights to security professionals, helping them stay ahead of potential breaches.

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.
- Atos and Ooredoo partnered to provide key cybersecurity threat detection and response services to Qatar Smart Program "TASMU," which is a smart city program in the country driven by the Ministry of Transport and Communication (MOTC). It also supports Qatar National Vision 2030. Atos and Ooredoo's solution integrates cloud-native, intelligent security analytics and AI capability from the Atos Alsaac platform to secure TASMU's infrastructure and applications.
- The number of cyberattacks is steadily increasing on a global scale. Cybercriminals attack endpoints, networks, data, and other IT resources. Infrastructure is costly for citizens, companies, and governments. Cybercriminals' primary motivations are political rivalry, monetary gain, reputational harm, global competitiveness, and the interest of radical religious organizations. The majority of cyberattacks try to make money. WannaCry, Petya, NotPetya, and BadRabbit are significant ransomware that have severely

harmed businesses and government organizations.
- Implementing machine learning with AI enables threats and malware to be proactively prevented rather than only detected. This is expected to help create a vast market opportunity for artificial intelligence in the security market during the forecast period.
- About 97% of Indian organizations have begun investing in AI/ML, while 84% are investing in infrastructure around cloud technology, according to the Data Security Council of India. The intersection of AI with cybersecurity is poised to drive a significant increase in investments in the sector. Also, the nation expects a few investment opportunities in AI and cyber security governance areas. Dallas Venture Capital (DVC) claimed that AI technologies, such as machine learning (ML) and behavioral analytics, are game changers in cybersecurity.
- The rising frequency and sophistication of cyber threats have made traditional security measures insufficient. AI offers advanced capabilities to detect and respond to evolving threats in real time. For instance, South Korea's ICT ministry spent KRW 670 billion (USD 607 million) in 2023 to bolster the country's cybersecurity capabilities to respond to growing new digital threats. The government plans to develop infrastructure to quickly respond to cybersecurity threats by collaborating with central cloud and data center companies to collect threat information in real time, compared to the current system that relies on individual reports.
- The need for more skilled AI professionals and the 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. The average cost of a data breach increased by 2.6% from USD 4.24 million in 2021 to USD 4.35 million in 2022.
- The Russia-Ukraine war significantly impacted the AI security market. Increased tensions led to heightened cybersecurity concerns, prompting governments and businesses to invest more in AI-driven security solutions to protect against cyber threats, including espionage and hacking attacks. Additionally, geopolitical instability could disrupt supply chains for AI hardware and software components, affecting the availability and pricing of AI security products.

AI In Security Market Trends

The Healthcare Sector is Significantly Driving Market Growth

- AI significantly strengthens healthcare security by providing advanced threat detection, data protection, fraud detection, privacy preservation, and predictive analytics capabilities. By leveraging AI-driven security solutions, healthcare organizations can better safeguard patient data, ensure compliance with regulatory requirements, and mitigate the risks posed by cybersecurity threats.
- The increasing adoption of medical and Internet of Things (IoT) devices in healthcare settings introduces new security challenges. AI can enhance the security of these instruments by monitoring device behavior, detecting anomalies, and identifying potential security vulnerabilities or breaches.
- In March 2024, Microsoft made the promise of AI real by empowering the industry to tackle its most significant challenges and create a real difference in the lives of clinicians and patients. At the 2024 HIMSS Global Health Conference & Exhibition, the company highlighted how providers are adopting generative AI solutions and the impact the technology is making.
- Healthcare organizations require real-time threat detection capabilities to respond swiftly to cyber threats and prevent data breaches. AI-powered security solutions can analyze streaming data from various sources, such as network traffic, medical devices, and user activities, to detect and respond to real-time security incidents, minimizing the impact of potential breaches. Also, the proliferation of electronic health records (EHRs), medical imaging data, wearable device data, and other healthcare data sources has generated vast amounts of data that need to be protected. AI-based security solutions analyze large volumes of healthcare data in real time to detect anomalies and identify potential security threats more effectively than traditional methods.
- Various hospitals use this technology to deliver more accurate diagnoses and treatment plans. For instance, in March 2024, Microsoft announced a unique initiative to provide the responsible development of AI in healthcare at the HIMSS Global Health Conference & Exhibition. The tech giant is teaming up with more than a dozen of America's most prominent hospitals to form the Trustworthy & Responsible AI Network, also dubbed TRAIN.

- In December 2023, AJ Hospital and Research Centre started using 50 beds in the hospital's private ward new Dozee Artificial Intelligence-based Continuous Remote Patient Monitoring and Early Warning System, which helps the hospital continuously monitor the vital parameters of patients after they moved out of the intensive care unit. Such activities are expected to drive the market demand.

Asia-Pacific is Expected to Witness Significant Growth

- In the Asia-Pacific region, 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.
- With increasing security threats such as cyberattacks, terrorism, and geopolitical tensions across the region, the demand for advanced security solutions powered by AI is growing to detect, prevent, and respond to emerging threats. According to MeitY (India) (CERT-In), more than 1.3 million cyber attacks were reported across India. The country was among the top five with the most cyber security incidents in the same year. India ranks third in terms of internet user numbers.
- 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. 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.
- 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 2024, to help clients counter cyber threats with earlier and more accurate detection, IBM announced new AI-enhanced versions of the IBM FlashCore Module technology available inside new IBM Storage FlashSystem products and a new version of the IBM Storage Defender software to help organizations improve their ability to detect and respond to ransomware and other cyberattacks that threaten their data.

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 of the market players include IBM Corporation and Cisco Systems Inc.

- November 2023: Commvault announced its all-inclusive Commvault Cloud software infrastructure and established numerous security supplier arrangements to offer comprehensive cyber security, resilience, and data intelligence proficiencies. The company believes in setting up partnerships with cyber security, artificial intelligence (AI), and cloud suppliers to offer joint customers more choices to protect, detect, and answer possible threats and attacks while enlightening data visibility and ascendency.
- November 2023: Rubrik, a US-based company working in the data security sector, launched Ruby. It is a generative AI extension

designed for Rubrik Security Cloud as well, and it is projected to speed up cyber hazard detection retrieval and resilience.

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 (2025 - 2030)

Market Report | 2025-04-28 | 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	2026-02-25
		Signature