# Significant growth projected for AI vulnerability scanning market



The global market for AI vulnerability scanning is projected to experience significant growth, expected to rise from USD 2.41 billion in 2024 to around USD 9.09 billion by the year 2034. This growth translates to a compound annual growth rate (CAGR) of 14.20% during the period from 2025 to 2034. The AI vulnerability scanning market encompasses tools and services aimed at identifying, assessing, and mitigating security vulnerabilities present in AI models and systems, which have become increasingly essential as artificial intelligence technology pervades various industries.

North America currently stands as the dominant player in this market, holding over 36% of the total share and generating an estimated USD 0.86 billion in revenue in 2024. Within this, the United States alone accounts for approximately USD 0.80 billion and is exhibiting substantial growth, showcasing a CAGR of 12.8%. The trends indicate a heightened focus on robust security measures as AI continues to integrate into mission-critical applications, notably in sectors such as healthcare, finance, and autonomous vehicles.

The increasing sophistication of cyber threats targeting AI systems is cited as a key driving factor for the growth of this market. Cybercriminals are rapidly adapting their strategies to exploit vulnerabilities inherent in machine learning models, deep learning algorithms, and neural networks. Consequently, the need for advanced vulnerability scanning tools capable of identifying and addressing these risks has surged.

The primary segments of the AI vulnerability scanning market highlight that software solutions command a substantial 67% of market share, attributing their dominance to their capability to provide comprehensive security measures against various vulnerabilities. Furthermore, cloud-based deployment models account for over 55% of the market, as businesses increasingly favour scalable, flexible, and cost-effective solutions.

Large enterprises emerge as the leading user segment, comprising 62% of the market share, primarily due to their higher adoption of advanced AI technologies which necessitate robust security measures. The IT and Telecom sector represents a significant portion as well, capturing over 30% of the total share. Given these sectors' reliance on AI for optimising operations, enhancing cybersecurity, and managing sensitive data, the demand for effective AI vulnerability scanning solutions is particularly pronounced.

The market is experiencing notable opportunities for innovation, particularly in automated vulnerability detection, real-time monitoring, and security tools driven by AI. Partnerships between cybersecurity firms and AI technology providers are expected to enhance the development of solutions that successfully address existing security gaps in AI systems. Trends indicate a shift towards continuous vulnerability assessment, allowing companies to promptly address emerging threats rather than relying on periodic checks.

Despite the promising outlook, the market faces challenges such as the high costs associated with advanced AI vulnerability scanning solutions, which may deter small and medium-sized enterprises from investing in necessary cybersecurity infrastructure. Furthermore, there is a notable absence of standardised protocols for AI security, complicating the establishment of uniform security practices across different systems.

Recent developments within the sector illustrate an active push towards enhancing security capabilities. CRYPTTECH has unveiled an AI-driven vulnerability scanning engine aimed at detecting both known and unknown vulnerabilities across systems. Meanwhile, SecPoint has expanded its offerings with the introduction of tools specifically tailored for cloud vulnerability assessment.

As the landscape for AI technologies continues to evolve, the demand for specialised vulnerability scanning solutions is anticipated to grow substantially, reinforcing the necessity for innovative and proactive cybersecurity strategies across various industries.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.prnewswire.com/news-releases/ai-vulnerability-scanning-market-size-to-grow-usd-7-574-30-million-by-2030-at-a-cagr-of-13-52--valuates-reports-302180469.html> - This URL supports the claim that the AI vulnerability scanning market is experiencing significant growth due to increasing cybersecurity threats and the integration of AI across various sectors.
* <https://www.prnewswire.com/news-releases/ai-vulnerability-scanning-market-size-to-grow-usd-7-574-30-million-by-2030-at-a-cagr-of-13-52--valuates-reports-302180469.html> - It also highlights the dominance of North America in the AI vulnerability scanning market and the importance of cloud-based solutions for large enterprises.
* <https://reports.valuates.com/market-reports/QYRE-Auto-12L15782/global-ai-vulnerability-scanning> - This report lists major players in the AI vulnerability scanning market, such as CRYPTTECH and SecPoint, which are innovating in AI-driven vulnerability scanning solutions.
* <https://www.futuremarketinsights.com/reports/security-and-vulnerability-management-market> - This URL supports the trend of increasing investments in AI-enabled security solutions and the growth of the security and vulnerability management market, driven by rising cyber threats.
* <https://www.futuremarketinsights.com/reports/security-and-vulnerability-management-market> - It also highlights the importance of strict government regulations and the integration of AI and ML in enhancing security measures across industries like BFSI and healthcare.