# CyberArk partners with Accenture to enhance identity security for AI agents



CyberArk has announced a collaboration with Accenture aimed at tackling the increasing identity security challenges associated with artificial intelligence (AI) agents in enterprise settings. The partnership, revealed on 14 April, intends to combine CyberArk’s Identity Security Platform with Accenture's AI Refinery to assist organisations in implementing Zero Trust-based identity access controls tailored for AI systems.

As organisations begin to adopt agentic AI architectures at scale, the need for stringent identity and access management measures has become more pronounced. AI agents, which are becoming increasingly autonomous and integrated into vital business systems, present new risks, particularly concerning privileged access to these systems.

Matt Cohen, CEO of CyberArk, highlighted the importance of robust security measures, stating, "AI agents have the potential to gain privileged access to systems and processes, so they require the same level of identity security controls as human and machine identities." He expressed the intent behind the collaboration, noting that "by combining the comprehensive identity security capabilities of the CyberArk Platform with the powerful functionality of Accenture's AI Refinery, we will be enabling our customers to realise the full potential of agentic AI to transform their businesses with the peace of mind that comes with knowing the agent identities are secure."

CyberArk's Identity Security Platform is specifically designed to protect human, machine, and AI identities across various environments. With the rise of AI agents, businesses may face the challenge of managing the lifecycle, access, and credentials for potentially millions of machine identities.

The collaboration with Accenture’s AI Refinery, which acts as a foundational platform for transforming AI technology into practical applications, is poised to equip organisations with robust tools necessary for the secure management of AI agents. Accenture's AI Refinery is accessible on both public and private cloud platforms and is structured to facilitate rapid AI deployment within cloud and Software as a Service (SaaS) environments.

A recent report by Accenture, titled Technology Vision 2025, revealed that 77% of executives believe AI agents will revolutionise how their organisations construct digital systems. This widespread expectation highlights the crucial need for securing AI agent identities within the evolving digital workforce.

Damon McDougald, global Cybersecurity Protection lead at Accenture, underscored the complexity of identity security posed by AI agents, stating, "AI agents operate autonomously, presenting unique identity security challenges. Ensuring secure authentication, credentialing, and authorisation is crucial for their safe operation both within and outside of organisations." He described the integration of Accenture's AI Refinery with CyberArk's platform as a “significant step forward” in enabling clients to achieve secure identity access controls and improved credential management.

The partnership focuses on delivering several key capabilities to bolster the safe deployment of AI agents in operational environments. These capabilities include:

* Visibility and Control: Providing enterprises with comprehensive oversight of AI agent activities, allowing for the swift identification of risks or anomalies.
* Least Privilege and Just-in-Time Access: Upholding Zero Trust principles so AI agents receive access only to necessary resources, thereby minimising potential attack surfaces.
* Secure Authentication: Creating strong verification and authentication protocols for AI agents interacting with systems and other agents.
* Protection Against Manipulation: Establishing safeguards aimed at defending AI agents from internal and external threats that may result in data breaches or operational disruptions.

As enterprises increasingly depend on autonomous AI systems, embedding security measures within the core of AI adoption is becoming increasingly essential. The strategic partnership between CyberArk and Accenture seeks to address these emerging needs, aiming to provide organisations with confidence in managing the secure deployment of AI agents.

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

## References

* <https://www.stocktitan.net/news/CYBR/cyber-ark-strengthens-identity-security-for-ai-agents-with-accenture-19uu3xs7hu2c.html> - This article corroborates the collaboration between CyberArk and Accenture to enhance identity security for AI agents, integrating Accenture's AI Refinery with CyberArk's Identity Security Platform, addressing identity-centric cybersecurity challenges in AI deployments.
* <https://www.cyberark.com/press/cyberark-strengthens-identity-security-for-ai-agents-with-accentures-ai-refinery> - It supports the integration of CyberArk's and Accenture's technologies to provide robust tools for securing AI agents based on Zero Trust principles, ensuring secure authentication and management of AI agent identities across various cloud environments.
* <https://newsroom.accenture.com/news/2025/cyberark-strengthens-identity-security-for-ai-agents-with-accenture-s-ai-refinery> - This article highlights the strategic partnership between CyberArk and Accenture, detailing how the collaboration aims to ensure secure identity access controls for AI agents by combining CyberArk's comprehensive identity security capabilities with Accenture's AI Refinery.
* <https://www.cyberark.com/press/cyberark-strengthens-identity-security-for-ai-agents-with-accentures-ai-refinery> - It confirms Matt Cohen's statement emphasizing the importance of robust identity security controls for AI agents, similar to those applied to human and machine identities, underscoring the collaboration's goal to secure AI agent identities.
* <https://newsroom.accenture.com/news/2025/cyberark-strengthens-identity-security-for-ai-agents-with-accenture-s-ai-refinery> - This article supports Damon McDougald's views on the challenges posed by AI agents' autonomous operation and the need for secure authentication and authorization, highlighting the partnership's focus on addressing these needs through integrated solutions.