Red Hat baut KI-Fabrik mit Nvidia aus

19. Mai 2026 - Red Hat baut seine gemeinsam mit Nvidia entwickelte AI Factory aus. Die Plattform soll Unternehmen dabei unterstützen, autonome KI-Agenten sicherer und kontrollierter in den produktiven Betrieb zu bringen.

Mit dem Ausbau der Red Hat AI Factory will Red Hat den Einsatz autonomer KI-Agenten in Unternehmen besser absichern. Laut Unternehmen sollen die neuen Funktionen vor allem dabei helfen, Agenten nicht nur zu testen, sondern dauerhaft zu betreiben, zu überwachen und über ihren Lebenszyklus hinweg zu verwalten.

Ein Schwerpunkt liegt auf Openshell, einem von Nvidia gestarteten Open-Source-Projekt. Es soll eine geschützte Umgebung für KI-Agenten schaffen und regeln, welche Aufgaben ein Agent ausführen darf, auf welche Werkzeuge er zugreifen kann und wie seine Arbeit nachvollziehbar bleibt. Red Hat arbeitet daran, Openshell in die eigene KI-Plattform einzubinden.

Zusätzlich erweitert der Konzern die Plattform um Funktionen für besonders geschützte

Ausführungsumgebungen. Dabei kommt Nvidia Confidential Computing in Verbindung mit Openshift Sandbox Containers zum Einsatz. Die Technik soll Agenten und ihre Daten während der Verarbeitung besser abschirmen und ist zunächst als Technologievorschau verfügbar.

Weitere Neuerungen kommen mit Red Hat AI 3.4. Dazu gehören ein einfacherer Zugriff auf ausgewählte KI-Modelle über das Red Hat AI Gateway sowie Funktionen zur Nachverfolgung von Modellaufrufen, Werkzeugnutzung und einzelnen Entscheidungsschritten. Die Updates für Red Hat AI Factory und Red Hat AI 3.4 sollen voraussichtlich Ende dieses Monats verfügbar sein.