CyberArk führt erste Identity-Security-Lösung für KI-Agenten ein

- *Speziell entwickelte Lösung bietet privilegierte Zugriffskontrollen, Transparenz und Compliance für die neue Klasse von KI-Agenten-Identitäten.*
- *Sie erweitert die Identity-Security-Funktionen von CyberArk, um KI-gestützte Automatisierung im Unternehmen abzusichern.*

München – 5. November 2025 – CyberArk (NASDAQ: CYBR), der weltweit führende Anbieter im Bereich Identity Security, gibt die allgemeine Verfügbarkeit[1] der CyberArk Secure AI Agents Solution bekannt, einer speziell entwickelten Lösung zur Absicherung jeder KI-Agenten-Identität. Die Lösung erweitert die CyberArk Identity Security Platform um eine branchenweit erste privilegierte Zugriffskontrolle, die speziell für die Absicherung der rasant wachsenden Anzahl von KI-Agenten-Identitäten entwickelt wurden.

Da Unternehmen KI-Agenten zunehmend einsetzen, um Aufgaben zu automatisieren und Effizienz zu steigern, entsteht eine neue, privilegierte Identitätsklasse. KI-Agenten bringen neuartige Risiken mit sich, darunter Fehlverhalten und die mögliche Übernahme durch Angreifer. Diese Risiken erhärten sich, wenn Agenten privilegierte Zugriffe benötigen.

Die CyberArk Secure AI Agents Solution adressiert diese Herausforderungen, indem sie das richtige Maß an privilegierten Zugriffskontrollen durchsetzt und sicherstellt, dass KI-Agenten nur genau die Zugriffsrechte erhalten, die sie benötigen – nicht mehr und nicht weniger. Dieser Ansatz reduziert Risiken, verhindert unautorisierte Zugriffe und ermöglicht es Unternehmen, KI-gestützte Initiativen sicher und skalierbar umzusetzen.

„Wenn Unternehmen KI-Agenten einführen, müssen sowohl Entwickler als auch Sicherheitsverantwortliche verstehen, wie sich identitätszentrierte Risiken verändern, sobald Agenten privilegierte Zugriffe benötigen“, sagte **Matt Cohen, CEO von CyberArk**. „Ohne starke Erkennungsmechanismen, robuste privilegierte Zugriffskontrollen und ein umfassendes Lifecycle Management riskieren Unternehmen den Verlust von Transparenz und öffnen die Tür für schwerwiegende Angriffe. CyberArk schützt das gesamte Spektrum an Identitäten - Menschen, Maschinen und KI-Agenten - durch privilegierte Zugriffskontrollen und ermöglicht so Innovation ohne Abstriche bei Sicherheit und Compliance.“

Absicherung von KI-Agenten erfordert einen Privilegien-zentrierten Ansatz

Laut neuer CyberArk CISO Studie wird die Einführung von KI-Agenten in den nächsten drei Jahren voraussichtlich 76% erreichen – doch weniger als10 % der Unternehmen verfügen über angemessene Sicherheits- und Privilegienkontrollen. Der Bericht Securing Agentic AI: Identity as the Emerging Foundation for Defense zeigt:

- Fast 40% der großen Finanzinstitute und Softwareunternehmen haben KI-Agenten bereits produktiv im Einsatz.
- Weniger als jedes zehnte Unternehmen hat Sicherheitskontrollen für Agenten wie Risk Registries oder dynamische Autorisierung im großen Maßstab eingeführt.
- Zwei Drittel der CISOs aus Finanzdienstleistungen und Software zählen agentische KI zu ihren drei größten Cyberrisiken – über ein Drittel sogar zu ihrem größten.
- Die meisten erwarten, dass Sicherheitsanforderungen für KI-Agenten die Cybersecurity-Budgets im kommenden Jahr erhöhen werden.

KI-Agenten handeln autonom, treffen Entscheidungen und greifen auf sensible Systeme zu - häufig mit privilegierten Berechtigungen. Ohne angemessene Kontrollen können diese Privilegien missbraucht oder kompromittiert werden, was schwerwiegende geschäftliche und regulatorische Folgen nach sich ziehen kann.

Privilegienkontrollen für jede Identität

Die CyberArk Identity Security Platform bietet umfassende privilegierte Zugriffskontrollen für das gesamte Identitätsspektrum: menschliche, maschinelle und KI-basierte Identitäten. Mit der neuen Secure AI Agents Solution werden diese bewährten Fähigkeiten nun auf autonome KI-Agenten ausgeweitet - basierend auf den gleichen Grundprinzipien wie Just-in-Time-Zugriff, Least Privilege und kontinuierliche Sitzungsüberwachung, die CyberArks Führungsrolle im Bereich Identity Security prägen.

Dieser einheitliche Ansatz stellt sicher, dass jede Identität mit derselben Konsequenz verwaltet, geschützt und überwacht wird – und unterstützt Innovation, ohne Sicherheit oder Compliance zu gefährden.

Die CyberArk Secure AI Agents Solution bietet:

- **Umfassende Agent Discovery**: Automatische Erkennung von KI-Agenten in SaaS-, Cloud- und Entwicklerumgebungen inklusive angereicherter Profile mit Eigentümerinformationen, Rollen und Zugriffsrechten.
- **Sicherer Agentenzugriff:** Durchsetzung starker Authentifizierung und Least-Privilege-Zugriff mit Zero Standing Privileges und vollständiger Auditierung aller Agentenaktivitäten.
- **Echtzeit-Erkennung von Bedrohungen:** Kontinuierliche Überwachung auf Anomalien und unautorisierte Zugriffe mit automatisierten Warnmeldungen und schnellen Reaktionen.
- **Lifecycle Management & Compliance:** Verwaltung von KI-Agenten vom Anlegen bis zur Außerbetriebnahme, inklusive Unterstützung regulatorischer Anforderungen und Auditfähigkeit.

Weitere Informationen:

- Mehr über die CyberArk Secure AI Agents Lösung
- Blog: The CyberArk Secure AI Agents Solution – A Closer Look
- Forschungsbericht: Securing Agentic AI: Identity as the Emerging Foundation for Defense - Eine Umfrage unter 104 CISOs aus Nordamerika und Europa.

[1]Die allgemeine Verfügbarkeit der CyberArk Secure AI Agents Solution ist für Dezember 2025 geplant, weitere Releases folgen 2026.

Über CyberArk

CyberArk (NASDAQ: CYBR) ist der weltweit führende Anbieter im Bereich Identity Security und wird von Unternehmen auf der ganzen Welt vertraut, um menschliche und maschinelle Identitäten

im modernen Unternehmen abzusichern. Die KI-gestützte Identity Security Platform von CyberArk wendet intelligente Privilegienkontrollen auf jede Identität an und bietet kontinuierliche Bedrohungsprävention, -erkennung und -reaktion über den gesamten Identitätslebenszyklus hinweg.

###

Cautionary Language Concerning Forward-Looking Statements

This release contains forward-looking statements, which express the current beliefs and expectations of CyberArk's (the "Company") management. In some cases, forward-looking statements may be identified by terminology such as "believe," "may," "estimate," "continue," "anticipate," "intend," "should," "plan," "expect," "predict," "potential" or the negative of these terms or other similar expressions. Such statements involve a number of known and unknown risks and uncertainties that could cause the Company's future results, levels of activity, performance or achievements to differ materially from the results, levels of activity, performance or achievements expressed or implied by such forward-looking statements. Important factors that could cause or contribute to such differences include, but are not limited to: risks related to the Company's acquisitions of Venafi Holdings, Inc. ("Venafi") and Zilla Security Inc. ("Zilla"), including potential impacts on operating results; challenges in retaining and hiring key personnel and maintaining business; risks related to the successful integration of Venafi's or Zilla's operations and the ability to realize anticipated benefits of the combined operations; disruption of the current plans and operations of the Company and/or Zilla as a result of the announcement of the transaction, including risks of cyberattacks; changes to the drivers of the Company's growth and the Company's ability to adapt its solutions to the information security market changes and demands, including artificial intelligence ("AI"); the Company's ability to acquire new customers and maintain and expand the Company's revenues from existing customers; intense competition within the information security market; real or perceived security vulnerabilities, gaps, or cybersecurity breaches of the Company, or the Company's customers' or partners' systems, solutions or services; risks related to the Company's compliance with privacy, data protection and AI laws and regulations; the Company's ability to successfully operate its business as a subscription company and fluctuation in its quarterly results of operations; the Company's reliance on third-party cloud providers for its operations and software-as-a-service ("SaaS") solutions; the Company's ability to hire, train, retain and motivate qualified personnel; the Company's ability to effectively execute its sales and marketing strategies; the Company's ability to find, complete, fully integrate or achieve the expected benefits of additional strategic acquisitions; the Company's ability to maintain successful relationships with channel partners, or if the Company's channel partners fail to perform; risks related to sales made to government entities; prolonged economic uncertainties or downturns; the Company's history of incurring net losses, the Company's ability to generate sufficient revenue to achieve and sustain profitability and the Company's ability to generate cash flow from operating activities; regulatory and geopolitical risks associated with the Company's global sales and operations; risks related to intellectual property claims; fluctuations in currency exchange rates; the ability of the Company's products to help customers achieve and maintain compliance with government regulations or industry standards; the Company's ability to protect its proprietary technology and intellectual property rights; risks related to using third-party software, such as open-source software; risks related to stock price volatility or activist shareholders; any failure to retain the Company's "foreign private issuer" status or the risk that the Company may be classified,

for U.S. federal income tax purposes, as a "passive foreign investment company"; changes in tax laws; the Company's expectation to not pay dividends on the Company's ordinary shares for the foreseeable future; risks related to the Company's incorporation and location in Israel, including wars and other hostilities in the Middle East; and other factors discussed under the heading "Risk Factors" in the Company's most recent annual report on Form 20-F filed with the Securities and Exchange Commission. Forward-looking statements in this release are made pursuant to the safe harbor provisions contained in the U.S. Private Securities Litigation Reform Act of 1995. These forward-looking statements are made only as of the date hereof, and the Company undertakes no obligation to update or revise the forward-looking statements, whether as a result of new information, future events or otherwise, except as required by applicable law.

Pressekontakt

The Hoffman Agency GmbH

Ina Rohe/Carolin Joos

Emil Riedel Str. 18

80538 München

E: cyberarkde@hoffman.com