NEWS RELEASE

ServiceNow stellt Autonomous Security & Risk vor und integriert Armis und Veza für eine autonome Sicherheits- und Risikosteuerung

2026-05-05

Armis liefert kontinuierliche Asset-Transparenz über Code, IT, OT, IoT und vernetzte Geräte hinweg; Veza ergänzt dies um granulare Einblicke in Berechtigungen sowie Governance für menschliche und nicht-menschliche Identitäten.

Die ServiceNow AI Platform ist eine der umfassendsten Plattformen für Sicherheit, Risiko und Compliance für Enterprise-KI.

München – Knowledge 2026 -, 5. Mai 2026 - Auf seiner jährlichen Kunden- und Partnerkonferenz **Knowledge 2026** hat **ServiceNow** (NYSE: NOW), der AI Control Tower für die geschäftliche Neuerfindung, heute **Autonomous Security & Risk** vorgestellt. Die Lösung dient der Steuerung aller KI-Agenten, Identitäten und vernetzten Assets. Dabei ermöglicht Armis eine kontinuierliche, kontextbezogene Transparenz über sämtliche Assets hinweg – von Code über IT- und OT-Systeme bis hin zu IoT-Geräten. Veza bietet detaillierte Einblicke in Berechtigungen sowie Governance-Funktionen für menschliche und nicht-menschliche Identitäten. Gemeinsam bilden diese Technologien eine der umfassendsten Plattformen für Sicherheit, Risiko und Compliance im Bereich Enterprise-KI.

Im vergangenen Jahr überschritt der Bereich Security & Risk bei ServiceNow einen jährlichen Vertragswert (ACV) von über einer Milliarde US-Dollar und zählt damit zu den am schnellsten wachsenden Geschäftsfeldern der ServiceNow AI Platform. Der Druck nimmt weiter zu, da KI die Anzahl von Identitäten, Berechtigungen, vernetzten Assets und Entscheidungen, die Governance erfordern, exponentiell steigen lässt. KI-Agenten erhalten Zugriff, treffen Entscheidungen und agieren mit maschineller Geschwindigkeit – und die dahinterstehenden nicht-

menschlichen Identitäten übertreffen die menschlichen bereits bei Weitem. Gleichzeitig fehlt in den meisten Unternehmen der Überblick darüber, wer Zugriffe genehmigt, warum sie bestehen und ob sie noch gültig sind. Isolierte Sicherheitslösungen können diese Lücke nicht schließen – ein Plattformansatz hingegen schon.

„„CISOs stehen heute vor der Herausforderung, gleichzeitig zwei Aufgaben zu bewältigen: Bedrohungen in Echtzeit abzuwehren und Risiken gegenüber dem Vorstand klar und überzeugend zu kommunizieren“, so John Aisien, Senior Vice President und General Manager, Central Product Management, Security & Risk bei ServiceNow. „Autonomous Security & Risk ersetzt fragmentierte Tool-Landschaften durch einen zentralen Graphen, der jede Identität, jede Berechtigung und jedes vernetzte Asset abbildet, sodass Prävention, Erkennung und Reaktion mit Maschinengeschwindigkeit erfolgen.“

Jeder KI-Agent ist eine Identität – meist unzureichend gesteuert

Jeder KI-Agent, der innerhalb eines Unternehmens agiert, tut dies über eine eigene Identität. Er greift auf Systeme zu, liest Daten aus und führt Workflows aus. All das geschieht auf Basis von Berechtigungen, die in der Regel für menschliche Nutzer konzipiert wurden und nicht für die Geschwindigkeit, Skalierung und Autonomie von KI-Agenten. Die Lücke hinsichtlich Transparenz, Steuerung und Governance von Identitäten zu schließen, ist daher entscheidend.

Der Access Graph von **Veza** erstellt eine kontinuierliche Echtzeit-Abbildung sämtlicher Zugriffsbeziehungen innerhalb einer Unternehmensumgebung. Er zeigt, wer oder was Zugriff hat, was damit möglich ist und wie sich diese Berechtigungen verändern, wenn sich Kontexte verschieben, Systeme weiterentwickeln und die Zahl der Agenten steigt. Durch die Integration von Veza in die ServiceNow AI Platform werden sowohl menschliche als auch nicht-menschliche Identitäten in einem einheitlichen operativen Rahmen gesteuert: Risiken werden transparent gemacht, das Prinzip der minimalen Rechtevergabe direkt bei der Nutzung durchgesetzt und nachgelagerte Gegenmaßnahmen angestoßen. Außerdem wird eine nachvollziehbare, revisionssichere Dokumentation aufgebaut, wie sie Auditoren und Regulierungsbehörden verlangen. ServiceNow Veza arbeitet dabei eng mit den bestehenden Funktionen für Schwachstellen-, Expositions- und Incident-Management von ServiceNow zusammen, um Risiken vor und nach Sicherheitsvorfällen zu minimieren. Dabei wird gesteuert, wer und was Zugriff hat, während berechtigungsbezogene Schwachstellen kontinuierlich identifiziert und behoben werden.

Man kann nur schützen, was man auch sieht

Transparenz über Assets ist seit jeher eine grundlegende Voraussetzung für Unternehmenssicherheit - zugleich aber auch eine ihrer größten Schwachstellen. Die heutigen IT-Umgebungen von Unternehmen umfassen Software-Code, IT-Infrastrukturen, Betriebstechnologie, vernetzte Geräte, Cloud-Workloads, medizinische Systeme und inzwischen auch KI-Agenten. All diese Komponenten interagieren über Systemgrenzen hinweg, die kein einzelnes

Tool jemals vollständig erfassen konnte.

Nach der Integration in ServiceNow liefert **Armis** ein kontextbasiertes Echtzeitverständnis aller vernetzten Cyber-Assets, einschließlich solcher Geräte und Systeme, die von herkömmlichen Tools bislang nicht erfasst wurden. Armis analysiert den Netzwerkverkehr agentenlos und ohne den laufenden Betrieb zu beeinträchtigen. Zudem ergänzt Armis jeden Asset-Datensatz um Informationen wie Gerätetyp, Klassifizierung, Firmware-Version, Verhaltensdaten sowie die aktuelle Risikobewertung. Diese Erkenntnisse fließen direkt in die ServiceNow CMDB (Configuration Management Database) ein und verwandeln ein bislang statisches Inventar in ein dynamisches, aktuelles Abbild der tatsächlichen Angriffsfläche. Wird ein Asset als verwundbar, falsch konfiguriert oder auffällig erkannt, reagiert ServiceNow in Maschinengeschwindigkeit und berücksichtigt dabei den jeweiligen Kontext der Umgebung.

Gemeinsam stärken Veza und Armis die Position von ServiceNow als Plattform, die sowohl Transparenz darüber schafft, welche Assets in der Umgebung vorhanden sind, als auch darüber, wer oder was mit ihnen interagieren darf. Diese Echtzeit-Asset-Intelligenz fließt direkt in die Security-Incident-Response-Workflows von ServiceNow ein. Dadurch steht derselbe Kontext, der zur Risikobewertung vor einem Sicherheitsvorfall genutzt wird, unmittelbar auch für dessen Eindämmung danach zur Verfügung.

Der Bauplan für vertrauenswürdige KI

Wenn KI innerhalb eines Unternehmens agiert, muss jede Entscheidung auf einer fundierten, unternehmensweiten Grundlage beruhen, einschließlich gesteuerter Berechtigungen, kontinuierlicher Überwachung und einer revisionssicheren Nachvollziehbarkeit. Genau das leistet Autonomous Security & Risk. Die Lösung vereint Asset-Transparenz, Identitäts-Governance, Risikomanagement und Workflow-Automatisierung in einem integrierten System, in dem KI durchgängig operiert. **Zwei neue KI-Spezialisten**, die heute im Rahmen der Erweiterung der Autonomous Workforce von ServiceNow vorgestellt wurden, übernehmen das Schwachstellenmanagement sowie Security Operations durchgängig: Sie bearbeiten eigenständig bestehende Rückstände bei Schwachstellen und untersuchen Phishing-Vorfälle in Zusammenarbeit mit menschlichen Teams.

Der **ServiceNow AI Control Tower** steuert KI-Agenten und stellt sicher, dass sie vom ersten Moment an erfasst, kontinuierlich hinsichtlich ihres Risikos bewertet und Zugriffsrechte nach dem Prinzip der minimalen Berechtigung in Echtzeit durchgesetzt werden. Bewertungen erfolgen laufend während des Betriebs. Abweichungen erkennt der AI Control Tower frühzeitig, bevor sie sich ausweiten. Dank der Interoperabilität über A2A (Agent2Agent) und MCP (Model Context Protocol) hinweg können Agenten plattformübergreifend in einem gesteuerten Rahmen arbeiten, der Entscheidungen in ihren Kontext einordnet und Verantwortlichkeiten klar zuweist. Dieser Governance-Rahmen erstreckt sich auch auf das Partner-Ökosystem von ServiceNow, sodass bereits eingesetzte Sicherheitslösungen von Drittanbietern in ein kontinuierlich aktualisiertes Gesamtbild der Sicherheitslage im Unternehmen einfließen. Das

eigene Team für den IT-Sicherheitsbetrieb von ServiceNow nutzt Autonomous Risk & Security und bearbeitet Sicherheitsvorfälle mithilfe von KI-Agenten siebenmal schneller als mit bisherigen Workflows – bei vollständiger Dokumentation aller Maßnahmen und lückenloser Nachvollziehbarkeit aller Entscheidungen.

Unternehmen erzielen bereits messbare Ergebnisse mit der **ServiceNow AI Platform**. Ein weltweit tätiger Energiekonzern, der in über 70 Ländern aktiv ist, sparte durch die Automatisierung des IT-Sicherheitsbetriebs 1,2 Millionen Arbeitsstunden und verkürzte die Zeit zur Eindämmung von Bedrohungen um 97 %. Ein großes US-Finanzinstitut eliminierte 96 % inaktiver nicht-menschlicher Identitäten und machte das Prinzip der minimalen Rechtevergabe von einem strategischen Ziel zur gelebten Praxis. Ein Luft- und Raumfahrtunternehmen aus den Fortune 100 reduzierte den Zeitaufwand für Kontrollnachweise um 75 % und schloss Compliance-Lücken um 85 % schneller – anstelle manueller Audit-Vorbereitung sorgen nun automatisiert generierte Nachweise für Transparenz.

Unternehmen, die diese Grundlage aus umfassender Transparenz, gesteuerten Identitäten, integriertem Risikomanagement und automatisierten Reaktionen schaffen, werden mit fortschreitender KI-Entwicklung klar im Vorteil sein. ServiceNow ermöglicht Verantwortlichen für Sicherheit und Risiko eine zentrale Sicht darauf, wie sich Angriffsflächen, Sicherheitsvorfälle und identitätsbezogene Entscheidungen in Echtzeit auf das Risikoprofil des Unternehmens auswirken – inklusive der revisionssicheren Nachvollziehbarkeit, die Regulierungsbehörden verlangen.

Über ServiceNow

ServiceNow (NYSE: NOW) ist der AI Control Tower für die geschäftliche Neuerfindung. Die ServiceNow AI Platform lässt sich in jede Cloud, jedes Modell und jede Datenquelle integrieren, um die Arbeitsabläufe im gesamten Unternehmen zu koordinieren. Durch die Vereinheitlichung von Legacy-Systemen, abteilungsspezifischen Tools, Cloud-Anwendungen und KI-Agenten bietet ServiceNow eine zentrale Oberfläche, die Intelligenz mit der Umsetzung in allen Unternehmensbereichen verbindet. Mit mehr als 95 Milliarden Workflows, die jedes Jahr auf der Plattform ausgeführt werden, hilft ServiceNow Unternehmen dabei, fragmentierte Abläufe in koordinierte, autonome Workflows umzuwandeln, die messbare Ergebnisse liefern. Erfahren Sie unter **www.servicenow.de**, wie ServiceNow KI für Menschen nutzbar macht.

Zukunftsgerichtete Aussagen

Diese Pressemitteilung enthält „zukunftsgerichtete Aussagen“ zu Erwartungen, Annahmen, Planungen und Absichten im Zusammenhang mit den Innovationen der KI-Plattform von ServiceNow. Dazu zählen insbesondere Aussagen über zukünftige Produktfunktionen und -angebote sowie erwartete Vorteile für ServiceNow. Zukunftsgerichtete Aussagen unterliegen bekannten und unbekannten Risiken und Unsicherheiten und basieren auf Annahmen, die sich als unzutreffend erweisen können. Dies kann dazu führen, dass die tatsächlichen

Ergebnisse erheblich von den in den zukunftsgerichteten Aussagen ausdrücklich oder implizit dargestellten Ergebnissen abweichen. Sollten sich solche Risiken oder Unsicherheiten realisieren oder sich Annahmen als falsch herausstellen, können die tatsächlichen Ergebnisse von ServiceNow erheblich von den prognostizierten abweichen.ServiceNow übernimmt keine Verpflichtung und beabsichtigt nicht, diese zukunftsgerichteten Aussagen zu aktualisieren.

Zu den Faktoren, die dazu führen können, dass die tatsächlichen Ergebnisse wesentlich von den in zukunftsgerichteten Aussagen dargestellten abweichen, gehören unter anderem:
(i) Verzögerungen sowie unerwartete Schwierigkeiten und Kosten bei der Umsetzung der Produktfunktionen und -angebote,
(ii) Veränderungen im regulatorischen Umfeld im Zusammenhang mit KI sowie
(iii) Unsicherheiten darüber, ob die Umsätze die Investitionen in die Produktfunktionen und -angebote rechtfertigen.

Weitere Informationen zu Faktoren, die die finanziellen und sonstigen Ergebnisse von ServiceNow beeinflussen können, sind in den regelmäßig bei der Securities and Exchange Commission (SEC) eingereichten Unterlagen von ServiceNow enthalten.

Pressekontakt

ServiceNow

Mathias Raeck
Senior Manager Corporate Communications, EMEA Central
E-Mail: mathias.raeck@servicenow.com

Daniela Preis
Senior Specialist Corporate Communications
E-Mail: daniela.preis@servicenow.com

Maisberger GmbH
Maren Voß / Tanja Stricker
Claudius-Keller-Straße 3c
D-81669 München
E-Mail: servicenow@maisberger.com
Web: **www.maisberger.de**