

ServiceNow stärkt mit AI Passport und erweitertem Super Intelligence Control Tower die Steuerung von KI in Unternehmen

2026-10-15

Die neue Lösung AI Passport überprüft in Echtzeit die Berechtigungen eigener und externer KI-Agenten

Der Super Intelligence Control Tower bietet erweiterte Funktionen zur Erkennung und Steuerung von KI, schafft mehr Transparenz und erleichtert die Bewertung von KI-Kosten und -Nutzen auf Basis eines einheitlichen Datenmodells

SANTA CLARA, 15. Oktober 2026 – **ServiceNow** (NYSE: NOW), der Super Intelligence Control Tower für die geschäftliche Neuerfindung, hat heute seine neue Lösung AI Passport sowie umfassende Erweiterungen des Super Intelligence Control Tower vorgestellt. Beide Lösungen helfen Unternehmen, KI-Agenten sicher in den produktiven Betrieb zu überführen. Dazu verbindet ServiceNow Governance zur Laufzeit, Plattformintegration und umfassende Überwachung in einem gemeinsamen operativen Rahmen für KI. AI Passport bildet dabei eine neue Berechtigungsebene: Unternehmen können während der Ausführung kontrollieren, welche Aktionen KI-Agenten in jeder Phase eines Workflows ausführen dürfen. Mit den erweiterten Funktionen des Super Intelligence Control Tower können Unternehmen zudem erfassen, welche KI im Einsatz ist, die Aktionen von KI-Agenten steuern und die Ausgaben den erzielten Ergebnissen gegenüberstellen.

Damit KI-Agenten Unternehmensprozesse sicher ausführen können, brauchen sie mehr als ein Reasoning-Modell. Sie benötigen klare Vorgaben: Auf welche Daten und Werkzeuge sie zugreifen dürfen, welche Aktionen zulässig sind

und wer diese autorisiert hat. Letzteres muss nachvollziehbar dokumentiert sein. ServiceNow schafft die operative Grundlage: AI Passport ist ein kryptografisch signierter Berechtigungsnachweis, anhand dessen KI-Agenten während der Ausführung prüfen, einschließlich Umgebungen wie NVIDIA OpenShell, welche Aktionen sie ausführen dürfen. Dabei wird der Geschäftskontext des Unternehmens berücksichtigt, damit Entscheidungen im Rahmen der geltenden Vorgaben getroffen werden. Solange ein Agent innerhalb dieser Berechtigungen handelt, kann er eigenständig agieren. Weicht er davon ab, lassen sich abgestufte Maßnahmen durchsetzen: Der Agent kann neu ausgerichtet, in seinen Handlungsmöglichkeiten eingeschränkt oder erneut mit dem erforderlichen Kontext versorgt werden. Falls erforderlich, lässt er sich über eine Kill Switch-Funktion in Maschinengeschwindigkeit stoppen. Der Super Intelligence Control Tower dokumentiert dabei lückenlos, wer welche Aktion autorisiert hat und wie sie ausgeführt wurde. So wird die Arbeit von KI-Agenten steuerbar und überprüfbar, und Verantwortlichkeiten bleiben nachvollziehbar.

„Je mehr KI-Agenten in Unternehmen eingesetzt werden, desto weniger reicht Transparenz allein aus. Unternehmen müssen sich darauf verlassen können, dass jeder KI-Agent innerhalb seiner Berechtigungen handelt“, sagt Jon Sigler, Executive Vice President und General Manager AI Platform bei ServiceNow. „ServiceNow schließt diese Lücke mit einem operativen Steuerungsrahmen auf Basis von AI Passport und Super Intelligence Control Tower. Er umfasst die Berechtigungen der Agenten, Governance und die Überwachung im laufenden Betrieb – und schafft damit die Grundlage für eine kontrollierte Skalierung von Agentic AI.“

AI Passport: Überprüfbare Berechtigungen, die direkt beim Einsatzpunkt greifen

AI Passport basiert auf offenen Spezifikationen. Dadurch können Governance-Lösungen, Identitätsanbieter und Kontrollinstanzen Berechtigungsnachweise für eigene KI-Agenten und KI-Agenten von Drittanbietern ausstellen und überprüfen. Diese Nachweise lassen sich bei jedem Schritt eines Multi-Agenten-Workflows verifizieren.

Der Ansatz verlagert den Fokus grundlegend von der Reaktion zur Prävention. Während Audit-Protokolle im Nachhinein dokumentieren, was geschehen ist, hilft AI Passport, unzulässige Aktionen im Vorfeld zu verhindern, indem er zur Laufzeit prüft, welche Aktionen ein KI-Agent ausführen darf. Das setzt den “Shift Zero“-Ansatz von ServiceNow um: Sicherheit von Anfang an mitgedacht.

Jeder KI-Agent erhält einen eigenen AI Passport, der vom Super Intelligence Control Tower ausgestellt wird. Als Grundlage dient der aktuelle Geschäftskontext des Unternehmens, abgebildet durch die ServiceNow Configuration Management Database (CMDB), die Richtlinien für Governance, Risk und Compliance (GRC) sowie Workflow-Freigaben. Gerade bei externen KI-Agenten entsteht so ein überprüfbarer Berechtigungsnachweis, der über die bloßen Angaben des Agenten zu seinen eigenen Berechtigungen hinausgeht.

Durch diesen Ansatz lassen sich Berechtigungen gezielt widerrufen und kontrolliert delegieren. Bei jeder

Weitergabe wird der Handlungsspielraum enger begrenzt. Hinzu kommen Audit-Protokolle mit vollständigen Compliance-Signaturen. ServiceNow gibt außerdem NVIDIA als ersten Entwicklungs- und Markteinführungspartner bekannt. NVIDIA entwickelt über seine AI Factories die erste produktionsreife Implementierung zur Durchsetzung der Berechtigungen. Grundlage dafür ist die NVIDIA Open Agent Safety Platform, die aus der quelloffenen Sicherheitssoftware NVIDIA OpenShell und dem Sicherheitsframework NVIDIA Sentry besteht.

„Immer mehr Unternehmen gehen dazu über, KI-Agenten nicht mehr nur zu testen, sondern im Arbeitsalltag einzusetzen. Um diese Agenten zuverlässig abzusichern, müssen Sicherheitsvorgaben direkt auf Infrastrukturebene durchgesetzt werden“, sagt Itay Ozery, Director of Product Marketing für Netzwerke und Cybersicherheit bei NVIDIA. „Durch die Kombination von AI Passport mit der NVIDIA Open Agent Safety Platform können ServiceNow-Kunden während des laufenden Betriebs kontinuierlich überprüfen und durchsetzen, welche Aktionen ein KI-Agent ausführen darf – automatisiert und in Maschinengeschwindigkeit.“

Super Intelligence Control Tower: KI zentral erfassen, überwachen und bewerten

Ergänzend zu AI Passport hat ServiceNow den Super Intelligence Control Tower erweitert. Er bietet durchgängige KI-Governance, von der Erfassung eingesetzter KI über Transparenz und Steuerung bis hin zu Erfolgsmessung und Compliance. Die neuen Funktionen bauen auf den bestehenden Möglichkeiten zur autonomen Problembehebung und zum Abschalten von KI-Agenten auf.

Die ServiceNow AI Platform nutzt ein einheitliches Datenmodell. Dadurch lassen sich Governance-Entscheidungen auf Basis von Informationen zu IT-Assets, Identitätssicherheit und KI-Observability automatisieren. Manuelle Übergaben zwischen Teams entfallen:

- Erkennung von Schatten-KI: Identifiziert nicht genehmigte KI-Agenten im Netzwerk.
- Mehr als 400 vorkonfigurierte Konnektoren: Ermöglicht die Erkennung von KI über Plattformen und Anbieter hinweg ermöglichen.
- Zuordnung von Zugriffsrechten: Stützt Autorisierungsentscheidungen auf tatsächlich vorhandene Berechtigungen.
- Transparenz über die Aktivitäten von KI-Agenten im Unternehmen: Verfolgt die Ausführungsabläufe und das Verhalten von KI-Agenten.

Neben der Frage, welche KI im Einsatz ist, müssen Unternehmen auch beurteilen können, ob sie einen Mehrwert liefert und im vorgesehenen Budget bleibt. Dafür bietet der Super Intelligence Control Tower jetzt folgende Funktionen:

- Kosten-Governance: Erfasst Ausgaben nach Nutzung, Abteilungen und Laufzeit.
- Value Intelligence: Setzt Nutzung, Kosten, Qualität und den tatsächlich realisierten Nutzen für Anwender in Beziehung. Teams können dadurch den KI-Einsatz optimieren, Budgets einhalten und den geschäftlichen Mehrwert nachweisen.
- AI Cost Management als Bestandteil des IT Asset Management (ITAM): Wird in den Super Intelligence Control Tower integriert, um die Kosten für führende KI-Modelle, in SaaS eingebettete KI, Hyperscaler sowie GPUs in Rechenzentren in einer zentralen Übersicht zusammenzuführen. Die Funktion soll vor möglichen Budgetüberschreitungen warnen und Ausgaben im geschäftlichen Kontext einordnen.
- Durchsetzung von Richtlinien: Wird abgestufte Maßnahmen steuern, von Warnmeldungen über Drosselung bis hin zur Blockierung.

Super Intelligence Control Tower für stark regulierte Branchen

Für Finanzinstitute erhöhen unkontrollierte Assets und Schatten-KI die Risiken bei der Einhaltung regulatorischer Meldefristen. Aufsichtsbehörden verkürzen die Fristen für die Meldung von Vorfällen schneller, als manuelle tabellenbasierte Prozesse Schritt halten können. Der ServiceNow Banking AI Maturity Index 2026 verdeutlicht diese Lücke: 100 Prozent der befragten Banken geben an, KI einzusetzen, aber nur 24 Prozent verfügen über eine entsprechend entwickelte Governance. Nicht verwaltete Servicekonten, Schatten-KI-Agenten und nicht registrierte Geräte bleiben damit potenzielle Angriffsflächen.

Die neue ServiceNow-Lösung Operational Resilience vereint KI-Governance, Risikomanagement und Sicherheit auf einer zentralen Plattform. Eine gemeinsame Datenbasis hilft Finanzinstituten, schnell zu reagieren und bietet Risikoverantwortlichen (CROs) und Sicherheitsverantwortlichen (CISOs) einheitliche Transparenz und Kontrolle in Echtzeit. Der Super Intelligence Control Tower erkennt Assets, Identitäten und KI-Agenten, die sich der zentralen Kontrolle entziehen – über IT-, OT- und Cloud-Umgebungen sowie Drittsysteme hinweg.

Ein nicht regelkonform handelnder KI-Agent wird wie jedes anderes gefährdete Asset behandelt: Das System erkennt ihn, kennzeichnet ihn und kann ihn bei Bedarf abschalten. Bei einem Vorfall können Banken die Lage innerhalb regulatorischer Fristen prüfen, den Vorfall eindämmen und Zugriffsrechte widerrufen können, einschließlich nachvollziehbarer Nachweise.

Kundenstimmen

LTM Limited

„Im Zuge unserer Weiterentwicklung als KI-orientiertes Unternehmen haben wir bei LTM bereits 1.500 KI-Agenten

unternehmensweit eingeführt. Jedem sind eine Mitarbeiter-ID und eine Führungskraft zugeordnet, um Verantwortlichkeit, Kontrolle und kontinuierliche Verbesserung sicherzustellen“, sagt Chandan Pani, Chief Information Security Officer bei LTM. „Der ServiceNow Super Intelligence Control Tower bietet uns ein zentrales System of Record für diese KI-Agenten und damit einen einheitlichen Überblick über Bestand, Risiken und Compliance. Durch ein effizienteres KI-Asset-Management und stärkere Governance erwarten wir unsere operative Effizienz deutlich zu steigern. Diese Funktionen bilden eine Grundlage dafür, KI bei LTM verantwortungsvoll zu skalieren, Risiken besser zu überwachen und einen höheren geschäftlichen Nutzen aus unseren KI-Investitionen zu erzielen.“

Verfügbarkeit

Der AI Passport, die Erkennung von Shadow AI und AI Cost Management werden voraussichtlich im vierten Quartal 2026 verfügbar sein. Die ServiceNow-Lösung Operational Resilience für Finanzdienstleister ist ab sofort verfügbar.

Besucherinnen und Besucher der NVIDIA GTC Berlin können in der Session **SB61172** mehr über AI Passport erfahren. Die Lösung basiert auf der ServiceNow AI Platform und der NVIDIA Open Agent Safety Platform.

Über ServiceNow

ServiceNow (NYSE: NOW) ist der Super Intelligence 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 100 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.

© 2026 ServiceNow, Inc. Alle Rechte vorbehalten. ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc. in den Vereinigten Staaten und/oder anderen Ländern. Andere Firmennamen, Produktnamen und Logos können Marken der jeweiligen Unternehmen sein, mit denen sie in Verbindung stehen. **<http://www.servicenow.de>**

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

Maren Voss / Tanja Stricker

E-Mail: servicenow@maisberger.com