Saviynt™

2026

CISO AI Risk Report Germany

Vorwort

Künstliche Intelligenz* breitet sich in Unternehmen schneller aus, als Sicherheitsstrukturen Schritt halten können.
In den meisten Fällen geschieht dies nicht kontrolliert oder strategisch, sondern beiläufig: Ein Copilot wird aktiviert, ein Agent getestet, ein KI-Assistent eingeführt – oft ohne formale Freigaben oder klare Zuständigkeiten.

Was einzeln harmlos wirkt, entwickelt sich in Summe zu einem System, das eigenständig im Namen von Menschen handelt, und das häufig außerhalb etablierter Sicherheitsmechanismen.

In unserer Umfrage unter CISOs, Führungskräften und Experten beleuchten wir den sicheren Umgang mit KI-gestütztem Identitätsmanagement. Dabei soll die Herausforderung, diese Sicherheit innerhalb der Strukturen im Unternehmen zu wahren, ebenfalls beleuchtet werden.

KI-Systeme verfügen bereits häufig über substanzielle Zugriffe, oft mit Privilegien, die niemand explizit zugewiesen hat. Diese lösen Aktivitäten aus, welche im Umkehrschluss nur schwer von den Sicherheitsteams zuzuordnen sind, indem sie sich nicht wie Menschen verhalten und teils unvollständige oder lediglich temporäre Spuren hinterlassen. Für sich genommen ist das im ersten Step nicht tragisch, jedoch erschwert es die Beantwortung der Grundfragen, auf die Security-Teams angewiesen sind: „Wer hat welche Aktion initiiert?“ und „war diese Aktion überhaupt erlaubt gewesen?“

Nicht wenige Führungsteams sind zunehmend beunruhigt, wenn KI bereits Kundendaten liest, darüber hinaus Konfigurationen ändert, APIs aufruft und Aktionen verkettet – auf eine Art und Weise, welche sich nicht eindeutig einer verantwortlichen Person zuordnen lässt. KI-Identitäten verhalten sich weder wie menschliche Nutzer noch wie klassische Service Accounts.

Aus diesem Grund sehen Security-Verantwortliche die klare Herausforderung: Sie brauchen praktikable Sichtbarkeit, möchten verstehen, wie Systeme operieren, und suchen nach realistischen Wegen, um Privilegien am unkontrollierten Wachstum zu hindern.

*In diesem Bericht bezieht sich “KI” oder “KI-Identitäten” auf GenAI- oder LLM-Entitäten, einschließlich Copiloten, Agenten und LLM-basierte Apps.

Der nachfolgende Report beschäftigt sich mit den Herausforderungen für Security Teams im Umgang mit KI und sicherem Identitätsmanagement. Denn KI ist generell produktiv aktiv, jedoch können nur die wenigsten Organisationen transparent aufzeigen, wie weit deren Zugriff reicht — oder warum sie ihn überhaupt haben.

WICHTIGSTE ERKENNTNISSE (DE-SURVEY, N=100)

- **Zugang zu Kernsystemen:** 93 % der deutschen Großunternehmen geben an, dass KI-Identitäten bereits Zugriff auf kritische Geschäftssysteme wie SAP, Salesforce oder ServiceNow haben.
- **Doch nur ein Viertel dieser Organisationen steuert diese Zugriffe mit starker Governance.** Der Rest arbeitet mit teilweisen Kontrollen, Pilotansätzen – oder ohne klare Richtlinien.
- **Sichtbarkeit:** 58% haben keine vollständige Sichtbarkeit über alle KI-Identitäten (42% „vollständige Sichtbarkeit“, 49% „teilweise“, 9% „gering“).
- **Besorgnis um Zugriffe:** 66% sind besorgt (davon 16% „sehr“, 50% „etwas“).
- **Governance-Parität:** Nur 8% steuern > 75% ihrer KI-Besorgnis über KI-Identitäten mit der gleichen Strenge wie menschliche Identitäten; 39% erreichen 50–75%, der Durchschnitt liegt bei 57,8%.
- **Unbeabsichtigtes Verhalten & Vorfälle:** 40% sahen unbeabsichtigtes/unerlaubtes Verhalten durch KI; 40% berichten von einem Incident oder Near-Miss in den letzten 12 Monaten.
- **Shadow AI:** 76% haben unsanktionierte KI-Tools identifiziert (davon 29% signifikant).
- **Aktuelle Tools:** 56% nutzen GenAI-spezifische Access-Monitoring-Tools und SSO/MFA, 49% ISPM, 48% IGA, 46% PAM.
- **Verantwortung:** Primär CIO/IT (72%) statt CISO/Security (19%) verantwortet KI-Identitäten.
- **Kompetenz zur Eindämmung:** 89% sind zuversichtlich, Missbrauch kompromittierter KI zu erkennen und zu enthalten (davon 47% „sehr“).

KI-Identitäten bewegen sich schneller als Sicherheit

KI-Agenten handeln schneller, autonomer und mit größerem Wirkungskreis, als klassische Sicherheitskontrollen je vorgesehen haben.

Zwei Drittel der befragten CISOs äußern konkrete Sorge über KI-Zugriffe. Gleichzeitig berichten 40 % von unerwünschtem Verhalten oder sicherheitsrelevanten Vorfällen innerhalb von nur zwölf Monaten.

Das Kernproblem ist nicht KI – sondern unkontrollierter Zugriff. Breite API-Scopes, permanente Privilegien und fehlende Attribution machen KI-Identitäten zu Hochrisiko-Akteuren.

66%

der CISOs sind besorgt über den KI-Zugang

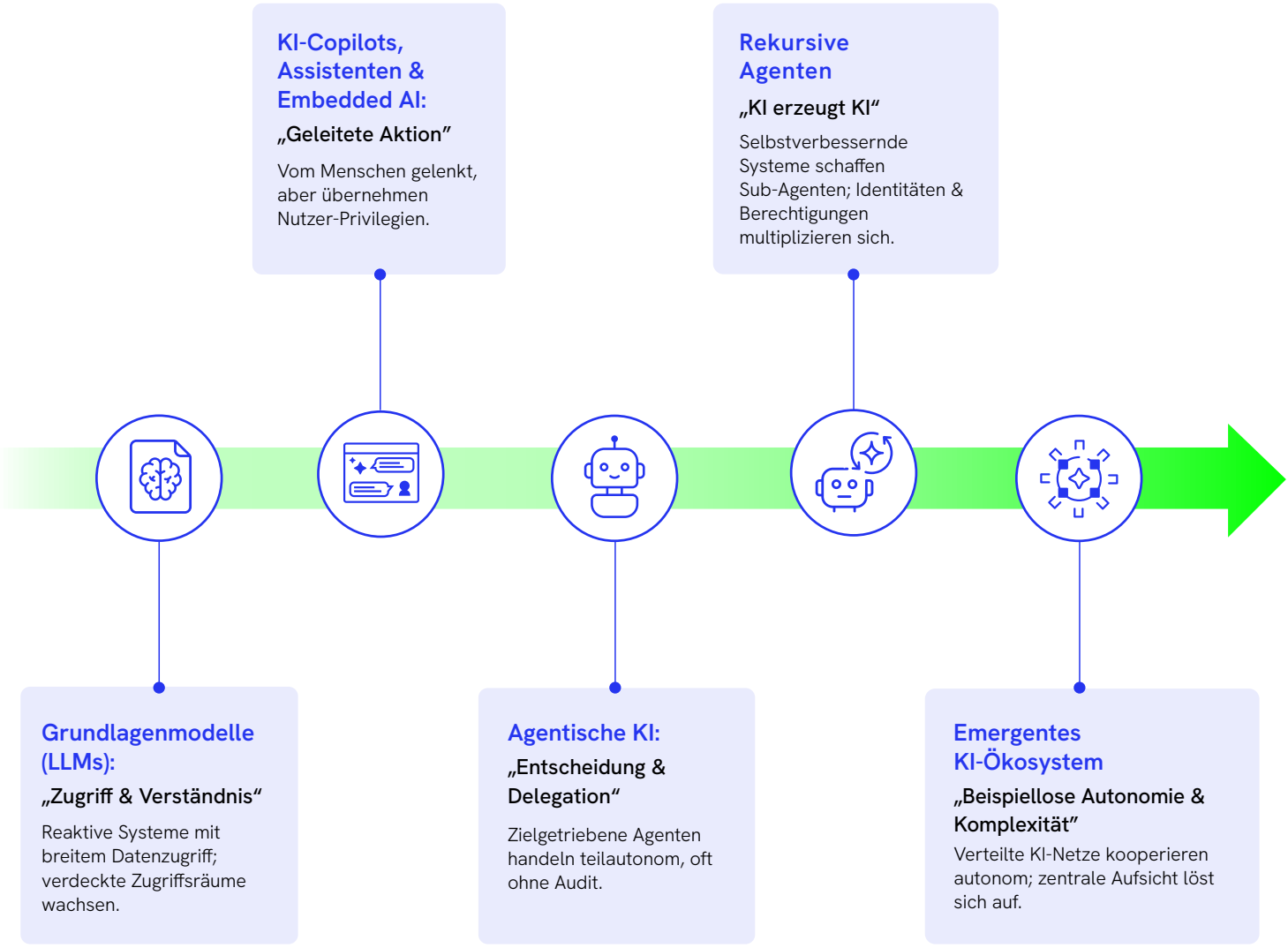
Konsequenz: Jede KI-Integration ist eine eigene Identität, die wie ein Hochrisiko-Nutzer für Governance ist — einschließlich des Admins: (Wer überwacht den Administrator?).

Aktionsempfehlung: KI-Identitäten neu denken.

Sie verhalten sich nicht wie Menschen oder klassische Maschinenkonten. Erforderlich ist ein Paradigmenwechsel: kontinuierliche Validierung von Intention, Privilegien und Verhalten mit Kontext und Rigorosität.

Die Evolution autonomer KI-Identitäten

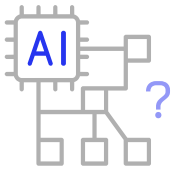
Jeder KI-Identitätstyp erfordert unterschiedliche Governance-Ansätze; der gemeinsame Nenner ist:
Sie operieren schneller und autonomer, als traditionelle Identitätskontrollen ausgelegt sind.



Die Sichtbarkeitskrise: Man kann nicht sichern, was man nicht sieht

Vor Kontrolle steht Transparenz. 58% haben keine vollständige Sichtbarkeit über KI-Identitäten; 95% in klassischen Berichten bezweifeln oft die Erkennungsfähigkeit. Befragte zeigen dagegen hohe Zuversicht (89%), aber Fragmentierung bleibt: KI agiert über SaaS, APIs und Workloads hinweg, oft ohne klaren Owner.

Ein architektonischer Grund: Traditionelles IAM ist auf Menschen ausgelegt (Login-Events, Workflows, statische Rollen). Es trackt nicht zuverlässig Systeme, die eigene Accounts erstellen, autonom handeln oder Privilegien eskalieren. Zudem sind KI-Workflows nicht-deterministisch, was Baseline-Verhalten erschwert.



Die meisten Teams haben keine vollständige Sichtbarkeit, was KI wo macht.

Investitionsprioritäten (wenn Budget kein Thema):

76%
AI-Analytics & Anomalie-Erkennung

46%
API- & Workload-Identity Discovery/Inventory

39%
Kontinuierliches Monitoring & Posture Analytics

47%
Unified Identity-Plattform

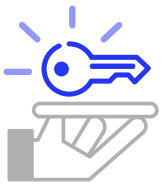
Aktionsempfehlung: Das vollständige Bild erzeugen.

Auffinden, identifizieren, klassifizieren aller Identitäten — mit klarer Trennung von KI vs. Mensch und Typisierung (LLMs, Agenten, Bots). App-lokal klassifizieren, nicht nur systemweit: Shadow AI verbreitet sich schnell; fehlende App/Identität kann Problemketten auslösen. Danach: Continuous Discovery und proaktives Posture-Management.

KI-Governance ist das schwächste Glied

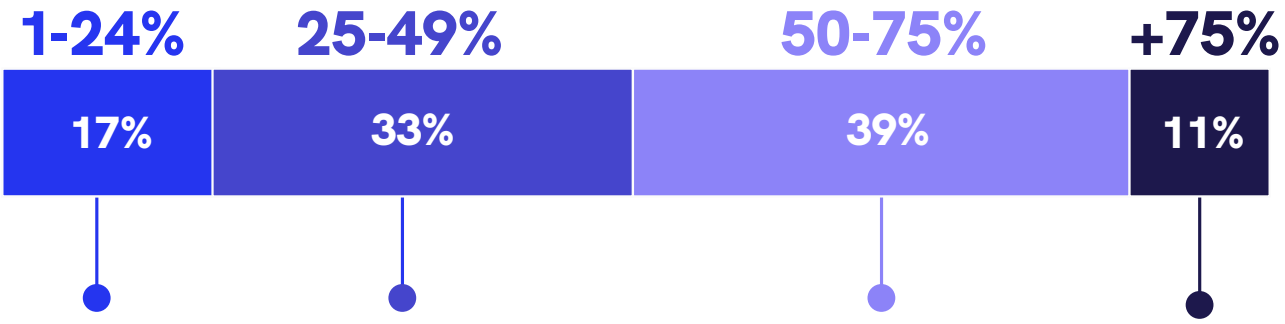
KI-Tools handeln mit echter Autorität und Privilegien, aber oft ohne belastbare Governance: Nur 8% steuern > 75% ihrer KI-Identitäten wie Menschen; 39% liegen bei 50–75%. Viele KI-Konten werden nicht durch strukturierte Workflows provisioniert, zertifiziert oder de-provisioniert.

Teams beginnen, KI in bestehende Governance-Modelle zu bringen — Lifecycle-Kontrollen als Baseline. Doch Parität ist nur ein Startpunkt: KI handelt autonom, systemübergreifend, im Auftrag von Nutzern oder anderen Agenten. Wenn eine KI eine andere KI aufruft, wird Attribution unklar, Privileggrenzen verschwimmen. Notwendig sind Kontrollen für Autonomie und Policies für Delegation, Eskalationspfade und Maschinen-Geschwindigkeit.



Privilegien ohne Richtlinien werden zum Normalfall.

Prozentualer Anteil der geschäftskritischen Anwendungen, die durch Identitätssicherheitsprogramme verwaltet werden:



17% gaben an, dass 1% bis 24% durch Identitäts-sicherheitsprogramme verwaltet werden

33% gaben an, dass es bei ihnen 25% bis 49% sind

39% gaben an 50% to 75% steuern zu lassen und

11% nannten mehr als 75% ihrer geschäftskritischen Anwendungen.

Aktionsempfehlung: Reale Nutzung verstehen.

Welche Apps berührt KI bereits, warum wurde sie eingeführt, wer hat sie integriert? Daraus ergeben sich Regeln & Guardrails pro Identität. Governance muss Least-Privilege durchsetzen und nur erforderlichen Zugriff erlauben. Ziel: einheitliche Lifecycle-, Least-Privilege- und Zertifizierungs-Kontrollen für menschliche und KI-Identitäten.

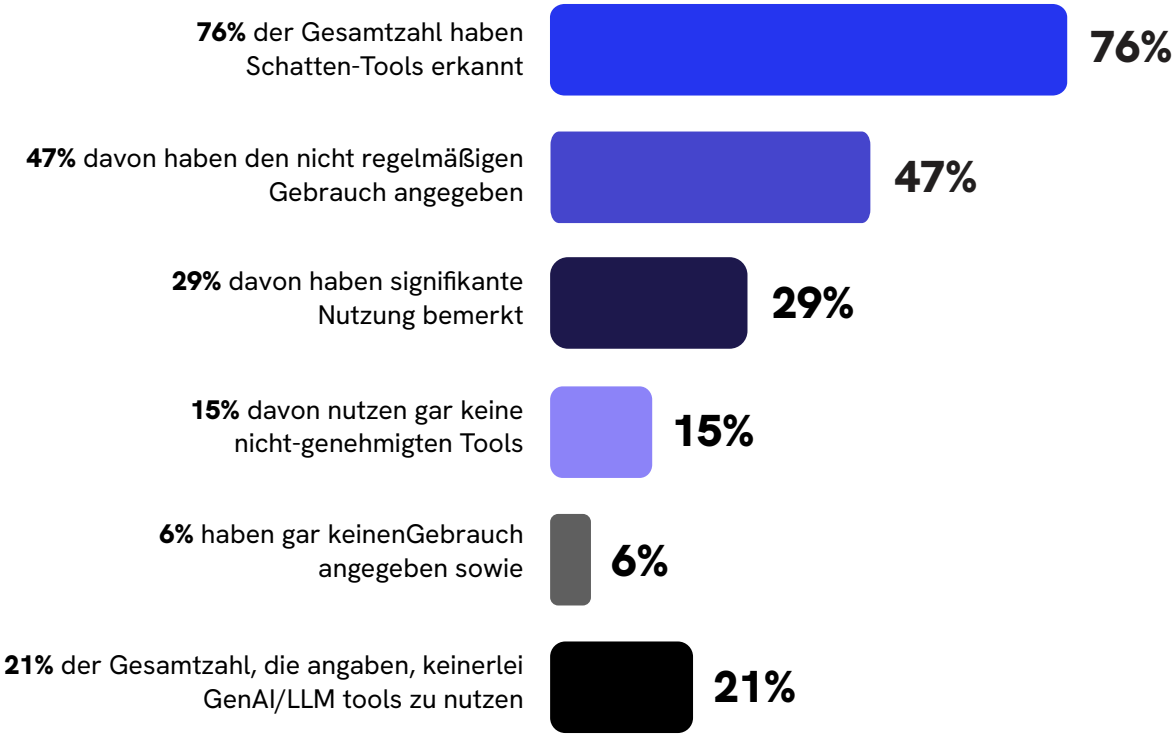
Shadow AI ist bereits im System

KI wird nicht nur über IT-Projekte ausgerollt. Unsanktionierte Tools werden eigenständig eingebracht: 76% haben Shadow AI entdeckt (29% signifikant, 47% „einige“).
Diese Tools sind nicht auf Browser-Assistenten beschränkt: eingebettete Credentials, API-Integrationen oder OAuth-Tokens verbinden sich direkt mit Unternehmenssystemen — häufig mit erhöhten Berechtigungen, außerhalb standardisierter Provisioning-Workflows. Jede KI-Tool-Einführung schafft zudem eine Vertrauensbeziehung zu einem externen Anbieter, dessen Security & Data Handling außerhalb eurer Kontrolle liegt.

Security-Teams behandeln Shadow AI zunehmend wie unmanaged identities: Scannen nach unbekannten Konten/Tokens, Inventarisieren, Policies nachziehen. Faktisch ist KI jedoch tief eingebettet und verbreitet sich schneller, als aktuelle Kontrollen nachziehen können.

Nicht genehmigte KI-Tools breiten sich aus.

Gebrauch von Shadow- oder nicht-genehmigten GenAI/LLM-Tools, die innerhalb der Organisation identifiziert wurden:



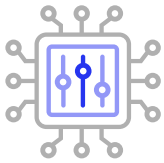
Aktionsempfehlung: Stakeholder beim Einführen von KI unterstützen.

Nutzer werden KI verwenden — ob genehmigt oder nicht. Es ist zentral, einen klaren, sicheren Onboarding-Pfad zu bieten, inklusive eines kleinen Governance-Gremiums und einfacher Review-Prozesse. Access-Scope, Credentials und Datenexposition müssen pro Tool evaluiert werden. So verwaltet man das Risiko, bevor es systemweit streut.

CISOs können sich nicht mehr auf Legacy-Tools verlassen

Viele Organisationen managen KI-Risiko mit Tools einer vergangenen Ära, gebaut für On-Prem, menschliche Nutzer und statischen Zugriff. AI-Identitäten benötigen API-first-Kontrollen: Token-Lifecycle, Scope-limitierte Autorisierung und Runtime-Enforcement.
Zwar nutzen 56% bereits GenAI-spezifisches Monitoring, dennoch bleibt die Praxis oft manuell: Agenten agieren in Maschinen-Geschwindigkeit, während Enforcement punktuell erfolgt. Das Ergebnis: Fragmentierte Punktlösungen für Access, Privileg, Governance — mit Lücken in Sichtbarkeit, Policy-Alignment und Reaktionszeit.

Zur Schließung der Lücken werden Identity-Daten (Access Logs, Privileg-Nutzung, Konto-Verhalten) in eine einheitliche Kontextebene gezogen. Heute sind diese Daten oft über nicht integrierte Tools verstreut — bis das Gesamtbild steht, ist die KI-Identität weitergezogen. Investitionswünsche (wenn Budget frei ist) sind AI-Analytics (76%), Unified Identity-Plattform (47%), API/Workload-Discovery (46%) und Posture Monitoring (39%).



Nur
1 von 2
Organisation überwacht KI gezielt oder kontrolliert deren Einsatz.

Investitionen mit höchster Priorität zur Sicherung von GenAI-/LLM-Identitäten (falls Budget vorhanden ist):

76%
priorisieren Anwendungen zur KI-gesteuerten Analyse und automatisierten Abwehr

47%
sehen höchste Priorität in der Einführung eines einheitlichen Plattformansatzes zur Identitätssicherheit

36%
angesichts automatisiertem Lifecyclemanagement und Governance

15%
bei Anmelde- und Passwort-Rotation bzw. sicherer Speicherung

1%
priorisieren anderweitige Investitionen

46%
legen ihren Fokus auf die Erkennung und Inventarisierung von API und Workload Identity

39%
in der kontinuierlichen Überwachung und nachgelagerten Analyse

Aktionsempfehlung: Ehrlich inventarisieren und modernisieren.

Zu viele Punktlösungen schaffen Komplexität, die gerade noch mit menschlichen Nutzern mithält und KI macht die Risse unübersehbar. Man sollte den Moment zur Neuaufstellung nutzen: Legacy-IGA abschalten, Konvergenz von IGA, PAM, ISPM/Access Analytics in eine Plattform (31% streben dies bereits an).

Der Weg nach vorn: Identität schafft Durchsetzungsvermögen

Perimeter-Kontrollen folgen KI nicht in Cloud-Plattformen, Geräte-Policies gelten nicht für Headless-Agenten. Identität bleibt die konstante Enforcement-Schicht, in der Zugriffsentscheidungen, Privileggrenzen und Audit Trails zusammenlaufen.

Security-Teams priorisieren entsprechend: Identity Discovery & Inventory (API/Workload) sowie kontinuierliches Monitoring & Posture Analytics und AI-getriebene Erkennung. Der gemeinsame Nenner: Automatisierung und Kontrollen, die sich so schnell bewegen, wie die Identitäten, die sie steuern sollen.

In fortgeschrittenen Umgebungen werden Investitionen operationalisiert: automatisierte De-Provisionierung von inaktiven KI-Service-Accounts, Just-in-Time Privileg-Elevation mit Zeitbegrenzung, Policy-basierte Revocation bei Risikogrenzen, Self-Healing-Workflows zur Least-Privilege-Restaurierung. Ziel: Zeit von Detection zu Action verkürzen, solange jede neue Identität noch kontrollierbar ist.

Wenn traditionelle Grenzen verschwimmen, wird Identität zur ersten Kontrollinstanz.

Aktionsempfehlung: Identity-First vorbereiten.

Mit Sichtbarkeit beginnen: Discovery, Identifikation, Klassifikation im gesamten Ökosystem. Auf dieser Baseline erkennt man größte Lücken (fehlende Systeme, unmanaged Privileged Users, inkonsistente Governance) und geht High-Risk zuerst an. Identität wird konstanter Enforcement-Punkt für KI: Wer (oder was) handelt, mit welchen Privilegien, wie lange?

Zwei Dinge müssen immer mitgedacht werden: „Wer überwacht KI, die zur Sicherheit genutzt wird?“ und „Wer überwacht den Administrator?“.

Wie CISOs auf das KI-Risiko reagieren

	HERAUSFORDERUNG	WAS CISOS BEGINNEN ZU TUN	WARUM ES ZÄHLT
1	**KI-Agenten bewegen sich schneller als Kontrollen**	Automatisierte Lifecycle-Governance zur Provisionierung, Rezertifizierung, Revocation nach Plan; Agenten wie Hochrisiko-Nutzer behandeln.	40% beobachteten unerwünschtes Verhalten; 40% Incidents/Near-Misses. Reaktive Kontrollen reichen nicht für autonome Systeme.
2	**Begrenzte Sichtbarkeit**	Identity-Inventare (46% geplante Priorität) und Continuous Monitoring (39%) — Wechsel von periodischen Audits zu Realtime-Telemetry über KI-Aktionen.	58% haben keine vollständige Sichtbarkeit; man kann nicht governancen, was man nicht sieht.
3	**Governance-Lücken**	IGA-Workflows auf KI anwenden: Provisioning, Access Reviews, De-Provisioning für bisher außerhalb der Policies agierende Agenten.	Nur 8% haben > 75% Parität; strukturiertes Governance-Onboarding reduziert Exposure direkt.
4	**Shadow AI**	Scans für unsanktionierte Tools & Credentials; Onboarding der gefundenen KI-Identitäten in zentrale Steuerung, statt Adoption zu blockieren.	76% fanden Shadow AI; Ziel ist Sichtbarkeit & Kontrolle nachträglich, nicht Prävention um jeden Preis.
5	**Fragmentierte Identity-Tooling**	Konvergenz zu Unified Identity-Plattformen (IGA, PAM, ISPM/Analytics) — 31% bewegen sich dorthin.	Fragmentierung erschwert Antworten wie „Wem gehört das?“ oder „Sollte dieser Zugriff existieren?“ in Echtzeit.

Schlussfolgerung

Digitale Transformation, Zero Trust und Compliance prägen Unternehmen seit Jahren. KI hat den Cybersecurity-Status quo jedoch fundamental verändert: autonome Agenten, LLMs und MCP-Server müssen nahtlos mit Menschen zusammenarbeiten.

KI-Identitäten sind heute faktisch privilegierte Nutzer – aber ohne die Governance, die wir für Menschen längst als selbstverständlich betrachten.

Dieser Report zeigt: Die KI-Ära braucht einen anderen Sicherheitsansatz. Traditionelle Tools und Prozesse halten nicht Schritt — Organisationen benötigen ein System, das so schnell evolviert und skaliert wie KI. KI-Identitäten besitzen bereits bedenkliche Zugriffe, oft privilegiert, während vielerorts Leitplanken fehlen.

Die KI-Ära zwingt Unternehmen, Identity Security neu zu denken.

Wer heute nicht weiß, welche KI-Identitäten mit welchen Privilegien handeln, verliert unabhängig von Cloud, Zero Trust oder Compliance-Frameworks die Kontrolle.

Identity Security, korrekt umgesetzt, wird zur einzigen Schicht, die konsistente Durchsetzung über KI-Identitäten und Systeme umgebungsübergreifend liefert.
Unternehmen, die früh ihre Identity-Security-Posture evaluieren, Lücken identifizieren und den Weg zu intelligenter, vereinheitlichter Identity Security beschleunigen, sichern sich Wettbewerbsvorteile und können KI sicher nutzen und als Wachstumshebel einsetzen. Dieser Shift passiert jetzt — gerade rechtzeitig.

Was mit neuer Identity-Intelligence & Automatisierung möglich ist:

Automatisierte De-Provisionierung inaktiver KI-Service-Konten	Just-in-time Privileg-Elevation mit zeitlichem Limit	Policy-basierte Entziehung bei Risikogrenz-Verletzung	Self-Healing-Workflows zur Least- Privilege-Wiederherstellung

Diese Kontrollen müssen KI-Geschwindigkeit erreichen und den Loop zwischen Detection–Decision–Action schließen.

Methodik & Demografie (DE)

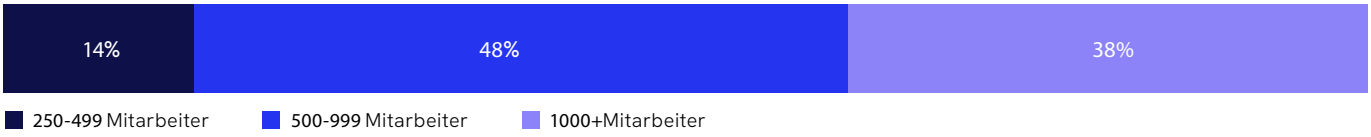
Die Umfrage wurde als Online-Erhebung im CAWI-Verfahren (Computer Assisted Web Interviewing) durchgeführt. Die Feldzeit erstreckte sich vom 21. bis 31. Oktober 2025. Befragt wurden ausschließlich CISOs und CIOs in deutschen Großunternehmen mit mindestens 250 Mitarbeitenden. Die Auswahl der Teilnehmenden erfolgte über eine zufällige 1-in-n-Selektion aus einem Panel. Im Originalprojekt wurde ein UK-Panel genutzt; die hier dargestellten Ergebnisse beziehen sich auf das deutsche Subset (n=100). Routing-Informationen sind dokumentiert und geben an, welche Teilgruppen welche Fragen beantwortet haben. Die Basisgröße (base n) ist für jede Frage separat ausgewiesen.

Gewichtung: Wo erforderlich, wurden die Daten von OnePoll nach den ONS Mid-Year Estimates gewichtet.

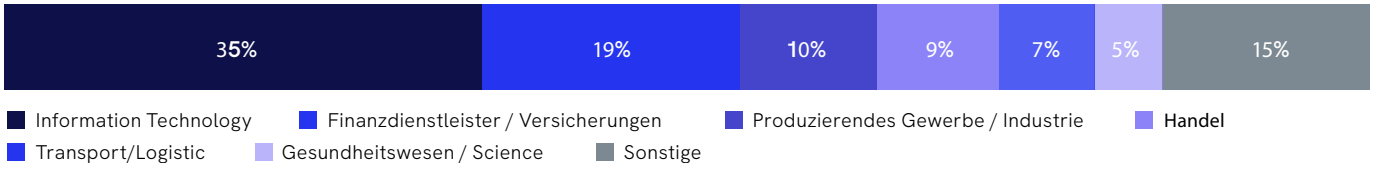
Hinweis: Für Erhebungen mit Teilnehmenden, die sich nicht binär identifizieren, wird deren Anteil gemäß Rohdaten berücksichtigt; die männlichen und weiblichen Gruppen werden entsprechend angepasst.

PRIMÄRE BERUFLICHE FUNKTION

UNTERNEHMENSGRÖßE



BRANCHE



Über Saviynt

Saviynt bietet eine KI-gestützte Identity-Plattform, die den Zugriff von menschlichen und nicht-menschlichen Identitäten auf Unternehmensanwendungen, Daten und Geschäftsprozesse verwaltet und steuert. Als anerkannter Marktführer im Bereich Identity Security hilft Saviynt Organisationen, Risiken zu reduzieren, Compliance zu vereinfachen und KI- sowie Cloud-Technologien sicher einzusetzen. Zu den Kunden zählen Fortune-500-Unternehmen, Regierungsorganisationen und führende globale Marken. Mehr Informationen: **www.saviynt.com.**