Keeper Security Infobericht

Identitätssicherheit in Maschinengeschwindigkeit

Mai 2026

Überblick

Identität ist heute die Grundlage für die Funktionsweise moderner Unternehmen. Es regelt den Zugriff der Mitarbeiter, die Interaktion mit Maschinen, Dienstkonten, Automatisierungs-Workflows und KI-gesteuerte Prozesse in Cloud- und Hybridumgebungen. Was einst eine verzeichnisbasierte Funktion war, hat sich zu einer operativen Infrastruktur mit einer immer größer werdenden Cyber-Angriffsoberfläche entwickelt.

Da sich Identitätsökosysteme auf menschliche und nicht-menschliche Identitäten (NHIs) ausweiten, muss sich die Governance auf ein breiteres und dynamischeres Spektrum erstrecken. Fast 89 % der leitenden IT-Manager berichten, dass die Verwaltung dieser wachsenden Identitätslandschaft eine Herausforderung darstellt, was den Umfang und die Komplexität moderner IT-Umgebungen widerspiegelt. Gleichzeitig ist die Identitätsautorität oft über verschiedene Systeme verteilt, wobei 96 % der Befragten unzusammenhängende oder schlecht integrierte Sicherheitstools als Ursache für ausnutzbare Sicherheitslücken nennen. Dies unterstreicht die Notwendigkeit einer Überwachung, um eine einheitliche Durchsetzung zu gewährleisten.

Diese Erweiterung überschneidet sich direkt mit der Überwachung. In Umgebungen, in denen die Automatisierung kontinuierlich abläuft und Identitäten mit Maschinengeschwindigkeit arbeiten, gewinnt die Echtzeit-Transparenz zunehmend an Bedeutung. Dennoch berichten 72 % der Organisationen, dass der Missbrauch von Zugangsdaten nicht in Echtzeit erkannt wird. Die meisten stellen einen unberechtigten privilegierten Zugriff erst nach Stunden statt Minuten fest – wenn nicht sogar nach Tagen, Wochen, Monaten oder Jahren.

Die von Keeper Security durchgeführte Studie, an der 3.200 Entscheidungsträger im Bereich Cybersicherheit und leitende IT-Führungskräfte in Nordamerika, Europa, dem asiatisch-pazifischen Raum und dem Nahen Osten teilnahmen, untersucht, wie sich Unternehmen an diese Infrastrukturveränderungen anpassen. Es analysiert, wie sich Identitäten ausweiten, wie der Zugriff team- und systemübergreifend verwaltet wird, wie privilegierte Zugriffe geregelt werden und wie effektiv Organisationen Bedrohungen in Umgebungen erkennen und darauf reagieren, in denen Aktivitäten zunehmend in Maschinengeschwindigkeit ablaufen. Zusammengenommen liefern die Ergebnisse einen Überblick über den aktuellen Stand der Identitätsgovernance im großen Maßstab und die strukturellen Kräfte, die die Unternehmenssicherheit im Jahr 2026 prägen.

89%
empfinden die Bewältigung des Identitätswachstums als Herausforderung

96%
geben an, dass nicht miteinander verknüpfte Tools Sicherheitslücken schaffen

72%
können den Missbrauch von Zugangsdaten nicht in Echtzeit erkennen

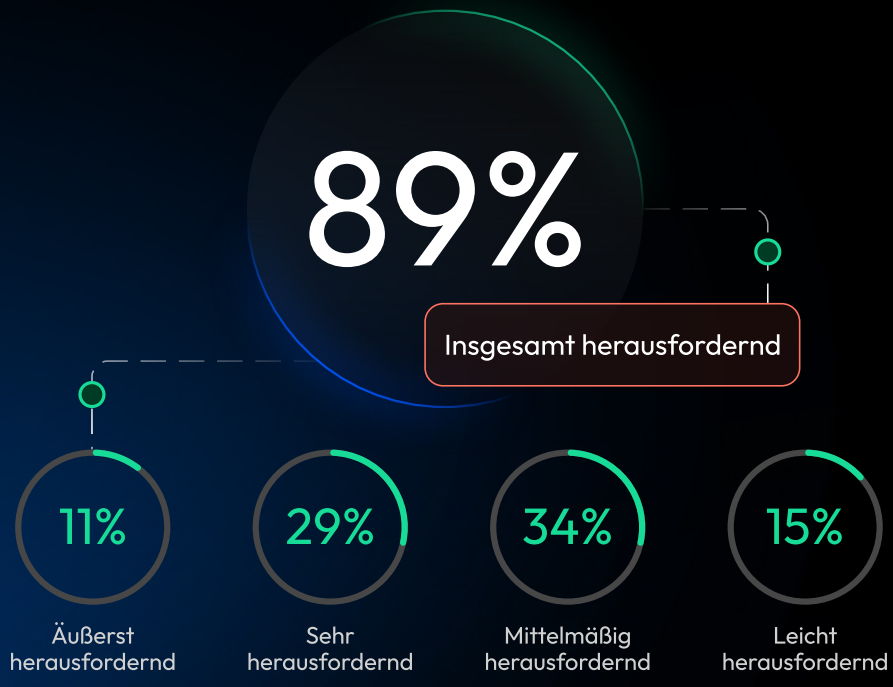
Identität ist jetzt Unternehmensinfrastruktur

Identität ist nicht mehr nur eine Benutzerauthentifizierungsfunktion. Es handelt sich um die operative Ebene, über die moderne Unternehmen ihre Tätigkeiten ausführen. Jede Mitarbeiteranmeldung, jede Zugriffsanfrage eines Auftragnehmers, jeder API-Aufruf, jedes Dienstkonto, jeder Automatisierungs-Workflow und jeder KI-gesteuerte Prozess ist auf Identitätsprüfungen zur Authentifizierung, Autorisierung und Aufzeichnung von Aktivitäten angewiesen.

Dieser Wandel vollzog sich zwar allmählich, seine Auswirkungen sind jedoch struktureller Natur. Die Identität vermittelt heute den Zugriff über Cloud-Plattformen, SaaS-Anwendungen, KI-Agenten, Entwicklungspipelines und Infrastrukturumgebungen hinweg. Es regelt nicht nur, wer Zugriff auf Systeme hat, sondern auch, wie Maschinen interagieren, wie Dienste Zugangsdaten austauschen und wie Automatisierung in großem Umfang abläuft. Das Ergebnis ist eine Zunahme sowohl des Umfangs als auch der Komplexität.

Eine deutliche Mehrheit der Organisationen (89 %) gibt an, dass die Verwaltung der wachsenden Anzahl von Identitäten in ihren Umgebungen eine Herausforderung darstellt, da diese Identitäten mittlerweile Mitarbeiter, Auftragnehmer, Dritte und NHIs wie Dienstkonten und maschinelle Zugangsdaten umfassen.

Das Wachstum ist nicht mehr ausschließlich an die Einarbeitungszyklen der Mitarbeiter gebunden. Jedes neue System, Automatisierungsskript oder jede Integration künstlicher Intelligenz (KI) führt zusätzliche Authentifizierungsereignisse, Zugangsdaten und Zugriffspfade ein. Identitätsökosysteme sind heutzutage eher kontinuierlich und voneinander abhängig als linear und diskret.



KI beschleunigt diese Entwicklung zusätzlich. Generative Copiloten, Orchestrierungs-Engines und KI-gesteuerte Analysesysteme interagieren direkt mit geschäftskritischen Infrastrukturen, indem sie sich authentifizieren, Daten abrufen und Befehle über definierte Zugangsdaten und Berechtigungen ausführen. Mit zunehmender Verbreitung von KI steigt auch die Anzahl der in Unternehmensumgebungen eingesetzten NHIs. Organisationen erkennen an, dass KI-bezogene Identitätsrisiken über das Verhalten von Mitarbeitern hinausgehen.

Die größten Lücken in der KI-bezogenen Identitätsverwaltung

56%
Mitarbeiter nutzen KI und geben versehentlich vertrauliche Informationen weiter

44%
Mangelnde Steuerung des KI-gestützten Zugangs und der Automatisierung

43%
KI-bezogene NHI-Verwaltung und -Sicherheit

42%
Mangelnde Transparenz hinsichtlich der von Mitarbeitern genutzten KI-Tools

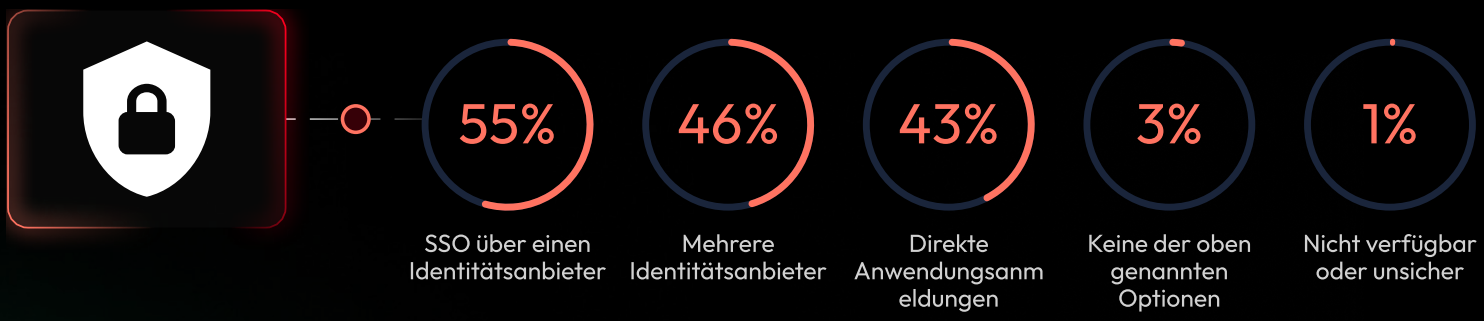
Während 56 % Bedenken hinsichtlich der unbeabsichtigten Offenlegung vertraulicher Informationen äußern, identifizieren mehr als vier von zehn Befragten Governance-spezifische Lücken, darunter die Aufsicht über KI-gesteuerte Zugriffe, die Verwaltung KI-bezogener NHIs und die Transparenz der Nutzung von KI-Tools. Dies deutet darauf hin, dass das mit KI verbundene Risiko nicht auf Benutzerfehler beschränkt ist. Es spiegelt die Notwendigkeit wider, die Identitätsverwaltung auf automatisierte und maschinengesteuerte Arbeitsabläufe auszudehnen, bei denen Berechtigungen, Sichtbarkeit und Aufsicht über menschliche und nicht-menschliche Identitäten hinweg konsistent funktionieren müssen.

Identität bildet heute die Grundlage eines hybriden Ökosystems aus menschlichen und maschinellen Identitäten, die gleichzeitig in einer verteilten Infrastruktur operieren. Mit der Erweiterung dieses Ökosystems muss die Governance über das Identitätsmanagement der Belegschaft hinaus auf ein umfassenderes, stärker integriertes Sicherheits- und Kontrollmodell ausgeweitet werden.

Die Sorge über den Missbrauch durch Mitarbeiter variiert je nach Region

67%	55%
64%	55%
62%	52%
56%	51%
56%	51%

Identitätssicherheit und-kontrolle sind fragmentiert



Mit der Zunahme des Identitätsvolumens hat sich auch die Autorität über Identitäten auf verschiedene Systeme ausgedehnt. Organisationen führen Identitätsanbieter, Cloud-Zugriffskontrollen und privilegierte Zugriffsplattformen im Laufe der Zeit ein, typischerweise als Reaktion auf unmittelbare betriebliche oder regulatorische Anforderungen. Diese Systeme existieren zwar im selben Umfeld nebeneinander, funktionieren aber nicht immer als eine einzige, einheitliche Steuerungsebene.

Die Verteilung ist in Authentifizierungsmustern sichtbar. Während 55 % der Befragten angeben, Single Sign-On (SSO) über einen Identitätsanbieter zu nutzen, betreiben 46 % mehrere Identitätsanbieter und 43 % erlauben immer noch direkte Anwendungsanmeldungen außerhalb einer zentralen Durchsetzung.

Diese Zahlen spiegeln ein Umfeld wider, in dem Identitätsentscheidungen nicht auf eine einzige Autorität beschränkt sind. Authentifizierung, Rechtevergabe und Sitzungsüberwachung können je nach Infrastrukturgrenzen von unterschiedlichen Systemen gesteuert werden. Richtlinien können zwar einheitlich definiert, aber uneinheitlich angewendet werden, und Protokollierung kann plattformübergreifend erfolgen, ohne dass sie von einer einheitlichen Datenquelle stammt.

Diese Dynamik wird durch die Wahrnehmung verstärkt: 96 % geben an, dass unzusammenhängende oder schlecht integrierte Sicherheitstools ausnutzbare Sicherheitslücken schaffen. Die Sorge gilt weniger dem Vorhandensein von Kontrollmechanismen als vielmehr deren Koordination. Wenn die Identitätsautorität verteilt ist, wird die Ausrichtung zu einer operativen Aufgabe und nicht mehr zu einer architektonischen Eigenschaft.

Da der Identität eine zentrale Rolle bei der Unternehmensführung zukommt, hat die Verteilung der Kontrolle weitreichendere Konsequenzen. Sicherheit und Governance hängen nicht nur von der Leistungsfähigkeit einzelner Systeme ab, sondern auch davon, wie kohärent diese Systeme zusammenarbeiten.

Privilegienerweiterung ohne vollständige Reife

Privileged Access Management (PAM) Bereitstellungsstatus

Mit der zunehmenden Verteilung der Identitätsautorität entwickelt sich das Privileg zu einem entscheidenden Kontrollpunkt. Privilegierter Zugriff ist nicht länger auf eine kleine Anzahl administrativer Konten beschränkt. Dies erstreckt sich nun auch auf Automatisierungspipelines, Serviceidentitäten und maschinengesteuerte Arbeitsabläufe, bei denen für routinemäßige operative Aufgaben häufig erhöhte Berechtigungen erforderlich sind. Cloud-native Infrastrukturen benötigen definierte Zugriffsrollen, um zu funktionieren, und KI-gestützte Systeme interagieren direkt mit empfindlichen Datensätzen und Produktionsumgebungen. Mit zunehmender Größe dieser Interaktionen ist die Unterscheidung zwischen operativer und privilegierter Identität weniger deutlich geworden.

Die Einführung von Privileged Access Management (PAM) spiegelt die Anerkennung dieses Wandels wider, allerdings ist der Reifegrad der Implementierung unterschiedlich. Weltweit geben 36 % an, dass PAM vollständig implementiert ist, während 31 % eine teilweise Bereitstellung angeben und 16 % über die aktive Implementierung berichten. Tatsächlich arbeiten 64 % noch nicht mit einer vollständig konsolidierten Verwaltung privilegierter Zugriffe.

Die Privilegienerweiterung schreitet voran, da neue Systeme online gehen, die API-Integration zunimmt, die Anzahl der NHIs steigt und die Cloud-Rollen sich in den verschiedenen Umgebungen vervielfachen. Wo privilegierte Arbeitsabläufe teilweise zentralisiert bleiben, können Sichtbarkeit und Durchsetzung zwischen den Systemen unterschiedlich sein, was die Struktur der zugrunde liegenden Architektur widerspiegelt.

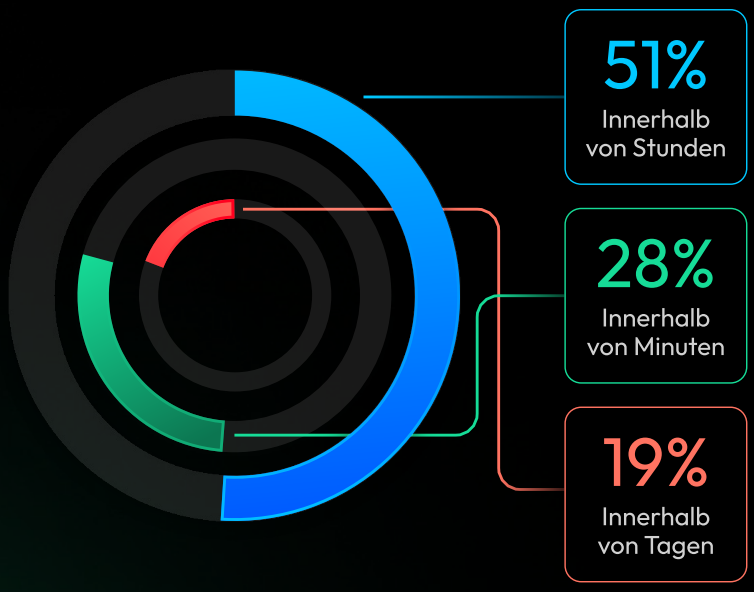
Es geht nicht um die Bedeutung von Privilegien, die allgemein anerkannt ist. Es geht um die Konstanz der Kontrolle über privilegierte Zugriffsrechte. Bei zentraler Steuerung gewährleisten Privilegien die Nachvollziehbarkeit und die Ausrichtung an den Unternehmensrichtlinien. Wenn Autorität ohne einheitliche Aufsicht verteilt wird, werden Messung und Management komplexer. Da Identität eine infrastrukturelle Rolle einnimmt, wird Berechtigung zu ihrer sensibelsten Ebene, und die Reife der Governance bestimmt, ob diese Ebene im gesamten Unternehmen vorhersehbar funktioniert oder je nach Systemgrenzen variiert.

Die Erkennung arbeitet in einem anderen Tempo

Da Identität zu einer unternehmensweiten Infrastruktur wird und sich Berechtigungen über verschiedene Umgebungen ausdehnen, wandelt sich die Überwachung von einer unterstützenden zu einer bestimmenden Funktion. Die Erkennung verläuft jedoch nicht immer im gleichen Tempo wie die Ausführung. Fast drei Viertel (72 %) der Organisationen können den Missbrauch von Zugangsdaten nicht in Echtzeit erkennen; die meisten stellen einen unberechtigten privilegierten Zugriff erst nach Stunden statt nach Minuten fest.

Die Erkennungsgeschwindigkeit wird weniger von der Absicht als vielmehr von der Architektur bestimmt. Wenn Identitätssicherheit und Berechtigungsdurchsetzung auf verschiedene Systeme verteilt sind, hängt die Überwachung davon ab, Signale miteinander zu verknüpfen, anstatt die Aktivitäten durch eine einheitliche Linse zu betrachten. Die Protokollaggregation, Sitzungsaufzeichnung und plattformübergreifende Analysen führen zu Verzögerungen, die eher auf strukturelle Gestaltung als auf operative Aufsicht zurückzuführen sind.

Zeit zur Erkennung von Zugangsdatenmissbrauch

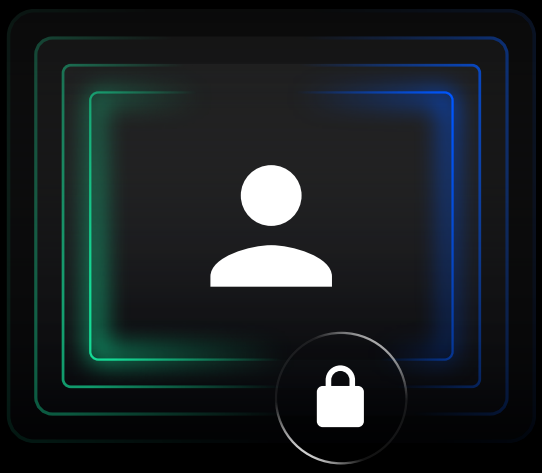


Dieser Effekt verstärkt sich mit zunehmender Automatisierung. Authentifizierungsereignisse treten kontinuierlich auf, Dienstkonten erzeugen nicht-menschliche Aktivitätsmuster und privilegierte Arbeitsabläufe erstrecken sich auf CI/CD-Pipelines und Cloud-native Dienste. In solchen Umgebungen wird die Fähigkeit, Aktivitäten in Echtzeit zu erkennen, dadurch bestimmt, wie kohärent Identitätsmanagement, Rechtedurchsetzung und Überwachung zusammenarbeiten.

Das Erkennungstempo dient als praktischer Indikator für die Integration. Je mehr Identitätsfunktionen als einheitliche Steuerungsebene fungieren, desto genauer kann die Überwachung mit der Ausführungsgeschwindigkeit abgestimmt werden.

Identitätssicherheit in großem Umfang

Da Identitätsökosysteme mittlerweile auch Menschen und Maschinen umfassen, die parallel agieren, hat sich die Governance auf mehrere Systeme ausgedehnt. Authentifizierung, Durchsetzung von Berechtigungen und Überwachung wurden in verschiedenen Phasen des Infrastrukturwachstums eingeführt, oft um konkrete Probleme zu lösen. Im Laufe der Zeit hat dies zu einem verteilten Autoritätsmodell geführt, anstatt zu einer einzigen, konsolidierten Cybersicherheits-Kontrollebene.



Berechtigungen sind nun in Automatisierungspipelines, Serviceidentitäten und KI-gestützten Workflows integriert und verringern so die Unterscheidung zwischen operativem und erhöhtem Zugriff. Die Überwachungsfähigkeit spiegelt diese Struktur wider. Wo Identitätsgovernance integriert ist, können Aktivitäten mit minimaler Verzögerung ausgewertet werden. Wo die Steuerung dezentralisiert bleibt, spiegelt die Reaktionszeit den erforderlichen Koordinierungsaufwand zwischen den Systemen wider.

Die Identitätsverwaltung hat sich von einer verzeichnisbasierten Funktion zu einer operativen Infrastruktur entwickelt. Es ist kontinuierlich und nicht episodisch, und seine Autorität ist nicht mehr standardmäßig zentralisiert. Die Reife der Governance wird zunehmend durch Kohärenz definiert – wie konsistent Authentifizierung, Berechtigungen und Überwachung in verschiedenen Umgebungen zusammenarbeiten.

Über Keeper Security

Keeper Security ist der weltweit führende Anbieter für Zero-Trust- und Zero-Knowledge-Identitätssicherheit und schützt Passwörter, Passkeys, Secrets, Endpunkte sowie privilegierte Zugänge für Tausende von Organisationen und Millionen von Nutzern weltweit. Um mehr zu erfahren, besuchen Sie **Keepersecurity.com** oder kontaktieren Sie uns unter **communications@keepersecurity.com**.

Methodik

The research was conducted by Censuswide in 2026, among a sample of 3,200 professionals who are cybersecurity decision makers/managers+ and who work in IT Security, Executive Leadership or DevOps (500 respondents in the UK, US, France, Germany, Japan, APAC (Australia, India, New Zealand, China) and 200 in the Middle East). Censuswide is a member of the Market Research Society (MRS) and the British Polling Council (BPC), and a signatory of the Global Data Quality Pledge.