Vorbereitet für

KEEPER

Jenseits des Tresors:
Optimierung des Privileged Access Managements in modernen Unternehmen

Juli 2025 EMA Whitepaper
von **Ken Buckler, CASP;** Forschungsdirektor
Informationssicherheit, Risiko- und Compliance-Management

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Inhaltsverzeichnis

Einleitung

In einer Ära unerbittlicher Cyberbedrohungen und schneller digitaler Transformation hat sich das Privileged Access Management (PAM) zu einer grundlegenden Sicherheitsdisziplin entwickelt. Die Unternehmen von heute verlangen mehr als nur die Speicherung von Anmeldeinformationen in Tresoren. Sie benötigen ein umfassendes Framework, das kritische Assets schützt, den Zugriff mit den geringsten Rechten durchsetzt und sich nahtlos in lokale und Cloud-Umgebungen integrieren lässt.

Effektives PAM beginnt mit einem robusten Identitätsnachweis und einer Multi-Faktor-Authentifizierung, um Hardware-Token, mobile Genehmigungen und biometrische Überprüfungen zu kombinieren, die durch End-zu-End-Verschlüsselung und Zero-Knowledge-Sicherheit unterstützt werden. Fein abgestufte, rollenbasierte Kontrollen und Just-in-Time-Bereitstellung innerhalb einer Zero-Trust-Architektur stellen sicher, dass Benutzer die erforderlichen Mindestberechtigungen erhalten, wodurch die Auswirkungen von Sicherheitsverletzungen drastisch reduziert werden. Gleichzeitig erfassen Überwachungsprotokolle jede privilegierte Sitzung, von ausgeführten Befehlen über visuelle Wiedergaben bis hin zur Sitzungsdauer. Die Audit-Protokolle speisen dann automatisierte Compliance-Engines, die die Praktiken an die HIPAA-, SOX- und PCI DSS-Standards anpassen, während Rezertifizierungskampagnen verwaiste oder überzählige Konten eliminieren.

Eine nahtlose Integration mit Cloud-Diensten und bestehenden Tools ist unerlässlich. Die Injektion von Zugangsdaten in Skripte, Pipelines und Remote-Zugriffsgateways sorgt für eine aufrechte Benutzerproduktivität, ohne die Übersicht zu beeinträchtigen. Fortschrittliche Verhaltensanalysen und agentische KI machen PAM dann zu einer aktiven Verteidigung. Echtzeitwarnungen und -aktionen können Bedrohungen sofort beenden und Berechtigungen widerrufen. Die Ausweitung dieser Kontrollen auf Dritte durch zeit- und gerätegebundenes Teilen, automatische Passwortrotation und strenge Genehmigungsworkflows mindert die Risiken für Auftragnehmer und die Lieferkette weiter.

In diesem Whitepaper untersuchen wir die Herausforderungen, mit denen Unternehmen bei der Erfüllung dieser PAM-Prioritäten konfrontiert sind, und bewerten, wie die KeeperPAM-Plattform von Keeper Security im Vergleich zur gesamten Branche abschneidet.

Zero-Trust by Design

Zero-Trust und Zero-Knowledge

Zero-Trust-Prinzipien von Grund auf zu verankern, ist für privilegierte Zugriffsverwaltung keine Option mehr– sondern eine Notwendigkeit. Ein „Zero-Trust by Design“-Framework behandelt jede Anforderung nach erhöhten Privilegien als von Natur aus nicht vertrauenswürdig und erfordert eine kontinuierliche Überprüfung, eine strikte Segmentierung und die Durchsetzung der geringsten Rechte. Durch die Umstellung von statischen, allmächtigen Zugangsdaten auf kurzlebige, kontextsensitive Zugriffstoken können Unternehmen die Angriffsfläche drastisch reduzieren und die laterale Bewegung im Falle einer Sicherheitsverletzung einschränken. Mit Zero-Trust by Design werden bei jeder Zugriffsentscheidung die Benutzeridentität, die Gerätehaltung, der Standort, die Tageszeit und der Verhaltenskontext berücksichtigt. Die Just-in-Time-Bereitstellung stellt sicher, dass privilegierte Rechte nur für die genau benötigte Dauer gewährt und danach automatisch widerrufen werden. Fein abgestufte, rollenbasierte Zugriffskontrollen minimieren die Vergabe von Überberechtigungen, während Multi-Faktor-Authentifizierung und kontinuierliche Sitzungsüberwachung vor Kompromittierung von Anmeldeinformationen und Insider-Bedrohungen schützen.

“[Wenn es um das Privileged Access Management geht, sind unsere Prioritäten] die Integration mit Zero-Trust-Architektur und kontinuierliches Validierungs-Framework.”
- IT-Direktor, 500-749 Mitarbeiter, verwendet KeeperPAM

Der Zero-Knowledge-Ansatz von Keeper für das Produktdesign verbessert diesen Ansatz weiter, indem er sicherstellt, dass alle Ver- und Entschlüsselungen lokal auf Ihrem Gerät erfolgen – nur Chiffretext wird jemals in die Cloud von Keeper übertragen. Ein Master-Passwort und abgeleitetes Schlüsselmaterial verlassen niemals ein ausgewähltes Gerät, was bedeutet, dass die Server von Keeper nicht auf unverschlüsselte Daten oder die Schlüssel, die sie schützen, zugreifen oder diese speichern können. Selbst wenn ihre Infrastruktur verletzt würde, würden die Angreifer nur eine unlesbare Zeichenfolge erhalten, die eine echte End-zu-End-Vertraulichkeit garantiert.

Umfragedaten unterstreichen die Wirkung dieses Ansatzes: 60 % der Benutzer von Keeper Security betrachten ihre PAM-Implementierung als “Zero-Knowledge” und “Zero-Trust by Design”, verglichen mit nur 34,9 % der Benutzer aller anderen Anbieter. Diese Lücke spiegelt eine proaktive Sicherheitslage wider – Keeper-Kunden legen Wert auf kontinuierliche Validierung, Eliminierung gemeinsam genutzter Konten und automatisiertes Privilege-Lifecycle-Management – im Gegensatz zu einer reaktiveren, Compliance-orientierten Denkweise anderswo.

Zero-Trust-PAM beschleunigt auch die Einhaltung von Vorschriften und die Bereitschaft zu Audits. Jede privilegierte Sitzung wird durchgängig protokolliert – komplett mit ausgeführten Befehlen, visueller Wiedergabe und Dauermetriken – und speist automatisierte Compliance-Engines, die auf die HIPAA-, SOX- und PCI DSS-Anforderungen abgestimmt sind. In der Praxis stärken Unternehmen, die Zero-Trust in ihre PAM-Architekturen integrieren, nicht nur ihre Abwehrmaßnahmen, sondern rationalisieren auch den Betrieb, senken die Kosten im Zusammenhang mit verwaisten Konten und zeigen messbare Verbesserungen bei der Eindämmung von Sicherheitsverletzungen.

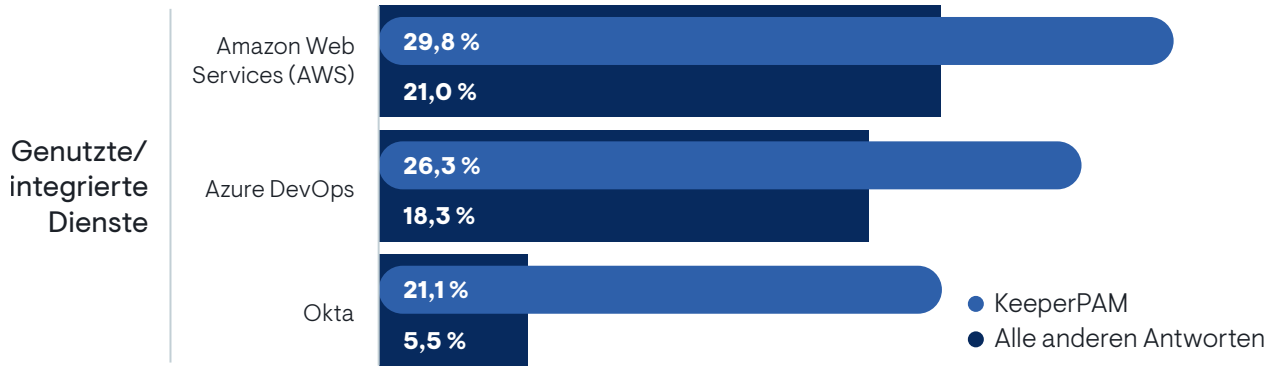
Letztendlich verwandeln der Zero-Knowledge-Ansatz und das Zero-Trust-Design von Keeper den privilegierten Zugriff von einer potenziellen Belastung in einen kontrollierten, überprüfbaren Prozess – ein Prozess, der sich in Echtzeit an sich ändernde Risiken anpasst und sicherstellt, dass kritische Systeme sicher, konform und widerstandsfähig bleiben.

Einfache Bereitstellung, Konfiguration und Integrationen

Es gibt keinen „Easy Button“, aber Keeper kommt dem sehr nahe

Die einfache Bereitstellung, Konfiguration und Integration kann über den ROI eines PAM-Projekts entscheiden. Laut der EMA-Umfrage bewerteten 60 % der Kunden von Keeper Security die anfängliche Bereitstellung als “sehr einfach”, verglichen mit nur 22,1 % der Benutzer auf anderen PAM-Plattformen. Umgekehrt bezeichneten 10 % der Kunden aller anderen Lösungen die Bereitstellung als “etwas schwierig” oder “sehr schwierig”, ein Problem, das bei KeeperPAM-Anwendern völlig fehlt. Die Migration älterer, lokaler PAM-Tools in die Cloud bringt immer noch 39 % der Unternehmen zum Stolpern – eine Komplexität, die durch die Cloud-native Architektur von Keeper umgangen wird. Integrationshürden plagen 11 % der Nicht-Keeper-Bereitstellungen, bei denen oft proprietäre Konnektoren und manuelle Skripte erforderlich sind, um sich in SIEM-, Ticketing- oder DevOps-Pipelines einzubinden. Die modulare API von KeeperPAM, Plug-and-Play-Konnektoren und die nahtlose Cloud-Orchestrierung beschleunigen die Wertschöpfung und minimieren betriebliche Reibungsverluste.

Arbeitet gut mit anderen zusammen



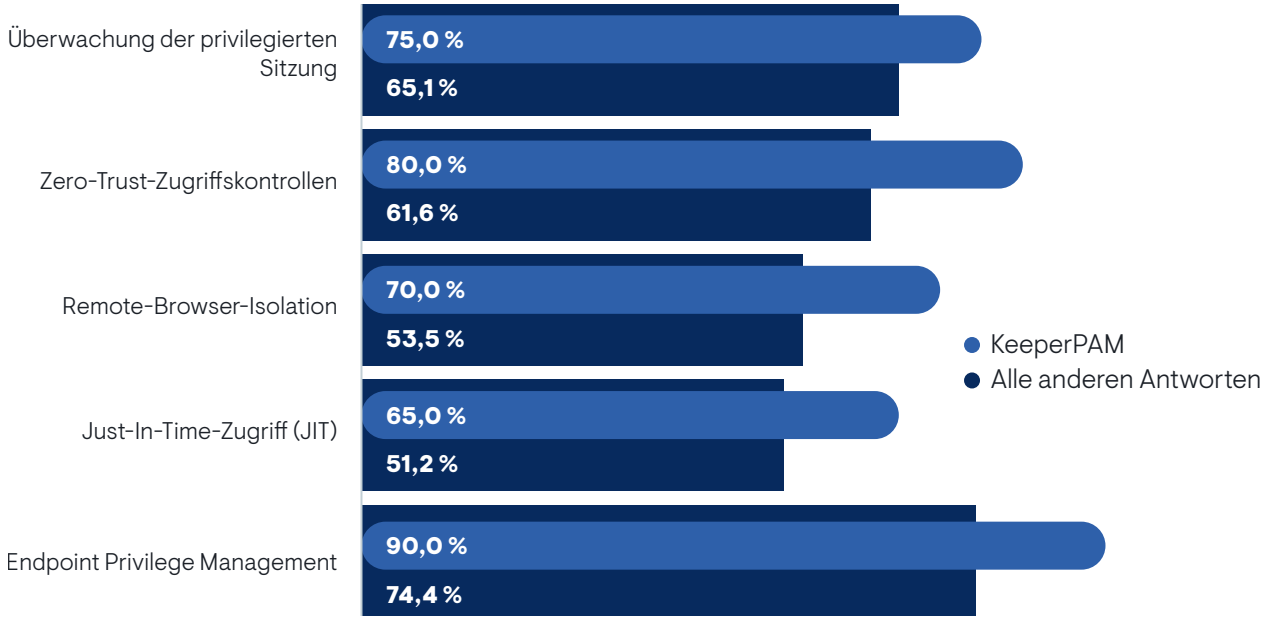
Nahtlose Integrationen sind ein Eckpfeiler jeder modernen PAM-Strategie, und Keeper ist auch hier führend. Out-of-the-Box-Konnektoren und -APIs ermöglichen eine schnelle, bidirektionale Integration mit Kernplattformen – ganz gleich, ob Sie EC2-Instances in Amazon Web Services einrichten, Pipelines in Azure DevOps automatisieren oder die Authentifizierung über Okta zentralisieren. KeeperPAM-Benutzer berichten von einer weitaus höheren Akzeptanz dieser Integrationen im Vergleich zu anderen PAM-Lösungen, wodurch zeitaufwändiges benutzerdefiniertes Scripting oder manuelle Konnektorwartung überflüssig werden. Durch die direkte Einbettung privilegierter Zugangsdateninjektion in Ihre CI/CD -Workflows, Cloud-Konsolen und Identitätsanbieter minimiert KeeperPAM Reibungsverluste, steigert die Produktivität der Entwickler und stellt sicher, dass Geheimnisse auf jeder Ebene geschützt bleiben.

Mit weniger Personal mehr erreichen

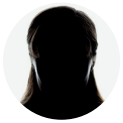
Der Personalbedarf für PAM-Implementierungen variiert stark je nach Plattform. Nur 15 % der Kunden von Keeper Security geben an, dass sie dank der intuitiven Benutzeroberfläche, der geführten Einrichtungsassistenten und der umfassenden Dokumentation von Keeper dediziertes Personal für die Verwaltung der Bereitstellung, Konfiguration und Integration benötigen. Im Gegensatz dazu benötigen 39,5 % der Unternehmen, die andere PAM-Lösungen verwenden, einen oder mehrere Vollzeitadministratoren, um ihre Umgebungen am Laufen zu halten. Diese Teams jonglieren oft mit komplexer Wartung von lokalen Geräten, maßgeschneiderten Skripten und manuellen Konnektor-Updates, was die Mitarbeiterzahl erhöht und die vorhandenen IT-Ressourcen auslastet. Das Cloud-native Design und die Self-Service-Tools von Keeper minimieren die Abhängigkeit von spezialisierten Fähigkeiten. Administratoren können neue Systeme integrieren, Berechtigungsrichtlinien anpassen und ohne umfangreiche Anpassungen in SIEM- oder DevOps-Pipelines integrieren. Letztendlich führt ein geringerer Personalaufwand zu schnelleren Rollouts und nachhaltigeren, erschwinglicheren langfristigen Abläufen.

Jenseits der Passwort- und Geheimnisverwaltung

Erweiterte PAM-Funktionen



Modernes PAM erfordert weit mehr als das Vaulting von Anmeldeinformationen – es erfordert einen umfangreichen Funktionsumfang, der aktiv Bedrohungen abwehrt, überwacht und sich an neue Bedrohungen anpasst. KeeperPAM zeichnet sich durch fortschrittliche Funktionen aus, die viele ältere Anbieter einfach nicht anbieten oder in großem Umfang implementieren. Die Überwachung privilegierter Sitzungen ist beispielsweise entscheidend, um jeden Tastendruck, jeden Befehl und jede visuelle Wiedergabe von Aktivitäten mit hohem Risiko zu erfassen. Keeper-Kunden nutzen diese Funktion häufiger als Mitbewerber und ermöglichen so die Erkennung von Bedrohungen und forensische Analysen in Echtzeit.



"Der Einsatz von PAM stärkt unsere Datenintegrität und unseren Ruf."
- VP Development/Engineering, 1.000-2.499 Mitarbeiter, verwendet KeeperPAM

Zero-Trust-Netzwerkzugriff erweitert das Prinzip der geringsten Rechte über Passwörter hinaus auf jede Zugriffsanforderung. Keeper bettet kontextbezogene Richtlinienprüfungen ein – Gerätestatus, Standort, Zeit und Verhaltens-Baselines – und stellt so sicher, dass selbst authentifizierte Sitzungen kontinuierlich überprüft werden. Dieses granulare Gating privilegierter Vorgänge reduziert das potenzielle Gefährdungsfenster im Vergleich zu statischen Alles-oder-Nichts-Modellen erheblich.

Remote Browser Isolation (RBI) ist ein weiterer Bereich, in dem Keeper die Konkurrenz übertrifft. Durch das Proxying von Administrationskonsolen über isolierte, sichere Browser eliminieren Unternehmen den direkten Endpunktzugriff für Dritte und Auftragnehmer und stellen potenzielle Malware oder den Diebstahl von Anmeldeinformationen effektiv unter Quarantäne. Nur wenige andere PAM-Lösungen integrieren RBI so nahtlos. Sie erzwingen stattdessen manuelle Problemumgehungen, die sowohl die Sicherheit als auch die Benutzererfahrung untergraben.

Just-in-Time-Bereitstellung und automatisiertes Privilege-Lifecycle-Management runden das fortschrittliche Toolkit von Keeper ab. Vorübergehende, zeitgebundene Erhöhungen verhindern, dass sich bestehende Konten mit hohen Berechtigungen ansammeln, während automatische Deprovisionierungs- und Rezertifizierungskampagnen die Einhaltung von Compliance-Vorschriften ohne manuelle Gemeinkosten. Schließlich schützt das Endpoint-Privilege-Management – das Entfernen lokaler Administratorrechte bei gleichzeitiger Vergabe von bereichsbezogenen Berechtigungen bei Bedarf – sowohl vor externen Angriffen als auch vor Insider-Missbrauch.

Durch den Blick über Passwörter und Geheimnisse hinaus verwandelt Keeper PAM in eine aktive Verteidigungsplattform: eine, die Angriffe antizipiert, Zero-Trust auf jeder Ebene durchsetzt und die fortschrittlichen Kontrollen bietet, die die komplexen Umgebungen von heute erfordern.

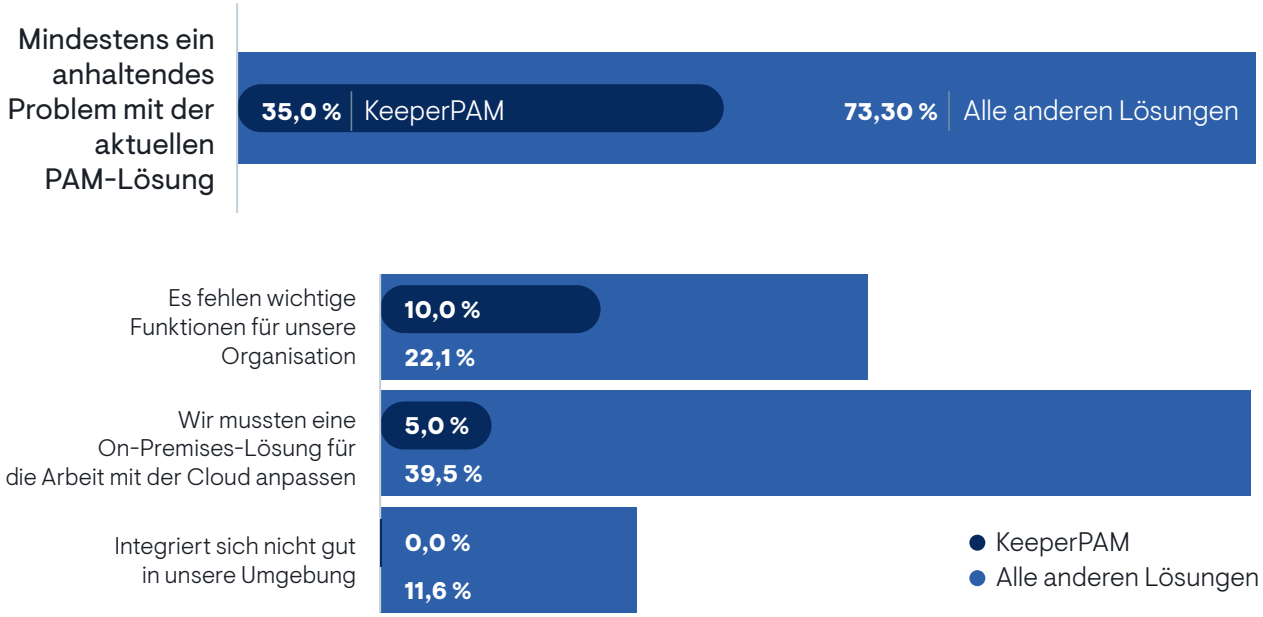
Allgemeine Zufriedenheit

Does Your PAM Solution Weather the Storm?

Die Kundenzufriedenheit ist das ultimative Barometer für den Wert und die Langlebigkeit einer PAM-Lösung. Wenn 5 % der Unternehmen, die andere Plattformen nutzen, aktiv nach einem Ersatz suchen, deutet dies auf kritische Lücken in Bezug auf Zuverlässigkeit, Benutzerfreundlichkeit und/oder Support hin. Im Gegensatz dazu gab kein Benutzer von Keeper Security an, dass er plante, sein PAM-Tool aufzugeben, was die Fähigkeit von Keeper unterstreicht, die sich entwickelnden Sicherheits- und Betriebsanforderungen zu erfüllen.

Darüber hinaus bezeichnen sich 75 % der Keeper-Kunden insgesamt als “sehr zufrieden” – weit mehr als die 53,5 % der Nutzer konkurrierender Anbieter. Eine hohe Zufriedenheit korreliert mit einer schnelleren Einführung, einer effektiveren Risikoreduzierung und niedrigeren Gesamtbetriebskosten, da zufriedene Teams in tiefere Integrationen und fortschrittlichere Funktionen investieren. In einer Landschaft, in der privilegierter Zugriff ständig ins Visier genommen wird, ist die Wahl einer Plattform, die ihre Benutzer begeistert, nicht nur schön, sondern auch geschäftskritisch.

Funktionen und Integrationen sind kritische Schmerzpunkte



Trotz ihrer entscheidenden Rolle haben viele PAM-Bereitstellungen mit anhaltenden Hindernissen zu kämpfen. 73 % der Unternehmen, die Lösungen verwenden, die nicht von Keeper stammen, berichten von mindestens einer erheblichen Herausforderung, verglichen mit nur 35 % der Keeper-Kunden. Zu den häufigsten Problempunkten gehören das Fehlen wesentlicher Funktionen, die Teams dazu zwingen, Tools von Drittanbietern zu verwenden, eine schlechte Integration in die bestehende Infrastruktur und die Kopfschmerzen bei der Nachrüstung von On-Premises-Plattformen zur Unterstützung von Cloud-Umgebungen. KeeperPAM-Benutzer haben diese Probleme dank der umfassenden Funktionsoptionen, der nativen Cloud-First-Architektur und der umfangreichen Bibliothek von Konnektoren weitaus seltener. Durch die Minimierung von Funktionslücken und die Vereinfachung hybrider Bereitstellungen verkürzt Keeper nicht nur die Zeit bis zur Wertschöpfung, sondern reduziert auch den Aufwand für Fehlerbehebungen und Problemumgehungen, sodass sich Sicherheitsteams auf die proaktive Risikominderung konzentrieren können, statt auf die Bekämpfung von Altlasten.

Bessere Lösung, bessere Prioritäten

Andere PAM-Implementierungen können ihr Potenzial nicht

Schwerpunktgebiet	Keeper-Kunden	Andere PAM-Lösungen
Authentifizierung	Kontinuierlich, Zero-Trust	Rollenbasiert, MFA
Verwaltung der Zugangsdaten	Eliminierung von statischen/gemeinsam genutzen Zugangsdaten	Grundlegende Steuerung und Überwachung des Zugriffs
Schulung	Explizite Priorität	Nicht hervorgehoben
Automatisierung	Fokus auf die Risikominderung (da der Prozess bereits effizient ist)	Fokus auf Prozesseffizienz
Compliance	Fokus auf Missbrauch von Anmeldeinformation & Audits	Mindesteinhaltung gesetzlicher Vorschriften

Keeper Security ermöglicht es Unternehmen, von einer Wartungs- und Compliance-orientierten Haltung zu einer proaktiven, sicherheitsorientierten Haltung überzugehen. KeeperPAM-Kunden eliminieren statische und unsicher geteilte Anmeldeinformationen durch eine Zero-Knowledge-Vaulting-Engine, die kurzlebige Geheimnisse mit den geringsten Rechten ausgibt und so sowohl externe Angriffsvektoren als auch Insider-Missbrauch im Vergleich zu herkömmlichen reinen Vault-Ansätzen drastisch reduziert. Kontinuierliche Authentifizierung und Zero-Trust-Zugriffskontrollen – einschließlich Gerätezustandsprüfungen, Geolokalisierung und Verhaltensanalysen – stellen sicher, dass jede Sitzung noch lange nach einer einmaligen MFA-Aufforderung unter die Lupe genommen wird, was es Angreifern praktisch unmöglich macht, gestohlene Anmeldeinformationen unentdeckt auszunutzen. Die risikoorientierte Automatisierung von Keeper deckt den gesamten Lebenszyklus von Berechtigungen ab – von der Erkennung und dem Onboarding bis hin zur automatischen Rotation und Deprovisionierung – so werden die Ausbreitung von Anmeldeinformationen und verwaiste Konten verhindert, während viele andere Lösungen lediglich Genehmigungsworkflows oder Compliance-Berichte automatisieren. Wichtig ist, dass Keeper-Kunden die Schulung und das

Bewusstsein der Mitarbeiter ausdrücklich als zentrale Sicherheitskontrolle integrieren und erkennen, dass menschliche Faktoren genauso wichtig sind wie Technologie, um die Akzeptanz zu fördern und riskante Workarounds zu verhindern.

"Ich glaube, dass die dauerhafte Überwachung privilegierter Konten mir dabei hilft, nachts besser zu schlafen."
– VP Development/Engineering, 2.500-4.999 Mitarbeiter, verwendet KeeperPAM

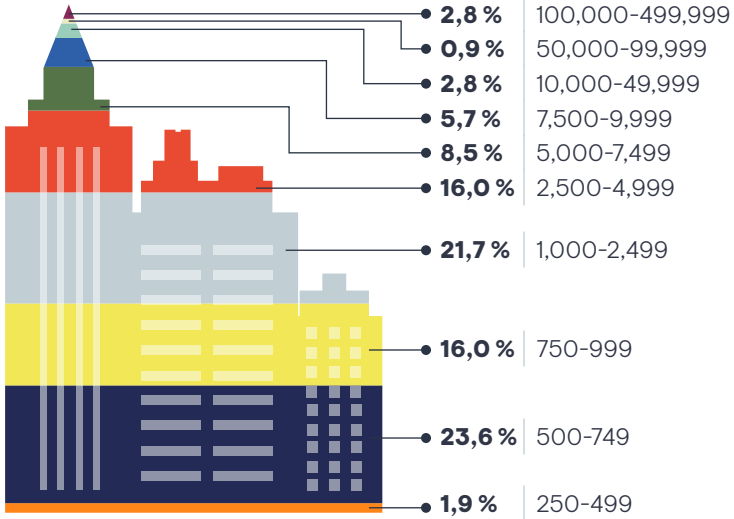
Im Gegensatz dazu legen Benutzer anderer PAM-Tools oft Wert auf traditionelle Kontrollen, wie z. B. rollenbasierten Zugriff, Überwachung nach dem Zugriff und betriebliche Effizienz, was eine reaktive Denkweise widerspiegelt, die mit Funktionslücken, brüchigen Integrationen und der Komplexität der Nachrüstung von On-Premises-Lösungen für die Cloud zu kämpfen hat. Die Cloud-native Architektur von Keeper und die umfangreiche Bibliothek von Plug-and-Play-Konnektoren beseitigen diese Probleme und ermöglichen eine schnelle Integration mit SIEM-Plattformen, Identitätsanbietern wie Okta und CI/CD-Pipelines in AWS oder Azure DevOps. Erweiterte Funktionen wie die Überwachung privilegierter Sitzungen, Remote Browser Isolation, Just-in-Time-Bereitstellung und die Verwaltung von Endpunktberechtigungen sind alle nativ in Keeper integriert, und reduzieren so Reibungsverluste bei der Bereitstellung und laufendem Personalbedarf.

Durch die Kombination dieser Funktionen der nächsten Generation mit einer nahtlosen Benutzererfahrung versetzt Keeper Sicherheitsteams in die Lage, Bedrohungen zu antizipieren, kontinuierlichen Schutz durchzusetzen und ihre privilegierte Zugriffsumgebung wirklich zu stärken.

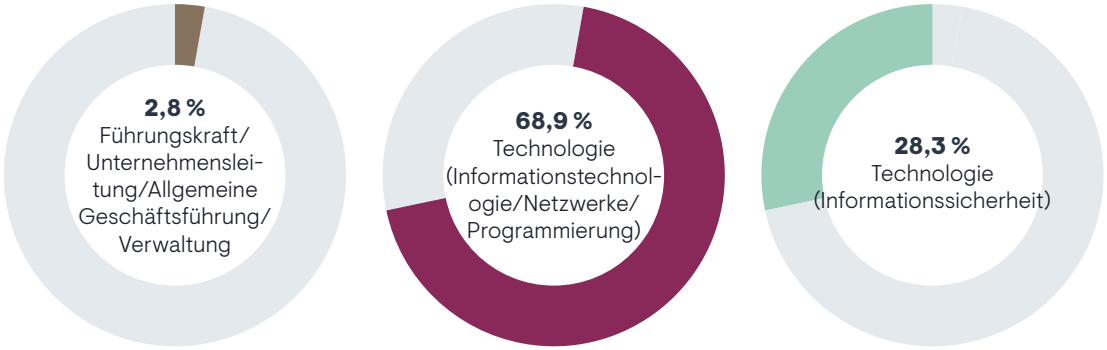
Methodologie

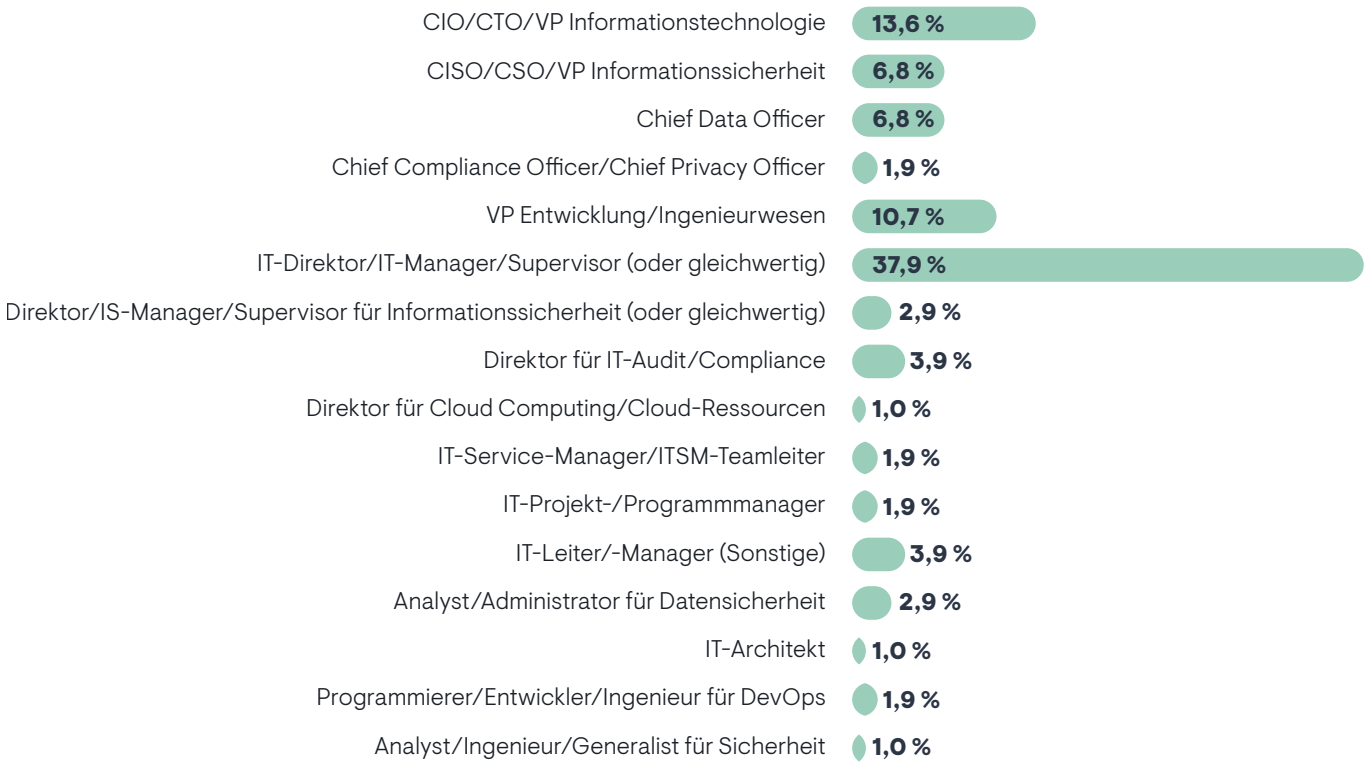
Insgesamt 106 Fachleute, die BeyondTrust, CyberArk, Delinea, Devolutions, Keeper Security, ManageEngine, One Identity oder StrongDM nutzen (Stand Juni 2025). Alle Daten in diesem Whitepaper basieren auf den Antworten auf Umfragen und offenen Antworten zu den Prioritäten und Herausforderungen des Privileged Access Managements in Unternehmen.

Größe der Organisation



Rolle der Befragten




CIO/CTO/VP Informationstechnologie 13,6 %
CISO/CSO/VP Informationssicherheit 6,8 %
Chief Data Officer 6,8 %
Chief Compliance Officer/Chief Privacy Officer 1,9 %
VP Entwicklung/Ingenieurwesen 10,7 %
IT-Direktor/IT-Manager/Supervisor (oder gleichwertig) 37,9 %
Direktor/IS-Manager/Supervisor für Informationssicherheit (oder gleichwertig) 2,9 %
Direktor für IT-Audit/Compliance 3,9 %
Direktor für Cloud Computing/Cloud-Ressourcen 1,0 %
IT-Service-Manager/ITSM-Teamleiter 1,9 %
IT-Projekt-/Programmmanager 1,9 %
IT-Leiter/-Manager (Sonstige) 3,9 %
Analyst/Administrator für Datensicherheit 2,9 %
IT-Architekt 1,0 %
Programmierer/Entwickler/Ingenieur für DevOps 1,9 %
Analyst/Ingenieur/Generalist für Sicherheit 1,0 %

Branche


Luft- und Raumfahrt/Verteidigung 3,8 %
Automobilindustrie 6,6 %
Unternehmensdienstleistungen/Beratung 1,9 %
Computer-/Technologie-Hardware (Geräte, Chips, Computer-/Netzwerk-Hardware) 2,8 %
Computer/Technologie-Software (mobile App, Verbraucher, kundenspezifisch, webbasiert) 11,3 %
Computer-/Technologiedienstleistungen (IaaS, SaaS, MSP, MSSP, Cloud-Anbieter) 7,5 %
Computer/Technologie: Sonstige 1,9 %
Bildung (Bund, Länder und Region) 0,9 %
Finanzen/Finanzdienstleistungen/Banken/Krypto 3,8 %
Regierung (Bund, Länder und Region) 1,9 %
Gesundheitswesen/Medizin/Pharmazie 12,3 %
Herstellung 11,3 %
Gemeinnützig/Nicht gewinnorientiert 0,9 %
Öl/Gas/Chemie 1,9 %
Professionelle Dienstleistungen (nicht-technisch) 1,9 %
Einzelhandel/Großhandel/Vertrieb 6,6 %
Transport/Fluggesellschaften/Lkw- und Schienenverkehr 4,7 %
Reisen/Gastgewerbe/Freizeit 5,7 %
Versorger/Energie 12,3 %

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4577.081225-DE