KEEPER®

Sicherung des privilegierten Zugriffs

Der Schlüssel zur modernen Unternehmensverteidigung

Einleitung

In der digital vernetzten Welt von heute verlassen sich Unternehmen auf ein vielfältiges Netzwerk von Benutzern, Anwendungen und Infrastrukturen, um effizient und sicher arbeiten zu können. Mit der Erweiterung dieses Netzwerks über Cloud-, Hybrid- und Multi-Vendor-Umgebungen hinweg, wird die Verwaltung des privilegierten Zugriffs immer komplexer – und wichtiger.

Gleichzeitig nutzen Angreifer weiterhin ausgeklügelte Kampagnen, die auf Anmeldeinformationen abzielen – nicht nur, um Erstzugriff zu erhalten, sondern auch, um Berechtigungen zu erweitern, die Erkennung zu umgehen und die Kontrolle über sensible Systeme zu übernehmen. Dies führt zu einer größeren Verantwortung für Unternehmen, um sicherzustellen, dass die richtigen Personen zur richtigen Zeit Zugang zu den richtigen Systemen und Daten haben.

Privileged Access Management (PAM) hilft bei der Bewältigung dieser Herausforderung, indem es Unternehmen ermöglicht, den Zugriff auf kritische Infrastrukturen zu kontrollieren, zu überwachen und einzuschränken. Da sich die Umgebungen jedoch mit der Einführung der Cloud, Remote-Arbeit und der zunehmenden Automatisierung weiterentwickeln, haben herkömmliche Zugriffskontrollen oft Schwierigkeiten, Schritt zu halten.

Um besser zu verstehen, wie Unternehmen moderne Umgebungen schützen, führte Keeper Security eine globale Umfrage unter 4.000 IT- und Sicherheitsexperten in Unternehmen mit 250 oder mehr Mitarbeitern durch. Dieser Bericht beleuchtet deren Perspektiven auf PAM: die Beweggründe, welche die Einführung vorantreiben, die Hindernisse, die eine effektive Bereitstellung erschweren und die Funktionen, die als wesentlich für die Sicherung des Zugriffs in den heutigen dynamischen Betriebsumgebungen angesehen werden.

© 2025 Keeper Security, Inc.

Warum Unternehmen auf PAM umsteigen

Die Hauptfunktion von PAM besteht darin, Organisationen bei der Verwaltung von Konten mit erhöhtem Zugriff zu unterstützen. Diese Konten, die von Administratoren, Dienstanwendungen und Automatisierungstools verwendet werden, können umfassende Systemberechtigungen freischalten. Wenn sie missbraucht oder kompromittiert werden, können die Folgen erheblich sein.

Die wichtigsten Gründe, weshalb Organisationen PAM eingeführt haben

Schutz vor Diebstahl von Anmeldeinformationen und Cyberbedrohungen

69%

Sicherer Zugriff auf Cloud- und Hybridumgebungen

65%

Erfüllung von Compliance-Anforderungen

60%

Sicherung von Dienstkonten

54%

Bereitstellung eines sicheren Fernzugriffs für Dritte

53%

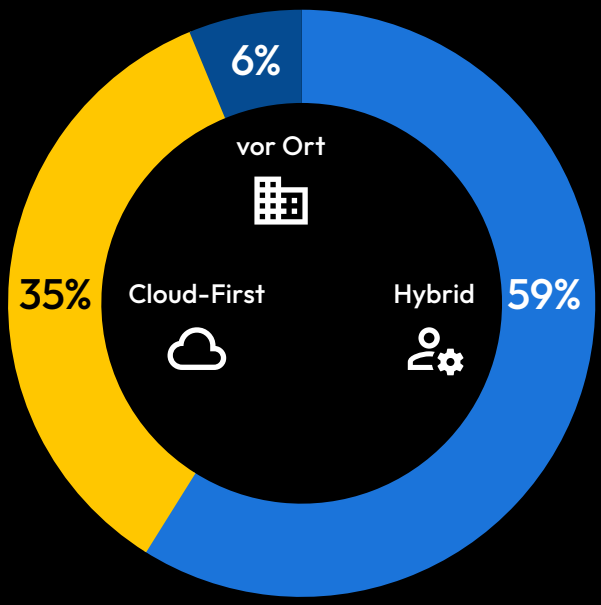
Diese Prioritäten spiegeln ein ausgeprägtes Verständnis des Wertes von PAM für die Unternehmen wider – sowohl für die Sicherheit als auch für den Betrieb.

© 2025 Keeper Security, Inc.

Verschiebung der Infrastruktur, Ausweitung des Risikos

Die IT-Landschaft hat sich in den letzten zehn Jahren dramatisch verändert, da täglich neue Technologien eingeführt werden. Da der traditionelle Burg-und-Burggraben-Ansatz (Castle-and-Moat) für die Netzwerksicherheit so gut wie veraltet ist, zeigt die Studie, dass die Mehrheit der Unternehmen in hybriden Umgebungen arbeitet.

Diese Realität mit mehreren Umgebungen erhöht die Komplexität der Verwaltung des privilegierten Zugriffs. Privilegierte Konten müssen gesichert werden – nicht nur auf herkömmlichen lokalen Servern, sondern auch über Cloud-Plattformen, SaaS-Anwendungen, Entwicklertools und verschiedene Remote-Endpunkte hinweg. Jede Umgebung birgt einzigartige Risiken und erfordert maßgeschneiderte Kontrollen, um sicherzustellen, dass sensible Systeme geschützt bleiben. Da Unternehmen weiterhin Cloud- und Hybridmodelle nutzen, dehnt sich der Perimeter für privilegierten Zugriff über die Netzwerkgrenze hinaus aus – was einen nuancierteren und anpassungsfähigeren Ansatz für das Zugriffsmanagement erfordert.



> Jedes System – ob in der Cloud, vor Ort oder remote – ist ein potenzieller Einstiegspunkt, der adaptive und sichere Kontrollen erfordert, um sich gegen moderne Bedrohungen zu verteidigen.
>
> – **Darren Guccione**, CEO und Mitbegründer Keeper Security Inc.

© 2025 Keeper Security, Inc.

Navigation bei der PAM-Einführung

Während 86 % der Befragten der Meinung sind, dass ihre Unternehmen von einer PAM-Lösung profitieren würden, stehen viele immer noch vor praktischen und organisatorischen Herausforderungen, die die Implementierung behindern und ihre Wirksamkeit einschränken können.

Bedeutendste Hindernisse, über die Organisationen nach der Einführung von PAM berichten

Komplexität der Implementierung

Budgetbeschränkungen

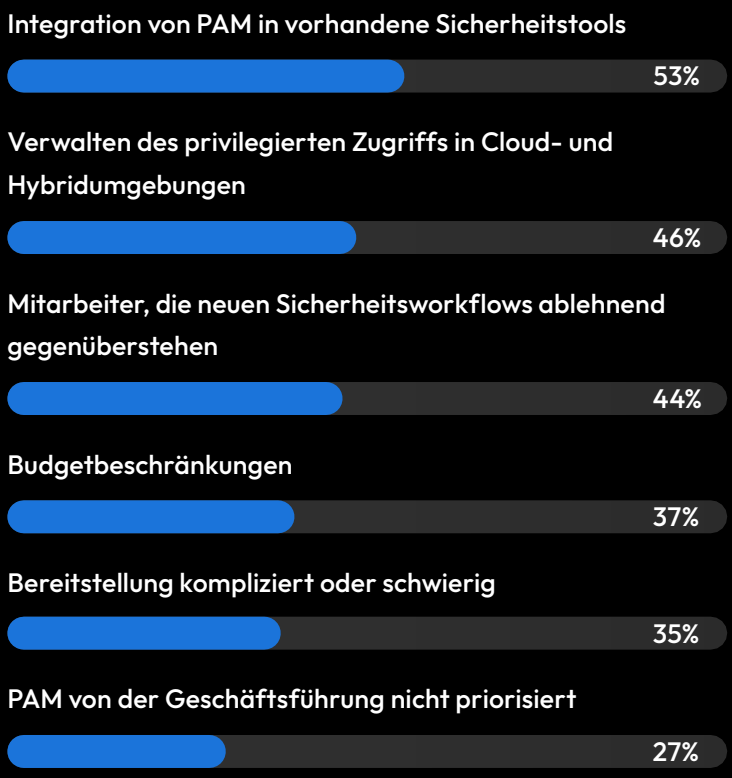
Komplikation von Cloud-/Multi-Cloud-Umgebungen

Personalmangel für die Implementierung/Verwaltung einer PAM-Lösung

© 2025 Keeper Security, Inc.

Herausforderungen enden nicht unbedingt nach der ersten Bereitstellung. Unter denen, die über eine Form von PAM verfügen, stoßen viele auf Schwierigkeiten bei der Skalierung und Operationalisierung ihrer Lösung.

Wichtige Hindernisse, die von Organisationen nach der PAM-Bereitstellung gemeldet wurden



Diese Ergebnisse unterstreichen, wie wichtig es ist, sich für eine PAM-Lösung zu entscheiden, die flexibel und einfach zu implementieren ist und die so konzipiert ist, dass sie sich nahtlos in die bestehende Infrastruktur integrieren lässt. Der Erfolg hängt auch von der organisatorischen Ausrichtung ab und davon, dass sowohl die technischen als auch die Business-Teams die richtige Unterstützung erhalten.

© 2025 Keeper Security, Inc.

Wie effektives PAM aussieht

Bei effektiver Implementierung bietet PAM messbare Sicherheits- und Betriebsvorteile im gesamten Unternehmen, wobei die Anwender unter anderem von besserem Datenschutz, Effizienz und weniger Cybervorfällen berichten. Organisationen, die PAM eingeführt haben, schildern signifikante Verbesserungen, die weit über optimierte Zugriffskontrollen hinausgehen.

Befragte, die PAM vollständig implementiert haben

53% verbesserten den Schutz sensibler Daten

50% sahen eine höhere Effizienz bei der Verwaltung privilegierter Anmeldeinformationen

49% verbesserten die Sicherheit für Remote-Verbindungen zur Infrastruktur

49% reduzierten Sicherheitsvorfälle im Zusammenhang mit dem Missbrauch von Privilegien

48% erhielten eine bessere Transparenz und Kontrolle über privilegierte Konten

47% reduzierten die Belastung des IT-Helpdesks, die mit der manuellen Verwaltung von Anmeldeinformationen verbunden ist

47% stärkten ihre Compliance-Haltung

40% optimierten Workflows für Zugriffsanfragen und Genehmigungen

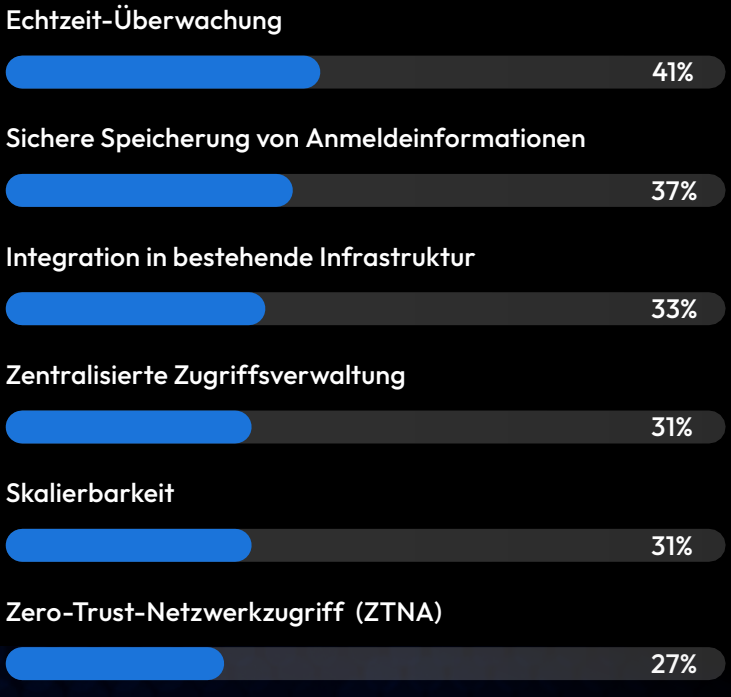
Diese Ergebnisse zeigen, dass modernes PAM nicht nur Risiken mindert, sondern auch die Agilität verbessert, den Overhead reduziert und Unternehmen dabei hilft, die Sicherheit mit den betrieblichen Zielen in Einklang zu bringen.

© 2025 Keeper Security, Inc.

Die wichtigsten PAM-Funktionen

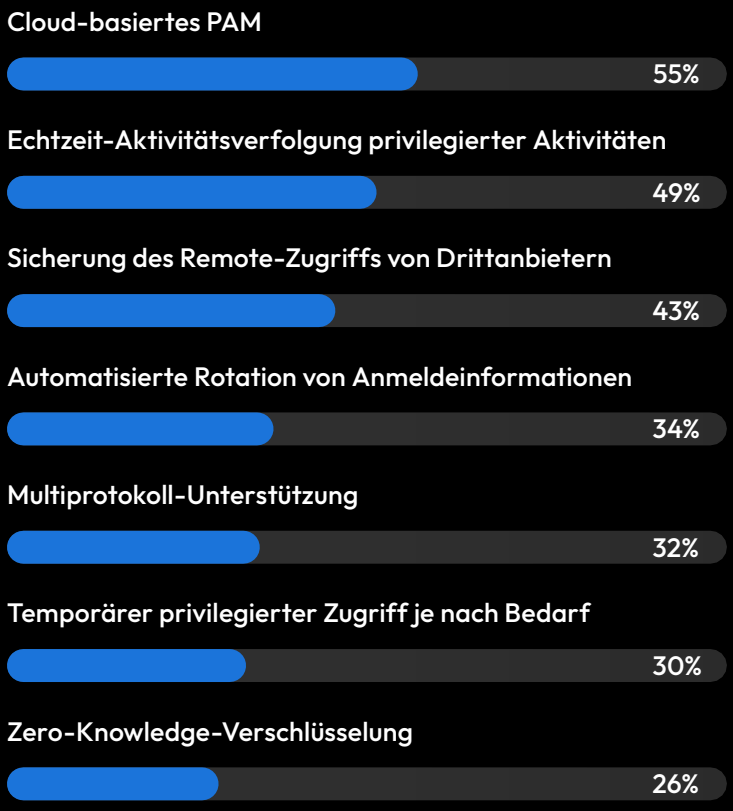
Da Unternehmen immer Cloud-zentrierter werden, benötigen sie Funktionen, die moderne Workflows und Architekturen widerspiegeln. Zu den am meisten geschätzten Funktionen, die von PAM-Benutzern in Cloud- und Hybridumgebungen verwendet werden, gehören:

Top-Funktionen von Cloud-/Hybrid-Umgebungen



© 2025 Keeper Security, Inc.

Auf die Frage, welche PAM-Funktionen insgesamt am wichtigsten sind, nannten die Befragten Folgendes



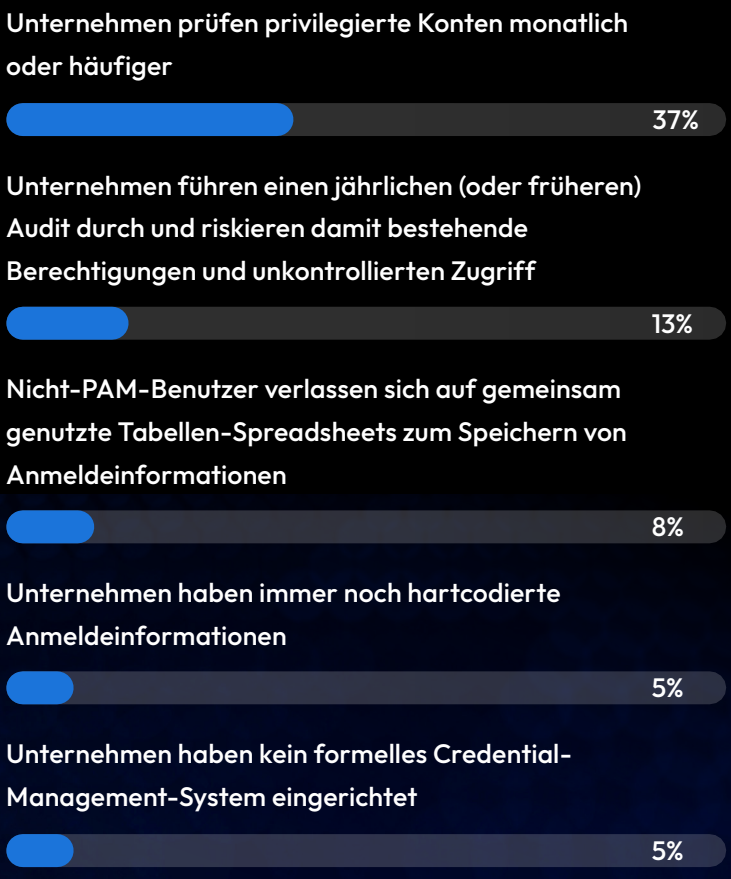
Diese Ergebnisse verstärken die Verschiebung hin zu Cloud-nativen, flexiblen Plattformen, die hohe Sicherheit bieten, ohne die Benutzerfreundlichkeit zu beeinträchtigen. Im Gegensatz dazu erfordern herkömmliche lokale PAM-Lösungen erhebliche Vorabinvestitionen, wobei sie nicht über die Skalierbarkeit und Flexibilität von Cloud-basierten Alternativen verfügen und damit weniger für Cloud- und Hybridumgebungen geeignet sind.

© 2025 Keeper Security, Inc.

Warum Bildung immer noch wichtig ist

Technologie ≠ Bewusstsein

Selbst wenn PAM-Tools vorhanden sind, können menschliche Faktoren Risiken mit sich bringen. Eine starke Sicherheitslage erfordert sowohl die richtigen Systeme als auch die richtigen Verhaltensweisen.



Ohne regelmäßige Schulungen, strenge Zugangsrichtlinien und kulturelle Stärkung können selbst gut ausgestattete Unternehmen auf riskante Praktiken zurückfallen. Die Aufklärung der Teams darüber, warum bestimmte Verhaltensweisen – wie das Hartcodieren von Anmeldeinformationen oder das Überspringen regelmäßiger Audits – Risiken darstellen, ist für eine breite Akzeptanz unerlässlich. Wenn Mitarbeiter nicht nur das “Wie”, sondern auch das “Warum” des sicheren Zugriffsmanagements verstehen, ist es wahrscheinlicher, dass sie PAM-Tools effektiv einsetzen.

Die Abstimmung von Technologie und Bildung trägt dazu bei, die Lücke zwischen Kontrolle in der Theorie und Sicherheit in der Praxis zu schließen.

© 2025 Keeper Security, Inc.

Wie geht es weiter mit PAM?

Mit der Weiterentwicklung von Sicherheitsbedrohungen müssen sich auch die Tools zur Abwehr dieser Bedrohungen weiterentwickeln. IT- und Sicherheitsverantwortliche auf der ganzen Welt haben die folgenden Trends als wichtig für die Zukunft von PAM identifiziert:

KI-gestützte Sicherheitsanalysen zur Erkennung von Anomalien beim privilegierten Zugriff

72%

Breitere Akzeptanz von Cloud-nativen PAM-Lösungen

60%

Vereinfachte Benutzererfahrung, um Reibungsverluste zu reduzieren und die Akzeptanz zu verbessern

56%

Stärkere Integration mit Zero-Trust-Architekturen

56%

Dies deutet auf eine Zukunft hin, in der PAM nicht nur leistungsfähiger, sondern auch zugänglicher ist und es Unternehmen jeder Größe ermöglicht, privilegierten Zugriff zu schützen und neue Technologien einzuführen, ohne die Teams zu überlasten.

© 2025 Keeper Security, Inc.

Schlussgedanke: Kontrolle schafft Vertrauen

In einer Sicherheitslandschaft, in der es mehr Identitäten als Geräte gibt und der Zugriff von überall und jederzeit gewährt werden kann, ist die Kontrolle privilegierter Konten für den Schutz kritischer Systeme und Daten von grundlegender Bedeutung. Privileged Access Management ermöglicht es Unternehmen, von reaktiver Verteidigung zu proaktiver Kontrolle überzugehen. Durch die Kombination der Speicherung von Anmeldeinformationen, rollenbasiertem Zugriff und Echtzeitüberwachung tragen moderne PAM-Lösungen dazu bei, Risiken zu reduzieren und die betriebliche Ausfallsicherheit zu verbessern.

Methodologie

Diese Studie wurde von Keeper Security in Zusammenarbeit mit dem unabhängigen Forschungsunternehmen OnePoll durchgeführt. Für die Studie wurden 4.000 IT- und Sicherheitsentscheider in Unternehmen mit 250 oder mehr Mitarbeitern in den USA, Großbritannien, Frankreich, Deutschland, Japan, Australien, Neuseeland und Singapur befragt. Die Feldforschung wurde zwischen dem 25. März und dem 11. April 2025 online durchgeführt.

> Der Zugriff kann überall erfolgen – PAM sorgt dafür, dass er sicher erfolgt. Es ist die Art und Weise, wie Unternehmen verwalten, überwachen und schützen, was am wichtigsten ist.
>
> – **Darren Guccione**, CEO und Mitbegründer Keeper Security Inc.

Über Keeper Security:

Keeper Security verändert die Cybersicherheit für Millionen von Einzelpersonen und Tausende von Unternehmen weltweit. Die intuitive Cybersecurity-Plattform von Keeper basiert auf einer Ende-zu-Ende-Verschlüsselung und wird von Fortune-100-Unternehmen zum Schutz jedes Benutzers, jedes Geräts und jedes Standorts eingesetzt. Unsere patentierte Zero-Trust- und Zero-Knowledge-Privileged-Access-Management-Lösung vereint die Verwaltung von Unternehmenspasswörtern, Geheimnissen und Verbindungen mit Zero-Trust-Netzwerkzugriff, Endpunkt-Privilege-Management und Remote-Browser-Isolation. Durch die Kombination dieser kritischen Identitäts- und Zugriffsmanagement-Komponenten in einer einzigen Cloud-basierten Lösung bietet Keeper unvergleichliche Transparenz, Sicherheit und Kontrolle und stellt gleichzeitig sicher, dass Compliance- und Audit-Anforderungen erfüllt werden. Erfahren Sie, wie Keeper Ihr Unternehmen vor den heutigen Cyber-Bedrohungen schützen kann unter KeeperSecurity.com.

© 2025 Keeper Security, Inc.