



Keeper Security 2025 Rückblick: Ein Jahr voller Dynamik, Modernisierung und identitätsorientierter Innovationen

Keeper hat seine einheitliche Plattform für privilegierten Zugriff weiterentwickelt, seine globale Reichweite ausgebaut und Forschungsergebnisse vorgelegt, die den Umgang von Unternehmen mit moderner Identitätssicherheit geprägt haben.

MÜNCHEN, 22. Dezember 2025 – [Keeper Security](#), ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Cybersicherheitssoftware zum Schutz von Passwörtern und Passkeys, Infrastrukturgeheimnissen, Fernverbindungen und Endpunkten sieht das Jahr 2025 als ein Jahr bedeutenden Wachstums. Angesichts der Zunahme von Angriffen auf Zugangsdaten, der raschen Einführung von KI und den betrieblichen Anforderungen hybrider Umgebungen hat Keeper seine Plattform für privilegiertes Zugriffsmanagement (PAM) gestärkt, seine globale Präsenz ausgebaut und Branchenstudien durchgeführt, die den Ansatz von Unternehmen für eine identitätsbasierte Verteidigung geprägt haben.

„Die diesjährigen Ergebnisse spiegeln den unermüdlichen Einsatz unseres globalen Teams und das Vertrauen wider, das uns Tausende von Unternehmen entgegenbringen, die sich auf Keeper verlassen, um ihre sensibelsten Systeme und Daten zu schützen“, so Darren Guccione, CEO und Mitbegründer von Keeper Security. „Wir sind stolz auf das, was wir gemeinsam erreicht haben, und zutiefst dankbar gegenüber unseren Kunden, Partnern und Mitarbeitern, die Keeper zu seiner Position als Marktführer im Bereich Identitäts- und Zugriffsmanagement verholfen haben.“

Ein Wendepunkt für privilegierten Zugriff

Einer der prägenden Momente des Jahres war das [Debüt von Keeper im Gartner® Magic Quadrant™](#) für Privileged Access Management. Diese Anerkennung stand im Einklang mit der [Weiterentwicklung von KeeperPAM®](#), das die Bereiche Passwortverwaltung für Unternehmen, Geheimnisverwaltung, Verbindungsmanagement, Zero-Trust-Netzwerkzugriff, Remote-Browser-Isolation und Endpunkt-Privilegienkontrolle in einer einheitlichen, cloud-nativen Plattform vereinte.

Unternehmen weltweit haben KeeperPAM eingeführt, um privilegierten Zugriff mit Zero-Trust- und Zero-Knowledge-Sicherheit zu modernisieren, ohne die Komplexität herkömmlicher PAM-Tools in Kauf nehmen zu müssen. Im Laufe des Jahres hat Keeper seine Plattform mit innovativen Funktionen weiterentwickelt. [Endpoint Privilege Manager](#) ermöglicht eine präzise, zeitnahe Berechtigungserweiterung und reduziert gleichzeitig die mit lokalen Administratorrechten verbundenen Risiken. [Keeper Forcefield](#), das einzige Produkt seiner Art in der Branche, schützt vor speicherbasierten Angriffen auf Windows-Rechner.

Keeper hat außerdem die Transparenz und Kontrolle über privilegierte Sitzungen durch [KeeperAI™](#) erweitert, das auf einem Sovereign-AI-Framework basiert und eine agentenbasierte KI-Bedrohungserkennung und -reaktion in Echtzeit ermöglicht. Dadurch wird sichergestellt, dass risikoreiche Sitzungen automatisch beendet und alle

Benutzeraktivitäten analysiert und kategorisiert werden. Als Teams damit anfingen, KI in Betriebs- und Entwicklungsabläufen einzusetzen, fügte Keeper die Unterstützung für das [Model Context Protocol \(MCP\)](#) innerhalb des Keeper Secrets Managers hinzu. Die Integration von Keeper ermöglicht es den KI-Tools von Drittanbietern, wie lokalen oder cloudbasierten Assistenten, die in ihrem Tresor gespeicherten Geheimnisse sicher abzurufen oder zu verwalten, ohne die Zero-Knowledge-Sicherheitsarchitektur von Keeper zu beeinträchtigen.

Plattformverbesserungen wie [bidirektionales One-Time Share](#), verbesserte [biometrische Anmeldung mit Passkeys](#), eine [WearOS-Smartwatch-App](#), [QR-Code-WLAN-Aufzeichnungen](#) und Verfeinerungen der Mobil- und Tresorerfahrung spiegeln das kontinuierliche Engagement von Keeper wider, Benutzerfreundlichkeit mit kontinuierlichen Sicherheitsverbesserungen in Einklang zu bringen. Keeper vertieft auch die Integrationen im gesamten Cybersicherheits-Ökosystem, darunter neue Verbindungen mit [CrowdStrike Falcon® Next-Gen SIEM](#), [Google Security Operations](#) und [Microsoft Sentinel](#), und half Unternehmen dabei, privilegierte Zugriffstelemetrie in umfassendere Erkennungs- und Reaktionsworkflows zu integrieren. Das Engagement des Unternehmens für starke Verschlüsselung wurde durch die [FIPS 140-3](#)-Validierung seines kryptografischen Moduls erneut bestätigt.

„2025 war ein entscheidendes Jahr für unsere Entwicklerteams, da wir unsere einheitliche Plattform für privilegierten Zugriff weiterentwickelt und Funktionen bereitgestellt haben, die die Abwehrmaßnahmen unserer Kunden messbar stärken“, so Craig Lurey, CTO und Mitbegründer von Keeper Security. „Mit KeeperAI haben wir die Echtzeit-Bedrohungserkennung direkt in privilegierte Sitzungen integriert. Wir haben den Endpunktsschutz erweitert, sichere Verbindungen modernisiert und die Geheimnisverwaltung sowie den Zero-Trust-Zugriff auf der gesamten Plattform weiter verbessert. Diese Verbesserungen sind das Ergebnis fokussierter, disziplinierter Entwicklungsarbeit und kontinuierlichen Feedbacks von Kunden. Wir haben eine PAM-Plattform entwickelt, die schnell, skalierbar und von Grund auf sicher ist – und das ist erst der Anfang.“

Globales Wachstum und Anerkennung

Die Weiterentwicklung der Keeper-Plattform führte zu einem erheblichen weltweiten Wachstum. Das Unternehmen überschritt die Marke von vier Millionen zahlenden Nutzern und verzeichnete eine starke Akzeptanz in Nordamerika, Europa und im asiatisch-pazifischen Raum. Besonders bemerkenswert war das Wachstum in Japan, wo Keeper seinen jährlichen wiederkehrenden Umsatz verdreifachte und seine Präsenz in den Bereichen Finanzen, Telekommunikation, Fertigung und im öffentlichen Sektor ausbaute.

Keeper hat sein globales Vertriebsnetz durch sein erweitertes Partnerprogramm gestärkt und neue Beziehungen zu Wiederverkäufern und Distributoren in den Vereinigten Staaten, Kanada, Frankreich, Spanien, Singapur, Japan, Australien und Neuseeland aufgebaut. Das Unternehmen hat außerdem seine Präsenz im öffentlichen Sektor ausgebaut, indem es einen Platz auf der [CISA Continuous Diagnostics and Mitigation \(CDM\) Approved Product List](#) erhalten hat, sich der [Secure by Design Pledge](#) angeschlossen hat und erfahrene Sicherheitsexperten wie CISO Shane Barney, Federal Advisory Board-Mitglied David Epperson und CRO Tim Strickland willkommen geheißen hat.

Die Beiträge von Keeper in den Bereichen Produktinnovation, Identitätssicherheit und Forschung wurden das ganze Jahr über von Branchenanalysten und Award-Programmen gewürdigt. Neben dem Debüt von Keeper im Gartner Magic Quadrant hob [Enterprise Management Associates](#) (EMA) Keeper für seine einfache Bereitstellung, Architektur und Kundenzufriedenheit hervor. [GigaOm](#) ernannte Keeper zum vierten Mal in Folge zum Gesamtführenden in seinem Password Management Radar Report, und [KuppingerCole](#) würdigte Keeper als Gesamtführenden in seinem 2025 Leadership Compass Report für Non-Human Identity Management.

Keeper wurde außerdem mit den [Computing Security Awards](#), den [Cybersecurity Excellence Awards](#), den [Fortress Cybersecurity Awards](#), den [Global InfoSec Awards](#) und den [Globee Awards](#) ausgezeichnet und erhielt darüber hinaus Verbraucherauszeichnungen von [Newsweek](#), [CHIP \(DE\)](#) und [Connect Professional](#).

Branchenforschung liefert datengestützte Erkenntnisse

Keeper investiert weiterhin in Forschungsarbeiten, die sich mit den Herausforderungen und Realitäten moderner Sicherheitsteams befassen. Der Insight-Bericht von Keeper mit dem Titel „[Navigating a Hybrid Authentication Landscape](#)“ (Navigieren in einer hybriden Authentifizierungslandschaft) untersuchte, wie Unternehmen angesichts der Weiterentwicklung von Authentifizierungssystemen einen Ausgleich zwischen Passwörtern, Passkeys und hybriden Identitätsumgebungen finden.

Der Bericht „[Securing Privileged Access: The Key to Modern Enterprise Defense](#)“ (Sicherung privilegierter Zugriffe: Der Schlüssel zur modernen Unternehmensverteidigung) beschrieb detailliert die Motivationen und Herausforderungen im Zusammenhang mit der Skalierung von PAM-Programmen, einschließlich der Einführung der Cloud, der operativen Reife und der Auswirkungen privilegierter Zugriffe auf das Gesamtrisiko. Perspektiven, die direkt von Sicherheitsexperten auf drei großen Fachmessen gesammelt wurden, flossen in „[Identity, AI and Zero Trust: Cybersecurity Perspectives from Infosecurity Europe, Black Hat USA and it-sa Expo&Congress](#)“ ein und bieten einen Regionen übergreifenden Überblick darüber, wie Identität und KI die nächste Phase der Sicherheitsstrategie prägen.

Die Studie „[KI in Schulen: Balance zwischen Einführung und Risiko](#)“, die im Rahmen der Initiative „[Flex Your Cyber](#)“ von Keeper durchgeführt wurde, lieferte wichtige Daten darüber, wie Bildungseinrichtungen die Cybersicherheit im Zusammenhang mit KI in Lernumgebungen handhaben – und hob dabei besorgniserregende Lücken bei den Zugriffskontrollen und dem Sicherheitsbewusstsein hervor. Die gemeinnützige Initiative soll Schüler, Familien und Pädagogen dabei unterstützen, sich über Cybersicherheit zu informieren. Sie stellt leicht zugängliche Ressourcen bereit, die Gemeinden dabei helfen, mit neuen digitalen Risiken umzugehen und grundlegende Sicherheitsgewohnheiten zu stärken. Damit steht sie im Einklang mit der übergeordneten Mission von Keeper, die Identitätssicherheit sowohl in Unternehmens- als auch in Verbraucherumgebungen zu verbessern.

Identitätssicherheit auf globaler Ebene

Die Partnerschaft zwischen Keeper und Atlassian Williams Racing trug weiterhin dazu bei, Identitätssicherheit in Hochleistungsumgebungen zu gewährleisten, in denen Datenintegrität

und blitzschnelle Entscheidungen von entscheidender Bedeutung sind. [Keeper und Williams verlängerten ihre mehrjährige Vereinbarung](#) in diesem Jahr und bekräftigten damit ihr gemeinsames Engagement für die Sicherheit der Daten, Systeme und Wettbewerbsinformationen, die den modernen Formel-1-Betrieb ermöglichen.

Um die Authentizität der Partnerschaft zu unterstreichen, implementierte das Team KeeperPAM zum Schutz sensibler technischer und leistungsbezogener Informationen in Strecken- und verteilten Umgebungen und trug so zum Schutz kritischer Systeme bei, auf die sich Renningenieure, Strategen und Support-Teams verlassen. Während der gesamten Saison wurden [Co-Branding-Inhalte](#) mit den Fahrern Carlos Sainz und Alex Albon, Teamchef James Vowles und Craig Lurey, CTO und Mitbegründer von Keeper, veröffentlicht, um einem weltweiten Formel-1-Publikum auf anschauliche und ansprechende Weise Konzepte der Identitätssicherheit näherzubringen.

Keeper war stolz darauf, das Team während einer herausragenden Saison zu unterstützen. Im Jahr 2025 belegte Atlassian Williams Racing den fünften Platz in der Konstrukteurswertung und machte damit einen bedeutenden Schritt nach vorne in der Wiederbelebung des Teams. Dazu gehörten zwei Podiumsplätze, wobei die Fahrer Albon und Sainz den achten bzw. neunten Platz in der Fahrerwertung belegten und damit ihre konstante Leistung und Dynamik während des gesamten Jahres unter Beweis stellten.

Ein Blick auf das kommende Jahr

Keeper startet ins Jahr 2026 mit dem Ziel, Unternehmen dabei zu unterstützen, jeden Benutzer, jedes Gerät und jede Verbindung durch einen einheitlichen Zero-Trust- und Zero-Knowledge-Tresor zu schützen. Aufbauend auf einem Jahr bedeutender Innovationen, globalem Wachstum und erweiterter Forschung wird das Unternehmen weiterhin KI-gesteuerte Funktionen vorantreiben, privilegierte Zugriffskontrollen stärken und Kunden unterstützen, da Identitätssicherheit sowohl für Einzelpersonen als auch für Unternehmen weltweit immer wichtiger wird.

„Mit Blick auf das Jahr 2026 bleiben wir unserem Engagement für die Förderung von Zero-Trust-Cybersicherheit treu und unterstützen Unternehmen dabei, sich selbstbewusst gegen moderne Bedrohungen zu verteidigen“, so Guccione. „Die Identität steht im Mittelpunkt jeder Angriffsfläche, und Keeper setzt sich kompromisslos für ihren Schutz ein. Wir werden weiterhin innovative Funktionen bereitstellen, die den privilegierten Zugriff stärken, die Sicherheit für Benutzer und Teams vereinfachen und sicherstellen, dass unsere Kunden trotz immer häufigerer und ausgefeilter Cyberbedrohungen mit Zuversicht arbeiten können – unterstützt durch die Leistungsfähigkeit der KI.“

###

Über Keeper Security:

Keeper Security verändert die Cybersicherheit für Millionen von Einzelpersonen und Tausende von Unternehmen weltweit. Die intuitive Cybersicherheitsplattform von Keeper ist mit einer End-to-End-Verschlüsselung ausgestattet und genießt das Vertrauen von Fortune-100-Unternehmen, um jeden Benutzer auf jedem Gerät und an jedem Standort zu schützen. Unsere patentierte Zero-Trust- und Zero-Knowledge-Lösung für das Privileged Access

Management vereint die Verwaltung von Unternehmenspasswörtern, Geheimnissen und Verbindungen mit Zero-Trust-Netzwerkzugriffen und Remote-Browser-Isolation. Durch die Kombination dieser wichtigen Identitäts- und Zugriffsverwaltungskomponenten in einer einzigen cloudbasierten Lösung bietet Keeper beispiellose Transparenz, Sicherheit und Kontrolle und gewährleistet gleichzeitig die Einhaltung von Compliance- und Audit-Anforderungen. Erfahren Sie unter [KeeperSecurity.com](https://www.KeeperSecurity.com), wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Folgen Sie Keeper auf [Facebook](#) [Instagram](#) [LinkedIn](#) [X](#) [YouTube](#) [TikTok](#)

Pressekontakt für Keeper in DACH:

Alexandra Schmidt, +49 170 387 10 64

Thilo Christ, +49 171 622 06 10

keeper@tc-communications.de