KEEPER | Pressemitteilung

Keeper Security präsentiert optimiertes KeeperPAM und definiert Privileged Access Management mit Zero-Trust-Sicherheit neu

KeeperPAM bietet Unternehmen eine robuste Zero-Trust-Infrastruktur, um privilegierten Zugriff zu verwalten und Cyberrisiken zu minimieren.

MÜNCHEN, 18. Februar 2025 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Passwörtern, Passkeys, privilegiertem Zugang und Remote-Verbindungen, präsentiert die nächste Generation seiner Privileged Access Management (PAM)-Plattform, KeeperPAM®. Mit der neuen Version wird eine vollständig cloud-native Lösung eingeführt, die alle PAM-Prozesse nahtlos in den verschlüsselten Keeper-Tresor integriert. Dieses einheitliche System bietet maximale Sicherheit, Einfachheit und Skalierbarkeit und ermöglicht es Unternehmen, privilegierte Anmeldedaten und Geheimnisse sicher auf einer einzigen Plattform zu verwalten.

Da privilegierte Konten ein Hauptziel von Cyberkriminellen sind, ist die Implementierung einer robusten PAM-Lösung unerlässlich. 80 Prozent der Unternehmen, die PAM-Lösungen einsetzen, berichten von einer deutlichen Reduktion erfolgreicher Angriffe im Zusammenhang mit gestohlenen oder missbrauchten Anmeldedaten. KeeperPAM baut auf dem Ansatz mit einem integrierten Zero-Trust-Sicherheitsmodell auf und stellt sicher, dass nur verifizierte, autorisierte Benutzer auf kritische Systeme zugreifen können. Die Zero-Knowledge-Architektur gewährleistet dabei vollständigen Datenschutz. KeeperPAM hebt die Sicherheit privilegierter Zugriffe durch fortschrittliche Automatisierung und Echtzeitüberwachung auf ein neues Niveau: Jeder Zugriffsversuch wird dynamisch verifiziert, Anmeldedaten sicher gespeichert und privilegierte Sitzungen lückenlos überwacht.

Hauptfunktionen von KeeperPAM

- **Zero-Trust-Authentifizierung:** Jede Zugriffsanfrage wird dynamisch überprüft, um sicherzustellen, dass nur vertrauenswürdige Benutzer auf sensible Systeme zugreifen.
- **Sicheres Speichern:** Anmeldedaten werden verschlüsselt im Keeper-Tresor abgelegt und sind vor Diebstahl geschützt.
- **Automatisierte Passwortrotation:** Passwörter privilegierter Konten werden automatisch geändert, wodurch das Risiko von Missbrauch und Diebstahl minimiert wird.
- **Sicherer Fernzugriff:** Agentenlose, Zero-Trust-Verbindungen zu Infrastrukturen und webbasierten Ressourcen direkt aus dem Keeper-Tresor.
- **Überwachung privilegierter Sitzungen:** Echtzeitüberwachung verhindert unbefugte Aktionen und liefert einen klaren Audit-Trail.
- **Granulare Zugriffskontrolle:** Spezifische Richtlinien für privilegierte Konten reduzieren Risiken durch das Prinzip der minimalen Rechtevergabe.

Diese Funktionen ermöglichen es Unternehmen, kritische Systeme zu schützen und die Einhaltung von Branchenstandards und Vorschriften sicherzustellen. Durch die Automatisierung manueller Prozesse und die Vereinfachung von Auditberichten steigert KeeperPAM zudem die betriebliche Effizienz. Für Branchen mit strengen Compliance-Anforderungen, wie das Gesundheitswesen oder der Finanzsektor, unterstützt KeeperPAM die Einhaltung von Vorschriften wie dem Health Insurance Portability and Accountability Act (HIPAA) oder dem Payment Card Industry Data Security Standard (PCI-DSS). Gleichzeitig reduziert es den administrativen Aufwand für das Audit- und Zugangsmanagement.

Die dynamische Authentifizierung und Sitzungsüberwachung von KeeperPAM ermöglicht es Unternehmen, ungewöhnliche Zugriffsmuster zu erkennen und sowohl auf interne als auch externe Bedrohungen schnell zu reagieren. Dank einer flexiblen und skalierbaren Architektur

können Unternehmen strenge Sicherheitskontrollen auch auf Drittanbieter, Remote-Mitarbeiter und Auftragnehmer ausweiten, ohne dabei Arbeitsabläufe zu stören.

„Sicherheit bedeutet nicht nur, auf Bedrohungen zu reagieren, sondern sie auch vorauszusehen und Schutzebenen zu schaffen“, sagt Craig Lurey, CTO und Mitbegründer von Keeper Security. „Mit KeeperPAM helfen wir Unternehmen, der Entwicklung voraus zu sein, indem wir eine Lösung bereitstellen, die sich nahtlos in ihre bestehende Sicherheitsarchitektur einfügt und ihre Fähigkeit stärkt, Bedrohungen zu bewältigen, bevor sie zu Sicherheitsverletzungen führen.“

Neues Zeitalter der Sicherheit für privilegierte Zugriffe
Da Unternehmen zunehmend auf hybride Cloud-Umgebungen umsteigen, ist der Schutz privilegierter Konten wichtiger denn je. Jüngste prominente Sicherheitsvorfälle haben die schwerwiegenden Folgen kompromittierter Zugriffsrechte deutlich gemacht, bei denen Angreifer diese Konten nutzten, um Netzwerke zu infiltrieren und sensible Daten zu stehlen. KeeperPAM begegnet dieser Herausforderung mit dem integrierten Zero-Trust-Ansatz, der jede Zugriffsanfrage überprüft und sicherstellt, dass nur explizit autorisierte Personen Zugang zu kritischen Systemen erhalten.

„Privilegierte Konten gehören heute zu den häufigsten Angriffspunkten für Cyberkriminelle, und traditionelle Sicherheitsmodelle sind unzureichend, um moderne Gegner abzuwehren“, sagt Darren Guccione, CEO und Mitbegründer von Keeper Security. „Mit KeeperPAM befähigen wir Unternehmen, resiliente Sicherheitsstrategien wie Zero Standing Privilege zu übernehmen, um strenge Kontrollmechanismen effizient umzusetzen, die Angriffsfläche zu minimieren und interne sowie externe Bedrohungen abzuwehren.“

Stärkung der Unternehmenssicherheit in einer sich wandelnden Bedrohungslandschaft
Da Cyberangriffe immer raffinierter werden, können Unternehmen sich nicht länger auf veraltete Sicherheitsmaßnahmen und Legacy-Systeme verlassen. KeeperPAM wurde speziell mit Blick auf diese modernen Bedrohungen entwickelt und bietet einen umfassenden Schutz für privilegierte Konten, ohne dabei die Benutzerfreundlichkeit zu beeinträchtigen. Unabhängig davon, ob lokale Systeme oder cloudbasierte Infrastrukturen gesichert werden müssen, ermöglicht KeeperPAM die Implementierung einer umfassenden Zugriffskontrollrichtlinie, die sich flexibel an die individuellen Anforderungen und Risikoprofile von Unternehmen anpasst.

KeeperPAM erfüllt eine Vielzahl von Branchenstandards und Vorschriften, darunter FedRAMP- und StateRAMP-Zulassungen, SOC 2 Typ II Attestierungen, FIPS 140-3 Validierungen sowie ISO 27001-, 27017- und 27018-Zertifizierungen. Diese Standards garantieren, dass die Lösungen den höchsten Anforderungen an Datenschutz, Privatsphäre und Sicherheit entsprechen und Unternehmen die Gewissheit bieten, dass ihre Lösung für das Management privilegierter Zugriffe auf branchenführenden Sicherheitsstandards basiert.

Weitere Informationen zu KeeperPAM und wie es Ihrem Unternehmen helfen kann, die Sicherheit privilegierter Zugriffe zu stärken, finden Sie unter www.keepersecurity.com.

###

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, 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