Pressemitteilung

Keeper Security erweitert Privileged Access Management Browser-Isolation für fortschrittliche Web-Browsing-Workflows

Neue Funktionen beseitigen Nutzungsbarrieren durch Unterstützung von Multi-Tab-Browsing, sicheren Datei-Uploads/Downloads und KeeperAI-Bedrohungserkennung innerhalb privilegierter Vault-Sitzungen

MÜNCHEN, 9. April 2026 – Keeper Security, eine führende Zero-Trust- und Zero-Knowledge-Plattform für Privileged Access Management (PAM), kündigt heute die Veröffentlichung neuer Remote Browser Isolation (RBI)-Funktionen innerhalb von KeeperPAM an. Diese sind in Keeper Vault 17.6 und KCM 2.24 verfügbar und bieten bedeutende Verbesserungen bei der Akzeptanz und Benutzerfreundlichkeit für moderne Web-Workflows innerhalb privilegierter Vault-Sitzungen. Diese Erweiterungen adressieren eine anhaltende Herausforderung in Zero-Trust-Umgebungen: die Möglichkeit von sicherem, richtlinienbasiertem Zugriff auf dynamische, Multi-Tab-Webanwendungen und dateibasierte Workflows direkt innerhalb privilegierter Sitzungen. Mit der Unterstützung für Multi-Tab-Browsing, sichere Datei-Uploads und volle JavaScript-Interaktion schließt Keeper die Lücke zwischen Sicherheit und Produktivität beim Remote-Zugriff über den Browser.

Zusätzlich erweitert Keeper seine KI-gestützten Funktionen für die Sitzungsüberwachung auf weitere Protokolle, einschließlich RBI. Diese Sitzungen können mithilfe von KeeperAI kontinuierlich analysiert, zusammengefasst und in Echtzeit bewertet werden, um anomales Verhalten zu erkennen und sicherzustellen, dass die Aktivitäten im Rahmen der zugewiesenen privilegierten Aufgaben bleiben.

„Viele Organisationen setzen Remote Browser Isolation nur selektiv ein, da traditionelle RBI moderne Web-Workflows unterbricht und Benutzer gezwungen sind, Kontrollen zu umgehen, wenn Aufgaben unpraktisch werden“, sagt Craig Lurey, CTO und Mitbegründer von Keeper Security. „Die Aktualisierungen von Keeper beseitigen die häufigsten Herausforderungen und stellen sicher, dass Benutzer ein nahtloses Erlebnis haben, während gleichzeitig eine kontinuierliche Überwachung und intelligente Bedrohungserkennung in jeder privilegierten Sitzung ermöglicht wird.“

KeeperPAMs RBI ermöglicht den sicheren, effizienten und VPN-losen Zugriff auf cloudbasierte und interne Webanwendungen direkt aus dem Keeper Vault. Durch das Hosting von Browsing-Sitzungen in einer kontrollierten Remote-Umgebung isoliert RBI Web-Browsing-Aktivitäten von den Endgeräten der Benutzer und minimiert damit das Risiko von Datenexposition, falls ein Gerät kompromittiert wird. Alle Sitzungen sind vollständig in die privilegierten Zugriffs-Workflows von Keeper integriert und bieten zentrale Sichtbarkeit, Prüfbarkeit und KI-gestützte Risikoanalyse.

Wichtige Funktionen von RBI umfassen:

- **Sicherer Zugriff ohne VPN:** Sicheres Aufrufen nicht gehärteter Websites und Tools ohne die Notwendigkeit eines VPN.

- **Aufgezeichnete Web-Sitzungen:** Erfüllung von Compliance- und Prüfungsanforderungen durch vollständig aufgezeichnete Website-Interaktionen sowie volle Sichtbarkeit und Kontrolle der Sitzungen.
- **Kontrolliertes Web-Browsing:** Bereitstellung des Zugriffs auf eine vorab genehmigte Liste von URLs innerhalb einer sicheren Browser-Umgebung.
- **Automatische Passwort-Eingabe:** Automatisches Ausfüllen von Anmelde- und Passwortdetails in isolierten Browsersitzungen, ohne dass Anmeldedaten jemals an das Gerät des Benutzers übertragen werden.
- **KI-gestützte Sitzungsüberwachung:** Nutzung von KeeperAI zur Analyse der Sitzungsaktivitäten in Echtzeit, Erstellung von Zusammenfassungen und Erkennung anomalen oder nicht autorisierten Verhaltens.

Remote Browser Isolation, die mit realen Webanwendungen funktioniert
Traditionell haben RBI-Lösungen erhebliche Nutzbarkeitsbeschränkungen, was die Akzeptanz einschränkte und einige Benutzer dazu veranlasste, Kontrollen zu umgehen, wenn Workflows zu restriktiv wurden. Die neueste Aktualisierung der RBI-Funktionen in KeeperPAM adressiert diese Herausforderungen.

Die Unterstützung mehrerer Tabs innerhalb von RBI-Sitzungen ermöglicht es Benutzern, mehrere Tabs und Fenster innerhalb einer einzelnen isolierten Browsersitzung zu öffnen und zu navigieren. Dies gestattet eine nahtlose Interaktion mit modernen Webanwendungen, einschließlich Workflows, die auf Pop-ups, Weiterleitungen und Single Sign-On (SSO) angewiesen sind, ohne dass Sitzungen neu gestartet oder Isolationsgrenzen verletzt werden müssen. Native JavaScript-Warnungen, Eingabeaufforderungen und Bestätigungsdialoge werden nun vollständig innerhalb von RBI unterstützt, sodass Webanwendungen wie erwartet funktionieren. Benutzer können auch übermäßige oder bösartige Warnschleifen unterdrücken und behalten die Kontrolle, wenn Webseiten nicht wie erwartet funktionieren.

Alle Aktivitäten innerhalb dieser Sitzungen werden kontinuierlich von KeeperAI überwacht, sodass Sicherheitsteams sicherstellen können, dass die Benutzeraktionen mit den beabsichtigten Workflows übereinstimmen und potenziellen Missbrauch in Echtzeit erkennen können. Gemeinsam ermöglichen diese Verbesserungen es Organisationen, RBI breiter in geschäftskritischen Webzugriffsszenarien einzusetzen, Reibungsverluste zu reduzieren und gleichzeitig eine strenge Isolation von Endgeräten aufrechtzuerhalten.

Sichere Datei-Uploads, welche die Isolation nicht verletzen
KeeperPAM führt administrativ kontrollierte Datei-Uploads über Remote Browser Isolation ein und adressiert damit eine weitere häufige Einschränkung, die Benutzer bisher gezwungen hat, geschützte Umgebungen zu verlassen.

Wenn dies von Administratoren explizit aktiviert wird, können Benutzer Dateien auf zugelassene Websites direkt innerhalb einer isolierten Sitzung hochladen. Dies unterstützt Workflows wie Dokumenteneinreichungen, Video-Uploads und webbasierte Zusammenarbeit. Datei-Uploads sind standardmäßig deaktiviert und müssen bewusst pro Verbindung autorisiert werden, was das Zero-Trust-Sicherheitsmodell von Keeper stützt.

Diese Funktion ist besonders wertvoll für Organisationen, die sicheren Zugriff auf hochriskante oder extern gehostete Webplattformen benötigen, während sie gleichzeitig Malware-Exposition, Datenlecks oder Kompromittierung von Anmeldedaten auf lokalen Endgeräten verhindern.

Speziell entwickelter Zero-Trust-Zugriff
Remote Browser Isolation ist vollständig in KeeperPAM, der cloudnativen Privileged Access Management-Plattform von Keeper, integriert und kann auch als selbstgehostete, lokale Lösung bereitgestellt werden. Entwickelt von den ursprünglichen Machern von Apache Guacamole, bietet Keeper's Sitzungsmanagement-Technologie schnellen, agentenlosen Zugriff auf Infrastruktur, Webanwendungen und isolierte Browsing-Sitzungen mit vollständiger Sitzungsaufzeichnung und Zero-Knowledge-Verschlüsselung.

Durch die Weiterentwicklung der Remote Browser Isolation, um den Bedürfnissen der Benutzer gerecht zu werden, zeigt Keeper, dass starke Sicherheitskontrollen nicht auf Kosten von Benutzerfreundlichkeit oder Produktivität gehen müssen. Mit der zunehmenden Reife von Zero-Trust-Architekturen müssen Sicherheitskontrollen die Arbeitsabläufe in der Praxis unterstützen, anstatt Ausnahmen zu erzwingen.

Die RBI-Erweiterungen werden in den kommenden Wochen über Gateway 2.24 und Keeper Vault 17.6 in KeeperPAM verfügbar sein.

###

Über Keeper Security:
Keeper Security ist eines der am schnellsten wachsenden Unternehmen für Cybersicherheitssoftware, das Tausende von Organisationen und Millionen von Menschen in über 150 Ländern schützt. Keeper ist ein Pionier der Zero-Knowledge- und Zero-Trust-Sicherheit für jede IT-Umgebung. Das Herzstück, KeeperPAM®, ist eine KI-unterstützte, Cloud-native Plattform, die alle Benutzer, Geräte und Infrastrukturen vor Cyberangriffen schützt. Keeper wurde für seine Innovationen im Gartner Magic Quadrant für Privileged Access Management (PAM) ausgezeichnet und sichert Passwörter und Passkeys, Infrastrukturgeheimnisse, Remote-Verbindungen und Endpunkte mit rollenbasierten Durchsetzungsrichtlinien, Least-Privilege und Just-in-Time-Zugriff. Erfahren Sie auf KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Erfahren Sie mehr unter KeeperSecurity.com
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