KEEPER | Pressemitteilung

Neu: Zero-Knowledge Remote-Browser-Isolation im Keeper Connection-Manager

Die Sicherheit beim Surfen im Internet wird ohne die Komplexität und Latenzzeiten traditioneller VPNs auf das nächste Level gehoben.

MÜNCHEN, 26. Juni 2024 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Anmeldedaten, privilegiertem Zugang und Remote-Verbindungen, stellt heute seine Remote-Browser-Isolation als neue Komponente im Keeper Connection Manager vor. Die Remote-Browser-Isolation bietet Anwendern über jedem Standard-Webbrowser einen sicheren Zugriff auf webbasierte Ressourcen wie beispielsweise interne Web- oder Cloud-Anwendungen.

Der Keeper Connection Manager bietet Teams den sofortigen Zugriff auf RDP-, SSH-, Datenbanken, Web-Applikationen und Kubernetes-Endpunkte über einen sicheren Webbrowser. Entwickelt von dem Team, das Apache Guacamole erstellt hat, wird Keeper als Container in jeder Umgebung bereitgestellt, um einen nahtlosen und sicheren Zugriff, ohne die Notwendigkeit eines VPNs, zu ermöglichen.

Mit dem neuesten Update unterstützt der Keeper Connection Manager nun das Starten von Web-Sitzungen direkt innerhalb der Oberfläche des Connection Managers mithilfe der Remote Browser Isolation-Technologie. Genau wie bei jedem anderen Verbindungstyp des Keeper Connection Managers können diese Sitzungen in Echtzeit geteilt, aufgezeichnet und überprüft werden.

Die Remote Browser Isolation von Keeper injiziert sicher und automatisch Anmeldedaten, sendet Formulare und steuert die Ziel-Webanwendung, ohne die Anmeldedaten jemals an das Gerät des Benutzers zu senden. Keeper ist mit allen Desktop- und mobilen Webbrowsern kompatibel, einschließlich Chrome, Edge, Safari, Opera, Firefox und Brave.

„Typischerweise müssen Unternehmen VPNs oder Cloud-basierte ZTNA-Produkte verwenden, um Zugang zu internen Webanwendungen oder Cloud-basierten Apps zu bieten", sagt Craig Lurey, CTO und Mitbegründer von Keeper Security. „Mit dieser neuen Funktion können Organisationen nun einen Keeper Connection Manager-Container einfach in jeder lokalen oder Cloud-Umgebung bereitstellen und ihren Benutzern und Auftragnehmern sicheren Remote-Zugriff auf Web-Ressourcen bieten. Die Benutzererfahrung ist so nahtlos, dass die Nutzer nicht einmal merken, dass sie sich in einem virtualisierten Browser befinden."

Da der Keeper Connection-Manager als Container in jeder beliebigen Umgebung eingesetzt werden kann, haben Unternehmen die vollständige Kontrolle über den Netzwerkverkehr sowie die Laufzeitumgebung der Remote-Browser-Isolation. Der gesamte Prozess basiert auf dem Zero-Knowledge-Prinzip, das gewährleistet, dass der Prozess niemals über das Netzwerk eines Drittanbieters läuft.

Zusätzlich zu den Vorteilen des sicheren Zugriffs auf webbasierte Anwendungen bietet die Funktion der Remote-Browser-Isolation von Keeper einen weiteren Schutz vor Cyber-Bedrohungen, die von bösartigen Websites ausgehen. Die Website wird niemals lokal auf dem Gerät des Benutzers ausgeführt, sodass der Benutzer gegen viele verschiedene Angriffsvektoren wie Cross-Site-Scripting-Schwachstellen, Cross-Site-Request-Forgery und API-Missbrauch immun ist.

Administratoren können steuern, auf welche Webanwendungen über den Connection-Manager zugegriffen werden können, und sie haben die Möglichkeit, bestimmte Websites und Domänen zuzulassen oder zu verbieten. Keeper integriert sich mit OIDC und SAML 2.0, um Benutzer sicher zu authentifizieren und den Zugriff auf die Ziel-Web-Sitzung zu kontrollieren, selbst wenn die Anwendung Single Sign-On (SSO) nicht unterstützt. Mehrere Methoden der Multi-Faktor-Authentifizierung (MFA) stehen zur Verfügung, und der öffentliche Sektor kann CAC/PIV zur Authentifizierung verwendet werden.

Remote-Browser-Isolation ist die neueste Erweiterung von KeeperPAM, der benutzerfreundlichen und skalierbaren PAM-Lösung, welche die Art und Weise verändert, wie sich Organisationen – unabhängig von deren Größe - in einer Welt verteilter Arbeitsplätze und von Multi-Cloud-Computing vor Cyber-Angriffen schützen können. Der Passwortmanager und Privileged Access Manager der Keeper Security Government Cloud ist FedRAMP- und StateRAMP-autorisiert und unterstützt das Zero-Trust-Sicherheitsframework von Keeper Security zusammen mit einer Zero-Knowledge-Sicherheitsarchitektur, so dass die Anwender vollständige Kenntnis, Verwaltung und Kontrolle über ihre Anmeldedaten und Verschlüsselungsschlüssel haben.

Entdecken Sie, wie die Remote Browser Isolation-Lösung von Keeper die Art und Weise revolutioniert, wie Unternehmen sensible Daten schützen und gleichzeitig eine ununterbrochene Produktivität gewährleisten.

###

Über Keeper Security:
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die erschwinglichen und benutzerfreundlichen Lösungen von Keeper basieren auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer auf jedem Gerät zu schützen. Unsere Privileged-Access-Management-Lösung der nächsten Generation ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in jede Technologieumgebung integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern sowie Tausenden von Unternehmen und ist der führende Anbieter von erstklassigem Passwort- und Passkey-Management, Geheimnisverwaltung, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging.

Erfahren Sie mehr unter KeeperSecurity.com
Folgen Keeper: Facebook Instagram LinkedIn X YouTube

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de