



Keeper stellt Risikomanagement-Dashboard für hohe Risikotransparenz und aktive Bedrohungsabwehr vor

Das Dashboard bietet Administratoren einen Überblick über die Sicherheitspraktiken und die Compliance-Situation des Unternehmens, unterstützt durch dynamische Benchmarks und Risikobewertungen in Echtzeit.

MÜNCHEN, 3. Dezember 2024 – [Keeper Security](#), ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Passwörtern, Passkeys, privilegiertem Zugang und Remote-Verbindungen, stellt heute sein Risk Management Dashboard vor. Diese neue Funktion innerhalb der Keeper Admin Console ermöglicht Administratoren einen umfassenden Einblick in die Sicherheitspraktiken und die Compliance-Situation des Unternehmens und setzt damit einen neuen Standard für ein rationalisiertes Cybersecurity-Management.

Das Risk Management Dashboard beinhaltet eine intuitive Risikobewertung. Diese basiert auf den wichtigsten Metriken, die das Risikoprofil des Unternehmens beeinflussen – einschließlich des Einsatzes von Anwender-Tresoren, der Verwendung von Passwort-Management-Tools und der Multi-Faktor-Authentifizierung. Auch in unterschiedlichen Sicherheitslandschaften passt sich das Dashboard automatisch an Single Sign-On (SSO)-Umgebungen an und gewährleistet so ein maßgeschneidertes Risikomanagement.

Vereinfachte Sicherheits-Benchmarks

Da sich Sicherheitsbedrohungen schnell weiterentwickeln, nutzt das Risk Management Dashboard von Keeper einen dynamischen Satz von [Keeper Security Benchmarks](#). Diese Benchmarks werden laufend aktualisiert, um die neuesten Sicherheitsstandards zu reflektieren und helfen Unternehmen, das Prinzip der geringsten Privilegien durchzusetzen und die Sicherheit auf höchstem Niveau zu halten. Administratoren erhalten umsetzbare, leicht zu befolgende Schritte, um Sicherheitslücken zu schließen und den Schutz von Anmeldeinformationen zu verbessern.

Die Integration mit dem Advanced Reporting and Alerts Module (ARAM) von Keeper erweitert die Funktionalität des Dashboards um detaillierte Ansichten von Sicherheitsereignissen. Dazu gehören:

- Kuratierte Ansicht der kritischsten Sicherheitswarnungen
- Häufigkeit des Auftretens
- Einzigartige Benutzeraktivitäten
- 30-Tage-Trends

Mit diesem Grad an Detailinformationen erhalten Administratoren tiefe Einblicke in die Sicherheit von Anmeldeinformationen sowie potenzielle Bedrohungen. Dies ermöglicht es Unternehmen, Schwachstellen aktiv zu beheben und eine stabile Sicherheitslage aufrechtzuerhalten.

„Unser neues Risk Management Dashboard stellt einen bedeutenden Fortschritt in der Art und Weise dar, wie Unternehmen ihre Sicherheitslage verwalten und visualisieren können.“

Durch die Integration von dynamischen Benchmarks und Echtzeit-Risikobewertungen bieten wir Administratoren entscheidende Einblicke und Empfehlungen, die sie für das Entschärfen von Sicherheitsbedrohungen benötigen und die Einhaltung von Vorschriften zu gewährleisten", sagt Craig Lurey, CTO und Mitbegründer von Keeper Security. „Diese Innovation unterstreicht unser Engagement, hochmoderne Sicherheitslösungen zu liefern, die sowohl technisch robust als auch benutzerorientiert sind, um die Bedürfnisse unserer Kunden zu erfüllen."

Erweiterungen durch Kunden-Feedback

Das Risk Management Dashboard ist die jüngste in einer Reihe von Verbesserungen, die durch das Feedback der Kunden (Voice of the Customer, VoC) angeregt wurden. Die Verpflichtung, auf die Bedürfnisse der Benutzer einzugehen, ist die Grundlage dafür, dass Keeper weiterhin Informationen intelligent umsetzt und eine hohe Benutzerfreundlichkeit bietet.

Erfahren Sie hier mehr über das [Risk Management Dashboard](#) von Keeper.

###

Über Keeper Security:

Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die intuitiven Lösungen von Keeper basieren auf einer End-to-End-Verschlüsselung, um jeden Anwender auf jedem Gerät und an jedem Standort zu schützen. Die Keeper Zero-Trust-Plattform für die Verwaltung von privilegierten Zugängen ist in wenigen Minuten einsatzbereit. Sie lässt sich nahtlos in jeden Technologie-Stack integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern und Tausenden von Unternehmen und ist führend bei der Verwaltung von Passwörtern, Passkeys und Geheimnissen, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Erfahren Sie, wie die Zero-Trust- und Zero-Knowledge-Lösungen vor Cyber-Bedrohungen schützen auf 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