ENDPOINT PRIVILEGE MANAGER

Implementieren Sie Zugriffsrichtlinien mit den geringsten Rechten, eliminieren Sie bestehende Administratorrechte und ermöglichen Sie Just-in-Time-Zugriff (JIT) sowohl auf Prozess- als auch auf Maschinenebene mit Endpunktrechteverwaltung für Windows-, Linux- und macOS-Endpunkte.

Robuste privilegierte Zugriffskontrollen sind für Unternehmen unerlässlich, um ihre Sicherheitslage zu stärken, die betriebliche Effizienz sicherzustellen und gesetzliche Compliance-Anforderungen zu erfüllen.

Der Endpoint Privilege Manager von Keeper sichert Endpunkte durch schlanke Agenten, die bestehende Administratorrechte entfernen und nur bei Bedarf eine vorübergehende, richtlinienbasierte Erhöhung von Berechtigungen ermöglichen. Das System setzt anpassbare Sicherheitsrichtlinien durch JIT-Zugriff mit optionalen Genehmigungsworkflows und der Durchsetzung der Multi-Faktor-Authentifizierung (MFA) durch.

Privilegierte Aktionen können entweder über kurzlebige Konten ausgeführt werden, die für jede Sitzung automatisch bereitgestellt und deren Bereitstellung aufgehoben wird, oder durch vorübergehendes Erhöhen von Berechtigungen für Standardbenutzerkonten. Unternehmen können je nach Sicherheitslage und betrieblichen Anforderungen eine der beiden Methoden auswählen.

Keeper Endpoint Privilege Manager funktioniert in Windows-, macOS- und Linux-Umgebungen und bietet Transparenz über ein zentrales Dashboard, das alle Erhöhungsaktivitäten für Auditing und Compliance protokolliert.

Vorteile von Keeper Endpoint Privilege Manager

Sicherheit

Eliminiert dauerhafte Administratorrechte und ermöglicht Just-in-Time-Erweiterungen, nur für genehmigte Anwendungen, um Angriffsflächen zu reduzieren und die Sicherheit zu verbessern.

Einhaltung

Bietet umfassende Prüfpfade für die Nutzung von Berechtigungen und stellt die Einhaltung gesetzlicher Anforderungen durch dokumentierte administrative Zugriffskontrolle sicher.

Betriebliche Effizienz

Reduziert die Arbeitsbelastung des Helpdesks durch die Automatisierung von Genehmigungen für routinemäßige Verwaltungsaufgaben.

Benutzererfahrung

Ermöglicht es Benutzern, notwendige Aufgaben ohne IT-Verzögerungen durch automatische Erhöhung von Berechtigungen für genehmigte Anwendungen zu erledigen.

Skalierbarkeit

Ermöglicht es Unternehmen, Richtlinien mit den geringsten Rechten effizient durchzusetzen und privilegierten Zugriff über Tausende von Windows-, macOS- und Linux-Endpunkten von einer zentralen Plattform aus zu verwalten.

Überprüfbarkeit und Transparenz

Bietet Einblicke in erhöhte Aktivitäten, Genehmigungen und die Durchsetzung von Endpunktrichtlinien mit detaillierter Protokollierung und Integration in SIEM-Tools für eine schnellere Reaktion auf Vorfälle.

Erfahren Sie mehr
keepersecurity.com

Fordern Sie eine Demo an
keeper.io/demo

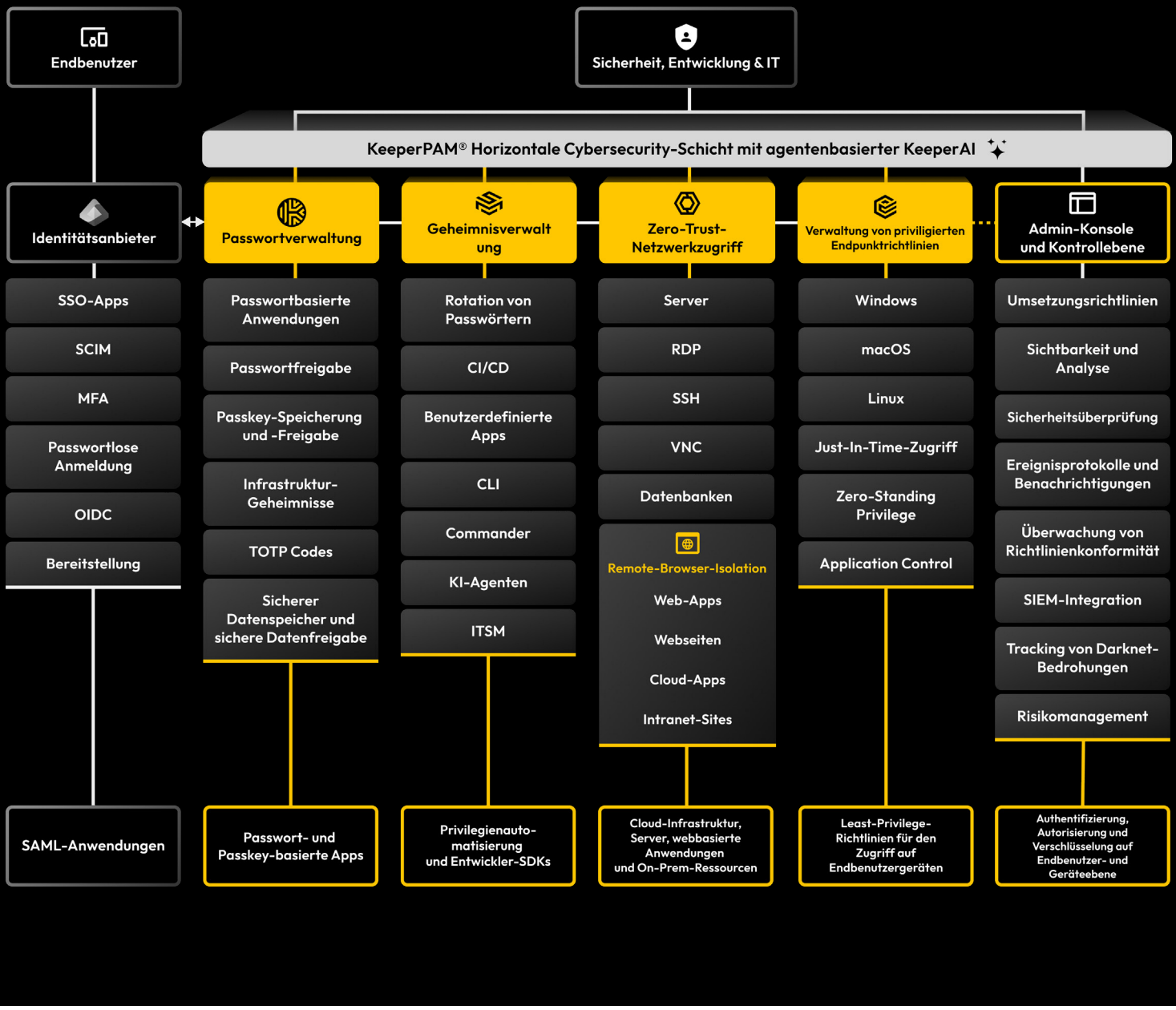
Partneranfragen
partners@keepersecurity.com

Über Keeper Security

Keeper Security verändert die Cybersicherheit für Menschen und Unternehmen auf der ganzen Welt. Die intuitiven Lösungen von Keeper sind mit End-zu-End-Verschlüsselung ausgestattet, um jeden Benutzer auf jedem Gerät und an jedem Ort zu schützen. Keeper genießt das Vertrauen von Millionen von Einzelpersonen und Tausenden von Organisationen und ist der Marktführer für Privileged Access Management.

KEEPER PAM

Keeper Privileged Access Management-Plattform



Erweitern Sie Zero-Trust auf Endpunkte

Endpoint Privilege Manager erweitert den Zero-Trust-Ansatz von KeeperPAM, indem es die Erhöhung von Berechtigungen direkt auf Endpunkten steuert und so die sicheren Verbindungsfunktionen der umfassenderen PAM-Lösung ergänzt. Während der Rest der KeeperPAM-Plattform sicherstellt, wie Benutzer sich mit Systemen verbinden, regelt Endpoint Privilege Manager, welche administrativen Rechte sie ausüben können, sobald die Verbindung hergestellt ist.

Wie Keeper Berechtigungen erhöht

1. **Richtlinie** - Wenn für eine Anwendung oder einen Prozess erhöhte Rechte erforderlich sind, überprüft der Keeper-Agent die entsprechende Richtlinie.
2. **Genehmigung** - Wenn eine Genehmigung erforderlich ist, wird die Anfrage über die Admin-Konsole oder die Befehlszeilenschnittstelle (CLI) an einen Administrator weitergeleitet.
3. **MFA-Option** - Wenn keine Genehmigung erforderlich ist, wird die Erhöhung automatisch fortgesetzt. Die MFA-Durchsetzung ist ein optionaler zusätzlicher Schritt.