

Cyberresilienz 2026 |
AERAssec GmbH & hannoverimpuls



PRIVILEGED ACCESS MANAGEMENT

PAM als zentraler Baustein moderner IAM-Strategien

VISION

”

Digitale Souveränität ist ein grundlegendes Recht für Menschen, Institutionen und die Gesellschaft.

Marcus Scharra
CEO Segura®



Aktuelle Marktsituation:

Wachsende Komplexität privilegierter Zugriffe

- Cloud- und Automatisierungsprojekte erhöhen die Anzahl privilegierter Zugriffe
- Klassische Userverwaltung allein reicht nicht mehr aus
- Maschinen, Anwendungen, IoT und DevOps erweitern die Angriffsfläche erheblich
- Unkontrollierte Zugriffe gefährden Daten- und Digitalisouveränität
- Neue Compliance-Anforderungen (u.a. NIS2, DORA, CRA, ISO) verschärfen den Handlungsdruck

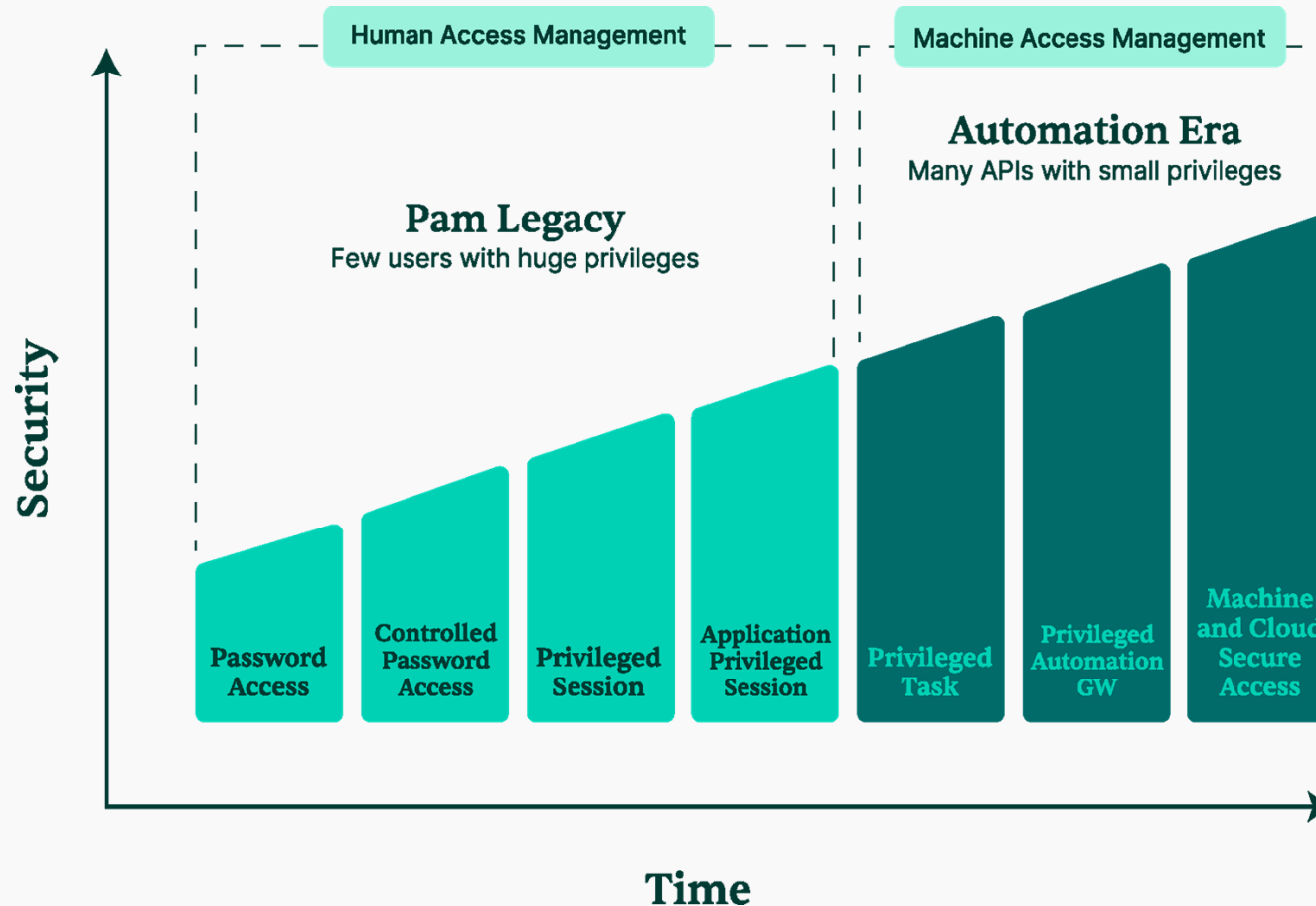


Viele Unternehmen verlieren die Kontrolle über privilegierte Identitäten und Zugriffe.



Aktuelle Marktsituation:

Die Automatisierungsära erhöht die Anzahl privilegierter Zugriffe



Neue privilegierte Zugriffe durch:

- DevOps
- API-Zugriffe / -Identitäten
- Cloud-Zugriffe
- IoT-Identitäten
- Industrie 4.0
- KI-Bots



Der nächste Schritt:

Wie lassen sich diese
Anforderungen
zuverlässig in der
Praxis umsetzen?

**PRIVILEGED
ACCESS
MANAGEMENT**



Was ist PAM?

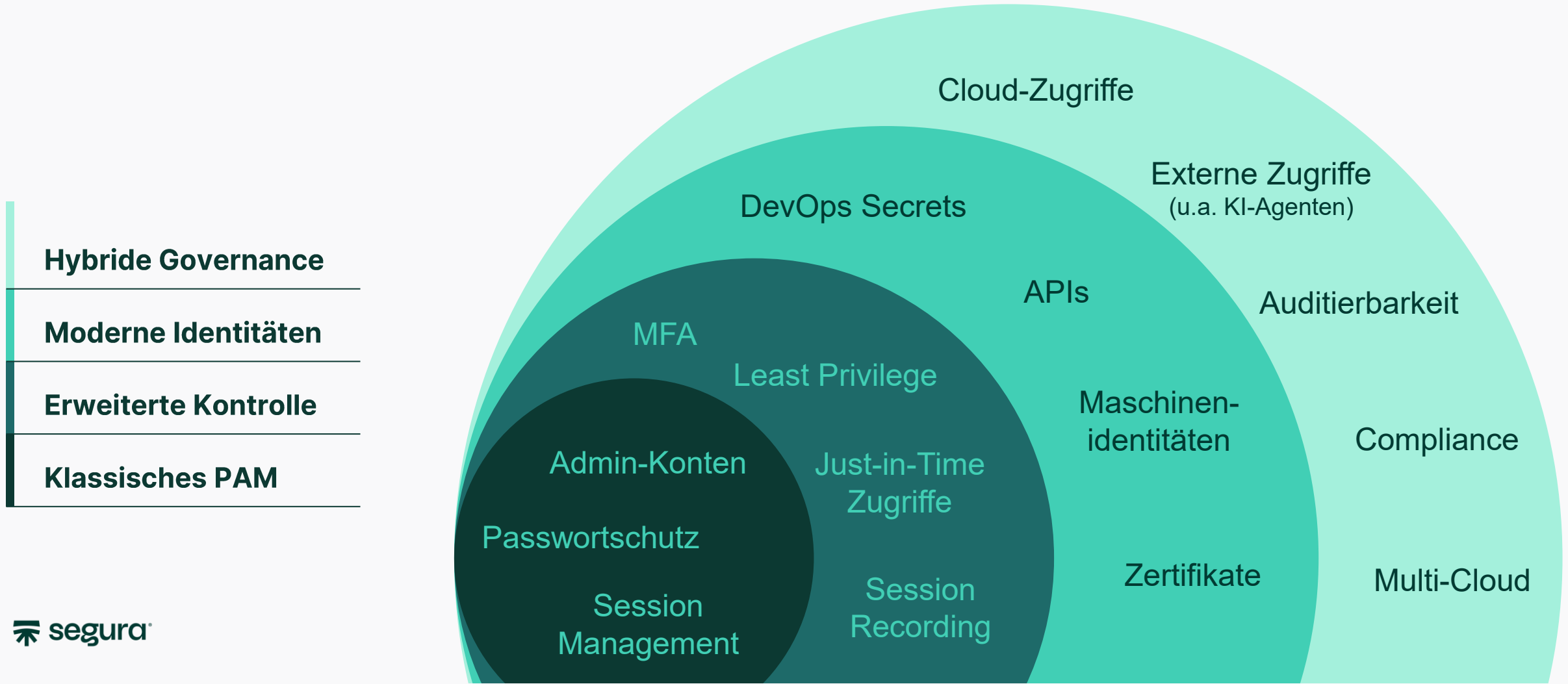
PAM schützt und kontrolliert privilegierte Zugriffe auf kritische Systeme, sensible Daten und Infrastrukturen.

- Kontrolle privilegierter Identitäten
- Sichere Zugriffssteuerung
- Überwachung privilegierter Aktivitäten
- Nachvollziehbarkeit & Auditierbarkeit



Moderne PAM-Anforderungen:

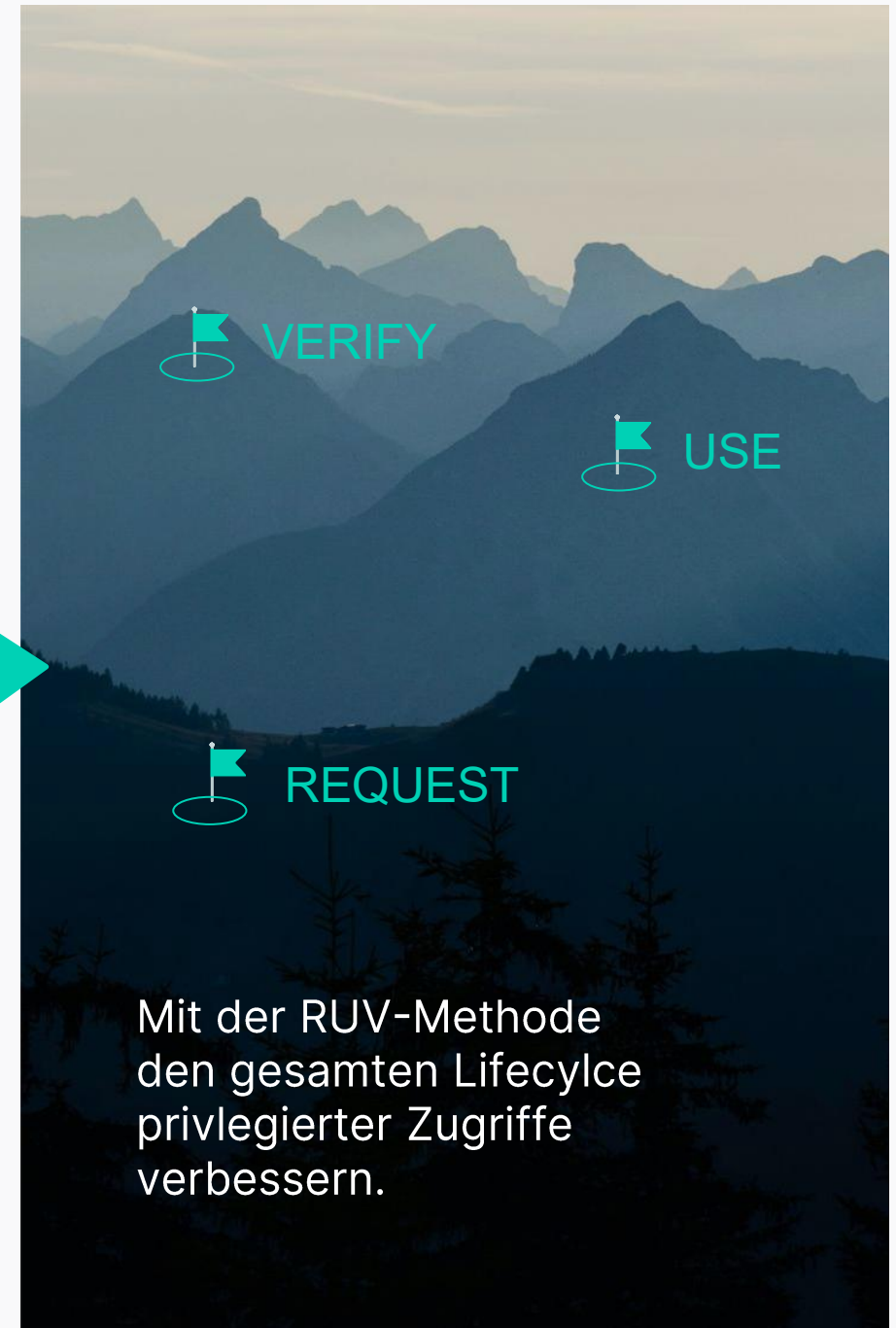
Neue Identitäten verändern die Anforderungen an PAM





Zentrale Herausforderung:

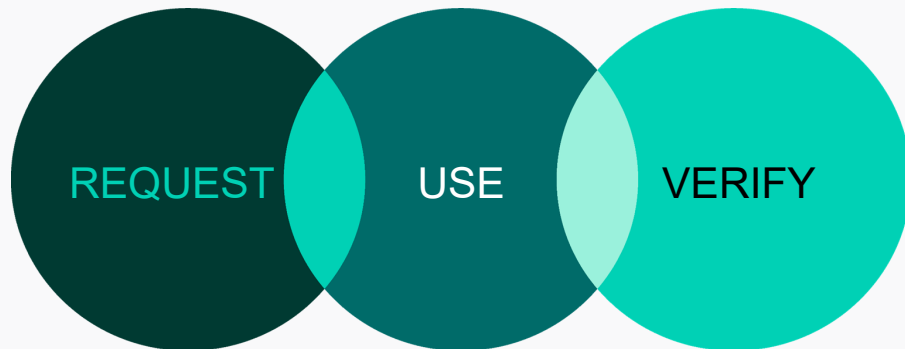
Wie lässt sich die
Komplexität
privilegierter Zugriffe
verhindern?



Mit der RUV-Methode
den gesamten Lifecycle
privilegierter Zugriffe
verbessern.



Lösungsansatz:
RUV-Methode



REQUEST:

User identifizieren & Zugriffe steuern

USE:

Zugriffe ermöglichen & verwalten

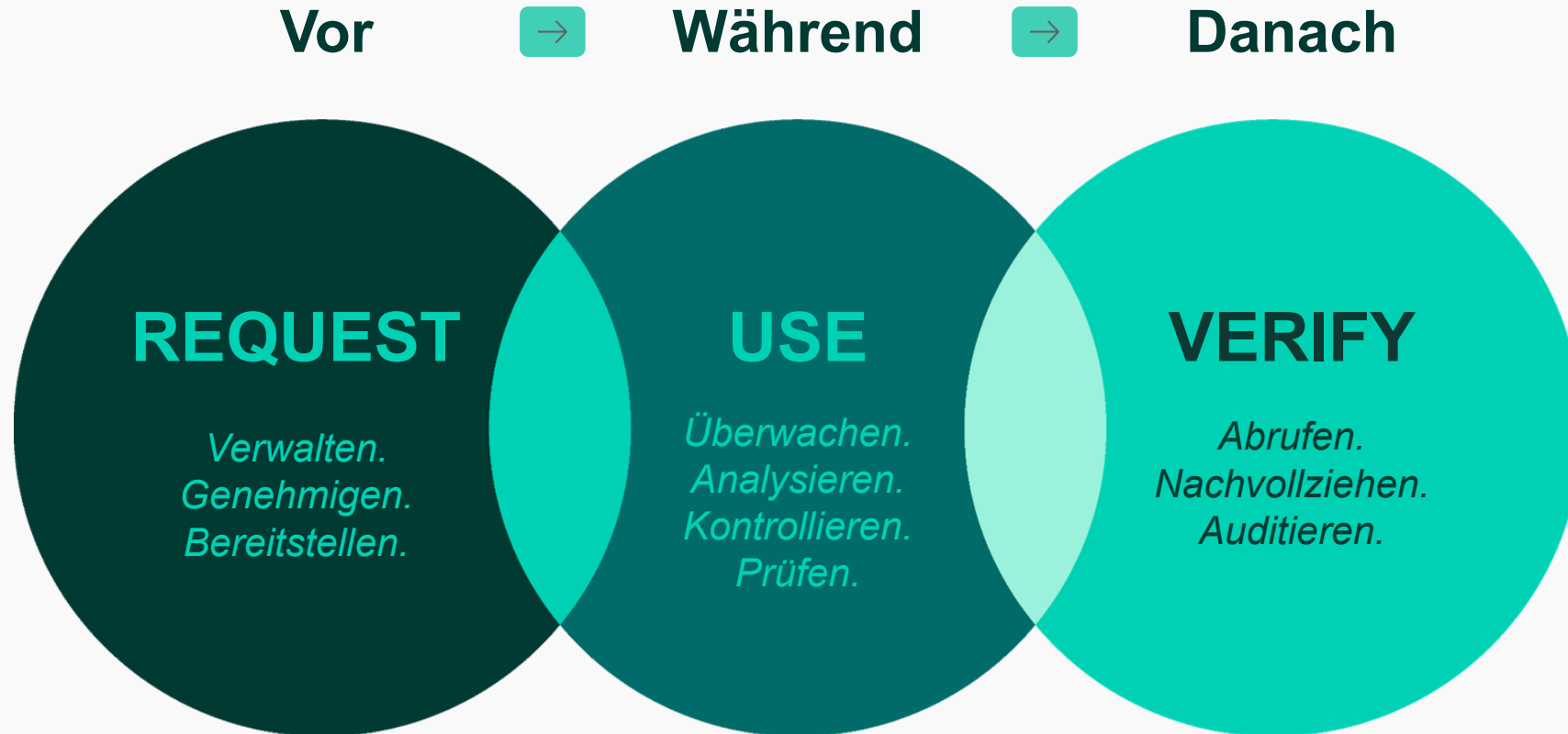
VERIFY:

Aktivitäten protokollieren & kontrollieren



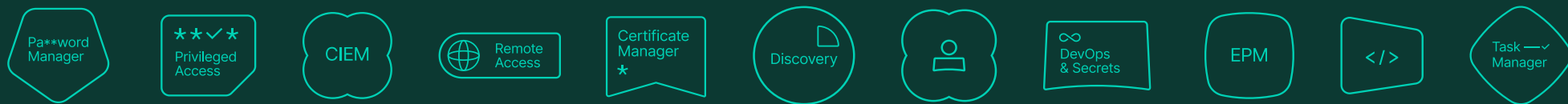
Ergebnis:

Verbesserte Sicherheit **vor**, **während** und **nach** Zugriffen





Die All-in-One Plattform für moderne PAM-Anforderungen





Kundenfeedback als Maßstab:

5x Gartner Peer Insights Customers' Choice



Gartner



Gartner



Modulübersicht: 360 Grad PAM-Plattform

PRIVILEGED ACCESS MANAGEMENT

Kontrolle, Überwachung und Audit von privilegierten Zugriffen

ZERTIFIKATSMANAGER

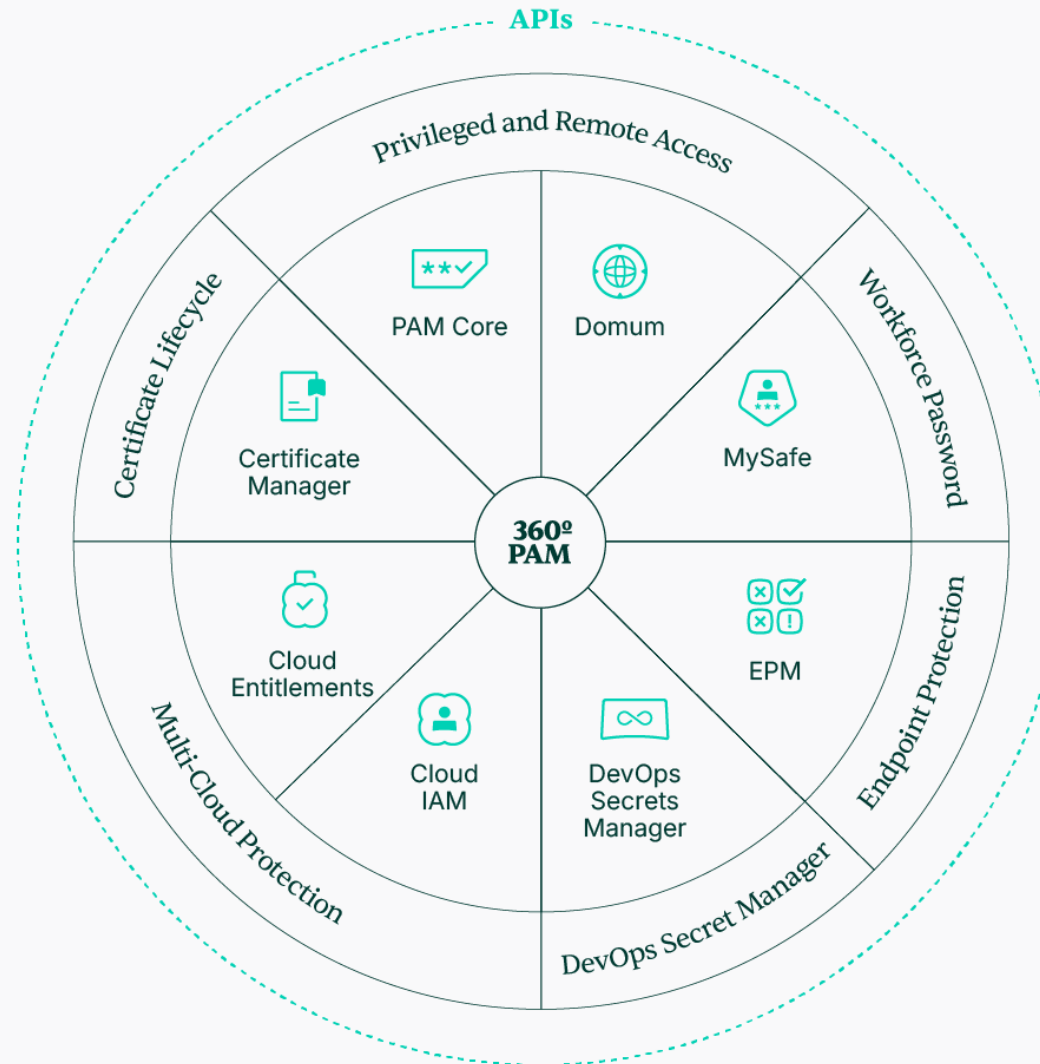
Verwaltung, automatische Erneuerung und Veröffentlichung. Erfüllt A1- und SSL-Zertifikate.

CLOUD ENTITLEMENTS

Transparenz und Kontrolle über Cloud-Berechtigungen

CLOUD IAM

Identitätsmanagement in Multi-Cloud-Umgebungen



DOMUM REMOTE ZUGRIFF

Sicherer Remote-Zugriff für externe Nutzer ohne VPN

PASSWORTMANAGER

Verwaltung starker Passwörter für Mitarbeiter und Teams

EPM WINDOWS | LINUX | MAC

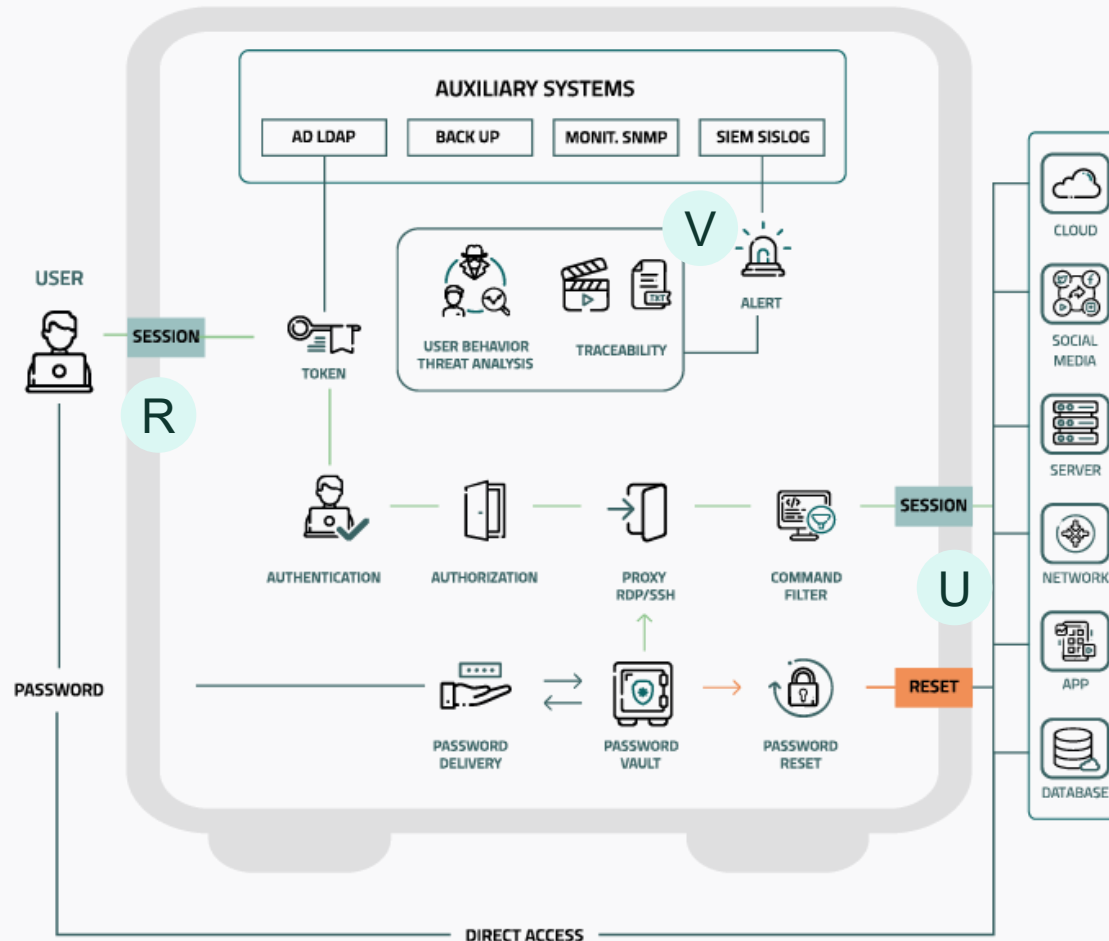
Steuerung und Erhöhung von Berechtigungen auf versch. Endpoints

DEVOPS SECRET MANAGER

Automatisierung und Sicherheit im DevSecOps-Wake



Die 360°-PAM-Plattform im Überblick: Umsetzung der RUV-Methode



R

REQUEST

- User-Authentifizierung
- Access Management & Genehmigungsworkflows
- Passwort-Management & Rotation

U

USE

- Session Management
- Unterstützte Protokolle (u.a. RDP, SSH)
- Privilegierte Remote-Zugriffe

V

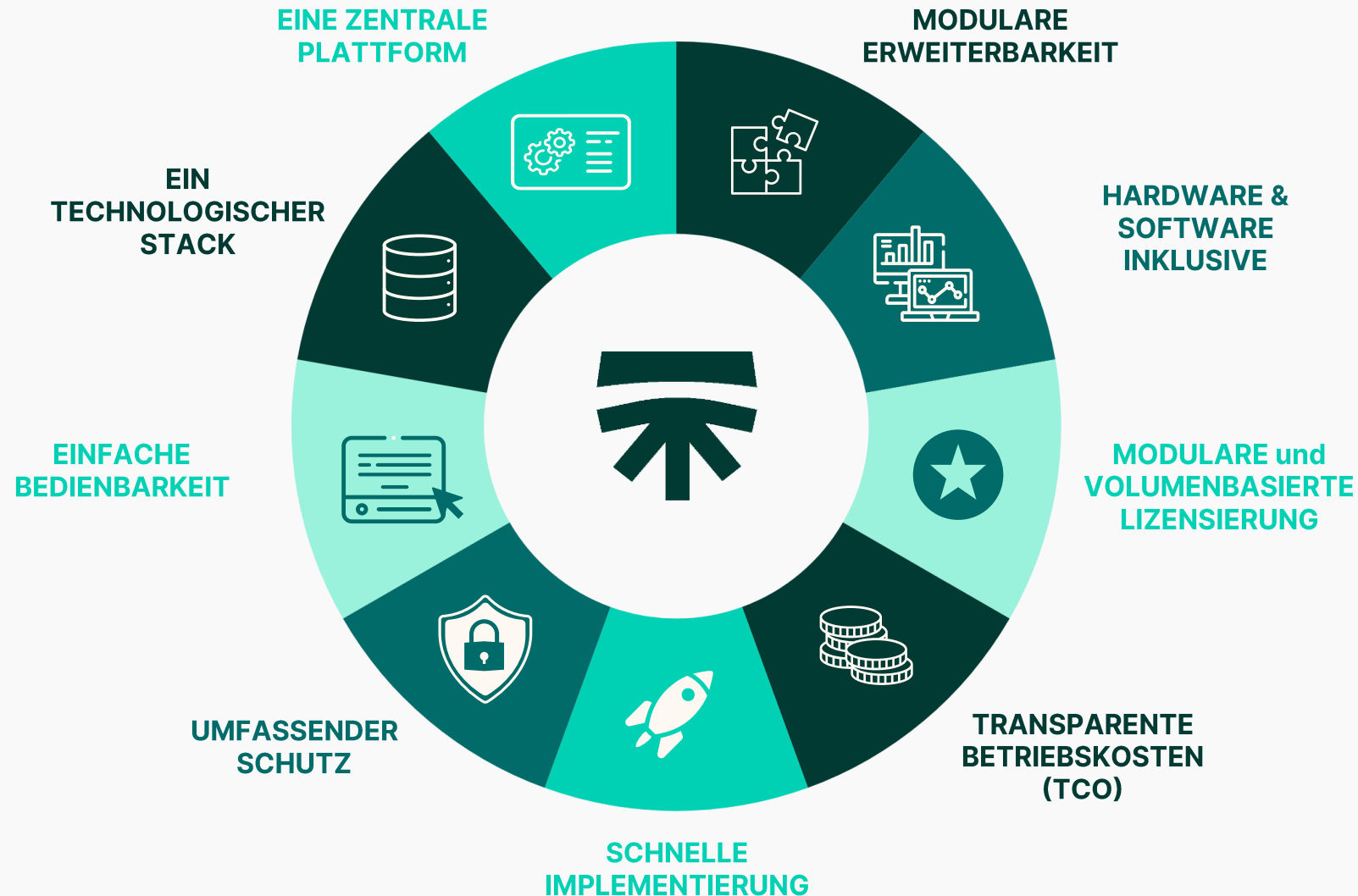
VERIFY

- Machine Learning & Alarmfunktionen
- Session-Aufzeichnung
- Auditierung & Nachvollziehbarkeit



Weniger Komplexität. Mehr Kontrolle.

Die zentrale Plattform für modernes PAM von Segura®





ALEXANDER BÖRSEL

Channel Manager DACH

DAGMA GmbH

boersel.a@dagma.eu

+49 (0) 176 6127 4571

DANKE!