



## PAM Core

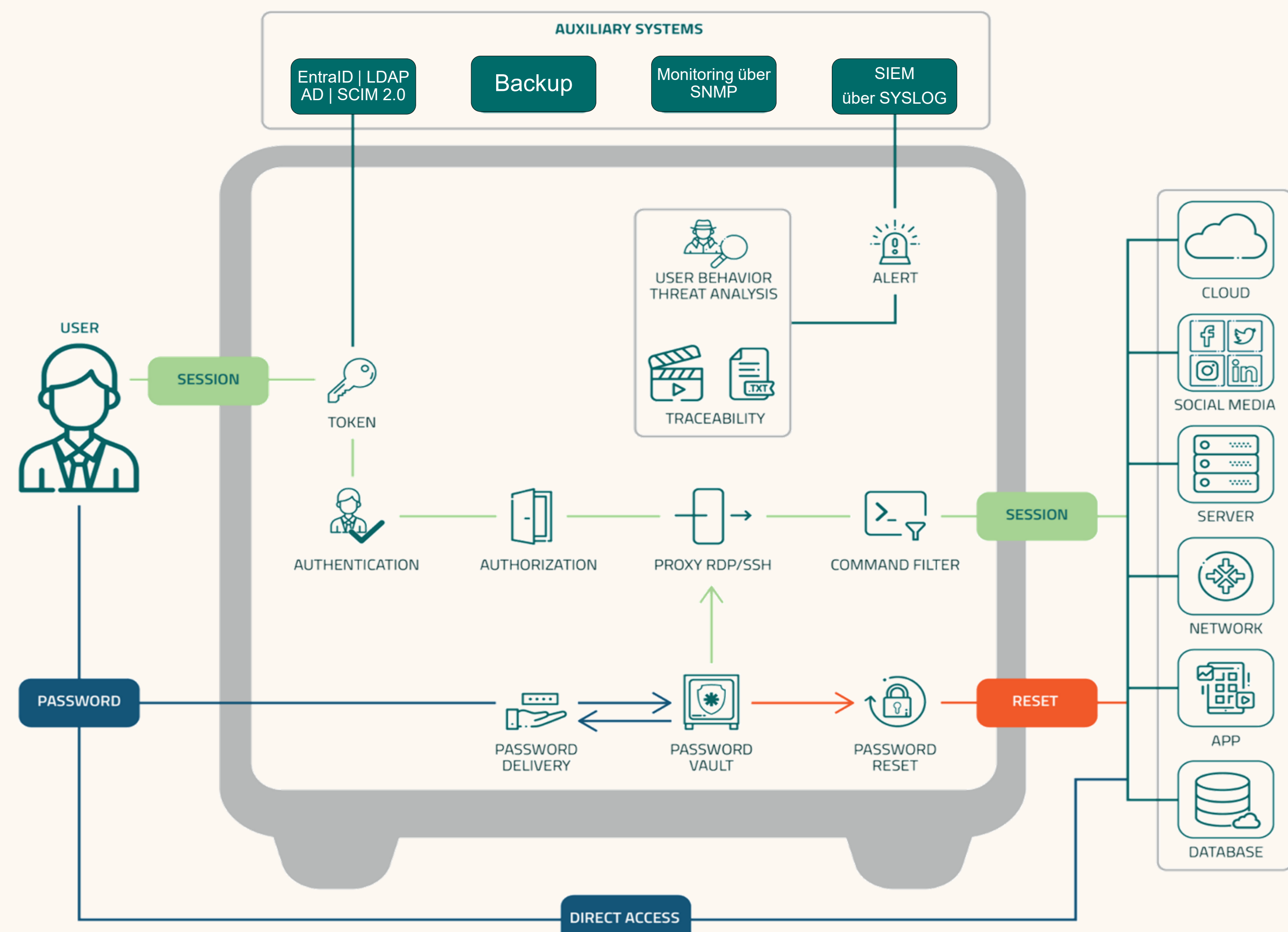
Privilegierte Zugangsdaten ermöglichen den Zugriff auf geschäftskritische Aktionen, etwa die Änderung von Domain-Controller-Einstellungen oder die Durchführung von Finanztransaktionen über Unternehmenskonten.

Dadurch zählen hochprivilegierte Zugangsdaten zu den beliebtesten Angriffszielen für Cyberkriminelle. Tatsächlich sind bereits 84 % aller Cyberangriffe identitätsbasiert.

Zusätzlich verpflichten regulatorische Vorgaben wie PCI, ISO, SOX, DSGVO, DORA und NIS-2 IT-Verantwortliche dazu, Berechtigungen regelmäßig zu überprüfen und das Prinzip der minimalen Rechtevergabe umzusetzen.

**Privileged Access Management (PAM)** dient dem Schutz und der Kontrolle generischer sowie privilegierter Zugangsdaten. Dies umfasst die sichere Speicherung, die Trennung von Zugriffen sowie die vollständige Nachvollziehbarkeit der Nutzung.

Die Implementierung von Schutzmechanismen für privilegierte Zugangsdaten ist ein zentraler Bestandteil einer ganzheitlichen Cybersicherheitsstrategie – unabhängig von Unternehmensgröße oder Branche.

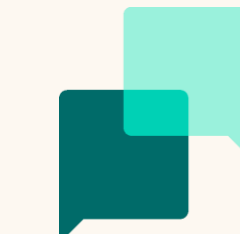


## So funktioniert eine PAM-Lösung



### Herausforderung

Unzureichende Kontrolle über privilegierte Zugangsdaten erschwert die Nachvollziehbarkeit sicherheitsrelevanter Aktivitäten und erhöht das Risiko von Cyberangriffen.



### Lösung

Zentrale Erkennung und Verwaltung aller privilegierten Zugangsdaten sowie die Etablierung eines wirksamen Prozesses für Authentifizierung, Autorisierung und Verantwortlichkeit bei deren Nutzung.



### Ergebnis

Reduzierung der Angriffsfläche durch die Eliminierung nicht benötigter Zugangsdaten.

## Features

- **Scan Discovery**  
Offene Konnektoren ermöglichen eine leistungsfähige Erkennung privilegierter Zugangsdaten und Secrets. Dies schafft vollständige Transparenz über privilegierte Zugriffe und unterstützt eine durchgängige Governance.
- **Session Recording**  
Die Aufzeichnung privilegierter Sitzungen dokumentiert sämtliche während eines Zugriffs ausgeführten Aktionen. Dies unterstützt Audit-Anforderungen und ermöglicht die Analyse von Vorfällen oder missbräuchlicher Nutzung.
- **Automatische Passwortrotation**  
Die automatisierte Rotation privilegierter Zugangsdaten verhindert statische Passwörter, reduziert die Angriffsfläche und schützt vor Brute-Force- sowie Wörterbuchangriffen.
- **Audited Commands**  
Ermöglicht die Definition granularer Filter für die Ausführung von Befehlen auf kritischen Systemen, um Vorfälle und missbräuchliche Aktivitäten zu verhindern.
- **App-To-App (A2A)**  
Als API-Schnittstelle ermöglicht A2A die sichere und authentifizierte Integration von Drittanwendungen mit Segura®, basierend auf zentral verwalteten Informationen.
- **KDI (Keystroke Dynamic Identity)**  
KI-gestützte Funktionen analysieren das Tippverhalten von Nutzern, um potenziell missbräuchliche Aktivitäten bei der Verwendung kompromittierter Zugangsdaten zu erkennen.
- **Just in time**  
Aktivierung und Deaktivierung sowie das Anlegen und Entfernen von Zugriffsrechten in Echtzeit.

## Weitere Differenzierungsmerkmale

- **Keine zusätzlichen Kosten**  
Segura® ist eine vollständig integrierte Gesamtlösung inklusive Datenbanken und Betriebssystemen und reduziert damit den Implementierungsaufwand.
- **Schnelle Implementierung**  
Sehr kurze Implementierungszeit. Innerhalb von nur sieben Minuten lässt sich eine hochverfügbare Software- und Hardware-Architektur inklusive Disaster Recovery bereitstellen.
- **Intuitive Benutzeroberfläche**  
Im PAM-Markt anerkannt für eine intuitive Benutzerführung und hohe Usability, wodurch Schulungs-, Support- und Betriebskosten reduziert werden.
- **Offene Konnektoren**  
Geräte- und Credential-Discovery sowie -Management erfolgen über technologiebasierte, offene Konnektoren – unabhängig von Herstellern. Die Anbindung von Legacy-Systemen ist möglich, ebenso die kundenseitige Erweiterung ohne professionelle Services.
- **Kundenanerkennung**  
Segura® ist die am höchsten bewertete PAM-Lösung auf Gartner® Peer Insights und wurde zuletzt als „Challenger“ anerkannt. Zudem wurde Segura® viermal mit dem Customers' Choice Award ausgezeichnet. Zusätzlich erreichte die Lösung 4,9 Sterne sowie eine Weiterempfehlungsrate von 98 % im Gartner Voice of the Customer-Report.

