segura | Futureproof Identity Security

Gartner Peer Insights Customers' Choice 2025

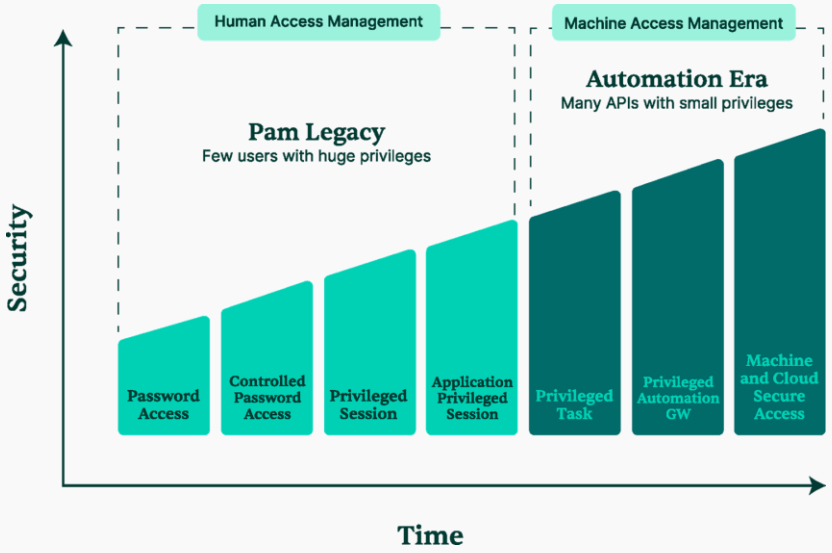
Produktübersicht

Einblicke in die 360° Privilege Plattform

März 2026

DAGMA IT SECURITY

Die Transformation digitaler Identitäten:
Vom Menschen zur Maschine



Die Automatisierungsära ist geprägt durch:

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

segura

DAGMA IT SECURITY

Schutz privilegierter Zugangsdaten

Es gibt **zwei- bis fünfmal** mehr privilegierte Konten in Unternehmen, als allgemein angenommen wird.

44% der Datenschutzverletzungen betreffen kompromittierte Zugangsdaten.

Quelle: Verizon

292 Tage vergehen durchschnittlich, bis Sicherheitsverletzungen mit gestohlenen Zugangsdaten erkannt werden.

Quelle: IBM

4,1 Mio. € betragen die durchschnittlichen Kosten von Sicherheitsverletzungen durch kompromittierte Zugangsdaten.

Quelle: IBM

segura

Schutz privilegierter Zugangsdaten

Wie lässt sich Zero Trust auf Privileged Access Management anwenden?

Wenn über 40% der Angriffe auf **Zugangsdaten** abzielen…

Dann ist **Identität** entscheidend für die Verhinderung von Sicherheitslücken.

Es ergibt sich folgende Schluss-folgerung:

segura

Die Logik priveligierter Identiäten:

Wenn

"**Identität**" der neue Sicherheitsperimeter ist

Und

Privilegien im Zentrum der Angriffskette stehen

Dann

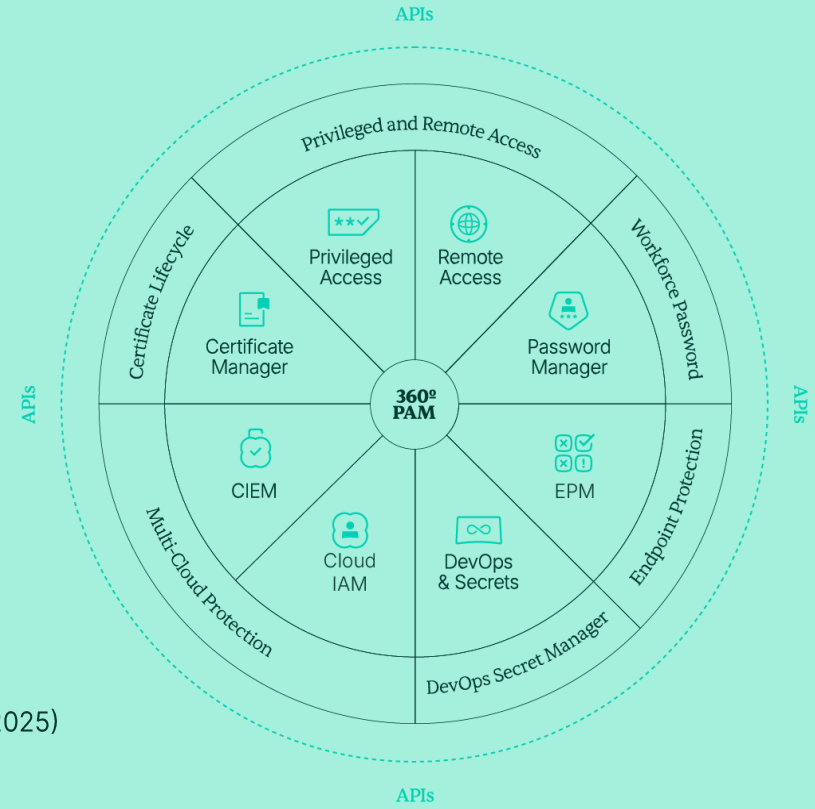
müssen priveligierte Identitäten das **am stärksten geschützte Asset** im Unternehmen sein.

DAGMA IT SECURITY

segura®

All-in-One-Lösung zur sicheren Verwaltung privilegierter Konten

- **All-in-One Architektur**
- **Keine versteckten Kosten**
- **Benutzerfreundlich & in wenigen Minuten einsatzbereit**
- **Agentenfreie Installation**
- **Mehrfach ausgezeichnet** (Gartner® Challenger & Customers Choice 2025)



segura®

Privileged Access · Remote Access · Pa**word Manager · DevOps & Secrets · Certificate Manager · EPM Endpoint Privilege Management · Cloud IAM

DAGMA IT SECURITY

PAM Core

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

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.

Scan Discovery
Offene Konnektoren ermöglichen eine leistungsfähige Erkennung privilegierter Zugangsdaten und Secrets. Dies schafft vollständige Transparenz über privilegierte Zugriffe und unterstützt eine durchgängige Governance.

App-to-App (A2A)
Als API-Schnittstelle ermöglicht A2A die sichere und authentifizierte Integration von Drittanwendungen mit Segura®, basierend auf zentral verwalteten Informationen.

Genehmigungsworkflow
Granulare mehrstufige Genehmigungsworkflows, die von Segura® angeboten werden, ermöglichen reduzierte Bereitstellungskosten und eine bessere Einhaltung von Zugriffsrichtlinien.

Automatische Passwortrotation
Die automatisierte Rotation privilegierter Zugangsdaten verhindert statische Passwörter, reduziert die Angriffsfläche und schützt vor Brute-Force- sowie Wörterbuchangriffen.

TOTP-Generator
Segura® kann OTP-Token generieren und verwenden. Dadurch wird der Kennwortaustausch in Fällen sichergestellt, in denen Anmeldeinformationen mit TOTP für MFA geschützt sind.

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.

Überwachte Befehle (Audited Commands)
Ermöglicht die Definition granularer Filter für die Ausführung von Befehlen auf kritischen Systemen, um Vorfälle und missbräuchliche Aktivitäten zu verhindern.

KDI (Keystroke Dynamic Identity)
KI-gestützte Funktionen analysieren das Tippverhalten von Usern, um potenziell missbräuchliche Aktivitäten bei der Verwendung kompromittierter Zugangsdaten zu erkennen.

Datenbank-Proxy
Bietet Zugriff auf die Datenbankverwaltung und stellt PAM-Funktionen bereit, um die Sicherheit von Datenbanken zu gewährleisten. Administratoren können Vorgänge aktivieren, überwachen und einschränken.

segura

DAGMA
IT SECURITY

DOMUM

Remote Access

Domum Remote Access ist eine Sicherheitslösung zur Bewältigung von Herausforderungen moderner Remote-Arbeitsmodelle und ermöglicht sicheren Zugriff auf Basis des Zero-Trust-Prinzips.

Domum Remote Access stellt einen sicheren Zugriff auf Systeme der Unternehmensinfrastruktur bereit – ohne VPN, ohne Agenteninstallation, ohne zusätzliche Lizenzierung und ohne weitere Konfigurationen. Der Zugriff erfolgt unmittelbar und geschützt.

Dadurch werden sämtliche (Remote-) Zugriffe abgesichert und die Administration vereinfacht.

Zugriff auf Knopfdruck
Zugriff auf Systeme ohne zusätzliche Anmeldedaten.

Erweiterte Optionen
Zugriffsteuerung nach Geolokalisierung, Tageszeit, Wochentag und Dauer.

Zentrale Übersicht
Einheitliche Oberfläche zur Überwachung aller Aktivitäten in der Umgebung.

Kein VPN erforderlich
Der Einsatz eines VPN sowie zusätzlicher Konfigurationen für Remote-User entfällt.

Granulare Steuerung
Ermöglicht eine differenzierte Zugriffstrennung auf Basis der Segura®-Funktionalitäten.

Sofortiger Zugriff
Schneller, unkomplizierter und sicherer Zugriff für Mitarbeitende und externe Dritte.

Granularer Zugriff
Workflows mit fein abgestufter Steuerung auf Basis definierter Zugriffsgruppen.

Intuitive Dashboards
Zentrale Verwaltung über benutzerfreundliche Dashboards.

Schlanke Architektur
Kein Einsatz von Agenten, zusätzlicher Software oder weiterer Lizenzierung erforderlich.

Operative Effizienz & Auditing
Optimiert die Verwaltung von Remote-User sowie alle Funktionen für Remote-Sitzungen wie Aufzeichnung und Live Stream.

segura

DAGMA IT SECURITY

MySafe

MySafe ist eine Sicherheitslösung zur sicheren und effizienten Speicherung sowie Weitergabe vertraulicher Informationen.

Der digitale Tresor ermöglicht die strukturierte Verwaltung von Passwörtern und weiteren sensiblen Daten, reduziert die Notwendigkeit, sich an mehrere Zugangsdaten zu erinnern, und schützt diese vor unbefugtem Zugriff.

Mithilfe der Generierung starker, zufälliger Passwörter wird das Sicherheitsniveau signifikant erhöht & ermöglicht ein effizientes Passwortmanagement.

segura

Verschlüsselung
Alle verwalteten Passwörter werden verschlüsselt gespeichert und sind ausschließlich über **MySafe** zugänglich.

Passwortfreigabe
Ermöglichung einer sicheren und benutzerfreundlichen Freigabe von Passwörtern zwischen autorisierten Usern.

Administratives Dashboard
Unterstützung unternehmensweiter Kampagnen sowie die Analyse sicherheitsrelevanter Daten mit grafischen Auswertungen.

Maximale Sicherheit
Verwendung von robusten Verschlüsselungsverfahren und Multifaktor-Authentifizierung, einschließlich biometrischer Authentifizierung auf mobilen Endgeräten.

Schutz sensibler Daten
Schutz sensibler Informationen durch mehrschichtige Sicherheitsmechanismen und restriktive Zugriffskontrollen.

Automatische Passworteingabe
Passwörter können automatisiert in Webanwendungen eingefügt oder bei Bedarf überprüft werden.

Generierung starker Passwörter
MySafe erzeugt zufällige, komplexe Kombinationen und steuert die Weitergabe von Passwörtern inkl. nachvollziehbarer Zugriffsdokumentation.

Nachvollziehbarkeit
Administratoren können nachvollziehen, auf welche Passwörter zugegriffen wurde, und daraus ableiten, welche Zugangsdaten gegebenenfalls angepasst werden müssen.

Browser-Erweiterung & Segura® App
Die Browser-Erweiterung ermöglicht die direkte Nutzung von **MySafe** im Webbrowser. Die Segura® App enthält **MySafe**-Funktionen wie Notizenverwaltung und Passwortmanagement.

Automatische Passwort-Injektion
Passwörter können automatisch in Websites eingefügt oder bei Bedarf einfach ausgecheckt werden.

DAGMA
IT SECURITY

DevOps

Mit der zunehmenden Migration von Unternehmen in Cloud-Infrastrukturen rückt die schnelle und effiziente Bereitstellung qualitativ hochwertiger Produkte und Services in den Mittelpunkt, was zur verstärkten Einführung von DevOps-Methoden führte.

DevOps fördert Kommunikation, Zusammenarbeit sowie schnelle Bereitstellung, Integration, Auslieferung und Entwicklung.

Der **Segura® DevOps Secret Manager** schützt und verwaltet Secrets innerhalb der DevOps-Pipeline und ermöglicht eine sichere sowie effiziente Softwarebereitstellung.

segura

Schutz und Verwaltung von Secrets und Zugangsdaten

Schutz und Verwaltung von Secrets und weiteren Zugangsdaten in DevOps-Umgebungen zur Absicherung sensibler Informationen gegen unbefugten Zugriff und Missbrauch.

Integrierter Cloud-IAM-Broker

Segura® ist die einzige PAM-Lösung mit integriertem Cloud-IAM-Broker, der nicht nur die Sicherheit erhöht, sondern auch die Zugriffssteuerung mehrerer Cloud-Plattformen vereinheitlicht.

Zentrale Verwaltung geteilter Secrets und Passwörter

Konsistente und kontrollierte Steuerung kritischer Zugangsdaten sowie Risikoreduzierung von unbefugtem Zugriff durch die zentrale Verwaltung geteilter Secrets und fest hinterlegter Passwörter.

Bibliothek sicherer und flexibler APIs

Einfache und schnelle Integration in bestehende Systeme und Werkzeuge. Dies vereinfacht Implementierungs- und Integrationsprozesse.

Discovery, Inventarisierung und Verwaltung von Secrets

Segura® bietet leistungsfähige Discovery-Funktionen. Dabei scannt die Lösung die DevOps-Pipeline automatisiert, um Secrets in der Umgebung zu identifizieren, zu inventarisieren und zu verwalten.

Granulare Zugriffskontrolle und Principle of Least Privilege (PoLP)

Branchenweit anerkannte Zugriffskontrollengranularität ermöglicht die Umsetzung des PoLP und reduziert das Missbrauchsrisiko von Berechtigungen.

Zentrale Dashboards und Reports

Vollständige Transparenz über die gesamte Umgebung. Dies unterstützt Monitoring, Auditierung und die Einhaltung von Sicherheitsrichtlinien sowie regulatorischen Anforderungen.

Funktion zur Ver- und Entschlüsselung sensibler Daten

Die Funktion ermöglicht die Ver- und Entschlüsselung von Daten während der Übertragung, ohne dass diese im DSM gespeichert werden müssen.

Integration mit DevOps-Tools

Nahtlose Integration mit führenden DevOps-Tools, einschließlich Containerisierung und CI/CD. Diese Integration gewährleistet reibungslose Workflows und erhöht die Sicherheit innerhalb der DevOps-Pipeline.

Skalierbare und integrierte Lösung

Segura® DSM ist vollständig in die Segura® PAM Security Plattform integriert und bietet einen umfassenden, einheitlichen Ansatz für PAM.

DAGMA IT SECURITY

Zertifikate

Digitale Zertifikate sind anfällig für menschliche Fehler und unterliegen festen Laufzeiten. In vielen Organisationen erfolgt das Zertifikatsmanagement weiterhin manuell, häufig auf Basis von Tabellenkalkulationen.

Mit dem **Segura® Certificate Manager** lässt sich der gesamte Lebenszyklus digitaler Zertifikate zentral steuern – von der Identifikation über das automatisierte Scannen von Websites, Verzeichnisdiensten und Webservern bis hin zur automatisierten Verlängerung über interne oder externe Zertifizierungsstellen.

Zertifikatserkennung
Automatisierte Identifikation sämtlicher Zertifikate im Netzwerk zur Vermeidung von Verlust, Inkonsistenzen und Desorganisation.

Kontinuierliches Monitoring
Echtzeitüberwachung von Zertifikaten inkl. Benachrichtigungssystem für Ablaufdaten und Fehlfunktionen.

Ablaufwarnungen
Frühzeitige Benachrichtigungen über bevorstehende Zertifikatsabläufe zur Vermeidung von Serviceunterbrechungen.

Einfacher und sicherer Import
Zertifikate lassen sich effizient in die Segura® Plattform integrieren und zentral verwalten.

Vollständige Automatisierung des Zertifikatslebenszyklus
Automatisierte Verwaltung der Zertifikatsverlängerung und -veröffentlichung zur Reduzierung von Fehlerquellen und administrativem Aufwand.

Veröffentlichung auf Webservern und in Keystores
Vereinfachte Bereitstellung von SSL/TLS-Zertifikaten auf Servern zur Erhöhung der Online-Sicherheit.

Dashboards und Berichte
Zentrale Übersicht über alle Zertifikate zur strukturierten Steuerung und fundierten Entscheidungsfindung.

Integration mit Zertifizierungsstellen
Anbindung führender Zertifizierungsstellen (CAs) zur sicheren Beantragung und Ausstellung von Zertifikaten.

Verwaltung persönlicher Zertifikate
Verwaltung digitaler Zertifikate für rechtsverbindliche Finanztransaktionen und Dokumentensignaturen.

Unterstützung einer Zero-Trust-Strategie
Stärkung der Zero-Trust-Architekturen durch die kontinuierliche Ausstellung und Validierung vertrauenswürdiger Identitäten für Maschinen und Anwendungen.

segura

DAGMA
IT SECURITY

EPM

EPM
Endpoint
Privilege
Management

In zunehmend komplexen IT-Infrastrukturen sind eine konsequente Kontrolle administrativer Berechtigungen sowie die effektive Umsetzung des Least-Privilege-Prinzips entscheidend, um das Sicherheitsniveau zu erhöhen und das Risiko von Datenvorfällen zu minimieren.

An dieser Stelle setzt der **Segura® Endpoint Privilege Manager (EPM)** an.

Als leistungsfähige Privileged Elevation and Delegation Management (PEDM)-Lösung ermöglicht EPM die kontrollierte und sichere Ausführung privilegierter Funktionen auf Windows- und Linux-Endpunkten.

segura

Privilegierte Ausführung auf Basis genehmigter Aktionslisten
Autorisierte User können Administratorrechte zur Ausführung definierter Anwendungen anfordern, sodass ausschließlich geschäftskritische Applikationen mit erhöhten Berechtigungen sicher ausgeführt werden.

Sitzungsaufzeichnung über Windows und Linux
Es ist möglich, SUDO-Aktionen auf Linux-Endpunkten und Sitzungen in Windows aufzuzeichnen, um Überwachungsanforderungen zu erfüllen.

Schutz vor Datendiebstahl & Verhinderung von Privilegienmissbrauch
Die EPM-Lösung korreliert Ereignisse zur Identifikation verdächtiger Aktivitäten, isoliert kritische Umgebungen und stellt erweiterte Sicherheitsmechanismen zum Schutz geschäftskritischer Daten und zur frühzeitigen Erkennung von Missbrauchsmustern bereit.

Sitzungsaufzeichnung unter Windows und Linux
SUDO-Aktionen auf Linux-Endpunkten sowie Sitzungen unter Windows werden aufgezeichnet, um Audit-Anforderungen zu erfüllen, Compliance sicherzustellen und eine lückenlose Nachvollziehbarkeit privilegierter Aktivitäten zu gewährleisten.

Integration von Linux-Login-Informationen in Gruppenrichtlinien (nur Linux)
Jede Authentifizierung wird auf Basis von Zeitparametern, Aufrufen, Berechtigungen sowie zusätzlichen Gruppenrichtlinien validiert, wodurch die Sicherheit von Linux-Endpunkten gestärkt wird.

Vollständiges SUDO-Management (nur Linux)
Durch die Definition granularer Richtlinien wird eine vollständige Kontrolle über mit SUDO ausgeführte Aktionen auf Linux-Endpunkten ermöglicht und das Sicherheitsniveau erhöht.

Automatisierte Anwendungsausführung und Zugriff über Makros (nur Windows)
Wiederkehrende Aufgaben werden durch Automatisierung optimiert, während gleichzeitig eine strikte Kontrolle über privilegierte Aktionen erhalten bleibt.

Sicherer Zugriff auf sensible Daten in Netzwerkverzeichnissen (nur Windows)
Gewährleistet ein Höchstmaß an Sicherheit für freigegebene Dateien und Verzeichnissen im Netzwerk und schützt geschäftskritische Informationen vor Bedrohungen.

Zugriff auf die Systemsteuerung mit Administratorrechten (nur Windows)
User können administrative Aufgaben wie die Anpassung von Datums- und Uhrzeiteinstellungen durchführen, wodurch eine effektive Verwaltung zentraler Systemkonfigurationen gewährleistet wird.

Malware-Analyse (nur Windows)
Spezialisierte Funktionen zur Malware-Analyse schützen Windows-Endpunkte zuverlässig vor Cyberbedrohungen.

Workflow-Erstellung (nur Windows)
Aufgaben und Prozesse lassen sich durch individuell definierte Workflows automatisieren und vereinfachen, wodurch das Privilegien-Management optimiert und die operative Effizienz gesteigert wird.

Ausführung und automatisierter Zugriff auf Anwendungen über Makros (nur Windows)
Optimierung sich wiederholender Aufgaben und Steigerung der Produktivität.

DAGMA
IT SECURITY

Cloud IAM

Transparenz und Kontrolle über Identitäten und Access Keys verschiedener Cloud Service Provider (CSPs) sind zentrale Voraussetzungen für Compliance und Sicherheit. Denn die Nutzung von Multi-Cloud-Architekturen erhöht die Komplexität im Identity- und Access-Management für IT- und Security-Teams erheblich.

Unzureichende Kontrolle führt zu Risiken wie unbefugtem Zugriff, Compliance-Verstößen und Datenschutzvorfällen.

Segura® Cloud IAM bietet eine robuste Lösung zur Sicherstellung von Identity Governance in hybriden und Multi-Cloud-Umgebungen.

segura

Benutzer- und Access-Key-Management
Intuitive & zentrale Oberfläche zur Verwaltung von Identitäten und Access Keys einschließlich auditierte Bereitstellung, Löschung und Steuerung von Usern.

Auditierte Bereitstellung und Löschung
Protokollierung & revisionssichere Nachvollziehbarkeit sämtlicher Vorgänge zur Erstellung und Löschung von Identitäten und Access Keys.

Zentrale Transparenz
Dashboards ermöglichen eine einheitliche Übersicht über sämtliche Identitäten und Access Keys und unterstützen Verwaltung sowie Auditierung.

Auditierter Remote-Zugriff auf CSP-Konsolen
Überwachung & Protokollierung sämtlicher Remote-Zugriffssitzungen auf CSP-Konsolen und Gewährleistung vollständiger Audit-Trails.

Just-in-Time (JIT) Zugriff
Steuerung temporärer Zugriffe und Sicherstellung der ausschließlich zeitlich begrenzten und bedarfsgesteuerten Gewährung von Berechtigungen.

Identity-Zentralisierung
Bündelt das Identity-Management unterschiedlicher CSPs und schafft eine konsolidierte Gesamtsicht auf alle User und deren Berechtigungen.

Session Recordings
Aufzeichnung, Prüfung & Nachvollziehbarkeit von Konsolenzugriffen im Rahmen von Compliance-Anforderungen.

Risikoreduzierung
Die automatisierte User- und Berechtigungsverwaltung reduziert das Risiko unbefugter Zugriffe und stellt sicher, dass ausschließlich berechtigte Personen zum definierten Zeitpunkt über angemessene Zugriffsrechte verfügen.

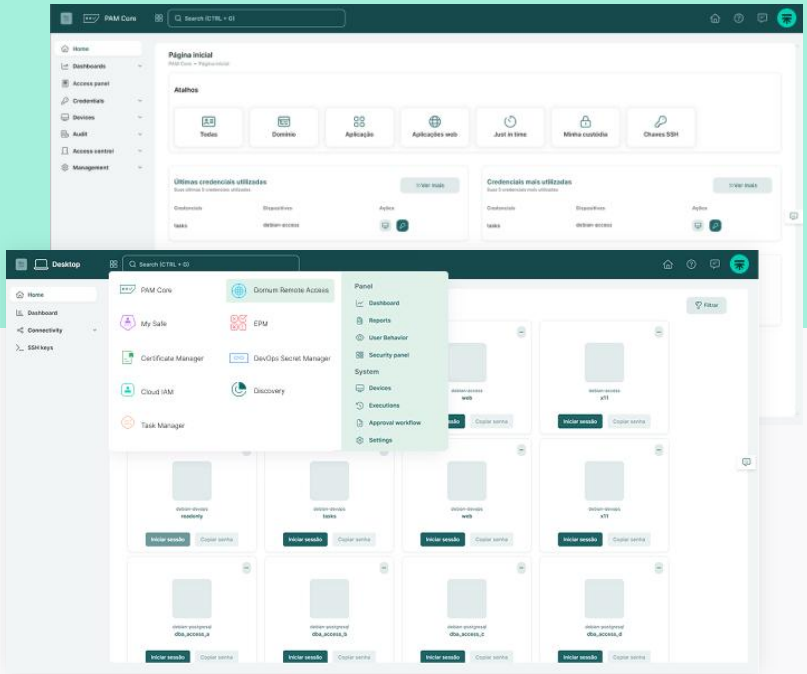
DAGMA
IT SECURITY

segura

DAGMA
IT SECURITY

Alles, was für Privileged Access Management benötigt wird – in einer Plattform!

Keine Extra-Tools. Keine Komplexität. Vollständiger Schutz.



98%

Empfehlungsrate auf **Gartner Peer Insights**

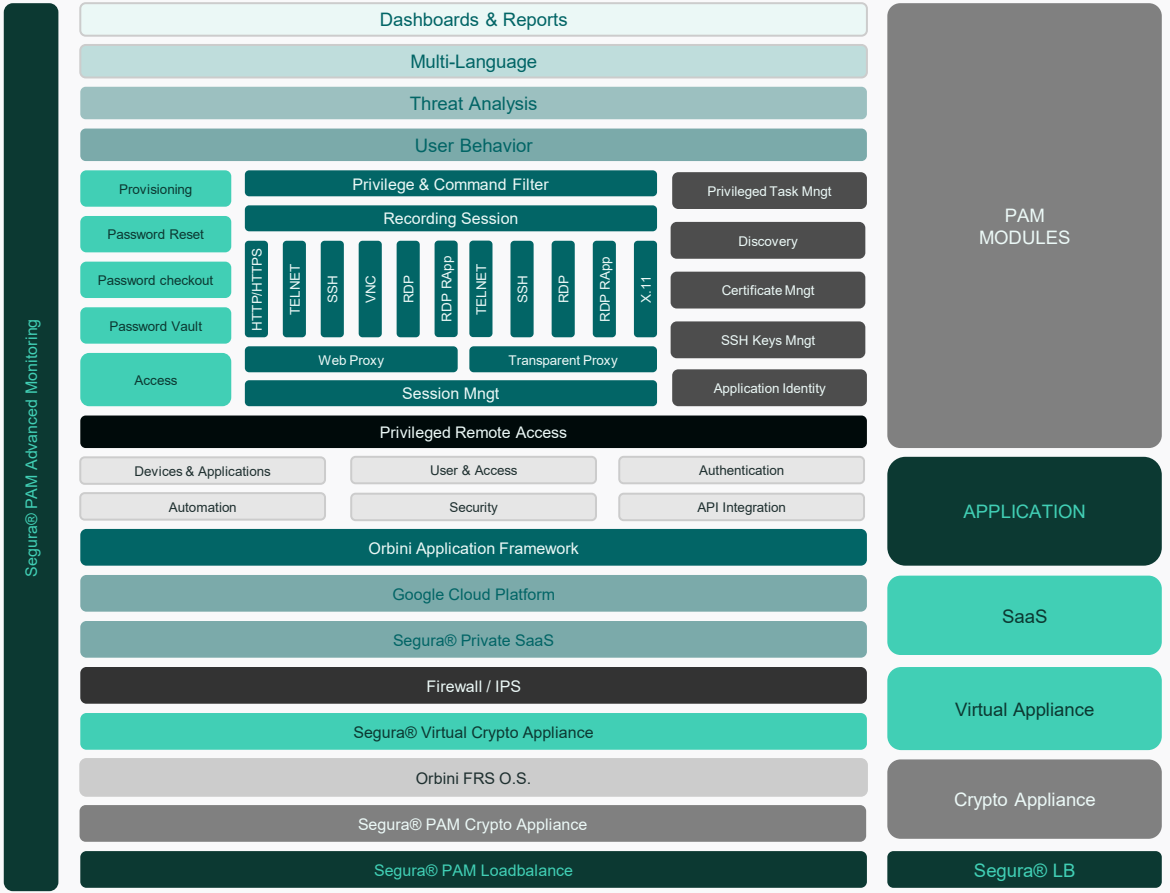
90%

Schnellere **Time-to-Value (ToV)**

70%

Niedrigere **Gesamtbetriebskosten (TCO)**

Full-Stack-Architektur



segura

DAGMA IT SECURITY

Direkt. Persönlich. Auf Augenhöhe.

Wir beraten Sie gerne!

FLORIAN KRAUS
General Manager

P: +49 151 4285 9022
kraus.f@dagma.eu

ALEXANDER BÖRSEL
Channel Manager

P: +49 176 6127 4571
boersel.a@dagma.eu

SEBASTIAN MAHN
Business Development Manager

P: +49 162 5985 732
mahn.s@dagma.eu

WALTER KARL
Principal Sales Architect

P: +49 170 2714 138
karl.w@dagma.eu

JÜRGEN ZORENC
Head of Technical Sales

P: +49 157 5807 6752
zorenc.j@dagma.eu

MATTHIAS MEIERHOFER
Marketing Specialist

P: +49 30 6920 62 988
meierhofer.m@dagma.eu

UNSER PORTFOLIO

Identity · Exposure · Detection · Enforcement

Bare.ID GATEWATCHER HADRIAN HOLM SECURITY segura Sekoia

DAGMA IT SECURITY

CYBERSECURITY FROM EUROPE