senhasegura is now segura®

# Produktübersicht

Einblicke in die 360° Privilege Plattform

segura ist der einzige Anbieter mit einer 5-Sterne-Bewertung. Die höchste Bewertung in Bezug auf Produktfunktionen.

Diese hervorragende Bewertung spiegelt nicht nur die Kundenzufriedenheit wider, sondern ist auch ein Beweis dafür, wie fortschrittlich und innovativ unser Produkt ist.


Gartner
Peer Insights™

# PAM Core

Privileged Access Management (PAM) zielt darauf ab, die Verwendung generischer und privilegierter Anmeldeinformationen zu schützen und zu kontrollieren, indem es eine sichere Speicherung, eine Trennung des Zugriffs und eine vollständige Rückverfolgbarkeit der Nutzung bietet.

segura ermöglicht es Unternehmen, die strengsten und komplexesten Kontrollen für den Zugriff auf privilegierte Anmeldeinformationen automatisiert und zentralisiert zu implementieren und so die IT-Infrastruktur vor Datenschutzverletzungen und potenziellen Compliance-Verstößen zu schützen.

**Scan Discovery**
Offene Konnektoren bieten erstklassige Erkennungsfunktionen für privilegierte Anmeldeinformationen und Geheimnisse und bieten vollständige Transparenz des privilegierten Zugriffs für maximale Governance.

**KDI (Keystroke Dynamic Identity)**
Durch KI-basierte Funktionen ist es möglich, die Tastenanschlagmuster von Benutzern zu analysieren und mögliche böswillige Aktivitäten mit gestohlenen Anmeldeinformationen zu erkennen.

**Automatische Rotation von Anmeldeinformationen**
segura bietet integrierte Plugins und Out-of-the-Box-Vorlagen für die automatische Rotation von Anmeldeinformationen auf Geräten, Diensten, Konfigurationsdateien und Anwendungen durch konfigurierbare Kriterien.

**Genehmigungs-Workflow**
Granulare mehrstufige Genehmigungsworkflows, die von segura angeboten werden, ermöglichen reduzierte Bereitstellungskosten und eine bessere Einhaltung von Zugriffsrichtlinien.

**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.

**App to App**
Lokale Aktionen für Anwendungs- und Bereitstellungsskripts, z. B. das Pushen von Geheimnissen aus der PAM-Lösung und das Einfügen in Konfigurationsdateien oder Umgebungsvariablen.

**Sitzungsaufzeichnung**
Sitzungsvideos können in einem Videoformat mit hoher Komprimierung aufgezeichnet werden, ohne dass lokale Agenten erforderlich sind.

**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. Wir sind Pioniere, wenn es darum geht, einen Befehlsfilter für Oracle anzubieten.

**Überwachte Befehle (Audited Commands)**
Es ist möglich, Richtlinien mit Punkten zu erstellen, die jedem ausgeführten Befehl zugewiesen werden. Wenn ein hohes Risiko erreicht wird, werden Warnungen für Administratoren ausgelöst und auf grafischen Dashboards gekennzeichnet.

# DevOps Secret Manager

Um die Sicherheit in der DevOps-Umgebung zu erhöhen, bietet segura eine Lösung an, die Automatisierung, Agilität und Kontrolle bietet und die Sicherheit der gesamten Umgebung gewährleistet.

DevOps Secret Manager hilft beim Schutz und der Verwaltung von Geheimnissen in der DevOps-Pipeline und ermöglicht es Unternehmen, eine sichere und effiziente Softwarebereitstellung zu erreichen.

### Schutz und Verwaltung von Geheimnissen und Anmeldeinformationen

Schutz und Verwaltung von Geheimnissen und anderen Anmeldeinformationen, die in DevOps-Umgebungen verwendet werden, Schutz sensibler Informationen, um unbefugten Zugriff und Missbrauch zu verhindern.

### Ermittlung, Inventarisierung und Verwaltung von Geheimnissen

segura bietet erstklassige Discovery-Funktionen. Es scannt automatisch die DevOps-Pipeline, um Geheimnisse zu erkennen, zu inventarisieren und zu verwalten.

### Integrierter Cloud-IAM-Broker

segura ist die einzige PAM-Lösung, die einen integrierten Cloud-IAM-Broker bietet, der die Sicherheit erhöht und die Zugriffskontrolle über mehrere Cloud-Plattformen hinweg optimiert.

### Zentralisierte Verwaltung von Shared Secrets und Passwörtern

Zentralisierte Verwaltung von Shared Secrets und hartcodierten Passwörtern, um einen konsistenten und kontrollierten Zugriff auf kritische Anmeldeinformationen zu gewährleisten und das Risiko eines unbefugten Zugriffs zu verringern.

### Verschlüsseln

Es ist möglich, Daten während der Übertragung zu verschlüsseln und zu entschlüsseln, ohne diese Daten zu speichern, wodurch die Anwendungsleistung optimiert wird.

### Granularität des Zugriffs und Prinzip der geringsten Rechte

Die branchenweit anerkannte Zugriffsgranularität ermöglicht es Unternehmen, das Prinzip der geringsten Rechte (Principle of Least Privilege, PoLP) zu implementieren und so das Risiko des Missbrauchs von Privilegien zu verringern.

### Zentralisierte Dashboards und Berichte

Vollständiger Einblick in die Umgebung. Dies erleichtert die Überwachung, Prüfung und Einhaltung von Sicherheits-richtlinien und -vorschriften.

### Integration mit DevOps-Tools

Nahtlose Integration mit den wichtigsten DevOps-Tools, einschließlich Containerisierung und CI/CD. Diese Integration gewährleistet reibungslose Arbeitsabläufe und erhöht die Sicherheit in der gesamten DevOps-Pipeline.

### Bibliothek mit sicheren und flexiblen APIs

Einfache und schnelle Integration mit anderen Systemen und Tools. Dies vereinfacht den Implementierungs- und Integrationsprozess.

### Skalierbare und integrierte Lösung

segura DSM ist vollständig in die segura PAM Security Plattform integriert und bietet einen umfassenden und einheitlichen Ansatz für das Privileged Access Management.

# Domum Remote Access

Der Zugriff wird sofort, einfach und sicher gewährt, ohne dass Gerätekennwörter preisgegeben werden und ohne dass der Benutzer Anmeldeinformationen für den Zugriff auf die PAM-Sicherheitsplattform benötigt.

Um die Probleme im Zusammenhang mit der Remote-Arbeit von Mitarbeitern und Dritten zu lösen, bietet Domum Benutzern einen sicheren Zugriff auf der Grundlage von Zero Trust auf die Geräte der Unternehmensinfrastruktur von überall aus, ohne dass VPN, die Installation von Agenten und Lizenzen oder zusätzliche Konfigurationen erforderlich sind.

**Ein-Klick-Zugriff**
segura Domum ermöglicht den Zugriff auf Geräte, ohne dass Zugangsdaten erforderlich sind.

**Erweiterte Optionen**
Zugriffsbeschränkung basierend auf Aspekten wie Geolokalisierung, Uhrzeit oder Wochentag und Dauer.

**Zentralisierte Ansicht**
Ein einziger Desktop-Bildschirm, der eine zentrale Ansicht der in der Umgebung ausgeführten Aktionen ermöglicht.

**Auditing**
Alle Funktionen für Remote-Sitzungen wie Aufzeichnung und Live Stream.

**Granularer Zugriff**
Greifen Sie auf Workflows mit maximaler Granularität zu, die auf branchenweit anerkannten Zugriffsgruppen basieren.

**Sofortiger Zugriff**
Sofortiger, einfacher und sicherer Zugriff für Mitarbeiter und Dritte, ohne dass auf die PAM-Plattform zugegriffen werden muss.

**Kein VPN**
Kein VPN oder zusätzliche Einstellungen für Remote-Benutzer erforderlich.

**Maximale Granularität**
Maximale Zugriffstrennung basierend auf der von segura gebotenen Granularität.

**Einfache Architektur**
Die Architektur von segura ohne die Notwendigkeit von Agenten erfordert keine zusätzliche Software oder Lizenzierung.

**Dashboards**
Zentralisierte Verwaltung durch intuitive Dashboards.

# Certificate Manager

Mit branchenweit anerkannten Erkennungsfunktionen, automatisierter Erneuerung und der Integration mit führenden Zertifizierungsstellen können Unternehmen mühelos den gesamten Lebenszyklus von Zertifikaten verwalten.

Durch zentralisierte Verwaltung, Automatisierung und umfassende Transparenz gewährleistet segura Certificate Manager maximale Verfügbarkeit, betriebliche Effizienz und verbesserte Sicherheit.

### Erkennung von Zertifikaten

segura bietet branchenweit anerkannte Best-in-Class-Erkennungsfunktionen für die vollständige Sichtbarkeit digitaler Zertifikate.

### Warnung zum Fälligkeitsdatum

Konfigurieren Sie automatisch die regelmäßige Erneuerung und Veröffentlichung der Zertifikate, um Verluste aufgrund von Zertifikatsabläufen zu vermeiden.

### Generierung von Anfragen

Führen Sie die Anforderungen mit den vorregistrierten Informationen aus und reduzieren Sie die Fehler bei der Erstellung der Zertifikate.

### Erneuern und Veröffentlichen

Behalten Sie die vollständige Kontrolle über den Ablauf der Baumabläufe der verwalteten Zertifikate. Senden Sie Benachrichtigungen in konfigurierbaren Zeiträumen an bestimmte Teams.

### Dashboards und Berichte

Grafische Ansicht des Status aller Zertifikate, die z. B. Kryptografie aus den Sicherheitsrichtlinien der Organisation verwenden.

### Unterschrift des Zertifikats

Nutzen Sie die Integration mit den wichtigsten Zertifizierungsstellen des Marktes, um die Zertifikate innerhalb der Lösung automatisch zu signieren, einschließlich der selbstsignierten.

# GO Endpoint Manager

segura GO Endpoint Manager ist eine robuste PEDM-Lösung, die es Unternehmen ermöglicht, Administratorrechte zu kontrollieren und zu verwalten und gleichzeitig eine sichere, konforme und effiziente Infrastruktur auf Windows- und Linux-Endpunkten aufrechtzuerhalten.

Mit seinen umfassenden Funktionen und Vorteilen ist es ein unverzichtbares Werkzeug für Unternehmen, die die Sicherheit erhöhen, Datenschutzverletzungen verhindern und das Prinzip der geringsten Rechte durchsetzen möchten.

**Ausführen von Anwendungen mit Berechtigungen basierend auf Listen genehmigter Aktionen**
Autorisierte Benutzer können Administratorrechte zum Ausführen von Anwendungen aufrufen und so sicherstellen, dass kritische Anwendungen, die erhöhte Berechtigungen erfordern, sicher ausgeführt werden können.

**Zugriff auf die Windows-Systemsteuerung mit Administratorrechten (nur Windows)**
Benutzer können Aufgaben wie das Ändern von Datums- und Uhrzeiteinstellungen ausführen. Dadurch wird sichergestellt, dass wesentliche Systemkonfigurationen effektiv verwaltet werden können.

**Zugriff auf vertrauliche Daten, die an Netzwerkadressen freigegeben sind (nur Windows)**
Diese Funktion bietet maximale Sicherheit für Dateien und Verzeichnisse vor Bedrohungen und schützt kritische Informationen innerhalb des Netzwerks.

**Ausführung und automatisierter Zugriff auf Anwendungen über Makros (nur Windows)**
Optimieren Sie sich wiederholende Aufgaben und steigern Sie die Produktivität, während Sie gleichzeitig die strikte Kontrolle über privilegierte Aktionen behalten.

**Zusätzliche Sicherheitsebene über Tools**
segura GO Endpoint Manager verhält sich direkt, wie LSM (Linux Security Machines) über ACL, PAM, Linux, ohne dass der Kernel neu kompiliert werden muss.

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

**Integration von Linux-Login-Informationen in Gruppenrichtlinien**
Es ist möglich, jede durchgeführte Authentifizierung anhand von Zeit, Anrufen, Autorisierungen und zusätzlichen Gruppenrichtlinien zu validieren.

# MySafe

segura MySafe ist ein Passwort-Manager, der die Sicherheit Ihres Unternehmens erhöht, indem er die Anmeldedaten aller Benutzer schützt. Das bedeutet, dass Unternehmenspasswörter, sowohl persönliche als auch kollaborative, ordnungsgemäß gesichert sind.

segura MySafe hilft Benutzern, ihre vertraulichen Daten mit wenigen Klicks ohne Risiko zu speichern und zu teilen. Die Lösung generiert starke und zufällige Passwörter, damit Benutzer das Sicherheitsniveau erhöhen können.

### Verschlüsselung

Alle verwalteten Passwörter werden verschlüsselt gespeichert, so dass der Zugriff nur über segura MySafe erfolgen kann.

### Gemeinsame Nutzung von Passwörtern

segura MySafe ist in der Lage, Passwörter auf benutzerfreundliche Weise über Web oder Mobile zu verwalten.

### Nachvollziehbarkeit

Es ist möglich, zu überprüfen, auf welches Passwort Personen Zugriff hatten, um Administratoren darüber zu informieren welche Passwörter sie möglicherweise ändern müssen, nachdem jemand das Unternehmen verlassen hat.

### Browsererweiterung und mobile App

Benutzer können Passwörter einfach über die Browsererweiterung und die mobile Anwendung anzeigen und generieren.

### Automatische Passwort-Injektion

Passwörter können automatisch in Websites eingefügt oder bei Bedarf einfach ausgecheckt werden.

### Maximale Sicherheit

segura MySafe ist durch starke Verschlüsselungsmethoden und mehrere Methoden der Multi-Faktor-Authentifizierung gesichert. Beginnend mit der Verwendung von Fingerabdrücken, damit Benutzer auf Passwörter auf ihrem Smartphone zugreifen können.

# Cloud-Berechtigungen

segura Cloud Entitlements bieten eine vollständige Governance des Cloud-Zugriffs, indem sie unnötigen Berechtigungen Transparenz gewähren und Richtlinien verfeinern, ohne den Entwicklungsfluss und ihre Notwendigkeit an Agilität zu unterbrechen.

segura Cloud Entitlements unterstützen Unternehmen bei der Verwaltung von Cloud-Zugriffsrisiken durch Administrationszeitkontrollen für die Steuerung von Berechtigungen in Hybrid- und Multi-Cloud-IaaS.

**Sichtbarkeit der Identität**
Zeigen Sie zentral menschliche und maschinelle Identitäten an, die über alle von Ihnen verwendeten Cloud-Anbieter verteilt sind.

**Größenänderung von Berechtigungen**
Passen Sie die Berechtigungen von IAM-Entitäten basierend auf der Ressourcennutzung und dem tatsächlichen Bedarf automatisch an.

**"Least privilege" Prinzip**
Verwenden Sie Cloud-Berechtigungen, um sicherzustellen, dass Identitäten dem Prinzip der geringsten Rechte entsprechen.

# Kontaktieren Sie uns


FLORIAN KRAUS
General Manager
DACH
P: +49 151 4285 9022
kraus.f@dagma.eu

JÜRGEN ZORENC
TECHNICAL
SALES DACH
P: +49 157 5807 6752
zorenc.j@dagma.eu


DAGMA
IT SECURITY