segura | Futureproof Identity Security

Gartner Peer Insights Customers' Choice 2025

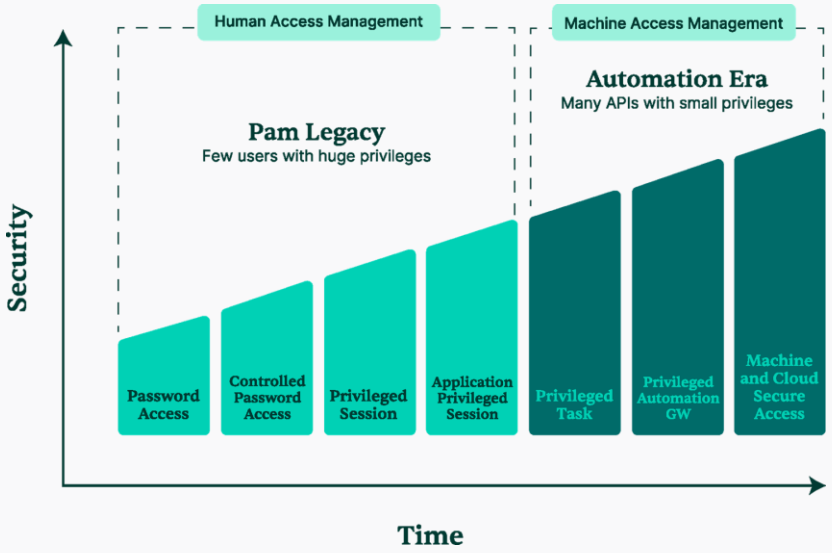
Product overview

Insights into the 360° Privilege platform

March 2026

DAGMA IT SECURITY

Identity Journey:
From humans to machines



Automation era defined by:

- DevOps
- API Access/Identity
- Cloud Access
- IoT Identity
- Industry 4.0

segura

DAGMA IT SECURITY

Protecting Privileged Credentials

There are 2 to 5 times the number of privileged accounts in the company than people realize.

44% of data breaches involve credentials.

Source: Verizon

292 days to identify breaches involving stolen credentials

Source: IBM

€4.1M is the average cost of breaches involving compromised credentials

Source: IBM

segura

Protecting Privileged Credentials

How does Zero Trust apply to Privileged Access Management?

If >40% of attacks target Credentials

Then Identity is the key to preventing breaches...

Which leads us to this conclusion...

segura

The Boolean Logic of Privileged Identity:

If

Identity is the New Perimeter

And

Elevated Privilege is at the Core of the Kill Chain

Then

Privileged Identity **MUST** be an Enterprise's Most Protected Asset.

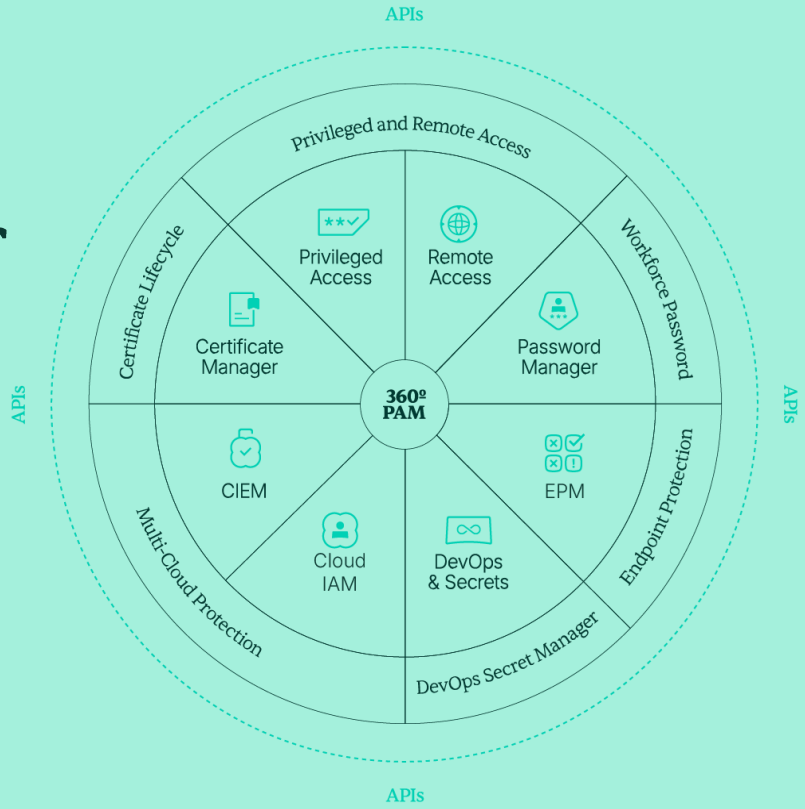
DAGMA IT SECURITY

segura

Comprehensive Security

All-in-one solution for managing privileged accounts securely.

- All-in-One Architecture
- No Hidden Fees
- Lowest Total Cost of Ownership (TCO)



PAM Core

Privileged credentials provide access to critical actions, such as modifying domain controller settings or transferring funds from an organization's accounts.

Privileged Access Management (PAM) aims to protect and control the use of generic and privileged credentials, providing secure storage, access segregation, and full traceability of usage.

Implementing controls to protect privileged credentials should be part of the cybersecurity strategy for organizations of all sizes and industries.

segura

Scan Discovery
Open connectors offer best-in-class discovery capabilities for privileged credentials and secrets, providing full visibility of privileged access for maximum governance.

App to app (A2A)
As our API interface, A2A enables third-party applications to integrate with Segura®, using managed information in an authenticated and secure manner.

Approval workflow
The approval workflow guarantees the four-eyes principle, where privileged actions must be approved by at least two people, ensuring transparency and authorization control.

Automatic credential rotation
Automated credential rotation ensures that high-privilege passwords are not static, reducing the attack surface and mitigating brute force and dictionary attacks.

Open connectors
Device and credential discovery and management are done through open connectors based on technology, not vendors. They allow connection with legacy devices and can be developed by the customer without the need for professional services.

Session Recording
Session recordings allow the registration of all actions performed during a high-privilege access, aiming to comply with audits and enable investigation in case of incidents or privilege abuse.

Audited Commands
Allows defining granular filters for executing commands on critical devices, preventing incidents and malicious actions.

KDI (Keystroke Dynamic Identity)
AI-based features allow the analysis of users' keystroke patterns to detect possible malicious activities using stolen credentials.

No additional costs & fast deployment
Segura® is a complete and integrated solution, including databases and operating systems, reducing deployment efforts. It has the shortest deployment time in the market. In just 7 minutes, it is possible to configure and deliver software and hardware architecture with high availability and disaster recovery.

Just in time
Activating/deactivating or creating/removing access in real time.

DAGMA
IT SECURITY

DOMUM

Domum Remote Access is a security solution designed to address the challenges of remote work, offering secure access based on the Zero Trust concept.

Domum Remote Access provides secure access to corporate infrastructure devices without the need for a VPN, agent installation, licensing, or additional configurations. Access is granted instantly and securely, without exposing device passwords and without requiring users to have credentials to access the PAM security platform.

This ensures that the security team can protect all accesses, simplifying management and enhancing the security of the corporate environment.

segura

One-Click Access
Access devices without additional credentials.

Advanced Options
Control access by geolocation, time of day, day of the week, and duration.

Centralized View
Single interface to monitor actions in the environment.

No VPN Needed
Eliminates the need for a VPN and additional configurations for remote users.

Granularity
Provides detailed access segregation based on Segura® functionalities.

Instant Access
Fast, easy, and secure access for employees and third parties.

Granular Access
Workflows with granularity based on recognized access groups.

Intuitive Dashboards
Centralized management through easy-to-use dashboards.

Simple Architecture
No need for agents, software, or additional licensing.

Operational Efficiency & Auditing
Improves the management of remote users as well as all functions for Session recording and LiveStream.

DAGMA
IT SECURITY

MySafe

MySafe is a security solution designed to help users securely and efficiently store and share confidential data.

This digital vault allows users to manage passwords and other sensitive information with ease, eliminating the need to remember multiple passwords and ensuring these credentials are protected against unauthorized access.

MySafe generates strong, random passwords, significantly boosting security levels. In addition, it enables efficient password management and secure information sharing, ensuring protection against unauthorized access and data leaks.

segura

Encryption
All managed passwords are stored in an encrypted form, ensuring they can only be accessed through **MySafe**.

Password Sharing
Allows secure and user-friendly sharing of passwords among users.

Administrative dashboard
Available to assist in corporate campaigns and data analysis.

Maximum Security
Uses robust encryption methods and multifactor authentication, including fingerprint authentication on smartphones.

Protection of Sensitive Data
Protects sensitive data with multiple layers of defense and restricted access.

Generation of Strong Passwords
Minimizes the risk of password discovery by generating random combinations.

Traceability
Enables administrators to verify which passwords have been accessed, helping identify which data needs to be changed.

Browser Extension & Segura® App
Facilitates the use of **MySafe** directly in the browser. The Segura® App includes **MySafe** for functionalities such as notes and password management.

Automatic Password Insertion
Passwords can be automatically entered into websites or checked on demand.

DAGMA
IT SECURITY

DevOps

As organizations increasingly migrate to cloud infrastructure, the focus on delivering high-quality products and services quickly and efficiently has led to the adoption of DevOps methodologies.

DevOps emphasizes communication, collaboration, and rapid deployment, integration, delivery, and development.

Segura® DevOps Secret Manager helps protect and manage secrets in the DevOps pipeline, enabling organizations to achieve secure and efficient software delivery.

segura

Protection and management of secrets and credentials
Protection and management of secrets and other credentials used in DevOps environments, safeguarding sensitive information to prevent unauthorized access and misuse.

Integrated Cloud IAM broker
Segura® is the only PAM solution that offers an integrated Cloud IAM broker, which enhances security and streamlines access control across multiple cloud platforms.

Centralized management of shared secrets and passwords
Centralized management of shared secrets and hardcoded passwords, ensuring consistent and controlled access to critical credentials, reducing the risk of unauthorized access.

Library of secure and flexible APIs
Easy and fast integration with other systems and tools. This simplifies the implementation and integration process.

Discovery, inventory, and management of secrets
Segura® offers best-in-class discovery capabilities. It automatically scans the DevOps pipeline to discover, inventory and manage secrets in the environment.

Granularity of access and Principle of Least Privilege (PoLP)
Industry-recognized granularity of access enables organizations to implement the PoLP, reducing the risk of privilege misuse.

Centralized dashboards and reports
Complete visibility into the environment. This facilitates monitoring, auditing, and compliance with security policies and regulations.

Functionality to encrypt and decrypt sensitive data
The functionality can encrypt and decrypt data in transit, without the need to save this data in the DSM.

Integration with DevOps tools
Seamlessly integration with the main DevOps tools, including containerization and CI/CD. This integration ensures smooth workflows and enhances security across the DevOps pipeline.

Scalable and integrated solution
Segura® DSM is fully integrated with the Segura® PAM Security platform, providing a comprehensive and unified approach to Privileged Access Management.

DAGMA
IT SECURITY

Certificates

Digital certificates are prone to human error and expiration. In many cases, certificate management is still done manually using spreadsheets.

With **Segura® Certificate Manager**, you can centrally manage the entire lifecycle of digital certificates within your organization – from discovery, through automated scanning of websites, directories, and web servers, to the automated renewal of certificates via external or internal certificate authorities.

segura

Certificate Discovery
Automatically identify all certificates across the network, preventing loss and disorganization.

Continuous Monitoring
Monitor certificates in real time with an alert system for expirations and failures.

Expiration Alerts
Receive early notifications about certificate expirations to prevent service disruptions.

Simple and Secure Import
Easily import certificates into the Segura® Platform, ensuring efficient management.

Complete Certificate Lifecycle Automation
Automatically manage the renewal and publishing of certificates, reducing errors and saving time.

Native Integration with PAM Core
Includes native integration with Segura® PAM Core, centralizing the management of certificates and privileged access accounts in a single platform.

Publishing to Web Servers and Keystores
Simplify SSL/TLS deployment on servers, enhancing online security.

Visibility Dashboard
Gain a clear and strategic view of all your certificates, simplifying management and decision-making.

Integration with Certificate Authorities (CA)
Connect to leading CAs to securely request and issue certificates.

Personal Certificate Management
Manage digital certificates used in legally valid financial transactions and document signing processes.

Supports Zero Trust strategy
Strengthens Zero Trust architecture by ensuring trusted identities for machines and applications through continuous certificate issuance and validation.

DAGMA
IT SECURITY

EPM

EPM
Endpoint
Privilege
Management

In an era of increasingly complex IT infrastructures, rigorous control over administrative privileges and the efficient implementation of the Principle of Least Privilege are crucial for shielding security and minimizing the risks of data breaches.

This is where **Segura® Endpoint Privilege Manager (EPM)** comes in.

As a robust Privileged Elevation and Delegation Management (PEDM) solution, EPM empowers your users to execute privileged functions on Windows and Linux endpoints with security and control.

Privilege Execution Based on Approved Action Lists
Authorized users can invoke administrator privileges to run specific applications, ensuring that only critical applications requiring elevated privileges are executed securely.

Session Recording on Windows and Linux
Record sudo actions on Linux endpoints and sessions on Windows to meet audit requirements and ensure compliance, providing a complete trail of privileged activities.

Data Theft Prevention & Stop Privilege Abuse
The EPM solution correlates events to identify suspicious behavior and provides enhanced security measures to protect critical data assets. By isolating critical environments and correlating events, Segura® Endpoint Privilege Manager allows for early detection and mitigation of privilege abuse incidents.

Complete Action Traceability
Comprehensive tracking of privileged actions improves auditing processes, enables better forensic analysis, and ensures accountability within the infrastructure.

Login Information Integration in Group Policies (Linux only)
Validate each authentication based on time, calls, authorizations, and additional group policies, strengthening the security of your Linux endpoints.

Complete SUDO Management (Linux only)
Gain complete control over actions executed with SUDO on your Linux endpoints by defining granular policies for enhanced security.

Automated Application Execution and Access via Macros (Windows only)
Optimize repetitive tasks and boost productivity with automated execution while maintaining strict control over privileged actions.

Secure Access to Sensitive Data in Network Locations (Windows only)
Provides maximum security for shared files and directories on the network, protecting critical information from threats.

Access Control Panel with Administrative Privileges (Windows only)
Users can perform administrative tasks, such as changing date and time settings, ensuring effective management of essential system configurations.

Malware Analysis (Windows only)
Protect your Windows endpoints from cyber threats with the dedicated malware analysis functionality.

Workflow Creation (Windows only)
Automate and simplify tasks and processes with customized workflows, optimizing privilege management and increasing operational efficiency.

Offline Use (Windows only)
Manage the privileges of your Windows endpoints even when they are offline, ideal for scenarios with limited connectivity.

segura

DAGMA
IT SECURITY

Cloud IAM

Ensuring visibility and control over identities and access keys across Cloud Service Providers (CSPs) is crucial to maintaining compliance and security. The adoption of multi-cloud environments has made identity and access management a complex task for IT and security teams.

Ineffective control can lead to risks such as unauthorized access, compliance failures, and data breaches.

Segura® Cloud IAM offers a robust solution to ensure identity governance in hybrid and multi-cloud environments.

User and Access Key Management
Intuitive interface to manage identities and access keys, with audited user provisioning, deletion, and control.

Audited Provisioning and Deletion
Ensures that all operations for creating and deleting identities and access keys are logged and audited.

Centralized Visibility
Dashboards provide a unified view of all identities and access keys, facilitating management and auditing.

Audited Remote Access to CSP Console
Monitors and records all remote access sessions to CSP consoles, providing complete audit trails.

Automatic Compliance
Facilitates compliance with regulations such as SOX, GDPR, PCI-DSS, NIS2, among others, through access controls and session audits.

Just-in-Time (JIT) Access
Controls temporary access, ensuring that users have access only for a limited time and on-demand.

Identity Centralization
Unifies identity management from different CSPs, providing a consolidated view of all users and their permissions.

Recorded Sessions
Console access sessions are recorded, allowing for audit and review to ensure compliance.

Risk Reduction
Automate the management of users and permissions, reducing the risk of unauthorized access and ensuring that only the right users have appropriate permissions at the right time.

segura

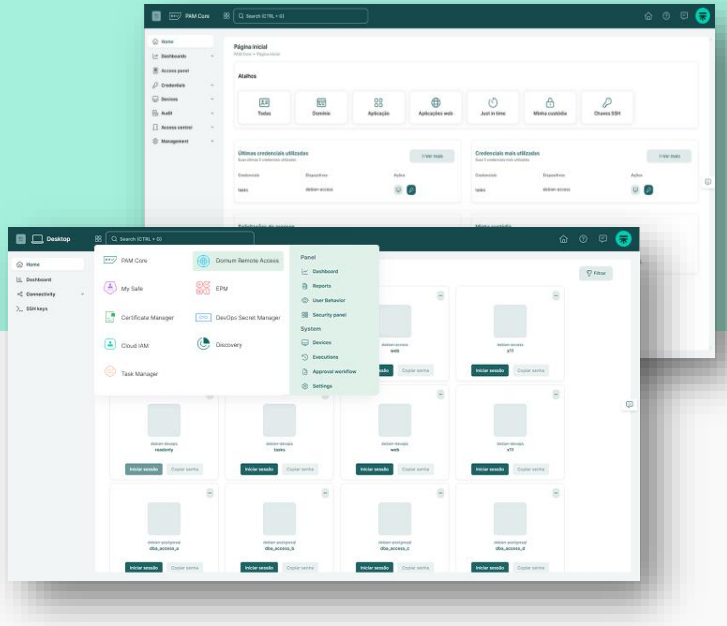
DAGMA
IT SECURITY

segura

DAGMA
IT SECURITY

Everything you need for privileged access management in a single, powerful platform.

No extra tools, no complexity - just complete protection.

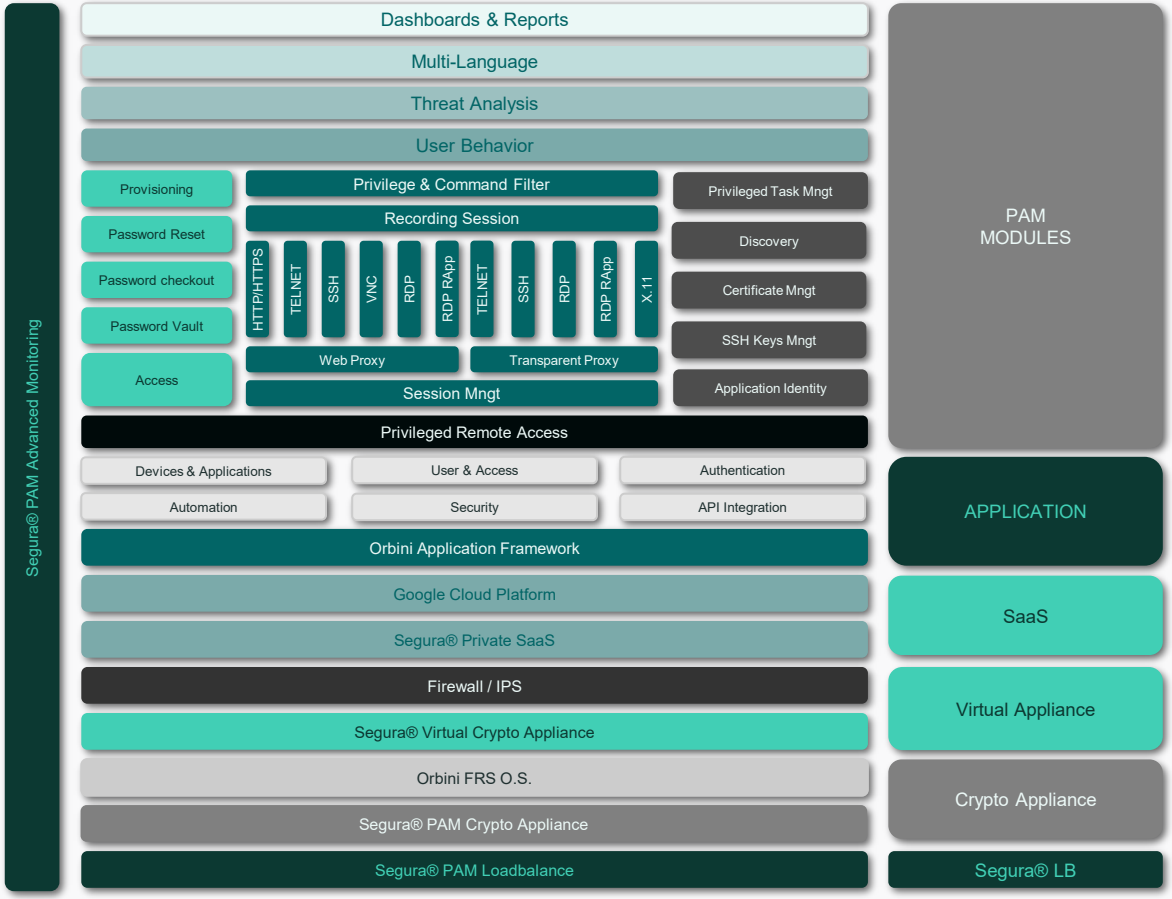


98%
Recommendation on Gartner Peer Insights

90%
Faster Time to Value (TTV)

70%
Lower Total Cost (TCO)

Full stack architecture



segura

DAGMA IT SECURITY

Direct. Personal. On equal footing.

We are happy to support!

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

OUR PORTFOLIO

Identity · Exposure · Detection · Enforcement

Bare.ID GATEWATCHER HADRIAN HOLM SECURITY segura Sekoia

DAGMA IT SECURITY

CYBERSECURITY FROM EUROPE