segura®

DATASHEET EN

PAM Core

Document Classification: Public | May 2025

segura®

PAM Core

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

This makes high-privilege credentials one of the favorite targets for malicious attackers to carry out their activities. In fact, 84% of cyberattacks are identity-related.

Additionally, regulatory requirements such as PCI, ISO, SOX, GDPR, LGPD, and NIST require IT administrators to review credential privileges and implement the principle of least privilege.

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.

How a PAM Solution Works

Problem

Lack of control over privileged credentials inhibits security accountability and increases the chances of cyberattacks.

Solution

Discover and manage all privileged credentials and create an effective process of authentication, authorization, and accountability for their use.

Impact

Reduce the attack surface by eliminating unnecessary credentials.

Features

Scan discovery

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

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.

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.

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.

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

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.

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

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

Other Differentiators

No additional costs
Segura® is a complete and integrated solution, including databases and operating systems, reducing deployment efforts.

Fast deployment
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.

Intuitive user interface
Recognized in the PAM market for its intuitive interface and excellent UX, resulting in less training and support time and cost.

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.

Customer recognition
Segura® is the highest-rated PAM solution on Gartner Peer Insights and has received the Customers' Choice award four times. It also achieved a 4.9-star rating and a 98% willingness to recomend in Gartner's Voice of the Customer report.

Discover the benefits of Segura® for your company

Watch Demo

/segura

segura.security

www.segura.security

segura®