segura

Gartner Peer Insights Customers' Choice 2025

Datasheet Segura®
PAM Core

May
2025

Visión general

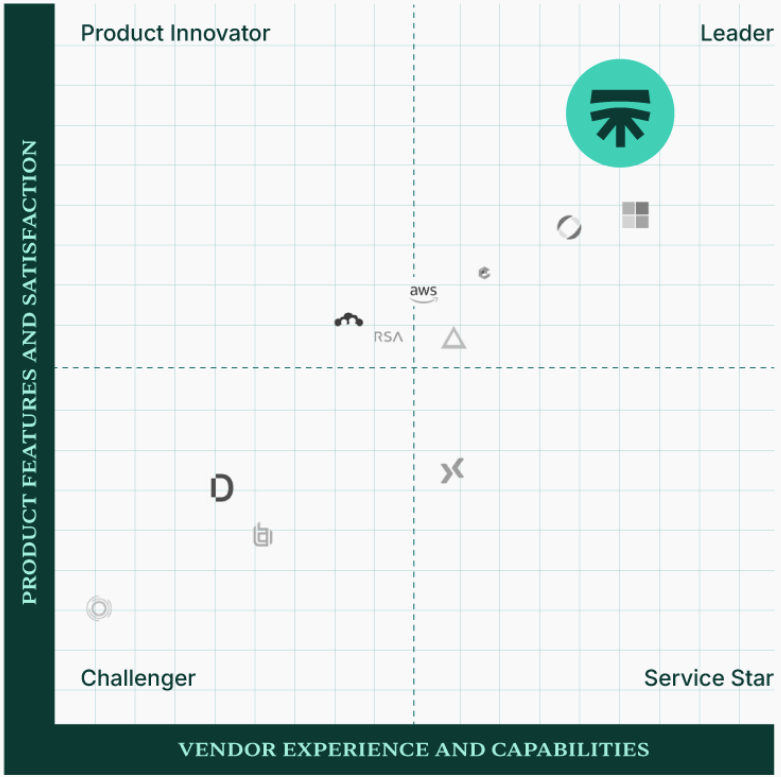
Las credenciales con privilegios proporcionan acceso a acciones críticas, como modificar la configuración del controlador de dominio o transferir fondos de las cuentas de una organización.

Esto hace que las credenciales de alto privilegio sean uno de los objetivos favoritos de los atacantes. De hecho, el 84% de los ciberataques están relacionados con la identidad.

Además, los requisitos normativos como PCI, ISO, SOX, GDPR, LGPD y NIST exigen que los administradores de TI revisen los privilegios de las credenciales y apliquen el principio del mínimo privilegio.

El objetivo de la Gestión de Acceso Privilegiado (PAM) es proteger y controlar el uso de credenciales genéricas y privilegiadas, proporcionando almacenamiento seguro, segregación de acceso y trazabilidad completa del uso.

La implantación de controles para proteger las credenciales privilegiadas debería formar parte de la estrategia de ciberseguridad de las organizaciones de todos los tamaños y sectores.



Cómo funciona una solución PAM

➔ **Problema**

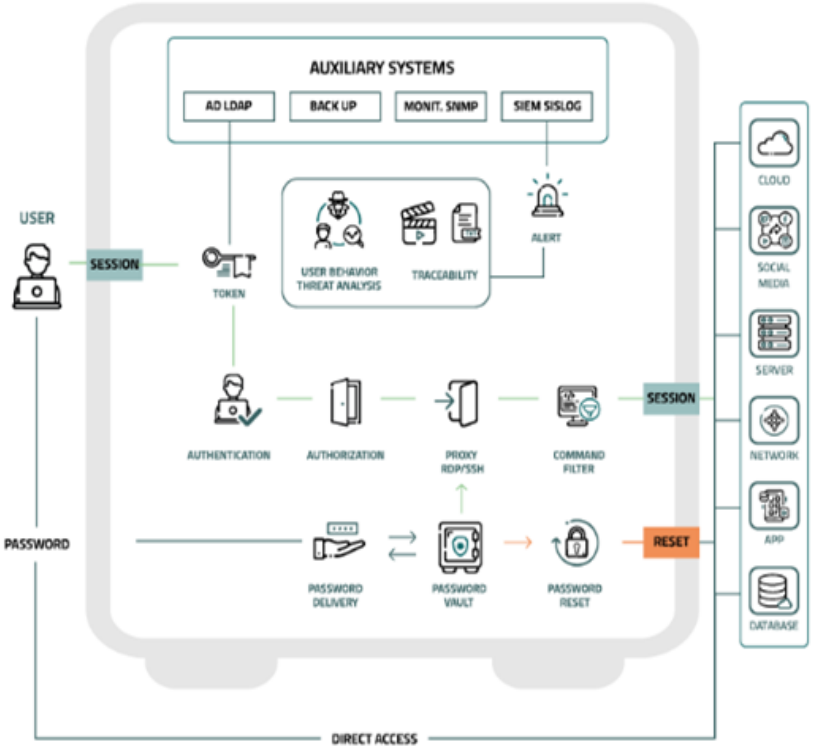
La falta de control sobre las credenciales privilegiadas inhibe la responsabilidad en materia de seguridad y aumenta las posibilidades de ciberataques.

➔ **Solución**

Descubra y gestione todas las credenciales privilegiadas y cree un proceso eficaz de autenticación, autorización y responsabilidad para su uso.

➔ **Impacto**

Reduzca la superficie de ataque eliminando las credenciales innecesarias.



Features

➔ **Escaneo de descubrimiento**

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

➔ **Grabación de sesiones**

Las grabaciones de sesiones permiten registrar todas las acciones realizadas durante un acceso con privilegios elevados, con el objetivo de cumplir con las auditorías y permitir la investigación en caso de incidentes o abuso de privilegios.

➔ **Rotación automática de credenciales**

La rotación automatizada de credenciales garantiza que las contraseñas con privilegios elevados no sean estáticas, lo que reduce la superficie de ataque y mitiga los ataques de fuerza bruta y de diccionario.

➔ **Flujos de aprobación**

El flujo de trabajo de aprobación garantiza el principio de los cuatro ojos, según el cual la ejecución de acciones privilegiadas debe ser aprobada por al menos dos personas, lo que garantiza la transparencia y el control de las autorizaciones.

➔ **Auditoria de Comandos**

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

➔ **App to app (A2A)**

Como nuestra interfaz API, A2A permite que aplicaciones de terceros se integren con Segura® , utilizando información gestionada de forma autenticada y segura.

➔ **KDI (Identidad dinámica de pulsación de teclas)**

Las funciones basadas en IA permiten analizar los patrones de pulsación de teclas de los usuarios para detectar posibles actividades maliciosas mediante credenciales robadas.

➔ **Just in time**

Activar/desactivar o crear/eliminar accesos en tiempo real.

Beneficios

➔ **Sin costes adicionales**

Segura® es una solución completa e integrada, que incluye bases de datos y sistemas operativos, lo que reduce los esfuerzos de implantación.

➔ **Despliegue rápido**

Tiene el tiempo de implantación más corto del mercado. En solo 7 minutos es posible configurar y entregar una arquitectura de software y hardware con alta disponibilidad y recuperación ante desastres.

➔ **Interfaz de usuario intuitiva**

Reconocida en el mercado PAM por su interfaz intuitiva y su excelente UX, lo que se traduce en menos tiempo y costes de formación y asistencia.

➔ **Conectores abiertos**

La detección y gestión de dispositivos y credenciales se realiza a través de conectores abiertos basados en tecnología, no en proveedores. Permiten la conexión con dispositivos heredados y pueden ser desarrollados por el cliente sin necesidad de servicios profesionales.

➔ **Reconocimiento de los clientes**

Segura® ha recibido dos veces el premio Customer's Choice en el informe Voice of the Customer de Gartner.

➔ **100% de recomendación**

Segura® obtuvo un índice de recomendación del 100% y una calificación de 5 estrellas en el informe Voice of the Customer 2022, la más alta del mercado de PAM.

segura

Gartner Peer Insights Customers' Choice 2025

Datasheet Segura®
PAM Core

Apr
2025

Segura is a leading cybersecurity company specializing in Privileged Access Management (PAM) solutions that help organizations tackle ransomware, insider threats, risky user behavior, and secure Human-to-Machine (H2M) and Machine-to-Machine (M2M) communications. Our comprehensive and affordable platform ensures optimal protection of your organization's critical assets while offering exceptional customer support.

segura | Futureproof Identity Security | segura.security