

Gestión de Accesos Privilegiados

ASEGURANDO LO QUE REALMENTE IMPORTA



Sectona - PAM Es una solución integral de gestión de privilegios, creada para proteger lo que realmente importa: las cuentas privilegiadas.

Sectona-PAM está diseñada cuidadosamente para ayudar a las organizaciones a atender y adaptarse con facilidad a las necesidades emergentes. Permite a una amplia variedad de usuarios —ya sean administradores principales, proveedores remotos o desarrolladores— acceder de forma segura a sistemas y aplicaciones críticos desde cualquier equipo, en cualquier lugar y en cualquier momento.

Aspectos destacados de Sectona PAM

Gestión de sesiones multiplataforma
Acceso ágil y transparente para los usuarios, sin importar dónde se encuentren.

Monitoreo inteligente y gobierno integrado
Revisiones basadas en riesgos con registros completos y análisis de privilegios.

Arquitectura ligera y para múltiples ubicaciones
Despliegue flexible y a la medida de cualquier organización.

Bóveda empresarial de máximo nivel
Autogestionada y no expuesta, asegura un almacenamiento inviolable de credenciales, llaves SSH y secretos.

Análisis avanzado de sesiones
Interpreta datos en texto y video para anticipar riesgos y reforzar la seguridad de forma proactiva.

40%

De ahorro de costos

Gracias a su arquitectura ligera y componentes integrados.

90%

De retención de clientes,

Garantizando confianza en el soporte postventa.

2x

Ciclos de implementación

Más rápidos con paquetes a medida que aceleran tu camino en la gestión de accesos privilegiados.

Funcionalidades principales



Descubrimiento continuo

Reducción de hasta 99% del tiempo en conciliación de cuentas privilegiadas.



Gestión de contraseñas

Bóveda empresarial autogestionada y no expuesta, garantizando almacenamiento inviolable de credenciales, llaves SSH y secretos.



Acceso Just-In-Time

Elimina los privilegios permanentes y aprovecha la combinación de enfoques para implementar políticas Just-In-Time.



Gobernanza de accesos privilegiado

Mejora la seguridad y el cumplimiento con un módulo integrado para la supervisión y el control centralizados de las cuentas privilegiadas y sus permisos dentro de una organización.



Gestión de secretos DevOps

Elimina la necesidad de incluir a nivel del código (hardcode), secretos incrustados en los tareas desarrollo-prueba-deployment (DevOps), reduce los riesgos de seguridad y respalda los requisitos de cumplimiento mediante el uso de accesos autorizados a través de APIs.



Revisión automatizada de accesos privilegiados

Programa y realiza revisiones periódicas de las cuentas privilegiadas y sus permisos para eliminar privilegios innecesarios.



Análisis de cuentas privilegiadas

Supervisa y analiza el comportamiento de los usuarios privilegiados en diversos sistemas para detectar actividades sospechosas o anómalas que puedan indicar posibles brechas de seguridad o amenazas internas.



Arquitectura distribuida y alta disponibilidad

Implementa PAM fácilmente en distintas regiones o sedes, en la nube o en entornos locales, con capacidades de replicación integradas, manteniendo la flexibilidad para gestionar la autenticación de manera centralizada o mediante un enfoque distribuido.



Autenticación multifactor

Habilita la autenticación multifactor integrada con tokens basados en SMS y aplicaciones, y permite soluciones de MFA en la nube como Okta, Cisco Duo, Google Authenticator, entre otras.



Gestión de cuentas de servicio

Mantiene el control de las cuentas de servicio distribuidas en la infraestructura de TI mediante el descubrimiento dedicado de cuentas de servicio y la gestión de contraseñas.



Gestión de contraseñas de aplicaciones

Protege las contraseñas y secretos almacenados en archivos de configuración o scripts, o incrustados en aplicaciones.



Gestión de tareas privilegiadas

Reduce los inicios de sesión innecesarios de los administradores mediante la automatización de la asignación de privilegios, permitiéndoles concentrarse en operaciones de alta prioridad o sensibles.



Desarrollo simple de conectores

Integra y gestiona el acceso a aplicaciones personalizadas y/o complementos de forma dinámica, sin incrementar la carga operativa ni requerir el desarrollo de habilidades internas específicas.



Acceso remoto seguro (sin VPN)

Habilita el acceso remoto sin VPN para las fuerzas laborales modernas, proporcionando a los equipos externalizados acceso a través de la plataforma Sectona, lo que reduce los riesgos operativos y técnicos.



API extensible

Gran Flexibilidad con el API RESTful de la plataforma para integrar, conectar y orquestar el ecosistema tecnológico, encaminado en la transformación digital.

¿Por qué Sectona?

Ir más allá

Integra no solo RDP y SSH, sino también aplicaciones web, utilitarios especializados y clientes pesados bajo demanda con un kit DIY de desarrollo de plugins.

Escalar con facilidad

Controla entornos en la nube o locales, de un solo sitio a múltiples, gracias a componentes flexibles y desacoplados.

Confiabilidad y seguridad

Bóveda integrada con disponibilidad comercial de alta gama, evitando pérdidas de datos y con seguridad robusta.

Mayor valor

ROI más alto con MFA integrado, gobernanza de accesos privilegiados y análisis de cuentas privilegiadas.



Sectona is a Privileged Access Management company that helps enterprises mitigate the risk of targeted attacks on privileged accounts spread across data centres and the cloud. Sectona helps secure dynamic remote workforce access across on-premise or cloud workloads, endpoints and machine-to-machine communication.

Más información en: www.sectona.com and Síguenos en [@SectonaTech](https://twitter.com/SectonaTech) on X (Twitter) or [@Sectona](https://www.linkedin.com/company/sectona) on LinkedIn

Distribuidor Autorizado

Green Light Technology

555 Winderley Place Suite 300, Maitland, FL, 32751. USA | glinfo@greenlt.com | www.greenlt.com