ENDPOINT PRIVILEGE MANAGER

Implemente políticas de acceso de privilegio mínimo, elimine los derechos de administrador permanentes y habilite el acceso Just-In-Time (JIT) tanto a nivel de proceso como de máquina, con la gestión de privilegios de punto de conexión en Windows, Linux y macOS.

Los controles de accesos con privilegios robustos son esenciales para que las organizaciones fortalezcan su postura de seguridad, aseguren la eficiencia operativa y respeten los requisitos de cumplimiento normativo.

Keeper Endpoint Privilege Manager protege los puntos de conexión a través de agentes livianos que eliminan los derechos de administrador permanentes, y permiten la ampliación temporal de los privilegios basada en políticas solo en caso necesario. El sistema impone políticas de seguridad personalizables mediante el acceso JIT con flujos de trabajo de aprobación opcionales y la aplicación de la autenticación multifactor (MFA).

Las acciones con privilegios pueden ejecutarse mediante cuentas efímeras que se aprovisionan y desaprovisionan automáticamente para cada sesión, o ampliando temporalmente los privilegios de cuentas de usuario estándar. Las organizaciones pueden elegir cualquiera de los dos métodos en función de su postura de seguridad y sus necesidades operativas.

Keeper Endpoint Privilege Manager funciona en entornos Windows, macOS y Linux, a la vez que proporciona visibilidad a través de un panel centralizado que registra todas las actividades de elevación para la auditoría y el cumplimiento.

Beneficios de Keeper Endpoint Privilege Manager

Seguridad

Elimina los derechos de administrador permanentes y permite la elevación justo a tiempo solo para aplicaciones aprobadas para reducir las superficies de ataque y mejorar la seguridad.

Cumplimiento

Proporciona registros de auditoría exhaustivos del uso de los privilegios y garantiza el cumplimiento de los requisitos normativos mediante un control de acceso administrativo documentado

Eficiencia operativa

Reduce la carga de trabajo del servicio de asistencia al automatizar las aprobaciones para tareas administrativas rutinarias.

Experiencia de usuario

Permite a los usuarios completar las tareas necesarias sin retrasos del departamento de TI mediante la elevación automatizada de privilegios para aplicaciones aprobadas.

Escalabilidad

Permite a las organizaciones aplicar de forma eficiente las políticas de mínimos privilegios y gestionar el acceso privilegiado a miles de endpoints de Windows, macOS y Linux desde una plataforma centralizada.

Auditabilidad y visibilidad

Proporciona información sobre la actividad de ampliación, las aprobaciones y la aplicación de políticas de puntos de conexión con un registro detallado e integración en herramientas SIEM para responder más rápido a los incidentes.

Aprenda más
keepersecurity.com

Solicite una demostración
keeper.io/demo

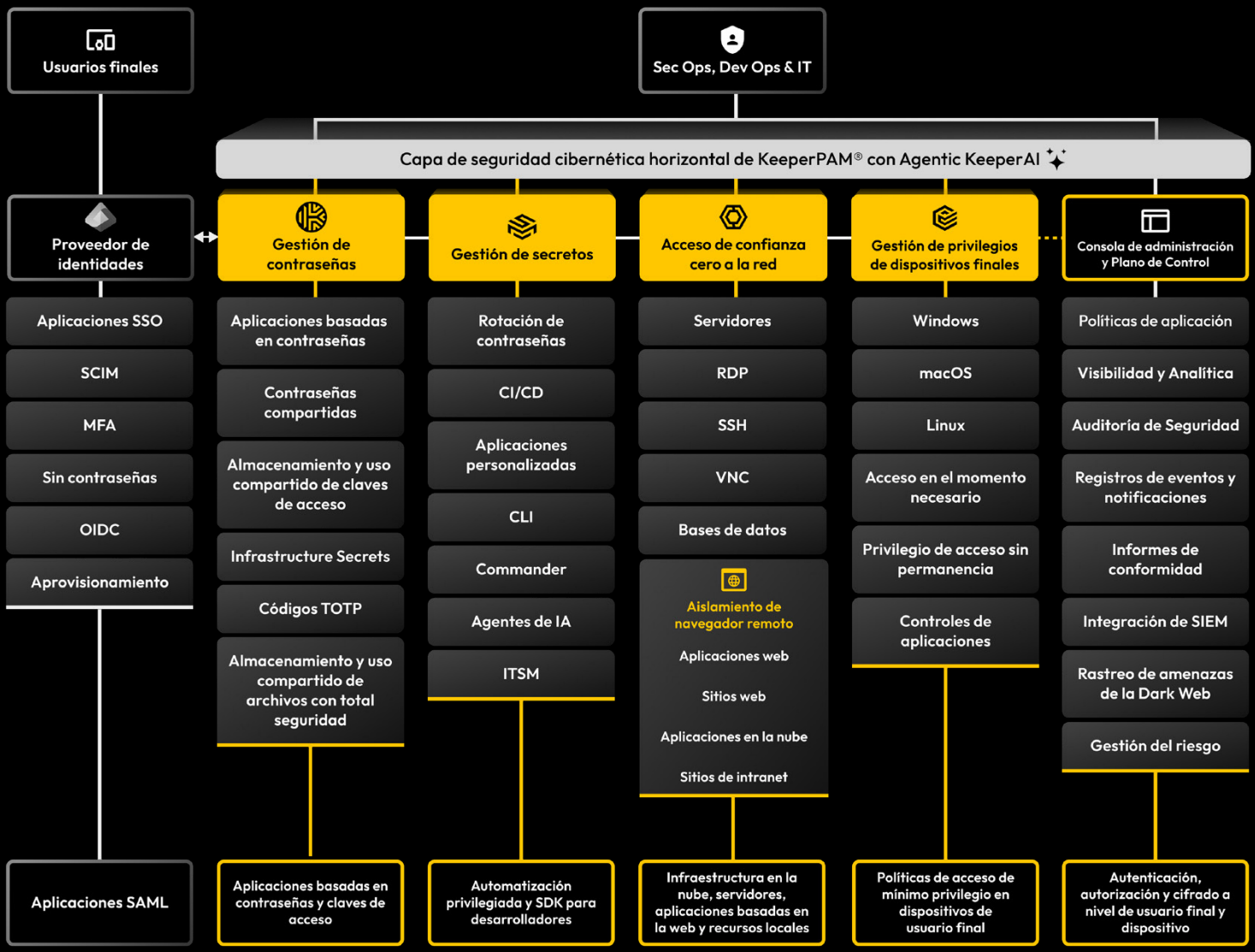
Consultas de socios
partners@keepersecurity.com

Acerca de Keeper Security

Keeper Security está transformando la ciberseguridad para las personas y las organizaciones de todo el mundo. Las soluciones intuitivas de Keeper están diseñadas con cifrado de extremo a extremo para proteger a todos los usuarios, en todos los dispositivos y en todas las ubicaciones. Con la confianza de millones de personas y miles de organizaciones, Keeper es el líder en gestión de acceso privilegiado.

KEEPER PAM

Plataforma de gestión del acceso privilegiado de Keeper



Extienda la confianza cero a los puntos de conexión

Endpoint Privilege Manager amplía el enfoque de confianza cero de KeeperPAM, al controlar la ampliación de privilegios directamente en los puntos de conexión, complementando las capacidades de conexión segura de la solución PAM más extensa. Mientras que el resto de la plataforma KeeperPAM protege la forma en que se conectan los usuarios a los sistemas, Endpoint Privilege Manager regula qué derechos administrativos pueden ejercer una vez conectados.

Cómo Keeper eleva privilegios

1. **Política** - si una aplicación o proceso requiere ampliación, el agente Keeper comprueba la política pertinente.
2. **Aprobación** - si se requiere la aprobación, la solicitud se envía a un administrador a través de la consola de administración o la interfaz de línea de comandos (CLI).
3. **Opción MFA** -si no se requiere la aprobación, la ampliación se produce automáticamente. La aplicación de MFA es un paso adicional opcional.