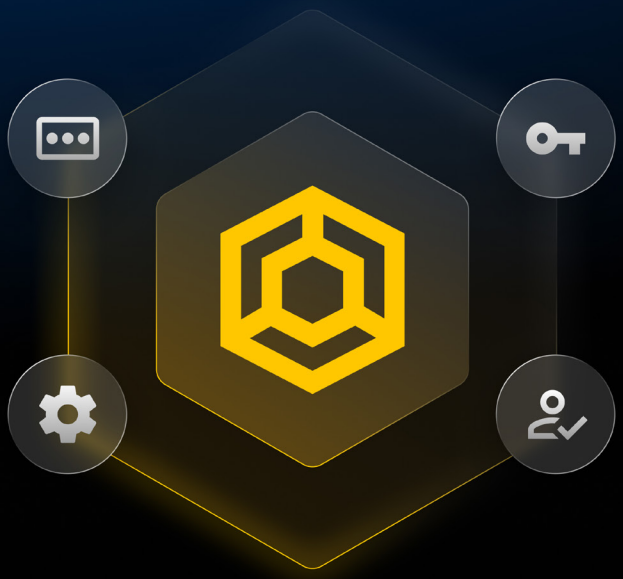
CASO PRÁCTICO

Asite protege credenciales, secretos y accesos privilegiados a nivel de empresa con KeeperPAM®



Contexto

Asite es una empresa de SaaS que presta servicios al sector de la construcción y ayuda a las organizaciones a gestionar proyectos complejos —desde modelos 3D y gemelos digitales hasta el control de documentos y la colaboración con proveedores— en equipos y regiones de todo el mundo. Asite opera en diversas zonas geográficas, con centros de datos en nueve ubicaciones y una plantilla de más de 500 empleados.

Sector
Tecnología de la construcción (SaaS)

Empleados
Más de 500

Soluciones
KeeperPAM

El reto

Para una empresa internacional de SaaS que presta apoyo a importantes programas de construcción, entre los que se incluyen clientes que operan en infraestructuras críticas y entornos relacionados con la defensa, es esencial garantizar la gestión segura de las credenciales y el acceso privilegiado. Asite necesitaba un enfoque más centralizado y fácil de aplicar en materia de contraseñas, secretos y gestión del acceso privilegiado (PAM) en toda la organización.

Herramientas heredadas con visibilidad fragmentada -la dependencia de los gestores de contraseñas basados en navegadores limitaba la visibilidad y el control , lo que aumentaba el riesgo debido a la reutilización de contraseñas, las credenciales débiles y una capacidad reducida para aplicar controles de seguridad que garantizasen el cumplimiento normativo y la seguridad de los clientes. Los anteriores proveedores de gestión de secretos y PAM de la organización eran costosos y difíciles de implementar.

Además de proteger a los usuarios internos, Asite necesitaba ampliar el mismo nivel de protección a los socios externos y proveedores que colaboraban en proyectos de construcción complejos, para garantizar que cumplieran con las expectativas de los clientes y las obligaciones contractuales. La organización buscaba una solución segura y fácil de usar que pudiera satisfacer todas sus necesidades de ciberseguridad dentro de una plataforma centralizada.

> **«La arquitectura (de seguridad) y la flexibilidad con KeeperPAM es insuperable».**
>
> **Tiago Rosado | Director de Seguridad de la Información**

La solución de Keeper

Asite seleccionó **KeeperPAM** como su plataforma unificada para proteger el acceso privilegiado, las credenciales, las conexiones y los secretos en toda la organización. Al centralizar su tecnología de ciberseguridad en una única plataforma de confianza y conocimiento cero, Asite redujo la complejidad y mejoró la seguridad y el cumplimiento normativo.

Acceso privilegiado centralizado con bajos costes operativos - KeeperPAM proporciona un acceso privilegiado seguro y auditable a servidores, infraestructuras y sistemas confidenciales sin exponer las credenciales. La actividad de las sesiones se registra y almacena de forma centralizada, lo que facilita las investigaciones, la rendición de cuentas y el cumplimiento normativo en entornos regulados y de clientes. KeeperAI finaliza automáticamente las sesiones de alto riesgo y genera resúmenes de actividad con detalles forenses precisos que facilitan la auditoría y la respuesta ante incidentes.

Gracias a su rápida implementación y su arquitectura flexible, KeeperPAM sustituyó las herramientas heredadas de gestión de PAM y secretos de Asite, al tiempo que amplió la cobertura del acceso privilegiado a otros sistemas sin aumentar el coste ni la complejidad.

> **«La implementación de KeeperPAM fue sumamente sencilla, una de las mejores según mi experiencia. Ojalá otras herramientas fueran tan fáciles de implementar».**
>
> **Tiago Rosado | Director de Seguridad de la Información**

Enterprise Password Management, integrada en KeeperPAM - dentro de la plataforma KeeperPAM, Asite estandarizó la **gestión de contraseñas** en toda la empresa para todos los empleados, sustituyendo los gestores de contraseñas basados en navegadores y estableciendo un enfoque centralizado y fácil de aplicar para la seguridad de las credenciales.

De este modo, se pudieron aplicar políticas de contraseñas controladas por el administrador en cuanto a longitud y complejidad y se evitó la reutilización de credenciales en diferentes aplicaciones. El equipo de TI ahora puede identificar las credenciales comprometidas utilizando la herramienta de supervisión de la web oscura de Keeper, BreachWatch®, lo que refuerza aún más la estrategia de seguridad de la organización. El acceso a la gestión de contraseñas dentro de la misma bóveda que KeeperPAM garantiza una gobernanza uniforme tanto para las credenciales de los usuarios finales como para las privilegiadas, además de una experiencia de usuario más sencilla.

Gestión moderna de secretos con Keeper Secrets Manager - para proteger los secretos de las aplicaciones y la infraestructura, Asite implementó **Keeper Secrets Manager** como componente nativo de la plataforma KeeperPAM, en sustitución de su anterior herramienta de gestión de secretos. Keeper Secrets Manager automatiza la creación y rotación de contraseñas, claves y secretos, elimina las credenciales de larga duración o que se gestionan manualmente y se integra fácilmente a través de **API sencillas y una documentación exhaustiva**, todo ello con unos costes operativos mínimos para los equipos de TI y seguridad.

> **«Los costes operativos son mínimos... la automatización y rotación de contraseñas y claves es fantástica».**
>
> **Tiago Rosado | Director de Seguridad de la Información**

La gestión de los secretos junto con las contraseñas y el acceso privilegiado en KeeperPAM permitió una gobernanza uniforme de identidades humanas y no humanas.

La mejor seguridad de su clase - la arquitectura de seguridad de confianza y de conocimiento cero de Keeper es incomparable a la hora de proteger la información y mitigar el riesgo de violaciones de datos. Keeper combina a nivel de dispositivo la criptografía de curva elíptica (ECC) con **varias capas de cifrado** (a nivel de bóveda, carpeta y registro), autenticación multifactor y biométrica, así como cifrado AES de 256 bits validado por FIPS 140-3 más PBKDF2. Keeper es **compatible con SOC 2 e ISO 27001** —con la conformidad más antigua del sector— y cuenta con la autorización de FedRAMP High y GovRAMP.

Impacto en la organización

Al implantar la plataforma PAM completa de Keeper para gestionar contraseñas, secretos y accesos privilegiados, Asite estableció un marco de seguridad unificado y escalable que mejora la protección y reduce la complejidad operativa para sus equipos de TI y seguridad.

Mejora de la posición de seguridad con resultados cuantificables – la centralización de la gestión de credenciales y accesos permitió a Asite reforzar significativamente su posición de seguridad general. Una mayor protección de las contraseñas, la rotación automatizada de secretos y el control del acceso privilegiado redujeron la exposición tanto a amenazas externas como a riesgos internos. Las credenciales ya no se crean, comparten ni reutilizan manualmente, lo que favorece la aplicación sistemática de las políticas de seguridad en toda la organización.

Es fundamental destacar que estos controles son cuantificables y auditables, lo que ayuda a cumplir los requisitos normativos y contractuales en todas las zonas geográficas y entornos de clientes.

> **«Las principales ventajas de la plataforma KeeperPAM serían la reducción de costes, la reducción de la gestión de los costes operativos de los sistemas, un mayor cumplimiento de los requisitos de seguridad y, sin duda, una posición de seguridad reforzada».**
>
> **Tiago Rosado | Director de Seguridad de la Información**

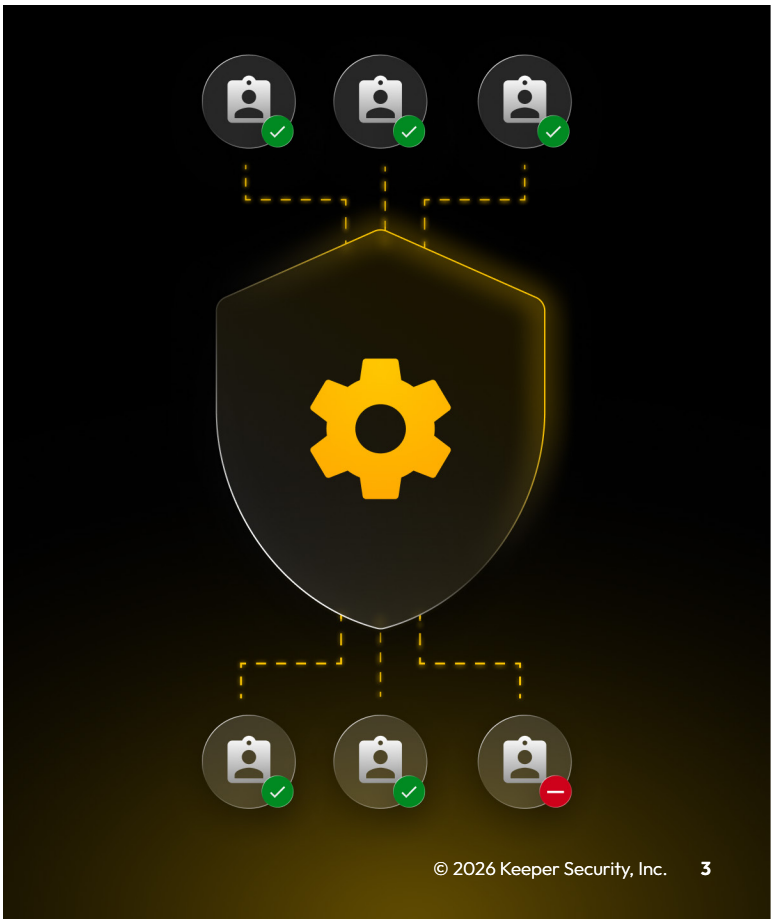
Reducción de los costes operativos y unificación de herramientas – al unificar la gestión de contraseñas, la gestión de secretos y la gestión de acceso privilegiado (PAM) en una única plataforma, Asite redujo la proliferación de herramientas y simplificó la administración, lo que redujo los costes operativos. Esta estrategia permitió a los equipos de TI y seguridad gestionar los controles de acceso de forma más eficiente sin aumentar la plantilla ni la carga operativa, al tiempo que se ampliaba la cobertura para proteger una gama más amplia de sistemas y entornos.

Menor exposición al riesgo interno y mayor responsabilidad – gracias a la gestión y monitorización centralizadas del acceso privilegiado, Asite reforzó su capacidad para detectar, investigar y responder a actividades de alto riesgo. La monitorización de sesiones y los registros de auditoría facilitan la rendición de cuentas y reducen la probabilidad de uso indebido, ya sea intencionado o accidental.

Colaboración y capacitación continuas – más allá de la tecnología, Asite destacó la importancia de contar con un servicio de asistencia y capacitación fiables durante todo el proceso de implementación y adopción. Los equipos de asistencia y capacitación de Keeper desempeñaron un papel fundamental a la hora de garantizar que la plataforma se implementara de forma eficaz y se ajustara a las necesidades operativas de la organización.

> **«La calidad del servicio de asistencia: incluso si se trata de la pregunta más técnica, la analizan en profundidad [...] El equipo de formación [fue] absolutamente fundamental, ya que adaptó la formación a nuestra realidad».**
>
> **Tiago Rosado | Director de Seguridad de la Información**

KeeperPAM se convirtió en la base de la estrategia de seguridad de acceso de Asite, al proporcionar un control centralizado sobre las identidades humanas y no humanas en entornos internacionales. Al reunir el acceso privilegiado, la gestión de contraseñas y la gestión de secretos en una única plataforma, Asite reforzó la seguridad, mejoró la eficiencia operativa y estableció una base flexible para impulsar el crecimiento en el futuro.



KeeperPAM

KeeperPAM es una plataforma de gestión de acceso privilegiado de última generación que protege y gestiona el acceso a recursos críticos, como servidores, aplicaciones web, bases de datos y cargas de trabajo. Basada en una arquitectura de seguridad de confianza cero y conocimiento cero, KeeperPAM ayuda a organizaciones de cualquier tamaño a proteger cuentas privilegiadas, aplicar el principio del mínimo privilegio, proteger la infraestructura remota y cumplir los requisitos de conformidad, con una facilidad de uso y una rapidez de implementación sin igual.

Keeper es intuitivo y fácil de implementar, independientemente del tamaño de la empresa. KeeperPAM utiliza un servicio de puerta de enlace de confianza cero para acceder a cada entorno. No se necesitan actualizaciones del cortafuegos ni cambios de entrada, lo que permite un acceso seguro y sin complicaciones. Gracias a las funciones de sesión remota, el usuario nunca tiene acceso a las credenciales ni a las claves SSH. El acceso a un recurso puede estar limitado en el tiempo, y las credenciales rotan automáticamente después de que se haya revocado el acceso, lo que proporciona un acceso justo a tiempo (JIT) sin exponer nunca las credenciales.

Keeper está diseñado para adaptarse a organizaciones de cualquier tamaño. KeeperPAM centraliza el acceso en una única interfaz de usuario (UI) en distintos proveedores de nube, cargas de trabajo locales y entornos de clientes, lo que permite la gestión multinube.

Casos de uso empresarial: KeeperPAM

- Controlar y monitorizar todas las cuentas privilegiadas
- Proporcionar acceso JIT sin exponer credenciales
- Unificar las herramientas de desarrollo en una plataforma con una interfaz de usuario intuitiva
- Gestionar fácilmente los entornos de nube, híbridos y multinube
- Grabar sesiones multiprotocolo con detección de amenazas de IA y terminación automática de sesiones
- Automatizar la rotación de contraseñas
- Aplicar la protección MFA en todos los sistemas
- Implementar sin problemas a través de la app web o de escritorio con aprovisionamiento automatizado de SCIM

Proteja su organización con Keeper

Para más información sobre cómo Keeper puede proteger su organización con una plataforma fácil de usar, **comuníquese con nuestro equipo de ventas** para obtener una prueba gratuita o una demostración personalizada.

Acerca de Keeper

Keeper Security es una de las empresas de software de ciberseguridad de mayor crecimiento, que protege a miles de organizaciones y millones de personas en más de 150 países. Keeper es pionera en seguridad de conocimiento y confianza cero, diseñada para cualquier entorno de TI. Su oferta principal, KeeperPAM®, es una plataforma nativa en la nube con inteligencia artificial que protege a todos los usuarios, dispositivos e infraestructuras de los ciberataques. Reconocida por su innovación en el Magic Quadrant de Gartner para la gestión de accesos privilegiados (PAM), Keeper protege contraseñas y claves de acceso, secretos de infraestructura, conexiones remotas y puntos finales con políticas de aplicación basadas en roles, privilegios mínimos y acceso justo a tiempo.

Miles de empresas y millones de personas de todo el mundo confían en Keeper.

Gartner

KeeperPAM® reconocida en Magic Quadrant™ 2025 de Gartner en la categoría PAM

Premio a la Excelencia en Ciberseguridad
Gestión del acceso privilegiado

Cyber Defense Magazine
Premio del Editor: Privileged Access Management (PAM)

Newsweek
La mejor plataforma de ciberseguridad

Enterprise Management Associates
KeeperPAM® reconocido por la solidez de su producto