

Gestión de secretos de CipherTrust

Proteger secretos a escala

CipherTrust Secrets Management (CSM) es una solución de gestión de secretos de última generación, impulsada por la plataforma **Akeyless Vault**, que protege y automatiza el acceso a secretos de misión crítica a través de herramientas **DevOps** y cargas de trabajo en la nube, incluidos secretos, credenciales, certificados, llaves API y tokens. Las nuevas funciones mejoran las capacidades de la plataforma **CipherTrust Data Security** para ayudar a los equipos de seguridad y gobierno a reducir los riesgos al optimizar los procesos de seguridad en todas sus operaciones.

La gestión de secretos lista para la empresa proporciona procesos automáticos para crear, almacenar, rotar y eliminar secretos. Reduzca la posibilidad de errores humanos y aplique sistemáticamente políticas de seguridad en toda su organización con:

- Gestión centralizada para todos los tipos de secretos
- Funcionalidad automatizada y fácil de usar para DevSecOps
- Escalabilidad SaaS (Software como Servicio) para entornos híbridos y multinube.

Protección integral de datos con gestión de secretos en una sola herramienta

The screenshot displays the THALES CipherTrust Manager dashboard. On the left, a navigation menu lists categories like Products, Access Management, Keys, CA, Alarms, Records, Quorums, and Admin Settings. The main area features a grid of feature cards:

- Data Discovery and Classification:** Find Sensitive Data in your Systems
- Cloud Key Manager:** Manage and bring your own keys to the cloud
- Transparent Encryption:** Transparently Encrypt Data at Rest, On-premise and in the Cloud
- Database Protection:** Configure Column and Field Encryption for your Databases
- ProtectFile & Transparent Encryption UserSpace:** Configure File and Folder Encryption
- Secrets Store:** Secure your credentials, certificates and keys
- Credential Rotation:** Maintain compliance and security across your organization
- Secrets Sharing:** Collaborate more securely and enable auditing with secure secrets sharing
- Secure Kubernetes Secrets:** Automate, encrypt, and manage all your Kubernetes secrets
- Just-in-Time Credentials:** Eliminate standing privileges with temporary access
- Short-Lived SSH Certificates:** Simplify management of SSH keys

A callout box on the right highlights the **Secrets Management** feature, stating: "Manage application secrets with Akeyless Vault".

Bóveda segura para todos los tipos de secretos

CSM, impulsado por Akeyless Vault, permite una gestión completa de los secretos de credenciales, certificados y claves. Esto incluye secretos estáticos, secretos dinámicos, claves SSH, claves API y tokens.

Los principales casos de uso incluyen:

- Tienda de secretos
- Rotación de credenciales automatizada
- Compartir secretos
- Generación y gestión de secretos dinámica y justo a tiempo.
- Registros de secretos utilizados para auditoría y cumplimiento.

Gestión de claves y gestión de secretos desde una sola herramienta

Combinar la gestión de secretos con la gestión de claves es como tener una bóveda fortificada para todos sus activos valiosos en un solo lugar. Genere eficiencias confiando en un proveedor para todas sus necesidades de protección de datos. Ninguna otra organización ofrece la amplitud y profundidad de protección de datos que proporciona la plataforma de protección de datos CipherTrust. Con una única plataforma, puede realizar la transición sin problemas a la plataforma Akeyless Vault a través de una puerta de enlace segura sin iniciar sesión por separado.

Reducir la complejidad operativa

El 62% de las organizaciones hoy en día no sabe cuántas claves o certificados tienen en toda su empresa¹. Esto los deja vulnerables a accesos no autorizados e infracciones. A medida que DevSecOps utiliza más servicios y herramientas para crear soluciones, dependen de claves y secretos para autenticar estas herramientas y servicios entre sí y en la nube. En consecuencia, la proliferación

de secretos se convierte en un riesgo cada vez mayor. A medida que la cantidad de secretos aumenta exponencialmente con la cantidad de servicios y herramientas utilizados en su organización, la expansión de los secretos crea riesgos significativos al facilitar que los atacantes malintencionados accedan a sus secretos y los comprometan.

Mejore la eficiencia de DevSecOps con una separación total de funciones

DevSecOps puede integrar rápidamente la gestión de claves, las operaciones de cifrado y la gestión de secretos en aplicaciones multinube para asegurar y acelerar los procesos de integración y entrega continua. En un entorno DevSecOps, la separación total de funciones implica distribuir responsabilidades relacionadas con la gestión de claves, las operaciones de cifrado y la gestión de secretos entre varios equipos o individuos. La separación total de funciones ayuda a prevenir violaciones de seguridad, promueve la responsabilidad y mejora la eficiencia general de los procesos de desarrollo, seguridad y operaciones.



Contáctenos: para conocer todas las ubicaciones de las oficinas e información de contacto, visite cpl.thalesgroup.com/contact-us

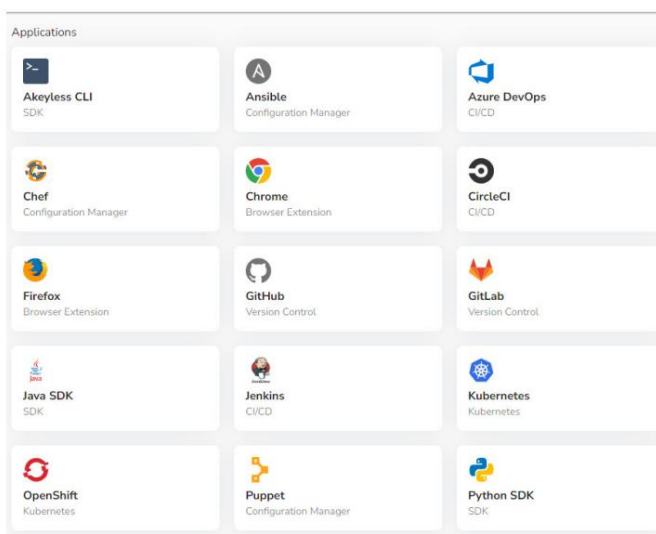
¹ Informe sobre el estado de la gestión de identidades de las máquinas de 2023

Soluciones híbridas y multinube

Pasar a la nube es una transición que a menudo resulta en entornos híbridos de múltiples nubes, con algunos recursos locales y otros distribuidos en múltiples nubes públicas y privadas. CSM está diseñado para funcionar en estos entornos y configuraciones.

Integración perfecta

CSM impulsado por Akeyless Vault se integra fácilmente con otras aplicaciones de terceros como GitHub, Kubernetes, OpenShift y más.



Implemente y escale rápidamente

Se puede acceder fácilmente a CipherTrust Secrets Management desde el panel de CipherTrust Manager. Se puede acceder a CSM desde el panel de CipherTrust Manager a través de un mosaico que utiliza las mismas credenciales utilizadas para acceder a CipherTrust Manager. Esto hace que empezar a utilizar CSM sea rápido y sin esfuerzo. Simplemente haga clic en el mosaico de Gestión de secretos, elija la configuración con la que desea trabajar y estará listo para tener control sobre sus secretos.

Acerca de Akeyless

La combinación única de tecnología innovadora y arquitectura nativa de la nube de Akeyless permite a las empresas proteger rápidamente DevOps, cargas de trabajo en la nube y entornos heredados, al tiempo que cumplen con el cumplimiento y las regulaciones.

Acerca de Tales

Las personas en las que usted confía para proteger su privacidad confían en Thales para proteger sus datos. Cuando se trata de seguridad de datos, las organizaciones se enfrentan a un número cada vez mayor de momentos decisivos. Ya sea que se trate de crear una estrategia de cifrado, migrar a la nube o cumplir con los mandatos de cumplimiento, puede confiar en Thales para asegurar su transformación digital.

Tecnología decisiva para momentos decisivos.