

# Gerenciamento de segredos CipherTrust

## Protegendo segredos em grande escala

**CipherTrust Secrets Management (CSM) é uma solução de gerenciamento de segredos de última geração, desenvolvida pela plataforma Akeyless Vault, que protege e automatiza o acesso a segredos de missão crítica em ferramentas DevOps e cargas de trabalho em nuvem, incluindo segredos, credenciais, certificados, chaves API e tokens. Os novos recursos aprimoram os recursos da plataforma CipherTrust Data Security para ajudar as equipes de segurança e governança a reduzir riscos, simplificando os processos de segurança em suas operações.**

O gerenciamento de segredos pronto para empresas fornece processos automáticos para criação, armazenamento, rotação e remoção de segredos. Reduza o potencial de erro humano e aplique consistentemente políticas de segurança em toda a sua organização com:

- Gerenciamento centralizado para todos os tipos de segredo
- Funcionalidade automatizada e fácil de usar para DevSecOps
- Escalabilidade SaaS (Software as a Service) para ambientes híbridos e multinuvem

### Proteção abrangente de dados com gerenciamento de segredos em uma única ferramenta

The screenshot displays the THALES CipherTrust Manager interface. On the left, a navigation menu lists products such as 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
- Protect File & 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, which allows users to manage application secrets with Akeyless Vault.

## Cofre Seguro para todos os tipos de Segredo

O CSM, desenvolvido pelo Akeyless Vault, permite o gerenciamento abrangente de segredos de credenciais, certificados e chaves. Isso inclui segredos estáticos, segredos dinâmicos, chaves SSH, chaves de API e tokens.

Os principais casos de uso incluem:

- Loja de Segredos
- Rotação automatizada de credenciais
- Compartilhamento de segredos
- Geração e gerenciamento de segredos dinâmicos e just-in-time
- Registros de segredos usados para auditoria e conformidade

## Gerenciamento de chaves e gerenciamento de segredos em uma única ferramenta

Combinar o gerenciamento de segredos com o gerenciamento de chaves é como ter um cofre fortificado para todos os seus ativos valiosos em um só lugar. Crie eficiência contando com um único fornecedor para todas as suas necessidades de proteção de dados. Nenhuma outra organização oferece a amplitude e profundidade de proteção de dados que a **CipherTrust Data Protection Platform** oferece. Com uma única plataforma, você pode fazer uma transição perfeita para a plataforma Akeyless Vault por meio de um gateway seguro, sem fazer login separadamente.

## Reduza a complexidade operacional

62% das organizações hoje não sabem quantas chaves ou certificados possuem em toda a empresa<sup>1</sup>. Isso os deixa vulneráveis a acessos não autorizados e violações. À medida que os DevSecOps usam mais serviços e ferramentas para criar soluções, eles dependem de chaves e segredos para autenticar essas ferramentas e serviços entre si e na nuvem. Consequentemente, a expansão de segredos torna-se um risco cada vez maior. À medida que o número de segredos aumenta exponencialmente com o número de serviços e ferramentas utilizados na sua organização, a expansão de segredos cria riscos significativos, facilitando o acesso e o comprometimento dos seus segredos por parte de atacantes mal-intencionados.

## Melhore a eficiência do DevSecOps com separação total de tarefas

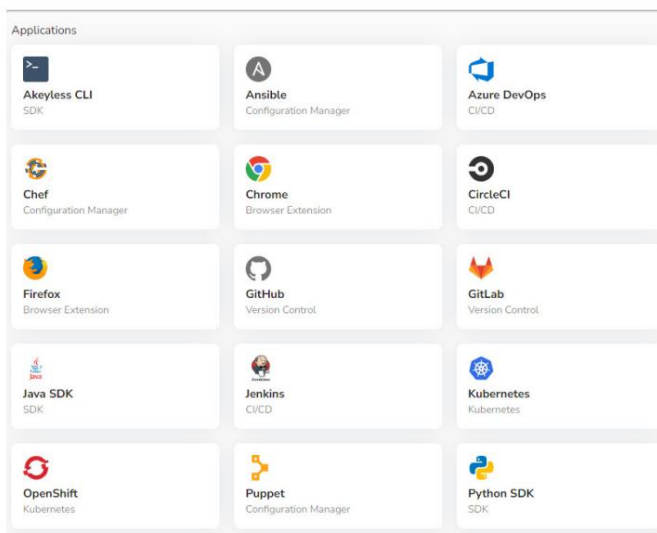
O DevSecOps pode integrar rapidamente o gerenciamento de chaves, operações de criptografia e gerenciamento de segredos em aplicativos multinuvem para proteger e acelerar processos de integração contínua e entrega contínua. Num ambiente DevSecOps, a separação total de funções envolve a distribuição de responsabilidades relacionadas com a gestão de chaves, operações de encriptação e gestão de segredos entre várias equipas ou indivíduos. A separação total de funções ajuda a prevenir violações de segurança, promove a responsabilização e melhora a eficiência geral dos processos de desenvolvimento, segurança e operações.

## Soluções híbridas e multinuvm

A mudança para a nuvem é uma transição, muitas vezes resultando em ambientes híbridos de múltiplas nuvens, com alguns recursos no local e outros distribuídos em diversas nuvens públicas e privadas. O CSM foi projetado para funcionar nesses ambientes e configurações.

## Integração perfeita

O CSM desenvolvido por Akeyless Vault integra-se facilmente com outros aplicativos de terceiros, como GitHub, Kubernetes, OpenShift e muito mais.



## Implante e dimensione rapidamente

O CipherTrust Secrets Management é facilmente acessível no painel do CipherTrust Manager. O CSM pode ser acessado no painel do CipherTrust Manager por meio de um bloco usando as mesmas credenciais usadas para acessar o CipherTrust Manager. Isso torna a introdução ao CSM rápida e fácil. Basta clicar no bloco Gerenciamento de Segredos, escolher a configuração com a qual deseja trabalhar e você estará pronto para ter controle sobre seus segredos!





## Sobre a Akeyless

A combinação exclusiva de tecnologia inovadora e arquitetura nativa da nuvem da Akeyless permite que as empresas protejam rapidamente DevOps, cargas de trabalho em nuvem e ambientes legados, ao mesmo tempo em que atendem à conformidade e aos regulamentos.

## Sobre Thales

As pessoas em quem você confia para proteger sua privacidade confiam na Thales para proteger seus dados. Quando se trata de segurança de dados, as organizações enfrentam cada vez mais momentos decisivos. Quer o momento seja construir uma estratégia de criptografia, migrar para a nuvem ou cumprir exigências de conformidade, você pode confiar na Thales para proteger sua transformação digital.

Tecnologia decisiva para momentos decisivos.

>cpl.thalesgroup.com<    

Contate-nos – Para todos os locais de escritórios e informações de contato, visite [cpl.thalesgroup.com/contact-us](https://cpl.thalesgroup.com/contact-us)