AKEYLESS | **THALES**
Building a future we can all trust

CipherTrust Secrets Management
Securing Secrets at Scale

CipherTrust Secrets Management (CSM) is a state-of-the-art Secrets Management solution, powered by the Akeyless Vault Platform, which protects and automates access to mission-critical secrets across DevOps tools and cloud workloads, including secrets, credentials, certificates, API keys, and tokens. The new features enhance the capabilities of the CipherTrust Data Security platform to help security and governance teams reduce risks by streamlining security processes across their operations.

Enterprise-ready secrets management provides automatic processes for creating, storing, rotating, and removing secrets. Reduce the potential for human error and consistently enforce security policies across your organization with:

- Centralized management for all secret types
- Easy to use, automated functionality for DevSecOps
- SaaS (Software as a Service) scalability for hybrid and multi-cloud environments

Comprehensive Data Protection with Secrets Management in One Tool
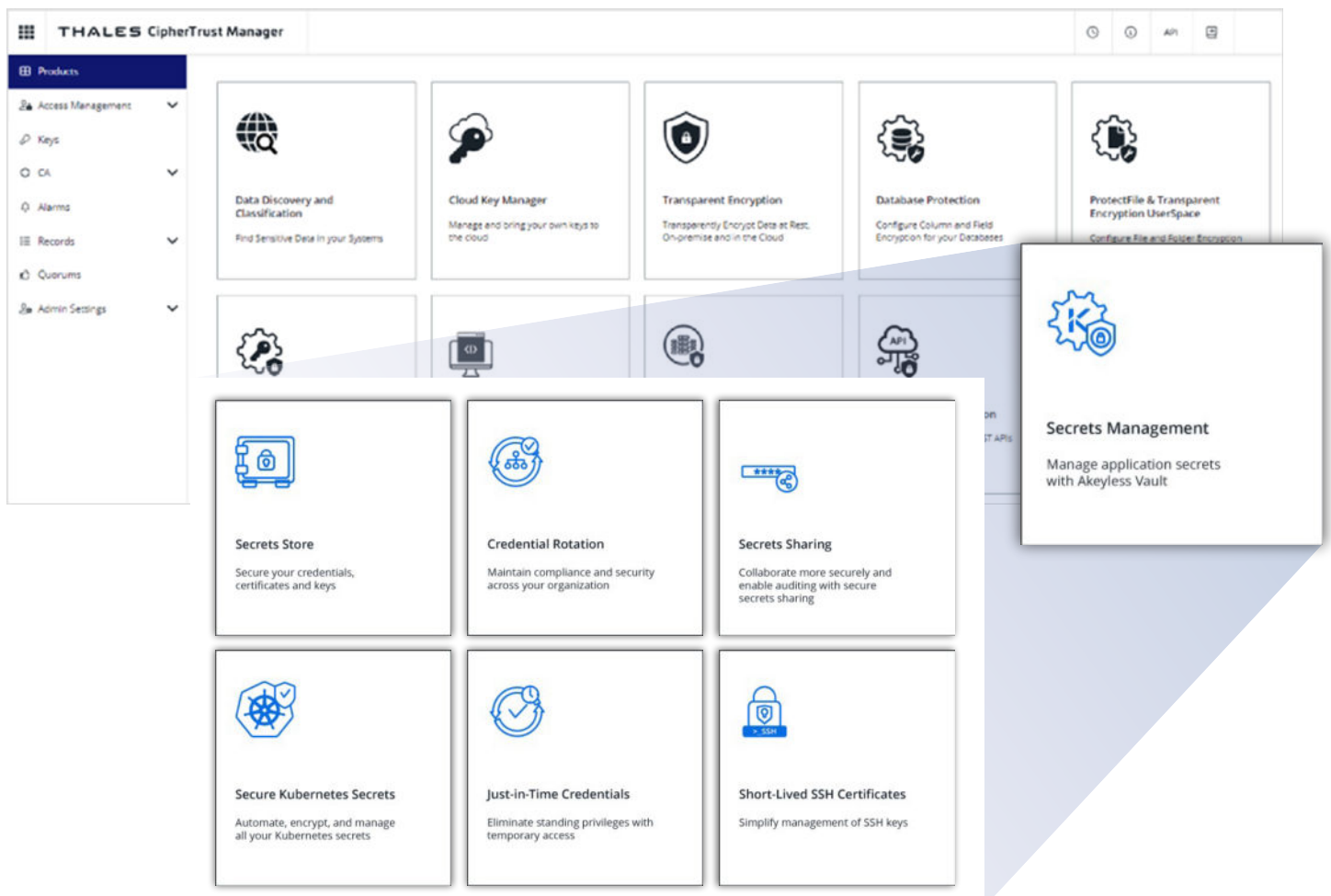
Secure Vault for All Secret Types

CSM, powered by Akeyless Vault, enables comprehensive secrets management of credentials, certificates and keys. This includes static secrets, dynamic secrets, SSH keys, API keys and tokens. Top use cases include:

- Secrets Store
- Automated Credential Rotation
- Secrets Sharing
- Dynamic, Just-in-Time secret generation and management
- Logs of secrets used for auditing and compliance

Key Management and Secrets Management from One Tool

Combining secrets management with key management is like having a fortified vault for all your valuable assets in one place. Create efficiencies by relying on one vendor for all your data protection needs. No other organization offers the breadth and depth of data protection that the CipherTrust Data Protection Platform provides. With a single platform, you can seamlessly transition to the Akeyless Vault platform via a secure gateway without signing in separately.

Reduce Operational Complexity

62% of organizations today do not know how many keys or certificates they have throughout their company[1]. This leaves them vulnerable to unauthorized access and breaches. As DevSecOps use more services and tools to build solutions, they rely on keys and secrets to authenticate these tools and services to each other and to the cloud. Consequently, secrets sprawl becomes an ever-increasing risk. As the number of secrets increase exponentially with the number of services and tools used in your organization, secret sprawl creates significant risks by making it easier for malicious attackers to access and compromise your secrets.

## Improve DevSecOps Efficiency with Full Separation of Duties

DevSecOps can rapidly integrate key management, encryption operations, and secrets management in multi-cloud applications to secure, and speed-up continuous integration and continuous delivery processes. In a DevSecOps environment, full separation of duties involves distributing responsibilities related to key management, encryption operations, and secrets management among various teams or individuals. Full separation of duties helps prevent security breaches, promotes accountability, and improves the overall efficiency of the development, security, and operations processes.

Hybrid, Multi-cloud Solutions

Moving to the cloud is a transition, often resulting in hybrid multi-cloud environments, with some resources on-prem, and others distributed across multiple public and private clouds. CSM is designed to work across these environments and configurations.

Seamless Integration

CSM powered by Akeyless Vault easily integrates with other third party applications such as GitHub, Kubernetes, OpenShift, and more.
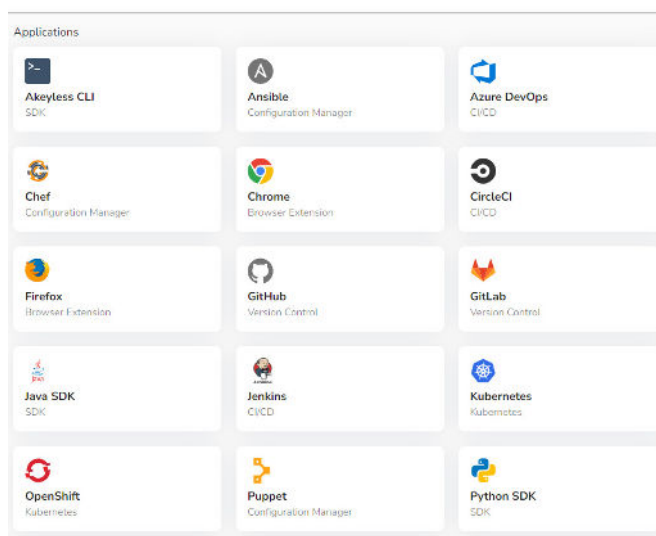
Quickly Deploy and Scale

CipherTrust Secrets Management is easily accessible from the CipherTrust Manager dashboard. CSM is accessible from the CipherTrust Manager dashboard via a tile using the same credentials used to access CipherTrust Manager. This makes getting started with CSM quick and effortless. Just click on the Secrets Management tile, pick the configuration you wish to work with, and you are all set to have control over your secrets!

About Akeyless

Akeyless' unique combination of innovative technology and cloud-native architecture enables enterprises to quickly secure DevOps, cloud workloads, and legacy environments, while meeting compliance and regulations.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.