Brochure

CipherTrust Secrets Management vs. Cloud Service Providers

Keep secrets secure across all environments

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

AKEYLESS

Why CipherTrust Secrets Management powered by Akeyless?

- Connects to all environments: Hybrid & Multi-cloud
- Supports all secret types: Static, Rotated, Dynamic
- Connectivity to third-party tools and environments
- Unified Secrets Management across teams & technologies
- Exclusive ownership and access to secrets

The Limitations of CSP solutions

Cloud Service Providers (CSPs) such as Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP) are an important part of organizations' move to the cloud. But are they secure?

While CSP platforms provide baseline Secrets Management tools, these tools fall short in several important ways.

Support for Hybrid and Multi-Cloud

Today organizations' resources and workloads frequently span both on-prem and cloud environments, and usually include more than one cloud platform. But a Secrets Management solution that is particular to one CSP is not intended to support on-prem processes or other cloud platforms. CSP solutions do not have a federation service for authentication, so a Secrets Management solution proprietary to one cloud platform cannot support services and resources found in a different cloud platform. In addition, on-prem workloads cannot take advantage of the CSP secrets vault without an access key. This results in the dilemma of where and how this key can be secured.

Access to Keys and Data

An additional concern, particularly for organizations who handle sensitive data for customers or employees, is vendor access to company data. When using a CSP's secrets solution, an organization is in effect giving the CSP access to both the company's keys and data, since the CSP has complete access to the encryption key used for these secrets. This makes the organization vulnerable, particularly as the CLOUD act compels CSPs to turn over both keys and data to the government if requested.

Thus, most organizations who choose a CSP secrets solution sacrifice coverage for secrets and processes found on-prem or in other cloud platforms. Such a situation is potentially dangerous, and does little to solve the growing problem of "secret sprawl" as secrets can still be found throughout the company's databases, code repositories, and CI/CD tools.

Secrets functionality: Rotated & Dynamic Secrets

An important part of Secrets Management is the need to regularly rotate secrets. Without the ability to rotate secrets periodically, any leaked secret can be activated at any time, endangering organizational data and processes. In fact, as organizations seek to improve their security posture, many have begun to use Just-In-Time (JIT), dynamic secrets, which expire automatically and further limit the window opportunity for a malicious attack.

In general, CSP secrets solutions only handle static secrets, and lack the ability for regular rotation and to create dynamic and Just-In-Time secrets for ephemeral resources. Rotating secrets and creating dynamic secrets requires ongoing connectivity with services and resources outside of the cloud platform, or with third party services within the platform, which can present a problem for CSPs.

This lack of functionality can leave the organization vulnerable to hacks and leaks in the long term, as static secrets are not changed or revoked.

The "Walled Garden" of Cloud Service Providers

Cloud Service Providers use a "walled garden" approach to secrets which is not appropriate for today's rapidly growing and distributed IT environment . CSP's secrets solutions are intended to make secrets available for processes that run within that cloud platform.

However, these solutions have poor connectivity to third-party platforms, such as self-deployed CI/CD tools, non-managed Kubernetes clusters and similar workload elements. This can create tremendous problems for DevOps teams who need to quickly develop applications that use multiple secrets on a minute-to-minute basis, with the ability to quickly inject secrets as needed.

CipherTrust Secrets Manager provides the Secrets Management that modern organizations need:

- Hybrid & Multi-Cloud
- All Secret Types
- Connectivity with DevOps Tools & Processes
- Full control of secrets & data

The CipherTrust Secrets Management Solution

CipherTrust Secrets Manager (CSM) is built to support hybrid multi-cloud and DevOps environments. It provides a centralized service that handles secrets for multiple cloud platforms and on-prem environments. CSM authenticates to cloud platforms using the CSP's default connectivity, and securely authenticates on-prem services and resources through its Universal Identity feature.

CSM enables your security, cloud and DevOps teams to easily manage static, rotated and dynamic (Just-In-Time) secrets through a CLI or easy web interface. Teams can easily configure a wide range of rotated secrets and dynamic secrets for any protocol, cloud platform, database or service.

CSM also fits easily into existing DevOps tools and processes, with multiple integrations and plugins that allow developers to automatically inject or create secrets as needed without slowing down development.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.