



The Secrets to Secrets Management:
The Ultimate Guide to Managing Secrets in 2024

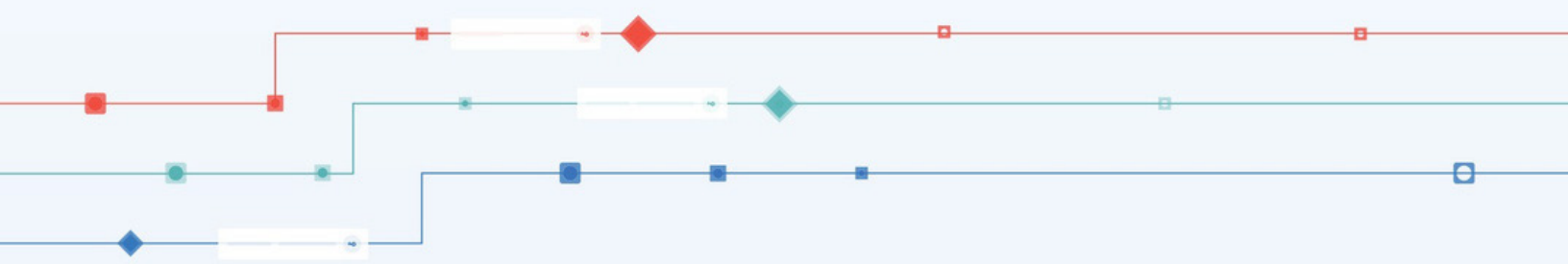
Choosing the Best Secrets Management Tool for Your Enterprise

Insider knowledge to evaluate the best
secrets manager for your environment



Table of Contents

Introduction	3
How Secrets Managers Work and Storing Secrets Online	3
How a Repository Works in Secrets Management	4
Advantages of Akeyless: Akeyless vs. HashiCorp Vault vs. Azure Key Vault vs. Google Secret Manager vs. AWS Secrets Manager	6
Recap	8

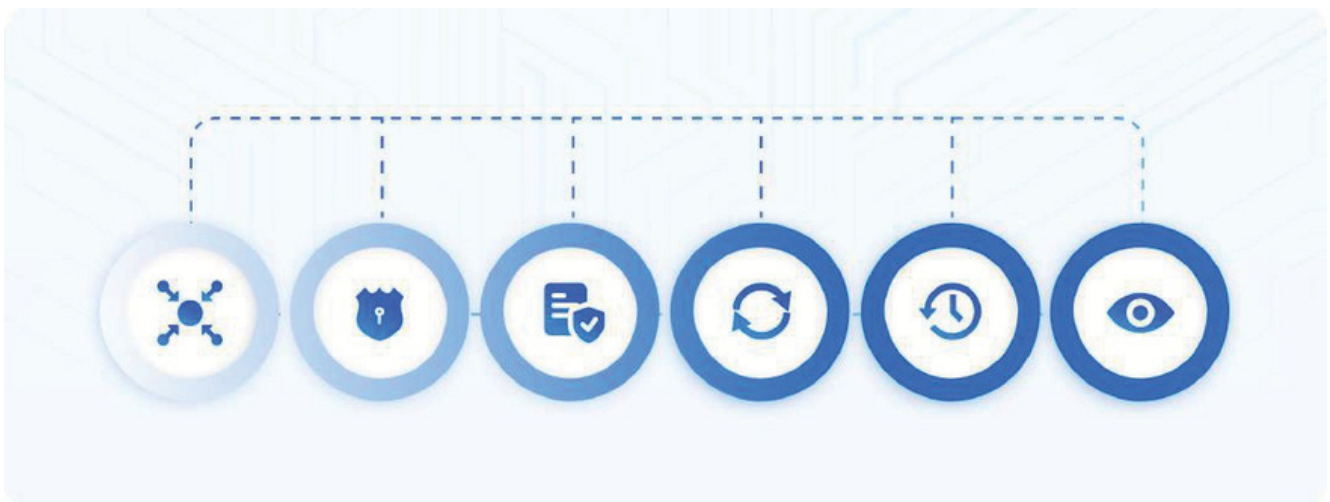


Introduction

Welcome to “Choosing the Best Secrets Management Tool for Your Enterprise,” a comprehensive exploration into the world of secrets management tools.

We'll delve into the fundamental workings of secrets managers, their advantages, and how they facilitate online secrets storage. We'll also discuss the architecture of a secrets management platform and how it protects valuable data. The latter part of this guide includes an in-depth comparison of popular secrets management platforms: Akeyless, HashiCorp Vault, Azure Key Vault, Google Secret Manager, and AWS Secrets Manager.

By navigating this landscape, this guide is designed to help you identify the optimal platform that meets your organizational needs while maximizing data security and operational efficiency.



How Secrets Managers Work and Storing Secrets Online

Risks of Not Properly Managing Secrets

Secrets managers are an essential tool in maintaining secure and efficient handling of sensitive data or "secrets". Here's a high-level overview of how they function:



Centralizing Secrets

Secrets managers usually consolidate all secrets within an organization into one secure location. This enhances the uniformity of security measures across all secrets and simplifies their management.



Securing Secrets

Security is the core function of secrets managers. They encrypt secrets to protect them from unauthorized access, ensuring that only those with necessary decryption keys can access the information.



Enforcing Access Policies

Strict access policies are enforced by secrets managers. They use mechanisms like Multi-Factor Authentication (MFA) as well as role-based access controls (RBAC) to ensure that only authorized individuals can access the secrets.



Automating Secrets Rotation

To enhance security, secrets managers support automated secrets rotation, generating and updating new secrets at regular intervals. This automation maintains high security without adding significant administrative burdens.



Temporary, Just-in-Time Dynamic Secrets

Some secrets managers can create auto-expiring temporary secrets, which eliminate the danger of standing privileges and ensure that access is unavailable as soon as it is not needed.



Temporary, Just-in-Time Dynamic Secrets

Secrets managers provide robust tracking and visibility capabilities, allowing organizations to maintain governance and meet auditing requirements. They enable organizations to track, monitor and log activities related to secret creation, access, and modification, providing an audit trail for compliance purposes. This visibility ensures transparency and accountability, helping organizations demonstrate adherence to security policies and regulatory standards.

Different Types of Secrets Managers

There are several types of secrets managers, including open-source, self-deployed, or cloud-based secrets managers.



Open-Source Secrets Managers

Open-source secrets managers are built on freely accessible source code. They are typically flexible and customizable, allowing you to tailor them to your specific needs. Although open-source tools are popular in the development community, they can often require more resources in terms of setup and management compared to other options. Often, this can be a headache to deploy and maintain for large organizations, and are frequently difficult to scale to more than one team or environment.



Self-Deployed Enterprise Secrets Managers

Self-deployed secrets managers are deployed within an organization's own infrastructure. This can provide more control over the data and system compared to cloud-based options and might be required for organizations with stringent data sovereignty or regulatory requirements. The drawback is that these systems require significantly more management overhead and hardware resources, and may not scale as easily or cost-effectively as cloud-based alternatives.



Cloud-Based Secrets Managers

While convenient and scalable, the use of cloud-based secrets managers like AWS Secrets Manager, Azure Key Vault, and Google Secret Manager can raise security concerns because these providers have full ownership of the keys used for encrypting and decrypting data, limiting the organization's control of their own data. Organizations can explore technologies like [Akeyless Distributed Fragmentation Cryptography \(DFC\)™](#) to regain control over encryption keys and enhance data privacy and security.

Old vs. New: Vaults and Vaultless Secrets Management

Traditional secrets management relied heavily on the use of centralized vaults for storing sensitive credentials, certificates, and keys. This approach was a cornerstone of secrets policy in an era of simpler, more centralized IT landscapes. But as the digital environment expanded, giving rise to multi-cloud, multi-region, and automation-centric setups, conventional vault methodology faced significant challenges. In this expanded digital environment, each site required the deployment, configuration, and upkeep of multiple, resilient vaults, a process that proved expensive, burdensome, and labor-intensive.

Responding to this shifting landscape, secrets management is transitioning towards a vaultless paradigm. This innovative approach is not just a simple SaaS adaptation of existing vault systems. It represents a reimagining of secrets management architecture, purpose-built to meet the demands of the evolving digital environment.

Vaultless secrets management removes the complexities associated with managing numerous vaults across diverse locations. It reduces the operational overheads of deployment, maintenance, and scaling, offering a solution more in tune with the dynamic nature of modern, distributed IT environments.

While vault-based secrets management continues to serve certain scenarios well, the emerging vaultless approach aligns more seamlessly with the increasingly complex, distributed IT environments. This transition to vaultless secrets management embodies an important evolution in aligning secrets management with the demands of the future.

Comparison of Secrets Management Solutions

Choosing the right secrets management tool for your organization depends on a range of factors, including the nature of your environment, your regulatory obligations, and your specific requirements. Let's compare four popular options:



HashiCorp Vault

HashiCorp Vault Enterprise is a self-deployed secrets management platform that is known for access control for sensitive data. It includes security features such as end-to-end encryption and dynamic secrets, providing an enterprise-level solution. However, the HashiCorp self-deployed solution has considerable implementation and maintenance costs, and along with a complex architecture that can make scaling difficult for larger organizations, may require dedicated 24/7 support to ensure smooth operation and maximize its effectiveness.



Azure Key Vault

Azure Key Vault, a product of Microsoft, is designed to safeguard cryptographic keys and other secrets used by cloud apps and services. It integrates seamlessly with other Azure services, making it a good choice if you're already using Azure extensively. Using Azure Key Vault ties you into the Azure ecosystem, which is less suitable if your applications are not primarily Azure-based or if you are using other cloud service providers as well.



Google Secret Manager

Google Secret Manager is a secure and convenient method for storing API keys, passwords, certificates, and other sensitive data. As a cloud solution, it integrates with Google Cloud services, making it easy to use if you're a heavy user of Google's cloud offerings. It can be less flexible, however, if you have a diverse, multi-cloud, or non-cloud environment. Similar to Azure Key Vault, it can be limiting if your applications are not primarily Google-based or if you have secrets in other cloud service providers besides GCP.



AWS Secrets Manager

AWS Secrets Manager is a fully managed secrets management service provided by Amazon Web Services (AWS). It simplifies the management and protection of secrets such as database credentials, API keys, and secure strings. AWS Secrets Manager seamlessly integrates with other AWS services and offers extensive features such as automatic secrets rotation and integration with AWS Identity and Access Management (IAM). [AWS Secrets Manager](#), while a powerful and fully managed secrets management service, may present drawbacks such as vendor lock-in, limited integration options, and potential cost implications. Like other cloud service provider secrets managers, AWS Secrets Manager does not support secrets located in other cloud service providers.



Akeyless

Akeyless stands out as a universal, scalable, and secure secrets management solution delivered through a Software-as-a-Service (SaaS) platform. SaaS-based secrets management saves organizations significant costs in computing resources and engineering time. At the same time, powered by Distributed Fragments Cryptography™ (DFC™), a NIST FIPS 140-2 validated cryptography technology, Akeyless ensures the security of secrets by utilizing a unique approach called Zero-Knowledge Encryption. This enables organizations to protect their sensitive data while leveraging the flexibility and convenience of a SaaS environment. With DFC™ and Zero-Knowledge Encryption, Akeyless provides a highly secure secrets management solution, empowering organizations to safeguard their data within a user-friendly SaaS platform.

While HashiCorp Vault, Azure Key Vault, Google Secret Manager, and AWS Secrets Manager each have their advantages, they also come with significant limitations. Akeyless fills these gaps, providing a robust, flexible solution for managing your organization's secrets. By choosing Akeyless, organizations can take control of their secrets management strategy, enhance security, and ensure the utmost protection for their digital assets. With its comprehensive features, strong security measures, and innovative use of DFC™ and Zero-Knowledge Encryption, Akeyless emerges as the ideal choice for organizations seeking a reliable, efficient, and highly secure secrets management solution.

See a detailed comparison of [Akeyless vs HashiCorp Vault](#).

Recap of Key Points

We've explored quite a breadth of content in "Choosing the Best Secrets Management Tool for Your Enterprise."

Here are our main takeaways:

- ✓ **Secrets Managers Functions:** We dove into how secrets managers work by centralizing and securing secrets, enforcing access policies, automating secrets rotation, and providing robust tracking and visibility.
- ✓ **Types of Secrets Managers:** We differentiated between the main types of secrets managers, namely open-source, self-deployed, and cloud-based secrets managers, each with its pros and cons.
- ✓ **A Repository's Role in Secrets Management:** We examined the role and function of a repository in secrets management and discussed why organizations use them for centralized, secure storage, access control, and usage tracking.
- ✓ **Comparison of Secrets Managers:** We provided a comprehensive comparison of five secrets management platforms, Akeyless, HashiCorp Vault, Azure Key Vault, Google Secret Manager, and AWS Secrets Manager. Each of these platforms has its strengths and weaknesses.
- ✓ **Akeyless:** We highlighted Akeyless as a vaultless solution that is scalable, secure, and a universal solution for secrets management, offering unique features like Distributed Fragments Cryptography™ (DFC™) and Zero-Knowledge Encryption.

This guide has aimed to enhance your understanding of secrets management platforms, highlighting the importance of choosing a platform that aligns with your organizational needs and data security requirements. By implementing a robust secrets management strategy, organizations can safeguard their digital assets effectively and improve operational efficiency.

Thanks for joining us!

Congratulations on completing the The Secrets to Secrets Management Kit. We hope you have been able to build a holistic perspective of secrets management—from the basics, best practices, and industry insights.

Review the first two ebooks in the series:

Mastering Secrets Management: 7 Essential Strategies for Best Practices

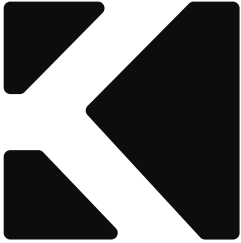


[Read about Best Secrets →](#)

Secrets Management 101



[Read about Secrets →](#)



Ready to take your secrets management to the next level?

Explore the Akeyless platform today.

[Schedule a demo →](#)