AKEYLESS

Akeyless Vault Platform

Secrets Management

Secrets Management is a solution for centrally creating, managing, and securing the lifecycle of secrets, including the credentials, certificates, and keys used to authenticate users and/or machines to access applications or services across the organization's hybrid multicloud IT/DevOps environment.

The Risk of Secrets Sprawl

The surge of secrets usage due to containerization, orchestration, and DevOps, has put many organizations at risk, as many do not have consistent policies in place to regulate how secrets are used and where they can safely store their SSH or API keys. Without a centralized secrets management solution, security teams do not know how many secrets are used, and who uses them. Therefore, there is no option to audit all secrets usage, revoke access, or avoid secret duplication.

Static secrets, with long-standing privileges, are unfortunately still the norm. What's worse, is that these secrets are often hardcoded in source code or configuration files. Such behavior results in an inability to audit and control access to their values and has been the source of several recent data breaches. By compromising static secrets, a bad actor can gain carte blanche access to systems and data, and a great ability to move laterally across the broader IT environment and complete the killchain.

DevOps Platforms

CI/CD, Configuration Management, and Orchestration platforms contain SSH keys, Certificates and more

Applications Code

Source code and code repositories contain API Keys, DB Credentials and many other secrets

Developers Team

Passwords, API Keys and SSH Keys are stored locally on laptops or shared files

Akeyless Secrets Management SaaS

The Akeyless Vault Platform provides a SaaS-based Secrets Management solution that enables security teams with centralized oversight and control of all secrets, for all humans and machines, across hybrid multicloud environments. It empowers DevOps and Cloud Transformation initiatives while enforcing continuous security compliance.

Akeyless' patented, FIPS 140-2 certified DFC™ technology enables a Zero-Knowlege platform, where customers have exclusive ownership of their secrets, without the overhead and cost of hardware HSMs.

Secrets Management is delivered from the cloud and consumed as a service, so it is fast to deploy and eliminates the operational overhead associated with on-premise vault clusters. Traditional and virtualized vault instances require continuous hardware and/or software maintenance, and are complex to scale. Our SaaS solution eliminates maintenance outages, and auto-scales for demand peaks, with built-in multi-regional high availability, and disaster recovery.

Key Considerations for Secrets Management Products

Scope

Cloud Provider Vaults primarily focus on workloads within their own cloud platform.

DON'T EXCHANGE SECRETS SPRAWL FOR A SOLUTION SPRAWL.

Trust

Cloud Provider Vaults, and virtualized Vaults, require access to your master keys. Custodial key ownership increases risk as keys and data can be compromised through mandates such as the CLOUD act, rogue administrators, or platform vulnerabilities.

IF YOU DON'T OWN YOUR KEYS, YOU DON'T OWN YOUR SECRETS.

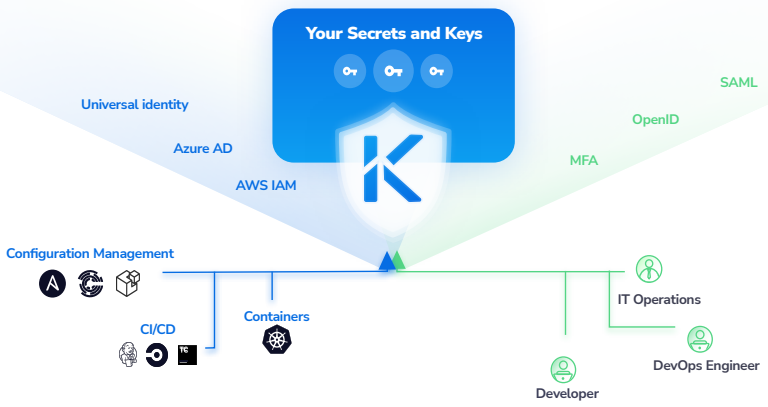
Overhead

On-premise Vault clusters create operational overhead as they require hardware infrastructure and continuous software maintenance.

SCALING ON-PREMISE VAULT INSTANCES IS COMPLEX AND MAY RESULT IN SECURITY BLIND SPOTS.

Centralized Secrets for Hybrid Multicloud Organizations

The Akeyless Secrets Management solution keeps secrets accessible for both human and machine identities, regardless of whether they are located on-premise, in AWS, Azure, or GCP.
With centralized secret storage and management, security teams have complete insight into the scale and usage of secrets, across the entire organization. Meanwhile, the multi-tenancy feature allow different teams and business units to manage their own secret realms autonomously.



Seamless Integration into Workflows

Akeyless Secrets Management easily deploys in any environment and seamlessly integrates with the tools your different teams use. A complete list is available at akeyless.io/integrations

- **Complete Authentication**
  Simplify authentication using external Identity Providers like Okta, AWS IAM, Azure AD, and more
- **Universal Identity™**
  Eliminate the Secret Zero problem for legacy on-premise workloads by providing a machine identity to secure the initial vault connection
- **Integrate your DevOps**
  Use various plugins to push secrets into your CI/CD pipelines, Configuration Management, and Container Orchestration tools
- **Integrate into Code**
  Eliminate secret exposure in code by using various SDKs
- **Password Management for Teams**
  Enable humans with multi-tenant secrets management via a browser extension, providing quick access to private and teams shared secrets
- **Simple Secrets Migration**
  Easily import secrets from other secrets management platforms such as Kubernetes Secrets, AWS Secrets Manager, Azure Key Vault, or HashiCorp Vault
- **Keep Existing Plugins**
  Continue using your community-created plugins: Akeyless provides API compatibility with HashiCorp Vault OSS

Enterprise-Grade Security and Privacy

By implementing a centralized Secrets Management solution, organizations can control the lifecycle of all the secrets they have, and which roles may use them. **Your secrets are safe with the Akeyless Vault Platform.**

Our patented, FIPS 140-2 certified, Akeyless DFC™ technology ensures you maintain full custody of your keys. This next-generation Zero Knowledge technology stores key fragments across different cloud platforms, as well as your on-premise environment. Keys never exist as a whole, so not even Akeyless can access and decrypt your keys.

Protect static secrets

Manually create and update secrets, for example connection strings, passwords, API tokens, SSH key, or even personal identifiers such as credit card numbers and social security numbers are managed in our encrypted secrets store.

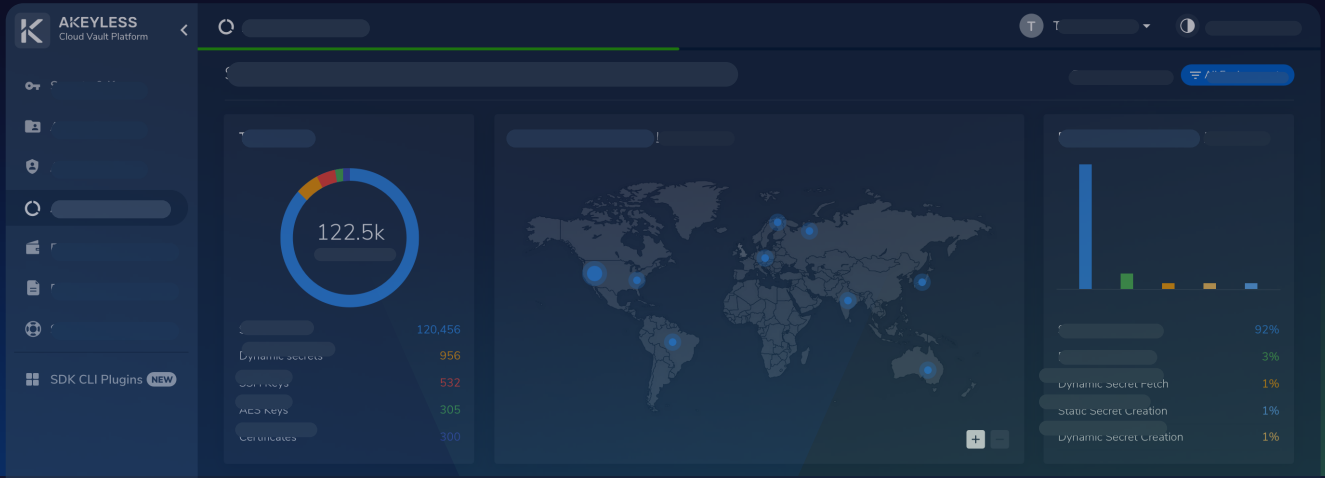
Generate dynamic secrets on-demand

Secrets are created on-the-fly; a temporary user is created on a target for a specified period of time in order to support just-in-time access. Akeyless Secrets Management supports many different types of targets including:

AWS | Azure AD | Chef Infra | Databases (including MySQL, MSSQL, PostgreSQL, Mongo DB, Oracle DB, Cassandra, Redshift, Snowflake) | EKS | GCP | GKE | JFrog Artifactory server | Kubernetes | LDAP | RabbitMQ | RDP | Snowflake | Custom

Automatically rotate secrets

Protect privileged system accounts such as an Administrator account on a Windows server, a root account for a Linux server, or an Admin account for a network device, by automatically resetting its password periodically.



Ensure Auditing & Compliance

Granular Machine Identities
Segregate access between identities at various levels (i.e. pods, namespaces, playbooks, jobs, and more).

Encrypted Key/Value Store
Protect any type of secret, such as connection strings, passwords, tokens, and encryption keys with Zero-Knowledge Encryption

Least Privileges
Limit machines and users' access rights, to the minimum they need

Log Usage & Admin Tasks
Collect detailed audit logs of any operation that was made by either users or machines, together with time-stamped trace

Analytics & Insights
Analyze the status of secrets posture in various environments from a birds eye view

Integrate with SIEM
Empower the analysis of your logs by shipping them to a central SIEM or your log management system

Data Protection

Akeyless empowers organizations with the ability to fulfil data protection use cases by providing centralized access to encryption keys for databases and storage devices

Full Key Life Cycle Management

Centrally manage the lifecycle of encryption key including generate, rotate / versioning and delete based on Akeyless DFC™

Multi Cloud KMS

Provision and enhance your control of encryption keys across cloud providers KMS

Encryption-as-a-Service

Encrypt and decrypt application data with a simple API call, without prior knowledge of cryptography operations

Storage-Level Encryption with KMIP

Unify encryption processes by connecting databases and storage devices, including MongoDB, VMware ESX and more

Tokenization (coming soon)

Accelerate privacy and compliance by encrypting select sensitive data (PII, HIPAA, PCI, GDPR)

Akeyless Gateway

The Akeyless Gateway adds an extra level of protection between your private network and the cloud, as an extension of the Vault Platform. It deploys easily, as a lightweight container, without requiring complex "network trust" mechanisms. The Akeyless Gateway provides additional benefits and features such as:

- **Performance acceleration through in-memory caching**
- **Zero Knowledge assurance with customer fragment hosting as part of the Akeyless DFC™ Innovative KMS technology**
- **Service continuity during network connectivity issues via secrets snapshots**
- **Secure communications for your internal resources by generating dynamic secrets**
- **Automatically migrate from existing secrets repositories**
- **Expand events oversight through Log Forwarding for your internal SIEM**