AKEYLESS

Akeyless Identity Security Platform for the AI Era

Built for machines, AI agents, and the people who depend on them.

A New Model for Identity Security

Enterprises are connecting more systems, workloads, and AI agents than ever. Each new connection introduces another identity to manage across hybrid, multi-cloud, and on-prem environments. Legacy tools designed for human access can't scale to this level of automation.

The Akeyless Identity Security Platform secures every identity, from machines, to AI agents, to humans, through one cloud-native solution. It replaces static secrets with just-in-time access, automates authentication, and enforces least privilege everywhere. Powered by Distributed Fragments Cryptography™ (DFC), it keeps every secret and key protected with zero-knowledge assurance.

Key Benefits

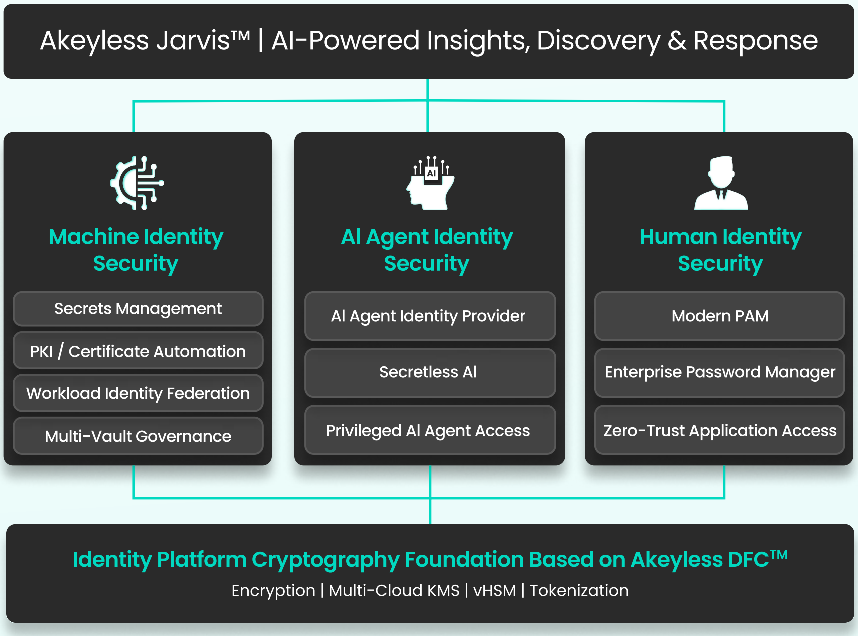
- Remove hardcoded credentials and standing privileges
- Authenticate workloads and AI agents without shared secrets
- Automate secret, key, and certificate lifecycle management
- Enforce least privilege with full audit visibility
- Simplify compliance with unified policy and reporting
- Reduce cost and complexity by consolidating tools

Architecture Overview

Akeyless delivers unified identity security across every environment.

The Akeyless platform unifies secrets management, access, encryption, and governance across every environment. It connects directly with cloud, SaaS, and on-prem systems to enforce access policies and prevent credential exposure.

Distributed Fragments Cryptography™ (DFC) provides the foundation of trust, separating cryptographic control from infrastructure so keys remain private and mathematically protected.



Akeyless Jarvis™ | AI-Powered Insights, Discovery & Response

Machine Identity Security
- Secrets Management
- PKI / Certificate Automation
- Workload Identity Federation
- Multi-Vault Governance

AI Agent Identity Security
- AI Agent Identity Provider
- Secretless AI
- Privileged AI Agent Access

Human Identity Security
- Modern PAM
- Enterprise Password Manager
- Zero-Trust Application Access

Identity Platform Cryptography Foundation Based on Akeyless DFC™

Encryption | Multi-Cloud KMS | vHSM | Tokenization

AKEYLESS

Platform Capabilities

Secrets Management

Centralized, policy-driven control for application, container, and pipeline secrets. Automate rotation and dynamic credential delivery through Kubernetes, OIDC, and SPIFFE integrations, with complete auditing and granular access policies.

AI Agent Identity Security

Authenticate AI agents and workloads without static credentials using SecretlessAI™. Issue short-lived identities via MCP and enforce least privilege across hybrid, multi-cloud, and on-prem environments.

Workload Federation

Federate workload identities across AWS, Azure, GCP, and on-prem systems without shared secrets. Use native IAM trust policies for temporary, cross-cloud access with complete audit consistency.

Modern PAM

Deliver just-in-time privileged access to servers, databases, and containers without endpoint agents or standing credentials. Enforce policy-based sessions with full recording and visibility.

Certificate Lifecycle Management & PKI

Automate certificate issuance, renewal, and revocation with real-time visibility and ACME or API integration. Protect all certificates using DFC for zero-knowledge encryption and continuous uptime.

Encryption & Multi-Cloud KMS

Centralize encryption and key management across hybrid and multi-cloud infrastructures. Support TDE, signing, tokenization, and FPE, secured by DFC for full key ownership and post-quantum resilience.

Multi-Vault Governance

Unify secrets visibility and policy enforcement across AWS, Azure, GCP, HashiCorp Vault, and more. Automate rotation and compliance reporting without migration.

Password Manager

Securely store, share, and rotate human credentials with zero-knowledge protection and role-based access. Integrate with PAM and Secrets Management for unified governance.

Akeyless Jarvis™ (AI-Powered Insights)

Use AI-driven discovery, detection, and response to identify unmanaged or risky identities and compliance gaps across human, machine, and AI entities. Integrate with SIEM and SOAR systems for natural-language insights and actionable intelligence.

Zero-Knowledge Cryptographic Protection

Using patented Distributed Fragments Cryptography™, each key is fragmented across regions and providers, with one fragment always retained by the customer. Built-in support for hybrid TLS 1.3 with ML-KEM768 ensures post-quantum protection

Built for the Most Demanding Environments

Akeyless meets the highest standards for enterprise security and compliance.

- FIPS 140-2 validated encryption
- SOC 2 Type II and ISO 27001 certified
- GDPR and PCI DSS aligned
- Global SaaS availability and resilience

Every deployment follows a zero-knowledge design, ensuring your secrets, keys, and credentials remain fully under your control.

Take control of your identities and secrets.

Request a demo to see how at **akeyless.io/demo**

Akeyless.io