Fortanix®

Solution Brief

Secret Management

Secret management solution that DevOps and security teams love!

Problem

SECRET SPRAWL

Cloud native development and multicloud infrastructures has led to proliferation and decentralization of secrets. If left to their own devices, these secrets can sprawl over time, leading to data breaches and privacy concerns.

A DISPARATE SET OF TOOLS

DevOps teams uses multiple tools for different phases of the development process. Centralized system that can integrate with all these tools and systems is a rarity. Cloud-native secrets management tools are limited to the specific cloud provider and fail under a multi-cloud scenario.

DEVOPS BLIND SPOTS

Most enterprises are unaware of where their secrets are located, access level or whether the secrets have been changed. This lack of understanding of the functioning of the DevOps pipeline often increases the risk of an internal data breach.

Solution Overview

Fortanix provides a single centralized platform to securely store, control and manage secrets outside the source code in a FIPS 140-2 level 3 certified HSM. With flexible deployment modes and scalable architecture, Fortanix secret management works across environments, on-premises, natively in the cloud, hybrid and multicloud. Integrates with any DevOps environment with Rest APIs.

info@fortanix.com | +1 (650) 943-2484 | 800 West El Camino Real, Suite 180, Mountain View, CA 94040

Solution Benefits

SINGLE-PANE VIEW TO MANAGE AND ACCESS THE SECRETS

With Fortanix, your teams get a single source to access all secrets like encryption keys, tokens and passwords and your security teams get a Single-Pane view to manage and audit the access.

HSM GRADE SECURITY AND COMPREHENSIVE AUDIT LOGS

Secured with Intel® SGX and built using Fortanix patented Runtime Encryption® Technology, Fortanix runs every operation in HSM-grade security, ensuring complete control over your keys, data and secrets. Comprehensive audit logs provide insight into how secrets are being used, helping you meet compliance.

API BASED SECRET MANAGEMENT WITH EXTENSIVE INTEGRATIONS

Fortanix can manage secrets natively in the cloud and on-premises, providing extensive RESTful APIs through open standards such as OAuth, OpenID (SAML), LDAP, JWT, and PKI. Integrates with any DevOps environment with Rest APIs. Supports upcoming technologies like Kubernetes, Docker etc.

A FLEXIBLE DEPLOYEMENT MODEL

On-premises, natively in the cloud or any hybrid/multi-cloud combination. Deploy anywhere, run everywhere.

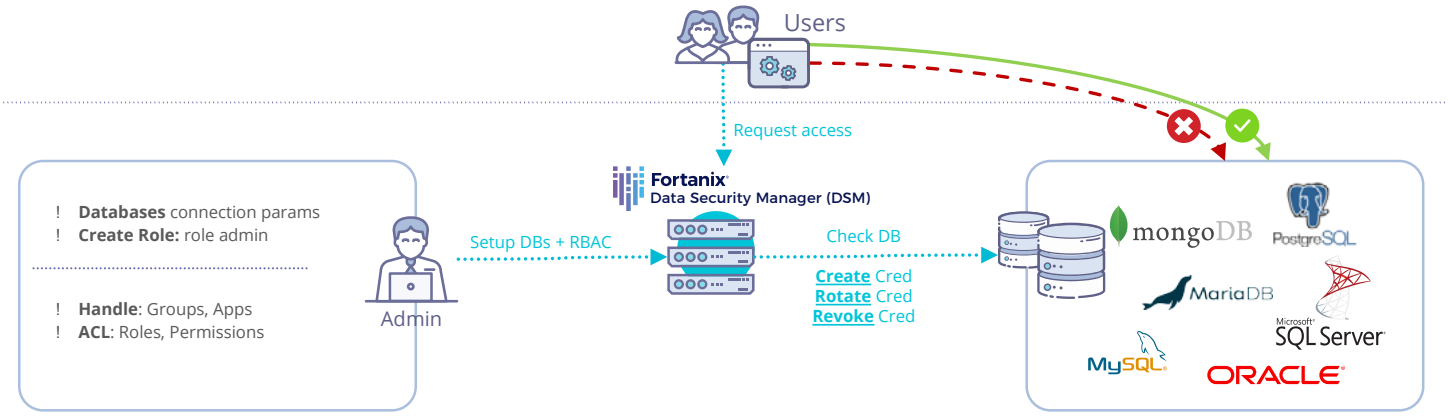
> Secrets — typically sensitive credentials or encryption keys — have proved increasingly dangerous in DevSecOps environments, although the challenge is hardly new. Developers have always routinely hard-coded passwords and other types of credentials in scripts and programs. More-enlightened organizations might move the credential to a configuration file or a metadata service — helping somewhat, but still typically leaving the credential in plaintext in a location readily accessible to malicious users.

Gartner

info@fortanix.com | +1 (650) 943-2484 | 800 West El Camino Real, Suite 180, Mountain View, CA 94040

Solution Highlights

- **STORE SECRETS OUTSIDE THE SOURCE CODE:** Sensitive data and credentials can be stored outside the source code in FIPS 140-2 level 3 certified HSM.
- **SUPPORTS KUBERNETES:** The secrets don't need to be exposed while building or deploying the application. Rather, the utility can monitor the environment in real-time and inject secrets at runtime when they are required.
- **STRONG SEGREGATION WITH ROLE-BASED ACCESS CONTROL:** Role-based access control (RBAC) for users, applications, and groups with segregation of duties. This gives more visibility into who is reading secrets on the client side.
- **JSON WEB TOKENS:** Supports JWT authentication to further secure and trust requests, collecting and managing secrets.
- **SECURE CUSTOMIZED PLUGINS:** Easily customizable plugins allow you extend functionality and connect to any DevOps environment.



API-driven Credential Manager for DevOps and Apps

How the solution works?

Fortanix Data Security Manager provides a very simple and intuitive GUI for all users, regardless of their role. Secrets "belong" to Groups. Each secret stored in Data Security Manager is associated with its creator and is stored in a specific Group. Only the user(s) associated with that group have access to the secret, according to their role/privileges, which may be further controlled by means of a quorum approval policy. It is easy to inspect (through the GUI or REST API) who is the creator of a secret and which other users are in the Group (and their roles). Additional users can be added to the Group (thereby gaining access to the secrets therein) at any time. Groups in Data Security Manager can be mapped to external AD groups via an external role mapping feature that further allows applying AD group based RBAC.

info@fortanix.com | +1 (650) 943-2484 | 800 West El Camino Real, Suite 180, Mountain View, CA 94040