SECUREKI®

SecureKi Secret Management

www.secureki.com

SecureKi Secret Management

As organizations increasingly rely on digital technologies to store and transmit sensitive information, securing that information has become a critical priority. A secret management system is an essential practice for any organization that deals with sensitive data and provides a centralized repository for securing and managing sensitive information with the right level of encryption, access controls, and policies to mitigate the risk of data breaches.

What is Secret Management?

Secrets management is the practice of securely storing, sharing, and managing sensitive information, such as passwords, API keys, cryptographic keys, and other credentials, needed to access protected resources, services, and systems. The goal of secret management is to prevent unauthorized access to sensitive information while allowing authorized users and applications to access it when needed. Secret management also ensures that secrets are rotated and updated regularly to minimize the risk of a security breach.

KEY BENEFITS

- Mitigating the risks of cyber-attacks and data breaches in the DevOps environment.
- Improved security maturity in DevOps (DevSecOps) environments.
- Reduced risks associated with unauthorized access to confidential data.
- Satisfying audit and compliance by meeting the regulatory requirements.

Effective secret management involves several vital principles, including secure storage, limited access, rotation, and monitoring. Secrets should be stored securely, such as using encryption or hashing, to protect them from unauthorized access. Access to secrets should

C-13-09, Sunway Nexis, No 1, Jalan PJU 5/1, Kota Damansara, 47810 Petaling Jaya, Selangor
info@secureki.com
+603 7652 1188
+603 7652 1189

be limited to only those who need them, and access should be logged and monitored for any suspicious activity. The rotation of secrets is important to prevent long-term exposure of sensitive information, significantly if a secret is compromised. Lastly, monitoring should be in place to detect unauthorized access or changes to secrets. Secrets management is essential in modern software development, where applications often rely on external services and APIs. Having good secret management practices is vital to protect sensitive data and ensuring the security and reliability of applications.

The Challenges

Secrets management can present several challenges, particularly as organizations scale and their systems and infrastructure become more complex. Some of the common challenges include

Security

Keeping secrets secure is the primary challenge of secret management. Unauthorized access to sensitive information can have serious consequences, such as data breaches, data loss, and other security incidents. Maintaining strong security practices and using secure storage mechanisms are essential to minimize these risks.

Scale

As organizations grow, the number of secrets they need to manage can increase rapidly, making it a challenge to track of them all. Scaling secret management requires tools and processes that can accommodate large numbers of secrets and users while maintaining high levels of security.

Complexity

Secret management can be complex, particularly in environments with diverse systems and infrastructure. Secret management systems need to be flexible enough to work with a various of systems, platforms, and tools.

Compliance

Many organizations are subject to regulations that require them to protect sensitive information, such as financial data, personal information, and medical records. Secret management systems must comply with these regulations and provide audit trails and other documentation to prove that secrets are managed securely.

Automation

Automating the management of secrets can help reduce the risk of human error and increase efficiency. However, automation also presents security risks if not implemented carefully. Balancing automation with strong security practices is critical for effective secret management.

DevOps Integration

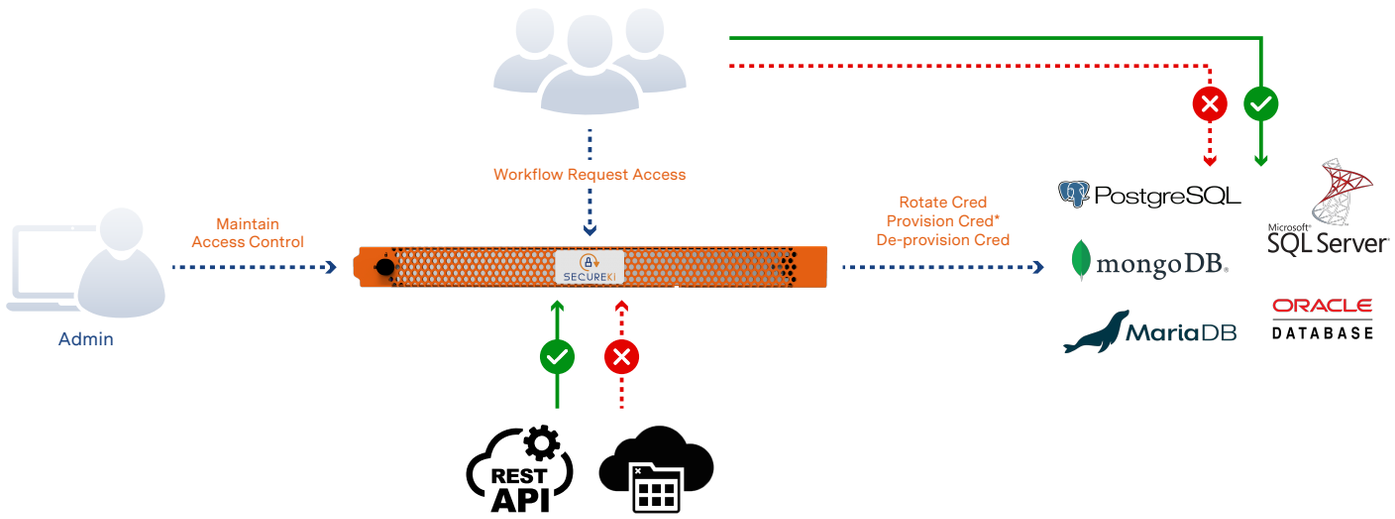
Integrating secrets management into DevOps pipelines can be challenging, particularly if the pipeline is distributed across multiple environments and tools. Secret management systems must be designed to work seamlessly with DevOps tools and workflows while maintaining strong security and compliance standards.

Addressing these challenges requires a comprehensive approach that considers security, scalability, complexity, compliance, automation, and integration. By developing a robust secret management strategy that accounts for these factors, organizations can minimize the risks associated with managing sensitive information and maintain the security of their systems and data.

SecureKi Secret Management Solution Overview

SecureKi extended ACM provides a single centralized platform to securely store, control and manage secrets outside the source code in the credential management vault with flexible deployment modes and scalable architecture. SecureKi secret management works across environments, on-premises, natively in the cloud, hybrid, and multi-cloud. It integrates with any DevOps environment with methods like CLIs, Rest APIs, and PULL/PUSH.

How SecureKi Secret Management Works?



SecureKi Secret Management module enables the protection and proper management of secrets in Kubernetes/K8s or hardcoded passwords in source code. Based on the diagram above, the admin can establish access control through role-based permissions within the SecureKi Web portal. This feature ensures that specific groups of users or applications can only access what they have been authorized to do so. Additionally, SecureKi audits track each usage of the database credentials. Through SecureKi's privileged request workflow, users can apply for admin credentials to perform tasks such as data modification or patching. This process is in place to ensure a least privileged approach is taken, thereby minimizing the risk of misuse of the admin credentials. SecureKi provides a solution to prevent service account passwords from being hardcoded in scripts or runtime on K8s by offering admin credentials retrieval via REST API/Sidecar method. This method ensures that secrets are not exposed during the application building or deployment process.

Solution Highlights

Full Visibility of Secrets in The Environment

Prevent unauthorized access and limit access to resources once entry is granted to the network. Protect passwords and other credentials from unauthorized use and compromise. Limit the actions users can perform on systems and prevent the execution of unauthorized commands and prevent lateral movement within the network.

Controlled and Monitored Access to Sensitive DevOps Resources

Centralizes access to DevOps features for maximum control and visibility.

Centralized Protection, Management, and Auditing of Secrets

Automatic management and protection of user and machine secrets from the moment they are created. All events related to secrets are automatically and permanently recorded for audit purposes.

Secrets Rotation

Secure storage, rotation, and access control for secrets objects, which automatically reset/change the secret password according to your company's security policies.

Secrets Kubernetes and Openshift

The secrets must not 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.

C-13-09, Sunway Nexis, No 1, Jalan PJU 5/1, Kota Damansara, 47810 Petaling Jaya, Selangor
info@secureki.com
+603 7652 1188
+603 7652 1189

Benefits of having secret management

Enhanced security

Secret management helps to secure sensitive data by preventing unauthorized access and misuse. It ensures that sensitive data is protected with the right level of encryption, access controls, and policies to mitigate the risk of data breaches.

Centralized management

Secret management provides a centralized repository for storing sensitive data. It allows organizations to manage all their secrets in one place, making enforcing policies, rotating keys, and revoking access easier.

Compliance

Secret management ensures that organizations comply with regulatory requirements, such as HIPAA, PCI-DSS, and GDPR. It enables organizations to store, manage, and protect sensitive data in a way that meets regulatory standards and avoids penalties.

Scalability

Secret management enables organizations to scale their security infrastructure as their needs evolve. It allows them to manage secrets across multiple environments, including on-premises and cloud-based systems.

Simplified auditing

Secret management makes it easier to track who has access to sensitive data, when they accessed it, and what actions they performed. It enables organizations to simplify the auditing process and generate comprehensive reports that demonstrate compliance with regulatory requirements.

Collaboration

Secret management facilitates team collaboration by providing secure access to sensitive data. It enables teams to share secrets without compromising security or violating compliance requirements.

In summary, secret management is critical for protecting sensitive data and ensuring the continued success of an organization. A secret management system can safeguard your organization from data breaches and other security threats while enabling collaboration and innovation.

C-13-09, Sunway Nexis, No 1, Jalan PJU 5/1, Kota Damansara, 47810 Petaling Jaya, Selangor
info@secureki.com
+603 7652 1188
+603 7652 1189