BeyondTrust

DEVOPS SECRETS SAFE

SECURE SECRETS MANAGEMENT FOR ENTERPRISE DEVOPS

Enforce Secrets Management Best Practices

Secure and automate the storage and access of secrets used by applications, tools, and other processes across your DevOps environment.

Support Peak DevOps Agility

A REST API-first approach and CLI tool provide your teams with a preferred UX that helps drive fast adoption and increased productivity.

Integrate with DevOps Toolchain

Enable faster application delivery via frictionless native integrations with common DevOps tools such as Ansible, Jenkins, and Azure DevOps.

DevOps Secrets Safe enables enterprise teams to secure and manage credentials and other secrets used in their continuous integration and continuous delivery (CI/CD) toolchain, applications, and other automated processes. The solution helps organizations to reduce the security and compliance risks associated with secrets sprawl, while improving agility.

Features and Capabilities

- **Centralized Secrets Management:** Bring all secrets and privileged credentials used by applications, tools and other non-human identities under centralized administration (storage, access, and audit) in a solution designed specifically for dynamic DevOps environments. Replace hard-coded credentials in scripts and code with API calls to further control privileged access and harden the attack surface.
- **REST API-First Approach and CLI Tool:** REST APIs enable DevOps workflows and a Command Line Interface (CLI) tool allows for easy API interaction, increasing velocity and agility for DevOps teams.
- **Native Integrations with DevOps Toolchain:** Leverage out-of-the-box integrations to secure and manage secrets used by IaaS cloud platforms, CI/CD tools, containers, orchestration tools, and more. DevOps Secrets Safe also integrates with common identity repositories for authentication.
- **Enterprise-Class Availability and Performance:** Mitigate the risk of downtime with a highly available solution based on microservices. The DevOps Secrets Safe architecture and deployment model meets the fault-tolerance and scalability requirements of complex enterprise environments.
- **Automated Audit and Recordkeeping:** Create an audit trail of all secrets operations so you always know who accesses what and when. You also have the ability to audit the entire secrets lifecycle.

Shift Security Left

Credentials and secrets used in DevOps environments are a prime target for attackers. Implementing a centralized administration solution like DevOps Secrets Safe reduces the risk of exposure without slowing down the application delivery process.

DevOps Secrets Safe is built to meet the dynamic requirements of highly elastic DevOps environments. The underlying architecture and deployment model balance the need to operate securely with the velocity and high-availability requirements of enterprise teams.

BUSINESS BENEFITS

Increase Productivity

Automate the storage, access, and audit of secrets so your teams are liberated from manual, insecure, and inconsistent practices.

Simplify Compliance

A complete, readily accessible audit trail of all secrets and credential operations helps to demonstrate compliance with regulations and avoid the costs associated with failed audits.

Reduce Risk

Enforce best-practice credential management across all DevOps environments to eliminate some attack vectors outright and to shrink other risks related to compromised credentials, while supporting compliance initiatives.