# DevOps Secrets Safe v20.1

## New Product Release

**BeyondTrust DevOps Secrets Safe** is a new, standalone product for centralized secrets administration (store, access, and audit) designed for the high volume and dynamic nature of workloads found in DevOps environments. The solution helps organizations to secure credentials and other secrets (passwords, API keys, certificates, etc.) used in their continuous integration and continuous delivery (CI/CD) tool chain, applications, and other automated processes.

DevOps Secrets Safe is designed for enterprise teams committed to DevOps best practices and dedicated to applying secure solutions at every step of the process. The DevOps Secrets Safe architecture and deployment model helps organizations meet enterprise security and compliance requirements, and is aimed at supporting teams transitioning from open source tools to a comprehensive secrets management solution.

## Feature Highlights

### Securely Store & Retrieve Secrets

Securely store and retrieve credentials or secrets of any kind: API Keys, Passwords, Certificates. Grant access to users and applications.

This is the foundational tenet of the solution, designed to help organizations to reduce the risks associated with secrets sprawl. DevOps Secrets Safe secures and automates the storage and access of credentials or secrets used by applications, tools, and other non-human identities in dynamic DevOps environments. Customers can bring all secrets under centralized management into a safe with authentication, authorization, and auditing, providing full control and visibility into secrets usage.

### REST API Support

Developers aim to continually deliver code faster. Their agile workflows may be disrupted by security tools that work counter to their practices, slowing down productivity. DevOps Secrets Safe is designed to enable DevOps teams by providing a REST API-first approach. This enables DevOps workflows with full application coverage for peak agility.

## Command Line Interface (CLI) UI

As the preferred UX for developers, providing CLI support for tool administration and easy API integration enables faster solution deployment and adoption. This increases velocity and agility in the DevOps pipeline.

## High Availability & Performance

Architected with micro-services built on Docker containers and targeting Kubernetes as a deployment platform provides a highly scalable, fault-tolerant deployment.

Enterprises must meet security standards around privileged access management in all areas, including traditional IT and highly elastic DevOps environments. These requirements are best addressed by enterprise-class solutions that offer uncompromising security and stability, while enabling the speed and agility required by DevOps workflows. DevOps Secrets Safe's architecture and deployment model helps organizations to meet these stringent resiliency, scalability, and performance requirements.

## Audit Every Action

Every action creates an actionable event stream for log aggregation and security workflow triggers.

Enterprises must meet compliance requirements around privileged access. A complete, readily accessible audit trail is generated by DevOps Secrets Safe for log aggregation of all secrets and credential operations. This approach leverages the enterprise aggregator tools and helps to demonstrate compliance with security policies and regulations. Customers also have the ability to audit the entire secrets lifecycle.

## Applications as Identities

Create identities for applications with specific authorization grants. Audit automated secret access.

In the context of secrets management, applications are nonhuman consumers of secrets. Applications assume privileged access in automated workflows, so it is critical that they are identified, authorized, and audited. This feature enables the automated administration of applications as identities and the audit of secrets access.

## Safelists

Secure API access by applying IP filters to inbound requests.

Add a layer of security by limiting access to secrets based on IP filters applied to inbound requests.

## Native Integrations

Leverage centrally controlled secrets directly from CI/CD toolchain applications.

An effective secrets management solution that truly enables DevOps agility leverages native integrations with common DevOps tools. DevOps Secrets Safe supports integrations with a number of tools such as Ansible, Jenkins, Azure DevOps, and a simple REST interface for broad integration support.

About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing data breaches related to stolen credentials, misused privileges, and compromised remote access.

Our extensible platform empowers organizations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. BeyondTrust unifies the industry's broadest set of privileged access capabilities with centralized management, reporting, and analytics, enabling leaders to take decisive and informed actions to defeat attackers. Our holistic platform stands out for its flexible design that simplifies integrations, enhances user productivity, and maximizes IT and security investments.

BeyondTrust gives organizations the visibility and control they need to reduce risk, achieve compliance objectives, and boost operational performance. We are trusted by 20,000 customers, including half of the Fortune 500, and a global partner network. Learn more at www.beyondtrust.com.