DevOps Secrets Safe v20.2

Feature Release - April 14, 2020

BeyondTrust DevOps Secrets Safe is a standalone product for centralized secrets administration (create, store, access, and audit) designed for the high volume and dynamic 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, automated processes and other non-human identities.

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 solution's architecture leverages the full stack of Kubernetes as the DevOps deployment platform of choice. This allows our customers flexibility in deployment to meet their business needs (e.g. their preferred cloud provider or on-prem) and to cost-effectively meet enterprise security and compliance requirements.

New Feature Highlights

Secret Generation

As infrastructure is deployed to support a DevOps workflow, there is often a need to create either default or specific application accounts. It's important to initialize these accounts with unique, secure credentials even during a fully automated build process. DevOps Secrets Safe can now generate policy-based secrets that comply with strict security requirements as part of your automated build pipeline.

Generating a password or credential for these newly created accounts helps to mitigate the practice of embedding static credentials in applications, tools or even code. We do this by creating a secret that can be dynamic and managed within DevOps Secrets Safe solution.

Azure DevOps Integration

Native integrations are a key component of allowing DevOps teams to easily consume DevOps Secrets Safe services from their CI/CD tools. This allows them to focus on the applications they are building rather than the toolset involved. Adding to the list of native integrations, Azure DevOps marketplace now has a DevOps Secrets Safe integration that can be used as a task for

secret retrieval during a build pipeline helping to secure your build process and increase the agility of your toolset.

MSSQL Support

One of the goals of DevOps Secrets Safe is to be vendor agnostic across various aspects of the solution including deployments, audit, and the backend database that supports persistent storage of Secrets and configuration. We have extended our supported backend databases to include Microsoft SQL Server. Simply define MSSQL at deployment and utilize your existing enterprise database infrastructure meeting all your speed, scale, and resiliency requirements.

CLI Auto Complete

DevOps Secrets Safe includes a convenient CLI wrapping the REST API for administration of the solution. This CLI is now even easier to use and navigate with the addition of bash-completion providing easy, application specific command completion.

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.