BeyondTrust DevOps Secrets Safe v20.4

Feature Release – December 8, 2020

DevOps Secrets Safe is BeyondTrust's solution for centralized secrets administration (create, store, access, and audit) designed for the high volume and dynamic workloads found in DevOps environments. DevOps Secrets Safe 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.

See the release notes for details.

New Feature Highlights

Dynamic Accounts

Every cloud service provider offers an extensive API that enables DevOps engineers an automated way of managing their entire infrastructure. The accounts used to access these APIs are considered highly privileged, are primary targets for attackers, and therefore should be protected. The recommended step for securing these accounts is to utilize a centralized secrets management solution to store these sensitive API keys used for access. In v20.4 DevOps Secrets Safe builds on its secrets management capabilities by dynamically generating these API accounts with a just-in-time model for privileged access. Automated workflows typically only need a short window of access to accomplish a specific task. The persistence of a privileged account outside of this window represents a vulnerability for your infrastructure and introduces unnecessary risk. By brokering access to cloud environments through DevOps Secrets Safe, organizations can mitigate this risk and drastically reduce the security footprint of their automated workflows.

Native 2FA

DevOps Secrets Safe already offers the protection of multi-factor authentication through 3rd party integrations. In v20.4 we introduced a built in time-based one-time password (TOTP) 2FA workflow for all users of DevOps Secrets Safe. This native 2FA capability is an essential component in any security solution and ensures that every account can be protected regardless of type or availability of other external dependencies.

Kubernetes Sidecar

The DevOps Secrets Safe integration with Kubernetes enables service accounts as identities for access to secrets. It also provides a simple init container for interacting directly with DevOps Secrets Safe on behalf of the application container at startup. In some situations, the secrets provided to an application may need to be updated during the lifecycle of the applications container. For these instances, the BeyondTrust secrets-agent container can be defined as a sidecar retrieving secrets on a defined interval, keeping your application up to date with the latest available secret.

Kubernetes v1.19

The entire DevOps tool landscape is continually changing. This pattern of constant change directly impacts DevOps Secrets Safe or its underlying Kubernetes infrastructure. With a commitment to supporting the latest tools and services, DevOps Secrets Safe is now certified for deployment on v1.19 (current latest) Kubernetes clusters. This means our customers can take advantage of the most current technology updates within their own DevOps toolchain.

About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud, and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network. Learn more at www.beyondtrust.com.