BeyondTrust DevOps Secrets Safe v21.1

Feature Release – April 15, 2021

DevOps Secrets Safe is a solution for centralized secrets administration (create, store, access, and audit), designed for the high volume and high change workloads found in DevOps environments. The solution helps enterprises secure credentials and other secrets (passwords, API keys, certificates, etc.) used by applications and other non-human identities. Built on a fault-tolerant, highly available architecture and deployment model, DSS helps customers meet their most demanding scalability and performance requirements while providing a full audit trail of all secrets operations and the entire secrets lifecycle.

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 architecture 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

Enhanced - Dynamic Accounts

DevOps Secrets Safe can dynamically generate API accounts for automated processes to access various cloud environments. This workflow utilizes a "provider account" responsible for creating and deleting the requested service account on Secrets Safe's behalf. While this provider account should not have excessive permissions, it is still a source for potential stale credentials. Additionally, the responsibility of managing the lifecycle of dynamically generated accounts resides with the automated workflow. If proper deletion of accounts is missed during this workflow, it could leave service accounts active for longer than necessary and lead to additional cleanup activities and increased risk of exposure.

In this release, Dynamic Accounts have been enhanced by automating account lifecycle management and strengthening their security profile. Service accounts generated by Secrets Safe can now be configured with a "time to live" duration, limiting their access.

When this period is reached, these accounts will be automatically removed from the cloud infrastructure, significantly reducing their availability as a potential attack vector. Furthermore, the minimally privileged but longer-lived provider account can now continually self-manage its credentials by rotating the cloud API key and further enhancing its security.

Dynamic Accounts with Ansible

Ansible is often used to stand up infrastructure in the Cloud. This process requires Ansible workflows to have automated access to cloud APIs, which leverage service accounts' API keys. This automated access makes the API keys highly privileged and, therefore, must be secured accordingly. It is recommended to apply the principle of least privilege to the specific task being done by removing hard-coded API keys from source and configuration files, effectively limiting potential account compromise.

In this release, customers can secure their Ansible playbooks when interacting with cloud APIs by leveraging a dynamic account generated by DevOps Secrets Safe. This integration secures automated workloads by using a credential created just-in-time (JIT) with just the right level of privilege and scope, while eliminating hard-coded or embedded Cloud API keys. This approach meets best practices for least privilege and JIT, significantly enhancing your Ansible playbooks' security.

New - RPA Tool Integration: Blue Prism

RPA tools automate business processes for systems that require manual steps or user interaction. These processes often require passwords or API keys for authentication and access to various systems or information. The integration between DevOps Secrets Safe and Blue Prism enables the secure storage and usage of this sensitive information by centrally vaulting the secrets, controlling access to them, and maintaining rich audits for all secrets operations.

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 can easily 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.