GitLab

OpenBao

LF EDGE

# OpenBao @ GitLab

## Building Native Secrets for GitLab CI/CD Pipelines

**Alex Scheel**
Staff Software Engineer - Secrets Management @ **GitLab**
TSC Chair, Dev WG Chair, Maintainer @ **OpenBao**

@cipherboy-gitlab, @cipherboy

@cipherboy

# What is OpenBao?

# Open Source Secrets Management [1]

## Static Secrets

- Encrypted key/value storage for sensitive application data
- Version history

✓ Centralized Rotation

## Dynamic Secrets

- Just-in-time database credentials
- On-demand cloud identities
- TOTP generator & provider

✓ Lower Exposure Risk

## Encryption Services

- PKI certificate issuance
- SSH certificate & password generation
- Encryption as a service (Transit)

✓ Transport Security

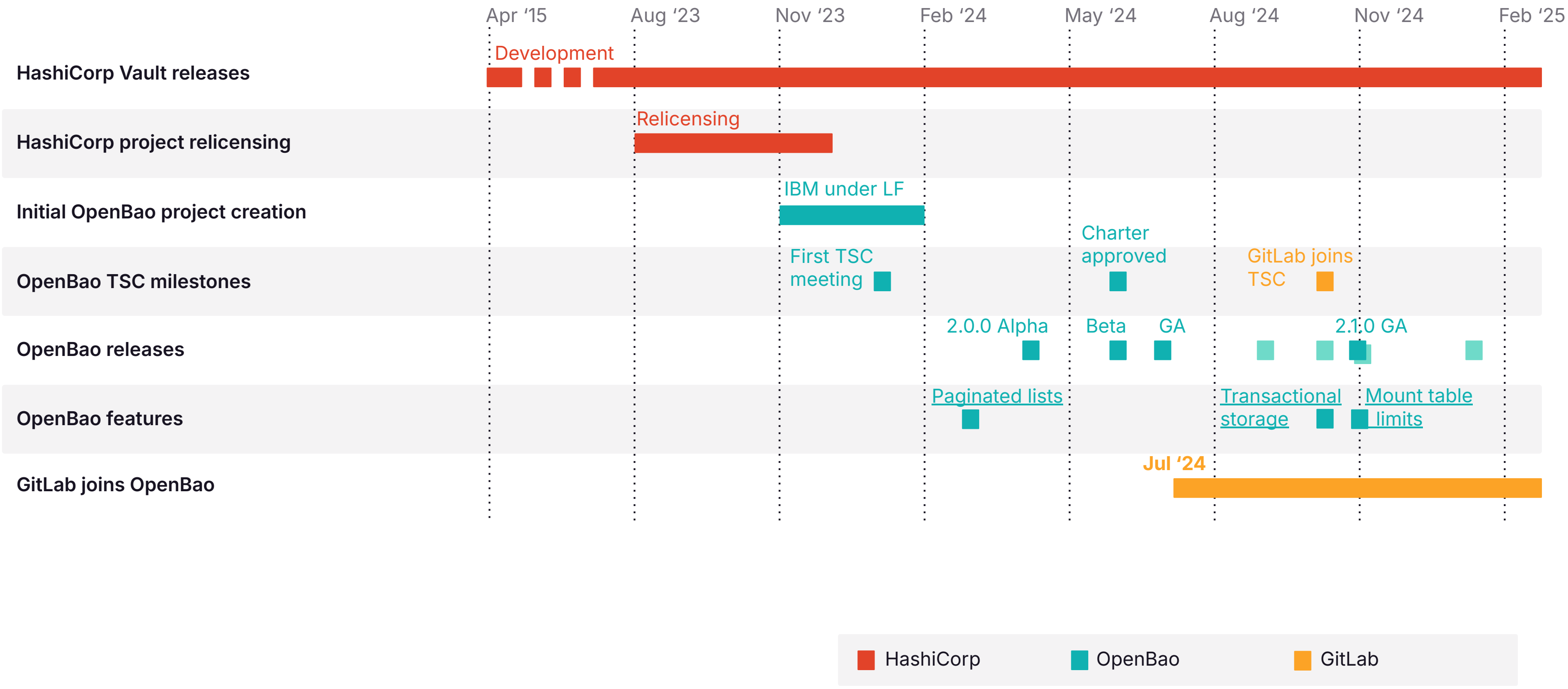
## Sync, Visibility, & Management

- Kubernetes External Secrets Operator
- Audit logs for secret reuse detection
- Agent for last-mile sync and delivery

✓ Better Incident Response

[1] OpenBao is licensed under the MPL and has open governance under the LF Edge subproject of the Linux Foundation.

# A (Brief) History of OpenBao



# What differentiates OpenBao?

Key technological improvements coupled with an open organization structure grants confidence in the future of OpenBao

### Storage improvements

Paginated listing and transactional storage allow plugin authors and core developers to build more scalable, reliable secrets engines. Explicit support for PostgreSQL.

### Scalability improvements

Removing technological limits on the number of mount tables and eventually namespaces allows scaling OpenBao to larger deployments.

### Open governance

Transparent project governance, from Technical Steering Committee to Development Working Group and Maintainership, ensures clear path for recognition.

### Clear contribution process

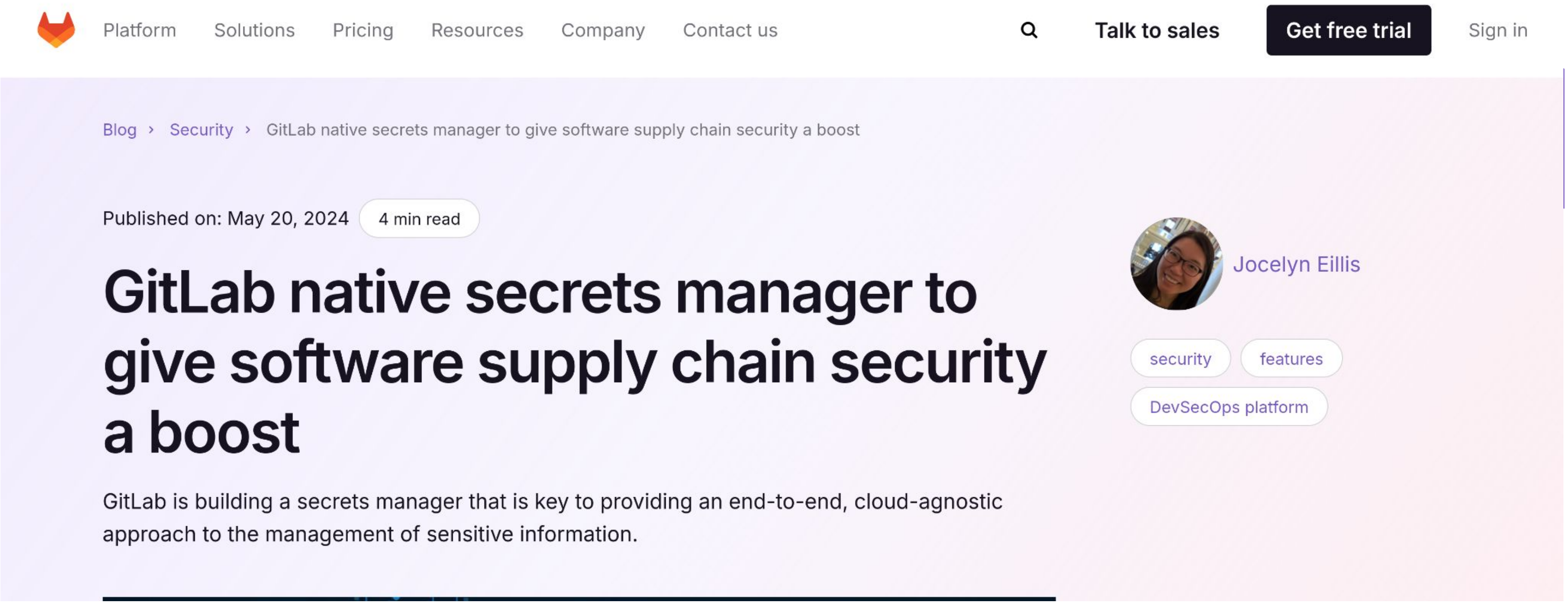
Open Request For Comment (RFC) process ensures equal playing field for feature contributions from everyone.

### Open source license

MPL source license retains the original spirit of the HashiCorp Vault before their proprietary relicensing.

# What is GitLab using OpenBao for?

# Pipeline Secrets Management



Blog › Security › GitLab native secrets manager to give software supply chain security a boost

Published on: May 20, 2024 4 min read

## GitLab native secrets manager to give software supply chain security a boost

Jocelyn Eillis

security features DevSecOps platform

GitLab is building a secrets manager that is key to providing an end-to-end, cloud-agnostic approach to the management of sensitive information.

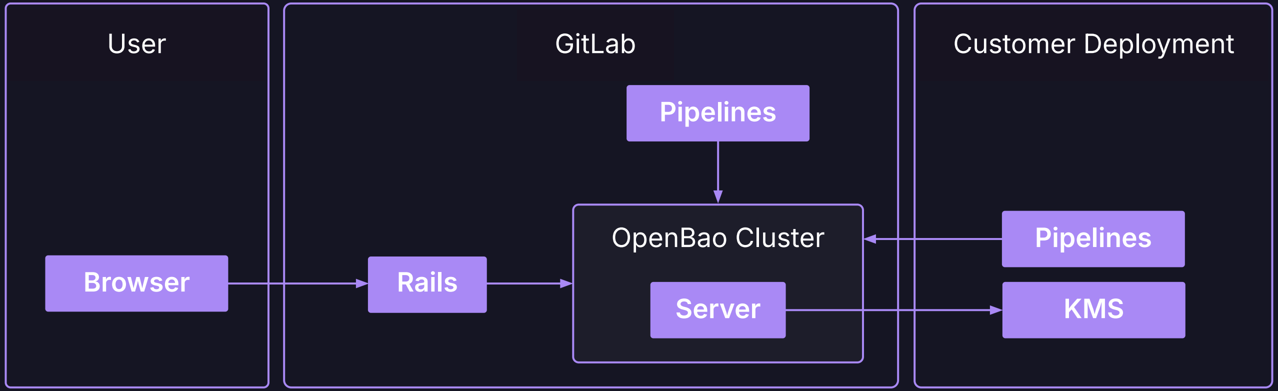
Blog: https://about.gitlab.com/blog/2024/05/20/gitlab-native-secrets-manager-to-give-software-supply-chain-security-a-boost/
Design: https://handbook.gitlab.com/handbook/engineering/architecture/design-documents/secret_manager/

# OpenBao: a familiar program

GitLab already has a HashiCorp Vault pipeline secrets integration; by bundling OpenBao, we can offer a product-native pipeline security solution without the operator overhead.

- Repository-centric control of access policy
- Centralized audit reports
- Native pipeline integration avoids application changes
- Clear security division between Rails and secret store

# Architecture overview



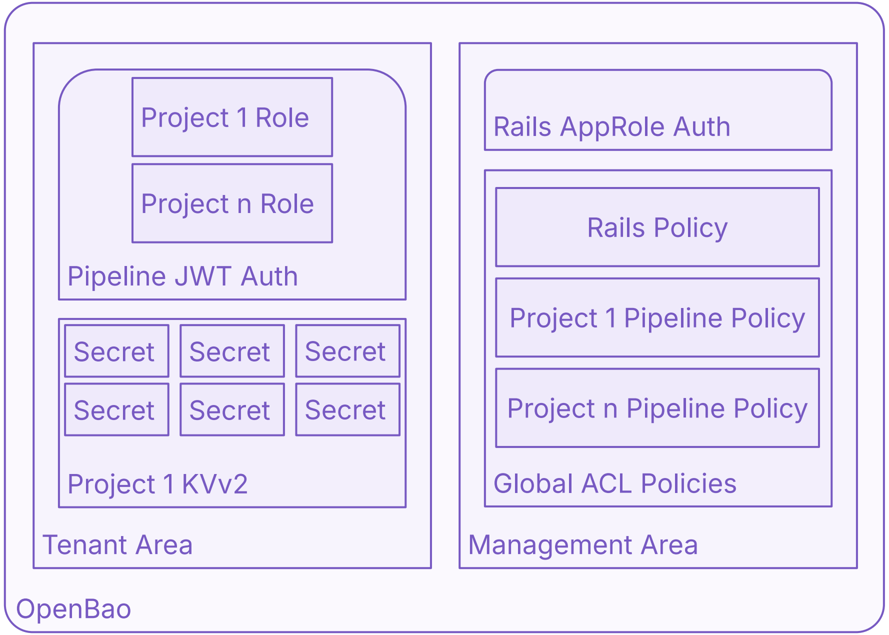
# OpenBao: Data Layout

Now:

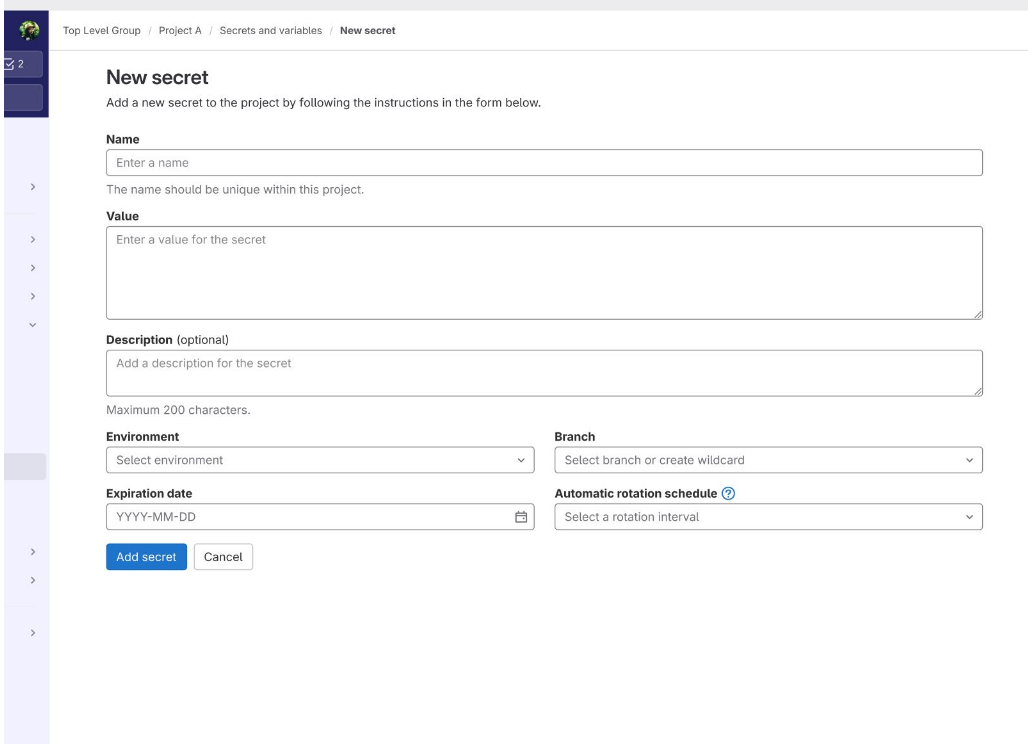
- **AppRole** for Rails auth
- **JWT** for Pipeline auth
- **KVv2** secret store

Long-term:

- Per-tenant **namespaces**, **seals**
- Per-user **Rails auth**



# View from a Pipeline Author



Top Level Group / Project A / Secrets and variables / New secret

## New secret

Add a new secret to the project by following the instructions in the form below.

**Name**

Enter a name

The name should be unique within this project.

**Value**

Enter a value for the secret

**Description** (optional)

Add a description for the secret

Maximum 200 characters.

**Environment**

Select environment

**Branch**

Select branch or create wildcard

**Expiration date**

YYYY-MM-DD

**Automatic rotation schedule**

Select a rotation interval

```
image: fedora:latest

stages:
  - build

build:
  stage: build
  secrets:
    REGISTRY_PASS:
      gitlab_secrets_manager:
        name: REGISTRY_PASS
  script:
    - push-container \
      --password="$REGISTRY_PASS"
```

/.gitlab-ci.yml

# How can you get involved?

Weekly community calls:
10AM US Central / 5PM GMT+1

@OpenBao

✉ openbao@lists.lfedge.org

## #569

Develop a roadmap item on GitHub

## 3

Working groups: Namespaces, PKCS#11, and Horizontal Scalability

## Like

Share or author OpenBao blog posts on social media and with colleagues

## Beta

Ask your account team about joining the GitLab Pipeline Secrets beta program

GitLab

# Questions? Thank you!

**Alex Scheel**
Staff Software Engineer - Secrets Management @ **GitLab**
TSC Chair, Dev WG Chair, Maintainer @ **OpenBao**

@cipherboy-gitlab, @cipherboy

@cipherboy

openbao.org