



RADICALBIT

AI Gateway

Open Source vs Enterprise

What each edition includes, and how to choose.

Open-source to Adopt, Enterprise to Govern

The split follows feature type, not maturity



OPEN SOURCE

Routing, guardrails, caching, configuration and observability.
Open to drive adoption and community contributions.



ENTERPRISE

Identity, control and compliance: SSO, roles, audit trail and cloud secret managers.
Required by SOC 2, ISO 27001 and DORA.

How Enterprise Is Built

A front-end and plugins on top of the OS back-end

- **OS front-end**: public repo
- **EE front-end**: private repo
- **Enterprise plugins**: Python packages installed into the image, including Keycloak / IDP, cloud secret managers and audit log
- **Open Source Gateway back-end**: the same engine in both editions, and the Docker image base for Enterprise

There is no separate Enterprise backend. Enterprise is the OS back-end plus plugins.

Configure and Route Traffic

The open source core, part of every edition

ROUTING

Routes and fallbacks, plus advanced routing by keyword, cost, token length, semantic similarity and LLM judgment.

GUARDRAILS & CACHING

String matching, LLM Judge and Presidio guardrails, plus response caching.

AI-ASSISTED CONFIGURATION

Write the YAML with AI help or by hand, with validation and separate Prod and Dev slots.

Observe and Secure Access

The rest of the open source core

OBSERVABILITY

Usage and cost dashboard, tracing, application logs, and rate, budget and token limits with alerts.

MANY API TYPES

Chat, embeddings, transcription billed per second of audio, and MCP.

CREDENTIALS & GROUPS

Local API keys and groups, associated with routes inside a project.

Side by Side

Capability	Open Source	Enterprise
Routing, guardrails, caching, AI-assisted config	✓	✓
Usage, tracing, limits	✓	✓
MCP support	✓	✓
Alert rules	Email	Email, other channels under evaluation
Credentials	Local API keys	Local keys + IDP credentials, JWT
Secret management	Local file	Local + Vault, AWS, GCP, Azure
Login and SSO (Keycloak / corporate IDP)	—	✓
Roles: Admin, Builder, Auditor	None, everyone has the same access	✓
User-to-project association	—	✓
Immutable audit log	—	✓

What Enterprise Adds: Governance

Why it matters for SOC 2, ISO 27001 and DORA



IDENTITY & SSO

Keycloak or corporate IDP login. Routes can use a JWT.



ROLES (RBAC)

Admin, Builder and Auditor, with read-only access for Auditors.



AUDIT LOG

Append-only record of who did what and when, exportable for audits.



CLOUD SECRETS

Read keys from Vault, AWS, GCP or Azure instead of a local file.

Which Edition Fits?

Start with Open Source

- One team runs and trusts the gateway
- Secrets live in a local file
- You want routing, guardrails, MCP and alerts at no cost
- You want to read the code or contribute to it

Move to Enterprise

- Several teams or projects need separate access
- You already have a corporate IDP and a cloud KMS
- Auditors need a read-only view and an audit trail
- You must meet SOC 2, ISO 27001 or DORA

Same engine underneath. Moving to Enterprise adds plugins and the enterprise UI on top of the Gateway you already run.



Thank you

radicalbit.ai

info@radicalbit.ai

