



AI Gateway

Open Source vs Enterprise

Cosa include ciascuna versione e come scegliere.

Open-source per l'Adozione, Enterprise per la Governance

La suddivisione dipende dal tipo di funzionalità, non dalla maturità.



OPEN SOURCE

Routing, guardrails, caching, configurazione e osservabilità.

Codice aperto per guidare l'adozione e i contributi della community.



ENTERPRISE

Identità, controllo e conformità: SSO, ruoli, audit trail e cloud secret manager.

Richiesto dalle normative e dagli standard SOC 2, ISO 27001 e DORA.

Com'è costruita la versione Enterprise

Un front-end e dei plugin basati sul back-end OS

- **Front-end OS:** repository pubblico
- **Front-end EE:** repository privato
- **Plugin Enterprise:** pacchetti Python installati nell'immagine, inclusi Keycloak / IDP, secret managers and audit log
- **Back-end del Gateway Open Source:** lo stesso motore in entrambe le versioni e la base dell'immagine Docker per la versione Enterprise

Non esiste un back-end Enterprise separato. La versione Enterprise è il back-end OS con l'aggiunta dei plugin.

Configurazione e Route Traffic

Il core open source, parte di ogni versione

ROUTING

Routes e fallbacks, oltre a un routing avanzato per keyword, costo, lunghezza dei token, similarità semantica e valutazione tramite LLM.

GUARDRAIL & CACHING

String matching, guardrails basati su LLM Judge e Presidio, oltre al response caching.

CONFIGURAZIONE ASSISTITA DALL'AI

Scrivi lo YAML con l'aiuto dell'AI o manualmente, con convalida e slot separati per Produzione e Sviluppo.

Osservare e proteggere l'Accesso

Il resto del core open source

OSSERVABILITÀ

Dashboard dei consumi e dei costi, tracciamento, log dell'applicazione e limiti di rate, budget e token con avvisi.

MOLTI TIPI DI API

Chat, embedding, trascrizione fatturata al secondo di audio e MCP.

CREDENZIALI E GRUPPI

API key locali e gruppi, associati a route all'interno di un progetto.

Confronto diretto

Funzionalità	Open Source	Enterprise
Routing, guardrail, caching, configurazione assistita dall'AI	✓	✓
Utilizzo, tracciamento, limiti	✓	✓
Supporto MCP	✓	✓
Regole di avviso	Email	Email, altri canali in fase di valutazione
Credenziali	API key locali	API key locali + credenziali IDP, JWT
Gestione dei secret	File locale	Locale + Vault, AWS, GCP, Azure
Login e SSO (Keycloak / IDP aziendale)	—	✓
Ruoli: Admin, Builder, Auditor	Nessuno, tutti hanno lo stesso accesso	✓
Associazione utente-progetto	—	✓
Audit log immutabile	—	✓

Cosa aggiunge la versione Enterprise: Governance

Perché è importante per SOC 2, ISO 27001 e DORA



IDENTITÀ & SSO

Login tramite Keycloak o IDP aziendale. Le route possono utilizzare un token JWT.



RUOLI (RBAC)

Admin, Builder e Auditor, con accesso in sola lettura per gli Auditor.



AUDIT LOG

Registro append-only di chi ha fatto cosa e quando, esportabile per gli audit.



CLOUD SECRETS

Legge le chiavi da Vault, AWS, GCP o Azure anziché da un file locale.

Quale versione scegliere?

Inizia con l'Open Source

- Un singolo team gestisce e si fida del gateway
- I secret risiedono in un file locale
- Vuoi routing, guardrail, MCP e avvisi a costo zero
- Vuoi leggere il codice o contribuirvi

Passa all' Enterprise

- Diversi team o progetti necessitano di accessi separati
- Disponi già di un IDP aziendale e di un KMS cloud
- Gli auditor hanno bisogno di una visuale in sola lettura e di un audit trail
- Devi soddisfare i requisiti SOC 2, ISO 27001 o DORA

Stesso motore alla base. Il passaggio a Enterprise aggiunge i plugin e l'interfaccia utente enterprise sopra il Gateway che stai già eseguendo.



Grazie per l'attenzione

radicalbit.ai

info@radicalbit.ai