

Invinse AI Firewall & LLM Gateway

Secure, Govern, and Scale Enterprise AI Usage

Infopercept

Office Address

3rd floor, Optionz Complex
Opp. Hotel Regenta, CG Road,
Navrangpura, Ahmedabad -
380009, Gujarat, INDIA

Contact Detail

www.infopercept.com
sos@infopercept.com
+91 9898857117

Overview

Invinse AI Firewall & LLM Gateway provides a secure, governed, and scalable access layer for enterprise AI adoption. It acts as a central control point between enterprise AI applications and multiple LLM providers, ensuring safe, compliant, and optimized AI usage.

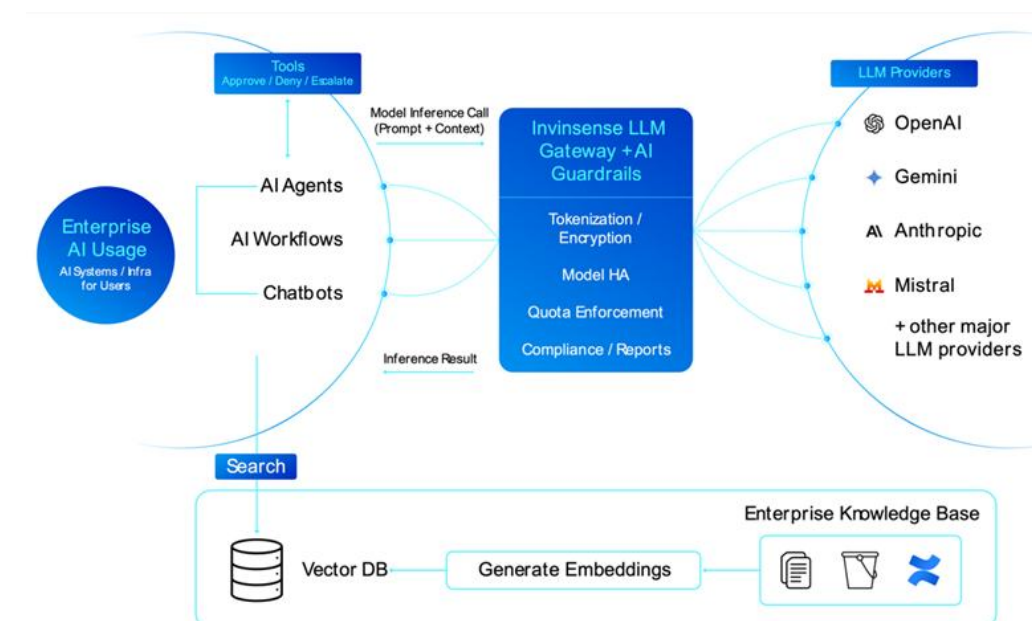
The platform enables organizations to confidently deploy AI agents, workflows, and chatbots while maintaining data protection, policy enforcement, and operational control.

Problem Statement

As enterprises rapidly adopt AI:

- Sensitive data is exposed to external LLMs without control
- No centralized governance over AI usage
- Multiple LLM providers create complexity and inconsistency
- Lack of visibility into prompts, responses, and usage patterns
- Compliance and data residency risks increase

Result: Uncontrolled AI usage, data leakage risks, and governance gaps



Solution Approach



Centralized LLM Gateway

- 1. Single integration layer for:
 - OpenAI, Gemini, Anthropic, Mistral, and others
- 2. Abstracts LLM providers behind a unified API layer
- 3. Enables multi-model strategy without vendor lock-in



AI Firewall & Guardrails

- 1. Enforces
 - Prompt filtering and sanitization
 - Data masking and redaction
 - Policy-based access control
- 2. Prevents
 - Sensitive data leakage
 - Unauthorized AI usage



Secure Inference Management

- 1. Controls full inference lifecycle
 - Prompt + context validation
 - Secure model invocation
 - Response filtering
- 2. Includes
 - Tokenization & encryption
 - Model High Availability (HA))



AI Agent & Workflow Enablement

- 1. Supports
 - AI Agents
 - AI-driven workflows
 - Enterprise chatbots
- 2. Enables controlled execution:
 - Approve / Deny / Escalate actions
- 3. Integrates with enterprise tools for real-world actions



Enterprise Knowledge Integration (RAG)

- 1. Connects to
 - Internal knowledge bases
 - Documents, wikis, structured data
- 2. Uses
 - Vector databases
 - Embeddings for contextual search
- 3. Ensures context-aware and accurate responses



Usage Governance & Quota Enforcement

- 1. Tracks and controls:
 - Token usage
 - API consumption
 - User-level and app-level quotas
- 2. Prevents cost overruns and misuse



Compliance, Audit & Reporting

- 1. Provides:
 - Full audit trails of prompts and responses
 - Compliance reporting
- 3. Supports:
 - Regulatory and internal governance requirements

Key Capabilities



Centralized LLM Gateway
(Multi-Provider Support)



AI Firewall with
Policy-Based Guardrails



Secure Prompt &
Response Management



RAG-Based Enterprise
Knowledge Integration



Tokenization, Encryption
& Data Protection



Quota Management
& Cost Control



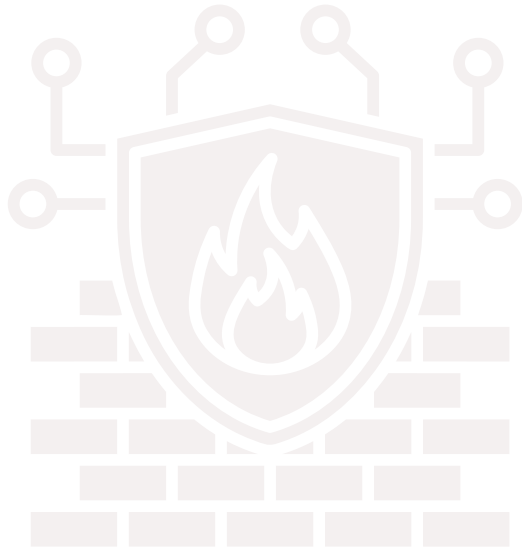
AI Agents & Workflow
Enablement with Action
Control



Compliance, Audit &
Usage Visibility



No Vendor Lock-in
(Multi-LLM Strategy)



Value Proposition



Secure AI Adoption:

Prevent data leakage and
misuse



Centralized Governance:

One control layer for all AI
usage



Flexibility:

Use multiple LLM
providers seamlessly



Cost Optimization

Control and monitor AI
consumption



Better Accuracy

Context-aware AI using
enterprise data



Compliance Ready

Full auditability and
policy enforcement