

Invinsense LLM Gateway & AI Guardrails

Secure, Govern, and Optimize AI at Scale —
Without Compromise

The Enterprise AI Challenge

The explosion of AI adoption

AI adoption has exploded across industries. From customer service to code generation, enterprises are deploying generative AI faster than their security and compliance frameworks can keep up.

LLM Risks

Each interaction with an LLM carries hidden risks – from prompt injection and data leaks to runaway API costs.

Purpose-built AI Gateway

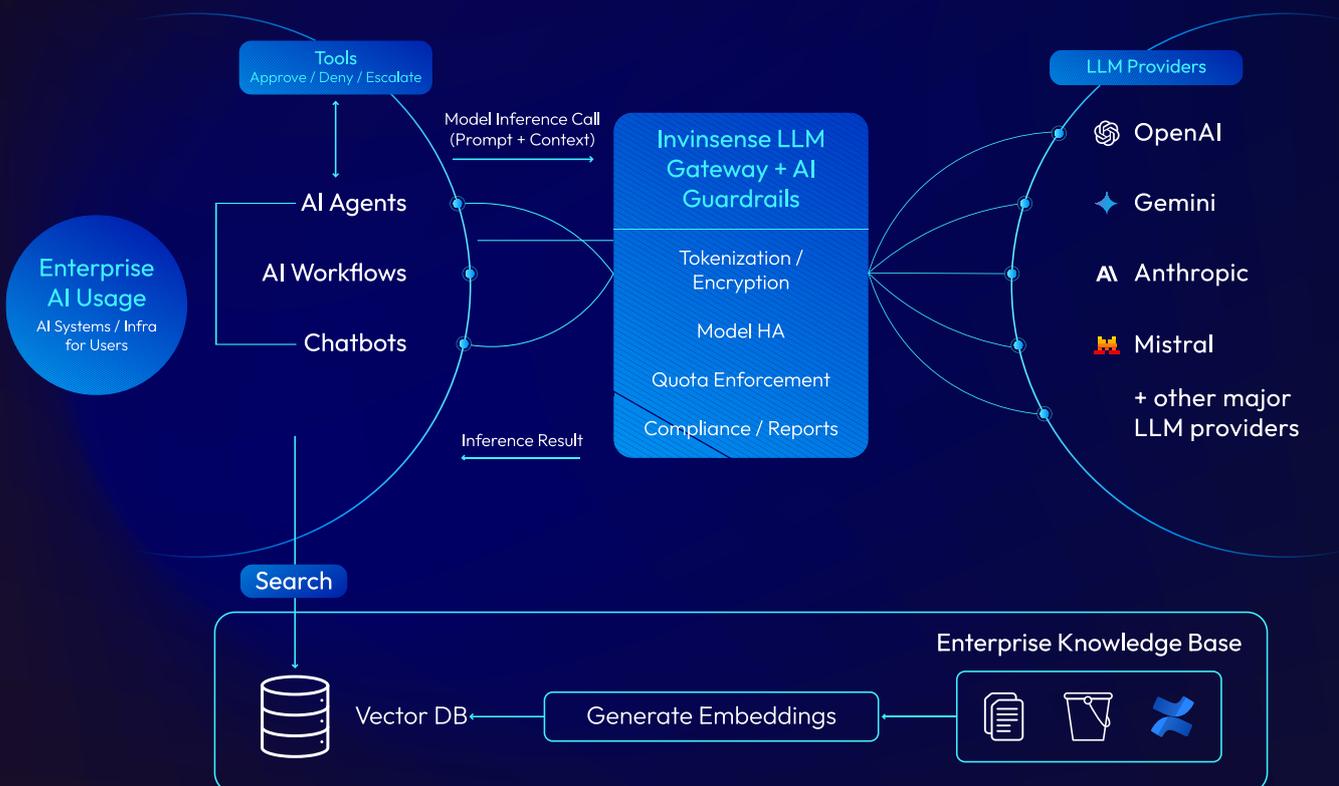
Traditional security tools weren't built for this era. You need a purpose-built AI Gateway – one that enforces control, compliance, and confidence across every AI interaction.

Introducing Invisense LLM Gateway

Your Central Command for Secure and Governed AI Access

Invisense LLM Gateway acts as an intelligent security and governance layer between your enterprise applications, AI agents, and any LLM provider.

It centralizes access, enforces guardrails, optimizes cost, and ensures compliance – enabling innovation without risk.



Core Capabilities

Outcomes

Access Control

Ensure only the right users and apps interact with AI.

- Role-Based Access Control (RBAC) and Policy Enforcement
- SSO, Directory, and OAuth2.0 / OIDC Integration
- Centralized API Key Lifecycle Management
- Comprehensive Audit Logging for Compliance

Eliminate unauthorized access and maintain airtight accountability for all AI activity.

Cost Management

Optimize token usage and prevent runaway AI spending.

- Real-time usage-based cost tracking and attribution
- Dynamic prompt optimization to reduce token consumption
- Intelligent routing to lower-cost models
- Quota, rate-limit, and budget enforcement at every level
- Automated alerts and spend analytics

Up to 60% reduction in AI costs through optimized routing and token control.

Multi-Model & Multi-Provider Routing

Connect once, govern everywhere.

- Unified gateway for OpenAI, Anthropic, Google, Azure, and custom models
- Dynamic model selection based on performance, cost, or compliance
- Load balancing and automatic failover for high availability
- Model-agnostic protocol translation and standardization

One secure entry point for every AI interaction — scalable, portable, and vendor-neutral.

Operational Monitoring & Analytics

End-to-end visibility into your AI ecosystem.

- Real-time telemetry and dashboards
- Health checks and anomaly detection for all model endpoints
- Request tracing and performance analytics
- Compliance audit trails and SLA metrics
- Cost, latency, and reliability insights for optimization

Continuous observability ensures governance, reliability, and peak performance.

Security Enforcement & Guardrails

Defend your AI systems from emerging threats.

- Prompt Injection Detection
- Adversarial Input Filtering & Output Sanitization
- Real-time Sensitive Data Detection (PII, PHI, Financial Data)
- Masking, or Blocking of Sensitive Prompts
- Data Residency and Regulatory Enforcement
- Centralized AI API Key Vaulting and Encryption

Prevent data loss, enforce compliance, and neutralize adversarial AI attacks before they impact your business.

Advanced Features



Agentic AI Governance

Enforce “Should I?” and “How do I?” controls – balancing innovation with accountability.

- **Governing Gateway** - Decides what should be allowed by policy, ensuring compliance and ethical AI use.
- **Routing Gateway** - Decides how to execute safely and efficiently, optimizing model selection, cost, and performance.

Together, they create the Invsense Twin Gateway Architecture – governing and routing intelligence in harmony.



Data Loss Prevention Built for AI

Traditional DLP doesn't understand AI context. Invsense does.

- Context-aware detection
- Compliance assistance for regulated industries
- Policy-driven masking or blocking



Performance Without Compromise

Deploy anywhere - **on-prem**, or **cloud** - while maintaining consistent enforcement and governance.



Extensible and Future-Ready

Why Enterprises Choose Invsense

Challenge

Fragmented AI Usage

Rising AI Costs

Security Risks

Compliance Pressure

Lack of Visibility



Invsense Advantage

Unified governance and control across all models and providers

Dynamic routing and token optimization cut costs by up to 60%

Multi-layered guardrails and DLP for AI interactions

Compliance assistance

Real-time observability, audit trails, and usage telemetry

Deploy Confidently with **Invinsense**

Invinsense LLM Gateway and AI Guardrails give your organization the visibility, control, and assurance needed to scale AI securely and cost-effectively. Whether you are building enterprise chatbots, AI copilots, or multi-agent systems

Invinsense ensures every interaction is



Secure



Compliant



Optimized

Start Your **Secure AI Journey Today**

Visit www.infopercept.com/invinsense-llm-gateway or schedule a demo call with our experts to see how Invinsense can govern and optimize your enterprise AI stack.

Click For **Demo**

Demo Call

