itbigtec 艾体宝 truefoundry

AI Gateway

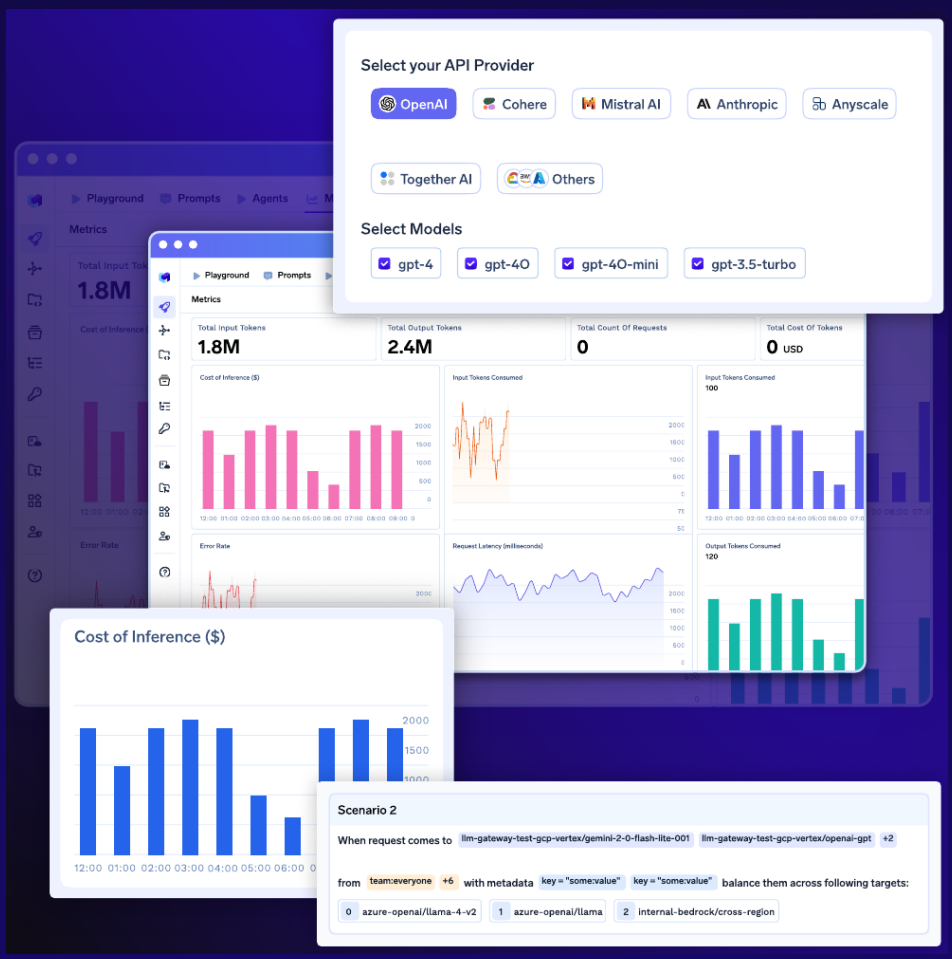
企业 AI 统一网关

一个控制平面，统一管理企业运行的
每一个模型、工具与智能体。

1T+
每日处理 Token 数

30%
成本节省

99.99%
可用性



产品界面截图保留原文

让 AI 的规模化应用，有统一治理可依。

至少 **60% 的 AI 智能体**将自主与外部系统交互，形成复杂的跨供应商成本网络。企业并未预料到这种无序扩张：API 密钥被硬编码在各处代码中，却没有明确负责人；团队因未设定支出上限，收到意料之外的模型账单；安全团队看得到风险，却缺少统一的策略执行入口。

每个团队连接工具和智能体的方式都不同。没有人能完整掌握哪些系统正在运行、花了多少钱，以及它们是否安全。

根本原因在于架构。缺少集中管理层，就无法在规模化应用中统一执行策略、观测流量或控制访问权限。

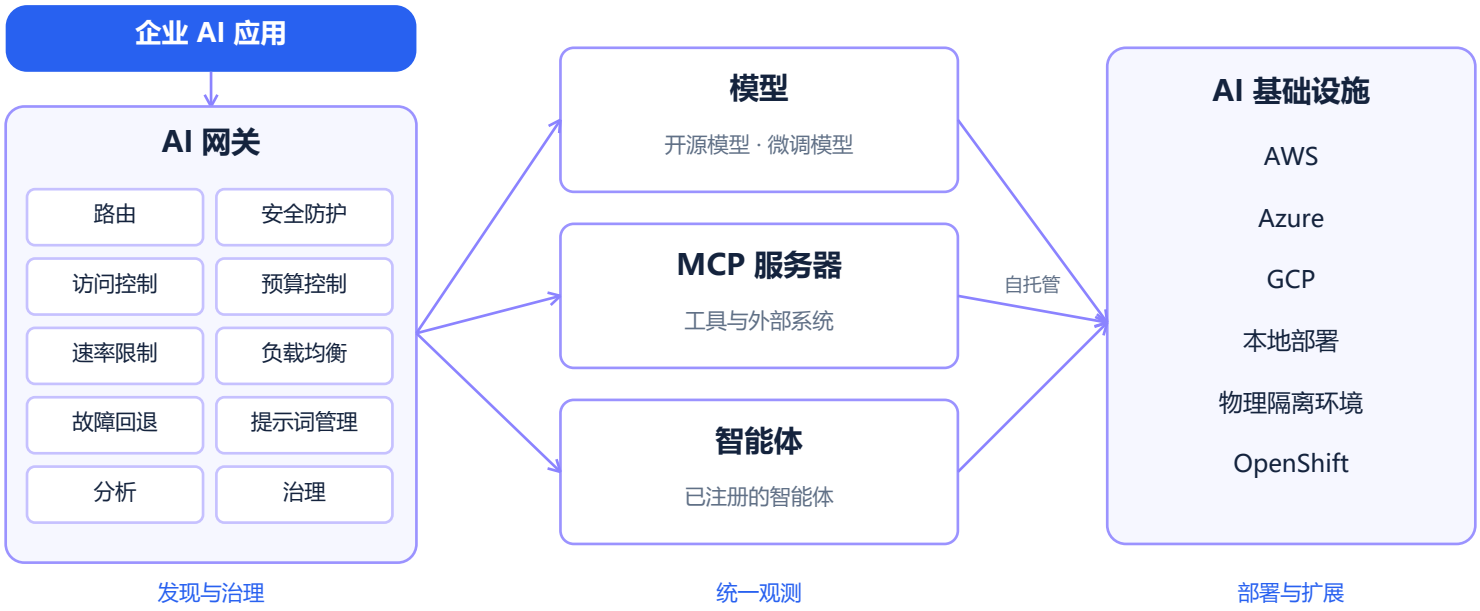
补齐 AI 技术栈缺失的基础设施层

TrueFoundry AI Gateway 是一个统一控制平面，连接组织内的所有 AI 使用方（用户、应用和智能体），以及它们需要访问的 AI 资源：大语言模型（LLM）、MCP 服务器和已注册的智能体。

控制平面与网关平面分离

控制平面供平台与安全团队使用，负责注册模型和工具、设置策略、配置安全防护，以及管理团队和预算。**网关平面**负责处理所有实时流量。两者完全独立，控制平面不处于请求的关键路径上。

即使控制平面不可用，网关仍可继续运行。配置会实时同步至每个网关实例。

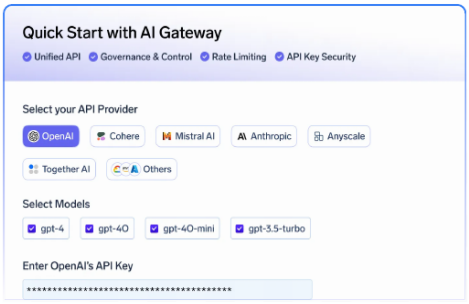


三类网关，一个平台

truefoundry

LLM 网关

为组织运行的所有模型，提供统一访问端点。



- 连接 1,600+ 个模型，覆盖 Bedrock、Azure OpenAI、Anthropic Direct、Vertex、Gemini 及自托管端点。无需更换 SDK，也无需重写代码。
- 按权重、优先级或延迟智能路由；可为每个目标配置参数覆盖与故障回退行为。
- 实时追踪成本，支持按企业协商价格核算，而非按公开标价估算。

MCP 网关

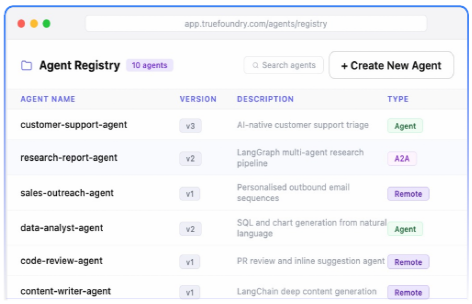
对智能体可调用的每一项工具，实施访问治理。



- 网关统一处理出站认证（OAuth、API 密钥、令牌透传），每个应用只需使用一个令牌完成入站认证。
- 虚拟 MCP 可将多个 MCP 服务器中精选的工具组合成一个命名端点，并为其配置独立的访问控制。
- 连接官方外部 MCP 及任意远程 MCP。直接托管于网关，无需额外基础设施。

智能体网关

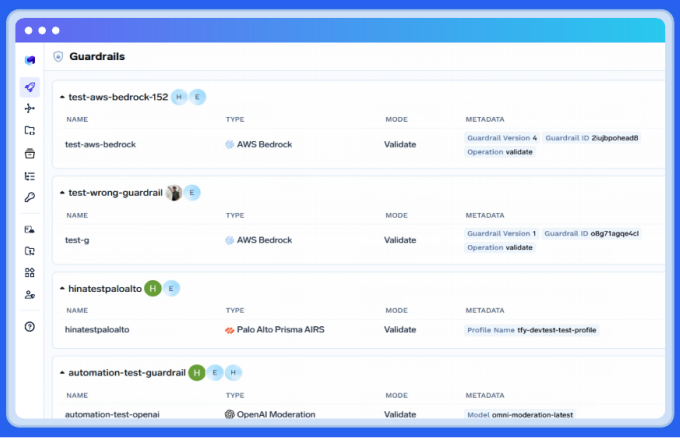
像管理模型和工具一样，注册、开放和治理智能体。



产品界面截图保留原文

- 通过集中式智能体注册中心，实现基于角色的访问控制（RBAC），并对各类框架提供全面监控。
- 同时支持兼容 A2A 的智能体与自定义智能体。
- 端到端追踪每次智能体调用，以及由此触发的模型调用和工具调用。

企业级治理，融入每一次请求



安全防护
内置敏感凭据检测、个人身份信息（PII）与受保护健康信息（PHI）脱敏、SQL 净化和代码安全防护。

访问控制与身份管理
通过 OIDC 或 SAML 实现单点登录（SSO），支持 SCIM 自动配置用户。

速率限制与预算控制
按用户或团队，基于请求数或 Token 数设置速率限制。

可观测性
为每次 LLM 调用、MCP 调用和安全防护评估提供完整的瀑布式链路追踪。

关于艾体宝 & TrueFoundry

truefoundry

广州艾体宝科技有限公司（ITBIGTEC）是一家聚焦数据与 AI 基础设施、AI 平台与应用治理、安全与合规的创新技术产品与解决方案服务商。携手全球优秀技术厂商，为企业提供涵盖数据库与数据平台、AI 开发与治理、数据分析与智能决策、软件供应链安全、数字产品安全及企业风险治理等领域的专业技术产品与服务。

TrueFoundry 由 Nikunj Bajaj、Anuraag Gutgutia 和 Abhishek Choudhary 于 2021 年创立，旨在构建“由 AI 管理 AI”的平台，打造一个能够自主运行、自我维持、持续演进并实时优化的生态系统。

如今，TrueFoundry 总部位于旧金山，与全球领先企业及《财富》 50 强企业合作，帮助它们管理、治理并扩展业务关键型 AI 应用。

获得领先分析机构认可

Gartner

26+ 次报告收录
涵盖 AI 网关与生成式 AI 工程

Frost & Sullivan

HFS Research
Everest Group · Avasant

IDC

2024 年 IDC 创新者厂商
获评生成式 AI 领域创新者

深受领先企业信赖

RIOT GAMES · baloise · #loQast · CVS pharmacy · WNS · Payoneer · Pfizer · MARS · AUTOMATION ANYWHERE

“TrueFoundry 的 AI Gateway 已成为我们的统一管控层，让 AI 应用既安全又可治理。开发者获得跨云、跨模型的一致接口，管理层则获得治理能力与可预测性。它显著减少了企业 AI 规模化应用过程中的阻力。”



Nilav Ghosh
Innovaccer 人工智能高级总监

面向企业，为真实业务中的规模化 AI 而构建

在任意环境中部署 TrueFoundry
在 VPC、本地或物理隔离环境中运行，全面掌握数据主权。

自托管模型服务
部署 LLaMA、Mistral、Falcon 等开源模型，无需更换 SDK。