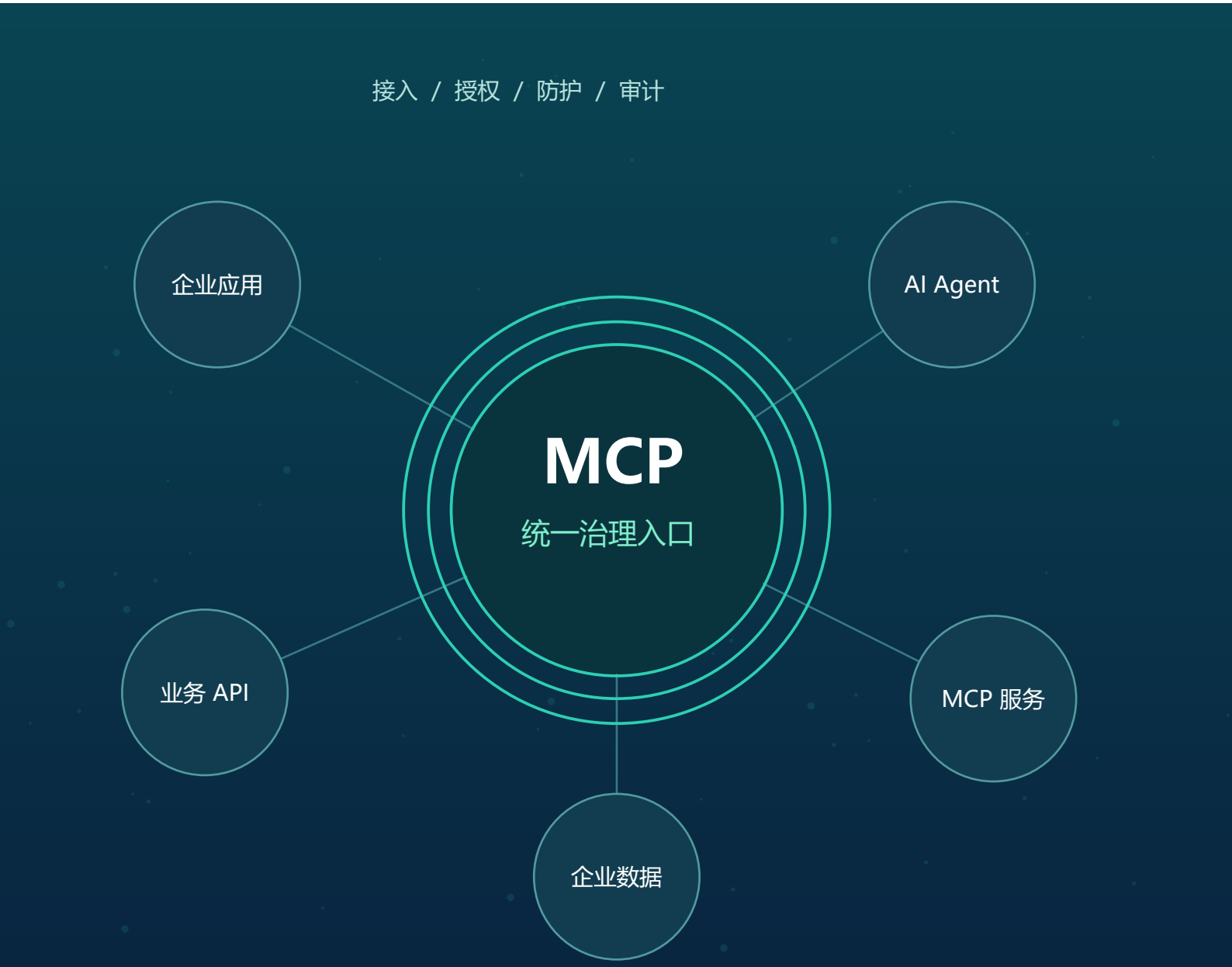


艾体宝 TrueFoundry

企业 MCP 网关

产品介绍

统一连接 AI 应用与企业工具，集中管理访问和调用

中文版 | 2026.09

01 产品概览

让企业工具接入 AI 更易管理

TrueFoundry MCP Gateway 连接 AI 应用与企业工具，集中管理接入、身份、策略和调用记录。

当多个团队分别接入业务 API、SaaS 服务和内部工具时，连接配置、凭据与权限容易分散在不同应用中。MCP 网关提供统一管理入口，让企业复用已有系统，并逐步扩大 AI 工具的使用范围。



01 统一接入

将已有 API 和不同来源的 MCP 服务纳入目录，减少各应用重复配置连接的工作。

02 明确访问边界

按用户、团队或应用身份授予访问权限，并通过 Virtual MCP 提供适合各应用的工具集合。

03 保留调用依据

关联工具调用、策略执行与异常记录，支持排障、审计与持续管理。

02 接入与工具管理

复用已有接口，组织可用工具

从少量接口开始接入，再按应用需要扩展工具目录和访问入口。

已有 API 转为 MCP

导入 OpenAPI 3.0 / 3.1 规范，将接口名称、说明和参数映射为 MCP 工具，业务逻辑仍由原有 API 执行。

接入远程 MCP 服务

登记企业自建或公共 MCP 服务，配置后端地址与认证方式，集中查看服务和工具信息。

托管运行 MCP 服务

对于需要托管运行的 MCP 服务，可结合平台托管能力部署和管理，运行环境按接入方式选择。

组合 Virtual MCP

从一个或多个 MCP 服务挑选工具，形成应用专用入口，结合访问授权定义使用范围。

一次接入，持续管理

从接口准备到应用调用，逐步建立可复用的工具接入流程。

1. **注册** — 确认接口与认证
2. **筛选** — 选择开放的工具
3. **授权** — 分配用户或应用
4. **调用** — 接入客户端或助手

接入前应准备接口规范、认证方式，并确认网关能够访问后端。

03 身份与访问控制

把调用者与后端凭据分别管好

在统一入口验证谁在调用，再决定可访问哪些服务与工具。



入站身份与出站凭据可以独立配置，适配不同的企业应用入口。

按使用方式选择身份

个人用户	通过个人 Token 或受支持的身份集成调用。	按个人权限访问，保留调用主体。
团队	为一组成员配置共同的访问权限。	统一授权，同时保留成员身份。
虚拟账户	为应用或后台服务配置专用身份与 Token。	按应用管理权限、策略和记录。

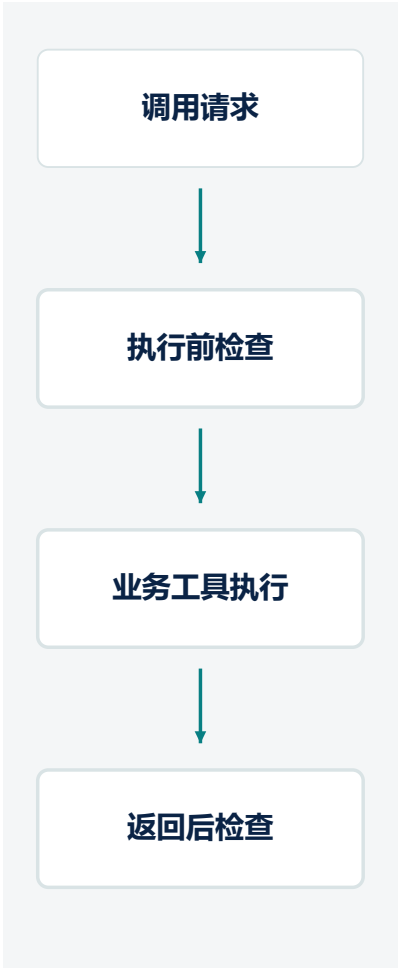
延续业务系统的数据权限

若业务系统要求按员工区分可见数据，可结合个人凭据、OAuth 或可信身份传递，由后端执行数据授权。多人共用一个虚拟账户时，网关默认识别的是同一个应用主体。

04 安全与可观测性

在工具执行前后设置检查

将敏感内容处理、人工审批、调用追踪与策略配置纳入统一治理。



敏感内容检查与处理

按需选择正则、PII、Secrets Detection 或自定义护栏，检查工具参数和返回结果，并对命中内容阻断或替换。

指定工具人工审批

对需要人工确认的工具设置审批。Once 模式批准一次执行，调用方在批准后重新发起调用。

调用轨迹与使用统计

查看调用主体、工具、时延、结果与护栏记录，结合汇总指标定位异常和追踪使用情况。

按目标绑定策略

按模型、MCP 服务及调用主体等条件匹配策略，选择输入、输出或工具执行前后的检查位置。

区分输入保护与日志保护

输入脱敏处理发往模型或工具的内容，日志脱敏处理保存的副本。工具执行后的检查不能撤销已经产生的业务操作。

按数据流向选择检测方式

正则与 Secrets Detection 可在网关内运行；其他检测集成可能调用外部服务。可按识别范围、处理位置及检查失败时的行为选择合适的护栏。

05 企业应用场景

把治理能力嵌入现有工作入口

围绕企业已有应用和业务接口，逐步引入工具调用与访问治理。



内部知识与信息检索

连接文档、知识库和业务查询工具，为员工提供统一访问入口。

配置重点：员工身份、工具访问范围、返回内容处理。



企业 IT 与运维助手

将自动化脚本或平台 API 封装为工具，供内部助手查询资源与辅助运维。

配置重点：个人凭据、操作权限、敏感工具审批和追踪。



业务数据查询与分析

复用业务 API，支持查询指标、获取记录和组合多个系统的信息。

配置重点：接口认证、参数检查、原系统数据权限。



需人工确认的业务操作

对创建、变更或推送类工具设置审批，将人工确认纳入工具调用流程。

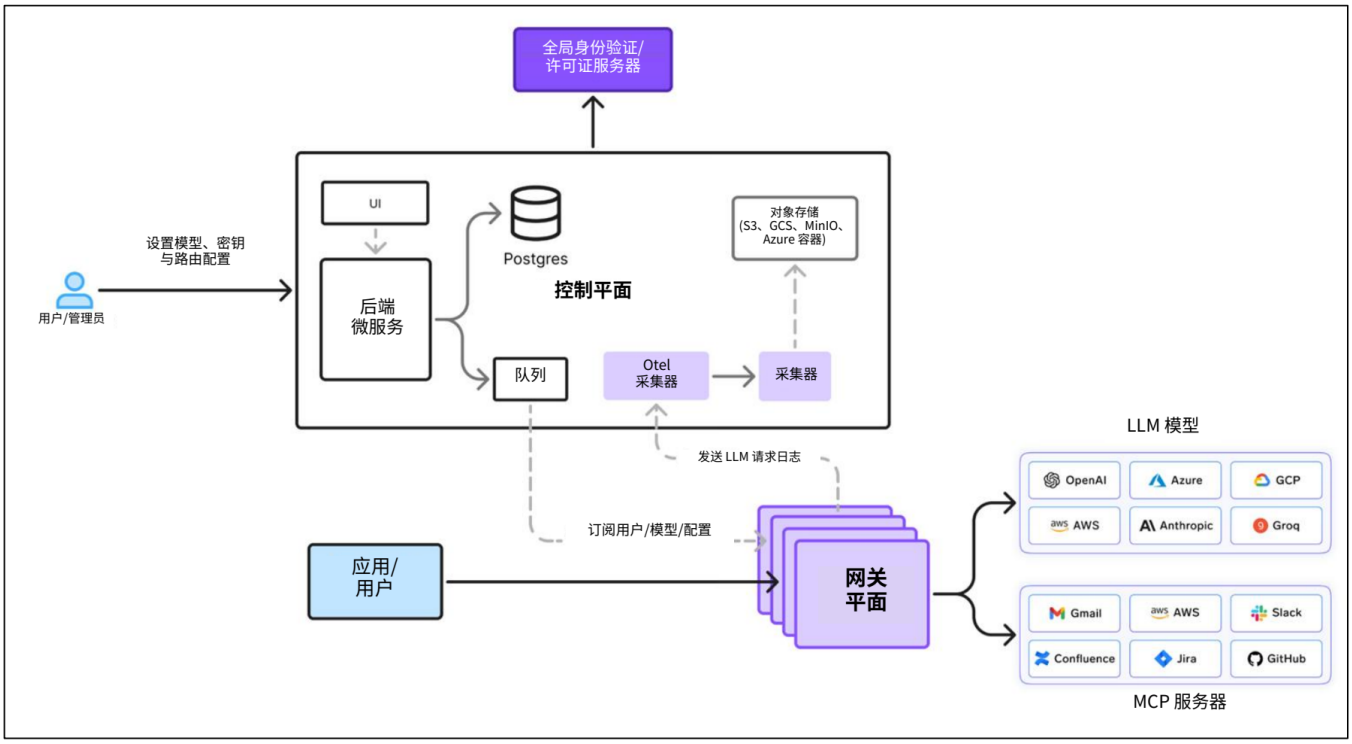
配置重点：审批范围、调用状态处理、后端操作幂等。

企业可保留自己的应用界面与业务系统，由 MCP 网关提供共用的接入和治理能力。

06 架构与部署

按企业环境规划控制面与网关

平台采用分离式架构，将配置管理与请求处理分开，支持托管和企业自有环境部署。



网关连接应用、模型与 MCP 服务，并提供统一治理能力。

托管接入

使用托管控制面与网关，连接可访问的模型和工具服务，快速开始接入与治理评估。

企业自有环境

按部署方案将网关部署至自有云或本地环境，规划控制面与日志存储位置。

与模型网关协同

结合 Model Gateway 管理模型供应商凭据、访问、路由与用量，将模型和 MCP 工具调用统一纳入治理。部署时一并规划认证、护栏与日志的数据流向。

07 客户案例

NetApp

统一内部助手的工具入口，连接员工身份与企业基础设施。

约 150 个

工具汇聚到统一虚拟入口

数千名员工

可通过内部应用访问工具

业务需求

NetApp 的开发者平台工程团队希望员工以自然语言调用 Kubernetes 自动化能力，并在扩展 Agent 使用时保留身份和权限控制。

实施方式

01 自建 MCP 服务，连接集群运维与底层基础设施。

02 通过单一 Virtual MCP Server 汇聚多个 MCP 服务，内部助手 NetAI Chat 使用统一端点访问工具。

03 将用户身份经网关传递到自有 MCP 服务，关联个人集群账号及短期凭据。

应用价值

员工沿用内部应用入口，工具能力可被不同 Agent 复用；企业在网关与自有工具层之间形成一致的身份和访问治理。

08 客户案例

FloQast

让财务工具调用与模型推理共享治理和可观测能力。

约 13.9 万次

MCP 工具调用

财务数据 · 业务规则
表格 · 会计分录

业务需求

FloQast 为财务与会计团队提供结账、对账和合规平台。随着 AI 功能接入业务数据和工具，公司需要统一管理模型与 MCP 调用，并满足访问治理和区域数据管理要求。

实施方式

01 采用 TrueFoundry AI Gateway 管理模型推理、MCP 服务及相关治理能力。

02 将读取财务数据、检索规则、获取表格和会计分录处理纳入受治理的工具调用入口。

03 结合区域化网关，将提示词与调用轨迹存储在客户自有基础设施内，并保持集中可观测性。

应用价值

在扩展财务 AI 功能的同时，统一查看模型和工具调用、实施访问管理，并按部署要求规划提示词与追踪数据的保存位置。