

让 AI 成为 组织的一员

有岗位，有权限，有审计记录，可指定负责人。
可被分配，可被冻结，也可被回收。

FusionAI 是企业级数字员工平台。它把大模型从「会聊天的工具」，变成能进入企业已接入业务链路的组织成员。

治理在架构
不在提示词

9

态生命周期

4

道治理关卡

3

级工具风险

01 产品定位

企业不缺一个更聪明的聊天框。企业缺的是一个敢把事交给它的理由。

能演示，不等于能上线。
问题不在模型，在治理。

过去三年，几乎每个部门都试过让大模型干活。写文案、查资料、做表格，演示效果都不错。但一旦要它进入合同、财务、客户数据、生产系统，项目就停住了。

失败的原因不是模型不够聪明，而是个人 AI 工具天生缺少进入企业核心业务链路的三样东西：它不知道自己是谁，不知道自己能碰到什么，也不知道自己做过什么。

一个无法被授权、无法被追究、无法被收回的「员工」，企业不敢把真正重要的事交给它。

BARRIER 01

可信

它做错了，我能拦住吗？

提示词里的「不要做危险操作」，在审计室门口站不住。边界必须写进架构：沙箱硬隔离、工具风险分级、高危动作中断。

BARRIER 02

可控

谁，在什么时候，用哪个数字员工，读了哪些数据，调了哪些工具？

权限必须可授予、可回收；每一次访问必须留痕；人离职、员工下线，权限要能真正收回，而不是留在库里。

BARRIER 03

可复用

能力能不能从个人手艺，变成组织资产？

谁能创建、谁能发布、谁能分配、谁能回收，每一步都要有明确的责任主体。否则三十个 Agent 里，二十个在重复造轮子。

■ WHAT FUSIONAI IS

FusionAI 是面向企业的数字员工平台。

面向企业私有化部署。数字员工不是「更强的大模型应用」，而是有岗位身份、权限边界、审计记录，可指定负责人、可被冻结和回收的组织成员。它站的位置是：既能像助手一样把任务做完，又能像企业系统一样被授权、被管控、被追究。

FUSIONAI

01 治理在架构，不在提示词

检索、执行、审批、记账四道关卡，全部是服务端的确定性判断。提示词可以绕过、可以诱导、可以随时间腐化；代码里绕不过去的那一段，才能向审计师交代。

03 共享定义，隔离实例

同一个岗位能力可以分配给多人；共享的是能力定义，隔离的是会话、记忆、权限与审计。个人创建资产不能反向扩权。

02 判断权在服务端

能访问哪些知识库、能绑定哪些高危工具、审批卡上写什么，都由服务端依据会话上下文判定，不由调用方在参数里自报身份。

04 过程透明，随时可干预

对话不是黑箱，是任务驾驶舱。用户能看到它在做什么、用了什么、走到第几步，也能在计划、审批、执行中途随时介入。

02 产品特性

四个能力域、十六个模块，围绕同一个目标：让数字员工能干活，也让企业管得住。

■ CAPABILITY MAP

四个能力域，十六个模块

从组织治理到业务写回，FusionAI 把数字员工所需的能力拆成可独立配置、可独立授权的模块。先看全景，再看十三项核心能力。

组织与治理

GOVERN

数字员工

八维配置 · 九态生命周期

权限与审批

租户 / 组织 / 角色 · 审批策略

沙箱与安全

文件 / 网络 / 超时约束 · 出网白名单

审计、用量与可观测

操作审计 · Token 用量归因 · 调用记录

工作与执行

EXECUTE

员工工作台

数字员工轨 · 待办 / 审批

任务驾驶舱

实时轨迹 · 人工介入

工作空间

文件 / 邮箱 / SSH / FTP

工作流

画布编排 · 定时 / API

知识与能力

KNOW & ACT

知识中心

多模态 RAG · 双门控

工具与 MCP

三类工具 · 三级风险

技能中心

技能包 · 跨员工复用

数据集

语义构建 · 自然语言问数

业务融合

本体反推 · 动作编译

平台与接入

PLATFORM

模型接入

多提供商 · 本地模型

平台管理

用户 / 角色 / 组织 / 租户 / 菜单

部署与授权

私有化 · 授权签名

01

数字员工

有生命周期的组织成员

把模型、提示词、技能、沙箱、记忆与子智能体装配成一个可对话执行、可发布、可分配、可回收的岗位。

- 八维配置：模型、系统提示词、对话、技能包、沙箱策略、归属、子智能体、编排形态
- 九态生命周期与四态运行态正交；状态流转是白名单，不在表里的边一律拒绝
- 十四类内置岗位模板，四种执行模式：单任务 / 单对话 / 多任务 / 多对话
- 发布必须指定审批人，支持或签；分配覆盖用户、角色、组织节点；退役回收全部有效分配

8 维配置

9 态生命周期

三级分配

发布审批

02

员工工作台

选人、干活、处理待办

员工侧的统一入口。数字员工按分配出现在工作台，待办与待审批聚合在一处；任务与审批不散落在多个系统。

- 数字员工轨：只展示已分配且处于可用状态的岗位
- 发布审批详情：指定审批人、或签、审批留痕
- 待办抽屉与审批铃铛：跨会话聚合待处理事项
- 个人资料、通知设置、意见反馈与租户切换

数字员工轨

待办聚合

审批铃铛

发布审批

03

任务驾驶舱

对话是手段，任务才是主体

对话页不是「聊天窗口 + 回复文本」，而是一次任务的完整执行过程。思考、工具、计划与人工介入在同一条时间线上。

- SSE 实时轨迹：思考过程、工具调用卡、执行清单、执行计划卡、执行统计
- 可随时停止；审批等待默认 6 小时，超时按策略拒绝或升级
- 资源面板：任务、资源、工具、技能、业务系统、知识库，组织结构按宿主出现
- 人工介入三件套：审批卡、追问卡、跨人审批；等待期间输入自动锁定
- 主链路中断状态外置 Redis，服务重启后仍可续跑（单 worker 部署）

SSE 全事件流

审批 / 追问 / 跨人

断点续跑

04

工作空间

文件、邮箱、SSH、FTP 在同一个上下文里

与当前会话绑定的资源面板。模型不需要猜路径，用户用 @ 直接引用文件、目录或邮件；沙箱文件、共享目录、邮箱与主机都在同一处。

- 页签：任务、资源、工具、技能、业务系统、知识库；
工具 / 技能 / 业务系统为只读视图
- 沙箱文件系统：上传、新建目录、重命名、删除
- FTP / SFTP 共享目录、邮箱收发 / 草稿 / 附件、SSH 直连 / 跳板机 / Web 终端
- @ 引用文件、目录、邮件，资源由面板注入，不让模型猜路径



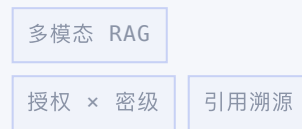
05

知识中心

能被授权、能被追溯的知识

文档、图片、视频、音频统一入库，检索与问答带引用溯源。敏感知识不是「建议不要看」，而是检索结果在交给模型之前就被门控拦下。

- 多模态统一入库，十种分块策略，五阶段进度可视化，失败可查
- 授权 × 密级双重门控，独立于模型之外执行；两者取交集
- 引用溯源、命中测试、近义词库与检索配置
- 撤销授权即时生效，后续检索不再命中；授权变更留痕



06

工具与 MCP

风险分级的能力生态

工具是数字员工的手，也是最需要管住的地方。内置、自定义、MCP 三类工具统一编目，按只读、写入、高危分级，高危绑定走独立闸门。

- 工具目录自动对账；工具统计与代码安全扫描
- 自定义工具全流程：Schema、源码、依赖、沙箱测试、校验
- MCP 服务器管理、连接测试、工具自动发现与刷新、批量注册、分组管理
- 风险等级决定能不能用，审批策略决定用的时候要不要问人



07

技能中心

把经验封装成可复用资产

把「专业提示词 + 作业脚本 + 参考资料」打包成技能包。个人经验不再停留在某个人手里，而是成为可发布、可归档、可跨员工共享的能力单元。

- 上传、URL 导入、在线编辑器与沙箱测试
- 发布、归档、分类与标签；跨数字员工绑定
- 绑定关系有删除保护，避免在线员工能力被误删
- 平台内置演示文稿技能，开箱可用，可绑定给数字员工

技能包

沙箱测试

跨员工复用

08

工作流

确定性流程的画布

数字员工擅长对话式任务，工作流擅长固定流程。画布式编排把「采集、过滤、摘要、成文、发送」这类确定性工作固化下来，可调试、可版本化、可回滚。

- 可视化画布，十余类节点，变量引用与自动补全，迭代容器
- 三层校验、草稿调试、节点级实时状态
- 版本管理与回滚、执行监控、执行恢复、死信队列
- 定时调度与对外 API：API Key、限流、同步 / 异步

画布编排

版本回滚

定时 / API

09

数据集

让数字员工能问数

业务人员不必会写 SQL。数据源接入后完成语义构建，注册为工具，数字员工即可用自然语言取数、分析并生成图表，SQL 与命中数据集可核查。

- 六类数据源：MySQL、PostgreSQL、SQL Server、Oracle、ClickHouse、Doris
- 三步向导接入，多表批量导入
- 语义构建、字段语义编辑、关系发现与拓扑
- 五维可见性与权限合并预览；数据集组统一管理
- 五类脱敏（全脱敏 / 部分 / 哈希 / 范围 / 泛化）与 AI 推荐；脱敏在数据出库前生效

六类数据源

语义构建

字段级脱敏

业务融合

让数字员工进入业务系统

不只是查数，还要能办事。从业务系统里反向梳理实体、属性、关系、动作与规则，编译成数字员工可调用的工具，并把动作写回已接入的业务系统。

- 七类反推源：OpenAPI、数据库、源码、JAR 字节码、文档、MCP、人工声明
- 证据分级放行：直读自动通过、推断待确认、矛盾阻断；可人工裁决
- 本体七要素：实体、属性、动作、规则、状态机、关系、事件
- 系统级 / 动作级 / 浏览器授权；能力必须显式授权给数字员工或用户

本体反推

动作编译

业务写回

治理与安全

四道绕不过去的关卡

租户、组织、角色、权限点、审批策略、沙箱、审计与用量归因，构成企业治理基座。安全不是配置页上的选项，而是数据流与执行流上的硬约束。

- 多租户；租户级数字员工 / 工作流数量上限；三层组织架构；自定义角色与权限点
- 审批策略：自动 / 必须 / 条件；审批人可为用户或角色；超时拒绝 / 自动通过 / 升级
- 沙箱策略：文件权限、出站网络、执行超时，只能收紧；一次性容器；操作审计与 Token 用量归因
- 数据范围支持租户级 / 组织级；更细档位未开放时按拒绝处理
- 检索关卡、执行关卡、审批关卡、记账关卡；收紧可自助，放宽需审批

审批策略

四道关卡

沙箱收紧

用量归因

模型接入

不绑定单一厂商

云端模型与本地模型统一接入，按能力标签决定处理路径；密钥加密存储、日志脱敏、界面不回填。

- 多提供商：OpenAI、DeepSeek、文心、星火、GLM，兼容 Azure / Moonshot / MiniMax
- 本地模型：通过兼容协议接入私有化模型服务
- 能力标签：对话、视觉、原生音频、向量、排序、语音识别、推理
- 连通性测试、模型清单拉取、API Key 加密与脱敏

多提供商

本地模型

能力标签

密钥加密

监控与可观测

知道系统在忙什么、消耗在哪

围绕模型调用与平台操作，把 Token 消耗、调用归因与关键操作记录集中呈现。

- Token 监控：总消耗、调用次数、用量趋势、按模型 / 业务模块分布
- 用量报表：Token 按用户 / 数字员工归因，支持 24 小时 / 7 天 / 30 天窗口
- 最近调用记录：时间、模块、供应商、租户、模型与输入 / 输出 Token
- 操作审计：数字员工、权限与系统配置等关键操作留痕，可按条件追溯

Token 监控

用量报表

调用记录

操作审计

03 两种生产力

WorkBuddy 企业版把 AI 铺进团队协作；FusionAI 把 AI 接进核心业务链路。两者都做数字员工，但治理对象不同：一个治理「人与 Agent 的协作」，一个治理「Agent 对业务系统的写操作」。

REFERENCE · ENTERPRISE

WorkBuddy 企业版

企业级 AI 智能体平台 · 从超级个体到超级团队

以 7×24 数字员工、SINGLE / SQUAD 多 Agent 协作、项目制人机协同和企业管理后台为核心；深度连接企业微信、腾讯文档、网盘与乐享。强在办公协同、技能生态与团队规模化使用。

FUSIONAI

FusionAI

企业级数字员工平台 · 从岗位到业务链路

以业务本体、实体动作编译、工具风险分级和九态治理为核心；能力经授权、执行有边界、过程可审计、成本可归因。强在核心业务系统的受控执行与写回。

WorkBuddy 企业版的强项

- ◇ **办公生态**：企业微信、腾讯文档、腾讯网盘、腾讯乐享，覆盖日常协作。
- ◇ **多 Agent**：SINGLE / SQUAD 两种模式，7×24 云端数字员工，异步并行。
- ◇ **技能规模**：SkillHub 7 万+ Skills、Connectors、CodeBuddy 开发者生态。
- ◇ **可观测**：可观测中心、会话追踪、Trace / Span / Token、评估测评。

FusionAI 的差异化

- ◇ **业务本体**：七类反向源取证，实体、属性、关系、动作与规则入本体；状态机与事件可人工补齐。
- ◇ **受控写回**：实体动作编译为工具，执行前校验权限与规则，写回已接入系统。
- ◇ **治理深度**：九态生命周期、三级分配、工具风险分级、跨人审批、运行时冻结。
- ◇ **私有化优先**：数据留在客户环境，文件 / 网络 / 超时沙箱、出网白名单、一次性容器。

维度

WorkBuddy 企业版

企业级 AI 智能体平台

FusionAI

企业数字员工平台

设计出发点	从超级个体到超级团队，推动 AI 原生组织进化	从岗位到业务链路，让数字员工进入受控执行
产品组合	CodeBuddy + WorkBuddy + Managed Agents + Agent Suite	管理端 + 员工工作台 + 运行时 + 业务融合引擎
数字员工	云端 7×24 常驻；SINGLE / SQUAD 两种调用模式	岗位化数字员工；九态生命周期、发布审批、三级分配
协作模式	项目制人机协同，共享上下文、Skills、MCP 资产	会话工作空间 + 任务 + 审批；按岗位分配能力
能力扩展	SkillHub 7 万+ Skills、Connectors、MCP、开放 API	内置/自定义工具、MCP、业务实体动作、数据集、浏览器 / SSH / 邮箱 / FTP
业务系统	连接 OA / CRM / 项目工具与内部系统，重心在办公协同与流程编排	七类反向源取证构建本体；实体动作编译为工具；执行前规则校验；写回已接入系统
知识与数据	企业知识库 + 腾讯文档 / 网盘 / 乐享 + 连接器；本地文件不上传	多模态知识中心；授权 × 密级双门控；引用溯源；撤权即时生效
高危动作	计划模式先确认；角色化工作流可编排审批；iOA 零信任 + PC 管家沙箱	三级工具风险；执行真实中断；审批卡 / 跨人审批；运行时冻结
执行隔离	本地安全沙箱保护终端；云端 Agent 独立沙箱、异步并行	文件 / 网络 / 超时三维沙箱、出网白名单、一次性容器
可观测与审计	可观测中心：Trace / Span / Token、会话追踪、评估测评、安全审计	操作审计；模型 Token 消耗归因到用户、数字员工与模型
部署与合规	SaaS 企业版、专享 VPC、私有化；信创适配	私有化优先；x86_64 / arm64 与信创适配；授权签名与硬件指纹；网络最小暴露
生态强项	企业微信、腾讯文档、腾讯网盘、腾讯乐享、CodeBuddy 开发者生态	业务系统融合、本体建模、受控写回、审批治理
最适合	团队办公协同、知识复用、编码与日常提效	合同、财务、客户、生产等核心链路的受控执行

**不是替代关系，
而是分工关系。**

WorkBuddy 企业版解决团队「协作效率」：把办公套件、企业微信、Skills 生态和多 Agent 协作铺到日常。FusionAI 解决核心业务「执行信任」：谁能用、能碰什么、写操作是否合规、出事能不能查、权限能不能收回。

一个企业可以同时拥有两者：日常协作交给 WorkBuddy 企业版，核心业务链路交给 FusionAI。真正进入合同、财务、客户数据与生产系统的写操作，需要的不是更强的提示词，而是可审计的边界。

04 整体功能架构

一张图看清 FusionAI 如何把「人、岗、权、事、数」装进同一条执行链路；能力层中的业务融合把业务系统变成可执行的本体。

入口层 ENTRY	员工工作台 管理控制台 对外 API / 定时任务
工作空间 WORKSPACE	任务驾驶舱 资源面板：文件 / 邮箱 / SSH / FTP 审批与追问 执行轨迹
运行时 RUNTIME	多智能体编排 任务规划 短期 / 长期记忆 子智能体 工具调用 HITL 中断 / 续跑
能力层 CAPABILITIES	知识中心 工具与 MCP 技能中心 工作流 数据集 业务融合：本体 / 动作 / 写回 模型与提示词
治理基座 GOVERNANCE	租户 / 组织 / 角色 权限点与数据权限 审批策略 沙箱（文件 / 网络 / 超时） Token 用量归因 操作审计
基础设施 INFRASTRUCTURE	配置数据库 / 向量数据库 Redis 对象存储 容器运行时 模型网关

业务融合不是连接器， 而是把业务系统变成可执行的本体。

连接器解决「能不能调通」，业务融合解决「能不能按业务规则办事」。它把既有系统里的实体、属性、关系、动作与规则还原出来，编译成数字员工可调用的工具，并把结果写回业务系统。

01 / 反向建模

从既有系统还原业务本体

七类反向源：OpenAPI、数据库、源码、JAR 字节码、文档、MCP、手工声明。各源能说的话不同：接口与参数多来自直读，规则、状态机与事件多数要人工确认或手写。



02 / 本体建模

七个要素，描述业务怎么运转

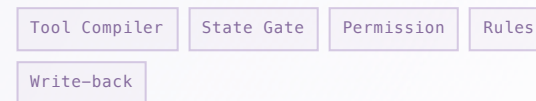
实体、属性、动作、规则、状态机、关系、事件。不是一张表清单，而是一套带证据等级的语义：直读的自动采信，推断的进待确认，矛盾证据阻断。



03 / 动作编译

把实体动作编译成 Agent 工具

EntityAction → Tool；写动作要求先配齐状态机（初始态 + 终态）；执行时校验权限点、前置规则与参数映射，再调用已接入系统完成写回。



没有业务融合

AI 只能查、只能聊，最后一步仍要人工录入，数字员工停在业务系统门口。

有了业务融合

AI 能在规则与权限约束下执行动作，把最后一步从人工录入变成受控写回。

一次任务，六道关

EXECUTION PATH

01

身份与租户

请求进入即确定租户、组织、角色与数据权限。

02

选人

只有「已发布」且已分配的数字员工，才会出现在工作台。

03

装配

知识按授权 × 密级过滤，工具按风险分级装配，业务实体动作按授权注入。

04

推理

多智能体编排、任务规划、记忆调用与子智能体分工。

05

执行

沙箱里跑代码，业务系统里做动作；写操作过权限与前置规则，高危动作按审批策略真实中断。

06

留痕

全链路审计，模型 Token 消耗归因到具体的用户、数字员工与模型。

前端控制台地图

CONSOLE SURFACE

工作台与执行

- 工作台首页 / 数字员工轨
- 待办抽屉 / 审批铃铛
- 发布审批详情
- 对话执行页 / 执行历史
- 数字员工创建 / 编辑 / 群组

业务融合

- 业务融合中心 / 业务系统详情
- 数据 / 接口 / 实体 / 主题
- 概念注册 / 绑定复核 / 关联规则
- 本体反推调查 / 结论确认台
- 用户映射 / 凭证 / 浏览器现场

知识与数据

- 知识库管理 / 文档详情
- 向量检索 / 命中测试 / RAG 对话
- 近义词库 / 知识图谱 / 状态机图
- 数据集 / 数据连接 / 关系拓扑
- 智能分析

平台管理

- 模型配置
- 用户 / 角色 / 组织 / 租户 / 菜单
- 授权管理 / 第三方集成 / 审计日志
- 邮件配置 / 邮件模板 / API Key

能力编排

- 工具仓库 / 工具编辑 / 工具统计
- 审批策略
- 技能市场 / 技能编辑
- 工作流画布 / 执行监控 / 版本历史
- 定时调度 / 会话管理

监控与个人

- Token 监控 / 用量报表
- 个人资料 / 通知设置
- 意见反馈 / 登录与租户切换

S1

企业知识问答与合规检索

知识中心

授权 × 密级

■ 痛点

企业知识散落在各个系统，员工查资料靠问人；敏感文档又不能对所有人开放。

■ 方案

制度、手册、合同模板、技术文档统一入库，按组织与岗位授权、按敏感度设密级。回答自动标注引用来源，逐条可回溯。

■ 价值

查资料从「问人」变成「问数字员工 + 看引用」；敏感信息的可见范围由系统保证，而非靠自觉。

S2

合同与文档审核

技能中心

审批中断

■ 痛点

合同审核依赖资深法务，产能有限，审核标准难以统一。

■ 方案

用技能封装企业审核要点与话术，绑定给合同审核数字员工。逐条比对后输出意见与风险点；「修改合同文件」这类写操作强制人工确认。

■ 价值

审核标准被固化进技能包，可复用、可版本管理；高风险动作由审批卡兜底。

S3

业务问数与经营分析

数据集

字段级脱敏

■ 痛点

业务人员不会写 SQL，取数需求排队等待数据团队，经营分析滞后。

■ 方案

数据源接入并构建语义，注册为工具。业务人员自然语言提问，数字员工选择数据集、生成 SQL、返回表格与图表，并展示思考过程。

■ 价值

取数自助化；SQL 与命中数据集可核查，不是黑箱；脱敏在数据出库前生效。

S4

数据录入与业务写回

业务融合

动作编译

■ 痛点

大量重复录入、状态变更、跨系统同步占用人力；让 AI 直接操作业务系统又担心越权与误写。

■ 方案

从 OpenAPI、数据库、源码与文档反推业务本体，把实体动作编译成工具，显式分配给数字员工。写入前校验权限与前置规则，高危动作按审批策略中断；写动作要求先配齐状态机。

■ 价值

数字员工从「会查」走到「会办」；每一次写回都过权限与规则校验。

S5

定时情报与周期性报告

工作流

定时调度

■ 痛点

竞品动态、行业资讯、周报月报等周期性工作占用大量人力，且容易遗漏。

■ 方案

用工作流编排「采集、过滤、摘要、成文、发送」的固定流程，配置定时调度；也可为数字员工配置定时任务，产物沉淀到工作空间。

■ 价值

周期性工作自动化，流程可见、可版本管理、可回滚，失败可恢复。

S6

IT 运维与终端操作

SSH

沙箱

■ 痛点

运维操作需要登录跳板机、执行命令，过程难以留痕，权限边界依赖个人习惯。

■ 方案

把 SSH 主机作为工作空间资源纳入，按空间与凭据授权访问；直连或经跳板机操作，终端在会话内打开。

■ 价值

运维入口从个人终端收回到平台，谁能碰哪台主机由资源分配决定。

06 交付与部署

私有化不是「可选方案」，而是企业核心业务的默认前提。

数据不出企业，
边界不靠自觉。

私有化部署 单机容器化交付，数据库、缓存、向量库、后端、AI 服务、前端与沙箱统一编排，数据留在企业侧。	x86_64 / arm64 同时支持主流服务器架构，适配企业既有基础设施。	网络最小暴露 仅开放必要端口，出网走白名单，减少攻击面。
授权与指纹 授权签名与硬件指纹绑定，启动闸门校验，定时复核。	交付完整性 交付包完整性校验，部署脚本与验证脚本配套。	

从一个岗位开始

ADOPTION PATH

Phase 01

试点

选一个高频、边界清晰的岗位，例如知识问答或合同审核。用真实资料与真实审批流跑通一个可验收的任务闭环。

Phase 02

扩展

把验证过的技能、工具与工作流沉淀为组织资产，接入业务系统与数据集，扩展到相邻岗位。

Phase 03

规模化

建立发布审批、分配、审计与用量归因的运营流程，让数字员工像真实岗位一样被管理、评估与回收。

先交付一个可审计的数字员工， 再谈组织级规模化。

不需要一次性重构所有系统。从一个岗位、一条业务链路、一个可验收的产物开始，让治理能力随业务一起长出来。

预约产品演示 · 请联系 FusionAI 项目团队

手机号 **15862457629**

微信号 **15862457629**



产品介绍 · v3.0

2026 年 10 月

本册所述产品能力以实际交付版本及项目配置为准。WorkBuddy 企业版相关信息来自其公开资料（截至 2026 年 10 月），仅用于产品定位对照，不构成对其当前或未来版本的完整描述。文中数据为产品能力参数，不构成性能承诺。