

出版说明

竹势 AI 营销智库出品

本报告面向企业经营层与采购治理团队，讨论 AI 营销产品和服务的采购对象、组合方式、成本、控制面、合同责任、验证方法与退出机制。报告中的“产品层级”是决策分类，不代表厂商只能处于单一层级；同一供应商可能同时提供模型、平台、应用、实施和托管服务，企业仍应逐项拆分责任。

法规部分仅说明与企业采购设计直接相关的适用边界。企业内部研发和应用生成式人工智能、未向境内公众提供服务时，不当然适用《生成式人工智能服务管理暂行办法》的全部提供者义务；但个人信息、数据安全、网络数据处理、内容发布、行业监管与合同义务仍可能适用。具体项目应由法务、数据保护、网络安全与业务负责人结合场景判断。

报告中的结果数字均保留主体、时间、对象、指标与披露口径。供应商客户案例标注“供应商自报”，不将其视为独立因果证据；未披露经营结果的案例明确写为“未披露”。

版权：竹势 AI 营销智库。允许在注明出处的前提下合理引用；不得篡改关键边界或将定性判断改写为厂商排名。

执行摘要：先确定责任，再选择产品

竹势 AI 营销智库出品

BOARD DECISION / 核心判断

先确定企业愿意承担什么责任，再决定购买模型、SaaS、Agent、营销 OS、实施服务或私有部署。

责任先于产品

真实任务验证

退出机制前置

企业 AI 营销采购的首要错误，是把名称当作能力边界。市场上“平台、Agent、OS、私有化”高度趋同，但供应商实际交付可能分别止于模型 API、一个任务应用、 workflow 编排器、统一经营系统、项目人力或基础设施托管。名称不能回答谁对数据接入负责、谁拥有任务状态、谁能停止动作、谁承担上线后的运营、谁证明经营结果，也不能回答合同终止后数据、workflow 和模型路由能否迁出。

本报告建议董事会采用“任务—能力—控制面—交付责任”四步法。先定义真实任务与经营基线，再判断所需能力；随后确定控制面归属，包括身份、数据、任务状态、工具调用、审核、日志、成本、版本和退出；最后把责任写入 RFP、验收和合同。产品组合应遵循最少必要层级：能用通用模型完成的低风险认知任务，不采购重平台；能用成熟单点 SaaS 形成闭环的任务，不自建通用 Agent 平台；跨系统、长周期、有状态、有高风险动作的流程，才需要平台或 OS；流程不清、组织权责不清、数据不可用时，先购买诊断与实施能力。

十个核心结论

- 名称不构成责任。“Agent”“OS”“私有化”只有在合同中对应身份、状态、权限、日志、变更、运维和退出责任时才有采购意义。
- 模型是可替换底座，不是营销系统。模型提供认知与生成能力，但不天然拥有企业目标、业务状态、品牌规则、渠道权限和结果归因。
- 单点 SaaS 的优势是快速任务价值。成熟的任务界面、行业数据和平台连接可缩短上线时间；代价是账号、数据、指标与审批分散。

4. Agent 平台的核心不是“自主”，而是控制。企业级平台必须支持状态持久化、最小权限、人工接管、可观察性、预算限制、停止与回滚。
5. 营销 OS 必须拥有经营闭环。只有把目标、任务、数据、资产、协同、审批、复盘和知识沉淀连成持续运行系统，才超出工具门户。
6. 咨询实施购买的是变化能力。诊断、流程重构、数据准备、角色设计、采用推动和收益实现不能被软件许可证替代。
7. 私有部署是一种责任转移。它可能改善数据驻留与定制控制，却把容量、补丁、模型升级、监控、灾备和安全运营责任转给企业或托管方。
8. TCO 必须按七项账本计算。订阅与模型调用通常只是显性成本；数据、集成、审核、运维、迁移和风险决定长期经济性。
9. ROI 自报只能进入假设池。厂商案例可帮助形成待验证场景，但采购决策应以企业真实任务集、基线、对照和经营五账本为准。
10. 退出权应在上线前设计。可导出数据、工作流、提示模板、评测集、日志和配置；可替换模型和身份系统；可在限定时间内停止、回滚和迁移。

董事会采购取舍

经营条件	优先采购对象	不应先买	决策理由
低风险、短任务、无系统写回	通用模型或办公 Copilot	通用 Agent 平台	先验证任务质量与采用率，保持模型可替换
高频、规则清晰、单一渠道	成熟营销单点 SaaS	自建营销 OS	利用现成连接、模板与运营经验
跨系统、有状态、需审批与回滚	Agent 平台 + 专业应用	纯聊天机器人	控制面和运行状态比生成质量更关键
跨部门目标与预算需要统一经营	营销 OS + 数据与身份底座	工具门户式“套壳 OS”	必须形成目标—行动—结果—复盘闭环
流程不稳定、Owner 不清、数据不可用	咨询诊断 + 小规模试点	大额多年软件合同	先消除组织与流程约束
高敏数据、低延迟、强定制或连续性要求	混合 / 专有云 / 私有部署服务	仅以“数据不出域”为理由全量私有化	按数据分级和任务风险选择部署，不追求单一形态

1. 市场为什么“名称趋同、责任分化”

竹势 AI 营销智库出品

六层市场地图层级越向下，企业承担的集成、治理与运营责任越多。

L1	通用大模型 认知与生成底座
L2	营销单点 SaaS 快速价值与孤岛成本
L3	Agent 平台 连接、状态与权限
L4	营销 OS 目标与任务闭环
L5	咨询实施 购买变化能力
L6	私有 / 混合部署 位置、责任与连续性

判断

AI 营销市场的竞争语言正在趋同，采购对象却进一步分化。供应商普遍同时使用“大模型、智能体、平台、操作系统、企业级、私有化”等表述，因为这些名称有利于扩大预算边界；真正决定项目成败的是控制面和交付责任是否落到具体主体。

机制

一个营销任务要进入经营流程，至少经过六种对象：认知生成底座、任务应用、行动编排平台、经营系统、变化实施服务、部署运维服务。每向上一层，供应商需要承担更多业务状态、权限、流程和结果责任；企业也会承担更高的集成、治理和锁定成本。

产品与服务六层市场地图

层级	购买对象	核心控制面	典型交付物	主要边界
底座：通用大模型	推理、生成、多模态与工具调用能力	模型版本、上下文、配额、安全策略	API、模型服务、模型路由	不拥有企业真实任务状态与经营结果
单点：营销 SaaS	一个任务或渠道的完成能力	应用账号、模板、素材、渠道数据	内容、投放、社媒、CRM 等任务结果	跨应用状态、统一治理与数据复用有限
平台：Agent / 自动化	跨工具编排与运行控制	身份、权限、状态、工具、日志、预算	Agent、工作流、连接器、监控	需业务团队定义流程与结果语义
系统：营销 OS	目标到结果的持续经营闭环	目标、任务、数据、资产、协同、治理	统一工作区、运营机制、知识与复盘	若没有统一状态与经营机制，只是门户
实施：咨询与集成	把能力变成组织可用系统	流程、角色、数据、采用、收益	蓝图、配置、集成、培训、变革	项目结束后的能力转移与持续运营
部署：私有 / 混合运维	运行环境和服务连续性	基础设施、补丁、容量、灾备、SLA	部署、监控、安全、升级、托管	部署位置不等于合规结论或业务价值

边界判定表

供应商自称	必须追问的判定问题	满足条件才可接受的定义
大模型平台	是否只提供模型 API？是否提供评测、路由、版本冻结、数据承诺？	可管理多模型生命周期与企业调用策略
Agent 平台	任务状态存在哪里？谁能停止、接管、回滚？工具权限如何限制？	对长任务、状态、工具与异常承担运行控制责任
营销 OS	是否拥有目标、预算、任务、资产、客户、审批、复盘的统一数据对象？	持续经营系统，而非应用入口集合
私有化	模型、应用、日志、监控、密钥、更新分别部署在哪里？谁运维？	明确部署边界、责任矩阵和服务连续性
一体化	哪些组件同源？哪些为转售或第三方？故障和退出由谁负责？	合同中形成单一责任窗口且保留组件透明度

管理含义

RFP 第一页不应要求供应商介绍“产品定位”，而应让其填写六层地图、控制面清单和责任矩阵。任何无法指出任务状态、系统 Owner、业务 Owner、风险 Owner与退出交付物的方案，都不应进入价格谈判。

2. 通用大模型：认知与生成底座

竹势 AI 营销智库出品

采购门	业务任务
证据口径	控制面
交付责任	退出路径

判断

通用模型适合低风险、可人工复核、上下文可控的认知与生成任务；它不是营销事实库、权限系统或经营责任主体。模型采购应从“哪个模型最强”改为“哪种任务以何种质量、时延、成本和风险完成”。

能力与边界

能力	适合任务	必须补充的企业能力	常见误判
文本 / 多模态理解	摘要、分类、信息抽取、初步洞察	来源追溯、企业知识、评测集	把流畅表达当作事实正确
内容生成	初稿、变体、结构化改写	品牌上下文、审核、标识与版权规则	把产能提升直接等同收入增长
推理与规划	方案候选、任务拆解、异常解释	业务约束、工具权限、状态机、验证器	把计划文本当成执行能力
工具调用	检索、API、代码、浏览器动作	白名单、参数验证、最小权限、回滚	看到演示成功即授权生产系统
模型微调 / RAG	专业知识与格式适配	数据治理、版本、召回评测、更新机制	认为“私有知识库”自动消除幻觉

评测与路由

模型 benchmark 只能说明特定数据集、版本和评分规则下的相对表现。企业应建立真实任务集：以历史营销任务、已知答案、边界案例、敏感输入和异常条件构成；评分至少覆盖正确性、依据、品牌一致性、合规、工具调用、延迟和单任务成本。路由策略应允许低成本模型承担分类、抽取与改写，高能力模型处理复杂推理；关键任务保留模型降级与人工接管。

完整案例 1：P&G / Harvard Business School “The Cybernetic Teammate”

主体与时间：Procter & Gamble 与 Harvard Business School 等研究团队，2024 年开展、2025 年发布工作论文。业务情境：专业人员处理真实的新产品创新挑战，随机分配为个人或双人团队，并设置使用或不使用生成式 AI 的条件。研究版本对样本数曾有 776 与 791 的更新口径；正式引用应以所采用版本为准。具体动作：参与者在限定任务中使用生成式 AI 辅助提出与整合方案。结果证据：论文报告 AI 可提高方案表现，并帮助不同职能专业知识更均衡地进入产出；个人加 AI 在部分指标上可达到传统团队水平。归因限制：这是预注册现场实验，内部效度较强，但任务集中于产品创新，时间受控，参与者来自一家大型消费品企业，不能外推到长期营销运营、渠道执行或收入结果。适用边界：支持企业先验证“模型作为认知队友”的任务设计，不支持直接购买自治平台或裁减团队的结论。

完整案例 2：Coca-Cola 全球生成式 AI 营销体验

主体与时间：The Coca-Cola Company，2023—2025 年多次开展生成式 AI 消费者创作和全球活动，微软客户材料披露其中一项活动在 60 天内上线，覆盖 43 个市场和四个区域，并集成 15 项服务。具体动作：以云端 AI 与全球品牌资产构建消费者互动和内容生成体验。结果证据：覆盖范围与上线周期由技术供应商客户案例披露；独立的增量收入、品牌提升或长期留存未披露。归因限制：全球品牌资产、媒体预算、法务与技术资源显著高于一般企业；“60 天上线”包含既有平台能力和供应商支持。适用边界：证明复杂品牌可用模型底座加治理快速形成活动，不证明通用模型单独产生营销 ROI。

管理含义

模型应被视为可替换生产要素。合同需要版本通知、数据使用承诺、地域与子处理器、可用性、速率限制、内容安全、日志、价格变更和终止迁移条款。企业内部则需要模型目录、路由策略、任务评测集与模型切换演练。

3. 营销单点 SaaS：快速价值与孤岛成本

竹势 AI 营销智库出品

采购门	业务任务
证据口径	控制面
交付责任	退出路径

判断

单点 SaaS 往往是最快获得任务价值的采购对象，因为它把模型、界面、模板、渠道规则和运营经验封装在一起。问题不是“单点不够先进”，而是企业同时采购多个单点后，身份、素材、客户、审批和指标会重复。

Jobs to Be Done 连接

Jobs to Be Done 强调客户购买产品是为了完成特定进展。应用到 AI 营销采购，企业应从“生成内容、优化投放、处理线索、监测舆情”等任务出发，而不是从技术品类出发。其当代修正是：任务完成还必须包含数据进入、审核、发布、结果回写与异常处理；仅生成一段文本通常不构成完整 Job。

单点类型	最快价值	隐藏成本	升级 / 退出触发器
内容与创意	模板化生产、多规格适配	品牌资产重复、版权与审核分散	内容需进入统一资产、审批和效果学习
社媒运营	排期、发布、互动与平台数据	账号权限、平台规则和数据导出限制	多品牌、多区域、统一客户身份
广告优化	账户诊断、创意测试、预算建议	归因口径、自动动作风险、平台依赖	跨平台预算与统一实验管理
CRM / 线索	评分、触达、销售辅助	个人信息、同意、字段与流程锁定	营销销售统一状态与客户主数据
舆情 / 研究	持续抓取、告警、报告	数据源覆盖、噪音、许可与黑箱评分	需要证据库、行动闭环与跨部门处置

完整案例 3：Microsoft 365 Copilot 在 Localiza 的采用

主体与时间：巴西出行企业 Localiza，微软于 2024 年披露。业务情境：员工存在重复性知识工作和信息处理负担。具体动作：部署 Microsoft 365 Copilot，并在既有办公套件中使用。结果证据：供应商客户案例称，平均每名员工每月节省 8.3 个工作小时；具体样本、计量方法与对照条件在公开摘要中有限。归因限制：属于供应商自报，且涵盖通用办公而非营销收入；节省时间是否被转化为经营价值取决于岗位重分配。适用边界：说明嵌入既有工作流的 SaaS 可降低采用摩擦，不能用作企业营销 ROI 的直接预测。

完整案例 4：广告自动化案例的归因边界

主体与时间：Microsoft Advertising 2026 年披露 ADAC 在 1 月 1 日至 11 月 30 日期间使用 Performance Max 等能力。具体动作：围绕新客户获取优化广告活动。结果证据：供应商材料称点击增长 89%、转化增长 104%、CPA 下降 4%、转化率增长 8%。归因限制：缺少完整基线、预算变化、季节性、创意和其他渠道因素；结果来自广告平台自报。适用边界：可作为 PoC 指标设计线索，不能据此承诺同类企业结果。

反例与边界

当一个单点工具要求用户手工复制客户资料、提示、内容和结果到其他系统时，其许可证可能便宜，但交易成本转移给员工。采购团队应统计每次跨系统复制、账号维护、权限审批、数据清洗和复盘拼表的时间；达到一定频率后，应通过集成或平台收敛。

4. Agent 平台：连接、状态、权限与可观察性

竹势 AI 营销智库出品

采购门	业务任务
证据口径	控制面
交付责任	退出路径

判断

Agent 平台的价值不在于让 AI“更像人”，而在于让长周期任务可运行、可监督、可停止。企业应采购状态管理和控制能力，而不是采购一组带人格名称的聊天机器人。

企业级 Agent 最小控制面

控制面	最低要求	验收问题
身份	人、Agent、服务账号可区分，支持最小权限和生命周期	员工离职或角色变化后，相关 Agent 权限多久收回？
状态	任务步骤、输入、输出、审批、错误和责任人结构化保存	服务重启后能否从确定节点恢复？
工具	白名单、参数约束、凭证隔离、dry-run	是否能证明 Agent 无法调用未授权接口？
人工接管	关键节点审批、超时升级、暂停和替代执行	异常发生时谁在多长时间间接管？
可观察性	链路、模型、工具、成本、质量与错误日志	能否定位一次错误由模型、数据、工具还是流程引起？
停止与回滚	全局停机、任务取消、补偿动作、版本回退	错误发布或错误写回后如何恢复？
预算	单任务、单用户、单模型与周期上限	超预算时是降级、排队还是停止？

康威定律与 Agent 架构

康威定律指出，组织设计的系统会反映组织的沟通结构。若营销、销售、法务和 IT 权责割裂，Agent 平台会复制这些断点：一个 Agent 生成内容，另一个发布，第三个回写 CRM，却没有共同 Owner。架构设计必须先明确跨部门决策权和异常升级，再决定 Agent 边界。

完整案例 5：Klarna AI 客服的规模与回摆

主体与时间：Klarna 于 2024 年公开称 AI 助手承担大量客服对话，并披露处理时间等改善；随后公司管理层在 2025 年公开强调恢复和增加人工客服选择。业务情境：高量客户服务需要降本和扩展。具体动作：引入生成式 AI 处理查询，同时保留升级路径。结果证据：早期结果主要来自公司与供应商披露；后续回摆表明成本与速度不能替代复杂问题处理、信任和服务体验。归因限制：客服与营销不同，且公开口径持续变化。适用边界：Agent 应按任务风险分层，规模化必须保留人工接管与服务质量指标。

完整案例 6：企业 Agent 平台官方能力边界

主体与时间：Microsoft Copilot Studio、Google Vertex AI Agent 平台、Amazon Bedrock Agents、百度智能云千帆等在 2024—2026 年持续扩展企业 Agent 开发、工具连接和治理功能。具体动作：提供模型接入、Agent 构建、工具或连接器、部署与管理。结果证据：官方文档可证明产品声明和控制功能，不能证明某企业已取得经营结果。归因限制：平台能力依赖具体许可、区域、版本、连接器和客户配置。适用边界：用于建立 RFP 功能要求，不用于厂商排名。

管理含义

Agent PoC 必须主动制造异常：接口超时、权限不足、返回脏数据、模型拒答、预算耗尽、审批人缺席、外部系统部分成功。只展示正常路径的 Demo 不具备采购证明力。

5. 营销 OS：目标、任务、数据与治理闭环

竹势 AI 营销智库出品

采购门	业务任务
证据口径	控制面
交付责任	退出路径

判断

营销 OS 不是“大而全功能集合”，而是负责营销经营状态的系统。它应将目标、预算、任务、资产、渠道、客户、审批、风险和复盘组织为统一对象，并让人和 AI 在同一运行机制中协作。

营销 OS 判定的八道门

门槛	必须具备	伪 OS 信号
目标门	目标和 KR 可关联到行动与结果	只有首页仪表盘
任务门	跨周期任务有状态、Owner、期限、依赖	聊天记录代替任务状态
数据门	关键业务对象有统一标识和质量规则	每个应用自建客户和素材
行动门	可调用工具并记录结果	只能生成建议
协同门	人、Agent、供应商和部门在同一责任链	多个机器人各自对话
治理门	权限、审批、日志、预算、风险分级	只有内容安全过滤
学习门	结果回写为规则、模板、评测与知识	每次任务从零提示
退出门	数据、配置、流程和评测可导出	终止合同即失去业务状态

模块化设计与 Porter 取舍

模块化设计要求通过稳定接口拆分变化速度不同的组件：模型应可替换，身份与主数据应稳定，任务应用可渐进增加。Porter 的战略取舍提醒企业，系统不能同时追求最高定制、最低成本、最快上线和最少运维。董事会需要选择主导目标，并明确放弃项，例如“优先 30 天形成闭环，暂不追求全量私有部署”。

完整案例 7：竹势 AI 营销智库的营销 OS 主张（厂商自述）

主体与时间：竹势 AI 营销智库，2026 年产品与服务材料。业务情境：企业营销工具分散，内容、渠道、线索、投放和复盘脱节。具体动作：提出以 OKR、行动看板、AI 会议、营销日历、工作流、Agent、权限、审批、日志、知识库和本土连接器组成企业级 AI 营销系统，并配套咨询、定制构建与持续优化。结果证据：公开素材说明产品设计与交付主张，未披露经独立审计的客户经营结果。归因限制：属于厂商自述，功能完成度、连接器可用性、性能、SLA 与客户结果必须在 PoC 中验证。适用边界：可作为“营销 OS 应承担哪些控制面”的结构案例，不构成采购推荐。

反例

如果所谓 OS 只提供统一登录和应用卡片，任务状态仍在各工具内、客户和素材无法复用、审批与日志不统一，它只是门户。门户可以改善发现与入口，但不能承担经营系统责任。

6. 咨询与实施：购买变化能力

竹势 AI 营销智库出品

采购门	业务任务
证据口径	控制面
交付责任	退出路径

判断

AI 营销项目失败通常不是因为缺少模型，而是流程没有稳定定义、数据不可用、角色和激励不一致、业务负责人无法持续运营。咨询实施购买的是把不确定业务转化为可运行机制的能力。

交易成本经济学连接

交易成本经济学关注搜寻、谈判、协调、监督与机会主义成本。企业多买一个工具，会增加供应商协调、接口变更、责任争议和退出谈判。高度专用、频繁变化且结果难度量的任务更需要内部能力或深度合作；标准化、可验收的任务更适合外购。

实施责任	供应商应交付	企业必须承担	合同验收
诊断	现状、任务、数据、风险与依赖地图	提供真实流程、数据与决策人	问题定义经业务 Owner 签字
流程重构	目标流程、控制点、异常和回滚	决定权责与政策	真实场景走查通过
数据准备	字段、质量、权限、保留与映射	数据合法性和主数据 Owner	质量阈值与缺陷清单
配置与集成	连接器、工作流、测试与文档	账号、接口、变更窗口	端到端和异常测试
采用推动	角色培训、SOP、运营节奏	经理使用、绩效与资源安排	采用率和任务完成率
收益实现	基线、指标、复盘与优化	确认财务与业务归因	价值五账本按周期复核
知识转移	架构、配置、运行手册与培训	指定内部 Owner	可独立运行和退出演练

约束理论连接

约束理论要求先识别系统瓶颈。若瓶颈是销售未跟进，增加内容生成只会制造更多未处理线索；若瓶颈是法务审批，自动生成更多素材会扩大等待队列。试点应围绕瓶颈设计，而不是围绕最容易演示的功能。

完整案例 8：Coca-Cola 60 天跨市场活动的实施含义

该案例除模型能力外，还涉及 15 项服务、全球区域协调、品牌资产、云工程、内容体验与上线治理。公开材料没有把结果归因于单一模型。其管理含义是：复杂营销项目的周期由集成、审批与组织协调决定；购买模型许可证无法替代实施责任。

管理含义

咨询合同应避免只交付 PPT。每个阶段必须产生可运行资产：真实任务集、数据字典、责任矩阵、配置、测试记录、运行手册、采用计划和价值复盘。收益承诺应区分供应商可控、共同可控和企业独立可控因素。

7. 私有／混合部署：位置、责任与连续性

竹势 AI 营销智库出品

采购门	业务任务
证据口径	控制面
交付责任	退出路径

判断

部署形态解决的是数据驻留、延迟、定制、容量、连续性和责任分配问题。“私有化”不自动意味着安全、合规或低成本；未维护的私有系统可能比成熟云服务风险更高。

形态	主要价值	新增责任	适合条件	常见误区
公有云 SaaS / API	快速上线、弹性、持续更新	供应商风险、数据与地域审查	低至中敏任务、标准能力	认为云端必然不安全
专有云 / 隔离租户	增强隔离、网络与密钥控制	配置、专属容量与费用	中高敏、需云能力与隔离	把逻辑隔离等同本地部署
混合架构	敏感数据与高能力模型分层	路由、身份、日志与跨域复杂度	任务与数据可清晰分级	没有统一控制面导致双重运维
本地私有部署	数据驻留、定制与自主升级节奏	算力、容量、补丁、安全、灾备、人才	强监管、低延迟、稳定负载、能力成熟	只计算服务器，不计算持续运维

中国法规边界

《生成式人工智能服务管理暂行办法》主要适用于向中国境内公众提供生成内容服务；企业内部研发和应用且未向公众提供服务时，不适用该办法所述范围，但《个人信息保护法》《数据安全法》《网络数据安全条例》及行业规则仍可能适用。2025 年发布的《人工智能生成合成内容标识办法》及强制性国家标准规定了适用服务提供者和传播平台的显式、隐式标识责任，并于 2025 年 9 月 1 日实施。GB/T 45654–2025《网络安全技术 生成式人工智能服务安全基本要求》于 2025 年 11 月 1 日实施，为推荐性国家标准。

数据分级部署决策

数据 / 动作等级	示例	优先架构	控制要求
L1 公开	公开品牌资料、公开竞品信息	公有云模型 / SaaS	来源、版权、内容标识与账号安全
L2 内部	未公开营销计划、普通运营数据	企业云 / 隔离租户 / 混合	访问控制、保留期、供应商数据承诺
L3 敏感	客户个人信息、报价、合同、精细画像	混合或专有环境	最小化、同意 / 合法基础、脱敏、审计
L4 核心 / 高风险动作	核心数据、自动预算变更、公开发布、客户权益决策	强隔离 + 人工审批，必要时本地	双人复核、回滚、灾备、持续监控

私有部署 TCO 边界

自建推理成本不仅取决于 GPU 采购，还包括峰值容量、冗余、模型量化与适配、推理框架、监控、漏洞与补丁、升级兼容、数据备份、值班与人才。负载低或波动大时，公有 API 往往更经济；负载稳定、高且数据与时延要求明确时，私有部署可能形成优势。

8. 企业组合架构：最少必要层级

竹势 AI 营销智库出品

最少必要层级以任务为入口，把可替换能力与不可外包责任分开。

经营目标与任务组合
营销 OS / Agent 编排
单点 SaaS 与专业工具
模型路由与知识资产
统一控制面：身份 · 权限 · 审批 · 日志 · 评测 · 成本 · 回滚

判断

优秀组合不是产品最多，而是每个控制面只有明确主责系统，同时保留替换接口。身份、客户主数据、内容资产、任务状态、日志和财务计量应避免多套“事实源”。

企业组合架构蓝图

架构域	主责对象	可替换组件	关键接口	Owner
体验与入口	营销 OS / 任务应用	聊天、桌面、移动、消息渠道	统一身份、任务 API	业务 Owner
流程与 Agent	Agent 平台 / 工作流	模型、工具、Agent 模板	状态、事件、审批、补偿	系统 Owner
营销应用	内容、投放、社媒、CRM 等 SaaS	同类单点产品	标准数据对象、导入导出	场景 Owner
模型与知识	模型网关、RAG、评测	国内外模型、开源模型	统一调用、版本、成本与评测	AI 平台 Owner
数据与资产	CDP / CRM / DAM / 数据仓库	分析和数据服务	主数据、血缘、权限	数据 Owner
身份与安全	企业 IAM、密钥、审计	安全工具	SSO、SCIM、RBAC、日志	风险 Owner
运营与财务	监控、FinOps、SLA、价值账本	观测和成本工具	指标、告警、账单	运营 Owner

任务—能力—控制面—交付责任矩阵

真实任务	必要能力	关键控制面	主责交付对象	验收结果
生成品牌文章初稿	模型 + 品牌知识	来源、语气、敏感词、版本	模型 + 内容 SaaS	盲评质量、事实与审核时长
多平台排期发布	适配、账号、调度、回写	账号权限、审批、失败重试	社媒 SaaS / Agent 平台	发布成功率与错误恢复
广告账户优化建议	数据连接、分析、实验	预算、归因、dry-run、审批	广告 SaaS + 实施	增量实验与风险控制
线索自动跟进	客户状态、内容、渠道动作	同意、身份、频控、人工接管	CRM / 私域 SaaS + Agent	响应时间、有效推进、投诉率
营销战役闭环	目标、任务、资产、渠道、复盘	预算、状态、跨部门责任	营销 OS + 实施	经营五账本和复用资产

委托代理问题

供应商、实施商、业务部门和 AI Agent 都可能成为“代理人”，而董事会是最终委托人。信息不对称会导致供应商强调可见功能、隐藏集成和运维成本；业务团队可能追求产量而忽略经营价值。治理应通过可审计指标、共同基线、分阶段付款、退出权和职责分离降低代理风险。

9. 采购经济学：TCO、价值五账本与锁定风险

竹势 AI 营销智库出品

TCO 七项成本

许可 · 集成 · 数据 · 推理 · 运营 · 风险 · 退出

价值五账本

成本 · 速度 · 质量 · 收入 · 风险与资产

TCO 七项成本账本

成本项	必须计入	常见漏项	计量方式
1 订阅 / 许可	席位、模块、最低承诺、环境	闲置席位、测试与生产重复	月度有效用户与任务量
2 模型调用	输入输出、缓存、检索、工具、图像视频	重试、长上下文、峰值与价格变更	每完成任务成本
3 数据	采集、清洗、标注、知识更新、存储	历史数据修复、权限审批	每数据域准备与维护工时
4 集成	接口、连接器、身份、测试、变更	第三方 API 费用、版本升级	初始 + 年度变更成本
5 审核与运营	人工复核、异常处理、内容标识、培训	经理协调、影子流程	每任务人工分钟与运营 FTE
6 运维与连续性	监控、SLA、安全、补丁、灾备、值班	模型升级回归测试	年度运行成本与停机损失
7 迁移与风险	导出、重构、违约、数据事件、监管与声誉	锁定溢价、退出停机	情景概率×影响 + 退出报价

经营价值五账本

账本	指标示例	基线要求	避免的误判
成本	每任务成本、外包费、返工、人力时间	同任务历史成本与质量	把节省时间全部按工资变现
速度	周期、响应时间、上线时间、等待时间	端到端而非生成步骤	只测“生成快了多少”
质量	事实、品牌、创意、转化、客户满意	盲评、抽检与错误等级	用产量替代质量
收入	合格线索、转化、客单、留存、增量毛利	对照组、实验或合理归因	把相关性当因果
风险	违规、投诉、数据事件、越权、恢复时间	事件定义与风险暴露量	把“零事件”当零风险

平衡计分卡连接

平衡计分卡提醒企业同时观察财务、客户、内部流程与学习成长。AI 项目若只看节省工时，会忽略客户体验、流程可靠性和组织能力；若只看创新活动数量，也无法证明财务价值。价值五账本可视为面向 AI 营销的扩展，将风险单独列账。

供应商锁定与退出风险矩阵

锁定对象	低风险	中风险	高风险	退出控制
数据	标准格式可随时导出	部分字段或历史受限	无法导出完整业务状态	合同定义格式、频率、费用和时限
流程	开放编排或可移植定义	依赖专有连接器	流程只存在黑箱平台	交付流程文档、规则和测试集
模型	支持多模型路由	仅同厂模型切换	应用与单一模型深度绑定	抽象模型接口与回归评测
身份	企业 SSO 与自动回收	平台内角色映射	供应商账号为主身份	IAM 主导、最小权限、SCIM
知识 / 提示	企业拥有并可导出	模板部分可见	提示、评测和知识不可得	知识产权属与导出条款
运维	多方可接管	需认证伙伴	仅原厂可运行	运行手册、源代码 / 托管安排、退出演练

价格比较原则

不要直接比较“每百万 token”或“每席位”。统一换算为每个成功完成的真实任务成本，并计入失败、重试、人工审核、检索、工具调用和外部系统费用。模型价格变化快，合同应允许路由和替换，而非用某一时点价格锁定多年架构。

10. 真实任务集 PoC：14 天验证、30 天闭环、90 天决策

竹势 AI 营销智库出品

14 DAYS

真实任务验证

能力、边界、基线

30 DAYS

受控闭环

权限、异常、运营

90 DAYS

投资决策

复制、重构或停止

判断

PoC 的目的不是证明产品能运行，而是减少四类不确定性：任务价值、技术可行性、组织采用和风险可控性。必须使用企业真实数据和任务，同时控制敏感范围。

真实任务集设计

任务类别	样本要求	异常样本	评分者
标准任务	20—50 个高频真实任务	输入缺失、格式变化	一线用户 + 业务主管
高价值任务	5—10 个影响收入或关键客户的任务	多约束、跨系统、长上下文	资深专家 + 财务
高风险任务	公开发布、客户触达、预算或个人信息	越权、敏感内容、错误工具参数	法务 / 安全 / 风险 Owner
边界任务	产品明确不承诺或能力不稳定	未知问题、冲突指令、服务中断	系统 Owner

PoC 评分卡（100 分）

维度	权重	评分依据	一票否决
任务结果质量	25	正确性、依据、品牌与专业盲评	高风险错误不可拦截
端到端完成率	15	从输入到写回 / 发布 / 交付	关键步骤依赖人工复制
控制与安全	15	权限、审批、日志、标识、数据边界	越权或敏感数据违规
异常恢复	10	超时、部分失败、重试、回滚	无法停止或恢复
用户采用	10	有效用户、重复使用、学习成本	关键岗位拒绝使用且无替代流程
速度	10	端到端周期和等待时间	速度提升牺牲质量
TCO	10	每成功任务全成本	成本不可观测或无预算控制
可替换与退出	5	数据、配置、模型与流程可迁移	核心业务状态不可导出

14 / 30 / 90 天决策门

时间	目标	必须产出	继续条件	停止 / 回滚条件
14 天	证明任务与边界	基线、真实任务集、评分、风险清单	质量和控制达到最低阈值	越权、无法审计、价值假设不成立
30 天	形成一个运营闭环	真实用户、数据回写、异常处理、价值账本	端到端完成率和采用稳定	靠项目人员手工维持、成本失控
90 天	决定规模化	架构、Owner、SLA、TCO、合同与扩展计划	价值可复现、运营可移交	无明确 Owner、收益无法归因、退出不可行

验收原则

每项结果同时记录平均值、尾部风险和失败分布。一个平均质量 90 分但 2% 情况会错误发送客户消息的系统，可能不适合自动执行。高风险动作采用更严格阈值，并要求人工批准、dry-run 和补偿流程。

11. 中国企业分型决策

竹势 AI 营销智库出品

分型不是贴标签，而是重算约束	大型集团
成长企业	强渠道企业
高合规行业	

判断

中国市场的选型受国产模型与云生态、数据出境、备案与标识、平台渠道接口、交付网络、行业监管和服务连续性共同影响。企业不应以“国产 / 海外”二分替代任务级风险判断，而应建立可替换、多层控制的组合。

企业类型	典型条件	建议组合	重点风险	首个 PoC
成长型中小企业	团队小、预算有限、流程未标准化	通用模型 + 1—2 个单点 SaaS + 轻实施	工具堆叠、无人运营	内容—线索—跟进闭环
成熟中型企业	已有 CRM / 内容 / 投放系统	模型网关 + Agent 平台 + 核心 SaaS 集成	接口、身份、指标口径	跨系统高频任务
大型集团	多品牌、多区域、多供应商	统一身份 / 数据 / 治理 + 分层应用 + 混合部署	影子 AI、重复采购、总部与业务冲突	一个事业群可复制样板
高监管行业	敏感数据、审计与行业规则	数据分级 + 强审批 + 专有 / 混合 + 专业实施	合规泛化、私有系统运维不足	低风险内部知识任务
B2B 长销售周期	高客单、线索少、内容与销售协同	研究 / 内容 SaaS + CRM + Agent workflow	归因周期、销售采用	线索研究一个个性化跟进
消费与连锁	高频内容、多门店、多渠道	营销 OS / 社媒 SaaS + 资产与权限中心	账号、品牌一致性、平台规则	总部策略—门店执行—复盘

国产化与连续性

国产化可以降低部分地域、采购和生态风险，也可能提高本地部署与中文场景适配；但仍需评估模型质量、版本稳定、许可证、硬件适配、人才和供应商持续服务。海外模型可能在部分任务表现领先，但需审查地域可用性、数据处理、合同与连续性。最佳实践是把模型与业务状态解耦，关键任务保留至少一个可接受的替代路径。

渠道生态边界

中国营销大量发生在微信、企业微信、抖音、小红书、淘宝 / 天猫、京东及广告平台。连接器是否“存在”不等于可生产使用：需要核对官方 API 权限、账号主体、审核、速率、数据字段、自动化限制与平台政策。浏览器自动化可用于低风险辅助，但不应替代稳定官方接口承担高价值生产流程。

12. 董事会、CMO 与采购负责人行动路线

竹势 AI 营销智库出品

14

定任务与责任

30

跑受控闭环

90

做组合决策

365

沉淀能力资产

14 / 30 / 90 / 365 天路线

阶段	董事会 / CEO	CMO / 业务	采购 / 法务 / IT	交付门
14 天	确定一个经营瓶颈与风险偏好	定义任务集、基线和用户	完成供应商责任、数据与安全初筛	是否值得进入闭环试点
30 天	审查价值五账本与一票否决事件	运行真实闭环与周复盘	核验日志、权限、成本和异常	是否具备可运营性
90 天	批准组合架构、预算与 Owner	形成 SOP、角色和扩展场景	完成 RFP、合同、SLA、退出条款	是否规模化或停止
365 天	季度审查价值、风险与供应商组合	扩展场景并淘汰低价值工具	执行续约、替换、灾备和退出演练	是否形成持续经营能力

董事会决策清单

- 我们购买的是六层中的哪一层？供应商对哪一层承担合同责任？
- 真实任务、业务基线、价值五账本和一票否决条件是否已批准？
- 身份、数据、任务状态、工具、日志、预算和退出控制面分别归谁？
- 规模化后谁承担业务 Owner、系统 Owner、数据 Owner 与风险 Owner？
- 若主模型、主供应商或关键渠道不可用，替代路径是什么？

CMO 运营清单

- 优先解决经营瓶颈，不以内容产量作为默认目标。
- 将品牌规范、客户状态、渠道规则和审批转化为结构化资产。
- 把异常、投诉、低质量和人工接管计入运营指标。
- 每月关闭低使用、低价值或重复能力，防止工具自然增长。

采购与 RFP / 合同责任清单

条款域	必须写清	不可接受表述
范围	组件、版本、环境、用户、任务、接口和排除项	“提供企业级 AI 平台”
责任	设计、配置、数据、集成、测试、上线、运维、收益各方 RACI	“双方共同推进”而无主责
数据	用途、地域、保留、训练、子处理者、导出与删除证明	“按行业惯例处理”
安全	身份、权限、加密、日志、事件通知、漏洞与审计	仅提供认证清单
模型	版本、替换、降级、价格、限流、回归测试	默认自动升级且无通知
服务	SLA、支持、恢复、容量、变更和停服	“尽商业合理努力”覆盖关键系统
验收	真实任务、阈值、异常、尾部风险、复测	演示通过即验收
知识产权	输入、输出、配置、工作流、知识、定制与第三方许可	所有衍生配置归供应商
退出	导出格式、时限、费用、协助、删除、过渡服务	终止后仅提供静态报告
价值	基线、可控因素、计量和审计	以行业平均 ROI 承诺项目收益

RACI：四类 Owner

角色	不可转让责任	典型岗位
业务 Owner	定义任务、价值、质量与采用；决定是否继续	CMO、增长负责人、业务单元负责人
系统 Owner	架构、集成、运行、变更与服务连续性	CIO、数字化负责人、营销技术负责人
数据 Owner	数据合法性、质量、访问、保留与主数据	业务数据负责人、数据平台主管
风险 Owner	风险偏好、审批门、事件处置与监管沟通	法务、合规、信息安全、品牌风险负责人

13. 管理者工具包

竹势 AI 营销智库出品

工具 1：采购对象一页纸

问题	填写内容
真实任务与经营瓶颈	
六层采购对象	
现有系统与事实源	
关键控制面及 Owner	
价值五账本基线	
一票否决风险	
14 / 30 / 90 天决策门	
退出与替代路径	

工具 2：供应商会议十问

1. 请用一个真实任务说明你们承担到哪一步，哪一步由客户或第三方负责？
2. 任务状态、客户数据、内容资产和日志分别存在哪里？
3. 发生部分成功、重复执行或错误写回时如何补偿？

4. 哪些功能是自研、第三方、开源或转售？对应 SLA 谁承担？
5. 模型如何选择、升级和降级？客户能否冻结版本或切换模型？
6. 哪些数据用于训练、改进或人工查看？如何证明删除？
7. 私有化后谁负责容量、补丁、漏洞、监控、灾备和升级兼容？
8. 请展示异常路径、人工接管、全局停机和回滚，而非只展示正常 Demo。
9. 合同终止后可导出哪些数据、配置、工作流、知识、评测和日志？
10. 请把客户案例中的结果拆分为事实、供应商自报、归因假设和未披露项。

工具 3：停止、回滚与退出触发器

触发器	立即动作	后续决策
越权访问或敏感数据不当处理	暂停相关 Agent / 连接器，保全日志，启动事件流程	修复并复测；重大事件退出
高风险公开错误无法拦截	关闭自动发布，恢复人工审批	提高阈值或取消自动化
连续两周期价值低于基线	冻结扩展与新增许可	优化、替换或终止
每成功任务成本持续超预算	降级模型、减少上下文、改流程	重新招标或自建部分能力
供应商重大变更 / 停服 / 涨价	启动替代模型和导出	执行过渡服务与迁移
核心状态或数据无法导出	停止新增业务依赖	合同整改；不整改则退出

14. 术语边界与来源索引

竹势 AI 营销智库出品

术语边界

术语	本报告定义
通用大模型	提供通用认知、生成、多模态或工具调用能力的模型服务 / 权重，不等同于业务系统。
营销单点 SaaS	围绕一个营销任务、渠道或对象封装的应用服务。
Agent 平台	管理模型、工具、状态、权限、运行与观察的行动编排基础设施。
营销 OS	对营销目标、任务、数据、资产、协同、治理与复盘承担统一经营状态责任的系统。
咨询实施	把业务、组织、数据和技术转化为可运行机制的专业服务。
私有部署	模型或应用在企业控制的专属环境运行；不自动代表所有组件均本地。
混合部署	不同数据、模型、应用或控制面按风险和能力分布在多个环境。
控制面	定义身份、权限、状态、策略、日志、成本、版本、停止和退出的管理层。
TCO	采购期内许可证、调用、数据、集成、审核、运维、迁移与风险的全成本。
PoC	以真实任务、基线、异常和决策门减少采购不确定性的验证。

具名专业观点与管理思想

思想 / 观点	在本报告中的使用与边界
Michael Porter, 《What Is Strategy?》, 1996	战略要求取舍与活动系统一致性；用于确定上线速度、定制、成本与控制之间的放弃项。
Herbert Simon, 有限理性	决策者无法掌握全部信息；采购应通过阶段门、真实任务和可逆选择降低不确定性。
Ronald Coase / Oliver Williamson, 交易成本经济学	边界取决于协调、监督、专用性与机会主义成本；用于判断外购、深度合作或内部建设。
Melvin Conway, Conway’s Law, 1968	系统结构映射组织沟通；用于先设计跨部门责任再设计 Agent 边界。
Clayton Christensen 等, Jobs to Be Done	客户购买进展而非功能；用于从真实任务而非技术名称出发。
Eliyahu Goldratt, 约束理论	系统绩效由瓶颈决定；用于避免在非瓶颈环节堆叠 AI 产能。
Robert Kaplan / David Norton, 平衡计分卡	财务、客户、流程、学习需共同衡量；用于扩展 AI 价值评价。
NIST AI RMF / GenAI Profile, 2023—2024	以 Govern、Map、Measure、Manage 组织风险；用于建立持续风险管理而非一次性合规。
Fabrizio Dell’Acqua 等, “The Cybernetic Teammate”, 2025	现场实验显示 AI 可改变个人与团队的表现及专业整合；边界是受控创新任务，非长期经营结果。
Ethan Mollick, Co-Intelligence, 2024	强调把 AI 作为协作对象并持续实验；本报告将其转化为任务集、边界和人工接管要求。

来源索引（可检索纯文本）

[1] 国家互联网信息办公室等，《生成式人工智能服务管理暂行办法》，2023-07-13；适用范围：向中华人民共和国境内公众提供生成内容服务。

- [2] 国家互联网信息办公室等,《人工智能生成合成内容标识办法》, 2025-03-14; 与强制性国家标准同步于 2025-09-01 实施。
- [3] 国家市场监督管理总局、国家标准化管理委员会, GB 45438-2025《网络安全技术 人工智能生成合成内容标识方法》, 2025。
- [4] 国家市场监督管理总局、国家标准化管理委员会, GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》, 发布日期 2025-04-25, 实施日期 2025-11-01。
- [5] 全国人民代表大会常务委员会,《中华人民共和国个人信息保护法》, 2021-08-20。
- [6] 全国人民代表大会常务委员会,《中华人民共和国数据安全法》, 2021-06-10。
- [7] 国务院,《网络数据安全管理条例》, 2024; 2025-01-01 起施行。
- [8] NIST, Artificial Intelligence Risk Management Framework 1.0, 2023.
- [9] NIST, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, NIST AI 600-1, 2024-07-26.
- [10] Fabrizio Dell'Acqua et al., The Cybernetic Teammate: A Field Experiment on Generative AI Reshaping Teamwork and Expertise, HBS Working Paper 25-043 / NBER Working Paper 33641, 2025; 不同版本样本口径为 776 / 791, 引用时需注明版本。
- [11] Microsoft Customer Story, Localiza saves up to 19 hours of work with Microsoft 365 Copilot (摘要披露平均每名员工每月节省 8.3 小时), 2024-03-12; 供应商自报。
- [12] Microsoft Customer Story, The Coca-Cola Company: 60 days to launch, 43 markets, four regions, 15 services, 2025-04-15; 供应商自报, 经营增量未披露。
- [13] Microsoft Advertising, ADAC Success Story, 2026-01-20; 供应商自报, 披露点击、转化、CPA 与转化率变化。
- [14] Microsoft, Microsoft 365 Copilot and Copilot Studio official product and pricing documentation, accessed 2026-07; 版本与价格随时间变化。
- [15] Google Cloud, Generative AI / Agent Platform official documentation, accessed 2026-07。
- [16] Amazon Web Services, Amazon Bedrock and Agents official documentation, accessed 2026-07。
- [17] 百度智能云, 千帆大模型平台官方产品说明, accessed 2026-07。
- [18] 华为云, 盘古大模型与 ModelArts 官方资料, 2024—2025。
- [19] 阿里云, PAI-EAS 大模型部署官方文档, 更新日期 2026-07-01。
- [20] Michael E. Porter, What Is Strategy?, Harvard Business Review, 1996.

[21] Ronald H. Coase, The Nature of the Firm, Economica, 1937； Oliver E. Williamson, Transaction Cost Economics.

[22] Melvin E. Conway, How Do Committees Invent?, Datamation, 1968.

[23] Clayton M. Christensen et al., Competing Against Luck, 2016.

[24] Eliyahu M. Goldratt, The Goal, 1984.

[25] Robert S. Kaplan and David P. Norton, The Balanced Scorecard, 1992—1996.

[26] 竹势 AI 营销智库，《竹势 AI 营销智库产品及服务介绍素材》，2026；厂商自述，未披露独立经营结果。

[27] 竹势 AI 营销智库，《公司介绍与品牌定位》，2026；机构与产品定位资料。

[28] 竹势 AI 营销智库，《竹势 AI 营销智库目标客群研究》，2026-04-28；用于理解中小民企采购心理，文档明确其为公开资料与策略推演、非一线访谈。

结束语

董事会不需要预测哪一家模型或平台最终胜出。更稳健的策略是：用真实任务定义价值，用控制面定义责任，用七项 TCO 管理经济性，用五账本管理经营结果，用阶段门控制不可逆投入，并在第一天保留替换和退出权。

关于竹势 AI 营销智库

竹势 AI 营销智库出品

竹势 AI 营销智库关注企业增长、营销组织变革、智能体运营与 AI 治理，帮助企业老板、CEO、CMO 和数字化管理者把复杂技术议题转化为可讨论、可比较、可执行的经营决策。

本报告用市场分层、责任边界、采购经济学与真实任务集工具，帮助管理团队选择最少必要产品层级，并在签约与规模化之前建立证据、权限、交付责任和退出机制。