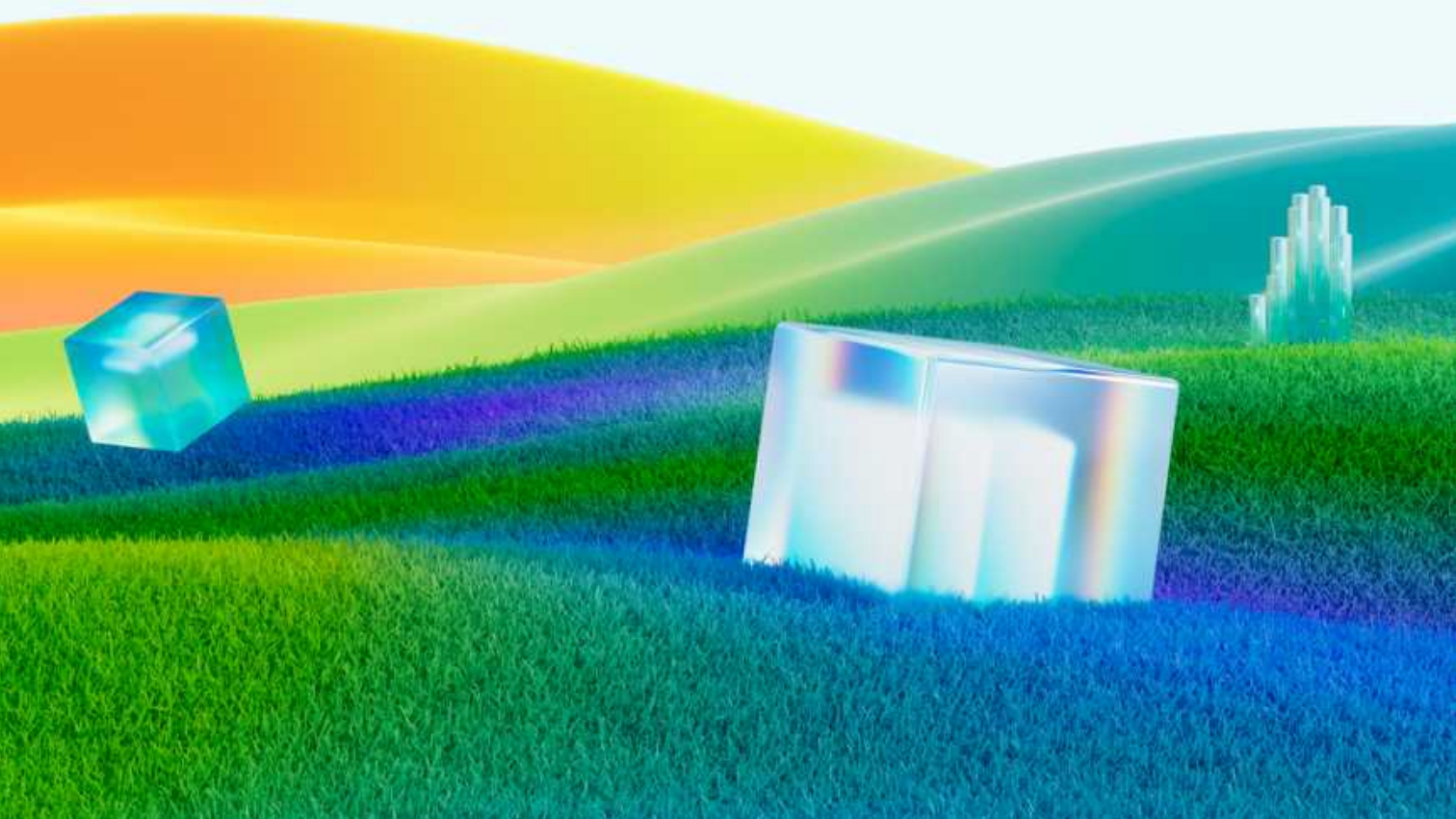


企业进化与价值重塑

AI 超级公司白皮书

AI Super Company White Paper
Enterprise Evolution and Value Reshaping



前言

人类历史上，每一次技术革命都曾深刻重构社会组织形态——蒸汽机催生了工厂制度，电气化重塑了流水线生产，互联网打破了物理空间的边界。而本次由 AI 引领的变革更像是一场内生式的能力重构，AI 不再是外部工具的简单叠加，而是将数据处理、智能预测、自主决策与持续学习能力嵌入 workflows，赋予系统自主感知与主动响应的能力，从而在产品服务、基础能力与组织形态层面不断自我再造，其催化深度与变革速度均前所未有。

随着 AI 能力不断演进和迭代，2025 年无疑成为 AI Agent 元年。大模型推理能力的突破以及协议的标准化使得具备自主决策的 Agent 能力越来越强，这标志着 AI 从单点工具向系统级生产力的转变。从科技巨头到初创公司，从应用软件到智能硬件，几乎所有产品都在被“Agent”概念重构。AI Agent 的演进助推 AI 超级公司悄然浮现，并将长期发展；在激烈的市场竞争中，未来真正的赢家，将是敢于基于 AI 重构自身基因的组织。

为了帮助企业领导者理解未来的 AI 组织将如何演变，阿里云研究院分析了一系列 AI 创新案例，并结合 1500 家 AI 企业调研（其中与数百家 AI 原生初创公司企业管理者、学者、经济学家、科学家和思想领袖进行了交流），共同探索未来 AI 组织可能的形态。本白皮书目的是结合技术趋势与产品服务变革、组织理论创新、以及 AI 实践案例，解析 AI 超级公司的形态特征和底层逻辑，为企业的未来转型提供框架性参考。



第一章 AI 超级公司的进化与特征	1
1.1 什么是“AI 超级公司”	1
1.2 AI 超级公司的典型特征	3
第二章 超级 AI 产品/服务	4
2.1 产品形态的智能化跃迁	5
2.1.1 从“被动工具”到“主动智能体”	5
2.1.2 超级 AI 硬件产品	6
2.1.3 超级 AI 软件产品	8
2.2 服务模式的预见式重构	9
2.2.1 从“响应需求”到“创造需求”	9
2.2.2 服务的“全生命周期陪伴”	10
2.3 生而全球的跨越式发展	11
第三章 超级AI 基础/能力	12
3.1 多模态高效数据平台	13
3.2 AI 基础设施与 AI 原生架构	15
3.2.1 AI 基础设施	15
3.2.2 AI 原生架构	16
3.3 Agent 商业应用与开发构建	18
3.3.1 Agent 商业应用	19
3.3.2 Agent 开发构建	20
3.4 端到端安全与治理	21

第四章 超级 AI 组织/架构22

4.1 通用职能流程迈向智能化重塑	23
4.2 从增强组织到液态组织的演进	24
4.2.1 AI 增强型组织	24
4.2.2 人机协同型组织	25
4.2.3 智能液态型组织	25
4.3 人机协作开启超级员工时代	26
4.3.1 人机协作新型能力体系	26
4.3.2 AI 思维与 Agent 管理能力	28
4.4 共生性文化适配与泛在治理	29
4.4.1 基于 AI 迭代的机制文化	29
4.4.2 基于 AI 伦理的泛在治理	29
4.5 组织边界的模糊化与生态化	30

第五章 AI 超级公司发展阶段评估体系31

5.1 AI 超级公司的进化与形态	31
5.2 AI 超级公司发展阶段评估体系（4D-12I 模型）	33
5.3 AI 超级公司评估体系应用	34
5.3.1 技术基建维度	35
5.3.2 组织协同维度	35
5.3.3 产品服务维度	36
5.3.4 价值创造维度	36

第六章 AI 超级公司的挑战与突围路径37

6.1 AI 发展的核心挑战	38
6.2 AI 应用的突围路径	41

结语45

第一章

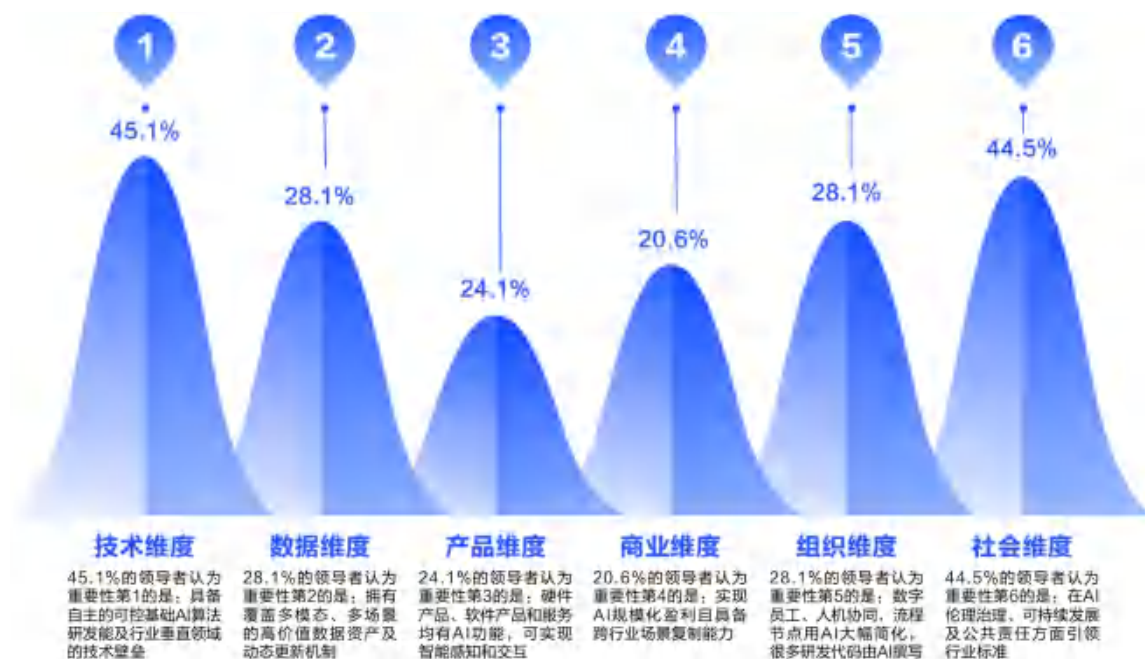
AI 超级公司的进化与特征

1.1 什么是“AI 超级公司”

传统认知中，“AI 超级公司”常与科技巨头画等号——但随着 AI 技术从“集中突破”走向“普惠渗透”，其定义早已超越“规模大小”或“行业出身”。真正的 AI 超级公司，核心是以 AI 为“底层生产力”，能持续创造独特价值、突破行业边界、引领场景创新的组织，它可以是手握核心技术的科技巨头，也可以是深耕细分场景的创业公司，甚至是完成 AI 转型的传统企业。

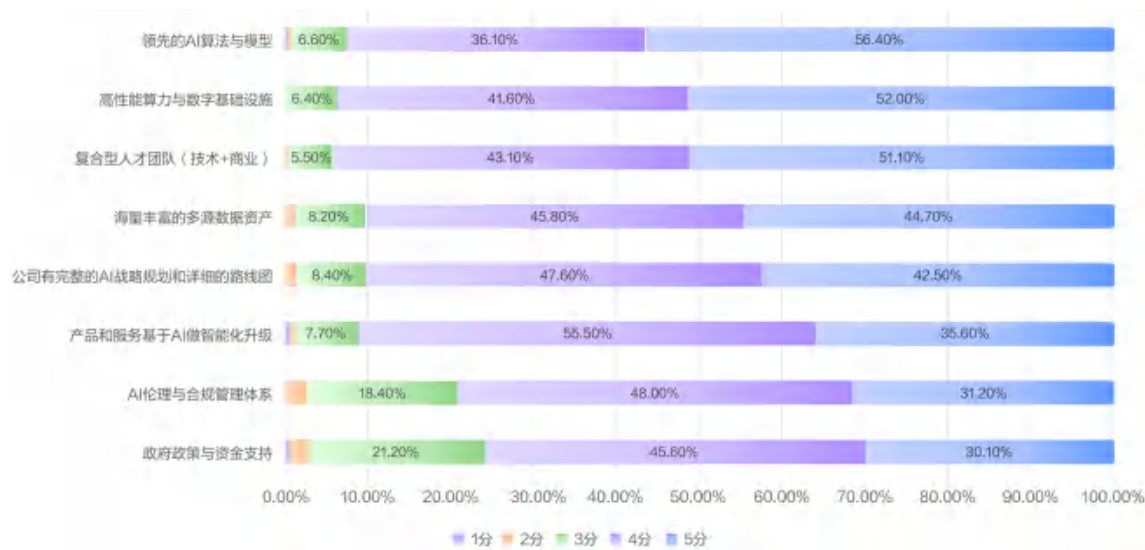
AI 超级公司——是深度整合人工智能技术，以人机协作、AI 智能协同为核心驱动力的新型组织形态。具备“产品 / 服务 - 组织 / 架构 - 基础 / 能力”三维度典型创新特征，最终实现效率、创新和竞争力的质变。

问题：您认为“AI 超级公司”的核心内涵应包含以下哪些要素？（重要性排序）



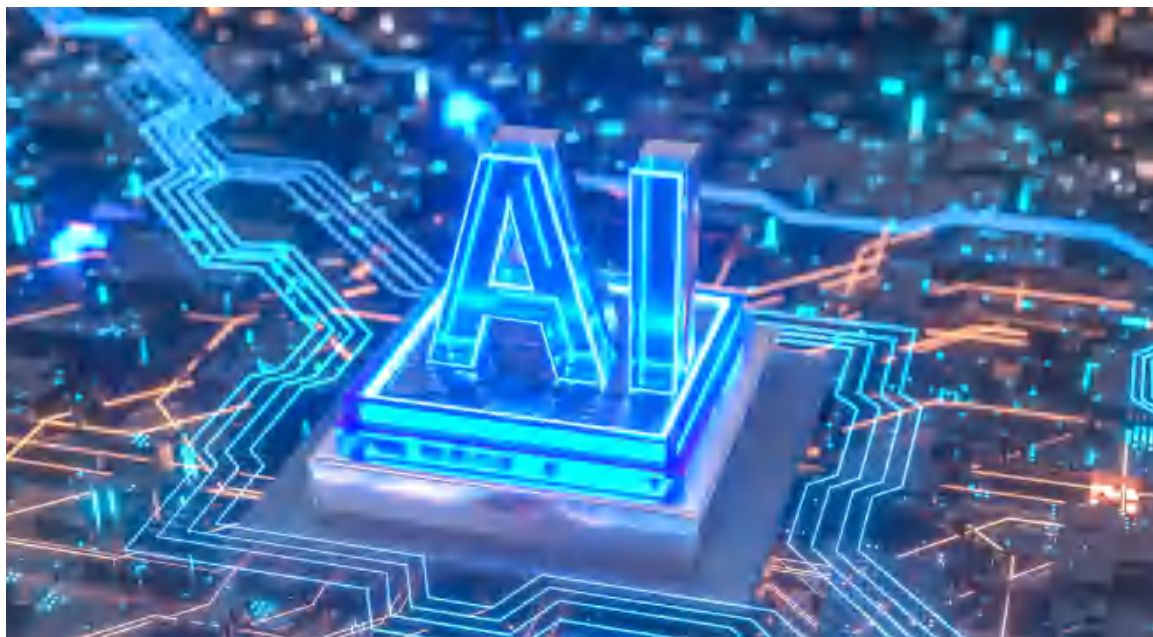
图：AI 超级公司核心内涵重要性排序（企业管理者调研） 来源：阿里云研究院 样本 n=500

问题：您认为建设 AI 超级公司需要哪些关键要素？（按重要性进行打分，1-5 分，1 为最低，5 为最高）



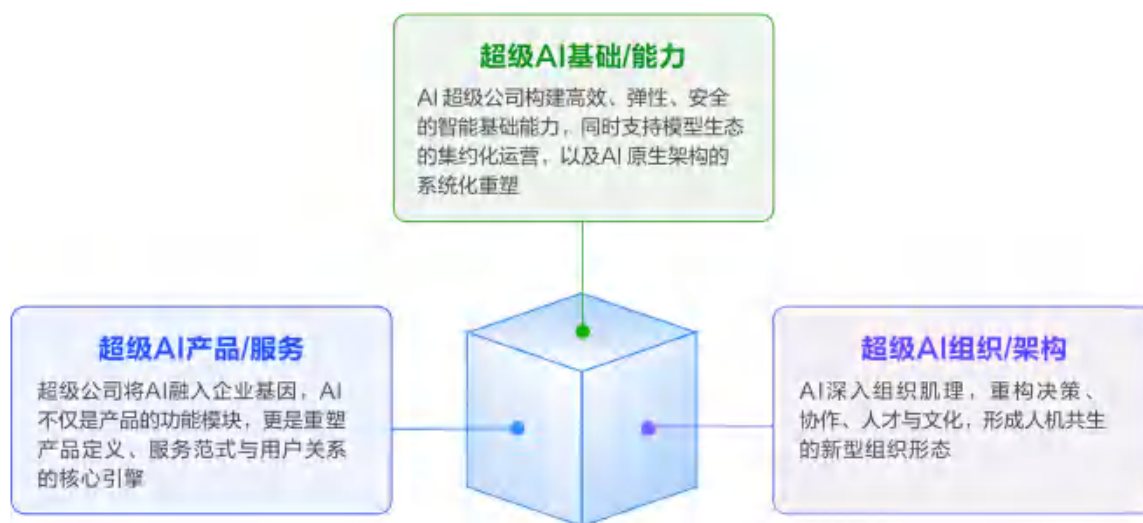
图：AI 超级公司关键要素重要性排序（企业管理者调研） 来源：阿里云研究院 样本 n=500

基于以上企业调研结果以及众多原生 AI 公司企业管理者的访谈交流，面向未来的 AI 超级公司核心内涵以及关键要素主要可以归纳为“产品/服务（AI 化升级与重构）- 组织/架构（战略、人才与人机协同）- 基础/能力（技术与数据）”三个大维度的 AI 化影响，其中每个维度又包含相关的细节要素，白皮书将针对这些关键要素展开分析。



1.2 AI 超级公司的典型特征

任何一种重大技术变革都需要长周期才能充分释放其巨大潜能，例如仅第一次工业革命就持续了 80 余年，互联网时代变革也经历了 20 余年；AI 超级公司作为一种不断演化的未来组织，目前正处在逐步浮现的过程中，其过程可能需要十几年甚至更长，这其中还交织着广泛的技术、社会和经济变化。总体而言，AI 超级公司存在三维度典型特征。



图：AI 超级公司的三维度典型特征 来源：阿里云研究院

超级 AI 产品 / 服务：Agentic AI 深度重塑软件产业的形态与用户体验，同时为硬件领域注入强劲创新动能，催生出一批拥有全新形态与体验的智能硬件产品；不仅如此，AI 还在持续推动各成熟产业的服务体验升级，从根本上革新着产业生态与用户交互模式。

超级 AI 基础 / 能力：AI 超级公司基于高效、弹性、安全的智能基础能力，支持完善的数据服务和模型训练、推理及优化服务，并基于 AI 基础设施和 AI 原生架构实现 Agent 的编排、部署及优化。

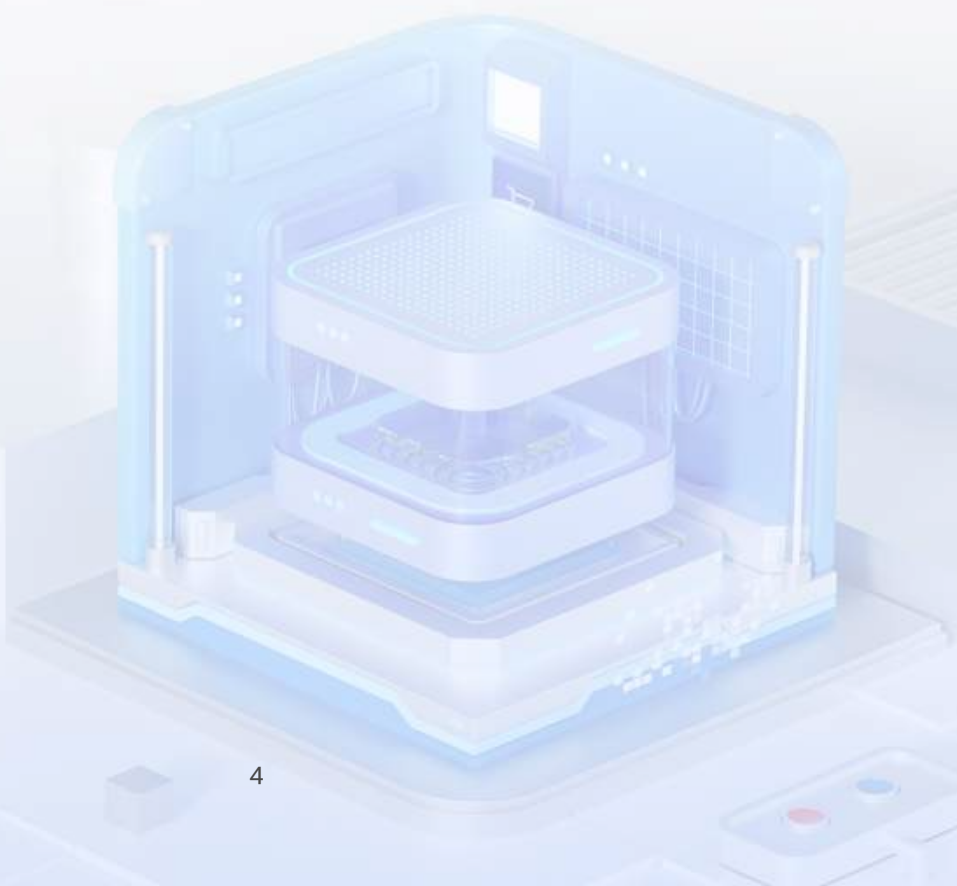
超级 AI 组织 / 架构：Agentic AI 深度融入研发、运营、销售、市场、服务等组织各个环节，重构决策与协作流程。同时在组织方面，随着 AI 个体能力的增强，员工和 Agent 之间的协作方式成为新型生产关系，整体组织形态出现动态变化。

为了便于理解 AI 超级公司的典型特征，后续章节将展开每一个特征背后的内涵，通过拼图方式让大家更立体了解 AI 超级公司从内到外的价值重构。

第二章

超级 AI 产品 / 服务： 从“工具供给”到“智能共生”

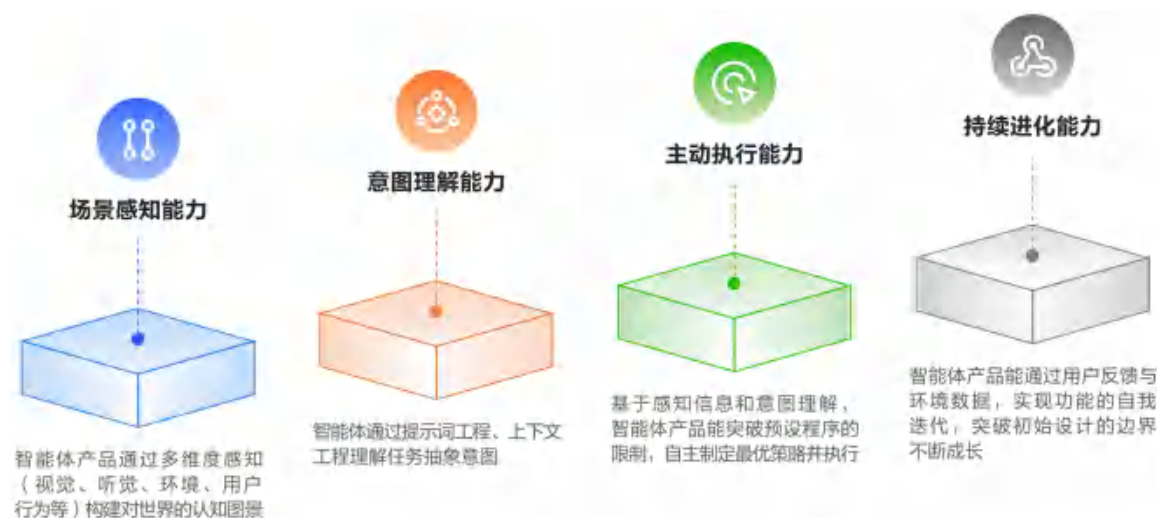
尽管未来有不确定性。但 AI 超级公司的产品形态演进之路仍然有迹可循。AI 赋予软硬件产品更强大的智能感知、自主决策、工具调用与灵活交互能力，基于此能力出发。可以展开对未来硬件设备、应用软件形态以及服务模式的价值展望。



2.1 产品形态的智能化跃迁

2.1.1 从“被动工具”到“主动智能体”

不管是硬件还是软件，传统产品的本质是“被动工具”——功能在出厂时即被固化，用户必须通过明确操作才能实现功能。例如，传统汽车仅能按照驾驶员的操控行驶，空调只能根据设定温度启停，它们按指令行事，既无法感知环境变化，也不能主动适配用户需求。办公软件分门别类，按功能进行使用。而 AI 驱动的“主动智能体”产品，拥有自主意识，能通过多维度感知捕捉信息、理解抽象意图、基于理解主动执行、结合反馈持续进化，从被动执行转向主动创造价值。



图：主动智能体产品的四大核心能力 来源：阿里云研究院

这种主动性体现在四个层面递进。一是场景感知能力，可通过视觉、听觉等多维度传感器构建认知图景，如智能汽车能识别路况、捕捉用户生理状态与情绪变化等；二是意图理解能力，主要通过文本、语音、行为、图片等多模态理解人类任务的抽象意图；三是主动执行能力，能基于感知信息和意图理解，突破预设程序自主制定最优策略并执行，例如文旅助手 Agent 可结合用户的喜好以及游览疲倦程度推荐最适合的景点参观路线；四是持续进化能力，能依据用户反馈与环境数据实现功能自我迭代，例如 AI 设计软件会记录设计师习惯，优化工具链、推送新趋势模板，从被动满足需求升级为引领创意方向。

2.1.2 超级 AI 硬件产品

智能硬件设备担任着将 AI 融入物理世界的角色。而超级 AI 硬件产品的出现也是 AI 超级公司的典型特征之一，随着 Agentic AI 时代到来，硬件产品模式迎来颠覆性重塑，从最开始的 AI 辅助型硬件产品开始，逐步过渡到模型驱动型、原生智能型这几种形态的硬件产品出现。

1.AI 辅助型硬件

这一类硬件产品是最初始的 AI 功能叠加产品，主要是消费电子类硬件产品的 AI 升级。包括少量的场景感知能力。主要在传统硬件产品的基础上增加特定的 AI 功能，作为产品的附加值。AI 并非产品的核心，硬件本身的功能依然是主要卖点。

特点：AI 功能通常是孤立的、针对特定任务的，类似图像识别、语音识别等。例如 AI 增强机顶盒遥控器：通过语音实现电视机机顶盒功能遥控。例如 AI 增强手机：在传统手机相机上，通过 AI 算法实现背景虚化、夜景增强、移除路人等功能。例如智能扫地机器人：增加了 AI 路径规划和障碍物识别，以及语音识别，但其本质还是清洁工具。



2. 模型驱动型硬件

这一类硬件产品开始植入大模型并开启云端协同模式，生成式 AI 深度植入硬件产品中，具备场景感知和意图理解能力，并基于意图完成执行动作。产品的核心价值和关键体验由 AI 来定义和驱动。硬件的设计和服务完全围绕 AI 能力展开，AI 不再是附加功能，而是产品的灵魂。

特点：AI 深度融入硬件产品的核心工作流，具备一定的上下文理解和持续学习能力。例如智能驾驶汽车：其核心竞争力不再是传统的机械性能，而是以完全自动驾驶为代表的、可不断通过远程升级的 AI 驾驶大脑。例如高端智能音箱：不再只是互动音箱工具，而是能够理解家庭场景、联动全屋智能设备、主动提供服务的家庭 AI 管家。

示例：创维酷开科技发布超级智能体，在电视机中内置 AI 大模型，通过端云协同，实现家庭助手功能。它能陪伴用户健身、辅导孩子学习、为出行者查询天气……甚至在你犹豫看什么时，只需一句简单的指令，如“我想看两个男人在天台上决斗的电影”，系统便能找出并推荐“《无间道》”。



3. 原生智能型硬件

这一类硬件产品有强自主意识，AI Agent 交互成为人机关系的主要互动方式，能够准确识别人类意图并完美执行。硬件本身被简化，成为纯粹的“物理入口”或“感官延伸”，其目的是让人类能与具备自主意识的 AI Agent 进行交互。硬件的价值被 AI 服务所取代。

特点：追求无屏幕、自然语言交互，硬件本身能力由背后的 AI 代理动态定义。例如 AI 胸针 / 吊坠：可穿戴的无屏幕设备，通过投影和语音与 AI 进行交互，可独立也可桥接手机进行大模型的云 - 边 - 端互联协同。例如具身智能机器人：硬件只是 AI 思想的物理化身，机器能够自主在物理世界中执行拟人的复杂任务。

2.1.3 超级 AI 软件产品

回顾过去，移动互联网把软件产品从 PC 桌面搬上手机，SaaS 把本地程序拉上云端，今天的 Agentic AI 正在从根本上重塑软件的基本逻辑，Agent 驱动软件从底层开始思考如何转型为智能体生态的一部分。尽管复杂软件和 Agent 在很长时间内将长期共存，但软件 Agent 化的趋势是明确的，软件的价值核心正从“提供功能供人使用”，转变为“自主完成人类委托的目标”。我们正在从一个由应用构成的世界，迈向一个由代理构成的世界。未来 Agent 将成为重要的软件形态。AI 影响下的软件演进主要有以下几类：

1. 软件智能助手

AI 被嵌入到现有的软件应用中，它能理解用户的任务上下文，提供建议、自动完成部分操作，但最终的决策和驱动权仍在人类手中。

特点：AI 是被动的、辅助性的，响应用户的指令或提供建议，通常在单一应用内工作。例如微软 Copilot：在 Word 中帮助起草文档，在 Excel 中分析数据，在 Teams 中总结会议，但每一步都需要用户确认和引导。

2. 任务型 Agent

传统软件拆分为多个功能（上传、编辑、保存、发送等），用户需要自己组装功能以完成任务；用户是功能的调用者和流程编排者。Agent 则演变成软件的重要形态，接收任务目标、拆解任务、选择工具、安排顺序；用户变成了目标委托者，系统则成为代理执行者。

特点：目标驱动，具备自主规划和工具使用能力。它可以跨越多个应用或服务来完成一个复合型任务。例如 AI 旅行代理：告诉它“下周帮我预订去上海的性价比最高的旅行方案，包括机票和酒店”，它会自主地浏览各大网站、比较价格、完成预订并生成行程单。

3. 协作式 Agentic AI

软件不再是单个应用或单个 Agent，而是一个由无数个专业化、可互操作协同的 AI Agent 组成的去中心化网络。这些代理能够相互发现、沟通、协商并协作，以完成复杂或开放式的任务。同时允许失败重试、反思重规划；在复杂场景下表现出容错性和应变能力。

特点：软件的形态从“实体”变成了“关系”和“协同”。本质从预设流程到动态策略编排，软件变得更有判断力。例如 AI 自主供应链：销售 Agent 接到订单后，会自动与库存 Agent、生产 Agent 和物流 Agent 进行协商，动态安排生产和配送，整个过程无需人工干预。

2.2 服务模式的预见式重构

2.2.1 从“响应需求”到“创造需求”

传统服务模式中，企业往往在用户明确提出需求后才被动响应，而 AI Agent 驱动的服务彻底扭转这一被动逻辑，它通过多维度数据（用户行为、生理特征、环境变化等）挖掘用户未被察觉的潜在需求，将“满足需求”升级为“创造超预期价值”。例如健康管理 Agent，不仅在用户查询“血糖偏高怎么办”时提供解答，更可通过工具调用持续监测用户的血压心率、睡眠质量、餐饮记录等数据，当发现用户连续一周深夜血糖波动异常且膳食纤维摄入不足时，会提前推送包含餐饮调整建议、轻度运动计划等个性化预防方案，并联动社区医院预约血糖复查，让服务从事后应对变为事前预防，超越用户的常规期待。

示例：在大模型技术和 AI Agent 智能体的新技术赋能下，美年健康已经展开多个场景化应用，包括数智健管师“健康小美”、智能主检医生、血糖管理师“糖豆”、智能销售助理“美年小星”等智能体。其中健康小美能建立全生命周期的数字健康档案，生成多学科报告并进行风险分级，还可为客户制定个性化健康计划，向用户提供全天候专业实时咨询。



2.2.2 服务的“全生命周期陪伴”

在 AI 超级公司，AI 驱动的“全生命周期智能陪伴”，将服务贯穿于用户与产品交互的每一个关键节点，从用户初识产品的认知阶段，到日常使用的体验阶段，再到反馈建议的优化阶段，最终到产品随用户成长而迭代的进化阶段，形成完整闭环，让用户与产品从简单的使用与被使用关系，升级为共同成长的共生关系。以教育 Agent 为例，它并非仅在用户学习某门课程时提供辅导，在认知阶段，会根据用户的学科基础、兴趣偏好推荐适配的选课方案；在使用阶段，会实时分析学习和解题数据，动态调整知识点讲解节奏与习题难度；在反馈阶段，会收集用户对课程内容的建议，反向优化教学模块；甚至在用户完成当前学业后，还会结合其能力特质与行业趋势，提供长期职业规划指导，真正实现从短期学习辅助到终身成长陪伴的跨越，让产品始终与用户的需求同频共振。

示例：山东瀚海云教育科技有限公司基于通义大模型 + 多模态 + OCR 构建阅卷 Agent。过去传统人工阅卷需逐题阅读、打分、写评语，尤其主观题较多的试卷费力耗时，且老师对班级整体知识掌握情况只有一个大致的印象，无法实现精细化、数据化分析。基于阅卷 Agent，可从长时间的传统“人工批改”转变为“AI 主判 + 人工校核”；阅卷流程效率显著提升，减轻教师负担的同时降低人工误差；此外批改一致性与可追溯性增强；系统自动汇总班级与个人的薄弱知识点，实现学生对知识点掌握情况的精确数据分析，为后续精准讲评提供指导。



2.3 生而全球的跨越式发展

在全球化竞争加剧与跨国业务扩张的背景下，传统企业面临“地域文化差异大、跨区域资源协同难、全球合规标准复杂”等痛点，而新一代人工智能凭借多语言适配、实时跨域协同、运营动态调整的核心能力，成为 AI 超级公司实现生而全球创新发展的关键载体——它能打破地域与流程的限制，让企业从业务起步阶段就具备服务全球市场、整合全球资源的能力，实现从区域经营到全球协同的跨越式突破。

在业务服务端，凭借 Agent 多模态语言能力与本地化适配，可支持几十种主流语言实时交互（如中东客服规避宗教敏感词），并结合区域消费习惯、政策与节日（如中国“双 11”、欧美“黑五”）调整营销售后策略，自动适配支付接口与合规要求，实现全球用户无差别服务；在资源协同端，借助 AI 整合全球工厂数据（产能、成本、技术）完成跨国生产调度以匹配最优路径，同时实时追踪全球供应商、物流与库存实现供应链整合，风险发生时自动切换备用资源，并结合关税政策优化策略以降低成本；在风险管控端，Agent 支持实时更新各个国家法规（如 GDPR、《数据安全法》）并自动调整业务流程（如数据本地化存储、用户隐私权限设置），还可整合地缘政治、汇率等风险数据推送应对方案，助力企业规避跨国违规风险。

示例：爱诗科技作为 AI 视频领域的代表企业，自成立之初即采取全球化战略，已在全球市场形成规模化影响：PixVerse（拍我 AI）全球用户规模已突破一个亿，若干模板化产品（如“变身特效”“3D 手办”）爆火，模板全球曝光量已突破百亿。爱诗以多代自研视频大模型与模板化生成为核心，将复杂提示词封装为一键创作，实现秒级生成高质量视频、并通过云-边-端部署与阿里云的跨区复制、算力优化与实时分析能力，显著加快训练与上线节奏。爱诗将技术基建、产品工程化与本地化运维同步推进，成功把国内研发能力复制为可规模化的全球服务能力。



第三章

超级 AI 基础 / 能力： 支撑组织进化的“智能基建”

AI 超级公司的演进，核心在于逐步搭建起 AI 超级基础能力。这套基础能力将直接决定企业未来价值创造的速度与智能密度，是其在数字经济格局中建立代际优势的根本。其核心主要包括多模态高效数据平台、面向 AI Agent 开发、构建的 AI 基础设施和 AI 原生应用架构，并以此为根基开发构建 Agent 应用。虽然 AI 原生架构尚无统一的标准，但其形态正被 Agent 技术的需求所塑造和定义：它必须是一个能够为 AI Agent 提供持久数据流、统一工具调用和无缝协作能力的原生环境，这正是 AI 超级公司自主进化的基石。



3.1 多模态高效数据平台

在 AI 时代，数据规范和治理的重要性推向了新的高度，未来 AI 超级公司以大量 Agent 协同、多层级模型矩阵为核心竞争力，而这一切都高度依赖高质量、高可用的数据支撑——无论是基础大模型训练、行业垂类模型优化，还是 Agent 的实时智能决策，都离不开海量合规、精准、有序的数据基础。由于企业运营过程中存储的数据非常多元化，多模态数据按照分类适配处理逻辑，需要制定统一的数据标准和规范格式，确保跨业务、跨场景数据可互通；并建立数据清洗与质量校验机制，过滤无效数据、修正偏差数据，保障数据准确性。可以说数据规范和治理的完善程度，直接决定了 AI 超级公司数据价值的释放效率，也影响着模型迭代速度与 Agent 服务质量，其重要性随 AI 业务深化不断凸显，成为不可替代的核心能力之一。



图：数据治理流程示意图 来源：阿里云研究院

要顺畅实现数据治理，AI 超级公司的数据平台在底层技术架构上也需要进行技术变革，演变为多模态、服务化的智能数据底座。企业传统数据库和数据技术已无法满足 AI 时代的需求，取而代之的是由云原生等技术构成的“多模态数据库”、“大数据平台与数据中台”。

云原生多模态数据库：云原生多模态数据库不止于“存储数据”，更在于通过日常数据处理能力，赋能 AI 技术与业务的深度耦合，为 AI 超级公司的模型后训练、RAG 增强提供数据支撑。例如工业企业的 AI 质检模型，可通过数据库存储的历史检测数据，用于模型迭代时“误差分析”（如对比不同批次产品的缺陷数据，优化模型识别精度）；同时还可作为 AI 超级公司的 Agent 应用提供数据基础。例如零售场景的导购 Agent，需通过向量数据库存储“商品特征向量”以记忆商品信息，通过图数据库构建“商品 - 用户 - 场景”关联图谱以推理用户需求，通过文档数据库存储用户历史交互日志以优化导购行动。

大数据平台与数据中台：两者构成了数据的“中央厨房”和“服务总线”。大数据平台负责对海量原始数据进行批处理和实时流处理，完成模型训练前的数据加工和特征工程等重度计算任务。而数据中台则将这些原始、复杂的数据处理能力，封装成标准、易用的数据服务或 API 接口。为 Agent 的工具库提供了最核心的数据类工具，使得 Agent 无需理解底层数据库的复杂性，只需调用一个简单的服务就能获取所需信息，极大提升了其行动效率和应用开发速度。

示例：福田汽车为应对商用车存量市场竞争与数据系统不互通的挑战，携手瓴羊引入 Dataphin 数据治理平台，对分散在近 20 个业务系统中的客户数据、产品数据及用车行为数据进行全面整合、清洗与治理，构建了统一的数据资源中心与“人－车－路－货”数据标签体系，关联超 1000 万数据资产。这一数据治理工作不仅实现了数据资源的标准化与资产化，更打通了原本孤立的系统，为业务场景如精准营销、售后服务和用户运营提供了可靠数据支撑。整体上，该举措为福田推进 AI 应用奠定了高质量的数据基础，是实现智能化运营的重要前提。



3.2 AI 基础设施与 AI 原生架构

3.2.1 AI 基础设施

AI 基础设施是支撑大模型训练与服务化落地的底座，包含计算、存储、网络、安全等要素，并需同时满足 AI 大模型高吞吐训练与低延迟推理的需求。

在核心硬件层面以 GPU 为主，同时整合 IPU、NPU、FPGA 及专用推理芯片等异构算力，通过高速互联构建包含计算、分布式存储与多级高速缓存的弹性云端算力池；并采用并行文件系统、对象存储与冷热数据分层等机制，保障训练数据与特征流的高效读写。

能力层面支持大规模分布式训练（数据并行、模型并行、混合并行、混合精度）、训练流水线化（数据预处理、增强、同步检查点）、以及推理加速（量化、蒸馏、剪枝、批处理与动态批次），并通过统一的模型管理与 LLMOps（大语言模型运维）平台实现训推一体（模型注册、版本管理、A/B 测试、自动化 CI/CD、监控与回滚）。

由于 AI 基础设施建设存在一定的技术和资金门槛，企业无需完全自建全部能力，公共云厂商的弹性 AI 服务（弹性 GPU、训练集群、托管推理、模型仓库与 LLMOps 工具）可以显著降低初期投入与运维复杂度，企业可采用更灵活的部署策略，快速迭代并按需扩展。



3.2.2 AI 原生架构

AI 原生应用架构是以大模型为认知核心、Agent 为任务编排与执行单元、数据为决策及个性化支撑，依托工具实现环境感知与实际执行，最终构成具备智能能力的应用体系。其中包括一些典型的功能模块。



图：AI 原生应用架构图 来源：阿里云

API 网关：作为所有客户端请求访问后端服务的统一入口，在 AI 应用架构中，它负责对 Agent 对外暴露的接口进行认证、授权、流量控制和安全防护，确保只有合法、合规的请求才能到达 AI 服务；同时它还能路由不同类型的 API 和 AI 请求（如对话、图像生成）、管理调用频率、实现熔断限流，并集中监控和日志记录，从而提升系统的安全性、稳定性和可维护性，是连接用户侧与 AI 能力的核心枢纽和关键基础设施。

AI 网关：AI 网关不仅实现身份鉴权，还要完成流量控制、模型代理、防刷防攻击等一系列安全防护能力（例如基于 Token 级别的精细化流量控制，确保入口流量的安全防护）。此外，随着通信协议从短连接向流式传输演进，AI 网关不仅要支持传统的 API 路由和鉴权，还必须原生支持 SSE（Server-Sent Events）或 WebSocket 等流式协议，实现边生成、边返回的能力。这是保障模型用户体验和系统稳定性的基础。

云原生服务管理平台：在 AI 时代，云原生服务管理平台超越了云原生作为服务注册中心和配置中心的角色。成为 Prompt 提示词工程的动态管理中心以及 MCP 服务注册中心角色。可将后端的工具类服务（比如数据库查询、搜索引擎、高德地图、第三方 API 等）统一注册到云原生服务管理平台，并通过 MCP 协议暴露给大模型调用。这样外部接口就能被模型“理解”并按需调用，形成真正的工具链集成能力。从而实现 Agent 智能体自动规划与执行任务的基础。

AI 观测 & 评估: 还需建立完整的 AI 可观测性体系与数据评估机制，功能包括调用链追踪 --- 定位哪一步出了问题；提示词效果评估 --- 量化不同提示词的准确率；知识召回率分析 --- 判断 RAG 是否命中有效内容；生成结果质量打分 --- 自动识别幻觉、错误等低质输出。这样才能系统地优化 AI 应用的稳定性和输出质量。

事件驱动架构：通过引入消息队列作为核心中间件，实现了请求与处理的解耦，极大提升了系统的并发能力和资源利用率。同时结合流式返回机制，可以在生成过程中逐步推送结果，兼顾实时性与稳定性。

工具集：MCP 已经被视为 AI 原生时代“新 API 标准”，MCP 协议的核心思想是为 API 注入语义元数据——通过标准化的描述格式，让模型能够理解每个参数的含义、调用条件和返回结构。这样模型可以像程序员一样，自主选择合适的工具、构造正确的请求、解析返回结果，真正实现自动化工具调用与任务编排。

AI 原生架构的意义远不止于技术层面的迭代升级，更意味着底层逻辑的根本性转变。它打破了过去“以服务为中心”的模式，转向“以模型为中心”的全新范式——大模型成为整个架构的核心引擎，所有服务、工具和流程都围绕模型能力的高效释放与场景适配来设计。基于这样的架构，企业能够构建起真正贴合 AI 时代特征的原生应用体系，真正释放 AI 对业务的重塑价值。



3.3 Agent 商业应用与开发构建

Agent 应用将长期呈现“商业标品”与“定制开发”并存的格局。一方面，市场上已涌现出大量可直接商用的标准化 Agent 产品，覆盖客服响应、会议助理、文档辅助等通用场景，例如电商领域的智能客服 Agent 可自动处理订单咨询、售后问题，企业无需投入研发资源，通过 API 对接或 SaaS 化部署即可快速启用；另一方面，对于涉及行业专属规则、核心业务逻辑的场景（如金融领域智能风控 Agent、制造业设备故障诊断 Agent），标准化产品难以满足个性化需求，需要基于业务场景进行定制开发，通过适配专属数据、嵌入专业算法，让 Agent 具备解决行业特定问题的能力。

从企业实践角度，如果商业应用 Agent 成品能覆盖大部分常规需求（如通用会议纪要整理、基础客户问答），可优先选择直接部署，既降低开发成本，也缩短落地周期；同时需针对性储备 Agent 定制开发能力，可通过组建专项技术团队、沉淀行业专属开发框架、建立与业务部门的协同机制等方式，确保能够快速定制专业 Agent 解决特殊业务痛点。



3.3.1 Agent 商业应用

Agent 凭借自主决策、流程自动化、场景适配等核心能力，正在逐步重塑企业运营与用户服务模式，既为企业带来降本增效、模式创新等核心价值，也为用户带来更精准、更便捷的交互体验；其通用商业应用场景广泛，可基于行业特性、岗位需求、专业任务、服务对象划分为以下几类：

1. 行业垂直 Agent

场景：面向电力、金融、医疗、教育、公共事务等行业场景，内置行业规程、合规约束、专有知识库与领域模型，支撑电力调度、金融风险识别、医疗临床决策、教育个性化教学与智能政务服务等复杂流程。

特点：需要嵌入行业规则与监管合规约束，并接入专业知识库（行业 / 企业专属数据），需强调审计与可解释性。

2. 通用职能 Agent

场景：面向企业客服、市场、人力资源、法务、财务等通用职能岗位，提供标准化对话模板、流程编排等能力，包括智能客服与工单自动化、市场营销智能投放、潜在客户智能挖掘、HR 智能招聘与入离职自动化、合同智能审核、财务发票自动识别及智能报销等场景。

特点：深度集成 CRM / 工单 / HR 等专业软件系统，并接入企业专属内部数据，支持多渠道交互与过程监控。

3. 任务专用 Agent

场景：面向专业应用领域场景，例如安全情报与威胁检测、智能化数据分析、代码生成与自动化测试等场景。用于 AI 分析、威胁检测、智能编程、自动化测试等点状任务。

特点：常作为商业 Agent 的能力组件，强调接口化、可编排性与高可靠性。

4. 个人助理 Agent

场景：面向企业员工个人的工作助理，类似会议智能摘要、研究与信息智能检索、文档写作辅助、多语言智能翻译等场景。侧重多模态交互、上下文记忆与个性化服务，提升个体工作效率与决策质量。

特点：多模态交互、上下文记忆与个性化，其中隐私保护与数据隔离需要进行严格管控。

未来随着大模型能力的提升与 Agentic AI 化程度的加深，Agent 在企业中的应用将从“单一环节赋能”走向“全业务链路协同”，成为 AI 超级公司的核心载体，推动企业向高阶智能协同跨越。

3.3.2 Agent 开发构建

Agent 开发构建是将大模型能力工程化为可用、可控、可迭代的业务服务全过程，主要包括 Agent 创建、配置、部署和运行等环节。通常具有四大特点：技术集成性（大模型调用、提示词优化、上下文工程、各类插件、知识库等）、操作易用性（可视化、模块化、工具即插即用）、功能扩展性（可扩展 Agent 能力和应用场景）、发布灵活性（流程自动化执行）。企业级 Agent 构建根据面向对象的不同，主要包括低代码 Agent 开发平台、全能力高代码 Agent 开发框架两部分。



图：Agent 开发构建主要能力模块 来源：阿里云

低代码 Agent 开发平台：主要面向平民开发人员以及技术开发者（提效），低代码可视化模式可以在编写少数代码的情况下构建、发布和管理 AI 驱动的 Agent。甚至通过图形可视化的托拉拽方式构建 Agent，从而提高个人生产力以及标准化业务效率。

高代码 Agent 开发框架：主要面向专业技术开发者，开发者通过深度编码实现 Agent 精细化定制的工具体系。以多语言运行时、异步调度、资源隔离为基础层保障扩展；核心功能包含可编程的任务规划、工具调用、记忆管理、环境交互及反馈学习模块，适配不同业务场景；配套编码辅助、调试监控、部署运维工具链降低开发复杂度；此外通常还支持集成企业中间件与多主流大模型，实现 Agent 全流程可控。

Agent 构建还需考虑平台的生态能力。包括大模型供应商、Agent 配套的插件 / 功能模块的专业开发者、API 供应商等。生态能力决定了平台的吸引力、活跃度、可持续性，一个拥有丰富生态、开放合作、可持续发展且治理有方的平台，无疑是企业实现业务智能化转型，迈向 AI 超级公司征程的最佳伙伴。

3.4 端到端安全与治理

AI 超级公司的超级基础能力还必须将安全、合规与可控性从设计端贯穿到生产端，构成“设计即安全、运行可审计、迭代可追溯”的闭环。具体可包括：

- 将身份与最小权限访问、网络隔离与加密、密钥与机密管理纳入基础设施；
- 对数据实行分级管理、脱敏与访问审计，采用数据版本化与血缘追踪以保证可回溯性；
- 对模型实行备案注册、版本管理与风险分类，并嵌入单元 / 回归 / 安全 / 偏差 / 可解释性测试与自动化质量门控；
- 运行时实施实时监控、异常检测（输出漂移、对抗攻击、策略违规）、日志与端到端事务追踪，并在关键路径启用灰度发布与自动回滚策略；
- 针对第三方模型与供应链，执行合约性评估、完整性校验与供应商审计；
- 隐私保护涵盖脱敏、差分隐私与联邦学习等技术选项，配合法律合规与数据主权策略。

此外，还须常态化开展红蓝对抗测试与仿真演练，并建立明确的组织流程（模型审批、上线门控、应急响应与问责机制），用可量化的 KPI（如审计覆盖率、偏差检测率、平均回滚时间、合规缺陷修复时长）驱动持续改进。最终目标是把安全与治理内置为产品特性，使智能能力在可控、可解释与可持续的前提下大规模交付。



第四章

AI 超级组织 / 架构： 向“液态协同”结构进化

Agent 正推动企业组织架构向“人类员工 - 数字员工”共生网络进化。这种协同模式下，企业通用流程开始出现智能化变革，并且企业组织架构也在逐步发生变化，这种变化和影响主要体现在推动组织架构向扁平化、灵活化、液化化转型，并促进高效协作机制的形成。对于未来的企业领导者而言，最大的挑战不再是管理员工，而是设计和治理一个人机共生的、能够不断适应和创造价值的智能组织系统。对于未来的员工而言，其职责将从工作“执行者”转变为其个人 Agent 的“管理者”和“教练”，从而形成组织集体智能的指数级放大。



4.1 通用职能流程迈向智能化重塑

对于大多数企业而言，应用 AI 的路径并非一开始就颠覆核心业务或生产流程，而是从企业通用流程的智能化改造开始，这是相对务实的切入点。市场营销、人力资源、客户服务、法务、财务等职能部门往往是首批被改造的领域。原因在于这些通用环节的工作流程相对标准化，高度依赖文档处理和知识检索，其智能化改造能够带来清晰、可量化的投资回报，且实施风险相对可控。

市场营销：AI Agent 可以辅助分析市场数据，协助生成多样化的文字、图片和视频类的营销文案初稿，并自动化进行市场趋势分析和行业舆情预警。

人力资源：在招聘环节，AI Agent 可用于自动筛选简历、进行初步的岗位匹配，并与候选人进行智能互动；在入离职环节，AI 可处理标准化的入、离职流程手续，提升人力资源流程效率。

法务部门：AI Agent 能够快速起草标准合同，并自动审查外部合同的风险条款。秒级读取合同文件，对照企业内部的法务知识库和风险条款模型，自动识别、标示出不合规或高风险的条款，并提供修改建议，将法务人员从繁琐、重复的初审工作中解放出来。

财务部门：AI Agent 可以自动处理发票、审核报销、并完成月度结账等重复性工作。同时还能监控预算执行情况、分析业务数据以预警异常情况，此外还能自动审阅合同财务条款、识别合规风险。使得财务团队能从事后记账转向事前预警和事中控制。

客户服务：在现有问答机器人基础上，增强其多轮对话和调用内部系统工具的能力，使其能处理更复杂的查询，如订单状态跟踪、退换货申请等，分担人工客服压力。

数据分析：AI Agent 可实现从数据接入、清洗到洞察生成的自动化闭环。例如瓴羊的用户行为分析工具、智能 BI 平台等产品，可自动整合企业内外部多源数据，基于数据分析模型与行业模板，自动生成标准化分析报告（如月度销售复盘、用户转化漏斗分析等）。

通用流程智能化的核心价值体现在两个方面：首先显著提升运营效率与执行标准的一致性，直接带来企业成本效益；其次 AI Agent 承担了大量重复性的流程化任务，使得员工能将更多精力投入到需要战略判断、创造性思考和复杂沟通的增值工作中。因此推动通用流程的智能化，不仅是降本增效的战术手段，更是 AI 超级公司构建 AI 原生能力、培育人机协同工作文化的关键一步。

4.2 从增强组织到液态组织的演进

4.2.1 AI 增强型组织

这是 AI 渗透到企业组织最初级的形态，AI 作为“生产力工具”被引入，嵌入到现有的工作业务流程中，以增强员工的效率。组织的基本架构（层级、部门、汇报关系）保持不变。Agent 只是人类助手，决策权和任务驱动权完全在人，组织传统的金字塔或矩阵式结构得以保留。例如市场部员工使用 AI 工具生成文案和图片，但部门的目标、KPI 和审批流程不变；研发团队使用 AI 辅助编程，但项目管理、团队协作和代码审查流程依然由人主导；管理层通过 AI 工具分析报表，以辅助决策，但决策过程本身没有改变。

示例：一汽红旗推出 AI Agent，能够对客户语音数据进行转写和总结提炼，结合客户行为数据和兴趣点，评估客户潜在购买意愿，并制定定制化的营销话术内容和促销策略，提升客户粘性和交易转化率。帮助一线营销团队更精准地追踪和管理客户，提高营销效率和客户满意度。

示例：作为 SaaS-ERP 领域的头部企业，用友集团的业务复杂多样，服务大、中、小微等不同企业，覆盖财务、供应链、制造等十大领域。截止 2025 年 8 月，用友超过 60% 的研发人员正在使用通义灵码，已覆盖核心代码研发场景。其中，用友的 AI 代码生成占比已经达到 37%，采纳率高达 29%。

示例：百果园推出 AI 智能体，能够对客户上传的退货图片进行快速识别，精准判断水果的品类、状态，并智能调用知识库中的审核标准与参考图进行比对，从而实现秒级自动化判定并给出相应建议，大幅提升服务效率与标准一致性，在降低人力成本的同时优化客户体验。



4.2.2 人机协同型组织

这个阶段的企业组织开始进行结构性重组，以最大化人与 AI 的协同效应。Agent 不再仅仅是工具，而是被视为数字员工，能够自主执行完整的任务流程。这个阶段开始出现由人类管理者和 AI Agent 组成的混合单元团队。人类角色向“管理者”、“教练”、“验证者”转变，企业迎来“超级员工”时代。业务流程开始出现明显变化。传统中层管理者转变为设计和优化人机协作流程，并处理 AI 无法解决的异常情况。例如：客户服务部重组为小型的人类专家团队和一个庞大的 AI 客服坐席团队。AI 处理 95% 的常规请求，人类专家则专注于复杂情感问题和 AI 模型的持续训练和微调。

示例：普华永道 2025 年 5 月针对 AI Agent 的调查，42% 采用 Agent 的公司高管表示，他们正在围绕 AI Agent 重新设计业务流程；50% 的高管认为，由于 AI Agent 的存在，他们的运营模式将在两年内发生翻天覆地的变化；66% 采用 Agent 的人表示，他们通过提高生产力实现了可衡量的价值。

4.2.3 智能液态型组织

这是最先进的 AI 超级公司组织形态。组织本身变得像一个“去中心化的软件系统”。其核心由 AI 代理网络构成，能够根据外部市场变化和内部目标，动态地自我组织、调整和进化。决策权大量下放给 AI 代理。组织从“命令 - 控制”模式转变为基于规则和协议的“感知 - 响应”模式。这个阶段不再有固定的部门或团队。AI Agent 会根据特定项目或任务临时组成团队，通过实时联动跨部门数据，实现从决策到执行的敏捷闭环，同时支撑大规模业务协同，任务完成后自动解散。组织结构处于液态协同阶段，极度灵活、敏捷。

示例：某新产品创意被提出后，项目管理 Agent 自动启动，它在全网（包括内部和外部）寻找并雇佣产品设计 Agent、市场分析 Agent 和软件开发 Agent，并协调它们完成工作。Agent 自主进行预算分配、风险监控和合规审计，只有在出现重大异常或需要战略调整时才需要人类干预。

4.3 人机协作开启超级员工时代

4.3.1 人机协作新型能力体系

超级 AI 公司时代，AI 介入彻底重构了人机分工逻辑，Agent 主动承接重复性工作，帮助每一位员工成为超级员工，将人类从机械劳动中解放出来，使其能聚焦于需要战略思维、创新能力与情感温度的核心领域，这种分工模式下，AI 成为基础服务执行者，人类则成为复杂问题解决者与情感连接者，人机协作既提升了整体服务效率，又保障了高价值场景中的人文温度。

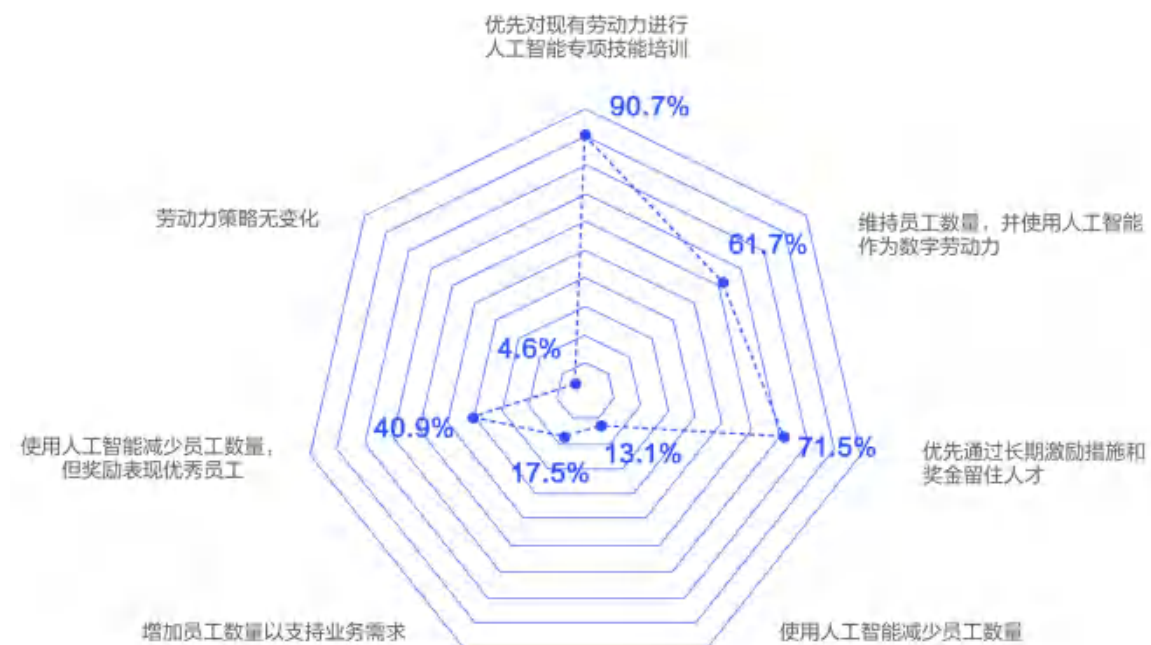
这对企业员工提出了全新的能力要求，新型能力并非要求员工精通 AI 底层技术，而是聚焦于“让 AI 更好地服务业务需求”，这套新型能力体系，本质上是让员工成为 AI 协作指挥官——既能清晰传达业务需求，又能保障 AI 输出质量，最终实现人类主导方向、AI 提升效率的协作闭环。以下五种能力为未来企业员工需要掌握的能力体系示例。



图：人机协作的新型能力体系要求示例 来源：阿里云研究院

首先是提示词 / 上下文工程，通过优化提示词，以及接入相关数据，为大模型提供最相关优质的上下文；其次是数据治理，员工需要具备把业务数据转化为 AI 可识别格式的能力，确保高质量数据可被调用；场景化模型调优，则需依据具体业务场景调整 AI 模型参数，比如客服场景中 AI 解答售后纠纷类问题准确率低时，可补充案例、调整关键词权重；AI 结果校验，需要对 AI 输出内容进行合理性与准确性审核，这里员工可结合业务常识校验数据逻辑；最后是隐私与合规把控，员工要掌握数据脱敏、权限分级等合规操作，确保人机协作合规。

问题：当你考虑用人工智能加强在人力和人才管理中的作用时，你认为公司在未来 2 年内应该考虑哪些策略？（选最有可能的前三项）



图：AI 加强的人力资源策略（企业管理者调研） 来源：阿里云研究院 样本 n=500



4.3.2 AI 思维与 Agent 管理能力

AI 超级公司要形成“全员 AI 素养”，从核心管理高层到全体员工，都需建立统一且适配岗位的 AI 思维和能力，形成上下同频、协同发力的 AI 联动生态。

对管理高层而言，主要体现为 AI 战略思维。即能将 AI 战略与组织长期目标绑定，而非局限于短期降本需求。例如零售企业管理层，需明确 AI 不仅是优化库存的工具，更能通过用户行为分析驱动产品创新、重构会员体系，让 AI 成为业务增长的核心引擎；同时需理解 AI 能力边界，避免落入“AI 万能论”误区，从而合理规划 AI 投入与人工决策的分工。

未来最有价值的员工不再是执行任务最快的人，而是最懂得如何委托、引导和训练其 AI Agent 的超级员工。因为在不远的未来，每个人都将配备专属的 AI Agent。员工的核心职责将从“执行者”转变为其个人 Agent 的“管理者”和“教练”。例如清晰地设定目标与约束、高效地提供上下文与反馈、明智地评估 Agent 的工作成果并进行纠偏。当这种 Agent 管理能力成为组织内每一个人的基础素养时，整个公司的运营模式将被彻底颠覆。它不再是个人生产力的简单叠加，而是组织集体智能的指数级放大。

示例：麦肯锡内部已部署超过 1.2 万个 AI 智能体，这些多样性智能体有的可以一键润色报告，有的可以审查方案中的漏洞，确保推理严丝合缝，有的可以快速消化海量客户访谈和研究文献，并给出核心洞见。麦肯锡的目标是在不久的将来，为每一位员工都配备一个专属 AI 智能体。（华尔街日报报道）

问题：您是怎么看待未来公司加大力度使用 AI 工具 /AI 大模型的？



图：员工对 AI 大模型的接纳态度 来源：阿里云研究院调研 样本 n=1500

4.4 共生性文化适配与泛在治理

4.4.1 基于 AI 迭代的机制文化

AI 超级公司需要建立起基于 AI 的人机共生、学习机制文化，从“追求零错误”到“拥抱迭代”。企业员工在监督 Agent 执行工作的过程中，不再将 AI 的错误视为需要避免的“Bug”，而是将其视为驱动组织进化的数据燃料。文化上积极鼓励基于 AI Agent 应用的快速实验，并建立起高效的“实验 - 复盘 - 反馈 - 优化”闭环。将 AI 的每一次不完美的失败数据都转化为一次反馈、学习和迭代的机会，从而打造出一个能够自我完善、持续进化的智能生命体。

这种文化的本质，是让 AI“实验”成为日常工作的一部分，让“学习”和“迭代”贯穿工作的每一个环节——组织提倡基于 Agent 应用的快速实验、快速学习、快速进化，这也是 AI 超级公司保持行业竞争力的关键之一。

4.4.2 基于 AI 伦理的泛在治理

传统企业为追求技术突破或商业效率，可能忽视 AI 应用的潜在风险：比如推荐算法为提升点击量刻意制造“信息茧房”、风控模型因数据偏见导致对特定群体的歧视等等。这些问题不仅损害用户权益，更会透支组织长期信任。未来 AI 超级公司的核心竞争力，需要超越单纯的技术创新，将“AI 向善”从合规要求升级为文化内核，通过价值观渗透与制度落地，实现创新速度与伦理责任的动态平衡。

在落地实施过程中，企业可制定并公开伦理准则与影响评估模板；在产品 / 模型设计阶段执行伦理影响评估；设立伦理委员会或伦理审查岗。通过制度与文化双管齐下，将伦理治理转化为组织的实践能力。这种基于 AI 伦理的泛在治理，本质上是企业对“长期主义”的坚守，当 AI 向善成为全员共识，不仅能规避技术滥用的风险，更能让企业在用户、社会层面建立不可替代的信任基础。



4.5 组织边界的模糊化与生态化

随着超级 AI 公司的发展，Agent 成为企业对外连接的核心模式，组织边界开始变得模糊。企业不再只是在供应链上单向交易，而是把自己的技术能力和数据有选择地开放给上下游伙伴、客户和生态合作者，大家一起协作创造价值。参与方由过去各自为政转为共同发展，形成跨公司、跨领域的生态协作网络。此时商业关系更多基于互惠和信息共享收益，而不只是单纯的买卖合同关系。要在这种新形态中稳健运营，企业间需要建立清晰的接入规则、治理和激励机制，既鼓励开放与协同，也保护核心资产与合规底线。



第五章

AI 超级公司发展阶段评估体系

5.1 AI 超级公司的进化与阶段

在技术快速变革的 AI 时代，有少数公司（例如大型科技公司）生来就是 AI 超级公司。它们的组织架构、商业模式乃至文化基因，均围绕 AI 的发展而构建的，其企业价值主张本身就是“智能”。然而，对于绝大多数拥有深厚行业根基的传统企业而言，通往 AI 超级公司的道路并非一蹴而就的革命，而是一场目标明确、分步骤分阶段的进化之旅。

我们通过 AI 技术发展的趋势以及行业应用的发展实践，结合众多企业高管的调研访谈综合判断，未来 AI 超级公司的发展大致可分为三个阶段，每一步都标志着 AI 在组织中的角色升级：

表：AI 超级公司发展三阶段

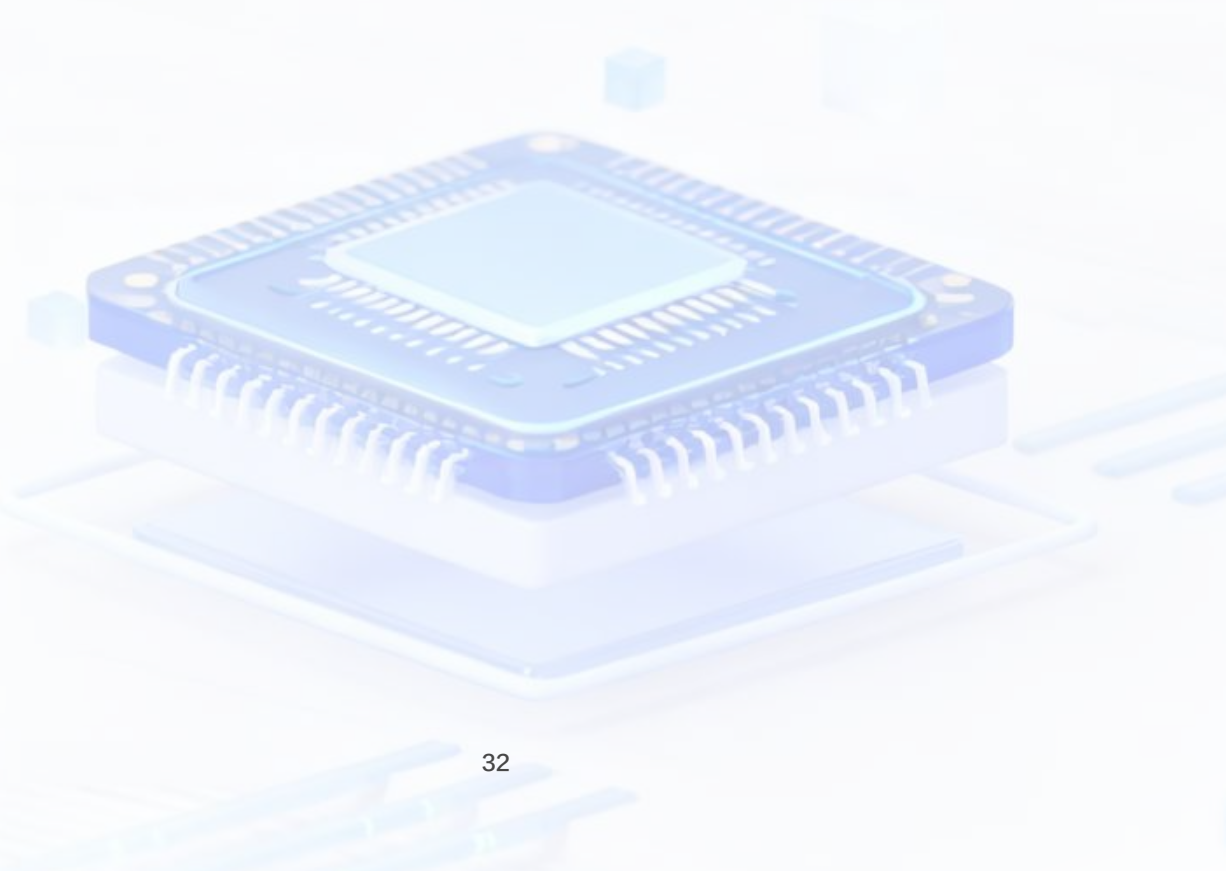
阶段	AI 角色	人类角色	典型场景
阶段 1：AI 协作 Agent 应用普及， 人机协作启航	Agent 成为员工得力助手，聚焦单一简单任务，提升局部效率	人类委托，Agent 作为效率工具，提升工作质量	示例：银行基于 Agent 梳理解析复杂信贷数据，将中小企业贷款审批时效从 3 天压缩至 0.5 小时
阶段 2：AI 协同 Agentic AI 深度协同，重塑业务流程	AI 智能体具备更强的感知、自主学习与决策能力，能够相互协同承担更复杂的任务	人类驱动，人类与 AI 跨部门、跨系统多任务协同，AI 成为数字同事并相互协同	示例：AI 智能体制定市场进入策略，人类审核并决策；Agent 相互协同，处理物流调度、库存平衡及供需匹配，人类解决异常问题
阶段 3：AI 驱动 AI 成为智能中枢，企业进入超级智能体时代	AI 成为企业数字神经系统，企业内部形成高度智能化的生态网络，智能体主导大部分工作	人类监督，人类设定方向，授权并监控结果	示例：AI 智能体管理整个供应链，人类仅需定期检查关键节点；AI 驱动研发，人类聚焦创新方向

来源：阿里云研究院

阶段 1: AI 协作（Agent 应用普及） AI 成为组织标配能力，人机协作启航，AI 作为单点效率工具，以降本增效为目标，承担重复性、标准化任务。例如 AI 自动生成邮件并调用工具完成发送、AI 自动整理会议纪要并形成邮件进行分发、智能 OCR 识别合同关键信息并根据内容触发相关提示等。这其中人类主导决策，AI 作为数字助手提供基础支持。AI 的价值局限于局部流程优化，未涉及业务核心逻辑。

阶段 2: AI 协同（Agentic AI 深度协同） 人机共生成为主流组织形态，Agentic AI 深度嵌入业务流程，成为“准员工”级别的协作伙伴，具备场景化推理与动态优化能力。Agent 相互协同共同承担复杂任务。例如制造企业通过 AI 协同，生产 Agent、物流 Agent、市场 Agent 相互联动，动态调整排产计划匹配供需平衡；医疗 AI 辅助医生诊断时，Agent 不仅提供症状匹配和药物建议，还能联动药物研发 Agent 基于数据预测相关药物的不良反应。这其中人类与 AI 相互协作，AI 从执行工具升级为认知增强系统。

阶段 3: AI 驱动（AI 成为智能中枢） AI 成为组织的“数字神经系统”，企业内部形成高度智能化的生态网络，智能体之间高度协作。AI 推动企业从“条块制”、“矩阵制”向“液态网络”转型。智能体主导大部分工作，随时根据任务组建 Agent 团队，这个阶段的 AI 超级公司是在组织架构、决策机制、运营流程、产品设计、数据获取与分发等全方位将 AI 融入基因的企业。这其中人类主要设定方向并监控结果。



5.2 AI 超级公司发展阶段评估体系（4D-12I 模型）

基于 AI 超级公司进化逻辑，可构建包含 4 大维度（Dimension）、12 项关键指标（Indicator）的评估模型，通过阶段阈值区分“AI 协作（Agent 应用普及）- AI 协同（Agent 深度协同）- AI 驱动（AI 智能中枢）”三阶段特征。

表：AI 超级公司发展阶段评估体系

4 大维度（Dimension）	12 项关键指标（Indicator）
技术基建维度：AI 原生的底层支撑力	智能算力占比 AI 数据就绪率 模型迭代频率
组织协同维度：人机共生的系统运转效率	人机协作比例（H/A Ratio） 流程节点 AI 自主率（Agentic 率） AI 代码生成率
产品服务维度：AI 原生的价值输出能力	产品智能化程度 服务主动触发率 跨场景体验连贯率
价值创造维度：AI 驱动的效能与创新跃迁	AI 驱动效率提升率 AI 创新孵化占比 AI 治理范围程度

来源：阿里云研究院



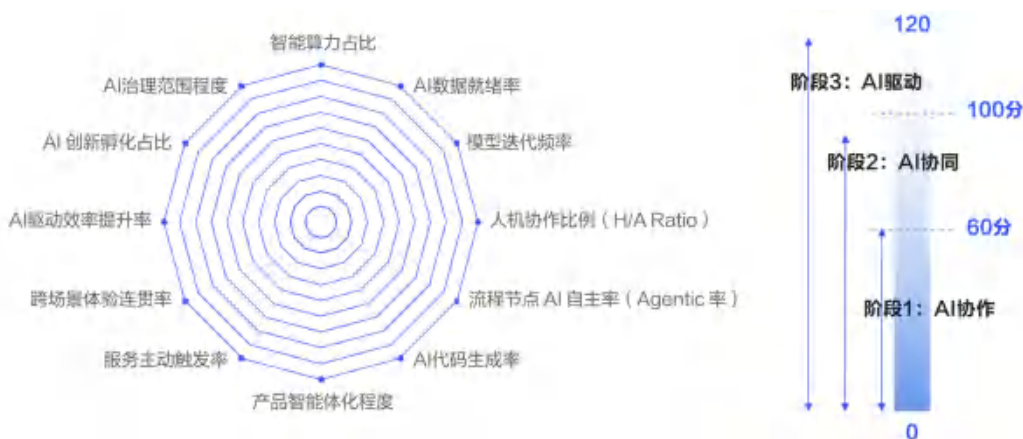
5.3 AI 超级公司评估体系应用

阶段定位工具：通过 12 项指标加权，总分计算“AI 超级公司指数”（0-120 分），快速定位企业所处阶段，明确 AI 转型短板及方向。

阶段 1 AI 协作：总分 < 60 分；

阶段 2 AI 协同：总分 60 ~ 100 分；

阶段 3 AI 驱动：总分 > 100 分。



图：AI 超级公司评估体系雷达图 来源：阿里云研究院

短板诊断框架：通过指标雷达图识别薄弱环节（如“流程节点 AI 自主率低”可能指向组织架构僵化），针对性制定改进措施。

行业细分权重：不同行业可调整指标权重分值（如制造业更侧重“智能算力占比”“流程自主率”，服务业更侧重“服务主动触发率”），使得细分领域评估更合理。

5.3.1 技术基建维度

用于衡量 AI 基础设施的规模化与自主化水平，决定组织智能化的基础能力。主要包括智能算力、数据资产 AI 化以及模型迭代三个指标。每个指标可按 10 分制进行评估打分。

1. 智能算力占比

用于 AI 训练 / 推理的专用算力在企业总算力中的占比，通常 AI 超级公司的智算占比随着场景部署的范围以及应用深度扩大逐步扩大。

2. AI 数据就绪率

经过清洗、标注、结构化，可直接支撑 AI 模型训练、后训练、微调的高质量数据与企业总数据量的占比。治理后的 AI 数据就绪率直接决定了 Agent 应用的准确性和价值放大。

3. 模型迭代频率

AI 垂直模型基于实时数据完成训练、调优、再部署的周期（次 / 月）。由于垂直模型需持续更新以适应行业 / 企业变化。不同场景的迭代频率有差异，例如金融领域反欺诈模型需每日更新交易数据以应对新型欺诈手法，制造业缺陷检测模型需每周迭代优化算法以适应新工艺流程。因此模型迭代频率需结合应用场景需求综合评判。

5.3.2 组织协同维度

主要聚焦协作、流程、研发核心指标，量化人机协作深度与组织弹性。包括人机协作比例、流程节点 AI 自主率、AI 代码生成率三个指标。每个指标可按 10 分制进行评估打分。

1. 人机协作比例（H/A Ratio）

人类员工与 AI Agent 智能体在核心业务流程中的工作量占比，通常较理想的 AI 超级公司人机协作比例较高。

2. 流程节点 AI 自主率（Agentic 率）

无需人工干预、由 AI 智能体独立完成的业务流程节点占所有业务流程节点的比率。

3. AI 代码生成率：

AI 辅助生成的代码占企业新增代码总量的比例（含应用开发、模型调优）。

5.3.3 产品服务维度

主要衡量 AI 对产品服务形态的重构深度，体现企业的市场产品竞争力。包括产品智能化程度、服务主动触发率、跨场景体验连贯率三个指标。每个指标可按 10 分制进行评估打分。

1. 产品智能化程度

产品中具备自主感知、决策、进化能力的模块占比。例如消费电子硬件的语音控制、智能汽车的自动泊车、工业设备的预测性维护等。

2. 服务主动触发率

AI 预判用户需求并主动提供服务的次数占总服务量的比例。主动触发包括部分场景主动服务，如健康预警、设备保养提醒；包括全场景主动服务，如个性化教育路径规划、供应链风险预判等。

3. 跨场景体验连贯率

AI 打通多场景数据，实现用户体验无缝衔接的比例。包括场景联动，如电商浏览 - 支付 - 物流自动跟踪；如智能家居 - 出行 - 办公的无感切换。通常较理想的 AI 超级公司跨场景体验连贯率较高。

5.3.4 价值创造维度

主要评估 AI 对企业核心竞争力的实质性提升，体现智能化转型价值。包括 AI 驱动效率提升率、AI 创新孵化占比、AI 伦理合规率三个指标。每个指标可按 10 分制进行评估打分。

1. AI 驱动效率提升率

核心业务流程（研发 / 生产 / 客服等）因 AI 优化带来的效率提升比例。包括局部流程提效，如客服响应速度提升；跨流程提效，如供应链周转周期缩短；系统性效率革命，如整体研发周期缩减一半以上。

2. AI 创新孵化占比

由 AI 辅助产生的新业务、新产品或专利占总量的比例。包括 AI 辅助现有业务优化；AI 驱动部分业务创新（如新材料研发、新市场预测）；AI 自主设计产品等。

3. AI 治理范围程度

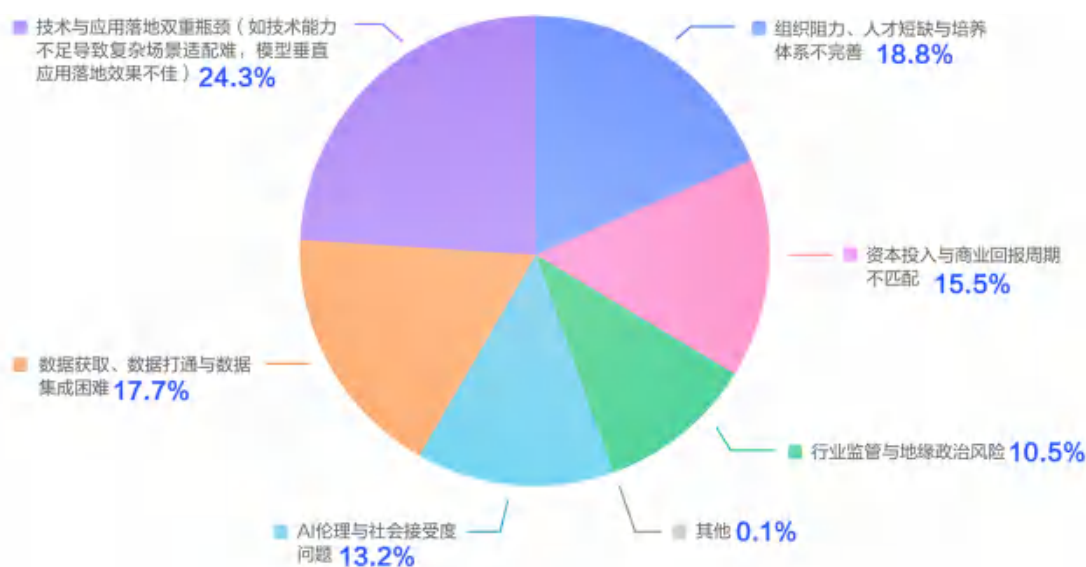
覆盖数据治理（如数据采集及数据隐私）、技术治理（如算法透明可控）、应用治理（如公共利益保护）、组织治理（AI 责任归属）、伦理治理（价值观及公平底线）的范围程度，确保实现“负责的 AI 发展”。

第六章

AI 超级公司的挑战与突围路径

随着大模型技术的不断发展，AI 应用范围逐步扩大，但大部分传统企业在尝试应用 AI 技术、尤其是大模型和 Agent 技术落地时，仍然面临着一系列挑战和困难。

问题：您认为当前制约企业应用 AI 的主要挑战有哪些？



图：制约企业应用 AI 的主要挑战（企业管理者调研） 来源：阿里云研究院 样本 n=500

6.1 AI 发展的核心挑战

6.1.1 数据孤岛与集成应用困难

AI 超级公司在演进过程中，数据层面可能面临“孤岛林立、集成受阻”的瓶颈，企业的数据分散在不同的系统中，类似 ERP（企业资源计划）系统包括财务与库存数据、CRM（客户关系管理）系统存储用户交互记录、SCM（供应链管理）系统则主要包括物流信息、MES（制造执行系统）负责生产流程数据等。这些数据不仅存储在独立系统、归属不同部门，格式和质量也参差不齐，这种“分散、异构、低质”的普遍状态，导致数据难以通过简单整合形成统一、可信的高质量领域数据。例如供应链 Agent 需同时调用 SCM 的物流数据与 ERP 的库存数据优化补货计划，却因两者格式不兼容、数据时间戳不一致，无法精准匹配关联；质检 Agent 依赖 MES 的生产数据与传感器的设备数据训练模型，却因异常数据未过滤，导致模型识别准确率大幅下降。最终数据缺乏治理成为制约 AI 超级公司业务深化的重要障碍。

6.1.2 技术与应用落地双重瓶颈

技术层面，当前通用 AI 驾驭复杂场景的能力仍有短板，大部分 AI 大模型基于通用开源数据集训练，与企业实际业务需求存在显著鸿沟。以零售行业 AI 大模型全渠道需求预测系统为例，即便基础大模型在通用消费趋势预测上表现优异，但若未深度融合“区域消费习惯、本地商圈特性、线下门店促销活动”等个性化业务数据，落地后仍难以精准匹配不同区域、不同业态门店的补货需求，最终形成“实验室测试效果优异、实际生产环境表现不足”的落差。

此外在应用落地层面，算力成本也成为规模化推广的关键制约——尤其是大规模部署 AI Agent 集群时，单是支撑实时推理、动态微调的算力消耗，就可能占据相当一部分企业技术投入预算，再加上自建算力中心带来的建设周期时间成本，因此选择合适的按需弹性伸缩的云计算实现方式也是 AI 超级公司发展路径的关键选择。



6.1.3 组织阻力与应用落地脱节

AI 超级公司在发展过程中，还需突破组织层面的深层阻力，避免应用与业务脱节。**首先是**员工层面的抵触心理，例如游戏开发企业引入 AI 游戏创意辅助系统后，游戏策划师因担心“多年积累的创意构思技巧被替代、对游戏玩法的决策权减弱”，在实际项目策划中，依旧执着于凭借经验撰写剧情大纲，不愿启用大模型基于“热门游戏趋势、玩家反馈数据”生成的创意启发方案，导致 AI 工具使用率低；**其次是**传统管理模式的惯性制约，部门墙导致 AI 应用难以跨流程协同，例如某零售企业的 AI 库存预测模型，虽能精准输出补货建议，但因采购部门与门店销售部门数据不互通、决策流程相互独立，模型建议无法快速转化为采购行动，最终只能在销售部门单独使用，无法形成“预测 - 采购 - 补货”的全链路价值。**再次**，还存在人才结构的断层问题，AI 应用落地需“技术 + 业务”双视角的复合型人才，例如某金融 AI 风控方案，技术团队能搭建模型框架，但因缺乏对信贷业务流程的理解，模型输出的风险评分与实际审批标准脱节；业务团队熟悉客户资质审核逻辑，却无法向技术团队清晰传递需求，导致方案反复修改仍难以落地，制约 AI 从技术方案到业务成果的转化效率，延缓 AI 超级公司全场景协同价值的释放。

示例：德勤调研揭示，尽管 65% 的高管认为 AI 将带来颠覆性变化，但仅 22% 的员工接受过系统培训，35% 的人对技术应用持消极态度。贝恩咨询发现，战略层面的矛盾同样显著，64% 的 CEO 因目标模糊导致项目止步试点，而跨部门协同的缺失使得 70% 的 AI 应用沦为“孤岛”。

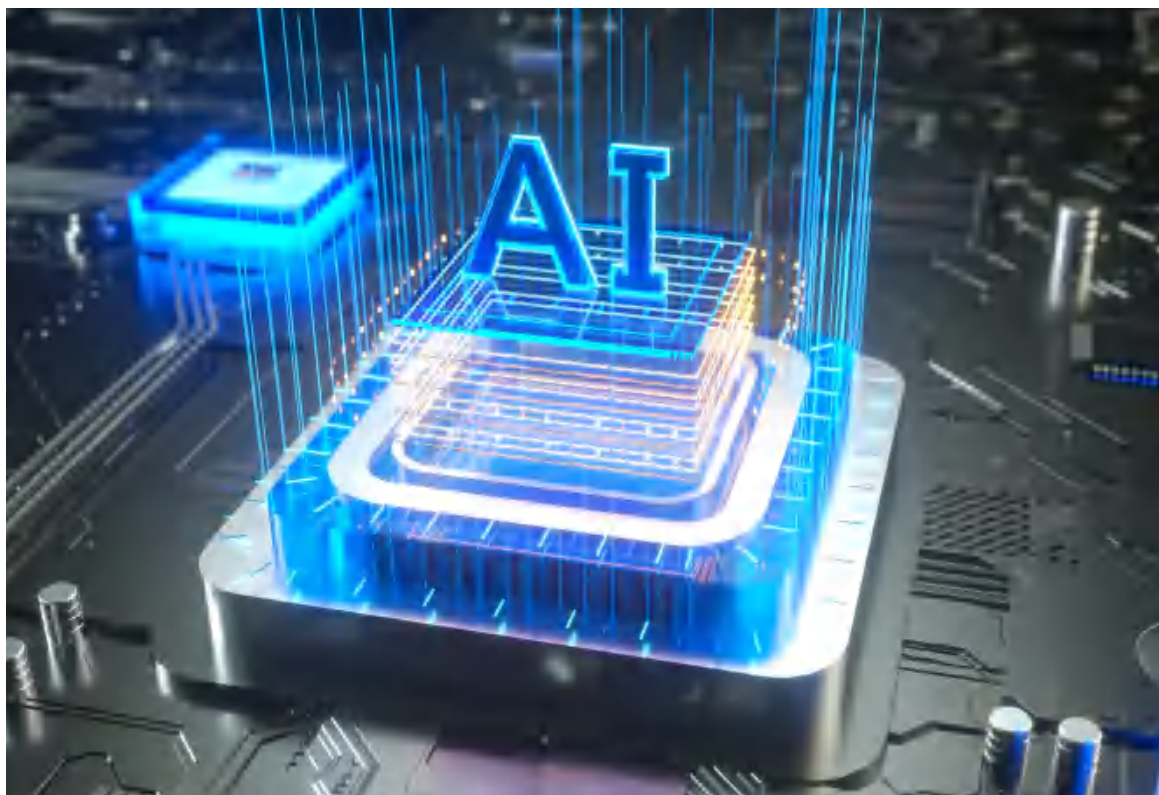
6.1.4 伦理风险伴随应用扩散加剧

AI 应用落地时，伦理风险也成为制约应用信任度的关键挑战，首先是算法偏见的场景化扩散，例如 AI 招聘系统若基于历史“男性主导岗位”的简历数据训练，可能在筛选时自动降低女性求职者的匹配评分，导致招聘歧视；金融领域的 AI 风控模型，如果过度依赖区域、职业等非核心数据，可能对特定低收入群体产生不公平拒贷结果，这类偏见随 AI 在人力资源、金融等关键领域的渗透，会引发社会信任危机。其次是数据隐私泄露风险的攀升，AI 应用为提升决策精准度，需收集处理海量用户数据——如智能导购 Agent 需获取用户消费记录、偏好标签，健康管理 Agent 需存储用户生理指标，一旦数据加密措施不到位或权限管理疏漏，易出现数据被窃取、滥用的问题，不仅违反相关法律法规，更会重创用户对企业的信任。

6.1.5 外部约束限制应用落地进程

AI 超级公司还需直面外部环境约束带来的多重挑战，延缓全场景规模化进程。一方面，监管政策的不确定性与区域差异推高合规成本——例如某企业计划在欧洲、东南亚同步部署智能招聘 Agent，却需应对欧盟《人工智能法案》对“高风险 AI 应用”的严格备案要求，以及东南亚部分国家对用户数据本地化存储的特殊规定，均需投入大量资源与精力调整数据处理流程、适配不同地区的合规标准。

另一方面，全球技术竞争加剧与供应链不稳定冲击资源保障——AI 应用的持续迭代与大规模部署，高度依赖核心算力资源、关键技术组件及核心算法等关键要素。当前部分国家对高端算力资源输出的限制、核心算法专利的壁垒，可能导致企业面临关键资源获取受阻的风险。例如某公司计划扩容 AI 模型训练集群，却因高端算力资源供应短缺，只能推迟模型迭代计划；部分核心算法依赖外部授权，一旦合作终止，已落地的 Agent 应用可能因无法获取算法更新支持，逐渐丧失智能优势，最终影响 AI 超级公司业务推进的稳定性与连续性。



6.2 AI 应用的突围路径

6.2.1 通过数据治理挖掘数据价值

突破数据孤岛、质量参差、隐私风险瓶颈，可将系统化数据治理作为数据层突围的关键路径——通过加强数据治理搭建基础，制定跨系统统一的数据标准（如规范 ERP 的财务数据、CRM 的用户数据、传感器的时序数据格式），建立“清洗 - 校验 - 标注”全流程机制，过滤冗余数据、修正传感器异常值、补全历史数据标签，解决数据格式不互通、质量不可信的问题，为 AI 应用筑牢数据基础。

数据治理是一个复杂且需要长期建设的项目，它贯穿整个数据生命周期，从数据的产生、清洗加工，再到存储、计算和服务应用，每个阶段都需要通过相应的工具与方法论进行规范与定义。对于部署 AI 应用的企业来说，数据资源的质量直接决定了 AI 应用能否成功落地。大型企业的数据治理可以协同生态伙伴共同推进。

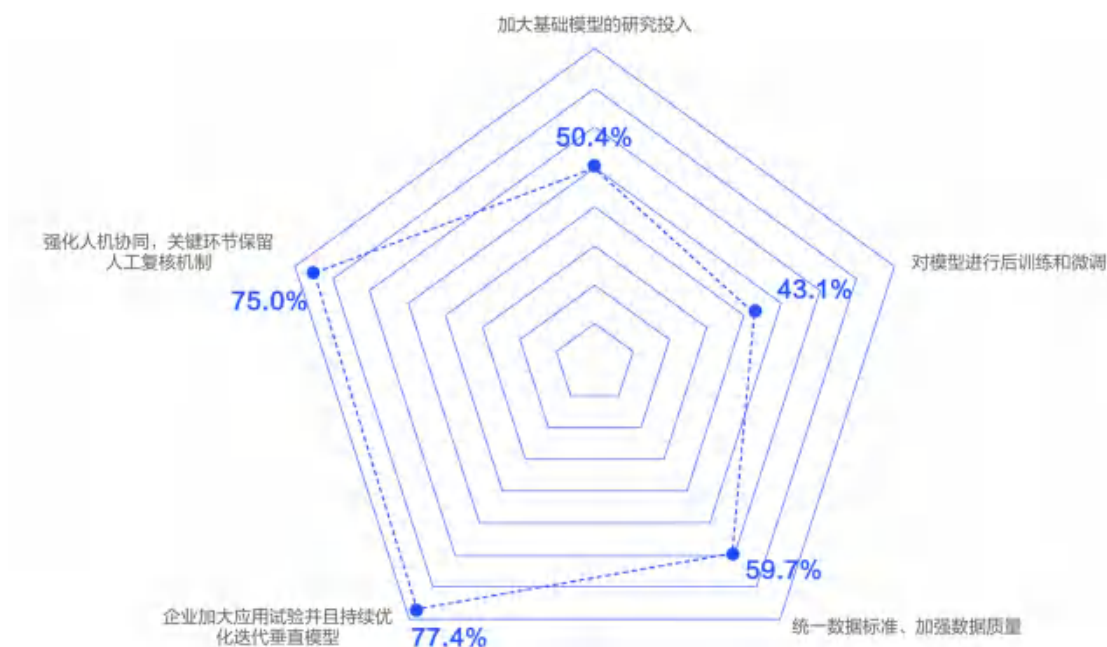


6.2.2 技术与应用协同突围

在技术方向上，不再依赖通用 AI 覆盖全场景，而是聚焦制造业质检、零售导购等具体业务痛点开发专用 AI Agent，比如针对工厂质检“光线波动、多缺陷叠加”的生产场景，用车间真实数据训练专用模型，解决“实验室准确率高、生产环境效果差”的落差，从而提升生产环境质检准确率；同时以小步快跑的数据微调缩短验证周期，如零售导购 AI Agent 先在 10 家门店试点，每 2 周时间基于用户互动数据优化一次推荐逻辑，快速提升用户转化率后再推广，避免大规模部署前的试错成本；

此外，云计算凭借弹性伸缩能力可按需调配算力资源，企业可按优先级动态分配算力，例如将高性能算力优先供给工厂质检、实时风控等核心场景，非核心的后台数据统计场景可复用闲时算力，从而整体降低算力成本，平衡大规模部署时的算力消耗与投入产出比，推动 AI 应用从局部试点走向规模化落地。

问题：针对“AI 应用落地不佳”的问题，您认为最有效的应对策略是？



图：AI 应用落地不佳应对策略（企业管理者调研） 来源：阿里云研究院 样本 n=500

6.2.3 通过数据治理挖掘数据价值

AI 超级公司组织转型可通过“试点验证－跨部门协同－人才赋能”的路径循序渐进。

在推进策略上，除了制定完整的 AI 战略规划以外，可采用“顶层设计指引＋基层试点突破”的思路，优先选择客服、财务、招聘等业务价值高、试点见效快的场景落地 AI 应用。例如在客服部门部署 Agent 辅助应答系统，缩短客户线上咨询平均响应时间，从而提升客户满意度；在财务部门上线 Agent 报销审核工具，大幅提升单据审核效率，用这些可感知的实际成果，让员工直观看到 AI “辅助而非替代”的价值，逐步消除抵触情绪。

在协作机制上，打破传统部门墙，由高层领导挂帅，组建由技术、业务、运营人员组成的跨部门 AI 推进小组。例如在推动 AI 供应链库存应用时，虚拟小组可涵盖 IT 部（负责技术落地）、采购部（提供业务规则）、门店销售部（反馈实际需求），确保 AI 库存预测模型能顺畅对接采购流程、同步销售数据，避免 AI 应用“停留在单一部门”的碎片化问题。

在人才建设上，通过内部培训＋外部引进双管齐下，打造技术＋业务复合型团队，针对现有员工开展 AI 业务应用培训，例如让财务人员掌握 AI 数据分析工具的基础操作，让业务经理能清晰向技术团队传递需求；同时引进兼具 AI 技术背景与行业经验的复合人才，牵头 Agent 应用从规划到落地的全流程，确保技术方案与业务需求精准匹配，全面提升 AI 应用的落地效率与价值转化能力。

6.2.4 伦理建设护航应用推广

在治理架构上，成立 AI 伦理（治理）委员会，汇聚技术、法律、业务及外部专家，制定“透明、公平、可控”的应用准则。针对招聘 AI、金融风控 AI 等涉及公平性的场景，落地前需通过伦理审查，校验模型是否存在“性别、地域”等偏见，例如针对健康管理、智能营销等涉及用户隐私的应用，审查数据收集范围与加密措施，确保符合隐私法规。

在技术设计上，推动 AI 应用的可解释性优化。如金融 AI 风控系统会生成“拒贷原因说明书”，清晰标注“用户负债比例过高、近期征信查询频繁”等关键决策依据，让用户与信贷经理直观理解判断逻辑；客服 AI 在推荐解决方案时，同步说明“基于历史 1000 多同类咨询的最优方案”，增强业务人员与用户的信任度。

在风险应对上，明确应用落地时配套风险应对方案，例如若 AI 导购推荐出现偏差，自动触发人工介入流程，快速修正推荐结果，避免用户投诉升级。通过这套伦理保障体系，AI 超级公司既能规避伦理风险，又能提升用户与业务端对 AI 应用的接受度，为规模化推广筑牢信任基石。

6.2.5 生态协同加速应用规模化

一方面，用联合共建整合全产业链资源，搭建 AI 应用落地的生态能力集群，帮企业降低单点突破成本。主动联合产业链里不同角色的强伙伴，形成“技术供给 - 需求对接 - 算力支撑”的闭环：例如对接云厂商，按 AI 应用需求灵活调用算力，企业不用自建大型算力中心；联动 AI 大模型厂商引入优质基础模型，节约企业自研的时间和成本；同时跟业务需求方深度合作，梳理业务需求和历史数据，通过 Agent 落地结合，避免技术与业务脱节。

另一方面，以经验共享 + 模板复用模式加速企业内规模化复制。企业可系统梳理自身及生态伙伴的 AI 应用落地经验，将试点中反复验证过的技术框架、业务逻辑、部署流程提炼为可复用的标准模版。例如零售企业在试点门店落地的“智能推荐 Agent”模版，内置用户行为分析、实时偏好预测、商品匹配算法等核心模块，还可预设“节日促销推荐、新客首购推荐、本地天气变化、地域差异文化”等细分场景的参数配置，其他门店接入后，仅需根据自身客群特征微调少量参数，即可快速规模落地智能推荐 Agent。

这种生态协同模式，让 AI 超级公司通过资源共享与模板复用，降低整个行业的 AI 应用门槛，最终实现整个 AI 产业的协同升级。



结语：从“适应 AI”到“定义 AI” —— AI 超级公司的进化密码

当蒸汽机轰鸣着改写工业文明的轨迹时，没有人能预见工厂制度会重塑人类的协作方式；当互联网打破物理边界时，也鲜有人料到它会颠覆商业的底层逻辑。今天，生成式 AI 引发的变革正在重复相似的历史叙事——但这次它的渗透速度与重构深度远超以往。AI 超级公司的崛起，不仅是技术迭代的产物，更是一场关于价值创造的底层逻辑革命：从被动适应 AI 工具，到主动用智能定义商业规则、产品形态、组织架构与产业生态。

AI 超级公司的诞生，无关乎团队规模的大小。无论是三五人的小型团队，还是独当一面的个人公司，都可能在这个机会均等的时代，凭借对智能的创新应用跻身 AI 超级公司的行列。这种平等的机遇，打破了传统商业中“规模决定实力”的固有认知，让每一个拥有创新理念的主体，都能在 AI 浪潮中找到破局的可能。

从“适应 AI”到“定义 AI”，这条路或许需要十年、二十年，甚至更长。注定不会一帆风顺。技术瓶颈的突破、组织阻力的消解、伦理风险的规避、全球规则的协同等等，每一步都充满挑战。但可以确定的是，那些最终成为 AI 超级公司的组织，必然是既懂技术的力量，更懂人性的温度；既追求效率的极致，更坚守文明的底线。

AI 革命的终极战场，从来不是技术的比拼，而是对“价值本质”的重新理解。当 AI 超级公司用智能重构商业、组织与生态时，它们定义的不仅是未来的企业形态，更是人类与智能时代共处的新范式。这正是 AI 超级公司留给时代的进化课题。