

AI时代数据可信流通产业 周期洞察报告（2026）

可信筑基 · 智能无界

作者：肖艺学

序言

以OpenClaw、Hermes Agent为代表的自主式AI，让数据的发展同时面临着机遇与挑战。首先，AI导致的数据泄露失控是亟待解决的新型数据安全问题；同时，自主式AI让数据的战略价值与流通需求呈指数级攀升，其自主迭代依赖动态鲜活的业务数据。而无论是专业场景模型训练，还是AI智能体动态迭代，所需要的各类机密数据，在流通过程中均面临着严格的安全合规要求，尤其是当数据进行跨主体、跨行业、跨区域的流通时，对隐私保护的需求变得更加强烈。

放眼于数据可信流通产业，目前可信数据空间正在如火如荼地建设，结合密态计算等隐私保护技术，为数据可信流通提供了坚实保障。我们同时也需要清醒认识到，这一切只是起点，下一阶段的攻坚重点将从数据可信流通基础设施的搭建，转向上层数据治理体系与应用生态的构建。

产业参与者需兼具前瞻战略眼光与务实落地精神：一方面，要围绕AI时代的数据可信流通发展趋势进行前瞻布局；另一方面，要立足具体业务场景，在金融、医疗、政务等领域打磨可复制的落地范式，推动数据在安全合规的前提下充分释放价值，确保AI能够规模化可靠落地，构建面向AI时代的数据可信流通产业新生态。

艾瑞咨询（iResearch）作为长期深耕新经济与前沿科技领域的研究咨询机构，旨在以独立、客观、专业的视角，基于问卷调

研、深度访谈与项目案例研究，从技术周期、落地实践、客户需求、厂商能力等多维度，剖析AI时代的数据可信流通的发展现状与演进趋势，力求为业界提供一份具备参考价值的研究成果。

独行者速，众行者远。产业发展离不开各方的协同推进。期待本报告能够成为凝聚共识、推动行业创新的一块基石，为数据可信流通及AI的高质量可持续发展注入不竭动力。让我们乘可信之舟，渡数据价值之海，驶向更加智能、可信、繁荣的数字未来。

可信筑基，智能无界！

联系作者

肖艺学 Eason

WeChat : NCR9393

E-mail : xiaoyx9@iresearch.com.cn

目录

CONTENTS

01 AI时代背景

数据流通在AI时代所面临的机遇和挑战

02 E - Cycle：周期洞察

产业研究：AI时代下的数据可信流通发展

03 TechValue：穿越周期

企业评估：穿越产业周期的价值创造者

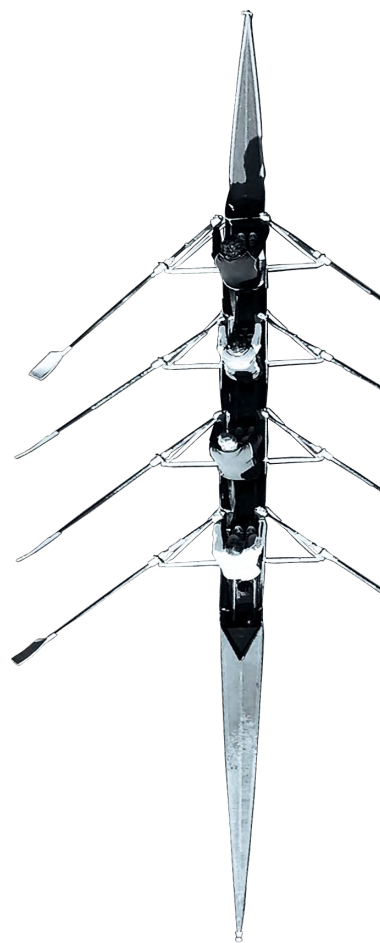
安全挑战、效率革命

AI智能体的落地，让数据面临：

安全挑战、效率革命

面向所有业务场景：AI导致的数据泄露失控是亟待解决的新型数据安全问题。

面向数据业务场景：AI智能体让数据治理、加工等数据类业务场景实现效率的革命性提升，但数据泄露风险也被放大。



AI带来的创新价值与冲击挑战

辅助式AI到自主式AI的变革式能力跃迁将推动“AI Agent Anywhere”的趋势发展，同时也伴随着“人对AI的失控、AI自身的失控、AI导致的数据泄露失控”三大冲击挑战

AI Agent Anywhere的发展趋势：以OpenClaw、Hermes Agent等智能体的落地应用为分水岭，行业便迈入了自主式AI的创新发展周期。相较于仅能被动响应指令的传统AI，以及以Copilot为代表、仅能辅助人工操作、缺乏自主闭环迭代能力的辅助式AI，自主式AI实现了能力范式的根本性跃迁。自主式AI以动态鲜活数据为核心持续优化自身决策与执行能力，向目标方向不断收敛，摆脱对人工干预的依赖，具备了目标驱动、自主规划、动态决策、工具调用、升级迭代的全链路自主作业能力。自主式AI智能体与前代AI产品形成了本质代差，它不再是依附于人类的辅助工具，而是能够独立承接复杂任务、自主推进目标落地的“硅基员工主体”，这种巨大的生产力变革将推动AI应用于千行百业，让AI Agent无处不在。

AI能力演进带来的创新价值与冲击挑战



注释：Agentic AI：自主式AI（或能动式AI）。行业习惯将 Agentic AI 翻译成代理式AI。但是站在AI技术能力及价值表现的角度，区分传统的Copilot和目前的AI Agent，将Agentic AI翻译成自主式AI（或能动式AI）会更加贴切。自主式AI，是具备目标驱动、自主规划、决策、工具调用、自我迭代能力的新一代AI，代表AI从辅助智能向自主智能的演进。

来源：艾瑞咨询。

AI带来的三大冲击挑战：由于AI智能体存在无边界上下文暴露和开放动态命令执行的本源性风险，AI智能体的落地面临安全体系崩溃挑战，同时面临着“人对AI的失控、AI自身的失控、AI导致的数据泄露失控”三大冲击挑战。释放自主式AI创新效能的同时，构建与AI迭代收敛闭环相匹配的全链路数据治理、风控与安全体系，成为企业必须同步推进的核心战略议题。

AI智能体的本源性风险及三重失控表现 & 企业应对态度



AI智能体的本源性风险

无边界上下文暴露

UBCE (unbounded context exposure)

—— 自主式AI智能体的本源性风险 ——

自主AI在任务执行中无差别聚合内外部数据，导致敏感信息泄露、上下文污染等安全隐患。

开放动态命令执行

ODCE (open dynamic command execution)

—— 所有AI智能体的本源性风险 ——

AI智能体存在开放动态命令执行漏洞，一旦被诱导即可执行对应指令，将穿透现有安全防线。



人对AI的失控

自主式AI调用ERP、CRM、数据库等系统及工具操作时，人类难以对其展开行为干预，造成人对AI的失控。



AI自身的失控

自主式AI的决策和行为脱离预设框架，且难以保证其工作成果的质量、可靠性与合规性，造成AI自身的失控。



AI导致的数据泄露失控

AI使数据主权、访问权限与敏感信息面临前所未有的无边界暴露风险，引发AI导致的数据泄露失控。

80%

的组织领导者因担忧核心业务数据在AI交互（如Hermes Agent访问数据）中的安全风险，选择放缓或调整AI项目的落地节奏。



冰山一角

已暴露的失控风险事件，是露出的“冰山一角”，敲响行业警钟

典型案例：Meta内部，AI智能体回答员工的技术问题时，不仅给出错误建议，还引发了数据权限配置失误，导致海量公司及用户数据在两小时内对一批无权访问的工程师开放。

深水暗礁

未暴露的潜在失控风险，藏于“深水暗礁”，企业需防患于未然

开始应用自主式AI智能体产品的“AI领先型企业”已经关注到失控风险，其中的大部分企业愿意以“防患于未然”的态度进行投资。

关注“人对AI的失控”风险

73%

关注“AI自身的失控”风险

83%

关注“AI导致的数据泄露失控”风险

93%

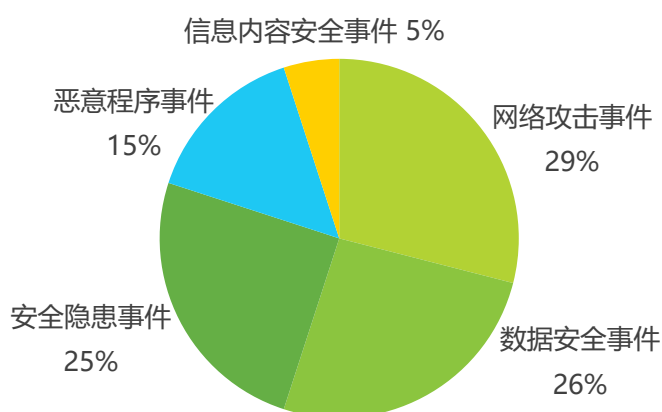
注释：N=100，受访企业是已经采纳自主式AI产品的企业。
来源：艾瑞咨询。

在“AI Agent Anywhere”的发展趋势下，自主式AI智能体导致的数据泄露失控是正在面临的新型数据安全问题，若不加以有效管控和解决，企业将会陷入“越用AI、数据风险越高”的危险递增循环

AI时代的数据安全问题愈发严峻：2025年，13%的数据泄露事件与AI系统直接相关（预计2028年将达35%），超过四分之一的AI安全事件和数据安全相关。

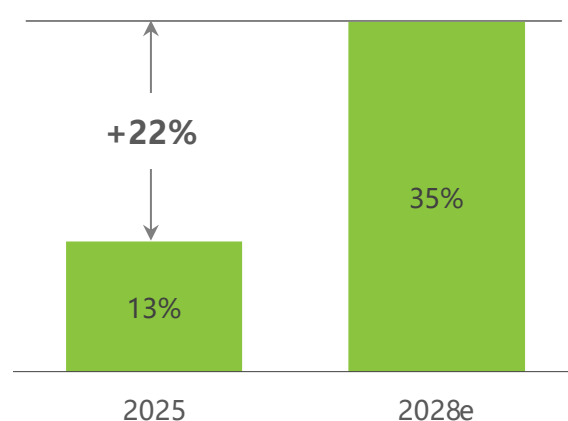
自主式AI的快速演进正面临着日益严峻的失控问题，由此带来了数据安全领域全新的增量风险。这类风险并非传统安全威胁的简单延伸，而是源于自主式AI在运行机制上的根本性变化。相较于传统技术攻击（如漏洞利用、病毒植入）以及人为泄露（如内部人员误操作、权限滥用）等常见安全隐患，此类风险具备更强的安全防护体系穿透能力。随着越来越多的企业开始采纳自主式AI智能体，由AI导致的数据泄露失控，成为业界需要亟待解决的问题。

2025年全球AI安全事件类型分布情况



来源：数据来源国家病毒中心。

AI导致的数据泄露事件占比



来源：基于公开资料及行业专家访谈综合研究产出。

数据类场景的AI智能体开始逐步落地应用。这类产品能够提升数据治理及加工的效率，但也带来了更严峻的数据泄露风险。企业需优先确保此类智能体的可靠性与可控性，增强对高敏感数据的密态保护。



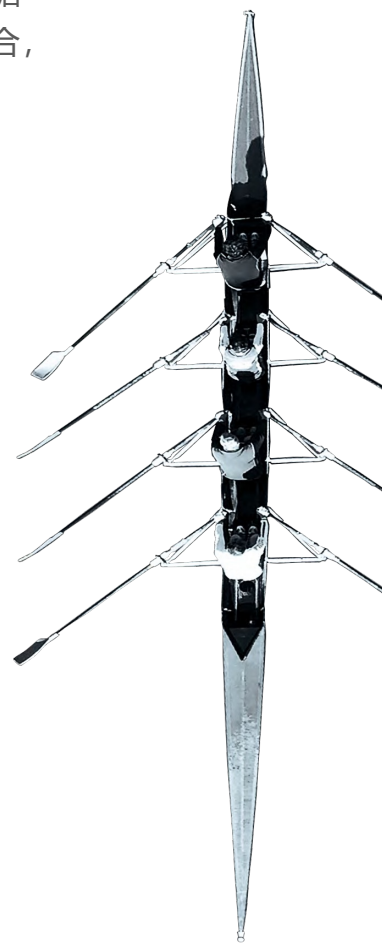
我们看到一些企业推出了数据分析、数据治理加工等数据类AI智能体产品。这类产品直接面对的是用户隐私、商业机密等高敏感数据。

由于自主式AI的自主决策与跨系统协同特性，使其可能因指令理解偏差、权限失控或外部攻击引发数据泄露，让原本可控的数据业务，新增了由AI带来的安全隐患，企业需构建更严密的全链路安全防护体系和数据密态保护措施来增强安全性，此外还可以结合行为控制、核验机制等手段，提高AI智能体的可控性和可靠性。

专业场景模型训练、AI智能体动态迭代，将促进：

数据可信流通需求的增长

专业场景模型训练、AI智能体动态迭代，通常需要业务、用户等机密数据作为核心燃料，且很多时候需要进行跨主体、行业、区域的数据流通融合，将进一步激发数据的数据可信流通需求。



企业AI落地激发数据可信流通需求

企业AI落地所涉及的各类数据面临多种泄露风险，基于密态计算等数据隐私保护技术所构建的数据可信流通范式，将逐渐内化为企业AI落地的原生安全能力

企业AI落地过程中的AI就绪数据、AI生成或调用的各种数据，存在诸多数据泄露风险。而自主式AI无边界上下文暴露等问题，虽可通过AI架构设计、权限边界管控等方式前置防范，但伴随AI技术持续迭代，仍可能涌现新的安全问题。而基于密态计算的数据隐私保护能力，是数据安全兜底的终极护盾，其将逐渐内化为企业AI落地的原生化安全能力。下文以“基于密态计算的受控匿名化个人数据保护”做为典型案例展开描述：



企业AI落地的数据可信流通场景举例

典型场景：基于密态计算的受控匿名化个人数据保护，推动集团内部子公司跨主体数据的合规共享，支持大模型训练

目前，大模型研发、训练到工程化落地，对算力、数据、技术人才与资金均有极高门槛，往往大型集团企业具备全流程建设与实施能力。因此我们以大型集团企业为典型对象展开分析。

问题描述：

集团型企业的AI大模型落地过程中，需要整合旗下各独立子公司主体的用户信息等个人数据资源，以提升模型训练效果。但受《个人信息保护法》等法律的规定，各主体间原始个人数据直接共享存在隐私合规风险，法务层面的严格限制让数据形成壁垒，导致跨主体数据的融合难以推进。

在大模型训练的实际场景中，若试图获取个人数据授权，更是面临着极高的门槛。

解决方案：

基于密态计算的受控匿名化，是目前解决这一问题的最佳方案。在《中华人民共和国网络安全法》与《中华人民共和国个人信息保护法》中引入的“个人信息匿名化条款”，将匿名化后的数据与个人信息进行了区隔。因此，采用受控匿名化的方式对个人信息进行处理，既为AI发展提供必需的数据支撑，又能切实守护个人隐私安全。

该方案在数据融合前期便对敏感信息进行可控的匿名化处理，依托密态计算技术让数据在密文状态下完成计算与分析，全程不暴露原始明文。

这一模式从技术层面规避了个人信息泄露风险，完全满足监管及法务合规要求，同时最大程度保留数据的可用性与分析价值，能够安全合规地打通集团内各子公司的数据壁垒，实现跨主体数据的可信、合规、高效流通。



~63% 的企业在训练大模型的过程中，曾因合规约束和法务限制，导致跨主体的个人数据难以融合共享而影响项目进度。

注释：N = 80，受访企业均为集团型企业。

来源：艾瑞咨询。

目录

CONTENTS

01 AI时代背景

数据流通在AI时代所面临的机遇和挑战

02 E - Cycle：周期洞察

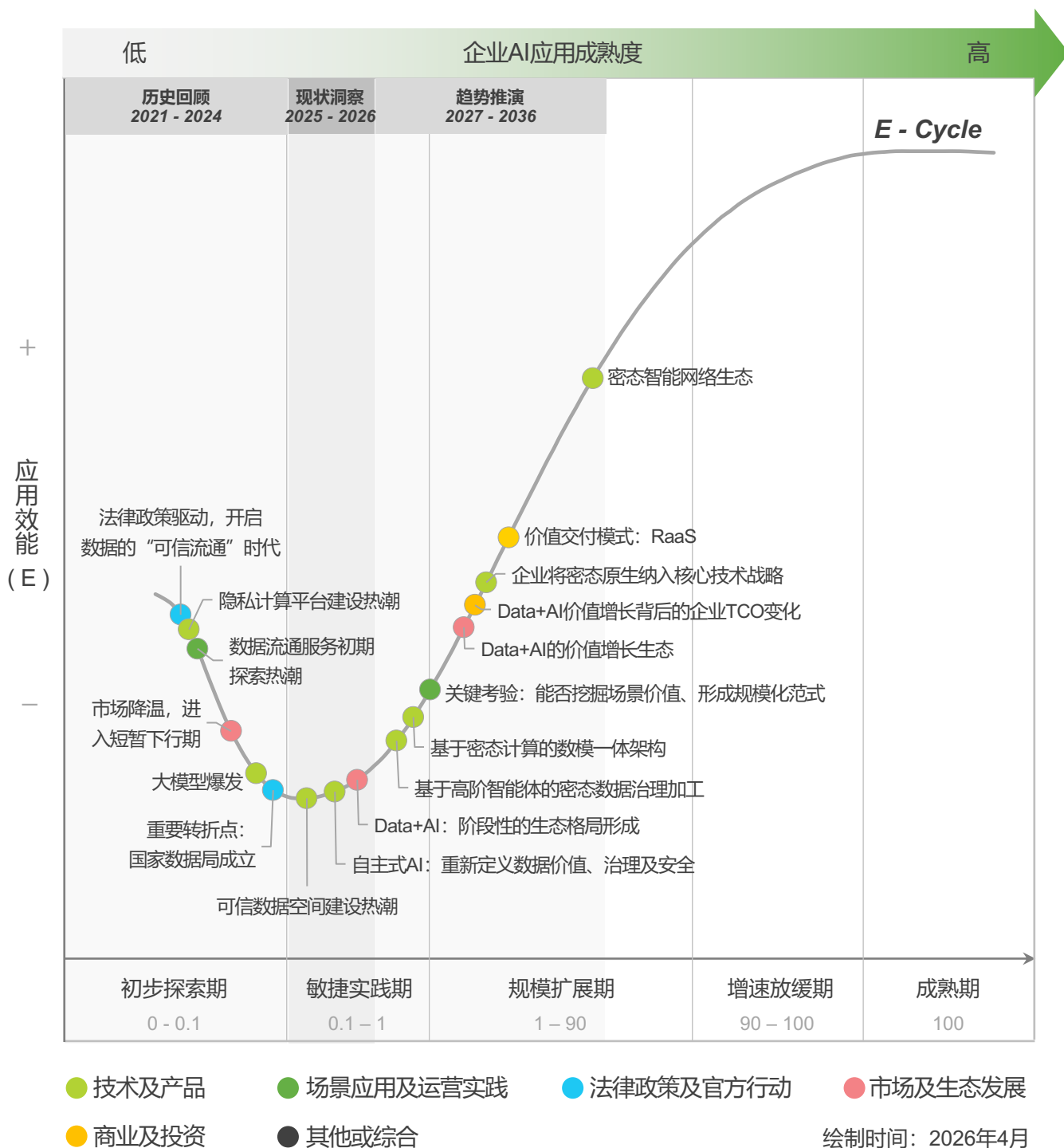
产业研究：AI时代下的数据可信流通发展

03 TechValue：穿越周期

企业评估：穿越产业周期的价值创造者

周期概览

中国AI时代的数据可信流通产业周期洞察



注释1：横纵坐标轴定义

- 横轴体现技术发展所处的阶段（综合应用范围、用户覆盖度等指标综合评估）。
- 纵轴定义的应用效能表示技术带来的价值回报（综合总体拥有成本<TCO>、投入产出比<ROI>等指标综合评估）。

注释2：各发展阶段的周期规律和具体表现，在对应章节部分详细解读。

来源：艾瑞咨询。

研究概述

本报告定义的“AI时代的数据可信流通”产业周期，以“数据可信流通产业的发展”为主线，同时关注以大模型、自主式AI为代表的新一代AI技术对数据可信流通的机遇和挑战。

报告基于E – Cycle曲线表达的技术周期规律，对“AI时代的数据可信流通”的历史、现状和趋势进行分析和推演。

周期的关键节点划分：

- 周期的起点：2021年《数据安全法》《个人信息保护法》等法律的正式实施以及市场开始采纳隐私计算的行动热潮，是数据可信流通产业周期正式开启的节点。
- 当前周期阶段主要包含的内容：2025—2026年，可信数据空间建设掀起热潮；自主式AI重新定义了数据的价值、治理和安全；阶段性的产业生态格局形成。
- 未来10年将迈向何方：分析未来长中短期数据可信流通产业的发展及自主式AI的影响。

本研究的叙事结构为：

- 历史回顾（2021—2024）：覆盖初步探索期的完整阶段，包含6个周期用例。
- 现状洞察（2025—2026）：覆盖敏捷实践期的部分阶段，包含3个周期用例。
- 趋势推演（2027—2036）：覆盖敏捷实践期的部分阶段、规模扩展期的部分阶段，包含8个周期用例。

各产业周期的发展规律及具体表现，请见报告各章节的详细论述。

中国企业AI应用成熟度AIM²模型

数据可信流通的发展需要同步考虑“AI失控对数据安全的影响、AI自主迭代过程中对数据密态可信流通能力的需求”等相关问题。企业AI应用成熟度是一个值得关注的内容。

本研究以“E-Cycle曲线：中国数据可信流通产业周期”为研究主线，利用“中国企业AI应用成熟度AIM²模型”在关键周期节点和事件中判断企业AI应用成熟度，以更好地分析AI时代的数据可信流通发展走势。

中国企业AI应用成熟度AIM²模型

报告关注的是企业对“大模型为核心的新一代AI”的应用成熟度



L1 探索试验级 企业内单点应用

此阶段的AI尝试是自发、零星且混乱的。企业缺乏正式的AI战略和资源投入，应用通常局限于个别员工或团队的孤立探索，成果难以预测和复制。此时的重心是“点”上的突破，验证AI在特定任务上的可行性。



L2 局部赋能级 企业内多点应用

企业开始有意识地在特定部门或业务场景中以项目制方式应用AI，并取得了一定的业务效果。但项目之间缺乏整体规划和协同，成功往往依赖于少数个人的推动。这个阶段，企业开始通过多个“+AI”项目积累经验。



L3 体系优化级 企业内体系应用

AI应用走向标准化和体系化。企业开始建立集中的数据治理体系、统一的AI开发平台和标准化的流程规范。AI能力不再是孤立的，而是作为一种可复用、可共享的内部资源，在核心业务领域进行规模化复制，实现“面”上的运营级全面集成。这是从“+AI”向“AI+”过渡的关键准备期。



L4 生态重构级 行业内赋能应用

AI能力不仅深度融入企业核心业务，更开始作为一种核心产品或服务，向产业链上下游的生态伙伴输出。企业利用AI重构与供应商、客户和合作伙伴的协作模式，打造基于AI的生态竞争力。这标志着企业开始具备“AI+”的能力，用技术影响和重塑行业。



L5 认知引领级 跨行业创新应用

AI成为驱动企业“自我进化”的核心引擎。组织本身演化为一个由AI驱动的、能够持续学习和自我优化的“认知有机体”，能够敏锐地洞察市场变化，甚至自动发现并创造全新的商业模式，实现跨行业的创新引领。此时，企业真正成为“AI+”的典范，形成“企业即智能体”。

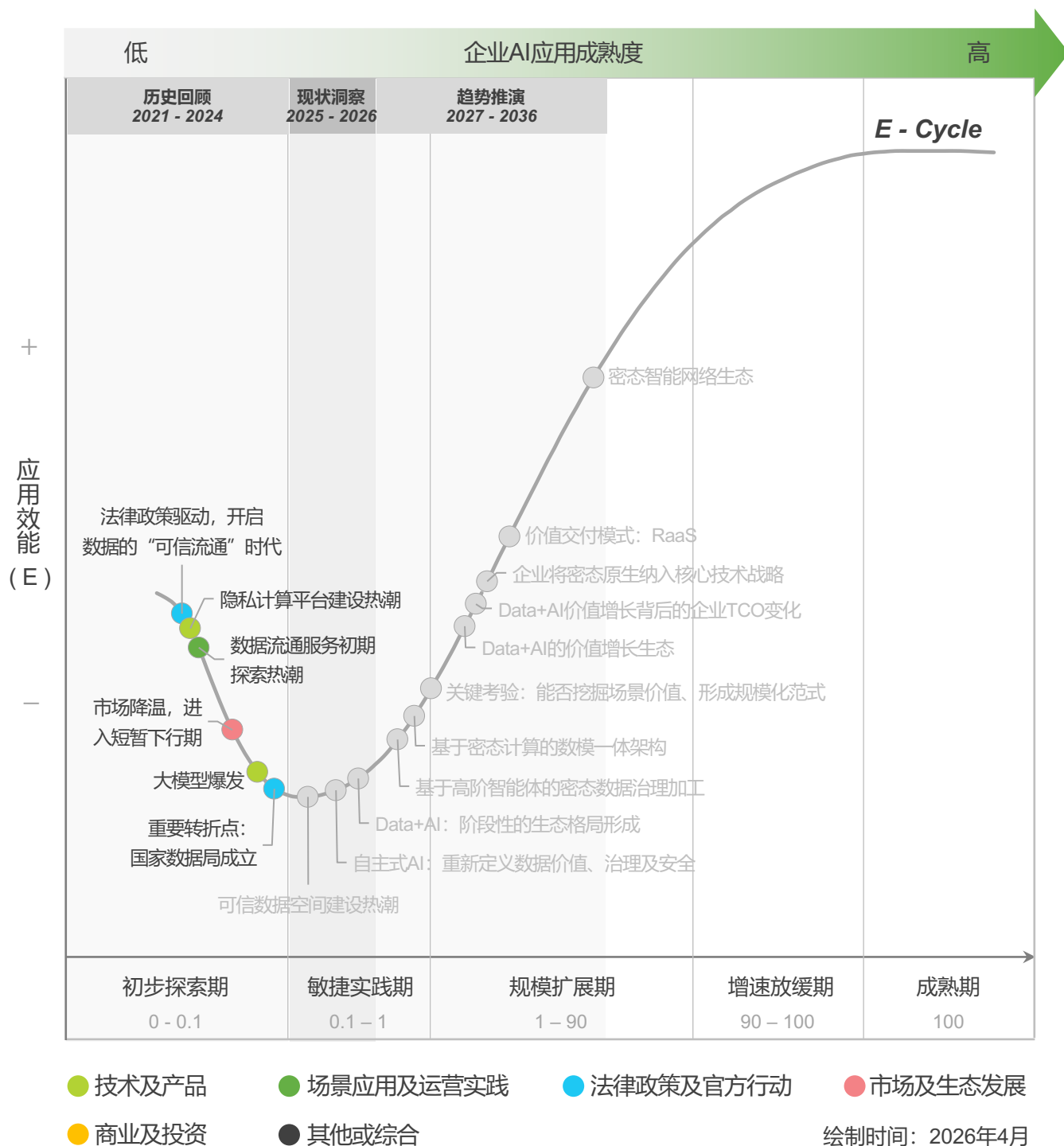
注释：中国企业AI应用成熟度AIM²模型的使用已获得版权持有方授权。
来源：艾瑞咨询。

历史回顾

2021年 — 2024年

一、历史回顾

中国AI时代的数据可信流通产业周期洞察 – 历史回顾



注释1: 横纵坐标轴定义

- 横轴体现技术发展所处的阶段 (综合应用范围、用户覆盖度等指标综合评估)。
- 纵轴定义的应用效能表示技术带来的价值回报 (综合总体拥有成本<TCO>、投入产出比<ROI>等指标综合评估)。

注释2: 各发展阶段的周期规律和具体表现, 在对应章节部分详细解读。

来源: 艾瑞咨询。

发展历史（2021 - 2024年）覆盖产业周期“初步探索期”的完整阶段。

初步探索期的规律及经验

- 

该阶段的核心目标：技术走出实验室，形成初代产品向市场推广，厂商或技术布道者进行早期的市场教育，赢取客户认可和持续投资。
- 

该阶段的关键表现：初代产品进入落地探索阶段，早期接受者开始试用。初代产品的项目多处于POC、部署实施、试运行等初期环节，整体仍属技术投资建设期，回报低于投入，因此E-Cycle曲线呈下行走势。同步伴随的是，市场对技术的关注度上升，媒体炒作增加，供应商数量增长。
- 

风险警示：初步探索期技术发展的抗风险能力较弱。初代产品的应用效果未达预期、市场需求增长乏力、资本市场趋冷等一种或多种因素的叠加，且市场未能推出新一代产品、没有新的行业驱动因素（如利好政策出台等），行业将面临发展停滞或失败的风险。

核心摘要 @ 历史回顾（2021 – 2024）

- 

初代数据可信流通产品的发展：隐私计算平台作为初代数据可信流通产品，2021年是商用落地元年。伴随着2022年资本市场降温，同步逐渐出现厂商价格战、市场增长乏力叠加客户回款周期长等问题，市场发展面临极大挑战，一些供应商陆续退出市场或转型，市场进入低谷期。
- 

数据流通服务初期探索热潮：数据交易所、数据商、数据经纪人、技术厂商等各类企业机构的数据运营和交易等数据流通服务所发挥的作用有限，远未能形成规模化且可持续的价值流通范式，但收获了探索性的实践经验。

面临问题：很多数据源面临不愿、不敢、不会、不能开放的问题，且缺乏杀手铜级别的数据产品或价值场景，数据生态网络的建设和运营更加需要国家的自上而下推动。
- 

国家数据局的成立，恰逢其时：市场发展面临阶段性困境时，国家数据局于2023年10月25日正式挂牌成立，是一项行业利好。国家数据局出台的相关政策和举措，推动数据可信流通产业周期迈入下一发展阶段。
- 

在这个阶段，以大模型为核心的新一代AI仅处于探索性落地阶段，其对数据可信流通的需求尚处酝酿期。市场仍以传统AI业务小模型的可信联合建模项目为主。

大模型爆发，标志着“数据可信流通”和“新一代AI”的双轮技术周期进入叠加发展阶段，也预示着新一代AI将影响数据可信流通的下一周期阶段（敏捷实践期）的发展路径。

二、历史要点分析

1. 法律政策驱动，开启数据的“可信流通”时代

政策法律的本源驱动：数据可信流通产业先天镌刻国家战略基因



法律法规：2021年，随着《数据安全法》《个人信息保护法》《民法典》等法律的正式施行，加之2017年已实施的《网络安全法》（后于2025年修订）等相关法律，确立了数据需要安全合规流通的法定要求，推动着市场摆脱非密态的数据包传输和API调用等传统数据流转模式，转向基于隐私计算的新型数据可信流通范式，**中国迈入数据可信流通的发展时代。**



同时期的政策规划：同时期的《关于构建更加完善的要素市场化配置体制机制的意见》提出将数据作为一种新型生产要素、以及《要素市场化配置综合改革试点总体方案》提出建立健全数据流通交易规则。多项政策与发展规划，为数据安全合规流通提供了关键指引。由于这些政策规划的重要性及高度，**数据可信流通行业先天镌刻国家战略基因，叠加数据本身的关键价值，使数据可信流通成为依托国家自上而下系统推进、价值渐进释放、发展韧性强的关键领域。**

2. 隐私计算平台建设热潮

（一）隐私计算平台是初代的数据可信流通产品。在数据安全合规需求的牵引下，数据源和数据使用方开始纷纷建设隐私计算平台

隐私计算在确保数据提供方不泄露原始数据的前提下，对数据进行分析计算，让数据以“可用不可见、用途可控可计量”的方式安全流通。2021年，业界的三条主流技术路线为：以密码学为核心（如MPC）、融合隐私保护技术的联合建模（TFL）、依托可信硬件（TEE）。主流的隐私计算平台还融合了区块链技术强化数字身份、计算、监管等方面的信任机制。安全性和性能是平衡，是客户最关注的隐私计算能力指标，平台功能完备性、易用性、跨平台互联互通能力，也是重点关注的方向。

基于隐私计算的数据可信流通模式（以多方安全计算为例）



该图（以多方安全计算为例）仅用作隐私计算应用实践的简单示意，不代表隐私计算的全部实践逻辑和技术方案。

（二）2021年是隐私计算平台建设（商用落地）元年，金融、政务、运营商是核心落地领域

法律法规及政策的推动下，隐私计算平台迎来了建设热潮。2021年中国隐私计算的市场规模约为4.9亿元人民币，其中平台建设和服务占比96%；金融、政务、运营商的市场份额占比在75%~80%，医疗领域占比约为10%。

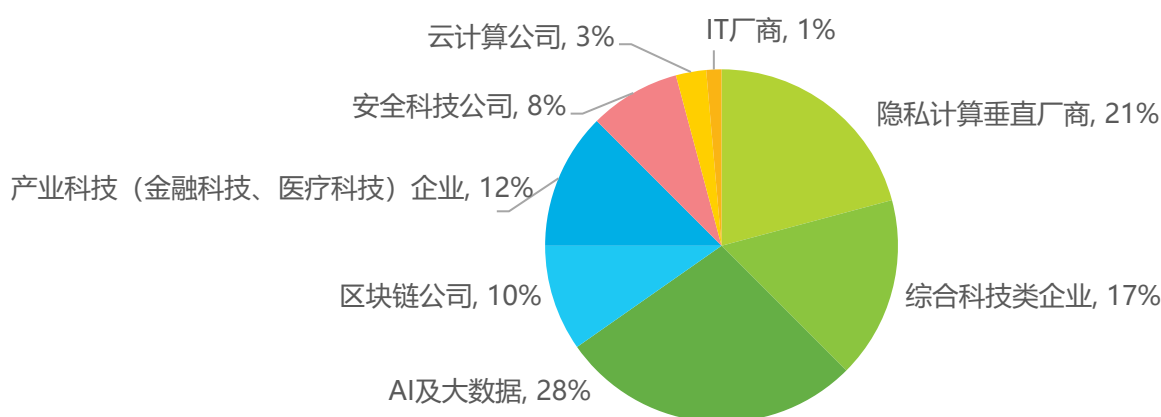
隐私计算商用元年的市场表现



（三）产品供应商：多元化背景的科技企业布局隐私计算，资本也推动着创业型隐私计算厂商加入市场，呈现百家争鸣的格局

虽然2021年是隐私计算的商用落地元年，但一些具备前瞻技术布局的企业早已开始探索隐私计算技术，如蚂蚁集团早在2016年便开始布局隐私计算；微众银行在2018年开始探索联邦学习的应用。资本也在推动着创业型企业进入市场，在2016年便有相关融资事件，但资本热度高峰期（融资事件最多的年份）体现在2020年和2021年。此外，还有AI、大数据、区块链、云计算、金融科技等多元化背景的企业，也都在市场热度的影响下，纷纷入局隐私计算赛道，市场呈现百家争鸣的格局。

隐私计算市场初期的供应商类型及占比



注释：“隐私计算市场初期的供应商类型及占比”统计范畴是：通过了“中国信通院、国家金融科技测评中心（银行卡检测中心）、中国金融认证中心（CFCA）隐私计算产品测评”的科技企业（金融机构、运营商等非技术企业不在统计范畴内）；此图反映的是市场初期的供应商类型，所以统计时间截至2022年12月。

来源：艾瑞咨询。

3. 数据流通服务初期探索热潮

在这个周期阶段（2021~2024），数据运营和交易等数据流通服务所发挥的作用有限，远未能形成规模化且可持续的价值流通范式，但收获了探索性的实践经验

早于2021年，部分数据流通服务机构已先行成立，但随着2021年数据可信流通市场热潮和部分相关政策陆续推动，数据交易所、数据商、数据经纪人等机构的数量在接下来的几年里不断增加。但受制于数据持有方开放意愿低、缺乏杀手铜级别的数据产品或价值场景、安全合规顾虑以及确权定价等制度尚未完善，多数早期探索者陷入“叫好不叫座”的困境。在这个发展时期，部分技术公司试图以隐私计算跨平台互联互通生态来探索数据运营业务，同样未能规模化落地，数据运营业务仍以撮合为主而非依靠生态平台，未形成可持续收入。这些初期探索，为后续的产业发展和政策制定积累了宝贵的探索实践经验。

概念说明，避免读者混淆



数据流通服务的统一用语来源于：国家数据局等部门于2026年2月3日公开发布的《关于培育数据流通服务机构 加快推进数据要素市场化价值化的意见》中的定义。在产业初步探索期（2021~2024）还未将“数据流通服务”作为统一用语。市场多见数据交易、数据运营等表达方式，但这些均属于数据流通服务的一部分。

数据流通服务：是指链接数据供需双方、促进数据要素全链条价值转化的专业化服务。涵盖数据归集、治理、加工、产品开发、供需撮合、交易交付、合规安全、收益分配等完整流程，**是数据要素市场化配置的核心业务范畴。**

市场早期的数据流通服务机构举例：

这里列举的是一些代表性的案例供读者参考，不代表市场全局。

1



数据交易所/中心：这是市场初期最具代表性的探索者，由政府或国资主导建立，旨在搭建一个合规、可信的数据流通平台。贵阳大数据交易所挂牌运营后，北京、上海、深圳等各地也纷纷跟进，掀起了一波建设热潮。

2



数据商：作为数据交易的“卖水人”，他们直接提供数据产品和服务。例如，专精于国有数据增值运营的“数据宝”，其客户包括字节跳动、华为等知名企业；广西智桂通科技有限公司则通过建设公共数据运营平台汇聚政务数据资源。

3



数据经纪人：这是一种制度创新，类似于数据交易中的“持牌中介”。例如：2022年8月，广州市海珠区率先试点，遴选出广东电网能源投资有限公司、广州金控征信服务有限公司、广州唯品会数据科技有限公司作为全国首批“数据经纪人”。

4



技术服务商：期望通过隐私计算跨平台互联互通生态建设，建立一个数据可信运营网络来链接数据源和数据使用者，并在他们具备业务KnowHow的领域，提供数据对接、数据产品销售等服务。

4. 市场降温，进入短暂下行期

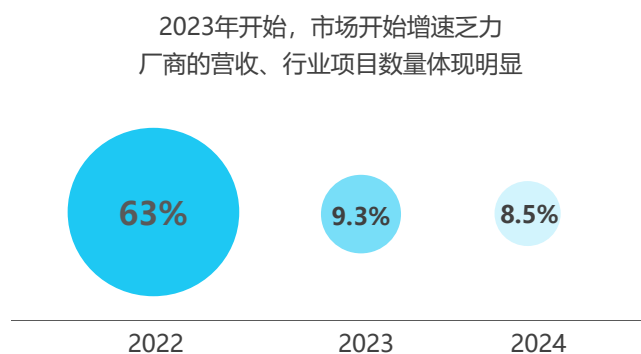
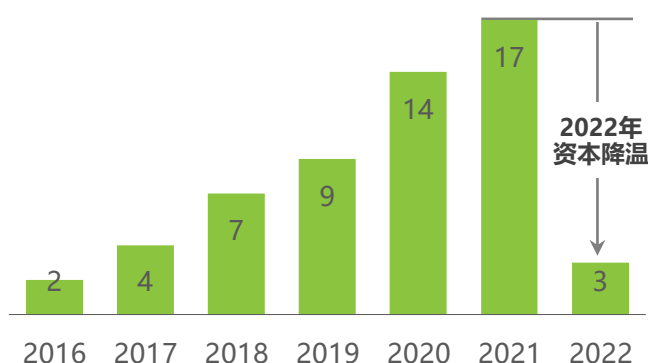
2022年资本热度骤降，一些无法自我造血的厂商在未来1~2年内陆续退出市场。能够商业闭环的企业也因市场需求增长乏力，叠加客户回款周期长等因素而面临生存挑战，市场开始了第一轮大浪淘沙，随之行业中的“否定声音”也层出不穷

自2021年的资本热度高峰期后，2022年受经济环境下行等多维因素影响，行业融资事件数骤降。这对于创业初期的科技企业来说，是一个极大的生存挑战。即便头部隐私计算厂商年营收可达6000万上下（2021~2022头部厂商平均水平，各厂商会有不同程度的上下波动），但他们通常需要经营百人规模的团队，且同时期客户预算增长乏力、叠加很多企业回款周期较长（部分大型企业回款周期可达12~18个月），导致这些即便能够自我造血的厂商，也会受到“资本拖累，回款拖累”的双重打击而不得不裁剪团队规模或寻求被收购。

价格战也是影响市场发展的关键原因，很多厂商为了拿下标杆客户来赢取资本的信任，以接近0元的价格竞标，导致市场上的项目价格持续走低，10万元以下的项目占比接近20%。这样的市场乱象，也一度行业口碑下滑，更让厂商利润表现不佳。

最终的表现是：在2022~2024年，一些企业逐渐淡出市场——例如营收较低的隐私计算厂商、战略方向不满足此阶段市场需求的厂商（如聚焦算力加速的星云Cluster）关闭公司，也有头部隐私计算厂商被收购的案例。另外，一些布局了隐私计算的科技公司，也在逐渐战略放弃或淡化隐私计算业务。在这个阶段，市场中也不断出现“项目价值不明显、市场增长挑战、价格战不良竞争、数据运营及交易缺乏实质性进展”等否定的声音。

2016-2022年中国隐私计算融资事件数 2022~2024年中国隐私计算市场增速



站在当下回望过去：市场始终存在一些能够穿越周期考验的技术坚守者和价值创造者，例如大型互联网科技背景的蚂蚁集团，他们是中国互联网科技企业中，对数据可信流通相关技术投入最多且唯一能够持续10年坚定战略方向的企业，是真正穿越周期的企业。还有创业型公司（洞见科技等），他们在行业低谷期积极寻求新的出路并持续创造价值。这些企业经历了周期考验的同时，也在2025年可信数据空间建设的市场中，收获了新一轮产业增长的红利。

5. 大模型爆发

（一）大模型爆发，标志着“数据可信流通”与“新一代AI”的双轮技术周期进入叠加发展阶段

2022年底大模型、新一代AI技术开始快速发展：大模型于2022年11月30日ChatGPT发布后正式爆发，两个月内月活破亿；2023年GPT-4发布、国产模型集中亮相。随后的2024年大模型落地加速，政策规范与产业应用双轮驱动。

此时企业的大模型应用成熟度为“L1-探索试验级”阶段。通常是技术领先且拥有资金实力的大型企业，会进行大模型项目的采购，企业级落地场景处于探索阶段。

**L1****探索试验级**

企业内单点应用

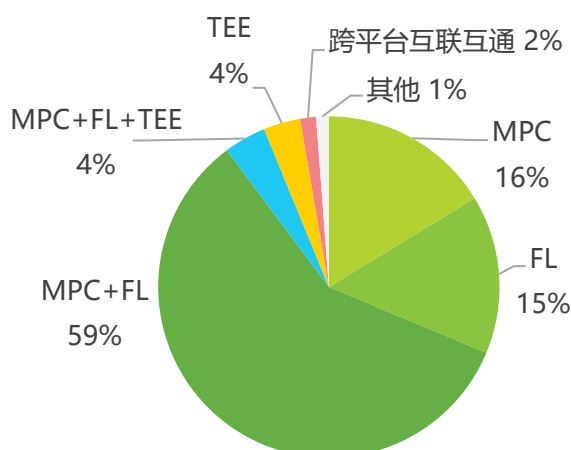
此阶段的AI尝试是自发、零星且混乱的。企业缺乏正式的AI战略和资源投入，应用通常局限于个别员工或团队的孤立探索，成果难以预测和复制。此时的重心是“点”上的突破，验证AI在特定任务上的可行性。

@ 中国企业AI应用成熟度AIM²模型，完整内容见报告前文。

（二）在这个阶段，以大模型为核心的新一代AI仅处于企业探索性落地阶段，其对数据可信流通的需求尚处酝酿期。市场仍以传统AI业务小模型的可信联合建模项目为主

由于此时的数据可信流通市场正在经历下行波折，因此一些大厂背景的隐私计算厂商，开始寻找隐私计算和大模型的结合机会，当时，这些思考更多是一种战略性探索，此时大模型主要以公开数据训练为主，且在落地初期阶段，暂未涌现对数据可信流通的规模化需求，但我们发现，在这个阶段的一些大模型厂商却已经开始关注AI带来的数据安全问题并开始采纳密态计算技术。综合来看，这一阶段隐私计算对AI的赋能还主要停留在传统AI，即：面向场景或业务的小模型可信联合建模，具体可见下述数据。

数据可信流通产业的初步探索期（2021年-2024年）的隐私计算项目类型占比

**~74%**

和联邦学习相关的隐私计算平台类项目占比达到74%。

在多种类型的技术方案及方案组合中，客户对MPC+FL技术方案的选择集中度最高，其次是FL类项目。

6. 重要转折点：国家数据局成立

面对市场增长困境，2023年国家数据局的成立恰逢其时，是中国数据可信流通产业能够从“初步探索期”迈入“敏捷实践期”的核心驱动力

如前文所述，此时的市场面临着需求增长乏力、资本市场趋冷等多重挑战，按照技术发展的周期性（E-Cycle曲线）规律来看，如果此类挑战出现在初步探索期阶段，会让技术面临发展停滞或失败的风险。国家数据局的成立破解了这一困境。

相比于大模型爆发所带来的只是技术趋势下的数据可信流通需求的增长愿景；而数据局的成立，则为中国数据可信流通产业的发展提供明确的方向和实质的推进行动：

国家数据局于2024年推出《可信数据空间发展行动计划（2024—2028年）》，并于2025年确定了首批试点单位；以及国家数据局联合有关部门陆续出台的《国家数据基础设施建设指引》《关于促进企业数据资源开发利用的意见》《关于促进数据产业高质量发展的指导意见》《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》等多项政策，为产业发展提供了系统化的政策支撑。

这些政策及举措，破解了阶段性市场困境，让数据可信流通产业周期可以迈入下一发展阶段。

国家数据局成立以来，发布的数据要素流通相关政策（部分列举）

虽本章节的研究时间范围是2021—2024年(历史回顾)，但为确保内容完整，此处列举的政策不限制时间范围

时间	文件名称	涉及部门	主要内容与价值
2023年12月31日	《“数据要素×”三年行动计划（2024—2026年）》	国家数据局等17部门	选取12个重点行业和领域，推动发挥数据要素乘数效应，提出到2026年底，打造300个以上典型应用场景，实现数据产业年均增速超过20%的核心目标。
2024年12月31日	《国家数据基础设施建设指引》	国家发展改革委 国家数据局 工业和信息化部	文件提出：2024—2026年，利用2—3年左右时间，围绕重要行业领域和典型应用场景，开展数据基础设施技术路线试点试验；2027—2028年建成支撑数据规模化流通、互联互通的数据基础设施，数网、数算相关设施充分融合；到2029年，基本建成国家数据基础设施主体结构。
2024年9月21日	《关于加快公共数据资源开发利用的意见》	中共中央办公厅 国务院办公厅	以促进公共数据合规高效流通使用为主线，聚焦破除公共数据流通使用的体制性障碍、机制性梗阻，从扩大资源供给、规范授权运营、鼓励应用创新、营造良好环境、强化组织保障等方面提出了17项具体措施，旨在充分释放公共数据要素潜能。

—— 更多见下页 ——

—— 接上页 ——

时间	文件名称	涉及部门	主要内容与价值
2024年11月21日	《可信数据空间发展行动计划（2024—2028年）》	国家数据局	文件提出：分类施策推进企业、行业、城市、个人、跨境可信数据空间建设和应用。到2028年可信数据空间运营、技术、生态、标准、安全等体系取得突破，建成100个以上可信数据空间。
2024年12月20日	《关于促进企业数据资源开发利用的意见》	国家数据局 中央网信办 工业和信息化部 公安部 国务院国资委	围绕健全企业数据权益实现机制、培育企业数字化竞争力、赋能产业转型升级、服务经济社会高质量发展、营造开放透明可预期的发展环境、保障措施方面给出了具体意见。
2025年1月6日	《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》	国家发展改革委 国家数据局 中央网信办 工业和信息化部 公安部 市场监管总局	文件提出：到2027年底，规则明晰、产业繁荣多方协同的数据流通安全治理体系基本构建，数据合规高效流通机制更加完善，治理效能显著提升，为繁荣数据市场、释放数据价值提供坚强保障。
2025年1月8日	《公共数据资源授权运营实施规范（试行）》	国家发展改革委 国家数据局	明确了公共数据资源授权给符合条件的运营机构开展合规治理开发、提供脱敏去标识化的公共数据产品与服务的全流程条件、程序及监管规则，旨在规范授权运营活动、保障数据安全与主体权益、培育全国一体化数据市场、充分释放公共数据要素价值。
2026年2月3日	《关于培育数据流通服务机构 加快推进数据要素市场化价值化的意见》	国家数据局 工业和信息化部 公安部 中国证监会	明确三类数据流通服务机构：数据交易所（中心）、数据流通服务平台企业、数据商。到2029年底，数据流通服务机构能力显著提升，流通交易形态更加多元，数据产品和服务更加丰富，各类主体供数用数意愿持续增强，全社会数据流通利用水平明显提高。
2026年4月15日	《关于推进行业高质量数据集建设行动的实施方案（征求意见稿）》	国家数据局综合司	文件提出：到2028年底，建成一批覆盖重点领域、经过应用验证的行业高质量数据集，打造一批数据驱动人工智能创新发展的典型应用场景，培育一批具备领先优势的创新型数据企业 and 专业人才，形成一批行业高质量数据集建设标准和工具。

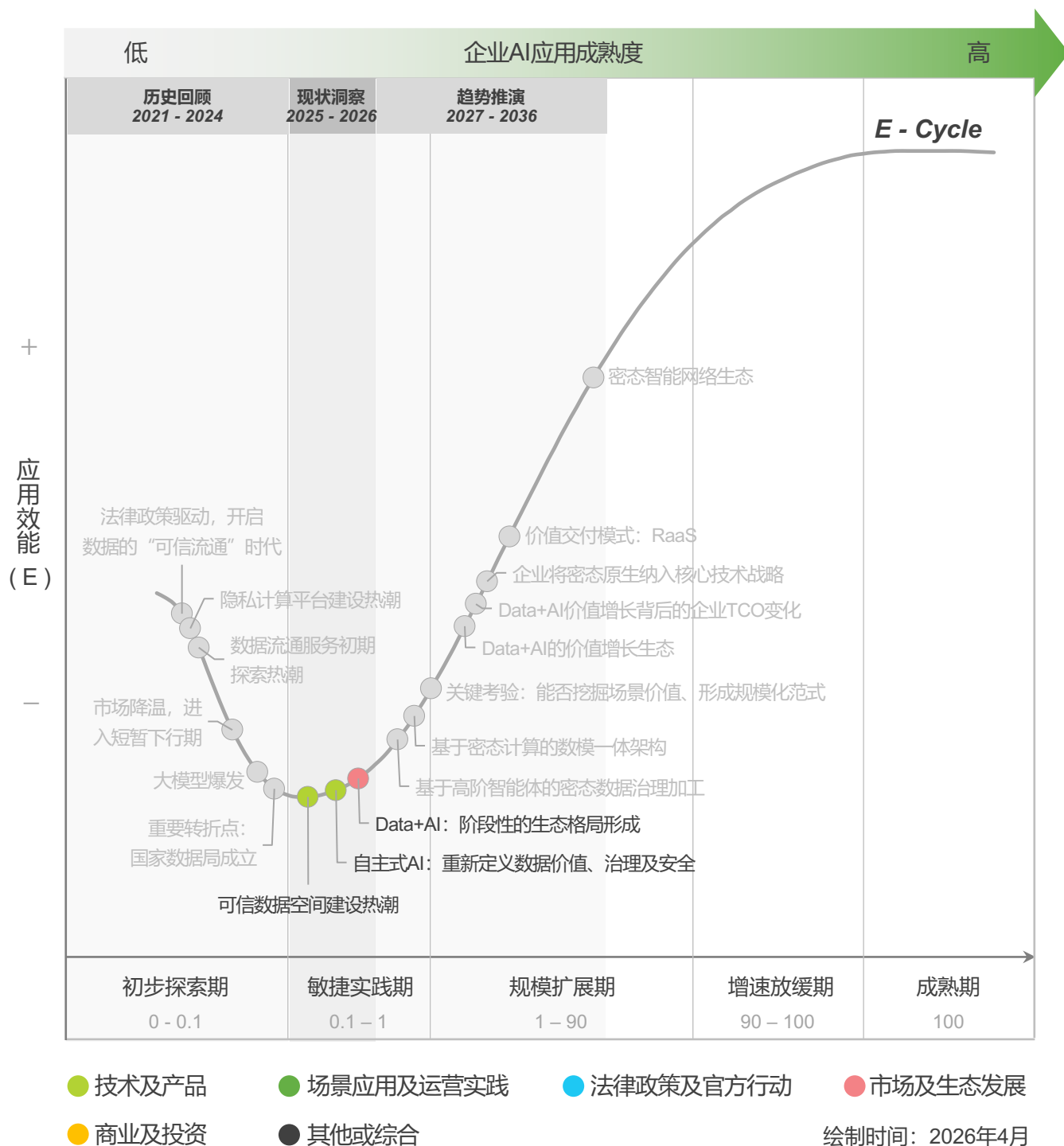
来源：国家发展改革委官网、国家数据局官网等公开信息，艾瑞咨询研究绘制。

现状洞察

2025年 — 2026年

现状洞察

中国AI时代的数据可信流通产业周期洞察 – 现状洞察



注释1: 横纵坐标轴定义

- 横轴体现技术发展所处的阶段 (综合应用范围、用户覆盖度等指标综合评估)。
- 纵轴定义的应用效能表示技术带来的价值回报 (综合总体拥有成本<TCO>、投入产出比<ROI>等指标综合评估)。

注释2: 各发展阶段的周期规律和具体表现, 在对应章节部分详细解读。

来源: 艾瑞咨询。

当前（2025—2026年）正处于产业周期的“敏捷实践期”阶段。

敏捷实践期的规律及经验

- 1  **该阶段的核心目标：**产品由早期接受者向更广泛的用户拓展，并在业务场景中通过持续敏捷实践，探索规模化范式。

该阶段的关键表现：

整体上处于技术价值回报的初期阶段（E-Cycle曲线开始呈现上升走势），由于初步探索期的部分项目走向失败，市场期望也逐步回归理性。

- 2  **产品更迭：**一些技术的发展周期中，此周期阶段会出现新一代产品，尤其是在初步探索期的初代产品未能取得客户持续投资的情况下。新一代产品可能是：前一代产品在原有技术或功能上的升级迭代、与新技术融合的新一代产品、更高级战略定位的产品。新一代产品的出现或将带来新的投资热度，让市场迎来第二轮增长的小周期。

市场供应商更迭：无法实现正向营收、亦未获得持续资本支持的企业逐步退出市场；新一代产品会促进新的供应商同步进入市场。

- 3  **风险警示：**如果此阶段无法探索出产品、运营或商业价值方面的规模化落地范式，技术发展将停滞或宣告失败。这里定义的规模化范式是指在小范围验证且可推广的策略。

核心摘要 @ 现状洞察（2025 – 2026）

- 1  **可信数据空间由国家自上而下推动建设，开启了建设热潮：**2025年是可信数据空间建设的元年，国家及地方推出了可信数据空间试点项目。城市可信数据空间项目数约占五分之一，项目金额相对较大；行业和企业可信数据空间项目数量占比最高；跨境可信数据空间已开始落地探索。

- 2  自主式AI的发展，让数据从被动支撑业务，变为主动循环创造价值。推动数据治理从传统静态管控，转向静态与动态并重的综合治理模式。自主式AI需要在不影响其自主运行前提下，在密态环境中使用数据完成自主作业，确保原始明文数据不出权属主体、不泄露，规避数据被反向溯源的风险。

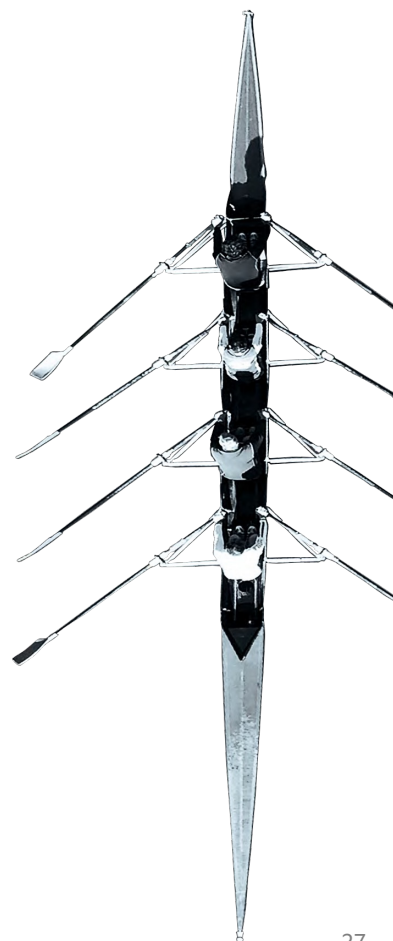
- 3  **现阶段数据治理加工断层，成为场景用数鸿沟，生态格局仍在不断发展和完善中。**国家数据局等部门提出培育数据流通服务机构。预计部分传统的数据流通服务机构（如数据交易所等）或将被清退和整合。
中国数据可信流通产业有望撬动万亿市场规模，早期实践探索将产生关键影响。

E-Cycle - 现状洞察部分，包含下述三个周期用例：

用例1 | 可信数据空间建设热潮

用例2 | 自主式AI：重新定义数据价值、治理及安全

用例3 | Data+AI：阶段性的生态格局形成



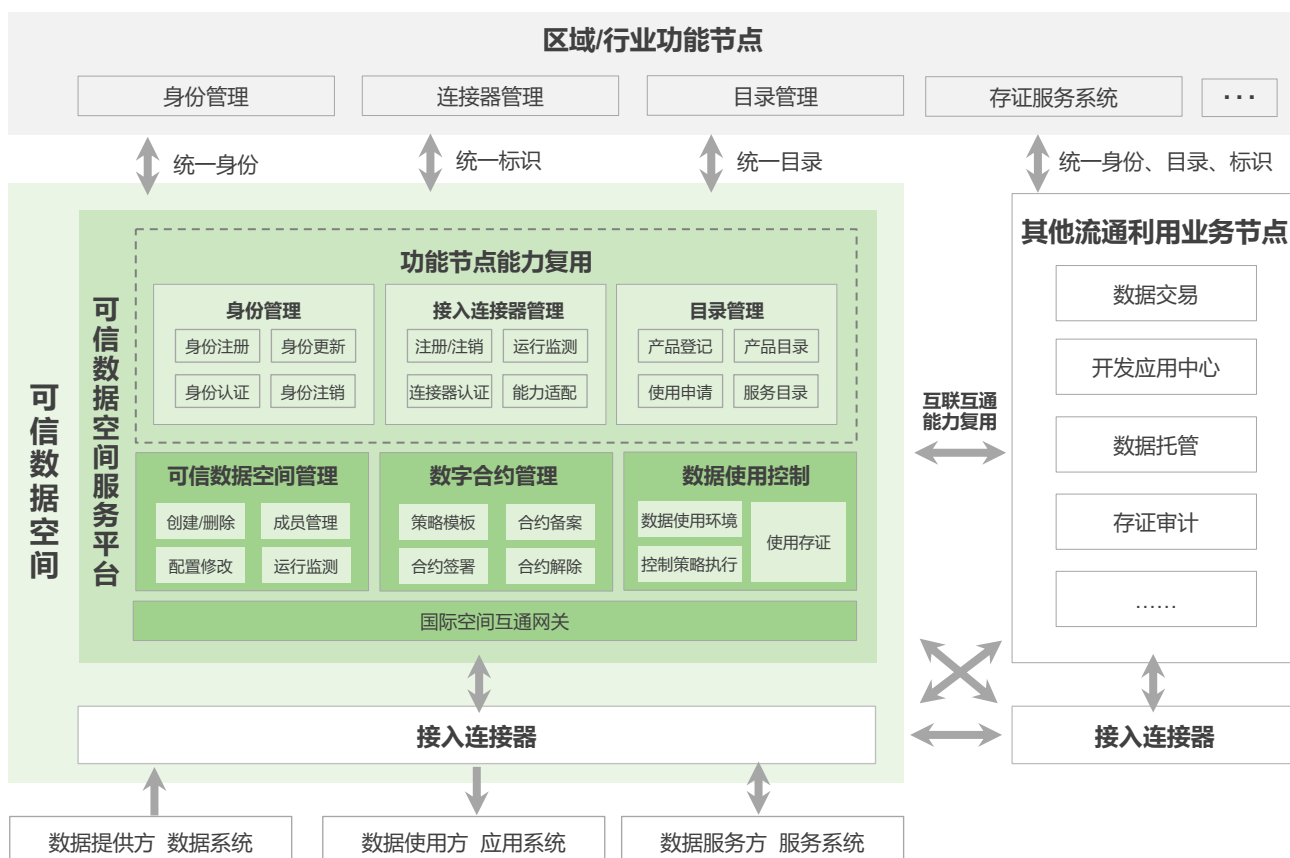
可信数据空间 – 简要介绍

可信数据空间是基于共识规则，联接多方主体，实现数据资源共享共用的一种数据流通利用基础设施，是数据要素价值共创的应用生态、支撑构建全国一体化数据市场的重要载体

国家数据局于2024年推出《可信数据空间发展行动计划（2024—2028年）》，提出分类施策推进企业、行业、城市、个人、跨境可信数据空间建设和应用，数据可信管控、资源交互、价值共创是可信数据空间须具备的三类核心能力。在此基础上，国家数据局还指导全国数据标准化技术委员会秘书处，组织地方政府、科研院所、高等院校、企业等160余家单位，编制了《可信数据空间 技术架构》并于2025年4月发布，从技术功能、业务流程、安全要求等方面对可信数据空间进行了规范。此后陆续出台的《可信数据空间 能力要求》《可信数据空间标准体系建设指南》等多项文件，为可信数据空间落地建设提供标准规范。

安全能力的集成补充：通用可信数据空间架构主要包含可信数据空间服务平台、接入连接器。隐私计算/密态计算并不是这个架构中的原生化必选能力，但供应商为了满足客户对高敏感数据的隐私保护需求，会在接入连接器的扩展能力中集成隐私计算（如洞见科技、安恒信息）来提供数据隐私保护的能力，或是在通用可信数据空间架构中增加密态计算底座（如蚂蚁密算）实现基础设施安全能力的内生性。

通用可信数据空间架构



来源：可信数据空间的定义来源于《可信数据空间发展行动计划（2024—2028年）》、艾瑞咨询研究绘制。

可信数据空间 – 试点推进情况

2025年是可信数据空间建设的元年，国家及省市区域联动推进可信数据空间试点建设

顶层规划：国家数据局发布的《可信数据空间发展行动计划（2024—2028年）》提出，到2028年，可信数据空间要在运营、技术、生态、标准、安全等体系上取得突破，建成100个以上可信数据空间，形成一批数据空间解决方案和最佳实践，基本建成广泛互联、资源集聚、生态繁荣、价值共创、治理有序的可信数据空间网络。

国家和省市区域上下联动、分层推进，构建全国可信数据空间试点体系：国家数据局2025年7月启动首批63个可信数据空间创新发展试点，涵盖13个城市、22个行业 and 28个企业三类可信数据空间。一些省市区域也同步推出了可信数据空间试点项目，和国家层面形成上下联动、分层推进的协同发展。

2025年国家及代表性省市的可信数据空间试点情况

国家可信数据空间创新发展试点		
63个可信数据空间创新发展试点 (13个城市类、22个行业类、28个企业类)		覆盖全国 20 余个省区市、 32 个国民经济行业大类
江苏省 可信数据空间“123+”项目库入库项目 40个 企业类9个 行业类20个 城市类7个 跨境类4个	北京市 第一批可信数据空间储备项目 21个	无锡市 可信数据空间首批入库名单 20个 企业类9个 行业类9个 城市类1个 企业、跨境类1个
上海市 第一批可信数据空间创新试点项目 18个 企业类5个 行业类13个	河北省 可信数据空间创新发展试点 15个 企业类7个 行业类4个 城市类4个	
天津市 可信数据空间创新发展试点 15个 企业类7个 行业类7个 城市类1个	湖北省 可信数据空间创新发展试点 15个 企业类4个 行业类8个 城市类3个	其他

来源：国家数据局、各地方数据局（大数据管理局）或地方政府相关官网、艾瑞咨询研究绘制。

可信数据空间 – 项目落地情况

政策指导

国家数据局对五类可信数据空间培育推广行动的态度分别为——积极推广企业可信数据空间、重点培育行业可信数据空间、鼓励创建城市可信数据空间、稳慎探索个人可信数据空间、探索构建跨境可信数据空间。



- **市场中的项目概述：**2025年~2026年4月份，市场已涌现数百个可信数据空间项目，除了国家及地方政府推进的试点项目外，还有市场中自主发起的相关项目。项目需求极为多元化，订单金额最低至数十万元（大多为咨询服务，而非平台建设）、最高可达数亿元。一些预算过亿的项目，通常会包含算力和存储等数据基础设施或其他非可信数据空间的服务内容。项目通常会根据功能建设需求、实施阶段规划、项目金额与管理效率等因素来划分标段（目前1~3个标段居多）并在各个标段选择对应的供应商。
- **试点项目之外，一些市场中自主发起的项目存在失败风险：**市场热度高涨带来的项目数量激增的背后，一些市场中自主发起的项目，存在缺乏明确建设目标、投资运作不透明等现象，未来或将面对建设不善或无法持续运营等问题而让项目失败。
- **客户信任关系 vs. 产品竞争力：**集成与分包，是可信数据空间项目的常见情况，但在一些中标项目中，甚至发现一些中标企业没有可信数据空间产品，而是完全依靠将项目分包给产品厂商，来为客户提供交付。此类项目更多是基于客户信任关系驱动。
- **供应商竞合生态：**由于很多可信数据空间项目金额较大，招标单位会对供应商的企业发展稳定性、团队规模等方面拥有一定的要求，大型国企或者大型科技公司在这方面更具优势，一些垂类技术背景的专业供应商、或是规模较小的厂商会选择和集成商合作，但是这些公司在一些项目中也会直面客户签约，因此构成了市场的竞合生态。

一、当前城市可信数据空间项目数约占五分之一，项目金额相对较大

- 很多此类项目金额集中在千万级到几亿元区间，同时也有一些城市可信数据空间项目的金额在百万级别。招标单位多见于城市数据集团、地方数字产业集团等类型的企业。
- 城市可信数据空间是很多供应商的主要目标市场，典型供应商包含三大运营商、中国电子云、浪潮云等央国企背景的公司；蚂蚁集团等大型科技背景的公司；以及垂类技术赛道背景（如隐私计算、区块链、安全等）的供应商；还包括一些地方性平台企业等，一些城市可信数据空间项目会优先于地方公司参与建设。



各价格区间典型项目举例 – 城市可信数据空间项目

百万级

常州市城市可信数据空间
建设项目金额为274.5万元

千万级

雄安新区城市可信数据空间项目建
设实施（一批次）金额约3166万

上亿级

济南城市可信数据空间建设项目
金额为1.8亿元
(一标段约1.2亿元、二标段约0.6亿元)

二、行业和企业可信数据空间项目数量占比最高

- 因为各行业/企业拥有差异化的数据应用场景和逻辑，因此这两类平台建设会有更多样化的定开需求。两类项目在部分情况下会存在一定的边界模糊性，例如一些领域的头部企业更偏向以行业可信数据空间进行立项，但在落地过程中，主要是和其供应链上下游企业之间进行跨主体数据流通，更符合企业可信数据空间的用途定位。
- 此类项目的建设方多见于行业主管部门、行业头部企业、各领域的代表型企业等各类主体。
- 从公开的招投标信息来看，行业类可信数据空间项目投资规模和场景范围相对更大，企业级项目则更聚焦于其供应链上下游或特定应用场景，这两类项目类型丰富度较高，难以简而概之。同时市场也充斥着一些预算高但实际服务内容与可信数据空间关联度低的项目。
- 除了市场主流的可信数据空间供应商外，具备产业KnowHow的供应商同样是重要的参与者，他们在金融、医疗、能源等专业领域积累了丰富的数据治理及应用经验而更加受到客户青睐。



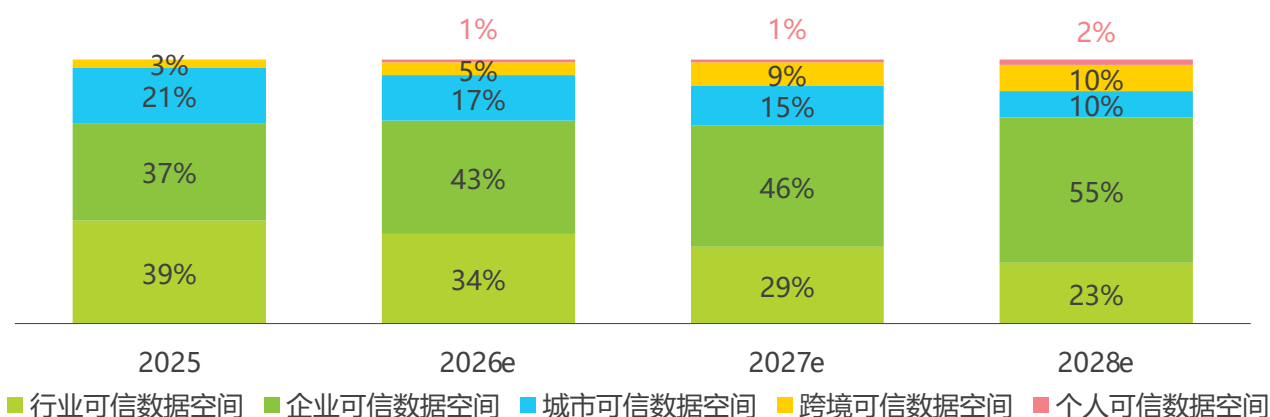
三、跨境可信数据空间已在探索中，世界数据组织的成立有望推进其发展；个人可信数据空间需要稳慎落地

- 跨境可信数据空间已在探索中：江苏省、无锡市推出了跨境可信数据空间试点项目。珠海市国资数字科技有限公司《粤港澳大湾区跨境及企业可信数据空间珠海枢纽建设项目》总投资1亿元对跨境及企业可信数据空间展开落地探索。
- 世界数据组织正式运行，将开启全球数据治理新格局，推动中国跨境数据可信流通的发展进而推动跨境可信数据空间的建设。
- 个人可信数据空间的落地需要稳慎探索，即便当前已经看到运营商等企业机构在探索其落地范式，但其价值场景和法律合规等诸多问题让其落地面临不确定性。

四、可信数据空间项目发展走势

- **项目收敛，优胜劣汰：**虽然目前市场的项目数量较多，但这其中不乏一些套用可信数据空间概念的低质量项目，长期来看，市场必将向着高质量、可落地运行的项目进行收敛。因此，未来的市场项目将呈现动态增减的趋势，新项目涌现的同时，也同步伴随着既有项目的优胜劣汰。
- 在未来四年的市场化项目上，企业类可信数据空间由于目标受众基数大而将获得明显的增长，这也和国家数据局提出的“积极推广企业可信数据空间”的指导方向一致。世界数据组织会成为推进跨境可信数据空间发展的关键力量。此外，行业可信数据空间将得到重点培育而获得高质量发展，推进数据的产业化价值落地。城市可信数据空间将推动公共数据资源开放。长期来看，在数据资源统筹规划和集中管理的背景下，各类可信数据空间的部署建设方式和数量，需要基于这四年发展探索的经验沉淀再进一步适配最优方案。

2025 - 2028年中国可信数据空间项目数量分布



注释：由于市场中出现一些省级的可信数据空间项目（例如：山西数据要素流通交易可信数据空间建设项目），虽然城市可信数据空间一词的命名未包含省级区域，但我们同样都将其纳入城市可信数据空间的统计范畴。

五、扩展研究 —— 其他数据可信流通产品的市场发展

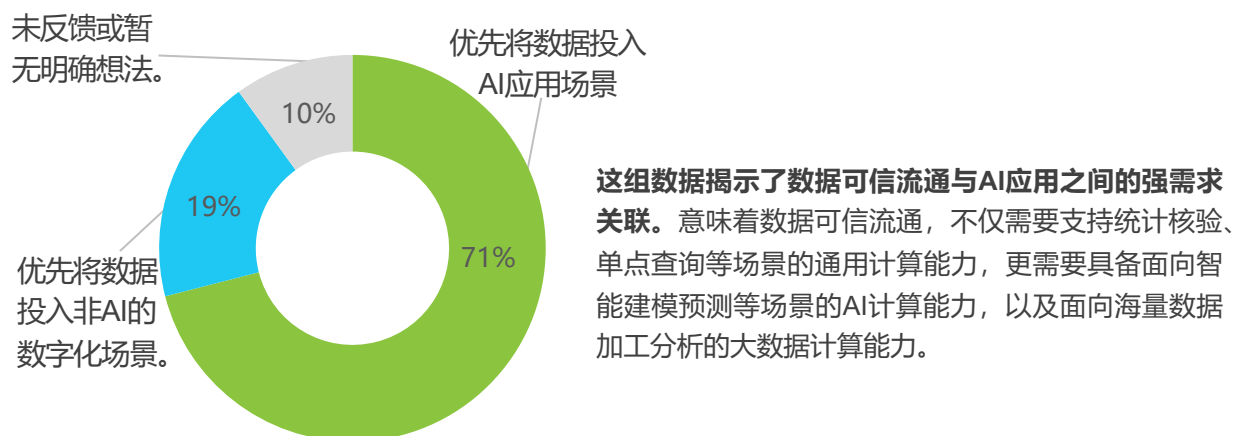
- 本报告定义的数据可信流通产品包括：增加密态底座的可信数据空间（密态可信数据空间）、在接入连接器中集成隐私计算的可信数据空间、隐私/密态计算平台、可信数据沙箱等一系列能够让高敏感数据实现可信流通的产品或技术解决方案。各类产品的定位、目标受众、需求场景会有所不同。**可信数据空间之外的其他产品发展情况，现进行概述说明：**

- 目前金融、政务等领域，依旧很多企业在采购密态计算/隐私计算平台、可信数据沙箱等产品，用以支持高敏感数据流通共享的隐私保护以及满足合规需求。相比于在初步探索期(2021—2024)，企业采购需求集中在可信联邦建模服务、基于密码学的数据可信流通解决方案，现阶段(2025—2026)，可信数据沙箱的采购占比在提升，我们还发现一些供应商推出了TEE+数据沙箱的软硬协同解决方案，也间接带动了TEE的使用占比。
- 站在隐私计算供应商的视角，他们的隐私计算平台销售不仅来源于终端企业客户，还有一些可信数据空间项目的集成商，需要在接入连接器中集成隐私计算时，也会与隐私计算厂商合作，对项目进行分包。
- 此外，大模型训练及AI智能体应用也在产生对密态计算的应用需求，我们已经看到此类项目的落地，例如通过密态计算支持医疗大模型训练保护患者个人隐私及医疗信息安全。

六、扩展研究 —— 数据可信流通产品应该支持多元化的计算能力

为适配数据的多元应用需求，数据可信流通产品必须具备多类型计算支撑能力，这是适配企业复杂业务场景、应用落地的前提。尤其是在企业级AI落地场景中，唯有支持AI计算与大数据计算能力，才能让数据要素的价值得以充分释放。而目前业内部分可信数据空间或企业数据可信流通平台仅支持通用计算。

企业获取跨主体的高价值数据的应用方向



多类型计算

通用计算

AI计算

大数据计算

高性能计算

其他

数据可信流通产品 / 平台

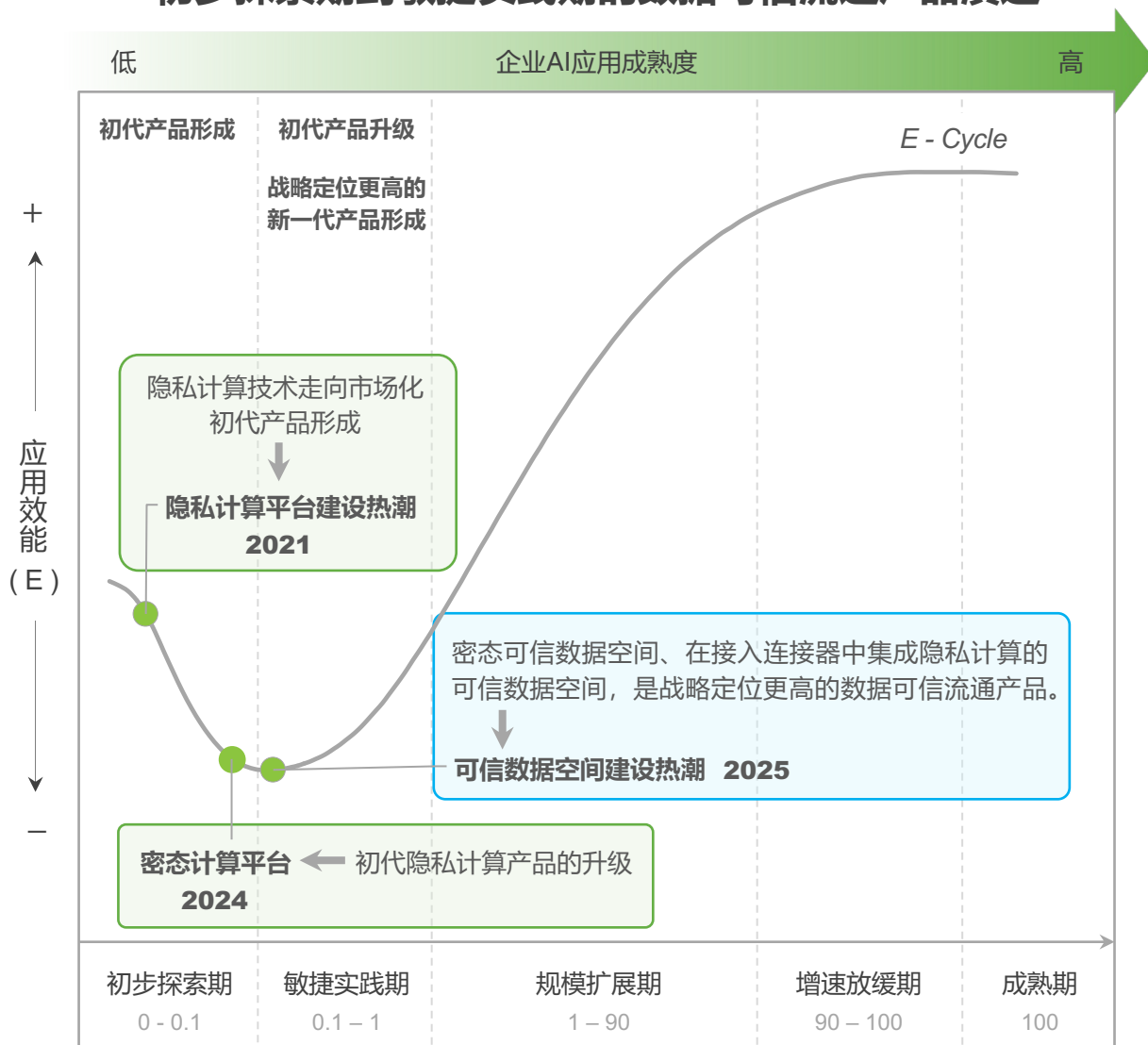
注释：N（机构数量）= 100，受访机构来自金融、政务、通信运营商、科技、医疗与健康、消费品与零售、制造业、能源与材料、工程与建筑等行业。我们的研究团队以访谈统计、问卷辅助的方式展开调研，以确保受访者能够更全面、更准确地表达观点。

来源：艾瑞咨询。

七、扩展研究 —— 回归技术周期视角的数据可信流通产品演进

- 初步探索期：初代数据可信流通产品是隐私计算平台，在前文初步探索期的回顾中已阐述。
- 敏捷实践期：此阶段的数据可信流通产品主要有两个关键的演进。1) 初代数据可信流通产品——隐私计算平台，现阶段已经出现了新一代的升级产品：密态计算平台。密态计算在传统隐私保护计算技术基础之上，强化了对全链路复杂计算的密态保护能力，且密态计算成本低于明文计算的1.5倍，提升了安全性和性能。2) 在接入连接器中集成隐私计算的 可信数据空间 或 增加密态计算底座的可信数据空间，是战略定位更高的数据可信流通产品，其不仅是一种数据基础设施，更是数据共享共治、价值协作的产业生态，也是推进全国一体化数据市场建设，推动数据要素市场化价值化的重要抓手。
- 规模扩展期：未来，一些数据可信流通产品或将逐步演变成支持数据价值落地和业务增长的系统。我们已经看到一些厂商在他们的数据可信流通平台上增加了数据治理、场景建模、甚至是场景应用等一系列能力，在数据流通服务场景中为客户提供更加全栈的解决方案。

初步探索期到敏捷实践期的数据可信流通产品演进



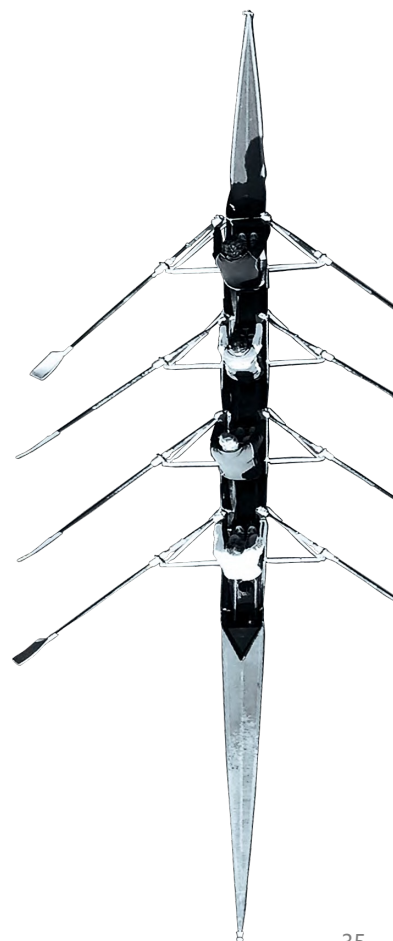
来源：艾瑞咨询。

E-Cycle - 现状洞察部分，包含下述三个周期用例：

用例1 | 可信数据空间建设热潮

用例2 | 自主式AI：重新定义数据价值、治理及安全

用例3 | Data+AI：阶段性的生态格局形成

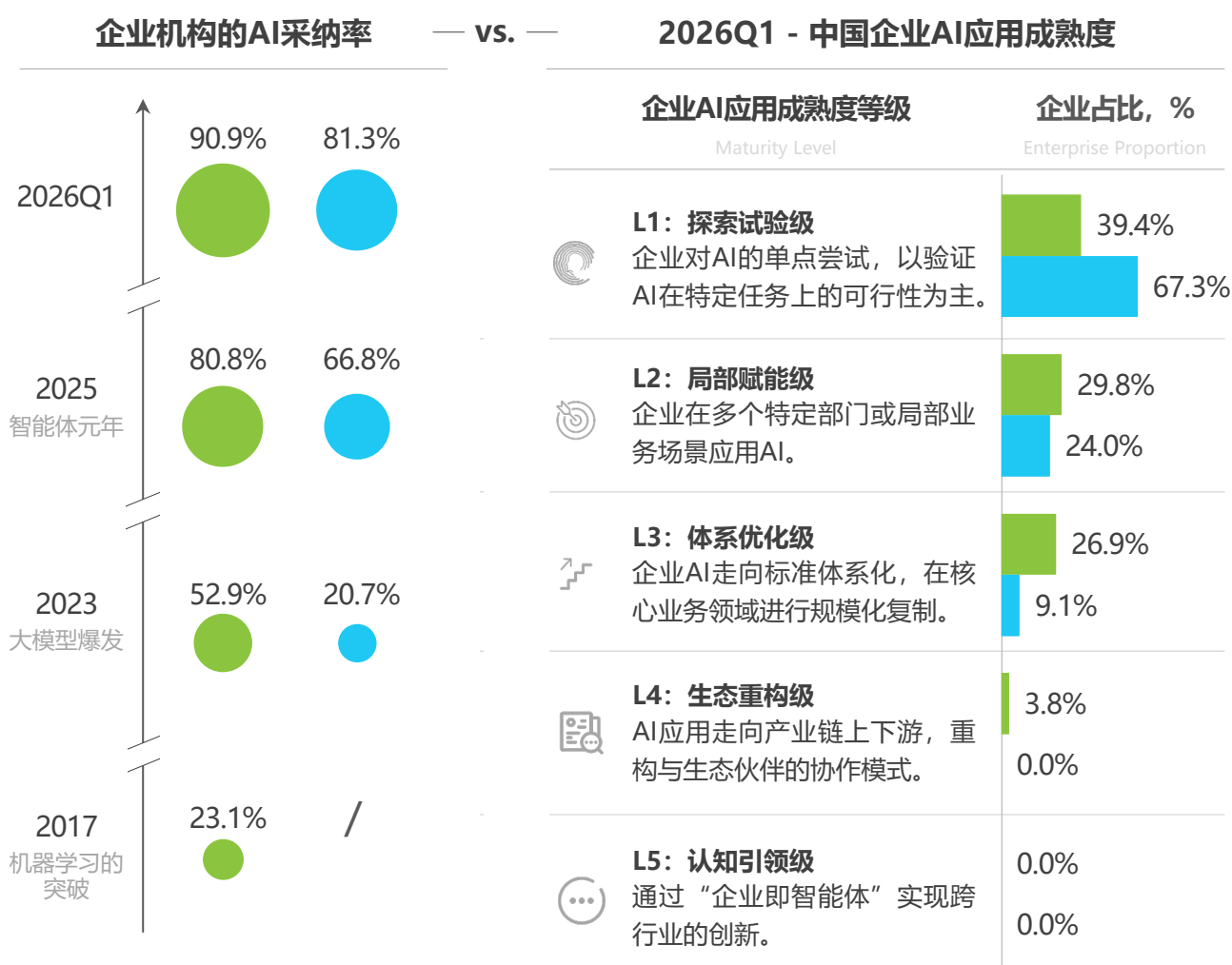


企业AI采纳率和AI应用成熟度

自主式AI的突破，驱动企业AI采纳率持续走高；但目前的企业AI应用呈现“浅层繁荣、广而不深”的特点，未能在专业场景中实现规模化可靠的落地

AI正在走进“千家万户”的企业中，企业AI采纳率持续高位。尤其是以OpenClaw为代表的自主式AI在2026年Q1这段时间集中爆发，让企业的AI采纳率进一步攀升。目前新一代AI在企业中的应用成熟度主要集中在L1、L2级别，主要是在通用辅助场景中快速普及，尚未在核心业务领域实现规模化复制，其落地深度与业务价值兑现远未达预期。

中国企业机构的AI采纳率及应用成熟度



● 整体的AI（包括大模型之前的传统AI、大模型为基础的新一代AI） ● 新一代AI（大模型为基础的新一代AI）

注释：N（机构数量）= 208，受访机构来自金融、政务、通信运营商、科技、医疗与健康、消费品与零售、制造业、能源与材料、工程与建筑等行业。我们的研究团队以访谈统计、问卷辅助的方式展开调研，以确保受访者能够更全面、更准确地表达观点。因四舍五入，各百分比之和可能不为100%。

来源：艾瑞咨询。

企业应该如何应用自主式AI

一、安全是首要问题

报告前文分析了自主式AI对数据的机遇和挑战，重点描述了因无边界上下文暴露、开放动态命令执行两类AI智能体的本源风险所催生的三大失控问题。本次的208家企业调研显示：失控问题导致对AI的信任缺失、数据隐私与安全顾虑已成为影响企业AI落地的三大核心问题的其中两项。风险敏感领域，如金融行业更是将安全列为采纳自主式AI的底线。

92.1%



92.1%的金融机构将安全合规作为智能体应用实践的前提和底线，表示如果影响安全合规将会立即终止对智能体的应用，直到能提供值得信赖的安全合规解决方案。

来源：艾瑞咨询《中国金融智能体发展研究与厂商评估报告（2025）》

二、企业应打造“数据 - 知识 - 智能体”自驱式增长飞轮，建立可靠、可控、可敏捷迭代的自主式AI系统

企业采纳AI的三大核心需求

□ **可靠性是企业采纳AI最为关注的方向之一。**企业核心关注的是AI能否按照业务要求可靠地解决专业领域的问题，例如在金融和医疗领域，业务决策的准确度直接关乎资金安全与生命健康，AI可靠性必须达到99%以上。因此，AI需要具备专业领域的KnowHow。本次企业调研显示，AI缺乏专业场景Know-How是影响AI落地的首要影响因素，也验证了上述观点。但目前企业AI面临着业务知识转化挑战：专业场景的核心Know-How多为资深业务专家掌握的隐性、非结构化经验，如果需要专家以大量的人工标注的方式进行知识注入，成本高

且专家参与意愿低。

- **失控的AI无法被企业采纳。**本次调研发现，“失控问题导致对AI的信任缺失”是制约企业采纳AI的第二位因素，这其中90%以上的受访者表示AI导致数据泄露失控让他们对是否应用自主式AI产生迟疑。企业AI的落地需要以决策受控、行为受控为前提。
- **受欢迎的专业AI背后一定有敏捷的迭代机制。**本次的208家企业调研发现，38.5%的企业会认为静态模型难适配动态业务是影响企业落地AI的原因。企业核心业务场景会随着市场、政策、流程持续动态变化，AI能否动态自适应业务是评估其效能的关键影响因素。企业需要AI能够通过鲜活动态数据进行不断地迭代优化、不断向任务目标收敛的自适应AI。形成越用越可靠、越用越专业的AI业务系统。

打造“数据 - 知识 - 智能体”自驱增长飞轮。

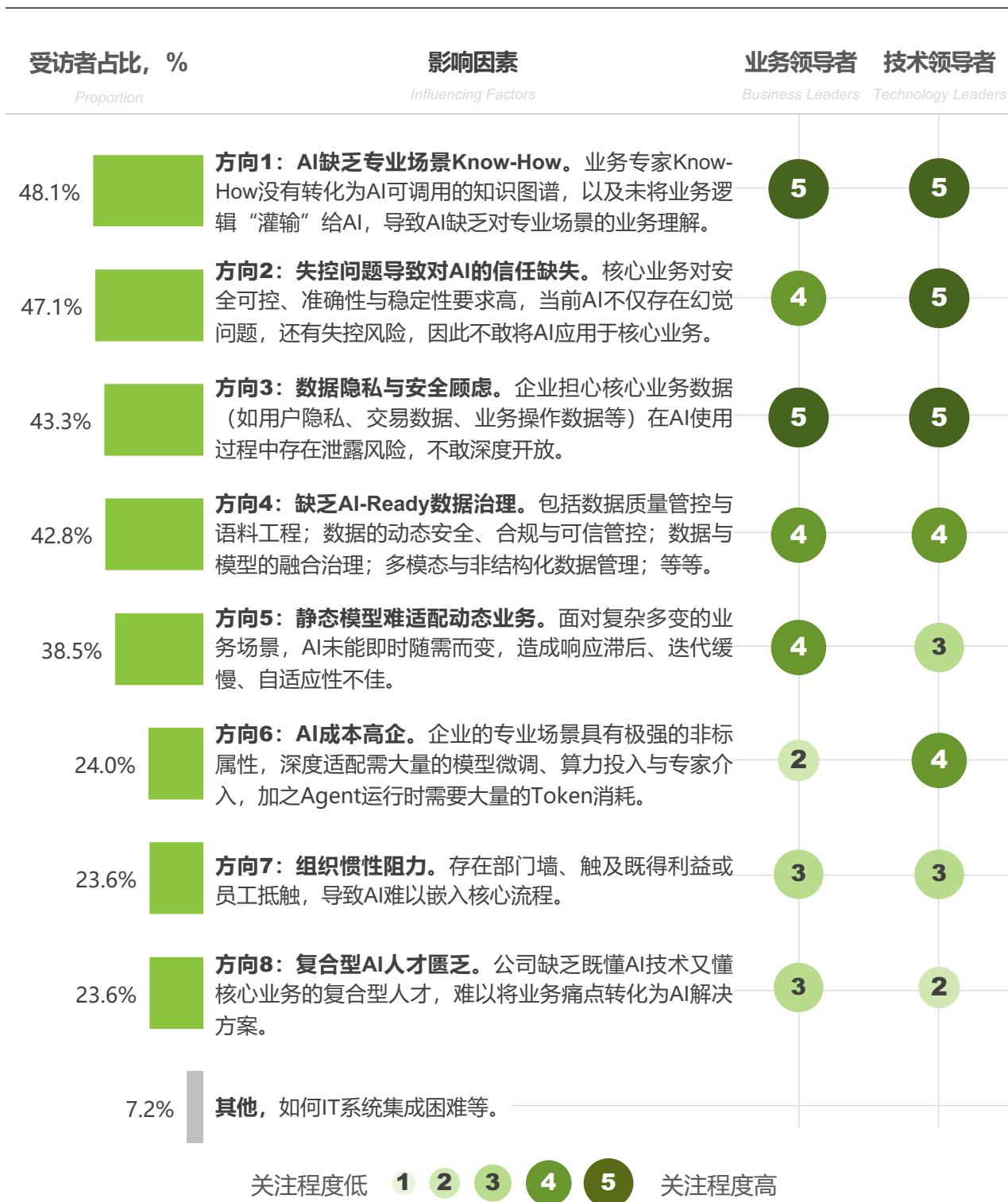
我们需要跳出传统只依赖模型训练、从沉淀的静态数据中寻求规律和经验的思维框架，而是在数据可信流通能力的保障下，构建“以智能体动态挖掘数据价值，通过闭环迭代的知识治理能力，来动态优化和沉淀业务知识，并持续对AI智能体执行结果进行核验”的自驱式增长飞轮。建立可靠、可控、可敏捷迭代的AI系统。



——接上页——

下述数据，支撑上文对企业应用AI需求的论述。

影响企业成功应用AI的关键因素



注释：N（机构数量）= 208，受访机构来自金融、政务、通信运营商、科技、医疗与健康、消费品与零售、制造业、能源与材料、工程与建筑等行业。208家企业机构中接受调研的专家画像包括：技术领导者、业务领导者、一线技术人员、一线业务人员。每位受访者根据实际的AI应用体验，选择“影响AI在企业核心业务中落地的原因”，每位受访者最多可以选择3个选项。我们的研究团队以访谈统计、问卷辅助的方式展开调研，以确保受访者能够更全面、更准确地表达观点。对于“影响AI在企业核心业务中落地的因素关注程度”的等级量表题，只有技术领导者、业务领导者参与此题的调研。每位受访的领导者会对各选项的关注程度进行1-5的评分，表格展示的是平均值的四舍五入计算结果。

来源：艾瑞咨询。

自主式AI让数据产生哪些变化

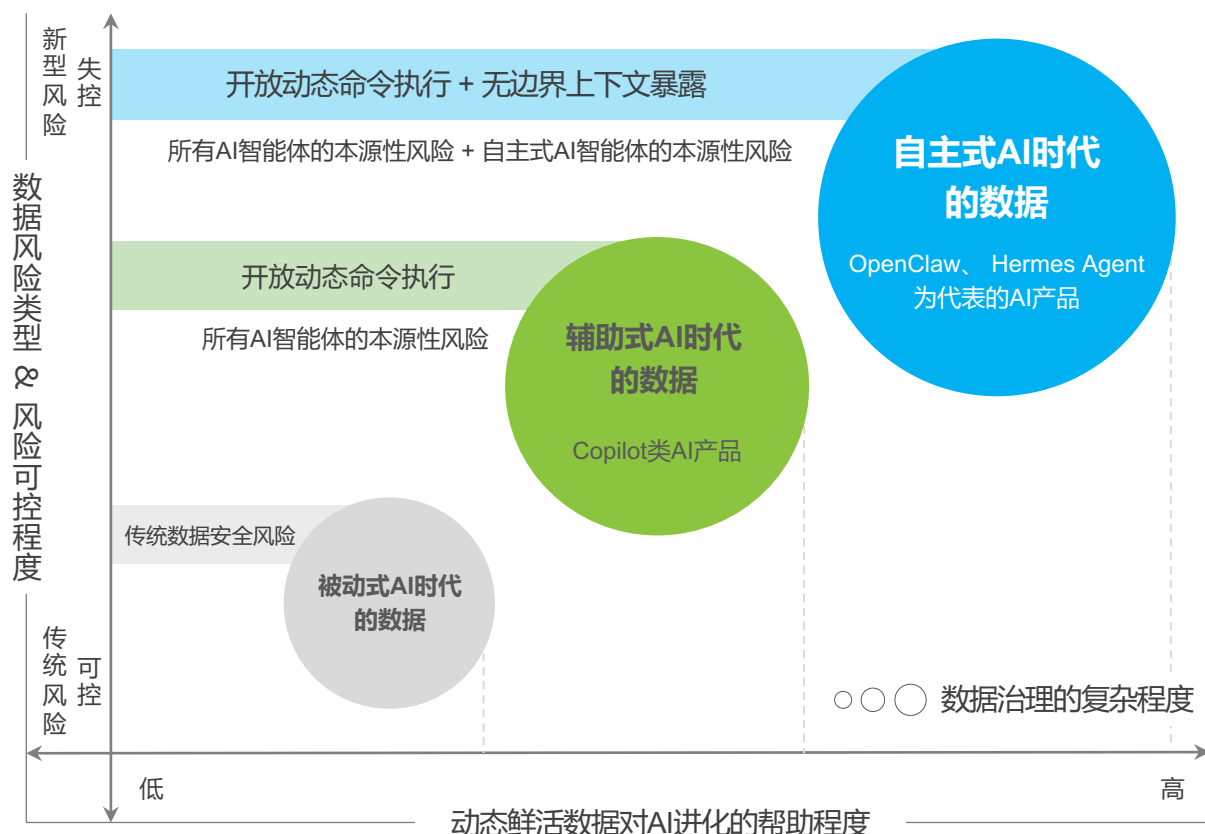
数据价值：自主式AI依托动态鲜活数据实现闭环收敛的自主迭代，重新定义了数据的时效价值与流动价值

传统模式下，数据多为静态采集、被动使用，价值释放高度依赖人类加工与场景匹配。而自主式AI的发展下，数据不再仅通过作为燃料用来训练模型而提升AI能力，更是可以通过在AI自主交互、推理、迭代过程中持续产生新数据和新知识，形成“数据训练AI→AI产生新数据”的自循环价值链条，让AI实现自主进化。数据由此从单一的业务支撑资源，升级为驱动自主式智能体决策与迭代的核心燃料。在未来，或将会影响数据价值的评估、流通与应用规则。

数据治理：自主式AI推动数据治理从传统静态管控，转向静态与动态并重的综合治理模式，传统的人工治理方式将无法满足需求，企业需要构建利用AI进行数据治理的新范式

在自主式AI落地之前，数据治理更多面向结构化、存量型的静态数据，治理上侧重数据标准、质量校验、资产目录等内容维度，难以适应实时变化的数据场景。新一代数据治理应建立双轨体系：一方面，延续对存量静态数据的规范管理，保障基础数据资产稳定可靠；另一方面，需要面向动态数据流构建实时治理能力，适配智能业务发展。传统的人工数据治理模式无法满足需求，数据治理智能体的应用将成为重要趋势（详细内容见趋势推演的Forecast 01）。

AI范式跃迁下的数据价值、风险与治理的变化



来源：艾瑞咨询。

数据安全：自主式AI需要在不影响其自主运行前提下，在密态环境中使用数据完成自主作业，确保原始明文数据不出权属主体、不泄露，规避数据被反向溯源的风险

自主式AI的数据密态可信流通需求，与传统多方数据共享、联合建模模式存在差异：传统模式下的数据处理多以静态数据为主，多需人工参与调度；而自主式AI可以在无人工干预的情况下，实时处理外部输入、运行中间数据与自主生成的衍生数据，动态性与全流程闭环特性更强。而这些动态数据涉及用户隐私、企业商业机密，一旦随意流转就触犯合规条例或引发商业/信誉危机。

对此，企业应根据自主式AI的不同业务场景与数据敏感度，选择差异化的数据隐私保护技术方案，例如可信联邦学习、密态计算等，在保障AI自主运行效率的同时，平衡数据安全性。

在《数据安全法》《个人信息保护法》的法律法规框架下，自主式AI的数据隐私保护已是刚性刚需。目前已有不少率先应用自主式AI的技术领先型企业，开始关注自主式AI的数据可信流通价值场景，其关注的方向如下图所示：

领先的AI实践者关注的自主式AI数据可信流通价值场景

场景类型 <i>Scene</i>	非技术背景从业者 <i>Business</i>	技术背景从业者 <i>Technology</i>
 防范AI导致数据泄露： 防止AI把敏感信息编进生成内容、通过交互诱导AI吐出数据。	 91.3%	 81.7%
 防止从生成结果反推原始数据： 例如通过企业经营AI做预测而反推商业隐私数据等场景。	 64.9%	 78.4%
 防止通过交互、嗅探AI运行窃取数据。 防止模型参数、业务规则、商业策略等内容泄露。	 63.0%	 64.9%
 只要处理AI数据中的敏感信息，就要开启隐私保护模式，实现最小必要性的合规要求。	 28.8%	 26.4%
 防止跨主体运行的AI智能体协同导致的数据出域的合规性和隐私安全性。	 24.0%	 28.8%
 其他	 7.2%	 13.9%

注释：N（机构数量）= 208，受访机构来自金融、政务、通信运营商、科技、医疗与健康、消费品与零售、制造业、能源与材料、工程与建筑等行业。我们的研究团队以访谈统计、问卷辅助的方式展开调研，以确保受访者能够更全面、更准确地表达观点。每位受访者最多可以选择3个选项。

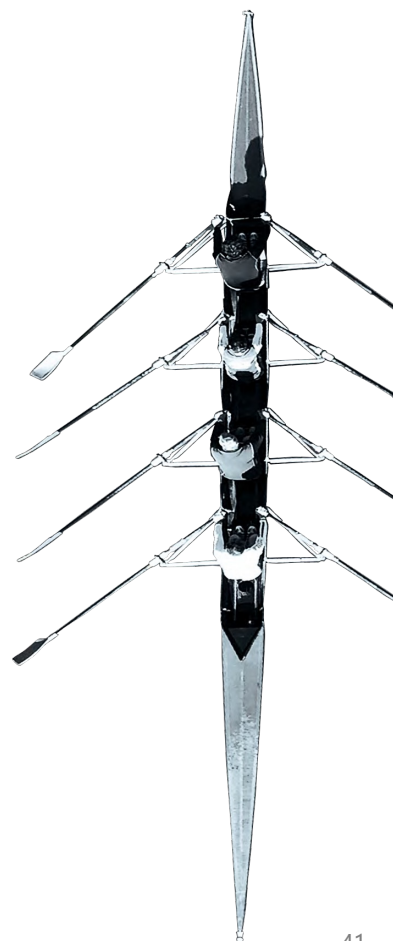
来源：艾瑞咨询。

E-Cycle - 现状洞察部分，包含下述三个周期用例：

用例1 | 可信数据空间建设热潮

用例2 | 自主式AI：重新定义数据价值、治理及安全

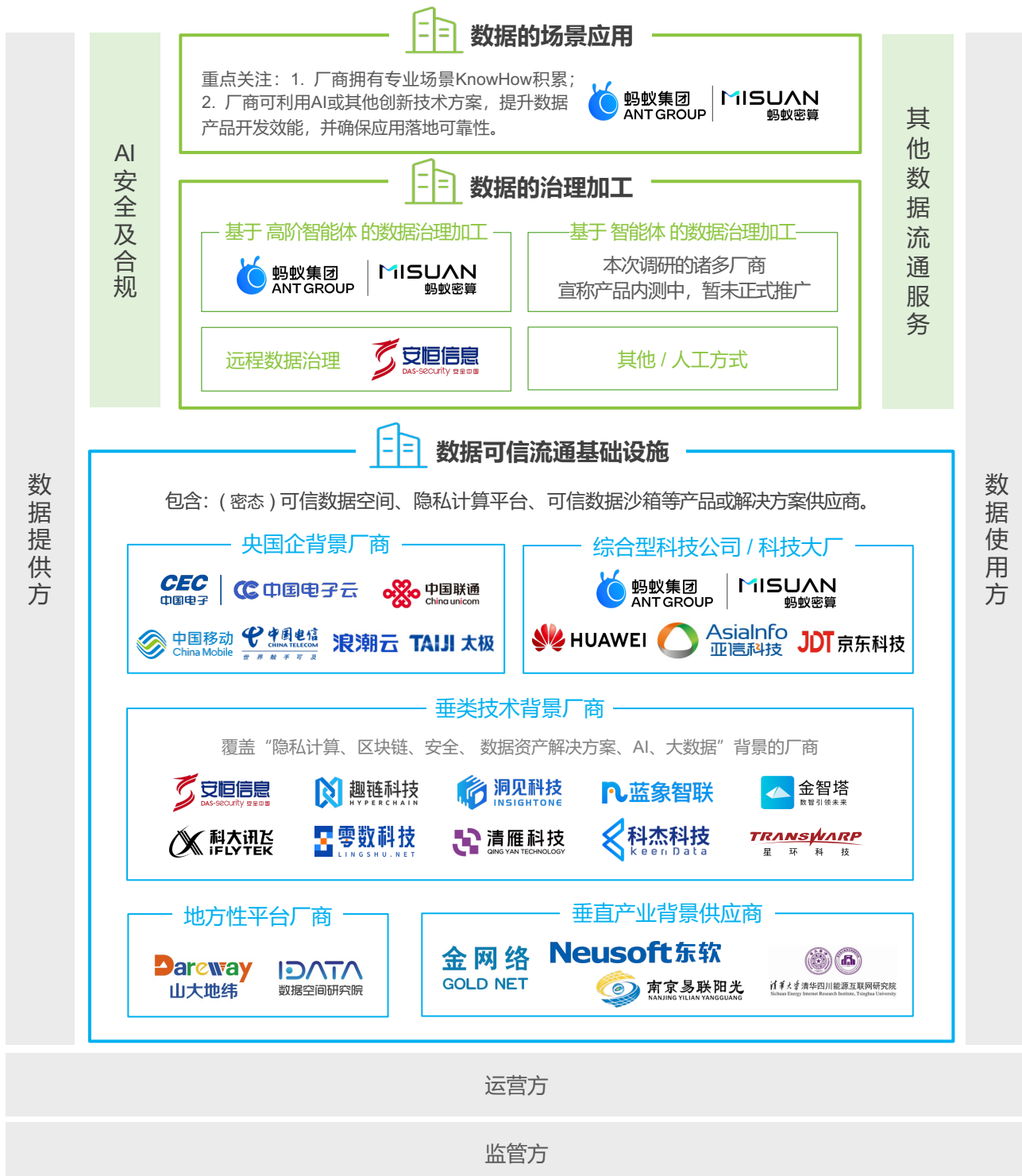
用例3 | Data+AI：阶段性的生态格局形成



产业图谱

本产业图谱并非基于公开信息的简单汇编，而是基于对厂商的基本评估后，确定的入围企业。入选图谱的供应商，需在对应能力领域满足任一条件：拥有成功中标的商业项目、与生态伙伴开展过创新实践。此外，图谱亦会收录甲方企业结合项目招标过程中和厂商的接触经验而推荐的代表性企业。

AI时代的数据可信流通产业图谱（2026）



说明：上述产业图谱不代表排名，企业logo位置和大小无任何实际意义。入选图谱的厂商是在有限范围内的甄选（通过厂商主动参与、市场调研、公开信息参考等方式），而不代表未入选的厂商便不具备相应能力。由艾瑞咨询研究绘制。

面对AI时代的数据使用需求，目前的数据治理加工出现了供给断层，成为场景用数的鸿沟，产业生态仍在不断完善中

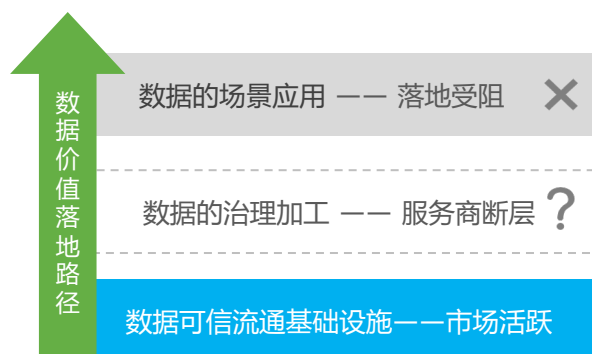
一、基础设施建设市场活跃

可信数据空间成为兵家必争之地。供应商包括央国企背景厂商、综合型科技公司/科技大厂、垂类技术背景厂商、地方性平台厂商、垂直产业背景供应商。厂商之间呈现竞争合关系：因目标客户一致而产生竞争，但也有集成合作。地方性平台厂商、垂直产业背景厂商相对分散。除技术公司争夺标的外，也发现有极个别的行业可信数据空间项目由院校背景科研单位中标。

目前仍有很多企业会采购隐私计算平台、可信数据沙箱等产品来满足数据可信流通需求，这些同样是数据可信流通市场的一个重要的组成部分。提供这些产品的供应商主要是上述提及的可信数据空间供应商中的“综合型科技公司/科技大厂、垂类技术背景厂商”

二、数据治理加工是数据价值落地的动力引擎，传统依赖人工的治理加工模式无法满足AI时代的数据使用需求，出现了市场供给断层的表现，成为场景用数的鸿沟

传统依赖人工的数据治理成本高、效率低，难以满足当下的数据治理需求，目前可以提供AI数据治理的厂商数量有限，这是场景用数的核心阻碍。本次调研中，很多厂商宣称自己拥有数据治理智能体产品并计划在年内发布。



三、国家数据局等部门提出：培育数据流通服务机构

数据流通服务机构包含三类：数据交易所（中心）、数据流通服务平台企业、数据商。上文提及的数据治理加工属于数据商范畴。

部分传统的数据流通服务机构（如数据交易所等）或将被清退和整合（例如武汉长江大数据交易中心退场）。同时还会培育出一批能够提供数据治理、数据场景应用、数据运营等多元化能力的优质数据流通服务商。

此外，我们发现基础设施建设供应商中，一些企业的未来增长战略为经营“数据运营、数据治理、场景数据应用”等业务。因为平台建设市场空间的天花板较低，而各类数据流通服务具备可持续增长的特点。

- 一些厂商期望基于可信数据空间建设，能够和数据集团相关单位建立信任，进而承接公共数据运营业务。
- 一些厂商的优势在于产业KnowHow的积累，他们期望在数据治理、场景价值挖掘方面获取更多市场份额。

四、关于AI服务

面向AI时代，越来越多的数据业务环节会采纳AI智能体来提升效率，对此各类AI服务商也应属于生态的一部分。亦或是目前生态的既有玩家通过自身的AI能力或集成AI厂商的产品来实现能力交付。

产业规模 – 基础设施部分

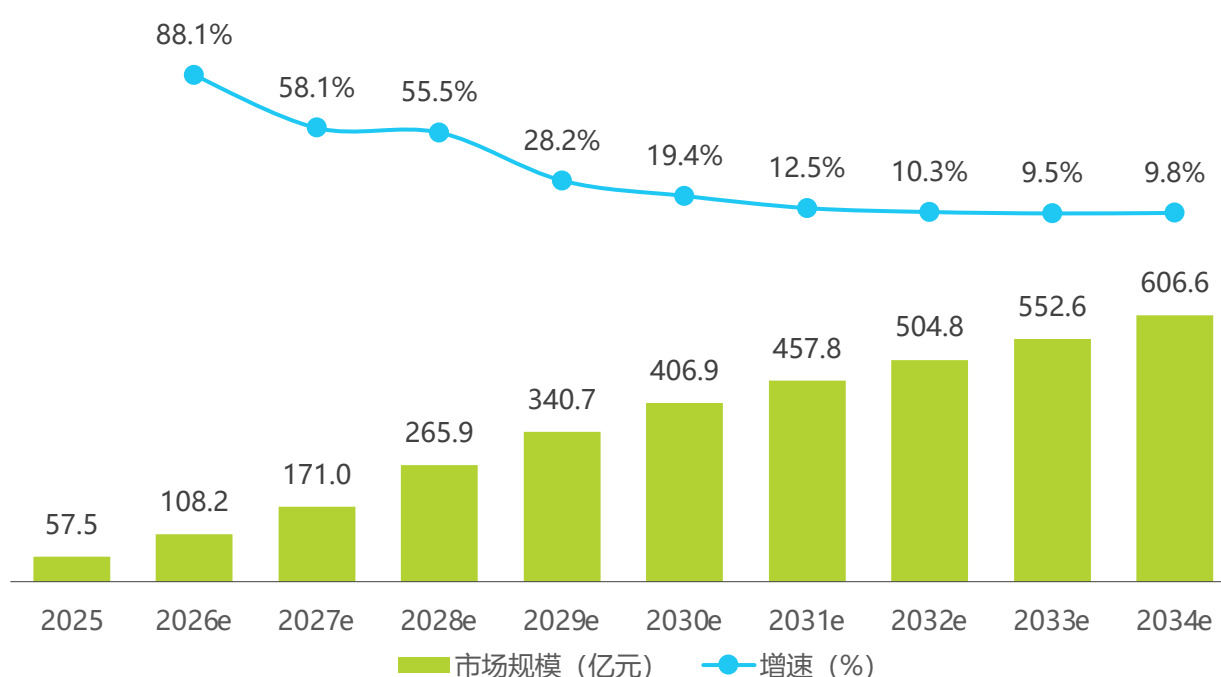
中国数据可信流通基础设施的市场呈现“前高后稳”的增长特征，2034年市场规模将达到606.6亿元

当前我国正处于数据可信流通基础设施的集中建设期，在《可信数据空间发展行动计划（2024—2028年）》的政策牵引下，全面推进以可信数据空间为核心的新型数据基础设施布局。本次市场规模核算采用全口径统计：除了增加密态底座、在接入连接器集成隐私计算能力的可信数据空间产品外，同时纳入了隐私/密态计算平台、可信数据沙箱等具备数据隐私保护能力的软硬件平台，覆盖数据可信流通的核心供给品类。

市场整体呈现“前高后稳”的增长特征：

- 2025—2028年为重点基建周期，行业整体保持在55%—90%的增速区间，可信数据空间增速区间为60%—110%，高于行业整体水平。
- 重点基建期之后的市场增长，主要集中在新增需求的平台建设、既有客户的节点扩展部署、功能更新迭代，以及日常运维保障等方面，市场增速逐步放缓至平稳增长区间。

2025 - 2034年中国数据可信流通基础设施市场规模及增速



注释：数据可信流通基础设施的市场规模包含：增加密态计算底座的可信数据空间项目、在接入连接器中集成隐私计算的可信数据空间项目、隐私/密态计算平台或可信数据沙箱等可以提供数据隐私保护能力的产品或平台项目；融合了数据可信流通能力的数据基础设施建设类项目、以及其他融合了数据可信流通能力的多元化类型项目。项目统计包含两大渠道，一方面是基于公开招投标项目信息的遍历，另一方面是厂商提报的项目信息。

来源：艾瑞咨询。

产业规模 – 整体

中国数据可信流通产业有望撬动万亿市场规模，早期实践探索对未来市场发展会产生关键影响

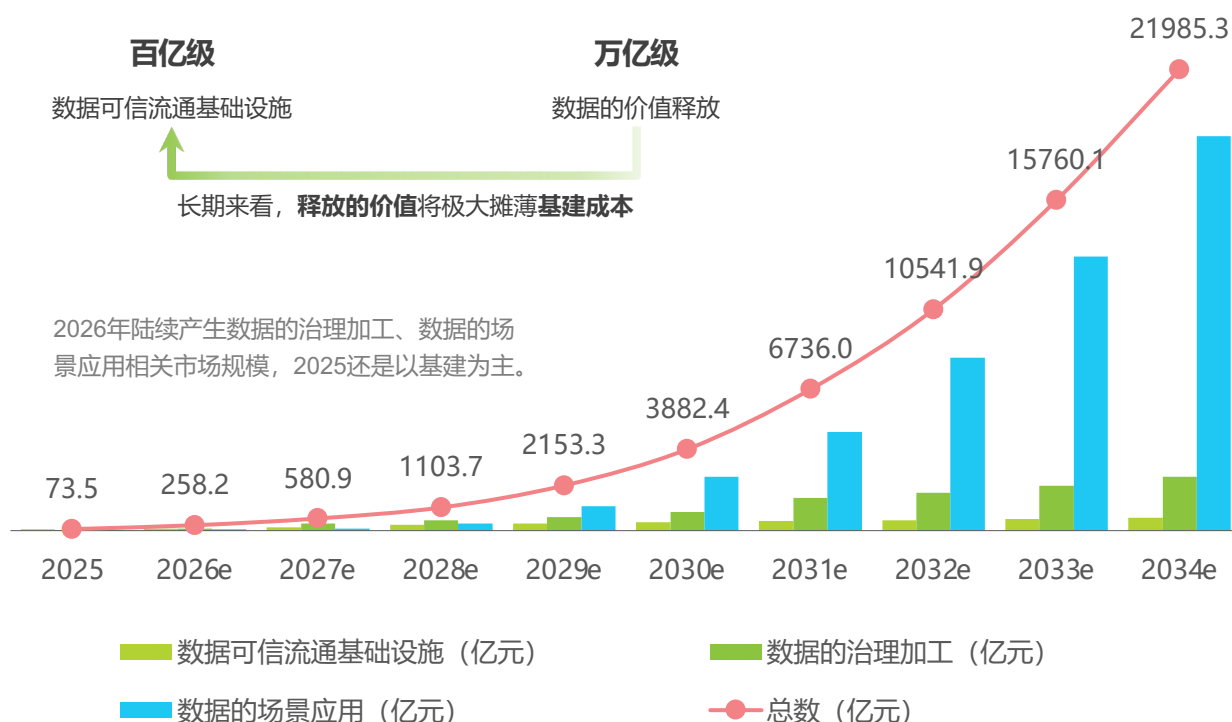
产业规模主要由三大板块构成：一是报告上文界定的数据可信流通基础设施；二是数据的治理加工，作为数据价值挖掘的核心动力引擎，是实现数据价值释放必不可少的环节；三是数据价值落地的场景应用，也是整个产业最核心、最具规模前景的部分。

未来，数据的场景应用将是9~12倍于数据的治理加工市场规模，数据的治理加工将是8~10倍于数据可信流通基础设施市场规模，这个规模比例将在产业未来的持续发展中动态体现。

数据的场景应用是数据价值释放的直接体现，其规模依托基础设施完善与治理加工成熟而持续扩大。未来规模将达到万亿级，将极大摊薄百亿级的基础设施投入成本。

数据价值释放依赖数据治理与加工，该环节直接决定数据能否接入、是否可用、以及能否充分释放价值。且经过治理加工的数据是否能够发挥预期的落地价值也需要经过进一步的实践验证。这些都是市场投资信心的影响因素。下述市场规模是站在早期市场实践取得成功且未来持续保持高增长的战略假设而展开的推演。

2025 - 2034年中国数据可信流通产业规模



注释：数据可信流通基础设施的市场规模包含：增加密态计算底座的可信数据空间项目、在接入连接器中集成隐私计算的可信数据空间项目、隐私/密态计算平台或可信数据沙箱等可以提供数据隐私保护能力的产品或平台项目；融合了数据可信流通能力的数据基础设施建设类项目、以及其他融合了数据可信流通能力的多元化类型项目。项目统计包含两大渠道，一方面是基于公开招投标项目信息的遍历，另一方面是厂商提报的项目信息。数据的场景应用是指，治理加工后的数据，基于场景应用需求而打造的各类产品、解决方案或服务。

来源：艾瑞咨询。

打开面向AI时代的数据可信流通产业大门，还需要攻克很多问题：

如何实现高效且高质量的数据治理、数据要素如何才能形成规模化且可持续的价值流通范式、自主式AI将如何影响数据可信流通产业的发展……

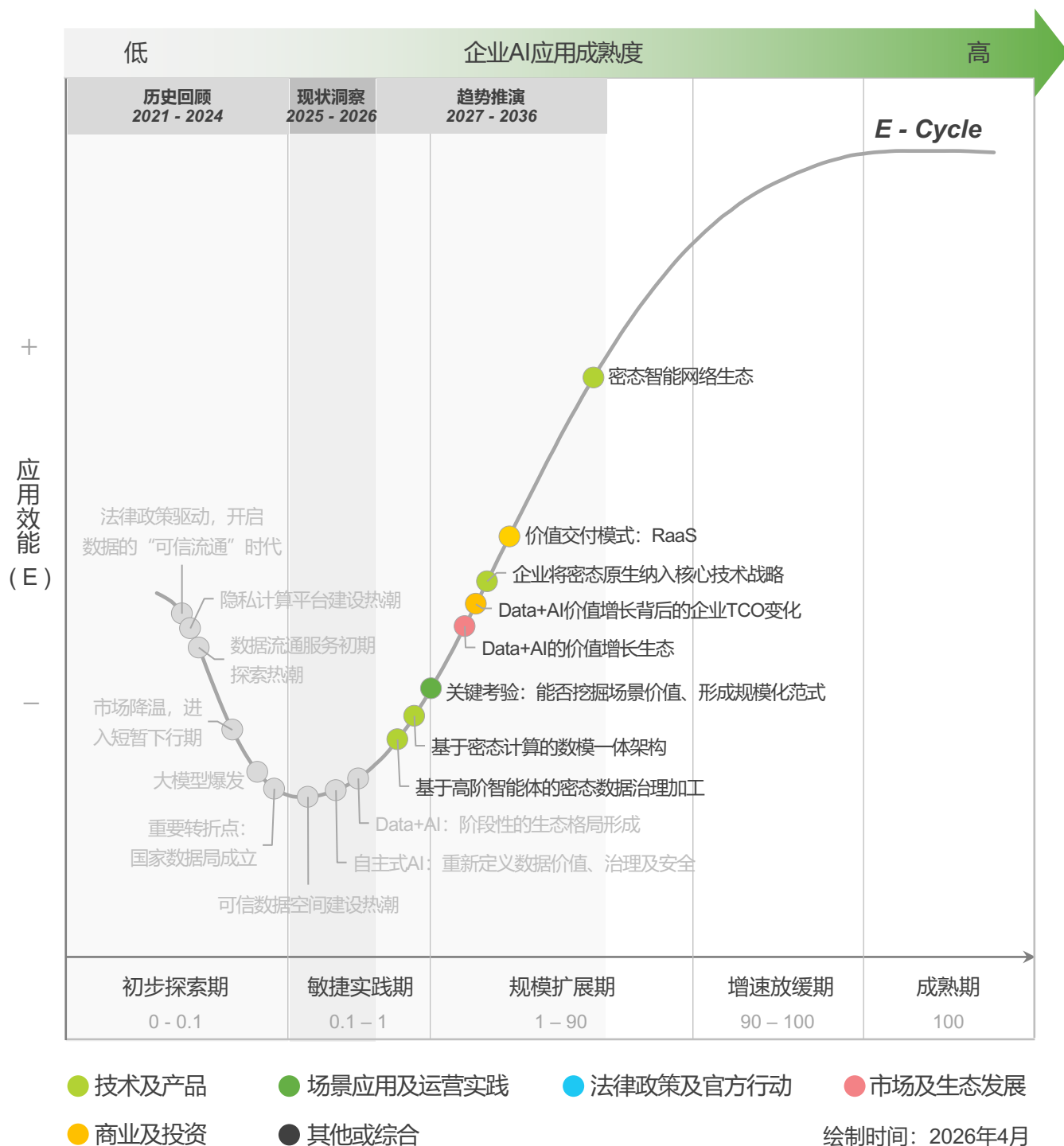
让我们带着关注的问题，探索未来趋势~

趋势推演

2027年 — 2036年

趋势推演

中国AI时代的数据可信流通产业周期洞察 – 趋势推演



注释1: 横纵坐标轴定义

- 横轴体现技术发展所处的阶段 (综合应用范围、用户覆盖度等指标综合评估)。
- 纵轴定义的应用效能表示技术带来的价值回报 (综合总体拥有成本<TCO>、投入产出比<ROI>等指标综合评估)。

注释2: 各发展阶段的周期规律和具体表现, 在对应章节部分详细解读。

来源: 艾瑞咨询。

趋势推演，覆盖了产业周期中的“敏捷实践期的部分阶段”和“规模扩展期的部分阶段”，敏捷实践期的阶段特点在前文已介绍，规模扩展期具备下述发展特点：

规模扩展期的规律及经验

- **1 该阶段的核心目标：**完成技术规模化落地范式的系统性验证，实现商业价值的规模化兑现。建立合理的产品技术架构、组织适配、安全合规及风险管理机制，保障技术落地的可持续性与稳定性。
- **2 该阶段的关键表现：**技术应用形成规模化扩展范式，市场热度回升，用户的接受度提升，企业的投资增长。产品服务形态从“定制化”向“标准产品、可配置能力、定制化满足个性需求的组合模式”演进。供应商也会推出面向不同规模或类型客户的分级产品矩阵。没有能力提供新一代产品及服务的供应商将失去竞争力，同时也会有新的市场玩家入局。
- **3 风险警示：**缺乏合理的产品技术架构、组织适配、安全合规及风险管理机制可能会让项目投资走向失败，如果此类项目比例过高，规模化扩展期会发展不畅甚至停滞。一些技术也会因为无法实现标准化产品（以及客户高度依赖定制开发）而让供应商交付成本高企，也会影响技术市场的正向发展。

核心摘要 @ 趋势推演 (2027 – 2036)

影响AI时代的数据可信流通产业周期的发展因素有很多，例如法律政策制度、基础设施建设、数据源生态开放、数据治理运营等一系列数据流通服务。然而，**一切技术发展均要归于价值的收敛**，我们认为AI时代的数据可信流通流通，最终要收敛闭环到对场景价值的挖掘，我们将以此为主线，展开趋势推演。

● 技术及产品



Forecast 01 | 基于高阶智能体的密态数据治理加工

高阶智能体能够在保障数据安全的前提下，提供可靠、可控、可敏捷迭代的数据治理加工服务，2027—2028年将逐渐被更多企业应用。且预计至2029年，65%以上的企业机构将采纳基于高阶智能体的密态数据治理加工产品或服务。

● 技术及产品



Forecast 02 | 基于密态计算的数模一体架构

到2029年，60%的大型企业将采用基于密态计算的数模一体架构，实现数据治理与模型治理的融合，提升AI的应用效率，同时降低数据泄露风险，基于密态计算的数模一体架构将成为企业构建AI竞争力的核心支柱。

● 场景应用及运营实践

**Forecast 03 | 关键考验：能否挖掘场景价值、形成规模化范式**

一切技术发展均要归于价值的收敛，能否挖掘数据的场景使用价值，并抽象出规模化的应用范式，是数据要素能否规模化流通的关键考验。未来1~3年，拥有产业KnowHow，能够为企业价值增长的服务商将更加具备竞争力。

● 市场及生态发展

**Forecast 04 | Data+AI的价值增长生态**

2030年，当部分传统的数据流通服务商被清退或整合、以及市场涌现一批新的优质数据流通服务商后，市场生态将会随之发生重塑。此阶段，AI也将广泛应用于数据治理、数据应用开发等服务环节，形成Data+AI的价值增长生态。

● 商业及投资

**Forecast 05 | Data+AI价值增长背后的企业TCO变化**

未来企业的总体拥有成本（TCO）将发生结构性改变：数据、安全成本攀升，IT及软件开发成本快速下降，业务人才结构向高级专家集中。这些变化将随着企业对数据和AI的不断应用而逐渐产生，至2030年底，65%的企业将完成TCO结构升级与组织适配。

● 技术及产品

**Forecast 06 | 企业将密态原生纳入核心技术战略**

随着数据可信流通的逐步规模化发展、AI安全风险的驱动，企业对安全投资的增长，“密态原生”将变得和“AI原生”同等重要，成为企业技术战略的核心组成部分。2030年，50%~60%的企业会将密态原生纳入三大核心技术战略之一，并进一步扩大投资。

● 商业及投资

**Forecast 07 | 价值交付模式：RaaS**

2031年，35%~40%的数据流通服务将采取RaaS交付模式。面对一些行业的客户，RaaS模式会更加受到青睐。RaaS和传统的产品及解决方案交付模式各具优势，长期来看将是融合共生的。

● 技术及产品

**Forecast 08 | 密态智能网络生态**

2036年，80%的大中型企业会通过密态智能网络生态获取数据智能服务，同时将普惠50%~60%的小型企业。数据流通服务平台类企业将担任重要生态节点，数据商将成为重要的价值贡献者，并因此而获取价值回报。

一切技术发展均要归于价值的收敛

AI时代的数据可信流通发展趋势



● 技术及产品

Forecast 01 | 基于高阶智能体的密态数据治理加工

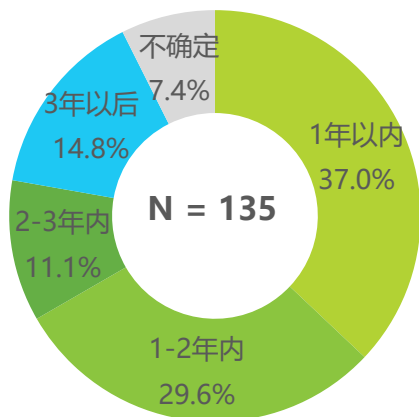


高阶智能体能够在保障数据安全的前提下，提供可靠、可控、可敏捷迭代的数据治理加工服务，2027—2028年将逐渐被更多企业应用。且预计至2029年，65%以上的企业机构将采纳基于高阶智能体的密态数据治理加工产品或服务。

该周期用例位于E-Cycle曲线的敏捷实践期。以场景价值挖掘为导向：数据治理加工是数据价值落地的动力引擎，其将决定数据能否有效接入，以及能否被有效使用。面向AI时代的数据使用需求，目前数据治理加工出现供给断层，因此我们认为这是现阶段最值得关注的趋势。

传统依赖人工的数据治理加工方式，效率低、成本高，难以适应AI时代对数据的需求。目前很多领先的企业为了解决传统数据治理加工效率低和成本高的问题，开始探索AI智能体的解决方案。一些供应商也在规划或准备推出相关的产品，以及部分供应商开始将数据治理加工Agent嵌入在既有产品中。

企业机构计划在数据治理加工业务中应用并投资智能体的时间（2026年Q1调研）



数据安全顾虑：虽然很多企业在数据治理加工业务中愿意尝试对智能体的投资，但一定需要确保数据安全问题，这是采纳智能体的底线。尤其是金融等合规要求高的企业。

AI智能体的专业性和可靠性顾虑：一些企业会认为目前的AI智能体处于通用化的能力阶段，不能够解决企业级数据治理问题，他们更青睐于行业出现成熟的解决方案后再投资。

1. 企业的数据安全顾虑——数据隐私保护成刚需

由于目前AI导致的数据泄露问题正在日益凸显，企业中需要治理的数据多是用户隐私、商业机密等高敏感数据，无法承担数据泄露带来的风险。对此，技术前瞻的企业逐步开始探索如何将数据隐私保护技术和数据治理Agent结合。

85.9%
重视数据安全问题

85.9%的企业表示：期待通过智能体工具提升数据治理效率，但希望这些智能体是安全受控的。并表示无法承担因为AI导致的数据泄露风险，如果风险不能被有效规避，可以继续使用传统数据治理方式。



来源：研究团队基于对135位来自金融、医疗、零售电商、制造业、能源等领域的数据智能或大数据相关部门的从业者展开访谈，获取了他们在数据治理工作中面临的问题以及对相关能力的价值期待，艾瑞咨询研究绘制。

2. 企业对AI智能体的专业性和可靠性顾虑 —— 高阶智能体成最佳推荐方案

数据治理要贴合业务，才能找准数据治理的关键点、避免无用治理，需对齐业务目标，梳理数据标准，落地数据质量与安全管控，支撑业务决策。这本质上是对业务KnowHow的掌握，企业需要专业智能体（而非通用化），需要智能体可控、可靠、可敏捷迭代。

68.9 %



68.9%的企业期望引入的数据治理智能体能够更加灵活地适应数据治理规则的变化，希望能降低因规则变化而导致的智能体Skill更新成本。

59.3%



59.3%的企业期待数据治理智能体工具可以基于业务逻辑来提供可靠的治理数据服务，而非只是通用化的Agent工具。

技术市场调研中，我们发现了一种创新技术方案：高阶程序（HOP，High-order Program），而构建于HOP之上的高阶智能体，是目前能够满足“企业对AI的可靠、可控、可适应业务敏捷迭代”需求的最佳方案。目前高阶智能体的能力已经在企业级场景中得到了验证，是一种可行的技术方案。

高阶智能体可以从工程化视角解决数据治理加工问题，可以将数据治理加工进行逻辑程序化显性表达，流程可编排、动作可追溯，工具调用与执行全程受控；通过将复杂任务原子化拆解、融合程序精准执行与多层核验机制，规避AI幻觉，提升数据治理加工任务产出的准确率，让结果稳定可验证。数据治理加工经验可沉淀为知识图谱与可复用模板，快速适配新规、新场景，迭代高效且成本低。

HOP的构成、执行核验框架及敏捷迭代

HOP敏捷迭代

在“完成率”这一指标的牵引下，能真正地区分专业场景下的大模型能力极限，并在“正确率”不能达到行业标准时激发迭代，针对不同原因导致的错误，HOP提供了“任务颗粒度、信息不足、知识不足、推理能力不足”等维度的迭代选择。

HOP执行核验框架

Step 01：任务分拆与派生

Step 02：混合任务执行

Step 03：执行结果核验

HOP的构成

程序化业务逻辑

将SOP用程序化语言表达

领域知识图谱

领域积累的概念关系的知识表达

工具链

负责具体的动作执行

来源：研究团队基于对135位来自金融、医疗、零售电商、制造业、能源等领域的数据智能或大数据相关部门的从业者展开访谈，获取了他们在数据治理工作中面临的问题以及对相关能力的价值期待，艾瑞咨询研究绘制。

● 技术及产品

**Forecast 02 | 基于密态计算的数模一体架构**

到2029年，60%的大型企业将采用基于密态计算的数模一体架构，实现数据治理与模型治理的融合，提升AI的应用效率，同时降低数据泄露风险，基于密态计算的数模一体架构将成为企业构建AI竞争力的核心支柱。

该周期用例位于E-Cycle曲线的敏捷实践期。该趋势是基于上一个趋势的延伸，高阶智能体完成数据治理的闭环，而数模一体则将治理范畴拓展至模型的层面，这是面向Data+AI时代的基础能力，是所有产业参与者值得关注的技术趋势。

数模一体是以密态计算为安全底座，将数据与模型视为一体两面的技术范式，核心是打破数据治理与模型应用的割裂状态，在统一安全框架下实现数据全生命周期治理与模型应用的全流程可控的深度融合。在AI规模化落地的关键期，基于密态计算的数模一体架构成为必然趋势有三重驱动力：

1. 数据安全与模型可靠的双重诉求：传统模式下数据泄露、模型幻觉等问题频发，亟需统一安全框架保障和模型可靠性提升。
2. 产业效率提升的现实需求：数据作为生产要素需通过模型赋能释放价值，而模型迭代又依赖高质量数据供给，二者协同方能最大化生产力。因此，数模一体架构的推广和普及，也在一定程度上将促进国家数据要素战略和“人工智能+”行动计划的落地。
3. 技术可行性：高阶智能体能力的演进，将为模型治理提供支撑。经过我们的调研，目前该技术的能力已经在企业级场景中得到验证。

基于密态计算的数模一体架构

来源：艾瑞咨询。

55

● 市场及生态发展

Forecast 04 | Data+AI的价值增长生态



2030年，当部分传统的数据流通服务商被清退或整合、以及市场涌现一批新的优质数据流通服务商后，市场生态将会随之发生重塑。此阶段，AI也将广泛应用于数据治理、数据应用开发等服务环节，形成Data+AI的价值增长生态。

该周期用例位于E-Cycle曲线的规模扩展期。在上一个趋势的基础上，如果产业在敏捷实践期探索出了场景价值的规模化范式，并成功迈入规模扩展期，那么服务商的企业经营表现将是市场发展的晴雨表。

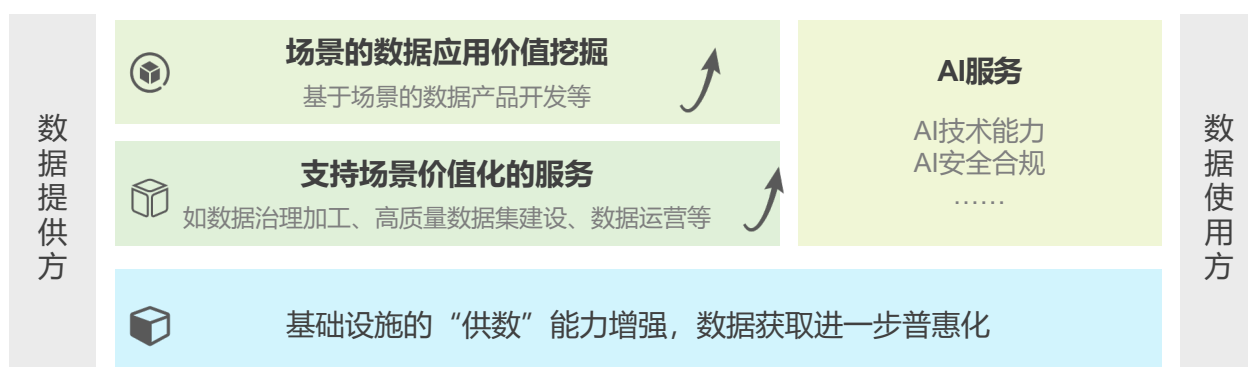
任何技术在每个周期阶段都会发生市场格局的变化甚至是重塑。在这个阶段：一些传统的数据流通服务机构（如数据交易所等），会进行清退和整合。此外，还会涌现能够提供数据治理、数据场景应用、数据运营等一系列多元化的数据流通服务商。

包含直接面向场景价值解决方案的服务商，以及支持场景价值化实现的服务商。这其中也会包含在基建期提供技术服务的供应商，因为这些供应商中，原本就有一些是具备产业KnowHow背景并将未来的企业增长战略聚焦在数据流通服务市场。

与此同时，随着高阶智能体的逐步应用和普及，AI将会更加可靠、可控地应用在数据治理、数据产品开发等环节，场景应用层的价值将被不断释放，也会有一些AI背景或者相关能力的厂商加入市场，他们会提供AI的技术支持，AI安全及合规服务等内容，同样成为生态的参与者之一。这些厂商也可能会和数据服务商绑定生态合作，共同为客户提供服务。

此阶段，基础设施的“供数”能力增强，跨主体、行业和数据获取会逐渐走向普惠。此阶段的客户在选择合作伙伴时，应该尽量选择能够给出明确价值衡量和评估标准的服务商以确保项目回报和预期偏差在可控范围。如果企业计划展开规模化的投资，需要重点关注AI时代的企业TCO结构变化。

Data+AI的价值增长生态结构



● 商业及投资

Forecast 05 | Data+AI价值增长背后的企业TCO变化



未来企业的总体拥有成本（TCO）将发生结构性改变：数据、安全成本攀升，IT及软件开发成本快速下降，业务人才结构向高级专家集中。这些变化将随着企业对数据和AI的不断应用而逐渐产生，至2030年底，65%的企业将完成TCO结构升级与组织适配。

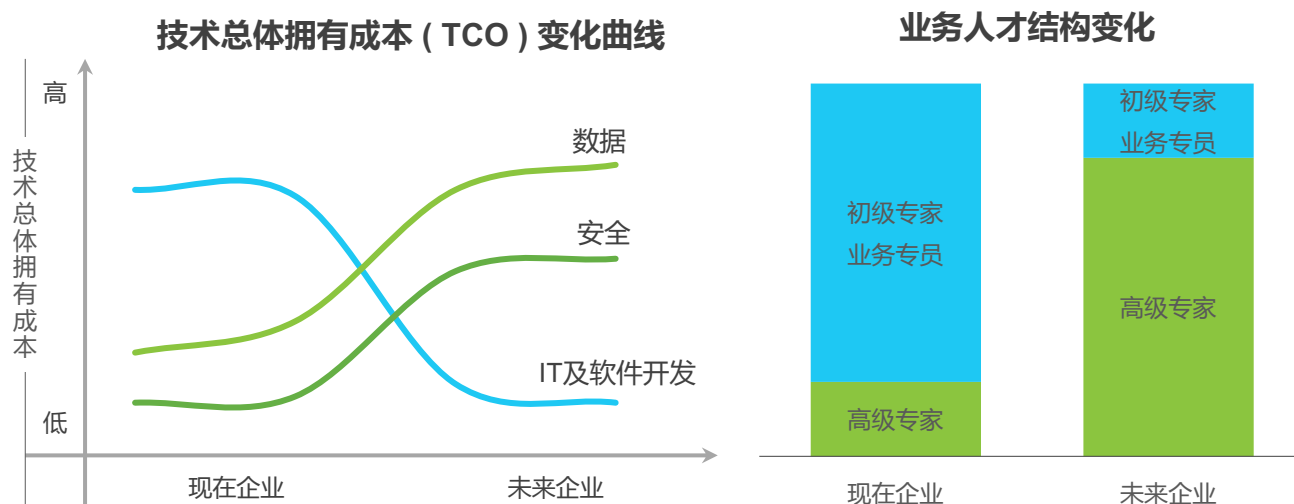
该周期用例位于E-Cycle曲线的规模扩展期。在上一个趋势的基础上，企业对Data和AI的不断采纳和落地应用的过程中，企业的TCO结构也将发生变化。

首先是三类技术成本的显著变化：

- 数据相关成本持续攀升：数据是AI的核心燃料，数据打通、治理、合规保护的需求日益提升；同时，数据的敏感性与智能体价值高度绑定，数据的稀缺性与重要性直接推高了数据获取、管理与保护的成本，数据成本将成为未来的核心成本项。
- 安全成未来企业的一项重要投资：企业未来会接入海量数据，既包括支撑业务运营的常规数据，也包含支持AI应用的就绪数据，而依托这些数据训练出的智能体，更是企业的核心资产。数据和智能体的安全保护将推动企业安全成本的提升。
- IT及软件开发成本快速下降：企业开展场景化数据应用开发时，AI可全面赋能开发流程，极大提升研发效率。以往专家提出业务需求后，软件开发与落地周期漫长，如今借助AI能够快速响应、高效实现需求落地，不仅大幅缩短开发周期，也持续降低企业IT与软件开发成本，成为行业发展的明确趋势。

另外是业务人才结构的变化：未来企业人力结构将向高级专家集中，初级人员占比持续下降。高级专家负责制定规则与提出需求，由高阶智能体直接执行，大幅削弱初阶人员价值，推动整体人才结构升级。

未来企业的TCO变化趋势



来源：艾瑞咨询。

● 技术及产品

**Forecast 06 | 企业将密态原生纳入核心技术战略**

随着数据可信流通的逐步规模化发展、AI安全风险的驱动，企业对安全投资的增长，“密态原生”将变得和“AI原生”同等重要，成为企业技术战略的核心组成部分。2030年，50%~60%的企业会将密态原生纳入三大核心技术战略之一，并进一步扩大投资。

该周期用例位于E-Cycle曲线的规模扩展期。在前两个趋势的基础上，密态原生的价值将在实践中不断被认可，进而逐渐演进为企业的核心技术战略。

密态/隐私计算等数据隐私保护技术的价值早已被行业认可，但对很多企业来说，这些技术并不像AI、云计算等技术占据着企业技术战略的核心位置。其将受到下述两类因素的驱动而逐渐演进为企业的核心技术战略：

- **数据可信流通驱动密态原生成为AI的标配：**当前企业在搭建AI应用时，多将密态化隐私保护能力视为附加功能，而非核心组成部分。随着数据可信流通产业持续成熟，跨组织、跨行业、跨区域的多源数据融合，将成为AI规模化应用的重要基础。在多方数据协同、数据价值外溢的趋势下，密态计算等数据隐私保护技术不再是附加选项，而是支撑数据安全流转和AI可靠落地的关键支撑。未来，密态能力将深度融入AI架构设计，成为企业构建AI应用时不可或缺的原生组成部分。
- **AI自身安全风险推动密态原生能力内生普及：**AI在快速发展中，也带来一系列安全风险。例如AI智能体的无边界上下文暴露导致敏感信息泄露，开放动态命令执行权限被滥用；Prompt注入攻击可劫持模型行为逻辑，这些架构级漏洞已突破传统安全防御边界。基于密态计算构建的原生安全范式，能让数据、模型、计算全链路实现全程密态化的安全防护。这种“主动防御”举措，将从可选方案升级为企业AI落地的必选配置，成为抵御智能体失控风险、保障业务连续性的核心安全能力。

85%+

2026年，85%以上的企业技术领导者表示，隐私保护计算是一项非常具备价值的技术，但还没有纳入到企业核心技术战略层面，而是会根据需求展开投资建设。并表示目前AI及相关技术才是核心技术战略方向。

50%~60%

2030年，50%~60%的企业会将密态原生纳入三大核心技术战略之一，并进一步扩大投资。

注释：N=100，受访者是来自金融、零售、互联网、医疗、制造业、能源等领域的企业。

来源：艾瑞咨询。

● 商业及投资



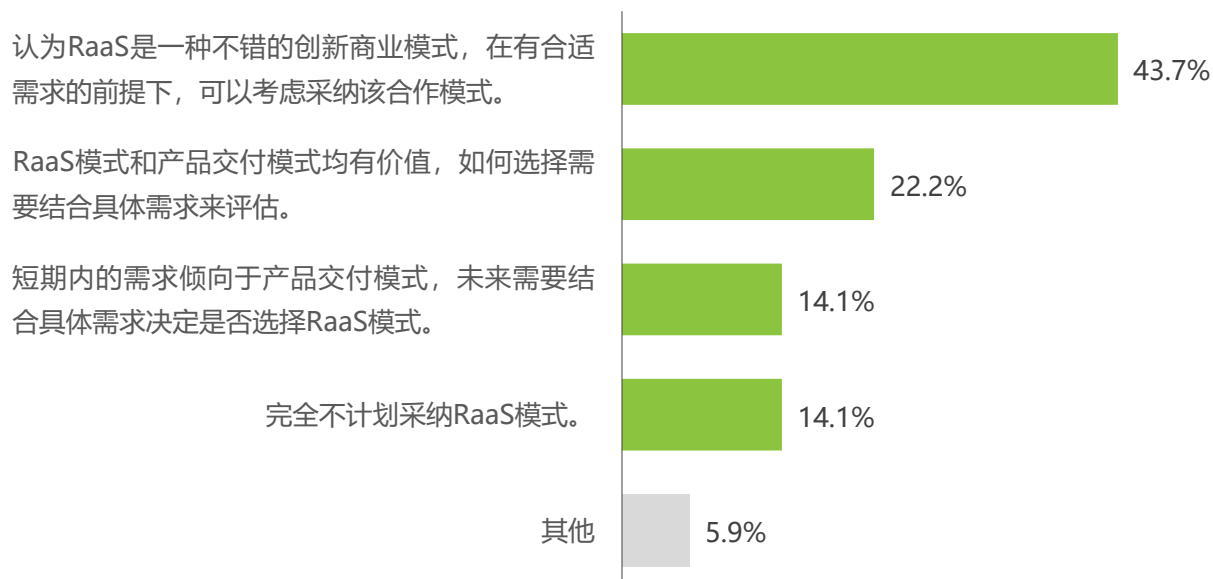
Forecast 07 | 价值交付模式：RaaS

2031年，35%~40%的数据流通服务将采取RaaS交付模式。面对一些行业的客户，RaaS模式会更加受到青睐。RaaS和传统的产品及解决方案交付模式各具优势，长期来看将是融合共生的。

该周期用例位于E-Cycle曲线的规模扩展期。在前面所述的趋势之上，如何满足差异化的客户需求，提供多元化的商业模式，同样是市场功能的关键。

- 未来，企业对数据密态可信流通服务的价值期望，将从“合规安全保障”转向“数据价值落地和业务增长”。然而，一些客户在采购相关服务时却对ROI与落地效果产生担忧，以结果交付为核心的模式（RaaS, Result as a Service）将成为一种值得选择的方案。
- RaaS模式曾被应用在一些新兴技术落地初期，或是需要深度业务认知（如金融）的行业中。此模式的可持续性，需要厂商能够为客户提供难以复制的价值增长解决方案。相比于产品销售模式，RaaS虽然理论上拥有更广阔的市场空间，但落地难度同时存在。
- 支持这类服务模式的厂商，需要在数据可信流通、数据治理和应用场景价值挖掘等方面拥有KnowHow，厂商需能够建设与客户共识的项目价值衡量标准及合理的收益分配机制。这种模式将改变密态可信数据流通市场的竞争范式，标志着一些厂商从产品供应商，转变为数据价值实现的共创伙伴，其收入直接与为客户创造的收益呈正向关联。
- 这一趋势的提出，源于一些前瞻企业反馈对未来的数据流通服务是否能提供可靠的业务价值表示顾虑。对此，我们探索性地询问了RaaS模式的接受程度，调研结果如下：

企业机构在数据流通服务方面对RaaS模式的接受态度



注释：研究团队基于对135位来自金融、医疗、零售电商、制造业、能源等领域的业务或技术领导者展开了访谈。

来源：艾瑞咨询。

● 技术及产品

Forecast 08 | 密态智能网络生态

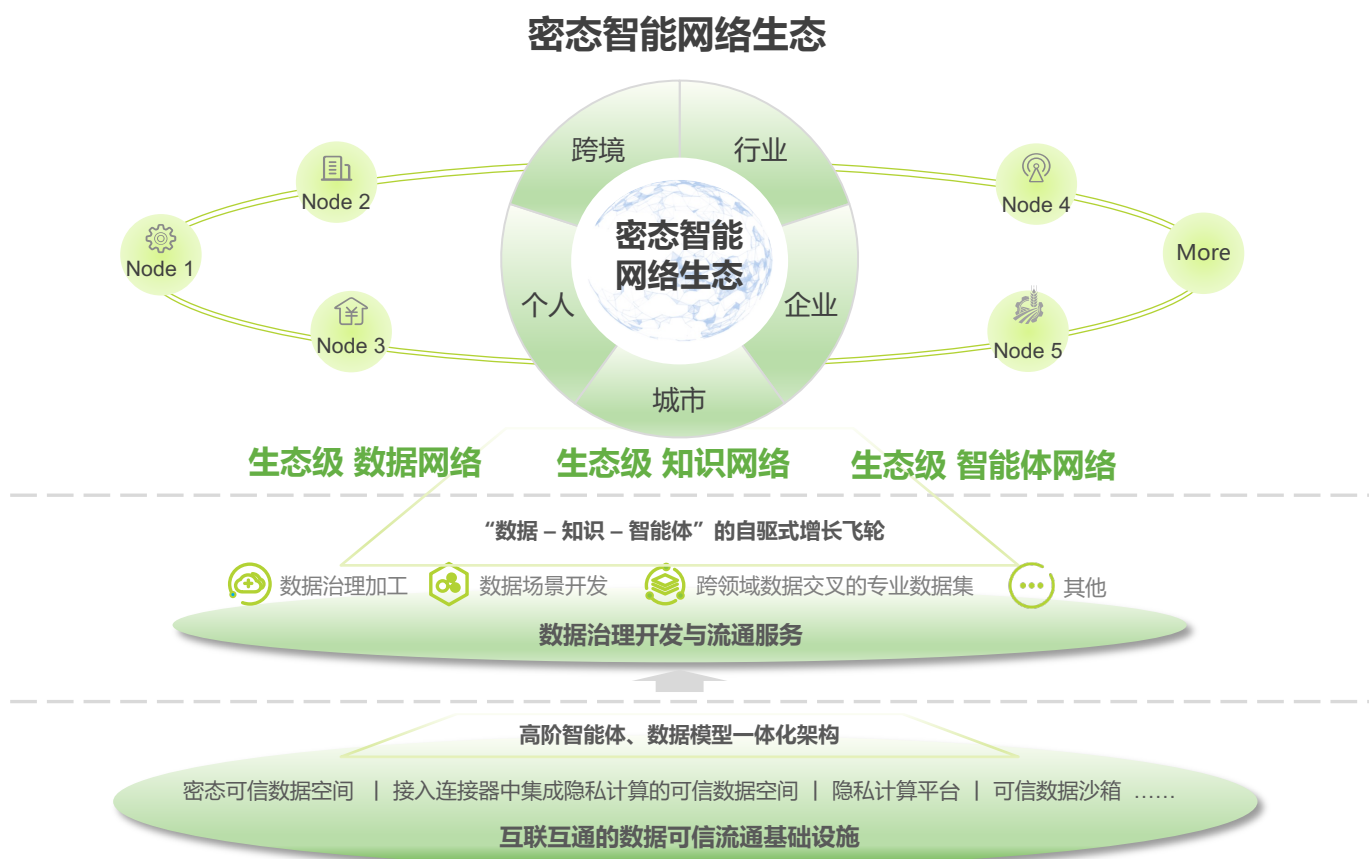


2036年，80%的大中型企业会通过密态智能网络生态获取数据智能服务，同时将普惠50%~60%的小型企业。数据流通服务平台类企业将担任重要生态节点，数据商将成为重要的价值贡献者，并因此而获取价值回报。

该周期用例位于E-Cycle曲线的规模扩展期。是站在“看十年”的视角所展开的趋势判断。

密态智能网络生态，是在城市、行业、企业、跨境、个人可信数据空间深度互联互通的基础上，以密态安全为底层保障搭建的生态级数据流通体系；2036年，企业AI应用成熟度已达到 L4（行业内赋能应用）至 L5（跨行业创新应用），企业开始将AI智能体对外输出并进行业务交互，以企业AI智能体跨主体协同交互为纽带，同步构建起了分布式智能体协同网络，两大网络融合联动、持续沉淀行业知识体系，成为实现数据要素生态化高效配置、产业间智能协同升级的核心产业基础设施。

该网络的建设遵循点、线、面、体的发展逻辑。在这个网络中，企业获取跨主体、跨区域、跨行业数据的效率将极大提升。目前很多企业尚不明确可使用的外部生态数据范畴，以及哪些数据能为自身业务创造价值，企业在该网络中可高效获取答案，推动数据智能服务普惠化。另外，“生态级知识网络”沉淀了大量可借鉴、可复用的行业KnowHow与解决方案，其价值远高于直接获取数据本身。



来源：艾瑞咨询。

目录

CONTENTS

01 AI时代背景

数据流通在AI时代所面临的机遇和挑战

02 E - Cycle：周期洞察

产业研究：AI时代下的数据可信流通发展

03 TechValue：穿越周期

企业评估：穿越产业周期的价值创造者

1. TechValue：穿越周期

TechValue：穿越周期——艾瑞咨询推出的企业研究项目，旨在发掘那些能够在技术热度高峰期引领行业前行，在市场期望低谷期发现并解决问题、最终穿越周期并持续创造价值的企业。他们是技术的信仰者、价值的贡献者、行业的推动者。

在技术的潮起潮落之间，多数企业竞逐风口，于行业繁荣期骤然膨胀，亦在周期切换之际迅速陨落。而“TechValue：穿越周期”这一企业研究项目，聚焦于那些既能立于技术浪潮之巅引领创新，亦能在技术热度下行而回归理性、在资本寒冬与产业重构之际保持增长、持续创造价值的企业。能够“穿越周期”的企业，绝非仰仗一时的运气或产品的短期爆发，而是源于对技术的信仰，以及深植于企业之中的韧性与战略定力。

2. 研究介绍 @ TechValue：穿越周期（AI时代的数据可信流通，2026）

数据要素可信流通和AI的高质量发展，已经上升至国家战略，在顶层设计的规划下，行业的发展需要依托战略的实践推进者，以及市场中具备相应能力的企业共同推动发展。

站在产业周期的视角：数据可信流通的发展正处于“敏捷实践期”迈向“规模扩展期”跨越的关键阶段。本次TechValue：穿越周期（AI时代的数据可信流通，2026）的评选会重点关注下述三类企业。

1



国家数据要素产业发展的**战略推进者**

推进数据要素市场化价值化流通，是产业能够迈入“规模扩展期”的关键，国家数据要素产业发展的战略推进者，是面向未来周期发展的关键力量。

2



技术创新和应用实践的**前瞻领航者**

面向AI时代和未来的数据可信流通产业，十分需要能够站在前瞻视角定义技术方向、以落地实践验证应用价值的领航者，为穿越周期的不确定性提供清晰的路标与可行的路径。

3



技术发展和应用实践的**核心竞争者**

产业的发展需要能够快速响应市场需求、具备成熟产品方案和可靠落地能力的实干型厂商推动发展，这些企业是数据可信流通产业发展不可或缺的中坚力量。

3. 企业研究的执行流程

- **Step1: 企业提名。**艾瑞咨询内部专家与外部产业专家对“TechValue：穿越周期（AI时代的数据可信流通，2026）”进行企业提名。这一阶段主要目的是明确值得关注的企业。
- **Step2: 厂商初筛。**研究团队将按照入围基准对提名企业进行初筛，对于符合条件的企业，我们会展开进一步研究。“TechValue：穿越周期（AI时代的数据可信流通，2026）”中的三类企业入围基准各有不同，报告下文的入围结果展示内容中，有详细的介绍。
- **Step3: 厂商研究。**我们会采取多元化的企业研究方法，来评估通过初筛的企业。这一轮的研究目的是为了选择出更具代表性的企业。例如：核心竞争者的入围企业，会限定“隐私计算、安全、区块链、AI”每一类背景的技术厂商只入围1家企业，因此我们会通过厂商高管访谈、问卷调研、厂商客户及生态伙伴访谈、互联网公开信息研究等方式，来进一步评估企业。
- **Step4: 交叉验证。**为了规避企业研究的主观性，我们会将入围结果和一线产业专家进行多方信息较验，以确保企业研究结果的客观性。在这个过程中，我们和产业专家的沟通内容只包括企业是否适合入围的信息判断，我们在厂商调研过程中获取的一切信息，均不会向其他任何组织及个人传递，以确保厂商信息的隐私安全。
- **Step5: 艾瑞研究院审核。**当我们形成最终的研究报告后，便进入了发布就绪的阶段。在报告发布之前，艾瑞研究院会再一次对研究内容展开系统性审核，以确保研究的合理性。

4. 企业入围情况

TechValue：穿越周期（AI时代的数据可信流通，2026）入围者



国家数据要素产业发展的 战略推进者

企业先后顺序不代表排名

国家
数据集团

北京
数据集团

上海
数据集团

福建省
大数据集团

江苏省
数据集团

其他

面向未来的增长周期，数据集团是关键的战略推进者。数据集团以“数据”为核心生产资料，承担公共数据授权运营、数字基础设施建设、政企数字化服务等关键职能，是推动数据要素市场化配置改革的重要载体（目前数据集团在陆续成立，上述列举了本次调研中，产业界关注度较高的代表性企业）。



技术创新和应用实践的 前瞻领航者



蚂蚁集团
ANT GROUP

MISUAN
蚂蚁密算

成功当选“前瞻领导者”的厂商，既是AI时代数据可信流通领域技术演进的风向标，也是市场中少数能将前瞻技术愿景与卓越市场洞察深度融合的引领者。入围者需满足以下基准条件：

引领性：在数据可信流通、数据的治理加工、数据的场景应用、AI数据安全等方向推出过创新的技术理念，且已落地验证。

持续性：公司或集团母公司将数据隐私保护及可信流通作为核心战略方向，且拥有不低于10年的持续投入。

影响力：具备全球影响力（可为以下一种或多种证明：全球领先的发明专利、主导国际标准、全球顶尖人才等）。

实践力：需要覆盖“数据可信流通基础设施、数据的治理加工或运营、数据的场景应用”全部方向的实践经验。



技术发展和应用实践的 核心竞争者

企业先后顺序不代表排名

科技背景 – 代表性央企

CEC | 中国电子云

中国联通
China Unicom

中国移动
China Mobile

中国电信
China Telecom

浪潮云

科技背景 - 市场化企业：覆盖“科技大厂、隐私计算、安全、区块链、AI”背景的厂商。

HUAWEI

趣链科技
HYPERCHAIN

安恒信息
DAS-security

洞见科技
INSIGHTONE

科大讯飞
IFLYTEK

AsialInfo
亚信科技

垂直产业背景的技术服务商：选取了“金融、医疗健康”领域的代表性服务商。

金网络
GOLD NET

Neusoft 东软

成功跻身“核心竞争者”的厂商，是当前AI时代数据可信流通产业的中坚力量。此类厂商凭借提供契合市场需求的产品解决方案或服务，确立了其在所处的赛道上，作为市场主要供应商的地位。入围者需满足以下基准条件：

影响力：在厂商所处的赛道上，受到客户、生态伙伴或产业专家的认可，进而构建了值得信赖的影响力。

实践力：需要拥有“数据可信流通基础设施、数据的治理加工或运营、数据的场景应用”方向的一项或多项实践经验。

5. TechValue Vendor

不同背景的供应商基于自身基因差异，在战略定位与能力资源储备上呈现出分化特征，各类市场玩家均是不可或缺的重要力量。

- TechValue Vendor是从“TechValue：穿越周期（AI时代的数据可信流通，2026）”中选择的代表性供应商，并基于下述核心维度，对入选企业的综合能力展开介绍。
- 本次研究，从“央国企、科技大厂、隐私计算、安全、区块链”五类背景的供应商企业中，分别选择1家公司，作为代表展开介绍。

TechValue Vendor 关键能力维度

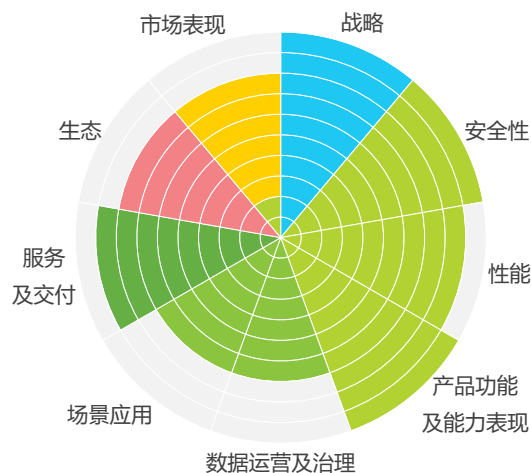
指标覆盖战略、产品技术、服务、生态及市场等多个维度。重要性 低    高

指标	说明	重要性
战略	评估厂商的战略取舍是否明确，资源规划分配是否合理，评估其战略是否符合市场趋势、是否有助于厂商在未来发展中建立优势。	
安全性	厂商的数据可信流通产品 ¹ 及解决方案的安全能力表现，厂商所采纳的技术路线、技术的领先性，以及和市场需求的匹配程度。	
性能	在保障安全需求的基础上，厂商的数据可信流通产品及解决方案的性能表现，以及和市场需求的匹配程度。	
产品功能及能力表现	厂商的数据可信流通产品功能的完备性、易用性、是否易于集成、互联互通支持等方面的综合表现。	
数据运营及治理	厂商在数据运营及治理方面的经验。数据运营的策略、数据治理加工的方式及采用的技术或工具。以及如何通过这两项能力支持场景应用。	
场景应用	面向场景的数据应用，厂商所能提供的产品及解决方案和市场需求的匹配度。此外，需要重点评估厂商的业务KnowHow和场景理解能力。	
服务及交付	围绕售前、交付、售后等客户服务的全生命周期，厂商将产品及解决方案交付给客户并确保可靠落地、可持续运营的能力。	
生态	厂商生态伙伴类型（如技术、定开服务、数据运营及治理、AI场景解决方案、专家及咨询、渠道等）覆盖度、生态伙伴数量及合作情况。	
市场表现	厂商的产品或者服务被采用的情况，以及客户的综合评价。	
注： ¹ 数据可信流通产品包括但不限于集成隐私计算的可信数据空间、密态计算平台、可信数据沙箱等。		

安恒信息

作为数字安全和数据要素领域的代表性企业，安恒信息数据可信流通领域已有多年的行业探索经验，目前该厂商已经将数据要素定位为公司级的战略，在数据可信流通市场需求方面，可以提供隐私计算平台、可信数据空间等多类产品及服务。

在目前的可信数据空间市场热潮中，该厂商参与了很多城市和行业类可信数据空间项目的建设，其中也包括具有代表性的国家类创新试点项目。



核心能力介绍

在隐私计算方面，安恒信息支持MPC、FL、TEE三条技术路线，在保证安全性的前提下，可以支持上百个节点的联合计算。该厂商的隐私计算平台在多年的客户服务中沉淀了面向真实业务场景的企业级功能。

该厂商的可信数据空间主要分为业务平台和安全交付能力。安恒数由空间产品在安全交付上，复用了其自身的多项安全产品的核心能力，包括TEE、MPC、FL、数据安全网关、数据分类分级、数据沙箱等。

该厂商的产品支持软硬一体机形态、裸金属部署的多种方式，支持开箱即用。产品支持与企业现有IT系统的高效集成。在复杂的跨机构系统集成与异构底层平台互联互通对接方面，表现出较高的兼容性与工程化落地能力。

该厂商还将AI应用于自身产品中以增强易用性，包括数由器接入连接器中的数据智能推荐能力，数据智能自动登记能力，数据库自动探查能力；在隐私计算中，有代码智能性能优化能力，代码智能编排与生成能力等能力。

值得被关注的是，该厂商在宁波城市可信数据空间建设中推出了“连接器远程加工”功能，可帮助客户实现远程数据治理，通过在数据源部署安全可信连接器，确保数据治理过程始终在数据持有方信任的环境下进行。

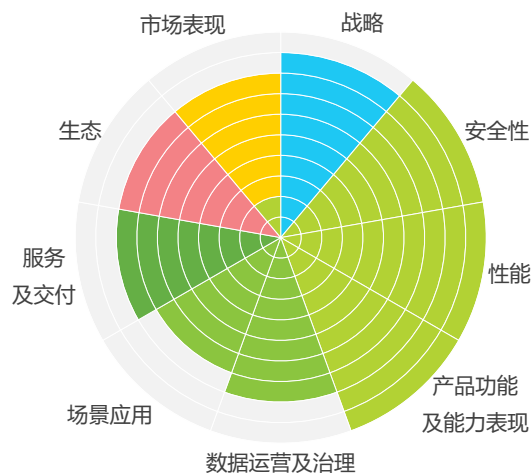
除了数据可信流通的产品矩阵，该厂商通过成立全资子公司“数瀚”专攻于数据要素场景开发和运营。

该厂商能够成为TechValue Vendor的主要原因，一方面是其在数据可信流通领域拥有多年的实践经验，产品成熟度和行业KnowHow值得信任；另一方面是，该厂商正在积极布局数据运营业务，并在远程数据治理方面已有领先的落地实践，加之目前该厂商已帮助很多城市建设了可信数据空间，这些基础设施建设也为其后续发展数据运营、治理和场景价值挖掘提供了一定的基础优势。

洞见科技

洞见科技致力于以隐私计算与可信AI技术构建密态智能基座，提供从数据基础设施到可信数据链接，并服务于业务场景应用的AI数据可信流通的全栈技术支持。

选择洞见科技的客户，更多看重的是其在隐私计算等产品的成熟度，他们的隐私计算产品基于在客户侧的应用而逐渐打磨成熟。此外，他们还会通过和集成商的合作，将可信数据空间、隐私计算、数据沙箱等产品能力对外输出。



核心能力介绍

该厂商的战略取舍清晰坚定，无论是在曾经的隐私计算市场热潮期，还是在当前的可信数据空间建设发展期，他们始终坚持并践行“布点、连线、结网”的战略方向。

该厂商自主研发了洞见隐私计算平台、洞见可信数据空间、洞见可信数据沙箱、洞见密态计算一体机、洞见安全可信大模型等核心产品。

洞见隐私计算平台（InsightOne）是该厂商于2020年推出的基于多方安全计算、可信联邦学习、可信执行环境等技术的数据智能应用平台，支持一体化数据接入、探索分析、联合运算、多方建模、辅助决策等能力，主要用于解决跨企业协作无法安全利用各方数据的困境。该产品经过6年以上的推广、部署和应用，已经完成了多个版本迭代，通过服务政企、金融等行业客户不断丰富产品功能并提升产品的综合能力。

面向当前市场需求，该厂商推出了洞见可信数据空间（InsightSpace）产品。该产品基于其多年积累的隐私计算、数据沙箱、区块链、密态存储、硬件加速等技术，并以相关国家标准为基础，构建了统一的规

则机制和可信高效的平台系统，促进数据提供方、使用方、服务方、运营方、监管方等生态主体汇聚与异构互联互通，推动数据资源的规模化流通利用。该产品已在国家数据局及各地方政府公布的可信数据空间试点项目中落地应用。

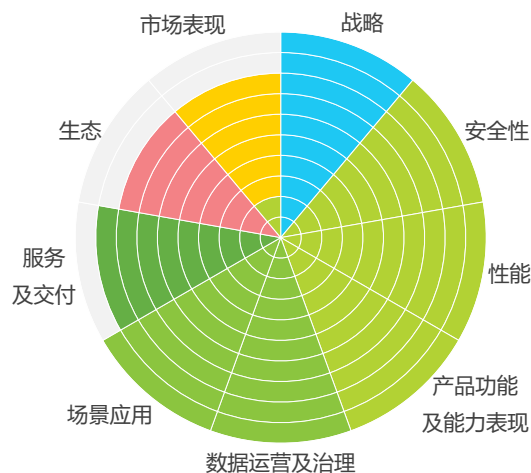
洞见科技期望构建“基础设施+生态建设+场景服务”的数据流通闭环服务体系。因此该厂商也在推进数据源生态的建设来提供数据运营服务，目前他们的数据源生态覆盖通信、金融、互联网、生活、征信等领域，主要服务内容为数据撮合交易、基于业务KnowHow的积累帮助客户选取合适的数据快速展开模型训练。

该厂商目前还围绕数据治理全流程，在他们的产品矩阵中，融入了数据治理AI Agent功能。

该厂商能够成为TechValue Vendor的主要原因，是其在数据可信流通市场的长期客户服务经验，并能够积极拥抱AI发展，探索数据治理和运营的新模式。以及该厂商过往服务客户所积累的金融KnowHow会让其在面向场景的服务中具备优势。

蚂蚁密算

蚂蚁集团升级科技战略，成立了蚂蚁密算公司，助力数据要素安全可信流通体系的持续建设。该厂商在2016年便开始探索TEE、MPC、FL在内的多条隐私计算技术路线。蚂蚁密算是中国市场少有的能够在数据隐私保护、AI应用可靠性方面有着原创技术的创新型科技公司。此外，他们还在大模型密算服务等前沿创新场景、城市可信数据空间试点建设以及金融、医疗等诸多产业的商业化项目中有所实践。



核心能力介绍

目前，蚂蚁密算致力于打造“基建供数-融合炼数-场景用数”的产业闭环，在医疗健康、民生就业、新能源出行、消费金融等领域实现规模化落地，该厂商以密态计算构建安全基座，凭借1.21倍明文开销、全链路等保四级的核心优势，依托“四纵两横”技术体系，保障数据全程可控、智能体不被窃取滥用。

蚂蚁密算在技术上进行前沿探索，推出密态计算技术，在传统隐私保护计算技术基础之上，强化了对全链路复杂计算的密态保护能力。该厂商还首创了高阶程序 (HOP, High-order Program)，致力解决大模型在专业应用中的可靠性困境，创新性地融合自然语言与编程语言。这项创新技术目前已经在密算金融风控全链路、医疗重复收费等真实的企业级场景中得到验证。此外，构建于HOP之上的高阶智能体，可以有效满足企业级AI落地可靠、可控、可迭代的需求。在数据要素领域，可以广泛应用于数据治理加工，是目前行业最值得推荐的技术方案。

该厂商的密态可信数据空间产品在通用可信数据空间架构之上增加了密态底座，基

于硬件密态环境和密码协议，支持机密虚拟机、TEE OS、机密容器，以及密态胶囊、数据血缘、密态网关等密态组件。支持可信密钥服务、可信账号身份服务、可信应用系统管控、可信日志审计以及密态数据计算等实现数据全链路密态保障。此外，该厂商还有包括大数据密算平台、大模型密算平台、隐语云知识库等系列产品。

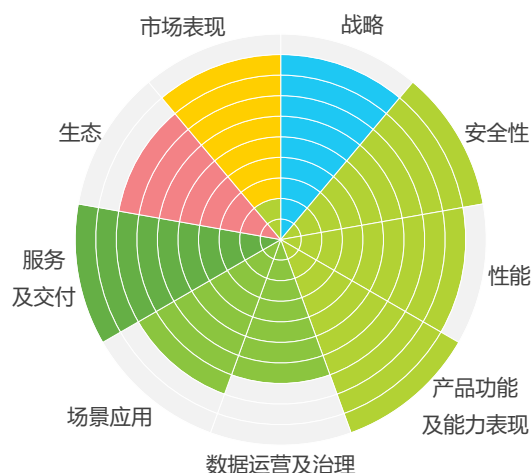
在技术落地实践和商业化方面，该厂商在城市可信数据空间（如湖南省公共数据流通利用基础设施建设-可信数据空间升级建设项目）、杭州市密态计算中心以及金融、健康等行业均拥有成功的商用实践。

该厂商能够成为TechValue Vendor的主要原因，一方面是他们的技术自主创新能力对行业发展推动有着重要价值，尤其是面对自主式AI迅速发展所带来的多种失控风险，他们提出的高阶智能体解决方案是目前行业独有的工程化技术创新。另一方面是，在市场的数治理加工服务断层的当下，该厂商具备基础设施、数据治理加工、场景用数的全栈能力，且依托于蚂蚁集团，他们对金融等业务场景的深度理解，是数据要素价值落地所需的重要能力。

趣链科技

趣链科技定位于可信数据基础设施与运营服务提供商。本次调研发现，趣链科技在城市可信数据空间等项目上展现了领先的市场力。该厂商聚焦区块链与隐私计算两个可信技术方向，在平台层构建了覆盖数据运营、数据互联互通与“AI+Data”的平台化能力体系。

该厂商在省级数据要素基础设施、医疗可信数据空间、公共数据授权运营服务等方面落地了相关实践案例。



核心能力介绍

趣链科技受益于浙江大学背景，在学术生态方面拥有较高的影响力，先后参与国内外的多项技术标准制定，并实现技术成果转化。

在数据的隐私保护方面，趣链科技为企业客户提供多方安全计算、数据沙箱、联邦学习和可执行环境四种主要方案，其自主研发的链原生数据可信协作平台BitXMesh，将区块链与安全多方计算、联邦学习等技术结合，可以实现隐私保护下的数据价值传递。

该厂商推出了面向政企场景的Safort安全沙箱平台，支持灵活适配政务、金融、医疗、工业等多种数据合作模式，支持数据跨域共享、权限可控访问、全程合规监管。

在数据互联互通方面，该厂商的接入连接器HyperConnector通过支持身份认证、网络接入、数据可信交付等功能，实现供需双方的数据共享。支持选择增加隐私计算集成、数据目录管理、合约管理功能，加强数据安全和提升数据管理效率。

该厂商的可信数据空间支持通过数据沙箱、

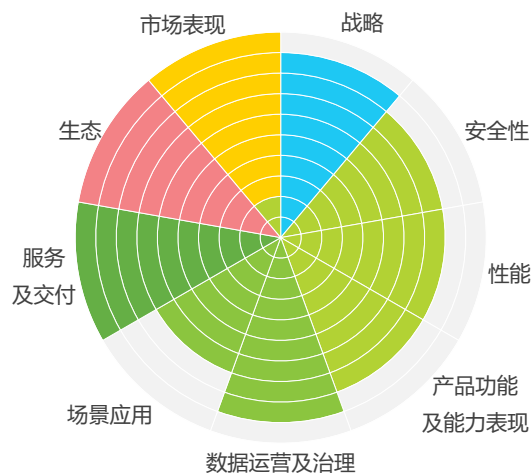
隐私计算实现数据可信流通，支持构建逻辑专区与物理专区多类数据子空间，并可在可信空间管理平台实现综合空间管理业务。该厂商还面向政府及公共机构推出了公共数据授权运营服务平台，该平台构建了基于区块链的运营服务与监管架构，以全栈安全矩阵为设计基础，对接入数据进行统一授权与治理开发。

此外，趣链科技还通过AI高质量数据集公共服务和AI高质量数据集测试验证等平台构建了Data+AI的产品体系，支持企业机构客户的高质量数据集流通与AI应用落地的场景需求。

除了丰富的产品矩阵，该厂商能够成为TechValue Vendor的另一方面原因是其在政企领域拥有较多的客户成功案例。在我们进行市场调研中，趣链的客户或生态伙伴，同样认为其在政务领域拥有值得客户信赖的服务经验。目前该厂商已建成超过20个城市及行业可信数据空间或数据要素基础设施类项目。

中国电子云

数据要素流通领域，中国电子云是典型的央企供应商代表，该厂商凭借过往在政务领域的客户服务经验和信任基础，在城市可信数据空间建设方面取得了良好的商业化成绩。该厂商推出的AI可信数据空间支持从连接器、可信计算到运营管理的全栈能力。让数据提供方、使用方和服务方之间建立信任并保障安全，让数据的流通和应用可靠、可追溯。该厂商还构建了丰富的技术生态，确保项目落地交付的可靠性。



核心能力介绍

中国电子云推出的AI可信数据空间，可集成多元技术开发组件，支持数据加密核验、数据沙箱、隐私计算等数据隐私保护方式。

厂商宣称可以实现从数据到模型到应用的全链路闭环，支持轻量接入至高密态计算的多形态连接器快速组网能力。虽然目前业内的连接器跨域互操作性和节点间调度效率尚未经过大规模跨组织部署验证，但在数据要素流通发展趋势下，连接器高效组网能力的确不可或缺。

在数据可信流通业务布局上，该厂商不仅提供产品技术能力的输出，还通过数据运营和数据服务结合的业务模式，探索数据流通服务。凭借多年政务数据治理经验和政务客户服务经验，该厂商推出中电云“数据港”运营模式，以供给港、数港网络、需求港为核心组成，实现数据可信流通闭环。是业内较为典型的政务数据运营案例。

数据赋能AI方面，提供全模态数据智能治理能力，让数据敏捷服务于智能，支持数据交易标的以高质量数据集、行业大模型、

智能体等形态在AI场景中应用。

多年的大型央企项目交付经验的沉淀让该厂商在生态建设与对外服务方面展现出优势，可提供覆盖规划、设计、运营、评估的全链条服务。该厂商宣称在深圳、广州（南沙）、郑州、大连、北京、长春、济南等超10个核心城市，以及电力行业、省级医保、金融科技等行业完成可信数据空间项目落地，深度参与了国家数据流通利用基础设施与可信数据空间试点建设。

此外，中国电子云同时联合产学研用单位，参与制定国家技术架构标准，支撑国家级行业试点申报，联合头部企业发布行业级方案。

该厂商能够成为TechValue Vendor的主要原因，一方面是其在政务及信创领域具备优势，并以此为基础，在当下的可信数据空间建设热潮中，取得了不错的市场成绩，并通过生态资源为项目落地提供保障。另一方面，该厂商在政务领域的数据运营和数据治理经验，同样值得被关注。

BUSINESS
COOPERATION
业务合作

联系我们



400 - 026 - 2099



ask@iresearch.com.cn



www.idigital.com.cn

www.iresearch.com.cn

官 网



微信公众号



新浪微博



企业微信



LEGAL STATEMENT 法律声明

版权声明

本报告为艾瑞咨询制作，其版权归属艾瑞咨询，没有经过艾瑞咨询的书面许可，任何组织和个人不得以任何形式复制、传播或输出中华人民共和国境外。任何未经授权使用本报告的相关商业行为都将违反《中华人民共和国著作权法》和其他法律法规以及有关国际公约的规定。

免责条款

本报告中行业数据及相关市场预测主要为公司研究员采用桌面研究、行业访谈、市场调查及其他研究方法，部分文字和数据采集于公开信息，并且结合艾瑞监测产品数据，通过艾瑞统计预测模型估算获得；企业数据主要为访谈获得，艾瑞咨询对该等信息的准确性、完整性或可靠性作尽最大努力的追求，但不作任何保证。在任何情况下，本报告中的信息或所表述的观点均不构成任何建议。

本报告中发布的调研数据采用样本调研方法，其数据结果受到样本的影响。由于调研方法及样本的限制，调查资料收集范围的限制，该数据仅代表调研时间和人群的基本状况，仅服务于当前的调研目的，为市场和客户提供基本参考。受研究方法和数据获取资源的限制，本报告只提供给用户作为市场参考资料，本公司对该报告的数据和观点不承担法律责任。



THANKS

艾瑞咨询为商业决策赋能