

2023年中国隐私计算行业研究报告

数据流通生态加速开展建设，场景布道仍需多方齐力推动

部门：TMT金融组 署名：李梦瑶

前言

自2016年伊始，我国隐私计算在政策、学术研究、技术与解决方案问世等多因素驱动下，随着资本热潮的席卷下，市场期望不断攀升。以金融为代表的重点行业率先开展隐私计算平台建设
与细分场景的试点应用，可谓是“百花齐放”。然而，当资本泡沫逐渐褪去时，市场对于技术
认知逐渐趋于深入，在短期内技术自身仍需不断迭代与优化，离规模化商业应用还有一段时间，
2023年陷入行业“冷静期”。

在此期间，我国利好隐私计算的政策不断出台，“公共授权运营平台建设”、“数据二十条”、
“《“数据要素×”三年行动计划（2024—2026年）》”等政策率先奠定了隐私计算为发展我国数
字经济的地基，也为隐私计算场景应用的广度和深度起到了助推作用。

**本报告将从以下四个维度解析当下隐私计算行业的重要发展状况，为未来发展重心和发展路径
提供启示：**1) 明晰隐私计算的所处环境，在政策与监管和市场需求导向下，对于当下隐私计算
行业宏观发展历程、现处位置、产业与各行业应用场景情况做出判断；2) 纵览2023年全年行
业发展实况，针对供给侧、需求应用与认知、监管推动下的新应用场景建设实况进行解析，更
好地明确当前所处方位；3) 提出隐私计算发展的现存挑战，并从供给侧、技术侧、需求侧企业
建设与全行业生态完善四大维度展望未来核心发展路径；4) 重点展示典型厂商的战略定位与产
品优势。

概念界定

隐私保护计算

(Privacy Preserving Computing)

隐私保护计算 (Privacy Preserving Computing)，又称“隐私计算”，是指在提供数据隐私保护的前提下，对数据进行分析计算的一类技术。进而在保障数据隐私安全的基础上，可以让数据以“可用不可见”的方式进行安全流通。隐私保护计算是一个技术体系，而非一项单一的技术。

市场中主要采用“隐私计算”的表述形式，因此本报告中均以“隐私计算”作为统一的表达方式。

实际上，还有资料将“隐私计算”和“隐私保护计算”进行了分别定义与解释，可见目前关于“隐私计算”存在多样化的概念界定方式。

对于此类问题，报告不再过多赘述。**本报告定义仅用于统一读者理解，方便后文的相关研究论述。**

概念界定

数据的可信流通

隐私计算可以构建“数据可用不可见，用途可控可计量”的数据可信流通范式

隐私计算通过在保证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，可以保障数据以“可用不可见”的方式进行安全流通。除了“数据可用不可见”的特性外，隐私计算中的多方安全计算技术还可以控制数据的用途以及用量，进而做到数据“用途可控可计量”。在应用实践中，隐私计算还可以融合区块链技术来强化在“数字身份、算法、计算、监管”等方面的信任机制，进一步完善数据要素的确权、定价与交易的可信体系建设。

基于隐私计算的数据可信流通



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。

CONTENTS

目 录

01 宏观发展环境概述

02 2023年中国隐私计算市场现状

03 中国隐私计算行业现存挑战和未来发展路径展望

04 中国隐私计算行业卓越厂商与优秀案例

05 行业专家之声

01 / 宏观发展环境概述

隐私计算在不断深化的政策布局与指引下加速发展

数据要素政策布局不断深入，隐私计算作为重要支撑工具在政策支持下在全国各地加强技术研发、实施与应用

2023年2月国务院发布《数字中国建设整体布局规划》，强调在数字基础设施、数据要素资源配置、数字经济、数据安全等维度在2025年取得重要进展；2023年12月，国家数据局发布《“数据要素×”三年行动计划（2024—2026年）（征求意见稿）》提出数据要素应用场景广度和深度大幅度拓展。而隐私计算作为其重要支撑技术，在行业政策指引下各省市2023年以来积极响应，加强隐私计算技术攻关、深化实施与部署应用，支持隐私计算技术加速发展。

数据要素布局不断细化深入

2023.12 国家数据局《“数据要素×”三年行动计划（2024—2026年）（征求意见稿）》

意见提出，到2026年底，数据要素应用场景广度和深度大幅拓展，在经济发展领域数据要素乘数效应得到显现，打造300个以上示范性强、显示度高、带动性广的典型应用场景

2023.02 中共中央、国务院印发了《数字中国建设整体布局规划》

到2025年，基本形成横向打通、纵向贯通、协调有力的一体化推进格局，数字中国建设取得重要进展。数字基础设施高效联通，数据资源规模和质量加快提升，数据要素价值有效释放，数字经济发展质量效益大幅增强

2022.12 中共中央、国务院《关于构建数据基础制度更好发挥数据要素作用的意见》

提出构建数据基础制度体系，促进数据合规高效流通使用

2022.04 中共中央、国务院《关于建设统一大市场的意见》

提出加快培育统一的技术和数据市场

《数据安全法》
《个人信息保护法》

国家
政策
与
指导
意见

法律
法规

数字中国建设核心方向



数字基础制度建设



数据要素资源配置



数字经济关键要求



数据安全合规保障

隐私计算为实现数字中国建设的重要支撑技术

2023.01 工信部、国家网信办等十六部门《要素市场化配置综合改革试点总体方案》

提出加强隐私计算技术攻关，加强隐私计算产品研发，推动多方安全计算、联邦学习等数据开发利用制程技术的部署应用



2023年4月以来，河南、江苏、山东青岛、甘肃、北京、广东在内的六大省市，率先针对省数字政府建设实施、促进数据要素市场发展等主题发布政策文件，多次提出完善隐私计算技术体系、加强技术攻关、开展技术部署与应用。在政策支持下，隐私计算得以进一步在各地区深化部署与实施。

行业
政策

各省
市
深化
实施

隐私计算发展历程回顾

隐私计算技术期望趋向“冷静期”，数据要素政策为市场注入新动能

隐私计算技术崛起已久，在2000后逐渐脱离基础概念，向落地应用全面迈进。中国在2016-2021年期间资本市场追捧之下，市场期望迅速爬升，供给侧驱动着在以金融为代表的重点行业开展平台建设与试点应用。随着需求侧客户对技术的认知逐渐深入，开始主动探索场景实践。随着技术期望趋于冷静时，部分泡沫化严重的企业出局，而我国利好隐私计算的政策不断出台，行业在冷静期下稳中向前。

iResearch：中国隐私计算发展历程

2016-2023期间重点法规政策一览

仅示意，非穷尽

2016: 工信部《大数据产业发展规划（2016-2020）》支持企业加强多方安全计算等数据流通关键技术攻关和测试验证

2019-2020: 《工业大数据发展指导意见》、《金融科技发展规划（2019-2021）》、《关于构建更加完善的要素市场化配置体制机制的意见》指出试验和推广隐私计算等技术

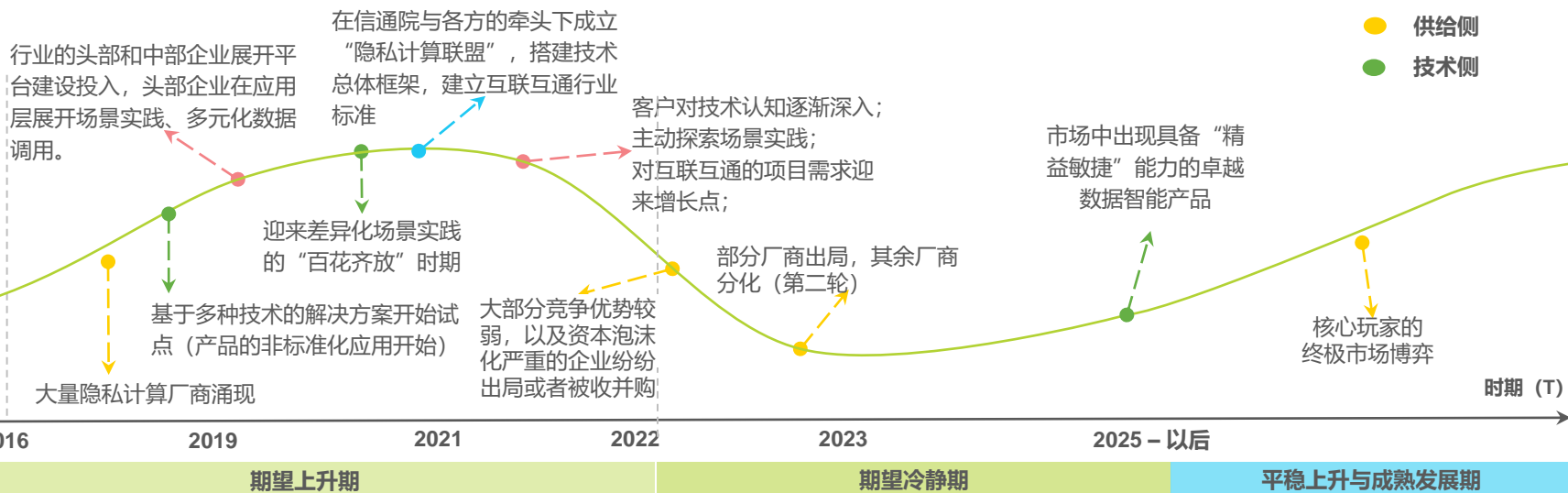
2021: 《数据安全法》
《个人信息保护法》

2022: 《全国一体化政务大数据体系建设指南》
《关于构建数据基础制度更好发挥数据要素作用的意见》

2023: 《“数据要素×”三年行动计划（2024—2026年）（征求意见稿）》

The Hype Cycle 纵轴：技术期望

- 自21世纪以来，在国内外学术界研究与碰撞之下，隐私计算逐渐脱离基础概念，差分隐私、全同态加密方案、联邦学习、算法框架应用等多个解决方案陆续问世，标志着技术创新向落地应用的迈进。



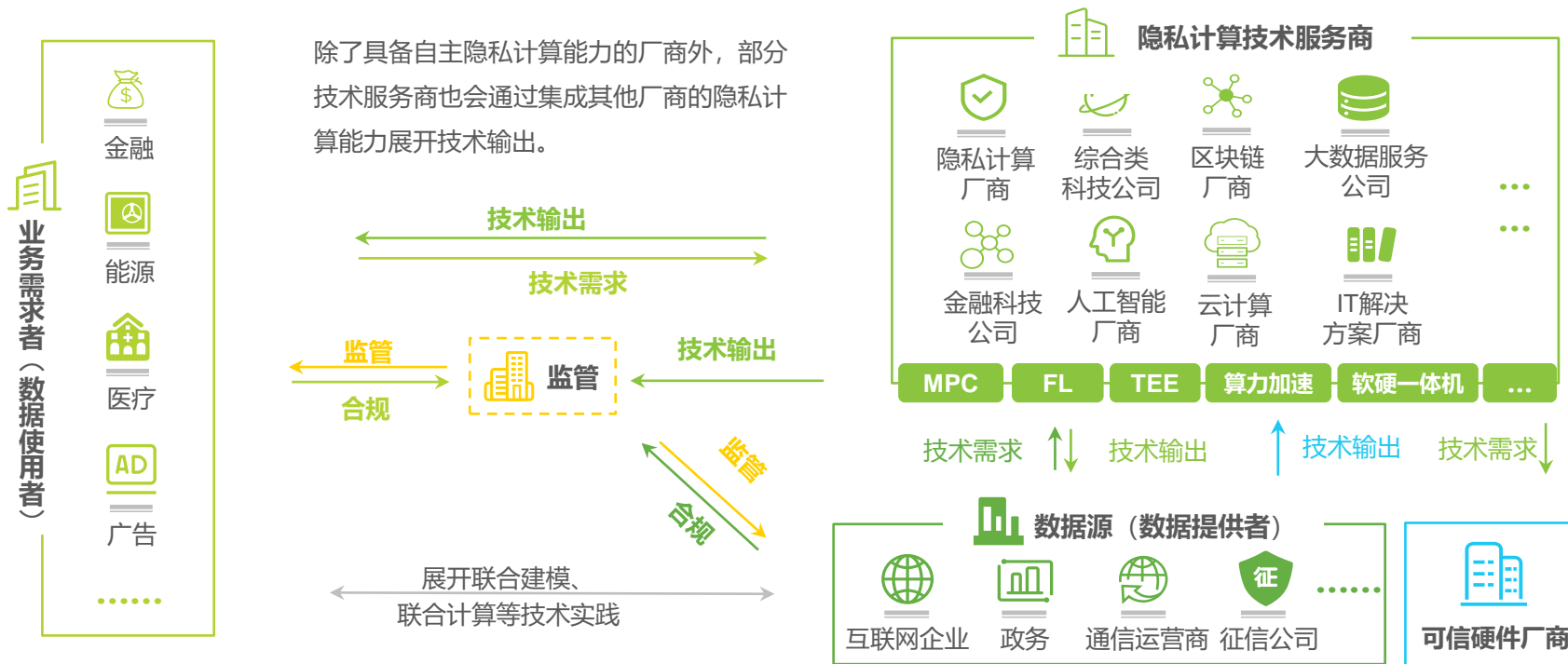
来源：综合公开资料整理，外部专家访谈，艾瑞自主研究绘制。

市场参与者类型

中国隐私计算行业呈现百舸争流、千帆竞发的市场格局

多方协同是隐私计算商用实践的一大特点，不同于其他类型技术，隐私计算在商用实践中，**技术服务商除了提供平台建设外，还会为客户提供数据调用（寻找数据源）服务，且隐私计算也经常需要两方以上的参与者展开联合计算，因此多方协同特性十分明显。**目前，中国隐私计算市场的参与者越来越多，除了垂直的隐私计算厂商外，各类技术企业纷纷入局，目前行业处于基础设施建设期，随着行业客户在应用层实践的逐步加深，数据运营、算力加速等需求也将不断涌现。

隐私计算市场参与者类型（2023，中国市场）



2023年中国隐私计算产业图谱



注释：1. 图谱中所展示的公司logo顺序及大小并无实际意义，不涉及排名。2. 各种类型的市场参与者“上下/左右”位置并无实际意义，不代表排位。如有任何疑问，[请联系团队分析师。](#)
来源：艾瑞咨询研究院自主研究及绘制。

隐私计算技术在各行业的应用环境与主要场景概览

随着隐私计算技术在2021年以来开展商用实践，现阶段，各行业由于不同的数字化基础和业务诉求，在数据流通中呈现了不同的角色。以政务、能源、医疗和工业为代表的行业，数字化基础中等，以隐私计算作为工具多为满足其保障内部数据安全、对外输出利用数据价值和共享与开放推动同业和异业经济发展的诉求，由于现阶段处于内部基础建设阶段，离数据共享和链接还需一段时间；而以金融、互联网、通信为代表的行业更聚焦于业务创新、对内对外赋能，率先探索数据流通和释放数据价值，所涉及的数据共享参与链接方较多，主要应用场景也呈现细分多样化。

隐私计算在各行业的应用环境与主要应用场景

仅示意，非穷尽



来源：外部专家访谈，公开资料整理等，艾瑞咨询研究院自主研究及绘制。

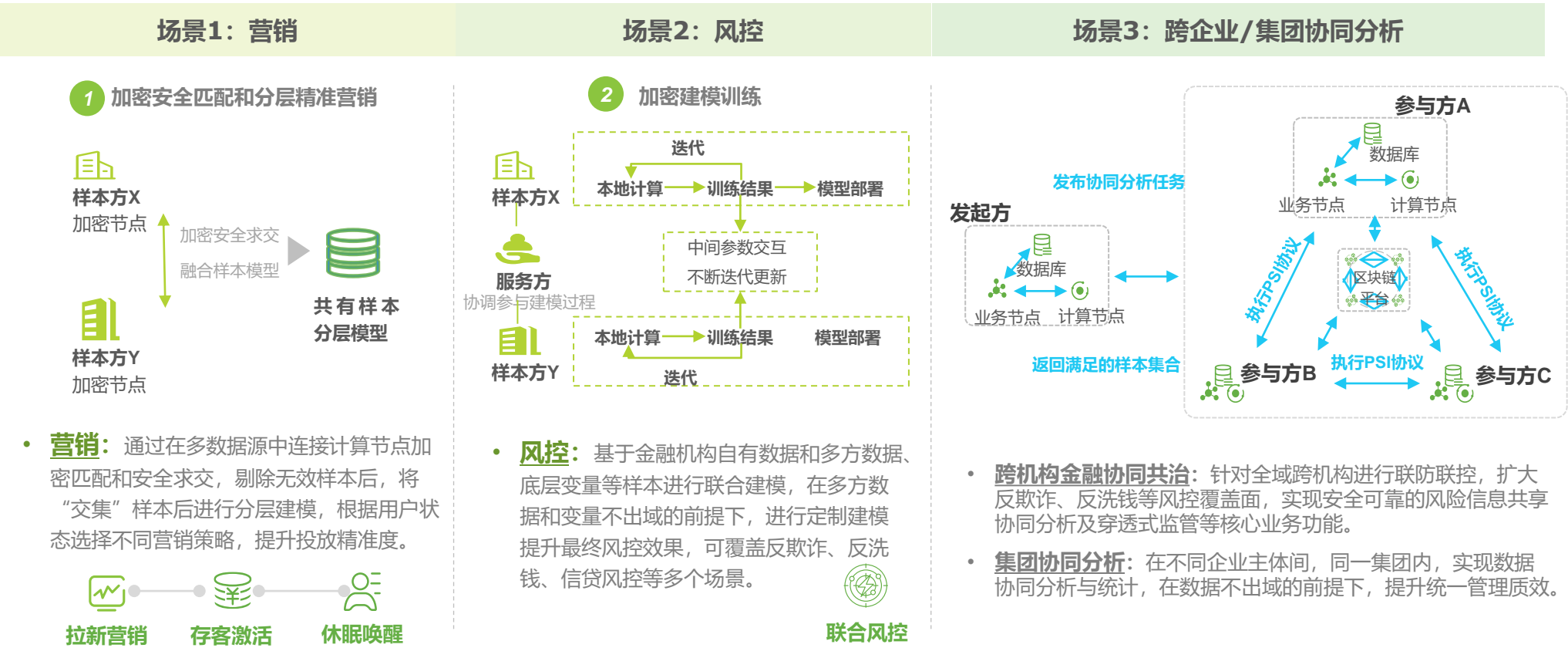
隐私计算技术典型应用场景解析—金融

隐私计算应用以营销和风控场景为主，金融行业作为数据使用方，连接多种数据源的需求较强

金融行业以营销和风控两大场景为主导，跨机构与集团协同共治场景为辅助，整体来看多种类数据源方的连接诉求较强。每一类场景中，涉及个人主体数据、征信、各大APP上的消费行为数据、企业数据和其他行业数据等多种类数据，需对接多方数据源加密匹配以提升营销、风控的精准度，以支撑运营决策。同时，跨机构与同集团的协同分析，通过安全求交的方式在数据不出域的情况下，实现数据共享与协同分析。

解决方案

场景说明



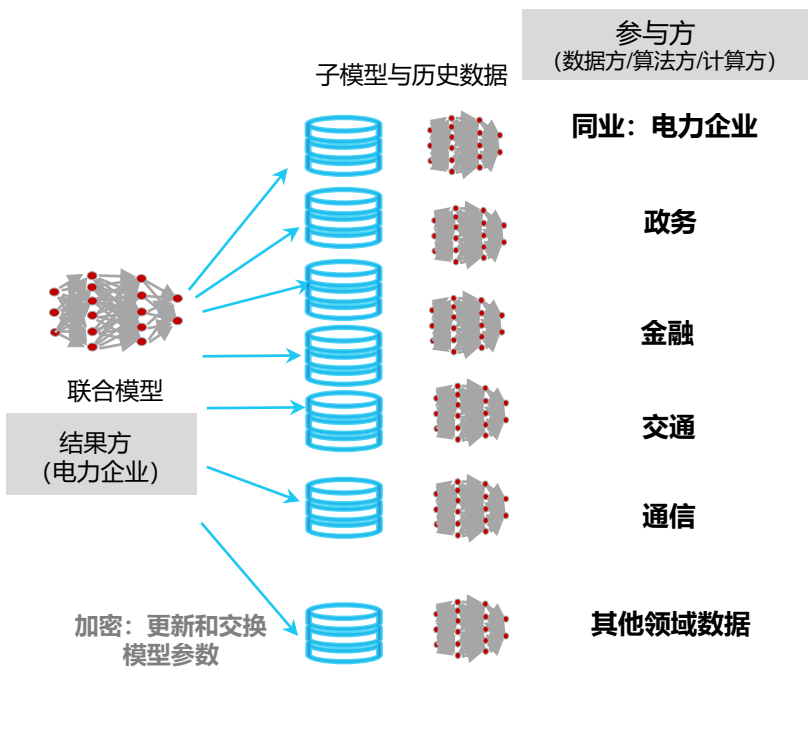
来源：外部专家访谈，公开资料整理，艾瑞咨询自主研究绘制。

隐私计算技术典型应用场景解析—电力

电力行业数据由于具备公共行业数据属性，多作为数据供给方，通过加密的方式赋能其他行业应用

基于联邦学习平台，在各行业部署安全节点之后，电力企业可链接各行业用于各类场景应用：1) 从横向来看，可通过电网能源大数据中心，跨省市进行数据调取与安全统计；2) 纵向来看，一方面在自有系统内，连接其他数据进行实时性电力负荷评估与回收；另一方面，安全输出电力数据赋能城市经济运行、税收和小微信贷风控，以及为新能源电桩建设布局提供精细化决策支撑等，最终促进与政务、金融、交通、新能源等多行业的深入结合，推动数据流通生态建设。

基于联邦学习在电力行业的应用



横向

纵向应用

具体场景与应用能力

-  跨区域数据共享
-  城市数字大脑
-  税收风险分析
-  小微信贷风控
-  电桩布网
-  电力负荷评估
-  电费回收预测

- 基于电网能源大数据中心，在各省市地区分别部署联邦学习平台节点：各省市可接入本地重点企业的能耗数据，以及跨省市进行耗能统计、对比和评估。
- 通过连接各单位组织（企业、家庭、机关及事业单位等）实时电力数据与智慧城市中心，协助与支持政府进行民生情况、用电实际等更精准地监测和决策，推动经济发展与运行。
- 关联税收情况与电力数据，通过用电成本反应企业的真实运转情况，与税收反应的企业生产活动强弱度共同监测、交叉分析，针对企业真实生产经营情况建立全面深刻的监测与洞察。
- 通过隐私计算联合建模，在保证数据安全不出库的前提下帮助金融机构更精准建立风控画像，评估风险状况，优化整体的风险决策路径。
- 通过深入场景，关联交通、支付情况、园区车辆数量、停车时段等维度数据，精细化预判区域内所需新能源充电桩数量，为充电网络规划与预测提供支撑。
- 电力系统自身在规划用电和调度过程中，负荷预测是其中的重要组成部分。通过结合气温、交通流量、移动网络等维度，对用电负荷情况进行实时监控，保障供应情况平衡稳定。
- 通过结合运营商对用电主的通信、缴费和信用情况进行综合评估，对欠费未缴的用电主进行风险模型评分，综合提升风险查全率。

隐私计算技术典型应用场景解析-工业制造业

隐私计算通过加密保护的方式，在跨产业链上下游、生产制造监控等场景内发挥着增强数据流通的作用

在工业制造业场景中，隐私计算在保障数据安全不出域的情况下，发挥着促进数据流通，释放数据价值的作用。其中主要场景有：1) 在横向产业链上下游可信和 2) 纵向制造企业内部联合监控与预测。1) 产业链上下游当中，涉及整体生产制造企业与多家零件供应商合作的情况，在此场景下，传统的质检和零件安全验收环节通过人工抽样进行，安全可信度不高，而通过部署安全可信的节点以加强质检模型训练，可助推质检全自动化；2) 通过联合企业内多生产设备，在数据不出设备的前提下，进行互联互通，统一归纳管理，完善全生命周期的生产制造管理准确性及可控性。

基于多方安全计算在制造业的应用

数据提供方: 零件供应商



计算方



发起方: 制造企业



场景1: 产业链上下游数据流通可信合作

- 工业制造企业通常涉及多个零件采购供应商的管理，以往生产质检过程中，需要人工质检，依赖经验和工作态度，抽样方式的准确性和可信度不高。
- 基于隐私计算保护和区块链存证技术，可通过安全可信的计算节点，链接零件供应商的本地相关数据，在通过训练后，提供密文数据给计算方加密计算后，输出机器学习模型所需的质检参数，助推实现质检全自动化，提升生产管理的质效。



场景2: 制造企业内部多设备联合监控与预测

- 在生产制造的实际场景当中，通常涉及企业内多环节、多类型、多个数的生产器械，连贯性的生产制造流程产生了繁杂大量的数据，不同的生产设备之间数据无法直连互通，对于全周期的生产流程监测预警和日常管理增添了不少成本。
- 通过部署加密安全隐私计算节点，在数据本身不出所在设备主体的前提下，通过加密计算节点进行传输、归集汇总，并建模计算以实现各生产设备之间的数据联动，异常预警和日常实时监控以确保生产安全，完善并提升生产制造的管理效率。

隐私计算技术典型应用场景解析-医疗

医疗健康数据安全必要性日趋攀升，隐私计算助力探索医疗数据共享与流通

医疗场景当中，保护医患就诊个人隐私的必要性和重要性日趋增强。这一特性也导致了各医疗机构和医药产业链相关企业主体之间，具备较大的信息壁垒，广泛地造成了就医不变、医疗应用数据资源有限无法共享应用等问题。隐私计算在智慧医疗、医学科研应用和药物研发三大细分场景中，均通过保护数据源不出域的情况下，增强数据的共享与流通，发挥数据多次利用的价值，赋能多个实践应用。

智慧医疗生态

围绕个人就诊的全流通智慧医疗生态



以往为了保护医疗就诊人的信息隐私，往往会出现无法跨院信息调用的情况，导致就诊就医和医院诊疗决策上数据无法共享的情况。

基于隐私计算保护技术，可通过安全可信的计算节点，连接打通各医院之间的就诊系统、临床医疗诊断的决策系统等，一方面可帮助就诊者跨院、异地治疗更加高效便捷，在安全保护的前提下实现就诊资料互通；另一方面增加数据储备与建模，优化临床辅助决策模型的精准度。

医学科研应用

多机构联合的医学科研平台



- 针对部分罕见疾病、关联归因分析等场景常面临数据不足、共享可行性小，临床患者隐私泄露等问题。
- 隐私计算可用联邦学习技术建立医学科研应用平台，连接各方数据，在医患数据不出本地的同时，加密提供模型参数得以在各方内部所部属的模型进行训练，得出所需结果与应用。

药物临床研发与试验

数据共享加速新药研发



新药研发过程往往耗时10-20年之久，医院临床和病患健康等数据涉及隐私问题无法与研发侧共享，造成研发难度大耗时长。

基于隐私计算保护技术，可通过加密数据不出本地的方式提供民众健康、临床病患诊断详情等数据，为药企研发和模型优化提供更多的燃料，加快研发速度与研发精准性，以更贴合实际病患情况。

02 / 2023年中国隐私计算市场 现状

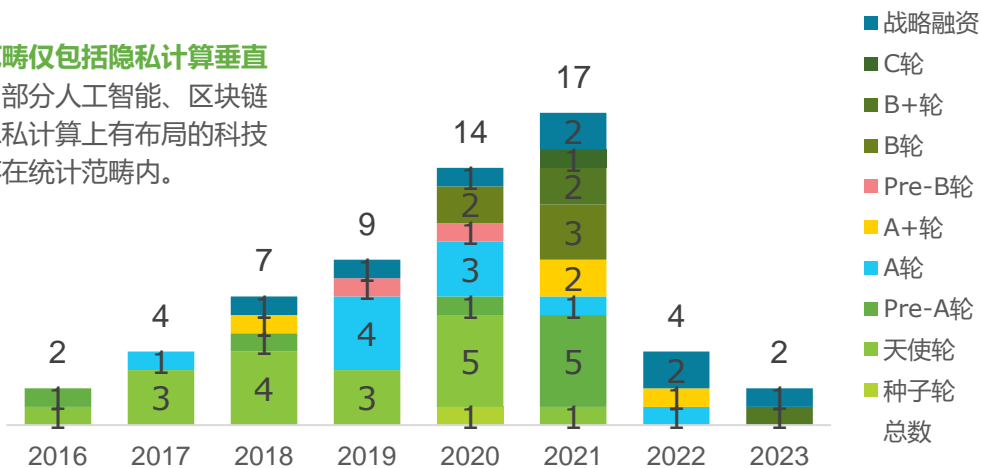
资本市场寒冬，行业趋于“冷静”

2023年隐私计算融资数量与市场规模增速双双回落，但预计2024年开始将会加速增长

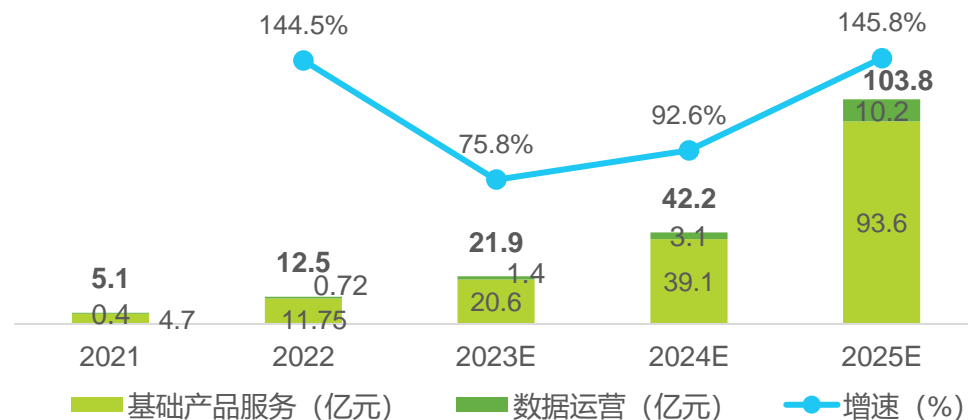
2021年后投融资持续降温，融资事件数量回归个位数。同期，2022年隐私计算市场规模约12.5亿元，主要由基础产品服务采购贡献；而受市场趋于冷静的影响，2023年市场规模增速有所回落，市场规模将约达21.9亿元。随着公共数据授权运营平台持续建设，数据运营业务有望快速增长；整体来看，业务模式在中期内未有较大的结构性变化，随着多行业多场景应用持续扩大，预计2025年中国隐私计算市场规模将增长至103.8亿元。

2016-2023年12月中国隐私计算行业投融资事件数

统计范畴仅包括隐私计算垂直厂商，部分人工智能、区块链等在隐私计算上有布局的科技公司不在统计范畴内。



2021-2025年中国隐私计算市场规模（亿元）



随着市场对于隐私计算技术认知的提升，市场同时受资本市场寒冬的影响，逐渐趋于“冷静”，2022年以金融为代表的行业陆续部署采购与部署基础产品服务，而2023年随着小部分企业用户开展场景类应用外，市场增速降低至75.8%，预计2023年全年市场规模将达21.9亿元。

- 随着公共数据授权运营平台建设加速开展，能源、医疗等其他行业也在陆续入局，预计2025年将持145.8%的增速，市场规模将有望达103.8亿元。

注释：1. 2021-2022年的市场规模统计了市场公开招投标信息+非公开招投标信息（通过对行业客户的调研、厂商营收调研等形式获取）；2. 2023~2025年的市场规模发展，研究团队分别对金融、政务、运营商、医疗等领域的技术应用者展开了大规模调研，征询了其在未来3~5年的隐私计算投入规划。在此基础上，研究团队还参考了《“十四五”大数据产业发展规划》等相关政策中的大数据产业发展目标，进而对隐私计算市场的发展展开了综合预判。
来源：市场调研、行业专家访谈、艾瑞数据统计模型、艾瑞咨询研究院自主研究及绘制。



2020年和2021年是近年来资本热度最高的两个年份，轮次分别多集中于种子轮~A+轮，以及Pre-B轮~C轮；

- 2021年后，随着资本泡沫化消退，2022与2023年间隐私计算融资事件数仅分别为4起和2起。

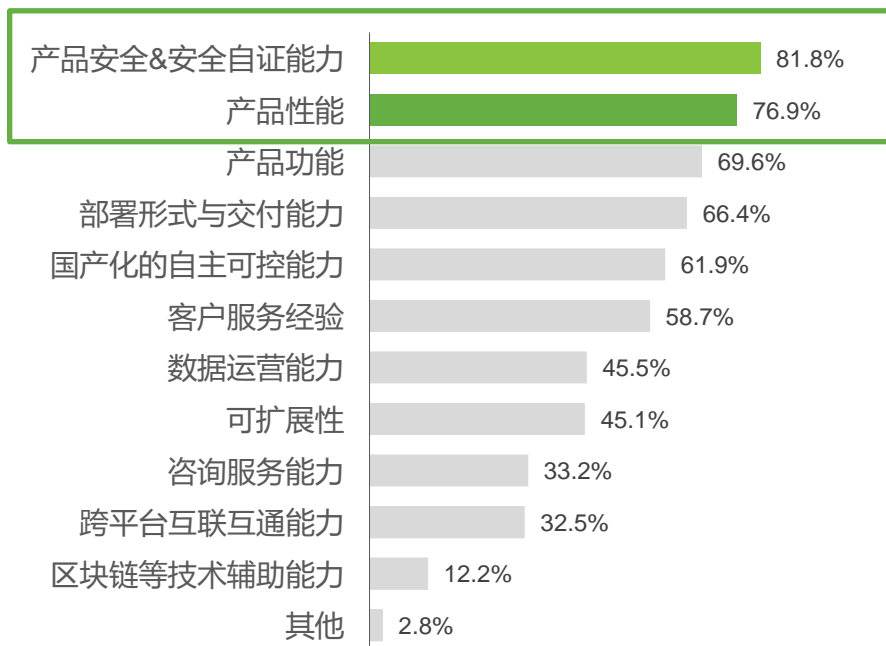
来源：1. 2023年的投融资事件数统计截至2023年12月20日；2. 部分企业的投融资信息未进行对外公开的情况，不在上述统计范畴内。
来源：企查查、IT桔子等行业公开信息、厂商调研、艾瑞咨询研究院自主研究及绘制。

需求侧：安全与性能并重

在应用实践中，隐私计算在安全自证和性能方面迎来新的挑战

在实践应用隐私计算产品与服务的过程中，艾瑞调研泛行业用户发现，产品安全&安全自证能力和产品性能是用户选型过程中首先考量的两大因素，分别占81.8%和76.9%。1) 在产品安全&安全自证维度，隐私计算包含2大安全风险：产品自身的算法可解释难度和部署过程中平台及系统安全；2) 在应用过程中，28.9%的应用者反馈真实业务环境远比POC测试更加复杂，对性能表现未达预期。再者，复杂的真实业务环境会加剧算法和平台系统安全两大方面的风险，在多种风险相互糅杂的情况下，隐私计算在业务上的部署在安全和性能方面面临新的挑战。

泛行业用户所关注的隐私计算技术服务商能力



隐私计算产品与实践应用中的安全与性能问题

两大安全风险

算法可解释难度

- 算法自身安全性
- 算法可解释难度

产品本身方面

平台及系统安全

- 平台及系统自身的安全性
- 外部攻击风险
- 三方机构介入带来的潜在风险

部署过程中方面



28.9%应用者反馈：产品在真实业务环境中的性能表现和POC测试环节中的性能表现存在差异。

➢ 性能表现存在差异的前三个原因为：

- ① 真实业务环境中的多方协同计算场景要远复杂于测试环境。
- ② 是由于产品测试环节中的加密轮次低于真实业务环境中的要求所形成的差异。
- ③ 是由于数据预处理情况不同所导致的性能差异。

✓ 真实业务环境的复杂度会加剧上述两大安全风险，多种风险会相互糅杂，业务部署的安全和性能方面迎来新的挑战。

注释：1. 左图（N=286；其中金融领域151位、政务领域135位；受访者包括技术岗位从业者、业务岗位从业者，针对目前阶段的能力关注点发表了看法。）2. 右图（N=135；调研样本来自银行、保险、政务、运营商、医疗等领域的隐私计算技术应用者（含IT/科技部门应用者、业务部门技术应用者））
来源：艾瑞咨询研究院自主研究及绘制。

需求侧：技术认知逐渐深入

随着需求侧对隐私计算技术认知的逐渐深入，部署重点由“大而全”向“小而美”场景应用转移

自2021年进入隐私计算商用元年后，以金融行业为代表，业内头部机构开展了隐私计算平台建设及试点应用。随着对于技术认知的逐渐深入，2023年内在金融行业基于隐私计算的招标投标采购中陆续出现了细分场景的数据服务、平台升级等项目；同时，以电力、能源、政务大数据等为代表的行业和领域也陆续开展隐私计算的平台建设，数据源和使用方链接进一步连点成线。未来可以预见，在各行业的持续探索下，隐私计算技术将持续搭载着各行业连线成面，建设可信数据网络，促进数据流通，进一步释放数据价值。

时间线
与
市场特征

2021年

2021年是隐私计算商用元年。

- 头部金融机构开始试水隐私计算：工商银行借助多方安全计算技术，探索建立了跨行资金流向监测工具，各地金融科技创新监管试点工作的13项涉及隐私计算项目中，交通银行成功申请3项；光大银行上线了企业级多方安全计算平台；
- 农业银行、招商银行、浦发银行、微众银行等多家银行也已启动隐私计算技术研究、试点应用；
- 落地场景多为“大而全”的隐私计算平台建设。

2023年

- 2023年随着金融机构对隐私计算技术认知逐渐深入，隐私计算部署重点开始向“小而美”的场景应用转移。细分场景数据服务、隐私计算的平台升级等招标投标项目有所增加；
- **领域多元扩张**：电力、能源、政务大数据、港口等领域进行招标投标采购基于隐私计算的平台项目数量逐渐攀升。

未来

- 平台搭建完成，各行业领域持续探索并深化，以互联互通为基础底座，建设可信数据网络，发挥数据价值，促进数字经济蓬勃发展。

隐私计算应用
实践发展
路线

1

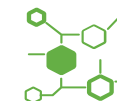
隐私计算平台建设

2

数据源和数据使用方的链接

3

可信数据网络



公共数据授权运营平台开展建设

政策推动下，各省市地区开展公共数据授权运营平台建设

2022年12月，中共中央和国务院联合发布《关于构建数据基础制度更好发挥数据要素作用的意见》（简称“数据二十条”）明确提出建立公共数据授权确权机制。2023年以来，各省市不断出台相关政策，加强所在地区的平台建设与实施应用。现阶段，公共数据一体化平台已基本建设完成，将继续优化和不断完善，支撑公共数据流通和数据要素价值释放。隐私计算将会作为关键技术模块，全方位助力公共数据授权运营安全有序开展，促进公共数据与社会数据融合。

公共数据授权运营生态建设重点政策解析

国家
政策

2022.12 中共中央、国务院《关于构建数据基础制度更好发挥数据要素作用的意见》（“数据二十条”）
提出构建数据基础制度体系，促进数据合规高效流通使用

2023.12 国家数据局《“数据要素×”三年行动计划（2024—2026年）（征求意见稿）》

意见提出，到2026年底，数据要素应用场景广度和深度大幅拓展，在经济发展领域数据要素乘数效应得到显现，打造300个以上示范性强、显示度高、带动性广的典型应用场景



各省市
授权运营
专项政策
出台

2023年以来，浙江、杭州、河南、江苏、青岛、甘肃、北京、广州、贵州等省市，发布公共数据授权运营地方政策文件，**强调建立完善公共数据授权运营管理机制，多次提出完善隐私计算技术体系、加强技术攻关、开展技术部署与应用，促进公共数据授权运营规范化发展。**

公共数据授权运营生态建设架构与建设情况



03 / 中国隐私计算行业现存挑战和未来发展路径展望

隐私计算现存挑战与探索路径的进展情况

计算性能、技术壁垒和场景应用深化为中国隐私计算行业发展的三大现存挑战，相应地在行业协会、业内从业者等多方的推动下，在底层增强技术可用性，生态与应用持续建设与深化等方向上持续努力

中国隐私计算行业的现存挑战

计算性能

- 密文计算自身需要耗费较大的通信量和计算量，对计算性能存在较大挑战。目前，安全求交、匿踪查询等应用场景，部分为了提高计算量，选择离线计算，应用场景上有所限制，性能优化仍为隐私计算仍待突破的主要挑战之一。

技术壁垒 & 安全性

- 同技术路线下，不同厂商由于知识产权问题在底层协议和算法两方面，均有异同。这两方面的异同导致了业务方同一集团内搭载不同厂商的产品后，难以连接和互通；同时，在对接多种数据源的过程中，“黑盒”问题持续出现，且被不断放大。
- 再者，多种技术壁垒会导致在回溯、审计与验证密文计算过程时，对安全性的评估难度不断加大，挑战重重。

场景应用

- 随着技术常态化，在市场供需双方对于隐私计算技术本身的理解趋于冷静后，一方面技术优化仍需持续努力；另一方面，由于隐私保护的重要性适用于全行业，各行业业态中，需要有前瞻性的行业专家带领着，主动去探索隐私计算技术在业务应用上的适配与实践，以更好地发挥数据价值。现阶段，如何衔接隐私计算技术与行业应用，仍面临较大的挑战。



中国隐私计算行业探索路径进展

技术上性能优化

- 分布式计算与并行处理提高计算效率
- 加速GPU等硬件设备的对接和兼容，通过硬件加速运算过程

生态上多方联动的互联互通

- 厂商自身加速融合多种技术路线
- 厂商联合业务需求方进行算法层面的互联互通共建
- 由隐私计算联盟牵头的进行探索互联互通行业试点，开放算法协议簇，以及通过开源助力互联互通透明化和安全化

应用上行业持续布道

- 《“数据要素×”三年行动计划（2024—2026年）（征求意见稿）》提出加强数据要素在各行业的应用
- 蚂蚁摩斯连接行业各方进行社区共建，探索场景应用深化
- 厂商联合生态合作伙伴在各行业细分场景中进行深入探索

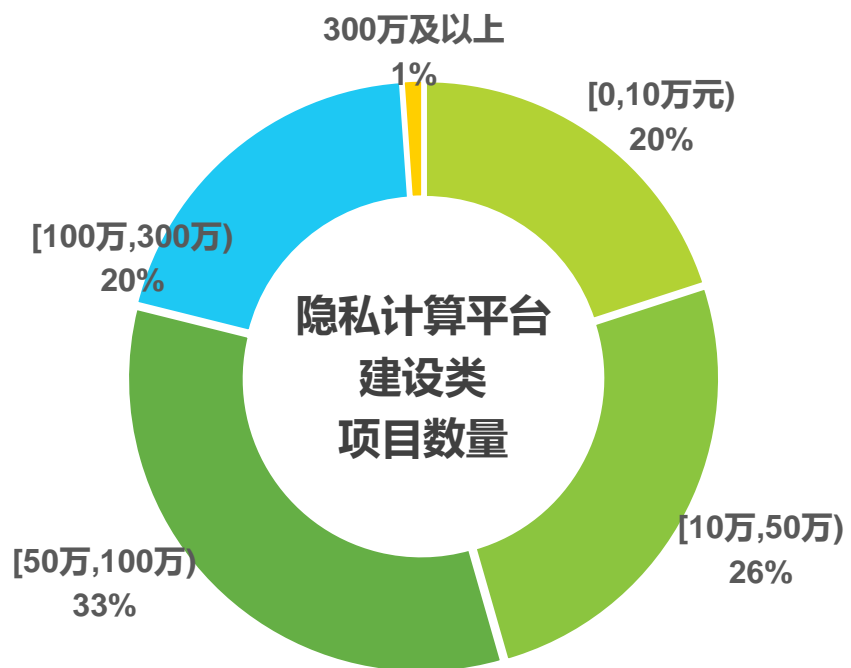
中国隐私计算行业未来发展路径展望

@iResearch

- 供给侧厂商可持续发展特征
- 隐私计算技术应用路线
- 隐私计算产品选型重点
- 基于隐私计算技术的可信数据流通模型
- 企业内外：隐私保护管理的生态建设
- 全行业数据要素流通与循环应用

冷静期的市场环境下，对供给侧资本储备和变现能力提出更高要求

中国金融机构隐私计算平台建设类项目的价格分布
(%) (含2021与2022年)



Insight 1

- 价格战：金融机构对隐私计算平台建设类项目的预算设置多集中在100万上下或数十万，部分项目甚至设置了更高预算，但因为价格战，许多项目实际采购价格远低于预算金额。
- 金融机构客户更加注重后续服务的质量和可持续性，因此部分客户抗拒过度的价格战。

Insight 2

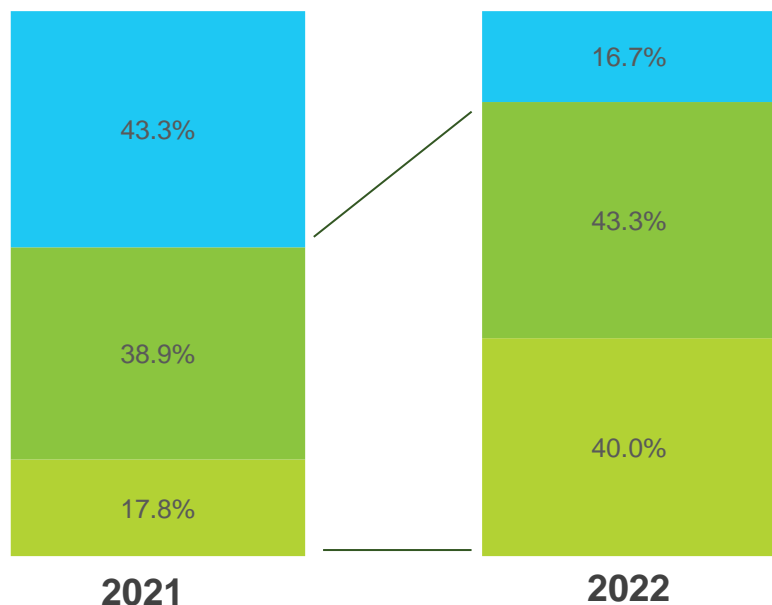
- 部分不能自负盈亏的创业厂商，已经开始转型；
- 少部分创业厂商甚至退出市场

Insight 3

- 对金融机构而言，招投标中，如果选择创业型原生隐私计算厂商，需要综合考虑厂商的可持续发展情况。

安全与性能的需求平衡下，软硬结合的实践应用需求有望进一步释放

行业用户对隐私计算机软硬件结合技术方案
关注度调研 (%)



■ 重点关注 (%) ■ 关注，但不作为重点 (%) ■ 不关注 (%)

Insight 1

- 隐私计算机软硬件结合的技术方案可以兼顾性能和安全性保障：
- 关注软硬件结合的解决方案的行业用户（如左图，包含“重点关注”+“关注，但不作为重点”）占比从56.7%攀升至83.3%。软硬结合的技术方案可以通过加速卡、可信硬件等多维技术方式，兼顾性能和安全性保障。

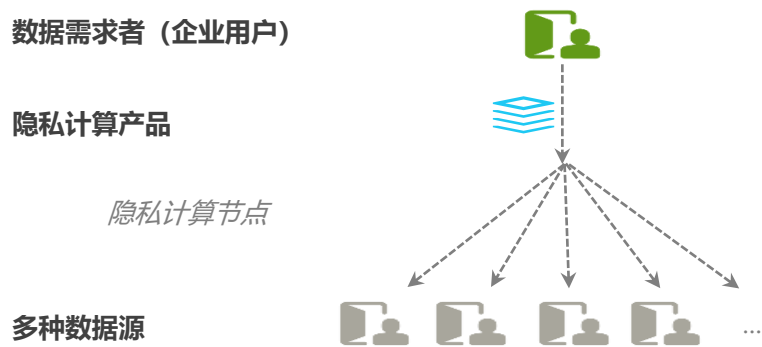
Insight 2

- 越来越多的市场玩家在软硬结合技术方案上展开布局：
- 蚂蚁摩斯、冲量在线、洞见科技、数牍科技、可利邦等越来越多隐私计算厂商的入局也促进了软硬结合的正向发展趋势。

注释：随着技术应用的持续深入，研究团队分别在不同的时期内，对同样的90位技术负责人进行了相同的调研。
来源：市场调研、艾瑞咨询研究院自主研究及绘制。

数据资源和行业Knowhow将持续为融合隐私计算技术与场景实践的主要抓手

- 从数据需求者（企业用户）视角出发，有数据源储备、链接多方数据供给源能力较强的厂商将帮助数据需求者在落地隐私计算技术于场景实践的过程中，更好地契合自身需求，减少链接成本，提升实践效益。
- 再者，随着需求侧企业用户的技术认知逐渐深入，细分场景的需求将不断被释放，行业knowhow与场景认知较强的厂商有助于解决方案深入场景，更贴近真实业务环境，进而驱动业务创新，提升整体企业效益。



Section 1 数据资源的厂商将提升实践应用效益

- 以数据需求者（企业用户）为出发点，通过隐私计算的技术，隐匿的方式来连接多种数据源，服务于自身的业务场景。
- 以金融业为例，金融细分场景在应用过程中所需连接数据源包含互联网、公共、运营商、金融同业等多方，能够率先布局有数据资源储备、连接通畅的厂商能够更高效地帮助数据需求者将业务需求化为应用，减少部署与链接成本。

Section 2 行业Knowhow与场景认知为隐私计算技术服务商的稀缺竞争优势

- 随着需求侧企业用户对于隐私计算技术认知愈发深入，部署与应用重心向细分场景倾斜时，解决方案中行业knowhow与场景认知重要性愈发凸显。
- 由于真实业务环境趋于复杂，场景认知更深入、行业理解更透彻的技术服务商能更好地洞悉客户需求，融合技术与真实场景，最大化贴近开箱即用，提升好用性以发挥技术作用，转而赋能业务。



互联互通的生态建设背景下，TDaaS是一项值得被业内关注的可信流通能力范式

TDaaS的三层关键能力模型



无论是技术厂商，还是终端用户，TDaaS均可以作为一项值得关注的战略技术目标或趋势

Insight 1 TDaaS的架构封装了可信运营所需要的所有能力

- 在实践经验积累的过程中，TDaaS将对算法、模型、数据调用功能等多元化能力进行抽象与封装，可以让用户按需调用相关功能，且TDaaS应该支持单点功能的部署与使用。
- TDaaS不只是功能的集大成者，还可以帮助用户在安全可信的前提下，快速接入所需数据，TDaaS的产品提供方还应该建设参与者丰富的跨平台互联互通生态。

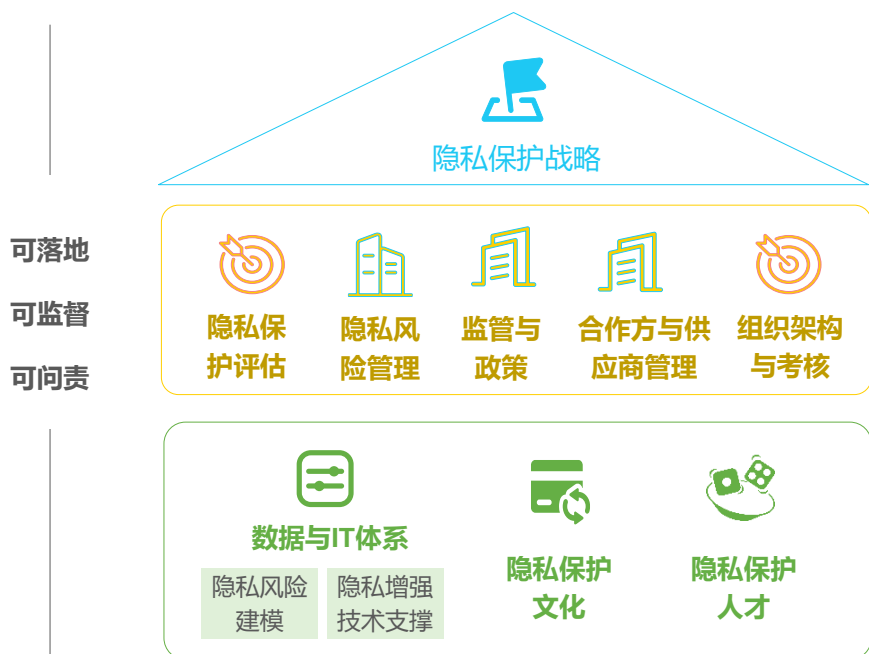
Insight 2 赋能生成式AI，基于可信数据方案，构建可信金融行业大模型

- DaaS产品需要融合自适应AI能力来应对变化莫测的业务环境和规则以及数据的调整与更新，根据即时的动态反馈来敏捷调整模型，帮助客户实现业务敏捷响应。而这项能力应该出现在TDaaS 2.0或TDaaS 3.0阶段，并不成为TDaaS 1.0的必选项。

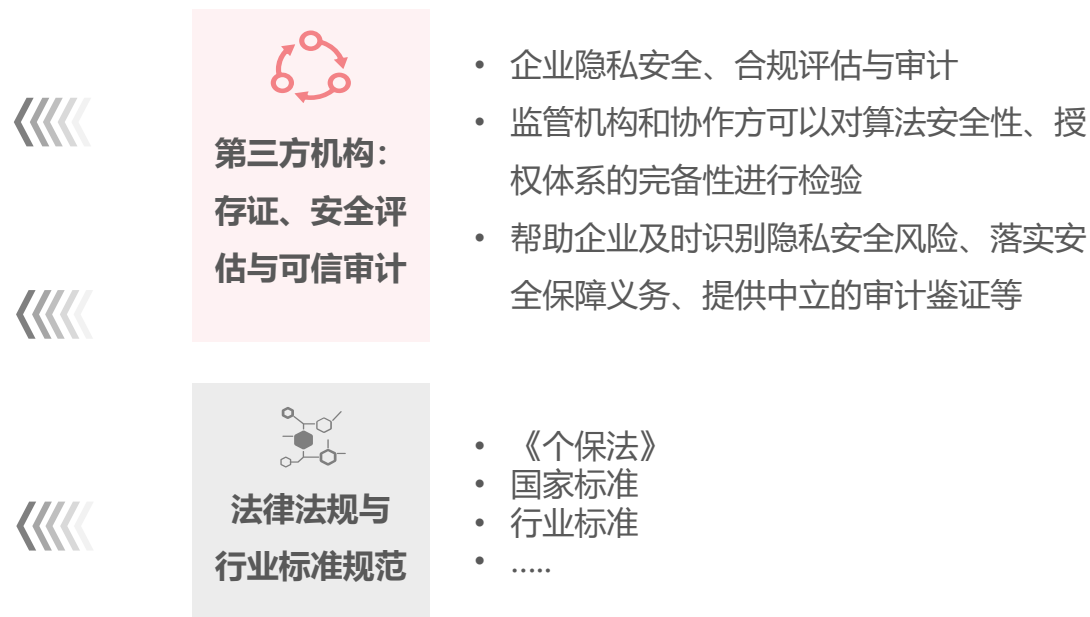
基于多技术融合的基础底座，完善隐私工程体系建设，强化隐私保护与安全合规

- **企业内：全生命周期的隐私保护管理：**隐私保护要求融合进企业管理，从数据与隐私保护IT体系建设、文化与意识和人才培养出发，搭建涵盖隐私保护评估、风险管理、监管与政策响应、合作方管理和组织架构与考核的全生命周期的隐私保护管理，服务于隐私保护战略，促进企业内部上下运行与监督管理，确保隐私保护工作的可落地、可监督、和可问责。
- **企业外：**基于国家法律法规，外部建设第三方存证、安全评估与可信审计机构，与企业内部的隐私工程管理形成衔接，加强隐私工程的安全评估与存证审计，弥合技术与法规之间的鸿沟，推进行业在安全可信基础上良性发展。

企业内：全生命周期的隐私保护工程管理体系



外部监管与监督



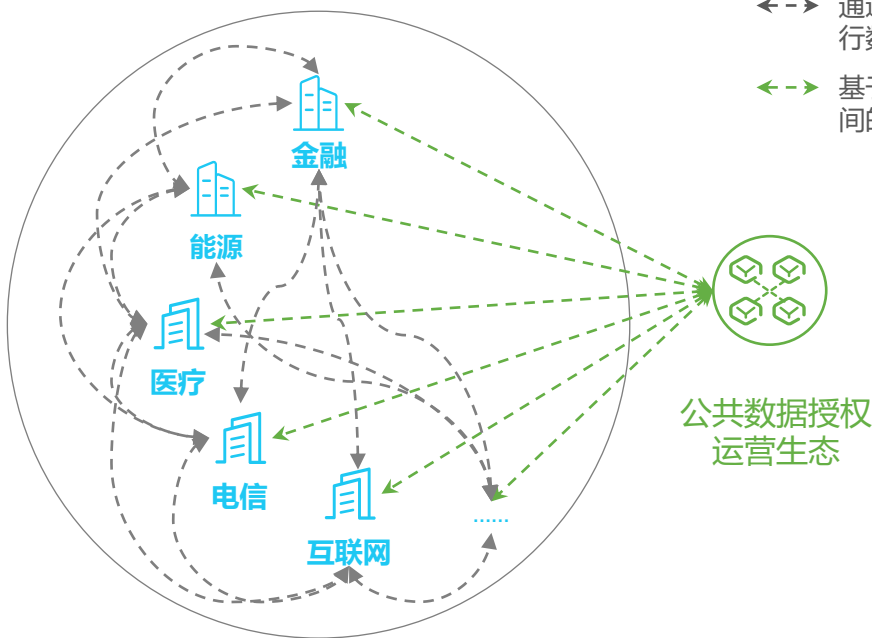
公共数据授权运营与多行业场景应用并行，共同促进数据要素流通与循环

- “数据二十条”的推动下，各省市地区纷纷开展公共数据授权运营平台建设，隐私计算作为其中的关键技术模块，其厂商陆续与各地政府开展合作，将助力政府进一步探索公共数据的授权运营和管理，释放数据要素的价值，服务实体业发展。
- 同时，随着隐私计算在各行业的市场商业化应用不断探索和持续深入，以金融行业为例，作为数据需求方，通过在实践中凝结了公共、电信、互联网、金融同业等数据提供方，在应用过程中不断碰撞与探索真实业务环境与技术发展，越来越多的行业数据需求方和供给方进入生态圈。
- 随着市场化应用与公共数据授权运营的并行发展，以技术为底层驱动力，更好地促进数据要素的流通与循环，有效释放数据要素价值，增强数字经济发展效益。

基于隐私计算的数据要素的流通与循环应用

市场化应用

- 各行业通过开展对于隐私计算技术的探索和应用，由数据需求方的行业发起，在实践中连接了同业以及其他行业等数据方，在探索过程中，越来越多行业进入生态圈。



- 通过隐私计算在同业、不同行业之间进行数据“可用但不可见”
- 基于公共设施数据授权运营与各行业之间的连接

数据授权运营

- 通过将数据按照应用场景进行分类分级后，承接不同行业和场景的数据需求，根据隐匿方式进行输出；
- 同时作为统一的空间，协调多方数据，让数据提供方与消费方数据空间交换过程中，均得到端到端的安全保护。

04 / 中国隐私计算行业卓越厂商 与优秀案例

iResearch-隐私计算卓越者 入围介绍



如何确定入围者?

“隐私计算 卓越者”的评选由内外两部分评审团组成：内部评审团的评审权重为20%、外部评审团的评审权重为80%。



步骤1 卓越者提名

由“隐私计算 卓越者”的内、外部评审团队，共同进行隐私计算企业提名（本次共计提名企业45家，展开调研企业39家）。



步骤2 内部评审

由“隐私计算 卓越者”的内部评审团队对提名企业进行评选，输出评选结果。



步骤3 外部评审

由“隐私计算 卓越者”的外部评审团队对提名企业进行评选，输出评选结果。



步骤4 结果的审核校验

对评审结果进行校验审核，保证结果的准确公正性，确定最终入围者名单（本次最终入围企业17家）。



入围者的评估指标有哪些?

根据企业类型的不同，我们将“隐私计算 卓越者”分为“前瞻推动者、精益融合者”两个类别。每个类别企业均有相应的入围基准（在入围者名单公布的内容中有介绍），在此基础上，我们将对企业从下述维度展开能力评估。

$$\text{综合得分} = \text{技术\&产品力} \times 0.25 + \text{场景应用能力} \times 0.25 + \text{市场能力} \times 0.20 + \text{生态资源能力} \times 0.15 + \text{管理\&财务} \times 0.15$$



技术&产品能力 (25%)

- 产品安全
- 产品性能
- 产品功能
- 易用性
-



场景应用能力 (25%)

- 场景理解与复用
- 客户反馈和需求理解
-



市场能力 (20%)

- 覆盖行业数量
- 客户数量
- 商业营收
-



生态资源能力 (15%)

- 合作伙伴数量
- 上下游支持
-



管理&财务 (15%)

- 团队背景
- 团队规模
- 企业文化
- 融资规模
- 资源支持
- 资方平均
-

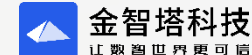
注释：评选指标括号内的百分数代表指标的评审权重。如有任何疑问，[请联系团队分析师。](#)
来源：艾瑞咨询研究院自主研究及绘制。

iResearch-隐私计算卓越者 入围企业



前瞻推动者

按企业汉语名称
音序排列



大型科技企业/大型机构对隐私计算的前瞻性布局，有效地推动了行业的发展。“前瞻推动者”要求企业拥有顶尖的科研团队、3年以上的隐私计算投入与研发、具备隐私计算技术的前瞻性探索经验、卓越的产品技术创新能力、优秀的技术落地实践能力，是推动隐私计算技术发展、商用落地的核心力量。



精益融合者

按企业汉语名称
音序排列



产业专家及艾瑞研究团队一致认为：隐私计算将与多元科技实现深度融合，而非“孤立式”的应用。“精益融合者”主要为非垂直于隐私计算领域的科技公司，包括区块链公司、人工智能公司、云计算公司、大数据服务公司、金融科技公司等。这类企业在隐私计算与多元技术融合的探索中发挥了高效的推动价值。

数纳斯—跨域流通商业增长引擎，以隐私计算为底座，提供一站式场景化数据应用服务，助力企业业务增长！

阿里巴巴集团的使命是让天下没有难做的生意。旨在助力企业，帮助商家、品牌、零售商及其他企业变革营销、销售和经营的方式，并借助新技术的力量与用户和客户进行互动，提升经营效率。业务包括中国商业、国际商业、本地生活服务、菜鸟、云业务、数字媒体及娱乐以及创新及其他业务。除此之外，我们的非并表关联方蚂蚁集团为我们平台上的消费者、商家及其他企业提供数字支付服务和数字金融服务。围绕着我们的平台与业务，一个涵盖了消费者、商家、品牌、零售商、第三方服务提供商、战略合作伙伴及其他企业的生态体系已经形成。



资质及行业贡献

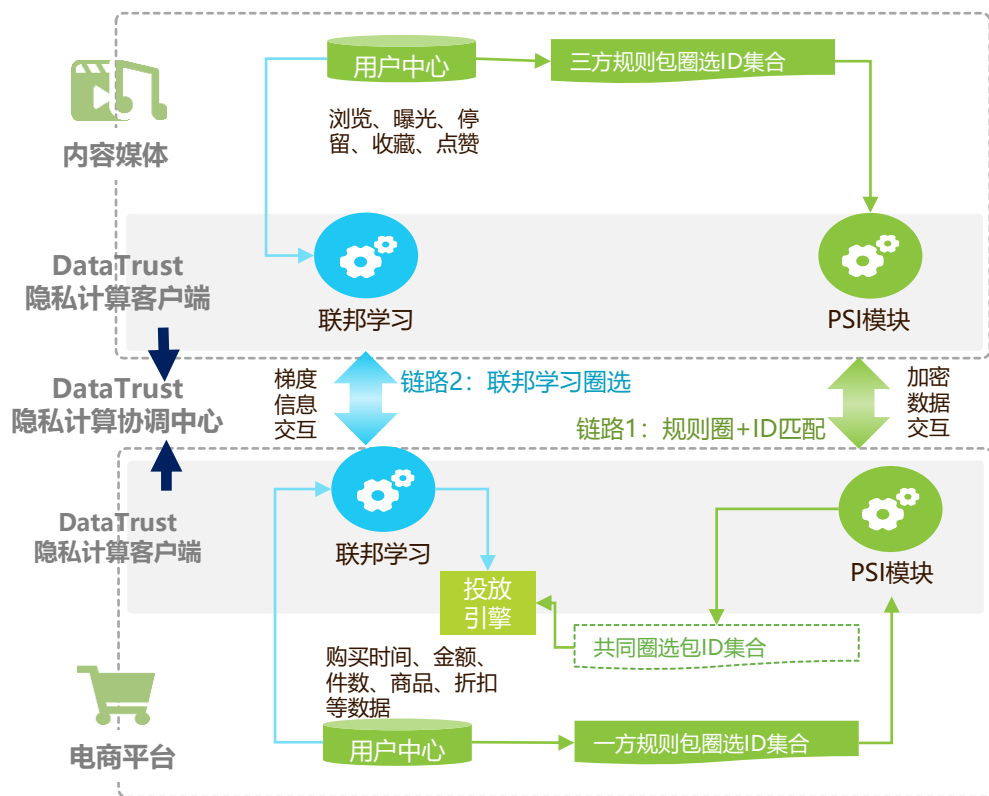
副理事长	20+项	10篇	2个	5个	4本
信通院隐私计算联盟	密码学算法专利	(7-A类、3-B类) 国际顶会	国家标准	行业标准	教研著作

权威认证



数纳斯—跨域流通商业增长引擎，以隐私计算为底座，提供一站式场景化数据应用服务，助力企业业务增长！

落地案例 – 电商营销场景



Part 1 项目概况

痛点：

- 1) **单平台流量见顶**：品牌触达消费者数据分散多个平台，单平台流量见顶，需要做全域精细化运营，做联合营销。
- 2) **营销成功率低**：过度营销造成营销成本增加，同时降低用户的体验感。

Part 2 实践方案与成效

- 借助数纳斯·DataTrust隐私计算的ID安全匹配、联邦学习，在人群自有特征平台方之间互不可见的前提下，得出更加优质的人群，从而优化品牌活动决策。
- 投放转化ROI提高25%。
- 优化用户体验，实现市场拓展。

生态合作伙伴

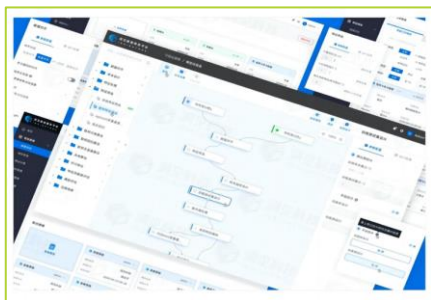


建设密态数据计算网络 赋能数据价值安全释放

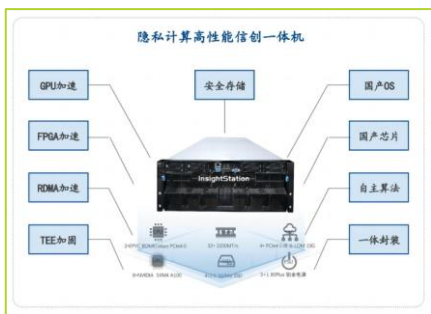
洞见科技是国内领先的隐私计算技术与数据要素生态服务商，致力于以“原始数据不出域、数据可用不可见、使用可控可计量”的方式赋能数据价值的安全释放，聚焦于为政务、金融、通信、能源、工业、医疗、汽车、互联网等各行业客户提供高质量的隐私计算基础设施、高可信的数据生态资源接入与高增效的数据智能应用服务。

洞见科技：隐私计算及数据要素产品能力介绍

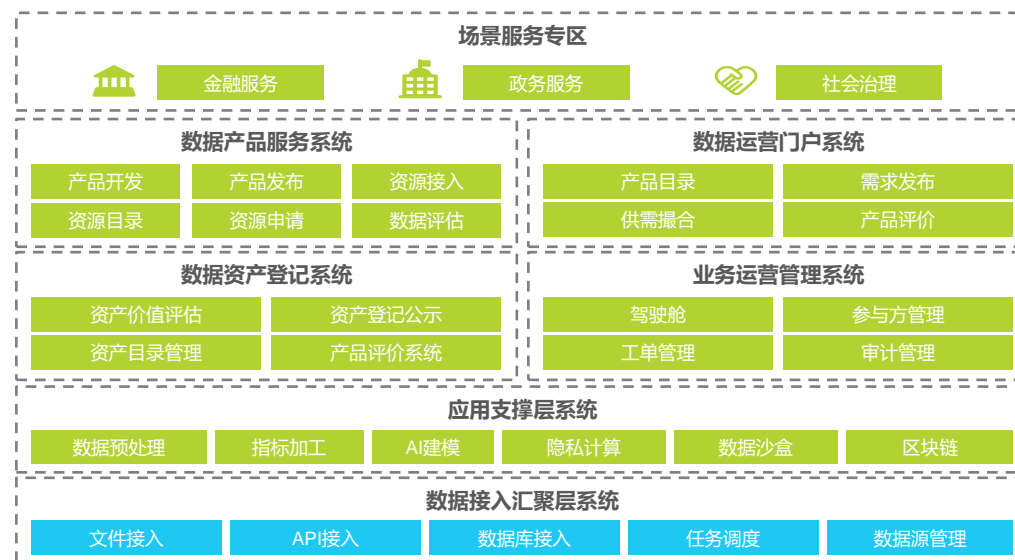
隐私计算平台：“软件+硬件+算法+模型”的一站式服务



- **高可控**
 - 密码学原理保障、信息论安全级
 - 数据、计算、监管分离、无中心
- **易应用**
 - 底层算法与算子优化、场景化专业引擎
 - 硬件专用芯片加速、海量数据实时处理
- **高安全**
 - 数据与计算分离，支持安全合规审计
 - X86与ARM全面适配，国产化自主可控
- **高性能**
 - 软硬件集成封装，支持开箱即用
 - 低代码技术架构，支持二次开发



公共数据授权运营平台：数据要素安全开放流通“全链路”支撑



平台价值

- 提供“技术+业务+运营”的一站式公共数据授权运营解决方案
- 实现公共数据“全生命周期”及授权运营“全流通链路”技术支撑
- 既能保障原始数据安全，又能释放数据要素价值，还能合规应用数据智能
- 面向场景的应用运营赋能，发挥“数据要素×”和“隐私计算+”倍增效应

洞见科技：隐私计算实践案例解读

洞见科技正在加速推进其“布点-连线-结网”战略：已在政务、金融、通信、能源、工业、医疗等领域部署了数百个隐私计算节点；基于上述节点并根据营销、风控等不同场景需求，将数据供给方与数据需求方的多方数据安全连接与融合，已落地大量商业化数据智能应用；同时，通过支持黑、白、灰盒的异构互联互通底座技术，正在构筑跨行业、跨平台、多层次、多领域的密态数据计算网络，推进实现全域数据智能。

洞见科技互联互通联合建模案例：某股份制商业银行线上消费贷新客预筛模型

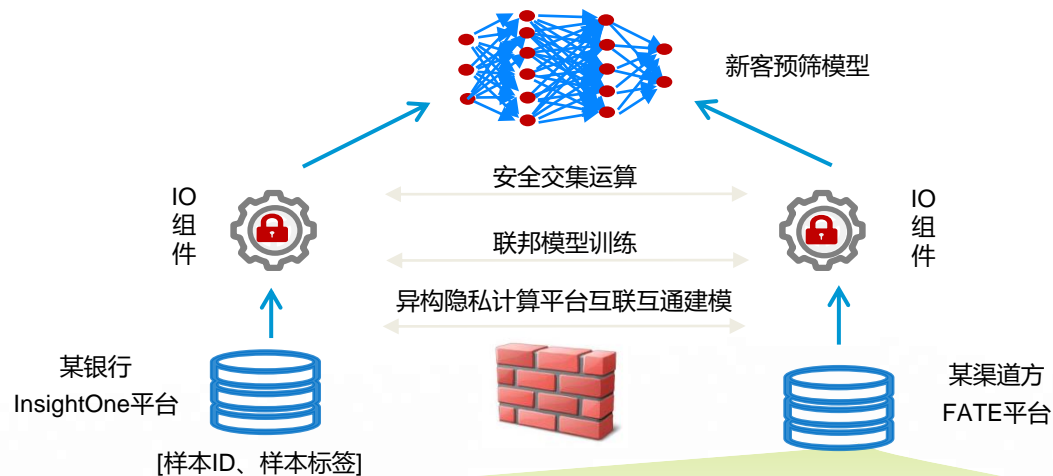
Part 1 项目概况

痛点：某银行希望提高线上消费贷产品在某渠道方的营销转化率，优化客群质量，通过隐私计算方式安全引入该渠道方的支付交易数据开展联合建模，构建新客预筛模型。

目标：通过隐私计算技术以异构平台互通方式构建新客预筛模型，实现风控预筛。

Part 2 实践方案与成效

- 模型AUC达到**0.8+**、KS达到**0.5+**
- 模型上线后，审批通过率提升**3-4**倍
- 最高区间通过率的提升度为**6**倍
- 异构隐私计算平台间的互联互通建模应用



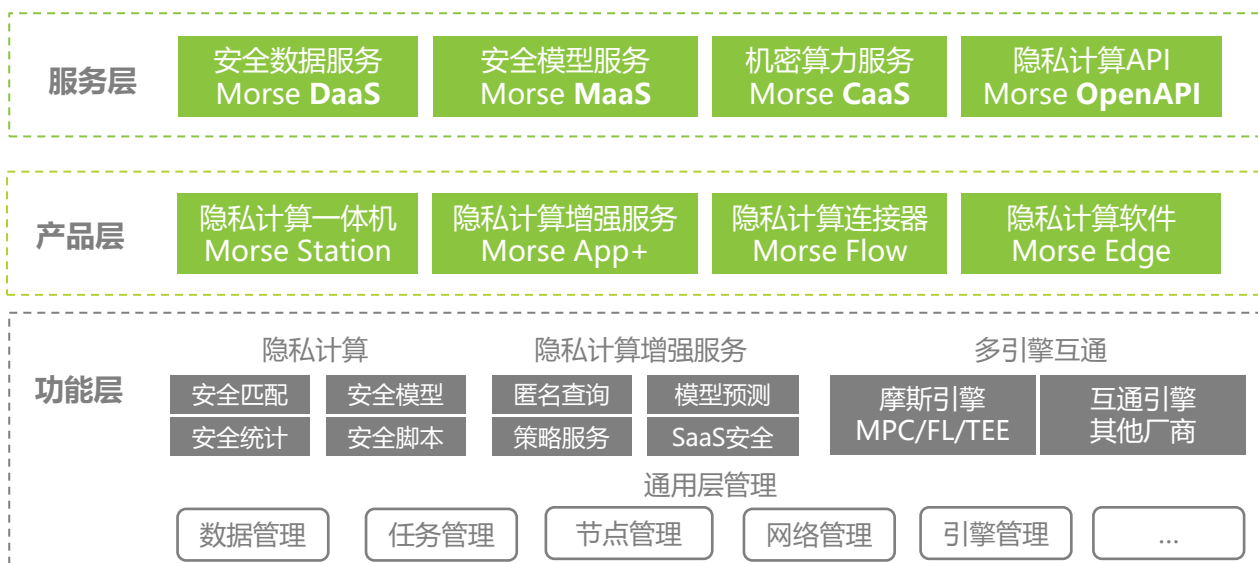
交易行为特征约2800维，涵盖不同交易类型、不同支付方式的交易笔数、天数、金额等多个维度。

- | | | |
|--|---|--|
| <ul style="list-style-type: none"> • 成功交易 • 失败交易 • 线上交易 • POS交易 • ATM交易 | <ul style="list-style-type: none"> • 消费金融类 • 娱乐类 • 公共事业类 • 医疗机构类 • 加油类 | <ul style="list-style-type: none"> • 节假日交易类 • 工作日交易类 • 周末交易类 • 分时段交易类 • |
|--|---|--|

中国隐私计算行业的领先布局者，致力于保障数据安全的前提下促进数据流动迸发价值

蚂蚁摩斯基于多方安全计算、可信执行环境、联邦学习等技术，致力于解决企业数据协同计算过程中的数据安全和隐私保护等问题，助推实现数据可用不可见，融合创新以进一步释放数据价值。蚂蚁链摩斯产品历经长期不断打磨，在安全合规、性能、生产可用性、服务完善度、产品多元性和资源储备六大方面持续深耕于扩充，已获得20余家领先权威机构认证，参与制定20+行业标准。蚂蚁链摩斯将持续加大对隐私计算研发和应用的相关投入，将持续保障数据安全，探索数字经济的合理运用。

蚂蚁链摩斯 (MORSE) : 产品能力及优势



300+ 客户实践 覆盖10+行业

20+ 领先权威 机构认证

20+ 行业标准 制定

1100+ 自主研发 专利

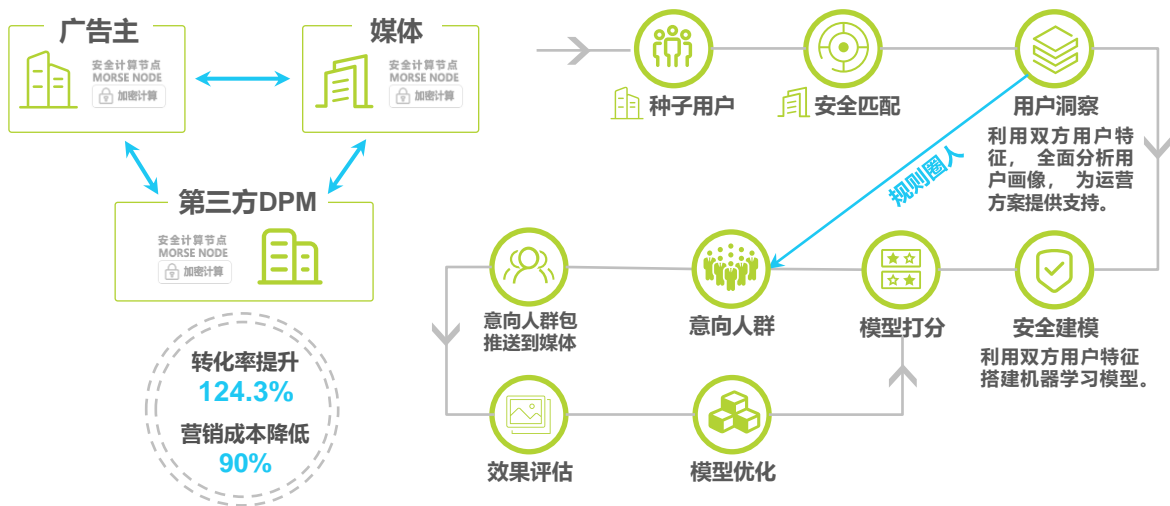
6 大产品优势

- 安全合规**
 - 全生命周期安全保障：计算前分级授权，计算中算法+规则双重保护，计算后日志审计
 - 20多项权威认证：信通院、BCTC、国密等。
 - 多安全引擎：MPC、TEE、FL
- 性能超群**
 - 在线服务支持千万级QPS：性能为同类产品5-60倍
 - 大数据分布式框架：支持10亿级数据计算
 - 低耗能：比传统MPC协议CPU占用低80%，带宽减少50%
 - 多次获得国际大奖：国际大赛性能PK中多次获得世界冠军
- 生产高可用**
 - 实践经验丰富：300+机构实践打磨，积累了大量经验
 - 可拓展的架构设计、自动化运维、数据备份与恢复等
 - 系统对接：支持与上下游系统打通，提升作业效率
- 多产品可选**
 - 软件：支持分布式和集中式
 - 软硬一体机：软件+密码卡/TEE卡/GPU加速
 - 连接器：open api系统标准化对接、Flow多引擎互联互通
- 服务完善**
 - 售前：专业团队为不同客户定制解决方案
 - 售后：交付/升级、日常运维、产品培训等，全流程专人跟进，全面保障
- 资源丰富**
 - 蚂蚁阿里系平台流量资源
 - 外部平台流量资源
 - 数据服务商资源

中国隐私计算行业的领先布局者，致力于保障数据安全的前提下促进数据流动迸发价值

从2017年以来，蚂蚁摩斯历经6年的技术打磨和大规模商业化应用实践，目前其产品已广泛应用于联合营销、政务数据开放、联合科研等领域，已落地银行、保险、电信、汽车、零售和互联网等10+行业在内的300余家机构。

蚂蚁链摩斯：精准营销场景解决方案

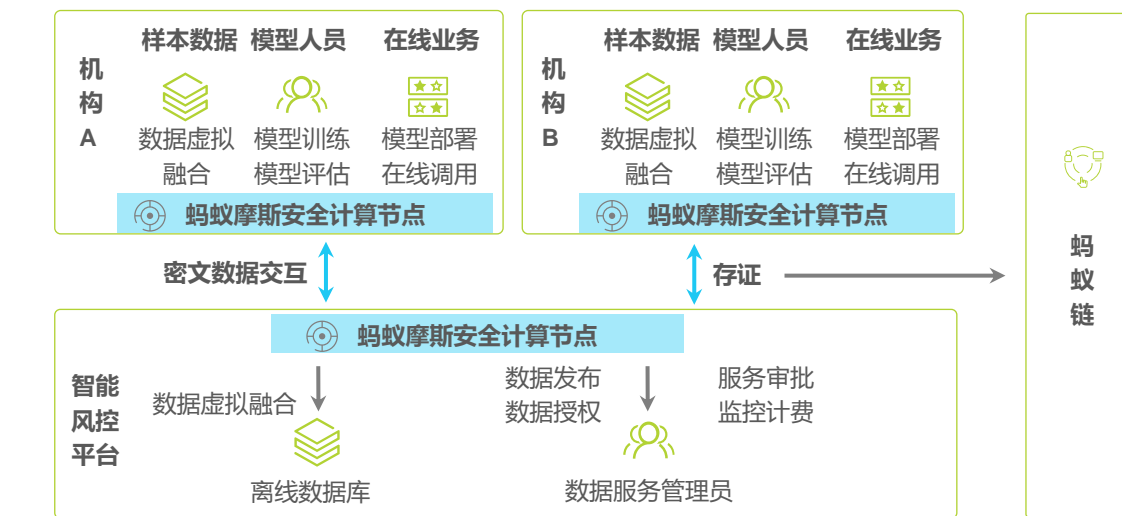


多方ID安全碰撞，保证ID安全。
多方标签数据安全联合圈人画像，精准触达，提升转化率。

多方数据安全建模，
客群自动排序，进一步人群优化。

效果数据安全统计，可进行
渠道转化分析，成本分析，轻松完成营销活动ROI测算。

蚂蚁链摩斯：政务数据安全开放场景解决方案



安全透明：政务数据“最小够用，只用不存”，“数据可用不可见”，整个数据使用链路相关方透明，保证合规性。

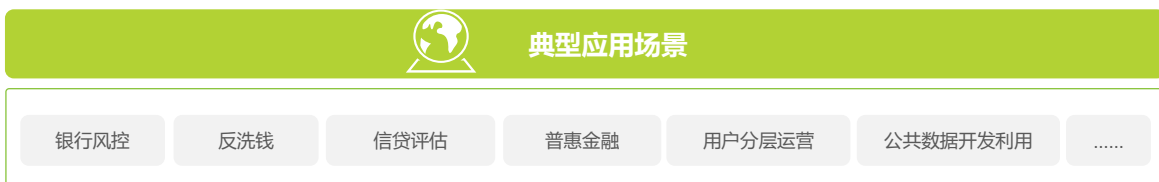
便捷高效：金融机构自主模型、策略开发，上线流程从3个月缩短至一周，根据业务需求和模型效果自主更新迭代模型。

多方数据打通：协助政府安全打通多机构数据共享互联通道，建设一站式政务数据平台。

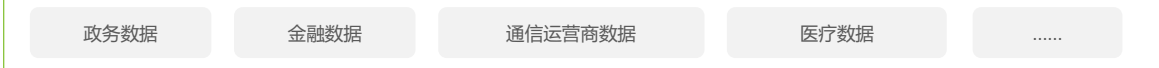
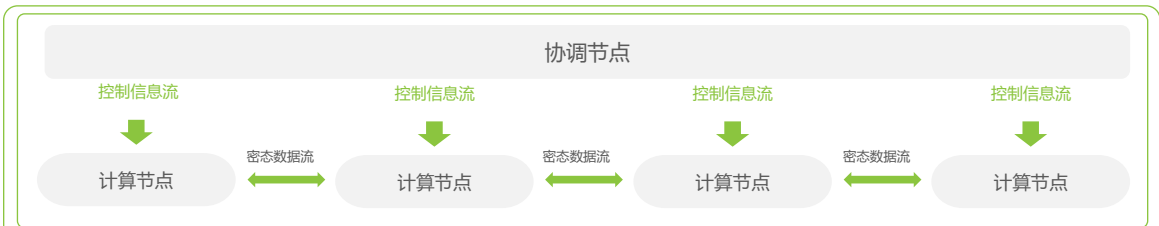
提供隐私计算技术全栈服务，促进数据要素市场建设，助力实现数字价值赋能

数牍科技以严格的隐私保护、数据安全前提下的共享和利用为目标，助力政府及企业实现安全高效的数据协作。2020年，数牍科技率先落地了行业TB级隐私计算商用标杆项目，目前数牍科技与三大运营商、银联、工商银行、北京银行等多家国央企、金融机构、头部互联网公司及其对应各行业数据协作生态企业达成合作，覆盖多个场景，致力于促进数据要素市场建设，实现多维度、多视角的数字价值赋能。

隐私计算平台Tusita架构与数牍科技优势展示



自研分布式并行框架



在数据协作过程中，实现完整的数据应用支撑。

平台运营方不触碰数据，保证数据的可用不可见。

用法用量可监管，协调节点实现对任务和数据传输的完整实时监管。

多方数据源

技术认证

- 已获“**北京市专精特新**”、“**国家高新技术企业**”
- 已通过**国家密码局、国家金融科技测评中心、工信部信通院、公安部、北京地方金融监督管理局**等多项技术权威认证，共计**34家**，位居行业前列。参与众多国际标准、国家标准，行业标准，团体标准以及地方标准的制定。
- 已发表论文数十篇。技术储备充裕，研究能力显著。

数据资源

- 与多家金融机构开展业务合作；
- 与北京、上海、深圳、福建、重庆和合肥等多地政府开展技术研究项目合作，助力实现安全高效的数据协作。

服务能力

- 通过自有的**50+多种类数据产品、80+模型**，针对政务、金融、大健康等多个领域，覆盖营销、风控、监管、产研等多个场景。

提供隐私计算技术全栈服务，促进数据要素市场建设，助力实现数字价值赋能

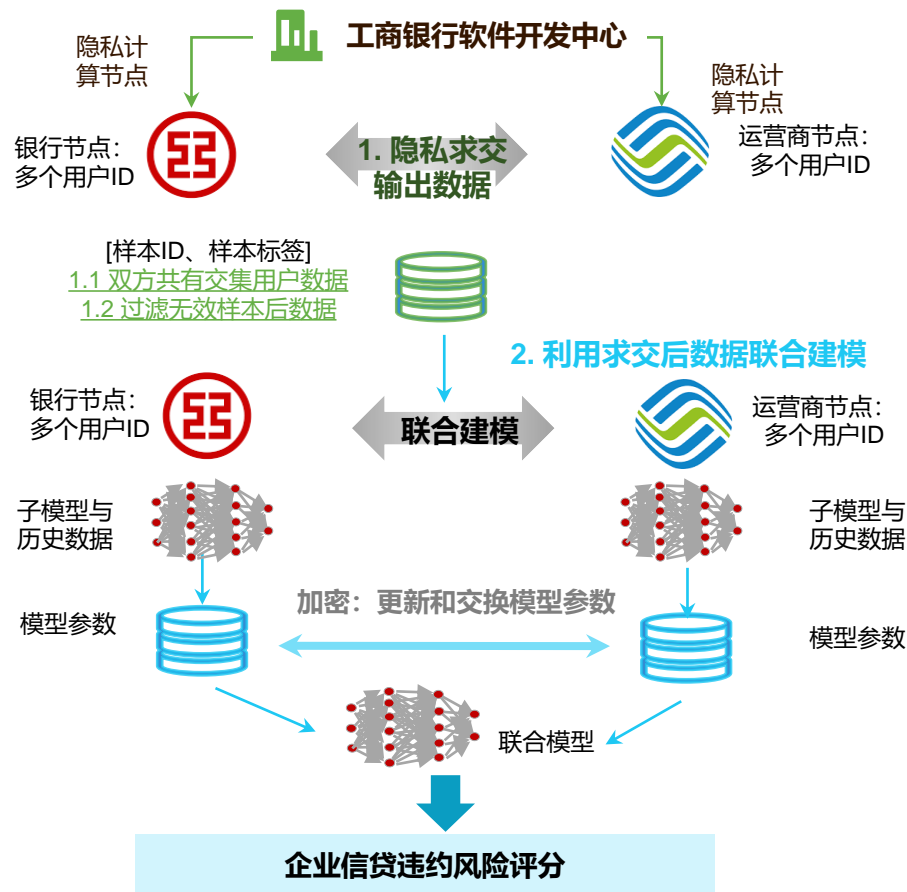
数牍科技案例：“基于联邦学习技术的普惠信贷风控服务”工商银行&数牍科技普惠金融创新实践

Part 1 项目概况

痛点：中小微企业受制于企业规模小、缺乏有效的抵押担保资产、信息不对称导致信贷风险高等因素，致使信贷需求和信贷供给错配，往往面临融资难的局面。亟需利用中小微企业的各维度信息打造更全面、更精细化的信贷风控系统，以降低不良率，提升资产质量，提高金融服务的普惠力度。而多方数据融合存有原始数据泄露与隐私泄露风险，且面临数据来源多、格式杂，数据处理及多方数据协作技术投入高难题。

Part 2 实践方案与成效

- 技术层面：**数牍科技运用联邦学习等隐私计算技术，在保证原始数据互不可见、合法合规的前提下，基于多样化的企业法人数据特征进行联合建模，丰富了企业用户画像信息，完善了贷前评估和贷后预警模型；
- 业务层面：**数牍科技帮助工商银行省级分行引入中国移动省级分公司的数据资源，为中小微企业信贷风控补充了具有地方特征的多样化信息。
- 收获成效：**1) 降低对数据分析人员专业能力的要求，普通工程师也可以通过该系统进行风控模型的训练；2) 通过融入多方数据，提高了模型的准确率；3) 规范工商银行的数据使用形式，降低了数据泄露的风险；4) 带动工商银行以创新技术应用赋能金融数据要素价值发挥的活力，打造面向小微商户的开放式融资服务新模式，客户可在线主动申请业务，由系统开展自动审批，大幅提高业务办理效率和客户体验，并进一步扩大普惠金融服务面。



多年客户服务经验，致力于成为整体性综合数字解决方案提供商

可利邦成立于2007年，专注于为客户提供综合性数字化解决方案。以客户为中心，在多元技术上积极创新发展，打造人工智能服务平台、整体IT解决方案、金融行业信息化解决方案、系统集成硬件销售和软件研发五大核心业务。现已推出自研开箱即用一站式隐私计算平台产品“筑信大数据隐私计算平台”，凭借过往所积累的140+金融客户服务经验，更好地将多技术融合，为客户提供可信、安全合规产品，进一步释放数据价值。



产品技术能力与安全性认证

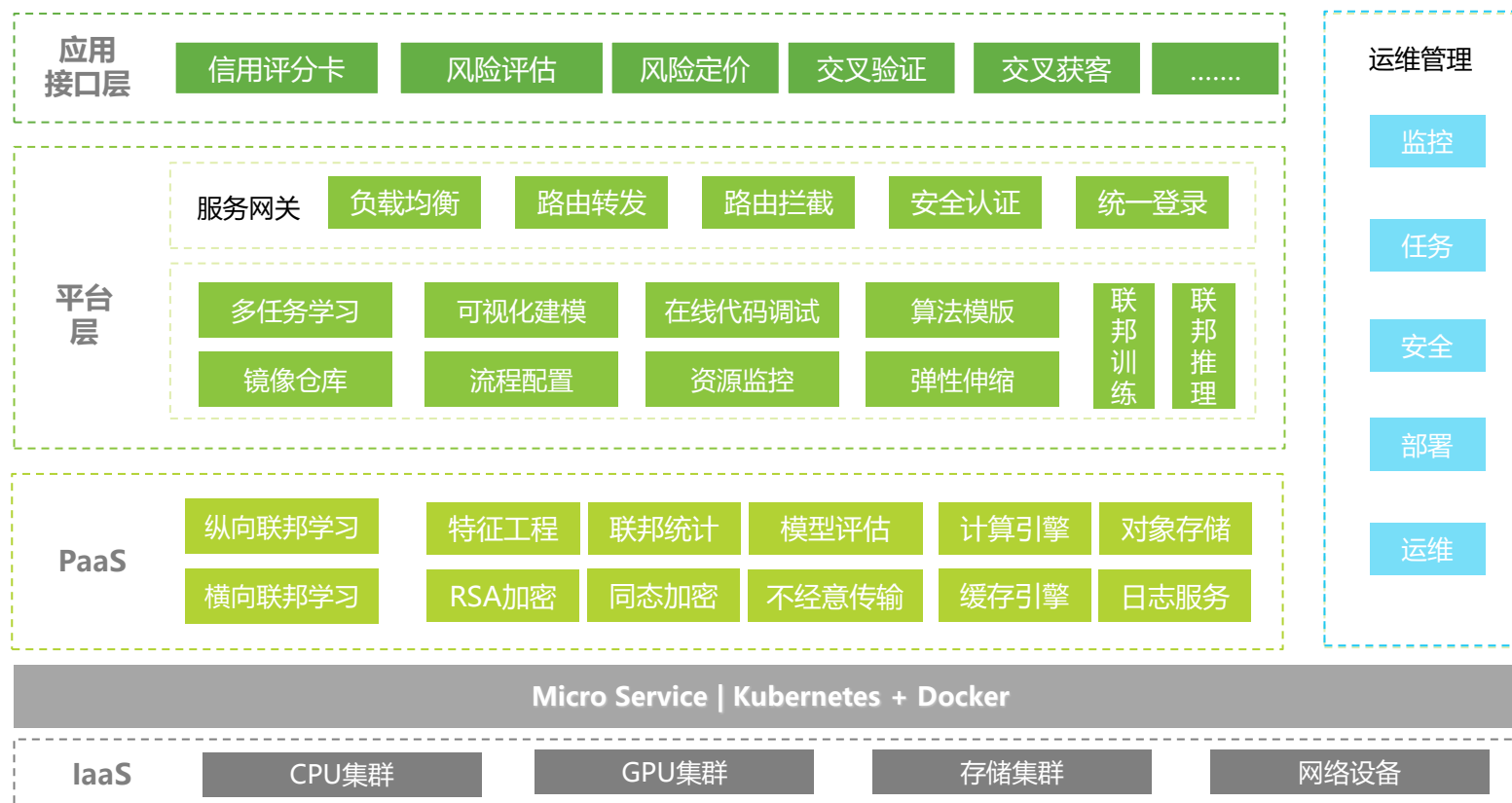
- 已通过中国信通院泰尔终端实验室、安全研究所以及中国互联网金融协会的专项能力测评，获得“联邦学习产品安全认证”与“多方安全计算基础能力”认证证书。

部分核心客户



多年客户服务经验，致力于成为领先的整体性综合数字解决方案提供商

筑信大数据隐私计算平台功能架构图与功能优势展示



易应用

- 提供简单方便的图形界面操作，支持自动模型训练，可视化，超参优化，训练进度日志查看，模型评估，模型测试
- 池化训练所需要的资源，自动任务分配到合适的算力资源上

多场景覆盖

- 支持联邦学习、联合统计、隐私求交、匿踪查询等独立模块

信创适配

- 在全部采用国产化硬件的基础上，支持国密、同态、椭圆曲线、MPC、联邦学习等安全技术，能满足银行、保险等各行业各类的数据合作需求
- 已支持飞腾3000A、海光等CPU，已通过海光CPU AMD Phenom(tm) 9550 Quad-Core Processor和飞腾CPU ARMv8 CPU测试

05 / 专家之声



宋一民

数牍科技创始人&CEO

守护数据流通安全，发挥数据要素乘数效应

“数牍科技在推动隐私计算工程落地的过程中积累了大量的实践经验。随着政策层面不断释放利好，隐私计算技术势必在更多的领域得到实际的应用，数牍科技未来会继续守护数据流通安全，蓄力发挥数据要素在各领域的乘数效应。”



李博

洞见科技合伙人、副总裁

拥抱“隐私计算+”与“数据要素×”新时代

“数据作为我国新型生产要素，激活数据要素潜能和保障数据资产安全已成为各界普遍共识，隐私计算作为国务院、发改委、工信部、中国人民银行、国家数据局等认可的数据要素安全流通关键技术，已在多个领域广泛应用。洞见科技作为国内隐私计算行业领军企业，始终致力于以独立自主、安全可控的隐私计算技术、数据要素生态和数据智能应用，为客户提供‘软件+硬件+算法+模型’的一站式全栈技术服务，以‘原始数据不出域、数据可用不可见、使用可控可计量’的密态数据计算方式赋能数据要素安全‘动’起来，让公共数据‘供得出’‘流得动’‘用得好’。”

洞见科技全速推进‘布点-连线-结网’发展战略，全力发挥隐私计算增效作用与数据要素乘数效应，已围绕‘隐私计算+政务’‘隐私计算+金融’‘隐私计算+通信’‘隐私计算+能源’‘隐私计算+工业’‘隐私计算+互联网’等与各行业头部客户落地了大量标杆示范案例，助力千行百业数据要素安全流通及应用场景提质增效。”



黄奉孝 (花名: 宝马)

蚂蚁数科金融解决方案专家

36kr、零壹财经、算力智库等

隐私计算特邀专栏作者

持续投入隐私计算应用，推动数字经济的合理运用

“信息化走到如今，不同机构之间的数字化水平以及数据合作依然很薄弱。不仅形成了大量的数据孤岛，还大大降低了机构之间协作创新的可能性。越来越多的企业和机构开始认识到，存储于不同机构的数据要流动起来、合并起来计算才有更多的价值，各个数据源之间无法互信成为亟待解决的桎梏。

蚂蚁摩斯安全计算平台提供了一种全新的安全和保护隐私的数据合作方式，能够在本地数据不泄露、原始数据不出域的前提下，高效、安全完成数据合作。

未来，蚂蚁摩斯将继续加大对隐私计算技术研发与应用的投入，充分遵守国家出台的相关政策，利用软硬一体化来保证数据安全和数据处理性能，通过实现产品、路线等特性的统一，推动隐私计算的互通，致力于在维护数字经济的合理运用方面取得更大的突破和成效。”



张磊

阿里巴巴集团数据中台技术总监

数据流通与治理负责人

数纳斯—跨域流通商业增长引擎，助力企业业务增长！

“随着数据作为第五大生产要素、数据资产入表的大步推进，高品质数据建设、标准化的数据定价、数据流通模式都需升级，方可有效释放数据价值。在全行业数字化、数实融合的浪潮中，企业对数据流通利用诉求会更加直接且广泛，除了对数据流通平台效率、合规安全提出高要求外，还会直接明确提出数据供给需要。

阿里巴巴数纳斯产品系列，在原有的数据流通产品能力之上融合多方高质量数据，提供场景化的可信数据服务。数纳斯提供了一整套产品服务，涵盖隐私计算平台、可信数据服务，并对产品能力和源代码进行无保留开源。数纳斯将持续探索新的数据合作方式，推动社会数据资源合规、安全、高效、有序流通！”



谢鲁

杭州金智塔科技有限公司

合伙人、产品总监

数据要素流通时代已来，隐私计算将成为数据价值流转的压舱石

“隐私计算技术作为数据合规流通的最优技术解，已经在金融、政务等行业得到深入应用，隐私计算平台市场规模已进入爆发期。

在未来两年，隐私计算平台会朝三个方向演进：第一，更轻量的组件部署，用户将获得安装APP般的便捷体验；第二，更多元的环境适配，安全监测系统将保护平台在内网、专网、公网交织的复杂环境零风险运行；第三，更高效的协作互通，平台将无感衔接数据要素流通体系的各类组件，成为释放数据价值的重要底座。金智塔科技自主研发的“智隐”隐私计算平台与“智通”数据要素流通平台，将助力政府、金融机构、大型企业等机构保护数据资产、释放数据势能。

隐私计算的发展将严守数据安全的初衷，在推动数据要素价值释放的同时，保持数据的持有方不变，进而保障数据持有方的资产权益不被稀释，为各机构实现数据资产化的宏远目标保驾护航！”

BUSINESS
COOPERATION
业务合作

官 网



微信公众号



新 浪 微 博



企 业 微 信



联系我们

-  400 - 026 - 2099
-  ask@iresearch.com.cn
-  www.idigital.com.cn
www.iresearch.com.cn

LEGAL STATEMENT

法律声明

版权声明

本报告为艾瑞数智旗下品牌艾瑞咨询制作，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