

iResearch Vendor

厂商竞争力象限

(2021Q1 – 2022Q3 , 隐私计算+金融 , 中国市场)

©2022.10 iResearch Inc.





厂商研究

- ❑ 在“iResearch Vendor：厂商竞争力象限（2021Q1 – 2022Q3，隐私计算+金融，中国）”的评估中，共计有10家厂商入围象限。象限定义了综合领导者、实践竞争者、持续竞争者、发展竞争者四类厂商，每一类厂商均有其值得被关注的优势能力。
- ❑ 基于市场调研及分析师研究，象限围绕“阶段性市场分化、厂商格局演变、厂商能力演变、客户关注的厂商能力”对金融市场的隐私计算供应商竞争现状及市场格局走势展开了解读。
- ❑ 艾瑞可信科技团队在行业中首次定义了TDaaS（Trusted Data（intelligence）as a Service，可信数据（智能）即服务）理念，这是一项值得被数据提供者、数据应用者及服务商共同关注的数据安全可信流通的能力范式。分析师给出了TDaaS的三层关键能力，并对TDaaS进行了概述性解读。



商用实践

- ❑ 研究团队围绕对金融机构用户、技术服务商的调研，对隐私计算在金融领域的整体商用实践情况进行了分析。包含隐私计算平台建设、平台选型研究、隐私计算应用场景实践、商业模式、技术实践扩展等方面的研究内容。
- ❑ 针对隐私计算平台建设类项目，报告基于客户类型、技术方案、市场特点与项目价格进行了统计与分析。围绕隐私计算平台选型象限，对10余个要点技术指标进行了分析，列举了值得关注的金融隐私计算平台能力。
- ❑ 应用场景实践方面，报告围绕基于隐私计算的数据源链接能力、金融业务理解和经验、数据调用的合规性、流量接入等多项要点能力展开了分析。
- ❑ 报告围绕“iResearch：隐私计算商用实践周期洞察矩阵（平台建设+场景实践的研究，中国金融市场）”从技术平台建设、应用场景实践两个角度洞察了全行业周期的发展走势。

iResearch Vendor

厂商竞争力象限

(2021Q1 – 2022Q3 , 隐私计算+金融 , 中国)

独立性、客观性声明



iResearch Vendor：厂商竞争力象限（2021Q1 – 2022Q3，隐私计算+金融，中国）的研究因不受任何组织或个人的委托而保持高度的独立性。评估过程将在分析师研究、金融机构用户反馈、厂商调研等多种形式与方法下展开执行，以确保研究及评估结果的客观性。

© iResearch Vendor：厂商竞争力象限（2021Q1 – 2022Q3，隐私计算+金融，中国）



金融机构用户发起的隐私计算项目中，服务商的两大方面能力被客户所关注

一方面是，隐私计算平台建设、跨平台互联互通建设等产品技术能力；另一方面是，基于隐私计算的数据链接调用、场景建模、流量接入等可信数据运营能力。因此，这两个方向将被纳入厂商评估的关键维度。



受技术多样性等因素的影响，客户难以仅通过POC对供应商的技术能力全貌展开完全精准的判断；部分金融机构会考虑采纳多个供应商

约25%的金融机构客户提出¹：真实业务环境的实践成效同POC及形式化验证中的表现存在差异（受技术多样性、产品特殊性、计算数据量、业务环境等因素的影响，会导致其差异性的出现。此外，市场调研发现，极少数技术供应商在POC中存在技术舞弊的现象，也是造成差异出现的原因之一）。

另外，部分用户反馈，未来的技术平台建设与应用场景实践中，如具备必要性条件，可考虑纳入不止一个服务商来丰富或强化综合能力。



厂商的当下服务能力与持续服务能力同样重要

65%+的金融机构客户提出²：除了关注厂商是否能够帮助机构在现阶段良好地实现隐私计算平台建设和可信数据运营及应用场景实践外，还需要关注厂商的持续服务能力以保证技术ROI的持续向好。

注释：1&2、受访的金融机构数量为90家，接受访谈的领导者共计151位。受访者涵盖金融机构中的IT/技术、金融业务团队的领导者与应用者。
来源：研究团队市场调研、艾瑞咨询研究院自主研究及绘制。

厂商竞争力象限（隐私计算+金融）

iResearch Vendor：厂商竞争力象限 （2021Q1 – 2022Q3，隐私计算+金融，中国）

象限说明

Qualification Statement for Quadrant

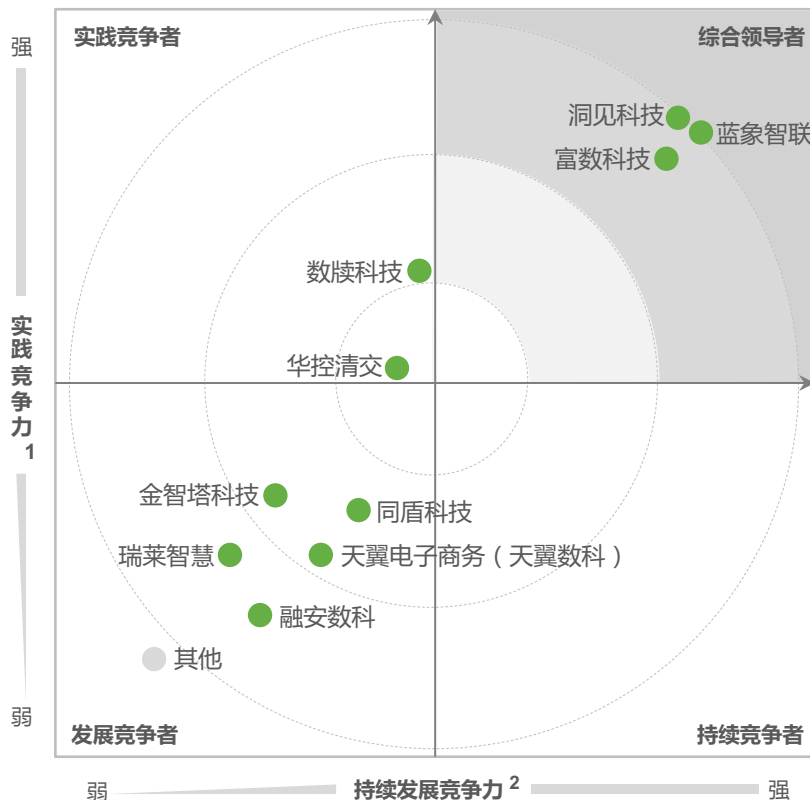
本次评估范畴涵盖25家隐私计算服务商(艾瑞可信科技团队提名+金融机构提名)，基于评估标准，共计10家厂商入围象限。

象限中每一个厂商用例的位置，反映的是产品与技术、场景应用与可信数据运营、商用实践在实践竞争力及持续发展竞争力上的综合评估。而**入围者均具备不同方面的差异化优势。比如某一入围者很有可能处于非综合领导者象限，但其在某项技术能力上，拥有全行业领先的水平。**

因此不建议金融机构用户仅根据厂商在象限所处的位置作为单一的供应商参考信息，金融用户应该结合具体需求及厂商专长，匹配最佳合作者。

有关象限咨询，请点击“联系分析师”进行交流

 [联系分析师](#)



© 2022.10 iResearch Inc.

注释：1、实践竞争力围绕厂商在“产品技术、场景应用&可信数据运营、商用实践经验”三个方面的现阶段综合能力展开考察，是对厂商目前实践能力的综合评估；2、持续发展竞争力围绕厂商在“产品技术、场景应用&可信数据运营、商用实践经验”三个方面的战略及其将战略付诸实践的能力展开评估，一方面考察厂商战略的合理性与领先性，另一方面结合厂商的现有能力及资源，考察厂商是否能将其设定的战略付诸于实践，是对厂商持续发展能力的综合评估。

来源：艾瑞咨询研究院自主研究及绘制。

评估方式及指标体系

评估方式

- 评估指标的设置重点参考了金融客户（覆盖技术及业务团队）在隐私计算商用实践中所关注的厂商能力。
- 象限评估围绕金融机构（客户侧）的意见征询、面向厂商的调研等多种形式展开。研究团队面向已经开展隐私计算实践的金融客户，征询了其正在合作或者POC中接触过的厂商在产品技术等多项能力上的评估意见。同时面向厂商展开问卷、访谈或产品演示等形式的调研。为了保证评估的客观性，我们不会只参考单一调研渠道的反馈信息。

iResearch Vendor：厂商竞争力象限(2021Q1 – 2022Q3，隐私计算+金融，中国)主要评估指标

实践竞争力					持续发展竞争力				
指标		重要性	指标		重要性	指标		重要性	
产品技术	安全性	高	场景应用 & 可信数据运营	数据源质量及稀缺性	高	产品技术	产品与技术能力发展策略	高	
	性能	高		数据源种类覆盖度	高		跨平台互联互通发展策略	高	
	功能与技术覆盖度	高		金融业务理解能力	高	场景应用 & 可信数据运营	可信数据运营理解及发展策略	高	
	跨平台互联互通	高		金融场景模型数量	中		数据源生态发展策略	高	
	信创适配能力	高		数据源的合规性审查	高		应用场景实践扩展策略	高	
	金融场景的适配能力	高		流量对接能力	中		数据源合规保障策略	高	
	计算的精确性	高		商业合作模式设定	低		流量引入策略	中	
	合规与审计	高	商用经验	客户数量与类型	高	商业拓展	销售与营销策略	高	
	无可信第三方的实现方式	中		平台建设类项目考察	高		技术及应用场景的商用扩展策略	高	
	服务能力	低		场景实践类项目考察	高		商业模式理解与发展策略	中	
其他	低	客户评价		高	每一项策略的评估中，会根据厂商的现有资源与能力来评估厂商能否将其予以实现，进而评估厂商的持续发展竞争力。				

来源：艾瑞咨询研究院自主研究及绘制。

象限的四类厂商描述及纳入说明



综合领导者

- 综合领导者在实践竞争力及持续发展竞争力中均拥有卓越的表现。
- 在金融隐私计算市场，综合领导者在客户数量上拥有领先的市占率，值得客户信赖的产品技术能力，在多数竞争性磋商中，可以获得优于其他厂商的成绩。在深刻理解金融应用场景的同时，可为客户提供可信数据链接调用及场景建模等服务。综合领导者往往基于隐私计算构建了符合TDaaS能力方向的发展战略，并有能力将战略付诸于实践，进而在未来的商用实践中保持竞争优势。



实践竞争者

- 实践竞争者在实践竞争力方面拥有卓越的表现。
- 在金融隐私计算市场，实践竞争者在实践竞争力评估中取得了相对于持续竞争者、发展竞争者更高的综合得分。实践竞争者可以在“产品技术、场景应用及可信数据运营、商用实践”的多项能力中均具备行业领先优势，亦或是在其中某一项能力上拥有领先于其他厂商的卓越影响力而提升了实践竞争力的总体评估得分。



持续竞争者

- 持续竞争者在持续竞争力方面拥有卓越的表现。
- 在金融隐私计算市场，持续竞争者基于对市场需求及技术发展的敏锐、深度的判断，在厂商的产品技术能力、场景应用及可信数据运营、商用实践策略及服务方式上设定了明确、符合市场需求及行业发展方向战略。更加重要的是，这些厂商有能力实现其所设定的战略，进而在未来的商用实践中赢得竞争优势。



发展竞争者

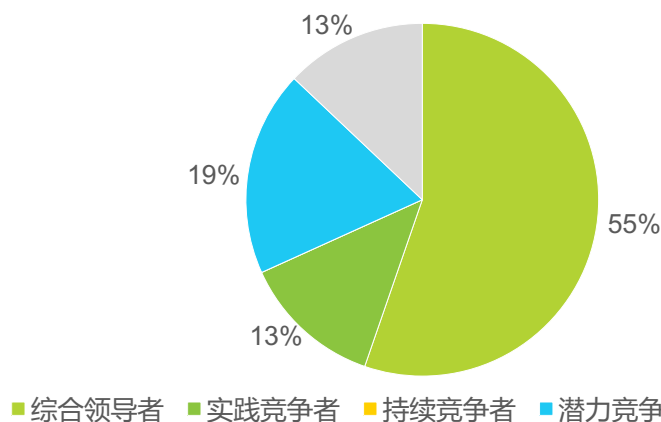
- 发展竞争者在某个（或某些）细分能力上，表现出了值得关注的优势。
- 在金融隐私计算市场，发展竞争者因具备某个细分方向的能力而值得被客户关注，这些细分能力可以是下述的一种或多种：专注于某一个细分领域的利基市场、拥有可以证明能力的客户案例、在某一项技术能力上存在特色优势、可基于隐私计算链接某类同金融业务高度匹配的价值数据源、对金融业务或某类金融场景拥有深度的理解能力、拥有潜在竞争力的市场后入局者。

要点解读1：阶段性市场分化

金融行业的隐私计算商用实践市场出现阶段性分化，在客户数量上，综合领导者厂商拥有55%的市场占有率

金融领域作为隐私计算商用实践的先锋市场，目前呈现出平台建设客单价低、客户数量多的特点。银行、保险为代表的金融机构数字化程度领先，对外部的多方数据应用需求强烈，构筑了巨大的基于隐私计算的可信数据运营及场景应用的市场空间。加之以银行为代表的金融机构目前对隐私计算项目的采购相比于其他行业的热度更高，因此各类隐私计算厂商纷纷入局金融市场。本次研究周期（2021Q1-2022Q3）内，金融市场的隐私计算服务商竞争格局已由最初的“百家争鸣”逐渐进入阶段性的强者愈强市场格局。在金融机构客户数量上，象限中综合领导者厂商的市占率已达55%，表现出行业阶段性的市场分化。因目前处于市场初期阶段，后续的市场环境、竞争格局、市场需求等因素或将让行业再次“大浪淘沙”，除自始至终持续保持领先优势的综合领导者外，或将出现新的竞争者发展成为综合领导者。

厂商竞争力象限（2021Q1 – 2022Q3，隐私计算+金融，中国）各类厂商的市场占有率及解读



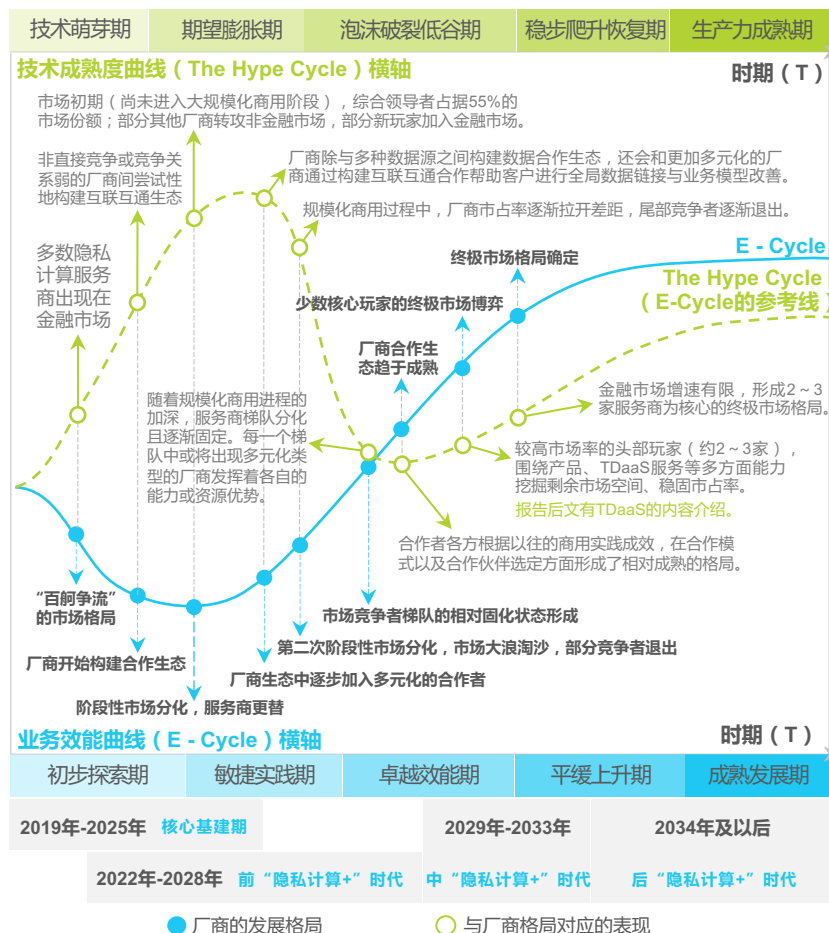
- 目前隐私计算的商用实践处于市场初期阶段，从技术的宏观发展周期来看，目前的市场格局主要是阶段性表现。当下的综合领导者是否能够一直保持领先优势取决于其产品成熟度的提升、可信数据运营&应用场景实践能力的发展、金融业务Know-How的沉淀积累等方面是否能够一直保持领先状态。
- 本次象限中的持续竞争者未有厂商入围。而实践竞争者可以通过在满足市场需求的战略方向上，通过强化产品成熟度、可信数据生态、金融场景理解等其中的一项或者多项能力，让战略付诸于实践，进而成为综合领导者。

注释：1、市场占有率的统计口径为客户数量，而非营收规模；2、以厂商正式展开合作的客户数量为统计范畴，非商业化的战略合作、处于POC阶段的项目均不包含其中；3、统计的项目类型包含隐私计算平台建设类、互联互通平台建设、在隐私计算平台建设基础上所提供的可信数据运营及应用场景实践类项目，对于仅在其他技术产品中融入隐私计算能力的项目不在统计范畴内。

来源：研究团队市场调研、艾瑞咨询研究院自主研究及绘制。

要点解读2：厂商格局演变

iResearch：隐私计算商用实践周期洞察矩阵 (厂商格局演变的研究，中国金融市场)



Insight ① 围绕技术能力的厂商格局阶段性演变

- 本次研究周期 (2021Q1 -2022Q3) 内，我们发现有部分曾经聚焦于金融市场的隐私计算厂商切换了市场战略方向而主攻其他市场机会，大致分为两类：1) 厂商在竞争性磋商类项目中难以取得优势、同时也难以通过产品服务能力及商务影响力在单一来源类项目中获得客户成功。2) 厂商产品在金融市场暂未拥有较大需求，如算力加速产品、一体机等。对于算力加速产品，目前在少数的商用实践案例中出现了实时营销等算力加速需求场景，未来的潜在机会有待在深度的场景实践中进行挖掘。
- 在部分厂商转攻其他领域的同时，金融市场也出现了部分后入局者，包含新生隐私计算厂商、发现金融市场机会而转攻金融市场的厂商、拥有金融市场经验的FinTech公司等类型的服务商。



Insight ② 围绕跨平台互联互通的厂商竞合关系

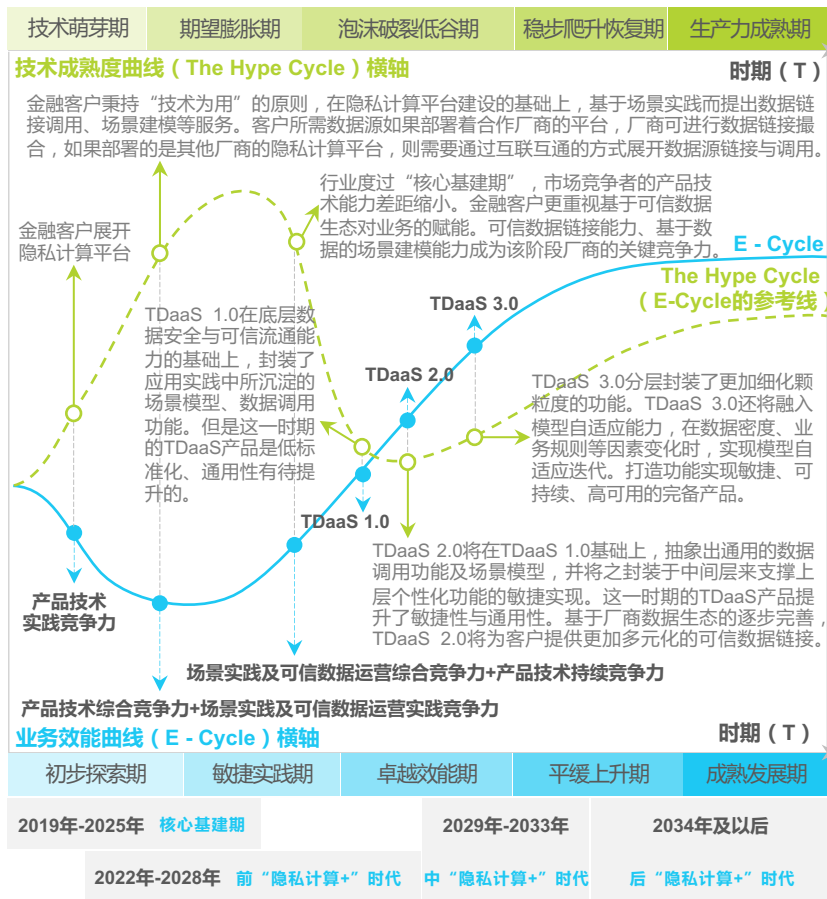
- 厂商为金融客户提供数据链接调用服务时，数据源可分为两类情况：1) 部署了本厂商平台的数据源、2) 部署了其他厂商平台的数据源。第2类情况需要实现不同隐私计算平台间的互联互通。
- **竞合关系的概述：**竞争关系强的厂商之间难以主动推进跨平台互联互通合作，而竞争关系弱或通过合作可实现商业利益最大化的厂商之间有动力去推动跨平台互联互通合作。
 - **客户需求的推动：**基于金融客户需求推动的跨平台互联互通项目将逐渐增多。若此类项目实现的是算法协议层与计算原语层的互联互通，将对不同数据生态之间的融合起到促进作用。
 - 在单考虑市场机制所形成的强者愈强的竞争格局下，在未来或将出现以少数厂商为核心的面向金融业务的可信数据生态网络。

关于市场格局现状及未来格局趋势的判断，可见“矩阵”所阐述的研究内容。期望获取“矩阵”更加详细的内容解读，可[联系分析师进行咨询](#)。

注释：E - Cycle (业务效能曲线) 的用例阐述不同技术应用阶段的市场格局；The Hype Cycle (技术成熟度曲线) 仅为参考线，阐述不同技术成熟度阶段下，与市场格局对应的表现。
来源：艾瑞咨询研究院自主研究及绘制。

要点解读3：厂商能力演变（1/2）

iResearch：隐私计算商用实践周期洞察矩阵 （厂商能力演变的研究，中国金融市场）



Insight 1 厂商能力演变概述

- **整体概述：**厂商能力演变取决于不同时期的客户需求，且不同时期的需求或将会出现新的市场竞争者。目前因处于“核心基建期”与前“隐私计算+”时代的叠加期，客户除考察厂商产品的安全性、性能等技术指标外，在客户的场景实践中，部分厂商也将提供可信数据链接及场景建模服务。在行业度过“核心基建期”后，对金融业务理解深刻、具备可信数据运营能力的厂商在“隐私计算+”的需求中将体现出更多的优势。
- **不同厂商的能力演变方向取决于其对金融机构客户服务方向的战略设定。**象限评估中发现，一类厂商聚焦于“平台建设+场景实践及可信数据运营”的体系化可信数据流通与应用能力建设；另一类厂商只聚焦于将技术直接或间接输出给金融机构客户，成为技术输出者的角色定位。



Insight 2 关于TDaaS

- **TDaaS所需的技术能力不止于隐私计算，并非所有隐私计算厂商都将走向TDaaS：**TDaaS是多元化的技术堆栈，完备的TDaaS产品需要融合隐私保护计算、区块链、安全防御、自适应AI等多元化技术。TDaaS在构建与客户需求精准匹配的数据源生态的基础上，封装了基于隐私计算的数据调用功能、模型训练算法、场景模型知识库（TDaaS能力架构见下文）。对于只聚焦于技术输出者角色定位的厂商不具备构建TDaaS能力的充要条件，聚焦于“平台建设+场景运营”双重能力建设的竞争者中也仅有少数厂商可以实现TDaaS 3.0的能力。
- **金融TDaaS潜力者：**象限中的三家综合领导者厂商在产品技术能力、场景应用与可信数据运营的实践现状及战略方向，贴合艾瑞定义的TDaaS能力方向，有望在未来构建出完备TDaaS产品。

期望获取“矩阵”更加详细的内容解读，可[联系分析师](#)进行咨询。

注释：E - Cycle（业务效能曲线）的用例阐述不同技术应用阶段的厂商能力；The Hype Cycle（技术成熟度曲线）仅为参考线，阐述不同技术成熟度阶段下，与厂商能力对应的表现。
来源：艾瑞咨询研究院自主研究及绘制。

要点解读3：厂商能力演变（2/2）

TDaaS是一项值得被数据提供者、数据应用者及服务商共同关注的数据安全可信流通的能力范式

TDaaS (Trusted Data (intelligence) as a Service) , 可信数据 (智能) 即服务。是由艾瑞咨询可信科技研究团队定义的一项“满足业务敏捷响应、高互通、高可用、可持续”的可信数据流通产品形式与服务理念。是一项值得隐私计算厂商与行业用户重点关注的重要战略技术趋势。2028年，60%以上的金融机构将通过金融级TDaaS获取安全、合规的数据调用及数据智能服务。

TDaaS的三层关键能力



TDaaS概述

- TDaaS是数据安全可信流通方向的一项重要战略技术趋势，其不仅被定义为多项功能集合而成的产品，也可以被定义为一种服务。在TDaaS 1.0产品出现之前，一切与TDaaS理念趋同的基于隐私计算的可信数据流通能力均可被定义为TDaaS服务，而这些服务及实践经验的积累，成为打造TDaaS产品的基石。
- 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。
- TDaaS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。

期望获得关于“TDaaS”更加详细的解读，可[联系分析师](#)进行咨询。

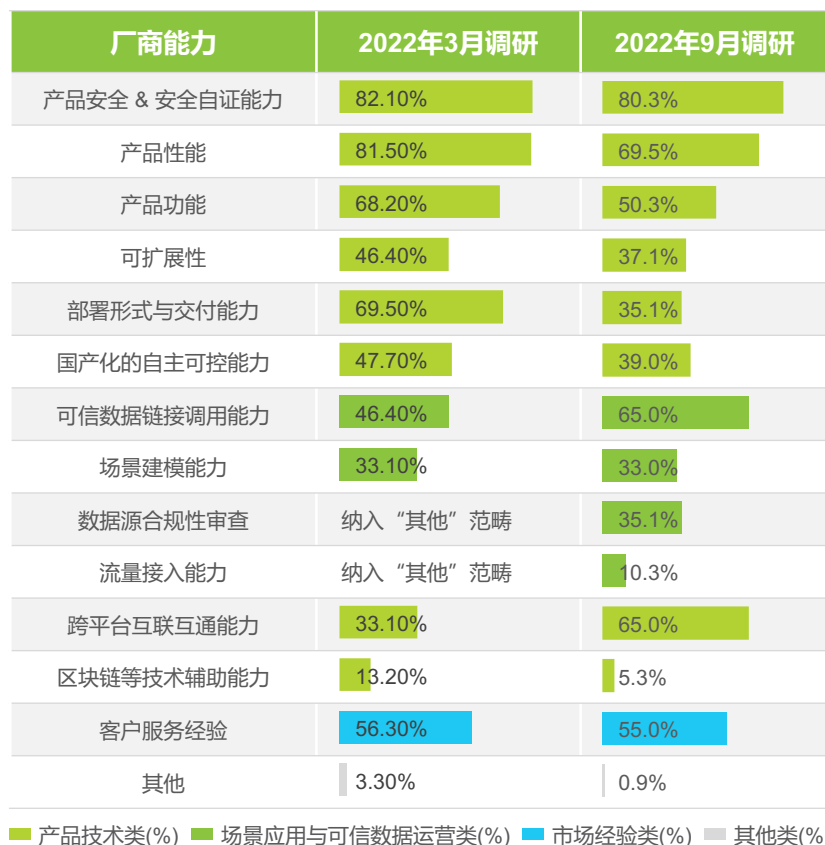
© 2022.10 iResearch Inc.

来源：艾瑞咨询研究院自主研究及绘制。

要点解读4：客户关注的厂商能力

除产品技术能力外，场景应用与可信数据运营能力同受关注

中国金融机构客户关注的隐私计算厂商能力



注释：1、N=151，受访者涵盖金融机构中的IT与科技部、金融业务团队的领导者与应用者；2、研究团队首先征集了相关技术应用者主要关注的能力方向，分析师对此进行归纳整理，并设计了选项；3、在调研过程中，每一位受访者最多选择六个选项。
来源：金融机构调研、艾瑞咨询研究院自主研究及绘制。

约 **80.3%** 的受访者（拥有实践经验的金融用户）关注：

隐私计算厂商在平衡性能的基础上，如何提供值得客户信任的安全证明或安全防御机制。

基于艾瑞咨询所提出的“最优安全设计+有效安全证明+实时安全防御”原则，本次象限评估中发现已有厂商率先实现了实时安全防御能力。

约 **65.0%** 的受访者（拥有实践经验的金融用户）提出：

目前机构已有固定的数据合作方，我们会将隐私计算厂商是否可以基于隐私保护计算的方式链接到这些数据源作为一项能力进行考察。此外，如果厂商可以基于隐私保护的方式链接到更多与业务需求匹配的高价值、稀缺性数据源将成为加分项。

如果金融机构客户所需要的数据源部署了其他隐私计算平台，将可能和金融机构的平台之间产生计算孤岛，所以部分客户会考察厂商是否有在其所关注的数据源端部署隐私计算节点。

约 **65.0%** 的受访者（拥有实践经验的金融用户）意识到：

建设跨平台互联互通生态有助于多样化数据的可信链接，有利于业务模型改善，是可信数据生态网络建设中不可或缺的部分。

我们发现，部分金融客户在可信数据应用场景的实践中，会基于明确的数据源链接需求而推动跨平台互联互通建设，还有部分机构通过公开招标采购磋商的方式选择合作厂商进行互联互通平台建设。

注释：N=151，受访者涵盖金融机构中的IT与科技部、金融业务团队的领导者与应用者。
来源：金融机构调研、艾瑞咨询研究院自主研究及绘制。

入围者能力优势分析（1/5）

D



洞见科技

洞见科技是象限中的综合领导者，孵化于中诚信。得益于中诚信的金融背景、数据服务及信用科技经验，洞见科技在金融业务理解、可信数据运营、核心技术研发方面具有多年基础能力沉淀。

实践竞争力

- 洞见科技服务了来自银行、保险、证券、资管等多种类型的金融机构，在金融客户数量上拥有着领先的市占率。根据研究团队的金融用户调研，洞见科技获得行业用户认可的主要原因在于：高质量的隐私计算平台建设及服务能力、通过多样化的数据资源链接能力帮助客户构建可信数据智能生态、基于对金融业务的理解及建模经验高效满足用户的场景实践需求。商业模式方面，除软件营收、数据分润之外，洞见科技还基于营销类场景对业务分润的商业模式展开了探索。
- 洞见科技不仅在金融风控与营销场景拥有丰富的商用实践，还拓展了债券指数编制、资产扫描等对算法及场景理解有着较高要求的资管类场景。洞见科技构建了包含三大运营商、互联网、征信、政务、电力等多领域的数据生态，同时依托中诚信的数据生态圈，可以在客户服务中提供更多的数据渠道保障。

- 洞见隐私计算平台（InsightOne）内置了丰富的适配金融场景的算法插件、场景模型。InsightOne在安全证明方面，除了基于流量监控的常规方式外，还成为业内率先将安全防御能力融入产品的厂商。在互联互通方面，除了制定标准、厂商间的实践外，洞见科技还在银行、支付等金融客户的商用实践中，通过跨平台互联互通帮助客户进行全局数据链接与业务模型改善。

持续发展竞争力

- 洞见科技践行“密态数据智能流通网络生态”战略，在帮助数据提供方和数据应用方进行节点部署的基础上进一步开展业务建模，实现了由点到面的阶段性成果。研究团队认为洞见科技通过多家国有银行、股份制银行、城商行、保险机构等头部标杆金融客户的服务，可提升产品成熟度及业务Know-How积累，具备“基础设施+场景运营”的全流程持续客户服务优势。

F



富数科技

富数科技是象限中的综合领导者。其核心团队来自华为、阿里巴巴、CapitalOne和IBM。评估中发现富数科技在隐私计算平台建设、场景应用创新方面拥有可被证明能力的项目实践。

注释：象限中四类厂商从如下角度展开优势分析：（1）综合领导者围绕实践竞争力、持续发展竞争力进行介绍。（2）实践竞争者围绕实践竞争力优势展开介绍。（3）持续竞争者围绕持续发展竞争力优势展开介绍。（4）发展竞争者围绕其值得被关注的某类优势能力展开介绍。因此四类厂商优势分析的内容篇幅存在不同。

来源：艾瑞咨询研究院自主研究及绘制。

入围者能力优势分析 (2/5)

实践竞争力

- 富数科技目前的金融客户数量行业领先，且在各类竞争性磋商中多次表现出优于竞品厂商的成绩。其客户覆盖国有大行、股份制银行等头部金融机构，涵盖隐私计算平台建设、互联互通平台建设、监管沙箱、场景建模及数据运营等多类项目。研究团队面向金融机构用户的调研中反馈，富数科技除了数据生态建设能力得到认可外，也表现出了较强的场景应用创新力。
- 富贵数科技构建了涵盖运营商、银联、数交所、航旅等类型的数据源生态，并可以为用户提供数据合规性证明。富数科技在存款、贷款、代销、表外等金融业务中储备了丰富的场景模型。
- 富数科技的隐私计算产品Avatar在功能、算法、模型能力上拥有较强的金融场景适配性，高度覆盖了金融隐私计算平台中的隐私保护计算能力、原理架构安全能力、平台管理能力。此外，富数科技还围绕商用实践客户、合作伙伴构建了隐私计算跨平台互联互通生态。

持续发展竞争力

- 基于富数科技在技术竞争性磋商、金融业务理解、场景实践经验及成效来看，在金融市场表现出良好的持续发展竞争力。而在富数科技的规划中，还将进一步丰富数据源生态、互联互通合作生态，这也让其可信数据运营的持续发展竞争力得到提升。

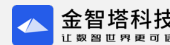
H —



华控清交

华控清交是象限中的实践竞争者。因华控清交目前处于战略拓展发展期，报告暂不展开能力分析 & 信息披露。

J —



金智塔科技

金智塔科技是象限中的发展竞争者。由浙江大学人工智能研究所和浙江大学金融科技研究院联合发起。评估中发现，金智塔科技值得关注的差异化优势在于，其是面向中小银行市场的利基玩家：

- 金智塔科技拥有浙江地区城商行、农商行等客户基础。围绕客户的企业贷款、个人贷款、智能获客、智能风控、小微（科创）企业信用评估、住房贷款等业务场景提供基于隐私计算的数据流通服务。
- 金智塔科技可以提供更加匹配中小银行客户特点的产品及服务。基于中小银行的商用实践积累，更加精准地提供与客户业务相匹配的数据源，并展开场景应用。

注释：象限中四类厂商从如下角度展开优势分析：（1）综合领导者围绕实践竞争力、持续发展竞争力进行介绍。（2）实践竞争者围绕实践竞争力优势展开介绍。（3）持续竞争者围绕持续发展竞争力优势展开介绍。（4）发展竞争者围绕其值得被关注的某类优势能力展开介绍。因此四类厂商优势分析的内容篇幅存在不同。

来源：艾瑞咨询研究院自主研究及绘制。

入围者能力优势分析 (3/5)

L —

蓝象智联

蓝象智联

蓝象智联是象限中的综合领导者。公司团队主要来自阿里巴巴、蚂蚁金服、国有大行等企业机构。得益于团队背景，蓝象智联拥有较强的金融基因，在面向金融客户的服务中具备其他厂商难以替代的优势。

实践竞争力

- 蓝象智联的金融客户覆盖国有大行、股份制银行、城商行、保险、证券等机构，客户数量上拥有领先的市场份额。研究团队面向客户的调研中发现，蓝象智联获得客户成功的核心竞争力在于其对金融业务场景的深刻理解与创新能力、可以为不同业务精准匹配数据源、基于创新的产品架构支持敏捷的业务响应。
- 蓝象智联构建了涵盖政务、支付、运营商、出行、供应链等17类精准匹配金融业务需求的数据源生态。在营销、风控、反欺诈等多场景具有全链路金融场景模型能力，在此类场景的理解上具备领先于竞品的优势。蓝象智联可以通过头部互联网企业、流量工具包为客户提供流量对接实现业务转化，在专家团队丰富的金融Know-How基础上，为金融机构客户提供可信数据运营端到端的方案及业务转化落地实践。

- 蓝象智联GAIA系列产品拥有创新的产品架构及强大的组件库，客户可以通过组装式功能启动应用实践，最大程度方便用户的使用。GAIA可以同鲲鹏、飞腾、麒麟等CPU与操作系统实现信创适配，融合了与金融场景适配的算法插件、场景模型。GAIA将互联互通纳入产品的原生能力，以产品化方案实现一次接入、全网互联的架构。

持续发展竞争力

- 蓝象智联践行“隐私计算+”战略，为客户提供基于数据、场景理解、算法模型、流量、合规的全域可信数据网络服务。蓝象智联在头部及代表性客户的服务中打磨产品，提升产品成熟度，凭借精准深入的场景理解及可信数据运营创新能力，在客户的持续服务中表现出领先的竞争力。

R —

融安数科
ronganbigtech

融安数科

融安数科是象限中的发展竞争者，成立于2021年。其母公司神州融安2019年开始投入隐私计算的技术研究及产品开发。本次评估

注释：象限中四类厂商从如下角度展开优势分析：（1）综合领导者围绕实践竞争力、持续发展竞争力进行介绍。（2）实践竞争者围绕实践竞争力优势展开介绍。（3）持续竞争者围绕持续发展竞争力优势展开介绍。（4）发展竞争者围绕其值得被关注的某类优势能力展开介绍。因此四类厂商优势分析的内容篇幅存在不同。

来源：艾瑞咨询研究院自主研究及绘制。

入围者能力优势分析（4/5）

中，融安数科表现出的值得关注的优势之处在于：

- 融安数科创新性地提出隐私度量理念，在多方安全计算的目标函数或算子联合计算前，数据提供方使用少部分真实数据或伪数据对目标函数或算子的性质以及使用方的输入参数进行测试检验，度量数据隐私保护程度并给出隐私保护评分。
- 融安数科正式成立不到一年的时间内，在银行及保险领域快速取得客户成功。得益于母公司的金融科技背景，使其在金融客户服务及后续的市场拓展具备经验优势。

R —

RealAI
瑞莱智慧

瑞莱智慧

瑞莱智慧是象限中的发展竞争者，是一家人工智能服务商，提供算法安全、隐私计算等技术服务，其在隐私计算方面值得关注的的能力在于：

- 在银行领域，拥有基于隐私计算的场景建模商用实践经验。
- 其隐私计算平台RealSecure搭载联邦AI编译器，支持机器学习算法到联邦机器学习算法的自动转换。充分利用基于格的全同态加密算法中的SIMD技术，对多条数据进行同时处理，性能比半同态加密算法更优。提供“协议模型及安全性假设、技术

实现原理、数据抓包监测、运算日志打印审计”的全方位的安全评估验证体系。

S —

数牍
sudo

数牍科技

数牍科技是象限中的实践竞争者。其创始团队来自于Facebook（现Meta）、Google、字节跳动等科技公司及国内大型金融机构。

实践竞争力

- 数牍科技是国内较早以系统性综合工程视角提供数据隐私计算服务的厂商。数牍科技隐私计算产品自研分布式计算框架，以资源动态横向扩展的方式提升处理能力和处理效率，实现“计算无中心，控制有中心”系统架构，使得计算节点进行数据本地化分布式计算、控制节点监管节点任务和数据使用。产品实现了算子插拔能力，提供组装式算法搭建，提升建模效率。产品支持数据中台、AI中台、区块链等平台的高效集成。
- 数牍科技构建了涵盖通信运营商、互联网企业、征信机构、政府机构等多方位的数据源生态，基于数牍专家团队的场景Know-How，结合场景需求提供精准数据源对接服务。

注释：象限中四类厂商从如下角度展开优势分析：（1）综合领导者围绕实践竞争力、持续发展竞争力进行介绍。（2）实践竞争者围绕实践竞争力优势展开介绍。（3）持续竞争者围绕持续发展竞争力优势展开介绍。（4）发展竞争者围绕其值得被关注的某类优势能力展开介绍。因此四类厂商优势分析的内容篇幅存在不同。

来源：艾瑞咨询研究院自主研究及绘制。

入围者能力优势分析（5/5）

- 数读科技已为多家银行、保险等金融机构提供隐私计算平台建设，围绕反洗钱、反欺诈、存量用户分层运营、营销获客、普惠信贷风控等业务场景展开场景建模或数据源对接。数读科技还和FinTech公司等企业构建合作生态进一步打开金融市场。

T —



同盾科技

同盾科技是象限中的发展竞争者，是一家专注于决策智能的人工智能公司。其值得关注的能力在于：

- 同盾科技拥有数个可被证明能力的商用实践项目（如招商银行隐私计算平台互联互通项目等）。
- 战略上，同盾科技将探索基于隐私计算的SaaS服务，为金融客户提供可信数据智能产品。其原生业务围绕金融风控场景积累了丰富的数据智能实践经验且拥有大量的金融客户基础，对金融业务的数据分析与决策有着深刻理解。同盾科技基于隐私计算构建了打通覆盖设备、司法、公安、物流、运营商、地图、支付等类型的数据源生态，拥有贷前信用评估、金融用户分群、贷前反欺诈、贷中预警、贷后监控等可信业务模型。

T —



天翼电子商务（天翼数科）

天翼电子商务（天翼数科）是象限中的发展竞争者。其值得关注的能力在于：

- 天翼电子商务（天翼数科）较早地布局隐私计算技术研发，评估发现其综合技术能力较优、产品高度覆盖了同金融业务高度适配的算法、场景模型、平台管理等能力。
- 天翼电子商务（天翼数科）拥有在银行领域可被证明能力的商用实践经验，项目类型包括隐私计算平台建设、场景建模（例如其在中国农业银行隐私计算平台建设公开招标的竞争性磋商中脱颖而出）。< 注：该项目客户对服务商营收及资质方面拥有限制条件，因此竞争性磋商的竞争者不包含绝大部分处于创业期的原生隐私计算厂商 >

注释：象限中四类厂商从如下角度展开优势分析：（1）综合领导者围绕实践竞争力、持续发展竞争力进行介绍。（2）实践竞争者围绕实践竞争力优势展开介绍。（3）持续竞争者围绕持续发展竞争力优势展开介绍。（4）发展竞争者围绕其值得被关注的某类优势能力展开介绍。因此四类厂商优势分析的内容篇幅存在不同。

来源：艾瑞咨询研究院自主研究及绘制。

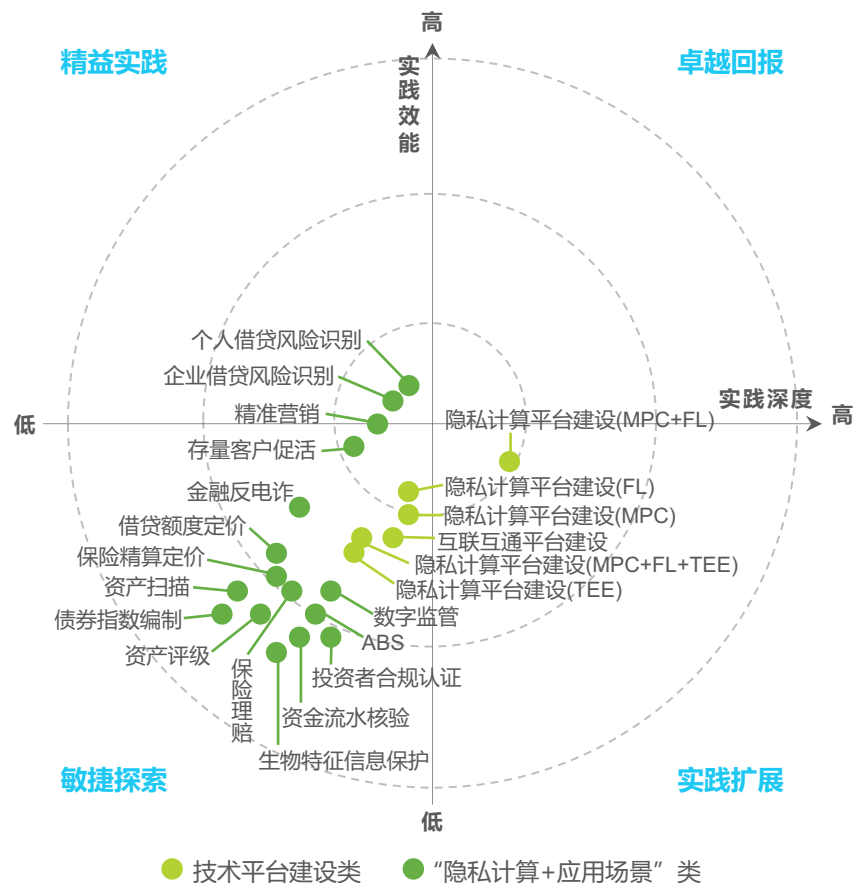
附

商用实践市场概述

(2021Q1 – 2022Q3 , 隐私计算+金融 , 中国)

总起：商用实践概述

iResearch：隐私计算商用实践洞察象限 (2021Q1 – 2022Q3，金融，中国)



绘制时间：2022年9月

来源：艾瑞咨询研究院自主研究及绘制。



Insight 1 技术实践概述 (2021Q1 – 2022Q3)

- **隐私计算平台建设**：国有大行、股份制银行等数字化领先的金融机构往往对可信数据能力建设拥有自上而下的推动方式，通过竞争性磋商引入技术供应商开展隐私计算平台建设。部分中小金融机构也在业务侧的需求推动下，以场景+可信数据的需求推动隐私计算平台建设实践。目前，金融客户在选择服务商时，除了评估安全性、性能等关键技术能力外，同样将可信数据链接调用、场景建模等纳入关注的能力方向。
- **客户侧在逐渐推动隐私计算跨平台互联互通的建设**：目前招商银行、银联为代表的机构开展了互联互通平台建设的项目，随着金融客户对数据合作者多样性需求的提升，此类项目数量也将不断增多。
- **隐私计算+应用场景的实践**：对比《艾瑞：2022年中国隐私计算行业研究报告》中的发布结果，营销类、风控类场景用例已迈入精益实践象限，证明这类场景的大部分实践案例在金融机构用户的业务中获得了相应实践成效，但目前主要以局部业务实践为主，实践深度有待扩展。**其余场景的突破依然需要1~3年的探索驱动。**



Insight 2 商用市场概述 (2022)

- 2022年H1，受到疫情等因素的影响，部分已中标项目无法实施、新项目招标开展缓慢，商用实践进程放缓。进入2022年Q3，金融隐私计算商用市场开始回温，机构招标数量渐渐增多，且出现千万级金融类项目(科研类机构采购)。
- 排除不可控因素的影响，隐私计算的金融类项目采购将在2022年底或2023年表现出理性的市场增量。

注释：2021年的商用实践情况在《艾瑞：2022年中国隐私计算行业研究报告》中已详细分析，此报告不再重复阐述。

象限解读说明

@ iResearch：隐私计算商用实践洞察象限(2021Q1 -2022Q3，金融，中国)

象限的每一个用例，均是基于大量的案例实证与数理实证，以**定量评估**或者**分级评估**的方式展开统计与计算，进而确定用例在象限中的位置。对此，研究团队面向行业用户、技术服务商展开了大量市场调研。**象限解读，即是对调研发现与研究成果的阐述，以及对支撑象限研究成果的实证进行解读。**

围绕象限解读，将阐述商用实践的现状、趋势及建议。

读者欲了解更加详细的研究成果，可点击“联系分析师”进行交流。

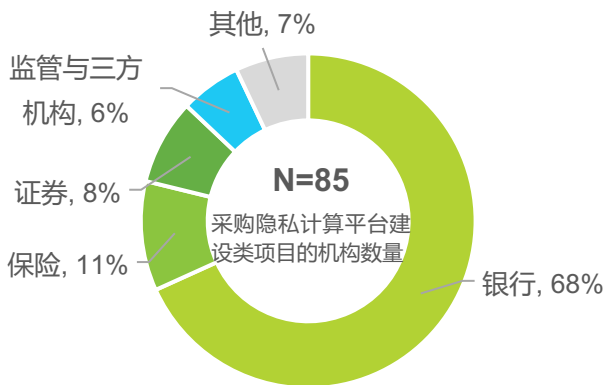
 [联系分析师](#)

技术平台建设：客户类型与技术方案

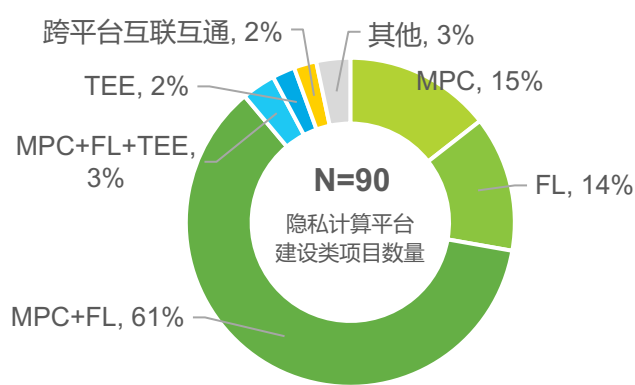
银行成为隐私计算平台建设的领先实践者，保险行业被视为高潜力市场；客户选择MPC+FL技术方案的集中度最高

在法律与相关政策的推动下，各类金融机构都在积极开展数据安全与合规能力的建设，隐私计算被视为一项重要的数据可信流通技术方案而被广泛采纳。艾瑞近期的市场调研发现，银行成为隐私计算平台建设的领先实践者，除了国有大行、股份制银行的率先实践外，部分城商行也展开了相应技术投入。其余类型的金融机构也根据自身需求而展开了隐私计算平台建设。其中，保险行业的定价、核保、理赔、风控与营销等主要业务均对多方数据有着较高程度的依赖，被视为继银行之外的重要目标市场。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，除了隐私计算平台建设类的项目外，先后涌现了互联互通平台（跨平台互联互通）建设类项目。

2021年Q1–2022年Q3中国金融行业隐私计算平台建设类项目的采购机构分布



2021年Q1–2022年Q3中国金融行业隐私计算平台建设类项目的技术方案分布



注释：1、左组数据统计的是金融机构数量，右组数据统计的是项目数量，存在同一机构分部门或分批次等情况采购了不同的项目，所以两组数据的总样本量N不同；2、部分项目会分拆成诸如“包件1、包件2、包件3、……”的形式，且会选择不同供应商，此类情况算作一个项目进行统计；3、在“iResearch：隐私计算商用实践洞察象限(2021Q1–2022Q3，金融，中国)”研究中，分析师面向技术服务商、金融机构客户展开了双向调研与交叉验证，以最大程度覆盖行业项目数量与具体项目信息（公开招标、非公开招标项目皆包含其中）。来源：艾瑞咨询研究院自主研究及绘制。

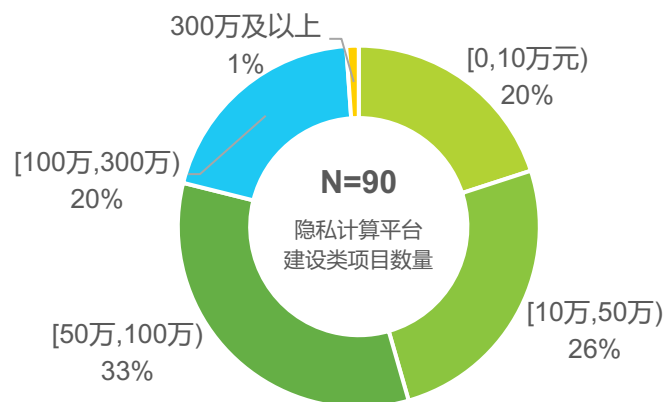
技术平台建设：市场特点与项目价格

金融机构的隐私计算平台建设市场的特点是客户数量多、客单价有限、存在扩展需求；目前市场存在低价竞争现象

市场特点：隐私计算平台建设类项目通常以节点为单位进行收费。目前金融机构发起的项目中，多为初期阶段的平台建设，预算多见于百万上下（具体因项目差异而预算不同）。随着业务应用范围的逐渐深入，金融机构客户将扩展节点数量而增加预算投入。由此可见，隐私计算在金融市场的特点是：客户数量多、客单价偏低、客户存在扩展需求。

低价竞争现象：以银行、保险为代表的金融机构是隐私计算平台建设商用实践的主力军，且拥有场景实践与可信数据运营的巨大的外延市场，因此成为隐私计算厂商的“兵家必成之地”。为了获得更多代表性客户或是出于其他目的，目前部分厂商利用低价竞争的方式来获取客户，行业不断涌现成交金额在10万元以下的项目。低价竞争拥有“联动效应”进而将会让更多厂商被迫降低竞标价格。此外，存在客户因项目的过度低价竞争而需重新展开招标的情况，影响了项目实施计划。

2021年Q1 – 2022年Q3中国金融行业隐私计算平台建设类项目的价格分布及要点解读



□ **关于价格分布：**2021Q1-2022Q3，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，部分项目设置了更高的预算金额，主要以项目需求不同而形成差异，调研发现部分项目的实际采购金额远低于预算金额。10万元以下项目，非公开招标市场的数量高于公开招标市场。

□ **很多客户对过度低价竞争持有担忧或不赞同的态度：**根据近期的一次市场调研，约65%的行业用户表示：机构核心关注的是项目最终交付效果，担心过度的低价竞争会影响项目交付质量。且部分项目如服务商无法交付，将按照合同价格的数倍进行违约赔付，过度的低价竞争也降低了服务商的违约成本。

注释：1、研究团队在厂商调研的基础上，重点面向金融机构客户展开了深度调研与交叉验证，以获取相关项目的具体金额或金额分布区间（公开招标、非公开招标项目皆包含其中）；2、部分项目会分拆成诸如“包件1、包件2、包件3、……”的形式，且会选择不同供应商，此类情况算作一个项目统计；3、数据只统计了金融机构的采购，非金融机构的采购不包含其中。此外，报告前文提及的千万级金融类项目(科研类机构采购)于10月份确定招标成果，不在上图统计时间范畴内。

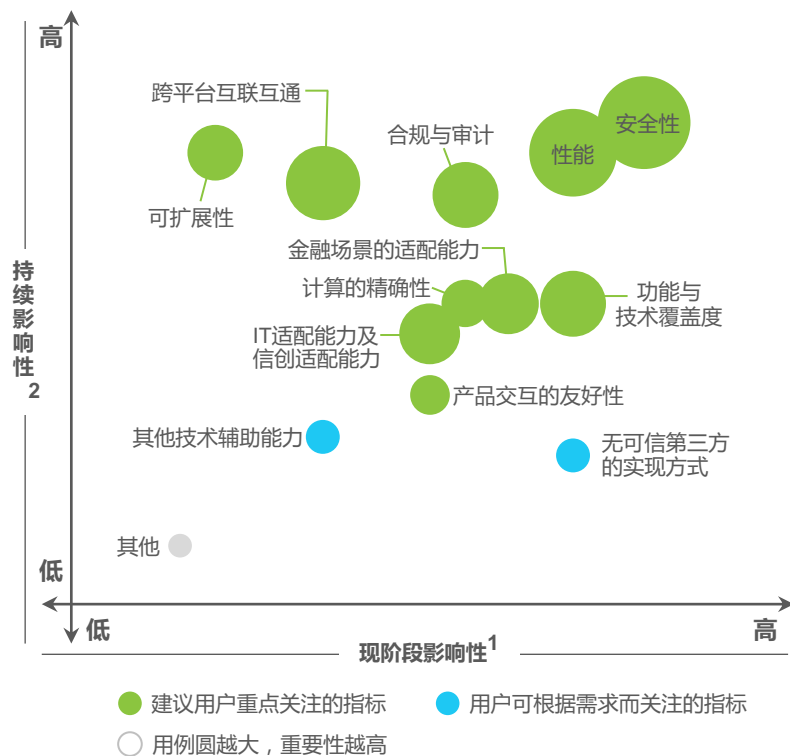
来源：艾瑞咨询研究院自主研究及绘制。

金融隐私计算平台选型研究

隐私计算平台指标及选型要点概述（金融领域）

隐私计算平台选型象限（金融领域）

绘制时间：2022年10月



1、现阶段影响性：某一指标对现阶段技术实践成效的影响；
2、持续影响性：某一指标对后续平台扩展与技术实践成效的影响。



选型要点解读 & 领先实践者的关键反馈

金融客户进行隐私计算平台建设的核心诉求是为实现数据的可信流通能力建设，以致于从战略上构建可信数据生态圈。下述从要点能力展开解读。

- **安全性**：80%以上的金融客户期望厂商在提供安全证明的基础上，能够提供安全防御的策略及能力，对此，艾瑞咨询提出了“最优安全设计+有效安全证明+实时安全防御”原则。在年初的调研中，市场内的服务商主要是通过流量监控、攻防形式化验证、三方评测等方式进行安全证明。本次调研发现已有厂商增加了主动性防御、动态对抗博弈等能力，补齐了实时安全防御的空白。
- **性能**：隐私计算在金融领域的业务实践已经出现了实时精准营销等对性能要求较高的场景，在不影响安全性的前提下，可以通过硬件加速、算法优化、并行计算、通信优化等方式来优化隐私保护计算的性能。
- **跨平台互联互通**：跨平台互联互通建设的重要性随着用户场景实践的深入及多样化的可信数据链接需求而逐渐显现。目前部分用户正在推动算法协议层与计算原语层的互联互通。
- **其他选型要点**：在金融机构自主可控的信创架构下，隐私计算平台的信创适配能力成为基础要求。在应用实践中，产品功能、内置算法、场景模型若能同金融业务的场景需求形成较高的适配性，可以帮助用户降低业务实践成本，提升业务实践效能。此外，部分业务对联邦学习的计算精确性存在要求。合规性方面，监管及相关技术应用规范要求算法所使用的数据、模型、模型参数与计算结果均需可追溯审计，因此合规与审计能力成为必选项。

除上述要点内容的解读外，读者欲对平台选型的相关研究内容进行更加详细的了解，可以[联系分析师](#)进行交流。

值得关注的金融隐私计算平台能力

近期调研¹发现，尚未开启隐私计算平台建设的用户中，约70%的用户关注隐私计算平台包含哪些技术能力。下述为一个金融隐私计算平台可以包含的技术能力，但非所有厂商都会完全实现。用户可在“隐私计算平台选型象限（金融领域）”的基础上，根据需求选择性地将下述能力纳入关注范畴（下述所列仅为值得关注而非全部能力）。

6项隐私保护计算能力

隐私匹配查询能力

- ☐ 离线隐私求交/匹配
- ☐ 实时匿名匹配
- ☐ 实时隐私信息检索
- ☐ 离线隐私信息检索

基础多方运算能力

- ☐ 加减乘除算法
- ☐ 比较算法
- ☐ 基础统计运算

联合特征工程能力

- ☐ 数据清洗
- ☐ 特征转换
- ☐ 特征筛选
- ☐ 分箱

多方联合建模能力

- 有监督学习
 - ☐ 线性回归模型训练
 - ☐ 逻辑回归模型训练
 - ☐ XGBoost模型训练
 - ☐ DNN模型训练
- 无监督学习
 - ☐ K-Means模型训练
- 其他
 - ☐ 迁移学习

模型评估能力

多方联合预测能力

- 有监督学习
 - ☐ 线性回归模型离散/实时预测
 - ☐ 逻辑回归模型离散/实时预测
 - ☐ XGBoost模型离散/实时预测
 - ☐ DNN模型离散/实时预测
- 无监督学习
 - ☐ K-Means模型离散/实时预测
- 其他
 - ☐ 迁移学习离散/实时预测

5+N项金融场景应用能力

- ☐ 金融风控场景
- ☐ 客户画像场景
- ☐ 多方黑名单查询场景
- ☐ 反洗钱场景
- ☐ 精准营销场景
- ☐ 其他

5项原理架构安全能力

- ☐ 匿名匹配/查询安全性论证
- ☐ 基础多方运算安全性论证
- ☐ 多方联合建模安全性论证
- ☐ 多方联合预测安全性论证
- ☐ 计算架构安全性论证

10项平台管理能力

- ☐ 用户管理功能
- ☐ 节点管理功能
- ☐ 任务管理功能
- ☐ 数据库支持能力
- ☐ 接口安全防护能力
- ☐ 网络容错能力
- ☐ 系统日志审计功能
- ☐ 系统监控告警功能
- ☐ 数据管理功能
- ☐ 超两方的多方计算能力

注释：1、包含银行、保险、证券在内的共计75家金融机构，共计103位科技部门的相关负责人接受了调研。
来源：行业专家调研、艾瑞咨询研究院自主研究及绘制。

基于隐私计算的应用场景实践（1/3）

隐私计算+金融的场景实践中：可信数据链接能力、金融业务Know-How成为厂商的两大关键竞争力

金融机构客户围绕隐私计算的应用场景实践概述：部分银行等金融机构正式启动自上而下的隐私计算平台建设前，通常会选取特定应用场景展开尝试性的实践来验证技术的可用性及可靠性，此阶段处于客户对一项新技术的考察期，多数客户会采用非公开招标竞争性磋商的方式选择供应商，甚至部分项目会以单一来源形式指定供应商。在结束考察期而展开正式的平台建设及应用场景实践中，总行级/机构总部级的平台建设会通过公开招标竞争性磋商的方式选定供应商，且若存在必要需求，不排除选择多个供应商或在后续的实践中新增/替换供应商的可能。客户选择厂商进行平台建设时通常也需要为后续的应用场景实践进行考虑。首先需要考虑的是基于合作厂商所建设的平台是否可以链接机构日常所使用的数据源，对于未能覆盖的数据源，需要通过跨平台互联互通等方式予以满足数据调用需求。未来，应用场景实践的需求往往会分散在不同的业务团队，场景建模类项目也可能选择多样化的供应商。目前极少数营销类项目中，供应商会为客户提供可信数据源链接+场景建模+流量接入的综合解决方案，此类项目主要采用联合分润的合作模式。此外，基于隐私计算的应用场景实践中，除了对数据计算的安全保障外，还需要保证数据源的合规性。

基于隐私计算的金融应用场景实践中所涉及的非技术类关键能力



可信数据链接能力

Section 01

- ❑ 可以帮助金融机构用户在隐私计算+金融的应用场景中提供多样性高可用的数据链接调用，而非单一化可用度低的数据源。可以帮助金融机构链接稀缺性及同金融业务匹配的数据源。
- ❑ 除厂商本身的数据源生态外，可以通过跨平台互联互通的能力帮助用户链接数据源。



数据源合规性审查

Section 02

- ❑ 通过数据提供方出具合规性证明等方式来保证数据调用的合规性。



流量接入能力

Section 03

- ❑ 在营销等场景中，帮助用户进行流量接入。



金融业务理解及经验

Section 04

- ❑ 基于对金融业务场景的理解，可以为客户明确指出业务应该匹配的数据源，提升模型训练效果。
- ❑ 基于金融业务建模经验及对金融业务的理解，通过精准的参数调整降低建模成本。

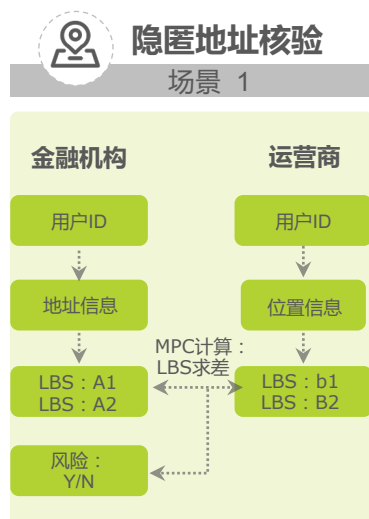
基于隐私计算的应用场景实践（2/3）

典型应用场景：金融反电诈

金融反电诈近来受到了金融及监管机构的重点关注，银行陆续建立了企业级的反诈体系，行业多方也在尝试成立数据风控联盟组织的形式加强金融反诈能力，而隐私计算在促进数据可信流通的同时也在帮助金融行业构建反欺诈能力体系。

基于隐私计算的金融反电诈应用实践

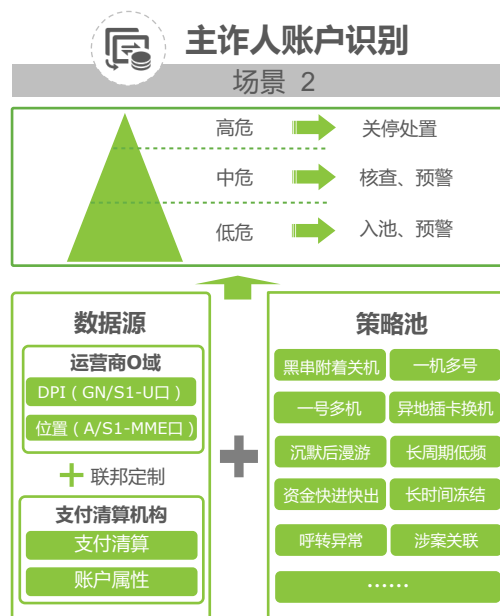
以蓝象智联的金融反电诈场景为例，围绕隐匿地址核验、主诈人账户识别、实时风控数据联盟三类场景及应用展开介绍。



场景
某城商行消费贷反欺诈，通过地址核验，识别黑灰产用户。

效果
叠加多头信息，业务拦截率降低至1.3%，被拦截用户风险对比大盘人群Lift6~8倍。预计运行后减少2700万资损/年。

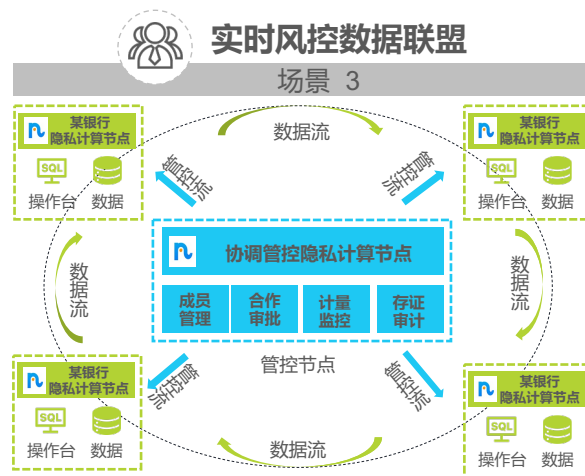
来源：艾瑞咨询研究院自主研究及绘制。



场景及效果

2020年至今，某省受害的61人中通过该模型验证可识别34人，识别率55.7%。目前该模型正在逐步进入生产应用。

注：因数据原因，优先考虑该省移动的诈骗人。



该联盟基于蓝象智联的隐私计算平台与金融同业机构和数据合作方实现安全联合建模，建立智能化的反诈识别模型、多头借贷风险监控模型、信用风险预审批模型等，对申请人的违法违规行为、资金水平、关联方信息等进行全方位分析，进一步丰富大数据预警规则和预警指标体系，在一定程度上减少被诈风险损失。

实践效果

截至2022年7月，联盟已经汇集**100**多家金融机构，每天的查询笔数超百万笔。

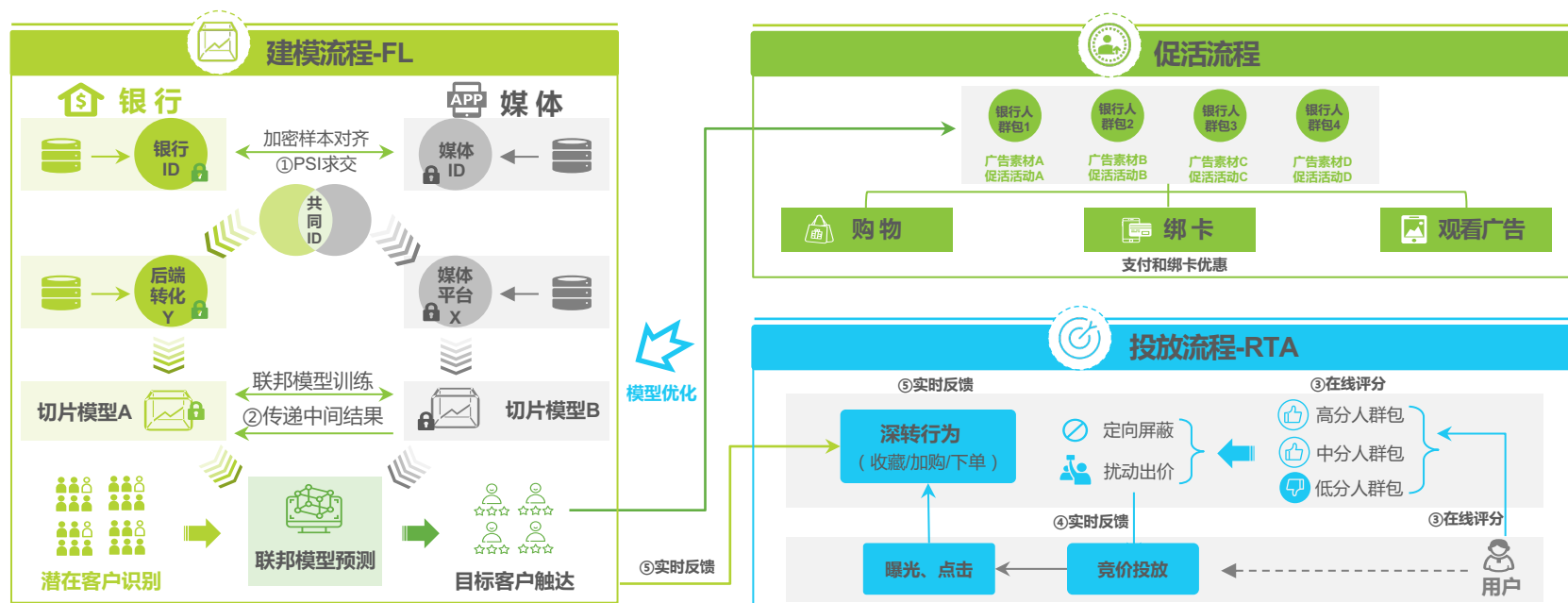
基于隐私计算的应用场景实践（3/3）

典型应用场景：营销投放（拉新及促活）

金融营销是隐私计算的关键商用实践场景之一，也是厂商竞争较为集中的方向。营销场景需要基于精准数据源及算法展开模型训练，不同技术供应商的业务场景理解及建模经验将直接影响业务效果。

基于隐私计算的金融营销投放（拉新及促活）应用实践

以洞见科技服务的某金融机构客户为例，在营销投放拉新及促活场景下，通过隐私计算完成了“联邦学习+RTA”场景的落地。



项目背景

某金融机构面临新客投放效率低和存客激活效率差的问题，希望在保证数据安全的前提下，通过隐私计算优化转化率。

来源：艾瑞咨询研究院自主研究及绘制。

解决方案及实践效果

- 基于隐私计算的联邦学习技术，结合RTA技术，实现新客实时精准出价，金融机构的授信通过率提升了12%，单客授信成本降低6%。模型KS值达0.34。
- 基于隐私求交技术，金融机构的存客支付绑卡率提升30%，转化成本降低23%。

除产品技术销售的商业模式外，数据分润，业务分润的商业模式均处于探索期

关于隐私计算商业模式的分析，我们在《艾瑞：2022年中国隐私计算行业研究报告》中已有详尽阐述，此处不再过多赘述。面对金融隐私计算市场，目前正值“核心基建期”的发展阶段，产品技术市场处于快速增长阶段。越来越多金融机构在通过竞争性磋商的方式选择合适的技术厂商开展隐私计算平台建设，现阶段该类项目金额有限且市场存在低价竞争（前文有具体分析），厂商难以通过此类项目获得可观营收。部分厂商还会基于隐私计算能力为客户提供数据源链接、场景建模等可信数据运营及应用场景实践相关服务。这类服务将衍生数据分润和业务分润的商业模式，目前这两类模式处于探索阶段，商业模式尚未完全成熟，市场没有统一的分润比例，且业务分润目前主要适合于营销等类型的业务场景。

隐私计算在金融市场的主要商业模式分析



产品技术销售及服务

Section 01

- ❑ 产品技术销售商业模式明确，客户数量多、但普遍客单价偏低、市场存在价格战，厂商竞争激烈。
- ❑ 客户完成第一阶段的建设后，后续节点扩展在不更换供应商的前提下，可以形成复购增量。在排除不可控因素的影响下，因此未来3~5年技术市场将保持稳定增长。以银行为例，预计至2025年，国有商业银行、股份制银行、40%~50%的城市商业银行均将完成隐私计算的平台建设。



数据分润

Section 02

- ❑ 数据分润商业模式目前尚不成熟，分润比例行业暂无统一标准。而诸如运营商等数据源，也会独立建设可信数据开放流通平台，即使数据源和金融客户间部署着不同的隐私计算平台，客户可以通过跨平台互联互通的方式链接数据源端的数据。因此并非所有数据源调用均会通过隐私计算厂商。
- ❑ 无论数据分润的市场前景如何，建设数据生态必会有助于提升隐私计算厂商的综合客户服务能力。



业务分润

Section 03

- ❑ 业务分润商业模式目前仅极少数厂商基于营销场景展开了探索，该类商业模式对厂商数据源链接、业务建模、流量引入、数据源合规处理、场景理解的综合能力要求较高。
- ❑ 不同金融客户对此合作模式的接受程度不一。业务分润比例难以形成高度的行业统一，往往会基于具体业务类型、投入成本、业务难易程度等因素来进行双方磋商。

要点说明：1、不选择业务分润合作模式的情况下，场景建模将按照项目制收费，且场景建模按照项目制收费是较为常见的合作模式，此处作以说明，不再对场景建模类合作模式展开描述。2、我们仅结合目前市场中所表现出的商业模式展开了分析，未来TDaaS产品的出现及合作模式属于趋势性判断，此处暂不展开讨论。

来源：艾瑞咨询研究院自主研究及绘制。

组织管理角度的实践扩展建议

未来，随着隐私计算应用实践的加深，一些金融机构的不同部门、分子机构可能将单独建设平台或引入数据源，通过设立CoE组织可以保持平台的互通性及数据资源的共享性

金融机构现阶段的隐私计算平台建设多处于技术实践尝试性阶段，虽然部分银行等金融机构开启了总行级的隐私计算平台建设项目，但节点部署数量有限，未来的实践扩展中，如果有必要需求也存在替换或增加技术供应商的可能。此外，对于部分金融机构可能会存在不同部门、分支机构基于自身需求而选择不同的技术供应商单独建设隐私计算平台或链接新的数据源，这样的方式或将出现不同隐私计算平台之间未形成互联互通而造成数据流通计算的阻碍，同时也会让机构对数据的协同计算及管理效率产生影响。从长远实践的角度来看，金融机构有必要通过构建CoE（Centre of Excellence）组织的方式来解决上述问题，以帮助机构实现平台及数据资源的最大化协同共享。而CoE组织也并非必须是一个完全独立的部门，也可以通过科技部、数据管理部等部门去承担这部分职责。

金融机构的“数据安全可信CoE组织”的建设方式及建议



数据安全可信CoE的具体构建形式需根据不同类型的金融机构展开差异化调整。科技部或数据管理部更加适合承担关键职责。

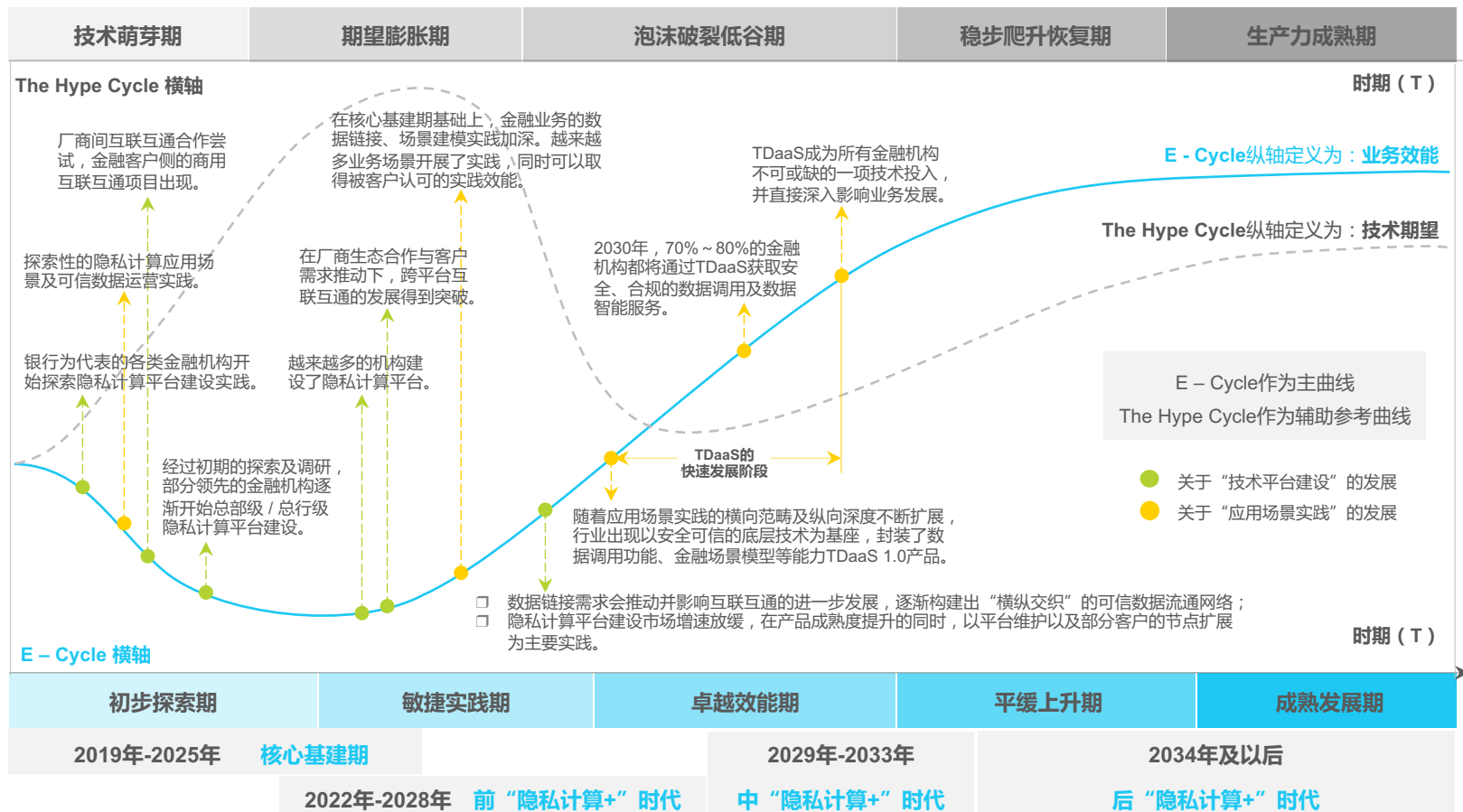
来源：艾瑞咨询研究院自主研究及绘制。

- Section 01 确定职能 & 发现机会**
数据安全可信CoE首先需要明确职能范畴，同时设定CoE的工作成果考核机制。在职能内CoE应该通过协同管理机制及时发现各部门或分支机构对暂未合作的外部数据源的链接及调用需求、新的隐私计算平台建设需求。
- Section 02 协同与执行**
在发现机会的基础上，CoE需要对新的需求（平台建设、数据源链接）和机构现有资源（隐私计算平台、数据源）通过部门协同以及跨平台互联互通等技术手段，促进新旧资源及能力互通融合。
- Section 03 持续运营与改进**
在持续运营中改进CoE组织的模式及管理机制，根据数据流通需求持续保持机构内平台间的互通性、优化机构数据管理机制。

总结：商用实践发展周期

iResearch：隐私计算商用实践周期洞察矩阵（平台建设+应用场景实践的研究，中国金融市场）

绘制时间：2022年10月



注释：“矩阵”通过被验证的方法论，基于大量案例实证、数理实证、市场调研信息、顶级专家观点、技术领导者意见等内容的研究而综合绘制。
来源：隐私计算的案例实证研究、数理实证研究、行业用户调研、隐私计算厂商调研、艾瑞咨询研究院自主研究及绘制。



2022年

中国隐私计算应用实践与平台选型研究报告

 联系分析师

报告将围绕“行业发展、客户洞察、选型指南、厂商推荐”展开研究。

市场发展：分析师将对中国隐私计算的落地实践情况（各领域的平台建设/场景应用实践）、细分领域的隐私计算技术渗透情况、各类技术方案（MPC/FL/TEE/.....）落地实践现状、市场整体竞争态势、产业落地趋势等内容展开分析。

客户洞察：研究团队将面向金融、政务、通信运营商、医疗等领域的行业客户，针对隐私计算的技术认知、技术应用需求、技术投入规划等关键内容展开调研，为隐私计算厂商的产品发展方向、市场战略、客户服务策略提供决策依据。

选型指南：结合“隐私计算平台选型象限”，从多项指标（安全性、性能、功能、部署形式与交付能力、可扩展性等）来阐述隐私计算平台选型策略。

厂商推荐：报告将围绕“产品能力、服务能力、市场能力、客户反馈”等关键维度，选择具备卓越实践力的厂商，入围「iResearch：隐私计算 供应商名录」。

艾瑞新经济产业研究解决方案



行业咨询

- 市 场 进 入 为企业提供市场进入机会扫描，可行性分析及路径规划
- 竞 争 策 略 为企业提供竞争策略制定，帮助企业构建长期竞争壁垒



投资研究

- IPO行业顾问 为企业提供上市招股书编撰及相关工作流程中的行业顾问服务
- 募 投 为企业提供融资、上市中的募投报告撰写及咨询服务
- 商业尽职调查 为投资机构提供拟投标的所在行业的基本面研究、标的项目的机会收益风险等方面的深度调查
- 投后战略咨询 为投资机构提供投后项目的跟踪评估，包括盈利能力、风险情况、行业竞对表现、未来战略等方向。协助投资机构为投后项目公司的长期经营增长提供咨询服务

关于艾瑞



艾瑞咨询是中国新经济与产业数字化洞察研究咨询服务领域的领导品牌，为客户提供专业的行业分析、数据洞察、市场研究、战略咨询及数字化解决方案，助力客户提升认知水平、盈利能力和综合竞争力。

自2002年成立至今，累计发布超过3000份行业研究报告，在互联网、新经济领域的研究覆盖能力处于行业领先水平。

如今，艾瑞咨询一直致力于通过科技与数据手段，并结合外部数据、客户反馈数据、内部运营数据等全域数据的收集与分析，提升客户的商业决策效率。并通过系统的数字产业、产业数据化研究及全面的供应商选择，帮助客户制定数字化战略以及落地数字化解决方案，提升客户运营效率。

未来，艾瑞咨询将持续深耕商业决策服务领域，致力于成为解决商业决策问题的顶级服务机构。

联系我们 Contact Us

 400 - 026 - 2099

 ask@iresearch.com.cn



企 业 微 信



微 信 公 众 号

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。

为商业决策赋能

EMPOWER BUSINESS DECISIONS

