2022·爱分析

隐私计算

厂商全景报告

ifenxi

2022年06月

报告编委

报告指导人

张扬	爱分析	合伙人&首席分析师

报告执笔人

洪逸群	爱分析	高级分析师
孟晨静	爱分析	分析师

媒体支持

51CTO

目录

CHAPTER

01

研究范围定义

1. 研究范围定义

研究范围

隐私计算，又称隐私保护计算（Privacy-Preserving Computation），是指基于一套融合密码学、信息论、分布式计算、安全硬件、数据科学等多学科技术，能对处于加密或非透明状态的数据进行计算的技术体系。常见的隐私计算技术包括了多方安全计算、联邦学习、可信执行环境、同态加密、差分隐私等，通过应用隐私计算技术，企业用户能在提供数据隐私保护的前提下，实现数据在流通共享中的“可用不可见”。

在本报告中，爱分析将隐私计算市场分为应用层、平台层和算力层。其中，应用层是指针对金融、政务、医疗、零售、电信、交通等各行业业务场景提供的包含隐私计算产品和服务的应用解决方案；平台层是指用于支撑构建应用解决方案的平台型产品，即隐私计算平台；算力层是指针对隐私计算性能提升提供的各类算力解决方案，包括算法优化、硬件加速等。

综合考虑企业关注度、行业落地进展等因素，爱分析在本次研究中选取了应用层的金融隐私计算解决方案、政府与公共服务隐私计算解决方案、医疗隐私计算解决方案，以及平台层的隐私计算平台，共 4 个特定市场，进行重点研究。

本报告面向企业和政务机构的决策层，以及大数据与人工智能部门、科技创新部门、各业务部门负责人，通过对各特定市场的需求定义和代表厂商的能力解读，为各行业企业和政务机构的隐私计算应用规划与厂商选型提供参考。

图 1： 隐私计算市场全景地图

图:爱分析绘制

厂商入选标准

本次入选报告的厂商需同时符合以下条件：

- 厂商的产品服务满足各市场定义的厂商能力要求；
- 近一年厂商具备一定数量以上的付费客户（参考第 3 章各市场定义部分）；
- 近一年厂商在特定市场的收入达到指标要求（参考第 3 章各市场定义部分）。

CHAPTER

02

厂商全景地图

2. 厂商全景地图

爱分析基于对甲方企业和典型厂商的调研以及桌面研究，遴选出在隐私计算市场中具备成熟解决方案和落地能力的入选厂商。

金融隐私计算解决方案

（以下厂商均按简称首字拼音排序）

政府与公共服务隐私计算解决方案

（以下厂商均按简称首字拼音排序）

医疗隐私计算解决方案

（以下厂商均按简称首字拼音排序）

隐私计算平台

（以下厂商均按简称首字拼音排序）

百度智能云	冲量在线 IMPULSEONLINE	洞见科技 INSIGHTONE	富数	光之树 points technology
華控清交 TSINGJIAO INFORMATION SCIENCE	蓝象智联	零数科技	蚂蚁集团 ANT GROUP	锘崴科技 NUOWEI TECH
RealAI 瑞莱智慧	数牍 sudo	腾讯云	同盾科技 www.tongdun.cn	TONGTAI 同态科技
UCLOUD优刻得	WeBank 微众银行	CLUSTAR 星云	BaseBit.ai 翼方健数	

图:爱分析绘制

CHAPTER

03

市场定义与厂商评估

3. 市场定义与厂商评估

爱分析对本次隐私计算项目重点研究的特定市场定义如下。同时，针对参与此次报告的部分代表厂商，爱分析撰写了厂商能力评估。

3.1 金融隐私计算解决方案

定义：

金融隐私计算解决方案是指面向银行、保险、证券等金融机构的数据流通场景，实现用户数据可用不可见的隐私计算产品和服务，主要应用于精准营销、联合风控、反欺诈、合规认证、金融监管等场景。

终端用户：

银行、保险、证券等金融机构的大数据部门，科技创新部门，风控、营销、信贷、信用卡中心、资管等业务部门

核心需求：

随着银行等金融机构全面拥抱互联网和数字化转型，数据已经成为支撑其产品服务创新的核心要素。尽管凭借广泛的客户基础，金融机构已经积累了海量的用户数据，但这些数据往往存在数据维度单一的问题。为了提供更精准、更多元的金融产品和服务，金融机构需要从外部引入更多的用户行为、场景等数据，从而丰富数据维度，延伸应用场景。以往受政策、观念、技术等因素限制，机构之间的数据安全共享难以突破，而隐私计算技术能够在保障数据隐私的前提下，实现数据在机构间安全地流通、共享和应用，正被金融机构广泛关注并开始采用。金融机构对隐私计算解决方案的核心需求包括：

- **能在类型多样，且个性化程度较高的场景中应用隐私计算技术。**金融领域数据类型丰富，相应地，隐私计算的应用场景也非常多样，并且每家金融机构对于隐私计算应用都存在一定的个性化需求，因此金融机构需要应用多种隐私计算技术，并能以灵活的方式对不同技术方案进行融合。此外，在一些常用场景，如匿踪查询、隐私求交中还需要能快速使用标准化的解决方案。

- **在对实时性要求较高的场景中具备较强的端到端性能。**金融机构的一些业务场景，如信贷审批、交易监控等，需要以很低的时延获得计算结果，以保证客户服务质量，并快速识别风险、降低损失。因此，在此类实时场景中，金融机构需要隐私计算解决方案具备较强的端到端性能。
- **通过引入第三方数据源和专业机构的建模咨询服务，在特定场景中提升模型效果。**金融机构应用隐私计算的根本在于提升产品服务的业务收益，而实现这一目标的关键是在业务场景中构建更有效的模型，因此，金融机构一方面需要引入合适的第三方数据，丰富样本数据的数据维度，另一方面需要引入专业机构的建模咨询服务，在数据、算法的选择、模型训练、隐私计算工具使用等方面提供专业的指导，从而提升模型效果。
- **隐私计算解决方案能以较低的成本进行快速部署和与原系统集成。**一方面，金融机构希望隐私计算应用能快速落地并产生效果，因此需要解决方案能以便捷和快速的方式进行部署；另一方面，金融机构通常已经建立了较复杂的业务和 IT 系统，因此需要隐私计算解决方案能在对原系统改造尽量小的前提下，与原系统集成。
- **满足安全合规要求。**金融数据的敏感性，加上监管机构对于金融数据安全的多重要求，使得金融机构对于隐私计算解决方案在数据安全保护、系统环境、计算流程的可解释性等方面有较高的安全性要求，并要求供应商的产品通过权威测评机构的安全标准测评。

厂商能力要求：

- **具备多方安全计算、联邦学习等多种隐私计算技术能力，并能以较灵活的方式为用户提供服务。**一方面，厂商需要提供丰富的加密算法的算子库和联邦学习算法组件，允许用户自定义组合实现针对特定应用场景的隐私计算应用，兼顾安全性、性能、精度的不同需求。另一方面，厂商需要提供可直接调用的匿踪查询、隐私求交等应用解决方案，满足金融用户在跨机构数据协作中广泛的数据对齐、ID 融合的需求。
- **在实时业务场景中提升端到端的性能。**由于在实时计算中网络延迟是目前会影响端到端性能的主要因素，因此厂商需要着重对通信效率进行优化，如通过优化流程编排、任务调度，提高算子并行度等方式提升多节点间的通信效率，从而提升性能。
- **能够链接较丰富的第三方数据资源。**厂商需要建立较广泛的数据资源生态，具备运营商、支付、互联网、政务等领域的数据资源链接能力，为金融机构提供更多的用户行为、场景等数据。此外，厂商还需要与其它厂商建立互通互联协议，方便金融机构跨平台调用第三方数据。

- **提供专业的建模咨询服务。**厂商相关团队需要具备金融领域丰富的从业经验，能够为金融机构在模型构建中提供常用的算法，并在数据、算法的选择、模型训练、隐私计算工具使用等方面提供专业建议，为金融机构实现更好的模型效果。
- **能快速部署和集成隐私计算解决方案。**在解决方案部署方面，厂商需要提供敏捷化的部署和交付方式，如平台采用云原生架构，支持容器化的交付方式；以 SDK 或 API 的方式提供隐私计算能力，支持用户快速构建隐私计算应用；在与原系统集成方面，厂商需要提供组件化和接口化服务支撑金融机构在隐私计算平台与原系统之间做数据与模型的传输与对接，减少对原系统的改造。
- **隐私计算解决方案具备较高的安全性。**厂商需要通过提供完善的数据加密技术、完善平台系统的安全性设计等方式提高解决方案的安全性；并需要支持算法流程可视化，以及支持接入第三方流量审计工具对数据用途进行验证等方式提高解决方案的可解释性和可信度。同时，厂商的产品需获得权威测评机构的安全标准测试。

入选标准：

1. 符合金融隐私计算解决方案的厂商能力要求；

2. 近一年在该市场服务客户数 3 家以上；

3．近一年该市场相关服务收入规模在 200 万元以上。

代表厂商评估：

（注：以下代表厂商评估均按厂商简称首字音序排序）

洞见科技

厂商介绍：

洞见科技是由中国最大的信用产业集团“中诚信”孵化、网信事业国家队“中电科”投资的领先的专精型隐私计算技术服务商，专注于为政务、金融、通信等行业客户提供隐私计算技术平台建设以及面向场景的数据智能服务。公司核心成员来自中诚信、大型银行、保险公司以及人工智能企业，具备丰富的行业知识和服务经验。

产品服务介绍：

洞见科技的核心软件产品洞见数智联邦平台（InsightOne）是其自主研发的金融级隐私计算平台，拥有面向场景的“MPC+FL”融合引擎、可监管的分布式信任架构、全计算链路隐私安全保护、深入场景的专业化算法、无可信第三方联邦学习、区块链增信隐私计算、多方安全图计算与图联邦学习、跨平台互联互通容器等核心技术。通过匿踪查询、隐私求交、集合运算、联合统计与联合建模等功能矩阵的构建，为用户提供信贷风控、精准营销、保险精算、资管评级、债指编制等金融场景应用服务。此外，在 InsightOne 软件服务基础上，洞见还研发了融合计算、网络、存储等硬件资源的隐私计算高性能信创一体机产品 InsightStation，能够满足金融与政企客户自主可控、开箱即用的需求。

厂商评估：

洞见科技的隐私计算产品与服务在平台的通用性与安全性、面向金融行业用户的场景服务能力、对金融机构业务效果提升程度，以及跨平台协同等方面具备优势。

洞见科技的隐私计算平台 InsightOne 具备较高的通用性与灵活性。InsightOne 平台采用面向计算场景的融合引擎架构，将多方安全计算、联邦学习等算法拆分为细化的算子，并结合差分隐私、同态加密、零知识证明等技术，用户可以根据需求对底层的算子进行灵活组合，融合多种技术并取

长补短，形成针对特定需求的计算过程，从而满足客户在不同计算场景中对于功能、性能、安全、计算精度等方面不同的需求。

针对金融行业用户的需求，洞见科技具备包括数据链接和业务建模在内的场景服务能力。对于有多方数据融合应用需求的用户，洞见科技在政府、运营商、电力、互联网、征信等大量合规数据拥有方部署了隐私计算节点，具备较丰富的数据资源链接能力，结合隐私计算技术，能够为下游的金融行业用户持续赋能。同时，洞见科技基于其长期在金融领域的技术和服务积累，也为用户提供业务建模与咨询服务，在其 InsightOne 平台上内置了几十种银行、保险、证券、资管等行业常用的算法，能更好地供场景应用建模使用。例如，洞见科技为渤海银行搭建隐私计算平台，并基于平台能力更安全地将行内信用卡用户表现数据与外部运营商、电商等多方数据联合，开展信用卡账单分期营销模型构建，服务于行方差异化营销策略制定，提升用户体验。

InsightOne 平台能在对金融机构原有系统很小改造的情况下良好兼容用户原有的技术栈。一方面，通过分布式引擎将隐私计算算法模型与金融机构原有的风控、营销等业务场景模型做了深度优化与融合；另一方面，通过组件化和接口化服务，在隐私计算平台与用户原有各类系统之间做数据与模型的传输与对接。因此，InsightOne 平台能在不改变用户原有系统使用习惯的基础上，最大程度地兼容不同技术栈。

洞见科技也积极探索跨平台互联互通能力。在技术创新方面，洞见科技研发了“资源容器+算法容器+原语容器”的三层容器技术，即为客户提供一个像“插线板”一样的隐私计算底座，实现不同厂商的算法插件的兼容和互通，打破了不同隐私计算厂商的“计算孤岛”；在标准制定方面，洞见科技积极牵头和参与了 IEEE、CCSA、TC601、TC260 等机构制定的隐私计算跨平台互联互通系列技术标准；在应用实践方面，洞见科技与蚂蚁集团、锘崴科技实现了业界首次多方异构隐私计算平台之间完全对等的算法协议互通，还在招商银行总行的牵头下，落地了国内首个大型股份制商业银行互联互通平台建设。

在产品安全性方面，InsightOne 平台通过了中国信通院多方安全计算和联邦学习功能、性能、安全、区块链辅助等隐私计算全系列产品测评，以及国家金融科技测评中心多方安全计算和联邦学习金融应用双项评测。其独立自研的无可信第三方联邦计算框架，通过对等网络之间的交互学习和分布式学习，解决了开源联邦计算框架中存在的依赖第三方参数算子和密钥分发等风险问题。

典型客户：

招商银行、北京银行、华夏银行、渤海银行、中国人寿

富数科技

厂商介绍：

富数科技成立于 2016 年，是国内领先的隐私安全计算技术服务商之一，专注于联邦学习、安全多方计算、匿踪查询等加密计算领域，业务场景以金融、运营商、政务为主，并拓展到医疗、司法监管、工业互联等领域。富数科技是隐私计算互联互通协议首个国家标准的牵头单位，深度参与信安标委、金标委、工信部等标准的制定。

产品服务介绍：

富数科技的核心产品是 Avatar 安全计算平台，平台包含了联邦学习、安全多方计算、匿踪查询、开放平台等模块，可为金融等行业客户提供联合统计、联合建模、匿踪查询等功能。其中，FMPC 开放平台将富数科技的隐私计算能力以 SDK 和 API 的形式提供给用户，方便用户快速构建隐私计算解决方案，并与其他用户的平台进行适配和互联。

在 Avatar 安全计算平台基础上，富数科技也为用户提供针对金融等行业业务场景的建模咨询服务。

厂商评估：

富数科技隐私计算产品与服务，在平台功能的完整性、使用方式的灵活性、平台开放性与安全性，以及面向金融行业用户的建模咨询服务等方面具备优势。

富数科技的 Avatar 安全计算平台具备完善的功能，并且使用方式灵活。Avatar 安全计算平台融合了联邦学习、安全多方计算、零知识证明等多种隐私计算技术，用户可以在可视化的操作界面中调用平台中丰富的算子以及功能模块进行组合，形成所需的应用解决方案。同时，平台也提供了操作管理组件、系统安全组件、合规审计组件、基础设施层、服务层等多个功能组件，让用户可以实现开箱即用、快速部署。

Avatar 安全计算平台具有较高的开放性。一方面，FMPC 开放平台将富数科技的多方安全计算与联邦学习能力以 SDK 和 API 的形式提供给用户，用户可以快速构建隐私计算应用解决方案。另一方面，FMPC 开放平台支持用户通过规范的协议接口在数据、算法、模型等资源方面实现互通互联，帮

助用户实现多方的数据融合与联邦学习建模。同时，富数科技积极推动行业内互联互通工作，并牵头制定隐私计算互联互通首个国家标准。

富数科技着重为金融行业用户提供专业的建模咨询服务，以实现更好的模型效果。在数据对接方面，富数科技已经积累了丰富的运营商、支付、互联网设备等数据源资源，同时，基于对数据的深入了解，富数科技能为金融用户在建模中提供有效的数据源、以及数据字段选用建议；在模型构建方面，富数科技团队具备大型金融机构、金融科技公司丰富的从业经验，对金融领域的业务场景、专业知识有深刻理解，并结合丰富的算法经验和对隐私计算工具的了解，能够帮助金融行业用户在客户拉新、高净值客户识别、风控反欺诈、增信评估等各类模型构建中提供专业的咨询服务，提高模型效果。

在平台安全性方面，Avatar 安全计算平台更侧重安全性，在兼顾性能的同时，保证数据加密范围和加密强度，以提高平台安全性。同时，富数科技具备一套体系化的方法论和工具，从系统安全、算法安全、实现安全等多方面提供平台的安全保障，并通过隐私计算流程可视化让用户清楚各个环节逻辑和数据流向，避免黑箱操作，增加用户安全感。此外， Avatar 安全计算平台已通过信通院多方安全计算产品的安全专项测评。

典型客户：

中国银联、中国银行、交通银行、招商银行、广东农信

锘崴科技

厂商介绍：

锘崴科技成立于 2019 年，是一家专注隐私保护计算技术的服务提供商，创始团队来自加州大学圣地亚哥分校 UCSD 等高校，具备深厚的隐私计算、生物医疗信息等领域的学术和实践经验，团队成员多来自 IBM、Google、Thermo 等世界五百强企业。锘崴科技开发了一整套自主、安全、可控的隐私保护计算平台产品，业务场景覆盖医疗、金融、保险、政务、安防等。

产品服务介绍：

锘崴科技的锘崴信隐私保护计算平台是拥有自主知识产权，已通过多项权威测评，安全、可控的隐私计算基础设施平台。平台包括了安全联邦学习系统、多方安全计算 MPC 系统、超融合沙箱（TEE）三个核心模块，可为用户提供隐私查询、隐私建模/分析、隐私推理等隐私计算功能，并兼顾性能、安全性、精度等多种要求。

针对金融行业用户，锘崴科技提供了金融服务隐私保护计算平台（NovaFintech)。作为锘崴信隐私保护计算平台的子平台，其能够满足金融行业用户对数据源、分析功能、使用交互的差异化需求。提供跨多个数据源（远大于 3 方）的联合隐私求交和隐私建模能力，同时可以支持恶意模型、防止侧信道攻击等安全功能。同时提供差异化的数据源链接资源，满足特定金融场景的需求。

同时，锘崴科技也提供基于国产化 CPU、加速卡、可信执行环境的锘崴信一体机产品，为用户提供软硬件结合的隐私保护计算解决方案。

厂商评估：

锘崴科技的隐私计算产品与服务在面向金融行业用户中，具备支持丰富的应用场景、面向复杂应用场景的高性能与高精度、多数据源链接、以及平台安全性等优势。

锘崴科技的隐私保护计算平台能支持金融行业用户丰富的应用场景。锘崴信金融服务隐私保护计算平台（NovaFintech)是面向金融场景的隐私计算子平台。该平台基于锘崴科技通用的隐私保护计算平台底座，通过对上层应用的灵活部署，从而解决金融客户在不同场景下的隐私计算需求。

NovaFintech 帮助银行保险机构借助全行业数据来进行安全的联合分析建模，已在金融行业中的业务拓展、数字营销、精准获客、智慧风控、智能反欺诈等具体场景中不断落地。

锘崴科技的隐私保护计算平台在处理复杂的金融业务场景过程中具备性能与精度的优势。锘崴科技的隐私保护计算技术最早基于医疗领域的复杂场景中的非结构化数据不断迭代优化，因此平台在复杂的金融场景中的性能及精度优势明显。例如，锘崴科技在与某金融机构合作过程中，需要对人脸识别系统进行隐私保护计算处理，由于人脸图像数据的复杂度远高于结构化数据的复杂度，传统的多方安全学习技术无法满足其对精度与性能的要求。锘崴科技通过融合机器学习技术模型与自研的隐私保护计算算法，在保证人脸识别系统高精确度的同时，最大程度上保证了隐私计算性能。

锘崴科技通过连接丰富的数据源为金融客户提供基于隐私计算的数据连接能力。锘崴科技在通信运营商、银行、银联、公安部门等机构，部署了多个隐私计算节点，加强隐私计算生态网络建设，为下游的金融行业用户持续赋能。如反赌反诈反洗钱平台的搭建过程中，锘崴科技通过对多源数据的特征提取，模型设计及策略匹配，对交易过程数据、IP 数据、卡片数据进行综合分析，对资金和账户进行定性，对涉赌、涉诈、虚拟币、洗钱账户进行全方位监管，并向相关机构提供预警服务。

在产品安全性方面，锘崴隐私保护计算平台已通过了信通院联邦学习及可信执行环境基础能力专项测评，以及公安部隐私保护计算平台产品测评与国家信息系统安全等级保护三级备案与测评。

同盾科技

厂商介绍：

同盾科技是中国领先的人工智能科技企业，专注于决策智能领域，通过基于人工智能的决策智能平台和基于隐私计算的共享智能平台，聚焦金融风险、安全和政企数字化三大领域，利用公司的算法、工具以及数据生态，帮助客户防范欺诈和安全风险，推动智能化决策进程，提升业务决策的灵活性、敏捷性和准确性。

产品服务介绍：

智邦平台是同盾科技的隐私计算平台，平台基于联邦学习、多方安全计算、隐私安全求交等多种隐私计算技术，并结合工业级算子库 Caffeine、联邦数据安全交换协议 FLEX、计算与通信引擎 Ionic 等功能组件，可为客户在精准营销、风控联合建模、反电诈、反洗钱等多种场景实现隐私计算应用。

同时，智邦平台构建了从数据到知识转化的知识联邦生态系统，能够实现知识的共享，并利用各参与方数据进行联合计算、联合建模、联邦预测，以及利用知识网络进行知识推理、知识演绎，从而让知识能在不同知识源之间自由流动，支撑智能决策。

厂商评估：

同盾科技的隐私计算产品及服务具备能快速部署并实现业务效果，支持基于知识网络的智能决策，能提供丰富的数据源、应用场景与建模咨询，以及较高的性能和安全性等优势。

智邦平台提供全流程的隐私计算解决方案能力，能够快速部署并实现业务效果。在平台架构方面，平台采用 k8s 云原生分层架构，可无缝对接用户的私有云、公有云、混合云等环境，并支持容器化的敏捷交付和快速发布；在隐私计算使用方式方面，同盾科技自研的经过工业级验证的算子库包含隐私计算典型的算子和协议，用户可以灵活自主地构建隐私计算工作流，也可以直接调用平台内已经封装过的算子组合，降低使用门槛；在应用服务方面，平台在上层对接了同盾科技或第三方的营销、风控等各类 SaaS 应用，能加快应用的落地；此外，平台还提供数据交换沙箱功能，解决多源异构数据接入难，以及数据标准不一致的问题。

智邦平台可基于同盾科技的知识联邦框架体系进一步将数据转化为知识，以在各类业务场景中实现智能决策。知识联邦框架体系通过平台的一系列工具组件依次从信息层、模型层、认知层、知识层四个层面实现数据到知识的转化。在信息层，平台对各参与方的数据进行清洗、转化和加密；在模型层，平台通过联邦学习将参与各方训练的模型参数进行聚合更新；在认知层，平台通过神经网络中的全连接层、特征提取后的高层语义特征等嵌套特征进一步更新模型，提升其精度；在知识层，平台则通过构建知识网络，以及知识融合、知识推理，实现智能决策。

同盾科技积累的庞大的客户生态可为金融等行业客户提供丰富应用场景以及专业的建模咨询服务。同盾科技服务客户数量已经超万家，客户类型涵盖 22 个行业，118 个细分领域，一方面，能为客户触达多元化的数据源，支持精准营销、智能风控、反电信欺诈、反洗钱等金融业务场景；另一方面，能够为隐私计算技术落地提供广泛的应用场景，并提供专业的建模咨询服务。此外，同盾科技通过智邦产品与招商银行慧点平台及友商间系统间的产品级互联互通，并开放其自研的数据交换协议 FLEX 或兼容其它互通互联协议，为客户构建知识共享生态。

智邦平台具备较高的计算性能，能满足金融等行业用户在特定场景中的实时性要求。平台对海量数据下的内存数据分片进行了深度的定制优化，能在小时级耗时内完成十亿级别数据的安全对齐；同时，同盾科技自研的通信框架 Ionic 通过优化流程编排、任务调度，提高算子并行度等方式提升了联邦算法等通信效率，平台的建模计算效率因此提升了 9 倍、资源消耗降低了 70%-80%、模型精度与本地误差在 0.1%；此外，平台还支持分布式在线预测，单机性能可达上千 qps。基于这些性能的提升，平台可以在信贷审批、反欺诈等实时性要求较高的场景中满足低于 200 毫秒响应的性能要求。

在安全合规方面，智邦平台采用最高安全等级的不经意传输、同态加密算法构建隐私计算应用。同时，平台可以兼容可靠的第三方流量审计工具，如 Tcpdump，对每一条数据的用途进行验证，及时发现明文泄露等风险，保障计算结果符合隐私计算要求。此外，智邦平台也已通过信通院基于多方安全计算，以及基于联邦学习的数据流通产品基础能力专项测评。

典型客户：

工商银行、招商银行、桔子数科

3.2 政府与公共服务隐私计算解决方案

定义：

政府与公共服务隐私计算解决方案是指面向政府与公共服务的数据流通场景，实现用户数据可用不可见的隐私计算产品和服务。主要应用于政务部门各类数据共享和数据对外开放场景。

终端用户：

各地大数据局、数据交易所、委办局等政府和公共服务机构的信息化部门、大数据部门、业务办理部门等

核心需求：

随着数据要素市场化、政企数据融合等政策的相继出台，政府与公共服务等政务机构近年来正积极推动政务数据在不同部门间的内部共享，从而提高政府治理水平和公共服务效能，同时，政务数据进一步的对外开放还可为众多行业企业赋能，提高社会经济效益。由于政务数据包含社保、公积金、税务、交通、水电等多种数据，分散在不同部门，加上政务数据涉及大量公民隐私，管控严格等因素，以往的政务数据流通共享审批手续繁琐，协调非常困难。隐私计算技术能够在保障数据隐私的前提下，实现数据在机构间安全地流通、共享和应用，正被政务机构开始尝试采用。政务部门对隐私计算解决方案的核心需求包括：

- **能用隐私计算技术打通多方数据，且隐私计算的使用门槛要低。**目前政务部门对隐私计算应用的主要诉求在于打通多方数据，满足常见业务场景的需求，如统计分析、联合建模、数据查询等，因此政务部门需要使用多方安全计算、联邦学习等技术实现这些应用。此外，政务隐私计算解决方案存在大量业务部门的用户，因此需要在常用场景中可以直接调用已封装好的应用。
- **在多参与方的应用场景中保障良好的计算性能。**政务隐私计算应用通常涉及多个政务部门的数据源，且随着政务数据进一步对外开放，数据应用方也将可能达到数十甚至数百家。因此，政务部门需要在这类场景中保障较高的计算性能。
- **能让数据要素以安全可信的方式对外充分流通和开放。**政务数据通过隐私计算发挥协同价值的前提是数据能够跨部门、跨区域、跨行业充分流通和开放，因此，政务部门需要完善的数据运营体系支撑数据的流通和开放，并通过区块链技术对数据进行确权，实现数据资产化。

- **满足安全合规要求。**政务数据涉及大量公民隐私，政务部门对其管控严格，因此政务部门需要隐私计算解决方案在数据安全保护、系统环境等方面具备很高的安全性。同时，为保证隐私计算核心技术的自主可控，政务部门要求隐私计算解决方案相关软硬件的核心模型实现完全的国产化。此外，政务部门还要求供应商的产品通过了权威测评机构的安全标准测评。

厂商能力要求：

- **具备多方安全计算、联邦学习、同态加密等多种隐私计算技术能力，并能较低的门槛供业务用户使用。**一方面，厂商需要提供多方安全计算、联邦学习等技术支撑政务部门的统计分析、联合建模、数据查询等应用需求，且厂商尤其需要具备高性能的同态加密技术，以在多参与方的计算场景中提高计算性能，并降低对政务部门业务系统的改造。另一方面，厂商需要为一些政务部门常用的场景定制隐私计算应用，并以可视化的方式供业务用户调用，或以软硬件一体机的形式提供给用户。
- **在多参与方的应用场景中提升计算性能。**一方面，厂商需要针对联合计算、匿踪查询等场景提升计算性能，包括算法优化、通信优化、硬件加速等多方面的性能优化；另一方面，厂商需要进一步提供多租户管理能力，对计算资源进行切割，提升高并发和多租户模型下的计算性能。
- **提供基于区块链技术的数据运营服务。**厂商需提供数据流通/共享平台，并以平台为中心构建数据运营服务体系，连接多方的数据源机构和数据应用机构，以支撑各方在平台上完成数据的流通和共享。同时，厂商需要在平台中应用区块链技术，通过对数据、数据处理路径和规则、参与方身份、分配机制等进行上链存证，保障数据流通各环节中数据和参与方的安全可信。
- **隐私计算解决方案具备较高的安全性。**厂商需要通过提供完善的的数据加密技术、完善平台系统的安全性设计等提高解决方案的安全性；同时，厂商需要实现隐私计算相关软硬件核心模型的全部国产化；此外，厂商的产品需获得权威测评机构的安全标准测试。

入选标准：

1. 符合政府与公共服务隐私计算解决方案的厂商能力要求；

2. 近一年在该市场服务客户数 3 家以上；

3．近一年该市场相关服务收入规模在 200 万元以上。

代表厂商评估：

（注：以下代表厂商评估均按厂商简称首字音序排序）

零数科技

厂商介绍：

零数科技成立于 2016 年 8 月，是一家具备领先区块链底层技术及深度应用场景的国家高新技术企业。公司旨在通过区块链及隐私计算技术，打造数据价值流通基础设施，确保数据在多主体间可信有序流通和安全高效应用，服务于汽车、金融、政务、双碳、文化等领域深度数字化。

产品服务介绍：

零数隐私计算服务平台基于多方安全计算、联邦学习、同态加密等技术，为用户提供从多方数据融合、模型训练、模型评估到应用部署的全流程服务。同时，平台提供联合建模、隐匿查询、安全匹配、安全统计等独立的功能或服务组件，可让政务数据安全高效地服务金融、双碳等场景，并实现隐私计算应用。

帮助政务等行业用户实现对数据要素全生命周期的隐私安全管理，零数科技结合隐私计算和区块链技术，推出了零数数据流通服务平台，在提供完整的隐私计算平台功能的基础上，通过应用区块链技术，将数据流通全流程的操作和处理记录上链保存，并在链上用智能合约对计算过程进行协作管理，保证数据使用安全合规。

厂商评估：

零数科技的隐私计算产品与服务具备使用灵活、能结合区块链技术保障数据和数据共享参与者身份可信、性能和安全性较高等优势。

零数隐私计算服务平台的隐私计算功能具备较高的灵活性，可实现多种隐私计算应用，并兼顾用户在不同场景中对性能和安全性的不同偏好。零数科技将平台隐私计算引擎系统中的联邦学习和多方安全计算引擎解耦为算子库，其中，联邦建模组件库包含了数据融合、数据预处理、特征工程、

线性回归、逻辑回归、XGBoost、K-Means、模型报告等算法组件；联合计算算子库则包含了能实现四则运算、逻辑运算、统计计算等不同计算能力的算子，用户可通过可视化界面组合不同算子构建所需的隐私计算模型。同时，平台的隐私计算引擎系统也包含了面向具体应用场景的隐匿查询、安全匹配引擎，用户可直接调用其功能模型，实现相关应用。

零数数据流通服务平台是一款隐私计算与区块链结合的产品，能够保障数据以及数据共享参与者身份的可信，提升数据共享流通的效率。一方面，借助区块链技术，平台可对数据采集、数据处理的路径和规则等进行上链存证，并通过平台的数据共享目录开放给第三方使用，从而保证数据在流通的全生命周期合规、可信，并支持事后的审计追溯；另一方面，平台可借助区块链技术实现去中心化的隐私计算调度，当发起一项隐私计算任务时，平台可以在链上生成智能合约作为调度指令，由合约规定参与方身份，以及每个参与方需要提供的数据或计算规则等，从而防止调度指令被篡改。此外，平台还可进一步通过智能合约设定各参与方认可的分配机制，对各参与方的贡献度进行评估和认定，并基于贡献度对收益进行分配。例如在“区块链+园区能源双碳”应用场景，对企业的绿色程度的评价需要多维度的数据，包括企业用水、电、气、热能的情况，还包括企业的所属行业、规模、经营收入、纳税等指标，还包括企业对于光伏等绿色投入情况。传统互联网填报模式收集数据效率低下，且容易泄露企业隐私，对企业带来不利影响等因素，因此企业往往不愿意填报。通过零数数据流通服务平台，可以实现多方数据的隐私求交与安全融合，并采用联邦学习相关特征与模型算法，训练形成企业绿色信用评级模型。通过内置企业绿色评分与财务评分的综合经验逻辑模型，即根据模型各指标权重的设置，可以有效评估企业的绿色信用状况，最终输出园区各企业的绿色信用评级结果。整个过程中利用隐私计算数据提供方不泄露数据，平台不泄露计算模型，而区块链解决了信任问题，确保关键数据未经篡改、计算过程透明可溯。

零数隐私计算服务平台具备较高的计算性能。零数科技对平台内置的算法进行了大量优化，通过降低通信次数，通过使用更加底层的开发语言来实现基础算法算子以提高运算效率，优化计算逻辑等提高计算性能。同时，结合硬件加速卡，以及计算调度流程的优化等，平台可以在一些隐私计算场景，如亿级数据量的隐匿查询中，比同类解决方案效率提升 25%。

在隐私计算的安全性方面，零数科技从系统、算法协议、数据、应用、通信、密码等多个层面做了大量权限控制、加密处理等工作，能保障用户的安全性需求。同时，零数联邦学习平台也已通过了信通院联邦学习基础能力专项测评，在调度管理能力、数据处理能力、算法实现、效果及性能、安全性等方面，获得了权威认可。

典型客户：

青岛某区大数据局、江苏某市大数据局、上海某大数据中心

同态科技

厂商介绍：

同态科技是一家隐私计算数据保护服务商，基于自主可控的同态加密技术，在政务、金融、军民融合等领域为用户提供数据交换共享及隐私计算数据保护服务，实现数据可用不可见、合规数据标准化、数据应用全流程可控等。

产品服务介绍：

“隐私计算应用一体化平台”是同态科技主要的隐私计算平台产品，基于自研的超高速同态加密算法，隐私计算应用一体化平台为用户提供数据隐私保护和数据共享应用能力，可用于机器学习、数据统计、隐私查询等场景。同时，用户可在该操作系统中直接使用预置的隐私计算应用，或基于开发接口定制上层的隐私计算应用，作为底层基础设施赋能联邦学习与多方安全计算。

同态科技的隐私计算一体机是全球首款超高速全同态加密机，集成 SM2、SM3、SM4 和高速同态加密算法，为数据共享隐私计算提供标准化的数据输出能力，实现免侵入式隐私计算解决方案。采用硬件算法高速芯片，提供隐私计算硬件化能力，依托标准的商密硬件平台，对外提供超高速同态加密能力以及多种开发接口，赋能数据隐私保护。同时，提供安全授权管理服务，为各客户端用户提供独立设备密钥，保障上层以及设备的安全授权及使用。

厂商评估：

同态科技的隐私计算产品与服务在面向政府行业用户中，具备满足不同技术水平用户需求、对业务系统改造小、能在多参与方的隐私计算场景中保障性能、以及较高的安全性等优势。

同态隐私计算应用一体化平台能满足不同技术水平用户需求，并保障良好的交互体验。业务用户可通过可视化页面直接调用平台内置的数据授权、数据协同、身份认证、数据建模等隐私计算应用，快速构建应用；应用开发用户可通过服务级 API 接口调用平台内置的数据隐私保护服务、数据隐私计算服务等隐私计算能力，定制专属的隐私计算应用；技术研发用户可通过内核级 API 接口调用包

括同态加密、同态解密、属性解密、国密算法 SM2/SM3/SM4、ID 去标识化等在内的同态加密能力，用于与多方安全计算、联邦学习等技术融合形成隐私计算解决方案。

同态隐私计算应用一体化平台对用户业务系统改造影响较小，降低政务用户与其业务系统进行集成的成本。基于同态加密技术，隐私计算应用一体化平台能让数据在加密后保持原有的计算能力，不影响原有业务系统中的数据流向、数据使用方式，数据源仅需在原系统中添加隐私计算一体机，数据逻辑、业务逻辑、系统逻辑、代码逻辑以及通信逻辑均无需修改，系统侵入性降到最低。如在公安机关的反欺诈系统中，公安机关只需要部署一套同态加密应用系统，对外提供经同态加密保护的数据，就能完成对不同反欺诈场景的数据支撑。

同态科技自研的同态加密算法能在多参与方的数据交换、数据查询等场景中保障计算性能。一方面，同态科技自研的超高速同态加密算法是一种高效的全同态加密算法，解决了经典全同态加密技术效率低、密文长度大等问题，能显著降低密文膨胀率，提升加解密与密文应用的效率，对比开源的同态加密算法，整体性能实现千倍级提升。另一方面，由于同态加密算法在数据层加密，无需搭建多套应用系统，相对比多方安全计算，同态加密能大幅降低通信交互频次，节省算力，提高计算性能。

在安全性方面，一方面，同态科技的超高速同态加密算法自主可控，并且相关软硬件产品的核心模块全部国产化，核心技术安全可控，能充分实现数据安全和应用安全。另一方面，金融领域技术能力获得中国人民银行下属检测中心认证、密码领域技术能力获得国家密码检测中心认证、数据交换共享模式获得国家信息中心认可。

典型客户：

公安部第三研究所、浪潮云、上海数据交易所

3.3 医疗隐私计算解决方案

定义：

医疗隐私计算解决方案是指针对医疗领域的数据流通场景，实现用户数据可用不可见的隐私计算产品及服务，主要应用于临床诊断、医学研究、医保管理、医药研发、基因分析、疾控管理等场景。

终端用户：

医院各科室，各地卫健委、医保局、疾控中心等医疗机构的大数据部门、科技研发部门，医药企业的药物研发部门等

核心需求：

伴随医疗信息化的持续推进，医疗机构积累了大量医疗数据，通过人工智能和统计分析，这些数据可以被应用在临床诊断、医学研究等众多场景。然而，医疗数据的应用通常需要收集来自不同地区、不同人群的样本数据，并需要包含临床、检验、基因等多种维度。由于单个医疗机构积累的样本数据量通常有限，因此医疗机构需要采用隐私计算技术对不同的数据源进行联合建模或联合计算。医疗机构对隐私计算解决方案的核心需求包括：

- **能在多种不同安全假设与计算复杂度的场景中应用隐私计算。**医疗隐私计算应用场景多样且复杂，如疾病诊断、医学影像、基因组学、药物靶点发现等，各类场景对于精度、性能和安全性的要求差别较大，因此医疗机构需要应用多种隐私计算技术，并根据需求对不同技术方案进行融合。
- **应用多种医疗领域专业的 AI 模型和统计分析方法来处理各类医疗数据。**医疗数据的类型较复杂，包含各种结构化和非结构化数据，尤其是基因、医学影像等数据的复杂度极高；与此同时，医疗领域的数据处理高度专业化，需要广泛结合医学、生物学、药学等领域的专业知识。因此，医疗机构在处理数据时需要应用多种医疗领域专业的 AI 模型和统计分析方法。
- **在多参与方的应用场景中保障良好的计算性能。**医疗隐私计算应用场景，如联合多家机构的病例对比，药物有效性研究，经常需要联合十多家甚至更多的参与方。医疗机构因此需要在这类场景中保障较高的计算性能。

- **在特定应用场景中实现很高的计算精度。**一些医疗隐私计算应用场景，如病人用药和疗程规划等，要求计算结果非常精确，因此，医疗机构需要隐私计算解决方案在这类场景中具备很高的模型精度。
- **链接同一区域或同一领域多方的医疗数据资源。**医疗隐私计算应用经常会受限于样本数据量，如疾病诊断，单个医院拥有的病例样本量往往有限，因此医疗机构通常需要链接同一区域或同一领域多方的数据源满足模型训练或联合计算要求。
- **满足安全合规要求。**医疗数据涉及大量病患隐私，这些数据的泄漏会造成法律和道德风险，因此医疗机构需要隐私计算解决方案在数据安全保护、系统环境等方面具备很高的安全性。

厂商能力要求：

- **具备多方安全计算、联邦学习、同态加密、差分隐私、可信执行环境等多种隐私计算技术能力。**厂商需要提供多种密文计算技术，以实现对联合建模或联合计算不同环节的加密，满足安全性要求的同时，兼顾性能和精度；针对医疗行业用户，厂商尤其需要提供基于可信执行环境的解决方案，以在计算复杂度，以及性能、精度和安全性要求都很高的场景中，满足用户需求。
- **提供专业的医疗领域的 AI 模型和统计分析方法。**如针对临床诊疗，提供辅助诊断、治疗方案推荐、用药推荐等方面的 AI 模型；针对医学影像分析，提供病灶识别等 AI 模型；针对基因分析，提供基因对齐、全基因组关联分析、人口分层等分析方法。
- **在多参与方的应用场景中提升计算性能。**一方面，厂商需要对计算效率、数据压缩、带宽等进行优化，提升多参与方之间的通信效率，从而提升计算性能。另一方面，厂商也可以通过算力网络为用户调度第三方算力资源来提升计算性能。
- **在特定场景中提供高精度的联邦学习模型。**厂商需要在对计算结果精确度要求很高的场景中提高模型精度，如通过自研联邦学习框架，降低联邦学习模型拆分造成的精度损失。
- **在特定区域或领域范围建立数据生态，通过数据运营为用户提供丰富的数据资源。**医疗隐私计算应用落地的关键是数据资源，厂商需要在特定区域，如省市级内，或特定领域，如针对某一疾病的研究，联合卫健委、医院、医保局、医药公司等多方建立丰富的数据生态，并提供数据运营服务。

- **隐私计算解决方案具备较高的安全性。**厂商需要通过提供高等级的数据加密技术、完善平台系统的安全性设计等提高解决方案的安全性。并获得权威测评机构的安全标准测试。

入选标准：

1. 符合医疗隐私计算解决方案的厂商能力要求；

2. 近一年在该市场服务客户数 3 家以上；

3. 近一年该市场相关服务收入规模在 200 万元以上。

代表厂商评估：

（注：以下代表厂商评估均按厂商简称首字音序排序）

锘崴科技

厂商介绍：

锘崴科技成立于 2019 年，是一家专注隐私保护计算技术的服务提供商，创始团队来自加州大学圣地亚哥分校 UCSD 等高校，具备深厚的隐私计算、生物医疗信息等领域的学术和实践经验，团队成员多来自 IBM、Google、Thermo 等世界五百强企业。锘崴科技开发了一整套自主、安全、可控的隐私保护计算平台产品，业务场景覆盖医疗、金融、保险、政务、安防等。

产品服务介绍：

锘崴科技的锘崴信隐私保护计算平台是拥有自主知识产权，已通过多项权威测评，安全、可控的隐私计算基础设施平台。平台包括了安全联邦学习系统、多方安全计算 MPC 系统、超融合沙箱（TEE）三个核心模块，可为用户提供隐私查询、隐私建模/分析、隐私推理等隐私计算功能，并兼顾性能、安全性、精度等多种要求。

针对医疗行业用户，锘崴科技提供了锘崴信医疗大数据保护计算平台（NovaVita）。作为锘崴信隐私保护计算平台的子平台，其能够满足医疗行业用户对数据源、分析功能、使用交互的差异化需求。

同时，锘崴科技也提供基于国产化 CPU、加速卡、可信执行环境的锘崴信一体机产品，为用户提供软硬件结合的隐私保护计算解决方案。

厂商评估：

锘崴科技的隐私计算产品与服务在面向医疗行业用户中，具备平台功能完善、使用体验良好、能保障多参与方的良好计算性能、提供面向医疗场景的专业分析功能、满足高精度和高安全性等优势。

锘崴科技的隐私保护计算平台能适配针对医疗行业用户需求的完善功能，并提供良好使用体验。

锘崴信医疗大数据保护计算平台（NovaVita)是面向医疗场景的隐私计算子平台，该平台基于锘崴科

技通用的隐私保护计算平台底座，在上层部署可编排的功能模块组，为医疗领域的不同客户提供匹配的隐私计算解决方案。该平台在帮助医药企业、医疗机构等提供安全高效的数据融合同时，也提供医疗大数据监管支撑服务，平台通过病例数据共享，结合 AI 学习模型等技术，赋能医学诊断、新药研发、基因分析等具体应用场景。

锘崴科技的隐私保护计算平台能够保障在大规模参与方（比如，10~100 方）的医疗场景中的良好计算性能。锘崴科技在平台底层架构的设计中，对多参与方联合计算场景进行了深度优化，在保证计算性能的同时，也解决了大规模的多方数据带来的通信性能下降问题。如在汇聚模型过程中，通过融合 SIMD 技术提高整体计算效率；在通信传输过程中，通过分布式压缩等方式，对通信效率进行重点优化；在隐私求交中，通过对称加密的解决方案对带宽进行优化等。

锘崴科技的隐私保护计算平台能提供针对医疗场景中各类专业度和复杂度较高的分析功能。锘崴科技基于在医疗领域多年沉淀的方法论，将特征选择、统计匹配、基因对齐、全基因组关联分析、医学影像分割与归类等多种医疗领域的分析方法与隐私计算技术相互融合并形成功能模块，能够实现对医学影像、基因数据等非结构化数据的计算。

锘崴科技的隐私保护计算平台能够满足一些特定医疗场景对模型的高精度要求。锘崴科技自研的联邦学习框架支持复杂的无损模型拆分方式，有效的弥补了通常的 Model Averaging 方式所造成的精度损失，能够保证拆分下的联邦学习模型的精度数值上完全等价于数据合并以后明文下的计算精度。

在产品安全性方面，锘崴隐私保护计算平台已通过了信通院联邦学习及可信执行环境基础能力专项测评，以及公安部隐私保护计算平台产品测评与国家信息系统安全等级保护三级备案与测评。此外，锘崴科技在平台中引入防止合作方之间串谋或篡改的能力，进一步强化了针对医疗场景的隐私计算安全性。

典型客户：

华西医院、新华医院、神州医疗、新加坡基因研究所、美国雷迪儿童医院

BaseBit.ai 翼方健数®

翼方健数

厂商介绍：

翼方健数（Basebit.ai）是“数据和计算互联网”的先行者，是一家专注隐私安全计算、人工智能和大数据的高科技公司。翼方健数以隐私安全计算为核心，服务医疗、政务、金融、保险、营销、科学等领域，建设在数据安全和个人隐私保护基础上的数据开放生态和数据共享协作环境，并在此基础上发展人工智能的能力，为行业赋能。

产品服务介绍：

翼方健数技术的特点是针对数据跨域流通的全流程，提供一套全栈的技术解决方案。通过隐私安全计算平台翼数坊 XDP，实现数据分享和价值获取的能力，核心模块包括分布式文件系统 XFS、计算资源调度与适配引擎 XEE、高效的数据发现与整合模块 DaaS 以及为不同信任假设场景储备的安全计算技术路径 PCT，利用全栈技术产品保证数据隐私和安全的同时，解锁数据价值。翼数坊 XDP 平台具备数据全生命周期管理、坚实的隐私安全计算技术体系、数据驱动的差异化 AI 应用三大核心能力。

在医疗健康领域，通过隐私安全计算与人工智能结合，为医疗机构、科研机构、生物医药企业提供端到端的全链条数据解决方案。

针对有数据清洗与治理的医疗行业用户，翼方健数还提供了基于人工智能的高效数据治理工具 DataWand。

厂商评估：

翼方健数旨在以隐私计算为核心，打造数据和计算互联网（IoDC，Internet of Data and Computing），提供贯穿数据全价值链的全栈技术解决方案，并在医疗行业丰富的落地案例、自研的隐私计算平台、面向多行业多场景的 AI 能力、通过 IoDC 提供数据和算力资源、平台安全性等方面具备优势，在隐私计算医疗行业中处于领先水平。

结合隐私计算与人工智能，翼方健数搭建了从医疗数据到智能应用端到端的能力，并且服务医疗多场景。例如基于医学大脑打造的以智慧病案为核心的一系列智能应用、针对医保或商保的风控解决方案、数据驱动的 AI 制药、真实世界研究、多模态组学数据分析协作、院内数据资产管理平台、传染病防控等围绕数据的医疗数字产业化解决方案。隐私计算的目标是为客户解锁数据的价值，在医疗健康领域，尤其是针对各级各类医疗机构，需要具备医疗领域的全栈技术包括从数据汇集到数据治理，从隐私计算到智能工具模型建设，再到最终形成各种智能应用在不同场景下提供落地的服务。翼方健数建立了这样的端到端能力，并在诸如瑞金医院等头部三甲医院实现以数据驱动的未来智慧医院的建设。

在翼数坊 XDP 平台中，进行数据安全存储、汇聚与发现、计算资源调度及隐私计算技术，能够从数据中获取价值，实现数据要素全生命周期的管理和流通。内置多种自研的隐私计算技术，能够满足不同安全信任假设和计算复杂度场景的用户需求。安全沙箱 XSSBox 可为单体平台提供零信任的本地计算环境；可信执行环境 XTEE 可为 XDP 平台内和平台间的计算任务提供基于硬件的可信执行环境；自研的联邦学习框架 XFL 支持包括横向、竖向和联邦迁移学习等多种主流算法，性能、模型精度和安全性优于主流开源框架；自研的密文计算框架 SXCE 能集成 MPC/FHE/DP/ZKP 等多种隐私计算技术，可用于不同精度和性能要求的密文计算，也可配合联邦学习，加强联合建模的安全性。

翼方健数具备适用医疗场景的 AI 模型和医疗知识库，能够处理复杂的多模态医疗数据。医学知识库基于机器学习、知识图谱技术构建了 200 万+医学概念、2000 万+医学关系、10 万+医学推理规则、500 万+互映射医学编码。平台内置了大量医疗领域自主研发的 AI 模型，如病历后结构化、传染源发散传播、辅助诊断、辅助检查/用药、影像病灶识别、医保欺诈监测、DRG/DIP 智能费控等，为各医疗场景实现数据驱动赋能。

此外，基于翼数坊 XDP 构建的 IoDC 能够帮助用户触达更多的数据和算力资源。翼方健数通过隐私计算“数据可用不可见”的能力，在保护数据隐私安全的前提下，通过构建数据网络，帮助数据在可管控、可度量且受隐私安全保护的前提下为人工智能提供数据上的助力。在翼方健数构建的 IoDC 中，通过平台的隐私计算能力，以及分布式文件系统、数据发现与整合、计算资源调度与适配等功能，每个节点都具备了完整的数据价值实现能力。一方面，用户可以通过 IoDC 使用来自各类政务和医疗机构的授权数据。例如，在湖北宜昌市，通过打通多个政企内外部数据源并跨平台联合计算，进行传染病多点触发预警。通过政企数据融合，各方数据协作，利用不同数据源筛选出传染疾病的高风险人群，精准筛选、消除误报，实现数据驱动的智能传染病防控。另一方面，通过 IoDC 调配超算中心、高校的数据和算力资源。例如翼方健数与南京江北新区生物医药公共服务平台合作，

调用数据和算力资源，推进区内 IoDC，可以一站式解决生物医药产业的科研、生产和临床转化、药物研发等实际问题。

安全性方面，翼方健数能充分满足医疗用户对数据安全合规的需求。翼方健数参与制定中国通信标准化协会、中国信通院组织的多项隐私计算安全、互联互通标准，翼数坊 XDP 平台已通过信通院“可信执行环境”、“联邦学习”、“多方安全计算”的相关能力测评以及健康医疗大数据可信选型评估。

典型客户：

宜昌市卫生健康委员会、厦门市健康医疗大数据管理中心、上海交通大学医学院附属瑞金医院、四川大学华西第二医院、中山大学肿瘤防治中心

3.4 隐私计算平台

定义：

隐私计算平台，是指基于安全多方计算、联邦学习等多种隐私计算技术，在为数据提供隐私保护的前提下，实现数据在流通中可用不可见的平台型工具。隐私计算平台具备通用的隐私计算技术服务能力，能够支撑企业用户构建各类隐私计算应用解决方案。

终端用户：

金融、政务、医疗、零售、电信、交通等各领域企业或机构的 IT 部门、大数据部门、科技创新部门

核心需求：

随着数据成为各行业企业创新业务、优化运营管理的关键要素，跨组织的数据流通共享成为企业越来越重要的需求。与此同时，《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规的陆续出台，为数据流通增加了诸多合规要求。因此，近年来各行业众多企业和机构都开始关注隐私计算，并希望搭建隐私计算平台，为进一步探索隐私计算的应用场景构建基础设施。企业对于隐私计算平台的核心需求通常包括：

- **具备较高的通用性。**企业潜在应用场景非常广泛，但在平台部署初期这些应用场景往往不够明确。因此，企业需要平台具备较高的通用性，能满足企业未来潜在的多种应用场景和功能需求。
- **操作方式灵活。**不同隐私计算应用场景的定制化程度存在差异，从调用算子来组合计算流程，到自定义计算流程，其对于用户技术水平要求也不同。因此，企业需要平台具备多种操作方式，灵活满足用户需求。
- **易于部署和集成。**一方面，企业希望隐私计算应用能快速落地并产生效果，因此需要解决方案能以便捷和快速的方式进行部署；另一方面，很多企业已经建立了较复杂的业务和 IT 系统，因此需要隐私计算解决方案能在对原系统改造尽量小的前提下，与原系统集成。
- **具备较高的性能。**在联合建模、联合统计分析等离线场景中，随着数据规模的增加，以及应用场景的丰富，其计算性能会受到制约；而在联合预测、匿踪查询等实时性要求较高的场景中，随着请求量的增加，计算时延也会逐渐显现。企业需要平台能在这些场景中具备较高的性能。

- **具备较高的安全性。**为保障数据资产安全，以及为满足相关法律法律的要求，企业需要平台在数据安全保护、系统环境、计算流程的可解释性等方面满足较高的安全性要求。

厂商能力要求：

- **平台在隐私计算技术和系统功能方面具备通用性。**在隐私计算技术方面，平台需要具备联邦学习、多方安全计算等多种隐私计算技术能力，能支撑联合建模、联合统计、隐私求交、匿踪查询等多种应用场景；在系统功能方面，平台需要将系统功能模块化，支持用户根据需求自助增加功能模块，如区块链存证、AI 计算、SQL 等模块。
- **平台具备灵活的操作使用方式。**一方面，平台需要将多方安全计算、联邦学习等算法拆分为细化的算子，支持用户根据需求以图形化的方式组合算子，构建计算流程；另一方面，平台还需要支持一些用户在定制化程度更高的场景中采用 Python 和 SQL 等方式编译计算脚本，自定义计算流程。
- **平台能被快速部署和集成。**在部署方面，除了本地部署模式，平台需要提供敏捷化的部署和交付方式，如平台采用云原生架构，并支持容器化的交付方式；以 SDK 或 API 的方式支持用户快速构建隐私计算应用；在与原系统集成方面，平台需要提供组件化和接口化服务支撑隐私计算平台与原系统之间在数据、账号、日志等方面快速对接。
- **平台在各类离线和实时场景中具备较高的性能。**在离线场景中，平台需要支持大规模分布式计算和硬件加速能力，提高计算性能；在实时场景中，平台需要在通信效率上做深度优化，并保证实时计算的稳定性，降低实时计算的时延。
- **平台具备较高的安全性。**厂商需要通过提供完善的数据加密技术、完善平台的权限控制等方式提高平台的安全性；并需要支持算法流程可视化，以及支持接入第三方流量审计工具对数据用途进行验证等方式提高计算流程的可解释性和可信度。

入选标准：

1. 符合隐私计算平台的厂商能力要求；

2. 近一年在该市场服务客户数 5 家以上；

3．近一年该市场相关服务收入规模在 500 万元以上。

CHAPTER

04

入选厂商列表

4. 入选厂商列表

	厂商	简称	市场
B	百度智能云	百度点石	金融隐私计算解决方案 政府及公共服务隐私计算解决方案 医疗隐私计算解决方案 隐私计算平台
C	冲量在线 IMPULSEONLINE	冲量在线	金融隐私计算解决方案 政府及公共服务隐私计算解决方案 隐私计算平台
D	洞见科技 INSIGHTONE	洞见科技	金融隐私计算解决方案 政府及公共服务隐私计算解决方案 隐私计算平台
F	富数	富数科技	金融隐私计算解决方案 政府及公共服务隐私计算解决方案 隐私计算平台
G	光之树 points technology	光之树	金融隐私计算解决方案 政府及公共服务隐私计算解决方案 隐私计算平台
H	華控清交 TSINGJIAO INFORMATION SCIENCE	华控清交	金融隐私计算解决方案 政府及公共服务隐私计算解决方案 隐私计算平台
L	蓝象智联	蓝象智联	金融隐私计算解决方案 政府及公共服务隐私计算解决方案 隐私计算平台

	零数科技	零数科技	政府及公共服务隐私计算解决方案 隐私计算平台
M	蚂蚁集团 ANT GROUP	蚂蚁摩斯	金融隐私计算解决方案 隐私计算平台
N	锘崴科技 NUCWEI TECH	锘崴科技	金融隐私计算解决方案 政府及公共服务隐私计算解决方案 医疗隐私计算解决方案 隐私计算平台
R	RealAI 瑞莱智慧	瑞莱智慧RealAI	金融隐私计算解决方案 隐私计算平台
S	数牍 sudo	数牍科技	金融隐私计算解决方案 隐私计算平台
T	腾讯云	腾讯云	隐私计算平台
	同盾科技 www.tongdun.cn	同盾科技	金融隐私计算解决方案 政府及公共服务隐私计算解决方案 隐私计算平台
	TONGTAI 同态科技	同态科技	金融隐私计算解决方案 政府及公共服务隐私计算解决方案 隐私计算平台
U	UCLOUD优刻得	UCloud优刻得	政府及公共服务隐私计算解决方案 医疗隐私计算解决方案 隐私计算平台
W	WeBank 微众银行	微众银行	金融隐私计算解决方案 隐私计算平台

X	CLUSTAR 星云	星云Clustar	金融隐私计算解决方案 隐私计算平台
Y	BaseBit.ai 翼方健数	翼方健数	金融隐私计算解决方案 政府及公共服务隐私计算解决方案 医疗隐私计算解决方案 隐私计算平台

5. 关于厂商全景报告

- 爱分析厂商全景报告面向数字化市场的甲方用户，由爱分析定期撰写并公开发布，为甲方采购旅程中的数字化规划、厂商选型等环节，提供决策依据和支撑。
- 报告提供所覆盖领域的数字化市场全景地图、特定市场定义与入选标准，以及入选厂商列表、代表厂商评估等研究成果。
- 甲方用户可以依据入选厂商列表，拟定潜在供应商名单，并通过爱分析第三方评估，了解厂商在特定市场的产品服务优势，选择合适的厂商进行选型。

6. 关于爱分析

爱分析是中国领先的数字化市场研究与咨询机构，成立于中国数字化兴起之时，致力于成为决策者最值得信任的数字化智囊。

凭借对新兴技术和应用的系统研究，对行业和场景的深刻洞见，爱分析为数字化大潮中的企业用户、厂商和投资机构，提供专业、客观、可靠的第三方研究与咨询服务，助力决策者洞察数字化趋势，拥抱数字化机会，引领中国数字化升级。

7. 研究与咨询服务

技术研究

新兴技术研究，厂商能力调研，助力数字化最优决策

客户洞察

企业用户需求及实践调研，辅助制定业务与市场策略

行业研究

行业数字化趋势与实践研判，辅助业务与战略决策

商业研究

基于研究、数据和案例调研积累，辅助业务可靠落地

品牌&营销

权威背书，树立行业地位；教育市场，精准触达客户

投资研究

成熟方法论，一手数据，助力研判机会、稳健投资

联系我们

联系人：李喆

邮箱：lizhe@ifenxi.com

手机/微信：135-2162-2835

8. 法律声明

ifenxi

咨询/合作

微　信：ifenxi888

网　址：www.ifenxi.com

地　址：北京市朝阳区酒仙桥南路2号院东风kaso4层406

如欲了解更多爱分析精彩洞见
请关注我们的微信公众号

ifenxi

专 注 数 字 化