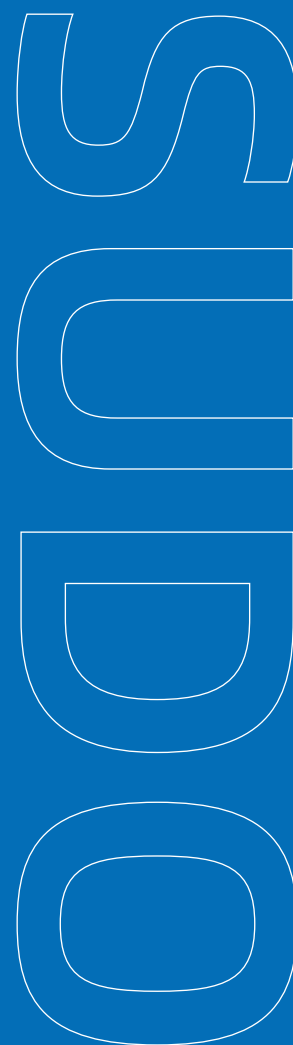


隐私计算 创造数据使用新范式

sudoprivacy.com

数牍科技



为数据要素市场发展创造更好的流通环境

目录

Contents

01-02

公司简介

ABOUT US

03-04

数牍科技团队

SUDO TEAM

05-08

市场背景

MARKET SITUATION

09-10

核心产品及服务

CORE PRODUCTS AND SERVICES

11-12

应用场景

APPLICATION SCENARIOS

13-22

解决方案

SOLUTIONS

23-26

业内影响力

MARKET IMPACT

SUDO CHRONICLE OF EVENTS

数牍科技大事记

2016-2019 — 2019 ————— 2020

2016-2019

团队成员在Facebook
从0-1主导实践TB级数
据隐私计算项目

2019.10

数牍科技第一版完
全国产化自主研发
隐私计算产品上线

2020.9

在多个国有银行及股
份制银行开展隐私计
算试点工程项目

获得HICOOL全球创
业大赛优胜企业奖

获得浦发银行金融科
技创新大赛金奖

2020.11

与中国信通院、阿里
安全共同发布国内首
个隐私计算技术研究
报告

2019.3

获得红杉中国种子
基金数千万天使轮
投资

2020.5

获得招商局创投、
红杉中国、红点中
国近亿元PreA轮
投资

2020.10-11

成为中国联通隐私计
算平台技术合作方，
率先落地行业内TB
级隐私计算商用项目



2021

2021.4

联合中国信通院、阿里安全、腾讯研究院、智联出行研究院、工商银行等共同撰写《隐私保护计算与合规应用研究报告(2021年)》

2021.5

入选中国电子工业标准化技术协会信息技术应用创新工作委员会

2021.6

通过国家金融科技测评中心“多方安全计算金融应用检测规范”认证

2021.7

通过中国信通院“卓信大数据计划-联邦学习安全专项”认证

联合中国信通院发布《隐私计算白皮书(2021)》

2021.9

与中国联通、工商银行、北京银行开展基于隐私计算的项目合作

2021.10

获得纪源资本、上海人工智能产业基金、红杉中国等新一轮投资，数牍A轮融资累计超3亿元

获评国家高新技术企业

获评2021中国明日之星、海淀明日之星称号

2021.11-12

成为上海数据交易所、西部数据交易平台首批签约数商

深度参与深圳数据交易所关键技术预研项目，并将作为深圳数据交易所首批数据服务商之一参与数据交易服务

ABOUT SUDO PRIVACY

关于数牍科技

数牍科技成立于2019年，是国内较早以系统性综合工程的视角实现隐私保护技术服务的企业。公司以“为数据要素市场发展创造更好的流通环境”为愿景，以“严格的隐私保护、数据安全前提下的共享和利用”为目标，基于多方安全计算、联邦学习和分布式系统等隐私计算技术，致力于打造具有完全自主知识产权、自主可控的隐私计算平台，助力政府间、政企间和企业间进行安全高效的数据协作，释放数据价值。

愿景

为数据要素市场发展创造更好的流通环境

使命

创造数据使用新范式

价值观

开放透明、崇尚行动、追求极致、赢得信任

作为国家高新技术企业，数牍科技拥有数十项知识产权，并获得公安部、工信部、国家金融科技测评中心等国家部委和权威机构的多项认证，成为行业首批通过信通院金融场景隐私保护计算平台测评的公司，已与多家政府单位、监管机构、研究机构等联合制定了十余项数据安全协作相关标准、数据分级分类管理指南和隐私计算相关技术要求与测试方法，并牵头编写多篇行业白皮书、研究报告等。

数牍科技率先实现TB级隐私计算工程落地，助力北京、上海、深圳等多地政府，中国联通、工商银行、北京银行等大型企业实现安全高效的数据协作，在风控、营销、集团内协作、智慧城市等场景落地应用。

创始团队



宋一民

创始人兼CEO

Texas A&M University 网络安全领域理学硕士

北京金融科技产业联盟监管科技专委会副主任委员

北京金融科技产业联盟分布式数据库专委会委员

2021行业信息化创新人物

拥有网络安全、云计算和数据工程多年研究和管理经验，专注隐私计算领域。先后在Facebook广告和隐私部门，作为技术主管主导了Instagram广告服务、Universal广告服务、Signal/Identity Growth等大型项目，从0到1主导了Facebook与多家世界500强企业的数据协作和隐私计算项目。



蔡超超

联合创始人兼CTO

加州大学洛杉矶分校（UCLA）机器学习博士

信通院互联网新技术新业务安全评估专家

北京金融科技产业联盟人工智能专委会委员

拥有机器学习、联邦学习多年研究和工作经历。先后于Amazon、Facebook担任机器学习团队负责人，负责推荐算法、用户画像、广告转化通道和模型学习等，作为技术领军人物主导了Cross-Device Graph, User Profile Traits Prediction等项目，获得Facebook Distinguished Equity称号，在机器学习、联邦学习等领域拥有30多项专利。

研发团队

数牍科技核心技术成员均来自Facebook、Google、Amazon、Microsoft等企业，70%以上具有研究生学历，其中逾20%具有博士学位，包括多个ACM获奖者。团队在密码学工程、分布式计算、联邦学习、数据科学和数据工程、网络安全等领域具有10年以上隐私工程落地经验，并已具备了国际领先的隐私计算技术和工程实践能力。

20% +
博士学位

10年 +
隐私工程落地经验

70% +
硕士学位



数据要素市场稳健发展 顺应国家战略

大数据作为生产资料，在推动经济发展，促进社会治理和公共管理方面起着重要作用。数据作为重要的生产要素，只有在流通中才能发挥其最大价值。因此，安全共享和转化是政策导向，也是大数据和数字经济发展的关键。

为响应国家大数据战略，目前中央部委、各级政府、央企、国企都在大力发展大数据业务，充分发挥大数据在推动产业转型、提升国家、社会治理现代化水平等方面的重要作用。



- | | |
|--------------|---|
| 2016年 | 《中华人民共和国网络安全法》规定，网络运营者未经被收集者同意，不得向他人提供个人信息，但经过处理无法识别特定个人且不能复原的除外。 |
| 2017年 | 习近平总书记在十九届中共中央政治局第二次集体学习中强调推动实施国家大数据战略，加快建设数字中国。 |
| 2020年 | 《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》中首次将数据作为重要生产要素。 |
| 2021年 | 2021年，国家十四五规划五次提到“数据安全”，数据安全成为国家安全战略。9月1日正式实施的《数据安全法》，坚持保障数据安全与促进数据开发利用并重的原则。11月1日《个人信息保护法》正式落地，对于个人重要信息、数据进行了界定，也明确了六大场景中各方的法律关系和相应要履行的义务。 |

数据价值挖掘的需求空间

当前，我国的大数据产业尚处于起步阶段，数据流通与协作仍面临诸多难点，比如数据在管理和使用上的安全性和可用性难题，包括数据孤岛、数据泄露及滥用、数据定价难等。



隐私泄露问题频发 数据协作面临信任鸿沟

在传统的协作过程中，由于数据所有权不清晰、数据所有方和使用方安全意识欠缺、技术手段不足等原因，造成数据泄露或滥用，甚至形成数据被恶意窃取、转卖等黑色产业链。大规模数据泄露事件一旦爆发，一方面影响公共信息安全，另一方面严重损害企业声誉及数据资产安全，数据协作产生信任鸿沟。



法律法规对数据安全协作 提出了更高要求

近年来，国内关于网络安全、个人信息保护、数据安全的法律法规不断出台，对数据的采集、共享、挖掘等生产活动进行规范要求，如《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等，数据要素必须在遵守法律法规、履行数据安全保护义务的前提下有序开放共享。



信息孤岛问题突出

相关法律法规和监管制度的要求各政府部门之间、企业之间、政府和企业间数据安全有序融合，但由于缺乏有效的技术手段，导致大量数据存在“不愿公开、不敢公开、不能公开、不会公开”，而已开放的数据也因格式标准缺失无法进行关联融合，形成孤岛。



新技术应用场景受限

数字经济、智能经济发展的基础在于数据，底层数据缺失或样本不足，数据分析也就无从谈起。应用层面，数据的价值在于开放共享，由于缺少数据的样本和维度，在很大程度上制约了人工智能等新兴技术及相关场景应用的发展。

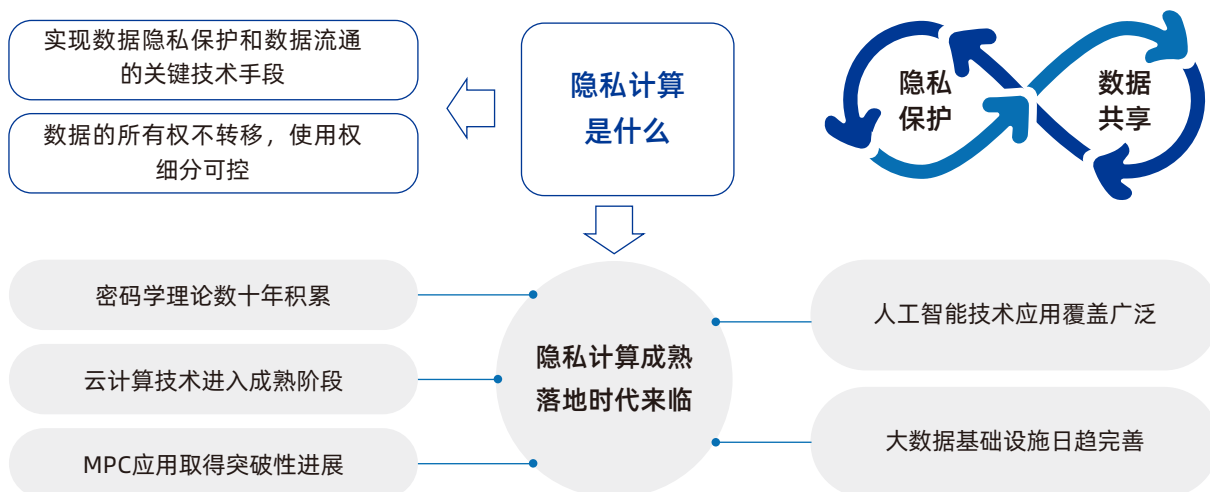


隐私计算技术提供 行之有效的解决路径

在推动数字经济发展，加强数据要素流通，助力大数据产业升级方面，构建一个安全的数据协作、流通的技术环境具有极大的战略意义及紧迫性，如何在保证数据的私密合规使用的前提下，实现多方数据协作分析结果精准无误，达到数据隐私保护与数据价值挖掘的有效平衡？

作为数据安全协作的关键技术手段，隐私计算技术可保障数据的所有权不转移，使用权细分可控，综合多方安全计算、联邦学习、可信执行环境、同态加密、差分隐私等前沿技术，能够对数据的采集、存储、使用、转让、共享及公开披露进行区分管理。

Gartner将隐私计算技术列为2022年需要探索的重要战略技术。Gartner预计到2025年，60%的大型企业机构将使用一种或多种隐私增强计算技术。在数据、软件或硬件层面保护个人和敏感信息的PEC技术能够在不影响保密性或隐私的情况下安全地共享、汇集和分析数据。





隐私计算是包含人工智能、密码学、数据科学等多领域融合的技术体系

多方安全计算 (MPC)

多方安全计算主要针对无可信第三方情况下，安全地进行多方协同计算问题，同时保证各方输入信息的隐私安全。

优势：安全理论完备、通用性高、性能不断提升。

差分隐私 (DP)

差分隐私是一种通过对原始数据加入噪声，在损失部分数据精度的前提下保护数据隐私的技术。

优势：计算和通信性能与直接明文计算几乎无区别，可以对数据结果和输入数据进行保护。

联邦学习 (FL)

在原始数据不出库的前提下完成建模工作任务，主要用于AI模型训练和预测。

优势：效率较高，综合运用MPC、DP、HE方法。

同态加密 (HE)

对加密数据进行处理得到一个输出，将这一输出进行解密，其结果与同一方法处理未加密的原始数据得到的输出结果保持一致。

优势：原始数据不暴露、可以隐藏运算，安全性高。

可信执行环境 (TEE)

通过软硬件方法在中央处理器中构建一个安全的区域，保证其内部加载的程序和数据在机密性和完整性上得到保护。

优势：通用性高，计算效率高。

区块链 (BC)

基于带时间戳的块链式储存、智能合约、分布式共识等技术辅助隐私计算。

优势：保证原始数据、计算过程及结果可验证。



数牍科技自主研发的隐私计算平台Tusita 助力数字经济新基建

数牍科技完全自主知识产权的隐私计算产品Tusita，基于自主研发的联邦学习建模、多方安全计算框架及大数据系统，已实现了包括多方安全匹配、多方数据分析、多方数据清洗、多方安全建模及报告、多方安全预测、数据匿名查询、ID隐私融合等的全流程的隐私计算。

平台帮助多方用户在原始数据无需暴露的前提下进行联合建模及计算，达到数据可用不可拥、用法及用量可监控的目的。



数据生命周期视角

数牍科技以数据生命周期为视角，结合多方安全计算、联邦学习、可信执行环境、差分隐私、同态加密等隐私计算技术，自主创新，研发出具有完全自主知识产权的隐私计算平台及多行业解决方案。



产品化思维

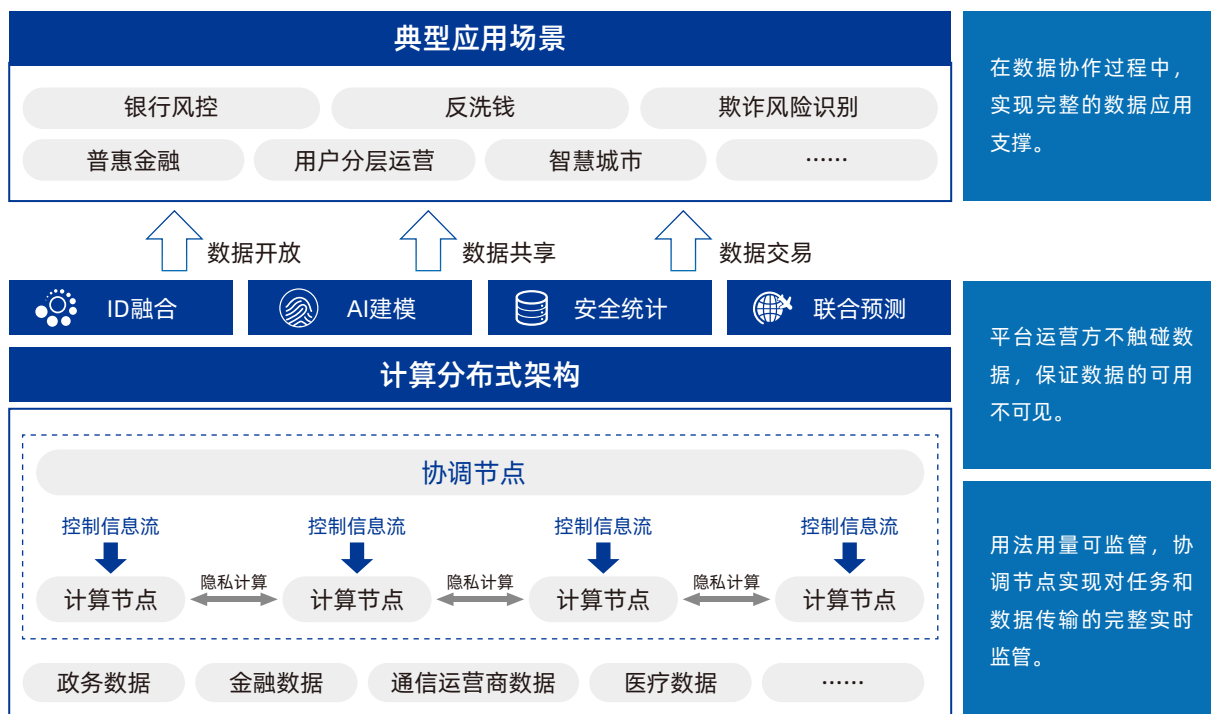
数牍科技较早使用产品化思维打造隐私计算平台及解决方案，并提出隐私计算综合工程。数牍科技提供中立、安全、高效的隐私计算产品及全栈技术服务，已具备工程化落地能力。



更好的数据助力更好的AI

在数据智能时代，人工智能等新一代技术的发展离不开良好的数据环境，数牍科技致力于数据要素市场的底层关键基础设施建设。

数牍Tusita隐私计算系统是以数据生命周期为视角多种技术的融合产品



平台优势

数牍科技自主研发的隐私计算平台，从系统架构、计算性能、业务支持等方面，帮助用户构建高性能、高可用的数据要素流通信任底座，并在此基础上实现灵活的隐私\敏感数据价值融通的解决方案。



完全自主研发，安全中立

计算分布式架构，用法用量可监管；
平台不参与计算，不触碰数据，不运营数据；
平台从授权管理、算法实现、结果输出等多个层面保护用户ID、特征、标签等核心数据。



完整的数据科学应用

可实现大规模无代码化规则标签能力、支持算法标签全流程可视化搭建，提高建模效率，灵活易用；
平台具有良好的可集成性，充分考虑了同数据中台、AI中台、区块链等平台的对接，极大降低隐私计算同现有技术环境的融合成本。



工业级落地能力

平台具备高可扩展性，支持快速实施部署和平台迭代；
支持亿级数据联邦学习建模能力，支持亿级数据隐私求交；
数据应用通信成本低，具备高并发、高实时性，毫秒级响应能力，满足多场景业务需求。

应用场景

通信

COMMUNICATION



政府

GOVERNMENT



金融

FINANCE



汽车

AUTOMOBILE



广告营销

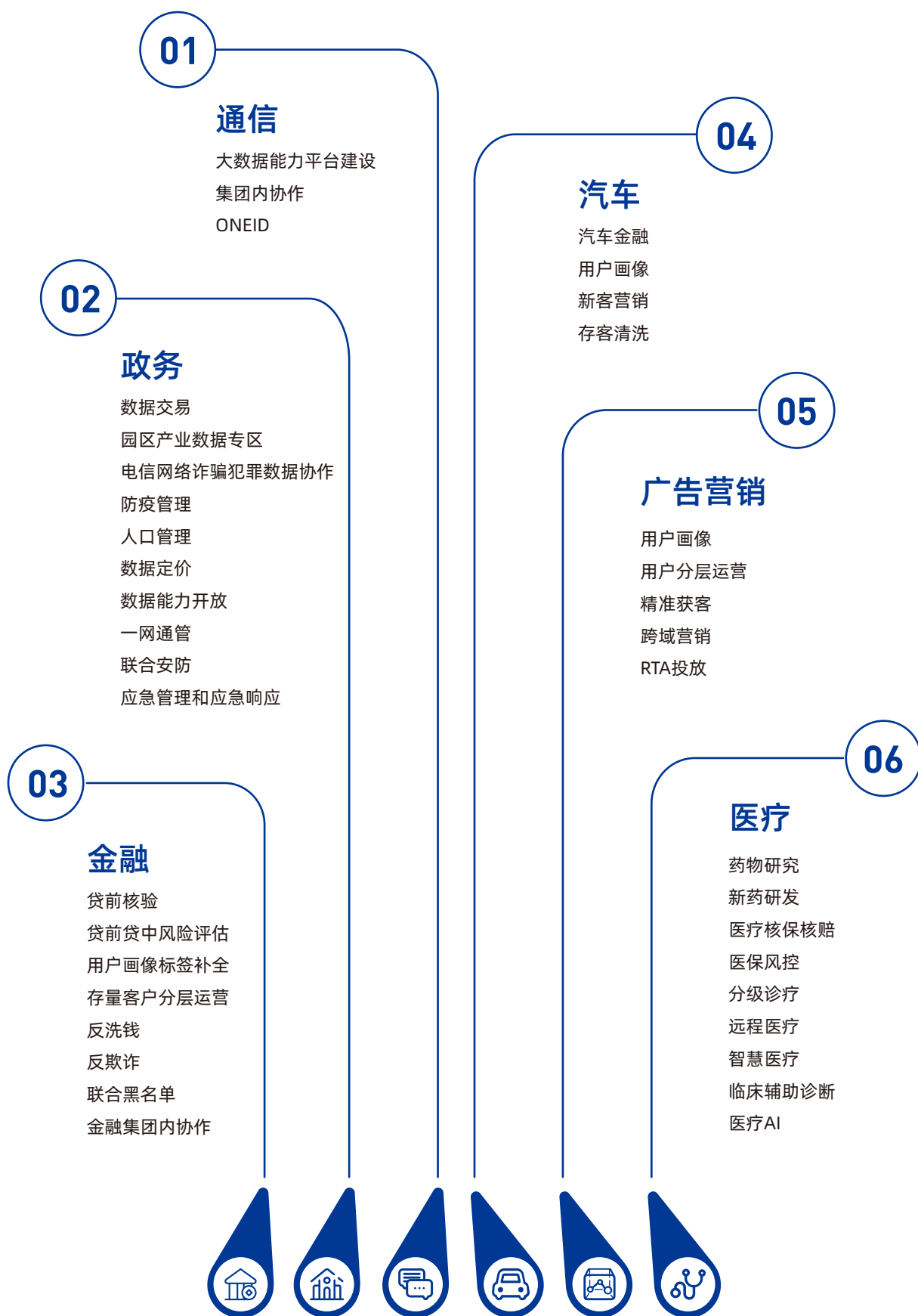
ADVERTISING MARKETING



医疗

MEDICAL CARE





解决方案

通信领域

通信运营商数据特征及数牍科技实践

数牍科技是行业内较早将隐私计算在通信领域落地应用的企业。

目前，数牍科技与中国联通、中国移动、中国电信均已建立紧密合作，在集团内大数据能力底座建设、多方数据协作、营销、风控、数据服务等多个场景进行应用探索与落地，并帮助通信运营商与政府、银行、保险、广告等多行业领域进行基于隐私保护的数据协作实践。

- 2020年11月，数牍科技中标联通大数据数据安全计算平台项目。
- 2020-2021年，数牍科技为运营商与政务、金融等领域协作方在营销、风控、集团内协作等领域提供基于隐私计算的解决方案。
- 2021年6月，由中国信通院与中国商务广告协会发起，联合三大通信运营商推出ONEID产品，数牍科技负责隐私计算技术研发及ONEID产品运营。
- 2021年9月，数牍科技中标联通研究院安全多方计算项目。

典型案例：数牍科技助力联通隐私计算平台建设



中国联通
大数据能力底座

含联邦学习、多方安全计算模块，实现多方加密计算的机器学习，可迭代验证，保护专有数据，实现多方数据源安全联合建模

在联通大数据公司数据科学研究平台建设项目中，数牍科技通过联合技术攻关的方式，帮助联通大数据实现了原始数据不出库情况下的“数据可用不可拥”，有效解决了数据孤岛问题。

基于隐私计算技术合作，联通大数据建立了以联通全网数据为基础，以安全合规的数据协作为支撑，面向政企数据融合应用的新型大数据服务平台——联通数享平台。在安全合规的前提下，为合作伙伴提供算力、算法支撑，能够为政府、企事业单位、各大科研教育机构提供便捷高效的大数据开发环境和一站式数据开发管理服务，大大降低了政府和企业对数据能力平台的建设门槛和数据科技的使用成本。

2020年联通大数据公司数据科学研究平台建设项目中标候选人公示

标包2:数据安全计算平台的功能采购与定制研发

北京数牍科技有限公司为第一中标候选人

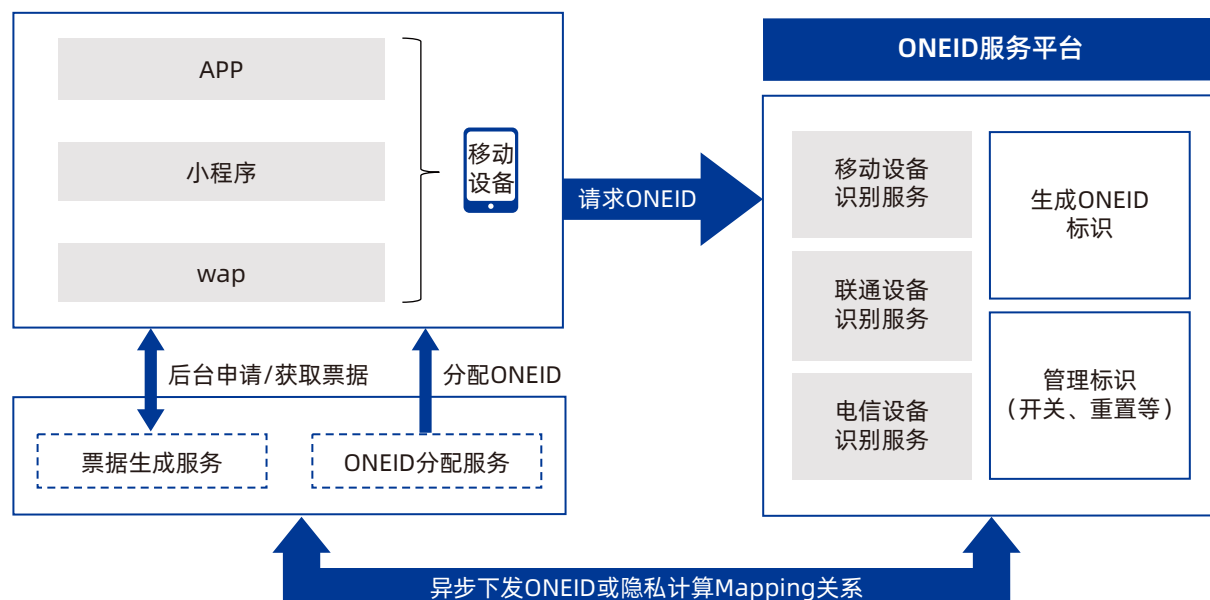
典型案例：数牍科技助力匿名ID体系-ONEID解决方案

目前，流量欺诈产业已经发展的相当成熟，刷量行为可以高度模拟真实用户的操作，使得视频网站、直播平台、广告联盟、搜索引擎、电商等难以有效应对。2021年6月，中国信通院和中国商务广告协会，联合三大通信运营商，由数牍科技参与技术研发及运营推广的匿名ID解决方案-ONEID正式发布商用，该方案解决了当前移动互联网面临的ID难点。



ONEID作为匿名反欺诈ID，可结合设备指纹技术，在广告监控等场景，实现流量反欺诈，识别虚假设备，严防虚假设备模拟的广告曝光、广告点击等行为，断绝虚假流量。

* 整个过程基于网络实现，不依赖操作系统，并且无需嵌入SDK。





政务领域

隐私计算助推政务数据要素安全流通

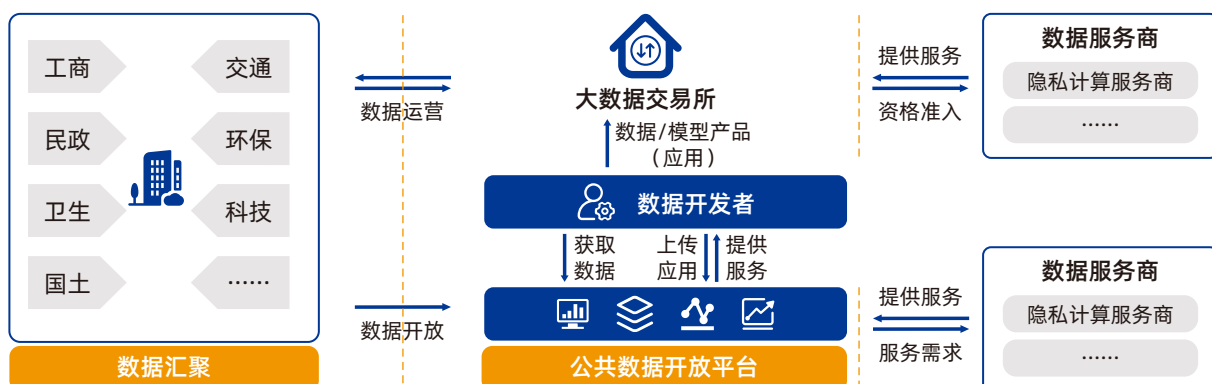
数据只有在共享、开放、交易中才能产生最大的社会价值。当前，共享数据多为宏观数据，应用价值有限，由于技术手段限制，政企数据、企业数据共享难以大规模实际应用，形成数据孤岛。

为了提升数据收集的协调能力，解决各部门之间数据协作难题，同时对于各方数据的用法和用量进行有效监管，数牍科技使用隐私计算技术，为政府机构提供增强数据协作的新型数据开放平台。



应用场景：隐私计算助力构建数据开发利用生态

当前，北京、上海、深圳、贵州等省市正持续探索数据要素市场构建，积极推动数据开放共享，通过搭建大数据交易所、公共数据交易平台等形式，促进数据流通，挖掘数据价值。隐私计算技术作为数据流通中的底层关键基础设施，已成为多地政府鼓励发展的创新技术之一。





(图片来源：新华社 方喆)

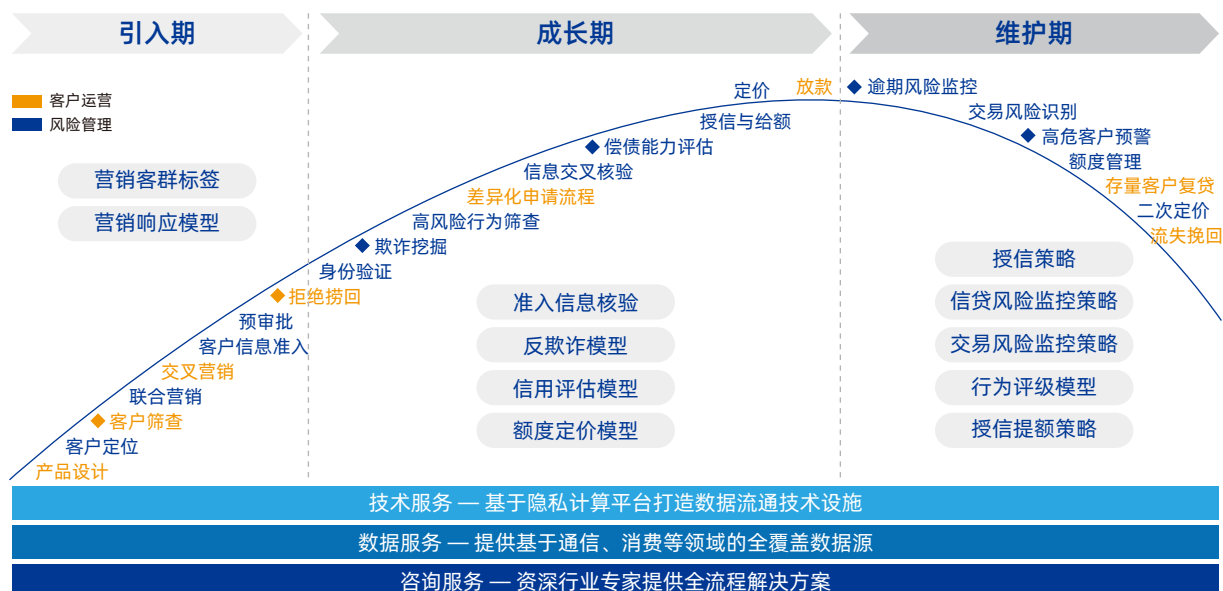
数牍科技将自主研发的隐私计算平台及关键技术成果应用到数据开放利用生态研究与建设中，已与北京、上海、深圳等多地政府机构展开技术研究及项目合作。2021年11月，上海数据交易所揭牌成立，数牍科技作为交易所首批数商签约。公司深度参与了深圳数据交易所关键技术预研项目，为数据交易所提供数据流通环节中的隐私计算技术支持，并将作为深圳数据交易所首批数据服务商之一参与数据交易服务。此外，公司还积极参与北京市大数据中心相关课题、数据流通分级分类指南撰写，并首批入选北京国际数据交易联盟成员单位。



金融领域

面向零售业务全生命周期的隐私计算技术及产品服务

数牍科技使用联邦学习等技术打造的Tusita隐私计算平台，在金融行业领域，可以支持面向零售业务全生命周期提供基于隐私计算的数据协同服务，特别在风控、营销、存量客户分层运营、集团内协作等场景帮助金融机构显著提升营销效率，降低运营成本。

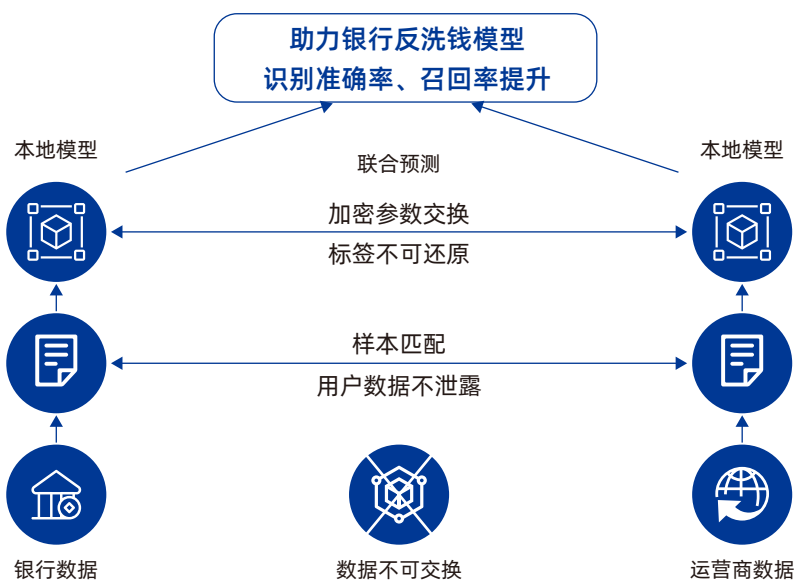


● 风控场景：银行引入通信运营商数据助力反洗钱、反欺诈模型

反洗钱模型增强

某银行反洗钱中心仅用自有的数据特征对洗钱客户的识别能力相对较弱，因此在现有的反洗钱模型基础上，急需引入运营商特征数据，丰富反洗钱模型。

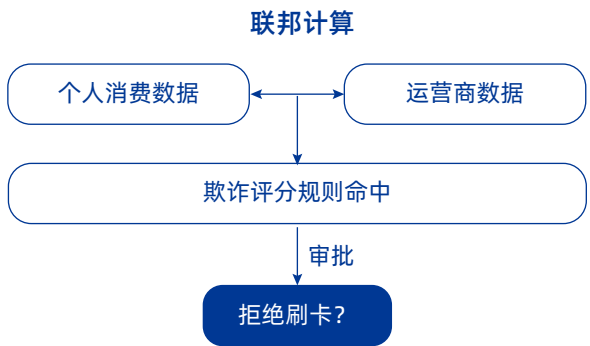
数牍科技通过隐私计算技术，为反洗钱场景引入运营商数据，使用用户电信诈骗场景等40余万样本数据，进行隐私计算联合建模。通过隐私保护集合求交、联邦学习等技术对双方用户ID进行隐私保护，在双方不交换原始数据的前提下，为反洗钱场景模型补充了更多有效数据。



信用卡消费反欺诈模型

当前，金融诈骗黑产业链逐步走向成熟化、专业化，结合移动互联网衍生出信用卡消费诈骗、套现、薅羊毛等上百种手段的欺诈方法，给银行消费反欺诈带来难点。

数牍科技通过隐私计算技术，让运营商的部分用户个人数据，在不出库的前提下和消费数据进行实时欺诈模型计算，大大提升了发卡机构的反欺诈能力。

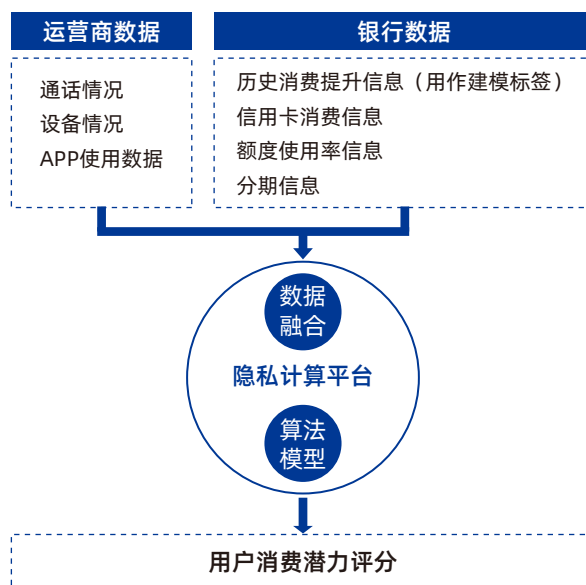


营销场景：银行用户消费潜力评分

银行在对所有用户营销过程中，由于数据维度不足，难免出现客户分层管理能力缺乏，营销资源浪费等现象。而银行在整合外部数据构建数字化获客模型的过程中，也面临着己方数据出库、触碰隐私保护相关法律法规的风险。

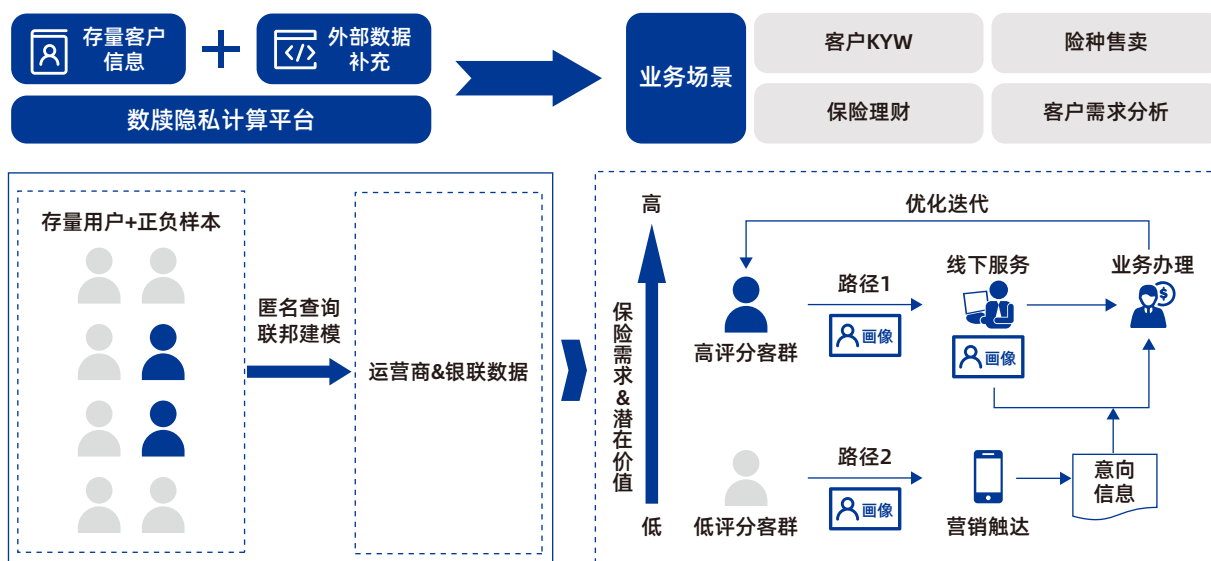
在信用卡用户存量精细化运营场景中，数牍科技隐私计算产品可以在数据不出库的前提下，基于银行历史和运营用户特征构建营销响应模型，对客户营销活动激活作出预测，进行客户分层管理，匹配营销策略和用户权益，促进存量用户价值提升。

数牍科技提供的基于隐私计算的技术服务，可以应用在银行、保险等行业的存量客户针对性经营活动触达，大型企业的会员客户针对性营销活动触达，大型企业的存量客户保有针对性营销活动触达等多种场景。



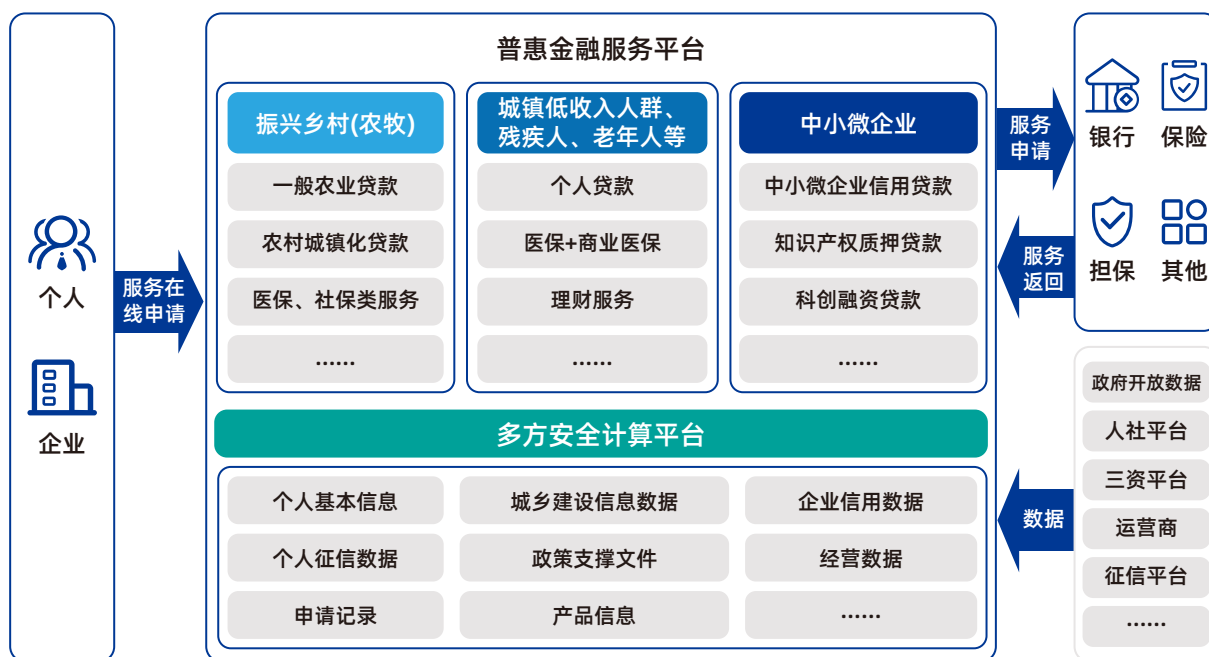
解决方案：财险客户高潜在转化名单输出

某财险公司具有大量的新客户及存量客户线索，在传统的营销方式下，公司基于自身数据对客户的运营分析效果有限，无法及时高效地触达意向客户。数牍科技可通过隐私计算技术引入外部合规数据，帮助财险公司完善用户画像，构建用户分层运营模型，基于业务场景开展对存量客户进行有效营销，提升企业用户运营效率。



● 应用场景：隐私计算助力构建普惠金融平台

为贯彻及落实国家政策，各地政府联合不同金融机构积极搭建普惠金融平台，为中小微企业及个人进行金融服务。隐私计算技术可以在确保个人和企业数据不泄露的前提下，帮助政府及金融机构间实现安全合规的数据协作，增强普惠金融平台对个人和企业的信用服务能力，助力构建普惠金融生态。

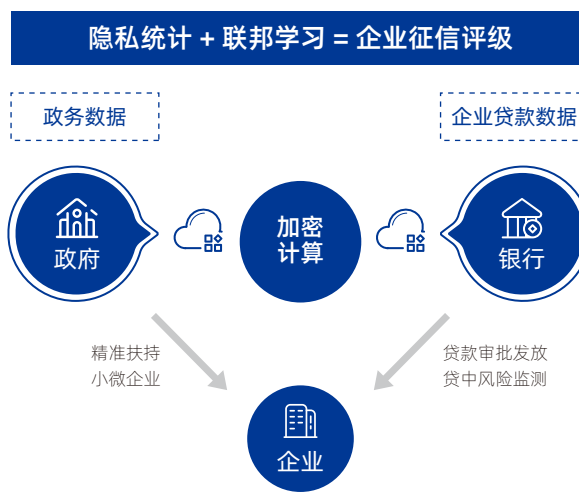


● 典型案例：某国有银行-政务数据企业贷中监控

数牍科技应用联邦学习等隐私计算技术，联合政务数据和国有银行企业贷款数据，在双方数据互不出库的基础上，共同建立联邦模型，辅助该行贷中管理能力提升，为分析企业信用风险和企业贷款良性运转提供支撑。

数牍科技在双方数据不出库前提下进行模型训练（联邦学习）和业务规则（隐私统计），打造企业征信评级，结合企业数据特征进行特征衍生、模型建立、风险评级等。

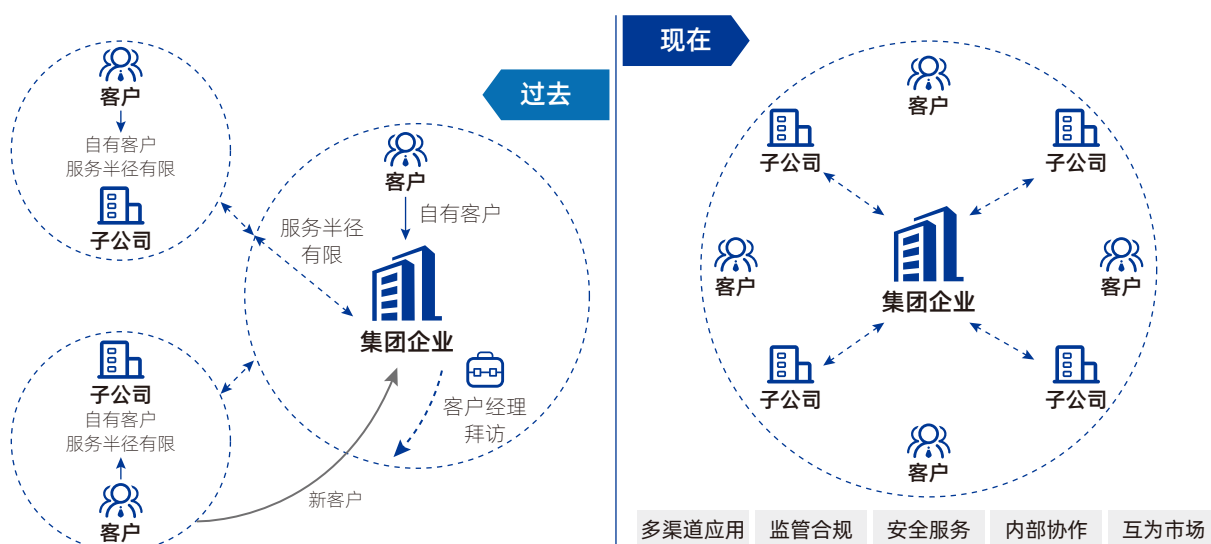
联邦学习模型比国有银行自有贷款监测模型的效果提升了4%，通过联邦学习技术引入政府数据，实现政府数据安全对外共享，显著提升了银行对企业贷款的贷中监测能力。



集团数据协作场景：集团内协作的数字化转型

在数字化建设过程中，由于大多数国内集团的子公司都是独立经营，集团各子公司间数据互不相通，无法真正做到内部协作、互为市场。为了提高集团数字化程度，提升企业管理和内部运营效率，越来越多的集团公司已经开始探索安全高效的数据协作模式。

数牍科技提供基于隐私计算技术的数据协作模式，帮助集团企业在合法合规的前提下打通集团内部数据，构建集团生态产业链的全链路经营新能力，真正实现集团内部协作、互为市场，提高经营效率，避免资源浪费。

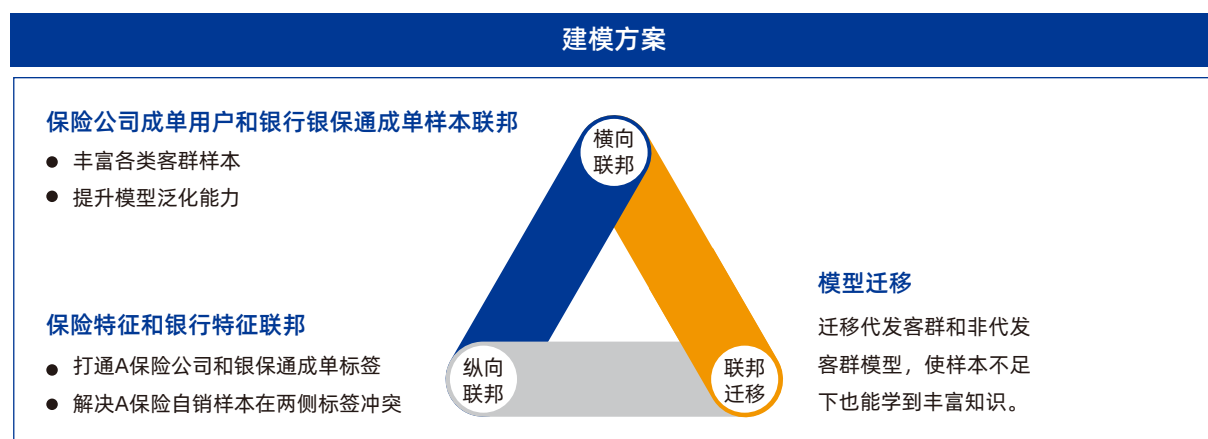


典型案例：某银行引入联邦学习技术助力保险子公司营销

某银行为其人寿子公司(如下分别简称A行、A保险)代销各类保险产品，已有多年成功运营经验，且在双方独立积累大量历史数据；现有保险营销模式更依赖于客户经理触达，且数据显示：银保渠道成功销售客群平均资产比保险自销渠道高很多；A行立项运用联邦学习技术实现A行内部数据打通(A行和A保险的客户数据和成单标签)，从5亿用户中挖掘潜在购险用户，辅助代理人展业。

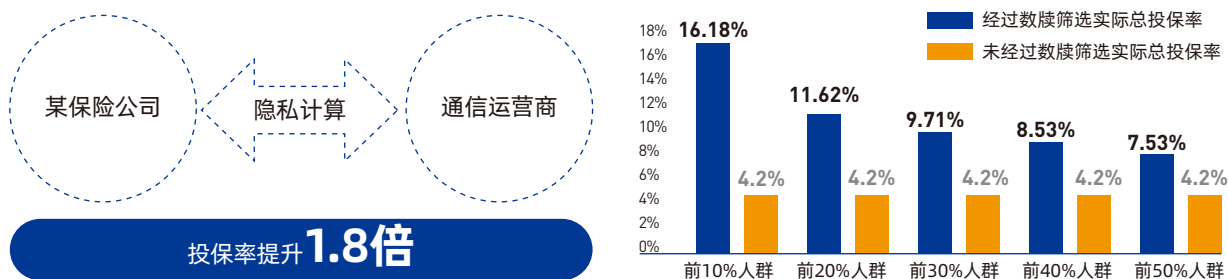
数牍科技发现保险销售除了关心潜在客户名单外，更需要相对应的潜在客户保险画像辅助代理人展业。因此，数牍科技根据该客户的实际痛点，提出基于联邦学习技术的客群探查解决方案。

数牍科技服务于A行的联邦学习解决方案在保险意向客户挖掘的场景中，相比银行自身非联邦学习解决方案在购买转化率上提升了16.4%。



典型案例：保险企业数字化运营

数牍科技为保险公司数字化赋能，通过引入外部数据将保险公司及运营商数据进行联合建模，对海量存量客户进行高效运营，通过保险公司历史样本10万条与运营商2.2亿活跃用户求交、特征匹配以及联邦建模，提升了投保转化率，避免保险公司用户数据和外部数据交互过程中的商业价值流失，模型结果可将投保率提升1.8倍，且模型开发时间 < 2小时。



汽车领域

典型案例：汽车线索挖掘与营销

某通信运营商联合数牍科技的隐私计算平台，应用联邦学习技术提出综合解决方案。该方案在不交换用户原始数据和标签的前提下，成功帮助某知名车企和通信运营商建立高质量的机器学习模型。该模型极大提高了分层模型的预测精度，提升了客户数据的利用效率和价值，降低了该车企的获客成本。该方案既解决了该车企对核心客户资产数据保护的顾虑，同时建立了打通数据孤岛下的数据交互解决方案。通过筛选高价值用户线索，提高企业运营效率。



落地成果

车企二次回访标定有效率提高 42.3% (41.8% → 59.5%)

	线索量	有效线索	有效率	历史有效率
区域1	894	564	63.1%	42.1%
区域2	962	576	59.9%	39.0%
区域3	496	255	51.4%	40.2%
区域4	782	415	53.1%	41.8%
区域5	235	148	63.0%	43.5%
区域6	277	213	76.9%	44.1%
合计	3646	2171	59.5%	41.8%



业内影响力

研究成果

- 联合中国信息通信研究院、阿里安全共同发布国内首个《隐私保护计算技术研究报告》及《隐私保护计算与合规应用研究报告》
- 联合隐私计算专委会发布《联邦学习金融应用白皮书》
- 联合隐私计算专委会发布《多方安全计算金融应用白皮书》
- 联合中国信息通信研究院云大所/隐私计算联盟发布《隐私计算白皮书》
- 联合中国信息通信研究院云大所/隐私计算联盟发布《隐私计算与区块链技术融合研究报告》



参与数十项隐私计算技术相关标准制定

积极参与央行金标委、中国信通院、中国电子标准化研究院、北京市经信局大数据中心、北京市金融科技产业联盟等国家部委、省市级政府、行业协会的标准制定（技术、监管、业务）及安全评估体系的建设试点，如：

- 参与中国电子标准化研究院《数据安全共享指引》标准制定
- 参与北京市经信局大数据中心《数据流通分级分类指南》制定
- 参与中国信息通信研究院二十余项标准制定：《基于多方安全计算的数据流通产品技术要求与测试方法》《基于可信执行环境的数据计算平台技术要求与测试方法》《联邦学习技术与应用技术要求》《电信和互联网数据对外合作安全管理实施指南》等



资质认证

- 公安等保三级测评资质认证
- 国家金融科技测评中心“多方安全计算金融应用技术测评”认证
- 中国信通院“卓信大数据计划-联邦学习安全专项”认证
- 中国信通院泰尔实验室“基于多方安全计算的数据流通产品基础能力专项”认证
- 国家高新技术企业认证
- ISO9001、ISO20000、ISO27001认证
- 软件企业认证、软件产品认证



信用认证

- AAA级信用企业
- AAA级诚信经营示范单位
- AAA级质量服务诚信示范企业
- AAA级重服务守信用企业
- AAA级重合同守信用示范企业
- AAA级重质量守信用企业
- AAA资信等级证书



资质荣誉

- HICOOL全球创业大赛优胜企业
- 浦发银行创新大赛“金奖”
- 中国信通院“隐私计算标杆案例奖”
- 2021数字政府方案案例创新奖
- “IDC中国FinTech 50”榜单
- 2021行业信息化创新企业
- 2021中国明日之星、海淀明日之星
- 2021年度人工智能最具价值创业公司TOP20
- 2021CB Insights中国“数据链路安全领航者”



行业权威技术联盟成员单位

- 中国电子工业标准化技术协会信息技术应用创新工作委员会成员企业
- 全国信息安全标准化技术委员会成员企业
- 中国通信标准化协会成员企业
- 北京国际数据交易联盟成员企业
- 中国网络空间安全协会成员企业
- 中国信通院“医疗科技安全实验室”成员企业
- 中国信息通信研究院隐私计算联盟成员企业
- 北京金融科技产业联盟成员企业
- 中关村金融科技产业联盟理事单位
- 中国电子商会数据资源服务创新专业委员会理事单位



部分合作伙伴





公司官网: <http://www.sudoprivacy.com>

联系电话: 010-8288 5402

商务咨询: business@sudoprivacy.com

市场合作: mkt@sudoprivacy.com

加入我们: recruiting@sudoprivacy.com

公司地址: 北京市海淀区优盛大厦A座18层

官方公众号



官方客服号

