AISWare MPC隐私计算平台

基于密码学、分布式计算等技术，实现在原始数据不出本地的前提下进行隐匿查询、安全求交、多方计算、联合建模等数据开放合作的产品。

产品概述
Overview

产品定位　解决企业数据协同计算过程中的数据安全和隐私保护问题实现数据不出域，安全高效地完成联合风控、联合营销等跨机构数据合作业务。

目标客户　广泛应用于运营商、金融、政务、医疗、零售等各行业。

产品简介　以数据管理、项目管理、程序编排、任务监控实现双方或多方的多方安全计算、联邦学习、匿踪查询、安全求交的数据流通。

核心功能
Core Functions

安全求交算子
获取双方的交集信息，无法获取交集之外的信息。保护两方数据不泄漏。

多方直接求交
通过两方及以上的参与方进行安全求交，以更多维度对数据安全融合，以得出求交结果。

智能运营驾驶舱
以中心节点与边缘节点实现数据价值流通，再分别对各方的数据集、项目、任务、资源等进行监控。

运营服务门户
数据持有者将数据开放，再产品特性能力，实现运营门户实现合作入驻的引流。

方案优势
Advantages

安全合规
数据不出域，从节点认证、算法认证、数据存取、密文计算、可信存证等多方面保护用户数据安全。

集成能力强
可集成多个厂商的隐私计算组件、区块链、数据中台，有助于平台运营方引入多样化的合作伙伴。

资源丰富
支持用户共享经过安全验证的算法和模型，可在生态内持续构建丰富的算法超市和模型仓库。

操作便捷
提供图形化IDE，支持拖拉拽方式进行程序编排，操作灵活便捷，提升程序开发效率。

定制开发
通过组件化方式，根据客户需求定制化的解决方案。

性能优异
采用分布式密文计算架构，数据通信成本低，实现密文计算的高并发、高实时、高可用。

AISWare MPC隐私计算平台

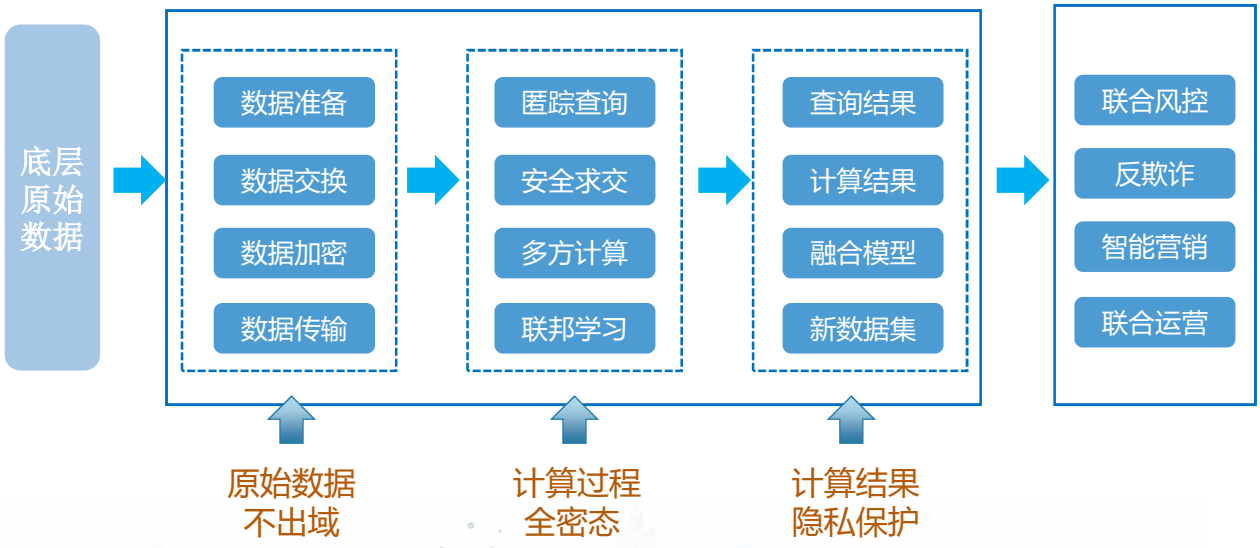
基于密码学、分布式计算等技术，实现在原始数据不出本地的前提下进行隐匿查询、安全求交、多方计算、联合建模等数据开放合作的产品。

应用成效
Key Figures

构建数据集管理、参与方管理、算子编排、协同计算、能力运营等多方安全计算全过程的能力体系，解决企业内外数据交互的安全问题，助力企业安全高效地完成联合风控、联合营销、联合科研等跨机构数据协同计算，充分挖掘企业数据资产价值，推动企业数字化发展。

产品价值
Core Values

隐私计算的核心功能是围绕着数据隐私的保护。将一个隐私计算的任务进行抽象化处理，可以呈现出一个包括输入、计算和输出的过程，使得原始数据不出域，保障数据流通过程，数据安全，助力合规，释放数据价值。



AISWare MPC隐私计算平台

基于密码学、分布式计算等技术，实现在原始数据不出本地的前提下进行隐匿查询、安全求交、多方计算、联合建模等数据开放合作的产品。

应用场景
Scenarios

匿踪查询

通过隐私计算，需求方可隐藏被查询对象关键词或客户ID信息，提供方提供匹配的查询结果却无法获知具体对应哪个查询对象。

安全求交

在不泄露原始数据额前提下，比对双方数据，并得出相同的部分。通过隐私计算，持有各自集合的两方来共同计算两个集合的交集。

联合统计

在不泄漏任何隐私数据的前提下，让多方数据共同完成某项计算任务(四则运算、比大小等)，并获得准确的结果。

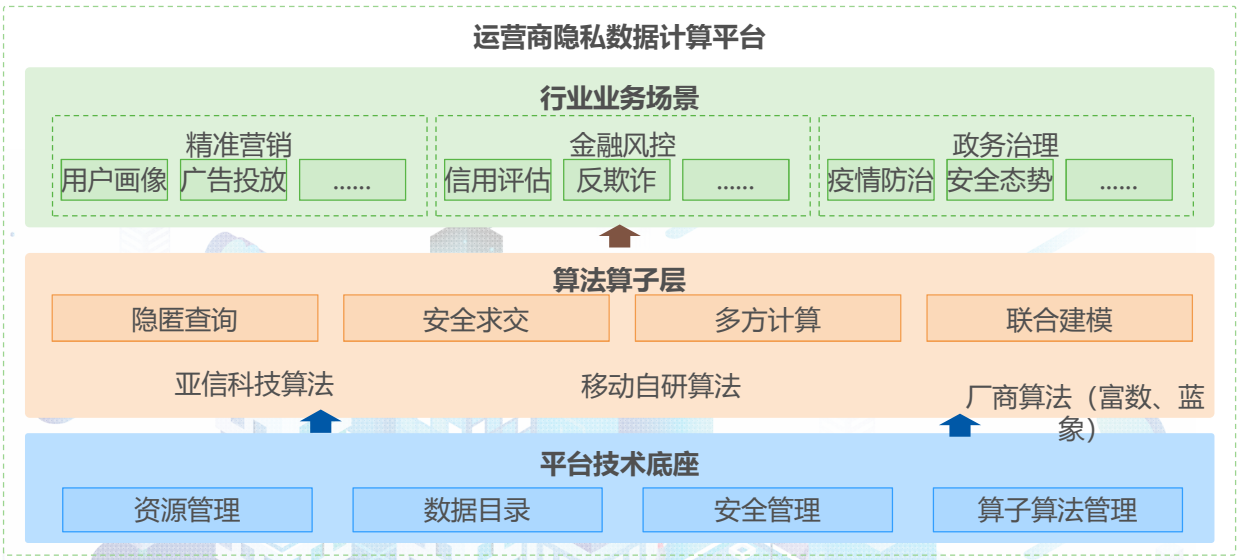
联邦学习

为了训练出效果更好的模型，需要联合多个数据实体来扩充样本数量或丰富特征维度。

应用案例
Use Cases

1 某集团之隐私计算平台

某集团隐私计算平台已形成海量数据和应用场景优势，聚焦政务、金融、交通、医疗、能源等垂直行业需求，通过隐私计算新兴技术及产品，跨越市场、行业、安全合规性等壁垒，创新推进运营商自身大数据生态建设，赋能“千行百业”数智化转型。



AISWare MPC隐私计算平台

基于密码学、分布式计算等技术，实现在原始数据不出本地的前提下进行隐匿查询、安全求交、多方计算、联合建模等数据开放合作的产品。

2 某省凤栖隐私计算多维生态平台

依托某省丰富的数据资产，并基于多元的隐私计算技术，隐私计算平台，提供统一门户供用户入驻；可在参与各方数据不出库的情况下提供安全求交、密态统计、联邦学习、匿踪查询等多种隐私计算服务，具备开放性、灵活性、扩展性和安全性。