区块链安全及企业级数字资产保护

杨大江

UCloud简介

- UCloud（上海优刻得信息科技有限公司）**成立于 2012 年**，是国内领先的云计算服务商，也是国内知名云计算服务商中**唯一一家纯内资**资本的厂商；
- 公司员工**近700人**，为**5万余家企业级客户**在中国大陆、香港、台湾地区、以及布局在东南亚、北美、和欧洲等地的业务给予支持，间接服务用户数量**超过10亿**，部署在UCloud平台上的客户业务总产值**逾千亿人民币；**
- **2017年4月**，UCloud完成由**元禾控股和中金甲子**参与的D轮融资，总金额达**9.6亿元人民币**，成为云计算行业获融资最多的企业。

主讲人

- 杨大江
  - 负责区块链产品
  - 微信18707552976

目录

区块链的安全

- 安全性是制约区块链发展的重要因素
  - 保密性
    - Fabric AC
    - Fabric 通道
  - 数据完整性
    - 签名(Signature)、共识(Consynsus)、数据上链、时间戳

应用与链码的安全

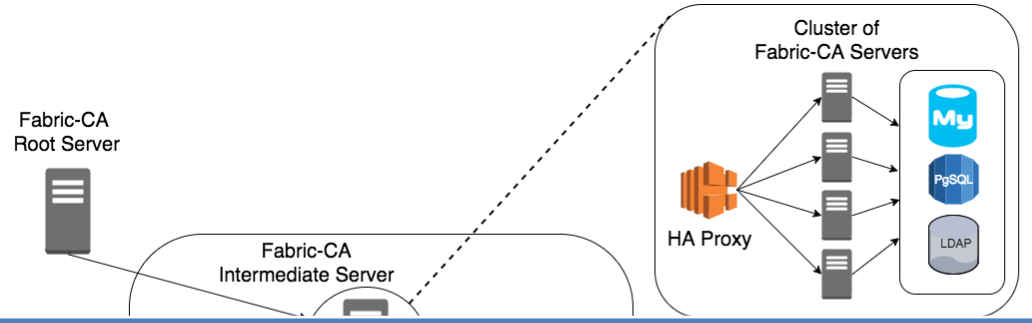
- Web与移动客户端应用安全
  - 各种漏洞
  - 缺少安全配置
  - 敏感数据泄露
  - 编程
- 链码的最佳实践（下一页）

链码开发最佳实践

- 链码作为一种新型的应用逻辑，由于天然运行在分布式系统中，被封装在容器内，跟现有的应用场景往往存在较大差异。在开发链码过程中，也需要始终注意其独特的运行特点，设计合理的代码逻辑。
  - 1.重视资源限制
  - 2.无状态设计
  - 3.避免非确定性逻辑
  - 4.链码结构设计：
  - 5.链码的生命周期管理

链码中的身份管理与访问控制

- 链码中的身份管理与访问控制
  - Fabric CA
- 基于区块链技术的身份验证



问题	区块链的解决思路
碎片化的身份	不存储在中心机构，而是用户可控的终端如手机，区块链上存储加密随机数。对用户是中心化，对黑客是去中心化
用户对身份无控制权	数据由客户掌握，按交易需求吐露一部分数据
大量口令管理	利用公钥、私钥管理，也可以结合生物验证
昂贵的身份证明过程	利用区块链数据不可篡改性，证明结果加密发布到区块链上。需要证明的机构，在获得授权的前提下利用API调用
静态的身份	利用智能合约实现动态的、灵活的身份管理

私钥的安全

- 私钥保护的正确“姿势”
  - 私钥的生成
  - 私钥的存储
  - 私钥的使用

目录

云际计算阶段成果：安全屋

- 国家重点研发计划：云计算和大数据
- 重点专项：软件定义的云际计算基础理论和方法
- 云际计算阶段成果：安全屋
  - 数据源端：资源平面数据访问、增加水印功能
  - 控制平面：合规检查、智能合约机制
  - 业务平面：数据请求、订单管理功能
  - 信息平面：价值交换转移记录、审计信息收集
- 高校合作：国防科大、上海交大、北京大学、南京大学

微博微信 | English | 公务邮箱 | 加入收藏

中华人民共和国科学技术部
Ministry of Science and Technology of the People's Republic of China

站内搜索

首 页 | 组织机构 | 新闻中心 | 信息公开 | 科技政策 | 科技计划 | 办事服务 | 公众参与 | 专题专栏

当前位置：科技部门户 > 新闻中心 > 科技动态 > 科技部工作

www.most.gov.cn

【字体：大 中 小】

云际计算阶段成果——“数据交易安全屋”产品发布

日期：2017年07月13日　　来源：科技部

国家重点研发计划“云计算和大数据”重点专项“软件定义的云际计算基础理论和方法”项目组于2017年6月27日在上海市举行“数据交易安全屋”（简称安全屋）产品发布会。会上，上海市杨浦区副区长谈兵、上海优刻得信息科技有限公司CBO季昕华、云际计算项目负责人王怀民教授等分别致辞。“云计算和大数据”重点专项管理办公室负责同志、专项总体专家组专家北京大学张世琨教授、南京大学赵建华教授也应邀参加了发布会。

安全屋是一种用于数据流通共享的云际计算产品。云际计算是中国学术界和产业界共同提出的新的云计算模式，是指以云服务实体之间开放协作为基础，通过多方云资源深度融合，方便开发者通过“软件定义”方式定制云服务、创造云价值的新一代云计算模式，力求实现服务无边界、云间有协作、资源易共享、价值可转换的云计算愿景。

安全屋遵循云际计算的对等协作机制框架，在数据源端实现了资源平面数据访问和增加水印功能，在控制平面实现了合规检查和智能合约机制，在业务平面实现了数据请求和订单管理功能，在信息平面实现了价值交换转移记录以及审计信息的收集。对等协作机制是一组虚拟化和软件定义的机制集合，是数据服务提供者与云际协作环境联接交互的通道。安全屋在对等协作机制和云际协作环境的支撑下打破了数据服务提供者和数据服务消费者之间的供需信息不对称，通过区块链、堡垒机、审核流程等手段保证数据的安全性，做到数据所有权和使用权分离，不仅促成了供需双方的互赢，而且保证了数据交易过程的安全、透明。

安全屋是该项目研究取得的阶段性成果和重要研究案例，可支持云服务提供者在其数据所有权不变的情况下实现数据使用权的可信流通共享。

打印本页　　关闭窗口

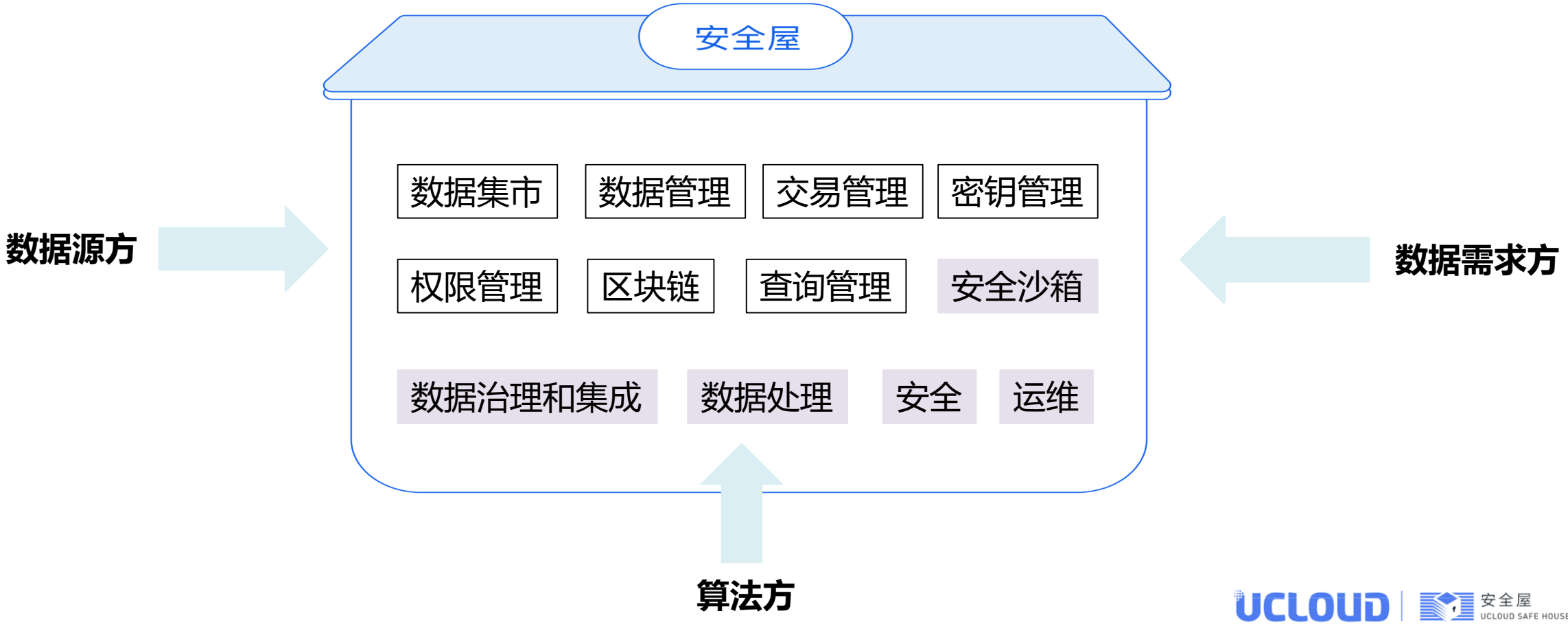
党政机关

版权所有：中华人民共和国科学技术部
地址：北京市复兴路乙15号 | 邮编：100862 | 地理位置图 | ICP备案序号：京ICP备05022684

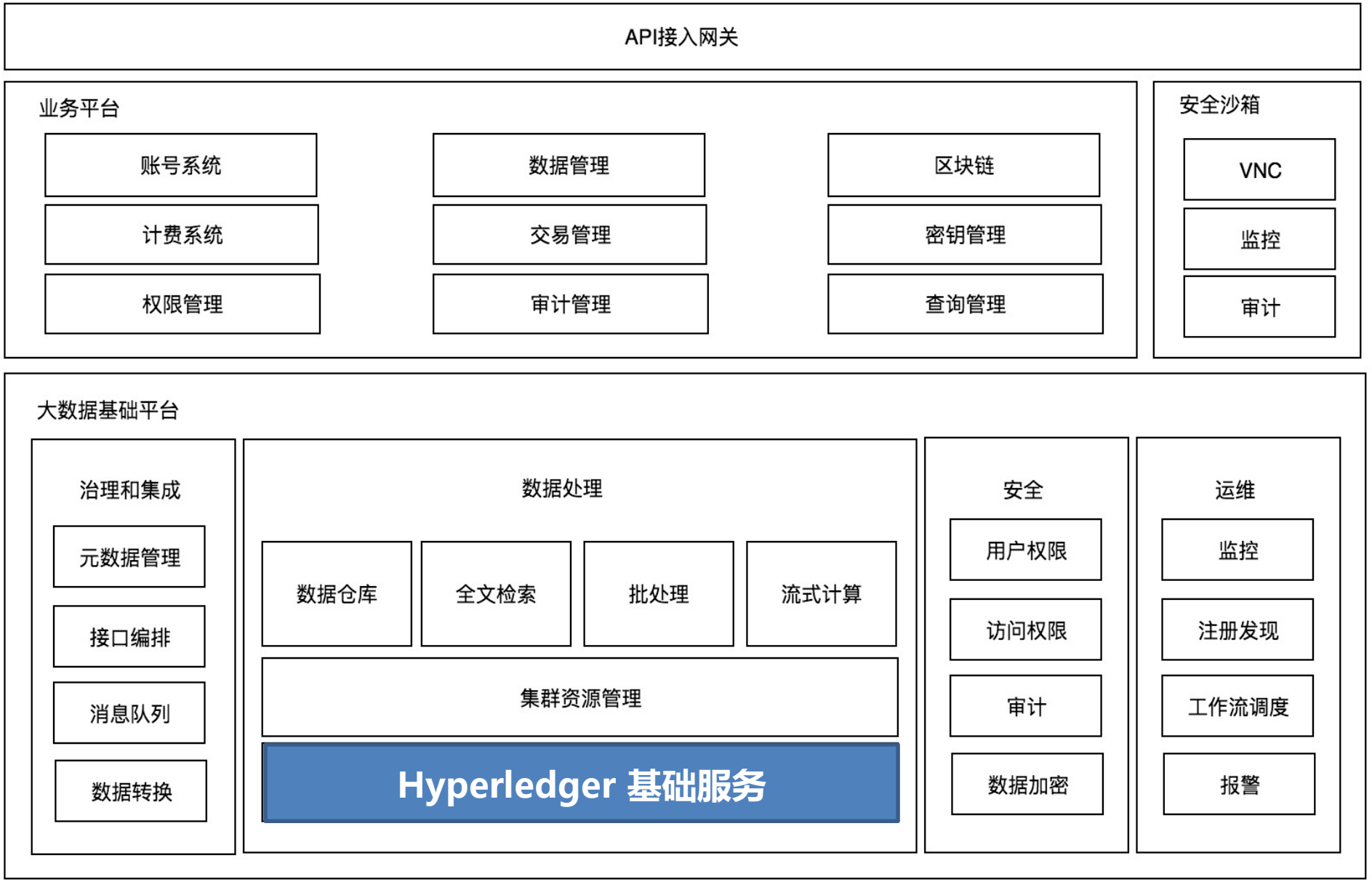
安全屋产品介绍：无价数据、极致安全

安全屋定义：实现数据所有权和使用权分离的一整套产品技术，确保数据流通过程安全可控

我们的愿景：打破数据垄断，让数据流通便捷安全，实现数据民主化



安全屋技术架构

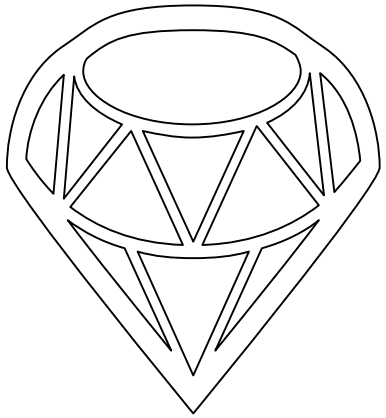

API接入网关
业务平台
账号系统
计费系统
权限管理
数据管理
交易管理
审计管理
区块链
密钥管理
查询管理
安全沙箱
VNC
监控
审计
大数据基础平台
治理和集成
元数据管理
接口编排
消息队列
数据转换
数据处理
数据仓库
全文检索
批处理
流式计算
集群资源管理
Hyperledger 基础服务
安全
用户权限
访问权限
审计
数据加密
运维
监控
注册发现
工作流调度
报警

安全屋的优势

01 区块链等安全技术

02 广泛汇集数据源

03 先进算法和第三方服务



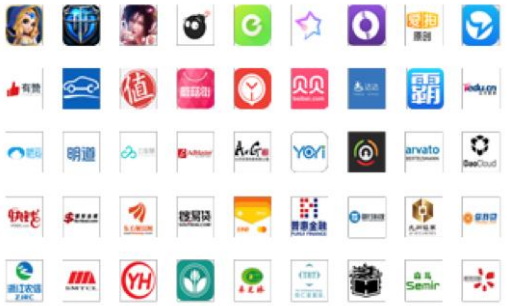
04 海量数据价值挖掘和应用转化

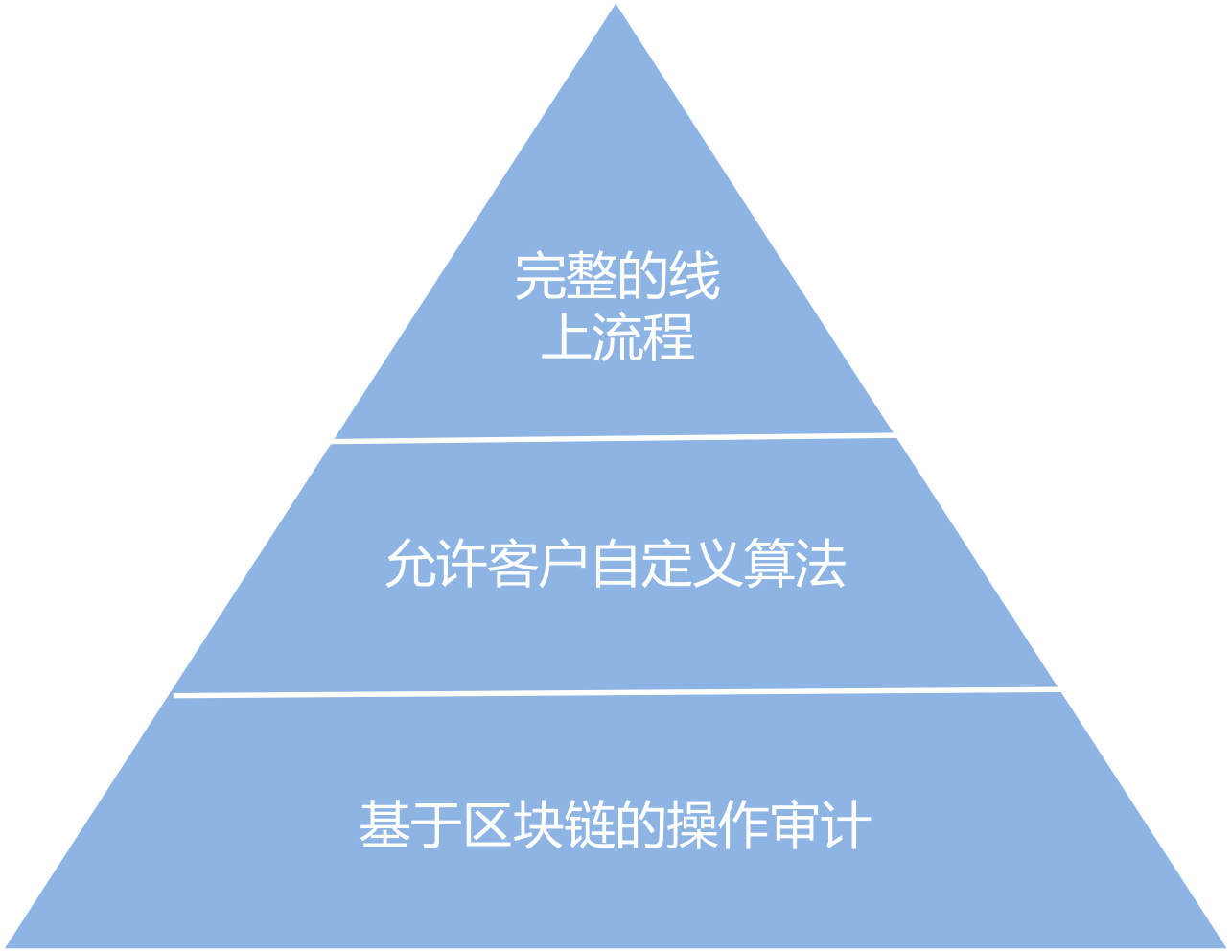
05 公有/私有、中心化/去中心化灵活部署

06 UCloud专业运营能力

安全屋产品亮点

服务于海量客户



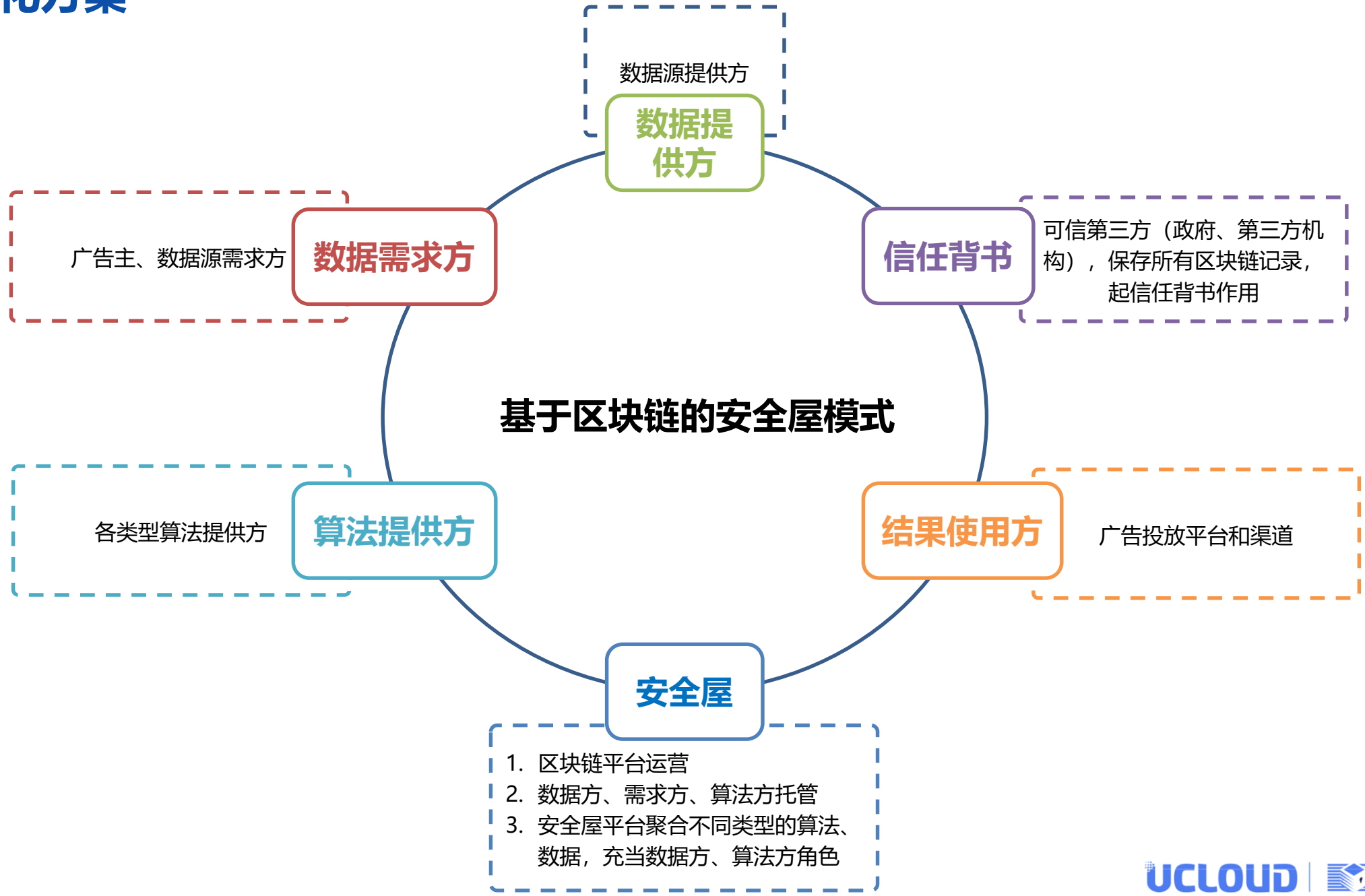


与生产环境解耦

不影响主系统

汇聚第三方数据，进行数据融合

去中心化方案


数据源提供方
数据提供方
广告主、数据源需求方
数据需求方
信任背书
可信第三方（政府、第三方机构），保存所有区块链记录，起信任背书作用
基于区块链的安全屋模式
各类型算法提供方
算法提供方
结果使用方
广告投放平台和渠道
安全屋
1. 区块链平台运营
2. 数据方、需求方、算法方托管
3. 安全屋平台聚合不同类型的算法、数据，充当数据方、算法方角色

去中心化方案产品架构


安全屋市场
完整的商业流程：数据源的快速查询，区块链入场申请、搭建，
算法提供商、广告投放商撮合等
安全屋平台
官网与客户端组成的联合系统
去中心化安全屋数据环境
数据源和计算资源组成的数据生产环境去中心化，公有云和私有云部署
安全屋 CA 服务
负责区块链的成员出入事务
Hyperledger
区块链基础服务
安全屋区块链中继服务
负责复杂内容的对接

目录

五大应用场景

1. 精准营销
2. 产业链数据共享
3. 人工智能
4. 政务数据共享
5. 企业内部数据打通

精准营销

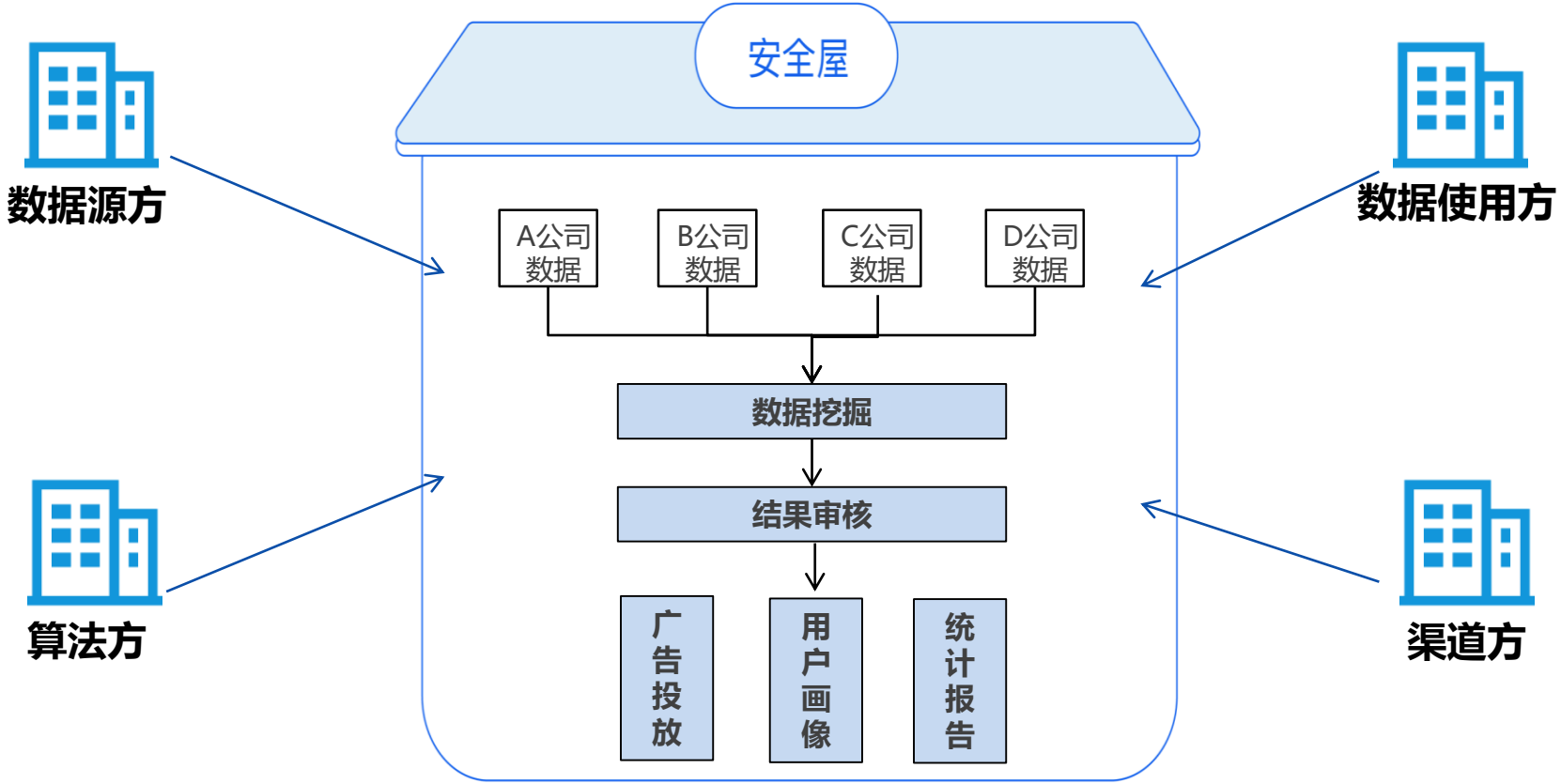
- 安全屋**联合数据源，将各方（数据方、流量方）媒体资源结合起来**，为广告主提供**高性价比、效果更优的营销服务**；
- 除广告投放外，提供**用户画像完善、统计报告**等，帮助企业更了解会员、优化商业决策

精准营销

多维度数据带来更好的营销效果，以及更低的成本

敏感数据希望共享，但不希望外泄

交叉营销没有合适平台



产业链数据共享

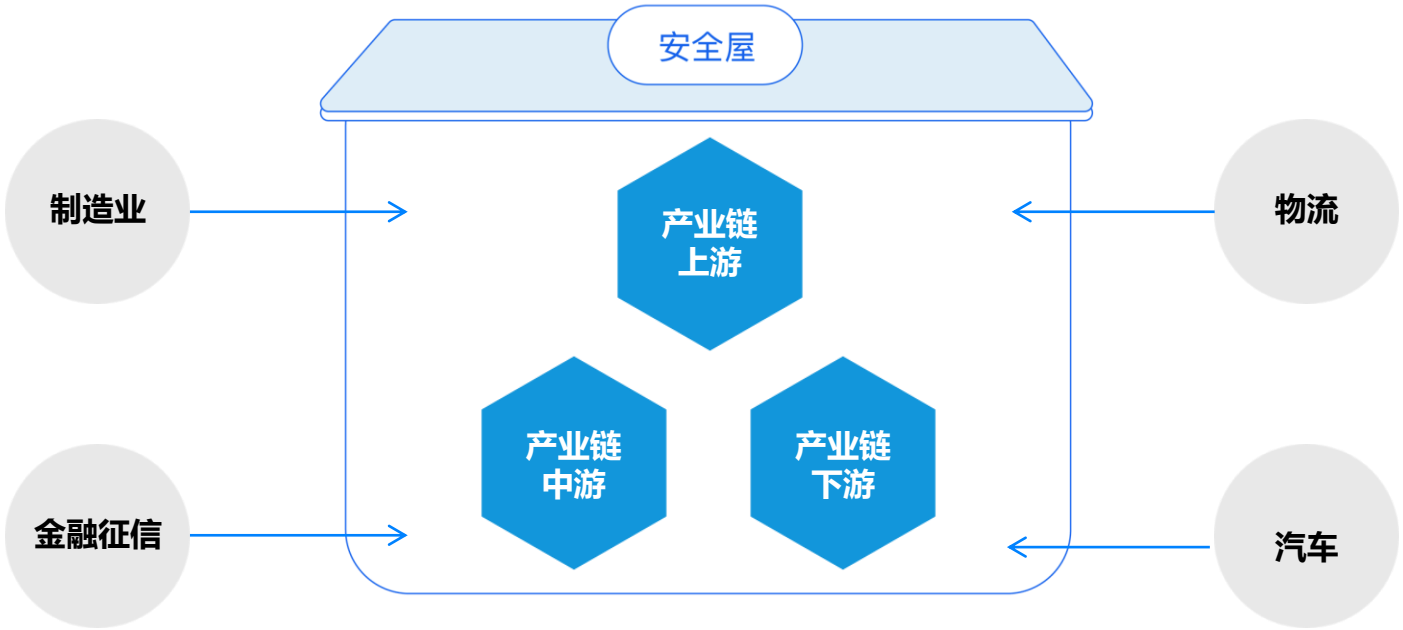
- 产业链相关企业将数据放在安全屋，交叉计算之后**只将结果输出**给各方，各机构的数据并没有给到其他结构；
- 参与机构实现了“1+1>2”的效果，横向和纵向打通产业链，实现更大产业效率，提高参与公司盈利水平。

产业链数据共享

横向纵向打通，实现更大产业效率

敏感数据希望共享，但不希望外泄

数据不流通形成孤岛，无法产生价值



人工智能

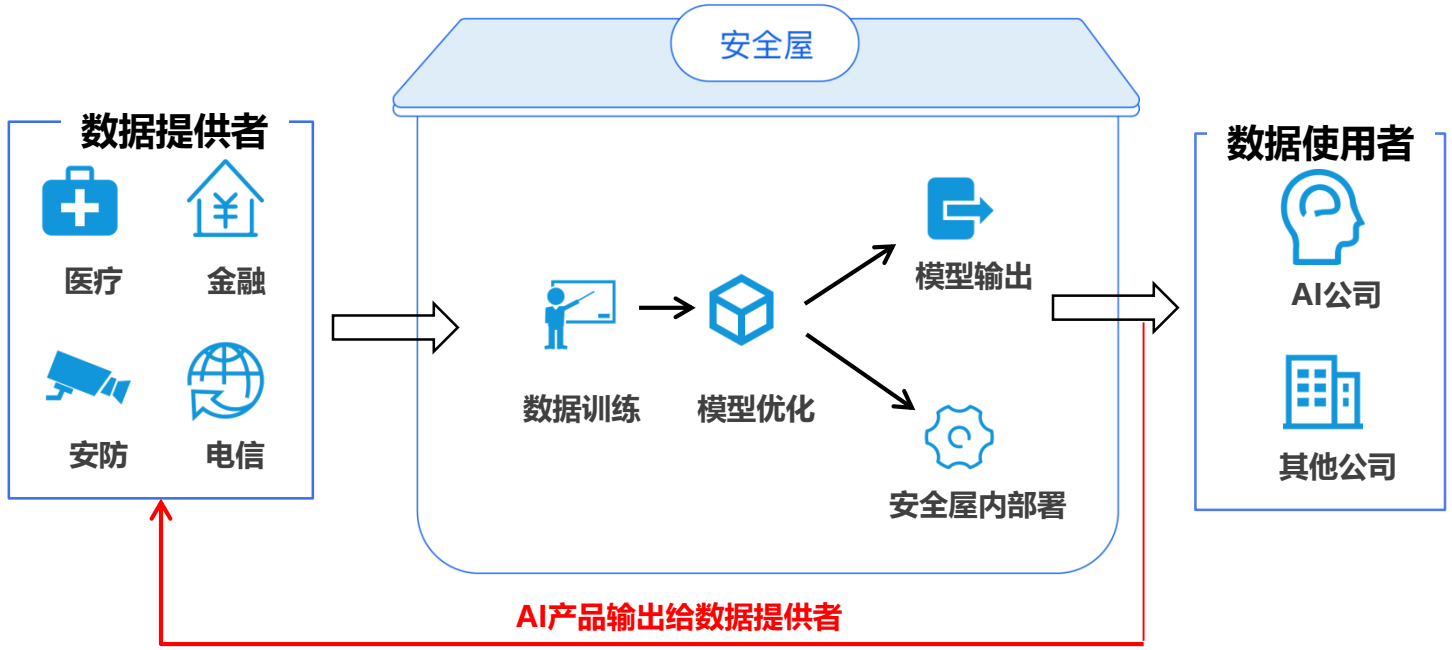
- **人工智能行业的快速发展将催生大量的训练数据交易的需求**，包括医疗、金融、安防、电信等数据提供者为AI公司提供数据，帮助AI公司优化算法，最终帮助AI公司和其他公司进行决策和分析；
- 数据提供方提供数据到安全屋，数据在安全屋根据算法进行计算、分析、优化等，数据使用方获取数据计算结果进行使用。

人工智能

将算法和数据匹配起来，加快产业发展

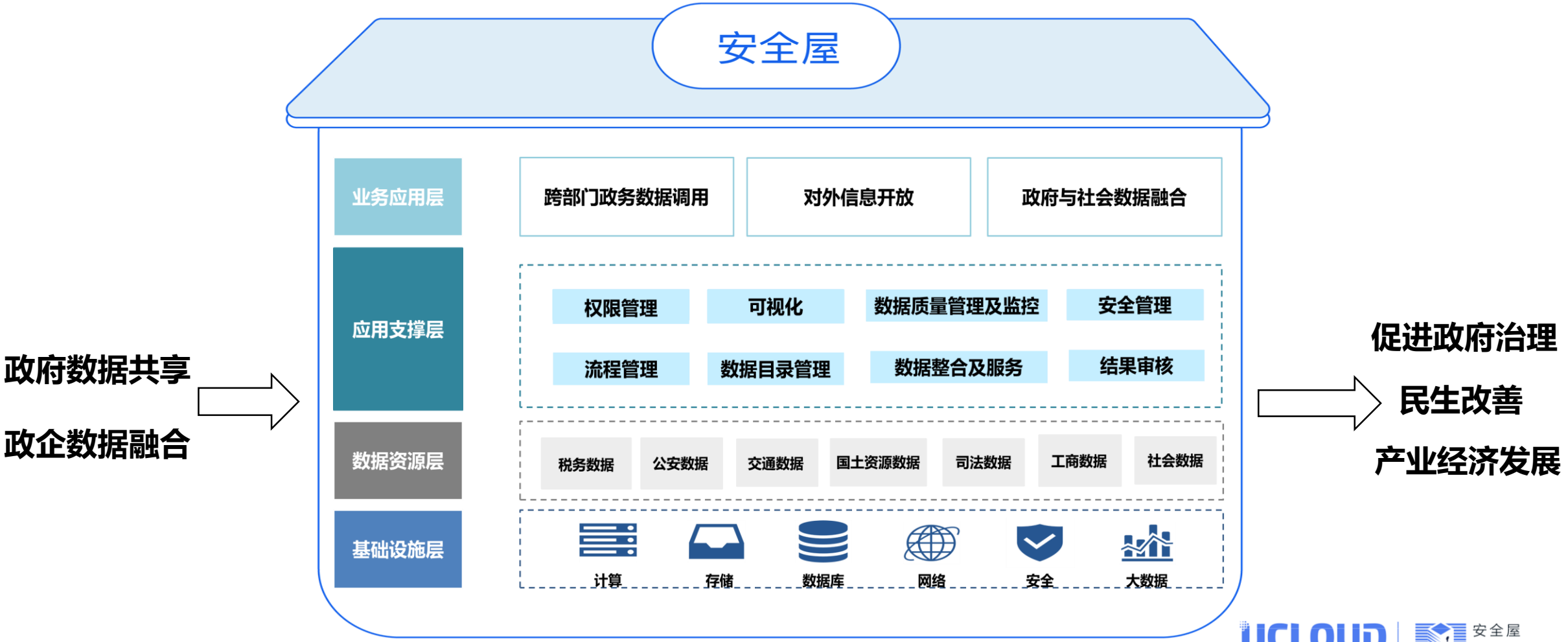
敏感数据希望共享，但不希望外泄

需要使用昂贵计算资源，交易成本过高



政务数据共享

- **促进地市级、省/市级、全国数据打通：**打破政府数据孤岛、实现跨部门互联互通，提升政府治理能力；
- **加快对外信息开放：**在安全可控合规的前提下，让企业利用政务数据开发便民应用、让数据造福民生；
- **推进同企业积累的社会数据进行平台对接：**推动互联网、大数据、人工智能同实体经济深度融合、产业经济发展。



企业内部数据打通

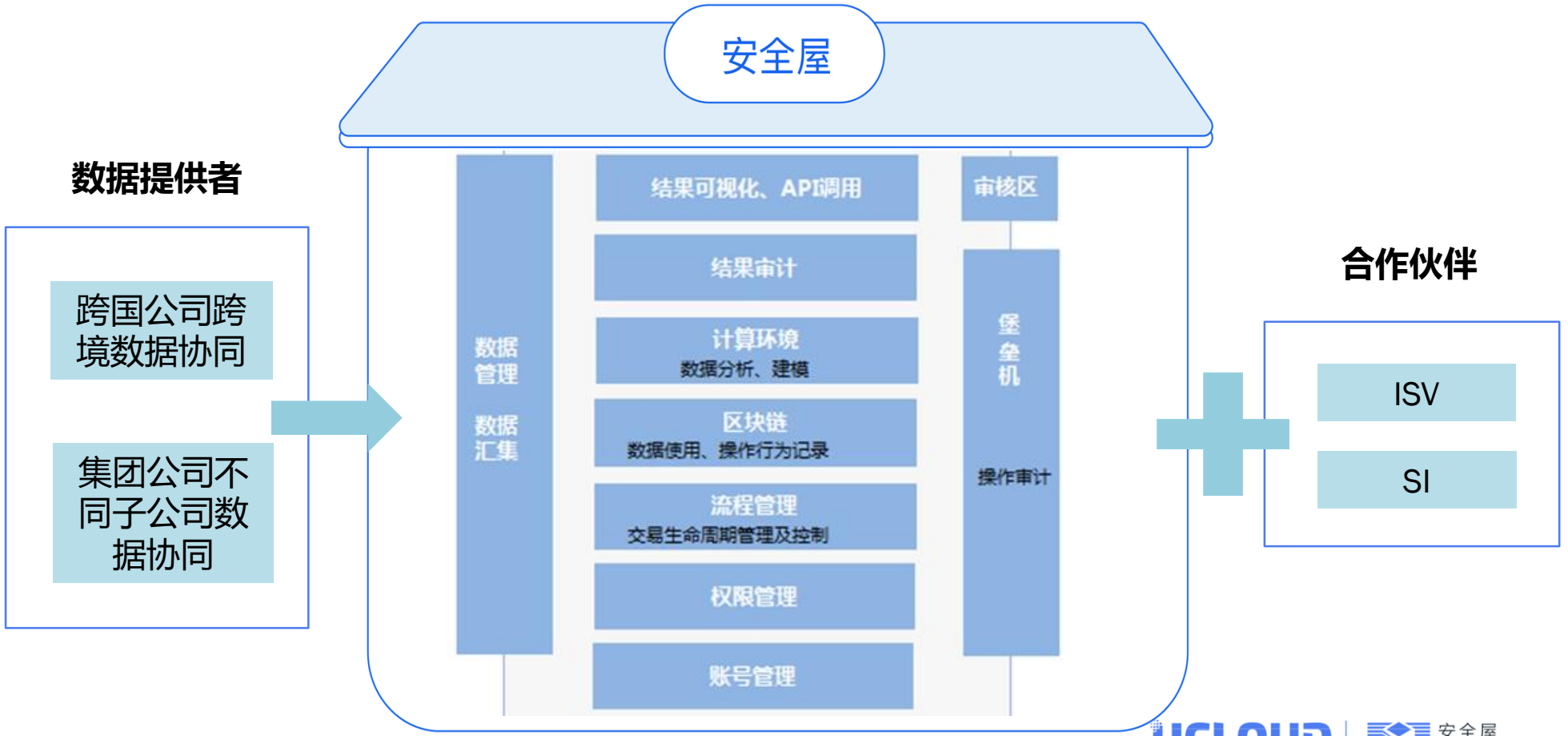
- 集团公司对内部数据打通的需求越来越多，但是**涉及敏感信息不能上公有云**；
- 安全屋私有化部署可为大型集团子公司间、内部部门间数据互通提供安全保障、打破数据孤岛现状，**提升协同办公的工作效率**；
- 打造**开放生态，与传统行业ISV/SI合作**，共同致力于帮助政府和大型集团提高内部效率。

集团数据共享

集团内部数据协同、流通、共享，利于整体商业决策

敏感数据不希望外泄，高度自控、安全的需求

结构化、非结构数据打通



截至目前引入的主要数据源

类型	客户名称	数据内容
运营商	中国联通	共2.7亿活跃用户 1. 基础属性数据 2. 话单数据 3. 互联网日志数据 4. 位置数据
	中国电信（谈判中）	共2亿移动用户+1亿固网用户 1. 基础属性数据 2. 用户行为标签数据 3. 部分时效性LBS数据 4. 其他按照合规可提供数据等
SDK	Mob	共8亿月活跃设备： 1. 基础属性数据 2. 线下轨迹数据 3. APP安装列表 4. 设备属性数据

类型	客户名称	数据内容
工具类APP	WIFI伴侣	2亿存量用户，3千万月活用户： 1. APP安装列表 2. 线下轨迹数据 3. 游戏行为和充值数据
	墨迹天气	1. 全国实时天气数据（中央气象台） 2. 约1亿月活用户的精准位置信息（GPS） 3. 客户APP装机列表等其他信息
	梦享科技	1. 月活约1亿的用户WiFi位置信息 2. 月活约几百万的用户POI信息（线下门店访问轨迹，消费行为和其他交互数据）
垂直行业	玖富金融	4,000万用户的理财和贷款信息数据
	车轮网	月活过亿汽车人群用户
	绘客科技	8,000万简历数据
	优志愿	数百万高中阶段学生及家长数据

精准营销案例1：联通安全屋平台介绍

中国联通自有数据中心

安全屋

应用管理平台

数据集市	数据管理	交易管理	营销模块
权限管理	区块链	查询管理	DSP平台

安全屋管理平台

计算环境	交易管理	流程管理	区块链
运维审计	结果审计	计费管理	

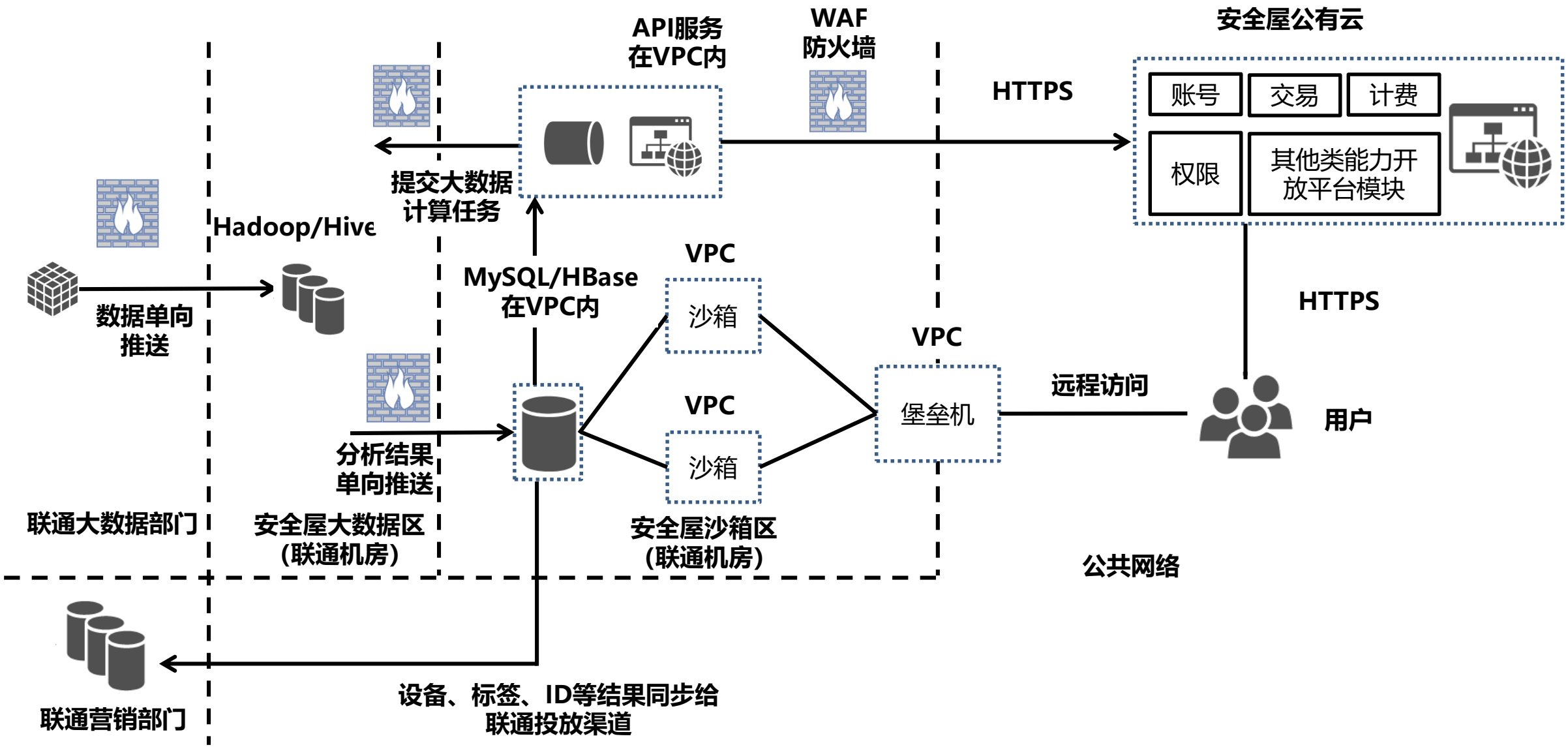
增值服务

- 短信服务（联通提供）
- 外呼服务（联通提供）
- 数据挖掘
- DSP合作商

安全屋客户

中国联通&UCloud安全屋专项

精准营销案例1：联通安全屋平台系统架构图



精准营销案例2：同程旅游商旅人群 & Mob

通过Mob数据挖掘商旅两地人群，短信投放同程旅游的火车票广告。

数据源

mob.com

China unicom中国联通

数据挖掘&验证

定向人群的挖掘逻辑

A. 年龄（25~44）；有高频跨城位移（过往3个月内月均≥4次）；位移城市为特级城市、一线城市和省会城市

B. 安装并打开APP（APP包含出行类&地图类）（打开频次为连续4周每周有打开行为）

结果的尺数据验证

A. 以联通数据为尺数据，验证Mob数据的挖掘结果和质量

B. 验证方式：抽取500个联通号码拥有者的IMEI号，以最近两个月内漫游次数≥4作为验证指标

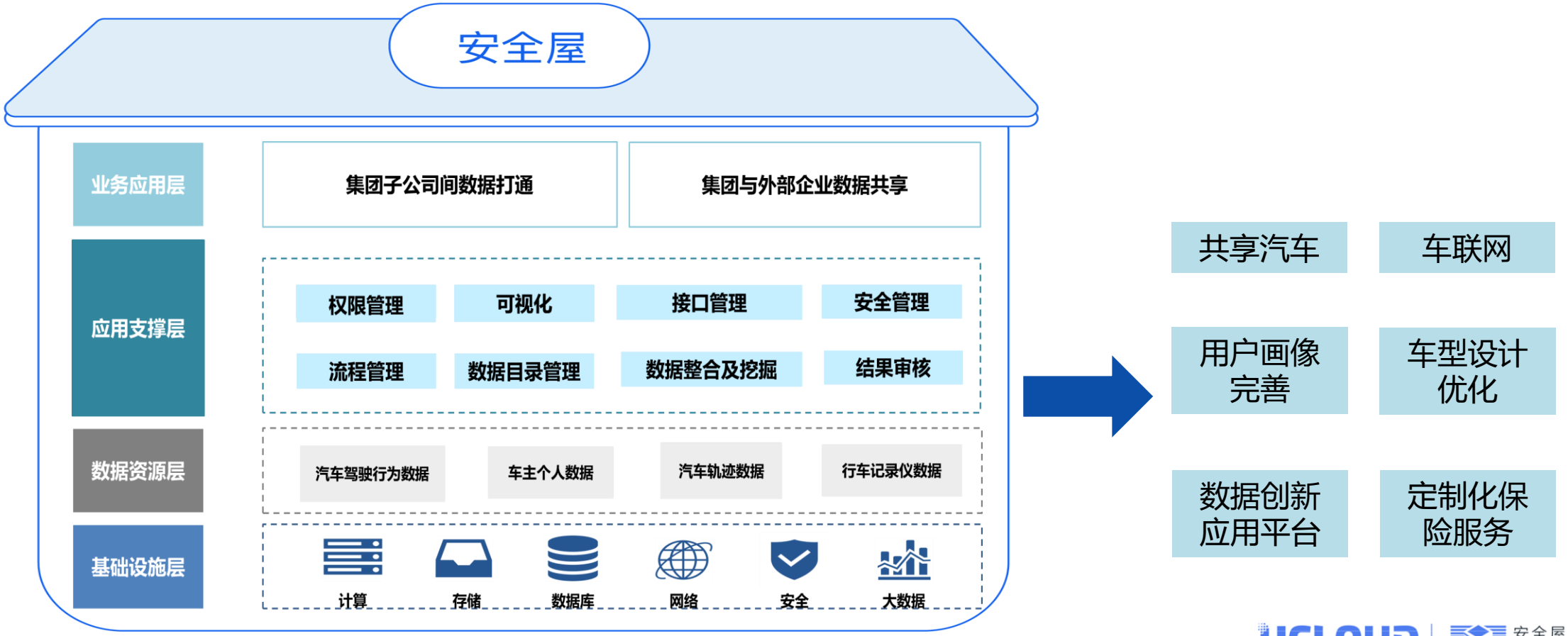
数据应用

极推黑盒：IMEI → 手机号码 → 短信推送

1. IMEI成功匹配手机号码比率为62.41%（30000条成功匹配18723条）
2. 手机号码成功推送比率为55.96%（18723条成功推送10477条）
3. 截至目前的短信整体送达率为34.92%

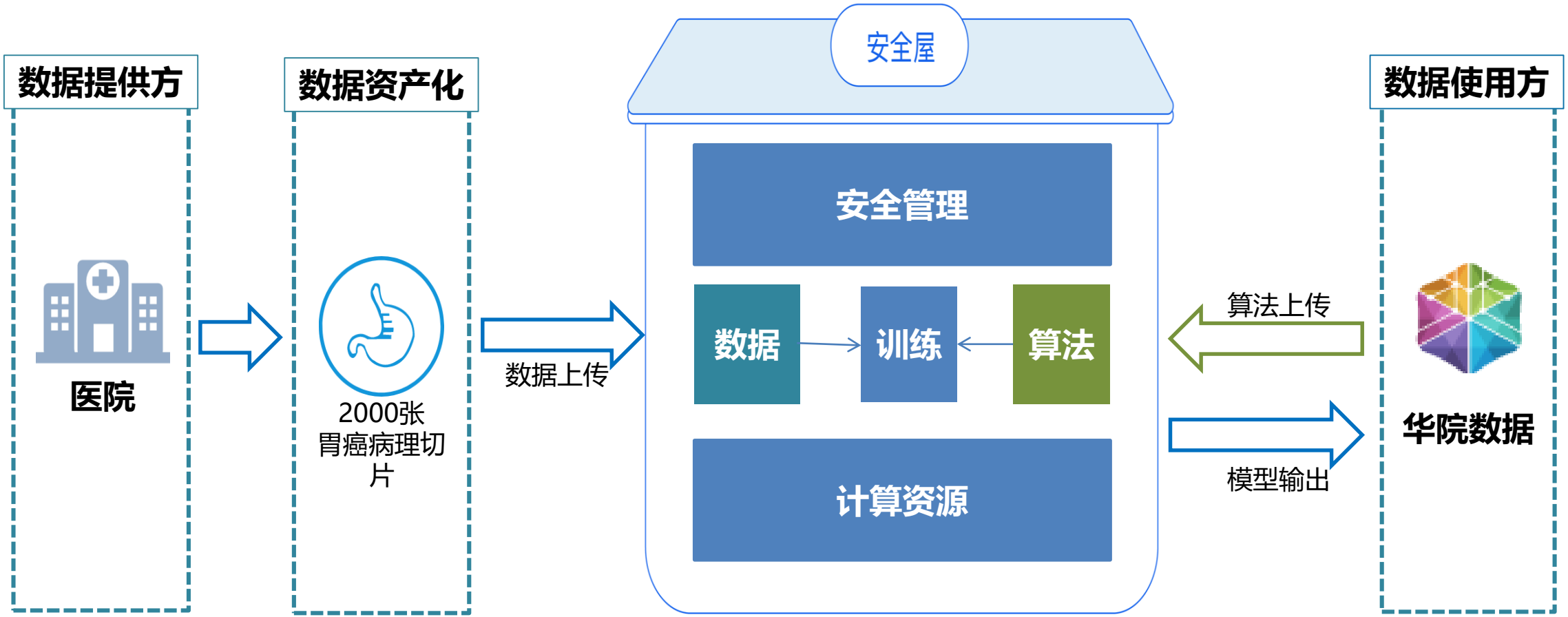
产业链数据共享案例：吉利汽车车联网数据创新平台

- UCloud提供**底层计算平台和数据安全技术**，汽车集团子公司**亿咖通提供汽车驾驶行为数据、车主个人数据、汽车轨迹数据、行车记录仪数据等**；
- 通过**应用支撑层各功能模块**，如权限管理、流程管理、数据挖掘、接口管理等实现**集团子公司间数据打通、集团与外部企业数据共享**；
- 支持**共享汽车、车联网、用户画像完善、车型设计优化、数据创新应用平台，以及对接保险公司，实现定制化保险服务。**



人工智能案例：医疗AI

- 华院数据通过安全屋使用医院的**胃癌病理切片数据做训练，医院可采购优秀的模型**；
- 安全屋提供海量计算资源、保障医疗数据不泄露，**发挥医疗数据价值、促进AI应用落地。**



政务数据共享案例：香港离岸数据流通平台

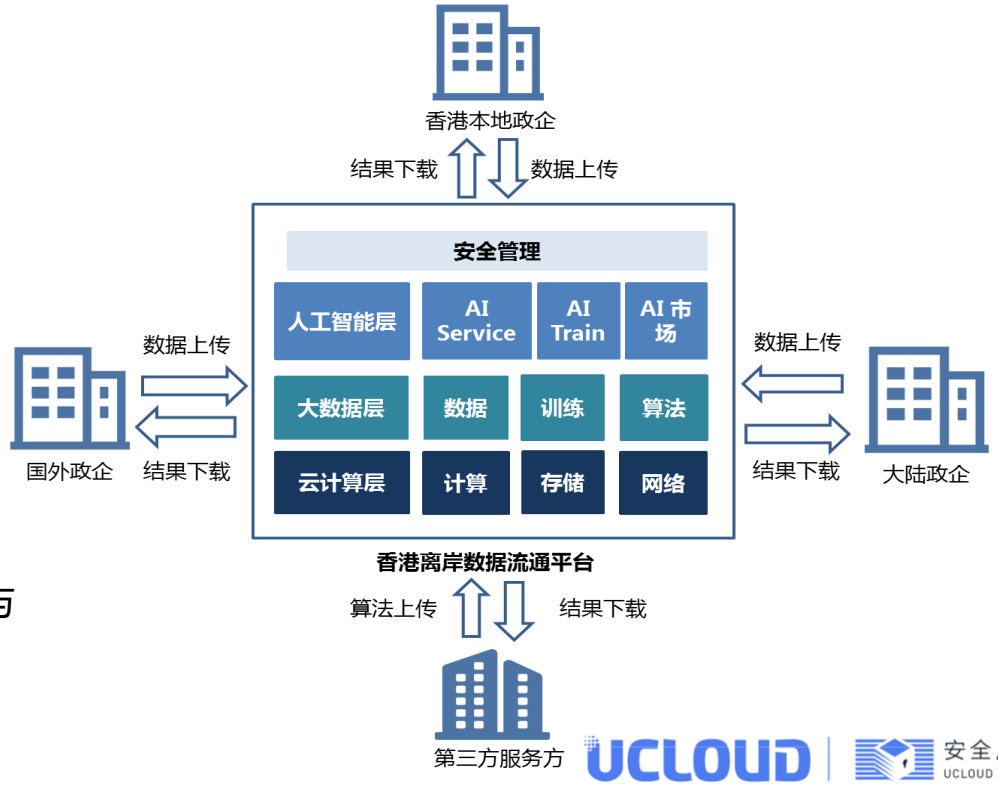
建设目标：

- 通过数据分析、业务流程优化等**提高香港贸易、金融、物流、地产等行业的运营效率**；
- 促进本土新兴产业，发展大数据、人工智能产业生态，将新的技术带给金融、贸易、航运行业；
- 平台将秉承中国对隐私和安全性的政策，**以便政府监督、执法**的同时，**促进隐私和数据保护方面的国际互操作性，促进各国企业、政府之间的跨境数据合作，消除数字贸易壁垒**，促进制定更好的数字经济和贸易措施，**将香港打造为全球数据港。**

设计方案：

- **云计算层：**提供网络、存储、计算等云计算服务，支撑大数据分析、人工智能服务
- **大数据层：**提供数据、训练、算法等大数据层服务，充分挖掘数据价值
- **人工智能层：**提供人工智能层服务，促进数据有效应用；
- **安全管理：**提供一整套完善的安全管理系统，保障平台安全、数据安全

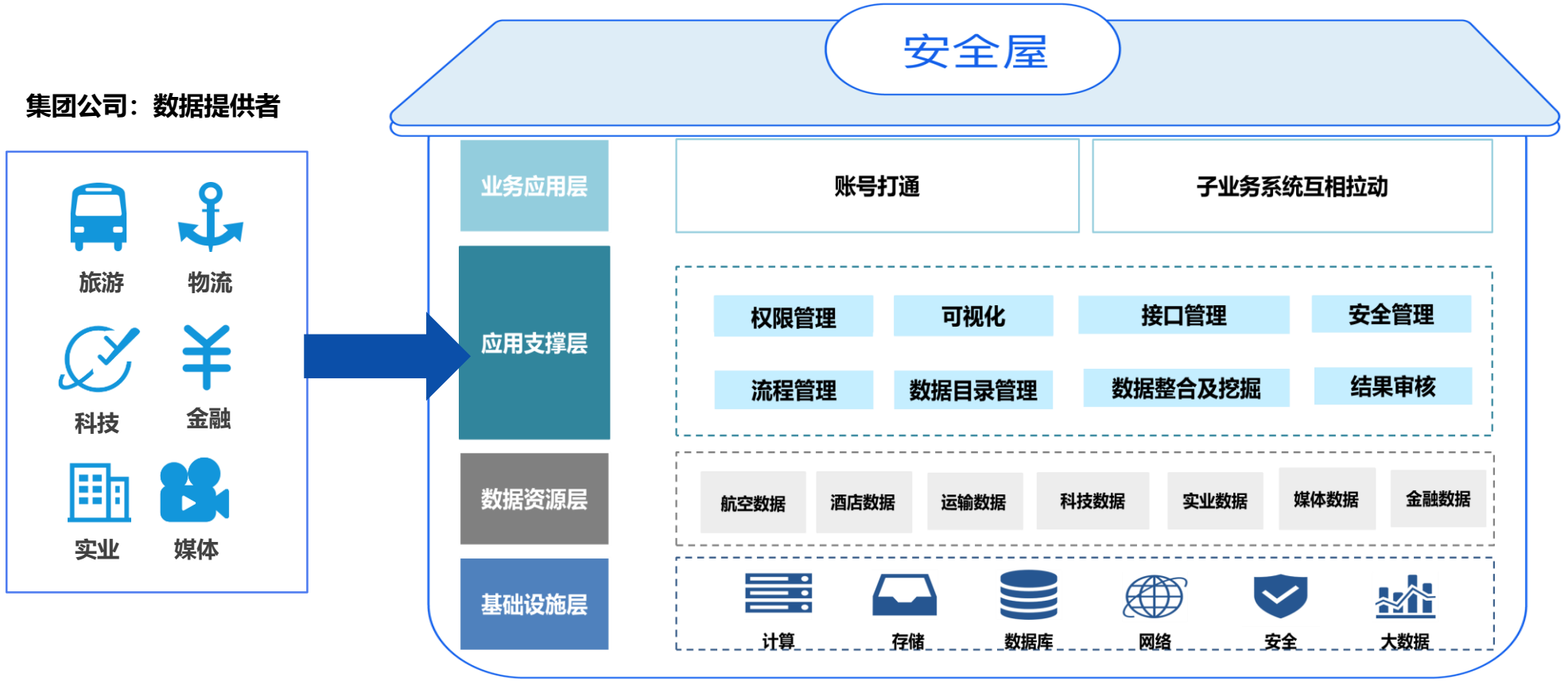
平台将**联合第三方服务方**，共同服务国外、内地、香港的政府和企业的数据与数据分析需求。



企业内部数据打通案例：海航集团内部数据共享

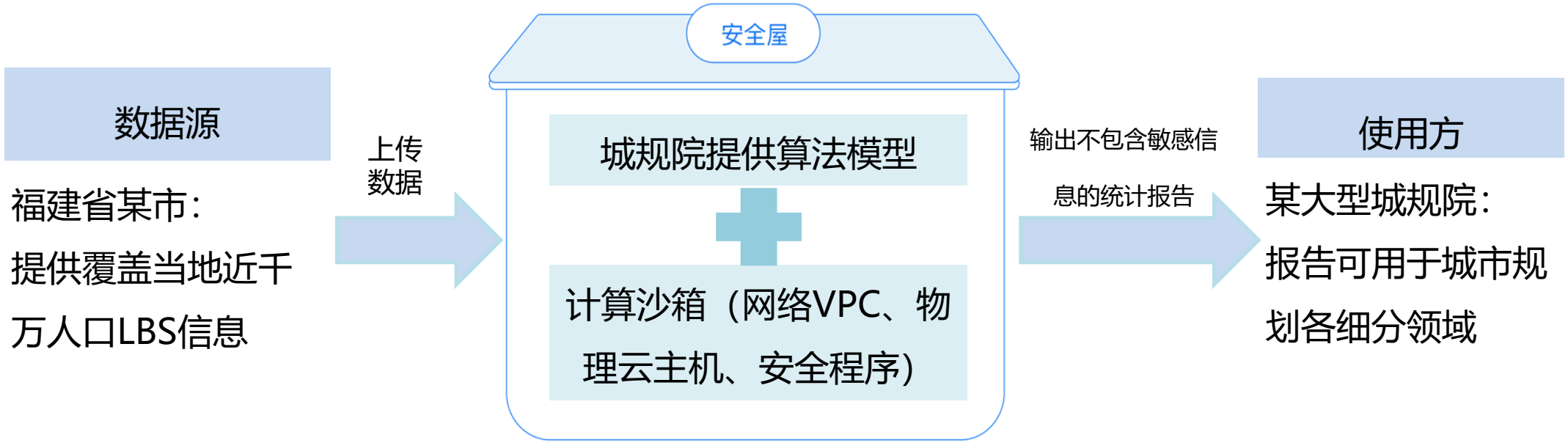
UCloud将在海航机房部署安全屋系统，实现：

- **在云上汇集旅游、物流、科技、金融、实业、媒体数据，**打通子公司间数据、打破部门间数据孤岛；
- 通过应用支撑层各功能模块，如权限管理、流程管理、数据挖掘、接口管理等实现账号打通、子业务系统互相拉动；
- 新的数据体系催生崭新管理模式，提高集团经营效率，**促进业务创新**，提升效益，同时保证**数据安全、自控。**

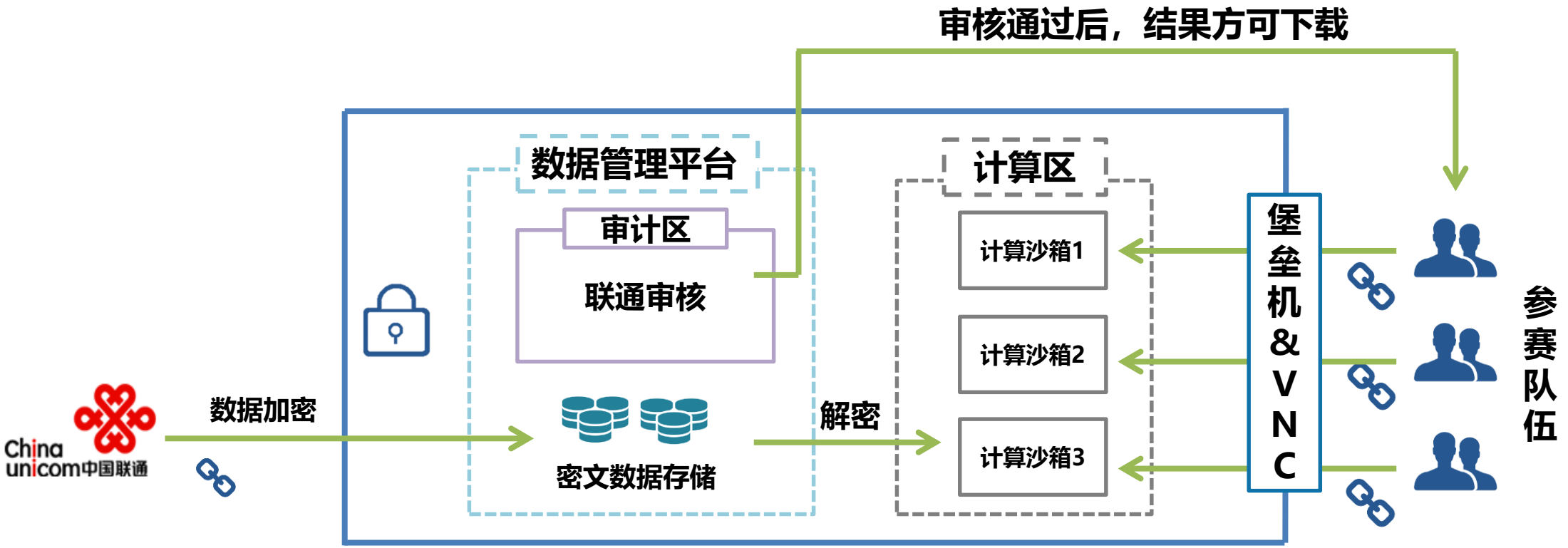


报告案例：城市规划报告

- 政府、公共数据以及商业数据，对**城市规划**（重大民生设施综合评价、城乡空间发展研究、城市低碳发展、交通规划等）以及**企业商业决策**（现状综合分析、店铺选址、营销策略、产品策略等）具有重要应用价值；
- 安全屋支持**多数据源大规模分析，输出统计报告**，优化城市规划和企业决策。



大赛案例：2017年上海联通“沃+海创”数据大赛



方案说明：

1. 联通**控制密钥**，密钥可分发给参赛者，加密后的数据通过API上传至安全屋数据管理平台存储；
2. 数据解密后在安全屋内进行明文计算；
3. 参赛队伍通过堡垒机上传算法，浏览数据和结果，堡垒机**仅支持屏显不可下载；**
4. 如果联通允许参赛队伍下载结果，必须经过**审计区**（联通审计），审核通过后方可下载；
5. 整个流程由**区块链记录**，不可篡改，可追溯。

谢谢！

UCLOUD | 安全屋 UCLOUD SAFE HOUSE

无价数据、极致安全