数据安全与隐私计算实践

Data security and privacy computing practices

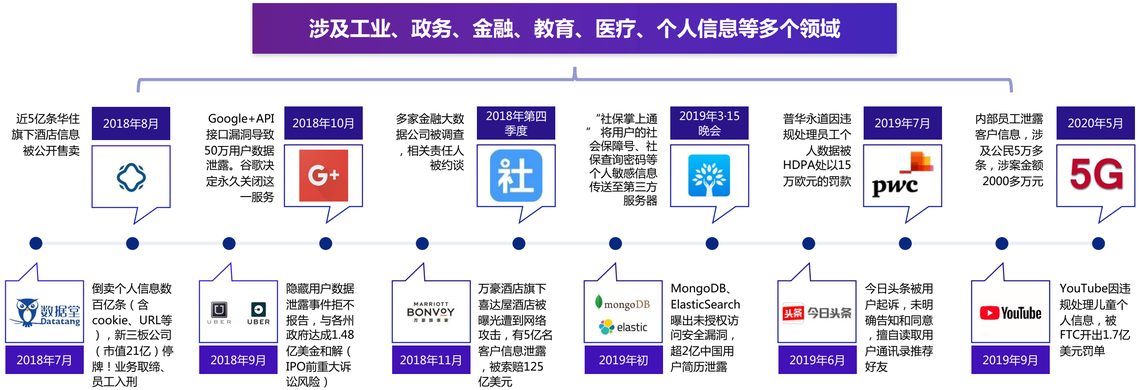
刘博

杭州安恒信息技术股份有限公司 首席科学家

之江实验室网络安全研究中心 副主任

数据安全风险频发，需网络安全、数据安全和隐私计算技术联合应对

■ 数据安全泄露事件



■ 防止数据和隐私泄露的技术

隐私计算：数据在开放给组织外第三方或者与第三方进行联合计算导致的泄漏。

数据安全：员工或者合作伙伴在内部数据使用过程中有意或者无意导致的泄露。

网络安全：网络攻击所导致的泄露。

网络安全技术、数据安全技术和隐私计算技术，共同构建安全可信的数字世界

构建安全可信的数字世界

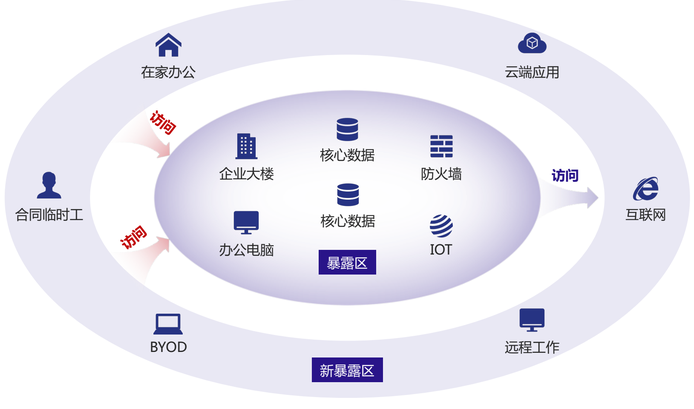
数据安全与隐私计算

数据安全咨询与运营体系

数据安全监督管理体系

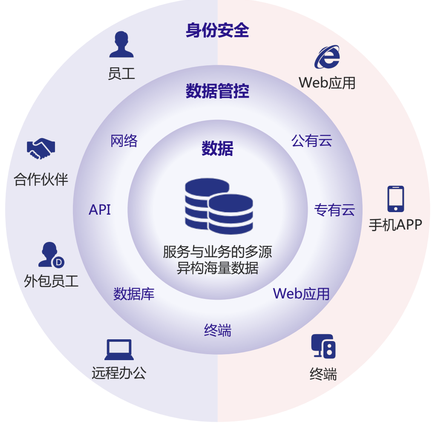
■ 防御外部的网络安全威胁：

全天候全方位网络安全态势感知



■ 细粒度感知和管控内部数据使用：

访问主体、客体、以及访问关系的可信、可用、可管



■ 可用不可见的数据共享和交易

原始数据不可见、计算模型授权可控

安恒数盾 DBAPP Data Shield

身份安全
AiTrust

身份安全

AiTrust 零信任体系

构建可信的身份认证体系、动态的权限访问控制

数据保护
AiGuard

数据保护

AiGuard 数据安全管控体系

实现全方位、全链路、全生命周期数据安全管控

数据流通
AiLand

数据流通

AiLand 安全岛体系

构建可用不可见的数据交易和数据开放平台

咨询规划
Consulting

咨询规划

前期顶层规划 /中期建设评估 /后期持续运营

帮助数据安全技术和管理制度轻松落地

万物互联，网络无边界

大部分网络攻击的目标为 **数据窃取**

数据流通环节，增加了网络攻击风险

新型攻击不断增加

网络安全态势 | 智能安全分析 | 高质量威胁情报 | 安全能力生态 | 自动化安全响应置 | 智能安全运营

AiLPHA新一代网络安全态势感知

AiLPHA新一代网络安全态势感知

■ 超过60%的数据泄露是由网络攻击造成

工信部信息化中心产业观察：

2022年第一季度全球35起影响较大的已公开信息泄露事件，从总体情况来看，**数据泄露规模超过17TB**，敏感信息泄露涉及**人数近9000万人**。

服务器的密码为弱口令	API未经授权调取信息	漏洞攻击
配置错误的AWS S3	AWS入侵	DDoS攻击
钓鱼攻击	勒索病毒	利用微软SEAL漏洞，实施侧信道攻击

缺乏快速有效的数据泄露事件分析和处理手段

■ 数据安全基础：新一代网络安全态势感知

■ 提升安全运营效率

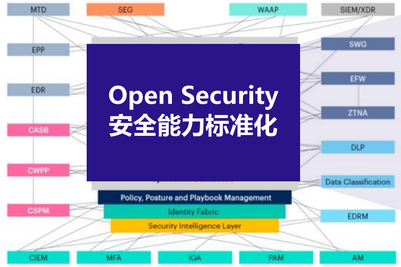
承载**80%**的安全分析与运营工作；提升**80%**的安全分析与运营效率

Open Security：互联互通、异构兼容、标准开放、一体化安全

■ 你们单位有多少款安全工具？
小型单位15-20、中型50-60、大型>130，工具之间不协同

安全工具数量数据来源：Gartner　全景图来源：安全牛

■ 定义了20+标准能力API、集成了200+安全产品&服务



流量分析 Network Analysis API

终端安全 Endpoint Security API　**资产管理** Asset Manage API　**访问控制** Access Control API

Web安全 Web Security API　**安全扫描** Security Scan API　**身份管理** Identify Manage API　**活动列表** Active Directory API

IT管理系统 ITMS API　**配置变更管理** CMDB API　**沙箱分析** Sandbox API　**威胁情报** Threat Intelligence API

版本控制 Git API　**消息通知** Messaging API　**外部数据源** Data Source API

Web Hook Web Hook API

➢ 能力模型

Open Security能力模型

定义标准化安全能力，支持异构兼容、开放生态，依赖社区反馈，持续迭代进化

➢ 能力中台

APIHub 安全能力中台

基于标准化能力模型打造，开放安全产品与服务能力注册，支持多语言SDK

➢ 数据模型

Open Security数据模型

定义安全分析与运营全链路过程中的标准化数据格式，衔接检测、研判、响应、处置

➢ 开发者社区

Open Security开放社区

促成能力提供方和能力调用方的交流，促进网络安全行业的互联、互通、互操作

SOAR：协同联动、智能处置、提质增效

安全运营的痛点

- **专家能力稀缺**

  安全运营工作依赖专家经验，出现复杂的安全问题大部分运营人员无法妥善解决……

- **资源呈孤岛状**

  安全设备各自为战，缺少统一协同工作能力，需要人作为连接器……

- **分析处置流程乱**

  事件分析处置没有标准流程，全凭当天运营人员的状态，无法稳定运营质量……

- **重复性工作多**

  例如红蓝对抗期间，每天面对海量高强度的扫描攻击束手无策，没有时间精力判断如何处置……

  日常运营期间，精力都耗费在发起扫描、编写报告的重复工作中……

安全能力API化

支持多种设备联动协同能力，16个种类，100+安全设备。

定义标准化的能力API，实现安全能力接入APP集中分发。

自动化/半自动化编排

剧本编排：内置丰富的安全编排剧本，场景化的编排剧本，支持拖拽、自定义编辑、多标签管理

案件处置：根据事件触发，绑定剧本，生成案件，自动化执行剧本

作战室调用：若存在人工判断，作战室相关人员协同配合进行处置

联动处置：支持调用多种设备联动、阻断、隔离、取证、封堵、通报

安全能力中心

剧本编排中心

基础安全设备	网络防护设备	安全审计设备	终端防护设备	数据共享/消息通知	告警接入	安全事件	安全告警	资产信息	威胁情报

SOAR上线后

1	通过沉淀知识每日**自动化处理已知场景**
2	每条告警处置需要**1-10分钟**
3	至少能**节约70%**以上人力投入
4	通过编排系统**解决设备孤岛**
5	提供**集中case管理**和**协同处置空间**

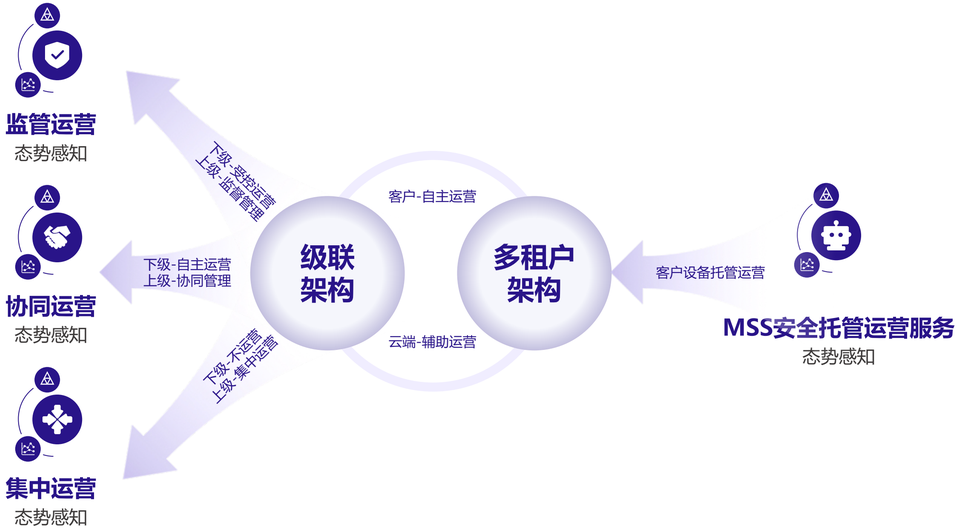
事件响应效率提升**400%**以上

SOAR上线前

1	每日上万条告警，**无法分析处置**
2	每条告警处置需要**30分钟-3小时**
3	重保活动需要大量人员**24小时**值守
4	各节点安全防护系统**互相孤立**
5	**没有统一操作平台**进行安全处置闭环

网络安全态势感知建设成果

■ 立足国内，覆盖全球，为**全球**超过**3000家客户**，提供高质量的态势感知技术和服务。承担国家级/省级课题**10**项，参与国家/行业标准**20**项，拥有专利**300**余项。获得中央网信办、工信部等荣誉**60**余项。



中国态势感知市场排名第一

IDC：赛联《中国态势感知解决方案市场2019/2021年厂商评估》《中国网络安全最具成长价值新型科创企业分析报告》《安全牛中国网络安全创分领域矩阵图》

国家地方联合
工程研究中心
国家发展和改革委员会

ALPHA
携手构建网络空间命运共同体最佳实践

部分国家&行业标准

- **信息安全技术 网络安全态势感知通用技术要求**
- 信息技术 安全技术 网络安全 第2部分：网络安全设计和实现指南
- 信息技术 安全技术 网络安全 第1部分：综述和概念
- **信息安全技术　安全能力编排与自动化响应**
- 信息安全技术 智慧城市安全体系框架
- 信息安全技术 政府网站云计算服务安全指南
- 信息安全技术 Web应用安全检测系统安全技术要求和.....

入选精品案例展示的唯一网络安全项目

发明专利

- 一种用户行为特征提取方法及系统
- 基于随机森林的策略自学习和优化方法及装置
- 一种基于多维行为模型的用户风险评估与分析方法
- 一种基于马尔科夫模型的访问异常检测方法和系统
- 一种基于贝叶斯模型优化的webshell检测方法
- .....

安恒数盾数据安全解决方案全景图

全场景、全链路、全生命周期数据安全

数据安全管控平台

数据资产地图	数据风险感知	动态权限管理	数据安全合规	数据安全运营
数据分类分级	风险事件溯源	以身份为中心	合规知识库	运营工单管理
数据链路测绘	实体行为分析	以数据为中心	检查指标模型	安全风险处置
访问热度分析	数据安全态势	动态权限策略	自查督查协同	安全事件处置

国家法律

- 《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》

国家标准

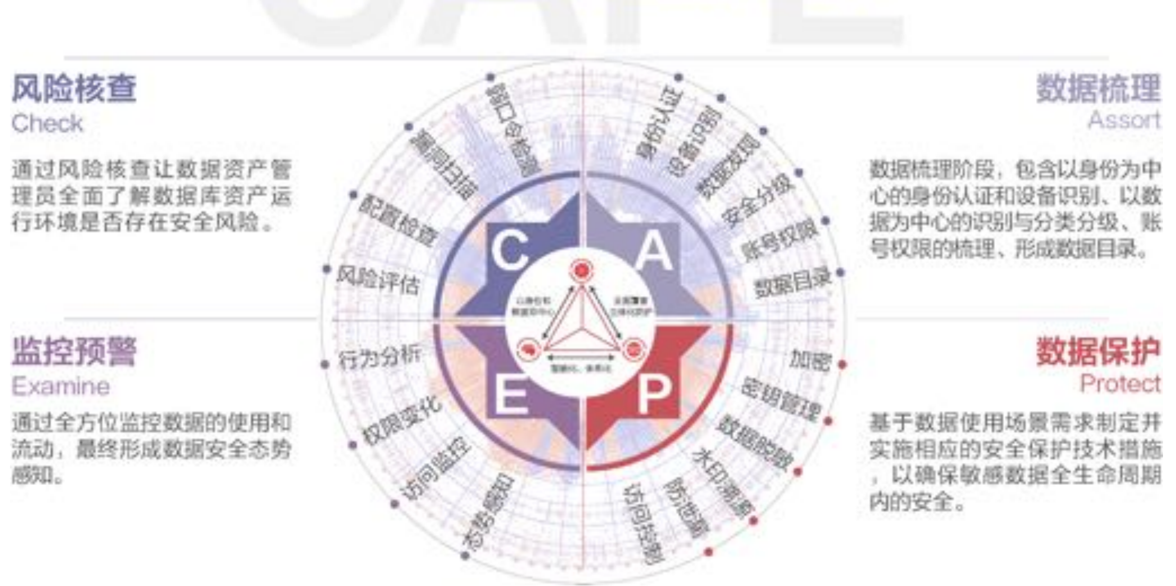
- 《信息安全技术 数据安全能力成熟度模型》
- 《信息安全技术 大数据服务安全能力要求》
- 《信息安全技术 个人信息安全影响评估指南》

行业指引

- 《基础电信企业数据分类分级方法》
- 《金融数据安全 数据生命周期安全规范》
- 《汽车数据安全管理若干规定（试行）》

可信 可用 可管

CAPE数据安全能力框架



数据安全咨询与服务

前期	中期	后期
顶层规划	建设评估	持续运营

数据安全场景

东数西算	数据要素市场
大数据交易中心	公共数据授权运营
智慧城市	政务数据共享交换
数据上云	关键信息基础设施
数据中台	API安全
终端安全	远程办公

以数据安全治理的思路落地安恒数盾

安全战略

合规保障

风险可控

开发利用

第一步：安全规划

法律法规	《网络安全法》、《数据安全法》《网络安全等级保护基本要求》《个人信息保护法》等
国家标准	《数据安全能力成熟度模型》《大数据服务安全能力要求》《数据交易服务安全要求》等
行业标准	《基础电信企业数据分类分级方法》《个人金融信息保护技术规范》《健康医疗数据安全指南》等

治理评估

数据安全战略规划

数据安全组织架构规划

数据安全制度流程规划

数据安全功能建设规划

第二步：安全建设

组织建设	制度体系	能力体系建设			
决策层	方针政策目标原则	风险核查（C）		数据梳理(A)	
管理层	管理办法制度标准	漏洞扫描	配置核查	资产梳理	数据发现
执行层	操作指南具体规范	弱口令	风险评估	权限梳理	分类分级
普通员工	表单模板日志记录	预警监测（E）		数据保护（P）	
监督层		行为分析	权限变化	加密存储	数据脱敏
		访问监控	态势感知	访问控制	防泄漏
		人员安全意识培养		人员安全能力提升	

第三步：检查评估

防护能力评估	
风险、脆弱性评估	分类分级执行检查
安全策略执行检查	数据脱敏执行检查
影响评估	
权益影响分析	权益影响程度
安全保护措施有效性分析	安全事件可能性程度

第四步：安全运营

数据资源安全运营	数据安全策略运营	数据安全风险运营	数据安全事件运营	数据安全应急响应
数据分布地图	安全合规运营	风险持续监测	涉敏数据事件	应急组织机构
敏感数据视图	安全策略指标	异常行为监测	安全运维事件	应急人员配置
分类分级视图	安全策略视图	安全风险告警	安全事件告警	编制应急预案
访问热度视图	安全策略下发	安全风险处置	安全事件处置	开展应急演练
数据流向视图	安全策略优化	安全风险防范	安全事件防范	快速应急响应

通过安全运营反补能力持续提升

数据安全咨询规划服务

01 数据安全顶层规划咨询服务

- 以保障业务正常运转为基本要求，遵守国家数据安全法律法规合规要求、行业转型方针，**将安全聚焦在数据本身，围绕数据的生命周期来设计规划数据安全技术能力。**
- **以数据安全保障为基石，设计规划数据安全保障体系框架。**

交付成果 《数据安全保障体系规划报告》

02 数据分类分级咨询服务

- 借鉴数据治理成果，梳理需保护的数据资产目录，根据数据其价值及敏感程度建立统一的数据资产安全等级标准，为落实数据保护措施夯实基础。
- **数据安全等级一般至少分为公开、内部、敏感、高度敏感4个等级。**

交付成果 《数据分类分级管理指南》
《数据分类分级示例清单》

03 数据安全合规评估咨询服务

- 与先进理论、先进实践案例进行全方位对标，遵循国内外标准法规要求，找出合规差距，明确某单位组织在整个数据安全领域所处的位置。
- 充分分析数据安全合规风险，帮助企业对自身目前数据安全现状清晰认识。

交付成果 《数据安全合规性基线》
《数据安全合规性基线对标结果报告》

04 数据安全成熟度差距评估咨询服务

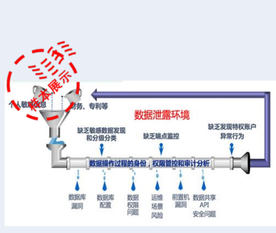
- 借鉴**DSMM思想**基于组织的数据生命周期，通过四个能力维度对数据安全能力进行标准化级别定义。
- **针对评估对象组织、围绕数据生命周期、聚焦组织在数据上的安全能力，**开展能力成熟度的评估工作，发现数据安全能力短板和数据安全风险。

交付成果 《数据安全差距评估报告》

05 数据安全风险评估咨询服务

- 以数据为中心，重点关注数据流转中的动态安全风险，特点是**基于业务场景识别数据流转各要素的安全风险。**
- 通过科学的数据安全风险评估方法，有效防范、降低关键业务系统的数据安全风险，**达到风险可控、最大限度地提升关键业务系统的安全保障能力。**

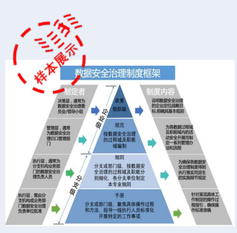
交付成果 《数据安全风险评估报告》



06 数据安全治理咨询服务

- 遵循自上而下原则，基于政策总纲确定数据安全整体目标、范围，从数据安全工作重心、数据安全全生命周期、体系建设等角度细化内容，制定适合某单位组织的数据安全治理体系。
- **数据安全治理建设目标是立战略、定组织、制总纲、建体系、 赋培训。**

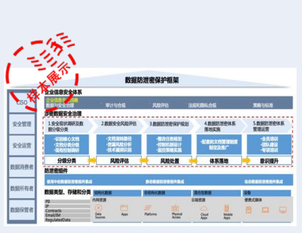
交付成果 《数据安全管理体系文件》（含方针政策、管理规范、操作指南单、流程表单）
《数据安全培训课件》



07 数据防泄密体系建设咨询服务

- 通过定位敏感数据，确保控制机密信息分发，防止数据丢失；
- 部署数据泄密防护系统，防止敏感信息泄露，确保对向外部实体传输控制；
- 管理新需求并支持事件管理，支持解决方案持续维护和有效性，确保企业对敏感信息安全处理的正确认识。

交付成果 《数据安全防泄密体系规划报告》

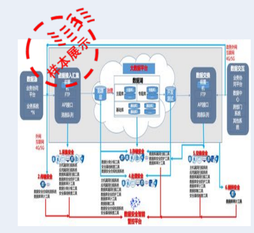


08 数据安全运营体系建设咨询服务

建设以“数据生命周期结合业务场景”的数据安全运营体系，遵循以下思路：

- 基于**一体化的建设思路**，避免单点能力组件堆砌所带来的风险；
- **数据安全能力综合能力输出**，包括规范、技术、运营、最佳实践；
- **自顶向下数据安全治理与管理、技术能力实现逐渐向运营落地转换。**

交付成果 《数据安全运营体系规划报告》



数据安全技术能力体系

CAPE数据安全能力框架

- 基于NLP和机器学习的自动精准数据分类分级
- 基于访问行为的动态最小化授权
- 大数据分布式高性能脱敏
- 支持机器学习建模等智能数据脱敏
- 多源数据的深度水印溯源

十大核心竞争力

- 敏感数据全链路测绘和管控
- 动态智能数据泄漏风险监测
- 支持大数据计算的TEE可信执行环境
- 兼容国内外多家TEE芯片的隐私计算技术
- 云网数用端：全方位、全链路、全生命周期

数据全生命周期安全防护体系

数据采集	数据存储	数据传输	数据处理	共享交换	数据销毁
分类分级	存储加密	传输加密	数据脱敏	访问控制	数据销毁
身份认证	备份恢复	身份鉴别	身份认证	数据脱敏	流程管理
采集审计	.....	数据脱敏	权限管理	数据水印	审计检查
.....		.....	.....	.....	.....

首创敏感数据全链路测绘，绘制数据流转图谱，全面风险感知及溯源

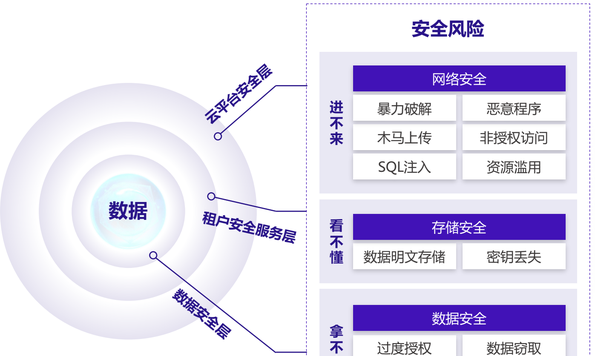
■ **日志源覆盖流量、终端、应用/API等图计算引擎自动关联**

■ **精准全链路测绘**
可视化界面高效感知风险及溯源风险

■ **覆盖全链路与数据全生命周期**
提供全方位安全保护

助力某大数据管理机构建立“可信、可用、可管”的数据安全管控体系

■ 以数据为中心，全面管控，风险进不来、数据看不懂、取不走



化理念为实践

安全方案

云平台安全

物理网络	虚拟化	云服务	安全管理
防火墙	资源隔离	认证鉴权	堡垒机
WAF	镜像安全	传输加密	漏洞扫描
入侵检测	安全补丁	API安全	日志审计
流量清洗	系统加固	安全日志	统一认证

租户安全服务

虚拟网络	主机安全	数据安全	应用安全
云火墙	主机安全	存储加密	云WAF
边界防火墙	容器安全	密钥管理	网页防篡改
安全组		数据库加密	
VPC		数据库审计	

数据安全

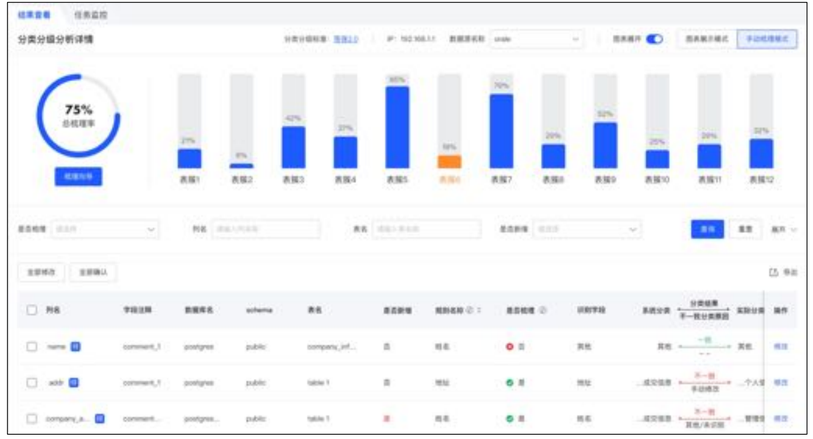
分类分级	数据安全	安全管控	安全运营
分类分级	数据脱敏	认证鉴权	资产风险
敏感数据发现	数据水印	统一策略	行为分析
	数据防泄漏	安全组	数据流监控
	数据库审计	VPC	运维审计

■ 数据安全管控平台

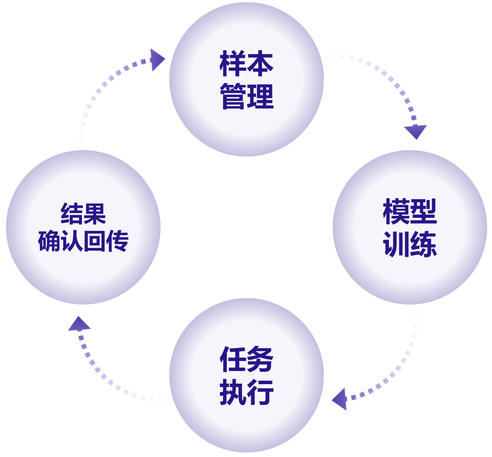
■ 开展常态化数据安全运营

帮助某金融客户建立线上化、自动化的数据安全分类分级能力

■ **无监督学习：**
对相似表/字段进行聚类，提高人工梳理打标效率



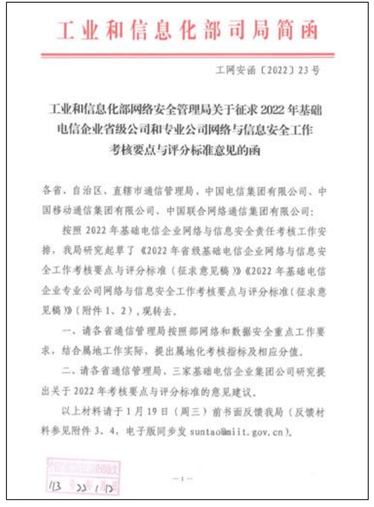
■ **有监督学习：**
不断积累分类分级标签，迭代模型释放人力



■ **敏感数据访问态势感知**

助力某基础电信企业数据安全标准贯标，落实重要数据安全管理工作

■ 工信部考核要点与评分标准



工业和信息化部司局简函

工网安函〔2022〕23号

工业和信息化部网络安全管理局关于征求2022年基础电信企业省级公司和专业公司网络与信息安全工作考核要点与评分标准意见的函

各省、自治区、直辖市通信管理局，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司：

按照2022年基础电信企业网络与信息安全责任考核工作安排，我局研究起草了《2022年省级基础电信企业网络与信息安全工作考核要点与评分标准（征求意见稿）》《2022年基础电信企业专业公司网络与信息安全工作考核要点与评分标准（征求意见稿）》（附件1、2），现转去。

一、请各省通信管理局按照部网络和数据安全重点工作要求，结合属地工作实际，提出属地化考核指标及相应分值。

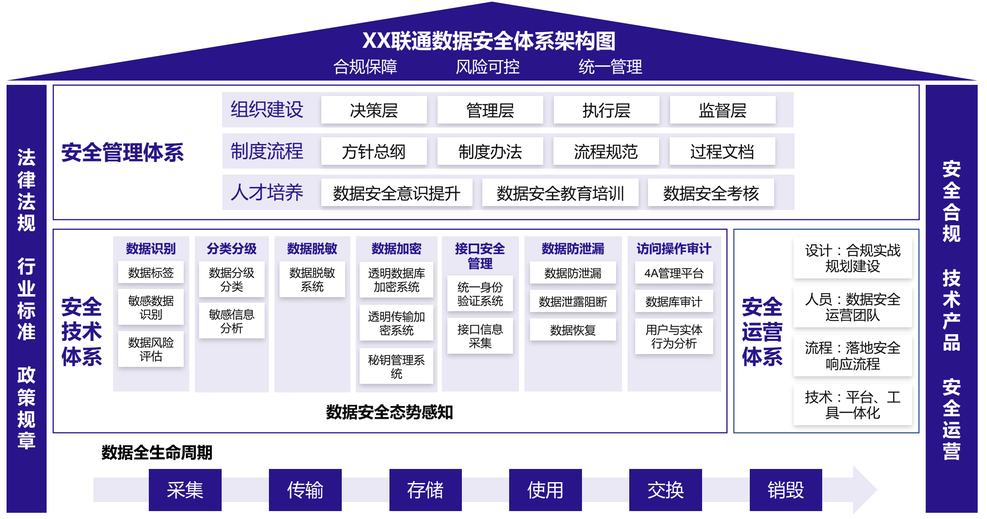
二、请各省通信管理局、三家基础电信企业集团公司研究提出关于2022年考核要点与评分标准的意见建议。

以上材料请于1月19日（周三）前书面反馈我局（反馈材料参见附件3、4，电子版同步发suntao@miit.gov.cn）。

■ 具体考核项扣分参考

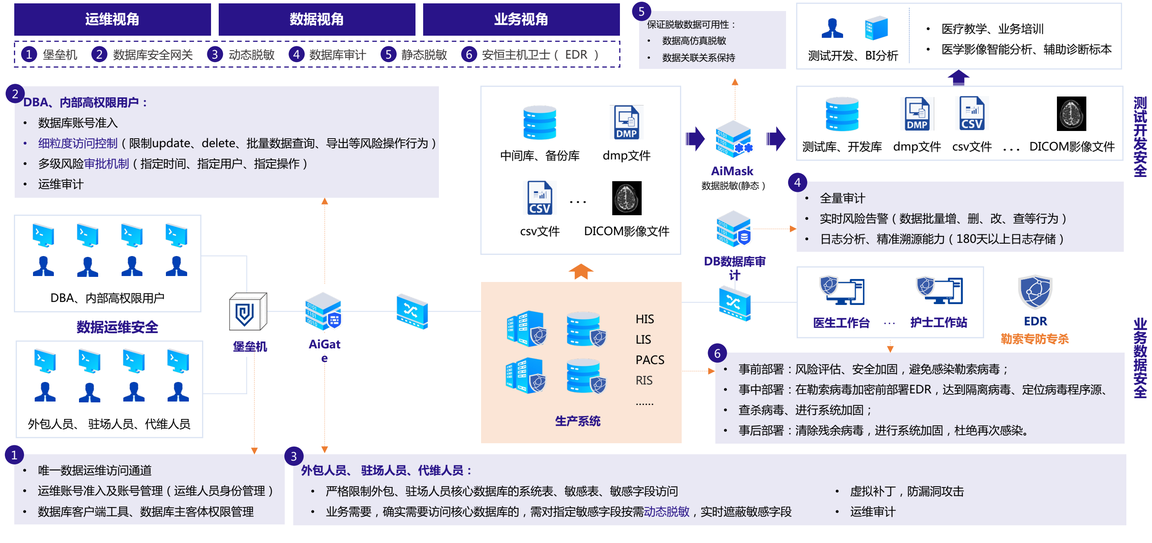
序号	考核项	指标定义	分值
1	按照《电信和互联网企业网络数据安全合规性评估要点》完成数据安全合规性评估，于数据安全公共服务平台(ds.cisns.cn)登记并更新评估完成情况，各项评估要点要求应于11月底前完成。对于处理大规模数据的业务，应开展新技术新业务安全评估，并形成评估报告。	础性评估要点 数据生命周期评估 技术能力评估	未按要求完成的，扣10分。
2	实施数据分类分级管理，对数据处理活动相关平台系统进行全面清查，输出数据资源分类分级清单:识别重要数据，形成重要数据清单。	数据分类分级 重要数据识别	未按要求完成的，每发现一项扣10分。
3	强化企业侧数据安全重点技术能力建设和使用，具备对数据资产的识别脱敏、接口安全管理、访问和操作行为安全审计等技术能力。	数据资产识别 数据脱敏 接口安全管理 访问和操作行为安全审计	未其备上述能力的，每发现一项扣10分。
4	建立数据安全态势信息报备制度，每季度末通过通信行业信安综合管理系统（kh.cisns.cn）向属地管局、集团公司报送企业数据识别梳理情况、数据安全态势、数据共享情况以及敏感数据处理及使用情况，集团公司汇总后报部网安局。	数据安全态势信息报备制度 企业数据识别梳理情况报备 数据安全态势情况报备 数据共享情况报备 敏感数据处理及使用情况报备	未定期报送信息累计发生两次及以上的扣10分。
5	规范数据对外合作使用与共享安全管理，在相关行为开展前进行合规审查，持续加强安全风险监测，并对异常行为进行预警。	数据对外合作使用合规审查 数据共享安全合规审查 安全风险监测 异常行为告警	对违规使用或提供数据的行为，每发现一起扣20分。

■ 落实重要数据安全管理，开展数据安全标准贯标工作



为某医院提供对机器学习友好的脱敏技术，大幅提高医学影像辅助诊断效率

■ 医院整体数据安全防护方案



■ 医疗机构脱敏技术的典型运用

➢ **医学影像文件在医疗教学、业务培训中的广泛使用（医学影像文件用作医疗培训）**

医学影像实训依托多媒体、人机交互、数据库等信息化技术，构建高度仿真的虚拟实验环境和实验对象，学生在虚拟环境中开展实验，达到教学大纲所要求的教学效果。

➢ **人工智能通过模型训练实现医学影像辅助诊断（科研教学和模型训练实现医学影像辅助诊断）**

医疗机构快速诊断。利用人工智能方法开展医学影像智能分析及辅助诊断方法，在实际应用中帮助医生提高工作效率、减少漏诊。在AI学习、分析过程中，需要大量的数据标本作为学习依据。

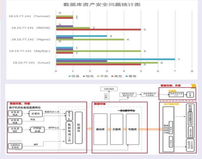
连续多年服务某交通运输行业客户，实现其一体化数字平台数据安全的全面保障

■ 建立适应客户自身业务特点的数据安全标准管理体系

1 数据安全现状调研

了解内部数据安全现状，梳理问题，评估一体化数字平台数据安全风险

弱点类型	风险数量	合计（91）
数据内容本身安全弱点	高等级风险：8	高等级风险：58 中等级风险：20 低等级风险：13
数据承载整体安全弱点 数据库资产弱点	高等级风险：30 中等级风险：6 低等级风险：11	
应用资产弱点	高等级风险：8 中等级风险：14 低等级风险：2	
典型数据安全管理弱点	高等级风险：12	



2 数据安全合规性分析

分析数据安全相关法律法规标准等要求，对比厅一体化数字平台情况，找出差距。

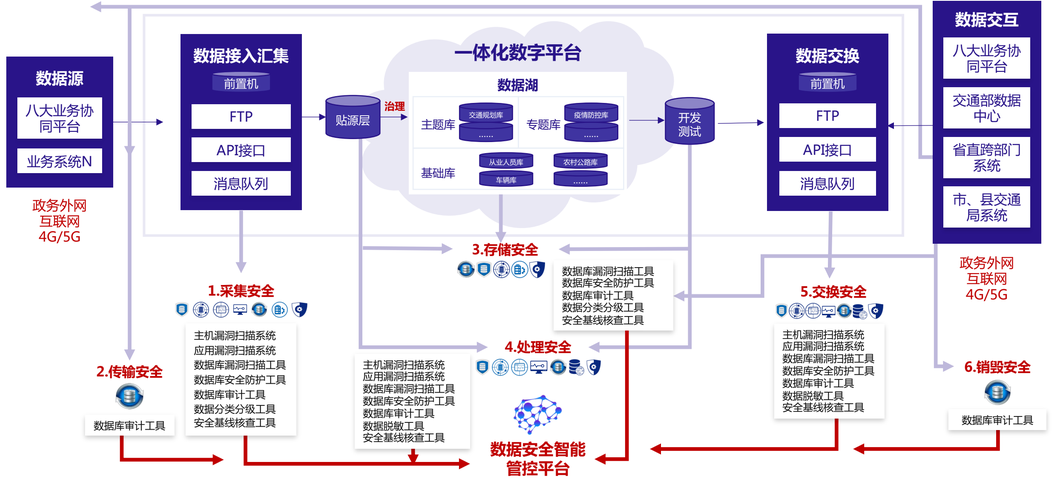
3 分类分级试点工作

联合编制《XX省交通运输厅非涉密政务数据分类分级指南》开展了3个业务系统分类分级试点工作。

4 数据安全专项规划

结合厅现状及发展需求，制定XX省“数字交通运输厅”数据安全专项规划。编制《XX省“数字交通运输厅”数据安全专项规划》。

■ 建立全链路全生命周期的数据安全防护体系



安恒自用零信任实践，以数字办公为基，为可控环境把好身份安全大门

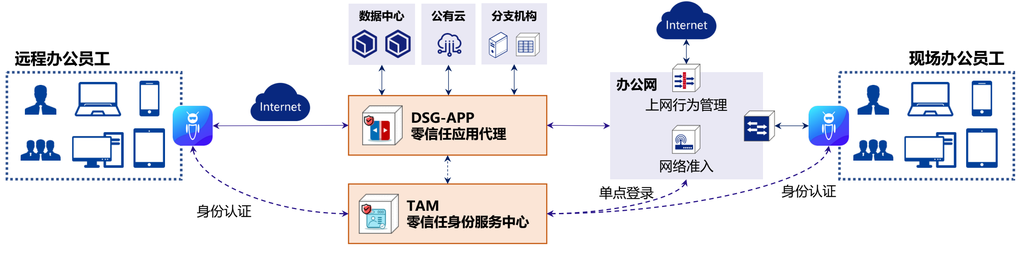
■ AiTrust零信任助力员工安全高效办公

一阶段建设

统一身份、多因子认证、应用隐藏、行为分析

二阶段建设

远程接入、网络隐身、 环境感知、智能选路



AiTrust助力安全高效办公：

- 随时随地安全访问公司内部应用
- 对接公司达邻门户 统一身份、快捷访问
- 动态的信任模型，兼顾身份安全及效率

■ AiTrust零信任三大亮点优势

➢ 灵活的身份安全适配

- 快速引入第三方身份安全设施及能力
- 全面身份认证及多维度身份鉴别

➢ 安全的业务访问通道

- 细粒度权限管控及访问控制
- 全流量业务加密
- 数据安全能力加持

➢ 动态的安全联动响应

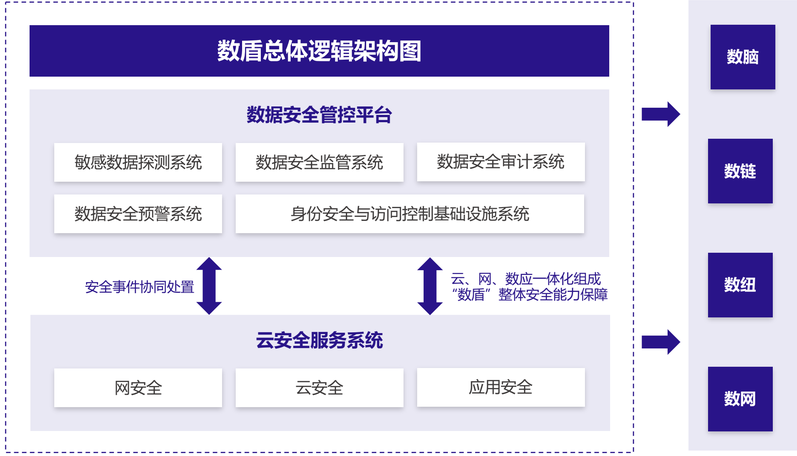
- 持续的身份安全评估
- 第三方安全分析、管理平台联动
- 终端环境安全感知及联动

助力“东数西算”工程，建设全国一体化大数据中心算力枢纽体系，确保网络数据安全

■ 四部委联合印发通知，“东数西算”工程全面启动

2022年2月，国家发展改革委、中央网信办、工业和信息化部、国家能源局联合印发通知，同意在京津冀、长三角、粤港澳大湾区、成渝、内蒙古、贵州、甘肃、宁夏等**8**地启动建设国家算力枢纽节点，并规划了**10**个国家数据中心集群。标志着“东数西算”工程全面启动。

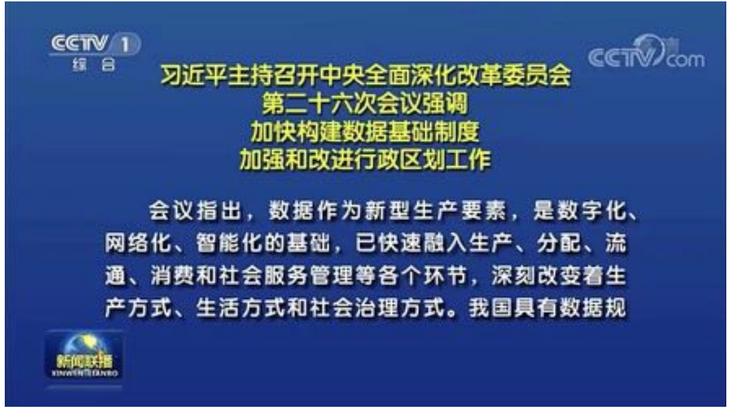
■ “数盾”为“数纽”、“数链”、“数脑”等提供全方位安全保障服务。



- 数盾实现大数据中心云、网、数和应用的安全保护工作，定位于一体化安全威胁防御者、安全态势分析者、安全事件处置者、安全机制管理者的四位一体角色。
- 包括数据安全管控平台和云安全服务系统。
- 为“数纽”、“数链”、“数脑”等提供认证、脱敏、加密、代理及可信接入等安全保障服务。

数据要素市场

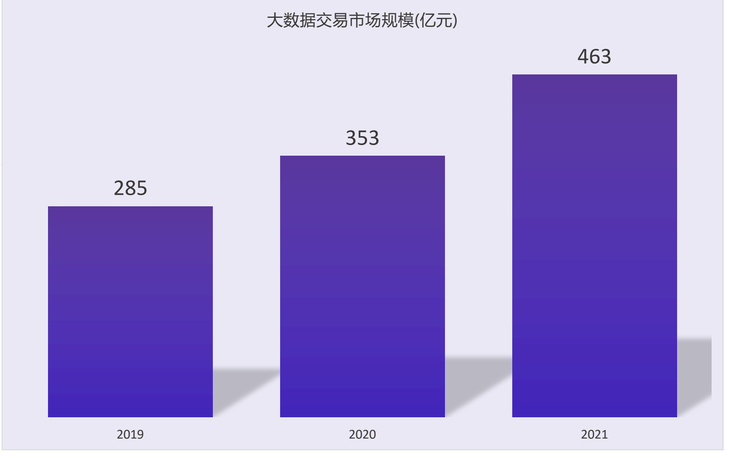
数据要素市场发展脉络



各地数据交易中心建设情况

序号	名称	成立时间	机构性质	
1	哈尔滨数据交易中心	2015年1月	国资参股转民营	注册资金3000万
2	贵阳大数据交易所	2015年4月	国有控股	注册资金5000万元
3	武汉东湖大数据交易中心	2015年7月	国资参与转民营	注册资金6000万
4	长江大数据交易所	2015年7月	国资参股，亚信控股51%	注册资金6000万
5	江苏大数据交易平台	2015年11月	江苏盐城国有控股	注册资金3000万
6	钱塘大数据交易中心	2015年12月	国资控股40%	注册资金3000万
7	西咸新区大数据交易所	2016年4月	国资控股70%	注册资金1000万
8	上海数据交易中心	2016年4月	国资参与民营控股	注册资金2亿元
9	浙江省大数据交易中心	2016年11月	国资控股	注册资金1亿元
10	青岛大数据交易中心	2017年4月	国资参股20%	注册资金5000万
11	山东数据交易有限公司	2020年1月	国资控股75%	注册资金5000万
12	北京国际大数据交易所	2021年3月	金控65%	注册资金2亿元
13	上海数据交易所	2021年11月	国资控股	注册资金2.5亿元
14	华南（广东）国际数据交易有限公司	2021年11月	国资控股	注册资金5000万
15	广州数据交易有限公司	2022年3月	国资控股	注册资金1亿元

大数据交易市场规模



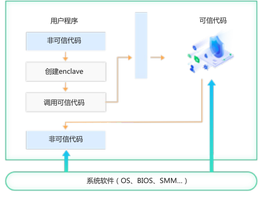
隐私计算技术与典型应用场景

AiLand数据安全岛

隐私计算中台

BDTEE

- 安全调试沙箱
- 可信执行环境
- 大数据计算集群
- SQL开发环境
- Python开发环境
- 分布式任务调度



MPC

- 隐私求交
- 匿踪查询
- 秘密分享
- 零知识证明
- 不经意传输
- 混淆电路

Federated Learning

- 水平联邦学习
- 垂直联邦学习
- 迁移联邦学习
- LR、xgboost、线性回归、决策树...

基础支撑系统

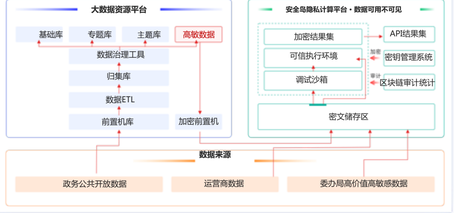
- 基于区块链技术和数字签名技术的行为审计系统
- 数据要素全生命周期加密系统
- 智能合约系统
- 密钥生成、分发、管理系统
- 数据要素流通流程审核审批系统
- 交易评估、报告系统

政务公共数据授权运营

大数据交易中心

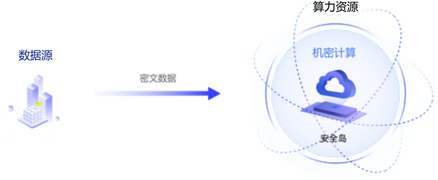
多方联合计算

敏感高价值政务数据共享开放



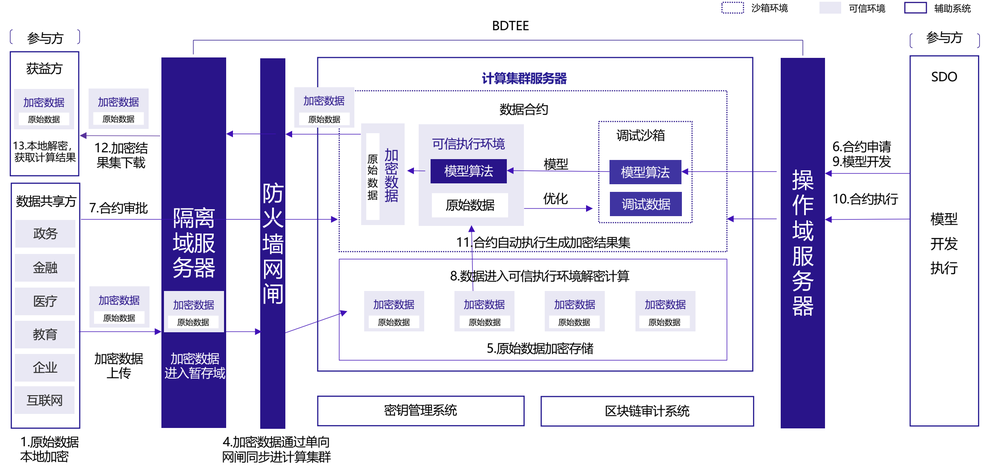
企业内部敏感数据使用和分析

外包计算

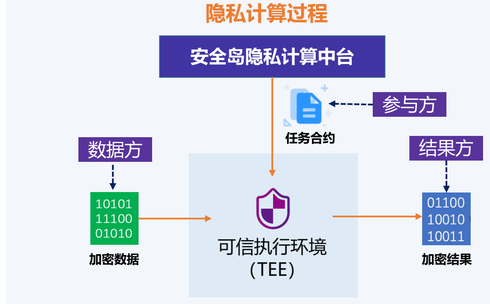


安恒BDTEE技术优势

安全岛平台系统架构



可信执行环境国产服务器适配



蚂蚁隐私计算一体机

华为鲲鹏

海光CPU

BDTEE技术优势

➢ 可信

- 参与方可信
- TEE可信

  1). 远程认证过程

  2). 引入CA模块
- 任务合约可信
- 操作记录上链可信
- 国产设备信创可信

➢ 端到端安全

- 数据全生命周期加密
- 数据使用全流程审批

➢ 隐私保护

- 数据全生命周期加密，原始数据不出域
- 调试环境和执行环境分离，数据可用不可见

浙江省大数据交易中心数据安全合规加工平台

交易中心“前店后厂”系统架构

下架 ↓ ↑ 上架

安全岛隐私计算平台

数据产品研发

车牌识别	信用分	规划选址
智能识别	四要素认证	...

模型加工 ↓ ↑ 数据服务

数据源

阿里	网易	华为
移动	电信	...

价值呈现

业务合法合规

《数据安全法》第三十三条
从事数据交易服务的机构提供服务，应当要求数据提供方说明数据来源、审核交易双方身份，并留存审核、交易记录。

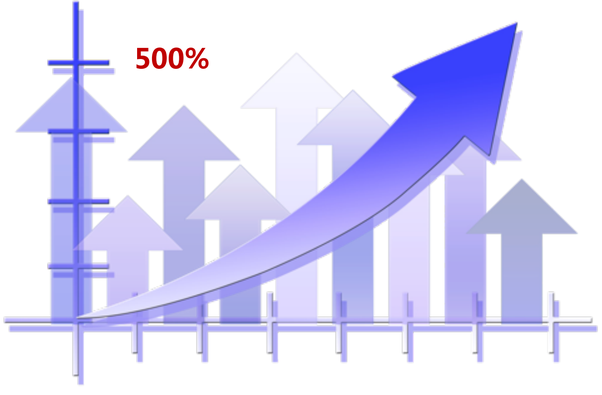
传统交易模式
数据资源交易

→

浙江省大数据交易中心
数据价值交易

数据确权	需要明确数据所有权	避免了原始数据确权问题，只对数字服务和产品确权
数据定价	需要对原始数据定价	无需对原始数据定价，数字服务和产品的价格由市场供需所决定
合法合规	交易中心承担合法合规风险	完全符合欧盟GDPR，美国CCPA，中国数据安全法等相关法律法规的要求
安全性	存在数据安全隐患	原始数据不出域，无安全隐患

2021年业绩增长



某市政务公共数据授权运营赋能智慧金融实践案例

三法联动

《网络安全法》《数据安全法》《个人信息保护法》三法联动，确立数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开 放相关法律法规；强调个人用户信息搜集的安全合规；网络数据的完整性、安全性、保密性等

相关政策

《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》提出要加快培育数据要素市场《国家十四五规划纲要》提出，要建立健全数据要素市场规则、浙江省数字经济发展“十四五”规划提出要深入实施数字经济“一号工程”，坚持发展和规范并重

■ 红线不清、场景不明正是当下数商们的集体焦虑

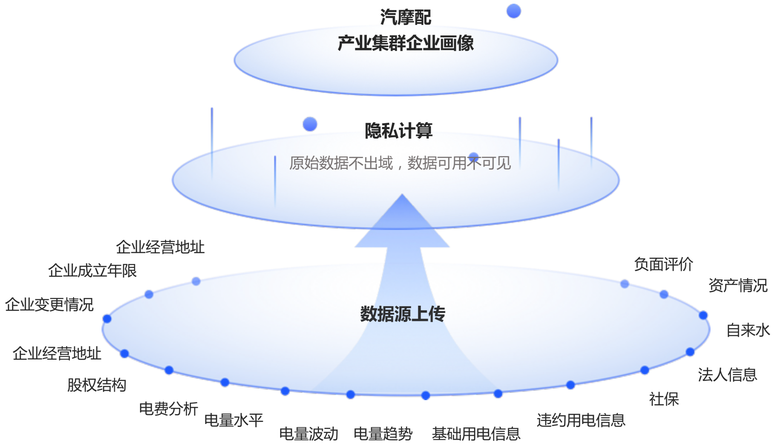
一大难题是如何做到数据安全？

另一大难题是如何深挖数据最大价值？

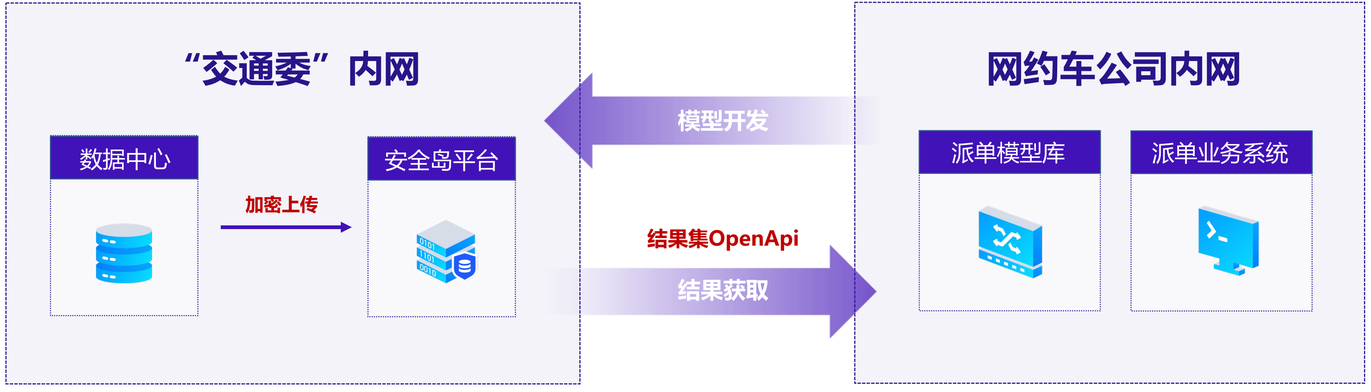
再一大难题是数据合法利用的边界在哪里？

架构设计

实践案例：当地银行对相关企业做针对性帮扶



某知名网约车公司和交通部门数据联合建模场景



➢ 网约车公司需求：

需要公交车站数据、公交车站乘客数量、公交车的状态、公交车到站时间等数据，制定网约车派单规则，形成数据出行生态系统

➢ 交通委数据安全需求：

- 数据共享通道安全
- 数据使用最小化授权，乘客个人信息、司机个人信息杜绝外传
- 数据使用安全审批

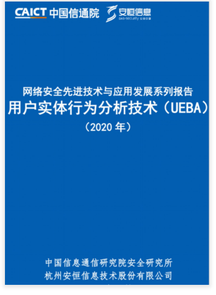
荣誉成果

研究成果与标准

- 承担国家级、省级示范课题76项，国家级课题30项
- 入选Gartner研究Toolkit: Vendor Identification for Cloud Security, Data Security, IAM and Security Operations in China
- 入选IDC中国数据市场研究报告
- 中国信通院DSI专家库
- 参与《金融数据安全数据生命周期安全规范》制定
- 参与《金融数据安全 数据安全评估规范》编写工作
- 信通院数据安全能力评测：安恒AiSort分类分级获基础级和进阶级认证
- 安恒信息担任“杭州数据安全联盟”理事长

发明专利

- 数据库内核对象入侵检测方法及系统
- 基于数据库协议的SQL注入审计或防护方法及装置
- 一种防数据库敏感数据泄漏的方法及系统
- MySQL数据库弱密码检测方法
- 数据库账号管理方法
- 数据库内核入侵隐藏触发器的探测方法及系统
- 数据资产管理方法及系统
- 一种基于多维度数据计算安全隐患评分方法和系统



客户案例

- 东数西算
- 数据要素市场
- 大数据交易中心
- 公共数据授权运营
- 智慧城市
- 政务数据共享交换
- ……

实践经验

- 2019年联合赛博研究院发布 《数据安全治理白皮书》
- 2019年联合阿里发布《政府数据安全保障实践》
- 2021年网络安全周，联合赛迪发布首个《智慧城市安全白皮书》
- 2022年联合CSA（云安全联盟）发布《隐私科技白皮书》
- 《数据安全治理白皮书》联合单位全国信息安全标准化技术委员会
- 《新一代数据要素市场建设》联合单位浙江大数据交易中心
- 《数字化转型浪潮下的数据安全最佳实践指南》书籍

助力构建安全可信的数字世界

“让业务放心大胆地使用数据，创造更大的商业和社会价值！”

2022 WEST LAKE
CYBERSECURITY
CONFERENCE

谢 谢

THANK U