CSA GCR 6th Congress 第六届云安全联盟大中华区大会

中孚信息 CSA GCR cloud security GREATER CHINA REGION alliance®

场景化数据安全思考与实践

演讲人：张振山

中孚信息股份有限公司

CSA GCR 6th Congress 第六届云安全联盟大中华区大会

目　录

CONTENTS

中孚信息

数据安全新要求

中孚信息

• 法规标准逐渐健全 • 数据安全监管增强 • 保障数据安全促进数据合法合规开发利用

2016 《网络安全法》

建立**网络安全监测预警**和信息通报制度
建立健全**网络安全风险评估**和应急工作机制
国家实行**网络安全等级保护制度**
采取**数据分类、重要数据备份和加密**等措施

2018 《网络安全等级保护条例》（征求意见稿）

落实**数据分类、重要数据备份和加密等措施**；地市级以上人民政府**建立网络安全监测预警和信息通报制度**；**对网络运行状态、网络流量、用户行为、网络安全进行动态监测**
建立并落实**重要数据和个人信息安全保护制度**
第三级以上网络应用采用密码保护，并使用**国家密码管理部门认可的密码技术、产品和服务**；**开展密码应用安全性评估**

2019 《密码法》

商用密码应用安全性评估与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接
法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施
建立**统一的商用密码监督管理信息平台**
密码管理部门和有关部门**建立日常监管和随机抽查相结合的商用密码事中事后监管制度**

2019 《关键信息基础设施安全保护条例》

推动**网络安全防护能力建设，开展网络安全监测、检测和风险评估**
每年至少进行一次**网络安全检测和风险评估**
运营者应当**优先采购安全可信的网络产品和服务**
建立健全本行业、本领域的关键信息基础设施**网络安全监测预警制度以及网络安全检查检测**

2021 《数据安全法》

国家建立集中统一、高效权威的**数据安全风险评估、报告、信息共享、监测预警机制**
开展数据处理活动**应当依照法律、法规，建立健全数据安全管理制度，采取相应的技术措施和其他必要措施**，保障数据安全
开展数据处理活动应当加强风险监测，定期开展风险评估

2021 《个人信息保护法》

个人信息处理者的义务：制定内部管理制度和操作规程；**对个人信息实行分类管理；**
采取相应的加密、去标识化等安全技术措施；合理**确定个人信息处理的操作权限**，并定期对从业人员**进行安全教育和培训**；制定并组织实施个人信息安全事件应急预案

2022 《网络数据安全管理条例》（征求意见稿）

数据处理者应当按照网络安全等级保护的要求，**加强数据处理系统、数据传输网络、数据存储环境等安全防护，应当使用密码对重要数据和核心数据进行保护**
重要数据的处理者**定期开展数据安全风险监测、数据安全宣传教育培训、风险评估、应急演练等活动**
对处理重要数据或者赴境外上市的数据处理者，**应当自行或者委托数据安全服务机构每年开展一次数据安全评估**

2022 《国务院关于加强数字政府建设的指导意见》

构建**全方位、多层级、一体化安全防护体系**
建立健全**数据分类分级保护、风险评估、检测认证等制度**，加强数据全生命周期安全管理和技术防护。**加大对涉及国家秘密、工作秘密、商业秘密、个人隐私和个人信息等数据的保护力度**
建立健全网络安全、保密监测预警和密码应用安全性评估的机制，定期开展网络安全、保密和密码应用检查
建立健全动态监控、主动防御、协同响应的数字政府安全技术保障体系。加强大规模网络安全事件、网络泄密事件预警和发现能力
强化安全可靠技术和产品应用，切实提高自主可控水平

数据安全成为保障经济发展、社会稳定和国家安全的重要基石，密集出台的法规政策对数据安全提出了新的要求

数据安全新挑战

中孚信息

➢组织数据资产体量大，资产信息难梳理

- 组织数据量大、结构复杂且不断生产，面对海量多源异构的原始数据难以一次性完成所有数据的分类分级管理。
- 在数据交换、共享等过程中，数据脱离原有载体再次引发数据分类分级及安全防护策略设置，快速摸清数据底账并保持数据分类分级的一致性以及防护策略的有效性成为政企面临的新挑战。

➢网络安全与数据安全分而治之，防护能力未融合

- 网络安全层面，已形成完备的安全防护体系；数据安全层面，已形成分类分级、加密、审计、脱敏等单点安全防护能力。但数据安全防护能力与网络安全防护体系尚未形成有机融合，缺乏围绕数据生命周期流转过程的整体化防护管理能力

➢多法多标准并轨并行，合规治理难统一

- “三法三条例多标准”体系已经成为网络安全防护和数据安全治理的主要合规驱动力。 政企需积极落实不同维度、不同方向的各类监管合规要求。如何应对众多且仍持续颁布的法律法规的合规要求，是摆在企业或组织面前的合规遵循难题

➢单点安全防护能力未闭环，数据流动风险难规避

- 数据具有广泛的流动性与易传播性，单点的安全防护手段缺乏协调联动能力，导致安全策略一致性差、管控效率低、全面性弱等问题， 出现“头痛医头， 脚痛医脚”的现象，无法发挥围绕数据全生命周期的整体防护合力。

➢传统风险评估应对数据安全，风险行为难检测

- 数据资产的量级与状态时刻发生动态变化，海量汇聚、指数增长、高频的特征，使得面向网络环境下的数据安全载体资产，基于某个 标准作为基准的传统静态、固化信息安全风险评估，无法顺应数据流动过程中不同环境、 不同目标下的安全评估要求。

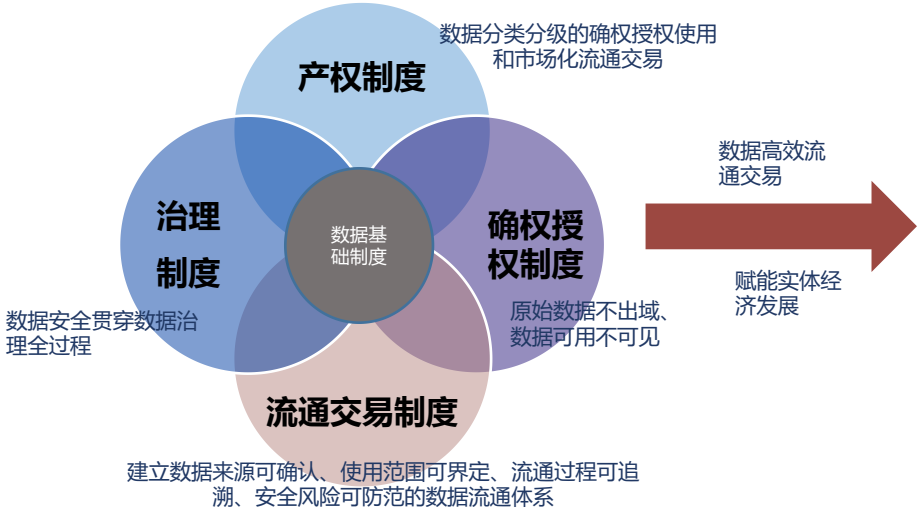
➢安全事件响应不及时，威胁溯源难取证

- 由于外部攻击、内部风险带来的数据泄露、窃取、篡改等安全事件发生后，事件响应延时长、告警信息不全面
- 数据流转共享流程长接触人员多，安全事件无法多源关联分析事件链条难还原威胁溯源过程取证不完整，如何形成围绕数据生命周期流转与安全事件全流程防护响应联动的整体化安全防护与管理能力成为新挑战

➢数据安全缺乏全局性顶层设计，安全体系建设难以发挥效力

- 现有数据安全体系有效性不可知，缺乏系统性评估诊断手段
- 数据安全新手段与现有体系、业务场景融合落地实施难度加大，缺乏全局性梳理与咨询手段
- 数据安全实施指导细则仍待完善，缺乏全面性合规落地实施指导
- 数据安全技术持续演进，智能化、场景化、平台化、国产化成为趋势，新技术风险评估缺乏标准规范

数据安全新方向



- 建立组织体系，落实主体责任
- 建立分类分级数据目录体系，分类分级制度从技术上确保落地
- 充分实践加密、脱敏、隐私计算、溯源认证、态势感知等等技术手段，严格规范数据流动与共享
- 建立定期体检机制，定期评估重要数据、个人隐私及跨境数据安全
- 建设确权授权机制，构建基于隐私计算的数据授权管理平台，与纵深防御体系联防联控

2022年12月2日，国家发展改革委发布了《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》（简称“数据二十条”）。“数据二十条”的发布，确立了明确的法规制度，指导正在落实数据安全制度的企业和组织，建设形成覆盖数据要素获取、加工、流通、利用等阶段的安全体系，我国正式进入数据合规高速流通赋能的全新阶段。

CSA GCR 6th Congress 第六届云安全联盟大中华区大会

目　录

CONTENTS

中孚信息

数据安全治理流程-加强顶层设计，整体建立数据安全体系

组建专门的**数据安全组织团队**：

- 是数据安全治理建设的首要任务；
- 是保证数据安全治理工作能够持续执行的基础。

1.定义组织-驱动治理

- 组织和职能
- 人员和岗位

2. 资产梳理-支撑治理

- 数据合规梳理
- 数据责任确权
- 数据资产梳理
- 安全风险评估
- 数据分类分级
- 安全整改方案

通过资产梳理能够掌握**数据资产分布、数据责任确权、 数据使用流向**等，使数据资产安全管理更全面。

3.策略制定-指导治理

- 战略规划
- 实施指南
- 管理要求
- 灾备方案
- 操作规程
- 应急预案
- 技术标准

掌握了数据资产概况后，需要制定**安全策略**来作为数据资产管控的安全规则。

4. 技术实施-落实治理

- 数据加密
- 数据安全监测
- 数据审计
- 数据态势感知
- 数据脱敏
- 数据授权运营
- 数据防护
- 数据共享交换

根据策略实施技术能力，事半功倍。

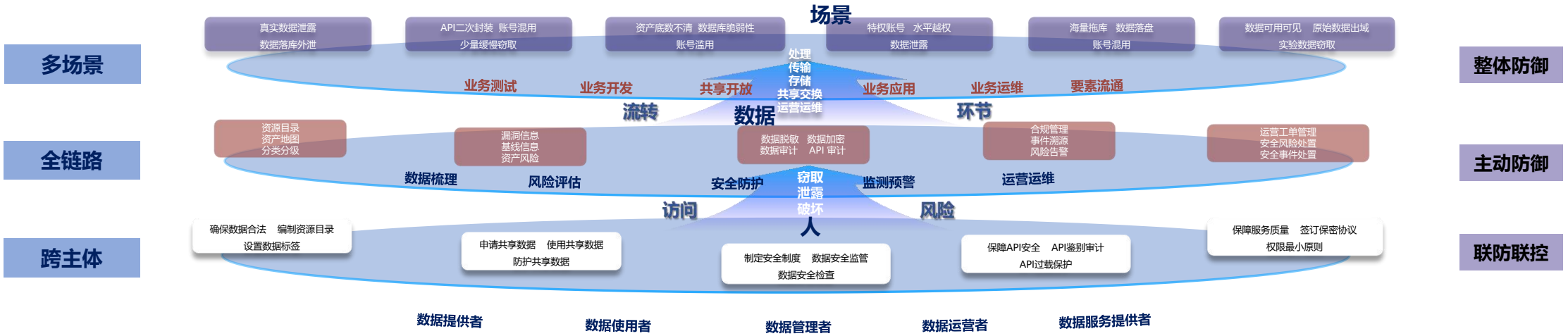
根据安全需要动态跟踪， **持续改善**。

- 通过资产梳理， 持续掌握数据资产动态；
- 通过预警演练， 提升应急响应能力；
- 通过数据安全评估，了解数据安全管控现状，持续优化安全策略。

5.安全运营-深化治理

- 有效验证
- 安全评估
- 考核评价
- 安全审计
- 安全检查
- 监督整改

数据安全体系模型-以场景为核心，抽象底层模型，支撑安全建设要求



数据安全技术架构-注重实效，按需投递安全技术能力

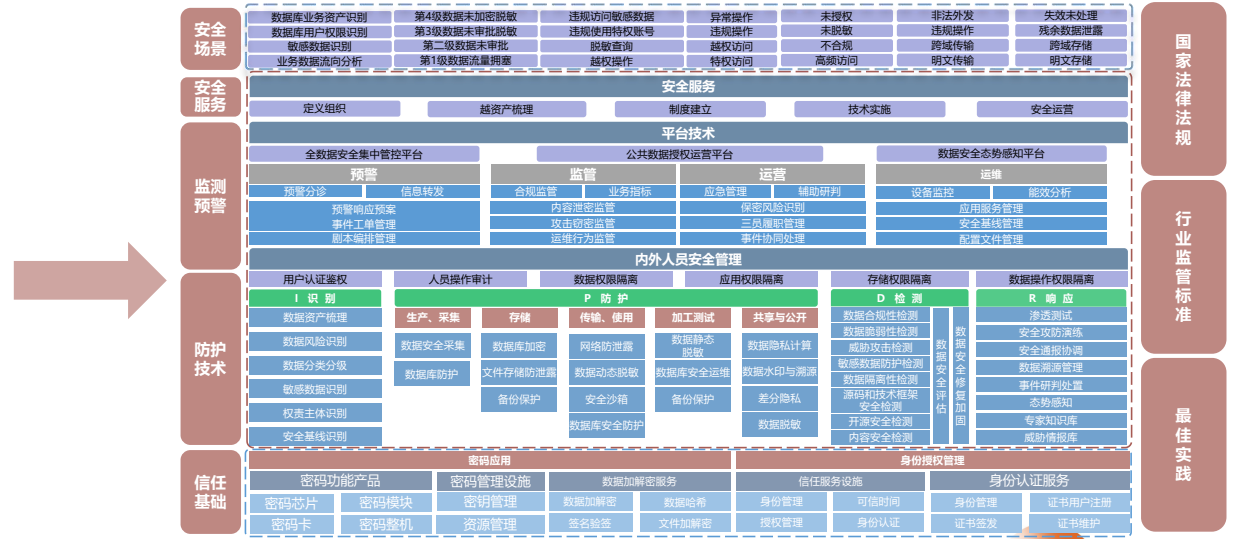
中孚信息

借鉴IPDR模型，围绕“人、数据、场景”深度关联的实际安全需求。

通过数据安全咨询规划设计组织机构、人员管理等制度流程，建立与之相配套的安全技术能力，有效融合形成平台化应用，发挥技术合力作用，达到安全实效。

+

通过持续对数据全生命周期内各使用场景进行风险监测，评估已有数据安全控制措施的有效性及薄弱环节，及时进行数据安全整改，优化数据安全制度流程及技术措施，提升数据安全防护能力，确保全数据安全。



数据安全方案框架-以风险为导向，三位一体打造综合防御能力

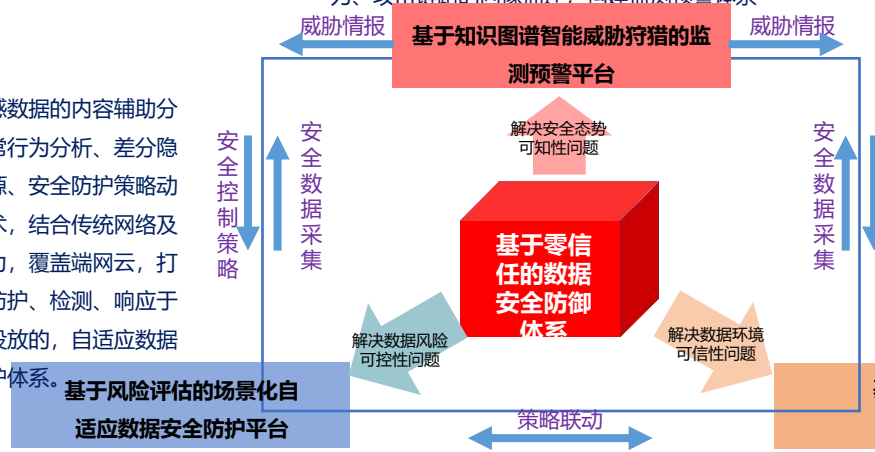
中孚信息

针对数据流转过程中的窃密、泄密、勒索等安全风险，基于数字化发展趋势，建设**基于环境感知的动态信任平台、基于风险评估的场景化自适应数据安全防护平台、基于知识图谱智能威胁狩猎的监测预警平台**，打造对终端数据、网络传输数据、云及应用系统数据的全方位安全保障、综合审计、监测预警等能力，服务于军工、政务、科技、金融等高安全**内部工作网络。**

打造**环境可信、风险可控、态势可知**“三位一体”的新一代数据安全智能防御体系

面向攻击窃密、内部泄密、加密勒索等数据安全防护场景，以全景数据安全知识图谱、智能威胁狩猎为手段，实现对攻击者、攻击行为、攻击链路的画像描述，构建监测预警体系

采用基于敏感数据的内容辅助分析、用户异常行为分析、差分隐私、隐写溯源、安全防护策略动态构建等技术，结合传统网络及平台安全能力，覆盖端网云，打造集识别、防护、检测、响应于一体的按需投放的，自适应数据安全主动防护体系。

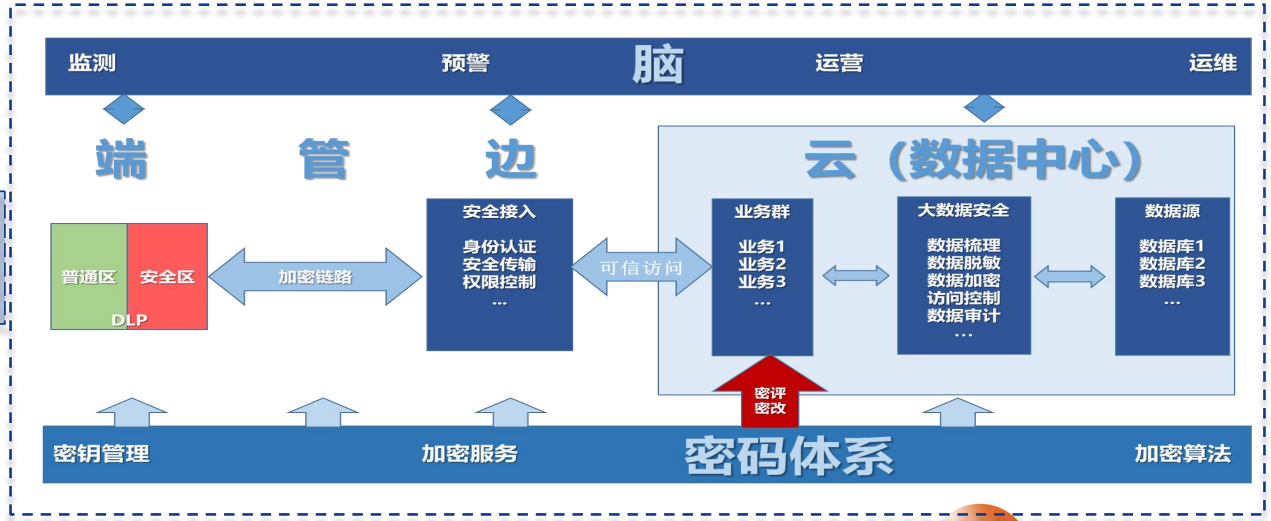


在传统网络安全的基础上，采用安全与保密手段相配合，密码与隔离技术相融合，以身份定义网络安全边界，实时感知环境变化，在主体与客体之间建立智能化、精细化的动态可信关系。

数据安全解决方案-数据安全与网络安全融合，构建全数据安全能力

基于全数据资产（结构化数据和非结构化数据）安全管理与防护需求及合规要求，以安全咨询服务为切入点设计顶层规划，融合零信任理念与数据安全新技术，**以密码为基石，身份为边界，敏感数据为核心，风险管理为导向**，内容与行为分析为抓手，合理编排多种安全技术能力，建立**云、管、端、边全链路**安全防线，打造全维防护、全程监管、全时运营、全面对抗的安全大脑，保障全生产要素、全业务流程、全生命周期数据安全，形成具备实战、实用、实效价值的**全数据安全解决方案。**

数据安全与纵深防御体系融合，安全工具集成一体化“全数据”安全平台



CSA GCR 6th Congress 第六届云安全联盟大中华区大会

目　录

CONTENTS

中孚信息

数据可信流通场景-公共数据授权运营

合规：实现数据收集遵循最小必要原则、数据用途可控可计量的目标，数据不出域，确保数据运营全流程合规

安全：基于云沙箱、多方安全计算和脱敏加密等数据安全套件的创新数据开发实验室，是数据生产力激活的利器

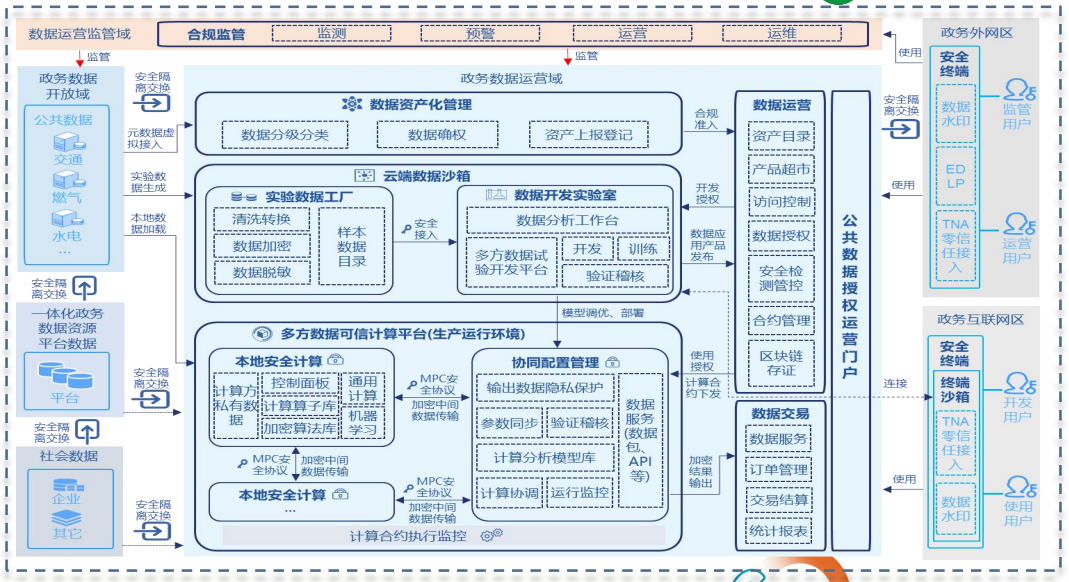
功能强：包括科学计算、神经网络预测、联邦建模等近千个密文计算函数和机器学习算法库，覆盖数据安全运营使用全部场景

高性能：国内领先的隐私计算技术，相比通用框架，通信量和速度有数量级提升，解决隐私计算技术推广使用的最大问题：性能问题

自主可控：基于严密的密码学理论的通用计算体系，支持国密算法，确保全栈的完全自主可控

存证追溯：基于区块链技术的用户认证、数据发布、数据申请、融合计算全业务流程存证

权威认证：通过信通院隐私计算技术标准认证，确保数据在可信、安全的环境中计算使用



数据安全使用场景-一机两用及工作秘密防护

依据**《政务外网终端一机两用安全管控技术指南》GW0015-2022、工作秘密信息防护指南（征求意见稿）**要求，部署架构设计如下：

➢ 终端数据安全

1、通过准入控制确保终端可信接入和安全管控，通过零信任网关实现基于身份的应用级别精准控制、审计，通过终端DLP实现敏感数据的流转跟踪、预警追溯；

2、采用沙箱隔离技术确保网络隔离、会话隔离、数据隔离，通过零信任终端与安全沙箱实施策略联动，确保数据外发、打印、刻录、防截屏等行为受控；

➢ 运行管理安全

1.通过数据安全态势感知平台实现数据资产统计，数据分类分级，数据流向跟踪，数据风险发现，安全事件预警，数据安全态势等可视化呈现。

➢ 边界安全

1、通过零信任网关建立加密通道，确保数据传输安全；

2、通过全流量检测器对所有流量进行安全检测，识别恶意行为并告警和阻断；

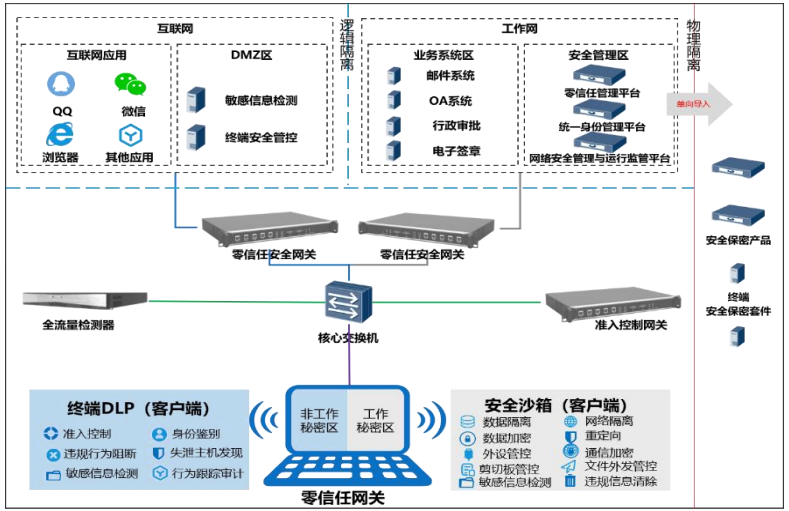
➢ 云端数据安全

1、通过数据库脱敏实现数据隐私保护；

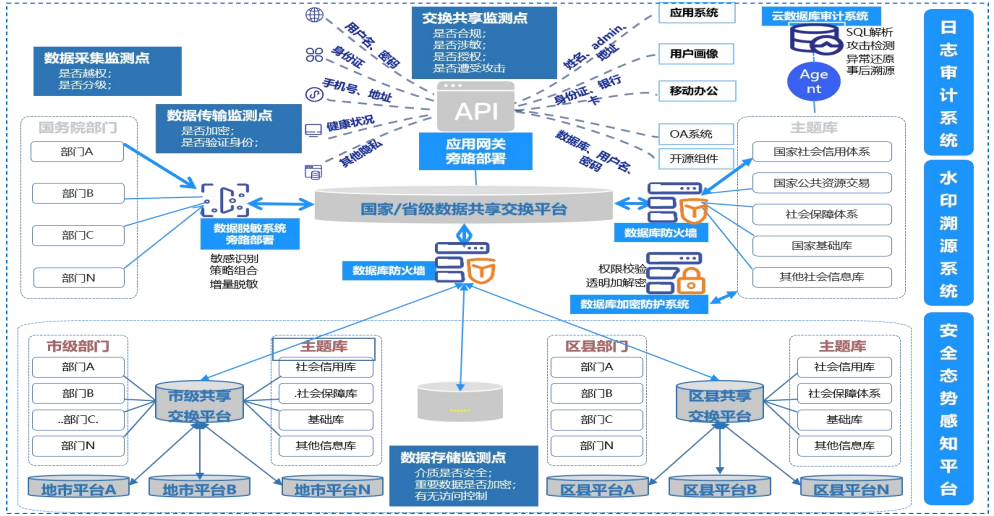
2、通过数据库防火墙实现访问控制；

3、通过数据库审计实现全链路跟踪审计；

4、通过数据库加密实现重要数据保护；



数据共享开放场景-全链路安全审计



重点基于**情报构建API行为**基线，发现未知攻击风险，包括历史行为异常模型、账号/IP行为异常模型、特征基线异常模型；

◆采用基于大数据分析的UEBA技术，构建全链路数据交换共享的攻击、窃取、篡改等高危操作、违规操作、越权访问行为识别发现并预警；

◆采用“关键字、规则引擎、上下文+NLP分析”等多种技术对全域个人隐私数据、敏感数据、重要数据构建“有无特征”的自动识别能力；

◆构建全链路数据处理活动日志记录系统，对数据处理活动中的关键环节进行埋点，根据“一数一源”的指导思想，绘制每批次数据的流经轨迹和时序图，便于追踪溯源；

◆构建全流程数据水印溯源系统，包括电子文档、音视频等非结构数据的数字水印和结构化数据的数据水印；

◆根据SIEM架构理念，构建全流程数据安全态势感知平台，对数据安全风险进行及时预警、响应、（处置）安全防护联动、跟踪及处理成效评估。

CSA GCR 6th Congress 第六届云安全联盟大中华区大会

中孚信息 CSA GCR cloud security GREATER CHINA REGION alliance®

THANK YOU.