数据安全市场研究报告

Data security research report

2022-10

数说安全研究院有限公司

• 目录

数据安全背景与政策

1. 数据安全新旧定义
2. 等级保护标准下的数据安全要求
3. 数字经济上升为国家重要发展战略
4. 《数据安全法》颁布，数据安全新时代到来
5. 数据安全法律体系及标准体系逐步完善

• 数据安全的新旧定义

在网络架构相对简单的早期，数据一般只在服务器、网络和办公电脑之间流存，因此数据安全通常被定义为数据库安全和内部数据防泄漏，通过如设置数据库权限、复杂密码等方式保护好数据库，通过规范员工行为、文档加密等方式防止内部数据泄漏。

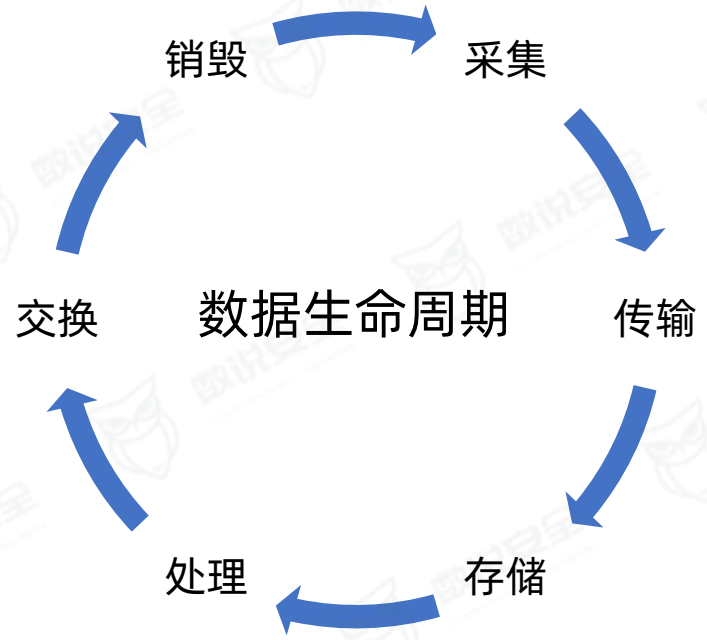
随着互联网的快速发展，信息化程度的不断提升和数据时代的到来，数据的流存节点和区域变得繁杂，流动量呈现指数级增长，使用方式也不断多样化，原有的保护方式已无满足当下的安全需求，数据安全作为独立的安全体系被重新定义。

《中华人民共和国数据安全法》的第三条中，给出了新的数据安全定义：
数据，是指任何以电子或者其他方式对信息的记录。
数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。
数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

数据安全和网络安全的边界：

狭义的网络安全（Network Security）是以网络为中心安全体系，使用防火墙、网络访问控制、分布式拒绝服务攻击等防护手段，强调节点和区域的保护形式。随着云、网、端的不断延伸，网络安全（Network Security）的概念逐步拓展至网络空间安全（Cyberspace Security），也就是广义的网络安全，泛指一切处于通信网络覆盖下的安全体系。

新的数据安全（data Security ），是指以数据为中心的安全体系，以数据的采集、传输、存储、处理（使用）、交换（共享）、销毁等覆盖全生命周期的安全为目标，侧重于从数据产生到销毁的全生命周期的保护，保护方式类似于伴随数据全生命周期的安保人员，强调数据的所有权、管辖权、隐私权等。



• 等级保护标准下的数据安全要求

过去，我国数据安全建设包含在网络安全的建设之中，以满足等级保护规范要求为主要标准，围绕数据库保护、数据防泄漏、数据脱敏等展开。

以大多数企业需要满足的等级保护2.0中的第三级安全要求为例，对其中与数据安全相关性较高的标准进行梳理，“边界防护、访问控制、安全审计、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护、审查与检查、密码管理、安全事件处置”等构成了在等级保护标准体系下的数据安全要求，也因此形成了围绕数据库保护和数据防泄漏为中心的“数据库防火墙、数据库审计、数据防泄漏，数据脱敏，容灾备份”等主要产品，及相应的管理制度、审查办法和安全运维。

等级保护2.0通用安全要求

要求类型	一级标题	次级标题
通用安全要求	安全通信网络	通信传输
	安全区域边界	边界防护、访问控制、安全审计
	安全计算环境	访问控制、安全审计、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护
	安全管理中心	系统管理、审计管理、安全管理、集中管控
	安全管理制度	安全策略、管理制度
	安全管理机构	审查和检查
	安全运维管理	介质管理、网络和系统安全管理、密码管理、备份与恢复管理、安全事件处置、紧急预案管理、外包运维管理

等级保护2.0扩展安全要求

要求类型	对象	次级标题	项目
扩展安全要求	云计算	安全区域边界	访问控制、安全审计
		安全计算环境	访问控制、镜像和快照保护、数据完整性和保密性、数据备份恢复、剩余信息保护
		安全管理中心	集中管控
	移动互联网	安全区域边界	边界防护、访问控制
	物联网	安全计算环境	网关节点设备安全、抗数据重放、数据融合处理
	工业控制系统	安全通信网络	通信传输
		安全区域边界	访问控制、无线使用控制
		安全计算环境	控制设备安全

• 数字经济上升为国家重要发展战略

近年来，政策规划不断加强对数字经济和数据要素的指导及要求，数据要素和数字经济的重要性不断提升。

2021年12月国务院印发《“十四五”数字经济发展规划》，指出数字经济成为继农业经济、工业经济之后的主要经济形态，是重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量，要求到2025年，数字经济迈向全面扩展期，数字经济核心产业增加值占GDP比重达到10%。数据作为数字经济时代下的基础性资源和战略性资源，是决定国家经济发展水平和竞争力的核心驱动力。

发展数字经济正式上升为国家重要发展战略，数据安全则成为保障数字经济健康发展的重要基石。

发展数字经济的战略规划文件

时间	文件名称	数据关键内容	数据安全关键内容
2020年4月9日	《关于构建更加完善的要素市场化配置体制机制的意见》	将数据列为生产要素并强调要加快数据要素市场的培育。	加强数据资源整合和安全保护：制定数据隐私保护制度和安全审查制度，推动完善适用于大数据环境下的数据分类分级安全保护制度。
2021年11月30日	《“十四五”大数据产业发展规划》	加快培育数据要素市场，完善数据要素产权性质、建立数据资源产权相关基础制度和标准规范、培育数据交易平台和市场主体。	筑牢数据安全保障防线：加强数据安全管理，加大对重要数据、跨境数据安全的保护力度，提升数据安全风险防范和处置能力，做大做强数据安全产业，加强数据安全产品研发应用。
2021年12月12日	《“十四五”数字经济发展规划》	优化升级数字基础设施，充分发挥数据要素作用，大力推进产业数字化转型，加快推动数字产业化，提升数字化公共服务水平，完善数字经济治理体系。	提升数据安全保障水平：依法依规加强政务数据安全保护，做好网络安全审查，云计算服务安全评估，增强重点行业数据安全保障能力，进一步强化个人信息保护，规范身份信息、隐私信息、生物特征信息的采集、传输和使用，加强对收集使用个人信息的安全监管能力。

• 《数据安全法》颁布，数据安全新时代到来

数说安全

2021年6月10日《数据安全法》颁布，并于2021年9月1日正式施行，作为数据领域的纲领性和基础性法律，以准确定义数据、数据处理、数据安全为出发点，提出解决数据全生命周期中的数据安全问题，达到数据开发利用、产业发展和数据安全相互促进的目标，重新改写了数据安全的定义，标志着数据安全新时代的到来。

随着数据的价值被不断认知，数据的应用场景不断拓宽，数据的安全问题也不断放大，数据攻击、数据泄露、个人信息滥用等数据安全问题日益加剧，给社会各领域数字化转型的持续深化带来了严重威胁（2020年全球数据泄漏达到360亿条，创历史新高，其中个人隐私信息泄露事件更是超出过去15年总和，数据诈骗、大数据杀熟和个人生物特征信息滥用等多类危害国家政府安全和个人合法权益的事件层出不穷），为保障国家数字经济健康有序的发展和个人及组织的合法权益，提高数据安全风险防控能力，《数据安全法》、《网络安全法》和《个人信息保护法》三部上位法相继颁布。

全国人民代表大会通过颁布

2017年6月施行

鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展；
明确网络运营者和关基设施运营者应做好数据分类、重要数据备份、加密和重要数据境内留存等措施，防止数据泄露或者被窃取、篡改；
明确相关法律责任及处罚措施。

2021年9月施行

明确数据的定义和边界，促进以数据为关键的数字经济发展；
明确建立健全数据分类分级制度，安全审查制度，风险评估、检测预警等机制，促进数据安全监测评估、认证的发展，建立数据交易管理制度等，加强数据出境的监管；
明确数据处理者和关基设施运营者的应建立全流程数据安全管理制度，做好数据安全保护、监测、应急处置和风险评估等措施。
进一步明确数据安全相关的责任，细化相应处罚措施。

2021年11月施行

构建完整的个人信息保护框架，采取分级保护制度；
进一步细化、完善个人信息处理活动中个人的权利，及处理者的原则、要求和权利、义务；
明确个人信息跨境提供规则；
明确相关法律责任及处罚措施。

• 数据安全法律体系逐步完善，上位政策加速出台

伴随数据安全及相关上位法的相继颁布，数据安全上位政策也在加速出台，数据安全法律体系正在加速建立。

2019年5月28日

《数据安全管理办法（征求意见）》

明确数据收集应制定并公开收集使用规则，提出收集动作和规则制定的相关要求。
明确数据处理使用时，应参照国家有关标准，采用数据分类、备份、加密等措施加强对个人信息和重要数据保护。
明确国家主管部门和网络运营者应对数据安全进行监督管理。

2019年6月13日

《个人信息出境安全评估办法（征求意见稿）》

规定网络运营者向境外提供个人信息，应进行安全评估，并明确相关要求。

2020年4月10日

《网络数据安全标准体系建设指南（征求意见稿）》

明确了网络安全数据安全标准体系框架；
明确需要建立基础共性标准、关键技术标准、安全管理标准和重点领域标准。

2021年9月1日

《关键信息基础设施安全保护条例》

明确运营者应履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度，发生关键信息基础设施重要数据泄露、较大规模个人信息泄露、特别重大网络安全事件或者发现特别重大网络安全威胁时，及时向国家网信部门、国务院公安部门报告。

2021年10月29日

《数据出境安全评估办法（征求意见稿）》

规定数据处理者向境外提供重要数据和个人信息，应进行安全评估，并明确相关要求。

2021年11月14日

《网络数据安全管理条例（征求意见稿）》

明确建立数据分类分级保护制度，将数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。
明确对数据处理者的一般规定，和涉及个人信息、重要数据及数据跨境时的要求；
明确互联网平台运营者的义务；明确国家部门的监督管理责任和内容；
明确法律责任和处罚制度。

2021年12月31日

《网络安全标准实践指南——网络数据分类分级指引》

给出了网络数据分类分级的原则、框架和方法，可用于指导数据处理者开展数据分类分级工作，也可为主管监管部门进行数据分类分级管理提供参考。

• 数据安全标准体系加速建立，行业和地方规范标准密集落地

数说安全

安全发展、标准先行，标准化工作是保障网络数据安全的重要基础，近年来各行业、地方的数据安全标准规范密集落地，加紧制定，数据安全逐步迈入有法可依，有据可查的强监管时代。

电信行业	《基础电信企业数据分类分级方法》	《电信运营商 大数据安全管控分类分级技术要求》	《基础电信企业重要数据识别指南》
	《电信网和互联网数据安全通用要求》	《电信和互联网行业数据安全标准体系建设指南》	《电信网数据泄露防护系统（DLP）技术要求》
	《电信大数据平台数据脱敏实施方法》	《电信网和互联网数据安全评估规范》	《电信网和互联网数据安全评估实施技术要求》
	《电信运营维护管理数据的管理技术要求》	《电信网和互联网数据安全风险评估实施方法》	……
金融行业	《金融数据安全分级指南》	《个人金融信息保护技术规范》	《金融大数据 术语》
	《证券期货业数据分类分级指引》	《金融业数据能力建设指引》	《金融数据安全数据生命周期安全规范》
	《金融大数据平台总体技术要求》	《中国银保监会监管数据安全管理办法（试行）》	《金融数据安全评估规范（征求意见稿）》
	《数字函证银行应用数据规范》	《保险行业信息共享平台数据交换规范》	……
政府行业	《政务服务平台基础数据规范》	《政务数据分类分级规范/指南》	《政务服务平台接入规范》
	《公共安全大数据 数据采集与预处理》	《信息安全技术 个人信息去标识化指南》	《信息安全技术 个人信息安全规范》
	《信息技术 大数据 政务数据开放共享》	《政务数据平台 第3部分：数据存储规范》	《基于云计算的电子政务公共平台服务规范》
	《信息安全技术 数据交易服务安全要求》	《信息安全技术 政务信息共享 数据安全技术要求》	……
	……		
计划制定	《信息安全技术 重要数据处理安全要求》	《信息安全技术 个人信息跨境传输认证要求》	《信息安全技术 政务数据处理安全要求》
	《信息安全技术 公共数据开放安全要求》	《信息安全技术 敏感个人信息处理安全要求》	《信息安全技术 数据安全评估机构能力要求》
	《信息安全技术 数据安全风险评估方法》	《信息安全技术 电子数据收集提取技术要求》	……

数据安全市场发展概况

1 • 市场空间及客户分布

2 • 行业发展情况及增速

3 • 数据安全关键词热度

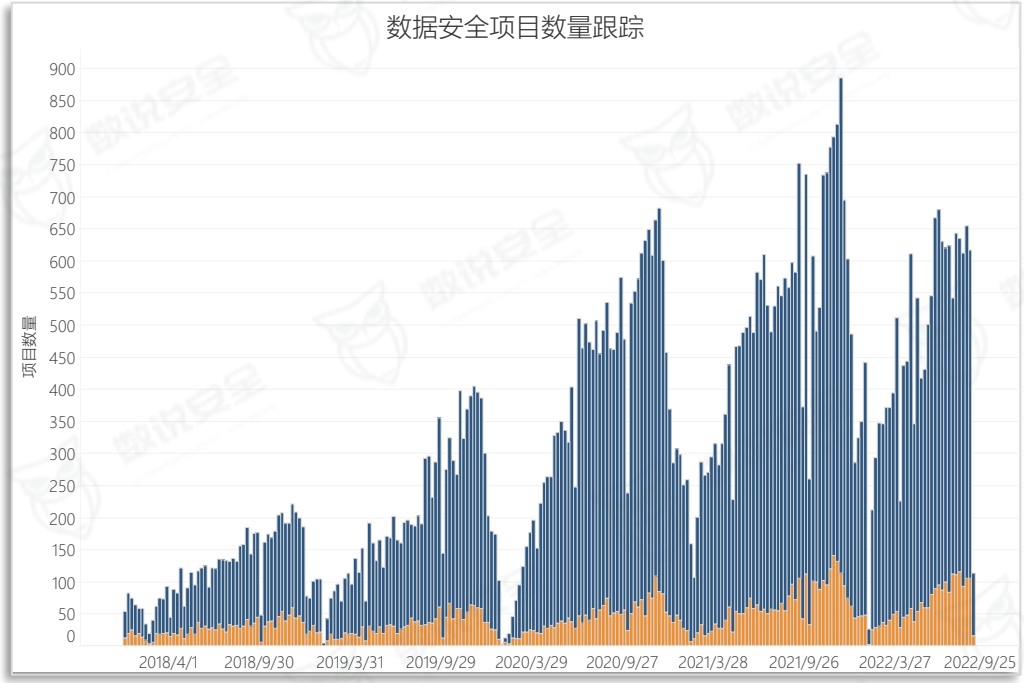
4 • 产品采购情况及增速

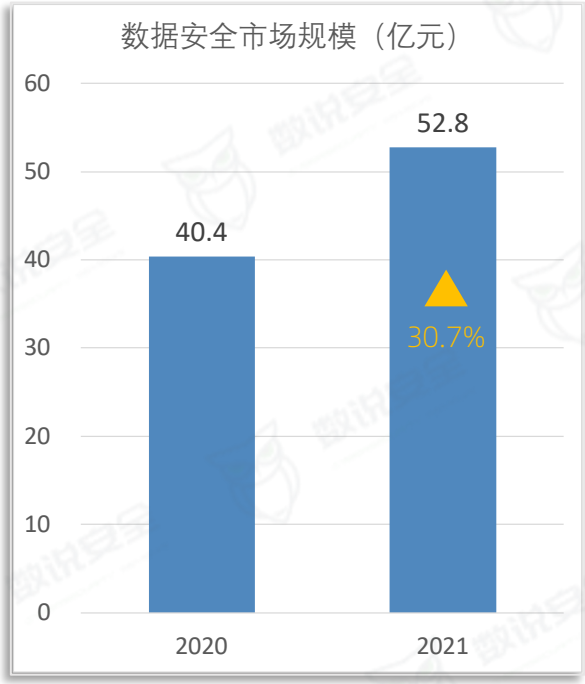
• 数据安全市场快速增长，经济发达地域建设先行

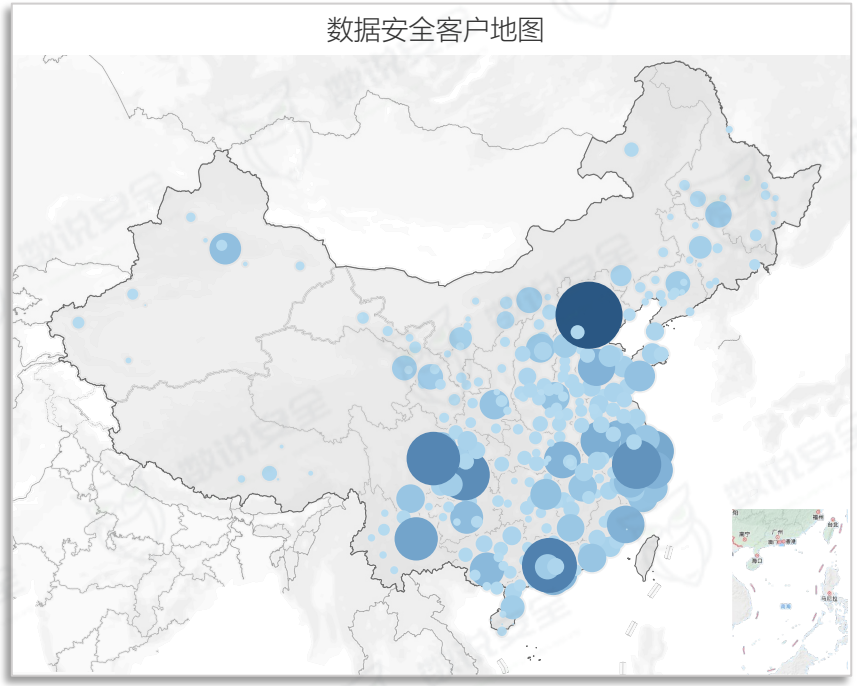
2021年我国数据安全市场规模约为53亿，同比增长30.7%，随着上位法律和政策的出台，以及规范标准的加速落地，未来数据安全市场仍将保持较好的增长态势。

社会整体对数据安全的重视程度显著提升，2021年采购数据安全产品的项目数量约23000个，同比增长28%，其中，2021年数据安全专项采购项目约3000个，同比增长约43%，明显高于行业平均增速。

数据安全能力的提升和信息化建设的进程紧密相关，因此采购数据安全项目的客户多集中在经济发展较快、数字化建设程度较高的京津冀地区、长三角地区、粤港澳大湾区和川渝地区。





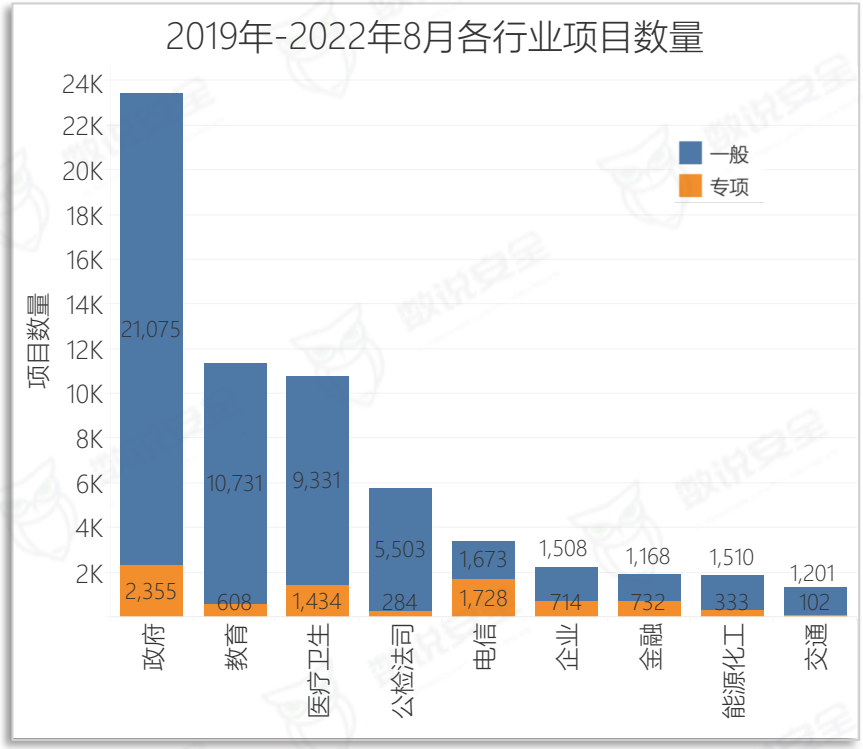


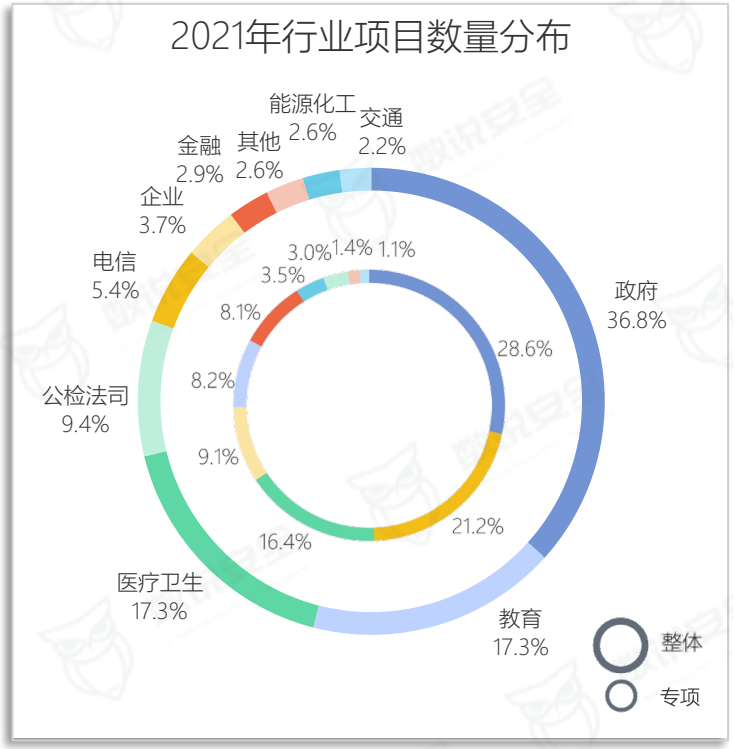
• 政府、电信、金融等行业数据安全建设领先

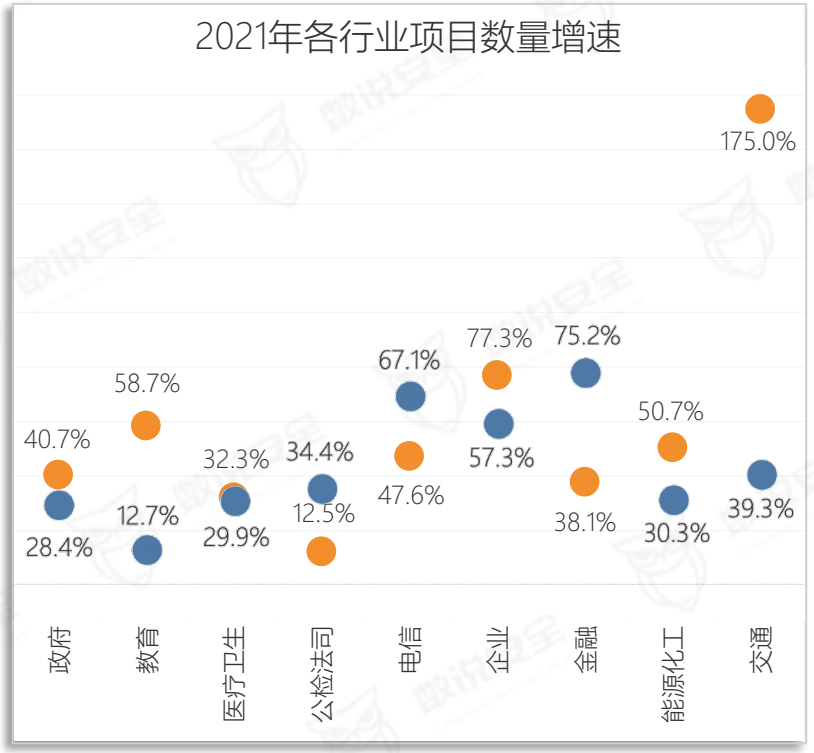
由于各行业对数据的采集保存量和使用频率不同，以及相关数据安全法律法规、政策要求出台时间的先后之分，数据安全项目采购需求呈现出明显不同。

政府、医疗卫生、教育和公检法司行业是数据安全项目的主要建设行业，占到了整体采购量的81%，虽然项目采购数量居前，但专项项目占比和2021年专项项目增速不高（教育行业基数较低导致2021年增速高），说明以上行业整体的数据安全治理建设进程相对较慢，或只有少量细分领域的客户开始进行数据安全建设。

其中电信、企业、金融和能源化工行业的项目数量虽然不多，但专项项目占比和2021年增速相对较高，说明这些行业的数据安全建设相对领先，其中电信和金融的进程明显领先。







• 解决方案、隐私计算关注度提升

根据数说安全统计（2018年至2022年6月），数据库安全、数据防泄露、数据脱敏依然是市场的主流关注点，作为数据安全基础产品，在未来很长一段时间依然会处于数量热度的高位；数据分类分级、数据安全管控、数据安全治理类解决方案和隐私计算（多方安全计算、可信执行环境、联邦学习）的热度增速明显提升，说明一些行业数据安全规范标准进展较快及数据共享业务需求已经展开，预计未来依然会保持较高增速。

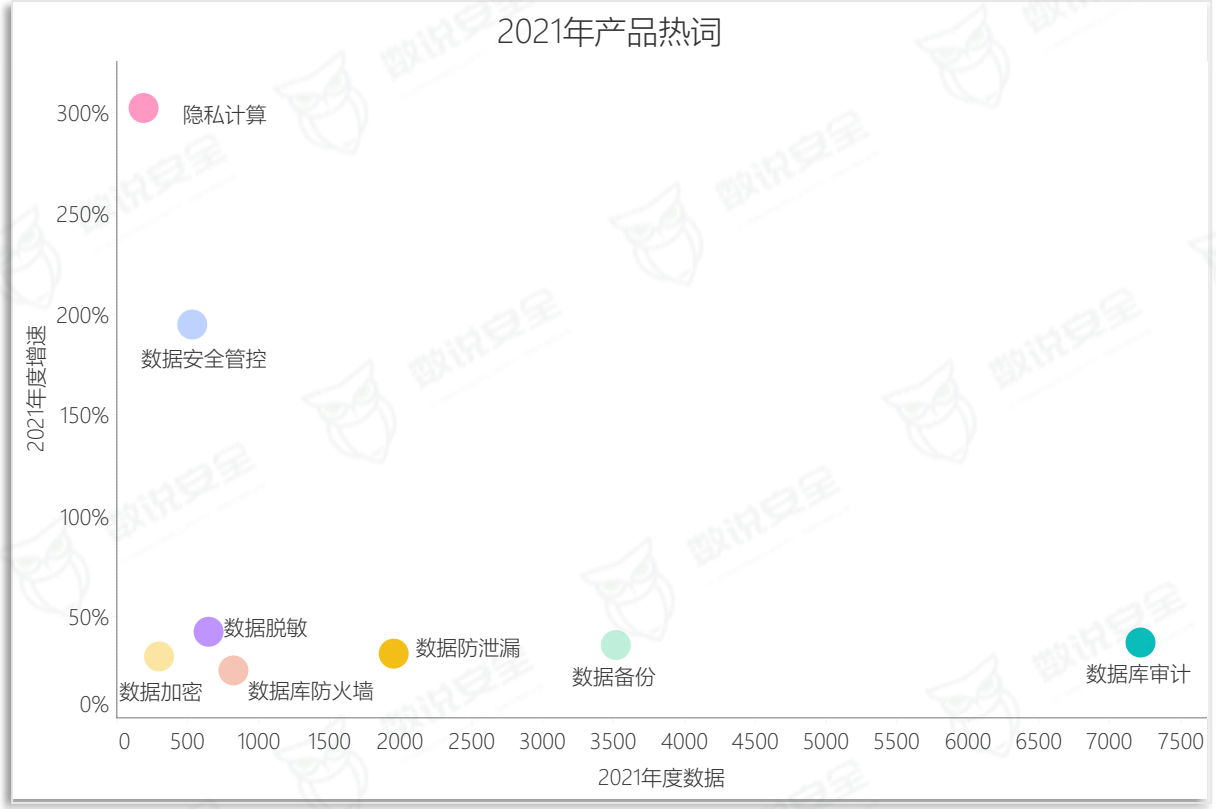
数据安全关键词热度

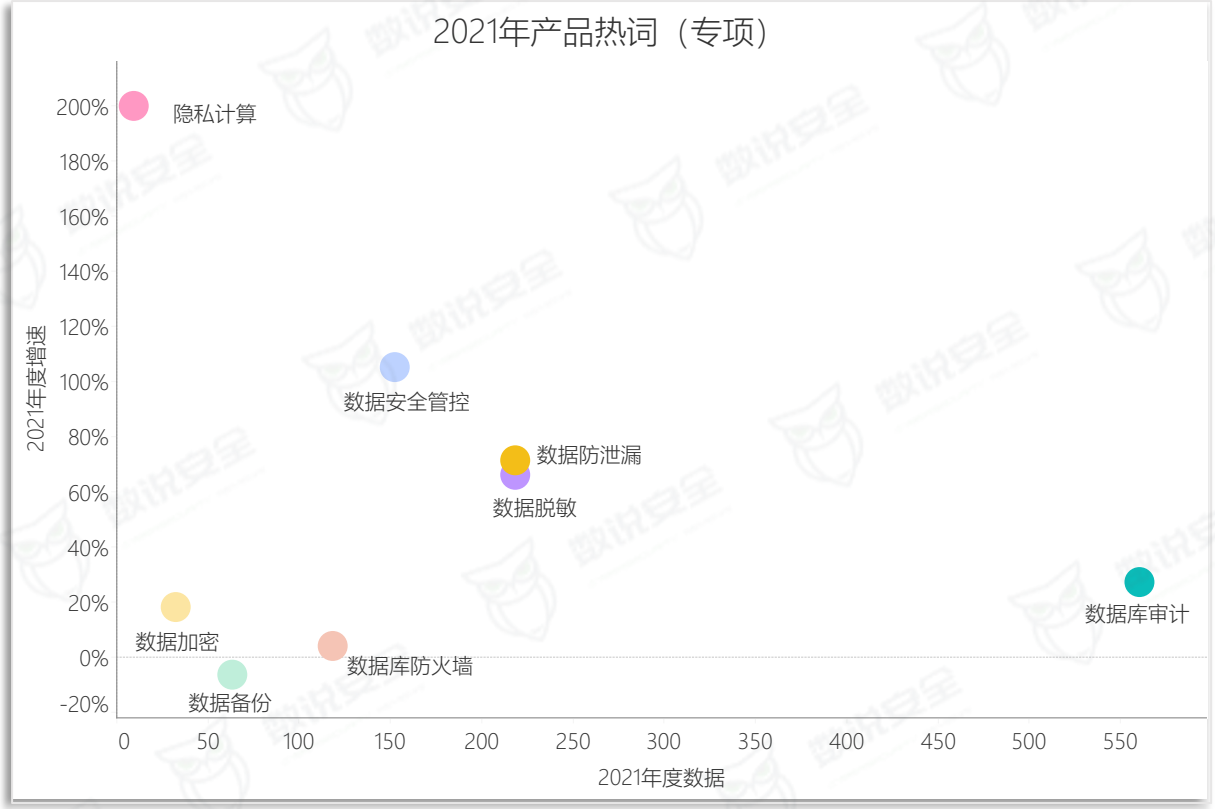
字体由小到大表示数量热度由低到高，颜色由绿到红表示增速热度由低到高

• 数据安全建设由产品向体系发展

以往的数据安全产品的采购，主要以等保合规和预防重大安全事件为目标，围绕数据库审计、数据防泄漏、数据脱敏等产品展开，随着数据安全法律体系和标准体系逐渐完善，以及数字时代下产业和经济发展带来的数据流域和流量的扩大，平台型产品、一体解决方案、隐私计算类产品的采购开始增多，数据分类分级、数据安全评估、数据安全运维、数据安全服务的项目数量也明显增长，数据安全建设开始由产品向体系化发展。

如图（2021年产品热词/(专项)）所示，数据安全管控平台的采购数量逐渐增多，增速较高，代表了未来数据安全建设的趋势；隐私计算类产品采购的从2021年开始出现，虽然数量较少，但随着数据共享、交易数量会不断增加，隐私计算将成为保障数据价值最大化的重要产品领域。





数据安全需求分析

1 • 数据安全建设方案展示

2 • 政府行业分析

3 • 电信行业分析

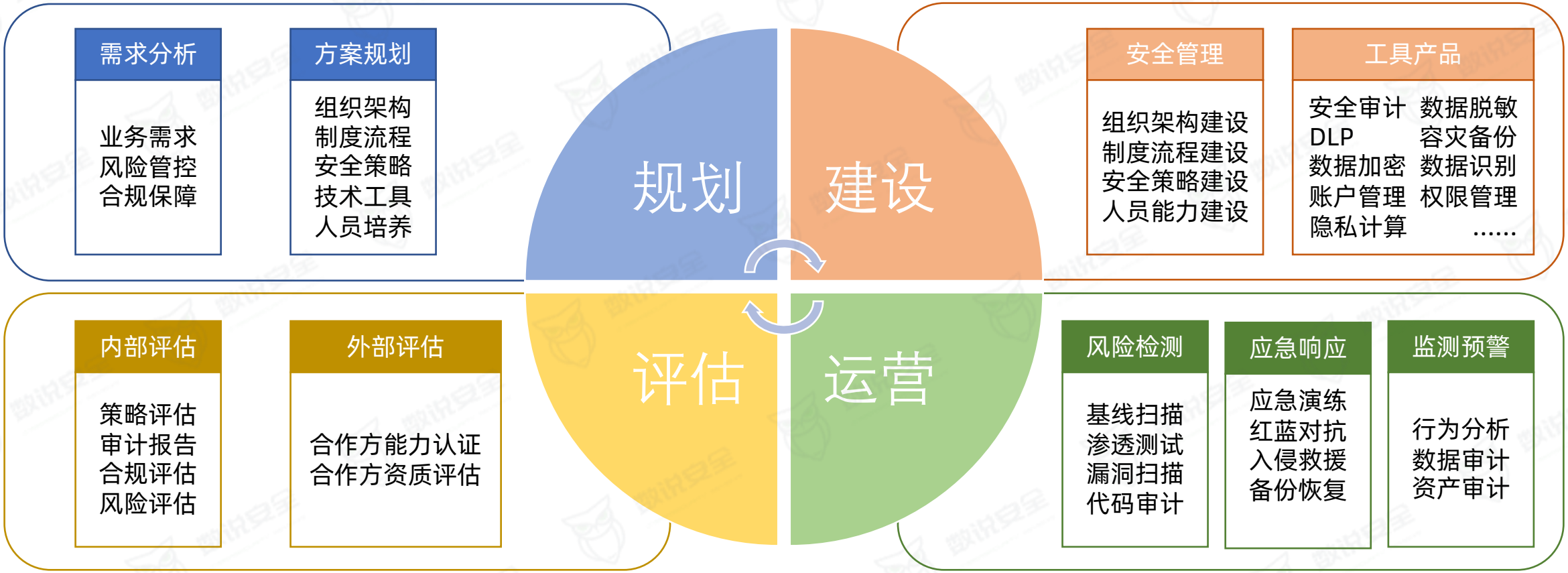
4 • 金融行业分析

5 • 医疗卫生行业分析

• 数据安全建设方案展示

数说安全

数据时代下，数据的流通共享才能最大限度的释放数据的价值，与数据开发利用和产业发展相结合的数据安全才是时代背景下需要的安全体系。综合数据安全合规建设、数据安全风险防范、数据业务健康发展的体系，已取代通过部署单点产品来满足合规建设的方式，数据安全建设需要围绕数据全生命周期，涉及安全规划、部门配合、组织管理、全流程制度制定、体系化技术融合、专业化人才培养等一系列综合协作。



政府行业需求分析

• 政府行业——深化政务数据有序共享与开发利用

数说安全

2021年12月《“十四五”数字经济发展规划》发布，深化政务数据的有序共享、开发利用和数据安全成为政府行业数字化工作的重点，《规划》指出当下我国数字政府建设成效显著，一体化政务服务和监管效能大幅度提升，要求在“十四五”期间数字化公共服务更加普惠均等，电子政务服务水平进一步提升，网络化、数字化、智慧化的利企便民服务体系不断完善，数字鸿沟加速弥合。

四、充分发挥数据要素作用

深化政务数据跨层级、跨地域、跨部门有序共享，建立健全国家公共数据资源体系，统筹公共数据资源开发利用，推动基础公共数据安全有序开放，构建统一的国家公共数据开放平台和开发利用端口，提升公共数据开放水平，释放数据红利。

对具有经济和社会价值、允许加工利用的政务数据和公共数据，通过数据开放、特许开发、授权应用等方式，鼓励更多社会力量进行增值开发利用。

七、持续提升公共服务数字化水平

建立健全政务数据共享协调机制，加快数字身份统一认证和电子证照、电子签章、电子公文等互信互认，推进发票电子化改革，促进政务数据共享、流程优化和业务协同；

推动政务服务线上线下整体联动、全流程在线、向基层深度拓展；

开展政务数据与业务、服务深度融合创新增强基于大数据的事项办理需求预测能力，打造主动式、多层次创新服务场景。聚焦公共卫生、社会安全、应急管理等领域，深化数字技术应用，实现重大突发公共事件的快速响应和联动处置。

八、健全完善数字经济治理体系

增强政府数字化治理能力，加大政务信息化建设统筹力度，强化政府数字化治理和服务能力建设，有效发挥对规范市场、鼓励创新、保护消费者权益的支撑作用；

建立完善基于大数据、人工智能、区块链等新技术的统计监测和决策分析体系，提升数字经济治理的精准性、协调性和有效性；

推进完善风险应急响应处置流程和机制，强化重大问题研判和风险预警，提升系统性风险防范水平。探索建立适应平台经济特点的监管机制，推动线上线下监管有效衔接，强化对平台经营者及其行为的监管。

《规划》对政务数据安全也做出要求，「九、着力强化数字经济安全体系」中指出：“要依法依规加强政务数据安全保护，做好政务数据开放和社会化利用的安全管理”。

《数据安全法》中也明确提出国家机关应建立和完善相应的数据安全管理制度，保护政务数据安全，对不履行数据安全保护义务的主管人员和责任人可依法追责；明确了国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应经过严格审批且合同应有确保数据安全的相关条款；明确了政务数据以公开为原则、不公开为例外的基本理念。

• 政府行业——政务大数据局领域政策健全度较高

自党的十八届五中全会部署推进机构与行政体制改革以来，地方政府开始逐步设立大数据管理局，过去政府各级各部门之间缺乏沟通与协调，众多数据无法共享，难以实现数据的互联互通，导致了“数据孤岛”。政务大数据局主要负责政府数据业务的统筹治理，数据效用价值的全面实现。通过建立数据管理组织体系，解决“数据孤岛”问题，使数据多元联动，发挥更好效用，服务经济，引领产业升级。

目前，各省、直辖市均已组建大数据管理局机构，政务大数据局系统正在快速建设中，各省市也已出台的《数据管理条例》、《数据安全管理办法》，配合《网络安全法》、《数据安全法》、《关键信息基础设施安全保护条例（征求意见稿）》、《网络安全标准实践指南》、《信息技术大数据政务数据开放共享》等规范，政务数据安全相关的标准体系也在不断明确与建立。

以浙江省丽水市大数据发展管理局的数据安全采购项目为例，项目的执行标准要求共十余项：

《中华人民共和国网络安全法》	《浙江省公共数据开放与安全管理暂行办法》(省政府令第381号)
《关键信息基础设施安全保护条例（征求意见稿）》	《浙江省公共数据安全管理总则（讨论稿）》
《浙江省深化“最多跑一次”改革推进政府数字化转型工作总体方案》	《浙江省网络安全协调指挥平台建设指南》（2018）
《浙江省数字化改革总体方案》	《政务网络安全监测平台总体技术要求》TCIIA 005—2019
《省大数据局关于一体化智能化公共数据平台方案》	《丽水市公共数据共享安全管理规范》（DB3311_T 127—2020）
《浙江省公共数据和电子政务管理办法》省政府令354号	《丽水市公共数据资源管理办法》（丽政办发〔2020〕5号）

政务大数据局综合了以数字城市、市民一卡通、应急指挥、一站式行政服务大厅、全程网上政务服务、网格化治理、数据中心为主的建设内容，涵盖以服务人民为导向的各类社会活动，因此被授予了极高的政策的重视度和充足的财务支持，使得政务数据安全体系在高标准、严要求的方向上的不断健全。

• 政府行业——部分省份政务大数据局建设脚步领先

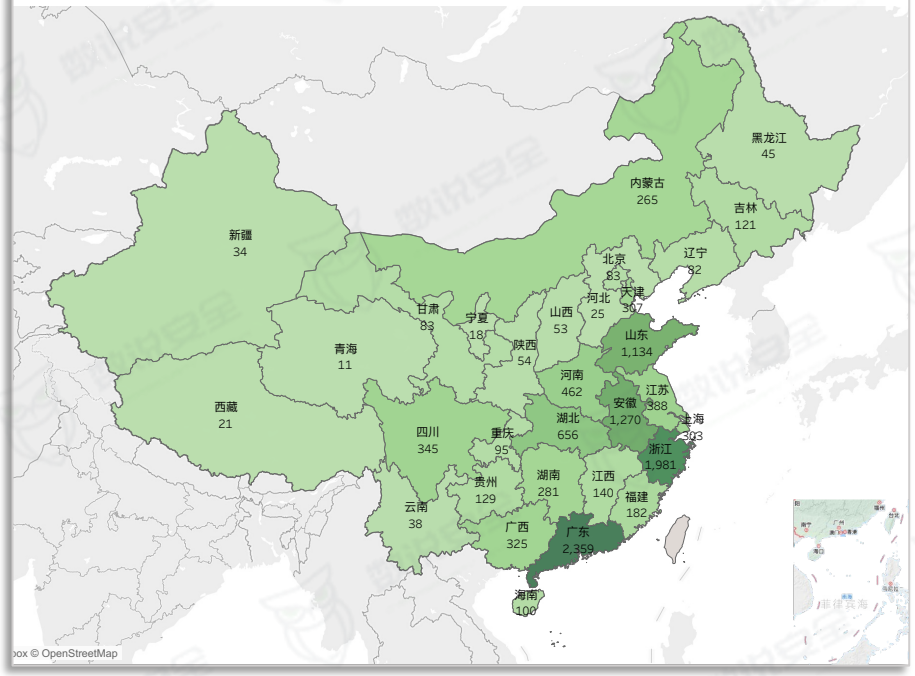
目前，各省、直辖市级数据管理局组织体系的系统平台基本建立，根据数说安全统计，2021年政务大数据管理局采购的网络安全项目数量约为4000个，同比增长约55%，其中数据安全项目数量719个，同比增长56%，数据安全专项项目数量171个，同比增长80%，高于平均项目增速。

根据采购项目数量来看，浙江、广东、安徽、山东等省份项目建设速度领先，省下辖地市级数据管理局组织体系及系统的建设也相对领先，例如广东、浙江、安徽等省份的下辖地级市的政务数据管理局已全部建立，并全部进行过数据安全采购，其中更不乏千万级的采购项目。

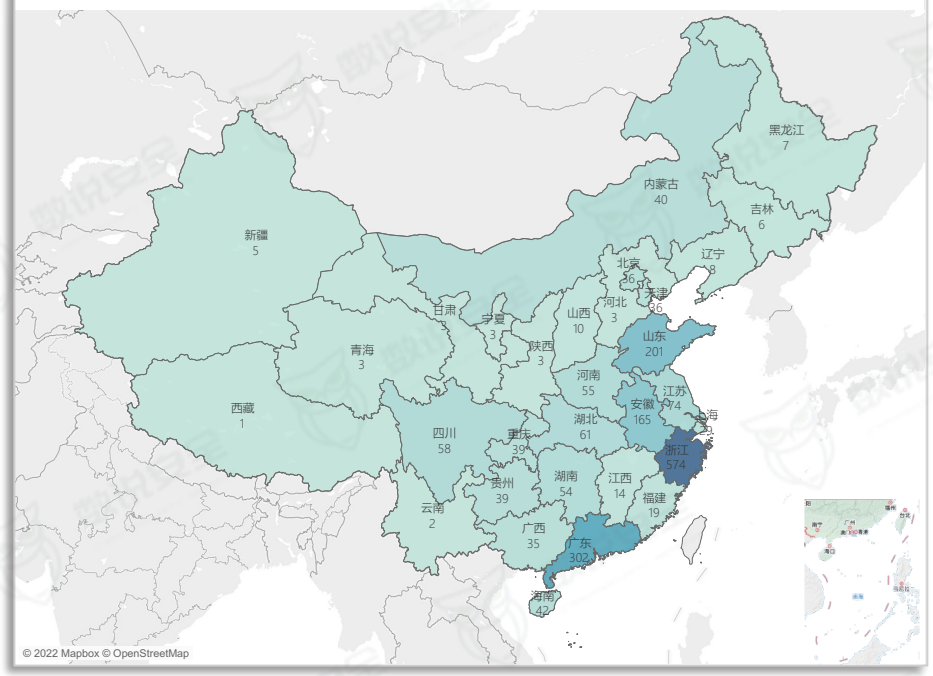
政务业务需要汇集和融合的数据体量庞大，在安全方面不仅要保障数据完整性、保密性和可用性，更需要确保数据在联合使用过程中的隐私性，应重点使用和关注包括采用安全多方计算、联邦学习、同态加密等在内隐私计算技术措施。

近期部分省、市级数据管理局的数据安全建设大单明显增多，数据安全建设脚步加快，为同级别单位做出了良好示范样例，预计数据安全建设脚步较慢的省份将会在未来释放较好的增速。

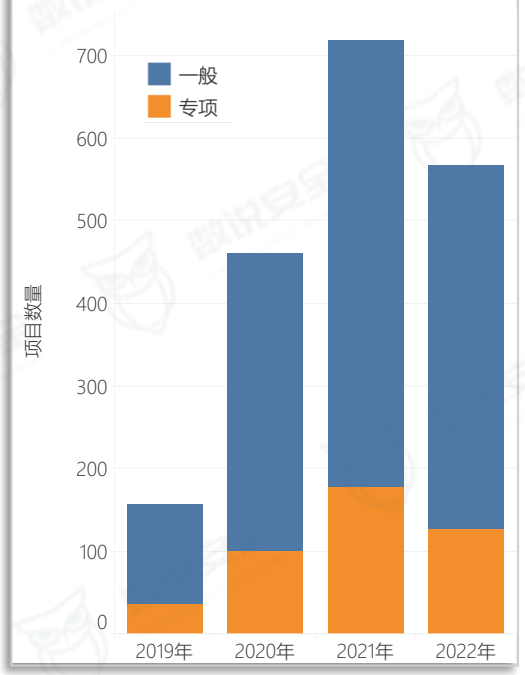
政务大数据局网络安全项目分布



政务大数据局数据安全项目分布



政务大数据局数据安全项目数量



图中数据采样时间为2018年-2022年8月

• 政务大数据管理局——XX省大数据安全体系建设项目（一）

数说安全

2021年9月，xx省大数据管理局发布大数据安全体系建设项目，项目分为（A包- 省电子政务外网安全体系改造）和（B包- 省政务大数据安全保障体系建设），本项目总采购预算：2504.11万元。

其中A包预算：1181.21万元；B包预算 1322.90万元。B包建设内容为①建立省政务云监管平台；②建立可信计算免疫平台；③建立大数据安全保障平台；④建立省政务安全制度规范体系；⑤实施政务大数据安全运营监管服务。

xx省大数据安全体系建设项目的时间相对较晚，建设标准相对较高，为后续各省市的同类项目提供了较好的参考和借鉴，下面将各项详细内容做出展示，以供参考。

可信免疫计算平台采购成品软件，具体清单如下：

名称	技术参数要求	数量
可信计算免疫平台管理中心	1.服务端安全管理软件：B/S 管理模式，实现客户端软件的策略统一管理、日志统一收集、软件集中管理及分发等安全管理功能。基于操作系统内核技术，是安全功能控制的一组安全模块软件，安装于需要受保护的操作系统中，其实现功能包括静态度量、动态度量、强制/自主访问控制、性能监控、可信链接、安全认证等。 2. ▲提供所涉及产品原厂商针对本项目专项授权和原厂商盖章的 3 年原厂标准服务承诺函，提供 7×24 小时热线受理，远程处理问题，上门技术支持。	1套

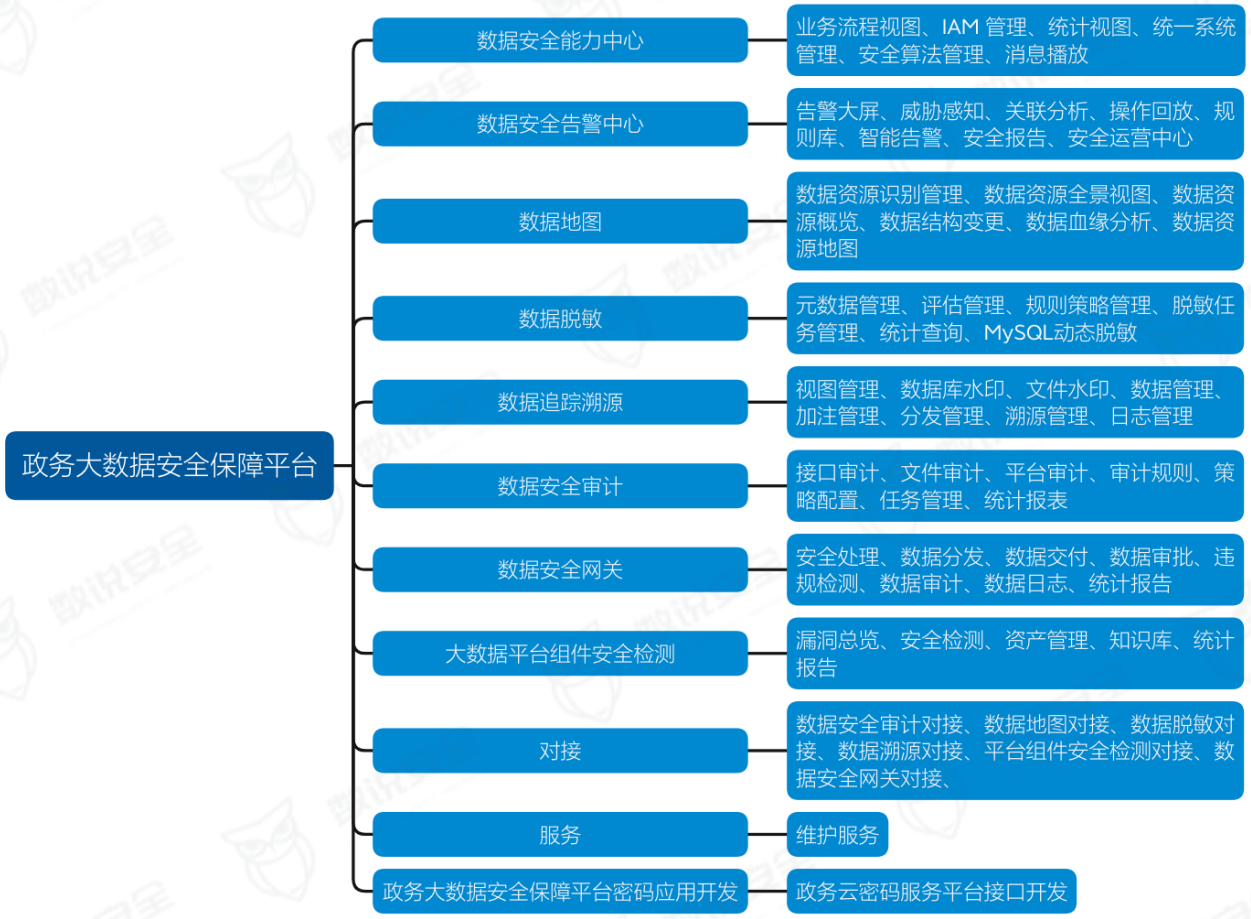
名称	技术参数要求	数量
可信计算免疫平台客户端	1.客户端安全模块软件：基于操作系统内核技术，是安全功能控制的一组安全模块软件，安装于需要受保护的操作系统中，其实现功能包括静态度量、动态度量、强制/自主访问控制、性能监控、可信链接、安全认证等。服务期内业务升级、业务扩容、业务重大变更时需派技术人员进行支撑保障。服务期内公共服务平台如增加服务器数量不超过 5 台，则增加的服务器可免费安装该软件。 2. ▲提供所涉及产品原厂商针对本项目专项授权和原厂商盖章的 3 年原厂标准服务承诺函，提供 7×24 小时热线受理，远程处理问题，上门技术支持。	37套

资料来源： 市场公开招投标文件

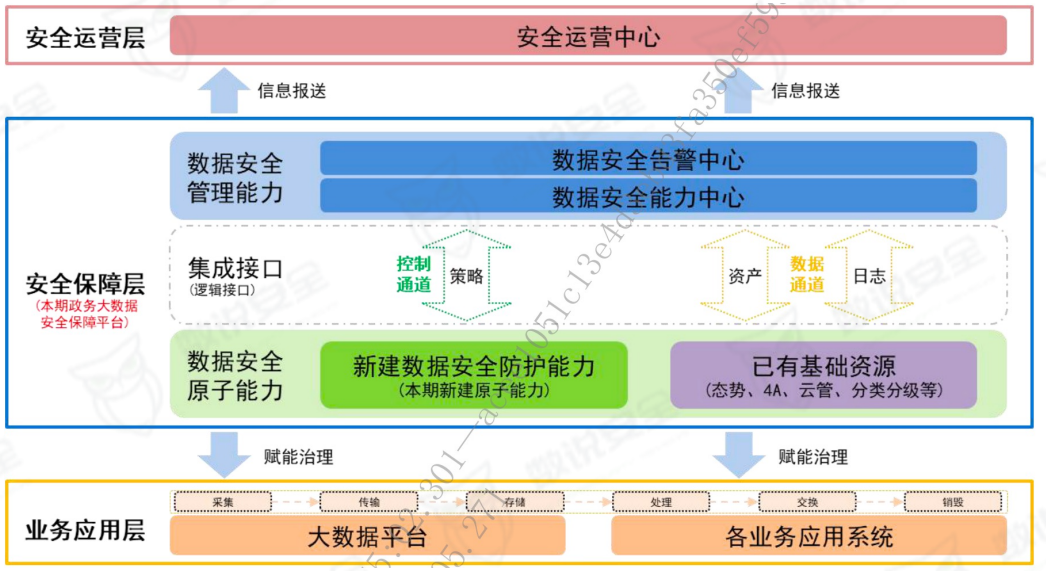
• 政务大数据管理局——XX省大数据安全体系建设项目（二）

数说安全

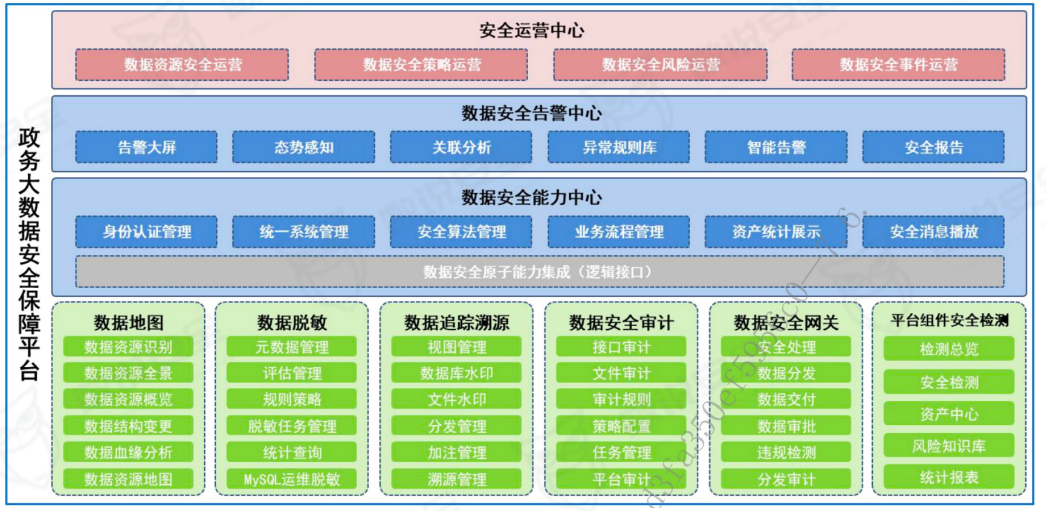
政务大数据安全保障平台聚焦于数据全生命周期，按照数据分类分级的要求，针对数据的采集、传输、存储、加工、开放、共享、销毁的全生命周期中风险，利用脱敏、溯源等安全技术实现数据本身的安全防护，实现对政务数据对服务中数据对外出口统一监测与管控，确保对外服务和使用的数据安全合规，可以追踪溯源，严控数据安全风险，杜绝数据泄漏、误用与滥用。



政务大数据安全保障平台总体逻辑架构图



系统功能结构示意图



资料来源： 市场公开招投标文件

• 政务大数据管理局——XX省大数据安全体系建设项目（三）

项目要求建立省政务安全制度规范体系：在省大数据安全体系规划架构之下，结合政府数据安全管理的实际情况，设计省政务大数据安全制度规范体系。建立大数据安全制度规范体系，为大数据安全防护、运营提供依据，数据安全管理策略的完善，为大数据安全防护、审计、运营提供了依据，使政务数据安全管控有据可依。

一级管理制度	《政务数据安全管理办法》
二级管理规范和技术标准	《政务数据安全管理规范》、《大数据平台安全基线配置标准》、《网络分区分域安全防护标准》、《政务云安全体系规范》、《海南省电子政务外网管理规范》、《政务外网网络安全建设指南》、《大数据安全体系宣培训与宣贯》

政务大数据安全运营监管服务要求采用集约化管理运营模式，集聚安全手段、安全能力、安全人员等资源，在大数据安全运营监管中心的统筹下实现联合同步防御，打通风险评估、运维保障、监测预警、应急响应各环节，共享安全情报和知识库，协同执行防御任务，大幅度提升整体数据安全协同防御能力，严格控制政务数据安全风险，杜绝数据泄漏、误用与滥用等事件。

安全运营监管服务清单	
资产证明	数据分级
系统安全检测	数据权限安全监管
数据输出安全监管	数据安全风险监测
安全应急及重保服务	大数据安全风险评估
安全检查与审计	大数据安全监管报告

安全运营监管团队	人员	能力
一线人员	8 人，7*24 小时在海南省大数据管理局驻场值守	负责大数据安全日常运营监管服务工作，在大数据管理局驻场服务，须具备相应的安全技术能力。
二线人员	4 人，5*8 小时值班	远程技术支持，必要时需现场支持，出现问题时 1 小时内能响应，具有较高的技术能力。
专家	5*8 小时，3 人。	远程技术支持，具备高级技术能力。

• 政务大数据管理局——XX市数据安全服务项目（一）

数说安全

2021年9月，xx省xx市大数据发展管理局发布《 xx市电子政务网络及数据安全服务项目》，项目预算2020万。

项目背景

2021年2月18日上午，xx省委召开全省数字化改革大会，发布《xx省数字化改革总体方案》，其中对政务网络安全体系提出明确要求：统筹发展网络安全与数据安全，树立网络安全底线思维，严格落实等级分级保护要求，加快建立关键信息基础设施安全保护体系、公共数据和个人信息安全保护体系，构建覆盖物理设施、网络、平台、应用、数据的网络安全技术防护体系，提升网络安全主动防御能力、监控预警能力、应急处置能力、协同治理能力，打造数字化改革网络安全屏障。

因此，加强xx市政务网络及数据安全建设是响应xx省数字化改革的要求，是推进xx市数字化改革的重要举措和基础工程，项目建设将集约化、一体化、智能化贯彻始终，争做数字化改革建设排头兵。

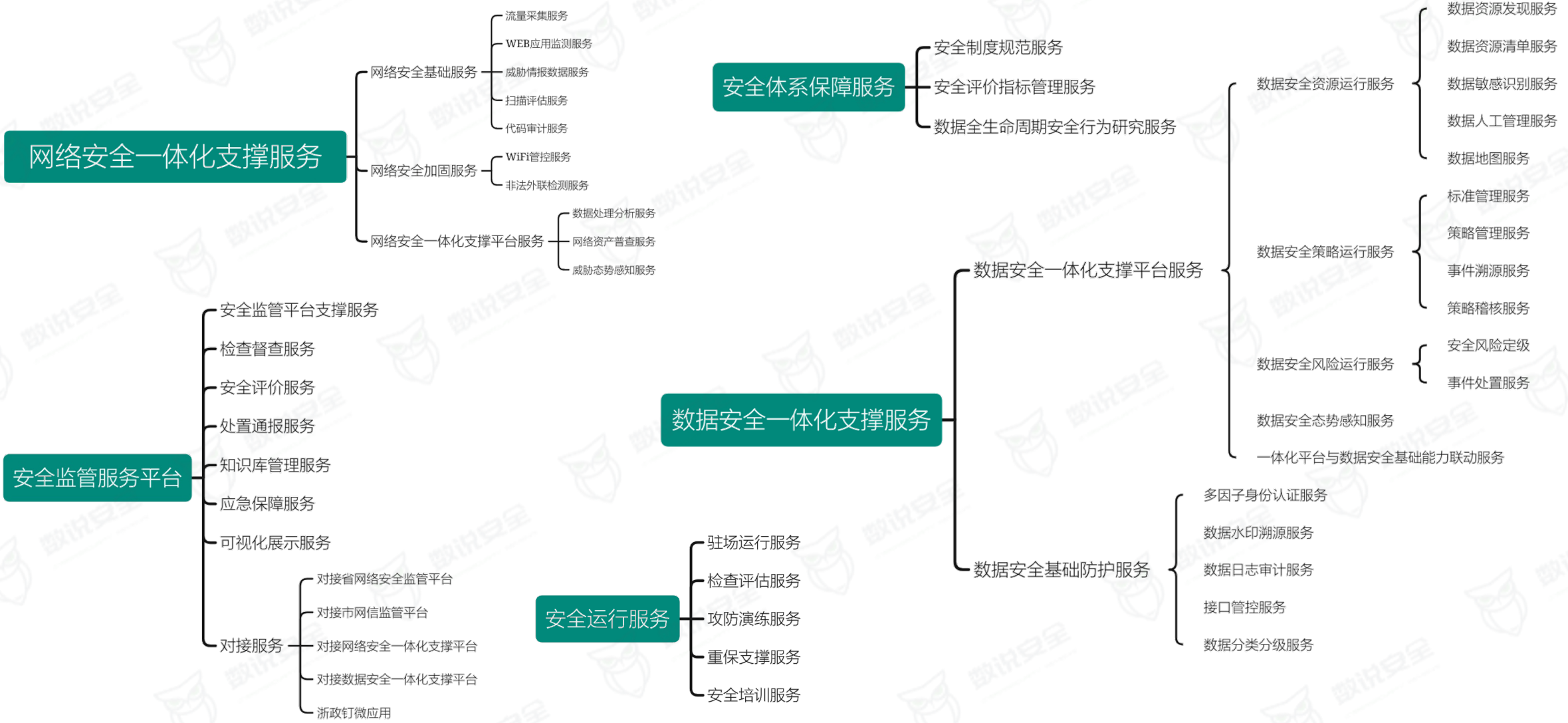
执行标准要求：

《中华人民共和国网络安全法》	《浙江省公共数据开放与安全管理暂行办法》(省政府令第381号)
《关键信息基础设施安全保护条例（征求意见稿）》	《浙江省公共数据安全管理总则（讨论稿）》
《浙江省深化“最多跑一次”改革推进政府数字化转型工作总体方案》	《浙江省网络安全协调指挥平台建设指南》（2018）
《浙江省数字化改革总体方案》	《政务网络安全监测平台总体技术要求》TCIIA 005—2019
《省大数据局关于一体化智能化公共数据平台方案》	《丽水市公共数据共享安全管理规范》（DB3311_T 127—2020）
《浙江省公共数据和电子政务管理办法》省政府令354号	《丽水市公共数据资源管理办法》（丽政办发〔2020〕5号）

资料来源： 市场公开招投标文件

• 政务大数据管理局——XX市数据安全服务项目（二）

项目建设内容主要由以下五项构成：



资料来源： 市场公开招投标文件

• 政务大数据管理局——XX市云办公数据安全管控平台

数说安全

2021年12月， xx市新城区大数据中心发布《云办公数据安全管控平台招标采购项目》，项目中标金额810万。项目要求及采购细则如下所示：

项目要求

数据安全系统包含：行为管理系统、内部威胁管理系统、终端检测响应系统、统一身份管理平台、数据安全系统配套数据处理终端；

云办公桌面云系统包含：云办公系统配套数据处理终端、存储虚拟化软件、虚拟桌面控制系统、虚拟桌面用户接入系统（VDI用户接入授权）、存储网交换机、业务网管理网交换机、云办公系统配套瘦客户机；

技术服务包含：配备驻场运维服务团队提供培训、讲解、维护服务。

序号	标的名称	品牌、规格型号/主要服务内容	数量	单位	单价（元）	总价（元）
1	数据安全系统配套数据处理终端	中科可控、R5230HA	2	台	108000	216000
2	行为管理系统	华讯软件、vAC-300	1	项	670000	670000
3	内部威胁管理系统	华讯软件、ITM	1	项	889000	889000
4	终端检测响应系统	深信服、EDR	1	项	180000	180000
5	统一身份管理平台	华讯软件、vIDTrust-1000	1	项	767000	767000
6	云办公系统配套数据处理终端	中科可控、R5230HA	16	台	108000	1728000
7	存储虚拟化软件	深信服、存储虚拟化软件 V3.0	16	套	30000	480000
8	虚拟桌面控制系统	深信服、深信服虚拟桌面接入管理软件 V5.0	1	项	400000	400000
9	虚拟桌面用户接入系统（VDI用户接入授权）	深信服、深信服虚拟化管理接入授权软件 V5.0	450	个	1000	450000
10	存储网交换机	信锐技术、RS6300-24X-LI-12X	4	台	7500	30000
11	业务网管理网交换机	信锐技术、RS5300-28T-4F	8	台	4000	32000
12	云办公系统配套瘦客户机	深信服、aDesk-STD-200H-s	450	台	1000	450000
13	3年技术服务	自项目交付后乙方提供技术服务，配备驻场运维服务团队提供培训、讲解、维护的服务。技术服务期三年。	1	项	1800000	1800000

资料来源： 市场公开招投标文件

电信行业需求分析

• 电信行业——数据安全规范标准体系完善度领先

2021年11月16日工信部公布《“十四五”信息通信行业发展规划》，提出“夯基础、深融合、护数据、促产业、强制力”五项网络安全工作重点要求，明确建立健全数据分级分类、重要数据保护、数据跨境流动等数据安全管理制度，加快构建数据安全风险技术监测体系，大力发展应用网络和数据安全先进适用技术等要求。

随着新一代信息通信技术加速向经济社会各领域渗透融合，基础通信网络安全的基石底座作用进一步凸显，融合业务安全风险不断加剧。近年来，国家、行业和电信企业先后出台多项规范标准，涉及分类分级、全生命周期技术要求、安全管理、安全评估等，并展开数据安全专项行动、贯标和考核工作，电信行业的数据安全体系规范标准建设程度相对领先，并在加速建立与完善中。

2019年7月

《电信和互联网行业提升网络数据安全保护能力专项行动方案》

对电信企业进行数据安全检查；完善数据安全管理制度和标准；开展风险评估；加强网络数据安全管理。

2020年12月

《电信和互联网行业数据安全标准体系建设指南》

进一步落实各项法律法规要求，在基础共性、关键技术、安全管理标准和重点重点行业方面指导电信和互联网行业数据安全标准化工作建设工作。

2020年12月

《基础电信企业数据分类分级方法》

规定了基础电信企业数据分类分级原则、工作流程及方法，并给出基础电信企业数据分类分级示例。

2021年5月

《基础电信企业重要数据识别指南》

给出了基础电信企业重要数据的定义、识别规则、识别方法和重要数据安全保护实施指导，并给出了基础电信企业重要数据示例。

2021年5月

《2021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的通知》

要求制定考核及评分标准；明确数据安全治理责任部门及职责，建立数据安全治理制度，完善相关防护技术，补全重大突发数据安全事件应急响应机制等。

2022年4月

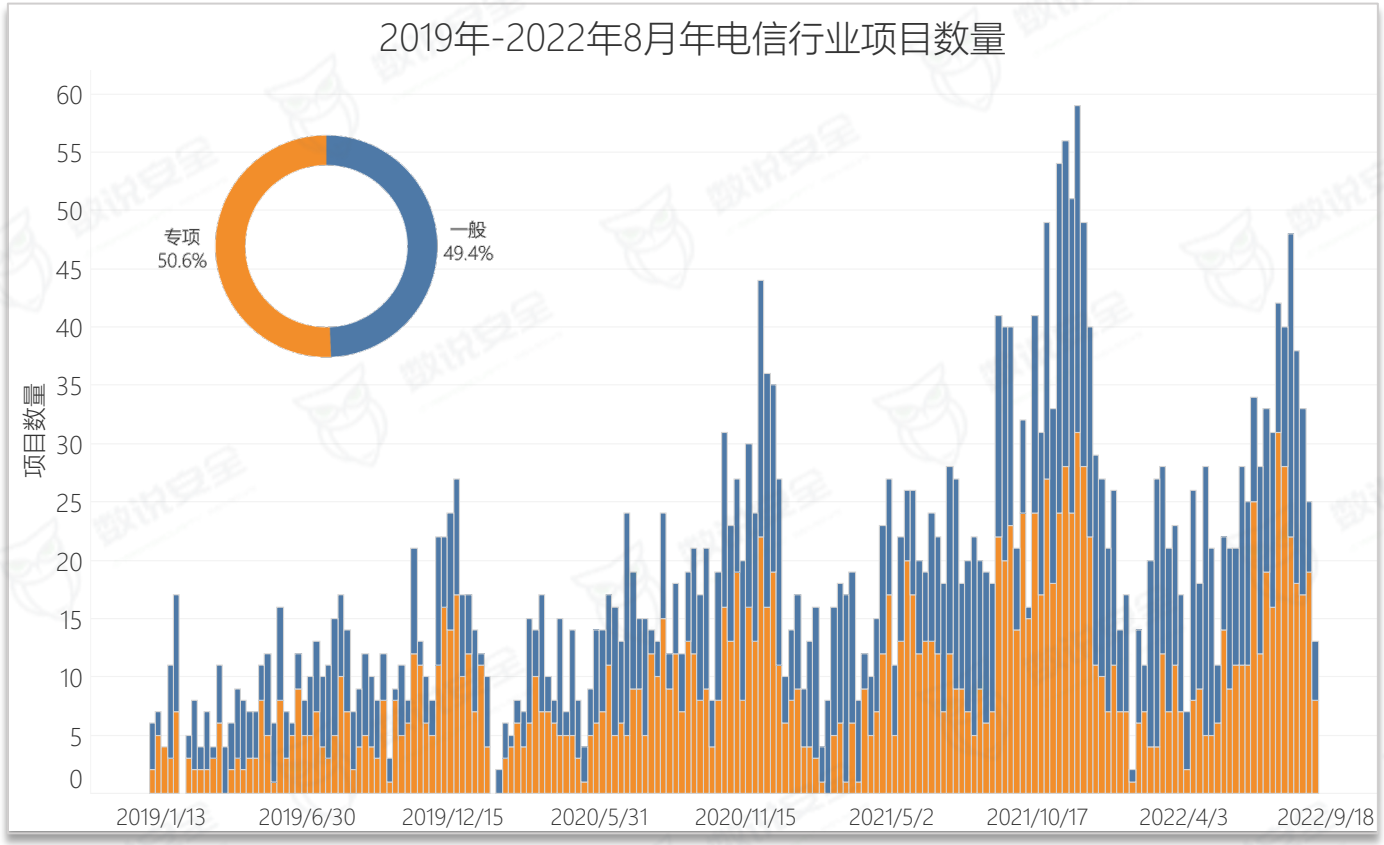
《电信网和互联网数据安全评估规范》

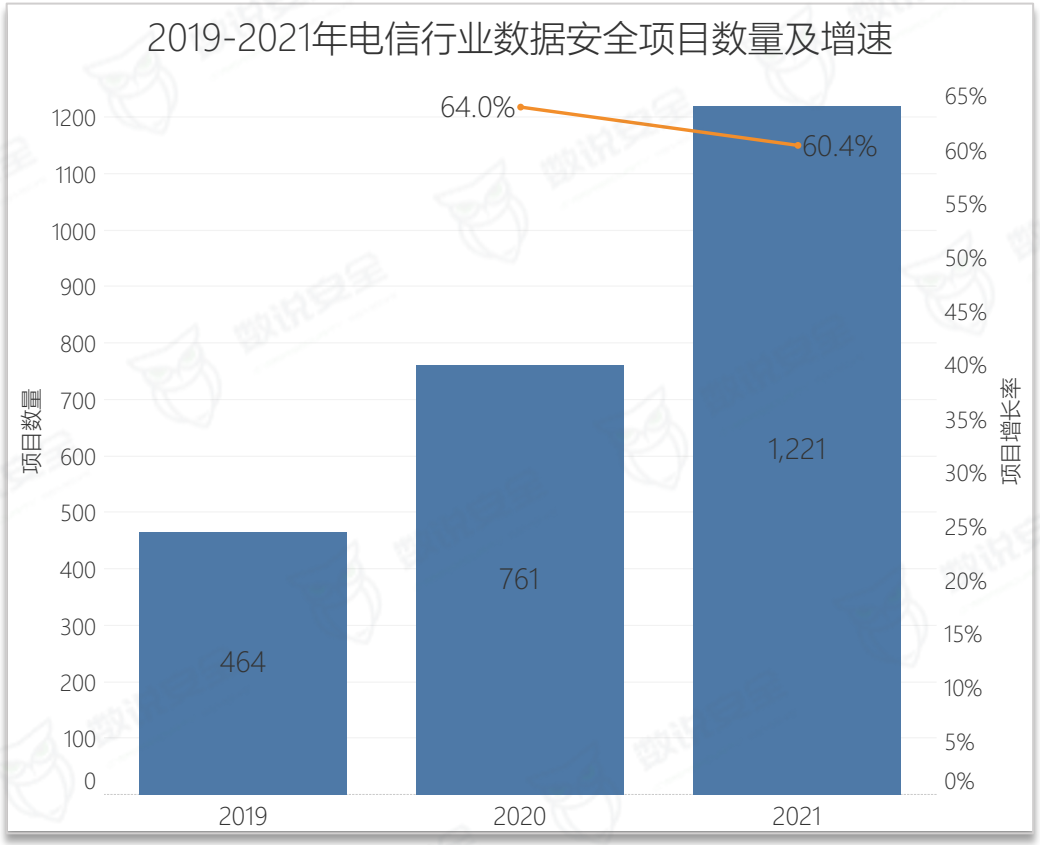
规定了电信服务和互联网信息提供商开展数据安全评估实施流程和数据安全相关管理及技术措施的评估要点。

• 电信行业——数据安全重视度较高

电信行业存储了大量的个人和企业基础信息，从2000年初开始，由于数据泄漏、窃取导致的通过电话、网络和短信方式，编造虚假信息，进行电信诈骗的事件一度愈演愈烈，涉及金额庞大，成为数据安全的重灾区，因此电信行业对数据安全的重视程度极高，数据安全专项项目的采购比例超过50%，位居各行业首位。

2020年7月，工信部发布《电信和互联网行业数据安全标准体系建设指南（征求意见稿）》，制定了电信和互联网行业数据安全标准研制数量目标，到2021年完成标准体系的初步建立，研制数量在20项以上；到2023年标准体系基本完善健全，研制数量在50项以上，电信行业数据安全项目增速也连续两年保持在60%高位。

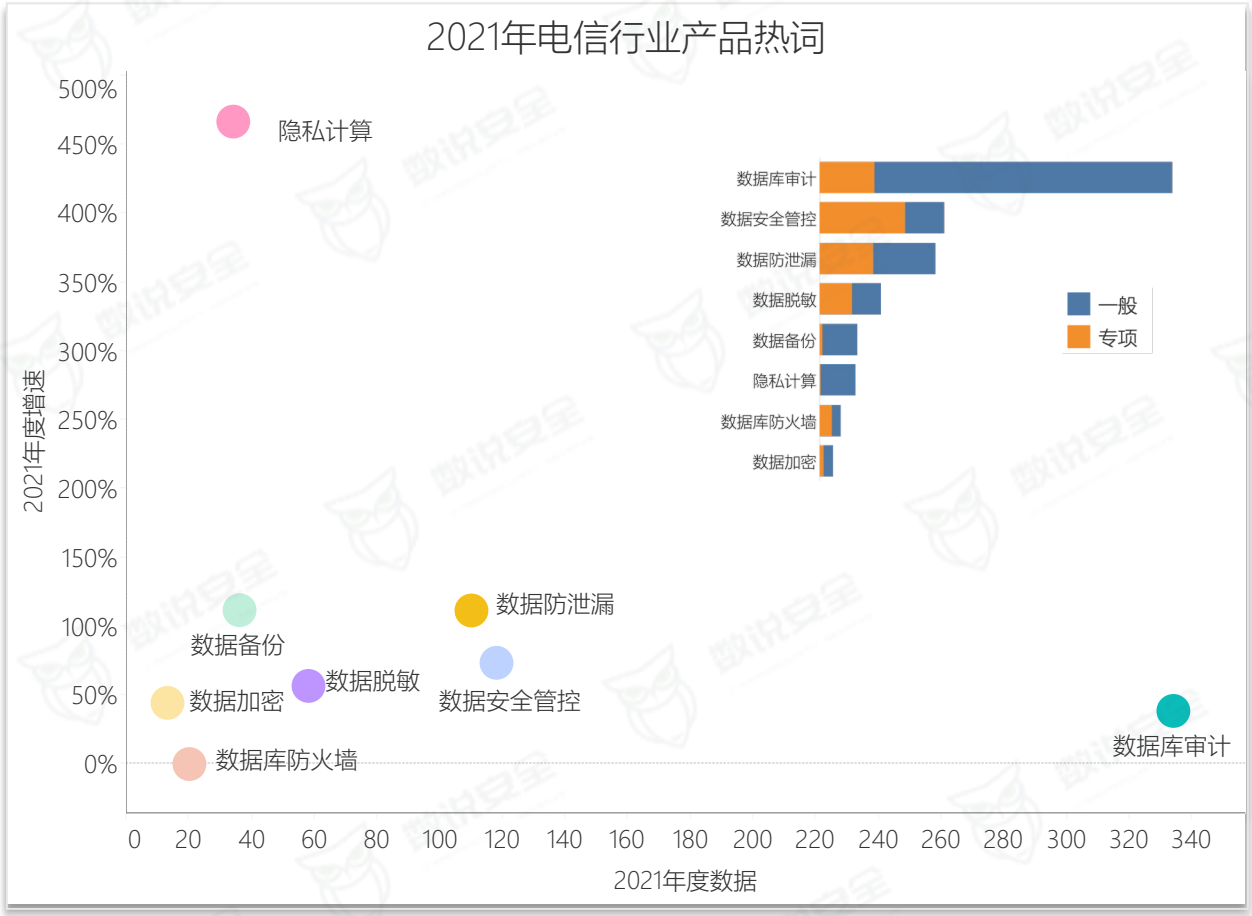


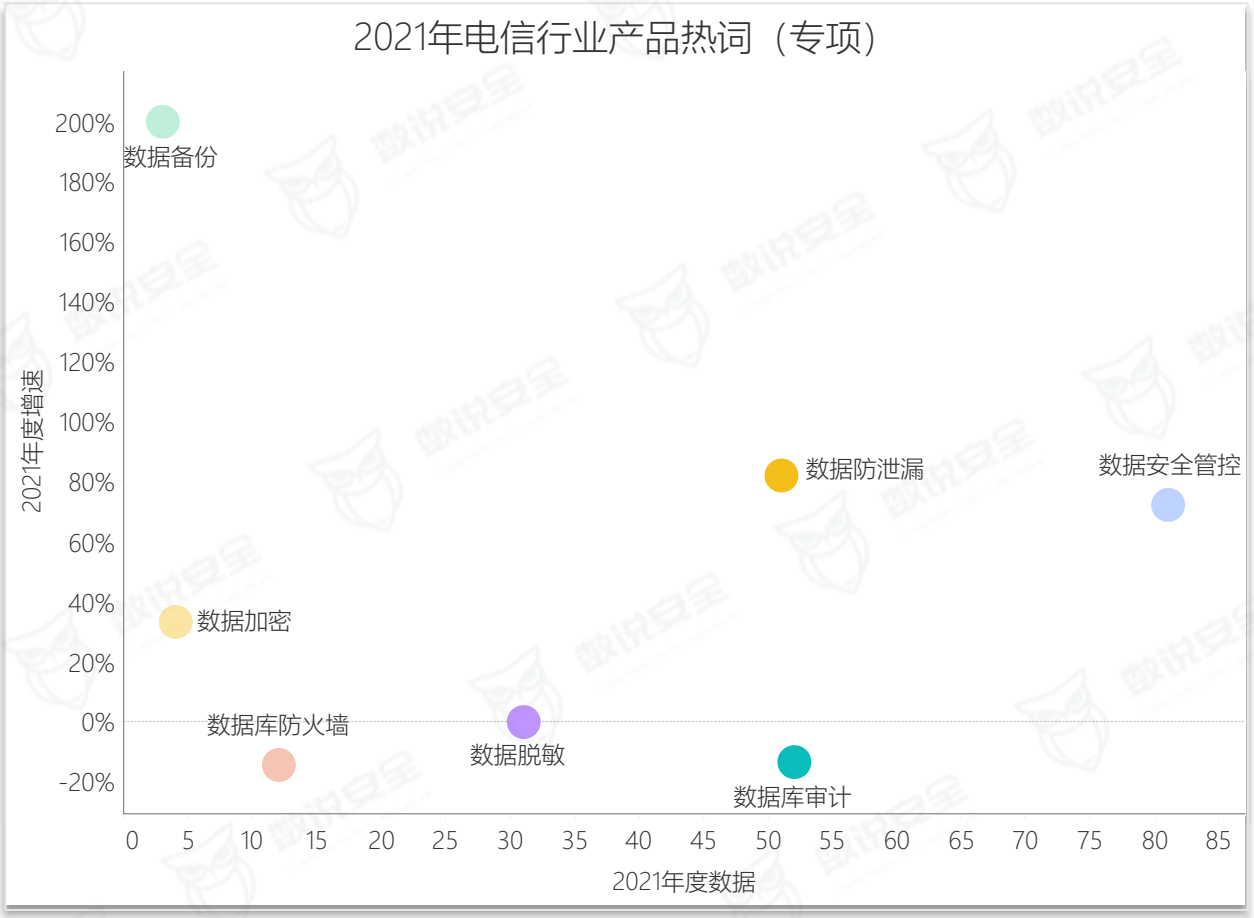


• 电信行业——数据安全建设全面展开

电信企业数据泄漏衍生问题频发，对数据安全的重视度较高，规范标准体系的建设相对领先，因此电信行业的数据安全建设进展较快。

根据数说安全统计，数据安全管控平台类项目建设已全面展开，专项项目占比较高，三大电信运营商在总公司或分公司层面都已开始相关建设；数据安全评估也进入正常轨道，多数运营商公司每年都会购买数据安全评估服务；数据泄漏仍然是运营商企业考核与建设的重点领域，在数据时代的背景下显得尤为突出，因此数据防泄漏产品的采购增速较高；隐私计算类项目也逐渐开始建设，数量较去年明显增多。





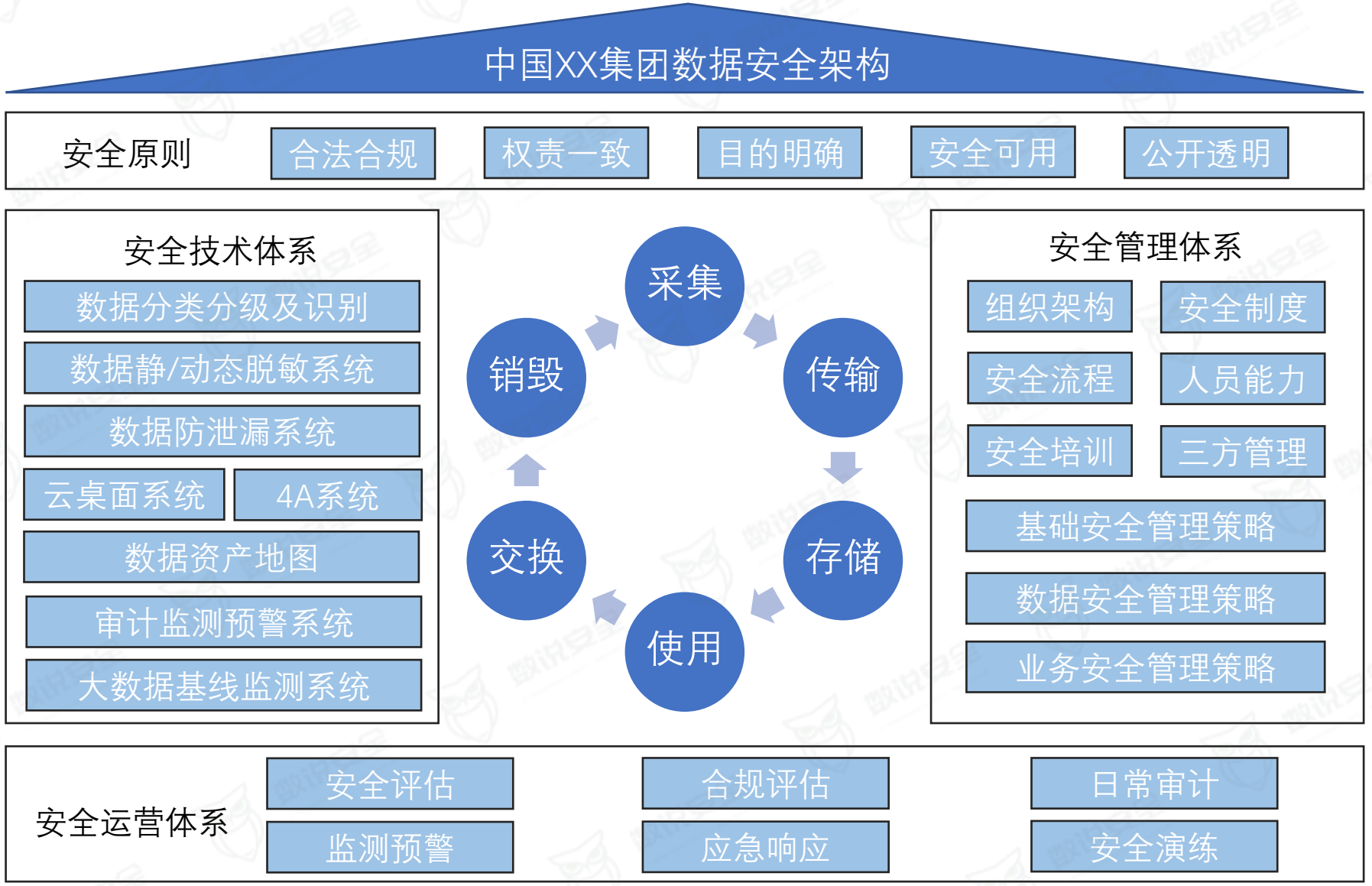
• 电信行业——以数据防泄漏为重点的数据安全防护架构

数说安全

电信运营商的业务网络存在区域和数据分散、系统繁多、环境复杂等特点，各个分散区域和系统中均会存储或使用大量的客户信息和企业核心数据，数据在不同的阶段也面临不同的风险点。

针对电信企业的业务特点，数据脱敏、数据防泄漏的安全能力和监管力度仍需不断加强，同时也更需要将数据安全管理和能力在更广的范围内协同联动，形成数据安全策略、制度、流程、运维等综管控调配系统才能满足合规及业务需求。

中国xx集团以防止数据泄漏和滥用为出发点，从安全管理体系、数据安全技术体系和数据安全运营体系三个方面构建了数据安全防护架构，涵盖数据生命周期，实现了职责清晰、管理规范、防护全面和运维完备的数据安全体系。



• 电信行业——数据安全评估项目

电信行业的数据安全评估工作已经全面展开，根据数说安全统计，2020-2021年有约38家中国电信旗下公司，20家中国联通旗下公司及24家中国移动旗下公司进行了数据安全评估项目的采购，项目金额从20万到300万不等。

中国移动湖北公司2022-2023年数据安全专项评估服务_比选公告

本项目为中国移动湖北公司2022-2023年数据安全专项评估服务（第二次），采购人为中国移动通信集团湖北有限公司，采购代理机构为湖北信通通信有限公司。项目资金由采购人自筹，并已落实。项目已具备采购条件，现进行公开比选，具有服务能力的供应商均可前来报名。

一、采购货物的名称、数量及主要技术参数

1.1项目名称：中国移动湖北公司2022-2023年数据安全专项评估服务

1.2项目编号：HBYD20210500297

1.3采购内容：主要服务内容包括对企业数据安全的全面管理落实情况进行梳理，涵盖组织架构、制度流程、人员培训、技术保障、第三方合作等；对涉及存储用户个人信息和重要数据的支撑系统和业务平台按照工信部监管要求开展数据安全评估服务工作，判断其符合性；结合工信部和集团公司对数据安全专项检查中发现的问题，提出整改建议。

1.4合同有效期：从合同签订之日起至2023年12月31日为止。

江苏电信2021年新技术新业务及数据安全评估服务项目比选公告

本比选项目为江苏电信2021年新技术新业务及数据安全评估服务项目（项目编号：JSZBZB20212395），比选人为中国电信股份有限公司江苏分公司，比选代理机构为江苏中博通信有限公司。项目资金已落实，具备比选条件。现进行公开比选，特邀请有意向的且具有提供标的物能力的潜在参选人（以下简称参选人）参选。

1.项目概况与采购内容

1.1项目概况：江苏电信2021年新技术新业务及数据安全评估服务项目

1.2采购内容及分包划分情况：

1.2.1采购内容：为贯彻落实《网络安全法》、《数据安全法》、《电信和互联网用户个人信息保护规定》（工业和信息化部令 第24号）、《工业和信息化部办公厅关于做好2020年电信和互联网行业网络数据安全管理工作的通知》（工信厅网安函【2020】103号）、江苏通管局新技术新业务及数据安全监管要求、中国电信集团新技术新业务和数据安全评估相关工作要求，保障企业新技术新业务信息安全、重点业务及核心系统数据安全，全面提升企业新技术新业务、数据安全风险防范能力，以应对日益增长的互联网新技术新业务及数据安全威胁，在此背景下启动了江苏电信2021年新技术新业务及数据安全评估服务项目。

序号	【涉及的主要评估产品品类】	产品名称	规格型号	采购预估规模（含税）万元
1	--	评估服务	--	160

中国电信河南公司2022年云网运营数据安全评估服务项目比选公告

本比选项目为中国电信河南公司2022年云网运营数据安全评估服务项目（项目编号：BJCG-HNDX211281），比选人为中国电信股份有限公司河南分公司，比选代理机构为北京诚公管理咨询有限公司。项目资金已落实，具备比选条件，现进行公开比选，特邀请有意向的且具有提供标的物能力的潜在参选人（以下简称参选人）参选。

1.项目概况与采购内容

1.1项目概况：为落实数据安全法，提升数据安全保护能力，根据工信部行业数据安全标准贯标工作及网信安工作考核要求，拟采购第三方专业公司提供云网运营数据安全合规性评估工作，现开展中国电信河南公司2022年云网运营数据安全评估服务项目，服务期限1年。项目预算44万元人民币（不含增值税）。

1.2采购内容及分包（标包）划分情况：本项目不划分分包。采购内容为根据基础电信企业数据分类分级方法、重要数据识别指南，健全重要数据清单；按照数据安全评估实施流程和评估要点，开展年度合规性评估工作，并形成评估报告;根据安全防护级别，对数据在采集、传输、存储、使用、开发共享、销毁等六个方面的安全能力进行技术评测;开展上级单位迎检保障工作。选取一名中选人，中选份额100%。

2022-2024年双新和数据安全评估支撑服务公开比选项目_比选公告

本项目为2022-2024年双新和数据安全评估支撑服务公开比选项目，采购人为中移(上海)信息通信科技有限公司，采购代理机构为浙江中通通信有限公司。项目资金由采购人自筹，并已落实。项目已具备采购条件，现进行公开比选，具有相应能力的供应商均可前来报名。

一、项目概况

1.1项目编号：CMSR20220500121。

1.2采购内容：采购双新和数据安全评估支撑服务。

1.3采购规模：332万元（不含税）。

1.4采购满足期：自合同签订之日起2年。

1.5本项目设置最高限价，最高限价为不含税332万元人民币，数据安全评估单价限价7万/个，双新评估单价限价5万/个，应答人报价超过最高限价，其应答将被否决。

1.6本项目不划分采购包。

1.7本项目中选人数量为1个，中选份额100%。

1.8 服务地点：全国。

• 电信行业——数据安全运营系统项目

2021年12月，联通总部发布了《2021年联通总部信息安全数据安全运营系统研发项目》招标公告，采购预算金额达1480万元，公告指出「为规范数据处理活动，保护个人、组织在网络空间的合法权益，满足上级单位的监管要求，中国联通将构建总部-省分两级架构数据安全运营系统，对31省分公司DCN网互联网出口的数据进行统一监测，并实现数据安全的统一运营」。

采购内容由“构建数据安全运营系统（总部一级平台）”和“构建省分互联网接口敏感数据监测能力”两部分组成，要求包括具备全景态势、数据流转回溯、数据资产管理、敏感信息识别、文件识别、数据分类分级等能力。

2021年中国联通总部信息安全数据安全运营系统研发项目招标公告

本招标项目为2021年中国联通总部信息安全数据安全运营系统研发项目（招标编号：YT09202102496ZB），招标人为中国联合网络通信有限公司，招标代理机构为中邮通建设咨询有限公司。项目资金由招标人自筹，资金已落实。项目已具备招标条件，现进行公开招标，有意向的潜在投标人（以下简称投标人）可前来投标。

1. 项目概况与招标内容

1.1 项目概况

国家陆续出台《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》，为落实关于数据安全管理的规定，规范网络数据处理活动，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益，满足上级单位的监管要求，中国联通依据现状需求将构建功能完备、能力领先的五全安全体系，实现纵向到底、横向到边、治理重构、实现穿透的全客户、全数据、全系统、全触点和全流程的数据安全运营体系和能力体系，重点建设总部–省份两级结构的数据安全运营系统以及对互联网接口的敏感数据进行监测的能力。

1.2 招标内容

1.2.1 采购内容：建设总部–省分两级架构数据安全运营系统，对31省分公司DCN网互联网出口的数据进行统一监测，并实现数据安全的统一运营。主要内容包括：

（1）构建数据安全运营系统（总部一级平台），结合国家法律法规、行业要求、监管要求，实现数字化专业线数据安全持续运营能力，包括全景态势、威胁分析、数据流转回溯、策略管理、数据资产管理、运营报告等，满足监管合规要求、报备、备案等标准和规范。

（2）构建省分互联网接口敏感数据监测能力，基于数据共享交换体系，实现敏感数据监测，包括协议解析、威胁监测能力、敏感信息识别、文件识别、API信息监控能力、数据分类分级等。

1.2.2 采购预算：采购预算金额为1480万（不含税），含在2021年项目批复投资内。

1.2.3 技术要求：详见招标文件“第五章 技术规范书”。

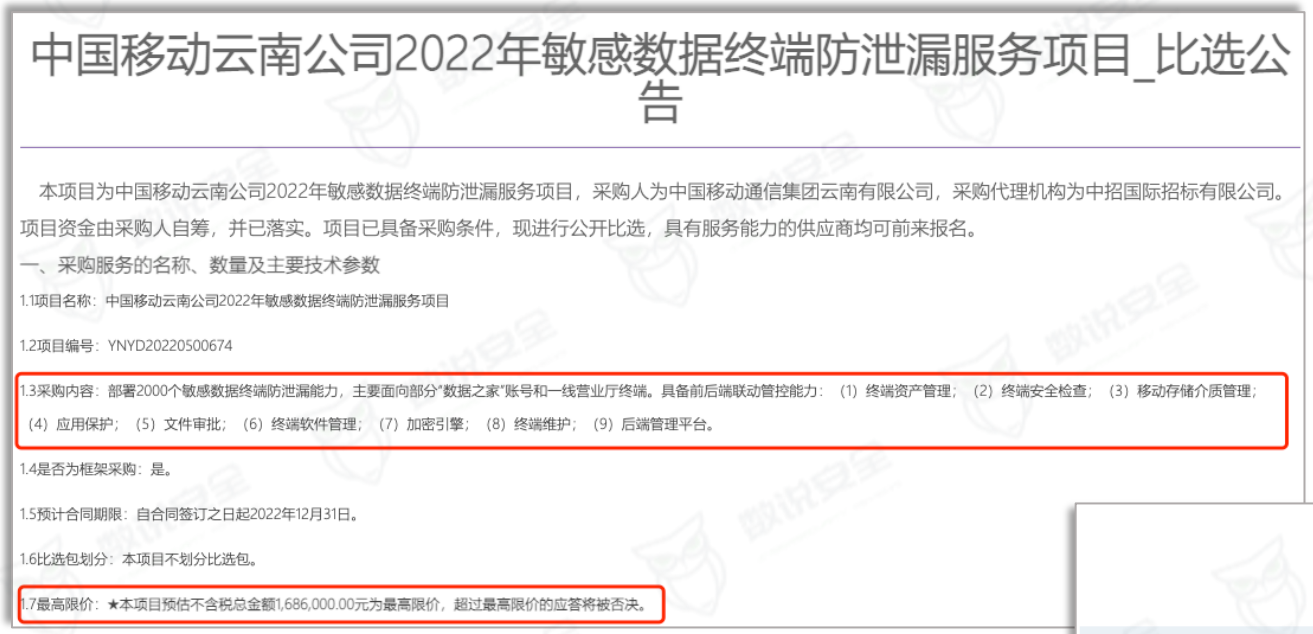
1.2.4 建设周期：自签订合同之日起，90天内完成系统部署，部署到买方指定地点。

1.2.5 保修期：提供终验后2年的免费维保服务。

1.2.6 实施地域：招标人指定地点。

资料来源： 市场公开招投标文件

• 电信行业——敏感数据终端防泄漏及数据安全管控平台项目



中国移动云南公司2022年敏感数据终端防泄漏服务项目_比选公告

本项目为中国移动云南公司2022年敏感数据终端防泄漏服务项目，采购人为中国移动通信集团云南有限公司，采购代理机构为中招国际招标有限公司。项目资金由采购人自筹，并已落实。项目已具备采购条件，现进行公开比选，具有服务能力的供应商均可前来报名。

一、采购服务的名称、数量及主要技术参数

1.1项目名称：中国移动云南公司2022年敏感数据终端防泄漏服务项目

1.2项目编号：YNYD20220500674

1.3采购内容：部署2000个敏感数据终端防泄漏能力，主要面向部分"数据之家"账号和一线营业厅终端。具备前后端联动管控能力：（1）终端资产管理；（2）终端安全检查；（3）移动存储介质管理；（4）应用保护；（5）文件审批；（6）终端软件管理；（7）加密引擎；（8）终端维护；（9）后端管理平台。

1.4是否为框架采购：是。

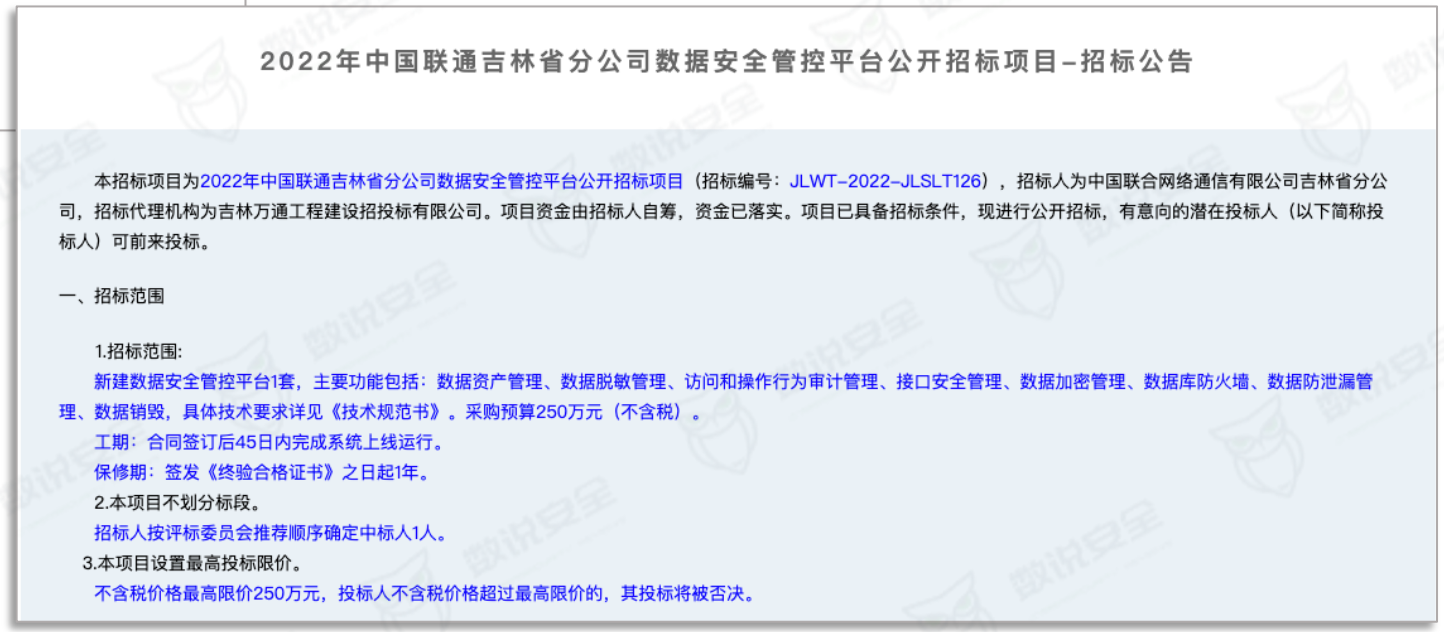
1.5预计合同期限：自合同签订之日起2022年12月31日。

1.6比选包划分：本项目不划分比选包。

1.7最高限价：★本项目预估不含税总金额1,686,000.00元为最高限价，超过最高限价的应答将被否决。

2022年6月，中国移动云南分公司发布了2022年敏感数据终端防泄漏服务的采购项目，项目预算168.6万。

2022年7月，中国联通吉林省分公司发布了2022年数据安全管控平台的招标采购项目，项目预算250万。要求新建数据安全管控平台一套，主要功能包括：数据资产管理、数据脱敏管理、访问和操作行为审计管理、接口安全管理、数据加密管理、数据防火墙、数据防泄漏管理、数据销毁等。



2022年中国联通吉林省分公司数据安全管控平台公开招标项目–招标公告

本招标项目为2022年中国联通吉林省分公司数据安全管控平台公开招标项目（招标编号：JLWT–2022–JLSLT126），招标人为中国联合网络通信有限公司吉林省分公司，招标代理机构为吉林万通工程建设招投标有限公司。项目资金由招标人自筹，资金已落实。项目已具备招标条件，现进行公开招标，有意向的潜在投标人（以下简称投标人）可前来投标。

一、招标范围

1.招标范围:

新建数据安全管控平台1套，主要功能包括：数据资产管理、数据脱敏管理、访问和操作行为审计管理、接口安全管理、数据加密管理、数据库防火墙、数据防泄漏管理、数据销毁，具体技术要求详见《技术规范书》。采购预算250万元（不含税）。

工期：合同签订后45日内完成系统上线运行。

保修期：签发《终验合格证书》之日起1年。

2.本项目不划分标段。

招标人按评标委员会推荐顺序确定中标人1人。

3.本项目设置最高投标限价。

不含税价格最高限价250万元，投标人不含税价格超过最高限价的，其投标将被否决。

资料来源： 市场公开招投标文件

• 电信行业——数据安全服务项目

2022年5月，中国移动广州公司和贵州公司分别发布了《2022-2024年IT域数据安全技术支撑服务公开比选项目》和《网络与信息安全管理中心2022-2024年数据安全支撑技术服务项目》，项目预算金额分别为347万元和276万元，具体内容如下：

中国移动广东公司2022-2024年IT域数据安全技术支撑服务公开比选项目_比选公告

本项目为中国移动广东公司2022-2024年IT域数据安全技术支撑服务公开比选项目（采购代理编号：ZJZB-2022-13101），采购人为中国移动通信集团广东有限公司，采购代理机构为中捷通信有限公司。项目资金由采购人自筹，并已落实。项目已具备采购条件，现进行公开比选，具有服务能力的供应商均可前来报名。

一、项目概况与采购内容

1.1 开展目的：根据2021年正式颁布的《数据安全法》、《个人信息保护法》的法律法规要求及目前广东公司面临数字化转型带来的数据安全风险，为满足考核管理要求以及提高内部数据安全保障能力，现拟开展本项目的采购工作。

1.2 采购清单：本项目需采购支撑服务4596人天：

项目名称	工作项	工作内容	工作量（人天）
中国移动广东公司2022-2024年IT域数据安全技术支撑服务公开比选项目	数据安全日常检查支撑服务	一、上线检查 1、应用版本（非app）上线数据安全测试。 2、app数据安全测试，包括：隐私政策审核与数据安全检测。 3、数据安全报告输出 二、能力上台检查 1、完成部门能力上台前的数据安全评估检查 2、数据安全评估报告输出	2346
	专项检查支撑服务	1、迎检检查方案、实施细则输出。 2、迎检准备自查自纠，包括：组织核心系统，准备检查资料，负责自查，指导整改，并输出应对方案。 3、配合现场检查工作，包括：检查材料复核、指导、配合解释等。	2136
	重大节假日数据安全应急保障	1、输出重大节假日保障工作方案与细则。 2、节前数据安全保障。 3、节日期间人员保障。	114
合计			4596

1.3 项目预算：不含税预算为3,469,980元。

1.4 本项目不分标段，综合分第一中选。

1.5 服务周期：合同签订之日起至2024年6月30日。

中国移动贵州公司网络与信息安全管理中心2022-2024年（24个月）数据安全管理支撑技术服务项目_竞争性谈判采购公告

本项目为中国移动贵州公司网络与信息安全管理中心2022-2024年（24个月）数据安全管理支撑技术服务项目，采购人为中国移动通信集团贵州有限公司，采购代理机构为中达安股份有限公司。项目资金由采购人自筹，并已落实。项目已具备采购条件，现进行公开竞争性谈判，具有提供服务能力的供应商均可前来报名。

一、项目概况

1.1项目名称：中国移动贵州公司网络与信息安全管理中心2022-2024年（24个月）数据安全管理支撑技术服务项目

项目编号：GZYD20220500120

采购代理编号：DAGZ20220502

1.2采购内容：本次采购2022-2024年（24个月）数据安全管理支撑技术服务，包括以下内容：

（1）、数据安全合规性评估：包括评估矩阵及方案制定、评估清单梳理及核查核验、企业整体数据安全保护水平评估、企业重点业务应用数据安全保护水平、企业核心数据处理活动平台系统数据安全保护水平评估、评估整改结果复查；

（2）、数据安全监督检查：对企业各单位数据安全管理情况和技术手段落实效果进行监督检查，主要包括监督检查矩阵及方案制定、监督检查实施、监督检查整改结果复查；

（3）、数据安全重点工作支撑：包括数据安全专项行动支撑、数据安全创新试点工作支撑、数据安全检查支撑、数据安全日常支撑、数据安全培训等；

（4）、数据安全审计：包括日志留存合规性排查、4A金库排查、数据安全日常审计、网络数据使用管理、网络数据共享管理；

（5）、智能终端应用（APP、小程序、公众号）安全评测：主要是利用静态代码扫描与动态行为检测技术，对Android-APP、iOS-APP、SDK、公众号、小程序等多平台应用形态提供包括配置安全、数据安全、程序安全、通信安全等检测能力，并提供准确的问题定位及详细的解决方案、评估整改结果复查。

1.3框架预算金额：含税276.4798万元（不含税260.83万元）。

1.4采购周期：框架采购（下单）截止日

1.4.1. 2022年9月17日起24个月止；

资料来源： 市场公开招投标文件

• 电信行业——隐私计算项目分析

2021年6月，联通研究院发布《2021年中欧国联通研究院分布式可信数据共享与隐私计算服务系统开发项目比选公告》，采购预算金额60万元，公告指出：集约化的数据共享面临数据权属、属地管理、归集效率及隐私泄露等问题，分布式数据共享与隐私计算服务提供了数据“可用不可见”的数据共享架构以及“算法找数据”的分布式应用与决策模型，能够促进网络数据要素共享效率及价值挖掘。

本次的分布式可信数据共享与隐私计算服务系统，将助力解决跨域跨管理实体场景数据贯通，消除碎片化及孤岛形式的数据管理影响，实现数据使用全流程可追溯，并构建隐私计算及计算负载调度能力，赋能数据共享“可用不可见”以及分布式应用与决策。

2021中国联通研究院分布式可信数据共享与隐私计算服务系统开发项目比选公告

招标编号：BTPDI-YJGN-2021032　　发布时间：2021-06-08 14:22:49

2021中国联通研究院分布式可信数据共享与隐私计算服务系统开发项目比选公告

本比选项目为2021中国联通研究院分布式可信数据共享与隐私计算服务系统开发项目，（采购代理编号：BTPDI-YJGN-2021032），采购人为中国联合网络通信有限公司研究院，采购代理机构为北京电信规划设计院有限公司。项目资金已落实，具备比选条件，现进行公开比选，特邀请有意向的且具有提供标的物能力的潜在应答方（以下简称应答方）参选。

1. 项目概况与采购内容

1.1
项目概况

随着数据被定义为一种新型生产要素，数据已成为各行业数字化转型的关键引擎。集约化的数据共享面临数据权属、属地管理、归集效率及隐私泄露等问题，分布式数据共享与隐私计算服务提供了数据“可用不可见”的数据共享架构以及“算法找数据”的分布式应用与决策模型，能够促进网络数据要素共享效率及价值挖掘。

运营商网络的IT域与CT域以及运营商参与的行业专网及OT系统中分布着大量网络数据，这些网络数据价值受限于技术、管理及政策无法被充分利用。在中国联通加速全面数字化转型驱动下，本项目以CUBE-Net3.0总体架构为引领，一方面构建去中心化的数据共享服务，提供CUBE-Net3.0云网大脑分布式数据共享引擎，助力解决跨域跨管理实体场景数据贯通，消除碎片化及孤岛形式的数据管理影响，实现数据使用全流程可追溯；另一方面，构建隐私计算及计算负载调度能力，赋能数据共享“可用不可见”以及分布式应用与决策。

本项目通过构建分布式数据共享与隐私计算服务系统，为CUBE-Net3.0云网大脑网络数据分析和数字孪生提供可信的数据共享服务，完善云网大脑底层数据共享基础设施。

1.2
采购内容

一套分布式可信数据共享与隐私计算服务系统，应满足如下技术要求：

1.数据共享目录服务：提供数据共享服务入口，具备共享数据目录服务、隐私计算网关可信验证、数据分析结果追溯、数据调取行为记录等服务功能。

2.数据共享平台：能够实现隐私计算网关节点注册/调度/管理、用户身份认证、数据计算负载匹配及分发、与数据共享目录服务接口等功能。

3.隐私计算网关：提供可信计算环境实例下隐私计算及必要的libOS库支持，能够单节点及多节点方式提供隐私计算能力、密钥管理及libOS具备主流数据分析、机器学习算法库及OTDR SOR文件格式解析库。

1.3
本项目设置最高限价，最高限价为60万元人民币(不含税)，应答方应答报价高于最高限价的，其应答文件将被否决。

1.4
服务期限: 合同签署后4个月内完成系统验收、交付及部署

金融行业需求分析

• 金融行业——银行业是规划制度的重点落脚领域

数说安全

2022年1月12日央行印发《金融科技发展规划（2022-2025年）》，数据要素是《规划》中新增的核心内容，数据要素被升级成为金融业的生产要素。

《规划》的重点任务部分明确了有关数据安全建设的要求，指出要“强化数据建设能力：建立协调一致、涵盖数据全生命周期的数据治理体系。”“推动数据有序共享：在技术方面，积极应用多方安全计算、联邦学习、差分隐私、联盟链等技术，探索建立跨主体数据安全共享隐私计算平台，在保障原始数据不出域前提下规范开展数据共享应用，确保数据交互安全、使用合规、范围可控，实现数据可用不可见、数据不动价值动。”“做好数据安全保护：建立健全数据全生命周期安全管理长效机制和防护措施，运用匿踪查询、去标记化、可信执行环境等技术手段严防数据逆向追踪、隐私泄露、数据篡改与不当使用，依法依规保护数据主体隐私权不受侵害。建立历史数据安全清理机制，利用专业技术和工具对超出保存期限的用户数据进行及时删除和销毁、定期开展数据可恢复性验证确保数据无法还原，确需作为样本数据保存的，应经用户同意并进行去标识化处理，移入非生产数据库保存，确保用户隐私信息不被直接或间接识别，切实保障用户数据安全。”

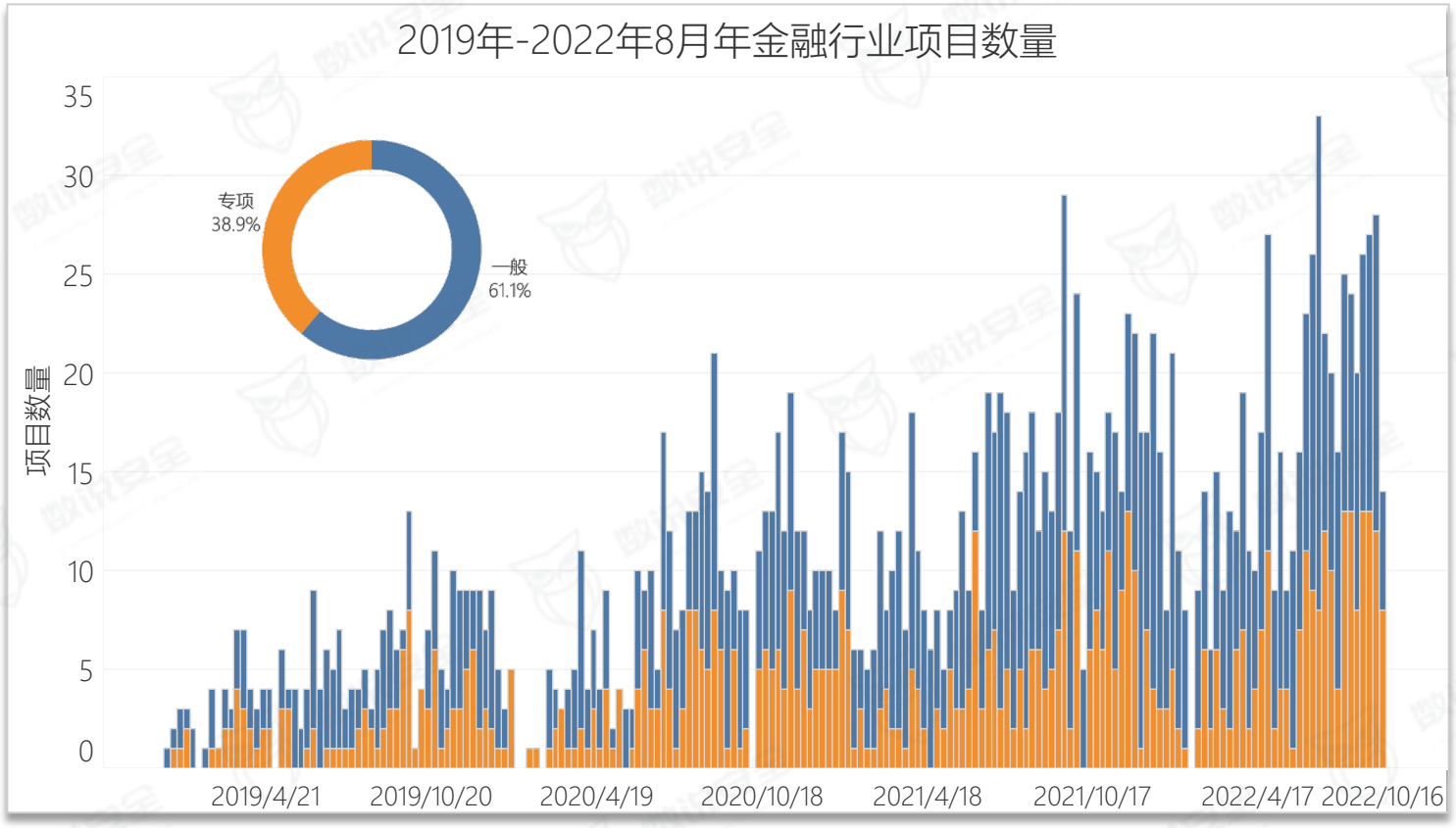
从2020年开始，央行、银保监会等金融部门，开始密集发布有关数据安全保护的规范规定，相关制度体系逐步完善。

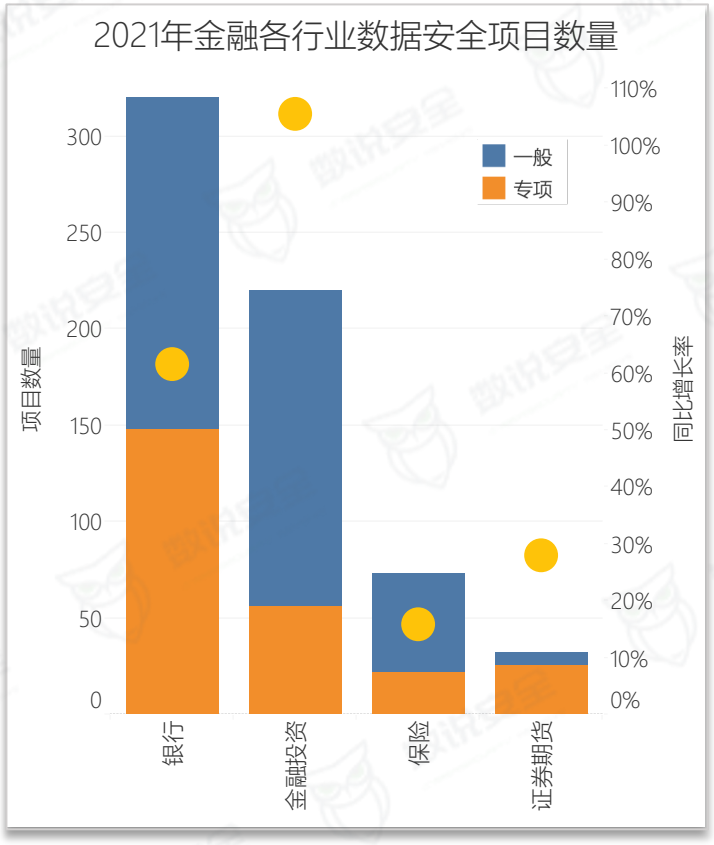
时间	发布单位	文件名称	重要内容
2020年2月13日	中国人民银行	《个人金融信息保护技术规范》	将个人金融信息按敏感度从高到低分为C3到C1三个类别，并实施不同级别保护；从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。
2020年9月23日	中国人民银行	《金融数据安全分级指南》	给出了金融数据安全分级的目标、原则和范围，以及数据安全定级的要素、规则和定级过程。
2021年1月15日	中国银保监会	《中国银保监会监管数据安全管理办法（试行）》	明确责任部门，制定了监管数据安全工作规则和管理流程、技术防护措施、评估和监督检查制度等。
2021年4月8日	中国人民银行	《金融数据安全数据生命周期安全规范》	规定了金融数据生命周期安全原则、防护要求、组织保障要求以及信息系统运维保障要求，建立覆盖数据采集、传输、存储、使用、删除及销毁过程的安全框架。
2021年12月3日	中国人民银行	《金融数据安全评估规范（征求意见稿）》	规定了金融数据安全评估触发条件、原则、参与方、内容、流程及方法，明确了数据安全管理、数据安全保护、数据安全运维三个主要评估域及其安全评估主要内容和方法。

• 金融行业——银行和金融投资企业数据安全建设提速

近三年金融行业数据安全项目数量不断增加，2021年项目数量为674个，同比增长60%，其中半数项目出自银行业，2021年银行业项目数量同比增长61%，专项项目同比增长33%，高于行业平均水平； 保险业、证券期货业和金融投资业项目数量同比增长率分别为16%、 28% 和106% ，专项项目同比增长率分别为-4.3%、 24% 和167% 。

银行在数据安全方面的规范标准更加健全完善，在金融行业的数据安全建设中更加领先；同时，数量众多的“影子银行”类——金融投资业，包括投资管理、资产管理、融资担保等机构的网络及数据安全防护能力相较于银行业差距较大，水准参差不齐，随着监管制度的规范化和严格化，数据安全项目在2021年增长显著，数据安全建设明显加速，但由于机构数量众多，仍然有相当大比重的企业需要补齐数据安全防护能力。





• 金融行业——数据安全进入初步建设阶段

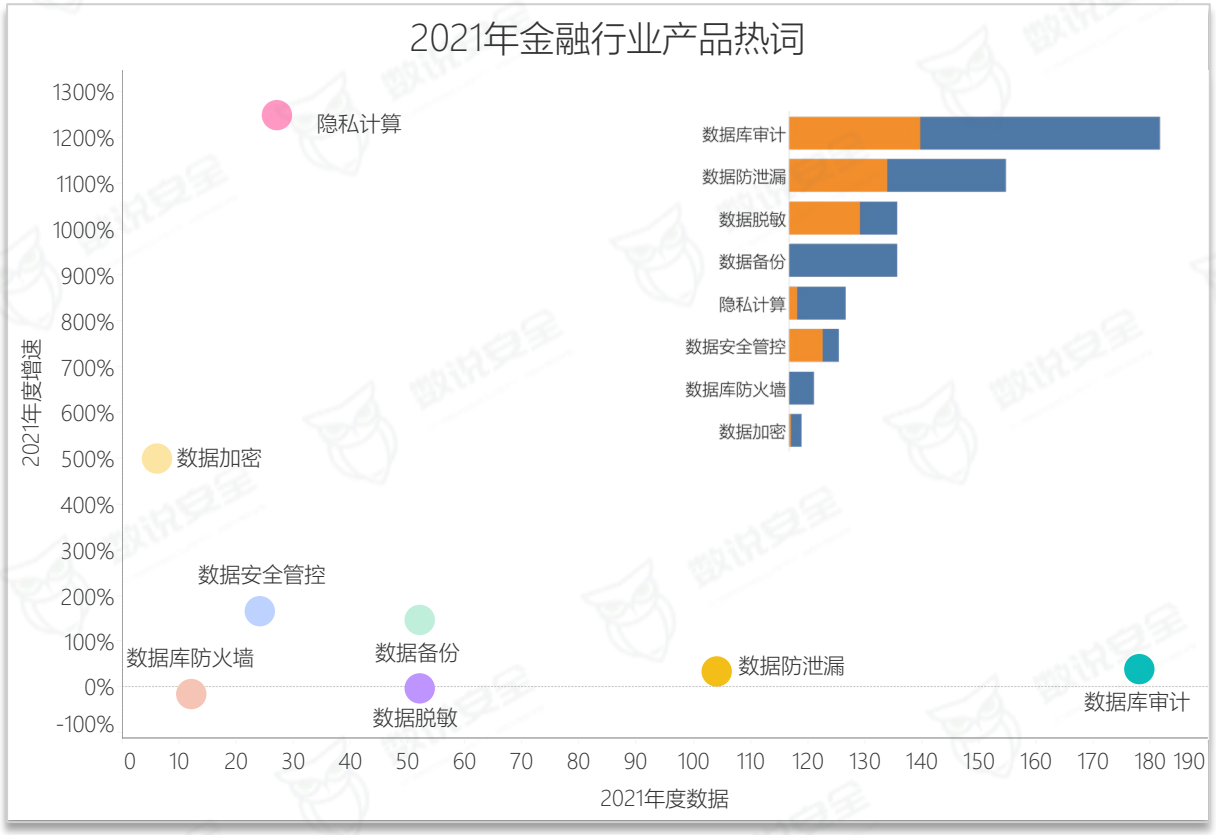
根据数说安全项目统计，2021年金融行业的数据安全进入有序推进阶段。

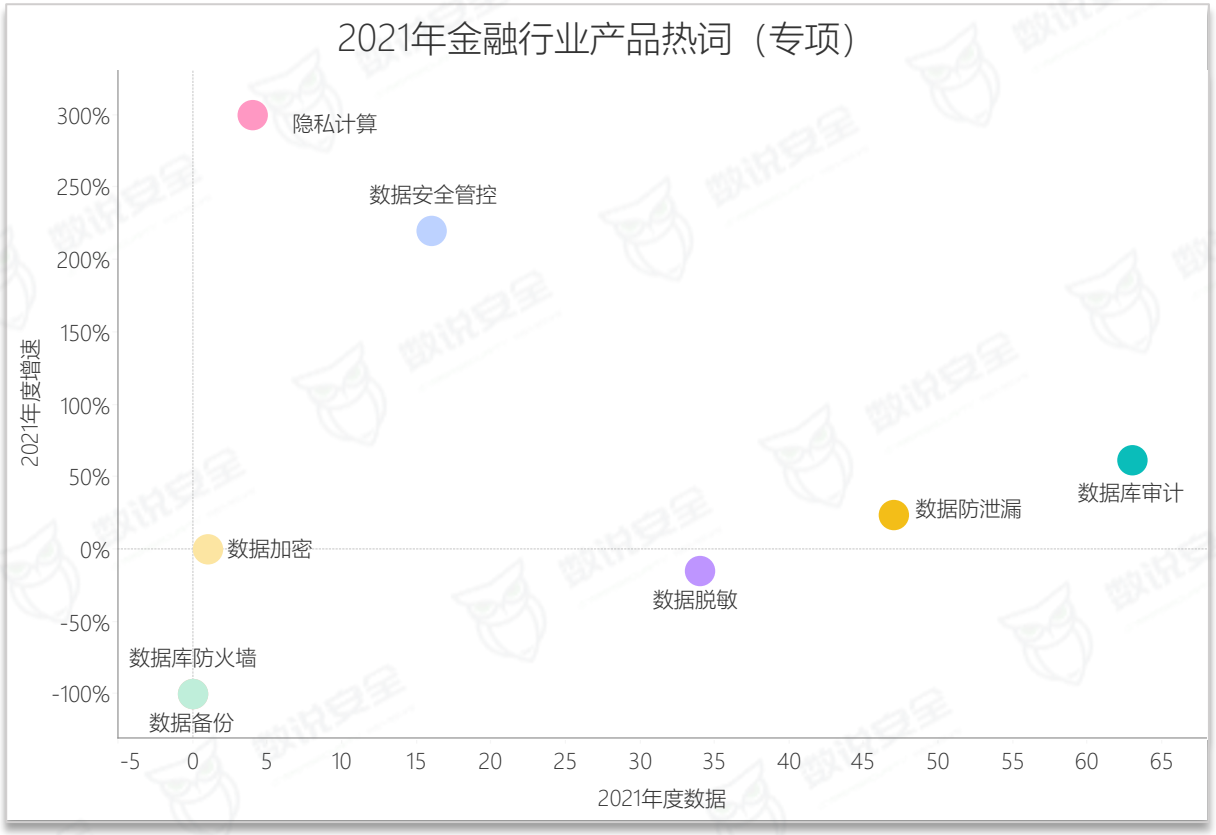
受益于《金融数据安全分级指南》和《个人金融信息保护技术规范》的出台，数据安全咨询、数据分类分级、数据安全评估项目数量明显增加。

数据库审计产品数量、数据防泄漏类产品采购数量较多。

2021年4月《金融数据安全数据生命周期安全规范》颁布，数据安全管控平台类项目采购数量明显增加，且专项项目占比较大。

响应金融“十四五”规划中对推动有序数据共享的要求，隐私计算类产品采购激增，且增速明显领先其他产品。





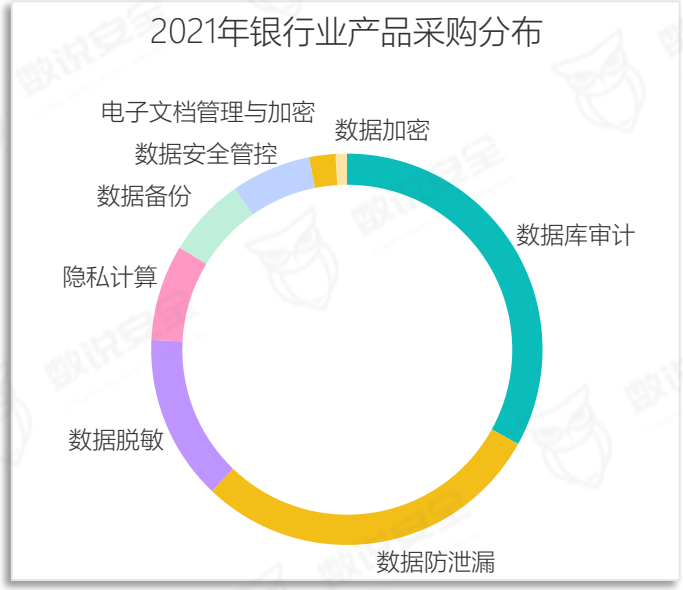
• 金融行业——各细分行业数据建设参差不齐

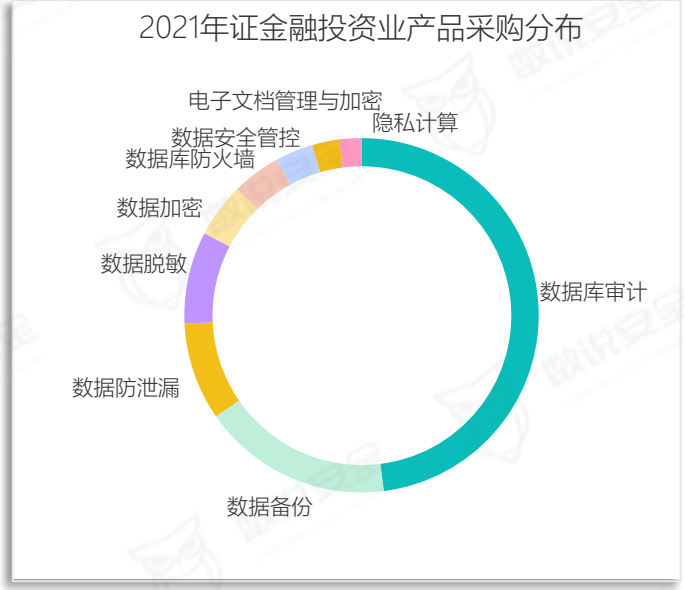
金融业机构由于内边界隔离建设较完善，且除银行业外的其他机构数据对外流动性需求较弱，数据环境相对封闭，因此对数据安全建设的需求差异较大，2021年各细分金融业机构的数据安全采购产品结构呈现出明显分化。

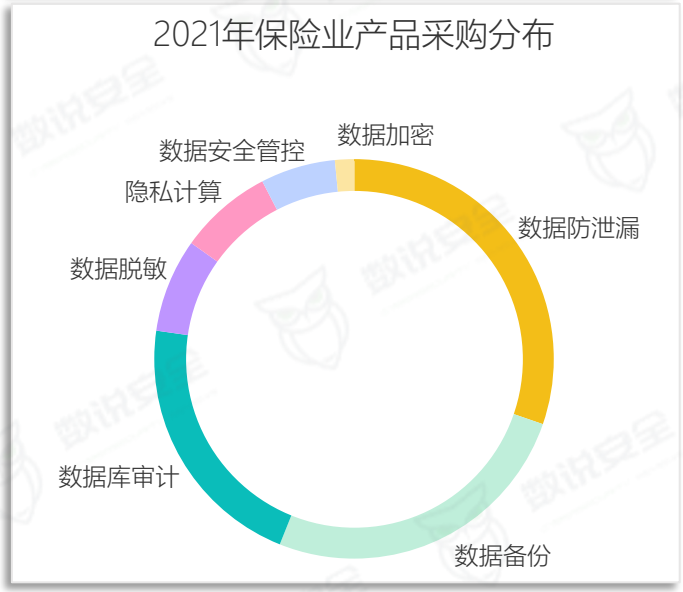
银行业和保险业受到政策重视度、业务广泛度、规范出台进度等因素的影响，采购的数据安全产品较为全面，数据库审计和数据防泄漏是重点的采购产品，数据安全管控平台比重逐步增加，隐私计算的采购数量也迈入产品Top5序列。

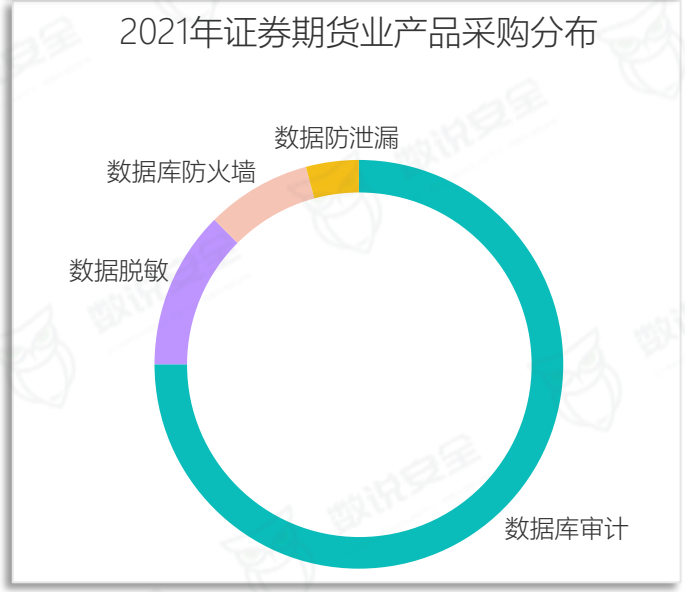
证券期货机构主要承担交易入口及交易管理服务的功能，资金流动需经过银行完成，系统相对独立，数据安全建设也较为滞后，以采购数据库安全产品为主。

金融投资行业企业众多且散乱，监管难度较大，数据安全建设水平也参差不齐，随着业务在监管领域的不断打通，未来也将成为政策监管逐渐加强的领域。









• 金融行业——数据生命周期安全框架指引

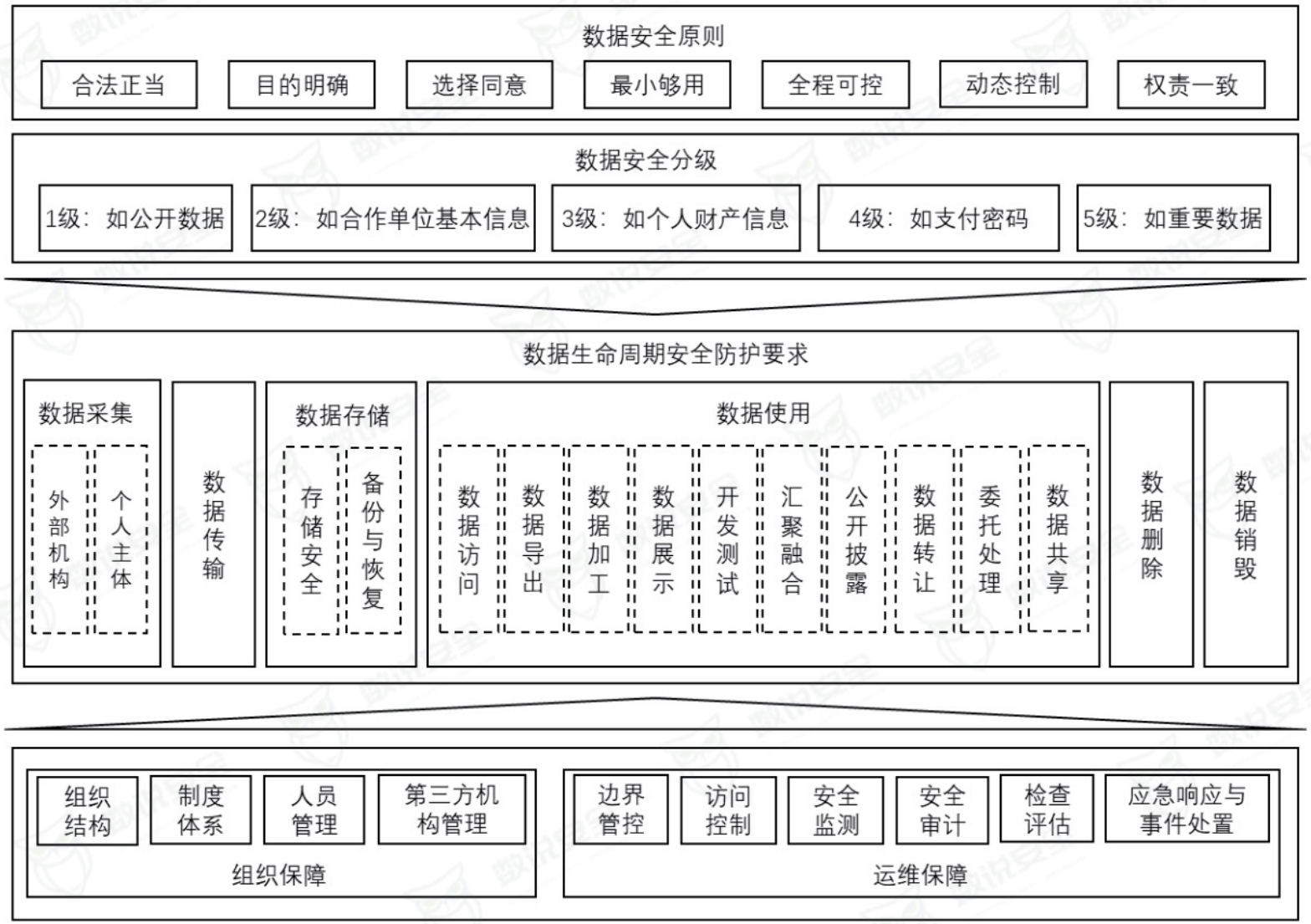
2021年4月8日，中国人民银行发布了《金融数据安全数据生命周期安全规范》，规定了金融数据生命周期安全原则、防护要求、组织保障要求以及信息系统运维保障要求，建立覆盖数据采集、传输、存储、使用、删除及销毁过程的安全框架。

金融业机构存储了大量的客户数据，借记卡、信用卡信息泄漏、网站地址钓鱼攻击、黑客入侵等事件频发，造成的经济损失通常较高，需要加强防护。

金融业机构在提供金融产品和服务、开展经营管理等活动中，涉及的数据访问、加工、展示、汇聚融合、公开披露、数据转让、委托处理、数据共享等处理工作较多，此环节中数据的使用目的和范围，以及可能产生的数据非法访问、窃取、泄漏、篡改、损毁等安全风险将成为未来数据安全的重点保护领域。

2021年出台的《金融科技发展规划（2022-2025年）》中提出要“推动数据有序共享：在技术方面，积极应用多方安全计算、联邦学习、差分隐私、联盟链等技术，探索建立跨主体数据安全共享隐私计算平台。”

数据生命周期安全框架



资料来源：《金融数据安全数据生命周期安全规范》

• 金融行业——数据使用过程安全要求

数说安全

数据访问

①按最小化原则确定二级及以上访问权限规则；
②三级及以上访问应建立防问申请、审批及验证机制；
③根据数据级别不同设置安全措施；
④对访问权限和情况进行定期审计，对访问规则和清单至少每半年进行一次复核；
⑤限制访问频繁人员的访问频率并留存访问记录。

数据导出

①根据最小够用原则，确定数据导出场景、范围和相应的权限规则；
②二级及以上数据导出操作应明确责任人，并进行身份认证措施和操作记录留存；
③ 三级及以上数据导出应设置权限申请、审核批准、多因素认证、二次授权等机制，并采用机密、脱敏等手段防止数据泄露。

数据加工

①明确加工过程中数据获取方式、访问接口、授权机制、逻辑安全、处理结构等内容；
②三级及以上数据加工前应进行数据安全评估，并采用数据加密、脱敏技术保证加工过程中的数据安全；
③除必须外，不应对四级数据进行加工；
④应对加工过程进行监督和检查，并记录操作日志。

数据展示

①展示前应评估展示需求，确定展示的必要性和安全性；
②展示时，应确保数安全性；
③展示后，应及时将数据从本地缓存中清除；
④二级数据展示应先审批；
⑤三级数据展示应在审批基础上采用屏蔽等技术防止数据泄漏；
⑥四级数据除额外规定不应明文展示。

开发测试

①开发测试环境数据与生产环境数据应有效隔离。
②以专用终端获取数据应经过审批，获取三级及以上数据是应控制数据获取范围，并进行脱敏处理；
③使用外部工具进行开发测试前应进行数据安全评估；
④开发测试的外部终端应进行统一安全管理；
⑤应定制开发测试审核流程。

汇聚融合

①汇聚融合数据不应超出采集时声明的范围；
②汇聚融合前应开展数据安全影响评估；
③涉及三方合作时应明确范围、责任和义务，并采取如多方安全计算、联邦学习、加密、防泄漏等技术；
④汇聚融合后的数据应重新明确所属单位和安全责任部门，并确定数据安全级别。

公开披露

①应按规定在官方渠道披露；
②数据披露前应对合规性、业务需求、脱敏方案、披露时间等进行审核与审批；
③采取防篡改等技术措施，保障披露数据的真实性与完整性；
④三级及以上数据原则上不应公开披露；
⑤应准确记录和保存公开披露情况。

数据转让

除以下情况外，原则上不应转让数据：国家与行业主管部门要求；已通过合同协议等约定获得数据转让授权；金融业机构收购、兼并、重组等情况时，依照国家及行业有关规定履行义务。

委托处理

①受委托的第三方应满足国家及行业主管部门要求，并经过金融机构事前尽职调查；
②应对委托数据进行安全影响评估；
③应对委托方数据安全防护能力进行评估；
④应采用脱敏、加密、水印等技术防止数据泄漏和滥用；
⑤应对委托数据进行全称审计并保存记录。

数据共享

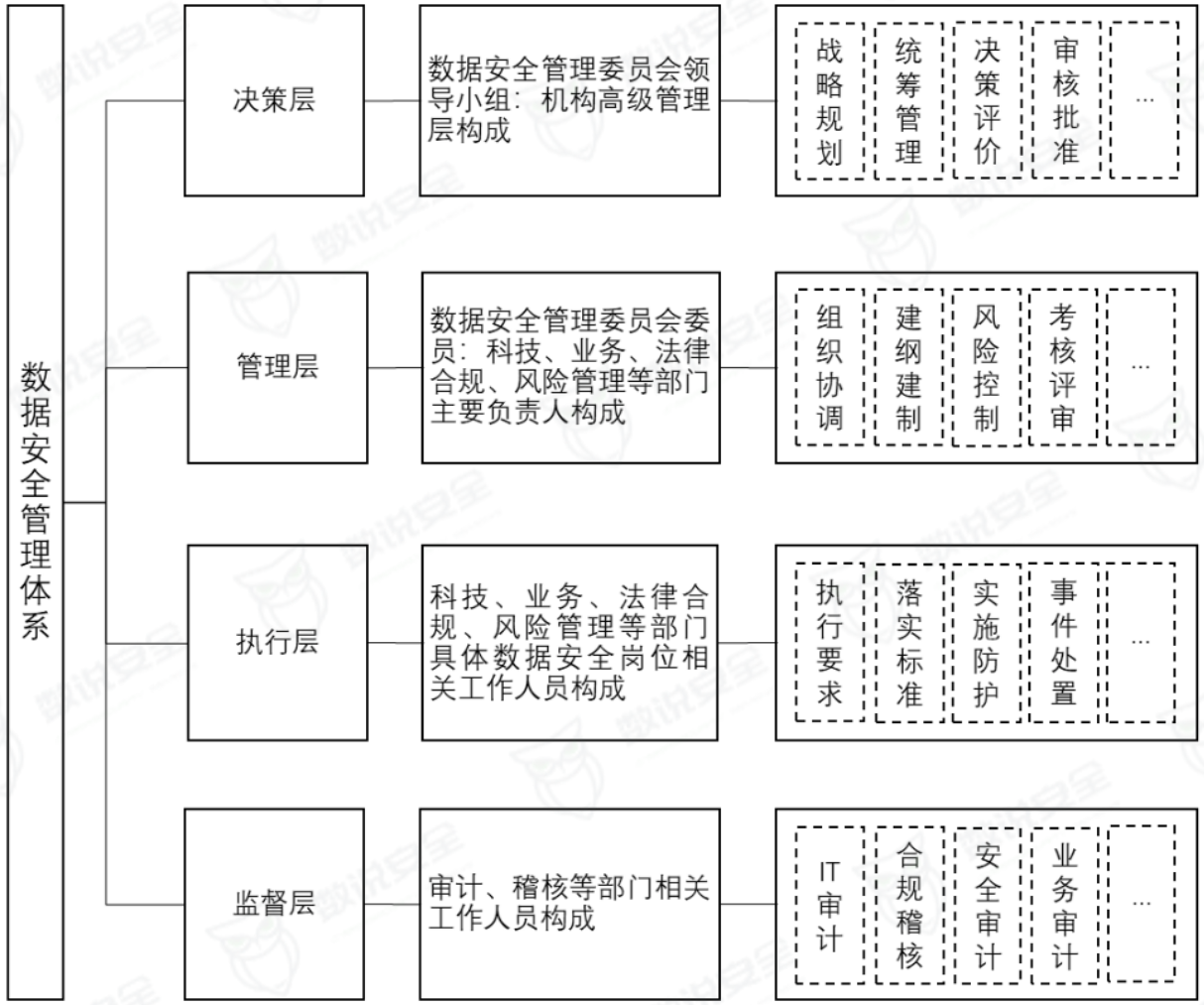
①内容数据共享应明确安全要求和责任部门，建立审核批准机制，对数据使用目的、内容、时间、防护措施、数据使用后的处置方式进行审批和审计，并留存记录；
②在①的要求基础上，对接收方数据保护能力进行评估，确保数据使用在事先约定范围内，制定应急响应措施等保证数据安全。

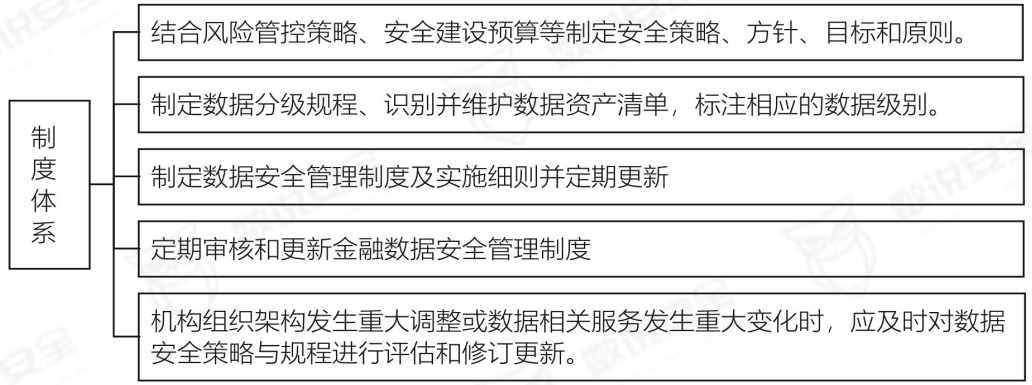
资料来源：《金融数据安全数据生命周期安全规范》

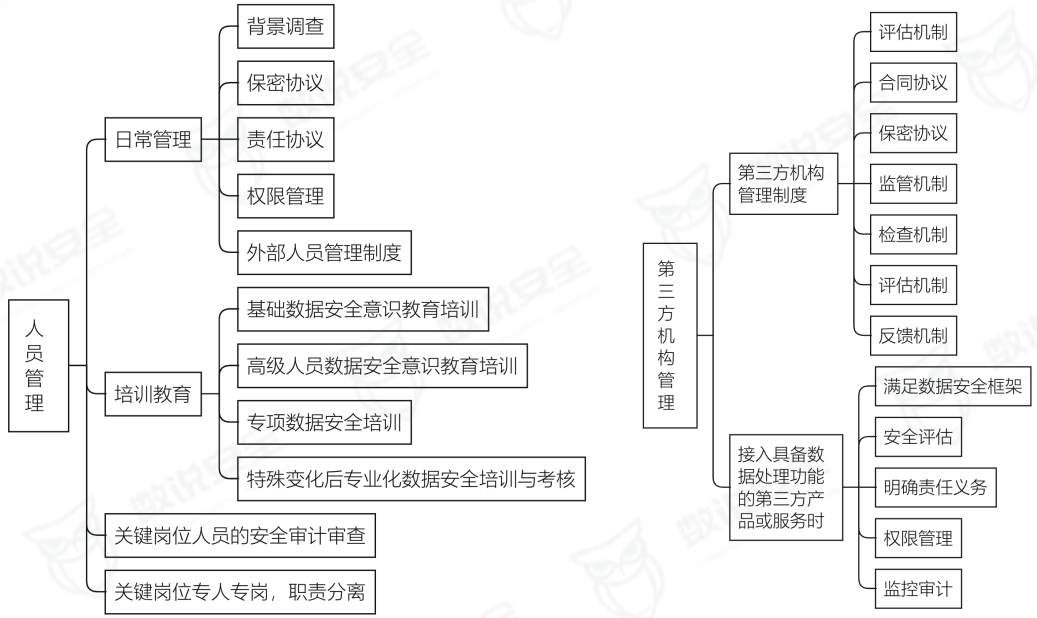
• 金融行业——数据安全组织保障细则

数据安全组织保障确保数据安全工具具有包括决策层、管理层、执行层以及监督层的完善管理体系。

信息系统运维过程中的数据安全防护工作能够加强在边界管控、访问控制、安全监测、安全审计、检查评估、应急响应与事件处置等过程中的风险防控能力，可有效保障数据安全防护机制的有效执行和数据安全问题的及时发现与应对。







资料来源：《金融数据安全数据生命周期安全规范》

• 金融行业——XX省地方金融监督管理局数据安全项目（一）

数说安全

2021年9月， xx省金融监督管理局发布了信息系统安全基础设施和运营服务（2021年）项目（数据安全管理与审计服务部分）招标文件。项目分为（采购包1：数据安全管理服务，预算金额70.25万元）和（采购包2：数据安全审计服务，预算金额128.6万元）。

项目建设背景	
（一）国家战略支持大湾区成为国际一流湾区	中共中央、国务院印发《粤港澳大湾区发展规划纲要》，对粤港澳大湾区建设提出重要战略性指导，xx省是粤港澳大湾区一体化的重要桥头堡。通过搭建省中小企业融资平台，提升金融机构的科技能力、风险管理能力，构建智能化的金融监管体系，及时有效反映金融机构业务运营状况，有助于完善创新投融资体系。
（二）企业融资难融资贵问题突出	xx省中小微企数量众多达 1100 万家，GDP 贡献高达全省 60%，解决了全省80%的城镇就业数量，是全省经济发展的主要动力之一。同时，xx省产业结构特征十分鲜明，工业制造业、零售批发业、房地产业等行业，在全国居于领先水平。但与此同时，xx省的中小微企业融资难、融资贵问题仍然突出，一方面融资的可获得性，信息不对称问题使得金融机构难以准确识别中小企业的信用风险，无法打破中小微企业抵押、担保瓶颈；另一方面融资的可操作性，大量金融机构缺少专业的、可靠的、具备公信力的信息化业务平台，无法满足中小微企业小、急、频的融资需求。
（三）金融机构与企业信息不对称	xx省已经形成了功能完备、层次丰富的金融生态，服务机构涵盖几乎所有的主流银行、500 余家的小额贷款公司、超过 8000 家的保理公司以及众多的 PE、VC，包括区域性股权市场，其资产规模、产品质量、科技实力及服务水平等领先于全国。但是，大量金融机构仍然主要服务大中型头部企业，在扩大对中小微企业有效金融供给方面发力不足，这既不利于激发中小微民营经济的活力和创造力，也制约了xx省金融机构自身的进一步发展。 近年来，在江苏、海南等多个省市，深圳、苏州、烟台等城市在地方政府和地方金融监督管理局的指导下建设省市级综合金融管理平台，政府负责搭建一站式服务，通过行政手段和市场手段相结合方式，一方面坚持政府引导驱动，通过窗口引导、政策落地等多种方式让金融机构动起来，另外一方面，以大数据、云计算等金融科技手段为解决中小企业融资问题赋能。平台建设起到示范和引领的作用，对解决中小企业融资问题起到很好的促进作用。

在上述背景下， xx省地方金融监督管理局建设了广东省中小企业融资平台，解决企业、金融机构之间信息不对称问题，缓释中小企业融资难题。

• 金融行业——XX省地方金融监督管理局数据安全项目（二）

数说安全

总体目标
通过安全管理服务，提高系统应对突发事件的能力，增强系统的抗攻击性，降低由于网络和信息安全的攻击对系统造成的影响。借助细节上的安全管理服务，宏观上的对安全趋势的把握，实现省金融局合理规划相应的安全工作。确保xx省中小企业融资平台的可持续性，从而为各使用群体提供高可用、优质的服务。实现数据的安全管控，对数据库进行访问行为控制、高危操作拦截、可疑行为审计。符合国家法律和法规要求，落实国家和主管部门的要求，切实做好信息安全保障体系的建设。

本项目围绕xx省中小企业融资平台开展安全运营。平台整体部署在省“数字政府”政务云及政务外网上，网络架构整体分为互联网接入区、政务云互联网区、政务云政务外网区、政务云大数据服务平台对接区4个部分，其中互联网区是客户、金融机构以及第三方数据源接入区；政务云互联网区利用接入网关和API网关对外提供服务；政务云政务外网区用于部署授信网络服务、业务核心应用、基础服务、中间件等应用集群；政务云大数据服务平台对接区用于对接外部政务系统和政务大数据服务。

采购包1：数据安全服务内容：

xx省中小企业融资平台整体部署在省“数字政府”政务云及政务外网上。 要求对xx省中小企业融资平台提供安全管理服务，包括应用系统渗透测试，安全应急演练服务，漏洞扫描服务，数据安全监测服务，数据、应用账号安全管理服务。

服务名称	服务交付	交付类型
应用系统渗透测试	《渗透测试服务方案》、《渗透测试报告及漏洞修复建议》、《漏洞整改复测报告》	文档
安全应急演练	《应急演练服务方案》、《应急演练场景脚本设计》、《应急演练总结》	文档
漏洞扫描服务	《漏洞扫描服务方案》、《漏洞修复报告及修复建议》	文档
数据安全监测服务	《月度数据安全服务检查报告》、《日常敏感数据问题处理报告》	文档
数据、应用账号安全管理服务	《账号安全管理报告》、《账号安全管理规范制度》	文档

• 金融行业——XX省地方金融监督管理局数据安全项目（三）

数说安全

采购包2：数据安全审计服

数据安全审计服务项目目标

本项目是为了保障xx省中小企业融资平台安全管理制度的各项要求真实有效地得到落实，同时为确保xx省中小企业融资平台的数据安全可控，防止在数据治理、数据运营及管理等过程中发生数据泄露事件。通过检查和评价对中小企业融资平台数据安全运维、运营、管理的日常业务活动、运营与保障、组织架构责任机制、关键控制环节和控制点等全生命周期的过程进行检查监督的活动，确保运维、运营和管理活动符合法律法规和管理制度的要求从而保证所有政务数据在使用过程中均得到有效保护、防止敏感数据泄漏、避免数据被非法操作、数据管理符合有关法律法规要求。

本项目的服务内容包括安全审计服务、数据全生命周期安全流量处理和存储服务、数据安全日志溯源服务等三部分：

- 数据安全审计服务
  - 安全组织管理审计：确认其是否满足广东省中小企业融资平台数据治理战略要求。
  - 安全规章制度审计：确认是否满足广东省中小企业融资平台数据安全管理要求。
  - 数据生命周期安全审计：检查和评价数据的安全性、可靠性和经济性，揭示可能存在的问题，提出完善信息系统控制的审计意见。
  - 数据业务安全审计：从数据业务方面的审批策略、风险管理、质量管理、服务管理、项目管理、业务连续性管理等方面，分析策略控制有效性及其风险，形成数据业务总体控制的审计评价和结论。
  - 数据系统安全审计：对系统应用控制过程、安全运行环境、计算分析过程等进行审查和评价。
  - 数据安全运营审计：进行安全运营策略审计、安全检查审计、安全应急审计、运维安全审计等，并提出数据安全运营审计意见和结论。
  - 数据安全管理审计：安全管理制度审计、数据安全管控审计、数据库安全监管审计、数据关键环节安全管控审计、人员行为安全监管审计、数据资源管理审计等，并提出数据安全管理审计意见和结论

- 数据全生命周期安全流量处理和存储服务
  - 数据安全日志处理服务：提供网络流量数据进行分析和预处理服务，根据安全运营和安全管理的制度流程，提炼出流量数 据类别，建立网络流量处理模型，来保留有价值的数据，将与安全监审无关的原始数据进行丢弃。
  - 数据安全日志存储服务：需自带2台经公安部门认证的专用定制设备，实时将包含重要的操作和安全信息的网络流量进行存储。
    数据安全日志存储服务应支持保存6个月以上的管理和安全流量数据，存储的流量数据在网络上无法直接访问，存储设备支持断网、拆机等对设备异常操作的告警。网络流量存储服务须采用"金库"管理模式，当需要进行日志溯源分析时，需由广东省地方金融监督管理局、安全审计 方等多方同时在场，通过专用的客户端接入设备获取网络流量数据。

- 数据安全日志溯源服务
  - 提供数据安全日志溯源服务。基于网络流量数据处理和存储服务所保存的日志数据，为采购人提供分析异常情况发生的部位、发生的原因，确定相关证据链。
  - 每季提供一次数据安全审计服务，审计内容包含安全组织管理、安全规章制度、数据生命周期安全、数据业务安全、数据系统安全、数据 安全运营、数据安全管理等方面内容，并提供季度数据安全审计报告。

• 金融行业——项目分析

2021年9月中国农业发展银行发布数据安全咨询项目招标公告，需要制定数据安全项目整体工作方案，包括工作所涉及的组织架构，建设方法、工作及管理机制、详细工作计划、规划里程碑、成果审议等内容，协助完成项目启动准备等工作，项目预算金额396万。

同期，徽商银行发布关于敏感数据识别及分类分级的采购招标公告，采购敏感数据识别、数据分类分级、数据安全风险评估等，项预算金额252万。

徽商银行关于敏感数据识别及分类分级的采购项目招标公告

徽商银行因业务发展需要，现对“徽商银行关于敏感数据识别及分类分级的采购项目”进行公开招标，欢迎符合条件的投标人参加投标，现将有关事宜公告如下：

一、采购项目名称及内容

1、招标人：徽商银行股份有限公司

2、项目名称：徽商银行关于敏感数据识别及分类分级的采购项目

3、项目编号：GN2021-10-3972

4、最高投标限价：252 万元

5、采购内容：敏感数据识别、数据分类分级、数据安全风险评估等，具体详见招标文件

中国农业发展银行数据安全咨询项目招标公告

发布时间：2021-09-26 11:21:24

采购人	采购方式	所在地区	品类	标签
代理机构发布	公开招标	全国	服务>咨询服务	咨询服务/中信国际

1. 招标条件

本招标项目的招标人为**中国农业发展银行**，资金来源：**企业自筹**。项目已具备招标条件。

中信国际招标有限公司（以下简称“招标代理机构”）受**中国农业发展银行**（以下简称“招标人”）的委托，就**中国农业发展银行数据安全咨询项目**（**招标编号：0733-21162932**）进行**公开**招标。欢迎合格的投标人前来投标。

2. 采购内容

2.1 中国农业发展银行拟采购数据安全咨询服务，制定数据安全项目整体工作方案，包括：工作所涉及的组织架构、建设方法、工作及管理机制、详细工作计划、规划里程碑、成果审议等内容，协助完成项目启动准备等工作。

2.2服务周期：合同签订后8个月。

2.3本项目最高投标限价：396万元。

详见招标文件第五章项目需求书。

资料来源： 市场公开招投标文件

• 金融行业——项目分析

2021年9月，长沙农村商业银行业发布DLP数据安全管控平台采购的公告，采购内容包括①终端DLP、②网络DLP、③邮件DLP、④统一后台管理平台、⑤配套数据分类分级咨询服务。主要实现对可能的数据泄密通道进行严密的检查和控制，对行内数据的创建、存储、使用、传输和销毁进行全生命周期的安全管理，能及时发现并阻断用户由于或无意的数据泄露行为，杜绝因数据泄漏引起的信息安全事件的发生。

2021年10月份，大连银行也发布了关于终端数据防泄密平台软件采购的公告，预算金额150万元。

长沙农村商业银行股份有限公司DLP数据安全管控平台采购项目招标公告

发布日期：2021-09-26

长沙农村商业银行股份有限公司（以下简称"招标人"）现就DLP数据安全管控平台采购项目进行招标，公开征集符合条件的投标人，欢迎符合资格条件并对此有兴趣的投标人前来报名参与投标。

一、项目概况

1.招标人：长沙农村商业银行股份有限公司。

2.项目名称：长沙农村商业银行DLP数据安全管控平台采购项目。

3.采购内容：长沙农村商业银行DLP数据安全管控平台采购项目，采购内容包括①终端DLP、②**网络**DLP、③**邮件**DLP、④统一后台管理平台、⑤配套数据分类分级咨询服务。主要实现对可能的数据泄密通道进行严密的检查和控制，对招标人行内数据的创建、存储、使用、传输和销毁进行全生命周期的安全管理，能及时发现并阻断用户有意或无意的数据泄露行为，保护招标人数据安全，杜绝因数据泄露引起的信息安全事件的发生；主要模块**功能包括但不限于**①内容识别；②水印管控；③U盘管控；④主动扫描；⑤外发数据需加上数字指纹或数字水印；⑥文档加解密及权限控制管控；⑦事后溯源；⑧审计管控；⑨终端文件扫描控制；⑩文件分类分级支持自动和手工等。拟通过公开招标，择优选取1家中标单位提供产品和服务，服务期限暂定伍年（具体内容与期限等以合同签订为准，招标人有权根据实际情况进行调整）。

（1）具体内容与期限等以合同签订为准，招标人有权根据实际情况进行调整。

（2）产品主要技术指标和要求详见附表《长沙农村商业银行DLP数据安全管控平台采购项目功能需求》。其中要求①硬件原厂免费质保和软件升级服务（闪盘或硬盘不返还）**不少于**5年、②软件原厂免费技术支持和软件升级服务不少于5年。

大连银行终端数据防泄密平台软件采购项目公开招标公告

2021年10月28日 16:46 来源：中国政府采购网 【打印】 【显示公告概要】

项目概况

大连银行终端数据防泄密平台软件采购项目 招标项目的潜在投标人应在大连汇金招标代理有限公司（大连市沙河口区星海广场9A区星海大观B座304室）获取招标文件，并于2021年11月18日 13点30分（北京时间）前递交投标文件。

一、项目基本情况

项目编号：HJZB2021-0100

项目名称：大连银行终端数据防泄密平台软件采购项目

预算金额：150.0000000 万元（人民币）

最高限价（如有）：150.0000000 万元（人民币）

采购需求：

大连银行终端数据防泄密平台软件采购

资料来源： 市场公开招投标文件

• 金融行业——项目分析

2022年6月，国信证券发布数据安全治理项目，项目预算260万：

项目背景	采购范围
数字化时代，数据已成为数字经济发展的核心生产要素，数据安全也成为事关国家安全与经济社会发展的重大问题。2021年以来，数据安全相关法律法规相继发布实施，《数据安全法》提出要“提升国家数据安全保障能力”，《个人信息保护法》提出“加速个人信息法制化进程”，数据安全进入“强监管”时代。 为落实数据安全保护和个人信息保护义务，保证数据在业务中的合规性使用及流转，提升数据价值以及满足监管要求，现计划开展数据安全治理项目，建设数据安全治理体系，开展数据安全制度建设、数据资产盘点、数据分类分级及安全风险评估活动。	本次数据安全治理项目包含5大服务项，分别是制度优化、资产盘点、数据安全风险评估、数据安全运营平台建设、数据安全培训宣贯，

资料来源： 市场公开招投标文件

医疗卫生行业需求分析

• 医疗卫生行业——规范标准有待进一步完善

伴随医疗卫生数据应用、“互联网+医疗健康”和智慧医疗的蓬勃发展，各种新业务、新应用不断出现，安全问题频发，医疗卫生数据在全生命周期各阶段均面临着越来越多的安全挑战，卫健委和医保局相继出台数据安全相关指南和管理办法，要求出台相应规范制度。

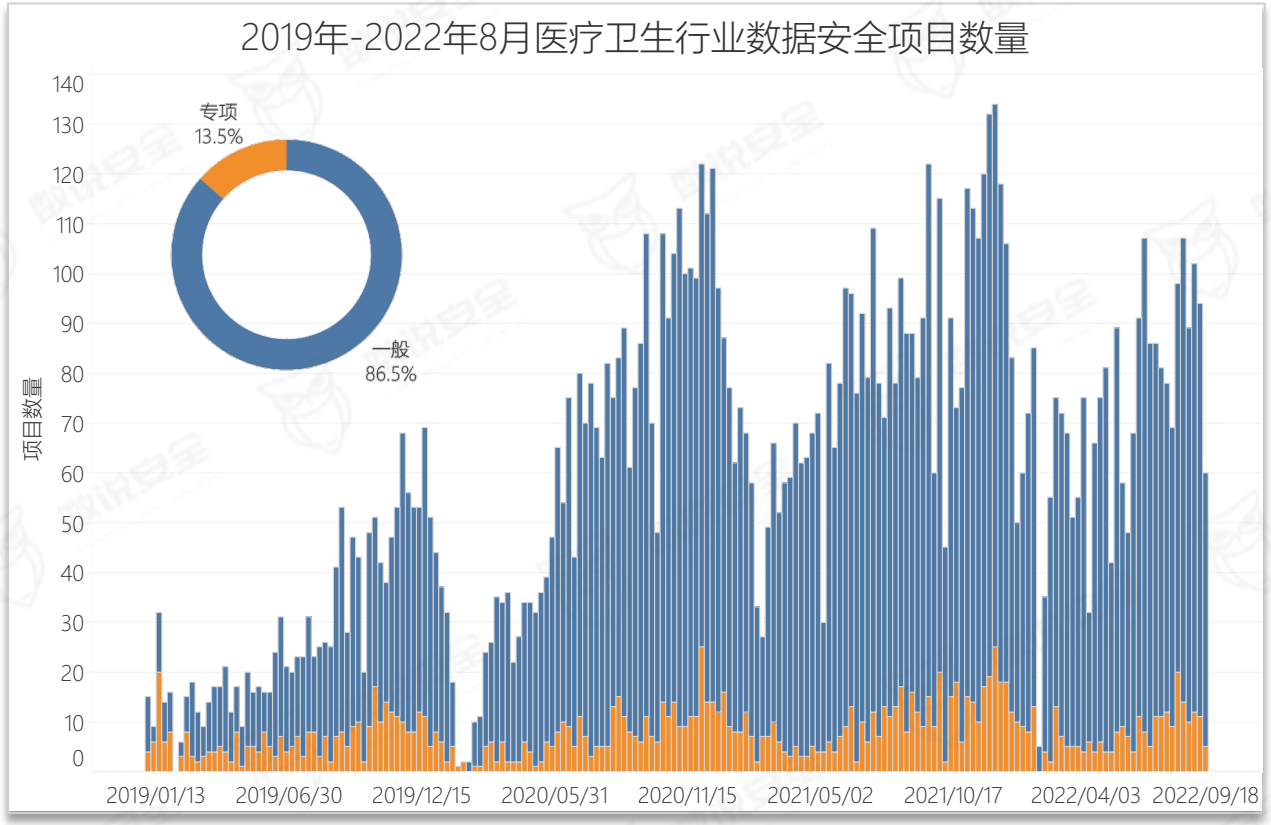
目前，医疗保障局和医院体系相关的数据安全规范标准仍不完善，如医疗行业的《数据生命周期安全规范》、《数据安全分级规范》、《数据安全评估规范》等仍未颁布，监管单位正在加紧研究制定。

时间	发布单位	文件名称	重要内容
2018年9月	卫健委	《国家健康医疗大数据标准、安全和服务管理办法（试行）》	明确建立健全健康医疗大数据安全管理人才培养机制，建立健康医疗大数据安全监测和预警系统，开展数据安全规范和技术规范的研究工作，建立数据安全管理、个人隐私保护、应急响应管理等方面管理制度等
2019年3月	卫健委	《关于落实卫生健康行业网络信息与数据安全责任的通知》	给进一步明确和落实网络信息与数据安全责任，建立健全网络信息与数据安全工作领导责任制。
2019年4月	卫健委	《关于印发全国基层医疗卫生机构信息化建设标准与规范》	规范了基层医疗卫生机构信息化建设的主要应用内容和建设要求，明确数据防泄漏、数据备份与恢复等具体内容和要求。
2020年9月	卫健委	《关于加强全民健康信息标准化体系建设的意见》	强化数据安全标准研制。围绕大数据应用和数据联通共享的安全需求，从个人信息安全、重要数据安全、跨境数据安全三个方面，研究编制数据分类分级、数据脱敏、去标识化、数据跨境、风险评估等标准。
2021年4月	医保局	《关于加强网络安全和数据保护工作的指导意见》	要求加强数据安全保护，实施数据全生命周期安全管理，实施分级分类管理，加强重要数据和敏感字段保护，强化数据安全审批管理，落实数据安全权限，推动数据安全共享和使用，建立健全数据安全风险评估机制等。
2021年	医保局	《国家医疗保障局数据安全管理办法》	要求各级医保部门进一步做好医保数据分级分类管理和应用安全管理，逐步建立规范、高效、安全的数据交换和信息共享机制。
2021年7月	国家市场监督管理总局	《信息安全技术健康医疗数据安全指南》	给出了健康医疗数据控制者在保护健康医疗数据时可采取的安全措施 。

• 医疗卫生行业——医疗保障局数据安全建设先行

2009年我国医院体系开始全面铺开信息化建设，从医院管理信息化（HIS）建设，到当下以电子病历信息化为重点的医院临床医疗管理信息化（EMR）阶段，信息化能力有了巨大的进展，但医院的信息和数据相对独立和封闭；伴随着2018年5月医保局的成立，及医联体医共体的建设，医院的数据在各科室、各级医院及医保局之间路径的打通，医疗数据泄漏问题频发，并成为勒索事件的重灾区，原有的数据安全体系已无法应对业务的需求，需要建立完整数据安全防护体系。

根据数说安全统计，医疗卫生行业2021年数据安全采购项目数量3700个，同比增长28.5%，其中专项项目数量469个，同比增长29%。结合项目内容分析，医疗行业的数据安全建设相对滞后，绝大部分医院仍然以满足等保为主要采购驱动力，采购单项的数据安全防护产品，规范标准的尚未完善及没有示范案例或是导致数据安全建设迟缓的主要原因；目前，已经有个别省市医保局开始数据安全治理类项目建设，伴随后续规范制度的逐渐出台，有望为行业建立良好的示范。



• 医疗卫生行业——XX省“智慧医保” 数据安全服务（一）

数说安全

2021年11月， xx省医保局发布《XX省“智慧医保”安全运维及系统数据安全服务项目招标文件》，预算金额2550万。

项目背景：

xx省医疗保障局高度重视医疗保障信息化安全建设，依照国家医疗保障局（以下简称国家局）《关于医疗保障信息化工作的指导意见》（医保发（20 19）1 号）、《国家医疗保障局关于加强网络安全和数据保护工作的指导意见》（医保发（2021）23 号）、《地方医疗保障信息平台验收指南》（医保网信办（2021）13 号）、《 地方医疗保障信息平台实施指引手册 》（2020 年 11月）等具体要求，“智慧医保”安全运维及系统数据安全工作应采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏，坚持技术和管理并重，保护和震慑并举，着眼于识别、防护、检测、预警、响应、处置等环节，从管理、技术、人才等方面加大投入，结合我省“智慧医保”软件开发项日数据安全现状和未来规划要求，开展全面建设。

主要依据	
《中华人民共和国网络安全法》	《浙江省公共数据和电子政务管理办法》省政府令第 354 号
《中华人民共和国数据安全法》	XJ-G02.1-2020《医疗保障信息平台身份认证与授权管理第1部分：系统建设规范V1.0》
《中华人民共和国个人信息保护法》	XJ-G02.4-2020《医疗保障信息平台身份认证与授权管理第4部分：安全应用接日规范V1.0》
《中华人民共和国密码法》	XJ-G02.1-2020《医疗保障信息平台身份认证与授权管理第6部分：系统建设指南V1.0》
《信息系统安全等级保护基本要求》	《国家医疗保障局关于印发全国医疗保障经办政务服务事项清单的通知》（医保发（2020）18 号）
XJ-AQWL.01-2019《医疗保障核心业务区网络安全接入规范》	国家医保局网络安全和信息化领导小组办公室关于印发《医疗保障信息平台建设指南 》的通知（医保网信办（2019）4 号）
XJ-A01-2019《医疗保障信息平台云计算平台规范》	国家医保局网络安全和信息化领导小组办公室关于印发《医疗保障信息平台云计算平台规范》等三部标准的通知（医保网信办 （2019） 5 号）
GM/T0054一2018《信息系统密码应用基木要求》	《国家医保局办公室关于进一步做好医疗保障信息平台建设有关工作的通知》（医保办发（2021）10 号）
《浙江省公共数据开放与安全管理暂行办法》省政府令第 381 号	《国家医疗保障局关于加强网络安全和数据保护工作的指导意见》（医保发（2021）23 号）

资料来源： 市场公开招投标文件

• 医疗卫生行业——XX省“智慧医保” 数据安全服务（二）

数说安全

总体目标

以“智慧医保”系统数据安全保障为业务目标，全面实现一体化安全保障体系。打造基础强、技术优、制度全、责任明、管理严的医疗保障网络信息安个和数据安全保护工作机制，通过完善的安全制度体系建设、强大的安全运维服务、专业的安全人才团队建设，全面服务浙江省“智慧医保”工程，有效支撑全省医疗数字化改革全周期。

分项目标

构建纵横防御数据安全架构体系	建立完整可靠数据安全防控体系	建设适度的保密信息的安全防控机制	建立全面完整的数据安全防控体系	构建一体化运维防控保障体系
引入国际先进技术体系、管理标准、以IS027001、等保三级为建设基准，打造立体、纵深、可追溯的数据安全防控系统，充分发挥和凝练经验积累，形成安全、合规、全面、稳定、高效的数据安全架构，夯实数据安全基础。	引进国际领先的零信任、DFI，DPI 等技术体系，在现有安全能力的基础下，引入增量安全技术服务，形成全面完全的异常流量、入侵检测、系统漏洞等全面的预警防控态势，有效解决每天海量入侵检测日志看不了、不会看的问题；全面提高风险评估、风险排查，以及安全事件，特别是 APT 等未知类型的网络攻击溯源等。	适当采用敏感数据脱敏、接口动态防护、电子水印保护等基本手段，建立可以灵活地根据特定时间、敏感数据、特殊群体、重点终端进行管理的信息安全态势感知和安全事件追踪溯源系统，形成“进不来、出不去、改不了、赖不掉、查得到”的信息安全体系；解决可以根据重点人员、特殊终端、敏感时期、应用系统等，提供按需分配的信息安全追踪溯源手段和技术，解决传统的信息安全保护技术受制于网络和组织架构、受制于终端和人员数量、受制于应用系统的变化等一列问题。	以“智慧医保”数据安全为基线，以数据采集、暗数据发现、数据资产分类分级、数据库防护技术为基础，有效防范数据全生命周期各阶段安全风险。	集成所有安全服务到统一的安全运维管理中心，并纳入到“智慧医保”一体化运维平台实现统一管理。确保数据安全运维工作既能与软件综合运维形成有机整体，又能稳定可靠、独立运行。

• 医疗卫生行业——XX省“智慧医保” 数据安全服务（三）

数说安全

总体框架：以“两不（不出事、不违规）三化（一体化、智能化、服务化）”为技术框架，遵循统一资产、统一策略、统一防护、统一运营，打造“智慧医保”坚实的数据安全底座，保障业务坚实稳步推进。整体技术框架包含三大技术体系，两大基础建设。

数据安全管理制度体系

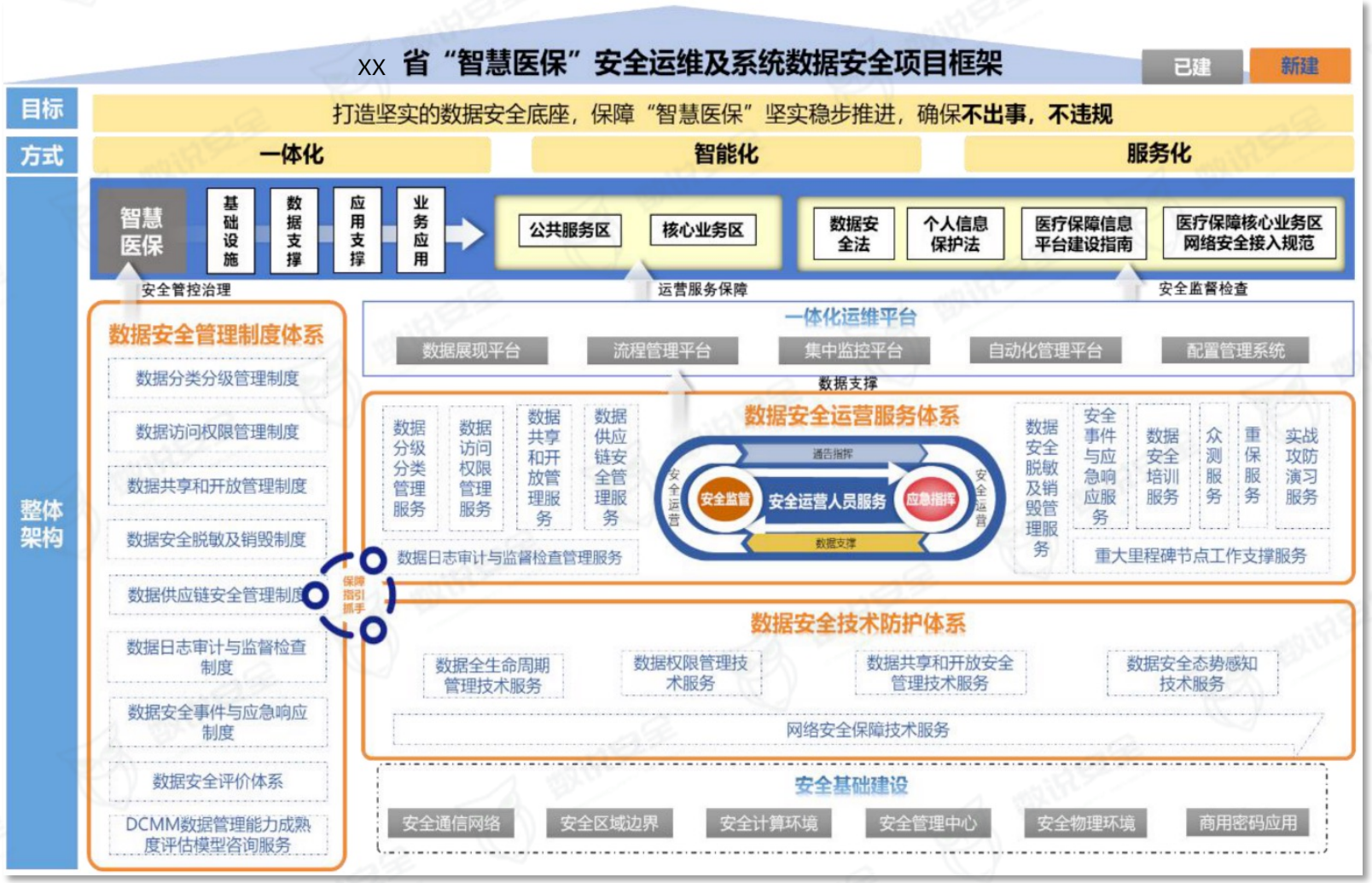
建立健全“智慧医保”数据安全制度规范体系，制定完善数据分类分级、访问权限、共享开放、脱敏销毁、供应链安全、口志审计、监督检查、安全事件应急处置等标准规范，促进数据安全管理工作标准化、流程化、规范化，使数据安全管理各项工作有规可依，形成“智慧医保”有效的安全管控治理能力。

数据安全技术防护体系

以“智慧医保”数据分类分级为基础，明确数据全生命周期各环节的安全防护要求。通过态势感知、权限管控、数据脱敏、高危操作阻断、数据水印溯源、口志审计等安全技术手段，加强数据安全常态化监测和智能风险预警，全而提升数据安全防护，筑牢数据安全防线。

数据安全运营服务体系

结合数据安全管理制度体系要求，充分利用数据安全防护技术工具，完善数据安全风险识别、安全防御、安全检测、安全响应和安全恢复管理手段，提升数据安全运行保障，建立事前管审批、事中全留痕、事后可追溯的全链路数据安全监管机制，及时发现处置各类数据安全风险，切实防范数据篡改、泄漏、滥用。



资料来源： 市场公开招投标文件

• 医疗卫生行业——XX省“智慧医保” 数据安全服务（四）

数说安全

- 数据安全运营服务
  - 数据分类分级运营服务
  - 日志审计和监督检查管理服务
    - 安全日志审计服务
    - 监督检查服务
      - 漏洞扫描
      - 渗透测试
      - 基线核查
      - 代码审计
      - 数据安全评估
  - 重保服务
  - 安全事件与应急响应服务
  - 实战攻防演习服务
  - 数据共享和开放管理服务
  - 数据访问权限管理服务
  - 供应链安全管理服务
  - 数据安全培训服务
  - 数据安全脱敏及销毁管理服务
  - 众测服务
- 数据安全制度规范体系
  - 智慧医保数据分类分级管理制度
  - 智慧医保数据访问权限管理制度
  - 智慧医保数据共享和开放管理制度
  - 智慧医保数据安全脱敏及销毁管理制度
  - 智慧医保数据供应链安全管理制度
  - 智慧医保安全日志审计和数据安全监督检查制度
  - 智慧医保数据安全与应急响应制度
  - 智慧医保数据安全评价体系
  - 数据管理能力成熟度评估模型
- 数据安全技术防护服务
  - 数据全生命周期管理技术服务
    - 数据采集技术服务
      - 网络日志转换分析服务
      - 数据库安全日志转换分析服务
      - 云上横向流量采集技术服务
      - 脆弱性探测数据采集技术服务
    - 暗数据分析技术服务
    - 数据源鉴别技术服务
    - 数据分类分级及标记技术服务
    - 数据防泄漏技术服务
    - 数据库攻击防护技术服务
  - 网络安全保障技术服务
    - 高级危险监测服务
    - 主动防御服务
    - 未知漏洞攻击防御服务
    - 供应链安全分析服务
    - 漏洞管理服务
  - 数据共享和开放安全管理服务
    - 重要数据和敏感字段保护服务
    - 数据接口动态防护服务
    - 数据水印溯源技术服务
  - 数据权限管理技术服务
    - 特权账号管理服务
    - 业务访问权限动态管控服务
    - 数据使用异常行为分析服务
  - 数据安全态势感知技术服务
    - 集中数据安全管控技术服务
      - 数据安全总体态势感知服务
      - 敏感数据安全态势感知服务
      - 数据流转安全态势感知服务
    - 数据安全风险监测预警技术服务
      - 敏感数据流转检测预警服务
      - 人员操作行为检测预警服务
      - 数据接口调用检测预警服务
      - 一体化运维平台对接开发服务

资料来源： 市场公开招投标文件

• 医疗卫生行业——浙大二附院数据融合与隐私计算平台（一）

数说安全

2021年8月16日浙江大学医学院附属第二医院发布数据融合与隐私计算平台及应用招标项目，项目金额300万。

建设背景

2019年9月19日，国家卫生健康委与浙江省签署国家区域医疗中心省委共建协议。其中，我院将牵头“国家心血管病区域医疗中心”建设。

为深化医疗服务领域供给侧结构性改革，调整优质医疗卫生资源布局，提升区域医疗技术、科研和管理层次，助力浙江省生命健康医学高地和科创高峰的建设，“国家心血管病区域医疗中心”必须能够胜任各类型、各程度、各人群的心血管病救治任务及相关公共事件应急救援/保障服务；建成覆盖全区域的三级诊疗体系、远程会诊和立体转诊体系、专病数据库和质控体系、临床研究和转化平台、预防体系、教学培训体系、人才队伍建设体系；实现区域内医疗能力整体大幅提升至国内领先、世界先进水平，成为国际医疗体系建设的典范，临床科研水平处于世界先进水平，区域影响力大幅提升。

为保障区域医疗中心建设任务的有序推进，抓住历史性发展机遇，我院亟须构建能够支撑区域医疗中心协同单位的分级诊疗、远程会诊/辅助诊断、立体转诊，专病数据库、质控体系和疾病预防，临床研究和转化，人才教育培训和队伍建设等工作的“全方位、数字化、规模化”全域协同网络，利用区块链、联邦学习技术打造“数据融合与隐私计算平台”。为“国家心血管病区域医疗中心”提供新型数据融合基础设施。

建设内容：

软件系统：数据融合与隐私计算平台及应用项目

数据融合与隐私计算平台由健康联盟链、联邦学习框架、数据资产价值评估框架、人工智能算法库、统计分析算法库、开放服务管控模块组成，前端由数据融合与隐私计算平台管理端为中心管理节点提供数据融合与隐私计算平台管理功能，由医院管理端为链上医院提供医院管理功能。

维保服务

1．为本项目提供自完成整体验收之日起为期1年的免费维保服务。

2．本项目应用范围包括浙大二院解放路院区、滨江院区、眼科院区、江干院区、浙大院区等一体化管理院区

• 医疗卫生行业——浙大二附院数据融合与隐私计算平台（二）

建设需求如表中所示：

功能		描述
健康联盟链	智能合约管理	对智能合约进行管理功能
	数据提交管理模块	对数据上链进行操作，可快速、批量上传数据。
	共识管理模块	包括共识节点的添加与删除，共识节点状态查看等功能。
	出块和上链管理模块	对区块链生成区块的配置参数进行管理。
	链上数据账本管理	包括数据筛选，状态查询等，为数据账本查询提供入口。
	客户端上链和查询管理模块	对健康联盟链节点进行添加成员、发放证书，并可对上链数据内容进行查询。
	链上组织、用户管理模块	对链上组织和用户进行管理。
	业务通道管理	业务通道创建，业务通道详情，业务配置等。
	CA节点服务管理	提供认证服务，保障健康联盟链的安全。
	区块链数据浏览器	包括链码查看、区块信息查看、区块数据检索等功能。
	区块链监控系统	可查看各节点cpu、内存、存储等资源的使用情况。
	证明资料	提供医疗区块链平台软件软著作权证明
数据资产价值评估框架	维度管理	对数据资产维度、权重、等级、系数等进行管理与设置
	度量衡定义	定义数据价值的度量衡标准
	评估模型管理	数据评估模型参数的维护、计算公式的维护等。
	数据价值计算	根据设定的评估模型计算数据的价值。

功能		描述
联邦学习	分布式计算引擎	支持多机通信、计算资源调度、计算任务提交和执行等功能。
	分布式存储引擎	用于管理涉及到文件存储。
	联邦建模流程	包括数据选择、数据清洗、算法选择、模型结构设计、模型超参数设置等功能。
	网络代理模块	作为跨网络系统的信息交换过程的中间代理机构。
	推理服务模块	使用在线的机器学习或深度学习模型进行计算、预测等。
	服务代理模块	提供各类联邦学习服务的代理功能。
	服务协调模块	提供服务代理模块的各类服务的协调与协作功能。
	任务仪表盘	联邦学习任务相关的信息的可视化功能。
	证明资料	提供联邦学习平台软件软著作权证明
分布式人工智能算法库	支持同构泊松回归、同构多层感知器、同构逻辑回归、异构逻辑回归、同构多元线性回归等5种人工智能算法，同时支持自定义算法模型	
分布式统计分析算法库	支持均值、最大值/最小值、中位数、频数、众数、方差/标准差、协方差、偏度、峰度、极差/中程数、四分位距、皮尔森相关系数等12种算法进行分布式统计分析	

资料来源： 市场公开招投标文件

• 医疗卫生行业——浙大二附院数据融合与隐私计算平台（三）

数说安全

数据融合与隐私计算平台管理端	数据字典	对平台数据字典的维护
	算法管理	对平台上算法的增加、修改、删除等功能。
	规范化管理	对平台的字段进行规范化管理。
	联盟链管理	对医院在健康联盟链上的节点信息进行统一管理。
	联邦学习节点管理	对医院在联邦学习框架上的节点信息进行统一管理与查看。
	医院管理模块	对医院的基本信息进行管理。
	平台运行状态分析模块	对平台运行状态进行不同维度的统计分析。
	链上数据管理模块	集中统计及展示多家医院在对应链上的数据数量、积分等信息。
	数据资产价值评估模型配置模块	进行数据资产价值评估模型配置管理的模块。
	证明资料	提供数据融合与隐私计算平台软件软著作权证明
医院管理端	数据上链模块	对医院端的数据进行上链。
	医院客户端运营统计分析模块	以用户角度对现有数据进行不同维度的统计分析，并可视化展现。
	可信存储区管理模块	包含可信存储的新增、删除、查询、编辑、测试链接等功能。
	联盟链管理模块	对医院联盟链节点进行管理
	联邦节点管理模块	对医院联邦学习节点进行管理
	服务网关	实现数据从医院数据中心到可信存储库的数据抽取、清洗以及数据的标准化转化处理。
	安全开放管理模块	对开放数据访问权限的配置管理、数据交互过程全程的可视化监管，保障数据的安全。
分布式多中心科研平台	科研项目管理模块	包括项目创建、项目信息的编辑与完善、项目CRF表单的配置、项目删除、项目查询等。
	CRF模板定义管理模块	实现CRF表单的可视化定义。

分布式多中心科研平台	研究对象信息录入模块	包括患者数据采集、添加、修改、提交、查看、导出等。
	数据字典	数据字典的维护。
	随访管理	对患者进行定期随访。
	标准化管理模块	主要包括字典标准化管理和立项标准管理。
	项目人工智能管理	包含项目人工智能训练列表、人工智能模型预测列表，项目信息查看及删除、模型预测的功能。
	模型训练发起模块	发起多种人工智能模型训练的模块。
	统计分析发起模块	发起多种统计分析的模块。
	统计分析管理模块	为统计分析结果提供可视化的前端展示页面。
	审批管理	包含立项管理、伦理管理。
	系统管理	对用户、角色的权限进行分配管理的功能。
	日志管理	系统相关日志的记录和展示。
国家心血管病数据上报及区块链溯源系统	基础数据库维护模块	为直报提供基础的数据支撑。
	直报接口维护模块	维护不同直报系统接口及参数的配置。
	直报数据源维护模块	对不同直报系统所需数据进行筛选、配置。
	直报接口与数据源映射维护	维护接口与数据源之间的对应关系，保证数据的正确性。
	数据补录模块	提供补录或修改功能。
	数据一键上报模块	实现数据一键上报功能。
	数据统计分析模块	按病例状态、病种、科室、日期范围统计病例数据，并以表格和图形的方式展示，同时支持报表导出。
	数据导出模块	数据导出模块可将数据导出为excel、pdf等文件。
	系统管理模块	对系统用户、数据同步时间、直报时间、区块链等进行相关的设置。
	区块链溯源模块	对上报数据的索引哈希值上链，保证数据隐私，并记录了数据源及上报时间等信息，确保原始数据可溯源并不可篡改，提高质控水平。

• 医疗卫生行业—广东省医保局数据安全项目（一）

数说安全

2022年2月，广东省医疗保障局发布了《省医保局医疗保障信息平台数据安全软件租赁及运营（2022-2024年）的采购项目》文件，项目预算金额2045万元。

项目总体目标：

到2022年，基本建成基础强、技术优、制度全、责任明、管理严的医疗保障网络安全和数据安全保护工作机制。到“十四五”期末，我省医疗保障系统网络安全和数据安全保护制度体系更加健全，智慧医保和安全医保建设达到新水平。

本次项目目标是按照《国家医疗保障局关于印发加强网络安全和数据保护工作指导意见的通知》（医保发〔2021〕23号）的要求，结合我省实际，进一步加强我省医疗保障数据安全保护建设。

通过加强我省医疗保障数据安全保护建设，实现如下目标：①、对医疗保障数据实施数据全生命周期安全管理。②、实施分级分类管理。③、加强医保重要数据和敏感字段保护。④、强化广东省医保数据安全审批留痕。⑤、落实广东省医保数据安全权限。⑥、推动数据安全共享和使用。⑦、建立健全数据安全风险评估机制。

项目背景

医疗保障信息化是医疗保障事业高质量发展的基础，是医保治理体系和治理能力现代化的重要支撑。广东省医疗保障局全面落实党中央关于网络安全工作的总体部署，扎实推进医疗保障信息平台建设，防范化解医保系统数据安全风险、促进数据开发利用，加强医疗保障网络安全和数据保护工作。

为支撑实现人民群众对美好生活向往的目标，确保医疗保障制度运行公平、提高医疗保障持续供给能力、推进医疗保障责权分担合理、提升医疗保障公共服务水平，通过不断规范、创新和完善医疗保障制度体系、政策机制、管理模式、业务流程、服务手段、标准规范，进一步建立健全全省医疗保障信息化体系。遵循国家医疗保障局信息化建设顶层设计，探索建立全省一体化医疗保障信息平台，形成“标准全区统一、数据区级集中、平台区级部署、网络全面覆盖”的医疗保障信息化体系。综合运用“互联网+”、大数据等现代思维和先进技术，采用“标准+平台+应用”的建设策略，全面开展集中式、一体化医保信息化建设，形成线上线下融合、服务衔接有序、规范安全高效的全区“互联网 + 医疗保障服务”新格局，实现全省医保业务经办一体化、公共服务人本化、监督管理智能化、决策依据大数据化、服务能力开放化、安全保障全息化，为新时期满足人民群众日益增长的医疗保障需求提供强有力的信息化支撑，实现医疗保障治理体系和治理能力现代化。

• 医疗卫生行业——广东省医保局数据安全项目（二）

数说安全

政策与法规：

《国家医疗保障局关于印发加强网络安全和数据保护工作指导意见的通知》（医保发〔2021〕23号）

《关于印发<国家医疗保障局数据安全管理办法>的通知》（医保网信办〔2021〕5号）

《国家医疗保障局印发<关于医疗保障信息化工作的指导意见>的通知》（医保发〔2019〕1号）

《关于印发<医疗保障信息系统安全开发规范>的通知》（医保网信办〔2019〕1号）

标准与规划：

《医疗保障信息平台建设指南》

《医疗保障核心业务区网络安全接入规范》

《信息安全等级保护管理办法》公通字〔2007〕43

GB17859-1999《计算机信息系统安全保护等级划分准则》

GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

《信息系统等级保护安全设计技术要求》信安秘字〔2009〕059号

《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安〔2007〕861号）

《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安〔2009〕1429号）

GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》

GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》

• 医疗卫生行业——广东省医保局数据安全项目（三）

数说安全

1、成品软件租赁服务		
租赁服务	部署区域	功能描述
数据安全统一管理中心系统	主数据中心（核心业务区）1套	包括数据资产盘点、风险告警、动态监测、账号权限统一管理。
数据审计系统	主数据中心的核心区、公共区各1套，共2套	包括面向大数据访问行为全程审计和监控、安全事件审计追溯。
数据访问控制系统	主数据中心、灾备数据中心的核心区、公共区各1套，共4套	包括数据高权限管控、高危操作阻断、可疑行为审计。
数据加密系统	主数据中心（核心业务区）1套	针对医保信息平台生产节点数据中台相关的数据报表统计类加密，支持国密算法对敏感数据加密，提供独立于数据库的访问授权机制，提供三权分离管理。
数据静态脱敏系统	主数据中心（核心业务区、公共业务区各1套）共2套	包括开发、测试、数据共享和分发场景下的敏感数据的静态脱敏。
数据防泄漏系统	主数据中心、灾备数据中心的核心区、公共区各1套，共4套	包含数据防泄露安全管理、网络防泄露（网络DLP）、终端防泄露（终端DLP）。
应用安全审计系统	主数据中心、灾备数据中心的核心区、公共区各1套，共4套	提供医保应用(API)数据安全审计能力，识别接口调用的异常用户行为。

2、运行维护服务
本项目对所租赁的成品软件提供服务期限内3年运行维护服务（投标报价需包含相关费用），以确保系统稳定运行。

• 医疗卫生行业——广东省医保局数据安全项目（四）

数说安全

3、安全运营服务	
服务内容	具体要求
医保数据安全管理体系规划	主要根据《国家医疗保障局数据安全管理办法》中关于对组织架构与职责的分工，结合当前广东省政府和省医疗保障局的机构设置，提供省医疗保障局数据安全管理组织架构设计，数据安全管理标准规范类编制。
数据安全分级分类	包括提供数据分级分类工具部署和配置、数据安全分级分类方案设计、数据安全分级分类方案实施。
数据安全风险评估	包括医保数据安全风险评估准备、数据安全风险识别、数据安全风险分析和数据安全风险处置。
数据安全成熟度评估	包括数据安全成熟度评估调研和数据安全成熟度分析，出具分析评估报告。
数据安全策略规划服务	包括数据操作权限审批流程策略规划、敏感数据范围确定、数据安全权限策略规划、数据安全共享使用策略规划和应用接口安全策略规划等医保数据安全策略制定，以及相应数据安全防护规划。
数据安全宣贯	提供包括远程和集中方式的数据安全运营培训和数据安全意识宣贯。
安全驻场运营	提供数据安全防护运营服务、数据安全事件响应服务、数据安全常态化评估服务和数据安全其它运营支撑服务。
信息安全常态化运营服务	包括文档审阅、现场检查和顾问访谈等风险评估，根据漏扫情况对系统环境和应用程序进行漏洞加固，每年最少一次的医保信息平台渗透测试，以及对突发事件的数据安全应急响应和重大活动保障数据安全。

数据安全供给分析

1 • 数据安全厂商全景图

2 • 隐私计算技术发展情况

3 • 厂商热度分布

4 • 厂商行业分布

5 • 解决方案展示

数据安全厂商全景图

数说安全

数据安全服务

思维世纪 · DBSEC 安华金和 · 美创 MEICHUANG · 观安 · NSFOCUS · 中安星云 Interstellar Security · 奇安信 · 启明星辰 · 天融信 TOPSEC · 全知科技 QUAN ZHI TECH · 数安行 DataSecOps · 安恒信息 DAS-security · 天空卫士 SkyGuard · 昂楷科技 ANKKI · 闪捷信息 SECSMART · 中安威士 VISUAL SEC · 云集至 · 鸿数科技 HONGSHU TECHNOLOGY · AOTAIN 傲天科技

数据采集安全

数据分类分级：美创 MEICHUANG · DBSEC 安华金和 · 思维世纪 · 观安 · 安恒信息 DAS-security · NSFOCUS · 奇安信 · 闪捷信息 SECSMART · 世平信息 SPINFO · 天空卫士 SkyGuard · 中安星云 Interstellar Security · AOTAIN 傲天科技 · 天融信 TOPSEC · 启明星辰

数字签名：数字认证 · KOAL · 吉大正元 · 深圳CA · 诚天信威 iTrusChina · 信大捷安 · 信安世纪 infosec · sansec 三未信安 · 亚洲诚信 TRUSTASIA

数据访问控制

PAM：齐治科技 · union 江南科友 · 派拉软件 PARAVIEW SOFTWARE · 海颐安全 HAIYI SECURITY · PIDSEC 帕拉迪 · KOAL · 尚思卓越 SHANGSIZHUOYUE · 奇安信 · 腾讯云 · edvance 安领科技 · ANYDEF

零信任：持安科技 · 数篷科技 DATACLOAK · 易安联 Enlink cloud · 数安行 DataSecOps · 蔷薇灵动 Dyarose · 虎符网络 · 雪诺科技 SNOW TECH · 腾讯安全 · 安几网安 ANGeek C.S. · 云深互联 CloudDeep Technology · 奇安信 · SANGFOR 深信服科技

数据传输安全

密码技术：数字认证 · Westone 卫士通 · sansec 三未信安 · 吉大正元 · KOAL · 江南信安 · TASS 江南天安 · fisec 渔翁 · union 江南科友 · DONJIN 东进技术 · 数盾科技 SHUDUN TECHNOLOGY · 炼石 CipherGateway · 中海闻达 ZHONG HAI WEN DA · OLYM 奥联 · 得安 · GO TECH 国泰网信

VPN：SANGFOR 深信服科技 · 奇安信 · Westone 卫士通 · DP tech 杭州迪普科技有限公司 · 启明星辰 · 天融信 TOPSEC · 江南信安 · fisec 渔翁

DLP：天空卫士 SkyGuard · 世平信息 SPINFO · 联软科技 · 奇安信 · 明朝万达 Wondersoft · 美创 MEICHUANG · 亿赛通 ESAFENET · 启明星辰 · vamtoo 华途软件 · 闪捷信息 SECSMART · cirrus gate 思睿嘉得 · 数篷科技 DATACLOAK

云桌面：SANGFOR 深信服科技 · Ruijie 锐捷 · H3C · VESYSTEM 和信创天

RBI：钛星数安 TISTARSEC · 安胜 · yytek 云涌科技 · 航斗腾云 SupraAXES

数据存储安全

电子文档管理与加密：亿赛通 ESAFENET · 前沿信安 Frontier InfoTech · vamtoo 华途软件 · 明朝万达 Wondersoft · 敬捷科技 agile technology · IP-guard · 七洲科技 · 北信源 VRV

数据库加密：美创 MEICHUANG · DBSEC 安华金和 · 闪捷信息 SECSMART · DP tech 杭州迪普科技有限公司 · 中安威士 VISUAL SEC · 云集至 · 安恒信息 · H3C · 启明星辰 · 昂楷科技 ANKKI · 中安星云 Interstellar Security · 360数字安全 · 炼石 CipherGateway · 世融能量 SHRONG ENERGY

存储备份与恢复：SCUTECH 鼎甲科技 · dataSure 数腾软件 · AI SHU 爱数 · 雷因 MAKE DATA POWER · 瑞数信息 RIVER SECURITY · 美创 MEICHUANG · SUNINFO 上讯信息 · 柏科数据 Bring Life to Data

数据处理安全

数据脱敏：闪捷信息 SECSMART · DBSEC 安华金和 · 神州数码 Digital China · 美创 MEICHUANG · NSFOCUS · 中安星云 Interstellar Security · 观安 · 奇安信 · 世平信息 SPINFO · 启明星辰 · 安恒信息 DAS-security · 中电华瑞 · 昂楷科技 ANKKI · 明朝万达 Wondersoft · 全知科技 QUAN ZHI TECH

数据库安全：美创 MEICHUANG · DBSEC 安华金和 · 中安星云 Interstellar Security · 安恒信息 DAS-security · 观安 · 闪捷信息 SECSMART · 海峡信息 · NSFOCUS · 昂楷科技 ANKKI · 中安威士 VISUAL SEC · 启明星辰 · 云集至 · 奇安信 · 亿赛通 ESAFENET · UXSINO 优炫软件 · 世平信息 SPINFO · 天融信 TOPSEC · Hillstone 山石网科 · H3C · 中信网安

个人隐私保护：红途科技 · 数安行 DataSecOps · 百度安全 · 海云安 secidea · 奇安信 · 指掌易 · 郴州安全 BANGCLE · 爱加密

数据交换安全

隐私计算：华控清交 HUA KONG TSINGJIAO · BaseBit.ai 翼方健数 · 洞见科技 INSIGHTONE · 数牍 sudo · DBSEC 安华金和 · 百度安全 · 富数 FUDATA.CN · 冲量在线 IMPULSEONLINE · 锘崴科技 NVXCLOUDS TECH · 医渡云 YIDUCLOUD · 腾讯安全 · 蚂蚁集团 ANT GROUP

API安全：金知科技 QUAN ZHI TECH · 星阑科技 · DBSEC 安华金和 · 红途科技 · 永安在线 EVER.SECURITY · 瑞数信息 RIVER SECURITY · 奇安信 · 赛沃安全 SERVICEWALL · 数猫科技 CYBERSERVAL · 从云科技

数据销毁安全

数据销毁：中超伟业 · 金盾保密 CASTLE SECURITY · 德佩安全 DEPEI SECURITY · TIPS鼎普 · 智恒网臣 ZHI HENG WANG CHEN · 中泾数据 · 航天润普 · 北信源 VRV · ELEX博智 · SUPER RED 方里红

数据安全治理平台

观安 · 美创 MEICHUANG · DBSEC 安华金和 · 思维世纪 · 中安星云 Interstellar Security · 世平信息 SPINFO · 天空卫士 SkyGuard · 奇安信 · NSFOCUS · 全知科技 QUAN ZHI TECH · 360数字安全 · 安恒信息 DAS-security · 天融信 TOPSEC · 闪捷信息 SECSMART · 启明星辰 · 昂楷科技 ANKKI · 数安行 DataSecOps · 数篷科技 DATACLOAK

• 数据安全技术简介

数说安全

数据采集安全	数据分类分级	数据分类主要从业务角度出发，明确数据的业务范畴；数据分级主要从安全和监管角度出发，明确数据的安全级别。通过规范标准对数据进行分类和分级打标，可以有效的确定数据在访问、使用、安全、隐私、质量等环节的优先级，以便于数据的使用和治理，对安全、隐私和数据治理的实施非常重要。 目前对于结构化数据的分类分级工作，通常借助自动化工具完成；但对于非结构化数据，如财务数据、生活参数据、图片、声音等则仍需要对用户进行培训，并借助机器学习和人工智能来提高效率。
	数字签名	是信息跟随数据生成的一段无法伪造的数字串，用于验证信息的真实性和完整性。一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。数字签名是非对称密钥加密技术与数字摘要技术的应用。
数据访问控制	PAM	是一套策略与技术的框架集合，用于控制、监视、保护和审核整个企业IT环境中所有特权身份和活动。主要涉及技术包括：身份识别与管理、统一认证（单点登录、密码认证、动态口令、证书认证，多因子认证）、特权管理、安全审计等。
	零信任	零信任是一种以“永不无条件信任，永远依据上下文验证身份”的思想为依托，要求尽可能多的收集信息，对人、设备、系统、被访问资源进行动态风险评估，从而给予用于或设备对资源访问的实时、动态访问授权的解决方案。 零信任的三大核心技术有软件定义边界（SDP），身份识别与管理（IAM），微隔离技术（MSG）,随着零信任思想的发展，范围也从身份识别与管理、授权管理、动态访问控制扩大至终端安全评估与防护技术、安全分析与决策技术、沙箱技术、自动化响应与编排能力、国密标准支持、第三方产品与服务集成能力等。
数据传输安全	密码技术	指对信息进行加密、分析、识别和确认以及对密钥进行管理的技术。在产品应用方面，主要包括：证书和密钥管理、签名验证、电子签章、数据加密、硬件加密、身份鉴别等相关产品；
	VPN	指虚拟专用网络，一般是在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。VPN通过对数据包的加密和数据包目标地址的转换实现远程访问，可通过服务器、硬件、软件等多种方式实现。
	DLP	指数据泄露防护产品，通过对运行、存储于主机内或者网络中传输的文件、数据进行内容识别，对数据的操作和传输过程进行监视和控制，实现对数据以非授权的形式流出安全域进行防护的功能，同时该类产品还应具有基本的身份鉴别、安全管理审计和报警功能。
	云桌面	指利用虚拟技术，对各种物理设备进行虚拟化处理，从而使资源的利用率得到有效提升。其本质是对各项用户信息进行统一储存和管理，通过简单的网络接入设备，用户端就能够进入云桌面实现集中管理，并且实现高效率的资源共享。
	RBI	指远程浏览器隔离技术，通常采用虚拟化或容器技术将用户的Web浏览活动与端点设备隔离，以此减少恶意链接和文件的攻击面。远程浏览器隔离将浏览活动从最终用户设备隔离到远程服务器，该服务器可以在公司内部部署（但不连接到公司的正规IT基础设施），也可以作为基于云服务交付。

• 数据安全技术发展情况

数说安全

数据存储安全	密码技术	数据库安全	指对信息进行加密、分析、识别和确认以及对密钥进行管理的技术。在产品应用方面，主要包括：证书和密钥管理、签名验证、电子签章、数据加密、硬件加密、身份鉴别等相关产品；
		数据库加密	指数据库加密产品，基于透明加密、主动防御等技术，能够实现对数据库中的敏感数据加密存储、访问控制增强、应用访问安全、安全审计以及三权分立等功能。有效防止明文存储引起的数据泄密、突破边界防护的外部攻击，从根本上解决数据库敏感数据泄漏问题。
		存储备份与恢复	指为防止系统出现操作失误或系统故障导致数据丢失，而将全部或部分数据集合从应用主机的硬盘或阵列复制到其他的存储介质中。当故障恢复后，重新启用信息系统的数据、硬件及软件设备，恢复正常商业运作的过程。
	电子文档管理与加密		指根据需要采取电子签名、数字加密、安全认证和权限管理等技术手段，保障电子文档安全，防止非授权访问及非法外泄的技术和产品。
数据处理安全	数据脱敏		指对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。通过数据脱敏产品，可以有效防止企业内部对隐私数据的滥用，防止隐私数据在未经脱敏的情况下从企业流出。
	数据库安全		此板块主要包括数据库防火墙和数据库审计两类产品。数据库防火墙是串联部署在数据库服务器之前，解决数据库应用侧和运维侧两方面的问题，是一款基于数据库协议分析与控制技术的数据库安全防护系统。数据库审计是以安全事件为中心，以全面审计和精确审计为基础，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行实时告警。
	个人隐私保护		指个人不愿意被外人知道的信息得到应有保护，其关注的主要问题是看系统是否提供了隐私信息的匿名化，通常可以从隐私性、数据准确性、延时和能量消耗这几个方面对隐私保护的性能进行评估。
数据交换安全	隐私计算		隐私计算是面向隐私信息全生命周期保护的计算理论和方法，包括但不限于密码学、访问控制、可信计算、机密计算、密文计算、安全多方计算、联邦学习等。
	API安全		解决应未授权用程序编程接口导致的安全等问题，主要通过API发现与管理、API风险监测、API入侵检测与防御等方式进行联动防护。
数据销毁安全	数据销毁		通过建立针对介质及数据内容的清除、净化机制，实现对数据的有效销毁，防止因对存储介质中的数据内容进行恶意恢复而导致的数据泄漏风险。需要结合数据分类分级建立数据销毁策略和管理制度，明确数据销毁的场景、销毁对象、销毁方式和销毁要求。
数据安全服务			通过前期咨询（业务需求、合规保障）、规划（组织架构、制度流程、安全策略、人员培训），中期建设，后期运营维护（风险监测、监测预警、应急响应）及持续评估，使数据安全体系能够动态的为客户提供数据安全保障。
数据安全治理平台			从数据分类分级开始，对各类数据安全工具、策略、风险及处置进行统一管理监控，实现制度、策略、人员、工具、服务之间的协同响应，统筹管理。

• 什么是隐私计算

隐私计算是近年来数据安全领域关注度最高的新技术， 是一种针对泛在互联环境下隐私信息共享的全生命周期隐私保护和管控的理论和方法。

在数据时代下，隐私计算既能满足将海量的数据的互联互通、共享利用，有效的释放数据的最大价值的要求，同时又能解决数据的在不同机构之间的流通带来的数据泄漏、篡改，非法利用等一系列的问题，保证数据以“可用不可见”的方式进行安全流通。

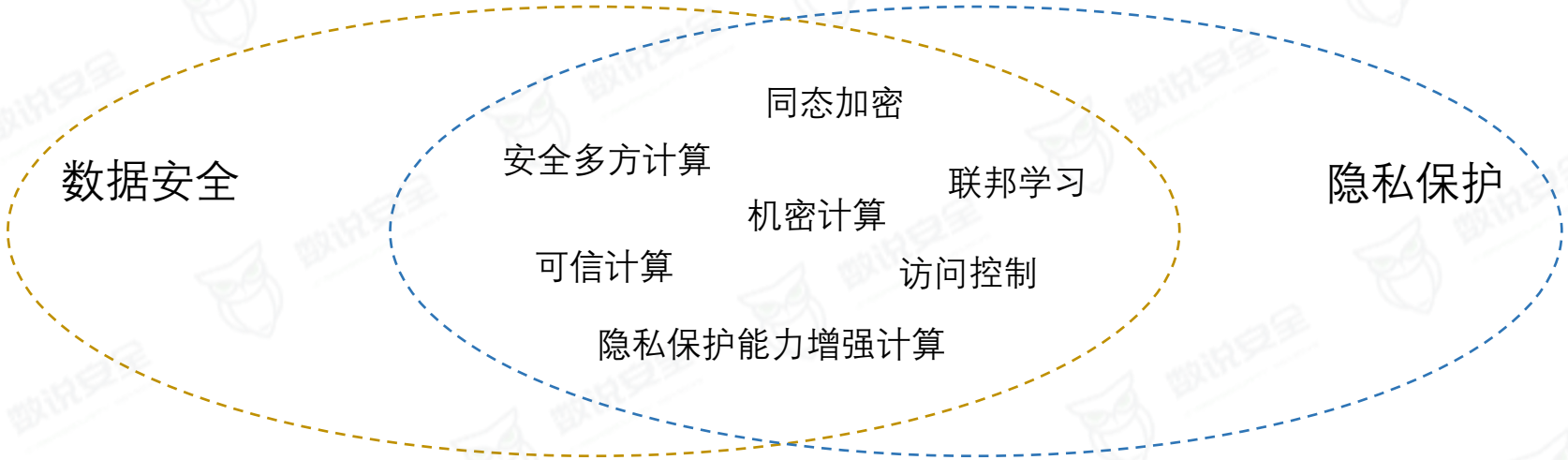
隐私计算的定义

隐私计算是面向隐私信息全生命周期保护的计算理论和方法，是隐私信息的所有权、管理权和使用权分离时隐私度量、隐私泄露代价、隐私保护与隐私分析复杂性的可计算模型与公理化系统。具体是指在处理视频、音频、图像、图形、文字、数值、泛在网络行为信息流等信息时，对所涉及的隐私信息进行描述、度量、评价和融合等操作，形成一套符号化、公式化且具有量化评价标准的隐私计算理论、算法及应用技术，支持多系统融合的隐私信息保护。隐私计算涵盖了信息搜集者、发布者和使用者在信息产生、感知、发布、传播、存储、处理、使用、销毁等全生命周期过程的所有计算操作，并包含支持海量用户、高并发、高效能隐私保护的系统设计理论与架构。隐私计算是泛在互联环境下隐私信息保护的重要理论基础。

资料来源：《隐私计算研究进展报告》

• 隐私计算主要技术介绍

隐私计算涉及领域较多，包括但不限于密码学、访问控制、可信计算、机密计算、密文计算、安全多方计算、联邦学习等。其中安全多方计算、同态加密、可信计算、密文计算、访问控制等技术是属于数据安全范畴，也可用于隐私防护，仅适用于特定知悉范围内没有信息损失的敏感信息保护。



密文计算：

是指计算过程中的数据不被计算参与方所获取，主要用于外包计算场景。同态加密是密文计算的代表性技术，是在事先确定转换规则的前提下，所有参与运算的明文数据使用该规则转换为密文，在密文空间中进行特定形式的代数运算并得到结果，密文运算的结果再通过相应的转换规则转换为明文。

• 隐私计算主要技术介绍

机密计算：

在受信任的硬件执行环境基础上构建安全区域，所有参与方将需要参与运算的明文数据加密传输至该安全区域内并完成运算，安全区域外部的任何非授权的用户和代码都无法获取或者篡改安全区域内的任何数据。机密计算过程中的元数据不被计算参与方所获取，主要用于云计算场景下计算结果以明文或者机密性保护的方式交换。机密计算可在可信硬件执行环境下实现隐私防护，但当数据离开可信硬件执行环境时无能为力，仅适用于云计算等特定场景下的隐私防护。

安全多方计算：

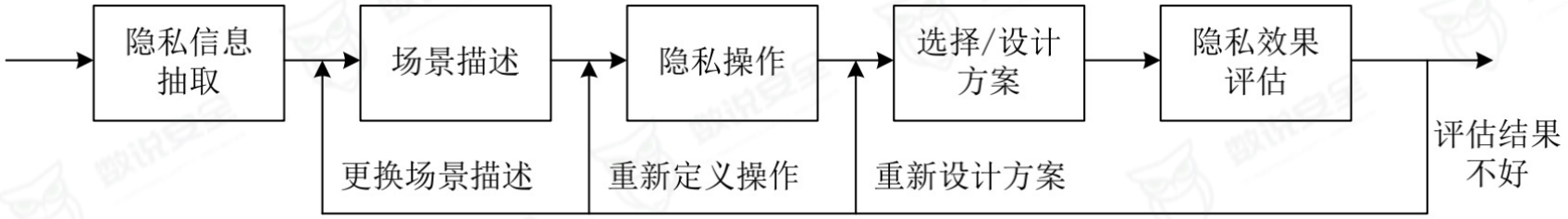
在事先确定参与方数目范围及交互协议的前提下，所有参与方以密文形式交互参与运算的信息并完成预先约定的运算任务，所有参与方都能得到运算结果的明文，但不能得到相互交互参与运算的明文信息。安全多方计算是无中心的计算架构，在有恶意参与者的情况下，诚实参与者仍能得到正确的结果，并且不泄露敏感信息。现阶段参与方的数目一般是两方和三方比较常见。秘密共享和不经意传输协议是构造安全多方计算协议的重要机制。本质上安全多方计算没有信息损失，适合于参与方较少场景下的隐私防护，但不适合于参与方高动态变化场景下的隐私防护。

联邦学习：

是多方利用自身拥有数据完成机器学习模型训练的一种分布式架构，合作方之间交换训练中间结果和模型参数，而不交换数据本身，自然而然减少了数据泄露，联邦学习的中间结果也会泄露数据的部分信息。因此，联邦学习是 AI 训练模型的一种模式，对隐私保护而言它仅是一种应用场景。

• 隐私计算框架

隐私计算框架是在隐私信息全生命周期的各个环节中建立应用场景、保护需求与计算模型之间的映射关系。基于场景描述和保护需求，适应性地选择相应环节的计算方法实现相应的计算功能。从全生命周期的角度出发，隐私计算框架如下图所示：



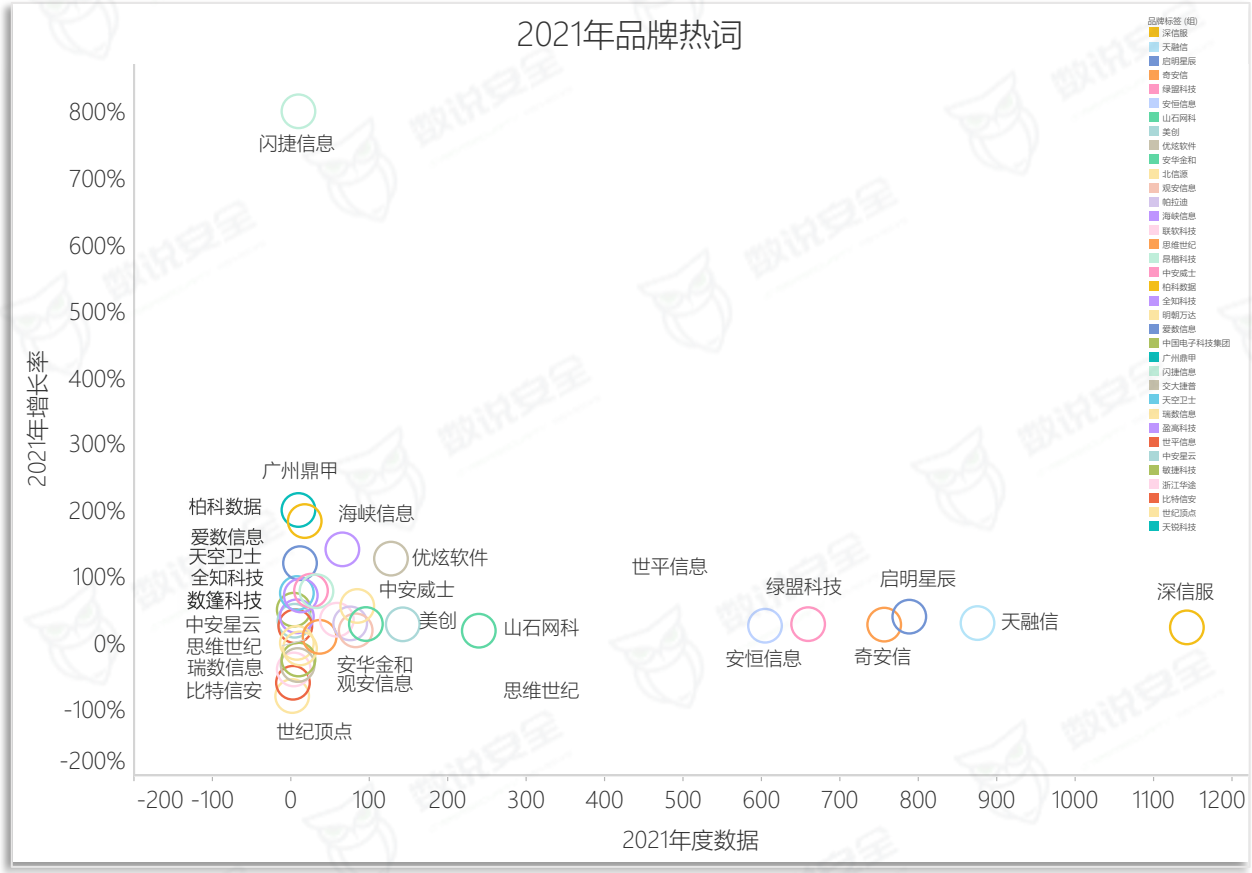
当下隐私计算技术在安全性上仍存在问题和风险，只能在某些特定场景下使用，相关的安全解决方案仍需不断完善进步，但计算效率已达到可用状态，也需要不断提高。例如安全多方计算，具备安全性高的特点，理论上的通用性较高，但由于加解密过程复杂使得对算力、带宽的要求较高；联邦学习，以多方联合建模场景为主，相比于安全多方计算拥有更好的性能，但存在通过梯度数据反推出原始数据的风险；因此，各类隐私计算技术通常被融合使用。

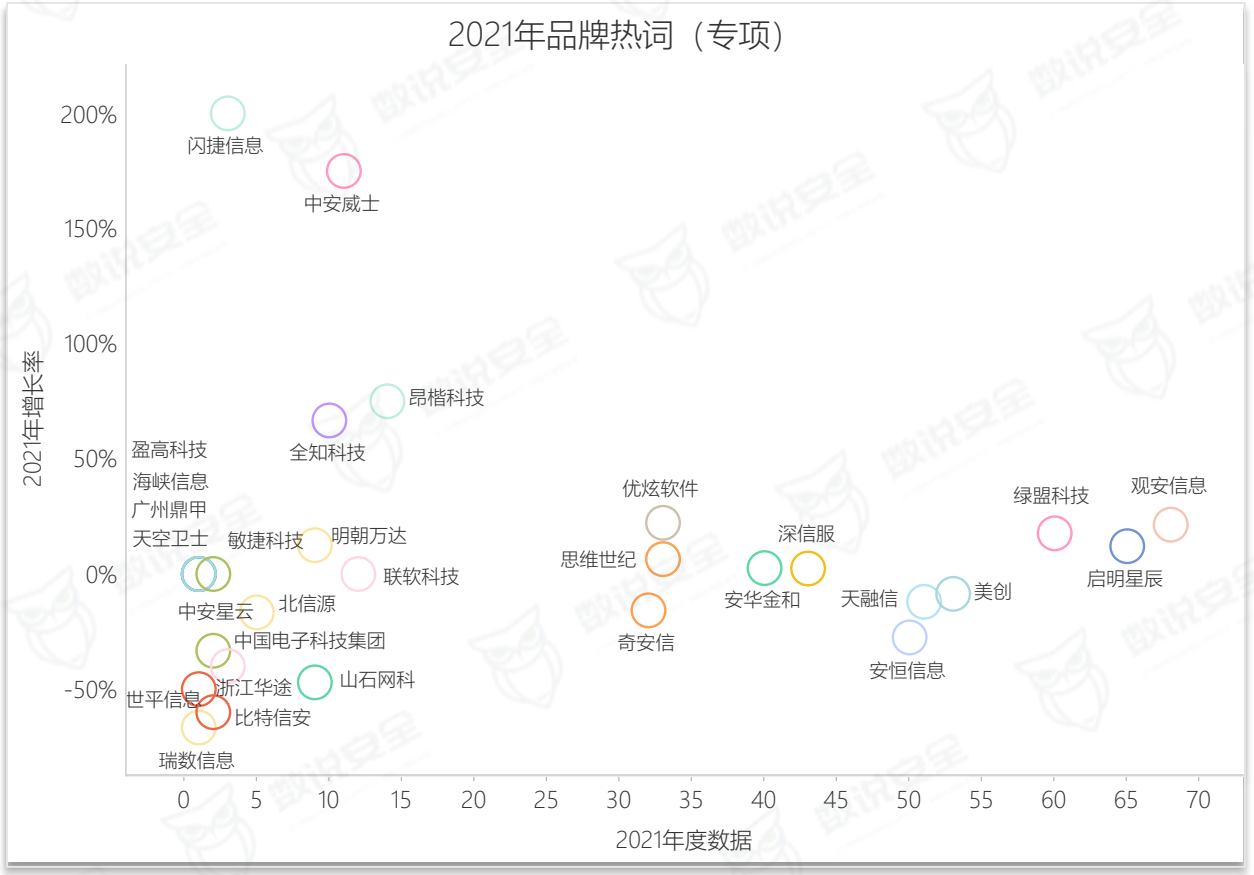
目前隐私计算在金融、政府政务、医疗行业的应用相对较多，例如在政府政务领域，涉及到交通、电力、环境、税收、社保数据等，隐私计算能有效保护和利用各类隶属于不同部门的数据，高效提升政府的治理水平；金融机构涉及信贷、保险、证券期货、互联网金融等数据，隐私计算能将金融数据安全融汇，有效的提升金融资产的清晰度，协助政府进行经济调控和风险管理。

• 2021年数据安全品牌热度

综合性安全厂商的产品线较全面，销售途径较广，且具备提供网络安全、数据安全整体解决方案的能力，因此在竞争中优势较强，如图（2021年品牌热词）所示，综合性厂商明显拉开了和其他厂商的距离，形成第一梯队。

专业数据安全厂商的在数据安全领域的技术和产品能力更强，也在不断健全数据安全整体解决方案的能力，并努力占领数据安全专业领域的高地，如图（ 2021年品牌热词（专项））所示，专业数据安全厂商在专项项目中已经与综合性厂商进行竞争。

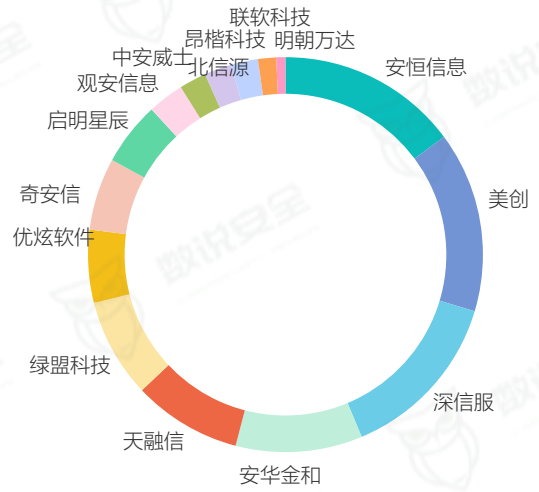




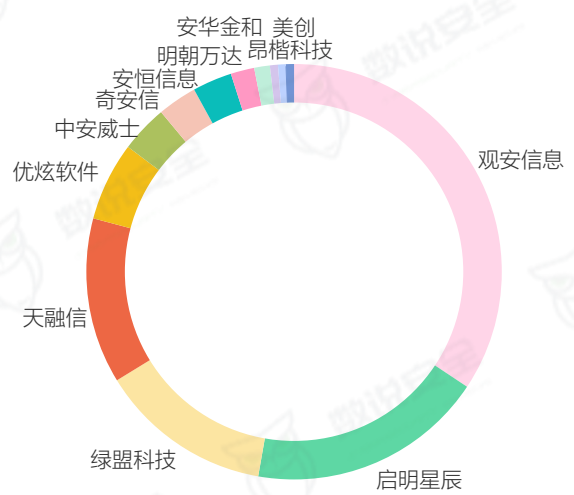
• 2021年数据安全品牌热度行业分布

无论综合性厂商，还是专业的数据安全厂商，都有自己的优势行业领域，经过积累和演进形成数据安全产品及解决方案也更能符合不同行业的合规及业务需求，数说安全以下列六大数据安全建设较为领先的行业为例，选取专项项目进行统计，给出不同行业的厂商专项项目占比情况。

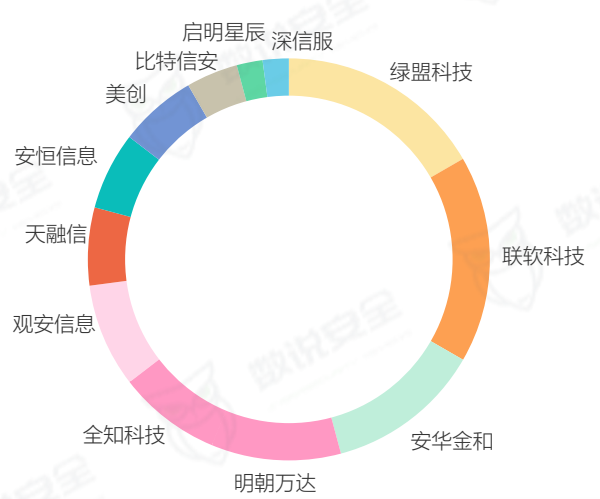
2021年政府行业品牌热词（专项）



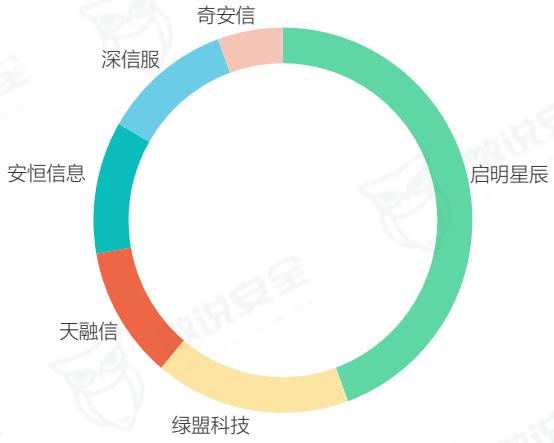
2021年电信行业品牌热词（专项）



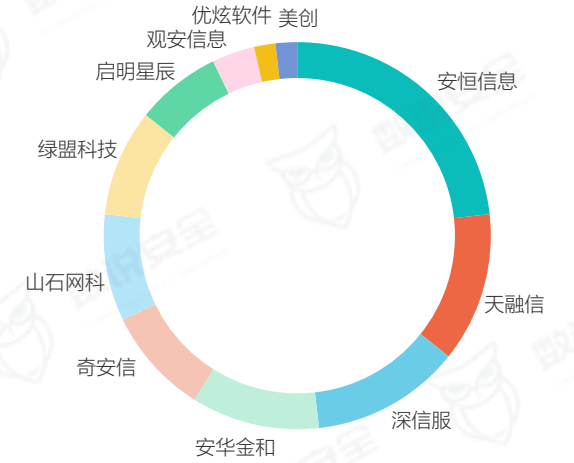
2021年金融行业品牌热词（专项）



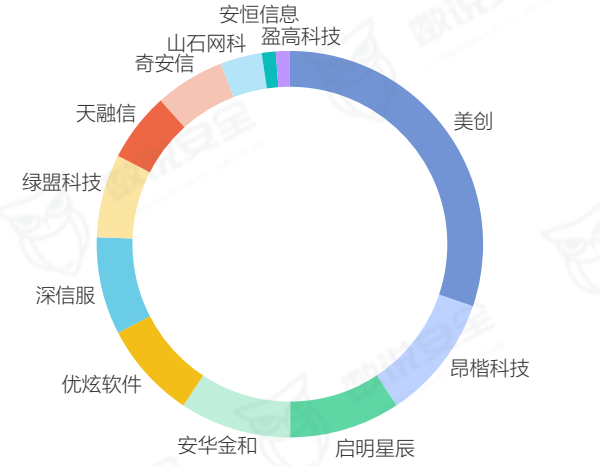
2021年公检法司行业品牌热词（专项）



2021年教育行业品牌热词（专项）



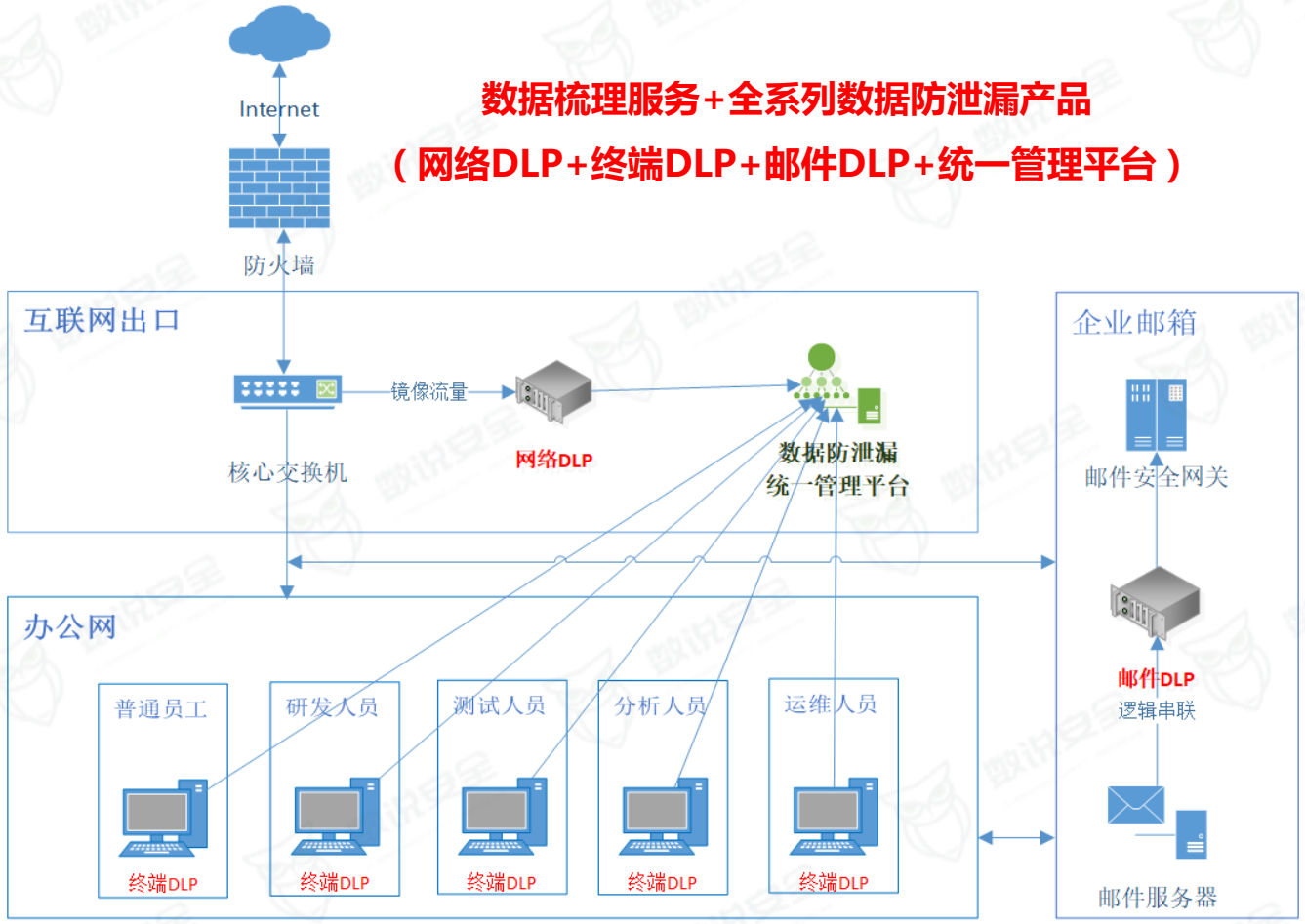
2021年医疗卫生行业品牌热词（专项）



• 奇安信——某烟草企业数据防泄漏整体方案

奇安信科技集团股份有限公司成立于2014年，总部位于北京，是国内领先的综合型网络安全厂商，公司客户覆盖政府、能源、电信、金融、医疗等行业，致力于为政企大客户提供全方位的网络安全解决方案；公司2021年营业收入58.1亿，其中数据安全与隐私保护产品收入突破 11 亿元，同比增长率超过 50%。

项目情况



数据梳理服务+全系列数据防泄漏产品

（网络DLP+终端DLP+邮件DLP+统一管理平台）

项目亮点

客户需求：

- 建设数据防泄露系统体系，为某烟草商业系统的信息系统保驾护航。
- 需要专业的安全集成服务，协助业主方完成相关数据安全方面的实施、检查等有关事项。
- 适配国产化操作系统，防止在国产化终端造成数据泄漏。

解决方案：

- 提供90人天的数据梳理服务，包括数据资产梳理、数据分类分级、配置防护策略、数据风险控制措施落地。
- 提供可落地的安全产品，包括数据防泄漏管理平台、网络防泄漏服务器、邮件防泄漏设备、终端防泄漏软件、上网行为管理设备、防火墙、应用防火墙、数据库审计。

价值收益：

- 完成了敏感数据分类分级管理要求，对烟草数据进行区别保护。
- 发现敏感数据外发的情况，通过对接客户系统快速的定位到人，并进行处理通告，起到威慑的作用。
- 发现员工邮件中带有敏感信息，并通过邮件DLP的阻断和审批功能对邮件泄密进行管控。
- 在员工终端上部署终端DLP，启用USB拷贝、端口管控、屏幕水印、打印水印功能，进行严格的管控。

• 绿盟科技——某省运营商数据安全运营平台案例

绿盟科技有限公司成立于2000年，总部位于北京，公司于2014年在创业板上市，是国内综合型网络安全厂商，可提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务，公司提出智慧安全3.0理念，向“全能力，全运营”方向进化。公司客服覆盖政府、金融、运营商、能源、交通、科教文卫等多个行业。

项目情况及核心亮点

项目背景

1. 数据保护条例、数据安全管理办法的实施及数据安全法的制定
2. 两部委、运营商集团以及工网安函【2021】45号文件考核要求
3. 基于建党100周年的终端及网络数据安全防控需求
4. 数据泄露事件频繁发生，造成的影响也越发严重。

建设方案

重点关注运营商各节点公网出口环境中数据泄露的风险和数据泄露行为的追溯。

重点关注运营商营业厅终端数据安全的行为管控，防范数据泄露的风险和泄露行为的追溯。

建设数据防泄漏，对网络、终端等多种数据外发渠道进行实时监控和预警拦截。

建设数据安全平台，实现对敏感数据规则的统一管理和下发以及事件统一管理、集中生成报告。

建设成效

方案优势

动态纵深防御检测分析　　数据资产自动化识别

全面的数据资产安全防护　　精准指挥联动防护

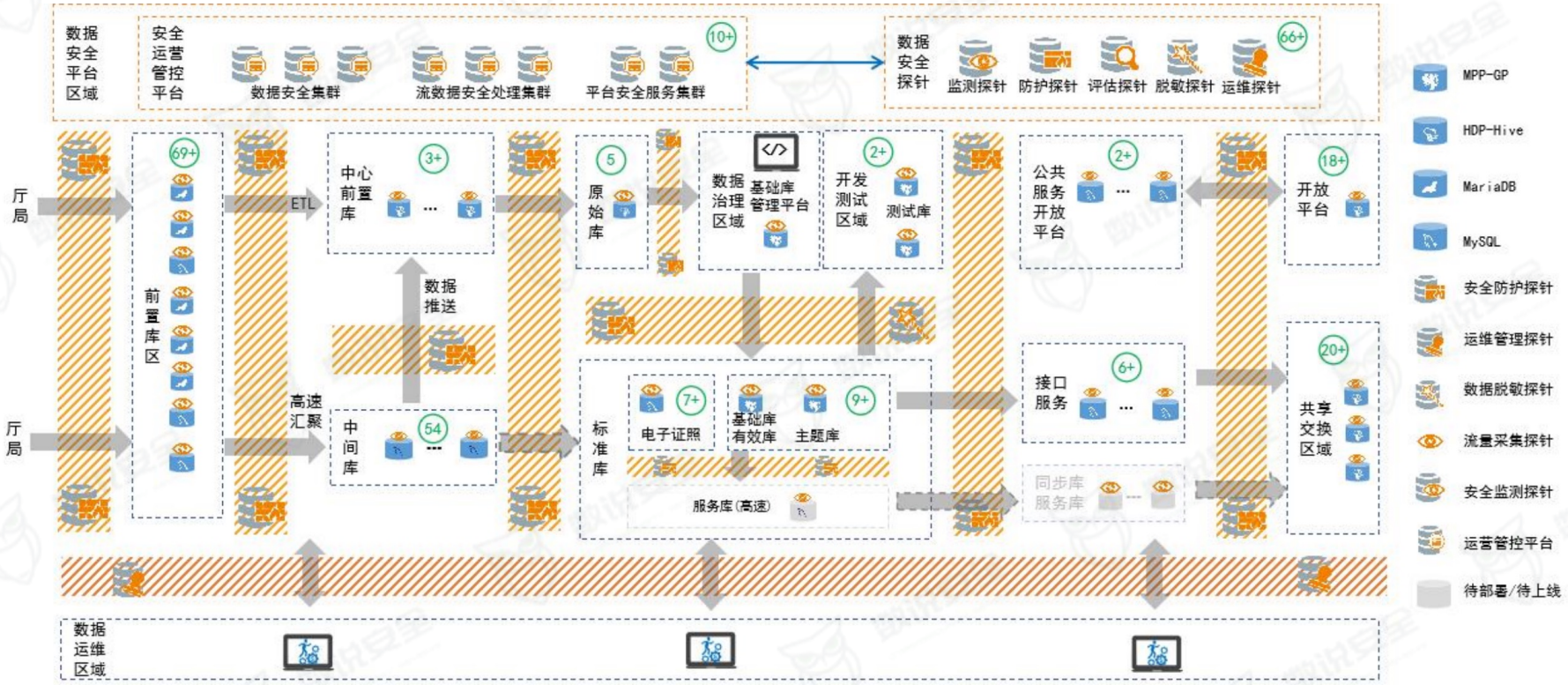
客户价值

- 防泄漏能力补充：补充客户对网络、终端等多种数据外发渠道进行实时监控和预警拦截的能力。
- 满足客户迎检需求：协助客户满足工信部、集团、两部委考核要求。
- 滚动扩容：可以通过本数据安全运营平台快速扩容其他底层探针，满足其余数据安全考核要求，如脱敏等。

• 安华金和——某政务大数据中心安全运营实践

北京安华金和科技有限公司成立于2009年，总部位于北京，是中国专业的数据安全产品与解决方案提供商，中国“数据安全治理”理念、体系的提出者和践行者。公司提供覆盖数据安全合规、数据安全保护、数据安全管理、数据安全共享四大领域的数据安全整体解决方案，产品、平台和服务覆盖数据全生命周期。客户已覆盖政务、金融、能源、医疗、教育、企业、运营商等重点行业，付费用户2500+，被保护数据库60000+。

项目情况



项目亮点

客户需求

- 建立完善的政务数据分类分级标准，区分重要数据，数据安全能力有的放矢。
- 面对复杂的网络现状，实现从数据使用角度对访问行为的监测，管理。
- 建设可视化的综合管理平台，实现对“数据的存量，流转，策略管理”的统一管控。完成常态化、持久化的数据安全运营建设。
- 提供数据安全流程化工作台，使数据安全工作常态化、流程化、规范化。

解决方案：

- 搭建数据安全运营平台（DSOP），提升数据安全保障能力，以面向数据资产梳理、监测、保护为需求方向，通过安全集中运营，针对数据存储使用不规范、敏感数据泄露、数据违规操作、数据违规开放共享、数据异常流转等数据安全问题，实时监测数据安全风险态势，从而保障了数据资产的安全、可靠。

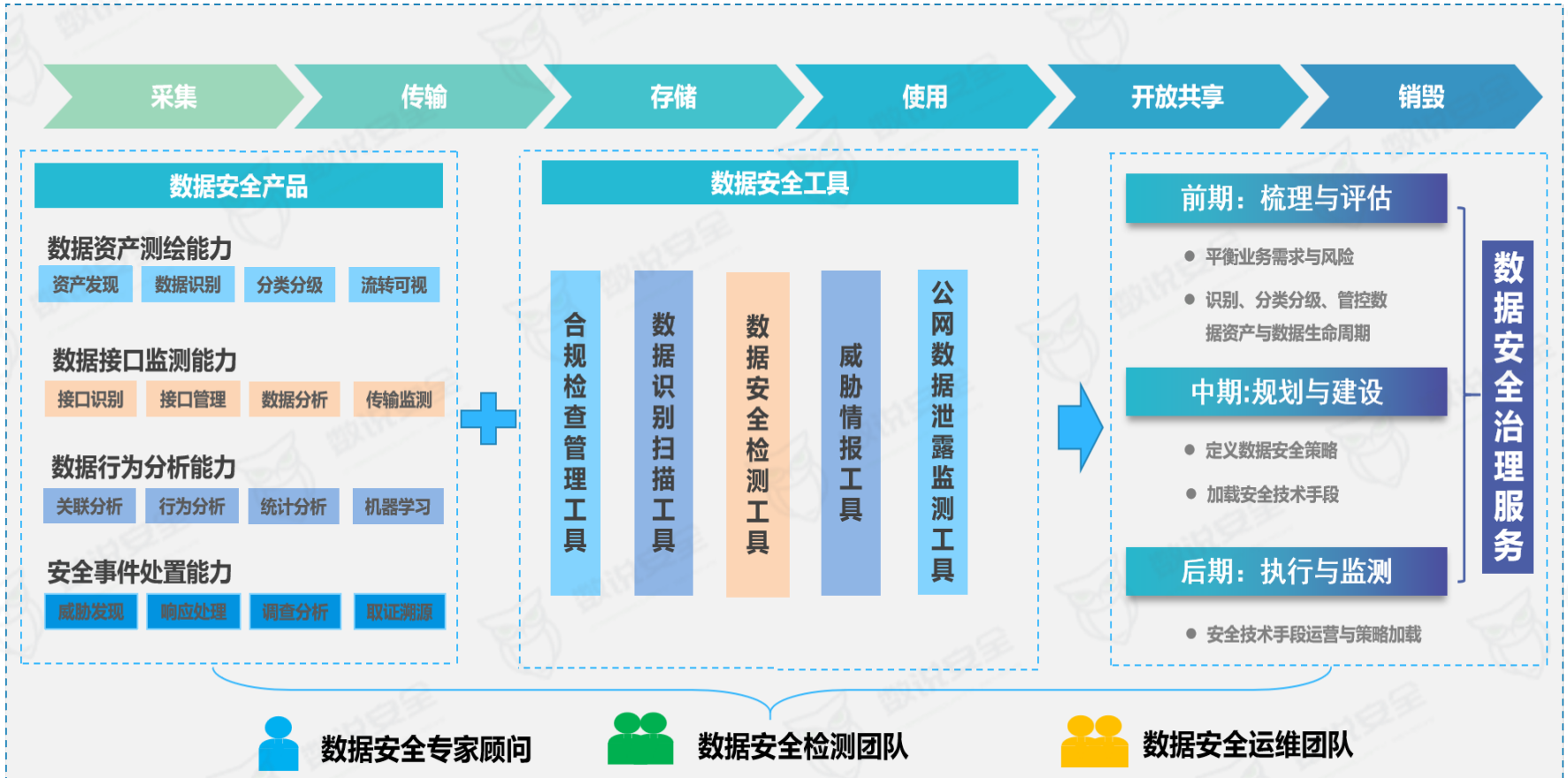
价值收益

- 通过数据安全运营平台，对信息化建设过程中的信息安全运行态势分析和安全优化提供强有力的支撑。
- 建设行业数据分类分级标准、数据使用等一些列规范标准，完善管理制度。
- 通过对安全措施的不同组合和先后依赖，形成对数据资产全链条防护。
- 提高数据安全监测与防护的集中化管理程度。

• 思维世纪——某省电子政务云平台之数据安全监管项目

成都思维世纪科技有限责任公司成立于2001年，公司总部位于成都，是国内数据安全、内容安全、安全服务的先导企业。公司致力于向客户提供“识别—检测—监测—管控”的数据安全治理服务，业务范围覆盖全国20余省份，为网信办、工信部、公安部等监管部门提供支撑，客户覆盖通信、政务、能源、金融、医疗等行业。

项目情况



项目亮点

项目亮点：

- 建设“监管咨询-常态监测-评估整改”三位一体的数据安全监管支撑体系
- 基于“专家团队+专业工具+专用产品”，构建精准、高效的数据安全风险监测、追溯与处置的平台体系。
- 结合“主动扫描+监测分析+黑产线索”多种方式，全方位无死角解决数据泄露风险

项目成效

- 风险业务识别：发现180余处数据通道业务、44个关键模块场景分类和流程、23个关键数据接口。
- 数据风险事件识别与处置：发现风险5000余次、封停58个业务账号、接口，追责违法违规人员1人。

• 美创科技——某政务大数据局数据安全管理平台

杭州美创科技有限公司成立于2005年，总部位于浙江杭州，专注深耕数据安全领域十数年，从医疗行业起步，已经形成数据安全咨询、防护、运维等全方位的能力和产品；公司以数据安全敏捷咨询为抓手，构建数据安全框架，指导数据安全防护体系的建设，客户数量过万，覆盖33个省市的医疗卫生、政府、教育、金融、能源电力、物流交通等行业。

项目情况

项目亮点

通过部署美创数据安全管理平台，接入数据库防水坝、数据静态脱敏、敏感数据动态脱敏、数据水印溯源等数据安全能力，统一调度和联动各类安全资源进行数据安全能力建设。

- 该大数据局作为监管端，采用多租户管理模式，为各委办局分配安全防护事件存储空间。
- 各委办局作为被监管端，被添加成为租户后，与该大数据局共用一套数据安全管理平台，无需额外自建即可拥有数据安全管理能力，同时可根据自身不同的安全诉求，按需开通相应的安全能力。
- 除进行该大数据局自身的安全风险监测外，还可统一监管各委办局的安全建设情况。

客户价值：

1、快速建立安全能力，统筹安全资源利用。政务云上统一搭建数据安全资源池，租户可按需开通，避免重复建设，同时保证建设的统一性。

2、持续安全运营，降低安全运营成本：统一管理安全设备，集中采集安全设备信息，联动安全设备日志，统一下发策略，提升数据安全运营管理能力。

3、级联态势感知，中心指挥调度：各委办局可查看本单位安全态势及平级其他委办局的综合态势，大数据局可实现态势的统一监管。

• 观安信息——某运营商集团数据安全管控平台项目

上海观安信息技术股份有限公司成立于2013年，总部位于上海，专注于数据安全领域，可提供全面保护业务系统的敏感数据安全使用和流通的一站式解决方案。公司采用上海、北京、深圳一级总部，成都、广州区域总部运营模式，同时设立多个实验室，业务覆盖全国绝大部分地区，客户涵盖运营商、政府、金融、电力、公安、医疗等主要行业。目前公司数管平台已在某头部运营商覆盖总部及11个省公司，市场份额处于行业领先地位。

项目情况

项目亮点

➢ 运营能力持续提升

以整合全网资源、标准化流程协同、统筹指挥为原则，实现全网数据安全风险工作的监督，指导评估安全管理与运维工作，形成安全运营的闭环管理模式。

➢ 先进技术创新应用

机制创新，提供领先的数据安全自动化规范化的风险检测响应机制，推动整个移动通信行业数据安全管理的发展。

➢ 全方位安全监控

对内全面监测，对外分析整体数据安全行为威胁成因及外网的数据资产暴露面监测能力，实现从外到内的全方位数据安全监测。

➢ 多维风险分析处置

全面感知数据安全威胁，加强取证与责任判定，及时止损与快速响应，建立纵深防御的数据安全防御体系。

• 中安星云——某智慧住建体系数据安全建设案例

中安星云软件技术有限公司成立于2014年，总部位于北京，公司专注于数据安全领域，以 “专注数据安全、护航数字经济”为使命，可以为用户提供涵盖数据全生命周期全场景的数据安全产品、服务和解决方案，能够满足云、大数据、信创等领域的数据安全需求；公司广泛服务于政府、电力、医疗、教育、金融和运营商等近千家客户。

项目情况

项目亮点

➢ 应用挑战

建设以CIM基础平台为核心的智慧住建体系，能够引导和促进城市开发建设方式的转型、提升城市品质、实现科学决策和精准调控。项目中涉及基础地理、电子地图、遥感影像、城市建设、城市管理、施工监管、市政设施监管等重要数据，一旦出现信息泄露、数据丢失等安全问题，后果严重。

➢ 方案描述

以PK体系和可信计算3.0为基座，为各类应用提供安全可靠可信的计算环境，有效抵御了各类网络攻击，构建安全基石；通过信创云平台，解决硬件堆砌带来的成本和管理问题，根据用户场景和规模，自主选择相关网络资源、计算资源以及安全资源，实现弹性扩展，按需服务现。通过全面的数据生命周期防护，以数据分类分级为基础通过安全监测、访问控制、数据加密脱敏、安全审计等手段保证数据各个场景的安全。

➢ 方案价值

数据更安全：通过国产化和可信计算3.0摆脱外国硬件平台的束缚，从底层硬件和操作系统层面保证安全可控，通过数据安全生命周期安全技术保证用户数据安全。

降低维护成本：通过统一的界面实现设备的统一管理，统一策略下发、统一日志上报， 使管理员及时准确的了解网络中的系统的安全状况。

扩展更简单：采用分布式处理架构，突破传统能力的瓶颈，可横向扩展安全防护能力和存储备份能力，实现海量日志的存储分析及响应。

• 世平信息——某运营商数据安全管控平台

杭州世平信息科技有限公司成立于2010年，总部位于杭州，在数据内容识别和数据安全合规领域深耕多年，为用户提供数据资产/敏感数据发现、数据分类分级与管理、数据安全合规性风险检测评估与监管，以及基于业务流程的精细化数据安全管控等业界前沿能力，产品与解决方案可实现针对涉密数据、个人信息和重要数据的合规性与内源性数据安全风险的识别管控，满足监管部门、政企用户的数据安全治理需求。

项目情况

项目亮点

➢ 安全产品联动管控
各个安全产品共享风险信息，促使数据安全产品联动管控，更加有效的避免数据安全事件发生。

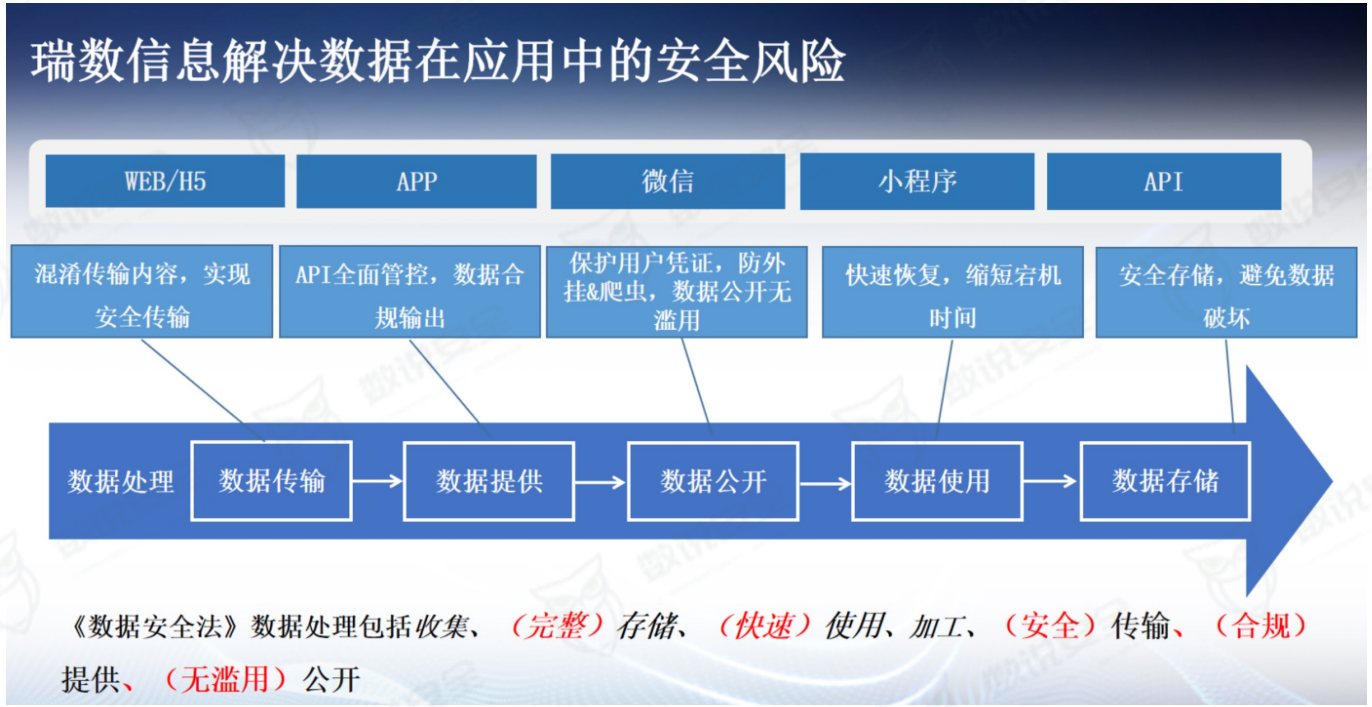
➢ 安全事件关联分析
构建多种场景的行为分析模型，通过实时和离线的检测方式，对用户、实体的行为进行有效的检测与分析，输出直观的风险评级和事件分析报告，便于安全人员能够及时响应异常和威胁。

➢ 基于零信任的接口管理
包括用户鉴权模型、设备鉴权模型、访问目标鉴权模型以及环境鉴权模型，并支持多种鉴权信息组合鉴权；支持生成SDK，供第三方产品快速集成。

• 瑞数信息——某运营商应用数据安全防护解决方案

瑞数信息（River Security）成立于2012年，中国动态安全技术的创新者和Bots自动化攻击防护领域的专业厂商。公司总部位于上海，在北京、广州、成都、深圳、南京等20多个城市设有分公司、办事处和服务团队， 并在成都、上海和北京分别设有研发中心和研发团队。目前业务覆盖三大运营商、金融、政府、制造、能源、交通、医疗、教育、电商互联网等众多行业上千家头部顶级客户。

项目情况



项目亮点

客户需求：

- 运营商应用系统在数据传输过程中高度重视数据被篡改的风险。
- API成为攻击者重点关注的目标之一，保护API对于运营商变得越来越重要。
- 勒索软件对于核心应用的攻击变得愈发频繁，传统安全方案及备份和容灾系统无法应对勒索软件攻击。

解决方案：

- 数据传输环节：以“动态防护”技术为核心，采用“一次一密”技术进行数据混淆，使得传输内容的混淆结果每次不同，从而提高攻击者的破解难度，实现安全传输。
- 数据提供环节：瑞数API动态安全方案，可以从敏感数据的接口识别、攻击检测、异常行为处置、行为审计四大方面，实现API的风险分类、评级和处置，避免因API滥用导致的敏感数据泄露。
- 数据公开环节：通过人机识别、行为分析、按需拦截等技术，对Web、APP、小程序、H5、微信、API等全应用接入渠道，实现外挂和数据爬虫的防护。
- 数据使用和存储环节：瑞数智能数据安全检测与应急响应系统，采用了基于创新AI人工智能的快速数据检测与响应技术，以数据安全底座为支撑，提供数据风险管理、实时智能检测、威胁验证和快速恢复等功能，有效反击黑客勒索、防止批量数据泄露和破坏的安全能力，构筑起事前、事中、事后三道防线的纵深防御体系。

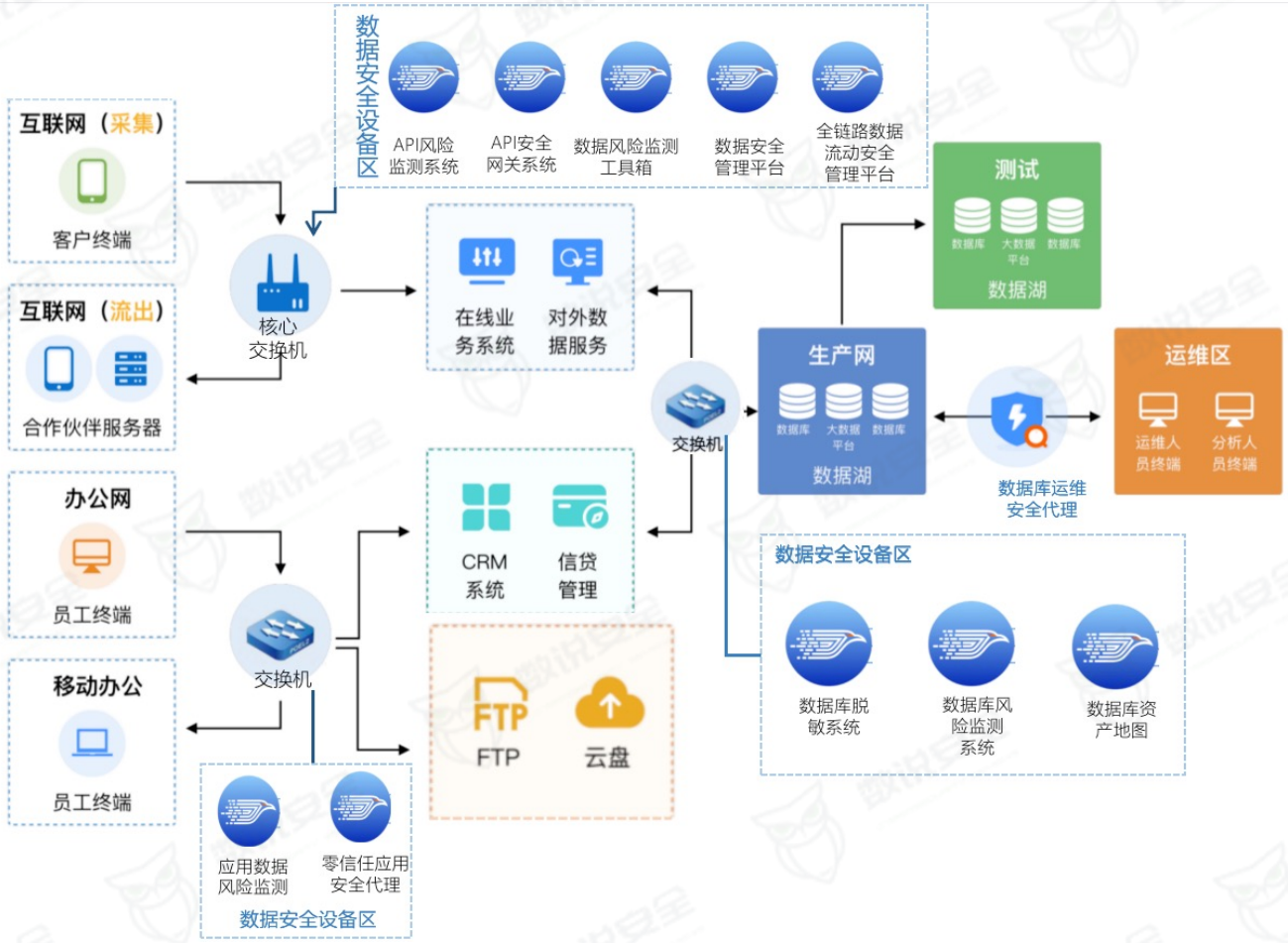
价值收益：

- 动态安全技术帮助运营商有效抵御各类自动化攻击，全面提升自身核心应用、业务及数据风险防范能力，构建更加主动的防护安全体系。
- 核心“动态安全+AI”技术，对客户端进行精准的合法性验证和行为识别，实现人机识别。
- 基于AI人工智能的行为分析技术可透视未知的威胁和风险。
- 全方位助力运营商解决数据传输保护、API敏感数据管控、身份信息防护和数据防爬、数据安全使用和存储的问题。

• 全知科技——某市电子政务系统数据安全风险监测平台

全知科技（杭州）有限责任公司成立于2017年，总部位于杭州，是数据安全领域的技术创新厂商，以提供数据为中心的数据流动安全解决方案为理念，基于API技术重点打造“知形-应用数据风险监测系统”与“知影-API风险监测系统”。全知科技已经与各地政府及多家银行、金融、运营商、互联网、物流、医疗等行业企业建立合作关系。

项目情况



项目亮点

➢ 让数据安全建设有章可循

以国家数据安全法和行业数据安全监管规范为准绳，全面动态掌控企业在数据安全方面的差距，并以此为基础完成数据安全治理组织、制度、体系的规划和设计，让数据安全建设有章可循。

➢ 让数据安全策略持续有效

动态适应保障数据安全策略的有效性和时效性

a)动态数据梳理和分级，让企业时刻都拥有一份完整的数据安全资产清单；

b)持续的数据安全监测体系，让企业时刻掌控着当前数据安全风险态势，第一时间响应和解决数据安全高危风险，持续为数据流动保驾护航。

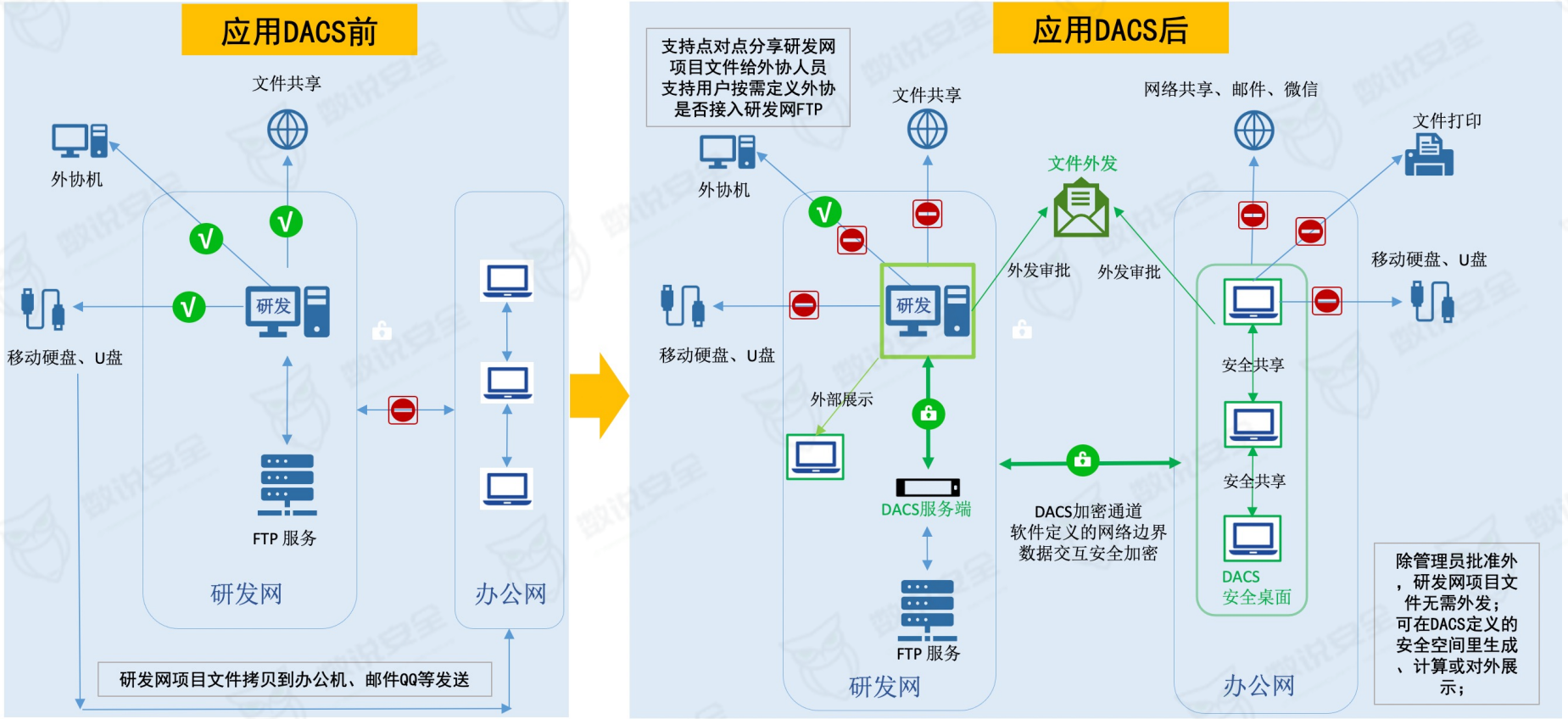
➢ 让数据安全落地成本可控

遵循国家和行业监管规范，以可控成本落地建设一套数据分级保护体系，缩减高等级数据的暴露面、最小化高等级数据的授权、严格控制和保护高等级数据的流出。

• 数篷科技——某大型IT企业数据安全管控安全项目

数篷科技有限公司成立于2018年，总部位于深圳，是一家数据安全技术创新公司，基于新一代沙箱、高性能网络隧道、软件定义边界、AI安全策略引擎等核心技术，公司推出了零信任终端安全工作空间 DACS Pro、零信任网络安全访问控制系统 DACS Lite、零信任移动安全工作空间 DACS Mobile 等产品，致力于为企业提供符合零信任架构标准的下一代数据安全解决方案。公司服务超百家知名企业，客户覆盖证券、保险、银行、电商、高端制造、游戏、互联网等行业。

项目情况



项目亮点

项目介绍：

该企业是国内本土顶尖的大型IT企业，数篷科技DACS主要应用于其硬件研发数据保护场景。接入DACS前，该企业采用内网与外网硬隔离的方式保护设计图纸、代码、客户资料等企业数字资产的安全，且设备之间的信息传输效率低，IT 设备成本昂贵。接入DACS后，根据不同职能和业务建立不同安全空间，员工可在DACS安全空间内运行安装在本地的开发、设计等程序，安全空间中的资料无法通过IM、邮件、U盘等任何方式泄露出去。

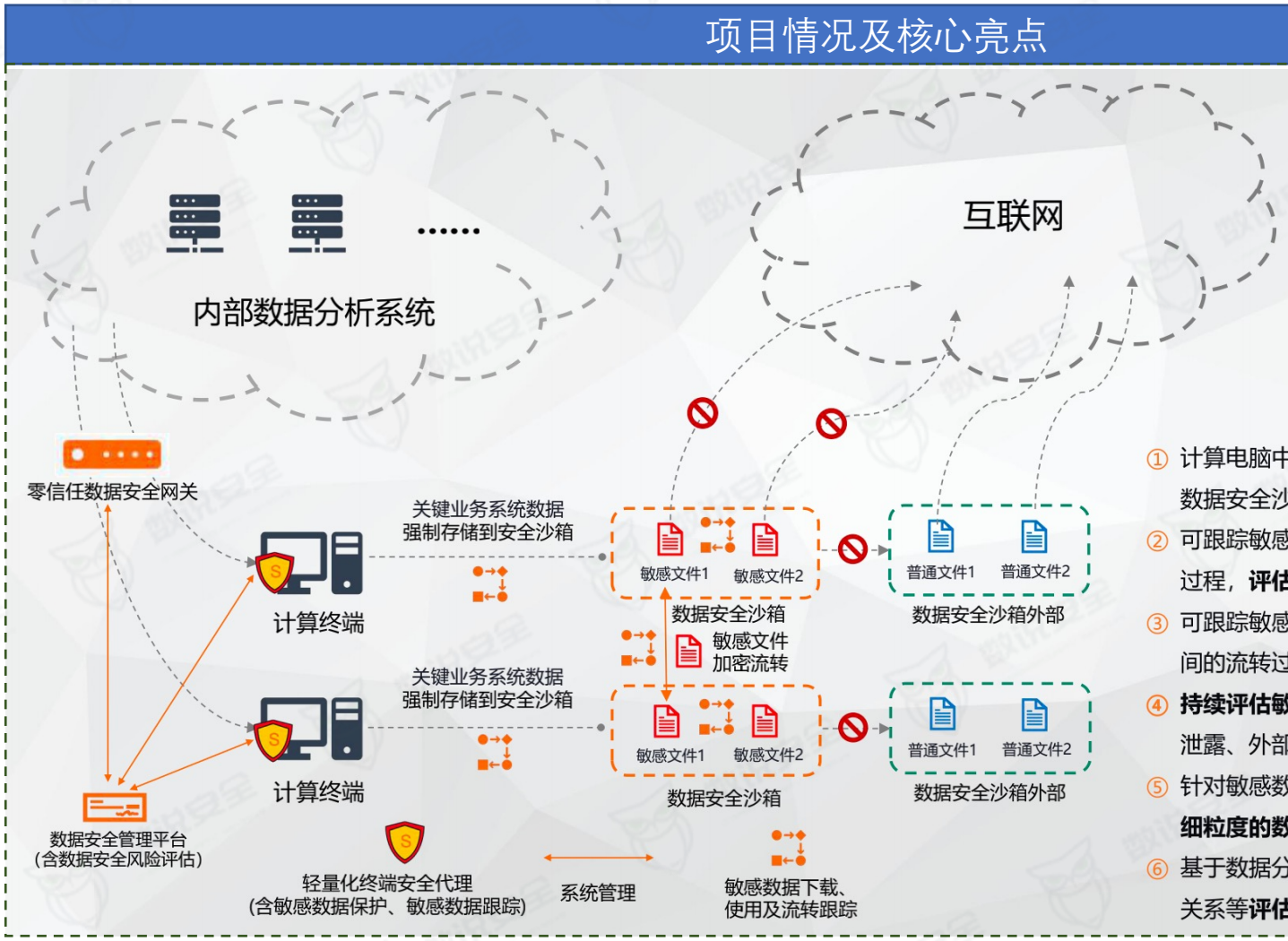
项目亮点：

- 分级分类管理： 通过DACS 对授权资源分级分类，遵循“最小化权限”原则，实现细粒度的权限和数据管控。
- 数据隔离防护：安全空间内的所有数据、资料，都无法通过任何方式泄露到安全空间外。
- 平台稳定易用：对网络质量没有额外负担，连接安全稳定，有效保证业务连续性；同时不改变用户原有的操作习惯，提升工作效率，使用体验好。

• 数安行——某券商数据安全计算分析与数据价值评估平台

北京数安行科技有限公司成立于2020年，总部位于北京，是一家专注于数据运营安全的新一代数据安全技术创新公司。公司建立AI驱动的零信任数据运营安全平台，为用户提供自动化的数据价值发现及数据安全服务，实现全类型多源数据资产发现及风险分析、全流程数据流动治理与风险感知以及自适应精准化的数据安全防护。

项目情况及核心亮点



安全收益

① 计算电脑中从内部数据分析系统下载的数据只能存储到数据安全沙箱中，**缩小敏感数据资产暴露面。**

② 可跟踪敏感数据下载、以及在数据安全沙箱内使用的全过程，**评估敏感数据使用风险。**

③ 可跟踪敏感数据在业务系统与终端电脑以及终端电脑之间的流转过程，可视化展示**敏感数据流转轨迹。**

④ **持续评估敏感数据流动风险**，识别内部数据扩散、数据泄露、外部攻击窃取等风险。

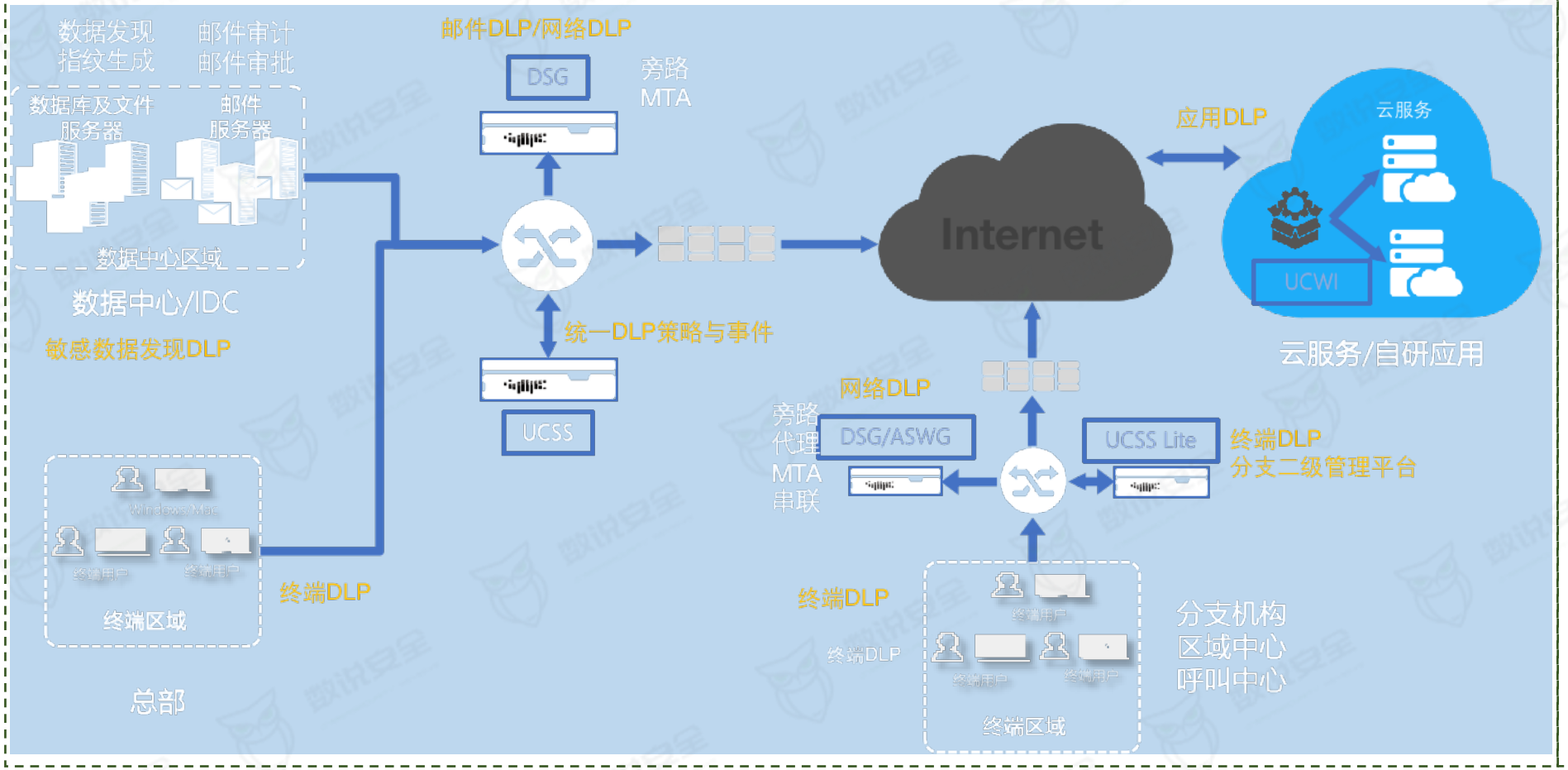
⑤ 针对敏感数据重要程度，数据处理用户风险等级，采取**细粒度的数据安全管控。**

⑥ 基于数据分类、数据与业务映射关系、数据与用户映射关系等**评估数据价值及重要程度。**

• 天空卫士——某大型新能源高科技公司数据安全案例

北京天空卫士网络安全技术有限公司成立于2015年，总部位于北京，公司以数据防泄漏技术为核心，发展以人和数据为核心的新一代数据安全技术，融合统一内容安全技术（UCS）和内部威胁管理技术（ITM）为基础，创立了内部威胁防护技术体系（ITP），已在政府、金融、高科技制造业、大型企业以及互联网等部门和行业广泛部署并使用，获得客户的高度认可。

项目情况



项目亮点

- 集团总部+分支机构，支持集中管理与分布式部署结合，覆盖完整的网络、终端、邮件的DLP解决方案，统一策略管理，为风控/内审部门实现数据安全价值的数据展现。
- 解决管理平台高可用、数据库外置集群问题，邮件泄密保护要求同时支持本地邮件服务+Office 365邮件服务集成问题，与内部应用进行DLP对接集成的问题。
- 具备全体系DLP产品，平滑替换与迁移原国外公司全套DLP系统，并能够进一步在管理能力与防护能力增强，具备千级数据安全策略迁移能力与实施交付能力。

总结

• 总结

随着数字经济时代的序幕开启，全球数据作为核心生产要素被利用、开发而产生的价值日益凸显，数据的规模呈现爆发式增长态势，数据的丢失、泄漏、篡改、勒索所引发的经济损失和社会负面影响愈发严重，数据的流通、交易、使用和产生的安全问题已经成为国家及社会各领域关注的重点，疫情的常态化发展更推动了这一进程。在这样的背景下，作为保障数字经济健康高效发展基石的数据安全已经上升至国家层级，成为国家安全战略的重要组成部分，是国家安全的重要建设领域。

一、需求角度的数据安全市场现状

- 从2018年至今，用户采购数据安全类产品、解决方案和服务的数量与金额都在快速增长，市场蓬勃发展；
- 市场公开招投标项目显示，只有少数领域的用户在进行数据安全建设时是以业务安全为核心导向，大多数用户还是以满足合规需求为主要驱动力进行产品采购；
- 近两年数据安全咨询、评估、分类分级等服务的采购数量有明显的增加，反映出用户当下的核心诉求是梳理自身业务流程中的数据生命周期情况及防护现状，并弄清楚该如何进行数据安全建设才能满足合规及业务安全要求；
- 用户对隐私计算、零信任等寄予了很高的期望，说明用户希望找到能解决数据安全问题的终极方法。

二、供给角度的数据安全市场现状

- 与中国的数据安全产品供给品类偏少，产品更新迭代速度偏低，与国外对比仍有一定差距；
- 数据安全产品和解决方案的成熟度尚不够高，例如授权管理与动态访问控制粒度不足，隐私计算的各项技术成熟度不高，数据分类分级工具的支撑力度和覆盖范围不足等；
- 数据安全与用户IT系统的耦合与解藕问题还有待解决，无论在理论方法层面，还是在实施执行中都还有待突破。

三、监管角度的数据安全市场现状

- 数据安全相关的三大上位法——《数据安全法》、《网络安全法》、《个人信息保护法》——已经颁布，下位法在逐步制定与出台中；
- 政府、金融、电信等领先行业已经发布了若干数据安全分类分级标准与数据安全有关的规定，更多的行业类似标准与规定正在制定过程中。

四、数据安全市场未来展望

在数字经济时代和国家安全战略的背景下，数据安全将是今后相当长一段时间内监管方、需求方、供给方所共同关注的重要问题。监管方以国家和经济安全为导向，以合规为基础手段，要求不出现重大数据安全事故；需求方的大多数用户主要以满足合规为驱动，少部分重点领域用户在合规的基础之上要求不发生数据安全问题或问题可控；供给方的产商则力争提供能为用户解决切实问题的产品、解决方案和服务，在数据安全市场中获得更高的市占率，使企业不断强大。各方诉求不尽相同，相互之间的协调、平衡也将会是一个漫长的过程。

社会各界对数据安全的关注度、重视度、期望度都非常高，希望很快就能获取到较为完美的数据安全解决方案，但数据安全相关的技术、产品、解决方案和服务还不完善，无法妥善解决当下的很多问题，技术的创新演进也非朝夕之间可以实现，数据安全体系的成熟还有很长路要走，但相信在未来2年-5年-10年间，有关数据安全的技术、产品、解决方案、服务会逐步推出并逐渐走向完善。

未来，数据安全市场将持续保持良好的增长态势，市场各方的诉求也会达到动态平衡，为数据安全市场的繁荣有序发展提供持续的动力，数据安全终将成长为一个可以和网络安全相比肩的市场。

THANK YOU

以数据为基础的网络安全产业研究平台

关注“数说安全”公众号，私信回复“数据安全报告”，获取报告完整版