BDS 国家工程研究中心和天枢智库联合出品

# 数字安全观察

DIGITAL SECURITY INSIGHT

数据安全专刊 No. 006(总第 208 期)

责编：钟力 zhongli1@360.cn

# 导 读

回顾刚刚过去的 2022 年，数据安全领域的技术创新与挑战同在。2022 年，数据泄露事件依旧频发、勒索软件更加猖獗，企业面临的数据安全风险只增不减；在《数据安全法》、《个人信息保护法》的指引下，十余项数据安全国家标准颁布实施，企业面临的合规监管挑战继续加大。值得一提的是，随着年末新冠疫情管控的放开，加之国家陆续出台了一系列促进数字经济的举措，数据安全市场有望在 2023 年迎来发展良机。

第六期《数字安全观察 数据安全专刊》对 2022 年全年数据安全形势进行了回顾与展望，以期为读者呈现数据安全发展的全年态势，本期分为政策形势总结、数据安全事件分析、技术产品与市场趋势盘点以及数据安全优秀实践案例、工程中心研究五个板块，主要内容如下：

**政策形势方面**，各国纷纷出台数据安全和隐私保护相关政策、规则，促进各自对数据战略秩序的控制，提升在国际化数字市场的竞争力。国际方面，面对日益严峻的数据安全形势，美国、欧盟、英国、新加坡、日本等主要国家和地区不断完善数据立法建设，重点加强数据隐私保护、数据市场、个人信息保护以及跨境数据流动等领域工作；国内方面，我国正稳步推进数字化转型与数字经济发展，加快数据要

素市场化配置，建立健全数据安全法规制度与标准体系，各行业也在逐步落实重点领域安全要求与合规建设。

**数据安全事件分析方面**，主要基于大数据协同安全技术国家工程研究中心（BDS 国家工程研究中心）2022 年发布的系列《全球数据安全观察》周报中收录的数据安全事件，从多个维度进行梳理和总结分析。整体来看，2022 年发生的数据安全事件仍以数据泄露类型为主，在所有事件中占比最高；其次，勒索攻击今年依旧比较活跃，占比为 30%；由于今年全球强监管的整体态势，数据合规事件也占到 15%的比例。从数据安全事件行业来源来看，信息传输、软件和信息技术服务业以 30%的比例位居行业之首，其次，卫生和社会工作、政府机关、金融业也都是数据安全事件频发的行业。

**技术、产品与市场趋势方面**，数据安全技术不断创新突破，标准逐步完善，市场迎来发展机遇。技术、产品方面，隐私计算技术与产品持续突破，其中机密计算成为隐私计算领域重要的解决方案；此外，量子计算等前沿技术受到学术界与产业界的广泛关注，可谓 2022 年炙手可热的研究领域，理论和硬件的一个个突破性进展让人们看到大规模通用量子计算机的脚步越来越近。市场方面，DLP、隐私计算、数据安全服务等市场均得到了快速发展，尤其是隐私计算技术，据 Gartner 预测，2025 年 60%的大型企业机构将在分析、商业智能或云计算领域使用一种或多种隐私增强计算技术。

**数据安全优秀实践案例方面**，本期收录了 BDS 国家工程研究中心征集的 2022 年业界优秀实践案例，以期为政企客户推荐优秀的数据安全解决方案。案例共分两类：优秀行业数据安全解决方案实践案例和优秀数据安全技术与产品实践案例。申报案例覆盖了政务、交通、公安、电信、金融、医疗、能源等行业领域，涉及数据流通共享安全、数据安全合规治理和数据安全保障等方面。

**工程中心研究方面**，本期收录了 BDS 国家工程研究中心关于数据安全方面最新的研究成果。其中，“《全国一体化政务大数据体系建设指南》数据安全解读分析”从数据安全角度分析了指南释放出的数据安全机遇；《完善数据安全治理机制 保障数据要素安全高效流通》对《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》中的数据安全进行了解读分析，并从多个视角对数据安全治理机制的建设与落实提出建议；关于“东数西算”工程中的数据安全问题，研究中心也专门进行了体系化建设的研究与探索，并邀请了业内知名专家进行了沙龙研讨，形成了观点合集，旨在为国家“东数西算”工程数据安全建设建言献策。

# 目 录

## 第一部分 2022 年政策形势总结



## 第二部分 2022 年数据安全事件分析

## 第三部分 2022 年技术、产品与市场趋势盘点



## 第四部分 数据安全优秀实践案例

## 第五部分 工程中心研究

# 一、2022年政策形势总结

2022 年全球各主要经济体复苏态势显著，数字经济成为刺激各国经济增长的重要手段，数据交易、数据市场、数据跨境、数据安全等围绕数据要素展开的数据产业活动作为数字经济的主要方向，为确保数据价值的稳定释放和持续挖掘，各国纷纷出台数据安全和隐私保护相关政策、规则，促进各自对数据战略秩序的控制，提升在国际化数字市场的竞争力。

## （一）国际数据安全政策形势

### 1、美国继续推动数据立法建设，强调国际规则制定与国际合作

美国联邦贸易委员发布**《遵守 FTC 健康违规通知规则》**、**《健康违规通知规则：业务基础》**，对健康信息的安全处理作出更明确的要求；美国国土安全部宣布成立**网络安全审查委员会（CSRB）**，审查和评估重大网络安全事件，以便政府、行业和安全社区能够更好地保护国家网络和基础设施；美国国务院成立**网络空间和数字政策局（CDP）**，强调联邦领域的数字现代化，重点关注国家网络安全、信息经济发展和数字技术三大领域；美国众议院和参议院发布了**《美国数据隐私和保护法案》（ADPPA）草案**，这是首个获得两党两院支持的全面的联邦隐私立法草案，从联邦层面推动分散的隐私立法走向统一；美国众议院通过了**《报告来自被选为监督和监控网络攻击和勒**

**索软件的国家的攻击法案》**，促使美国更容易应对来自外国对手的勒索软件攻击；美国联邦贸易委员会发布**《关于拟议中制度制定的预先通知》**，探索打击有害的商业监控和松懈的数据安全规则；美国拜登政府发布了**《国家安全战略》报告**，其中强调了加强与盟友在隐私、数据共享和数字贸易方面的合作，并继续推动对战略竞争对手的技术脱钩与数据孤立。

## 2、欧盟持续巩固统一治理机制，深化数据单一市场的整体布局

欧盟委员会公布数据治理立法**《数据法案》（Data Act）草案**，为欧盟内部和跨境数据流动构建相适应的规则框架，推动数据市场发展，为数据创新提供机会，并使所有人更容易获得数据；欧洲议会通过**《数字服务法案》**、**《数字市场法案》**为数字平台建立覆盖内容审核、算法数据、定向广告等方面的问责框架，并提出了“守门人”概念，严格规范其权利与义务，防止大型在线平台滥用市场支配地位；欧洲议会通过了**《数据治理法案》**，增加对数据中介服务的信任，并促进欧盟内的数据共享与开发利用；欧盟数据保护委员会（EDPB）先后发布了**《关于数据主体权利——访问权的第 01/2022 号指南》**、**《关于 GDPR 行政罚款计算的第 04/2022 号指南》**、**《执法领域人脸识别技术应用指南》**、**《关于数据跨境传输认证机制的第 07/2022 号指南》**、**《关于向俄罗斯联邦传输个人数据的第 02/2022 号声明》**、**《关于确定控制者或处理者主要监管机构的第 8/2022 号指南》**等文

件，就不同场景下个人数据访问、人脸识别技术应用规范、个人数据泄露通知等要求作出明确和细化，以推动通用数据保护条例（GDPR）以更准确、一致的方式有效落实。

### 3、其他各国不断建立完善战略政策，在全球数据热潮中不甘示弱

**英国**的数据跨境流动标准合同条款**《国际数据传输协议》（IDTA）**及**《欧盟 2021 年标准合同条款附录（英国附录）》**正式生效，发布了**《数据共享治理框架》**为推进公共部门数据共享提供指导，并制定了**ICO25 计划**对未来三年 ICO 的工作给出了规划和方向；**新加坡**推出**《数据保护要素计划》**帮助中小型企业获得基本水平的数据保护和安全实践，并发布**《在安全应用中负责任地使用生物特征数据的指南》**、**《区块链设计个人数据保护注意事项指南》**对如何安全使用生物特征数据、区块链技术中的个人数据保护进行指导；**日本**先后发布了**《<个人信息保护法>合规要点》**、**《企业隐私治理指南 ver1.2》**帮助企业更好地遵循《个人信息保护法》和应对隐私问题，并修订了**《个人信息保护法》**以增强用户权利、加重数据处理者义务、扩大域外适用范围；**泰国、越南、印尼、以色列**等国家也发布了相关政策对数据保护、隐私保护等作出约束和规定。

## 4、主要经济体热衷于建立伙伴关系，跨境数据流动成全球热题

美国、加拿大、日本、大韩民国、菲律宾、新加坡、中国台湾共同发布**全球跨境隐私规则声明**，正式对外宣告成立全球跨境隐私规则(CBPR)论坛，将亚太经合组织（APEC）框架下的 CBPR 体系转变成一个全球所有国家都可以加入的体系。

美国、欧盟成员国、日本、乌克兰等 60 个国家和地区发起**《互联网未来宣言》**，宣称“致力于全球的可互操作的互联网”、“以避免使用互联网进行秘密操作信息活动，破坏别国选举”。

美国与欧盟就**《跨大西洋数据隐私框架》**初步达成协议后，美国白宫签署了**《关于加强美国信号情报活动保障措施的行政命令》**以试图为恢复欧美跨大西洋数据流动提供相应的法律基础，欧盟委员会启动了**《欧盟-美国数据隐私框架充分性决定草案》**的推进进程，这是双方在就数据跨境了流通的第三次尝试。

中国与哈萨克斯坦共和国、吉尔吉斯共和国、塔吉克斯坦共和国、土库曼斯坦、乌兹别克斯坦共和国等中亚五国外长会晤通过**《“中国+中亚五国”数据安全合作倡议》**，共同应对数据安全风险挑战并在联合国等国际组织框架内开展相关合作。

中国证券监督管理委员会、中华人民共和国财政部与美国公众公司会计监督委员会（PCAOB）签署**审计监管合作协议**，形成了符合双方法规和监管要求的合作框架，致力于为企业依法合规开展跨境上市活动营造良好的国际监管环境。

## （二）国内数据安全政策形势

### 1、稳步推动数字化转型与数字政府建设，促进数字经济发展

为加速数字经济的发展，1 月 12 日，国务院印发**《“十四五”数字经济发展规划》**，明确了“十四五”时期推动数字经济健康发展的指导思想、基本原则、发展目标、重点任务和保障措施，并强调着力强化数字经济安全体系，提升数据安全保障水平；7 月 25 日，国务院办公厅发布**《关于同意建立数字经济发展部际联席会议制度的函》**，同意建立由国家发展改革委牵头的数字经济发展部际联席会议制度，以加强统筹协调，不断做强做优做大我国数字经济；河南省、广州市、成都市、陕西省、江苏省、上海市、广东省、西安市等地区先后发布了政策条例、规划报告推动数字经济高质量发展。

为推进数字化转型、建设数字政府等，2 月 22 日，国务院办公厅印发**《关于加快推进电子证照扩大应用领域和全国互通互认的意见》**，为各地区各部门依托全国一体化政务服务平台，积极推进电子证照应用，持续优化政务服务提出电子证照扩大应用互通互认的指导意见；5 月 22 日，中共中央办公厅、国务院办公厅印发了**《关于推进实施国家文化数字化战略的意见》**，应对互联网快速发展给文化建设带来的机遇和挑战，从建设社会主义文化强国、厚植数字时代文化自信的高度，对国家文化数字化作出的战略部署；6 月 23 日，国务院印发**《关于加强数字政府建设的指导意见》**，为全面贯彻网络强国

战略，把数字技术广泛应用于政府管理服务，推动政府数字化、智能化运行制定了总规划、总方针和路线图；民政部、海南省、浙江省、黑龙江省、杭州市等部门、地区相继印发了实施方案推进数字政府建设,**《关于扩大政务服务“跨省通办”范围进一步提升服务效能的意见》**、**《全国一体化政务大数据体系建设指南》**以及各地区的政务数据管理办法等为推进我国数字政府建设、数字化转型提供有力支撑。

## 2、加快推进数据要素市场化配置，探索数据交易平台与市场

1 月 6 日，国务院办公厅印发**《要素市场化配置综合改革试点总体方案》**，提出从公共数据开放共享、数据流通交易、数据开发利用、数据安全保护等方面，完善市场制度规则；4 月 10 日，**《中共中央 国务院关于加快建设全国统一大市场的意见》**发布，提出要加快培育统一的技术和数据市场，深入开展数据资源调查，推动数据资源开发利用；12 月 19 日，**《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》**发布，为充分发挥数据要素作用，赋能实体经济，推动高质量发展提出了四个制度和四项措施，构建了数据基础制度体系的重要支柱；湖南省、广州市、深圳市、广东省、苏州市等地区先后开始了数据交易中心的运营，并积极探索数据交易工作方案，促进数据流动与价值挖掘。

### 3、多举措建立数据跨境安全机制，促进我国数据有序开放

6 月 30 日，网信办就**《个人信息出境标准合同规定》（征求意见稿）**向社会公开征求意见，明确了可以通过签订标准合同的方式向境外提供个人信息的情形、标准合同的主要内容、备案流程等要求，并提供了《个人信息出境标准合同》文本；7 月 7 日，网信办公布**《数据出境安全评估办法》**，规定了评估触发条件、评估内容、具体流程、评估主体等相关要求，在 8 月 31 日又发布了《数据出境安全评估申报指南（第一版）》，再次明确适用范围、申报方式及流程与申报材料，随后江苏省、海南省等地区的网信办开通数据出境安全评估申报通道；12 月 16 日，全国信息安全标准化技术委员会秘书处发布**《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》**，从基本原则、个人信息处理者和境外接收方在个人信息跨境处理活动的个人信息保护、个人信息主体权益保障等方面提出了个人信息跨境处理活动安全认证要求。

同时，深圳与上海也开始数据跨境流动活动的探索与试点工作。1 月 24 日，**《国家发展改革委 商务部关于深圳建设中国特色社会主义先行示范区放宽市场准入若干特别措施的意见》**中明确指出要放宽数据要素交易和跨境数据业务等相关领域市场准入；2 月 18 日，**《中国（上海）自由贸易试验区临港新片区条例》**通过表决，提出在临港新片区内探索制定低风险跨境流动数据目录，促进数据跨境安全有序流动；7 月 15 日，上海发布**关于促进“五型经济”发展的若干意见**，

推进上海数据交易所建设，开展“正面清单+安全评估”数据跨境试点，在自贸试验区临港新片区探索跨境数据流动分类监管模式，打造国际数据港。

## 4、建立健全制度体系，开展检查、认证等工作推进数据安全能力建设

2 月 15 日，修订后的新版**《网络安全审查办法》**生效实施，增加了针对数据处理活动的审查要求，明确要求影响或者可能影响国家安全的数据处理活动在审查范围内、超过 100 万用户个人信息的运营者赴国外上市应申报审查；6 月 9 日，国家市场监督管理总局、国家互联网信息办公室发布**《关于开展数据安全管理认证工作的公告》**，对组织的数据安全管理体系进行认证并颁发证书，鼓励网络运营者通过认证方式规范网络数据处理活动；11 月 4 日，国家市场监督管理总局、国家互联网信息办公室发布《关于实施个人信息保护认证的公告》，鼓励个人信息处理者通过认证方式提升个人信息保护能力；北京市、广东省、上海市、安徽省等地区相继开展电信和互联网行业网络与数据安全检查，进一步提升行业网络与数据安全防护水平。

此外，今年工信部依据《个人信息保护法》《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，**6 次**组织第三方检测机构对不同类型的移动互联网应用程序（APP）及第三方软件开发工具包（SDK）进行检查，最终对存在侵害用户权益行

为且未按要求整改的**340 款** APP（SDK）进行通报；11 月 3 日，国家网信办依据《个人信息保护法》《App 违法违规收集使用个人信息行为认定方法》等法律法规规定，对存在强制索要非必要权限、未经单独同意向第三方共享精确位置信息、无隐私政策、超范围收集上传通讯录、首次启动未提示隐私政策、未告知相关个人信息处理规则、默认勾选隐私政策、无法或难以注销账号等问题的 **135 款**违法违规 App 进行通报并予以下架处置。

## 5、各行业加紧数据安全保障体系建立，加速重点领域安全要求落实

### （1）金融行业

3 月 15 日，银保监会消保局组织开展**银行业保险业个人信息保护专项整治工作**，推动银行业保险业切实落实《中华人民共和国个人信息保护法》；4 月 6 日，银保监会发布**《中国银保监会办公厅关于 2022 年进一步强化金融支持小微企业发展工作的通知》**，规定通过第三方机构获取外部涉企数据的，要关注数据源合规风险，明确数据权属关系，加强数据安全技术保护；5 月 18 日，银保监会发布**《银行保险机构消费者权益保护管理办法（征求意见稿）》**，强调落实消费者身份识别和验证的规定，并严格控制合作方行为与权限，防范数据滥用或泄露风险；8 月 9 日，银保监会发布**《关于开展银行保险机构侵害个人信息权益乱象专项整治工作的通知》**，要求各机构全面摸

排本机构 2021 年以来与消费者个人信息处理活动相关的经营行为和管理情况，查找侵害个人信息权益乱象的问题根源；11 月，证监会发布的金融行业标准中，**《证券期货业机构内部接口 证券交易》**、**《证券期货业数据安全管理与保护指引》**、**《证券期货业数据安全管理与保护指引》**等数据安全管理要求、数据接口规范等进行明确规定。

**（2）交通运输和邮政业**

2 月 25 日，工信部发布**《车联网网络安全和数据安全标准体系建设指南》**，明确指出数据安全标准主要规范智能网联汽车、车联网平台、车载应用服务等数据安全和个人信息保护要求，包括通用要求、分类分级、出境安全、个人信息保护、应用数据安全等 5 类标准；3 月 29 日，工业和信息化部办公厅、交通运输部办公厅等五部门联合发布**《关于进一步加强新能源汽车企业安全体系建设的指导意见》**，要求企业要切实履行数据安全保护义务，建立健全全流程数据安全管理制度，采取相应的技术措施和其他必要措施保障数据安全；4 月 6 日，交通运输部办公厅发布**《关于做好道路客运电子客票推广普及有关工作的通知》**，要求规范电子客票相关信息的采集、传输、存储、应用流程，严防旅客个人信息等重要数据泄露；4 月 21 日，国家邮政局等三部门联合部署开展为期半年的**邮政快递领域个人信息安全治理专项行动**，最终取得积极进展，累计侦破窃取、贩卖寄递信息案件 189 起，寄递企业信息安全基础得到进一步夯实；10 月 9 日，民

航局组织印发了**《关于民航大数据建设发展的指导意见》**，强调要强化安全管理责任和提升安全保障能力。

**（3）司法**

2 月 22 日，最高人民法院印发**《人民法院在线运行规则》**，要求各级人民法院应当确保智慧法院信息系统相关数据全生命周期安全，制定数据分类分级保护、数据安全应急处理和数据安全审查等制度；5 月 25 日，最高人民法院发布**《关于加强区块链司法应用的意见》**，提出充分运用区块链数据防篡改技术确保司法数据防篡改，提升数据安全水平，保障司法数据安全；6 月，最高人民检察院印发**《关于加强刑事检察与公益诉讼检察衔接协作严厉打击电信网络犯罪加强个人信息司法保护的通知》**，要求深入开展依法打击行业“内鬼”泄露公民个人信息违法犯罪工作，聚焦重点行业、重点领域、重点群体开展监督办案，包括处理大规模个人信息特别是个人敏感信息，容易产生个人信息泄露风险的重点行业；10 月 20 日，浙江省湖州市人民检察院等单位发布了**《执法司法信息采集及共享交换技术规范（征求意见稿）》**，对了执法司法信息的数据采集、数据处理和存储、数据传输、数据共享、数据交换和数据管理等方面的要求进行了规定；12 月 9 日，最高人民法院发布**《关于规范和加强人工智能司法应用的意见》**，明确要加强司法数据分类分级管理，强化重要数据和敏感信息保护，完善司法数据安全共享和应用模式。

**（4）医疗健康**

3 月 22 日，科学技术部发布**《人类遗传资源管理条例实施细则（征求意见稿）》**，规定将人类遗传资源信息向境外组织、个人及其设立或者实际控制的机构提供或者开放使用可能影响我国公众健康、国家安全和社会公共利益的，应当通过科技部组织的安全审查；5 月 10 日，国家发展改革委印发**《"十四五"生物经济发展规划》**，提出促进区域医疗健康数据安全有序汇聚与共享，支撑区域卫生健康大数据产业发展；5 月 11 日，国家药监局印发**《药品监管网络安全与信息化建设"十四五"规划》**，指出强化数据资源共享与大数据应用，积极探索大数据、人工智能、区块链、物联网、隐私计算等新技术在审评审批、监管检查、执法取证、全链条追溯等各类场景的应用潜力；8 月 8 日，国家卫健委等三部门印发**《医疗卫生机构网络安全管理办法》**，明确提出建立数据安全管理组织架构、每年对数据资产进行全面梳理、建立健全数据安全管理制度等数据安全管理要求；11 月 7 日，国家卫健委等三部门发布**《"十四五"全民健康信息化规划》**，明确要夯实网络与数据安全保障体系，并提出了数据安全能力提升行动。

**（5）其他行业/领域**

6 月 14 日，国家能源局发布**《电力行业网络安全管理办法（修订征求意见稿）》**，要求电力企业应当建立健全全流程数据安全管理和个人信息保护制度，按照国家和行业重要数据目录及数据分类分级保护相关要求，确定本单位的重要数据具体目录，对列入目录的数据进行重点保护；9 月 19 日，中国气象局印发**《气象数据开放共享实**

**施细则（试行）》**，进一步规范气象数据开放共享工作，推进气象数据安全、合规、有序开放共享，提升气象数据资源价值和应用效益；12 月 8 日，工业和信息化部印发**《工业和信息化领域数据安全管理办法（试行）》**，从数据分类分级管理、数据全生命周期安全管理、数据安全监测预警与应急管理、数据安全检测、认证、评估管理等方面对工业和信息化领域的数据安全管理提出要求。

## 6、主要地区积极推动政策法规的体系搭建，推动数据安全能力示范建设

### （1）上海市

1 月 13 日，上海市人民政府发布**《上海市推进治理数字化转型实现高效能治理行动方案》**，方案强调优化安全制度保障，按照相关法律法规要求，落实数据分类分级保护、信息安全等级保护和个人信息保护制度，健全安全风险评估、安全责任落实、安全应急处置等相关机制；2 月 18 日，上海市十五届人大常委会第三十九次会议高票表决通过了**《中国（上海）自由贸易试验区临港新片区条例》**，强调按照支持临港新片区推进国际数据产业发展，培育发展数据经纪、数据运营、数据质量评估等新业态，建立数据跨境流动、数据合规咨询服务、政企数据融合开发等公共服务平台；4 月 20 日，上海市发布**《上海城市数字化转型标准化建设实施方案》**，围绕“经济、生活、治理”全面数字化转型要求，通过研制实施一批能用、管用、好用的

数字化转型标准，构建具有系统性、协调性、开放性的城市数字化转型标准体系，为打造具有世界影响力的国际数字之都提供标准支撑；6 月 10 日，上海市通信管理局发布**《新型数据中心“算力浦江”行动计划（2022-2024 年）》**，将通过构建高性能算力为主的多元算力服务生态体系，依托上海新型互联网交换中心平台交换架构的独特性，探索打造全国首个算力交易集中平台，助力上海打造国际数字经济标杆城市；7 月 12 日，上海市人民政府办公厅发布关于印发**《上海市数字经济发展“十四五”规划》**的通知，在发展目标中指出要基本建立数据要素市场体系；8 月 5 日，上海经信委印发 **《2022 年上海市公共数据开放重点工作安排》**，推动公共数据开放机制巩固深化，制定公共数据开放细则，优化完善清单开放、分级分类、协议开放等工作机制；8 月 24 日，上海市委网信办、市政府办公厅（以下简称试点工作组）组织 16 家试点单位约 50 人召开**数据分类分级、制定重要数据目录试点工作会议**；9 月 23 日，上海数据交易所在“元宇宙大厅”发布**一站通金融数据交易板块**，支持各类金融数据要素对接，推进实现金融板块银行领域数据全品类覆盖，扩大交易规模，助力金融数据要素安全高效有序流通。

**（2）广东省**

2 月 28 日，**《广东省数字政府改革建设 2022 年工作要点》**印发，提出探索运用区块链、隐私计算等新技术强化数据安全防护，建设粤港澳大湾区大数据中心，健全大湾区数据基础设施体系；4 月 6 日，

**《广州市数字经济促进条例》**公布，为首席数据官、数据经纪人等创新试点提供法律保障；6 月，全国首批“**数据经纪人**”经广东省政数局批准同意诞生，在政府的监管下，围绕重点领域开展数据要素市场中介服务，推动数据流通规范化；6 月起，深圳数据交易有限公司率先在全国开展**数据商分级分类**工作，促进数据要素市场专业化分工体系形成，进而有利于数据要素市场的规模化发展；8 月 25 日，广东省发布**《广东省企业首席数据官建设指南》**，明确了数据安全职责包括建立企业数据资产安全保障制度和分类分级安全管理制度，组织制定并实施企业数据安全防护方案，提升数据全生命周期安全防护能力，定期组织数据安全评估等；11 月 15 日，**深圳数据交易所**正式揭牌，并发布了深圳数据要素市场及数据交易系列成果。

**（3）浙江省**

1 月 21 日，浙江省十三届人大六次会议审议通过**《浙江省公共数据条例》**，聚焦破解部门间信息孤岛、提升数据质量、赋能基层、保障安全等共性难题，推动浙江打造全球数字变革高地；5 月 18 日，国内设立的首个以受理数据资源案件为核心业务的专业法庭——温州市瓯海区人民法院**数据资源法庭**正式揭牌设立，覆盖个人信息侵犯、数字资源窃取、监管失职等案件；8 月 4 日，浙江省发布**《关于深化数字政府建设的实施意见》**，以数字化改革助力政府职能转变，不断提升政府治理体系和治理能力现代化水平，加快建设现代政府；10 月 19 日，**《浙江省推进产业数据价值化改革试点方案》**印发，提出

实施产业数据分类分级安全防护、推进工业领域数据安全管理试点工作、加强数据产品流通交易合规监管以提升产业数据安全化能力；11月8日，**《杭州市深化数字政府建设实施方案》**印发，提出要进一步强化政府部门数据安全管理职责，健全网络安全工作责任体系，强化网络安全、数据安全监管，构建数据安全防护能力评估指标体系，严格落实公共数据安全制度规范体系，完善公共数据安全技术防护体系等。

## 7、不同层级数据安全标准不断完善，促进数据处理安全有序发展

3月9日，全国信息安全标准化技术委员会印发 **《2022年网络安全国家标准需求清单》**，包括《信息安全技术 重要数据处理安全要求》、《信息安全技术 数据安全风险评估方法》、《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》等多项数据安全相关标准规范；7月21日，**GB/T 41574-2022《信息技术 安全技术 公有云中个人信息保护实践指南》**发布，对公有云中的个人信息保护作出指导；8月5日中国互联网协会发布 **T/ISC 0015-2022《金融场景隐私保护计算平台 技术要求与测试方法》**，提出了联邦学习参考架构、多方安全计算参考架构、可信执行环境参考架构，并从隐私保护计算能力、金融场景应用能力、原理架构安全能力、平台管理能力等方面明确金融场景隐私保护计算平台的技术要求；

9 月 20 日至 22 日，**国际标准《基于区块链的可信数据流通标准》**成功立项并正式成立工作组，定义了区块链可信数据流通平台的系统架构，规定了平台功能模块、数据流通流程和技术安全等要求；10 月 14 日，14 项国家标准正式发布，其中针对步态识别、基因识别、声纹识别、人脸识别、即时通信服务、网上购物服务、网络支付服务、网络音视频服务、网络预约汽车服务相关的**10 项数据安全标准规范**，均提到了开展上述相关服务的数据处理者应符合 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》中数据安全能力成熟度等级为 3 级或 2 级的要求；10 月 14 日，**GB/T 38664.4-2022《信息技术 大数据 政务数据开放共享 第 4 部分：共享评价》**发布，旨在推进政务数据高效有序共享，深化政务数据开发利用，提升政务数据共享的规范性、实效性和创新性；10 月 17 日至 28 日，联邦学习**国际标准《Assessment criteria of federated learning platforms》**立项成功，以指导联邦学习相关的实践方怎样以合理地方式评估联邦学习平台及主要的联邦学习算法；11 月 25 日，电信终端产业协会（TAF）公开发布 9 项电信领域团体标准，其中，《APP 收集使用个人信息最小必要评估规范 第 1 部分：总则》、《软件开发包（SDK）个人信息处理规范》、《基于差分隐私的用户个人信息保护技术要求》等 5 项标准对不同场景的个人信息保护技术提出要求。

# 二、2022年数据安全事件分析

2022 年，全球数据安全事件形势依旧严峻，数据泄露、数据加密勒索、数据合规等事件频发，且呈现爆发增长的态势，有组织、有目的的攻击形势愈加明显，数据安全风险持续增加。和 2021 年相比，大规模数据泄露事件依旧层出不穷，数据加密勒索事态恶化，成为全球面临的重大数据安全威胁之一，数据安全违法处罚事件所带来的严重后果亦为企业敲响数据安全风险的警钟。

## （一）整体态势分析

本部分基于大数据协同安全技术国家工程研究中心 2022 年发布的《全球数据安全观察》周报中收录的数据安全事件，从数据泄露、勒索攻击、数据合规三种类型进行统计和总结分析。

### 1、数据安全事件类型分析

如图 1 所示，从统计结果来看，数据泄露事件占 2022 年整体数据安全事件的 53%，在所有类型中占比最高；勒索攻击事件依然活跃度较高，该类事件占比为 30%；数据合规类型事件主要指由于数据违法违规问题而被监管机构处罚的事件，占比为 15%，相比 2021 年该类型事件的数量增加了 30.5%；其他类型事件占比为 2%，主要包括数据滥用、人为恶意删除等事件。

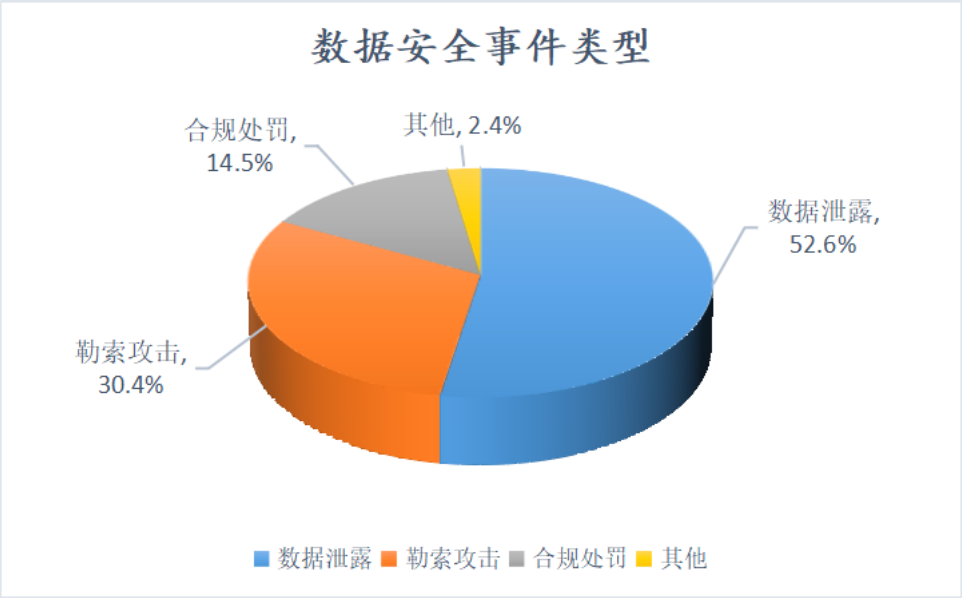



图 1 数据安全事件类型分布情况

## 2、数据安全事件行业分布

本报告里事件所属行业的划分，主要参考《国民经济行业分类》（GB/T 4754-2017）。对 2022 年《全球数据安全观察》周报里收录的数据安全事件所属行业进行统计分析，结果如图 2 所示：

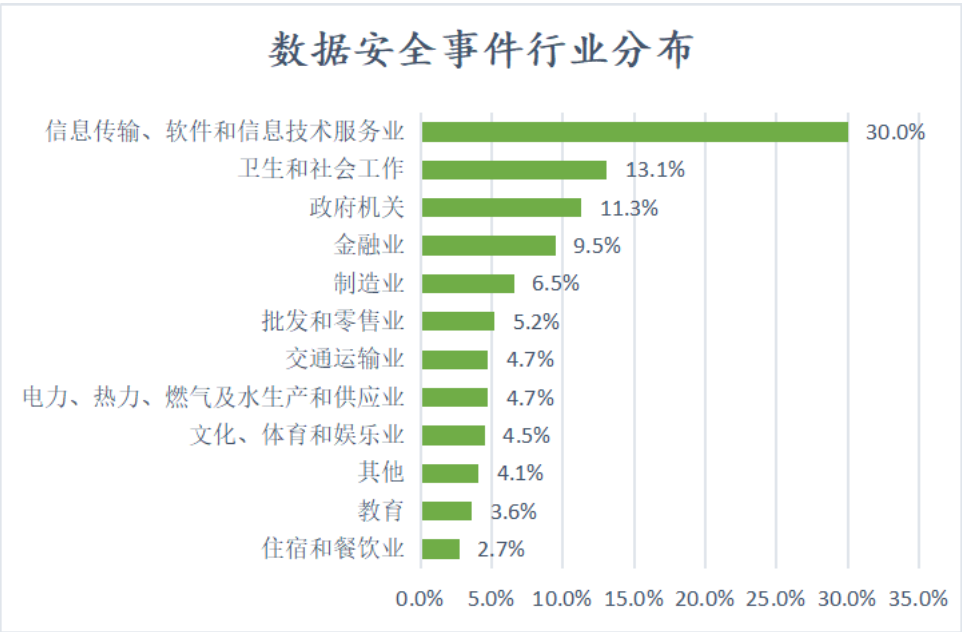



图 2 数据安全事件行业分布情况

信息传输、软件和信息技术服务业以30.0%的比例高居行业之首，反映了数字化程度越高的行业，越容易遭遇数据安全相关事件；卫生和社会工作行业是攻击者关注的重点，排在第二位，占比为 13.1%；政府机关依旧受到网络犯罪分子的青睐，以11.3%的占比排在第三位；金融业、制造业、批发和零售业也是数据安全事件频发的行业，占比均在5%-10%区间内；其次，交通运输业、供应业、文化、体育和娱乐业、教育业的占比相当，均为 3%-5%；住宿和餐饮业在本次分析中占比最低，为2.7%。

## （二）数据泄露事件分析

2022年全球数据泄露事件依旧层出不穷，数据泄露发生的频率、泄露数据量、泄露规模都在快速增长，以下从行业分布、泄露规模、泄露原因、泄露数据类型四个方面进行梳理和总结分析。

### 1、信息技术行业数据泄露事件频发

2022 年，数据泄露事件发生最多的行业为信息传输、软件和信息技术服务业，占比达30.3%。该类型包括门户网站、社交网站、电子通信、IT技术服务公司以及运营商等。

其次，随着新冠疫情的常态化爆发，卫生和社会工作大类行业数据泄露也较为严重，在所有类别中排名第二，占比为15.1%，该类型主要包括医疗机构以及健康服务中心等组织。

政府机关、金融、交通运输业、文化、体育和娱乐业分别以 12.2%、10.1%、6.3%位列第三、四、五位；电力、热力、燃气及水生产和供应业占比最低，为 2.1%。

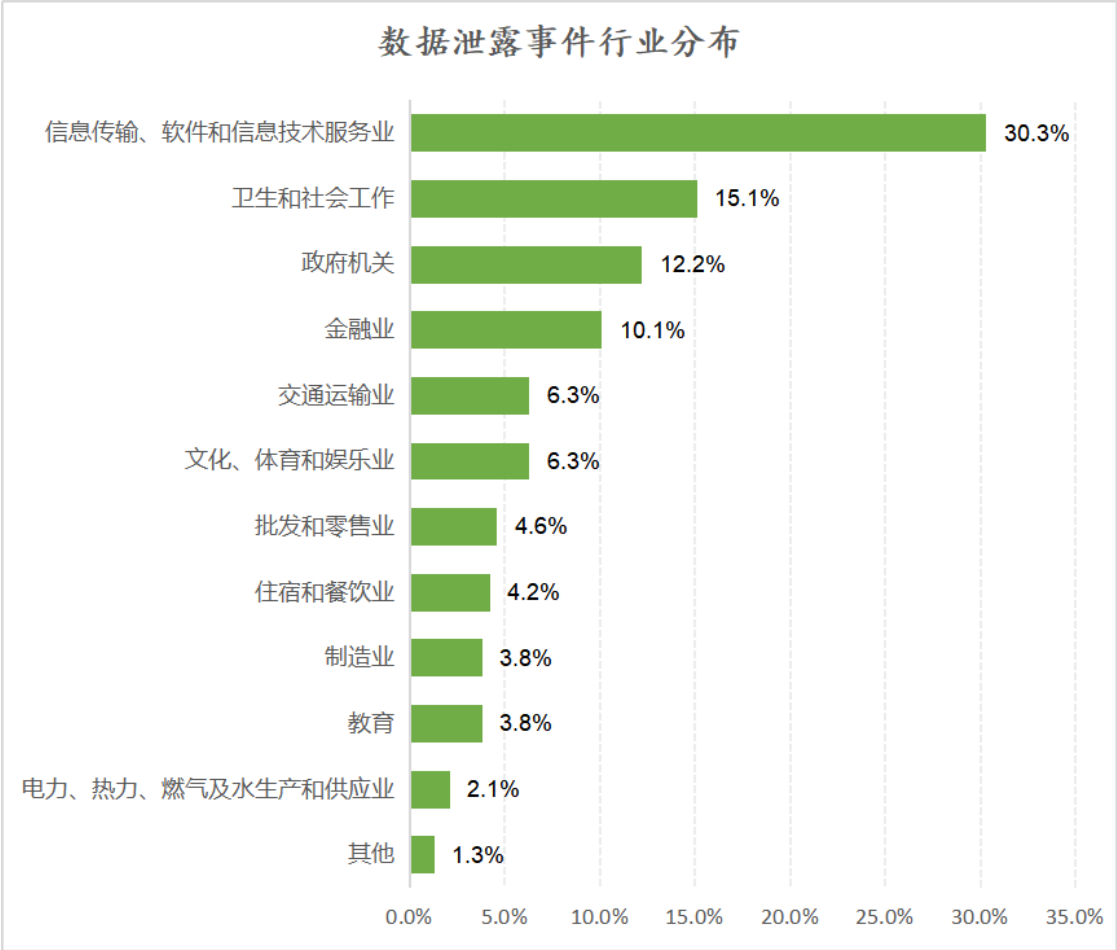



图 3 数据泄露事件行业分布情况

## 2、大规模数据泄露情况较为严重

从数据泄露的条数来看，大规模数据泄露情况较为严重，其中，数据泄露量级在 1 亿条以上的数据数据泄露事件占比高达 19.3%，100 万条以上的泄露事件更是占据了大半比例，达 57.9%。如下图 4 为数

据泄露条数占比统计，表 1 为泄露量在 1 亿条以上的典型数据泄露事件列举。

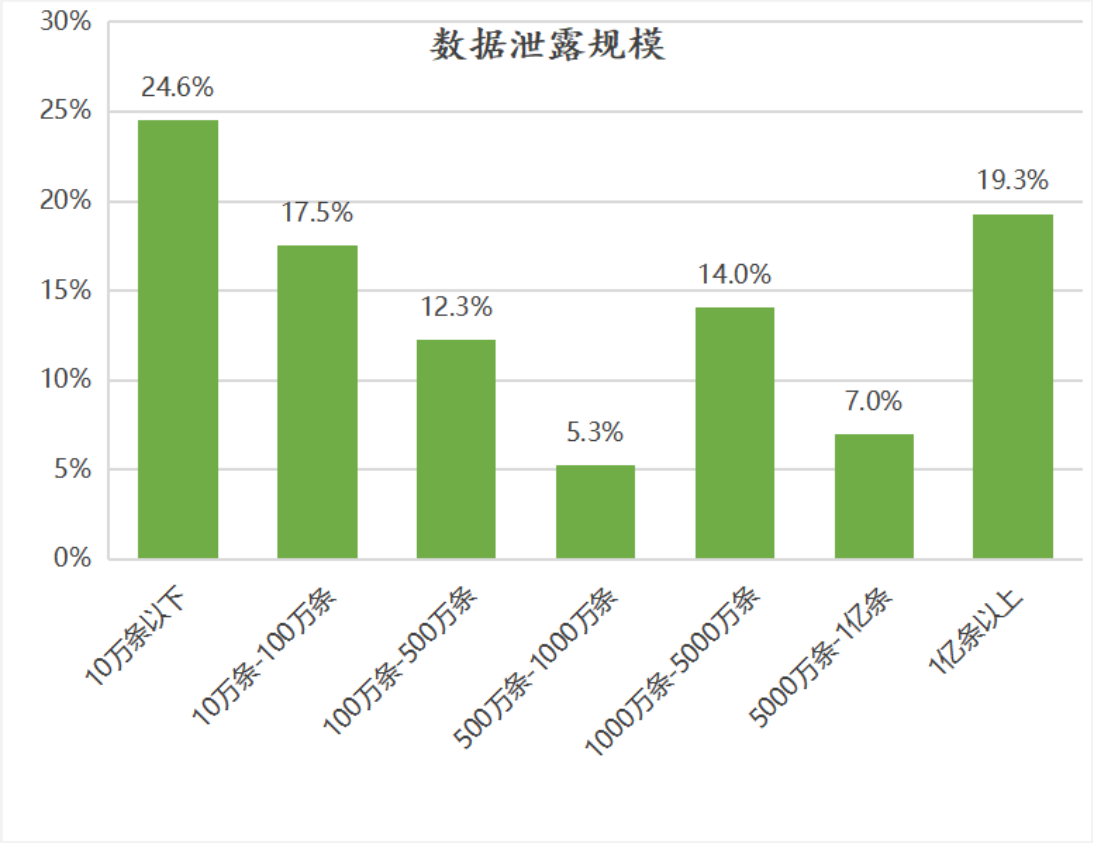



图 4 数据泄露条数占比

表 1 泄露量在 1 亿条以上的典型数据泄露事件

| 序号 | 时间 | 机构 | 事件 | 泄露数量 |
|---|---|---|---|---|
| 1 | 2022.05 | 乌克兰、哈萨克斯坦和俄罗斯公民 | 某配置错误的 ES 服务器泄露数百万贷款申请人的信息 | 8.7 亿条 |
| 2 | 2022.08 | 杭州新爱电子有限公司 | 一个庞大的中国人脸和车牌数据库在网上泄露 | 8 亿条 |
| 3 | 2022.06 | 持续集成开发工具 Travis CI | 数以万计开源项目开发账户遭大规模泄露 | 7.7 亿条 |
| 4 | 2022.11 | WhatsApp | WhatsApp 数据大泄露，近 5 亿条用户号码在暗网出售 | 5 亿条 |

| | | | | |
|---|---|---|---|---|
| 5 | 2022.05 | ElasticSearch 服务器 | ElasticSearch 服务器配置错误，暴露 579GB 用户网站记录 | 3.59 亿 |
| 6 | 2022.09 | 社交网站 Ask.FM | 黑客 Data 在暗网出售约 3.5 亿条 Ask.FM 用户的记录 | 3.5 亿条 |
| 7 | 2022.08 | 印度养老基金 | 2.88 亿条印度养老基金持有人的身份数据被暴露在互联网 | 2.8 亿 |
| 8 | 2022.11 | 亚马逊 | 泄露的 Amazon Prime 视频服务器暴露了用户的观看习惯 | 2.15 亿 |
| 9 | 2022.05 | 米高梅酒店 | 米高梅 1.42 亿条客户记录遭泄露，影响大约 3000 万人 | 1.42 亿条 |
| 10 | 2022.12 | 在线零售平台 Vevor | 在线零售平台 Vevor 服务器配置错误泄露超过 1 亿条记录 | 1 亿 |

从数据泄露的量级来看，1TB 以上泄露量的事件占比高达 24.2%，100GB 以上泄露量的事件占比为 42.4%，将近一半，该趋势和泄露的数据量级趋势一致，如图 5 所示。可见，大规模数据泄露形势严峻且占比量惊人。下表 2 为泄露量在 1TB 以上的典型数据泄露事件列举。

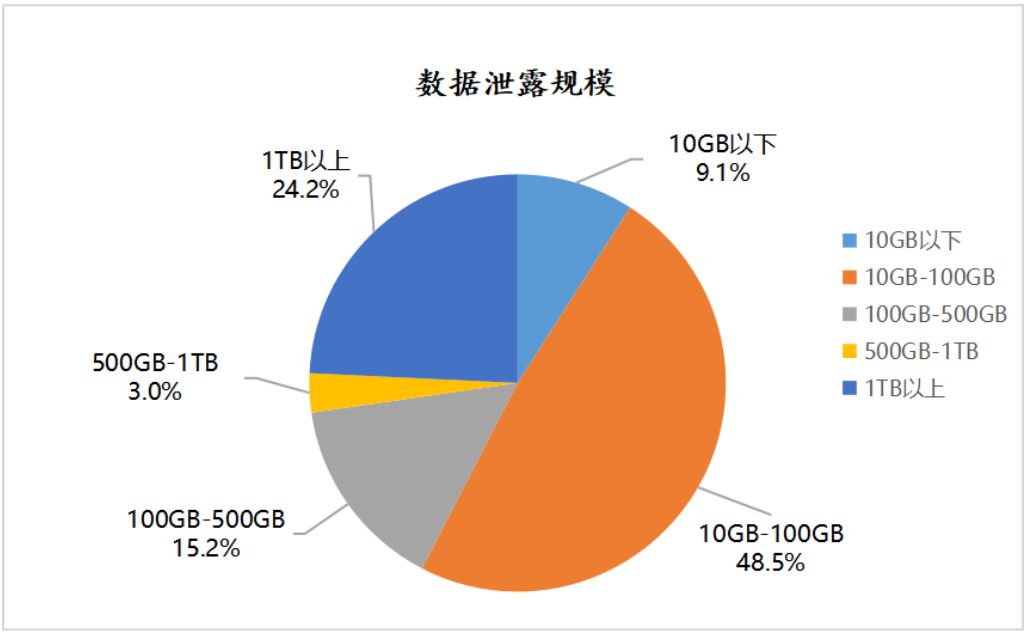



图 5 数据泄露量占比

表 2 泄露量在 1TB 以上的典型数据泄露事件

| 序号 | 时间 | 机构 | 事件 | 泄露量 |
|---|---|---|---|---|
| 1 | 2022.12 | McGraw Hill | McGraw Hill 的 AWS S3 存储桶配置错误泄露 22TB 数据 | 22TB |
| 2 | 2022.10 | 澳大利亚联邦警察 | 澳大利亚警方特工在哥伦比亚数据泄露事件中暴露 | 5 TB |
| 3 | 2022.03 | 美国征信巨头 TransUnion 的南非公司 | 南非公民征信数据全泄露：弱密码惹祸，美国巨头将赔偿超百亿元 | 4 TB |
| 4 | 2022.10 | 汤森路透公司 | 汤森路透 3 个数据库处于公开访问状态，至少包含 3TB 敏感数据 | 3TB |
| 5 | 2022.07 | 亚马逊 | 云配置错误暴露了 Amazon S3 存储桶中的 3TB 敏感机场数据 | 3TB |
| 6 | 2022.10 | 微软 | 微软数据泄露暴露全球 111 个国家超 6.5 万实体的客户个人信息 | 2.4TB |
| 7 | 2022.08 | 中美洲和南美洲多家矿业公司 | 黑客组织公开 2TB 电子邮件，揭露南美洲多家矿业公司内幕 | 2TB |
| 8 | 2022.10 | 英国保险公司 Kingfisher Insurance | 黑客称他们从英国一保险公司窃取了 1.4TB 数据 | 1.4TB |

从数据泄露影响到的用户规模来看，数据泄露影响的用户数量在 100 万以上规模的事件占比高达 39.3%，其中 1000 万以上用户受影响的占比为 8.5%，如图 6 所示。下表 3 为数据泄露影响的用户数量在 1000 万以上的典型数据泄露事件列举。

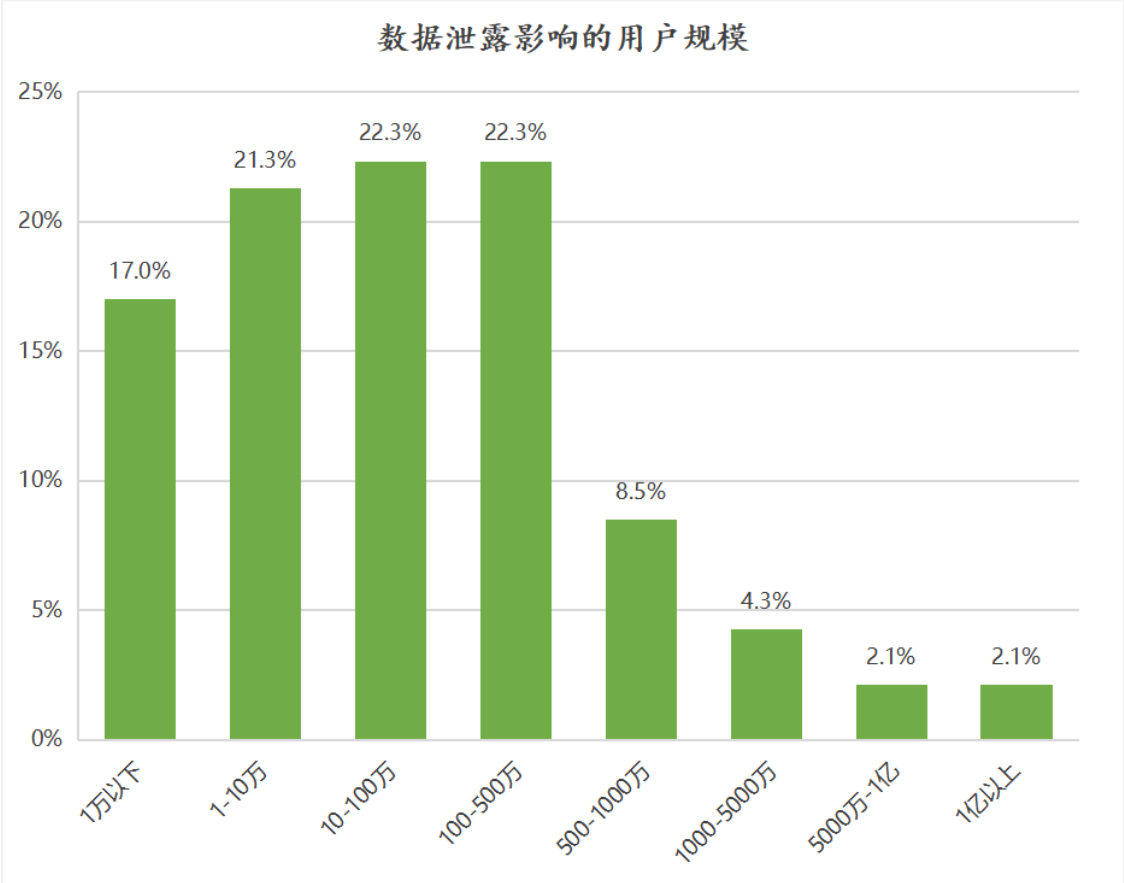



图 6 数据泄露影响的用户规模分布

表 3 数据泄露影响的用户数量在 1000 万以上的典型数据泄露事件

| 序号 | 时间 | 机构 | 事件 | 影响的用户数量 |
|---|---|---|---|---|
| 1 | 2022.09 | 印尼多家国有企业、手机运营商及大选委员会 | 一黑客兜售印尼 13 亿手机卡用户数据，公开嘲讽多名高官 | 13 亿 |
| 2 | 2022.12 | Twitter | 黑客出售 4 亿 Twitter 用户数据库 | 4 亿 |
| 3 | 2022.07 | 虚拟宠物网站 Neopets | Neopets 数据泄露暴露了 6900 万会员的个人数据 | 6900 万 |
| 4 | 2022.03 | 美国征信巨头 TransUnion 的南非公司 | 南非公民征信数据全泄露：弱密码惹祸，美国巨头将赔偿超百亿元 | 5400 万 |
| 5 | 2022.07 | 漫画阅读平台 | Mangatoon 数据泄露暴露了 | 2300 万 |

| | | | | |
|---|---|---|---|---|
| | | Mangatoon | 2300 万个账户的数据 | |
| 6 | 2022.05 | 国民登记局 | 2250 万马来西亚人的数据在暗网以 10,000 美元价格出售 | 2250 万 |
| 7 | 2022.05 | Telegram | 约 2100 万个 VPN 用户的个人信息在 Telegram 上被公开 | 2100 万 |
| 8 | 2022.09 | Swachh City 平台 | Swachh City 平台遭受数据泄露，涉及 1600 万条用户记录 | 1600 万 |

## 3、外部攻击仍为头号威胁，因配置错误导致的数据泄露多发

对数据泄露事件所发生的具体原因进行深入剖析，将主要原因归类为：外部攻击、配置错误、安全漏洞、内鬼、内部人员操作失误、第三方合作伙伴泄露、缺乏安全措施等，以下为主要结论。

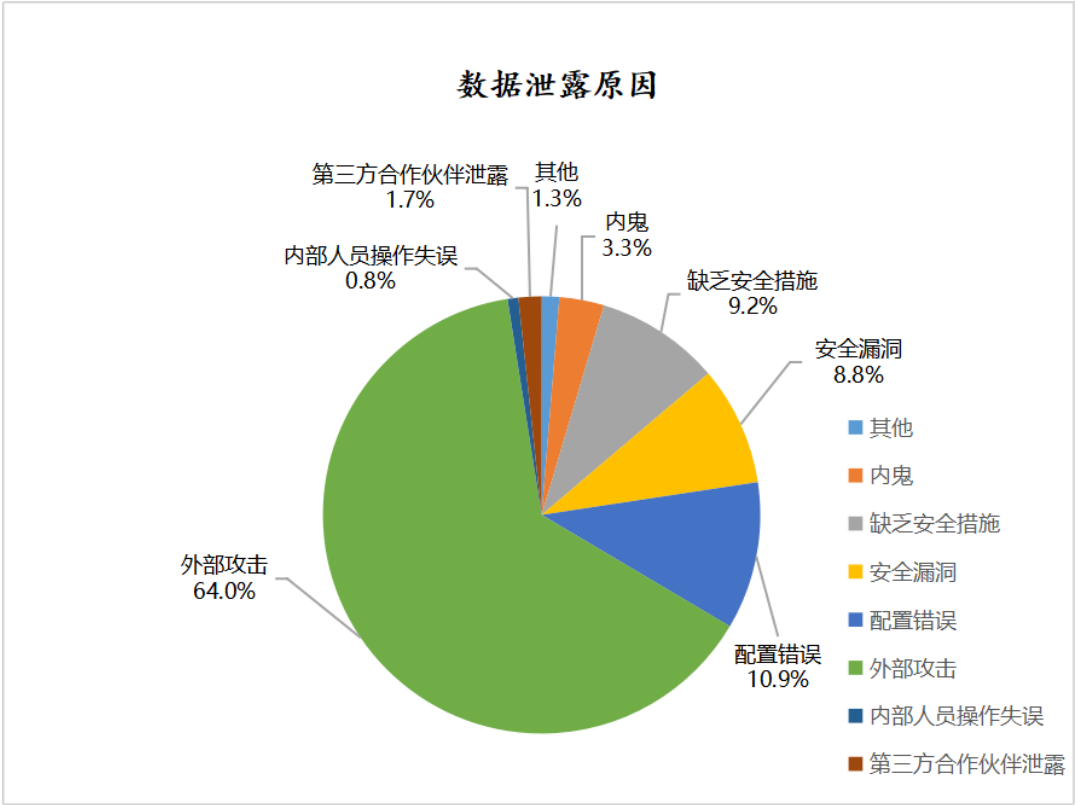



图 7 数据泄露原因

外部攻击是大部分数据泄露的罪魁祸首。本报告中共有 64.0%的数据泄露事件可以归因为外部攻击，具体原因包括黑客入侵、网络钓鱼及未经授权访问等；

配置错误是第二大原因，在本次分析中占有 10.9%的比例。主要原因包括服务器配置不当、云存储配置错误及开发人员错误配置等；

安全漏洞和缺乏安全措施也是导致数据泄露的重要原因，在本报告中均占据 9%左右的比例，其中，安全漏洞类型主要原因包括软件本身安全漏洞、安全机制缺陷、系统缺陷或数据库漏洞等；缺乏安全措施类型主要由数据库或服务器未做任何加密等安全措施引起，使数据公开暴露而导致泄漏；

其次，由于组织内鬼导致的泄露事件占据 3.3%，第三方合作伙伴原因导致数据泄露的占 1.7%，内部人员操作失误占比较小，仅为 0.8%。

## 4、个人信息泄露为数据安全“重灾区”

从泄露的数据类型来看，个人信息泄露最为严重，占据了 65.8%的比例，主要涉及姓名、电话、身份信息、银行卡、地址等；内部资料也是最常见的被泄露信息，21.3%的泄露事件涉及此类数据，其中，内部资料包括内部机密、企业商业机密信息、技术机密信息等数据；其次，8.8%的数据泄露涉及用户访问凭据，主要包括账号密码、口令信息、证书及其他证明身份的信息等。

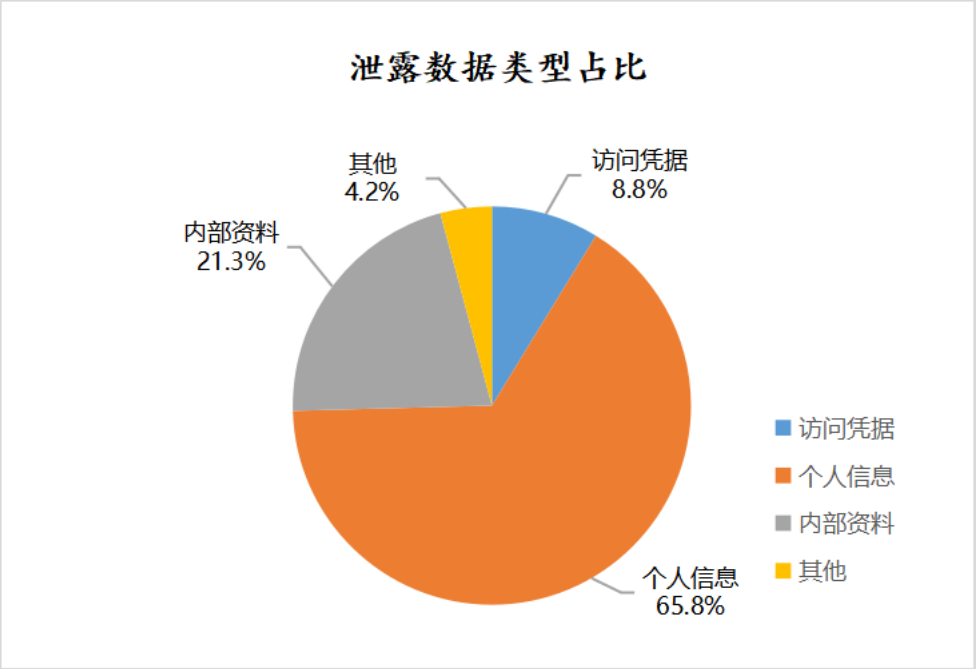



图 8 泄露的数据类型统计

## （三）勒索攻击事件分析

勒索软件攻击通过加密用户文件、绑架用户数据，以恢复系统和数据为条件向受害者勒索钱财，已成为目前最具威胁的攻击手段，且呈现逐年大规模增加的趋势。以下内容针对 2022 年勒索攻击态势进行了研究分析，并从行业影响、家族分布、赎金要求等多个角度进行了阐述。

### 1、信息技术服务业、政府机关和制造业是勒索攻击的重点目标

如图 9 所示，据统计，信息技术服务业、政府机关和制造业是遭受勒索攻击的重灾区。

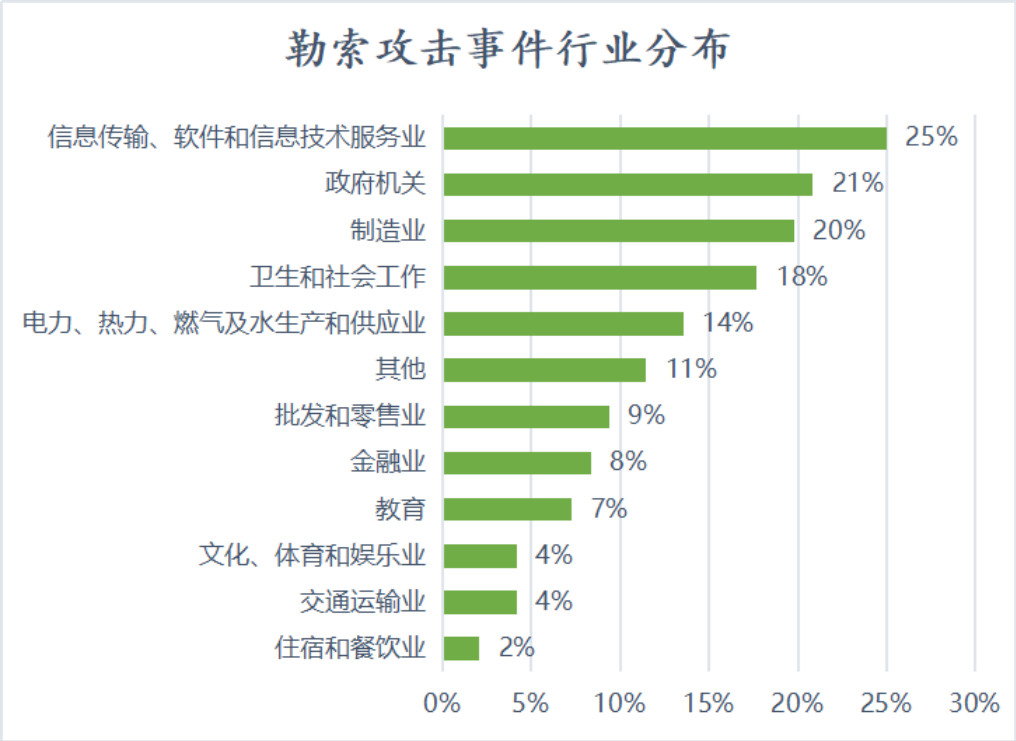



图 9 勒索攻击事件行业分布统计

在全球范围内，信息技术服务行业受勒索软件的影响最为严重，占整体攻击事件的 25%。成功攻击这一垂直行业引起的危害极大，信息技术行业多为提供服务的第三方，犯罪分子可能利用此为跳板从而立足于价值更高的目标。

政府机关是遭受攻击次数排名第二的垂直行业，占比达到了 21%，可见政府实体和关键基础设施依然是勒索软件攻击的重点对象；制造业以 14%的占比也同样成为勒索攻击的重点目标，该行业因勒索攻击或面临运营中断问题，造成的补救和恢复成本巨大，因此对于攻击者来说回报“丰厚”；由于个别勒索组织承诺不再攻击医疗机构或是其他可能导致个人死亡的组织系统，针对医疗卫生行业的攻击有所下降，

但在所有行业当中仍然占比较高，为 15%；此外，供应业、批发与零售业、金融业等行业也影响较重，占比均在 8%及以上。

## 2、勒索软件攻击伴随数据泄露已成趋势

如图 10 所示，在众多勒索攻击事件中，约 83%的勒索攻击伴随着数据泄露。

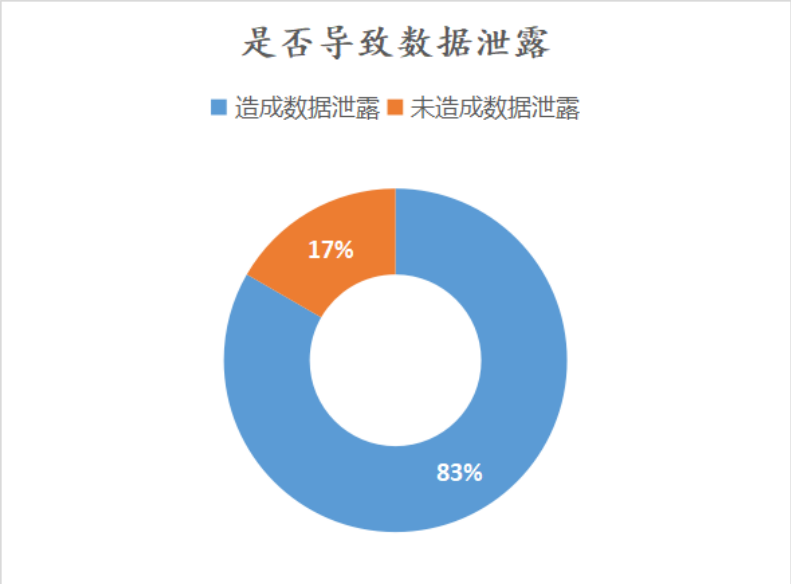



图 10 勒索攻击事件数据泄露情况统计

为了提高受害者的赎金支付率，诸如加密目标系统文件之前先窃取数据的“双重勒索”策略正变得越来越普遍。攻击者以“拒绝支付就泄露敏感数据”加以施压，逼迫受害者支付赎金，更有甚者直接在暗网倒卖窃取来的数据，以获取更大的利益。

## 3、20 余个勒索团伙持续活跃，LockBit 勒索病毒占比领跑榜单

在 2022 年的勒索攻击事件中，攻击活动最为频繁的是 LockBit 组织，占全年攻击事件的 14.3%；Hive 组织以 12.2%的占比排在活跃

度第二位；排名第三的 Conti 团队在 5 月正式关闭运营，基础设施下线。AlphV/BlackCat 和 Anonymous 组织今年也相当活跃，攻击了多个国家的重要机构和实体，例如俄罗斯太空研究所、中欧天然气管道公司、奥地利卡林西亚州政府、哥伦比亚能源供应商等。

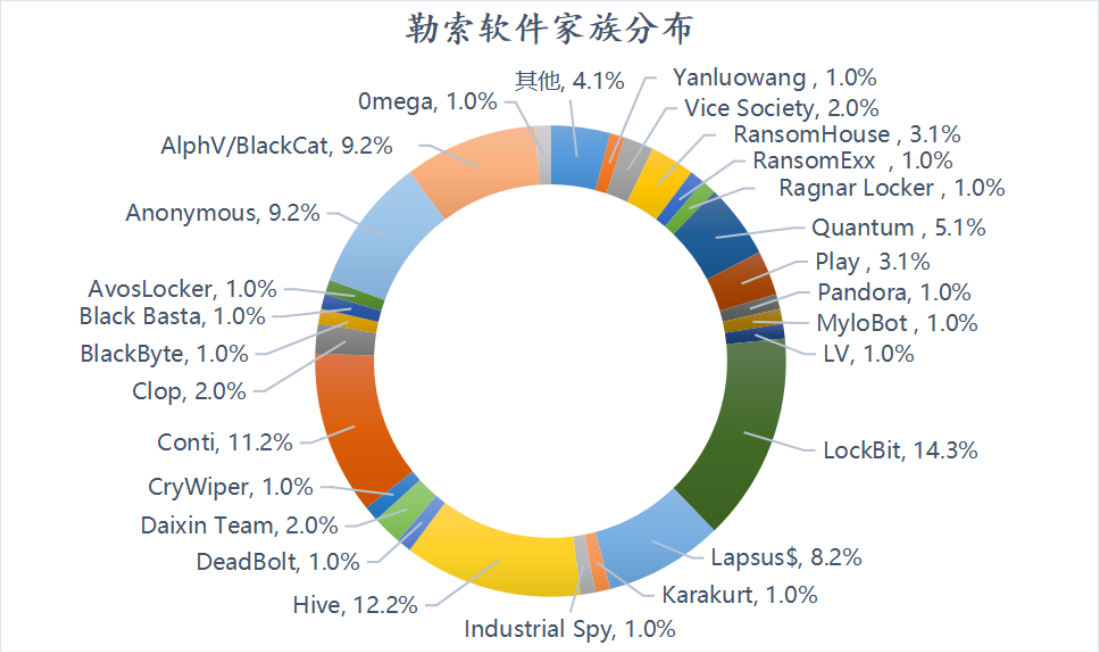



图 11 勒索软件家族情况统计

## 4、勒索攻击事件的赎金金额规模居高不下

勒索软件攻击事件的赎金规模不断攀升，如图 12 所示，勒索金额在 500 万美元以上的总占比就占到了 46%。索要 100 万-500 万美元勒索赎金的事件在所调查的勒索数额中占比最高，达到 31%。

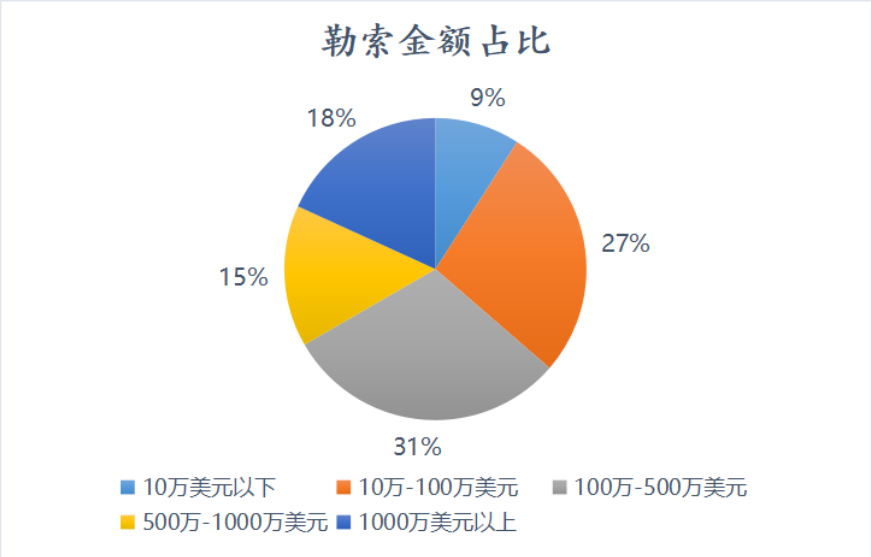



图 12 勒索金额情况统计

勒索组织通常“看碟下菜”，因此大型企业遭受恶意攻击后往往会被勒索更高额度的赎金，从而拉高了整体赎金规模水平。此外，由于多数被勒索的企业机构不愿披露勒索金额，本报告认为实际数据可能比已记录数据还要高。

## （四）数据合规事件分析

随着国内外对数据合规的监管不断加强，数据违法违规事件带来的后果也愈重，违反相关法规的主体可能被监管部门处以巨额罚款、暂停业务、停业整顿、吊销业务许可证等严厉的行政处罚，给企业组织带来巨额财务与信誉损失，影响日常经营和业务的持续发展。以下从行业分布、处罚金额、处罚原因三个方面对 2022 年的数据安全合规事件进行梳理和总结分析。

## 1、信息技术服务业与金融业易触及数据安全合规“红线”

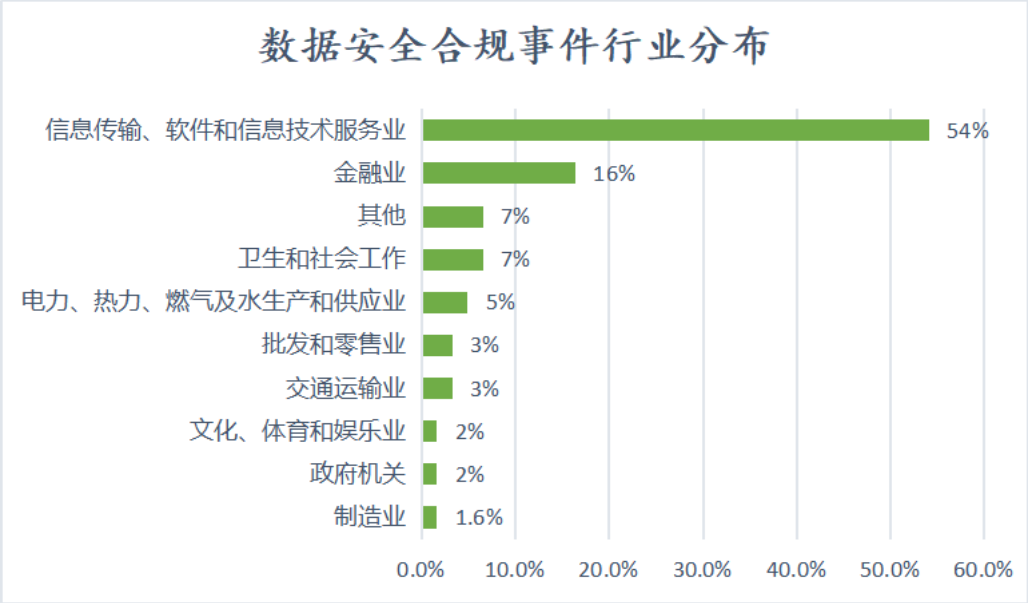



图 13 数据安全合规事件行业分布统计

根据图 13 的统计数据显示，数据安全合规事件主要集中发生在信息传输、软件和信息技术服务业，占比高达 54%。这主要是因为信息技术相关行业主体往往是提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，面对趋严的监管，稍有不慎就容易触及数据安全的“红线”。

金融业以 16%的占比排在第二位，随着各国在司法和行政监管方面针对个人信息保护的重视程度和保护力度不断加大，多家银行因个人信息保护问题被监管机构施以重拳。

## 2、针对数据安全违规事件的处罚力度只增不减，高额罚金案例攀升

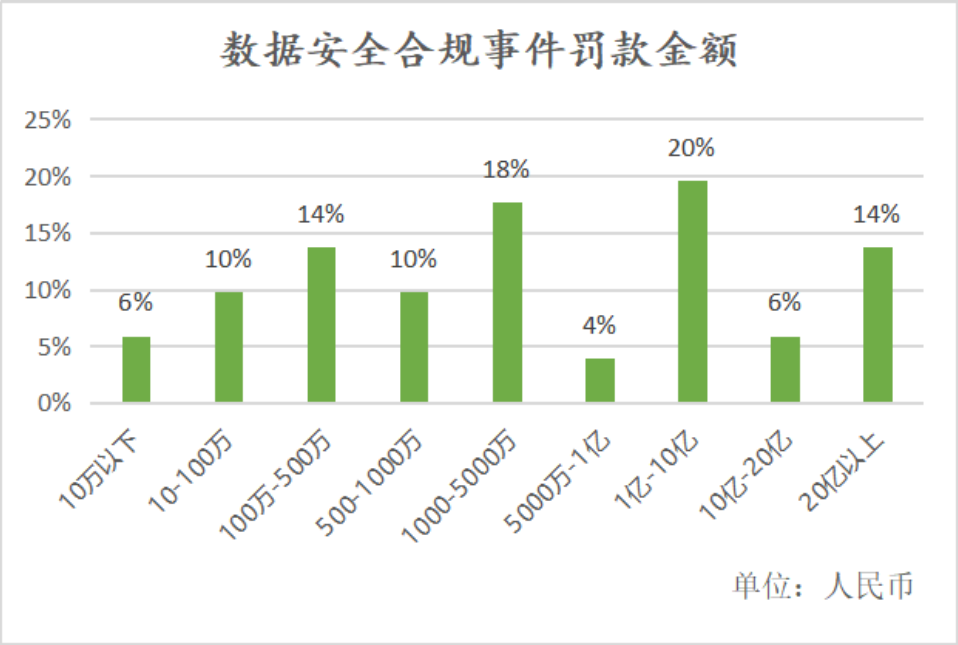



图 14 数据安全合规事件罚金统计

从图 14 已披露的罚款金额来看，罚金在 1 亿-10 亿区间的事件占比最高，达 20%；其次是处在 1000 万-5000 万的罚金，占 18%。其中，1 亿元以上的大额罚款事件就占了总体的 40%，如国家网信办对滴滴处以超 80 亿人民币重罚、谷歌脸书因违反欧盟隐私规定被罚超 15 亿元、美国 T-Mobile 对大规模数据泄露达成 5 亿美元和解、Meta 因泄露 5.33 亿用户数据被罚 2.65 亿欧元等案例。

从不断攀升的高额罚款案例可以看出，全球范围内相关执法机构与监管部门对于数据安全违规事件的处罚力度只增不减。而巨额罚款对某些企业来说可能是致命打击，将导致企业出现资金周转困难、信任流失等严重后果，从而失去市场竞争力。

## 3、安全保护措施的缺乏成为企业数据安全违规的主要原因

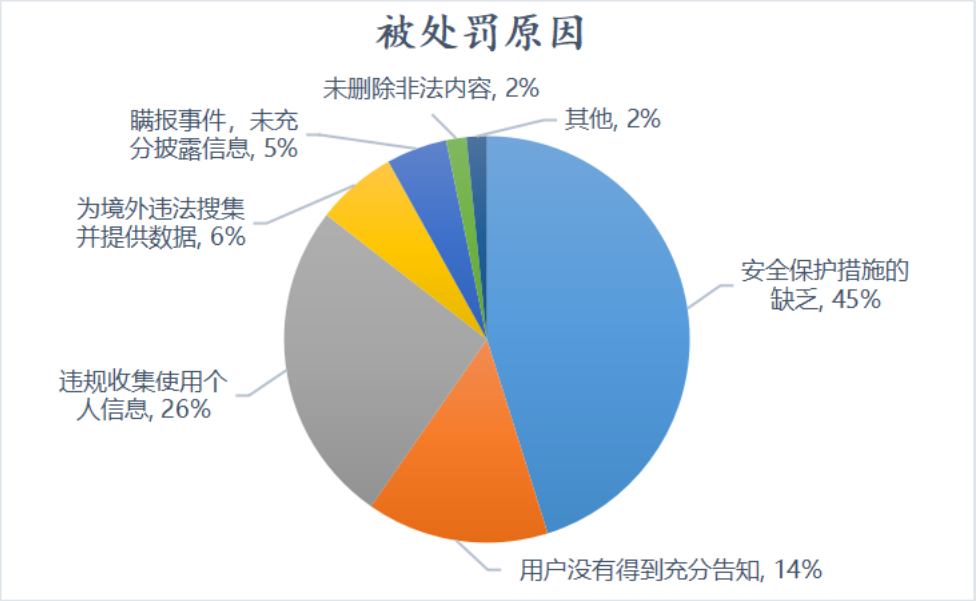



图 15 数据安全合规事件被处罚原因统计

如图 15，本年度数据安全合规事件的罚款原因主要包括：安全保护措施的缺乏（45%）、个人信息的不当收集与使用（26%）、处理用户个人信息未能充分告知（14%）、向境外非法传输个人数据（6%）、瞒报数据安全事件（5%）、未删除非法数据内容（2%）等。可以看出，监管多集中于企业收集和使用用户数据的合规性，以及数据采集、使用、存储等各方面的安全措施等。

归纳根因我们注意到，一方面，大量数据处理相关企业机构未采取有效防护措施履行数据安全保护义务，未能进行有效的敏感数据识别保护与针对性管控，而导致数据泄露的风险事件。另一方面，企业机构在开展业务的过程中，缺乏体系化的个人信息保护机制，加之内部监管不到位，致使业务在上线运行后，存在不当的个人信息收集、

存储和使用现象，且尚未经过个人信息主体的授权或同意，侵害了用户的合法权益。

数据安全能力建设是一件需要不断调整与优化的长期工作，我们需要从历史安全事件中反思不足，吸取宝贵经验及教训，不断指导数据安全能力建设工作持续开展。以下整理了 2022 年度有代表性的数据安全处罚事件，以此加强大家对数据安全的重视度，敲响警钟。

表 4 代表性数据安全合规处罚事件

| 时间 | 机构 | 罚金 | 起因 |
| --- | --- | --- | --- |
| 2022.01 | 东亚银行 | 1674 万元 | 违反信用信息采集、提供、查询及相关管理规定 |
| 2022.03 | Clearview AI | 2000 万欧元 | 违反欧盟《通用数据保护条例（GDPR）》，未经同意对用户的生物特征进行监控收集 |
| 2022.05 | 推特（Twitter） | 1.5 亿美元 | 滥用 1.4 亿用户数据，将其收集的用户个人数据用于非法销售广告，违反了联邦贸易委员会和 Twitter 之间的 2011 年同意令 |
| 2022.07 | T-Mobile | 3.5 亿美元 | 造成大规模数据泄露事件，暴露了多达 7660 万人的个人敏感信息 |
| 2022.07 | 滴滴 | 80.26 亿元 | 违反《网络安全法》《数据安全法》《个人信息保护法》，存在严重影响国家安全的数据处理活动，拒不履行监管要求，给国家关键信息基础设施安全和数据安全带来严重安全风险隐患 |
| 2022.07 | 欧盟委员会 | 未披露 | 传送居民 IP 地址等数据到美国，涉嫌 |

| | | | |
|---|---|---|---|
| | | | 非法传输数据，而且未能充分披露有关其数据处理的信息 |
| 2022.09 | 摩根士丹利 | 3500 万美元 | 在替换公司硬盘和服务器期间未删除敏感数据，泄露约 1500 万客户的个人信息 |
| 2022.09 | Meta | 4 亿美元 | 违反 GDPR，滥用儿童数据 |
| 2022.10 | 某科技公司 | 5 万元 | 违反《中华人民共和国数据安全法》，在处理政务类数据时违规操作，且未采取相应的技术措施和其他必要措施保障数据安全，导致数据存在泄露风险 |
| 2022.11 | 谷歌 | 3.91 亿美元 | 对其用户的位置数据进行不透明的跟踪和收集 |
| 2022.11 | Facebook | 2.65 亿欧元 | 违反 GDPR，未实施适当的技术和管理措施保护数据主体的权利，导致 5.33 亿用户的隐私数据泄露 |
| 2022.11 | 盘锦银行 | 140 万元 | 监管要求落实严重不到位、敏感数据信息存在泄露风险、外包管理职责存在缺失、瞒报信息系统突发事件 |
| 2022.12 | 法国电力公司（EDF） | 未披露 | 违反了 GDPR 的多个要求，使用了有已知漏洞的 MD5 算法，未使用随机“加盐”的方式对密码进行转换，并提供了“关于收集的数据来源的不准确信息” |

# 三、2022年技术、产品与市场趋势盘点

2022 年，数据安全技术与产品不断创新突破，标准逐步完善。技术、产品方面，隐私计算、量子计算、数据交易、分类分级等均实现了关键技术创新与应用突破；市场方面，DLP、隐私计算、数据安全服务等市场得到了快速发展，尤其是隐私计算技术。随着年底疫情防控的放开，数据安全市场将在 2023 年迎来发展良机。

## （一）技术、产品趋势总结

### 1、隐私计算重要技术持续创新，标准逐步完善，呈现多元化发展态势

**关键词：隐私计算技术创新 隐私计算标准 互联互通**

**隐私计算技术创新方面：一是**蚂蚁集团可信密态计算（Trusted-Environment-based Cryptographic Computing，简称 TECC）领域的“分布式多方安全计算系统、方法和节点”（CN113992439B）专利被授权。该技术根据资源消耗和任务可并行拆分程度的不同，可将 TECC 的计算速度提升 10 倍到 100 倍，实现在 1 小时内完成亿级样本密态 GBDT（Gradient Boosting Decision Tree，一种树模型集成算法）建模训练，在 10 分钟内完成亿级数据密态 SQL 分析，可以为顶级数据规模带来非常友好的计算体验，达到了隐私计算现阶段最佳性能效果，也使得 TECC 计算效率接近于数据非加密的明文计算。二

是由原语科技自主研发的隐私计算平台 Primihub 已正式在 GitHub 平台上开源：http://docs.primihub.com/。Primihub 平台融合了 MPC（多方安全计算）、FL（联邦学习）、HE（同态加密）、TEE（可信执行环境）等多种技术路线，提供多安全级别、多性能要求、多场景支持的解决方案，帮助企业用户保护数据隐私的同时，深度连接各个合作方，实现跨数据、跨行业的合作共赢。**三是**华控清交研发了业界首款半同态计算加速卡 TsingJ Homomorphic Processing Card X1（以下简称"TsingJ X1"），能够高效解决半同态计算的性能问题，大幅提升半同态计算效率。具体而言，无论是联合建模还是联合预测，两块 TsingJ X1 加速卡相对单颗 AMD 旗舰 CPU 而言能让每个参与方的计算性能提升 5 倍左右。

**隐私计算标准发展方面：**首个"隐私计算安全需求"国际标准立项，IEEE SA 标准委员会正式通过了"隐私计算安全需求"（Standard for Security Requirement of Privacy-preserving computation，P3169）国际标准的立项。该标准由蚂蚁集团主导，行业内专家共同参与，将对隐私计算技术本身潜在的安全隐患进行分析，并对隐私计算系统抵御的安全风险进行分级。目前，IEEE SA 已成立专门工作小组，蚂蚁集团牵头推进下一步实质性工作。全球首个 IEEE 隐私计算互联互通国际标准正式启动，6 月 21 日，IEEE SA 隐私计算互联互通标准 P3117《Standard for Interworking Framework for Privacy-Preserving Computation》（IEEE P3117）第一次工作启动会成功召开，标志着

全球首个隐私计算互联互通国际标准工作组正式成立并启动标准制定工作。


Gartner 2022 年新兴技术成熟度曲线列出了 25 项值得关注的新兴技术，其中隐私计算相关技术高达 6 项，占比 24%，堪称当前兼具潜力价值和讨论热度的前沿技术领域。市场方面，IDC 数据显示，2021 年中国隐私计算市场规模已突破 8.6 亿元，未来有望实现 110%以上

的市场增速。艾瑞咨询预计，到 2025 年，中国隐私计算市场规模将达到 145.1 亿元。

总体来看，隐私计算技术呈现多元化发展态势，包括多方安全计算、联邦学习、可信执行环境、同态加密等不同的技术路线，但商业环境尚未成熟，整体上市场还有很大上涨空间。当前，隐私计算发展呈现三大特点：**一是市场处于蓬勃发展的早期阶段，竞争格局尚未确定；二是产业发展环境、发展配套正在逐步完善；三是商业模式仍需进一步探索。**近年来，我国出台多项政策支持隐私计算发展，市场关注热度持续提升，未来几年国内隐私计算市场将迎来快速发展期。

（参考：“开放隐私计算”公众号）

## 2、量子计算技术在理论与应用方面均取得显著进步

**关键词：量子密钥分发技术 量子安全系统**

6 月 6 日，加拿大量子安全公司 Quantropi,Inc.在加利福尼亚州旧金山举行的 RSA 大会上展示了其最新的量子安全加密产品——SEQUR™ SynQK，该产品可生成并以数字方式分发同步的量子密钥。Quantropi 的 SEQUR™ SynQK 有效地打破了几个世界记录，在 4000 到 15000 公里的距离内以 130 到 190 兆每秒的速度同时传送至少 5 个量子密钥流(5 个数据流中的每一个都相当于 Google.com 每秒使用的 8 - 12 倍)。SEQUR™是 Quantropi 的 TrUE 加密解决方案系列中的熵产品，此产品系列提供量子密钥生成和分发功能。目前，该

系列产品包括 SEQUR™ QEaaS、SEQUR™ NGen 和最新发布的 SEQUR™ SynQK。

IBM 推出了下一代大型机系统 IBM z16，搭载人工智能处理器和量子安全系统，可为人工智能、混合云、量子计算、开源等领域提供充分支持。IBM z16 **集成量子安全系统，为数据安全保驾护航**，除应对欺诈活动外，还可应用于诸如货币加密、贷款审核、防止盗窃等产业。IBM 以普及加密和机密计算技术为基础，采用网格密码学技术，在 IBM z16 上增加了一个保护组织免受未来技术，以破解当今加密文件威胁的量子安全系统。

量子计算应用方面，10 月 11 日消息，金融服务巨头万事达卡（Mastercard）推出抗量子技术非接触式支付卡，该卡结合了量子密码技术，旨在防止当前经典计算机和未来量子计算机的黑客攻击；11 月 19 日，谷歌宣布启用抗量子密码(或 PQC)，避免未来黑客使用量子运算技术，破解当前经加密的资料。11 月 24 日消息，SSH 公司宣布即将推出全球首款用于大型机的量子安全数据通信软件 Tectia

SSH Server for IBM z/OS。通过量子安全升级，该软件可以与 6 月发布的 Tectia 客户端/服务器及相关第三方应用程序进行通信，创建安全远程访问、文件传输以及大型机出入连接隧道，从而实现大型机用户的文件传输、终端连接具有量子安全性能。

（参考：信息安全与通信保密杂志社、安全内参）

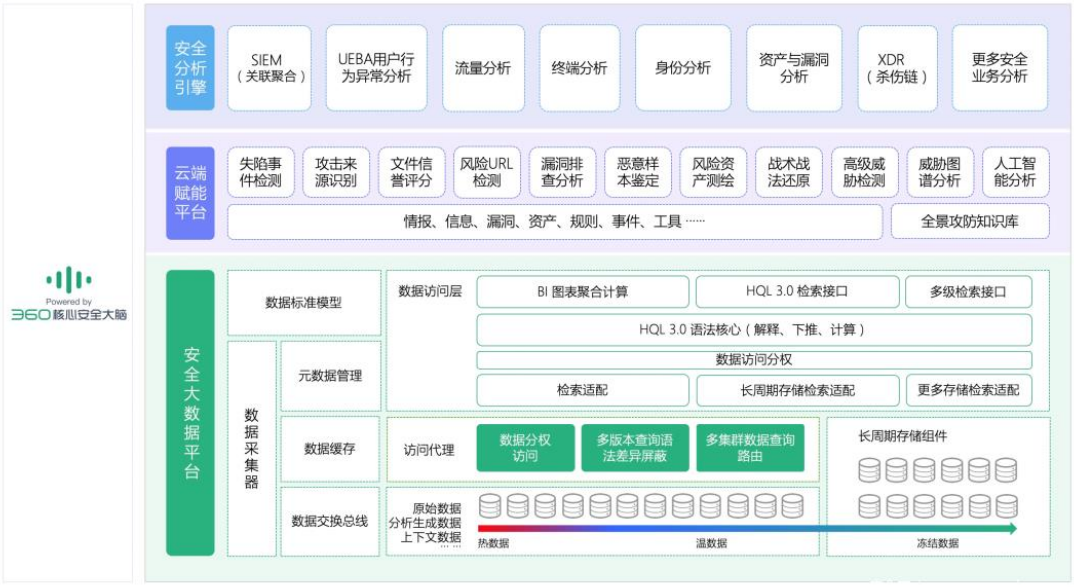
## 3、安全大脑助力用户构建“能力中枢平台”，带动数字时代能力体系升级

**关键词：安全大脑 数字安全 能力体系**

在数字时代安全威胁不断演进的今天，对数字安全体系化、实战化提出了更高的要求。但越来越多政企用户清晰地看见——自身的网络安全建设存在着企业设备各自为战、生态产品难以联动、外部能力无法融合等多重协同壁垒。

在此背景下，360 政企安全集团正式推出 360 核心安全大脑 3.0。具体构成上，360 核心安全大脑 3.0 由一个安全大数据平台、一个云端赋能平台和多个安全分析引擎，以及内嵌 360 十七年经验所积累的实战方法论组成。其中安全大数据平台通过模型化管理的数据标准，接入各类安全数据使之集中管理，并在内部融合数据品类，协调数据流程决策与步骤，为安全业务提供从数据接入到存储、清洗到运算，最终到图表展示的全生命周期一站式服务。安全大数据平台具有“运

营商”级别的数据处理能力，助力提升安全运营中的数据处理效率 5 倍以上。




云端赋能平台通过云地协同、能力下沉，为安全设备提供从漏洞到资产、从情报到知识、从线索到规则、从事件到态势等百余种基础的安全数据及分析能力，可以满足各类安全设备的通用化威胁检测与分析需求。此外 360 核心安全大脑 3.0 中还预置了近百类安全分析引擎，2000 多个安全策略，可以把专业相关的分析能力通过配置组合的方式赋能特定的安全产品，应对纷繁复杂的安全业务，从多个维度指导安全设备发现、防护高级别网络威胁，提升自身网络安全能力。

（参考：安全客）

## 4、数据交易所掀建设热潮，交易平台迎来蓬勃发展

**关键词：数据交易 交易所 交易平台**

2022 年全国数据交易所建设明显加快，仅下半年，苏州大数据交易所、广州数据交易所、深圳数据交易所、杭州国际数字交易中心先后揭牌。据不完全统计，截至 2022 年 12 月，国内已公布的（含筹建）的大数据交易所（中心）已有 46 个。

1 月 11 日，湖南大数据交易所正式投入运营。该交易所是继贵州、陕西、北京、上海之后的全国第五家、中部第一家新型大数据交易所。交易所运营后预计 5 年内营收达到 5 亿元，并实现公司上市。

7 月 26 日，福建大数据交易所正式揭牌。交易所将探索大数据资源合规交易、有序流通、高效利用，建立全省一体化的数据要素交易市场。当日，完成挂牌的数据产品近 100 个，涉及能源类、金融类、通信类、征信类等类别，并完成了首批交易。

9 月 16 日，苏州大数据交易所正式揭牌。苏州大数据交易所依托苏州市公共数据开放平台、苏州大数据交易平台两大平台，支持数字金融、数字制造、数字文旅等 N 个应用创新的“1+2+N”运营模式，不断整合公共数据、社会数据、算法算力等多方资源，打造具有苏州特色的数据资源化、资产化、价值化商业模式。

9 月 30 日，广州数据交易所正式揭牌。广州数据交易所采用“一所多基地多平台”体系架构运营，按照“省市共建、广佛协同”的思路，引入央企控股及省市区龙头国企优势资源建设，为区域数据交易服务设立多基地。当日，首批数据经纪人、数商企业签约进场，在交易所

已申请挂牌的交易标的超 300 个，进场交易标的超 200 个，并达成首日交易总额超 1.55 亿元。

11 月 15 日，深圳数据交易所正式揭牌，同时启动首批线上数据交易。深圳数据交易所以建设国家级数据交易所为目标，从合规保障、流通支撑、供需衔接、生态发展四方面，提升覆盖数据交易全链条的服务能力。截至目前，深圳数据交易所完成登记备案交易 415 笔，交易金额超 11 亿元，覆盖金融科技、数字营销、公共服务等 53 类应用场景，其中跨境交易 14 笔，交易金额 1115 万元。

12 月 12 日，在杭州国际数字交易中心正式揭牌。该交易中心聚焦数据可信流通与数字文化，在数据要素服务和数字资产交易双赛道齐发力。截至目前，杭州国际数字交易中心已与 215 家企业建立合作关系，上架产品 428 件，实现 457 笔数据业务交易，累计实现交易金额超 13 亿元，其中海外交易金额 2065 万美元。

国家工业信息安全发展研究中心发布的《2022 年数据交易平台发展白皮书》显示，从交易平台发展趋势上看，数据产权制度日趋受到关注，各大数据交易平台将以数据登记、技术赋能数据权益使用等多种形式探索破解数据确权难题。数据应用场景不断拓展，参与交易流通的数据类型从金融数据将逐步扩展到医疗、交通、工业等多种类型的数据。隐私计算等技术加速应用，将进一步助力数据要素安全流通。公共数据日益成为交易平台数据的重要供给源，而数据交易平台

也彰显出越来越大的公共价值，开始反哺数据产业发展。数据交易上下游产业链开始浮现，有望在未来形成商业生态。

（参考：中国大数据产业观察）

## 5、自动化分类分级工具在数据安全供方市场蓬勃发展

**关键词：数据分类分级 数据资产 智能化分类分级**

数据分类分级正在持续发展和越发完善，市场上自动化程度较高的数据分类分级工具尤为受欢迎。从 2019 年 “等保 2.0”推动各行业的数据分类分级工作萌芽，到 2021 年《数据安全法》明确提出要对数据实行分类分级保护。随着政府、金融、运营商等各行业分类分级制度的相继发布，各行业开始迫切需要自动化程度高、人工参与少的分类分级工具，进而对海量数据进行有效数据分类分级管理。

据中国信通院“可信数安”评估体系统计，2022 年分类分级工具或服务的参评企业从 2021 年的 4 项增加至 14 项。通过研发智能化的分类分级平台来提升数据分类分级的整体效能成为一大趋势。

2022 年 2 月 25 日，御数坊智能化数据分类分级工具 DGOffice 顺利通过了中国信通院的数据分类分级工具评测，其利用 NLP、机器学习、知识图谱等技术，以智能模型的驱动方式实现数据资产的分类分级，通过智能化分类分级的应用节省大量的人力投入；2022 年 9 月 6 日，天空卫士发布《数据安全治理自动化技术框架（DSAG）》白皮书，其中提到通过自然语言处理、自动聚类技术、以及深度学习

等技术对海量的数据进行自动的分类分级，将人工干预降到最少，并在需要人工介入的环节通过工具和界面做到智能辅助。

（参考：通信世界全媒体、数据安全推进计划、“天空卫士SkyGuard”公众号、“天融信”公众号）

## 6、AI 赋能数据安全，助推数据安全防护能力提升

**关键词：人工智能 敏感数据智能识别 异常行为分析**

IDC 定义下的变革型技术将会彻底重塑市场及技术投资策略，其可以创造新的市场机会、新的技术公司以及新的用户需求。其中的细分项“AI 赋能数据安全”技术聚焦人工智能在数据安全市场的应用，可以运用在数据的收集、清洗，数据分类分级、脱敏、加密、防泄露、数据安全运营等诸多领域，以提高数据安全检测监测、分析、防御效果。

在数据分类分级、用户异常行为分析、数据指纹溯源和智能控制策略推荐方面，采用 AI 技术都能够帮助企业更好地完成数据安全治理。美国人工智能计算公司英伟达发布云原生应用程序框架 Morpheus，利用机器学习检测识别网络钓鱼、数据泄露等威胁；思科与数据安全解决方案提供商 Securiti 合作，利用基于人工智能的数据隐私和安全保护技术，实现能源、制造业等行业敏感数据的有效识别、跟踪和精细控制。

在 AI 赋能数据安全异常行为分析模型方面，安恒信息基于敏感对象表元素频度访问、敏感对象的操作类型、访问源的行为、去参数化的语句模板、去参数化的应用 URL 行为等，形成多样的数据分析模型，从而自动发现危险的用户数据访问行为。

在敏感数据智能识别方面，明朝万达利用 AI 技术，通过分析上下文语义，识别敏感数据，具有识别类型宽泛，识别颗粒度细等优势；百度推出智能数据安全网关，支持基于 AI 模型的敏感数据识别，可以对姓名、地址、毕业院校等正则无法识别的敏感信息进行识别。

（参考：IDC TechScape、“安恒信息”公众号、数据安全推进计划）

## （二）市场洞察

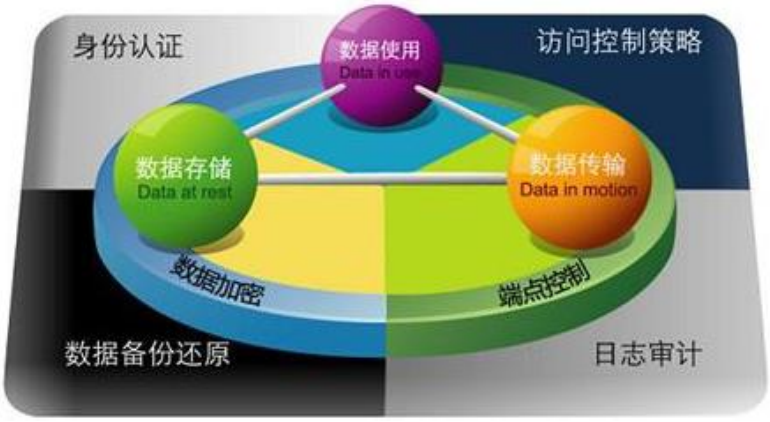
### 1、企业数据泄露防护 (DLP) 市场年复合增长高达 21%

**关键词：DLP 市场规模**

根据 Research And Markets 最新发布的调查数据，未来五年全球企业数据泄露防护（DLP）市场预计将以 21.03%的复合年增长率高速增长，到 **2026 年市场规模将达到 62.65 亿美元**，而 2019 年为 16.47 亿美元。

DLP 解决方案可按照网络、存储/数据中心、端点、服务、咨询、系统集成、培训等不同应用领域进行分类。根据部署模式，DLP 还可分为内部部署和云端防护两大类。由于云数据丢失防护为电子邮件、

USB 驱动程序、笔记本电脑和移动电话提供了解决方案，因此预计云 DLP 细分市场将会进一步增长。




从垂直行业来看，新兴行业中越来越多地开始使用企业数据丢失防护，此外，航空航天和国防、通信和技术、政府、医疗、制造和其他行业的 DLP 市场也将以高复合年增长率增长。

（引用来源：安全内参）

## 2、IDC 发布《中国数据安全服务市场洞察》：数据安全服务引领全流程数据安全体系建设

**关键词：数据安全 安全服务**

IDC 对众多安全厂商和最终用户进行了深入访谈，发现最终用户在其数据安全建设前或建设过程中普遍面临数据安全建设无从入手、摸清家底难、分类分级落地难、对于数据安全风险和建设成果的无感知以及缺乏专业的数据安全建设治理人才等问题。针对以上痛点，IDC 给出以下几点建议供技术买家参考：

**（1）数据安全体系建设是“一把手”工程。**数据全生命周期的安全体系建设涉及到众多的利益相关方，仅 IT 部门的管理者很难推动业务部门和其他部门协同共同建设。企业的数据安全体系需要自上而下推动，“一把手”亲自抓、亲自控才能真正协同各部门责任共担，共同建设，最大程度地发挥安全产品和服务的效能。

**（2）数据安全需体系化、阶段化、模块化建设。**数据安全建设前期需要做好体系化建设规划，根据权责划分等管理制度，分阶段、分业务、分模块进行建设。这一过程中，数据安全的战略与规划服务将更好地在深入业务的基础上帮助最终用户规划建设蓝图、管理制度和实施方案，从而帮助用户解决数据安全建设杂乱、难入手等问题。最终用户需要明确的是，数据安全规划建设方案是需要根据业务的变化、数据的变化等不断进行调整更新，才能逐步建成自适应的管理体系。

**（3）清晰、明确的组织架构和管理制度是企业数据安全体系建设的“地基”。** 组织架构、管理制度的制定可以帮助用户明晰权责，做好分配和管理，并在其基础之上建设标准的组织管理运行机制和体系，是企业进行数据安全体系建设规划的第一步，更是企业未来数据安全体系良好运行的保障。

**（4）分类分级、数据治理是组织建好、管好数据安全的前提。**数据资产的梳理、分类分级工作对组织来说意义重大，是后续一系列产品和服务发挥安全作用的基础和前提条件。

**（5）数据安全建设需服务先行。**最终用户在购买数据安全服务时需要重点关注服务提供商的服务全面化、流程化能力、服务场景化、行业化能力、服务团队能力以及服务质量和效果的评估能力。

**（6）数据安全教育和培训是一件需要长期坚持的事。**数据安全的意识培训、技能培训未来将成为数据安全领域的基础服务，是企业需要广宣传、持续坚持的一项重要活动。定期开展数据安全、个人信息保护相关的服务培训将潜移默化地提升整体企业人员安全意识水平，从而提高整体企业安全水位，对于企业业务长期稳定发展具有重要意义。

（引用来源：安全内参）

## 3、Gartner：2025 年 60%的大型企业机构将使用隐私增强计算技术

**关键词：隐私增强计算 Gartner**

Gartner 日前发布了 2022 年银行和投资服务行业的三大热门技术趋势，分别是：**生成式人工智能（生成式 AI）、自主系统和隐私增强计算。**这三项趋势将在未来两到三年内继续增长，推动金融服务机构的增长和转型。


隐私增强计算（PEC）能够保障在不可信环境中处理个人数据时的信息安全，而随着隐私和数据保护法的不断发展以及消费者的日益关注，这一点正变得越来越关键。隐私增强计算运用各种隐私保护技术使金融服务机构在从数据中获取价值的同时满足合规要求。

Gartner 预测，**2025 年 60%的大型企业机构将在分析、商业智能或云计算领域使用一种或多种隐私增强计算技术。**

数据在金融服务领域的各种分析、计算和数据变现工作中都起到了不可替代的作用。金融服务机构正越来越多地在欺诈分析、智能运维和数据共享等应用中采用 PEC。

（引用来源：环球网）

## 4、Gartner：2022 年云计算支出将达到 5000 亿美元

**关键词：云计算 Gartner**

根据研究公司 Gartner 的数据，今年全球在公共云服务上的支出将接近 5000 亿美元，到 2023 年将达到 6000 亿美元。云原生基础设

施服务的日益普及被认为是关键驱动因素之一，但疫情大流行驱动的混合工作场景的趋势也发挥了作用。


**基础设施即服务(IaaS)** 预计将在 2022 年实现最高的最终用户支出增长，达到 30.6%，作为云堆栈的基础级别，支撑着每一个主要的以消费者为中心的在线产品和移动应用程序。第二高的增长将是**桌面即服务(DaaS)**，增长 26.6%，因为混合工作促使组织不再使用台式机等传统客户端计算解决方案为员工提供动力。由于对云原生功能的需求，在最终用户支出增长中紧随 DaaS 的是**平台即服务(PaaS)**，其支出达到 1096 亿美元，比 2021 年增长 26.1%。

随着核心云服务的成熟，提供商之间差异化的重点正在转移到可以直接破坏企业数字业务和运营的能力上。云计算中的新兴技术，如超大规模边缘云计算和安全访问服务边缘(SASE)，正在扰乱相邻市场并形成新的产品类别，进而为公共云提供商创造额外的收入来源。Gartner 预计，将云与此类新兴技术相结合的组织将在其数字化转型之旅中取得最大成功。

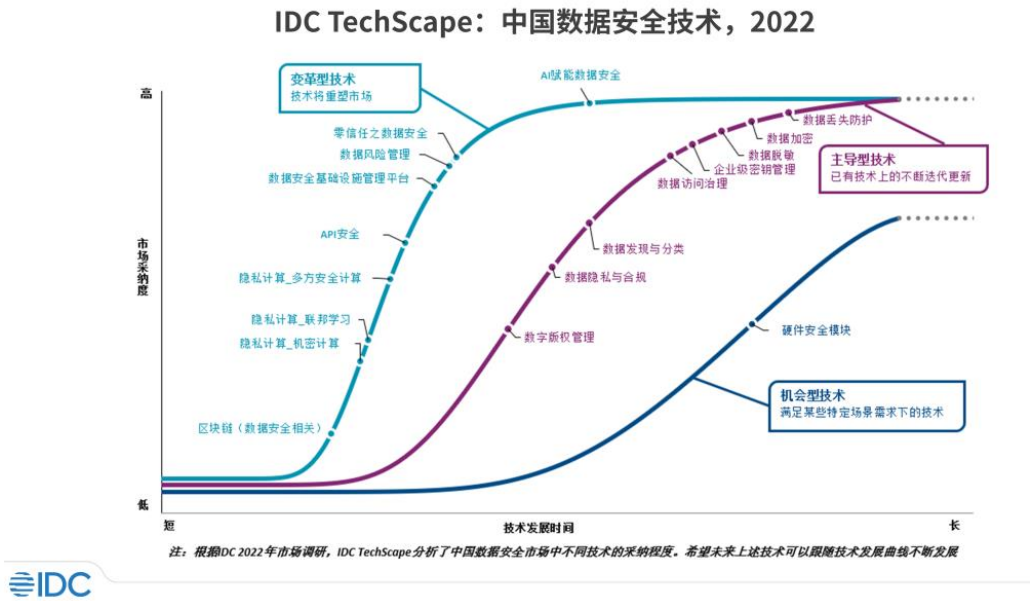
（引用来源：theregister.com）

## 5、IDC 发布 2022 年中国数据安全发展路线图

**关键词：IDC 数据安全**

8 月 29 日，IDC 2022 CSO 全球网络安全峰会（中国站）在上海隆重开幕，会上首次发布《IDC TechScape：中国数据安全发展路线图，2022》。报告认为，**帮助用户构建全方位数据安全治理体系将成为大趋势**，各项数据安全和密码技术将在治理体系中作为重点能力模块，赋能用户实现数据安全治理目标。

本次发布的 TechScape 选取了 18 个新兴及重要的数据安全技术进行分析，并对数据安全技术的市场采纳度进行了可视化展示。此外，根据技术的市场影响以及各技术的发展阶段将技术分为**变革型技术、主导型技术以及机会型技术**三大类别，并给出了每项技术的三个推荐厂商。



**变革型技术**将会彻底重塑市场及技术投资策略，其可以创造新的市场机会、新的技术公司以及新的用户需求。此类技术可能与现有技术存在很大的区别并且可能存在大多情况下难以辨认的市场影响或机会。包括：**AI 赋能数据安全、API 安全、零信任之数据安全、区块链（数据安全相关）、数据安全基础设施管理平台、隐私计算-安全多方计算、机密计算、联邦学习。**

**主导型技术**是指在现有技术的基础上进行了可衡量的迭代更新，以提供更好的业务成果。包括：**企业级密钥管理、数据丢失防护（DLP）、数据发现与分类、 数据访问治理、数据加密、数据脱敏、数据隐私与合规、数字版权。**

**机会型技术**将基于具体的落地场景来发展，它们在改进现有技术/流程方面的能力不确定或有限，其适用于某些特定领域的创新技术。包括：**硬件安全模块。**

（引用来源：安全内参）

## 6、Gartner 发布 2022 年中国安全技术成熟度曲线

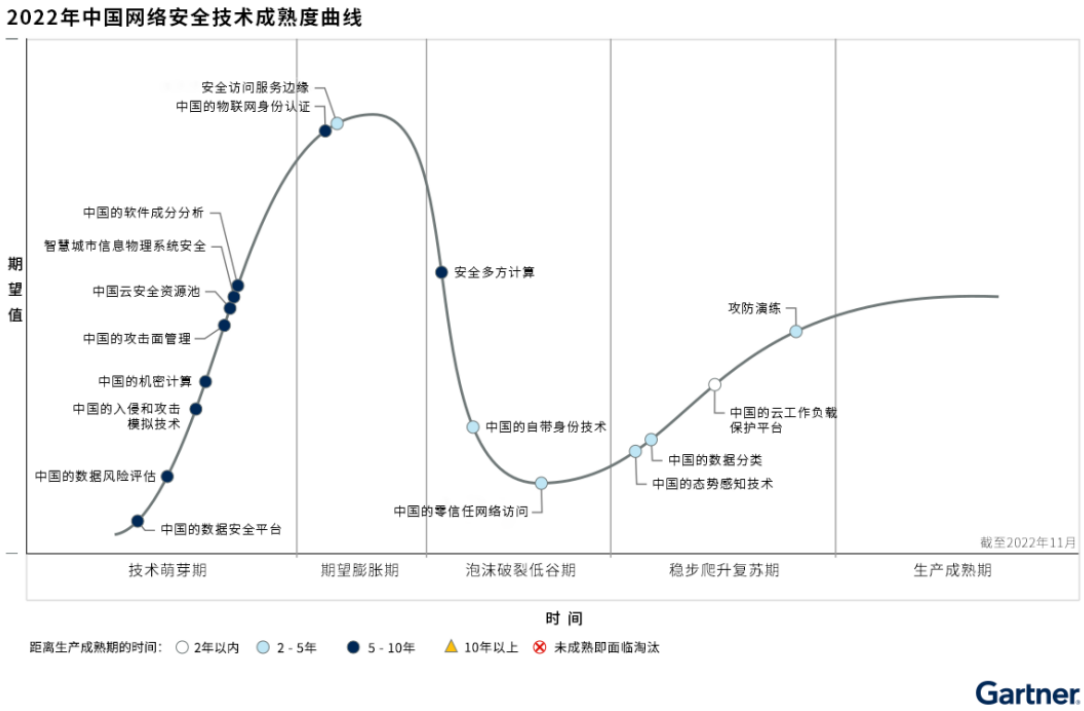
**关键词：安全技术成熟度 Gartner**

Gartner 于 2022 年首次发布《2022 年中国安全技术成熟度曲线》，该曲线指出，随着国内数字化转型的推进，尤其是云计算、大数据、人工智能、物联网和电子商务的发展，企业机构数字资产保护已成为安全和风险管理领导者的关键任务。

国内法规日趋严格，安全的重要性更甚以往。这篇报告是全新的中国安全创新领域技术成熟度曲线。中国安全技术与市场，在技术成熟度、产品、供应商等方面与国际市场存在差异，因此针对国内特点筛选了一批创新安全技术和服务。

报告中，**萌芽阶段**包括**数据安全平台**（Data Security Platforms）、**数据风险评估**（Data Risk Assessment ）、**入侵与攻击模拟**（Breach and Attack Simulation，BAS）、**机密计算**（Confidential Computing）、攻击面管理（Attack Surface Management，ASM）、云安全资源池（Cloud Security Resource Pool）、智慧城市网络物理系统安全（CPS Security in Smart Cities）、软件组成分析技术（Software Composition Analysis）；**膨胀阶段**包括物联网认证（IoT Authentication）、安全访问服务边缘(Secure Access Service Edge，SASE)；**破裂阶段**包括**安全多方计算**（Secure Multiparty Computation ，SMC）、自备身份（BringYour Own Identity，BYOI）、零信任网络访问（Zero Trust Network Access，ZTNA）技术；**破裂阶段**包括**态势感知**（Situational Awareness）、**数据分类**（Data Classification）、云工作负载保护平台(Cloud Workload Protection

Platforms)，CWPP)、攻防演练（Attack and Defense Teaming）。




（引用来源：安全内参）

# 四、数据安全优秀实践案例

为深入贯彻习近平总书记关于“要切实保障国家数据安全”的重要思想，落实《数据安全法》、《个人信息保护法》等法律法规，不断完善数据安全产业供给能力和生态体系，保障数据要素充分开发利用，为数字经济持续健康发展筑牢安全屏障，宣传推广一流的方案、技术和产品，BDS 国家工程研究中心于 2022 年 11 月开启了“2022 年数据安全优秀实践案例”征集活动。

社会各界相关单位积极响应、踊跃参加，活动收到了众多应用在政务、交通、公安、电信、金融、医疗、能源等行业领域的实践案例，涉及数据流通共享安全、数据安全合规治理和数据安全保障等方面。经中心审核申报材料，并邀请来自中国网络安全审查技术与认证中心、中国信息安全测评中心、北京市政务信息安全保障中心、信息产业信息安全测评中心、中科院信工所、中科院软件所、北京大学、北京科技大学等单位 8 位专家，从实践案例的合理性、相关性、实用性、先进性和开放性五个方面进行综合评审，最终遴选出了一批优秀行业数据安全解决方案实践案例和优秀数据安全技术与产品实践案例。

## （一）优秀行业数据安全解决方案实践案例

### 1、基于隐私计算的一体化政务大数据开放平台

该案例是深圳市洞见智慧科技有限公司（洞见科技）申请，由洞见科技和智慧齐鲁公司合作，为山东省大数据局建设了国内首个省级政务数据隐私计算平台，已于 2021 年 10 月正式上线运营。该平台采用隐私计算技术，有效提升公共数据通用支撑和服务管理等能力，完

成多方安全协同计算与企业数据资源合规市场化、安全应用化、价值最大化，安全有序地推进各政府部门和公用事业单位等公共机构数据资源向社会分级分类开放和流通应用，进一步提高了政务大数据融合流通的服务质量及效率。

技术方面，平台实现了隐私计算技术的重要突破，基于多方安全计算和可信联邦学习双引擎设计，保证了数据安全性及模型精确度；支持跨平台互联互通，实现多个厂商隐私计算平台的无缝对接；应用无可信第三方联邦学习技术，较大程度上提升了算法性能；采用算法容器框架设计，使算法可以在计算框架内自定义设计、实现和执行。

应用方面，实现了数据价值的“重组式”创新和跨域数据开放融合业务应用全生命周期安全保障；外部政务大数据分布式统一访问应用机制，实现外部政务大数据分布式访问和对异构应用访问的适应性；良性闭环的数据价值链生态，打通跨域数据的应用价值链；加快推进数据在数字金融、智慧城市等领域的场景应用和生态建设。

## 2、基于“城市大脑”的政务大数据安全治理

该案例由天津市武清区大数据管理中心申请，基于“城市大脑”的政务大数据安全治理项目通过组织、人员、资金、制度等保障，坚持内生安全理念和网络安全“三同步”原则，针对天津市武清区政务大数据全流程、全覆盖、多层次安全防护。该案例核心内容是对网络及数据安全风险的识别、防护、监测及服务的四个维度，协同区网络安

全态势感知系统，发挥数据态势感知持续运营监测能力，通过“城市大脑”赋能增效，最终达到项目“党管数据”的整体目标。

（1）体系建设创新性。该案例高标准形成区县级政务大数据“平台防护+安全治理”的“1+1”安全模式，建立武清区政务大数据的安全保障体系，覆盖数据中台、基础库、专题库，制定形成武清区《数据安全管理办法》《数据安全分类分级指南》《数据安全能力成熟度评估报告》《数据分类分级清单》《典型业务数据活动场景 SDL 建模图》《典型业务系统数据流向视图》《数据安全技术保护体系设计》等 10 项管理制度和标准。

（2）技术应用先进性。该案例依托国内知名网络安全和云服务商的核心技术，基于对业务系统零影响的流量解析技术，实现对象化的梳理监测、画像分析和涉敏管理；采用非侵入式数据流动动态监测、对象化的数据流动安全管理、业务化数据流动视图构建，建立安全视角的数据流动态势。

（3）性价比和实用性。该案例通过部署数据安全网关、数据库静态脱敏、数据防泄露等系统，开展数据安全治理，组织数据分类分级、重要系统数据流向梳理及场景调研，已梳理 18 个重要业务系统数据资产清单，确认结构化数据字段 86901 个。通过集约化建设，已为智慧武清“城市大脑”、重点专项应用以及全区各单位相关业务系统的网络及数据安全防护基础设施建设累计节约资金上千万元。

## 3、合规监管的金融反欺诈解决方案

该案例由神州融安数字科技（北京）有限公司（融安数科）申请，可为金融集团应用融安隐私计算平台合法合规使用内外部数据，提高反欺诈风控模型精度，加强风险识别能力。

融安隐私计算平台是以密码技术为基础，整合多方安全计算（MPC）和联邦学习（FL）两个计算引擎，综合同态加密、隐私求交、匿踪查询等高效隐私计算组件，实现在保证数据流通过程中不泄露原始数据的前提下，对数据进行分析和计算，确保敏感数据在存储、计算、应用、销毁等数据流通全流程各个环节“可用不可见”。

方案中应用融安隐私计算平台多方安全计算引擎实现金融集团、运营商、电力公司三方联合计算，输出企业信用评分，用于金融反欺诈场景；方案创新性的引入第三方监管机构，应用融安隐私计算平台合规监管技术框架中的隐私度量技术、参数一致性监管技术、匿踪计量计费技术等一系列密文监管技术对交易全生命周期合规监管，在数据流通合规监管方面做了有意义的探索和实践。

## 4、金融公共数据专区安全监管

该案例由北京中安星云软件技术有限公司（中安星云）申请。金融数据专区通过对批量导入数据和接口服务数据进行加工处理和模型算法向合作机构提供数据服务。中安星云项目组为确保金融公共数

据专区使用数据合法合规使用，监管引导金融公共数据更好地服务金融机构和小微企业，规划进行以下四项服务：

一是在深入调研金融公共数据专区，梳理金融公共数据专区资产，然后进行组织、服务体系、数据资产、对接接口服务、专区数据管理总体情况调研等，为后续工作做准备；

二是部署网络安全专业监测工具，通过专业的工具和数据安全服务，定期进行漏洞检查、API 服务监测、个人信息探测、日志和数据库审计等，逐步剖析金融数据专区数据管控和运营监测等方面存在的问题，形成周报和月报；

三是研发一套流程管控和运营监测可视化系统，与大数据平台及现有系统对接集成，提供数据汇聚监测、个人信息脱敏、数据服务授权、接口服务调用、企业注册和服务量化等可视化服务，推进数据安全管控和运营监测。

四是开展数据安全检查和合规评估，通过数据安全专家和法律专家共同对金融公共数据专区的数据处理进行安全检查和合规性评估，提出针对数据专区的数据管控制度和技术体系建设等方面的建议和实现路径，形成数据专区数据管控和运营管理研究报告。

为金融公共数据专区建立了一套完整的数据安全防御系统，为数据汇聚共享提供了基本安全保障，理清并掌控数据资产的分类分级、防止数据被非授权使用、滥用、破坏及泄露窃取的风险，提高对数据安全事件的检测、分析、识别及处置水平。

## 5、省经信厅数据安全建设

该案例由杭州美创科技股份有限公司（美创科技）申请，案例通过数据风险评估、数据安全权限管控系统、数据脱敏系统、数据水印系统、数据安全能力集中管控等建设，有效提升省经信厅产业数据仓数据安全防护水平，一期已成功部署在省经信厅核心业务，其中涉及产业数据仓平台、产业链一键通、数字经济系统企业分系统、包含产业数据仓落地场景，重点防护敏感产业数据资产。

整体的实施分为以下四个步骤：

（1） 数据安全风险评估。结合自动化工具进行安全能力评估、合规能力评估、全生命周期评估，生成全面风险清单、风险预估及风险处置建议方案。

（2）建设规划及安全建设。基于风险现状规划数据安全架构和建设路径，完成防护措施加固，包括身份鉴别、访问控制、流动管控、运维管控等。

（3）安全能力集中管理。建立集中安全管控平台，实现安全能力集中管理、策略统一下发、安全态势感知、实现数据安全全域可管、风险常态化监管。

（4）持续化支撑防范。通过运维保障、应急响应、定期评估及整改加固等安全能力支撑，实现安全风险持续防范，安全能力持续改进优化。

该案例提供了一套针对数据仓/信息中心数据安全建设的整体解决方案，通过构建零信任数据安全体系架构，部署先进的数据安全技术等手段，有效提升数据安全能力水平，保障政府数据开放共享，目前该方案已成功推广至多个政府部门并具有良好成效。

## 6、数安行金融大数据安全计算与安全计量

该案例是北京数安行科技有限公司（数安行）申请，来源于某证券公司数字化转型背景下建设的项目。该证券公司在业务方面积累了大量的客户数据，公司期望在对数据充分分析、开发利用的基础上做商业模式的调整，但大数据的计算、分析意味着给这些数据可能带来新的问题，比如哪些数据具有更高价值，如何计量数据价值；计算分析过程中，计算节点上会积聚数据，这个积聚数据的规模超出以前公司使用数据的历史经验，一旦发生问题，当前的数字化转型必然受到影响。

通过该项目的建设，一方面保障了公司数字化转型中数据开发、利用的数据全链路的安全；另一方面符合金融监管机构、证券业监管机构对数据安全的监管合规性要求；同时还为数据资产的价值计量提供有效的手段，为公司在数据创造价值方面开拓新的商业盈利模式提供依据和基础。

该项目颠覆传统的技术理念，采用 DataSecOps 理念，能够在保障数据处理活动无感知无影响的前提下保护数据安全。引入小数据机

器学习技术，能够在小数据样本的条件下智能识别数据并进行精细化分类，不受数据样本数量的限制。

该项目在某证券的大数据安全计算、大数据安全计量、数据全链路安全监测、风险评估与安全防护等方面取得了显著的成效。其关键技术、方案规划、主要解决的安全问题、方案的适用场景，都具有普遍的适应性，在该公司内的落地实践具有示范引领作用。应用场景方面，该项目适合向涉及大数据计算、数据资产计量的大数据计算分析领域、数据安全监测与风险评估的场景、数字化转型企事业单位的数据安全防护场景进行推广。

## 7、“欧数中算”跨境数据互联互通

该案例由上海同态信息科技有限责任公司（同态科技）申请，基于同态科技自主可控的同态加密算法，该案例可实现数据全生命周期内的安全管控与自由流通，主要在政务、金融、军民融合领域实现数据可用不可见、合规数据标准化应用、数据应用全流程可控。

该案例主要应用基于同态加密的隐私保护技术体系，构建中俄两国间数据跨境隐私加密节点，旨在为用户提供数据安全云托管、多维度授权监管、流转全周期管控、安全融合计算等能力，解决数据跨境互联互通过程中的所有权不清、价值稀释、乱用滥用等核心痛点。该案例先进性及创新点有以下几点：

（1）实现高效、安全、自主可控的密态数据流通

平台采用自主可控的密码算法实现数据的密态流通与隐私保护，一方面满足了数据要素市场化流通时的“可用不可见”要求，另一方面充分响应国家对于国产化密码创新应用的号召。

（2）实现核心技术的性能“瓶颈”突破

为解决目前同态加密算法大量消耗计算资源和存储成本、加密过程易产生噪音等痛点，同态科技实现传统算法的性能瓶颈突破。目前，所构造全密文的业务系统已能够有效支持大数据量场景下的数据交换、共享、应用，实现高敏感数据的标签补齐、第三方安全外包计算、重要数据开放共享等场景。

（3）复用原有业务模式，业务部署便捷

该案例采用自主可控的密码硬件产品对外提供密码服务，保证密码算法运行环境的安全，降低不同业务定制化开发需求，实现原有业务模式不受影响，有效降低了适配与重复开发的成本。

（4）实现权责分明的数据流通模式

该案例成功分置数据源所有权与需求方使用权，确保双方的数据权益不受侵害。

（5）实现灵活安全的数据开放共享模式

在数据分类分级基础上提供多种数据开放共享模式，在确保数据安全合规的前提下，支持沙箱交付、接口交付等多种数据开放共享模式，有效支撑查询、统计、机器学习等多种业务场景，实现数据多维度灵活开放共享。

## 8、互联网医疗数据分类分级和交换安全管理

该案例由北京新医强国科技有限公司（好大夫）申请。互联网医疗企业在开展线上问诊过程中积累了大量医生个人信息和患者医疗健康数据。在处方购药、挂号服务等业务场景中涉及到患者身份信息、病情描述、处方等个人敏感信息与合作方进行数据交换。该案例将互联网医疗企业开展数据分类分级工作和数据交换安全管理的实践经验进行总结，形成了互联网医疗数据安全分类分级思路框架和数据交换安全思路框架，并对详细建设过程进行阐述。

互联网医疗数据安全分类分级包含：互联网医疗数据分类分级工作思路框架、数据分类分级工作输入、数据安全分类分级制度建设、数据安全分类分级工具建设、数据安全分类分级流程建设、数据分类分级结果呈现。该方案可推广应用于互联网医疗企业开展数据安全分类分级工作，按照互联网医疗数据分类分级工作思路框架在企业内部进行制度、工具、流程建设。方案中所涉及分数据资产管理平台、敏感数据识别工具、数据安全监控大盘均为开源或轻量级自研，互联网医疗企业可借鉴复用工具进行建设，大大降低了互联网企业数据安全建设成本。

互联网医疗数据交换安全管理包含：数据交换安全管理思路框架、合作方信息管理、数据交换安全评估设计、数据交换 API 接口安全测试、数据交换安全监控分析。互联网医疗企业可以按照本案例的思路框架在企业内部针对自身合作业务进行制度、流程建设。能够帮助互

联网企业降低数据泄露、数据使用异常等安全风险，同时对数据交换场景进行有效管理能够满足相关法律法规的合规要求。

该方案对互联网医疗企业开展数据安全分类分级和数据交换安全管理具备理论和实践方面的指导借鉴意义。

## 9、某酒店管理系统数据安全

该案例由中国电信股份有限公司北京分公司申请，该公司践行央企责任与担当，在“全业务发展、全产品发展、全地域发展、全客户发展”战略的指引下，积极响应国家在网络安全、数据安全政策，始终把安全作为头等大事来抓，积极构建“云、网、端、边、用”一体化的安全保障体系，整合中国电信云网、安全、数据等优势资源和能力，为客户提供云网安全、数据安全、信息安全等各类安全产品和服务，不断筑牢行业数字化转型的安全防线。

在大数据时代，对于一个能够为客人提供优质服务的酒店来说，首先是尊重和保护客人的隐私，这是前提，也是重要的安全原则之一，一旦酒店发生客人信息泄露就会失去客源。北京电信在针对该项目客户酒店管理系统数据量大，涉及用户多，敏感字段多等主要特点为客户进行了全面体系化的数据安全建设。

首先，通过工具探查、人工辅助的方式对客户资产进行资产清点并结合酒店行业务属性进行分类，按照数据重要程度等进行分级；然后，借助电信天翼云上数据防护手段帮助客户从入侵防护、访问控制、

存储加密、风险监测预警和容灾备份等方面实现了数据安全的全生命周期的技术管控，并为客户建立了统一的数据安全管控平台，实现各数据安全服务之间的策略联动，以及智能数据安全应用；最后，根据客户实际业务的开展机制量身打造了数据安全治理的流程跟环节，帮助客户建立数据安全管理的组织架构，明确了部门职责与人员角色，建立了部门之间的动态协同机制。

该项目在建设初期也遇到了疫情爆发和冬奥重保的双重考验，北京电信在有限的时间窗口内动态调整策略，积极响应需求，快速落地方案，时刻保持“越是险阻越向前”的战斗姿态，借助天翼云优质高效的数据安全防护服务，迅速上线一系列安全措施，同时保证了项目落地的时效性和有效性，保障了客户业务数据和个人隐私安全。忠诚履职诠释了央企担当的深刻内涵，同时体现了电信在数据安全领域的践行实力，打造了行业标杆。为今后助力中国乃至国际更多客户的数字化转型和数据安全防护保驾护航！

## 10、老年多病共患大数据安全共享

该案例由中电长城网际系统应用有限公司（长城网际）申请，应用于多源异构医疗数据在协同分析过程中的安全共享场景，针对个人隐私泄漏风险导致的“不敢共享”、数据安全级别混乱导致的“不能共享”以及权责界定模糊导致的“不愿共享”等难点，通过安全计算环境、虚拟资源目录、细粒度访问控制、多维安全审计等核心技术，建设老

年多病共患临床大数据安全共享平台，汇聚多家医疗机构数据和算法，在权限范围内进行本地计算，并对数据使用和分析过程进行血缘追溯与审计，实现“数据不动算法动，数据可用不可见，用途可控可测量”的安全目标。

目前在“老年人多病共患临床大数据与生物样本库综合管理共享平台建设”项目实施，支持 HIS 系统、电子病历数据库等多源异构数据的安全接入，采集 1000 万例以上老年病患者的临床数据，存储规模达 PB 量级，应用于病理智能判读、老年衰弱患者临床优化方案等模型的安全分析。平台采用以北京安贞医院为总中心，各地区健康大数据为分中心的模式，以河北省唐山市数据为数据样本，建立模型后，陆续在河北唐山、吉林长春、内蒙古通辽、四川乐山等地建立数据安全仓，对接数据源。此平台在老年多病共患临床大数据的共享利用与安全保护方面具有显著创新，其建立促进了老年多病共患临床大数据共享分析，提升医疗数据价值，其提供的数据资源将作为国家制定“健康老龄化”战略、医改等重要政策的基础数据支撑，实现可持续、高质量的老年多病共患研发公共资源平台。该案例已取得 9 项专利、6 项软件著作权、2 项标准及奖项荣誉。

## 11、运维侧数据多要素全路径安全治理

该案例由国网英大国际控股集团有限公司（英大集团）申请。英大集团近年来紧跟金融和电力行业网络安全管理要求，针对公司重要

数据持续加强安全防护，于 2020 年率先开展业务系统数据分类分级试点并取得一定成效，并在此基础上不断开展“内生威胁”专项治理，针对运维侧环境科学制定数据安全防护策略，开展了行之有效的数据安全治理实践工作。

“运维侧数据多要素全路径安全治理实践”具有以下特点：

（1）规划高封闭数据运维路径。谨密设计网络和主机访问控制策略，依托现有防护措施铺设高线性数据运维路径，确保运维数据流域与规划数据路径严格匹配。

（2）融合高异构数据防护措施。针对运维环境中系统、数据、终端、介质、人员及账号等要素层叠交叉的特点，将数据库防火墙、运维安全网关、数据外发管控、终端管理等系统紧密融合，集结使用针对性控制功能，以体系化防御实现运维环境数据保护的可视可控可追溯。

（3）实现高管控数据合规使用。对运维环境数据实现黑盒化管理，运维安全网关中数据不允许本地导出，运维环境受控终端作为数据离境（运维环境）的唯一通路，配合用户账号实名制认证，确保只有特定实名制用户提交下载申请并经批准后，方可下载到受控终端。

英大集团通过开展此实践应用，取得了良好成效。一是通过对系统、数据、终端、介质、人员及账号统一管理，实现运维环境内数据防护措施的立体联动，加大了数据防护范围、加深了数据保障能力，弥补传统单点数据防护措施的短板；二是满足运维数据使用的安全要

求，在运维侧有效防范金融数据尤其是个人敏感数据的泄漏风险，大幅提升英大集团金融数据全生命周期防护能力；三是在运维数据可视可控可追溯的前提下，进一步拓展了运维弹性，避免紧急情况下发生运维资源挤兑的情况，提升了英大集团整体数据运维的能力。

## （二）优秀数据安全技术与产品实践案例

### 1、360 企业安全云

该案例是由三六零安全科技股份有限公司（以下简称“360”）申请，为护航中小企业完成数字化升级转型推出的新一代数字安全与管理 SaaS 服务平台。360 企业安全云，基于 360 安全大脑国家级安全能力，依托 290 亿安全样本、22 万亿安全日志以及 2EB 安全大数据，实现从本地到远程、从终端到云端的硬件、软件、数据、行为、人的全方位数字化管理。

360 企业安全云依托 360 安全大脑，围绕终端、网络、软件、数据与资产、防勒索进行立体化模块建设，发挥 SaaS 模式优势，打造企业级数字化安全与管理平台，提出以下解决方案：（1）终端统一安全防护（2）网络安全实时检测（3）人员身份及行为管控（4）全流程数据防护（5）即用即懂、灵活部署的 SaaS 服务。

截至目前，360 企业安全云已在制造、教育、医疗、公共事务、园区、金融、零售等行业及场景落地实践，为中小企业提供了一种“拎包入住”的安全云服务。已服务近百万家中小企业、7000 余家教育机

构、4000 余家政府机关、5000 家银行/医院等；累计检出 400 万企业终端木马病毒、2.9 亿企业终端漏洞风险，拦截风险域名及 IP1800 万次、数据库攻击 3100 万次，有效保护了企业用户的数字安全；拦截广告弹窗 3.8 亿次，管理外设接入 1000 万次，极大提升了 IT 管理效率，大幅降低了中小企业数字化成本。

## 2、观源商用密码云服务管理平台

该案例由观源（上海）科技有限公司（观源）申请。随着 2020《密码法》的实施，商业密码产业也进入发展的快车道，密码也正成为维护网络安全最有效、最可靠、最经济的技术手段。在国内，政务、关键基础设施单位的信息系统已经基本云化，数据从分散到集中，并走向共享运营，中国已经全面开启数字经济时代。但数据从生成、传输、存储到运营的各个环节，都存在较大的数据泄露风险，安全隐私保护的需求非常强烈。而传统安全手段已不能满足数据安全的实际需要，密码与数据的结合，给数据安全带了新的思路。

观源商用密码云服务管理平台，依据国家相关信息安全法规和规范，结合信息系统商用密码测评要求及信息系统现状，对现有密码技术资源进行整合，构建统一合规的密码资源池、搭建统一的密码资源管控平台，形成了统一的密码服务接口、管理体系和监管体系。平台通过密码应用的创新，实现了密码即服务（Cryptography as a Service - CaaS）的应用模式，为云上业务提供高强度的密码保护和高速的密码

运算服务，保障关键业务数据的机 密性、信息完整性和不可否认性。不仅满足了云上业务系统的合规改造需要，还全面保障了信息系统的自身安全和所承载的数据安全，实现信息系统建设的安全合规和成本节约。

## 3、Chinasec（安元）数据防泄漏应用

该案例由北京明朝万达科技股份有限公司（明朝万达）申请。在政务信创安全建设中，该案例首次进行专业化数据防泄漏规划，在政务内网及外网通过与保密检查工具、身份认证系统对接，在政务工作的前端用户、数据传输、终端使用上实现全方位的安全防护，降低内部人员泄密、无意失密等安全事件的发生概率以及其带来的负面影响。高度匹配《中华人民共和国数据安全法》，明确了数据治理与数据安全防护体系是必不可缺的，指导数据管理者应充分结合自身情况、监管要求，充分了解当前所面临的主要问题、行为与场景，以应对目前开放、复杂的数据安全环境。

该方案采用了领先的设计理念和成熟的安全技术，符合基于信创背景下国产化操作系统对数据安全需求，采用了 C/S、B/S 架构相结合的方式，采用基于微服务的容器化技术设计构建而成，将核心的功能模块抽象成服务落地，有效应对组织内部 IT 架构的快速变革与延伸，实现全 IT 架构下数据安全的联合管理与异构终端统一化管理。

平台以多年自主研发的数据加解密技术为核心，结合身份认证和访问管控等多种技术手段，为用户打造完善的数据安全体系。平台支持 PKI 体系数字证书，支持国际主流标准加解密算法，兼容国密 SM1、SM2、SM3 及 SM4 等算法，实现本地存储数据加密、移动存储数据加密、文档加密、邮件加密、业务应用数据加密和数据传输加密等丰富的加密功能，密钥体系严格遵守国家商用密码规范要求，并通过了国家保密局、国家密码管理局等权威机构的认定。

## 4、爱加密移动应用个人信息合规检测平台

该案例由北京智游网安科技有限公司（爱加密）申请，可针对移动应用、SDK 中出现个人信息的非法收集、滥用、泄露等不合规问题进行自动化检测。

随着数据安全法、个人信息保护法等有关数据安全法律法规的正式施行，数据的融合应用与价值落地面临新的机遇与挑战。当前，信息合规成为监管重点，国家网信办、市场监管总局等数据保护监管部门的执法力度加大，大量违法违规收集、使用个人信息的应用程序被责令下架、整改，安全合规已被提升到战略高度。作为国内知名的移动信息安全综合服务提供商，北京智游网安科技有限公司（爱加密）充分发挥自身技术优势和企业社会责任感，致力于移动应用的个人信息安全保护。

平台结合相关法律法规和监管要求，为监管机构、测评机构、应用开发企业等对象提供合规检测能力，通过该能力可对移动应用及SDK 出具专业的报告，报告中包括对检测的不合规问题描述、不合规问题过程信息展示、修复指导建议等内容。帮助监管机构准确、有效地提供行政执法依据；帮助测评机构出具专业的个人信息测评报告；帮助应用开发企业在应用发布前评估个人信息的安全性和合规性。

## 5、Sophon P℃：打破数据孤岛，为数据流通构建安全防线

该案例是星环信息科技（上海）股份有限公司（星环科技）申请，由星环科技与某支付机构共同打造的基于隐私计算的数据服务平台。某支付机构拥有优质数据资源，在数据安全管理方面遵循中国银联的制度和要求，定期接受审计和检查。该支付机构能提供多种数据产品和服务，如机构的数据和某汽车品牌的数据融合，为车企的客群补充该机构的消费数据标签，完善车企客户画像。数据来源包括该机构数据管理平台和品牌方的数据管理平台。

由于法律环境发生变化，某支付机构面临着较大的挑战，需要加强数据安全管理，为此，该支付机构决定与星环科技合作，利用星环科技的技术来提升数据安全管理能力，共同打造一个基于隐私计算的数据服务平台 DaaS 。星环科技根据客户需求，在基础设施层，星环提供了基于容器的云原生操作系统 TCOS，可以为用户提供独立的数据与计算环境，减少数据对外暴露的风险。在数据平台层，TDH 大

数据平台新版本增强了安全技术，支持行列级权限控制、动态脱敏等。在数据资产层，星环科技借助两款新产品：数据安全管理平台 Defensor 帮助企业构建整个数据安全管理域及数据流通平台 Navier：包含隐私计算平台 Sophon P₹ 和数据交易门户 datamall，提供包括联邦学习和差分隐私等技术能力。

## 6、数据流动风险监测

该案例由全知科技（杭州）有限责任公司（全知科技）申请，致力于建立对关键信息基础设置应用系统的数据安全自识别及评估能力，覆盖运营商、银行、电子政务等常见关键信息基础设施应用系统、文件服务系统、邮件服务系统、数据库服务。

现今数据安全的防护已不仅限于针对静态数据库存储安全进行防护，不是把数据关在笼子里，需要监测并守护业务数据在整个流转过程中的安全。因此在这个过程中，首先需要识别当前业务数据流转的现状，基于当前现状分析业务流转及暴露面的业务合规性，并通过监测手段识别流转过程中的业务数据风险，通过内部治理应对后，通过平台下发阻断及脱敏策略，及时遏制风险蔓延，并持续监测风险收敛态势，帮助安全运营人员提升业务整体安全性。全链路数据流动安全管理平台，使用网络流量分析技术，可以对企业内部的结构化日志进行分析记录，发现用户行为风险，遇到数据泄漏问题时可以有据可查。该案例创新性有如下几点：

（1）敏感数据识别及统一管理：研究基于旁路流量方式中各类协议中传输的敏感数据识别，包括：数据库数据、数据访问接口、文件、邮件的敏感数据识别技术。

（2）基于敏感数据链路关系生成：研究基于敏感数据内容的相似度，进行数据流动链路关系的还原。根据用户-接口-数据表关系、用户-应用服务-数据库关系、文件-用户调用关系、邮件-用户调用关系等多个维度进行汇总分析，形成企业数据流动全景画像。

（3）数据访问行为追踪及数据链路风险识别：研究异常数据访问行为感知技术：基于识别出的用户访问行为链路监控数据及指标，建立数据模型进行机器学习和大数据多维度分析，对数据访问建立动态行为基线，利用异常检测基础，从业务角度分析多维度来识别异常链路关系，正常链路上的异常访问行为，实现异常数据访问行为识别及监控预警；通过自定义访问控制规则，可实现对不同类型和等级数据访问的管控。

## 7、API 安全管控平台

该案例由深圳永安在线科技有限公司（永安在线）申请，属于金融行业的典型应用案例。

2022 年，永安在线监测到黑灰产售卖某大型金融企业的大量用户手机号、保单交易等重要敏感数据。经查证，发现起因是该企业 API 接口存在未授权访问、关键数据未脱敏等缺陷，攻击者通过这些

API 爬取敏感数据。通过交流发现，近几年该企业在业务数字化升级过程开发了大量内部运营系统与开放业务应用，大量未经过严格安全检测的承载敏感数据的 API 在线上运行，存在大量未知的数据风险敞口。

永安在线 API 安全管控平台以 API 为中心，通过精准的风险情报构建 API 安全基线。以旁路部署的方式接入，助力企业构建可预防、可解释、可溯源的安全管理体系。

（1）API 资产梳理

持续、动态、自动化梳理面向多种场景下的 API，建立完整 API 台账。并对流量中流动的敏感数据进行分级分类，确保数据资产持续更新可见。并且梳理 API 关联的账号资产，帮助企业应对账号共用、账号盗用、内部人员数据访问等类型的账号风险。

（2）API 缺陷检测

在 API 资产可见的基础上，平台会持续跟踪攻击者如何利用新型 API 漏洞进行攻击，能及时覆盖最新的业务 API 逻辑漏洞和第三方组件、开源系统 API 的未授权漏洞等。协助企业及时感知线上运行的 API 存在的数据暴露漏洞并跟进修复。

（3）API 风险感知

基于威胁情报及时感知低频数据爬取、敏感 API 境外访问、撞库攻击等场景的风险，并支持联动 WAF 等设备进行快速阻断。 避免未知的数据爬取攻击导致大规模数据泄露事件的发生。

永安在线 API 安全管控平台帮助该企业实现资产台账可见，整理出 API 2600+，出站涉敏 API 390+，涉及敏感数据类型 19 类，且发现 API 缺陷累计 770+个，涉及未授权、越权访问、数据伪脱敏、数据明文传输等高危缺陷 190+ ，发现内部数据泄露账号 5 个，违规借用账号 8 个，帮助企业杜绝数据泄露风险的发生。

## 8、360 企业文档云助力某大型制造业集团公司打造安全协同办公新模式

该案例由杭州奇亿云计算有限公司（奇亿云）申请。随着企业数字化转型和发展，企业的数据资产保护和高效协同工作越来越受重视，360 企业文档云为某大型制造业集团公司的数字化转型赋能，打造了一个非常安全的非结构数据中台，帮助公司将数据资产沉淀到云端，提升数据管理效率。

360 企业文档云提供了全生命周期的文件安全保障，包括数据加密、访问控制、审批流程等功能，保证文件在传输和存储过程中的安全性，解决了企业内部机密文件在传输及分享过程中出现的数据泄漏，且无从回溯的难题，同时也避免了因人员流动导致大量内部文件被带走，给企业带来的安全损失。文档云底层的数据容灾及数据加密能力，可以保障企业的核心数据安全存储、不丢失；“360 安全大脑”提供新型探针和动态安全赋能，保护云端文档、本地文档及外发文档安全不

泄露；此外文档云还能有效避免因病毒（如：勒索病毒等）攻击而导致的数据损毁。

360 企业文档云支持多人、多中心在线协作，通过在线文档编辑、评论、协作流程等功能，解决企业海量文件散乱存储、查找困难、应用效率低及共享协作不便的问题，帮助公司员工实现高效率远程协作。文档云为该集团搭建了“一中心、三节点”的一站式文件存储、共享和办公协作平台，汇聚多个城市办公场所的上百 T 文件资料，并完成企业微信 H5 集成、BPM 系统对接，满足企业的文件安全、文件存储、知识管理、灵活扩容、文件共享、文件流转等需求，实现全集团跨区域跨团队之间的文件共享与高效协同办公，为企业数据资产安全保驾护航的同时提高团队协作效率，为公司远程办公模式实现更多便利。

## 9、2022 年度工商银行新一代电子文档安全管理系统

该案例是北京北信源软件股份有限公司（北信源）申请，案例在北信源文档安全防护系统产品基础上，结合工行的实际情况，进行二次定制开发，确保敏感电子文档不落地，完成与业务部门全行性业务系统对接，实现电子文档的在线编辑和安全管控；确保业务系统中电子文档的安全存储。

北信源文档安全防护系统方案主要实现以下功能：

（1）基础的文档加密功能，全盘的文档加密。

（2）文档资产管理功能。

（3）和业务系统对接的功能，保证业务系统的数据加密存储、流转授权、使用过程中用户无感知。

方案具有以下先进性：

（1）使用驱动层透明加解密技术实现终端文档加密；提供标准接口供业务系统调用，保证从业务系统下载自动加密；提供批量扫描加密功能，对全盘和指定目录的存量进行扫描加密。

（2）多种密钥因子共同组成文档密钥，实现每个电子文档使用一个加密密钥。

（3）文档内部授权访问和细粒度的使用权限控制。

（4）基于文档属性的访问控制。

已完成境内 52 家分行以及其他一级机构总计 40 万用户、80 万终端（存在一个用户多台终端的情况，同时还有一些公共设备），境外若干家一级机构、合计若干用户终端的推广工作。系统上线至今，持续稳定运行，显著提高了工商银行商业秘密信息系统的安全。

同时，还在中国联通集团、中国电力投资集团等进行了推广使用，为企业的商业秘密信息系统（主要是企业公文系统）的安全建设提供技术支撑，取得了良好的应用效果和社会效益，获得了用户的广泛支持和好评。

## 10、河南移动客户信息识别与分类分级

该案例由中国移动通信集团河南有限公司（河南移动）申请。河南移动以“规范标准+技术”为主导方向，兼顾企业的业务发展趋势，引进敏感数据发现和分类分级系统推进数据识别和分类分级、数据安全制度标准建设，保障组织数据安全机密性、完整性、可用性。同时，根据公司生产经营管理现状和自身管理特点，将企业用户数据进行部分细化；在数据资产梳理的过程中，逐步针对数据分类进行细化并不断修订数据安全管理规范。满足公司生产经营及管理过程中数据安全防护需要，避免因数据泄露影响社会稳定，持续为社会产生带来价值。

通过欧式向量空间算法进行数据分类分级，可获取包含敏感数据信息的数据库表；将包含敏感数据信息的所述数据库表的字段进行数组量化，并分别计算数组量化的所述数据库表的字段与数组量化的全部分类信息之间的欧氏距离；将全部所述欧式距离从低到高进行排序，并选择最短的欧式距离所对应的分类信息为目标分类信息进行推荐。可通过数据源、数据表/文件、字段、敏感数据的类别级别等信息，索引数据的定位，支持导出数据目录清单。替代原先的手工或半自动化工作，达到降本增效的要求，并通过定时/周期的敏感数据发现，自动化更新企业敏感数据目录，相关部门可通过数据目录进行统一管理。

相较传统由人工进行分类分级，在处理单个业务系统数据效率可提高约 95%，每次进行数据资产梳理可大约节省 225 人天，为公司节

省约 3 名固定人员投入，极大程度节约了人力成本。减少企业数据安全风险，避免给企业造成损失，提升组织数字竞争力和拓展数字经济空间潜力。

## 11、大数据驱动下的全生命周期安全监测预警平台

该案例由中国联合网络通信有限公司上海市分公司（上海联通）申请。随着上海联通各种新业务上线运营带来的数据爆炸式增长，传统的人工审核模式效率日趋下降，无法满足当下复杂流转场景下敏感数据安全防护需求，安全防护风险随之增加。此外互联网暴露面应用的数据安全隐患依然存在，防止敏感数据泄露迫在眉睫。目前，业内对全生命周期敏感数据缺少强有力的捕捉能力，导致对网间流转的敏感数据无法自动发现、无法自动监测敏感数据访问使用情况等问题，存在敏感数据泄露风险。为此，上海联通针对敏感数据识别精准度、识别效率、覆盖场景等方向开展技术研究，打造基于智能算法模型的全生命周期数据监测预警平台。平台主要由敏感数据资产发现功能、页面敏感信息识别功能、实时数据监测功能、数据流敏感信息拦截功能、用户异常行为监测 5 大功能模块组成。针对全域的数据资产、数据库资产、应用资产以及用户资产，基于敏感数据的数据特征和数据类型，通过将上述功能模块深度融合应用，全面覆盖数据生命周期的各个环节，构建行业领先的敏感数据全环节的智能分析和安全风险监

测预警能力，基本满足数据安全风险防护基本要求，实现数据安全监测管理、技术防护和安全运营的有效协同。

# 五、工程中心研究

## （一）《全国一体化政务大数据体系建设指南》数据安全解读分析

近年来，国务院先后出台了一系列政策文件，统筹推进政务数据共享和应用工作。为整合构建标准统一、布局合理、管理协同、安全可靠的全国一体化政务大数据体系，充分发挥政务数据在提升政府履职能力、支撑数字政府建设以及推进国家治理体系和治理能力现代化中的重要作用，国务院办公厅印发了《全国一体化政务大数据体系建设指南》（简称“《指南》”）。

### 1、《指南》数据安全重点内容解读分析

#### （1）数据安全建设现状与问题

目前，全国 31 个省（自治区、直辖市）均已结合政务数据管理和发展要求**明确政务数据主管部门**，组织实施政务数据安全保护等工作，统筹推进数据资源开发利用。但是，**政务数据安全保障能力亟需强化**，随着《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》等法律法规的出台，亟需建立完善与政务数据安全配套的制度；数据全生命周期的安全管理机制不健全，数据安全技术防护能力亟待加强；缺乏专业化的数据安全运营团队，数据安全管

理的规范化水平有待提升，在**制度规范、技术防护、运行管理**三个层面尚**未形成数据安全保障的有机整体**。

解读分析：

明确指出目前政务数据安全保障能力还远不能满足安全要求，亟需从制度、技术、运营三个层面展开体系化建设，这对数据安全产业来说无疑是一个很好的发展机会。

**（2）提出数据安全总体要求**

《指南》在指导思想中明确要加强数据安全保护，明确了**坚持整体协同、安全可控**的基本原则，并在建设目标中提出：2023 年底前，全国一体化政务大数据体系初步形成，基本具备**安全防护能力，安全保障体系初步建立**，基础设施保障能力持续提升；到 2025 年，全国一体化政务大数据体系更加完备，政务数据标准规范、**安全保障制度更加健全，数据安全保障体系进一步完善**。

为推动全国一体化政务大数据体系的形成与完备，《指南》提出**安全保障一体化**的任务：**以“数据”为安全保障的核心要素**，强化安全主体责任，健全保障机制，完善数据安全防护和监测手段，加强数据流转全流程管理，形成**制度规范、技术防护和运行管理三位一体**的全国一体化政务大数据安全保障体系。

解读分析：

《指南》明确了“**坚持整体协同、安全可控**”的基本原则，提出“**安全保障一体化**”的任务，并强调该任务是“**以‘数据’为安全保**

**障的核心要素”**，要“形成**制度规范、技术防护和运行管理三位一体**的全国一体化政务大数据安全保障体系”。

**（3）健全数据安全制度规范**

贯彻落实《数据安全法》、《个人信息保护法》等法律法规，明确数据分类分级、安全审查等具体制度和要求。明确数据安全主体责任，按照“谁管理、谁负责”和“谁使用、谁负责”的原则，厘清数据流转全流程中各方权利义务和法律责任。围绕数据全生命周期管理，以“人、数据、场景”关联管理为核心，**建立健全工作责任机制**，制定政务数据访问权限控制、异常风险识别、安全风险处置、行为审计、数据安全销毁、指标评估等**数据安全管理规范，开展内部数据安全检测与外部评估认证**，促进数据安全管理规范有效实施。

解读分析：

《指南》提出明确数据安全主体责任、建立健全工作责任机制、制定数据安全管理规范，以及通过内外部评估认证促进规范有效实施的要求。

**（4）提升平台技术防护能力**

加强数据安全常态化检测和技术防护，**建立健全面向数据的信息安全技术保障体系**。充分利用电子认证，数据加密存储、传输和应用手段，防止数据篡改，推进数据脱敏使用，加强重要数据保护，加强个人隐私、商业秘密信息保护，严格管控数据访问行为，**实现过程全**

**记录和精细化权限管理。建设数据安全态势感知平台**，挖掘感知各类威胁事件，实现高危操作及时阻断，变被动防御为主动防御，提高风险防范能力，优化安全技术应用模式，提升安全防护监测水平。

解读分析：

《指南》提出了建立**以数据为中心**的安全技术保障体系，通过加强技术防护实现数据流转过程全记录和精细化权限管理，通过数据安全态势感知平台提升安全监测水平，实现主动防御。

**（5）强化数据安全运行管理**

完善数据安全运维运营保障机制，明确各方权责，加强数据安全风险信息的获取、分析、研判、预警。建立健全**事前管审批、事中全留痕、事后可追溯**的**数据安全运行监管机制**，加强数据使用申请合规性审查和白名单控制，优化态势感知规则和全流程记录手段，提高对数据异常使用行为的发现、溯源和处置能力，形成**数据安全管理闭环**，筑牢数据安全防线。加强政务系统建设安全管理，保障数据应用健康稳定运行，确保数据安全。

解读分析：

《指南》明确要求建立基于风险管理全流程的数据安全运行监管机制，并强调数据安全管理闭环的要求。

**2、推进数据安全保障一体化建设的建议**

根据《指南》“安全保障一体化”要求，结合 BDS 工程中心的数据安全研究与实践经验，特提出以下建议：

**（1）建立健全政务数据安全标准规范**

依据国家法律法规、安全审查、数据分类分级等方面要求，落实到各场景下相关责任主体处理各类型数据的具体环节，明确各方职责，规范数据收集、存储、使用、加工、传输、提供、公开等数据处理活动的安全要求，包括数据访问权限控制、异常风险识别、安全风险处置、行为审计、数据安全销毁等，**建立针对数据流转全流程的系列安全标准规范**，确保政务数据的安全规划、安全建设、安全运营都有规范化的依据和标准化的管理。

**（2）从数据和组织两方面强化政务数据安全治理**

针对政务数据复杂多样、各政务机构数据安全管理能力建设参差不齐的情况，为保证法律法规和监管政策的落实，促进数据安全管理策略与要求的有效实施，**应从数据和组织两个方面同时强化政务数据的安全治理。**在数据侧加速推进政务数据的分类分级和风险评估工作，对政务数据安全保障体系开展安全检测与评估，为政务数据流通共享和开放利用打下安全基础。在组织侧加速推进数据安全能力成熟度和数据安全管理体系测评认证，以系统提升政务机构和政务数据处理相关机构的数据安全能力，有效管控政务数据在不同组织间流转带来的安全风险。

**（3）打造以数据为中心的数据安全保障技术体系**

随着全国一体化政务大数据体系的建设与发展，政务数据将在不同部门、地域间流转，安全威胁的影响范围也随之转移扩大，只有**打造面向全流程、全场景的、以数据为中心的安全防护体系**才能全面降低数据暴露面，杜绝局部性或零散性防护的顾此失彼。为此，应建设数据资产安全管理平台，为数据资产梳理、分类分级和数据质量管理提供支撑；建设大数据安全管理平台，实现政务数据全生命周期安全保护、数据安全态势感知和全链路的精细化数据使用管控；建设数据流通共享安全平台，支撑数据转移、检索与访问、隐私计算支持的数据利用等不同模式的数据流通共享，以适应政务数据开放利用的不同应用场景。

**（4）加强以风险持续监控为目标的数据安全运营**

针对数据流转全流程的不合规、数据窃取、数据篡改、数据泄露数据滥用和加密勒索等内外部安全威胁，需**采取持续风险监控手段来实现风险的识别和预警**。为此，应建设大数据安全监管审计平台，基于政务云平台审计数据、安全设备告警数据和数据共享交换平台审计数据等进行大数据安全分析，形成实时掌握政务大数据体系风险状态与全流程追溯的能力，建立响应处置与防御恢复的风险管理闭环，实现政务数据的合规与安全监管、攻击行为识别追溯以及数据泄露与滥用的审计追溯。

## （二）完善数据安全治理机制 保障数据要素安全高效流通

12 月 19 日，《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》（以下简称《数据二十条》）对外发布，明确了构建数据基础制度的基本原则，并提出数据产权、流通交易、收益分配、安全治理等制度构成我国数据基础制度的“四梁八柱”，对于推动充分发挥数据要素作用、提高数据要素治理效能具有重要的指导意义。

### 1、《数据二十条》再次强调发展与安全的统筹

自《数据安全法》强调“国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展”之后，《数据二十条》在指导思想中再次强调要“统筹发展和安全，贯彻总体国家安全观，强化数据安全保障体系建设，把安全贯穿数据供给、流通、使用全过程，划定监管底线和红线”。同时，明确“加强数据分类分级管理，积极有效防范和化解各种数据风险，形成政府监管与市场自律、法治与行业自治协同、国内与国际统筹的数据要素治理结构”，以及“以维护国家数据安全、保护个人信息和商业秘密为前提，以促进数据合规高效流通使用、赋能实体经济为主线，以数据产权、流通交易、收益分配、安全治理为重点；充分认识和把握数据产权、流通和安全等基本规律，探索有利于数据安全保护、有效利用、合规流通的产权制度和市场体系；建立数据可信流通体系，

增强数据的可用、可信、可流通、可追溯水平”等数据安全相关工作原则。

这些原则对于推进数据安全保障体系顶层设计，数据流转全过程的安全合规、可控与监管，数据分类分级制度的落实，数据安全风险防范等工作具有清晰的指导作用，能够加快数据要素市场的培育建设进程，并为数字经济同步建成自律自治、安全有序、合规稳定的安全底座，对维护国家数据安全、保护个人信息和商业秘密，构筑全球范围安全高效健康的数字经济环境非常关键。

**2、《数据二十条》数据安全治理机制的解读分析**

为了促进数据安全合规的开发利用，保障数据产业稳定有序发展，《数据二十条》从数据确权授权、合规监管、多方协同治理等方面指出了数据安全治理的方向。

在数据产权制度中，《数据二十条》分别明确了公共数据、企业数据、个人数据的确权授权机制。针对公共数据明确了推进互联互通、打破“数据孤岛”的总体原则，规定公共数据的共享与开放开发需满足确保个人隐私保护与公共安全的前提，通过以模型、核验等产品和服务等形式向社会提供的方式符合“原始数据不出域、数据可用不可见”的要求，从而实现原始数据与数据应用的解耦，在保障安全的同时释放公共数据价值。针对企业数据，明确了数据收益权益归属原则，激励各方充分挖掘企业数据价值，鼓励头部企业向中小微企业授权合理使用企业数据以推动中小微企业完成数字化转型，同时提出对数据

应用相关产业的支持，以促进数据挖掘和应用创新。针对个人信息数据，再次重申不得“一揽子授权”、强制同意的个人信息收集原则，并提出要探索由受托者代表个人利益，监督市场主体对个人信息数据进行采集、加工、使用的机制，以此将分散的个人主体汇聚成易于对接、管控的集中主体。

在数据流通交易制度中，为保障数字经济双循环的安全合规，《数据二十条》围绕数据要素流通全流程，提出了建立数据流通准入标准规则、建立数据分类分级授权使用规范、探索数据流通安全保障的技术、加强企业数据合规体系建设、实施数据安全管理认证等维度共同发力，推动数据要素流通的合规可控与可监管审计。同时，强调要增强国际交流合作、推进跨境数字贸易基础设施建设、统筹数据开发利用和数据安全保护，构筑积极合作、安全开放的高效流通环境，促进跨境数据流通和共享朝着安全、合规、有序的健康路径发展。

《数据二十条》提出了政府、企业、社会多方协同治理模式，通过充分发挥政府的有序引导和规范发展作用，建立数据联管联治机制，划定安全红线与审查监管督促各方履行数据要素流通安全责任和义务。引导不同角色的企业在数据流通交易中践行社会责任感，在数字红利的公平分配中建成规范使用数据的良性可持续发展环境，促进企业经济效益与社会效益的平衡。通过行业协会等社会力量对数据要素安全可信流通的支持、数据要素市场信用体系的建立以及数据制度标

准体系的完善，探索政府、企业、社会组织等共同保障数据安全协同治理体系的路径。

**3、落实数据安全治理机制的建议**

**（1）以收益权为基础，以充分赋能企业为目标，加快数据产权建设**

产权制度的目的不应是保护数据资源的占有，而是促进交易，使产权主体能够分享不断增长的社会财富的一部分。企业是推动支持当前数据经济发展的中坚力量，其投入大量技术、资金和人力成本，是大数据得以形成和运营的关键前提。在数据全生命周期中，只有当企业的产权得到充分、合理、有效的保护，才能充分激发企业活力，盘活“孤岛”内的数据资源，充分赋能数字经济发展。建议按照“所有权与使用权分离”的创新思路，为相关数据主体分别赋权，推动数据确权从确所有权为主，转向确使用权为主，实现数据价值最大化。积极肯定企业作为数据搜集者、控制者、生产者在数据搜集、整理、储存、加工过程中付出的成本，按创新程度赋予其相应所有权，按贡献程度赋予其相应使用权。

**（2）强化落实数据分类分级，推进数据确权授权机制构建**

要实现公共数据在合适的范围内开放共享、企业数据持有者合理利用数据、个人信息数据保护原则的落实，需要确保数据在交易流通中的产权明晰、权责明确，其根本需要强化数据的分类分级管理。明确数据的分类分级，确定不同主体在数据收集过程中的责任、义务与

权利，推动数据流通准入规则的建立，促进数据要素权益保护制度的落实；通过明确不同类别数据的授权规则、保护要求，促进对数据依法依规利用、合理共用、规范使用过程中的细粒度管控，鼓舞数据主体积极参与数据开发与价值挖掘，实现数据创新发展与安全保障同步推进。

**（3）健全数据安全标准体系，促进数据安全流通的规范化**

围绕数据要素市场化各个场景、环节，如数据的采集、预处理、存储、数据产品的设计与运营等全流程，制定完备的数据安全标准规范，促进数据要素市场向着有序规范的方向发展，为参与数据流通的数据供应方、数据需求方、数据交易平台方、第三方服务商等各类市场主体建立数据安全合规要求，为数据流通交易市场的培育和监管提供安全合规指引，确保在数据流通全流程安全合规的前提下实现数据高效流通。

**（4）引领建立全球合作交流平台，布局安全互信的国际数据规则**

聚焦数据跨境合规路径、威胁与风险、场景特点、数据安全和隐私保护等重点方向，建立国际数据安全合作对话机制，组织开展国际合作交流，发挥我国强大算力基础、海量大数据规模、庞大数字经济体量的优势，充分利用数据安全和隐私保护技术创新和场景应用的丰富经验，积极引领和参与数字技术标准与规则的制定，增强我国在国际数字贸易规则制定与谈判中的话语权，推进形成公平竞争的国际化

数据市场，促进建设公平竞争、积极合作、安全流通、良性发展的数据流通环境。

**（5）建立数据安全流通与使用的基础设施，推进数据要素流通交易**

通过多方安全计算、数据沙箱、联邦学习、可信执行环境、差分隐私、数据加密、数据脱敏等隐私保护技术建设具有安全保障基础的数据处理环境，发挥数据要素的创新引擎作用，以数据为引，以数据价值为交易产品，为数据价值挖掘、应用研究、业务创新等搭建数据开发利用底座，为公共数据开放共享、企业数据有序共用、个人数据合规处理打造支撑平台，建立高效、安全的数据流通基础，加速推动数据要素市场化的国内大循环。

**（6）探索跨境数据流动安全机制，推动数据跨境示范区建设**

深圳正在探索建设离岸数据交易平台，上海临港计划开展数据跨境试点、打造国际数据港，为尽快摸索出适用于我国的数据跨境流通机制，激活数据要素流通的境外大循环，应迅速围绕各类型数据跨境场景，配合监管部门开展数据跨境的安全评估、流通监管，就数据跨境组织的数据安全能力建设、安全合规水平提升、境外数据安全保障能力评估等开展数据跨境服务，推动不同场景下数据跨境流通安全技术的研究开发、试验验证，形成管理机制与保障技术共同驱动的数据跨境安全流通机制，为全国推广数据跨境应用模式提供示范性、引领性案例。

**（7）建立大数据安全监管审计机制，构建数据要素市场监管体系，促进数字经济高质量发展**

要实现数据要素的安全有序流通，需推动数据产品、服务的安全审查与合规审计，通过建设大数据安全监管审计平台，针对数据流通、交易全流程的不合规、数据窃取、数据篡改、数据泄露、数据滥用和加密勒索等内外部安全威胁，采取持续监控手段来实现风险的识别和预警，为监管部门及时开展市场参与方的数据安全风险评估、威胁监测预警及事件应急处置提供技术支撑，形成数据要素流通的可审计、可追溯能力，有效推动各参与方履行数据安全保护义务、切实采取有效数据安全保障措施，促进数据流转生态体系的良性构建。

**（8）引导企业持续提升数据安全能力，开创数据要素市场自律有序流动的良好局面**

国家标准 GB/T37988-2019《信息安全技术 数据安全能力成熟度模型》（简称 DSMM）将组织的数据安全能力划分成非正式执行级、计划跟踪级、充分定义级、量化控制级、持续优化级五个持续提升的等级，从组织建设、制度流程、技术工具、人员能力四个维度对数据全生命周期的数据处理活动进行安全要求的全面明确。基于 DSMM 的能力成熟度等级，对组织参与数据流通、交易、共享的业务类型和范围形成有力约束，建立“数据安全能力越强，高价值数据获取机会越多，意味着更多业务潜能”的正向驱动模式，驱动组织积极主动提升数据安全能力，建设以数据为中心的数据安全治理体系，围绕数据

采集汇聚、加工处理、流通交易、共享利用等环节，建立数据流通全流程安全防护体系，有效降低确保数据流通、开发利用等过程中的数据安全风险，充分落实数据安全治理责任，为推动数据分类分级确权授权机制的落实提供支撑，逐步建成数据流通交易各方互信机制，助力数据要素市场自律发展。

## （三）“东数西算”数据安全体系建设研究

“东数西算”工程已全面启动，在全国布局了贵州、内蒙古、甘肃、宁夏、粤港澳大湾区、成渝地区、长三角地区、京津冀地区等八个国家算力枢纽节点，节点之间建立高速直联网络，从而支撑大规模算力调度，使算力资源有序向西部转移，形成以数据流为导向的新型算力网络格局。可以看到，算力调度将引发大规模数据的频繁流动和使用，而且，国家级的数据中心集群无疑将会引来国家级的、有组织的高级网络安全威胁。因此，数据安全将成为“东数西算”工程能否成功推进的关键因素，应从如下三个方面进行体系化的建设：

**一是强化数据安全治理。**建立数据安全能力成熟度模型（DSMM）测评认证的工作机制、组织和业务支撑平台，对“东数西算”数据相关方组织（提供方、接收方、处理方等）进行数据安全能力测评认证，从组织建设、制度流程、技术工具和人员能力四个方面系统提升组织的数据安全能力，从而有效管控数据跨组织、跨平台甚至跨境流通的安全风险。对“东数西算”网络运营者进行数据安全管理认证，以规范数据处理活动，加强数据安全保护。同时，建立和完善数据安全测评的相关机制、组织和安全检测评估手段，对出境数据进行安全评估，对数据中心的数据和数据服务进行量化风险评估。

**二是建设数据安全基础设施。**在加密、访问控制、数据库安全等常规数据安全手段基础上，面向数据流通共享和开发利用需求建设专门的数据安全基础设施，至少包括：数据资产安全管理平台，对枢纽

节点备份数据和离线计算大数据进行安全管理，更好支撑西部枢纽节点的后台加工、离线分析、存储备份等业务；大数据安全监管审计平台，为枢纽节点运营方提供数据处理活动感知、数据安全态势感知和应急处置等能力，以全面掌握本地计算任务、数据处理情况和数据安全合规状况；数据安全计算与共享交换平台，为枢纽节点提供数据安全传输、数据访问与检索安全、本地数据计算安全、多源数据联合安全计算、数据交易安全等能力，来支撑不同层次的数据流通共享与融合需求。

**三是建设高级安全威胁主动防御基础设施。**建设安全大脑及相关附属基础设施，通过“大数据安全分析+人工智能驱动+历史安全大数据+安全专家运营”相结合，各枢纽节点的协同联动，形成强大的高级数据安全威胁主动防御能力，防范数据窃取、数据泄露和加密勒索等安全风险。建设大数据安全靶场，虚实结合提升枢纽节点应对高级数据安全威胁的能力，同时培训合格的安全运营人员。

## （四）“东数西算”数据安全沙龙观点荟萃

为进一步探究东数西算工程的数据安全问题，11 月 16 日，BDS 国家工程研究中心策划举办了一期“东数西算”工程数据安全沙龙，邀请了国家信息中心、国家信息技术安全研究中心、甘肃省信息中心、韶关市发改局、贵州大数据安全工程研究中心、中国国际工程咨询有限公司、北京信百会信息经济研究院、新安盟数据安全专委会、融安

数科和太极集团等单位的领导和专家，就“东数西算”工程数据安全的需求与痛点、数据安全体系建设等问题进行了深入的探讨和交流，形成了如下观点。

数据安全成为“东数西算”工程能否成功推进的关键因素。“东数西算”工程将推进云网协同和算网融合发展，构建算力、算法、数据、应用资源协同的全国一体化大数据中心体系，其面临的数据安全风险变得复杂，数据应用场景多样，潜在攻击的暴露面和攻击路径增加，云网边端数据应用各环节都可能成为攻击目标，数据安全成为关键。为此，BDS 国家工程中心常务副主任杜跃进指出，“东数西算”工程作为国家的重大战略，其数据安全问题的解决，目前市面上并没有成熟方案，也不是一个一蹴而就的事情，需要持续改进，包括标准、方案、技术、能力等。不同枢纽和集群在“东数西算”工程整个部署里的定位、其数据本身、其所支撑的业务都不一样。数据安全方案应该有针对性，要贴近各自具体的应用、场景和特点来设计。

**数据安全顶层设计至关重要。**《全国一体化大数据中心协同创新体系算力枢纽实施方案》等文件明确了“数盾”体系和网络数据安全要求，但安全体系如何设计尚在研究之中。BDS 国家工程中心副主任钟力提出，需重点从数据安全治理、数据安全保障、高级安全威胁抵御三个层面，进行“东数西算”工程的数据安全顶层设计。国家信息中心首席工程师李新友指出，安全顶层规划非常重要，目前国家信息中心正牵头“数盾”体系技术架构的设计。国家信息中心陈东博士认

为，“东数西算”工程作为推动全国一体化大数据中心体系建设的落地性工程，安全在其中占据至关重要的位置，“数盾”是与其他“四数”环环相扣、紧紧相连。国家信息技术安全研究中心总师组专家李京春指出，云网协同是未来趋势，在前期规划中需要将安全前置，数据安全、网络安全和个人信息保护安全需要在建设初期同步进行规划设计，并确定具体的统筹部门。甘肃省信息中心副主任朱洪林、韶关市发改局副局长李剑虹、北京信百会信息经济研究院研究部主任安宜贵、新安盟数据安全专委会秘书长金舒原也都认为亟需加强整体规划，进行安全体系特别是数据安全的顶层设计。

**需发挥标准的引领和规范作用。**国家信息中心首席工程师李新友认为，需要制定一套全国一体化大数据中心体系安全保障、管理和技术方面的统一标准。贵州大数据安全工程研究中心常务副主任刘东昊同样认为标准特别重要，比如数据交易安全评估、数据安全能力测评认证、枢纽节点数据安全建设、安全管理和运营，都需要依据标准；标准研制可以一步步来，国家标准、行业标准、地方标准做到相互补充。甘肃省信息中心副主任朱洪林指出，数据安全技术和产品的评价指标、数据中心安全管理、云网协同安全能力、体系架构和工程组织实施等方面，均需要标准规范。

**需构建全国一体化大数据中心的数据安全治理体系。**算力调度本质上是数据调度，将引发大规模数据的频繁流动和使用，数据安全治理将变得非常重要。BDS 国家工程中心副主任钟力认为，应建立基

于数据安全能力成熟度模型（DSMM）的数据安全治理体系，在数据侧对数据进行分类分级、数据资产安全管理和数据安全评估，在组织侧对“东数西算”工程数据相关方（数据提供方、接收方、处理方等）进行 DSMM 测评认证，持续提升组织数据安全能力，在数据与组织间形成正向驱动关系，从而有效管控跨组织、跨平台甚至跨境数据流通的安全风险。贵州大数据安全工程研究中心常务副主任刘东昊进一步给出了东数西算数据交易场景下的安全思路：一是对数据交易主体进行数据安全能力评估，二是对数据或算力进行安全评估。

**需同步规划建设数据安全基础设施。**为保障数据安全，促进数据的流通共享和开发利用，除了数据中心、云平台和云网协同等的网络安全建设，“东数西算”工程需建设专门的数据安全基础设施。BDS 国家工程中心副主任钟力认为，枢纽节点需建设部署数据资产安全管理、大数据平台数据安全管理、数据流通共享安全（数据共享交换、数据公共服务、隐私计算）等基础设施，实现数据安全态势感知和安全的数据开放利用。融安数科创始人兼 CEO 李登峰也认为，通过隐私计算可以保护数据流通的安全，促进数据流通共享，目前隐私计算在金融、医疗、运营商等行业领域应用较广泛。

**需建设高级安全威胁主动防御基础设施。**“东数西算”工程的十个国家数据中心集群大都分布在经济不太发达、人才相对缺乏的三四线城市，与此同时它们又是国家级的关键信息基础设施，存储了海量的重要数据与核心数据。这无疑将会引来国家级的、有组织的高级网

络安全威胁。BDS 国家工程中心副主任钟力认为，各枢纽节点需建设安全大脑及相关附属基础设施，通过“大数据安全分析+人工智能驱动+历史安全大数据+安全专家运营”相结合，形成强大的高级安全威胁主动防御能力，从而防范各类网络安全和数据安全风险。同时，建设虚实结合的大数据安全靶场，来提升枢纽节点应对高级安全威胁的能力，并培训合格的安全运营人员。国家信息中心首席工程师李新友还指出，应建设针对全国一体化大数据中心体系的安全应急监测和应急响应队伍。

**需加强数据安全人才培训。**《数据安全法》、《网络数据安全管理条例（征求意见稿）》等均明确提出数据安全专业人才需求。各枢纽节点尤其西部地区人才相对缺乏，与“东数西算”工程数据安全要求还不相匹配，亟需大量培养数据安全管理和技术人才。国家信息中心首席工程师李新友、国家信息技术安全研究中心总师组专家李京春和北京信百会信息经济研究院研究部主任安宜贵均提出，枢纽节点的长期持续运营离不开人才，要加强人才培训。对此，甘肃省信息中心副主任朱洪林介绍了庆阳枢纽节点人才培养的情况，“规划依托庆阳本地高校和高职院校的信息工程学院进行专业调整和加强建设，成为服务东数西算集群的人才培训地点。”BDS 国家工程研究中心推出的注册数据安全官、数据安全工程师和 DSMM 测评师培训，能够为东数西算培养和输送大量数据安全专业人才。

**需围绕枢纽节点培育产业生态，推进可持续安全运营。**韶关市发改局副局长李剑虹称，政府有责无旁贷建设好枢纽节点的责任，除了当地政府、国家加大投入力度外，也希望企业可以筹建资金，通过共同成立的平台公司，找到盈利点，使枢纽节点长久、健康地运转发展。国家信息技术安全研究中心总师组专家李京春指出，可考虑建设全国统一大市场，加强跨区域跨部门的产业融合。北京信百会信息经济研究院研究部主任安宜贵认为，政府的重点应该是培育数据中心上下游的产业，来创造当地税收点和就业机会，出台政策激励企业通过市场的机制来制造盈利点。

“东数西算”工程的不同枢纽节点和集群各有其特点，其数据安全到底该怎么建设、跟产业之间怎么合作、方案如何持续改进、如何围绕着自身特点和业务来做等问题，都是需要持续研究的内容。作为大数据安全领域唯一的国家工程研究中心，BDS 国家工程研究中心承担着给国家有关部门建言献策、开展技术创新、成果转化和带动产业进步的任务。BDS 国家工程研究中心希望能够与政府相关部门、“东数西算”工程的建设运营单位、数据安全产业界、学术界等相关方持续进行研究讨论，从不同的角度来提出意见和建议，从而不断优化“东数西算”工程数据安全的架构设计、技术方案、管理能力和运营水平，为国家重要战略保驾护航。

# 领航计划
# — 未来数据安全人才专场培训

## 大数据协同安全技术国家工程研究中心

## 重磅消息

提供三大方向数据安全人才培训服务：

**注册数据安全官（CDSO）** 着眼于数据安全顶层规划设计与统筹管理，旨在培养业界一流的数据安全领导者。

**注册数据安全工程师（CDSE）** 着眼于数据安全方案的落地实施，旨在培养专业的数据安全工程技术人才。

**DSMM 测评师** 着眼于 DSMM（数据安全能力成熟度模型）实施，旨在培养专业的数据安全工程技术人才。

## 往期精彩

2021 年 10 月至 2022 年 11 月，“领航计划 — 未来数据安全人才培训”项目已成功举办 4 期，并首次引入新一代聚会元宇宙平台——“N 世界”，通过线上元宇宙沉浸平台的新模式打造首个未来数据安全专业人才培训，吸引了来自政府、交通、运营商、烟草、电网、医疗、金融等行业领域单位的信息部门领导、技术工程师以及大批数据安全从业者参训。

## 讲师团队

讲师团队由大数据协同安全技术国家工程研究中心 11 家联合单位、技术委员会和顾问委员会的资深安全专家，以及业内知名大咖组成，具备多年实践经验和极高的理论技术水平，以确保业内顶级教学质量。

## 培训课程

培训课程围绕数据安全治理方法论、数字经济与数据安全形势、数据安全法律法规、数据安全标准规范、数据安全技术与方案以及大数据安全实践等内容，针对企业数据安全需求，采用模块化教学方法，通过理论讲授、案例分析、互动讨论、讲师点评、项目展示等多种教学手段与方法，帮助学员快速提升数据安全专业技术水平。

**国内率先创立“数据安全官”品牌并开展培训**

**欢迎扫码垂询**

## 《数字安全观察》产品系列

- 每周动态：政策法规/行业动向/安全事件/技术趋势
- 深度分析：政策解读/行业洞察/市场预测/事件分析/技术前瞻/策略建议/国际智库精编
- 国防专刊：网空战略/力量建设/科装动态/空天态势
- 数据安全专刊：政策形势/安全事件/安全研究/大咖观点
- 公安专刊（筹备中）

**总编辑：**杜跃进

**执行编辑：**张义荣

**本期编委：**钟力、唐会芳、王雨薇、陈璐