

超配（维持）

计算机行业深度报告

数据安全赛道长坡厚雪

2023 年 4 月 27 日

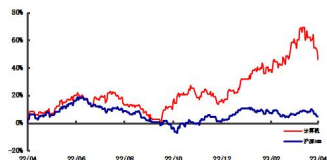
投资要点：

分析师：罗伟斌
SAC 执业证书编号：
S0340521020001
电话：0769-22110619
邮箱：
luoweibin@dgzq.com.cn

分析师：刘梦麟
SAC 执业证书编号：
S0340521070002
电话：0769-22110619
邮箱：
liumenglin@dgzq.com.cn

分析师：陈伟光
SAC 执业证书编号：
S0340520060001
电话：0769-22110619
邮箱：
chenweiguang@dgzq.com.cn

行业指数走势



资料来源：东莞证券研究所，Wind

相关报告

- **三维度看数据安全需求释放。**1) 近年全球数据泄露事件频频发生，数据泄露所造成的损失进一步上升。未来随着5G高速网络普及、万物互联场景实现，数据有望迎来井喷期。面对快速增长的数据量，数据风险敞口将进一步扩大，特别是大国博弈的背景下，数据安全亟需重视。2) 近年全球主要国家进一步加大了对于数据的重视程度，通过立法建立较为完善的数据保护、数据安全的框架，企业数据安全合规要求进一步提升，有望带来数据安全产品需求的增加。3) 数据要素是数字经济发展的关键，近年我国积极推动数据要素市场的发展，数据安全作为数据要素产业链核心环节，亦有望充分受益。工信部等十六部门在今年1月下发《促进数据安全产业发展的指导意见》，明确到2025年，我国数据安全产业规模超过1500亿元，年复合增长率超过30%。
- **数据安全贯穿数据全生命周期管理，行业领军企业产品矩阵丰富。**数据安全贯穿数据全生命周期管理，涉及从数据的采集、传输、存储到数据处理、交换、销毁等众多环节，每个环节都涉及相应技术和产品，行业增量空间巨大。综合型网络安全厂商由于普遍具有较强的技术背景、资金实力，布局数据安全领域有一定的先发优势，比如深信服、奇安信、启明星辰等相关公司，大部分在隐私计算、数据脱敏、数据泄露防护、数据库审计、防火墙、数据分类分级等领域有所布局，产品矩阵较为丰富。随着行业需求释放，部分公司数据安全产品的收入也进入到高速增长阶段。其中，2022年，电科网安数据安全业务收入同比大幅增长135%；奇安信数据安全产品收入同比增长55%以上；启明星辰数据安全2.0&3.0业务同比增长41%，呈现快速增长的态势。
- **投资建议：**在数据风险敞口扩大、政策合规需求以及数据要素市场加快发展等因素推动下，数据安全赛道长坡厚雪，国家政策明确2025年数据安全产业规模超过1500亿元，年复合增长率超过30%。综合型网络安全厂商由于具有较强的技术背景、资金实力，在数据安全领域的布局上有一定先发优势，大部分在隐私计算、数据脱敏、数据泄露防护、数据库审计、防火墙、数据分类分级等领域有所布局，产品矩阵丰富，有望形成强者恒强的态势。建议关注天融信、电科网安、启明星辰、绿盟科技、安恒信息、奇安信-U等相关标的。
- **风险提示：**政策推进不及预期；行业竞争加剧等。

本报告的风险等级为中高风险。

本报告的信息均来自已公开信息，关于信息的准确性与完整性，建议投资者谨慎判断，据此入市，风险自担。

请务必阅读末页声明。

目 录

1. 三维度看数据安全需求释放	3
2. 数据安全贯穿数据全生命周期管理，行业领军企业产品矩阵丰富	9
3. 投资建议	15
4. 风险提示	15

插图目录

图 1：近年全球数据泄露事件及数据泄露量	3
图 2：近年全球数据泄露平均损失	3
图 3：按行业分类，2022 年全球数据泄露平均损失（单位：百万美元）	4
图 4：近年全球数据流量情况	4
图 5：近年我国数据产量情况	4
图 6：2021 年全球主要国家数字经济规模	6
图 7：近年我国数字经济规模	6
图 8：近年数据要素对我国 GDP 贡献率	7
图 9：国网上海市电力公司提供的企业电智绘产品	7
图 10：我国数据要素市场规模	9
图 11：数据要素产业链	9
图 12：2021 年我国数据泄露防护市场份额	11
图 13：静态数据脱敏示意图	11
图 14：动态数据脱敏示意图	12
图 15：数据脱敏领域代表厂商	12
图 16：隐私计算三种技术方向	13
图 17：星环科技 Sophon P ² C 隐私计算平台	13
图 18：我国隐私计算市场规模	13
图 19：隐私计算市场竞争格局潜力象限	14

表格目录

表 1：数据安全贯穿数据全生命周期管理	5
表 2：近年关于大数据市场发展的政策	8
表 3：数据安全贯穿数据全生命周期管理	9
表 4：DLP 产品分类	10
表 5：布局数据安全领域的相关公司	14
表 6：重点公司盈利预测及投资评级（截至 2023/4/26）	15

1. 三维度看数据安全需求释放

1.1 数据井喷时代，风险敞口扩大

国际电信联盟将网络安全定义为用于保护网络环境、机构组织以及用户资产的政策、理念、技术等集合，主要提供保障网络可靠性、安全性的产品和服务。随着云计算、大数据、工业互联网等新兴技术的加速发展与应用，网络安全的内涵进一步丰富、边界进一步扩大，涉及到互联网、电信网、物联网、计算机系统、通信系统、工业控制系统等在内的所有系统相关的设备安全、数据安全、行为安全、内容安全等。数据安全指的是通过采取必要措施，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。与网络安全相比，数据安全更加具有针对性，数据在哪里，安全在哪里。

全球数据泄露事件频发，泄露损失进一步上升。近年针对数据的攻击、窃取、滥用等事件频频发生，对经济社会产生了巨大影响。2022 年包括英伟达、三星电子、Twitter 等公司相继发生数据泄露事件。其中，社交平台巨头 Twitter 在 22 年 7 月遭黑客攻击泄露了超过 540 多万用户数据，涉及邮件及电话号码等信息；今年 1 月，Twitter 用户数据再次发生泄露，有超过 2.35 亿个账号数据被泄露，涉及用户的名称、ID 等相关信息。据 Flashpoint 数据显示，2022 年全球发生数据泄露事件 4,518 件，事件数量虽有所下降，但泄露的数据量仍处于高位，2022 年达到 226.2 亿条。从数据泄露的损失来看，据 IBM 数据，2022 年全球数据泄露的平均损失进一步上升，达到 435 万美元。其中，数据泄露平均损失前五大行业分别为医疗、金融、制药、科技、能源等关键行业。

图 1：近年全球数据泄露事件及数据泄露量



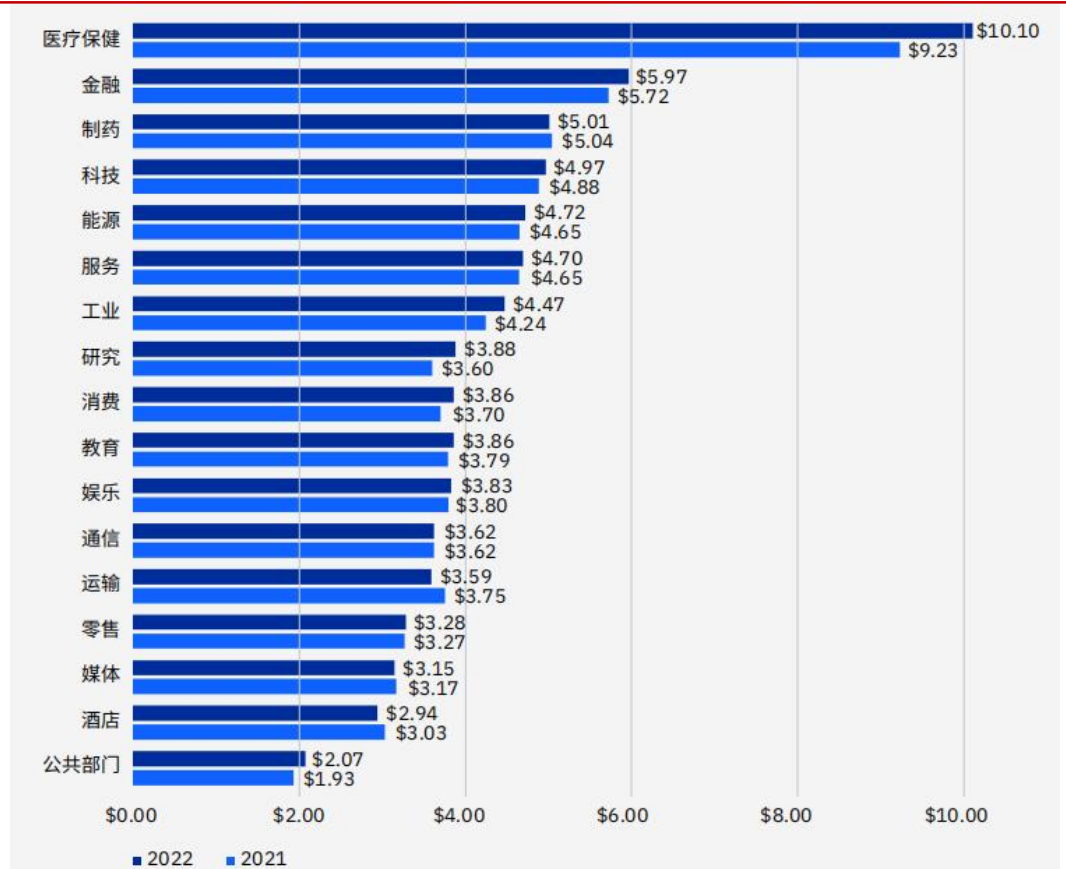
数据来源：Flashpoint, RBS, 东莞证券研究所

图 2：近年全球数据泄露平均损失



数据来源：IBM, 东莞证券研究所

图 3：按行业分类，2022 年全球数据泄露平均损失（单位：百万美元）



数据来源：IBM，东莞证券研究所

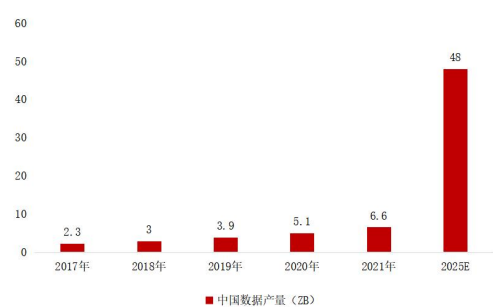
数据井喷时代来临，数据安全亟需重视。随着信息技术发展，通信基础设施不断完善，即时通信、短视频、网络游戏等消费级应用的革命带来了 C 端数据流量的爆发，而各行各业的信息化建设也进一步积累了 B 端的应用数据。未来随着 5G 高速网络普及、万物互联场景实现，数据有望迎来井喷期。据 Statista 预测，到 2025 年全球数据流量有望达到 181ZB，2021-2025 年复合增速为 23.03%。国内方面，预计到 2025 年数据量有望达到 48ZB（数据来源：易华录公告），2021-2025 年复合增速高达 64.22%，大幅高于全球的平均水平；同时，国内数据量占全球的比重也将从 2021 年的 8.35% 大幅提升至 2025 年的 26.52%。面对快速增长的数据量，数据风险敞口将进一步扩大，特别是大国博弈的背景下，数据安全亟需得到重视。

图 4：近年全球数据流量情况



数据来源：Statista，东莞证券研究所

图 5：近年我国数据产量情况



数据来源：观研网，易华录公告，东莞证券研究所

1.2 政策聚焦数据安全，合规要求进一步提升

随着数据在数字经济发展中的重要性不断凸显，以及近年数据风险事件的频频发生，全球主要国家进一步加大了对于数据的重视程度，通过立法建立较为完善的数据保护、数据安全的框架，企业数据安全合规要求进一步提升，有望带来数据安全产品需求的增加。

具体来看，欧盟在 2018 年发布了史上最为严格的数据管理法规《通用数据保护条例》（GDPR），该条例赋予了数据主体更多的权利，包括被遗忘权、可携带权等，同时进一步拓展了用户数据的保护范围，除了姓名、证件号码、地址等常规数据外，还将种族、宗教信仰等数据纳入保护范围。此外，GDPR 进一步加大对于数据处理者的合规力度，要求企业对数据的安全性、可用性、保密性和完整性负责，只要企业有收集、存储、处理欧盟境内相关数据的行为，均受到 GDPR 的约束。在处罚方面，GDPR 对于有严重违规行为的企业，最高可处以全球收入的 4%或 2000 万欧元的罚款（以较高者为准），企业的数据合规成本进一步上升。据 DLA Piper 数据，2022 年欧洲数据监管机构针对 GDPR 违规的罚款已经超过 29 亿欧元，同比大幅增长 2 倍。

美国方面，2022 年 6 月参众两院发布了《数据隐私和保护法》（ADPPA）草案，是获得两党两院支持的美国联邦全面隐私保护提案。相较于以往州级立法定义的敏感数据往往侧重于监控和人口统计信息等，此次法案进一步扩大敏感数据的定义，将收入水平、语音邮件、文字消息、与 17 岁以下儿童的有关数据纳入到敏感数据范围。同时，法案对大数据持有者设置了个人信息保护的额外义务，进一步强化其告知义务，包括提供隐私影响评估、算法影响评估等内容。

我国在 2021 年相继发布《数据安全法》、《个人信息保护法》等顶层设计加大对于数据安全的保护力度，为数据和个人信息保护提供了重要法律依据。在数据安全保护方面，《数据安全法》提出要对数据实行分类分级保护制度；开展数据处理活动的相关方应当采取相应的技术措施保障数据安全，要加强风险监测，定期开展风险评估等内容。《个人信息保护法》提出不得过度收集个人信息，个人信息处理者应当保障所处理的个人信息的安全。在法律责任方面，《数据安全法》、《个人信息保护法》加大对于违法活动的追究力度，其中《个人信息保护法》指出对于情节严重的违法行为，可以处五千万元以下或者上一年度营业额百分之五以下罚款。

表 1：数据安全贯穿数据全生命周期管理

地区	政策	主要内容
欧盟	《通用数据保护条例》	条例是欧盟法律中关于欧盟和欧洲经济区 (EEA) 数据保护和隐私的条例，解决了在欧盟和欧洲经济区区域之外传输个人数据的问题，主要目标是加强个人对其个人数据的控制和权利，并简化国际业务的监管环境。
美国	《数据隐私和保护法》	作为首份获得两党支持的美国联邦层面的综合性隐私保护法草案，该法案的目标是建立一个强有力的国家框架，保护消费者的数据隐私和安全，防止美国人的数据被歧视性地使用等，其中涵盖了数据最小化、忠诚义务、私人诉讼权、优先适用、特殊群体数据保护、大型数据持有者义务等核心内容。
中国	《数据安全法》	为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。该法一共七章内容，涉及总则、数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放、法律责任以及附则。

《个人信息保护法》

为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。该法一共八章内容，涉及总则、个人信息处理规则、一般规定、敏感个人信息的处理规则、国家机关处理个人信息的特别规定、个人信息跨境提供的规则、个人在个人信息处理活动中的权利、个人信息处理者的义务、履行个人信息保护职责的部门、法律责任以及附则。

数据来源：百度百科、维基百科、君合法律，东莞证券研究所

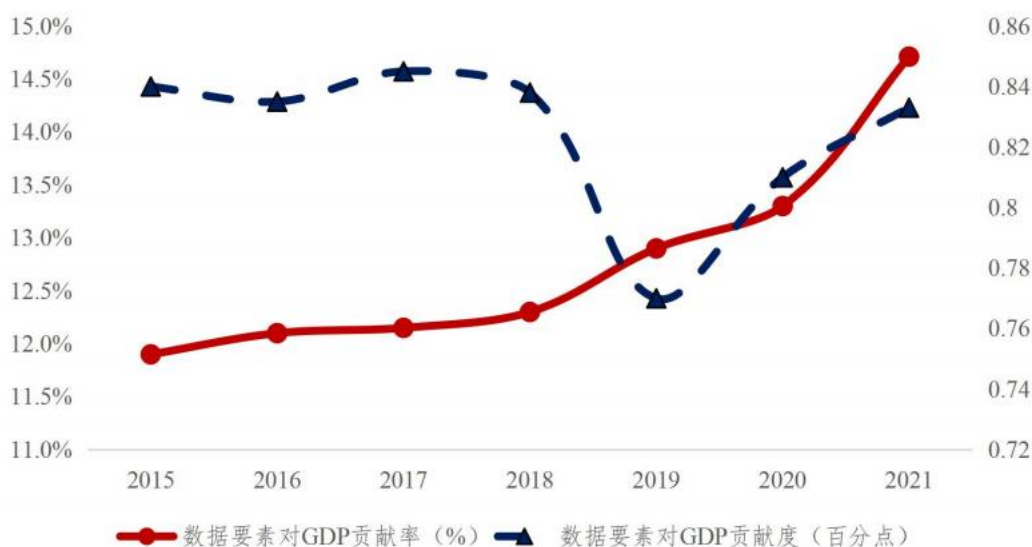
1.3 数据要素市场加快发展，带动数据安全需求释放

数字经济成为经济发展主要驱动力。随着信息技术的发展，数字经济成为继农业经济、工业经济后的主要经济发展形态，全球主要国家积极抢占数字经济发展的制高点，2021年全球47个主要国家的数字经济规模达到38.1万亿美元。其中，我国2021年数字经济规模为45.5万亿元，2017-2021年复合增速13.73%，数字经济占GDP的比重从17年的32.69%提升至21年的39.59%，逐渐成为我国经济发展的主要驱动力。据信通院预测，到2025年，我国数字经济市场规模有望突破60万亿元。

图 6：2021 年全球主要国家数字经济规模



图 8：近年数据要素对我国 GDP 贡献率



数据来源：《中国数据要素市场发展报告（2021-2022）》，东莞证券研究所

从供需角度来看，数据需求方需求旺盛，数据供方价值有望重塑。对于数据需求方来说，丰富的数据要素资源能够进一步赋能自身的生产经营、业务发展，如银行在对企业客户信贷需求进行评估时，除了关注企业自身提供的经营数据外，也可以通过企业注册、判决、用电等外部数据进行分析辅助决策。对于数据供给方来说，数据资产入表政策出台，数据供方价值有望重塑。2022 年 12 月，财政部发布《企业数据资源相关会计处理暂行规定（征求意见稿）》，提出对于企业内部使用的数据资源，可确认为无形资产；对于企业对外交易的数据资源，可确认为存货。过去数据要素的价值并未充分反映在报表上，此次数据资产入表政策的出台，通过建立数据资源相关会计处理准则，有助于全面反映数据资产的价值，数据持有方价值有望得到重估。

图 9：国网上海市电力公司提供的企业电智绘产品



数据来源：上海数据交易所，东莞证券研究所

从政策角度来看，近年政策支持加快数据要素市场化建设。2019年10月，十九届四中全会首次明确将数据纳入生产要素，数据要素的重要性进一步凸显。随着最高层对数据要素的定调落地后，国家陆续出台推进数据要素市场发展的基础制度文件。地方性政府层面，今年烟台、武汉等地陆续出台推动数据要素市场发展的相关行动计划。此外，今年出台的《党和国家机构改革方案》提出要组建国家数据局，专门负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等。此次国家数据局的组建将有助于进一步发挥中央集中统筹数据要素发展、打通全国数据壁垒的作用。

表 2：近年关于大数据市场发展的政策

时间	文件	内容
2019/10	十九届四中全会《关于坚持和完善中国特色社会主义制度 推进国家治理体系和治理能力现代化若干重大问题的决定》	健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制。
2020/04	关于构建更加完善的要素市场化配置体制机制的意见	加快培育数据要素市场。推进政府数据开放共享。提升社会数据资源价值。加强数据资源整合和安全保护。
2022/01	关于印发要素市场化配置综合改革试点总体方案的通知	探索建立数据要素流通规则。完善公共数据开放共享机制。建立健全数据流通交易规则。拓展规范化数据开发利用场景。加强数据安全保护。
2022/04	关于加快建设全国统一大市场的意见	打造统一的要素和资源市场。加快培育数据要素市场，建立健全数据安全、权利保护、跨境传输管理、交易流通、开放共享、安全认证等基础制度和标准规范，深入开展数据资源调查，推动数据资源开发利用。
2022/01	“十四五”数字经济发展规划	数据要素市场体系初步建立。数据资源体系基本建成，利用数据资源推动研发、生产、流通、服务、消费全价值链协同。数据要素市场化建设成效显著，数据确权、定价、交易有序开展，探索建立与数据要素价值和贡献相适应的收入分配机制，激发市场主体创新活力。充分发挥数据要素作用。强化高质量数据要素供给。加快数据要素市场化流通。
2022/12	关于构建数据基础制度更好发挥数据要素作用的意见	建立保障权益、合规使用的数据产权制度；建立合规高效、场内外结合的数据要素流通和交易制度；建立体现效率、促进公平的数据要素收益分配制度；建立安全可控、弹性包容的数据要素治理制度；保障措施。
2022/12	企业数据资源相关会计处理暂行规定（征求意见稿）	拟对数据资源的相关会计处理做出规定。对于企业内部使用数据资源，确认为无形资产，并对数据资源无形资产进行摊销；对于企业对外交易的数据资源，确认为存货，并对数据资源存货计提跌价准备。
2023/02	数字中国建设整体布局规划	指出要畅通数据资源大循环，释放商业数据价值潜能，加快建立数据产权制度，开展数据资产计价研究，建立数据要素按价值贡献参与分配机制。
2023/03	党和国家机构改革方案	提出组建国家数据局，由国家发展和改革委员会管理，负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等。
2023/4/14	武汉市数据要素市场化配置改革三年行动计划（2023—2025年）	到2023年，完善数据要素市场化配置改革工作制度体系框架，组建武汉数据集团，探索开展公共数据授权运营，制定数据要素标准体系，形成数据要素利用示范性成果，初步搭建起数据要素市场化整体框架。2024年，完善数据基础制度体系，初步建立数据要素市场化配置合规和监管体系，深化数据要素创新应用，大力培育各类数据服务市场主体，全面推进数据要素赋能产业数字化转型。2025年，数据要素市场化配置体制

		机制基本建立，数据资源汇聚治理、数据要素运营和交易、数据要素市场培育等体系基本形成，数据要素赋能实体经济发展成效凸显。
2023/4/10	烟台市激活数据要素潜能发挥数据要素作用行动方案(2023-2025年)	依托“数字烟台”建设成果，创新公共数据管理体制，构建数据要素市场供给、流通、应用、监管“四位一体”体系，建立全市统一开放的数据要素市场。到 2025 年底，公共数据授权运营模式、数据要素流通交易模式更加成熟，数据要素市场化配置更加高效，“政府供给激发社会应用、政府应用带动社会供给”的数据要素双轮驱动机制基本建立。

数据来源：互联网公开资料，东莞证券研究所

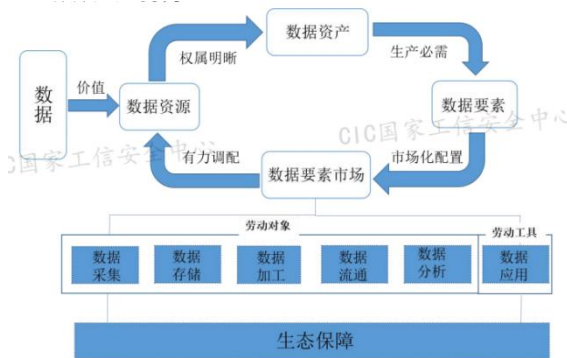
数据安全作为数据要素产业链核心环节有望充分受益。无论是从供需角度，或是政策角度，数据要素市场化建设有望加快发展，据国家工信安全发展研究中心预测，到 2025 年我国数据要素市场规模有望达到 1749 亿元，2022-2025 年复合增速达 28.99%。数据安全作为数据要素产业链核心环节，亦有望充分受益。

图 10：我国数据要素市场规模



数据来源：国家工信安全发展研究中心，东莞证券研究所

图 11：数据要素产业链



数据来源：国家工信安全中心，东莞证券研究所

2. 数据安全贯穿数据全生命周期管理，行业领军企业产品矩阵丰富

今年 1 月，工信部等十六部门下发《促进数据安全产业发展的指导意见》，对数据安全产业的市场规模提出了明确目标，指出到 2025 年，我国数据安全产业规模超过 1500 亿元，年复合增长率超过 30%。数据安全贯穿数据全生命周期管理，涉及从数据的采集、传输、存储到数据处理、交换、销毁等众多环节，每个环节都涉及相应技术和产品，行业增量空间巨大，关注 DLP、数据脱敏、隐私计算等技术产品。

表 3：数据安全贯穿数据全生命周期管理

环节	内容
数据采集安全	主要关注数据的分类分级和数字签名
数据访问控制	需要保证数据资源访问的统一认证与实时控制，主要技术手段包括 PAM 和零信任；
数据传输安全	通过密码技术、VPN、DLP、云桌面、RBI 等技术保证数据的传输安全；
数据存储安全	对于结构化数据，主要涉及数据库加解密、存储备份与恢复；对于非结构化数据，可采用电子文档管理和加密技术；
数据处理安全	可采用数据脱敏技术进行数据变形；可采用数据库审计或数据库防火墙对相关操作进行记录，对数据

	库遭受的风险进行实时的预警与阻断；
数据交换安全	关注隐私计算和应用之间的接口调用安全；
数据安全服务	通过前期咨询与调研，了解企业业务系统、厘清业务流程、掌握业务数据及访问权限等。而后，对企业的组织架构、制度体系、安全策略进行有效规划。最后，通过风险监测、紧急响应等系列手段，动态保障数据安全。
数据安全治理平台	数据资产进行可视化管理，对数据安全设备进行联动管控，进一步做到数据安全主动防御。

数据来源：山石网科，东莞证券研究所

数据泄露防护（DLP）：防止敏感数据泄露。DLP 是指通过一定的技术手段，通过数据识别技术以及设定的安全策略，对存储和使用过程中的敏感信息进行发现、监测和保护，防止敏感数据违反安全策略流出。根据应用场景不同，DLP 可分别终端 DLP、网络 DLP、邮件 DLP、应用 DLP 以及发现 DLP 等。其中，天融信的终端 DLP 在终端主机安装后，能够捕获终端存储的敏感数据，监控文件外发、文件拷贝等多种操作，并对违规的行为进行警告、阻断、追溯等操作，进一步降低数据泄露的风险。据 IDC 数据，2021 年我国数据防泄漏市场规模为 1.25 亿美元，同比大幅增长 39.2%。从行业格局来看，行业头部企业如天空卫士、亿赛通、明朝万达，均出身于数据安全领域，2021 年市场份额分别为 23.1%、16.3%和 11.2%；天融信市场份额排第四，为 8.4%。

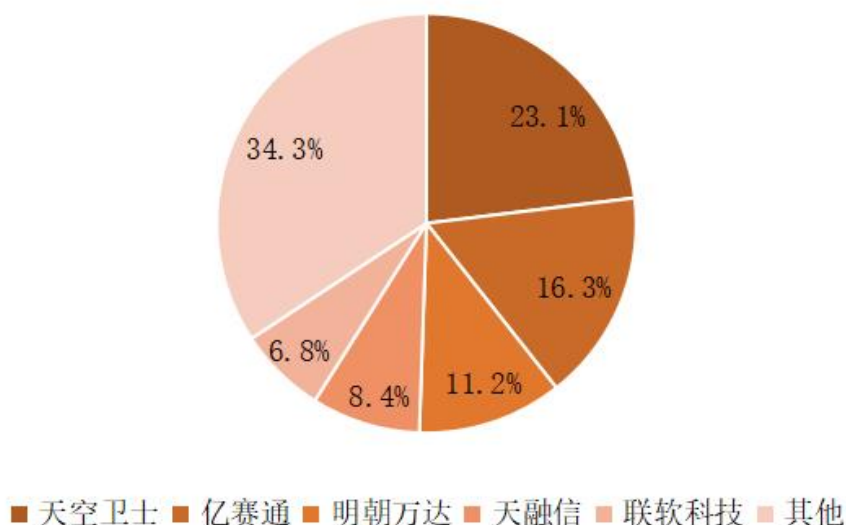
表 4：DLP 产品分类

产品	介绍
终端数据防泄漏（终端 DLP）	系统采用底层数据截取和数据内容检测技术，能够有效挖掘终端 PC 存在的敏感数据，并主动监听用户文件外发、文件拷贝、文件打印等多种操作，对违规外泄敏感文件行为进行记录、告警、隔离、阻断等操作，全方位提升用户数据安全防护措施，保证用户敏感数据安全。
网络数据防泄漏（网络 DLP）	对敏感数据实施事中、事后全面保护与审计的独立网关类产品，可以对网络传输协议 SMTP、http/https、FTP、SMB 等以及 RESTful 接口传输数据进行抓取，基于深度内容识别技术，通过定义关键字、指纹库、数据标识符、权重词典、机器聚类等多种敏感数据规则，对传输数据进行监测，对违规传输行为作出告警、审计、阻断、审批等响应。
邮件数据防泄漏（邮件 DLP）	通过纯透明代理、正反向代理、旁路监听、MTA 等多种部署形式针对企业员工发送邮件中的内容进行深度内容感知，可基于关键字、正则表达式、指纹库、数据标识符、文件属性、机器聚类检测条件构建的数据安全防护策略对邮件外发内容进行深度检测识别和审计保护，有效阻止员工有意识或无意识地将企业核心敏感数据资产以电子邮件的形式外发造成泄漏的行为。
应用数据防泄漏（应用 DLP）	通过对 HTTP/HTTPS 的内容进行读取分析，识别发现 API 接口，自动识别网络中活跃的 API 接口数据，发现对外暴露接口类型、接口传输数据；基于事前备案的接口信息，发现违规接口传输行为、违规传输接口内容，统计风险接口数量、风险接口事件；针对备案的合规接口进行全量审计，并绘制多视角画像，包括应用画像、接口画像、账户画像、IP 画像。可应用于 IPv4、IPv6、云等多种场景。
发现数据防泄漏（发现 DLP）	通过以自动扫描为主、人工手动标记为辅的方式，实现对数据的资源探测、数据扫描、分类分级、数据资产可视化。系统内置金融、电信、工业等多种行业模板以及大量的数据识别规则库，可精准高效的梳理并标识数据资产，建立数据分类分级清单，帮助企业明确数据资产分布情况，为企业数据安全治理提供依据。

数据来源：天融信官网，东莞证券研究所

图 12：2021 年我国数据泄露防护市场份额

2021年我国数据泄露防护市场份额



数据来源：IDC，东莞证券研究所

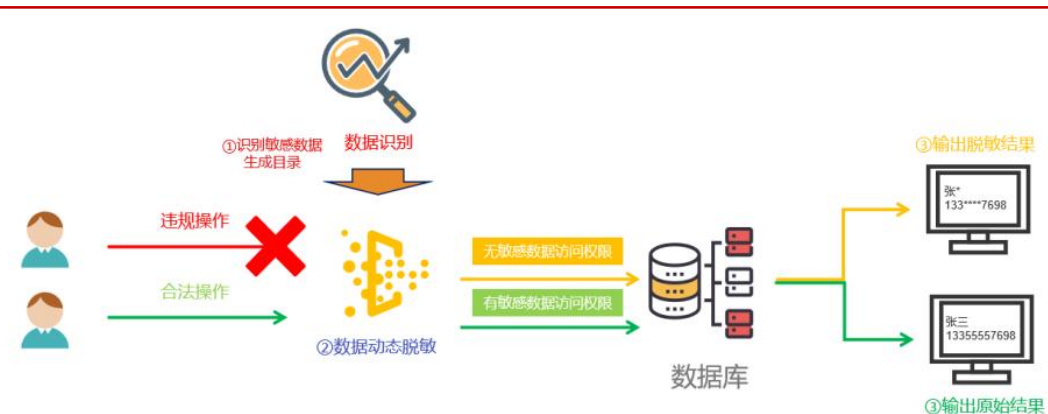
数据脱敏：对敏感数据进行变形。数据脱敏技术是指通过数据变形方式对敏感数据进行处理，既能够降低敏感数据泄露的风险，又能够保持敏感数据原本的特征，仍然能够用于数据的分析和价值的挖掘。根据不同的业务场景，可以选用不同的脱敏策略，常见的规则包括加密、掩码、替换、模糊等。从技术分类来看，主要分为静态数据脱敏和动态数据脱敏两类。其中，静态脱敏是指按照预先制定好的脱敏规则，对敏感数据进行一次脱敏处理，脱敏后的数据能够随意取用和读写；动态脱敏则是在访问敏感数据的同时进行脱敏处理，可针对人员、权限、客户端、主机、时间等不同维度配置脱敏策略。据 Gartner 数据，2017 年使用数据脱敏技术的企业占比约为 15%，预计到 2022 年达到 50%。行业竞争格局方面，仅安华金和一家中国公司入选 Gartner 2020 年发布的数据脱敏领域代表厂商。

图 13：静态数据脱敏示意图



数据来源：中孚信息官网，东莞证券研究所

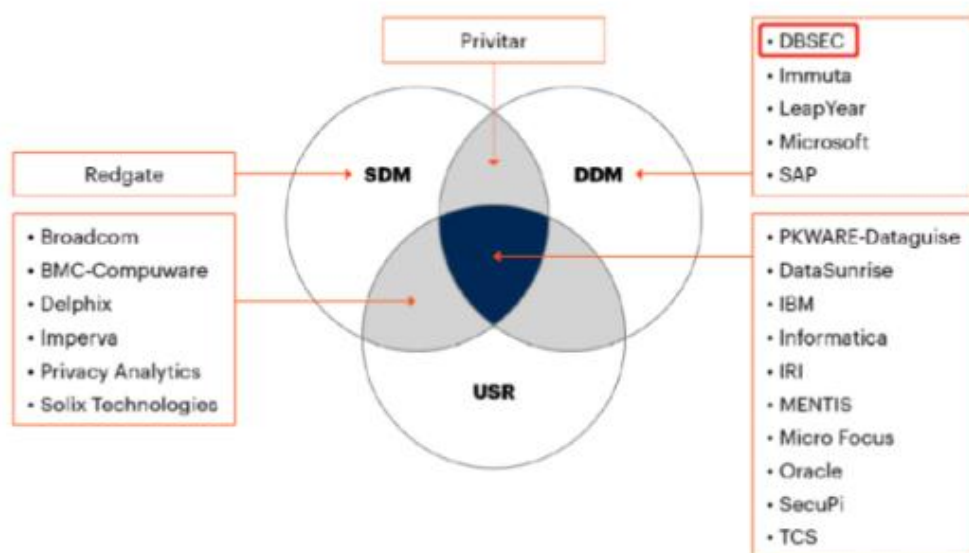
图 14：动态数据脱敏示意图



数据来源：中孚信息官网，东莞证券研究所

图 15：数据脱敏领域代表厂商

DM Technologies Supported By Representative Vendors

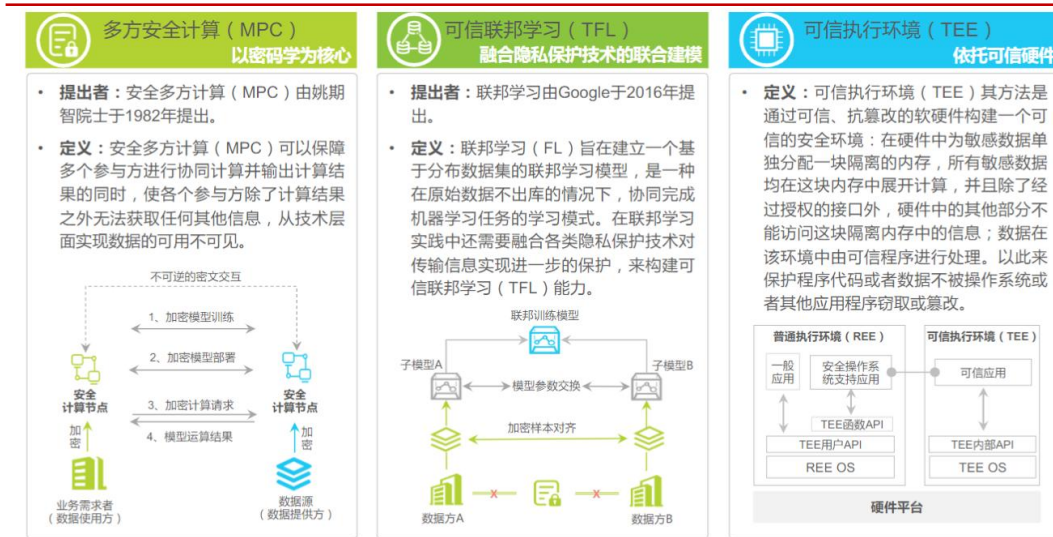


数据来源：Gartner，东莞证券研究所

隐私计算：实现“数据的可用不可见”。隐私计算是指利用密码学、人工智能、数据科学等多个领域的科学体系，在保证数据本身不对外泄露的前提下实现数据分析计算的技术集合，具有“原始数据不出域、数据可用不可见”的特征，能够在充分保护数据和隐私安全的前提下，实现数据价值的转化和释放。从技术分类看，隐私计算主要分为联邦学习、多方安全计算、可信执行环境。其中，联邦学习是指参与方对本地数据进行训练后将更新的参数发往服务器进行聚合，得到总体参数的学习方法，在实现数据聚合的同时也保证了本地数据的隐私。多方安全计算是指多个参与方进行协同计算并输出计算结果的同时，使得各个参与方除了计算结果之外无法获取任何其他信息。可信执行环境是指在本地建立可信执行环境，在该环境下对数据进行处理。其中星环科技推出的隐私计算平台 Sophon P²C，能够支持不同场景的隐私计算需求，包括联邦学习、多方安全计算、

基于差分隐私的数据发布、匿踪查询等，为多方数据安全协作提供完整的平台底座。据艾瑞咨询预测，到 2025 年我国隐私计算市场规模约为 145.1 亿元，2021-2025 年复合增速 133.27%。

图 16：隐私计算三种技术方向



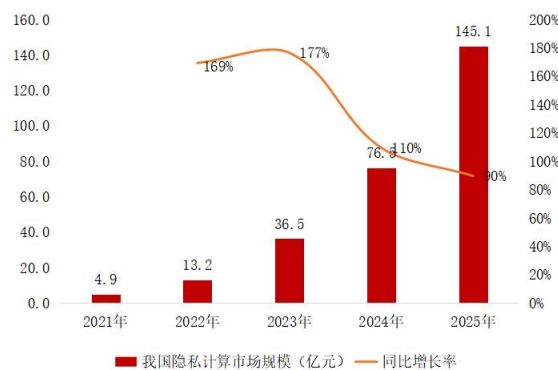
数据来源：艾瑞咨询，东莞证券研究所

图 17：星环科技 Sophon P2C 隐私计算平台



数据来源：星环科技官网，东莞证券研究所

图 18：我国隐私计算市场规模



数据来源：艾瑞咨询，东莞证券研究所

图 19：隐私计算市场竞争格局潜力象限



数据来源：甲子光年，东莞证券研究所

行业领军企业产品矩阵丰富，产品收入高速增长。综合型网络安全厂商由于普遍具有较强的技术背景、资金实力，布局数据安全领域有一定的先发优势，比如深信服、奇安信、启明星辰等相关公司，大部分在隐私计算、数据脱敏、数据泄露防护、数据库审计、防火墙、数据分类分级等领域有所布局，产品矩阵较为丰富，有望形成强者恒强的态势。随着行业需求释放，部分公司数据安全产品的收入也进入到高速增长阶段。其中，2022年，电科网安数据安全业务收入同比大幅增长 135%；奇安信数据安全产品收入同比增长 55%以上；启明星辰数据安全 2.0&3.0 业务同比增长 41%，呈现快速增长的态势。

表 5：布局数据安全领域的相关公司

代码	简称	2022 年营业收入 (亿元)	隐私计算	数据脱敏	数据泄露 防护	数据库审 计	数据库防 火墙	数据分类 分级
300454.SZ	深信服	74.13		√	√	√	√	√
688561.SH	奇安信-U	62.23	√	√	√	√	√	√
002439.SZ	启明星辰	44.37		√	√	√	√	√
002212.SZ	天融信	35.43		√	√	√		√
002268.SZ	电科网安	34.38	√	√	√	√		√
300369.SZ	绿盟科技	27.50	√	√	√	√	√	√
688023.SH	安恒信息	19.82	√	√		√		√
688225.SH	亚信安全	17.25	√	√				√
300768.SZ	迪普科技	8.93		√		√	√	√
688030.SH	山石网科	8.14		√	√	√		
300311.SZ	任子行	6.95		√	√		√	
300659.SZ	中孚信息	6.44		√	√	√	√	
300352.SZ	北信源	5.43		√	√	√		
688031.SH	星环科技-U	3.73	√	√		√		√

数据来源：wind，东莞证券研究所

注：绿盟科技2022年营业收入采用业绩预告的中值，任子行采用2021年营业收入

3. 投资建议

在数据风险敞口扩大、政策合规需求以及数据要素市场加快发展等因素推动下，数据安全赛道长坡厚雪，国家政策明确 2025 年数据安全产业规模超过 1500 亿元，年复合增长率超过 30%。综合型网络安全厂商由于具有较强的技术背景、资金实力，在数据安全领域的布局上有一定先发优势，大部分在隐私计算、数据脱敏、数据泄露防护、数据库审计、防火墙、数据分类分级等领域有所布局，产品矩阵丰富，有望形成强者恒强的态势。建议关注天融信、电科网安、启明星辰、绿盟科技、安恒信息、奇安信-U 等相关标的。

表 6：重点公司盈利预测及投资评级（截至 2023/4/26）

代码	股票简称	股价（元）	EPS（元）			PE（倍）			评级	评级变动
			2022A	2023E	2024E	2022A	2023E	2024E		
002212.SZ	天融信	11.12	0.17	0.40	0.55	64.24	27.65	20.33	买入	首次
002268.SZ	电科网安	31.50	0.36	0.48	0.62	86.89	65.97	51.05	买入	维持
002439.SZ	启明星辰	29.71	0.66	1.01	1.35	45.21	29.29	22.01	买入	维持
300369.SZ	绿盟科技	12.86	0.05	0.64	0.87	257.20	20.19	14.82	买入	维持
688023.SH	安恒信息	200.10	-3.19	1.08	2.99	——	185.64	66.88	买入	维持
688561.SH	奇安信-U	63.35	0.08	0.50	1.03	761.27	126.55	61.28	买入	维持

资料来源：wind，东莞证券研究所

注：绿盟科技尚未披露 2022 年报，以业绩预告披露的中值进行计算

4. 风险提示

政策推进不及预期：若行业政策推进进度或力度不及预期，将影响下游需求释放，进而对相关公司业绩产生不利影响；

行业竞争加剧：若市场竞争加剧，将对相关公司业绩产生不利影响。

东莞证券研究报告评级体系：

公司投资评级	
买入	预计未来 6 个月内，股价表现强于市场指数 15%以上
增持	预计未来 6 个月内，股价表现强于市场指数 5%-15%之间
持有	预计未来 6 个月内，股价表现介于市场指数±5%之间
减持	预计未来 6 个月内，股价表现弱于市场指数 5%以上
无评级	因无法获取必要的资料，或者公司面临无法预见结果的重大不确定性事件，或者其他原因，导致无法给出明确的投资评级；股票不在常规研究覆盖范围之内
行业投资评级	
超配	预计未来 6 个月内，行业指数表现强于市场指数 10%以上
标配	预计未来 6 个月内，行业指数表现介于市场指数±10%之间
低配	预计未来 6 个月内，行业指数表现弱于市场指数 10%以上

说明：本评级体系的“市场指数”，A 股参照标的为沪深 300 指数；新三板参照标的为三板成指。

证券研究报告风险等级及适当性匹配关系	
低风险	宏观经济及政策、财经资讯、国债等方面的研究报告
中低风险	债券、货币市场基金、债券基金等方面的研究报告
中风险	主板股票及基金、可转债等方面的研究报告，市场策略研究报告
中高风险	创业板、科创板、北京证券交易所、新三板（含退市整理期）等板块的股票、基金、可转债等方面的研究报告，港股股票、基金研究报告以及非上市公司的研究报告
高风险	期货、期权等衍生品方面的研究报告

投资者与证券研究报告的适当性匹配关系：“保守型”投资者仅适合使用“低风险”级别的研报，“谨慎型”投资者仅适合使用风险级别不高于“中低风险”的研报，“稳健型”投资者仅适合使用风险级别不高于“中风险”的研报，“积极型”投资者仅适合使用风险级别不高于“中高风险”的研报，“激进型”投资者适合使用我司各类风险级别的研报。

证券分析师承诺：

本人具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，以勤勉的职业态度，独立、客观地在所知情的范围内出具本报告。本报告清晰准确地反映了本人的研究观点，不受本公司相关业务部门、证券发行人、上市公司、基金管理公司、资产管理公司等利益相关者的干涉和影响。本人保证与本报告所指的证券或投资标的无任何利害关系，没有利用发布本报告为自身及其利益相关者谋取不当利益，或者在发布证券研究报告前泄露证券研究报告的内容和观点。

声明：

东莞证券股份有限公司为全国性综合类证券公司，具备证券投资咨询业务资格。

本报告仅供东莞证券股份有限公司（以下简称“本公司”）的客户使用。本公司不会因接收人收到本报告而视其为客户。本报告所载资料及观点均为合规合法来源且被本公司认为可靠，但本公司对这些信息的准确性及完整性不作任何保证。本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，可随时更改。本报告所指的证券或投资标的的价格、价值及投资收入可跌可升。本公司可发出其它与本报告所载资料不一致及有不同结论的报告，亦可因使用不同假设和标准、采用不同观点和分析方法而与本公司其他业务部门或单位所给出的意见不同或者相反。在任何情况下，本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并不构成对任何人的投资建议。投资者需自主作出投资决策并自行承担投资风险，据此报告做出的任何投资决策与本公司和作者无关。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任，任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。本公司及其所属关联机构在法律许可的情况下可能会持有本报告中提及公司所发行的证券头寸并进行交易，还可能为这些公司提供或争取提供投资银行、经纪、资产管理等服务。本报告版权归东莞证券股份有限公司及相关内容提供方所有，未经本公司事先书面许可，任何人不得以任何形式翻版、复制、刊登。如引用、刊发，需注明本报告的机构来源、作者和发布日期，并提示使用本报告的风险，不得对本报告进行有悖原意的引用、删节和修改。未经授权刊载或者转发本证券研究报告的，应当承担相应的法律责任。

东莞证券股份有限公司研究所

广东省东莞市可园南路 1 号金源中心 24 楼

邮政编码：523000

电话：（0769）22115843

网址：www.dgzq.com.cn