计算机

报告日期：2023 年 03 月 11 日

# 数据安全——为数据要素奠基，为数字经济护航

## ——行业深度报告

## 投资要点

- **数据安全是数据要素市场和数字经济建设的重要基础设施之一。在我国数据安全防护和数据开发利用并重的数据安全监管格局下，数据安全市场正从传统以数据承载环境为中心的“系统视角”向以数据全生命周期流转为中心的“业务视角”转变，逐步演进为独立的赛道。在此背景下，我们认为数据安全赛道市场具有广阔成长空间，2025 年市场天花板接近千亿元，2019-2025 年复合增长率可达 67%。**
- **数据安全监管框架：防护与开发并重，未来 2-3 年落地可期**

  数据的敏感性和价值性驱动我国形成了现阶段数据安全防护和数据开发利用并重的数据安全监管思路，监管核心分别在于“止损”和“创利”。

  2020 年 6 月发布的《数据安全法》（草案）预示着我国进入数据安全战略全面落地时期，受到政策实施、试点开展、以及产业指引三方面因素驱动，我们认为数据安全未来 2-3 年落地可期。
- **数据安全市场发展趋势：从“系统视角”到“业务视角”，追求更高回报率**

  传统网络安全市场从“攻防视角”或“系统视角”出发，形成了以防护数据库、网络、服务器等数据使用/存放环境为核心的数据安全产品体系；在现阶段数据监管框架下，数据安全向“业务视角”转变，产品体系围绕数据全生命周期（数据采集、数据存储、数据传输、数据使用、数据共享、数据销毁）防护展开。

  我们认为未来数据安全市场有望沿着三个趋势发展：1）**更高的安全投资回报**，即从事后、外挂式的数据安全防护演变至涵盖事前事中事后、与业务紧耦合式的数据安全防护；2）**更合规的数据开发**，即借助隐私计算等技术手段，在保障数据“可用不可见”的前提下实现数据共享；3）**更轻量化的数据安全改造**，即在补齐存量系统数据安全短板时尽量减少对前端业务的影响，降低改造成本和复杂度。
- **数据安全市场空间：考虑“数据二十条”，中短期 186 亿元，长期近千亿空间**

  若从中国数据总量在全球数据量的占比来看，考虑数据量增加和数据安全渗透率的提升，我们预计 **2025 年数据安全市场潜在空间有望达到 820 亿元，相较于 2019 年复合增长率为 67%**。

  若从“数据二十条”中数据要素基础制度带来的潜在增量市场来看，我们预计中短期（数据要素市场探索建设期，预计 2023-2025）市场增量需求约为 **186 亿元**，远期（数据要素市场成熟落地期，预计 2025-2030）市场增量需求接近**千亿元**。
- **安全厂商布局：各有侧重，自有产线布局和战略投资并行**

  通过对部分安全厂商在数据安全领域布局的梳理，我们发现：1）网安厂商在数据安全领域的布局节奏自 2020 年开始显著加快，且布局侧重点大致分为整体解决方案以及聚焦特定行业两类；2）头部安全厂商大多从自身优势领域切入数据安全赛道进行落地，随后进行扩展布局；3）除基于自身行业和技术优势发布自有产品及解决方案外，头部厂商还通过战略投资创业公司的方式进行布局。
- **数据安全投资框架**

  **需求侧**，建议短期跟踪政策变化，长期关注数据交易带来的商业模式变化；

  **供给侧**，建议关注厂商布局产品结构和产品矩阵协同，产品布局前瞻或行业聚焦深入的公司有望获得更高胜率。
- **风险提示**

  市场空间测算存在主观假设；数据安全市场落地不及预期；市场竞争风险加剧；数据安全政策发生重大变化。

**行业评级：看好(维持)**

**分析师：刘雯蜀**
执业证书号：s1230523020002
liuwenshu03@stocke.com.cn

**相关报告**

1 《2019 年后，国央企数量增加、质量提升》 2023.03.05

2 《人工智能行业点评报告：OpenAI 发布 Whisper API，再添新收费产品》 2023.03.03

3 《人工智能行业深度：潮起潮落，拐点已过，AIGC 有望引领人工智能商业化浪潮》 2023.02.12

# 正文目录

# 图表目录

# 1 数据安全监管框架

## 1.1 两条主线：数据防护与数据利用

我们认为数据的敏感性和价值性驱动我国形成了现阶段**数据安全防护和数据开发利用并重的数据安全监管思路**。

**1）数据防护**

**对于数据安全防护的监管核心在于“止损”**，延用了网络安全领域等保制度的建设思路，旨在防止因为数据泄露、丢失、以及不当操作等对社会秩序、公共利益或者对国家安全造成损害。通过对数据防护相关政策的梳理，我们认为对于数据安全防护的监管渊源可追溯至**2015 年 7 月全国人大发布的《国家安全法》**，其中提到“建设网络与信息安全保障体系”和“实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”。之后在《国家安全法》的基础上，全国人大和网信办陆续发布《网络安全法》、《数据安全法》、《个人信息保护法》、《数据出境安全评估办法》等跟数据安全防护直接相关的法律法规，**各行业亦出台相关指导文件，数据安全防护监管要求逐步细化**。

**2）数据利用**

**对于数据开发利用的监管核心在于“创利”**，旨在打破数据孤岛，实现数据的跨场景流通共享，也是现阶段构建数据要素市场的核心。同样基于对于数据开放共享相关政策文件的梳理，我们认为对于数据开发利用的监管渊源可追溯至**2015 年 9 月国务院发布的《促进大数据发展行动纲要》**，其中提到“加快政府数据开放共享，推动资源整合，提升治理能力”、“稳步推动公共数据资源开放”、“统筹规划大数据基础设施建设”。之后的 2016-2020 年间**政务、医疗、交通、气象、水利、工业等领域主管部门陆续发文，促进行业数据共治共享**。2022 年国务院发布《要素市场化配置综合改革试点总体方案》和《关于构建数据基础制度更好发挥数据要素作用的意见》，将数据流通共享纳入数据要素体系框架。

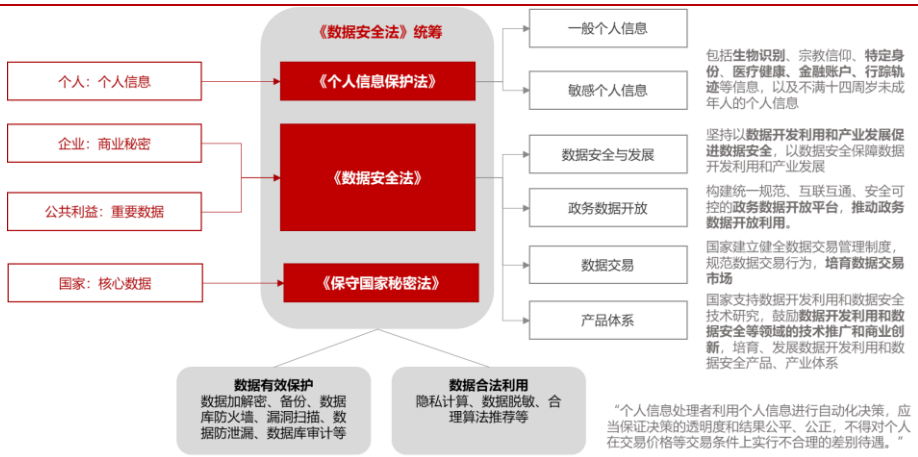
图1：我国数据安全监管两条主线


资料来源：中央人民政府网、国务院新闻办公室网站、中国人大网、浙商证券研究所

我们认为 **2020 年 6 月发布的《数据安全法》（草案）预示着我国进入数据安全战略全面落地时期。一方面，《数据安全法》从更全面的角度统筹了我国各类数据的监管**。根据数据的关联场景，我国数据可被划分为个人信息(与个体相关)、商业秘密（与企业相关）、重要数据（涉及公共利益）以及核心数据（涉及国家秘密）。《数据安全法》整合了个人、企业、

公共利益以及国家四个维度的数据安全监管，**形成以《个人信息保护法》、《数据安全法》、《保守国家秘密法》为核心的三位一体数据安全监管框架。另一方面**，数据安全法在统筹数据安全防护的同时，也花了相当的篇幅对数据利用和开发进行描述和指引，**进一步巩固和奠定了我国数据防护与数据利用并重的监管思路**。

图2： 我国数据安全监管框架




资料来源：中国人大网、浙商证券研究所

表1： 数据安全相关政策文件梳理

| 数据防护 | 数据利用 |
|---|---|
| 法律法规： | 顶层要求： |
| 2015.7 《国家安全法》 | 2015.9 国务院《促进大数据发展行动纲要》 |
| 2016.11 《网络安全法》 | 2017.6 发改委<br>《大数据产业发展规划（2016－2020 年）》 |
| 2020.6 《数据安全法（草案）》<br>2021.6 《数据安全法》（正式稿） | 2020.4 国务院 《关于构建更加完善的要素市场化配置体制机制的意见》 |
| 2020.10 《个人信息保护法（草案）》<br>2021.8 《个人信息保护法》(正式稿） | 2021.12 工信部<br>《“十四五”大数据产业发展规划》 |
| 2019.5 《数据安全管理办法（征求意见稿）》 | 2022.12 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》 |
| 数据出境： | 2022.10 全国人大<br>《国务院关于数字经济发展情况的报告》 |
| 2017.5 网信办<br>《个人信息和重要数据出境安全评估办法（征求意见稿）》 | 2023 国务院 《数字中国建设整体布局规划》 |
| 2019.6 网信办<br>《个人信息出境安全评估办法（征求意见稿）》 | 行业侧： |
| 2022.7 网信办<br>《数据出境安全评估办法》 | **医疗——**<br>2016 国办 《关于促进和规范健康医疗大数据应用发展的指导意见》 |
| 行业侧： | **教育——**<br>2018 教育部 《教育部机关及直属事业单位教育数据管理办法》 |
| **金融——**<br>2020 中国人民银行 《个人金融信息保护技术规范》<br>2020 中国人民银行 《金融数据安全-数据安全分级指南》<br>2021 中国人民银行 《金融数据安全-数据生命周期安全规范》 | **遥感——**<br>2018 国防科工、发改委、财政部 《遥感卫星数据开放共享管理暂行办法》<br>2018 国防科工、发改委、财政部 《国家民用卫星遥感数据管理暂行办法》 |
| **电信互联网——**<br>2019 工信部 《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》<br>2020 工信部 《电信和互联网行业数据安全标准体系建设指南》<br>2021 工信部 《关于开展工业互联网企业网络安全分类分级管理试点工作的通知》<br>2021 工信部 《关于组织开展工业领域数据安全管理试点工作的通知》<br>2022 工信部 《工业和信息化领域数据安全管理办法（试行）》 | **政务——**<br>2016 国务院 《政务信息资源共享管理暂行办法》<br>2018 国务院 《关于加快推进全国一体化在线政务服务平台建设的指导意见》<br>2021 国办《关于建立健全政务数据共享协调机制加快推进数据有序共享的意见》<br>2022 国务院 《关于加强数字政府建设的指导意见》<br>2022 国务院 《全国一体化政务大数据体系建设指南》 |

2023 工信部 《工业领域数据安全管理试点典型案例和成效突出地区名单公示》

**医疗——**

2018 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）》

**交通——**

2019 交通运输部 《推进综合交通运输大数据发展行动纲要（2020—2025 年）》

**教育——**

2020.9 教育部 《关于加强教育系统数据安全的指导意见》

2021.4 教育部等七部门 《关于加强教育系统数据安全工作的通知》

**水利——**

2020 水利部 《水利信息资源共享管理办法（试行）》

**交通——**

2021 工信部、网信办等 《汽车数据安全管理若干规定（试行）》

2022 网信办 《关于做好 2022 年度汽车数据安全管理情况报送工作的通知》

**气象——**

2020 气象局 《气象数据管理办法（试行）》

**能源——**

2022 能源局 《电力行业网络安全管理办法》

**工业——**

2020 工信部 《工业和信息化部关于工业大数据发展的指导意见》

资料来源：中国人民政府网、中国人大网、发改委、工信部、网信办、教育部、国防科工局、国务院新闻办公室、气象局、国家能源局、海南工信厅网站、全国标准信息公共服务平台、国地科技公众号、中国日报、常州大学网站、浙商证券研究所

表2： 地方政府数据条例/数据开放细则梳理

| 地区 | 时间 | 文件 |
|---|---|---|
| 贵州 | 2016.3 | 《贵州省大数据发展应用促进条例》 |
| | 2019.10 | 《贵州省大数据安全保障条例》 |
| | 2020.12 | 《贵州省政府数据共享开放条例》 |
| 天津 | 2019.1 | 《天津市促进大数据发展应用条例》 |
| 海南 | 2019.11 | 《海南省大数据开发应用条例》 |
| 山西 | 2020.7 | 《山西省大数据发展应用促进条例》 |
| | 2023.1 | 《山西省数字经济促进条例》 |
| 吉林 | 2021.1 | 《吉林省促进大数据发展应用条例》 |
| 安徽 | 2021.5 | 《安徽省大数据发展条例》 |
| 广东 | 2021.9 | 《广东省数字经济促进条例》 |
| 深圳 | 2022.1 | 《深圳经济特区数据条例》 |
| 山东 | 2022.1 | 《山东省大数据发展促进条例》 |
| 福建 | 2022.2 | 《福建省大数据发展条例》 |
| 浙江 | 2022.3 | 《浙江省公共数据条例》 |
| 上海 | 2022.1 | 《上海市数据条例》 |
| | 2022.12 | 《上海市公共数据开放实施细则》 |
| 河北 | 2022.7 | 《河北省数字经济促进条例》 |
| 重庆 | 2022.7 | 《重庆市数据条例》 |
| 黑龙江 | 2022.7 | 《黑龙江省促进大数据发展应用条例》 |
| 江苏 | 2022.8 | 《江苏省数字经济促进条例》 |
| 辽宁 | 2022.8 | 《辽宁省大数据发展条例》 |
| 江西 | 2022.11 | 《江西省数据应用条例（草案）》 |
| 北京 | 2023.1 | 《北京市数字经济促进条例》 |
| 四川 | 2023.1 | 《四川省数据条例》 |
| 陕西 | 2023.1 | 《陕西省大数据条例》 |
| 广西 | 2023.1 | 《广西壮族自治区大数据发展条例》 |

资料来源：信息安全国家工程研究中心公众号、上海经信委网站、浙商证券研究所

## 1.2 落地节奏：逐步细化、落地可期

根据上海社会科学院国际问题研究所叶成城博士的研究，**数据是数字时代大国博弈的重要生产要素**，而对于生产资料（可进一步细分为数据、硬件和算法三个方面）的控制和运用就成为新时代重要的权力来源，即**“数字权力”**。从现阶段国内经济发展的角度来看，我们认为数字经济有助于加快产业数字化转型，使得我国以制造业为内核的实体经济实现提质增效发展。因此，近年来我国在数字经济和数字要素领域的政策不断推出，且**逐步深化**。

从数据要素相关政策的发布情况来看，我们认为**政策落地节奏呈现出提出总体意见→规划长期目标→制定建设方案→针对方案落地提出具体意见的发展规律**。具体而言：

- 2019 年十九届四中全会**首次将数据明确纳入生产要素**；
- 2020 年 4 月，中共中央国务院在《关于构建更加完善的要素市场化配置体制机制的意见》中**首次提出培育数据要素市场**；
- 2021 年 12 月国务院在《“十四五”数字经济发展规划》中**明确指出“十四五”时期的发展目标**：“充分发挥数据要素作用，到 2025 年，数据要素市场体系初步建立”；
- 2022 年 1 月（2022 年 12 月成文），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》，其中在数据要素方面，提出“探索建立数据要素流通规则”，从四个方面拆解数据要素市场建立方法，并**对要素市场化配置综合改革试点的时间节点作了进一步细化**：“2022 年上半年，完成试点地区布局、实施方案编制报批工作；到 2023 年，在数据要素市场化配置基础制度建设探索上取得积极进展；到 2025 年，基本完成试点任务，要素市场化配置改革取得标志性成果，为完善全国要素市场制度作出重要示范”；
- 2022 年 4 月，中共中央、国务院提出《关于加快建设全国统一大市场的意见》，要求“加快建立全国统一的市场制度规则”、“强化市场基础制度规则统一”，以求**进一步“打破地方保护和市场分割，打通制约经济循环的关键堵点”**；
- 2022 年 12 月，中共中央、国务院提出《关于构建数据基础制度更好发挥数据要素作用的意见》（“数据二十条”），**为数据要素市场的建设打下底层制度基础，为后续数据在要素市场中的流通进一步提供了可行性**。

图3：数据要素政策落地节奏


资料来源：中国信通院《数据要素白皮书（2022 年）》、浙商证券研究所

参考以上数据要素市场的落地节奏，我们认为**数据安全作为数据要素市场的底层基础设施，未来 2-3 年落地可期**，主要基于以下三个方面考虑：

1）**行业/地方政策实施层面：**2020 年《数据安全法（草案）》发布以来，金融、电信、互联网、工业、互联网、教育、能源等行业陆续出台数据安全相关政策法规，促进数据安全在行业内落地，且自 2021 年《数据安全法》正式实施以来地方政府在数据安全领域的政策布局显著加快；

2）**试点工作层面：一方面**，2020 年网信办中国网络空间安全协会首次开始征集数据安全实践案例并于当年发布“中国网络空间安全协会数据安全实践案例库”和“2020 年数据安全典型实践案例”，此后 2021、2022 年连续发布年度数据安全典型实践案例，入选典型案例的数量呈现增多趋势；**另一方面**，2021 年工信部组织开展工业领域数据安全管理试点工作，在多个行业（原材料工业、装备工业、消费品工业、电子信息制造业、软件和信息技术服务业）、多个领域（数据安全管理、数据安全防护、数据安全评估、数据安全产品、数据安全监测、数据出境安全）开展试点工作，2022 年地方政府积极响应，2023 年工信部发布《工业领域数据安全管理试点典型案例和成效突出地区名单公示》；

3）**产业指引层面：**2023 年 1 月工信部等十六部门联合发布《关于促进数据安全产业发展的指导意见》，为开年众多部委联合发布的重磅文件，并提出“到 2025 年数据安全产业规模超过 1500 亿元，年复合增长率超过 30%”。

# 2 数据安全市场定义

## 2.1 网络安全 vs 数据安全：“器”与“物”

我们认为，从广义上来看，数据安全和网络安全都是信息安全的一部分。在传统网络安全市场的框架下，数据安全从“攻防视角”或“系统视角”出发，即**保障数据产生和存放的系统设备的安全，从而保护在系统设备上的数据**。在这一体系下，形成了以**防护数据库、网络、服务器等数据使用/存放环境为核心的数据安全产品体系**。

图4：“系统视角”下的数据安全产品体系


资料来源：元起资本、浙商证券研究所

而在现阶段数据安全防护和数据开发利用并重的监管体系下，我们看到数据安全正在从传统的“系统视角”（保护存放数据的系统设备）向“业务视角”（围绕数据流动展开全生命周期防护）转变。在“业务视角”体系下，**对于数据的防护作用于数据本身，且伴随数据全生命周期流程，涵盖数据采集、数据存储、数据传输、数据使用、数据共享、数据销毁六个阶段**，同时对涉密、重要、隐私等敏感数据进行靶向监控，实施针对数据的分类分级型安全防护。

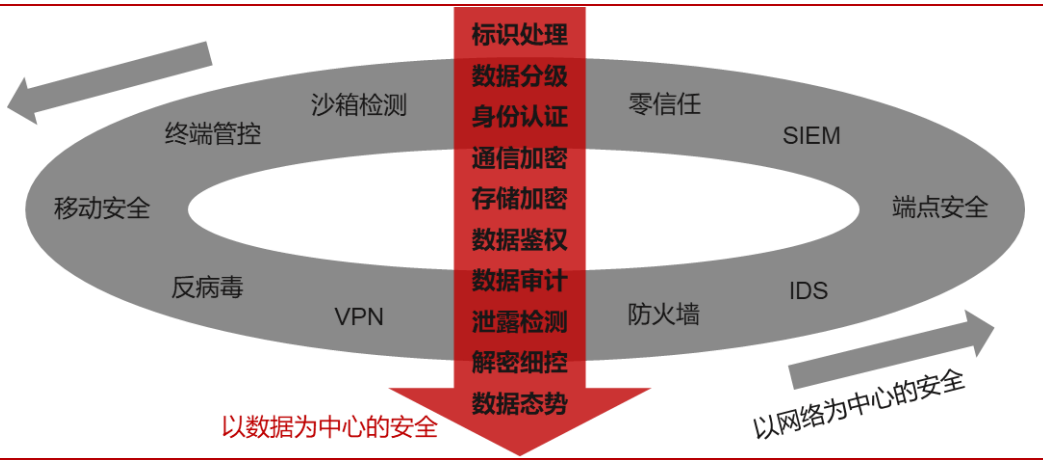
图5： “业务视角”下的数据安全治理体系


资料来源：CNCERT 国家工程研究中心公众号、浙商证券研究所

总结而言，我们认为可将网络比作为“器”，将数据比作置于器中的“物”。**在“系统视角”下**，更加关注“器”的安全，即数据安全通过保护承载数据的系统设备实现，故而**数据安全是传统网络安全市场下的一个分支**；而**在“业务视角”下**，更加关注“物”本身的安全，对于数据本身的安全防护伴随业务场景流转日益丰富，故而**数据安全在当下正在逐步演进为独立的赛道**。

我们认为未来**网络安全和数据安全有望保持相互关联、依赖和演进的关系**。**一方面**，传统“系统视角”下的数据安全演进成为“业务视角”下独立数据安全赛道的重要组成部分；**另一方面**，以网络为中心的安全是保证数据安全的前提和基石，而以数据为中心的安全，着手数据本身，能够有效增强数据防护能力，使得防护更加精准高效。

图6： 网络安全与数据安全的关系




资料来源：关键基础设施安全应急响应中心公众号、浙商证券研究所

## 2.2 数据安全市场需求发展趋势推衍：IRR、合规与轻量化

在数据安全市场围绕“数据全生命周期”向独立赛道发展演进的过程中，我们认为**下游对于数据安全的需求也在发生变化**：**对于新建系统而言**，数据安全的部署和投入节点被前置，事前和事中环节的防护需求增大；**对于潜在的数据共享和数据交易需求**，隐私计算技术的应用场景落地逐步清晰；**对于存量系统而言**，数据安全的改造需求增多，轻量化改造方案有望更加获得下游客户的认可。

### 2.2.1 事前防护：追求更高的安全投资回报率

参考美国国家标准与技术研究所（NIST）提出的企业安全能力框架(IPDRR)，在安全能力维度可对数据安全威胁防护时间轴划分为识别（identity）、防御（protect）、检测（detect）、响应（response）、恢复（recover）、反制（counter）六个环节，覆盖事前(识别、防御)、事中（检测、响应）和事后（恢复、反制）三个重要节点。基于此，我们从事前、事中、事后的维度可对数据安全市场需求进行进一步拆解：

1）**事前需求**：主要目的为“防患于未然”，在安全事件发生前即已经对数据进行了预防式防护措施，贯穿业务流程，包含数据分类分级、数据加密、数据脱敏等；

2）**事中需求**：能够在数据安全受到威胁时即时发现，并给出相应措施以中止正在遭到的安全威胁，包含数据防泄漏、数据风险监测等；

3）**事后需求**：能够在事后对各类操作行为进行回溯分析，从而更新对应防护策略，包含数据库审计等。

我们认为，**越偏向于事前的防护手段，防护效率越高，具有更高的安全投资回报率**。在“系统视角”阶段，由于事后防护大多可通过旁路部署的形式实现，对系统的改造以及操作要求低，容易成为客户的首选项。然而随着业务场景的日益复杂，数据安全防护难度增大，仅通过涂鸦式的“事后防护”难以解决数据安全需求，而引入“事前防护”和“事中防护”可为政企客户省去事后无休止的回溯与补漏成本，提升投资回报率。

图7： IPDRRC 流程示意图


资料来源：SecUN 安全村公众号、浙商证券研究所

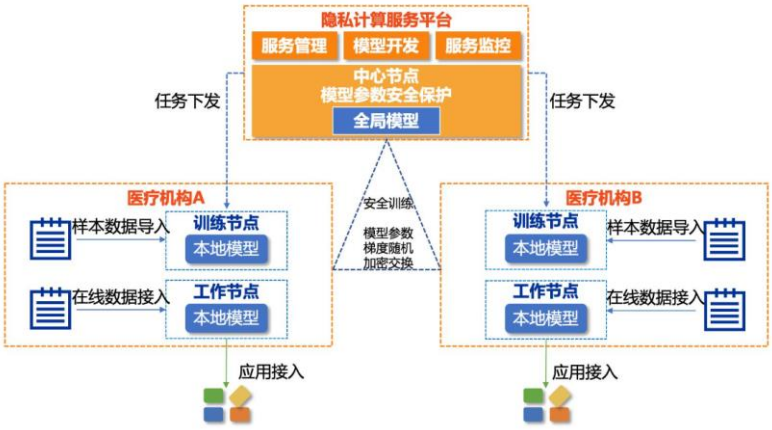
### 2.2.2 隐私计算：追求更合规的数据开发

随着数据安全领域监管日益严格，我们认为**政府和企业在数据安全领域所面临的合规成本增大**。根据《个人信息保护法》，违法处理个人信息，或者处理个人信息未履行法律规定的个人信息保护义务者，**最高罚款额可达上一年度营业额的百分之五，甚至可以责令其停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照**。以“滴滴事件”为例，

由于存在严重违法违规处理个人信息的问题，2022 年滴滴公司被国家信息网络安全审查办公室联合多个部门实施了网络安全审查，最终被处以 80.26 亿元罚款，是**其 2021 年全年营业额的 4.6%**。

在此背景下，如何在保证数据安全的情况下实现数据价值开发演化成为新的市场需求，隐私计算技术从而成为新晋热点话题。隐私计算是包含 AI 大数据、密码学等多领域的技术体系，可以在处理和分析数据的过程中保证数据的不透明、不泄露，**实现数据的“可用不可见”**。自 2016 年我国出现独立的隐私计算商业项目后，隐私计算迅猛发展，在**联合风控、电子政务、智慧医疗及精准营销等领域落地应用**。根据艾瑞咨询测算，2023 年我国隐私计算市场规模有望达到 36.5 亿元，预计**到 2025 年市场规模突破 100 亿**，前景广阔。

图8： 医疗领域隐私计算应用框架




资料来源：中国信通院、浙商证券研究所

### 2.2.3 免改造数据安全：追求更轻量化的数据安全改造

伴随数据安全监管趋严以及合规成本提升，政府和企业对数据安全的重视程度提升明显，补齐数据安全建设短板需求增加。在补齐短板过程中，除对新增信息系统进行安全“三同步”建设，还需对存量应用系统进行安全能力改善。考虑到政府和企业存量数据应用系统数量教大，改造存量系统需花费较多成本和精力，**免改造或轻量化的改造成为数据安全市场新兴需求**。以炼石网络 CASB 业务数据加密平台为例，该平台无需对应用进行任何源代码修改，只需配置级部署，即可实现任意指定字段的数据库存储加密（防范内部 IT 人员、外部黑客等），同时实现结合登录用户身份的数据动态脱敏和审计（防范内部业务人员越权），**实现数据安全防护前置**。

# 3 数据安全市场空间测算

## 3.1 以数据量对标，潜在近千亿赛道

对标全球数据安全市场，我们认为**我国数据安全市场存在较大提升空间**。我们认为**数据安全市场理应受到数据总量规模的驱动**，即数据总量越大，需要防护的信息量越复杂，对数据安全市场的需求空间就越广阔。

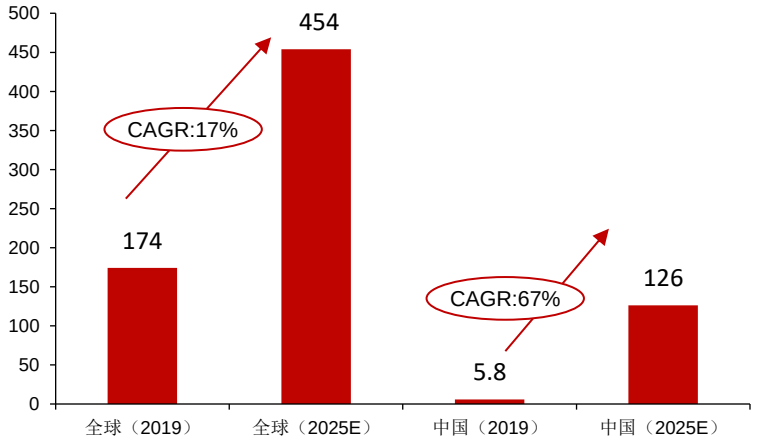
**从数据安全市场规模的角度来看**：根据研究机构 VMR 的统计，2019 年全球数据安全市场空间约为 173.8 亿美元，且预计 2027 年该规模增加至 572.9 亿美元，复合增长率为 17.35%。

而根据中商产业研究院的测算，我国 2019 年数据安全市场规模仅为 38 亿元，**在全球数据安全市场占比仅为 3.4%**。

**从数据量的角度来看：**根据 IDC 的研究，2018 年我国数据量占全球数据量的 23.4%，预计到 2025 年在全球的占比将达到约 28%（远超 2019 年中国数据安全市场在全球 3.4%的占比）。

考虑到中国数据安全市场规模全球占比相较于中国数据总量全球占比仍有较大差距，我们认为中国未来数据安全市场增长潜力较大。我们假设到 2025 年中国数据安全市场规模在全球的占比与数据量占比相匹配（达到 28%），进一步估算得到**中国数据安全市场潜在空间在 2025 年有望达到 126 亿美元（820 亿元人民币），相较于 2019 年复合增长率为 67%**。

图9： 全球 vs 中国数据安全市场规模（单位：亿美元）




资料来源：VMR、中商产业研究网、IDC、浙商证券研究所

## 3.2 从“数据二十条”看数据安全市场增量空间

2022 年 12 月，中共中央、国务院印发了《关于构建数据基础制度更好发挥数据要素作用的意见》（“数据二十条”），提出从数据产权制度、数据要素流通和交易制度、收益分配制度以及数据要素治理制度四个层面建立数据基础制度，且强调**保障数据安全是建立数据基础制度的前提**。

表3： “数据二十条”各项制度对数据安全的要求

| 制度 | 政策要求原文 |
|---|---|
| 数据产权制度 | 在保障安全前提下，推动数据处理者依法依规对原始数据进行开发利用，支持数据处理者依法依规行使数据应用相关权利，促进数据使用价值复用与充分利用，促进数据使用权交换和市场化流通 |
| 数据要素流通和交易制度 | 建立实施数据安全管理认证制度，引导企业通过认证提升数据安全管理水平；<br>制定全国统一的数据交易、安全等标准体系；<br>构建数据安全合规有序跨境流通机制 |
| 数据要素收益分配制度 | 结合数据要素特征，优化分配结构，构建公平、高效、激励与规范相结合的数据价值分配机制 |
| 数据要素治理制度 | 把安全贯穿数据治理全过程，构建政府、企业、社会多方协同的治理模式 |

资料来源：中央人民政府网、浙商证券研究所

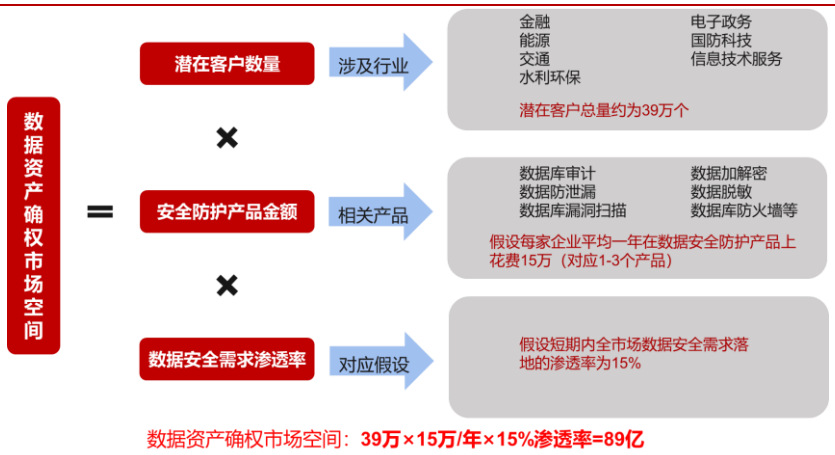
基于以上，我们从**数据资产确权市场**（对应“数据产权制度”）、**数据治理市场**（对应“数据要素治理制度”）以及**数据交易市场**（对应“数据要素流通、交易制度和收益分配制度”）三个需求维度测算数据安全增量市场空间。

**1）数据资产确权市场：以数据安全防护产品为主**

我们对于数据资产确权市场的测算范围涉及**公共数据、企业数据和个人数据**。从行业侧来看，我们认为数据安全的主要需求方涵盖关键信息基础设施领域；从产品侧来看，我们认为主要涉及对于数据资产确权后的防护，以传统数据安全防护产品（包括数据库审计、数据防泄漏、数据库漏洞扫描、数据库防火墙、数据加解密、数据脱敏等）为主。

根据我们测算，**数据资产确权市场的潜在客户总量约为 39 万个**（包括公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业领域的潜在客户数量），假设每家企业平均一年在数据安全防护产品上花费 15 万元（对应 1-3 个产品），同时假设短期内全市场数据安全需求落地的渗透率为 15%，**对应数据资产确权市场的短期市场规模约为 89 亿元**。

图10：数据资产确权市场空间测算




资料来源：国家统计局、财经窝、网易、采招网、浙商证券研究所基于合理假设测算

**2）数据治理市场：以数据安全治理平台产品为主**

通过对数据安全治理领域招投标信息的梳理，我们认为**数据治理市场目前落地以政务和大数据场景为主，包括大数据局、各部委厅局的日常数据安全治理、高校和交通领域的数据中台、城市大脑的数据安全规划设计需求**等。

表4：部分数据安全治理项目招投标信息统计

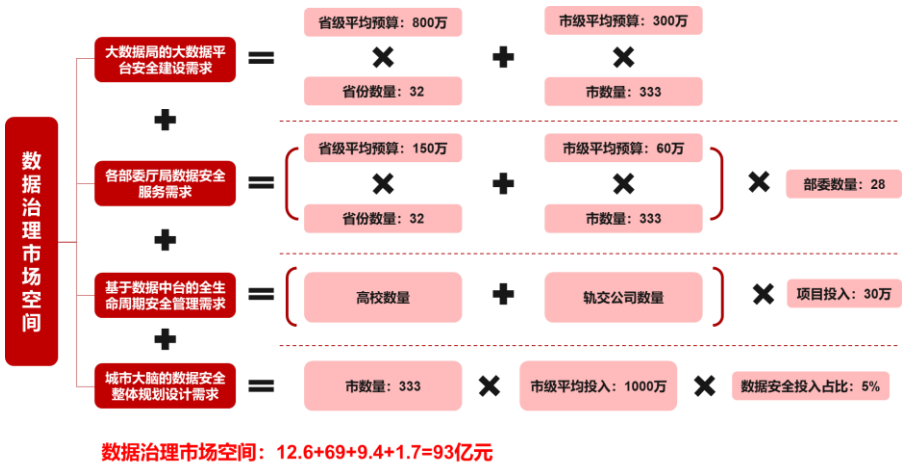
| 项目 | 时间 | 招标单位 | 中标/预算金额（万元） |
|---|---|---|---|
| 安徽大数据交易中心建设项目 | 2021 | 安徽大数据产业发展有限公司 | 890 |
| 上海国资监管网络与数据安全服务 | 2023 | 上海市国有资产监督管理委员会 | 299.6 |
| 龙泉市数据安全服务（2023 年） | 2023 | 龙泉市大数据发展中心 | 100 |
| 国家税务总局黑龙江省税务局数据安全服务、云安全及渗透测试服务项目 | 2022 | 国家税务总局黑龙江省税务局 | 68.3 |
| 普陀区大数据中心公共数据安全保障购买服务项目 | 2022 | 上海市普陀区大数据中心 | 1382 |
| 聊城市一体化大数据平台建设及监理项目 | 2022 | 聊城市大数据局 | 354.9 |
| 山东省烟台市福山区大数据局一体化大数据平台县级节点建设项目 | 2022 | 烟台市福山区大数据局 | 306.5 |
| 扬州大学数据安全管理平台项目 | 2022 | 扬州大学 | 30 |
| 桂城街道城市大脑二期项目 | 2022 | 佛山市南海区桂城街道公共服务办公室 | 700 |
| 郑州数据交易中心数据要素综合服务平台采购项目 | 2022 | 郑州数据交易中心有限公司 | 757.9 |

资料来源：采招网、山东政府采购网、浙商证券研究所

- 大数据局的大数据平台安全建设需求：假设省级大数据平台项目平均预算为 800 万元，市级大数据平台项目平均预算为 300 万元，乘以省市数量，测算得到中短期需求约为 12.6 亿元；
- 各部委厅局数据安全服务需求：假设省级数据安全服务平均预算为 150 万元/年，市级数据安全服务平均预算为 60 万元/年，对应 28 个部委存在构建数据安全服务的需求，测算得到中短期需求为 69 亿元；
- 基于数据中台的数据全生命周期安全管理需求：根据中标项目情况，我们先初步测算高校和交通领域的市场需求，假设全国分别有 3013 所高校和 109 家轨交公司将有构建数据中台的需求，平均每个项目投入为 30 万元（增量投入），测算得到中短期需求为 9.4 亿元；
- 城市大脑的数据安全整体规划设计需求：假设每个市级数据安全规划设计项目平均投入为 1000 万元，其中数据安全投入占比约为 5%，测算得到对应市场需求为 1.7 亿元；

基于以上，我们测算得到**数据治理市场的短期市场规模约为 93 亿元**。

图11：数据治理市场空间测算




资料来源：采招网、教育部网站、RT 轨道交通公众号、安全内参、浙商证券研究所基于合理假设测算

**3）数据交易市场：以数据交易产品为主**

我们认为数据交易市场涉及到**中短期**（数据要素市场探索建设期，预计 2023-2025 年）**数据交易基础设施建设和长期**（数据要素市场成熟落地期，预计 2025-2030 年）**数据交易收益共享的需求**。其中：

- **数据交易基础设施建设：**

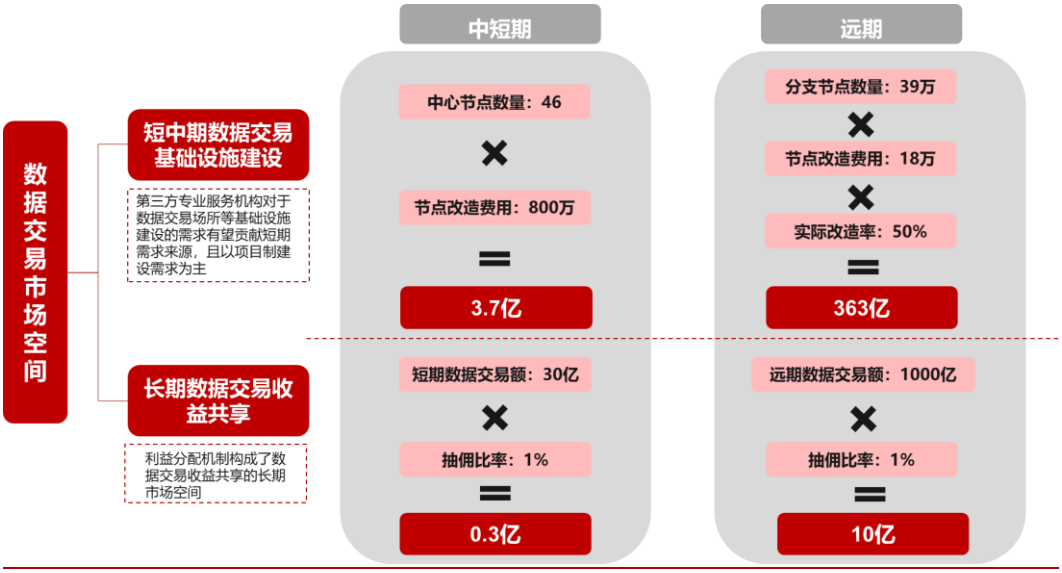
“数据二十条”中提到“构建数据交易场所，有序培育安全审计、数据公证、数据保险、数据托管等第三方专业机构”，我们认为**第三方专业服务机构对于数据交易场所等基础设施建设的需求有望贡献中短期需求来源，且以项目制建设需求为主**。

考虑到现阶段已成立或拟成立的数据交易所（中心）共计 46 家，假设短期以这些数据交易所（中心）为中心建设中心节点，每个节点产生 800 万元改造费用，则**对应 3.7 亿元的市场建设空间**；远期来看，假设以数据交易所（中心）为中心向数据交易参与方延伸，则有望在数据资产确权潜在客户端衍生出 39 万个分支节点，我们假设每个节点产生 18 万元改造费用，且实际改造率为 50%（假设一半的潜在用户有数据交易需求），**对应市场远期需求有望达到 363 亿元**。

- **数据交易收益共享：**

“数据二十条”中提到“第三方专业机构通过分红、提成等多种收益共享方式，平衡兼顾不同环节相关主体之间的利益分配”，我们认为利益分配机制构成了数据交易收益共享的长期市场空间。参考毕马威关于隐私计算的报告，我们假设参与数据交易的抽佣比率为 1%，若中短期和远期数据交易额分别达到 30 亿元和 1000 亿元，则对应市场中短期和远期需求分别为 0.3 亿元和 10 亿元，且随着数据交易规模的扩大具有较高弹性空间。

图12：数据交易市场空间测算




资料来源：采招网、数据交易网公众号、微众银行&毕马威《2021 隐私计算行业研究报告》、同花顺财经、浙商证券研究所基于合理假设测算

表5：数据安全市场规模测算汇总（单位：亿元）

| 细分市场需求 | 中短期市场规模 | 远期市场规模 |
|---|---|---|
| **数据资产确权** | **88.6** | **295.2** |
| *对应渗透率* | *15%* | *50%* |
| **数据治理** | **93.0** | **278.9** |
| 一体化大数据平台 | 12.6 | 考虑到：1）现有数据治理场景的持续建设需求（二期、三期）；2）数据治理场景数量持续增加；3）数字中国和信创建设需求提升下游信息系统建设频率，对应需求频率增加，我们假设**远期市场规模可达到现阶段的三倍** |
| 数据安全服务 | 69.4 | |
| 数据中台数据全生命周期安全管理 | 9.4 | |
| 城市大脑数据安全设计 | 1.7 | |
| **数据交易** | **4.0** | **373.1** |
| 基础设施建设 | 3.7 | 363.1 |
| 收益共享（抽佣比例 1%） | 0.3 | 10.0 |
| *对应数据交易金额（亿元）* | *30* | *1000* |
| **合计** | **185.5** | **947.2** |

资料来源：浙商证券研究所参考图 10-图 12 整理

中短期：数据要素市场探索建设期，预计 2023-2025 年；远期：数据要素市场成熟落地期，预计 2025-2030 年

# 4 网络安全厂商数据安全布局

## 4.1 解决方案和行业侧各有侧重

通过对部分厂商在网络安全领域布局的梳理，我们主要有以下三个发现：

1）**网安厂商在数据安全领域的布局节奏自 2020 年开始显著加快**，我们认为与前文“2020 年 6 月发布的《数据安全法》（草案）预示着我国进入数据安全战略全面落地时期”的观点互为印证。

2）**各网安厂商在数据安全领域布局的侧重点有所不同**，大致可分为两类：**一部分厂商侧重于解决方案领域的布局，提供对数据全生命周期防护**，此类厂商以安恒信息、启明星辰、奇安信、绿盟科技、山石网科等为代表；**另一部分厂商更关注于行业侧布局，产品发布策略更偏向于向某一垂直领域渗透**，此类厂商以深信服、天融信、迪普科技等为代表。其中，深信服主要聚焦于数字政府、教育及交通行业，天融信聚焦于工业互联网领域数据安全，迪普科技主要聚焦于运营商数据安全。

3）**各厂商在数据安全领域的布局以政策指引为导向**。以《数据安全法》为例，我们在前文中提出“数据安全法进一步巩固和奠定了我国数据防护与数据利用并重的监管思路”，而从各网安厂商的布局中亦可看出，2021 年开始各厂商的布局范围由传统数据安全防护产品进一步扩大至数据全生命周期防护体系、隐私计算、数据出境等领域。

## 4.2 基于自身优势产品切入数据安全赛道

我们对 2020-2022 年网信办中国网络空间安全协会发布的年度数据安全典型案例进行统计，观察到**头部安全厂商大多从自身优势领域切入数据安全赛道进行落地，随后进行扩展布局**。比如：

1）**基于行业优势切入**：绿盟科技基于其在运营商行业的积累，在运营商侧数据安全的两项落地案例分别入选 2020 年案例库/2021 年典型案例；数字认证在医疗行业深耕多年，开发的电子病案归档系统入选 2020 年数据安全案例库。

4）**基于产品优势切入**：启明星辰自 2017 年开始布局城市安全运营中心业务，其在城市大数据局落地的数据安全治理案例入选 2021 年典型案例；中孚信息在保密领域拥有一定优势，其商业秘密敏感数据安全实时监测解决方案入选 2021 年典型案例；美亚柏科基于其在取证方面的技术优势，构建了电信网络诈骗综合取证分析平台，入选 2020 年典型案例。

表6：部分安全厂商数据安全布局时间线梳理

| 公司名称 | 产品布局 | | | | | |
|---|---|---|---|---|---|---|
| | 2020.11 | 2021.7 | 2022.10 | | | |
| 深信服 | 针对数字政府数据安全问题发布数据共享安全治理与运营体系模型（DSSG） | 教育行业数据安全治理体系 | 联合交通部发布《综合交通数据安全蓝皮书》 | | | |
| | 2020.9 | 2020 | 2021.7 | 2022.5 | | |
| 安恒信息 | 智慧政务数据安全管控解决方案入选2020年数据安全实践案例库 | 提出"CAPE"数据安全能力框架，发布数据安全管控平台、数据安全岛平台、零信任解决方案、数据安全分级与风险评估系统四项创新产品 | 发布数据安全整体解决方案 | 战略升级，发布数盾数据安全全景图 | | |
| | 2020.9 | 2021.5 | 2021.8 | 2022.1 | 2022.3 | 2022.5 |
| 奇安信 | 发布数据安全开放平台——防水堡 | 升级数据安全开放平台，发布“数据交易沙箱” | 发布“数据安全能力框架”以及“数据安全运行构想图”（数据安全 ConOps） | 发布数据卫士套件（特权卫士、权限卫士、API卫士、隐私卫士和数据安全态势感知运营中心） | 针对政企内部数据安全治理问题推出“奇安信网神应用数据访问控制系统” | 数据跨境卫士 |
| | 2020.7 | 2021.12 | 2022.4 | | | |
| 启明星辰 | 以传统数据安全产品为支撑构建天榕数据安全管控平台 | 启明星辰集团DT（数据时代）总部落地杭州并发布数据安全新版图数据绿洲 | 提炼总结数据安全治理体系 | | | |
| | 2019.4 | 2020.5 | 2020.10 | 2021.6 | 2020.12 | 2022.10 |
| 绿盟科技 | 发布全新数据安全解决方案 | 数据库审计与防护（DAS）全新版本发布 | 发布数据安全运营平台（NSFOCUS ISOP-DS） | 发布工业互联网数据安全监测解决方案与数据安全运营平台ISOP-DS新版本 | 发布数据脱敏系统DMS | 创新推出源代码暴露核查服务和“数安湖”隐私计算平台（联合海光信息） |
| | 2018.11 | 2018.12 | 2021.10 | 2021.11 | 2022.7 | |
| 天融信 | 发布新一代天融信数据库安全网关 | 发布新一代数据脱敏系统 | 发布基于IPDRR的工业互联网数据安全体系 | 三类数据隔离摆渡解决方案 | 发布数据出境自评估解决方案 | |
| | 2017.8 | 2018.3 | 2019 | 2021.11 | 2022 | |
| 山石网科 | 发布数据安全产品线（数据泄露防护系统和数据库审计与防护系统） | 发布数据库审计与防护系统新版本 | 推出静态数据脱敏系统 | 发布全新的数据安全治理体系和数据安全综合治理平台 | 发布数据库加密与访问控制系统和应用（API）数据安全审计系统，布局规划数据泄露防护系统、动态数据脱敏系统、应用数据安全网关、数据库运维安全网关系统 | |
| | 2019.7-2020 | | 2020.11 | | | |
| 迪普科技 | 推出数据安全管控平台 | | 发布《运营商数据安全白皮书》 | | | |

资料来源：各公司官方微信公众号、中国网络空间安全协会公众号、浙商证券研究所

表7：网信办中国网络空间安全协会 2020-2022 数据安全典型案例

| 2020 | | 2021 | | 2022 | |
|---|---|---|---|---|---|
| 公司 | 案例 | 公司 | 案例 | 公司 | 案例 |
| 安恒信息 | 智慧政务数据安全管控解决方案 | 安恒信息 | 基于协同签名的充电桩物联网端到端数据安全加密方案<br>安恒信息 AiLand 数据安全岛可信融合计算平台 | 安恒信息 | AiLand 数据安全岛隐私计算平台<br>安恒信息全链路数盾管理平台 |
| 绿盟科技 | 海南移动运营商云计算数据安全建设实践 | 绿盟科技 | 某省运营商大数据安全一体化运营建设项目 | 绿盟科技 | 工业互联网数据安全项目 |
| 闪捷信息 | 政务大数据平台数据安全防护项目 | 闪捷信息 | 某国家级标准协会-基于人工智能的数据资产安全管理系统建设 | 闪捷信息 | 数字政务一体化数据平台数据安全解决方案<br>兴业银行基于人工智能的数据防泄漏防护系统建设方案 |
| 美亚柏科 | 电信网络诈骗综合取证分析平台 | 奇安信 | 基于数据沙箱技术的数据服务平台在医疗领域的应用 | 奇安信 | 奇安盘古隐私卫士软件 |
| 国舜股份 | （集智）商业银行内控数据安全风险预警系统 | 启明星辰 | 某城市大数据局数据安全治理案例 | 国舜股份 | 安信证券终端数据防泄漏项目实践 |
| 数字认证 | 电子病案归档系统 | 中孚信息 | 商业秘密敏感数据安全实时监测解决方案 | 元支点 | 欺骗防御数据安全解决方案 |
| 北信源 | 工商银行新一代电子文档安全管理系统实践案例 | 蚂蚁集团 | 蚂蚁隐私计算智能服务平台互联网医疗应用解决方案 | 易安联 | EnBox 零信任安全工作空间助力企业终端管控及数据防护 |
| 明朝万达 | 光大银行-办公环境客户数据安全管理项目 | 瑞莱智慧 | 隐私保护机器学习平台 RealSecure | 安华金和 | 安华金和数据安全协同平台 |
| 畅享信息 | 内外网安全共享服务平台 | 同盾科技 | 面向数据安全的可信 AI 知识联邦平台 | 中国移动 | 面向 5G 融合应用的数据安全服务关键技术研发与应用 |
| 爱城市网 | 浪潮数据铁笼（IDS） | | | 视联动力 | 基于新型自主通信协议的数据安全加密技术研究 |
| 腾讯 | 政务大数据平台数据安全体系建设<br>腾讯云数据安全中台 | | | 西安电子科技大学 | 开放互联环境下敏感数据安全融合与共享关键技术及应用 |
| 航天信息 | 基于多层级安全管控体系的税务大数据智能分析平台与应用 | | | 中兴通讯 | 在高效产品开发流程(HPPD)中嵌入数据保护活动 |
| 观安信息 | 面向大数据中心的大数据安全管控平台的建设 | | | 北京市信息安全测评中心 | 北京市政府云数据专区建设项目 |
| 南开大学 | 隐私保护的多平台联合广告推荐业务 | | | 通付盾 | 通付盾能源数据安全共享解决方案 |
| 联通智慧安全 | 中国联通超大规模数据安全服务核心能力平台 | | | 乐信软件 | 乐信数据动态安全运营管理 |
| 智贝科技 | 浙江省财政电子票据安全加固案例 | | | | |
| 数梦工场 | 人口综合库数据安全实践 | | | | |
| 天空卫士 | 汽车之家数据治理防护项目 | | | | |
| 长城网际 | 晋城市政务大数据安全管控平台 | | | | |

资料来源：中国网络空间安全协会公众号、网信办中国网络空间安全协会、浙商证券研究所

## 4.3 战略投资布局垂直赛道初创公司

除基于自身行业和技术优势发布自有产品及解决方案外，我们观察到头部厂商还通过战略投资创业公司的方式进行数据安全领域的布局。我们认为**战略投资有助于帮助头部厂商更高效地在数据安全领域进行布局**：一方面，战略投资可降低头部公司在新赛道的试错成本，在短时间内增强自身数据安全产品能力；另一方面，创业公司通常在某一垂直赛道具有较强的研发实力，公司可将自身研发与创业公司的技术能力进行协同，利用自身渠道和客户资源优势，构造全方位的解决方案交付能力。

表8：部分头部网安厂商在数据安全领域投资布局情况

| 上市公司 | 被投项目 | 项目简介 |
|---|---|---|
| 启明星辰 | 合众数据 | 专注数据安全与大数据领域研发，提供安全数据交换、网络边界接入、大数据分析处理与应用开发等方面的产品及解决方案。 |
| | 数驭未来 | 数据治理、数据交换共享和大数据安全 |
| | 大成天下 | 专注信息防泄密和文档安全领域 |
| 奇安信 | 昂楷科技 | 大数据安全技术产品研发商 |
| | 天际友盟 | 专注 DRP 数字风险防护，致力于提供全生命周期的数字风险防护服务 |
| | 凯馨科技 | 数据安全使用全场景解决方案服务商 |
| | 观安信息 | 信息数据安全整体解决方案服务商 |
| 绿盟科技 | 亿赛通 | 数据安全服务商 |
| | 安华金和 | 数据库安全维护服务提供商 |
| 安恒信息 | 浙江数安 | 针对政府和企业数字化转型提供一站式数据安全保障服务和解决方案 |
| | 高维数据 | 专注于数据安全及隐私保护 |
| 360 | 瀚思科技 | 数据安全技术服务商，以大数据的收集、处理与分析技术为驱动 |
| 深信服 | 科力锐 | IT 业务系统备份及容灾产品提供商 |
| 亚信安全 | 富数科技 | 隐私计算服务商 |

资料来源：企名片网站、浙商证券研究所

# 5 数据安全投资框架

我们认为数据安全领域的投资框架可从需求侧和供给侧两个维度来进行搭建：

**1）需求侧：短期跟踪政策变化，长期关注数据交易带来的商业模式变化**

**短期来看，我们认为数据安全市场需求受到政策推动。一方面**，2023 年 1 月发布的“数据二十条”赋予数据要素市场基础制度框架，且同步明确“数据安全是各项制度得以成立的前提”，故而展望未来，**我们对制度执行以及市场建设相关政策的持续发布保持乐观态度**，且认为数据安全作为数据要素市场的基础设施之一，**市场需求有望伴随各项政策的落地而获得释放。另一方面，行业内以及区域性的政策发布有望推动某一特定下游的数据安全市场需求**。以工信部为例，2021 年工信部率先开展工业互联网企业网络安全分类分级管理试点以及工业领域数据安全管理试点工作，2022 年推出《工业和信息化领域数据安全管理办法（试行）》，落地节奏处于各行业前列。

基于以上，**我们建议跟踪：**

- **短期政策利好带来的数据安全市场需求的加速释放**
- **行业内的数据安全政策发布以及安全厂商在行业侧数据安全的布局**
- **区域性的数据安全政策发布以及安全厂商在各区域内的客户基础**

**长期来看，我们认为数据交易和利润分配制度带来的利益分成模式有望对现阶段数据安全市场的商业模式带来较大变化**。短期的数据安全项目以项目制建设为主，而随着数据交易量的增大，第三方服务机构有望从数据交易流水中抽取一定比例分成，这将使得**传统数据安全产品/解决方案交付制的业务模式向轻量化以及可持续化的方向发展**，且伴随着数据交易量的增加，厂商的规模化优势有望获得加深。

基于以上，**我们建议跟踪**：

- **新设（拟设）数据交易所（中心）建设进度以及数据交易规模**
- **数据交易监管权责划分**
- **数据资产确权以及政务/行业数据开放共享进展**
- **安全厂商参与数据交易所建设情况（含股权和业务平台建设两个维度）**

**2）供给侧：关注厂商布局产品结构，以及产品矩阵协同**

从供给侧来看，我们认为两类公司在数据安全领域或有更大的发展潜力：一方面，**产品布局前瞻的公司具有先发优势**，有望在短期数据要素基础设施建设需求中抢占先机，获得更多落地标杆案例，尤其在隐私计算领域，现阶段拥有落地能力的公司能够参与到数据交易平台的建设，有望在后续数据交易场景招标项目中获得更大的话语权。另一方面，**在某一垂直行业纵深布局的公司能够对下游客户的业务场景建立更加深刻的认知**，从而使得数据安全产品更贴合行业实际需求，**有望在垂直行业获得更高的市占率**。但与此同时**此类公司的发展亦受限于行业本身的数据安全需求天花板**。

# 6 风险提示

1）**市场空间测算存在主观假设**：报告中我们对于数据安全中短期和远期的市场规模进行了测算，在测算过程中引入了较多主观假设，假设设定基于相关公开资料披露数据情况以及我们对于行业的理解，故而测算结果仅作参考，不代表数据安全市场实际市场规模。

2）**数据安全市场落地不及预期**：尽管我们对于未来 2-3 年数据安全市场的落地保持乐观态度，但相关市场仍受到行业内公司的产品研发进度、宏观经济周期波动、疫情反复等其他因素影响，故而市场落地或存在不及预期的风险。

3）**市场竞争风险加剧**：由于数据安全市场有望进入规模化落地阶段，各厂商在数据安全领域的布局节奏加快，或导致市场竞争风险加剧。

4）**数据安全政策发生重大变化**：我们在报告中提到，我们认为数据安全市场需求受到政策推动，故而数据安全政策发生重大变化或导致潜在市场需求受到较大影响，进一步引发数据安全市场落地不及预期的风险。

**股票投资评级说明**

以报告日后的 6 个月内，证券相对于沪深 300 指数的涨跌幅为标准，定义如下：
1.买　入：相对于沪深 300 指数表现 + 20％以上；
2.增　持：相对于沪深 300 指数表现 + 10％～ + 20％；
3.中　性：相对于沪深 300 指数表现 - 10％～ + 10％之间波动；
4.减　持：相对于沪深 300 指数表现 - 10％以下。

**行业的投资评级：**

以报告日后的 6 个月内，行业指数相对于沪深 300 指数的涨跌幅为标准，定义如下：
1.看　好：行业指数相对于沪深 300 指数表现 + 10%以上；
2.中　性：行业指数相对于沪深 300 指数表现 - 10%～ + 10%以上；
3.看　淡：行业指数相对于沪深 300 指数表现 - 10%以下。
我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重。
建议：投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者不应仅仅依靠投资评级来推断结论。

**法律声明及风险提示**



## 浙商证券研究所

上海总部地址：杨高南路 729 号陆家嘴世纪金融广场 1 号楼 25 层
北京地址：北京市东城区朝阳门北大街 8 号富华大厦 E 座 4 层
深圳地址：广东省深圳市福田区广电金融中心 33 层
上海总部邮政编码：200127
上海总部电话：(8621) 80108518
上海总部传真：(8621) 80106010
浙商证券研究所：https://www.stocke.com.cn