证券研究报告—深度报告

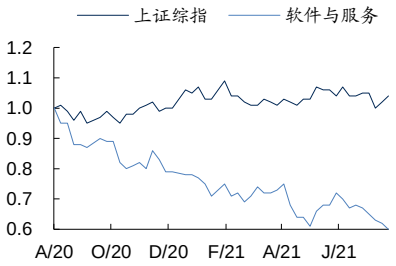
软件与服务

信息安全深度剖析 3

超配
（维持评级）

2021 年 08 月 18 日

一年该行业与上证综指走势比较



相关研究报告:

《海外科技跟踪：海外科技跟踪—谷歌首次自研智能手机处理器，Facebook 战略布局元宇宙》 ——2021-08-10

《国信证券-工控系统行业报告:看 PLC、DCS、SCADA 市场的中国机遇》 ——2021-07-28

《海外科技跟踪：海外科技跟踪—微软发布 Windows365，自动驾驶汽车初创企业 Aurora 拟上市》 ——2021-07-26

《海外科技跟踪：海外科技跟踪—3nm 芯片最快于明年投产，券商平台 Robinhood 上市在即》 ——2021-07-12

《国信证券-地产数字化专题—全球 3D 云设计软件龙头厂商（群核科技）》 ——2021-07-10

证券分析师：熊莉
E-MAIL: xiongli1@guosen.com.cn
证券投资咨询执业资格证书编码：S0980519030002
证券分析师：库宏垚
电话：021-60875168
E-MAIL: kuhongyao@guosen.com.cn
证券投资咨询执业资格证书编码：S0980520010001

独立性声明:

作者保证报告所采用的数据均来自合规渠道，分析逻辑基于本人的职业理解，通过合理判断并得出结论，力求客观、公正，其结论不受其它任何第三方的授意、影响，特此声明

行业专题

数据安全和隐私计算站风口,等保和关保再启增长

- **数据严格治理是大势所趋，政策密集推动数据安全建设**

数据已经成为新生产要素，当前数据泄露事件频出，叠加互联网行业数据监管趋严，数据安全成为建设重点。数据安全强调数据生命周期的保护，需要技术、产品、管理多方协作，建设体量不亚于网络侧安全。当前《数据安全法》即将在 9 月 1 日正式实施，各地数据安全条例逐步落地，政策节奏和推进速度明显加快，数据安全产品有望开启高增长。

- **数据交易探索 3.0 模式，隐私计算开启千亿市场**

上海成立全国数据交易联盟，利用智能合约、区块链、多方安全计算技术探索数据交易 3.0 模式，有望盘活数据交易市场。隐私计算正走向成熟，我国具备技术优势和生态环境，尤其是政府领域数据利用。Gartner 预测市场有望达到 150 亿美金，安恒信息和奇安信已推出隐私计算产品。

- **安全产业增长有望加速，安全投入比持续提升**

安全产业规模 IDC、信通院、工信部口径有所不同。工信部规划 2023 年网络安全产业规模超过 2500 亿，以工信部数据计算，复合增速要达到 18.62%；与 IDC 复合增速 17.9%接近，相比历史增速有所提升。安全投入比计算，IDC 和工信部计算均不超过 3%；从第三方安全预算调研，2021 年各行业增速明显。政府、电信等行业安全投入有望率先达到 10%。

- **等保 2.0 测评带来确定性增量，关保接力为安全预算增长再添筹码**

等保 2.0 的测评报告模板发生了重大修订，扣分制导致企业过关难度剧增。新模板将数据作为独立测评对象，进一步提升数据安全的必要性。同时，新模板带动了态势感知、APT 等新产品采购。《关键信息基础设施安全保护条例》终出台，关保在等保和密评基础上进一步严格，明确了机构设置和经费支持，政企安全预算有望再增长。

- **投资建议：看好网络安全板块，关注数据安全卡位厂商**

数据安全带来新成长赛道，政策推进为行业带来预算增长。网络安全板块集体股权激励，验证当前产业发展信心。重点关注安恒信息、奇安信、绿盟科技、启明星辰、迪普科技、深信服等。

- **风险提示：**政策推进不及预期；疫情反复影响 IT 支出；行业竞争加剧。

重点公司盈利预测及投资评级

公司代码	公司名称	投资评级	昨收盘（元）	总市值（亿元）	EPS 2021E	EPS 2022E	PE 2021E	PE 2022E
688023	安恒信息	买入	299.00	221	2.58	3.76	115.89	79.52
688561	奇安信-U	买入	93.65	636	-0.13	0.48	-	195.10
300369	绿盟科技	买入	19.90	159	0.52	0.69	38.27	28.84
002439	启明星辰	买入	30.40	284	1.13	1.42	26.90	21.41
300768	迪普科技	买入	39.50	158	0.90	1.17	43.89	33.76
300454	深信服	买入	260.00	1076	2.49	3.45	104.42	75.36

资料来源：Wind、国信证券经济研究所预测

投资摘要

关键结论与投资建议

数据安全是产业发展新方向，等保 2.0 和关保等政策带来确定性增量，网络安全行业均大为受益。互联网监管趋严，叠加《数据安全法》推出，数据安全成为新建设重点。隐私计算逐步成熟，成为数据安全的新衍生，千亿市场为安全厂商打开新成长空间。等保 2.0 测评变化，以及关保在等保基础上更为严格的要求，为行业预算带来确定性增长。网络安全板块集体股权激励，验证当前产业发展信心。重点关注关键技术和市场卡位厂商：安恒信息、奇安信、绿盟科技、启明星辰、迪普科技、深信服等

核心假设或逻辑

第一，数据被定义为新“生产要素”，《数据安全》法即将在 9 月 1 日正式实施，各地迅速出台数据安全条例，数据安全是下一轮安全建设重点。

第二，隐私计算技术不断发展成熟，成为数据安全发展的新方向，我国具备技术优势和生态环境，千亿市场打开安全行业新发展空间。

第三，等保 2.0 测评模板变化巨大，导致原来普遍 80、90 分过关的企业现在可能只有 60 多分，甚至更低。关保针对关键信息基础设施，是在等保 2.0 基础上的进一步要求。为了确保等保和关保测评通过，安全预算投入必然会增加。

与市场预期不同之处

第一，市场认为互联网监管催化的数据安全仅是情绪炒作。滴滴事件后，安全板块情绪高涨明显。我们认为，数据安全事件频出，其关乎每个个体，政策不断推出，相关技术和产品持续在验证，是推动安全产业下一轮增长的关键。

第二，市场认为数据交易难有成功模式。我们认为，早期数据交易所不温不火是技术发展的必然探索。隐私计算为数据安全提供了新的模式，我国在该领域具备技术优势和生态环境，隐私计算有望成为安全厂商新一轮成长动力。

第三，市场低估了等保 2.0 测评变化和关保给行业带来的确定性增量。等保 2.0 新模板将数据作为独立测评对象，进一步提升数据安全的必要性。同时，新模板带动了态势感知、APT 等新产品采购。关保虽然从 2017 年就已经提出，但正式文件已发生较大变化，明确了机构设置和经费支持。关保是在等保 2.0 基础上更为严格的要求，因此各行业安全预算均有望增长。

股价变化的催化因素

第一，网络安全政策持续推出和发酵，资金支持得以保障。等保 2.0 测评模板变化、数据安全法推进、关保在等保 2.0 上更进一步，为行业带来切实增量。

第二，数据安全社会影响不断扩大，隐私计算产品及商业模式持续落地。信息安全事件直接催化板块热情，数据安全建设成为各类机构的新重点。隐私计算成功落地，有望为安全行业打开新市场空间。

第三，网络安全行业公司业绩持续高增长。四季度有望看到新政策带来的订单增长，进一步增强明年向好的确定性。各厂商数据安全、云安全等各类新产品有望逐步放量，带动公司业绩和估值提升。

核心假设或逻辑的主要风险

第一，各类信息安全政策实施力度不及预期。

第二，疫情反复和经济下行环境中，IT 支出下降。

第三，行业竞争加剧，全行业盈利能力下滑。

内容目录

图表目录

数据严格治理大势所趋，数据安全成为建设重点

如何理解网络安全和数据安全

网络安全侧重流量管控，数据安全重点在数据本身。网络和数据安全并非相互独立，在建设过程中必然是相互融合的。相较而言，网络安全更常被提及，以防火墙为代表的各类产品也更普及。网络安全核心是保护 IT 系统的软件、硬件等资产，主要工作网络模型中的网络层和应用层，通过是对网络流量的管控和分析，实现对网络攻击的阻断和病毒过滤等。数据安全则重点在于保护数据本身，将数据视为一项与“软硬件”相似的新资产，主要工作是对数据库的保护、审计、访问控制，以及对数据的加密、脱敏、防泄露、安全共享、多方安全计算等。数据安全涉及密码、网络、隐私计算等多种新老技术，建设过程中同样离不开网络安全的保护，可以说网络安全是第一道防线。在此基础上，全局视角的态势感知平台，结合网络和数据安全各类防护，实现完整的安全解决方案。

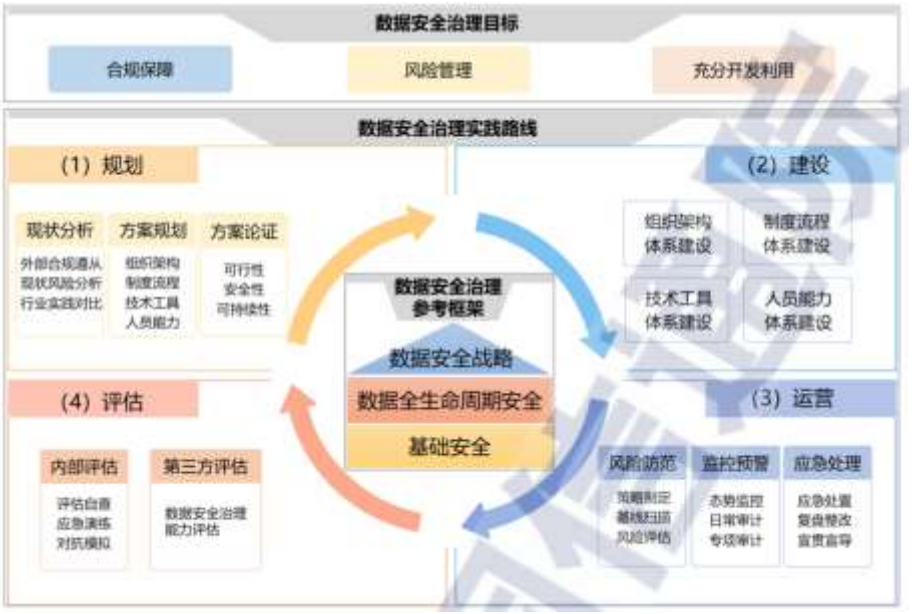
与现实映射，网络与数据安全相辅相成。将数字世界与现实中的家庭进行映射，家庭中的防盗门、室内监控扮演了网络安全的角色，即将陌生人全部隔离在外，只允许业主和邀请客人进出；对恶意闯入者进行驱逐；对内部人员进行监控等。网络安全主要作用于流量，如同对人的管控。数据安全则类似于家庭里保险柜，将最有价值的金钱（如同数据）进行严格保护，如对保险柜加密、每个成员收入和支出的审计、不同成员的使用权限、金钱合作方银行账户的管理等，即数据安全需要对数据全生命周期的保护。整体上，小区监控室扮演了态势感知的角色，对每个家庭人员和资产进行全面管控（如企业对各个部门及 IT 系统的安全管控），网络和数据安全实现一体化建设。

图 1：网络安全和数据安全的现实映射

资料来源：《计算机网络》，国信证券经济研究所整理

数据安全治理需要技术、产品、管理、运营等多方面共同协作。随着数据价值日益凸显，数据安全治理不再只是简单一个加密和备份这么简单。围绕数据全生命周期，数据安全涉及组织内多部门协作、流程制定、体系化技术、专业人才运维等一系列工作。数据安全治理的目标是在合规保障及风险管理的前提下，实现数据的开发利用，保证数据和业务共同安全发展。整个数据安全治理路线分为规划、建设、运营、评估，基础安全和数据全生命周期安全都要覆盖。

图 2：数据安全治理总体视图



资料来源：《数据安全治理实践指南 1.0》，国信证券经济研究所整理

数据安全不容忽视，严格治理成为大势所趋

数据泄露事件频出，安全成本逐年上升。全球各公司和组织数据泄露事件屡见不鲜，深刻威胁每个个体，已经成为全球政府的重点问题。根据 IBM 一项安全研究报告，2021 年企业平均每起数据泄露事件成本为 424 万美元，是自 2004 年以来最高值。尤其在疫情发生后，远程办公、在线运营等新 IT 架构弱化了曾经的安全防护，导致安全成本平均提升了 10%左右。如果未对远程办公等及时跟进安全建设，数据泄露发生更为容易，直接阻碍企业运营和发展。

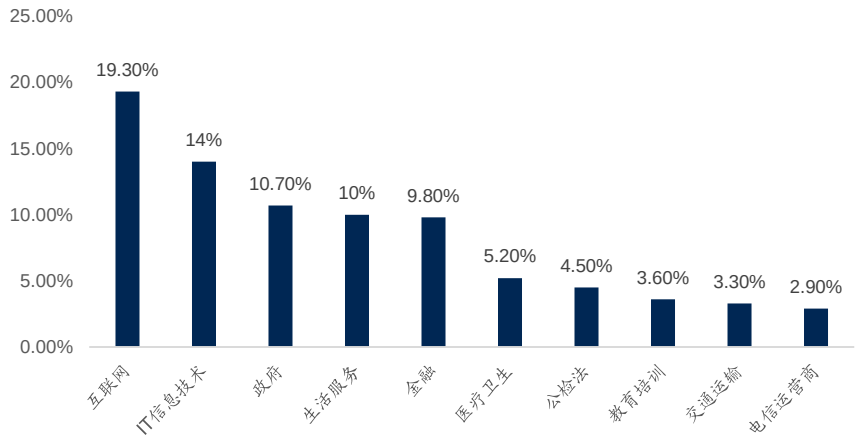
表 1：2021 年上半年数据泄露若干事件

时间	事件
2021 年 1 月	巴西的一个数据库 30TB 数据被破坏，泄露的数据包含有 1.04 亿辆汽车和约 4000 万家公司的详细信息，受影响的人员数量可能有 2.2 亿
2021 年 1 月	日产北美公司一台 Bitbucket Git 服务器的信息在 Telegram 频道和黑客论坛上传播，近 20GB 源代码遭到泄露
2021 年 3 月	印度 800 万核酸检测结果泄露，含有姓名、年龄、婚姻状况、检测时间、居住地址等敏感个人信息
2021 年 3 月	美国保险巨头 CNA 公司的 IT 系统被勒索软件锁定，攻击者还窃取了数据，公司支付了 4000 万美元勒索赎金
2021 年 5 月	应用 Omiai 最近遭黑客攻击，约 170 多万用户个人数据遭泄露

资料来源：腾讯新闻，国信证券经济研究所整理

数据泄露问题普遍，互联网 IT、政府、金融等是重灾区。根据奇安信发布的《中国政企机构数据安全风险研究报告》，从 2019 年 1 月至 2020 年 8 月，全球政企机构重大数据安全事件中，数据泄露事件高达 406 起，占总体数据安全事件的 96.7%。从行业分布来看，信息化程度最高的的互联网和 IT 产业，以及与国计民生深度融合的政府、生活服务、金融等行业数据安全影响最严重。这些行业掌握了全民级数据，数据安全治理不容忽视。

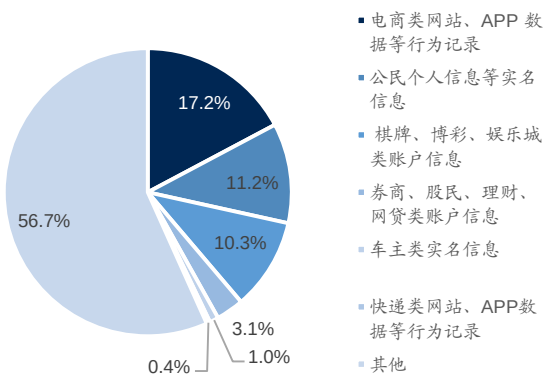
图 3：全球政企机构重大数据安全事件行业分布



资料来源：奇安信，国信证券经济研究所整理

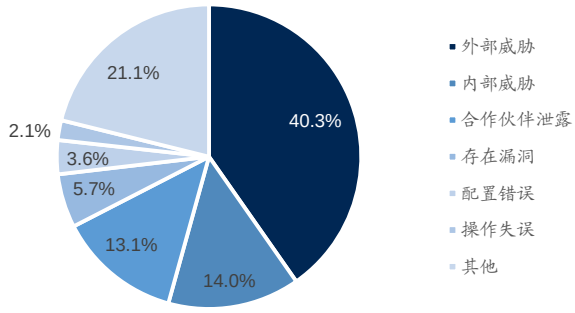
个人信息和记录黑色交易成灾，数据内外部威胁是主要原因。根据报告，奇安信公司从某暗网交易平台上，抽样收录了 2019 年 5 月-2020 年 2 月以来发布的 6357 则交易信息约 11.7 亿条可交易数据。从统计中可以看出，暗网上数据交易量最大的是电商类网站、APP 数据行为记录、公民实名信息、棋牌博彩、券商理财等信息。个人数据的黑色交易泛滥成灾，骚扰电话、大数据杀熟、垃圾邮件和短信等损害了每个人的利益。根据调查，超过 40%的数据安全事件由外部攻击导致，14%是由于内部人员的违规操作造成，13%是由于合作伙伴，如供应商和服务商泄露。因此数据安全内部和外部均需要治理，当前政策和法律不断趋严。另一方面，数据需要交易共享才能发挥价值，但黑色交易理应严厉打击，以隐私计算等为代表的新兴技术，将为数据安全交易和利用带来曙光。

图 4：2020 年暗网交易数据规模分布



资料来源：奇安信，国信证券经济研究所整理

图 5：2020 年全球数据安全事件主要原因



资料来源：奇安信，国信证券经济研究所整理

数据安全产品和技术众多，市场空间广阔

数据安全强调数据生命周期的保护。对数据安全的强调，进一步推动信息化建设中内生安全的融入，即进入数据全生命周期的各个环节，不再只是后 IT 时期的修修补补。数据生命周期涉及采集、传输、存储、处理、交换、销毁。当前的网络安全建设，主要仍基于传输和存储两个环节，像“交换”之类敏感环节，并未成熟，才导致数据泄露和数据黑市的存在。因此传统及新兴数据安全技术有望得到迅速应用和发展，如数据加密（叠加当前国密改造）、脱敏；数据监测

（态感、UEBA）、数据审计（堡垒、水印）；隐私计算；数据容灾等，当前也能看到持续的产品化及方案落地。

图 6：数据生存周期安全

资料来源：《绿盟数据安全白皮书 2.0》，国信证券经济研究所整理

基础数据安全是体系重要支撑，功能点众多。基础安全能力是数据全生命周期安全能力建设的基本支撑，是整个安全体系的通用要求，实现各类资源的有效整合。基础安全主要包括数据分类分级、合规管理、合作方管理、监控审计、鉴别与访问、风险和需求分析、安全事件应急等 7 大内容，覆盖了 11 大功能项。基础数据安全主要有数据库审计、日志审计、态势感知等，也是数据全生命周期安全建设的重要基石。

表 2：基础数据安全要求

基础数据安全要点	主要内容
数据分类分级技术	敏感数据识别，分类分级规则定义、管理、打标等
分类分级规则定义及管理	数据资产的识别、录入、管理，以及分类分级标识
工单审批管理平台	覆盖数据全生命周期和业务场景的各类工单的申请、审批、流转跟踪等；根据申请内容，与其他平台形成联动管理机制等
合规管理平台	法律、合规等文件管理，合规风险库管理，合规评审计划、记录、报告、整改的管理
合作方管理平台	合作方录入、删除、更新等；合作商机评审管理；合作方安全评估计划、记录、报告等管理
监控审计平台	覆盖全部业务场景、系统、平台等的数据流动及人员操作监控及审计；监控点及监控阈值管理；风险告警策略的配置管理等
日志管理平台	数据处理日志收集、记录等；全部数据访问者的操作日志收集、记录；日志监控与分析
账号及权限管理平台	账号申请、分配、回收等的管理；权限申请、分配、变更、回收等的管理；涉敏账号及权限管理
需求管理平台	业务数据安全需求的申请、分析及安全方案管理
风险管理平台	数据安全风险的登记、评估、更新；防控措施记录及更新
数据安全事件管理平台	数据安全事件的登记、应急处置记录；宣贯宣导管理等

资料来源：《数据安全治理实践指南 1.0》，国信证券经济研究所整理

数据安全的系统治理需要完整方案，单点产品和安全平台均不可或缺。参考中国联通数据治理实践，公司从管理、技术、运营三个方面构建了整体数据安全体系。从数据采集、传输、存储、使用、交互等全生命周期环节出发，技术点覆盖事前、事中、事后的数据状态，主要有 7 大系统：

（1）数据资产地图，动态管理数据资产信息，形成统一管控视图；

（2）数据脱敏系统，对数据分类分级，敏感数据加密和脱敏；

（3）统一账号认证授权审计系统，实现用户的统一认证、授权，对 IT 资产集中管理；

（4）数据安全监测与审计系统，基于零信任模型，分析用户操作行为，保证数

据行为可控、可审计;

（5）云桌面系统，保证数据在云桌面内可读可控防泄漏;

（6）数据追踪溯源系统，基于水印技术，对内容标识，能追踪泄露者;

（7)数据安全网关系统,对外数据输出唯一出口,确保数据输出内容安全合规。

结合产品和平台，联通数据安全治理取得了良好的效果。公司完成了多个高危漏洞的整改，保障大数据平台超过 100P 的数据存储以及每天新增超过 200T 压缩数据量的安全。因此，数据安全建设不是一蹴而就，**需要持续的产品和平台迭代建设，建设体量不亚于网络安全侧**。

图 7：中国联通数据安全体系总体框架

资料来源:《数据安全治理实践指南 1.0》，国信证券经济研究所整理

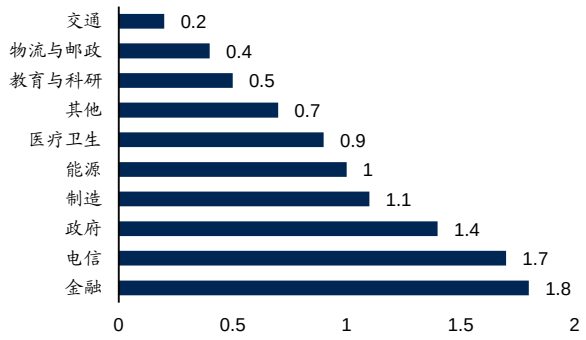
传统数据安全产品较多，有望迎来加速发展期。传统主要有数据脱敏，数据库审计、数据防泄漏 DLP 等方向。数据脱敏主要是通过一些算法，如变形、转换等内置规则降低数据敏感度。数据库审计，主要是记录、分析和汇报用户访问数据库行为，帮助用户事后生成合规报告、事故追根溯源。数据防泄漏 DLP 主要审计一切外发的数据，做到事中管控，事后溯源取证（存储、使用、传输三种场景）。除此之外，数据安全还包括终端加密、文档加密、数据资产测绘、数据库防火墙等产品。虽然每一款产品当前市场并不大，但是随着《数据安全法》等逐步普及，数据安全行业有望迎来高增长，根据中国信通院预测，2023 年中国数据安全市场有望达到 97.5 亿元。

DLP 领域，绿盟科技子公司亿赛通占据优势。根据赛迪 2020 报告数据，DLP 市场 2019 年达到 9.7 亿元，虽然体量较小，行业将保持 20%左右的增长，预计 2022 年市场达到 16.6 亿元。在 DLP 下游中，金融、电信、政府占比仍是最高的三个。绿盟科技在 2014 年 9 月以 4.98 亿收购专业数据安全厂商亿赛通 100%股权，亿赛通是 DLP 市场龙头，2019 年以 17.1%的份额位居行业第一。

图 8：2019 年中国数据泄露防护（DLP）市场规模

资料来源：赛迪顾问 2020.05，国信证券经济研究所整理

图 9：2019 年中国 DLP 产品行业结构



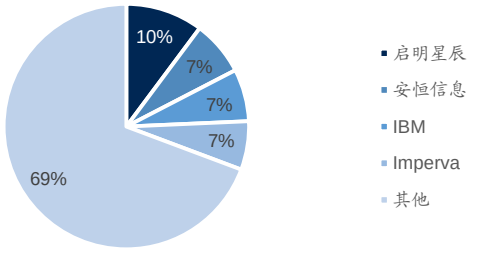
资料来源：赛迪顾问 2020.05，国信证券经济研究所整理

数据库审计中，启明星辰和安恒信息保持领先。2017 年，我国数据库安全审计与防护市场保持了 16.9%的增长率，市场规模达到 10.4 亿元；预计 2020 年将达到 16.7 亿元，复合增长率为 17.1%。该领域中，启明星辰以 10.2%的份额位居第一；安恒信息市场份额 7.2%，仅次于启明星辰，领先于国外厂商 IBM 和 Imperva。

图 10：国内数据库安全市场规模（亿元）

资料来源：赛迪顾问 2018.10，国信证券经济研究所整理

图 11：国内数据库安全市场份额



资料来源：赛迪顾问 2018.10，国信证券经济研究所整理

互联网监管发酵，网络和数据安全政策密集出台

滴滴事件持续发酵，互联网安全审查程度空前

“滴滴”引发网络安全审查。2021 年 7 月 2 日晚，国家网信办官网发布公告称，为防范国家数据安全风险，维护国家安全，按照《网络安全审查办法》，对“滴滴出行”实施网络安全审查，首先暂停了“滴滴出行”新用户注册。7 月 4 日晚，经检测核实，“滴滴出行”App 存在严重违法违规收集使用个人信息问题。目前各应用商店已下架“滴滴出行”App。7 月 9 日晚，同样因为“严重违法违规收集使用个人信息问题”，滴滴旗下另外 25 款 APP 也被国家网信办要求下架。在“滴滴事件”期间，美股上市不久的 BOSS 直聘、满帮集团也同样被启动网络安全审查；而计划赴美上市的 Keep、喜马拉雅、零氪科技也纷纷暂停 IPO。

表 3：滴滴事件梳理

时间	事项	涉及公司
7 月 2 日	网信办宣布对“滴滴出行”App 实施网络安全审查，称“为配合网络安全审查工作，防范风险扩大，审查期间‘滴滴出行’停止新用户注册”。	滴滴
7 月 4 日	网信办要求各应用商店下架“滴滴出行”App，通报，称“滴滴出行”App“存在严重违法违规收集使用个人信息问题”。	滴滴
7 月 5 日	网信办宣布对在线招聘公司 BOSS 直聘、两家货运调度平台运满满和货车帮实施审查，审查期间以上平台停止新用户注册。注：运满满和货车帮于 2017 年合并为满帮集团（Full Truck Alliance）。	BOSS 直聘、运满满、货车帮
7 月 7 日	微信、支付宝无法搜索“滴滴出行”小程序，“滴滴出行”也从微信支付出行服务栏内消失。	滴滴、微信、支付宝
7 月 8 日	健身软件 Keep、播客平台喜马拉雅、阿里系医疗数据公司零氪科技（LinkDoc Technology）等取消赴美 IPO 计划	Keep、喜马拉雅、零氪科技
7 月 9 日	网信办要求各网站、平台下架“滴滴企业版”等 25 款 App，称 25 款 App 存在“严重违法违规”，各网站、平台均不得为这 25 款 App 提供访问与下载服务。	滴滴
7 月 16 日	国家网信办会同公安部、国家安全部、自然资源部、交通运输部、税务总局、市场监管总局等部门联合进驻滴滴，开展网络安全审查	滴滴
7 月 30 日	美国证监会要求赴美上市的中企提交风险信息，同时出示得到我国有关部门“许可”上市的文件。	所有赴美上市公司
7 月 30 日	工信部召开贯彻落实《数据安全法》座谈会，阿里、腾讯、美团、奇安信、小米等 12 家企业参会	各互联网公司

资料来源：新浪财经，国信证券经济研究所整理

移动 APP 安全审查近年来已经持续加强。2019 年关于 app 治理方面的政策不断出台，2021 年开始进入密集整治期。根据工业和信息化部数据，截至 6 月 21 日，APP 侵害用户权益专项整治行动共检查 117 万款 APP，对 4002 款违规 APP 提出了整改要求，公开通报 1248 款整改不到位的 APP，组织下架 329 款拒不整改的 APP。包括滴滴在内，多数被整改的知名 APP 应用，问题均是出在违规收集个人信息上。因此，各类《网络安全审查办法》、《数据安全法》、《个人信息保护法》等政策陆续落地，不断推动全社会信息安全建设。

表 4：APP 治理事件梳理

时间	事项
2019 年 1 月 25 日	中央网信办、工信部、公安部、市场监管总局四部门联合发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》(以下简称《公告》)，决定自 2019 年 1 月至 12 月，在全国范围组织开展 App 违法违规收集使用个人信息专项治理
2019 年 5 月 27 日	百款常用 App 申请收集使用个人信息权限情况公布
2019 年 12 月 30 日	中央网信办、工信部、公安部、市场监管总局四部门联合印发《App 违法违规收集使用个人信息行为认定方法》，《方法》提出，征得用户同意前就开始收集个人信息或打开可收集个人信息的权限、实际收集的个人信息或打开的可收集个人信息权限超出用户授权范围等行为可被认定为“未经用户同意收集使用个人信息”。
2021 年 3 月 22 日	国家互联网信息办公室等四部门联合印发《常见类型移动互联网应用程序必要个人信息范围规定》，
2021 年 5 月 1 日	关于输入法等 33 款 App 违法违规收集使用个人信息情况的通报
2021 年 5 月 15 日	关于腾讯手机管家等 84 款 App 违法违规收集使用个人信息情况的通报
2021 年 5 月 21 日	关于抖音等 105 款 App 违法违规收集使用个人信息情况的通报
2021 年 6 月 11 日	国家网信办通报 Keep 等 129 款 App 违法违规收集使用个人信息的情况

资料来源：新浪新闻，国信证券经济研究所整理

滴滴直接导致《网络安全审查办法》修改升级。《网络安全审查办法》由国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局等 12 个部门联合发布，已于 2020 年 6 月 1 日正式实施。该《办法》重点强调了“关键信息基础设施”的保护，主要依据《网络安全法》第三十五条规定：“关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查”。简单来说，就是“关键单位”采购 IT 产品时，必须符合“安全审核”。当前主要涉及电信、广播电视、能源、金融、公路水路运输、铁路、民航、邮政、水利、应急管理、卫生健康、社会保障、国防科技工业等关键行业。显然，“滴滴”作为交通行业重要运营者，也需要网络安全审查。在“滴滴事件”发生后，《网络安全审查办法》于 7 月 10 日征求意见，《网络安全审查办法（修订草案征求意见稿）》强调，掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。法律迅速升级，进一步扩大审核覆盖范围。

表 5：《网络安全审查办法》主要内容

	内容	说明
目的	关键信息基础设施供应链安全	维护国家网络安全
适用范围	关键信息基础设施运营者（以下简称运营者）采购网络产品和服务，影响或可能影响国家安全的	网络产品和服务主要指核心网络设备、高性能计算机和服务器、大容器存储设备、大型数据库和应用软件、网络安全设备、云计算服务等
主管机构	网络安全审查办公室；具体工作委托中国网络安全审查技术与认证中心承担	设在国家互联网信息办公室，负责制定网络安全审查相关制度规范，组织网络安全审查
运营者事先预判	应当预判该产品投入使用后可能带来的国家安全风险	如有影响，则需申报审查
获取供应商合同承诺	运营者应通过采购文件、协议等要求产品和服务提供者配合网络审查	包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或必要的技术支持服务等

资料来源：《网络安全审查办法》，国信证券经济研究所整理

网络和数据安全政策法律不断出台，节奏明显加快。滴滴事件引发了广泛的社会影响，有望成为我国网络和数据安全建设的重要转折点，未来对各类 IT 系统的网络、数据等各类信息安全审查和投入有望实现质的提升。在最前沿的智能汽车领域，8 月 12 日出台政策，强调了汽车数据安全，以及加强了 OTA 升级的安全管理。当前，个人信息保护法草案三次审议稿即将进入审议阶段，进一步规范 APP 过度收集个人信息。同时，2021 年 8 月 4 日，《党委（党组）网络安全工作责任制实施办法》首度公开，该政策自 2017 年 8 月 15 日起已经施行，进一步强调了党委（党组）的网络安全责任。8 月 17 日，《关键信息基础设施安全保护条例》正式公布，该政策已于 2021 年 4 月 27 日通过，将于 2021 年 9 月 1 日起施行。安全政策推进速度明显加快，可以预期《个人信息安全保护法》正式文件也即将出台。

表 6：网络和数据安全政策密集出台

日期	相关部门	名称	要点
2020.04.27	网信办、发改委、工信部、公安部、国安部等 12 个部门	《网络安全审查办法》	关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当按照本办法进行网络安全审查。
2020.10.21	全国人大法工委	《中华人民共和国个人信息保护法(草案)》	明确生物特征、医疗健康、金融账户、种族民族等多种敏感信息，增强了违法个人信息处理行为的法律责任，最高处罚可达 5000 万元或上一年度营业额 5%
2021.03.22	网信办、工信部、公安部、市场监督管理总局	《常见类型移动互联网应用程序必要个人信息范围规定》	App 不得因为用户不同意提供非必要个人信息，而拒绝用户使用其基本功能服务。
2021.06.10	全国人大常委会	《数据安全法》	确立数据分级分类管理以及风险评估，检测预警和应急处置等数据安全管理各项基本制度；明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任；同时加大对违法行为的处罚力度
2021.07.10	网信办	《网络安全审查办法（修订草案征求意见稿）》	掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。
2021.07.12	工信部	《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》	至 2023 年网络安全产业规模将超过 2500 亿元、年复合增速超过 15%；电信等重点行业网络安全投入占信息化投入比例达 10%
2021.08.12	工信部	《关于加强智能网联汽车生产企业及产品准入管理的意见》	明确企业应当建立健全汽车数据安全管理制度，依法履行数据安全保护义务。明确未经审批，不得通过在线等软件升级方式新增或更新汽车自动驾驶功能。
2021.08.17	国务院	《关键信息基础设施安全保护条例》	保障关键信息基础设施安全，重点在公共通信和信息服务、能源、交通、水利、金融等关乎国家安全、国计民生的行业。运营者需要建立制度，保证人、财、物投入，主要负责人对关键信息基础设施安全保护负总责

资料来源：网信办、工信部、国务院官网，新浪新闻，国信证券经济研究所整理

数据安全成为当前建设重点，各地方加速落地

数据成为最重要生产要素之一，互联网巨头成为整治重点。在“十四五”规划纲要草案中，首次将“数据”作为“生产要素”写入其中。草案明确要建立健全数据要素市场，加快完善“数据生产要素市场化”配套法律制度。当前阿里巴巴和腾讯相继被“反垄断”处罚，某些互联网厂商利用海量用户数据，针对性设计产品、大数据杀熟等现象屡见不鲜，因此互联网厂商也成为数据安全重点关注对象。工信部在 2021 年 7 月 30 日也召集了阿里、腾讯、美团、奇安信、小米等 12 家互联网企业，开展了贯彻落实《数据安全法》座谈会，对互联网厂商提出了明确的要求。

数据安全法将于 2021 年 9 月 1 日正式实施。《数据安全法》是数据领域的基础性法律，已于 2021 年 6 月 10 日表决通过，将于 2021 年 9 月 1 日起正式施行。《数

据安全法》将建立数据分类分级保护制度，要求各个行业明确自身的监管职责。同时，对数据“跨境流动”提出明确监管要求，规定了数据安全审查、数据出口管制、重要数据出境管理、对等反制措施等。另一方面，政府也会进一步完善政务数据的公开和共享机制。在《数据安全法》总纲之下，以深圳、上海、浙江为代表的各个地方也加速了本地数据条例的进程；上海同时成立了全国数据交易联盟，在数据开放上进一步探索。

表 7：数据安全政策及各地方实践

日期	相关部门	名称	要点
2021.06.10	全国人大常委会	《数据安全法》	确立数据分级分类管理以及风险评估，检测预警和应急处置等数据安全管理各项基本制度；明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任；同时加大对违法行为的处罚力度
2021.07.06	深圳人大	《深圳经济特区数据条例》	内容涵盖了个人数据、公共数据、数据要素市场、数据安全等方面，确立以“告知-同意”为前提的个人数据处理规则。
2021.07.10	上海数据交易中心，及 13 个省市数据交易机构	《数据交易上海倡议》	推动以公共数据开放、政企数据融合为基础的创新应用，共同推动数据要素市场建设和发展
2021.07.27	上海市政府	《上海市数据条例》草案	研究公共数据授权运营的相关条例，未来第三方数据服务机构或将通过备案或注册的形式“持牌”运营，公共数据市场化运营将获得法律保障
2021.08.02	浙江人大	《浙江省公共数据条例(草案)》	建设一体化智能化公共数据平台，促进省域整体智治、高效协同。明确省和设区的市、县(市、区)公共数据平台是公共管理和服务机构开展数据共享、开放的唯一通道和载体

资料来源：深圳市人民政府门户网站，新浪新闻，国信证券经济研究所整理

深圳率先发布《经济特区数据条例》，全国各地方有望加速落地。在践行《数据安全法》上，深圳于今年 7 月 6 日率先发布了《深圳经济特区数据条例》，是国内数据领域首部基础性、综合性立法。该条例涵盖了个人数据、公共数据、数据要素市场、数据安全等方面，明确自然人对个人数据依法享有人格权益。同时，该条例强调了以城市大数据为核心的公共数据治理体系，最大限度开放利用公共数据；探索培育数据要素市场，促进数据要素价值实现和市场公平竞争。该条例进一步强调了保护数据全生命周期安全，对违法者最高处罚可达到 5000 万元。深圳条例于 2022 年 1 月 1 日执行，其进一步明确了数据安全的做法和细则，有望成为全国各地方借鉴的样本，在全国加速落地。

表 8：条例中对个人数据的保护

个人数据保护要点	主要内容
明确处理个人数据的基本原则	处理个人数据应当具有明确、合理的目的，并遵循最小必要和合理期限原则
确立以“告知——同意”为前提的个人数据处理规则	处理个人数据具有告知义务，应当征得自然人的同意，提供撤回同意的途径
合理限制生物识别数据的处理	要求处理生物识别数据时，除该生物识别数据为处理个人数据目的所必需，且不能为其他非生物识别数据所替代的情形外，应当同时提供处理其他非生物识别数据的替代方案
规范用户画像和个性化推荐的应用	自然人有权拒绝数据处理者对其进行上述用户画像和基于用户画像进行的个性化推荐，数据处理者应当为其提供拒绝的途径
强化对未成年人个人数据的保护	将未满十四周岁未成年的个人数据视作敏感个人数据，适用敏感个人数据的有关规定

资料来源：《深圳经济特区数据条例》，国信证券经济研究所整理

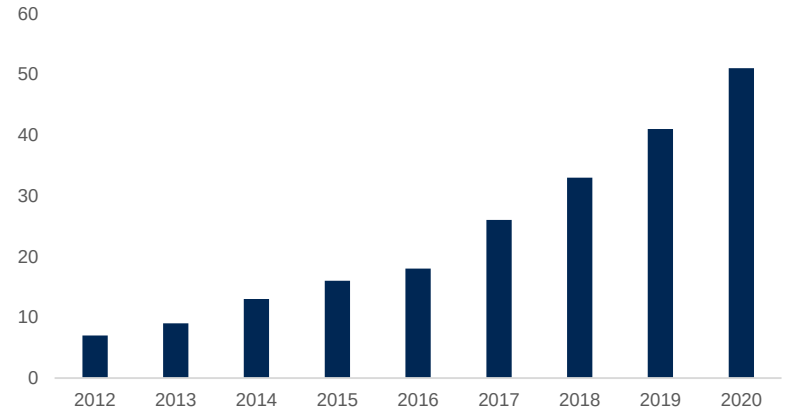
数据安全建设成新篇章，隐私计算开启千亿市场

传统数据交易所举步维艰，上海开启探索数据交易 3.0 新模式

数据量爆炸增长，价值亟待挖掘。随着物联网、边缘计算等智能终端设备不断普及，受到来自物联网设备信号、元数据、娱乐相关数据、云计算和边缘计算的数据增长的驱动，数据圈未来可预见呈现加速爆发。根据 IDC 预测，全球数据圈将从 2018 年的 33ZB 增至 2025 年的 175ZB，增长超过 5 倍；中国平均增速快于全球 3%，预计到 2025 年将增至 48.6ZB，占全球数据圈的比例由 23.4% 提升至 27.8%。其中，中国企业级数据圈将从 2015 年占中国数据圈的 49％增长到 2025 年的 69％。数据量迅速增长后，成为新的生产要素，亟待价值

挖掘。但是当前普遍现状是各类数据孤立，无法安全地形成多方共享和利用，始终无法发挥大数据真正有益价值。因此，数据的安全交易是当前重点技术和市场方向，尤其我国立法已逐步完善，且已在各地摸索尝试。

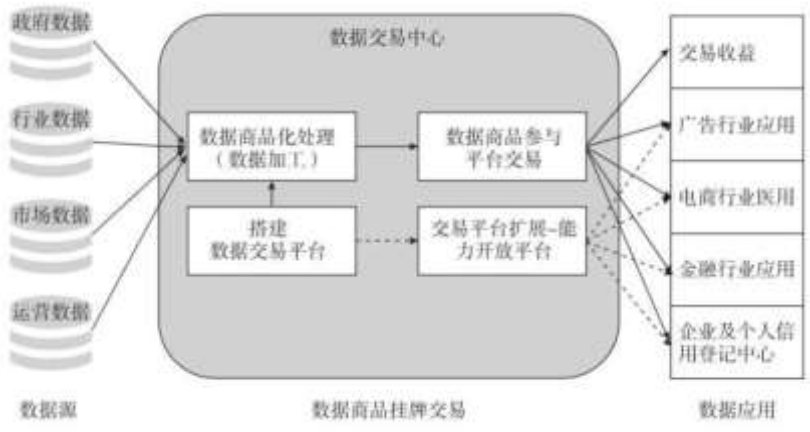
图 12：全球数据量迅速增长（ZB）



资料来源：IDC，国信证券经济研究所整理

各地数据交易所被寄予厚望，但发展不达预期。2015 年国务院印发了《促进大数据发展行动纲要的通知》，大力推动数据产业的发展。各地也纷纷成立数据交易所，其中有北京、贵阳、长江、东湖、西咸新区、河北、江苏、哈尔滨、上海、浙江等多个。这类数据交易所作为中立第三方，在交易过程中发挥制定规则和标准的作用，对供给方数据进行清洗、分析、建模等，在数据上线后负责撮合交易。其中贵阳数据交易所是全球第一家大数据交易所，根据 2018 年的数据，会员数量突破 2000 家，链入 225 家优质数据源，可交易数据产品近 4000 个，涉及金融、政府、电商、电信等 30 多个领域；贵阳大数据交易额一度突破 1.2 亿元，并实现盈利。但整体上，各地大数据交易所发展均不达预期，多数机构步履维艰。即使最老牌的贵阳数据交易所，根据最新报道，其业务量也微不足道，面临股改。不过，数据交易涉及法律、技术、合规等多个环节，这些都是发展的必要探索。在当前政策对数据安全重视空前的背景下，《数据安全法》出台后，隐私计算等技术有望重启行业。

图 13：大数据交易中心功能定位



资料来源：《2018 年中国大数据交易发展分析报告》，国信证券经济研究所整理

上海成立全国数据交易联盟，新技术助力 3.0 新模式，数据交易新发展可期。7 月 10 日上海数据交易中心携手 13 个省市数据交易机构正式成立全国数据交易联盟，积极响应“十四五”提到的“建立健全数据要素市场”。上海在数据流通交易领域

始终处于全国领先地位，上海数据交易中心 2020 年数据流通峰值日流通量达 1 亿条。全国联盟发起成立数据要素智能合约创新联合体，发布了基于区块链的新一代数据交易系统，以及多方安全计算服务平台，志在推动以公共数据开放、政企数据融合为基础的创新应用。从深圳和上海来看，数据安全相关建设率先在一线城市落地和启动，预计将逐步走向全国。相比之前各个地方数据交易所单兵作战，难以形成系统和规模，此次全国数据交易联盟有望实现技术和应用突破。

表 9：上海数据交易中心成果发布

技术创新	主要内容
数据要素智能合约联合创新体	多家机构共同发起成立数据要素智能合约创新联合体。智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议，是保障数据要素可信交易的关键技术之一，这些交易可追踪且不可逆转
基于区块链底层技术的新一代数据交易系统	利用区块链的可追溯和不可篡改等特性，对每笔交易和数据进行确权和记录。目前系统已纳入开放数据资源，汇聚超过 1 万个高质量数据集、全国 18 省公共数据 100,000 个开放数据集、人工智能行业 2000 余个高质量开放数据集，以及覆盖五大领域超过 100 个可流通算法集
多方安全计算服务平台	将堡垒机、密钥管理、权限控制等安全技术相融合，提供一整套基于云端的安全技术、计算技术和流通规则，确保数据所有者对数据的绝对控制权，数据需求方仅可获得计算分析后的结果，无法接触原始数据

资料来源：上海数据交易中心，国信证券经济研究所整理

隐私计算成为数据安全新蓝海，我国具备技术和场景优势

隐私计算融合多种技术，目前正逐步走向成熟。隐私计算交叉融合了密码学、人工智能、计算机硬件等多种技术，其中密码学包括混淆电路、秘密分享、不经意传输等底层技术，以及同态加密、零知识证明、差分隐私等辅助技术。最终形成了三大隐私计算方向：

第一、多方安全计算（MPC）。多方安全计算由图灵奖得主姚期智院士于 1982 年通过提出和解答百万富翁问题而创立。该技术在无可信第三方情况下，多个参与方共同计算一个目标函数，其中每一方只得到自己的结果，无法获得其他方的输入数据。该技术可以使用通用硬件架构，核心在于密码学技术，实现多方在各自数据保密下，数据进行融合计算，达到数据“可用而不可见”。

第二、以联邦学习（FL）为代表的人工智能和隐私保护融合衍生技术。联邦学习保证在本地数据不出库的情况下，通过对中间加密数据的流程和处理来完成多方联合的机器学习训练。该技术也是基于通用硬件，解决了数据拥有方，在进行 AI 训练时，数据可能泄露的问题。联邦学习实现了“数据不动模型动”。

第三、可信执行环境（TEE）。该技术通过软硬件技术，在 CPU 中构建了一个安全区域，保证内部加载的数据和程序在机密性和完整性上得到保护。目前，主流的通用计算芯片厂商均有发布 TEE 方案，如海外的 Intel 的 SGX、AMD 的 SEV、ARM 的 TrustZone；国内的兆芯的 ZX-TCT、海光的 CSV、基于 ARM 的飞腾和鲲鹏也有 TrustZone。TEE 技术主要是底层需要可信硬件，同样也需要对数据的加密和验证。

表 10：隐私计算相关技术主要对比

技术	性能	通用性	安全性	可信方	整体描述	技术成熟度
多方安全计算(MPC)	低~中	高	高	不需要	通用性高、计算和通信开销大、安全性高，研究时间长，久经考验，性能不断提升	已达到技术成熟的预期峰值
可信执行环境(TEE)	高	高	中~高	需要	通用性高，性能强，开发和部署难度大，需要信任硬件厂商	快速增长的技术创新阶段
联邦学习(FL)	中	中	中	均可	综合运用 MPC、DP、HE 方法，主要用于 AI 模型训练和预测	快速增长的技术创新阶段
同态加密(HE)	低	中	高	不需要	计算开销大，通信开销小，安全性高，可用于联邦学习安全聚合、构造 MPC 协议	快速增长的技术创新阶段
零知识证明(ZKP)	低	低	高	不需要	广泛应用于各类安全协议设计，是各类认证协议的基础	快速增长的技术创新阶段
差分隐私(DP)	高	低	中	不需要	计算和通信性能与直接明文计算几乎无区别，安全性损失依赖于噪声大小	快速增长的技术创新阶段
区块链 (BC)	低	中	中	不需要	基于带时间戳的块链式存储、智能合约、分布式共识等技术辅助隐私计算，保证原始数据、计算过程及结果可验证	逐渐接近技术成熟的预期峰值

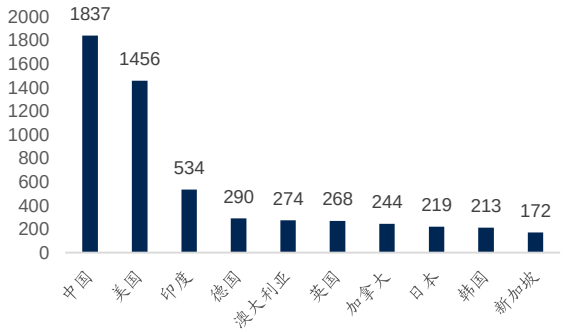
资料来源：《隐私技术白皮书 2021》，国信证券经济研究所整理

隐私计算技术逐步成熟，国内在该领域具备优势。Gartner 在 2021 年 7 月再次关注到隐私计算，强调加强对个人数据使用的控制，减轻数据滥用的风险等，并在“技术成熟曲线”中加入了联邦学习和主权云。隐私计算的技术从 2011 年开始，全球已经累计有 5280 篇，且每年新发论文数均保持 10%以上的增速。国内姚期智院士是多方安全计算领域的泰山北斗，同时中国也是全球该领域论文数量最多的国家，该领域中国具备技术优势。

图 14：联邦学习和主权云加入“技术成熟度曲线”

资料来源：Gartner 2021，国信证券经济研究所整理

图 15：各国隐私计算领域论文数量



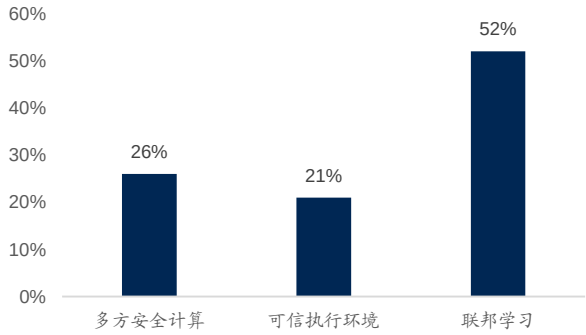
资料来源：《隐私技术白皮书 2021》，国信证券经济研究所整理

国内隐私计算已经进入发展期。隐私计算商业化最早可以追溯到 2008 年丹麦公司 Partisia，随后微软、谷歌等互联网巨头也纷纷入局。国内从 2016 年开始逐步有隐私计算商业化落地，并且已经进入快速发展期，越来越多的行业客户开始愿意尝试。根据中国信通院调研，2021 年上半年各隐私计算项目进展顺利，已经有 81%的隐私计算产品进入了试点阶段或实施阶段。在技术选择上，由于 AI 训练等需求较为明确，且有成熟的开源社区，运营商和金融科技公司大多选择联邦学习的路线开发隐私计算产品，占比高达 52%。对于各行业龙头企业，致力于打造平台化的多方安全计算基础设施，26%企业选择多方安全计算路线。

图 16：国内隐私计算平台应用情况

资料来源：《隐私技术白皮书 2021》，国信证券经济研究所整理

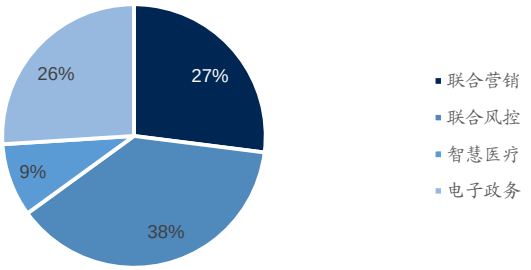
图 17：国内隐私计算平台技术路线



资料来源：《隐私技术白皮书 2021》，国信证券经济研究所整理

隐私计算具备千亿市场规模，下游应用广泛。根据 Gartner 测算，到 2023 年底，世界上 75%人口的个人数据讲受到隐私法规保护，现在只有 25%；全球 80%以上的公司将面临至少 1 项以隐私为重点的数据保护法；在技术支出上，到 2024 年，隐私驱动的数据保护和合规技术将在全球突破 150 亿美金。根据信通院统计，隐私计算典型应用场景包括联合营销、联合风控、智慧医疗、电子政务。例如，联合营销中，整合各产品商、银行、互联网公司等多方数据通过隐私计算建模，得到更精准的用户画像。联合风控中，多方金融机构联合打破“数据孤岛”，通过隐私计算实现跨机构数据挖掘和风险评估。智慧医疗中，疫情防控可以利用隐私计算追溯高位人群，同时保护个人隐私。电子政务中，政府通过隐私计算平台共享公共数据，实现多方共同使用，真正发挥数据价值。

图 18：隐私计算应用场景



资料来源：《隐私技术白皮书 2021》，国信证券经济研究所整理

安全产业规模和投入再梳理，等保和关保催化带来切实增量

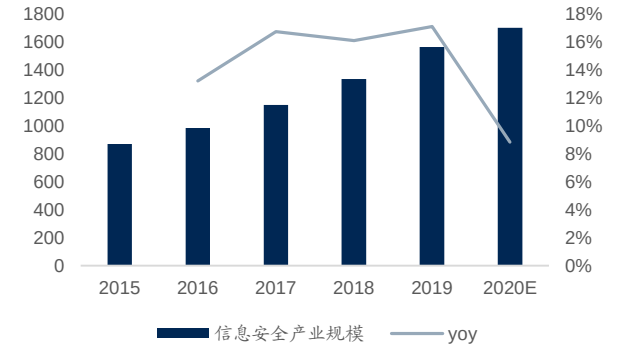
当前网络安全市场规模到底如何？

工信部规划 2023 年网络安全产业规模超过 2500 亿。根据工信部在 2021 年 7 月发布的《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》，计划到 2023 年网络安全产业规模超过 2500 亿元，年复合增长率超过 15%；其中电信等重点行业网络安全投入占信息化投入比例达 10%。

不同口径下，行业规模统计差别大。行业里常用的 IDC 数据，主要由网络安全硬

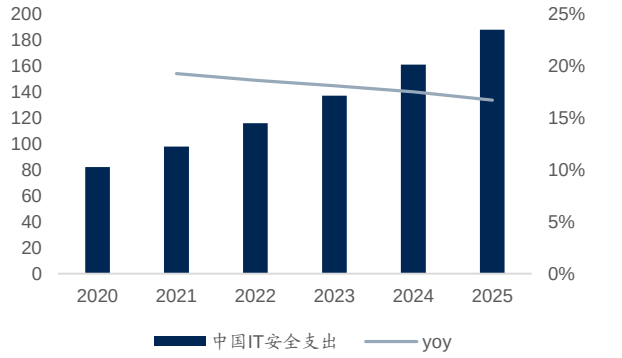
件（防火墙、UTM、行为管理、VPN、IDPS 等）、软件（身份管理、终端安全、AIRO 等），以及服务（咨询、托管、培训等）构成，2020 年大约是 500 多亿人民币，也是国内主流网络安全上市公司的主要覆盖领域。根据中国信通院发布的《中国 IT 安全软件市场跟踪报告 2020》，最新测算中，信通院调整了产业统计口径，将区块链应用、密码、以及云服务商、运营商、车联网企业的安全业务纳入计算范围。中国信通院统计下，2019 年网络安全产业规模达到 1563.59 亿元，预计 2020 年达到 1702 亿元。因此，IDC 和信通院统计口径差距较大，造成了二者网络安全市场规模相差较大。

图 19：我国网络安全产业规模（亿元）



资料来源：中国信通院，国信证券经济研究所整理

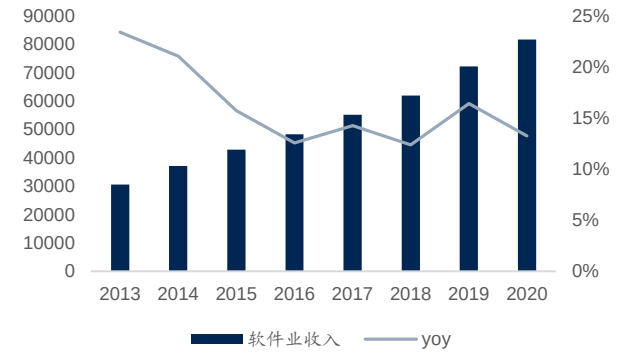
图 20：中国 IT 安全牛市场支出预测（亿美元）



资料来源：《IDC 全球网络安全支出指南》、国信证券经济研究所整理

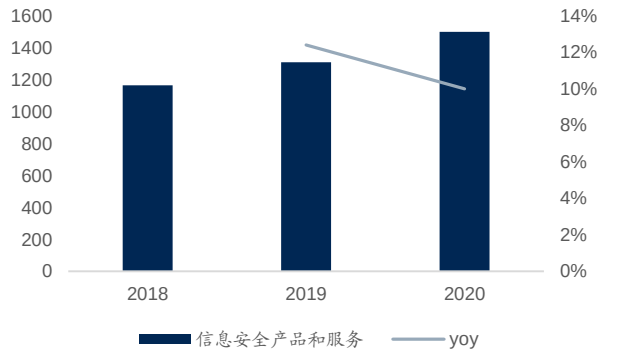
工信部口径数据与信通院接近，2020 年安全收入达到 1498 亿元。根据工信部 2020 年软件和信息技术服务业统计公报，2020 年全国软件和信息技术服务业规模以上企业超 4 万家，累计完成软件业务收入 81616 亿元，同比增长 13.3%。受疫情影响，信息安全产品和服务收入达到 1498 亿元，增速回落至 10%。工信部在 2019 年对信息安全口径进行了调整，从近三年数据来看，信息安全收入规模与中国信通院数据接近。

图 21：全国软件业务收入（亿元）



资料来源：工信部，国信证券经济研究所整理

图 22：全国信息安全产品和服务收入（亿元）



资料来源：工信部、国信证券经济研究所整理

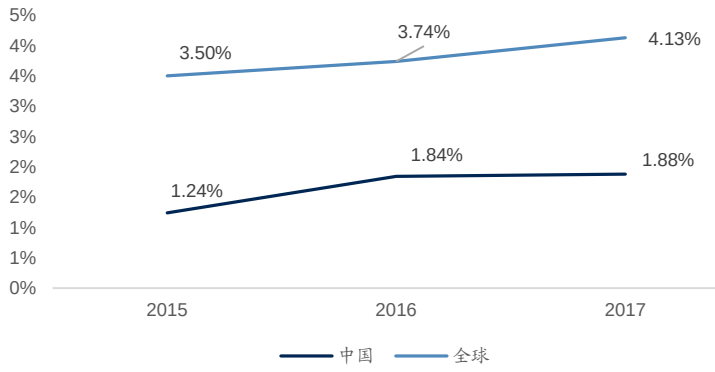
产业增速确定向上，行业空间进一步打开。以同一口径的工信部数据为参考，2020 年网络安全市场为 1498 亿元，2023 年要达到 2500 亿，复合增速要达到 18.62%；相比之前的增速提升了 5 个百分点以上。参考 IDC 指引，2025 年中国网络安全市场有望达到 187.9 亿美元，五年复合增速达到 17.9%，接近全球增速两倍水平。因此，网安产业增速确定向上。另一方面，工信部在 2019 年 9 月的《关于促进网络安全产业发展的指导意见（征求意见稿）》中也提出，到 2025 年，网络安全产业规模超过 2000 亿，形成一批年营收超过 20 亿的网络安全企业。根据工信部最大的规划，产业规模以 2500 亿为目标，空间进一步打开，且时间也得到提前。

网络安全占 IT 投入比到底是多少？

10%成为网络安全占 IT 投入比的新目标。2021 年 7 月 9 日，在上海举办的世界人工智能大会安全论坛上，上海市经济和信息化委员会软件和信息服务业处处长裘薇表示，正和网信办协商，在今年发布的网络安全“十四五”规划，以及即将发布的网络安全产业的行动计划当中，进一步明确政府和公共企事业单位在网络安全上的投入比例不低于 10%。无独有偶，在 2020 年 11 月底，北京的 2020 年中国网络安全产业高峰论坛中，工信部副部长刘烈宏也说到“增加网络安全占信息系统建设投入的比重。我们希望这个比重要至少突破 5%”。紧接着，工信部 7 月最新规划中，再次提出电信等重点行业安全投入比要达到 10%。

多方测算下，当前国内安全投入比仍低。根据 IDC 口径数据，2017 年我国安全占 IT 投入比为 1.88%，全球平均 4.13%，仍有一倍以上差距。根据 2020 年 IDC 数据，我国 IT 市场 2.07 万亿，其中安全市场约 79 亿美金，500 多亿人民币；结合其他第三次机构测算也不到 600 亿人民币，因此计算下来，整体安全占 IT 投入比不到 3%。另一方面，根据工信部 2020 年软件和信息技术服务业统计公报计算，全年信息安全收入 1498 亿元，整体软件业务收入 81616 亿元，安全投入比也仅为 1.8%。因此，全国平均信息安全占 IT 投入比仍处于较低水平。

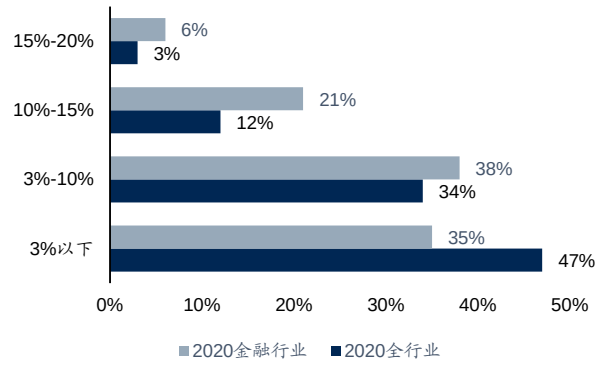
图 23：全球及中国信息安全投入占 IT 投入比



资料来源：IDC，国信证券经济研究所整理

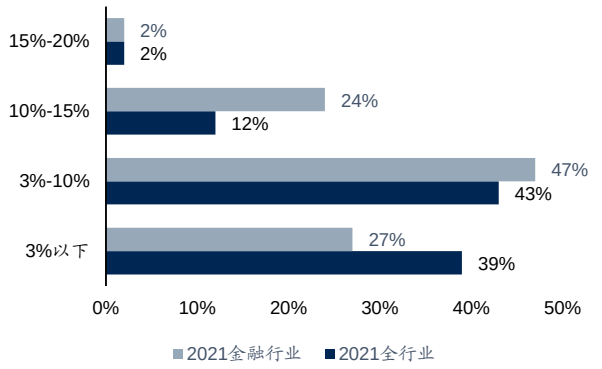
预算角度来看，国内安全投入提升是确定性方向。根据第三方安全咨询机构 FreeBuf 对企业安全预算的调研，国内各类甲方对安全占 IT 预算比均有提升。调研样本中，互联网/电商占比 29%、金融占比 21%、通信及 IT 业占比 16%，三大信息化和安全水平较高行业合计占比 66%，一定程度上拉高了安全投入比的平均水平。尤其金融行业是安全投入最重的一个行业，投入在 3%以下的企业 2021 年占比仅为 27%，安全投入一直高于行业平均水平。全行业来看，2020 年安全投入在 3%以下的占比有 47%，2021 年有望下降为 39%。虽然调研数据主要来自对安全重视程度高的行业，但是持续加大安全投入是确定无疑。

图 24：2020 年金融及全行业安全占 IT 预算比



资料来源：FreeBuf，国信证券经济研究所整

图 25：2021 年金融及全行业安全占 IT 预算比

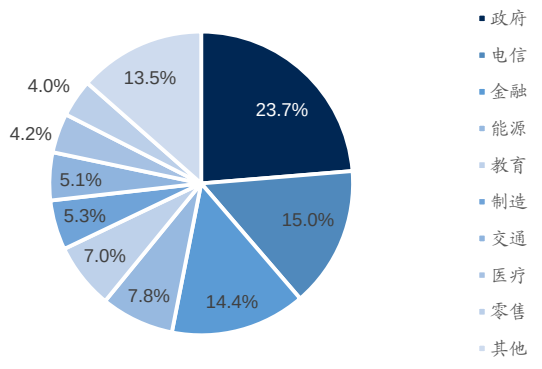


资料来源：FreeBuf、国信证券经济研究所整理

政府、电信等行业国内占比高，10%为目标有望带来百亿以上增量市场，其他行业有望逐步跟进。网络安全建设理论上没有严格边界，细分行业和产品众多；因此 IT 预算和安全投入最为重要，只要有足够预算，市场可以持续扩张。政府、电信、金融三大行业由于合规和信息化水平要求高，是网络安全最大的下游市场，合计占比超过 50%；即使安全投入比高于平均水平，也远未到 10%。政府等大行业安全投入比提升至 10%，有望带动至少百亿以上市场空间。另一方面，对比全球行业结构，我国政府之外的其他行业安全投入更低，因此随着各行业信息化提升，以及相关政策覆盖，其他行业安全投入有望逐步跟进。

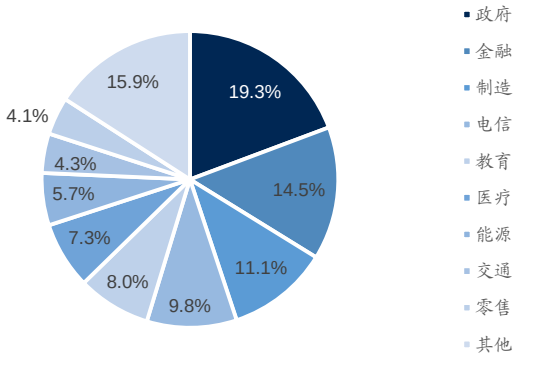
美国联邦政府 2021 财年网络空间安全预算占 IT 预算比值超过 20%。根据美国联邦政府公布 2021 财年预算草案，2021 财年网络空间安全（Cybersecurity）领域的预算有 188 亿美元（不含涉密预算），其中国防部占了 98.5 亿美元，占比超过一半；民事部门是 90 亿美元；国土安全部占了 26 亿美元；司法部占了 9.3 亿美元。按技术划分，识别、保护、检测、响应和恢复五个环节的预算都有所增长。整体上，美国联邦政府的网络安全预算占 IT 预算的比重是 20.4%，绝对金额和占比均有增加。参考美国，我国政府领域信息安全投入有望持续加大。

图 26：2019 年中国网络安全市场行业划分



资料来源：Frost&Sullivan，国信证券经济研究所整

图 27：2019 年全球网络安全市场行业划分



资料来源：Frost&Sullivan、国信证券经济研究所整理

等保 2.0 测评标准变化，再强调数据安全，直接带动网安新品放量

等保 2. 0 在 2019 年开启信息安全建设新篇章。《信息安全技术网络安全等级保护基本要求》2.0 版本（等保 2.0）已于 2019 年 12 月 1 日正式实施。等保 2.0 是对我国所有企业信息系统安全建设的基础要求，对各类信息系统进行 1-5 级定级，并

定期进行打分测评（3 级及以上系统每年均需要等保测评）。等保 2.0 发布在 2007 年等保 1.0 版本的 10 多年之后，对 1.0 标准进行了调整，同时加大了对云计算、移动互联、工控安全、物联网的覆盖。等保 2.0 在评分上也进行了提高，要求是 70 分及格（原来是 60 分）。等保 2.0 是我国当前各行业信息安全建设的基础，2019 年的发布再次推动了信息安全产业的发展。

图 28：等保 2.0 监管范围扩大

资料来源：e 安在线，国信证券经济研究所整理

图 29：等保 2.0 评分标准

资料来源：等保 2.0 测评模板、国信证券经济研究所整理

等保 2.0 测评标准重大修订，扣分制导致企业过关难度剧增。2021 年 6 月等保 2.0 的测评报告模板发生了重大修订，其中技术修订属于“重大修订”，与 2019 年版本有较大差异，如评分计算公式调整，将直接导致企业测评合规与否。从最新《等级测评报告模板(2021 版)》来看，企业测评通过难度明显加大，主要系技术修订上的三大变化:

第一、调整综合得分计算公式。由于 2019 年测评模板计算公式综合得分偏高（集中在 80 分以上），且安全类权重一样（技术和管理各 50%），计算量较大；2021 版公式改为缺陷扣分法，技术和管理分数也可以调整权重，同时对于测评指标细分为一般、重要和关键，关键测评指标不符合将扣除 3 倍基准分，重要测评指标不符合扣除 2 倍基准分。

第二、将数据作为独立测评对象。2021 版测评中将数据单列测评，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据和个人信息及大数据等。2021 版报告中从不同测评对象上汇总测评证据，包括数据完整性、数据保密性、剩余信息保护、备份恢复和个人信息保护等，覆盖网络设备、安全设备、服务器和终端及系统管理软件/平台等所涉及的鉴别数据和重要配置数据等。

第三、删除控制点得分计算。扣分制下，不再试用原控制点得分。

等保 2.0 新测评模板，企业得分大打折扣。本次等保 2.0 新测评模板已经过公安部培训和下发，相关测评机构在 2021 下半年也会陆续采用新模板开展测评工作，将直接影响各企业单位新旧 IT 系统的信息安全建设。对于三级级以上信息系统，每年均需要测评，因此即使今年在新模板前已经通过测评，明年仍会按照新模板要求重新测评。三级通用标准共有 211 个指标，其中关键指标 137 个，占比 65%（且扣分最重）；重要指标 71 个，占比 34%；一般指标 3 个，占比 1%。因此，关键测评指标对分数影响很大，官方也做过测试，如果大多数关键测评指标不符合，则 2021 版测评相比 2019 版分数要要低的多。

表 11：多种测评场景下评分差别

场景	风评	2019 版	2021 版	差值
安全技术类指标均为不符合，安全管理类指标均为符合	差	50	50	0
各个大类下均有一个一般指标（10 个）不符合和一个重要指标（10 个）部分符合	良	90.91	83.89	-7.02
安全计算环境类有 10 个重要指标均为不符合，其他指标均为符合	良	97.62	90.05	-7.57
各个大类下均有一个重要指标（10 个）不符合和一个关键指标（10 个）部分符合	中	89.53	80.57	-8.96
各个大类下均有一个一般指标（10 个）和一个重要指标（10 个）不符合	中	87.64	77.73	-9.91
各个大类下均为一个重要指标（10 个）和一个关键指标（10 个）不符合	差	84.53	73.93	-10.6
安全计算环境类有 10 个关键指标均为不符合，其他指标均为符合	中	96.74	85.78	-10.96
关键指标（不符合 5，部分符合 5）、重要指标（3，5）、一般指标（3，3），各一个对象	中	91.85	79.15	-12.7
安全通信网络和安全区域边界类指标均为不符合，其他指标均为符合	差	80	66.35	-13.65
安全物理环境类所有指标均为不符合，其他指标均为符合	差	90	73.46	-16.54
关键指标（不符合 5，部分符合 9）、重要指标（3，9）、一般指标（3，6），各一个对象	中	89.93	71.8	-18.13
安全计算环境类有 10 个重要指标、10 个关键指标均为不符合，其他指标均为符合	差	94.36	75.83	-18.53
一般指标（12 个）、重要指标（12 个）、关键指标（12 个）不符合	差	77.24	55.92	-21.32
安全计算环境类指标均为不符合，其他指标均为符合	差	90	56.87	-33.13
一般指标（17 个）、重要指标（19 个）、关键指标（17 个）不符合	差	71.71	36.49	-35.22
所有指标均为部分符合	差	50	0	-50

资料来源：等保测评报告模板（2021）版培训文件，国信证券经济研究所整理

新测评模板下的低分，将倒逼企业增加网络安全投入。在具体案例中，也可以看到多数信息系统在新测评中，分数均有不同程度的下降。原来企业某系统 80 以上，乃至 90 多分都是非常普遍现象，但是在新模板下，该系统测评下来可能只有 60 多分，甚至更低，如地质调查骨干网络系统、国库外围平台等。因此，企业在无法顺利通过等保 2.0 测评的情况下，必然要加强网络安全投入，相关产品采购以及预算必然增长。

表 12：新测评模板下 9 大实例评分情况

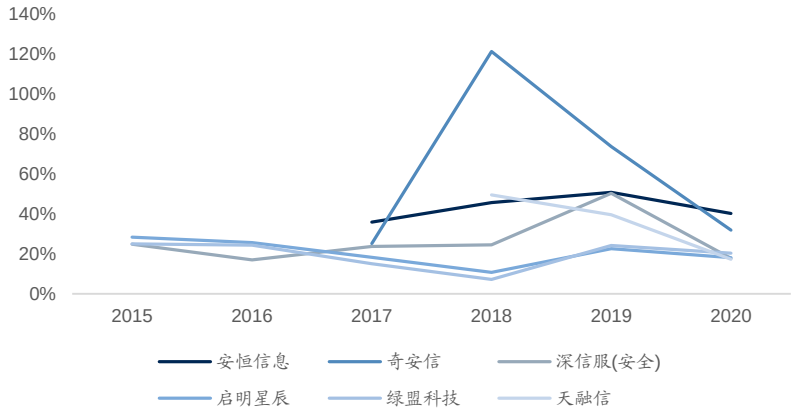
序号	信息系统	安全保护等级	指标符合情况	等级测评结论	适用项数	2019 版公式	2020 版-3 倍 扣	2020 版-2 倍 扣
1	中航信航班控制系统	S3A3	一般指标：不符合 1 个 重要指标：不符合 2 个，部分符合 1 个 关键指标：不符合 7 个，部分符合 1 个	良	188	97.85	87.77	91.49
2	中国石油加油站管理系统	S3A3	一般指标：不符合 1 个 重要指标：不符合 1 个，部分符合 2 个 关键指标：不符合 4 个，部分符合 4 个	良	154	90.75	81.49	87.18
3	地质调查骨干网络系统	S2A3	一般指标：不符合 2 个 重要指标：不符合 4 个，部分符合 6 个 关键指标：不符合 9 个，部分符合 13 个	良	174	88.62	64.08	75.00
4	阿里云平台	S3A3	一般指标：不符合 3 个 重要指标：不符合 1 个，部分符合 4 个 关键指标：不符合 0 个，部分符合 22 个	优	252	97.53	83.33	88.29
5	国库外围平台	S3A3	一般指标：不符合 3 个 重要指标：不符合 0 个，部分符合 24 个 关键指标：不符合 0 个，部分符合 57 个	良	199	87.99	43.47	60.08
6	百度云信息系统	S3A3	一般指标：不符合 3 个 重要指标：不符合 0 个，部分符合 1 个 关键指标：不符合 3 个，部分符合 4 个	良	239	98.00	92.05	94.25
7	新华云基础平台	S3A3	一般指标：不符合 3 个 重要指标：不符合 3 个，部分符合 6 个 关键指标：不符合 4 个，部分符合 12 个	良	215	84.00	79.07	85.12
8	全票通系统	S3A2	一般指标：不符合 0 个 重要指标：不符合 0 个，部分符合 5 个 关键指标：不符合 13 个，部分符合 7 个	良	197	95.00	73.86	82.36
9	石油公共云基础服务平台	S3A3	一般指标：不符合 3 个 重要指标：不符合 3 个，部分符合 3 个 关键指标：不符合 X 个，部分符合 X 个	良	241	97.53	68.88	78.53

资料来源：等保测评报告模板（2021）版培训文件，国信证券经济研究所整理

等保 2.0 新测评模板为行业带来切实增量，有望复制 2019 年行业景气。虽然等保 1.0 时期也有对信息安全建设的要求，但时间过久，且监管放缓，导致各地各行业信息安全重视程度下降。等保 2.0 测评于 2019 年 12 月正式实施，但是 2019 年全年就已经开始在各个行业进行推进，并且建设力度和监管力度加大，为整个信息安全行业带来新增长。受益于等保 2.0 在 2019 年的推动，全行业主要上市公司增速

均有明显提升，例如深信服和安恒信息安全增速达到 50%以上，启明星辰和绿盟科技也重回 20%以上增长。原来企业过等保，可选类产品设备如态势感知、APT 检测、蜜罐、数据库审计、日志审计等产品并非必需品，而本次新测评模板采用后，相关产品缺失成为扣分项，因此将显著推动这类产品的需求。网络安全市场有望迎来切实增量。

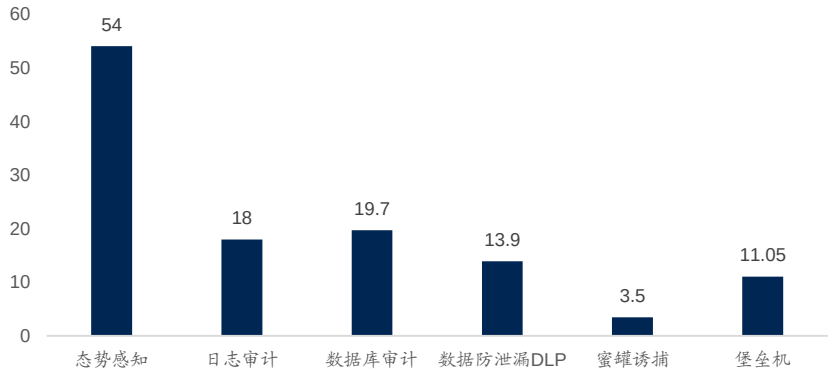
图 30：2019 年各主要安全上市公司业绩增速回暖



资料来源：公司公告，国信证券经济研究所整理

等保 2.0 测评变化将带来切实产业增量，各类安全厂商充分受益。原来常规安全建设中，防火墙、IDPS、WAF、VPN、上网行为管理、终端杀毒等是主要产品，也是曾经通过等保 2.0 的基本产品。当前测评评分等变化后，由于扣分压力，企业对于态势感知、审计类产品、数据安全产品、APT 防护和蜜罐等均会加大采购需求。根据多方预测，这些产品市场规模 2021 年加总约 120 亿，对整个网络安全行业产生实质利好，尤其是在数据安全、新兴攻防领域布局的安全厂商。

图 31：各产品 2021 市场规模预测



资料来源：赛迪咨询、数世咨询、Frost&Sullivan、国信证券经济研究所整理

《关键信息基础设施安全保护条例》再接力，安全预算增长再添筹码

关保终落地，重磅政策再为安全产业加码。2021 年 8 月 17 日，《关键信息基础设施安全保护条例》终于公布，关保已经于 2021 年 4 月 27 日被国务院通过，将于 2021 年 9 月 1 日起施行。关保条例从提出、草案、审议，已历经多年，当前终于落定，进一步验证我国对安全建设的不遗余力。关保主要针对安全问题可能会危害国家安全、国计民生的重点行业，如公共通信和信息服务、能源、交通、水利、金融等，其中能源和电信被重点提及，要求优先保障。关保规定了运营者责任义务，

运营者需要建立制度，保证人、财、物投入，主要负责人对关键信息基础设施安全保护负总责。具体要求有安全与关键信息基础设施同步规划和建设；设置专门安全管理机构；保障机构的运行经费及人员等。

表 13：关键信息基础设施安全保护条例要点

核心点	主要内容
关键信息基础设施认定	1.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、国防科技工业等重要行业，安全问题存在危害国家安全、国计民生的可能 2.关基发生较大变化，运营者应及时报告保护工作部门，3 个月内完成重新认定
关保主要统筹机构	1.国家网信部门统筹协调，公安部门负责指导监督关保工作。国务院电信主管部门、其他有关部门、省级人民政府有关部门也要负责对关基的保护和监督管理 2.网信办统筹下，公安部、电信主管部门等需要建立网络安全信息共享机制、关基安全检测、关基安全技术支持等
行业要求	1.制定本行业、本领域关键信息基础设施安全规划 2.建立本行业关键的监测预警制度，掌握关基的运行状况、安全态势 3.建立本行业的网络安全事件应急预案，定期组织应急演练 4.定期组织开展本行业关基的网络安全检查
运营者责任义务	1.安全与关键信息基础设施同步规划、建设、使用 2.建立健全网络安全保护制度和责任制，保障人力、财力、物力投入，运营者的主要负责人对关键信息基础设施安全保护负总责 3.设置专门安全管理机构，负责本单位关基保护，报告制度、演练、检测、培训、管理等 4.保障专门安全管理机构的运行经费、配备相应的人员 5.自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估 6.发生事件和威胁时，向保护工作部门、公安机关报告 7.优先采购安全可信的网络产品和服务，与提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任 8.运营者发生合并、分立、解散等情况，应当及时报告保护工作部门
重点提及行业	1.优先保障能源、电信等关键信息基础设施安全运行 2.加强网络安全军民融合，军地协同保护关键信息基础设施安全

资料来源：《关键信息基础设施安全保护条例》，国信证券经济研究所整理

关键信息基础设施保护是安全重点，国外政府已经走在前列。关键信息基础设施被攻击造成的危害是无法承受的，如 2010 年伊朗核设施被“震网”病毒攻击，2021 年美国最大输油管道遭网络攻击关闭等。因此，对关键信息基础设施的保护在全球都是重中之重。世界主要国家和地区均有将“关键信息基础设施”作为立法和保护的重点，美国和欧盟走在前列，我国在等保 2.0 之后进而推出关保。当前，进一步加大对网络安全的投资已成为全球共识。

表 14：国外关键信息基础设施保护政策

最早政策时间	国家	主要政策
2001 年	美国	《2001 年关键基础设施保护法》，之后相继出台《改进关键基础设施网络安全行政令》《增强联邦政府网络与关键基础设施网络安全行政令》。近期发布了《2021 年临时国家安全战略方针》《2021 年关于加强国家网络安全的行政命令》
2008 年	欧盟	《2008 年欧盟关键基础设施认定和安全评估指令》，《2016 年网络与信息安全指令》，2020 年的《欧盟安全联盟战略》中，将提升关键基础设施的保护和恢复能力作为未来五年网络安全工作的重中之重
2013 年	俄罗斯	《俄联邦关键网络基础设施安全》，《联邦关键信息基础设施安全法》
2015 年	德国	《德国网络安全法》，加强对关键信息基础设施的保护力度
2018 年	澳大利亚	《关键基础设施安全法》

资料来源：网信中国，国信证券经济研究所整理

关保在等保 2.0 上更进一步，安全预算增长更确定无疑。等保 2.0 主要是面向我国各行各业所有的信息系统，理论上均需要按时进行等保定级和测评。等保 2.0 是各企业都需要通过的，最基础的安全建设测评，覆盖范围最广，要求相对也最低，即使当前测评模板升级后，通过难度有所增加。另一方面，《密码法》于 2020 年 1 月正式实施，其规定使用商用密码进行保护的关键基础设施，其运营者应履行开展密评工作。因此，关保是在等保 2.0 和密评基础之上展开，虽然其覆盖范围仅限于关键信息基础设施，但是其要求更严格。关保条例中明确说明，“在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件”。同时，关保也明确提出了设立机构、配备人员、保障经费；叠加等保 2.0 测评变化，以及数据安全法实施，将确定性提升明年安全预算。

图 32：关保、密评、等保关系

资料来源：上海 CA 中心，国信证券经济研究所整理

行业高增长确定性十足，重点关注数据安全厂商

全行业股权激励，行业高增充满信心

全行业积极股权激励，捆绑核心人才看好发展。信息安全行业人才稀缺性大，各个厂商均有加大对核心技术人才的激励。从考核目标上看，均没有设置过高的目标。从激励时间来看，全行业均集中在 2020Q3 开始，一定程度上也认为 2020 年上半年是行业发展低点，下半年开始行业进入全面回暖。从 2020 年下半年开始，截止目前，网络安全 9 大厂商共做了 10 次股权激励，彰显了全行业高增长信心。在众多安全厂商中，安博通作为厂商的厂商，扮演了行业上游的角色，其 2021 年收入目标在 2020 年目标基础上增长了 40%，也表明了行业对明年产业回暖的信心。结合当前一系列政策密集出台，网络安全产业有望加速发展。

表 15：网络安全全行业股权激励

公司	时间	业绩考核
奇安信	2020 年 10 月 30 日	以 19 年营收为基数，20-23 年收入增长率不低于 25%/55%/90%/135%
深信服	2020 年 7 月 7 日	以 2019 年营业收入为基数，20-22 年营收增速不低于 5%/10%/15%
安恒信息	2020 年 8 月 26 日	以 2019 年营业收入为基数，20-23 年营收增长率不低 25%/50%/75%/100%
启明星辰	2020 年 9 月 23 日	以 2019 年营业收入为基数，20-22 年营业收入增长率不低于 5%/10%/15%
天融信	2020 年 9 月 9 日	以 2019 年营业收入为基数，20-22 年营业收入增长率不低于 10%/20%/30%；或者 20-22 年净利润不低于 6.5/7.5/8.5 亿元(二选一)
安博通	2020 年 10 月 31 日	20-22 年营业收入不低于 2.5/3.5/4.5 亿元
山石网科	2020 年 12 月 4 日	以 2020 年营收为基数，21-24 年营收增长率不低于 25%/50%/75%/100%
迪普科技	2021 年 3 月 5 日	以 2020 年营收为基数，21-23 年营收增长率不低于 20%/40%/60%
绿盟科技	2021 年 4 月 23 日	以 2020 年营收为基数，21-23 年三档考核目标分别为复合 20%、复合 10%、复合 5%营收增速
天融信	2021 年 5 月 31 日	以 2020 年营业收入为基数，21-23 年营业收入增长率不低于 10%/20%/30%；或者 21-23 年净利润不低于 7.5/8.6/10 亿元(二选一)

资料来源：公司公告，国信证券经济研究所整理

安恒信息——数据安全起家，数据安全岛布局隐私计算

安恒信息以应用和数据安全起家，数据库审计行业领先。安恒早期以数据安全起家，数据库审计产品市场份额保持前二，如数据库安全网关、数据库审计与风险控制系统、数据库漏洞扫描系统。2021 年 7 月 21 日，公司再次发布数据安全解决方案，提出“CAPE”数据安全能力框架为基础保护数据安全，即风险核查（C）、数据梳理（A）、数据保护（P）、监控预警（E）。新兴数据安全产品主要是平台类，如 AiLPHA 数据安全管控平台、AiLand 数据安全岛平台、

Aisort 数据安全分级与风险评估系统、AiTrust 零信任应用代理系统等。

数据安全岛已获得市场认可，入选隐私计算平台。安恒发布 AiLand 数据安全岛，是一个专注于保障数据安全流通的隐私计算平台，实现共享数据的所有权和使用权分离，确保原始数据的“可用不可见”、“可用不可取”。产品采用了综合应用安全计算沙箱，联邦学习，区块链，密文计算等多种数据安全技术，在赛迪“2021 IT 市场年会”中获得“新一代信息技术创新产品”奖。同时，安恒数据安全岛在 2021 年 7 月通过中国信通院隐私计算测试，首批入选 50 大隐私计算平台。AiLand 数据安全岛未来有望在数据开放、挖掘、共享、交换等领域发挥价值。

图 33：安恒信息数据安全岛

资料来源：安恒信息官网，国信证券经济研究所整理

奇安信——数据安全增长快，发布隐私计算产品

奇安信数据安全高增长，各类数据安全产品线全面。公司数据安全产品丰富，边界侧有数据安全交换平台，数据安全单向导入平台；数据侧有数据库审计与防护系统、数据库防火墙、数据库漏洞扫描系统、数据脱敏系统、运维安全管理与审计系统（堡垒机）、数据交易沙箱（防水堡）；文件侧有电子文件密级标志管理系统、电子文档安全管理系统等。2021 上半年，公司数据安全相关产品整体收入超过 2.8 亿元，同比增长率超 100%。大数据安全与隐私保护及零信任数据安全增长率均超过 60%，电子数据取证收入增长率超过 300%。

奇安信 2021 年 5 月正式发布数据安全开放平台“数据交易沙箱”，布局隐私计算。针对最敏感的“数据交易”环节，数据拥有方提供数据，在“数据交易沙箱”中进行交易和计算，这样需求方只能使用而无法获取，真正实现数据隐私安全，达到“数据不动程序动”、“数据可用不可见”的安全理念。尤其是政府单位，拥有最全面的数据，如果充分利用价值难以估量。但现实往往是害怕数据泄露，而“不敢”，“不能”充分利用。奇安信“数据交易沙箱”是当前隐私计算技术应用、数据安全领域的代表产品。

图 34：奇安信数据交易沙箱

资料来源：奇安信官网，国信证券经济研究所整理

绿盟科技——亿赛通 DLP 优势明显，数据安全运营平台应运而生

专业数据安全子公司助力，绿盟持续加大数据安全开拓。绿盟在 2014 年 9 月以 4.98 亿收购亿赛通 100%股权，双方数据安全能力进一步整合。亿赛通 2020 年收入 1.68 亿，利润 0.34 亿，DLP 产品以 17.1%的份额位居行业第一（2019 年赛迪数据）。公司数据安全产品线丰富，包括审计检测类（DLP 为主），加密防护类（磁盘、文档加密及管理），安全管理类（数据库审计、脱敏、防火墙等），安全平台类（数据安全态势感知平台）等。2020 年 10 月，绿盟进而发布数据安全运营平台，通过联动数据安全防护系统，基于相关日志等多类数据源，提供完善数据资产识别与自动分类分级、数据安全风险监控、数据安全访问权限统一管控和数据全生命周期安全运营能力。

图 35：绿盟科技数据安全运营平台

资料来源：绿盟科技，国信证券经济研究所整理

启明星辰——数据安全不容小觑，2020 年收入规模约 6 亿

启明星辰最早进入数据安全领域，产品线齐全。启明星辰于 2013 年涉足数据安全领域，是业界最早进入数据安全领域的网络安全公司。首款数据安全产品—数据库审计与防护系统自 2014 年取得市场份额第一以来，连续蝉联第一至今。启明星辰于 2014 年收购书生电子、合众数据，进一步完善数据安全能力。数据安全产品线

包括数据防泄密 DLP、数据加密、数据防护、数据脱敏、数据安全交换、电子签章、安全文档等，最新推出数据安全治理管控平台，可以形成完整的数据安全解决方案。公司 2020 年销售数据安全类产品约 6 亿，保持数据安全领先地位。

迪普科技——运营商领域数据安全有望发力

迪普科技与中国移动携手发布《运营商数据安全白皮书》。运营商领域安全建设有望重点发力，不管是工信部提出的电信行业安全占比达到 10%，还是关保条例也重点提到了电信行业，随着 5G 建设逐步深入，数量和流量进一步爆发背景下，安全投入有望持续加大。迪普科技与移动围绕数据生命周期安全进行了研究，运营商领域数据安全建设有望发力。迪普数据安全产品包括敏感数据发现系统、数据库防火墙、数据安全管控平台、数据库审计，数据安全持续加大投入。

深信服——将 AI 技术引入数据分类分级

深信服率先在智能数据分类分级上进行探索。数据分类分级工作是建设数据安全的基础工作，但当前主要依靠人力，成本高且准确率低。深信服智能数据分类分级平台率先引入了人工智能与机器学习算法，通过对分类分级策略定义，实现多维数据特征提取，完成智能分类分级推荐。分类分级结果以 API 的形式对外开放，智能推荐率达到 90%以上。目前，深信服智能数据分类分级平台已在多个客户完成测试、验证和使用，均受到用户好评。

风险提示

各类网络安全政策推进和执行不达预期。

市场竞争加剧，全行业盈利能力下滑。

疫情等负面影响反复，导致 IT 支出下降。

国信证券投资评级

类别	级别	定义
股票投资评级	买入	预计 6 个月内，股价表现优于市场指数 20%以上
	增持	预计 6 个月内，股价表现优于市场指数 10%-20%之间
	中性	预计 6 个月内，股价表现介于市场指数 ±10%之间
	卖出	预计 6 个月内，股价表现弱于市场指数 10%以上
行业投资评级	超配	预计 6 个月内，行业指数表现优于市场指数 10%以上
	中性	预计 6 个月内，行业指数表现介于市场指数 ±10%之间
	低配	预计 6 个月内，行业指数表现弱于市场指数 10%以上

分析师承诺

作者保证报告所采用的数据均来自合规渠道，分析逻辑基于本人的职业理解，通过合理判断并得出结论，力求客观、公正，结论不受任何第三方的授意、影响，特此声明。

风险提示

证券投资咨询业务的说明

本公司具备中国证监会核准的证券投资咨询业务资格。证券投资咨询业务是指取得监管部门颁发的相关资格的机构及其咨询人员为证券投资者或客户提供证券投资的相关信息、分析、预测或建议，并直接或间接收取服务费用的活动。

证券研究报告是证券投资咨询业务的一种基本形式，指证券公司、证券投资咨询机构对证券及证券相关产品的价值、市场走势或者相关影响因素进行分析，形成证券估值、投资评级等投资分析意见，制作证券研究报告，并向客户发布的行为。

国信证券经济研究所

深圳
深圳市罗湖区红岭中路 1012 号国信证券大厦 18 层
邮编：518001　总机：0755-82130833

上海
上海浦东民生路 1199 弄证大五道口广场 1 号楼 12 楼
邮编：200135

北京
北京西城区金融大街兴盛街 6 号国信证券 9 层
邮编：100032