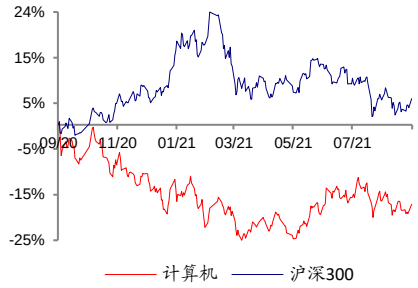
计算机行业

从法律法规细节和美国现状对比解析中国数据安全产业链

行业评级	买入
前次评级	买入
报告日期	2021-09-07

相对市场表现



核心观点：

- 2021 年 9 月 1 日《数据安全法》正式施行（资料来源：司法部官网），其在规范数据处理活动，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、安全和发展利益等方面有着重大意义。在对数据安全领域提出发展要求的同时，也为我国数据安全行业，特别是数据加密、隐私计算等细分领域带来了巨大的增量需求。
- 在 2021 年中国互联网大会数据安全论坛上，中国信息通信研究院安全所信息安全部主任魏薇表示，2020 年全球数据泄漏超过去 15 年总和，预测 2023 年中国数据安全行业市场规模有望达到 97.5 亿元，市场前景广阔（数据来源：信息安全与通信保密杂志社）。
- 从海外互联网巨头对数据安全的前沿布局、海内外多个初创公司布局数据安全，以及我国关于数据安全的明确立法，能看到数据安全是大势所趋。数据全流程防护包括访问、存储、流转、共享、计算等各个环节，国内头部公司已在早期有数据安全布局，有些公司在近期发布了数据安全产品。国内数据安全产业已有一定基础，并非从 0 到一，此前由于缺乏强制要求，发展是循序渐进，由于数据安全的相关立法等催化，数据安全产业有望进入从 1 到 10 的加速期。
- 美国大型互联网公司安全问题主要自行解决，在于其数据量庞大、业务量大（一旦有安全问题波及面广）、技术资金实力雄厚。非大型互联网公司的安全由第三方解决，第三方公司还是有非常广阔的市场空间。
- 海外没有出现过第三方接管、运营互联网公司数据的模式，是通过法律监管达到安全防护的目的。关于在国内是否会出现商业企业接管互联网公司数据，技术上上有较大挑战，能否通过其他方式达到强化监管的目的有待观察。原因在于：①互联网公司数据量巨大，现有安全公司没有能力和经验“托管”此类大型互联网公司的数据维护运营。②所有数据都需要加密不现实，加密和安全防护会导致业务系统时效性受影响，性能衰减。③若是由权威部门监管，网安公司按要求深入到互联网公司安全数据的运营层面，大概率也是混合而非完全依赖单一第三方。从产业技术的复杂性和整合来看，没有也不可能有一家公司能承担得了全部要求，正文所述的十几个领域各有各的优势。
- **相关标的：**绿盟科技、安恒信息、启明星辰、天融信、卫士通、奇安信、深信服、中孚信息。
- **风险提示：**网安行业下游客户仍以大型政企为主，政府等行业需求或会受财政支出波动影响。

相关研究：

计算机行业:Q2 增速环比减弱，龙头公司表现显著优于行业	2021-09-05
计算机行业:高成长性的结构性机会凸显	2021-09-05
计算机行业:北交所设立，市场相关方 IT 升级扩容在即，全面利好恒生电子等证券资管 IT 公司	2021-09-03

重点公司估值和财务分析表

股票简称	股票代码	货币	最新收盘价	最近报告日期	评级	合理价值（元/股）	EPS(元)		PE(x)		EV/EBITDA(x)		ROE(%)	
							2021E	2022E	2021E	2022E	2021E	2022E	2021E	2022E
安恒信息	688023.SH	CNY	329.72	2021/04/25	买入	381.09	2.69	3.87	122.57	85.20	718.34	183.64	10.70	13.30
绿盟科技	300369.SZ	CNY	18.19	2021/08/29	买入	24.40	0.46	0.60	39.54	30.32	36.40	29.76	9.40	11.00
启明星辰	002439.SZ	CNY	28.96	2021/08/13	买入	37.49	0.99	1.24	29.25	23.35	29.17	24.62	13.30	14.30
天融信	002212.SZ	CNY	17.27	2021/08/20	买入	25.10	0.57	0.78	30.30	22.14	23.93	18.17	6.60	8.20
深信服	300454.SZ	CNY	249.99	2021/08/20	买入	307.93	2.29	3.01	109.17	83.05	185.75	161.16	12.70	14.30
奇安信-U	688561.SH	CNY	90.45	2021/08/13	买入	120.75	-0.05	0.44	-1809.00	205.57	-339.62	512.26	-0.30	2.90

数据来源：Wind、广发证券发展研究中心

备注：表中估值指标按照最新收盘价计算

目录索引

图表索引

一、国内数据安全情况

（一）我国《数据安全法》对数据安全的全流程防护提出要求

2021年6月10日，第十三届全国人民代表大会常务委员会第二十九次会议通过了《中华人民共和国数据安全法》（以下简称《数据安全法》），并在2021年9月1日实施（资料来源：司法部官网）。

《数据安全法》在规范数据处理活动，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、安全和发展利益等方面有着重大意义。在对数据安全领域提出发展要求的同时，**也为我国数据安全行业，特别是数据加密、隐私计算等细分领域带来了巨大的增量需求**。

1.发展要求:

（1）国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。

（2）国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

（3）国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

（4）国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

2.技术需求:

《数据安全法》对数据全流程的防护都有相应要求，所需技术几乎涉及到了所有数据安全相关技术，根据《数据安全法》提出的要求，分析得到其所需的技术:

表1: 《数据安全法》与技术需求

法律原文	技术需求
第七条 国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。	明确数据是关键要素的属性，鼓励数据合法利用与自由流动，促进数据经济的发展。为实现该目标，可通过**联邦学习、安全多方计算、TEE** 等新兴技术方案解决数据流通与共享问题，同时满足数据安全需求，通过**区块链技术**可实现数据确权，数据流动和处理环节状态信息的安全记录。
第十六条 国家支持数据开发利用和数据安全技术研究，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。	数据安全技术包括**密码技术、数据脱敏、数据水印、数据防泄漏、访问控制和容灾备份**等关键技术，同时包括一些新兴技术，包括**同态加密、安全多方计算、联邦学习和区块链**等，需要做好创新技术的攻关。
第十八条 国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。	鼓励第三方开展数据安全评估与认证服务，涉及根据一些标准规范制定评估流程以及评估工具，比如**密码测评**、个人信息安全影响评估、App 个人信息收集的安全评估、基于数据安全能

	力成熟度模型的评估。
第二十七条 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。 重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。	明确指出除了依照法律法规外，还需“在网络安全等级保护制度的基础上”建立数据安全制度，即参照现行等级保护 2.0 系列国家标准。 等保 2.0 系列标准中与数据安全的相关技术将在下表中详细介绍。
第三十三条 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。	**身份认证**：利用身份认证技术实现交易双方身份审核； **区块链存证**：利用基于区块链的数据存证技术，将留存的审核、交易记录上链存储，防止数据丢失、篡改。
第三十五条 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。	**授权管理**：批准/授权国家机关对数据的调取权限； **访问控制**：对授权机关/人员在数据接入/调取过程的权限控制； **授权监管**：对授权机关/人员在数据调取、使用、销毁全流程的监管； **安全审计**：对授权机关/人员在数据调取全流程的操作行为审计。 如果审批手续为线上进行，潜在相关技术还包括： **身份认证技术**：手续批准环节对各审批人/报批人身份进行认证； **数字签名**：防止审批电子文件恶意篡改； **基于区块链的数据存证**：电子审批文件、记录的安全存证，便于时候安全审计。
第三十八条 国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。	除**数据加密传输、数据脱敏发布、差分隐私、安全多方计算、联邦学习技术**外，由于国家机关的特殊性，对数据的收集和使用更加严格，增加技术点包括： **访问控制**：对数据的接入和使用人员进行授权访问控制； **数据安全销毁**：国家机关收集、使用数据时，考虑到移动介质传输场景，传输完毕后需保证传输介质中的数据不可恢复； **安全审计**：需要对数据全生命周期内的访问、处理活动进行记录并安全审计。
第四十条 国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。	**数据加密存储：**保护重要数据存储过程安全； **数据加密传输：**保护数据向他人提供时的传输安全； **访问控制：**保护电子政务系统维护、数据存储、加工等过程对数据的访问安全； **身份认证：**系统维护、数据存储、数据加工时对数据访问人员的身份识别； **数据安全销毁：**重要数据在移动介质传输完毕后移动介质中的数据安全销毁、数据接收方数据使用完毕后接收方本地存储的安全销毁； **授权监管：**数据存储、加工、提供、使用、接收等处理行为的授权处理和以上行为动作的监督；

	安全多方计算：可实现安全的数据加工； **联邦学习：**可实现安全的数据加工和共享； **安全审计：**对数据生命周期内的数据存储、访问、加工、提供、接收、授权等所有相关操作行为的日志记录和事后安全审计，并可结合区块链技术实现操作记录的不可篡改性。
第四十一条 国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据。依法不予公开的除外。	**数据脱敏：**保证数据公开时，无法将公开数据映射到具体的某个人或组织； **差分隐私：**数据公开时，可保证在受到差分查询攻击时，不会造成数据泄露。
第四十二条 国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。	**资源目录安全：**保护由不同机构联合构建的资源目录的安全性； **安全多方计算：**保护不同机构数据做联合查询时的查询过程安全； **身份认证：**识别政务数据开放平台数据维护、访问过程操作人员的真实身份； **访问控制：**保护政务数据开放平台数据维护、访问过程的安全可控； **授权监管：**保证政务数据开放平台数据维护过程、重要数据访问过程的授权和安全监管； **安全审计：**保证政务数据开放平台数据维护过程、重要数据访问过程的可审计性，并可结合区块链技术实现操作记录的不可篡改性。

数据来源：司法部官网，绿盟科技公众号，广发证券发展研究中心

（二）主流数据安全技术

总结数据安全防护的全流程技术，涉及到的环节包括数据的访问、存储与传输、审计与监管、加工与共享过程、隐私计算、可信执行环境等环节，各个环节可细分出不同的技术点。

1.数据访问：

身份认证：对数据访问人员的身份识别；

访问控制：在数据访问过程中对访问人员进行权限控制；

授权管理：批准/授权访问人员对数据的调取权限。

2.数据存储与传输：

数据加密存储：保护重要数据存储过程安全；

数据加密传输：数据采集和共享使用阶段，可采取加密传输的方式保证数据在网络

传输时的安全;

数据安全销毁：重要数据在移动介质传输完毕后移动介质中的数据安全销毁、数据接收方数据使用完毕后接收方本地存储的安全销毁。

3.数据审计与监管:

区块链存证：利用基于区块链的数据存证技术，将留存的数据访问，使用等操作记录上链存储，防止数据丢失、篡改。

安全审计：对数据生命周期内的数据存储、访问、加工、提供、接收、授权等所有相关操作行为的日志记录和事后安全审计，并可结合区块链技术实现操作记录的不可篡改性。

4.数据加工与共享:

差分隐私：数据公开时，可保证在受到差分查询攻击时，不会造成数据泄露;

数据脱敏：保证数据公开时，无法将公开数据映射到具体的某个人或组织;

联邦学习：保证各方数据不出本地安全域前提下，实现安全的数据加工和共享;

安全多方计算：保证各方数据保密性前提下，保护不同机构数据做联合查询时的查询过程安全。

5.隐私计算:

在数据处理过程中，**隐私计算**的重要性日益凸显。隐私计算使企业在数据合规要求前提下，能够充分调动数据资源拥有方、使用方、运营方、监管方各方主体积极性，实现数据资源海量汇聚、交易和流通，从而盘活第三方机构数据资源价值，促进数据要素的市场化配置，在《数据安全法》颁布的背景下，隐私计算更凸显价值，其基本的技术有:

（1）多方安全计算

多方安全计算是指，在无可信第三方的情况下，多个参与方协同计算一个约定的函数，并且保证每一方仅获取自己的计算结果，无法通过计算过程中的交互数据推测出其他任意一方的输入和输出数据，其包含6种基本技术理论:

① 同态承诺

同态承诺是一种允许一个人向其他人提交任何选定数值而又不泄露该值的密码协议，承诺提交后不能更改，且事后可公开验证。同态承诺允许在提交的承诺上进行计算而不失去承诺的保密、不可更改及事后可验证的特征。

② 同态加密

同态加密是各参与者将自己的输入加密后一起发给某计算服务器，服务器直接在密文上进行计算，计算后将得到的结果的密文发送给指定结果方，结果方再将结果的密文解密，即可得到最终的计算结果。这样，计算服务器一直在密文上操作，无法看到任何有效信息，而参与者也只拿到最后的结果，看不到中间结果。

③ 秘密分享

秘密分享的基本思想是将数据切割成多份，并分发给不同的参与者，每个参与者持有其中一份，协作完成计算任务（比如加法、乘法运算）。因为参与者看不到数据全量信息，从而实现数据隐私保护。

④ 混淆电路

混淆电路的基本思想是将计算电路的每个门都加密并打乱，保证计算过程中不会泄露原始输入和中间结果。双方根据各自输入依次进行计算、解密方可得到唯一的正确结果，无法得到结果以外的其他信息，从而实现双方安全计算。

⑤ 不经意传输

不经意传输是一种可保护隐私的双方通信协议，能使通信双方以一种选择模糊化的方式传送消息。不经意传输协议是密码学的一个基本协议，它使得服务的接收方以不经意的方式得到服务发送方输入的某些消息，这样就可以保护接受者的隐私不被发送者所知道。S每次发送2个信息m0和m1，而R每次输入一个选择b。当协议结束的时候，S无法获得关于b的任何有价值的信息，而R只能获得mb，对于m1−b，R也一无所知。

⑥ 零知识证明

零知识证明是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完成一项任务所需采取的一系列步骤。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。

（2）联邦学习

联邦学习是一种分布式机器学习技术和系统，包括两个或多个参与方，这些参与方通过安全的算法协议进行联合机器学习，可以在各方数据不出本地的情况下，通过交换中间数据的形式，联合建模和提供模型推理与预测服务。

（3）差分隐私

差分隐私是指，通过使用随机噪声来确保，查询请求公开可见信息的结果，并不会泄露个体的隐私信息，即提供一种当从统计数据库查询时，最大化数据查询的准确性，同时最大限度减少识别其记录的机会，简单来说，就是保留统计学特征的前提下去除个体特征以保护用户隐私。

6.可信执行环境

可信执行环境是指，计算平台上由软硬件方法构建的一个安全区域，可保证在安全区域内部加载的代码和数据在机密性和完整性方面得到保护。其目标是确保一个任务按照预期执行，保证初始状态的机密性、完整性，以及运行时状态的机密性、完整性，可分为：

（1）可信硬件

TEE/SGX: SGX的保护是针对应用程序的地址空间的。SGX利用处理器提供的指令，在内存中划分处一部分区域（EPC）并将应用程序地址空间中的Enclave映射到这部分内存区域。这部分内存区域是加密的，通过CPU中的内存控制单元进行加密和地址转化。

TrustZone: TrustZone 是为消费电子产品构建一个安全框架来抵御各种可能的攻击，在概念上将SoC的硬件和软件资源划分为安全(Secure World)和非安全(Normal World)两个世界，所有需要保密的操作在安全世界执行（如指纹识别、密码处理、数据加解密、安全认证等），其余操作在非安全世界执行（如用户操作系统、各种应用程序等）。

（2）可信环境

安全屋: 安全屋主要是通过物理方式对数据的所有权和使用权进行分离，通常使用中心化和分布式相结合的混合架构，即各个数据提供方按照主控平台的接入规范统一接入平台，而所有管理权限由主控平台统一提供，各个参与的数据源方提供数据区的维护能力，通过这种方式来确保数据的整个流通过程安全可控的一种技术方案。

安全沙箱: 安全沙箱是指利用操作系统提供的技术，对外所建立的一道屏蔽“墙”，墙内屏蔽系统权限只做具体的处理，并通过IPC(进程间通讯协议)传递消息。

（三）国内数据安全公司布局

头部公司普遍已在数据安全领域有所布局，亦有一些初创公司专攻新型细分领域，但由于之前对数据安全没有明确法律要求，国内安全公司有关数据安全的收入普遍较少。7月14日，在2021年中国互联网大会数据安全论坛上，中国信息通信研究院安全所信息安全部主任魏薇表示，2020年全球数据泄漏超过去15年总和，她预测

2023年中国数据安全行业市场规模有望达到97.5亿元，数据安全市场前景广阔（数据来源：信息安全与通信保密杂志社）。

安恒信息专注于网络信息安全领域，逐步拓展数据安全产品线。2021年4月，公司发布AiGuard数据安全产品，包括风险核查、数据梳理、数据保护、监控预警等功能，对数据资源行为活动的整个生命周期提供全天候全方位的感知保护。2021年5月，公司发布AiLand数据安全岛平台，是一个致力于保障数据安全流通，解决数据共享过程中的安全、信任和隐私保护问题的隐私计算平台。公司的AiLand产品切入到数据安全中最前沿的隐私计算领域，结合联邦学习、区块链、密文计算等技术，可用于人工智能模型的训练过程中，具有很好的应用前景。我们认为公司在网络安全领域积累的技术和客户有利于AiGuard和AiLand两款数据安全产品的推广，在数据安全业务上的产品布局紧跟技术和市场发展趋势，前景向好。

图1：安恒信息AiLand数据安全岛平台

数据来源：安恒信息官网，广发证券发展研究中心

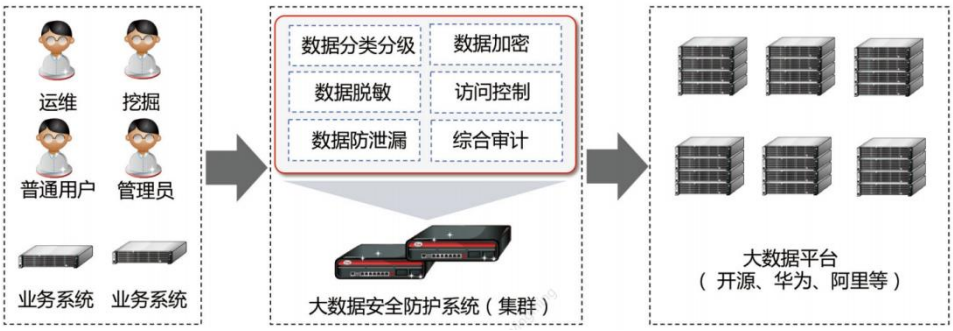
绿盟科技的全资子公司亿赛通拥有完整的数据安全产品矩阵，产品协同力强。亿赛通于2009年就开发出了核心产品数据泄露防护软件，服务于包括政府、部队、企业组织等一万多家的签约用户和600多万的终端用户。目前，公司已形成包括审计检测类、加密防护类、安全管理类和安全平台类完整的数据安全产品矩阵。具体包括：1、审计检测类产品可实时监控系统中潜在威胁，并实时报警；2、加密防护类产品可从云、网、端三层为需要保护的数据进行加密；3、安全管理类产品采用软硬件一体化方式，对各类网络数据、安全产品进行统一管理。公司的安全平台可将产品和资源统一管理，整合各产品功能，形成协同防护能力。

启明星辰拥有完整的数据安全底层能力组件，可实现产品的快速开发。公司拥有包括数据库审计、加密、脱敏、防泄漏、运维网关等多项底层能力组件。公司在针对特定场景的定制化产品开发方面具有一定优势，其产品已广泛应用于工业制造、电

信运营等领域。此外，公司正致力于采用智能化手段实现数据全生命周期的自适应管理，预计将有效提升产品毛利率。数据安全治理平台对数据的采集、存储、传输、共享、销毁等进行了全面的管控，实现了敏感数据自动发现与分级分类管理、数据风险态势中心、数据安全运营等功能。公司在数据安全领域技术积淀深厚，紧跟行业前沿技术，产品具有很强竞争力。

天融信在大数据安全防护领域的布局较早，具有先发优势。天融信在数据安全领域的产品线较为完整，包括数据防泄漏系统、数据安全智能管控平台、数据安全交换平台等。产品已经实现了一定程度智能化，例如在数据防泄漏系统中增加了OCR识别功能，增强了对于图片、视频等非结构化数据的识别。此外，公司在大数据领域精心布局。其开发的大数据安全防护系统具备数据分类分级、加密、脱敏、防泄漏等功能，能够为大数据提供全生命周期的安全防护。目前大数据市场正快速成长，我们认为天融信在大数据防护领域取得一定先发优势，已应用于金融、政府、能源、卫生、海关等多个领域。

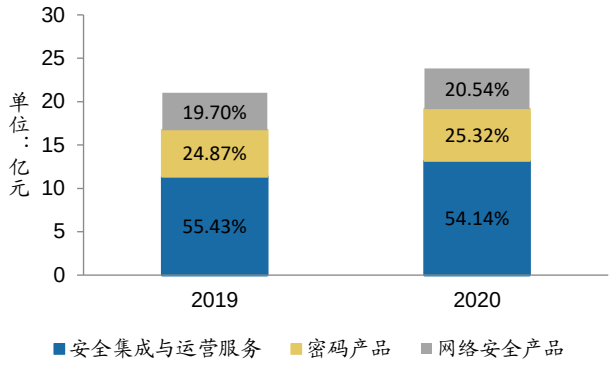
图2：天融信大数据安全防护系统



数据来源：天融信官网，广发证券发展研究中心

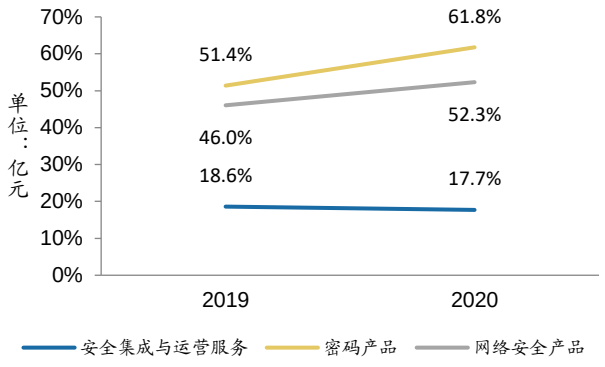
卫士通深耕数据安全和加密领域超过20年，技术沉淀深厚、渠道分布广阔。卫士通于1998年由中国电子科技集团公司发起，已形成网络安全、数据安全、加密服务完整的信息安全产品体系。公司的核心数据安全产品是密码产品，包括密码模块、密码机和基础设施。密码模块有智能密码钥匙和商用PCI-E密码卡；密码机有服务器密码机、签名验签服务器；基础设施有密钥管理系统、数据证书认证系统。公司的密码产品2020年营收5.9亿元，同比增加11.3%，占营收的比重为24.9%。2020年公司密码产品的毛利率为61.8%，同比提升10.4个百分点。

图3：2019-2020年卫士通分产品营收



数据来源：Wind，广发证券发展研究中心

图4：2019-2020年卫士通分产品毛利率



数据来源：Wind，广发证券发展研究中心

奇安信构建以零信任为基础的数据安全产品，注重数据共享环节的安全性。零信任是信息安全领域的前沿理念，指的是数据、网络、系统等采取零信任的方式来防护无法明确身份的外部人员。基于此理念，奇安信构建了完整的基础架构，开发出了完整的数据安全产品，具体包括数据安全交易沙箱、数据防泄漏、源代码安全、APP隐私合规、电子数据取证等。奇安信的产品在数据交换和共享环节提供的产品较多。2020年9月，公司发布的数据安全交易沙箱，采用了安全分离学习技术，数据分析师只能带走不含敏感数据的分析模型和结果，确保了敏感数据的安全性。

图5：奇安信数据交易安全沙箱

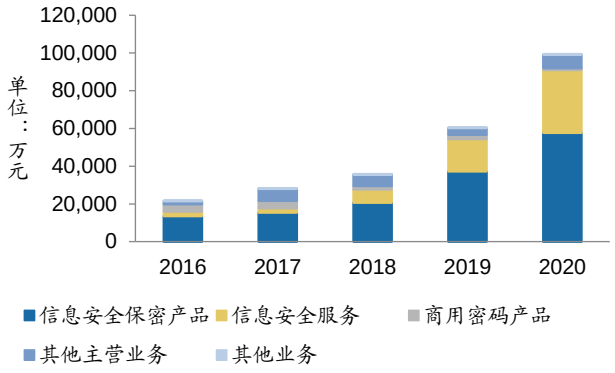
数据来源：奇安信官网，广发证券发展研究中心

深信服数据安全产品以数据库安全审计系统为主。公司已构建了覆盖云、网、端各层面的安全防护技术架构。公司的数据安全产品是整体信息安全架构中重要的一环，满足用户实时监测数据安全威胁、及时发现内网数据安全隐患等需求。公司在数据

安全领域的产品主要是数据库安全审计系统DAS（Database Security Audit System）。DAS将数据安全防护与大数据分析结合，为用户提供完整的数据库审计分析、泄密轨迹分析、数据库访问关系可视、数据库攻击威胁分析。DAS目前已应用于地产、媒体等多个领域。未来，公司在完整的信息安全架构下，将逐渐拓展数据安全产品品类。

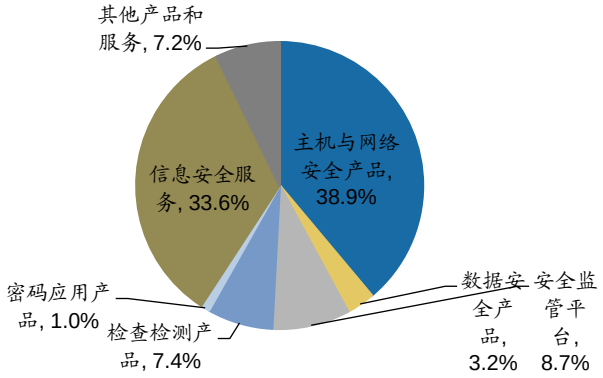
中孚信息数据安全产品品类逐渐扩展，未来向智能化方向发展。公司着力打造信息安全、人工智能和大数据技术深度融合的特色优势。公司的数据安全产品采用数据加密、数据保护、数据管控等技术，实现敏感数据的防泄漏、防窃取、可追溯。公司目前的数据安全产品主要有电子文件密级标志管理系统、文档发文信息隐写溯源系统、数据泄露防护系统等。2020年，公司的数据安全产品营收3174万元，占公司总营收3.2%，主要客户为政府部门。未来公司将重点提升产品智能化水平，包括感知、理解、预测及判断等能力在数据安全产品中应用。

图6：2016-2020年中孚信息分产品收入



数据来源：Wind，广发证券发展研究中心

图7：2020年中孚信息分产品收入份额



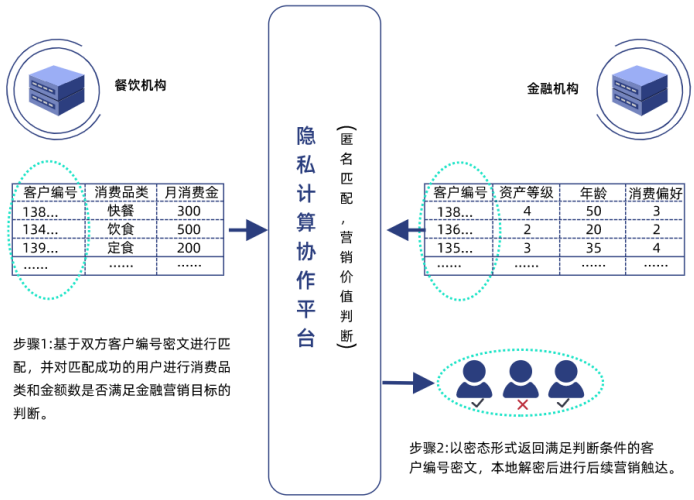
数据来源：Wind，广发证券发展研究中心

富数科技成立于2016年，专注于联邦学习、安全多方计算等加密计算科技领域。公司的FMPC安全多方计算产品支持私有化部署，通过秘密共享，混淆电路，同态加密等多种技术，实现安全多方求交、安全统计、安全矩阵运算等多种算子。公司在密码学和机器学习领域拥有多项自主技术,已经应用于金融、政务、医疗等领域，帮助客户提高智能风控、营销和运营的效率。

矩阵元成立于2014年，专注于密码学、计算复杂性理论、分布式计算等领域。公司目前有超过110名员工，获得融资总额超过1.5亿元。公司在隐私计算领域开发的产品较多，包括：1）PSI隐私交集：通过隐私求交集与隐私联合查询，实现两家机构的客群重合度匹配与客户是否达到营销价值的判断结果；2）PCSBox隐私计算沙盒：实现集存储、加密、计算、认证的全数据链隐私保护；3）RossetaFlow隐私AI平台：用户可以在保证隐私的前提下训练高性能AI模型。公司提供隐私计算、数据安全、

人工智能等软硬一体化的解决方案，已经为企业、机构、政府等各类客户提供服务。

图8：矩阵元PCSBox隐私计算协作平台



数据来源：矩阵元官网，广发证券发展研究中心

数牍科技成立于2019年，公司团队在数据科学工程、AI、密码学等前沿技术研发和工程落地方面都具有丰富经验。由于公司发展历史较短，目前在数据安全方面主要推出两款产品：1）基于融合秘密共享、模糊传输、同态加密等技术的多方安全计算系统；2）在加密机制下完成数据交换，并协同模型训练与预测的联邦学习和预测系统。该系统确保了在多系统的数据协作训练过程中无需传输原始数据，防止数据泄露。公司的客户包括政府机构、央企、国企及大型互联网企业。

翼方健数成立于2016年，以隐私安全计算为核心，在数据安全和个人隐私保护基础上的数据开放生态和数据共享协作环境，并在此基础上发展人工智能的能力，为行业赋能。公司开发的翼数坊产品在数据安全、授权使用和隐私保护下提供了数据采集、清洗、分析、应用的数据全生命周期管理，为科研协作提供一站式服务，大大地提高了科研效率。公司目前的客户来自于医疗、金融、政务等行业。

表2：国内数据安全公司对比

公司	数据安全业务发展重点	产品
安恒信息	数据安全产品布局紧跟市场和技术趋势，目前有隐私计算平台和数据监控预警等产品	1.数据安全岛平台（可用于 AI 数据训练的隐私计算平台） 2.数据智能安全平台 3.数据安全管控平台 4.数据安全分级与风险评估系统 5.零信任身份服务中心
绿盟科技	其全资子公司亿赛通已经形成完整的数据安全产品矩阵，各产品间的协同力较强	1.绿盟数据脱敏系统 DMS 2.敏感数据发现与风险评估系统 IDR 3.绿盟数据库审计系统 DAS 4.数据安全运营平台 5.绿盟数据泄露防护系统 DLP
启明星辰	公司已形成完整的数据安全底层组件，可实现定制化产品的快速开发；未来也计划将产品智能化升级	1.数据防泄漏系统 2.数据库审计与防护 3.数据库动态/静态脱敏 4.数据库防火墙 5.文档加密 6.电子签章
天融信	公司已将人工智能技术应用到数据安全产品中；公司重点布局大数据领域的数据安全产品	1.终端/网络数据防泄漏系统 2.数据安全智能管控平台 3.数据安全交换平台系统 4.数据库安全网关 5.备份一体机
奇安信	重点布局数据共享环节的安全防护	1.数据安全交换平台 2.数据升级与防护系统 3.数据库漏洞扫描系统 4.数据脱敏系统 5.运维安全管理与审计系统 6.数据交易沙箱
卫士通	以加密为核心的数据安全产品，提供软硬件一体的加密产品	1.数据脱敏平台 2.电子文件密级标志管理系统 3.金融数据密码机 4.数字证书认真系统 5.秘钥管理系统 6.移动终端密码软卡
中孚信息	公司现有数据安全产品品类较少，未来公司将重点提升产品智能化水平	1.电子文件密级标志管理系统 2.电子文档安全管理系统 3.智能辅助定密管理系统 4.文档发文信息隐写溯源系统 5.数据泄露防护系统 6.数据安全行业监管方案

数据来源：各公司官网，广发证券发展研究中心整理

二、海外数据安全情况

（一）欧美相关法律规定

1.欧盟《通用数据规则》（GDPR）

GDPR的目的是为了保护个人隐私，尤其是针对当前互联网公司利用大数据侵犯个人隐私的行为。也就是说，GDPR保护的仅是“个人数据”（personal data），不涉及个人数据以外的其他数据。对于公司，GDPR提出以下义务:

（1）通过设计以默认方式保护数据的义务

（2）记录处理活动的义务

（3）与监管部门合作的义务

（4）确保处理安全的义务

（5）个人数据泄露的通知义务

（6）开展数据保护影响评估的义务

（7）设立数据保护官的义务

如果公司不符合GDPR的规定，则将面临上限一千万欧元，或全球年营业额的2%的罚款，具体包括:

（1）没有默认采用隐私保护设计

（2）安全防护措施不当

（3）未执行数据保护评估等

(资料来源：卫士通官方公众号)

2.《加利福尼亚消费者隐私法案》

《加利福利亚消费者隐私法案》（CCPA）是继GDPR以来又一具有全球影响力的个人信息保护法案，它对消费者隐私的保护有着严格的规定，如:

如果任何消费者的未加密或未经处理的个人信息，由于经营者违反义务、未实施和采取合理安全程序以及未采取与信息性质相符的措施来保护个人信息，从而遭受了未经授权的访问和泄露、盗窃或披露，则消费者可为以下任何一项请求而提起民事诉讼:

（1）赔偿每起事件每个消费者不少于一百美元（100美元）且不超过七百五十美元（750美元）的损害赔偿金或实际损害赔偿金，以数额较大者为准;

（2）申请禁止令或确认性法律救济;

（3）法院认为适当的任何其他救济。

（资料来源：中国信息安全公众号）

表3：中国与欧美相关法律处罚对比

法律	处罚
《中华人民共和国个人信息保护法》	对于违法的个人信息处理行为中情节严重的，除没收违法所得，还可以并处五千万元以下或者上一年度营业额百分之五以下罚款，并责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照； 同时，对于直接负责的主管人员和其他直接责任人员不仅要给予罚款，还可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。有个人信息保护法规定的违法行为的，还将按照法律、行政法规的规定记入信用档案，予以公示。
《中华人民共和国数据安全法》	不履行规定保护义务：责令改正和警告，给予单位 5 万至 50 万元罚款，给予负责人 1 万至 10 万元罚款；拒不改正或造成大量数据泄漏等严重后果的，给予单位 50 万至 200 万元罚款，最高责令吊销相关业务许可证或者吊销营业执照，给予负责人 5 万至 20 万元罚款； 危害国家安全和损害合法权益的：给予 200 万至 1000 万元罚款，责令停业整顿、吊销相关业务许可证或者吊销营业执照，构成犯罪的，追究刑事责任； 向境外提供重要数据的：由有关主管部门责令改正，给予警告，可以并处 10 万至 100 万元罚款，对直接负责的主管人员和其他直接责任人员可以处 1 万至 10 万元罚款。情节严重的，给予 100 万至 1000 万元罚款，责令停业整顿、吊销相关业务许可证或者吊销营业执照，对负责人给予 10 万至 100 万元罚款。
欧盟《通用数据规则》（GDPR）	GDPR 未规定刑事责任，但允许成员国对违反法规和适用国家法规的行为施加刑事处罚。 行政处罚：最高处以 2000 万欧元的罚款，或企业全球年度营业额的 4％。 民事救济。
《加利福尼亚消费者隐私法案》（CCPA）	行政处罚：对于每次违反处以不高于 2500 美金的处罚；对于每次故意违反处以不高于 7500 美金的处罚； 民事救济：个人仅在数据泄露时可以就安全措施不完善提起民事诉讼。

数据来源：司法部《中华人民共和国个人信息保护法》全文，司法部《中华人民共和国数据安全法》全文，卫士通官方公众号，中国信息安全公众号，广发证券发展研究中心

（二）美国大型互联网公司的数据安全自行解决

大型互联网公司由于数据量大、业务重要、自己技术、资金实力强，自身的业务安全主要由自身保障。以下列举一些知名互联网公司的网络安全布局。

谷歌：如2019年3月5日，从Google X中分拆出的信息安全业务、Alphabet旗下Chronicle本周发布了首款商用产品:一个名为Backstory的信息安全数据平台（资料来源：36氪）。2019年8月谷歌是网安领域的技术先导，如其开源了Private Join and Compute项目，这是一种新的安全多方计算（MPC）工具（资料来源：巴比特网）。2020年7月谷歌云（Google Cloud）推出了一款“可保密虚拟机”(Confidential VMs)。这种新型的虚拟机可以利用谷歌的加密计算，实现对静止状态和内存内数据的保密（资料来源：Phala可信网络公众号）。

微软：2021年1月，微软宣布2020年安全业务创造了100亿美元，获得超40%的年增长率。微软每年要花费10亿美元来更新现代化设施、创建新的产品安全团队。全球有超过120个国家和地区的400000用户使用微软安全解决方案，90家财富百强企业

使用微软至少4种以上安全解决方案（资料来源：比特网）。

亚马逊：19年1月，亚马逊作为ExNow战略合作伙伴，将共同推进网络安全建设。亚马逊与ExNow（全球区块链资产交易平台）联合推进拟态安全等虚拟化异构安全体系、可信计算体系等技术体系架构创新应用，打通基础研究和技术创新衔接的绿色通道，力争以基础研究带动应用技术群体突破（数据来源：Exnow区块链百度百家号）。

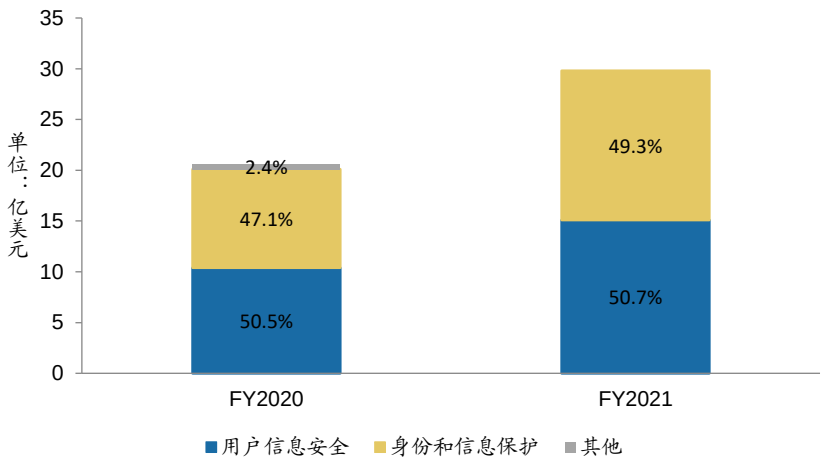
（三）美国数据安全公司情况

NortonLifeLock原名为赛门铁克，是美国著名的信息安全提供商。在标准化的病毒防护软件的基础上，公司新增远程管理、数据过滤、VPN、数据安全等多项功能，持续更新产品，拓展业务线。公司在个人隐私数据防护方面的产品线也较为完整，提供身份认证、入侵监测与预警、隐私数据防泄露等产品。公司2021财年中，身份和信息保护业务收入14.7亿美元，同比增加51.5%，占比达到49%。

NortonLifeLock目前总市值159亿美元，PS（TTM）是5倍（2021年9月5日），NortonLifeLock曾是知名老牌安全厂商，但是经过一系列收并购，整合效果并不佳，近3年来收入几乎无增长，利润波动幅度巨大，产品创新上亦无突出表现。

美股安全公司的估值与其产品所处赛道、商业模式、创新能力、以及财务表现（收入增速等指标）等综合因素有关，估值分化差异非常大。

图9：NortonLifeLock公司分产品业务收入



数据来源：Wind，广发证券发展研究中心

McAfee公司的产品以C端和B端的杀毒软件为主。公司于2010年被英特尔以76.8亿美元的价格收购，收购完成后，McAfee以全资子公司继续营运。公司的数据安全功能是融合在既有的杀毒软件中的，以C端的杀毒软件来看，其推出的“Total Protection”

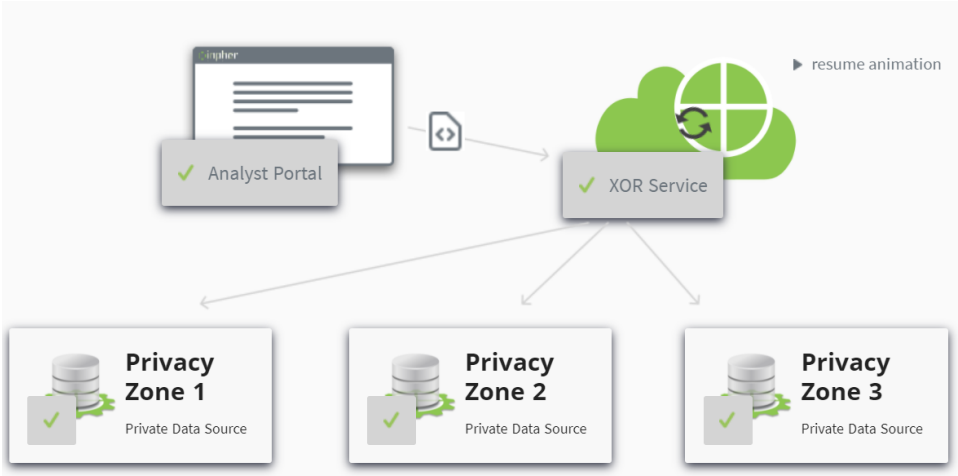
和“LiveSafe”两项功能提供设备安全性、在线隐私和互联网身份保护等功能。在未来的发展战略中，公司也将数据安全作为重点发展领域，未来计划推出云端、企业端和多设备端的数据安全产品。

McAfee总市值120亿美金，PS（TTM）是3倍（2021年9月5日）。McAfee一直专注于防病毒软件，一直没有拓展业务边界，近2年收入增速在10%左右，增速与美国网安行业增速持平，仍处于亏损阶段。

Cape Privacy公司成立于2018年，专注于密码学、机器学习、数据科学和软件工程等领域。公司已经推出的加密学习平台，针对于多数据源的机器学习场景，实现了模型训练的同时防止了原始数据的泄露。公司开发的加密学习平台兼容市场上主流的机器学习工具，包括Python和Docker。公司的数据安全产品已应用于金融、政府以及医疗领域。

Inpher公司成立于2015年，目前有29名员工，已募资1400万美元。公司专注于隐私计算领域。公司开发的XOR隐私计算平台，实现了在保护各方数据隐私的前提下进行人工智能模型的数据训练。公司的产品在政府、金融、医疗领域已经广泛应用。

图10：Inpher公司的XOR隐私计算平台



数据来源：Inpher 官网，广发证券发展研究中心

Zama公司专注于同态加密技术，即在数据检索、存储、运算过程中保持数据的加密形态，确保数据提供方数据的安全性。公司推出的Concrete平台，解决了同态加密技术中多项技术难题，例如容错学习问题和容错环式学习问题。公司的创始人Pascal在同态加密技术领域研究了25年，具有很强的技术能力。公司目前有26名员工，其中16位为博士。我们认为公司在同态加密领域具有很强的技术壁垒，技术竞争力较强。

Sharemind公司提供隐私计算软硬件解决方案。公司开发的多方计算平台提供了全面完整的隐私计算算法及API，方便研发人员进行相关应用软件的开发。此外，公司还开发了专用于数据安全的服务器，从硬件层创建了可信任执行环境，保障数据的安全性。

Baffle公司在加密技术、密码学具有深厚技术积淀，在其应用于存储和企业基础架构设计方面具有一定经验。公司在数据安全领域的产品线较为完整，包括数据库加密、云平台数据加密、数据分享加密及动态数据加密等。此外，公司针对于Snowflake和AWS等主流云平台提供定制化的数据安全产品。

Secata公司在多平台应用隐私计算具有一定优势。公司开发的隐私计算产品可以搭载于本地服务器、云端还有区块链端。公司的特色产品是隐私区块链平台，有效保障上链数据的安全性。公司的产品已经应用于丹麦统计局和医疗健康数据中心。

表4：国外数据安全公司对比

公司	领域	产品	产品形态	主要客户
NortonLifeLock	数据防泄漏	公司拥有包括身份认证、入侵监测与预警、隐私数据防泄露等完整的数据安全产品，2020 年收入占比 49%	标准化和定制化的软件	C 端和 B 端的客户
McAfee	数据防泄漏	公司的数据安全产品是以功能的形式嵌入在杀毒软件中的，未来计划推出面向云端、企业端的专用数据安全产品	嵌入在个人杀毒软件中的功能	C 端和 B 端的客户
Cape Privacy	隐私计算	针对多源数据机器学习场景，提供模型训练时隐私数据防护服务	平台类产品	政府、金融、医疗等领域
Inpher	隐私计算	在保护各方数据隐私的前提下进行人工智能模型的数据训练的多方计算平台	平台类产品	政府、金融、医疗领域
Zama	同态加密	Concrete 同态加密平台，可以保障数据在检索、存储、运算过程中的安全性	平台类产品	政府、金融
Sharemind	隐私计算	提供数据安全软硬件一体化的解决方案：Sharemind MPC 多方计算平台和 Sharemind HI 数据安全服务器	平台类软硬件产品	政府、金融
Baffle	数据加密	公司关于数据加密产品线较全面，包括数据库加密、云平台数据加密、数据分享加密及动态数据加密等产品	应用类和平台类产品	政府、金融
Secata	隐私计算	公司推出的隐私区块链平台保障上链数据的安全	应用类和平台类产品	政府、金融

数据来源：各公司官网，广发证券发展研究中心整理

三、国内数据安全产业发展的结论

1. 数据安全是大势所趋

从海外互联网巨头对数据安全的前沿布局、海内外多个初创公司布局数据安全，以及我国关于数据安全的明确立法，能看到数据安全是大势所趋。数据全流程防护包括访问、存储、流转、共享、计算等各个环节，国内头部公司已在早期有数据安全布局，有些公司在近期发布了数据安全产品。国内数据安全产业已有一定基础，并非从0到一，此前由于缺乏强制要求，发展是循序渐进，由于数据安全的相关立法等催化，数据安全产业有望进入从1到10的加速期。

2. 参考美国经验，大型互联网公司安全问题主要自行解决

美国大型互联网公司安全问题主要自行解决，在于其数据量庞大、业务承载量大（一旦有安全问题波及面广）、技术资金实力雄厚。非大型互联网公司的安全还是要由第三方解决，第三方公司还是有非常广阔的市场空间。

3. 参考海外，互联网公司的安全数据交由第三方商业企业接管技术上挑战较大

海外没有出现过第三方接管、运营互联网公司数据的模式，是通过法律监管达到安全防护的目的。关于在国内是否会出现商业企业接管互联网公司数据，我们的看法是，技术上上有较大挑战，能否通过其他方式达到强化监管的目的有待观察。原因在于:

（1）互联网公司数据量巨大，现有安全公司没有能力和经验“托管”此类大型互联网公司的数据维护运营。如2020年4月，美团自研的OCTO数据中心日均处理万亿级数据量（资料来源：美团技术团队）。2019年10月，滴滴旗下小桔车服车联网业务负责人黄智信表示，滴滴大概每天处理超过106TB的轨迹数据，4875TB的综合数据，滴滴整体数据量更为庞大（资料来源：科技观察猿）。2020年京东618期间，京东云的系统面对数百亿访问流量、每秒数百万次的高并发请求、数十亿的实时消息推送（资料来源：京东科技官网）。

（2）所有数据都需要加密不现实，加密和安全防护会导致业务系统时效性受影响，性能衰减。

（3）若是由权威部门监管，网安公司按要求深入到互联网公司安全数据的运营层面，大概率也是混合而非完全依赖单一第三方。从产业技术的复杂性和整合来看，没有也不可能有一家公司能承担得了全部要求，正文所述的十几个领域各有各的优势。单纯从要求互联网服务商从用户的敏感数据隔离开的角度看，也有多个环节需要涉入。