计算机应用

数据安全政策密集发布，千亿产业爆发拐点已至

车联网、工业及电信领域数据安全政策持续落地，进一步催化产业爆发。1）2021 年 9 月 15 日，工信部发布《关于加强车联网网络安全和数据安全工作的通知》，2021 年世界互联网大会，特斯拉也重点展示其数据架构和数据安全内容。随着自动驾驶、物联网等技术的快速应用，车联网日渐成为车企竞争焦点，与此同时，由于技术本身存在风险性，以及行业标准规范滞后缺失，网络安全及数据安全威胁也愈发凸显，政策细化有望加快落地节奏；2）2021 年 9 月 30 日，为提升工业、电信行业数据安全保护能力，防范数据安全风险，工信部发布《工业和信息化领域数据安全管理办法(试行)(征求意见稿)》。推动数据敏感企业建立数据全生命周期安全管理制度，针对不同级别数据，明确制定数据收集、存储、使用、加工、传输、提供、公开等环节的具体分级防护要求和操作规程。

除互联网厂商外，医疗、金融、能源等关保行业数据安全潜在空间巨大。企业侧数据安全需求巨大、有望爆发：1）金融数据天然具有商业价值，需加强监管。通过分析金融交易相关“敏感个人信息”总结、归纳、演绎后得到的“衍生个人信息”，对于风控及业务价值巨大；2）智能医疗设备供应商将收集越来越多样化的数据，其使用必将面临强监管，随实体医院将诊疗活动延伸至互联网端，数据流通成业务刚需，关乎患者隐私、种类繁多的医疗数据也迫切需求安全监管；3）以自动驾驶为代表的 AI 技术日益普及，汽车数据处理量级及能力日益增强，汽车数据依法合理有效利用同时维护了国家安全利益与个人合法权益。

监管政策加码与大数据加速应用驱动数据安全发展，短期百亿市场以技术服务收入为主，长期 SAAS 运营收入有望达千亿。近期《数据安全法》、《关保条例》、《个人信息保护法》等法律法规密集发布并实施，仅从数据安全的组成部分隐私计算来看，据 Gartner 预测，2023 年，全球 80%以上的公司将面临至少一项以隐私为重点的数据保护法规，2024 年隐私驱动的数据保护和合规技术支出将在全球突破 150 亿美元。随《数据安全法》等落地、数据交易市场快速发展，KPMG 预计 2023 年国内数据安全技术服务有望达百亿,随 IT 架构走向云化，长期将撬动千亿级的数据安全 SaaS 运营收入。

竞争格局：典型的数据安全应用场景通常包含三类参与方，互联网作为数据使用方，相关部门作为监管方，具备良好政治素养、技术储备的第三方企业提供技术服务。以隐私计算场景为例：（1）数据的使用方，需考虑业务特征与支付能力，互联网厂商合规需求迫切，未来数据“最小化采集、避免滥用”，此外如联合建模下的银行业、医疗机构；（2）作为数据的提供方，做到原始数据不出本地，将加密后的信息发送至中间方；（3）数据计算技术服务商，为客户搭建计算系统，包括在业务方、数据方以及可信第三方部署服务节点。考虑国内实际，极可能是由监管单位监管，相关技术储备的第三方企业提供技术服务及运营。

产业机遇：1）卫士通作为数据安全核心公司，参与国家数据安全顶层规划和多项数据安全国家标准制定，具备符合国家合规思路的领先解决方案。基本加密业务信创在手订单充裕，安全芯片等产品军工需求高景气，且成本有望在研究所和上市公司再平衡，净利率预计将显著改善，我们测算 2021 年安全边际市值为 600 亿，2023、2025 年潜在总市值或达 1570.89、3195.93 亿元；2）**奇安信前瞻布局的隐私卫士等产品有望核心受益，**对应用行为和隐私政策采用可扩展的插件方式进行检测，包括隐私政策完整性检测、与应用行为的实质符合检测、非必要信息收集检测、数据出境等；**3）安恒信息已发布完备数据安全解决方案，**包含“CAPE”数据全生命周期防护体系、数据安全咨询服务体系、AiLand 数据安全岛、AiTrust 零信任解决方案、AiDSC 数据安全管控平台、EDR 与数据勒索防护等六大产品服务。**4）天融信数据安全解决方案以数据为核心，**贯穿数据梳理、体系设计、问题解决到智能管控，为企业建立与业务相适应的统一安全服务平台进行统一化管理，实现数据全生命周期安全管控，凭借优质客户基础与技术储备受益。

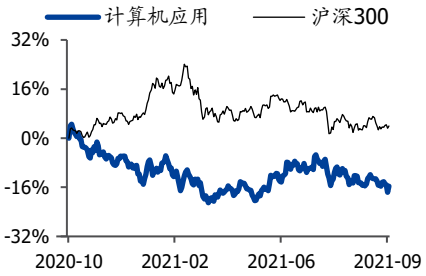
隐私安全：卫士通、安恒信息、奇安信。

网络安全：奇安信、卫士通、安恒信息、深信服、天融信、启明星辰、绿盟科技。

风险提示：行业竞争加剧风险；政策力度不及预期风险；宏观经济风险；测算可能与实际存在误差。

增持（维持）

行业走势



作者

分析师　刘高畅
执业证书编号：S0680518090001
邮箱：liugaochang@gszq.com

相关研究

1、《计算机应用：数据安全，后互联网时代的盛宴》2021-09-26

2、《计算机应用：《个人信息保护法》，2018 年的 GDPR》2021-08-29

3、《计算机应用：《个人信息保护法》落地，数据安全产业拉开序幕》2021-08-22

内容目录

图表目录

智能车时代已至，数据安全安全关注度持续提升

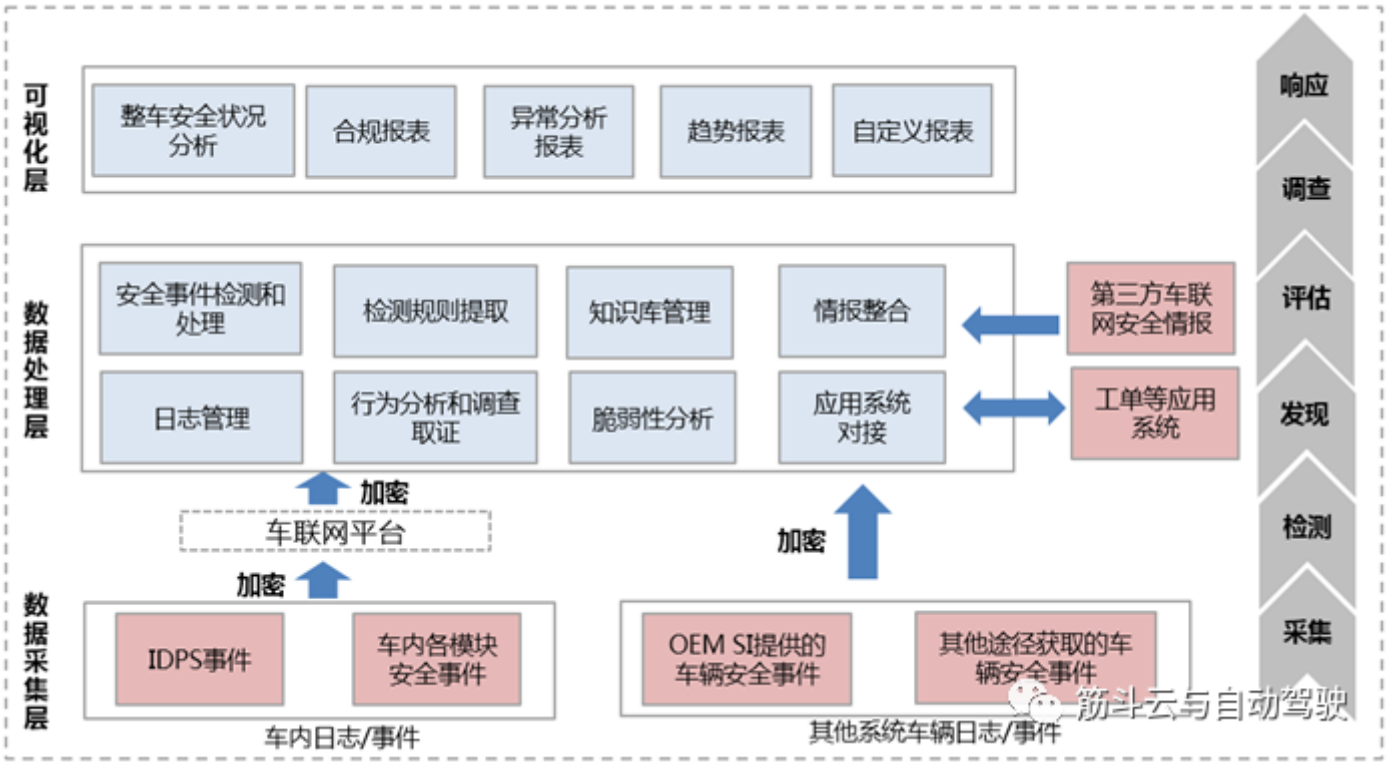
车联网安全领域，**《汽车数据安全管理若干规定(试行)》的通知**主要强调了四方面的防护：其一是智能网联汽车完全防护。《通知》表示，要保障车辆网络安全，智能网联汽车生产企业要加强整车网络安全架构设计，加强车内系统通信安全保障，加强关键设备和部件安全防护和安全检测，加强诊断接口、通用串行总线端口、充电端口等的访问和权限管理。同时智能网联汽车生产企业要落实安全漏洞管理责任，及时发现并处理威胁与漏洞。

其二是车联网网络安全防护。《通知》强调，车联网网络安全防护涉及五个方面，各相关企业和国家部门要加强车联网网络设施和网络系统安全防护能力;全力保障车联网通信安全;积极开展车联网安全监测预警;做好车联网安全应急处置;以及做好车联网网络安全防护定级备案。

其三是车联网服务平台安全防护。《通知》要求，车联网服务平台运营企业要采取必要的安全技术措施，加强平台网络安全管理，防范网络侵入、数据窃取、远程控制等安全风险。并且加强在线升级服务安全和漏洞检测评估，定期评估网络安全状况，防范软件被伪造、篡改、损毁、泄露和病毒感染等网络安全风险。此外还要强化应用程序安全管理，加强车联网应用程序安全检测。

其四是数据安全保护。《通知》提出，按照"谁主管、谁负责，谁运营、谁负责"的原则，智能网联汽车生产企业、车联网服务平台运营企业要加强数据分类分级管理;同时提升数据安全技术保障能力，防范数据泄露、毁损、丢失、篡改、误用、滥用等风险;以及规范数据开发利用和共享使用，强化数据出境安全管理，防范在使用技术处理数据时，侵犯用户权利，危害国家安全。

图表 1：车联网网络安全及数据安全层级



资料来源：CSDN，国盛证券研究所

今年世界互联网大会上，特斯拉将其自身的数据架构和数据安全设置当成重点内容进行展示，特斯拉表示其终端会产生四类数据：
一是与车辆使用、操作和状况有关的车辆数据：例如车速、里程、电机转速、方向盘扭矩、软件版本等。
二是车载触摸屏使用的信息娱乐系统数据，包括客户使用功能或应用程序的汇总计数，电台收听时间和频道等。
三是诊断数据，包括车辆配置、固件、能量使用、电子系统状态的详细信息，以及不同系统间传输的用于识别错误并进行技术评估的数据。
四是 Autopilot 自动辅助驾驶数据，包括车辆使用摄像头提供自动辅助驾驶、智能召唤和自动泊车等高级功能所需的数据。

工业及电信领域数据安全政策持续落地，进一步催化产业爆发

2021 年 9 月 30 日，为提升工业、电信行业数据安全保护能力，防范数据安全风险，工信部发布《工业和信息化领域数据安全管理办法(试行)(征求意见稿)》。推动数据敏感企业建立数据全生命周期安全管理制度，针对不同级别数据，明确制定数据收集、存储、使用、加工、传输、提供、公开等环节的具体分级防护要求和操作规程：

数据收集：工业和电信数据处理者收集数据，应当遵循合法、正当、必要的原则，不得窃取或者以其他非法方式收集数据。数据收集过程中，应当采取配备技术手段、签署安全协议等措施加强对数据收集人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行记录。通过间接途径获取数据的，应当要求数据提供方做出数据源合法性的书面承诺，并承担相应的法律责任。

数据存储：工业和电信数据处理者应当依据法律规定或者与用户约定的方式和期限存储数据。存储重要数据的，还应当采用校验技术、密码技术等措施进行安全存储，不得直接提供存储系统的公共信息网络访问，并实施数据容灾备份和存储介质安全管理。存储核心数据的，还应当实施异地容灾备份。
数据使用加工：工业和电信数据处理者未经个人、单位等同意，不得使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原等加工处理活动。利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。使用、加工重要数据和核心数据的，还应当加强访问控制，建立登记、审批机制并留存记录。工业和电信数据处理者提供数据处理服务，涉及经营电信业务的，应当按照相关法律、行政法规规定取得电信业务经营许可。

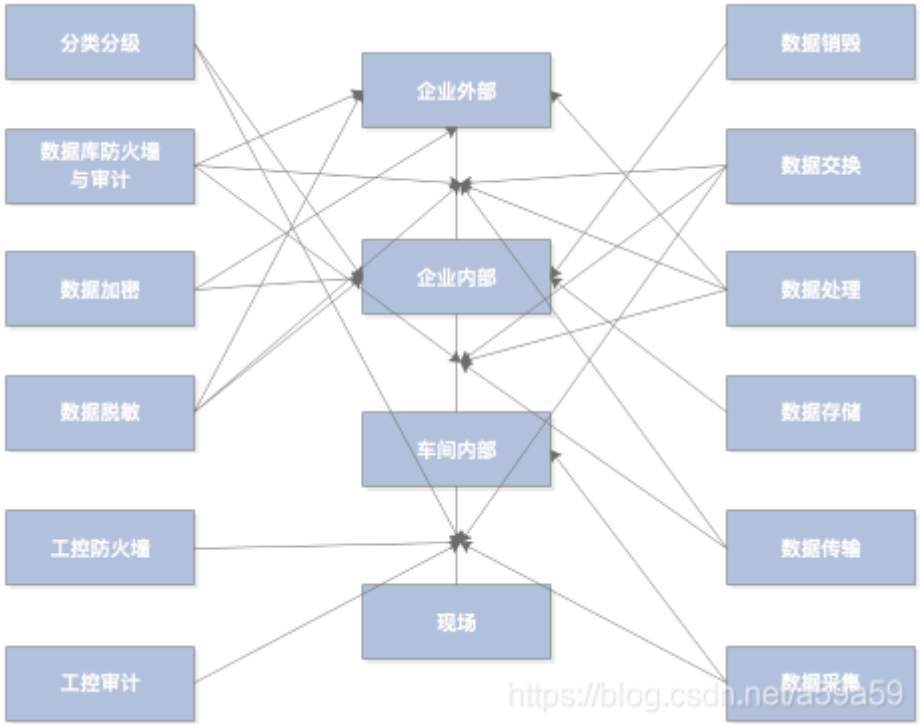
数据传输：工业和电信数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据的，还应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施，涉及跨组织机构或者使用公共信息网络进行数据传输的，应当建立登记、审批机制。跨不同数据处理主体传输核心数据的，还应当通过国家数据安全工作协调机制审批。

数据提供：工业和电信数据处理者应当依据行业数据分类分级管理要求，明确数据提供的范围、数量、条件、程序等。提供重要数据的，还应当采取数据脱敏等措施，建立审批机制。提供核心数据的，还应当通过国家数据安全工作协调机制审批。工业和电信数据处理者应当事先对数据接收方的数据安全保护能力进行核实，并与数据接收方签订数据安全协议，明确数据提供的范围、使用方式、时限、用途以及相应的安全保护措施、违约责任，并督促数据接收方予以落实。

数据公开：工业和电信数据处理者公开数据应当真实、准确，并在公开前开展安全评估，对涉及个人隐私、个人信息、商业秘密、保密商务信息以及可能对公共利益及国家安全产生重大影响的，不得公开。

数据销毁：工业和电信数据处理者应当建立数据销毁策略和管理制度，明确销毁对象、流程和技术等要求，对销毁活动进行记录和留存。销毁重要数据和核心数据的，不得以任何理由、任何方式对销毁数据进行恢复。

图表 2：数据安全技术、安全位置、数据周期节点间关联关系

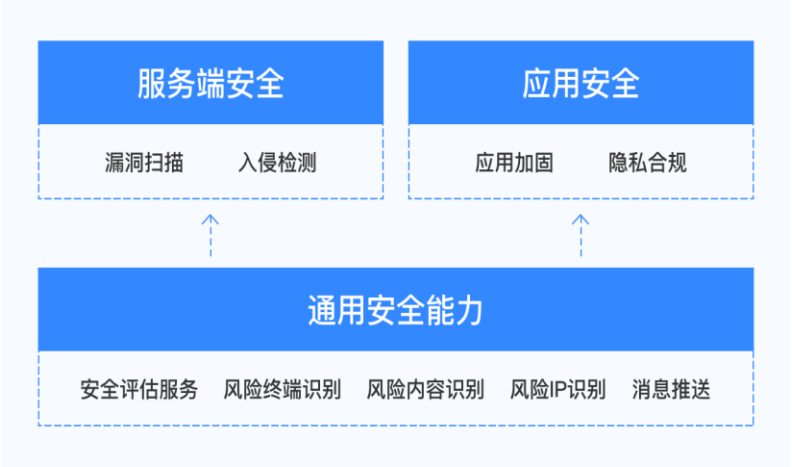


资料来源：CSDN，国盛证券研究所

除互联网需求迫切外，金融、医疗、汽车、能源等数据安全潜在市场巨大

百度推出"史宾格"安全和隐私合规平台，基于 AI 检测技术，比照《App 违法违规收集使用个人信息行为认定方法》《工业和信息化部关于开展 App 侵害用户权益专项整治工作的通知》《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》《信息安全技术个人信息安全规范》等规范性文件、国家标准，提供隐私风险项检测、隐私专项检测、场景检测、权限过度收集与使用情况检测等产品服务，助力监管机构、应用市场、大型企业、App 开发者等完成 App 隐私合规自查，发现隐私违规风险。

图表 3：百度 APP 安全解决方案



资料来源：百度官网，国盛证券研究所

金融机构在客户所掌握的"个人信息"，依据其获取途径和发挥作用的不同，在《信息保护法》之下可归于不同的类型，相应地由金融机构进行不同程度的保护。

图表 4：金融结构涉及相关个人信息

金融机构“个人信息”	《个人信息保护法》下“个人信息”类型
员工个人信息	个人信息
客户相关信息	敏感个人信息
业务合作方相关个人信息	
衍生个人信息	非个人信息

资料来源：《个人信息保护法》，国盛证券研究所

随着实体医院将诊疗活动延伸至互联网端，数据共享和流通成为刚性业务需求，静态的隔离保护措施难以控制数据在流动中的风险，关乎患者隐私、种类繁多的医疗数据也迎来愈加严峻的安全挑战，互联网医院需要通过动态变化的视角分析和判断数据安全风险。

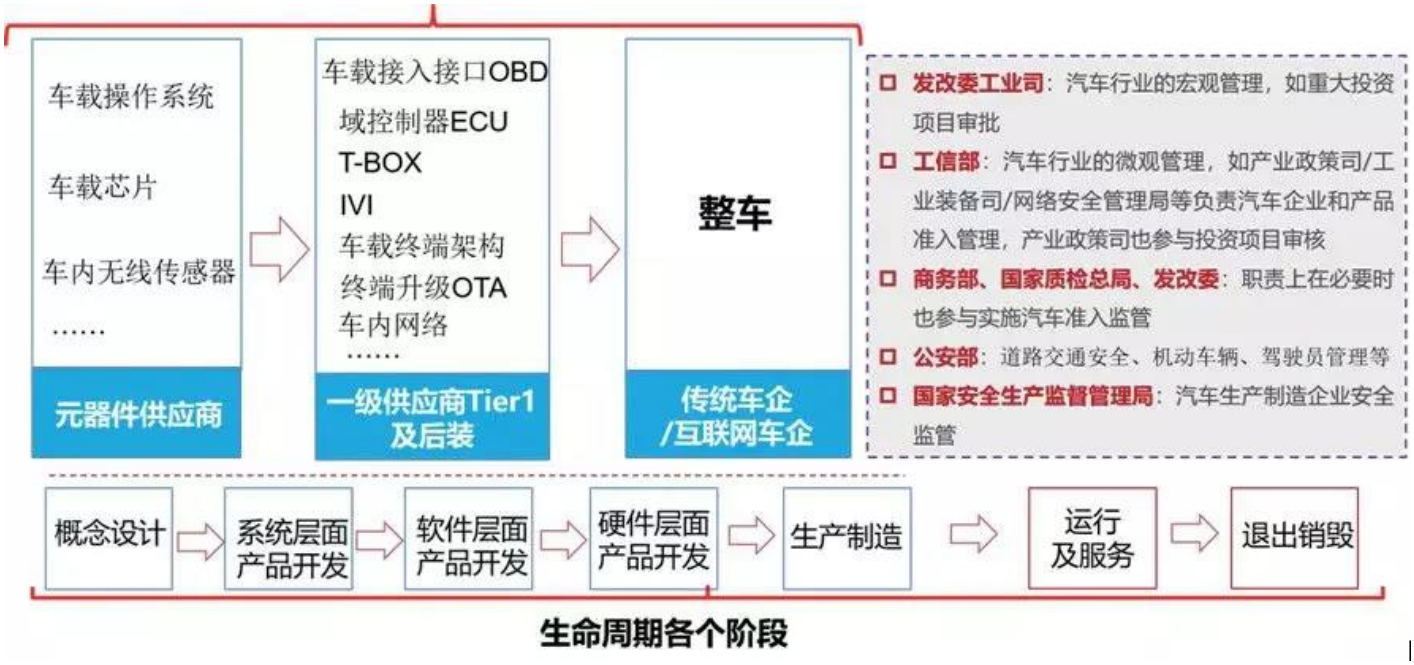
图表 5：互联网医院面临的主要数据安全风险

资料来源：医疗数据安全，国盛证券研究所

随着智能汽车产业、车联网技术的快速发展，以自动辅助驾驶为代表的人工智能技术日益普及，汽车数据处理能力日益增强，暴露出的汽车数据安全问题和风险隐患日益突出。在汽车数据安全管理领域出台有针对性的规章制度，明确汽车数据处理者的责任和义务，规范汽车数据处理活动，是防范化解汽车数据安全风险、保障汽车数据依法合理有效利用的需要，也是维护国家安全利益、保护个人合法权益的需要。

《规定》明确，汽车数据处理者应当履行个人信息保护责任，充分保护个人信息安全和合法权益。开展个人信息处理活动，汽车数据处理者应当通过显著方式告知个人相关信息，取得个人同意或者符合法律、行政法规规定的其他情形。处理敏感个人信息，汽车数据处理者还应当取得个人单独同意，满足限定处理目的、提示收集状态、终止收集等具体要求或者符合法律、行政法规和强制性国家标准等其他要求。汽车数据处理者具有增强行车安全的目的和充分的必要性，方可收集指纹、声纹、人脸、心律等生物识别特征信息。

图表 6：我国车联网安全监管机制现状

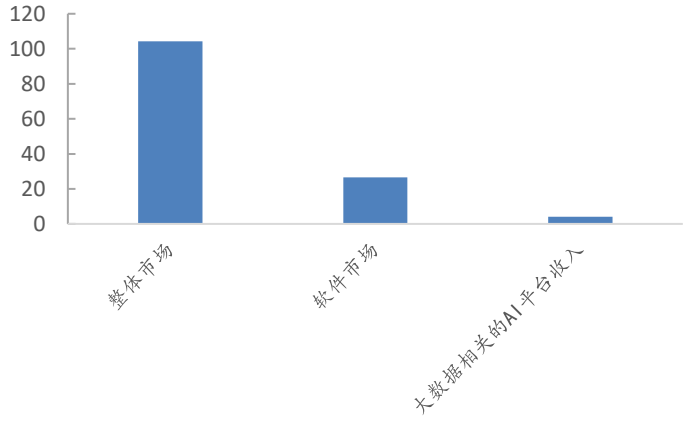


资料来源：信息安全与通信保密杂志社，国盛证券研究所

大数据加速应用与政策双轮驱动，短期技术服务市场超百亿

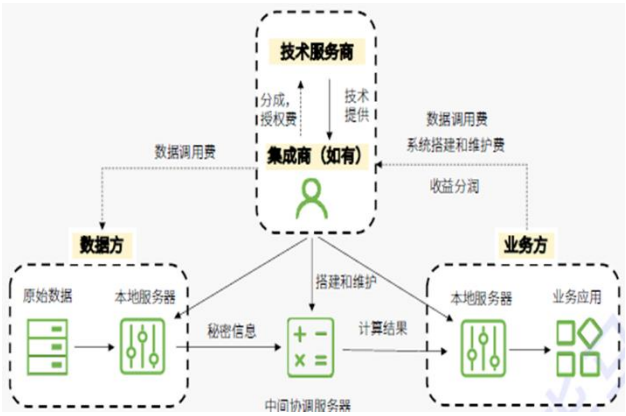
数据安全市场空间测算，依据大数据市场中 AI 平台收入推算 2023 年有望达百亿，长期潜在空间有望达千亿。数据安全计算模块常见于大数据服务场景，添加至 AI 计算平台，并且与 AI 应用同样以数据为基础，进行安全、存储以及计算等服务，故以 AI 平台收入为隐私计算产值上限，根据 IDC 预测 2020 年我国大数据市场约 104.2 亿美元，其中软件市场规模为 26.5 亿美元，AI 平台收入约 4 亿美元，IDC 预测 2018 至 2024 年 AI 产业年均复合+39%，则 AI 平台收入 2024 年有望达 15 亿美元，则数据安全方案上限近百亿人民币。

图表 7：数据安全 2023 年规模上限超百亿



资料来源：IDC，国盛证券研究所

图表 8：隐私计算商业模式



资料来源：KPMG，国盛证券研究所

数据深度价值挖掘过程中需要兼顾数据应用和安全，平衡效率和风险，在保障安全的前提下发挥数据价值。以多方安全计算（Secure Multi-Party Computation，MPC）、可信执行环境（Trusted Execution Environment，TEE）、联邦学习（Federated Learning，FL）等为代表的隐私计算技术为解决了数据流通过程中的"可用不可见"难题，有助于破解数据保护与利用之间的矛盾，已在金融、医疗、政务等领域开始推广应用：

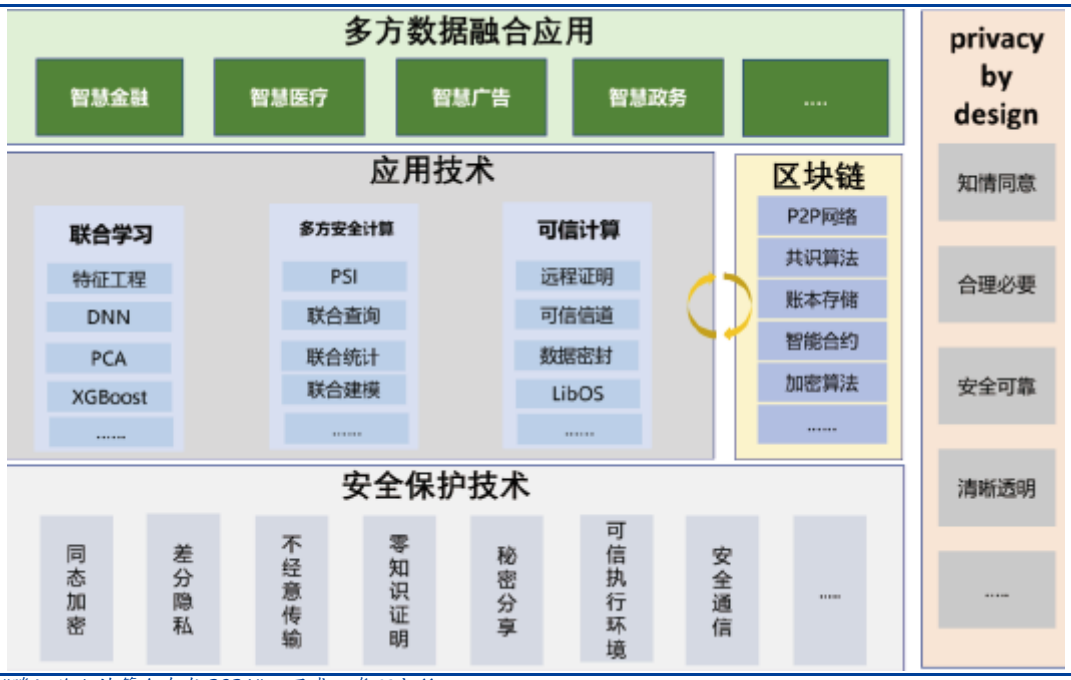
1） **对于个人消费者，隐私计算应用有助于降低隐私数据在应用过程中的泄密风险；**随着信息化程度不断提高，个人信息被采集和广泛应用，同时也面临着信息泄露风险，而隐私计算在很多场景的应用，可以提升对个人信息的保护水平，降低个人信息在应用过程中泄露的风险。

2） **对于 B 端企业，隐私计算兼顾数据协作过程中的安全性与效率性，监督企业履行数据保护义务。**企业内部借助隐私计算，能够切实保护企业在采集、存储、分析等过程中的关键信息。另一方面，隐私计算能够促进企业的跨界数据合作，由于隐私计算能够实现数据可用不可见，能够帮助不同企业和机构与产业链上下游的主体进行联合分析。

3） **对于 G 端政府、社会机构，隐私计算可促进数据价值和社会福利最大化。**一是借助隐私计算能够在政府数据开放过程中，在采集、存储、协作等方面提升数据安全和隐私保护水平，在保障数据安全的同时增强全社会的数据协作，通过数据的应用最大化社会福利。二是借助隐私计算推动数据要素赋能产业升级

隐私计算（Privacy Computing）是一种由两个或多个参与方联合计算的技术和系统，参与方在不泄露各自数据的前提下通过协作对他们的数据进行联合机器学习和联合分析。

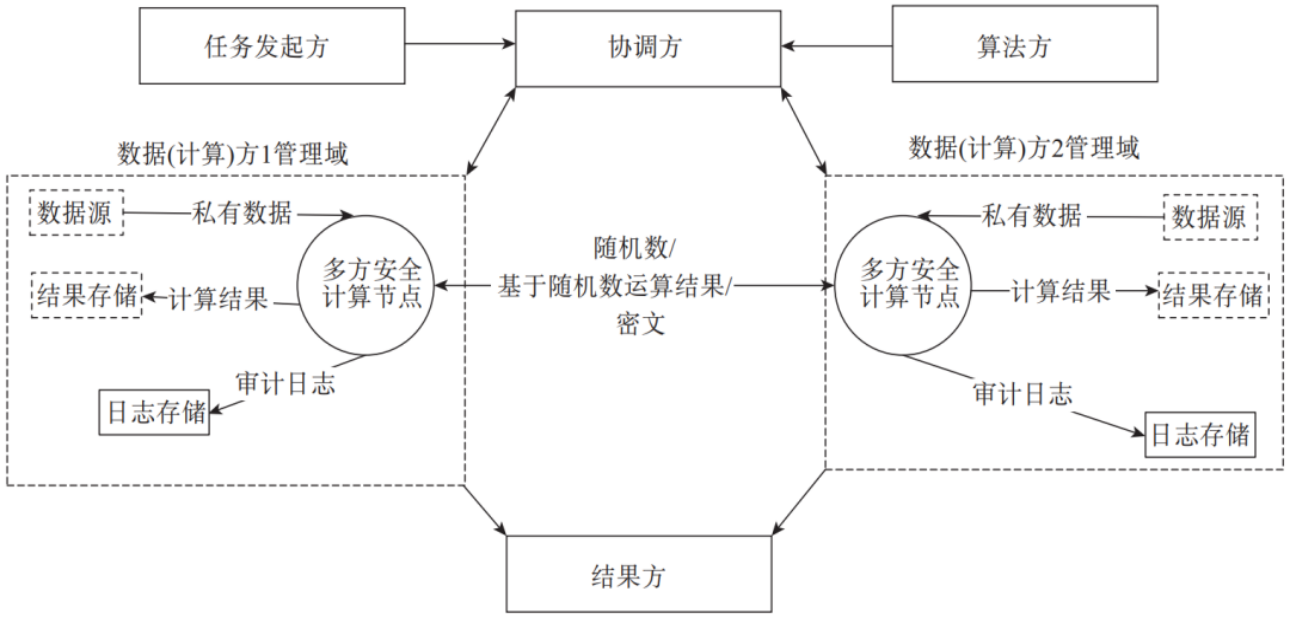
图表 9：隐私计算体系架构



资料来源：《腾讯隐私计算白皮书 2021》，国盛证券研究所

多方安全计算技术的核心思想是设计特殊的加密算法和协议，基于密码学原理实现在无可信第三方的情况下，在多个参与方输入的加密数据之上直接进行计算。多方安全计算由姚期智等人于 20 世纪 80 年代提出，以交互不可逆的密文数据的方式实现了对数据的安全保护，每个参与方不能得到其他参与方的任何输入信息，只能得到计算结果。

图表 10：基于多方安全计算的数据流通产品技术架构



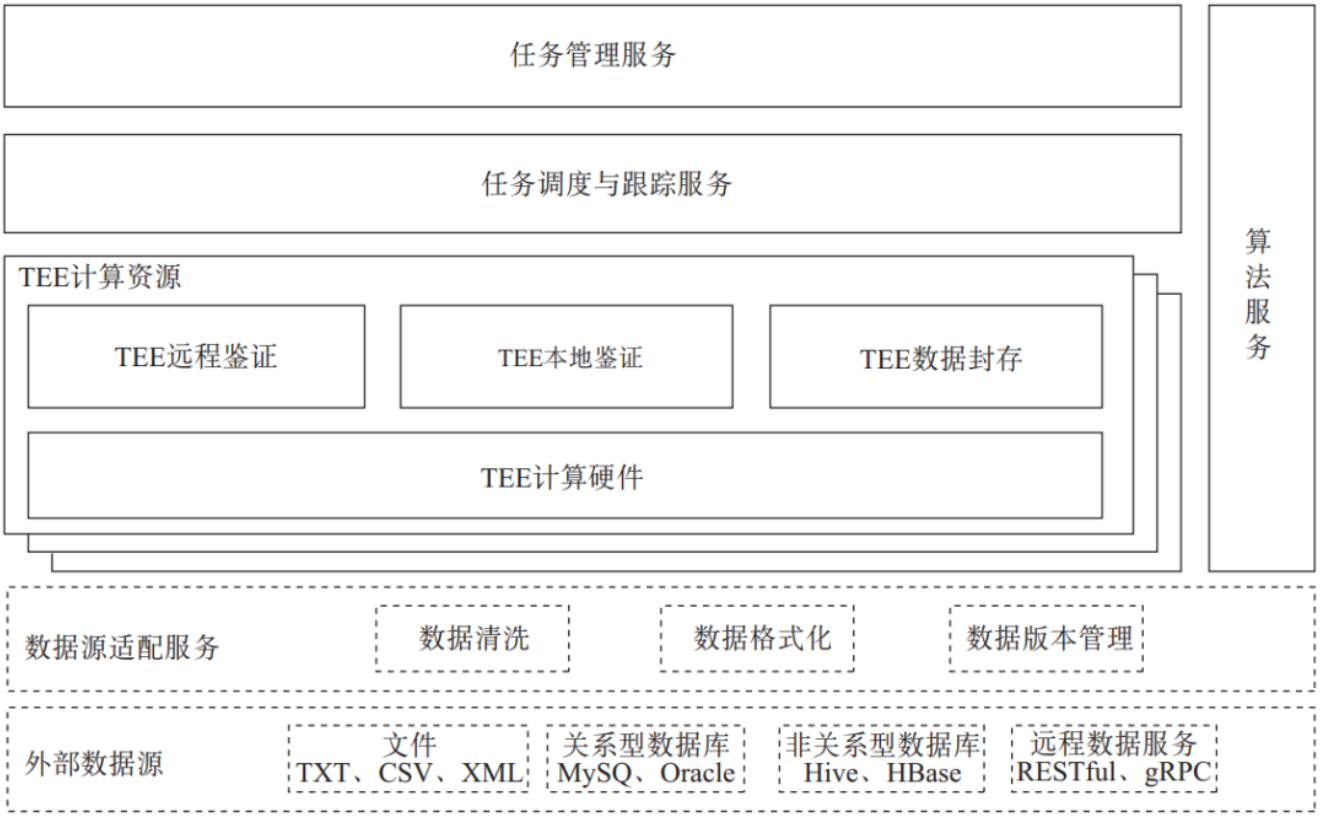
资料来源：隐私计算联盟，国盛证券研究所

可信执行环境的核心思想是构建一个独立于操作系统而存在的可信的、隔离的机密空间，数据计算仅在该安全环境内进行，通过依赖可信硬件来保障其安全。

可信执行环境的最本质属性是隔离，通过芯片等硬件技术并与上层软件协同对数据进行保护，且同时保留与系统运行环境之间的算力共享。目前，可信执行环境的代表性硬件产品主要有 Intel 的 SGX、ARM 的 TrustZone 等，由此也诞生了很多基于以上产品的商

业化实现方案，如百度 MesaTEE、华为 iTrustee 等。

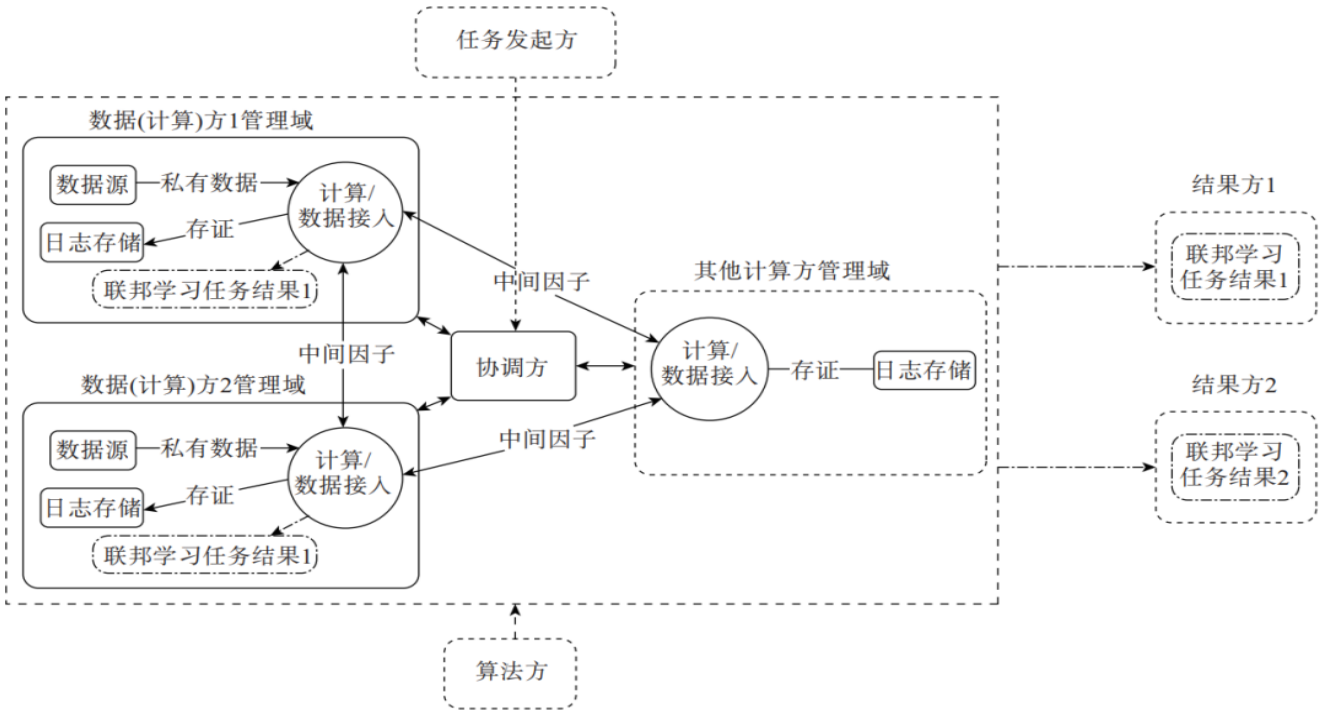
图表 11：基于可信执行环境的数据计算平台技术架构



资料来源：隐私计算联盟，国盛证券研究所

除上述可信计算环境、多方安全计算技术外，还比较常见为联邦学习算法，其本质是分布式的机器学习，在保证数据隐私安全的基础上，实现共同建模，提升模型的效果。联邦学习的目标是在不聚合参与方原始数据的前提下，实现保护终端数据隐私的联合建模。根据数据集的不同类型，联邦学习分为横向联邦学习、纵向联邦学习与联邦迁移学习。

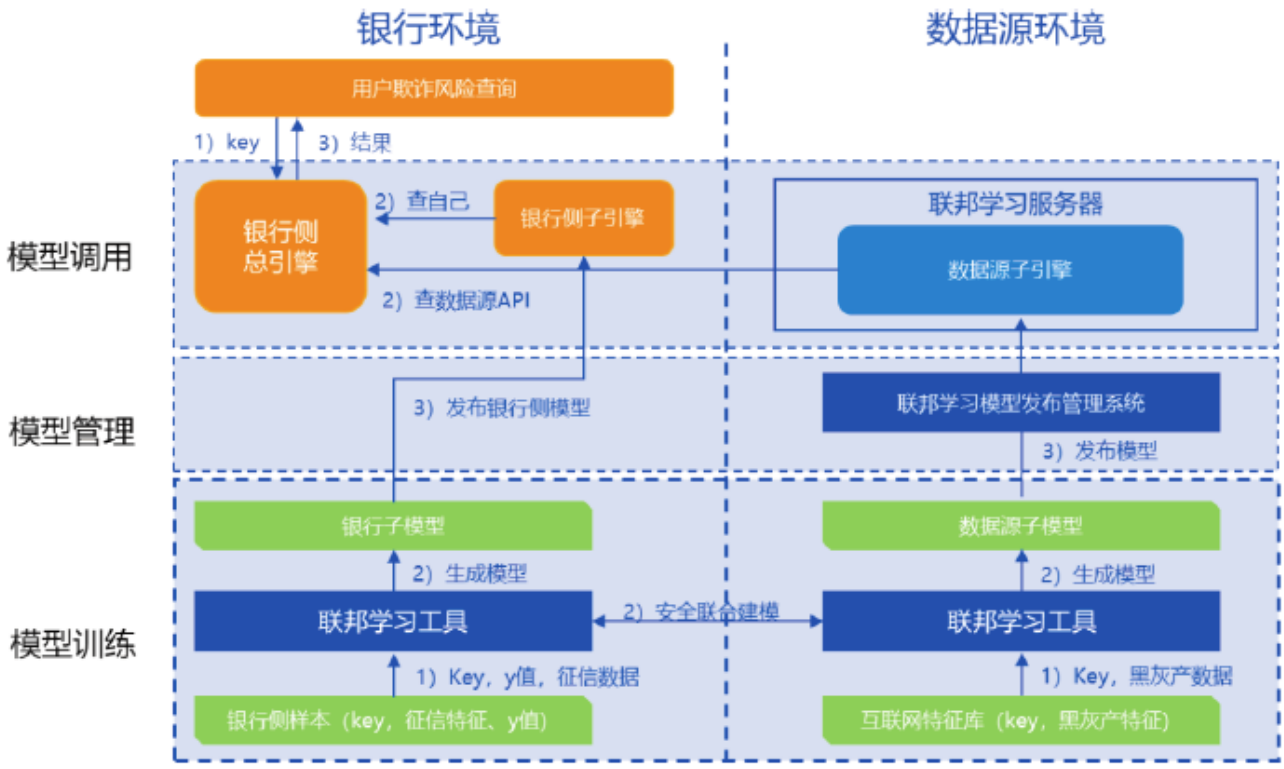
图表 12：基于联邦学习的数据计算平台技术架构



资料来源：隐私计算联盟，国盛证券研究所

联邦学习应用于银行联合建模，提升反欺诈模型水平，降低资产不良率。传统上，银行都是基于收入水平、征信数据、还款履约情况等变量分来做贷前反欺诈建模，但仍存在数据维度缺乏、数据量较少等情况，需要融合多方数据联合建模才能构建更加精准的反欺诈模型，联邦学习可以有效解决合作中数据隐私与特征变量融合矛盾，保障特征变量交换时的信息安全。

图表 13：隐私计算在金融反欺诈场景应用示例



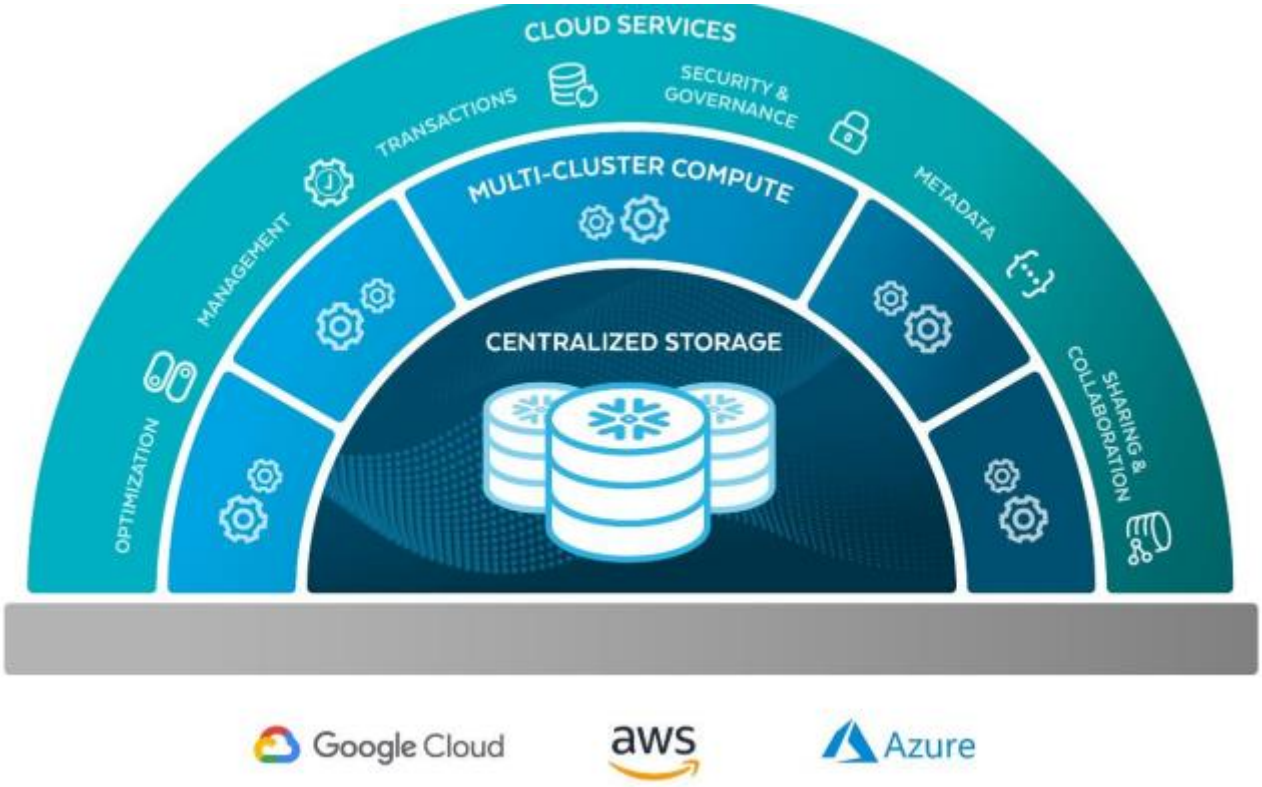
资料来源：《腾讯隐私计算白皮书 2021》，国盛证券研究所

随 IT 架构演变，长期数据安全 SaaS 运营收入有望达千亿

随 IT 架构上云，长期数据安全 SaaS 运营收入有望达千亿，商业模式改善带来估值提升机遇。以消费贷款场景为例，假设 2030 年金融机构信用风险建模使用联邦学习渗透率达 60%，服务费率为 1%，国内短期消费信贷市场 2019 年已达 9.92 万亿元，假设直到 2030 年年化复合增速为 8%，则 2030 年市场有望达 21.42 万亿元，数据安全收入有望达 1285 千亿元，考虑互联网、医疗及政务大数据等场景，空间巨大。

平台经济垄断本质是数据垄断，通过数据协作运用打破垄断过程中的安全性愈发重要，未来隐私计算领军企业除具备完备隐私计算服务能力外，还将具备“Snowflake+CrowdStrike”特征，即同时具备“DaaS+SECaaS”能力。
Snowflake 提出 Data-Warehouse-as-a-Service（DaaS）概念，即云原生并专注于分析型数据仓库的 SaaS 服务。Snowflake 将各类客户的各类数据整合至云数据平台，方便用户进行数据分析，简化了数据共享，还能够将数据管理和合规问题的风险降到最低。Snowflake 可以解决的痛点包括：数据孤岛、数据更高效的搜索和维护、数据分析的速度和成本。相较于传统的硬件服务器存储传输、单一 IaaS 厂商而言，其优势在于：可伸缩性、易操作、SaaS 订阅模式、多云架构，商业模式天然具备网络效应等。

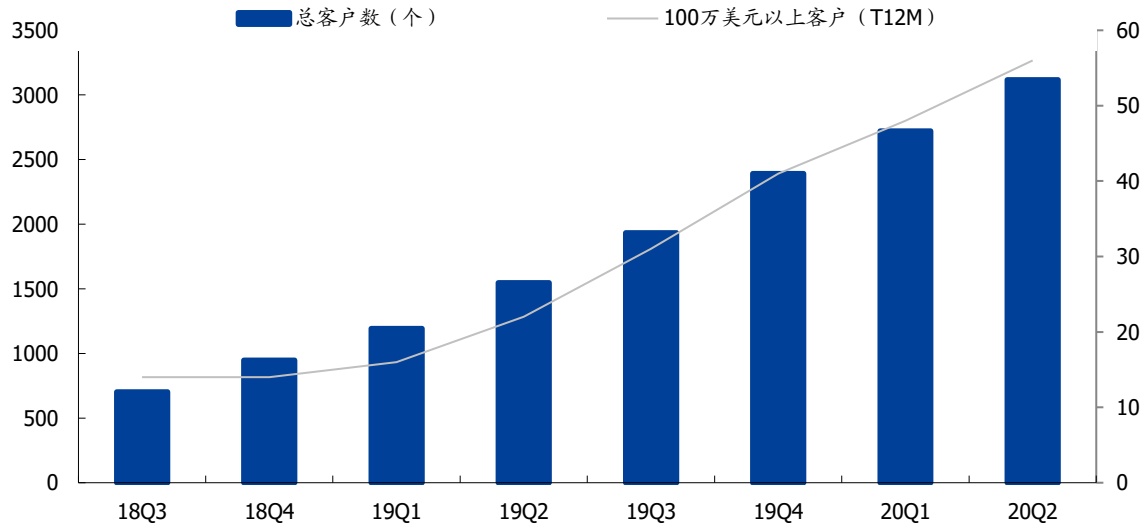
图表 14：Snowflake 基于三朵公有云的云原生分析型数据仓库



资料来源：公司招股说明书，国盛证券研究所

伴随 IT 结构云化程度不断提高，Snowflake 凭借云计算方式摆脱底层引擎的限制，最大程度利用现成的数据资源。同时，Snowflake 的定价方式与典型的 SaaS 公司按月按年订阅不同，它的收入和定价模型是基于使用量的，存储、计算和数据转移都单独定价。

图表 15：Snowflake 客户开拓进展迅速

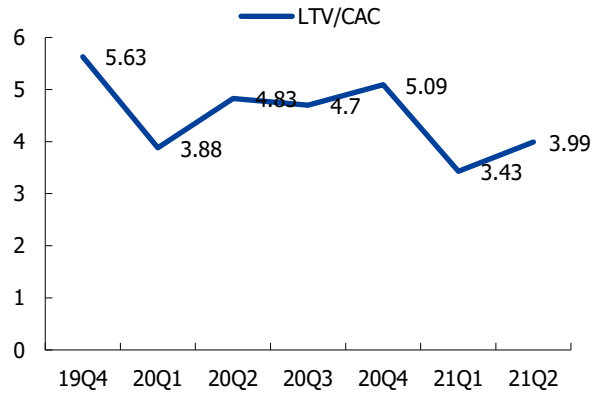


资料来源：公司招股说明书，国盛证券研究所

Snowflake 的 LTV/CAC 比率历史数据均在 3.0 以上（假设客户留存率在 97%以上），说明在获取新客户方面实力较强，毛利率约 60%多，SaaS 公司中并不算很高，主要是向

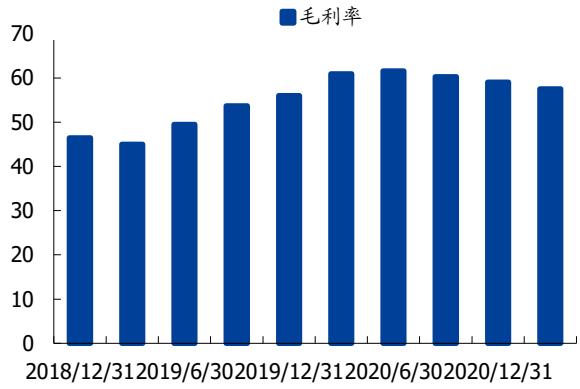
三家公有云公司支付基础设施费用，Snowflake 尚未参与云基础设施建设，未来毛利率提升空间或主要来自自建基础设施。

图表 16：Snowflake 的 LTV/CAC 指标优秀



资料来源：公司年报，国盛证券研究所

图表 17：Snowflake 毛利率（%）维持较高水平



资料来源：公司年报，国盛证券研究所

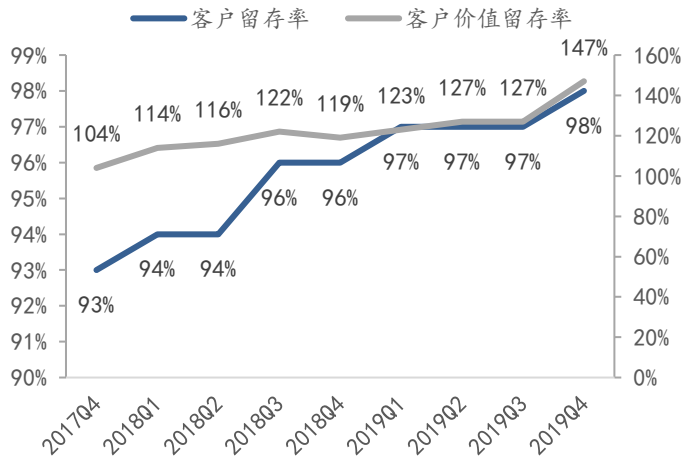
CrowdStrike 的发展路径，以平台形式不断扩充功能模块，客户粘性与单价不断提升，营收及估值天花板不断抬高。以 CrowdStrike 为代表，成立于 2011 年，分别在 2012、2013 年发布威胁情报服务 Falcon X 及终端检测与响应产品 Falcon OverWatch、Falcon Insight 等。2017 年，公司迅速丰富基于 SaaS 模式的终端安全产品线，公司已构建 SaaS+PaaS 的安全生态，在第三方安全厂商中处于领先地位。Falcon 终端安全平台提供的云安全服务模块完全基于 SaaS 模式，具备敏捷性易用、可拓展性强、持续迭代优化等优点，且于 2020 年推出 PaaS 安全平台 CrowdStrike Store，构建了终端安全产品+威胁情报服务+专家服务，SaaS+PaaS 的完整安全生态。

图表 18：CrowdStrike 细分业务市场空间

市场	公司布局	市场规模
企业终端安全	公司于 2013 年推出 Falcon OverWatch 与 Falcon Insight 云模块前身， 2017 年发布 Falcon Prevent 产品，进军 EDR 与下一代防病毒市场	据 IDC 预测，2019 年全球威胁情报市场规模为 16 亿美元，2021 年预计将达到 20 亿美元
威胁情报	2012 年,公司发布 Falcon X 云模块前身产品，进入威胁情报市场	据 IDC 预测，2019 年企业终端安全市场规模达到 76 亿美元，2021 年预计将达到 88 亿美元
安全漏洞	2017 年，公司发布 Falcon Spotlight 云模块，进入安全漏洞管理市场	据 IDC 预测，2019 年安全漏洞市场规模达到 84 亿美元，2021 年预计将达到 104 亿美元
IT 资产管理	2017 年，公司发布 Falcon Discover 云模块，首次进入 IT 资产管理这一非安全市场	据 IDC 预测，2019 年 IT 资产管理市场规模达到 26 亿美元，2021 年预计将达到 31 亿美元
安全托管服务	2018 年，公司瞄准小型企业缺乏网络安全预算与技术实力，推出 Falcon Complete 云模块，帮助中小企业更便捷安全地进行网络安全管理，与此同时大企业也可借助这一模块简化人员配置	据 IDC 预测，2019 年安全托管服务市场规模达到 248 亿美元，2021 年预计将达到 296 亿美元，公司预计可参与市场规模 2019 年约为 44 亿美元，2021 上升至 51 亿美元

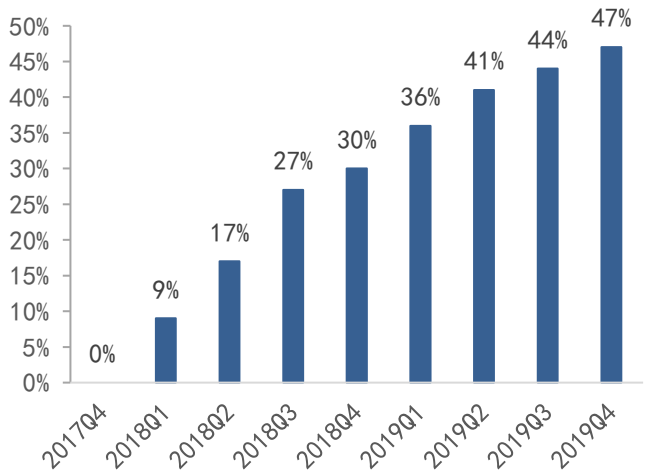
资料来源：IDC、国盛证券研究所

图表 19：CrowdStrike 客户及其价值留存率



资料来源：公司年报，国盛证券研究所

图表 20：消费 4 个及以上 CrowdStrike 云安全模块的客户比例



资料来源：公司年报，国盛证券研究所

卫士通数据安全空间巨大，安恒、奇安信有望显著受益数据安全发展

竞争格局：典型的数据安全应用场景通常包含三类参与方，互联网作为使用方，未来国内或由网信办等监管单位牵头平台建设，具备国资股东背景、技术储备的第三方企业提供技术及运营：（1）数据的使用方，需考虑业务特征与支付能力，互联网厂商合规需求迫切，包括数据“最小化采集、避免滥用”，此外如联合建模下的银行业、医疗机构；（2）作为数据的提供方，做到原始数据不出本地，将加密后的信息发送至中间方；（3）隐私计算技术服务商，为客户搭建计算系统，包括在业务方、数据方以及可信第三方部署服务节点。考虑国内实际，有可能是由网信办等监管单位牵头平台建设，相关技术储备的第三方企业提供技术及运营。

图表 21：数据安全涵盖存储、传输、计算等多项产品需求

生命周期	数据存储	数据传输	数据计算过程	数据计算结果
相关技术	SM2、SM3 SM4、RSA、SHA2、AES、…	SM2、SM3 SM4、RSA、AES、SHA2、SSL/TLS、…	MPC(GC、SS)、FL OT、FHE、TERE、Paillier、	DP、…

资料来源：金融科技微洞察&KPMG，国盛证券研究所

产业机遇：卫士通将成为数据安全市场最核心标的。1）数据安全监管政策持续加码，公司具备领先解决方案与技术实力，有能力作为核心公司直接受益于数据安全订单落地；2）基本加密业务信创在手订单充裕，安全芯片等产品军工需求高景气，且成本有望在研究所和上市公司再平衡，净利率预计将显著改善；3）互联网厂商数据安全安全需求迫切，平台经济垄断的背后是数据，监管与民众担忧进一步促使互联网巨头加大隐私保护支出，互联网厂商极愿意采购规范化方案实现合规（厂商合计市值已回落明显）；4）公司作为电科旗下网安版图唯一控股上市公司，具有天然股东优势与监管公信力。数据安全类似于公共资源管理，是未来的石油、稀土，必须掌握在国家手中，多因素共振驱动卫士通成为核心标的。

卫士通潜在市值测算：

中性假设下，按照分部估值思路，考虑公司基本网安业务、数据安全业务， 2023/2025 年对应潜在市值或达 1570.89、3195.93 亿元

假设：1）据 IDC、亿欧智库、智研咨询等统计国内互联网厂商、金融、医疗、政务等领域数据安全市场规模上限，市占率保持先上升后增速放缓的趋势；

2）考虑卫士通目前方案领先，互联网厂商数据合规需求旺盛，假设市占率为 25%，部分密级相对较低场景下互联网厂商，翼方、富数科技等垂直行业厂商占据剩下空间；

3）参考隐私、营销、安全和数据治理公司 OneTtust 估值 15X PS， 2023/2025 数据安全业务业务潜在市值分别为 1112、2508 亿元。

我们预计密码业务 2021/2022/2023 年公司营业收入为 30.10/38.03/48.05 亿元，归母净利润为 3.52/5.11/7.65 亿元，2021 年安全边际市值为 600 亿，2023、2025 年潜在总市值或达 1570.89、3195.93 亿元，维持“买入”评级。

图表 22：卫士通密码业务及数据安全潜在市值测算

		2018	2019	2020	2021E	2022E	2023E	2024E	2025E
基本网安业务	安全集成与服务（亿元）	10.08	12.4	13.21	16.64	20.97	26.42	33.29	41.95
		-3.54%	23.02%	6.53%	26.00%	26.00%	26.00%	26.00%	26.00%
	单机与系统产品（亿元）	9.23	8.64	5.93	7.35	9.12	11.31	14.02	17.39
		-15.55%	-6.39%		24.00%	24.00%	24.00%	24.00%	24.00%
	网安产品（亿元）			4.69	6.10	7.93	10.31	13.41	17.43
					30.00%	30.00%	30.00%	30.00%	30.00%
	产品（亿元）	19.31	21.04	23.84	30.09	38.02	48.05	60.72	76.77
	毛利率		32.54%	35.48%	38.83%	40.00%	42.00%	43.00%	44.00%
	净利率			6.82%	11.71%	13.43%	15.92%	16.92%	17.92%
	净利润（亿元）				3.52	5.11	7.65	10.28	13.76
	网安业务目标 PE				70	65	60	55	50
	网安业务目标市值（亿元）				246.62	332.02	459.01	565.19	687.94
数据安全业务	互联网数据安全市场规模（亿）			40.29	56.41	78.97	110.56	164.73	245.44

金融、医疗、政务数据安全市场（亿）	200	240	288	345.6	414.72	497.66
数据安全渗透率	5%	20%	50%	65%	80%	90%
数据安全规模（亿）	12.01	59.28	183.48	296.5	463.56	668.8
卫士通市占率			25%	25%	25%	25%
卫士通份额（亿）			45.87	74.13	115.89	167.2
参考 OneTrust 融资估值 PS			15	15	15	15
数据安全潜在市值（亿）			688.07	1111.88	1738.34	2507.99
总市值（亿）			1020.09	1570.89	2303.53	3195.93

资料来源：Wind，IDC，国盛证券研究所

奇安信进度领先，数据要想真正成为新型生产要素，数据安全是重要前提，数据安全是重要使能器。作为当今互联网时代的新型生产要素，在大数据、人工智能等新兴技术的加持下，数据流动愈加频繁、数据价值日益凸显，已经成为各行业科技转型的核心推动力。奇安信基于“数据不动程序动，数据可用不可见”的技术理念，在国内率先兼顾数据隐私安全与商业价值挖掘的隐私卫士产品。

奇安信网神隐私卫士检测系统包括沙箱、隐私协议分析仪、应用行为检测模块、合规评估模块、系统管理模块组成。被检测的安卓或 iOS 应用上传到检测系统后，系统利用真机沙箱或模拟器沙箱对应用进行运行检测，并通过隐私协议分析仪对其隐私政策协议进行自动化分析。应用行为检测和隐私政策检测采用可扩展的检测插件方式进行检测，包括隐私政策完整性检测、与应用行为的实质符合检测、非必要信息收集检测、数据出境、第三方收集、隐私泄漏风险、使用权限检测等。

具备较强产品竞争力，按照《App 违法违规收集使用个人信息行为认定方法》描述的 6 大类 31 项收集行为进行检测项拆解，按照全自动检测、半自动检测和人工检测的分类要求进行全面的、深度的隐私合规检测。

图表 23：奇安信网神隐私卫士检测系统

资料来源：奇安信官网，国盛证券研究所

核心功能包括:

1）应用行为检测，通过真机和模拟器对移动应用进行各类触发操作检测各类隐私行为，深度发现 APP 以及 SDK 获取、存储和上传的各类个人信息，综合其中的明文存储、明文传输、信息出境等行为进行全方位的应用行为检测。

2）隐私政策检测，通过分析应用收集的各类个人信息，与隐私政策中描述的个人信息进行一一比对，结合法律法规要求给出具体不合规项及法律法规适用条款，最终给出针对隐私政策的规范性、完整性和一致性的检测

3）法规对齐分析，隐私卫士系统对各类精细化的检测内容可依据《App 违法违规收集使用个人信息行为认定方法》进行回归分析，将各类检测结果与《认定方法》等多项法律法规进行对齐分析，更利于企业对通报问题的分析。

数据安全法的最大特点是在鼓励数据流动、共享，乃至交易的情况下确保数据的安全。数据这一新的资源，必须在交换流动中才能被释放出更大的价值，这已经逐步成为各行业的基本共识。而如何对重要数据进行有效保护，就成为了整个共享交换场景中的关键点。

数据脱敏，是指对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。在涉及客户安全数据或者一些商业性敏感数据的时，在不违反系统规则条件下对真实数据进行改造并提供测试使用，如身份证号、手机号、卡号和客户号等重要个人信息都需要进行数据脱敏。

图表 24：大数据脱敏流程图示

资料来源：卫士通官网，国盛证券研究所

深信服率先在智能数据分类分级上进行了探索，目前国内大部分的数据分类分级依旧停留在基础层面，且大部分以人力为主，导致一方面会比较耗时，成本较高，另一方面，由于受到人力因素的影响，传统的以正则表达式为主的工具识别准确率非常低。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，相较于传统数据分类分级做法，采用机器学习技术，大大提升了准确率，进一步提升了工作效率，减少了人力成本，在数据分类分级上作了一次有效实践。

安恒信息定增募投数据安全岛项目，公司可利用自身在大数据安全领域的技术积累，丰富网络信息安全平台产品线，提升整体盈利能力。根据赛迪顾问的预测，2019-2021 年，大数据安全市场规模年均增长率为 35.3%，2017-2019 年，公司大数据安全产品收入年复合增长率达到 100.2%，随着《个人信息保护法法》、《数据安全法(草案)》相继公布，政策规范有望驱动数据交易平台及相关技术服务需求增长。

天融信作为国内最早发布数据安全防护体系的网络安全企业，依托数据安全多年的经验，构建了以行业特征为基础，通过数据安全治理、数据安全防护、数据安全监管、数据安全运营赋能，实现数据全生命周期的安全防护整体解决方案，目前已在运营商、金融、政府、能源、卫生、海关等行业领域得到广泛应用。
同时，天融信是中国信息安全测评中心授权的注册数据安全治理专业人员（CISP-DSG）运营机构，是首家且目前唯一一家运营机构，负责注册数据安全治理专业人员（CISP-DSG）专项证书的知识体系研发和维护、考题研发、考试服务、授权培训机构管理及市场推广等内容，助力国家培养数据安全专业人才。

风险提示

行业竞争加剧风险：网络安全行业竞争较为激励，如果行业行业竞争进一步加剧，或对毛利率产生不利影响。
政策力度不及预期风险：等保 2.0、护网行动等合规政策执行力度若不及预期，将影响企

事业单位对于网安产品及服务的需求。

宏观经济风险：疫情影响下，宏观经济面临下行风险，可能导致各行业企业网安支出受到影响。

测算可能与实际存在误差：目前隐私计算仍处于初始发展期，存在落地节奏及渗透不及预期风险。

免责声明

国盛证券有限责任公司（以下简称"本公司"）具有中国证监会许可的证券投资咨询业务资格。本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为客户。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。

本报告的信息均来源于本公司认为可信的公开资料，但本公司及其研究人员对该等信息的准确性及完整性不作任何保证。本报告中的资料、意见及预测仅反映本公司于发布本报告当日的判断，可能会随时调整。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。本公司不保证本报告所含信息及资料保持在最新状态，对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

本公司力求报告内容客观、公正，但本报告所载的资料、工具、意见、信息及推测只提供给客户作参考之用，不构成任何投资、法律、会计或税务的最终操作建议，本公司不就报告中的内容对最终操作建议做出任何担保。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。投资者应当充分考虑自身特定状况，并完整理解和使用本报告内容，不应视本报告为做出投资决策的唯一因素。

投资者应注意，在法律许可的情况下，本公司及其本公司的关联机构可能会持有本报告中涉及的公司所发行的证券并进行交易，也可能为这些公司正在提供或争取提供投资银行、财务顾问和金融产品等各种金融服务。

分析师声明

本报告署名分析师在此声明：我们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，本报告所表述的任何观点均精准地反映了我们对标的证券和发行人的个人看法，结论不受任何第三方的授意或影响。我们所得报酬的任何部分无论是在过去、现在及将来均不会与本报告中的具体投资建议或观点有直接或间接联系。

投资评级说明

投资建议的评级标准		评级	说明
评级标准为报告发布日后的 6 个月内公司股价（或行业指数）相对同期基准指数的相对市场表现。其中 A 股市场以沪深 300 指数为基准；新三板市场以三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）为基准；香港市场以摩根士丹利中国指数为基准，美股市场以标普 500 指数或纳斯达克综合指数为基准。	股票评级	买入	相对同期基准指数涨幅在 15%以上
		增持	相对同期基准指数涨幅在 5%~15%之间
		持有	相对同期基准指数涨幅在-5%~+5%之间
		减持	相对同期基准指数跌幅在 5%以上
	行业评级	增持	相对同期基准指数涨幅在 10%以上
		中性	相对同期基准指数涨幅在-10%~+10%之间
		减持	相对同期基准指数跌幅在 10%以上

国盛证券研究所

北京
地址：北京市西城区平安里西大街 26 号楼 3 层
邮编：100032
传真：010-57671718
邮箱：gsresearch@gszq.com

上海
地址：上海市浦明路 868 号保利 One56　1 号楼 10 层
邮编：200120
电话：021-38124100
邮箱：gsresearch@gszq.com

南昌
地址：南昌市红谷滩新区凤凰中大道 1115 号北京银行大厦
邮编：330038
传真：0791-86281485
邮箱：gsresearch@gszq.com

深圳
地址：深圳市福田区福华三路 100 号鼎和大厦 24 楼
邮编：518033
邮箱：gsresearch@gszq.com