计算机应用行业点评：安全事件与政策双驱动 千亿隐私安全产业加速

大数据加速应用与隐私保护政策双轮驱动隐私安全，短期以技术服务收入为主，中长期平台运营收入有望达千亿。据 Gartner 预测，2023 年底之前，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，到 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，而随着国内《数据安全法》等落地、各地数据交易市场快速发展，有望牵引隐私计算产业高速增长。

隐私计算助力数据价值挖掘，互联网巨头等合规需求迫切，同时数据协作需求推动隐私计算应用从政务、金融、医疗等向其他行业快速延伸，商业化速度显著加快。《数据安全法》实行在即，隐私数据安全将有法可依，互联网巨头及私域流量运营平台合规需求迫切，以联邦学习、多方安全计算、可信执行环境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，益处体现在：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；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。3）对于 G 端政府、社会机构，隐私计算可促进数据价值深度挖掘和社会福利最大化，打破各部门”烟囱式”信息系统。

典型的隐私计算场景通常包含三类参与方，考虑国内实际，未来有可能是由网信办等监管单位牵头平台建设，具备相关股东背景、技术储备的第三方企业提供通用技术模块，部分垂直行业或有平台商：（1）数据的使用方，需考虑业务特征与支付能力，如联邦学习联合建模的银行业、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。

隐私计算服务商通过搭建平台与运营来实现利润分成，以订阅服务收费模式作为盈利落脚，千亿赛道空间与优质商业模式有望诞生极具价值的投资标的，核心推荐兼具国资背景与过硬产品能力的卫士通。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，即依靠“DaaS+SECaaS”能力打开空间。随 IT 架构迈向云化，隐私计算服务或由云计算方式提供，广阔的市场空间与优质的商业模式奠定隐私计算赛道具备极强的可投资性，考虑到隐私安全监管对象，具备独立公信力的国资厂商更具优势。

隐私安全：卫士通、安恒信息、奇安信。

投资建议：奇安信、卫士通、安恒信息、天融信、启明星辰、深信服。

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