证券代码：002212　　证券简称：天融信

天融信科技集团股份有限公司

投资者关系活动记录表

编号：2026-003

投资者关系活动类别	□特定对象调研　□分析师会议 □媒体采访　□业绩说明会 □新闻发布会　□路演活动 □现场参观 √其他（投资者交流会）
参与单位名称及人员姓名	本次线上会议在线参会人员 35 人，详细名单信息请参阅文末附表。 因本次投资者关系活动采取线上会议形式，部分参会者无法签署调研承诺函。但在交流活动中，我公司严格遵守相关规定，保证信息披露真实、准确、及时、公平，没有发生未公开重大信息泄露等情况。
时间	2026 年 07 月 15 日 15:30-17:20
地点	天融信科技集团股份有限公司会议室
形式	线上会议
上市公司接待人员姓名	李雪莹：董事长、总经理 孔继阳：董事、副总经理、财务负责人 吴亚飚：职工代表董事 彭韶敏：副总经理、董事会秘书 孙　嫣：证券事务代表 杨　斌：高级副总裁 寇增杰：高级副总裁 雷晓锋：副总裁 马腾辉：副总裁

交流内容及具体问答记录	**一、公司情况介绍** **（一）2026 年半年度业绩预告数据说明** **1、主要经营数据** 2026 年上半年预计归属于上市公司股东的净利润亏损 24,000 万元至 29,000 万元，上年同期亏损 6,469.35 万元；扣除非经常性损益后的净利润预计亏损 25,500 万元至 30,500 万元，上年同期亏损 7,657.78 万元。 **2、净利润亏损原因** 1）收入规模下降：对净利润的负面影响占比约 80%；2）毛利率下降：对净利润负面影响占比约 20%。 **3、收入下滑原因** 核心因素：传统安全产品市场需求复苏不及预期。 其他因素：1）上年度结转订单同比减少；2）项目交付周期拉长；3）部分项目中标后签约滞后。 **4、毛利率下降原因** 1）原材料涨价：其中硬盘价格同比上涨 3－5 倍，内存价格同比上涨 7－8 倍，对硬件成本的影响较大；2）收入结构变化：智算云收入增长，占收入比重提升，但毛利率相对较低，拉低整体毛利率水平。 **5、收入结构** 传统安全产品收入下降，智算云收入及订单均实现同比增长。 **（二）2026 年上半年业务进展** **1、网络安全已经进入全新发展期** **1）AI 发展带来网络安全新需求** （1）AI 安全防护：大模型、智能体应用快速发展带来新的安全需求。 （2）智算基础设施安全：各行业智算基础设施大规模建设，带来智算云、智算数据中心新的安全需求。 （3）AI 产业链上下游企业安全：AI 产业链上下游众多企业信息化、数字化业务快速发展，带来大量新的安全需求。 **2）AI 安全市场规模** IDC 预测：AI 安全防护（中国）2025 年市场规模 44 亿元，占网络安全整体市场（中国）规模的 5.3%；2030 年预测 AI 安全防护（中国）市场规模

	340 亿元（复合年均增长率 50.5%），占网络安全整体市场（中国）规模的 24.28%。 Gartner 预测：AI 安全防护（全球）2025 年市场规模 15 亿美元，占网络安全整体市场（全球）规模的 0.7%；2030 年预测 AI 安全防护（全球）市场规模 164 亿美元（复合年均增长率 60.4%），占网络安全整体市场（全球）规模的 4.4%。 **2、面对网络安全全新发展期，公司已做好充足准备** **1）国外公司进展** （1）新时期海外安全市场回报已显现且成长空间巨大 ①Fortinet：2025 年营业收入 68 亿美元（同比增长 14%），防火墙占 55%。 ②Palo Alto：2025 年营业收入 92.2 亿美元（同比增长 15%），预计 2026 年增长 31%。 ③CrowdStrike：2025 年营业收入 39.5 亿美元（同比增长 29%），订阅收入 37.6 亿美元（同比增长 31%）。 （2）公司与 Fortinet、Palo Alto 的底层发展逻辑高度趋同 Fortinet、Palo Alto 的一些优势做法： ①AI 双轮战略：AI 赋能安全、AI 安全防护； ②顶层架构：一体化安全织网，边-云-端 三域打通； ③底层基座：以 NGFW 硬件为核心锚点，依托自研统一 OS，实现全域安全能力的调度与下沉； ④产品全栈覆盖：NGFW、大数据、云安全、工业互联网安全等布局完整，AI 能力的延伸落地。 **2）国外公司发展节奏** 战略进化路径：均经历“硬件→平台→AI 赋能→大模型驱动”四阶段。 （1）硬件设备时代：2005 年—2012 年，发展特点为“单点防护，性能为王”，Fortinet 代表产品 ASIC 防火墙，Palo Alto 代表产品 App-ID NGFW； （2）平台整合时代：2012 年—2018 年，发展特点为“统一调度，产品矩阵”，Fortinet 代表产品Security Fabric，Palo Alto 代表产品 Strata/Prisma/Cortex； （3）AI 赋能时代：2018 年—2023年，发展特点为“AI 作为工具，辅助

	人类”，Fortinet 代表产品 FortiAI 模块，Palo Alto 代表产品 Precision AI 插件； （4）大模型驱动时代：2023 年至今，发展特点为“智能体自主运营，人机协同”，Fortinet 代表产品FortiAI Agent 体系，Palo Alto 代表产品 Precision AI Agent。 **3）天融信 AI 安全进展** 核心优势：适配国内市场监管环境、全栈技术自主可控、全域信创深度适配、垂直行业深耕积淀、完备权威合规资质。 （1）战略定位：三大方向+双轮驱动 AI 赋能安全、AI 安全防护、AI 基础设施建设。 （2）顶层架构：天问大模型为核心的智能体矩阵 ①基座大模型：多年沉淀海量高质量安全数据，本地化开源模型训练； ②安全智能体层：6 大垂直场景智能体； ③工具/插件层：与 FW、IDS、SOC、EDR 等 50+品类产品联动。 （3）产品全栈：AI 能力延伸落地的完整矩阵 ①AI 赋能安全：NGFW、APT、入侵检测/防御、NGSOC、数据安全、云安全、工业安全等； ②AI 安全防护：大模型多模态安全防护网关、大模型漏洞扫描系统、API 安全审计系统、大模型数据安全监测系统、AI MSS 安全托管服务等； ③AI 基础设施建设：超融合、桌面云、企业云、智算云、安全智能体一体机等。 **4）对标国际，立足本土的 AI 安全能力体系** （1）安全运营：天问大模型产品的特点是告警降噪率 99%、安全策略秒级生成、漏洞自动修复时间缩短 90%；获得首批大模型产品安全性检测证书、首批安全大模型能力评估证书。 （2）安全评估：①大模型安全评估产品：特点是 AI 资产、内容安全、应用安全、语料安全等全面评估；在政府、运营商、公安、企业等多个客户开展测试和应用；②AI 安全服务产品：包括大模型安全评估服务、OpenClaw 安全评估服务、智能体安全评估服务；获得首批大模型安全服务能力评定资格证书、首批人工智能服务安全建设能力与人工智能服务安全检测能力最高

	级认证。 （3）安全监测：①大模型数据安全监测产品：特点是内置合规特征库、敏感数据监测库、攻击检测库，实现大模型全生命周期的数据安全风险监测；获得第三届“数信杯”数据安全大赛获评优秀案例征集赛银奖；②API 审计与防护产品：特点是 API 视角管理资产、发现漏洞、监控行为、识别敏感数据，实现智能体防护；获得首家数据安全产品检验证书、首批 OpenClaw 类智能体安全防护产品能力评估证书。 （4）安全防护：大模型安全网关产品的特点是文本、图像、音频、视频等多模态安全防护，实现对“执行者”的管控；获得首家网络安全产品认证证书（增强级）。 （5）内容安全：内容智能管控产品的特点是集成 AI 算法与边缘计算能力，监测文字、图片、视频等信息，识别违规内容；获得网络安全产品认证证书。 公司 AI 安全重点满足两类客户需求，已在多场景多行业落地： （1）合规市场需求：满足政务数据安全、算法备案、监管核查硬性要求，构建事前-事中-事后闭环合规体系。 （2）业务发展刚需：满足智算中心建设、制造业等行业业务发展需求，提供算力防护、智能体安全等 AI 安全能力。 **5）政策驱动需求，大单品抢跑先行** （1）API 审计与防护 ①政策：公安部发布《信息安全技术 网络安全等级保护数据安全基本要求》6 月 1 日正式实施，明确提到接口安全要求；国标《数据安全技术 数据接口安全风险监测方法》7 月 1 日正式实施。 ②重点行业及市场规模：政府、运营商、金融、教育、医疗、税务等各行业具有 API 安全防护建设合规需求。 ③公司进展：产品发布时间为 2025 年 12 月，已落单政府、运营商、教育、医疗、公安、企业等行业，全国 20 多个区域、13 个行业测试中，在途预计订单 1,200 万元左右。 （2）内容智能管控 ①政策：2023 年网信办发布《生成式人工智能服务管理暂行办法》；上

	海市公安局对上海辖区内公共电子屏安全提出明确要求，并制定地方标准进行落实。 ②重点行业及市场规模：政府、公安、交通、教育、医疗、广电、文旅等具有公共区域电子屏内容安全建设需求。 ③公司进展：产品发布时间为 2026 年 3 月，在途预计订单 2,500 万元左右。 **6）AI 增强安全，全栈 AI 内化** （1）边界安全：AI 防火墙，增强加密流量识别与防护、未知威胁检测与防护能力。 （2）安全检测：①APT 安全监测：内置九大 AI 智慧引擎，有效提升各类威胁检测效率与准确性；②智能网络审计：新增 OpenClaw 对大模型 API 的调用行为识别能力，降低智能体应用访问风险。 （3）安全运营：AI MSS，AI 能力贯穿“感知—分析—研判—响应—复盘”全链路，将安全响应时效缩短至分钟级。 （4）安全智能体：发布安全检测、安全评估、安全运营、数据安全、威胁情报、调查溯源、威胁分析、告警研判、攻击研判、pcap 分析、未知漏洞分析、钓鱼邮件分析、网关策略分析、网关策略优化、智能阻断、资产分析、代码审计、渗透测评、漏洞挖掘、漏洞验证、漏洞规则编写、传统知识问答、安全知识问答、漏洞问答、运维值守、安全设备评估、告警分诊等安全智能体。 **3、智算云，公司第二增长曲线** **1）智算云跻身千亿赛道** （1）IDC 数据显示，智算云高速发展，多行业算力需求爆发 ①2025 年下半年国内 AI IaaS 增速 132.1%，全年 486.7 亿元，预计 2030 年突破 2,000 亿元，推理算力将成为核心增量（复合年均增长率为 26.8%）； ②2026 年 Q1 超融合市场规模 5 亿美元，同比增长 14.1%，预计 2030 年 37.58 亿美元（复合年均增长率为 9.6%）； ③互联网企业、基建企业为算力基础设施主要采购主体，汽车自动驾驶、金融风控、智能投顾等新兴场景需求持续增长； ④制造业资金储备充足，数字化、信息化改造需求旺盛，行业算力投入

	规模已超过政府行业，位居首位； ⑤金融行业受国产化替换政策驱动，2026 年一季度算力采购需求集中释放； ⑥医疗、交通行业需求逐步回暖，政策推进省级数据平台建设。 （2）行业实施类政策密集发布，打开智算云落地空间 ①2026 年 1 月，《“人工智能+制造”专项行动实施意见》发布，智算云从通用算力向工业专属算力升级，加大工业算力建设投入，为公司超融合、智算云、安全智能体一体机带来市场机遇； ②2026 年 2 月，发布《关于组织开展国家算力互联互通节点建设工作的通知》，全国算力枢纽加大建设，打破算力孤岛，实现跨区域调度，为公司超融合、智算云、等保一体机带来市场机遇； ③2026 年 4 月，发布《普惠算力赋能中小企业发展专项行动》，算力超市/银行模式激活下沉市场，小微轻量化算力需求旺盛，为公司智算一体机、安全云服务带来市场机遇； ④2026 年 6 月，发布《“人工智能+信息通信”创新发展实施意见（2026—2028 年）》，运营商算力基建投入体量大，通算智算一体化底座，为公司超融合、智算云、商用密码带来市场机遇。 **2）国产化替代加速需求释放** （1）国产化替代 ①VMware：政企大规模国产化替代，规模百亿级，公司超融合、桌面云、安全网元获市场机遇； ②Nutanix：超融合+智算云融合架构替代，规模十亿级，公司超融合、智算一体机获市场机遇； ③Citrix：桌面云客户亟需国产化替换，规模数亿级，公司桌面云、终端安全获市场机遇。 （2）行业分布 ①互联网：智能算力占比 54.93%，通用算力占比 40.17%，核心应用场景包括大模型、短视频、电商推荐、游戏渲染、公有云、内容分发，预计算力需求稳定增长，推理算力占比持续提升； ②服务：智能算力占比 14.55%，通用算力占比 9.80%，核心应用场景包

	括数字文创、物流调度、元宇宙、供应链管理，预计智能算力需求快速增长； ③政府：智能算力占比 7.25%，通用算力占比 9.98%，核心应用场景包括智慧城市、政务云、大数据治理、电子政务，预计通用算力需求稳定，智能算力占比逐步提升，政务大脑建设带动算力增长； ④运营商：智能算力占比 6.84%，通用算力占比 14.40%，核心应用场景包括云服务、网络运维、算力调度、运营商云、边缘计算，预计通用算力需求稳定，智能算力占比不断扩大； ⑤制造：智能算力占比 4.09%，通用算力占比 4.69%，核心应用场景包括工业互联网、数字孪生、AI 质检、生产调度、工艺优化，预计大模型在工业场景规模化部署，算力需求爆发式增长； ⑥金融：智能算力占比 4.55%，通用算力占比 9.54%，核心应用场景包括智能风控、量化交易、反欺诈、信用画像、核心交易系统，预计智能算力渗透率持续提升，大模型应用带动算力需求快速增长； ⑦教育：智能算力占比 2.36%，通用算力占比 2.34%，核心应用场景包括 AI 教育、虚拟教学、教育大数据、校园信息化，预计算力需求稳步增长，AI 教育场景带动智能算力占比提升。 **3）公司产品精准匹配智算市场核心需求** 五大核心维度构筑差异化竞争力： （1）全域产品：超融合+桌面云+企业云+智算云+安全智能体一体机，四大产品矩阵+一体机构成全栈能力； （2）原生安全：三十余年网络安全龙头，安全内核原生注入云底座，原生安全区别于友商外挂模式； （3）一体管控：一站式解决智能体部署、算力调度、安全防护、运维协同，智能体运行全过程可见、可控、可管； （4）全栈国产：全面支持国产 CPU/GPU/NPU/DCU、操作系统、数据库，获自主原创测评认证； （5）多元交付：软硬一体/纯软两种模式，支持利旧服务器，平滑迁移，保护投资。 **4）公司智算云标杆落地，增长可期** （1）标杆项目

	①教育：纳管异构算力、统一管理、完备迁移替换方案； ②医疗：高性能分布式存储、VDI\VOI\IDV 三合一架构、容灾双活方案； ③政府：全栈国产化适配、内生安全能力、运维便捷； ④企业：通算与智算融合、灵活扩容、降低建设成本； ⑤金融：数据多副本、实时备份、容灾双活、高性能存储。 （2）下半年行业机会 ①教育：高校 AI 智算中心建设、VMware 替换及高职云桌面信创替代；公司在兼容国产异构算力，支持平滑迁移替换，算力、超融合、桌面云一体化交付等方面具有优势； ②医疗：医院 VMware 迁移替换、医疗 AI 算力持续扩容，医学影像场景增量稳定；公司在无感知在线扩容，高可用全闪存储、跨集群容灾，三合一桌面方案全面替换传统 PC 等方面具有优势； ③政府：信创国产化资源池建设、政务 AI 大模型算力建设、信创云桌面改造、政务智算建设；公司在全栈适配信创生态，原生安全，大模型合规防护等方面具有优势； ④企业：企业私有 AI 知识库/智算中心建设、研发场景云桌面建设、传统数据中心改造；公司在低成本灵活扩容、利旧老旧设备，全 AI 模型适配、支持智能体开发，研发数据不外泄等方面具有优势； ⑤金融：信创国产化资源池建设、VMware 迁移替代、核心业务容灾备份；公司在金融级高可靠架构、数据多副本保护，多路径平滑替代，存储深度优化、读写性能高等方面具有优势。 **4、深耕工业安全，拓展业务边界** **1）政策持续落地，有望迈入高景气赛道** 2024 年中国工业互联网安全市场规模 87.6 亿元，近五年复合年均增长率 22.3%，显著高于网安市场平均 13.2%。 2030 年市场规模有望突破 250 亿元，覆盖工信部 41 个工业大类中 30 余个高价值行业——赛迪顾问（CCID）。 三层政策约束体系： （1）顶层战略：“十五五”规划（2026）/2026 政府工作报告（2026），工业安全纳入国家核心布局，驱动从单点设备采购向体系化运营升级；

	（2）监管要求：关基保护条例（2021）/等保 2.0（2019）/工业互联网企业网络安全分类分级（2021）等，工业控制系统纳入安全保护合规体系，催生安全产品采购与迭代； （3）行业政策：电力监控系统安全防护规定（2024）/煤矿安全规程（2025）/船舶网络韧性要求 URE26（2024）等，将工业安全纳入项目建设硬性验收指标，推动安全与产业同步建设； （4）公司进展：公司已发布 6 大类 15 款全栈产品矩阵，已有规模化标杆案例可快速复制，全线成熟国产化产品适配，行业化产品快速适配产业需求。 **2）夯实重点行业，拓展新兴赛道** （1）重点行业市场结构：能源电力行业规模 28.47 亿元、石油化工行业规模 17.35 亿元、轨道交通行业规模 11.91 亿元、装备制造行业规模 7.71 亿元、其他（钢铁/烟草/水利等）行业规模共 22.16 亿元。 （2）新兴高增长行业： ①半导体：国内集成电路制造企业 6209 家、半导体封测企业 2.48 万家；晶圆厂 200 余家； ②商业航天：国内运载火箭企业 49 家、卫星制造与运营企业 493 家、上下游配套企业 115 家； ③海运船舶：国内规上造船企业 57 家（年产出 1,500-3,000 条各类型商用船舶）； ④海外市场：中国境内投资者共在全球 190 个国家和地区设立境外企业 5.2 万家、共建“一带一路”国家设立境外企业 1.9 万家。 **3）全栈国产化，AI 深度赋能** 6 大类 15 款产品，全栈国产化： （1）安全防护：产品有工业防火墙、工业安全隔离与信息交换、工业主机卫士，AI 赋能基于小模型实现流量与行为实时处置、实现工业物理信息的 AI 语义解析，其中工控网闸市场占比为 15.9%、工控防火墙市场占比为 9.4%； （2）安全监测：产品有工业入侵检测与审计、工业安全监测审计，AI 赋能基于小模型实现流量与行为实时检测、基于小模型的工业生产逻辑行为验证，其中工控 IDS 市场占比为 11.6%；

	（3）安全运维：产品有工业运维审计、USB 安全管理、工控安全服务（咨询、评估、应急响应、培训等），AI 赋能面向工业领域的辅助决策托管运维，其中工控安全服务市场占比为 22.8%； （4）安全检测：产品有工业漏洞扫描、工业安全检查工具箱，AI 赋能基于大模型的漏洞风险评估与辅助决策，其中工控漏扫市场占比为 13.7%； （5）安全管理：产品有工业互联网态势分析与管理、工业安全集中管理、工业日志审计，AI 赋能基于大模型的告警降噪与资产风险分级、基于大模型的专家辅助系统、安全事件-风险资产-运维管理自然人实时关联，其中工业网络安全态势感知市场占比为 10.8%、工控安全管理平台市场占比为 12.8%； （6）攻防实训：产品有工业互联网安全攻防演练靶场、工业互联网安全教育实训靶场、工业攻防演示试验箱，AI 赋能面向工业领域的攻击链识别与推理模型优化，其中工控靶场及蜜罐市场占比为 12.4%。 **二、交流环节** **1、公司业绩预告提到“传统网络安全产品需求复苏不及预期，但持续布局 AI 安全产品方案体系”，我们关注到北美以 CrowdStrike 和 Palo Alto 为代表，AI 赋能安全正在成为网安投资的核心叙事，IBM 也反馈客户 capex 正在转向基础设施和网络安全。请问公司目前在 AI 安全领域的产品布局有哪些具体落地案例？AI 安全相关收入何时能对公司整体收入产生显著拉动？** 答：1）对标国际、立足本土的 AI 安全能力体系打造：公司一直关注国外 AI 安全发展，围绕其整体趋势，近几年持续打造公司 AI 安全能力体系（即在整体运营平台下的评估能力、智能体安全能力、API 审计和防护能力、边界防护能力、监测能力、分析能力等一整套能力），然后将能力转化成产品、方案、服务。公司既关注 Palo Alto，也关注 Fortinet，不仅因为都是防火墙公司，还因为这两家公司面对的客户群不同，所采用的技术架构、交付模式有差异，而公司涵盖了这两家公司的不同客户群类型，因此在 AI 安全能力打造时，同时关注了这两类技术路线。 2）AI 安全大单品抢跑先行：公司选择了需求规模化的标准化产品作为大单品，快速交付，在全新市场快速切入，包括：大模型安全网关、API 审计和防护、内容智能管控。目前，这三个大单品在全国各省绝大部分行业都

	有需求产生，在运营商、金融、能源、教育、医疗等行业有落地。 3）关于 AI 安全收入对公司整体收入的拉动，收入增速一定很快，收入绝对规模和市场发展速度相关。 **2、深信服、奇安信等也在积极布局 AI+SASE、大模型安全等方向。在这个 AI 安全的新赛道上，请问公司的差异化竞争策略？公司在“数据安全+AI 安全”方向有哪些技术或客户？** 答：1）公司在 AI 安全赛道的差异化竞争策略： （1）AI 安全的体系架构差异：公司具备一整套从底层往上延伸的完整架构（从底层架构，到算力，到云平台，到安全能力，到大模型，AI 安全的延伸）。 （2）从架构落实到产品、方案的技术路线差异：①针对大模型应用的多模态 AI 安全，公司在业内首发，源于技术上的前瞻布局和落地。②公司具备硬件研发能力（如硬件加速卡等），软硬协同，国内具备这种能力的安全公司为数不多。③公司自研安全能力最全，因此安全智能体能全域管理。 （3）已有客户群积累和商业模式差异：公司已有客户群既覆盖大行业、关基客户，也覆盖中型企业客户，双轮驱动。面向大行业、关基客户，公司以直销方式提供原厂 AI 安全，该商业模式需要厂商具备从产品、方案到服务的完整体系能力，以及对行业客户需求的深度了解；面向中型企业客户，公司以渠道方式覆盖，已具备一定合作伙伴基础，能提供标准化、偏轻量级 AI 安全产品。 2）在“数据安全+AI 安全”方向，公司已构建覆盖大模型全生命周期的数据安全技术体系，包括内置合规特征库与敏感数据监测库的大模型数据安全监测系统、数据脱敏及提示词注入防护等。API 审计与防护系统为国内首家通过中国信通院检验的同类产品，已在全国 20 余个区域、13 个行业完成测试并成单；内容智能管控已落地教育、医疗等行业；数据安全产品已在国企、航空、运营商等场景深度应用，并获“数信杯”数据安全大赛银奖，形成了从训练数据防护到 API 交互再到内容管控的 AI 数据安全完整体系。 **3、随着 AI 在企业更多以智能体形式落地，会带来哪些新的安全风险？**

	公司是否有智能体安全产品布局和储备，后续是否有可见放量和收入指引？ 答：1）智能体的安全：主要涉及 Agent 身份认证、工具调用白名单、最小权限控制、关键操作审批等，重点防范 Agent 越权访问系统、执行危险命令等安全风险。 2）公司智能体安全产品布局和储备：（1）Agent 统一安全入口方面，推出了大模型安全网关、大模型 API 审计与防护等产品，解决提示词注入、越狱攻击、违法违规内容、隐私泄露以及模型调用、接口滥用等安全问题，为 Agent 与大模型交互提供统一安全防护能力。（2）在 Agent 执行层面，公司的大模型 API 审计与防护产品首批通过中国信通院组织的智能体安全防护产品能力评估；公司大模型安全网关产品部署于 Agent 与大模型之间，可对 Agent 身份、行为以及最小权限执行情况进行实时检测与防护。（3）公司大模型安全评估产品、大模型数据安全检测产品也已支持智能体安全场景。随着企业 Agent 应用不断增加，针对 Agent 的安全防护已成为公司产品设计的重要考虑内容，各产品都会结合自身定位持续完善相关安全能力。 3）智能体安全业务进展及市场展望：（1）在智能体安全领域，公司目前已有部分项目落单，主要涉及安全评估服务、API 审计与防护、大模型安全网关等产品和服务。从现有项目的落地形态来看，部分客户将大模型安全与智能体应用安全进行一体化规划和建设，部分客户则从单点能力切入，主要部署 API 审计与防护产品。（2）从市场需求看，尤其是近两三个月，公司已明显感受到客户对智能体安全的关注和需求提升。具体产出方面，公司会在半年报中披露统计后的 AI 安全收入，从全年趋势看，公司预计该业务将快速增长。 **4、相对于传统的数据中心，请问智算中心对安全需求的异同？请问公司面向智算中心的安全业务进展？** 答：智算中心的安全需求，在传统安全底座基础上扩展增加了数据与模型安全、AI 应用安全、算力网络安全。传统数据中心业务模型的防控基础是“主机-网络-应用-数据”，智算中心在此基础上，增加了对模型资产、AI 服务链、GPU 集群、高速算力网络的保护，主要体现在：1）核心保护对象的增加，较传统数据中心增加了训练数据集、模型、向量库、推理结果、GPU 算

	力。2）主要的攻击面有变化，除了传统的漏洞利用、横向移动、数据泄露，还增加了模型的窃取、训练数据的投毒、提示词注入等攻击。3）流量特征发生重大变化，训练中会产生超大规模的东西向流量。4）在安全运营上，智算中心增加了“用户-数据-模型-算力-输出”的完整调用链，和传统安全运营关心的用户 IP 端口行为不同。 公司在智算中心安全业务上，以“安全原生”差异化切入，将安全能力直接注入智算云的底座。发布太行云 5.0，同时推出大模型安全网关（国内首家获得大模型围栏产品的增强级认证）；推出大模型的 API 审计与防护、大模型安全评估产品，已在教育、医疗、政务等行业落地。 **5、国外大模型公司与网安厂家合作，以及对安全公司业绩的带动，在国内是否有类似的趋势和机会？请问 AI 安全收入兑现的后续节奏预期？** 答：1）国外“大模型厂商+安全厂商”协同已成验证路径，Anthropic 与 Palo Alto 联合开展 Project Glasswing、OpenAI 能力深度嵌入微软 Security Copilot，均显示 AI 安全对网安公司业绩的显著拉动。国内趋势类似但路径存在差异：大模型备案、算法备案等合规要求必须由独立第三方完成，这为网安厂商创造了大模型厂商无法覆盖的“外部合规”刚需市场，另外国内与国外的重要差异是国内大模型开源，公司也与国内主流大模型厂商保持密切交流。 2）国外安全厂商 2025 年收入增长主要来源于两方面：（1）AI 应用快速发展带来了新的安全风险和安全需求，AI 安全形成了新的市场增量；（2）AI 增强后的安全产品能够更好地解决传统安全问题，部分客户会采用技术能力更好、更新的产品替代原有产品，以提升整体安全防护水平。 从国内来看：（1）对于 AI 应用发展带来的新增安全需求，市场正在逐步意识到相关需求，但从意识转化为采购行为，会是一个缓释过程。目前该需求增长速度较快，由于市场基数相对较小，短期内还难以形成快速放大的市场，但未来发展到一定阶段后，市场有望呈现“荷花效应”。（2）对于 AI 增强型安全产品替代传统安全产品带来的市场增量，国内客户主动替代行为较国外滞后，相关市场增量预计不如国外市场，会是一个缓释过程。

	6、请问公司在抗量子密码方面的业务布局？公司了解到国内抗量子密码标准未来的落地节奏如何？ 答：1）目前，国内外已出现一些量子计算机原型，对现有密码体系构成一定挑战。现有密码体系中使用的一些椭圆曲线等密码算法，未来可能较容易被量子计算攻破。此外，目前国内外学界认为，即使当前还无法破解密文，也可以先将所有密文存储下来，待未来量子计算机成熟后再进行破解。因此，后量子密码已经提上日程。 2）公司已做好相关技术准备。抗量子密码的基本思路，是采用量子计算机不擅长求解的数学问题进行密码设计。公司参考了国际上的一些论文和技术实现，已将常用的一些 PQC 密码算法率先实现在公司的 VPN 产品中，并完成原型验证，以验证相关密码算法的可行性。未来在主管机关批准 PQC 算法后，公司将在统一的技术框架下，为所有有需要的产品提供抗量子能力，包括身份认证、密码服务器以及各类数据加解密等方面。 3）关于国内标准落地进度，据公司了解，目前主管机关仍在评估 PQC 的可行性及具体实施时间。量子计算机对现有密码体系的破解风险已经迫在眉睫，预计相关工作推进时间不会太长，具体仍需等待主管机关决定。 **7、请问国内是否进入防火墙更新换代的时间节点？传统网安产品的后续业绩趋势展望？** 答：1）国内防火墙市场正处于规模信创替代加速期与早期信创产品更新换代周期叠加的节点。2022 年政策明确央国企 2027 年完成 100%信创替代，当前已进入冲刺阶段；金融、运营商、能源等八大行业的存量防火墙正在向国产 CPU 与国产操作系统全栈重构，目前正在加速进行。另一方面，2019 至 2021 年政府领域首批信创部署的防火墙已步入 3 至 5 年自然更新换代周期。在存量替换需求与新增信创建设形成双重叠加下，构成未来 2 年确定的采购需求。 2）传统网安产品业绩将呈结构性分化：传统边界防护增速放缓，但信创防火墙、信创主机安全等国产化替代产品还处于政策红利释放期，未来 2 至 3 年还会保持增长。具备全栈国产化适配能力、且在政府与关键行业有深度交付经验的厂商，将在此轮更新中占据核心份额。

	综上，国内防火墙市场已明确进入以信创替代为主线的更新换代窗口，存量更新与八大行业增量渗透双轮驱动，具备全栈信创资质和行业纵深壁垒的厂商订单确定性最强。 **8、公司业绩预告提到“传统网络安全产品需求复苏不及预期”，请问哪些下游行业表现较好，哪些下游行业相对较弱？** 答：医疗、教育、企业、能源、金融、运营商行业表现较好，政府行业（尤其是地方政府）表现相对较弱。 **9、今年上半年原材料涨价造成毛利率下降，请问该因素对公司目前影响程度，如何展望全年毛利率？** 答：上半年毛利率下降主要受两方面影响：1）存储元器件价格涨幅巨大（呈数倍上涨），对上半年毛利率的影响已体现，对下半年及全年影响或将进一步扩大；2）产品结构方面，上半年毛利率较低的智算云业务持续增长，收入占比提高，进一步降低整体毛利率。 **10、在当前亏损扩大的阶段，公司在 AI 安全等新方向的研发投入强度是否会调整？短期保利润和长期抢 AI 安全赛道之间的平衡策略是什么？** 答：1）公司前期在 AI 安全方面已完成前置布局和较强研发投入，已陆续发布多款 AI 安全产品，并在多个行业落地。2）未来公司会根据技术发展和行业需求，进一步加大 AI 安全的研发投入。3）在短期利润和长期抢 AI 安全赛道之间，抢 AI 安全赛道是公司的首要选择。 **11、公司智算云业务收入及订单保持上行，但传统安全业务仍承压。请问公司今年上半年整体订单情况及全年预期？** 答：1）公司今年上半年新增订单同比持平略增，去年结转至今年的订单同比减少，截至上半年末，公司未交付、未确认收入的在手结余订单高于去年同期。2）如果传统安全产品业务逐步恢复，AI 安全等新产品快速放量，全年订单可期。
关于本次活动是否涉及应披	本次活动不涉及应披露重大信息。

露重大信息的说明	
活动过程中所使用的演示文稿、提供的文档等附件（如有，可作为附件）	无

附表：参与单位及人员名单（按参与单位名称首字母排序）

序号	参与单位	人员姓名
1	IGWT Investment	廖克銘
2	Oxbow Capital Management (HK) Limited	刘金清
3	博时基金管理有限公司	张锦
4	光大证券	李海强
5	广东南洋电缆股份有限公司	曾钦武
6	国投证券	夏瀛韬
7	国投证券	王永彬
8	国信证券	库宏垚
9	国元证券	耿军军
10	华创证券	胡昕安
11	上海度势投资有限公司	顾宝成
12	上海汇正研究所	刘勇
13	上海君璞投资咨询有限公司	刘欢
14	上海君璞投资咨询有限公司	高翔
15	上海润义投资管理有限公司	陆懿晨
16	申万宏源发展成都股权投资管理有限公司	马可
17	深圳市鲲鹏恒隆投资有限公司	彭飞虹
18	深圳市尚诚资产管理有限责任公司	黄向前
19	深圳市鑫融长弘投资管理有限公司	戴溪
20	深圳市裕晋私募证券投资基金管理有限公司	张恒
21	天风证券	王祺深
22	西安江岳私募基金管理有限公司	吕政和
23	信达证券	姜佳明
24	兴业证券	蒋佳霖
25	长城证券	黄俊峰
26	中电产融私募基金管理有限公司	房海强
27	中金公司	韩蕊

序号	参与单位	人员姓名
28	中金公司	梁善晴
29	中国人保资产管理有限公司	孔文彬
30	中泰证券	李霓
31	中泰证券	王雪晴
32	中泰证券	边金鑫
33	中信建投证券	李楚涵
34	中信期货有限公司	魏巍
35	中信证券	潘儒琛