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：2026-006

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
参与单位名称及人员姓名	参加广东上市公司协会举办的“2026 人工智能产业上市公司集体路演与投资者交流会”的投资者。 因本次活动为集体路演与投资者交流会，参会者未签署调研承诺函。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 09 月 23 日 09:00-12:00
地点	广州凯旋华美达大酒店三楼会议厅
形式	现场会议
上市公司接待人员姓名	雷晓锋：副总裁
交流内容及具体问答记录	**一、公司介绍** 天融信是中国网络安全领军企业，创始于 1995 年，亲历中国网络安全产业的发展历程，为全行业客户提供网络安全、智算云产品服务及综合解决方案。 积淀深：国内网络安全上市公司中成立最早； 可信赖：国内防火墙连续 26 年市场排名第一； 能力全：国内网络安全公司自研产品线最全。 当前核心业务为网络安全与智算云。

二、公司重点业务

（一）AI 安全已经进入全新发展期

1、AI 安全发展机会

1）市场规模：爆发式增长，千亿级增量空间显现

（1）Gartner 市场预测（全球）

AI 赋能安全：2026 年为 485 亿美元，2030 年为 2,044 亿美元，五年复合增长率为 53%；

AI 安全防护：2026 年为 28 亿美元，2030 年为 164 亿美元，五年复合增长率为 60.4%。

（2）IDC 市场预测（中国）

AI 赋能安全：2026 年为 43 亿元，2030 年为 593 亿元，五年复合增长率为 106.5%；

AI 自身安全：2026 年为 65 亿元，2030 年为 340 亿元，五年复合增长率为 50.5%。

2）核心驱动力：风险共识与政策红利双轮驱动

（1）事件驱动：风险共识加速形成

①Anthropic CEO 呼吁放缓前沿大模型迭代，模型能力提升速度远超安全治理能力。

②OpenAI 智能体越狱攻击事故曝光，多个 AI 智能体突破隔离。

③Kimi K3 利用测试环境中的网络配置漏洞突破了原本的限制。

④OpenClaw 安全风险集中暴露，监测发现 500+漏洞。

（2）政策护航：顶层设计持续完善

①国务院：《关于深入实施“人工智能+”行动的意见》

②国家网信办等七部门：《生成式人工智能服务管理暂行办法》

③工信部：《关于开展人工智能应用服务商培育专项行动的通知》

④强制性国标《智能体应用安全基本要求》立项

3）AI 安全属于典型的“荷花效应”，增长快、确定性高、集中爆发的新赛道。

2、国外网安公司 AI 安全业务进展

1）Palo Alto Networks：AI 赋能的安全防护平台

	（1）AIRS 突破 1 亿美元； （2）AI 安全运营突破 7 亿美元； （3）2026 年整体营收 115 亿美元，增长 24%。 2）Fortinet：AI 驱动的统一安全架构 （1）AI 安全运营订单 6.7 亿美元； （2）2026 年度预计整体营收 80 亿美元，增长 19%。 3）CrowdStrike：AI 原生的端点安全防护 AIDR 意向订单 5,000 万美元，增长 250%。 4）新时期海外安全市场回报已显现且成长空间巨大，天融信与 FT、PA 的底层发展逻辑高度趋同。 **（二）面对 AI 安全全新发展期，我们已经做好了充足准备** **1、天融信 AI 安全进展** 1）战略定位：四大方向+双轮驱动 AI 安全防护、AI 赋能安全、AI 安全运营、AI 基础设施建设 2）顶层架构：以天问大模型为基座的智能体体系 （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：7 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）全栈产品：AI 安全能力全域布局 （1）AI 安全防护：大模型安全网关、大模型安全评估、API 安全审计与防护、大模型数据安全监测等； （2）AI 赋能安全：NGFW、APT、IDPS、NGSOC、数据安全、云安全、工业安全等； （3）AI 安全运营：天问大模型、AI MSS 安全托管服务、智能体安全评估服务等； （4）安全智能体：安全运营、安全检测、安全合规、数据安全、代码安全等； （5）AI 基础设施建设：智算云、安全智能体一体机、超融合、桌面云、企业云等。

	（6）公司具有全栈自主可控、全域信创适配、行业深厚积淀、权威合规资质。 **2、AI 安全防护-增量市场** 1）大模型安全网关 大模型、智能体安全管控。多模态、软件、硬件、国产化。获得首家网络安全产品认证证书（增强级），在政府、能源、教育等行业落地。 2）API 审计与防护 智能体管控。看清家底、看穿漏洞、看懂调用、看住数据。获得首批 OpenClaw 类智能体安全防护产品能力评估证书，在运营商、公安、医疗等行业落地。 3）大模型数据安全监测 大模型全生命周期数据安全监测。获得 2026 年度北京网络空间安全协会科学技术奖（WAL 奖）二等奖，在航空、环保、科研机构等行业落地。 4）大模型安全评估 大模型、智能体安全评估。入选《IDC Market Scape 中国生成式 AI 的安全评估平台 2026 年厂商评估》，在运营商、航空等行业落地。 5）2026 上半年，公司 AI 安全防护业务营收同比增长超过 130%。 **3、AI 赋能安全-提升竞争力** 1）AI 防火墙 获得公安三所检测报告。增强加密流量识别与防护、未知威胁检测与防护。 2）APT 安全监测 获得网安三新认证。九合一集成 AI 引擎、全链条攻击溯源、全流量留存。 3）自动化渗透测试 获得网专认证。智能攻击编排、人机协同研判、可审计可管控。 4）内容智能安全 获得网络安全产品认证。多模态 AI 识别、内容+网络双重防护、公共安全领域新市场。

	5）市场机会 AI 攻击门槛降低，安全防护能力亟需提升；Palo Alto、Fortinet 等国产化替代市场机会；第一批已部署的国产化产品更新换代。 6）2026 上半年，公司 AI 赋能安全业务直接收入超过 8,000 万元，收入占比持续提升。 **4、AI 安全运营-降低运营成本** 1）天问大模型 安全策略秒级生成，告警降噪率 99%、漏洞修复时间缩短 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）AI MSS 毫秒级告警分析，分钟级安全响应。七大安全智能体自动威胁溯源、攻击链还原、风险研判、安全策略调优。 3）智能体安全评估服务 覆盖 9 个维度、39 项通用标准化检查项，主流 Agent 专项检测清单，Skills 插件/MCP 服务专项。获得首批人工智能服务安全建设能力、人工智能服务安全检测能力最高级认证。 4）大模型安全评估服务 全栈多维度评估框架，自动化测评平台+专家渗透双引擎。获得首批大模型安全服务能力评定资格证书。 **5、重点领域大单品-市场规模大** 潜力爆款标准化单品：典型场景案例覆盖。 合规刚需强、适配行业多：试点及落地项目可复制。 1）大模型安全网关 典型场景：大模型私有化部署、智能办公、智能客服、AI 编程等。 公司业务进展：智算企业、政府、教育等项目落地。 2）API 安全审计与防护 典型场景：应用接口资产管理、接口安全监测、接口访问审计等。 公司业务进展：政府、电信、教育、医疗、公安等落地实践。 3）AI MSS 典型场景：①运营商、部委：数据安全要求高，本地化运营；②教

育、医疗、地方政府、中小企业：能力及资源有限，云端运营。

公司业务进展：教育、医疗、政府、企业等行业落地。

4）内容智能安全

典型场景：政府-政务展板；教育-室外大屏；医疗-公共大屏；交通-高速展板。

公司业务进展：高校、交通、政府等项目落地

（三）智算云，公司第二增长曲线

1、智算云跻身千亿赛道

1）市场规模：IDC 数据显示，AI 算力市场进入千亿级爆发期

（1）2025 下半年国内 AI IaaS 增速 132.1%，2025 全年市场规模 486.7 亿元，2030 年预测规模突破 2,000 亿元（复合年均增长率 26.8%）。

（2）2026 年 Q1 超融合市场规模 5 亿美元，同比增长 14.1%，2030 年预测规模 37.58 亿美元（复合年均增长率 9.6%）。

（3）核心驱动力

推理算力将成为核心增量；互联网、基建企业为主采购主体，自动驾驶、金融风控、智能客服等新兴场景需求持续释放。

2）市场机会：三大替代窗口，带来广阔市场空间

（1）Vmware：政企大规模国产化替代，百亿级市场规模，公司在超融合、桌面云、安全网元方面有市场机遇。

（2）Nutanix：超融合+智算云融合架构替代，十亿级市场规模，公司在超融合、智算一体机方面有市场机遇。

（3）Citrix：桌面云客户亟需国产化替换，数亿级市场规模，公司在桌面云、终端安全方面有市场机遇。

2、智算云-全栈一体化能力

从算力底座到安全防护，天融信提供全栈一体化智算云解决方案。

1）智算云平台

全栈集成轻量可扩展、通算与智算深度融合、异构算力统一调度、全栈内生安全能力。

2）超融合

多云异构、多引擎统一管控；一云多芯、200+兼容认证；18 类 52 款

	安全网元。 3）桌面云 自研 TADP 体验流畅、信创全栈适配、安全能力深度融合。 4）安全智能体一体机 分钟级部署、智能体一键上岗；全生命周期可视化管理；全栈内生安全能力；配套评估与运营。
关于本次活动是否涉及应披露重大信息的说明	本次活动不涉及应披露重大信息。
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