证券代码：002212　　证券简称：天融信　　公告编号：2023-021

天融信科技集团股份有限公司 2022 年年度报告摘要

一、重要提示

本年度报告摘要来自年度报告全文，为全面了解本公司的经营成果、财务状况及未来发展规划，投资者应当到证监会指定媒体仔细阅读年度报告全文。

所有董事均已出席了审议本报告的董事会会议。

非标准审计意见提示

□适用 ☑不适用

董事会审议的报告期利润分配预案或公积金转增股本预案

□适用 ☑不适用

公司计划不派发现金红利，不送红股，不以公积金转增股本。

董事会决议通过的本报告期优先股利润分配预案

□适用 ☑不适用

二、公司基本情况

（一）公司简介

股票简称	天融信	股票代码	002212
股票上市交易所	深圳证券交易所		
联系人和联系方式	董事会秘书	证券事务代表	
姓名	彭韶敏	孙嫣	
办公地址	汕头市珠津工业区珠津二街 1 号大院内	北京市海淀区西北旺东路 10 号院西区 11 号楼东侧	
传真	010-82776677	010-82776677	
电话	0754-87278712	010-82776600	
电子信箱	ir@topsec. com. cn	ir@topsec. com. cn	

（二）报告期主要业务或产品简介

1、公司主营业务、主要产品及用途

1）主营业务：公司长期坚持自主创新、开放融合的发展理念，基于下一代可信网络安全架构 NGTNA（Next-Generation Trusted Network Architecture），以网络安全为核心、大数据为基础、云服务为交付模式，形成全面感知、智能

协同、动态防护、聚力赋能的综合安全保障体系。公司围绕网络安全、数据安全、云计算三大领域，构建全系列产品与服务，为各行业客户业务安全和可持续性运行赋能。

（1）网络安全：公司提供全系列网络安全产品，涉及边界安全、安全检测、接入安全、端点安全、应用安全、无线安全、安全管理等领域，覆盖所有网络安全场景，包括防火墙、VPN、入侵检测、入侵防御、病毒过滤网关、应用安全网关、Web 应用防火墙、加密机、网闸、上网行为管理、负载均衡、抗 DDoS、僵木蠕监测、高级威胁检测、流量分析、主机监控与审计、EDR、智慧无线管理、堡垒机、漏洞扫描、日志审计、安全管理、SD-WAN、零信任等产品，可为各行业客户提供全面的网络安全产品和解决方案。

（2）数据安全：公司在数据安全领域深耕多年，积累了丰富的数据安全管理经验，率先提出“以数据为中心的安全建设体系”的建设思路，形成了一套“以数据安全治理为基础、数据安全全生命周期监管、数据安全技术手段防护”的数据全生命周期的解决方案，为客户打造具备识别、防护、检测、响应、恢复闭环能力为一体的纵深数据安全防御体系。推出了数据安全智能管控平台、数据分类分级、数据脱敏、网络数据防泄漏、终端数据防泄漏、大数据安全防护、数据库审计、数据安全治理咨询、数据安全体系建设、数据安全合规评估等 20 余款数据安全类产品及服务，并广泛应用于政府、运营商、能源、金融等多个行业。

（3）云计算：公司持续加大云计算研发投入，依托深厚的技术积累和研究成果，发布了集网络、计算、存储、安全一体的天融信太行云企业解决方案，提供超融合、桌面云、云存储、云灾备、云容器、云安全、云管理等能力，满足各行业差异化需求，帮助客户建设边缘云、私有云、混合云等全场景全栈的云平台，截止报告期末共发布 12 类 38 款安全网元。云存储方面，支持构建云双活容灾和云主备容灾，本地备份、异地备份、快照、CDP 持续数据保护等多种数据备份方式，全方位保障业务数据安全。另外，在云安全方面，公司围绕安全云化、云内生安全、云环境安全，发布了虚拟化分布式防火墙、云安全资源池、API 安全网关、自适应安全防御系统、云 WAF、云抗 D、云安全管理平台、云原生容器安全、API 应用安全等产品，当前已经在运营商、政府、能源、医疗等多个行业取得了大量落地实践。

2）重点领域：公司面对企业数字化转型过程中的新技术、新热点、新场景、新趋势持续探索，发力信创推进全面国产化，布局大数据与安全运营助力服务化，融合工业互联网、物联网、车联网新场景，采用人工智能技术实现安全能力智能化。

（1）信创：公司始终坚持走自主创新之路，积极推动国产化网络安全生态建设。公司网络安全产品与国产 CPU、操作系统、数据库、浏览器、中间件等完成全面适配，已取得 1700 余项兼容性认证证书。公司已推出了涵盖边界安全、安全接入、安全检测、安全审计、安全管理、数据安全、工控安全、云安全、端点安全、云计算等多个细分领域的“天融信昆仑”系列产品，为客户提供完整的网络安全解决方案。核心产品包括防火墙、VPN、WAF、网闸、单向导入、加密机、安全准入、IDS、IPS、抗 DDoS、漏洞扫描、网络审计、数据库审计、运维安全审计、主机审计、服务器审计、EDR、打印刻录审计、安全登录、安全管理、态势感知、日志审计、数据脱敏、数据防泄漏、数据备份与恢复、文件监测等 63 类网络安全产品。

（2）大数据与安全运营：基于大数据技术，公司发布了态势感知、大数据分析、智能内网威胁分析、风险探知等产品，公司安全云服务中心具备线上、线下安全服务能力，为客户提供多元场景下的安全运营模式。在产品技术方面，态势感知平台从指挥调度、安全监测、安全分析、态势分析、策略管理和安全运营等多个维度为各类业务场景构建基于数据中台的安全运营系统；大数据分析平台基于大数据、机器学习等技术，提供安全场景分析、告警画像分析、安全响应编排（SOAR）、威胁狩猎等能力，提升安全运营效率；智能内网威胁分析（UEBA）系统依托大数据分析平台架构，以发现异常行为为核心目标，捕捉内网行为异常变化，发现潜伏在内网高级威胁；风险探知系统帮助客户绘制资产基础信息底图，全面、准确掌握所辖网络中资产、应用情况和安全状态。安全云服务中心依托遍布全国的探测、监测分析引擎集群，结合安全专家团队 7×24 小时云端值守，提供互联网暴露面检测、风险监测、攻击防护、威胁分析于一体的订阅式线上安全服务；通过“事件响应、红蓝对抗、威胁狩猎、情报预警”四轮驱动，为客户提供安全运营类、咨询保障类、红蓝对抗类、安全集成类、新技术测试类、行业专项类六大类线下安全服务。

（3）工业互联网、物联网、车联网：在工业互联网安全方面，公司率先提出以生产过程“行为基线”为基础，白名单策略为核心判断依据，黑名单策略为辅助验证手段的核心理念，推出包括工控防火墙、工控网闸、工控主机卫士、工控入侵检测与审计、工控安全监测审计、工控日志审计、工控堡垒机、工控漏洞扫描、工控安全检测工具箱、工控态势感知、工控集中管理、攻防演示试验箱 12 类专用产品。在物联网安全方面，公司以物联网安全管理中心为核心，从云、数据、应用、网、边界、端六维构建安全、可信、合规的一体化物联网安全纵深防御体系，推出物联网安全接入网关、物联网视频

上云网关、物联网安全标识管理、物联网安全管理平台、物联网使能平台、视频安全监测与分析、视频安全审计、视频数据防护、无人机反制系统等 12 类物联网安全产品。在车联网安全方面，针对智能网联汽车及网络关键设备，推出车载防火墙、车载入侵检测、车内认证加密、车联网安全态势感知等系列车载安全产品；针对车联网平台及应用，通过建设车联网安全运营中心、车联网数据安全管控平台、车联网安全合规检测平台，提供全方位、多手段、深融合的安全保障。

（4）AI 网络安全：公司在恶意样本、风险信息、威胁知识、安全情报等方面具有多年的安全数据积累，从 2019 年起，应用 AI 技术，陆续发布了融入 AI 技术的防火墙、入侵防御、僵木蠕监测、沙箱、大数据分析、态势感知、EDR、数据防泄漏、智能内网威胁分析等多款创新型产品。基于大模型技术，在恶意样本检测与分析、攻击行为发现与溯源、安全情报推理与生成、自动化漏洞挖掘与评估、智能化安全服务与运营等方向形成了丰富技术成果。

表 3-1　报告期内公司发布的主要产品/版本

业务领域	产品/版本名称	产品/版本更新与创新
网络安全	Smart 防火墙	采用国产硬件平台，具备三权分立，满足小型网络或单点安全防护、国产化和分保合规要求。
	擎天六防火墙	基于 7U 机框设计，支持双主控板、双业务板、三块交换板，可实现全威胁吞吐 200Gbps，能满足大流量场景下对高性能、高安全、高稳定和易扩展的需求。
	SD-WAN 边缘安全网关	增强了接入认证和零配置上线能力，提升了 IPSec 隧道并发和吞吐性能以及整机处理性能，满足对广域网快速、灵活、高性价比的接入和组网需求。
	新一代入侵防御	新一代智慧引擎全面升级，增强系统检测能力，增加 SSL 通用证书卸载、国产化飞腾及海光平台、IPv4/IPv6 双栈和多路检测防御能力。
	服务器密码机	采用国产密码算法，具备密钥管理、数据加解密、完整性校验、签名和验证等功能，保证数据的机密性、完整性和有效性。
	Web 应用防火墙	专为特殊场景的 Web 安全防护而研发设计，增加 XML 防护、扫描器防护、威胁可视化等功能，并且提升产品处理性能。
	新一代网络审计	基于开放性的系统架构及模块化设计，新增网络协议审计的深度和细粒度，同时丰富协议审计类型，优化了日志和报表的展示效果。
	安全隔离与信息交换	增加了文件客户端同步、安全 MD5 校验、Oracle RAC 集群、音视频 GB28181 协议以及相关安全过滤功能，优化了设备的业务处理能力和安全能力。
	主机监控与审计	增加了软件仓库、多系统统一管理、级联一体管理、服务端解耦、资产管理等功能，优化了系统并发量以及日志数据处理性能和报表展示功能。
	基线管理	增强了配置审计、弱口令检测等多种功能，同时对 UI 界面进行全面升级，并支持扩展运营商、金融、能源等多个行业的安全配置核查知识库。
	网络接入控制系统	支持无线准入和有线准入，提供多种准入模式，能在复杂网络环境中实现混合准入，以达到对终端接入网络的认证、检查、管控等效果，实现终端入网可信的目标。
	策略集中管理系统	基于自主操作系统研发，增强了对防火墙、VPN 等安全设备及策略的集中管控能力，提升了系统的处理性能。
	网络流量分析审计	基于大数据分析架构，具备资产发现管理、安全事件检测、系统性能监控、历史数据回溯等多维度、全流量的监控分析能力。
	流量汇聚分流器	具备高密度接入能力，并搭载国产化芯片，集汇聚分流、负载均衡、安全控制、可视化管理等功能于一体，为客户提供便捷高效的数据采集解决方案。
	病毒过滤网关	支持深度病毒检测引擎和快速病毒检测引擎，新增了加密流量的病毒检测功能以及与防火墙的联动功能，增强了访问控制、流量管控、抗 DDoS 等网络防护能力。
	新一代 VPN	增强了日志管理功能和身份认证校验能力，优化了系统诊断和域名校验规则，提升了 IPSec 隧道通信上传及下载速度。
	终端威胁防御	增强了主动防御、威胁监控、对终端软件应用的信息收集等功能，同时针对国产化终端进行适配升级，实现统一管控。
数据安全	网络数据防泄漏	优化检测算法、事件分析和搜索功能，增强检测能力和应用协议识别能力，增加对国产化硬件的支持。

业务领域	产品/版本名称	产品/版本更新与创新
	数据脱敏	增强了敏感数据自动发现、脱敏项目处理和跨库脱敏能力，增加对国产数据库和国产化硬件的支持。
云计算	超融合	增加了服务器虚拟机模式、流量监控、网络微分段、双因子认证、单主机多副本等功能，优化了 CDP 及主备容灾功能。
	超融合安全网元	发布了下一代防火墙、WAF、基线核查、日志审计、负载均衡等 12 类 38 款安全网元，构建具有多种安全能力的私有云，提供丰富的安全防护能力。
	桌面云	增加了软件分发、在线用户查看、双因子认证、单主机多副本、外设精细化管控等功能，支持 FC 和 ISCSI 类型共享存储。
	分布式防火墙	增加了云内安全大屏展示功能，优化了流量可视化、入侵威胁可视化、恶意代码可视化功能，帮助客户了解云内威胁动态，为安全策略配置提供参考。
	虚拟化防火墙	新增流量 TOP N 排名统计，完善了风险发现、入侵检测、安全基线等功能，提升了威胁情报、安全分析、安全检测等能力。
	等保一体机	整合了运营平台和自服务平台页面，加入了“等保自评”、“等保场景化模板”、“安全风险分析”等实用功能。
	自适应安全防御（CWPP）	基于新一代检测引擎和数据分析技术，增加了对风险发现、威胁监测的预览与统计功能，实现按照各种时间段统计安全事件，有效强化安全运营的监测与响应能力。
	安全云服务平台	集云监测、云检测、云防护、云分析和云管理 5 大能力于一体，通过一键订购，实现安全能力云化订阅交付和弹性扩展，覆盖云端赋能、安全响应、多云防护等场景。
	远程安全评估系统	增强了工单联动、镜像扫描、漏洞管理、配置审计等功能，并且加强了产品的漏洞管理能力，增加了专项漏洞验证以及检测的功能。
信创	数据库审计	国产化数据库审计，提供数据库实时监控、数据库风险预警、数据库威胁阻断等功能，满足政府、金融、能源、运营商、教育、交通等行业数据库审计需求。
	新一代入侵检测	国产化入侵检测，具备三权分立功能，能够精准发现网络中漏洞利用攻击、DDoS 攻击、僵尸网络、恶意 URL 访问等威胁。
	工控入侵检测与审计系统	基于国产化硬件平台和操作系统进行研发，支持工业入侵检测、工业行为审计、僵尸主机检测、威胁情报分析、工业资产发现等安全功能，保障工业生产网络安全运行。
	安全运维审计	基于国产化飞腾平台研发，支持最新 H5 技术，可对目标设备快速运维，增强资产管理能力及自定义改密能力。
大数据与安全运营	态势分析与安全运营	增加了态势三屏展示、分权分域、安全监测概览等功能，同时优化了监测任务、响应编排管理、日志检索和分析画像等模块，增强了工单管理能力。
	安全管理系统	增加了对国产软件操作系统的支持，增强了 NTP 同步、与三合一漏扫的联动支持等功能，优化了资产管理、安全处置、安全分析、日志解析等模块。
	日志收集与分析	基于国产处理器和国产操作系统研发，通过对日志的采集、处理、存储、备份、查询统计、合规报表以及关联分析，实现海量日志的全生命周期管理。
工业互联网 物联网 车联网	工业互联网态势分析与安全管理	面向工业企业网络环境的大数据安全分析系统，支持多源异构的工业网络安全数据采集，分析潜在的安全风险，提升工业企业安全运营管理水平。
	工控漏洞扫描	集工控扫描、无损扫描、系统扫描、数据库扫描、Web 扫描、弱口令检测以及基线核查等多种漏洞扫描技术，满足工业企业客户安全评估需求。
	工控防火墙	基于自主操作系统开发，支持多种工业协议深度解析与控制，可有效保障工控网络安全，同时具备宽温、防尘、抗强电磁干扰等工业级特性，适用于各种工业场景。
	工控安全监测审计	集工业协议审计、工艺行为审计、工业流量审计、工业资产管理等安全能力于一体，可实时发现异常流量、违规操作、误操作、非法指令等异常行为。
	工控主机卫士	专为工业主机安全防护设计研发，具备程序白名单、硬件白名单、网络白名单、资产管控等专业化安全能力，全面满足工业主机防护的安全需求。

业务领域	产品/版本名称	产品/版本更新与创新
	工控日志收集与分析	采用智能分析技术对工业网络中设备、软件、系统的日志进行采集、分析和管理，具备精准识别、高效搜索、智能分析等能力，全面满足工业行业对日志的安全管理需求。
	工控入侵检测与审计系统	基于国产化硬件平台和操作系统进行研发，支持工业入侵检测、工业行为审计、僵尸主机检测、威胁情报分析、工业资产发现等安全功能，保障工业生产网络安全运行。
	工控安全检查工具箱	专为工业控制系统信息安全检查工作研发，具备资产探测、漏洞扫描、基线核查、流量分析、合规性评估等功能，能够全面检测工控系统存在的安全问题。
	物联网安全接入网关	聚焦电力行业物联网泛在接入需求，增强私有协议解析、数据中继与物联网边缘计算能力，提升电力物联网终端运行的安全性。
	车载入侵检测与防御系统	支持丰富的车端安全检测引擎，以软件形式集成于车端零部件，对车内安全事件进行深度检测，精准识别攻击和异常行为，并支持在线防御。
	车载防火墙	内置国密安全芯片，支持车规级硬件的综合性车载通信，可为新一代智能网联汽车、自动驾驶巴士、无人驾驶出租车、无人物流车等提供网络接入与安全防护。
	车联网安全检测平台	产品为软硬件结合的自动化汽车网络安全检测工具集。平台融合多种测试用例库和多元化测试工具集，能够为检测机构、整车厂、零部件供应商等提供体系化的车联网安全合规验证与渗透测试能力。

表 3-2 报告期内公司发布的解决方案

业务领域	方案名称	解决方案发布
网络安全	远程办公密评解决方案	方案参照企业远程办公、密码应用、信息安全相关标准规范，为远程办公系统提供密码应用的技术支撑，由 VPN 加密机、服务器密码机、签名验签服务器等产品提供密码应用技术支撑。
	医院系统密码应用解决方案	从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个方面设计，全面满足 GB/T 39786《信息安全技术信息系统密码应用基本要求》第三级密码应用的基本要求。
	外防内清“挖矿”专项治理方案	推出外防内清“挖矿”专项治理方案，将下一代防火墙、病毒过滤网关、APT 沙箱、WAF、EDR 等“边端”产品联合部署，为各级客户构建防御、防护、监测、阻断于一体的外防内清“挖矿”防御治理体系。
	医疗行业应用安全综合解决方案	以 Web 应用防火墙、网页防篡改、Web 漏洞扫描、网站监测等产品为核心的多点融合、协同联动的综合解决方案，集风险感知、漏洞探知、安全防护、事后恢复四位一体，全面提升客户网站安全防护能力。
	医疗传统 IT 架构转型方案	旨在帮助医院客户完成传统 IT 架构的平滑升级，天融信太行云提供百万级 IOPS，承载数据库类关键应用，支持块、文件、对象等多样存储协议接口，高效满足医院各类业务数据的存储需求。
数据安全	数据出境监测和防护解决方案	通过数据防泄漏系统的出境数据合规自查、敏感数据检测与阻断、出境传输协议审计与监管和出境异常行为风险判别能力，为数据处理者的数据出境活动保驾护航。
云计算	TopSASE 解决方案	将网络（SD-WAN）和安全（SSE）解决方案深度融合，基于云交付统一服务，围绕全边缘接入、安全服务边缘（SSE）、统一管理平台三大功能，提供全栈交付、多元融合、随需订阅、云地一体的网络与安全服务。
	5G 端到端闭环安全解决方案	基于 5G 的业务和信令特点设计，利用切片隔离和编排防护、隐私保护等技术，统筹资源协同和防护处理，构建了立体化的安全防护体系。具备 5G 应用加固、5G 访问控制、5G 应用监控、API 安全、应用审计等安全能力。
	信创“云+安全”融合解决方案	将防火墙、Web 应用防火墙、网络审计、数据库审计等多项核心安全能力部署于安超云内，形成基于软件定义的安全资源池。通过联动 ArSDN 控制器，实现业务流量智能调度、安全能力弹性扩展。
大数据与安全运营	政务大数据应用安全防护方案	以下一代防火墙、Web 应用防火墙、Web 漏洞扫描、网页防篡改等产品为核心，涵盖“事前”、“事中”、“事后”全生命周期的应用安全防护解决方案，旨在助力政府客户全面提升应用安全防御能力。

业务领域	方案名称	解决方案发布
工业互联网 物联网 车联网	“双安融合”下的工业互联网安全协同防护解决方案	基于双安融合逻辑框架，在控制过程安全、通信过程安全、平台安全运营等层面实现功能安全与信息安全的深度融合，更好地发挥信息安全防护技术效用，实现“工业互联网+安全生产”的目标。
	金融物联网安全解决方案	采用 5G 物联网安全接入网关+物联网安全管理平台的组合方案，提供覆盖感知层、网络层、平台层和应用层的安全防护能力，实现金融业务全生命周期的安全防护。

2、公司经营模式

1）盈利模式：公司盈利主要来自网络安全产品销售、服务提供及能力订阅三种模式。

产品销售：公司提供全系列网络安全、大数据与云计算产品及覆盖物理环境和云环境的全面解决方案。根据客户或合作伙伴需要，设计并提供满足其需求的解决方案，向客户或合作伙伴提供满足其需求的产品，以产品销售模式实现公司营业收入。

服务提供：公司基于产品工具化、运营平台化和人员本地化手段，为客户或协助合作伙伴为客户提供安全规划与咨询、安全评估与加固、安全业务定制开发、安全运维和安全运营，以提供服务模式实现公司营业收入。

能力订阅：公司面向已销售的安全产品提供以月、年计费的安全知识（包括威胁情报信息等），面向客户或合作伙伴提供以天、月、年和流量计费的云端检测和防护，以安全能力订阅模式实现公司营业收入。

公司近 5 年盈利模式对比如下：

表 3-3　公司近五年盈利模式对比

单位：百万元

项目	2018 年	2019 年	2020 年	2021 年	2022 年
产品销售	1,430	1,888	2,185	2,531	2,655
服务提供	177	337	439	534	571
能力订阅	124	191	204	283	313
产品销售占比	82.62%	78.16%	77.27%	75.60%	75.01%
服务提供占比	10.24%	13.96%	15.52%	15.95%	16.15%
能力订阅占比	7.14%	7.88%	7.21%	8.45%	8.84%
合计	**1,731**	**2,416**	**2,828**	**3,348**	**3,539**

2）研发模式：公司坚持自主研发、自主创新，采取预研先行、需求引领、平台支撑、统一规划和分布实施、产学研合作的研发策略。

（1）预研先行：公司设有安全技术研究院和多个安全实验室，主要承担前沿技术研究、安全新领域探索、攻防研究、威胁追踪、智能检测、协议分析、红蓝对抗等研究工作，并将安全能力输出给产品开发团队。

（2）需求引领：根据行业与客户需求，公司采用标准产品开发与定制项目并行的模式。标准产品支撑项目，同时定制项目中的业务需求不断沉淀、积累，并整合到标准产品中，实现产品和技术创新。

（3）平台支撑：公司建立了专门的硬件平台、软件平台、威胁情报知识平台研究与开发团队，在软硬件和威胁情报知识基础平台支撑下，产品开发团队无需过多考虑底层架构实现，更聚焦于产品本身核心功能和业务创新，有效提升研发效率和质量。

（4）统一规划：公司采用研发总部+分中心的研发模式，除北京总部外，在武汉、深圳、成都、西安等地设立研发分中心，对研发项目统一管理，保障研发创新成果快速产品化、产业化。

（5）产学研合作：公司深耕网络安全、数据安全、云计算领域，聚焦基础网络、工业互联网、物联网、车联网新场景，深入研究大数据、人工智能、5G、隐私计算等新技术，通过与高校、科研机构等共建联合实验室、承担前沿科研课题等方

式，实现关键技术的攻关和创新突破。

3）安全服务模式：公司提供“线上+线下”一站式服务。

公司在全国各省级行政区域已建立 32 个二级线上安全云服务运营中心和 3 个客户联合运营中心，依托总部云服务平台、各分中心及分布在全国的 1000+人员，提供线上、线下相结合的服务模式，为客户提供“线上实时监测、分析预警、指挥协调”+“线下本地化服务、应急响应、整改修复”的一站式服务能力。

4）销售模式：公司采用直销加分销的销售模式。

一方面，公司在全国市场向政府、重要行业、重要客户直接销售产品和服务；另一方面，公司与渠道生态合作伙伴合作，利用合作伙伴的渠道进行全区域的分销，公司产品和服务覆盖更多的区域市场和广泛的企业、商业客户。

5）生产模式：公司具有独立的硬件设计和软件研发能力。

公司独立设计的硬件模块由具有相关能力的供应商代为加工生产；硬件类产品是将自主研发的软硬件功能模块及安全能力与工控机或服务器进行高度匹配和融合后，交付给客户；软件类产品以软件研发为主要生产模式。公司依托自有厂房、设备和人员以自行组织生产为主，部分原材料由供应商代工生产，生产过程有高效的质量管理制度和研发管理制度，能够保障硬件、软件、测试、检验、包装、入库等整个环节规范且高效有序地开展；产品产量主要根据市场需求、经销商需求及项目需求实行评估与报备相结合的模式进行预生产，有效保证了客户的供货效率，同时也有效提升了原材料的使用率，实现库存高周转率。

3、公司产品市场地位、竞争优势

公司防火墙产品已连续 23 年位居国内市场第一，VPN、WAF、安全咨询服务、MSS（托管安全服务）、MSS+PSS（安全服务）、网闸等产品和服务已连续多年位居市场前三，工控防火墙、工控漏洞扫描、工控安全隔离与信息交换、EDR、态势感知、零信任、工控主机卫士等多款产品处于领导者行列，IDPS、安全资源池、安全管理、响应和软件编排、信息和数据安全、终端安全软件等产品位居市场前列。

表 3-4　公司主要产品市场地位

产品/领域	市场排名/位置	数据来源
防火墙	第一	IDC
安全咨询服务	第二	IDC
VPN	第三	IDC
网闸	第三	IDC
FW/VPN	第一	CCID
终端安全	第三	CCID
安全服务	第三	CCID
Web 应用防火墙（WAF）	中国区第三	Frost ＆ Sullivan
托管安全服务（MSS）	中国区第二	Frost ＆ Sullivan
安全服务（MSS+PSS）	中国区第一	Frost ＆ Sullivan
EDR	领导者	IDC
态势感知	领导者	IDC
零信任（ZTNA）	领导者	IDC
工控防火墙系统	领导者	CCID

产品/领域	市场排名/位置	数据来源
工控漏洞扫描系统	领导者	CCID
工控安全隔离与信息交换系统	领导者	CCID
工控主机卫士系统	领导者	CCID
工控入侵检测与审计系统	领导者	CCID
工控安全集中管理系统	领导者	CCID
工控安全服务	领导者	CCID
工控安全监测审计系统	领导者	CCID
工业互联网态势分析与安全管理系统	领导者	CCID
工业攻防演示试验箱系统	领导者	CCID
入侵检测与防御系统（IDPS）	前列	IDC
数据防泄漏（DLP）	前列	IDC
安全资源池	前列	IDC
响应和编排软件	前列	IDC
信息和数据安全	前列	IDC
终端安全软件	前列	IDC
安全管理平台	前列	CCID
安全云服务	入选	Gartner
超融合	入选	Gartner
零信任（ZTNA）	入选	Gartner
攻防演练	入选	Gartner
数据分类分级	入选	Gartner
数据防泄漏（DLP）	入选	Gartner
CPS 安全	入选	Gartner
SASE	入选	Gartner
云安全资源池	入选	Gartner
态势分析与安全运营系统	入选	Gartner
威胁情报系统	入选	Gartner
脆弱性扫描和管理系统	入选	Gartner
数据安全智能管控平台	入选	Gartner
终端数据防泄漏	入选	Gartner

产品/领域	市场排名/位置	数据来源
网络数据防泄漏系统	入选	Gartner
数据库审计系统	入选	Gartner
数据脱敏系统	入选	Gartner
AI 防火墙	独家案例入选	IDC
数据安全	案例入选	IDC
SD-WAN	案例入选	IDC
零信任（ZTNA）	案例入选	IDC
工业互联网安全	案例入选	IDC
政务云云安全	入围专业安全厂商	IDC

4、主要业绩驱动因素

报告期内，国家政策、信息化发展和公司业务布局拓展是公司业绩增长的主要驱动因素，主要体现在以下两个方面：

1）外部驱动因素：随着数字经济发展、安全威胁加剧、国家政策法规等外部因素驱动，网络安全需求市场持续增大。新业务、新场景下的安全需求不断涌现，网络安全行业将迎来更大的发展机遇。

2）内部应对措施：跟随国家政策指引及市场需求变化，公司积极采取应对措施，积极布局新方向、新产品、新业务，不断创新研发，丰富产品线，不断提升服务能力，保障客户业务安全交付，不断拓展生态客户，构建国产化安全生态圈，不断优化人才结构，提升公司管理能力和水平。

（三）主要会计数据和财务指标

（1）近三年主要会计数据和财务指标

公司是否需追溯调整或重述以前年度会计数据

□是 ☑否

单位：元

	2022 年末	2021 年末	本年末比上年末增减	2020 年末
总资产	11, 985, 841, 800. 54	11, 596, 312, 907. 43	3. 36%	11, 324, 258, 269. 10
归属于上市公司股东的净资产	9, 778, 684, 730. 08	9, 477, 132, 606. 50	3. 18%	9, 585, 715, 260. 44
	2022 年	2021 年	本年比上年增减	2020 年
营业收入	3, 543, 003, 938. 99	3, 351, 566, 360. 03	5. 71%	5, 704, 169, 340. 66
归属于上市公司股东的净利润	205, 091, 336. 88	229, 996, 891. 02	-10. 83%	400, 114, 581. 27
归属于上市公司股东的扣除非经常性损益的净利润	153, 699, 730. 36	153, 921, 194. 07	-0. 14%	447, 025, 097. 18
经营活动产生的现金流量净额	-271, 077, 474. 97	169, 731, 731. 68	-259. 71%	203, 570, 689. 50
基本每股收益（元/股）	0. 1805	0. 2031	-11. 13%	0. 3535
稀释每股收益（元/股）	0. 1793	0. 1991	-9. 94%	0. 3501

加权平均净资产收益率	2. 13%	2. 48%	-0. 35%	4. 34%	

注 1：公司 2020 年实现收入 570,416.93 万元，其中网络安全业务收入 283,234.05 万元、电线电缆业务收入 287,182.88 万元。2020 年 9 月公司实施完毕重大资产出售后，不再从事电线电缆业务，主要业务聚焦至网络安全领域。

注 2：为加快客户货款回笼，客户 2022 年度到期的 1.06 亿元货款以客户通过自身结算平台向公司开具的“金单”以保理业务方式支付，保理费用由客户承担，该取得的现金计入筹资活动现金流致经营活动产生现金流量净额减少 1.06 亿元。

（2）分季度主要会计数据

单位：元

	第一季度	第二季度	第三季度	第四季度
营业收入	378, 417, 242. 54	501, 535, 340. 17	583, 309, 685. 74	2, 079, 741, 670. 54
归属于上市公司股东的净利润	-64, 735, 862. 07	-140, 865, 061. 51	-214, 190, 577. 29	624, 882, 837. 75
归属于上市公司股东的扣除非经常性损益的净利润	-71, 374, 986. 59	-167, 252, 044. 26	-219, 092, 391. 45	611, 419, 152. 66
经营活动产生的现金流量净额	-272, 460, 710. 75	-263, 760, 992. 33	-335, 930, 502. 85	601, 074, 730. 96

上述财务指标或其加总数是否与公司已披露季度报告、半年度报告相关财务指标存在重大差异

□是 ☑否

（四）股本及股东情况

（1）普通股股东和表决权恢复的优先股股东数量及前 10 名股东持股情况表

单位：股

报告期末普通股股东总数	39, 708	年度报告披露日前一个月末普通股股东总数	37, 476	报告期末表决权恢复的优先股股东总数	0	年度报告披露日前一个月末表决权恢复的优先股股东总数	0
前 10 名股东持股情况							
股东名称		股东性质	持股比例	持股数量	持有有限售条件的股份数量	质押、标记或冻结情况	
						股份状态	数量
郑钟南		境内自然人	7. 11%	84, 301, 969	0		
明泰汇金资本投资有限公司		境内非国有法人	6. 24%	74, 000, 997	0	质押	74, 000, 997
						冻结	74, 000, 997
中电科（天津）网络信息科技合伙企业（有限合伙）		境内非国有法人	4. 89%	58, 000, 000	0		
香港中央结算有限公司		境外法人	2. 55%	30, 210, 352	0		
全国社保基金一零二组合		其他	2. 26%	26, 732, 921	0		
天融信科技集团股份有限公司－“奋斗者”第一期员工		其他	2. 00%	23, 719, 000	0		

持股计划						
林芝腾讯科技有限公司	境内非国有法人	1.94%	23,000,000	0		
申万宏源证券有限公司	国有法人	1.47%	17,374,866	0		
章征宇	境内自然人	1.45%	17,184,835	0		
深圳前海珞珈方圆资产管理有限公司－珞珈方圆慎独一期私募基金	其他	1.19%	14,064,344	0		
上述股东关联关系或一致行动的说明	上述股东中郑钟南是公司第一大股东，公司第一大股东与上述其他股东之间不存在关联关系，公司未知其他股东之间是否属于《上市公司收购管理办法》中规定的一致行动人。					
参与融资融券业务股东情况说明（如有）	不适用					

（2）公司优先股股东总数及前 10 名优先股股东持股情况表

□适用 ☑不适用

公司报告期无优先股股东持股情况。

（五）在年度报告批准报出日存续的债券情况

□适用 ☑不适用

三、重要事项

报告期内，公司经营情况无重大变化。重要事项详见《2022 年年度报告全文》第三节“管理层讨论与分析”及第六节“重要事项”相关内容。

天融信科技集团股份有限公司

法定代表人：李雪莹

二〇二三年四月二十二日