证券代码：002212　　证券简称：天融信　　公告编号：2024-058

天融信科技集团股份有限公司
关于2023年度计提资产减值准备的公告

本公司及董事会全体成员保证信息披露的内容真实、准确、完整，没有虚假记载、误导性陈述或重大遗漏。

根据《企业会计准则》及天融信科技集团股份有限公司（以下简称“公司”）会计政策的相关规定，本着谨慎性原则，公司对截至2023年12月31日合并报表范围内存在减值迹象的资产计提了相应的减值准备。本次计提资产减值准备事项已经普华永道中天会计师事务所（特殊普通合伙）审计确认。现将具体情况公告如下：

一、本次计提资产减值准备情况概述

（一）本次计提资产减值准备的原因、资产范围、总金额和计入的报告期间

根据《企业会计准则》及公司会计政策的相关规定，本着谨慎性原则，公司以2023年12月31日为基准日，对合并报表范围内的应收票据、应收账款、其他应收款、存货、合同资产、长期股权投资、固定资产、无形资产、商誉等各项资产进行全面清查，对各项资产减值的可能性进行了充分的评估和分析，对存在减值迹象的资产计提了相应的减值准备。本次计提资产减值准备事项已经普华永道中天会计师事务所（特殊普通合伙）审计确认。

根据评估和分析的结果判断，公司本次计提各项信用减值损失和资产减值损失共计509,178,155.61元，计入的报告期间为2023年1月1日至2023年12月31日。具体如下：

单位：元

项　目	本期计提/转回（-）	占2023年度经审计归属于上市公司股东净利润的比例
信用减值损失：		
应收票据坏账损失	61,701.12	0.02%
应收账款坏账损失	53,852,690.73	15.94%
其他应收款坏账损失	4,784,304.48	1.42%
小计	58,698,696.33	17.37%
资产减值损失：		
存货跌价损失	5,853,906.45	1.73%
合同资产减值损失	1,345,452.83	0.40%
商誉减值损失	443,280,100.00	131.18%
小计	450,479,459.28	133.31%
合　计	509,178,155.61	150.68%

（二）公司对本次计提资产减值准备的审批程序

本次计提资产减值准备事项是按照《企业会计准则》等相关法律法规、规范性文件及公司会计政策的有关规定执行，无需提交公司董事会或股东大会审议。

二、本次计提资产减值准备的依据及合理性说明

（一）信用减值损失

公司对于以摊余成本计量的金融资产、以公允价值计量且其变动计入其他综合收益的债务工具投资和应收租赁款等，以预期信用损失为基础确认损失准备。

公司考虑在资产负债表日无须付出不必要的额外成本和努力即可获得的有关过去事项、当前状况以及对未来经济状况的预测等合理且有依据的信息，以发生违约的风险为权重，计算合同应收的现金流量与预期能收到的现金流量之间差额的现值的概率加权金额，确认预期信用损失。

对于因销售商品、提供劳务等日常经营活动形成的应收票据、应收账款和应收款项融资，无论是否存在重大融资成分，均按照整个存续期的预期信用损失计量损失准备。对于应收租赁款，亦选择按照整个存续期的预期信用损失计量损失准备。

除上述应收票据、应收账款、应收款项融资和应收租赁款外，于每个资产负债表日，对处于不同阶段的金融工具的预期信用损失分别进行计量。金融工具自初始确认后信用风险未显著增加的，处于第一阶段，公司按照未来12个月内的预期信用损失计量损失准备；金融工具自初始确认后信用风险已显著增加但尚未发生信用减值的，处于第二阶段，按照该工具整个存续期的预期信用损失计量损失准备；金融工具自初始确认后已经发生信用减值的，处于第三阶段，按照该工具整个存续期的预期信用损失计量损失准备。

（二）资产减值损失

1、存货

存货跌价准备按存货成本高于其可变现净值的差额计提。可变现净值按日常活动中，以存货的估计售价减去至完工时估计将要发生的成本、估计的合同履约成本和销售费用以及相关税费后的金额确定。

2、商誉

公司每年聘请评估机构对商誉进行减值测试，将商誉分摊至相关资产组或资产组组合。这些资产组或资产组组合是公司内能够独立产生现金流入的最小资产组合。资产组或资产组组合的可收回金额根据预计未来现金流量的现值确定。公司考虑了资产组或资产组组合最近可合理估计的未来现金流量以及合理的折现率，计算上述资产组或资产组组合的预计未来现金流量的现值。

可收回金额是资产组或资产组组合的公允价值减去处置费用后的净额与资产组预计未来现金流量的现值两者之间的较高者，其计算需要采用会计估计。在预计未来现金流量现值时，需要对该资产组或资产组组合生产产品的预测期增长率、稳定期增长率、毛利率以及计算现值时使用的税前折现率等作出重大判断。公司在估计可收回金额时会采用所有能够获得的相关资料，包括根据合理和可支持的假设所作出有关预测期增长率、稳定期增长率、毛利率及税前折现率的预测，内容有关于估值时采用适当的估值方法及应用适当假设。

3、长期资产

投资性房地产、固定资产、在建工程、使用权资产、使用寿命有限的无形资产及对子公司、合营企业、联营企业的长期股权投资等，于资产负债表日存在减值迹象的，进行减值测试；尚未达到可使用状态的无形资产，无论是否存在减值迹象，至少每年进行减值测试。减值测试结果表明资产的可收回金额低于其账面价值的，按其差额计提减值准备并计入资产减值损失。

4、合同资产

合同资产无论是否存在重大融资成分，公司均按照整个存续期的预期信用损失计量损失准备。

公司本次计提资产减值准备符合《企业会计准则》和公司相关会计政策的规定，依据充分，符合公司的实际情况。

三、单项资产减值计提情况说明

2023年度，公司计提商誉减值准备44,328.01万元，单项资产计提的减值准备占公司2023年度经审计的归属于上市公司股东的净利润绝对值的比例超过30%且单项金额超过1,000万元，具体情况说明如下：

单位：元

项目	内容
资产名称	北京天融信科技有限公司合商誉资产组
账面价值	6,289,926,800.00
资产可收回金额	5,846,646,700.00
本次计提资产减值准备的依据	依据《企业会计准则》及公司会计政策的相关规定，详见“二、本次计提资产减值准备的依据及合理性说明”
资产可收回金额的计算过程	在进行商誉减值测试时，公司将相关资产或资产组组合（含商誉）的账面价值与其可收回金额进行比较，如果可收回金额低于账面价值，相关差额计入当期损益。经比较相关资产组组合的公允价值减去处置费用后的净额和预计未来现金流量的现值后，采用预计未来现金流量的现值确定其可收回金额，可收回金额为5,846,646,700.00元，并计提减值准备443,280,100.00元。 采用未来现金流量折现方法的主要假设如下： 预测期收入增长率：6.00%-16.00% 稳定期收入增长率：0.00% 毛利率：60.28% 税前折现率：12.39%
本期计提金额	443,280,100.00
计提原因	2023年度，国内宏观经济环境较为复杂，行业复苏不均，公司第四季度新增订单不及预期，影响了公司2023年度的收入规模和利润完成，公司对网络安全行业和公司的长远发展充满信心，预计2024年市场环境和业务发展处于逐步向好的态势，行业需求将继续恢复，但恢复到较高增速需要时间，公司对恢复程度保持谨慎乐观，对之前作出的发展节奏预测进行了调整。

四、本次计提资产减值准备对公司的影响

2023年度公司计提信用减值损失58,698,696.33元，计提资产减值损失450,479,459.28元，减少公司2023年度合并报表利润总额509,178,155.61元，符合《企业会计准则》规定及公司资产实际情况，在计提信用减值损失和资产减值损失后，能够更加公允地反映公司资产状况，公司资产价值会计信息更加真实、可靠，不存在损害公司和全体股东利益的情形。

特此公告。

天融信科技集团股份有限公司董事会

二〇二四年四月二十日

证券代码：002212　　证券简称：天融信　　公告编号：2024-053

天融信科技集团股份有限公司
2023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。公司围绕网络安全与数据安全、云计算与云安全领域，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）网络安全与数据安全：公司提供全系列基础网络安全产品，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，覆盖所有基础网络安全场景，包括防火墙、VPN、入侵检测、入侵防御、Web应用防火墙、网闸、堡垒机、SD-WAN、零信任、病毒过滤网关、应用安全网关、EDR、加密机、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、漏洞扫描、日志审计、安全管理、智慧无线管理等产品，可为各行业客户提供全面的网络安全产品和解决方案。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。推出了数据库审计与防护、网络数据防泄漏、终端数据防泄漏、数据脱敏、数据库审计、数据分类分级、备份一体机、数据安全管理平台、数据安全保险、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、金融、运营商、能源等行业。

（2）云计算与云安全：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，在集网络、计算、存储、安全一体的超融合基础上，发布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、云迁移、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。在云安全领域，公司对已有的安全产品进行云原生化改造，通过将安全能力原子化，实现业务与安全的深度融合，基于云原生技术，陆续发布了云原生防火墙、云安全资源池、SASE、CWPP、云原生API安全网关、CNAPP等云安全产品。公司持续推进“云计算+安全”深度融合，通过与云平台、操作系统、服务器、芯片厂商的深度合作，天融信云安全解决方案可灵活应用于各类云计算场景，形成覆盖政务云、大型集团云、医疗云、托管云、多云、容器云、公有云等30+业务场景的完整解决方案，并在政府、运营商、能源、医疗、海关等众多行业广泛落地实践。

2）重点领域：公司面对企业数字化转型过程中的新技术、新场景、新趋势持续探索，发力信创推进全面国产化，采用人工智能技术实现安全智能化，融合工业互联网、车联网、物联网新场景，推进商用密码产品技术应用落地，提供多元场景下的安全运营能力。

（1）信创安全：公司始终坚持走自主创新之路，自2013年发布首款龙芯防火墙产品以来，基于国产软硬件的“天融信昆仑”信创系列产品种类不断丰富、产品平台持续更新迭代，已累计发布了涵盖边界安全、安全接入、安全检测、安全审计、安全管理、端点安全、数据安全、工控安全、云安全、云计算等方向的66类250款型号，覆盖所有主流网络安全产品类别，可以为客户提供完善的信创产品和解决方案。报告期内，公司重点推动全栈国产化能力建设，通过与国内生态上下游的紧密合作，将国密算法、联动协议、可信技术、拟态技术、人工智能等技术进行深度融合，打造高安全性、高可靠性、高性能的创新生态体系，提升公司信创产品和方案的核心竞争力。

（2）人工智能+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，陆续发布了融入AI技术的防火墙、入侵防御、入侵检测、僵木蠕监测、物联网安全接入网关、数据防泄漏、数据库审计、数据库审计与防护、网络审计、大数据分析、态势感知、智能内网威胁分析、EDR、沙箱等多款创新型产品。报告期内，基于类大模型、大模型等AI技术，公司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的技术成果，并推出天问大模型、天问系统，赋能公司全系列产品。

（3）工业互联网、车联网、物联网：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技术理念，同时提出基于IPDRR安全框架的工业互联网安全解决方案。在产品方面，推出包括工控防火墙、工控入侵检测与审计、工控安全监测审计、工控网闸、工控主机卫士、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、工业攻防靶场、工业实训平台、攻防演示试验箱14类专用产品。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。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。

（4）商用密码：公司持续深耕密码技术，将商用密码与新兴技术融合应用，从产品、方案、服务三个方面推动商用密码应用落地。公司自2000年研制并发布了SJW11网络密码机成为国内首批商用密码产品以来，先后推出了加密机、服务器密码机、签名验签服务器、安全认证网关、密码服务平台、协同签名等18类商用密码产品和整体解决方案，形成了完整的商用密码支撑体系。在量子计算和量子密码方向，公司将量子密码通信、量子密码认证、量子密码签名、量子密钥生成等技术深度融合，发布了IPSec VPN量子安全网关、SSL VPN量子安全网关等量子密码系列产品，进一步完善商用密码多场景应用。

（5）安全运营：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，结合公司安全云服务中心的线上、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。

表3-1 报告期内公司发布的主要产品

业务领域	产品/版本名称	产品/版本更新与创新
网络安全与数据安全	Smart防火墙	增强了威胁情报能力，提供丰富的情报威胁类型和情报上下文信息，具备高质量的IOC情报检测能力，能够针对最新威胁及热点威胁进行防护。
	金融防火墙	专为金融行业IT安全需求研发，支持IPv4/IPv6双栈，具备高性能、高安全、高可靠、易管理等能力，满足金融行业对防火墙的业务需求。
	下一代VPN	采用自主研发的密码卡，支持IPSec VPN和SSL VPN，具备高性能、高并发等特点，能够对远程网络中传输的数据提供私密性、完整性等安全防护。
	Web应用防火墙	采用全新硬件平台研发设计，规格和性能得到全面提升，同时在基本Web防护功能的基础上增加了API防护、联动防护、网站镜等功能，保证网站的安全运行。
	新一代入侵防御	增加了钓鱼邮件检测、DNS投毒检测、PCAP文件WEB导入检测等安全能力，增强了人工智能检测引擎、Web安全检测引擎、异常流量检测引擎等功能，检测能力大幅提升。
	堡垒机	采用高端硬件平台和国密加密卡，提升了产品性能，增强了国密算法加密校验能力，满足高性能、大并发和国密算法加密需求。
	负载均衡	采用全新硬件平台研发设计，具备链路负载、服务器负载和全局负载能力，同时集成了压缩、缓存、SSL卸载等网络优化技术，提高业务系统访问效率。
	协议转换交付	采用全新硬件平台，既能通过代理方式快速翻译实现IPv6的接入，又能支持IPv4/IPv6双栈模式部署，结合链路负载和服务器负载功能满足各种场景下用户对业务系统高可用的需求。
	病毒过滤网关	增强了IPv6路由交换、访问控制、QoS等网络控制能力和HTTPS病毒检测和DDoS防御等安全防护能力。
	僵木蠕	增强了攻击检测、Web安全检测、异常流量检测等能力，新增了恶意TLS检测、WebShell检测、移动恶意程序快速检测、HTTP隧道检测、命令注入检测等智慧引擎，检测能力大幅提升。
	上网行为管理	采用全新硬件平台，默认接口配置更高，接口扩展能力更强，具有良好的网络适应性，同时基于国产软件版本，有效提升了安全性、审计能力和稳定性。
	智慧无线	定位于企业级Wi-Fi6室内放装AP，支持全部Wi-Fi6特性、多种认证组合模式，提供安全快速的网络体验。
	网络审计	采用全新的硬件平台，提升了硬件配置和处理性能，通过多维度的网络行为分析和流量审计分析技术实现合规审计。
	SD-WAN	增加了链路健康检查、智能路由、双边加速等功能，增强了认证能力和管理能力，优化了产品处理性能。
	隐私计算平台	以数据流通生命周期安全为核心，隐私计算技术为基础，联合AI机器学习算法，提供节点管理、数据安全接入、隐私查询、联合建模、数据分析等能力。
	数据库审计	增加了静态脱敏功能，通过内置高效的脱敏算法将敏感信息转化为脱敏数据，解决企业在系统开发测试、数据分析等场景下的数据泄漏问题。
	网络数据防泄漏	增加了数据探针、链路聚合、数据库协议识别、水印服务、文档指纹、接口检测等功能，优化了设备处理性能以及日志上报和事件分析等功能。
	数据安全靶场	提供数据安全业务场景的模拟环境，内置各类型的业务系统、数据安全组件、数据安全管理平台等，支持数据流转过程中安全审计、风险监测、事件处置等关键能力的展现。
	数据库审计与防护	能够对国内外40余种数据库协议进行详细解析，结合内置规则，精确管控违规数据库操作行为，满足各行业对数据库的安全防护需求。
	备份一体机	新产品采用全新硬件平台，对CPU、内存、硬盘、接口、RAID卡进行了全面升级，优化了产品处理性能，提升了系统备份任务的稳定性和效率。
云计算与云安全	超融合	增加了CPU池化管理、磁盘IO加速、缓存盘卡慢检测、回收站自动清理等功能，优化了虚拟机迁移、快照策略、云服务器列表、CPU预留和NUMA等功能。
	桌面云	增强了终端管理、零信任桌面、打印机重定向、国产化VOI架构、安全模块等功能。
	云安全资源池	采用软件定义安全技术，具备按需使用、弹性扩展的特点，提供网络安全、主机安全、应用安全、安全审计、安全运维等安全能力，提升云上业务安全性。
信创安全	擎天六防火墙	专为大流量场景设计研发，具有高性能处理架构、多层级可靠设计、全方位安全防护和可视化业务感知等特点，能满足高性能国产化场景需求。
	网络审计	采用国产化硬件平台，支持4000种以上应用协议识别与审计，采用旁路部署、支持多点多级、分布式部署、集中管理等特性。
	负载均衡	采用国产硬件平台和操作系统，具备链路负载均衡、服务器负载均衡和全局负载均衡等能力。
	网闸	采用国产硬件平台和操作系统，具备协议剥离、内容还原、内容过滤、病毒查杀、访问控制、安全审计等隔离和防护机制。
	上网行为管理	基于国产化硬件平台和操作系统研发，具有良好的网络适应性，可应用于政府、运营商、金融、能源、教育、医疗、企业等各行业。
	超融合	采用国产海光、鲲鹏处理器，深度集成计算、存储、网络和安全等基础资源，助力客户快速构建安全、高效、可靠的新一代云计算数据中心。
	过滤网关	基于国产化硬件平台，采用网关级病毒检测扫描引擎，提高内网病毒防护能力，同时增强了流量管理、DDoS防护、防火墙联动等功能。
工业互联网物联网	工控防火墙	基于飞腾硬件平台和银河麒麟操作系统研发，支持工控协议细粒度解析、入侵防御、病毒过滤、IPSec VPN等功能，保证工控网络和控制设备的安全运行。
	工控入侵检测与审计	全新工业级硬件平台，采用无风扇、全封闭设计，具备工业入侵检测、僵尸主机检测、工业行为审计、数据库审计等核心安全能力，保障工业生产网络和设备的安全运行。
	工控安全监测审计	采用无风扇、全封闭设计的工业级硬件平台，具备工业协议解析、工业行为审计、工业流量审计、工业资产发现等核心安全能力，实现对工业生产网的实时安全监测。
	工控漏洞扫描	便携式加固笔记本形态，具备工控漏扫、系统漏扫、口令猜解、资产管理等核心功能，满足移动便携场景脆弱性检测与漏洞扫描。
	物联网安全接入网关	提供对物联网接入设备的资产识别、行为分析、非法外联检测等功能，可满足安防场景下的大规模物联网接入需求，实现设备快速接入和安全使能。
商用密码	服务器密码机	更新SDK功能，支持JAVA、Windows C、Linux C，增加数据结构说明、设备接口描述。
	签名验签服务器	采用商用密码加密卡实现对网络流量、信令的签名和验签功能，保障数据流量的完整性和不可抵赖性。
安全运营	态势分析与安全运营	增强了安全治理、响应编排、重保管理等能力，优化了告警管理、态势大屏、报告模板等功能，帮助企业更好地应对安全挑战，提高整体安全水平。
	潜听威胁发现	采用轻量级虚拟化与透明流量转发技术，支持多种服务仿真，构建高仿真环境，弥补网络防护体系短板，提升主动防御能力。
	大数据分析	增强了告警研判、溯源分析以及全局数据血缘管理等功能，优化了专项分析能力。

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
网络安全与数据安全	电信行业全流量分析解决方案	旨在帮助电信行业客户共同落实政策条令要求，全面提升网络安全监测预警能力和网络安全管理水平，可实现网络安全和数据安全已知、未知威胁的发现及溯源，实时了解安全态势，降低安全风险。
	金融行业外包活动安全运维解决方案	针对金融行业运维现状与政策要求，以运维安全审计系统、下一代防火墙、终端威胁防御系统等产品，构建具备资源整合、把控操作、精准定责、安全评估等能力的安全运维通道，助力银行保险机构满足合规需求。
	SD-WAN县域安全广域互联解决方案	构建一套分支极简部署、立体安全防护、统一便捷运维、业务韧性可靠的政务安全互联广域网络，实现各乡镇SD-WAN设备的批量快速上线、集中统一运维的同时，全面提升政务分支机构的网络安全综合防护能力。
	融合UEBA的零信任安全解决方案	基于标准SDP安全模型，与4A系统无缝对接，利用设备指纹、MFA等技术完成用户/终端身份认证与授权，配合动态防火墙技术，实现动态控制用户/终端网络应用访问权限。
	病毒过滤网关联动防御解决方案	过滤网关联动下一代防火墙、终端威胁防御系统、高级威胁检测系统、Web应用安全防护等产品，可构建一系列威胁防御方案，对勒索病毒、挖矿病毒提供全生命周期防御。
	SOAR解决方案	方案以数据中台为底层支撑平台，通过对数据的采集、建模、分析、计算，以SOAR为核心技术手段，实现终端安全、漏洞扫描、威胁情报等安全资源统一整合与管控，进行整体安全策略自动化编排，统一向业务系统提供联动服务。
	天韧数据勒索保障方案	方案将“网络防护、流量检测、终端防御”三大能力融为一体，并结合保险兜底，实现事前全面有效预防、事中精准监测阻断、事后高效恢复和保险理赔，有效防范勒索攻击等各类威胁，助力中小企业专注发展业务。
	天剑数据泄露防治方案	方案通过“数据、网络、终端”一体化立体防护矩阵，全方位检测防护数据各种泄密途径，通过网络防护阻断外部攻击和内部不当行为，采用先进的防病毒与合规管控技术，为终端安全提供双重保障，严防外部风险，筑牢内部防线，为中小企业数据安全提供坚实保障。
	天权数据特权管控方案	方案提供账号管理策略、身份认证机制、权限管控策略、服务器及数据库操作审计、风险行为分析等功能，为企业提供全方位、智能化的数据特权管控方案。
	天盟数据开发利用安全方案	方案提供数据集中管控、数据内容识别、行为阻断等安全能力，在研发设计、代码构建、验证测试等数据利用场景中，有效保护科研成果数据，为数据的开发利用提供全程防护，安全激发数据潜在价值。
	天享数据交换共享安全方案	方案提供跨网共享、敏感数据过滤、安全传输以及统一管理，为企业提供合规、安全、高效的跨网数据交换安全能力。
	天界数据跨境安全合规方案	方案将数据安全跨境评估能力与律师事务所的专业能力相结合，全面评估企业的数据跨境安全状况，帮助企业在数据跨境过程中理解法规要求，明确合规路径、确保合规操作。
云计算与云安全	原生安全超融合解决方案	通过安全与云计算深度融合创新，从系统层、存储层、业务层全面内置安全能力，并将安全原子、数据安全、隐私计算融入超融合内部，为以超融合为底座的云平台实现创建即安全的效果，是“云+安全”融合建设的最佳实践。
	太行云隐私计算解决方案	基于太行云平台，兼容多种隐私计算硬件，联合腾讯隐私计算和华为机密计算的相关产品和技术，提供互联互通平台、数据可信流通平台、机密虚机和机密容器等产品及服务。
	教育一朵云解决方案	通过利用云计算技术，以超融合架构，构建教育一朵云基础设施基座，提供数据中心云平台，二级学院科研计算平台，以及云桌面办公平台，完成全场景教学应用。
	医疗数据中心解决方案	以超融合架构为基础，构建医院外网、内网、灾备数据中心整体规划，构建临床业务、运营管理、科研应用等全场景业务承载平台。
	医疗云桌面解决方案	面向医院复杂终端建设场景，提供VDI与VOI两种桌面平台，为医院提供安全可靠、稳定兼容、管理简单的桌面终端建设模式，满足全场景建设需求。
工业互联网物联网车联网	基于“双融合”的数智转型升级安全解决方案	结合工业场景与安全需求，整合功能安全风险处置与信息安全威胁管控能力，构建融合安全体系，实现嵌入式底层技术、通信过程行为识别以及安全分析的融合应用。
	工业互联网数据安全一体化解决方案	方案涵盖工业互联网数据安全治理、组织建设、管理制度建设、技术能力建设、运营管控等维度，有效确保数据的可用性、完整性及保密性，全面提升数据安全管控能力。
	医疗IoT安全解决方案	基于对客户业务场景和实际需求的深入理解，综合数据安全理念提出基于物联网安全智能自动化识别、物联资产分类分级、物联网络接入、访问策略自动匹配的综合解决方案。
	密码+物联网安全创新融合解决方案	方案结合密码技术，增强智能设备指纹安全，并对各类加密流量建设、安全流量行为基线、对安全终端流量进行加密传输等内容，通过密码技术实现物联网接入过程的全过程安全。
	车联网态势感知解决方案	以大数据分析技术为核心，通过车内探针实时监控车端网络安全状态，提供安全事件动态感知、预警与处置、漏洞管理、告警评估、应急响应、海量数据分析和安全事件处理，为用户构建完备的车联网安全运营体系。
商用密码	商用密码应用安全建设方案	采用VPN、服务器密码机、签名验签服务器等核心产品，满足GB/T 39786《信息安全技术 信息系统密码应用基本要求》中网络和通信安全、设备和计算安全、应用和数据安全等要求，实现信息系统安全建设。
	基于商用密码技术的万物安全接入解决方案	方案融合商用密码、物联网物模型、物联网行为基线等技术，增强了物联网终端在网络接入过程中的身份认证、行为检测能力，有效保护物联网终端网络接入过程中各环节的网络安全。
	基于政务云商用密码应用安全建设方案	采用密码服务平台、云服务器密码机、协同签名系统等密码产品，为云上各租户提供密码服务，通过租用密码服务，满足GB/T 39786《信息安全技术信息系统密码应用基本要求》中的各项要求，实现信息系统安全建设。
	量子密钥的零信任网络通信安全解决方案	将量子密码技术、零信任理念与网络通信安全技术充分融合，以密码为基础、身份为核心，实现更细粒度的安全访问控制，进一步强化零信任远程访问过程中的网络访问控制安全强度。
安全运营	期货业团环安全运营体系建设方案	基于现有安全防护体系的基础上，为证券期货业机构构建“智能分析、纵深防御、高效可视”的安全运营体系，增强威胁分析、联动防御和自动化处置能力，整体提升证券期货业机构的网络安全运营能力。
	新一代漏扫实战化场景解决方案	方案全面支持云原生、大数据、工业互联网、物联网、国产化等新技术新应用场景，融合系统/Web/数据库/镜像/API扫描、基线检查、弱口令检测、配置审计等多种能力，并能与漏洞威胁情报、资产重要性等信息联动分析。
	一站式托管+平台化运营解决方案	依托安全云服务平台，全面支撑暴露面风险排查、网站安全监测、Web应用攻击防护、专项情报分析、事件通报预警等重保期间各类安全服务需求。
	API安全运营管控解决方案	该方案针对互联网医院业务API接口安全问题，提供API资产台账梳理、API管控策略优化、API监控态势分析、应急演练、安全运营平台等，保障互联网医院信息安全和业务顺畅流转。

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与方案销售、服务提供及能力订阅三种模式。

产品与方案销售：公司提供全系列网络安全、数据安全、云计算、云安全等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（包括知识库、威胁情报等），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年盈利模式数据如下：

表3-3 公司近五年盈利模式数据表

单位：百万元

项目	2019年	2020年	2021年	2022年	2023年
产品与方案销售	1,888	2,185	2,531	2,655	2337
服务提供	337	439	534	571	481
能力订阅	191	204	283	313	296
产品销售占比	78.16%	77.27%	75.60%	75.01%	75.05%
服务提供占比	13.96%	15.52%	15.95%	16.15%	15.44%
能力订阅占比	7.88%	7.21%	8.45%	8.84%	9.51%
合计	2,416	2,828	3,348	3,539	3,114

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，深入研究人工智能、大数据、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5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1700+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、服务和解决方案；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、主要业绩驱动因素

信息化发展、国家政策和公司经营拓展及管理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：数字经济发展、安全威胁加剧、国家政策法规等带来网络安全的持续需求，信息化的新场景带来新的安全应用。

2）公司经营拓展及管理