公司代码：688201　　公司简称：信安世纪

北京信安世纪科技股份有限公司 2024年年度报告摘要

第一节 重要提示

1、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https://www.sse.com.cn网站仔细阅读年度报告全文。

2、重大风险提示

业绩大幅下滑或亏损的风险

1、业绩大幅下滑和亏损的具体原因

报告期内，部分行业客户预算规模削减；部分客户采购节奏延缓，订单签订、项目交付、验收等环节延期；随着外部市场环境短期变化，行业竞争出现应激性反应，公司重视盈利能力，战略性放弃一些毛利率很低的项目。公司实现营业收入50,056.29万元，同比减少8.86%。管理运营方面，公司采取人员优化、降本增效措施，公司期间费用同比下降0.72%，共同导致公司实现归属于母公司所有者的净利润-4,781.76万元，同比减少526.08%。

2、所处行业景气情况，是否存在产能过剩、持续衰退或者技术替代等情形

信息安全行业近年来因国际形势，国家及行业出台了各类安全政策及行业合规的要求，人工智能、零信任、量子信息等前沿技术为网络安全产业发展注入新活力，信息安全技术得到了前所未有的发展。随着云计算、移动互联网、物联网、车联网、工业互联网等新业态、新应用、新场景的不断涌现，针对新技术环境下的数据安全和隐私保护等问题，不同行业都对网络安全和密码安全提出新需求，网络安全和商用密码市场仍将保持快速发展态势。报告期内，公司主营业务、核心竞争力均未发生重大不利变化，与网络安全行业整体趋势一致。

公司已在本报告中详细阐述公司在经营过程中可能面临的各种风险，敬请查阅本报告第四节“经营情况讨论与分析”中“风险因素”相关的内容。

3、本公司董事会、监事会及董事、监事、高级管理人员保证年度报告内容的真实性、准确性、完整性，不存在虚假记载、误导性陈述或重大遗漏，并承担个别和连带的法律责任。

4、公司全体董事出席董事会会议。

5、容诚会计师事务所（特殊普通合伙）为本公司出具了标准无保留意见的审计报告。

6、公司上市时未盈利且尚未实现盈利

□是　√否

7、董事会决议通过的本报告期利润分配预案或公积金转增股本预案

2025年4月25日，公司于第三届董事会第十一次会议审议通过了《关于<2024年度利润分配预案>的议案》，根据容诚会计师事务所出具的审计报告，公司2024年度实现归属于母公司所有者的净利润为-47,817,571.62元，母公司2024年度实现净利润为-68,011,163.58元，根据《公司章程》第一百六十三条，公司拟实施现金分红时应同时满足的条件之一为：“公司该年度实现的可分配利润（即公司弥补亏损、提取公积金后所余的税后利润）为正值”，尚不满足利润分配的条件，且为保障公司持续、稳定、健康发展，更好地维护全体股东的长远利益，拟定2024年度利润分配预案如下：不派发现金红利，不送红股，不以资本公积转增股本。

8、是否存在公司治理特殊安排等重要事项

□适用　√不适用

第二节 公司基本情况

1、公司简介

1.1 公司股票简况

√适用　□不适用

公司股票简况				
股票种类	股票上市交易所及板块	股票简称	股票代码	变更前股票简称
人民币普通股（A股）	上海证券交易所科创板	信安世纪	688201	不适用

1.2 公司存托凭证简况

□适用　√不适用

1.3 联系人和联系方式

	董事会秘书	证券事务代表
姓名	于艳	李明圆
联系地址	北京市海淀区建枫路(南延)6号院2号楼1层101	北京市海淀区建枫路(南延)6号院2号楼1层101
电话	010-68025518	010-68025518
传真	010-68025519	010-68025519
电子信箱	ir@infosec.com.cn	ir@infosec.com.cn

2、报告期公司主要业务简介

2.1 主要业务、主要产品或服务情况

公司以密码技术为核心，网络安全技术为基础支撑，致力于解决多种网络环境中的身份安全、数据安全和通信安全等信息安全问题，为各行业业务系统提供安全产品和解决方案。

公司产品分密码安全、网络安全、数据治理、涉密安全四个方面，并提供自有产品的维护服务。

1、密码安全

以密码技术为核心，完成网络环境中的身份认证、签名验证、隐私计算以及云计算、移动网络、车联网等业态下的对应产品，所有产品均已通过商用密码认证产品并取得型号认证证书，并适配各类不同信创环境。具体包含：

产品线	产品名称	产品介绍
身份安全	数字证书认证系统（NetCert）	是公钥密码基础设施解决方案的基础支撑系统，由CA数字证书认证系统、RA证书注册系统、KM密钥管理系统、OCSP服务器等组成，能够提供数字证书全生命周期的管理功能。支持X.509 V3/V4标准规范。采用安全的架构设计和权限管控，具备高级别安全机制及完善的管理、配置策略。
	动态密码系统（NetPass）	基于代表身份的密钥，结合时间、事件或挑战信息，实现了用户口令的“一次一密”特性，避免静态口令泄漏带来的安全隐患。为用户的合法身份认证提供了简捷、有效的认证手段。支持实体令牌、小程序令牌及短信令牌等多种形态动态令牌。
	统一身份认证管理系统（NetAuth）	提供单点登录、统一身份管理、统一身份认证、统一授权、集中安全审计等功能。统一适用于单位业务系统较多，需要提升IT管理员对业务系统帐号的管理效率，增强业务系统帐号的安全性，提供人员便捷的业务系统访问体验及等保、信创替代、密评、零信任等场景。
	安全认证网关（NetIAG）	以安全、合规为原则，融合零信任架构理念，提供基于商用密码技术的安全认证、网络隐身、动态授权、应用层动态脱敏和虚拟门户等安全功能，适用于零信任安全、旁路认证、移动安全办公等场景，在全面保障企业应用访问安全性的同时，最大程度简化接入过程，提升企业生产效率。
	车联网安全认证管理系统（V2X SCMS）	综合采用数字证书、数字签名、匿名化等技术手段，有效保障车载设备(OBU)、路侧设备(RSU)等V2X通信节点的身份合法性，以及通信消息的完整性、机密性、抗抵赖性、防篡改和隐私保护。可以为各类V2X终端设备签发符合相关标准的证书及全生命周期管理，提供制作各类BSM及SPDU消息的API，并提供全方位的安全监控及预警功能。
数据安全	签名验签服务器（NetSign）	能够对各类电子信息数据、电子文档等提供基于数字证书的数字签名服务，并对签名数据验证其签名真实性和有效性；支持不同CA的用户证书验证，提供CRL/OCSP等多种方式的证书有效性验证。满足用户在网络行为中不可否认、信息完整性、私密性等需求，并提供相关认证交易信息溯源验证。
	电子签章系统（NetSeal）	结合传统印章与电子签名技术，通过采用组件技术、PKI技术、图像处理技术等对电子文档签名并加盖签章。在保留了用户印章使用和管理习惯的同时提供了电子文档的完整性、真实性和抗抵赖性保护，为电子政务、企业办公、电子交易提供了安全与合规保障。
	可信时间戳服务器（NetTSA）	将经过时间戳服务器签名的一个可信赖的日期和时间与特定电子数据绑定在一起，对外提供精确可信的时间戳服务。通过采用精确的时间源、高强度高标准的安全机制，以确认系统处理数据在某一时间的存在性和相关操作的相对时间顺序，为信息系统中的时间防抵赖提供基础服务。
	密码模块软件（iSec）	是符合国密相关标准的软件密码模块产品，支持SM2、SM3、SM4商用密码算法及常见国际密码算法，可提供加解密、签名验签名、证书解析等基础密码运算功能，同时可提供TLS/TLCP等安全协议处理能力。
	视频安全一体机（NetVSG）	将网络协议解析技术与数字签名技术深度融合，为数据中心的视频监控系统提供透明、免改造的视频数据完整性保护服务，帮助用户以较低的投入、快速满足“密评”关于视频监控的相关合规要求。
	隐私计算平台（NetPEC）	是一种保护数据隐私的安全计算技术方案，以多方安全计算为基础，综合运用同态加密、混淆电路、不经意传输、秘密共享等技术，提供数据加密、安全计算、数据共享、数据授权等多种服务，在满足数据隐私、安全、合规的前提下，实现多机构的联合协同计算、数据融合与联合建模，拓宽了风控、营销和政企互联的覆盖能力，提升挖掘和使用数据要素所蕴含的巨大价值能力，解决数据孤岛和数据隐私保护两大问题，助力金融、保险、政务等领域的数据安全融合与共享流通。
	服务器密码机（UCypher）	能够为各类应用系统提供高性能、多任务并行处理的密码基础运算，支持SM1/2/3/4等多种国产密码算法，可以满足应用系统数据的签名/验证、加密/解密的需求，保证传输信息的机密性、完整性和有效性，同时提供安全、完善的密钥管理机制，提高系统整体安全防护能力。
移动安全	移动统一认证安全管理平台（MAuth）	采用密钥分割、协同签名、大数据分析感知等一系列技术，为移动端提供移动数字证书全生命周期管理及基于移动数字证书的协同签名服务，对移动应用服务提供签名数据验证其签名真实性和有效性，满足移动应用的基于数字证书的强身份认证、安全传输及抗抵赖性等安全需求，迅速提升移动互联网应用的信息安全防护能力。
	移动安全中间件（MAuth SDK）	采用密钥分割技术、移动隔离技术，与移动安全认证系统协同，实现在移动终端的密钥、数字证书全生命周期管理及密码运算，解决了加密硬件在移动端使用不便或无法与移动端结合的问题，提升了移动安全解决方案的兼容性和易用性。
	移动安全认证客户端（MAuth APP）	利用移动安全中间件构建的移动安全应用，能够通过“扫一扫”实现PC操作系统(Windows、Linux)或PC上各类应用的用户安全登录，为移动应用开发者和企业管理者提供简单快捷的基于数字证书的双因子认证解决方案；对各类移动应用的电子信息数据、电子文档等提供基于数字证书的协同签名服务，满足移动应用对信息不可否认、信息完整性、私密性等的需求。
云安全	云服务器密码机（CCypher-HSM）	保障云计算密码功能需求研发的高性能密码设备，通过虚拟化技术，可支持多个虚拟服务器密码机同时提供服务，并保持各个虚拟服务器密码机物理设备资源、密码运算资源等部件的共享与安全隔离，提供SM2、SM3、SM4等多种密码算法，满足应用系统数据的签名/验证、加密/解密的要求，能够为各类业务系统提供高性能、多任务并行处理的密码运算，保障信息的机密性、完整性和有效性。
	密码应用一体化系统（CCypher）	采用密码超融合技术实现的新一代密码基础设施专用一体机。产品配备高性能通用计算单元与专用密码运算单元，内嵌虚拟化管理系统与密钥管理机制，支持计算虚拟化、网络虚拟化、密码虚拟化等功能，单台设备可同时运行数字签名、电子签章、动态口令、SSL VPN等多种虚拟化密码应用。
	密码安全服务管理平台（CSSP- Cloud）	以“密码即服务”为核心理念，在安全、合规的原则基础上，实现密码设备资源池的弹性调度管理、典型密码应用服务的发布与管理、租户化管理与计费等功能的一体化密码云管理平台，可全面覆盖公有云模式、混合云模式、多云架构模式等复杂场景，完美解决用户在业务上云、数据上云过程中所面临的密码应用安全性合规难题。
平台安全	全密码安全服务平台（CSSP）	利用平台化技术手段实现识别、沉淀和复用密码服务，构建密码服务生态，提供标准化统一的密码服务和管理服务，有效支撑业务系统的快速创新；信安CSSP全密码安全服务平台结合客户自身业务发展的需要和监管方面的要求，从前台的业务接入到中台的统一调度到后台的密码设备统一管理以及整个业务运行状况的展示，为客户提供了全方位的密码安全服务。
	密码安全可视化监管系统（NetCVM）	采用B/S架构方式，提供统一、集中的密码应用设备集中监管服务，帮助用户实时监控密码应用设备的状态、密码服务的状态以及代理状态的监控以及密码应用日志的集中审计。
	密评工具箱系统(iCET)	是商用密码应用安全性评估工作的一体化专业便携装备，具有测评流程引导和管理、测评工具调用、测评结果分析和报告展示等功能；为测评机构提供了流程引导、数字化管理、以及专业的检测及分析工具。提高了密评工作整体的标准化、合规性和专业性。

2、网络安全

提供数据传输过程中的访问控制、安全代理加/解密、及性能优化，虚拟私有网络的远程安全接入，WEB通道的安全构建等功能，可以为应用系统打造一个安全、高性能的专属通信空间，提高系统整体的安全性。具体包含：

产品线	产品名称	产品介绍
通信安全	应用安全网关（NSAE）	支持基于证书的服务器和客户端身份认证，提供数据在传输过程中的机密性和完整性保护。全面支持SSL/TLS协议，配合产品自带的负载均衡、防火墙、HTTP压缩等功能，为应用系统提供全方位的安全代理和应用加速服务。
	应用交付系统（APV）	具备服务器负载均衡、链路负载均衡、全局负载均衡功能、HTTP主缓和WEB高速缓存等功能的专业硬件设备，打造网络安全资源池，实现设备与流量的统一调度，满足了个性化、差异化的安全流量编排需求，帮助用户提高业务应用稳定性和质量，避免服务器宕机或链路故障对业务应用的影响，确保用户的业务应用能够快速、安全、可靠地交付以及按需扩展。
	安全互联网关（NetSafe）	基于SSL安全协议实现的安全加密认证通信客户端硬件产品。集成身份认证、SSL安全链接、数字签名、验证签名、日志审计等功能，保证关键数据的数据安全，实现关键数据的防篡改、抗抵赖和数据提供方身份的真实性验证，为企业内部网络和银行、互联网电子商务等应用服务器之间构建安全的Web通道，保证交易数据的安全传输。
	安全接入网关（AG）	基于IPSec和SSL技术实现远程接入、跨区域组网的综合安全VPN平台。支持SSL加速、AAA认证、IPSec组网、虚拟站点、单点登录等功能，适用于远程办公、移动办公、多分支机构组网等场景，可为用户提供安全、高效、快速、稳定的远程接入方式，实现随时随地的安全访问。
	应用安全防火墙（ASF）	采用先进的64位SpeedCore多核处理架构，为关键业务应用提供全面的攻击和威胁的检测与防护。集负向WAF和正向WAF模型于一身，不仅能够检测和防范最新的已知安全攻击和漏洞，还能有效地防范“零日”攻击。可提供精细化的攻击防护控制，支持自动学习和动态防护模板刷新，通过客户端源认证提高攻击识别精度。

3、数据治理

公司凭借多年的安全产品研发与项目实战经验，发布了“1+2+N”数据安全治理能力框架—数据安全治理产品系列(Dsec)，通过敏感数据识别、协议解析、端口扫描、数据加密、脱敏等核心技术，实现数据分类分级、访问控制、风险识别、数据脱敏、数据加密、数据审计等功能，协助用户构建完善的数据安全治理体系。具体包含：

产品线	产品名称	产品介绍
态势感知	数据安全态势感知平台（DSecDSA）	以安全风险管理为核心的综合性平台，利用多维度的量化指标，精准描绘数据资产分布及数据安全实时风险。平台通过数据安全分析引擎实现对数据风险的主动发现、精准定位、智能研判、协同处置以及严格审计，进而助力用户构建数据安全运营中心，实现数据安全保护工作的闭环处置。
管控平台	数据安全管控平台（DSecDGP）	数据资产梳理、数据脱敏、数据审计等各类数据安全子系统的统一管理中心。平台通过标准化的管理接口实时获取全域数据资产分布情况及安全防护状态，并将数据分类分级标签作为策略联动基础，为安全管理人员提供流程化、自动化的数据安全策略管理能力，进而支撑用户高效开展常态化、合规化的数据安全治理工作。
	数据安全流转管控平台（DSecDFC）	将“流程表单”与“数据安全”技术深度融合，面向数据共享外发场景提供工作流审批、数据保护、数据溯源等综合安全能力。平台支持自定义数据审批工作流，对数据访问全流程进行灵活管控与审计；同时基于数据分类分级标签按需实现加密及脱敏；结合明暗水印技术，进一步实现数据文件及数据集的精准溯源。
治理系统	数据资产梳理与分类分级系统DSecDAC	以全数据梳理为核心目标的智能化产品。采用静态网络扫描和动态流量识别相结合的方式，建立精准可靠的数据资产台账，形成完整的数据分类分级清单，自动绘制全方位的数据资产地图以及动态监测数据资产状态，帮助用户一站式解决组织内数据资产的管理、使用、统计、合规问题，并为数据安全防护提供基础策略支撑。
	数据加解密服务系统（NetEDS）	基于商用密码算法与技术实现的高性能数据安全产品，拥有“强安全”“多场景”“高性能”三重优势，提供统一密钥管理、通用数据加解密、数据库加解密及凭据管理等安全服务，能够对敏感数据和重要信息等进行加密保护，有效降低因数据泄露带来的安全风险，帮助用户切实履行《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规要求的数据保护义务。
	数据静态脱敏系统（DSecDMS-SDM）	是一款高性能、高兼容、智能化、全场景的数据仿真产品。系统支持抑制、泛化、扰乱和随机四大类脱敏技术共计数十种算法和策略，使脱敏后数据具备“保真性”“关联性”“可逆性”“可重复性”“时效性”“安全性”等特性，满足测试、开发、数据分析等不同场景的安全与合规要求。
	数据动态脱敏系统（DSecDMS-DDM）	完全满足用户对数据库安全管控的需求，充分解决了运维人员、业务人员及第三方人员访问时的权限管控与数据脱敏问题。产品依据用户的角色、职责和其他IT身份特征，动态对生产数据库返回的数据进行专门的屏蔽、加密、隐藏和审计，实现在业务系统无改造情况下用户身份的可信和访问内容的可控，有效防止敏感数据的越权访问及泄露。
	数据库运维管控系统（DSecDMC）	针对敏感资产及敏感操作，提供数据库访问的最小化权限访问控制能力，解决数据库运维侧安全问题。系统将事前审批、事中控制、事后溯源贯穿整个运维过程，支持数据库准入控制、访问控制、运维审批、动态脱敏、全程审计、结果统计等核心功能。实现数据库运维侧多元化管理，解决敏感数据泄露、越权操作、高危风险操作等各类数据安全问题。
	数据库防火墙系统（DSecDBF）	以数据资产为防护核心，聚焦业务侧入侵风险防护，防止数据库由于应用程序逻辑漏洞或缺陷导致的数据安全问题。系统基于数据库协议解析与访问控制技术，提供虚拟补丁、访问控制、双白名单、三层关联等功能，使数据库免受漏洞攻击、恶意操作、SQL注入等威胁，全方面保障数据库安全，同时帮助用户满足法律法规的要求。
	数据库审计系统（DSecDBA）	信安数据库审计系统是一款对数据库访问行为进行记录、监控、跟踪溯源的安全产品。基于数据库协议解析分析技术，实现细粒度的双向审计、精准化行为回溯、用户行为风险分析、灵活报表模板、全方位风险告警等多重安全能力。帮助用户构建全面的数据安全防护体系，降低数据泄露和监用的风险，确保数据资产的安全性。
	API安全风险监测系统（DSecASM）	基于流量分析技术实现的应用层安全审计产品，提供API资产梳理、API访问记录、API风险监测、API敏感数据发现等功能。产品具有检索性能极高、风险模型丰富、行为审计粒度细等特点，能够帮助用户在海量流量中精准发现隐藏的API资产、动态监测API的敏感数据访问情况、标记API异常访问行为，真正实现API可视化安全管理。
	数据安全协同运营平台（DSecCOP）	数据安全协同运营平台以“协同”为核心，构建一体化安全运营体系。平台将“数据敏感度、数据流动行为、策略基线”等信息进行多维监测分析，从数据资产、安全风险、合规差距、安全状态等 多个视角呈现数据安全运营态势。配合流程工单及数据安全知识库，推动数据安全滚动治理，实现常态化数据安全运营。
	API安全监测与防护系统（DSecASG）	以API生命周期管理为核心，对API及传输数据进行监控、管理和保护。系统支持流动监测、访问控制、数据加密等安全机制，统一管理和保护接口数据安全。对外统一提供规范接口、认证授权、对内实现负载均衡，流量控制，确保API使用过程的高性能、高可用与安全性。

4、涉密安全

公司针对涉密载体管控，已全面布局从载体输入、载体输出、载体在位、载体出入到载体回收的安全管控，可为客户提供涉密载体的全生命周期产品体系。具体包含：

产品线	产品名称	产品介绍
终端安全	“科云”光盘安全隔离与信息单向导入系统	针对两个物理隔离网络之间数据跨网传输的需求，采用模拟人手工操作光盘方式，实现由外部网络到内部网络数据自动单向无反馈传输。
	“科云”影像摆渡单向导入系统	通过显示屏和摄像头模拟人眼观察目标的单向信息传递模式，采用先进的二维码及纠错技术，发送端和接收端无物理介质连接形态，实现由外部网络到内部网络数据自动单向无反馈传输。
	“科云”网络安全隔离与信息单向导入系统	光纤型：采用标准“2+1”架构设计，采用单向光纤传输通道，通过协议剥离、私有协议转换等隔离技术，实现由外部网络到内部网络数据自动单向无反馈传输。
		大气激光型：采用特制的空气隔离装置，通过空气传输单向光信号，实现由外部网络到内部网络数据自动单向无反馈传输，具备更好的安全隔离性。
	“科云”网络安全隔离与信息交换系统	通过协议剥离、私有协议转换等隔离技术，在保持逻辑隔离的状态下实现双向交互式应用数据的代理转发。
	“科云”数据跨网交换一体化设备	依据跨网GJB标准中的安全保密建设体系要求设计，将标准中各区域需要的安全软硬件和单向导入系统集成到一个设备内部署，采用标准机架式设计，极大的解决了跨网设备占用空间大、部署维护难等问题。
	“科云”数据交换网关	对进行跨网传输的用户、应用和设备进行安全核查和身份认证，确保安全合法实体的接入，实施加密保护和完整性保护，对交换数据进行各项安全检查，并按转发范围转发从隔离器接收的数据。
	“科云”互联缓冲代理网关	采用标准机架式设备，配有千兆网络电口和可扩展光口，具备数据审核、设备调度、转发控制、设备互认证、日志审计和系统管理等功能，用于强化对两网跨网数据的检查，作为数据安全交换代理网关的一个补充。
	“科云”接入控制网关	对进行跨网传输的用户、应用和设备进行安全核查和身份认证，确保安全合法实体的接入。
	“科云”数据安全交换代理网关	对跨网传输数据添加标识，实施加密保护和完整性保护，实现跨网数据的安全引接；对交换数据进行各项安全检查，根据配置调度相应隔离器进行数据传输，并按转发范围转发从隔离器接收的数据。
	“科云”业务协议代理网关	采用标准机架式设备，配有千兆网络电口和可扩展光口，具备业务协议代理、设备互认证、日志审计和系统管理等功能，该网关用于交互式双向应用协议向双单向协议的转换，即双向交互式应用才需要业务协议代理网关。
	“科云”交换管控与审计网关	对跨网交换的基础设施设备和交换应用、用户实施统一的运行监控和管理，对跨网跨域数据交换行为进行全流程审计，进行相关统计分析，并及时发出告警，支持对历史跨网交换行为进行全流程回溯、还原。
	“科云”跨网个人文件同步系统	针对内网用户导入外部文件数据需求，实现在两个网络物理隔离的条件下，与跨网传输系统结合，用户通过电脑、手机上传数据，跨网数据导入系统将数据导入到内网，实现数据的自动导入，信息及时全面的共享。
	“科云”跨网网站栏目同步系统	针对单位内部网站数据资源导入需求，以导入互联网或其他网络网站信息资源为目的，与跨网传输系统相结合，自动从外网抓取指定的网站栏目信息，通过跨网设备自动导入单位内网，并同步到内网内容管理系统进行发布展示。
	“科云”跨网事务提醒系统	针对内部业务系统产生的消息能够对用户进行提醒需求，系统通过与跨网传输系统结合，将内网业务系统产生的实时消息信息，通过跨网设备输送到外网，并以短信等形式发送至用户手机，使用户能够及时收到业务提醒，达到实时高效的移动办公效果。
	“科云”保密综合管理系统	具有对计算机终端安全管控、涉密电子文件全生命周期的可追溯和审计、电子信息集中加密存储、纸质文件打印复印输出、电子文件刻录复制外带等行为严格管控和审计等能力，全方位保护计算机终端运行环境和涉密数据的安全可控。
	“科云”主机监控与审计系统	针对涉密领域或安全等级较高行业用户终端安全保护需求，实现终端准入控制、合规检查、网络访问控制、桌面行为管理、外设及接口管理、移动磁盘管理和终端安全加固，对违规行为可实施断网、锁定、关机等处理手段。
	“科云”集中管控系统	采用保密管理的操作流程，针对“终端不存密”的安全保密要求开发设计，在终端操作系统环境中创建出一个受保护的、可控的相对封闭的安全隔离工作环境，对单位日常办公中产生的涉密电子信息实施集中存储、加密保护，并通过严格的身份认证、授权访问控制和全程审计等安全机制，实现用户对文件的所有操作均可控可查和文档生成、编辑、保存、输出全过程保护。
	“科云”打印刻录复印安全监控与审计系统	针对文印输出介质全生命周期管理而设计，以集中文印输出管理方式实现打印、复印、刻录输出的全流程管理与审计，并通过建立安全的文件输出机制，实现文印管理、业务审批、内容监控、身份认证、权限管理和标识嵌入、输出文件回收等功能。
	“科云”文印交互终端	针对集中文印系统用户在文印室或文印点现场操作需求设计，实现集中文印系统输出时的身份认证和任务管理功能。
	“科云”光盘打印刻录一体机	采用机电一体化设计，提供光盘刻录输出的同时实现盘面信息自动打印及载体信息记录。具有涉密载体标识条码以及图片、文字等多种类型信息的盘面打印功能，可有效支持涉密载体追溯。
	“科云”文件自助回收柜	将载体的自动化回收和涉密文件柜相结合，通过与集中文印系统或载体管理系统对接，实现对打印、复印、刻录输出的纸质文件和光盘进行自助回收。支持人脸识别、指纹、IC/ID刷卡等多种身份认证方式。有效消除涉密载体回收的安全性和效率之间的矛盾。
	“科云”安全保密套件	安全保密套件依据相关安全保密要求和标准规范，针对信创领域中通用主机的安全防护设计和研发，通过违规外联管控、身份鉴别、主机监控审计、接入控制、数据访问控制等多样的安全防护手段和多层次的安全管理措施，实现单位内部的主机安全和信息安全，保护数据免遭泄露和未经授权的访问，为单位构建一个全面可控的安全防御体系。
	“科云”离线文件单向导入系统	采用国产飞腾处理器和麒麟操作系统，配有触摸屏、内置服务器、只读光驱、摄像头、刷卡器等组件，具备用户身份认证、文件导入、数据安全检查、病毒查杀、断点续传、数据接收与转发、日志审计等功能。
	“科云”RFID智能交换柜	是一款基于RFID射频识别技术的高效智能化管理设备，专为涉密文件、重要物品的安全存储与流转设计。通过自动化识别与数字化管控，实现物品的精准定位、快速存取和全流程追溯，大幅提升管理效率与安全性，适用于政府、军工、金融、企业等高保密需求场景。
	“科云”涉密载体交换管控系统	涉密载体交换管控系统针对涉密载体在交接、流转过程中的安全管控需求而设计，通过智能化技术实现载体交接的全程可追溯、权限精细化控制及异常行为实时告警。系统以RFID智能交换柜为核心硬件，结合管控平台软件，对载体的取出、归还、转交等操作进行动态监控，确保载体在授权范围内有序流转，杜绝泄密风险。
	“科云”自助输出一体机	自助输出一体机将身份认证与输出控制、光盘刻录和纸质文件打印等功能集于一身，与集中文印系统部署在同一网络协同工作，为用户提供文印输出的一体化一站式服务，适用于文印室、楼道、大厅等公共服务场景。
	“科云”基于射频识别的涉密载体在位监控系统	基于射频识别的涉密载体在位监控系统针对载体存储位置的实时监控需求而设计，其核心设备为RFID智能存储柜，可实时检测载体所处位置，在涉密载体管控系统软件的配合下，可实现对单位辖区内所有登记载体的在位情况进行实时监控，及时发现异常并进行告警，支持载体丢失告警、错放位置告警等。
	“科云”涉密载体管控系统	用于对纸质文件、光盘、U盘、移动硬盘、便携机等涉密载体的制作、应用、流转、回收归零等多个环节的管控。
	“科云”基于射频识别的涉密载体出入管控系统	基于射频识别的涉密载体出入管控系统针对实时监控载体离开受控区域的需求而设计，在涉密载体管控系统软件的配合下，可检测到未授权带出载体并进行声光告警，及时提醒安保人员阻止载体的异常带出行为，规避失泄密风险。设备基于国产自主可控软硬件平台，适应不同的出入口安装条件，实现大范围内涉密载体RFID标签的快速精准识别，通过多型传感器，实现载体出、入双向检测和统计，适用于多种涉密敏感区域的出入监控管理。
备份归档	“科云”数据归档蓝光阵列	针对数据长期保存、永久保存需求而设计，采用磁盘缓存与蓝光光盘相结合的混合存储架构，利用蓝光存储介质和自动化光盘库的优势，结合数据备份归档系统软件，通过高速磁盘缓存技术及多台光驱并发工作原理，实现海量数据长期安全存储、快速查询与下载，统计分析等数据管理需求。

5、服务

公司具有信息安全服务资质，包括风险评估、安全运维、安全开发、安全应急、安全集成，目前向客户提供自有产品的运维服务、安全技术咨询和风险评估、定制开发服务等。

2.2 主要经营模式

公司主营业务为信息安全产品的研发、生产及销售，为客户的数字化环境和网络应用提供安全产品和解决方案、提供自有产品的服务，保障在多种网络环境下的身份安全、数据安全和通信安全。公司具有完善的研发、采购、生产、销售、服务模式和流程，实现对经营各环节的增效降本，提升经营效率。

1.研发模式

公司坚持“前沿技术驱动创新+业务需求驱动创新”的双线创新机制，以技术创新为驱动、市场需求为导向进行新产品规划。在软件成熟度模型CMMI L5、TSM可信研发运营安全能力成熟度评估和ISO 9001质量管理体系的规范指引下，公司建立了完善的研发制度和管理流程，从产品需求、设计、编码、测试到发布的各环节进行产品的全生命周期进行管理，保证产品质量。

2.采购模式

公司采购的主要物料为软硬一体机产品所需的各类硬件设备和配件，包括服务器、加密卡、加速卡等硬件，公司建立了独立、完整的供应链体系，包括供应商管理、重要物料招标和采购等环节。公司定期对供应商就资质、供货质量、规模和交货期等进行评估，并要求符合环保、工序变动通知等要求，建立稳定的商务合作关系。对重要物料进行招标以保证质量。公司采购计划以库存预警式为主，订单驱动式为辅，通过签订订单、跟踪交期、检验入库、给付货款等环节，来保证供应链正常进行。

3.生产模式

公司的产品形态主要为软硬一体机，需要将自主研发的软件灌装至硬件设备。生产环境恒温恒湿，全部铺设防静电地胶，按生产工序划分区域，设置明显标识，建立独立的局域网，与外网隔绝，以防病毒和恶意软件攻击。公司建立了包括原材料质量管理、生产过程控制、产成品出入库等方面的全过程质量管理，采用数字化系统管理严格管控，确保产品的质量符合规定要求，保质保量交付至下游客户，公司顺利通过国内龙头企业的供应商认证，制程能力获得高端客户的认可。

4.营销模式

公司采取“纵向深耕行业，横向拓展区域”的矩阵式销售模式，建立了全国性营销网络。建立重点行业销售团队，深刻理解行业需求和特点，应用中心节点的顶端优势，打造行业典型解决方案；建立北京总部和华北、华东、华南、华中、西南、西北、东北等七个大区及各省级办事处，积极和各地合作伙伴合作，拓展业务局面。

5.方案和交付模式

公司在北京总部和各大区均设立了产品方案中心和服务交付中心，由多年形成的专业化信息安全队伍提供标准化服务，形成了覆盖全国的营销服务网络。公司的产品方案中心依据信息安全相关技术标准，结合客户的安全需求和痛点，向客户提供完整先进、贴合应用的产品和解决方案。服务交付中心遵循ISO质量管理、信息安全管理、IT服务管理标准体系理念，向客户提供产品交付、质量保障、运行维护等专业化的标准安全服务，并对重点行业、重点客户提供的全天候安全保障、关键时段值守、重点保障、应急处理等金牌安全服务，保证客户业务系统的安全性和连续性。

2.3 所处行业情况

(1). 行业的发展阶段、基本特点、主要技术门槛

（1）行业发展阶段

随着数字化进程的开展，商用密码技术在不断发展，零信任、隐私计算、数据安全、后量子密码、智能威胁检测等新技术的发展，带来了基础架构升级，并带动了安全技术的创新和安全边界的拓宽，推动安全防御向自动化、智能化转型，信息安全行业进入了动态积极防御阶段。

各行业的安全需求也在同步增长，网络安全与低空经济、卫星互联网等新兴领域融合趋势日趋明显，带动了网络安全边界的扩展，进而促使信息安全的需求在不断增长。数字化应用较先进的客户对自身业务场景的安全需求正在不断提升。网络安全市场面临需求驱动、价值驱动，与新场景适配、高价值应用、实战化运营相关的安全需求将越来越多。

近年来，政策环境持续优化，国家通过《网络安全法》《数据安全法》等法规体系完善顶层设计，明确了信息安全与信息化发展并重的战略地位，提升了企业和个人的安全意识，也为网络安全市场提供了明确的合规指导。安全合规的要求与市场需求形成了双重驱动，促进了市场的健康发展。

据IDC发布的《全球网络安全支出指南》，中国网络安全市场规模预计从2023年的110亿美元增长至2028年的171亿美元，五年复合增长率为9.2%，其中，网络安全软件以11.5%的五年复合增长率增长。包括金融、政府、电信业、资本市场和医疗在内的行业，因数据密集性和敏感性，对网络安全需求更高。

（2）行业基本特点

从网络安全产业链看，上游为设备、系统等供应商，如芯片、内存、操作系统、引擎等；中游为不同细分领域的网络安全产品和服务厂商，如安全软件或运维、安全服务等；下游为应用领域，如金融、政府、军工等相关领域。行业具有以下特点：

行业特点一：政策鼓励和合规监管的强力驱动

近年来，国家高度重视网络空间安全及密码安全领域，继《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等重要法规后，2024年，国家和相关部委继续出台了多个政策，涉及密码安全、网络安全和涉密系统的相关信息安全法律法规体系逐步完善，为筑牢网络与信息安全防线，维护国家安全、社会公共利益以及保护公民合法权益提供了坚实有力的法治保障。

2024年9月，国务院颁布《网络数据安全管理条例》，明确提出网络数据处理者要在等级保护基础上，加强网络数据安全防护，建立健全相关管理制度，采取加密、备份、访问控制、安全认证等措施，保护网络数据免遭篡改、破坏、泄露或者非法获取与利用。2024年11月，国家密码管理局研究起草的《关键信息基础设施商用密码使用管理规定（征求意见稿）》，对关键信息基础设施商用密码使用管理要求的进一步细化。2024年11月，国家密码管理局发布《商用密码检测机构（商用密码应用安全性评估业务）目录》，标志着标准化、规范化的密评工作正式展开，推动信息安全行业健康发展。

此外，2024年《银行保险机构数据安全管理办法（公开征求意见稿）》《工业领域数据安全能力提升实施方案（2024—2026年）》《民航数据管理办法（征求意见稿）》《自然资源领域数据安全管理办法》等各行业管理部门发布的政策法规，也为行业领域内数据安全提出了规范要求。

序号	发文时间	发文单位	名称	主要内容
1	2023年12月	国家数据局	《“数据要素×”三年行动计划(2024—2026年)》	到2026年底，数据要素应用场景广度和深度大幅拓展，在经济发展领域数据要素乘数效应得到显现，打造300个以上示范性强、显示度高、带动性广的典型应用场景，数据产业年均增速超过20%，数据交易规模增长1倍。
2	2024年2月	全国人民代表大会常务委员会	《中华人民共和国保守国家秘密法》	保守国家秘密，维护国家安全和利益。