

公司代码：688225

公司简称：亚信安全

亚信安全科技股份有限公司 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 www.sse.com.cn 网站仔细阅读年度报告全文。

2、 重大风险提示

公司已在本报告中详细描述可能存在的相关风险，敬请查阅《2024 年年度报告》第三节管理层讨论与分析“四、风险因素”部分内容。

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、 致同会计师事务所（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

经致同会计师事务所（特殊普通合伙）审计，公司2024年度实现归属于上市公司股东的净利润为9,590,639.77元。截至2024年12月31日，母公司期末未分配利润为-24,221,165.15元。

根据中国证监会《关于进一步落实上市公司现金分红有关事项的通知》《上市公司监管指引第3号——上市公司现金分红》《亚信安全科技股份有限公司章程》等的相关规定，2024年12月31日母公司期末可供分配利润为负值，尚不满足利润分配条件。综合考虑公司经营发展战略和业务发展规划，为更好地维护全体股东的长远利益，保障公司长期稳定发展需求，经董事会决议，公司拟定2024年度不进行现金分红，也不进行资本公积金转增股本和其他形式的利润分配。

本次利润分配方案尚需提交公司2024年年度股东大会审议。

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
A股	上海证券交易所科创板	亚信安全	688225	/

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	王震	李宝
联系地址	北京经济技术开发区科谷一街 10 号院 11 号楼 13 层	北京经济技术开发区科谷一街 10 号院 11 号楼 13 层
电话	010-57550972	010-57550972
传真	010-56521402	010-56521402
电子信箱	ir@asiainfo-sec.com	ir@asiainfo-sec.com

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

亚信安全是业内具备安全+数智全栈能力的软件企业，是中国网络安全软件领域的领跑者。2024 年 11 月亚信安全完成对亚信科技（港股代码 01675.HK）的重大资产重组事项，以“懂网、懂云、懂安全”为优势基因，打造“云网安”一体的能力体系，赋能产业数智化的发展与变革。亚信安全业务体系主要由网络安全业务、数智业务两大板块构成。

1、网络安全业务

亚信安全专注于网络空间安全领域，向政府、企业客户提供网络安全产品和服务。客户广泛分布于电信运营商、金融、政府、制造业、能源、医疗、交通等关键信息基础设施行业。公司在云安全、终端安全、身份安全、安全管理、高级威胁治理及 5G 安全等领域拥有优势性技术实力，实力筑牢云、网、边、端的安全防线，并广获业界认可。亚信安全在中国网络安全电信行业细分市场市场份额占比第一，连续多年蝉联身份安全中国市场份额第一，终端安全中国市场份额占比第二，在云主机安全、威胁情报、EDR、XDR 等细分技术领域均居于领导者象限，是中国网络安全企业十强之一。公司网络安全业务包括网络安全产品、网络安全服务、云网虚拟化软件产品三大部分，

其中网络安全产品主要包括数字信任及身份安全产品体系、端点安全产品体系、云网边安全产品体系。

业务类别	产品体系	业务介绍	交付形式	典型应用场景
网络安全产品	数字信任及身份安全产品体系	数字信任及身份安全产品体系以身份识别与访问控制、数据安全相关的产品为主，为用户提供与数字身份相关的账号管理、接入认证、权限控制、访问过程审计以及数据安全管控等功能，保障用户以可信的数字身份接入网络或系统，在授权的范围内操作系统、访问和使用资源，同时能够对用户访问记录和使用数据情况进行监控分析，从入口和出口两个方向为政企用户的系统和数据提供安全防护，为用户打造可信任的数字化应用体系。	软件或软硬一体	主要解决客户在数字身份及数据资产管理的网络安全建设方面需求，如确保具备权限的用户才能访问网络、登录系统、访问资源和执行业务操作；对用户访问系统和数据的记录进行审计分析，防止敏感数据泄露等。该体系产品主要应用于电信运营商、政府、金融、能源等中大型企业。
	端点安全产品体系	以终端安全、云安全、高级威胁治理和边界安全产品为主，通过在不同的位置部署该体系产品，可以为用户的 IT 系统、资源和终端设备提供多方面的安全防护；通过在内网和外网的边界处部署高级威胁治理和边界安全产品，可以对进出组织的网络流量进行深度识别和分析，阻断带有一般恶意程序和高级威胁的流量进入内网；通过在终端设备上部署产品，可以有效发现和查杀入侵终端设备的恶意程序，保障终端设备的正常运转；通过在云主机、云计算服务器等介质上部署产品，可以增强云端资源抵御恶意程序攻击的能力。	软件或软硬一体	主要解决客户在终端、网络节点和云上的网络安全建设方面需求，该体系产品广泛应用于政府、电信运营商、金融、能源、医疗、制造业等各行业客户。
	云网边安全产品体系	主要聚焦在 5G 技术发展体系和云网融合的网络架构演进趋势下，利用威胁情报及大数据技术，提供智能化的态势感知分析、安全事件闭环管理及综合性网络安全管理能力。云网边安全产品体系着重于从用户进行安全运营及网络管理的全局视角出发，解决网络空间资产及网络设备管理、安全事件及威胁情报的关联分析及决策响应、安全管理及运营自动化、基础网	软件或软硬一体	主要解决客户在安全管理及网络管理的建设方面需求，如通过建设态势感知平台，联动其他安全设备能力，实现客户全天候、全方位的网络威胁识别、预警和处理能力；通过建设域名解析及网络准入系统，为运营者提供域名解析、安全防护、数据分析、安全监管等网络管理能力。该体系

		络运维管理等问题。综合采集处理多源数据，实现对安全对象的主动管理、安全空间内外部威胁与行为的实时监测，威胁事件智能分析和通报处置，联合威胁情报狩猎追踪，精密编排自动响应准确检测及制止威胁。		产品主要应用于电信运营商、政府、金融、能源、制造业等中大型客户。
网络安全服务	网络安全服务	提供全面的网络安全服务，包括威胁情报、高级威胁研究、红蓝对抗、攻防渗透、互联网资产弱点分析、风险评估和安全培训服务等多项业务，通过这些服务，能够有效提高客户的安全意识，增强客户抵御网络安全威胁的能力。	服务	主要解决客户在网络安全服务方面的需求，主要应用于电信运营商、金融、能源、政府等中大型客户。该体系产品的主要交付形式为根据客户需求，通过专家团队及能力中心为客户提供网络安全咨询等一系列服务。
云网虚拟化产品	云网虚拟化产品	为满足现有客户提出的云化转型及安全合规的需求，公司拓展与云基础架构领导厂商的业务合作，共同推进运营商及行业客户云网基础设施和云化管理运维方案的落地，以及和公司现有安全产品服务结合的探索。用户通过将该产品安装在通用的物理服务器上，将计算、存储、网络等功能与物理服务器进行解耦，虚拟成可灵活调用的云端计算、存储和通信资源，增强其 IT 系统的灵活性和可拓展性。	软件或软硬一体	主要解决客户在云计算虚拟化基础设施建设方面需求。

2、数智业务

2024 年 11 月公司完成对港股亚信科技控股有限公司（港股代码 01675.HK）的重大资产重组事项，亚信科技作为亚信安全的控股子公司整体纳入亚信安全的数智业务板块。亚信科技是国内领先的软件产品、解决方案和服务提供商，综合运用咨询规划、产品研发、实施交付、系统集成、数据运营、智能决策、客户服务等数智化全栈能力，为千行百业提供端到端、全链路数智化服务。亚信科技深耕数字化领域 30 余年，在 5G、云计算、大数据、人工智能、物联网、数智运营、业务及网络支撑系统等领域具有先进的技术能力和众多成功案例，客户遍及电信运营商、广电、能源、政务、交通、金融、邮政等行业。亚信科技秉承“一巩固、三发展”战略，坚持“产品与服务双领先”，高质量巩固 BSS 市场的领导地位，高速度发展数智运营、垂直行业数字化和 OSS 等新兴业务。亚信科技积极拥抱 5G、云计算、大数据、AI 大模型、物联网等先进的技术，形成了云网、数智、IT 三大产品体系。亚信科技产品及能力体系以各类基础设施为基础，以 AI 中台、数据中台及技术中台为支撑，形成了以 BSS 业务为基本盘，以 OSS、数智运营及垂直行业数字化为新业

务驱动的业务体系。

业务类别	业务介绍	交付形式	典型应用场景
业务支撑系统 (BSS) 业务	BSS 是一种用于客户信息、客户业务、服务流程以及与客户相关的服务及资源管理，通常与网络支撑系统 (OSS) 一起构成通信行业端到端综合业务运营管理系统。BSS 通常包括计费、结算、账务、客服、营业等模块，是面向运营业务和服务的前端支撑系统。通过该系统，电信运营商能够对用户执行相应的业务操作，提供各类电信服务。	软件、服务、软硬一体	电信运营商、广电等领域的计费、结算、账务、客服、营业等场景
网络支撑系统 (OSS) 业务	OSS 是通信运营商支撑网络运作的软件解决方案，是电信运营商的一体化、信息资源共享的支持系统，用于监控、分析和管理的电信网络。	软件、服务、软硬一体	电信运营商等领域的电信网络监控、分析、管理等场景
数智运营业务	数智运营业务以数据治理为基础，以数据智能为方向，为企业提供咨询规划、数据要素的管理加工和可信流通、人工智能模型的生产与服务，在支撑通信运营商领域通用智能的同时，赋能汽车、消费、金融等行业客户数字化转型升级。	以服务、研究报告等多种形式交付	面向千行百业的数字化营销、数字化治理、效率提升、咨询规划等场景
垂直行业数字化业务	垂直行业数字化业务主要聚焦于金融、能源、交通、政务和邮政等战略性垂直行业，提供企业数字化整体解决方案，如为能源行业提供 5G 专网解决方案、为政务行业提供大数据平台解决方案及服务以及为交通行业提供智慧高速解决方案等。	行业整体解决方案	能源行业：核电、风电、光伏、矿山等领域的 5G 专网、智慧解决方案等场景； 政务行业：政务互联网大数据及软件平台； 交通行业：智慧高速（如高速计费及大数据平台）、智慧枢纽（如枢纽交通管控、人员管控等）、数智物流（如货运数据服务、物流可视化服务等）

2.2 主要经营模式

1、销售模式

公司网络安全业务主要涉及网络安全产品销售、为客户提供专业的网络安全解决方案和安全服务。网络安全业务采取直销与渠道代理销售相结合的方式，对于电信运营商、金融、能源等领

域的头部大型客户，公司一般采用直销的方式，安排专门的销售及业务团队为其进行服务；对于其他客户，公司一般采取渠道代理销售的方式。

公司数智业务主要采用直接销售的销售模式，通过招投标、商务谈判等方式进行销售。通常情况下，对于 BSS 业务、OSS 业务而言，对于首次合作客户，客户通常采用招投标的方式确定供应商，对于后续合作，客户通常采用商务谈判等方式进行。公司配备专员对市场招标信息进行收集整理，经内部评估后执行投标程序；对于无需采用招投标的用户，公司通过协商谈判的方式与客户确定项目需求、确定项目价格并签订业务合同。

2、采购模式

公司采购主要分为软硬件物料采购和技术服务采购两大类。软硬件物料采购主要系为满足客户需要而采购的非公司自有的硬件（如服务器等通用设备及行业特殊设备等）、软件（如操作系统等通用软件及部分行业特殊软件等）、产品包装物等产品。技术服务类采购主要系项目制技术服务、人天/人月类技术服务两类。

公司制定了《采购管理制度》《供应商管理制度》及《招标管理制度》规范采购行为，需求部门提出采购申请后，由供应链管理统一负责采购的执行。供应链管理根据公司可能采购的所有货物进行详细的市场调研，明确不同供应商可能供应的材料的质量、价格及供应商的供货能力，制定采购策略并为公司提供决策依据。负责建立供应商管理档案，定期对供应商的货物品质、交货期限、价格、服务、信誉等进行分析，为公司采购优选供应商。最终公司主要通过招标、询比价、议价谈判等市场化方式进行采购。针对部分项目采购，如果客户有明确要求，则会根据客户的要求进行指定采购。

3、研发模式

（1）网络安全业务

网络安全业务的研发遵循统一的流程架构，同时对于网络安全产品和网络安全解决方案的不同特点和要求实行差异化的管理方式。

统一流程架构：网络安全业务研发流程主要分为需求阶段、设计阶段、开发阶段、测试阶段及交付阶段。

需求阶段：公司的市场营销团队和售前团队主动调研客户的痛点和需求，作为设计产品和解决方案的基础；同时基于公司管理层与研发团队对于未来网络安全行业前沿技术发展的调研、理解与预测，提出针对性的研发需求。

设计阶段：基于前沿的网络安全技术与发展趋势，并结合客户和市场的的需求，由研发团队进

行需求与技术整合，完成规划方案，架构师根据规划方案进行架构设计。

开发阶段：由各研发团队相互配合，根据设计方案进行代码编写；交互设计团队负责产品方案整体交互、原型、视觉、页面效果设计、优化、开发工作，确保产品方案的可用性、易用性及美观性。

测试阶段：测试部门在产品方案开发完成后，对产品进行测试，保障产品方案的安全性和质量。

交付阶段：公司根据产品方案的实施难易程度，进行发货或派遣人员至客户现场实施安装调试工作。

网络安全产品：公司在产品开发过程中，广泛采用持续集成、自动化测试、敏捷开发与瀑布开发相结合的方式，同时在部分产品开发中积极推进 DevOps 实践，以有效地提升研发效率，缩短产品的发布周期。公司遵循产品质量和安全是不能逾越的红线原则，对于产品研发有着一套严格的过程管理和质量控制机制，所有产品在发布前，需经过产品经理、安全测试团队、第三方模块评审委员会、QA 团队和技术支持团队的层层把关，只有符合发布标准的产品才会被推向市场，以保障产品交付版本的质量和安全性。

网络安全解决方案：针对行业客户的网络安全解决方案，公司采用“产品研发+系统开发+专业服务”三位一体的研发体系。其中：产品研发以技术为驱动，负责统一框架、核心功能、标准化方案等的研发工作；系统开发以行业为驱动，负责行业场景方案设计、接口开发、方案交付等工作；专业服务以客户为驱动，负责客户关系、项目管理、项目实施、项目节点测试以及客户需求和反馈的收集。三个团队紧密配合，有力地保障了公司提供网络安全解决方案的过程组织能力、研发能力和质量管理能力。

(2) 数智业务

数智业务建立了完善的研发项目管理系统，能够实现研发项目全生命周期管理。研发项目主要来自于新技术预研、存量技术演进以及市场需求。对于新技术预研类项目，公司通常根据预期技术路径、行业标准的推进与商用进度，提前 1-3 年进行前瞻性研发；对于存量技术演进项目，公司通过定期召开技术委员会、战略规划会，结合 IT、数智、云网三大产品体系，确定下一年度重点研发方向；对于市场需求中的普遍类需求，公司制定新产品、新技术开发计划，在整体研发计划内进行项目规划。

在研发流程方面，公司研发流程包括研发项目立项、项目开发管理、产品发布、产品运营、许可管理、代码管控等多个方面。在研发项目立项阶段，项目组提交立项报告，由公司技术委员

会进行评审考核，考核通过后在公司年度研发预算内，选择急迫性较高、必要性较强的项目准予立项；在项目开发管理阶段，通过项目制的方式对项目工时、项目开发进度以及项目代码进行管理，实现从产品需求到产品发布的端到端管理；在产品发布阶段，项目组向技术委员会提交项目结项报告，经评审后准予项目结项、产品发布；在产品运营阶段，由于公司主要面向企业级用户，产品需要根据用户的使用效果进行持续改进，公司研发团队根据产品在用户处内测的效能情况进行持续改进；在许可管理阶段，公司根据产品的开发情况申请相应的计算机软件著作权或专利，并对产品在交付过程中的具体使用及授权进行管理；在代码管控阶段，公司将软件产品的代码进行封装管控，纳入公司代码仓库进行管理，并对代码的使用及调阅权限进行管理。

4、生产模式

(1) 产品生产模式：公司的产品生产主要包括纯软件模式和软件灌装模式：纯软件模式由公司根据合同约定向客户交付软件；软件灌装模式是由硬件设备供应商将软件产品灌装到外购的硬件设备（工控机、服务器等），再交付给客户。硬件设备作为软件的硬件载体，是为了方便客户部署和应用，使客户无需准备软件运行环境。

(2) 服务模式：公司根据客户的实际需求，为客户提供技术、咨询及安全保障等服务，包括咨询与规划、评估与测试、分析与响应、情报与运营等。公司与客户洽谈、沟通达成合作意向后，成立服务项目小组开展前期调研、制定服务方案及组织服务的实施工作。

5、盈利模式

公司的盈利模式分为三类，具体如下：

(1) 销售产品：主要系公司基于用户采购需求，向其销售产品，以产品销售方式与用户签署购销合同，产品的增值部分即为公司的盈利来源。

(2) 提供解决方案：主要系针对客户需求，公司综合自身各个产品线和服务能力，为客户提供一揽子解决方案。公司盈利来源主要为项目收入与成本费用之间的差额。

(3) 提供服务：根据用户需求，提供系统集成、运维服务或网络安全相关服务，盈利来源为服务收入扣减人员成本及项目费用后的差额。子公司数智运营业务中的 DSaaS 业务还包括按照运营成果分成的盈利模式，即公司通过向客户提供智慧运营服务，在客户取得智慧运营的相关成果后，公司按照约定的比例取得部分收益。

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) 软件与信息技术服务业

根据《上市公司行业分类指引》和《国民经济行业分类》，公司所属的大行业分类为软件和信息技术服务业（以下简称“软件行业”）。2024 年在外部不确定性加剧的背景下，中国宏观政策清晰、经济稳中有进，展现出强大韧性，科技创新引领经济新动能。随着数字经济的蓬勃发展，新质生产力迅速崛起，科技产业正在经历着深刻且全方位的变革，在政策法规、技术创新、市场认知、应用场景向深向实等多个维度实现了跨越式发展。2024 年，我国软件与信息技术服务行业运行稳步向好，保持良好发展韧性与潜力。根据工信部数据，2024 年中国软件和信息技术服务业收入为 137,276 亿元，同比增长 10.0%，利润总额为 16,953 亿元，同比增长 8.7%，企业的盈利能力保持平稳。软件与信息技术服务业被誉为“数字经济的发动机”，不仅具有技术更新迭代迅速、产品附加值高等特点，更是广泛地渗透到各个行业，推动社会智能化和经济高质量发展。

新质生产力驱动的高质量发展趋势下，企业级数智与安全产品及服务迎来崭新发展机遇。数字经济背景下，数字技术与实体经济加速融合，对数智与安全相关产品和服务的需求加速释放。2025 年是十四五规划的收官之年，《2025 年政府工作报告》提出“加快数字中国建设，数字经济核心产业增加值占 GDP 比重要达到 10%左右”，首次明确提出“支持大模型广泛应用”，“持续推进‘人工智能+’行动，将数字技术与制造优势、市场优势更好结合起来”，同时“更好统筹发展和安全，坚持在发展中逐步化解风险，努力实现高质量发展和高水平安全的良性互动”。

近年来，我国已出台了《数字中国建设整体布局规划》《“十四五”数字经济发展规划》《“十四五”国家信息化规划》等一系列国家政策及产业政策推动软件和信息技术服务业的发展，对我国的数字经济发展、数字化技术的创新应用起到了重要的推进作用。随着云计算、大数据、人工智能 AI 等技术的飞速进步，软件与信息技术服务业成为全球竞争的核心领域之一，从传统 IT 服务延伸到智慧城市、工业互联网、金融科技等诸多方向。2024 年 7 月，中共中央二十届三中全会决议提出，支持企业用数智技术、绿色技术改造提升传统产业。随着大数据、人工智能等创新应用向深向实，数智与安全产品与服务将持续推动千行百业数智化转型，赋能实体经济提质增效，加速形成新质生产力。

AI 革新浪潮加速推进，驱动数智与安全在产业升级与应用需求的双向融合。人工智能已成为软件行业智能转型的核心驱动力，应用场景加速拓展，助力千行百业迈向数智化新阶段；软硬融合一体化趋势加快，软件能力加速赋能硬件，生态优势成为核心竞争力之一。随着数实融合稳步加快，软件与信息技术服务业对推进我国工业化、信息化、智能化向实向深，培育新质生产力的支撑作用将日益凸显。根据中国软件行业协会预测，未来 5-10 年我国软件产业规模年复合增长率有望保持在 12%-15%水平，到 2025 年我国软件产业规模有望突破 15 万亿元大关，到 2028 年有望

迈上新台阶，突破 20 万亿元大关。

与此同时，随着机器算法、算力地不断突破，AI 技术进入飞速发展阶段，人工智能将全面影响网络安全各个技术领域的发展，包括网络行为与威胁分析、安全事件管理、入侵检测、安全漏洞治理、端点保护、安全知识问答、数据与文件分类等多个方面。随着 AI 技术加速发展，云基础设施、系统软件中 AI 的采用不断增长，推动网络安全解决方案扩展 AI 能力、加速迭代升级。行业头部厂商均已扩展 AI 解决方案，特别是安全大模型已经在安全运营、情报解读、威胁分析、数据分类分级等方面展现出无与伦比的价值，并且仍在快速更新迭代，部分公司已开始从 AI 服务中获得商业价值，AI 研发投入开始兑现商业产出。同时，大模型应用及部署过程中面临非常多的数据泄露、外部勒索攻击等安全风险，需要网络安全行业加强核心技术创新，保护人工智能 AI 大模型自身的安全，网安厂商纷纷着手构建综合安全解决方案，助力千行百业客户安全高效地推进数智化转型。

行业盈利有望持续改善，并购整合趋势加快。随着下游需求的陆续恢复、人力成本增长速度的下降，行业产能扩张期告一段落，未来 2-3 年行业人效水平将有望提升，中国软件行业的盈利表现有望逐步改善，特别是中国头部软件公司正在不断改善其商业模型，软件上云提供 SaaS 服务，产品服务化的趋势不断深化。同时，行业政策不断释放利好，AI、大数据等新技术的加速融合有望改变行业生态系统，行业头部公司正在加速并购步伐，外延式扩张并购活动将有利于提高行业集中度。

（2）网络安全行业

网络安全行业作为软件与信息技术服务业的细分领域之一，是保障数智技术快速发展的安全基座。全球网络安全事件频发叠加地缘政治等不确定性增加，刺激网络安全领域支出增长。2024 年，微软蓝屏等网络安全事件频发，暴露了部分网络安全现存问题，且生成式 AI 的广泛使用会加剧网络资源安全防护的压力，为网络及信息安全增加了诸多挑战。同时，受全球地缘政治、经济竞合等形势影响，全球各国博弈正逐步扩散至网络领域，安全领域的支出不断增长。根据 IDC 2025 年 V1 版《全球网络安全支出指南》报告数据显示，2023 年全球网络安全 IT 总投资规模为 2,150 亿美元，并有望在 2028 年增至 3,770 亿美元，五年复合增长率（CAGR）为 11.9%。

中国网络安全市场进入稳健增长阶段，其中，网络安全软件和安全服务市场增速更高。近三年来，中国网络安全公司受宏观因素影响，业绩有所承压，未来随着地方化债、专项债等进程的深入，网络安全企业有望迎来基本面改善。同时，新质生产力的构建正在加速数字经济的成长，为网络安全行业带来新的发展动力。多重因素共振下，网络安全产业正逐步摆脱发展滞缓的状态。

根据 IDC 2025 年 V1 版《全球网络安全支出指南》报告数据，中国网络安全市场规模从 2023 年的 121.6 亿美元增长至 2028 年的 171 亿美元，期间年复合增长率为 9.2%。在整体技术市场组成中，安全防御硬件设备逐步云化，网络安全软件和服务市场将保持更快增长，五年复合增长率分别为 11.5% 和 11.9%。随着数字化转型、人工智能与大模型的迭代，新兴技术加速与网络安全融合，为政企用户提供更丰富、全面、有效的安全保障。技术进步和客户需求的演进会带动网络安全软件市场迎来更多创新机遇。

政策法规措施在中国网络安全产业发展过程中扮演着至关重要的角色。近年来，从宏观顶层的战略规划，到微观层面的具体操作指南，国家出台了一系列旨在促进网络安全建设的政策措施。《中华人民共和国网络安全法》明确了网络安全的基本原则和法律框架，为各行业构建坚实的网络安全基础提供了指导；《中华人民共和国数据安全法》则聚焦于数据保护和个人信息隐私，强化了企业在数据处理过程中的责任意识；还有针对特定领域的专门法规，如工业控制系统安全标准、金融信息安全规范等，它们共同构成了一个全面覆盖、层次分明的政策体系。除了立法层面的努力外，国家在审批流程和服务机制不断优化，以更好地服务于市场主体的需求。例如，2023 年 7 月起实行的新测评政策取消了原销售许可证制度，改为只需完成网络安全专用产品安全检测或认证即可上市销售，这一举措大大简化了企业的入市门槛，提高了效率。2024 年 9 月发布的《网络数据安全条例》将自 2025 年 1 月 1 日施行，对个人信息保护、重要数据安全、网络数据跨境安全管理等方面做出了规定。此外，国家还鼓励和支持网络安全企业参与国际标准制定工作，通过积极参与 ISO 等国际标准化组织的工作，提升了我国在全球网络安全治理领域的话语权。

人工智能 AI+网络安全双向融合赋能。人工智能（AI）是未来发展的重要技术，随着机器算法、算力地不断突破，AI 技术进入飞速发展阶段。云、管、端、边等基础设施持续深度融合，在以 5G、物联网、数字化等新兴技术为核心的“新基建”的加持下，万物互联和数据积累持续加速，全面推动 AI 技术广泛应用于千行百业，并且产生具有革命性的深远影响。人工智能将全面影响网络安全各个技术领域的发展，包括网络行为与威胁分析、安全事件管理、入侵检测、安全漏洞治理、端点保护、安全知识问答、数据与文件分类等多个方面。随着 AI 技术加速发展，云基础设施、系统软件中 AI 的采用不断增长，推动网络安全解决方案扩展 AI 能力、加速迭代升级。行业头部厂商均已扩展 AI 解决方案，特别是安全大模型已经在安全运营、情报解读、威胁分析、数据分类分级等方面展现出无与伦比的价值，并且仍在快速更新迭代，部分公司已开始从 AI 服务中获得商业价值，AI 研发投入开始兑现商业产出。同时，大模型应用及部署过程中面临非常多的数据泄露、外部勒索攻击等安全风险，需要网络安全行业加强核心技术创新，保护人工智能 AI 大模型自身的

安全，网安厂商纷纷着手构建综合安全解决方案，助力千行百业客户安全高效地推进数智化转型。

信创市场加速推进，有望保持高景气度。2023 年，我国信创安全市场整体规模约为 72 亿元，约占整体网络安全市场规模的 7%，同比增长 24%，是网络安全市场规模增速的 2.4 倍。信创安全的应用落地正从最初的少数几个行业迅速扩展至更多行业和领域，其拓展速度和规模大幅超出预期。根据安全牛的预测，到 2027 年信创安全有望全面占据网络安全市场的主导地位。信创安全技术产品正在从单一或特定类别向全面覆盖安全领域扩展，并在终端和云这两个主要领域朝着集约化方向发展，其发展方向与网络安全产业一致。信创安全的生态理念已达成高度共识，但同时也面临着生态建设成本较高、甚至成为信创安全产品研发和投入负担的商业挑战。

新一代网络安全技术产品正向服务化、集约化、智能化方向快速演进。随着数智化转型的深入发展，原生安全、零信任等新的网络安全技术理念与体系也在我国安全产业侧不断落地应用。网络安全厂商的新一代网络安全产品正在向“云网”和“端数”两个维度聚合发展，形成服务化、集约化、智能化等多个创新发展方向：一方面将传统网络安全的能力转化到云上，形成云平台的原生安全，实现安全的服务化；另一方面将原有的云下网络安全能力与终端安全打通，实现零信任理念下从身份认证到数据访问控制的动态防御体系。安全产品和工具的集成融合正在成为政企用户的普遍期待，技术提供商自身无法囊括所有网络安全技术，为了给政企用户提供全方位的安全防护体系，一方面需要提升自身产品和平台对外接口的标准化和开放性，另一方面需要通过广泛的生态合作提升整体解决方案的综合能力。

（3）行业基本特点

跨学科、跨领域：数智技术涉及计算机科学、数据科学、网络通信、人工智能等多个学科，需要跨学科的知识融合和技术创新。在云计算、大数据、物联网、人工智能等新兴技术的持续演进下，行业数字化水平快速更新迭代，进一步推进了不同学科、不同技术的发展与创新。

融合化、一体化：数智技术需要集成各类硬件、软件以及网络、数据等实现，并且客户对于数字化方案的一体性、融合性要求较高，需要行业内企业进行定制化的解决方案开发。此外，数字化技术需要遵循开放标准，实现不同系统和平台之间的兼容性，以支持大规模应用，因此数字化技术具备一体化的要求。

安全能力是数智技术快速发展的保障：在目前数字化相关系统日趋全面、网络环境日益复杂、海量数据的重要性日趋凸显的情况下，安全已成为数智时代的基石，只有强化安全保障能力建设，推动网络安全技术突破，提升安全产业供给能力，筑牢可信可控的数字安全屏障，才能确保数字化进程的顺利进行，推动数字化技术快速发展。

行业收入季节性特征：软件与信息技术服务业的下游客户以政府、金融、电信、能源、教育等行业为主，客户多采用集中采购制度和预算管理制度，其采购活动具有较强的季节性。许多客户在每年上半年对本年度的采购及投资活动进行预算立项、设备选型测试等，下半年进行招标、采购和项目建设、验收、结算，因此，每年的第三、四季度往往出现收入增加的现象，导致行业普遍呈现营业收入上下半年不均衡的分布特征。

(4) 行业主要壁垒

技术创新壁垒：公司所在行业是典型的技术密集型行业，行业进入需要较高的技术门槛。核心技术的积累沉淀与技术创新是软件企业打造核心竞争力的关键要素。数智化涉及云计算、大数据、人工智能、物联网等新兴技术，需要深厚的技术积累，新进入者需要投入大量研发资源来掌握这些技术，特别是服务运营商、金融等承载及处理大量数据的行业用户，需要软件服务商在提供产品系统的稳定性、安全性和响应速度方面具备极高的能力。同时，随着技术快速发展、用户应用场景的持续丰富，软件厂商需要不断进行升级和改造，以适应新的技术标准。

行业经验及客户壁垒：不同行业的数智化需求各不相同，业务流程和运营模式存在差异，行业数字化解决方案需要深入理解和适应这些行业特性。以电信运营商用户为例，需要管理和运营的网络基础设施庞大、提供的服务类型众多，并需满足不同客户群体的多样化服务需求，因此需要通过设计复杂的数字化系统来满足业务需要，因此对软件服务商的要求中，行业经验必不可少。与行业经验相匹配，由于数字化系统通常承载用户的核心业务、核心数据，数字化系统的替代成本相对较高，因此行业数字化企业的客户粘性相对较高，构成了行业客户壁垒。

人才壁垒：人才是软件产业发展的核心要素。在目前新兴技术快速发展的背景下，数智化及网络安全细分领域对人才的要求持续提升，对于行业人才的跨学科知识结构、前沿技术领域的熟悉程度等方面的要求较高。此外，行业人才还需要具备持续学习和创新的能力，并不断积累深刻的行业理解和经验。通常行业核心人才需要在长期技术研发及市场竞争中进行培养，行业外其他企业短期内难以掌握核心人才，构成了行业人才壁垒。

资源壁垒：当前创新技术大爆发的时代趋势下，软件企业需要具备强大的资源整合能力。在长期市场角逐中，领先企业锻炼出卓越的资源整合本领，与上下游产业链紧密协同，构建起稳固高效的产业生态。同时，通过投拓并举、跨行业、全方位整合资源，领先的软件企业能够营造出有利于自身加速发展的外部环境。

(2). 公司所处的行业地位分析及其变化情况

(1) 网络安全业务

公司网络安全核心产品与技术以及公司整体市场影响力获得了国内外市场研究机构的广泛认可，在身份和数字信任软件市场、终端安全、云安全、XDR、勒索治理、数据安全、AI+安全运营等众多领域均表现突出，奠定了在中国网络安全软件市场的领先地位。本报告期内，公司新获以下第三方机构的奖项：

• **身份安全：市场份额第一**

2024 年 10 月在 IDC《中国 IT 安全软件市场跟踪报告，2024H1》中，身份和访问管理软件市场份额连续 8 年位居第一。

• **身份安全（统一身份管理）：市场份额位居第一**

2024 年 5 月在 IDC《中国统一身份管理平台市场份额，2023：微服务化、标准化、智能化成为共识》中，统一身份管理产品市场份额位居第一。

• **终端安全：市场份额第二**

2024 年 10 月在 IDC《中国 IT 安全软件市场跟踪报告，2024H1》中，终端安全软件产品市场份额连续多年位居第二。

• **新一代终端安全：代表厂商、能力领航者**

2024 年 12 月，安全牛发布《2024 新一代终端安全技术应用指南暨年度 Top10 厂商推荐》，亚信安全作为中国新一代终端安全赛道的开创者，凭借全面且突出的终端安全技术能力，以及持续的技术和理念创新，再次获得市场认可，入围新一代终端安全领域十大代表性厂商。

2024 年 6 月在数世咨询出版的《数字安全蓝皮书》一书中，亚信安全 TrustOne 的领先技术及创新理念获得认可，被确认为新一代终端安全——能力领航者。

• **云工作负载安全：私有云云工作负载安全市场份额位居第三**

2024 年 6 月在 IDC《中国私有云云工作负载安全市场份额，2023：CNAPP 助力企业实现全方位云原生安全防护》中，云主机安全产品市场份额位居第三。

• **云工作负载保护平台（CWPP）、云安全态势管理（CSPM）：代表厂商**

2024 年 12 月，IDC 发布《生成式 AI 推动下的中国云安全市场现状及技术发展趋势，2024》，报告聚焦于公有云场景下的安全能力，亚信安全凭借产品技术优势，成为 CWPP、CSPM 技术领域被推荐厂商。

• **大模型安全：代表厂商**

2024 年 12 月，在 IDC《大模型安全检测与防护解决方案品牌推荐与洞察 2024》报告中，亚

信安全信立方大模型凭借技术优势，成为本次报告推荐品牌，并在大模型攻防检测，身份识别与管理等 12 个细分领域获得推荐。

- **邮件安全：技术代表厂商**

2024 年 6 月在 IDC《生成式 AI 推动下的中国网络安全硬件市场现状及技术发展趋势，2024》报告中，邮件安全 DDEI 凭借深度融合 AI 技术，荣获中国市场代表厂商。

2024 年 8 月在 数说安全《2024 网络安全十大创新方向》，亚信安全信桅高级威胁邮件防护系统 DDEI 荣获 AIGC+邮件安全典型厂商推荐。

- **数据安全：技术代表厂商**

2024 年 6 月在 IDC《中国数据安全隐私合规市场洞察，2024》中，数据安全隐私合规产品凭借突出的能力优势入围代表厂商。

- **数据安全运营平台（DSOP）、数据安全态势管理：代表厂商**

2025 年 1 月，在 Gartner 发布《China Context: Market Guide for Data Security Platforms》（中国背景：数据安全平台市场指南）中，亚信安全数据安全运营平台（AISDSOP）基于在数据安全领域的核心技术优势，入选中国代表性 DSP 厂商。

2024 年 12 月，安全牛发布《数据安全态势管理应用指南（2024 版）》，亚信安全 DSOP 凭借产品研发和应用推广中的出色表现，入围 2024 年度数据安全态势管理领域十大代表性厂商。

- **零信任（ZTNA）：代表厂商**

2024 年 9 月在 Gartner《Market Guide for Zero-Trust Network Access, China》（中国零信任网络访问市场指南）报告中，AISDP 连续两年荣膺 Gartner 中国零信任市场代表厂商。

- **特权账号管理（PAM）：代表厂商**

2024 年 11 月，在 Gartner 发布《Innovation Insight for Privileged Access Management in China》（中国特权访问管理创新洞察）中亚信安全 PAM 产品凭借领先技术，荣膺代表厂商。

- **托管检测与响应服务（MDR）：代表厂商**

2024 年 7 月在 Gartner 发布的《Market Guide for Managed Detection and Response Services, China》（中国托管检测和响应服务市场指南）报告中，亚信安全 MSS 托管安全运营服务凭借表现卓越，荣膺 MDR 代表厂商。

- **攻击面管理：代表厂商**

2024 年 9 月在《IDC Technology Assessment: 中国攻击面管理厂商技术评估，2024》报告中，亚信安全攻击面管理平台以外部攻击面管理（EASM）能力、威胁情报能力、入侵与攻击模拟

(BAS) 能力满分入围报告，荣获技术代表厂商。

2024 年 12 月，安全牛发布《新一代攻击面管理应用指南（2024 版）》报告，亚信安全攻击面管理解决方案的产品技术与应用案例获得双重肯定，荣获 2024 年该领域十大代表性厂商。

- **AI +安全运营**

2024 年 10 月在 IDC《革新安全防护-基于大模型的安全能力品牌推荐与洞察——安全运营，2024》报告中，亚信安全信立方大模型在 AI 与安全技术的融合与应用方面获得认可，成为此次报告推荐品牌，其中告警关联、编写检测规则、引导调查三大能力获得推荐。

- **Web 应用程序与 API 保护 (WAAP)：技术代表厂商**

2024 年 05 月在 IDC《中国 WAAP 厂商技术能力评估 2024》中，亚信安全 WAPP 凭借 WAF、BOT、威胁情报、行业应用等技术优势，斩获中国 WAPP 市场技术代表厂商，再次证明公司 WAPP 的技术领先优势。

- **可扩展检测与响应平台 (XDR)：位居领导者象限**

2024 年 6 月在《IDC MarketScape：中国扩展检测与响应平台 2024 年厂商评估》中，XDR 凭借综合实力位居“领导者”象限。

- **勒索治理：代表厂商**

2024 年 9 月在安全牛《2024 勒索软件攻击防护应用指南》报告中，亚信安全勒索治理体系凭借在勒索治理领域的核心技术以及丰富的实战经验，获得核心能力维度总分第一，入选 2024 年度“勒索攻击防护技术领域十大代表厂商”。

- **新一代网络安全服务：代表厂商**

2024 年 10 月在安全牛《新一代网络安全服务应用指南（2024 版）》，亚信安全凭借安全服务在品牌信誉、市场认可度、服务支撑能力、服务管理能力和服务技术能力的综合评分，荣获中国新一代网络安全服务十大代表性厂商。

- **中国网络安全十强企业**

2024 年 11 月安全牛发布《网络安全企业 100 强》（第十二版）亚信安全连续 9 年蝉联中国网络安全十强企业，并在信创排名第 2。

(2) 数智业务

子公司亚信科技是国内领先的软件产品、解决方案和服务提供商，通过综合运用咨询规划、产品研发、实施交付、系统集成、数据运营、智能决策、客户服务等数智化全栈能力，为千行百业提供端到端、全链路数智化服务，客户遍及电信运营商、广电、能源、政务、交通、金融、邮

政等行业。亚信科技是全球通信业权威标准化组织成员，在 3GPP 拥有独立投票权，与全球知名运营商、设备厂商共同参与电信行业的标准规范讨论及制定过程，并逐步在部分标准及工作组中起到主导作用。近年来，亚信科技牵头成立 IEEE P3398、IEEE P3127、TMF 5G 专网、TMF 数据协作等工作组并担任工作组主席，此外，还牵头立项 IMT-2030 6G 核心网数字孪生需求与技术要求项目，并担任负责人。2024 年持续深度参与 3GPP、ITU、ETSI、IEEE、TMF、O-RAN 等 9 个国际/国家技术标准组织工作，国际标准从跟随到主导占比显著提升，累计参与制定国际/国内标准共计 330 项，其中 2024 年新增 60 项，新增担任 TMF AI4DEMworkstream 主席、3GPP SA5 RedCap 管理特性标准报告人等标准组织 12 项重要职务。在产品及技术领域，公司一系列产品取得权威奖项及权威市场机构认证，具体如下：

在云网领域，亚信科技入选 OMDIA 核电领域 5G 专网最佳实践报告；基于 5G 专网的“风电行业 700MHz 5G 专网解决方案”在 Network X 欧洲通信展上获得“全球最佳行业方案奖”及工信部“绽放杯”全国总决赛一等奖；5G 网络智能化产品体系连续三年入选 Gartner “全球网络智能化主流供应商矩阵”，并新入选 Gartner “网络基础设施主流供应商矩阵”与“网络 IT 智能化主流供应商矩阵”；在 6 月举办的国际电信管理论坛 2024 DTW Ignite 数字转型世界系列峰会上，与运营商及合作伙伴联合打造的“GenAI 赋能算力网络”项目脱颖而出，荣获开放创新类的“杰出创新与未来影响奖”。

在数智领域，凭借在通信人工智能领域卓越的技术表现、强大的产品体系与服务能力，亚信科技荣获 Gartner 首次正式发布的通信人工智能领域全球“魔力象限”《Magic Quadrant for AI in CSP Customer and Business Operations》中的“领导者”（Leaders）地位，并在全部三项细分场景中均排名榜首；“渊思·行业大模型”入选 Forrester“中国行业大模型 MaaS 平台主流供应商”与“中国行业大模型人工智能平台主流供应商”；通用人工智能与认知增强平台 TAC MaaS、商业智能增强分析工具、知识对话机器人、机器人流程自动化平台等多款数智产品先后入选 Gartner “2024 年全球运营商客户与业务运营关键能力主流供应商矩阵”、“2024 年企业通信服务数据、分析和人工智能主流供应商矩阵”、“2024 年通信行业客户体验与货币化主流供应商矩阵”和“2024 年通信行业运营和自动化主流供应商矩阵”等报告；AI0ps 产品凭借规模化商用成果，获“北京市科技进步二等奖”；数据产品荣获国家数据局举办的“数据要素 X”大赛北京赛区一等奖及全国决赛三等奖。亚信科技构建并发布 AI Native 重构软件产品理论体系，并联合清华大学智能产业研究院、Intel 等产学研用合作伙伴共同发布《AI Native 技术重构软件产品白皮书》；承担多项国家重大科研项目，包括工信部 AI 平台“揭榜挂帅”国家级任务，科技部“面向通用视觉的跨模态暗

知识应用”等重大项目。

在 IT 领域，亚信科技凭借在数字孪生领域成熟的产品、解决方案及客户成功案例，入选 Gartner《新兴技术：仿真孪生技术的采用趋势显示出新的长期营收机会》报告、并再次入选 IDC 报告：《中国数字孪生解决方案市场份额，2023》、《中国智慧园区解决方案市场份额，2023》；在信创生态上，积极参与并通过国家安全可控评测专项。通过独立软件开发商（ISV）、系统集成商（SI）等生态伙伴，为数据库产品（AntDB）建立覆盖全行业、有区域纵深的信创生态合作体系，产品生态合作伙伴包括百余家主流的硬件及中间件厂商。

此外，亚信科技及多款产品数十次入选 Gartner、IDC、Forrester、OMDIA 等主流市场机构相关榜单及认证，具备突出的行业地位。

(3). 报告期内新技术、新产业、新业态、新模式的发展情况和未来发展趋势

中国数字经济蓬勃发展、数据要素成为核心的大趋势背景下，云计算和网络成为新一代数字经济底层基础设施。伴随着用户新场景、新业务、新标准的涌现，需要行业内企业通过持续的新技术运用和新产品的研发以满足用户需求。同时，数智化系统承载并处理大量的用户、业务等高价值数据，其稳定性、安全性和响应速度要求较高，对行业内企业的技术能力要求较高。因此，“云网安”融合将成为大势所趋，安全+数智一体化的综合服务能力将成为软件企业的核心竞争力。

(1) AI Agent 重塑软件行业价值，推动商业模式变革。 AI Agent 在大模型的推动下，引发生产力范式的双重革命。AI Agent 以其强大的计算能力和学习能力逐步重塑软件行业的价值体系：首先，通过自动化、智能化的解决方案显著提高软件开发和维护效率。而且 AI Agent 能够通过学习和自我优化，自动生成代码、检测漏洞，从而大幅度缩短开发周期，降低人力成本。其次，AI Agent 改变了软件行业的价值链。随着 AI Agent 应用的普及，越来越多的公司开始采用基于订阅和服务的商业模式获取收入，不仅增加了收入稳定性，还可以为客户提供更为个性化和持续的服务，从而提升客户满意度和忠诚度。最后，AI Agent 将推动软件行业的创新与多元化发展，AI 技术的进步使得软件产品能够更好地理解和预测用户需求，进而开发出更加智能化和人性化的应用程序。这种能力不仅扩大了软件的应用场景，也激发了更多新兴市场的出现，促使企业不断探索新的商业机会。

(2) 云计算与智算加速融合，提振云安全能力需求。 云计算与智能计算的加速融合已成为不可逆转的趋势，这种融合不仅在技术层面上带来了深刻的变革，也在商业应用中展现出巨大的潜力。云计算作为一种资源共享和服务交付的模式，极大地提高了企业的运营效率和灵活性；而智能计算则通过机器学习、人工智能等技术，赋予计算过程更强的分析和决策能力。当这两者结

合在一起时，能够实现更为智能化的资源调度和数据处理，从而推动整个行业向更高效、更智能的方向发展。然而，随着云计算与智能计算的加速融合，对云安全能力的需求也随之显著增加。云安全不仅涉及到传统的网络安全问题，还需要应对数据隐私、身份认证、访问控制等多方面的挑战。在智能计算的背景下，数据的敏感性和复杂性进一步提高，要求云安全技术能够提供更为全面和精细的保护措施。企业和用户在享受云计算与智能计算带来的便利时，也必须确保其数据和应用的安全性不受威胁。因此，提升云安全能力不仅是技术发展的必要步骤，也是保障用户信任的重要环节。通过不断创新和优化安全技术，企业可以更好地保护其数据资产。云计算与智能计算的融合为安全技术的创新提供了契机，未来的云安全解决方案将更加智能化、自动化，能够主动检测和响应潜在的安全威胁，为用户提供更加可靠和安全的云服务体验。

(3) 终端生态日趋一体化、智能化和多元化，新一代终端安全技术呼应而出。数据隐私安全将伴随 AI 应用发展而更加重要，未来终端安全问题覆盖范围越来越广泛且复杂。终端的数据隐私安全问题在 AI 应用愈发广泛的过程中显得更加重要，并且影响和覆盖范围逐渐广泛。终端面临钓鱼攻击、无文件恶意软件、勒索软件、零日攻击、加密劫持等众多严峻的安全挑战，叠加组织的多个终端安全软件种类多、管理难度加大、黑产积极利用 AI 技术提高供给效率，这对终端安全防护技术提出更高要求。因此，新一代终端安全的轻量化、一体化、智能化发展，通过融合诸多终端安全能力、统一管控终端暴露面、智能化检测、持续优化检测响应框架等能力，将较大程度上解决上述安全挑战，从而帮助客户降本增效。

(4) 数据赋能经济提质增效作用显现，驱动数据要素价值释放与安全保障需求增加。2024 年 1 月 4 日，国家数据局等 17 部门近日联合印发《“数据要素×”三年行动计划（2024—2026 年）》，明确在 12 个重点行业（如金融、医疗、交通）推动数据要素应用场景落地，打造 300 个以上示范案例，强化数据流通与安全协同，推动数据要素价值创造的新业态成为经济增长新动力，数据赋能经济提质增效作用更加凸显，成为高质量发展的重要驱动力量。规划明确要求数据来源合规和治理有效，推动隐私计算、区块链等技术在数据安全流通中的应用。数据资产作为战略性资源，将成为企业核心竞争力之一，数据已经成为推动企业发展的核心资源。

数据的生产、获取、存储、分析和应用贯穿于企业的各个环节，随着经济数字化、网络化、智能化的进程加速，企业对数据的需求大幅提升，数据已经从传统的生产要素转变为企业核心的战略资源，对企业的组织运营、决策优化以及市场定位等方面产生深远影响。近年来，我国出台了一系列国家政策及产业政策推动软件和信息技术服务业的发展，对我国的数字经济发展、数字化技术的创新应用起到了重要的推进作用。同时，我国在通信网络、数据中心等基础设施建设方

面取得了显著成效，为软件行业的发展及行业数字化提供了良好的基础设施条件。与此同时，数据要素市场发展也驱动数据安全技术攻关和应用进程加快。根据 IDC 的数据显示，在网络安全软件市场中，信息与数据安全软件（Information and Data Security Software）以 16.7% 的五年复合增长率成为软件最大子市场。

（5）“东数西算”工程牵引建成全国算力网络服务体系，智能算力渗透率加速提升。数字产业化与产业数字化转型迭代升级进程加快，5G、大数据、人工智能等新兴技术的普及应用，导致全社会数据总量急剧增长，数据资源存储、计算和应用需求大幅提升，对算力基础设施提出了更高要求，特别是算网深度融合对实现算力灵活调度、数据高速传输的应用意义重大。在国家政策大力支持、东数西算工程牵引下，我国已形成算力资源储备充足、算力调度初具规模、算力交易雏形初显的算网服务体系。算力网络以算为中心、网为根基，网、云、数、智、安、边、端、链等深度融合，未来以实现算力泛在、算网共生、智能编排、一体服务为目标，像水电一样，算力网络将成为“一点接入、即取即用”的社会级服务，是数智时代全社会的新型基础设施，提升面向生活、行业、社会新兴业务的已有场景体验，同时构筑未来新型场景，赋能千行百业。根据六部门联合发布的《算力基础设施高质量发展行动计划》，到 2025 年算力规模超过 300EFlops，智能算力占比达到 35%，地方省份上海、广东等多省提出 2025 年智能算力占比达到 50% 以上，智能算力已成为算力发展的主赛道。同时，算网融合架构下，由于异构节点数量众多、网络互联程度加深、资源调度智能自动化，打破了安全边界，暴露面放大，数据安全、网络安全、新技术安全相互影响渗透，可能会造成单点风险影响全局的安全挑战。因此，建设算力网络，需要多维度构建算力网络安全保障体系，实现算网建设与安全保障同步化、一体化、全局化推进。

（6）第三张网卫星互联网加速到来，6G 空天地一体化发展前景广阔。我国卫星航天产业进入发展快车道，中国星网“GW 星座”、上海垣信“千帆星座”进入组网加速期，卫星互联网作为第三张网迎来规模化发展机遇期，星地一体融合网络值得期待。这一技术的崛起不仅改变了传统的通信方式，也为全球通信网络带来了革命性的变革，为人类的沟通、信息共享以及数据传输提供了更为广阔的空间。我国已建成全球规模最大的 5G 网络，拥有多项 5G 核心技术，领跑 5G 行业应用场景，产业生态蓬勃发展，在地面移动通信方面实现了标准与产业引领，中国可利用地面移动通信强大的技术队伍与完备的产业生态优势赋能卫星互联网产业，助力空天地一体信息基础设施顺利部署，实现空天地一体的深度融合，也为我国 6G 空天地一体全球领先奠定基础。未来，随着空天地一体的深入发展，卫星互联网将逐步向各行业渗透，其能力将逐步扩展并催化衍生出大量创新场景。同时，新的安全挑战也不容忽视。首先，随着低轨卫星星座的大规模部署，网络攻

击的潜在入口显著增加，如何确保卫星通信链路的加密性和抗干扰能力成为关键。未来，量子加密技术和区块链技术可能在卫星互联网安全中得到广泛应用，以增强数据传输的保密性和完整性。其次，卫星互联网的全球覆盖特性使其成为关键基础设施，信关站、地面基础设施等面临的网络安全威胁不容忽视，可能对国家安全和经济活动产生深远影响。因此，各国正在加强卫星互联网的安全监管与国际合作，制定统一的安全标准和应急响应机制。此外，人工智能和机器学习技术的引入，将在威胁检测、入侵防御和网络恢复中发挥重要作用，提高卫星互联网的安全防护能力。

3、公司主要会计数据和财务指标

3.1 近 3 年的主要会计数据和财务指标

单位：元 币种：人民币

	2024年	2023年	本年比上年 增减(%)	2022年
总资产	13,369,849,942.79	3,400,977,486.04	293.12	3,682,656,570.16
归属于上市公司股东的净资产	2,154,169,475.31	2,117,938,483.39	1.71	2,647,146,253.85
营业收入	3,595,082,344.03	1,608,088,384.17	123.56	1,720,951,997.61
归属于上市公司股东的净利润	9,590,639.77	-291,075,848.53	不适用	98,483,055.93
归属于上市公司股东的扣除非经常性损益的净利润	-16,256,643.63	-324,941,753.06	不适用	15,774,329.48
经营活动产生的现金流量净额	1,145,412,642.37	-379,335,701.16	不适用	-260,712,946.69
加权平均净资产收益率(%)	0.45	-12.03	增加12.48个百分点	3.88
基本每股收益(元/股)	0.0248	-0.7302	不适用	0.2483
稀释每股收益(元/股)	-	-	-	-
研发投入占营业收入的比例(%)	15.32	27.78	减少12.46个百分点	18.74

3.2 报告期分季度的主要会计数据

单位：元 币种：人民币

	第一季度 (1-3 月份)	第二季度 (4-6 月份)	第三季度 (7-9 月份)	第四季度 (10-12 月份)
营业收入	288,288,068.83	372,418,608.16	447,674,651.15	2,486,701,015.89
归属于上市公司股东的净利润	-145,908,760.07	-46,201,008.86	-16,231,477.60	217,931,886.30

归属于上市公司股东的扣除非经常性损益后的净利润	-150,661,374.43	-46,755,612.15	-16,880,333.07	198,040,676.02
经营活动产生的现金流量净额	-204,413,659.57	-95,802,450.55	-88,040,972.74	1,533,669,725.23

季度数据与已披露定期报告数据差异说明

适用 不适用

4、股东情况

4.1 普通股股东总数、表决权恢复的优先股股东总数和持有特别表决权股份的股东总数及前 10 名股东情况

单位：股

截至报告期末普通股股东总数(户)								6,970
年度报告披露日前上一月末的普通股股东总数(户)								8,675
截至报告期末表决权恢复的优先股股东总数(户)								/
年度报告披露日前上一月末表决权恢复的优先股股东总数(户)								/
截至报告期末持有特别表决权股份的股东总数(户)								/
年度报告披露日前上一月末持有特别表决权股份的股东总数(户)								/
前十名股东持股情况(不含通过转融通出借股份)								
股东名称 (全称)	报告期内 增减	期末持股数 量	比例 (%)	持有有限售 条件股份数 量	质押、标记或冻 结情况		股东 性质	
					股份 状态	数量		
亚信信远(南京) 企业管理有限公司	0	80,948,488	20.24	80,948,488	无	0	境内非 国有法 人	
南京亚信融信企 业管理中心(有限 合伙)	0	62,013,649	15.50	62,013,649	无	0	其他	
天津亚信信合经 济信息咨询有限 公司	0	30,656,621	7.66	30,656,621	无	0	境内非 国有法 人	
先进制造产业投 资基金(有限合 伙)	0	19,328,859	4.83	0	无	0	其他	
南京安融企业管 理合伙企业(有限 合伙)	0	11,259,494	2.81	0	无	0	其他	

北京亚信融创咨询中心（有限合伙）	0	11,073,117	2.77	11,073,117	无	0	其他
广州亚信信安投资中心（有限合伙）	-100,000	10,201,138	2.55	0	无	0	其他
广州亚信铭安投资中心（有限合伙）	0	10,159,154	2.54	0	无	0	其他
中国互联网投资基金（有限合伙）	0	10,147,655	2.54	0	无	0	其他
南京安宸企业管理合伙企业（有限合伙）	0	9,380,250	2.35	0	无	0	其他
上述股东关联关系或一致行动的说明	1、控股股东亚信信远及其一致行动人亚信融信、亚信信合、亚信融创均为受实际控制人田溯宁先生控制的同一控制企业。 2、南京安融、南京安宸、亚信铭安的普通合伙人均为公司董事长何政先生控制的主体，为一致行动人。 3、除以上说明的关联关系之外，公司未知上述前十名无限售条件股东之间是否存在关联关系或一致行动关系。						
表决权恢复的优先股股东及持股数量的说明	/						

存托凭证持有人情况

适用 不适用

截至报告期末表决权数量前十名股东情况表

适用 不适用

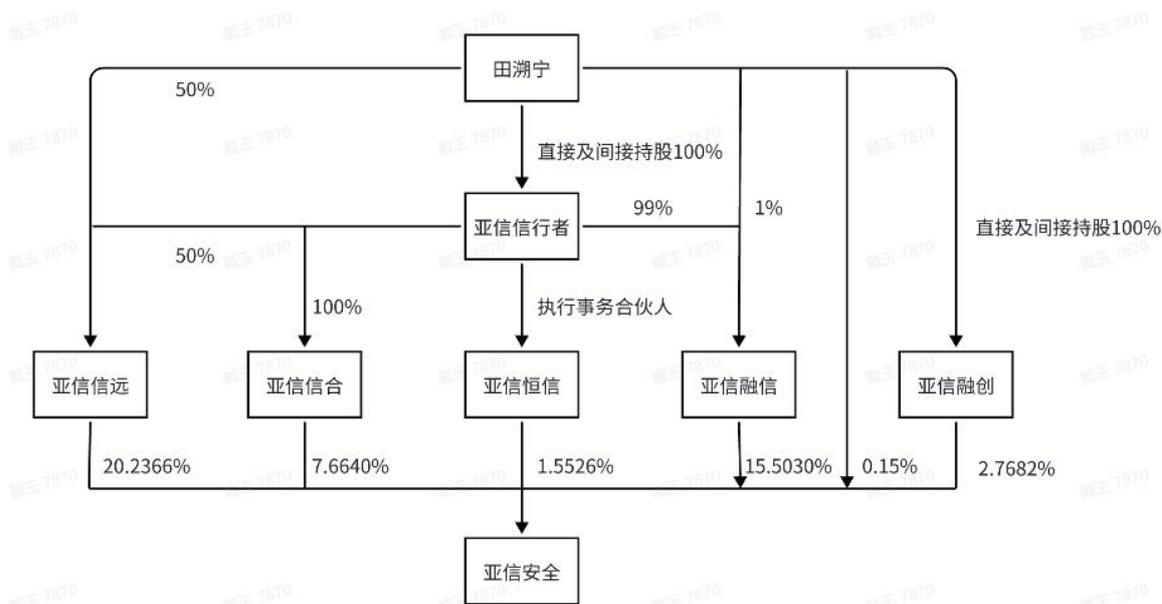
4.2 公司与控股股东之间的产权及控制关系的方框图

适用 不适用



4.3 公司与实际控制人之间的产权及控制关系的方框图

适用 不适用



截至 2025 年 4 月 28 日，田溯宁先生直接控制亚信安全 0.15% 股份，通过亚信信远及其一致行动人亚信融信、亚信信合、亚信融创、亚信恒信间接控制亚信安全 47.72% 股份，直接和间接合计控制亚信安全 47.87% 股份。田溯宁先生还作为南京安融、南京安宸、亚信信安、亚信铭安、亚信安宇、亚信乐信、亚信君信、亚信信宁、亚信信智、亚信信宇、亚信信达、亚信合信、亚信信雅、亚信新信、亚信践信等持股平台的有限合伙人持有合伙份额，合计间接持有亚信安全 4.8059% 的股份。

4.4 报告期末公司优先股股东总数及前 10 名股东情况

适用 不适用

5、公司债券情况

适用 不适用

第三节 重要事项

1、公司应当根据重要性原则，披露报告期内公司经营情况的重大变化，以及报告期内发生的对公司经营情况有重大影响和预计未来会有重大影响的事项。

报告期内，公司于2024年11月完成对亚信科技的非同一控制下的控股合并，导致公司各项财务数据同比变化较大。报告期内，公司实现营业收入35.95亿元，较上年同期上升123.56%。整体毛利率有所提高，从47.82%上升至51.61%。销售费用较上年同期上升25.87%，研发费用较上年同期增加21.03%。报告期内归属于母公司所有者的净利润959.06万元，实现扭亏为盈；归属于母公

司所有者的扣除非经常性损益的净利润-1,625.66万元，较上年同期亏损大幅减少。

2、公司年度报告披露后存在退市风险警示或终止上市情形的，应当披露导致退市风险警示或终止上市情形的原因。

适用 不适用