

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

2025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 在报告中详细描述可能存在的相关风险，敬请查阅公司《2025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、 本公司董事会及董事、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2025年度合并报表中归属于上市公司股东的净利润为-445,781,096.42元（人民币，下同），截至2025年12月31日，公司合并报表期末未分配利润为-9,615,963.36元，公司母公司报表中期末可供分配利润为-99,826,140.68元。

根据《上海证券交易所科创板上市公司自律监管指引第1号——规范运作》《亚信安全科技股份有限公司章程》等有关规定，鉴于公司2025年度归属于母公司所有者的净利润为负、且公司母公司报表中期末可供分配利润为负，综合考虑外部行业环境、公司未来发展等因素，为保持公司稳健发展，更好地维护全体股东的长远利益，2025年拟不进行现金分红，也不进行资本公积金转增股本。

上述利润分配方案已经第二届董事会第二十八次会议审议通过，尚需提交公司2025年年度股东大会审议。

母公司存在未弥补亏损

适用 不适用

截至2025年12月31日，公司母公司报表中期末可供分配利润为-99,826,140.68元。

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

（一）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。面对智能体互联网的浪潮，亚信安全正式升级使命与愿景：以“联结智能世界，护航数智互联”为使命，以“让数智生态茁壮”为愿景，进一步强化“安全+数智”的战略联动，持续为产业发展注入智能与安全的双重动力。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。
	终端安全产品体系	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。	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 月公司完成了对亚信科技控股有限公司（港股代码 01675.HK）的控股，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。

亚信科技已确立“AI 优先”为未来十年核心战略，通过重塑组织边界、业务体系以适配硅基时代生产力，构建起运营商核心系统、智能数据运营、智能连接产品三大业务体系，同时深化与亚信安全的战略联动，将安全能力原生植入，筑牢智能体时代数字安全基石，以“数据、智能、连接、安全”全栈能力快速驶向智能体互联网新大陆。

业务类别	业务介绍	交付形式	典型应用场景
运营商核心系统	为运营商客户提供业务、网络及管理（BOMD）等领域的核心 IT 系统，并在通信、算力等方向与客户共同开展应用创新等相关业务。公司作为运营商数据资产治理及业务价值交付的最佳合作伙伴，助力运	软件、服务、软硬一体	聚焦三大电信运营商，以及广电、铁塔、星网、HKT 等新型运营商客户，涵盖通信服务、算力服务等应用领域的业务支撑以及 AI 创新应用，包括：计费、结算、账务、客服、营业、网络规划、建设、维护、优化，以及算力调度、多云管理、算力确权、智能体互联网，智能体 Token 计费、交易与结算、身份认证与应用运营等场景。

<p>业务</p>	<p>营商在智能体互联网时代实现从规模竞争向价值深耕的战略转型。具体包括传统 IT 支撑业务、创新业务（通信、算力等方向的创新应用）、内生安全业务（结合亚信安全的技术和产品，实现业务内生安全）。</p>		
<p>智能数据运营业务</p>	<p>通过与阿里、火山及运营商等生态伙伴深度合作，为通信、能源、制造、零售等行业客户提供“数据治理服务→大模型/智能体建设→智能体运营”全流程服务。智能数据运营业务包括数据服务、智能交付、智能运营三类服务，持续累积数智资产，形成数智资产复利的商业模式。</p>	<p>软件、服务、软硬一体</p>	<p>1.智能运营业务场景：聚焦通信、互联网金融、汽车、消费等领域的运营全流程及 AI 赋能场景，包括：存量运营、价值运营、私域运营、权益运营、精准营销、效果营销、投流业务、RaaS 效果付费、商圈选址、智能风控、数据洞察、智慧运营工具、社交媒体运营产品工具、垂直行业智能体应用等。 2.智能交付业务场景：能源、制造、零售等领域的大模型应用开发与生态集成交付场景，包括：智能问答、智能风控、智能客服、设备故障诊断、智能运维、财务运行、知识库管理、工业机器人 Physical AI、行业/企业大模型交付、智能制造大模型解决方案及应用交付等。 3.数据服务业务场景：聚焦 ITO 服务、数据工程及知识资产沉淀，包括：软件开发、ICT 测试、IT 运维，数据标注工程、预训练数据工程、语义结构与本体工程、数据合成与仿真工程、知识资产沉淀、知识即时赋能等。</p>
<p>智能连接产品业务</p>	<p>构建下一代通信与连接底座，为能源行业与卫星互联网客户，以“标准产品+服务”的模式，提供 5G/5G-A/6G 专网软硬一体化产品与行业解决方案服务。</p>	<p>软件、服务、软硬一体</p>	<p>1.能源智连产品：能源专网核心网、能源专网基站控制器 AI RAN、能源专网基站 2.空天智连产品：星载 NTN 基站、卫星地面核心网、星载核心网、信关站/物联网载荷/相控阵天线/卫星终端</p>

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，公司一般采用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适配工作。

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

根据国家统计局《战略性新兴产业分类（2018）》，公司属于“1、新一代信息技术产业”；根据《上市公司行业分类指引》和《国民经济行业分类》，公司属于软件和信息技术服务业（以下简

称“软件行业”)。

2025 年我国经济运行总体平稳、稳中有进，展现强大韧性。根据工信部的数据显示，2025 年我国软件和信息技术服务业运行态势良好，软件业务收入稳健增长，利润总额增势放缓。2025 年我国软件行业收入 154831 亿元，同比增长 13.2%；其中，软件产品收入 32361 亿元，同比增长 10.4%；信息安全产品和服务收入 2235 亿元，同比增长 6.7%。2025 年我国软件业利润总额 18848 亿元，同比增长 7.3%。2025 年至 2026 年软件行业的头部企业将继续呈现“多极化”但“集中度稳步提升”的市场格局。从竞争策略与市场行为看，头部企业正围绕核心技术、生态布局与区域扩张展开多维博弈，预计未来中国软件行业将展现出强劲的发展韧性和结构优化特征。

从政策环境来看，我国政府高度重视软件和信息技术服务业的高端化、智能化和绿色化发展，通过鼓励核心技术研发投入、推动产业链协同发展、加强国际合作等措施，持续优化行业生态，为行业长期增长奠定了制度基础。从技术演进来看，人工智能、大数据、云计算等关键技术正加速渗透我国软件与信息技术服务业，推动行业进入深度融合与迭代升级的新阶段。在行业应用层面，软件与信息技术正深度嵌入金融、制造、医疗、教育与政务等重点行业，推动其数字化转型从“点状突破”向“系统重构”演进。从转型趋势来看，软件与信息技术服务业的数字化转型正呈现出从“技术驱动”向“场景驱动”、从“局部优化”向“系统重构”的演进路径。一方面，企业级市场整合加速，头部企业通过技术绑定、渠道合作与信任体系构建，推动 AI 应用从“试点落地”向“规模化复制”迈进。另一方面，地方层面正加快人工智能产业生态与应用场景的系统构建，形成“政策引导+资金支持+人才集聚+基础设施+场景融合”的五维联动机制。从趋势延展性看，未来软件与信息技术服务业将更加强调“技术融合”与“生态协同”，推动行业从“单一技术应用”走向“多技术融合创新”，从“企业内部优化”走向“产业链协同升级”。未来软件行业的增长将更依赖技术渗透深度而非广度扩张。市场规模增长的核心驱动力将来自传统软件向标准化、云服务订阅的持续转化、AI 技术驱动的产品价值提升，以及在电信、金融、制造等垂直行业解决方案的深化。

(2) 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，网络安全已成为数字经济发展中不可或缺的关键基础能力，是保障千行百业数智化转型的安全基座。网络安全行业在 2025 年步入了深度调整与结构性重塑的关键阶段，其特征是“需求分化、财务修复、结构重构、技术跃迁”的复合状态，增长逻辑从过去依赖《网络安全法》、《数据安全法》等政策红利的“合规保障驱动”，转向源于企业数智化转型和业务连续性需求的“业务刚需驱动”。这意味着安全投入正从满足监管的“可选项”，演变为保障企业生存与发展的“必须项”。根据 IDC《中国 IT 安全市场预测，2025—2029》报告显示，在政策法规持续强化、企业安全投入意愿提升以及新技术应用加速的共同作用下，中国网络安全市场保持稳健增长，IDC 预计到 2026 年，整体市场规模有望突破 800 亿元人民币，2024 年至 2029 年年复合增长率达到 8.9%。

中国网络安全行业政策更新呈现多维强化与体系化治理特征，2026 年修订版《中华人民共和国网络安全法》标志着我国网络安全监管体系进入以场景化、精准化为核心的新阶段。此次修订首次将关键信息基础设施运营者和大型互联网平台经营者作为责任主体进行精准化定位，使监管对象更清晰、责任划分更明确，从而增强政策执行的可操作性与可追溯性。此外，数据出境规则体系的构建亦是政策更新的重要亮点，通过“安全评估、标准合同、保护认证”三条合规路径的明确与衔接，为数据跨境流动提供了清晰的制度框架与操作指引，推动企业从被动应对转向主动合规。同时，法律责任的威慑化升级显著提升了违法成本，最高可对企业处以年度营业额 5% 的罚款，并辅以停业整顿、吊销许可等非经济性处罚手段，形成对企业与个人双重责任的闭环管理。这些修订不仅提升了违法成本，也强化了企业对网络安全合规的重视程度，为网络安全行业提供了制度性发展红利。

展望未来，AI 与大数据在网络安全中的深度融合将推动行业从“被动响应”向“主动防御”

转变。根据 Gartner 和安全牛等研究机构的预测，2026 年网络安全将迈入“智能化对抗博弈与多层次纵深防御”新阶段，AI 驱动的自动化攻击将成为主要威胁，而防御端则需构建 AI 驱动的智能纵深防御架构，部署异常检测平台、开展专项培训并建立多渠道验证机制。同时，AI 在威胁情报领域的应用也日益成熟，基于大数据的威胁情报系统能够实时分析全球攻击特征，预测潜在攻击路径，并结合历史攻击数据进行模式识别，从而实现主动防御安全。随着算力、算法和数据供给的持续优化，AI 与大数据的融合将推动网络安全从“被动响应”向“主动防御”转变，形成更加智能、高效的安全生态。

（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，数智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，在身份安全、终端安全、云安全、大模型一体机、安全大模型、大模型安全、AI Agent、AI XDR、安全浏览器、勒索治理、数据安全、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。报告期内，公司获得以下第三方机构的奖项：

身份安全：市场份额第一

2025年10月在IDC《中国IT安全软件市场跟踪报告，2025H1》，身份和访问管理软件市场份额连续多年位居第一。

终端安全：市场份额位居第二、技术代表厂商

2025年10月在IDC《中国IT安全软件市场跟踪报告，2025H1》在终端安全产品市场连续多年排名第二。2025年8月在IDC《中国统一终端安全技术评估，2025》中，TrustOne 凭借技术前瞻性以及对市场需求的深刻理解，一举斩获5项评估满分，凭实力入选中国统一终端技术代表厂商，持续领跑终端技术领域。

身份安全（统一身份管理）：市场份额位居第一

2025年6月在IDC《中国统一身份管理平台市场份额，2024：自动化与智能化将主导产品竞争力》，统一身份管理平台产品连续3年市场份额排名第一。

云工作负载安全：私有云市场份额位居第三

2025年6月在IDC《中国AI赋能的私有云云工作负载安全市场份额，2024：自动化、智能化、云原生成为主旋律》中，云主机安全产品市场份额位居第三。

云原生应用保护平台CNAPP：位居领导者象限

2025年06月在《IDC MarketScape：中国CNAPP厂商评估，2025》中，CNAPP产品凭借综合实力荣登“领导者”象限在营收规模、战略能力上均处于Top前列。

安全大模型一体机、安全智能体、AI Agent、大模型安全：代表厂商

2025年06月在IDC《中国安全大模型一体机市场洞察及品牌推荐，2025：大模型席卷全球，AI与安全相辅相成》中，亚信大模型一体机获得“具备丰富安全防护能力的大模型一体机”品牌推荐，亚信安全信立方安全大模型（AICube）入选深度融合垂域大模型能力的安全一体机品牌推荐。

2025年07月在IDC《中国安全智能体市场概览，2025：东风已至，未来可期》中，安全运营智能体、安全检测智能体获得推荐。

2025年4月在IDC发布《中国AI Agent应用市场概览》报告中，亚信安全凭借在大模型安全领域的研究与创新，成为安全领域代表厂商。

2025年7月在IDC发布的《中国大模型安全保护市场概览，2025》，亚信安全入围全部7个细分领域，包括大模型输入控制，大模型输出内容控制，大模型访问控制，保护大模型接口，大模型可用性检测，构建大模型安全，保护大模型数据存储，彰显领先的AI技术能力。

特权账号管理（PAM）：代表厂商

2025年7月，在 Gartner发布《Market Guide for Privileged Access Management in China》（中国特权访问管理市场指南报告）中亚信安全AISIFORT产品凭借领先技术，荣膺代表厂商。

数据安全平台、数据安全态势管理、数据防泄露DLP：代表厂商

2025年7月，在Gartner发布《Hype Cycle for Cybersecurity in China 2025》（2025中国安全技术成熟度）中，亚信安全入选数据安全态势管理Data security posture management（DSPM），以及数据安全平台Data security platforms（DSPs）两大领域代表厂商。

2025年11月在《Gartner China Context Market Guide for Data Loss Prevention》（数据防泄漏市场指南——中国篇）中，信数数据防泄漏系统AISNDLP获得推荐。

WAAP：技术代表厂商

2025年9月在IDC《协同大模型防火墙能力的中国WAAP 厂商技术能力评估，2025》中WAF、

API保护及监视、Bot流量管理、威胁情报、行业应用五大维度获得满分评估，连续两年成为WAAP市场技术代表厂商。

MDR：代表性厂商

2025年9月在《Gartner Market Guide for Managed Detection and Response Services, China 2025》（中国托管检测和响应服务市场指南）中，亚信安全MSS-XDR Remote Security Operations（基于XDR的远程安全托管运营服务）连续两年获得推荐。

ZTNA：代表性厂商

2025年10月在《Gartner Market Guide for Zero-Trust Network Access, China》（中国零信任网络访问市场指南）中，信磐零信任访问控制系统AISDP系统连续三年获得报告推荐。

XDR、CNAPP、企业浏览器、终端安全：代表厂商

2025年10月在IDC《中国网络安全软件技术发展路线图，2025》中，凭借深厚技术沉淀与丰富实践经验成为XDR、云原生应用保护平台（CNAPP）、企业浏览器及终端安全四大领域代表厂商。

安全浏览器：代表厂商

2025年11月在IDC《中国安全工作空间实践方案市场洞察与品牌推荐，2025》中，凭借在数据安全、零信任等领域的突出技术实力，以及多年服务企业用户的丰富经验，信界企业浏览器入选报告并获得推荐。

勒索治理：代表厂商

2025年12月在IDC《中国勒索防护市场洞察，2025》中，亚信安全勒索治理方案凭借深厚的技术沉淀、持续的产品创新及广泛的行业落地案例，深度契合勒索防护技术发展趋势，成为中国勒索防护技术代表厂商。

（2）数智业务

子公司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。2025年公司持续深度参与3GPP、ITU、ETSI、IEEE、TMF、O-RAN等国际/国家技术标准组织工作，国际标准主导占比显著提升，截至2025年12月，累计参与制定国际/国内标准达384项，其中2025年新增54项，涵盖数智化大模型、智能体、5G专网、AI RAN、5G-A/6G等核心技术领域，进一步夯实公司在行业技术领域的影响力及话语权。在知识产权方面，2025年公司软件著作权新增170项，发明专利获得新增86件，专利申请新增98项，知识产权储备持续丰富，为技术创新与产品迭代提供坚实保障，进一步筑牢核心技术壁垒。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：

2025年，亚信科技聚焦“云网”“数智”“IT”三大核心产品体系，推动产品向AI Native、Agent、Ontology等前沿方向演进，加大研发投入、强化成果转化，以技术引领优势为“AI优先”战略落地提供坚实的产品与技术支撑，助力各行业数智化转型提质增效。

在云网领域，国际影响力持续提升，成果丰硕。公司加入AI-RAN Alliance，推进5G专网和OSS的AI Native化发展；入选OMDIA报告，斩获Glotel Awards、GTI Awards等国际大奖，联合成果获WCA、TM Forum卓越大奖。此外，多款产品获中国电子学会、通信学会科技奖，5G网络智能化产品体系连续4年入选Gartner矩阵，4G和5G专网服务入选Gartner全球“4G和5G专网服务魔力象限”Niche Player象限；联合伙伴发布AI-RAN白皮书与AI原生RAN基站，助力网络能力升级。

在数智领域，实现通信AI国际引领、数据及行业AI国内领先。公司构建起“2个大模型平台+5个行业大模型+N个行业智能体工具”的行业大模型产品体系，全年落地案例362个；连续两年入选Gartner全球“通信服务商客户与业务运营AI能力魔力象限”领导者象限；跻身中国大模型应用交付供应商六强；新增数智本体平台等创新产品，牵头启动“本体开源计划”；在电力行业，携手阿里云打造国内首个千亿级多模态行业大模型项目，实现电力设备智能诊断与健康度预测；与天津联通联合打造全国首个“AI大模型+智能体”智能查号系统，为通信行业智能化转型提供标杆样本。

在IT领域，构建智能应用新型基础设施，推动AI原生通用IT技术产品体系向AI Native深度融合演进，提供智算管控、推理加速等核心能力。升级DevOps能力，构建SDLC（软件开发生命周期）智能体；联合亚信安全推出AI网关安全版并入选中国AI智能体百强，数字孪生提出的SimOps（仿

真孪生)概念被Gartner引用,获得国际行业认可;图灵智能开发套件成为全国首批通过中国信通院“可信AI”软件智能化能力三级评估的产品,体现出在AI软件智能化领域的领先水平。

(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

从行业整体发展趋势看,中国软件与信息技术服务业将迎来由数字化转型深化、AI技术应用加速和数据要素市场化进程共同驱动的结构增长。软件行业的价值创造逻辑将从“提供工具”彻底转向“交付业务成果与保障业务韧性”,技术深度与商业深度的结合将成为软件企业长期胜出的关键路径。

网络安全有望成为千行百业的“智能驱动的数字免疫系统”。软件开发将全面实现“AI优先”,安全能力以内置和左移的方式融入开发全流程,网络安全将进化成以AI智能体网络为核心的“主动免疫”模式,实现威胁的预测、自动防御与系统自愈。中国网络安全行业各细分赛道预计将呈现出鲜明的结构分化与技术驱动特征,云安全、终端安全、身份安全、安全服务、AI+安全等细分领域将成为增长的主引擎。云安全领域,从技术演进维度看,多云与混合云架构正推动云安全从“边界防御”向“零信任+动态访问控制”范式转型。终端安全领域,在移动设备与IoT终端数量激增的背景下,终端安全防护需求呈现显著扩张趋势,终端攻击面的扩展呈现多维度、多层级的复杂形态,终端安全防护策略的升级正从被动响应向主动防御转变,技术融合与智能化成为关键趋势。身份安全领域,AI驱动的零信任架构以身份中心化、从静态管控转向动态智能验证、通过AI快速识别行为偏差并允许主管审查,实现内部管理效率的提升。安全服务领域,AI与云原生重塑MSS与SOC运营范式,安全服务正从“人力密集型”向“技术驱动型”转变,企业对高效、智能的安全运营能力需求日益迫切。

AI安全与智能体安全成为新兴创新投入方向:AI模型在训练与推理过程中存在显著的安全漏洞,为对抗性攻击提供了可乘之机,对抗性攻击的类型多样且对AI系统的实际影响日益加剧,AI安全防护技术正逐步成熟,模型鲁棒性增强、对抗训练与模型加密成为主流方向。同时,攻防对抗的升级正推动智能体安全进入更高维度的技术博弈。随着攻击自动化与防御智能化的同步演进,攻防双方的技术较量正从“工具对抗”向“系统对抗”转变。攻击者不断优化AI生成攻击代码的隐蔽性与适应性,而防御者则通过强化AI模型的泛化能力与实时学习能力来应对。在政策与技术的双重推动下,智能体安全正成为网络安全行业未来发展的关键方向,其技术演进路径与攻防对抗格局将深刻影响整个行业的生态结构与竞争态势。

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

	2025年	2024年	本年比上年 增减(%)	2023年
总资产	11,663,440,389.80	13,369,849,942.79	-12.76	3,400,977,486.04
归属于上市公司股东的净资产	1,736,348,038.44	2,154,169,475.31	-19.40	2,117,938,483.39
营业收入	7,740,582,438.17	3,595,082,344.03	115.31	1,608,088,384.17
扣除与主营业务无关的业务收入和不具备商业实质的收入后的营业收入	7,734,914,751.14	3,594,669,876.65	115.18	1,607,032,330.10

入				
利润总额	-424,924,528.99	400,507,737.20	-206.10	-294,208,031.98
归属于上市公司股东的净利润	-445,781,096.42	9,590,639.77	-4,748.09	-291,075,848.53
归属于上市公司股东的扣除非经常性损益的净利润	-337,892,175.52	-16,256,643.63	不适用	-324,941,753.06
经营活动产生的现金流量净额	224,429,461.90	1,145,412,642.37	-80.41	-379,335,701.16
加权平均净资产收益率(%)	-22.92	0.45	减少23.37个百分点	-12.03
基本每股收益(元/股)	-1.1533	0.0248	-4,750.40	-0.7302
稀释每股收益(元/股)			-	
研发投入占营业收入的比例(%)	16.16	15.32	增加0.84个百分点	27.78

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	1,290,212,702.17	1,833,664,491.07	1,766,709,446.02	2,849,995,798.91
归属于上市公司股东的净利润	-227,359,290.08	-128,793,144.60	-43,833,741.97	-45,794,919.77
归属于上市公司股东的扣除非经常性损益后的净利润	-229,474,646.10	-22,918,148.91	-51,133,785.04	-34,365,595.47
经营活动产生的现金流量净额	-685,566,642.10	-239,081,292.07	-252,751,960.34	1,401,829,356.41

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)	10,148
年度报告披露日前上一月末的普通股股东总数(户)	9,207

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	0	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	0	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	0	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
北京亚信融创咨询中心（有限合伙）	0	11,073,117	2.77	0	无	0	其他
广州亚信铭安投资中心（有限合伙）	-686,531	9,472,623	2.37	0	无	0	其他
广州亚信信安投资中心（有限合伙）	-863,612	9,337,526	2.33	0	无	0	其他
中国互联网投资基金（有限合伙）	-1,014,766	9,132,889	2.28	0	无	0	其他
南京安融企业管理合伙企业（有限合伙）	-4,388,560	6,870,934	1.72	0	无	0	其他
天津亚信恒信咨询服务合伙企业（有限合伙）	0	6,210,362	1.55	0	无	0	其他
上述股东关联关系或一致行动的说明			<p>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、亚信恒信均为受实际控制人田溯宁先生控制的同一控制企业。</p> <p>2、亚信铭安、南京安融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</p>				

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。

2025年，公司实现营业总收入77.41亿元，同比增长115.31%，主要因2024年11月完成对亚信科技的并购，2025年首次完整合并其全年财务数据，推动收入规模快速扩张；但受网络安全行业竞争加剧、并购贷款利息支出增加、信用及资产减值增加以及参股公司公允价值变动损失、核心产品集聚等多重因素叠加影响，公司盈利指标出现大幅下滑，归母净利润为-4.46亿元。2025年，公司网络安全业务精准施策、主动作为，通过主业、产品、客户三大维度的聚焦发力，以及生态协同的深度拓展抵御行业调整压力，营收降幅呈现逐季收窄的向稳态势，并持续提升经营韧性。数智业务板块经营趋稳，现金流大幅改善，新业务快速增长。2025年，公司持续深化“安全+数智”云网安一体化战略，核心产品实现更高层次的融合与能力扩展，形成“业务场景驱动、安全能力共生”的新型协同模式。

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