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

2023 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《2023 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2023年度实现归属于上市公司股东的净利润-291,075,848.53元（人民币，下同），母公司实现的净利润为-66,206,854.53元。截至2023年12月31日，母公司累计未分配利润为54,650,192.32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，鉴于公司2023年度归属于上市公司股东的净利润为负，未实现盈利，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，公司拟决定2023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。

同时，公司于2023年2月27日召开第一届董事会第十七次会议，审议通过了《关于以集中竞价方式回购公司股份方案的议案》，同意公司使用自有资金以集中竞价交易方式回购公司部分已发行的人民币普通股（A股）股份。截至2023年12月31日，公司已使用自有资金270,010,630.35元（不

含交易费用）回购公司股份13,490,585股。根据《上海证券交易所上市公司自律监管指引第7号—回购股份》第八条：“上市公司以现金为对价，采用集中竞价方式、要约方式回购股份的，当年已实施的股份回购金额视同现金分红，纳入该年度现金分红的相关比例计算。”上述金额视同现金分红，公司以回购方式实现了对投资者的权益回报。

本次利润分配方案已经公司第二届董事会第八次会议和第二届监事会第六次会议审议通过，尚需提交股东大会审议。

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

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	/

公司存托凭证简况

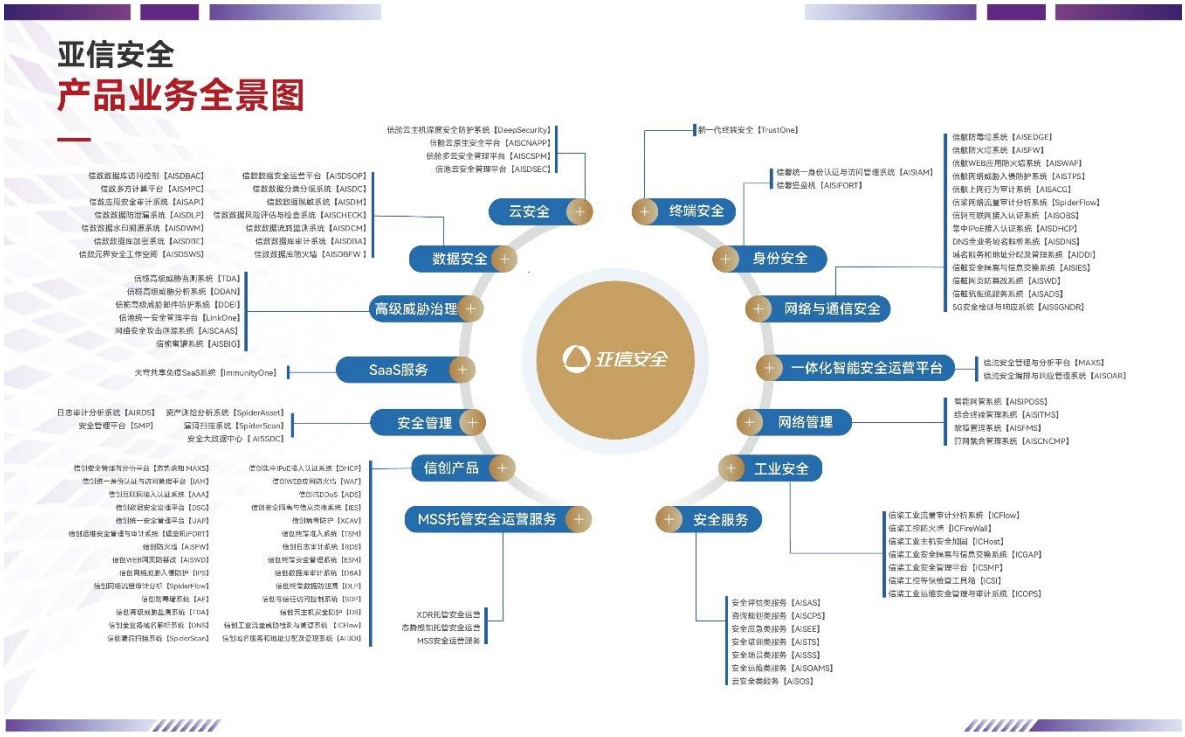
□适用 √不适用

联系人和联系方式

联系人和联系方式	董事会秘书（信息披露境内代表）	证券事务代表
姓名	王震	李宝
办公地址	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
电子信箱	ir@asiainfo-sec.com	ir@asiainfo-sec.com

2 报告期公司主要业务简介

(一) 主要业务、主要产品或服务情况



公司专注于网络空间安全领域，主营业务为向政府、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。公司是中国网络安全软件领域的领跑者，作为“懂网、懂云”的安全公司，致力于护航产业互联网，成为在5G云网时代，守护云、网、边、端的安全智能平台企业。公司提出了“安全定义边界”的发展理念，以身份安全为基础，以云网安全和端点安全为重心，以安全中台为枢纽，以威胁情报为支撑，构建“云化、联动、智能”的产品技术战略，赋能企业在5G时代的数字化安全运营能力。报告期内，公司主营业务包括网络安全产品、网络安全服务、云网虚拟化三大部分。其中网络安全产品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。

1、网络安全产品

（1）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。

产品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。

（2）端点安全产品体系

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。

该产品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。

（3）云网边安全产品体系

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。

该产品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。

2、 网络安全服务

公司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。

网络安全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。

3、云网虚拟化

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。

云网虚拟化产品主要解决客户在云计算虚拟化基础设施建设方面需求。

(二) 主要经营模式

1、销售模式

公司盈利主要来源于网络安全产品的销售，以及为客户提供专业的网络安全解决方案和安全服务。公司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。

2、采购模式

公司采购的主要内容为两大类：（1）服务器、U盘、产品包装物及第三方软硬件等产品；（2）技术服务。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

公司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。

（1）统一流程架构

公司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。

1）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。

2）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。

3）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。

4）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。

5）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。

（2）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。

（3）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。

4、生产模式

（1）安全产品生产模式

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。硬件设备作为安全软件的硬件载体，方便客户部署和应用，使客户无需准备软件运行环境。

（2）安全服务模式

公司根据客户的实际需求，为客户提供的技术、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，成立安全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）提供网络安全服务：根据用户需求，提供网络安全相关服务。公司盈利来源为网络安全服务收入扣减人员成本及项目费用后的差额。

(三) 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）网络安全行业驱动力加速转向业务刚需，中国网络安全市场增速继续领跑全球。

在地缘政治冲突升级、供应链挑战加剧等多重冲击下，作为社会发展的基础性和战略性科技领域，网络安全产业发展面临的国际形势依然复杂严峻，网络安全成为大国角力和科技竞争主攻方向的趋势更加明显。与此同时，随着社会各领域向数字化、移动化、智能化的加速发展，千行百业逐渐加大对信息化建设与数字化转型的投入已成为共识，组织的信息系统及交互环境日趋多变复杂，业务场景发生较大变化，伴随的网络安全风险日趋严峻，安全能力建设从合规型转变为符合业务发展需要、抵御真实安全威胁的刚需型方向。网络安全企业积极应对市场需求，技术快速迭代和创新，从云安全到数据安全到人工智能的应用，前沿技术为网络安全领域注入了新的活力，从长期看网络安全产业仍处于较好的发展周期。

从全球网络安全市场来看，随着数字化、智能化的快速渗透，网络安全需求持续增长。根据IDC《全球网络安全支出指南》最新预测，2022年至2027年，全球网络安全IT总投资五年复合增长

率（CAGR）为11.7%；中国网络安全市场规模五年复合增长率为13.5%，高于全球平均水平。从国内网络安全市场来看，2023年中国网络安全市场面临宏观经济波动与产业生态调整的双重挑战，行业需求增速短期内继续放缓。但中国网络安全市场近年来基于数字化转型、业务内生安全的需求日趋强烈，对定制化解决方案能力、内生安全能力及与数字业务的深度协同等方面提出了更高要求，需求空间正在逐渐释放，未来将引导网络安全产业的长期增长趋势。中国网络安全市场增长的核心逻辑并没有变化，随着下游行业需求日渐复苏，中国网络安全市场仍将保持快速增长。

（2）网络安全法治体系日臻完善，新技术加速迭代升级，持续扩张行业发展机遇。

2023年中国网络安全法律法规、政策发布呈现高密度特征，引起行业高度关注的政策达50余项。数据安全领域、个人信息保护和数据跨境安全成为关注的热点，分别有7项、6项、6项政策围绕这些议题展开。数字中国和行业安全类别的政策都突出了数据安全的重要性，反映了当前推动数据资源转化为经济新优势的大背景下，数据安全正在从传统网络安全中逐渐独立出来的趋势。同时，传统网络安全领域的重要性愈加凸显，以网络安全为核心的政策数量达到12项，而涉及行业安全的政策更是高达13项，位居首位。这表明将网络安全与业务融合、并通过安全促进发展的理念已经获得了更广泛的认可。此外，密码安全和人工智能成为2023年网络安全政策的两个重点领域。数字中国领域也推出了多项重要政策，均涵盖了网络数据安全保障体系建设的内容，强调建立可信赖的数字安全防线。近年来，随着关键信息基础设施安全保护、网络安全审查、数据安全管理、个人信息保护等领域的一系列法律法规相继出台，不仅表明国家对网络安全行业监管呈现趋严、趋细的态势，也为相关企业提供了明确的指导和规范，行业健康发展得以有据可依、有法可循，有力地保障了网络安全行业的持续繁荣和健康发展。

全球各国加大对新兴技术的投研力度，零信任、生成式人工智能、隐私计算等网络安全新技术的布局与场景应用加速发展。网络威胁、安全态势以及攻防对抗力量的变化，持续推动着网络安全技术的创新。2023年以来，AIGC技术浪潮加快了网络安全知识和经验的大规模复制速度，提升了安全代码生成、智能研判等领域的实现效率，以ChatGPT为代表的生成式AI让行业看到了新的发展方向，并且正在尝试重新塑造网络安全产业技术方向。以量子计算、量子通信为代表的量子信息技术逐步走向落地应用，为网络安全技术的发展注入新动力。云安全、隐私计算、工业互联网安全、车联网安全、卫星互联网安全等创新应用场景也诞生了许多新解决方案，体现了各赛道为应对新形势、新风险的不断适应与创新，这为网络安全行业带来新的发展机遇。同时，随着“一带一路”倡议的深入推进，这一重要经济框架为相关国家的网络安全意识提升和网络安全市场拓展提供了契机，有助于推动我国网络安全行业的进一步发展壮大，中国网络安全公司日益加快布局

全球化业务，抢抓出海机遇。

（3）大国博弈加剧网络空间竞争烈度，产业供应链风险提升，网络攻击技术快速演进升级，网络安全挑战复杂多变。

2022年以来，国家间网络攻防、供应链攻击、勒索软件、数据泄露、黑客攻击等安全事件层出不穷，危害性更强，大国竞争趋势更加明显，叠加地缘政治冲突等负面影响，网络空间安全成为大国对抗的重要战场。2023年，80%以上的国家颁布了网络安全战略或法规，140多个国家设立了网络安全事务协调机构，110多个国家出台个人数据与隐私保护法规，60%以上的国家通过外资审查、市场许可证等方式管理网络安全产品准入，对跨国企业的合规运营产生一定的影响。同时，供应链攻击已成为主要网络攻击手段，供应链条较长的产业将面临更加严峻的供应链安全风险。全球安全态势的不确定性将对中国网络空间安全防护、供应链的安全稳定提出更大的挑战。

随着新兴技术的迅猛发展和广泛应用，新型攻击者也层出不穷，生成式人工智能新威胁崭露头角，勒索软件仍为主要攻击方式，网络攻击的重点行业主要集中在政府、医疗、通讯、金融、能源、汽车等重要领域，这使得网络安全形势更加复杂和严峻。新技术、新应用的涌现带来愈来愈多的网络安全风险和挑战，需要政府和企业不断更新安全理念，形成合力，筑牢网络安全防线。

综上所述，我国网络安全产业发展面临的形势依然复杂严峻，既有政策法规的细化深入、数字经济赋能、技术迭代创新等发展机遇，也面临大国博弈激烈、网络攻击复杂多元、行业需求阶段性趋弱等诸多挑战，网络安全行业将在高度不确定性的环境中探索前行。

2. 公司所处的行业地位分析及其变化情况

公司的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，在数字信任与身份安全软件、终端安全软件、网络安全检测与响应（NDR）、云安全、数据安全、安全服务等领域均位于市场领先地位，奠定了亚信安全在中国网络安全软件市场的领先地位。

目前，在第三方研究机构最近时期的评选中，公司核心产品及企业市场地位排名位居前列：

（1）身份安全：数字身份治理与管理代表厂商

2023年1月在安全牛《数字身份治理和管理（IGA）应用实践指南》，公司荣获代表厂商；

（2）身份安全（统一身份管理）：市场份额位居第一

2023年7月在IDC《中国统一身份管理平台市场份额，2022：安全建设,身份先行》，公司的身份安全产品市场份额位居第一；

（3）身份安全：市场份额排名第二

2023年10月在 IDC《2023年上半年中国IT安全软件市场跟踪报告》中，公司的身份和访问管理产品市场份额排名第二；

（4）终端安全：市场份额排名第二

2023年10月在IDC《2023年上半年中国IT安全软件市场跟踪报告》 中，公司的终端安全产品连续多年位居第二；

（5）云工作负载安全：私有云市场份额位居第三

2023年7月在IDC《中国私有云云工作负载安全市场份额，2022》中，公司的云主机安全产品市场份额位居第三；

（6）云工作负载安全：公有云市场份额位居第五

2023年7月在IDC《中国公有云云工作负载安全市场份额，2022》中，公司的云主机安全产品市场份额位居第五；

（7）网络威胁检测与响应：市场份额排名第五

2023年8月在IDC《中国网络威胁检测与响应市场份额，2022》中，公司的NDR产品市场份额排名第五；

（8）中国网络安全软件：市场份额排名第三

2023年8月在IDC《中国网络安全软件市场份额，2022》中，公司七大安全软件产品市场份额排名第三；

（9）态势感知：位居领导者象限

2023年7月在IDC《IDC MarketScape：中国态势感知解决方案市场2023年厂商评估》中，公司的态势感知产品位居领导者象限；

（10）零信任：技术代表厂商

2023年7月在IDC《IDC Technology Assessment：中国零信任网络访问解决方案技术评估，2023》中，公司的零信任产品SDP入围技术代表厂商；

（11）零信任：代表性厂商

2023年9月在Gartner 《Market Guide for Zero Trust Network Access, China》中，公司的零信任产品入围代表性厂商；

（12）云工作负载、云安全资源池：模范厂商

2023年10月在Gartner《Hype Cycle for Security in China, 2023》中,公司的云安全资源池、云工作负载、入选技术领域的 Sample Vendor（模范厂商），再次证明技术创新与市场实践能力；

（13）防勒索治理：防勒索领域代表厂商

2023年10月在IDC《中国热点威胁安全检测与防护解决方案，2023》中，亚信安全「方舟」勒索治理体系解决方案获评防勒索领域代表厂商，TrustOne对攻击面管理等新兴技术的创新应用，进一步推动勒索治理理念革新，助力勒索治理能力再升级；

（14）云安全生态建设代表厂商

2023年11月在IDC《中国云安全生态市场洞察，2023》中，公司凭借完整的云安全能力、云安全生态的持续建设，以产品+服务的发展模式，与云厂商一起推动云安全的升级发展，荣获云安全生态建设代表厂商；

（15）终端安全：新一代终端安全代表厂商

2023年12月在IDC《中国新一代终端安全市场洞察，2023——安全防御的“最前线”》中，正式定义了“中国新一代终端安全”的技术概念、技术演进和技术特点，公司的终端安全产品TrustOne凭借领先的技术能力，成为该领域代表厂商，其优秀行业实践成为唯一入选案例；

（16）数据安全：技术深耕型企业

2023年12月在CSA《《数据安全平台神兽企业报告（2023版）》中，公司的数据安全平台产品凭借核心竞争力、技术研发实力强、产品成熟度高，并且有良好的市场占有率，荣获“技术深耕型企业”；

（17）攻击面管理：技术代表厂商

2023年12月在安全牛《攻击面管理技术应用指南》中，公司的攻击面管理产品入围技术代表厂商；

（18）安全运营：电信行业代表厂商

2023年11月在数说安全《2023年中国网络安全运营市场研究报告》中，公司的安全运营入围2018-2022 电信行业TOP10安全运营服务商；

（19）2023年12月，在安全牛《中国网络安全企业100强》中，公司连续多年凭借综合能力入围综合能力十强，以及技术创新十强、行业应用十强、信创能力十强；

（20）新一代终端安全TrustOne ：CSA安全磐石奖

2023年12月，公司的新一代终端安全产品TrustOne凭借前瞻性理念和突出技术能力，引领中国新一代终端安全，荣获CSA 2023最高荣誉奖项——安全磐石奖。

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

（1）安全大模型的应用与大模型自身的安全正在深刻影响着网络安全行业

从安全防御视角来看，AI大模型带来的安全产品形态的改变，产品能力与响应效率的提升将带来竞争格局的改善。海外国际大厂AI+安全已初步形成生产力，以Microsoft Security Copilot和Crowdstrike Charlotte AI为代表，生成式AI技术广泛应用于安全产品与平台中，改善产品形态和功能，聚焦的功能主要在安全监控、威胁检测、资产风险、创建报告等，能够辅助安全管理人员提升安全运营的自动化水平。国内众多网络安全企业推出安全大模型，尚处于探索与测试阶段，应用方向领域相对有限，尚未真正形成生产力。

AI自身的安全也成为业内关注的热点。网络攻击的方式和手段，在人工智能技术的推动下也在不断演变，呈现出分布式、智能化和自动化的特点；同时，人工智能训练和应用过程中，会遇到数据非法获取、数据滥用、算法偏见与歧视以及敏感数据泄露等安全问题，进而带来行业总需求的提升，这将为网络安全厂商带来新的市场机遇。

（2）数据安全继续保持高热度，数据共享流通的安全成为焦点

2022年12月，中共中央、国务院发布了构建数据基础制度体系“数据二十条”，通过数据基础建设大力推进数据要素发展。随后数据要素发展进程明显加速，数据安全相关法律、法规和标准、规范也密集出台，针对数据安全的专项检查、监管和处罚明显增加。2023年10月25日，国家数据局正式挂牌，主要职责是负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等。至此，国家在数据领域的顶层规划设计已经基本成型。2023年是数据要素发展和数据安全的主要目标是完成顶层规划设计，2024年将全面进入落地行动阶段。

在数据要素加速开放共享的新形势下，隐私计算正成为支撑数据要素流通的核心技术基础设施，该领域的技术如联邦学习、多方安全计算、可信执行环境等，在确保数据不泄漏、限定数据处理目的方面具有原生的优势。未来数据流通交易、数据安全保护等市场将掀起新一轮热潮。因此，如何实现数据的共享交易流通、如何建立起各行业的跨境数据安全保护机制以及如何以持续运营的思路开展数据安全治理工作等将成为未来的重点。

（3）云原生安全发展迅速，注重云环境安全可信

随着云计算技术得到更广泛的采用，越来越多的企业根据不同业务系统的特性选择多云或混合云的模式进行部署，更多敏感数据会存储到云端，但大部分组织缺乏云安全实时评估能力，云数据泄露事件高发、API安全成为云计算应用的重大隐患。同时，云原生技术的敏捷性、可观察性、性能效率和可移植性等技术优势，以及成本优势促使数字化转型中的企业积极拥抱云原生。云原生安全技术将持续发展并成为云安全领域的重要趋势，容器安全和微隔离安全等云原生安全技术

将得到更广泛的应用部署。AI和机器学习技术在云安全领域的应用更加深入，实现更高效的威胁检测与响应机制，云安全技术向自动化方向演进，全面的云安全防护方案将成为主流。因此，云安全仍将是未来企业安全与风险管理支出中增长最快的领域之一。

（4）终端安全轻量化、一体化、智能化助力降本增效

数字化转型带来安全边界泛化，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。

（5）身份安全建设优先性、主动性增强，零信任架构持续演进

根据中国信通院《2023年零信任发展研究报告》，零信任能力涵盖六大领域，数字身份是基础组件、是核心，联合网络环境安全、终端安全、数据安全、应用工作负载安全和安全管理五个关键能力，共同赋能整体安全防御。数字身份主要解决用户身份不统一以及架构中所有对象数字身份缺失、不合法等问题。针对身份基础设施的攻击很常见，防御者使用身份检测与响应（ITDR）等策略来应对攻击，身份安全正在成为安全的关键控制面。因此，IAM在组织安全中的作用越来越大，身份安全优先建设、由被动识别向主动检测和响应转变成为业界共识。

（6）网络战、勒索攻击将继续提振APT防护需求

从2022年的俄乌战争到2023年的巴以战争，国家间的网络攻防对抗成为必要的战争手段之一，且地缘政治冲突的紧张态势极大地加重了APT防护需求。作为一种针对特定目标的复杂、隐蔽和持久的网络攻击手段，高级持续性威胁（APT）攻击近年来已演化为集各种社会工程学攻击与零日漏洞利用的综合体，成为最严峻的网络空间安全威胁之一。同时，在全球经济发展不景气的影响下，网络犯罪团伙持续涌入勒索软件攻击领域以掠取丰厚的非法利润，国内高端制造业、金融业等行业面临非常高的挑战及风险，成为勒索团伙攻击的主要目标。勒索软件攻击不仅危害个人用户的隐私和财产，还可能影响关键基础设施行业的正常运行，甚至威胁到国家安全和社会稳定。随着勒索软件即服务（RaaS）运营模式不断成熟和勒索软件构件（IABs）的兴起，勒索软件的门槛和成本显著下降，勒索攻击活动更为猖獗。

该领域要求网络安全厂商具备全网安全大数据、威胁情报、攻防知识库以及具备实战化攻防能力的安全专家等，能够进行零日漏洞的挖掘、储备，漏洞利用程序的研究、分析等，帮助客户建立完备的响应机制和预案、立体化检测和防护方案及专业化安全服务支撑。

（7）安全建设的平台化、集约化特征进一步凸显

随着连接数量的增加以及SaaS和云应用的普及，组织机构面对的攻击面在不断扩大，因此需要提高可见性和打造中心化平台，持续地监测各类威胁与暴露面情况。组织机构在连续多年的安全建设中，配置了各类安全产品工具，但因数据孤岛、信息孤岛现象突出，且企业安全运维人员能力不足以应对海量的告警及处理高级威胁事件，因此推进安全供应商的整合、安全产品的融合平台化势在必行，原来碎片化的安全能力开始向集约化、整合化、平台化转换。安全平台的多源数据汇聚、数据分析、检测与响应、智运维等优势能力将极大地提高客户的安全能力，通过平台的搭建，将离散、碎片的安全能力最小化、组件化集成于平台之中，更好地匹配业务逻辑和特性，真正实现安全能力整合的要求。

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

	2023年	2022年	本年比上年增减(%)	2021年
总资产	3,400,977,486.04	3,682,656,570.16	-7.65	2,489,526,807.56
归属于上市公司股东的净资产	2,117,938,483.39	2,647,146,253.85	-19.99	1,458,075,252.77
营业收入	1,608,088,384.17	1,720,951,997.61	-6.56	1,667,467,958.09
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	1,607,032,330.10	1,720,457,133.33	-6.59	1,667,083,818.17
归属于上市公司股东的净利润	-291,075,848.53	98,483,055.93	-395.56	178,685,242.30
归属于上市公司股东的扣除非经常性损益的净利润	-324,941,753.06	15,774,329.48	-2,159.94	94,995,540.59
经营活动产生的现金流量净额	-379,335,701.16	-260,712,946.69	不适用	143,648,403.06
加权平均净资产收益率（%）	-12.03	3.88	减少15.91个百分点	13.29
基本每股收益（元／股）	-0.7302	0.2483	-394.08	0.4963
稀释每股收益（元／股）	-	-	-	-
研发投入占营业收入的比例（%）			增加9.04个百分点	

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	236,212,569.11	327,012,162.53	428,631,503.98	616,232,148.55
归属于上市公司股东的净利润	-94,897,763.93	-76,456,114.71	-39,871,689.60	-79,850,280.29
归属于上市公司股东的扣除非经常性损益后的净利润	-112,748,669.93	-79,335,952.27	-51,408,861.49	-81,448,269.37
经营活动产生的现金流量净额	-304,829,575.00	-91,592,802.23	-212,760,038.12	229,846,714.19

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)	8,047
年度报告披露日前上一月末的普通股股东总数(户)	7,793
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

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	包含转融通借出股份的限售股份数量	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		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）		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		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）		19,328,859	4.83			无	0	其他
南京安融企业管理合伙企业（有限合伙）	-206,803	11,259,494	2.81			无	0	其他
北京亚信融创咨询中心（有限合伙）		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）	-6,611,614	10,301,138	2.58			无	0	其他
广州亚信铭安投资中心（有限合伙）	-157,564	10,159,154	2.54			无	0	其他
中国互联网投资基金管理有限公司－中国互联网投资基金（有限合伙）		10,147,655	2.54			无	0	其他
南京安宸企业管理合伙企业（有限合伙）	-2,074,434	9,380,250	2.54			无	0	其他
上述股东关联关系或一致行动的说明				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。				
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

单位:股

序号	股东名称	持股数量		表决权数量	表决权比例	报告期内表决权增减	表决权受到限制的情况
		普通股	特别表决权股份				
1	亚信信远（南京）企业管理有限公司	80,948,488		80,948,488	20.24%		/

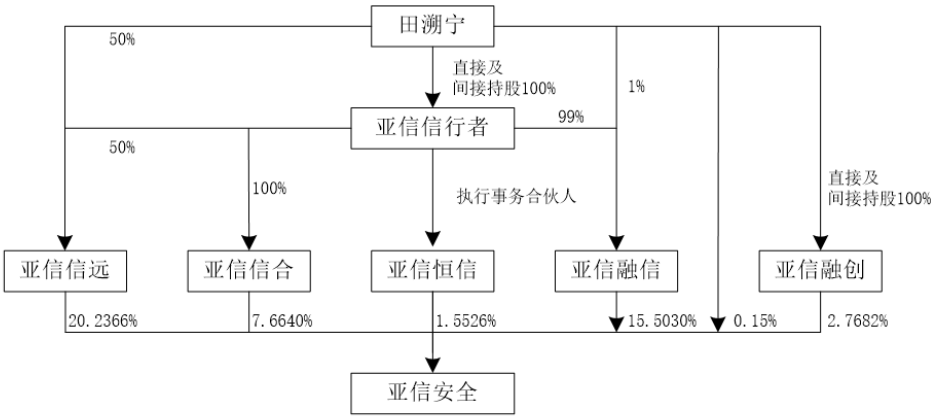
2	南京亚信融信企业管理中心（有限合伙）	62,013,649		62,013,649	15.50%		/
3	天津亚信信合经济信息咨询有限公司	30,656,621		30,656,621	7.66%		/
4	先进制造产业投资基金（有限合伙）	19,328,859		19,328,859	4.83%		/
5	南京安融企业管理合伙企业（有限合伙）	11,259,494		11,259,494	2.81%	-206,803	/
6	北京亚信融创咨询中心（有限合伙）	11,073,117		11,073,117	2.77%		/
7	广州亚信信安投资中心（有限合伙）	10,301,138		10,301,138	2.58%	-6,611,614	/
8	广州亚信铭安投资中心（有限合伙）	10,159,154		10,159,154	2.54%	-157,564	/
9	中国互联网投资基金管理有限公司－中国互联网投资基金（有限合伙）	10,147,655		10,147,655	2.54%		/
10	南京安宸企业管理合伙企业（有限合伙）	9,380,250		9,380,250	2.35%	-2,074,434	/
合计	/	255,268,425		255,268,425	/	/	/

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



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，公司实现营业收入16.08亿元，较上年同期减少6.56%。整体毛利率略有下降，从52.79%降至47.82%。公司销售渠道体系建设趋于完善，销售费用较上年同期降低0.34%，同时持续加大研发投入，研发费用较上年同期增加38.54%。报告期内归属于母公司所有者的净利润-29,107.58万元，较上年同期下降395.56%；归属于母公司所有者的扣除非经常性损益的净利润-32,494.18万元，较上年同期减少2,159.94%。

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