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

2022 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2022年年度报告中详细描述可能存在的相关风险，敬请查阅公司2022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

公司2022年度利润分配预案为：拟以实施权益分派股权登记日登记的总股本扣减公司回购专用证券账户中股份为基数分配利润，拟向全体股东每10股派发现金红利0.25元（含税；最终以公司实施本次利润分配股权登记日时，总股本扣除回购专用账户中股份数为计算基数，以公告为准）。

根据《上市公司回购股份实施细则》等有关规定，上市公司回购专用账户中的股份，不享有利润分配的权利。因此，本公司回购专用证券账户中的股份将不参与公司本次利润分配。

截止2023年3月31日，公司总股本400,010,000股，回购专用证券账户中股份总数为20,000股，以此计算合计拟派发现金红利9,999,750元（含税；最终以公司实施本次利润分配股权登记日时，总股本扣除回购专用账户中股份数为计算基数，以公告为准），占公司2022年度合并报表归属于上市公司股东净利润的10.15%。公司不进行资本公积金转增股本，不送红股。

公司2022年度利润分配预案已经由公司第一届董事会第十九次会议审议通过，尚需公司2022年年度股东大会审议通过。

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	郑京	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，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）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

随着全球数字化的蓬勃发展，以及5G、云计算、数据中心、人工智能、物联网等网络基础设施的日益完善，社会、经济、企业的数字化转型持续加速。伴随着数字化时代的来临，网络安全问题日益凸显，网络安全已成为影响国家安全的重要因素。

“十四五”时期，伴随着数字经济的快速发展，网络安全行业长期向好；网络安全作为国家战略，顶层设计和全面布局持续加强；在日益不稳定的全球网络安全冲突中，关键信息基础设施成为各国关注的焦点；数据作为数字经济的重要生产要素，数据安全领域将保持快速增长；网络安全理念发生重大改变，网络安全建设从碎片化的安全产品堆砌，向以安全平台为核心的整体防御思想转变；安全SaaS服务将成为新的商业模式，网络安全服务将成为产业高速发展的重要动力。

（1）“十四五”迈入数字经济快速发展时期，我国网络安全市场增速持续领跑全球

“十四五”时期，我国迈入由工业经济向数字经济转变的关键时期，经济社会数字化转型成为大势所趋。作为数字经济的基础保障，国家陆续出台了多项政策，推动网络安全行业发展。《“十四五”国家信息化规划》、《“十四五”数字经济发展规划》等政策提出，全面加强网络安全保障体系和能力建设，为网络安全行业的健康发展提供了良好的环境。

国内外网络安全市场未来将长期保持高速增长态势。全球方面，网络安全市场迎来复苏，知名研究机构IDC《全球网络安全支出指南》指出，2022年全球网络安全IT总投资规模1,955.1亿美元，并有望在2026年增至2,979.1亿美元，五年复合增长率（CAGR）为11.9%。

中国网络安全市场增速持续领跑全球。2026年中国网络安全IT支出规模将达到288.6亿美元，五年CAGR约为18.8%。在全球主要网络安全市场中，中国市场增速持续领跑全球。

（2）网络安全作为国家安全战略，顶层设计和全面布局持续加强，铸牢行业发展的政策基础

全球各国深化政策法律体系建设，发挥政府在网络安全中的主导作用，出台法规推进网络安全事件强制汇报机制。美国、欧盟、澳大利亚等相继通过立法，2022年3月，美国通过《关键基础设施网络事件报告法》，推动建立强制性的网络安全汇报机制，明确运营商安全事件报告要求，提升国家网络安全态势感知能力。

我国加强顶层设计，网络安全政策法规和制度体系基本形成。《中华人民共和国网络安全法》是我国网络安全领域的基础性、框架性、综合性法律，之后相继颁布《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》、《关键信息基础设施安全保护条例》等一系列法律法规。截至2022年9月，发布340余项网络安全国家标准，基本构建起网络安全政策法规的完整体系。

（3）关键基础设施网络防御已经成为网络空间对抗的主战场，已成为国家网络安全保护的重点

围绕关键信息基础的网络攻防已成为网络空间对抗的主战场，因此确保基础设施对网络威胁的防御至关重要。2022年7月，美国提出建立跨政府部门的网络风险管理机制，确保关键基础设施的安全。七国（G7）发布联合声明，将加强在基础设施网络安全方面的配合与防御。

关键基础设施已成为国家保护的重点，也是网络安全投入的重点。《关键基础设施安全保护条例》确立了我国关键基础设施安全保护的法治基础。《网络安全产业高质量发展三年行动计划（2021-2023）》提及电信等行业的安全投入比重不低于10%，其目的也在于提高关键基础设施保护的水平。针对金融、电信、能源、交通、水利等领域关键信息基础设施，国家建立了网络安全信息共享机制，加强风险评估和安全检测，强化监测预警能力，关键基础设施安全保护体系和能力建设成为国家网络安全建设的重中之重。

（4）数据成为数字经济的重要生产要素，数据安全领域将保持快速增长

随着数字经济新模式新业态的蓬勃发展，数据丢失与泄露、数据隐私保护、数据安全合规等问题越来越受到关注，数据安全防护内容不断增加，数据安全领域将保持高速增长。

数据安全和隐私保护已成为全球各国和企业非常重视的问题，根据欧盟《通用数据保护条例》

(GDPR)，欧盟可对最严重的违规行为处以高达企业年营收4%的罚款，亚马逊、Meta、谷歌、苹果等科技企业曾遭到过欧盟或相关国家的处罚。

我国网络安全市场在“十四五”期间逐步迈入高速发展阶段，受益于国家数字经济的快速发展，数据已成为重要生产要素，国家陆续出台数据安全和个人信息保护法规条例。《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》、《网络数据安全管理条例（征求意见稿）》等法律和政策文件，逐步铸牢数据安全和个人信息保护的法治屏障，数据安全逐步迈入高速发展阶段。

（5）传统碎片化防护方式难以应对新型网络威胁，以安全平台为核心的整体防御思想成为新的网络安全理念

随着网络攻击的复杂化、产业化、多样化，传统的碎片化防御手段难以应对快速变化的威胁，不同的防护设备和系统之间相互孤立，无法形成合力，难以适应新的网络安全形式。面对逐渐模糊的网络边界、数量庞大的接入终端、无处不在的攻击面、日益复杂的攻击手段，需要建立数据驱动、智能分析、协同联动的整体防御体系，才能真正帮助客户全面提升网络安全综合防护能力。

全球领先的网络安全企业纷纷把建立安全平台，构筑整体防御体系作为企业新的发展方向。CrowdStrike、Palo Alto、Fortinet等国际领先企业纷纷构建了自己的安全平台，实现了产品的协同联动。这些平台化企业在收入增长、客户粘性、盈利能力等方面远远高于传统的网络安全企业。

网络安全理念向整体防御思想演变，网络安全思想从被动式转变为主动式，注重从防御、检测、响应和预测四个维度解决构建网络安全体系，业界开始认识到安全建设需要走向更加体系化的道路，以平台为核心的“整体防御体系”已成为新的网络安全理念。

（6）商业模式面临突破，安全即服务（SECaaS）将成为云计算时代下的新型服务模式

随着数字化进程的不断加快，企业的IT架构发生重大变化，越来越多的企业机构选择上云。将安全产品功能模块部署在公有云，以订阅制方式向客户提供安全能力，已逐渐成为海外网络安全厂商的新商业模式。

安全即服务，通过订阅化方式为安全厂商带来可持续性收入，同时在成本上，可降低厂商的边际成本。我国目前主要以私有云为主，与国外以公有云为主有明显差异。我国网络安全产品的SaaS化仍处于萌芽期，面临商业模式的突破。

2. 公司所处的行业地位分析及其变化情况

公司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、终端安全软件市场、网络安全检测与响应（NDR）、云安全市场等领域均位于市场领先地位，奠定了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：市场份额位居第一

2023年4月在IDC《2022年下半年中国IT安全软件市场跟踪报告》，公司身份和数字信任产品市场份额连续6年排名第一；

（2）终端安全：市场份额位居第二

2023年4月在IDC《2022年下半年中国IT安全软件市场跟踪报告》，公司终端安全产品市场份额连续多年排名第二；

（3）威胁情报：综合型代表厂商

2022年8月在IDC《IDC Perspective：中国网络安全威胁情报市场洞察，2022》，公司威胁情报产品入选综合性代表厂商；

（4）NDR：市场份额为排名第五

2022年7月在IDC《中国网络威胁检测与响应市场厂商份额概况，2020—2021》，公司NDR产品市场份额排名第五；

（5）云工作负载、态势感知、云安全资源池：模范厂商

2022年10月在Gartner《Hype Cycle for Security in China, 2022》公司云安全资源池、云工作负载、态势感知产品入选以下三个技术领域的 Sample Vendor（模范厂商），再次证明技术创新与市场实践能力；

（6）云安全资源池：代表性厂商

2022年6月在 Gartner《中国云安全资源池创新洞察》，云安全资源池入选代表者厂商；

（7）2022年03月在Gartner《Toolkit：Vendor Identification for Cloud Security,Data Security,IAM and Security Operations in China》云主机安全、零信任身份安全产品、数据脱敏系统、数据安全治理平台、态势感知（威胁情报、漏洞管理作为功能之一入选）；

（8）身份安全：代表性厂商

2023年1月安全牛《数字身份治理与管理（IGA）应用实践指南》，数字身份治理与管理领域代表者厂；

（9）SOAR：代表者厂商

2022年1月安全牛《企业安全运营自动化（SOAR）应用指南》，SOAR领域代表者厂商；

（10）2022年3月，安全牛《2022年中国网络安全行业全景图》，入选其中的12大安全领域，47个细分领域，综合实力及各细分领域进一步得到认可；

（11）2023年2月，FreeBuf咨询《CCSIP 2022中国网络安全产业全景图》（第五版）中入选其中的17大安全领域，61个细分领域；

（12）2022年11月，在安全牛《2022中国网络安全百强企业》中入选10强企业；信创能力位十强位列第二名，细分领域代表性优秀安全企业。“基础安全防护”,“身份与访问安全”,“安全服务与运营”；

（13）2022年6月，在数世咨询《2022年中国数字安全100强》报告中，公司凭借领先的技术优势和综合实力，位居领导者象限、领军力量企业；

（14）2022年6月，在CCIA《2022年中国网安产业竞争力50强》，领导者企业；

（15）零信任：科技标杆企业

2022年11月在CSA《2022中国零信任神兽方阵》中，国内零信任领域中具有中国特色的科技标杆厂商。公司成功入选“零信任科技标杆企业”；

（16）CSA2021安全金盾奖

2022年3月，亚信安全凭借统一身份认证解决方案、云安全一体化解决方案、大终端一体化解决方案、XDR解决方案的核心竞争力，荣获国际云安全联盟大中华区2021年CSA安全金盾奖；

（17）ESM、Officescan、AISEDGE：赛可达优秀产品奖

2023年2月,信端病毒防护(OfficeScan)、信端端点安全管理系统(ESM)、信舷防毒墙(AISEDGE)在评选中表现卓越，在众多产品中脱颖而出，以突出的产品能力和技术实力成功登榜；

（18）运营商行业、制造业综合型厂商

2022年12月，嘶吼《中国网络安全产业势能榜》入选制造行业、运营商行业综合型安全厂商。

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）行业客户需求发生重大变化，从以合规驱动向实战化转变

行业客户的安全需求已经发生重大变化。在网络安全建设的前期，网络安全的合规是主要驱动力，主要是通过购买不同的网络安全产品满足合规要求。在这个过程中，不同的防护设备和系统之间相互孤立，无法形成合力。随着网络攻击的复杂化、产业化、多样化，传统的碎片化防御手段难以应对快速变化的威胁，难以适应新的网络安全形式。

针对愈发复杂的网络安全问题，需要基于网络安全实战化需要，构建体系化的整体防御体系。为此，公安部提出“三化六防”的安全思想，以“动态防御、主动防御、纵深防御、精准防御、整体防御、联防联控”为指导方针，深入推进等保和关保的落地。在此背景下，国家主管部门主导的网络安全实战演习数量显著增多，参与演习的行业与企业也愈加广泛。实战攻防演习成为政企客户网络安全保护的常态化工作，也成为政企用户检验网络安全防御体系有效性、实战性的重要手段，有效推动了政企用户对网络安全实战化、体系化建设的投入。

（2）国际网络安全形势日益紧张，关键信息基础设施领域成为行业投入重点

全球网络空间局部矛盾冲突接连不断，在日益不稳定的全球网络安全格局中，大规模针对性网络行动大幅增加，网络安全已成为影响国家安全的重要因素。美国提出2024年建立跨政府部门的网络风险管理合作机制，确保关键信息基础设施的安全。G7国家将加强在关键基础设施安全方面的配合与防御。

关键信息基础设施一旦遭到网络攻击，很可能危害国家安全、国计民生和公共利益，关键信息基础设施越来越成为保护的焦点和重点。《关键信息基础设施安全保护条例》已经正式实施，《信息安全技术关键信息基础设施安全保护要求》国家标准将于2023年实施，这些政策的实施将推动关键信息基础设施网络安全建设投入快速增长。

（3）数字经济规模持续扩大，数据安全产业迎来高速增长

我国数字经济规模持续扩大，数据安全越发受到重视，数据安全产业增速明显。随着我国数字化转型步伐加速，数据规模持续扩大，金融、医疗、交通等新兴领域数据安全投入持续增加，稳定增长的市场需求吸引越来越多的网络安全企业推出数据安全产品和服务。

随着数据安全日益成为重要的生产资料，数据安全的理念也发生重大变化，从对静态数据进行保护的狭义数据安全，向基于数据全生命周期进行保护的广义数据安全转变。企业需要基于数据安全管控平台，构建以数据为核心的数据安全保护体系。具备综合的安全能力、能够为客户提供完整解决方案的企业将迎来新的发展机遇。

2023年，《网络数据安全管理条例》有望出台，在政策法规和企业数据保护需求的双重驱动下，数据安全产品和服务市场需求更加凸显，数据安全领域增速有望进一步提高。在下游需求及国家政策推动下，各行业对数据安全的投入占比将持续增加。

（4）网络安全SaaS服务逐渐接受，将成为未来重大发展机遇

云计算已经成为新型IT基础上设施，在公有云、私有云、混合云环境中保障安全已经成为刚需。网络安全厂商需要积极应对软件化趋势，提升产品的虚拟化、云化、SaaS化，从而把握网络安全市场的下一个发展机遇。

云化为网络安全产品和服务提供了重大机遇。安全即服务，将安全产品功能模块部署在云上，以订阅制方式向客户提供安全能力，已逐渐成为海外网络安全厂商的新商业模式。通过订阅化方式为安全厂商带来可持续性收入，同时在成本上，可降低厂商的边际成本。

（5）安全数据成为核心能力，人工智能将扮演关键技术角色

在网络安全的整个攻击链中，各个环节都积累了大量的安全数据。从边界防火墙、网络流量监测、端点安全、邮件网关、云主机安全等等，存在着大量的日志数据、流量数据、威胁数据，这些网络安全数据蕴藏了威胁攻击的完整信息，从中可以识别网络攻击的完整链条。

人工智能可以通过发现和检测网络攻击的安全威胁，来提升自身网络安全保护水平。同时，人工智能也可能被恶意用于创建更加复杂的攻击，增加网络攻击监测发现的难度。随着人工智能技术的发展，攻击方将利用人工智能更快、更准地发现漏洞，产生更难以检测识别的恶意代码，发起更隐秘的攻击。另一方面，防守方则可以利用人工智能提升检测、防御及自动化响应能力。未来，人工智能将在网络安全中扮演至关重要的角色。

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

	2022年	2021年	本年比上年增减(%)	2020年
总资产	3,681,530,966.95	2,489,526,807.56	47.88	1,970,252,609.37
归属于上市公司股东的净资产	2,646,021,699.68	1,458,075,252.77	81.47	1,230,747,760.16

营业收入	1,720,951,997.61	1,667,467,958.09	3.21	1,274,594,672.06
归属于上市公司股东的净利润	98,550,790.37	178,685,242.30	-44.85	170,377,721.72
归属于上市公司股东的扣除非经常性损益的净利润	7,647,434.71	94,995,540.59	-91.95	140,012,725.33
经营活动产生的现金流量净额	-260,712,946.69	143,648,403.06	-281.49	205,070,000.55
加权平均净资产收益率（%）	3.88	13.29	减少9.41个百分点	19.55
基本每股收益（元／股）	0.2483	0.4963	-49.97	0.4778
稀释每股收益（元／股）	0.2483	0.4963	-49.97	0.4778
研发投入占营业收入的比例（%）	18.74	13.92	增加4.82个百分点	12.72

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	284,761,842.78	308,153,528.01	435,840,109.69	692,196,517.13
归属于上市公司股东的净利润	-78,257,613.43	-92,344,933.83	4,126,610.96	265,026,726.67
归属于上市公司股东的扣除非经常性损益后的净利润	-93,814,551.67	-103,003,246.91	-8,955,434.26	213,420,667.55
经营活动产生的现金流量净额	-224,648,376.03	-134,299,588.42	-44,364,727.37	142,599,745.13

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)	8,863
年度报告披露日前上一月末的普通股股东总数(户)	8,546
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	-	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	-	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	-	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	19,328,859	-	无	-	其他
广州亚信信安投资中心（有限合伙）	-	16,912,752	4.23	16,912,752	-	无	-	其他
成都亚信融安企业管理中心（有限合伙）	-	11,466,297	2.87	11,466,297	-	无	-	其他
成都亚信安宸企业管理中心（有限合伙）	-	11,454,684	2.86	11,454,684	-	无	-	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	-	其他
广州亚信铭安投资中心（有限合伙）	-	10,316,718	2.58	10,316,718	-	无	-	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	10,147,655	-	无	-	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、亚信融安的执行事务合伙人为北京亚信融安咨询有限公司，成都安宸的执行事务合伙人为北京亚信安宸咨询有限公司，亚信铭安的执行事务合伙人为北京亚信铭安咨询有限公司，亚信融安、亚信安宸、亚信铭安的执行事务合伙人均为公司董事长何政先生持股60%的公司；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

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	广州亚信信安投资中心（有限合伙）	16,912,752	/	16,912,752	4.23%	/	/
6	成都亚信融安企业管理中心（有限合伙）	11,466,297	/	11,466,297	2.87%	/	/
7	成都亚信安宸企业管理中心（有限合伙）	11,454,684	/	11,454,684	2.86%	/	/
8	北京亚信融创咨询中心（有限合伙）	11,073,117	/	11,073,117	2.77%	/	/
9	广州亚信铭安投资中心（有限合伙）	10,316,718	/	10,316,718	2.58%	/	/
10	中国互联网投资基金管理有限公司－中国	10,147,655	/	10,147,655	2.54%	/	/

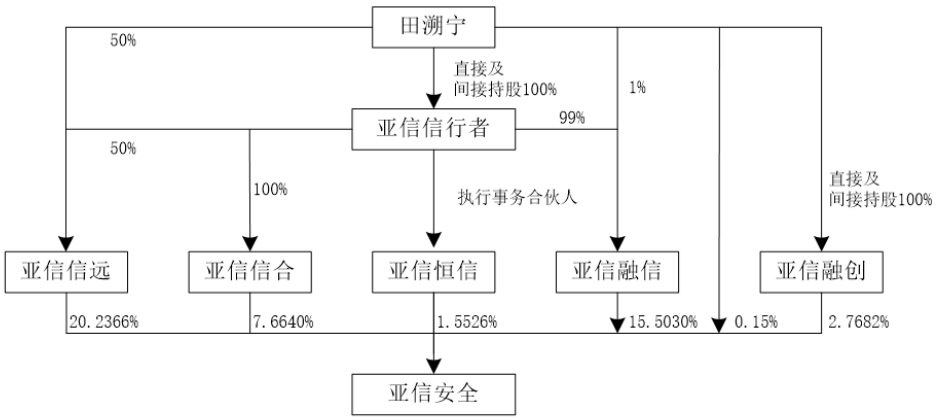
	互联网投资基金（有限合伙）						
合计	/	264,318,840		264,318,840	/	/	/

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17.21亿元，较上年同期增加3.21%。整体毛利率略有下降，从53.35%降至52.79%。公司大力投入销售和渠道体系建设，销售费用较上年同期增加28.34%，同时持续加大研发投入，研发费用较上年同期增加38.88%。报告期内实现归属于母公司所有者的净利润9,855万元，较上年同期下降44.85%；归属于母公司所有者的扣除非经常性损益的净利润764.74万元，较上年同期减少91.95%。

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