公司代码：688561　　公司简称：奇安信

奇安信科技集团股份有限公司

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 http://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“第三节管理层讨论与分析”之“风险因素”中说明了可能对公司产生重大不利影响的风险因素，并提请投资者特别关注如下风险：

1、业绩下滑或亏损的风险

2023 年公司营业收入 644,248.73 万元，同比增长 3.53%。但是，公司未来营收能否保持持续增长，受到宏观经济、产业政策、行业竞争态势等宏观环境等因素的影响，同时公司未来经营业绩也取决于公司技术研发，产品市场推广及销售等因素。市场规模的变化、细分领域的市场竞争加剧、产品更新换代、新市场需求的培育等因素均可能导致下游市场需求发生波动。如果未来公司现有主要产品市场需求出现持续下滑或市场竞争加剧，同时公司未能及时培育和拓展新的应用市场，将导致公司主营业务收入、净利润面临下降的风险。公司将持续在产品研发、市场推广及销售等方面进行投入，如公司收入未能按计划增长，或规模效应未按预期逐步显现，则可能导致亏损进一步增加。如果上述影响公司持续成长的因素发生不利变化，且公司未能及时采取措施积极应对，则不能保证收入按计划增长，以致于公司存在持续亏损的风险，且将导致公司存在成长性下降或者不能达到预期的风险。

2、财务风险

1）研发投入占营业收入比重较高，持续资金需求较大的风险

公司所处的网络安全行业技术发展和 IT 行业技术发展有密切的关系，随着 IT 行业新技术的不断推出，网络安全行业也需要采用大量的新技术推出新的可以匹配客户需求的产品，如泛终端、新边界、大数据、云计算和人工智能等安全防护产品，开发这些产品要采用大量新技术，因此对研发人员能力的要求高，导致公司研发支出一直处于较高的水平。此外，网络安全行业与国际形势、技术发展、威胁变化均有较强的关联性，当攻防角色、模式或技术出现重大变化时，仍然需要进行较大的研发投入。

2）毛利率下降的风险

未来，在政企单位信息化改造以及新基建建设过程中，公司仍可能承接系统集成性质的网络安全项目。公司在系统集成性质的网络安全项目中向第三方采购的硬件，由于该等第三方硬件的市场较为成熟，价格相对透明，因此硬件及其他业务毛利率相对较低。此外，由于集成类项目最终客户多为政企单位，受其预算管理和集中采购制度等因素影响，付款周期较长，对公司形成营运资金占用，并使得公司应收账款增加，使得该等业务收入的增长对公司净利润贡献度较低，尽管公司产品和服务毛利率较高，但受该等业务影响使得公司主营业务毛利率存在下降的风险。

3）公司现金流持续紧张的风险

随着公司业务规模逐步增大，政企业务部分特性凸显，应收账款占营业收入的比例逐渐增加，占用公司现金的比例也同步变大。如果应收账款出现大量无法按期收回，公司业务回款出现问题，则对公司整体现金流运转情况会产生较大的负面影响。同时，公司现金流目前尚处于持续净流出状态，公司自有资金相对紧张，如果遇到市场流动性紧缩，公司生产运营资金可能会出现不足。以上情况均可能导致公司出现现金流持续紧张的风险。

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 大华会计师事务所（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

网络安全产品及技术研发以及销售和服务网络的搭建完善需要大量投入。报告期内，公司净利润为 7,494.30 万元，归属于上市公司股东的净利润为 7,175.04 万元，归属于上市公司股东的扣除非经常性损益后的净利润-9,666.86 万元。截至 2023 年 12 月 31 日，公司累计未分配利润为-292,333.56 万元。公司虽然在报告期内净利润为正，但是扣除非经常性损益后仍处于亏损状态。公司持续亏损的主要原因是选择了高研发投入的发展模式并且不断建立完善公司的销售网络和服务能力。具体而言，首先，公司核心产品主要为网络安全领域产品，随着 IT 技术的不断发展，开发这些产品要采用大量新技术，对研发人员能力要求高，因此公司研发投入依旧保持在较高水平；此外，公司在盈利模式的建设期仍需扩充研发团队和技术支持及安全服务团队，以期夯实规模性研发底座，向客户提供高质量的安全产品和服务，增加客户粘性，产生持续性商机，因此产生大量人员费用。报告期内公司研发平台已量产，研发效率显著提升，并已加强各项费用管控，但因研发费用投入总额仍较高，公司扣除非经常性损益后尚未盈利且存在累计未弥补亏损。随着公司营业收入持续增长，规模经营效益逐年提升，但未来公司扣除非经常性损益后净利润能否扭亏仍有不确定性，无法保证短期内公司可进行利润分配。

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2023年度利润分配预案为：不派发现金红利，不送红股，不以资本公积金转增股本。以上利润分配预案已经公司第二届董事会第十九次会议审议通过，尚需公司2023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

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	奇安信	688561	—

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	徐文杰	张腾
办公地址	北京市西城区西直门外南路26号院奇安信安全中心	北京市西城区西直门外南路26号院奇安信安全中心
电话	010-56509268	010-56509268
电子信箱	ir@qianxin.com	ir@qianxin.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市场，主营业务为向政府、企事业类客户提供新一代企业级网络安全产品和服务。公司创建了面向万物互联时代的网络安全协同联动的主动防御体系，并凭借持续的创新研发和以实战攻防为核心的安全能力，已发展成为国内领先的基于安全大数据、人工智能和安全运营技术的网络安全产品及服务提供商。公司面向新型基础设施建设、面向数字化业务，结合“内生安全”思想，将新一代网络安全框架作为顶层设计指导，以“数据驱动安全”为技术理念、以打造网络安全颠覆性和非对称性能力为目标，创建了面向万物互联时代的网络安全协同联动防御体系。公司针对云计算、大数据、物联网、移动互联网、工业互联网和 5G 等新技术下产生的新业态、新业务和新场景，为政府与企业等机构客户提供全面、体系化的网络安全解决方案。

报告期内，公司主营业务分为网络安全产品、网络安全服务、硬件及其他。

1、网络安全产品

公司将网络安产品分为终端安全、边界安全、数据安全、实战型态势感知四大类安全产品。

终端安全产品，包括面向万物互联场景下的各类终端安全防护产品，如终端安全防护平台、终端环境感知系统、移动终端安全防护系统、国产化安全可信浏览器等。

边界安全产品，包括防火墙及下一代防火墙、虚拟化防火墙系统、Web 应用防护系统、入侵防御与检测、VPN 安全网关、网闸（数据交换平台）、SD-WAN、边界安全栈等品类。

数据安全品类，包括数据安全态势感知平台、零信任数据安全产品、特权账号管理系统、运维安全管理系统、大数据安全交易沙箱、数据库安全审计与防护、数据防泄漏、APP 隐私合规检测平台等围绕着数据全生命周期以及云、大、移、工场景下的数据安全防护品类。

实战型态势感知产品，包括以安全大数据驱动的十类态势感知平台级产品，即网信态势感知、公安态势感知、工信态势感知、行业监管态势感知、工业互联网态势感知、安全运营态势感知、车联网态势感知、安全攻防态势感知、云场景 API 安全态势感知。

2、网络安全服务

安全服务系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，包括安全咨询与规划、评估与测试、分析与响应、订阅式威胁情报与远程托管式安全运营等。

3、硬件及其他

硬件及其他业务系公司在为客户提供体系化网络安全解决方案的过程中涉及到的政企客户信息化配套改造类项目，基于客户需求为客户外采第三方硬件产品并销售给客户的产品及运营服务等业务。

(二) 主要经营模式

1、研发模式

公司秉承“数据驱动安全”的技术理念，以市场需求为导向，坚持自主研发、自主创新，针对不同种类的产品和服务，针对不同客户的多样化需求，打造了独特的研发模式。

公司通过采用“产品（项目）开发+平台研发”的“横向”分层设置，覆盖公司业务开展中的研发场景，避免了通用性功能或模块在不同产品中的重复开发，通过委员会“纵向”技术管理组织，加强公司各类产品、安全平台、工程技术能力建设。两者形成“纵横”协同，保证了公司研发体系有序开展研发工作，能够极大地提高产品研发效率，缩短产品创新周期，降低产品成本，提高产品质量。

2、盈利模式

公司盈利主要来源于为政企客户体系化交付自主研发的网络安全产品，提供安全咨询规划、安全运营等各类安全服务，并满足政企客户在数字化转型过程中所遇到的各类网络安全建设需求。

3、采购模式

公司主要采购两大类软硬件设备，主要包括两大类：一类是公司自有产品所需的服务器、工控机等相关硬件设备；另一类是公司承接网络安全集成类业务所需的第三方软硬件产品及服务。

对于第一类物料的采购，公司建立了相关制度规范采购行为，由商务与供应链中心汇总项目及产品需求，合同订单和产品出货情况，综合考虑公司库存等因素，制定采购计划并实施采购。对于第二类物料的采购，公司主要通过招投标等市场化方式进行，如果客户有明确要求，则会根据其要求进行指定采购。

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。

（2）安全服务模式

安全服务是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、订阅式威胁情报与远程托管式安全运营等。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。

（3）安全集成模式

公司的安全集成业务主要为客户提供包含自有安全产品、安全服务、集成服务和第三方软硬件产品的销售及体系化交付。

5、销售模式

公司的产品和服务的销售采用直接销售与渠道销售相结合的模式。

（1）直接销售模式

对于大中型政企客户，如政府、公安、特种行业、金融、互联网以及能源、电力、运营商等央企和其他大型企业，公司一般采用直销的方式，安排专门的销售及技术团队为其服务，从而确保与客户持续、稳定的合作，为公司带来长期收益。

（2）渠道销售模式

对中小型客户，公司采取了区域与行业相结合的渠道销售模式，以便最大程度地覆盖更多的客户，提高市场占有率。区域经销体系是全国总经销商与各层级经销商相结合的多层次体系，各层级经销商在市场拓展、渠道建设等方面各有分工；行业渠道商主要覆盖政府、公检法司等重点行业客户，包括经销和项目合作两种模式。区域和行业渠道商根据需求采购公司产品，通常在采购后即交付给最终用户，因此项目合作伙伴的采购一般均有明确的最终用户需求。

(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

近年来，全球网络空间局部矛盾冲突接连不断，以网络战为代表的“非对称战争”手段被演绎得淋漓尽致。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，攻击复杂性持续上升，网络安全已成为影响国家安全的重要因素。为此，各国持续加强网络顶层设计、加速网络空间军事竞争、加快网络安全技术赋能，国家级网络安全能力建设正与民营企业技术融合发展，网络强国建设已经从“粗放式”发展延伸至“精细化”耕耘的新阶段。国内关键信息基础设施行业客户对网络安全实战化、体系化的重视程度持续增强。目前，网络安全建设正在从“被动式、零散式”安全产品堆砌方案逐步发展为“全面型、体系化、实战化”的主动安全防御方案；以安全服务带动产品方案的销售模式将成为产业发展的新业态，托管式安全运营将成为未来的新安全运营模式。

（1）得益于行业需求驱动，网络安全与数据安全支出未来将持续增长。

国家安全层面，网络空间安全已成为各国国防安全建设的重要组成部分，是国家关键信息基础设施行业的刚性需求。俄乌冲突期间出现了人类历史上首次公开、大规模的网络战，已引发全球国家的重要关注，促进国内关键信息基础设施行业客户加大网络空间安全能力建设的预算投入。

经济建设层面，“十四五”时期，我国经济社会数字化转型成为大势所趋，为推动战略科技创新，确保产业链、供应链安全，国家将会在包括网络安全在内的科技领域继续加大投入。同时，个人隐私和信息泄露事件频发，也推动各国通过立法加强个人信息保护工作。企业面临的隐私保护合规压力不断增加，企业需要努力适应新的、更为严苛的数据隐私法规，上述这些将有力地推动网络安全产业的快速发展。

市场空间层面，增长潜力巨大，重要行业客户的安全预算投入持续增加。2023 年 1 月，工信部等十六部门印发《关于促进数据安全产业发展的指导意见》，提出了 2025 年和 2035 年两个阶段性发展目标：到 2025 年数据安全产业规模超过 1500 亿元，年复合增长率超过 30%；到 2035 年数据安全产业进入繁荣成熟期，数据安全关键核心技术、重点产品发展水平和专业服务能力跻身世界先进行列，涌现出一批具有国际竞争力的领军企业。

（2）客户转向追求实战效果，取得先发技术优势并建立壁垒的企业将成为最大受益者。

从行业客户需求变化而言，客户的安全需求已从传统的形式化合规转向实战化效果合法。全行业客户的数字化、智能化、云转型已开展如火如荼，信息系统的安全也逐步改变之前围墙式、补丁式、形式合规式的业态，网络安全场景进入多元化发展期。在技术发展方面，激增的新应用、新场景需要网络安全的新技术、新场景，促进网络安全技术进入升级换代核心期。

在当前的转折期，传统碎片化防护方式虽然还在发挥合规作用，但面对已经模糊的网络边界、面对难以计数的接入终端，面对无处不在的攻击面，已经无法解决新技术、新场景和新业态下的安全问题。针对愈发复杂的攻防性的网络安全问题，需要建立实战化、协同联动的纵深防御体系。只有掌握基于大数据能力下的新一代网络安全技术，拥有高效全面的应急响应能力、更强的实战化效果的安全厂商，才能给客户交付具备阻断网络安全威胁的防御方案，从而获得更多的市场商机。

（3）实战攻防演习的效果日益突现，有力推动行业客户向实战化、体系化的建设方向的转变。

随着政企数字化转型的深入开展，网络攻击者的目标系统逐步转向核心业务数据和承载核心数据的业务应用。攻击工具的武器化、攻击手段的战术化，均对政企用户的网络安全防御提出了更高要求。为此，国家主管部门以“实战化、体系化、常态化”为安全监管新理念，以“动态防御、主动防御、纵深防御、精准防护、整体防护、联防联控”为新举措，构建国家网络安全综合防控系统。在此背景下，在国家级网络安全实战攻防演习中，参与演习的行业更加广泛，参与演习的主体数量显著增加。实战攻防演习成为政企用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、全面提升网络安全综合防护能力的重要手段，有效地推动了政企用户增加对网络安全实战化、体系化及安全运行能力的建设投入。

（4）行业技术门槛高且高端人才稀缺，研发效率需要创新思路提升。

网络安全行业属于技术密集型行业，对产品研发和技术创新要求较高。不同行业、不同政企用户对网络安全产品的技术需求不尽相同，网络安全企业只有在充分了解用户需求的基础上，才能研发出匹配用户真实需求的产品和解决方案。此外，网络攻击和防御技术在对抗过程中会形成海量数据与知识库，如威胁情报数据库、漏洞库、病毒库等，这些知识库都需要专门的技术研究团队和产品应用团队长时间积累才能获得。

网络安全行业属于智力密集型行业，是一个高端人才极为稀缺的行业。目前国内的网络安全高端人才主要集中于国内外一些大的安全厂商以及研究机构，数量稀少，这使得市场新进入者短期内难以获得一批了解市场需求、掌握核心技术的人才团队，无法突破研发领域中的技术壁垒，从而难以形成自身的技术或差异化优势。

网络安全行业存在大量新场景和新技术，需要不断更新迭代新产品，传统依靠“堆人”的研发模式已无法满足。网络安全创新型厂商需要持续打造以“平台+工具+数据”为核心的网络安全创新性企业，提升中长期的研发效率降低研发成本，降低网络安全行业对人才个体的依赖，未来才能够获得可持续性的增长。

2. 公司所处的行业地位分析及其变化情况

公司是业内领先的企业级网络安全产品及服务提供商，持续为政企客户提供全面的网络安全软硬件产品以及安全运营与实战化服务。2023 年公司实现营业总收入 64.42 亿元，同比增长 3.53%。2023 年 6 月，在中国网络安全产业联盟（CCIA）发布的《2023 年中国网络安全市场与企业竞争力分析报告》中，公司连续三年蝉联“中国网安产业竞争力 50 强”第一，市占率进一步提升至 9.83%。参考 IDC 报告，公司多项核心产品份额持续领先：终端安全软件连续六年稳居市场首位，安全分析和情报市场份额连续四年第一，安全咨询服务连续四年市场份额排名第一，数据安全市场份额排名第一，私有云云工作负载安全市场份额排名第一，工业互联网安全管理平台排名第二，托管安全服务市场份额排名第一。

（1）行业引领性的安全理念及安全方法论

公司率先提出并成功实践“数据驱动安全”、“内生安全”、“数智安全，内生为本”等安全理念，这些安全理念成为引领国内安全产业发展的风向标；目前，内生安全框架已经纳入到近百家央企及重要行业客户的“十四五”及未来规划中，获得了客户的良好反馈。

（2）产品线覆盖全面，拥有实战化、体系化的创新产品布局

公司是全领域覆盖的综合型网络安全厂商，具有全面的产品布局，根据 2024 年 4 月安全牛发布的《中国网络安全行业全景图（第十一版）》，共包含了 16 项一级安全分类，108 项二级安全分类，公司几乎覆盖了全部的一类安全领域，在二级安全分类覆盖广度也位居领先地位，连续多年蝉联入选全景图细分领域最多的企业；公司在数据安全、终端安全、AI+安全、态势感知、高级威胁检测、零信任、云安全、代码安全、托管服务和 SASE、工业互联网安全、车联网安全、安全运营、网络安全保险等领域进行重点布局，针对信息化建设中的重点领域和风险领域，在网络安全市场未来发展的“主航道”中夺取先机。报告期内，公司数据安全、终端安全和边界安全等品类产品营业收入占公司主营收入比例增加，市场竞争力进一步提升。

（3）打造“工具+数据+平台”进行降本提效，核心竞争力不断提升

公司作为国内网络安全产业龙头企业，更加注重网络安全领域研发模式创新，持续多年的研发投入已经初现成效，通过打造研发平台级能力来提升中长期的研发效率并降低研发成本，满足新市场新产品的快速更新迭代及低成本投入的企业发展需求。通过持续打造以“工具+数据+平台”为核心的技术研发模式，中长期降低网络安全行业对人才的依赖，增强公司核心竞争力，最终实现降本增效的目标。

（4）应急响应能力在国家级重大活动中得到充分证明

公司致力于打造体系化和强化实战化的网络安全攻防能力、威胁情报和威胁发现能力、态势感知能力与应急响应能力，建立了一支覆盖全国的应急响应团队和安全服务团队，在政企客户出现应急响应、重大安保和攻防演练需求时能够实时响应，已经形成成熟的一线专家值守、二线应急支撑、三线产品保障以及后勤保障的专业重保运营机制。奇安信多次承担国家重要活动安全保障任务，在建国 70 周年、建党 100 周年、北京冬奥会、二十大、两会等国家级重大活动和会议上履行了网络安全“守门人”的职责，为国家网络安全贡献力量。

（5）核心技术能力得到国内外权威机构的广泛认可

2023 年 5 月，国务院国资委发布《中央企业科技创新成果推荐目录（2022 年版）》，公司的态势感知与安全运营平台成功入选，并成为唯一入选的网络安全产品。

2023 年 6 月，IDC 发布《中国零信任网络访问解决方案技术评估，2023》，公司零信任网络访问解决方案在终端安全能力、身份认证管理能力、零信任网关能力、零信任控制中心能力、数据安全-零信任能力、综合服务支撑能力等所有六项关键技术能力评估中，均取得最优成绩（五项五星，一项四星），成为所有入围企业中，唯一获得五个五星且技术评估雷达图最接近正六边形的企业。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》报告中，公司凭借技术、服务以及市场等多方面的绝对领先优势，再次入选“领导者象限”，这是自 2019 年 IDC 推出该系列报告以来，公司连续三次被评为“领导者”，且能力和市场双领先。2023 年 10 月，在《IDC MarketScape: 中国数据安全管理平台 2023 年厂商评估》报告中，公司凭借综合优势位列领导者类别。在《中国数据安全市场发展趋势，2023》中，公司入选 IDC 推荐的数据安全技术和服务提供商名单。

2023 年 6 月，Gartner 发布 2023 年《Market Guide for Security Orchestration, Automation and Response Solutions》报告，继 2022 年入选后，公司再次被列为 SOAR 市场具有代表性的供应商（Representative Vendors）。 2023 年 7 月，在 Gartner 技术成熟度曲线《Hype Cycle for ICT in China, 2023》中，公司成功入选中国云安全和 SASE 代表厂商。2023 年 8 月，在 Gartner 发布的《Hype Cycle for Smart City and Sustainability in China, 2023》报告中，公司连续两年被评为 CPS 安全领域的代表供应商。2023 年 10 月，在 Gartner 发布的《中国 API 管理市场指南》中，公司入选为 API 安全领域的代表性供应商。在报告《Market Guide for Zero Trust Network Access, China》中，公司被列为具有代表性的供应商。

2023 年 7 月，国际权威机构 Forrester 发布报告《The Cybersecurity Consulting Services Landscape In Asia Pacific, Q3 2023》，公司凭借实战导向的安全咨询服务被提名，并被评为知名供应商。在《Software Composition Analysis Landscape, Q1 2023》报告中，评选出全球 23 家软件成分分析代表厂商，公司凭借在软件成分分析领域出色的产品和市场能力，公司成为亚太区少数入选的三家厂商之一。在《The External Threat Intelligence Service Providers Landscape, Q1 2023》报告中，公司入围全球中型威胁情报厂商。在 Forrester 发布的《网络分析和可视性（NAV）格局，2023 年第一季度》报告中，公司凭借天眼威胁监测与分析系统在 Forrester 报告中被提名，并在细分市场规模中跻身“大型供应商”。

2023 年 6 月，赛迪顾问发布《中国工控安全市场研究报告（2022）》，在工业安全态势感知系

统和工业主机安全市场，公司双双入围领导者象限。2023 年 8 月，在赛迪顾问发布的《中国数据安全防护与治理市场研究报告（2023）》中，公司共计入选 9 大类、38 小类数据安全各细分领域，全面覆盖数据全生命周期安全治理和数据流动各个环节安全防护，是入选该报告细分领域最多的企业。

2023 年 12 月，安全牛发布《车联网安全技术应用研究报告》，凭借车-云一体化持续风险监测方案，公司成功入选该报告并被评为车联网安全代表厂商。

报告期内，公司行业市场地位领先，多项产品市占率第一：

获得年份	报告名称	排名	来源
2023	中国终端安全软件市场份额（2022 下半年）	1	IDC
	中国安全分析和情报市场份额（2022 下半年）	1	IDC
	中国数据安全市场份额（2022 下半年）	1	IDC
	中国工业互联网安全管理平台市场份额（2022 全年）	2	IDC
	中国 IT 安全咨询服务市场（2022 下半年）	1	IDC
	中国托管安全服务市场份额（2022 下半年）	2	IDC
	中国私有云云工作负载安全市场份额（2022 全年）	1	IDC
	中国零信任网络访问解决方案市场份额（2022 全年）	2	IDC
	中国零信任网络访问场景之软件定义边界市场份额（2022 全年）	2	IDC
	中国网络安全软件市场份额（2022 全年）	1	IDC
	中国网络威胁检测与响应市场份额（2022 全年）	1	IDC
	中国数据安全市场份额（2023 上半年）	1	IDC
	中国终端安全软件市场份额（2023 上半年）	1	IDC
	中国安全分析和情报市场份额（2023 上半年）	1	IDC
	中国 IT 安全咨询服务市场（2023 上半年）	1	IDC
	中国托管安全服务市场份额（2023 上半年）	1	IDC
	中国终端安全检测与响应市场（2022 全年）	1	赛迪

报告期内，公司核心产品/创新方案上榜以下第三方机构报告：

获得年份	报告名称	品类	来源
2023	软件成分分析全景图 2023Q1	开源卫士	Forrester
	网络分析和可视性（NAV）格局，2023Q1	天眼威胁监测与分析系统	Forrester
	政企终端安全（EDR）	天擎终端安全管理系统（EDR）	赛可达实验室
	杀毒引擎	天擎终端安全管理系统（EDR）	赛可达实验室
	数据安全整体解决方案	数据安全管理认证建设指引	安全牛
	网神数据安全管理平台	数据安全管控平台应	安全牛

		用指南	
	安全威胁情报产品和服务市场指南	威胁情报	Gartner
	静态应用安全测试全景图，2023Q2	代码卫士	Forrester
	Market Guide for Security Orchestration, Automation and Response Solutions	SOAR 解决方案	Gartner
	中国态势感知解决方案市场 2023 年，厂商评估	态势感知产品	IDC
	Hype Cycle™ for ICT in China, 2023	云安全和 SASE	Gartner
	中国工控安全市场研究报告	工业安全态势感知系统和工业主机安全	赛迪
	中国等保合规市场洞察，2023	网络安全等级保护（等保 2.0）解决方案	IDC
	中国工控安全市场研究报告	工业安全态势感知系统和工业主机安全	赛迪

此外，报告期内，公司荣获以下第三方机构奖项：

获得年份	奖项名称	奖项授予	来源
2023	2022 年度优秀成员单位	奇安信	工业信息安全产业发展联盟
	2022 年度信创政务产品安全漏洞专业库优秀技术支撑单位	网神股份	国家工业信息安全发展研究中心
	优秀成员单位	奇安信	中国计算机行业协会数据安全专业委员会
	2022 年软件和信息技术服务名牌企业	奇安信	中国电子信息行业联合会
	新一代信息技术领军企业	奇安信	赛迪
	优秀技术支撑单位	网神股份	国家信息安全漏洞库
	高价值漏洞优秀贡献单位	网神股份	国家信息安全漏洞库
	高价值通报优秀贡献单位	网神股份	国家信息安全漏洞库
	2023 优秀科技成果奖	奇安信	中国国际大数据产业博览会
	网络安全优秀创新成果软件安全方向第一名	开源软件供应链安全检测关键技术研究及产业化应用	中国网络空间安全协会
	科技技术奖一等奖	奇安信（第一完成单位）	中国通信学会
	科技技术奖一等奖	网神股份（第五完成	中国通信学会

		单位）	
	2022 年度广东省科技进步一等奖	大规模网络仿真验证平台（鹏城靶场）关键技术与系统	广东省科学技术厅
	科技进步一等奖	无连接网络中安全可信的端到端传送关键技术及应用	中国电子学会
	科技进步一等奖	内部威胁敏感的高可信云服务关 键技术及应用	中国电子学会
	科技进步二等奖	移动操作系统安全关键技术及产业化	中国电子学会
	2022 年“科创中国”先导技术榜	大禹平台	中国科学技术协会
	2022 年度技术卓越奖	特权账号管理系统	IT168
	2022 年度技术卓越奖	终端安全管理系统	IT168
	数据安全治理方案赛道金奖	奇安信数据安全治理实践	2022 年数据安全大赛
	数据安全产品能力评比赛道金奖	奇安信 API 安全卫士分析与管理系统	2022 年数据安全大赛
	安全磐石奖	冬奥网络安全“零事故”解决方案	云安全联盟大中华区大会
	大数据最佳实践案例	基于数据沙箱技术的数据安全流通平台	中国国际大数据产业博览会
	云原生安全技术创新大奖	CNAPP 云原生安全管理平台	工业和信息化部
	汽车网络安全创新技术奖	奇安信	SAE 国际汽车工程师学会
	2023 年网络安全优秀创新成果大赛优胜奖	奇安信	中国网络安全产业联盟
	2023 年中国网安产业竞争力 50 强第一名	奇安信	中国网络安全产业联盟
	2023 年网络安全优秀创新成果大赛优胜奖	金融行业零信任业务安全解决方案	中国网络安全产业联盟
	2023 中国先进计算企业百强	奇安信	赛迪
	2023 年北京民营企业科技创新百强	奇安信	北京市工商联
	2022 年度漏洞信息报送突出贡献单位	奇安信	国家信息安全漏洞共享平台
	2022 年度 CNVD 技术组支撑单位	奇安信	国家信息安全漏洞共享平台
	2022 年度 CNVD 协作特别贡献单位	奇安信补天平台	国家信息安全漏洞共享平台

	2023 年软件和信息技术服务名牌企业	奇安信	中国电子信息行业联合会
	2023 民营企业研发投入 500 家	奇安信	全国工商联
	2023 民营企业发明专利 500 家	奇安信	全国工商联
	2022 年中国反网络病毒联盟优秀成员单位	奇安盘古	中国反网络病毒联盟
	2023 年优秀成员单位&优秀技术支持单位	奇安信	国家工业信息安全发展研究中心
	2023 年网络安全优秀创新成果大赛优胜奖	移动应用隐私合规解决方案	中国网络安全产业联盟
	中国网络安全 100 强榜首	奇安信	安全牛
	2023 工业信息安全监测应急优秀支撑单位	奇安信	国家工业信息安全发展研究中心
	2023 北京企业百强	奇安信	北京企业联合会

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

回顾 2023 年，数智时代安全威胁持续升级，国家级网络攻防对抗、针对关键基础设施及重要经济机构的网络攻击事件频发，直接影响国家安全和社会经济运行。黑客攻击次数和规模不断增加，攻击目标也更加广泛，不仅针对政府部门，也针对电信、银行、医疗等关键基础设施，导致业务中断和数据泄露，后果非常严重。并且随着业务开放和数据流转，新技术应用也带来了数据安全新风险，新欧盟数据立法和我国的数据安全法等均表明监管力度在不断加强，这也给政企安全建设带来了新要求。

网络安全建设正在实现“三大转变”：1）从关注 IT 到关注业务的转变，并从生产、研发以及管理等视角进行转变；2）从关注设备到关注“人”的转变，通过对身份分析、环境感知持续对“人”的行为进行监测分析和控制；3）从关注建设到关注运营的转变，通过对资产、数据以及策略的变化，加速网络安全体系化创新，包括新模式、新架构和新服务的支撑。

具体而言：

1、人工智能技术催生全新的需求与供给。人工智能大模型的出现使得在人机交互、资源管理、科学研究、内容创作等应用领域出现了全新的且强有力的工具。但同时也产生了包括数据安全、使用规范、可信伦理、知识产权及模型安全等多方面的问题。1）数据安全和隐私保护方面，涉及“显式”风险,如对训练数据不合理的存储和使用，以及“隐式”风险，如虚假信息诱导等。2）使用规范方面，在缺乏规范约束的情况下人工智能可能被恶意使用，如诈骗短信、钓鱼邮件、恶意代码、勒索软件等，因此需要强有力的法律和监管对其进行约束。3）可信伦理问题方面，面对人工智能经常性“一本正经的胡说八道”，需要用户具备基本鉴别能力，此外人工智能生成的内容是否政治正确且符合我国国情的基本价值观原则，尚存在不确定性。4）知识产权问题，目前的 AI 技术还不具备自主思维和独立思考的能力，因此不满足独创性要求，侵权问题随之产生。5）模型安全问题，如数据投毒、prompt 攻击和后门攻击等，从而引起输出错误。

任何一个时代，“矛”与“盾”产生技术革命的同时，都会带来全新的需求与供给，从而推动

市场规模的显著提升，面向攻与防的网络安全领域更是如此。从防御者，即网络安全厂商的角度来看：1）以 AIGC 为代表的人工智能技术加快了安全知识与经验的大规模复制速度，基于人工智能专用算力，大大提升了智能研判、安全代码生成等领域的实现效率。2）面对人工智能的数据隐私保护和模型安全问题，迫切需要对其进行全程监控和闭环管理，发现、检测、策略、保护、响应、处置缺一不可。因此形成了一个全新的领域，即人工智能风险与安全管理工具市场。3）面对人工智能的使用规范、可信伦理和知识产权等问题，催生了涵盖内容鉴伪、安全评估和咨询服务等为代表的一系列 AI 安全治理相关的全新市场。4）人工智能技术带来降本增效，网络安全行业百万级专业人才缺口的历史问题未来将得到极大缓解，预计行业中会逐渐诞生出诸如算法工程师、知识工程师和提示工程师等全新的技术工种。

2、内生安全框架从顶层视角构建动态综合防御体系。新基建带来复杂的应用场景，对安全防护提出更高要求，内生安全框架应运而生，从“甲方视角、信息化视角、网络安全顶层视角”出发，构建了适应不同业务场景的网络安全整体防御能力分析模型，设计了复杂异构环境下的协同联动机制，形成了全生命周期的一体化安全体系。

3、数据要素化的背景下，数据安全技术与数据合规要求不断升级。个人信息保护与数据保护是数据安全治理体系的重要组成部分，也是构建数字经济、数据中国的重中之重，随着大数据技术的发展，数据的挖掘、收集、整合和交易越来越普遍便利，大数据开发利用中的安全合规问题凸显。未来，我国数据产业将会迎来更加严格的数据安全标准和监管要求，推动数据安全在创新能力提升、标准体系建设、技术产品推广应用、产业生态构建等方面实现明显进展。

零信任及其在多业务场景的全面落地愈发显现。零信任作为数字时代的创新安全理念，不仅能解决单点的远程办公安全问题；经历过大浪淘沙后，零信任也将逐渐回归其本源，即通过以数据资源保护为核心，遵循最小权限原则，基于身份进行细粒度的权限设置与判定，持续打通用户、设备、网络、应用、数据等实体安全防护，构建端到端的网络安全体系，旨在移除隐式信任，实现主体身份可信、行为操作合规、计算环境与数据实体有效防护。

4、网络安全保险市场开始崛起。得益于政策支持及发展条件的成熟，网络安全保险作为发达国家的成熟业态，开始进入中国市场，安全厂商的安全建设能力、风险评估能力、应急响应能力等将成为合作方保险公司进行风险定价的基础，也是其筛选安全厂商作为合作伙伴的最重要参考依据。

5、车联网的网络安全场景已成为客户关注的重要领域。随着车路协同、智能驾驶技术不断成熟，智能联网车辆的数量正在快速增长，智能网联汽车已经成为未来智慧交通的重要场景，与此同时，从联网汽车到自动驾驶，软件控制功能的数量也在增加。这两个因素结合在一起增加了车辆的攻击面以及相关的网络安全风险的数量和严重性。未来主要的安全技术方向包括：智能网联汽车安全芯片技术，提高加密安全等级；入侵检测技术，使得对智能网联汽车入侵更快的响应；供应链情报威胁分析技术，能够即时反馈威胁情报，增强安全风险防御能力。

6、工业控制系统的网络安全防护成为重要方向。随着工业互联网快速发展，以及国家关键信息基础设施安全防护要求落地实施，加强工业网络安全建设越来越迫切，未来主要的安全技术发展方向包括：针对工业生产网络的高级威胁（APT）攻击检测、防护与追踪溯源技术；工业生

产网络勒索病毒检测、防护与恢复处置技术；工控系统信创替代与相应安全防护体系；工业生产网络安全防护与业务安全保障融合技术；工业互联网安全从车间、企业到行业监测监管体系持续建设与完善。

7、攻防演习推动安全产品向实战化能力方向演进。为了提升国家及相关重点单位的网络安全防护水平，实战攻防演习成为了一种常态化的重要手段，通常以实际运行的信息系统作为演习目标，通过有监督的攻防对抗，最大限度地模拟真实的网络攻击，以检验信息系统的安全性和运行保障的有效性，进而推动了网络安全产品从功能趋同向防护效果差异化转变。因此，以“攻防”视角做安全的公司开始关注打造更多具备主动防御能力的产品及实战化防护效果的安全方案落地。

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
		调整后	调整前		
总资产	16,265,493,461.40	13,759,161,754.97	13,758,541,801.57	18.22	13,482,919,295.32
归属于上市公司股东的净资产	10,162,720,175.15	9,953,774,041.17	9,953,154,891.33	2.10	9,896,102,939.90
营业收入	6,442,487,305.41	6,222,788,172.46	6,222,788,172.46	3.53	5,809,075,572.53
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	6,414,767,276.46	6,211,607,818.97	6,211,607,818.97	3.27	5,781,087,273.21
归属于上市公司股东的净利润	71,750,440.44	57,630,364.80	57,011,214.96	24.50	-554,749,572.44
归属于上市公司股东	-96,668,595.61	-305,578,250.26	-306,197,400.10	不适用	-788,162,456.44

的扣除非经常性损益的净利润					
经营活动产生的现金流量净额	-777,871,646.77	-1,261,202,932.68	-1,261,202,932.68	不适用	-1,301,961,129.80
加权平均净资产收益率（%）	0.71	0.58	0.57	增加0.13个百分点	-5.63
基本每股收益（元/股）	0.10	0.08	0.08	25.00	-0.82
稀释每股收益（元/股）	0.10	0.08	0.08	25.00	-0.82
研发投入占营业收入的比例（%）	23.06	27.23	27.23	减少4.17个百分点	30.10

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	925,073,379.88	1,557,498,481.14	1,203,729,172.16	2,756,186,272.23
归属于上市公司股东的净利润	-533,471,177.62	-346,598,469.94	-342,849,719.46	1,294,669,807.46
归属于上市公司股东的扣除非经常性损益后的净利润	-632,933,720.27	-345,741,756.29	-326,990,965.91	1,208,997,846.86
经营活动产生的现金流量净额	-724,833,101.62	-674,187,135.31	-428,682,719.64	1,049,831,309.80

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)	21,857
年度报告披露日前上一月末的普通股股东总数(户)	21,818
截至报告期末表决权恢复的优先股股东总数（户）	0
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）	0
截至报告期末持有特别表决权股份的股东总数（户）	0
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）	0

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	
齐向东		149,561,640	21.83	149,561,640		无	0	境内自然人
宁波梅山保税港区明洛投资管理合伙企业（有限合伙）		121,962,240	17.80			无	0	其他
宁波梅山保税港区安源创志股权投资合伙企业（有限合伙）		49,679,460	7.25	49,679,460		无	0	其他
天津奇安壹号科技合伙企业（有限合伙）		40,653,900	5.93			无	0	其他

招商银行股份有限公司－华夏上证科创板 50 成份交易型开放式指数证券投资基金	7,781,749	22,940,654	3.35			无	0	其他
天津奇安叁号科技合伙企业（有限合伙）		22,247,460	3.25	22,247,460		无	0	其他
国投（上海）创业投资管理有限公司－国投（上海）科技成果转化创业投资基金企业（有限合伙）		20,852,100	3.04			无	0	其他
北京金融街资本运营集团有限公司	-7,536,121	16,672,123	2.43			无	0	国有法人
产业投资基金有限责任公司		12,558,140	1.83			无	0	国有法人
香港中央结算有限公司	8,626,118	8,626,118	1.26			无	0	境外法人
上述股东关联关系或一致行动的说明				1、齐向东先生与宁波梅山保税港区安源创志股权投资合伙企业（有限合伙）、天津奇安叁号科技合伙企业（有限合伙）为一致行动人；2、天津奇安壹号科技合伙企业（有限合伙）和间接持有宁波梅山保税港区安源创志股权投资合伙企业（有限合伙）合伙企业份额的部分有限合伙人重合；3、国投（上海）科技成果转化创业投资基金企业（有限合伙）持有部分天津奇安叁号科技合伙企业（有限合伙）的合伙企业份额；4、中国电子信息产业集团有限公司为宁波梅山保税港区明洛投资管理合伙企业（有限合伙）实际控制人，同时持有产业投资基金有限责任公司部分股权。除此之外，公司未知上述其他股东之间是否存在关联关系或属于一致行动人。				
表决权恢复的优先股股东及持股数量的说明				无				

存托凭证持有人情况

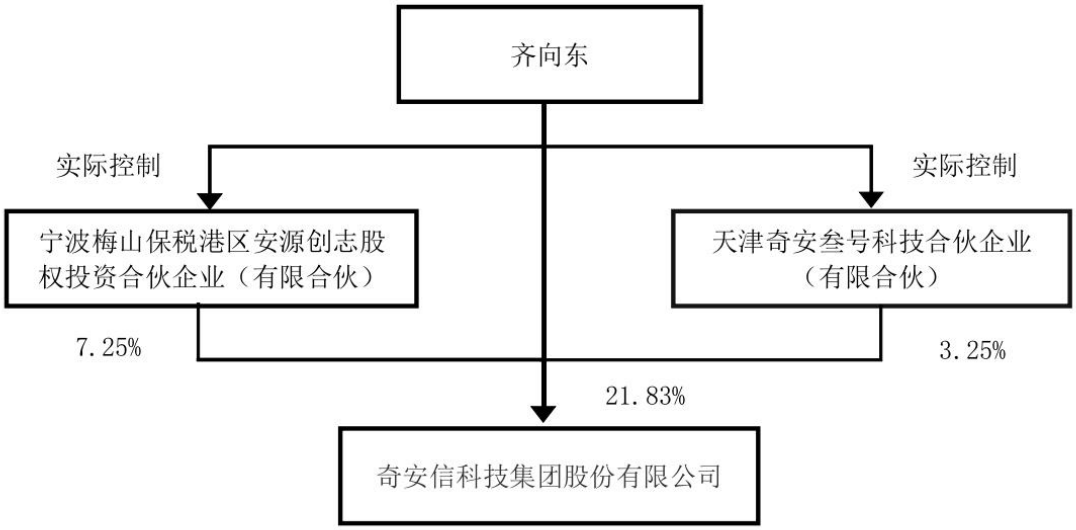
□适用 √不适用

截至报告期末表决权数量前十名股东情况表

□适用 √不适用

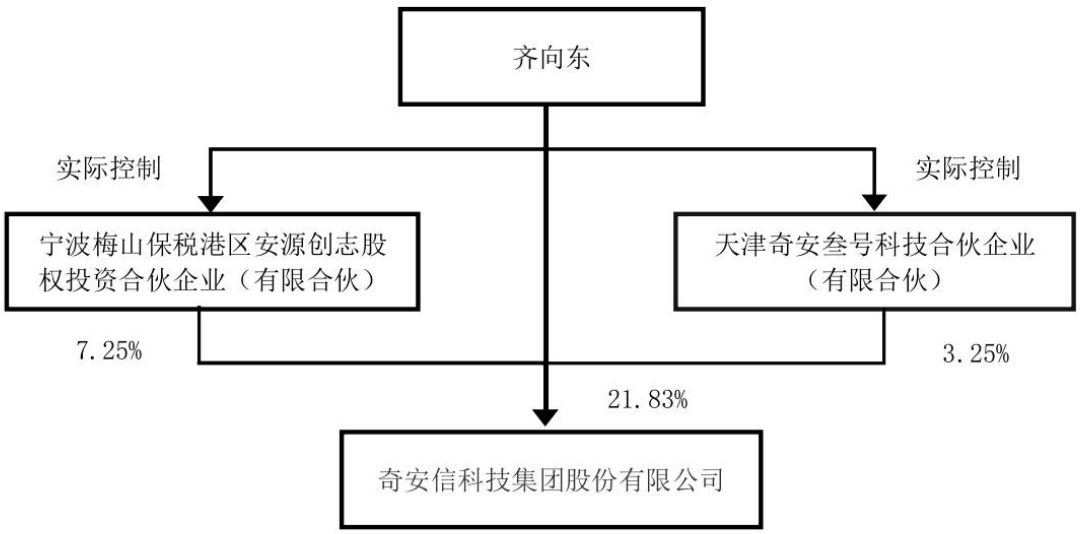
4.2 公司与控股股东之间的产权及控制关系的方框图

√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



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，公司实现营业总收入 644,248.73 万元，比上年同期增长 3.53%，其中，安全产品业务收入 473,991.37 万元，较上年度增长 4.67%，安全服务业务收入 77,904.55 万元，较上年度减少 5.71%。公司毛利率由 2022 年度的 64.34%提升至 65.38%。

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