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 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 http://www.se.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：业绩下滑或亏损的风险。2022 年公司营业收入 622,278.82 万元，同比增长 7.12%，尤其是布局的新赛道产品、主动防护类产品。公司未来能否保持持续成长，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，公司存在持续亏损的风险，将导致公司存在成长性下降或者不能达到预期的风险。

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 信永中和会计师事务所（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 5,758.96 万元，归属于上市公司股东的净利润为 5,701.12 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 -30,619.74 万元。截至 2022 年 12 月 31 日，公司累计未分配利润为 -299,654.15 万元。公司虽然在报告期内首次实现净利润扭亏为盈，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，研发平台聚焦核心技术能力的平台化输出，为安全产品提供共性核心能力，这些研发平台的开发具有周期长、投入高的特点；其次，公司核心产品主要为网络安全领域的“新赛道”产品，开发这些产品要采用大量新技术，对研发人员能力要求高，增加了公司的研发投入；此外，公司在盈利模式的建设期仍需扩张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技术服务，积聚品牌效益，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，公司研发效率显著提升，但因研发费用投入总额仍较高，尽管公司已加强各项费用管控，并且已取得良好的效果，但各项费用总额仍较高。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，随着公司各项费用管控措施的实施，营业收入持续高速增长，规模经营效益已逐年提升，但未来扣除非经常性损益后能否扭亏仍有不确定性，无法保证短期内实现盈利或进行利润分配。

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 2022 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九次会议审议通过，尚需公司 2022 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	张鹏
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、军队、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

2022 年，全球网络空间局部矛盾冲突接连不断，现实冲突与网络空间冲突相互交织。俄乌冲突期间，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。

中国网络安全市场在“十四五”期间逐步迈入高速发展阶段，受益于国家数字经济快速发展，数据已成为第七大生产要素，网络空间安全是数字经济的核心支撑，我国网安产业规模与发达国家相比仍具备很大的成长空间，产业增速将持续跑全球网络安全市场。具体而言，大数据、云计算、人工智能、5G、工业互联网、车联网等新技术新场景的快速发展，带来更多的安全需求；“十四五”规划中，强调加快推动数字产业化，培育壮大大数据、云计算、网络安全等新兴数字产业，又进一步扩大了需求侧；全行业客户数字化转型、云化转型、智能化转型的加速，让网络安全从传统的本地网络零散式安全建设到覆盖更复杂业务场景全面型体系化安全建设方案转变；俄乌冲突中网络战发挥了关键作用，俄乌战争加速了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，促进了大型政企客户持续加大网络安全建设的预算投入。

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，参考海外发达国家的安全产业特性，中国网络安全服务市场的快速发展将成为产业高速发展的重要助力。

（1）行业宏观环境持续释放利好，网络安全支出有望大幅增长。

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。俄乌战争是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，我国进入由工业经济向数字经济大踏步迈进的关键时期，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。宏观经济下行以后的经济振兴，国家发展以扩大内需为目的的新型基础设施建设，也将促进对网络安全建设的巨大需求。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，这将有力地推动网络安全产业的快速发展。

市场空间层面，我国网络安全市场增长潜力巨大，重要行业客户的安全预算投入持续增加。2021 年 7 月，工信部印发《网络安全产业高质量发展三年行动计划（2021-2023 年）》征求意见稿，到 2023 年，我国网络安全产业规模超过 2500 亿元，电信等重点行业网络安全投入占信息化投入比例不低于 10%，将培养一批面向车联网、工业互联网等新赛道的“专精特新”中小企业。2022 年 11 月，市场监管总局、中央网信办、公安部网络安全局在京联合召开了《信息安全技术关键信息基础设施安全保护要求》（国家标准发布宣贯会，同月工信部公开征求过《关于促进网络安全保险规范健康发展的意见（征求意见稿）》的意见。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）行业客户需求发生重大变化，取得先发优势并建立技术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到实战化效果合法转变。全行业客户的数字化、智能化、云化转型已开展如火如荼，“互联网 +”、“智能 +”、“5G 战略”等，推动大数据、云计算、工业互联网、物联网广泛应用，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，暴增的新应用、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。

在当前的转折关键期，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。因此，能够满足行业客户新需求并取得先发优势、已建立技术壁垒的网络安全企业将成为未来网安市场的最大受益者。

（3）实战攻防演习的监管效果日益突现，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。攻击者的角色也从普通的个人网络犯罪，到有组织的攻击甚至有境外背景的国家级对抗。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，公安部提出“三化六防”新思想，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，深入推进等保和关保的积极实践。在此背景下，国家主管部门主导的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）行业技术门槛较高、高端人才极其稀缺，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。一方面，网络安全技术和产品的创新能力是推动企业取得竞争优势的关键因素；另一方面，不同行业、不同政企用户对网络安全产品的技术需求也不尽相同，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，是一个高端人才极其稀缺的行业。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。

网络安全行业具备大量新场景、新技术需求，需要不断更新迭代新产品，传统依靠“堆人”的研发模式已经无法满足面对不断膨胀的市场新场景安全需求，网络安全创新型厂商需要通过打造“研发平台”级能力来提升中长期的研发效率降低研发成本，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。持续打造以“平台 + 工具 + 数据”为核心的网络安全创新性企业，中长期通过“工具 + 数据 + 平台”的方式降低网络安全行业对人才的依赖，未来将会获得可持续性的快速增长。

2、公司所处的行业地位分析及其变化情况

公司是行业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。2022 年公司实现营业总收入超过 62.23 亿元，位列中国网安公司营收排名第一。公司多项新赛道核心产品的市场占有率持续保持国内第一，核心产品市场竞争力和公司品牌影响力持续提升。公司作为 2022 年北京冬奥会和冬残奥会唯一网络安全服务与杀毒软件官方赞助商，通过实战化、体系化的网络安全建设，圆满完成了网络安全保障任务，实现了奥运网络安全零事故的优异成绩，公司的品牌影响力得到了进一步的提升。2022 年 6 月，由中国网络安全产业联盟发布的“2022 年 CCIA 中国网安产业竞争力 50 强”中，公司蝉联“中国网安产业竞争力 50 强”第一。参考 IDC 报告，公司多项产品份额持续领先；终端安全软件连续 6 年稳居市场首位，安全分析和情报市场份额连续 4 年第一，安全咨询服务连续 4 年市场份额排名第一，托管安全服务市场份额排名第一，网络威胁检测与响应市场份额排名第一，云工作负载安全市场份额排名第一，数据安全市场份额在网络安全公司中排名第一。

（1）公司的安全理念及安全方法论继续引领行业发展

公司率先提出并成功实践“数据驱动安全”、“内生安全”、“经营安全、安全经营”等安全理念，这些安全理念成为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”规划中，获得了客户的良好反馈。

（2）实战化、体系化的创新产品布局，新赛道产品先发优势明显

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 2023 年 4 月安全牛发布的《中国网络安全行业全景图（第十版）》，公司的产品线覆盖 14 个一级安全领域和 85 个二级细分领域，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、泛终端安全、态势感知、高级威胁检测、数据隐私保护、云安全、代码安全、SD-WAN、工业互联网安全、零信任身份安全、车联网安全、物联网安全等新领域、新赛道进行重点布局，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，公司数据安全和实战型态势感知产品营业收入占公司主营收入比例明显增加，市场竞争力显著提升。

（3）通过持续打造“工具 + 数据 + 平台”的方式进行“降本提效”，持续提升核心竞争力

网络安全行业具备“海量新场景、技术更新迭代快、新威胁不断增加”等特点，需要网络安全厂商不断更新迭代产品和技术能力，传统安全公司依靠“堆人”的研发模式已经无法满足客户日益膨胀的新网络安全需求。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，公司持续多年的研发投入已经初现成效。公司通过打造“研发平台”级能力来提升中长期的研发效率降低研发成本，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“平台 + 工具 + 数据”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，公司坚信“平台 + 工具 + 数据”的技术研发模式将助力公司未来获得可持续性高质量增长。

（4）应急响应和服务能力在实战攻防演习、重保网络安全防护中扮演中流砥柱的角色

奇安信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。在国家级实战攻防演习中，公司承担众多的防守任务，实战攻防能力得到了主管机构、政企客户的广泛认可。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、联合国生物多样性大会等国家级重大活动和会议上，奇安信履行了网络安全“守门人”的职责。截至目前，奇安信已累计参与超过 80 场国家网络安全重保、组织和参与超过 950 场实网攻防演习、协助超过 500 家国家监管机构和关键基础设施单位构建了态势感知系统，为国家网络安全贡献力量。

（5）公司核心技术能力受国内外权威机构认可

公司具有领先的安全攻防与对抗技术、终端安全防御技术、大数据与安全智能检测技术、安全运营与应急响应技术。在终端安全、安全管理、安全服务、云安全、威胁情报、态势感知领域，公司的市场占有率及技术先进性排名持续领先。2021 年 12 月，北京市经济和信息化联合北京市工商业联合会发布了北京市第一批“隐形冠军”企业认定名单，名单上共有 20 家企业，公司成功入选。2022 年 6 月，国际权威机构 Gartner 正式发布了 2022 年《Market Guide for Security Orchestration, Automation and Response Solutions》报告，详细分析了 SOAR 的市场发展情况并给出相关建议，帮助政企组织安全负责人评估 SOAR 如何支持和优化其更广泛的安全运营能力。其中，公司被列为具有代表性的供应商（Representative Providers）之一。此外，公司 SOAR 还入选了 Forrester《Now Tech: Security Orchestration, Automation, And Response (SOAR), Q2 2022》报告，进一步说明公司在该领域的强大竞争力。

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	项目	排名	来源
2022	中国终端安全软件市场份额（2022 上半年）	1	IDC
	中国 IT 安全咨询服务市场份额（2022 上半年）	1	IDC
	中国托管安全服务市场份额（2022 上半年）	1	IDC
	中国数字政府 IT 安全软件市场份额（2021 全年）	1	IDC
	中国网络威胁检测与响应市场份额（2021 全年）	1	IDC
	中国云安全市场份额（2021 全年）	1	赛迪
	中国安全管理平台份额（2021 全年）	1	赛迪
	中国安全服务份额（2021 全年）	1	赛迪
	中国终端安全产品市场份额（2021 全年）	1	赛迪
	中国云工作负载安全市场份额（2021 全年）	1	IDC
	中国终端安全软件市场份额（2021 全年）	1	IDC
	中国安全分析和情报市场份额（2021 全年）	1	IDC
	中国 IT 安全咨询服务市场（2021 全年）	1	IDC

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
2022	Innovation Insight for Cloud Security Resource Pools in China	云安全管理平台	Gartner
	Market Guide for Security Orchestration, Automation and Response Solutions	SOAR	Gartner
	“极盾 -2021”推荐名录	工业互联网安全领域 7 款产品	中国电子主办的首届“极盾”众测专项活动
	2022 全球威胁情报平台雷达图	威胁情报平台（TIP）	Frost & Sullivan

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
2022	中国先进计算企业百强	奇安信集团	赛迪
	中国网络安全企业 100 强	奇安信集团	安全牛
	中国网安产业竞争力 50 强	奇安信集团	中国网络安全产业联盟（CCIA）
	2022 年数据安全服务前十家企业	奇安信集团	中国互联网协会
	数据安全技术与产品应用优秀案例	奇安信集团	中国信通院“数据安全共同体计划（DSC）”
	隐私计算技术应用优秀案例	奇安信集团	中国信通院“数据安全共同体计划（DSC）”
	公安部科学技术奖一等奖	公安部第三研究所、奇安信集团	中华人民共和国公安部
	北京软件和信息服务业综合实力百强企业	奇安信集团	北京软件和信息服务业协会
	2022 北京软件核心竞争力企业（规模型）	奇安信集团	北京软件和信息服务业协会
	“AutoSec Awards 安全之星”2022 年度汽车网络安全突出贡献奖	奇安信集团	谈思实验室 AutoSec China Week 组委会
	北京民营企业科技创新百强（2021 年度）	奇安信集团	北京市工商业联合会
	2021 年度赛可达优秀产品奖	奇安信天擎终端安全管理系统、奇安信 OWL 反病毒引擎	赛可达实验室
	2021 年度漏洞信息报送突出贡献单位	奇安信网神	国家计算机网络应急技术处理协调中心
	2021 年度 CNVD 协作特别贡献单位	奇安信网神	国家计算机网络应急技术处理协调中心
	CNVD 技术组支撑单位	奇安信网神	国家计算机网络应急技术处理协调中心
	中国网络安全与信息产业金智奖 - 优秀产品	奇安信安全访问服务	信息安全与通信保密杂志社、中关村智能终端操作系统产业联盟
	CSA 2021 安全磐石奖	奇安信集团	云安全联盟大中华区
	2021-2022 年度新一代信息技术领军企业	奇安信集团	赛迪
	2021-2022 年度数字化创新实战案例	奇安信北京冬奥网络安全保障任务	赛迪
	2021-2022 年度新一代信息技术创新产品	奇安信网神态势感知与安全运营平台（NGSOC）、奇安信天擎终端安全管理系统奇安信 网 神 云 安 全 运 营 中 心（CSC）、奇安信网神威胁监测与分析系统（天眼）、奇安信特权账号管理系统（PAM）	赛迪
	2022 中国国际大数据产业博览会领先科技成果奖“商业模式”荣誉	奇安信冬奥网络安全应急响应 9S015 公共服务平台	数博会
	2022 领先科技成果奖“新技术”奖	奇安信开源软件供应链安全检测关键技术与产业化应用	数博会

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 2022 年，世界主要国家网络空间政治和军事领域力量继续保持增长态势，具有国家背景的黑客组织得到快速发展，网络空间主权的保障能力愈发重要，网络空间规则主导权和话语权争夺更加激烈。面对网络空间竞争的持续性对抗状态，以及俄乌战争中网络战的全关重要的作用，我国进一步增强网络防御手段、优化装备建设、研发自主技术已迫在眉睫。面对大国之间日益严峻的网空对抗形势，面对宏观经济下行后的经济复苏、面对“十四五”规划及新基建的快速推进，网络安全在维护国家安全、支撑产业转型、促进社会发展、保障公众利益等方面的重要作用愈加凸显。党的二十大对于涉及国家安全的整个大安全产业也提出了全新的指导要求，网络安全建设已成为中国数字经济发展的底板工程。

从维护国家安全看，网络空间正在成为大国竞争博弈的新战场，极限施压、技术脱钩、技术民族主义等趋势对于信息技术产业链、供应链的负面影响上升，网络空间的地缘政治属性日益显现，未来万物互联的智慧社会对于网络安全防御技术能力的综合性、及时性的要求也将更高。

从支撑产业数字化转型看，产业转型升级引导网络互联互通，实现跨行业跨领域连接和海量数据采集汇聚，同时网络威胁也能直达生产一线，有效应对工业信息安全风险已经成为支撑产业转型升级的重要保障，亟需加强网络安全技术研发的前瞻性布局。

从维护社会稳定看，此前的宏观经济下行加速了信息化手段在城市建设和政务服务中的推广，城市治理和公共服务的泛在化、融合化、智能化水平日益提升。城市公共服务和电子政务服务对于网络安全防护的需求与日俱增，构建体系化安全保障能力是必然趋势。

从保障人民利益看，用户个人信息泄露和非法利用等风险正在增加，APP 越权收集个人信息、个人隐私数据被暗网贩卖等各类网络违法犯罪行为层出不穷，数据安全与隐私保护领域需要全新的数据安全与隐私保护的创新型安全方案。

当前复杂又严峻的网络安全形势，加速了网络安全新技术、新理念、新业态和新模式向落地实践的转化，具体而言：

（1）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。

（2）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，我国数字经济将进入专业化的发展推进阶段，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。

（3）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，基于身份证明程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）生成式人工智能（AIGC）技术为网络安全行业发展带来全新的挑战和机遇。以 ChatGPT 为代表的生成式人工智能（AIGC）技术快速演进迭代。从攻击者的角度来看，恶意攻击代码和钓鱼攻击变得“唾手可得”，大大降低了网络犯罪的门槛，同时加剧了数据泄露以及个人隐私泄露等问题。而从防御者的角度来看，生成式人工智能（AIGC）技术浪潮又加快了安全知识与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，且为数据安全防护的实现路径提供了新的解决思路，并极大缓解了网络安全专业人才存在巨大缺口的历史问题。在“矛”与“盾”共同推动网络空间安全市场规模显著增长的同时，对于人工智能领域的安全规范化监管要求也迫在眉睫，从而催生了涵盖生成式人工智能（AIGC）内容鉴伪、安全评估与咨询服务等为代表的一系列 AI 安全治理相关的全新市场机遇。

（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；人侵检测技术、使得对智能网联汽车人侵更快的响应；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。工业控制系统的网络安全防护与互联网有显著区别，工业控制系统设计之初以功能为核心，未充分考虑网络安全设计，而工业生产的可靠性、连续性要求较高，通过对工业控制设备的系统升级来加固安全的措施通常很难实施。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）实战化安全运行能力建设成为客户建设的重要领域。“实战化安全运行能力建设”是立足于业务架构衍生出安全架构的组织体系建设解决方案。通过识别业务架构中支撑“生产运行”的业务驱动力、组织构成和组织行为，设计对应“安全运行”的组织建设，最终实现“生产运行”与“安全运行”的同步运行。

（8）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

	2022 年	2021 年	本年比上年增减(%)	2020 年
总资产	13,758,541,801.57	13,482,919,295.32	2.04	12,424,319,146.93
归属于上市公司股东的净资产	9,953,154,891.33	9,896,102,939.90	0.58	10,007,666,178.88
营业收入	6,222,788,172.46	5,809,075,572.53	7.12	4,161,174,135.75
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	6,211,607,818.97	5,781,087,273.21	7.45	4,153,504,586.22
归属于上市公司股东的净利润	57,011,214.96	-554,749,572.44	不适用	-334,366,055.61
归属于上市公司股东的扣除非经常性损益的净利润	-306,197,400.10	-788,162,456.44	不适用	-539,268,446.84
经营活动产生的现金流量净额	-1,261,202,932.68	-1,301,961,129.80	不适用	-688,556,343.32
加权平均净资产收益率(%)	0.57	-5.63	增加 6.20 个百分点	-4.71
基本每股收益(元 / 股)	0.08	-0.82	不适用	-0.54
稀释每股收益(元 / 股)	0.08	-0.82	不适用	-0.54
研发投入占营业收入的比例(%)	27.23	30.10	减少 2.87 个百分点	29.51

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	659,277,140.24	1,308,693,812.91	1,223,713,425.90	3,031,103,793.41
归属于上市公司股东的净利润	-480,816,938.06	-428,880,172.85	-215,399,956.81	1,182,108,282.68
归属于上市公司股东的扣除非经常性损益后的净利润	-604,585,988.60	-448,771,