奇安信科技集团股份有限公司

公司代码:688561 公司简称:奇安信

2025 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“四、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、业绩大幅下滑或亏损的风险

2025年公司实现营业收入43.92亿元,同比上升0.97%,归属于上市公司股东的净利润为-12.87亿元,同比亏损幅度收窄6.68%。公司亏损的主要原因包括:一是受宏观经济及政府财政情况影响,网安行业客户普遍削减预算,项目延期情况存在,行业价格竞争激烈;二是公司坚定贯彻“现金流优先”战略,业务的取舍在一定程度上影响了营收规模;三是公司持续坚持网络安全核心技术及创新产品的研发,研发费用投入总额仍处于较高水平,2025年研发投入占营业收入比例为24.82%;四是毛利率同比下降5.67个百分点,主要受行业价格竞争加剧、低毛利率的特种行业客户占比提升等因素影响。参考IDC排名数据,公司的拳头产品连续多年位居国内第一,核心文客户已成为市场端的中流砥柱,公司主营业务与核心竞争力均未发生重大不利变化。2025年,公司经营性现金流净额同比改善2.81亿元,创上市以来最佳,造血能力不断增强,主要财务指标实现行行业趋势一致。公司所处的网络安全行业政策法规持续完善,从顶层设计、法律、标准、产业政策、人才培养、资金投入等多维度全面发力,为行业发展提供了坚实的政策保障。公司已战略性地调整布局了基于AI的“安全智能”和面向AI的“智能安全”等新兴领域,技术替代风险相对可控。公司收入规模稳中有增,融资渠道畅通,且通过聚焦核心客户战略、推进产品AI化转型、深化费用管控、强化现金流管理等措施实现了提质增效,目前企业持续经营能力不存在重大风险。与此同时,公司研发投入占营业收入比例较高,未来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,如果未来公司现有主要产品市场需求出现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。

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,如人工智能、云终端、新边界、大数据和云计算等安全防护产品,开发这些产品需要采用大量新技术,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

报告期内,公司毛利率为50.32%,同比减少5.67个百分点。对公司毛利率带来下行影响的主要因素包括:受宏观环境影响,行业价格竞争短期内加剧;相对低毛利率的特种行业客户在公司业务中的占比逐年提升;公司渠道改革进行中,尚未充分发挥渠道与大客户直销体系间的互补作用。同时,在政企单位信息化改造以及新基建建设过程中,公司未来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。公司计划聚焦核心客户,聚焦有效市场,深度改革营销体系,聚焦经销商体系效能提升,克服短期因素对公司营收及盈利能力的影响。但前述因素及其他因素在未来可能会持续影响公司毛利率,使得公司毛利率在未来仍存在下降的风险。

(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。如果大量应收账款无法按期收回,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、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

报告期内,公司净利润为-12.85亿元,归属于上市公司股东的净利润为-12.87亿元,归属于上市公司股东的扣除非经常性损益后的净利润为-15.26亿元。截至2025年12月31日,公司累计未分配利润为-55.90亿元。公司亏损的主要原因为:从网安行业整体情况来看,受宏观环境及政府财政情况影响,客户普遍削减预算、项目延期情况依旧存在,行业价格竞争激烈。从公司层面而言,一方面公司坚定贯彻“现金流优先”的战略,经营性现金流实现持续改善,但业务的取舍也在一定程度上影响了公司的营收规模;另一方面,公司持续坚持网络安全核心技术及创新产品的研发,持续坚持强大的安全咨询规划、安全运营和应急响应服务能力的建设,以上都需要公司持续加大对研发、产品、服务等方面资源和费用的投入。报告期内,公司已着手实现产品AI化,利用AI新技术重新赋能公司产品线,研发效率提升,同时加强各项费用管控,但研发费用投入总额仍处于较高水平,未来公司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2025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三届董事会第八次会议审议通过,尚需公司2025年年度股东会审议。

母公司在本弥补亏损

√适用□不适用

截至报告期末,公司母公司财务报表中存在累计未弥补亏损3,742,785,409.65元。根据《中华人民共和国公司法》及《上市公司监管指引第3号——上市公司现金分红》等相关法律法规的规定,公司不满足实施现金分红的条件。敬请广大投资者注意相关投资风险。

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	奇安信	688561	不适用

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	徐文杰	张腾
联系地址	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
传真	010-56509199	010-56509199
电子信箱	ir@qianxin.com	ir@qianxin.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

公司专注于网络空间安全市场,主营业务为向政府和企业类客户提供领先的网络安全产品和服务。面向新型基础设施建设和客户数字化转型,公司结合“内生安全体系”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”和“AI驱动安全”为技术理念,打造了面向万物互联时代的网络安全协同联动防御体系,以及相应的产品体系和解决方案。

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

公司将网络安全产品分为终端安全、边界安全、云与大数据安全、安全运营四大类安全产品。

终端安全产品,通过“体系化防御、数字化运营”方法,帮助政企客户构建持续有效的终端安全能力,确保各类终端都能可信、安全、合规地访问业务和数据,具体包括零信任工作系统、零信任网络访问系统(ZTNA)、零信任身份分析系统(IDA)、零信任安全访问服务边缘平台(SASE)、AI可信浏览器、终端安全运营平台(ESOP)、漏洞攻击防护、SaaS终端安全管理系统等。

边界安全产品,形成了完整的纵深防御解决方案,具体包括新一代智慧防火墙、流量解密编排器(SSLO)、边界安全栈、SD-WAN、安全融合机、单向光闸、双向网闸、跨网文件安全交换管理系统(FES)、上网行为管理等。

云与大数据安全产品,其中云安全产品为客户提供覆盖云基础设施安全、云网安全、云主机安全、应用安全和数据安全的全栈式云安全能力,能满足公有云、私有云、混合云和边缘云等多种云环境下,客户对云安全及相关服务的需求,具体包括云安全管理平台(CSMP)、云原生安全保护平台(CNAPP)、云工作负载安全保护平台(CWPP)、容器安全、云安全代理网关(SWG)、云安全运营中心(CSC)等;其中数据安全产品以加强数据安全前瞻性技术创新为核心,探索构建多层次的数据安全产品及技术服务体系,持续性推出系列工具和方案,在帮助政企客户应对数字时代的数据安全难题的同时,更好地基于能力框架进行数据安全体系建设,提升整体数据安全水平,具体包括数据安全管控平台(DSCP)、数据安全网关、数据库审计与防护、特权账号管理系统(PAM)、数据脱敏、数据库防火墙、堡垒机等。

安全运营产品,主要分为监管类态势感知、运营类态势感知、攻防类态势感知,以及情报分析与支持这四个大类,具体包括态势感知与安全运营平台(AISOC)、网络资产攻击面管理系统(CAASM)、威胁监测与分析系统(天眼)、安全有效性验证(BAS)、渗透测试、攻击诱捕、邮件威胁检测、威胁情报平台(TIP)、日志收集与分析(LAS)等。

2、网络安全服务

公司秉承“内生安全”的核心理念,以“实战攻防”为导向,以“专家服务”为保障,以“云地协同”为机制构建网络安全服务体系,围绕识别、防护、检测、监测、对抗和响应(IPDMCR)的能力模型,通过安全咨询规划、安全实战攻防、安全集成实施、安全运行保障、安全应急响应、安全教育培训等一系列实战化、常态化、体系化的安全服务业务,为客户提供全生命周期的安全保障能力。

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。

2.2 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、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“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,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)后,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、制定服务方案并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。

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)法规政策持续修订并颁布,网安产业发展基础不断夯实

新修订的《中华人民共和国网络安全法》于2026年1月起正式施行,在重点强化网络安全法律责任,并加大对违法行为处罚力度的同时,还新增了人工智能安全与发展相关的内容,加强AI风险监测评估和安全监管,促进人工智能应用和健康发展,标志着我国AI治理进入“法治引领、政策支撑、企业实践”的新阶段。以此为基础,中央网信办、公安部、网安标委等密集发布相关配套文件,标志着合规体系从“原则性要求”迈向“精细化治理”。多项关键法规与标准陆续发布或更新,勾勒出一条“技术驱动、治理跟进、安全与发展并重”的清晰主线。

表:2025年内颁布的主要政策法规

时间	政策法规名称及事件	颁发部门
5月	《中国人民银行业务领域数据安全管理办法》发布	中国人民银行
6月	《关键信息基础设施商用密码使用管理规定》发布	国家密码管理局、网信办、公安部
6月	《汽车数据出境安全指引(2025版)(征求意见稿)》发布	工信部、网信办、国家发展和改革委员会、国家数据局、公安部、自然资源部、交通运输部、国家市场监督管理总局
8月	《国务院关于深入实施“人工智能+”行动的意见》发布	国务院
9月	《数据安全国家标准体系(2025版)》《个人信息保护国家标准体系(2025版)》《网络安全标准实践指南——生成式人工智能服务安全应急响应指南》发布	全国网络安全标准化技术委员会
10月	《中华人民共和国网络安全法(2025年修正)》通过	全国人民代表大会常务委员会
11月	《国家网络安全事件报告管理办法(征求意见稿)》	网信办
11月	《公安机关网络空间安全监督检查办法(征求意见稿)》发布	公安部
12月	《网络数据安全风险评估办法(征求意见稿)》发布	网信办
12月	《能源行业数据安全管理办法(试行)》发布	国家能源局

(2)AI正在重塑网络安全产业形态

近年来,以LLM(大语言模型)以及AI Agent(AI智能体)等为代表的技术正在重塑网络安全产业形态、生产力变革的同时也引入了新的威胁。与传统网络攻击相比,针对AI智能体的攻击速度更快、可利用权限更高、传播更隐蔽,传统安全监管模式往往难以及时发现和响应。攻防双方“矛”与“盾”都在加速进化,这将对网络安全产业的供给和需求产生深远影响。“AI+安全”方面,安全运营、威胁检测、渗透测试、代码安全等应用领域率先突围,预计未来还会有更多的产品能够站在AI的肩膀上,实现功能更强和性能更优。在AI应用场景侧,如何保护百亿千行的大模型,实现“管得住、看得清、防得稳”,将成为全新的蓝海市场。在上述“安全智能”(AI for Security)以及“智能安全”(Security for AI)领域,产品的打磨同时需要技术积累、人才储备和资金支持,在发展门槛上显著高于以往的产品。专有数据、切换成本、支持维护、资质认证、客户关系等形成的“护城河”会使得头部厂商获得更大的发展优势。

(3)行业技术门槛高,高端人才稀缺

网络安全行业属于技术密集型行业,不同类型用户对产品和技术的需求存在差异,因此对产品研发和技术创新的要求较高。例如,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,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,高端人才极为稀缺。目前国内的网络安全高端人才主要集中于头部安全厂商以及研究机构,数量稀少。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,不易突破研发领域中的技术壁垒,从而难以形成自身的核心技术或差异化优势。

(4)实战化效果需求凸显

伴随《公安机关网络空间安全监督检查办法(征求意见稿)》等法规相继出台,网络安全监管引入实质性判断标准,监管逻辑正经历从“静态合规”向“防御实效”的深刻转型。这一变革使传统的客户需求从合格底线要求转向为业务创造价值的运行能力支撑,从而推动行业价值从同质化的“合规盒子”流向实战化安全运营平台,产品模式从孤立设备部署转向集成化平台交付,商业模式从“产品销售”向覆盖风险评估、方案设计、安全运营、效果验证的全流程“价值交付”转型。

(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。参考第三方市场研究机构IDC排名,公司连续八年位居终端安全软件市场第一,连续六年位居安全分析和情报市场第一,连续六年位居IT安全咨询服务市场第一,连续四年位居网络威胁检测与响应市场第一,连续四年位居数据安全软件市场第一。

(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“重塑内生安全体系”、“AI驱动安全”、“数据驱动安全”等安全理念,这些安全理念成为引领网络安全产业发展的风向标;目前,内生安全框架已被纳入百余家央企及重要行业客户的业务规划中,获得了客户的良好反馈,并且正在协助客户开展“十五五”网络安全建设规划。

(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。安全牛最新发布的《中国网络安全行业全景图》共包含了17项一级安全分类和118项二级安全分类,公司几乎覆盖了全部的一级安全领域,在二级安全分类中的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。

(3)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与强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。2025年,奇安信积极参与各类国家级网络安全重保任务,在全国“两会”、九三阅兵仪式、哈尔滨亚洲冬季运动会、成都世界运动会、全国运动会、上海进口博览会等重大活动中提供7×24小时应急响应安全保障服务,获得国家相关部门及客户的高度认可。截至2025年末,奇安信累计承担国家及地区重要活动会议时期的安全保障任务108次。

(4)核心技术能力得到国内外权威机构的广泛认可

2025年6月,CCIA公布了网络安全新技术新产品新服务(第一批)遴选结果,公司凭借在人工智能反诈、安全大模型应用、威胁监测分析及渗透测试服务领域的四项成果,成为唯一同时入选“网安三新”的企业。2025年8月,在CCIA“2025年网络安全优秀创新成果大赛”中,公司凭借“新能源全场景自主可控网络安全保障体系解决方案”和“奇安信网神工业协议漏洞挖掘系统V1.0”两项成果,分别在解决方案类和创新产品类赛道中荣获优胜奖。

2025年7月,公司大模型卫士系统正式获得公安部第三研究所颁发的《大模型安全防护围栏产品认证(增强级)》证书。该认证标志着奇安信大模型卫士在安全能力上得到了权威机构的认可。

2025年11月,网络安全等级保护与安全保卫技术国家工程研究中心、公安部第三研究所(网络安全等级保护中心)正式为公司QAX-GPT安全机器人系统V1.0颁发“大模型系统安全能力评价证书”,认证其安全能力达到领先级,公司成为网络安全行业中首家大模型获此级别认证的企业。

2025年5月,公司成为中国国家信息安全漏洞库(CNNVD)首批8家“核心技术支撑单位”之一,并同时斩获7项重磅大奖,包括“优秀技术支撑单位”、“高质量通报优秀贡献单位”、“漏洞信息共享优秀厂商”、4项“漏洞奖励贡献奖”,成为蝉联获奖数量最多的网络安全企业。2025年12月,CNNVD颁发了2025年度奖誉奖项,公司凭借在漏洞挖掘、情报共享、协同治理等领域的表现,斩获六项国家级荣誉,即“优秀技术支撑单位”、“高质量漏洞优秀贡献单位”、“高质量通报优秀贡献单位”、“协同软硬件优秀漏洞管理企业”、两项“第三期漏洞奖励”。

2025年9月,在国家信息安全漏洞共享平台(CNVD)年度优秀支撑单位及个人名单中,公司凭借在漏洞报送、威胁情报共享、协同防御试点等领域的表现,斩获四项国家级荣誉。

2025年11月,在2025年世界互联网大会上,公司的AISOC智能安全运营平台蝉联“新光”产品奖。在该会议期间发布的《全球人工智能标准发展报告》中,公司入选全球负责任人工智能标准实践典型案例。

2025年3月,全球领先的IT市场研究与咨询机构IDC发布《IDC Market Glance:中国AI Agent应用市场概览,1Q25》报告,公司凭借在“AI Agent+安全”应用领域的持续创新力,入选该报告。2025年6月,IDC发布《IDC中国GenAI赋能的网络威胁检测与响应市场份额,2024:大模型深入应用,产品能力与运营效率双提升》,公司连续四年位居国内网络威胁检测与响应(NDR)市场第一。2025年6月,IDC发布《IDC MarketScape:中国CNAPP 2025年厂商评估》,公司凭借云原生应用保护平台(CNAPP)成功跻身“领导者”类别。2025年7月前后,IDC连续发布《中国大模型安全保护市场概览,2025:全方位安全检测与防护构建可信AI》以及《中国安全智能体市场概览,2025:东风已至,未来可期》,公司凭借大模型安全保护和安全智能体这两大领域的全面布局,不仅入选了中国大模型安全保护市场的全部7个细分领域(构建安全大模型、保护大模型数据存储、大模型可用性检测、保护大模型接口、大模型访问控制、大模型输入内容控制、大模型输出内容控制),还入选了中国安全智能体市场的五大领域(安全运营智能体、安全检测智能体、数据安全智能体、代码安全智能体、安全攻防智能体)。2025年9月,在IDC报告《中国私有云安全市场份额:2024》中,公司私有云安全、私有云安全软件的市场份额均在所有专业安全厂商中位列第一。2025年10月,IDC发布《中国IT安全软件市场跟踪报告,2025H1》,公司在终端安全、数据安全、安全分析与情报三大关键领域再度斩获市占率第一,持续巩固了在网络安全核心赛道的领先地位。2025年10月,IDC发布《2025上半年中国安全服务市场跟踪报告》,公司安全咨询服务连续六年位居该市场份额第一。2025年10月,IDC发布《中国大模型安全评估服务市场洞察,2025》,公司在模型安全、数据安全、内容安全等核心维度的大模型安全评估服务获得认可,成功入选该报告推荐厂商。2025年11月,IDC发布《IDC TechScape:中国网络安全软件技术发展路线图,2025》,在该报告重点关注的安全副驾驶、应用安全态势管理(ASPM)、云原生应用程序保护平台(CNAPP)、企业浏览器、零信任网络访问(ZTNA)、终端安全、网络检测与响应(NDR)、电子发现与取证、威胁情报共享9个关键技术领域中,公司均被列为推荐厂商,成为覆盖领域最多的企业。2025年12月,IDC发布报告《中国低空安全技术市场洞察与品牌推荐,2025》,公司凭借“端-网-云-机”一体化防御体系及在低空安全领域的研究与实践,入选为推荐厂商,彰显了在“低空经济”这一新质生产力赛道中的核心安全保障潜力。

2025年1月,国际权威咨询机构Forrester发布《The External Threat Intelligence Service Providers Landscape, Q1 2025》,评估了全球29家主要的外部威胁情报服务提供商(ETISP),公司凭借全面的威胁情报产品矩阵和领先的威胁情报赋能能力,入选为代表性厂商。2025年5月,Forrester发布《The Network Analysis And Visibility Solutions Landscape, Q2 2025》报告,公司连续三次获此权威认可,彰显了在网络分析与可视化(NAV)领域的技术引领能力和实战化安全能力。2025年5月,Forrester发布《Static Application Security Testing Solutions Landscape, Q2 2025》报告,评选出全球22家静态应用安全测试(SAST)代表厂商,公司成为亚太区仅入选的三家厂商之一。

2025年1月,国际市场研究与咨询机构Gartner发布《中国环境:数据安全平台市场指南》(China Context: Market Guide for Data Security Platforms),公司凭借数据安全管控平台,被认定为国内该领域的代表供应商。2025年6月,Gartner发布《中国特权访问管理市场指南》(Market Guide for Privileged Access Management in China),公司凭借特权账号管理系统(PAM)及运维安全管理系统(堡垒机)成功入选,成为国内特权访问管理代表供应商。2025年7月,Gartner发布《2025年中国网络安全技术成熟度曲线》(Hype Cycle™ for Cybersecurity in China, 2025),公司被列为10个关键领域的代表供应商,包括数据安全态势管理(DSPM)、中国AI网关、数据安全平台(DSP)、暴露评估平台(EAPs)、安全服务边缘(SSE)、软件组成分析(SCA)、物联网(IoT)身份认证、安全接入服务边缘(SASE)、零信任网络访问(ZTNA)以及安全信息和事件管理(SIEM)。2025年10月,Gartner发布《安全信息与事件管理(SIEM)魔力象限》(Magic Quadran™ for Security Information and Event Management)2025年报告,公司连续第二年入选该魔力象限,获得了全球顶尖机构的持续认可。

2025年10月,赛迪顾问发布《2024-2025年中国云安全市场研究报告》,公司连续七年蝉联中国云安全市场第一,并位居云主机安全、云安全管理平台细分市场第一。2025年10月,赛迪顾问发布《中国网络安全准入产品市场研究报告(2025)》,公司依托在信创生态适配能力、大型行业客户规模化落地等方面的优势,位居中国网络安全准入产品市场第一。2025年11月,赛迪顾问发布《2024-2025年中国网络信息安全市场研究年度报告》,公司连续六年位居中国网络信息安全市场第一,并在终端安全、安全管理平台和安全服务三大核心领域蝉联市场份额首位。2025年12月,赛迪顾问发布《中国威胁情报市场研究报告(2025)》,公司在威胁情报领域连续三年斩获国内市场份额第一。

2025年4月,国内知名安全媒体安全牛发布《智能化安全运营中心(ISOC)应用指南(2025年)》,公司凭借QAX安全大模型为核心的AISOC解决方案,成为本次报告的推荐厂商。2025年10月,安全牛发布报告《AI赋能主动防御技术应用指南(2025)》,公司AISOC智能安全运营解决方案以其实战成效与创新价值,为全行业提供了可落地、可复用的标杆经验,获得该报告优秀案例推荐。

2025年1月,公司QAX-GPT安全机器人系统荣获中国计算机行业协会网络和数据安全专业委员会颁发的“2024年度十佳网络和数据安全产品创新奖”。

2025年5月,在开源鸿蒙安全委员会主办的“聚智聚力,共筑OpenHarmony安全生态”论坛上,公司盘古实验室荣获“2025年度开源鸿蒙社区漏洞挖掘突出贡献团队”称号。

2025年6月,在中国信息技术应用创新峰会上,公司成功入围“2025政务行业信创生态图谱”,凭借为某部委打造的信创替换及业务升级解决方案,获得《2025信创中国一重点行业成功实践案例》推荐。

2025年6月,在“工信部网络安全威胁和漏洞信息共享平台——车联网产品安全漏洞专业库(NVDB-CAVD)2025汽车信息安全春季赛”中,公司代码安全实验室在15支赛队伍中荣获第一名,展现了在智能网联汽车信息安全领域的技术积累与实战攻防能力。

报告期内,公司行业地位领先,多项产品市占率第一:

获得年份	报告名称	排名	来源
2025	2024上半年中国安全托管服务市场份额	1	IDC
	《中国IT安全软件市场跟踪报告,2025H1》终端安全	1	IDC
	《中国IT安全软件市场跟踪报告,2025H1》数据安全	1	IDC
	《中国IT安全软件市场跟踪报告,2025H1》安全分析和情报	1	IDC
	《2025上半年中国安全服务市场跟踪报告》安全咨询服务	1	IDC
	《中国私有云安全市场份额:2024》私有云安全	1	IDC
	《中国威胁情报市场研究报告(2024)》	1	赛迪
	《中国网络威胁检测与响应市场研究报告(2024)》	1	赛迪
	《中国工控安全市场研究报告(2024)》工业态势感知	1	赛迪
	《中国工控安全市场研究报告(2024)》工控准入	1	赛迪
	《2024-2025年中国网络信息安全市场研究年度报告》终端安全	1	赛迪
	《2024-2025年中国网络信息安全市场研究年度报告》安全管理平台	1	赛迪
	《2024-2025年中国网络信息安全市场研究年度报告》安全服务	1	赛迪
	《2024-2025年中国云安全市场研究年度报告》云安全	1	赛迪
	《中国网络安全准入产品市场研究报告(2025)》网络安全准入	1	赛迪

(下转B620版)

本公司董事会及全体董事保证本公告内容不存在任何虚假记载、误导性陈述或者重大遗漏,并对其内容的真实性、准确性和完整性依法承担法律责任。

奇安信科技集团股份有限公司

2026 第一季度报告

证券代码:688561 证券简称:奇安信

重要内容提示

公司董事会及董事、高级管理人员保证季度报告内容的真实、准确、完整,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。

公司负责人、主管会计工作负责人及会计机构负责人(会计主管人员)保证季度报告中财务信息的真实、准确、完整。

第一季度财务报表是否经审计

□是√否

一、主要财务数据

(一)主要会计数据和财务指标

单位:元 币种:人民币

项目	本报告期	上年同期	本报告期比上年同期增减变动幅度(%)
营业收入	716,556,472.14	686,081,196.14	4.44
利润总额	-400,151,433.09	-422,732,463.16	不适用
归属于上市公司股东的净利润	-388,107,947.81	-417,684,036.61	不适用
归属于上市公司股东的扣除非经常性损益的净利润	-360,834,993.65	-410,352,297.08	不适用
经营活动产生的现金流量净额	-494,756,510.51	-763,794,623.61	不适用
基本每股收益(元/股)	-0.57	-0.61	不适用
稀释每股收益(元/股)	-0.57	-0.61	不适用
加权平均净资产收益率(%)	-5.35	-4.88	减少0.47个百分点
研发投入合计	234,440,582.43	281,253,635.06	-16.64
研发投入占营业收入的比例(%)	32.72	40.99	减少8.27个百分点
	本报告期末	上年度末	本报告期末比上年度末增减变动幅度(%)
总资产	13,411,749,181.30	13,668,699,739.48	-1.88
归属于上市公司股东的所有者权益	7,060,887,830.81	7,447,560,205.32	-5.19

(二)非经常性损益项目和金额

√适用□不适用

单位:元 币种:人民币

非经常性损益项目	本期金额	说明
非流动性资产处置损益,包括已计提资产减值准备的冲销部分	-139,150.78	
计入当期损益的政府补助,但与公司正常经营业务密切相关、符合国家政策规定、按照确定的标准享有、对公司损益产生持续影响的政府补助除外	7,233,570.18	
除同公司正常经营业务相关的有效套期保值业务外,非金融企业持有金融资产和金融负债产生的公允价值变动损益以及处置金融资产和金融负债产生的损益	-42,449,794.86	
计入当期损益的对非金融企业收取的资金占用费		
委托他人投资或管理资产的损益		
对外委托贷款取得的损益		
因不可抗力因素,如遭受自然灾害而产生的各项资产损失		
单独进行减值测试的应收款项减值准备转回		
企业取得子公司、联营企业及合营企业的投资成本小于取得投资时应享有被投资单位可辨认净资产公允价值产生的收益		
同一控制下企业合并产生的子公司期初至合并日的当期净损益		
非货币性资产交换损益		
债务重组损益		
企业因相关经营活动不再持续而发生的一次性费用,如安置职工的支出等		
因税收、会计等法律、法规的调整对当期损益产生的一次性影响		
因取消、修改股权激励计划一次性确认的股份支付费用		
对于现金结算的股份支付,在可行权日之后,应付职工薪酬的公允价值变动产生的损益		
采用公允价值模式进行后续计量的投资性房地产公允价值变动产生的损益		
交易价格显失公允的交易产生的收益		
与公司正常经营业务无关的或有事项产生的损益		
受托经营取得的托管费收入		
除上述各项之外的其他营业外收入和支出	873,735.03	
其他符合非经常性损益定义的损益项目	2,397,804.50	系个税手续费返还
减:所得税影响额	-4,820,375.28	
少数股东权益影响额(税后)	9,493.51	
合计	-27,272,954.16	

对公司将《公开发行证券的公司信息披露解释性公告第1号——非经常性损益》未列举的项目认定为非经常性损益项目且金额重大的,以及将《公开发行证券的公司信息披露解释性公告第1号——非经常性损益》中列举的非经常性损益项目界定为经常性损益的项目,应说明原因。

√适用□不适用

项目	涉及金额	原因
增值税退税	816,630.06	详见说明

说明:根据财政部、国家税务总局颁布的《关于软件产品增值税政策的通知》(财税[2011]100号),增值税一般纳税人销售其自行开发生产的软件产品,对其增值税实际税负超过3%的部分实行即征即退政策。该项税收优惠政策长期保持稳定,预期未来相当长一段时间内将继续保持;且软件产品增值税即征即退收入与公司产品销售情况密切相关,是常态化的补助。故将该项收入定义为经常性损益。

(三)主要会计数据、财务指标发生变动的情况、原因

√适用□不适用

项目名称	变动比例(%)	主要原因
经营活动产生的现金流量净额	不适用	主要系报告期内公司坚定贯彻“现金流优先”的战略,经营性现金流实现持续改善所致

二、股东信息

(一)普通股股东总数和表决权恢复的优先股股东数量及前十名股东持股情况表

单位:股

报告期末普通股股东总数	26,548	报告期末表决权恢复的优先股股东总数(如有)	

前10名股东持股情况(不含通过转融通出借股份)

股东名称	股东性质	持股数量	持股比例(%)	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	
						股份状态	数量
中电金投控股有限公司	国有法人	158,242,784	23.19			无	
齐向东	境内自然人	149,561,640	21.92			无	
宁波梅山保税港区安源创志股权投资合伙企业(有限合伙)	其他	49,679,460	7.28			无	
天津奇安叁号科技合伙企业(有限合伙)	其他	22,247,460	3.26			无	
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)	其他	20,852,100	3.06			无	
产业投资基金有限责任公司	国有法人	12,558,140