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

2024 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、业绩大幅下滑或亏损的风险

2024年公司实现营业收入43.49亿元,同比下降32.49%,归属于上市公司股东的净利润为-13.79亿元,较2023年有较大幅度下滑。公司营业收入受到宏观经济、产业政策、行业竞争态势等因素的影响,同时公司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,如人工智能、泛终端、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55.99%,同比下降8.36个百分点。给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;公司收入结构发生变化,下游需求结构中的网络安全服务占比上升,影响了公司整体毛利率;公司渠道发展不及预期,没有充分发挥好渠道与大客户直销体系间的互补作用,导致公司毛利率相对较高的渠道收入同比下降。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,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

报告期内,公司净利润为-13.77亿元,归属于上市公司股东的净利润为-13.79亿元,归属于上市公司股东的扣除非经常性损益后的净利润-16.12亿元。截至2024年12月31日,公司累计未分配利润为-43.03亿元。2024年公司经营出现较大亏损,是由多重因素导致的。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,项目延期情况较为突出。行业价格竞争出现应激反应,同时客户在预算受限的情况下更关注现有系统的维护而非项目新建,预算向毛利率相对较低的网络安全服务倾斜,对行业盈利能力带来冲击。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,创上市以来最好水平,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能力的研发,持续坚持网络安全领域创新产品的研发,持续坚持建设强大的安全咨询规划、安全运营和应急响应服务能力,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,公司研发平台已量产,并已着手实现产品AI化,利用AI新技术重新赋能公司产品线,研发效率显著提升,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2024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二十五次会议审议通过,尚需公司2024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

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	上海证券交易所创板	奇安信	688561	—

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	010-56560298	010-56560298
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”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、安全运营这四个大类:

终端安全产品,即面向万物互联场景下的各类终端安全防护产品,包括终端安全防护、办公终端安全、移动终端安全和个人安全产品等细分类型,通过“体系化防御、数字化运营”的方法,帮助政企客户构建持续有效的终端安全能力,目标实现各类终端都能可信、安全、合规地访问业务和数据。

边界安全产品,涵盖智慧防火墙、入侵防御系统、入侵检测系统、Web应用防火墙系统、双向网闸、单向光闸、防毒墙系统、安全SD-WAN、抗DDoS、负载均衡、数据交换平台、边界安全栈、跨网文件交换系统、SSL流量解密编排器等多款产品,为客户提供完整的纵深防御解决方案。

云与大数据安全产品,其中的云安全产品包括云基础设施安全、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。其中的数据安全产品覆盖数据加密保护、数据完整性鉴别、数据传输安全、数据实体防护、数据防泄漏、数据安全运维、数据权限精准管控、数据交易共享、数据跨境检测、数据安全管理平台等领域,实现数据资产管理、敏感数据识别、终端数据管控、外发邮件管控、数据流转管控、数据访问监测、数据脱敏、账号自动发现与安全存储、账号自动改密、库表级运维访问控制、API资产识别与防护等功能,可以满足政企客户“一站式”数据安全建设需要,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下进行数据安全体系建设,提升整体数据安全水平。

安全运营产品,主要包括专门面向实战的攻防类态势感知产品,为安全运营人员提供威胁发现、调查分析及响应处置的运营类态势感知产品,以及监管类的态势感知产品。

2、网络安全服务

安全服务团队司秉承“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。

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,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“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),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,通常在采购后固定付给最终用户,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)政策逐步完善,网安产业发展基础不断夯实

目前,我国已经逐步建成以《网络安全法》《数据安全法》《个人信息保护法》和《关键信息基础设施安全保护条例》《网络数据安全管理条例》等为核心网络安全法律法规体系框架,为网络空间的守护及产业的健康发展提供了坚实的法律支撑和政策依据。伴随“数智化”应用场景的不断丰富和演进,国家同时也在持续细化和完善网络安全和数据安全法规细则,以确保“三法两条例”等上位法能够得到有效落实。以人工智能领域为例,我国已通过制定相关政策和标准,加强对数据安全和伦理规范的管理,同时为了应对新挑战,也在积极为人工智能安全立法做好准备。

(2)AI正在重塑网络安全产业形态

近年来,以LLM(大语言模型)为代表的GenAI(生成式人工智能)技术开始重塑网络安全产业形态,“矛”与“盾”攻防双方都在加速进化,这将对网络安全产业的供给和需求产生深远影响,安全运营、威胁检测、渗透测试、数据安全、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。而“AI+”的方向上需要技术积累、人才储备和资金支持,在发展门槛上显著高于以往的产品,头部厂商往往能够获得更大的发展优势。

(3)实战演练趋于常态化

近年来,国家相关主管部门提出并推动以“三化六防”——即以“实战化、体系化、常态化”作为安全监管新理念,和以“动态防御、主动防御、纵深防御、精准防护、整体防护、联防联控”作为新举措,构建国家网络安全综合防控系统。每年开展的实战攻防演练已成为政企客户,尤其是关基行业客户开展网络安全防护的常态化工作,在检验有效性的同时,通过对抗演练不断提升防护能力,对于推动网络安全产业由合规驱动迈向效果驱动,实现产业健康发展意义重大。

(4)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。

(5)行业发展情况与宏观经济关联度较高

网络安全行业下游客户以政企客户为主,下游需求与财政预算关系密切,经济环境会对行业小别年份的增速产生扰动。参考第三方研究机构数说安全的预测,2024年中国网络安全厂商收入规模预估为592亿元,同比下降3.5%,并且是历史上首次出现规模下降。2024年,受宏观环境及政府财政情况影响,客户预算普遍削减,项目延期情况突出,对行业发展带来一定程度的波动影响,但不改变行业长期向好的趋势。

(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。2024年9月,公司连续四年蝉联中国网络安全产业联盟(CCIA)颁布的“中国网安产业竞争力50强”第一。参考IDC等权威第三方市场研究机构排名,公司连续七年位居终端安全软件市场第一、连续五年位居安全分析和情报市场第一、连续五年位居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、连续三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“A1驱动安全”、“数据驱动安全”、“内生安全”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,并且正在为客户开展“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,根据安全牛最新发布的《中国网络安全行业全景图》,其包含了17项一级安全分类,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。

(4)核心技术能力得到国内外权威机构的广泛认可

2024年6月,公司参与申报的“超大规模多领域融合联邦靶场(鹏城网络靶场)关键技术及系统”项目获得国家科学技术进步二等奖,成为2024年度网络攻防领域唯一的国家级科学技术进步奖。

2024年1月,公司参与申报的某电子数据取证技术研究及应用项目,获评2023年公安部科学技术奖一等奖。这是公司继2022年凭借“关键信息基础设施安全保护关键技术与应用”获得公安部科学技术奖一等奖后,再次获此殊荣。

2024年11月,奇安信入选IDC产品荣获2024年世界互联网大会“新光”产品奖。

2024年7月,IDC发布《中国安全资源池技术能力评估,2024》,公司CSMP云安全资源池在众多产品中脱颖而出,获得了5项满分(总共6项维度)的成绩。2024年10月,IDC发布《IDC TechScape:中国网络安全软件技术发展路线图,2024》,公司凭借在ZTNA(零信任网络访问)、NDR(网络检测与响应)、企业浏览器、态势感知、特权访问管理、终端安全、电子发现与取证等七项技术的推荐,成为入选领域最多的推荐厂商。2024年10月,IDC发布《中国IT安全软件市场跟踪报告,2024H1》,公司在终端安全、数据安全、安全分析与情报三大关键领域进一步强化了市场领导地位。2024年11月,IDC发布《2024上半年中国安全服务市场跟踪报告》,公司在安全咨询服务、托管安全服务两大子市场均位居第一,进一步彰显了在安全服务市场领先综合实力和市场地位。2024年11月,IDC发布《生成式AI推动下的中国网络安全软件市场现状和技术发展趋势,2024》,公司凭借在终端安全、网络检测与响应(NDR)、威胁情报、API安全、零信任网络访问、态势感知等全系列产品AI化的突出表现,成为代表厂商之一。2024年11月,IDC发布报告《IDC MarketScape:中国数据安全服务2024厂商评估》,对18家数据安全服务提供商的市场规模、产品技术能力、行业客户拓展、生态系统建设等关键领域进行了专项评估,公司凭借全面的综合实力位居数据安全服务市场领导者类别。

2024年4月,国际市场研究与咨询机构Gartner发布2024年《网络检测与响应市场指南》,公司凭借天眼(威胁监测与分析系统),入选为网络检测与响应(NDR)领域全球代表性供应商,这也是公司及天眼连续第二年被Gartner评定为全球NDR领域的代表性供应商。2024年6月,Gartner发布2024年SIEM魔力象限报告,公司成功上榜,标志着NGSOC进入国际领先产品行列。2024年7月,Gartner发布技术成熟度曲线报告《2024年私有移动网络服务成熟度曲线》,公司入选成为我国攻击面管理(ASM)领域代表厂商。2024年8月,Gartner发布报告《Hype Cycle? for Security in China, 2024》,公司入选成为攻击面管理(ASM)、软件组成分析(SCA)、安全服务边缘(SSE)、IoT身份认证、安全接入服务边缘(SASE)、零信任网络访问(ZTNA)、数据安全平台(DSP)、安全信息和事件管理(SIEM)等八大领域的代表供应商。

2024年2月,公司在国际权威机构Forrester的报告《运营技术安全解决方案前景,2024年第一季度》中,凭借全生命周期的工业互联网安全能力被评为代表厂商,这是公司工业互联网安全能力又一次获得的国际权威认可。2024年6月,Forrester发布报告《Software Composition Analysis Landscape, Q2 2024》,评选出全球21家软件成分分析代表厂商,公司再次入选。同月,公司企业级防火墙凭借过硬的产品技术和安全解决方案能力,入围Forrester《The Enterprise Firewall Landscape, Q2 2024》报告,连续三次获得国际权威机构的认可和推荐。

2024年7月,中国信息通信研究院“数字安全护航计划”发布首期《数字安全护航技术能力全景图》。公司凭借全面的技术能力,成功入选全景图全部14大安全领域、103个细分领域,彰显了公司在网络安全领域的全面覆盖能力和行业领先地位。

2024年7月,赛迪顾问发布《2023-2024年中国云安全市场研究年度报告》,公司凭借产品能力和市场积淀,以及完整的云及云原生安全体系,收入规模位居国内榜首,连续6年夺冠。

2024年4月,公司推出的QAX-GPT安全机器人凭借多个方面的综合表现,获得由中国计算机行业协会人工智能专委会、中国软件测评中心(工业和信息化部软件与集成电路促进中心)联合颁发的国内首批“大模型安全评定证书”,被认定符合二级评定资格要求。这是迄今为止大模型安全服务能力的最高级别认证,处于业界领先水平。

2024年5月,全球网络安全行业盛会RSAC期间,公司的云原生应用安全保护平台(CNAPP)、网络资产攻击面管理系统(CAASM)荣膺国际领先的信息安全媒体CDM(《网络防御杂志》)颁发的先锋产品系列奖项。

2024年6月,国家信息安全漏洞库(CNNVD)2023年度工作总结暨优秀支撑单位表彰大会在中国信息安全测评中心隆重举行。公司作为CNNVD一级技术支撑单位,凭借在漏洞挖掘、漏洞消控、漏洞通报等方面的突出贡献,以综合排名第一名的成绩在262家技术支撑单位中独占鳌头,荣获8项重磅大奖,分别为“优秀技术支撑单位”、“高质量漏洞优秀贡献单位”、“漏洞消控优秀贡献单位”、“高质量通报优秀贡献单位”、“优秀特聘技术专家”、3项“漏洞奖励一级贡献奖”,其中“漏洞奖励一级贡献奖”获奖数量位居第一。

2024年8月,中国信息安全测评中心对外公布了首批安全运营二级资质企业名单。公司凭借在安全运营领域的业务规模、运营管理、人员能力、技术平台和流程管理等综合实力,成为国内首批5家获得安全运营二级资质的企业之一。

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
2024	中国云安全市场份额(2023全年)	1	赛迪
	中国威胁情报市场份额(2023全年)	1	赛迪
	中国IT安全咨询服务市场份额(2023全年)	1	IDC
	中国终端安全软件市场份额(2023全年)	1	IDC
	中国数据安全软件市场份额(2023全年)	1	IDC
	中国安全分析和情报市场份额(2023全年)	1	IDC
	中国网络威胁检测与响应市场份额(2023全年)	1	IDC
	中国私有云云工作负载安全市场份额(2023全年)	1	IDC
	中国终端安全市场份额(2023全年)	1	赛迪
	中国安全管理平台市场份额(2023全年)	1	赛迪
	中国安全服务市场份额(2023全年)	1	赛迪
	中国云安全市场份额(2023全年)	1	赛迪
	中国终端安全软件市场份额(2024H1)	1	IDC
	中国数据安全软件市场份额(2024H1)	1	IDC
	中国安全分析和情报市场份额(2024H1)	1	IDC
	中国安全咨询服务市场份额(2024H1)	1	IDC
	中国托管安全服务市场份额(2024H1)	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
2024	2023软件供应链优秀成果案例名单	云原生场景下的软件供应链安全应用实践	信息通信软件供应链安全社区
	2023年工业和信息化领域数据安全典型案例名单	数字管网数据安全与共享流通一体化方案设计与验证案例	工业和信息化部网络安全管理局
	中国工控安全市场研究报告(2023)	工业安全勒索软件	赛迪
	运营技术安全解决方案前景,2024年第一季度	工业互联网安全能力	Forrester
	网络安全保险典型服务方案目录	网络安全终端(主机)防护类产品	工业和信息化部
	网络安全保险典型服务方案目录	网络安全保险方案	工业和信息化部
	华为终端安全2023年优秀合作伙伴奖	X实验室	华为终端安全
	中央企业科技创新成果产品手册(2023年版)	奇安信威胁情报运营系统TIOS	国资委
	2024年网络检测与响应市场指南	天眼(威胁监测与分析系统)	Gartner
	2024百市场权威榜单-新一代信息技术创新产品	QAX-GPT安全机器人	赛迪
	2024百市场权威榜单-新一代信息技术创新产品	天盾数据安全保护系统	赛迪
	2024百市场权威榜单-新一代信息技术创新产品	网络资产攻击面管理系统(CAASM)	赛迪
	2024百市场权威榜单-新一代信息技术创新产品	安全代理网关SWG	赛迪
	2024百市场权威榜单-新一代信息技术创新产品	威胁溯源分析系统	赛迪
	《网络防御杂志》荣膺先锋产品奖	云原生应用安全保护平台(CNAPP)	信息安全媒体CDM
	《网络防御杂志》荣膺先锋产品奖	网络资产攻击面管理系统(CAASM)	信息安全媒体CDM
	2023年网络安全国家标准优秀实践案例	《信息安全技术 网络数据处理安全要求》	全国网络安全标准化技术委员会
	《Software Composition Analysis Landscape, Q2 2024》	开源卫士	Forrester
	国家科学技术进步二等奖	超大规模多领域融合联邦靶场(鹏城网络靶场)关键技术及系统	国务院
	Magic Quadrant? for Security Information and Event Management	NGSOC	Gartner
	《The Enterprise Firewall Landscape, Q2,2024》全球代表性供应商推荐	奇安信企业级防火墙	Forrester
	《云上勒索攻击防护系统安全能力检验证书》	奇安信棱图	中国信通院、泰尔实验室联合
	2023年度SD-WAN优秀产品奖	奇安信安全SD-WAN	中国通信标准化协会算网融合产业及标准推进委员会
	2024年《Market Guide for Security Threat Intelligence Products and Services》	奇安信威胁情报中心	Gartner
	《IDC MarketScape:中国零信任网络访问解决方案2024厂商评估》	奇安信零信任网络访问系统(奇安信ZTNA)	IDC
	2024年大模型安全实践优秀案例	奇安信QAX-GPT安全机器人系统	中国电子信息产业发展研究院,中国软件评测中心
	首批大模型系统安全能力评价证书	奇安信QAX-GPT安全机器人系统	公安部网络安全等级保护评估中心
	Innovation Insight for Privileged Access Management in China	奇安信特权账号管理系统(PAM)及配套解决方案	Gartner
	鸿蒙HarmonyOS NEXT技术认证书	奇安信网神Trustspace移动安全管理系统V3.0版本	华为
	世界互联网大会“新光”产品奖	奇安信ASIOC智能网络安全运营	世界互联网大会国际组织
	世界互联网大会领先科技奖	奇安信加密流量高效检测与动态弹性编排关键技术及应用	世界互联网大会国际组织
	2024年度(第八届)中国网络安全与信息产业“金智奖”	奇安信ASIOC智能网络安全运营	信息安全与通信保密杂志社
	先锋产品奖	云原生应用安全保护平台(CNAPP)	信息安全媒体CDM(《网络防御杂志》)
	先锋产品奖	网络资产攻击面管理系统(CAASM)	信息安全媒体CDM(《网络防御杂志》)
2024	2023年网信领域重点支撑单位	奇安信	中关村科创智慧军工产业技术创新战略联盟
	2023年度先进会员单位	奇安信	中国网络安全产业联盟会员大会(CCIA)
	中国网络安全产业联盟技术支持单位	奇安信	中国网络安全产业联盟会员大会(CCIA)
	2023年公安部科学技术奖一等奖	奇安信	公安部
	数据安全研究优秀贡献奖	奇安信	中国计算机行业协会数据安全专业委员会
	2023年度贡献奖	奇安信	中国计算机学会计算机安全专业委员会
	甲级网络安全应急服务支撑单位	奇安信	国家互联网应急中心(CNCERT)
	网络安全优质企业大奖	奇安信	香港警务处
	突出贡献奖	鼎古实验室	华为终端安全
	优异表现奖	奇安信	中国网络安全产业联盟数据安全工作委员会
	优秀技术支撑单位	奇安信	国家信息安全漏洞库
	高质量漏洞优秀贡献单位	奇安信	国家信息安全漏洞库
	漏洞消控优秀贡献单位	奇安信	国家信息安全漏洞库
	高质量通报优秀贡献单位	奇安信	国家信息安全漏洞库
	国家级安全运营二级资质	奇安信	中国信息安全测评中心
	国家信息安全漏洞库核心技术支撑试点单位	奇安信	国家信息安全漏洞库
	国家信息安全漏洞库优秀漏洞管理企业	奇安信	国家信息安全漏洞库
	漏洞信息报送突出贡献单位	奇安信	国家计算机网络应急技术处理协调中心
	2023年度CNVD协作特别贡献单位	奇安信补天平台	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	国家计算机网络应急技术处理协调中心
	协同防御试点“优秀成员单位”	奇安信	国家计算机网络应急技术处理协调中心
	湖南省科学技术进步一等奖,	奇安信	湖南省人民政府
	世界互联网大会杰出贡献奖	奇安信	世界互联网大会国际组织
	北京市“隐形冠军”企业	奇安信	北京市经济和信息化局,北京市工商业联合会
	三星级技术支撑单位	奇安信	网络安全威胁和漏洞信息共享平台
	中国网络安全企业100强第一名	奇安信	安全牛
	中国网安产业竞争力50强	奇安信	中国网络安全产业联盟会员大会(CCIA)

(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

2024年,随着数字化转型的持续深入,网络安全行业站在了前所未有的历史交汇点上。技术革新方兴未艾,政策法规密集落地。从技术趋势方面,DeepSeek的火爆加速了GenAI(生成式人工智能)在各行业的落地普及,尤其在网络安全领域,GenAI(生成式人工智能)重塑了安全防护模式,更催生了智能对抗的新战场。安全防御从合规建设走向以实战化为核心的价值交付,成为行业共识。而量子计算的发展则预示着加密技术将迎来颠覆性变革。此外,国际技术封锁和供应链中断的风险,进一步促使我国加快自主可控技术的研发和应用。

从政策法规来看,《国家数据基础设施建设指引》的出台,《网络数据安全管理条例》的实施,为数字经济安全发展提供了坚实的政策法规基础。同时,“数字中国”战略的深入推进,促使网络安全从单纯技术问题上升至国家安全和经济发展的核心议题。

展望2025年,网络安全产业有望呈现以下几大发展趋势:

1、AI重塑网络攻防对抗,全场景赋能与价值验证将成为发展重点

AI武器化导致黑客攻击愈演愈烈,网络空间“易攻难守”成常态。安全人员已经在使用GenAI(生成式人工智能)进行漏洞挖掘,提高产出和效率,而AI大模型是一把双刃剑,攻击者也可用来侦查和攻击目标系统。AI武器化将使得攻击更快、更容易,手段更多元和隐蔽,进一步加剧攻防不平衡的状况,企业将面临空前严峻的网络安全状况,以AI对抗AI成为必选题。AI将不仅在安全运营领域逐步普及,还将在攻防安全渗透测试、漏洞分析与挖掘、数据安全、代码安全等领域应用,得到进一步深化和价值验证。AI对网安产业的重塑具体将围绕安全运营全流程AI化、AI智能体工具化和数据标准统一化这三个趋势展开。

1)AI全面融入安全运营流程,解放安全团队生产力

国内外安全厂商继续积极探索GenAI(生成式人工智能)在网络安全各领域的应用,其中安全运营场景是目前应用最广泛的领域,如Microsoft Security Copilot、Google SecOps、Paloalto Network Cortex Copilot以及奇安信基于QAX-GPT安全大模型发布的AISOC,通过AI数字员工帮助企业客户实现7*24全天候监控安全告警,对告警进行100%覆盖秒级研判分类,通过Copilot进行辅助调查和自动化处置,将安全告警的响应时间从天和数小时减少到分钟级,极大提升安全运营工作效率,完成以往人力不可能完成的工作。同时AISOC还可以执行原本只有高级安全分析师才能执行的操作,从而帮助他们发现未知和高级威胁,提高安全效能。而对AI时代外部威胁加剧、安全运营效率低下等问题,预计数智化程度较高、业务高度依赖IT系统的政企客户,随着自身安全运营的成熟度提升,且在有明确的效果度量指标时,会加快将AI能力应用到安全运营工作流程中,自动化繁琐的初级任务,让安全团队的精力花在真正的威胁事件上。

2)AI智能体将成为安全运营人员的基础工具

安全厂商为了解决GenAI(生成式人工智能)的准确性、复杂任务及客户环境复杂性等问题,会构建调用安全大模型、RAG和外部工具等各类专有任务的AI智能体,同时开放给客户侧的安全运营人员可以灵活地根据本企业的实际情况制定基于工作流的AI Agent。除了安全运营领域,AI在攻防安全渗透测试、漏洞分析与挖掘、数据安全、代码安全等领域的应用,也将得到进一步深化和价值验证。

3)基于AI的数据访问标准将走向统一化

为了提升AI驱动安全运营的效果,AI能访问到从网络、端点、云和应用中收集的全方位的信息和数据,是AI能提高准确决策及执行任务的关键。为了使客户侧部署的现有安全产品在安全大模型的加持下发挥更好作用,并高效协作做好安全保障,预计未来业内会推动构建基于AI的统一数据访问标准。

2、国家数据基础设施建设加速,全流程动态安全保障或将成为重点

随着《国家数据基础设施建设指引》等出台,构建从底层到应用层的全流程保护体系,成为数据安全建设重点。展望2025年,围绕数据基础设施的安全建设将有望围绕以下四个方面展开:1)为国家数据基础设施打造内生防护能力,筑牢安全底座;2)为国家算力网基础平台提供一体化的安全保障服务能力;3)构建全链条的数据安全动态防护体系,让数据“能看清、能管好、能防住”;4)为数据流通利用构筑安全可信的环境,实现有效保护、合法利用、高效流通。

3、“车路云一体化”微友万亿级市场,数据安全合规建设有望率先展开

“车路云一体化”是智能网联车领域发展和落实新质生产力的重要实践,是未来新型的交通关键基础设施,主要参与方持有交通、地理信息、高精地图、车辆信息以及个人信息等重要数据,涉及智慧出行乘用车、智慧公交、智慧环卫、智慧物流等八大业务场景,一旦遭受网络攻击和数据泄露,势必带来交通秩序和公共安全事件。因此,保障数据安全合规,给“车路云一体化”提前系好“安全带”,是行业稳健发展的前提。展望2025年,“车路云一体化”数据安全建设将有望围绕以下层面率先开展:1)构建纵深防御的内生安全体系,确保基础架构安全;2)建立全链条的数据安全防护体系,确保各环节数据流转安全合规;3)建设车路云一体化安全运营管理中心,确保全局联防联控。

4、终端安全融合加速,一体化办公空间安全平台或成为趋势

展望2025年,终端安全会继续向着一体化办公空间安全平台演进,并成为越来越多企业客户的战略选择。一体化办公空间安全平台将有望呈现以下三个突出特点:1)终端安全产品将精简,成为用户侧统