公司代码：688030　　公司简称：山石网科

山石网科通信技术股份有限公司

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 www.sse.com.cn 网站仔细阅读年度报告全文。

2 重大风险提示

公司已在本报告中详细说明公司在经营过程中可能面临的各种风险，敬请查阅本报告第三节“管理层讨论与分析”。

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

经公司第二届董事会第二十四次会议决议，截至2023年12月31日，母公司期末可供分配利润为-84,021,930.49元，根据《关于进一步落实上市公司现金分红有关事项的通知》《上市公司监管指引第3号——上市公司现金分红》《山石网科通信技术股份有限公司章程》等相关规定，不满足利润分配条件，综合考虑公司未来经营计划和资金需求，公司2023年度拟不进行利润分配，也不进行资本公积转增股本和其他形式的分配。

上述利润分配方案需经公司2023年年度股东大会审议通过后实施。

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	山石网科	688030	无

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	唐琰	何远涛
办公地址	苏州高新区景润路181号	苏州高新区景润路181号
电话	0512-66806591	0512-66806591
电子信箱	ir@hillstonenet.com	ir@hillstonenet.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

公司主营业务聚焦网络安全领域，围绕公司提出的“可持续安全 2.0”理念，公司明确了四大业务场景，分别为：安全连接、安全计算、安全数据、安全运营；目前公司的业务线已涵盖边界安全、云安全、应用安全、数据安全、工业互联网安全、安全运营、安全服务、安全教育在内的 8 大类产品和服务，并已形成数十种行业和场景的解决方案。

1、公司主要业务及产品

2、报告期内公司主要业务及产品进展情况

（1）边界安全

边界安全是网络安全中不可或缺的能力，无论未来网络边界如何发展，企业始终需要边界安全对自身业务进行安全防护。山石网科的边界安全解决方案主要包括智能下一代防火墙、数据中心防火墙、入侵检测和防御系统等产品。

作为公司的传统强项产品，公司持续巩固并提升在该细分领域的竞争优势。报告期内，公司边界安全产品线的主要进展如下：

1）基于新一代硬件平台，持续研发并推出了多款 A 系列智能下一代防火墙，可覆盖不同规模企业需求，包括 3 款 25G-40G 档位防火墙，满足中大型企业网络层吞吐需求；5 款 2U 形态防火墙，配备 2U Bypass 插卡后，可保障安全组网的稳定与可靠性；4 款 10G-20G 档位防火墙，满足中小型企业安全组网建设需求；3 款 2G-6G 档位防火墙，满足微小型企业、连锁机构和微小营业网点等场景的网络安全需求。

2）面向运营商 5G、云数据中心等大流量应用场景，公司发布了数款高性能分布式防火墙，整机吞吐量覆盖 600Gbps~3.5Tbps，以极强的高稳定和高可靠性，巩固公司数据中心防火墙在运营商、大型集团集采入围的竞争力。

3）公司 Stone OS 软件平台持续更新，陆续发布了 Stone OS 5.5R10 系列等 8 个版本，新增共计 16 项功能，大幅增强了产品在系统、监控、认证、威胁防护、访问控制等方面的能力，持续提升产品的易用性和稳定性。

4）公司 IDPS 产品软件平台持续迭代，先后进行了 3 个主线版本的迭代，推出 2 款国产化 IPS 产品和 3 款国产化 IDS 产品，持续增强 IDPS 安全防护能力。

5）公司持续布局信创市场，新增推出 2 款基于国产关键元器件的国产化防火墙产品，国产化防火墙系列实现覆盖 2Gbps~100Gbps 档位，同时，发布多款基于国产关键元器件的入侵检测和防御系统，进一步丰富边界安全产品的档位。

报告期内，公司边界安全产品及服务实现收入 66,247.53 万元，同比增长 9.46%。

（2）云安全领域

公司致力于开发云计算安全原子能力、云工作负载防护平台、云安全管理平台、主机安全防护平台等，为用户提供全面的云计算安全解决方案。这些解决方案可以覆盖私有云、公有云、多云、混合云等不同场景，并支持物理服务器、虚拟机、容器等工作负载。通过这些解决方案，为用户构建安全可靠的计算环境，从而保障其业务在云计算环境中的安全。

报告期内，公司在云安全业务线的主要进展如下：

山石云·界（Cloud Edge）基于自研 Stone OS 软件平台，围绕合作云厂商的需求持续迭代，增加了在不同云平台的云原生适配能力，且可在云平台上实现云原生集成融合。

山石云·格（Cloud Hive）主要应用于云内东西向之间的安全防护，具备较高的云平台适配能力，公司正在积极拓展与更多厂商的合作，共同打造更加智能、灵活、高效的微隔离产品。

山石云铠（Cloud Armour）主机安全防护平台发布全新版本，以用户日常运营管理为基点，完善资产管理功能、增强威胁检测能力、提升微隔离适用性、新增对外 API 联动能力，为用户提供场景丰富、检测精准、能力开放、功能易用的主机安全防护平台。

山石云·池（Cloud Pool）致力于为云租户提供等保安全解决方案，不断加强安全网元的完善

和升级，以满足不同行业和场景的安全需求。公司积极推动与行业客户的深入合作，根据不同行业的特点和需求，提供定制化的行业解决方案，助力客户实现数字化转型和升级。

报告期内，公司云安全产品及服务实现收入 6,229.12 万元，同比增长 26.22%。

（3）其他安全领域

I.安全运营

报告期内，山石网科以“扩展”为核心理念，进一步优化安全运营产品，并将“多场景”融合其中，更好地满足业务需求。

报告期内，山石智源安全运营平台新增发布三个版本，可实现威胁事件的多视角智能聚合，有利于加强终端安全联动能力，优化安全运营的闭环过程；进一步整合与山石网科威胁探针以及山石网科防火墙的数据通道，提升信息流的安全性；新增重保工作台、勒索/挖矿/弱密码等安全治理专项，适配特定安全场景需求；完成标准对外 API 接口，强化安全运营开放性；发布首个国产化山石智源安全运营平台，满足国产化市场安全需求。同时，整体功能在组件管理、联动响应、资产管理、安全场景等方面实现了较大提升。

报告期内，山石网科还发布了国产化安全管理平台 HSM-P500-GC，更好地满足政府机关及企事业单位、金融、电信等行业对国产化安全管理平台的市场需求。同期发布了 HSM V5.5.0 版本平台软件，新增更多运维功能，满足行业用户的安全运维需求。

II.端点安全

报告期内，山石智铠统一终端安全管理系统发布了 v5.0R4 版本，适配主流国产操作系统，满足市场对国产化的需求；强化了威胁检测能力：包括新增违规外联检查、弱密码检测、勒索专项防护等功能。

III.数据安全

山石网科持续强化数据安全治理能力，为企业数字化转型升级保驾护航。报告期内，公司数据安全业务线主要进展如下：

1）发布了数据库运维安全防护网关系统和数据库动态脱敏系统，不断完善围绕数据全生命周期的技术解决能力。

2）发布了国产化数据安全综合治理平台、国产化数据库审计与防护系统、国产化数据泄露防护系统、国产化静态数据脱敏系统，均采用基于国产处理器和操作系统的自主可控硬件，可为政府、金融、企业、医疗、教育等行业用户构筑安全可靠的数据防护体系。

3）对数据安全综合治理平台进行了迭代更新，延展对数据源资产管理的类型，增加基于行级数据标记的梳理能力，合规检查、状态监控等可视化能力的扩充也为数据安全运营提供了便利。

4）对数据泄露防护系统架构及性能、功能进行了升级，推出了“网络监控、网络保护、终端保护、数据发现”四大模块，同时对产品硬件款型进行了迭代。

5）推出了应用（API）系统安全审计平台两款虚拟版型号，以扩充完善 API 审计适配场景，提升产品的性能，进而满足企业客户业务云化递增的需求。

6）推出了数据安全治理专家服务，通过数据安全管理制度咨询规划服务、数据分类分级服务、数据安全风险评估服务、数据安全培训服务等专业的数据安全服务，护航数据安全治理项目全过程，全方位保障企业关键业务数据的安全及可靠性。

7）在政府、医疗、教育、企业等多个领域赢得数据安全标杆项目，尤其是在数据安全分类分级、数据安全风险评估等数据安全治理领域的实践；同时展开与国内科研院所的合作交流，共同探索数据安全领域前沿技术。

IV.应用安全

应用安全是应用的交付和守护者，同时也是公司重点打造的产品线之一。

（1）应用交付

报告期内，公司应用交付产品新增 6 款硬件平台，其中 4 款基于国产芯片，进一步完善国产化产品布局。同时在功能上完成了 4 个主线版本的迭代，结合行业用户的需求进一步完善产品功能适配。

（2）WAF

报告期内，Web 应用防火墙在国产化方面继续规划新增 3 款国产芯片硬件平台，覆盖了 5G~15G 的范围，进一步完善国产化产品布局。

（3）内网安全

报告期内，山石智•感智能内网威胁感知系统新增发布了 2 个版本，基于 R10 合入 WAF 新引擎，进一步增强了威胁检测能力；包括加密流量检测、明文密码检测和远控工具风险检测；同时，在产品易用性和威胁取证能力方面做了一定提升，通过 ATT&CK（对抗战术、技术和常识）框架映射为用户提供了更详实的威胁信息，丰富了全流量检测结果的详细证据内容，为用户提供易用的威胁事件调查体验。

V.安全服务

2023 年，山石网科安全服务团队持续提升专业服务水平，尤其在数据安全服务领域取得较为明显进步。团队始终坚持“产品+服务”，不断提升服务交付能力，拓展服务交付范围，以满足客户多元的安全需求。目前，公司的安全服务包括了安全评估、应急保障、安全通告、安全培训、威胁检测订阅、欺骗诱捕、安全咨询等服务类型。

2023 年，山石网科获得中国通信企业协会通信网络安全服务能力评定证书并通过 CCRC 信息系统风险评估、信息安全应急处理、信息系统安全运维、信息系统安全集成四大领域最高级安全服务年度监督审核认证，公司的安全服务管理能力、安全服务技术能力、安全服务过程能力得到国家权威机构认定。

报告期内，公司不仅提供了全方位的网络、数据安全服务和综合解决方案，还积极参与全国各地区的网络安全建设，提供了可靠的网络安全支撑保障工作，全年共计荣获相关保障单位 20 余封感谢信。同时，凭借扎实的技术水平、优秀的服务态度，山石网科在各省市多次受到表彰，荣获江苏省、辽宁省、河南省、苏州市等多地、多行业网络安全技术支撑单位。

此外，Gartner 发布的《Hype Cycle for Security in China, 2023》报告中，山石网科在攻防对抗等五项技术领域被列为代表厂商（Sample Vendors），展示出了山石网科在攻防对抗等方向的高技术水平和强防护能力。山石网科的实战攻防体系有效结合客户业务环境和场景，通过攻防对抗识别可利用风险点以及流程阻塞点，构建组织“知攻善守”的安全能力，建设合理、有效的主动防御体系，赢得了业界的高度认可，并成为山石网科在攻防对抗领域的代表性成果。

VI.综合实训平台

报告期内，公司完成教学培训服务、实训平台、竞赛平台、攻防演练平台四大类产品，秉承以实战为导向，按照“成体系、全覆盖、可通用、易扩展”的指导思想，对产品进行了全面迭代升级与资源整合；同时新增了靶场测评与活体漏洞功能，为系统加固、工具研制、技术研究、战

术推演、实战对抗创造先决条件。此外，针对网络安全细分领域，例如工控安全领域、数据安全领域、信创领域、能源电力领域用户提供一站式且可定制化的解决方案，并打造了工控安全数字化靶场、数据安全数字化靶场等案例。

VII.工业互联网安全

工业互联网安全是数字经济高质量发展的重要保障。目前，公司融合先进技术的安全生产可信环境理念，发布了“Trust-E”工业互联网安全解决方案，在满足客户“等保”、“关保”、行业规范等合规需求下，形成的一套涵盖工业互联网边缘层、控制层、应用层与平台层的整体解决方案。报告期内，公司发布了工业防火墙 4 款型号、工业安全主机卫士系列、工业主机白名单软件等多项工业互联网安全产品，逐步构建出完善的工业安全产品布局。

报告期内，公司其他安全类产品及服务实现收入 16,589.82 万元，同比增长 23.43%。

(二) 主要经营模式

1、销售模式

报告期内，公司采用直销和渠道代理销售相结合的模式，并以渠道代理为主。

（1）直销模式

基于部分电信运营商、金融机构及大型企业对于采购成本、服务质量的严苛要求，公司对此类重要客户主要采取直销模式，便于公司安排专业销售及技术人员为客户提供更好的服务。此外，公司以直接供应商身份参与国家重点行业集中采购并入围集中采购名录，是对公司技术、实力的一项重要认可，有利于打造公司品牌形象。

公司通过参与招投标、邀标谈判的方式获取直销客户。直销模式下，公司严格履行客户的招投标程序，公司定价以市场竞争为原则，根据客户对产品性能需求、预算和市场竞争情况确定投标价格和谈判的报价。一般情况下，公司根据直销客户招投标或邀标的要求、客户合同模板约定、客户内部建设项目竣工验收安排等因素确定信用期，通过电汇、银承、商承结算。

（2）渠道代理模式

报告期内，公司渠道代理商分为总代理商、白金和金牌、认证代理商。其中，总代理商可以直接向公司进行采购。一般情况下，白金、金牌、认证代理商直接与总代理商签订订单合同，并通过总代理商下单提货。

报告期内，公司采用直销和渠道代理销售相结合并以渠道代理为主的销售模式，降低了企业的资金风险，加大了对终端用户的覆盖面，公司将延续现有的经营模式，并不断加强渠道建设工作。

2、采购模式

公司物料采购可以分为生产性物料采购和非生产性物料采购，其中生产性物料包括委托加工类和直采类。公司采购的主要物料包括自主研发的硬件平台（委托加工模式）、工控机、服务器、硬盘、电源、光模块、包装材料等。公司拥有独立的供应链体系，物料采购主要由采购部门执行，工程部、计划部、质量部、仓储部等进行必要协助，确保采购的产品和服务持续满足公司客户的要求，并通过持续稳定的供应链体系支持公司整个业务发展的需求。

3、生产模式

公司主要销售的网络安全硬件设备和软件由公司自主研发设计，经过严格缜密的组装灌装，并最终交付给客户。公司硬件设备主要采取代工模式生产，产品全部在公司认证的专线完成电子线路板生产，统一经过严苛的设备组装、生产测试、预装软件、烤机、检测包装等环节。部分产品下线后安装公司自主研发安全软件并由公司质量部门进行检验，检验通过后采取直运模式交付给终端客户或渠道代理商。同时，为满足不同重要客户的需求，公司少量产品由代工厂组装后交付至公司质量部门检验，检验通过后交付给公司自有车间进行定制生产，保证了该部分产品的特殊性及保密性。

公司产品主要采取标准化生产模式，根据不同部署场景及性能需求，公司提供多种性能层级的标准化的安全解决方案。

4、研发模式

公司的产品研发设计，以技术创新为导向，将客户需求及反馈融入到产品规划、设计、研发和服务的全过程中，研发工作通过“规划—设计—交付—反馈—升级”的良性循环，不断加强产品能力并提升用户体验。

公司的产品研发采用矩阵模式进行，除产品研发团队外，市场部、销售部、运营部也有指定资源全程参与，从而保证产品在设计研发的所有阶段，可以充分考虑市场需求和客户反馈。产品在交付后，确保可以迅速实现大规模生产和销售。

公司的研发部门主要由苏州、北京、美国硅谷三地研发团队构成。研发阶段主要分为需求阶段、设计阶段、开发阶段及测试阶段 4 个阶段。随着公司产品品类的不断丰富和市场变化逐渐加快，公司在瀑布式开发模式的基础上，引入了敏捷开发模式，针对不同特点的产品采用不同的开发方式。

报告期内，公司主要经营模式未发生重大变化。

(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

2023 年度，全球网络安全市场供需两侧格局基本稳定，随着数字化转型的加速和信息技术的广泛应用，全球网络安全仍然表现出持续、稳定的市场需求。从云安全、数据安全到人工智能的应用，前沿技术为网络安全领域注入了新的活力，从长期来看，网络安全产业仍处于较好的发展周期。

2023 年度，在国际环境日趋复杂、宏观经济波动和产业需求调整的背景下，国内网络安全市场虽然较上年有所回暖，但仍然表现出增速放缓的趋势。近年来网络安全生态日益扩展，除传统的综合网络安全厂商外，运营商、IT 厂商、集成商纷纷投入网络安全业务板块，带动了网络安全业务板块的繁荣，拓宽了网络安全厂商的生态渠道，但同时也进一步加剧了国内网络安全市场的竞争态势。

整体上，目前因宏观财政压力，部分政企客户的数字化建设的节奏有所放缓，对国内网络安全产品的需求存在短期调整，整体安全产业发展面临压力，但同时，结合国内市场的多项表现，我们仍然可以看到国内在部分行业、部分细分市场仍然存在稳定的、强劲的市场需求，足以支撑网络安全行业的短期发展，并提供了充足的发展潜力。根据 IDC《2023 年第二季度中国 IT 安全硬件市场跟踪》报告显示，2023 年上半年中国 IT 安全硬件市场规模达到 75 亿元人民币，其中基于 UTM 平台的防火墙是最大的品类，占比近 35.7%。根据 IDC《全球网络安全支出指南》（IDC Worldwide Security Spending Guide）2024 年 V1 版预测，面对更加复杂的网络威胁环境和不断提高的合规要求，统一威胁管理（Unified Threat Management）市场份额将持续上升，以 7.5%的五年复合增长率成为硬件最大子市场。

除防火墙外，数据安全、安全运营及服务等新兴市场，随着近年来市场的培育孵化，已逐步展现出更高的市场增速和更多的市场潜力。

随着《中华人民共和国网络安全法》《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》相继施行，数据安全上升为国家安全重要组成部分。2023 年 1 月，工业和信息化部与国家互联网信息办公室等十六部门印发《关于促进数据安全产业发展的指导意见》提出“到 2025 年，数据安全产业规模超过 1,500 亿元，年复合增长率超过 30%”的目标，数据安全已成为网络安全市场新的增长点。从发展阶段看，数据安全市场从“等保”驱动向“合法”驱动，未来可能逐步向“交易/交换价值”驱动发展。基于此，数据安全类产品和服务也随之逐步演变，数据安全治理需要网络安全厂商具备顶层的设计和服务能力。公司已提出“数据安全治理白皮书”等数据安全治理理念，并先后发布了“数据安全综合治理平台”等多类数据安全产品，在 Gartner 发布的《2023 中国安全技术成熟度曲线》报告，公司在数据安全平台等五项技术领域被列为代表厂商（Sample Vendors）。公司的企业数据安全治理解决方案凭借持续的创新能力和优质的方案，荣获由信息安全与通信保密杂志社主办的 2022-2023 年度中国网络安全与信息产业金智奖以及“年度优秀解决方案奖”。

根据 IDC《2023 上半年中国 IT 安全服务市场预测报告》，中国安全服务市场未来五年将保持稳定增长的态势，2027 年服务支出规模预计达 472 亿元，五年复合增长率约为 17.9%。其中，安全运营及服务的重要性更为明显。目前看，多数企业已完成合规建设，基础安全体系搭建完成，未来将进入深耕细作、建设与运营并重的新阶段。企业安全运营需求的快速释放也推动了安全运营市场蓬勃发展。

除数据安全、安全运营及服务等新兴细分需求展现出的快速增长趋势外，国内市场因信创发展带来的需求更为明显。信创趋势已经从“全面”转向“深化”的新阶段，信创应用正在从党政领域向全领域转化，预计未来几年，关键信息基础设施领域如金融、电信、电力领域将保持加速推进信创的趋势。尽管短期来看，信创市场亦受到了宏观环境的经济压力，但从中长期看，信创市场将迎来高速发展阶段。同时，针对信创市场，我们认为，技术仍是第一生产力，公司将把握这一轮信创市场的机会，同时借助如金融、运营商等行业的良好客情关系和市场基础，加速对信创的投入，以期在未来获得良好的增长。

整体上，短期的宏观经济波动和产业调整没有在实质层面影响到网络安全行业的长期发展节奏，国内网络安全市场仍然保持发展态势和乐观前景，安全产品与服务需要符合关键业务场景和生产网络，关键行业、信创市场、数据安全、安全运营及服务等细分赛道成为网络安全厂商的竞争主战场，网络安全厂商需要更深的技术沉淀和对客户需求的理解，进而具备符合网络安全市场发展趋势的综合能力。

2. 公司所处的行业地位分析及其变化情况

作为网络安全领域的技术创新领导厂商，截至报告期末，山石网科已累计服务超过 28,000 家用户，广泛获得了金融、政府、运营商、互联网、教育、医疗卫生、能源、交通等行业用户的认可。

根据 2023 年 5 月 IDC 发布的《IDC Technology Assessment：中国统一威胁管理硬件技术评估，2023》报告，山石网科凭借优秀的技术实力成功入选为 UTM 代表厂商之一。

根据 2023 年 6 月 IDC 发布的《IDC Technology Assessment：中国零信任网络访问解决方案技术评估，2023》报告，山石网科凭借优秀的技术实力成功入选为零信任代表厂商之一。

2023 年 10 月，IDC 发布《IDC MarketScape：中国数据安全管理平台 2023 年厂商评估》报告，山石网科作为典型代表入选报告，位于 Major Players 象限。

根据 IDC 数据，2016 年-2023 年，公司在中国“统一威胁管理 UTM”市场厂商市场规模中排名第 4（数据来源：IDC《2023 年第四季度中国 IT 安全硬件市场跟踪报告》）。

2023 年，公司连续第二年进入 Gartner®《中国安全技术成熟度曲线报告》，在五大项技术领域被评为代表厂商。

2023 年，公司下一代防火墙系列产品再次进入 Gartner®《Peer Insights™ “Voice of the Customer” for Network Firewalls 报告》获得“客户之选”称号，是全球仅有的两家、国内唯一一家连续四年获此称号的厂商；并入选 Frost & Sullivan《Frost Radar 2023“下一代防火墙”研究报告》，被评为“创新与增长领导者”。

2023 年，公司云工作负载防护平台山石云铠入选 Gartner《新兴技术：云工作负载保护平台的采用增长洞察报告》，并成为工作负载运行时可视化领域推荐厂商。

2023 年，公司山石智•感智能内网威胁感知系统首次进入 Gartner®《Peer Insights™ “Voice of the Customer” for Network Detection and Response》报告并荣获“强劲表现者”称号，并入选 Gartner《新兴技术：网络检测和响应的采用增长洞察报告》与《新兴技术：网络检测和响应的热门用例报告》。山石智•源智能安全运营平台入选 Frost&Sullivan《Frost Radar 2023 XDR 研究报告》，被评为“创新与增长领导者”，是唯一入选的中国厂商。

2023 年，公司零信任访问解决方案入选 Forrester《2023 年 Q4 安全服务边缘解决方案前景报

告》及《零信任资源指南》报告。

报告期内，公司所处行业地位未发生重大变化。

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

众所周知，报告期内 AI 已逐步成为信息技术发展的新高度，人工智能在算法、算力、数据等方面取得重要突破。AI 的发展带来潜在的巨大安全需求和产品与技术的创新空间，微软、PaloAlto、Crowdstrike 等国际大厂的生成式 AI 应用进入生产力生成阶段，广泛应用于其产品和平台中，改变产品形态和功能，提升能力和效率。

基于国内网络安全行业的格局及投入产出的考量，IDC 认为，对于网络安全专业厂商而言，更适合采用“模型+安全能力“的方式将 AI 融入安全产品及服务之中，即安全厂商将自身积累的安全领域数据与通用大模型相结合，进行模型的再次学习和微调，从而可生成安全垂直领域大模型。山石网科作为国内网络安全行业的技术创新型厂商，也已经计划在未来逐步把 AI 能力加入公司产品，实现产品能力、研发效率和竞争力的提升。

根据赛迪顾问发布的《中国工控安全市场研究报告（2023）》，2022 年中国工控安全市场规模为 58.5 亿元，增长率为 39.0%。从行业结构来看，目前能源电力、石油石化、烟草、轨道交通行业占中国工控安全市场 70%以上；从产品结构来看，中国工控安全市场中占比较高的依然是工控防火墙、工控安全审计及工控安全管理平台。随着国家工控安全市场的不断拓展，以及相关行业标准与政策的不断推进与落地，预计未来三年，中国工控安全市场仍将保持稳步高速增长，2025 年，市场规模可能将达到 151.4 亿元，三年复合增长率达 37.3%。

此外，如前文所述，数据安全和安全运营服务市场持续保持较高热度，2023 年是数据要素发展和数据安全完成顶层规划设计目标的一年，2024 年起将全面进入落地行动阶段。从目前公司内部的行业观察来看，数据安全市场未来规模较大，最近三年复合增速达 20%以上，具备较高增长潜力；安全运营及服务市场也得到了进一步的深化，安全厂商需要具备更强的安全运营能力、产品与服务的顶层方案设计能力，以满足日益发展的客户需求，并通过各项工具的使用，提高安全运营的自动化程度，以提高效率和降低成本。

综合来看，边界安全、云安全、安全运营及服务、态势感知等产品依然为安全市场的刚需，信创、数据安全治理、工业互联网安全等赛道持续成为市场热点，可能成为未来国内网络安全行业新的高速增长点。

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	1,852,071,698.16	2,116,178,696.15	2,116,062,712.28	-12.48	1,943,537,512.75
归属于上市公司股东的净资产	1,078,942,643.90	1,318,436,178.88	1,318,320,726.39	-18.16	1,507,258,047.57
营业收入	901,040,067.77	811,596,110.98	811,596,110.98	11.02	1,026,948,139.06
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	890,664,719.34	788,989,387.72	788,989,387.72	12.89	1,017,651,048.00
归属于上市公司股东的净利润	-239,811,522.01	-182,475,634.35	-182,502,253.08	不适用	75,526,102.89
归属于上市公司股东的扣除非经常性损益的净利润	-248,593,008.86	-205,530,649.81	-205,557,268.54	不适用	54,057,654.59
经营活动产生的现金流量净额	-58,254,382.32	-332,312,564.78	-332,312,564.78	不适用	-119,053,386.79
加权平均净资产收益率（%）	-20.01	-12.91	-12.92	减少7.10个百分点	5.16
基本每股收益（元／股）	-1.3306	-1.0125	-1.0126	不适用	0.4191
稀释每股收益（元／股）	-1.3306	-1.0125	-1.0126	不适用	0.4184
研发投入占营业收入的比例（%）	41.58	41.81	41.81	减少0.23个百分点	29.14

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	144,591,323.56	228,669,721.61	327,008,716.92	200,770,305.68
归属于上市公司股东的净利润	-87,456,433.30	-24,928,489.12	-60,625,786.19	-66,800,813.40
归属于上市公司股东的扣除非经常性损益后的净利润	-91,925,784.51	-25,754,062.60	-62,063,103.02	-68,850,058.73
经营活动产生的现金流量净额	-12,628,095.53	35,418,838.94	-140,470,364.77	59,425,239.04

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)	8,035
年度报告披露日前上一月末的普通股股东总数(户)	7,596
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	
神州云科（北京）科技有限公司	21,537,000	21,537,000	11.95	0	0	无	0	境内非国有法人
三六零数字安全科技集团有限公司	0	12,604,505	6.99	0	0	无	0	境内非国有法人

国创开元股权投资基金（有限合伙）	0	11,859,118	6.58	0	0	无	0	境内非国有法人
田涛	-1,800,000	11,603,662	6.44	0	0	无	0	境外自然人
宜兴光控投资有限公司	0	10,964,397	6.08	0	0	无	0	境内非国有法人
苏州工业园区元禾重元并购股权投资基金合伙企业（有限合伙）	-2,688,940	10,460,831	5.80	0	0	无	0	境内非国有法人
越超高科技有限公司	-21,537,000	8,985,850	4.99	0	0	无	0	境外法人
北京奇虎科技有限公司	0	5,406,698	3.00	0	0	无	0	境内非国有法人
卞伟	0	4,414,568	2.45	0	0	无	0	境内自然人
LUO DONGPING	-495,483	4,329,835	2.40	0	0	无	0	境外自然人
上述股东关联关系或一致行动的说明				1、苏州元禾控股股份有限公司为苏州工业园区元禾重元并购股权投资基金合伙企业（有限合伙）的有限合伙人（出资比例为33%），同时苏州元禾控股股份有限公司亦为国创开元股权投资基金（有限合伙）的有限合伙人（出资比例为 10%）。2、三六零数字安全科技集团有限公司和北京奇虎科技有限公司均为三六零安全科技股份有限公司全资子公司，属于受同一主体控制，根据《上市公司收购管理办法》第八十三条的规定，三六零数字安全科技集团有限公司和北京奇虎科技有限公司之间构成一致行动关系。除上述说明外，公司未接到上述股东有存在关联关系或一致行动协议的说明。				
表决权恢复的优先股股东及持股数量的说明				不适用				

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，公司实现营业收入 90,104.01 万元，较去年同期增长 11.02%；实现归属于上市公司股东的净利润-23,981.15 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-24,859.30 万元，较去年同期亏损扩大 31.42%和 20.95%。

报告期内，公司边界安全业务收入为人民币 66,247.53 万元，同比增长 9.46%，占公司主营业务收入比重 74.38%；

报告期内，公司云安全业务收入为人民币 6,229.12 万元，同比增长 26.22%，占公司主营业务收入比重 6.99%；

报告期内，公司其他安全业务收入为人民币 16,589.82 万元，同比增长 23.43%，占公司主营业务收入比重 18.63%。

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