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

2024 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

经公司第三届董事会第二次会议决议，截至2024年12月31日，母公司期末可供分配利润为-184,112,001.18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2024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2024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

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	山石网科	688030	无

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	唐琰	何远涛
联系地址	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
传真	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

2.1 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，基于以安全服务为核心，安全连接、安全计算、安全数据、安全运营为支撑的“一中心四基石”架构体系，公司业务线已涵盖边界安全、云安全、数据安全、应用安全、安全运营、工业互联网安全、安全服务、安全教育、信息技术应用创新等 9 大类产品及服务。2024 年，公司正式发布“开放融合、AI 赋能、智慧运维”下一代安全理念，着力构建行业协同创新生态，驱动安全运营效能系统性提升。

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

作为网络安全体系的关键防线，边界安全的重要性不言而喻。2024 年，山石网科在边界安全领域持续发力，进一步完善边界安全产品矩阵。报告期内，公司边界安全产品线的主要进展如下：

1）持续布局信创市场；新增发布信创分布式防火墙 K20803，盒式信创防火墙 K7680、K7280 和 K6680，依托 Hillstone Mars（FPGA 芯片）硬件加速引擎，以低时延和高性能的产品特性，强化了公司在高端信创防火墙市场的竞争力。同时，公司陆续发布了多款 K 系列中低端信创防火墙，为中小流量边界防护场景提供更多信创款型选择。

2）Stone OS 自研软件持续更新；陆续发布 Stone OS 5.5R11 系列等 27 个版本，新增并优化了多项功能，增强产品在威胁检测、策略运维、访问控制、零信任接入方案、IoT 安全防护方案等多方面的能力，持续提升产品的易用性。同时基于 LLM 大模型能力，发布面向用户的防火墙 AI 运维助手，为用户提供了智慧运维解决方案。

3）IDPS 产品持续创新升级；完成 3 大主线版本的迭代开发，推出 6 款标准化 IDPS 新型号产品，全面覆盖中小型企业的性能需求。新增 20 余项核心功能，在威胁检测精度、响应速度、防

护维度等方面均有所提升，进一步增强了产品的市场竞争力。

报告期内，边界安全业务线实现营业收入 74,833.80 万元，同比增长 12.96%，占主营业务收入比例 75.76%。

（2）云安全领域

公司深耕云计算安全领域的核心技术研发，聚焦打造云安全原子级防护能力、构建云工作负载全方位防护平台、优化云安全管理平台及强化主机安全防护体系，旨在为用户量身定制全面的云计算安全产品和方案。目前，公司云安全产品广泛兼容私有云、公有云、多云环境及混合云架构，无缝对接物理服务器、虚拟机、容器等多种工作负载形态，确保用户无论在任何云场景下，都能享受全方位的云安全防护。

报告期内，公司在云安全领域的核心业务取得了进展，协助客户在数字化转型的趋势中稳健前行。主要进展如下：

1）山石云·界（Cloud Edge）携手天翼、华为、中兴等五大核心伙伴深度合作，全年成功迭代 11 个版本，新增 200 多个功能项，从路由、网络、威胁防护、HA 等多个方面对产品能力进行强化，不断提升产品的稳定性和易用性，筑起稳固的云端防线。

2）山石云·格（Cloud Hive）主要应用于云内东西向之间的安全防护，通过不断聚焦项目实战打磨，已具备较成熟的云平台适配能力，能精准贴合多元业务场景，致力于打造智能、灵活、高效的网络微隔离产品。

3）山石云铠（Cloud Armour）主机安全防护平台发布 R4 版本，适配主流国产操作系统，满足市场对国产化主机安全场景的需求。同时，大幅增强了威胁检测能力，增加了多个维度的检测规则；并引入 CNAPP（Cloud Native Application Protection Platform）理念，强化了云原生应用的安全防护能力；此外，还优化了微隔离功能，实现了微隔离的便捷、平滑上线；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。

4）山石云·池（Cloud Pool）致力于为云租户提供等保安全解决方案，不断完善安全网元种类，升级安全网元功能；并积极与更多云平台厂商适配，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，公司云安全业务线实现营业收入 5,075.33 万元，同比下降 18.52%，占主营业务收入比例 5.14%。

（3）其他安全领域

I.安全运营

山石网科 Open XDR 可持续安全运营秉持“开放融合，AI 赋能，智慧运维”的理念，以山石智源智能安全运营平台为核心，与 NGFW、NDR、EDR、CWPP 等安全设备深度联动，通过大数据处理分类、智能关联分析并自动化协同处置响应，强化威胁检测能力、还原完整攻击过程、智能研判攻击结果、及时响应闭环，最终形成一体化的安全运营能力，帮助用户更高效的检测、分类、调查、研判和处置威胁，并将“多场景”融合其中，更好地满足业务需求。

报告期内，山石网科 Open XDR 平台山石智源发布了 2 个主线版本，引入“资产域”功能，构建分支机构等场景下"分权分域"管理能力；通过灵活的配置和可扩展架构，支持多种数据源、各类第三方设备数据的无缝接入，为用户提供一个全面开放的数据管理方案；推出案件调查功能，通过收集、分析和评估全域安全数据，以确定事件的性质、原因、影响范围和攻击者身份，进而构建起完整的攻击链，自动分析实体与实体之间的关联关系，梳理出一次攻击的完整故事，方便用户溯源与研判；引入 AI 大模型，对威胁事件的攻击报文、日志、PCAP 证据报文以及案件现状进行精准解读，有效降低安全运营复杂度，提高安全运营效率。

报告期内，山石网科安全管理平台（HSM）完成了 2 大主线版本的迭代开发，支持 Web 应用防火墙（WAF）集中纳管场景；支持等保设备集中纳管场景；支持工业安全纳管场景；支持特征库服务器场景。设备纳管能力进一步提升，助力企业实现安全设备高效运维。除此之外还优化了设备运维管理和 SD-WAN 管理功能，更好地满足行业用户的安全运维需求，提升用户体验。

报告期内，山石网科云端安全运维管理平台（云景）新增威胁分析服务，专注于解决挖矿、勒索、漏洞利用、木马及 APT 活动等企业安全挑战，实现云端辅助威胁分析，依托云端专家分析能力，确保专业安全报告的及时生成，有效弥补企业安全能力短板。

II.端点安全

报告期内，公司发布山石智铠统一终端安全管理系统 v5.0R5 版本，通过“实施零信任网络访问（ZTNA）+建设端点保护平台（EPP）+采用端点检测和响应（EDR）技术+终端数据泄露防护（DLP）”四重防护策略，实现全面、高效的终端安全保障。

III.数据安全

山石网科持续升级数据安全治理能力，为企业数字化转型稳健前行提供坚实保障。报告期内，公司数据安全业务线主要进展如下：

1）发布了《山石网科数据安全治理白皮书 3.0》，旨在全面解析从“框架模型”至“具体实践”的数据安全治理体系链条，助力处于不同数据安全建设阶段的企业用户深入理解并有效实施数据安全治理。

2）在数据安全治理专家服务方面，由四项扩充为九项，新增了数据安全咨询规划服务、数据安全驻场运营服务、数据安全资产梳理服务、数据跨境安全评估服务、数据安全专项定制化服务，进一步为企业的核心业务数据提供全方位的保护与可靠性保障。

3）继续深入医疗行业数据安全产业应用探索，联合华中科技大学同济医学院附属协和医院参与 CHIMA 2024 数据安全与治理分论坛，就如何借助新技术、新模式，推动医院数据安全治理工作展开深入且富有前瞻性的讨论，共话数据安全治理解决之道。

4）推出“医石无忧——一站式安全服务免费体检”活动，旨在助力医疗机构构建更加稳固的数据安全屏障。

5）推出国产化数据综合治理平台 DSGP，该平台作为数据安全治理的神经中枢，以数据安全治理七步法为规划内核，为用户提供面向数据全生命周期及业务场景的数据安全治理解决方案。

6）推出轻量化低成本分类分级与风险评估平台，聚焦分类分级和风险评估，满足客户在预算有限情况下的迎检合规需求。

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

山石网科持续布局高性能应用交付产品（ADC）系列，推出 3 款高性能型号设备：包括分布式应用交付，覆盖了 800G 档位；国产化分布式应用交付型号，覆盖了 600G 档位；以及国产化盒式应用交付型号，覆盖了 200G 档位；可应用于金融行业高性能数据中心、运营商级服务提供商、大型企业园区等高吞吐场景；另外发布了 2 个主线版本及 18 个小版本，全面提升应用交付在 SLB、LLB、GSLB 及 SSL 流量编排等方面的能力，赋能金融等行业客户数字化转型。

（2）WAF

山石网科 Web 应用防火墙（WAF）完成了 2 个重大版本迭代和 15 个小版本的功能升级，对应用安全精细化防护和运维管理等多个维度的能力进行了全方位补齐和优化，包括防护站点规格扩容、牵引模式下支持默认站点、批量配置站点访问控制策略等功能，有效提升在高校等一些场景中网络安全防护能力和运维效率，同时也确保了网络安全的自主可控和稳定运行，满足国产化替代的需求。

（3）内网安全

山石网科网络检测和响应（NDR）-山石智 感 BDS 产品推出了 4 款国产化平台，满足国产化市场对网络检测场景下的安全需求。同时完成了 2 大主线版本的迭代开发，通过优化与增强流量解析、威胁抓包、证据显示、联动响应和日志管理能力，提升威胁检测效率与精准度，优化用户操作体验，帮助用户有效地应对网络安全威胁。

V.安全服务

报告期内，安全服务能力的升级是公司的重点工作之一；其主要体现在推动业务模式创新，通过多元化行业布局、标杆项目落地及技术能力升级，在数据安全服务、安全运营服务等领域取得突破性进展。服务品牌影响力持续扩大。

在数据安全服务方面，成功签约多家大型央企集团总部项目，完成数据安全服务全流程交付，树立行业标杆案例。在医疗、教育行业，同步推进多个数据安全治理项目，兼具示范意义与长期战略价值。通过数据分类分级精细化实施，结合 AI 驱动的数据识别与分析技术，为客户构建多层次防护体系。此外，还通过了中国软件评测中心签发的数据安全建设二级、数据安全评估二级两项最高级级别的数据安全服务能力资格认证。

在安全运营服务方面，发布多项标准化安全运营基础服务，推出“按需订阅+灵活套餐”模式，快速实现安全运营业务的降本增效。通过一对一交付，验证服务效果，订单转化率显著提升。同时，通过云端智能运营平台，整合威胁情报与攻防实战经验，为客户提供全天候安全监测与快速响应能力。

在重点行业拓展方面，依托数据安全治理服务，深度绑定医疗、教育行业头部客户，形成可复制的行业解决方案。在能源、运营商、制造、政府等行业实现业务破冰，推动安全咨询服务与集成服务的规模化应用。

2024 年是山石网科安全服务业务全面升级元年，提出“新定位、新组织、新能力”的全面升级战略，深化生态合作，通过项目经理责任制和管家式服务，实现业务全流程支持，显著提升了内部事业部和外部客户的体验感。报告期内，公司安全服务实现营业收入 2,137.51 万元，同比增长 42.88%，对公司整体收入起到了牵引带动作用。

VI.综合实训平台

山石数字靶场系统完成了 v5.5 版本升级，在产品运维能力、安装部署能力等方面均有大幅提升，同时提高了软件的易用性和稳定性。数字靶场系统方面针对教学、竞赛场景，应用户需求分别增加了直播授课功能与攻防沙盒赛，且在系统资源方面也进行了显著的扩充。为了支撑使用者不同的需求，系统还增加了 AI 智能体，通过 AI 大模型赋能，为山石数字靶场系统提供更智能可靠的功能模块组。

VII.工业互联网安全

基于对工业互联网安全最新的市场洞察与用户反馈，公司升级发布了 OT/IT 融合的“Trust-E”工业互联网安全 2.0 解决方案。在产品方面，公司持续打造工业防火墙、工控安全监测审计、工业入侵检测为代表的工业互联网安全产品。在原有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基础上，进一步强调“开放融合、AI 赋能、智慧运维”的安全理念，帮助更多的工业用户实现“一网到底”架构下的整体安全防护。

1）工业防火墙：陆续发布多个版本和更多型号，新增多种工业协议的深度解析，覆盖更多工业场景；支持工业零信任访问，进行实时监控和操作，提升系统安全和信任度；作为探针，实现工业互联网安全 XDR 整体解决方案。

2）工控安全监测审计：陆续发布多个版本和更多型号，支持识别超百种工业协议，深度解析 S7Comm、Modbus 等几十种关键协议，支持功能码识别数千种。

3）工业入侵检测：发布新品类，提供专有工业入侵检测特征库超过千条，合计入侵检测特征数万条；支持自动生成并学习工业协议基线，比对自学习结果，实现异常检测；同时支持异常行为检测，包括工业协议非法关键指令行为检测等。

报告期内，公司实现其他安全业务收入 18,868.62 万元，同比增长 13.74%，占公司主营业务收入比例为 19.10%。

2.2 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。

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

2024 年度，宏观环境整体稳定，网络安全行业整体处于增速放缓趋势，除部分业务驱动型的行业客户外，下游客户预算普遍收紧，安全项目呈递延执行或缩减的态势。在前期整体投入较为激进的情况下，现阶段整体安全行业发展面临增长及竞争加剧的压力；基于此背景，网络安全厂商也积极调整业务发展方向，从追求规模快速增长转为实现有质量的稳健增长，通过推动产品创

新、能力整合，逐步提升自身产品价值及服务质量，增强其在市场中的核心竞争力。

从下游市场来看，信创领域仍然具备较为明确的长期增长动力。根据安全牛《信创安全能力建设技术指南（2024 年）》报告，随着各行业监管力度的不断增强，预计 2025 年-2027 年，该市场的整体规模将以超过 30%的速度扩张。近年来，公司持续丰富国产化产品矩阵及解决方案，同时大力推进 ASIC 安全芯片研发进度，为后续在信创市场建立差异化竞争优势奠定基础。

在传统安全方面，根据 2025 年 3 月 IDC 发布的《2024 年第四季度中国安全硬件市场预测报告》数据显示，2024 年防火墙整体市场规模 143 亿元，仍然是安全硬件里面不可或缺的、占据主流地位的单品市场。放眼未来，IDC 预测 2024-2029 年，防火墙整体市场五年复合增速为 4.9%，有望在 2029 年达到 182 亿元规模。目前，公司集中力量发挥在防火墙市场的竞争优势，聚焦金融、运营商、能源、教育等行业，在现有客户资源的积累基础上，通过产品更新迭代，提高产品易用性和丰富功能，巩固产品竞争力，以及加强与渠道伙伴的合作，扩大销售规模；同时，预计在 ASIC 安全芯片完成研发后，通过提供更高性价比的产品，将更有助于提升公司防火墙领域的市场份额。

在新兴安全领域方面，数据安全仍然是目前整体市场的热点产品。同传统安全市场相比，数据安全属于竞争相对不激烈的新兴市场，同时具备较大的潜在市场规模和快速增长趋势。2024 年，多项和数据安全具备强相关的政策和标准陆续发布：例如 2024 年 9 月发布的《网络数据安全管理条例》，该条例自 2025 年 1 月 1 日起施行，标志着数据安全管理领域迎来首部行政法规，填补了该领域的法规空白。根据 2024 年 11 月《IDC's Worldwide Security Spending Guide》的预测，到 2028 年，中国数据安全市场的投资规模将达到 173 亿元人民币、复合增长率 16.7%。山石网科较早涉及数据安全，先后提出“数据安全治理白皮书”等数据安全治理理念，并发布了“数据安全综合治理平台”等多类数据安全产品。同时，在 Gartner 发布的《2023 中国安全技术成熟度曲线》报告中，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），在《IDC MarketScape：中国数据安全服务 2024 厂商评估》报告中，山石网科凭借“成熟的数据安全治理体系，丰富的项目落地交付经验，密切的行业主管部门配合，持续的安全服务技术投入”成功入选，成为代表性厂商之一。目前，公司将安全服务和数据安全治理相结合，全力培育数据安全成为公司第二条规模过亿元的业务线。

目前，网络安全行业虽然出现阶段性的需求波动，但整体上，网络安全市场已经逐渐由合规驱动向业务及价值驱动转变，短期的波动并没有改变网络安全行业的长期发展趋势。作为网络安全厂商，公司也将秉承健康发展的经营理念，积极提升自身服务能力，为国内乃至国际网络安全

贡献自身力量，尽早跨越本轮行业周期，迎来新的发展阶段。

(2)．公司所处的行业地位分析及其变化情况

2024 年，公司连续第三年进入 Gartner®《2024 中国安全技术成熟度曲线报告》，在数据安全平台技术领域被评为代表厂商。

2024 年，公司下一代防火墙系列产品再次进入 Gartner® Peer Insights™ 'Voice of the Customers for Network Firewalls' 报告，连续五年入选该报告；并入选 Forrester《2024 年 Q2 企业防火墙前景报告》；公司国产化下一代防火墙入选 Gartner®《创新洞察：使用国产基础设施软件，满足购买本地产品的需求》报告。

2024 年，公司山石智•感智能内网威胁感知系统再次进入 Gartner® 'Voice of the Customer for Network Detection and Response' 报告，并连续两年获“强劲表现者”称号，是国内仅有的 2 家连续 2 年入选此报告的厂商之一；并再次入选 Gartner® 2024 年《NDR 市场指南》报告。

2024 年，公司山石云铠微隔离解决方案先后入选 Forrester《2024 年 Q2 微隔离解决方案前景》和《The Forrester Wave™：微隔离解决方案（2024Q3）》报告，并成为唯一入选后者的中国厂商。

2024 年，公司零信任访问解决方案入选 Gartner®《中国零信任网络访问市场指南》报告，被评为代表性供应商。

2024 年，公司获评知名网络安全媒体 Cyber Defense Magazine 颁发的 2024 年全球信息安全奖（Global InfoSec Awards）两个奖项：“编辑之选：安全公司”和“市场领导者：网络检测与响应”。

山石网科在由香港 IT PRO 杂志主办的 IT PRO Corporate Choice 2024 颁奖典礼上，荣获“CIO Award”大奖，是唯一一家获此荣誉的安全厂商。

根据 IDC 数据，2016 年至 2024 年第三季度，公司在中国“统一威胁管理 UTM”市场规模排名第 4。

根据 IDC《2024 年第二季度中国安全硬件市场跟踪报告》显示，2024 年上半年，山石网科在互联网行业排名第 2，已经连续 3 次（2023H1,2023H2,2024H1）半年位列前二。

2024 年 6 月《IDC Market Presentation：生成式 AI 推动下的中国网络安全硬件市场现状及技术发展趋势，2024》报告显示，生成式 AI 在网络安全的用例主要集中在安全运营、应用安全、数据安全、风险/暴露面管理以及安全合规五大方向；在提升威胁检测效率、统一安全策略、智能策

略编排、提高人效等方面具有重要意义。山石网科凭借防火墙、零信任、WAF、IDPS、沙箱等优秀的产品能力成功入选此报告，成为代表性厂商之一。

2024 年 9 月《IDC MarketScape: 中国零信任网络访问解决方案 2024 厂商评估》报告发布，山石网科成功入选，成为代表性厂商之一。

2024 年 11 月《IDC MarketScape: 中国数据安全服务 2024 厂商评估》报告发布，山石网科凭借“成熟的数据安全治理体系，丰富的项目落地交付经验，密切的行业主管部门配合，持续的安全服务技术投入”成功入选，成为代表性厂商之一。

2024 年 12 月 IDC 发布了《中国医疗数据分类分级市场洞察》报告，山石网科凭借“丰富的数据安全产品体系，专业的数据安全治理服务，头部三甲医疗客户案例”成功入选，成为代表性厂商之一。

根据数说安全《2024 年中国网络安全市场全景图》，山石网科凭借在安全服务、数据安全、云安全、工业互联网安全等多领域的技术优势及产业应用能力，入选 8 大分类中的 21 项二级细分领域。

根据信通院《数字安全护航技术能力全景图》，山石网科凭借在网络与通信安全、数据安全、云安全、应用与业务安全等多领域的技术优势及产业应用能力，入围 11 大安全领域、49 个细分领域。

山石网科凭借在政务、金融、能源等 11 个行业零信任落地总数第二，再次获评信通院《零信任产业图谱（2023）》“最受行业欢迎厂商”，相关案例入围信通院“2023 年度零信任最佳方案优秀案例”。同时，公司零信任安全入选安全牛《现代企业零信任网络建设应用指南》十大代表性厂商之列。

山石网科数据安全综合治理平台、山石网科数据库审计与防护系统、山石网科数据泄露防护系统共三款产品入选《数字医疗产品及服务高质量发展全景图》；山石网科“某委属三甲医院数据安全治理体系实践项目”也成功入选信通院《数字医疗产品及服务高质量发展案例集》。

(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

随着 DeepSeek 等大型语言模型（LLMs）的快速发展，AI 技术对网络安全行业的影响正在逐步深化，既带来了创新机会，也提出了新的挑战，公司认为，在安全公司、安全行业、安全需求

三个方面均产生了不同程度的影响：

（1）对安全公司的影响

AI 技术对于安全公司是一把双刃剑，它赋予了传统网络安全产品新的驱动力，降低了传统安全工具的开发成本与门槛；但也可能导致非安全公司的科技巨头利用 AI 资源抢占现有市场份额。这种竞争加剧了行业内的压力，促使安全公司必须不断创新，以保持其市场地位。与此同时，安全团队的研发、服务人才结构也面临转型的挑战。引入 AI 工程师或对现有人员进行 AI 培训，成为提升团队技术能力的关键。

（2）对安全行业的影响

AI 技术正在重塑安全行业的攻防对抗模式，攻击者可利用 AI 生成更复杂的攻击手段，而防御方则依赖 AI 提升威胁检测和响应效率。同时，AI 模型本身成为新的攻击目标，催生了“AI 安全”这一细分领域，行业需建立针对 AI 模型的评估标准与合规框架。整体上，AI 正在扩展安全边界，推动行业从传统网络安全向 AI 驱动的智能安全转型。

（3）对安全需求的影响

政企单位对安全的需求正从传统工具转向 AI 驱动的解决方案，例如自动化威胁检测、预测性防御等，同时需要加强员工对 AI 生成威胁（如深度伪造、钓鱼攻击）的识别能力。新型安全服务（如 AI 红队/蓝队、模型安全审计）逐渐兴起，满足企业对 AI 模型和数据的保护需求。此外，AI 技术降低了安全运维成本，激活了中小企业和垂直领域的长尾市场，推动安全需求向普惠化和定制化发展。

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

	2024年	2023年	本年比上年增减(%)	2022年
总资产	1,985,452,032.75	1,852,071,698.16	7.20	2,116,178,696.15
归属于上市公司股东的净资产	922,498,947.25	1,078,942,643.90	-14.50	1,318,436,178.88
营业收入	996,589,519.06	901,040,067.77	10.60	811,596,110.98
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	987,777,507.78	890,664,719.34	10.90	788,989,387.72

归属于上市公司股东的净利润	-137,208,201.10	-239,811,522.01	不适用	-182,475,634.35
归属于上市公司股东的扣除非经常性损益的净利润	-151,005,942.88	-248,593,008.86	不适用	-205,530,649.81
经营活动产生的现金流量净额	-90,212,983.42	-58,254,382.32	不适用	-332,312,564.78
加权平均净资产收益率（%）	-13.69	-20.01	增加6.32个百分点	-12.91
基本每股收益（元／股）	-0.7613	-1.3306	不适用	-1.0125
稀释每股收益（元／股）	-0.7613	-1.3306	不适用	-1.0125
研发投入占营业收入的比例（%）	39.71	41.58	减少1.87个百分点	41.81

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	151,082,170.00	229,710,046.26	324,379,404.96	291,417,897.84
归属于上市公司股东的净利润	-75,404,828.84	-4,603,915.27	3,430,660.10	-60,630,117.09
归属于上市公司股东的扣除非经常性损益后的净利润	-75,786,280.21	-9,808,128.11	2,462,576.83	-67,874,111.39
经营活动产生的现金流量净额	-10,708,537.97	-59,323,604.25	-26,193,169.95	6,012,328.75

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)	7,634
年度报告披露日前上一月末的普通股股东总数(户)	7,224
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（不含通过转融通出借股份）

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	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	1,820,932	23,357,932	12.96	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	无	0	境内非国有法人
田涛	0	11,603,662	6.44	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	无	0	境内非国有法人
国创开元股权投资基金（有限合伙）	-1,502,309	10,356,809	5.75	0	无	0	境内非国有法人
越超高科技有限公司	0	8,985,850	4.99	0	无	0	境外法人
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）	-1,689,222	8,771,609	4.87	0	无	0	境内非国有法人
北京奇虎科技有限公司	0	5,406,698	3.00	0	无	0	境内非国有法人
卞伟	0	4,414,568	2.45	0	无	0	境内自然人
LUO DONGPING	0	4,329,835	2.40	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 99,658.95 万元，同比增长 10.60%；实现归属于上市公司股东的净利润-13,720.82 万元，同比亏损减少 42.78%；实现归属于上市公司股东的扣除非经常性损益的净利润-15,100.59 万元，同比亏损减少 39.26%。

报告期内，公司边界安全业务收入为人民币 74,833.80 万元，同比增长 12.96%，占公司主营业务收入比重 75.76%；

报告期内，公司云安全业务收入为人民币 5,075.33 万元，同比下降 18.52%，占公司主营业务收入比重 5.14%；

报告期内，公司其他安全业务收入为人民币 18,868.62 万元，同比增长 13.74%，占公司主营业务收入比重 19.10%。

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