山石网科(688030)

网络安全行业的技术创新领导者

分析日期 2019 年 09 月 12 日

投资评级：中性/首次

证券分析师：黄伯乐

执业证书编号：S0630516070001

电话：021-20333213

邮箱：hbl@longone.com.cn

◎主要观点：

◆**网络安全行业的技术创新领导者。**山石网科是中国网络安全行业的技术创新领导厂商，自成立以来一直专注于网络安全领域前沿技术的创新，提供包括边界安全、云安全、数据安全、内网安全在内的网络安全产品及服务，致力于为用户提供全方位、更智能、零打扰的网络安全解决方案。

◆**公司营收和净利润保持较快增长。**公司营业收入和净利润增速较快。2016-2018 年，公司营收分别为 3.27 亿元，4.63 亿元和 5.62 亿元，2017 年到 2018 年的增速分别 41.82%和 21.43%；归属母公司股东的净利润分别为 0.01 亿元，0.60 亿元和 0.69 亿元，2017 年到 2018 年的增速分别为 4967.78%和 14.75%。

◆**公司技术能力突出。**公司拥有自主软件、硬件设计研发能力，保障产品高性能、高可靠。公司于 2007 年在国内率先自主研发出基于多核处理器的网络安全产品，具备了公司自主软硬件设计能力，确立了产品的高性能优势。公司于 2010 年自主研发出分布式防火墙产品，通过多个处理器集成到一个设备中，大幅提高了单设备的处理性能，进一步奠定了公司产品的性能优势。经过多年的研发积累，公司掌握了大交换容量、高冗余可靠性的硬件系统设计研发技术。公司掌握了云计算数据中心全面安全防护技术。山石网科的高性能高稳定性电信级防火墙技术，以及云计算安全技术在全球范围处于先进水平。山石网科能够为云计算数据中心提供对数据中心边界、私有网络、微隔离、虚拟机等层面的全面安全防护。

◆**行业经验丰富，优质客户群体广泛。**经过行业内数十年的耕耘及积累，公司得到了国内金融、电信运营商、互联网、政府、教育等行业高端客户群的认可。自身的产品和服务品质、研发创新能力及响应速度等多维度综合能力的结合，使公司拥有了广泛优质的客户群体。在国家不断加大对网络安全技术和商业安全性投入的趋势下，山石网科成为网络安全领域的优质厂商。

◆**广受认可的品牌形象。**山石网科连续五年入选 Gartner“UTM 魔力象限”、“企业级防火墙魔力象限”，连续两年入选 Gartner“IDPS 魔力象限”，与 Cisco 成为全球仅有两家同时入选三个魔力象限的厂商。2018 年 11 月，Gartner 发布的亚太地区“企业级防火墙魔力象限”，山石网科与华为被评为仅有的两家来自中国的“全球性厂商”。2016 年 2 月，山石网科通过 NSS Labs 严苛测试，被顺利评为“推荐级”最佳下一代防火墙厂商，成为全球获此评级的网络安全厂商之一。

◆**募集资金用途。**公司拟向社会公开发行不超过 4,505.60 万股，占发行后总股本的比例不低于 25%。发行后总股本不超过 18,022.35 万股。公司本次实际募集资金扣除发行费用后的净额将全部投资于以下项目：网络安全产品线拓展升级项目，高性能云计算安全产品研发项目，营销网络及服务体系建设项目。

◆**风险提示**

产品集中风险，股权分散风险。

正文目录

图表目录

1.公司基本情况

1.1.公司的发展历程

山石网科的前身为山石网科有限。山石网科有限系香港山石出资设立的有限责任公司，于 2011 年 7 月 20 日设立，其设立时的名称为“苏州山石网络有限公司”，注册资本为 1,000 万美元。

2018 年 12 月 20 日，山石网科有限召开董事会会议，同意山石网科有限整体变更为股份有限公司，以截至 2018 年 11 月 30 日经审计的归属于母公司的净资产人民币 285,257,606.27 元为基础，按 1：0.4738 的比例折合为整体变更后的发行人的股份总数 135,167,454 股，每股面值为人民币 1 元，剩余部分 150,090,152.27 元作为资本公积，由全体发起人按出资比例共享。

2018 年 12 月 23 日，发行人召开第一次股东大会，审议通过了山石网科有限整体变更为股份有限公司的相关议案、《公司章程》及其他内部制度。

2018 年 12 月 24 日，苏州市工商行政管理局出具《外商投资公司准予变更登记通知书》，同意核准山石网科通信技术股份有限公司名称、企业类型、营业期限、注册资本变更。同日，苏州市工商行政管理局核准山石网科有限整体变更为股份有限公司的工商变更登记，并向发行人核发变更为股份有限公司后的《营业执照》。

2019 年 1 月 7 日，苏州国家高新技术产业开发区商务局向山石网科出具了《外商投资企业变更备案回执》。

经过多次股权变更，形成了目前的股权结构

1.2.股权比较分散

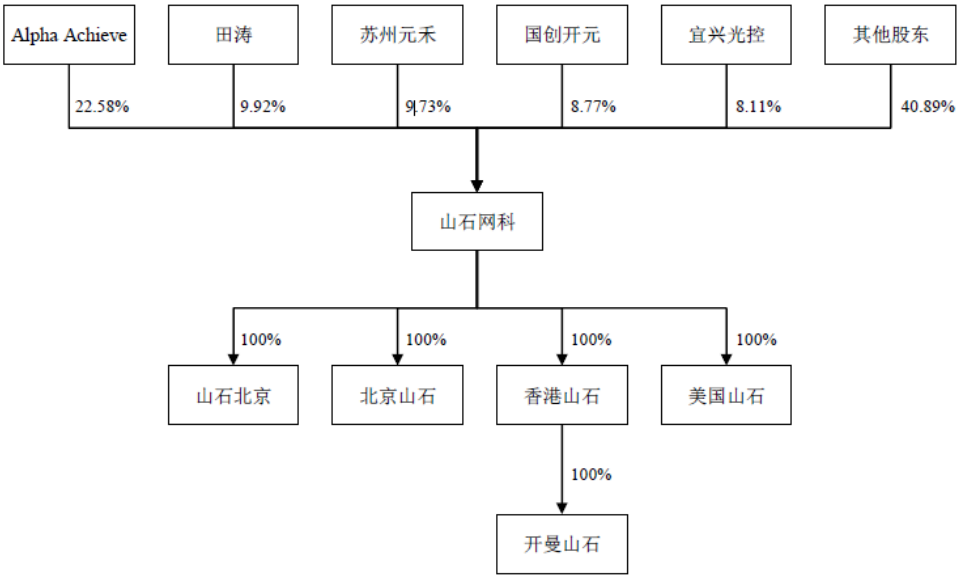
报告期内，公司股权结构较为分散，无控股股东和实际控制人。截至本招股说明书签署之日，公司持股 5%以上的股东包括 Alpha Achieve（22.58%）、田涛（9.92%）、苏州元禾（9.73%）、国创开元（8.77%）和宜兴光控（8.11%）。无任一股东依其可实际支配的发行人股份表决权足以对发行人股东大会的决议产生重大影响。任一股东均无法通过其提名的董事单独决定公司董事会的决策结果或控制公司董事会。

截至招股说明书签署之日，Alpha Achieve 的持股比例为 22.58%，是发行人持股比例最高的股东，但其不能单方面决定公司股东大会决议，无法对发行人的股东大会构成控制。目前发行人董事会 9 名董事中仅邓锋由 Alpha Achieve 提名并经发行人股东大会选举产生的，Alpha Achieve 也无法通过其提名的董事单方面决定董事会决议。根据 Alpha Achieve、田涛、苏州元禾、国创开元和宜兴光控分别出具的《声明承诺书》，该等 5%以上的股东作为财务投资人，其不参与公司经营管理，无意图、实际也未通过任何方式单独或共同控制发行人。

为维持公司股权以及治理结构的稳定性，Alpha Achieve、田涛、苏州元禾、国创开元承诺上市之日起三十六个月内不转让其持有的发行人股份。上述股东所持股权的锁定，在公司上市后的一定时期内有利于保持股权构架的稳定，但是上述股东所持股份锁定到期后，则可能存在公司股权结构和控制权发生变动的风险。

本次发行前公司总股本为 13,516.75 万股，公司本次公开发行股票的数量不超过 4,505.6 万股（行使超额配售选择权之前），占发行后股本比例不低于 25%，本次发行后公司总股本不超过 18,022.35 万股。

图 1 发行上市前公司股权结构



资料来源：公司招股说明书，东海证券研究所

1.3.公司的主营业务

山石网科是中国网络安全行业的技术创新领导厂商，自成立以来一直专注于网络安全领域前沿技术的创新，提供包括边界安全、云安全、数据安全、内网安全在内的网络安全产品及服务，致力于为用户提供全方位、更智能、零打扰的网络安全解决方案。公司为政府、金融、电信运营商、互联网、教育、医疗卫生等行业累计超过 17,000 家用户提供高效、稳定的安全防护。公司在苏州、北京和美国硅谷均设有研发中心，终端客户已经覆盖了美洲、欧洲、东南亚、中东等 50 多个国家和地区。

公司在网络安全全方位防护的能力和市场成绩被多家国内外第三方机构认可。公司连续五年入选国际权威分析机构 Gartner 的“企业级防火墙魔力象限”、“UTM 魔力象限”的“特定领域者”象限，连续两年入选 Gartner 的“IDPS 魔力象限”的“特定领域者”象限。2019 年公司成为中国唯一入选 Gartner《网络流量分析市场指南》的网络安全厂商；公司数据中心安全防护平台获得 Silicon Valley Communications 出版的《信息安全产品指南》“2019 年全球卓越奖”；公司数据中心防火墙、微隔离与可视化产品“山石云•格”、T 系列智能下一代防火墙分别获得《Cyber Defense Magazine》颁发的“最具创新数据中心安全产品奖”、“下一代云安全方案奖”、“突破性安全分析解决方案奖”。2018 年，公司被 Gartner 评为亚太地区企业级防火墙“全球性厂家”；公司“基于 NFV 的虚机微隔离安全解决方案”分别获得中国网络安全联盟的“2018 年网络安全解决方案优秀奖”和中国关键信息基础设施联盟的“2018 关键信息基础设施优秀解决方案之技术创新奖”；公司云安全产品“山石云•格”获得 VMware 公司的“VMware Ready”认证，成为全球十余家获得该认证的网络安全产品之一。2016 年，山石网科获得 NSS Labs“下一代防火墙推荐级别”荣誉。凭借卓越的技术水平和突出的市场表现，公司在国内外拥有较强的市场竞争力。

凭借较强的软硬件自主研发能力，公司为各行业客户提供完整的网络安全解决方案，主要覆盖下一代防火墙、入侵检测和防御系统、安全审计、安全管理、Web 应用防火墙、内网安全在内的网络安全产品及服务。此外，公司基于云计算场景，开发了完备的微隔离与可视化、虚拟化防火墙产品，为云端用户提供一站式、多平台安全解决方案。

表 1 公司的主营业务

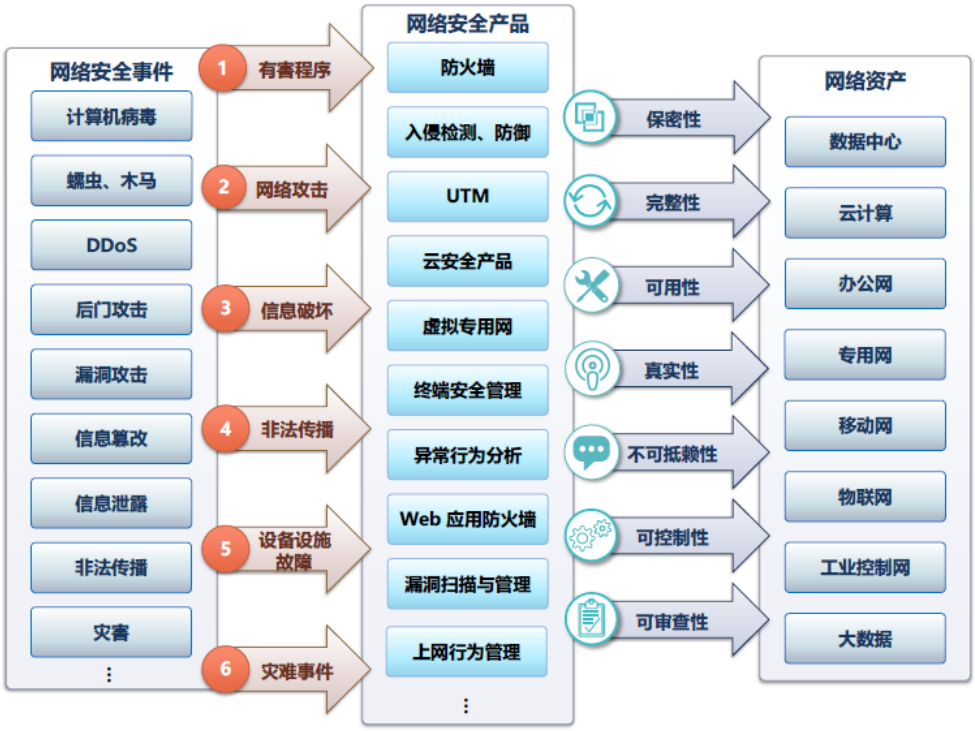
	毛利率	销售费用率	管理费用率
边界安全	下一代防火墙	E 系列/C 系列下一代防火墙	E 系列下一代防火墙采用多核硬件平台和模块化接口设计，提供丰富接口组合和不同档次处理能力，可以覆盖从 1Gbps 到 80Gbps 的网络吞吐环境，在桌面接入、Wi-Fi 接入、中小企业网络出口防护、大型企业内部隔离等场景中得到广泛应用。
		X 系列数据中心防护平台	X 系列数据中心安全防护平台，性能达到 1Tbps 级别，采用全分布软硬件架构，提供强大的网络安全处理能力，支持灵活接口配置，在金融、运营商、互联网数据中心、大型企业数据中心等大流量场景中广泛应用
		T 系列智能下一代防火墙	T 系列智能下一代防火墙，采用全新的智能威胁检测技术，基于机器学习进行行为分析，发现网络潜在威胁，对变种的恶意软件、病毒和内网异常行为进行全方位监控，弥补了传统检测技术的弊端。
	入侵检测和防御系统(IDS/IPS)	S 系列网络入侵防御系统	S 系列入侵防御产品不仅具有丰富的入侵检测手段，发现网络中的入侵行为，更能及时阻断非法入侵，确保网络的安全运行。S 系列入侵防御系统提供了从网络层到应用层分析、从应用识别到行为分析、从协议解析到业务语义分析的全方位检测，确保抵御各类网络攻击。
		D 系列网络入侵检测系统	D 系列入侵检测产品提供全面的入侵检测手段和完备的高级威胁检测方案，可针对各种已知和未知网络威胁进行深度检测，及时发现网络中入侵行为。
	安全审计平台	Hillstone Security Audit（HSA）	HSA 是山石网科的安全审计产品，能够配合公司其他网络安全产品，具有记录网络访问、地址转换（NAT）、网络攻击、上网行为等功能，并提供数据分析能力，协助用户进行网络安全审计，满足国家对重要网络基础设施的审计需求。
	安全管理平台	Hillstone Security Management（HSM）	HSM 是山石网科的网络安全管理平台，可集中管理公司各种网络安全产品，提供设备状态集中监控、统一安全策略管理与优化、全局日志管理、运行数据汇总等功能，为大型企业网络、多分支网络和数据中心网络的管理员提供有力的运维支撑。
	云沙箱	“山石云•影”	山石云•影”是公司的云沙箱平台，可以动态检测通过网页、电子邮件等方式传播的试图进入内部网络的恶意软件，发现已知和未知的病毒和恶意软件及其变种，可用于应对零日攻击和 APT 攻击。
云安全	微隔离与可视化	“山石云•格”	“山石云•格”是一款基于软件定义网络技术的网络微隔离与可视化云安全产品，是部署在云计算环境的全分布的安全防护产品，不仅具有传统网络安全产品的访问控制、流量控制、入侵检测、病毒防护等功能，更可以提供云计算环境下的微隔离、网络可视化、应用可视化、安全可视化等功能，为云计算环境提供安全保障和运维支撑。
	虚拟化防火墙	“山石云•界”	“山石云•界”是虚拟化形态的下一代防火墙产品，可灵活部署在云计算环境中,可以对数据访问流量进行全方位的安全控制，支持精细化应用识别、VPN、入侵防御、病毒过滤、负载均衡等功能，并支持与客户的自动化运维平台深度集成，提升客户的运维效率。
其他	Web 应用防火墙（WAF）	W 系列 Web 应用防火墙	W 系列 Web 应用防火墙是新一代 Web 应用安全防护产品，专注于为网站及 Web 应用系统提供专业的应用层深度防御
	数据安全	山石网科数据库审计与防护系统	山石网科数据库审计与防护系统采用精准的数据库协议解析技术，提供数据库审计与数据库防火墙双重功能，有效应对脱库、非法访问等来自

		内部和外部的各种数据库威胁。
	山石网科数据泄露防护系统	山石网科数据泄露防护系统采用精准的内容识别与基于大数据的行为分析技术，以保护用户数据安全为目标，对关键数据的使用、流转和外发进行实时监控和操作控制，有效防护企业敏感文件（如合同、设计文档、源代码等）通过网络、邮件或终端泄露。
内网安全	山石智•感	“山石智•感”是智能内网威胁感知系统采用基于大数据的智能安全技术。作为山石网科内网安全解决方案的核心组件，该系统聚焦于核心资产服务器监控，采用智能安全技术，聚焦于核心资产服务器监控，检测已知及未知网络威胁，精准定位风险服务器和风险主机，基于攻击链还原攻击细节，进行内网安全态势的深度可视化。
应用交付	AX系列应用交付系统	AX系列应用交付系统具备全面的链路负载均衡和业务负载均衡能力，帮助客户快速实现应用系统部署与性能扩展。产品同时具备高性能 SSL 处理能力，有效提高业务安全性和业务系统的处理能力，并能协助业务系统快速实现 IPv6 部署。
安全服务	“山石云•景”	安全领域的 SaaS 产品，帮忙用户通过移动端、网页实时监控山石网科各类设备的状态、网络流量、威胁等信息。
	安全服务	山石网科拥有安全服务专家团队，提供合规咨询、漏洞扫描、渗透测试、Web 测试、APP 测试、源码审计、日志分析、安全培训等全方位的安全服务

资料来源：Wind，招股说明书，东海证券研究所

公司主要产品及服务矩阵图如下。

图 2 公司主要产品及服务矩阵图



资料来源：公司招股说明书，东海证券研究所

1.3.1.边界安全

（1）下一代防火墙

公司下一代防火墙设备，主要应用于各类网络的边界区域，以保障用户应用安全为目标，通过针对链路层安全到应用层安全的全面威胁防御和应用安全管控技术，对边界流量进行精细化管理与监控，为用户提供全面的应用安全防护能力。

山石网科下一代防火墙分为 E 系列/C 系列下一代防火墙、X 系列数据中心防护平台和 T 系列智能下一代防火墙。全系列产品基于全并行软硬件架构，实现“一次解包、并行检测”，保障整个设备安全防护能力的高处理性能。通过全新一代基于应用特征、行为和关联信息的应用识别技术，为用户提供丰富的应用安全管控手段。同时，山石网科下一代防火墙内置了先进的威胁检测引擎和专业的网站服务器防护功能，能够抵御包括病毒、木马、僵尸网络、数据库注入、跨站脚本、慢速应用层攻击在内的各种网络攻击。产品有效保护用户网络健康及网站服务器安全。

山石网科下一代防火墙提供了全面的应用安全防护和灵活的扩展方式，可应用于各个行业，广泛适用于互联网出口、网络与服务器安全隔离、加密接入等多种网络应用场景。

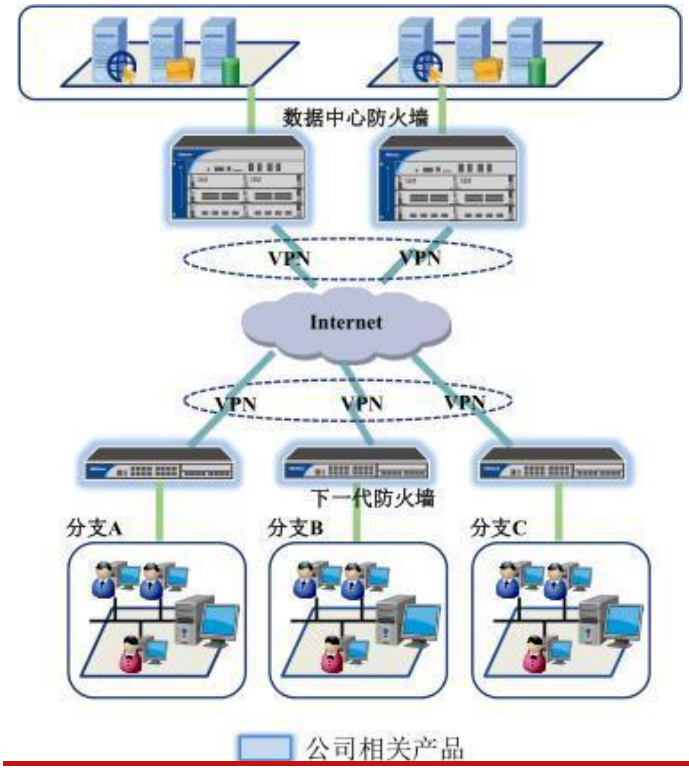
表 2 下一代防火墙的技术特点

技术特点	简要说明
应用精准识别及灵活控制	产品支持深度应用识别技术，能够准确识别数千种网络应用，并为用户提供包括应用类别、应用风险等级、所用技术、应用特征分布等多维可视化信息。产品同时支持灵活的应用安全控制功能，包括策略阻止、会话限制、

	流量管控、应用引流和或时间限制等。
丰富的用户认证及管控	产品支持丰富的用户认证方式，包括终端访问控制器访问控制系统、远程用户拨号认证系统、轻量目录等外部服务器用户认证，以及本地认证、网页认证等，并可针对用户实施精细化的访问控制、应用限制、带宽保证等管控手段。
全面威胁检测与防护	产品提供了基于深度应用、协议检测和攻击原理分析的入侵防御技术，可有效过滤病毒、木马、蠕虫、间谍软件、漏洞攻击、逃逸攻击等安全威胁，具备专业网页攻击防护功能，支持数据库注入、跨站脚本、慢速应用层攻击等检测与过滤，避免网页服务器遭受攻击破坏。高性能的病毒过滤和领先的基于流扫描技术的检测引擎可实现低延时的高性能过滤，及对网页流量、文件传输流量及各种邮件传输协议流量和压缩文件中病毒的查杀。
安全套接层加密流量全面威胁防护	产品可针对安全套接层加密流量综合运用包括入侵防御、病毒防护、域名过滤在内的多种管控手段，实现加密流量应用层威胁的全面防护。
网络适应性	产品支持多种动态路由协议，可根据网络系统的运行情况自动调整动态路由表，满足运营商、高校等复杂网络环境部署。产品内置虚拟专用网络加密加速芯片，可显著提升加解密性能，支持大规模网络环境中加密部署。产品具有智能链路负载均衡功能，其出站动态探测和入站智能域名解析等功能允许网络访问流量在多条链路上实现智能分担。
全并行高性能安全	产品采用一体式多安全功能模块综合检测技术。该技术实现单次报文解析情况下的多个安全功能模块的一体式处理，有效保障在开启多种威胁防护功能时的综合安全性能。产品采用全并行软硬件架构，基于多核硬件处理平台和拥有自主知识产权的 64 位操作系统山石操作系统，实现软硬件全并行操作。专有算法支持每个中央处理器核心上处理所有安全功能，并将会话负载均分到所有处理核，实现最优化的多核并行处理。

资料来源：Wind，招股说明书，东海证券研究所

图 3 公司下一代防火墙的应用场景



资料来源：公司招股说明书，东海证券研究所

（2）入侵检测和防御系统（IDS/IPS 系列产品）

公司入侵检测和防御系统（IDS/IPS 系列产品）是用于网络入侵攻击检测和防御的安全防护产品，检测和防御系统漏洞攻击、病毒蠕虫、木马、僵尸网络、洪水攻击（DDoS）、缓冲区溢出攻击等网络威胁。

山石网科的入侵检测和防御系列产品，分为 S 系列网络入侵防御系统和 D 系列网络入侵检测系统。山石网科入侵防御产品不仅具有丰富的入侵检测手段，发现网络中的入侵行为，更能及时阻断非法入侵，确保网络的安全运行。山石网科入侵检测产品提供丰富的入侵检测手段和完备的高级威胁检测方案，可针对各种已知和未知网络威胁进行深度检测，及时发现网络中入侵行为。

山石网科入侵检测和防御系列产品，通过建立主机和服务器的行为数据模型，对异常行为进行检测，并支持核心资产服务器的重点监控和未知威胁检测。该系列产品增强了网页服务器的安全防护能力，支持对数据库注入、跨站脚本、慢速应用层攻击等网页安全威胁的检测和防御。

（3）安全审计平台

山石网科安全审计平台产品（Hillstone Security Audit，简称“HSA”）为客户提供上网访问行为的监管和审计功能，该平台采用软硬件一体化设计，能够有效记录山石网科下一代防火墙、IDS/IPS、Web 应用防火墙等产品接入用户的网络日志和安全日志，帮助用户解决网络出口日志审计的困扰，并为用户提供丰富便捷的日志查询功能，有效满足《网络安全法》及相关法律法规监管要求。

（4）安全管理平台

公司安全管理平台（Hillstone Security Management，简称“HSM”）主要应用于大型企业网络、分支互联网络和数据中心网络等部署多台安全设备的场景，为用户提供有效的集中安全管理，降低运维管理成本。

HSM 综合运用全局性日志管理、统一策略管理、设备状态集中监控、监控数据汇总和报表统计等手段，解决网络安全状况不直观、安全策略管理乱、安全事件响应慢、安全故障定位难等问题，为用户网络提供全面的集中管理解决方案。

表 3 安全管理平台的技术特点

技术特点	简要说明
	私有策略，满足配置差异化需求。
多设备配置集中管理	支持对防火墙安全策略、路由、NAT、IPS、病毒过滤、统一资源定位地址等配置进行集中管理，支持配置恢复或变更，可即时或定时对网络设备进行配置修改。
设备状态和业务实时监控	支持实时和历史的流量监控，威胁监控、VPN 状态监控，支持网络及 VPN 拓扑呈现。
日志安全审计	支持接收管控设备日志信息及展示，支持日志搜索和书签，支持日志导入导出及远程备份。
统计报表	支持设备状态、流量报表、网页浏览审计报表、即时通信审计报表、网络行为审计报表、病毒过滤审计报表、设备的病毒数统计信息报表等；支持预定义和自定义报表任务；支持按照天、周、月、季等周期生成周期性统计报表，统计粒度可达到分钟、小时和天，并能够通过邮件发送指定人员。
告警响应	支持基于攻击次数、病毒数阈值、特征事件、关键字、日志级别等多种告警条件定义，支持邮件和短信方式告警。
权限管理	支持基于角色的用户管理和基于设备（或虚拟系统）的权限管理。
部署灵活	支持旁路部署、高可靠性部署和虚拟化环境 VMware 及 KVM 部署。

资料来源：Wind，招股说明书，东海证券研究所

（5）云沙箱

“山石云•影”是山石网科的云沙箱平台，可以动态检测通过网页、电子邮件等方式传播的试图进入内部网络的恶意软件，发现已知和未知恶意软件及其变种，可用于应对零日攻击和 APT 威胁。

山石网科沙箱产品由基于云端架构的恶意软件分析环境构建，包括了海量恶意样本库和高性能沙箱集群。“山石云•影”和山石网科下一代防火墙、IPS 等安全产品高度协同，将特征匹配无法判别的文件传送至云端进行行为分析，在以分钟为单位的范围内检测出未知威胁。同时，“山石云•影”通过全局威胁情报共享，将单个接入点检测到的未知威胁情报信息共享到所有站点，将未知威胁变已知威胁，快速阻断。

表 4 云沙箱的技术特点

技术特点	简要说明
动静结合、全面检测	云端的海量恶意样本库可到 10 亿+级别，可以通过快速匹配发现上传的文件是否存在恶意行为。通过沙箱技术模拟文件的真实运行环境，对触发文件的各种行为，包括创建进程、修改注册表、回链请求等进行分析，第一时间发现隐藏其中的未知威胁。
云端架构、即时启用	与山石网科现有的安全产品高度融合，兼容产品包括下一代防火墙、

	“山石云• 界”、IDS/IPS、“山石云• 景”（移动端可视化）等。无需新增硬件，无需中断业务，达到即时启用状态。
对加密流量提供保护	“山石云• 影”可以对 SSL 加密流量进行解密及深度检测，精确还原出加密流量中的各种文件并进行行为分析，使恶意软件无所遁形。
反沙箱技术的对抗策略	“山石云• 影”支持对反沙箱技术的识别和检测，通过隐藏沙箱运行的相关信息，包括内核模块、进程名称、注册表中的相关信息等，“山石云• 影”能够最大程度模拟真实的运行环境。对于恶意软件的躲避措施，“山石云• 影”通过模拟人工操作、交互操作、接管 API 等措施，可以最大限度的触发恶意代码的各种动作。
详尽的报表和威胁呈现	在检测到恶意软件和未知威胁后，“山石云• 影”会及时给出安全警报，这些警报会第一时间通过防火墙的管理界面在用户端呈现。同时，“山石云• 影”可提供恶意文件的详细行为报告，包括网络行为、进程行为、文件行为、文件关键信息等，并通过攻击链分析来还原攻击过程，为安全管理员提供威胁处理建议。
动态更新安全防御能力	“山石云• 影”可根据收集的各种恶意文件报告，生成最新的威胁情报，及时更新山石网科防火墙、入侵检测及防御系统的特征库，帮助管理员调整安全防护策略

资料来源：Wind，招股说明书，东海证券研究所

1.3.2.云安全

（1）“山石云•格”

“山石云•格”是基于软件定义网络技术（简称“SDN”）的网络微隔离及可视化云安全产品。产品不仅具有传统网络安全产品的访问控制、流量控制、入侵检测、病毒防护等功能，更可以提供云计算环境下的微隔离、网络可视化、应用可视化、安全可视化等功能，为云计算环境提供安全保障和运维支撑。

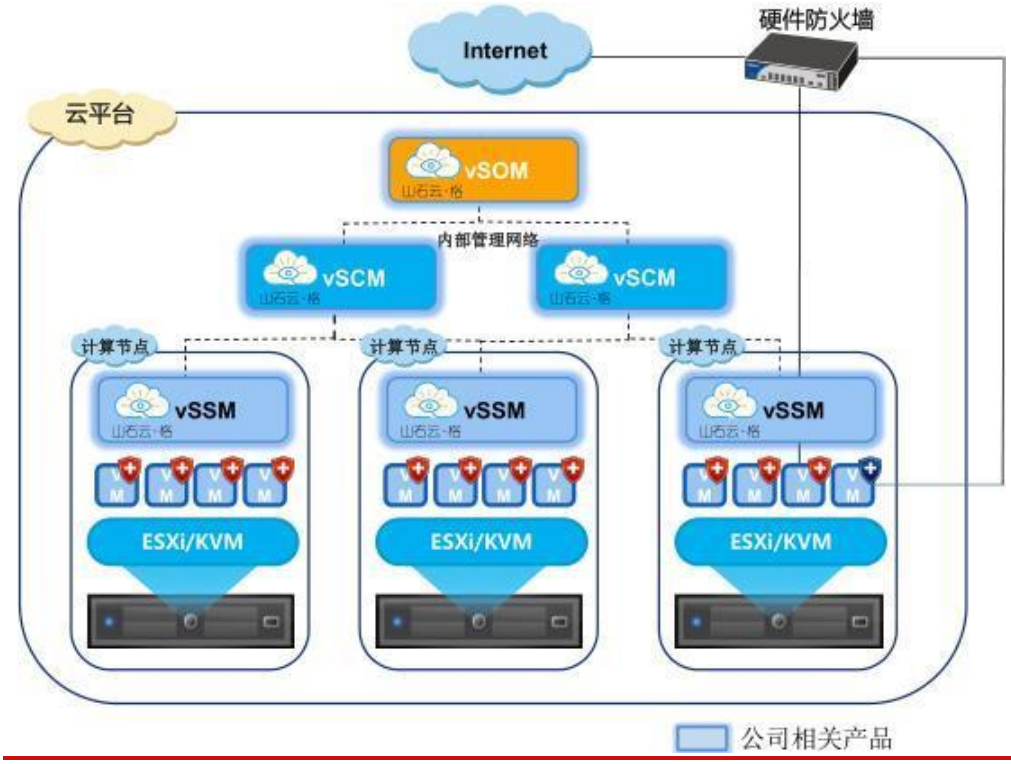
“山石云•格”采用了创新的分布式架构，通过专利引流技术实现了云内微隔离和可视化，为用户提供了全方位的云安全服务，帮助金融、运营商、政府、企业等快速搭建安全、合规的“绿色”云平台。

表 5 “山石云•格”产品的主要技术特点

简称	全称	主要功能
vSOM	云安全管理模块 (Virtual Security Orchestration Module)	负责管理整个“山石云• 格”安全服务生命周期，并兼顾云平台动态事务的感知。
vSCM	云安全控制模块 (Virtual Security Control Module)	负责安全配置管理，以及对云安全业务模块进行灵活调度。vSCM 通常采用冗余部署，可避免单点故障，提高可靠性。
vSSM	云安全业务模块 (Virtual Security Service Module)	负责执行具体安全功能，如访问控制、攻击阻断等，在每一台需要保护的物理服务器部署一个 vSSM 即可实现对该物理服务器上所有虚拟机的安全保护。
vDSM	云数据业务模块 (Virtual Data Service Module)	主要负责对所有 vSSM 产生的日志进行高效转发至外部系统日志服务器，且支持多模块负载平衡方式部署，满足大规模日志外发的应用场景需求。

资料来源：Wind，招股说明书，东海证券研究所

图 4 “山石云•格”系列产品主要应用场景



资料来源：公司招股说明书，东海证券研究所

（2）“山石云• 界”

山石云•界”系公司为云计算环境设计的虚拟化防火墙，可应用于云计算网络边界，对云计算网络进出流量进行监控和网络访问控制，实现云计算网络的安全防护。

“山石云•界”基于公司自主研发的嵌入式操作系统 StoneOS 而开发，支持主流的虚拟化监视器，适配阿里云、腾讯云、华为云、Azure、AWS 等公有云平台以及 OpenStack、VMware、中兴、华为等私有云平台。

表 6 “山石云• 界”的技术特点

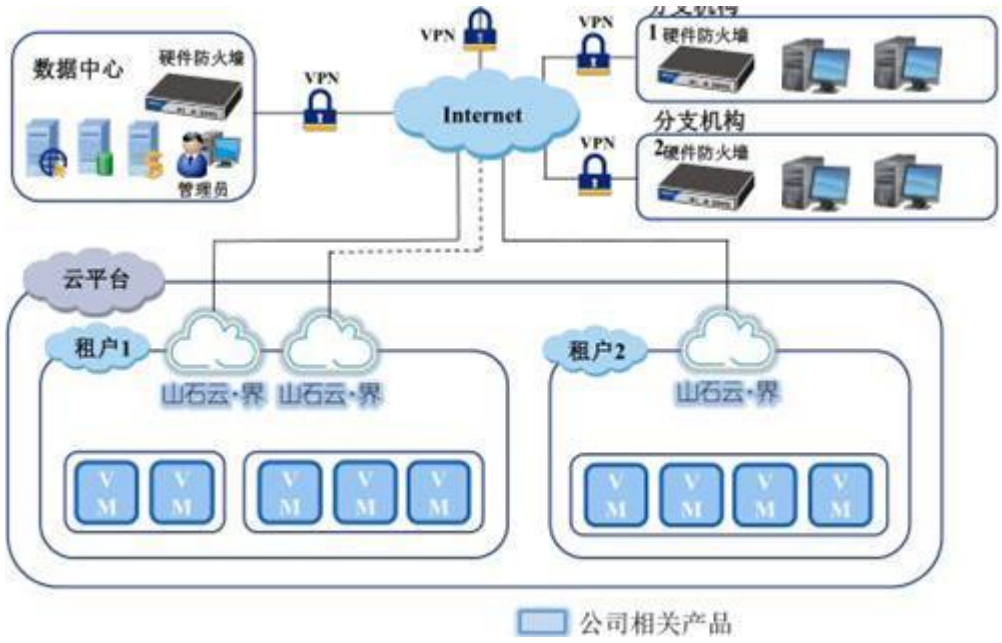
技术特点	简要说明
支持多种虚拟化监 视器	支持 VMware Hypervisor、支持 KVM Hypervisor、支持 Xen Hypervisor、支持 Hyper-V Hypervisor（Gen1）等。
支持公有云	支持阿里云、腾讯云、华为云、Azure、AWS 等公有云平台。
支持多种云平台	支持云平台包括 OpenStack、VMware vCenter、烽火 FitTelecom Cloud、华为 Huawei FusionSphere、浪潮 Inspur InCloud Platform、中兴 ZTE iROS 等。
多维的访问控制	基于深度应用识别的访问控制，基于应用/角色的安全策略。
丰富的路由、NAT 功 能	支持 IPv4/IPv6、静态路由、策略路由、RIP、OSPF、BGP 等多种路由协议；支持源地址 NAT、目的地址 NAT、端口 NAT、NAT444 等 NAT 功能。
全面的安全防护	支持攻击防护、入侵防御、网络防病毒、云沙箱、僵尸网络防御、IP 信誉

能 力	库等功能。
灵活的负载均衡	基于入流量、出流量的链路负载均衡，基于 L2-L4 的服务器负载均衡。
VPN 功能	支持 IPSec\L2TP\GRE VPN 及创新的 PnP（plug-and-play） VPN、支持 Android、iOS 等移动设备的安全接入。
全面的 RestAPI	主要功能及模块支持标准化 RestAPI 接口，易于第三方平台或产品进行对接。
智能许可证管理	迁移、重装时，无需更换授权文件；支持公网授权验证方式；支持内网授权验证方式；支持授权自动分发；支持授权回收、授权调度。

资料来源：Wind，招股说明书，东海证券研究所

“山石云•界”系列虚拟化防火墙广泛用于公有云、私有云和行业云的网络边界，实现网络隔离、网络网关以及边界地址转换。在针对运营商 5G 网络的 NFV 场景构架中，“山石云•界”可作为虚拟化网元，参与安全业务的编排。

图 5 “山石云•界”系列产品主要应用场景



资料来源：公司招股说明书，东海证券研究所

1.3.3.其他

（1）Web 应用防火墙（WAF）

山石网科 W 系列 Web 应用防火墙是新一代 Web 应用安全防护产品，Web 应用防火墙专注于为网站及各类网站应用系统提供专业的应用层深度防御，通过利用深层代理、智能流量学习、虚拟补丁技术，可实现对诸如注入攻击、跨站攻击、Cookie 篡改、信息泄露、应用层 DDoS 攻击等各种 Web 应用层威胁的检测及阻断，确保网站和关键业务系统的稳定运行。

（2）数据安全产品

公司数据泄露防护系统产品主要包括数据库审计与防护系统产品（Database Audit，简称“DBA”）和数据防泄漏系统产品（Data Loss Prevention，简称“DLP”）。

DBA 产品可对网络中用户的数据库访问行为进行独立审计和安全控制，帮助用户应对来自外部和内部的数据库安全威胁。

DBA 产品采用高性能硬件平台、精准协议解析、日志存储和检索等技术，对访问数据库的行为、内容等进行采集、存储和分析，实现数据库独立审计功能。

（3）智能内网威胁感知系统（BDS）

山石智•感是公司智能内网威胁感知系统，采用基于大数据的智能安全技术。作为公司内网安全解决方案的核心组件产品，山石智•感智能内网威胁感知系统聚焦于内网风险态势感知，致力于核心业务安全。

山石智•感采用山石智能安全技术，重点监控核心资产服务器，检测发现已知及未知网络威胁，精准定位风险服务器和风险主机，完整的还原攻击链行为，实现内网安全的可发现、可管理、可追溯、可信任。

（4）AX 应用交付系统

山石网科应用交付控制器 AX 系列是新一代专业的应用交付（简称“ADC”）产品，该产品支持完善的应用层服务器负载均衡、智能的链路负载均衡功能。山石网科 ADC 还支持基于硬件的安全套接层卸载，能够提供数倍于软件安全套接层卸载的处理性能，更好的满足高性能安全套接层卸载的需求。产品标配 1T 硬盘，支持大容量互联网协议第六版日志存储并支持溯源。

（5）安全服务

公司提供的安全服务主要包括 Web 漏洞扫描、综合漏洞扫描和黑盒渗透测试等服务，其主要名称和描述如下表所示

表 7 安全服务的主要内容

类型	描述
安全服务工具	
“山石云• 景”	安全领域的 SaaS 产品，帮助用户通过移动端、网页实时监控山石网科各类设备的状态、网络流量、威胁等信息。
安全服务	
WEB 漏洞 扫描	对 web 应用使用 WEB 漏洞扫描器进行自动化的扫描。扫描完成后分析扫描结果，去除误报，制作漏洞报告并协助客户的开发人员、运维人员等修复加固和复查。
综合漏洞 扫描	对服务器、网络设备、安全设备等各类 IT 系统设备使用综合漏洞扫描器进行自动化的扫描。扫描完成后分析扫描结果、去除误报，制作漏洞报告并协助客户对漏洞进行修复。
黑盒渗透 测试	模拟黑客入侵的思维、方式和工具进行渗透性测试，帮助客户检测其指定系统或网络的安全风险。服务内容包括信息收集、漏洞扫描、威胁建模、漏洞利用、权限提升、社会工程等，及出具人工编写的渗透测试报告、讲解报告、协助开发人员、运维人员等修复加固和复查。
WEB 安全 测试	帮助客户对其各类 web 应用的前端、后端中可能存在的安全风险、各种业务逻辑进行漏洞测试（灰盒测试）。测试内容包括水平权限、垂直权限、帐号注册、网络支付、密码更改、手机认证等环节里可能存在的安全问题。测试完成后出具报告、讲解报告、协助修复加固和复查。
APP 安全 测试	帮助客户对苹果安卓等平台的 APP 进行安全测试。对各种潜在的安全问题进行检测。这些问题包括客户端和服务端安全问题，例如：用户隐私、文

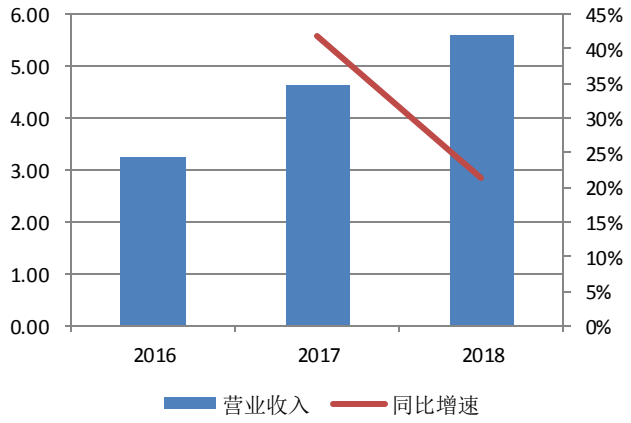
	件权限、网络通讯、组件权限、运行解释保护、数据库安全、代码反编译等。通过深度人工分析的方式，对用户单位 APP 进行上线前安全评估和漏洞检测，评估 APP 抵御黑客恶意篡改的能力、抵御敏感信息泄露的能力、抵御窃取账户密码的能力和抵御通信过程被黑客入侵的能力，帮助用户单位发现手机应用 APP 软件存在的安全隐患，并向用户提供详尽的安全评估分析报告和相应的风险修复建议。
白盒代码 安全审计	帮助客户对其 ASPX、PHP、Java 等脚本源代码进行白盒的安全审计和测试。该服务可以全面深入的挖掘出安全漏洞，并从代码层进行修复，提升系统的安全性。
攻防技术 培训	为客户提供各种类型的信息安全技术培训，传授公司安全服务团队多年来积累的技术实践和管理经验。另外也可以由客户自己选择技术培训内容，帮助客户的技术人员掌握自行检查和验证单位自身安全漏洞的能力。
信息安全 巡检服务	定期对网络安全设备、各类服务器进行安全检查，发现和处理潜在的风险并优化安全配置。巡检完成后出具信息安全巡检服务报告，如果有发现漏洞则协助客户的开发人员、运维人员等实施修复加固和复查。

资料来源：Wind，招股说明书，东海证券研究所

1.4.公司营收和净利润保持较快增长

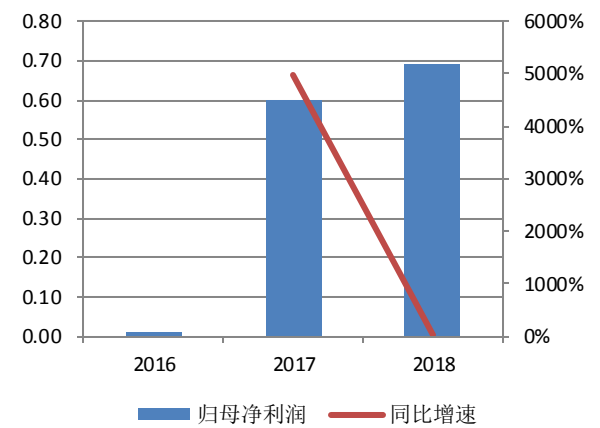
公司营业收入和净利润增速较快。2016-2018 年，公司营收分别为 3.27 亿元，4.63 亿元和 5.62 亿元，2017 年到 2018 年的增速分别 41.82%和 21.43%；归属母公司股东的净利润分别为 0.01 亿元，0.60 亿元和 0.69 亿元，2017 年到 2018 年的增速分别为 4967.78%和 14.75%。

图 6 公司营业收入（单位：亿元，%）



资料来源：Wind，东海证券研究所

图 7 公司归母净利润（单位：亿元，%）



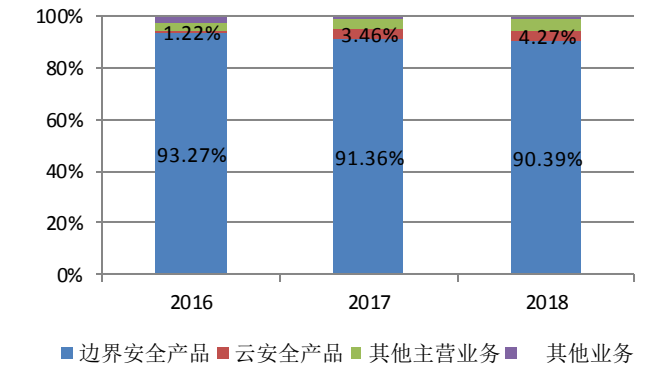
资料来源：Wind，东海证券研究所

1.5.公司净利率提升较快

公司主营业务以边界安全产品销售为主，近年来，公司业务构成基本稳定。2016-2018 年，边界安全产品销售占公司总营收的比例分别为 93.27%，91.36%，90.39%。公司近三年综合毛利率维持在 75%左右。2016-2018 年，公司主营业务综合毛利率分别为 75.14%，

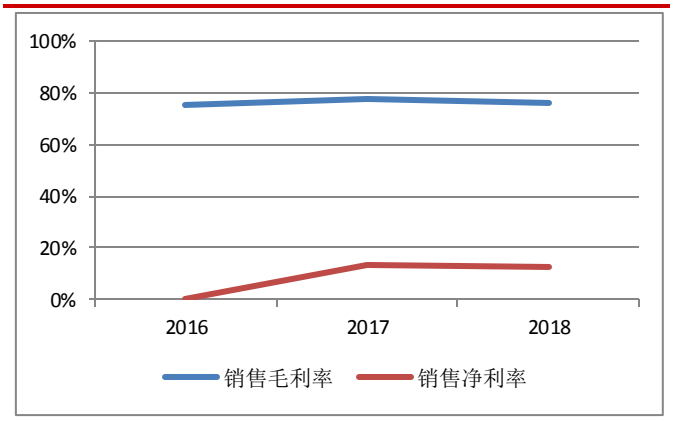
77.53%和 76.30%，毛利率水平较高。公司三年销售净利率分别为 0.36%，12.97%和 12.26%，净利率水平仍有提升空间。

图 8 公司各产品营收占比



资料来源：Wind，东海证券研究所

图 9 公司销售毛利率和销售净利率



资料来源：Wind，东海证券研究所

2.行业情况分析

依据国家统计局《国民经济行业分类》(GB/T 4754-2017)，公司所处行业属于“I65 软件和信息技术服务业”。依据证监会《上市公司行业分类指引》(2012 年修订)，公司所处行业属于“I65 软件和信息技术服务业”。

按照公司主营业务的产品和服务的领域，公司属于新一代信息技术行业。

2.1.全球网络安全市场格局

近年来，由于网络信息技术的持续升级，全球网络安全事件频频爆发，为各国造成了严重的经济损失。为应对网络安全问题，各国政府持续细化提升对网络安全保障的要求，加大在网络安全领域的投入力度，驱动全球网络安全产业规模持续稳步增长

2.1.1.网络攻击智能化、自动化、武器化趋势蔓延，网络安全事件频发

人工智能等新技术的普及以及网络武器泄露的延续效应，网络攻击越发倾向智能化、自动化和武器化，加速了对网络武器的研发和利用，通过机器实施的自动化攻击逐渐成为网络攻击的主流，带来的负面影响和潜在危害不断加深。

近期，网络安全事件频发并导致了严重的经济损失，数据泄漏、数据勒索、流量攻击等网络攻击形式成为重点关注领域。2018 年 6 月，由于缺乏有效防火墙的加密保护，美国 Exactis 公司泄露了约 3.4 亿条个人信息记录。2018 年 3 月，伊朗黑客对全球超过 300 所大学发动网络攻击，共窃取 31TB 的数据，涉及知识产权信息的预估价值达 30 亿美元。2018 年 2 月，代码托管网站 Github 遭遇史上最大规模的 DDoS 攻击，流量峰值达 1.35Tbps。2017 年 5 月，WannaCry 勒索病毒大规模爆发，全球范围内造成的经济损失高达数十亿美元。根据 Gemalto 的数据，自 2017 年以来，全球数据泄露事件数量激增，2018 年上半年数据泄露事件数量达 33 亿件，整体网络安全形势不容乐观，对网络安全强化的需求日益增强。

图 10　全球数据泄露数量

资料来源：公司招股说明书，东海证券研究所

2.1.2.各国持续细化提升网络安全保障要求

全球各国政府不断细化完善有关网络安全的政策和标准体系，以提升整体网络安全防御水平为重点，加大对网络安全预算的投入力度，通过顶层安全战略的制定来引导各国网络安全产业的发展。

2018 年以来，美国特朗普政府延续了对网络安全的重视态度，相继发布了《提升关键基础设施网络安全的框架》、《能源行业网络安全多年计划》、《网络安全战略》等多份相关政策文件，进一步强化对网络安全的政策指导。2018 年 6 月，英国政府内阁办公室发布实施网络安全最低标准，包括从识别、保护、检测、响应和恢复五个维度的最低建设要求。2018 年 5 月，欧盟推出的 GDPR 保护条例正式生效，详细更新对个人隐私数据的保护说明，大力加强对违规企业的处罚力度，防止个人信息被滥用。

近年来，网络空间保护的重要性已上升到国家安全层面，为有力支撑国际战略政策落地，各国对网络安全的国家级投入大规模增长。

2.1.3.全球网络安全产业规模稳步增长

在全球各国政府政策的有力推动下，全球信息安全产业规模进入持续增长阶段。根据 IDC 统计数据，2017 年全球网络安全产业规模达到 862.49 亿美元，2014-2017 年复合增长率为 12.48%，预计 2020 年将达到 1,125.85 亿美元，未来三年复合增长率为 9.30%，依然呈现中高速增长趋势。

图 11　全球网络安全市场规模

资料来源：公司招股说明书，东海证券研究所

从产品细分领域来看，网络安全市场可分为安全硬件、安全软件及安全服务。2017 年全球安全硬件、安全软件及安全服务市场份额分别为 162.73 亿美元、321.67 亿美元和 378.09 亿美元，全球网络安全市场持续以安全服务为主。

2014-2017 年，全球安全硬件、安全软件及安全服务复合增长率分别达到 13.76%、12.06%和 12.31%，安全硬件细分行业增长较快。根据 IDC 预测，2020 年全球安全硬件、安全软件及安全服务市场规模将达到 204.32 亿美元、403.01 亿美元和 518.51 亿美元。

图 12 全球安全硬件，软件，服务市场规模

资料来源：公司招股说明书，东海证券研究所

从地区来看，根据中国信息通信研究院数据，美国、加拿大为主的北美地区 2017 年网络安全行业规模达到 408.76 亿美元，较 2016 年增长 9.2%，市场规模全球占比 41.29%，牢牢占据全球最大份额；英国、德国、芬兰等 16 个西欧国家 2017 年网络安全行业规模合计 267.29 亿美元，同比增长 6.5%，全球占比为 27.00%；日本、澳大利亚、中国、印度等 10 个亚洲国家 2017 年网络安全行业规模合计 225.08 亿美元，同比增长 9.5%，全球占比 22.70%。亚洲地区网络安全行业市场潜力相比较大。

2.2.我国网络安全行业发展现状

2.2.1.网络安全上升为国家战略的重要组成部分，国家出台大量相关政策支持信息安全产业发展

我国一直对网络安全产业高度重视，相继出台各项政策措施支持网络安全产业发展，2003 年即发布《国家信息化领导小组关于加强信息安全保障工作的意见》。2014 年 2 月，中央网络安全和信息化领导小组成立，标志着信息安全在我国已经上升至国家战略层面。2017 年 6 月，《中华人民共和国网络安全法》正式实施，为网络安全工作提供切实的法律保障。自 2001 年起，我国“十五”、“十一五”、“十二五”、“十三五”连续四个五年规划均将信息安全保障体系建设列为重要内容。2016 年 12 月，工信部发布《软件和信息技术服务业发展规划（2016－2020 年）》明确提出到“十三五”末信息安全产业规模将达到 2,000 亿元，年均增长率达 20%以上的目标，远超全行业平均 13%的增速。在相关政策指引的推动下，我国持续完善网络安全保障措施，网络安全防护水平进一步提升，未来行业发展空间和潜力可期。

2.2.2.我国网络安全事件频发，经济损失居全球第一

我国自确立网络强国战略以来，数字化经济与信息建设发展迅速。然而，随着新技术的持续更新，网络空间安全问题日益复杂，面临的网络安全风险和防护难度不断加大。根据国家互联网应急中心发布的《2017 年中国互联网网络安全报告》，2016 年，我国敲诈勒

索病毒频频爆发，DDoS 攻击事件中峰值流量持续突破新高。同时，由于物联网快速发展，智能设备面临的安全威胁加剧，工业控制系统安全风险提升。

此外，根据普华永道发布的《2017 全球信息安全状况调查》报告，2016 年中国内地及香港企业监测到的信息安全事件平均数量高达 2,577 件，超过 2015 年数量的 2 倍。根据赛门铁克公司发布的《2017 诺顿网络安全调查报告》，中国是遭受网络犯罪攻击最严重的国家，2017 年，约 3.52 亿的中国消费者曾成为网络犯罪的受害者，造成经济损失高达 663 亿美元。我国网络安全环境安全性亟待提高，网络安全行业的发展将有力保障我国网络科技环境安全稳定。

图 13　全球主要国家网络攻击经济损失

资料来源：公司招股说明书，东海证券研究所

2.2.3.云我国网络安全行业处于发展期，市场规模保持较快增长

为满足网络安全强化的需求及网络强国战略的推进建设，我国网络安全产业将持续提升安全防护的创新技术，增强综合网络安全的保障能力，未来的行业发展前景明朗。根据 IDC 数据，2017 年我国网络安全产业规模达到 306.04 亿元，较 2016 年增长 25.99%，2014 年至 2017 年复合增长率为 30.79%，持续保持高速增长。预计 2020 年中国网络安全行业规模将达到 591.28 亿元，2018 年至 2020 年复合增长率为 25.78%，行业发展趋势较快，增长空间较大。

图 14 中国网络安全行业市场规模

资料来源：公司招股说明书，东海证券研究所

2.2.4.我国网络安全投入不足

根据 IDC 的数据，2015-2017 年我国信息安全投入占总 IT 投入比例距全球平均水平尚有差距，我国信息安全投入占整体 IT 投入低于 2%，低于全球市场 4%左右的水平，仍有较大的发展空间。随着国家战略的逐步落地，预计我国投入占比将逐渐向成熟市场看齐。

图 15 全球及中国信息安全投入占总 IT 投入比

资料来源：公司招股说明书，东海证券研究所

2.2.5.目前中国网络信息安全市场仍是以安全硬件为主

根据 IDC 数据，2017 年中国网络安全细分领域中硬件占比最大，达到 188.02 亿元，占整体网络安全行业 61.44%，另外安全服务占比 20.20%、软件占比 18.36%，与全球平均相比，安全硬件占比最大。2014 年至 2017 年，我国安全硬件市场复合增长率达到 32.60%，预计 2020 年规模达到 368.56 亿元，预计三年复合增长率达到 26.88%，仍然是我国网络安全行业重要组成部分。

根据 IDC 数据，我国安全硬件行业主要包括传统防火墙、统一威胁管理（UTM）、入侵检测/入侵防御、内容管理、VPN 及其他子产品线。其中，传统防火墙、统一威胁管理（UTM）、入侵检测/入侵防御占比较大，分别达到 37.64%、24.70%和 15.00%，2014 年至 2017 年复合增长率分别达到 31.22%、35.71%和 26.20%。根据预测，2020 年我国传统防火墙、统一威胁管理（UTM）、入侵检测/入侵防御子产品线将分别达到 130.46 亿元、105.25 亿元和 53.35 亿元，复合增长率分别达到 24.99%、30.56%及 25.37%，仍然保持较高速增长，行业增长空间较大。

图 16　中国网络安全硬件市场规模

资料来源：公司招股说明书，东海证券研究所

2.3.云计算行业发展概况

2.3.1.全球云计算市场规模庞大，增长趋于稳定

近年来，云计算产业在全球范围内高速发展，各国政府通过政策引导、资金投入等方式积极推动云计算的战略部署和规模发展，各信息企业通过加速技术创新、业务转型等方式抢占云计算的市场份额。根据中国信息通信研究院发布的《云计算发展白皮书（2018 年）》，2017 年全球公有云市场规模达到 1,110 亿美元，增速为 29.22%，预计到 2021 年市场规模将达到 2,461 亿美元，未来平均增长率为 22%左右。

图 17 全球云计算市场规模

资料来源：公司招股说明书，东海证券研究所

2.3.2.我国云计算市场规模相对较小，细分市场领域发展速度不一

根据中国信息通信研究院发布的《云计算发展白皮书（2018 年）》，2017 年我国云计算整体市场规模达 691.6 亿元，相比 2016 年增长 34.32%。与全球云计算市场相比，当前我国云计算市场整体规模相对较小，占全球市场份额不到 10%，仍存在进一步大规模发展的空间。

2017 年我国公有云市场规模达到 264.8 亿元，相比 2016 年增长 55.7%，预计 2018-2021 年仍将维持 30%以上的增速，2021 年市场规模将达到 902.6 亿元。

2017 年我国私有云市场规模达 426.8 亿元，较 2016 年增长 23.8%，预计 2018-2021 年仍将维持 20%以上的增速，2021 年市场规模将达到 955.7 亿元。

图 18 中国公有云市场规模

资料来源：公司招股说明书，东海证券研究所

图 19 中国私有云市场规模

资料来源：公司招股说明书，东海证券研究所

在云计算的背景下，“云上的世界更安全”已成为用户对公有云安全形态的“普遍认识”。无论是针对传统数据中心的安全防护还是基于云计算的虚拟化安全防护，业务驱动安全的

本质并没有改变，其不同之处在于虚拟化环境下，业务更为复杂，安全防护的方式也更加的多元化、复杂化。

近年来，云服务商对云计算安全越发重视。根据国家相关法律法规和监管部门要求，云服务商聘用第三方安全厂商对网络安全、系统安全、应用安全、数据安全等基础安全方面进行了落地实施，如在管理方面制定了安全管理制度和安全运维流程，确保安全工作开展合规；在技术方面严格控制运维人员的访问权限，定期开展对宿主机、应用软件、数据库软件的安全扫描及加固，确保安全风险可控。部分云服务商成立了专业部门负责推动安全工作的同步规划、同步建设、同步使用，确保其云计算平台运营安全。同时，根据云计算用户的安全需求，专业安全厂商研发推出了虚拟化防火墙、云抗 DDoS、云 Waf、云杀毒、云态势感知等安全服务，帮助云计算用户提升了安全防护水平。

3.公司看点

3.1.自主软件、硬件设计研发能力，保障产品高性能、高可靠

公司于 2007 年在国内率先自主研发出基于多核处理器的网络安全产品，具备了公司自主软硬件设计能力，确立了产品的高性能优势。公司于 2010 年自主研发出分布式防火墙产品，通过多个处理器集成到一个设备中，大幅提高了单设备的处理性能，进一步奠定了公司产品的性能优势。经过多年的研发积累，公司掌握了大交换容量、高冗余可靠性的硬件系统设计研发技术。同时，基于自主设计的软件架构，通过安全业务分布式并行处理软件设计技术，最大化发挥硬件处理能力，极大的保障了硬件冗余可靠性，确立了国内先进的从硬件到软件的全系统自主设计研发能力，成为以高性能、高可靠为核心竞争力的网络安全解决方案供应商。

在发展过程中，依托较强的软件开发能力和硬件设计能力，经过多年的精雕细琢，山石网科推出了一系列基于网络边界安全及云安全的硬件产品和软件产品。公司在业内率先推出了多系列具备领先技术的产品，包括基于多核技术高性能下一代防火墙、基于全分布式构架的 Tbps 级数据中心代防火墙、基于机器学习和大数据分析的智能下一代防火墙、应用于云安全微隔离的“山石云• 格”、针对金融业“两地三中心”而设计的数据中心“孪生模式”防火墙等产品。公司一举打破了国外厂商的技术壁垒，主要产品以其高性能和高可靠性得到了客户的认可。公司核心产品在国内主要电信运营商核心网络，银行的数据中心逐渐替代国外品牌产品，满足了客户对于网络安全处理能力与网络可靠性极高的要求。凭借自身软硬件研发及众多核心技术的积累，公司在行业内持续保持竞争优势。

3.2.云计算数据中心全面安全防护技术

山石网科的高性能高稳定性电信级防火墙技术，以及云计算安全技术在全球范围处于先进水平。山石网科能够为云计算数据中心提供对数据中心边界、私有网络、微隔离、虚拟机等层面的全面安全防护。

在即将到来的 5G 和物联网时代，移动网络将随之发生非常巨大的变化。其中，网络带宽和基站数量的提升使得与基站配套的边缘云计算中心数量也大幅提高。这些变化对网络安全的发展提出了新的要求。山石网科相关核心技术可以为正在建设的 5G 网络提供更完善、可靠的安全保护。

3.3.国际前沿技术优势、国际化视野，持续驱动技术创新

山石网科自成立以来，坚持以创新的技术服务客户，为客户打造出具备国际竞争力的网络安全产品。公司初创团队由前 NetScreen Technologies Inc.、Juniper Networks Inc. 公司的网络安全技术专家组建。目前，公司在苏州、北京和美国硅谷都设立了研发中心。美国硅谷研发中心的技术团队由一支长期从事网络安全行业的资深专家组成。该团队专注于新技术的创新，定期研究业界的技术发展趋势，致力于将大数据分析、人工智能等技术应用于网络安全领域。公司的云安全微隔离技术、基于机器学习的病毒检测技术和网络流量异常检测等技术均诞生于中美研发团队的长期稳定合作。

同时，公司在海外设有多个销售办事处，能够第一时间掌握海外客户特殊需求，并将需求反馈海外研发中心。随着海外客户需求的满足，公司的产品功能更加丰富，海外市场适应能力逐渐增强。开放的国际化视野及前沿的创新技术，使公司在网络安全硬件设计、软件开发、系统测试等领域形成了长期优势积累。公司始终坚持以国际前沿技术研发能力为核心驱动力，打造优质、稳定的产品与服务，进一步奠定山石网科在网络安全行业的技术创新优势。

3.4.行业经验丰富，优质客户群体广泛

经过行业内数十年的耕耘及积累，公司得到了国内金融、电信运营商、互联网、政府、教育等行业高端客户群的认可。自身的产品和服务品质、研发创新能力及响应速度等多维度综合能力的结合，使公司拥有了广泛优质的客户群体。在国家不断加大对网络安全技术和商业安全性投入的趋势下，山石网科成为网络安全领域的优质厂商。

截至报告期末，已有 50 多个国家的超过 17,000 个终端客户选择了山石网科的产品。在我国金融领域，山石网科产品覆盖了中国人民银行、包括中国农业银行、中国建设银行、中国交通银行、中国农业发展银行在内的 4 大国有银行、12 家股份制商业银行、133 家城商行；同时入驻了沪深两大证券交易所、35 家保险公司、50 余家证券公司等国家重要金融领域企事业单位。此外，公司在互联网行业，已成为腾讯、阿里、美团、京东等知名互联网企业的网络安全供应商。凭借优质的产品与良好的客户关系，公司多款产品入围了运营商、政府、高等院校等大型客户的集体采购名录。

广泛优质的客户群体为公司未来发展打下良好的基础，同时也为公司产品线的丰富以及生态圈的建立创造了优质的成长环境。公司一直秉承工匠精神为客户提供高质量、高性能的产品及服务，优质的客户基础已成为公司可持续发展的有效保证。

3.5.广受认可的品牌形象

公司产品辐射至重要政府、教育、企业等用户，在国内市场普遍形成高品质、技术领先的高端品牌形象。

山石网科连续五年入选 Gartner“UTM 魔力象限”、“企业级防火墙魔力象限”，连续两年入选 Gartner“IDPS 魔力象限”，与 Cisco 成为全球仅有两家同时入选三个魔力象限的厂商。2018 年 11 月，Gartner 发布的亚太地区“企业级防火墙魔力象限”，山石网科与华为被评为仅有的两家来自中国的“全球性厂商”。2016 年 2 月，山石网科通过 NSS Labs 严苛测试，被顺利评为“推荐级”最佳下一代防火墙厂商，成为全球获此评级的网络安全厂商之一。

此外，山石网科是全球较早投入云计算安全领域产品开发、销售服务的独立安全厂商，在云安全领域的品牌优势明显。2013 年山石网科成为全球领先的云计算公司 VMware 的

合作伙伴，2018 年获得 VMware 公司“VMware Ready”认证，成为全球十余家获得该认证的网络安全厂商之一。公司主打的云安全产品“山石云•界”先后通过严苛测试，在 AWS、Azure、阿里云、腾讯云、华为云等全球公有云市场上架，成为国内外首批云市场的虚拟化防火墙类安全产品，并取得了较高部署量排名。

基于创新性技术、产品性能和质量、售后服务上的良好口碑及专业认可，公司在国内外塑造了创新主导、技术领先的良好品牌形象。

4.募集资金用途

公司本次拟公开发行不超过 45,056,000 股（行使超额配售选择权之前），募集资金总额将根据发行时市场状况和询价的情况予以确定，本次发行不涉及老股东公开发售其所持有的公司股份。募集资金将全部用于公司主营业务相关的项目。

本次发行完成后，公司募集资金将存放于董事会指定的专项账户集中管理，做到专款专用。本次募集资金投资项目实施后不为发行人新增同业竞争，对发行人的独立性不产生不利影响。

表 8 募投项目及投资金额

募投项目名称	项目总投资	占比
网络安全产品线拓展升级项目	44,405.81	49.65%
高性能云计算安全产品研发项目	28,622.74	32.00%
营销网络及服务体系建设项目	16,411.81	18.35%
合计	**89,440.36**	**100%**

资料来源：招股说明书，东海证券研究所

5.可比公司

A 股上市公司中，与安恒信息业务类似的公司主要有启明星辰，绿盟科技，深信服，迪普科技，任子行等公司。

表 9 可比公司

	毛利率	销售费用率	管理费用率	研发费用占营收比重	市盈率（TTM）
启明星辰	65.47%	24.30%	6.25%	21.19%	54.80
绿盟科技	76.93%	37.79%	10.66%	20.14%	72.70
深信服	73.32%	36.32%	4.03%	24.16%	83.80
迪普科技	70.70%	26.25%	3.33%	22.43%	76.40
平均值	71.60%	31.17%	6.07%	21.98%	71.93
山石网科	76.30%	32.03%	6.94%	27.76%	

资料来源：Wind，招股说明书，东海证券研究所

6.风险提示

产品集中风险，股权分散风险。

分析师简介：

黄伯乐：武汉大学本科，中央财经大学金融学硕士，2014年加入东海证券，从事计算机行业研究

附注：

一、市场指数评级

看多——未来6个月内上证综指上升幅度达到或超过20%

看平——未来6个月内上证综指波动幅度在-20%—20%之间

看空——未来6个月内上证综指下跌幅度达到或超过20%

二、行业指数评级

超配——未来6个月内行业指数相对强于上证指数达到或超过10%

标配——未来6个月内行业指数相对上证指数在-10%—10%之间

低配——未来6个月内行业指数相对弱于上证指数达到或超过10%

三、公司股票评级

买入——未来6个月内股价相对强于上证指数达到或超过15%

增持——未来6个月内股价相对强于上证指数在5%—15%之间

中性——未来6个月内股价相对上证指数在-5%—5%之间

减持——未来6个月内股价相对弱于上证指数5%—15%之间

卖出——未来6个月内股价相对弱于上证指数达到或超过15%

四、风险提示

本报告所载的全部内容只提供给客户做参考之用，并不构成对客户的投资建议，并非作为买卖、认购证券或其它金融工具的邀请或保证，建议客户如有任何疑问应当咨询独立财务顾问并独自进行投资判断。

五、免责条款

六、资格说明

东海证券股份有限公司是经中国证监会核准的合法证券经营机构，已经具备证券投资咨询业务资格。我们欢迎社会监督并提醒广大投资者，参与证券相关活动应当审慎选择具有相当资质的证券经营机构，注意防范非法证券活动。

上海 东海证券研究所

地址：上海市浦东新区东方路1928号 东海证券大厦

网址：Http://www.longone.com.cn

电话：（8621）20333619

传真：（8621）50585608

邮编：200215

北京 东海证券研究所

地址：北京市西三环北路87号国际财经中心D座15F

网址：Http://www.longone.com.cn

电话：（8610）66216231

传真：（8610）59707100

邮编：100089