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

【2019】年度报告摘要

一 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,投资者应当到上海证券交易所网站等中国证监会指定媒体上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,敬请查阅本报告第四节“经营情况讨论与分析”。

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、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。

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 经董事会审议的报告期利润分配预案或公积金转增股本预案

经公司第一届董事会第十七次会议决议,公司2019年度拟以实施权益分派股权登记日登记的总股本为基数分配利润。公司拟向全体股东每10股派发现金红利56元(含税)。截至2019年12月31日,公司总股本180,223,454股,以此基数合计拟派发现金红利人民币10,092,513.42元(含税)。本年度公司现金分红金额占2019年度归属于上市公司股东的净利润比例为11.09%。

如在本报告披露之日起至实施权益分派股权登记日期间,因可转债转股/回购股份/股权激励授予股份回购注销/重大资产重组股份回购注销等致使公司总股本发生变动的,公司拟维持现金派发总额不变,相应调整每股分配比例,并将另行公告具体调整情况。上述利润分配方案已由独立董事发表明确同意的独立意见,需经公司2019年年度股东大会审议通过后实施。

7 是否存在公司的控股股东情况等事项

□适用 √不适用

二 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	尚喜鹤	邓丹
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	0512-68806591	0512-68806591
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

山石网科是中国网络安全行业的技术创新领军厂商,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、更新能、零打扰的网络安全解决方案。公司为金融、政府、运营商、互联网、教育、医疗卫生等行业累计超过18,000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中国以及美洲、欧洲、东南亚、中东的50多个国家和地区。

1、主要业务及主要产品

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,主要包括下一代防火墙、入侵检测和防御系统、安全审计、安全管理、Web应用防火墙、内网安全等网络安全产品及相关服务。此外,公司针对云计算场景开发了微隔离与可视化、虚拟化防火墙产品、虚拟化Web应用防火墙、虚拟化网元管理系统,为云端用户提供一站式、多平台安全解决方案。主要业务及主要产品如下图所示:

2、报告期内公司主要业务及主要产品进展情况

(1)边界安全领域

公司的边界安全解决方案可广泛应用于数据中心、互联网出口、网络隔离、多服务器、VPN接入等多种应用场景,帮助金融、政府、运营商、互联网、教育、医疗卫生等各个行业的用户应对安全挑战。作为公司的传统强项产品,2019年公司在边界安全领域持续加强产品优化和创新,进一步巩固了在该细分领域的竞争优势。

报告期内,公司边界安全产品的主要进展如下:

i. 发布了新一代数据中心防火墙产品平台X9180,针对数据中心网络安全对高性能、可扩展性、高可靠性以及虚拟化等要求而设计,同时提供高级威胁检测能力,并支持高性能VPN隧道技术,具有高性能、高可靠、高扩展、高智能和低能耗的特点。

ii. 发布了国产芯片高性能安全平台K9180,整机可以达到300Gbps的峰值性能,处于国内领先水平。此外,发布了基于国产芯片的一下一代防火墙产品K3000,并于一些重要行业用户开始安全产品类型。

iii. 发布了采用国产关键元器件和国产操作系统的入侵防御系统S2680-GC,符合国家相关标准要求,国产化程度高,适配具有国产芯片和国产化产品需求的用户场景。

iv. 发布了超百Gbps级入侵防御产品S6680,满足高端用户对高性能和高端口密度入侵防御产品的安全需求。

报告期内,网络安全设备的操作系统StoneOS针对下一代防火墙产品发布了新功能30余项,系统改进70余项,进一步提升了山石网科安全产品应对未来网络安全威胁的解决方案能力以及系统的稳定性和易用性。

报告期内,公司实现边界安全产品业务收入87,879.83万元,较上年同期增长14.05%。

(2)云安全领域

公司是国内最早进入云安全领域的安全厂商之一。公司的云计算安全解决方案可为多种云计算环境提供全方位的保护,纯软件化的NFV产品,极易在云计算环境中部署。此外公司还将能体现在产品上的一代防火墙产品云化产品,作为公司在云端的自有“瞭望塔与可视化”功能的产品山石云·格。2019年,公司完成了对山石云·界和山石云·格大量的优化工作,同时还新推出了安全网元管理系统山石云·集,业务规模获得稳定增长。

报告期内,云安全产品主要进展如下:

i. 山石云·界针对云计算安全的实践20余项,全面提升了山石云·界应对云安全威胁的解决方案能力。

ii. 山石云·格实现了业务性能监控(SPM)功能,可提供云内业务和网络的性能可视化监控,提高排错效率,改善总体运营质量;优化了遥测镜等可视化功能,进一步增强了监控能力,提升了用户体验;此外,山石云·格适配了作为FusionCloud云平台,进一步拓展了云安全的多场景。

iii. 开始了云计算SDNFV环境下虚拟化防火墙山石云·集化厂商对需要在云计算虚拟化环境下部署安全能力的场景,提供开放的标准接口,能快速与第三方云计算和SDNFV环境实现对接集成,实现业务的自动化编排。

iv. 山石vWAF也在原有基础上进行了性能优化并增加了更高端型号,支持了订阅模式,支持在AWS上进行部署。同时增加了HTTP管理、爬虫机器流量识别、用户识别及追踪功能,并支持根据用户进行访问控制,从而为Web应用提供更加全面的防护能力。

报告期内,公司实现云安全产品及服务收入3,571.20万元,较上年同期增长60.00%。

(3)其他安全领域

I.智能分析管理

2019年,网络安全的视角逐渐升维,市场中的行业客户更加重视包括单点威胁检测能力、信息集中性管理、关联分析、可视化呈现和风险预测等方面的安全防御体化建设,对于态势感知的需求和研究达到了新新的高度,相关的标准和认证也开始逐步形成。公司紧跟网络安全市场的发展趋势,高度重视网络安全态势的市场和技术产品解决方案,针对态势感知的市场需求,公司2019年发布了具备全网态势感知解决方案能力的智能分析管理平台——山石智·瞭,山石智·瞭以安全总数据模型为核心,向分析平台与丰富的探针共同构成整体解决方案,可为各行业客户提供网络威胁分析、态势呈现与溯源等功能,解决客户监控区域、潜在安全隐患、运维低效等问题。

山石智·瞭是一套软硬件结合的产品,集静态数据、流量、终端,可为公司现有产品形成联动,为客户提供安全整体解决方案,提升安全运维效率。作为网络安全的主控中心,山石智·瞭的独特生态要体现在以下三个方面:

i. 对数据的及时、准确、全面掌控;支持多源海量数据分析,包括流量、日志、威胁情报等;采用分布式实时计算框架,支持分布式存储,可实现弹性扩展和集群管理。

ii. 不仅是AI、更是AI+HI(人工智能+人类智慧);安全运营的本质是技术、产品、人、流程的结合,最终安全反映的是与人人的博弈;基于AI的智能分析引擎和智能搜索引擎帮助整理数据,分析信息,使用更专注于提炼知识,快速决策。

iii. 日动响应,及时致意;灵活的编排和度,实现威胁、弱点、资产等多层次的自动化工单响应;通过可视化事件响应系统,及时跟踪处置,直观了解处理进度,报告工作情况与成果。

报告期内,山石智·瞭已开始逐步应用于金融机构、省级高速、智慧监狱、各大高校的网络安全建设项目,获得了用户的认可。

II.内网安全

随着网络攻击技术的提升和手段变化,网络安全市场对于高级威胁、未知威胁的检测发现与定位防护的关注度持续增长,行业客户在网络安全建设时不仅要考虑网络边界,还需要进一步考虑内网安全的建设,尤其是需要具备内网东西向流量监测分析和内网安全态势的感知能力。公司在2016年发布了能够内网威胁感知系统山石智·感,提供布局内网威胁态势感知,聚焦于内网风险态势感知,致力于核心业务安全,利用山石智能安全技术,帮助行业客户快速定现、可管理、可信任的安全闭网。

报告期内,山石智·感在已有的内网威胁检测能力基础上,新增了热点威胁情报推送、云沙箱检测、垃圾邮件检测三大云端检测功能,内网威胁检测能力得到进一步的加强和提升。

III.数据安全产品

随着信息化的发展,企业数据资产的安全防护问题变得越来越重要。公司通过对市场需求的充分调研和客户应用场景的理解,针对数据安全防护方面提出了一体化的数据安全解决方案,包括数据库审计与防护系统、数据库漏洞扫描系统以及静态数据脱敏系统,进一步加厚了行业用户在数据安全方面的建设与防护。

报告期内,公司数据安全产品系列主要进展如下:

i. 山石网科数据库审计与防护系统新增了商旅便件型号,以覆盖数据库审计的低端细分市场,同时新增了对非关系型数据库的兼容,共计支持的数据库类型22种,目前处于业界领先地位。此外,随着IPv6的应用发展和普及,公司的数据安全产品最新版本已完全适配IPv6环境,解决了IPv6环境下的数据库安全审计和防护难题,产品在政府、教育科研、医疗、金融等行业中得到了认可及应用。

ii. 山石网科数据库脱敏系统作为一款高性能、多种安全算法可选、支持大规模生产环境的数据脱敏系统,可在不改变业务逻辑的情况下,为客户提供高效、安全、灵活、可信任的安全脱敏。

报告期内,山石智·感在已有的内网威胁检测能力基础上,新增了热点威胁情报推送、云沙箱检测、垃圾邮件检测三大云端检测功能,内网威胁检测能力得到进一步的加强和提升。

IV.数据安全产品

随着信息化的发展,企业数据资产的安全防护问题变得越来越重要。公司通过对市场需求的充分调研和客户应用场景的理解,针对数据安全防护方面提出了一体化的数据安全解决方案,包括数据库审计与防护系统、数据库漏扫系统以及静态数据脱敏系统,进一步加厚了行业用户在数据安全方面的建设与防护。

报告期内,公司数据安全产品系列主要进展如下:

i. 山石网科数据库审计与防护系统新增了商旅便件型号,以覆盖数据库审计的低端细分市场,同时新增了对非关系型数据库的兼容,共计支持的数据库类型22种,目前处于业界领先地位。此外,随着IPv6的应用发展和普及,公司的数据安全产品最新版本已完全适配IPv6环境,解决了IPv6环境下的数据库安全审计和防护难题,产品在政府、教育科研、医疗、金融等行业中得到了认可及应用。

ii. 山石网科数据库脱敏系统作为一款高性能、多种安全算法可选、支持大规模生产环境的数据脱敏系统,可在不改变业务逻辑的情况下,为客户提供高效、安全、灵活、可信任的安全脱敏。

报告期内,公司实现了数据安全建设整体解决方案的产品布局,全面覆盖数据安全防护的全部应用场景,较大程度上丰富了公司整体网络安全解决方案。

IV.应用安全和Web安全产品

针对互联网中越来越多的应用和业务上线需求,公司在报告期内发布了机器流量识别和管理方案。同时积极投入自主可控技术的研发,为了基于国产芯片和操作系统的Web应用防火墙W1060-GC,报告期内,公司新增了应用交付产品,支持全局负载均衡功能,完善了IPv6业务的改造方案,在多个项目进行部署和使用。

报告期内,公司实现其他安全类产品及服务收入5,618.16万元,较上年同期增长124.87%。

(二) 主要经营模式

1、销售模式

公司在报告期内仍然采用直销和渠道代理销售相结合的模式,并以渠道代理为主的经营模式,未发生重大变化。

(1)直销模式

基于国内外自信运营商、金融机构及大型企业对于采购流程、服务质量的严格要求,公司采取直销模式,便于公司对接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报价。一般情况下,公司与直销客户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。

(2)渠道代理模式

公司主要采取渠道代理模式,报告期内,公司渠道代理商分为总代理商、战略行业ISV(独立软件开发商,即Independent Software Vendors)和金牌、银牌渠道代理商,其中,总代理商及战略行业ISV可以直接向公司进行采购。一般情况下,金牌、银牌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买类。公司采购的主要材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,原材料采购主要由采购部门执行,工程师、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。

报告期内,公司采购模式未发生重大变化。

3、生产模式

公司物料的网络安全硬件设备和软件由公司自主研发设计,经过严格测试的组装调装,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,统一经过严格的设备组装、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,公司全量产品由代工厂组装完成后,公司质量部门进行检验,检验通过后交付给公司自有实验室进行定制化生产,以满足客户个性化需求。

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

报告期内,公司生产模式未发生重大变化。

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”的持续循环,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。产品在研发过程中,通常可以通过实现大规模生产和封装。

公司的研发组织主要由苏州、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。随着公司产品线的不断丰富和市场变化速率加快,公司在廊坊开发模式的基础上,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,公司研发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

根据赛迪发布的《2019中国网络安全市场研究报告》(Worldwide Security Spending Guide,2019H1),IDC预测2020年全球网络安全相关硬件、软件、服务市场的总投资将达到1,202.8亿美元,较2019年新增长10.1%。IDC认为,全球各国政府和企业对网络安全技术的采纳愈加重视,市场环境向好,在2019-2023年的预测期间内,全球网络安全相关支出将实现10.0%的年均复合增长率,预计2023年将达到1,571.6亿美元。

同时,IDC预测,2020年中国地区体发出将达到237.5亿美元,较2019年同比增长24.0%,增幅领跑美洲地区和欧洲地区。2020年,安全硬件在中国整体网络安全支出中将继续占据绝对主导地位,占比高达51%;安全软件和安全服务支出比例分别为18.4%和22.5%。

综合看来,相较于国外成熟市场,我国网络安全市场正处于快速成长期,安全软件和安全服务具备较大的提升空间。安全事件或勒、合规性政策法规、信息技术升级以及国家信息技术应用创新基础为网络安全市场的主要驱动力。

此外,从技术发展的角度看,网络安全行业的整体技术门槛较高,其中,硬件系统的设计尤其是高端产品的研发,需要具备较强的技术门槛。未来,随着网络信息技术的升级,对对用户日趋复杂的网络环境和实际需求,网络安全技术正朝着更复杂化、多元化、个性化、智能化的方向发展,且技术迭代时间愈发频繁,对网络安全企业的产品研发提出了更高的要求。

2. 公司所处的行业地位分析及其变化情况

经过多年发展,山石网科已成为网络安全领域的技术创新领导厂商。公司产品凭借高性能、高可靠的核心竞争力以及广受认可的品牌形象,得到金融、政府、运营商、互联网、教育、医疗卫生等行业用户的认可,累计已服务超过18,000家用户,获得了一定的品牌知名度。报告期内,研发投入的不断加大,有利于提升公司技术实力及产品竞争力,持续增强公司的技术创新能力,公司的产品和技术实力处于市场领先地位。“多处理器分析芯片计安全处理技术”与“高端硬件系统设计技术”的融合开发、“云安全隔离技术”、“孪生”模式(Twin Mode)应用技术等多项技术已达到国际先进水平。

根据IDC数据,2016-2019年公司在中国“统一威胁管理市场”排名第4(数据来源:IDC IPDC Quarterly Security Appliance Tracker,2019Q4);2019年,公司连续第六年入选国际权威分析机构Gartner的网络防火墙魔力象限报告;连续第二年入选Gartner亚太区防火墙魔力象限报告。在连续两年入选Gartner的“IDPS魔力象限”的“特定领域者”象限后,2019年IDPS被纳入Gartner入侵检测及防御系统市场指南的代表性供应商。

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

(1)网络安全威胁事件不断,网络安全重要性日益提升

近年来,网络安全威胁事件不断,攻击手段不断升级,造成较大影响的网络安全事件频现,引发社会广泛关注,推动网络安全市场快速成长。

从受到网络安全攻击的目标来看,企业信息与个人隐私泄露依然是重灾区。从网络威胁的攻击手段方面,2019年依然是利用多种手段并持续多个阶段的复杂攻击横行的一年,尤其是勒索病毒爆发和高级发展的一年,不断行生出新型的勒索病毒和已知勒索病毒家族的变种,利用应级邮件等社会工程学的攻击方式完成病毒投递,并且能够在知识产权、商业秘密、运维低效等问题。

如在本公告披露之日起至实施权益分派股权登记日期间,因可转债转股/回购股份/股权激励授予股份回购注销/重大资产重组股份回购注销等致使公司总股本发生变动的,公司拟维持现金派发总额不变,相应调整每股分配比例,并将另行公告具体调整情况。上述利润分配方案已由独立董事发表明确同意的独立意见,需经公司2019年年度股东大会审议通过后实施。

7 是否存在公司的控股股东情况等事项

□适用 √不适用

二 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	尚喜鹤	邓丹
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	0512-68806591	0512-68806591
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

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、更新能、零打扰的网络安全解决方案。公司为金融、政府、运营商、互联网、教育、医疗卫生等行业累计超过18,000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中国以及美洲、欧洲、东南亚、中东的50多个国家和地区。

1、主要业务及主要产品

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,主要包括下一代防火墙、入侵检测和防御系统、安全审计、安全管理、Web应用防火墙、内网安全等网络安全产品及相关服务。此外,公司针对云计算场景开发了微隔离与可视化、虚拟化防火墙产品、虚拟化Web应用防火墙、虚拟化网元管理系统,为云端用户提供一站式、多平台安全解决方案。主要业务及主要产品如下图所示:

2、报告期内公司主要业务及主要产品进展情况

(1)边界安全领域

公司的边界安全解决方案可广泛应用于数据中心、互联网出口、网络隔离、多服务器、VPN接入等多种应用场景,帮助金融、政府、运营商、互联网、教育、医疗卫生等各个行业的用户应对安全挑战。作为公司的传统强项产品,2019年公司在边界安全领域持续加强产品优化和创新,进一步巩固了在该细分领域的竞争优势。

报告期内,公司边界安全产品的主要进展如下:

i. 发布了新一代数据中心防火墙产品平台X9180,针对数据中心网络安全对高性能、可扩展性、高可靠性以及虚拟化等要求而设计,同时提供高级威胁检测能力,并支持高性能VPN隧道技术,具有高性能、高可靠、高扩展、高智能和低能耗的特点。

ii. 发布了国产芯片高性能安全平台K9180,整机可以达到300Gbps的峰值性能,处于国内领先水平。此外,发布了基于国产芯片的一下一代防火墙产品K3000,并于一些重要行业用户开始安全产品类型。

iii. 发布了采用国产关键元器件和国产操作系统的入侵防御系统S2680-GC,符合国家相关标准要求,国产化程度高,适配具有国产芯片和国产化产品需求的用户场景。

iv. 发布了超百Gbps级入侵防御产品S6680,满足高端用户对高性能和高端口密度入侵防御产品的安全需求。

报告期内,网络安全设备的操作系统StoneOS针对下一代防火墙产品发布了新功能30余项,系统改进70余项,进一步提升了山石网科安全产品应对未来网络安全威胁的解决方案能力以及系统的稳定性和易用性。

报告期内,公司实现边界安全产品业务收入87,879.83万元,较上年同期增长14.05%。

(2)云安全领域

公司是国内最早进入云安全领域的安全厂商之一。公司的云计算安全解决方案可为多种云计算环境提供全方位的保护,纯软件化的NFV产品,极易在云计算环境中部署。此外公司还将能体现在产品上的一代防火墙产品云化产品,作为公司在云端的自有“瞭望塔与可视化”功能的产品山石云·格。2019年,公司完成了对山石云·界和山石云·格大量的优化工作,同时还新推出了安全网元管理系统山石云·集,业务规模获得稳定增长。

报告期内,云安全产品主要进展如下:

i. 山石云·界针对云计算安全的实践20余项,全面提升了山石云·界应对云安全威胁的解决方案能力。

ii. 山石云·格实现了业务性能监控(SPM)功能,可提供云内业务和网络的性能可视化监控,提高排错效率,改善总体运营质量;优化了遥测镜等可视化功能,进一步增强了监控能力,提升了用户体验;此外,山石云·格适配了作为FusionCloud云平台,进一步拓展了云安全的多场景。

iii. 开始了云计算SDNFV环境下虚拟化防火墙山石云·集化厂商对需要在云计算虚拟化环境下部署安全能力的场景,提供开放的标准接口,能快速与第三方云计算和SDNFV环境实现对接集成,实现业务的自动化编排。

iv. 山石vWAF也在原有基础上进行了性能优化并增加了更高端型号,支持了订阅模式,支持在AWS上进行部署。同时增加了HTTP管理、爬虫机器流量识别、用户识别及追踪功能,并支持根据用户进行访问控制,从而为Web应用提供更加全面的防护能力。

报告期内,公司实现云安全产品及服务收入3,571.20万元,较上年同期增长60.00%。

(3)其他安全领域

I.智能分析管理

2019年,网络安全的视角逐渐升维,市场中的行业客户更加重视包括单点威胁检测能力、信息集中性管理、关联分析、可视化呈现和风险预测等方面的安全防御体化建设,对于态势感知的需求和研究达到了新新的高度,相关的标准和认证也开始逐步形成。公司紧跟网络安全市场的发展趋势,高度重视网络安全态势的市场和技术产品解决方案,针对态势感知的市场需求,公司2019年发布了具备全网态势感知解决方案能力的智能分析管理平台——山石智·瞭,山石智·瞭以安全总数据模型为核心,向分析平台与丰富的探针共同构成整体解决方案,可为各行业客户提供网络威胁分析、态势呈现与溯源等功能,解决客户监控区域、潜在安全隐患、运维低效等问题。

山石智·瞭是一套软硬件结合的产品,集静态数据、流量、终端,可为公司现有产品形成联动,为客户提供安全整体解决方案,提升安全运维效率。作为网络安全的主控中心,山石智·瞭的独特生态要体现在以下三个方面:

i. 对数据的及时、准确、全面掌控;支持多源海量数据分析,包括流量、日志、威胁情报等;采用分布式实时计算框架,支持分布式存储,可实现弹性扩展和集群管理。

ii. 不仅是AI、更是AI+HI(人工智能+人类智慧);安全运营的本质是技术、产品、人、流程的结合,最终安全反映的是与人人的博弈;基于AI的智能分析引擎和智能搜索引擎帮助整理数据,分析信息,使用更专注于提炼知识,快速决策。

iii. 日动响应,及时致意;灵活的编排和度,实现威胁、弱点、资产等多层次的自动化工单响应;通过可视化事件响应系统,及时跟踪处置,直观了解处理进度,报告工作情况与成果。

报告期内,山石智·瞭已开始逐步应用于金融机构、省级高速、智慧监狱、各大高校的网络安全建设项目,获得了用户的认可。

II.内网安全

随着网络攻击技术的提升和手段变化,网络安全市场对于高级威胁、未知威胁的检测发现与定位防护的关注度持续增长,行业客户在网络安全建设时不仅要考虑网络边界,还需要进一步考虑内网安全的建设,尤其是需要具备内网东西向流量监测分析和内网安全态势的感知能力。公司在2016年发布了能够内网威胁感知系统山石智·感,提供布局内网威胁态势感知,聚焦于内网风险态势感知,致力于核心业务安全,利用山石智能安全技术,帮助行业客户快速定现、可管理、可信任的安全闭网。

报告期内,山石智·感在已有的内网威胁检测能力基础上,新增了热点威胁情报推送、云沙箱检测、垃圾邮件检测三大云端检测功能,内网威胁检测能力得到进一步的加强和提升。

III.数据安全产品

随着信息化的发展,企业数据资产的安全防护问题变得越来越重要。公司通过对市场需求的充分调研和客户应用场景的理解,针对数据安全防护方面提出了一体化的数据安全解决方案,包括数据库审计与防护系统、数据库漏扫系统以及静态数据脱敏系统,进一步加厚了行业用户在数据安全方面的建设与防护。

报告期内,公司数据安全产品系列主要进展如下:

i. 山石网科数据库审计与防护系统新增了商旅便件型号,以覆盖数据库审计的低端细分市场,同时新增了对非关系型数据库的兼容,共计支持的数据库类型22种,目前处于业界领先地位。此外,随着IPv6的应用发展和普及,公司的数据安全产品最新版本已完全适配IPv6环境,解决了IPv6环境下的数据库安全审计和防护难题,产品在政府、教育科研、医疗、金融等行业中得到了认可及应用。

ii. 山石网科数据库脱敏系统作为一款高性能、多种安全算法可选、支持大规模生产环境的数据脱敏系统,可在不改变业务逻辑的情况下,为客户提供高效、安全、灵活、可信任的安全脱敏。

报告期内,公司实现了数据安全建设整体解决方案的产品布局,全面覆盖数据安全防护的全部应用场景,较大程度上丰富了公司整体网络安全解决方案。

IV.应用安全和Web安全产品

针对互联网中越来越多的应用和业务上线需求,公司在报告期内发布了机器流量识别和管理方案。同时积极投入自主可控技术的研发,为了基于国产芯片和操作系统的Web应用防火墙W1060-GC,报告期内,公司新增了应用交付产品,支持全局负载均衡功能,完善了IPv6业务的改造方案,在多个项目进行部署和使用。

报告期内,公司实现其他安全类产品及服务收入5,618.16万元,较上年同期增长124.87%。

(二) 主要经营模式

1、销售模式

公司在报告期内仍然采用直销和渠道代理销售相结合的模式,并以渠道代理为主的经营模式,未发生重大变化。

(1)直销模式

基于国内外自信运营商、金融机构及大型企业对于采购流程、服务质量的严格要求,公司采取直销模式,便于公司对接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报价。一般情况下,公司与直销客户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。

(2)渠道代理模式

公司主要采取渠道代理模式,报告期内,公司渠道代理商分为总代理商、战略行业ISV(独立软件开发商,即Independent Software Vendors)和金牌、银牌渠道代理商,其中,总代理商及战略行业ISV可以直接向公司进行采购。一般情况下,金牌、银牌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买类。公司采购的主要材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,原材料采购主要由采购部门执行,工程师、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。

报告期内,公司采购模式未发生重大变化。

3、生产模式

公司物料的网络安全硬件设备和软件由公司自主研发设计,经过严格测试的组装调装,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,统一经过严格的设备组装、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,公司全量产品由代工厂组装完成后,公司质量部门进行检验,检验通过后交付给公司自有实验室进行定制化生产,以满足客户个性化需求。

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

报告期内,公司生产模式未发生重大变化。

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”的持续循环,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。产品在研发过程中,通常可以通过实现大规模生产和封装。

公司的研发组织主要由苏州、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。随着公司产品线的不断丰富和市场变化速率加快,公司在廊坊开发模式的基础上,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,公司研发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

根据赛迪发布的《2019中国网络安全市场研究报告》(Worldwide Security Spending Guide,2019H1),IDC预测2020年全球网络安全相关硬件、软件、服务市场的总投资将达到1,202.8亿美元,较2019年新增长10.1%。IDC认为,全球各国政府和企业对网络安全技术的采纳愈加重视,市场环境向好,在2019-2023年的预测期间内,全球网络安全相关支出将实现10.0%的年均复合增长率,预计2023年将达到1,571.6亿美元。

同时,IDC预测,2020年中国地区体发出将达到237.5亿美元,较2019年同比增长24.0%,增幅领跑美洲地区和欧洲地区。2020年,安全硬件在中国整体网络安全支出中将继续占据绝对主导地位,占比高达51%;安全软件和安全服务支出比例分别为18.4%和22.5%。

综合看来,相较于国外成熟市场,我国网络安全市场正处于快速成长期,安全软件和安全服务具备较大的提升空间。安全事件或勒、合规性政策法规、信息技术升级以及国家信息技术应用创新基础为网络安全市场的主要驱动力。

此外,从技术发展的角度看,网络安全行业的整体技术门槛较高,其中,硬件系统的设计尤其是高端产品的研发,需要具备较强的技术门槛。未来,随着网络信息技术的升级,对对用户日趋复杂的网络环境和实际需求,网络安全技术正朝着更复杂化、多元化、个性化、智能化的方向发展,且技术迭代时间愈发频繁,对网络安全企业的产品研发提出了更高的要求。

2. 公司所处的行业地位分析及其变化情况

经过多年发展,山石网科已成为网络安全领域的技术创新领导厂商。公司产品凭借高性能、高可靠的核心竞争力以及广受认可的品牌形象,得到金融、政府、运营商、互联网、教育、医疗卫生等行业用户的认可,累计已服务超过18,000家用户,获得了一定的品牌知名度。报告期内,研发投入的不断加大,有利于提升公司技术实力及产品竞争力,持续增强公司的技术创新能力,公司的产品和技术实力处于市场领先地位。“多处理器分析芯片计安全处理技术”与“高端硬件系统设计技术”的融合开发、“云安全隔离技术”、“孪生”模式(Twin Mode)应用技术等多项技术已达到国际先进水平。

根据IDC数据,2016-2019年公司在中国“统一威胁管理市场”排名第4(数据来源:IDC IPDC Quarterly Security Appliance Tracker,2019Q4);2019年,公司连续第六年入选国际权威分析机构Gartner的网络防火墙魔力象限报告;连续第二年入选Gartner亚太区防火墙魔力象限报告。在连续两年入选Gartner的“IDPS魔力象限”的“特定领域者”象限后,2019年IDPS被纳入Gartner入侵检测及防御系统市场指南的代表性供应商。

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

(1)网络安全威胁事件不断,网络安全重要性日益提升

近年来,网络安全威胁事件不断,攻击手段不断升级,造成较大影响的网络安全事件频现,引发社会广泛关注,推动网络安全市场快速成长。

从受到网络安全攻击的目标来看,企业信息与个人隐私泄露依然是重灾区。从网络威胁的攻击手段方面,2019年依然是利用多种手段并持续多个阶段的复杂攻击横行的一年,尤其是勒索病毒爆发和高级发展的一年,不断行生出新型的勒索病毒和已知勒索病毒家族的变种,利用应级邮件等社会工程学的攻击方式完成病毒投递,并且能够在知识产权、商业秘密、运维低效等问题。

如在本公告披露之日起至实施权益分派股权登记日期间,因可转债转股/回购股份/股权激励授予股份回购注销/重大资产重组股份回购注销等致使公司总股本发生变动的,公司拟维持现金派发总额不变,相应调整每股分配比例,并将另行公告具体调整情况。上述利润分配方案已由独立董事发表明确同意的独立意见,需经公司2019年年度股东大会审议通过后实施。