远江盛邦(北京)网络安全科技股份有限公司

公司代码:688651 公司简称:盛邦安全

2023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

不涉及

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 天职国际会计师事务所(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

公司2023年年度拟以实施权益分派股权登记日登记的总股本扣除公司回购专用证券账户中股份为基数分配利润,不进行资本公积转增股本,不送红股。本次利润分配方案如下:上市公司拟向全体股东每10股派发现金红利0.6元(含税)。

本议案已经公司第三届董事会第十七次会议审议,尚需提交公司2023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

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	盛邦安全	688651	/

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	袁先登	杨烁璀
办公地址	北京市海淀区上地九街9号9号2层209号	北京市海淀区上地九街9号9号2层209号
电话	010-62966096	010-62966096
电子信箱	ir_public@webray.com.cn	ir_public@webray.com.cn

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

公司主营业务分为以下产品和服务体系:

1、网络安全基础类:包含以漏洞及脆弱性检测、应用安全防御、安全管理与溯源分析、安全审计为核心的网络安全基础类产品;

产品分类	主要产品	产品简介
安全检测类	一体化漏洞扫描评估系统(RayScan)	通过漏洞挖掘等关键技术对资产进行标准行能资性检测,并提供修复建议,为用户提供持续的、高品质的脆弱性评估服务。检测对象包括操作系统、交换机和路由器等网络设备、防火墙、物联网设备、安防设备、移动设备、系统中间件和数据库(包含国产数据库)等。
	Web应用扫描及监控系统(RayWVS)	利用漏洞产生的原理和攻击测试方法,对Web应用进行深度的弱点探测,可帮助应用开发者和运维者检测基于Web应用系统的脆弱性,为改善并提高应用系统安全性提供建议。
	工业互联网专用漏洞扫描系统(RayICSScan)	针对工业控制系统进行漏洞扫描与评估,支持对国内外常见厂商如西门子、施耐德、罗克韦尔等的NCADA、组态软件、HMI、PLC、DCS、应用系统等多种类型的系统或设备的针对性扫描,准确定位其脆弱点和漏洞。
	网站监控预警平台(RaySaaS)	从安全性、合规性、可用性三个角度,7*24小时自动化对远程目标开展安全检测,预警通知服务。服务包含远程漏洞扫描监测、内容合规性监测、黑暗毒监测、系统可用性监测等,并对信息目标系统存在的各种安全隐患与漏洞进行预警及提出整改方案,协助用户进行安全加固,保护信息资产的安全。
应用安全防御类	Web应用防护系统(RayWAF)	通过对HTTP/HTTPS协议的检测,通过多种机制的分析检测,针对当前的热点问题,如SQL注入攻击、跨站脚本、网页篡改、DDoS攻击等,能够有效的阻断攻击,保证Web应用合法流量的正常传输,保障业务系统的运行连续性和完整性。
	网页防篡改系统(RayLock)	基于内核层动态文件保护技术,对各类网页文件,包含各类动态页面脚本提供有效保护,防止黑客、病毒等对目录中的网页、电子文档、图片等文件进行非法篡改和破坏。
	入侵检测与防御系统(RayIDP)	基于异常流量检测技术和移动恶意程序监测处置技术,提供全流量的网络攻击、Web攻击、僵木蠕网络病毒、内部违规行为的检测、预警和防御,保障网络稳定优良。
	异常流量清洗与抗拒绝服务系统(RayADS)	基于流量识别与智能建模技术,对目标网络、数据中心服务器提供智能抽样分析,识别并清洗网络层DDoS攻击,应用层DDoS攻击。
	API安全防护系统(RayAPI)	本系统通过对访问流量进行分析,自动发现流量中的API接口,帮助用户快速梳理环境中未知API资产,并基于未知和已知API资产构建API资产画像;通过API资产画像,快速了解到API资产的访问行为以及存在的异常情况,并对性能进行安全分析和一键下线等操作,构建完整的API全生命周期安全防护方案。
安全管理与溯源分析类	诱捕控制与溯源分析系统(RayTRAP)	产品以攻防对抗思路为基础,以攻击者视角去发现威胁,通过构造仿真主机、服务、网络环境等诱饵,引诱攻击者去访问诱捕环境来及时发现攻击并对攻击者进行溯源取证,以保护客户真实资产。
	持续威胁检测与溯源系统(RayEYE)	基于多项AI智能检测技术,通过多维威胁洞察有效识别出病毒、木马等已知威胁;通过基因图谱检测技术检测恶意代码家族;通过沙箱行为检测技术发现未知威胁;对抗加密的网络流量无数据,进行情报检测、异常检测、流量基因检测,最后将所有安全威胁进行关联分析,助力检测结果,实现对APT攻击的检测。
	物联网流量探针系统	本产品可海阔空间主流物联网协议和主流互联网协议,通过与公司流量指纹信息进行匹配解析,帮助用户进行全方位的终端管理。产品还可提供安全检测与防护能力,提升流量溯源能力,为用户提供了一站式"的物联网安全解决方案。
	网络攻防演练综合平台(RayADT)	新一代实战类网络攻防演练综合平台,集合"靶、赛、评为一体,以精准发现和培养网络安全人才为核心,为网络安全人才提供全方位、一体化培训方案,旨在帮助各个行业培养符合需求的网络安全人才。平台为用户提供了多种安全靶赛模式,融绝的3D态势、严格的防作弊技术、海量安全工具、是第训练考核、实战演练、攻防对抗于一体的综合性平台。平台支持多种方式部署,可以快速创建多场高度仿真的网络安全攻防训练和竞赛环境,适政府、金融、通信、能源、教育、第队等行业客户网络安全人才培养、考核、选拔的产品。
安全审计类	综合日志审计与管理系统(RayLAS)	能够实时不间断地采集网络安全相关的各类设备和系统的日志与报警信息,实时地对采集到的信息进行归一化和关联分析,协助安全管理人员迅速准确地识别安全事件,实现全网综合安全审计。
	运维安全管理系统(RaySAG)	本产品是集单点登录、账号管理、身份认证、资源授权、访问控制和操作审计于一体的新一代运维审计产品,它能够对操作系统、网络设备、安全设备、数据库等操作过程进行有效的运维操作审计,使运维审计由事件审计提升为操作内容审计,通过系统平台的事前预防、事中控制和事后溯源来全面解决企业的运维安全问题,提供了稳定、安全、便捷、快速接入式的解决方案,从而在现有的业务环境下完善了运维管理模式、消除固有弊端,使运维操作管理进入一个真正安全与便利相结合的阶段,帮助客户使运维操作管理发挥更加简单、安全有效,进而提高企业的IT运维管理水平。

2、业务场景安全类:开发了围绕公共安全、电力能源、金融科技、运营商等场景类安全产品,包含网络威胁情报攻击阻断系统、电力资产测绘平台、网络安全单兵自动化检测系统、多接入网关系统、网络挂图作战指挥系统、金融科技风险管控平台等。

产品分类	主要产品	产品简介
基础业务平台	网络安全感知分析平台(RayThink)	集感知、分析、研判、预测和处置于一体,能够对海量网络安全事件数据进行采集、大数据存储与智能化关联分析,通过构建针对行业的安全模型实现风险预测,全面感知风险态势,并结合通报预警模块和应急处置流程形成闭环管理的安全解决方案。
公共安全	网络威胁情报攻击阻断系统(RayTI)	通过订阅云端威胁情报,结合本地内置资产识别引擎,双向攻击监测引擎,来知威胁检测引擎,对各类网络攻击进行监测,应对高级、持续、组织化的威胁,实现互联网入口攻击阻断、情报共享、联防联控。
	多源威胁情报融合分析系统(RayTBD)	通过开发多源威胁情报融合平台,汇聚各行业有效的威胁情报数据,并结合融合公司威胁感知情报、漏洞情报和高级位置情报,采用数据清洗、数据关联、数据分析、数据可视化等技术和多源融合处理技术,降低情报噪音,提炼高精准的威胁情报,可用于反击行为挖掘、网络空间犯罪行为追踪溯源。
	密码猎人	本系统采用公用IP协议多维路由分控模式,通过三个字典构造、权限限额策略等技术,结合海外安全多节点的资产指纹积累和专业安全攻防团队的实战经验,开展从质量化动态出口小模块随机探测动态构造应用字典口令猜解,再强高精度协议分级口令爆破的精度立体化深层口令检测,最大程度检测企业资产的口令,组合口令、缺省口令、泄露口令等口令风险。
	多接入网关系统(RaySDT)	构建用户自己的可监管传输网,专线带宽由用户自己重新分配,设备为每个业务专网集成独立的路由及交换模块,实现网点一体化解决方案,从而方便快捷的延伸多个业务专网(如生产、办公、监控等),减少各业务独立建设中复杂的路由、安全、可靠、QoS等问题,实现了脱投入、高安全、高可靠、易维护的广域网部署。
电力能源安全	电力安全分析室	针对电力行业的业务流程,帮助用户实现分析研判、溯源取证、主动联动防御、资源共享共建、构建态应实战化攻防场景的安全指挥系统。
	网络拓图作战指挥系统	构建网络空间与电力能源行业的地图映射,实现对电力行业数字资产的可视化表达,形成拓扑作战底图。在此基础上结合电力网络安全管理制度与应急管理预案形成事件通报与作战指挥系统,通过可视化、平台化的管理系统帮助电力用户安全专业人员实现"事件拓扑"、"管理拓扑"与"指挥拓扑"。
	网络安全单兵自动化检测系统(RayBox)	基于ATTACK技术框架实践,结合通用系统、工控系统、物联网设备等知识库,自动化完成"目标侦查、暴露面检测、渗透利用、事件调查"的完整攻击链检测流程。
金融科技安全	金融科技风险管控平台(RayCOM)	协助用户满足金融行业监管对信息科技风险管理的要求,为金融机构提供标准化、系统化、自动化、智能化的信息科技风险管理解决方案,提升信息科技风险管控效率和效果。
运营商安全	威胁情报联防联控安全平台	基于运营商自有网络流量和现有业务系统数据,生产符合运营商安全业务需求的情报数据,融合多源情报,建设集情报采集、情报聚合、情报存储、情报分析、情报应用为一体的威胁情报平台,并以平台关键能力为核心,逐步建立健全联防联、高精度、可运营、可闭环的威胁情报完整运营体系,实现多源情报的管理、评估和关联分析、情报检索与输出,满足运营商特色威胁情报应用场景的需求。
	全量资产安全运营平台	本产品通过多维度探测资产和漏洞,基于网络空间测绘实现量露面IP端口开放情况,服务指纹信息,识别运营商量露面资产设备类型,并通过与量露面资产量露弗明进行比对,精准锁标漏洞的量露面资产,溯源未知定取网资产的发现和收集手段,构建安全管理的技术手段,收敛运营商整体量露面,解决互联网量露面信息资产优况不清、安全底座不完的问题。

3、网络空间地图类:包含网络空间地图映射分析系统、网络空间资产测绘系统、网络资产安全治理系统、网络攻击面管理系统及网络空间开源信息监测预警系统等产品体系;

主要产品	产品简介
网络空间地图映射分析系统(RayMap)	基于网络空间测绘数据、被动感知数据、社会机构数据等将网络虚拟空间与地理空间关联,形成网络空间地图系统,实现虚拟空间与现实空间映射的功能。
网络空间资产测绘系统(RaySpace)	基于高性能主动探测,实现网络资产发现、资产信息识别、安全漏洞发现等功能,可以满足各行业的资产普查和风险管理的需求。
网络空间资产治理系统(RayGate)	通过资产模底、备案管理、资产风险监控、应急响应等模块协同工作,帮助用户建立业务系统、联网设备等资产的内部管理规范,实现对网络资产的全生命周期管理。
网络空间攻击面管理系统(RayASM)	通过对网络暴露面数据测绘,结合知识库进行关联分析、推演和可视化呈现,实现对攻击面的有效管理和管控,从而提供主动化、智能化的应对能力。
网络空间开源信息监测预警系统(RaySIN)	帮助目标用户排查数据泄露情况,通过自动化检索的方式,融合渗透技防经验,帮助目标用户发现网络资产、组织情况、人员数据、威胁情报等数据信息在互联网中的泄露情况,并利用大数据手段进行关联分析,输出高价值情报线索,排查数据信息泄露风险,指导用户减少威胁暴露面。
反测绘检测与防御系统(RaySIDS)	基于高仿真蜜罐技术、大规模网络流量多属性聚类技术、循环神经网络算法、大数据聚合关联技术、知识图谱模型等技术识别并发现不断迭代演进的网络空间测绘行为,构建测绘行为特征知识库,并实现网络测绘行为类型精确判定,精确有效处置,监控异常测绘行为,评防止测绘方得到己方资产真实信息,从而达到对网络空间资产的保护。

(4)网络安全服务:包含远程安全监测预警服务、暴露面/攻击面监测服务等SaaS服务,以及等保咨询服务、红蓝对抗的安全保障服务、网络安全评估服务等网络安全专家服务。

产品分类	主要产品	服务简介
SaaS安全服务	远程安全监测预警服务	通过对目标网络资产的7*24小时持续安全监测,发现目标信息系统存在的各种安全隐患与漏洞,实时预警并提出整改方案,协助用户进行安全加固,降低安全风险。
	暴露面/攻击面监测服务	利用平台的主动发现功能,及模糊匹配能力,识别出目标单位互联网资产;通过监控开源社区、网盘文库、暗网交易平台、快速发现企业泄露的信息或文档;通过SaaS化的持续监测能力专家级的人工研判,实现对目标单位互联网暴露面全方位监测。
	暗网监测服务	暗网情报监测系统是面向暗网的在线情报监测系统,以特定情报线索挖掘为导向,通过构建分布式暗网节点监控、服务发现、内容采集的数据处理平台,提供暗网内容、情报检索、线索发现及启动研究等功能,为业务人员提供高效情报发现、关联分析和挖掘服务。
	钓鱼演练服务	模拟钓鱼服务平台主要通过对企业内部员工进行社会工程学攻击,检验企业员工的安全意识水平,提高企业内部的整体安全水平。
	勒索监测服务	勒索病毒监测服务旨在帮助用户及时发现和应对勒索病毒攻击。一旦发现异常行为,如文件加密或勒索信息的显示,服务会立即发出警报,并采取必要的措施,如隔离受感染设备、恢复被加密文件等,以减少损失。勒索病毒监测服务还可以帮助用户识别潜在的安全风险,并提供建议和指导,提高对勒索病毒攻击的防范能力。
专家服务	等保咨询服务	根据客户信息系统的现状和等保政策要求,针对等级保护实施的不同阶段,为用户提供信息系统定级咨询、差距分析、风险评估、总体安全设计、安全方案实施、安全运维支持、应急响应、信息安全制度咨询和安全培训等服务。
	网络安全现状评估服务	以真实单位敏感信息或权限的深度渗透测试、基础渗透测试、漏洞扫描、供应链测试等方法对企业所在单位展开攻击,以获得客户内部权限或敏感信息为目标的渗透攻击,并结合在企业内部的网络架构安全分析、核心业务配置安全检查和环境安全检测等内部安全检查为一体的多角度安全体检服务,还帮企业在网络安全建设中的不足点和隐患点。
	敏感信息检测服务	主要服务内容有:对单位存在的移动端资产进行普查,主要涉及公众号、小程序、APP等相关内容,发现移动端资产信息;发现暴露在互联网中的网络资产,建立资产信息库,缩小暴露面,主要涉及域、主域名、子域名、开放服务、程序、框架等3.通过对开源社区监控,网盘文库监控,暗网交易平台监控,快速发现到企业泄露的信息,规避感知,减少企业损失等。
	重保及攻防演练服务	协助用户在重大活动、节日等特殊时期进行安全保障,帮助用户临补关键时期人员、技术、设备等方面的缺口。根据用户需求提供规模安全强守服务,对业务系统的安全状况进行实时监控和日志分析。
	挖矿检测服务	根据分析目标主流的挖矿木马类型,分析其标记感染主机所使用端口和挖矿通信时的默认端口,结合地址等信息,通过主动和被动探测特征方式对系统进行端口识别,域名识别及识别,大数据动静结合模式匹配,矿类通信协议等检测从而识别系统挖矿木马的存在情况。
	失陷检测服务	应用失陷检测通过数据采集、工具分析、人工标记、专家研判,成果交付五个过程对被分析系统的访问日志进行全面细化的分析,针对所有应用失陷检测系统输出应用失陷检测报告,描述其发现的问题并给出相应的解决方案。
	红队检测服务	针对授权测试范围内的资产进行漏洞等各类安全隐患发现以识别安全防御报板,测试方式包括发现并利用漏洞、远程社工、近距攻击等多种方式,通过模拟黑客入侵的方式识别系统的安全漏洞现状,员工安全意识高低并提供相关的安全风险隐患建议。
常规安全服务	渗透测试服务	模拟网络攻击者的渗透行为,对用户系统及网络开展深度安全性测试,基础渗透测试、漏洞扫描、供应链测试等渗透攻击,挖掘客户在网络安全的护中的缺陷,帮助客户提升网络安全的防御力。
	应急响应服务	应急响应是安全技术人员在遇到突发事件后所采取的措施和行动,包括采取紧急措施和行动,恢复业务到正常服务状态;调查安全事件发生的原因,避免同类安全事件再次发生;在需要司法机关介入时,提供法律认可的数字证据等。
	安全培训服务	结合评估过程中发现的问题对相关技术人员进行培训,提高安全及开发人员技术能力,增强安全及开发人员能力,主要包含:信息安全基础、安全意识培训、系统安全配置与管理、监队防守实战等。

(二) 主要经营模式

公司拥有完备的网络安全产品和创新的网络安全服务,拥有完善的盈利、研发、采购、生产和销售模式。

1、盈利模式

公司的盈利主要来源于自主研发的网络安全软硬件产品的销售以及为客户提供网络安全服务。公司研发并销售的网络安全产品包括业务场景安全类产品、网络空间地图类、网络安全基础类产品产品等。

2、研发模式

公司研发以创新驱动、市场需求为导向,遵守"客户第一"的原则,坚持"两精一深"的研发理念,坚持自主研发、快速迭代的总体思路,实现产品的加速落地和市场转化。公司采取"基座+能力模型+业务模型"的类积木形式研发模型。"基座"为公司自主研发的统一操作系统平台RayOS,通过建立通配信创、云化及虚拟化的通用基础操作系统,可运用于不同的应用场景。基于RayOS平台,公司将网络安全共性能力模块化/组件化,针对不同市场需求以搭积木的方式快速形成差异化产品,提高研发成果复用性,缩短研发工时,提高研发效率。"能力模型"是以漏洞为核心的六大检测能力,及以模块化引擎和一体化策略为核心的高速数据包转发处理能力。"业务模型"是针对不同行业、不同客户的业务需求,建立不同场景化的模型。采用该研发模型能够应对市场需求变化,对现有技术进行快速迭代并迅速形成标准产品,为公司业务"深入行业"提供技术保障。

3、采购模式

公司对外采购包括以下三大类:(1)网络安全产品使用的工控机、服务器、数据授权及相关配件;(2)网络安全解决方案相关的第三方软硬件;(3)技术服务。按照行业定制化产品和通用化标准产品的不同,公司分别实行订单驱动式采购和季度预测式采购。公司建立了《采购管理制度》规范采购行为,并设立供应链中心负责公司采购的执行,按供应商分类建立供应商台账。为满足公司网络安全产品和服务的质量要求,由采购部门牵头,根据供应商的供货能力、质量、价格、付款方式、售后服务及供应商的信誉度等对候选供应商进行综合评定,按照对比择优的原则,选择最佳合作供应商。

4、生产模式

公司网络安全产品主要形态是软件或软硬件一体化产品。硬件为服务器、工控机、计算机、网络设备等,通过对外采购方式获得。公司采用季度预测式和订单驱动式生产模式,直接向客户交付软件产品或将自主研发的软件灌装入硬件设备中,经搭机测试、产品质量检验、入库等环节完成生产交付。

5、服务模式

安全服务包括SaaS安全服务、专家服务及常规安全服务。公司根据客户的实际需求,为客户提供云监测、技术咨询及安全保障等服务。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实施等工作。

6、销售模式

公司产品及服务的销售采用直接销售与渠道销售相结合的模式,其中以直销模式为主。直销模式主要包括终端用户销售、技术能力输出、嵌入式集成销售等几种方式,渠道合作模式主要有签约渠道和项目合作渠道两种形式。

(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《网络安全法》的定义,网络安全是指通过采取必要措施,防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故,使网络处于稳定可靠运行的状态,以及保障网络数据的完整性、保密性、可用性的能力。在5G、云计算、大数据、物联网、人工智能等新一代信息技术的推动下,数字化转型发展越来越快,世界开启万物互联的新时代。在此背景下,虚拟空间和实体空间的结合更加紧密,网络安全威胁更加频繁及复杂,网络安全形势更加严峻。无处不在的数字组织及其创建的海量数据的安全需求为网络安全行业迎来更多技术挑战及发展机遇。

目前网络安全行业的基本特点有:

(1)国际形势复杂严峻,公共领域安全需求强烈。近年国际形势发生了复杂深刻的变化,伴随着物理世界国家间对抗的增加,网络世界的数字争端也在不断加剧。面对着常态化的网络空间对抗,各国政府对网络战的认识不断加深,网信办、公安等国家公共领域的网络安全的重要性被提升到了新的高度。俄乌战争为我们带来了三点重要启示:①网络攻击成为现代战争的一部分,呈现规模化、组织化的特征,持续时间长;②战争中关键信息基础设施是被攻击的重点对象;③关键信息基础设施安全防御体系的建设将促使网络安全行业的重大升级。常态化对抗的国际形势充分凸显出网信办、公安等公共领域安全的重要性。未来,围绕公共安全领域开展检测、防御、态势预警等网络安全体系化建设必将成为我国网络安全市场发展趋势。2023年5月1日,《信息安全技术关键信息基础设施安全保护要求》开始正式实施。这是《关键信息基础设施安全保护条例》发布后,首个正式发布的关键信息基础设施安全保护标准。该标准提供了更好的、更具体的操作指引,以帮助关键信息基础设施管理者更好地开展安全保护工作,进而推动和指导关键信息基础设施的关基保护落地。

(2)"新基建"加速数字化转型,网络空间地图重要性凸显。5G、人工智能、互联网等领域的"新基建"充分带动了数据的流动和集中。随着社会数字化转型的进程加快,数据跨界流转的速度越来越快,数据总量以指数级增长。海量数据为数字资产的管理带来巨大挑战,国家、监管部门、乃至各行各业都因数字化转型进发出大量资产测绘、分类和管理等需求,网络空间地图能够通过资产测绘、网络映射、资产管理等功能,维护网络世界中数字资产的秩序,为"新基建"建设提供数字底座。伴随着数字化转型深入各行业,物联网终端、5G新技术终端、云平台、SD-WAN等新业态衍生出了安全行业的新形势、新需求,驱动安全界限不断向网络物理融合空间延伸。例如网络空间的5G远程手术、车联网、卫星导航等遭到攻击,会直接影响到物理世界的生命安全及社会安全。在此背景下,通过网络空间地图将物理世界的资产在虚拟空间中完成映射,并对数字资产进行全生命周期的主动化、智能化的实时安全防御至关重要。据IDC《中国网络空间地图市场洞察,2023一一生成式AI加持》报告预测,到2027年,中国40%的企业将使用量化模型为网络风险进行金额量化。为了响应这一需求,企业将寻找网络风险量化供应商,以计算其遭受攻击的概率和金额损失。网络空间地图相应技术可以很好地支撑上述需求,并成为构建数字世界地必备基础技术能力。

(3)实战化攻防演练促进技术创新发展,智能化、主动化产品成为新趋势。实战化网络攻防演练行动成为推动安全技术和产品在新场景发展的重要动力,智能化、主动化能力成为产品技术竞争力关键所在。通过攻防演练,能够发现传统网络安全技术存在攻防能力不对等及不能及时适应新场景安全需求的问题。攻防能力不对等是指网络安全攻击方能够通过智能学习模仿、实施高级可持续威胁攻击等方式进行攻击,增加攻击发现和溯源难度,导致防御方基于已有规则特征的被动静态应对失效,难以发现攻击背后的联动风险,难以应对未知威胁和蛰伏攻击,防御产品亟需迎来技术升级。此外,5G、物联网、工业互联网等新场景衍生出了特殊的安全需求,为在广域覆盖、资源受限场景下的威胁应对提出了更高的技术要求。在此背景下,智能化、主动化安全技术成为了行业发展的新趋势,该技术不仅可实现安全威胁的快速感知、主动捕获、关联预测、动态对抗,还支持轻量化、场景定制化、全局安全联动部署。随着攻防态势演变和新场景安全需求迸发,智能主动安全类产品将迎来规模化应用,在网络攻防对抗与核心资产业务防护中凸显重要价值。

(4)工业互联网市场增速明显,推动网络安全需求的快速升级。工业互联网是新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业生态,为工业乃至产业数字化、网络化、智能化发展提供了实现途径,是工业4.0的重要基石。2018年以来,针对制造、通信、能源等关键信息基础领域的攻击事件频频发生,受到攻击的行业领域不断扩大,造成后果也愈加严重,工业互联网安全的市场关注度随之提升。近年来,随着我国智能制造和工业互联网推进政策的不断出台,政府及企业开始逐步重视对工业互联网安全的投入,工业互联网市场呈现快速增长的趋势。根据工信部发布的《"十四五"信息化和工业化深度融合发展规划》要求,"到2025年,我国工业互联网平台普及率达45%,系统解决方案服务能力明显增强,形成平台企业赋能、大中小企业融通发展新格局"。目前,我国工业互联网产业规模已达到万亿级别,工业互联网庞大的市场规模及高速的发展态势也将进一步推动对工业互联网安全保障需求的快速升级。

2. 公司所处的行业地位分析及其变化情况

公司作为全国领先的网络安全产品提供商,十几年来坚持核心技术研发投入,不断提升公司的自主创新能力和研发水平,公司核心产品和技术始终处于行业领先地位。

公司2021年被工信部认定为国家级专精特新"小巨人"企业,2020年-2023年连续被认定为国家规划布局内的重点软件企业。公司被中国网络安全产业联盟(CCIA)评为"网络资产测绘技术领域典型企业",2020年-2023年连续4年入选"中国网安产业竞争力50强",2023年位列27名,排名逐年上升。2023年入选"2022年度北京民营中小企业百强"、"2023北京专精特新企业百强"。

2023年度,公司是国家级网络安全应急服务支撑单位、国家网络与信息安全信息通报机制技术支持单位、CNVD国家信息安全漏洞共享平台支撑单位、CNNVD技术支撑单位(二级)、CITVID信创政务产品安全漏洞专业库技术支撑单位、工业和信息化部移动互联网APP产品安全漏洞库(CAPPVD)技术支撑单位。2023年获评工业和信息化部网络安全威胁和漏洞信息共享平台"2022年度漏洞报送最具贡献单位""2022年度治理合作最具贡献单位"。

公司主要产品近年市场份额持续位居行业前列,市场份额及行业认可如下表所示:

产品类别	产品名称	市场份额与排名	数据来源
安全检测类	漏洞扫描评估系统	最新发布报告显示,2023H1市场占比7.8%,排名第3;2022年度市场占比6.3%,排名第3。	IDC
安全防御类	Web应用防护系统(硬件WAF)	最新报告显示,2022年度市场占比5.7%,排名第5。	IDC
网络空间地图	资产管理与网络空间地图体系	2021年、2022年、2023年连续入选IDC《中国网络空间地图市场洞察》研究报告主要技术提供商。	IDC

2023年度,公司还入选IDC《中国态势感知解决方案2023》报告的"中国态势感知市场主要厂商"、IDC《中国热点威胁安全检测与防护解决方案2023》报告的"关键技术解决方案提供商"。

作为国内网络安全行业,尤其是网络空间地图领域的领军企业,在进行研发创新和市场开拓的同时,公司积极承担国家信息安全产业发展的社会责任,受邀参与了国家网络脆弱性扫描产品安全技术要求和测试评价方法、网络安全威胁信息格式规范、网络安全态势感知通用技术要求、网络安全审计产品技术规范、政务网站系统安全指南、信息安全服务分类与代码、网络安全信息报送指南、信息安全控制评估指南等多项国家与行业标准的制定。公司共参与14项国家/团体标准制定,已发布9项,其中,2023年度发布4项。

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

随着国内和国际局势日益严峻,网络安全事件频发,诸如数据泄漏、勒索软件、黑客攻击等层出不穷,网络安全风险持续增加,围绕公共安全领域开展检测、防御、态势预警等网络安全体系化建设、开展常态化攻防演练对国家信息安全至关重要。网络安全事件,特别是突发性的、造成较大范围影响的安全事件推动了各行业对网络安全的需求,促使各行业,尤其是对于社会安全稳定至关重要的网信办、公安等公共安全领域加大网络安全投入,为网络安全行业发展带来了更多机遇。

伴随5G基站的建设、IPv6网络带来的流量增长、区块链、物联网、云计算、智能制造、AI、VR、AR等新技术、新业态、新应用的涌现,各行业的数字化转型进程不断加速,对网络信息安全提出了新的要求。以云计算和物联网为例,云计算与传统计算方式不同,采用分布式计算的方式,使用虚拟化技术突破了时间、空间的界限,使IT基础架构发生了根本性的变化。这也使得云计算相较于传统计算方式面临更多的网络风险,例如云端数据泄漏、针对虚拟化技术hypervisor组件的安全漏洞等。而物联网的快速发展,使得人网设备数量快速增长,且这些人网设备通常不具备安全防护能力,容易遭受外部攻击者的攻击和利用,使物联网面临更多的安全风险。应用环境变化而不断产生的新的需求为网络信息安全行业产品和服务的升级与拓展带来了新的增长点。

当前,以5G、大数据、物联网、人工智能等新技术为代表的新型基础设施建设是国家经济复苏的关键举措之一,网络安全作为保障"新基建"安全的重要基石,与"新基建"相互共生、相互依存。各行业信息化建设的加速让网络安全产业得到更多蓬勃发展的新机遇。

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	1,140,755,800.32	368,913,205.09	368,205,222.39	209.22	314,874,733.98
归属于上市公司股东的净资产	1,002,906,634.26	268,920,798.59	268,926,840.16	272.94	230,862,826.26
营业收入	290,833,046.16	236,124,720.93	236,124,720.93	23.17	202,570,780.37
归属于上市公司股东的净利润	42,508,631.53	46,186,018.53	46,184,170.67	-7.96	47,781,833.85
归属于上市公司股东的扣除非经常性损益的净利润	34,559,245.89	42,474,519.07	42,472,671.21	-18.64	42,954,655.38
经营活动产生的现金流量净额	-10,682,187.62	13,249,620.80	13,249,620.80	-180.62	24,379,521.97
加权平均净资产收益率(%)	7.43	18.71	18.71	减少11.28个百分点	23.96
基本每股收益(元/股)	0.66	0.82	0.82	-19.51	0.85
稀释每股收益(元/股)	0.66	0.82	0.82	-19.51	0.85
研发投入占营业收入的比例(%)				减少1.05个百分点	

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	35,476,844.21	57,540,159.98	40,131,351.73	157,684,690.24
归属于上市公司股东的净利润	-7,064,113.64	759,637.11	-16,899,921.92	65,713,029.98
归属于上市公司股东的扣除非经常性损益后的净利润	-7,058,806.76	-1,206,679.46	-17,740,305.34	60,565,037.45
经营活动产生的现金流量净额	-10,799,341.04	6,840,826.24	-23,220,325.02	16,496,652.20

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)	9,669
年度报告披露日前上一月末的普通股股东总数(户)	4,950
截至报告期末表决权恢复的优先股股东总数(户)	
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)	
截至报告期末持有特别表决权股份的股东总数(户)	
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)	

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	
权晓文		18,424,712	24.44	18,424,712		无		境内自然人
北京远江星图网络科技有限公司		6,110,000	8.10	6,110,000		无		境内非国有法人
刘晓巍		6,076,510	8.06	6,076,510		无		境内自然人
韩卫东		3,531,335	4.68	3,531,335		无		境内自然人
北京远江高科股权投资合伙企业(有限合伙)		2,390,439	3.17	2,390,439		无		境内非国有法人
金凤霞		2,191,232	2.91	2,191,232		无		境内自然人
浙金盛邦网云科技服务合伙企业(有限合伙)		1,790,000	2.37	1,790,000		无		境内非国有法人
北京利安日成科技有限公司		1,578,900	2.09	1,578,900		无		境内非国有法人
周华金		1,415,168	1.88	1,415,168		无		境内自然人
王润合		1,408,886	1.87	1,408,886		无		境内自然人
上述股东关联关系或一致行动的说明		权晓文与刘晓巍、王润合为一致行动人关系;远江星图、远江高科、浙金网云同为控股股东、实际控制人权晓文控制的企业。						
表决权恢复的优先股股东及持股数量的说明		公司不存在优先股情况						

存托凭证持有人情况

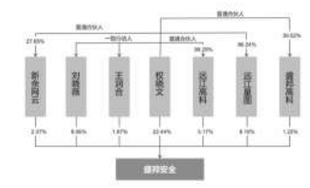
□适用 √不适用

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