

中信建投证券股份有限公司

关于

**奇安信科技集团股份有限公司
首次公开发行股票并在科创板上市**

之

上市保荐书

保荐机构



中信建投证券股份有限公司
CHINA SECURITIES CO.,LTD.

二〇二〇年六月

保荐机构及保荐代表人声明

中信建投证券股份有限公司及本项目保荐代表人董军峰、李彦斌根据《中华人民共和国公司法》（以下简称《公司法》）、《中华人民共和国证券法》（以下简称《证券法》）等有关法律、法规和中国证监会及上海证券交易所的有关规定，诚实守信，勤勉尽责，严格按照依法制订的业务规则和行业自律规范出具上市保荐书，并保证所出具文件真实、准确、完整。

目 录

第一节 本次证券发行基本情况	11
一、发行人基本情况	11
(一) 基本情况.....	11
(二) 主营业务情况.....	11
(三) 核心技术.....	14
(四) 研发水平.....	24
(五) 发行人的主要经营和财务数据及指标.....	26
(六) 发行人存在的主要风险.....	错误!未定义书签。
二、发行人本次发行情况	34
三、本次证券发行上市的保荐代表人、协办人及项目组其他成员情况，包括人员姓名、保荐业务执行情况等内容。	35
(一) 本次证券发行具体负责推荐的保荐代表人.....	35
(二) 本次证券发行项目协办人.....	36
(三) 本次证券发行项目组其他成员.....	36
四、保荐机构与发行人关联关系的说明	37
第二节 保荐机构承诺事项	39
一、保荐机构内部审核程序和内核意见	39
(一) 保荐机构关于本项目的内部审核程序.....	39
(二) 保荐机构关于本项目的内核意见.....	40
二、通过尽职调查和对申请文件的审慎核查，中信建投证券作出以下承诺	40
第三节 对本次发行的推荐意见	42
一、发行人关于本次发行的决策程序合法	42
(一) 董事会审议过程.....	42
(二) 股东大会审议过程.....	42
(三) 国家国防科技工业局的批准.....	42
二、发行人符合科创板定位	42

三、发行人符合《科创属性评价指引（试行）》及《上海证券交易所科创板企业发行上市申报及推荐暂行规定》的规定	45
（一）发行人符合科创板行业领域的规定.....	45
（二）发行人符合科创属性要求的规定.....	45
四、发行人符合《上海证券交易所科创板股票上市规则》规定的上市条件	46
（一）发行人符合中国证监会规定的发行条件.....	46
（二）发行后股本总额不低于人民币 3,000 万元.....	51
（三）公开发行的股份达到公司股份总数的 25%以上；公司股本总额超过人民币 4 亿元的，公开发行股份的比例为 10%以上	52
（四）市值及财务指标符合本规则规定的标准.....	52
（五）上海证券交易所规定的其他上市条件.....	53
五、发行人证券上市后持续督导工作的具体安排	53
六、保荐机构的结论意见	54

释 义

在本上市保荐书中，除非另有说明，下列词语具有如下特定含义：

保荐机构/本保荐机构/中信建投证券	指	中信建投证券股份有限公司
奇安信、公司、发行人	指	奇安信科技集团股份有限公司，整体变更前为北京奇安信科技有限公司
奇安信有限	指	北京奇安信科技有限公司，发行人前身
网神股份	指	网神信息技术（北京）股份有限公司，发行人控股子公司
网康科技	指	北京网康科技有限公司，发行人控股子公司
股票、A 股	指	发行人本次发行的人民币普通股股票
本次发行	指	发行人本次向社会公众首次公开发行不超过 10,194.1579 万股人民币普通股
中安信诚	指	中安信诚投资管理中心（有限合伙）
新余润信	指	新余润信鼎浩投资合伙企业（有限合伙）
青莹投资	指	宁波梅山保税港区青莹投资管理合伙企业（有限合伙）
《招股说明书》	指	《奇安信科技集团股份有限公司首次公开发行股票并在科创板上市招股说明书》
中国证监会	指	中国证券监督管理委员会
交易所、上市证券交易所	指	上海证券交易所
《公司法》	指	《中华人民共和国公司法》
《证券法》	指	《中华人民共和国证券法》
《科创板注册办法》	指	《科创板首次公开发行股票注册管理办法（试行）》
公司章程	指	公司现行有效的《奇安信科技集团股份有限公司章程》
公司章程（草案）	指	公司首次公开发行人民币普通股（A 股）股票并在上海证券交易所科创板上市之日起生效并开始实施的《奇安信科技集团股份有限公司章程》
股东大会	指	奇安信科技集团股份有限公司股东大会
董事会	指	奇安信科技集团股份有限公司董事会

监事会	指	奇安信科技集团股份有限公司监事会
报告期、最近三年	指	2017年、2018年及2019年
元、万元、亿元	指	人民币元、人民币万元、人民币亿元
5G	指	英文“The fifth generation mobile communication network”的简称，即第五代移动通信技术，法定名称是 IMT-2020，广泛应用于联网无人机、无人驾驶、智能制造、智慧能源、智慧物流、物联网、智慧城市等新兴技术领域
云计算	指	基于互联网的相关服务的增加、使用和交付模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源
物联网/IoT	指	英文“Internet of Things”的缩写，是指基于传感技术的物物相联、人物相联和人人相联的信息实时共享的网络
工业互联网	指	工业系统与高级计算、分析、感应技术以及互联网连接融合，通过智能机器间的连接及人机连接，结合硬件、软件、大数据、人工智能等新技术，升级关键的工业领域，重构全球工业、激发生产力
人工智能/AI	指	英文“Artificial Intelligence”的简称，是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学
木马	指	有隐藏性的、自发性的可被用来进行恶意行为的程序
漏洞/Bug	指	是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，可以使攻击者能够在未授权的情况下访问或破坏系统
威胁情报	指	威胁情报（Threat Intelligence）是某种基于证据的知识，包括上下文、机制、标示、含义和可行的建议，这些知识与资产所面临已有的或潜在的威胁或危害相关。
CDN	指	英文“Content Delivery Network”的缩写，即内容分发网络，是为能在传统的 IP 网发布宽带丰富媒体而特别优化的网络覆盖层
WAF	指	英文“Web Application Firewall”的缩写，指 Web 应用防护系统，通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护
DNS	指	英文“Domain Name System”的缩写，是指域名系统
VMware	指	全球桌面及数据中心虚拟化解决方案的领导厂商，官网： https://www.vmware.com/
KVM	指	英文“Kernel-based Virtual Machine”的缩写，一个开源的系统虚拟化模块
Xen	指	Xen 是一种开源虚拟化技术，通过一种准虚拟化的技术获得高性能

Gartner	指	高德纳咨询公司，成立于1979年，是第一家信息技术研究和分析的公司，全球最具权威的IT研究与顾问咨询公司。研究范围覆盖全部IT产业，就IT的研究、发展、评估、应用、市场等领域，为客户提供客观、公正的论证报告及市场调研报告，协助客户进行市场分析、技术选择、项目论证、投资决策
IDC	指	国际数据公司，全球著名信息技术、电信行业和消费科技市场咨询、顾问和活动服务专业提供商。IDC帮助IT专业人士、业务主管和投资机构制定以事实为基础的技术采购决策和业务发展战略，在IT领域的市场跟踪数据已经成为行业标准
Frost&Sullivan	指	弗若斯特沙利文咨询公司，全球最大的企业增长咨询公司，帮助客户加速企业成长步伐，取得行业内成长、创新、领先的标杆地位
Forrester	指	是一家国际知名的独立的技术和市场调研公司，针对技术给业务和客户所带来的影响提供务实和具有前瞻性的建议。已经被公认为可信赖的咨询商。
CNVD	指	英文“China National Vulnerability Database”的缩写，指国家信息安全漏洞共享平台。是由国家计算机网络应急技术处理协调中心、联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库
CNNVD	指	英文“China National Vulnerability Database of Information Security”的缩写，指中国国家信息安全漏洞库，隶属于中国信息安全测评中心，是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设运维的国家级信息安全漏洞库
态势感知	指	是一种基于环境的、动态、整体地洞悉安全风险的能力，以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式
APT/高级威胁	指	英文“Advanced Persistent Threat”的缩写，是指高级持续性威胁，本质是针对性攻击。利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式
UTM	指	英文“Unified Threat Management”的缩写，指统一威胁管理，是由硬件、软件和网络技术组成、集成多种安全功能的网关设备，能帮助用户以最便捷的方式实现防火墙、防病毒、入侵防御等功能需求
OCR	指	英文“Optical Character Recognition”的缩写，光学字符识别，指电子设备检查纸上打印的字符，通过检测暗、亮的模式确定其形状，然后用字符识别方法将形状翻译成计算机文字的过程
区块链	指	是一种共享数据库，存储于其中的数据或信息，具有“不可伪造”“全程留痕”“可以追溯”“公开透明”“集体维护”等特征。基于这些特征，区块链技术奠定了坚实的“信任”基础，创造了可靠的“合作”机制

深度学习	指	深度学习（DL, Deep Learning）是机器学习（ML, Machine Learning）领域中一个新的研究方向，它被引入机器学习使其更接近于最初的目标——人工智能。它的最终目标是让机器能够像人一样具有分析学习能力，能够识别文字、图像和声音等数据
神经网络	指	人工神经网络（Artificial Neural Networks，简称为 ANNs）也简称为神经网络（NNs）或称作连接模型（Connection Model），它是一种模仿动物神经网络行为特征，进行分布式并行信息处理的算法数学模型
第三代安全引擎	指	在网络普及之前的单机时代，安全引擎主要是基于黑特征匹配技术来实现，称为第一代安全引擎； 进入互联网时代之后，为了应对瞬息万变的安全形势，安全引擎开始转变为基于白名单匹配技术来实现，对系统及正规公司采用默认的信任机制，称之为第二代安全引擎； 随着漏洞、后门的泛滥，及 APT 攻击的盛行，安全行业时代进入到国家安全时代，而为解决漏洞、后门、可信程序作恶等问题而研发的新引擎被称之为第三代安全引擎
零信任	指	零信任架构是一种网络/数据安全的端到端的方法，提供一系列概念、理念、组件及其交互关系，以便消除针对信息系统和服务进行精准访问判定所存在的不确定性。零信任的技术本质是以身份为基石的动态可信访问控制，聚焦身份、信任、业务访问和动态访问控制等维度的安全能力，基于业务场景的人、流程、环境、访问上下文等多维的因素，对信任进行持续评估，并通过信任等级对权限进行动态调整，形成具备较强风险应对能力的动态自适应的安全闭环体系
安全资源池	指	在云环境中，由各种虚拟形态或物理形态的网络安全能力或设备所组成的，可以被统一部署、管理、调度，以软件定义及服务化方式实现特定安全能力的逻辑资源集合
防火墙/Firewall	指	设置在不同网络或网络安全域之间的一系列部件的组合。可通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以此来实现网络的安全保护
防病毒/AV	指	英文“Anti Virus”的缩写，通过计算机病毒特征发现并及时清除病毒，防止对计算机和网络的破坏
病毒	指	Virus，这里特指计算机病毒，是编制者在计算机程序中插入的破坏计算机功能或者破坏数据、影响计算机使用并且能够自我复制的一组计算机指令或者程序代码
后门	指	在网络安全行业，后门（backdoor）一般是指那些绕过安全性控制而获取对程序或系统访问权的程序方法
窃密木马	指	以窃取敏感秘密信息为目的木马
远控木马	指	以达成对设备进行远程控制为目的的木马

钓鱼网站	指	一种网络欺诈行为，指不法分子利用各种手段，仿冒真实网站的 URL 地址以及页面内容，或者利用真实网站服务器程序上的漏洞在站点的某些网页中插入危险的 HTML 代码，以此来骗取用户银行或信用卡账号、密码等私人资料
黑链/暗链	指	看不见但却被搜索引擎计算权重的外链
挂马	指	黑客通过各种手段修改网站页面的内容，向页面中加入恶意代码的行为
挖矿	指	将一段时间内区块链系统中发生的交易进行确认，并记录在区块链上形成新区块的过程
勒索软件	指	勒索软件（ransomware）是一种流行的木马，通过骚扰、恐吓甚至采用加密绑架用户文件等方式，使用户数据资产或计算资源无法正常使用，并以此为条件向用户勒索钱财
虚拟化	指	计算机元件在虚拟的基础上而不是真实的基础上运行，如服务器虚拟化、桌面虚拟化、存储虚拟化等
容器	指	一种内核轻量级的操作系统层虚拟化技术
Openstack	指	由 NASA 和 Rackspace 合作研发的，开源的云计算管理平台
分布式拒绝服务攻击	指	借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDoS 攻击，从而成倍地提高拒绝服务攻击的威力
AR	指	英文“Augmented Reality”的缩写，增强现实技术（AR）是一种将虚拟信息与真实世界巧妙融合的技术，广泛运用了多媒体、三维建模、实时跟踪及注册、智能交互、传感等多种技术手段
VR	指	英文“Virtual Reality”的缩写，虚拟现实技术（VR）是一种可以创建和体验虚拟世界的计算机仿真系统，它利用计算机生成一种模拟环境，使用户沉浸到该环境中
SIEM	指	英文“Security Information and Event Management”的缩写，是指安全信息和事件管理
HTTPS	指	英文“Hyper Text Transfer Protocol over SecureSocket Layer”的缩写，是以安全为目标的 HTTP 通道，在 HTTP 的基础上通过传输加密和身份认证保证了传输过程的安全性
TLS	指	英语“Transport Layer Security”的缩写，用于在两个通信应用程序之间提供保密性和数据完整性，前身是 SSL
Web	指	现广泛被译作网络、互联网，表现为三种形式，即超文本（hypertext）、超媒体（hypermedia）、超文本传输协议（HTTP）等
RESTful	指	RESTFUL 是一种网络应用程序的设计风格 and 开发方式，基于 HTTP，可以使用 XML 格式定义或 JSON 格式定义

JSON	指	英文“JavaScript Object Notation”的缩写，即 JS 对象简谱，是一种轻量级的数据交换格式
WebSocket	指	WebSocket 是一种在单个 TCP 连接上进行全双工通信的协议
SecOS	指	是指一个自主产权的安全操作系统
URL	指	英文“Uniform Resource Locator”的缩写，指统一资源定位符，是互联网上标准资源的地址
SaaS	指	英文“Software as a Service”的缩写，指软件即服务
DDoS	指	英文“Distributed Denial of Service”的缩写，即分布式拒绝服务
IT	指	英文“Information Technology”的缩写，是主要用于管理和处理信息所采用的各种技术的总称。它主要是应用计算机科学和通信技术来设计、开发、安装和实施信息系统及应用软件
IP	指	英文“Internet Protocol”的缩写，分配给用户上网使用的网际协议
IPv4	指	英文“Internet Protocol Version 4”的缩写，即互联网协议第 4 版
IPv6	指	英文“Internet Protocol Version 6”的缩写，即互联网协议第 6 版。是互联网工程任务组（IETF）设计的用于替代 IPv4 的下一代 IP 协议
IOC	指	英文 “Indicator Of Compromise”的缩写，通常被翻译为中文的入侵指示器、失陷指标、失陷指示器等，其作为识别是否已经遭受恶意攻击的重要参照特征数据，通常包括主机活动中出现的文件、进程、注册表键值、系统服务以及网络上可观察到的域名、URL、IP 等
IDS	指	英文“Intrusion Detection Systems”的缩写，指入侵检测系统，能依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性
IPS	指	英文“Intrusion Prevention System”的缩写，指入侵防御系统，能通过检查网络数据包并确定其真正用途，来检测并阻断攻击网络的恶意通信
ABAC	指	英文“Attribute-Based Access Control”的缩写，指基于属性的访问控制，是一种为解决行业分布式应用可信关系访问控制模型,它利用相关实体(如主体、客体、环境)的属性作为授权的基础来研究如何进行访问控制
RBAC	指	英文“Role-Based Access Control”的缩写，指基于角色的访问控制。在 RBAC 中，权限与角色相关联，用户通过成为适当角色的成员而得到这些角色的权限
NAT	指	英文“Network Address Translation”的缩写，指网络地址转换

Session	指	会话，在用户（或用户代理）端和服务器端之间建立关联，从而起到交换数据包的作用机制
ALG	指	英文“Application Layer Gateway”的缩写，指应用层网关，主要完成对应用层报文的处理，在与 NAT(Network Address Translation, 网络地址转换)、ASPF (Application Specific Packet Filter, 基于应用层状态的包过滤) 配合使用的情况下，可以实现地址转换、数据通道检测和应用层状态检查的功能。
QoS	指	“Quality of Service”，服务质量。指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力，是网络的一种安全机制，是用来解决网络延迟和阻塞等问题的一种技术
CPE	指	英文“Customer Premise Equipment”的缩写，是指客户侧设备
MapReduce	指	是一种编程模型，用于大规模数据集（大于 1TB）的并行运算
CPU	指	英文“Central Processing Unit”的缩写，即中央处理器。是一块超大规模的集成电路，一台计算机的运算核心和控制核心
MIPS	指	MIPS 技术公司推出的一种微型处理器
ARM	指	英文“Acorn RISC Machine”的缩写，一种微型处理器
磁盘 IO	指	磁盘的输入和输出(Input 和 Output 的缩写)
PoC	指	英文“Proof of Concept”的缩写，是业界流行的针对客户具体应用的验证性测试，根据用户对采用系统提出的性能要求和扩展需求的指标，在选用服务器上进行真实数据的运行，对承载用户数据量和运行时间进行实际测算，并根据用户未来业务扩展的需求加大数据量以验证系统和平台的承载能力和性能变化
SDN	指	英文“Software Defined Network”的缩写，是指软件定义网络

注：本上市保荐书若出现总数数值与各分项数值之和尾数不符的情况，为四舍五入原因造成。

第一节 本次证券发行基本情况

一、发行人基本情况

(一) 基本情况

公司名称:	奇安信科技集团股份有限公司
英文名称:	Qi An Xin Technology Group Inc.
注册资本:	57,767.4421 万元
法定代表人:	齐向东
有限公司成立日期:	2014 年 6 月 16 日
股份公司变更日期:	2019 年 5 月 31 日
注册地址:	北京市西城区新街口外大街 28 号 102 号楼 3 层 332 号
邮政编码:	100088
电话号码:	010-56509199
传真号码:	010-56509199
互联网网址:	https://www.qianxin.com/
电子信箱:	ir@qianxin.com
信息披露部门:	董事会办公室
信息披露部门负责人:	马勒思
信息披露部门电话号码:	010-56509139
本次证券发行的类型:	首次公开发行股票并在科创板上市

(二) 主营业务情况

公司专注于网络空间安全市场，主营业务为向政府、企业客户提供新一代企业级网络安全产品和服务。凭借持续的创新研发和以实战攻防为核心的安全能力，公司已发展成为国内领先的基于大数据、人工智能和安全运营技术的网络安全供应商。

公司面向新型基础设施建设、面向数字化业务，运用系统工程的方法论结合“内生安全”思想，将新一代网络安全框架作为顶层设计指导，以“数据驱动安全”为技术理念、以打造网络安全颠覆性和非对称性能力为目标、以“人+机器”协同运营为手段，创建了面向万物互联时代的网络安全协同联动防御体系。公司

针对云计算、大数据、物联网、移动互联网、工业互联网和 5G 等新技术下产生的新业态、新业务和新场景，为政府与企业等机构客户提供全面、有效的网络安全解决方案。

公司及核心产品和服务的技术和市场影响力获得了国内外市场研究机构的认可，主要产品和服务市场份额位居行业前列。主要标志性事件如下表所示：

标志性事件	来源	时间
公司入选全部 15 个一类、71 个二级分类安全领域，成为入围网络安全全景图细分领域最多的企业	安全牛	2020 年
2019 年北京民营企业科技创新百强第 5 名	北京市工商业联合会	2019 年
Gartner 亚太区防火墙魔力象限核心厂商（2019 年）	Gartner	2019 年
中国态势感知解决方案领导者企业	IDC	2019 年
“2018 年度中国网络安全 100 强企业”领导者	安全牛	2019 年
“2018 年赛迪网络安全潜力企业榜 80 强”第一名	赛迪咨询	2019 年
2018-2019 中国网络信息安全年度成功企业奖	赛迪咨询	2019 年
2018-2019 中国网络信息安全市场年度成长最快奖	赛迪咨询	2019 年
“云安全管理平台”被评为 2018-2019 中国网络信息安全市场年度优秀产品	赛迪咨询	2019 年
“虚拟化安全管理系统”被评为 2018-2019 中国网络信息安全市场年度优秀产品	赛迪咨询	2019 年
“天机 TrustSpace 安全工作空间”被评为 2018-2019 中国网络信息安全市场年度创新产品奖	赛迪咨询	2019 年
2018 年度中国区 Web 安全（SaaS）市场领导者奖	FROST&SULLIVAN	2019 年
“内部威胁敏感的高可信云服务关键技术及应用”项目获得科技进步一等奖	中国电子学会	2019 年
Gartner 亚太区防火墙魔力象限核心厂商（2018 年）	Gartner	2018 年
中国威胁情报安全服务市场领导者	IDC	2018 年
中国威胁情报市场领导者	安全牛	2018 年
中国态势感知解决方案领导者企业	IDC	2018 年
态势感知实力矩阵规模第一	安全牛	2018 年
“终端安全管理系统”被评为 2017-2018 中国网络信息安全市场年度最佳解决方案	赛迪咨询	2018 年
“态势感知项目”被评为 2017-2018 中国网络信息安全市场年度最佳解决方案	赛迪咨询	2018 年
“安全服务”被评为 2017-2018 中国网络信息安全市场年度创新产品	赛迪咨询	2018 年
“新一代智慧防火墙”被评为 2017-2018 中国网络信息安全市场年度创新产品	赛迪咨询	2018 年
2018 年度终端安全市场份额第一	赛迪咨询	2018 年

标志性事件	来源	时间
2018 年度安全管理平台市场份额第一	赛迪咨询	2018 年
2018 年度云安全市场份额第一	赛迪咨询	2018 年
2018 年度安全服务市场份额第一	赛迪咨询	2018 年
2018 年度终端安全软件市场份额第一	IDC	2018 年
2018 年 Web 安全市场份额第二	赛迪咨询	2018 年
2018 年 UTM 市场份额第二	赛迪咨询	2018 年
2018 年安全内容管理硬件市场份额第二	IDC	2018 年
2017 年入围 Gartner 终端防护平台魔力象限	Gartner	2017 年
2017 年度终端安全市场份额第二	赛迪咨询	2017 年
2017 年度安全管理市场份额第二	赛迪咨询	2017 年
2017 年度安全服务市场份额第二	赛迪咨询	2017 年
2017 年度 Web 安全市场份额第二	赛迪咨询	2017 年
2017 年度 UTM 市场份额第二	赛迪咨询	2017 年
2017 年度终端安全市场份额第二	IDC	2017 年
2017 年度安全内容管理市场份额第二	IDC	2017 年

（三）核心技术

发行人主要的核心技术及其技术先进性的具体情况如下：

技术类别	技术名称	技术概要	技术先进性及其具体表征	技术来源	所处阶段	相关专利	相关软件著作权	相关产品及服务
第三代安全引擎	“天狗”第三代安全引擎	引擎基于内存指令层的漏洞攻击检测技术，融合了机器学习等AI技术，脱离了对具体漏洞特征、文件特征、行为特征的依赖，解决技术的对 0Day 漏洞、可信程序被恶意利用、以及后门的检测方面的安全问题。	引擎基于内存指令层的漏洞攻击检测技术，融合了对具体漏洞特征、文件特征、行为特征的依赖，没有传统的白名单、黑特征概念。能有效防御针对终端的漏洞攻击行为，在断网情况下，也不影响效果。引擎的安全机制不仅可以防护应用层的攻击，针对各类软硬件供应商自身存在的后门问题也可以有效发现和防御。	自主研发	已投入使用并持续优化	201910755387.4 201910755388.9 201910755389.3 201910755390.6 201910755419.0 201910755420.3 201910755436.4 201910755437.9 201910755438.3 201910755440.0 201910755441.5 201910755442.X 201910755443.4 201910755444.9 201910755445.3 201910755461.2 201910755464.6 201910755465.0 201910755466.5 201910755467.X 201910755476.9 201910755481.X 201910755841.6 201910755844.X 201910755846.9 201910755848.8 201910755850.5 201910755851.X 201910755854.3 201910755855.8 201910755856.2	奇安信天狗第三代安全引擎软件[简称：奇安信天狗]V1.0（2020SR0369280）	泛终端安全防护、云计算安全防护

技术类别	技术名称	技术概要	技术先进性及其具体表征	技术来源	所处阶段	相关专利	相关软件著作权	相关产品及服务
						201910755857.7 201910755858.1 201910755859.6 201910755861.3 201910755864.7 201910755865.1 PCT/CN2019/105747 PCT/CN2019/100898 PCT/CN2019/100899		
终端识别检测技术	基于主动扫描和网络行为学习的终端识别技术	采用端口探查、协议分析、指纹识别等主动扫描技术并结合基于深度学习的设备行为相似性模型算法,实现设备准确识别。	1、从多个维度获取设备的特征,通过终端特征大数据分析引擎,提高终端类型和身份等的识别精度; 2、通过终端网络流量机器学习引擎,对终端行为进行建模,准确鉴别终端的网络特征和行为。	自主研发	已投入使用并持续优化	201710431772.4 201710434206.9	奇安信网神网络安全准入系统 V8.0 (2019SR0986029)	终端安全准入系统
新一代反病毒特征引擎	“猫头鹰”(QOWL)多功能跨平台反病毒特征引擎	“猫头鹰”(QOWL)反病毒引擎通过深度解析待扫描文件元数据,提取元数据及其他静态特征,组合成特定的序列,进行查杀毒匹配。	QOWL引擎是一款多功能特征引擎,包含APT样本聚类、检测、查杀毒等功能,采用不同的调度器可实现不同的功能。 QOWL引擎同时支持Windows、Linux、Mac及国产化操作系统,同时支持x86、mips、arm等多种CPU架构。通过模块化、病毒库细分、前置过滤条件匹配等手段,有效降低磁盘IO、CPU占用,大幅提升文件扫描速度,且精准度高,基本无误报。	自主研发	已投入使用并持续优化	ZL201510671125.1 ZL201510669982.8 201910346162.3 201910345206.0 201910346170.8 201910345232.3 201910345213.0 202010151746.8 202010143686.5 202010151740.0 202010144181.0	“猫头鹰”(QOWL)多功能跨平台反病毒特征引擎[简称:QOWL反病毒引擎]软件 V1.0 (2020SR0375110)	泛终端安全防护、云计算安全防护
新一代终端安全防御技术	基于行为和机器学习的终端安全防御技术	根据行为特征识别和拦截勒索、挖矿等病毒的恶意行为,基于终端的静态属性和动态行为数据,采用关联分析和AI技术进行未知威胁的分析和挖掘,配合后端	该技术结合云端安全技术和后端安全运营能力,可快速发现和拦截新型病毒的恶意行为,能够实时捕获未知样本和新型病毒,快速发现和拦截新出现的恶意程序的恶意行为。	自主研发	已投入使用并持续优化	201811646037.6 201811625858.1	奇安信终端安全管理系统 V8.0(2019SR0676840)	终端安全管理系统

技术类别	技术名称	技术概要	技术先进性及其具体表征	技术来源	所处阶段	相关专利	相关软件著作权	相关产品及服务
		运营的威胁情报可快速发现可疑行为并产生告警。						
基于云架构的安全扫描与监测技术	网站资产安全监测	网站监测引擎集群具有支持10万个以上网站并行扫描检测的能力,能够支持多种网站违规、漏洞隐患、网站可用性和未知资产发现的检测。	1、监测量大:能够支持10万以上网站的云端并行扫描检测能力; 2、监测项齐全:包含漏洞,暗链,篡改,违规内容,敏感信息,钓鱼,挂马,可用性,坏链,图片涉黄,图片涉赌,未知资产发现等十多项检测能力; 3、监测结果准确:暗链准确率在85%以上,违规内容准确率在75%以上。	自主研发	已投入使用并持续优化	201811561726.7 201811562767.8 201811598646.9 201811597967.7 201811640585.8 201811653703.9 201910945459.1 201910945443.0 201910943899.3	奇安信全球鹰网站云监测系统[简称:云监测]V5.0(2019SR1019876)	SaaS智能安全防护
	基于机器学习技术用于违规信息的检测	具有基于机器学习模型的违规文本检测能力,基于神经网络的双模型分类,分别使用网页全部文字和敏感字附近上下文的部分问题进行分类,克服了单一模型可能出现的偏差,提高了准确度;具有基于机器学习模型的涉黄图片检测能力,使用神经网络对样本文件训练,提高了准确度。	基于机器学习的违规信息检测,可同时检测文本和图像信息。其中,文本分类采用双模型验证,提高了检测的准确率,总检测准确率在75%以上。	自主研发	已投入使用并持续优化	201811631620.X 201811653926.5 201910945463.8	奇安信全球鹰网络空间安全态势感知平台V2.4(2020SR0076218)	SaaS智能安全防护
海量数据实时处理技术	新一代大数据流式关联分析引擎	是用于大数据流式分析的核心技术引擎,主要用于海量数据的实时分析,通过对系统或设备日志、网络流量日志、客户资产、漏洞和威胁情报等各类数据进行复杂的关联分析来生成实时的告警信息,以帮助网络管理员对网络安全事件作出快速的处置和响应。	对标国际领先厂商,并根据国内大数据安全运营领域的业务需求做了大量优化,具有完善的SIEM安全检测语义,突破了传统关联引擎无法分布式部署以及无法在大数据平台上部署和扩展的局限性。	自主研发	已投入使用并持续优化	201910252081.7 201910308704.8 201910309202.7 201910252103.X 201910309190.8 201910252111.4 201910253184.5 201910253186.4 201910252093.X 201910252105.9	奇安信网神安全分析与管理系统V4.0(2016SR401409)	大数据智能安全分析与监测

技术类别	技术名称	技术概要	技术先进性及其具体表征	技术来源	所处阶段	相关专利	相关软件著作权	相关产品及服务
网络安全与攻击检测技术	威胁检测技术	是一种通过对网络流量进行网络威胁检测和发现的技术。能够识别勒索软件、网络蠕虫、窃密木马、远控木马等恶意网络攻击行为，能够区分攻击成功与失败，并计算出攻击链。结合云端威胁情报，对于高级威胁也具备检测能力。	网络攻击威胁检测技术自主可控，基于云端大数据的威胁情报能力以及多年积累的恶意流量特征库和检测手段，具备在复杂流量情况下的威胁检测能力。	自主研发	已投入使用并持续优化	201710667103.7 201710668128.9 201710707596.2	奇安信天眼新一代威胁感知系统[简称：奇安信天眼]V3.0（2014SR119793）	大数据智能安全分析与监测
网络安全与大数据分析建模技术	多维可视分析技术	是一种针对海量数据的分析和可视分析技术，通过对海量异构数据做关联分析发现线索，从而洞察数据之间的联系，发现攻击组织及攻击线索。	1、具有通过海量异构数据关联分析技术及可视化技术还原技术构建攻击图谱及对攻击进行溯源分析的能力，在公司拥有的国内使用环境的海量数据和威胁情报支撑下，可准确发现攻击组织及攻击线索； 2、公司多次参与IEEE VAST挑战赛并获奖。	自主研发	已经投入并持续优化	201710707596.2	数据可视化关联分析系统V2.0（2017SR421760）	大数据智能安全分析与监测
云上安全管理与编排技术	安全资源池技术	支持虚拟化安全设备生命周期管理、编排管理和配置管理；支持多个云平台的对接，包括租户对接、用户对接和资产对接；支持云平台资产和云安全组件统一编排；还可以对接云端威胁情报，通过安全资源池的检测和防护能力，实现数据驱动的自适应云安全体系架构。	1、采用安全资源池技术，实现安全设备云化交付； 2、采用SDN思想，定义安全控制器，实现安全控制平面和安全防护平面分离，同时实现安全统一配置和自动化编排，提升安全运维和安全运营效率。	自主研发	已投入使用并持续优化	201811405774.7 201811405769.6 201811412893.5 201811406680.1 201811633529.1 201811579212.4	奇安信网神云安全管理平台软件 V2.0（2016SR399552）	云安全管理平台
基于云工作负载保护的云计算基础	虚拟化无代理文件防御技术	1、为云计算和虚拟化环境的虚拟机文件系统提供安全防护，将虚拟机的防病毒等安全检测模块移到虚拟机外部，在每台虚拟化宿主	1、采用无代理部署模式，支持虚拟化平台（KVM、Xen等）及容器技术，以实现虚拟机/容器的防恶意软件等安全功能； 2、在虚拟机资源开销上，相对于传	自主研发	已投入使用并持续优化	201911424792.4 202010023073.8	奇安信网神统一服务器安全管理系统[简称：奇安信统一服务器安全]V8.0(2019SR0941258)	虚拟化安全管理系统

技术类别	技术名称	技术概要	技术先进性及其具体表征	技术来源	所处阶段	相关专利	相关软件著作权	相关产品及服务
架构安全		机上仅部署一套安全组件就可以为宿主机上的所有虚拟机提供病毒防护能力，无需在虚拟机内部安装客户端软件； 2、该系统可降低虚拟机整体资源消耗，提高虚拟机部署密度，同时实现统一资源调度，避免病毒扫描风暴。	统的在虚拟机中部署安全客户端的方案，无代理部署模式整体资源占用更小，从而可以增加虚拟机部署密度； 3、在文件的查杀效率上，经过虚拟化层特有的优化，可以利用缓存技术加快对虚拟机上相同文件的扫描，提升查杀效率。					
	虚拟化无代理网络入侵防御技术	1、为云计算和虚拟化环境的虚拟机网络提供安全防护，将虚拟机的防火墙及入侵防御等安全检测模块部署到宿主机上，仅一套安全组件就可以为宿主机上的所有虚拟机提供网络防护能力，无需在虚拟机内部安装客户端软件。 2、利用深度包检测技术，对网络报文进行流量还原并进行应用协议识别，从而更精确的对恶意流量进行识别并拦截。实现虚拟补丁功能，在服务器不打实体补丁的情况下，依然可以拦截对系统及应用漏洞利用的网络入侵攻击。	1、利用虚拟化层核心技术，在虚拟机与虚拟交换机之间截获网络流量，对流量进行深度包检测并进行协议还原，以精确识别恶意攻击；该技术无需依赖其他SDN导流方案； 2、可以同时实现对虚拟机的东西向流量和南北向流量进行检测。	自主研发	已投入使用并持续优化	202010034035.2 201811109057.X	奇安信网神统一服务器安全管理系统[简称：奇安信统一服务器安全]V8.0(2019SR0941258)	虚拟化安全管理系统
零信任身份安全	可信应用代理技术	用于零信任用户访问业务场景的数据平面代理。通过高性能的专业TLS传输技术，实现业务流量的加密传输；通过三层、四层、七层	通过高性能的TLS转发引擎配合水平扩展能力，可以用于大型客户场景的安全访问平台；三层、四层、七层的代理转发能力可以满足各类业务场景；应用兼容性支持不可改造的老	自主研发	已投入使用并持续优化	201910694093.5 201910322523.0 201911415849.4 201911416505.5 201911416395.2	应用代理系统软件[简称：TAP]V5.0(2018SR1078320)	零信任身份安全

技术类别	技术名称	技术概要	技术先进性及其具体表征	技术来源	所处阶段	相关专利	相关软件著作权	相关产品及服务
		代理传输技术实现各类业务场景的流量代理；通过多层令牌技术，实现零信任和业务系统之间的信任传递；通过全流量日志导出能力，实现流量的可视化。	旧应用代理。					
	可信API代理技术	用于零信任数据API交换场景的数据平面代理。通过高性能的专业TLS传输技术，实现API流量的加密传输；通过应用层代理实现RESTful/WebService/MQTT等各类协议的API代理转发；通过多层令牌技术，实现零信任和业务系统之间的信任传递；通过全流量日志导出能力，实现流量的可视化。	通过高性能的TLS转发引擎配合水平扩展能力，可以用于大型客户场景的安全访问平台；主流API协议满足各种不同的数据交换场景；可扩展的多层令牌技术实现信任传递的纵深防御。	自主研发	已投入使用并持续优化	201910693985.3 201910322763.0 201911414669.4	API代理系统软件[简称：TIP]V5.0(2018SR1077792)	零信任身份安全
	零信任动态可信访问控制技术	零信任专用控制平面技术，实现零信任特有的动态访问控制和信任评估能力。采用RBAC+ABAC的授权模型实现灵活、风险感知的权限基线管理；通过持续信任评估计算信任等级，结合业务安全等级实现分级访问控制；通过环境风险感知对访问权限进行实时调整。	以RBAC+ABAC为基础进行优化，遵循零信任理念实现的分级访问控制能力，实现风险感知的最小权限授权；采用大数据和机器学习技术，基于人、设备构建的访问主体，充分考虑其安全属性和访问行为，结合外部风险感知输入，构造信任评估模型，对访问主体进行信任等级的计算。	自主研发	已投入使用并持续优化	201910693984.9 201910693982.X 201910322762.6 201911415231.8 201911421740.1 201911417478.3 201911421731.2 201911415388.0 201911421999.6	身份服务系统[简称：TAC]V5.0(2019SR0747471)	零信任身份安全
网络流量攻击的分布式对抗技术	DDoS攻击分布式检测防护	以多层分布式的系统架构对分布式拒绝服务攻击的数据进行收集、分析、统计及处理，在不同层面实现不同功能、不同粒度的检测防	基于多级分布式架构，系统可实现对DDoS攻击的实时检测与防护；基于MapReduce思想对检测与防护数据分层进行分析处理，即支持及时在节点内同步异常状态也支持全局的异	自主研发	已投入使用并持续优化	201710875523.4	奇安信网神WEB应用安全云防护系统[简称：奇安信网神安域]V4.0(2016SR327431)	网站安全云防护系统

技术类别	技术名称	技术概要	技术先进性及其具体表征	技术来源	所处阶段	相关专利	相关软件著作权	相关产品及服务
		护算法,使得不同层级具有一定的自主判断及决策能力,以实现秒级DDoS响应的能力。	常情况识别,最快可实现全网攻击的秒级检测及响应。					
新一代威胁检测技术	基于行为与内容的新一代威胁发现技术	对网络流量进行深度还原,使用多种机器学习模型和多种计算手段进行多维度分析,能够准确发现网络中的扫描、漏洞利用、恶意文件投递、远控等攻击行为。	可以精准发现威胁,并对攻击过程、攻击结果标签化处理,研判引擎能够根据攻击特点智能研判攻击是否成功、资产是否失陷,检测更具实时性、全面性,适用场景广泛。	自主研发	已投入使用并持续优化	201911424992.X 201911424081.7 201911425703.8 201911425741.3 201911425744.7 201911402244.1 201911406914.7	奇安信网神全流量采集系统V4.0(2020SR0097810)	新一代威胁态势感知与响应系统
新一代流量还原技术	资产识别技术	以硬件资产、操作系统、中间件、软件为核心内容,以网络协议指纹为基础,能够进行深度内容解析的实时被动资产识别技术。	基于网络标准协议、应用、行为等指纹技术进行内网资产识别,实现引擎和指纹库的分离,可以动态升级指纹库,便于运维。此外,资产识别与DPI技术深度融合,使识别更加精准。	自主研发	已投入使用并持续优化	201911422235.9 201911423185.6	奇安信网神全流量采集系统V4.0(2020SR0097810)	网络流量传感器
	应用还原技术	是基于机器学习的网络应用识别技术,具有自适应的高扩展性的动态应用还原框架,支持插件式的脚本语言应用还原,完整覆盖双边、单边、异常流量的应用还原。	通过机器学习技术精确识别通用及私有网络应用,识别范围广、精度高,为恶意流量识别大幅降低噪音;使用该技术的产品能够通过机器学习技术及海量的数据进行训练学习及不断优化纠偏,不断的提高精度。	自主研发	已投入使用并持续优化	201911422715.5 201911425691.9 201911415601.8 201911424693.6 201911424992.X 201911425724.X	奇安信网神全流量采集系统V4.0(2020SR0097810)	网络流量传感器
第四代SecOS高性能一体化引擎技术	全功能用户态协议栈技术	采用深度优化的数据收发包处理框架、高性能一体化安全处理引擎和高度统一的IPv4/v6双栈处理技术,实现系统的高性能和可高扩展性,并能提供包含IPv4/v6各种路由交换、各类NAT、隧道、session管理、ALG、QoS、抗攻击等的全功能支持。	大多数同行业厂商采用开源协议栈方案来完成安全业务的支持,一方面协议栈无法做到自主可控,存在协议栈自身安全性问题;另一方面开源协议栈并非为安全产品设计,且自身开发协议栈性能较低,无法做到更好的性能优化。通过此技术,可以实现更高的运行效率。	自主研发	已投入使用并持续优化	201911402221.0	奇安信网神防火墙系统V6.0(2020SR0308936)	新边界安全防护

技术类别	技术名称	技术概要	技术先进性及其具体表征	技术来源	所处阶段	相关专利	相关软件著作权	相关产品及服务
	高度统一的IPv4和IPv6双栈融合技术	采用高度统一的双栈融合技术，解决了底层网络基础通信模块和高级安全应用处理模块之间的强耦合，做到了整个架构和安全处理流程的双栈统一。利用该技术，高级应用安全能力可以适用广泛的不同的双栈接入场景。	大多数厂商均采用开源协议栈方案来完成安全业务的支持，其中IPv4和IPv6处理流程完全独立，不但代码复用率低，并且在NAT64或NAT46接入环境下处理难度高，使得高级应用安全功能很难支持。此技术保证了产品在不论是在IPv4还是IPv6网络接入环境中都具有高度的网络适应性，同时两者性能不会超过5%的差距。	自主研发	已投入使用并持续优化	201911424160.8	奇安信网神防火墙系统V6.0（2020SR0308936）	新边界安全防护
	实时高性能日志存储与查询技术	1、采用列式查询，将用户搜索条件进行语法树转换去冗余并翻译为基于列的查询代码并通过动态编译直接用于程序匹配； 2、查询支持多种复杂可扩展的语法，支持任意层级的“优先级”匹配，支持各种“与或非”组合的逻辑表达式以及模糊搜索、范围搜索、地址段匹配等； 3、结合异步IO机制、列式匹配计算和IO异步读取并行，依靠高IO压缩比实现高性能的日志查询。	同行业大部分厂商在网关产品这种资源极其有限的系统里，都没有十分有效的方法来实现高性能的日志写入、查询、聚合。通过此技术，克服了上述问题，实现了实时高性能的日志存储与查询。	自主研发	已投入使用并持续优化	201810050152.0	奇安信网神防火墙系统V6.0（2020SR0308936）	新边界安全防护
	一体化流量编排技术	接管网络流量，并基于网元（虚拟化网元或物理网元）对流量的业务需求，多条件精细化的将流量编排给多个业务网元处理，业务网元流量处理并返回后，进行统一的外发处理。	国内大多数同行业厂商采用openstack开源方案，网络接入能力差、性能低、无法做到精细化流量编排。使用该技术，可以实现与同行业其他厂商相同硬件配置条件下，提高性能，并实现强大的网络接入和精细化流量编排。	自主研发	已投入使用并持续优化	201911424631.5 201911424500.7 201911425207.2 201911422712.1 201911422789.9 201911424834.4	奇安信网神防火墙系统V6.0（2020SR0308936）	新边界安全防护
大数据	3D地理	该技术是基于GIS体系与高	1、支持多端运行，支持各类浏览器、	自主研	已投入使用	201710707596.2 ZL201410856952.3	3D地理空间可视化与可视	新一代IT基

技术类别	技术名称	技术概要	技术先进性及其具体表征	技术来源	所处阶段	相关专利	相关软件著作权	相关产品及服务
可视化技术与3D图形技术	空间可视化与可视分析引擎	性能游戏渲染引擎驱动的3D可视化平台，由3D地图引擎、2D/3D图表及UI组件数据接入与处理等核心组件构成，其中，3D地图引擎使用全国矢量二进制地理数据，是基于GIS体系与高性能游戏渲染引擎的实时3D可视化引擎。该平台能够展示包括2D图表、3D图表、3D场景组件、3D模型组件、3D特效组件、城市环境模拟、自然环境模拟等多种场景和状态；能够支持WebSocket接口、Restful接口、JSON文件、CSV文件等多种接入方式及接口；能够支持多源异构的数据同时接入与处理；还能支持包括常规键盘鼠标及Pad、AR、VR等远程控制的多种交互模式。	Windows客户端、Android系统等，兼容性良好； 2、多端互动支持，包括Pad、AR设备、VR设备等； 3、混合运行支持，例如可以通过在Windows客户端内置CEF定制浏览器运行网页； 4、具有超高分辨率支持能力，目前测试最高能支持8K的分辨率； 5、可将全国的矢量地图数据加密和压缩至不超过5G大小，支持离线部署和更新，提高了便利性； 6、多规格、多种类、多格式的3D建模与特效动画可与地理空间结合，具有自然的可视化效果； 7、内置多种组件及案例，可高效快速的搭建与定制可视化系统。	发	并持续优化		分析引擎软件 V1.0.01 (2020SR0369281)	基础设施防护产品体系、大数据智能安全监测与管控体系
新一代用户行为分析技术	用户行为分析技术	基于海量用户行为日志，通过基线分析、同组分析、用户画像、机器学习等手段，检测异常行为和异常用户，应用于数据泄露、账号异常、业务违规等场景分析。	可以同时针对多种日志源，综合使用规则、基线、概率、大数据异常算法等多种分析手段，从多个维度评估用户的风险情况，并使用风险分数合并呈现。	自主研发	已投入使用并持续优化	201710138260.9 ZL201610344784.9 ZL201510742786.9	用户行为分析系统[简称：UBA] V2.0(2017SR581483)	大数据智能安全分析与监测
第三代数据泄漏防护技术	基于AI的数据分类分级技术	基于机器学习技术处理文档的分类、源码文件的类型识别，具有比传统方案更高的识别准确度，可以检测出	使用人工智能技术进行敏感文档的分类分级处理及识别源程序类型，解决了传统方案无法实现高正确率识别源码语言类型的问题，对各种编程	自主研发	已投入使用并持续优化	201811450760.7 201811462678.6	奇安信网神数据防泄漏系统V6.0(2020SR0193361)	数据安全防护

技术类别	技术名称	技术概要	技术先进性及其具体表征	技术来源	所处阶段	相关专利	相关软件著作权	相关产品及服务
		传统方法容易误判的不能识别的目标或类型。基于文件指纹对文档内容进行语句级匹配检测处理。	语言的源代码类型进行精确的语言特征级别的识别。文件指纹技术可以对数据片段进行精确处理，支持语句级匹配检测处理。					
应用安全技术	源代码安全缺陷分析技术	立足于源代码静态分析技术，具体包括代码中间表示技术、数据流分析技术、符号执行技术等。	在传统的静态分析技术基础上，采用了针对数据编码过滤等安全相关API的建模分析、基于全路径约束求解剪枝算法的数据流分析、基于高精度语法的语义结构分析、基于动态替换的指针别名分析等特色技术，在保证检测的深度和覆盖度的同时，有效地减少了误报的产生。	自主研发	已投入使用并持续优化	ZL201610720865.4 ZL201610721116.3 ZL201610720863.5 ZL201610721120.X ZL201610720861.6 201811625048.6 201811636917.5 201811627973.2	奇安信网神代码卫士系统【简称：代码卫士】V7.0（2019SR1137229）	代码卫士
	软件成分分析技术	通过软件成分分析，可以识别软件代码中使用了哪些开源软件以及开源软件间的关联关系，自动生成开源软件信息清单。	1、从多种多样的数据来源收集开源软件的海量信息，包括软件名称、描述、许可协议、供应商、源代码、提交历史、安全漏洞等； 2、具有开源软件成分分析识别技术，采用多层次的软件依赖分析、高效的软件指纹分析等检测技术，能够对软件中所使用的开源成分进行精确识别； 3、具有开源软件关联分析技术，对收集来的海量信息，进行深度关联及依赖分析，进而找出开源软件引入的安全风险或隐患。	自主研发	已投入使用并持续优化	201811627959.2 201811627933.8	奇安信网神开源卫士系统【简称：开源卫士】V2.0（2019SR0669658）	开源卫士

（四）研发水平

公司一直以来都高度重视研发及创新，为了确保公司在安全攻防与对抗技术、终端安全防御技术、大数据与安全智能技术、安全运营与应急响应技术方面的领先优势，公司已经建立了一整套可行有效的技术与产品创新机制。

1、健全的研发机构设置

公司采用产品开发组织及平台研发组织与技术管理组织并存且互相协同的研发体系设置，通过采用“产品（项目）开发+平台研发”的“横向”分层组织设置，覆盖公司业务开展中的研发场景；通过专业委员会“纵向”技术管理的组织设置；加强公司各类产品、安全、工程技术能力建设。两者形成“纵横”协同，保证了公司研发体系有序运作，能够极大地提高产品研发效率，缩短产品创新周期，降低产品成本，提高产品质量。

上述研发机构的设置覆盖了顶层设计到具体实施、基础平台到具体产品研发的全部过程，在公司发展过程中经历了实践的考验，已经形成了健全的研发机构体系，能够有力保障公司技术与产品的创新。此外，公司会根据市场的发展和机遇及时调整公司研发组织结构，以整合相关的研发资源抓住市场机会，提升公司竞争力。

2、持续较高的研发投入机制

公司重视技术研发创新工作，一直保持较高的研发投入支出。报告期内，公司研发费用分别为54,083.45万元、81,834.51万元和104,710.40万元，占营业收入的比例分别为65.86%、45.04%和33.20%。通过持续较高的研发投入以及多年的技术积累，目前公司掌握的一系列安全攻防与对抗技术、终端安全防御技术、大数据与安全智能技术、安全运营与应急响应技术等核心技术已处于国内领先水平。未来，公司将保持或进一步加大研发投入力度，不断改善技术创新环境与条件，提升公司研发与创新水平。

3、有效的激励创新机制

目前，公司已经形成了科学、公正的研发考核和创新激励机制。在研发考核

方面，公司建立了系统性的专业能力评估体系，对研发工程师建立了专业的技术成长体系和评估体系，能够有效激励研发人员不断成长；在创新激励方面，公司建立了“研发优先”的薪酬策略，并建立了创新专利的激励机制和制度，对专利、技术发明人给予适当的创新奖励及予以表彰。上述相关制度的实施，有效地推动了技术研发人员的工作热情与积极性，在公司内形成了良好的技术创新氛围，使得公司的创新能够不断转化为专利和产品。

4、对先进技术的持续跟踪和对安全需求的深入挖掘

网络安全的实质是安全攻防的对抗和对客户安全需求的满足，因此，公司重视对先进技术的掌握和对网络安全需求变化的把握。在先进技术方面，公司成立了专门的团队，横跨管理层至基层研发人员，对国内外网络安全领域和其他技术领域的最新发展和研发投入进行跟踪及研究；在安全需求方面，公司广泛参与了国家大型研究项目和联合实验室，主要包括“工业控制系统安全国家地方联合实验室”、“工业控制系统安全北京市工程实验室”、“网络安全监测预警关键技术北京市工程实验室”和“应对新兴威胁的高性能应用层防火墙技术北京市工程实验室”等多个国家级和省级实验室，深入了解国家、大型组织的复杂安全需求。上述措施使得公司能够持续追踪先进技术，持续了解安全需求的变化，并结合公司的资源和能力为客户提供更好的安全产品及服务。

5、“产、学、研”合作创新机制

公司十分注重“产、学、研”相结合的技术研究与开发模式的运用。公司与国内顶尖高校及研究所共建了多个研究机构，包括“清华大学-奇安信网络安全联合研究中心”、“北大-奇安信区块链安全实验室”、“中科院信工所-奇安信网络安全联合实验室”、“中科院软件所-奇安信智能软件安全研究中心”、“广州大学-奇安信云安全联合实验室”、“国科大-奇安信联合实验室”、“天津大学-奇安信网络空间安全研究院”、“哈工大（深圳）-奇安信数据安全研究院”等机构，共同开展基础理论和前沿技术研究。其中，公司与清华大学共同设立的“网络安全联合研究中心”组建的团队在2018年国际安全极客大赛上获奖。上述“产、学、研”相互结合的研发模式能够帮助公司提升技术创新效率，突破研发过程中存在的技术瓶颈问题，有效地促进了公司研发具有自主知识产权和市场竞争力的新技术、新产

品，有利于进一步巩固公司在行业中的优势地位。

（五）发行人的主要经营和财务数据及指标

根据最近三年经审计的财务报表数据，公司主要财务指标如下：

项 目	2019年12月31日	2018年12月31日	2017年12月31日
流动比率（倍）	2.03	1.67	1.35
速动比率（倍）	1.65	1.41	1.12
资产负债率（母公司）	4.16%	7.61%	55.08%
资产负债率（合并）	29.55%	36.93%	37.57%
归属于母公司股东的每股净资产（元/股）	8.69	28.75	146.30
项 目	2019 年度	2018 年度	2017 年度
应收账款周转率（次）	3.13	4.26	3.89
存货周转率（次）	2.01	1.52	0.72
资产周转率（次）	0.45	0.30	0.19
息税折旧摊销前利润（万元）	-39,079.52	-86,003.82	-63,768.68
归属于母公司股东的净利润(万元)	-49,494.47	-87,175.97	-62,985.78
归属于母公司股东扣除非经常性损益后的净利润（万元）	-68,806.33	-96,136.40	-63,994.86
研发投入占营业收入的比例	33.20%	45.04%	65.86%
每股经营活动产生的现金流量净额（元/股）	-1.93	-6.40	-23.21
每股净现金流量净额（元/股）	-0.70	5.18	25.76

注：报告期各期，归属于母公司股东的每股净资产、每股经营活动产生的现金流量净额、每股净现金流量净额数据波动较大系由于报告期内发行人进行了多次股权融资并于 2019 年完成股改，各期末股本/实收资本增长幅度较大因素所致。按股改股份数折算调整的 2017 年末、2018 年末及 2019 年末归属于母公司股东的每股净资产分别为 6.74 元/股、7.96 元/股和 8.69 元/股，按加权平均股本计算的 2017 年、2018 年及 2019 年每股经营活动产生的现金流量净额分别为-1.37 元/股、-1.95 元/股和-2.03 元/股，按加权平均股本计算的 2017 年、2018 年及 2019 年每股净现金流量净额分别为 1.52 元/股、1.58 元/股和-0.74 元/股。

上述指标计算公式如下：

流动比率=流动资产/流动负债；

速动比率=速动资产/流动负债；

资产负债率（母公司）=总负债/总资产；

资产负债率（合并报表）=总负债/总资产；

归属于母公司股东的每股净资产=期末归属于母公司股东权益/期末股本总额；

应收账款周转率=营业收入/应收账款平均余额；

存货周转率=营业成本/存货平均余额；

资产周转率=营业收入/资产总额平均余额；

息税折旧摊销前利润=利润总额+利息费用+折旧+无形资产摊销+长期待摊费用摊销；

归属于母公司股东扣除非经常性损益后的净利润=归属于母公司股东的净利润-影响归属于母公司股东净利润的非经常性损益；

研发投入占营业收入的比重=研发费用/营业收入；

每股经营活动产生的现金流量=经营活动产生的现金流量净额/期末股本总额；

每股净现金流量=现金及现金等价物净增加额/期末股本总额。

（六）发行人存在的主要风险

1、报告期内连续亏损，2020年上半年扣非后净利润大幅下滑，且未来一段时期可能持续亏损的风险

网络安全产品及技术研发需要大量投入。2017年、2018年及2019年，公司归属于母公司所有者的净利润分别为-62,985.78万元、-87,175.97万元和-49,494.47万元，扣除非经常性损益后归属于母公司所有者的净利润分别为-63,994.86万元、-96,136.40万元和-68,806.33万元，截止2019年末，公司累计未分配利润为-216,443.71万元。2020年1-3月，公司归属于母公司所有者的净利润为-54,390.85万元，扣除非经常性损益后归属于母公司所有者的净利润为-54,888.70万元，预计2020年1-6月扣除非经常性损益后归属于母公司所有者的净利润-86,336.91万元至-75,961.42万元，大幅下滑。截至本招股说明书签署日，公司尚未盈利且存在累计未弥补亏损，预计未来仍可能持续亏损。

公司持续亏损的主要原因是选择了高研发投入且人员快速扩张的发展模式，与同行业公司有所区别，为建设四大研发平台、布局“新赛道”产品、提升攻防竞争力、建立全国应急响应中心而进行了大量投入。首先，公司以“数据驱动安全”为技术理念，重点建设了四大研发平台，聚焦核心技术能力的平台化输出，为安全产品提供共性核心能力，这些研发平台的开发具有周期长、投入高的特点；其次，公司核心产品主要为网络安全领域的“新赛道”产品，开发这些产品要采用大量新技术，对研发人员能力要求高，增加了公司的研发投入；此外，公司建立了覆盖全国31个省市自治区的应急响应中心，技术支持及安全服务人员的人数超过2,500人，向客户（包含已有客户和潜在客户）提供应急响应技术服务，可以产生良好的品牌效益，为公司带来大量商机，这些投入也导致公司产生了大量销售费用。

为此，公司快速扩张了人员规模，投入了大量资金，产生了大量亏损，目前，由于规模效应仍未显现，公司存在持续亏损的风险，不能保证收入按计划增长，无法保证未来几年内实现盈利或进行利润分配，上市后亦可能面临退市的风险。具体详见本招股说明书“第四节 风险因素”之“一、公司报告期内连续亏损，2020年上半年扣非后净利润大幅下滑且未来一段时间内持续亏损的风险”。

2、公司系自三六零集团分立出来，报告期内双方存在商标、技术互相无偿授权使用等业务安排，未来双方存在竞争关系的风险

公司前身奇安信有限成立于2014年6月，原系三六零集团所控制公司。2015年12月，齐向东与周鸿祎及相关方签订了《关于360企业安全业务之框架协议》（以下简称“框架协议”），就企业安全业务从三六零集团中拆分的事宜进行了框架性约定。根据《框架协议》，2016年9月，齐向东及其控制的安源创志完成对奇安信有限增资，齐向东变更为奇安信有限的实际控制人。报告期内，根据《关于360企业安全业务之框架协议的执行协议》约定，双方存在商标、技术互相无偿授权、许可使用等业务安排。

2019年4月29日，周鸿祎、三六零科技有限公司、三六零安全科技股份有限公司、齐向东和奇安信有限签署《终止协议》，对包括商标、技术等相关终止许可事项进行了约定，同时对过渡期安排进行了约定。《终止协议》生效后，双方存在在政企网络安全领域竞争的风险。2019年度，三六零股份“安全及其他”业务收入为4.73亿元，同比增长75.15%，增量主要来源于政企安全业务。

发行人与三六零集团拆分的相关情况具体参见本招股说明“第五节 发行人基本情况”之“二、发行人设立情况”之“（三）发行人与三六零集团拆分的相关情况”相关内容。

3、销售费用占营业收入比重较高的风险

报告期各期，公司销售费用分别为43,096.71万元、80,019.86万元和111,804.88万元，销售费用占营业收入占比分别为52.48%、44.05%和35.45%，高于同行业水平，销售费用规模呈现不断扩大但占比减少的趋势。此外，报告期内，公司营销体系人数快速上升，销售人员的平均人数分别为449人、716人及

976 人，技术支持与安全服务人员的平均人数分别为 575 人、1,185 人及 2,065 人。

一方面，公司处于快速成长及品牌推广阶段，销售网络覆盖全国、销售区域分布广泛，产品线种类较多且报告期内公司进行了品牌切换，因此公司进行业务拓展及品牌推广需要大量投入；其次，公司逐步建设了覆盖全国的应急响应服务体系，并在全国各地设立了应急响应团队，以形成公司大规模服务能力，为此公司快速扩张了人员规模并投入了大量的资金。目前，公司销售体系及应急响应服务体系已基本完成，销售费用增速将逐渐放缓，随着规模效应的显现，销售费用占比预计将进一步降低。

未来，如果公司收入无法按计划增长，或者新产品市场拓展不利，公司较大的销售费用规模可能对公司的盈利产生不利影响。

4、研发投入占营业收入比重较高，持续资金需求较大的风险

2017 年、2018 年及 2019 年，公司研发费用分别为 54,083.45 万元、81,834.51 万元和 104,710.40 万元，研发费用占营业收入的比例分别为 65.86%、45.04%和 33.20%，高于同行业水平，研发费用规模呈现不断扩大但占比减少的趋势。

一方面，公司以“数据驱动安全”为技术理念，重点建设了四大研发平台，聚焦核心技术能力的平台化输出，为安全产品提供共性核心能力，包括网络操作平台、大数据操作平台、可视化操作平台以及云控操作平台，将安全产品需要的通用且核心的网络流量智能解析与调度、安全大数据存储与分析、安全可视化分析与展示及云端安全管控能力平台化、模块化，避免了新产品研发过程中核心能力的重复研发，将极大降低未来新产品的研发成本及研发周期。但是上述四大研发平台的建设具有周期较长、投入较高的特性，需要公司投入大量的时间及资金进行开发、整合及完善，导致公司报告期内研发支出较高；另一方面，公司核心产品主要为网络安全领域的“新赛道”产品，如泛终端、新边界、大数据和云计算等安全防护产品，开发这些产品要采用大量新技术，对研发人员能力要求高，增加了公司的研发投入。

目前，公司正在持续将安全产品围绕四大研发平台进行模块化改造，仍然有

一定规模的研发投入需求；此外，网络安全行业与国际形式、技术发展、威胁变化均有较强的关联性，当攻防角色、模式或技术出现重大变化时，仍然需要进行较大的研发投入，客观上公司选择的发展模式仍然存在盈利周期较长的风险。

5、毛利率下降的风险

2017 年度、2018 年度及 2019 年度，公司主营业务毛利率分别为 74.39%、55.15%及 56.69%，呈下降趋势，主要由于公司毛利率较低的硬件及其他业务收入在 2018 年和 2019 年的增长幅度相对较高，导致该期间公司主营业务毛利率水平有所下降。

2017 年、2018 年及 2019 年，公司硬件及其他业务收入分别为 2,148.34 万元、38,986.07 万元和 68,742.13 万元，占主营业务收入的比例分别为 2.67%、21.72%和 21.83%，年均复合增长率为 465.67%。2017 年、2018 年及 2019 年，公司硬件及其他业务毛利率分别为 4.92%、1.36%和 3.18%，硬件及其他业务的成本主要来自公司在系统集成性质的网络安全项目中向第三方采购的硬件，由于该等第三方硬件的市场较为成熟、价格相对透明，因此硬件及其他业务毛利率相对较低，使得该等业务收入的增长对发行人净利润贡献度较低。

此外，由于集成类项目最终客户多为政企单位，受其预算管理和集中采购制度等因素影响，付款周期较长，对公司形成营运资金占用，并使得公司应收账款增加。未来，在政企单位信息化改造以及新基建建设过程中，公司仍可能承接系统集成性质的网络安全项目，使得公司主营业务毛利率存在下降的风险。

6、应收账款金额较大的风险

报告期内，公司收入主要集中于四季度，存在较为明显的季节性特征。随着公司营业收入持续快速增长，收入季节性特征及客户付款审批流程较长、部分付款进度滞后于合同约定等因素使得报告期各期末公司应收账款及应收票据余额较大，2017 年末、2018 年末及 2019 年末，公司应收账款及应收票据账面价值合计分别为 25,992.39 万元、61,945.84 万元和 130,776.96 万元，合计占各期末总资产的比例分别为 4.93%、9.13%和 18.28%。公司已按照应收账款及应收票据坏账计提政策足额计提坏账准备。

未来，公司应收账款及应收票据余额可能会随着经营规模的扩大而增加，若主要债务人的财务状况、合作关系发生恶化，或催收措施不力，则可能导致应收账款及应收票据无法收回形成坏账损失；若应收账款及应收票据规模进一步扩大、账龄进一步上升，坏账准备金额会相应增加，对公司经营成果造成不利影响；如果应收账款及应收票据规模扩大，也会影响公司经营性现金流量，对公司资金状况造成不利影响，并可能导致银行贷款和财务费用的增加而对盈利能力造成不利影响。

7、商誉减值的风险

截止 2019 年末，公司合并资产负债表中商誉的账面价值为 120,930.24 万元，主要系非同一控制下控股合并网神股份、网康科技等企业所致。

报告期前、报告期内，发行人实施收购形成的商誉及商誉减值准备计提情况如下：

单位：万元

项目	报告期前 (截至 2016.12.31)	2017.12.31	2018.12.31	2019.12.31
商誉原值	136,128.37	136,841.54	139,385.53	151,935.14
减值准备	999.34	19,687.75	31,004.90	31,004.90
商誉账面价值	135,129.04	117,153.79	108,380.64	120,930.24

由于网络安全向更深层次渗透，更加细分化的技术领域、产品需求使得更多的技术创新不断的在中小企业中涌现出来，发行人未来将继续对具有一定技术优势、与公司能够形成协同效应的企业实施收购，存在形成大额商誉的风险。

根据《企业会计准则》的相关规定，非同一控制下企业合并形成的商誉需在未来每年年度终了进行减值测试。如果网神股份、网康科技等企业未来由于市场环境发生重大不利变化等原因导致业务开展未达到预期；或未来被收购企业由于前沿技术的商业化高度不确定性导致其业务开展的不确定，均可能导致商誉减值，从而对公司业绩造成不利影响。

8、收入季节性波动的风险

报告期内，公司主营业务收入按季度分布情况如下：

单位：万元

项目	2019 年度		2018 年度		2017 年度	
	金额	占比	金额	占比	金额	占比
第一季度	37,457.96	11.89%	20,277.90	11.30%	8,216.94	10.21%
第二季度	60,302.67	19.15%	20,453.51	11.40%	9,911.65	12.32%
上半年合计	97,760.63	31.04%	40,731.41	22.69%	18,128.60	22.53%
第三季度	45,499.60	14.45%	29,415.39	16.39%	20,464.27	25.43%
第四季度	171,673.25	54.51%	109,346.30	60.92%	41,869.42	52.04%
下半年合计	217,172.85	68.96%	138,761.68	77.31%	62,333.69	77.47%
合计	314,933.48	100.00%	179,493.10	100.00%	80,462.29	100.00%

报告期内，公司终端客户主要来自于政府、公检法司、能源、金融、教育、医疗卫生、军队军工、运营商等领域，受上述终端客户预算管理和集中采购制度等因素影响，2017年、2018年及2019年，公司四季度收入占全年主营业务收入的比例分别为52.04%、60.92%和54.51%，收入主要集中于四季度，存在较为明显的季节性特征。又由于费用在年度内较为均衡的发生，而收入主要集中在第四季度，因此可能造成公司前三季度亏损较大的情况。公司收入和盈利有一定的季节性波动，投资者不宜以半年度或者季度报告的数据推测全年盈利情况。

8、公司子公司数量较多带来的内部管理和控制风险

截至2020年4月29日，本公司及下属公司共拥有56家控股公司、26家参股公司，主要为境内子公司，分散于全国各大省市，分布较为广泛。

由于各子公司地理位置、当地监管要求、政治文化上存在一定差异，公司的组织结构和管理体系较为复杂，对公司内部管理、统筹规划、生产组织、技术保障、项目研发和商务支持等方面提出较高要求，如果公司管理层不能持续保持满足前述要求的管理水平，保证公司的运作机制有效运行，将可能因管理和内部控制不到位而产生管理控制风险，可能对公司的经营业绩造成不利影响。

10、报告期内，公司人员规模快速扩张，人力成本较高，可能对公司运营效率及管理效率造成不利影响

报告期各期末，发行人员工人数分别为3,206人、5,093人和6,895人，呈快速扩张的趋势。报告期各期内，公司人均创收分别为25.10万元、35.24万元和

45.68 万元，虽然呈逐年上升的趋势，但仍远低于同行业平均水平。公司各类人力成本合计分别为 85,541.88 万元、143,487.38 万元及 194,644.86 万元，占发行人营业总成本的比例分别为 60.97%、50.85%及 48.00%，占比较高。

公司人力成本占比较高且人均创收远低于同行业水平，主要原因系公司为快速完成研发体系、产品体系、服务体系、销售及渠道体系等方面的建设，快速扩张了人员规模。上述基础体系在建设期间并不能为公司带来直接的经济利益，因此造成了人力成本占营业总成本的比例较高，人员规模与收入规模短期内无法匹配的情况，对公司盈利能力、经营业绩造成不利影响。

此外，在人员迅速扩张背景下，报告期内公司人员离职率为 15.35%、14.55% 及 13.63%，基本保持稳定且略低于高科技、互联网等行业平均水平。虽然公司并未因为人员迅速扩张而导致人员流失情况加剧，且人员流失情况符合行业特点，但仍可能造成对外招聘、人员培训成本的额外增加，业务团队磨合周期的延长，人员变动频繁导致客户流失等对公司的运营效率及管理效率造成不利影响。

11、公司来自政府等特定行业类客户收入占比较高，行业需求变化可能导致业绩产生波动

报告期内，公司来自政府、公检法司及军队军工部门的收入占主营业务收入的比重平均超过 50%，为发行人第一大收入来源。近年来，该等行业客户的网络安全产品及服务需求主要由信息化投资加大、安全威胁加剧、网络安全监管趋严等因素驱动。

未来，如因信息化投资增速、安全威胁程度、网络安全监管要求发生重大变化，可能导致该等行业客户的网络安全产品及服务需求发生波动，进而影响公司的经营业绩。如与当前行业发展趋势相反的情形，例如信息化投资放缓、安全威胁程度降低等持续出现，公司可能面临网络安全市场逐渐饱和、收入增速放缓甚至收入下降的可能性。

12、业务整合风险

网络安全行业细分领域多、技术需求变化快，公司在保持持续研发投入基础上，亦通过收购行业中具有一定技术优势、与公司能够形成协同效应的公司，提

高公司的市场竞争力。公司预计未来仍会实施类似收购行为，若不能有效的进行业务整合，将对公司技术提高和服务客户造成一定影响。

13、公司营运资金来源单一，可能造成公司资金状况紧张的风险

报告期各期，发行人经营活动现金流量净额持续为负且处于扩大趋势，投资活动现金流量金额亦持续为负，并通过吸收投资的方式取得持续大额筹资活动现金流入，筹资活动产生的现金流量为公司主要的营运资金来源，来源相对单一，可能造成公司资金状况紧张，未来发展不达预期的风险。

14、经营规模的扩大使得渠道管理难度加大，可能给公司品牌 and 产品销售带来不利影响

由于网络安全行业最终用户相对分散、用户具体需求各有差异，报告期内，公司的产品销售采用直接销售和渠道销售相结合的方式。2017年、2018年和2019年，公司渠道销售占主营业务收入的比重分别为71.61%、53.85%和68.54%。公司产品的客户地域及行业分布广，在渠道销售模式下公司可借助渠道合作伙伴的销售网络，实现在不同行业和地区的客户覆盖，提升公司产品的市场占有率。随着公司经营规模的不断扩大，渠道管理的难度也相应加大。一方面，如果个别经销商在销售公司产品过程中违反了有关法律法规，或在销售价格及售后服务等方面未按公司规定执行，可能会给公司的品牌及声誉带来负面影响；另一方面，如果经销商综合能力下滑，可能导致其市场份额下降，导致其向公司采购金额下滑，存在公司渠道销售收入下滑的风险。因此，若公司不能及时提高渠道管理能力，可能对公司品牌 and 产品销售造成一定影响。

二、发行人本次发行情况

股票种类	人民币普通股（A股）		
每股面值	人民币 1.00 元		
发行股数	不超过 10,194.1579 万股 （行使超额配售选择权之前）	占发行后总 股本比例	不低于 10%
其中：发行新股数量	不超过 10,194.1579 万股	占发行后总	不低于 10%

	(行使超额配售选择权之前)	股本比例	
股东公开发售股份数量	-	占发行后总股本比例	-
发行后总股本	67,961.60 万股 (行使超额配售选择权之前)		
发行方式	本次发行全部采取发行新股的方式。本次发行拟采用网下向询价对象配售与网上向符合资格的社会公众投资者定价发行相结合的方式或监管机构认可的其他发行方式 (包括但不限于向战略投资者、保荐机构依法设立的相关子公司或者实际控制保荐机构的证券公司依法设立的其他相关子公司、公司高级管理人员与核心员工设立的专项资产管理计划等法律法规允许的投资者配售股票)		
发行对象	符合资格的询价对象和符合法律法规规定的自然人、法人及其他投资者 (法律法规或监管机构禁止的购买者除外)		
承销方式	余额包销		

三、本次证券发行上市的保荐代表人、协办人及项目组其他成员情况，包括人员姓名、保荐业务执行情况等内容。

(一) 本次证券发行具体负责推荐的保荐代表人

中信建投证券指定董军峰、李彦斌担任本次奇安信科技集团股份有限公司首次公开发行股票并在科创板上市的保荐代表人。

上述两位保荐代表人的执业情况如下：

董军峰先生：保荐代表人，硕士研究生，现任中信建投证券投资银行部执行总经理，曾主持或参与的项目有：澜起科技 IPO、仙琚制药 IPO、华谊兄弟 IPO、光线传媒 IPO、中广天择 IPO、上海贝岭并购重组、拓尔思并购重组、贝瑞基因借壳天兴仪表、慈文传媒借壳禾欣股份等。作为保荐代表人现在尽职推荐的项目有：恒玄科技（上海）股份有限公司首次公开发行并在科创板上市、上海灿星文化传媒股份有限公司首次公开发行并在创业板上市。

李彦斌先生：保荐代表人，硕士研究生，现任中信建投证券投资银行部总监，曾主持或参与的项目有：金自天正 IPO、新野纺织 IPO、美邦服饰 IPO、汇川技术 IPO、亿通科技 IPO、岭南园林 IPO、祥和实业 IPO、凯迪股份 IPO（在会）、厦门银行 IPO（在会），中航三鑫非公开发行、福田汽车非公开发行、平潭发展非公开发行、同仁堂可转债、京能热电重大资产重组等项目等。作为保荐代表人现在尽职推荐的项目有：常州市凯迪电器股份有限公司首次公开发行、厦门银行股份有限公司首次公开发行。

（二）本次证券发行项目协办人

本次证券发行项目的协办人为梁文，其保荐业务执行情况如下：

梁文先生：硕士研究生，现任中信建投证券投资银行部高级经理，曾主持或参与的项目有：贝瑞基因借壳天兴仪表、光线传媒公司债、光线控股可交换债、华章投资收购慈文传媒等。

（三）本次证券发行项目组其他成员

本次证券发行项目组其他成员包括曾宏耀、杨明赫、薛屿晨、张宗源、许杰、刘喆汀、王浩。

曾宏耀先生：博士研究生，CFA，现任中信建投证券投资银行部总监，曾主持或参与的项目有：贝瑞基因借壳天兴仪表、天神娱乐借壳科冕木业、天神娱乐重大资产重组、光线传媒非公开发行、华谊兄弟非公开发行、慈文传媒非公开发行、华章投资并购慈文传媒等。

杨明赫先生：硕士研究生，现任中信建投证券投资银行部高级副总裁，曾主持或参与的项目有：银河证券 IPO、华录百纳非公开发行、立思辰公司债券项目等。

薛屿晨先生：硕士研究生，现任中信建投证券投资银行部副总裁，曾主持或参与的项目有：华谊兄弟非公开发行、华录百纳非公开发行、贝瑞基因借壳天兴仪表等。

张宗源先生：硕士研究生，现任中信建投证券投资银行部副总裁，曾主持或参与的项目有：中信出版 IPO、广电网络可转债、恒信移动重大资产重组、泛海控股债务融资工具等。

许杰先生：硕士研究生，具有法律职业资格，现任中信建投证券投资银行部高级经理，曾主持或参与的项目有：中信出版 IPO 项目等。

刘喆汀先生：硕士研究生，现任中信建投证券投资银行部高级经理，曾主持或参与的项目有：光线控股可交换债等。

王浩先生：硕士研究生，现任中信建投证券投资银行部经理，曾主持或参与

的项目有：国泰集团并购重组等。

四、保荐机构与发行人关联关系的说明

（一）截至本上市保荐书签署日，本保荐机构通过全资子公司中信建投证券投资有限公司及中信建投资本管理有限公司间接享有发行人 0.39%的权益，具体如下：

股东名称	持有发行人股权比例	与保荐机构的关系	保荐机构享有发行人的权益
中安信诚	0.26%	1、保荐机构全资子公司中信建投资本管理有限公司的控股子公司中安汇信投资管理有限公司作为普通合伙人持有中安信诚 0.02%的股权，中信建投资本管理有限公司持有中安汇信投资管理有限公司 66.50%的股权； 2、保荐机构全资子公司中信建投资本管理有限公司作为有限合伙人持有中安信诚 11.17%的股权； 3、保荐机构全资子公司中信建投投资有限公司作为有限合伙人持有中安信诚 8.08%的股权； 4、保荐机构全资子公司中信建投资本管理有限公司控股子公司中安汇信投资管理有限公司作为普通合伙人持有新余裕睿投资合伙企业（有限合伙）0.0001%的股权，中信建投资本管理有限公司持有中安汇信投资管理有限公司 66.50%的股权，新余裕睿投资合伙企业（有限合伙）持有中安信诚 12.99%的股权； 5、保荐机构全资子公司中信建投资本管理有限公司控股子公司中安汇信投资管理有限公司作为普通合伙人持有北京润信瑞泰股权投资管理中心（有限合伙）0.0032%的股权，中信建投资本管理有限公司持有中安汇信投资管理有限公司 66.50%的股权，北京润信瑞泰股权投资管理中心（有限合伙）持有中安信诚 41.35%的股权。	0.05%
新余润信	0.24%	保荐机构全资子公司中信建投资本管理有限公司作为普通合伙人持有新余润信 2.47%股权	0.01%
青莹投资	0.33%	保荐机构全资子公司中信建投投资有限公司作为有限合伙人持有青莹投资 99.99%的股权	0.33%
合计			0.39%

根据《上海证券交易所科创板股票发行与承销实施办法》等相关法律、法规的规定，保荐机构将安排相关子公司参与本次发行战略配售，具体按照上交所相关规定执行。保荐机构及其相关子公司后续将按要求进一步明确参与本次发行战略配售的具体方案，并按规定向上交所提交相关文件。

（二）发行人及其控股股东、实际控制人、重要关联方不存在直接或间接持有保荐机构或其控股股东、实际控制人、重要关联方股份的情况。

（三）保荐机构的保荐代表人及其配偶、董事、监事、高级管理人员不存在拥有发行人权益和在发行人任职等情况。

（四）保荐机构的控股股东、实际控制人、重要关联方与发行人控股股东、

实际控制人、重要关联方不存在相互提供担保或融资的情况。

（五）除上述情形外，保荐机构与发行人之间亦不存在其他关联关系。

基于上述事实，保荐机构及其保荐代表人不存在对其公正履行保荐职责可能产生影响的事项。

第二节 保荐机构承诺事项

一、保荐机构内部审核程序和内核意见

（一）保荐机构关于本项目的内部审核程序

本保荐机构在向中国证监会推荐本项目前，通过项目立项审批、投行委质控部审核及内核部门审核等内部核查程序对项目进行质量管理和风险控制，履行了审慎核查职责。

1、项目的立项审批

本保荐机构按照《中信建投证券股份有限公司投资银行类业务立项规则》的规定，对本项目执行立项的审批程序。

本项目的立项于 2018 年 11 月 30 日得到本保荐机构保荐及并购重组立项委员会审批同意。

2、投行委质控部的审核

本保荐机构在投资银行业务委员会（简称“投行委”）下设立质控部，对投资银行类业务风险实施过程管理和控制，及时发现、制止和纠正项目执行过程中的问题，实现项目风险管控与业务部门的项目尽职调查工作同步完成的目标。

本项目的项目负责人于 2020 年 3 月 31 日向投行委质控部提出底稿验收申请；2020 年 4 月 6 日至 2020 年 4 月 12 日，投行委质控部对本项目进行了现场核查，并于 2020 年 4 月 12 日对本项目出具项目质量控制报告。

投行委质控部针对各类投资银行类业务建立有问核制度，明确问核人员、目的、内容和程序等要求。问核情况形成的书面或者电子文件记录，在提交内核申请时与内核申请文件一并提交。

3、内核部门的审核

本保荐机构投资银行类业务的内核部门包括内核委员会与内核部，其中内核委员会为非常设内核机构，内核部为常设内核机构。内核部负责内核委员会的日

常运营及事务性管理工作。

内核部在收到本项目的内核申请后，于 2020 年 4 月 13 日发出本项目内核会议通知，内核委员会于 2020 年 4 月 17 日召开内核会议对本项目进行了审议和表决。

参加本次内核会议的内核委员共 7 人。内核委员在听取项目负责人和保荐代表人回复相关问题后，以记名投票的方式对本项目进行了表决。根据表决结果，内核会议审议通过本项目并同意向中国证监会、上海证券交易所推荐。

项目组按照内核意见的要求对本次发行申请文件进行了修改、补充和完善，并经全体内核委员审核无异议后，本保荐机构为本项目出具了上市保荐书，决定向中国证监会、上海证券交易所正式推荐本项目。

（二）保荐机构关于本项目的内核意见

本次发行申请已按照法律法规和中国证监会及上海证券交易所的相关规定，保荐机构对发行人及其控股股东、实际控制人进行了尽职调查、审慎核查，充分了解发行人经营状况及其面临的风险和问题，履行了相应的内部审核程序。并具备相应的保荐工作底稿支持。

二、通过尽职调查和对申请文件的审慎核查，中信建投证券作出以下承诺

（一）有充分理由确信发行人符合法律法规及中国证监会有关证券发行上市的相关规定；

（二）有充分理由确信发行人申请文件和信息披露资料不存在虚假记载、误导性陈述或者重大遗漏；

（三）有充分理由确信发行人及其董事在申请文件和信息披露资料中表达意见的依据充分合理；

（四）有充分理由确信申请文件和信息披露资料与证券服务机构发表的意见不存在实质性差异；

（五）保证所指定的保荐代表人及本保荐机构的相关人员已勤勉尽责，对发

行人申请文件和信息披露资料进行了尽职调查、审慎核查；

（六）保证保荐书、与履行保荐职责有关的其他文件不存在虚假记载、误导性陈述或者重大遗漏；

（七）保证对发行人提供的专业服务和出具的专业意见符合法律、行政法规、中国证监会的规定和行业规范；

（八）自愿接受中国证监会依照《证券发行上市保荐业务管理办法》采取的监管措施；

（九）中国证监会规定的其他事项。

第三节 对本次发行的推荐意见

一、发行人关于本次发行的决策程序合法

（一）董事会审议过程

发行人于 2020 年 2 月 14 日召开第一届董事会第六次会议，会议审议通过了包括《关于奇安信科技集团股份有限公司申请首次公开发行人民币普通股（A 股）股票并在科创板上市的议案》《关于股东大会授权董事会及其授权人士全权办理首次公开发行人民币普通股（A 股）股票并在科创板上市有关具体事宜的议案》等议案在内的与本次发行上市有关的议案，并同意将相关议案提交发行人 2019 年年度股东大会审议。

（二）股东大会审议过程

发行人于 2020 年 3 月 5 日召开 2019 年年度股东大会，会议审议通过了包括《关于奇安信科技集团股份有限公司申请首次公开发行人民币普通股（A 股）股票并在科创板上市的议案》《关于股东大会授权董事会及其授权人士全权办理首次公开发行人民币普通股（A 股）股票并在科创板上市有关具体事宜的议案》等议案在内的与本次发行上市有关的议案。

（三）国家国防科技工业局的批准

2019 年 5 月 15 日，国家国防科技工业局下发《国防科工局关于网神信息技术（北京）股份有限公司控股股东改制并上市涉及军工事项审查的意见》，原则同意网神股份控股股东奇安信有限改制并上市。

二、发行人符合科创板定位

保荐机构查阅了发行人相关行业报告和市场研究资料，了解了近年来行业相关政策，对发行人所在行业的市场情况和竞争格局进行了分析；对发行人高级管理人员及主要业务部门负责人进行了访谈，查阅发行人研发管理相关制度等文件，了解发行人在研项目进度情况，查阅发行人已取得的专利证书，查阅发行人的研发成果；实地查看发行人的经营场所，核查发行人实际经营情况；查阅了发

行人审计报告及财务报表，对发行人的主要客户、供应商进行了函证及走访，抽查了发行人的销售合同、采购合同，对主要客户销售流程、主要供应商采购流程进行了穿行测试等。

经核查，根据《科创板首次公开发行股票注册管理办法（试行）》第三条及《上海证券交易所科创板股票发行上市审核规则》第三条的规定，保荐机构就发行人符合科创板定位具体说明如下：

序号	科创板定位	具体依据
1	面向世界科技前沿、面向经济主战场、面向国家重大需求	<p>在网络空间国家竞争和对抗加剧，以及全球数字化转型的两大背景下，中国也加快 5G 网络、数据中心等新型基础设施建设；在数字化升级过程中，绝大部分安全问题集中在应用场景上，并和业务深度关联，网络安全已从辅助性工程变成基础设施。</p> <p>公司专注于网络空间安全市场，主营业务为向政府、企业客户提供新一代企业级网络安全产品和服务，为国家关键机构监控来自境内外的高级持续威胁（APT）攻击，成功发现了多个境内外的网络间谍组织；作为主要技术保障单位参与了国庆 70 周年、十九大、两会、抗战胜利 70 周年、澳门回归 20 周年等重大活动，一带一路高峰论坛、APEC、G20、中非论坛、金砖国家峰会、上合峰会、上海进博会等重大国际会议的网络安全保障工作；为网信、公安、工信等部门建设了针对关键信息基础设施的网络安全态势感知与防护系统。</p>
2	符合国家战略	<p>习近平总书记在全国网络安全和信息化工作会议上强调，没有网络安全就没有国家安全，就没有经济社会稳定运行，要树立正确的网络安全观，积极发展网络安全产业，做到关口前移，防患于未然。公司专注于网络空间安全市场，主营业务为向政府、企业客户提供新一代企业级网络安全产品和服务，符合《国家网络安全产业发展规划》、《信息安全技术网络安全等级保护基本要求》、《中华人民共和国网络安全法》等多项国家战略。</p>
3	拥有关键核心技术	<p>发行人拥有第三代安全引擎、终端识别检测技术、新一代反病毒特征引擎、新一代终端安全防御技术、基于云架构的安全扫描与监测技术、海量数据实时流处理技术网络安全与攻击检测技术、网络安全与大数据分析建模技术、云上安全资源管理与编排技术、基于云工作负载保护的云计算基础架构安全、零信任身份安全、网络流量攻击的分布式对抗技术、新一代威胁检测技术、新一代流量还原技术、第四代 SecOS 高性能一体化引擎技术、大数据可视化技术与 3D 图形技术、新一代用户行为分析技术、第三代数据泄漏防护技术、应用安全技术</p>

序号	科创板定位	具体依据
		等核心技术。在终端安全技术领域、第三代安全引擎技术领域、大数据安全分析技术领域、漏洞挖掘技术领域、软件定义安全技术领域、威胁情报技术领域等具有技术优势。
4	科技创新能力突出	截至本上市保荐书签署日，公司及子公司合法拥有 404 项主要专利，其中包括 368 项主要发明专利。公司科技创新能力突出，通过持续的技术创新和技术积累，构建了知识产权壁垒。
5	主要依靠核心技术开展生产经营	基于公司核心技术、专利、软件著作权及公司强大的数据能力和服务能力，公司通过将研发技术产业化，形成了包括基础架构安全产品、新一代IT基础设施防护产品以及大数据智能安全检测与管控产品的产品体系，覆盖了咨询与规划、评估与测试、分析与响应、情报与运营在内的安全服务体系，有效满足政企客户的各种安全防护需求。
6	具有稳定的商业模式	公司专注于网络空间安全市场，主营业务为向政府、企业客户提供新一代企业级网络安全产品和服务。拥有完善的研发、采购、生产、销售模式，以此实现对产品从研发到销售各个环节的有效控制。
7	市场认可度高	公司的客户范围覆盖大多数中央政府部门、中央直属企业和银行。公司获2019年北京民营企业科技创新百强第5名，在赛迪咨询发布的《2018年赛迪网络安全潜力企业榜80强》被评为第一名。根据赛迪咨询的市场排名情况看，公司在终端安全、安全管理平台、安全服务、云安全市场份额均为第一。
8	社会形象良好	2019年12月，公司成为北京2022年冬奥会和冬残奥会组委会官方网络安全服务和杀毒软件赞助商。 公司在每年8月举办的“北京网络安全大会”，已成为亚太地区最专业的、规模最大的网络安全盛会之一，大会“内生安全”的主题思想成为网络安全产业发展的风向标。 截至2019年12月31日，“奇安信威胁情报中心”首发披露的APT组织超过8个，持续跟踪的APT组织超过40个，共发布APT相关的分析跟踪文章报告54篇，已成为全球最知名的APT研究组织之一。 截至2020年3月末，“补天漏洞响应平台”拥有6万多名白帽子注册会员，已累计提交漏洞数量超过40万个，已成为全球最知名的网络安全社区之一。 经过多年的发展，奇安信已经成为网络安全领域的著名品牌，具有良好的社会形象。
9	具有较强成长性	报告期内，公司营业收入分别为82,124.38万元、181,677.28万元和315,412.92万元，最近三年营业收入复合增长率为95.98%，是国内企业网络安全领域中成长最

序号	科创板定位	具体依据
		快企业之一，具有较强的成长性。

综上所述，保荐机构认为，发行人符合科创板定位。

三、发行人符合《科创属性评价指引（试行）》及《上海证券交易所科创板企业发行上市申报及推荐暂行规定》的规定

（一）发行人符合科创板行业领域的规定

发行人专注于网络空间安全市场，主营业务为向政府、企业客户提供新一代企业级网络安全产品和服务。根据中国证监会《上市公司行业分类指引》（2012年修订），公司所属行业为“信息传输、软件和信息技术服务业（I）”之“软件和信息技术服务业（I65）”；根据《战略性新兴产业分类（2018）》，公司所属行业为“新一代信息技术产业”。

经核查，目前，科创板中发行人同行业公司主要包括安恒信息、山石网科等，根据上述同行业公司的公开披露信息，其行业领域均属于新一代信息技术领域，因此发行人与同行业公司行业领域归类划分一致，不存在显著差异。

综上所述，公司所属行业符合《上海证券交易所科创板企业发行上市申报及推荐暂行规定》第三条（一）中所规定的“新一代信息技术领域”行业领域。

（二）发行人符合科创属性要求的规定

1、研发投入符合相关指标

2017年、2018年和2019年，发行人研发费用分别为54,083.45万元、81,834.51万元和104,710.40万元，合计为240,628.35万元，最近三年累计研发投入合计超过6,000万元；发行人营业收入分别为82,124.38万元、181,677.28万元和315,412.92万元，合计579,214.58万元；发行人最近三年累计研发投入及占最近三年累计营业收入的比例为41.54%。

综上所述，发行人符合《科创属性评价指引（试行）》第一条第一款以及《上海证券交易所科创板企业发行上市申报及推荐暂行规定》第四条（一）的规定。

2、专利情况符合相关指标

截至本上市保荐书签署日，发行人及其控股子公司合法拥有 404 项主要专利，其中包括 368 项主要发明专利，公司形成主营业务收入的发明专利超过 5 项。

综上所述，发行人符合《科创属性评价指引（试行）》第一条第二款以及《上海证券交易所科创板企业发行上市申报及推荐暂行规定》第四条（二）的规定。

3、营业收入情况符合相关指标

2017 年、2018 年和 2019 年，公司营业收入分别为 82,124.38 万元、181,677.28 万元和 315,412.92 万元，最近三年营业收入复合增长率为 95.98%，超过 20%，且最近一年营业收入金额超过 3 亿元。

综上所述，公司符合《科创属性评价指引（试行）》第一条第三款以及《上海证券交易所科创板企业发行上市申报及推荐暂行规定》第四条（三）的规定。

四、发行人符合《上海证券交易所科创板股票上市规则》规定的上市条件

中信建投证券对发行人本次首次公开发行股票并在科创板上市是否符合《上海证券交易所科创板股票上市规则》规定的上市条件进行了逐项核查。经核查，发行人符合《上海证券交易所科创板股票上市规则》规定的上市条件，具体情况如下：

（一）发行人符合中国证监会规定的发行条件

1、本次证券发行符合《证券法》规定的发行条件

（1）发行人具备健全且运行良好的组织机构

保荐人查阅了发行人公司章程及发行人提供的股东大会、董事会、监事会的会议通知、会议议案及会议决议等相关会议材料等文件，发行人已按照《公司法》等法律、法规及公司章程等规定，设置了股东大会、董事会及其专门委员会、监事会；选举了董事（包括独立董事）、监事（包括职工代表监事）；聘任了总裁、财务总监、董事会秘书等高级管理人员，并根据经营需要建立了相关的业务部门和管理部门，发行人具备健全且运行良好的组织机构。

综上所述，发行人具备健全且运行良好的组织机构，符合《证券法》第十二

条第一款第（一）项的规定。

（2）发行人具有持续经营能力

发行人系依法设立并有效存续的股份有限公司，截至本上市保荐书签署日，发行人的生产经营符合国家产业政策，发行人的营业期限为长期，不存在因违法经营而被相关行政管理部门责令停业整顿或吊销营业执照的情形，不存在根据法律、法规及公司章程规定需要终止的情形。

发行人专注于网络空间安全市场，主营业务为向政府、企业客户提供新一代企业级网络安全产品和服务。公司是大型网络安全公司，目前员工人数已超过 7,000 人。公司的客户范围覆盖大多数中央政府部门、中央直属企业和银行，报告期内，公司营业收入的年均复合增长率为 95.98%，研发投入合计占营业收入合计比例为 41.54%，是国内企业网络安全领域中成长最快企业之一。发行人资产质量良好，运营管理能力较强，报告期内资产规模及收入规模持续扩大，具有持续经营能力。

综上所述，发行人具有持续经营能力，符合《证券法》第十二条第一款第（二）项的规定。

（3）发行人最近三年财务会计报告被出具无保留意见审计报告

保荐机构查阅了信永中和会计师事务所(特殊普通合伙)出具的《审计报告》（XYZH/2020BJA190009），发行人最近三年财务会计报告被出具无保留意见审计报告

综上所述，发行人最近三年财务会计报告被出具无保留意见审计报告，符合《证券法》第十二条第一款第（三）项的规定。

（4）发行人及其控股股东、实际控制人最近三年不存在贪污、贿赂、侵占财产、挪用财产或者破坏社会主义市场经济秩序的刑事犯罪

保荐机构取得了相关主管部门出具的合规证明和无犯罪记录证明，取得了发行人控股股东、实际控制人的调查表及出具的承诺，并查询了国家企业信用信息公示系统、中国执行信息公开网、中国裁判文书网、人民法院公告网、12309 中

国检察网、信用中国网、国家税务总局重大税收违法案件信息公布栏等网站，走访部分政府主管机关。发行人及其控股股东、实际控制人最近三年不存在贪污、贿赂、侵占财产、挪用财产或者破坏社会主义市场经济秩序的刑事犯罪。

综上所述，发行人及其控股股东、实际控制人最近三年不存在贪污、贿赂、侵占财产、挪用财产或者破坏社会主义市场经济秩序的刑事犯罪，符合《证券法》第十二条第一款第（四）项的规定。

2、本次证券发行符合《科创板首次公开发行股票注册管理办法（试行）》规定的发行条件

（1）发行人的设立时间及组织机构运行情况

保荐机构查阅了发行人的工商档案、有关主管部门出具的证明文件、相关审计报告、纳税资料。发行人自成立以来持续经营并合法存续，是依法设立且持续经营三年以上的股份有限公司，具备健全且运行良好的组织机构，相关机构和人员能够依法履行职责。

综上所述，发行人是依法设立且持续经营 3 年以上的股份有限公司，具备健全且运行良好的组织机构，相关机构和人员能够依法履行职责。符合《科创板首次公开发行股票注册管理办法（试行）》第十条的有关规定。

（2）发行人财务规范情况

保荐机构查阅了《审计报告》、财务报告等相关财务资料，并取得了财务相关的内外部文件。经核查，发行人会计基础工作规范，财务报表的编制和披露符合企业会计准则和相关信息披露规则的规定，在所有重大方面公允地反映了发行人的财务状况、经营成果和现金流量，并由注册会计师出具了无保留意见的审计报告。

综上所述，发行人会计基础工作规范，财务报表的编制和披露符合企业会计准则和相关信息披露规则的规定，在所有重大方面公允地反映了发行人的财务状况、经营成果和现金流量，并由注册会计师出具标准无保留意见的《审计报告》。符合《科创板首次公开发行股票注册管理办法（试行）》第十一条第一款的规定。

(3) 发行人内部控制情况

保荐机构查阅了《内控鉴证报告》等相关内控料，并与发行人相关人员进行访谈。经核查，发行人的内部控制制度健全且被有效执行，能够合理保证公司运行效率、合法合规和财务报告的可靠性，并由注册会计师出具无保留结论的《内部控制鉴证报告》（XYZH/2020BJA190011）。

综上所述，发行人内部控制制度健全且被有效执行，能够合理保证公司运行效率、合法合规和财务报告的可靠性，并由注册会计师出具无保留结论的内部控制鉴证报告。符合《科创板首次公开发行股票注册管理办法（试行）》第十一条第二款的规定。

(4) 发行人资产完整性及人员、财务、机构独立情况

保荐机构查阅了发行人的业务合同、《审计报告》、三会文件等资料。经核查，发行人业务完整，具有直接面向市场独立持续经营的能力；发行人资产完整，业务及人员、财务、机构独立，与控股股东、实际控制人及其控制的其他企业间不存在对发行人构成重大不利影响的同业竞争，以及严重影响独立性或者显失公平的关联交易。

综上所述，发行人业务完整，具有直接面向市场独立持续经营的能力；发行人资产完整，业务及人员、财务、机构独立，与控股股东、实际控制人及其控制的其他企业间不存在对发行人构成重大不利影响的同业竞争，不存在严重影响独立性或者显失公平的关联交易。符合《科创板首次公开发行股票注册管理办法（试行）》第十二条第（一）项的规定。

(5) 业务、控制权及主要人员的稳定性

保荐机构查阅了发行人《审计报告》、三会文件等资料。经核查，最近2年，发行人专注于网络空间安全市场，主营业务为向政府、企业客户提供新一代企业级网络安全产品和服务，主营业务未发生变化；公司的实际控制人为齐向东，未发生变化；公司主营业务、控制权、管理团队和核心技术人员稳定，最近2年内主营业务和董事、高级管理人员及核心技术人员均没有发生重大不利变化；控股股东和受控股股东、实际控制人支配的股东所持公司的股份权属清晰，最近2年实

际控制人没有发生变更，不存在导致控制权可能变更的重大权属纠纷。

综上所述，发行人主营业务、控制权、管理团队和核心技术人员稳定，最近 2 年内主营业务和董事、高级管理人员及核心技术人员均没有发生重大不利变化；控股股东和受控股股东、实际控制人支配的股东所持发行人的股份权属清晰，最近 2 年实际控制人没有发生变更，不存在导致控制权可能变更的重大权属纠纷。符合《科创板首次公开发行股票注册管理办法（试行）》第十二条第（二）项的规定。

（6）资产权属情况

保荐机构查阅了发行人《审计报告》、重要资产的权属证书、银行征信报告等资料，并查询了裁判文书网。经核查，发行人不存在主要资产、核心技术、商标等的重大权属纠纷、重大偿债风险、重大担保、诉讼、仲裁等或有事项，不存在经营环境已经或者将要发生的重大变化等对持续经营有重大不利影响的事项。

综上所述，发行人不存在主要资产、核心技术、商标等的重大权属纠纷，重大偿债风险，重大担保、诉讼、仲裁等或有事项，经营环境已经或者将要发生重大变化等对持续经营有重大不利影响的事项。符合《科创板首次公开发行股票注册管理办法（试行）》第十二条第（三）项的规定。

（7）发行人经营合法合规性

保荐机构查阅了发行人《审计报告》、发行人相关业务合同，并与发行人相关人员进行访谈，发行人专注于网络空间安全市场，主营业务为向政府、企业客户提供新一代企业级网络安全产品和服务。经查阅发行人《营业执照》、公司章程、有关产业政策，发行人的生产经营符合法律、行政法规和发行人章程的规定，符合国家产业政策。

综上所述，发行人生产经营符合法律、行政法规的规定，符合国家产业政策。符合《科创板首次公开发行股票注册管理办法（试行）》第十三条第一款的规定。

（8）发行人、控股股东及实际控制人的守法情况

保荐机构取得了相关主管部门出具的合规证明和无犯罪记录证明，取得了发

行人控股股东、实际控制人的调查表及出具的承诺，并查询了国家企业信用信息公示系统、中国执行信息公开网、中国裁判文书网、人民法院公告网、12309 中国检察网、信用中国网、国家税务总局重大税收违法案件信息公布栏等网站，走访部分政府主管机关。经核查，最近 3 年内，发行人及其控股股东、实际控制人不存在贪污、贿赂、侵占财产、挪用财产或者破坏社会主义市场经济秩序的刑事犯罪，不存在欺诈发行、重大信息披露违法或者其他涉及国家安全、公共安全、生态安全、生产安全、公众健康安全等领域的重大违法行为。

综上所述，最近 3 年内，发行人及其控股股东、实际控制人不存在贪污、贿赂、侵占财产、挪用财产或者破坏社会主义市场经济秩序的刑事犯罪，不存在欺诈发行、重大信息披露违法或者其他涉及国家安全、公共安全、生态安全、生产安全、公众健康安全等领域的重大违法行为。符合《科创板首次公开发行股票注册管理办法（试行）》第十三条第二款的规定。

（9）董事、监事和高级管理人员的守法情况

保荐机构取得了发行人董事、监事和高级管理人员分别出具的调查表、承诺及无犯罪记录，并查询了证券期货市场失信记录查询平台、中国证监会网站、中国证监会北京监管局网站、国家企业信用信息公示系统、中国执行信息公开网、中国裁判文书网、人民法院公告网、12309 中国检察网、信用中国网、国家税务总局重大税收违法案件信息公布栏等网站，走访了部分政府主管机关。经核查，发行人的董事、监事和高级管理人员不存在最近 3 年内受到中国证监会行政处罚，或者因涉嫌犯罪被司法机关立案侦查或者涉嫌违法违规被中国证监会立案调查，尚未有明确结论意见等情形。

综上所述，发行人的董事、监事和高级管理人员不存在最近 3 年内受到中国证监会行政处罚，或者因涉嫌犯罪被司法机关立案侦查或者涉嫌违法违规被中国证监会立案调查，尚未有明确结论意见等情形。符合《科创板首次公开发行股票注册管理办法（试行）》第十三条第三款的规定。

（二）发行后股本总额不低于人民币 3,000 万元

经核查，发行人本次发行前股本总额为 57,767.4421 万元，本次拟发行股份

不超过 10,194.1579 万元（行使超额配售选择权之前），发行后股本总额不超过 67,961.60 万元（行使超额配售选择权之前），不低于 3,000 万元。

（三）公开发行的股份达到公司股份总数的 25%以上；公司股本总额超过人民币 4 亿元的，公开发行股份的比例为 10%以上

经核查，发行人本次发行前股本总额为 57,767.4421 万元，本次拟发行股份不超过 10,194.1579 万元（行使超额配售选择权之前），公开发行的股份不低于发行后总股本的 10%。

（四）市值及财务指标符合本规则规定的标准

根据《上海证券交易所科创板股票上市规则》规定的上市条件，公司符合上市条件中的“预计市值不低于人民币 15 亿元，最近一年营业收入不低于人民币 2 亿元，且最近三年累计研发投入占最近三年累计营业收入的比例不低于 15%”，具体分析如下：

1、预计市值不低于人民币 15 亿元

根据报告期内发行人外部投资者入股估值以及可比公司在境内市场的近期估值情况，公司预计总市值不低于人民币 15 亿元。

2、最近一年营业收入不低于人民币 2 亿元

根据信永中和会计师事务所(特殊普通合伙)出具的标准无保留意见的《审计报告》(XYZH/2020BJA190009)，发行人 2019 年营业收入为 315,412.92 万元，不低于 2 亿元。

3、最近三年累计研发投入占最近三年累计营业收入的比例不低于 15%

根据信永中和会计师事务所(特殊普通合伙)出具的标准无保留意见的《审计报告》(XYZH/2020BJA190009)，2017 年、2018 年及 2019 年，发行人研发费用分别为 54,083.45 万元、81,834.51 万元和 104,710.40 万元，合计为 240,628.35 万元；发行人营业收入分别为 82,124.38 万元、181,677.28 万元和 315,412.92 万元，合计 579,214.58 万元；发行人最近三年累计研发投入及占最近三年累计营业收入的比例为 41.54%，不低于 15%。

综上，公司满足《科创板股票上市规则》第 2.1.2 条第（二）项“预计市值不低于人民币 15 亿元，最近一年营业收入不低于人民币 2 亿元，且最近三年累计研发投入占最近三年累计营业收入的比例不低于 15%”中规定的市值及财务指标。

（五）上海证券交易所规定的其他上市条件

经核查，发行人符合上海证券交易所规定的其他上市条件。

五、发行人证券上市后持续督导工作的具体安排

事项	工作安排
（一）持续督导事项	在本次发行股票上市当年的剩余时间及其后三个完整会计年度内对发行人进行持续督导
督导发行人履行有关上市公司规范运作、信守承诺和信息披露等义务，审阅信息披露文件及向中国证监会、证券交易所提交的其他文件	<ol style="list-style-type: none"> 1、督导上市公司建立健全并有效执行信息披露制度，审阅信息披露文件及其他相关文件，确信上市公司向交易所提交的文件不存在虚假记载、误导性陈述或重大遗漏； 2、对上市公司的信息披露文件及向中国证监会、交易所提交的其他文件进行事前审阅（或在上市公司履行信息披露义务后五个交易日内，完成对有关文件的审阅工作），对存在问题的信息披露文件应及时督促上市公司予以更正或补充，上市公司不予更正或补充的，及时向交易所报告； 3、关注公共传媒关于上市公司的报道，及时针对市场传闻进行核查。经核查后发现上市公司存在应披露未披露的重大事项或与披露的信息与事实不符的，及时督促上市公司如实披露或予以澄清；上市公司不予披露或澄清的，及时向交易所报告。
督导发行人有效执行并完善防止控股股东、实际控制人、其他关联方违规占用发行人资源的制度	<ol style="list-style-type: none"> 1、督导发行人遵守《公司章程》及有关决策制度规定； 2、列席董事会和股东大会重大事项的决策过程； 3、若有大股东、其他关联方违规占用发行人资源的行为，及时向中国证监会、交易所报告，并发表声明。
督导发行人有效执行并完善防止其董事、监事、高级管理人员利用职务之便损害发行人利益的内控制度	<ol style="list-style-type: none"> 1、督导发行人依据《公司章程》进一步完善法人治理结构，制订完善的经营制度； 2、督导发行人建立对高管人员的监管机制，完善高管人员的薪酬体系； 3、对高管人员的故意违法违规的行为，及时报告中国证监会、证券交易所，并发表声明。
督导发行人有效执行并完善保障关联交易公允性和合规性的制度，并对关联交易发表意见	<ol style="list-style-type: none"> 1、督导发行人进一步完善关联交易的决策制度，根据实际情况对关联交易决策权力和程序做出相应的规定； 2、督导发行人遵守《公司章程》中有关关联股东和关联董事回避的规定； 3、督导发行人严格履行信息披露制度，及时公告关联交易事项；

事项	工作安排
	4、督导发行人采取减少关联交易措施。
持续关注发行人募集资金的专户存储、投资项目的实施等承诺事项	1、督导发行人严格按照招股说明书中承诺的投资计划使用募集资金； 2、要求发行人定期通报募集资金使用情况； 3、因不可抗力致使募集资金运用出现异常或未能履行承诺的，督导发行人及时进行公告； 4、对确因市场等客观条件发生变化而需改变募集资金用途的，督导发行人严格按照法定程序进行变更，关注发行人变更的比例，并督导发行人及时公告。
持续关注发行人为他人提供担保等事项，并发表意见	1、督导发行人严格按照《公司章程》的规定履行对外担保的决策程序； 2、督导发行人严格履行信息披露制度，及时公告对外担保事项； 3、对发行人违规提供对外担保的行为，及时向中国证监会、证券交易所报告，并发表声明。
（二）保荐协议对保荐机构的权利、履行持续督导职责的其他主要约定	1、获取发行人通报的与保荐工作相关的信息，及时获取发表保荐工作相关独立意见所必需的资料，确保及时发表意见； 2、按照法律、法规、中国证监会、上交所信息披露规定，对发行人违法违规的事项发表公开声明。
（三）发行人和其他中介机构配合保荐机构履行保荐职责的相关约定	1、督促发行人和其他中介机构配合保荐机构履行保荐工作； 2、对其他中介机构出具的专业意见存在疑义的，督促其他中介机构做出解释或出具依据。
（四）其他安排	无

六、保荐机构的结论意见

中信建投证券接受发行人委托，担任其本次首次公开发行并在科创板上市的保荐机构。本保荐机构遵照诚实守信、勤勉尽责的原则，根据《公司法》《证券法》和中国证监会颁布的《证券发行上市保荐业务管理办法》等法律法规的规定，对发行人进行了审慎调查。

本保荐机构对发行人是否符合证券发行上市条件及其他有关规定进行了判断、对发行人存在的主要问题和风险进行了提示、对发行人发展前景进行了评价，对发行人本次首次公开发行履行了内部审核程序并出具了内核意见。

本保荐机构内核部门及保荐代表人经过审慎核查，认为发行人本次首次公开发行并在科创板上市符合根据《中华人民共和国证券法》、《证券发行上市保荐业务管理办法》《科创板首次公开发行股票注册管理办法（试行）》和《上海证券交易所科创板股票发行上市审核规则》等规定，同意保荐发行人本次首次公开发行并在科创板上市。

(本页无正文, 为《中信建投证券股份有限公司关于奇安信科技集团股份有限公司首次公开发行股票并在科创板上市之上市保荐书》之签字盖章页)

项目协办人签名: 梁文

梁文

保荐代表人签名: 董军峰

董军峰

李彦斌

李彦斌

内核负责人签名: 林焯

林焯

保荐业务负责人签名: 刘乃生

刘乃生

保荐机构法定代表人签名: 王常青

王常青

