证券代码：688023　　证券简称：安恒信息

杭州安恒信息技术股份有限公司

（杭州市滨江区西兴街道联慧街 188 号）

2020 年度向特定对象发行 A 股股票

募集说明书

（申报稿）

保荐机构（主承销商）

国泰君安证券股份有限公司
GUOTAI JUNAN SECURITIES CO., LTD.

（中国（上海）自由贸易试验区商城路 618 号）

二〇二一年四月

声　明

本公司及全体董事、监事、高级管理人员承诺本募集说明书及其他信息披露资料不存在虚假记载、误导性陈述或重大遗漏，并对其真实性、准确性、完整性承担相应的法律责任。

本公司控股股东、实际控制人承诺本募集说明书及其他信息披露资料不存在虚假记载、误导性陈述或重大遗漏，并对其真实性、准确性、完整性承担相应的法律责任。

中国证监会、证券交易所对本次发行所作的任何决定或意见，均不表明其对注册申请文件及所披露信息的真实性、准确性、完整性作出保证，也不表明其对本公司的盈利能力、投资价值或者对投资者的收益作出实质性判断或保证。任何与之相反的声明均属虚假不实陈述。

根据《证券法》的规定，股票依法发行后，本公司经营与收益的变化，由本公司自行负责；投资者自主判断本公司的投资价值，自主作出投资决策，自行承担股票依法发行后因本公司经营与收益变化或者股票价格变动引致的投资风险。

目 录

释 义

除非文中另有所指，下列词语具有如下涵义：

一、一般术语

公司、发行人、安恒信息	指	杭州安恒信息技术股份有限公司
有限公司、安恒有限	指	杭州安恒信息技术有限公司，安恒信息前身
阿里创投	指	杭州阿里创业投资有限公司
宁波润和	指	温州润和创业投资合伙企业（有限合伙），曾用名“宁波润和兴源投资合伙企业（有限合伙）”
嘉兴安恒	指	嘉兴市安恒投资管理合伙企业（有限合伙）
宁波安恒	指	宁波安恒投资合伙企业（有限合伙）
杭州九歌	指	杭州九歌股权投资合伙企业（有限合伙）
上海舜佃	指	上海舜佃投资管理中心（有限合伙）
上海梦元	指	上海梦元投资管理中心（有限合伙）
重庆麒厚	指	重庆麒厚西海股权投资管理有限公司
杭州爵盛	指	杭州爵盛新千投资管理合伙企业（有限合伙）
绿盟科技	指	绿盟科技集团股份有限公司
启明星辰	指	启明星辰信息技术集团股份有限公司
深信服	指	深信服科技股份有限公司
蓝盾股份	指	蓝盾信息安全技术股份有限公司
迪普科技	指	杭州迪普科技股份有限公司
北信源	指	北京北信源软件股份有限公司
任子行	指	任子行网络技术股份有限公司
奇安信	指	奇安信科技集团股份有限公司
山石网科	指	山石网科通信技术股份有限公司
知道创宇	指	北京知道创宇信息技术股份有限公司
阿里云	指	阿里云计算有限公司
《公司章程》	指	杭州安恒信息技术股份有限公司章程
股东大会	指	股份公司股东大会
董事会	指	股份公司/有限公司董事会
监事会	指	股份公司/有限公司监事会
高级管理人员	指	公司总经理、副总经理、财务总监、董事会秘书
中国证监会	指	中国证券监督管理委员会

国家发改委	指	中华人民共和国国家发展与改革委员会
工信部	指	中华人民共和国工业和信息化部
上交所	指	上海证券交易所
网信办	指	中华人民共和国国家互联网信息办公室
信创	指	信息技术应用创新产业
中国汽研	指	中国汽车工程研究院股份有限公司
股票或 A 股	指	公司发行的每股面值人民币 1.00 元的人民币普通股
本次发行、本次向特定对象发行、本次向特定对象发行 A 股股票	指	公司本次向特定对象发行不超过 22,222,222 股，占公司发行前总股本的比例不超过 20%
本机构、保荐机构、主承销商、国泰君安证券	指	国泰君安证券股份有限公司
本募集说明书	指	《杭州安恒信息技术股份有限公司 2020 年度向特定对象发行 A 股股票募集说明书》
发行人律师、国浩律所	指	国浩律师（杭州）事务所
审计机构、立信会计师、立信	指	立信会计师事务所（特殊普通合伙）
赛迪顾问	指	赛迪顾问股份有限公司
安全牛	指	北京谷安天下科技有限公司下属定位于企业级信息安全市场的专业新媒体
元、万元、亿元	指	人民币元、人民币万元、人民币亿元
《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》
《注册办法》	指	《科创板上市公司证券发行注册管理办法（试行）》
《实施细则》	指	《上海证券交易所科创板上市公司证券发行承销实施细则》
《网络安全法》	指	《中华人民共和国网络安全法》
《上市规则》	指	《上海证券交易所科创板股票上市规则（2019 年 4 月修订）》
最近三年及一期、报告期	指	2017 年、2018 年、2019 年、2020 年 1-9 月

二、专业术语

阿里云	指	阿里巴巴集团旗下云计算品牌
腾讯云	指	腾讯公司旗下云计算品牌
华为云	指	华为公司旗下云计算品牌
OpenStack	指	由 NASA 和 Rackspace 合作研发的，开源的云计算管理平台
中国电信天翼云	指	中国电信旗下云计算品牌
中国联通沃云	指	中国联通旗下云计算品牌

GDPR	指	General Data Protection Regulation，通用数据保护条例
WAF	指	Web Application Firewall，网络应用防火墙
堡垒机	指	运维审计与风险控制系统
天池	指	天池云安全管理平台
玄武盾	指	玄武盾云防护服务
URL	指	Uniform Resource Locator，统一资源定位符
DNS	指	Domain Name System，域名系统
IPv4	指	Internet Protocol version4，互联网协议第四版
IPv6	指	Internet Protocol version6，互联网协议第六版
漏洞	指	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，使攻击者能够在未授权的情况下访问或破坏系统
病毒	指	编制或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
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
SQL 注入	指	通过把 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意 SQL 命令的攻击手段
DDoS 攻击	指	分布式拒绝服务（Distributed Denial of Service）攻击，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攻击，使计算机或网络无法提供正常的服务
APT 攻击	指	高级持续性威胁（Advanced Persistent Threat）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
VPN	指	Virtual Private Network，虚拟专用网络
CVE	指	Common Vulner abilities & Exposures，公共漏洞和暴露
CNVD	指	China National Vulnerability Database，国家信息安全漏洞共享平台
0Day 漏洞	指	已经被发现（有可能未被公开），而官方还没有相关补丁的漏洞
CC	指	Challenge Collapsar，挑战黑洞，利用不断对网站发送连接请求致使网站拒绝服务
ISO27001	指	International Organization for Standardization，由英国标准协会指定的信息安全管理要求
MySQL	指	My Structured Query Language，是一种结构化查询语言撰写的数据库
SUMAP	指	公司开发的全球网络高速探测引擎，为态势感知、威胁监测等提供实时数据
EDR	指	终端检测与响应（Endpoint Detectionand Response）,是一种应用机器学习算法与行为分析提供精确、全面、实时的防护与响应的网络安全技术，能够有效发现未知威胁并减少误报
AI	指	Artificial Intelligence，人工智能。它是研究、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

UEBA	指	用户实体行为分析（Userand Entity Behavior Analytics），是一种通过机器学习来发现高级威胁，实现自动化的建模的网络安全技术
ERP	指	ERP（Enterprise Resource Planning），即企业资源计划。指建立在信息技术基础上，以系统化的管理思想，为企业决策层及员工提供决策运行手段的管理平台
软件基因	指	软件基因（Software Gene）是软件体上具有功能或承载信息的二进制片段
ISO9001	指	是由 TC176（TC176 指质量管理体系技术委员会）制定的所有国际标准
等级保护 2.0、等保 2.0	指	网络安全等级保护，俗称等级保护 2.0，提出了云安全、移动互联网安全、物联网安全、工业控制系统安全、大数据安全等网络空间扩展要求，且每个部分都有详细的安全标准
黑名单	指	设置不能通过的用户列表，在该列表以外的用户都能通过
Java 语言	指	一门面向对象编程语言
沙箱	指	一个虚拟系统程序，允许在沙盘环境中运行浏览器或其他程序，运行所产生的变化可删除
MIPS	指	一种采取精简指令集（RISC）的处理器架构
Jenkins	指	一个开源软件项目，是基于 Java 开发的一种持续集成工具，用于监控持续重复的工作，旨在提供一个开放易用的软件平台，使软件的持续集成变成可能。
CMMI	指	Capability Maturity Model Integration，即软件成熟度模型集成。由美国卡耐基梅隆大学软件工程学院发布，是一个可以改进系统工程和软件工程的整合模式，能够降低项目的成本，提高项目质量与按期完成率，在世界各地得到了广泛的推广与接受
云计算	指	一种商业计算模型。云计算将计算任务分布在大量计算机构成的资源池上，使各种应用系统能够根据需要获取计算力、存储空间和信息服务
信息安全等级保护	指	对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置
物联网	指	物联网，即基于传感技术的物物相连、人物相连和人人相连的信息实时共享的网络

除特别说明外，本募集说明书财务数值均保留二位小数，若出现总数与各分项数值之和尾数不符，均为四舍五入原因所致。

第一节　发行人基本情况

一、发行人基本情况

公司名称：	杭州安恒信息技术股份有限公司
法定代表人：	范渊
注册资本：	7,407.4075 万元
住所：	浙江省杭州市滨江区西兴街道联慧街 188 号
股票简称：	安恒信息
股票代码：	688023.SH
股票上市地：	上海证券交易所
经营范围：	信息安全设备、网络安全设备、网络安全软件、计算机软硬件、系统集成的技术开发、技术服务，成年人的非证书劳动职业技能培训（涉及前置审批的项目除外），会展服务；生产、加工：信息安全设备、网络安全设备、计算机设备；批发、零售：电子产品、通讯设备、计算机软硬件；货物进出口（法律、行政法规禁止经营的项目除外，法律、行政法规限制经营的项目取得许可证后方可经营）。

二、股权结构、控股股东及实际控制人情况

（一）前十大股东情况

截至 2020 年 9 月 30 日，本公司前十大股东持股情况如下：

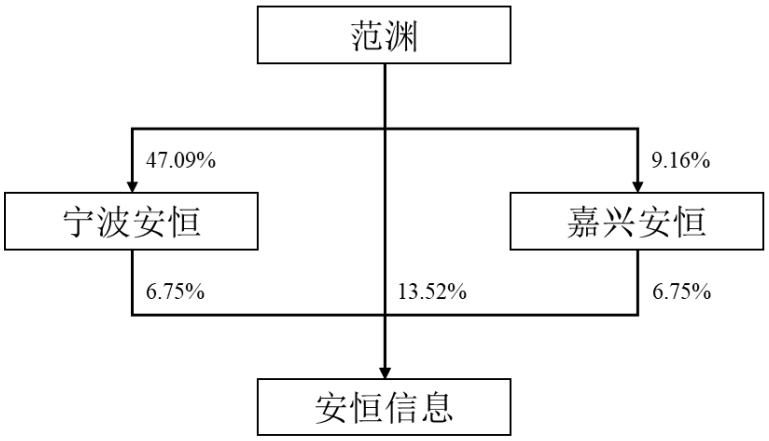
股东名称	股东性质	持股数量（股）	持股比例（%）	其中有限售条件的股份数量
范渊	境内自然人	10,018,362	13.52	10,018,362
阿里创投	境内非国有法人	8,008,337	10.81	8,008,337
宁波润和	境内非国有法人	5,200,040	7.02	5,200,040
宁波安恒	境内非国有法人	5,000,000	6.75	5,000,000
嘉兴安恒	境内非国有法人	4,999,990	6.75	4,999,990
杭州九歌	境内非国有法人	2,777,778	3.75	2,777,778
上海舜佃	境内非国有法人	2,440,000	3.29	2,440,000
上海梦元	境内非国有法人	2,292,592	3.09	2,292,592
浙江爵盛	境内非国有法人	1,666,667	2.25	1,666,667
重庆麒厚	境内非国有法人	1,666,603	2.25	1,666,603
合计		**44,070,369**	**59.48**	**44,070,369**

截至 2020 年 9 月 30 日，公司控股股东及实际控制人范渊分别持有公司前十大股东宁波安恒、嘉兴安恒 47.09%、9.16%的财产份额，且为上述两家合伙企业

的执行事务合伙人。宁波安恒、嘉兴安恒均系范渊的一致行动人，且为受范渊控制的企业。

（二）控股股东及实际控制人情况

截至 2020 年 9 月 30 日，公司的控股股东、实际控制人为范渊先生，其直接持有公司股票 10,018,362 股，直接持股比例为 13.52%。宁波安恒、嘉兴安恒分别持有公司股票 5,000,000 股和 4,999,999 股，持股比例分别为 6.75%及 6.75%。范渊分别持有嘉兴安恒、宁波安恒 9.16%和 47.09%的财产份额，且为上述两家合伙企业的普通合伙人及执行事务合伙人。根据范渊与嘉兴安恒及宁波安恒签署的《一致行动协议》，嘉兴安恒、宁波安恒系范渊的一致行动人，范渊合计控制上市公司 27.02%的表决权，持有表决权的比例超过任何其他单一股东。范渊为公司控股股东及实际控制人。实际控制人的控制关系图如下：



三、所处行业的主要特点及行业竞争情况

（一）公司所属行业类别

公司主营业务为网络信息安全产品的研发、生产及销售，并为客户提供专业的网络信息安全服务，属于网络信息安全行业。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”。依据国家统计局《国民经济行业分类》（GB/T4754-2017），公司所处行业属于“I65 软件和信息技术服务业”。依据国家统计局《战略性新兴产业分类（2018）》（国家统计局令第 23 号）标准，公司属于“新兴软件和新型信息技术服务”下属的“网络与信息安全软件开发”和“互联网安全服务”行业。

（二）所处行业的主要特点

1、网络信息安全简介

网络信息安全是指通过采取必要的措施对信息系统的硬件、软件、系统中的数据及依托其开展的业务进行保护，使得它们不会由于偶然的或者恶意的原因而遭到未经授权的访问、泄露、破坏、修改、审阅、检查、记录或销毁，保证信息系统连续可靠地正常运行。

一般而言，网络信息安全产品主要包括安全硬件、安全软件及安全服务。

分类	产品简介
安全硬件	指以物理硬件的形态直接集成到网络中的安全设备，主要包括防火墙、WEB应用防火墙、运维审计与风险控制系统、数据库审计与风险控制系统、综合日志审计、入侵检测与防御、统一威胁管理、安全内容管理、VPN等。
安全软件	指运行在服务器或者终端设备上的软件形态安全产品，主要包括身份管理与访问控制软件、终端安全软件、安全性与漏洞管理软件等。
安全服务	贯穿于企业整个IT基础设施建设过程中所需要的信息安全的计划、设计、建设、管理等全过程。通过IT安全服务可以发现企业IT系统中可能存在的安全风险，更新安全软件、安全硬件策略，减少IT安全防护体系的疏漏。

2、行业的经营模式、周期性、季节性和区域性特征

（1）行业特有的经营模式

由于网络信息安全涉及国家秘密、商业机密等重要数据的存储，诸如政府机构、金融机构和电信机构等客户对网络信息安全的敏感性强，因此网络信息安全产业的客户主要集中在上述领域。这类客户通常采用招投标或科研项目立项的方式进行网络信息安全产品与服务的采购。

资产特性方面，作为知识密集型的新兴行业，网络信息安全行业与资本、劳动密集型的传统产业有显著的不同，知识和人才发挥着重要作用、技术资本和人力资本是行业内企业的核心竞争力。因此，网络信息安全行业的企业固定资产占总资产的比例普遍较小，具有“轻资产”的特征。

同时，网络信息安全行业“重人才，重技术”的特性明显。网络信息安全产品的研发、生产，网络信息安全服务以及安全集成解决方案的提供都需要丰富的行业经验和专业知识，领先的技术水平和成熟的综合人才是行业内各个公司发展的关键因素和内在驱动力。

（2）行业的周期性和季节性特点

近几年，受国家信息化建设鼓励政策的陆续出台与网络威胁事件的持续爆发等因素影响，企业纷纷加大了网络信息安全投入，网络信息安全产业呈快速稳定的增长态势。从行业发展历史以及行业发展的生命周期来看，网络信息安全产业仍处于成长期，未呈现出明显的周期性特征。网络信息安全行业的主要客户对象为政府机构、电信运营商、金融、教育、能源等领域内的公司，这些客户受预算体制和采购习惯的影响，通常在上半年进行预算管理，制订采购计划，在下半年进行采购和付款。因此，网络信息安全行业内各公司在下半年实现的收入占比较高，收入具有一定的季节性。

报告期内，公司的主要客户为政府（含公安）、金融企业、教育机构、电信运营商等，上述单位通常采取财务预算管理和集中采购制度，一般在每年的下半年制定次年年度预算和投资采购计划，而审批则集中在次年上半年，采购招标安排在次年年中或下半年。因此，公司在每年上半年订单签订数量较少，自年中开始增长，至年底达到最高值，产品的交付和验收也集中在下半年尤其是第四季度。

最近三年，公司营业收入按前三季度/四季度分布情况如下：

单位：万元

项目	2019 年度		2018 年度		2017 年度	
	金额	比例	金额	比例	金额	比例
前三季度	47,119.85	50.10%	31,042.77	49.54%	22,004.57	51.13%
第四季度	46,934.18	49.90%	31,615.90	50.46%	21,035.25	48.87%

（3）行业的区域性特点

目前，我国的网络信息安全行业呈现较明显的区域性特征，客户信息化水平的高低较大程度上决定了其对网络信息安全的需求，而我国区域经济发展不平衡直接导致了区域信息化水平不均衡，因此市场需求主要集中在华东、华北和华南等经济较发达地区。

3、网络信息安全行业发展状况

（1）国内网络信息安全形势

随着近年来国际、国内重大网络安全事故的频发，我国政府对网络信息安全

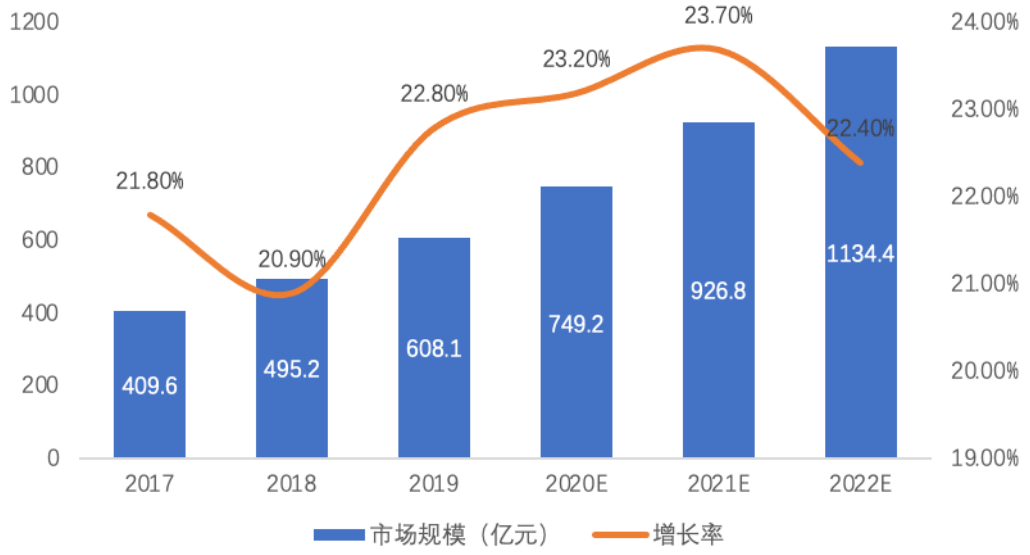
的重视程度不断提高。2013 年以来，我国先后设立中央国家安全委员会、中央网络安全和信息化委员会，发布新的《国家安全法》、《网络安全法》，制定多项鼓励行业发展的政策。2017 年 7 月 11 日，国家互联网信息办公室发布《关键信息基础设施安全保护条例（征求意见稿）》。2019 年 12 月 1 日，伴随着《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》的正式实施，我国网络信息安全行业正式宣告等保进入 2.0 时代。2020 年，国家相继推出《网络安全审查办法》、《关于工业大数据发展的指导意见》、《工业和信息化部办公厅关于开展 2020 年网络安全技术应用试点示范工作的通知》等关于网络安全产业发展的政策，这些政策为网络安全发展提供了新的契机。一系列法规政策提高了政府、企业对网络信息安全的合规要求，将带动政府、企业在网络信息安全方面的投入。

此外，随着信息技术和互联网技术在企业级用户中的广泛普及，云计算、大数据、移动互联网等新兴技术将得到广泛应用。大量新型复杂的业务系统的建设将带来新的安全漏洞，企业级用户面临着数据丢失、业务系统连续性等安全挑战，网络信息安全建设成为企业级用户在 IT 系统建设过程中关注的重要内容。

（2）国内网络信息安全产业发展前景

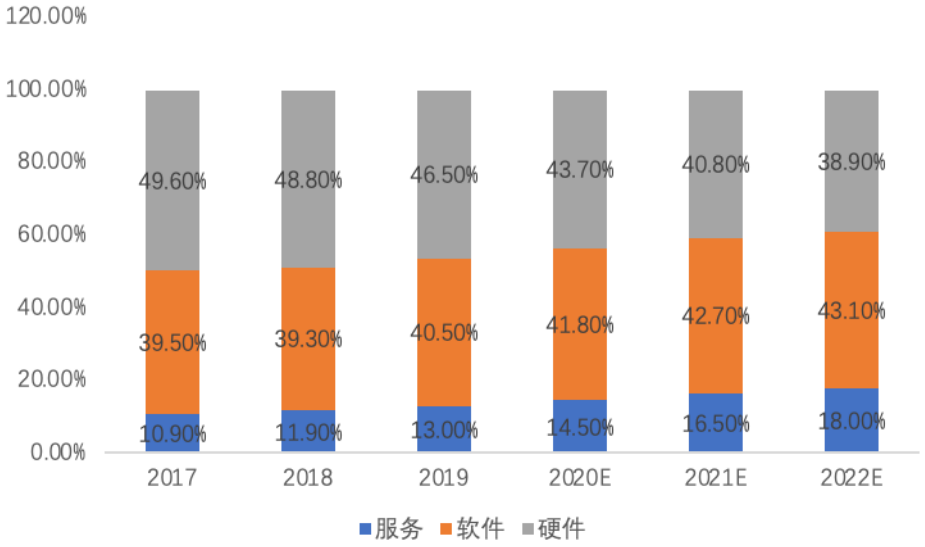
2019 年，网络安全政策法规持续完善优化，“等级保护 2.0”已经出台，网络安全市场规范性逐步提升，政企客户在网络安全产品和服务上的投入逐步增长。赛迪顾问预测，2019 年市场整体规模达到 495.2 亿元，到 2022 年中国网络信息安全市场将达到 1,134.4 亿元。

2017-2022 年中国网络安全市场规模及预测



网络安全产业的发展主要由合规需求驱动，近年来灾难性攻击促进企业把安全视为一项重要的商业风险，产生了大量网络安全方面的合规需求。随着虚拟化及云服务理念的渗透，网络安全盈利模式中网络安全服务的占比不断提升。

2017-2022 年中国网络安全市场结构及预测



（3）我国关键信息基础设施安全防护能力将显著提升

随着信息技术的广泛应用，我国高度重视关键信息基础设施保护，加强关键信息基础设施安全监管。一是开展安全检查和评估。工业和信息化部连续十年组织基础电信企业、互联网企业、域名机构对自身网络系统开展安全性检查，年均

处置数万起网络安全事件，有效保障了电信网和互联网安全稳定运行。二是加强对企业的考核通报。组织基础电信企业开展网络与信息安全责任考核，将监督检查及整改结果、安全事件和处置情况纳入年度考核。三是强化应急指挥能力建设。工业和信息化部构建了由各地通信管理局、基础电信企业等单位参与的行业一体化指挥体系。

（三）行业竞争情况

1、行业竞争格局

网络信息安全产品方面，近年来，我国网络信息安全产品市场快速增长，参与厂商众多。大型厂商占据一定的市场份额，但由于市场的细分程度较高，不同的细分市场又存在不同的领先厂商，总体来看，安全产品市场缺乏真正的龙头企业，市场集中度较低。本公司、启明星辰、绿盟科技、奇安信等企业是行业内的主要参与者。

在网络信息安全服务方面，与发达国家相比，我国安全服务市场还处于早期成长阶段，安全服务的产业投入和市场规模在网络信息安全产业中占比较低，国内安全服务市场还存在很大的发展空间。现阶段，我国各网络信息安全厂商主要向市场提供诸如安全设计、安全评估、安全运维和安全技术研发等方面的安全服务，该细分市场参与主体众多，模式尚不统一，竞争激烈，市场集中度低。

2、公司在行业内的市场地位

公司作为国内网络信息安全领域后起之秀，于 2007 年成立之初便以应用安全和数据安全作为切入点，推出市场首创性产品数据库审计与风险控制系统与 Web 应用防火墙产品，成功进入网络信息安全市场。目前公司核心基础安全产品持续多年市场份额位居行业前列。此外，公司核心产品的前瞻性和影响力也获得了国内外权威机构认可。在 IDC 发布的《中国态势感知解决方案市场 2019 年厂商评估》中，公司被评选为态势感知领导厂商，其中战略能力排名第一，市场份额排名第二。在 2019 年 IDC 发布的“中国 WEB 应用安全市场研究”中，公司被评为 Web 应用安全领导厂商，市场份额排名第一。公司 Web 应用防火墙在安全牛 2019 年发布的安全牛中国网络安全细分领域矩阵图中技术创新及规模均位列第一。公司日志审计系统在赛迪 2019 年发布的“中国日志审计产品市场研究

报告”中市场占比排名第一。在赛迪 2019 年发布的“2018-2019 中国云安全市场研究年度报告”中，公司云安全产品市场排名第二。在 Frost&Sullivan 发布的〞亚太区特权账号管理/堡垒机市场研究报告 2019〞中，公司的堡垒机产品市场份额排名亚太区并列第一，中国区第一。

公司始终坚持持续创新的发展战略，重视研发投入，同时紧跟全球信息技术发展趋势、贴近用户需求，不断更新迭代既有产品和解决方案，并孵化培育新兴产品及服务。安恒信息 2015-2018 年连续四年均被美国著名网络安全风险投资公司评选为全球网络安全创新 500 强。

公司自 2014 年开始陆续推出了云安全、大数据安全、态势感知和智慧城市安全等新兴安全领域相关产品和解决方案。凭借深厚的核心技术积累和对政企市场的深刻理解，公司在新兴领域取得了较好的发展成绩。在公有云安全领域，公司自 2015 年开始与阿里云合作，成为阿里云安全市场首批安全供应商，目前云安全产品已经上线包括阿里云、腾讯云、华为云、AWS 亚马逊、中国电信天翼云、中国联通沃云等在内的十余家国内主流公有云平台。

作为国内信息安全领域的领导者之一，在进行研发创新和市场开拓的同时，公司积极承担我国信息安全产业发展的社会责任，参与了众多国家与行业标准的制定。公司是我国“信息安全技术智慧城市安全体系框架”、“Java 语言源代码漏洞测试规范”、“信息安全技术移动智能终端应用软件安全技术要求和测试评价方法”等 13 项国家标准或国家标准计划的主要制定单位，并受邀参与制定“信息安全技术日志分析产品安全技术要求”、“信息安全技术数据库安全审计产品安全技术要求”、“信息安全技术网络型流量控制产品安全技术要求”等 7 项安全行业标准。

3、公司的竞争优势

（1）技术研发优势

公司自 2007 年创立以来始终坚持持续技术创新的发展战略，紧跟网络信息安全技术发展趋势和用户需求，不断在行业内率先推出创新产品，更新迭代既有产品和解决方案，并孵化培育新产品，提升市场竞争力。公司设立有安全研究院和产品研发中心两大研发机构。安全研究院致力于前沿技术预研、创新业务探索

和核心能力积累。研究院下设海特实验室和卫兵实验室，多年来在大数据安全、云安全、物联网安全、应用安全、人工智能、数据加密领域等均有重要成果输出，并且进行持续的漏洞挖掘研究，近三年内为国内外提交超过 300 个安全漏洞，其中 CVE 认证的安全漏洞超过 180 个，对象覆盖国内外多家大型互联网公司。研发中心主要由 AiLPHA 大数据实验室、明鉴事业群、网关事业群、天池、风暴中心等多个子部门组成，除负责公司现有产品的迭代升级研发外，还覆盖云安全、移动安全，智能设备安全、大数据安全、工控安全等多个新兴领域产品的开发。

截至 2020 年 9 月末，公司拥有研发人员 869 名，占员工总人数的比例达 32.87%，涉及攻防研究、应急响应、安全咨询、漏洞研究、产品研发等。公司拥有美国软件工程学会颁发的 CMMI5 权威认证，在软件开发过程的改善能力、质量管理水平、软件开发的整体成熟度居于行业前列。公司经过多年的探索和积累，已掌握了应用安全与数据安全等领域的重要核心技术，并形成了一系列具有自主知识产权的技术成果。截至 2020 年 9 月 30 日，公司拥有超过 130 项已获得授权的专利。

公司技术研发实力得到国家相关部门的肯定和支持，现已承担“国家发改委信息安全专项”、“工信部电子发展基金项目”、“科技部火炬计划”、“科技部网络空间重点专项”、“浙江省重点科技专项”等多项国家级、省市级科技计划项目。同时公司作为主要起草单位参与多项网络信息安全领域国家及行业相关技术标准的制定并积极引领技术标准在网络信息安全产品的落地工作。

（2）产品及服务优势

公司凭借多年的技术研发沉淀和经验积累，充分将其运用在应用安全和数据安全产品当中，不断在行业内率先推出创新产品，更新迭代既有产品和解决方案，既覆盖传统的应用与数据安全领域，同时，还将当前流行的云计算技术和大数据与人工智能技术应用其中，并将产品拓展至物联网、工控和智慧城市等新型领域。目前公司已形成了以应用安全及数据安全产品为基础，围绕新监管、新技术及新服务的完整产品线。公司核心产品在各自细分市场具有领导优势。

在服务方面，公司拥一支超过 450 人的专业安全服务团队，均具备一流网络与网络信息安全技术能力和丰富的安全攻防经验。多位服务团队成员具有国际注

册信息系统安全认证专家（CISSP）、国际信息系统审计师（CISA）、信息安全注册工程师（CISP）、信息安全管理体系（ISO27001）及主任审核员及高级项目经理（PMP）等资质；团队成员长期致力于各方向的安全漏洞研究。公司拥有中国信息安全测评中心安全工程类三级、国家计算机网络应急技术处理协调中心网络安全应急服务支撑单位（国家级）、中国网络安全审查技术与认证中心应急处理一级、中国网络安全审查技术与认证中心风险评估一级等在内的多项行业最高级别服务资质。公司服务团队先后参与了 2008 年北京奥运会、上海世博会、广州亚运会、连续五届世界互联网大会乌镇峰会、G20 杭州峰会、厦门金砖会议、青岛上合峰会、上海国际进口博览会、2018 第 14 届 FINA 世界游泳锦标赛等世界级重大活动的网络信息安全保障工作，以先进的理念和专业的服务获得各盛事主办方和监管机构的一致好评。

（3）综合服务能力优势

公司以客户需求为导向，在发展过程中逐步形成了涵盖安全产品研发、销售、安全服务和安全集成的完整业务体系，各产品线和业务模块相互促进、共同发展，形成了较强的综合服务能力。

公司的网络信息安全产品主要涉及应用安全、数据安全、安全智能、安全管理、云安全、物联网安全和工控安全等众多网络信息安全领域，可满足客户多方面的网络信息安全需求。此外，公司在现有安全产品的基础上还可为客户提供包括安全咨询与评估、安全检测与防护服务在内的网络信息安全整体解决方案，满足客户系统化、个性化的安全需求。

公司通过整合优势和平台优势，将公司已有的攻防经验、人员经验与外部情报加以整合、固化，完整的业务体系和丰富的产品种类，基本覆盖了不同行业及不同发展阶段客户的网络信息安全需求，极大地增强了公司的综合竞争力。

（4）客户资源与行业经验优势

通过持续的市场拓展，目前公司产品及服务已经进入了包括运营商、政府、能源、金融、教育、医疗等在内的众多行业，积累了上述领域大量优质客户，并长期保持着深入稳定的合作关系，这些客户自身具有雄厚的实力并在业界拥有良好的信誉，极大降低了公司的经营风险和财务风险。

公司通过在上述行业的长期耕耘与积累，与行业内的大量客户达成了紧密合作，积累了网络信息安全建设项目的实施经验，在满足客户信息化业务的发展规划及建设过程中，动态把握主要领域客户对于信息化建设的技术需求及发展趋势，进一步提高了公司产品、解决方案及服务的竞争力。

（5）品牌优势

公司凭借在自身的产品和技术优势、综合服务优势，获得了国内众多行业及专业人士的认可，“安恒信息”已成为我国网络信息安全领域的领导品牌之一。公司 Web 应用防火墙、数据库审计与风险控制系统、运维审计系统及网络安全态势感知预警平台等多款核心产品持续多年保持国内市场占有率领先的行业地位。公司在产品技术、服务和品牌等方面还获得多项国家、行业及省（市）级荣誉。

产品技术方面，先后获得“国家网络与信息安全信息通报机制先进技术支持单位”、国家信息安全漏洞共享平台（CNVD）原创漏洞报送突出贡献单位、公安部科学技术奖三等奖、全国工商联科学技术奖三等奖、中国计算机学会 CCF 科学技术杰出奖、2018 年中国电力科学技术进步奖三等奖等多项行业重要奖项与荣誉。

服务方面，先后获得由公安部网络安全保卫局颁发的“2019 国家重大活动网络安全保卫技术支持单位”和“2018 年网络安全管理优秀团队”、国家网络与信息安全信息通报中心颁发的“国家网络与信息安全信息通报——优秀技术支持单位”、2016 年 G20 峰会网络安全保卫工作技术支持单位等。安恒信息服务团队荣获了多项国家顶级信息安全服务资质，具有国家信息安全测评安全工程类三级（国内信息安全服务最高资质，目前仅有五家企业拥有该资质）、国家计算机网络应急技术处理协调中心网络安全应急服务支撑单位（国家级）、中国网络安全审查技术与认证中心应急处理一级、中国网络安全审查技术与认证中心风险评估一级等，能够为客户提供全面、规范、专业的安全服务。

四、主要业务模式、产品或服务的主要内容

（一）公司的主要业务

安恒信息自设立以来一直专注于网络信息安全领域，公司主营业务为网络信

息安全产品的研发、生产及销售，并为客户提供专业的网络信息安全服务。公司的产品及服务涉及应用安全、大数据安全、云安全、物联网安全、工业控制安全及工业互联网安全等领域。

凭借强大的研发实力和持续的产品创新，公司围绕事前、事中、事后几个维度已形成覆盖网络信息安全生命全周期的产品体系，包括网络信息安全基础产品（网络信息安全防护单品、网络信息安全检测单品）、网络信息安全平台以及网络信息安全服务，各产品线在行业中均形成了较强的竞争力。

报告期内，公司主营业务未发生重大变更。

（二）公司主要产品及服务

“没有网络安全就没有国家安全”。在信息化、互联网+、数字经济不断发展的时代，公司自成立之初即提出“数据是企业的核心资产”，围绕核心资产风险外防内防，构建事前预警、事中防御、事后溯源的全生命周期解决方案。

公司始终重视核心技术研发的作用，采用研发中心和研究院双线创新机制，取得了较好的成效。

依托网络信息安全基础类产品及公司较强的新技术整合能力，公司围绕着云计算、大数据、物联网、工业互联网为代表的新一代信息技术，形成了以“新场景、新服务”为方向的专业安全产品和服务体系。

公司在“新场景”方向围绕着新的监管政策要求、新的信息技术提出了有针对性的综合信息安全解决方案，推出了众多信息安全平台类产品，如态势感知预警平台、AiLPHA 大数据智能安全平台、天池云安全管理平台等，并逐步涉入物联网安全、工业控制及工业互联网安全等领域。该些产品正在助力众多公安机构、网信办以及其他监管部门，做到网络安全全面感知、监测预警、通报处置和监管追溯的闭环，提升网络安全监管和决策能力。并在数字经济时代的浪潮中，赋能云计算、大数据、物联网、工业互联网、人工智能与网络安全的深度融合。

公司“新服务”方向针对网络安全形势、政企用户需求的变化以及网络安全建设模式的改变，从提供专业产品向提供专业服务模式进行转变，为用户提供从安全规划、安全设计、安全建设到安全运营的一站式专业安全服务。公司风暴中心推出的 SaaS 云安全服务模式是国内较早利用云计算来提供集约化安全能力的

服务创新模式，实现了云监测、云 WAF、云 DDoS 清洗以及云端威胁情报的服务能力。上述能力加上城市安全大脑、全天候“三位一体”的态势感知、国家级网络安保团队组成了智慧城市安全运营中心服务的核心能力。

公司以基础安全产品为依托，构建的“新场景、新服务”的产品发展方向如下图所示：

注 1：安全研究院：公司设立的专门从事前沿安全攻防技术研究和新技术应用的研究机构，为公司产品技术创新提供基础研发支持。

注 2：威胁情报中心：公司设立的致力于安全数据归集共享和开发利用、研究和生产高质量核心威胁情报的团队。威胁情报中心通过提供标准化的情报库与数据接口，持续提升公司全系列产品与服务在区域安全态势感知、未知威胁检测、威胁溯源分析、主动防御等场景的威胁探测覆盖能力。

主要产品及服务情况如下：

分类	二级分类	主要产品	产品简介
网络信息安全基础产品	网络信息安全防护产品	Web 应用防火墙	解决传统网络层安全防护产品无法解决的应用层攻击威胁，抵御各种常见 Web 攻击：SQL 注入、跨站脚本攻击、数据泄露、应用层 DDOS、0day 漏洞等的影响，保护各类 Web 应用安全、稳定运行。
		综合日志审计系统	通过对客户网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，探测各种安全威胁、异常行为事件，确保用户业务的不间断运营安全。
		数据库审计	专业级的数据库协议解析设备，能够对进出核心数据

分类	二级分类	主要产品	产品简介
		与风险控制系统	库的访问流量进行数据报文字段级的解析操作，完全还原出操作细节，并给出详尽的操作返回结果，以可视化的方式进行访问痕迹呈现。
		运维审计与风险控制系统	通过账号管理、身份认证、同步监控、审计回放、自动化运维等功能，增强企业运维管理的安全访问合规性，对日常内部运维中各种误操作、恶意操作提供精细化控制和操作过程全审计。
		APT 攻击（网络战）预警平台	针对网络流量进行深度分析的一款软硬件一体化产品，能实时发现网络攻击行为，特别是新型网络攻击行为，检测能力完整覆盖整个 APT 攻击链。
		全流量深度威胁检测平台	一款对网络全流量进行深度数据包解析和审计、威胁监测、应用识别、行为溯源以及流量占用和趋势分析的软硬件一体化产品。
	网络信息安全检测产品	Web 应用弱点扫描器	利用漏洞产生的原理和渗透测试的方法，对 Web 应用进行深度弱点探测，可帮助应用开发者和管理者了解应用系统存在的脆弱性，为改善并提高应用系统安全性提供依据，帮助用户建立安全可靠的 Web 应用服务。
		信息安全等级保护检查工具箱	等级保护主体单位、监管检查部门开展等级保护网络信息安全检查的一体化专用便携式监察装备，具有规范检查、工具调用、结果展示等功能，集成定制有专门的安全检查工具。
		远程安全评估系统	提供 Web、数据库、基线配置核查、端口与服务识别等综合漏洞扫描功能，能够准确发现网络中各主机、设备、应用、数据库等存在的网络信息安全漏洞，完成整体系统的安全评估。
		网络安全事件应急处置工具箱	针对网络信息安全事件应急处置的一套专业装备。能够全程指导应急处置步骤，满足不同场景下对应急处置工具以及相关知识的需求，帮助实现网络信息安全事件的取证溯源并指导快速恢复。
		迷网系统	一种对攻击者进行欺骗的威胁检测防御系统，通过布置诱饵主机、网络服务，诱使攻击者实施攻击，对攻击行为进行捕获和分析，并通过技术和管理手段来增强实际系统的安全防护能力。
网络信息安全平台	云安全	天池云安全管理平台（私有云场景）	帮助行业私有云构建统一管理、弹性伸缩、协同防御、智能部署、满足等级保护安全能力需求的云安全资源池，能为用户提供一站式的云安全综合解决方案。
		玄武盾云防护平台	基于云计算和威胁情报能力，为私有云用户提供搭载硬件的安全流量清洗防护服务。
		安恒云（多云管理场景）	以 SaaS 化、集中化、智能化、生态化为主要特点的多云管理及安全建设平台，实现多云统一纳管、统一门户、统一运维以及统一运营。通过对云安全环境态势分析及将云安全能力统一规划管理，满足客户安全合规需求。
	大数据安全	AiLPHA 大数据智能安全平台	运用大数据技术对用户全网安全数据进行采集、集中存储管理，通过人工智能技术提高已知安全威胁检测的准确度并实现未知安全威胁的智能发现。

分类	二级分类	主要产品	产品简介
		网络安全态势感知预警平台	对用户重要信息系统、网络关键信息基础设施等 IT 资产，通过全要素的数据采集、数据治理、数据分析挖掘，结合威胁情报和管理需求。构建由被动到主动的实时网络威胁感知与预警响应能力，变被动防御为主动防御。该平台能够对网络安全威胁、隐患和事件进行通报预警和应急处置。帮助用户实时掌握网络安全态势，并开展预警通报、应急处置和管理工作。
		金融风险监测预警平台	集自有互联网大数据、行业监管数据和公安警务数据为一体的大数据分析平台。通过运用云计算、人工智能、情报挖掘等新一代信息技术，协助相关监管单位对金融风险进行全流程监测和预警。
	物联网安全	物联网安全心	一款嵌入式物联网终端防护产品，对物联网终端系统进行内核防护、数据加密和实时审计；同时能与物联网安全态势感知与管控中心联动形成云+端联动的防护技术方案，实现物联网终端安全态势感知与可信管控。
		物联网安全监测平台	采用自主研发的 SUMAP 超级搜索引擎，实现物联终端设备快速识别、漏洞检测及非法接入监测，从而实现物联网终端安全状态实时监测，是物联网终端一站式安全评估平台。
		工业控制漏洞扫描平台	针对工业控制系统漏洞的专业检测设备，通过对设备信息、漏洞信息的分析结果展示，能够让工控系统管理者全面掌握当前系统中的设备使用情况、设备分布情况、漏洞分布情况、漏洞风险趋势等内容。
网络信息安全服务	SaaS 云安全服务	云监测服务（先知）	云监测服务专注于云端安全监测，可实时对数百万个业务系统进行监测，发现暗链、黑页、后门、挂马、钓鱼、信息泄漏等安全事件，同时具备资产发现、漏洞检测和可用性监测等能力，结合 7*24 小时云安全专家服务，实时准确发现用户在线业务安全和可用性问题。
		云防护服务（玄武盾）	专注于云端安全流量清洗，基于云计算和威胁情报能力，可为用户提供零部署零运维云防护服务，抗 DDoS 清洗能力可达 2.5Tb/s，同时具备防黑、防泄露、防 CC 等业务安全防护能力。
		威胁情报服务（数据大脑）	依托 SaaS 云监测服务、云防护服务、蜜罐网络及全球资产探测等能力，提供追踪溯源、黑客画像、区域态势感知等高级威胁情报分析服务，可有效提升区域安全态势感知、未知威胁检测、威胁溯源分析、主动防御等场景的智能化程度。
	专家服务	专业安全服务	专业安全服务包括传统的安全检测服务、渗透测试服务、代码审计服务、移动 App 检测服务、风险评估服务、安全加固服务、驻场安全服务等，通过发现信息系统存在的各种安全隐患与漏洞，提出整改方案，协助客户进行安全加固，尽可能降低安全风险，抵御内外部安全攻击与入侵，保护信息资产的安全。
		可信众测服务	可信众测是安恒信息推出的一款重点为金融、政府、运营商等高端用户量身定制的安全众测服务。可信众测选取了安恒信息认证的安全测试人员，对风险等级要求较高的网站采用众测的模式进行测试，用户可以

分类	二级分类	主要产品	产品简介
			按照测试的效果进行付费，而测试人员仍按照约定的保密要求进行服务，在不增加用户的测试风险的情况下，大幅度提高安全测试的效果，同时降低安全测试的成本。
		安全咨询服务	安全咨询服务包括信息系统等级保护咨询、云安全咨询、信息系统安全规划建设咨询、ISO27001 信息安全管理体系咨询、数据安全咨询以及安全开发生命周期咨询。随着信息安全等级保护工作进入 2.0 时代，安恒信息通过专业和体系的安全咨询服务结合公司全产品线的优势，帮助客户开展符合等级保护 2.0 要求的信息系统安全保障体系的规划与建设。
		平台运营服务	为公司网络安全态势感知预警平台、AiLPHA 大数据智能安全平台及云平台用户提供的深度安全运营服务。通过深度数据分析，协助客户进行持续的安全威胁分析、安全检测、策略优化、实战演练和应急处理，建立积极防御体系。
		应急响应服务	应急响应服务包括 7*24 小时安全事件应急处置及应急演练两部分内容。其中安恒信息应急演练服务包括应急预案制定、应急演练平台构建、红蓝对抗服务等全场景演练内容。应急响应服务结合安恒信息应急响应工具箱和应急指挥平台，提供快速高效的处置能力。
		国家重大活动网络安保服务	国家重大活动网络安保服务是安恒信息最具品牌影响力和知名度的综合安全服务，在国家重大活动期间为活动主办方、监管机构、政企单位提供整体网络安全保障计划、方案及能力，通过专业有效的安全平台、安全设备，结合全方位的安全保障服务，确保活动的顺利举办，有效降低网络攻击风险。国家重大活动网络安保服务均具有任务重、要求高、影响大的特点。安恒信息凭借丰富的经验和一支融合专业技术精、素质高、有经验、能打持久战、能打胜仗的网络安保队伍，为每次重大活动网络安保提供坚实的护航力量。自 2008 年至今，安恒信息共参与近百场国家重要活动/事件的网络安保，多次承担安保组长及中坚力量的职责，确保网络安保工作万无一失。
	智慧城市安全运营中心服务		城市级安全运营保障平台，能实现对全市数字基础设施、重要数字资产和信息系统进行全天候全方位的安全监测、通报预警和应急处置，并提供统一的基础安全防护服务。
	网络安全人才培养服务		依托公司产品与服务经验，对产业资源、行业案例以及成熟的项目经验进行整理，并完成教育资源转化。公司开发了符合教学、应急演练和安全测试场景的攻防实验室平台、攻防演练平台和攻防靶场平台。 服务主要包括：协助在校学生、在职人员展开安全技能培训与国家认证培训；提供在线的网络信息安全人才学习平台。

（三）公司的主要经营模式

1、盈利模式

公司盈利主要来源于自主研发的网络信息安全产品的销售，以及为客户提供专业的网络信息安全服务。网络信息安全产品包括基础类产品（安全防护类产品、安全检测类产品）、平台类安全产品；网络信息安全服务，包括 SaaS 云安全服务、专家服务、智慧城市安全运营中心、国家重大活动网络安保服务、网络信息安全人才培养服务。

2、采购模式

公司采购的主要物料为相关产品、服务、解决方案所需的各类硬件设备及相关配件，采购的主要内容为以下三个方面：（1）网络信息安全产品使用的工控机、服务器及相关配件；（2）网络安全解决方案相关的第三方软硬件（3）第三方实施安装服务。

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。公司整体上建立《采购管理制度》规范采购行为，并设立采购部负责公司采购的执行，采购部根据需求部门提交的采购单，按供应商分类建立供应商台帐。

对于保证自身产品正常运行的软硬件等原材料，通常由公司供应链管理中心汇总项目需求后提交《原料内部审批表》，经部门负责人、财务部、分管负责人审批后，由供应链管理中心在 ERP 系统上建立请购单，提交给采购部采购负责人；对于合同第三方产品采购由销售合同商务评审后，由供应链管理中心在 ERP 系统上建立请购单，提交给采购部采购负责人。

为满足公司网络信息安全产品和服务的质量要求，公司会根据供应商提供产品的供货能力、质量、价格、付款方式、售后服务及供应商的信誉度等诸因素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。

由于公司资质信誉良好，主要供应商会给予公司 1-3 个月信用期。

3、生产模式

公司按照行业定制化产品和通用化标准产品的不同，分别实行订单驱动式生

产和季度预测式生产。由于生产的产品形态主要为软硬件结合产品，公司采购相应软硬件原材料后进行组装调试，然后将自主研发的软件灌装入硬件设备中，最后经拷机测试、产品质量检验、入库等环节完成生产，并通过快递公司发货至下游客户。

4、销售模式

报告期内，公司在产品销售上采用多级渠道经销和直接销售相结合的方式，并且充分依靠渠道销售等合作伙伴以最大程度实现市场覆盖。其中，渠道代理销售是指先将产品销售给渠道代理商，再由渠道代理商将产品销售给终端用户。直销模式是指直接将产品销售给终端用户。公司不同销售模式下的销售情况如下：

单位：万元

销售模式	2020 年 1-9 月		2019 年度		2018 年度		2017 年度	
	收入	占比	收入	占比	收入	占比	收入	占比
直销	29,157.87	44.50%	39,258.55	41.74%	27,613.95	44.07%	19,298.79	44.84%
渠道	36,368.53	55.50%	54,795.47	58.26%	35,044.73	55.93%	23,741.02	55.16%
合计	65,526.40	100.00%	94,054.03	100.00%	62,658.68	100.00%	43,039.81	100.00%

公司采取多级渠道经销和直接销售相结合的销售模式主要是因为公司产品的目标用户群多、用户的地域及行业分布广，采用该方式能够最大程度实现市场覆盖、最高效率为客户提供网络信息安全产品及服务。

（1）渠道模式

1）渠道经销商体系

公司根据不同客户的规模、需求特性，选择与不同特点的系统集成商进行合作，签订战略合作协议、商业总代理合作协议、商业二级代理合作协议、行业代理合作协议、安恒云代理合作协议或安全服务合作协议，将其加入公司渠道经销商体系。此外，为保证销售服务有序开展，渠道经销商均须先进行项目报备后才能下单销售。

2）公司对渠道经销商的管理

公司通过与渠道经销商签订框架性合作协议的方式确定合作关系。上述协议对渠道经销商类别、经销区域和行业、合作期限、授权产品、供货价格、资格要求、购销计划、结算付款、项目管理、销售支持和技术服务等内容进行了明确约定。

公司与渠道经销商签订合作协议后，渠道经销商需配置相应数量的在职人员并参加公司组织的培训。公司会对渠道经销商相关人员提供必要的市场销售、技术、项目实施等方面的培训与指导，并不定期组织集中培训，保障最终用户获得优质的产品和服务。

（2）直接销售模式

公司在全国各主要省份设有分公司或办事处等本地化分支机构，分支机构具备销售和售前售后等综合服务能力，以向国家级部委、省市级政府，以及电信运营商、金融、能源企业集团等战略性客户和重要客户提供直接服务。公司按照与终端客户签订的项目合同，根据项目进度收取货款。

五、科技创新水平以及保持科技创新能力的机制或措施

（一）科技创新水平

公司主营业务为信息安全产品的研发、生产及销售，并为客户提供专业的信息安全服务，于成立之初便以应用安全和数据安全作为切入点，推出市场首创性产品数据库审计系统与 Web 应用防火墙产品，成功进入信息安全市场并迅速成为应用及数据安全领域领军企业。目前公司在我国应用和数据安全市场处于行业领先位置，公司核心基础安全产品持续多年市场份额位居行业前列。此外，公司核心产品的前瞻性和影响力也获得了 Gartner、IDC 等国外权威机构认可。2019 年度，公司研发人员占总人数比超 30%，研发投入占总收入比超 20%，是国家级高新技术企业。

公司自创立以来始终坚持持续技术创新的发展战略，紧跟信息安全技术发展趋势和用户需求，不断在行业内率先推出创新产品，更新迭代既有产品和解决方案，并孵化培育新产品，提升市场竞争力。凭借优秀的技术研发团队及强大的技术创新能力，公司在 Web 应用安全、数据库审计、态势感知、云安全及大数据安全等领域实现了多项技术突破。截至本募集说明书出具日，公司共拥有 48 项核心技术，其中 22 项是公司基于云安全、大数据安全、物联网安全和智慧城市安全等新兴安全领域进行深入研发积累所得，该等核心技术确保了公司在多个相关细分市场处于行业领先位置。公司现有核心技术按照技术应用方向主要可以分为 13 项大类技术，该等核心技术先进性及产业应用情况具体如下：

（1）全网资产测绘技术

该技术旨在探测全球联网资产信息及脆弱性，提供安全感知、威胁预警以及风险检测能力。该技术结合大数据处理算法能实现高并发、低时延、全网覆盖、快速迭代的网络信息数据收集，并发探测速度达到 60 万每秒，能够识别分析 20 万种设备及 300 多种协议，在 2 小时内可完成全网探测。相比传统网络扫描技术，公司全网资产测绘技术采用大数据群集架构、插件化开发方式，具备更好的兼容及探测性能。该技术迭代紧跟新协议的应用、新安全漏洞发现频率，与全网资产及前沿技术产品紧密相关，需要对全网资产通讯协议及设备指纹进行长期持续的分析和数据积累，以覆盖大量通讯协议及 IP 数据，技术门槛较高。目前国际范围内同类技术主要有 Shodan 和 Zoomeye，公司该项技术在识别指纹量、并发的探测速度方面有较大优势，处于国际领先水平。

该技术是目前新兴的全球联网设备探测技术，未来主要向支持所有已知工控协议、物联网协议、网络通信协议的资产探测发展，并不断积累指数级别增长的全网实时数据，从而提升实时威胁预警、全网态势感知、精确脆弱性分布探测能力。

（2）多协议解析与数据治理技术

目前业界传统的数据解析与治理手段，主要基于静态的协议解析规则进行匹配，难以从云环境获取流量进行解析，无法实现对数据解析精准度的动态优化调整，公司该技术实现了对协议解析内容的动态跟踪，进一步反馈闭环调整提升了数据解析准确率，适用于 VMware、阿里云、华为云、天翼云等 90%以上国内外主流云环境，在协议解析识别广度（物理环境与云环境）、协议识别深度（协议行为特征、传输内容特征等）、协议检测精准度（数据库操作行为、邮件病毒、邮件域名、邮件附件别名等）较传统技术而言具有较大的优势。当该技术应用于数据库行为审计和邮件行为审计时，能实现对数据库操作行为数据和邮件行为数据的全方位解析，公司基于该项技术的日志审计产品和数据库审计产品均排在国内行业前列。

（3）运维访问控制审计技术

该技术可实现各种传统环境、专有云、公有云平台等各类资产的运维接入，

一机多用降低了企业内控建设的成本。基于该技术的深度协议代理解析引擎能够兼容支持市场上 3200 多种不同品牌及版本的资产设备，相比业内通用的协议有损还原，该技术可 100%还原协议细节特性及运维操作过程，保证了审计日志的权威性，是业内领先的运维审计控制技术，公司基于该项技术的运维审计产品目前市场占比居于国内领先地位。

目前该技术已经趋于成熟，迭代周期为 6-9 个月，技术的核心难度在协议代理兼容性、业务模型、用户运维习惯、统一认证平台、资产管理平台集成等方面的实践积累，短期内很难实现与该技术相当的功能水平，替代难度较大。

（4）Web 应用透明代理与深度攻击检测防护技术

该技术主要应用于透明网络环境下的各种 web 攻击检测，在网络接入层面兼容性强，转发性能相比于传统内核态转发技术，具有快速转发、低时延等优势，最高单机可处理 10Gbps 的应用层转发任务。基于该技术的用户态协议代理引擎具备实时双向数据包检测的能力，能识别包括无特征的攻击行为及 0day 攻击行为等在内复杂攻击行为，提升 Web 攻击防护准确率。

该技术大幅提升了公司 Web 应用安全产品的业务兼容性及数据包代理转发的性能，降低了攻击检测的误报率和漏报率，有效弥补了传统特征引擎检测技术高误报、高漏报等缺点，帮助公司 WAF 产品获得领先的 Web 攻击检测能力，使得公司成为国内 WAF 产品领先者。目前该技术日趋成熟，技术架构迭代周期约为 6 个月，攻击行为检测迭代周期 1-7 天。该技术需要在网络数据包快速转发、业务兼容、攻击检测算法模型方面大量实践经验积累，很难在短期内有较大的技术突破，替代难度较高。

（5）基于网络流量的未知威胁及 APT 攻击检测技术

基于对样本的动静态分析及基因图谱分析能力，该技术能有效发现 0day 样本及变种木马。在动态沙箱检测恶意文件领域，该技术通过对 Windows 文件过滤驱动实现文件重定向等功能，使沙箱具备防虚拟机检测、防调试器检测和防钩子检测等能力，共 200 种防逃逸机制、近似零时间消耗的快速还原检测环境的技术及单沙箱并发检测多个样本的能力，目前单沙箱一天可检测非 PE 文件达 4000 个，根据不同文件类型，一套沙箱系统一天可检测文件 12 万以上，处于业界领先位置。

该技术涉及的 Windows 内核层隔离模块在所有内核驱动开发中属于难度层级高、文档资料少的领域。因 Windows 系统的闭源特点，部分功能开发甚至需要逆向工程技术并配合复杂的调试过程，精通该类内核开发、调试并兼具逆向工程的高端开发人才稀缺，使得该技术具备较高的准入门槛；同时该技术包含的基因图谱分析需要通过对大量恶意样本进行深入分析和归纳，并通过软件块化、片段化、归一化及数据库存储和搜索技术来制定软件基因库，由于相关的二进制分析高度专业性以及收集大量恶意样本所需的渠道与时间成本，使得该技术准入门槛很高，可替代性较低。

（6）分布式漏洞发现与验证技术

相较业内同类技术，该技术具备漏洞发现率高、误报率低、对目标系统运行影响低等特点，凭借公司积累的 40,000 量级漏洞库实现业内领先的漏洞覆盖率。该技术通过分布式扫描方式加快了漏洞扫描速度与稳定性，扫描速度较传统技术提升 30%，同时利用动态流量控制方式减少了扫描对目标系统的影响。公司安全研究院借助该项技术多次在全球首先发现包括 JAVA 框架 Struts2 的 S-045、S-046 等在内的重大漏洞，基于该项技术的漏洞扫描系列产品目前市场占比排名前三。

该技术的迭代频率一般与漏洞挖掘的频率和网络公开漏洞的频率保持一致，通过实时爬取网络漏洞的方式，进行每日自动更新。由于该类技术的漏洞发现率和误报率性能改良需要掌握大量渗透测试技术、网络爬虫技术、流量控制技术以及代码语言特性的分析技术，壁垒较高，可替代性低。

（7）基于云架构的安全扫描与监测技术

业界的安全检测技术主要通过硬件盒子方式实现，检测能力受硬件性能限制，存在慢报及误报等问题。公司基于云架构的安全扫描与监测技术是国内首批运用 SaaS 模式进行安全检测的技术。该技术基于网站安全领域的安全事件监测技术，通过运用机器学习技术对全国 670 万 ICP 网站首页抽检样本进行分析、训练，能够实现文本语义准确分析识别，并结合公司威胁情报能力有效解决了孤链监测问题，丰富和扩展了黑名单库，大幅降低监测误报率并提升检测范围，能实现大容量、高并发、高准确率、高检出率的网站实时监测。该技术能做到检测数据完全自动标签化，自动化数据校验率达到 90%以上，当前监测网站数量峰值达

到 1,096,725 个（次）/天，平均监测值约为 476,880 个（次）/天。

相比较传统安全事件监测技术，公司的监测技术依托云端大数据能力处理分析海量安全事件样本，监测发现率不低于 95%。目前国内掌握同类技术的企业主要有知道创宇、奇安信等，公司监测技术在发现率和准确率上有较大优势，处于领先水平。

（8）SaaS 化云安全防护技术

业界的安全防护产品主要通过硬件方式，部署运维困难，防御能力受设备性能限制，检测误报率高且较难发现复杂的黑客攻击，难以对超大流量 DDoS、新型攻击进行防范。公司基于 SaaS 化云架构的安全防护技术在用户端无需部署任何软硬件，通过网络接入系统后，即可为用户提供远程实时安全防护，网络层最大清洗能力达到 2.5T/sDDoS。该技术区别于传统规则检测，通过自然语言处理和人工智能深度学习算法对云端每日 22.8 亿次访问数据进行采样分析，能够大幅提高召回率，降低误报率，2019 年度识别扫描 IP69.4 万个，每天拦截扫描攻击近 1.3 亿次，误报率仅为 1‰，实现对入侵、篡改、数据窃取、CC 等多种攻击的防护，技术领先性受到学术认可，曾被《信息安全研究》期刊收录，是国内首批运用云端威胁情报能力进行防范的技术。

该技术利用云端每日十亿级的访问数据采样分析过程进行模型训练，可以周为单位快速迭代优化自身安全检测算法，而传统安全防护技术并不具备该等庞大的云端数据基础支持。随着时间推进，公司该项技术将进一步拉开与业界主流的传统防护技术的性能差距。

（9）云平台融合对接和统一编排管理技术

目前业界云平台的 API 开放性、标准性较低，导致众多云安全解决方案和云安全产品难以交付、使用复杂、防护效果较差。公司是国内首批开展和云平台对接融合的安全厂商，已与华为云、浪潮云、OpenStack 等 3 家国内主流云服务商完成对接融合，并在此基础上研发提炼了一套云平台融合对接和统一编排管理技术。该技术可实现云管理平台、云安全管理平台、云安全产品三者的统一认证、授权、监测及管理，能够将安全产品与云平台的对接时间控制在 10 天左右，而行业平均对接时间在 30 天以上，单个安全模块的交付时间从数十分钟缩短到 60 秒以内。

该技术采用软件定义网络和容器化技术，相对同行业安全公司的手动编排和引流技术，实现了资产安全防护和安全流量路径的自动化编排，使得云上安全使用更加灵活简易。目前该技术能够兼容国内主流云平台，支持不同云平台的统一用户和管理，在对接效率、编排能力方面国内领先，云平台的对接成功数量，落地的实际案例也处于领先地位。公司与华为云、浪潮云融合对接的云安全解决方案，通过获得了 CSA 云安全联盟和公安部第三研究所的测评认证，获得了颁发的云计算产品信息安全认证证书和 CSACSTR 增强级证书和云计算产品信息安全认证证书（增强级），是业界首例安全厂商和云平台厂商融合对接云安全解决方案家的联合认证。

目前该技术和华为云、浪潮云版本基本保持同步更新迭代，平均迭代周期为一个季度。由于目前国内云平台标准化、开放性较低，要建立一套能够适配多云的对接方案，并提炼出标准 API 具有较高的技术难度。同时，云平台的融合具有较强的兼容依赖性，云平台厂商迁移成本高，因此该技术不可替代性较高，先发优势明显。未来该技术将向自动化、数据融合、接口标准化发展。同时，平台内云安全组件向轻量化发展，公司后续将探索云安全组件的全容器化，提升资源利用率和跨云平台的支持，以满足未来公有云和混合云的云安全防护需求。

（10）大数据深度安全检测与分析技术

业界传统的安全检测手段主要基于静态的策略规则匹配，一般采用阈值触发、关键词触发、情报对比触发等手段，存在数据量小、检测手段单一、时效性差、分析结果准确度低、风险事件定位难等问题。公司在国内率先提出安全分析模型自适应理念，并在产品中实现功能化。相比业界通用的安全检测分析技术，该技术在国内率先实现周期性异常事件检测，解决了多源异构数据的快速复杂关联分析与检索问题，并利用基于机器学习的扫描 IP 分类、策略自学习和优化、DGA 域名快速判别等 100 多个安全场景识别方法，能够实现多维度、细粒度的安全事件分析与跟踪，大幅提升风险定位的准确度，公司基于此项技术产品已发布多个迭代版本，技术处于国内领先水平。

（11）态势感知分析与挖掘技术

业内大多态势感知技术或产品仅停留在基于日志搜集统计可视化或网站漏

洞扫描统计可视化阶段，以少量维度的数据采集手段，加上简单的统计排序分析手段，配以可视化页面，实现初步的态势感知功能。公司大数据态势感知分析与挖掘技术真正围绕网络安全态势感知的三要素:态势获取、态势理解和态势预测，以发掘深度威胁和隐患为目标，对能够引发网络安全态势发生变化的要素进行全面、快速、准确地捕获和基础分析。相比业内同类技术，该技术具备实时在线还原恶意样本和域名能力，通过使用内置威胁情报匹配辅助验证功能，使流量的有效识别率提升至 99%以上，告警准确率达到 90%以上。并为恶意样本提供沉浸式的运行环境和无感调试，大幅降低恶意样本的反调试成功率，从恶意特征匹配转变为基于样本异常行为检测技术，该技术处于国内领先水平。基于该技术的态势感知平台产品在实战中多次输出具有重要价值的网络战情报，尤其是在重大活动网络安全保障期间多次输出黑客攻击的预警和攻击的发现。威胁线索分析和网络攻击追溯能力处于领先水平，对同源黑客的追踪和匹配上准确率达到 95%。

（12）物联网可信互联与智能防护技术

该技术具备较强的跨平台能力和较好的可移植性，能够实现端到端的安全加密，密钥分发能力高达 20000 次/S，单次加密延时低于 1.66ms，对终端数据传输效率几乎无影响。相比于传统网络层安全防护技术，该技术可以深入物联网终端内部进行安全防护，通过驱动级安全防护结合云端智能分析的防护能力构建完整的物联网安全防护体系，技术具有独创性。

（13）面向工业控制系统安全的定量评估和全生命周期防护技术

该技术是公司围绕国内火电、核电、冶金、石化的工业安全现状，在现有安全防护技术的基础上，提出的一种被动防御与主动防御相结合的安全防护技术。针对工控系统攻击机理和系统架构与业务特征，实现了覆盖工控系统各层级、全业务流程的异常检测，以及对工控系统未知威胁的主动发现，解决了跨越信息物理空间未知威胁的检测难题。该技术在线实时测评技术框架，综合考虑了各种度量因子，突破了工控安全难以度量、评估的技术瓶颈，在安全防护体系和主动防御理念方面均具有先进性，能够深度解析超过 30 种私有工控协议，提取 300 种以上主要的工业控制系统网络协议功能码，在理想状态下单个扫描任务速率达到每秒 160 万包，相关技术正在申请国家专利，已达到国内领先水平。

（二）保持科技创新能力的机制或措施

1、全面的创新研发模式

首先，公司选拔资深技术骨干组成安恒技术委员会。技术委员会通过接受业务需求部门对网络信息安全行业技术发展方面的调研信息，预测把控未来五年内的技术演进趋势和行业发展方向。

其次，公司在部门设置上设立安全研究院，致力于前沿技术预研、创新业务探索和核心能力积累，在保持技术领先性的基础上，实现由预研技术向具体产品的孵化。安全研究院下设海特实验室和卫兵实验室，多年来在云安全、大数据安全、物联网安全、应用安全、人工智能、数据加密领域等均有重要输出，其中已研前沿技术及产品原型包括：全球化高速网络探测系统、全球化网络扫描系统、先进漏洞挖掘技术、文件威胁溯源技术、APT 攻击检测技术、互联网应用加密技术、互联网金融风险监测技术等。

最后，公司设立多个产品研发中心。在安全研究院对前沿技术的探索取得阶段性成果后，研发中心承担具体产品的开发与落地工作。将理论研究的结果与网络信息安全的现实需求验证对比，把抽象的理论模型转换为具体的产品功能，并通过多轮测试与升级，完善产品功能模块。最终推出兼具技术先进性和功能完善性的产品，进行批量化生产投放市场。

此外，公司内部成立网络空间安全学院，先后与北京航空航天大学、电子科技大学、哈尔滨工业大学、南京邮电大学、上海交通大学、浙江大学、中国科学技术大学等多所一流高校展开全面合作，通过“产学研用”融合驱动校企协同育人、联合技术研发和合作技术成果转化，一方面服务于国家网络信息安全人才工程，同时驱动自主技术创新。同时公司还设立安恒信息创新专项基金，从创新人才职业规划、专业技术能力提升、创新激励等方面全方位服务自身发展人力资源战略。

2、全方位的人才培养和激励模式

（1）内部培训

人才的培养，需要长远清晰的职业规划。为此，公司在内部成立安恒大学，协助公司创新人才进行职业生涯规划，建立包括人才等级评聘、岗位任职制度、

重点员工培养计划等，使公司创新人才在发展方向上，拓宽发展面，保证核心骨干员工的稳定。

公司还创建了网络空间安全学院，助力网络信息安全人员技术能力的提升：第一、网络空间安全学院依托公司自身领先的产品和服务，把产业资源、行业案例，以及成熟的项目经验进行整理，并相应转化为教育资源，实现公司内部知识沉淀和传递，使技术人员能够通过在线学习和练习，掌握最新的安全检测与防御能力；第二、网络空间安全学院通过公司业务对接安全服务实际需求，使安全技术人员在线承担安全服务，理论结合实践进行检验；第三、网络空间安全学院构建在线考核和竞赛服务平台，通过多轮考核竞赛的方式使技术人员对自身水平有精准定位，为安全服务人员进行技术能力画像；第四、网络空间安全学院与各类招聘网站进行在线对接，为安全人员进行第三方能力背书，在为公司培养安全专业技术人才的同时，也能够实现对外培养输送。

（2）外部培训

公司在自身培养网络信息安全类专业技术人才的同时，还与全国 60 多所高校建立了各种形式的校企合作，协助培训专业网络信息安全人才，包括像浙江大学、北京航空航天大学、哈尔滨工业大学等 985 高校一起培养高端网络信息安全人才，也与温州职业技术学院、杭州职业技术学院等专科类学校培养网络信息安全一线工程师队伍，为完善国内网络信息安全人才梯队做出贡献。

（3）吸引人的激励制度

在激励创新措施上，公司成立“安恒信息创新专项基金”，并设立优秀员工、安恒之星、安恒战士、安恒工匠、总裁特别奖等各类奖项，对在硬件设计工艺创新、服务模式创新、销售模式创新、安全研究创新、产品研发创新过程中有突出贡献的员工予以奖励。

公司遵循“以人为本”的原则，把人才作为公司最宝贵的财富，重视和加强人员投入，建立了有竞争力的薪酬激励体系，为优秀者提供去美国硅谷培训或工作的机会。

3、广泛开展外部合作，积极参与国家级、省市级重大科研计划和标准制定

基于安全研究院对网络信息安全领域的前沿探索能力和产品研发中心强大

的产品开发能力，公司以明鉴事业部、安全研究院、风暴中心、AiLPHA 大数据实验室等研究性部门为载体，先后与浙江大学、浙江工业大学、浙江工商大学、杭州电子科技大学、杭州师范大学等国内多所高校开展全方面的科研合作，参与相关科研项目筹划和研究工作。激励科研人员积极创新、自主研发，完善合作机制，充分利用社会创新资源，降低创新风险，提高创新成效。

公司也得到了国内各级政府的肯定和支持，现已承担“国家发改委信息安全专项”、“工信部电子发展基金项目”、“科技部火炬计划”、“科技部网络空间重点专项”、“浙江省重点科技专项”等多项国家级、省市级重大科技计划项目。

与此同时，公司还参与了 9 项网络信息安全国家、4 项行业技术标准的研究制定，积极引领技术标准在网络信息安全产品中落地。公司产品在技术持续领先、功能不断丰富的同时，全面符合国家规定以及行业内部的技术规范。

4、科学完善的管理体系架构以及严谨的研发内控制度

目前，公司已建立较为完善的管理体系架构，自身科研开发和工程质量管理体系已通过国际 ISO9001 和 ISO14001 管理体系认证，具备行业内 ISO27001：2013 信息安全管理体系认证，并且开发过程已通过 CMMI5 级管理认证，以及涉密信息系统集成甲级资质。公司从需求分析、工程设计、软件开发、项目实施和工程服务，具备完整、严密的管理规定。

此外，公司还建立了一系列研发相关内控制度，包括项目开发流程规范及成果管理，具体包括《研发管理制度》、《安恒开发流程规范 2.0》、《知识产权管理制度》、《商标管理办法》、《专利奖励办法》以及一系列知识产权管理办法。同时，研发过程中严格执行《固定资产管理制度》、《无形资产管理制度》和《财务报销制度》等制度，对研发项目对应的人、财、物以及研发支出进行管理。

5、大量投入创新相关的基础设施建设

为保证产品创新和管理全面落实到位，公司在完善自身体系建设的同时，还大量投入与创新相关的基础设施建设。一方面，公司采购上百台高配置服务器支撑业务体系运行；另一方面，公司为提高产品开发质量，公司管理上遵循 ISO9001、ISO/IEC27001、能力成熟度集成模型最高级 CMMI5 管理体系的要求，

还采购建设多项先进软件开发与管理系统进行产品发开：①采购项目管理系统、MIPS 多核开发平台、BUG 管理跟踪、DPS 代码检测等智能软件系统等来提高产品创新开发质量，支撑员工完成创新性研发工作；②在需求管理及研发项目管理方面采购禅道和 Mainsoft 软件系统；③在配置管理方面采用了 SVN、GIT 系统对产品开发过程中输入/输出进行管理，并对工作成果进行实时备份、本地/异地备份；④在代码管理方面采用 Jenkins 集成 PC-Lint、Findbugs 进行代码审计；⑤在代码集成方面采用 Jenkins 集成产品打包脚本，自动完成代码集成部署；⑥在 Bug 管理方面有禅道系统进行 Bug 管理跟踪；⑦在系统集成测试实验室器材上做了大量投入，拥有专业的测试环境、网络设备和业内先进的测试仪表：思博伦 SPT-3U、JMeter 等；⑧结合产品管理要求自主开发了升级包管理系统、授权许可证管理系统、测试用例管理系统；⑨公司产品研发中心还有专门的受控配置服务器，进行工作成果本地及异地备份；⑩在网络环境方面，公司开发网和办公网物理隔离，相互独立，分支结构和移动办公人员可以通过 VPN 系统接入办公网，同时采用网络视频会议系统等信息化工具以随时保持信息沟通。此外，为使公司内部人员方便快捷地共享信息，具备更加完善的审核流程，公司采用 OA 系统高效协同办公，在客户关系管理方面有客户关系管理（CRM）系统，对业务进行高效支持。

六、现有业务发展安排及未来发展战略

（一）现有业务发展情况

得益于网络信息安全行业的快速发展和公司在新一代安全产品、安全服务业务的提前布局，2017-2019 年度，公司分别实现营业收入 43,039.81 万元、62,658.68 万元及 94,403.29 万元，2018 年较 2017 年增长 45.58%，2019 年较 2018 年增长 50.66%，业务增长势头强劲。

报告期内，公司始终坚持“云、大、物、智”的发展战略，积极贴合网络安全防护需求的变化，结合自身在云安全、大数据安全等领域的技术积累，致力于为客户提供更加完善的安全产品和安全解决方案，持续稳健发展。

在云安全业务领域，公司充分应用云原生技术，进一步增强了安全算力的弹性化、智能化进程，加速了产品云化的能力；天池云安全管理平台目前已完成华

为鲲鹏、海光 CPU 的技术兼容适配工作，并获得相关生态的技术互认证证书；在战略合作方面，公司继续保持着与华为云、阿里云等云服务商的良好合作关系，完成了华为云新版本的适配工作，并获得了阿里云 MSP 合作伙伴的认证。2020 年 9 月，公司推出安恒云平台，集多云管理和多云安全管理于一体，能够为客户提供 SaaS 化的多云场景、混合云场景的一站式安全防护服务。同时，安恒云平台能够连接国内外主流云平台以及传统数据中心，有助于智慧城市的落地和城市数字化转型。

在大数据安全业务领域，公司继续深耕公安、网信、金融、大数据局等多个行业及领域。基于大数据、人工智能、SOAR、UEBA 以及 IPDRR 等前沿技术，公司不断研发并优化新一代网络安全态势感知平台，为监管客户打造可进行统一协调指挥的实战化网络空间态势感知预警平台，为企业级客户构建网格化、常态化的纵深防御安全运营体系；同时，公司在全国范围内率先推出了网络安全大数据分析建模服务，为客户提供更符合其业务场景的智能安全威胁检测能力。

在物联网及工业互联网安全业务领域，公司继续专注于产品研发，加快版本迭代，推出了非接触式的云端物联网安全 SaaS 检测平台，并加快以“物联网安全心”为核心技术的物联网安全解决方案的全国推广，公司已与数源科技、云从科技在物联网市场拓展方面达成了战略合作；与此同时，公司着力打造以“一池一脑一网，多平台多生态”的一站式工业互联网安全服务平台，进一步提高公司在工业互联网领域的竞争力，营造工业互联网发展生态，协助推进工业互联网的高质量发展。

在智慧城市业务领域，公司加速布局，积极参与各地城市大数据平台（城市大脑）项目建设，为多个省市的大数据平台建设提供了安全保障服务。同时公司以体系、平台、人才赋能三位一体打造“智慧城市安全运营中心”，通过网络安全体系架构和运行机制的改造、“大数据+安全智能”为核心的安全大脑平台建设、本地化专业安全服务团队的组建，构建了城市级网络安全保障机制，并实现了区域关键信息基础设施、党政机关和企事业单位重要信息系统、工业互联网设施的全方位保护。智慧城市项目通过统一集中运营管理及常态化的威胁发现和应急处置，提高城市管理者决策的科学性和精准性，实现用“数据说话、用数据决策、用数据管理”的城市安全管理新模式。

在安全服务领域，公司以玄武盾为核心的云防护、云监测服务、以安全数据大脑为核心的情报订阅、行业监管 SaaS 服务模式，成功的为多个省市的政务云、政府网站群、政府在线系统提供了 7*24 小时云安全服务。专家服务方面，公司坚持服务一体化的拓展思路，布局重点区域及行业，加强生态合作，进一步实现创新型安全服务商业模式。

（二）未来发展战略

1、公司整体发展目标

（1）企业愿景

公司秉承“助力安全中国、助推数字经济”的企业使命，以“成就客户，责任至上，开放创新，以人为本，共同成长”作为企业价值观，不断提高核心技术创新能力，致力于成为一家具有优秀企业文化和社会责任感的新时代网络信息安全产品和服务提供商。

（2）技术方向

未来公司将牢牢抓住网络强国和数字中国战略背景下网络信息安全行业市场发展机遇，依托多年积累的行业经验，围绕“云、大、物、智”开发适用新技术、适应新场景的网络信息安全新产品，提供综合网络信息安全解决方案，具备真正的城市级感知、防护和运营能力。

（3）品牌及渠道建设

公司将依托西湖论剑网络安全大会的影响力，不断扩大产业生态圈的合作，深化渠道建设，发挥规模化的经营效应，加强品牌建设力度；为客户提供全生命周期的安全解决方案，力争成为新时代网络信息安全领域的领导者。

2、未来发展规划

未来公司将继续保持在网络信息安全领域的研发投入，并且不断深化产品和服务结构，持续提升云安全、大数据安全、物联网安全和智慧城市安全领域的竞争力。公司将从以下六个方面进行重点投入：

首先，公司未来希望成为重大安全风险的监测者，帮助监管部门利用态势感知平台，对全网进行全面监测，在这个基础上开发金融风险监测预警平台和涉网

犯罪侦查打击平台，协助公安和监管客户提高涉网犯罪侦查打击能力和金融风险监测预警能力，并且利用态势感知平台承担重大活动的安全保卫工作，针对关键基础设施，提供监测和保护服务。

第二，公司未来希望成为数字经济发展的助力者，利用公司在大数据智能安全分析、云安全防护、数据安全保障等领域的技术优势，解决大量的数据信息孤岛、信息不对称问题，为数据共享与业务协同的战略任务提供全生命周期的安全监测与防护整体解决方案，保障数据流动效率。

第三，公司未来希望成为信创产业的先行者，依托在网络安全领域的产品技术和人才基础，对公司基础及平台产品进行国产化适配，并全面开展信创领域的安全咨询、安全集成、安全运营等工作，加强对运维访问控制审计技术、分布式漏洞发现与验证技术、基于云架构的安全扫描与监测技术、SaaS 化云安全防护等技术的研发力度，推进和适应我国信息产品国产化替代趋势。

第四，公司未来希望成为网络安全人才的培养者，建设网络安全云靶场平台，为网络安全从业人员提供网络空间仿真实训竞技平台，为学校、大型企业和政府提供专业信息安全培训工具，并结合自身网络安全教育培训业务，丰富我国网络安全人才培养模式，提高网络安全人才培养能力和水平。

第五，公司未来希望成为企业数字化转型的守护者，全面防护工业互联网平台，保护企业数字化过程中终端、设备与云端服务。与物联网运营商共同提升物联网终端安全性，重点投入车联网安全和视频终端安全。

最后，公司未来希望成为新型智慧城市安全的运营者，在城市数字化、万物互联的背景下，依托互联网、物联网和工业互联网三网合一的态势感知技术，结合玄武盾与安全大脑的能力，利用团队多年国家重大活动网络安保经验，建立城市级安全运营中心，提供全方位的安全运营服务。

第二节　本次证券发行概要

一、本次发行的背景和目的

（一）本次发行的背景

1、信息安全上升至国家战略，利好政策助推产业发展

在我国综合实力不断增强，国家发展迎来机遇的同时，国家安全面临着诸多挑战。我国网络安全形势日益多样化、复杂化。在此背景下，信息安全上升至国家战略。2013 年以来，我国先后设立中央国家安全委员会、中央网络安全和信息化委员会，制定并颁布新的《中华人民共和国国家安全法》、《中华人民共和国网络安全法》及相应的配套法规，制定《国家网络空间安全战略》、《“十三五”国家信息化规划》、《软件和信息技术服务业发展规划（2016－2020）》、《信息通信网络与信息安全规划（2016-2020）》等政策，从制度、法规以及政策等维度促进网络安全的不断发展。同时，云计算、大数据、人工智能等新兴技术的加速发展使得网络安全产品的应用环境日益复杂，数据泄露、高危漏洞等网络安全问题频发，信息安全产品及技术迭代加速，进一步推升网络安全市场需求。

根据中国信通院 2020 年 9 月发布的《中国网络安全产业白皮书》，2019 年我国网络安全产业规模达到 1,563.59 亿元，同比增长 17.1%。根据最新发布的《IDC 全球网络安全支出指南》，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 1,252.1 亿美元，较 2019 年同比增长 6.0%；2020-2024 年，IDC 预计年均复合增长率达到 8.1%。IDC 预测，2020 年中国网络安全市场因受到疫情影响总体支出将达到 78.9 亿美元，较 2019 年同比增长 11.0%，与之前预期的 20%以上的增长下滑较大，但依然高于全球平均水平。2021 年开始，IDC 预期行业将恢复到 20%以上的增长，预计 2024 年将达到 167.2 亿美元。我国信息安全建设依然不足，服务和软件的结构上也与全球有较大差距，因此整体行业在政策的不断推动下，总体增长速度较快。

2、数字经济蓬勃发展，安全可信的数据交易成为行业新需求

数字经济蓬勃发展，已成为国民经济中最为核心的增长极之一，我国数字经济增加值规模从 2005 年的 2.6 万亿元扩张到 2019 年的 35.8 万亿元，数字经济占

GDP 比重由 14.2%提升至 36.2%，在国民经济中的地位逐步凸显。党的十八大以来，发展数字经济逐渐上升为国家战略，相关政策文件的出台优化了政策环境。根据中央《关于构建更加完善的要素市场化配置体制机制的意见》，数据资产被明确列入市场生产要素，要求“加快培育数据要素市场”，做到“推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护”。加强信息安全和对个人数据收集的保护已成为国家战略重点。数据价值化进程的加速和数字经济开放合作的深化，对保护数据资源安全提出挑战，新一代数据安全产品需求日益旺盛。

与此相对的，各机构和企业积累的数据信息由于缺乏信息共享平台，形成大量的数据信息孤岛，各方信息不对称，导致数据无法最大化发挥价值。此外，各经济主体在获取数据时，电子数据极易被篡改，篡改行为通过技术手段隐藏，数据真实性无法得到保障。市场对于信息可信环境下共享的需求无法得到有效满足。

3、传统犯罪加速向以互联网为媒介的非接触式犯罪转移，专业涉网犯罪侦查打击支撑工具及技术的需求迫切

我国信息社会快速发展、互联网快速普及使犯罪结构发生了深刻变化，传统接触式犯罪加速向以互联网为媒介的非接触式犯罪转移，目前，我国涉网犯罪呈现出案件持续高发多发、网络诈骗迅猛增长、诈骗窝点快速转移、作案群体逐步泛化、黑灰产业日益泛滥等特点，网络违法犯罪情况错综复杂，侦破难度大大提升。涉网犯罪的日益严峻催生了公安机关采购新型涉网犯罪侦查打击服务的需求。

经过多年的公安信息化建设，我国各级政府及公安部门购买了大量安全软硬硬件产品进行本地化部署。在科技快速发展的时代背景下，安全产品迭代更新加快，导致公安部门安全建设存在投入较大、安全产品重复购买等问题，也对公安网警业务培训提出了更高要求。考虑到该类安全产品本地化部署问题，公安机关采购需求呈现向服务化转变趋势。云计算产业的快速发展，虚拟化及云服务理念的渗透持续加深，也进一步吸引公安机关放弃传统的软硬件产品购置，进行服务采购。未来公安客户将倾向于集中采购安全运营服务，实现一网统办、一网统管，主动、强力、持续的综合性涉网犯罪侦查打击技术服务将成为新需求。

4、国产化替代加速推进，我国信创产业进入快速发展时期

信息技术应用创新产业是国家构建安全可控的自有 IT 产业的重要基础，已经成为经济数字化转型、提升产业链发展的关键。为了解决本质安全问题，大力发展信创产业已上升为一项国家战略。2016 年 4 月 19 日，网信工作座谈会明确提出，“核心技术受制于人是我们最大的隐患”，同年，国家再次强调“抓紧突破网络发展的前沿技术和具有国际竞争力的关键核心技术”。在中美关系动荡之际，信创产业受到了各界的广泛关注，建设安全可控的信息技术体系成为“新基建”和“数字中国”战略的重要内容。2020 年 12 月 16 日至 18 日，中央经济工作会议明确将强化国家战略科技力量和增加产业链供应链自主可控能力列入 2021 年经济工作八大任务。国产化的 IT 底层架构不断完善使得信息技术体系的国产化替代加速推进，我国信创产业进入快速发展时期。

信创产业主要包括新一代信息技术下的云计算、软件（操作系统、中间件、数据库、各类应用软件）、硬件（芯片、GPU/CPU、主机、各类终端）、安全（网络安全）等领域，涵盖了 IT 底层基础软硬件到上层应用软件的全产业链。随着云计算、大数据、物联网等新技术的发展应用，网络安全应用场景更加复杂，网络攻击组织性与目的性不断加强，社会危害性不断加大。网络安全建设作为信创产业的重要组成部分，自主创新需求更加迫切。

5、网络安全市场快速发展，专业人才缺口扩大，专业教育市场需求旺盛

近几年，随着《网络安全法》的出台，各级政府和企业在网络安全建设方面的投入不断加大。我国网络安全人才需求迅速攀升，截至 2019 年 9 月，我国网络空间安全人才数量缺口高达 70 万，预计到 2020 年将超过 140 万。公司近年业务规模快速增长，网络安全人才需求大幅提升，在不断提高招聘力度的情况下，校招人才缺口仍达 200-300 人。

2016 年 12 月，国家互联网信息办公室印发《国家网络空间安全战略》，提出实施网络安全人才工程，加强网络安全学科专业建设，打造一流网络安全学院和创新园区，形成有利于人才培养和创新创业的生态环境；2020 年 7 月，全国人大常委会印发《数据安全法（草案）》，再次指出要采取多种方式培养数据开发利用技术和数据安全专业人才。各地政府鼓励网络安全相关学科建设，启动区域

网络安全实训基地建设，加强网络安全人才培养成为增强国家网络安全实力的重点，网络安全教育市场空间广阔。

网络安全靶场能够为网络安全人员提供贴近实际生产环境的学习、训练和演练平台，服务于网络安全人才的实战能力养成环节，为网络安全人员的岗位胜任能力培育提供环境和业务形态支撑，随着市场对网络安全人才数量和质量两个维度需求的不断提升，未来网络安全靶场需求也将随之提升。

6、随着新兴技术发展，网关技术进入更新迭代的关键窗口期

随着人工智能、区块链、5G、量子通信、工业互联网、大数据、云计算、物联网等具有颠覆性的战略性新技术快速演进，大规模数据泄露、高危漏洞、新技术应用下的网络攻击等网络安全问题频发，攻击团伙的智能化、商业化生态已形成，网络威胁态势严峻。在云计算、大数据、物联网、工业互联网及 AI 智能防护等新兴技术领域需求的推动下，防火墙作为传统的网关产品处在向智能化、简易化及可视化方向技术更新迭代的关键阶段，现有产品技术架构受到挑战，市场需要能够满足云计算、大数据、物联网、工业互联网及 AI 智能防护等新兴技术领域安全防护需求的新一代网关产品，行业竞争格局或将面临较大变动，网关技术进入更新迭代的关键窗口期。

7、政策与技术不断完善，车联网及车联网安全发展前景明确

机动车保有量不断上升，导致行车安全和交通拥堵问题日益凸显，而根据美国高速公路安全管理局（NHTSA）提供的统计数据，引入车联网能有效改善现状，中轻型车辆可避免 80%的交通事故，重型车可避免 71%的交通事故，交通拥堵时间可减少 60%，现有道路通行能力提高 2-3 倍。

介于车联网技术优势，国家政策不断鼓励智能网联汽车发展，2019 年 9 月国务院发布《交通强国建设纲要》，明确提出加强智能网联汽车研发，车联网用户渗透率达到 30%以上，联网车载信息服务终端的新车装配率达到 60%以上。在技术方面，5G 与 V2X 技术也加速车联网加速落地。随着 V2X 技术路径的明确，在国家政策和 5G 商用的推动下，基于车联网在驾驶安全性和交通治理方面的突出优势，车联网发展前景进一步明确，目前我国已将车联网产业上升到国家战略高度，我国车联网产业化进程将逐步加快，根据前瞻产业研究院发布的《中

国车联网行业市场前瞻与投资战略规划分析报告》统计数据，截至 2017 年，全球车联网市场规模约为 525 亿美元，预计到 2022 年将增加至 1,629 亿美元，复合年均增长率为 25.4%；我国车联网市场规模将从 2017 年的 114 亿美元增长到 2022 年的 530 亿美元，复合年均增长率为 36.0%。随着政策推动与技术发展，车联网行业发展前景明确。

（二）本次发行的目的

1、满足数据安全可信交易的需求，拓展新的市场空间

随着数字经济的发展，网络信息安全作为数字经济发展的必要保障，其投入持续增加，且与全球安全产业结构发展趋势保持一致，我国网络信息安全市场将由软硬件产品逐步向综合安全平台和服务转移。根据赛迪顾问的预测，2019-2021 年度，网络信息安全市场规模的复合增长率为 23.45%，大数据安全市场规模的复合增长率为 35.26%，大数据安全市场规模增速高于网络信息安全行业整体水平，具有较好的市场发展前景。公司于 2015 年起便陆续开发了针对大数据安全的网络安全态势感知预警平台、AiLPHA 大数据智能安全平台等产品，作为首批切入大数据安全领域的企业，获得了较高的市场占有率，充分享有大数据安全市场规模增长所带来的红利，2017-2019 年度公司网络信息安全平台中大数据安全产品相关收入年复合增长率达到 100.22%。

通过本次数据安全岛平台研发及产业化项目的实施，公司能够更充分利用自身在大数据安全领域的技术积累，解决大量的数据信息孤岛、信息不对称问题，把握数字经济快速发展带动的数据交易平台及其有关技术服务需求增长，实现对公司网络信息安全平台产品系列的拓展与补充，进一步提升公司网络信息安全平台业务，进而提高公司整体盈利能力。

2、顺应公安客户对涉网犯罪打击工具的新需求，促进客户涉网犯罪打击能力提升

本次发行募集资金用于研发落地涉网犯罪侦查打击服务平台，平台基于浦东公安实际业务场景，利用大数据技术，开展犯罪行为监测预警、犯罪线索智能落地、辅助案件研判、犯罪业态感知、本地产业评价等业务，顺应客户对于 SaaS 化涉网犯罪打击工具的新需求，增加客户粘性提升公司盈利能力，同时促进客户

涉网犯罪打击能力的迅速提升，有利于提高我国网络安全综合治理能力和水平，推进构建安全清朗、和谐稳定的网络空间。

3、顺应国产化替代趋势，把握信创领域网络安全市场发展机遇

随着国产 CPU、操作系统等基础层产品不断完善，安全自主可控的信息化建设进程的推进，下游客户对信创网络安全产品和服务需求强烈，行业市场空间广阔。信创产业的不断发展下，国产化替代已从电信运营商、政府、金融等关键敏感行业逐步向全行业展开。

面对国产化替代明确的发展趋势，公司拟依托在网络安全领域的产品技术和人才基础，依据国家战略要求，对基础网络安全产品、云安全管控平台、态势感知平台和安全运营平台等进行国产化适配。基于国产化平台，全面开展信创领域的安全咨询、安全集成、安全运营等工作，加强对运维访问控制审计技术、分布式漏洞发现与验证技术、基于云架构的安全扫描与监测技术、SaaS 化云安全防护等技术的研发力度。本次信创产品研发及产业化项目是公司顺应国产替代安全可控大趋势，满足软件技术可控集采要求的必然选择，是公司保持并提升主要下游市场竞争力的重要战略。

4、提高网络安全教育培训能力，抢占市场份额

本次网络安全云靶场及教育产业化项目基于网络安全行业人才紧缺的现状，以及当前学历教育与职业技能水平不匹配的问题，搭建网络安全靶场，为网络安全人才培养提供了环境、专业工具和业务形态支撑，有助于解决高层次专业教师缺乏，教材良莠不齐，缺乏攻防演练平台，综合性、自主防御性试验难以构建和学生缺少实战等问题。通过网络安全靶场平台产品研发，加强现有网络安全产品向适用于教育教学产品的转化研发，为我国网络安全教学内容建设和网络安全人才培养提供实战化培训工具，有利于丰富我国网络安全人才培养模式，提高网络安全人才培养能力和水平，进而满足日益增长的网络安全人才需求。

同时该项目的建设实施有助于扩展公司网络安全教学类产品市场空间，实现以实战为导向的网络安全培训服务，对网络安全人才培养产品和服务进行一体化升级，从横向上扩展公司业务线。另一方面，公司为学校、大型企业和政府建设网络安全靶场提供相应的产品，有助于加强潜在用户对公司产品的认知，推广相

关网络安全产品，推进公司生态建设。项目将更好地满足国家培育行业人才战略的需要，同时拓展新的产品业务领域，在推动公司业绩增长的同时，进一步提升行业整体竞争力。

5、抓住网关行业技术迭代机遇，扩大公司相关产品市场规模

伴随国家网络强国战略和企业数字化转型的推进，云计算、大数据、人工智能等新兴技术的加速发展使得网络安全产品的应用环境日益复杂，迫使新一代网络安全产品综合协作能力快速提升，新一代网关产品进入技术更新迭代的关键窗口期，推动传统网关产品技术淘汰。目前，公司业务主要集中在应用层安全领域，基础层安全产品市场份额较小。本次新一代智能网关产品研发及产业化旨在把握行业技术迭代窗口期，对新一代智能网关产品进行研发升级，完善公司网关产品核心技术，适应新的应用环境和技术方向，提升公司在云计算、大数据、物联网、工业互联网及人工智能等新兴技术领域综合安全解决方案的完整性和适配性，抓住机遇抢占市场份额，进一步扩大公司产品业务规模，提升整体竞争力。

6、把握车联网明确的发展前景，拓展产品市场空间

公司拟通过身份认证体系、车辆安全检测、靶场虚拟化技术、威胁情报获取和车载微流量技术的研发，凭借公司在网络信息安全领域成熟的产品技术将传统安全产品技术向车联网场景研发转化，形成完善的车联网安全产品体系，满足车联网网络安全需求，推动车联网产业链的建设完善。通过开展车联网安全关键技术研发和储备，为公司未来拓展车联网安全业务提前进行产品技术布局，抓住车联网明确的发展前景以拓展网络安全产品的市场空间。

7、增强资金实力，为公司战略布局提供充分保障

通过本次向特定对象发行 A 股股票募集资金，将进一步增强公司资金实力，优化资产负债结构，提高公司抗风险能力。同时，本次向特定对象发行股票募集资金均用于公司的主营业务，募投项目与现有业务关联度高，是加强公司对前沿技术的研发、支撑行业应用的持续升级、深化公司在网络安全行业相关领域业务布局的重要举措。待本次募集资金投资投产后，公司将实现业务板块的延伸和扩展，随着募投项目的实施及效益的产生，公司的盈利能力和经营业绩将进一步提升。

二、本次向特定对象发行股票方案概要

（一）本次发行股票的种类和面值

本次发行股票的种类为境内上市人民币普通股（A 股），每股面值人民币 1.00 元。

（二）发行对象及与发行人的关系

本次发行对象为不超过 35 名符合中国证监会规定条件的证券投资基金管理公司、证券公司、信托投资公司、财务公司、保险机构投资者、合格境外机构投资者（QFII）、其它境内法人投资者和自然人等特定投资者。证券投资基金管理公司、证券公司、合格境外机构投资者、人民币合格境外机构投资者以其管理的二只以上产品认购的，视为一个发行对象；信托投资公司作为发行对象的，只能以自有资金认购。

最终发行对象将在本次发行经上海证券交易所审核通过并经中国证监会同意注册后，由公司董事会根据询价结果，与保荐机构（主承销商）协商确定。若发行时法律、法规或规范性文件对发行对象另有规定的，从其规定。

本次发行尚未确定发行对象，因而无法确定发行对象与公司的关系，最终本次发行是否存在因关联方认购本次发行的 A 股股票而构成关联交易的情形，将在发行结束后公告的《发行情况报告书》中予以披露。

所有发行对象均以人民币现金方式并以同一价格认购公司本次发行的股票。

（三）发行证券的价格或定价方式、发行数量、限售期；

1、发行价格和定价原则

本次发行采取询价发行方式，定价基准日为公司本次向特定对象发行股票的发行期首日，发行价格不低于定价基准日前 20 个交易日公司股票交易均价的 80%（定价基准日前 20 个交易日公司股票交易均价=定价基准日前 20 个交易日公司股票交易总额/定价基准日前 20 个交易日公司股票交易总量），并按照“进一法”保留两位小数。

最终发行价格将在公司取得中国证监会对本次发行予以注册的决定后，由股东大会授权公司董事会或董事会授权人士和保荐机构（主承销商）按照相关法律

法规的规定和监管部门的要求，遵照价格优先等原则，根据发行对象申购报价情况协商确定。

若公司股票在本次发行的定价基准日至发行日期间发生派发股利、送红股、公积金转增股本等除权除息事项，本次发行底价将作相应调整。调整方式如下：

派发现金股利：P1=P0-D

送红股或转增股本：P1=P0/（1+N）

派发现金同时送红股或转增股本：P1=（P0-D）/（1+N）

其中，P0 为调整前发行底价，D 为每股派发现金股利，N 为每股送红股或转增股本数量，调整后发行底价为 P1。

2、发行数量

本次向特定对象发行股票的股票数量不超过 22,222,222 股，本次发行的股票数量按照本次发行募集资金总额除以发行价格计算，不超过本次发行前公司总股本的 30%。最终发行数量由公司股东大会授权董事会根据中国证监会相关规定及发行时的实际情况，与本次发行的保荐机构（主承销商）协商确定。

若本公司股票在董事会决议日至发行日期间发生送股、资本公积金转增股本、新增或回购注销限制性股票等导致股本总额发生变动的，本次向特定对象发行股票的数量将进行相应调整。

若本次向特定对象发行的股份总数因监管政策变化或根据发行注册文件的要求予以变化或调减的，则本次向特定对象发行的股份总数及募集资金总额届时将相应变化或调减。

3、限售期

本次发行完成后，发行对象认购的股份自发行结束之日起六个月内不得转让。法律法规、规范性文件对限售期另有规定的，依其规定。

本次向特定对象发行股票结束后，由于公司送红股、资本公积金转增股本等原因增加的公司股份，亦应遵守上述限售期安排。

本次发行的发行对象因本次发行取得的公司股份在锁定期届满后减持还需

遵守《公司法》《证券法》《上市规则》等法律法规、规章、规范性文件、交易所相关规则以及公司《公司章程》的相关规定。

（四）募集资金投向

本次向特定对象发行股票募集资金总额不超过 133,332.17 万元，扣除发行费用后，募集资金净额拟投入以下项目：

单位：万元

	项目名称	总投资	募集资金拟使用额
1	数据安全岛平台研发及产业化项目	47,633.85	40,046.62
2	涉网犯罪侦查打击服务平台研发及产业化项目	13,006.66	10,216.18
3	信创产品研发及产业化项目	62,122.22	45,870.82
4	网络安全云靶场及教育产业化项目	15,753.23	12,541.34
5	新一代智能网关产品研发及产业化项目	22,622.09	17,924.13
6	车联网安全研发中心建设项目	10,235.45	6,733.08
	合计	**171,373.50**	**133,332.17**

在上述募集资金投资项目的范围内，公司可根据项目的进度、资金需求等实际情况，对相应募集资金投资项目的投入顺序和具体金额进行适当调整。募集资金到位前，公司可以根据募集资金投资项目的实际情况，以自筹资金先行投入，并在募集资金到位后予以置换。募集资金到位后，若扣除发行费用后的实际募集资金净额少于拟投入募集资金总额，不足部分由公司以自筹资金解决。

（五）本次发行是否构成关联交易

截至本募集说明书出具日，本次发行尚未确定发行对象，最终是否存在因关联方认购公司本次向特定对象发行股票构成关联交易的情形，将在发行结束后公告的发行情况报告书中予以披露。

（六）本次发行是否导致公司控制权发生变化

本次发行前，公司的控股股东、实际控制人为范渊，截至 2020 年 9 月 30 日，其直接持有公司 10,018,362 股股份，占公司总股本的 13.52%，并通过和员工持股平台嘉兴安恒、宁波安恒的《一致行动协议》，合计控制安恒信息 27.02%的表决权。

本次向特定对象拟发行不超过本次发行前公司总股本的 30%，即不超过

22,222,222 股（含本数），本次发行完成后公司的总股本不超过 96,296,297 股（含本数）。按发行 22,222,222 股上限测算，本次发行完成后，控股股东及实际控制人范渊可实际控制的表决权约占公司总股本的 20.79%，仍保持实际控制人的地位。本次发行不会导致公司控股股东和实际控制人发生变更。

（七）本次发行方案取得有关主管部门批准的情况以及尚需呈报批准的程序

本次向特定对象发行的方案及相关事项已经于 2020 年 12 月 25 日召开的公司第一届董事会第二十三次会议、于 2021 年 1 月 11 日召开的公司 2021 年第一次临时股东大会审议通过，尚需履行以下呈报批准程序：

1、本次向特定对象发行股票尚需取得上海证券交易所审议通过；

2、本次向特定对象发行股票尚需获得中国证监会注册同意。

第三节　董事会关于本次募集资金使用的可行性分析

一、本次募集资金使用计划

本次向特定对象发行股票募集资金总额不超过 133,332.17 万元，扣除发行费用后，募集资金净额拟投入以下项目：

单位：万元

	项目名称	总投资	募集资金拟使用额
1	数据安全岛平台研发及产业化项目	47,633.85	40,046.62
2	涉网犯罪侦查打击服务平台研发及产业化项目	13,006.66	10,216.18
3	信创产品研发及产业化项目	62,122.22	45,870.82
4	网络安全云靶场及教育产业化项目	15,753.23	12,541.34
5	新一代智能网关产品研发及产业化项目	22,622.09	17,924.13
6	车联网安全研发中心建设项目	10,235.45	6,733.08
	合计	**171,373.50**	**133,332.17**

在上述募集资金投资项目的范围内，公司可根据项目的进度、资金需求等实际情况，对相应募集资金投资项目的投入顺序和具体金额进行适当调整。募集资金到位前，公司可以根据募集资金投资项目的实际情况，以自筹资金先行投入，并在募集资金到位后予以置换。募集资金到位后，若扣除发行费用后的实际募集资金净额少于拟投入募集资金总额，不足部分由公司以自筹资金解决。

（一）募集资金以外所需剩余资金的具体来源

本次募投项目公司拟自筹资金 38,041.33 万元用于项目建设及运营，该部分资金主要来源于公司现有资金盈余、公司未来经营活动经营现金流入以及募投项目所产生的经营活动现金流入。

截至 2020 年 9 月 30 日，公司货币资金余额及交易性金融资产余额合计为 112,427.70 万元，扣除公司首次公开发行尚未使用完毕的募集资金金额 82,771.35 万元以及受限货币资金 579.10 万元后，公司账面可使用资金共计 29,077.25 万元，可较大程度的满足本次募投项目对自有资金的需求。

同时，2017-2019 年度，公司经营活动产生的现金流量净额分别为 6,886.94 万元、9,598.26 万元以及 21,651.61 万元，经营活动资金流入情况良好，能够及时满足本次募投项目实施过程中的自有资金需求。

此外，本次募投项目自筹资金的 38,041.33 万元将在三年内分批投入，且主要用于募投项目日常费用类支出，不会在某一年度集中投入对公司资金造成较大压力。而且本次募投项目预计经营效益良好，自建设期第一年起将陆续产生经营活动现金流入，能够承担部分募投项目所需资金。

综上所述，公司可通过运用现有资金盈余、未来经营活动经营现金流入以及本次募投项目所产生的经营活动现金流入，满足本次募投项目除募集资金以外的资金需求。

（二）如募集资金不能全额募足或发行失败，项目实施是否存在较大的不确定性

截至 2020 年 9 月末，公司货币资金余额为 100,406.53 万元，应收账款及应收票据余额为 24,002.79 万元，若出现募集资金不能全额募足或发行失败的情况，公司可结合整体生产经营情况，调配自有资金及收回的应收款项用于项目建设。

2019 年公司营业收入为 94,403.29 万元，归属于母公司股东的净利润和扣除非经常性损益后归属于母公司股东的净利润分别为 9,222.04 万元和 7,959.44 万元。公司在 2020 年前三季度实现营业收入 66,020.92 万元，比上年同期增长 40.11%。总体而言，公司经营情况良好，可利用未来期间的经营积累弥补部分募投项目资金缺口。

此外，截至 2020 年 9 月末，公司合并报表资产负债率 25.86%，不存在短期借款，长期借款 9,600.00 万元，整体债务水平较低。公司具有良好的银行信用，银行融资渠道通畅，资信状况良好，具有一定的债务融资能力。若本次发行不能全额募足或发行失败，公司亦可采用债务融资弥补部分募投项目资金缺口。

综上，如募集资金不能全额募足或发行失败，募投项目的实施将面临一定的资金压力，但鉴于本次募投项目对公司的重大战略意义并具有良好的经济效益，公司将全力推进募投项目的实施，根据届时的实际经营和市场情况，综合考虑通过自有资金、经营积累及债务融资等方式筹措所需资金，全力确保募投项目持续推进，实现预期的经营效益，项目实施不会因为募集资金不能全额募足或发行失败而存在较大的不确定性。。

二、本次募集资金投资项目基本情况

（一）数据安全岛平台研发及产业化项目

1、项目基本情况

本项目拟以公司间接全资控股子公司上海安恒互联安全科技有限公司为实施主体，在上海临港新片区购置土地，依托上海临港区位优势，建设数据安全研发基地，重点开展数据交易安全平台即安全岛平台的研发及产业化，改善当前数据交易困境。数据安全岛通过数据全链路加密、操作留痕、各主体数据隔离、密文计算、异常情况动态分析等技术手段，规避数据泄露、篡改等风险，同时还可以提供数据自动脱敏服务提高数据流转效率。

2、项目经营前景

（1）我国数字经济蓬勃发展，数据安全产品需求日益旺盛

数字经济蓬勃发展，已成为国民经济中最为核心的增长极之一，我国数字经济增加值规模从 2005 年的 2.6 万亿元扩张到 2019 年的 35.8 万亿元，数字经济占 GDP 比重由 14.2%提升至 36.2%，在国民经济中的地位逐步凸显。党的十八大以来，发展数字经济逐渐上升为国家战略，相关政策文件的出台优化了政策环境，2020 年初政府加速布局“新基建”为数字经济发展提供了新动能。数据价值化进程的加速和数字经济开放合作的深化，对保护数据资源安全提出挑战，新一代数据安全产品需求日益旺盛。

与此相对的，各机构和企业积累的数据信息由于缺乏信息共享平台，形成大量的数据信息孤岛，各方信息不对称，导致数据无法最大化发挥价值。此外，各经济主体在获取数据时，电子数据极易被窃取，窃取行为通过技术手段隐藏，数据流动过程中安全性无法得到保障。

为抓住时代发展机遇，公司拟基于在数据安全领域的技术积累开发数据安全岛平台解决方案，为数据交易和共享平台提供技术支持服务。本项目实施将为数字经济发展提供安全可靠的数据交易平台，可供多方数据联合计算，有利于打破数据孤岛，实现数据流通，创造数据价值。公司针对政府和企业客户日益强烈的数据交易和共享需求设计的数据安全岛平台能够为我国数字经济发展提供所需的安全保障。

（2）本项目能够满足客户数据安全合规及降低数据泄露风险需求，拓展新的市场空间

近年来大数据行业在蓬勃发展的同时也滋生了大量数据黑灰产，非法收集、使用数据给数据拥有方造成了高昂的经济损失。根据 IBM 发布的《2020 年数据泄露成本报告》[1]，2019 年 8 月至 2020 年 4 月期间全球范围内发生了 524 起大型数据泄露违规事件，涉及 17 个地区和 17 个行业的各种规模的组织，平均每件数据泄露事件会造成 386 万美元的经济损失，受害者组织发现和控制数据泄露平均需要 280 天。根据报告，客户个人身份信息（PII）记录每条丢失或被盗的平均成本为 150 美元，知识产权记录平均每条丢失成本为 147 美元，员工信息丢失成本为 141 美元，全球范围内 80%的数据泄露都导致了丢失成本最为高昂的客户 PII 丢失。

加强信息安全，保护个人数据隐私不仅是各类组织经济层面的需求，更是企业满足合规性产生的法律层面的需求。数据安全领域立法已经进入了快车道，2018 年 8 月十三届全国人大常委会将《数据安全法》、《个人信息保护法》纳入一类立法计划，2020 年 7 月《数据安全法（草案）》公布，提出国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。同时，《草案》明确了数据安全制度和保护义务，列明任何组织、个人收集数据，必须采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。在数字经济发展带动数据流动需求快速增长和个人信息保护法律法规等政策环境逐步完善的背景下，对数据交易平台及平台的安全可信技术保障能力提出要求。

为了推动在合法合规条件下个人信息数据的收集和使用，各地政府等相关客户对数据安全交易和共享平台的建设需求快速涌现，公司拟充分利用区块链的去中心化、溯源、防篡改等特性，结合数据主动销毁、数据操纵行为监控、账户风险动态感知等技术，实现一个跨机构、跨地域的，集数据订阅、交换、联合计算等功能的可信平台，同时赋予平台脱敏等功能，实现交易自动化降低人力成本，

[1]《2020 年数据泄露成本报告》
https://securityaffairs.co/wordpress/106710/reports/2020-cost-of-a-data-breach-report.html

发挥数据的最大价值，实现数据交易过程中的数据安全和个人信息保护，顺应客户新需求，拓展新的市场空间。

（3）本项目是公司把握新的市场机遇，进一步提升网络信息安全平台业务的重要举措

随着数字经济的发展，网络信息安全作为数字经济发展的必要保障，其投入持续增加，且与全球安全产业结构发展趋势保持一致，我国网络信息安全市场将由软硬件产品逐步向综合安全平台和服务转移。根据赛迪顾问的预测，2019-2021 年度，网络信息安全市场规模的复合增长率为 23.45%，大数据安全市场规模的复合增长率为 35.26%，大数据安全市场规模增速高于网络信息安全行业整体水平，具有较好的市场发展前景。公司于 2015 年起便陆续开发了针对大数据安全的网络安全态势感知预警平台、AiLPHA 大数据智能安全平台等产品，作为首批切入大数据安全领域的企业，获得了较高的市场占有率，充分享有大数据安全市场规模增长所带来的红利，2017-2019 年度公司网络信息安全平台中大数据安全产品相关收入年复合增长率达到 100.22%。

通过本项目的实施，公司能够更充分利用自身在大数据安全领域的技术积累，把握数字经济快速发展带动的数据交易平台及其有关技术服务需求增长，研发数据安全岛平台，实现对公司网络信息安全平台产品系列的拓展与补充，进一步提升公司网络信息安全平台业务，提升公司整体盈利能力。

（4）打造临港数据交流安全可信平台有助于树立数据交易平台的建设标杆，助推公司产品市场拓展

2019 年 8 月，国务院印发《中国（上海）自由贸易试验区临港新片区总体方案》，提出实施国际互联网数据跨境安全有序流动，包括构建安全便利的国际互联网数据专用通道，支持新片区聚焦集成电路、人工智能、生物医药、总部经济等关键领域，试点开展数据跨境流动的安全评估，建立数据保护能力认证、数据流通备份审查、跨境数据流通和交易风险评估等数据安全管理机制。

基于临港数据流动和交易平台建设需求，本项目拟在上海临港新片区购置土地，重点开展数据安全岛平台研发，为政府等相关部门搭建可服务于国内外数据交流的安全可信平台提供完整的安全可信保障产品技术方案。本项目有助于树立

行业内数据交易平台的建设标杆，迅速建立公司产品在该领域的知名度和市场地位，确立竞争优势，保障未来业绩实现。

3、项目与现有业务或发展战略的关系

本项目拟建设以数据安全岛业务为核心的数据流通安全中心，数据安全岛是公司针对企业数字化转型推进过程中数据共享与交易的安全保障需求，依托公司在网络安全领域的产品技术和人才基础，为政府、金融、运营商等数据服务客户提供的数据交易安全保障平台产品。本项目是公司立足网络安全业务基础，针对数据安全标准提升和客户实际业务需求进行的新产品开发，能够进一步拓展公司业务边界，推进整体业绩增长。

4、项目实施准备和进展情况

本项目计划总投资额为 47,633.85 万元。其中，拟投入募集资金 40,046.62 万元，其余以自筹资金投入，项目具体投资内容如下：

单位：万元

序号	项目名称	投资总额	募集资金金额
1	**工程建设费用**	**33,583.35**	**33,583.35**
1.1	土地款	2,860.40	2,860.40
1.2	场地建造费	26,742.75	26,742.75
1.3	硬件购置	2,815.60	2,815.60
1.4	软件购置	1,164.60	1,164.60
2	**研发费用**	**10,353.75**	**6,463.27**
3	**基本预备费 2%**	**878.74**	**-**
4	**铺底流动资金**	**2,818.01**	**-**
	合计	**47,633.85**	**40,046.62**

本项目实施主体为公司间接全资控股子公司上海安恒互联安全科技有限公司。2021 年 1 月，公司已就本项目建设所需用地与中国（上海）自由贸易区临港新片区管理委员会签署《上海市国有建设用地使用权出让合同（研发总部产业项目类）》，约定中国（上海）自由贸易区临港新片区管理委员会将东至 NS1 路，西至 K03-01 地块边界，南至环湖南二路，北至云鹃路的地块转让给公司，宗地编号为 202000510826470864，宗地总面积 9067.90 平方米。

本项目已经完成项目备案，并取得了上海临港地区开发建设管理委员会出具

的《上海市企业投资项目备案证明》（国家代码：2021-310115-04-04-565489）。

根据《中华人民共和国环境影响评价法》、《建设项目环境保护管理条例》、《建设项目环境影响评价分类管理名录（2021 年版）》，公司本次发行所募集资金投资项目未列入《建设项目环境影响评价分类管理名录（2021 年版）》，属于不纳入建设项目环境影响评价管理的项目，无需办理环评报批手续，符合有关环境保护的要求。

5、预计实施时间及整体进度安排

本项目由公司间接全资控股子公司上海安恒互联安全科技有限公司实施，预计总投资额 47,633.85 万元，拟投入募集资金 40,046.62 万元，建设期 3 年。公司计划于第一年完成项目方案设计与评审，购置土地，开始场地建造，并于当年完成数据安全岛初始版本产品平台的研发，对特定客户小规模提供数据安全岛初代产品。第二至第三年开展数据安全岛平台针对不同需求的适配工作以及功能的迭代升级，于第三年年底前完成场地建造验收和成熟可量产数据安全岛平台的研发，项目建设完成。

6、发行人的实施能力

数据安全岛平台是对多种网络安全前沿技术的集成与融合，涉及数据隔离、可信环境执行、安全计算沙箱、用户实体行为分析以及多方数据联合建模等技术。公司自设立以来始终坚持持续技术创新的发展战略，重视研发投入，过去三年研发费用占营业收入比例均超过 20%，截至 2020 年 9 月 30 日，公司共拥有 48 项核心技术，研发人员数量达 869 人，涉及攻防研究、应急响应、安全咨询、漏洞研究、产品研发等各个领域。公司已完成本项目产品核心安全计算沙箱技术和多方数据联合建模技术应用框架研究，进入技术应用测试和优化开发阶段。目前已有一项相关专利获得授权，另有多项技术发明专利进入申请受理状态与实审状态。良好的研发创新能力、完善的技术体系和强大的人才团队为本项目的顺利实施提供了技术保障。

公司与临港新片区的合作也为本项目提供了一定的市场基础，临港新片区作为高开放程度的自由贸易园区，有大量存在数据交换需求的企业。截至本募集报告书出具日，公司已与临港新片区就数据安全岛平台达成合作意向，拟共

同开展上海临港跨境数据流通课题研究项目。此外，公司还与多地区大数据局、三甲医院等数字资源较为丰富的单位达成初步合作意向，市场前景良好。

7、资金缺口的解决方式

本次发行募集资金到账前，公司将根据募集资金投资项目的实际情况，以自筹资金先行投入，并在募集资金到位后予以置换。募集资金到位后，若扣除发行费用后的实际募集资金净额少于拟投入募集资金总额，不足部分由公司以自筹资金解决。

8、项目经济效益评价

经测算，本项目税后内部收益率为 22.00%，税后静态投资回收期为 7.03 年，项目预期效益良好。

（二）涉网犯罪侦查打击服务平台研发及产业化项目

1、项目基本情况

本项目拟以公司全资子公司上海安恒智慧城市安全技术有限公司为实施主体，在上海浦东新区租赁办公场地，研发落地涉网犯罪侦查打击服务平台，开展定制化侦查破案及案件线索检索平台等业务。平台利用大数据技术，开展犯罪行为监测预警、犯罪线索智能落地、辅助案件研判、犯罪业态感知、本地产业评价等业务，为公安客户提供涉网犯罪情报发现和线索分析等远程 SaaS 化服务，协助公安客户提高涉网犯罪侦查打击能力。

2、项目经营前景

（1）传统犯罪加速向以互联网为媒介的非接触式犯罪转移，专业涉网犯罪侦查打击支撑工具及技术的需求迫切

我国信息社会的快速发展、互联网的快速普及使犯罪结构发生了深刻变化，传统接触式犯罪加速向以互联网为媒介的非接触式犯罪转移，传统犯罪的组织方式、外在表现形式发生了持续动态的变化。目前，我国涉网犯罪呈现出案件持续高发多发、网络诈骗迅猛增长、诈骗窝点快速转移、作案群体逐步泛化、黑灰产业日益泛滥等特点，网络违法犯罪情况错综复杂，侦破难度大大提升。

涉网犯罪的日益严峻催生了公安机关采购新型涉网犯罪侦查打击服务的需

求。涉网犯罪侦查打击服务平台基于浦东公安实际业务场景，利用大数据技术，开展犯罪行为监测预警、犯罪线索智能落地、辅助案件研判、犯罪业态感知、本地产业评价等业务，能够促进涉网犯罪打击能力的迅速提升，有利于提高我国网络安全综合治理能力和水平，推进构建安全清朗、和谐稳定的网络空间。

（2）本项目是公司顺应客户采购模式变更的重要举措

经过多年的公安信息化建设，我国各级政府及公安部门购买了大量安全软硬硬件产品进行本地化部署。在科技快速发展的时代背景下，安全产品迭代更新加快，公安部门存在安全建设投入较大、安全产品重复购买等问题，也对公安网警业务培训提出了更高要求。考虑到该等安全产品本地化部署问题，公安机关采购需求呈现向服务化转变趋势。SaaS 服务采用后台自动升级的方式进行技术迭代，避免了重复购买的问题，同时，SaaS 平台受众多，软件升级成本由全国范围内所有需求者共同承担，可以大幅度减轻地方财政负担。云计算产业的快速发展带动虚拟化及云服务理念的持续渗透，也进一步吸引公安机关放弃传统的软硬件产品购置，进行服务采购。未来公安客户将倾向于集中采购安全运营服务，实现一网统办、一网统管，主动、强力、持续的综合性涉网犯罪侦查打击技术服务将成为新需求。

公安部门是公司最主要客户群体之一，2017-2019 年度，来自公安部门的收入占公司主营业务收入的比重均超过 10%。本项目拟采用云计算方式实现技术服务交付模式的转型，相比产品销售或定制化研发项目模式，服务模式更符合客户采购方式的变化，能够提升公司市场竞争力。同时，本项目有利于推动涉网犯罪侦查打击技术的更新迭代，为基层警力提供技术赋能，将办案模式由传统的被动式侦破升级为主动打击，进一步绑定公安客户、提升客户粘性。

（3）本项目为公司未来市场拓展提供重要基础

本项目拟落地的上海浦东新区具备良好的网安工作基础，且作为沿江经济发达地区，拥有以金融为代表的投资服务行业，以贸易平台、网上零售、新型购物中心等为代表的新经济行业和以“中国芯、创新药、蓝天梦、未来车、智能造、数据港”为代表的六大核心产业。该等产业相关企业的发展依赖于大数据、人工智能和互联网信息共享流通，对网络犯罪而言是具有高价值的重点攻击对象，也

是涉网犯罪的高风险企业。浦东新区公安干警案件侦查的丰富经验和高风险企业集聚环境为公司涉网犯罪侦查打击服务平台的研发和建设提供了业务经验和高频样本，有助于平台专题库的建设和完善。本项目立足浦东公安良好的网安工作基础和区域典型高频样本，有效保障了公司涉网犯罪侦查平台对复杂涉网犯罪案件的侦查能力，对后续全国各地平台的建设推广具有较强的可借鉴性。此外，本项目通过涉网犯罪侦查打击服务的拓展，有利于加强与公安部门的业务协作，在拓展涉网犯罪安全服务需求的同时，有助于进一步带动公司网络安全产品在公安领域的应用与推广，为公司未来市场拓展提供重要基础。

3、项目与现有业务或发展战略的关系

本项目拟建设以涉网犯罪侦查技术支撑服务为核心的安全服务中心，涉网犯罪侦查打击服务平台是公司针对公安机关实际业务需求，依托公司在网络安全领域的产品技术和人才基础，为公安客户提供的技术支撑服务平台。本项目是公司立足网络安全业务基础，为适应涉网犯罪日益猖獗、发案数量激增的发展趋势，进行的创新产品服务开发，能够进一步丰富公司产品服务类型，巩固现有客户的关系，拓展业务发展方向。

4、项目实施准备和进展情况

本项目预计建设期为 3 年，项目总投资 13,006.66 万元，拟投入募集资金 10,216.18 万元，其余所需资金通过自筹解决。项目具体投资内容如下：

单位：万元

序号	项目名称	投资总额	募集资金金额
1	**工程建设费用**	**5,806.22**	**4,291.10**
1.1	场地租赁费	1,515.12	-
1.2	场地装修费	864.00	864.00
1.3	硬件购置	2,434.60	2,434.60
1.4	软件购置	992.50	992.50
2	**研发费用**	**5,925.08**	**5,925.08**
3	**基本预备费 2%**	**234.62**	-
4	**铺底流动资金**	**1,040.74**	-
	合计	**13,006.66**	**10,216.18**

本项目实施主体为公司全资子公司上海安恒智慧城市安全技术有限公司。

2020 年 9 月，上海安恒智慧城市安全技术有限公司已就项目所需用楼与上海张江高科技园区开发股份有限公司签署《房屋租赁合同》。

本项目已经完成项目备案，并取得了上海市张江科学城建设管理办公室出具的《上海市企业投资项目备案证明》（国家代码：2021-310115-04-04-113188）。

根据《中华人民共和国环境影响评价法》、《建设项目环境保护管理条例》、《建设项目环境影响评价分类管理名录（2021 年版）》，公司本次发行所募集资金投资项目未列入《建设项目环境影响评价分类管理名录（2021 年版）》，属于不纳入建设项目环境影响评价管理的项目，无需办理环评报批手续，符合有关环境保护的要求。

5、预计实施时间及整体进度安排

本项目由公司间接全资子公司上海安恒智慧城市安全技术有限公司实施，预计总投资额 13,006.66 万元，拟投入募集资金 10,216.18 万元，建设期 3 年。公司计划于第一年完成项目方案设计与评审，租赁场地，开始场地装修，并于当年完成涉网犯罪侦查打击服务平台初始版本的研发。第二至第三年开展涉网犯罪侦查打击服务平台的迭代升级，于第三年年底前完成平台开发工作，项目建设完成。

6、发行人的实施能力

本项目主要客户为公安部门，经过多年的业务发展，公司在公安领域积累了深厚的客户基础。在涉网犯罪领域，公司曾多次收到并执行了浦东网警和经侦部门提出的协助进行涉网犯罪侦查需求，为公安机关提供了关键性辅助工作，获得了较高的客户认可度。

在与公安部门多年的合作中，公司在涉网犯罪侦查打击领域已经形成一定的技术和人才积累。本项目产品属于行业内较前沿产品，主要涉及大数据关联分析、嫌疑人目标画像技术和案件线索主动发现技术等，公司在相关领域已积累了部分技术与专利，具备良好的技术基础，未来将进一步加强技术原型研发。同时，公司在业务开展过程中，除网络安全研发人才外，积累培育了一支协助公安部门调查涉网犯罪的技术服务团队，以及需求分析和功能设计相关的人才队伍，为本项目的顺利实施提供了必要的人才储备。

7、资金缺口的解决方式

本次发行募集资金到位前，公司将根据募集资金投资项目的实际情况，以自筹资金先行投入，并在募集资金到位后予以置换。募集资金到位后，若扣除发行费用后的实际募集资金净额少于拟投入募集资金总额，不足部分由公司以自筹资金解决。

8、项目经济效益评价

经测算，本项目税后内部收益率为 23.27%，税后静态投资回收期为 6.64 年，项目预期效益良好。

（三）信创产品研发及产业化项目

1、项目基本情况

本项目拟以杭州安恒信息技术股份有限公司为实施主体，在杭州滨江区安恒大厦临近地块自建办公用楼，开展信创产品线开发、适配和产业化基地建设，同时建立省级信创适配实验室，逐步完成国产化技术路线适配工作，搭建符合国家网络安全法、国家密码管理法等法规要求的完善的信创产品体系，为客户提供定制化信创产品和基于国产化环境的网络安全解决方案。此外，项目还将加强网络资产测绘、新型未知威胁发现、攻击溯源等关键技术的研发，以适应日益复杂的网络安全环境，强化公司信创业务集成能力，在抓住信创产业发展机遇的同时，进一步提升公司的综合竞争优势。

2、项目经营前景

（1）本项目顺应我国信息安全产品国产化替代的必然要求

信息技术应用创新产业是国家构建安全可信的自有 IT 产业的重要基础，是国家经济数字化转型、提升产业链发展的关键。从“华为、中兴事件”体现出我国科技产业受制于人的现状制约了经济发展。2020 年 5 月 15 日，美国商务部在全球范围内限制使用美国软件和技术的公司向华为提供半导体等产品，中国芯片、系统的断供威胁持续增大，信息技术产业创新的必要性和紧迫性愈发凸显。为解决本质安全问题，信创作为国家战略成为我国“新基建”的重要内容。同时“数字中国”战略提出了建设“2+8”安全可控体系，标志着 2020-2022 年成为

国家安全可控体系推广的重要时期。国家对信息安全愈加重视，各级政府积极建立基于国产化的 IT 底层架构和标准，信创产业发展势头强劲，国产化替代形势不可逆转。

本项目依托公司在网络安全领域的产品技术和人才基础，依据国家战略要求，对基础网络安全产品、云安全平台、态势感知平台和安全运营平台等进行国产化适配。同时项目将基于国产化平台，全面开展信创领域的安全咨询、安全集成、安全运营等工作，加强对运维访问控制审计技术、分布式漏洞发现与验证技术、基于云架构的安全扫描与监测技术、SaaS 化云安全防护等技术的研发力度，有助于提升公司新一代网络安全产品研发能力，推进和适应我国信息产品国产化替代趋势。

（2）国产化 CPU 及操作系统已基本完成国产化替代，下游国产化软硬件需求逐步显现

目前，国产 CPU、操作系统已经实现从“能用”到“好用”的跨越，以龙芯、飞腾、兆芯、申威、海光、鲲鹏为代表的国产 CPU，以及以中标麒麟、银河麒麟、统信 UOS 为代表的国产操作系统，已经初步具备替代能力。

随着国产 CPU、操作系统等基础设备完成国产化替代布局，下游软硬件产品的国产化替代进程趋势明朗。过去国内一定程度上存在“重硬轻软”的情况，软件与智能硬件相比较少受到关注，随着“中国制造 2025”计划出台，近年来国家政策和地方政策逐渐向软件倾斜，为我国自主研发的软件发展注入了强心剂。2020 年 8 月 4 日，国务院印发《新时期促进集成电路产业和软件产业高质量发展的若干政策》，此次政策将软件产业核心技术的研发提升举国体制的新高度，强调以国家科技重大专项的方式支持软件产业，引导资金、人才向软件产业转移。

由于自主可控的产业链条上各生产环节的企业存在紧密的分工协作关系，上游的 CPU、操作系统等基础产品的更新换代促使下游软件国产化需求空间进一步扩大。公司主要客户政府、公安、电信运营商、金融企业等机构对于安全性、可控性要求的不断提高，在国产软件技术达到替代标准的情况下，开始引入软件技术自主可控的集采要求。本次信创产品研发及产业化项目是公司顺应国产替代

安全可控大趋势，满足软件技术可控集采要求的必然选择，是公司保持并提升主要下游市场竞争力的重要战略。

（3）信创产业发展势在必行，公司急需顺应趋势完成信创产品及市场布局

随着国产 CPU、操作系统等基础层产品不断完善，信创产业逐步成为当前形势下国家经济发展的新动能，以 2020 年为起点，信创产业开始全面推广，预计 2020 年我国自主可控的计算机市场规模约为 1.05 万亿元，到 2025 年市场规模将达到 1.3 万亿；未来 3 年信创领域国产芯片替代空间达 220 亿元；操作系统领域由于外资厂商高度垄断，未来 3 年信创领域国产操作系统替代空间可达 264 亿元，我国信创产业发展空间巨大。伴随安全自主可控的信息化建设进程的推进，下游客户对信创网络安全产品和服务需求强烈，行业市场空间广阔。

在信创产业的不断发展下，国产化替代将从电信运营商、政府、金融等关键敏感行业逐步向全行业展开。中国移动在 2020 年 7 月大规模采购国产数据库用于 OLTP 自主可控数据库联合创新项目，明确要求各参与投标的厂商拥有自主知识产权、产品核心代码为投标公司自主研发且具有数据库方面的发明专利，最终国内南大通用、人大金仓、阿里云、万里开源、中兴通讯五家公司中标。根据中国电信公布的 2020 年服务器采集清单，本年度将采购鲲鹏 920 系列处理器或 Hygon Dhyana 系列处理器，年度采购服务器中国产化比例达到了 20%。以银行为代表的金融行业也开始加快国产化替代的脚步，2020 年农行重点采购了 2000 台基于鲲鹏处理器的 TaiShan 服务器，将用于金融行业首个“基于 ARM 架构多路服务器+全开源中间层软件+自研应用”的业务系统。

作为公司重要下游行业，2017-2019 年该等电信运营商、政府、金融等关键敏感行业客户对公司的营业收入贡献比重分别达到 50.93%、51.94%和 48.71%。公司需要持续满足这三类客户对安全产品及服务的需求，建立与客户的良好合作关系，保持公司长期收入的稳定。面对该等客户已逐步实施的国产化替代采购策略，提前进行信创领域布局是公司维系客户巩固市场份额的重要举措。

信创行业暂未出现垄断性国产化平台，目前市场同时存在龙芯、飞腾、兆芯、申威、海光、华为海思等主流国产 CPU 以及中标麒麟、银河麒麟、中科方德、神威睿思、深度、普华等主流国产操作系统，不同客户基于业务需求，会自主选

择不同品牌的 CPU 和操作系统，各 CPU 与操作系统适配技术差异较大，需网络安全厂商进行针对性的适配、改造与研发，一定程度上丰富了细分市场，推升了信创产业的市场空间。

包括北信源、蓝盾股份在内的多家同行业信息安全厂商陆续通过各类直接或间接融资方式投资布局信创产业化项目。面对未来错综复杂的全球政治格局，国产化替代势在必行，尽早布局信创产业是整体信息安全产业及公司巩固原有市场份额、开拓新增市场的必然战略选择。

3、项目与现有业务或发展战略的关系

本项目是公司依据国家战略要求对公司现有产品业务的拓展与提升，凭借公司在网络安全领域的产品技术和人才基础，对公司现有网络安全产品进行国产化适配，以满足国家党政机关电子公文、电子政务国产化提及，以及“关键信息基础设施国产化替代”的要求。

公司现已在网信、网安新监管、大数据局、其他政府部委、金融、运营商、大型央国企全面开展业务支持，本次信创领域涉及的方向包括党政系统软硬件替换、信创私有云、混合云平台建设、覆盖关键基础设施相关行业，与现有网信、网安、大数据局、政府部委、金融、运营商高度一致，具有极强的业务延展和扩展。

在十四五规划中，新基建中对于自主创新的要求更为迫切，本项目是公司抓住信创产业发展的重大机遇，通过现有产品的国产化适配研发与升级，积极开拓系统集成，更好地满足客户需求，进一步增强公司在行业内的竞争力。

4、项目实施准备和进展情况

本项目预计建设期为 3 年，项目总投资 62,122.22 万元，拟投入募集资金 45,870.82 万元，其余所需资金通过自筹解决。项目具体投资内容如下：

单位：万元

序号	项目名称	投资总额	募集资金金额
1	**工程建设费用**	**32,522.61**	**31,166.61**
1.1	土地款	1,356.00	-
1.2	场地建造费	24,892.61	24,892.61
1.3	硬件购置	3,314.00	3,314.00

1.4	软件购置	2,960.00	2,960.00
2	**研发费用**	**23,555.21**	**14,704.21**
3	**基本预备费 2%**	**1,121.56**	**-**
4	**铺底流动资金**	**4,922.84**	**-**
	合计	**62,122.22**	**45,870.82**

本项目实施主体为安恒信息。项目拟在杭州滨江区安恒大厦临近地块自建办公用楼，进行信创产品线开发、适配和产业化基地建设，预计建设期为 3 年。2020 年 7 月，公司已就本项目建设所需用地与杭州市规划和自然资源局签署《国有建设用地使用权出让合同》，约定杭州市规划和自然资源局将东至规划网聚路，南至安恒信息技术股份有限公司，西至西兴路，北至杭州中胜智能科技有限公司、浙江星联合能源技术有限公司的地块转让给公司，宗地编号为杭政工出【2020】17 号，宗地总面积 10045 平方米。

本项目已经完成项目备案，并取得了杭州市滨江区发展和改革局出具的《杭州高新区（滨江）企业投资项目备案通知书》（编号：滨发改金融【2021】002 号）。

根据《中华人民共和国环境影响评价法》、《建设项目环境保护管理条例》、《建设项目环境影响评价分类管理名录（2021 年版）》，公司本次发行所募集资金投资项目未列入《建设项目环境影响评价分类管理名录（2021 年版）》，属于不纳入建设项目环境影响评价管理的项目，无需办理环评报批手续，符合有关环境保护的要求。

5、预计实施时间及整体进度安排

本项目由安恒信息实施，预计总投资额 62,122.22 万元，拟投入募集资金 45,870.82 万元，建设期 3 年。公司计划于第一年完成项目方案设计与评审，购置土地，开始场地建造，并于当年完成部分信创产品的研发。第二至第三年持续推进国产化核心技术攻关及适配工作，于第三年年底前完成场地建造验收和信创产品系列开发工作，项目建设完成。

6、发行人的实施能力

本项目主要建设目的为公司原有安全产品体系的国产化适配研发及产业

化，公司原有的网络安全底层技术优势在国产系统适配后仍将保持。公司拥有 48 项网络安全核心技术，并在云安全、大数据安全、物联网安全和智慧城市安全等多个细分市场形成核心技术优势，处于行业领先位置，能够有效保障本次项目公司原有安全产品体系的国产化适配研发及产业化进度。

截至本募集说明书出具日，公司已与龙芯、兆芯、鲲鹏、飞腾、申威、海光、统信 UOS、麒麟软件等芯片及操作系统厂商完成了共计 59 份产品兼容性互认证明。公司态势感知平台、天池云安全平台及 AILPHA 大数据平台等平台类产品已全面开展国产化芯片及操作系统适配工作；远程安全评估系统、Web 应用防火墙及综合日志审计等部分网络安全基础产品已完成国产适配转化。此外，公司在国家信创领域发展中担任了重要角色，帮助公司掌握国家信创发展战略及技术发展方向，进行精准产品研发。公司是信息技术应用创新工作委员会成员单位，参与整机工作组、龙芯工作组、飞腾工作组、鲲鹏工作组、人工智能工作组等的相关工作，同时参加了安全中心技术委员会安全开发治理、安全性测试、关键产品挑战赛、漏洞管理、终端安全 5 个专项组，是安全开发治理专项组的组长。

安恒信息通过持续的市场拓展，目前公司产品及服务已经进入了包括运营商、政府、能源、金融、教育等在内的众多行业，积累了上述领域大量优质客户，并长期保持着深入稳定的合作关系，该等客户所处领域的网络安全关乎国计民生和国家安全，是国家政策要求的处于优先实现自主可控的核心关键行业，是信创产品的刚需群体，有效降低了本次信创项目市场拓展经营风险和财务风险。

7、资金缺口的解决方式

本次发行募集资金到位前，公司将根据募集资金投资项目的实际情况，以自筹资金先行投入，并在募集资金到位后予以置换。募集资金到位后，若扣除发行费用后的实际募集资金净额少于拟投入募集资金总额，不足部分由公司以自筹资金解决。

8、项目经济效益评价

经测算，本项目税后内部收益率为 25.07%，税后静态投资回收期为 6.55 年，

项目预期效益良好。

（四）网络安全云靶场及教育产业化项目

1、项目基本情况

本项目拟以杭州安恒信息技术股份有限公司为实施主体，在杭州市滨江区新建办公楼的部分楼层进行网络安全演训产品及网络安全靶场云化部署的研发及产业化。项目将建设网络安全靶场平台，为参与培训的学员提供网络空间仿真实训竞技平台，以“学、练、测、评”一体化设计的方式加强学员专业技能。同时将网络安全靶场和安全综合实验室进行云化部署，建立 SaaS 化网络安全云靶场平台，结合网络安全教学产品和认证服务实现平台、教学内容和服务一体化，开展以实战能力养成为导向的网络安全培训服务。此外，本项目还将对公司目前商用网络安全基础及平台产品进行教育培训适用化开发，为学校、大型企业和政府提供专业信息安全培训工具。

2、项目经营前景

（1）项目建设为我国网络安全人才培养提供了有效工具

随着我国信息化进程不断深入和《数据安全法》等政策法规的出台，保障数据安全的重要性越发凸显，企业对网络安全人才培养领域的投入持续加大。网络安全团队需要以业务为导向，积极构建业务与网络安全之间的共生关系。同时，伴随等保 2.0 等新标准的实施，我国网络安全建设已从单一安全走向整体安全，对网络安全人才提出了更高的要求，网络安全人才培养的能力和水平亟待提高。

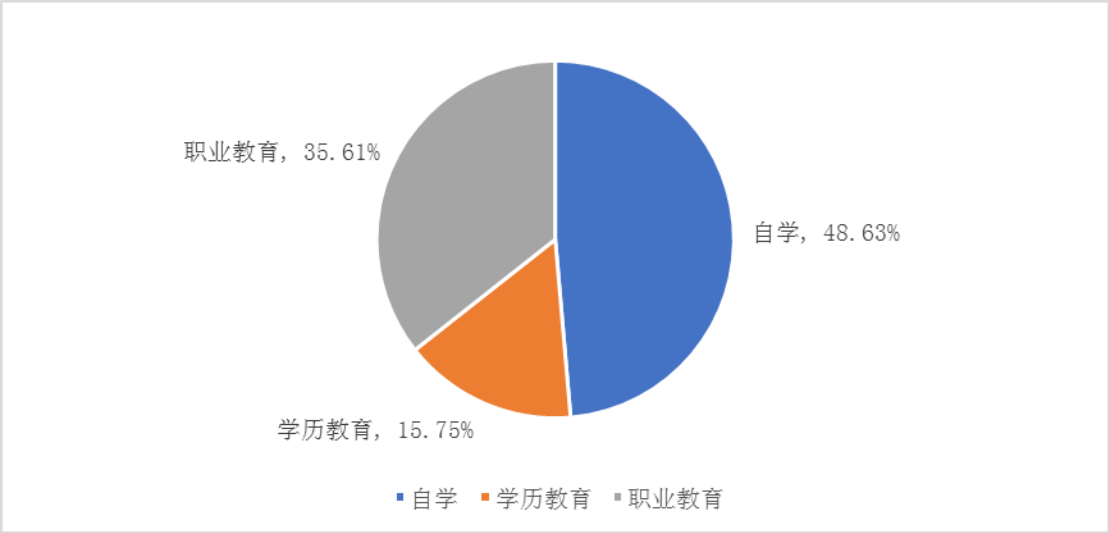
目前，我国网络安全人才培养的主要途径是大学教育，但相关专业发展时间较短，且偏重理论教学，缺乏实践和参与产业实践的机会和动力，知识更新速度较慢，存在学生理解较浅、培养目标不明确、学生自身能力和实战化能力的培养较为缺乏等问题。

本项目基于网络安全行业人才紧缺的现状，以及当前学历教育与职业技能水平不匹配的问题，为网络安全人才培养提供了环境、专业工具和业务形态支撑，有助于解决高层次专业教师缺乏，教材良莠不齐，缺乏攻防演练平台，综合性、自主防御性试验难以构建和学生缺少实战等问题。通过网络安全靶场平台产品研发，加强现有网络安全产品向适用于教育教学产品的转化研发，为我国网络安全

教学内容建设和网络安全人才培养提供实战化培训工具，有利于丰富我国网络安全人才培养模式，提高网络安全人才培养能力和水平，进而满足日益增长的网络安全人才需求。

（2）本项目是公司加强网络安全教育市场拓展、抢占市场份额的重要举措

伴随网络安全行业的快速发展，网络安全人才出现了较大缺口，根据新华网报道，截至 2019 年 9 月，我国网络空间安全人才数量缺口高达 70 万人，预计到 2020 年将超过 140 万人。面对市场巨大的人才需求缺口，校企合作、企业内训及职业类培训等人才培养模式加速发展，以人才培养和系统测试为驱动的网络安全教育培训需求快速增长。2019 年，我国网络安全行业“自学型”求职者占比达 48.63%、“职业教育型”求职者占比 35.61%，自学和职业教育已经成为求职者获取网络安全知识和技能的主要方式[2]。



数据来源：360 网络安全大学人才研究院

面对持续增长的市场空间，同行业领先企业相继开始布局网络安全人才教育市场，天融信、奇安信等企业设立专攻校企合作销售团队，天融信、启明星辰以及绿盟科技均设有网络安全培训学院，而蓝盾股份等企业已着手投资建设网络空间仿真靶场实训项目。尽管公司在网络安全教育行业已有所布局，成立了网络空间安全学院，但是尚未具备专属的教育培训自主产品与服务生态，目前采取的主

[2]数据来源：360 网络安全大学《2019 网络安全行业人才发展研究报告》

要方式是依附于公司商业化产品提供网络安全教育培训附加服务，针对专业教育培训的适配性较低。本项目将通过加强网络安全靶场产品研发和网络安全人才培训服务改善现状。通过网络安全靶场产品研发，有助于扩展公司教学类产品市场空间，升级以实战为导向的网络安全培训服务，实现网络安全人才培养产品和服务一体化升级，完成专业网络安全教育培训业务布局，从横向上扩展公司业务线。

（3）项目建设利于公司选拔网络安全人才

专业人才稀缺是网络安全行业近年发展的痛点。根据智联招聘发布的《2019 网络安全人才市场状况研究报告》，网络安全人才市场的需求在三年的时间内，扩大到了 2016 年初的 10 倍以上。目前我国每年网络安全学历人才培养数量不足 1.5 万人，网络空间安全人才培养的数量远远满足不了社会需求。2019 年，“等保 2.0”的发布及正式执行，对互联网企业、安全厂商、各大政企单位提出更高的安全合规要求。该等制度的落实推动了网络安全人才的需求增长，网络安全人员的需求缺口进一步扩大。人才是网络安全行业各企业的核心资源，专业从业人员的数量、质量、结构和作用的发挥，直接关系到网络安全企业专业水平和服务质量。

近年来随着公司业务规模的快速增长，网络安全人才需求大幅提升，在不断提高招聘力度的情况下，公司校招缺口仍达到 200-300 人。在行业高速发展的背景下，公司未来网络安全人才存在持续性缺口。

网络安全人才培养服务下游用户主要包括在校学生及网络安全从业人员。提供网络安全培训服务有利于公司在网络安全人才稀缺的社会背景下精准发现并锁定相关人才，从而推动公司人才团队的建设与壮大，为长远发展注入优秀新鲜的血液，进一步提升公司在行业内的人才优势。

（4）项目有助于连接与协同下游客户，推广公司网络安全生态

公司为学校、大型企业和政府建设网络安全靶场，提供网络空间安全教育服务与产品，由于相关教育产品均演化自公司原有商业产品，开展教育业务有助于深化潜在用户对公司商业产品体系的认知和应用。此外，网络安全防护产品由于具有适配性与衔接性，不同公司的网络安全产品互不相通难以混合使用，产品学习及转换成本较高，公司将打造基于原有自主研发商用产品的教育专属培训产品

体系，教育培训产品的应用能够有效推广宣传公司商业产品体系，从源头更好地绑定潜在客户，促进公司商业产品体系的未来销售。

3、项目与现有业务或发展战略的关系

本项目既在横向上扩展公司产品线，又在综向上完善公司生态建设。

一方面，本项目依托公司产品技术和人才基础，开发网络安全靶场平台，扩展教学类产品市场空间。通过自建网络云靶场，升级以实战为导向的网络安全培训服务，实现网络安全人才培养产品和服务一体化升级，从横向上扩展公司业务线；

另一方面，本项目基于网络安全行业人才紧缺的现状，以及当前学历教育与职业技能水平不匹配的问题，在国家积极加强网络安全人才培养的政策推动下，公司凭借在行业内的技术和产品积累，结合行业客户需求，进一步拓展教育领域市场，为学校、大型企业和政府建设网络安全靶场提供相应的产品的同时，深化用户对安恒产品的认知和熟悉，推进公司生态建设；

因此，本项目是公司抓住网络安全教育市场需求快速增长的机遇，通过产品、内容研发和服务升级拓展新的市场空间，在满足国家战略需求的同时，推动公司业绩增长，完善公司业务生态。

4、项目实施准备和进展情况

本项目预计建设期为 3 年，项目总投资 15,753.23 万元，拟投入募集资金 12,541.34 万元，其余所需资金通过自筹解决。项目具体投资内容如下：

单位：万元

序号	项目名称	投资总额	募集资金金额
1	**工程建设费用**	**9,094.67**	**9,094.67**
1.1	场地建造费	6,190.57	6,190.57
1.2	硬件购置	1,953.10	1,953.10
1.3	软件购置	951.00	951.00
2	**研发费用**	**5,521.34**	**3,446.67**
3	**基本预备费 2%**	**292.32**	-
4	**铺底流动资金**	**844.90**	-
	合计	**15,753.23**	**12,541.34**

本项目实施主体为安恒信息。项目拟在杭州市滨江区新建办公楼的部分楼层开展，预计建设期为 3 年。2020 年 7 月，公司已就本项目建设所需用地与杭州市规划和自然资源局签署《国有建设用地使用权出让合同》，约定杭州市规划和自然资源局将东至规划网聚路，南至安恒信息技术股份有限公司，西至西兴路，北至杭州中胜智能科技有限公司、浙江星联合能源技术有限公司的地块转让给公司，宗地编号为杭政工出【2020】17 号，宗地总面积 10045 平方米。

本项目已经完成项目备案，并取得了杭州市滨江区发展和改革局出具的《杭州高新区（滨江）企业投资项目备案通知书》（编号：滨发改金融【2021】003 号）。

根据《中华人民共和国环境影响评价法》、《建设项目环境保护管理条例》、《建设项目环境影响评价分类管理名录（2021 年版）》，公司本次发行所募集资金投资项目未列入《建设项目环境影响评价分类管理名录（2021 年版）》，属于不纳入建设项目环境影响评价管理的项目，无需办理环评报批手续，符合有关环境保护的要求。

5、预计实施时间及整体进度安排

本项目由公司实施，预计总投资额 15,753.23 万元，拟投入募集资金 12,541.34 万元，建设期 3 年。公司计划于第一年完成项目方案设计与评审，购置土地，开始场地建造，并于当年完成网络安全云靶场及网络空间安全教育培训平台产品初始版本的研发。第二至第三年开展相关产品的迭代升级，于第三年年底前完成办公和培训场地建造验收和正式产品开发工作，项目建设完成。

6、发行人的实施能力

公司在网络安全行业深耕多年，积累了行业领先的产品技术、人才基础与客户资源，能够有效保障本项目顺利实施。

在产品技术方面，网络安全靶场产品主要运用的如虚拟网络构建、多维网络互联、能效评估分析、复杂虚拟化网络管理、可视化展现、异构虚拟化平台统一接入等技术是公司现有产品体系成熟技术，仅需针对教育场景进行研发转化。目前公司已开展靶场产品开发工作并取得一定成果，为后续根据场景定制化开发有针对性的虚拟化技术、网络技术、虚实结合技术、数据分析算法等相

关技术提供了良好的基础。

在人才积累方面，除网络安全专业技术人员外，公司在虚拟化技术开发、数据分析、靶场环境开发、网络安全培训、场景运维和教务等方面人员均有一定积累，能够有效保障项目的顺利实施。

目前，公司已为部分客户提供了网络安全教育培训产品，具备一定的客户基础和品牌优势，为进一步客户拓展，扩大市场规模提供了有利条件。此外，安恒信息具备颁发国家级认证证书的资质，是最早一批联合中国信息安全测评中心认定的“授权培训机构”之一，也是目前浙江省唯一的一家CISP（信息安全国内第一认证）授权培训机构，可以为接受培训的合格学员提供注册大数据安全分析师（CISP-BDSA）、注册云安全工程师（CISP-CSE）认证资质。拥有颁发此项认证的资质是公司安全培训能力的有效背书，能够吸引更多潜在从业人员，有效提升公司在网络安全教育产业的市场开拓能力。

7、资金缺口的解决方式

本次发行募集资金到位前，公司将根据募集资金投资项目的实际情况，以自筹资金先行投入，并在募集资金到位后予以置换。募集资金到位后，若扣除发行费用后的实际募集资金净额少于拟投入募集资金总额，不足部分由公司以自筹资金解决。

8、项目经济效益评价

经测算，本项目税后内部收益率为16.23%，税后静态投资回收期为7.19年，项目预期效益良好。

（五）新一代智能网关产品研发及产业化项目

1、项目基本情况

本项目拟以公司全资子公司成都安恒信息技术有限公司为实施主体，在成都购置办公场地开展新一代智能网关产品研发及产业化，并结合新场景将其适配应用于云计算、大数据、物联网、工业互联网及人工智能防护等新兴应用环境和技术方向，满足客户在新时代技术发展下数字化转型的需求，提升公司综合安全解决方案的完整性和适配性，进一步扩大公司产品业务规模，提升整体竞争力。

2、项目经营前景

（1）本项目有助于抓住行业技术迭代机遇，扩大公司网关产品业务规模

安全内容管理、防火墙、IDS/IPS、统一威胁管理、VPN 等五个细分市场构成了网络安全基础设施市场的主体。根据 IDC 统计数据，2019 年防火墙是我国网络安全基础设施市场占比最大细分市场，占比达 38%。目前同行业主要竞争对手中绿盟科技、奇安信、山石网科、天融信等在网络层防火墙领域均有较大的业务体量，且各主要安全厂商在 AI 防火墙层面的战略布局持续加深。公司初期基于业务规模限制，业务及技术主要聚焦于应用层安全领域，对网络基础层防护产品的研发投入有限，相关产品收入占比相对较低。2019 年度，公司基础网络层防护产品收入为 4,897.23 万元，仅占公司主营收入的 5.19%，与细分行业领先企业相比存在较大差距，潜力较大。

随着人工智能、区块链、5G、量子通信、工业互联网、大数据、云计算、物联网等具有颠覆性的战略性新技术快速演进，大规模数据泄露、高危漏洞、新技术应用下的网络攻击等网络安全问题频发，攻击团伙的智能化、商业化生态已形成，网络威胁态势严峻。在云计算、大数据、国产化替代及 AI 智能防护等需求的推动下，防火墙作为传统的网关产品处在向智能化、简易化及可视化方向技术更新迭代的关键阶段，市场现有产品技术架构受到挑战，行业竞争格局或将面临较大变动。

基于网关产品在整个网络安全防护产品市场中重要地位，公司拟研发新一代智能网关产品，抓住行业技术迭代的机遇，快速抢占扩大网关产品市场份额，本项目的顺利实施对扩大公司网络层安全业务规模、提升整体竞争实力意义重大。

（2）本项目有助于完善网络安全生态建设，推进整体解决方案集成联动

网络层网关防护技术在其他安全产品中有着广泛的应用，是构建网络安全生态建设必不可少的基础技术，尤其是数据中心出口以及云化场景，需要进行较大的改造集成，通过解决云环境流量牵引、控制防护平面解耦、安全能力集成、安全防护检测服务链等技术提升边界网关整体解决方案防护能力，形成整体安全防护产品的集成联动。自有基础层防护产品及技术的缺失将影响公司整体网络安全解决方案适配及稳定性。

基于公司业务整体发展和业绩提升考虑，本项目拟自建智能网关产品生产线，快速切入网络层防火墙、IPS 及 IDS 等网关市场，充分发挥公司在云计算安全、大数据安全、物联网安全及工业互联网安全等领域的技术积累，提升公司网关产品在相关领域的防护能力和适配能力，完善自有安全防护产品生态，提升整体解决方案能力。

3、项目与现有业务或发展战略的关系

本项目拟开展新一代智能网关产品的研发和产业化，进一步补足公司网络层安全能力，借助网关产品迭代升级周期机遇，迅速切入网络层防火墙产品、DDOS、IPS、IDS 等市场，充分发挥公司在云计算安全、大数据安全、物联网安全及工业互联网安全等领域的技术积累，提升公司网关产品在相关领域的防护能力和适配能力，完善自有安全防护产品生态，提升整体解决方案能力。

4、项目实施准备和进展情况

本项目预计建设期为 3 年，项目总投资 22,622.09 万元，拟投入募集资金 17,924.13 万元，其余所需资金通过自筹解决。项目具体投资内容如下：

单位：万元

序号	项目名称	投资总额	募集资金金额
1	**工程建设费用**	**13,948.79**	**13,948.79**
1.1	场地购置费	11,360.11	11,360.11
1.2	场地装修费	1,832.28	1,832.28
1.3	硬件购置	709.40	709.40
1.4	软件购置	47.00	47.00
2	**研发费用**	**6,368.25**	**3,975.34**
3	**基本预备费 2%**	**406.34**	-
4	**铺底流动资金**	**1,898.71**	-
	合计	**22,622.09**	**17,924.13**

本项目实施主体为安恒信息全资子公司成都安恒信息技术有限公司。公司拟在成都购置办公场地开展新一代智能网关产品研发及产业化，预计建设期为 3 年。2021 年 1 月，成都安恒信息技术有限公司已就项目所需用楼与成都高投资产经营管理有限公司签署《购房意向书》。

本项目已经完成项目备案，并取得了成都高新区发展和改革委员会出具的

《四川省固定资产投资项目备案表》（编号：川投资备【2101-510109-04-04-596165】FGQB-0032号）。

根据《中华人民共和国环境影响评价法》、《建设项目环境保护管理条例》、《建设项目环境影响评价分类管理名录（2021 年版）》，公司本次发行所募集资金投资项目未列入《建设项目环境影响评价分类管理名录（2021 年版）》，属于不纳入建设项目环境影响评价管理的项目，无需办理环评报批手续，符合有关环境保护的要求。

5、预计实施时间及整体进度安排

本项目由公司全资子公司成都安恒信息技术有限公司实施，预计总投资额22,622.09万元，拟投入募集资金17,924.13万元，建设期3年。公司计划于第一年完成项目方案设计与评审，购置场地并装修，并于当年开始新一代智能网关产品的研发。第二年主要设备购置完毕，新一代智能网关产品实现初步定型，开始客户拓展。第三年新一代智能网关产品研发完毕，项目建设完成。

6、发行人的实施能力

公司网络信息安全基础产品具有广泛的市场销量和客户基础，其中 Web 应用防火墙、数据库审计与风险控制系统、综合日志审计平台等产品处于行业领先位置。公司自2017年开始完善渠道建设，致力于加大渠道合作伙伴扶持力度、落实渠道激励政策，建设公司级的合作平台，并已形成成熟的行业直销和渠道代理销售模式。随着公司营销网络及渠道体系的不断完善，成熟的行业直销和渠道代理销售模式为本项目新一代智能网关产品的销售实现提供了可靠保障。此外，公司作为网络安全综合解决方案提供商，整体产品体系具有较强联动性，公司将推动本项目新一代智能网关产品与自有云安全平台、大数据态势感知平台等集成整合，通过整体安全防护解决方案进一步带动产品销售。

同时，公司丰富的技术积累为本项目提供了技术保障。本项目将开展高性能报文转发引擎、高性能安全检测引擎、协议处理引擎、安全防护引擎、多场景支持、硬件加速等部件的研发，具有较高的技术要求。截至 2020 年 9 月 30 日，公司拥有超过 130 项已获得授权的专利，对于项目所涉及的关键技术包括 DDOS 识别技术、VPN 技术、威胁情报集成技术、国产多硬件平台支持技术、云

化支持技术等都已具备一定的研究基础，且部分研究成果已获得或正在申请专利授权。此外，公司目前在应用层有较多的安全防护检测能力及数据，能够有效助力新型智能网关产品研发，为项目提供技术保障。同时，公司已经在云安全、大数据安全、物联网安全及工业互联网安全等领域积累了丰富的技术和研发经验，为新一代智能网关产品在相关领域的研发与应用奠定了良好的技术基础。

7、资金缺口的解决方式

本次发行募集资金到位前，公司将根据募集资金投资项目的实际情况，以自筹资金先行投入，并在募集资金到位后予以置换。募集资金到位后，若扣除发行费用后的实际募集资金净额少于拟投入募集资金总额，不足部分由公司以自筹资金解决。

8、项目经济效益评价

经测算，本项目税后内部收益率为 24.50%，税后静态投资回收期为 5.82 年，项目预期效益良好。

（六）车联网安全研发中心建设项目

1、项目基本情况

本项目拟以杭州安恒信息技术股份有限公司为实施主体，在公司现有办公场所建设车联网安全研发中心，进行车联网安全领域产品技术的研发。项目拟搭建完善的研发环境，引进行业专业人才，积极与整车厂商和科研院所合作，开展车联网安全产品体系的研发，为公司向车联网安全领域的业务拓展布局。

2、项目经营前景

（1）本项目有助于推动车联网安全保障体系的完善

车联网作为物联网在交通领域的典型应用，内容丰富，涉及面广。基于车联网“云”、“管”、“端”三层架构，车联网的网络安全重点关注智能网联汽车安全、移动智能终端安全、车联网服务平台安全、通信安全，同时数据安全和隐私保护贯穿于车联网的各个环节。随着车联网智能化和网联化的推进，车联网网络安全事件已然显现，根据 Upstream Security 发布的 2020 年《汽车网络安全报

告》，汽车行业面临的网络威胁越来越普遍，自 2016 年以来发生的年安全事件数量增加了 605%。用户生命财产安全受到威胁，车联网安全已成为关系车联网发展的重要因素。2020 年 8 月工信部发布《关于开展 2020 年网络安全技术应用试点示范工作的通知》，将车联网安全列为重点方向。

本项目通过身份认证体系、车辆安全检测、靶场虚拟化技术、威胁情报获取和车载微流量技术的研发，能够进一步形成完善的车联网安全产品体系，满足车联网网络安全需求。凭借公司在网络信息安全领域成熟的产品技术，积极开展传统安全产品技术向车联网场景的研发转化，加强与车企客户和科研院所等在安全检测、验证、认证培训等方面的研发合作，推动公司车联网产业链的建设完善。本项目是公司顺应车联网产业发展的安全需求进行的产品技术研发，有助于推动车联网安全保障体系的建设完善。

（2）车联网明确的发展前景要求公司提前进行产品技术布局

2020 年是智能网联汽车行业政策和技术落地的关键节点。2019 年 9 月国务院发布《交通强国建设纲要》，明确提出加强智能网联汽车研发，形成自主可控完整的产业链。经过 2015-2019 年的前期重点培育，国内智能网联汽车行业逐步走向成熟，2020 年是智能网联企业行业落地的关键一年，国家对网联化水平确定了具体的考核指标，要求到 2020 年汽车 DA（驾驶辅助）、PA（部分自动驾驶）、CA（有条件自动驾驶）系统新车装配率超过 50%，网联式驾驶辅助系统装配率达到 10%；智能汽车新车占比达到 50%，中高级别智能汽车实现市场化应用，大城市、高速公路的车用无线通信网络（LTE-V2X）覆盖率达到 90%；开展 5G-V2X 示范应用，车联网用户渗透率达到 30%以上，联网车载信息服务终端的新车装配率达到 60%以上。

在技术方面，5G 技术的发展有望推进智能网联汽车加速落地。5G 低延时、高可靠、大容量、大带宽及多并发数等特点有力支撑了车联网技术的发展，加速 T-Box 前装，加速动态数字地图更新，提高车载智能终端的渗透率和车路相关基础设施的通信能力。同时，V2X 技术路径之争逐步清晰。2019 年 12 月美国联邦通信委员会（FCC）通过了重新分配 5.9GHz 频段的 75MHz 频谱的提案，其中一部分频谱将用于 C-V2X 技术，C-V2X 技术地位逐步确立。2019 年 4 月，上汽、一汽、宇通等 13 家车企共同发布 C-V2X 商用路标，2020 下半年至 2021 上半年

将陆续实现 C-V2X 汽车量产，2020 年是 C-V2X 产业化元年。

随着 V2X 技术路径的明确，在国家政策和 5G 商用的推动下，基于车联网在驾驶安全性和交通治理方面的突出优势，车联网发展前景进一步明确。目前我国已将车联网产业上升到国家战略高度，我国车联网产业化进程逐步加快，根据前瞻产业研究院发布的《中国车联网行业市场前瞻与投资战略规划分析报告》统计数据，截至 2017 年，全球车联网市场规模约为 525 亿美元，预计到 2022 年将增加至 1,629 亿美元，复合年均增长率为 25.4%；我国车联网市场规模将从 2017 年的 114 亿美元增长到 2022 年的 530 亿美元，复合年均增长率为 36.0%。本项目通过加强行业专业人才引进，开展车联网安全关键技术研发和储备，为公司未来拓展车联网安全业务提前进行产品技术布局。

（3）车联网应用新场景的拓展有利于进一步强化公司技术实力

车联网是以车内网、车际网和车载移动互联网为基础，按照约定的通信协议和数据交互标准，在车与车、车与路边设施、车与行人以及车与网络之间进行无线通信和数据交换与共享的网络系统。与传统网络系统相比，车联网系统有着新的系统组成、新的通信场景，给系统安全性及用户隐私保护带来了新的挑战。

车联网是物联网技术应用的重要落地项目之一，也是建设智慧城市的重要组成部分，本项目关于车联网安全产品技术的研发将是公司物联网安全平台和智慧城市安全运营技术和解决方案的有效补充，有利于推动公司现有产品技术的完善，进一步强化公司技术实力。

3、项目与现有业务或发展战略的关系

随着智能网联汽车的发展，车联网发展趋势明确。本项目是顺应车联网产业发展的安全需求进行的产品技术研发，有助于推动车联网安全保障体系的建设完善。同时，本项目关于车联网安全产品技术的研发将是公司物联网安全平台和智慧城市安全运营技术和解决方案的有效补充，有利于推动公司现有产品技术的完善，进一步强化公司技术实力。

4、项目实施准备和进展情况

本项目预计建设期为 3 年，项目总投资 10,235.45 万元，拟投入募集资金 6,733.08 万元，其余所需资金通过自筹解决。项目具体投资内容如下：

单位：万元

序号	项目名称	投资总额	募集资金金额
1	**工程建设费用**	**1,248.00**	**1,248.00**
1.1	硬件购置	1,057.00	1,057.00
1.2	软件购置	191.00	191.00
2	**研发费用**	**8,786.75**	**5,485.08**
3	**基本预备费 2%**	**200.70**	**-**
	合计	**10,235.45**	**6,733.08**

本项目实施主体为安恒信息。公司拟以现有办公场所安恒大厦为实施地点开展本项目，预计建设期为 3 年。

本项目已经完成项目备案，并取得了杭州市滨江区发展和改革局出具的《杭州高新区（滨江）企业投资项目备案通知书》（编号：滨发改金融【2021】001 号）。

根据《中华人民共和国环境影响评价法》、《建设项目环境保护管理条例》、《建设项目环境影响评价分类管理名录（2021 年版）》，公司本次发行所募集资金投资项目未列入《建设项目环境影响评价分类管理名录（2021 年版）》，属于不纳入建设项目环境影响评价管理的项目，无需办理环评报批手续，符合有关环境保护的要求。

5、预计实施时间及整体进度安排

本项目由安恒信息实施，预计总投资额 10,235.45 万元，拟投入募集资金 6,733.08 万元，建设期 3 年。公司计划于第一年完成项目方案设计与评审，开始主要设备购置和人才引进，开展车联网安全产品技术研发，于第三年年底前完成产品技术研发工作，项目建设完成。

6、发行人的实施能力

公司立足车联网安全场景，积极开展与中国汽研等专业机构的研发合作。基于中国汽研在车辆检测领域的市场地位，与中国汽研的研发合作一方面能够保证本项目研发的产品技术贴近汽车安全检测标准，同时，也为后续车企客户拓展提供了便利。

公司现有丰富的网络信息安全技术及人才积累为项目实施提供了有效技术保障。公司在车联网安全领域的开发已取得阶段性成果：在车辆安全检测方面，随着与各大车企的深入合作，公司已经具备了提供完整安全服务和安全检测工具的能力；在车载网关方面，公司安全检测设备如APT、IPS、WAF等都已成熟，可在现有产品技术基础上结合车联网特定场景进行开发；公司针对车联网的PKI和KMS平台目前已基本开发完成，进入客户验证阶段。

7、资金缺口的解决方式

本次发行募集资金到位前，公司将根据募集资金投资项目的实际情况，以自筹资金先行投入，并在募集资金到位后予以置换。募集资金到位后，若扣除发行费用后的实际募集资金净额少于拟投入募集资金总额，不足部分由公司以自筹资金解决。

8、项目经济效益评价

本项目为研发项目，不直接产生收益。本项目效益体现在产品技术研发对公司未来业务发展提供技术支撑。

三、本次募集资金投资于科技创新领域的主营业务的说明，以及募投项目实施促进公司科技创新水平提升的方式

（一）公司所处行业属于战略性新兴产业，科技创新属性突出

公司主营业务为信息安全产品的研发、生产及销售，并为客户提供专业的信息安全服务，公司研发人员占总人数比超过30%，研发投入占总收入比超过23%，是国家级高新技术企业。根据国家统计局颁布的《战略性新兴产业分类（2018）》，公司所处行业属于新一代信息技术产业——新兴软件和新型信息技术服务——网络与信息安全软件开发、互联网安全服务。同时，根据《上海证券交易所科创板企业上市推荐指引》第三条的规定，公司属于新一代信息技术、高端装备、新材料、新能源、节能环保以及生物医药等高新技术产业和战略性新兴产业的科技创新企业。

网络信息安全行业覆盖了网络通信、计算科学、数据应用、人工智能、密码技术、行为科学等众多技术领域。网络安全产业的范畴随着网络安全保障需求不

断延伸扩展，要求网络安全公司不断开展研发创新，以满足大数据安全、云安全、物联网安全、工业互联网安全、威胁情报等细分市场对网络安全防护技术的新要求。在 2016 年启动的“十三五”国家科技创新规划中，国务院提出网络空间安全行业有良好的科创基础，属于需要进一步布局体现国家战略意图的重大科技项目。网络安全行业企业响应国家号召，不断加大科技创新力度，融合前沿科学技术创新网络安全产品，保障国家网络安全环境，行业战略政策地位进一步提升，科技创新属性突出。

（二）公司积极开展技术研发，重视科技创新能力

公司是网络信息安全行业领先企业，坚持技术创新的发展战略，不断在行业内率先推出创新产品，更新迭代既有产品和解决方案，大胆开拓新市场，产品在网络安全领域内拥有较强的竞争力。在网络安全基础产品领域，公司于成立之初便以应用安全和数据安全作为切入点，推出市场首创性产品数据库审计系统与 Web 应用防火墙产品，相关产品的市场份额位居市场前列。在网络安全平台和网络安全服务领域，公司于 2014 年率先开始向云计算、大数据、物联网等新兴领域转型，贴合国内信息安全产业发展趋势，占据较大先发优势，拥有深厚的技术储备，相关业务已成为公司重要的营收增长点。

凭借研发团队多年的努力以及持续不断的研发投入，公司在产品技术上具有较强的研发能力，积累了丰富的研发和产业化密切结合的经验和雄厚的技术、专利储备。截至 2020 年 9 月 30 日，公司共拥有 48 项核心技术，拥有已授权专利超过 130 项。

（三）本次募投项目紧密围绕公司主营业务，促进公司科技创新能力提升

本次募投项目紧密围绕公司现有网络信息安全主营业务进行，募投项目与现有业务关联度高，是加强公司对前沿技术的研发、支撑行业应用的持续升级、深化公司在网络安全行业相关领域业务布局的重要举措。

其中，数据安全岛项目及涉网犯罪侦查打击项目在整合目前主营产品 AiLPHA 大数据智能安全平台以及态势感知预警平台的基础上拟进行数据隔离可信环境执行、安全计算沙箱、多方数据联合建模及案件线索主动发现等领域的研发，形成新的技术优势，为数字经济发展提供所需的安全保障；

信创产业化项目、云靶场与教育产业化项目及新一代智能网关项目是对公司现有产品及技术的适配改造及升级，以顺应当前国际局势与科技变革。面对国产化替代明确的发展趋势，公司拟依托其在网络安全领域的产品技术和人才基础，依据国家战略要求，对基础网络安全产品、云安全管控平台、态势感知平台和安全运营平台等进行国产化适配。基于国产化平台，全面开展信创领域的安全咨询、安全集成、安全运营等工作，加强对运维访问控制审计技术、分布式漏洞发现与验证技术、基于云架构的安全扫描与监测技术、SaaS 化云安全防护等技术的研发力度；本次云靶场与教育产业化项目通过网络安全靶场平台产品研发，加强现有网络安全产品向适用于教育教学产品的转化研发，为我国网络安全教学内容建设和网络安全人才培养提供实战化培训工具；新一代智能网关项目基于公司原有的应用层网关产品技术基础开发网络层网关产品，升级网关产品以适应云计算、大数据、人工智能等新兴技术发展下日益复杂的应用环境；

本次车联网安全研发项目拟通过身份认证体系、车辆安全检测、靶场虚拟化技术、威胁情报获取和车载微流量技术的研发，凭借公司在网络信息安全领域成熟的产品技术将传统安全产品技术向车联网场景研发转化，形成完善的车联网安全产品体系，满足车联网网络安全需求，推动车联网产业链的建设完善。通过开展车联网安全关键技术研发和储备，为公司未来拓展车联网安全业务提前进行产品技术布局。

同时，本次募投项目中强调对研发项目的投入，募投项目的实施能够有效保障公司研发投入，储备科研资金，为公司的新产品及服务的研发和产业化实施提供必要的硬件设施与资金支持，为研发团队进行行业前沿研究提供更加优越的研发环境与条件，进一步提升研发在公司发展过程中的战略地位，促进公司科技创新水平提升。

综上所述，公司所处行业属于战略新兴行业，科技创新属性突出。公司在日常经营中积极开展研发工作，重视科技创新。本次募投项目紧密围绕公司主营业务开展，投向科技创新领域，待本次募集资金投资投产后，公司将实现业务板块的延伸和扩展，随着募投项目的实施及效益的产生，公司的技术盈利能力和经营业绩将进一步提升。

四、募集资金用于研发投入的情况

本项目的部分资金将用于公司新产品的研发项目，研发投入的主要内容为研发人员的薪酬费用，各募投项目的主要研发内容如下：

（一）数据安全岛平台研发及产业化项目

1、研发内容

数据安全岛平台研发及产业化项目的研发内容涉及安全计算沙箱技术、多方数据联合建模技术、数据主动销毁技术、用户实体行为分析（UEBA）技术、动态数据网关技术等。

2、研发预算及时间安排

本项目建设期 3 年，研发投入主要包括研发人员薪酬及包括认证费等在内的其他研发费用，具体如下：

项目	第 1 年	第 2 年	第 3 年	合计
研发预算（万元）	1,665.00	3,176.25	5,512.50	10,353.75

3、目前研发投入及进展、已取得及预计取得的研发成果等

截至本募集说明书出具日，本项目研发进展、已取得及预计取得的研发成果情况如下：

技术方向	主要研发内容	进展情况	已取得及预计取得的研发成果
数据智能分类分级技术	数据测绘、数据分级分类引擎等技术研究	已完成初代产品开发，处于稳定开发优化阶段	在数据安全岛平台中对纳入共享交换的数据，需要根据国家、行业和地方法规进行分级分类，并根据结果进行针对性开放共享。
数据动态脱敏技术	敏感数据识别、数据动态脱敏等技术研究	已完成初代产品开发，处于稳定开发优化阶段	在数据安全岛平台中对需要对开放的数据进行脱敏处理，避免敏感信息泄露，保障脱敏后数据的一致性和业务关联性。
安全计算沙箱技术	数据隔离、可信执行环境 TEE、操作监控和历史行为回放等技术研究	已完成初代产品开发，正在实现硬件层面的可信计算	在数据安全岛平台的安全可信计算场景中，利用安全计算沙箱，解决多方数据融合计算过程中遇到的任务干扰、数据干扰以及数据可能被窃取的风险，用户可基于大数据环境提交算法、程序和学习模型执行分析，可实现基于数据共享需求的安全、自由建模能力。
多方数据联合建模技术	差分隐私、联邦学习、同态加密等技	前沿技术已具有一定的研究	在数据安全岛平台中需要实现跨组织多方数据的联合建模应用，实现

技术方向	主要研发内容	进展情况	已取得及预计取得的研发成果
	术研究	积累，正在提升稳定性、可靠性和易用性，实现产品化	“数据出域”和“数据不出域”两种联合建模方式，解决多方数据联合建模过程的信任难题。
数据主动销毁技术	数据级联销毁、区块链等技术研究	处于稳定开发优化阶段	在数据安全岛平台的安全计算沙箱，需具备计算任务完成后，主动销毁沙箱内的明文数据，并利用区块链技术保存沙箱审计日志，保障数据主动销毁的可信度。
用户实体行为分析（UEBA）技术	用户行为数据治理、用户特征工程、用户异常归一化映射评分等技术研究	处于稳定开发优化阶段	在数据安全岛平台的账户行为动态鉴权场景中，实现在数据的使用过程中，动态分析账户行为是否异常，识别可能会造成数据泄露风险的高危人员，保障数据不被攻击者利用伪装身份使用。
动态数据网关技术	代码语法分析解析、环境识别、SOAR（安全编排、自动化及响应）等技术研究	处于稳定开发优化阶段	结合 UEBA 技术的分析结果，利用 SOAR 和动态阻断策略，对非法行为的动态阻断，以此保障数据的动态安全。

4、预计未来研发费用资本化的情况

本项目研发投入均计入费用化支出，不存在研发费用资本化的情况。

（二）涉网犯罪侦查打击服务平台研发及产业化项目

1、研发内容

涉网犯罪侦查打击服务平台研发及产业化项目的研发内容研发涉及网络空间测绘技术、大数据挖掘技术、侦查过程再造技术等。

2、研发预算及时间安排

本项目建设期 3 年，研发投入主要包括研发人员薪酬及包括认证费等在内的其他研发费用，具体如下：

项目	第 1 年	第 2 年	第 3 年	合计
研发预算（万元）	1,545.00	2,031.75	2,348.33	5,925.08

3、目前研发投入及进展、已取得及预计取得的研发成果等

截至本募集说明书出具日，本项目研发进展、已取得及预计取得的研发成果情况如下：

技术方向	主要研发内容	进展情况	已取得及预计取得的研发成果
网络空间测绘技术	用搜索引擎技术提供交互，让基层公安机关可以方便的搜索到网络空间上与涉网犯罪相关的情报。用多种测绘方法描述和标注网络位置，利用主动或被动探测的方法，跟踪网络空间上情报对象的状态和关系，对其进行画像。	技术预研阶段	作为涉网犯罪侦查打击的基础数据，是案件线索的主要来源，为案件侦查提供研判支撑，也是感知犯罪产业现状的基础。
大数据挖掘技术	基于网络层的特征、区域的特征、时间的特征、DNS 应答的特征、TTL 的特征、域名信息等，使用层次聚类、决策树和 ELM、SVM 和隐含马尔可夫模型、朴素贝叶斯、LSTM 决策树、X-Means″等各类算法，挖掘精准线索，提供预警支撑。	技术预研阶段	作为涉网犯罪侦查打击服务平台的核心能力，为嫌疑人画像、精准线索发现、案件研判、业态感知提供能力支撑。
侦查过程再造技术	实现协同研判、沙盘推演、辅助研判等联合作战功能，提供数据提取、APK 逆向分析等关键项的靶向分析	技术预研阶段	实现多警种协同作战，将不同警种的能力和数据以案件目标为载体进行聚焦，实现复杂目标的联合打击

4、预计未来研发费用资本化的情况

本项目研发投入均计入费用化支出，不存在研发费用资本化的情况。

（三）信创产品研发及产业化项目

1、研发内容

信创产品的研发重点在于国产化适配工作，目前公司现有网络安全基础产品和平台产品的国产化适配工作已按计划开展。本项目的研发项目涉及攻击识别、行为分析、流量分析、追踪溯源等关键技术研发。

2、研发预算及时间安排

本项目建设期 3 年，研发投入主要包括研发人员薪酬及包括认证费等在内的其他研发费用，具体如下：

项目	第 1 年	第 2 年	第 3 年	合计
研发预算（万元）	5,160.00	7,607.25	10,787.96	23,555.21

3、目前研发投入及进展、已取得及预计取得的研发成果等

截至本募集说明书出具日，本项目研发进展、已取得及预计取得的研发成果情况如下：

技术方向	主要研发内容	进展情况	已取得及预计取得的研发成果
攻击识别	攻击行为识别技术研究	已完成国产化迁移，处于测试优化阶段	对攻击产生的影响进行判定，形成完整的入侵分析，对各种来源的攻击行为进行确认和归类确保原始攻击行为有效性，进一步挖掘和攻击链分析，降低攻击分析难度、提升效率，快速发现异常入侵，提升安全响应能力。
行为分析	自动化行为分析与自验证技术研究	已完成国产化迁移，处于测试优化阶段	对各种来源的攻击行为进行确认和归类确保原始攻击行为有效性，进一步挖掘和攻击链分析，降低攻击分析难度、提升效率，快速发现异常入侵，提升安全响应能力。
流量分析	对实时网络流量分析的深度检测技术研究	已完成国产化迁移，处于测试优化阶段	借助网络流量分析和持续监控，使用沙箱技术、实时监测方法与系统等，监测提取异常行为。
追踪溯源	追踪溯源、攻击画像的分析技术研究	已部分完成国产化迁移，处于进一步调试阶段	通过行为识别和监测提取，进行安全专家分析和大数据分析，提供高价值的威胁情报信息及追踪溯源的线索，具有重要的现实意义。
实体画像与特征自动更新技术	对实体画像进行数据建模，结合业务实际的需求，找出相关的数据实体，以数据实体为中心规约数据维度类型和关联关系，形成符合业务实际情况的建模体系。	已部分完成国产化迁移，处于进一步调试阶段	应用于用户实体行为特征提取与分析模块，实现对实体行为特征的提取。
复杂网络的资产自动重识别技术	提出双栈协议识别技术实现不同网络环境的发送协议识别；提出地址归一化技术，实现将识别到的不同类型的地址解析归一化为相同的地址格式；通过构建外部资产地址库，以实现对不同资产的识别和	已部分完成国产化迁移，处于进一步调试阶段	应用于资产发现与管理模块，实现对复杂网络环境下，不同的日志传输方式、不同的传输协议以及不同的网络之间的资产识别。

技术方向	主要研发内容	进展情况	已取得及预计取得的研发成果
	归类		
面向对象的安全数据分层技术	采用“分层解耦”的设计理念，根据数据的流转方式，进行数据分层设计，各层之间采用集中的数据总线进行数据传输和交换，以此降低各类安全应用对底层数据存储之间的强依赖性	已部分完成国产化迁移，处于进一步调试阶段	应用于安全大数据中心，实现数据的分层分类存储，为业务功能模块提供数据支撑。
基于语义化安全日志聚类的异常行为检测技术	设计基于语义化分析的安全日志聚类模型，采用向量相似度计算算法，计算日志元素间的相似度，得到历史日志间的相似度之后，采用聚类算法对其进行分组计算，快速将日志分类	已部分完成国产化迁移，处于进一步调试阶段	应用于异常行为分析模型的建立，通过对系统异常行为的监测，可以发现未知的攻击模式。异常行为检测的关键在于建立正常使用模式并利用该模式对当前用户行为进行比较和判断。
基于知识图谱的网络攻击自动化关联推理技术	从资产、威胁和脆弱性三个方面进行网络空安全威胁建模技术研究，主要研究网络空间中安全威胁的行为特征、生成机理、攻击流程、危害效果等建模技术	已部分完成国产化迁移，处于进一步调试阶段	应用于威胁感知模块，实现从资产、拓扑、网络空间多方面的风险检测与感知。
安全管理	安全服务实例的管理与编排	已完成国产化迁移，处于测试优化阶段	在云安全管理平台上统一管理编排安全组件，实现安全组件的生命周期管理，兼容纳管第三方安全组件。
资产中心	资产管理与风险评估	已完成国产化迁移，处于测试优化阶段	实现对租户资产信息同步统一管理，一键下发安全检查任务，协助用户发现资产漏洞与安全威胁。
网络安全	安全能力评估与运营	已完成国产化迁移，处于测试优化阶段	借助运营平台分析评估租户整体安全状态，协助管理员评

技术方向	主要研发内容	进展情况	已取得及预计取得的研发成果
			估租户安全态势，分析租户安全缺陷。
操作系统安全	针对国产操作系统进行深度研究	处于稳定优化更新阶段	1、进行操作系统安全代码研究、内核安全测试、Oday 漏洞跟踪、SRC 应急响应中心建设； 2、操作系统安全状态研究、桌面、服务器病毒、木马攻击防护、主机 IDS 防御性研究； 3、APP 市场安全研究、APP 漏洞研究、沙箱安全研究、SDK 安全研究； 4、全生命周期安全响应流程适配研究、客户现场应急响应工作研究、安全取证、恢复研究； 5、安全管理流程闭环研究。
数据库、中间件、应用安全研究	针对国产数据库、中间件、各类应用进行安全研究	相关服务已投入市场，处于稳定优化阶段，并在监管、安全服务等业务展开多方合作	1、安全机制研究，开展程序自身安全保护机制、沙箱环境等研究； 2、0DAY 研究，积极展开安全厂商、应用软件之间的漏洞研究、修复、通告等机制； 3、安全生态研究，依托操作系统 SRC，形成操作系统、应用软件、安全厂商、监管机构安全生态闭环。
CPU 安全	针对各类国产 CPU 漏洞、加密技术的研究	处于稳定优化更新阶段	1、研究各类技术路线 CPU 可能具有的架构漏洞； 2、研究 CPU 集成硬件级安全芯片，与 CPU 厂商一同研究、开发安全芯片的操作系统级应用，研究安全整合方案。

4、预计未来研发费用资本化的情况

本项目研发投入均计入费用化支出，不存在研发费用资本化的情况。

（四）网络空间安全教育培训项目

1、研发内容

网络空间安全教育培训项目的研究内容包括网络安全靶场在内的网络安全演训产品及网络安全靶场云化部署的研发，研发项目涉及虚拟网络构建技术、多维网络互联技术、镜像资源管理技术、大规模虚拟节点快速部署技术、背景流量模拟技术、用户行为模拟技术、并行任务安全隔离技术、复杂网络下全量数据采

集技术等。

2、研发预算及时间安排

本项目建设期 3 年，研发投入主要包括研发人员薪酬及包括认证费等在内的其他研发费用，具体如下：

项目	第 1 年	第 2 年	第 3 年	合计
研发预算（万元）	1,330.00	1,837.50	2,353.84	5,521.34

3、目前研发投入及进展、已取得及预计取得的研发成果等

截至本募集说明书出具日，本项目研发进展、已取得及预计取得的研发成果情况如下：

技术方向	主要研发内容	进展情况	已取得及预计取得的研发成果
虚拟网络构建技术	软件定义网络、链路仿真、网络节点生成等技术研究	已完成预研，正处于产品开发阶段	在靶场平台的目标网络环境构建中，实现虚拟网络的构建
多维网络互联技术	虚实互联、多网互联接入等技术研究	技术预研阶段	在靶场平台中目标网络环境高逼真还原及大规模网络仿真中，实现非虚拟化网络的快速接入及多仿真场景快速互联，形成规模化网络
镜像资源管理技术	大规模镜像存储、跨网镜像高速传输等技术研究	技术预研阶段	在靶场平台的底层资源管理中，实现镜像资源多服务间快速的同步
大规模虚拟节点快速部署技术	虚拟节点、容器节点、离散事件节点在大规模构建情况下实现快速部署的技术研究	技术预研阶段	在靶场平台的目标网络靶标构建中，实现靶标资源的快速构建
背景流量模拟技术	真实流量录制、流量拼接、流量叠加、混合流量生成与回放等技术研究	技术预研阶段	在靶场平台的目标网络构建环境仿真中，实现场景真实流量状态还原
服务、应用、用户行为模拟技术	服务行为复制、用户行为复制、软件模拟、模型模拟、协议模拟及多行为协同模拟等技术研究	前期论证阶段	在靶场平台的目标网络构建环境仿真中，实现场景真实服务、应用及用户行为复现
并行任务安全隔离技术	并行任务网络隔离、数据隔离、软件隔离等技术研究	前期论证阶段	在靶场平台的实际使用过程中，当多个任务在靶场中进行的时候，要实现多个任务所对应的目标网络环境的隔离、多个任务各自采集的相关数据隔离以及整个过程中涉

技术方向	主要研发内容	进展情况	已取得及预计取得的研发成果
			及到的软件等相关资源隔离
复杂网络下全量数据采集技术	虚拟网络中流量采集、终端数据采集、全节点日志采集、可编辑数据采集、可插拔终端数据采集器等技术研究	技术预研阶段	在靶场平台的实际工作过程中，实现对靶场目标网络环境中的相关数据进行全量的采集
攻防数据分析技术	安全事件分析、用户行为分析、KillChain 分析、追踪溯源、安全态势等技术研究	前期论证阶段	在靶场平台的运行过程中和完成相关任务后，实现对靶场目标网络环境整体安全态势、整体任务过程、任务结果进行综合分析
半自动化攻击技术	半自动化攻击链构建技术研究	前期论证阶段	在进行攻防训练和演练的时候可以通过实现对目标环境的攻击及测试
安全评估技术	人员安全能力评估模型、设备安全评估模型设计与研究	技术预研阶段	在靶场平台的测试评估过程中对训练人员、被测试的设备和环境进行安全评估
异构虚拟化平台统一接入技术	异构虚拟化平台统一接入技术实现	已完成预研，正处于产品开发阶段	在靶场平台的节点生成中，实现对异构虚拟化平台快速适配

4、预计未来研发费用资本化的情况

本项目研发投入均计入费用化支出，不存在研发费用资本化的情况。

（五）新一代智能网关产品研发及产业化项目

1、研发内容

新一代智能网关产品研发及产业化项目的研发涉及矢量数据包转发技术、高性能报文分类匹配技术、入侵检测技术、防病毒技术、过滤技术、识别技术、联动技术和设备集中管控技术等。

2、研发预算及时间安排

本项目建设期 3 年，研发投入主要包括研发人员薪酬及包括认证费等在内的其他研发费用，具体如下：

项目	第 1 年	第 2 年	第 3 年	合计
研发预算（万元）	1,260.00	2,021.25	3,087.00	6,368.25

3、目前研发投入及进展、已取得及预计取得的研发成果等

截至本募集说明书出具日，本项目研发进展、已取得及预计取得的研发成果情况如下：

技术方向	主要研发内容	进展情况	已取得及预计取得的研发成果
矢量数据包转发技术	高性能接口 IO 技术，报文零拷贝、报文高速解码、报文转发处理流程、高性能表项创建、查询、老化等技术研究	已完成项目评审及立项，正处于开发阶段	在网关设备中提供高性能、可扩展的报文处理机制，为数据转发引擎提供一个高性能的处理框架
高性能的报文分类匹配技术	数据包分类算法、多域网络数据包分类算法等匹配算法研究	已完成项目评审及立项，正处于开发阶段	在网关中通过该技术的研究提供高性能的报文匹配性能，提供网关的多维度的访问控制能力，如防火墙策略、NAT 策略。
入侵检测技术	入侵检测规则、入侵检测算法等技术研究	已完成项目评审及立项，正处于开发阶段	为网关提供入侵防御能力
防病毒技术	流式病毒检测技术、启发式病毒检测技术以及基于 AI 的神经网络病毒库训练以及识别等技术研究	已完成项目评审及立项，正处于开发阶段	为网关提供防病毒检测能力
URL 过滤技术	URL 分类技术以及 URL 高速匹配技术研究	已完成项目评审及立项，正处于开发阶段	提供网关在 URL 分类上的访问控制能力
内容过滤技术	流量基于不同协议以及不用应用的内容解析和匹配技术研究	已完成项目评审及立项，正处于开发阶段	提供网关在传输内容上的访问控制能力
应用识别技术	应用特征库、流量应用识别检测等技术研究	已完成项目评审及立项，正处于开发阶段	提供网关在应用上的访问控制能力
用户识别技术	用户管理、用户认证、用户访问控制以及用户流量统计等技术研究	已完成项目评审及立项，正处于开发阶段	提供网关在用户上的访问控制能力
DDOS 识别技术	开发多种 DDOS 攻击检测算法识别各种不同的 DDOS 攻击行为	已完成项目评审及立项，正处于开发阶段	提供 DDOS 攻击识别检测能力
IPv4/v6 双栈技术	IPv4/v6 双栈、过渡技术（nat64、dslite 等）等协议栈技术研究，	已完成项目评审及立项，正处于开发阶段	提供网关在 IPv4/v6 网络上的网络适配能力以及在过渡阶段的过渡技术
VPN 技术	L2tp、GRE、SSLVPN、IPsecVPN 等 VPN 技术研究	已完成项目评审及立项，正处于开发阶段	提供网关的分支互联组网以及外网安全接入的能力
联动技术	与其它安全产品的联动技术研究，如堡垒机、扫描器以及 EDR 等	已完成项目评审及立项，正处于开发阶段	提供网关支持各种层次的防护能力方案的能力
设备集中管	设备的北向标准接口提	已完成项目评审及立	提供设备第三方集成能

技术方向	主要研发内容	进展情况	已取得及预计取得的研发成果
控技术	供监控、配置管理以及接入授权等技术研究	项，正处于开发阶段	力
威胁情报集成	集成安恒已有的数据大脑中的各种威胁情报数据，提高防护性能和防护准确性	已完成项目评审及立项，正处于开发阶段	提高安全防护检测能力
机器学习引擎	实现对流量、应用、文件、防护策略等多维度的机器建模，通过机器学习实现智能基线防护	已完成项目评审及立项，正处于开发阶段	提高安全防护检测能力
文件沙箱检测	集成沙箱检测能力，实现对文件的深度检测	已完成项目评审及立项，正处于开发阶段	提高安全防护检测能力
多安全防护平台集成	实现与运维网关、数据库安全防护网关、数据安全防护平台、EDR、态势感知、大数据智能分析平台等的集成	已完成项目评审及立项，正处于开发阶段	提供多种安全平台防护能力的无缝标准整合，提高安全防护检测能力
国产多硬件平台支持	解决多种国产化硬件平台的低成本支持，降低转发平面、安全检测防护引擎对硬件和内核等的过渡依赖	已完成项目评审及立项，正处于开发阶段	实现低成本支持多种硬件平台
云化支持	实现与硬件的解耦，便于通过与多云管理平台的集成，实现快速对多云环境的支持	已完成项目评审及立项，正处于开发阶段	提供多云快速云化部署能力
SSL 加速卡	实现对网络层加密流量的硬件加解密	已完成项目评审及立项，正处于开发阶段	提供加密流量的高性能加解密，提高整体防护性能
FPGA	解决部分基于正则表达式等特征策略的安全引擎靠 CPU 检测防护性能较低的问题，部分引擎移植到 FPGA 里面实现硬件层面快速高性能安全防护检测	已完成项目评审及立项，正处于开发阶段	提高安全引擎检测性能

4、预计未来研发费用资本化的情况

本项目研发投入均计入费用化支出，不存在研发费用资本化的情况。

（六）车联网安全研发中心建设项目

1、研发内容

车联网安全研发中心建设项目的研发涉及身份认证体系、车辆安全检测、靶场虚拟化技术、安全芯片应用、威胁情报获取和车载微流量监测技术等。

2、研发预算及时间安排

本项目建设期 3 年，研发投入主要包括研发人员薪酬及包括认证费等在内的其他研发费用，具体如下：

项目	第 1 年	第 2 年	第 3 年	合计
研发预算（万元）	1,400.00	2,756.25	4,630.50	8,786.75

3、目前研发投入及进展、已取得及预计取得的研发成果等

截至本募集说明书出具日，本项目研发进展、已取得及预计取得的研发成果情况如下：

技术方向	主要研发内容	进展情况	已取得及预计取得的研发成果
身份认证体系应用	国密算法加密、车辆身份标示、数字证书、密钥管理、快速认证。	已完成初代产品开发，处于稳定开发优化阶段	在车联网身份认证及密钥管理平台中能对路边单元设备、智能网联汽车、TSP 云平台、移动手持设备等颁发唯一有效的许可证书，便于身份认证。
数据传输加密	数据传输加密算法及实现	技术预研阶段	在身份认证中提供可信支撑同时也为 V2X 环境下的数据交互提供保障
车辆安全检测	对于车辆软件、固件的安全分析及检测	已完成初代产品开发，处于稳定开发优化阶段	形成专业化的检测能力与服务，为客户提供车辆安全检测的能力
车辆安全检测工具	将车辆安全检测能力进行固化、工具化	技术预研阶段	形成车辆安全检测的一体化工具，为车辆安全风险的高效检测提供专业支撑
安全芯片应用(车端的身份认证)	基于安全芯片的密钥管理，身份认证	已完成初代产品开发，处于市场接触优化阶段	秘钥管理，证书申请下载，boot 启动，校验，OTA 安全升级等安全功能
安全芯片应用(车路协同)	定制化密钥管理，身份认证，签名验签	已完成初代产品开发，处于市场接触优化阶段	OBU，RSU 和边缘设备上的可信任链建立，安全认证
安全芯片应用(入侵防护)	基于安全芯片的入侵防护技术，bootload 安全验证。	已完成技术预研，处于产品开发阶段	为车辆提供芯片级的入侵检测以及安全防护能力，硬件安全隔离
辅助驾驶系统安全模块	对于辅助驾驶系统中的关键输出指令数据进行模型分析	技术预研阶段	保障辅助驾驶系统的业务安全，信息安全，防止被网络攻击，确保车辆正常行驶
靶场虚拟化技术	将汽车应用场景进行虚拟化靶场搭建，形成可操作的高仿真靶场实验室	技术预研阶段	作为和高校间搭建联合实训教学靶场的技术基础，人才培养
威胁情报	对于网络中的车联	相关产品已投入市场，处于	将获取到的情报信息整合

技术方向	主要研发内容	进展情况	已取得及预计取得的研发成果
分析平台	网相关的情报信息获取	稳定开发优化阶段	后可以为客户或者是其他智慧交通类平台提供情报支撑
车载微流量监测技术	车内模块报文捕获、解析	已完成技术预研，处于产品开发阶段	为车辆入侵检测系统提供数据来源，数据入口
车辆安全风险检测能力	对于车内的报文指令信息进行分析，输出安全规则	已完成初代产品开发，处于稳定开发优化阶段	为车辆入侵检测系统提供专业的安全规则，策略指令

4、预计未来研发费用资本化的情况

本项目研发投入均计入费用化支出，不存在研发费用资本化的情况。

（七）公司研发项目的技术可行性

1、强大的研发团队

公司一直以来注重人才引进及培养，通过完善的激励机制为员工实现自身价值提供条件，打造了一套稳定的经营团队以及与公司发展相匹配的人才结构。截至 2020 年 9 月 30 日，公司及子公司共有 2,644 名员工，其中研发人员 869 名，占在职员工总数的 32.87%。经过多年积累和发展，公司形成了以核心技术人员为首的多个强有力的研发团队。公司的核心技术人员均具有丰富的行业经验与扎实的专业知识，掌握着网络安全领域的关键技术，是公司技术水平持续提升的重要驱动力量。公司将继续坚持内部培养和外部引进相结合的人才制度，完善员工培训机制，并根据公司战略发展规划调整人力制度，提高团队素质，激发人才活力。

2、深厚的技术积累

公司自创立以来始终坚持持续技术创新的发展战略，紧跟网络信息安全技术发展趋势和用户需求，不断在行业内率先推出创新产品，更新迭代既有产品和解决方案，并孵化培育新产品。经过多年发展，公司拥有美国软件工程学会颁发的 CMMI5 权威认证，在软件开发过程的改善能力、质量管理水平、软件开发的整体成熟度居于行业前列，并掌握了应用安全与数据安全等领域的重要核心技术，形成一系列具有自主知识产权的技术成果。截至 2020 年 9 月 30 日，公司拥有超过 130 项已获授权的专利，并掌握 48 项核心技术，涉及攻防研究、应急响应、

安全咨询、漏洞研究、产品研发等各个领域。

公司技术研发实力得到国家相关部门的肯定和支持，公司现已承担“国家发改委信息安全专项”、“工信部电子发展基金项目”、“科技部火炬计划”、“科技部网络空间重点专项”、“浙江省重点科技专项”等多项国家级、省市级科技计划项目，并作为主要起草单位参与多项网络信息安全领域国家及行业相关技术标准的制定，积极引领技术标准在网络信息安全产品的落地工作。

3、丰富的实施经验

公司在网络信息安全行业耕耘数十载，已成为网络信息安全领域的领先品牌，多次入选全球网络安全创新 500 强，曾先后为 2008 年北京奥运会、上海世博会、广州亚运会、连续五届世界互联网大会乌镇峰会、G20 杭州峰会、厦门金砖会议、青岛上合峰会、上海国际进口博览会、2018 第 14 届 FINA 世界游泳锦标赛等众多重大活动提供网络信息安全保障。目前，公司产品及服务已经进入了包括运营商、政府、能源、金融、教育、医疗等在内的众多行业，积累了大量优质客户，并长期保持着深入稳定的合作关系，有利于公司在满足客户信息化业务的发展规划及建设过程的同时，动态把握客户对于信息化建设的技术需求及发展趋势，保障公司产品、解决方案及服务的竞争力。

综上所述，公司本次研发项目在人员、技术、市场等方面均具有良好基础。随着研发项目的开展，公司将进一步丰富人员、技术、市场等方面的储备，确保研发项目的顺利实施。

第四节　董事会关于本次发行对公司影响的讨论与分析

一、本次发行后公司业务及资产的变动或整合计划

本次发行完成后，公司不存在较大的业务和资产的整合计划，本次发行均围绕公司现有主营业务展开，公司业务结构不会产生较大变化，公司的盈利能力将有所提升，主营业务将进一步加强。

二、本次发行后，上市公司科研创新能力的变化

本次募投项目紧密围绕公司主营业务开展，投向科技创新领域，募投项目的实施有利于促进公司科技创新水平的提升。待本次募集资金投资投产后，公司将实现业务板块的延伸和扩展，随着募投项目的实施及效益的产生，公司的技术能力和经营业绩将进一步提升。

三、本次发行后，上市公司控制权结构的变化

本次发行前，公司的控股股东、实际控制人为范渊，截至 2020 年 9 月 30 日，其直接持有公司 10,018,362 股股份，占公司总股本的 13.52%，并通过与员工持股平台嘉兴安恒、宁波安恒的《一致行动协议》，合计控制安恒信息 27.02%的表决权。

本次发行的发行数量不超过本次发行前公司总股本的 30%，即不超过 22,222,222 股（含本数），本次发行完成后公司的总股本不超过 96,296,297 股（含本数）。按发行数量 22,222,222 股上限测算，本次发行完成后，控股股东及实际控制人范渊可实际控制的表决权约占公司总股本的 20.79%，仍保持实际控制人的地位。本次发行不会导致公司控股股东和实际控制人发生变更。

四、本次发行后，上市公司与发行对象及发行对象的控股股东和实际控制人从事的业务存在同业竞争或潜在同业竞争的情况

截至本募集说明书出具日，本次发行尚未确定具体发行对象，上市公司与发行对象及发行对象的控股股东和实际控制人从事的业务是否存在同业竞争或潜在的同业竞争，将在发行结束后公告的发行情况报告书中披露。

五、本次发行完成后，上市公司与发行对象及发行对象的控股股东和实际控制人可能存在的关联交易的情况

截至本募集说明书出具日，本次发行尚未确定具体发行对象，上市公司与发行对象及发行对象的控股股东和实际控制人从事的业务是否存在关联交易或潜在的关联交易，将在发行结束后公告的发行情况报告书中披露。公司将严格按照中国证监会、证券交易所关于上市公司关联交易的规章、规则和政策，确保上市公司依法运作，保护上市公司及其他股东权益不会因此而受影响。本次发行将严格按规定程序由上市公司董事会、股东大会进行审议，进行及时完整的信息披露。

第五节　与本次发行相关的风险因素

投资者在评价公司本次向特定对象发行股票时，除本募集说明书提供的其他各项资料外，应特别认真考虑下述各项风险因素：

一、对公司核心竞争力、经营稳定性及未来发展可能产生重大不利影响的因素

（一）技术风险

1、技术迭代风险

公司的核心技术主要应用于网络信息安全行业。随着信息技术的高速发展，网络信息安全领域的技术也伴随着处于快速成长期，应用的发展趋势表现为从搭载硬件的安全软件到提供云化网络信息安全保护、从传统数据保护到大数据保护、从互联网信息安全为主战场到物联网信息安全受到普遍重视、从分别提供安全软件和服务到提供整体安全解决方案等。进入该技术领域并将技术产业化需要长时间的研发积累和大量客户案例实践，技术壁垒和进入门槛较高。

如公司不能准确及时地预测和把握网络信息安全技术的发展趋势，对技术研究的路线做出合理安排或转型，在基础研究与市场应用上形成快速互动与良性循环，持续保持本公司技术领先优势，将可能会延缓本公司在关键技术和关键应用上实现突破的进度，导致本公司面临被竞争对手赶超，或者核心技术发展停滞甚至被替代的风险。

2、技术研发失败风险

网络信息安全行业是技术密集型行业。为保持市场领先优势，提升技术实力和核心竞争力，公司需要不断进行新技术创新、新产品研发，以应对终端客户日益增长的多样化需求。最近三年，公司的研发费用分别为 9,592.94 万元、15,195.19 万元和 20,453.95 万元，占营业收入的比重分别为 22.29%、24.25%和 21.67%。发生的研发费用直接影响公司当年的净利润水平。由于对未来市场发展趋势的预测存在一定不确定性，公司可能面临新技术、新产品研发失败的风险，从而对公司经营业绩和持续经营带来不利的影响。

3、核心技术人员流失风险

经过多年积累和发展，公司形成了以核心技术人员为首的多个强有力的研发团队。核心技术人员是公司的核心竞争力及未来持续发展的基础。随着行业竞争日趋激烈，企业对人才的竞争不断加剧。能否维持技术人员队伍的稳定，并不断吸引优秀技术人员加盟，关系到公司能否继续保持技术竞争优势和未来发展的潜力。如果公司核心技术人员大量流失，则可能造成在研项目进度推迟、甚至终止，或者造成研发项目泄密或流失，给公司后续新产品的开发以及持续稳定增长带来不利影响。

（二）经营风险

1、市场竞争加剧的风险

我国网络信息安全行业市场空间已颇具规模，多年来保持了快速增长态势。市场机遇也吸引了较多参与者，市场竞争较为激烈。目前国内网络信息安全行业厂商众多，主营业务涵盖在网络信息安全的物理安全、网络安全、系统安全、应用安全、数据安全等多个细分领域中。未来，随着网络信息安全市场空间进一步拓展，公司与行业内具有技术、品牌、人才和资金优势的厂商（如绿盟科技、启明星辰等）之间的竞争可能进一步加剧。

2、用户拓展失败的风险

网络信息安全危机事件频发，企业和社会民众对网络信息安全愈加重视，同时国家加强了政策对行业发展的引导和推动，行业下游客户范围逐步由政府（含公安）、金融机构、教育机构、电信运营商等单位向其他中小型企业覆盖，客户的需求也由产品需求增加了服务需求。公司目前客户群体主要集中在政府（含公安）、金融机构、教育机构、电信运营商等单位。公司计划加大营销网络建设方面的投入，建立多级销售渠道，以不断拓展中小企业客户，推广标准化网络信息安全产品，同时服务现有客户软件升级和新增业务的需要。但若公司的新行业拓展策略、营销服务等不能很好的适应并引导客户需求，公司将面临新行业市场开拓风险。

3、经营业绩季节性波动引起股价波动风险

公司报告期历年上半年营业收入较低，而下半年（特别是第四季度）营业收

入较高，存在较为明显的季节性特征。

最近三年，公司营业收入按前三季度/四季度分布情况如下：

单位：万元

项目	2019 年度		2018 年度		2017 年度	
	金额	比例	金额	比例	金额	比例
前三季度	47,119.85	49.91%	31,042.77	49.54%	22,004.57	51.13%
第四季度	47,283.44	50.09%	31,615.90	50.46%	21,035.25	48.87%

受政府部门和大型企事业的采购周期影响，这些用户大多在上半年对全年的投资和采购进行规划，下半年再进行项目招标、项目验收和项目结算。同时，由于软件企业员工工资性支出、固定资产摊销等成本所占比重较高，造成公司净利润的季节性波动比营业收入的季节性波动更为明显。因此，公司经营业绩存在季节性波动引起股价波动风险。

4、渠道商管理不善风险

报告期内，公司销售实行渠道加直销的销售模式，2017-2019 年度公司的渠道销售收入占主营业务收入的比重分别为 55.16%、55.93%和 58.26%，呈稳定上升趋势。公司产品具有客户集中度较低（2019 年前五大客户销售额占营业收入比为 15.59%，2020 年 1-9 月前五大客户销售额占营业收入比为 14.87%）、产品的目标用户数多、用户的地域及行业分布广的特点。随着未来公司经营规模的继续扩大，渠道管理的难度也将加大，若公司不能及时提高渠道管理能力，可能对公司品牌和产品销售造成不利影响。

5、因最终客户发生数据泄密及其他网络安全事件时，公司承担罚款或赔偿的风险

当最终客户发生数据泄密及其他网络安全事件时，如主管部门认定公司在提供相应产品或服务时违反了国家与网络安全和信息安全相关的法律法规，公司可能承担相应的法律责任，并可能需根据销售合同的约定向客户承担相应的赔偿责任，从而给公司的经营带来一定风险。

（三）行业风险

我国网络信息安全行业多年来保持了快速增长态势。市场机遇吸引了较多参

与者，市场竞争较为激烈。未来，随着网络信息安全行业的发展，不同细分领域的技术将会融合、协同，不同细分市场客户的需求将会交叉、重叠，不同细分行业的领先者将展开直接竞争，行业的发展对公司提供整体解决方案的能力将提出更高的要求，公司与行业内具有技术、品牌、人才和资金优势的厂商之间的竞争可能进一步加剧，行业内目前的主要参与者也将面临具有新一代信息技术优势的企业可能进入网络信息安全行业的潜在竞争，行业整体竞争加剧可能影响行业总体毛利率，从而导致公司毛利率存在下降的风险。

同时，公司所处的信息安全行业未来保持快速发展的趋势基于目前国家政策取向、全球信息安全形势和未来技术发展方向，这些因素共同推动我国政府和企业不断增加对信息安全产品和服务的购买。一旦外部因素发生重大变化，或者政府和企业的购买偏好发生变化，就可能会导致信息安全行业发展不及预期，进而影响公司业绩。

（四）法律风险

1、相关业务和产品资质证书续期或办理风险

网络信息安全及网络设备厂商从事研发、生产、销售和提供安全服务等经营活动，通常需取得计算机信息系统安全专用产品销售许可证等产品认证，并具备网络信息安全服务资质等业务资质。截至本募集说明书出具日，公司拥有 IT 产品信息安全产品认证证书、中国国家信息安全产品认证证书、信息技术产品安全测评证书、计算机信息系统安全专用产品销售许可证、信息安全服务资质认证证书、中国通信企业协会通信网络安全服务能力评定证书、信息安全等级保护安全建设服务机构能力评估合格证书等信息安全行业的主要产品和服务资质证书。虽然公司内部有专人负责产品和服务认证的申请、取得和维护，且未曾出现过已取得认证或资质被取消的情况，但如果未来国家关于产品和服务认证的政策或标准出现重大变化，公司无法为过期证书续证，产品和服务存在不能获得相关认证的风险。

（五）财务风险

1、应收账款大幅增加未来发生坏账的风险

截至 2020 年 9 月 30 日，公司应收账款账面价值为 23,936.79 万元，占资产

总额 11.91%。2019 年末应收账款余额较 2018 年末应收账款余额增加 19.26%，2018 年末应收账款余额较 2017 年末应收账款余额增长 52.46%。

随着业务规模的不断增长，公司每年实现销售的客户数量逐年扩大、市场区域不断扩大、客户类型继续增加，公司对客户的信用管理难度将增大，未来坏账风险可能增加。

（六）政策风险

1、税收优惠依赖风险

报告期内，公司享受的主要税收优惠政策包括：一是公司销售自主开发的软件产品增值税实际税负超过 3%的部分实行即征即退政策，二是公司作为国家规划布局内重点软件企业享受企业所得税 10%的优惠税率。

公司享受的税收优惠均与公司日常经营相关，具有一定的稳定性和持续性。2017-2019 年度公司实现收入 43,039.81 万元、62,658.68 万元及 94,403.29 万元，随着销售规模的快速增长，公司享受的税收优惠金额也逐步增加。

如果公司未来不能持续保持较强的盈利能力或者国家税收政策发生变动，则可能对公司利润水平产生一定的影响。

2、财政补贴变化产生的风险

报告期内，政府一直重视高新技术企业，并给予重点鼓励和扶持。报告期内，公司除增值税退税外政府补助收入分别为 1,508.04 万元、1,554.28 万元、1,507.60 万元及 1,543.11 万元。补助项目包括安恒信息智慧安全云省级重点企业研究院项目补助资金等。如果政府对公司所处行业及高新技术企业的扶持政策发生变化，将对公司的发展产生一定的影响。

（七）新冠肺炎疫情带来的风险

自 2020 年初新冠肺炎疫情发生以来，受经济活动减弱、人口流动减少或延后、企业大范围停工停产等因素的影响，公司业务受到一定程度的冲击，2020 年度上半年业绩增速较过往年度相比有所放缓。随着疫情情况得到基本控制，公司各项经营活动已基本恢复正常。但如果此次疫情发展趋势发生重大不利变化，或者在后续经营中再次遇到重大疫情、自然灾害或极端恶劣天气的影响，则可能

对公司的日常经营和本次募投项目的实施造成不利影响。

二、可能导致本次发行失败或募集资金不足的因素

（一）审批风险

本次发行尚需满足多项条件方可完成，包括但不限于公司股东大会批准本次发行、上海证券交易所审核通过并获得中国证监会注册等。本次发行能否获得上述批准或注册，以及获得相关批准或注册的时间均存在不确定性，提请广大投资者注意投资风险。

（二）发行风险

本次发行的发行对象为不超过 35 名（含 35 名）的特定对象，且最终根据竞价结果与本次发行的保荐机构（主承销商）协商确定，发行价格不低于定价基准日（即发行期首日）前二十个交易日公司 A 股股票交易均价的百分之八十。

本次发行的发行结果将受到宏观经济和行业发展情况、证券市场整体情况、公司股票价格走势、投资者对本次发行方案的认可程度等多种内外部因素的影响。

因此，本次发行存在发行募集资金不足甚至无法成功实施的风险

三、对本次募投项目的实施过程或实施效果可能产生重大不利影响的因素

（一）募集资金投资项目实施的风险

公司按照自身战略规划，围绕数据安全、涉网犯罪侦查打击、信创产业化、网络安全培训、新一代智能网关及车联网安全等方向设立募投项目，在现有网络信息安全产品及服务体系基础上进一步升级和拓展。公司已就本次拟实施募投项目进行了充分的市场调研和严格的可行性论证，并与部分客户签订意向订单或战略合作协议。但是由于本次拟募集资金投资项目涉及公司新晋研发方向，在后续研发过程中有可能出现一些不可控因素或目前技术条件下尚不能解决的技术问题，导致研发进度不及预期或失败。同时，网络安全行业景气度受国家产业政策、政府宏观调控影响较大，若上述因素出现不可预见的负面变化，将对募投项目的效益实现产生较大影响。基于上述情况，本次募投项目存在无法及时、充分实施

或难以达到预期经济效益的风险。

（二）募投项目无法达到预期收益的风险

公司募集资金项目的可行性研究是基于当前经济形势、行业发展趋势、未来市场需求预测、公司技术研发能力等因素提出，公司经审慎测算后认为本次募集投资项目预期经济效益良好。但是考虑未来的经济形势、行业发展趋势、市场竞争环境等存在不确定性，以及项目实施风险（成本增加、进度延迟、募集资金不能及时到位等）和人员工资可能上升等因素，有可能导致募集资金投资项目的实际效益不及预期。

第六节　与本次发行有关的声明

一、发行人及全体董事、监事、高级管理人员声明（一）

本公司及全体董事、监事、高级管理人员承诺本募集说明书内容真实、准确、完整，不存在虚假记载、误导性陈述或重大遗漏，按照诚信原则履行承诺，并承担相应的法律责任。

公司董事：

范渊	张小孟	吴卓群
姜有为	陈英杰	袁明坤
辛金国	朱伟军	赵新建

杭州安恒信息技术股份有限公司

2021 年 4 月 8 日

第六节　与本次发行有关的声明

一、发行人及全体董事、监事、高级管理人员声明（一）

本公司及全体董事、监事、高级管理人员承诺本募集说明书内容真实、准确、完整，不存在虚假记载、误导性陈述或重大遗漏，按照诚信原则履行承诺，并承担相应的法律责任。

公司董事：

范渊	张小孟	吴卓群
姜有为	陈英杰	袁明坤
辛金国	朱伟军	赵新建

杭州安恒信息技术股份有限公司

2021 年 6 月 8 日

第六节　与本次发行有关的声明

一、发行人及全体董事、监事、高级管理人员声明（一）

本公司及全体董事、监事、高级管理人员承诺本募集说明书内容真实、准确、完整，不存在虚假记载、误导性陈述或重大遗漏，按照诚信原则履行承诺，并承担相应的法律责任。

公司董事：

范渊	张小孟	吴卓群
姜有为	陈英杰	袁明坤
辛金国	朱伟军	赵新建

杭州安恒信息技术股份有限公司

2021 年 4 月 8 日

第六节　与本次发行有关的声明

一、发行人及全体董事、监事、高级管理人员声明（一）

本公司及全体董事、监事、高级管理人员承诺本募集说明书内容真实、准确、完整，不存在虚假记载、误导性陈述或重大遗漏，按照诚信原则履行承诺，并承担相应的法律责任。

公司董事：

范渊	张小孟	吴卓群
姜有为	陈英杰	袁明坤
辛金国	朱伟军	赵新建

杭州安恒信息技术股份有限公司

2021 年 4 月 8 日

第六节　与本次发行有关的声明

一、发行人及全体董事、监事、高级管理人员声明（一）

本公司及全体董事、监事、高级管理人员承诺本募集说明书内容真实、准确、完整，不存在虚假记载、误导性陈述或重大遗漏，按照诚信原则履行承诺，并承担相应的法律责任。

公司董事：

范渊	张小孟	吴卓群
姜有为	陈英杰	袁明坤
辛金国	朱伟军	赵新建

杭州安恒信息技术股份有限公司

2021 年 4 月 8 日

第六节　与本次发行有关的声明

一、发行人及全体董事、监事、高级管理人员声明（一）

本公司及全体董事、监事、高级管理人员承诺本募集说明书内容真实、准确、完整，不存在虚假记载、误导性陈述或重大遗漏，按照诚信原则履行承诺，并承担相应的法律责任。

公司董事：

范渊	张小孟	吴卓群
姜有为	陈英杰	袁明坤
辛金国	朱伟军	赵新建

杭州安恒信息技术股份有限公司

2021 年 4 月 8 日

一、发行人及全体董事、监事、高级管理人员声明（二）

本公司及全体董事、监事、高级管理人员承诺本募集说明书内容真实、准确、完整，不存在虚假记载、误导性陈述或重大遗漏，按照诚信原则履行承诺，并承担相应的法律责任。

公司监事：

冯旭杭	郑赳	王欣

杭州安恒信息技术股份有限公司

2021 年 4 月 8 日

一、发行人及全体董事、监事、高级管理人员声明（三）

本公司及全体董事、监事、高级管理人员承诺本募集说明书内容真实、准确、完整，不存在虚假记载、误导性陈述或重大遗漏，按照诚信原则履行承诺，并承担相应的法律责任。

公司非董事高级管理人员签名：

黄进	楼晶	戴永远

杭州安恒信息技术股份有限公司

2021 年 4 月 8 日

二、发行人控股股东、实际控制人声明

本人承诺本募集说明书内容真实、准确、完整，不存在虚假记载、误导性陈述或重大遗漏，按照诚信原则履行承诺，并承担相应的法律责任。

控股股东及实际控制人：

范渊

杭州安恒信息技术股份有限公司

2021 年 4 月 8 日

三、保荐机构（主承销商）声明

（一）保荐机构（主承销商）声明

本公司已对募集说明书进行了核查，确认本募集说明书内容真实、准确、完整，不存在虚假记载、误导性陈述或重大遗漏，并承担相应的法律责任。

项目协办人：

陈泽森

保荐代表人：

杨佳佳　　水耀东

法定代表人：

贺青

国泰君安证券股份有限公司

2021 年 4 月 8 日

（二）保荐机构董事长、总经理声明

本人已认真阅读杭州安恒信息技术股份有限公司募集说明书的全部内容，确认募集说明书不存在虚假记载、误导性陈述或者重大遗漏，并对募集说明书真实性、准确性、完整性、及时性承担相应法律责任。

总经理（总裁）：

王 松

董事长：

贺 青

国泰君安证券股份有限公司

2021 年 4 月 8 日

四、发行人律师声明

本所及经办律师已阅读《杭州安恒信息技术股份有限公司 2020 年度向特定对象发行 A 股股票募集说明书》，确认募集说明书内容与本所出具的法律意见书不存在矛盾。本所及经办律师对发行人在募集说明书中引用的法律意见书的内容无异议，确认募集说明书不因引用上述内容而出现虚假记载、误导性陈述或重大遗漏，并承担相应的法律责任。

经办律师：

徐旭青　　刘　莹

律师事务所负责人：

颜华荣

国浩律师（杭州）事务所（盖章）

2021 年　4 月　8 日

审计机构声明

本所及签字注册会计师已阅读募集说明书，确认募集说明书内容与本所出具的审计报告等文件不存在矛盾。本所及签字注册会计师对发行人在募集说明书中引用的审计报告等文件的内容无异议，确认募集说明书不因引用上述内容而出现虚假记载、误导性陈述或重大遗漏，并承担相应的法律责任。

签字注册会计师：

魏琴　　陈瑜

会计师事务所负责人：

杨志国

立信会计师事务所（特殊普通合伙）

2021 年 4 月 8 日

六、董事会声明与承诺

（一）关于公司未来十二个月内再融资计划的声明

除本次发行外，在未来十二个月内，公司董事会将根据公司资本结构、业务发展情况，考虑公司的融资需求以及资本市场发展情况综合确定是否安排其他股权融资计划，并按照相关法律法规履行相关审议程序和信息披露义务。

（二）关于本次向特定对象发行股票摊薄即期回报的风险提示及拟采取的填补措施

1、公司应对本次发行摊薄即期回报采取的措施

本次向特定对象发行股票可能导致投资者的即期回报有所下降，公司拟通过多种措施防范即期回报被摊薄的风险，以填补股东回报，充分保护中小股东利益，实现公司的可持续发展、增强公司持续回报能力。具体措施如下：

（1）聚焦公司主营业务，提高公司持续盈利能力

本次发行的募集资金投资项目紧密围绕公司主营业务，募集资金使用计划已经管理层、董事会的详细论证，符合行业发展趋势和公司发展规划。本次募投项目的实施有利于进一步提升公司核心竞争力和可持续发展能力。

（2）加快募投项目建设，推动募投项目效益实现

公司本次发行股票募集资金的募投项目紧紧围绕公司主营业务，有利于扩大公司整体规模、扩大市场份额，增强公司资金实力，进一步提升公司核心竞争力和可持续发展能力，有利于实现并维护股东的长远利益。

本次募集资金到位后，公司将根据募集资金管理相关规定，严格管理募集资金的使用，保证募集资金按照原方案有效利用。向特定对象发行股票公司将加快推进募集资金投资项目实施，推动募投项目效益实现，从而降低本次发行对股东即期回报摊薄的风险。

（3）加强募集资金管理，提高募集资金使用效率

公司将严格按照《上市公司监管指引 2 号—上市公司募集资金管理和使用的监管要求》、《上海证券交易所科创板股票上市规则》及公司《募集资金管理制度》的有关规定，规范募集资金使用，保证募集资金充分有效利用。公司董事会将持续监督对募集资金进行专户存储、保障募集资金用于规定的用途、配合保荐机构

等对募集资金使用的检查和监督，以保证募集资金合理规范使用，防范募集资金使用风险，提高募集资金使用效率。

（4）完善公司治理，为公司发展提供制度保障

公司将严格遵循《中华人民共和国公司法》、《中华人民共和国证券法》、《上市公司治理准则》等法律、法规和规范性文件的要求，不断完善公司治理结构，确保股东能够充分行使权利，确保董事会能够按照法律、法规和公司章程的规定行使职权、做出科学、迅速和谨慎的决策，确保独立董事能够认真履行职责，维护公司整体利益，尤其是中小股东的合法权益，确保监事会能够独立有效地行使对董事、经理和其他高级管理人员及公司财务的监督权和检查权，为公司发展提供制度保障。

（5）优化公司投资回报机制，强化投资者回报机制

公司将持续根据国务院《关于进一步加强资本市场中小投资者合法权益保护工作的意见》、中国证监会《关于进一步落实上市公司现金分红有关事项的通知》和《上市公司监管指引第 3 号—上市公司现金分红》的有关要求，严格执行《公司章程》明确的现金分红政策，在公司主营业务健康发展的过程中，给予投资者持续稳定的回报。同时，公司将根据外部环境变化及自身经营活动需求，综合考虑中小股东的利益，对现有的利润分配制度及现金分红政策及时进行完善，以强化投资者回报机制，保障中小股东的利益。

公司提醒投资者，以上填补回报措施不等于对公司未来利润做出保证。投资者不应据此进行投资决策，投资者据此进行投资决策造成损失的，公司不承担赔偿责任。

2、董事、高级管理人员关于向特定对象发行股票摊薄即期回报采取填补措施的承诺

根据《国务院办公厅关于进一步加强资本市场中小投资者合法权益保护工作的意见》（国办发[2013]110 号）、《国务院关于进一步促进资本市场健康发展的若干意见》（国发[2014]17 号）以及中国证监会发布的《关于首发及再融资、重大资产重组摊薄即期回报有关事项的指导意见》（中国证监会公告[2015]31 号）等法律、法规和规范性文件的相关要求，为确保公司 2020 年度向特定对象发行股票摊薄即期回报采取的填补回报措施能够得到切实履行，公司全体董事及高级管

理人员承诺如下：

“1、不无偿或以不公平条件向其他单位或者个人输送利益，也不采用其他方式损害公司利益。

2、对本人的职务消费行为进行约束，全力支持及配合公司对董事及高级管理人员职务消费行为的规范，严格遵守及执行公司该等制度及规定。

3、不动用公司资产从事与本人所履行职责无关的投资、消费活动。

4、全力支持公司董事会或薪酬与考核委员会在制定及/或修订薪酬制度时，将相关薪酬制度与公司填补回报措施的执行情况挂钩，并在公司董事会或股东大会审议该薪酬制度议案时投赞成票（如有投票/表决权）。

5、若公司后续推出或实施股权激励政策，全力支持公司将拟公布的公司股权激励的行权条件与公司填补回报措施的执行情况相挂钩，并在公司董事会或股东大会审议相关议案时投赞成票（如有投票/表决权）。

6、本承诺函出具后，若中国证监会、上海证券交易所等监管机构作出关于填补回报措施及其承诺的其他新的监管规定，且上述承诺不能满足监管机构该等规定时，本人届时将按照监管机构的最新规定出具补充承诺。

7、切实履行公司制定的有关填补回报措施以及对此作出的任何有关填补回报措施的承诺，若违反该等承诺并给公司或者投资者造成损失的，本人愿意依法承担对公司或者投资者的补偿责任。

本人若违反上述承诺或拒不履行上述承诺，本人同意按照中国证监会和上海证券交易所等证券监管机构制定或发布的有关规定、规则，对本人作出相关处罚或采取相关监管措施。”

杭州安恒信息技术股份有限公司董事会

2021 年 4 月 8 日