

国泰君安证券股份有限公司

关于杭州安恒信息技术股份有限公司

首次公开发行股票并在科创板上市之上市保荐书

上海证券交易所：

国泰君安证券股份有限公司（以下简称“保荐机构”、“国泰君安”）接受杭州安恒信息技术股份有限公司（以下简称“发行人”、“安恒信息”、“公司”）的委托，担任安恒信息首次公开发行股票并在科创板上市的保荐机构。

根据《中华人民共和国公司法》（以下简称“《公司法》”）、《中华人民共和国证券法》（以下简称“《证券法》”）、《科创板首次公开发行股票注册管理办法（试行）》（以下简称“《注册办法》”）、《证券发行上市保荐业务管理办法》（以下简称“《保荐业务管理办法》”）、《上海证券交易所科创板上市保荐书内容与格式指引》、《上海证券交易所科创板股票上市规则》等有关规定，保荐机构和保荐代表人本着诚实守信、勤勉尽责的职业精神，严格按照依法制定的业务规则和行业自律规范出具本上市保荐书，并保证所出具的本上市保荐书真实、准确和完整。

本上市保荐书如无特别说明，相关用语具有与《杭州安恒信息技术股份有限公司首次公开发行股票并在科创板上市招股说明书》中相同的含义。

一、发行人基本情况

（一）基本信息

公司名称	杭州安恒信息技术股份有限公司
注册地址	浙江省杭州市滨江区西兴街道联慧街 188 号
主要生产经营地址	浙江省杭州市滨江区西兴街道联慧街 188 号
有限公司成立日期	2007 年 5 月 15 日
股份公司成立日期	2018 年 1 月 25 日
联系电话	0571-28898076
传真号码	0571-28898076
电子信箱	ahxx@dbappsecurity.com.cn
互联网网址	http:// www.dbappsecurity.com.cn
业务范围	服务：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、成果转让，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）。（依法须经批准的项目，经相关部门批准后方可开展经营活动）

（二）主营业务

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。

（三）核心技术与研发水平

公司核心技术具体情况如下：

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
1	数据库协议解析及流量分析技术	通过行为预测、上下文关联、连接信息猜测、流量插件、sql 模板化等技术提高协议解析的准确率，解决云环境下的流量获取难题。	自主研发	原始创新	ZL200910101388.3	已授权	数据库审计与风险控制系统、AiLPHA 大数据智能安全分析平台、数据库防火墙、综合日志审计平台	成熟稳定
					ZL201410381264.6			
					201710734956.8	申请中		
					201710162887.3			
					2017111405539.5			
					201710803213.1			
					201710806265.4			
					201811334470.6			
2	邮件安全检测技术	通过机器学习的智能算法提高对邮件病毒、邮件域名、附件别名、暴力破解及邮件炸弹的检测精准度。	自主研发	原始创新	201811189040.X	申请中	AiLPHA 邮件安全审计平台、AiLPHA 大数据智能安全分析平台	成熟稳定
					201811527137.7			
					201811267249.3			
					201811202283.2			
					201811272654.4			
3	机器学习与识别技术	利用基于机器学习的扫描 IP 分类、策略自学习和优化、DGA 域名快速判别等方法，识别并分析各类日志，	自主研发	原始创新	201811227201.X	申请中	数据库审计与风险控制系统、AiLPHA 大数据智能安全分析平台、综	成熟稳定
					201711171060.X			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
		精准定位各类安全风险。			201710976231.X	已授权	合日志审计平台	
					ZL201610070844.2			
					ZL201410604098.1			
					ZL201210011117.0			
4	信息资产识别与评估技术	采用领先的硬件资产自动分类方法对硬件资产进行分类，利用归一化技术精确识别各类 IPv4/IPv6 资产，最后采用多因子融合模型对资产进行评分，精准识别并定位风险资产。	自主研发	原始创新	ZL201210193161.8	已授权	数据库审计与风险控制系统、AiLPHA 大数据智能安全分析平台、综合日志审计平台	成熟稳定
					201810768873.5	申请中		
					201811316088.2			
					201811420435.6			
5	大数据关联分析、检索处理技术	通过大数据快速索引技术极大提升数据存储能力和检索性能，同时提供基于关联网络异构大数据的 IP 信誉度评级处置以及 IP 组相似度计算方法，能从海量日志中挖掘出潜伏的攻击者及黑客组织。	自主研发	原始创新	ZL201110116710.7	已授权	数据库审计与风险控制系统、AiLPHA 大数据智能安全分析平台、综合日志审计平台	成熟稳定
					201510757700.X	申请中		
					201810103920.4			
					201710731889.4			
					201710715506.4			
					201811224104.5			
6	数据库异常行为检测、防护技术	利用机器学习和蜜罐蜜饵技术智能识别数据库访问行为中的 SQL 注入、拖库撞库、暴力破解等攻击，	自主研发	原始创新	ZL201510105673.8	已授权	数据库审计与风险控制系统、数据库防火墙等	成熟稳定
					201710765207.1	申请中		

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
		保障数据库的安全运行			201710765208.6			
					201710842336.6			
					201811277431.7			
					201710850224.5			
7	AI 智能算法	利用有监督无监督异常检测算法、时间序列分析技术、用户实体行为分析（UEBA）技术，实现对用户行为画像、网络攻击行为检测以及数据泄露篡改等安全检测、防护与阻断，并发现新型未知威胁。	自主研发	原始创新	201811545813.3	申请中	数据库审计与风险控制系统、AiLPHA 大数据智能安全分析平台、综合日志审计平台	成熟稳定
					201811430060.1			
					201811394982.1			
					201811328633.X			
					201811316089.7			
					201811224807.8			
					201811215437.1			
					201811205634.5			
					201811199470.X			
					201810960598.7			
					201810812326.2			
					201810807364.9			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
					201810267006.3			
					201710807649.8			
8	全网资产探测扫描技术	Sumap 全球网络空间超级雷达项目主要用于快速探测分析全球网络资产情况，包括端口资产、应用服务资产、物联网资产、工控设备资产等所有对网络开放的资产。探测引擎基于全网架构设计，实现了自主研发架构，系统内核重构，自建探测报文等多项创新，单台服务器配置情况下 Sumap 探测引擎就能够每秒 60w 并发的探测速度。让数据有效性、准确性都大大提高，同时支持在 ipv4/ipv6 网络环境下的探测。	自主研发	原始创新	201710944839.4	申请中	远程安全评估	成熟稳定
					201810103601.3			
					201811328574.6			
					201810809216.0			
9	恶意软件检测分析技术	通过对样本进行动静态分析，结合机器学习技，基于图片匹配技术，实现样本家族的自动聚类。文件威胁平台自动提取软件基因并找出相似代码、及相同代码，差异性代码等。	自主研发	原始创新	201710973051.6	申请中	文件威胁分析平台	基础研究
					201710776655.1			
					201710910162.2			
					201811272132.4			
					201811342306.X			
10	漏洞检测与验证技术	利用全新的漏洞挖掘技术，实现漏洞的高效发现和挖掘。深入通过 JAVA、PHP 等语言特性，实现基于语言的漏洞挖掘技术。	自主研发	原始创新	ZL201310631280.1	已授权	安全服务	基础研究
					201811328590.5	申请中		
					201811309430.6			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
					201811560041.0			
					201711322603.3			
11	物联网漏洞挖掘与安全威胁预警技术	实现基于物联网的设备漏洞挖掘与威胁预警；包含基于 Qemu 平台的漏洞挖掘方法、智能路由器设备的自动化漏洞挖掘及其他典型智能设备漏洞检测方法及渗透装置，并实现窄带物联网中的僵尸网络预警方法及装置	自主研发	原始创新	201811229341.0	申请中	物联网安全测试服务	基础研究
					201811272099.5			
					201811415420.0			
12	网站实时安全监测与识别技术	该技术通过网站篡改监测、网站指纹识别、文本语义正反面识别、反爬虫、网站服务质量、网站后门、行政归属识别等技术，实现网站的不间断实时监测，以发现网站被篡改内容，可用性异常、存在暗链、黑页、非法信息等问题。	自主研发	原始创新	201710856880.6	申请中	云监测服务（先知） 云防护服务（玄武盾） 威胁情报服务（数据大脑）	成熟稳定
					201710846340.X			
					201710866237.1			
					201711043173.1			
					201711201582.X			
					201710837652.4			
					201710845948.0			
					201710932123.2			
					201810922526.3			
					201811325785.4			
					201710749521.0			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
					201711398535.9			
13	云端 DDoS 及 WEB 防护技术	通过云端安全防护技术，为用户提供零部署零运维云防护服务，分钟级接入，针对 DDoS、篡改、数据泄露、CC 等攻击进行有效防护，利用大数据分析形成可视化报告和统计分析报表，并通过手机 App 云管理服务提供数据分析和查看。	自主研发	原始创新	201710749521.0	申请中	云监测服务（先知） 云防护服务（玄武盾） 威胁情报服务（数据大脑）	成熟稳定
					201711402643.9			
					201710656192.5			
					201711398535.9			
					201710856880.6			
					201810957269.7			
					201710851109.X			
					201810957288.X			
					201811067481.2			
					201710732558.2			
14	涉众型经济犯罪识别技术	是一种通过全网数据采集能力，结合图片识别、语言分析、机器学习等数据分析技术和舆情趋势发现、网络传销组织发展、传销推荐人网站识别、传销项目的奖金制度识别等分析模型，进行金融风险线索发掘、聊天群的舆情分析和运营主体判定的方法及技术。	自主研发	原始创新	201811007473.9	申请中	金融风险监测预警平台	成熟稳定
					201811034567.5			
					201811095794.9			
					201811067481.2			
					201811174968.0			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
					201811395905.8			
					201811083925.1			
15	DNS 监测与防护技术	根据访问用户的区域和线路等智能计算出最优线路服务 IP 返回给客户，从而提升用户访问速度、并监测实现智能防护，如 CC 攻击、网络钓鱼等；	自主研发	集成创新	201710927585.5	申请中	云防护服务（玄武盾） 威胁情报服务（数据大脑）	成熟稳定
					201710854025.1			
16	基于机器学习的攻击识别及防护技术	通过自然语言处理和人工智能深度学习算法、贝叶斯算法、逻辑回归算法等，实现对恶意攻击检测，降低误报，提升用户体验	自主研发	原始创新	201810963633.0	申请中	云防护服务（玄武盾）	成熟稳定
					201810957134.0			
					201811008753.1			
17	应用层协议代理引擎	通过标准协议级别地解析 rdp、ssh、vnc、ftp、sftp、Oracle、DB2、MySQL 等协议流程，细粒度地监控/控制运维人员在运维时的操作细节，实现全方位的运维数据记录及协议级控制能力。	自主研发	集成创新	201810908751.1	申请中	运维审计与风险控制系统	成熟稳定
					201811259823.0			
					201811198761.7			
					201811142877.9			
					201811141192.2			
					201710236691.9			
					201710593256.1			
					201710731586.2			
					201710818094.7			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
					201710861349.8	已授权		
					ZL201410317562.9			
					ZL201410106086.6			
18	运维记录审计平台	通过用户认证、权限访问控制、协议代理、协议审计日志回放等技术解决运维精细化管控和事后审计取证等内控风险隐患。	自主研发	集成创新	201810720486.4	申请中	运维审计与风险控制系统	成熟稳定
					201810961251.4			
					201810983227.0			
					201811141188.6			
					201811178763.X			
					201710993733.3			
19	混合云运维接入技术	本技术的目的在于提供一种基于运维审计系统的混合云管理方法，解决目前使用云服务器的用户越来越多，用户可能在不同的云平台都有云服务器，在本地局域网也有服务器的问题，使用户在通过运维审计系统进行混合云平台运维时，能高效便捷地进行各服务器的接入和管理。	自主研发	集成创新	201811230625.1	申请中	运维审计与风险控制系统	成熟稳定
					201710428890.X			
					201710731933.1			
20	运维权限管理技术	本技术通过账号管理、身份认证、自动改密、资源授权、实时阻断、同步监控、审计回放、自动化运维、流程管理等功能增强运维管理的安全性，广泛适用于需要统一运维安	自主研发	集成创新	ZL201310365539.2	已授权	运维审计与风险控制系统	成熟稳定
					201810646402.7	申请中		
					201810753431.3			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
		全管理与审计的各个行业。			201811210286.0			
					201710652645.7			
					201710898660.X			
					201710942039.9			
					201810646391.2			
21	网络转发与协议代理引擎	通过网络层透明代理技术实现网络 2 层 MAC 和 3 层 IP 的全透明，彻底解决串联部署网络兼容性等技术难题问题，支持各种复杂网络环境下透明串联部署等业务场景防护。	自主研发、转让获得	集成创新	ZL200810222505.7	已授权	Web 应用防火墙	成熟稳定
					ZL201210012058.9			
					ZL201410603197.8			
					ZL201510323671.6			
					201710734958.7	申请中		
					201811206441.1			
					201811272299.0			
					201811380028.7			
22	多种行为分析技术实现自动化攻击防护引擎	创新算法检测 CC 等异常行为攻击，基于蜜罐的 WEB 爬虫阻断，基于合规性的访问审计与防护，基于 JS 等客户端识别技术拦截恶意机器人；	自主研发	集成创新	ZL201310656760.3	已授权	Web 应用防火墙	成熟稳定
					ZL201410205916.0			
					201710655723.9	申请中		

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
					201711414550.8			
					201811211696.7			
					201811469922.1			
					201811548514.5			
23	使用应用层深度特征检测与机器学习建模双重互补机制的安全引擎	机器学习的流量建模与检测，深度优化的检测特征以及通过模糊诱导实现防猜解绕过，针对 cookie 进行加密和校验的防护方法；	自主研发	集成创新	ZL201310656486.X	已授权	Web 应用防火墙	成熟稳定
					ZL201310656527.5			
					201711483889.3	申请中		
					201811206594.6			
					201811292653.6			
24	云平台认证授权与网络编排技术	通过灵活的认证代理、智能许可、动态安全拓扑、自定义编排等专利技术实现了云安全产品的即开即用、满足公有云、私有云等不同售卖场景以及部署环境要求，并大大的提高了用户体验。	自主研发	集成创新	201811040412.2	申请中	天池云安全管理平台	成熟稳定
					201810882151.2			
					201810867643.4			
					201810867641.5			
					201810867949.X			
					201810951109.1			
					201810957544.5			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
					201811110086.8			
25	分布式云中心的虚拟链路监测和保护技术	通过机器学习与链路监控结合负反馈原理，提供了一种解决分布式系统中服务治理难以动态以及智能的难题。该发明的关键点是链路监控，智能预警，动态限流以及断路保护。	自主研发	集成创新	201811110086.8	申请中	天池云安全管理平台	成熟稳定
					201811165004.X			
26	沙箱检测技术	通过把文件提交到沙箱中动态模拟运行，捕获和分析其中的恶意行为，并判定该文件是否为恶意文件。该沙箱检测技术包括丰富的防逃逸能力、沙箱环境快速恢复技术、单沙箱并发检测多样本技术以及完整的沙箱报告，具有检测效率优异、报告丰富的特点	自主研发	原始创新	ZL201410381591.1	已授权	APT 攻击（网络战）预警平台	成熟稳定
					ZL201510141931.8			
					ZL201510455976.2			
					201710802842.2	申请中		
					201710855521.9			
					201710802842.2			
27	DNS 流量检测技术	通过对 DNS 请求的双向流量解析，结合机器学习算法和威胁情报数据，识别受控主机及所感染病毒家族、僵尸网络、C&C 服务器、隐蔽信道通信等威胁	自主研发	原始创新	201710850732.3	申请中	APT 攻击（网络战）预警平台	成熟稳定
					201810800900.2			
					201710824621.5			
					201710855704.0			
28	APT 攻击检测技术	通过对 APT 攻击链的各攻击阶段攻击行为，从多个维度进行深层次的分析检测，并且某一攻击阶段中发现的攻击线索可以进一步作为其他攻击阶段的检测依据，各攻击阶段	自主研发	原始创新	ZL201510854610.2	已授权	APT 攻击（网络战）预警平台、全流量深度威胁检测平台	成熟稳定
					201710731477.0	申请中		
					201810680180.0			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
		的检测结论还可以进一步关联，形成确定性更高的攻击证据，以更高效地发现 APT 攻击			201811240239.0			
					201811083781.X			
					201811083322.1			
					201710866230.X			
					201810732943.1			
29	恶意攻击识别与追踪溯源技术	通过勒索、WEBSHELL、爆破、SQL 注入等攻击识别,追溯网页篡改行为及通过 WEB 方式的恶意操作。	自主研发	原始创新	201811180960.5	申请中	主机与终端安全管理系统	成熟稳定
					201710225087.6			
					201810867948.5			
					201710931986.8			
					201710850495.0			
					201710223468.0			
30	物联网终端资产识别与检测技术	主要包括：物联网资产指纹识技术；资产非法接入识别；摄像头弱口令检测；物联网设备漏洞检测等核心技术；便能够快速分析出物联网设备可能存在的漏洞风险。	自主研发	原始创新	201811309438.2	申请中	物联网安全监测、物联网安全心、物联网安全态势感知系列产品	成熟稳定
					201810867467.4			
					201810705351.0			
					201810711928.9			
31	物联网终端防	主要包括:摄像头物联网拟态防护技	自主研发	原始创新	201810710903.7	申请中	物联网安全监测、物联	成熟稳定

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
	护、分析与取证技术	术；物联网嵌入式防护技术；驱动层防爆破方法；物联网设备取证方法；物联网资产安全横向分析方法等技术；进一步去判断是否存在风险，并通过防护技术进行安全防护。			201810721128.5		网安全心、物联网安全态势感知系列产品	
					201810867948.5			
					201810810228.5			
					201810680199.5			
32	Web 漏洞扫描技术	通过对网站的 SQL 注入检测、SSRF 检测、EL 表达式注入检测、任意文件下载等漏洞的检测与识别，及时发现网站应用的安全漏洞威胁。	自主研发	原始创新	ZL201410381334.8	已授权	漏洞扫描系列产品	成熟稳定
					201810944476.9	申请中		
					201710732152.4			
					201710788259.0			
					201811096606.4			
					201811096616.8			
					201811021145.4			
					201710664116.9			
					201710740476.2			
33	网页篡改监测技术	通过基线对比，敏感词库，静态检测和动态检测有效混合的高效方法、机器学习等技术对网页恶意代码、暗链、敏感信息等的篡改行为进行监测与识别	自主研发	原始创新	ZL201210092707.0	已授权	网站安全监测平台	成熟稳定
					ZL201410350025.4			
					201811085264.6	申请中		

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
					201810793341.7			
					201810922526.3			
					201811325782.0			
					201710794987.2			
34	漏洞扫描爬虫技术	包括基于浏览器内核动态执行的爬虫，冗余页面发现，动态流控，有效发现网站 URL 和不会对被扫描网站产生影响	自主研发	原始创新	201611005039.8	申请中	漏洞扫描系列产品	成熟稳定
					201710854632.8			
					201611057820.X			
					201710846183.2			
35	漏洞验证技术	包括对 JAVA 的动态漏洞检测、取证式扫描、自动化渗透、基于沙箱的漏洞验证，使得提高扫描出的漏洞准确率	自主研发	原始创新	ZL201310631280.1	已授权	漏洞扫描系列产品	成熟稳定
					ZL201410185544.X			
					ZL201410381582.2			
					201611005006.3	申请中		
					201710854522.1			
36	数据库漏洞扫描技术	包括对数据库的内核篡改、隐藏用户、隐藏触发器、敏感信息数据探测与识别等技术；	自主研发	原始创新	ZL201210358257.5	已授权	数据库漏洞扫描系列产品	成熟稳定
					ZL201210359074.5			
					ZL201210359049.7			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
					ZL201110401023.X			
					ZL201410356492.8			
37	攻击行为识别技术	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。	自主研发	原始创新	201711086376.9	申请中	网络安全态势感知通报预警平台	成熟稳定
					201810684242.5			
					201810884997.X			
					201810793341.7			
					201710767142.4			
					201710823565.3			
38	自动化行为分析与自验证技术	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。	自主研发	原始创新	201711086376.9	申请中	网络安全态势感知通报预警平台	成熟稳定
					201810684242.5			
					201810884997.X			
					201810793341.7			
					201810981730.2			
					201710823565.3			
39	对实时网络流量分析的深度检测技术	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；	自主研发	原始创新	201811165007.3	申请中	网络安全态势感知通报预警平台	成熟稳定
					201810743135.5			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
					201810657231.8			
					201810561442.1			
					201810809216.0			
					201810720924.7			
					201811118222.8			
					201710767142.4			
					201710713787.X			
40	追踪溯源、攻击画像的分析技术	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。	自主研发	原始创新	201810815080.4	申请中	网络安全态势感知通报预警平台	成熟稳定
					201810727242.9			
					201810720807.0			
					201811096596.4			
					201710981610.8			
					201810726143.9			
					201810774498.5			
					201810807347.5			
					201811010404.3			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
41	分布式微服务架构技术	通过对 java、数据库、docker、微服务等技术的应用和优化，提高产品的功能、性能和稳定性	自主研发	集成创新	201810703464.7		网络安全态势感知通报预警平台	成熟稳定
					201811047586.1			
					201711130896.5			
					201711037833.5			
					201711038679.3			
					201810790264.X			
					201811268870.1			
					201710953105.2			
42	工控协议流量异常检测技术	通过捕获网内工控流量数据进行解析，通过分析比对异常流量策略，检测异常流量。该异常流量策略，可自定义修改，添加，开关。	自主研发	原始创新	201811128424.0	申请中	工控安全监测审计平台，	成熟稳定
					201811180941.2			
					201810973981.6			
					201811031062.3			
43	工控设备识别与漏洞扫描技术	通过采集工控设备的指纹信息，识别设备型号以及存在漏洞。针对工控设备的性能低的情况，本技术能够利用负载均衡算法，有效优化工控设备的扫描流量，可针对大型局域网场景，进行并发多任务扫描提升扫描效率。	自主研发	原始创新	201811127549.1	申请中	工控漏洞扫描平台工控安全监测审计平台	成熟稳定
					201810897812.9			
					201810862584.1			
					201810957399.0			
					201810874059.1			
					201810998422.0			
					201810804871.7			
44	工控协议漏洞挖掘技术	能够自动化识别工控设备协议，针对不同的工控协议的特点及其自身的弱点，从协议本身各个字段生成具有针对性的测试用例。对测试用	自主研发	集成创新	201810693587.7	申请中	工业防火墙、工控漏洞扫描平台、工控安全监测审计平台	成熟稳定

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品和服务	所处阶段
		例中的字段进行不断的变化迭代测试，在测试过程中，利用状态检测器检测不同协议，以及设备的状态，并实时捕获异常数据测试任务落地存储，并生成分析报告。			201810897812.9			
45	工业互联网防护技术与可视化技术	能够自动化识别工控设备协议，针对不同的工控协议的特点及其自身的弱点，从协议本身各个字段生成具有针对性的测试用例。对测试用例中的字段进行不断的变化迭代测试，在测试过程中，利用状态检测器检测不同协议，以及设备的状态，并实时捕获异常数据测试任务落地存储，并生成分析报告。	自主研发	原始创新	201810803233.3	申请中	工业防火墙、工控漏洞扫描平台、工控安全监测审计平台	成熟稳定
					201811180865.5			
					201810793383.0			
					201810947120.0			
					201811308834.3			
46	仿真模型及终端	通过仿真模块对工业控制系统的网络结构、网络流量、网络主机进行安全合规性检测，网络主机以及网络安全培训场景仿真。	自主研发	原始创新	201810918968.0	申请中	蜜罐迷网系统	成熟稳定
47	网络安全事件分析技术	对采集日志的特征进行分析与识别形成网络安全事件分析基础数据，通过基于日志、时间线的网络安全事件分析方法，实现网络安全事件发生过程的分析、追溯、与还原，提高应急处置工作效率	自主研发	原始创新	ZL201720357629.0	已授权	网络安全事件应急处置工具箱	成熟稳定
					201710779745.6	申请中		
					201710802670.9			
48	等级保护合规性检查技术	通过面向等级保护的检查方法的实现，将等级保护的要求以指标形式进行细化，能够帮助用户加快合规性检查过程，并完成相关检测技术的实施。	自主研发	原始创新	ZL201510141097.2	已授权	信息安全等级保护检查工具箱	成熟稳定
					201710785914.7	申请中		
					201810864237.2			

经过多年不断地实践完善，公司形成了围绕“技术委员会-安全研究院-产品研发中心三级研发管理架构”为核心的全面独特的创新研发模式。

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 and 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。

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的质量管理体系已通过国际 ISO9001 和 ISO14001 管理体系的认证，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，具有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。

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”等国家级、省市级科技计划项目近 40 项。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。

（四）主要经营和财务数据及指标

1、合并资产负债表主要数据

单位：万元

项目	2018 年 12 月 31 日	2017 年 12 月 31 日	2016 年 12 月 31 日
资产总计	89,768.96	62,297.33	39,078.88
负债总计	38,039.52	18,862.74	15,351.08
股东权益	51,729.44	43,434.59	23,727.80
归属于母公司股东权益	51,703.46	43,478.50	23,332.09

2、合并利润表主要数据

单位：万元

项目	2018 年度	2017 年度	2016 年度
营业收入	64,042.08	43,039.81	31,671.38
营业利润	8,262.20	6,007.41	-3,389.11
利润总额	8,381.32	5,953.14	575.77
净利润	8,348.85	5,488.30	119.06
归属于母公司股东的净利润	8,462.45	5,491.13	78.05
扣除非经常性损益后归属于母公司股东的净利润	6,799.48	3,908.87	2,872.71

3、合并现金流量表主要数据

单位：万元

项目	2018 年度	2017 年度	2016 年度
经营活动产生的现金流量净额	9,598.26	6,886.94	6,375.49

项目	2018 年度	2017 年度	2016 年度
投资活动产生的现金流量净额	879.93	-8,314.93	-871.12
筹资活动产生的现金流量净额	7,378.41	14,685.17	238.25
现金及现金等价物净增加额	17,856.67	13,256.95	5,743.25

4、财务指标

指标	2018.12.31	2017.12.31	2016.12.31
流动比率（倍）	2.28	2.86	2.29
速动比率（倍）	2.09	2.65	2.06
资产负债率（母公司）	39.91%	27.89%	38.05%
资产负债率（合并）	42.37%	30.28%	39.28%
归属于母公司股东的每股净资产（元/股）	9.31	7.83	4.67
指标	2018 年度	2017 年度	2016 年度
应收账款周转率（次/年）	4.42	4.30	4.02
存货周转率（次/年）	4.99	5.10	4.42
息税折旧摊销前利润（万元）	9,655.64	6,974.35	1,460.19
归属于母公司股东的净利润（万元）	8,462.45	5,491.13	78.05
归属于母公司股东扣除非经常性损益后的净利润（万元）	6,799.48	3,908.87	2,872.71
研发投入占营业收入的比例	23.73%	22.29%	20.80%
每股经营活动产生的现金流量（元/股）	1.73	1.24	1.28
每股净现金流量（元/股）	3.21	2.39	1.15

注：资产负债率=负债总额/资产总额；

流动比率=流动资产/流动负债；

速动比率=（流动资产-存货-预付款项-其他流动资产）/流动负债；

归属于母公司股东的每股净资产=期末归属于母公司所有者权益/期末股本总额；

应收账款周转率=营业收入/应收账款期初期末平均余额；

存货周转率=营业成本/存货期初期末平均余额；

息税折旧摊销前利润=利润总额+利息支出+折旧+摊销；

每股经营活动现金流量净额=经营活动产生的现金流量净额/期末股本总额；

每股现金流量净额=现金流量净额/期末股本总额。

（五）主要风险

1、实际控制人变更的风险

公司的实际控制人为范渊，范渊直接持有安恒信息 18.03%的股份，安恒信息的员工持股平台嘉兴安恒、宁波安恒分别持有安恒信息 9.00%、9.00%的股权。范渊分别持有嘉兴安恒、宁波安恒 9.16%和 47.09%的出资份额，且为上述两家合伙企业的普通合伙人及执行事务合伙人，范渊共控制安恒信息 36.03%的表决权，合计持有表决权的比例超过任何其他单一股东（第二大股东持股比例为 14.42%、第三大股东持股比例为 9.36%）；同时，报告期内范渊一直担任发行人及其前身安恒有限的董事长兼总经理，主持发行人及其前身安恒有限的经营管理工作，目前实际控制人地位较稳固。考虑 IPO 至少发行 25%股份的稀释效果，被稀释后范渊直接加间接持股比例不高于 27.02%。由于两个员工持股平台限售期满后存在进行收益清算并解散的可能性，解散后范渊持股比例不高于 13.52%（稀释后第二大股东持股比例不高于 10.82%，第三大股东持股比例不高于 7.02%），公司在上市后可能面临实际控制人变更进而影响公司稳定经营的风险。

2、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）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。

(3) 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 6,586.39 万元、9,592.94 万元和 15,195.19 万元,占营业收入的比重分别为 20.80%、22.29%和 23.73%。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、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) 管理能力不能满足业务发展需求的风险

近年来,公司在人员及资产规模方面扩张较快,2016-2018 年末公司员工人数分别为 691 人、991 人和 1,332 人,最近三年末公司总资产分别为 39,078.88 万元、62,297.33 万元及 89,768.96 万元。并且未来随着公司首次公开发行股票并

上市、募集资金投资项目的逐步实施，公司的资产及业务规模将进一步扩大。目前，公司的管理层在上市公司规范治理方面尚缺乏经验，如果未来公司管理水平不能快速适应不断扩大的业务规模，解决上市公司经营管理面临的新课题，将对公司发展带来不利影响。

（3）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。

（4）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，公司营业收入和净利润（剔除股份支付）按上、下半年度分布情况如下：

项目	2018 年度		2017 年度		2016 年度	
	当期营业收入占比	当期净利润占比	当期营业收入占比	当期净利润占比	当期营业收入占比	当期净利润占比
上半年	26.01%	-59.45%	27.92%	-39.66%	26.32%	8.78%
下半年	73.99%	159.45%	72.08%	139.66%	73.68%	91.22%

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。

（5）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，最近三年公司的渠道销售收入占营业收入的比重分别为 52.38%、55.16%和 56.88%，逐年上升。公司产品客户集中度较低（2018 年前五大客户销售额占营业收入比为 10.87%）、公司产品的目标用户数多、用户的地域及行业分布广。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 and 产品销售造成不利影响。

（6）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。

4、财务风险

（1）应收账款大幅增加未来发生坏账的风险

2018 年 12 月 31 日，公司应收账款净额为 17,871.65 万元，占资产总额 19.91%，应收账款规模较大。2018 年应收账款余额较 2017 年应收账款余额增长 60.32%，2017 年应收账款余额较 2016 年应收账款余额增长 24.41%。

由于公司收入增长较快，行业的经营季节性特点造成四季度末应收账款较高，公司 2018 年年末应收账款中超过合同信用期（逾期）的金额为 8,322.79 万元，占比 43.17%。

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。

（2）对外投资减值的风险

报告期内弗兰科为发行人参股公司，以自有资金经营移动网络安全软件研发、销售业务，发行人持有弗兰科股权比例为 48.627%。报告期内，发行人对弗兰科长期股权投资期末余额分别为 1,451.10 万元、2,360.26 万元和 1,883.36 万元，各期投资收益分别为-173.01 万元、-417.29 万元和-476.89 万元。报告期末，弗兰科净资产 2,151.70 万元，天津中联资产评估有限责任公司出具了针对弗兰科 100% 股权的资产评估报告（中联评报字[2019]D-0013 号），弗兰科的评估值为 4,490.00 万元，低于其最近一次外部投资者的估值 13,750.00 万元。

弗兰科估值下降的原因为该公司前期研发投入较大，产品尚处于市场开拓阶段。未来可能继续产生长期投资减值，从而对本公司未来的利润产生一定影响。

（3）发行后净资产收益率下降的风险

预计本次发行完成后，公司净资产将有较大幅度的增长（募投项目拟投入资金 7.6 亿）。由于募集资金投资项目须有一定的建设周期，募集资金产生经济效益存在一定的不确定性和时间差。因此，短期内公司净资产收益率可能有一定幅度的下降，从 2018 年的 17.78%下降为发行后的 13.25%（假设 2019 年净利润与 2018 年无变化），从而存在净资产收益率下降的风险。

5、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。截至本招股说明书签署日，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。

（2）违反共有专利相关合同约定导致的法律诉讼风险

2013 年 9 月，公司与公安部第一研究所、北京中宇万通科技有限公司签署《技术开发合同》，共同开发“公安信息通信网综合安全审计系统定制开发项目”，并形成“通过 Session 进行请求的方法”的专利。上述合同约定，“对于本合同完成的系统，其版权由甲方、丙方双方共同拥有，任何一方在未取得共有人的合法授权的情况下，不得以任何形式进行销售或者处置”、“该系统的技术秘密所有权和使用权归在公安行业内归甲方所有，在全国除公安行业外的行业归甲方、丙方共同所有。在公安行业内，甲方具有该产品的销售权，乙方和丙方在未经甲方授权的情况下，不得独立在公安行业销售该产品。在销售活动中，甲方须优先选择乙方和丙方作为合作伙伴，选择其产品，共同开发公安行业市场。”

报告期内，公司未基于上述共有专利进一步开发、生产和销售相关产品。但如果未来公司未经公安部第一研究所授权销售或处置《技术开发合同》项下相关系统，或未经公安部第一研究所授权独立在公安行业销售基于共有专利开发生产的相关产品，公司将存在法律诉讼风险。

6、发行失败风险

根据相关法规要求，若本次发行时有效报价投资者或网下申购的投资者数量不足法律规定要求，或者发行时总市值未能达到预计市值上市条件的，本次发行应当中止，若发行人中止发行上市审核程序超过交易所规定的时限或者中止发行注册程序超过 3 个月仍未恢复，或者存在其他影响发行的不利情形，或将会出现发行失败的风险。

7、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。

报告期内，公司税收优惠金额分别为 3,197.46 万元、4,058.01 万元及 5,288.95 万元，占剔除股份支付后的利润总额的比例分别为 66.74%、68.17%及 63.10%。公司享受的税收优惠均是与公司日常经营相关，具有一定的稳定性和持续性。报告期内公司实现销售收入 31,665.13 万元、43,039.81 万元及 64,042.08 万元，公司报告期内销售规模不断提升且快速增长，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 1,443.31 万元、1,816.49 万元和 1,285.03 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。

8、募投项目达不到预期效益导致公司业绩受损的风险

根据公司战略规划，公司的募投项目将围绕着云安全、大数据安全、物联网安全和智慧城市安全的发展方向对自有的网络信息安全产品进一步升级和技术研发。同时为了更好的完成战略目标，公司将对现有营销网络及服务体系进行进一步扩建。

公司本次发行募集资金投资项目是依据公司发展战略制定的，并进行了详尽的可行性分析，但未来在开拓新市场、推销新产品的过程中依然会面临一定的不确定性。如果本次募投项目所推出的新产品、新服务的未来市场空间低于预期，或公司推广新产品、新服务的效果与预测产生较大偏差，公司将会面临募集资金投资项目投产后达不到预期效益从而导致经营业绩受损的风险。

二、发行人本次发行情况

证券种类	人民币普通股（A 股）
发行股数	本次拟向社会公众公开发行不超过 1,851.8519 万股，占公司发行后总股本的比例不低于 25%，超额配售部分不超过本次公开发行股票数量的 15%，若全额行使超额配售选择权，则本次发行股票

	的数量不超过 2,129.6296 万股，不超过发行后总股本的 27.71%。本次发行，公司股东不进行公开发售股份。
保荐人相关子公司拟参与战略配售情况	保荐机构将安排相关子公司参与本次发行战略配售，具体按照上交所相关规定执行。保荐机构及其相关子公司后续将按要求进一步明确参与本次发行战略配售的具体方案，并按规定向上交所提交相关文件。
发行方式	采用网下对投资者询价配售和网上向社会公众投资者定价发行相结合的方式或证券监管部门认可的其他方式
发行对象	在上交所科创板开户的投资者（国家法律、法规和规范性文件禁止购买者除外），或根据发行当时监管部门规定的其它投资者
承销方式	余额包销

三、本次证券发行上市的保荐代表人、项目协办人及其他项目组成员

（一）具体负责本次推荐的保荐代表人

余姣女士：国泰君安证券股份有限公司投资银行部执行董事，保荐代表人、中国注册会计师。曾任职于中瑞岳华会计师事务所。IPO 方面，曾参与北京正和工程装备等项目；并购重组方面，负责实施了上海华明借壳法因数控，井神股份并购控股股东资产、爱使股份并购游久游戏、威远生化重大资产重组等项目；再融资方面，曾参与太龙药业、康得新等上市公司的非公开发行股票项目。

李宁先生：国泰君安证券股份有限公司投资银行部董事总经理。保荐代表人，注册会计师协会会员，硕士研究生，具有 13 年丰富的投资银行业务经验。股权融资方面，近年主持的项目主要有鼎龙股份 IPO、力帆股份 IPO、爱建股份非公开发行、国金证券非公开发行、力帆股份非公开发行、中海发展可转债等，此外还主持或参与过浦发银行、锦州港等重大融资项目；并购重组方面，主持或参与了洪城水业、锦江旅游、上柴股份等上市公司重大资产重组，以及香港绿庭收购 ST 大江等项目。曾获得 2011 年“新财富百佳保荐代表人”、2011 年中国券商“金方向奖”优秀保荐代表人等多项殊荣。

（二）项目协办人及其他项目组成员

项目协办人：赵炜华

赵炜华先生，国泰君安证券股份有限公司投资银行部高级经理，准保荐代表人，金融硕士。曾参与井神股份重大资产重组项目。

其他项目组成员：陈泽森、是航、田昕、曹宁、何易韩。

四、保荐机构与发行人之间的关联关系

（一）截至本发行保荐书出具日，不存在保荐机构或其控股股东、实际控制人、重要关联方持有发行人或其控股股东、实际控制人、重要关联方股份的情况；

（二）截至本发行保荐书出具日，不存在发行人或其控股股东、实际控制人、重要关联方持有保荐机构或其控股股东、实际控制人、重要关联方股份的情况；

（三）截至本发行保荐书出具日，不存在保荐机构的保荐代表人及其配偶，董事、监事、高级管理人员拥有发行人权益、在发行人任职等情况；

（四）截至本发行保荐书出具日，不存在保荐机构的控股股东、实际控制人、重要关联方与发行人控股股东、实际控制人、重要关联方相互提供担保或者融资等情况；

（五）截至本发行保荐书出具日，不存在保荐机构与发行人之间的其他关联关系。

根据《上海证券交易所科创板股票发行与承销实施办法》等相关法律、法规的规定，保荐机构依法设立的相关子公司或者实际控制该保荐机构的证券公司依法设立的其他相关子公司，参与本次发行战略配售，具体事宜按照上海证券交易所相关规定执行。保荐机构及前述关联子公司后续将按要求进一步明确参与本次发行战略配售的具体方案，并按规定向上海证券交易所提交相关文件。

五、保荐机构承诺事项

（一）保荐机构对本次上市保荐的一般承诺

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

（二）保荐机构对本次上市保荐的逐项承诺

保荐机构已按照法律、行政法规和中国证监会等有关规定对发行人进行了充

分的尽职调查和辅导，保荐机构有充分理由确信发行人至少符合下列要求：

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

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

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

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

5、保证所指定的保荐代表人及本保荐机构的相关人员已勤勉尽责，对发行人申请文件和信息披露资料进行了尽职调查、审慎核查；

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

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

8、自愿接受中国证监会依照《证券发行上市保荐业务管理办法》采取的监管措施；

9、中国证监会规定的其他事项。

六、保荐机构对本次发行上市的推荐结论

在充分尽职调查、审慎核查的基础上，保荐机构认为，安恒信息首次公开发行股票并在科创板上市符合《公司法》、《证券法》、《注册办法》、《保荐业务管理办法》等法律、法规和规范性文件中有关首次公开发行股票并在科创板上市的条件。同意推荐安恒信息本次证券发行上市。

七、本次证券发行上市履行的决策程序

发行人就本次证券发行履行的内部决策程序如下：

2019 年 3 月 6 日，发行人召开了第一届董事会第七次会议，审议通过了关于公司首次公开发行人民币普通股（A 股）股票并在科创板上市等议案。

2019 年 3 月 23 日，发行人召开 2019 年第四次临时股东大会，审议通过了关于公司首次公开发行人民币普通股（A 股）股票并在科创板上市等议案。

依据《公司法》、《证券法》等法律法规及发行人《公司章程》的规定，发行人申请在境内首次公开发行股票并在科创板上市已履行了完备的内部决策程序。

八、保荐机构关于发行人是否符合科创板定位所作出的说明，及保荐机构的核查内容和核查过程

（一）安恒信息符合科创板定位要求的具体情况

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

序号	科创板定位	具体依据
1	面向世界科技前沿、面向经济主战场、面向国家重大需求	发行人旗下产品覆盖云安全、大数据安全及物联网安全等信息安全科技前沿产品领域，满足国家对国家网络安全保障的重大需求。
2	符合国家战略	发行人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，符合《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）年》、《信息通信网络与信息安全规划（2016-2020）年》等多项国家战略。
3	拥有关键核心技术	发行人通过多年持续研发已积累 48 项信息安全领域核心技术，部分核心技术已经处于国内领先水平。在国内相关产品的主流市场竞争中，掌握同等级别技术的公司主要包括奇安信、绿盟科技、启明星辰等。
4	科技创新能力突出	自成立以来，发行人对信息安全领域核心技术的发展持续跟踪并进行深入研究开发，目前发行人拥有 52 项发明专利和 146 项软件著作权。

序号	科创板定位	具体依据
5	主要依靠核心技术开展生产经营	公司自成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。目前公司在我国应用和数据安全市场处于行业领先地位,公司核心基础安全产品持续多年市场份额位居行业前列。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,自主研发了 48 项核心技术,该等核心技术广泛应用于公司主要产品或服务,核心技术产品所贡献的收入覆盖了公司营业收入的 90% 以上。
6	具有稳定的商业模式	公司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。
7	市场认可度高	发行人的产品方案已经被财政部、公安部、交通运输部、工业和信息化部、中国人民银行、中国外汇交易中心、北京市公安局、上海市公安局、中国电信、中国移动、中国联通、华为、阿里云、京东商城、海康威视等单位采用。
8	社会形象良好	发行人凭借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。
9	具有较强成长性	报告期内,发行人的营业收入分别为 31,671.38 万元、43,039.81 万元、64,042.08 万元,2017 年及 2018 年实现同比增长 35.89%、48.80%。 报告期内,发行人净利润分别为 119.06 万元、5,488.30 万元、8,348.85 万元,2018 年实现同比增长 52.12%。

(二) 保荐机构核查过程及意见

本保荐机构履行了查阅相关行业研究报告、行业法律法规及国家政策文件,取得并核查专利权等相关无形资产的证明文件,查阅公司的销售合同、采购合同在内的重大合同,实地走访重要客户及供应商,访谈公司高管及核心技术人员、核查公司及有关人员无违法违规情况并取得相关部门合规证明等核查程序。

经核查,本保荐机构认为,发行人所从事的业务及所处行业符合国家战略,属于面向世界科技前沿、面向经济主战场、面向国家重大需求的科技创新行业。同时,发行人具备关键核心技术并主要依靠核心技术开展生产经营,具有较强的科技创新能力,商业模式稳定,市场认可度较高,社会形象良好,成长性较强,

符合相关法律法规中对科创板定位的要求。

九、保荐机构关于发行人是否符合《上海证券交易所科创板股票上市规则》规定的上市条件的逐项说明

（一）发行人符合《上海证券交易所科创板股票上市规则》第 2.1.1 条之“（一）符合中国证监会规定的发行条件”规定

1、经核查发行人设立至今的营业执照、公司章程、发起人协议、创立大会文件、评估报告、审计报告、验资报告、工商档案等有关资料，发行人系于 2018 年 1 月整体变更设立的股份有限公司。保荐机构认为，发行人是依法设立且合法存续的股份有限公司，符合《注册办法》第十条的规定。

2、经核查发行人工商档案资料，发行人前身成立于 2007 年 5 月，发行人于 2018 年 1 月按经审计账面净资产值折股整体变更设立的股份有限公司，持续经营时间可以从有限责任公司成立之日起计算。保荐机构认为，发行人持续经营时间在三年以上，符合《注册办法》第十条的规定。

3、经核查发行人股东大会议事规则、董事会议事规则、监事会议事规则、董事会专门委员会议事规则、独立董事制度、董事会秘书制度、发行人相关会议文件、组织机构安排等文件或者资料，保荐机构认为，发行人已经具备健全且运行良好的组织机构，相关机构和人员能够依法履行职责，符合《注册办法》第十条的规定。

4、经核查发行人的会计记录、记账凭证等资料，结合立信出具的《审计报告》（信会师报字[2019]第 ZF10134 号），保荐机构认为，发行人会计基础工作规范，财务报表的编制符合企业会计准则和相关会计制度的规定，在所有重大方面公允地反映了发行人的财务状况、经营成果和现金流量，并由注册会计师出具了标准无保留意见的审计报告，符合《注册办法》第十一条的规定。

5、经核查发行人的内部控制流程及内部控制制度，结合立信出具的标准无保留意见的《内部控制鉴证报告》（信会师报字[2019]第 ZF10135 号），保荐机构认为，发行人内部控制制度健全且被有效执行，能够合理保证公司运行效率、合

法合规和财务报告的可靠性，并由注册会计师出具了无保留结论的内部控制审核报告，符合《注册办法》第十一条的规定。

6、经核查发行人业务经营情况、主要资产、软件著作权、专利、商标以及控股股东控制架构等资料，实地核查有关情况，并结合发行人律师出具的法律意见书、实际控制人调查表及对发行人董事、监事和高级管理人员的访谈等资料，保荐机构认为，发行人资产完整，业务及人员、财务、机构独立，与控股股东、实际控制人及其控制的其他企业间不存在对发行人构成重大不利影响的同业竞争，不存在严重影响独立性或者显失公平的关联交易，符合《注册办法》第十二条第（一）项的规定。

7、经核查发行人报告期内的主营业务收入构成、重大销售合同及主要客户等资料，保荐机构认为发行人最近2年内主营业务未发生重大不利变化；经核查发行人工商档案及聘请董事、监事、高级管理人员的股东大会决议和董事会决议、核心技术人员的《劳动合同》以及访谈文件等资料，保荐机构认为，最近2年内发行人董事、高级管理人员及核心技术人员均没有发生重大不利变化。经核查发行人工商档案、控股股东承诺等资料，结合发行人律师出具的法律意见书，保荐机构认为，控股股东和受控股股东、实际控制人支配的股东所持发行人的股份权属清晰，最近2年实际控制人没有发生变更，不存在导致控制权可能变更的重大权属纠纷，符合《注册办法》第十二条第（二）项的规定。

8、经核查发行人财产清单、主要资产的权属证明文件等资料，结合与发行人管理层的访谈、立信出具的《审计报告》（信会师报字[2019]第 ZF10134 号）和发行人律师出具的法律意见书，保荐机构认为，发行人不存在主要资产、核心技术、商标等的重大权属纠纷，重大偿债风险，重大担保、诉讼、仲裁等或有事项，经营环境已经或者将要发生重大变化等对持续经营有重大不利影响的事项，符合《注册办法》第十二条第（三）项的规定。

9、根据发行人取得的工商、税务等机构出具的有关证明文件、实际控制人提供的无犯罪证明及发行人律师出具的法律意见书，结合立信出具的《审计报告》（信会师报字[2019]第 ZF10134 号）等文件，保荐机构认为，最近3年内，发行人及其控股股东、实际控制人不存在贪污、贿赂、侵占财产、挪用财产或者破坏

社会主义市场经济秩序的刑事犯罪，不存在欺诈发行、重大信息披露违法或者其他涉及国家安全、公共安全、生态安全、生产安全、公众健康安全等领域的重大违法行为，符合《注册办法》第十三条的规定。

10、根据董事、监事和高级管理人员提供的无犯罪证明、调查表及中国证监会等网站公开检索等资料，结合发行人律师出具的法律意见书，保荐机构认为，发行人董事、监事和高级管理人员不存在最近 3 年内受到中国证监会行政处罚，或者因涉嫌犯罪被司法机关立案侦查或者涉嫌违法违规被中国证监会立案调查，尚未有明确结论意见等情形，符合《注册办法》第十三条的规定。

（二）发行人符合《上海证券交易所科创板股票上市规则》第 2.1.1 条之“（二）发行后股本总额不低于人民币 3000 万元”规定

经核查，发行人本次发行前股本总额为 5,555.5556 万元，本次拟发行股份不超过 1,851.8519 万股（不考虑超额配售选择权），发行后股本总额不超过 7,407.4075 万元。

（三）发行人符合《上海证券交易所科创板股票上市规则》第 2.1.1 条之“（三）公开发行的股份达到公司股份总数的 25%以上；公司股本总额超过人民币 4 亿元的，公开发行股份的比例为 10%以上”规定

经核查，本次发行后，公司股本总额不超过 7,407.4075 万元，本次拟发行股份不超过 1,851.8519 万股（不考虑超额配售选择权），公开发行的股份达到公司股份总数的 25%以上。

（四）发行人符合《上海证券交易所科创板股票上市规则》第 2.1.1 条之“（一）市值及财务指标符合本规则规定的标准”规定

根据《杭州安恒信息技术股份有限公司关于本次公开发行股票并在科创板上市的申请报告》，发行人选择的具体上市标准为《上海证券交易所科创板股票上市规则》第 2.1.2 条中规定的第（一）项标准，即“预计市值不低于人民币 10 亿元，最近两年净利润均为正且累计净利润不低于人民币 5000 万元，或者预计市值不低于人民币 10 亿元，最近一年净利润为正且营业收入不低于人民币 1 亿元”。

根据立信出具的《审计报告》（信会师报字[2019]第 ZF10134 号），发行人 2017

年、2018 年扣除非经常性损益前后孰低的归属于母公司股东净利润分别为 3,908.87 万元、6,799.48 万元，公司最近两年净利润均为正且累计净利润不低于人民币 5000 万元；根据立信出具的《审计报告》（信会师报字[2019]第 ZF10134 号），发行人 2018 年营业收入为 6.4 亿元，不低于 1 亿元，符合发行人选择的具体上市标准《上海证券交易所科创板股票上市规则》第 2.1.2 条中规定的第（一）项标准中的财务指标。

参照公司 2019 年初最近一次股权转让对应的估值 30 亿元，公司市值不低于 10 亿元，符合发行人选择的具体上市标准《上海证券交易所科创板股票上市规则》第 2.1.2 条中规定的第（一）项标准中的市值指标。

（五）发行人符合《上海证券交易所科创板股票上市规则》第 2.1.1 条之“（五）上海证券交易所规定的其他上市条件”规定

经核查，发行人符合上海证券交易所规定的其他上市条件。

十、对发行人证券上市后持续督导工作的具体安排

主要事项	具体计划
（一）持续督导事项	证券上市当年剩余时间及其后 3 个完整会计年度
1、督导发行人有效执行并完善防止主要股东、其他关联方违规占用发行人资源的制度	（1）督导发行人有效执行并进一步完善已有的防止主要股东、其他关联方违规占用发行人资源的制度；（2）与发行人建立经常性沟通机制，持续关注发行人上述制度的执行情况及履行信息披露义务的情况
2、督导发行人有效执行并完善防止其高级管理人员利用职务之便损害发行人利益的内部控制制度	（1）督导发行人有效执行并进一步完善已有的防止高级管理人员利用职务之便损害发行人利益的内部控制制度；（2）与发行人建立经常性沟通机制，持续关注发行人上述制度的执行情况及履行信息披露义务的情况
3、督导发行人有效执行并完善保障关联交易公允性和合规性的制度，并对关联交易发表意见	（1）督导发行人有效执行《公司章程》、《关联交易管理制度》等保障关联交易公允性和合规性的制度，履行有关关联交易的信息披露制度；（2）督导发行人及时向保荐机构通报将进行的重大关联交易情况，并对关联交易发表意见
4、督导发行人履行信息披露的义务，审阅信息披露文件及向中国证监会、证券交易所提交的其他文件	（1）督导发行人严格按照《公司法》、《证券法》、《上海证券交易所科创板股票上市规则》等有关法律、法规及规范性文件的要求，履行信息披露义务；（2）在发行人发生须进行信息披露的事件后，审阅信息披露文件及向中国证监会、上海证券交易所提交的其他文件
5、持续关注发行人募集	（1）督导发行人执行已制定的《募集资金管理制度》等制度，

主要事项	具体计划
资金的专户存储、投资项目的实施等承诺事项	保证募集资金的安全性和专用性；（2）持续关注发行人募集资金的专户储存、投资项目的实施等承诺事项；（3）如发行人拟变更募集资金及投资项目等承诺事项，保荐机构要求发行人通知或咨询保荐机构，并督导其履行相关信息披露义务
（二）保荐协议对保荐机构的权利、履行持续督导职责的其他主要约定	（1）定期或者不定期对发行人进行回访、查阅保荐工作需要的发行人材料；（2）列席发行人的股东大会、董事会和监事会；（3）对有关部门关注的发行人相关事项进行核查，必要时可聘请相关证券服务机构配合
（三）发行人和其他中介机构配合保荐机构履行保荐职责的相关约定	（1）发行人已在保荐协议中承诺配合保荐机构履行保荐职责，及时向保荐机构提供与本次保荐事项有关的真实、准确、完整的文件；（2）接受保荐机构尽职调查和持续督导的义务，并提供有关资料或进行配合
（四）其他安排	无

（以下无正文）

(本页无正文,为《国泰君安证券股份有限公司关于杭州安恒信息技术股份有限公司首次公开发行股票并在科创板上市之上市保荐书》之签章页)

项目协办人:

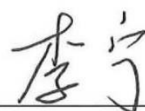


赵炜华

保荐代表人:

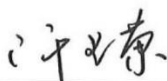


余 姣



李 宁

内核负责人:



许业荣

保荐业务负责人:



朱 健

法定代表人/董事长:



杨德红



国泰君安证券股份有限公司

2019年6月25日