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 2020 年度向特定对象发行 A 股股票并在科创板上市

之

上市保荐书

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）

二〇二一年六月

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 2020 年度

向特定对象发行 A 股股票并在科创板上市之上市保荐书

上海证券交易所：

杭州安恒信息技术股份有限公司（以下简称“安恒信息”、“发行人”或“公司”）拟申请向不超过 35 家的特定对象发行不超过 22,222,222 股（含本数）的人民币普通股股票（以下简称“本次证券发行”、“本次发行”或“本次向特定对象发行 A 股股票”），国泰君安证券股份有限公司（以下简称“国泰君安”）接受杭州安恒信息技术股份有限公司委托，担任安恒信息本次发行 A 股股票的保荐机构（以下简称“本保荐机构”、“本机构”或“保荐机构”）。

本保荐机构及保荐代表人根据《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“《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》等有关法律、行政法规和中国证券监督管理委员会（以下简称“证监会”）、上海证券交易所（以下简称“上交所”）的规定，诚实守信，勤勉尽责，严格按照依法制定的业务规则和行业自律规范出具上市保荐书，并保证所出具文件真实、准确、完整。

（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 2020 年度向特定对象发行 A 股股票募集说明书》中相同的含义。）

一、发行人基本情况

（一）发行人基本信息

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：	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）。
联系电话：	0571-28898076
公司传真：	86-571-28898076
公司网址：	http://www.dbappsecurity.com.cn
公司邮箱：	ahxx@dbappsecurity.com.cn

（二）发行人主营业务

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。

报告期内，公司主营业务未发生重大变更。

（三）发行人主要产品及服务

“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。

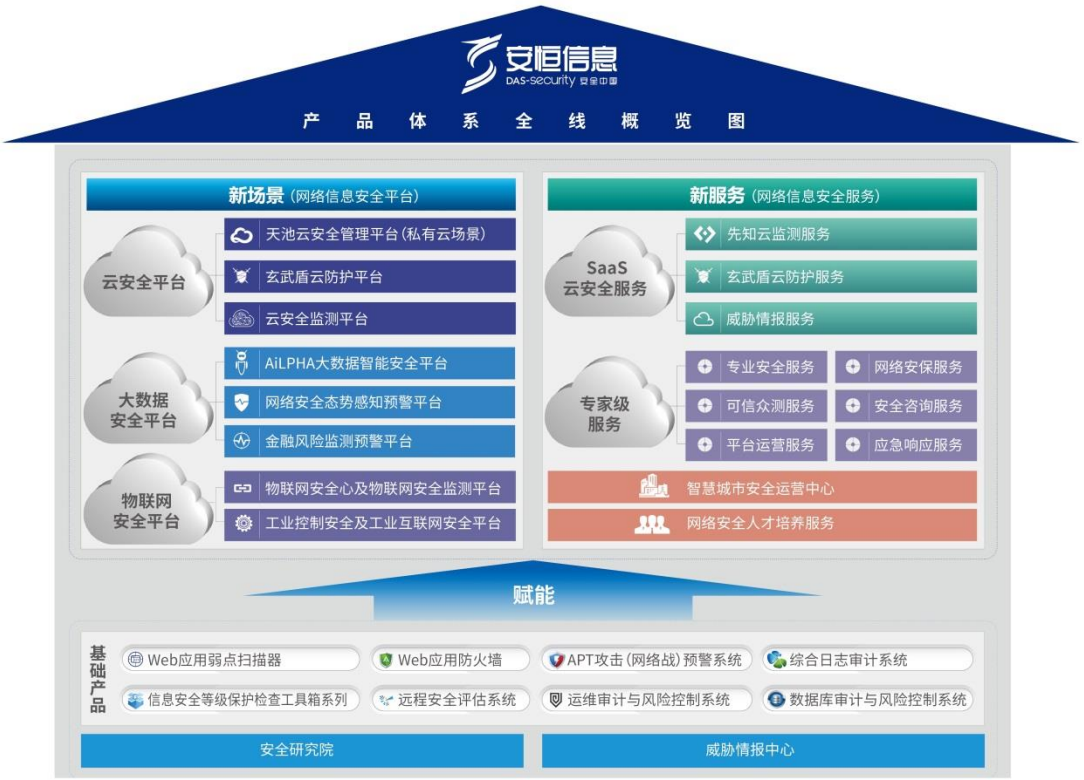
公司始终重视核心技术研发的作用，并将每年营收的 20%作为研发投入，采用研发中心和研究院双线创新机制，取得了较好的成效。

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。
		数据库审计与风险控制系统	专业级的数据库协议解析设备，能够对进出核心数据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	针对网络流量进行深度分析的一款软硬件一体化

分类	二级分类	主要产品	产品简介
		（网络战）预警平台	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。
		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。

分类	二级分类	主要产品	产品简介
		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	安全咨询服务包括信息系统等级保护咨询、云安全

分类	二级分类	主要产品	产品简介
		服务	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。

（四）核心技术与研发水平

1、核心技术

凭借优秀的技术研发团队及强大的技术创新能力，公司在应用安全和数据安全等领域实现了多项技术突破，截至报告期末，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，报告期内，公司主要针对现有核心技术进行优化，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 万个以上，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。

公司核心技术详细情况如下表所示：

序号	技术名称	技术特点	技术来源	技术创新类型	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	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
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	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
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，精准定位各类安全风险。	自主研发	原始创新	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	成熟稳定

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
					日志审计平台	
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	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
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	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
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，保障数据库的安全运行	自主研发	原始创新	数据库审计与风险控制系统、数据库防火墙等	成熟稳定

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
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	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

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
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	远程安全评估	成熟稳定
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	文件威胁分析平台	基础研究
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	安全服务	基础研究
11	物联网漏洞挖	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	自主研发	原始创新	物联网安全测试服务	基础研

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
	掘与安全威胁预警技术	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				究
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	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
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	自主研发	原始创新	云监测服务（先知） 云防护服务（玄武盾） 威胁情报服务（数据大	成熟稳定

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
		查看。			脑	
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	金融风险监测预警平台	成熟稳定
15	DNS 监测与防	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	自主研发	集成创新	云防护服务（玄武盾）	成熟稳

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
	护技术	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；			威胁情报服务（数据大脑）	定
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	云防护服务（玄武盾）	成熟稳定
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	运维审计与风险控制系统	成熟稳定

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
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	运维审计与风险控制系统	成熟稳定
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	运维审计与风险控制系统	成熟稳定
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全管理与审计的各个行业。	自主研发	集成创新	运维审计与风险控制系统	成熟稳定

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
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	Web 应用防火墙	成熟稳定
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	Web 应用防火墙	成熟稳定
23	使用应用层深	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	自主研发	集成创新	Web 应用防火墙	成熟稳

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
	度特征检测与机器学习建模双重互补机制的安全引擎	猜解绕过，针对 cookie 进行加密和校验的防护方法；				定
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	天池云安全管理平台	成熟稳定
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	天池云安全管理平台	成熟稳定
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	自主研发	原始创新	APT 攻击（网络战）预警平台	成熟稳定

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
		测效率优异、报告丰富的特点				
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	APT 攻击（网络战）预警平台	成熟稳定
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	自主研发	原始创新	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

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
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	主机与终端安全管理系统	成熟稳定
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	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
31	物联网终端防护、分析与取证技术	主要包括:摄像头物联网拟态防护技术；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。	自主研发	原始创新	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
32	Web 漏洞扫描	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	自主研发	原始创新	漏洞扫描系列产品	成熟稳

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
	技术	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。				定
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	网站安全监测平台	成熟稳定
34	漏洞扫描爬虫	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	自主研发	原始创新	漏洞扫描系列产品	成熟稳

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
	技术	网站 URL 和不会对被扫描网站产生影响				定
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	漏洞扫描系列产品	成熟稳定
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	数据库漏洞扫描系列产品	成熟稳定
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	网络安全态势感知通报预警平台	成熟稳定

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
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	网络安全态势感知通报预警平台	成熟稳定
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	网络安全态势感知通报预警平台	成熟稳定

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
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	网络安全态势感知通报预警平台	成熟稳定
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	网络安全态势感知通报预警平台	成熟稳定

序号	技术名称	技术特点	技术来源	技术创新类型	相关产品和服务	所处阶段
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	工控安全监测审计平台,	成熟稳定
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	工控漏洞扫描平台工控安全监测审计平台	成熟稳定
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	集成创新	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
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	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
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	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	网络安全事件应急处置工具箱	成熟稳定
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	信息安全等级保护检查工具箱	成熟稳定

2、研发水平

报告期内，研发费用及占营业收入比例具体情况如下：

单位：万元

项目	2021 年 1-3 月		2020 年度		2019 年度		2018 年度	
	金额	占营业收入比	金额	占营业收入比	金额	占营业收入比	金额	占营业收入比
研发费用	9,884.91	53.73%	31,172.50	23.56%	20,453.95	21.67%	15,195.19	24.25%

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 2021 年 3 月 31 日，公司共拥有 48 项核心技术，研发人员数量达 998 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。

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。

（四）主要经营和财务数据及指标

最近三年及一期，公司主要经营和财务数据及指标如下，其中，2021 年 1-3 月/2021 年 3 月 31 日数据未经审计：

1、合并资产负债表的主要数据

单位：万元

项目	2021.03.31	2020.12.31	2019.12.31	2018.12.31
资产总计	216,036.85	246,312.29	217,217.27	89,189.45

负债合计	**59,593.01**	**79,107.20**	62,180.62	38,477.31
归属于母公司所有者权益合计	**156,223.86**	**166,942.90**	155,036.65	50,686.16
所有者权益合计	**156,443.84**	**167,205.10**	155,036.65	50,712.14

2、合并利润表主要数据

单位：万元

项目	2021 年 1-3 月	2020 年度	2019 年度	2018 年度
营业总收入	**18,397.03**	**132,297.27**	94,403.29	62,658.68
营业总成本	**33,777.91**	**125,809.60**	90,238.00	60,851.36
营业利润	**-14,448.85**	**13,978.30**	9,212.39	7,401.87
利润总额	**-14,533.57**	**13,094.31**	9,101.41	7,520.99
净利润	**-12,759.37**	**13,179.20**	9,217.32	7,573.87
归属于母公司所有者的净利润	**-12,613.05**	**13,411.55**	9,222.04	7,687.47

3、合并现金流量表主要数据

单位：万元

项目	2021 年 1-3 月	2020 年度	2019 年度	2018 年度
经营活动产生的现金流量净额	**-34,517.75**	**27,999.39**	21,651.61	9,598.26
投资活动产生的现金流量净额	**-520.01**	**-39,743.08**	-11,919.69	879.93
筹资活动产生的现金流量净额	**-537.25**	**-5,483.43**	98,847.99	7,378.41
汇率变动对现金的影响	**-**	**0.03**	0.03	0.08
现金及现金等价物净增加额	**-35,575.01**	**-17,227.09**	108,579.94	17,856.67

4、财务指标

指标	2021.03.31	2020.12.31	2019.12.31	2018.12.31
流动比率（倍）	**3.28**	**2.83**	3.71	2.22
速动比率（倍）	**3.00**	**2.66**	3.48	2.06
资产负债率（母公司）	**29.04%**	**34.09%**	28.45%	40.63%
资产负债率（合并）	**27.58%**	**32.12%**	28.63%	43.14%
归属于母公司股东的每股净资产（元/股）	**21.09**	**22.54**	20.93	9.12

指标	2021 年 1-3 月	2020 年度	2019 年度	2018 年度
应收账款周转率（次/年）	0.69	5.50	5.09	4.46
存货周转率（次/年）	0.72	3.56	3.50	4.80
归属于母公司股东的净利润（万元）	-12,613.05	13,411.55	9,222.04	7,687.47
归属于母公司股东扣除非经常性损益后的净利润（万元）	-13,035.03	12,075.70	7,959.43	5,782.18
研发投入占营业收入的比例	53.73%	23.56%	21.67%	24.25%
每股经营活动产生的现金流量（元/股）	-4.66	3.78	2.92	1.73
每股净现金流量（元/股）	-4.80	-2.33	14.66	3.21

注：流动比率＝流动资产/流动负债
速动比率＝（流动资产－存货）/流动负债
资产负债率（母公司）＝母公司负债总额/母公司资产总额×100%
资产负债率（合并）＝合并负债总额/合并资产总额×100%
应收账款周转率＝营业收入/应收账款平均余额
存货周转率＝营业成本/存货平均余额
每股经营活动产生的现金流量＝经营活动产生的现金流量净额/期末股本总额
每股净现金流量＝现金及现金等价物净增加额/期末股本总额
应收账款周转率及存货周转率未作年化处理。

（五）与本次发行相关的风险因素

投资者在评价公司本次发行股票时，除本上市保荐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：

1、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

（1）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，持续保持公司技术领先优势，将可能会延缓公司在关键技术和关键应用上实现突破的进度，导致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 15,195.19 万元、20,453.95 万元及 **31,172.50 万元**，占营业收入的比重分别为 24.25%、21.67%**及 23.56%**。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。

（2）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	2020 年度		2019 年度		2018 年度	
	金额	比例	金额	比例	金额	比例
前三季度	66,020.92	49.90%	47,119.85	49.91%	31,042.77	49.54%
第四季度	66,276.35	50.10%	47,283.44	50.09%	31,615.90	50.46%

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，2018-2020 年度公司的渠道销售收入占主营业务收入的比重分别为 55.93%、58.26%和 58.57%，呈稳定上升趋势。公司产品具有客户集中度较低（2020 年前五大客户销售额占营业收入比为 15.18%，2021 年 1-3 月前五大客户销售额占营业收入比为 17.75%）、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。

（3）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。

（4）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。截至本上市保荐书出具日，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。

（5）财务风险

1）应收账款大幅增加未来发生坏账的风险

截至 2021 年 3 月 31 日，公司应收账款账面价值为 25,481.10 万元，占资产总额 11.79%。2020 年末应收账款余额较 2019 年末应收账款余额增加 39.80%，2019 年末应收账款余额较 2018 年末应收账款余额增加 19.26%。

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。

（6）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。2018-2020年度公司实现收入62,658.68万元、94,403.29万元及132,297.27万元，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1,554.28万元、1,507.60万元、1,958.76万元以及400.27万元。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。

（7）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。

2、可能导致本次发行失败或募集资金不足的因素

（1）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。

（2）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

3、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

（1）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。

（2）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。

二、发行人本次发行情况

（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）发行方式和发行时间

本次发行的股票全部采取向特定对象发行的方式，将在中国证监会同意注册后的有效期内选择适当时机向特定对象发行。

（三）发行对象及认购方式

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。

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。

（四）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。

（五）定价基准日、发行价格及定价原则

本次发行的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。

本次向特定对象发行股票采取询价发行方式，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。

（六）锁定期安排

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。

（七）募集资金数量及用途

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。

（八）上市地点

本次发行的股票拟在上海证券交易所科创板上市交易。

（九）滚存未分配利润的安排

公司本次发行前的滚存未分配利润由本次发行完成后公司的新老股东按照发行后的持股比例共同享有。

（十）本次发行的决议有效期

本次发行的决议自公司股东大会审议通过本次发行方案之日起 12 个月内有效。若国家法律、法规对向特定对象发行股票有新的规定，公司将按新的规定进

行相应调整。

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

杨佳佳先生：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。曾主持或参与锐奇工具 IPO、万和电气 IPO、恒立液压 IPO、大理药业 IPO、海螺水泥公司债、林华医疗 IPO 等项目。

水耀东先生：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。曾主持或参与安恒信息 IPO、金能科技 IPO、国栋建设 IPO、上海航空 IPO、凌云 B 股、粤华包 B 股、太阳纸业 IPO、九阳股份 IPO、正泰电器 IPO、长城汽车 IPO、京天利 IPO、乐歌股份 IPO、四川全兴公开增发、东方明珠公开增发、申能股份公开增发、青岛啤酒可分离债、上风高科非公开发行、菲达环保非公开发行、广电网络非公开发行、九阳股份非公开发行、百视通换股吸收合并东方明珠、上海机场资产置换、青岛金王重大资产重组、厦门港资产重组、英科医疗可转债、福莱特可转债、乐歌股份可转债等项目。

（二）项目协办人及其他项目组成员

项目协办人：陈泽森

陈泽森先生，国泰君安助理董事。曾参与安恒信息首次公开发行股票并上市项目、伯特利公开发行可转债、苏盐井神重大资产重组等项目，在执业过程中严格遵守《证券发行上市保荐业务管理办法》等相关规定，执业记录良好。

其他项目组成员：林飞鸿、夏静波、乔梁、胡时阳、田昕、王依、是航等。

四、保荐机构与发行人之间不存在可能影响公正履行保荐职责情形的说明

经核查，本保荐机构与发行人之间不存在可能影响公正履行保荐职责的情形：

（一）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：

国泰君安证裕投资有限公司（参与跟投的本机构依法设立的相关子公司）在发行人首次公开发行中获得配售股票数量为 740,741 股，截至本上市保荐书出具日，国泰君安证裕投资有限公司持有发行人配售股票 740,741 股。除上述事项外，截至本上市保荐书出具日，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）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：

截至本上市保荐书出具日，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）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：

截至本上市保荐书出具日，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、在发行人任职的其他情况。

（四）保荐机构的控股股东、实际控制人、重要关联方与发行人控股股东、实际控制人、重要关联方相互提供担保或者融资等情况：

截至本上市保荐书出具日，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）关于保荐机构与发行人之间其他关联关系的说明：

保荐机构与发行人之间不存在影响保荐机构公正履行保荐职责的其他关联关系。

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。

本保荐机构同意推荐发行人本次证券发行上市，具备相应的保荐工作底稿支持，并据此出具本上市保荐书。

（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、上交所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本次发行提供服务的其他中介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、保证本上市保荐书、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、行政法规和中国证监会、上交所的规定和行业规范；

8、自愿接受中国证监会、上交所依照《保荐管理办法》采取的监管措施；

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，本保荐机构认为，发行人符合《公司法》《证券法》《注册办法》《上市规则》等法律、法规及规范性文件的相关规定。本次发行申请文件不存在虚假记载、误导性陈述或重大遗漏。发行人内部管理良

好、业务运行规范，具有良好的发展前景，募集资金投向属于科技创新领域，具备上市公司向特定对象发行股票并在科创板上市的基本条件。因此，本机构同意向贵所推荐发行人本次向特定对象发行股票。

七、本次证券发行上市履行的决策程序

本保荐机构对发行人本次发行履行决策程序的情况进行了核查。经核查，本保荐机构认为，发行人本次发行已履行了《公司法》《证券法》和中国证监会及上交所规定的决策程序，具体情况如下：

发行人于 2020 年 12 月 25 日召开的第一届董事会第二十三次会议审议通过了《关于公司符合向特定对象发行 A 股股票条件的议案》、《关于公司本次向特定对象发行 A 股股票方案的议案》、《关于公司 2020 年度向特定对象发行 A 股股票预案的议案》、《关于公司向特定对象发行 A 股股票方案的论证分析报告的议案》、《关于公司向特定对象发行 A 股股票募集资金使用的可行性分析报告的议案》、《关于公司前次募集资金使用情况专项报告的议案》、《关于公司向特定对象发行 A 股股票摊薄即期回报与填补措施及相关主体承诺的议案》、《关于公司未来三年（2020 年-2022 年）股东分红回报规划的议案》、《关于提请股东大会授权董事会全权办理本次向特定对象发行 A 股股票具体事宜的议案》等与本次发行相关的议案。

发行人于 2021 年 1 月 11 日召开的 2021 年第一次临时股东大会以现场投票和网络投票相结合的方式，审议通过了与本次发行相关的一系列议案。

2021 年 5 月 21 日，本次发行已经上交所审核通过。根据《公司法》、《证券法》以及《保荐办法》、《注册办法》等相关法律、法规和规范性文件的规定，本次发行尚需获得中国证监会注册同意。在获得中国证监会注册同意后，发行人将向上交所和登记公司申请办理股票发行和上市事宜，完成本次发行的全部呈报批准程序。

八、保荐机构关于本次募集资金投向属于科技创新领域的专项意见

（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。2018-2020 月，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 20%，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 2021 年 3 月 31 日，公司共拥有 48 项核心技术，拥有已授权专利超过 200 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、安全计算沙箱以、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、网络安全培训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，以顺应当前政治局面与科技变革。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、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；本次网络安全培训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。

（四）核查意见

经核查，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。本次募集资金投向属于科技创新领域。

九、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 2 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控制度	（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控制度；（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资金的专户存储、投资项目的实施等承诺事项	（1）督导发行人执行已制定的《募集资金管理制度》等制度，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

主要事项	具体计划
	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

鉴于上述内容，保荐机构国泰君安证券股份有限公司推荐发行人杭州安恒信息技术股份有限公司股票在贵所上市交易，请予批准！

（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 2020 年度向特定对象发行 A 股股票之上市保荐书》之签章页）

项目协办人：

陈泽森

保荐代表人：

杨佳佳　　水耀东

内核负责人：

刘益勇

保荐业务负责人：

谢乐斌

总经理（总裁）：

王松

法定代表人（董事长）：

贺　青

国泰君安证券股份有限公司

2021 年 6 月 1 日