杭州安恒信息技术股份有限公司

公司代码：688023　　公司简称：安恒信息

2025 年度报告摘要

第一节 重要提示

1、本年度报告摘要来自年度报告全文，为全面了解本公司的经营成果、财务状况及未来发展规划，投资者应当到http://www.sse.com.cn/网站仔细阅读年度报告全文。

2、重大风险提示

公司已在本报告中详细阐述公司在经营过程中可能面临的各种风险和应对措施，本年度业绩亏损的主要原因敬请查阅本报告第三节“管理层讨论与分析”一一四、风险因素(二)业绩大幅下滑或亏损的风险。

3、本公司董事会及董事、高级管理人员保证年度报告内容的真实性、准确性、完整性，不存在虚假记载、误导性陈述或重大遗漏，并承担个别和连带的法律责任。

4、公司全体董事出席董事会会议。

5、立信会计师事务所(特殊普通合伙)为本公司出具了标准无保留意见的审计报告。

6、公司上市时未盈利且尚未实现盈利

□是√否

7、董事会决议通过的本报告期利润分配预案或公积金转增股本预案

公司2025年度拟不进行利润分配，不以资本公积金转增股本。上述利润分配方案已经第三届董事会第二十次会议审议通过，该议案尚需提交公司2025年年度股东会审议。

母公司存在未弥补亏损

√适用□不适用

截至报告期末，公司母公司财务报表中存在累计未弥补亏损人民币393,816,007.96元。根据《中华人民共和国公司法》及《上市公司监管指引第3号一一上市公司现金分红》等相关法律法规的规定，公司不满足实施现金分红的条件。敬请广大投资者注意相关投资风险。

8、是否存在公司治理特殊安排等重要事项

□适用√不适用

第二节 公司基本情况

1、公司简介

1.1公司股票简况

√适用□不适用

公司股票简况				
股票种类	股票上市交易所及板块	股票简称	股票代码	变更前股票简称
A股	上海证券交易所科创板	安恒信息	688023	/

1.2公司存托凭证简况

□适用√不适用

1.3联系人和联系方式

	董事会秘书	证券事务代表
姓名	李沐华	陈子杰
联系地址	浙江省杭州市滨江区西兴街道联慧街188号	浙江省杭州市滨江区西兴街道联慧街188号
电话	0571-28898076	0571-28898076
传真	0571-28898076	0571-28898076
电子信箱	ahxx@dbappsecurity.com.cn	ahxx@dbappsecurity.com.cn

2、报告期公司主要业务简介

2.1主要业务、主要产品或服务情况

公司自设立以来一直专注于网络信息安全领域，当前主营业务为AI+网络安全产品的研发、生产及销售，并为客户提供专业的基于AI的网络信息安全服务。公司的产品及服务涉及安全智能体、AI+网络安全、AI+动态数据安全、AI+安全服务、AI+安全运营、AI的安全等领域。凭借强大的研发实力和持续的产品创新，公司围绕DAS战略，构建新一代AI+安全全生命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。

公司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
AI	垂域模型和智能体	恒脑安全垂域大模型	恒脑安全垂域大模型是安恒信息基于18年网络安全经验积累，基于百亿安全语料、百万安全标注数据经多轮大规模增量预训练和微调而成的安全垂域大语言模型，具备多种参数尺寸规模，可根据各业务场景需求从容切换，以扎实的安全基本功迎接未来无限可能。
		恒脑安全智能体开发平台	恒脑安全智能体开发平台通过自研智能体框架，具备零代码和低代码创建智能体能力，内置各类安全工具、安全插件、安全知识、数据分析、数据转换和各类通用引擎等插件，支持通过MCP协议对接外部资源和服务，任何经过简单培训的服务人员可基于业务场景需求快速构建智能体。
		恒脑安全智能体	恒脑安全智能体面向日常网络安全运营、重大活动保障、数据全生命周期安全、数据流通利用、安全服务等具体网络安全场景，已孵化官方智能体超120个，其中重点智能体包括数据分类分级智能体、告警研判和降噪智能体、恶意邮件检测智能体、API安全智能体、终端数据防泄漏智能体、渗透测试智能体等。
AI+安全	AI+网络安全	安恒云-天池云安全管理平台	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上网络安全、云上密码安全和云上数据安全的综合解决方案，同时深度融合恒脑安全智能体技术，实现AI驱动的智能运营能力，为政务、金融、运营商等行业客户构建自主可控、合规高效的全栈云安全防护体系。
		安恒云-天池等保一体机	专为中小型客户等保合规需求打造的软硬一体化产品，通过深度集成等保所需的多种安全能力及特色的等保自测评功能，融入AI等保测评智能能力，以国产化自主可控、极简架构和轻量化交付特性，助力用户快速、高效、低成本的完成合规建设。
		AiLPHA安全分析与管理平台	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，核心依托AI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。增加扩展组件轻量终端微应用管理，通过AI算法分析主机多维度数据，精准检测终端主机上的异常行为；终端检测依托AI识别能力，精准识别和检测各种已知和未知的安全威胁，实时监测终端活动并快速响应取证，联动处置安全风险；通过AI欺骗防御技术实现终端伪服务感知扫描探测和诱捕攻击源，延缓攻击、降低风险。通过大数据智能安全平台打通流量与终端数据建立关联关系，依托AI算法精准定位告警源并溯源攻击路径。
		AiLPHA智能风险评估系统	一款基于入侵与攻击模拟技术，以安全设备策略有效性验证和风险度量为核心的安全设备评估系统，融入AI智能算法，具备安全设备验证，纵深防御体系验证与编排，资产风险评分算法等核心技术，实现更精准的风险评估与智能度量。
		AiLPHA关键信息基础设施安全保卫平台	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、AI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。该平台能够依托AI能力对网络安全威胁、隐患和事件进行智能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。
		AiLPHA网络安全协调指挥平台	该平台基于大数据分析、AI机器学习等先进技术，通过打造态势感知、信息共享、通报预警、应急指挥、网络安全责任制考核等业务闭环，形成网信部门与公安、通管、CERT等部门高效协同的网络安全态势感知、协调指挥和应急响应工作机制，并实现纵向、横向网络安全信息共享交换，最终建设成为本地区网络安全工作的协调指挥中心。
		AiLPHA公安大数据安全管理中心	一款结合大数据技术和AI智能算法的分析系统，作为公安大数据智能化安全管理的核心枢纽，凭借强大的大数据技术，广泛收集并整合全网安全数据。该系统精心构建了一个集资产管理、基线配置、策略控制及态势感知于一体的全方位安全管理平台，依托AI能力实现三大统一管控：统一安全资产管控、统一安全策略管控、统一安全能力管控。同时，它还确保了三个全覆盖：公安大数据全生命周期的安全防护、主体身份动态鉴证及鉴权行为安全、安全风险生命周期管理的全面覆盖。通过这一系统，公安机关能够显著提升内外部风险的AI智能感知能力、协同安全防护的效能、攻击检测与分析的准确性、违规行为发现的敏锐度、事件应急响应的速度以及态势感知与预警的先进性。
		AXDR高级威胁检测与分析平台	AXDR是一款为高级威胁监测与攻防实战而量身打造的监测类产品。通过网+端的数据采集，依托AI算法实现网端数据的统一采集关联；通过原始告警-聚合告警-安全事件的三层AI智能聚合，使得告警噪音大大降低，告警更加精准；通过22类研判场景及攻击面展示等技术，结合AI分析能力将原始日志与原始告警通过不同维度呈现，帮助安全运维人员更好地对细分领域进行深入分析；同时，通过安全验证(BAS)结合AI智能研判，将告警研判与处置紧密关联起来，即发现告警之后，可以立即通过BAS模块验证是否有安全设备出现策略设置缺失，实现安全闭环。
		明御防火墙	明御@防火墙(DAS-TGFW)是一款集传统防火墙、入侵防御、防病毒、上网行为管控、VPN、威胁情报等安全模块于一体，同时可联合态势感知、EDR等产品进行一体化建设的智能安全网关产品。产品秉持"持续边界安全态势改善"的理念，以用户为核心，以边界、应用、威胁、权限为防护对象，构建以资产为视角的可持续智能安全运营防护体系；依托安恒安全研究院强大的研发实力，能够通过AI智能识别自动发现内网资产、详细识别、归类、管理并实时刷新用户各类软硬件资产；并对用户各类策略进行AI智能分析，将分析结果可视化展示，简化运维管理难度。同时，明御防火墙充分结合AI技术提升整体防御与安全管理能力，包括构建AI智能模型，用于防御高级威胁，未知威胁；自动聚合、归一化并关联来自防火墙自身及网络的多源安全日志，提供攻击者、受害者两个安全日志分析维度进行分展示分析，使用户更全面掌握整体安全事件；内置AI智能客服，助力进行高效的安全运营。
		Web应用防火墙	明御?Web应用防火墙(简称“WAF”)是一款专注为网站、APP等Web应用提供安全防护的专业应用安全防护产品。能够对网站及APP业务流量进行多维度、深层次的安全检测和防护。系统内置五大安全引擎(包括语义分析引擎、BOT防护引擎、威胁情报引擎、行为分析引擎、基础特征引擎)，依托AI算法优化引擎能力，可通过主动防护与被动安全相结合的方式智能识别可疑、已知、未知安全威胁，有效保障网站及APP业务安全、可靠运行。
		综合日志审计系统	收集各类网络设备、安全设备、主机及业务系统的相关日志，通过对日志深度、精细化的解析，结合AI驱动的跨事件/设备的关联分析，智能识别网络环境和业务系统中存在的安全风险，同时日志审计系统可提供网络故障排查、基于日志的业务数据分析、内部审计等多种能力。归一化的日志和业务数据，可为第三方平台如态势感知、数据监管平台、安全管理中心、客户自建系统等提供出色的基础数据服务。
		AiLog用户与实体行为分析系统	AiLog/UEBA核心依托AI机器学习技术，通过收集整合全方位多维度以及用户上下文等数据信息，全局关联，进行行为基线分析和群体异常分析，通过AI机器学习异常检测算法，可以更深层次的进行安全事件洞察，迅速识别异常事件。
		数据库审计与风险控制系统	以全面审计和精确审计为基础，结合AI智能分析技术，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性分析管理，对数据库遭受到的风险行为进行实时智能告警，如SQL注入攻击、高危操作等。同时产品支持本地、云上、混合等部署模式，并支持分布式集群管理、用户本次操作审计、TOPSQL执行分析、日志归并分析等能力。
		运维审计与风险控制系统	明御@运维审计与风险控制系统(简称“DAS-USM”)是公司在多年运维安全管理的理论和实践经验积累的基础上，结合各类法律法规对运维审计的要求，采用B/S架构，集"身份认证(Authentication)、账户管理(Account)、控制权限(Authorization)、日志审计(Audit)"于一体，融入AI运维行为异常分析能力，支持多种字符终端协议、文件传输协议、图形终端协议、远程应用协议的安全监控与历史查询，具备全方位运维风险控制能力的统一安全管理与审计产品。
		APT攻击预警平台	明御?APT攻击预警平台(简称“DAS-APT”)是一款集流量威胁检测、恶意文件检测、威胁分析、威胁响应和回溯取证分析于一体的网络流量检测类产品，该产品基于丰富的特征库、全面的检测策略、智能的AI机器学习模型、智能的语义分析、高效的沙箱动态分析、海量的威胁情报等检测能力，实时发现网络未知与已知威胁，提升安全事件感知能力，助力溯源分析及事件取证，不止满足合规要求，更为用户提供实战化攻防检测分析能力，借助恒脑安全智能体强大的自然语言理解与关联分析AI能力，可实现对告警的智能降噪与研判，提升产品检出率，并降低误报率。
		入侵检测系统	明御?入侵检测系统(简称“DAS-NTA”)以全面深入的网络流量解析为基础，通过AI智能语义分析、精准全面的检测规则、多角度AI分析模型、流量异常识别等技术，提供“可信、精准”的网络攻击和威胁事件发现、攻击源与攻击目标定位、攻击行为关联分析等能力，还原网络入侵事件，多维视角实时呈现全网安全态势，为用户网络安全保障工作提供有力支持。
		Web应用漏洞扫描系统	利用漏洞产生的原理和渗透测试的方法，结合AI智能探测算法，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。
		网络安全等级保护检查工具箱	本装备是面向等级保护主体单位、监管检查部门打造的等保网络安全检查专用便携设备，深度契合公安部“十四五”重点装备工具规范技术要求，集规范检查、智能工具调用、检查结果可视化展示于一体，内置定制化专属安全检查工具矩阵，同时创新搭载AI等保测评能力，实现等保检查全流程数字化、智能化升级，大幅提升检查效率与测评专业性，全方位满足等保合规检查、日常监管核查、主体单位自查等多元场景需求。
		明鉴漏洞扫描系统	可针对系统、Web、数据库进行深入扫描，同时涵盖基线配置核查、镜像扫描、工控扫描、弱口令检测、勒索与风险监测、EXP渗透取证以及资产与服务识别等多项内容。该系统支持主动发包扫描方式，能精准发现网络中各主机、设备、应用、数据库镜像等存在的网络信息安全漏洞；同时提供不发包的模式，结合资产台账信息联动本地漏洞库或利用AI智能体联动外部官方漏洞自动预警漏洞，进而形成能够适应不同业务场景的AI智能机制，自动完成对整体系统的安全评估，为网络信息安全提供坚实保障。
		网络安全事件应急处置工具箱	面向网络安全应急响应场景打造的一体化专业处置装备，可全程标准化指导应急处置操作步骤，精准匹配不同安全事件场景下的工具调用、知识支撑需求，高效助力事件现场取证溯源、系统快速恢复。装备创新新增应急处置AI智能体核心能力，可自动采集现场全量数据，通过智能体联动30余款云端专业分析工具，实现溯源分析、问题定位全流程智能化，报告一键生成，大幅提升应急处置效率与专业性，让网络安全事件应急响应更高效、更精准、更规范。
		安恒资产脆弱性扫描与管理平台	基于攻击者视角、以快速理清资产和高效管理漏洞为目标的资产与风险统一管理平台。平台可兼容多品牌资产探测工具及扫描器，并进行全维度资产测绘，理清所有资产；平台基于AI权重自适应调整的弱点优先级分析技术，可快速分析海量弱点数据，并可联动威胁情报，及时捕捉威胁；同时基于用户组织架构，构建灵活的工单管理流程，推进漏洞处置闭环，完成资产与漏洞的全生命周期管理，帮助用户构建有效的资产风险管理机制。
		安恒资产攻击面管理平台	为了满足安全建设成熟度较高客户的打通资产数据孤岛，资产风险暴露面收敛的合规及业务驱动需求，我们建设统一数字化资产中台，依托AI技术实现多源资产数据采集融合、资产互联网访问链路还原、资产风险健康度分析、安全设备覆盖率度量和漏洞全生命周期管理。聚焦事前资产识别和风险管理，通过AI智能分析帮助用户的安全部门解决资产质量治理、互联网风险暴露面监测和场景化风险评估等问题。
		迷网系统	一种对攻击者进行欺骗的威胁检测防御系统，融入AI攻击行为智能分析技术，通过布置诱饵主机、网络服务，诱使攻击者实施攻击，对攻击行为进行智能捕获和深度分析，并通过技术和管理手段来增强实际系统的安全防护能力。
	AI+动态数据安全	AiSort数据安全分级与风险评估系统	AiSort基于网络嗅探技术，充分发现网络环境中存在的数据库资产，核心基于深度学习+条件随机场等AI识别模型算法，依据内置的法规、行业标准，对敏感数据进行AI智能识别和自动分类分级，生成数据资产目录。同时对数据库系统用户权限、弱口令、安全配置基线、安全漏洞和威胁等全方位梳理，进行智能化风险评估。
		AiMask数据脱敏系统	AiMask采用AI算法优化的独有的脱敏与水印溯源算法，对敏感数据进行去标识化、匿名化处理。支持固定值替换、置空、乱序、统计特征保留的脱敏算法和数据溯源算法。通过AI智能适配，保证脱敏后的数据保留原有业务逻辑特征的同时保证数据的有效性和可用性，支持可回溯的脱敏算法，便于用户追溯泄漏源。所有敏感数据全部在内存中处理，可保证整个环节敏感数据不落地，使脱敏后的数据可以安全的应用于测试、开发、分析和第三方大数据分析等环境。
		AiGate数据安全网关系统	AiGate是公司在多年数据安全访问控制理论和实践经验积累的基础上，集访问控制、动态脱敏、漏洞防护、运维管控等多种功能一体的产品，融入AI异常访问行为识别能力，有效防止未授权人员接触敏感数据，大大降低数据泄露的风险。
		AiDLP数据防泄漏系统	AiDLP数据防泄漏系统(网络DLP)是专为企事业单位打造的数据安全产品，旨在保护核心和重要数据。基于流量解析还原和AI驱动的敏感数据识别打标技术，系统自动识别传输中的敏感数据，监控预警违规使用行为，避免核心数据违反安全策略规定流出。一旦数据泄露事件发生，系统可通过AI算法快速进行溯源分析，协助企事业单位迅速定位泄露源头。
		AiAAS API风险监测系统	AiAAS API风险监测系统是一款能够对API数据进行保护和管理的专业型数据安全产品。系统以流量解析还原和AI敏感数据识别打标为基础，自动梳理业务系统API以及操作用户，通过AI算法自动分析业务系统API中可被利用的脆弱性，实时监测用户异常访问数据行为，并且支持在泄露发生时进行智能化溯源分析，全方面守护组织的API数据安全。
		AiCheck数据安全评估系统	AiCheck数据安全评估系统(数据安全检查工具箱)是开展数据安全检查评估工作的一体化专用便携式检查评估装备，具有规范检查、工具调用、结果展示等功能，融入AI智能检查评估能力，提供专业检查知识和检查方法，提高数据安全检查的常态化、标准化和规范化水平。
		安恒数盾安全隔离与信息单向导入系统	安恒数盾安全隔离与信息单向导入系统(简称：AiFGAP)放置在不同安全级别网络之间。通过物理单向光通道，从低安全域采集数据传输到高安全域，或将高安全域数据发布到低安全域使用。此过程中无任何反向光信号传输物理通道，既实现了两网之间的信息单向传输需求，又在物理硬件上彻底保证了高安全域机密数据无法泄露到低安全域。
		安恒数盾数据安全交换系统	安恒数盾数据安全交换系统(简称：AiDEP)是实现不同网域间业务系统跨网交换需求的产品。采用前、后置主机结构，需搭配隔离网闸AiGAP或单向光闸AiFGAP组合使用。系统前、后置机对外分别接入内、外网业务系统，提供标准的跨网交换应用接口，对内通过接入隔离网闸或单向光闸以私有协议接口进行数据摆渡，达到应用数据跨网交换的效果。
		安恒数盾安全隔离与信息交换系统	安恒数盾安全隔离与信息交换系统(简称：AiGAP)放置在可信网络和不可信网络之间，通过专用隔离硬件实现网络间物理隔离效果的同时，达到信息可控交换的目的；通过基于硬件设计的反射GAP系统，实现高速实时的数据交换，同时可以防止各种基于网络层和操作系统层的攻击，使数据跨域交换更安全、更高效、更省心。
		API安全网关系统	安恒API安全网关系统是一款部署在应用客户端和应用服务器之间的全场景API安全防护产品，在不改造现网API的情况下，通过反向代理模式，统一为API提供访问身份认证、权限控制、访问监控、数据脱敏、流量管控、流量加密等机制，融入AI异常访问行为识别与攻击智能拦截能力，通过阻止大部分的潜在攻击流量，使其无法到达真正的API服务侧，并对API访问进行全程智能监控，保障API的安全调用及访问可视。
		数据安全管控平台	数据安全管控平台以数据和身份为中心，依托AI可视化与智能分析技术，展示数据资产详情、数据分类分级、敏感数据访问、数据流向、数据访问热度、数据风险及安全事件处置等内容。平台提供数据资产发现、敏感数据发现、数据账号权限发现、AI自动化数据分级分类、数据安全策略集中管理和下发、数据安全事件智能运营等能力，同时提供数据安全访问控制、风险监测实时告警、数据脱敏、全生命周期数据审计、AI异常行为分析及数据交换共享的合规性监控能力，从而实现数据安全管理、技术防护和安全运营的有效协同，构建深化数据安全风险模型和度量指标体系，完善数据安全态势场景覆盖面，形成专业化的数据安全管理解决方案。
	AI+安全服务	AI安服数字员工	AI安服数字员工(安小龙)，是数字员工与恒脑平台深度融合的可独立交付的SaaS订阅服务产品，作为新一代AI安全基础设施的核心组成部分，已累计发布涵盖数据安全、安全运营、合规审计、威胁分析、代码审计等领域的数十款垂直场景智能体系统，沉淀安恒信息深厚的场景化知识与自动化能力。标志着安全服务从“专家驱动”迈向“人机协同”的新范式。产品由安全智能体基于安恒信息18年专业安全服务实战经验，自主规划与实施安全服务任务，为用户提供智能、高效的安全服务体验。 AI安服数字员工面向用户界面为GUI客户端，云端调用基于安全智能体的分析引擎，对接标准MCP(模型上下文协议)工具上百款，包括从渗透测试到应急响应高级威胁分析，再到软件供应链代码审计，从数据安全风险评估到安全运营规划设计，从MSS安全运营到数字教师等数字安服员工角色。
		智能安全服务	基于智能体与数字员工的数字化能力，打造并推出10项标准化智能服务产品，包括渗透测试、代码审计、应急响应、数据安全风险评估、数据安全管理制度专家、大模型合规安全风险评估、等级保护自评估、安全运营中心规划设计、安全运营成熟度评估、数字安全教师等服务，实现了从“项目定制”到“标准产品”的交付模式升级，完成从“出卖时间”到“交付成果与智慧”的根本性跨越，安服团队成为基于智能体的“安全价值运营商”，从项目交付转向持续性、结果性的安全运营。
	AI+安全运营	AI安全托管运营服务	AI安全托管运营服务(MSS)是以资产发现及闭环管理、外部攻击暴露管理(EASM)、漏洞及弱口令管理、威胁检测与响应、邮件安全监测等场景化服务为核心，依托统一的AI技术底座以及智能的AI数字运营工程师，将专业化运营经验、智能化运营工具、场景化运营流程紧密结合，形成的从“攻击面发现一风险评估一威胁处置一管理闭环”的全流程智能安全服务，为用户构建起7×24小时持续、主动、高效、可靠的智能安全运营体系。
		AiLPHA态势感知平台	公司核心产品AiLPHA态势感知平台通过接入智能体，实现告警研判、处置自动化，具备从海量告警中识别有效攻击行为大幅提升了安全运营效率。
		AiLPHA智能安全运营平台	AiLPHA智能安全运营平台通过接入智能体，实现AI驱动的自动化编排与智能研判，对海量安全数据实现一体化处理，精准识别潜在威胁并快速响应，有效支撑从日常安全运维到重大事件处置的全流程闭环。
		AiLPHA安全编排与协同响应管理平台	AiLPHA智能编排与协同响应平台是一款结合大数据技术和AI智能算法的安全运营系统，平台可通过AI驱动的智能灵活编排，把人、过程和技术整合起来，大幅提升安全运营工作效率，将分析人员从耗时且重复的分析工作中解放出来。支持拖拽式交互设计安全风险分析研判策略和联动响应剧本，支持多种AI策略编排动作，包括但不限于关联验证、告警聚合、联动、阻断。支持联动大量不同类型的安全设备，支持策略下发生成跟踪任务，任务执行过程中可加入安管人员控制环节。通过AI能力将人工分析经验沉淀为标准流程，不断优化响应流程，减少对人工的依赖，流程化完成事件管理，提高协作沟通效率，将响应时间从小时甚至天降低到分钟级别。
		AiLPHA一体化全链路网络安全监督管理与运营平台	适用于电子政务、行业主管和集团客户，满足多级安全监督管理，整体安全运营管理需求，依托AI智能算法实现告警提质降噪，运营降本增效。落实跨平台连接统一入口，跨部门参与齐抓共管，跨网络管理整体防御。提供安全监督检查通报工作机制的系统化流程和规范化制度保障，提供以应用为中心的AI驱动威胁实时监测，风险闭环管理，云上云下安全一体化管控。
AI的安全	大模型风险检测	大模型风险评估系统(智鉴)	大模型风险评估系统是一款专业大模型风险检测与管理平台，旨在精准评估并有效缓解大模型在数据处理、模型构建以及应用部署等全流程中潜藏的各类风险。该系统具备全生命周期的风险监测能力，全面覆盖大模型从开发、训练到部署、应用的各个关键阶段，为其提供无缝的安全保障。 系统聚焦于解决合规性、内容安全、数据泄露以及对抗攻击等核心挑战。采用全链路AI资产管理与多维度风险探测引擎，实现了对大模型底层系统、中间件、API以及业务组件的自动化深度扫描，能够精准识别其中存在的漏洞和敏感数据。同时，系统结合先进的提示词工程、RAG知识库以及多模型判定技术，模拟指令注入、角色扮演等复杂的对抗攻击场景，动态检测生成内容的合规性。凭借这些前沿技术和创新方法，安恒大模型风险评估系统为大模型的安全合规运行与持续优化提供了权威、高效的解决方案，让企业在使用大模型时更加安心、放心。
	大模型风险防护	AI全链路安全防护围栏	AI全链路安全防护围栏聚焦AI全生命周期安全防护需求，覆盖模型、工具、智能体全域安全场景。针对大模型应用中频发的敏感数据泄露、提示注入攻击、违规内容输出、供应链风险等问题，构建“九维防护全景”体系，通过安全垂域模型、三大内容安全引擎与网关代理的协同运作，为用户AI应用提供从训练数据、模型运行到内容输出的全链条安全保障，深度适配TC260监管要求及信创环境，助力用户合规、安全地拥抱AI技术。

2.2主要经营模式

1、盈利模式

公司主营业务为AI+网络安全产品的研发、生产及销售，并为客户提供专业的基于AI的网络信息安全服务。公司通过向下游客户销售AI+网络信息安全产品和提供基于AI的网络信息安全服务来实现收入和利润。

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账。

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，实行差异化生产交付模式：软硬件结合产品采用订单驱动式生产和季度预测式生产相结合，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。云产品及服务则采用订阅制交付模式，客户可通过云端灵活订阅安全能力，无需本地部署硬件。

4、服务模式

公司基于自身在应用安全和动态数据安全方面深厚的技术背景和安全实践经验，具备为对网络信息安全服务存在需求的客户提供安全托管运营服务MSS、安恒云-在线订阅式SaaS服务、专家安全服务、国家重大活动网络安保服务、网络空间安全人才培养服务等能力。通常，公司通过项目投标或市场化销售等方式与客户签订相应的年度或单次服务合同，然后通过现场实施或远程服务的方式对客户特定网站、系统提供安全检测防护服务。

5、销售模式

公司在产品销售上采用多级渠道经销、直接销售以及合作分成相结合的方式，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。合作分成模式，则是公司通过开放智能体开发平台给员工、客户、渠道及个体等合作伙伴，并提供相应的培训，鼓励合作伙伴开发各类安全智能体并在智能体商城上架后，通过销售智能体获取收入分成。

2.3所处行业情况

(1). 行业的发展阶段、基本特点、主要技术门槛

网络信息安全是指网络系统(包括硬件、软件、基础设施等)中的数据受到保护，不会由于偶然的或者恶意的原因而遭受未经授权的访问、泄露、破坏、修改、审阅、检查、记录或销毁。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。随着信息技术的迅速发展，特别是云计算、大数据、物联网和人工智能等新一代信息技术的飞速发展，网络信息安全风险全面泛化，种类和复杂度均显著增加。因此，网络信息安全产业范畴也得到不断延伸和拓展，产品与服务种类较传统分类不断得到充实与细化。

从产业链来看，网络信息安全行业的上游主要为工控机、服务器、存储器、芯片及操作系统、数据库等软硬件厂商。产业链上游市场竞争充分，主要参与者均为成熟的全球化厂商，产品更新快，产量充足，产品价格相对稳定，且产品性价比呈上升趋势；中游为提供安全产品、安全服务、安全集成的厂商；下游则是政府、金融、电信、能源等各行业用户。

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。自2016年《中华人民共和国网络安全法》正式施行以来，我国相继颁布《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》等法律法规，出台《网络安全审查办法》《云计算服务安全评估办法》《生成式人工智能服务管理暂行办法》《网络数据安全管理条例》等规章，建立等级保护、安全审查、密码测评、数据安全管理、个人信息保护、生成式人工智能健康发展和规范应用等一批重要制度，逐步形成了具有中国特色的网络安全政策体系，对促进网络安全产业及数字经济发展起到了重要作用。

2025年，中国网络安全政策体系进一步完善，国家对网络信息安全的法律框架和监管力度持续加强。

2025年1月1日，《网络数据安全管理条例》正式施行，作为我国网络数据安全领域首部基础性行政法规，系统承接《网络安全法》《数据安全法》《个人信息保护法》，构建覆盖数据全生命周期的监管框架，细化个人信息保护、重要数据管理、数据跨境流动合规等要求。同月，国家网信办就《个人信息出境个人信息保护认证办法(征求意见稿)》公开征求意见，首次对“出境认证”提出程序性、实质性双重要求。国家发改委、国家数据局、工信部联合发布《国家数据基础设施建设指引》，提出构建多层次、全方位、立体化的国家数据基础设施安全保障框架，贯穿数据生命周期全流程。

2025年3月，国家网信办发布《中华人民共和国网络安全法(修正草案再次征求意见稿)》进行公开征集意见，重点加大违法处罚力度，与《数据安全法》《个人信息保护法》实现责任条款衔接。

2025年5月，公安部发布《网络安全等级保护测评高风险判定实施指引(试行)》，统一全国测评机构“高风险”判定口径，强化重大隐患整改闭环。同月，公安部、国家网信办等六部门发布《国家网络身份认证公共服务管理办法》，推进国家网络身份认证公共服务建设，规范网号、网证申领规则(未成年人需监护人同意)，禁止平台强制索要明文身份信息。

2025年9月1日，由国家网信办等四部门发布的《人工智能生成合成内容标识办法》正式施行，把过去对生成式人工智能/深度合成算法规则中相对原则化的标识要求，升级为可被技术验证、可被执法引用的底线。在合规要求上，把“标识”拆解为显式标识与隐式标识：显式标识面对用户，用文字、声音、图形等可感知方式提示；隐式标识嵌入文件元数据，承载服务提供者与内容编号等要素，面向平台核验与监管追溯。

2025年10月28日，《中华人民共和国网络安全法》修订通过，首次将AI纳入监管，支持人工智能基础理论研究、算法研发，完善伦理规范，加强风险监测评估和安全监管。

2025年11月1日，国家网信办发布的《国家网络安全事件报告管理办法》开始施行，规范网络安全事件报告管理，及时控制网络安全事件造成的损失和危害。

同时，各行业也在2025年相继制定并发布了多项网络安全、数据安全相关的法规和政策文件。

2025年3月，工业和信息化部发布《工业互联网安全分类分级管理办法》，明确工业互联网企业应当按照工业互联网安全定级相关标准规范开展自主定级。

2025年5月，自然资源部发布《地理信息数据分类分级工作指南(试行)》，明确了地理信息数据分类分级原则，并给出重要数据、核心数据识别的判定指标。同月，中国人民银行发布《中国人民银行业务领域数据安全管理办法》，提出业务数据安全工作遵循“谁管业务，谁管业务数据，谁管数据安全”原则。

2025年6月，国务院发布《政务数据共享条例》，落实政务数据共享安全管理主体责任和政务数据分类分级管理要求，保障政务数据共享安全。6月13日，工信部等八部门发布《汽车数据出境安全指引(2025版)(征求意见稿)》，明确汽车数据出境安全评估申报情形。

2025年8月，国家密码管理局、国家网信办、公安部发布《关键信息基础设施商用密码使用管理规定》正式施行，要求运营者应同步规划、同步建设、同步运行商用密码保障系统，每年至少开展一次商用密码应用安全性评估。

2025年9月，交通运输部、国家发改委、工信部等七部门发布《关于“人工智能+交通运输”的实施意见》，要求加强人工智能网络和数据安全合规管理，建立应用安全分级分类管理制度，建立健全网络和数据安全保护体系。

2025年10月，由中国人民银行、中国证监会发布的《金融基础设施监督管理办法》正式施行，要求金融基础设施运营机构建立完善的技术系统及管理机制，加强数据安全管理，承担数据安全管理主体责任。

2025年12月，国家能源局制定发布《能源行业数据安全管理办法(试行)》，规范能源行业数据处理活动，加强数据安全管理，防范数据安全风险，促进数据开发利用。

在网络信息安全政策和技术的双重驱动下，中国网络信息安全行业继续保持较快增长。Gartner发布预测，2026年全球IT支出预计达6.15万亿美元，同比增长10.8%；AI基础设施保持快速增长，AI相关硬件和软件的支出持续攀升。预计2026年服务器支出同比增长36.9%，全球数据中心支出将从2025年近5,000亿美元增加至6,500亿美元以上，增长31.7%。2026年全球软件支出增速预测为14.7%，规模超1.4万亿美元。生成式AI模型支出增速将达到80.8%，2026年其在软件市场份额将提升1.8%。IDC报告《中国IT安全市场预测，2025一2029》认为中国网络安全市场继续保持稳健增长，预计到2026年，整体市场规模有望突破800亿元人民币，2024一2029年复合增长率达到8.9%。

在政策红利和技术驱动的双重作用下，中国网络信息安全行业景气度持续提升，政企客户在网络安全产品和服务上的投入基本稳定。但随着5G、物联网和人工智能等技术的深化应用，最终用户对网络安全产品和服务的需求将进一步提升，推动中国网络信息安全市场实现更高质量的发展。

(2). 公司所处的行业地位分析及其变化情况

公司于2007年成立之初便以应用安全和动态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，公司核心安全产品市场份额持续多年位居行业前列。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。2025年，公司主要产品和服务排名及获得荣誉列举部分如下：

2025年1月，恒脑·网络安全智能体获评2024年浙江省数字经济发展优秀案例。

2025年2月，由公司牵头，联合北京邮电大学、中国电子科技集团公司第三十研究所、中国科学院沈阳自动化研究所共同申报的“恒脑安全垂域大模型和智能体系统研发与产业化项目”作为年度唯一AI+安全项目荣获“2024年度吴文俊人工智能科学技术奖科技进步二等奖”。

2025年3月，Gartner®发布《China Context: ‘Market Guide for Data Security Platforms’》，公司成功入选中国数据安全平台(DSP)领域代表厂商。

2025年5月，IDC发布的《中国IT安全软件市场跟踪报告，2024H2》报告显示，公司在数据安全软件领域位列中国市场第二。

2025年6月，恒脑3.0以总分第一斩获第二届雄安未来之城场景汇“雄安垂直大模型应用大赛”一等奖。

2025年7月，IDC发布《中国AI赋能的Web应用防火墙硬件市场份额，2024：合规需求带动市场反弹，LLM-WAF成为未来市场新增量》报告，显示公司WAF主要市场集中在政府、金融、医疗、教育等行业，排名第三位，市场份额10.0%。同月，IDC发布的《中国数据安全管理平台市场份额，2024：数据安全统一管理成为趋势》(Doc # CHC53592625 ，2025年7月)显示，公司在2024中国数据安全管理平台市场份额位列第一；《中国数据库安全审计市场份额，2024：AI推动智能化审计转型》(Doc #CHC53571325 ，2025年7月)报告显示公司蝉联中国数据库安全审计市场第二的佳绩，连续两年保持行业领先地位。

2025年8月，Gartner®发布中国特权访问管理市场指南，公司凭借明御运维审计与风险控制系统入选Gartner®中国特权访问管理市场指南代表厂商。同月，Gartner®发布的《Market Guide for API Management, China》(《中国 API 管理市场指南》)显示，公司成功入选中国API管理领域代表厂商。

2025年8月，国家数研院发布《数据产业图谱(2025)》，公司入选数据基础设施企业(隐私计算)、数据应用企业(城市治理数据应用)、数据安全企业三大分类；其中，隐私计算位列第一。

2025年10月，国内权威网络安全媒体安全牛正式发布《实战网络靶场应用指南(2025版)》。在该报告中，公司凭借全栈式网络空间安全演训靶场体系，成功入选“优秀案例推荐”与“优秀厂商推荐”双榜单。

2025年10月，Gartner®发布《2025年中国数据、分析和人工智能技术成熟度曲线》报告，公司凭借在AI治理领域的技术实力，被认可为典型厂商(Sample Vendors)。

2025年11月，IDC发布“2025上半年中国软件安全数据追踪表”，公司在数据安全软件领域荣登中国市场第二。

2025年12月，2025年度中国网络安全与信息产业“金智奖”评选结果正式揭晓，公司“人工智能全域安全”解决方案荣获年度创新解决方案，恒脑数据库审计智能体荣获年度AI与数据安全创新应用。

2025年12月，Gartner®发布《数据防泄漏市场指南一一中国篇》，安恒信息及“AiDLP数据防泄漏系统”入选中国DLP代表性厂商。

公司始终坚持DAS战略，不断创新，重视研发创新力度，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。自2014年开始，公司陆续推出了云安全、大数据安全、物联网安全、工业互联网安全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。公司在动态数据安全、信创安全、安全托管运营服务MSS等领域全面发力，市场竞争力不断提升。2025年被视为“AI智能体元年”，安全智能体技术发展进一步加速，公司发布恒脑3.0，基于此开发出的“分类分级智能体”，正从1.0时代的“单环节AI辅助”迈向2.0时代的“全流程AI驱动”，提升分类分级效率60倍；除此之外，公司还打造了包括告警研判和降噪智能体、恶意邮件研判智能体、API安全智能体、终端数据防泄漏智能体、数据安全咨询服务智能体、安全运营咨询服务智能体、数据分类分级智能体、自动化渗透测试智能体、恶意软件检测智能体在内的九大主力智能体。

党的十八大以来，社会各界深入学习贯彻习近平总书记关于网络强国的重要思想，推动我国网络安全战略、政策、法规的体系不断健全。随着数字经济的发展，网络空间与实体社会深度融合，《网络安全法》《数据安全法》《个人信息保护法》《密码法》以及《关键信息基础设施保护条例》《商用密码管理条例》等系列法律法规的出台，为数字时代网络空间治理和数据保护提供坚实的法律保障底座。网络安全国家标准作为网络安全保障体系建设的重要组成部分，在支撑和落实网络安全法律法规、构建网络空间安全、推动网络治理体系变革等方面发挥着基础性、规范性、引领性作用。

公司始终高度重视网络安全标准化工作，截至2025年年末，已累计参与了174项标准的研制，其中包括64项国家标准，64项行业标准，46项地方标准和团体标准；方向覆盖了基础网络安全产品、安全服务、动态数据安全、密码算法安全、云安全、关键信息基础设施保护以及以人工智能、大数据为代表的新技术新应用安全等广泛领域。2025年，安恒信息深度参与研制或做出主要技术贡献的网络安全国家标准已经有13项正式发布，深度参与的网络安全行业标准有5项正式发布。公司也在参与国家网络安全标准体系建设过程中构建起企业自身的技术标准体系，紧跟国家网络安全建设前进的步伐，勾画自身的发展蓝图。

(3). 报告期内新技术、新产业、新业态、新模式的发展情况和未来发展趋势

近年来，我国云计算、大数据、物联网、5G和生成式人工智能等新技术的快速发展，在推动新兴技术市场持续增长的同时，也催生了新的安全需求和应用场景。随着数字化转型的深入和新技术的普及，企业网络边界逐渐模糊，传统的网络安全防护模式已难以应对日益复杂的威胁环境。因此，政府和企业的网络信息安全防护理念正在发生深刻转变，从传统的被动修补模式转向与信息系统建设同步规划、主动防御的新模式。

网络安全产业正经历从“合规驱动”向“价值驱动”的转型升级。报告期内，云安全、动态数据安全、AI安全等新兴细分领域快速崛起，成为产业增长的重要引擎。防护对象从传统的PC、服务器、网络边缘扩展到云计算、大数据、泛终端、智能设备和动态边界；防护思想从“风险发现、查缺补漏”转变为“关口前移、系统规划、主动防御”；核心技术从传统的围墙式防护升级为基于大数据、人工智能、零信任架构和隐私计算等技术的智能化威胁检测与响应体系。安全运营中心(SOC)向智能化、自动化方向演进；隐私计算技术在数据要素流通场景中得到广泛应用。产业边界持续拓展，安全能力与业务场景深度融合，网络安全产业与数字经济发展形成同频共振。同时，安全智能体作为新兴形态开始落地，通过“安全智能体+安全工具”的协同模式，实现安全运营的自主决策与自动化处置，推动安全防护从“工具辅助”向“智能自治”演进。

展望未来，随着数字化转型深入和新技术普及，网络安全将呈现以下趋势：一是智能化，生成式人工智能将深度赋能安全运营，安全智能体成为标配；二是融合化，安全能力与云、网、边、端全面融合，实现内生安全；三是服务化，人机协同的托管安全服务成为主流；四是体系化，从单点防护向“预测-防御-检测-响应”闭环演进，构建主动防御体系。

3、公司主要会计数据和财务指标

3.1近3年的主要会计数据和财务指标

单位：元　币种：人民币

	2025年	2024年	本年比上年增减(%)	2023年
总资产	4,474,428,330.96	5,035,768,395.71	-11.15	4,978,259,985.46
归属于上市公司股东的净资产	2,373,381,373.60	2,509,210,485.75	-5.41	2,559,900,847.15
营业收入	2,151,443,960.34	2,042,835,394.88	5.32	2,170,164,682.12
扣除与主营业务无关的业务收入和不具备商业实质的收入后的营业收入	2,145,215,548.15	2,035,747,382.11	5.38	2,162,549,839.53
利润总额	-12,808,067.55	-175,932,668.73	不适用	-367,375,248.95
归属于上市公司股东的净利润	-57,499,238.94	-197,849,927.16	不适用	-359,805,113.83
归属于上市公司股东的扣除非经常性损益的净利润	-91,534,848.26	-237,183,747.13	不适用	-387,818,496.58
经营活动产生的现金流量净额	352,501,072.87	160,840,916.93	119.16	-255,728,672.23
加权平均净资产收益率(%)	-2.31	-7.83	增加5.52个百分点	-12.60
基本每股收益(元／股)	-0.57	-1.94	不适用	-3.53
稀释每股收益(元／股)	-0.57	-1.94	不适用	-3.53
研发投入占营业收入的比例(%)	20.41	24.11	减少3.70个百分点	29.33

3.2报告期分季度的主要会计数据

单位：元　币种：人民币

	第一季度(1-3月份)	第二季度(4-6月份)	第三季度(7-9月份)	第四季度(10-12月份)
营业收入	311,118,492.11	421,721,452.87	471,668,301.11	946,935,714.25
归属于上市公司股东的净利润	-111,431,603.98	-82,685,144.26	-12,068,666.79	148,686,176.09
归属于上市公司股东的扣除非经常性损益后的净利润	-116,444,528.41	-91,950,139.84	-21,784,851.33	138,644,671.32
经营活动产生的现金流量净额	-276,283,635.13	-45,167,885.44	-4,349,740.40	678,302,333.84

季度数据与已披露定期报告数据差异说明

□适用√不适用

4、股东情况

4.1普通股股东总数、表决权恢复的优先股股东总数和持有特别表决权股份的股东总数及前 10 名股东情况

单位: 股

截至报告期末普通股股东总数(户)	11,655
年度报告披露日前上一月末的普通股股东总数(户)	13,327
截至报告期末表决权恢复的优先股股东总数(户)	0
年度报告披露日前上一月末表决权恢复的优先股股东总数(户)	0
截至报告期末持有特别表决权股份的股东总数(户)	0
年度报告披露日前上一月末持有特别表决权股份的股东总数(户)	0

前十名股东持股情况(不含通过转融通出借股份)

股东名称(全称)	报告期内增减	期末持股数量	比例(%)	持有有限售条件股份数量	质押、标记或冻结情况		股东性质
					股份状态	数量	
范渊	0	13,125,717	12.86	0	无	0	境内自然人
杭州阿里创业投资有限公司	-3,061,102	5,304,289	5.20	0	无	0	境内非国有法人
交通银行股份有限公司—万家行业优选混合型证券投资基金(LOF)	0	5,000,000	4.90	0	无	0	其他
宁波安恒嘉盛投资合伙企业(有限合伙)	0	3,657,216	3.58	0	无	0	其他
宁波安恒投资合伙企业(有限合伙)	0	3,656,250	3.58	0	无	0	其他
香港中央结算有限公司	428,294	3,099,604	3.04	0	无	0	其他
中国工商银行股份有限公司—万家自主创新混合型证券投资基金	500,000	3,000,000	2.94	0	无	0	其他
中国电信集团投资有限公司	0	2,302,455	2.26	0	无	0	国有法人
招商银行股份有限公司—万家经济新动能混合型证券投资基金	700,000	1,500,000	1.47	0	无	0	其他
招商银行股份有限公司—华富中证人工智能产业交易型开放式指数证券投资基金	509,628	509,628	0.50	0	无	0	其他
上述股东关联关系或一致行动的说明				1、截止报告披露之日，公司前十名股东中，宁波安恒投资合伙企业(有限合伙)、宁波安恒嘉盛投资合伙企业(有限合伙)与实际控制人范渊先生签署了《一致行动协议》，除此之外，公司未接到上述股东有存在关联关系或一致行动协议的声明。 2、公司未知上述其他股东之间是否存在关联关系或一致行动的说明。			
表决权恢复的优先股股东及持股数量的说明				无			

存托凭证持有人情况

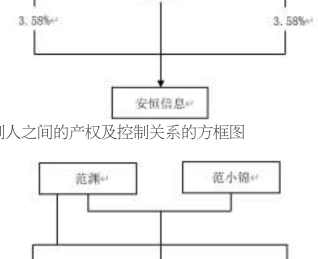
□适用√不适用

截至报告期末表决权数量前十名股东情况表

□适用√不适用

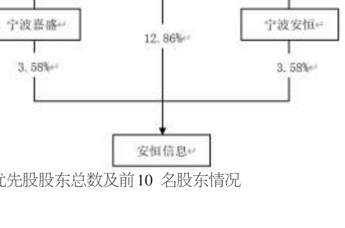
4.2公司与控股股东之间的产权及控制关系的方框图

√适用□不适用



4.3公司与实际控制人之间的产权及控制关系的方框图

√适用□不适用



4.4报告期末公司优先股股东总数及前10 名股东情况

□适用√不适用

5、公司债券情况

□适用√不适用

第三节 重要事项

1、公司应当根据重要性原则，披露报告期内公司经营情况的重大变化，以及报告期内发生的对公司经营情况有重大影响和预计未来会有重大影响的事项。

报告期内，公司实现营业总收入2,151,443,960.34元，比上年同期增长5.32%；实现归属于上市公司股东的净利润-57,499,238.94元，归属于上市公司股东的扣除非经常性损益后的净利润-91,534,848.26元。

2、公司年度报告披露后存在退市风险警示或终止上市情形的，应当披露导致退市风险警示或终止上市情形的原因。

□适用√不适用

证券代码：688023　　证券简称：安恒信息　　公告编号：2026-012

杭州安恒信息技术股份有限公司
关于续聘公司2026年度审计机构的公告

本公司董事会及全体董事保证本公告内容不存在任何虚假记载、误导性陈述或者重大遗漏，并对其内容的真实性、准确性和完整性依法承担法律责任。

重要内容提示：

拟聘任的会计师事务所名称：立信会计师事务所(特殊普通合伙)

杭州安恒信息技术股份有限公司(以下简称“公司”)于2026年3月25日召开了第三届董事会第二十次会议，会议审议通过了《关于续聘公司2026年度审计机构的议案》，拟续聘立信会计师事务所(特殊普通合伙)为公司审计机构，聘期一年。该议案尚需提请公司2025年年度股东会审议。现将相关事宜公告如下：

一、拟聘任会计师事务所的基本情况

(一)机构信息

1、基本信息

立信会计师事务所(特殊普通合伙)(以下简称“立信”)由我国会计泰斗潘序伦博士于1927年在上海创建，1986年复办，2010年成为全国首家完成改制的特殊普通合伙制会计师事务所，注册地址为上海市，首席合伙人为朱建弟先生。立信是国际会计网络BDO的成员所，长期从事证券服务业务，新《证券法》实施前具有证券、期货业务许可证，具有H股审计资格，并已向美国公众公司会计监督委员会(PCAOB)注册登记。

立信2025年业务收入(未经审计)50.00亿元，其中审计业务收入36.72亿元，证券业务收入15.05亿元。截至2025年末，立信拥有合伙人300名、注册会计师2,523名、从业人员总数9,933名，签署过证券服务业务审计报告的注册会计师802名。

2025年度立信为770家上市公司提供年报审计服务，主要行业：制造业、科学研究和技术服务业、信息传输、软件和信息技术服务业、批发和零售业、电力、热力、燃气及水生产和供应业、金融业及建筑业，审计收费总额9.16亿元。

2、投资者保护能力

截至2025年末，立信已提取职业风险基金1.71亿元，购买的职业保险累计赔偿限额为10.50亿元，相关职业保险能够覆盖因审计失败导致的民事赔偿责任。

近三年在执业行为相关民事诉讼中承担民事责任的情况：

起诉(仲裁)人	被诉(被仲裁)人	诉讼(仲裁)事件	诉讼(仲裁)金额	诉讼(仲裁)结果
投资者	金亚科技、周旭辉、立信	2014年报	尚余500万元	部分投资者以证券虚假陈述责任纠纷为由对金亚科技、立信所提起民事诉讼。根据有权人民法院作出的生效判决，金亚科技对投资者损失的12.29%部分承担赔偿责任，立信所承担连带责任。立信投保的职业保险足以覆盖赔偿金额，目前生效判决均已履行。
投资者	保千里、东北证券、银信评估、立信等	2015年重组、2015年报、2016年报	1,096万元	部分投资者以保千里2015年年度报告；2016年半年度报告、年度报告；2017年半年度报告以及临时公告存在证券虚假陈述为由对保千里、立信、银信评估、东北证券提起民事诉讼。立信未受到行政处罚，但有权人民法院判令立信对保千里在2016年12月30日至2017年12月29日期间因虚假陈述行为对保千里所负债务的15%部分承担补充赔偿责任。目前胜诉投资者对立信申请执行，法院受理后从事务所账户中扣划执行款项。立信账户中资金足以支付投资者的执行款项，并且立信购买了足额的会计师事务所职业责任保险，足以有效化解执业诉讼风险，确保生效法律文书均能有效执行。

3、诚信记录

立信近三年因执业行为受到刑事处罚无、行政处罚7次、监督管理措施42次、自律监管措施6次和纪律处分3次，涉及从业人员151名。

(二)项目信息

1、基本信息

项目	姓名	注册会计师执业时间	开始从事上市公司审计时间	开始在立信执业时间	开始为本公司提供审计服务时间
项目合伙人	陈瑜	2007年	2007年	2007年	2016年
签字注册会计师	张显赞	2017年	2017年	2021年	2026年
质量控制复核人	凌燕	2009年	2007年	2009年	2022年

(1)项目合伙人近三年从业情况：

姓名：陈瑜

时间	上市公司名称	职务
2025年	欣灵电气股份有限公司	签字合伙人
2024-2025年	杭州安恒信息技术股份有限公司	签字合伙人
2023-2024年	宁波太平鸟时尚服饰股份有限公司	签字合伙人
2023-2025年	君禾泵业股份有限公司	签字合伙人
2023-2025年	浙江万盛股份有限公司	质量控制复核人
2023-2025年	浙江寿仙谷医药股份有限公司	质量控制复核人
2023-2025年	上海岱美汽车内饰件股份有限公司	质量控制复核人
2023-2024年	浙江炜冈科技股份有限公司	质量控制复核人
2024-2025年	远信工业股份有限公司	质量控制复核人
2024年	浙江汇隆新材料股份有限公司	质量控制复核人

(2)签字注册会计师近三年从业情况：

姓名：张显赞

时间	上市公司名称	职务
2025年	杭州安恒信息技术股份有限公司	现场负责人

(3)质量控制复核人近三年从业情况：

姓名：凌燕

时间	上市公司名称	职务
2023-2025年	浙江万安科技股份有限公司	签字合伙人
2023-2025年	宁波江丰电子材料股份有限公司	签字合伙人
2023-2025年	浙江银轮机械股份有限公司	签字合伙人
2024-2025年	常州银河世纪微电子股份有限公司	签字合伙人
2024-2025年	华纬科技股份有限公司	签字合伙人
2024-2025年	浙江鼎龙科技股份有限公司	签字合伙人
2024-2025年	浙江万丰化工股份有限公司	签字合伙人
2024-2025年	上海通领汽车科技股份有限公司	签字合伙人
2023-2025年	日月重工股份有限公司	质量控制复核人
2023-2025年	杭州安恒信息技术股份有限公司	质量控制复核人

2、项目组成员独立性和诚信记录情况。

项目合伙人、签字注册会计师和质量控制复核人不存在违反《中国注册会计师职业道德守则》对独立性要求的情形。上述人员过去三年没有不良记录。

3、审计费用定价原则

主要基于专业服务所承担的责任和需投入专业技术的程度，综合考虑参与工作员工的经验和级别相应的收费率以及投入的工作时间等因素定价。

公司2025年度财务报表审计收费为115万元，内部控制审计报告收费为20万元。2026年度，董事会提请股东会授权公司管理层按照市场一般情况，综合考虑参与审计工作的项目组成员的经验、级别、投入时间和工作质量综合确定审计费用。

二、拟续聘会计师事务所履行的程序

(一)审计委员会的履职情况

公司董事会审计委员会对立信进行了审查，认为立信符合证券法的规定，具有多年为上市公司进行审计的经验和能力，在执业过程中坚持独立审计原则，切实履行了审计机构应尽的职责，能够客观、公正、公允地反映公司财务状况、经营成果。同意继续聘请其为公司2026年度审计机构并将《关于续聘公司2026年度审计机构的议案》提交公司第三届董事会第二十次会议审议。

(二)董事会的审议和表决情况

2026年3月25日，公司第三届董事会第二十次会议审议通过《关于续聘公司2026年度审计机构的议案》，同意聘任立信会计事务所(特殊普通合伙)为公司审计机构。

本议案尚需公司2025年年度股东会审议批准，并自公司股东会审议通过之日起生效。

特此公告。

杭州安恒信息技术股份有限公司董事会
2026年3月26日

证券代码：688023　　证券简称：安恒信息　　公告编号：2026-018

杭州安恒信息技术股份有限公司
关于召开2025年年度股东会的通知

本公司董事会及全体董事保证公告内容不存在任何虚假记载、误导性陈述或者重大遗漏，并对其内容的真实性、准确性和完整性依法承担法律责任。

重要内容提示：

- 股东会召开日期：2026年4月16日
- 本次股东会采用的网络投票系统：上海证券交易所股东会网络投票系统

一、召开会议的基本情况

(一)股东会类型和届次

2025年年度股东会

(二)股东会召集人：董事会

(三)投票方式：本次股东会所采用的表决方式是现场投票和网络投票相结合的方式

(四)现场会议召开的日期、时间和地点

召开日期时间：2026年4月16日　14点30分

召开地点：杭州市滨江区西兴街道联慧街188号安恒大厦3楼会议室

(五)网络投票的系统、起止日期和投票时间。

网络投票系统：上海证券交易所股东会网络投票系统

网络投票起止时间：自2026年4月16日

至2026年4月16日

采用上海证券交易所网络投票系统，通过交易系统投票平台的投票时间为股东会召开当日的交易时间段，即9:15-9:25，9:30-11:30，13:00-15:00；通过互联网投票平台的投票时间为股东会召开当日的9:15-15:00。

(六)融资融券、转融通、约定购回业务账户和沪股通投资者的投票程序

涉及融资融券、转融通业务、约定购回业务相关账户以及沪股通投资者的投票，应按照《上海证券交易所科创板上市公司自律监管指引第1号 一 规范运作》等有关规定执行。

(七)涉及公开征集股东投票权

不涉及。

二、会议审议事项

本次股东会审议议案及投票股东类型

序号	议案名称	投票股东类型
		A股股东
非累积投票议案		
1	关于公司《2025年年度报告》及摘要的议案	√
2	关于公司2025年度董事会工作报告的议案	√
3	关于公司2025年度财务决算报告的议案	√
4	关于公司2025年度利润分配方案的议案	√
5	关于续聘公司2026年度审计机构的议案	√
6	关于公司未弥补亏损达到实收股本三分之一的议案	√
7	关于公司2025年度独立董事述职报告的议案	√
8	关于确认公司2025年度董事、高级管理人员薪酬的议案	√
9	关于提请股东会授权董事会办理以简易程序向特定对象发行股票的议案	√
10	关于补选非独立董事的议案	√

1、说明各议案已披露的时间和披露媒体

上述议案已经公司于2026年3月25日召开的第三届董事会第二十次会议审议通过，具体内容详见公司于2026年3月26日在上海证券交易所网站(www.sse.com.cn)以及《证券时报》披露的相关公告及文件。

2、特别决议议案：议案9

3、对中小投资者单独计票的议案：议案4、议案5、议案8、议案9、议案10

4、涉及关联股东回避表决的议案：议案8

应回避表决的关联股东名称：作为公司董事、高级管理人员的关联股东对议案8回避表决。

5、涉及优先股股东参与表决的议案：无

三、股东会投票注意事项

(一)本公司股东通过上海证券交易所股东会网络投票系统行使表决权的，既可以登陆交易系统投票平台(通过指定交易的证券公司交易终端)进行投票，也可以登陆互联网投票平台(网址：vote.sseinfo.com)进行投票。首次登陆互联网投票平台进行投票的，投资者需要完成股东身份认证。具体操作请见互联网投票平台网站说明。

(二)为更好地服务广大中小投资者，确保有投票意愿的中小投资者能够及时参会、便利投票。公司拟使用上证所信息网络有限公司(以下简称“上证信息”)提供的股东会提醒服务(即“一键通”)，委托上证信息通过智能短信等形式，根据股权登记日的股东名册主动提醒股东参会投票，向每一位投资者主动推送股东会参会邀请、议案情况等信息。投资者在收到智能短信后，可根据《上市公司股东会网络投票一键通服务用户使用手册》(下载链接：https://vote.sseinfo.com/i/yjt_help.pdf)的提示步骤直接投票，如遇拥堵等情况，仍可通过原有的交易系统投票平台和互联网投票平台进行投票。

(三)同一表决权通过现场、本所网络投票平台或其他方式重复进行表决的，以第一次投票结果为准。

(四)股东对所有议案均表决完毕才能提交。

四、会议出席对象

(一)股权登记日下午收市时在中国证券登记结算有限公司上海分公司登记在册的公司股东有权出席股东会(具体情况详见下表)，并可以以书面形式委托代理人出席会议和参加表决。该代理人不必是公司股东。

股份类别	股票代码	股票简称	股权登记日
A股	688023	安恒信息	2026/4/10

(二)公司董事和高级管理人员。

(三)公司聘请的律师。

(四)其他人员

五、会议登记方法

1、自然人股东亲自出席的，应出示其本人身份证原件、股票账户卡原件(如有)办理登记手续；委托代理人出席会议的，应出示委托人股票账户卡原件(如有)和身份证复印件、授权委托书原件(授权委托书格式详见附件1)和受托人身份证原件办理登记手续。法人股东由法定代表人亲自出席会议的，应出示其本人身份证原件、加盖法人印章的营业执照复印件、股票账户卡原件(如有)办理登记手续；法人股东法定代表人委托代理人出席会议的，代理人应出示其本人身份证原件、加盖法人印章的营业执照复印件、法定代表人证明书、股票账户卡原件(如有)、法定代表人依法出具的授权委托书(加盖公章)办理登记手续。

2、异地股东可采用信函或传真的方式登记，在来信或传真上须写明股东姓名、股东账户、联系地址、邮编、联系电话，并附身份证及股东账户复印件，信封上请注明“股东会议”字样。

3、登记时间：2026年4月13日(上午10:00-12:00，下午14:00-18:00)；登记地点：杭州市滨江区西兴街道联慧街188号安恒大厦21楼证券事务部。

4、注意事项

股东请在参加现场会议时携带上述证件，公司不接受电话方式办理登记。

六、其他事项

联系地址：浙江省杭州市滨江区西兴街道联慧街188号安恒大厦21楼

联系电话：0571-28898076

传真：0571-28898076

邮政编码：310051

联系人：公司证券事务部

注意事项：会期半天，与会股东食宿及交通费用自理。

特此公告。

杭州安恒信息技术股份有限公司董事会
2026年3月26日

附件1：授权委托书

附件1：授权委托书

授权委托书

杭州安恒信息技术股份有限公司：

兹委托　　先生(女士)代表本单位(或本人)出席2026年4月16日召开的贵公司2025年年度股东会，并代为行使表决权。

委托人持普通股数：

委托人持优先股数：

委托人股东账户号：

序号	非累积投票议案名称	同意	反对	弃权
1	关于公司《2025年年度报告》及摘要的议案			
2	关于公司2025年度董事会工作报告的议案			
3	关于公司2025年度财务决算报告的议案			
4	关于公司2025年度利润分配方案的议案			
5	关于续聘公司2026年度审计机构的议案			
6	关于公司未弥补亏损达到实收股本三分之一的议案			
7	关于公司2025年度独立董事述职报告的议案			
8	关于确认公司2025年度董事、高级管理人员薪酬的议案			
9	关于提请股东会授权董事会办理以简易程序向特定对象发行股票的议案			
10	关于补选非独立董事的议案			

委托人签名(盖章)：　　受托人签名：

委托人身份证号：　　受托人身份证号：

委托日期：　年　月　日

备注：

委托人应在委托书中“同意”、“反对”或“弃权”意向中选择一个并打“√”，对于委托人在本授权委托书中未作具体指示的，受托人有权按自己的意愿进行表决。

证券代码：688023　　证券简称：安恒信息　　公告编号：2026-019

杭州安恒信息技术股份有限公司
关于2025年度利润分配方案的公告

本公司董事会及全体董事保证本公告内容不存在任何虚假记载、误导性陈述或者重大遗漏，并对其内容的真实性、准确性和完整性依法承担法律责任。

重要内容提示：

- 杭州安恒信息技术股份有限公司(以下简称“公司”)2025年度拟不进行利润分配，不以资本公积金转增股本。
- 公司2025年度拟不进行利润分配，主要原因为公司2025年度归属于母公司所有者的净利润为负，且综合考虑公司经营、全体股东回报及未来发展等因素。
- 公司不会触及《上海证券交易所科创板股票上市规则》(以下简称“《股票上市规则》”)第12.9.1条第一款第(八)项规定的可能被实施其他风险警示的情形。
- 本次利润分配方案已经公司第三届董事会第二十次会议审议通过，尚需提交公司股东会审议。

一、利润分配方案内容

经立信会计师事务所(特殊普通合伙)审计，截至2025年12月31日，公司母公司报表中期末未分配利润为人民币-393,816,007.96元。经董事会决议，公司2025年度拟不进行利润分配，不以资本公积金转增股本。本次利润分配方案尚需提交公司2025年年度股东会进行审议。公司不会触及《股票上市规则》第12.9.1条第一款第(八)项规定的可能被实施其他风险警示的情形。

二、2025年度不进行利润分配的情况说明

根据《上海证券交易所科创板上市公司自律监管指引第1号一一规范运作》《杭州安恒信息技术股份有限公司章程》(以下简称“《公司章程》”)等有关规定，鉴于公司2025年度实现归属于母公司所有者的净利润为负，综合考虑公司经营、全体股东回报及未来发展等因素，公司2025年度拟不进行利润分配，不以资本公积金转增股本。

三、公司履行的决策程序

公司于2026年3月25日召开第三届董事会第二十次会议审议通过《关于公司2025年度利润分配方案的议案》，本方案符合《公司章程》规定的利润分配政策。董事会同意将该议案提交至公司2025年年度股东会审议，经批准后实施。

四、相关风险提示

本次利润分配方案综合考虑公司目前的发展阶段、未来的资金需求等因素，不会影响公司正常经营，有利于公司稳定健康的发展。本次利润分配方案尚需提交公司2025年年度股东会审议通过后方可实施，敬请广大投资者注意投资风险。

特此公告。

杭州安恒信息技术股份有限公司董事会
2026年3月26日

证券代码：688023　　证券简称：安恒信息　　公告编号：2026-016

杭州安恒信息技术股份有限公司
关于补选非独立董事的公告

本公司董事会及全体董事保证本公告内容不存在任何虚假记载、误导性陈述或者重大遗漏，并对其内容的真实性、准确性和完整性依法承担法律责任。

杭州安恒信息技术股份有限公司(以下简称“公司”)于2026年3月25日召开第三届董事会第二十次会议，审议通过了《关于补选非独立董事的议案》，现将具体情况公告如下：

公司非独立董事吴司韵女士由于个人工作安排辞去公司第三届董事会非独立董事职务，辞任后将不在公司担任其他职务。根据《中华人民共和国公司法》(以下简称“《公司法》”)、《杭州安恒信息技术股份有限公司章程》的有关规定，经董事会提名、董事会提名委员会资格审查通过，公司于2026年3月25日召开第三届董事会第二十次会议，审议通过《关于补选非独立董事的议案》，董事会同意补选王瑞先生为公司第三届董事会非独立董事候选人(简历详见附件)，任期为自股东会审议通过之日起至公司第三届董事会任期届满之日止。

特此公告。

杭州安恒信息技术股份有限公司董事会
2026年3月26日

(下转B18版)