公司代码：688023　　公司简称：安恒信息

杭州安恒信息技术股份有限公司

2024 年年度报告摘要

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”——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、监事会及董事、监事、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2024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十三次会议及第三届监事会第十二次会议审议通过，该议案尚需提交公司2024年年度股东大会审议。

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，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、云安全、大数据安全、物联网安全、智慧城市安全和工业互联网安全以及数据安全等领域。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
人工智能安全	恒脑	安全垂域大模型	恒脑安全垂域大模型，秉承让安全更智能、让智能更安全的使命，依托底层多源异构模型（支持通义千问、DeepSeek、其他自定义模型）、算法调度引擎及海量安全知识，具备恶意代码检测、威胁情报分析、自动化安全编排响应和安全教育等能力，可根据各业务场景需求从容切换多种安全角色，以扎实的安全基本功迎接未来无限可能。经过多轮大规模增量预训练和数十次微调，并在重大安保场景下已进行实战检验。
	恒脑	DeepSeek安全垂域一体机	恒脑DeepSeek安全垂域一体机，以恒脑安全垂域大模型为底座，融合DeepSeek深度推理能力，结合安恒自研智能体框架，具备零代码和低代码创建智能体能力，全面支持等保、关基已部署安全产品作为插件注册到平台，支持各类外部知识库对接，运营人员可基于业务场景需求，结合运营最佳实践创建智能体，实现安全业务场景自闭环。平台已发布官方智能体超60个，业务场景涵盖安全运营、数据安全、数据分类分级、API接口安全、钓鱼邮件识别等多个场景。
AI大模型安全	大模型风险检测	恒脑智鉴	恒脑智鉴是一套专为评估和缓解大模型在数据处理、模型构建和应用部署中的风险而设计的风险管理平台。结合先进的内容检测引擎与恒脑内容判定模型，帮助客户审查大模型生成内容，保障信息输出遵守法律法规，维护企业品牌形象和避免法律风险。此外，系统还深入评估AI基础设施的网络安全风险，识别潜在威胁，加强客户的大模型数据完整性和AI业务连续性。

	大模型风险防护	恒脑智盾	恒脑智盾是一款针对大模型资产从语料输入、模型输入输出内容到事后审计封禁的全链路大模型安全防护产品。通过零信任体系保障语料隐私脱敏与动态风险识别，实时监控模型性能及网络流量，提供AI防火墙三重过滤（敏感词、语义分析、模型推理）实现输入输出内容实时阻断。支持多维度权限管控、异步违规追溯与策略自优化，确保从基础设施到内容交互的端到端安全，助力企业应对AI时代复杂威胁。
数据要素基础设施	数据运营	数据合规流通数字证书	数据合规流通数字证书运用区块链、密码学、机密计算等新兴技术，真实记录交易双方的全流程合规交易过程，为每笔交易产生一张类似“数据交易发票”的数字证书，可以溯源出整个数据交易过程，并提供交易稽核工具，让监管稽核部门能进行有效执法，快速高效判定交易的合规性。
		授权运营平台	公共数据授权运营平台围绕数据合规授权、溯源监管、原始数据不出域等问题，为授权运营单位提供加工处理、授权运营公共数据服务的特定安全可信平台，覆盖数据资产管理、授权运营管理、数据产品开发、审核与监管、数据产品交付、数据主体授权应用（“我的数据管家”）、全流程安全保障等内容，为授权运营多方主体提供一站式服务，促进数据增值开发与价值流通。
	数据流通	隐私计算	安全岛隐私计算平台是一个以隐私计算技术为核心的数据要素安全流通保障平台，致力于解决多源多方数据在联合计算、建模分析时的安全、信任和隐私保护的问题，以此最大化地释放数据价值。通过可信执行环境（TEE），可解决多个参与方海量数据安全共享的问题，并且支持大模型训练及推理，保护大模型在训练及推理过程中的参数样本的安全以及模型部署的安全；通过多方安全计算（MPC）、联邦学习技术，可解决多个机构互不信任且数据不能出域共享的问题。安全岛平台按照“原始数据不出域，数据可用不可见”的要求，配合关键行为数字验签和区块链审计技术，实现数据要素在流通过程中的所有权和使用权分离，在解决数据确权的基础上，完成最终数据结果或价值的流转，确保原始数据的“可用不可见”、“可用不可取”，保障多方数据联合计算过程的可靠、可控和可追溯。
		数由空间	数由空间是由接入点数由器、基础支撑平台、流通利用平台三个层面构成，再辅以动态安全防护以及统一的对接服务，是一种灵活、可扩展的可信数据空间框架与实现，能以低成本、高效的方式实现与多种数据流通利用设施的融合联通。基于数由空间可打造城市数据空间、企业数据空间、行业数据空间以及跨境数据空间等。
		数由器	数由器即数据空间内的连接器，一种将数据流通利用的参与方高效接入可信数据空间的终端设备，用来连接数据空间内的各个数据参与方。未来各数据主体在不依赖平台管理系统的前提下，数据提供方和数据使用方之间仍可通过数由器点对点进行数据流通利用的需求操作。
网络信息安全平台	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，然后基于深度学习+条件随机场等AI识别模型算法，依据内置的法规、行业标准，对进行敏感数据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，进行风险评估。
		AiMask数据脱敏系统	AiMask采用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。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。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。
		AiThink用户与实体行为分析系统	AiThink/UEBA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。
		AiTrust零信任	AiTrust秉持零信任安全理念，针对远程业务访问及数据开放共享场景下数据安全痛点，打造可信的数字身份体系，为用户的应用发布和数据开放共享提供持续化、动态化、自动化、精细化的访问控制及多项数据安全能力。
		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，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。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，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，通过可视化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、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、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。
	云安全	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，同时结合恒脑大模型实现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	等保一体机是专门针对中小型客户等保合规需求的软硬一体机产品，通过集成等保所需的多种安全能力和特色的等保自测评功能，帮助用户快速、高效的完成等保建设。
	大数据态势感知	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，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。增加扩展组件轻量终端微应用管理，通过收集主机来自不同维度的数据，如用户行为、网络流量、系统日志等，可以获得更全面的信息，从而更准确地检测终端主机上的异常行为；终端检测能够识别和检测各种已知和未知的安全威胁，包括恶意软件、网络攻击、异常攻击行为等，以预警和监测终端的安全；可以进行实时监测终端的活动，并迅速响应任何异常情况，以及及时联动处置采取必要的安全措施，以最小化潜在的风险和损害；终端伪服务感知扫描探测和诱捕攻击源，通过欺骗防御手段将风险引入蜜罐及降低攻击风险和延缓攻击，以确保各个环节风险都能够得到全面的监测、检测和感知。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，从而精准定位告警源并溯源攻击路径。
		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智能算法的安全运营系统，平台可通过智能灵活编排，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。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	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，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威胁实时监测，风险闭环管理，云上云下安全一体化管控。
		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，具有安全设备验证，纵深防御体系验证与编排，资产风险评分算法等核心技术。
		AiLPHA关键信息基	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

		础设施安全保卫平台	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。
		AiLPHA网络安全协调指挥平台	该平台基于大数据分析、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，致力于实现三大统一管控：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，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，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）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。
	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。
		安恒显示屏内容播放审计系统	一款专注于显示屏内容安全保障的产品。该产品基于“恒脑”安全大模型和边缘AI计算分析能力，可实时审计显示屏播出内容，防止各类显示屏免受内容恶意篡改、非法侵入和不良内容违规播出。为各场景的显示屏内容播出安全提供7*24小时技术保障，为千行百业显示屏内容安全保驾护航。
		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。
		视频安全准入系统	基于内置主流视频监控指纹信息库、视频应用协议库以及网络安全防护能力，采用黑白名单双重机制，实现视频网摄像头终端接入行为识别与精准管控，实现授权终端安全接入，实时阻断非法接入、仿冒私接等行为，帮助用户构建一张终端接入全程可视、可管的视频网。
		物联网安全感知与管理平台	物联网安全感知与管理平台是基于安恒大数据分析技术和威胁建模技术的物联网安全运营系统，以“资产风险全生命周期展示和治理，未知安全威胁快速识别和处置”为产品理念；产品功能围绕“一心三能”展开，一心是以IOT资产为核心，能看见资产及资产风险，能溯源安全风险，找到安全告警和安全事件的源头，最后做到能处置，联动安全处置产品进行风险处置或者将风险预警/通报给对应的风险运维人员，从而实现全网资产集中管控、资产隐患实时监测、资产安全威胁实时感知。

	终端安全	明御终端安全及防病毒系统（EDR）	安恒EDR是一款集成了丰富的系统加固与防护、网络加固与防护等功能的主机安全产品，具备业界独有的入侵威胁防护模块，ATT&CK框架覆盖率业界领先，能够精准识别未知威胁与攻击；通过自主研发的专利级文件诱饵引擎，有着业界领先的勒索专防专杀能力；通过内核级东西向流量隔离技术，实现网络隔离与防护；并具备网页防篡改与网站攻击防护等网页安全能力以及补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力。
		网站卫士网页防篡改系统（WPT）	网站卫士网页防篡改系统内嵌于Web服务器中，是一种主动和直接的网站文件保护方式。它不仅可以实现多个站点文件的保护，还可以实现单个站点中文件或目录的保护。该功能可以预先将站点文件或站点目录保护起来，除了指定的可信IP、进程、用户之外，禁止非法用户改写受保护的文件或目录。在非法进程侵入系统之前切断其连接，禁止其下一步行为。
		AiTrust零信任	以零信任安全理念，和UES融合，打造应用级的网络准入，针对远程业务访问及数据开放共享场景下数据安全痛点，打造可信的数字身份体系，为用户的应用发布和数据开放共享，做好身份、设备、网络、应用、数据综合一体化能力。
		办公智盾（安恒终端安全管理系统UES）	办公智盾提出新一代的一体化安全防护理念和解决方案，集成五大智能体（威胁防护、分级分类、行为分析、信创助手、安全接入），超越传统思维，从单一终端安全，变成人员、终端、网络、应用、数据全方位一体化安全，构建新一代智能安全基座。办公智盾融合了准入、零信任、防病毒、数据防泄漏、桌面管理、主机审计、沙箱等十多种业务，全面兼容Windows、Linux、MacOS、UOS、麒麟等主流操作系统，一个平台，一个终端，统一管理。
网络信息安全基础产品	网络信息安全防护产品	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，构建智能模型，用于防御高级威胁，未知威胁。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、机器学习引擎、威胁情报引擎、行为分析引擎、基础特征引擎），可通过主动防护与被动安全相结合的方式识别可疑、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，结合跨事件/设备的关联分析，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。
		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，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（如等级保护、赛班斯法案SOX、PCI、企业内控管理、分级保护、ISO/IEC 27001等）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，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，检测能力完整覆盖整个APT攻击链，能有效发现APT攻击。
		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，通过智能语义分析、精准全面的检测规则、多角度分析模型、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。
	网络信息安全检测产品	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，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，全面满足公安部“十四五”重点装备工具规范技术要求。
		明鉴漏洞扫描系统	提供系统、Web、数据库、基线配置核查、镜像扫描、勒索与风险监测、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、数据库镜像等存在的网络信息安全漏洞，完成整体系统的安全评估。
		信息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。
		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，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，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，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。
网络信息安全服务	安全托管运营服务MSS	安全托管运营服务MSS	以用户资产全生命周期的安全需求为导向，参考IPDRO框架，将云端安全专家团队、标准化运营流程、云端智能化安全托管运营服务平台深度结合，从资产管理、攻击面管理、威胁检测与响应、威胁狩猎、应急响应等五大核心攻防对抗域持续开展安全活动，助力用户建立高性价比、7*24h*365天、持续主动、有效闭环的安全运营体系。
	安恒云-在线订阅式SaaS服务	安恒云-在线订阅式SaaS服务	以SaaS化、集中化、智能化、生态化为主要特点的多云安全建设平台，实现统一门户、统一运维以及统一运营，对外提供网站安全、内容安全、云上等保合规能力建设等解决方案，满足用户多场景业务需求。
	专家服务	专业安全服务	专业安全服务深度融合AI安全能力，构建智能主动防御体系，包括安全检测服务、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	可信众测是公司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。
		安全咨询服务	安全咨询服务包括安全运营咨询服务、数据安全咨询服务、安全开发咨询服务、信息安全规划咨询服务、安全合规咨询服务。随着信息安全等级保护工作进入2.0时代，数字化战略与AI智能化在各行业信息安全建设的深入部署与应用，结合安恒信息自主研发的智能体开发框架，在安全咨询领域展开具身智能创新实践，通过将安全咨询能力应用到智能体，以此发挥安全咨询专业服务能力与效率优势，帮助客户科学合理地开展与落地信息系统安全保障体系规划与建设。
		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	应急响应服务涵盖7*24小时安全事件应急处置及应急演练两部分关键内容。在应急演练服务板块，公司为客户提供全方位的全场景演练内容，包含应急预案制定，精心构建贴合实际业务场景的应急计划，确保在危机来临时各部门能协同有序应对；应急演练平台构建，打造高度仿真、功能完备的演练环境，让参与人员能沉浸式体验应急流程；以及红蓝对抗服务，模拟真实攻击与防御场景，通过激烈对抗提升团队实战能力。 在应急响应服务中，公司依托应急响应工具箱和应急指挥平台，为快速高效的安全事件处置提供坚实支撑。公司基于专家多年工作经验自主研发的应急取证收集工具，结合AI分析引擎能对收集到的海量繁杂数据进行智能筛选，大幅提高一线应急取证分析效率。

		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公司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。公司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，公司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		以城市关键信息基础设施和重要信息系统为保障对象，聚焦全域网络安全统筹协调、监测预警、应急处置、智能防护等能力提升，协助用户从网络安全防护向数据安全和人工智能安全进行转变；通过统签统建统管的建设机制，完善城市级安全运营服务平台、组建协同响应的服务团队，帮助客户构建一个集安全防护、态势感知、监测预警、情报共享、通报处置、应急指挥、协调联动、攻防演练、人才培养为一体的网络安全运营中心，中心根据不同层级用户需求，为政府单位和企事业客户提供安全咨询、风险评估、告警研判、事件处置、智能防护、损失赔付等网络安全服务，降低客户的采购成本。
	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、研究成果以及成熟的项目经验进行整理，并完成教育资源转化。公司开发了符合不同层次教学、演练和评估场景的攻防实验室平台、攻防演练平台和攻防靶场平台，并且推出网络安全AI创新实验室，强化网络安全人才在AI基础能力和智能体开发方面的能力，提升人工智能专业人才在AI安全方面的理解和素养，并综合运用AI技术，在演练场景生成等方面显著提升用户体验和效率。 服务主要包括：协助在校学生、在职人员展开安全技能培训、国家认证培训和竞赛；协助各企业构建网络安全人才队伍；提供在线的网络信息安全人才学习平台。负责为安恒信息及产业链提供适应产业发展节奏的优质人才供给。
商用密码产品	密码整机类产品	服务器密码机	服务器密码机以现代密码技术为核心，为信息系统提供包括数据加解密、数字签名与验签、密钥管理、消息验证等密码服务，满足业务交易对数据从产生、传输、处理、存储过程中的机密性、完整性、不可抵赖性以及身份认证的要求，同时提供安全、完善的密钥管理机制，为信息系统的数据安全提供有力保障。
		云服务器密码机	云服务器密码机由宿主机、虚拟机、管理工具（宿主机管理端和虚拟机管理端）构成，利用虚拟化技术将一台物理密码机虚拟为多台虚拟密码机，为云场景中云平台和租户提供资源弹性扩容的密码服务、降低密码硬件的投入成本。
		签名验签服务器	签名验签服务器基于数字证书和PKI体系，为业务系统提供数字签名及验证、数字信封制作及解析、证书管理等功能，支持多种商用密码算法，结合安全、完善的密钥管理机制，保障业务数据从产生、传输、接收到处理整个过程的机密性、有效性、完整性和不可抵赖性。
		签名验签与时间戳二合一服务器	签名验签与时间戳二合一服务器基于PKI体系和可信时间源，可为各类信息系统提供数字签名及验证、数字信封制作及解析、时间戳签发及验证等功能。产品能够精准确认应用系统处理数据时，在某一时间内相关操作的相对时间顺序，解决业务交易中数据从产生、传输、处理、存储整个过程的机密性、完整性、不可抵赖性以及身份认证等安全问题。
		SSL VPN安全网关	SSL VPN安全网关是一款能够有效防止业务数据在网络传输中被窃取、篡改的网络安全产品，为用户提供了完善的内部网络或应用程序的安全远程接入服务以及各分支机构局域网之间的数据安全传输和安全访问服务。

		IPSec VPN网关	IPSec VPN网关系统是为防止数据在传输过程中被第三方获取或篡改的安全产品，提供安全隧道的协商建立，实现中心机构与分支机构、合作伙伴之间的远程接入等多种网络互联需求，同时对这些远程网络中传输的数据提供机密性、完整性等安全防护。
		IPSec/SSL VPN综合安全网关	IPsec/SSL VPN综合安全网关集SSL VPN技术和IPSec VPN技术于一体，采用商用密码算法，集认证以及传输加密于一体，同时支持点对网与网对网部署三大特点，为用户提供完善的内部网络安全远程接入服务以及各分支机构局域网之间的数据安全传输。
		安全认证网关	安全认证网关为网络应用提供基于数字证书的高强度身份认证、高强度数据链路加密服务，可以有效保护网络资源的安全访问。
	密码系统类产品	密钥管理系统	密钥管理系统基于国产密码算法（SM2、SM3、SM4），为应用系统提供密钥的生成、分发、存储、更新、归档、备份、恢复和销毁等全生命周期密钥管理能力，满足业务系统对密钥的管理需求。
		协同签名系统	协同签名系统主要针对移动端用户身份鉴别需求，基于商用密码算法，结合密钥分割与协同签名技术，通过移动端和服务端独立生成和存储密钥分量，经过协同运算最终得到完整签名，在保证用户使用便利性的同时，为移动终端提供安全合规的身份认证方案。
		密码应用安全测评工具箱	密码应用安全测评工具箱作为专用于密评合规的检测工具，能够将原本依靠人力的测评工作变得系统化、流程化，工具化，有效提升测试效率和测试结果的准确性，对整个测评过程起到强大的辅助作用。
	密码平台类产品	密码服务管理平台	密码服务管理平台是面向多云、多机房、多租户场景，利用多类密码服务，为用户提供一站式密评综合解决方案的密码产品，根据负载动态调整基础密码设施的规模，实现密码运算资源的动态调整和灵活调度，为用户提供按需高效、弹性可扩展的密码服务，满足密评要求。
	专家服务		提供信息系统过密评的解决方案咨询服务，包括密码应用方案编制、密评问题答疑等，满足密码应用安全性评估对于密码应用方案评审的要求。 根据密评要求，协助梳理密码应用安全管理制度，建立操作流程与执行记录模板，制定应急处置办法并形成报告模板等。 提供信息系统过密评的应用开发指导服务，包括密评改造过程技术指导、标准接口对接、POC测试等。

2.2 主要经营模式

1、盈利模式

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，公司通过向下游客户销售网络信息安全产品和提供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，分别实行订单驱动式生产和季度预测式生产。由于生产的产品形态主要为软硬件结合产品，公司采购相应软硬件原材料后进行组装调试，然后将自主研发的软件灌装入硬件设备中，最后经拷机测试、产品质量检验、入库等环节完成生产，并通过快递公司发货至下游客户。

4、服务模式

公司基于自身在应用安全和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渠道等合作伙伴，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》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。

2024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。

2024年5月，国家网信办联合相关部门发布《互联网政务应用安全管理规定》，提出落实网络安全与互联网政务应用“同步规划、同步建设、同步使用”，保障互联网政务应用安全稳定运行和数据安全。

2024年9月，国务院发布《网络数据安全管理条例》，旨在规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，维护国家安全和公共利益。

2024年12月，国家工业和信息化部联合相关部门发布《中小企业数字化赋能专项行动方案（2025-2027年）》，旨在全面增强中小企业数据与网络安全防护能力，引导中小企业建立健全网络和数据安全管理制度。

同时，各行业也在2024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。

2024年1月，工业和信息化部印发《工业控制系统网络安全防护指南》，旨在进一步指导企业提升工控安全防护水平，夯实新型工业化发展安全根基。

2024年3月，国家卫生健康委办公厅联合相关部门发布《关于进一步推进医师电子化信息管理工作的通知》，要求落实数据安全管理责任制，确保电子化注册系统数据信息安全。

2024年5月，国家能源局发布《电力网络安全事件应急预案》，保障电力系统安全稳定运行和电力可靠供应。

2024年12月，国家金融监管总局发布《银行保险机构数据安全管理办法》，进一步规范金融行业的数据安全治理。

党中央对网络安全和信息化工作始终保持高度关注。2024年8月，党的二十届三中全会审议通过的《中共中央关于进一步全面深化改革、推进中国式现代化的决定》提出“加强网络安全体制建设，建立人工智能安全监管制度”等一系列新任务新要求，为新时代网络安全工作指明前进方向。中共中央总书记、国家主席、中央军委主席习近平也多次强调要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民合法权益。

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。根据Gartner的最新预测，2025年全球IT总支出将达到5.61万亿美元，较2024年增长5.8%；2025年人工智能优化服务器的支出将达到2020亿美元，IT服务公司和超大规模企业将占到IT支出的70%以上。IDC预测，中国数据安全市场的投资规模到2028年将达到173亿美元，5年年复合增长率约为16.7%；2028年中国大数据IT支出规模预计为502.3亿美元，全球占比约8%，五年复合增长率约为21.9%，增速位居全球第一。

中国网络信息安全市场正在加速向服务化转型，与全球安全产业结构发展趋势保持一致。合规需求依然是推动行业发展的主要动力，但随着网络攻击的复杂性和破坏性不断升级，企业逐渐将网络安全视为重要的商业风险，并更加注重安全服务的持续性和有效性。云化、SaaS化等交付模式在2024年进一步普及，安全厂商加速布局云安全、隐私计算、零信任架构等新兴技术领域。根据Gartner的预测，2025年全球信息安全终端用户支出预计将达到2120亿美元，较2024年的1839亿美元增长15.1%，其中安全服务（包括咨询、IT外包、实施和硬件支持等）增速最快，支出预计将达到860亿美元，占总支出的40.6%。

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稳步增长。同时，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。公司主要产品和服务排名及获得荣誉列举部分如下：

●在IDC发布的《IDC 2022年中国工业互联网安全管理平台市场份额》报告中，公司工业互联网安全管理平台市场份额排名第一；

●在IDC发布的《中国Web应用防火墙硬件市场份额，2022：硬件增长受阻，寻求云上突破》报告中，公司Web应用防火墙产品市场份额排名第二；

●在IDC发布的《IDC 2022年中国工控安全审计市场份额》报告中，公司工控安全审计产品市场份额排名第二；

●在IDC发布的《IDC 2022年中国托管安全服务（驻场、远程、云托管）市场份额》报告，公司云安全托管运营服务位列市场第一；

●在赛迪顾问发布的《2022-2023年中国云安全市场研究年度》报告中，公司云计算安全市场份额综合排名第三，安全云服务市场排名第一；

●在《IDC MarketScape:中国态势感知解决方案市场2023，厂商评估》报告中，公司以突出的核心技术能力、丰富的行业实践以及领先的市场战略，继续成为中国态势感知解决方案领导者企业之一；

●2023年10月24日至26日，京西智谷·昇腾AI创新大赛2023全国总决赛于北京 国家会议中心顺利举办，安恒信息凭借《基于昇腾软硬件平台恒脑·安全垂域大模型解决方案》在本次全国总决赛中荣获金奖；

●在赛迪工业和信息化研究院（集团）四川有限公司正式发布的《2023中国人工智能大模型企业综合竞争力50强研究报告》中，“安恒恒脑”入选中国AI大模型综合竞争力50强；

●公司“基于密码技术实现云场景安全的统一服务平台方案”成功入围2023年信息技术应用创新典型解决方案名单；

●在中国信息安全测评中心正式公布的首批国家信息安全服务资质数据安全类一级获证企业名单中，公司获得国家信息安全服务数据安全类一级资质，且为国内首批获证企业；

●在浙江省科技厅正式公布首批认定的科技小巨人企业名单中，安恒信息凭借优秀的研发实力与创新能力等综合实力光荣上榜，获评2022年度浙江省“科技小巨人”；

●在浙江省科学技术厅正式公布的2023年度浙江省科技领军企业及科技小巨人企业名单中，安恒信息获选2023年度浙江省科技领军企业；

●安恒信息“AiLand数据安全岛隐私计算平台信创解决方案”成功入围“2022年信息技术应用创新解决方案（典型解决方案）”。此次入围，充分体现了安恒信息AiLand数据安全岛隐私计算平台信创解决方案在技术创新性、应用示范性、产业前景等方面的优势和实力。

●公司密码服务平台获评2022年首届全国商用密码应用优秀案例；

●Frost & Sullivan发布的《Asia Pacific (APAC) Managed and Professional Security Services Market》报告（以下简称《报告》）对中国地区安全托管服务(MSS)进行了深入研究。《报告》显示，公司MSS市场份额位列2022年中国地区安全托管服务（Managed Security Services，MSS）第一名。

●公司凭借卓越的数据安全能力，“恒星实验室”、“HAC”两支团队分别荣获2022年首届数据安全大赛“数据安全大闯关”优胜奖，公司申报的《面向健康医疗数据的安全治理体系方案和应用》获2022年首届数据安全大赛“数据安全治理方案”银奖。

●在第六届世界浙商大会杭州专场活动——杭州民营经济发展论坛暨新生代企业家论坛上，公司分别获得“2022杭州市民营企业服务业50强”和“2022杭州市民营企业研发投入50强”荣誉。

●公司荣获工业和信息化部“铸网2022”实网演练“优秀技术支撑单位”、“铸网2022”车联网网络安全演练“优秀攻击队伍”。

●公司申报的“面向杭州亚运会等重大赛事的云安全服务保障平台”成功入选2022工业和信息化部网络安全技术应用试点示范项目。

●根据上海市经济和信息化委员会公布的《2022年度上海市优质大数据服务供应商目录》，公司全资子公司上海安恒智慧城市安全技术有限公司成功入选该目录，标志着公司在金融行业的大数据服务能力得到了充分肯定与广泛认可。

●2022年，科创板开市三周年之际，公司入选“科创板创新力30强”、“科创板发明专利30强”以及“科创板软件著作权30强”。

●2024年，公司“云上商用密码应用解决方案”荣获网信自主创新推荐解决方案。

●2024年，公司“云上商用密码应用解决方案”荣获密码“丰”会优秀解决方案。

●2024年，经安全牛综合调研分析，安恒在信创安全领域产品研发和应用推广中表现出色，入选2024年度信创安全领域十大代表性厂商，并收录于《信创安全能力建设技术指南（2024年）》研究报告。

●2024年数字中国创新大赛·信创赛道，杭州亚运会网络安全管理平台基于鲲鹏Validated的实践应用、明御数据库审计与风险控制系统分别获得杭州城市赛二等奖、优胜奖。

●安恒信息取得中国电子工业标准化技术协会信息技术应用创新工作委员会授予的2024年度信息技术应用创新工作委员会卓越贡献成员单位。

公司始终坚持持续创新的发展战略，重视研发投入，同时紧跟全球信息技术发展趋势、贴近用户需求，不断更新迭代既有产品和解决方案，并孵化培育新兴产品及服务。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。2024年，AI大模型技术发展进一步加速，安恒信息在已发布“恒脑·安全垂域大模型”基础上，构建了“恒脑·智能体开发平台”，基于此平台开发出业界首个商业落地的智能体“分类分级智能体”，提升分类分级效率30倍，相关成果获得第六届浙江省青工创新创效大赛研发创新类金奖、第十八届“振兴杯”全国青年职业技能大赛研发创新银奖、入选2024年世界互联网大会《科技之魅》成果集、入选工信部2024年先进计算赋能新质生产力典型应用案例以及2024年浙江省数字经济发展优秀案例等诸多荣誉。

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。

安恒信息始终高度重视网络安全标准化工作，截至2024年年末，已累计参与了超过111项标准的研制，方向覆盖了基础网络安全产品、安全服务、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。2024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16项正式发布，深度参与的网络安全行业标准有27项正式发布。安恒信息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。

在新的应用场景下，包括云计算、大数据、物联网、5G、边缘计算、智能终端和生成式人工智能等，企业信息化程度的提升使得网络信息安全领域呈现出三大显著变化：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。

此外，随着生成式人工智能和数据基础设施的广泛应用，数据隐私保护和模型安全成为新的关注重点，推动了数据安全治理、身份认证和加密技术的快速发展。同时，零信任架构的推广和云安全、工业互联网安全等细分领域的崛起，进一步丰富了网络信息安全的内涵和外延。这些变化表明，网络信息安全正在从单一的技术防护向体系化、智能化、服务化方向演进，成为支撑数字经济发展的重要基石。

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

	2024年	2023年	本年比上年增减(%)	2022年
总资产	5,035,768,395.71	4,978,259,985.46	1.16	5,014,102,625.28
归属于上市公司股东的净资产	2,509,210,485.75	2,559,900,847.15	-1.98	2,907,180,081.32
营业收入	2,042,835,394.88	2,170,164,682.12	-5.87	1,980,012,417.18
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	2,035,747,382.11	2,162,549,839.53	-5.86	1,971,098,060.44
归属于上市公司股东的净利润	-197,849,927.16	-359,805,113.83	不适用	-253,556,281.82
归属于上市公司股东的扣除非经常性损益的净利润	-237,183,747.13	-387,818,496.58	不适用	-298,761,187.34
经营活动产生的现金流量净额	160,840,916.93	-255,728,672.23	不适用	-178,802,476.42
加权平均净资产收益率（%）	-7.83	-12.60	增加4.77个百分点	-8.48

基本每股收益（元/股）	-1.94	-3.53	不适用	-2.48
稀释每股收益（元/股）	-1.94	-3.53	不适用	-2.48
研发投入占营业收入的比例（%）	24.11	29.33	减少5.22个百分点	32.62

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	280,802,086.21	416,791,824.32	446,958,773.20	898,282,711.15
归属于上市公司股东的净利润	-200,369,144.75	-75,236,411.27	-60,389,660.56	138,145,289.42
归属于上市公司股东的扣除非经常性损益后的净利润	-204,236,989.39	-82,025,142.89	-68,899,222.01	117,977,607.16
经营活动产生的现金流量净额	-358,258,437.75	-70,476,010.22	31,456,478.05	558,118,886.85

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)	9,802
年度报告披露日前上一月末的普通股股东总数(户)	13,041
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	3,029,012	13,125,717	12.83	0	无	0	境内自然人
杭州阿里创业投资有限公司	357,054	8,365,391	8.18	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）	1,166,670	5,000,000	4.89	0	无	0	其他
宁波安恒嘉盛投资合伙企业（有限合伙）	843,973	3,657,216	3.58	0	无	0	其他
宁波安恒投资合伙企业（有限合伙）	843,750	3,656,250	3.58	0	无	0	其他
香港中央结算有限公司	1,700,612	2,671,310	2.61	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	1,000,000	2,500,000	2.44	0	无	0	其他
中国电信集团投资有限公司	531,336	2,302,455	2.25	0	无	0	国有法人
交通银行－汇丰晋信动态策略混合型证券投资基金	339,709	1,965,613	1.92	0	无	0	其他
交通银行股份有限公司－汇丰晋信低碳先锋股票型证券投资基金	461,130	1,298,978	1.27	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

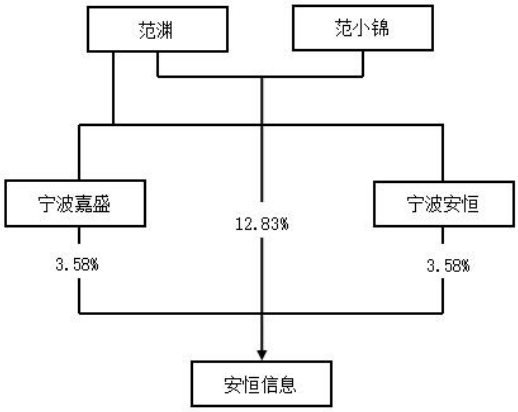
□适用 √不适用

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

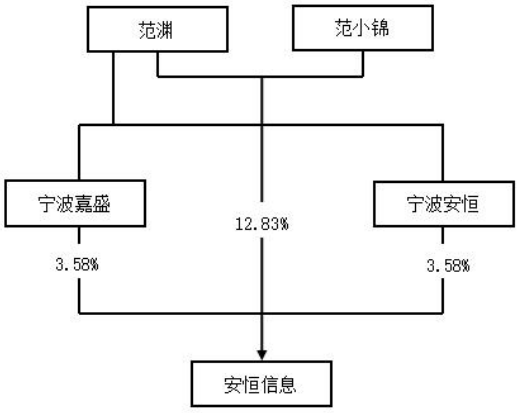
√适用 □不适用



截至报告期末，范渊先生直接持有公司股票 13,125,717 股，直接持股比例为 12.83%。范渊先生与范小锦女士为夫妻关系，且范渊先生与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）签署了《一致行动协议》，范渊先生合计控制公司 19.99%的表决权。

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



截至报告期末，范渊先生直接持有公司股票 13,125,717 股，直接持股比例为 12.83%。范渊先生与范小锦女士为夫妻关系，且范渊先生与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）签署了《一致行动协议》，范渊先生合计控制公司 19.99%的表决权。

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2,042,835,394.88元，比上年同期下降5.87%；实现归属于上市公司股东的净利润-197,849,927.16元，归属于上市公司股东的扣除非经常性损益后的净利润-237,183,747.13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