公司代码：688168　　公司简称：安博通

北京安博通科技股份有限公司

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描述可能存在的风险，敬请查阅第三节“管理层讨论与分析”部分“风险因素”的内容。

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、 公司全体董事出席会议。

5、 中瑞诚会计师事务所（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年度利润分配方案为： 2024年度不派发现金红利，不送股，不以公积金转增股本，未分配利润结转以后年度分配。

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	安博通	688168	不适用

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	但晨	杨帆
联系地址	北京市海淀区西北旺东路十号院东区15号楼A座301	北京市海淀区西北旺东路十号院东区15号楼A座301
电话	010-57649050	010-57649050
传真	010-57649056	010-57649056
电子信箱	xiazf@abtnetworks.com	xiazf@abtnetworks.com

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

1、主要业务

公司深耕行业多年，作为中国网络安全的核心系统、产品与安全服务提供商，专注网络安全核心技术和底层平台的研究、开发、销售及技术服务。公司于 2016 年首次在产业提出“可视化网络安全技术”创新，依托自主研发的应用层可视化网络安全原创能力，为国内众多部委与央企提供业务组件、分析引擎、关键算法等软件产品及相关的技术服务。

2024 年，公司在产品战略开启全面升级，公司继而提出“让 AI 与世界安全连接”创新。在此进程中，在原有业务的基础上对安全生态的进一步延申。致力于搭建 AI 与安全双向赋能的创新体系，推动安全技术、AI 技术与算力技术深度融合，为用户打造便捷、安全的算力基础设施，助力 AI 应用更快、更广泛、更深入地拓展至企业级场景。报告期内，公司主要业务未发生重大变化。

2、主要产品

公司以 ABT SPOS 系统平台为基础，面向网络安全防御控制、网络监测预警等形成了包含安全网关、安全管理、全流量安全、数据安全、云安全和安全服务在内的多品类网络安全产品。

网络安全系统平台 ABT SPOS 具备跨硬件平台的适应能力与云计算虚拟化能力，网络产品厂商、解决方案厂商、电信运营商、云服务提供商等合作伙伴均可基于该软件快速开发各种网络安全网关类硬件设备、云环境下虚拟化安全网关、安全监测预警与运维管理类产品，从而快速响应用户需求。该平台不仅可以应用在传统计算机网络与虚拟化云计算网络中，还可以应用于 IPv6 互联网、工业互联网、视频监控网络、IoT 物联网等下一代信息网络中，同时在国产自主可控的设备网络中也有多种专业用途。

安全网关品类

（1）嵌入式安全网关

应用于数据通信网络环境，包括下一代防火墙及网络行为管理与审计等组件产品，是一种软硬件结合的实体安全设备，通常用于网络互联网出口或网络关键区域边界，是网络中用于隔离、控制、防御的基础安全产品。

下一代防火墙产品采用先进的高性能并行架构，保障业务处理高效可靠，场景支撑灵活全面。产品具备应对高级持续性威胁的入侵防御能力和实时病毒拦截技术，将访问控制模块与漏洞扫描、Web 防护、入侵防御、沙箱仿真、数据防泄漏、威胁情报等系统形成智能的策略联动，通过并行处理的深度安全检测引擎和应用识别技术，实现对用户、应用和内容的攻击行为深入分析，为用户提供安全智能的一体化防护体系。

网络行为管理与审计产品提供全网终端统一管控功能，具备传统认证和主流社交软件等身份认证方式，保障用户接入安全可控。该产品内置千万条 URL 库和五千条主流应用行为特征库，配

合网络行为管理策略模板，可实现网络行为精细化识别和控制。通过智能流量管理特性，动态分配空闲时带宽资源，帮助用户提升用户上网体验；结合清晰易用的管理日志功能，为企业提供全面、完善的网络行为管理解决方案。

（2）虚拟化安全网关

应用于云计算和大型数据中心的虚拟化安全网关产品，通过虚拟化技术将安全防护特性与虚拟计算、虚拟存储、虚拟网络适配并融合到通用服务器中，形成标准化的防护单元，多个防护单元通过资源池方式汇聚成数据中心整体安全架构，并通过统一的管理平台实现可视化集中运维管理。

虚拟化安全网关以通用服务器为硬件载体，以安全资源池的形式满足公有云、私有云、混合云等多种云场景下的安全需求，并通过统一的管理界面实现全网安全资源池的分配和调度，主要用户包括政务云数据中心、运营商数据中心、金融数据中心和公有云服务提供商等。

安全管理品类

基于大数据分析与可视化技术，公司在 ABT SPOS 网络安全系统平台之上打造了安全管理运营产品，主要包括晶石、墨影、SOAR、方州、鹰眼、元溯、云安全资源池、天枢等。

晶石安全策略智能运维平台，通过对全网访问控制类设备的安全策略数据进行自动采集与解析，基于大数据分析与人工智能算法，提供策略优化清理、策略合规审计、逻辑拓扑可视、安全路径可视、网络攻击面可视、策略应急封堵以及策略自动开通等能力，从而实现全网安全策略的集中可视化管理与智能化运维，提升网络运维自动化水平以及安全防护保障能力。

墨影网络节点资源管理平台，围绕网络节点资源对象，通过图形拓扑方式快速串联节点资产、事件、地理等要素，明晰各要素之间的互动关系，形成网络空间全景地图，使资产底数更加清楚、事件发现更加精确、威胁定位更加准确、威胁分析更加智能、威胁溯源更加自动、变更告警更加直观，最终实现网络节点资源的全闭环管理，从而有效提高 IT 基础部门在安全事件与网络故障方面的能力和效率，使网络与安全运维工作更加智能化、自动化、可视化。

SOAR 产品，采用安全响应和自动化编排的技术，将技术人员的经验和知识结合实际工作管理的流程要求，转化成可视化编排的操作步骤，提高安全管理的效率，降低网络安全运维管理工作的复杂度，保证安全事件处理的正确性和时效性。

方州新一代安全业务中台，基于物理网络、逻辑网络、应用网络、数据网络四维网络仿真技术，构建网络基础架构孪生，通过丰富的接口技术连接用户的网络资产与安全能力，面向不同场景实现灵活的业务流程编排以及自动化，赋能用户安全运营业务。聚焦用户网络资产、安全能力、业务系统之间联系协同的问题，致力于帮助用户提升安全检测与分析的能力、提高事件处置与运营工作的效率、降低平台建设成本与缩短部署周期。

鹰眼全流量取证系统，立足于网络全流量的存储与溯源能力，提供业务访问梳理，网络故障定位、异常威胁检测、全流量回溯分析、网络与应用质量监测等价值，帮助用户迅速完成责任界定，提升网络流量可视化分析能力。通过将鹰眼产品与晶石产品结合，推出全链路监测解决方案，实现基于策略路径的业务质量分析与故障定位，提升运维可视化能力。

元溯数据资产监测与溯源分析平台，针对核心网络区域、关键业务应用等范围内的数据资产在网络中传输过程与行为进行监控与审计，包括数据资产的流向路径与流转关系，并结合用户、设备、应用等多维度进行关联分析，实时呈现数据资产在网络中的动态流动全息视图。同时支持敏感数据的异常行为监测与风险感知能力，主动发现数据泄露、滥用等异常行为并提供预警、告警、溯源以及处置响应，从而提升数据资产安全防护能力。

云安全资源池产品，基于软件的安全集合，集统一管理与监控、安全编排与自动化、合规管理服务于一体，与生态系统内的各种安全工具实现集成与整合，提供下一代防火墙、入侵检测、上网行为管理、日志审计、脆弱性评估等 13 类云安全产品，覆盖主机安全、网络安全、应用安

全、数据安全等各个层面，给用户全方位安全防护，让业务上云无后顾之忧。

天枢安全服务链控制器产品，融合自研多年的虚拟化技术及安全能力，将物理和虚拟设备与其接入模式、部署方式、实现功能进行解耦，底层抽象为安全资源池中的“资源”，顶层通过软件编程方式进行统一管理、应用编排与流量调度。将分散的安全能力按需调配、串联成链，从而实现灵活的安全防护。

安全服务品类

目前，公司网络安全服务主要为安全产品技术开发、安全运维服务、实战化攻防服务。公司根据客户的个性化需求，在公司主营产品基础上定制开发扩展功能或个性化功能，或按照定制化需求开发产品特性或提供解决方案。同时提供产品后期的运维保障和升级保障服务。近年公司对前沿产品和服务推广，公司开展实战化攻防服务，主要聚焦渗透测试、代码分析、事件响应、威胁检测、攻防培训等实施一系列实战化服务，为客户提供全流程的安全保障支撑。

安全人工智能品类：

算力网关可部署于数据中心或跨网节点，动态分配算力资源并保障网络传输质量，也可部署于边缘算力节点，支持 4G/5G、专网接入，集成分布式异网互联、确定性网络加速功能，实现边缘侧算力与网络协同。

异网异构编排调度平台，是基于多协议兼容技术构建的智能资源管理系统，可无缝整合跨品牌、跨架构、跨云环境的多元异构计算资源（包括异构服务器集群、混合云及边缘节点）。通过动态拓扑感知与负载均衡算法，突破网络边界、操作系统及硬件架构差异，实现异构资源的统一纳管与智能调度。平台运用自适应的资源匹配策略，结合任务优先级、算力特性及能耗指标进行全链路效能优化，达成计算资源利用率最大化与业务响应敏捷化的双重目标，为分布式计算、AI 训练等复杂场景提供弹性伸缩的算力支撑。

智算中心建设，涵盖从智算中心的规划、设计，到设备选型、供应、安装调试，再到后期运维管理等全流程工作。旨在为客户打造高效、稳定、安全的算力基础设施环境，满足不同行业、不同规模客户对于数据处理、存储和计算的需求。通过专业的技术团队和丰富的行业经验，确保算力中心具备高性能、高可靠性、可扩展性等特点，助力客户提升业务处理效率，推动数字化转型与智能化发展。

2.2 主要经营模式

公司自成立以来，坚持做网络安全能力的提供者和技术支持者，定位于网络安全行业上游系统、软件与技术提供商，为行业内产品与解决方案厂商提供产品和服务。

1、研发模式

（1）网络安全

公司坚持自主原创、自主创新的研发策略，具备保持技术引领的自研优势。核心产品和关键技术主要来源于内部创新与自主研发。公司各产品线研发主要以 ABT SPOS 平台为基础，自主定义软件的核心能力，为客户提供稳定可靠的产品，满足客户需求。

公司通过前期的需求分析和筛选，确保开发的产品符合市场需求并具有广阔的应用前景；通过产品的开发与测试，确保产品在质量和功能上满足市场需求；产品研发须经过市场调研、立项、设计、开发、测试、验收与发布等几个阶段，按研发项目设立明细账归集相关项目研发支出，并按费用性质进行明细核算。

（2）安全人工智能

公司秉持自主原创、自主创新的研发策略，具备技术引领的自研优势，核心产品和关键技术主要源于内部创新与自主研发。公司产品线研发主要以异网异构算力编排调度平台为基础，自主

定义软件核心能力，如多种算力硬件架构兼容、异构算力融合管理及跨资源池调度技术研发；针对算力网关，围绕边缘算力节点接入、分布式异网互联、确定性网络加速等功能进行技术攻关，为客户提供稳定可靠的产品，满足其在算力基础设施管理、边缘算力协同等方面的需求。

公司通过前期对算力市场需求的深入分析和筛选，确保开发的产品符合市场需求并具有广阔应用前景。产品研发需经历市场调研、立项、设计、开发、测试、验收与发布等阶段，按研发项目设立明细账归集相关项目研发支出，并按费用性质进行明细核算。

2、采购模式

（1）网络安全

公司采购的生产用物料主要包括嵌入式网络通信平台及服务器，对嵌入式网络通信平台采用定制化采购；服务器为通用型标准化产品，公司根据需求对服务器进行直接采购。

嵌入式网络通信平台采购中，公司产品部根据需求制定硬件平台的设计要求，由合格供应商提供满足设计要求的硬件产品，并经公司测试合格后进行批量采购，公司建立了《采购与付款制度》以规范采购行为。

a.供应商的选择

公司根据产品需求对能够提供合格产品的供应商发出合作邀请，综合考虑可选供应商的产品质量、产品报价、供货能力、售后服务、供应商实力等因素择优确定合作供应商。

b.采购流程

公司所需硬件产品达到批量生产标准后，供应链管理部门根据商务部反馈的销售订单量和对部分客户提供的销售预测制定采购计划，向供应商下达正式采购订单。对于嵌入式网络通信平台，供应商按照公司采购订单安排生产，经验收合格入库；对于服务器产品，供应商按公司要求直接发货给客户。

（2）安全人工智能

公司采购的生产用物料主要包括与算力网关相关的通信硬件模块及服务器等。服务器为通用型标准化产品，公司根据需求直接采购。

a.供应商的选择

公司根据产品需求向能够提供合格产品的供应商发出合作邀请，综合考虑可选供应商的产品质量（如硬件模块的稳定性、兼容性）、产品报价、供货能力、售后服务、供应商实力等因素择优确定合作供应商。

b.采购流程

公司所需硬件产品达到批量生产标准后，供应链管理部门根据商务部反馈的销售订单量和对部分客户提供的销售预测制定采购计划，向供应商下达正式采购订单。对于算力网关相关的通信硬件模块，供应商按照公司采购订单安排生产，经验收合格入库；对于服务器产品，供应商按公司要求直接发货给客户。

3、生产模式

（1）网络安全

公司产品有纯软件产品和软硬一体产品两种形态。

对于纯软件产品，公司产品研发部门进行软件系统研发，测试部门负责对软件版本进行调试检测无误后将软件系统刻录到光盘等存储介质并寄送客户，或保存在公司服务器中由客户自行下载并记录使用数量，由公司提供序列号给客户激活使用，期间严格把控产品及售后服务质量。

对于软硬件一体化产品，其中硬件设备全部为外购，公司向供应商采购硬件设备后，将软件产品灌装到硬件设备中，通过调试和检测后，交付给客户使用。由于公司的硬件产品标准化程度较高，为提高产品的交付时效、减少中间运输环节，公司对大部分客户采取供应商直运模式，由供应商将公司软件灌装到硬件设备，最终由公司对产品检测合格后对外销售。

（2）安全人工智能

公司产品有纯软件产品和软硬一体产品两种形态。

对于纯软件产品（异网异构算力编排调度平台），公司产品研发部门进行软件系统研发，测试部门负责对软件版本进行调试检测，无误后将软件系统刻录到光盘等存储介质并寄送客户，或保存在公司服务器中由客户自行下载并记录使用数量，由公司提供序列号给客户激活使用，期间严格把控产品及售后服务质量。

对于软硬件一体化产品（算力网关），其中硬件设备全部为外购，如采购支持 4G/5G、专网接入的硬件设备，公司向供应商采购硬件设备后，将软件产品灌装到硬件设备中，通过调试和检测后，交付给客户使用

4、销售模式

（1）网络安全

公司坚持定位于网络安全能力的提供者、上游系统、软件与技术提供商，通过直销模式向行业内各大产品与解决方案厂商销售网络安全产品或提供网络安全服务，专注于做网络安全行业上游网络安全软件系统的提供商。

客户根据其需求向公司商务部提出产品采购需求，商务部将审批后的销售合同/订单信息录入 ERP 系统中，经商务部经理审核通过。针对软硬一体化产品，商务部根据审核通过的销售合同/订单信息确定交货期后，向仓管人员下达发货指令，仓管人员根据发货指令发货，客户完成收货确认，由财务部开具发票。商务部根据双方约定的信用期，跟踪应收账款回款情况。

针对纯软件产品，包括两种交付方式：通过邮件发送产品授权码给到客户和通过寄送光盘形式。订单审核、收入确认入账、开具发票及收款流程与软硬一体产品相同。

（2）安全人工智能

公司是算力网络基础设施的关键组件供应商，专注于提供异构算力融合和高效连接的解决方案，通过直销模式向行业内各大产品与解决方案厂商销售异网异构算力编排调度平台、算力网关等算网产品或提供相关服务。

客户根据其在算力基础设施管理、边缘算力协同等方面的需求向公司商务部提出产品采购需求，商务部将审批后的销售合同/订单信息录入 ERP 系统中，经商务部经理审核通过。

针对软硬一体化产品（算力网关），商务部根据审核通过的销售合同/订单信息确定交货期后，向仓管人员下达发货指令，仓管人员根据发货指令发货，客户完成收货确认，由财务部开具发票。商务部根据双方约定的信用期，跟踪应收账款回款情况。

针对纯软件产品（异网异构算力编排调度平台），包括两种交付方式：通过邮件发送产品授权码给到客户和通过寄送光盘形式。订单审核、收入确认入账、开具发票及收款流程与软硬一体产品相同。

公司为加快布局数字经济产业，提升人工智能网络研发创新，从长远战略发展角度出发，正积极布局网络安全、算力安全及智算中心 AIGC 解决方案，以此来优化业务结构，延展新型数字基础设施整体解决方案服务商，提升公司综合竞争力。通过直销模式向政府部门、国资平台等合作方提供算力中心规划建设、方案产品、联合运营等全生命周期服务。

客户根据区域算力发展规划及数字化转型需求，向公司提出算力中心共建需求后，双方组建专项工作组进行可行性论证。商务部将经审批通过的共建协议及销售合同信息录入 ERP 系统，经公司管理层与法务部门联合审核确认。

针对算力中心基础设施建设项目（含 GPU 服务器集群、网络安全等），商务部依据项目进度制定交付计划，由交付实施团队完成设备交货、现场安装调试及系统集成，客户组织验收并签署确认文件，由财务部按合同节点开具发票。

针对算力调度管理平台等软件系统，采用两种交付方式：通过加密传输通道部署至客户指定云环境，或通过私有化部署方式完成系统配置。平台交付后由技术团队提供驻场培训及试运行支持，验收标准以合同约定的性能指标为准。

项目验收后转入共运阶段，商务部根据合作协议约定的收益分成机制，定期核算运营收入并开具对应票据。应收账款管理实行"项目责任制"，由公司委派项目团队协同财务部跟踪回款进度。

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

（1）网络安全行业

2024 年度，宏观经济运行稳定，我国政企数字化、信息化建设的节奏放缓，网络安全产业增快逐步放缓，市场回归稳健运行。下游客户普遍存在经营压力增大、降本需求增强、安全预算削减的现象，信息安全项目延期、缩减甚至取消的情况普遍存在。在政策层面，我国网络安全政策立法总体呈现不断优化、细化落实的趋势，在数据资产管理、数据要素与跨境流通、关键信息基础设施安全防护等方面，发布的系列政策法规更加注重实操要求，营造了良好的产业发展环境。在宏观大背景下，网络安全企业调整经营战略，聚焦优势领域和优势业务，加大研发投入，力求实现高质量发展。

在安全网关产品方面，根据 IDC 发布的《2024 年第四季度中国安全硬件市场跟踪报告》、《中国网络安全硬件市场预测，2024-2028》报告分析，2024 年中国网络安全硬件市场规模约为 210.2 亿元，到 2028 年预测将达到 350 亿人民币，年复合增长率将达到 5.6%，可以看出，网络安全硬件将持续成为网络安全市场中的主流产品和重要组成部分，并将保持良好增长态势。公司的安全网关产品，涵盖安全硬件中主要的防火墙、UTM、内容管理、入侵检测与防御、虚拟专用网等品类，通过不断迭代优化，将会持续保持产业链上游的优势位置。根据安全牛《信创安全能力建设技术指南（2024 年）》报告预测，到 2027 年信创安全有望全面占据网络安全市场的主导地位，公司的安全网关产品凭借硬件无关化的优势，全面适配国产化生态，已经实现了信创产品的规模化供货应用，帮助用户实现国产化替代，占据更多市场份额。

在安全管理产品方面，公司产品专注于安全运营、风险和暴露面管理以及安全可视化方向，而这些方向正是大模型技术在网络安全领域的主要应用场景。近年来，生成式人工智能在网络安全垂直领域的应用已经愈发成熟，越来越多的用户在安全运营工作中部署生成式 AI，以便辅助安全分析师进行检测和响应工作，提升预防、检测、调查、取证和处置安全事件的能力。根据 IDC 发布的《IDC Technology Assessment：中国安全大模型实测之安全运营，2024》报告预测，86%的中国客户将会在未来 1-3 年内采购安全大模型产品和服务，中国的安全大模型市场将在未来 3 年迎来市场的快速增长期。报告中，对厂商的模型围绕网络安全通用知识、告警关联与处置、自动化安全报告、漏洞管理与修复、策略创建与优化、引导式调查与修正以及威胁情报的收集与分析七大方向上进行了实测，安博通安全大模型在可靠性、可用性、可读性、可解释性、可指导性等多个方面表现优秀，成功入选。近日，公司发布了安博通“溢彩”AI 交付架构，构建了三位一体的 AI 交付体系，将帮助更多用户完成公司安全管理产品的交付。

尽管网络安全行业面临暂时的周期性波动，但人工智能、数据治理、威胁暴露管理等技术热点仍在促进产业发展，长期前景依然向好，公司将持续加大研发投入，积极提升产品方案竞争力，持续为客户创造价值。

2025 年 3 月，IDC 发布了 2025 年 V1 版《全球网络安全支出指南》（IDC Worldwide Security Spending Guide），给出了中国网络安全市场预测，结合中国网络安全产业联盟（CCIA）发布的《中国网络安全产业分析报告（2024 年）》综合评估，2025 年中国网络安全市场规模预估将达到 700 亿元以上，在行业维度，政府、能源、金融、电信行业占据网络安全项目支出的较大份额。

（2）安全人工智能行业

2024 年，是人工智能基础设施行业的腾飞之年，迎来爆发式增长与深度变革。全球大模型技术迭代迅猛，呈井喷之势，驱动我国 AI 基础设施全面升级。据 QYR（恒州博智）统计，2024 年

全球人工智能基础设施市场销售额飙升至 2547 亿美元，展现出行业的强劲发展势头。在计算资源层面，技术革新缓解了对昂贵资源的依赖，大幅降低 AI 模型训练与推理成本，为众多企业踏入 AI 领域降低了门槛。

政策利好不断为行业发展保驾护航。近年来，国家密集出台《“十四五”数字经济发展规划》《生成式人工智能服务管理暂行办法》等政策，将大模型安全、AI 基础设施防护纳入监管框架，三大领域协同发展格局深化。2024 年 6 月，工业和信息化部等多部门联合印发《国家人工智能产业综合标准化体系建设指南(2024 版)》，从顶层设计层面助力行业规范发展，推动各类资源高效整合。

AI 在各领域的广泛应用，网络安全风险也随之攀升。有数据显示，2024 年全球发生的 AI 风险事件，超过 30%与利用 AI 进行深度伪造相关。诈骗分子借助 AI 拟声换脸技术实施诈骗，大模型有时混淆事实虚构，令人防不胜防，AI 数据搜集也对个人隐私带来泄露风险。在此背景下，AI 技术也反向赋能网络安全领域。AI 防御系统能够实时监测网络流量，识别异常行为模式，在攻击形成前将其拦截，基于大数据分析的风险预警机制，已成为保护关键基础设施的核心技术手段，特别是在面对新型网络威胁时，这种基于 AI 的主动防御比传统的被动响应更具优势。

全球范围内各国积极布局，美欧日已对数智基础设施作出全面竞争性战略部署。我国也在政策推动下，企业积极响应，加速 AI Infra 建设，着重强调了对全国产化及安全防护的要求。因此 AI 与网络安全融合发展的中还在不断演进变化。早期，网络安全多依赖传统规则与人工防御，AI 仅作辅助。如今，随着 AI 技术成熟，网络安全领域从依赖静态规则防护，逐步转向以 AI 驱动的主动、智能防御体系构建阶段。

AI 与网络安全关联层面，其呈现出独特特点。一方面，二者相互依存，AI 技术应用规模扩大，网络攻击针对 AI 系统与应用场景的频率增加，促使网络安全防护对 AI 技术依赖加深；另一方面，二者融合创新迅速，新的 AI 安全技术与防护手段直接根植于智算基础设施中，从底层开始做好防御工作，以确保从体系上进入安全状态。在不断与国外先进技术合作时，做好全国产替代的准备。

⑵．公司所处的行业地位分析及其变化情况

（1）网络安全行业

2024 年，安博通被评为国家级专精特新“小巨人”企业、北京市知识产权优势单位、北京市共铸诚信企业，获得 CMMI 5 全球最高等级评估认证，子公司首批首家通过中国信通院“算力网络+”评估认证。

公司坚持核心技术自主创新，多项原创产品方案获得认可。下一代 AI 防火墙荣获网络安全领域创新产品奖。可信安全能力获中国信通院权威认可，20 领域入选数字安全护航技术能力全景图。

此外，公司还位列中国互联网协会发布的中国网络安全前二十家企业第 15 位、中国网络安全产业联盟（CCIA）发布的中国网安产业竞争力 50 强第 22 位，入选北京市工商联发布的北京民营企业“科技创新”“社会责任”百强、北京软件和信息服务业协会评定的北京软件核心竞争力企业（技术研发型）、安全牛发布的中国网络安全行业全景图等。公司自主研发的 SPOS 平台，是众多一线厂商与大型解决方案集成商广泛搭载的网络安全系统套件，公司凭借强研发实力、精产品方案和优技术服务，再获新华三集团年度优秀供应商称号。

（2）人工智能行业

2024 年，公司持续推进战略升级，从“网络安全可视化技术的创新者”向“AI 时代安全算力生态构建者”深度演进。在行业地位方面，公司九度入选《网络安全企业 100 强》，排名逐年稳步攀升，2024 年跃升至第 20 位，彰显了公司强劲的发展实力。

3 月，加入由中国科学院自动化研究所发起的多模态人工智能产业联合体，携手各方共同推动多模态智能产业在推进、应用推广及服务提升等方面的创新发展。8 月，与浪潮云达成战略合作，双方整合资源、优势互补，在技术研发、市场拓展等多个维度展开深度合作，共同探索行业

发展的新路径。8 月，与江原科技达成战略合作，聚焦软硬件 AIGC 产品研发与国产化解决方案，为行业提供更优质的产品与服务。9 月，安博通算力公司在加入信通院“算力网络+”先锋计划后，又成为算网融合推委会的伙伴单位。10 月，其异网异构算力调度编排平台顺利通过信通院“算力网络+”行业评估，荣获“算力网络融合调度平台证书”，体现了公司在算力技术方面的领先水平。12 月，公司承接无锡（国家）软件园人工智能智算中心平台搭建项目，为其提供智算中心平台搭建服务及 AI 算力设备，进一步拓展了业务版图。

(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

（1）传统安全持续威胁需求旺盛

在 Gartner 提出的 2024 十大网络安全战略技术趋势中，持续威胁暴露管理技术（Continuous Threat Exposure Management，CTEM）在过去几年被提出并迅速引起了广泛重视。在日常安全运营与红蓝对抗工作中，用户利用代码审计、渗透测试、漏洞扫描、威胁管理等手段了解风险全景，评估全局威胁暴露全景，进行关键目标加固和重要威胁管控，已经成为首要工作，对企业机构的业务持续性、稳定性和安全性产生正向影响。具体到产品层面，攻击面管理（ASM）、外部攻击面管理（EASM）、网络资产攻击面管理（CAASM）等威胁管理产品正在广泛应用，通过资产发现、风险评估、优先级排序、风险验证和主动修复的手段，持续监控和管理潜在攻击，从而增强整体安全防御能力。未来几年，持续威胁暴露管理技术一直是企业安全管理能力的建设重点。

（2）网络安全产品的 AI 性能升级

2022 年以来，人工智能技术进入爆发期，AI 无处不在的时代已经到来，对于安全业务管理者，AI 能力为攻击者带来的手段升级和为安全产品带来的防御提升同样值得关注。目前，多个安全厂商均已推出了垂域大模型，在以下方向上，大模型将持续发展和迭代：首先，大模型需要不断提升算力从而增强对用户的响应体验和可用性表现；其次，大模型需要在语义理解、上下文识别以及安全专业语料库方面进行专业化提升；第三，大模型需要在漏洞评级、威胁情报识别、告警关联、策略推荐等技术应用场景中进一步优化提升效率。

此外，安全大模型自身安全也不容忽视，在训练数据、算法模型、系统平台和业务应用方面，可能存在信息违规获取、输入输出内容不当、代码泄露、模型幻觉与偏见、数据保护访问控制不足等安全问题，同样需要给出切实有效的解决方案，从而打消最终用户的顾虑。

（3）低空经济与网络安全萌芽发展

低空经济指的是在一定高度范围内，通过航空器、无人机等空中交通工具进行的经济活动，是以各种有人驾驶和无人驾驶航空器的各类低空飞行活动为牵引，辐射带动相关领域融合发展的综合性经济形态。随着低空领域“云”“网”“端”的安全边界不断延展，接入终端数量、种类呈现指数级增长，网络攻击面将会越来越广、攻击手段越来越多样，飞行器在执行各类任务时将会涉及大量数据传输与处理行为，对于网络体系的低空基础设施中的边缘云、中心云和算力网络、无人机、低空飞行器等关键基础设施，提出了更高的网络安全防护需求，只有在做好安全保障的前提下，方可顺利实现低空经济的长远发展。

（4）AI 基础设施与网络安全底层融合

在算力、算法、数据协同驱动下，大模型通用泛化能力不断增强，应用边界持续拓展。行业应用市场的打开使推理场景算力需求爆发式增长，企业级 AI 应用场景构建中对智算硬件资源高效管理的需求愈发迫切。企业在应用智算硬件资源时面临 GPU 故障率高、运维难度大、异构 AI 芯片管理复杂等问题，催生了企业对安全 AI 基础设施的需求，以实现智算硬件资源的精准切分、有效调度、动态监测以及故障检测与自愈。具备模型管理能力的私有化部署安全 AI 基础设施成为企业刚需，其围绕模型开发应用全生命周期的模型服务工具链不断丰富，涵盖数据工程、RAG、SFT、模型评测等功能，降低了企业 AI 应用的开发部署门槛。同时，数据安全重要性日益提升，IDC 数据显示全球因数据泄露造成的经济损失每年高达数千亿美元，大模型安全事件频发，如训练数据

“投毒”、数据泄露等，成为制约大模型可持续发展的关键。私有化部署的安全 AI 基础设施将数据存储于企业数据中心，企业可完全掌控数据访问权限、存储位置与传输路径，极大降低了数据安全风险，越来越多的企业基于私有化部署的安全 AI 基础设施开展业务创新，使其成为企业数智化转型的重要底座，安全的 AI 基础设施趋势已然形成并将持续深化。

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	1,783,686,923.54	1,618,188,235.58	10.23	1,438,396,681.43
归属于上市公司股东的净资产	1,121,725,032.80	1,225,905,521.11	-8.50	1,205,942,594.54
营业收入	736,752,687.07	548,284,111.27	34.37	456,441,650.85
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	581,608,368.54	548,143,957.15	6.11	454,988,653.93
归属于上市公司股东的净利润	-118,667,233.77	11,783,753.80	-1,107.04	-8,462,038.73
归属于上市公司股东的扣除非经常性损益的净利润	-122,118,542.34	5,556,160.55	-2,297.89	-21,542,883.05
经营活动产生的现金流量净额	156,798,808.60	-126,437,627.75	不适用	-168,627,883.40
加权平均净资产收益率（%）	-10.14	0.97	减少11.11个百分点	-0.76
基本每股收益（元／股）	-1.55	0.15	-1,133.33	-0.12
稀释每股收益（元／股）	-1.55	0.15	-1,133.33	-0.12
研发投入占营业收入的比例（%）	21.68	23.11	减少1.43个百分点	22.91

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	56,544,466.22	134,782,093.14	106,085,956.23	439,340,171.48
归属于上市公司股东的净利润	-35,071,604.36	-26,235,949.65	-20,225,708.43	-37,133,971.33
归属于上市公司股东的扣除非经常性损益后的净利润	-35,807,446.26	-26,805,384.55	-21,491,884.35	-38,013,827.18
经营活动产生的现金流量净额	-89,151,944.82	-92,343,896.08	-39,227,583.00	377,522,232.50

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)	5,987
年度报告披露日前上一月末的普通股股东总数(户)	5,104
截至报告期末表决权恢复的优先股股东总数（户）	不适用
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）	不适用
截至报告期末持有特别表决权股份的股东总数（户）	不适用
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）	不适用

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	
钟竹		18,204,578	23.69		冻结	756,000	境内自然人
石河子市崚盛股权投资合伙企业（有限合伙）		8,710,358	11.33		无		其他

武汉光谷烽火产业投资基金合伙企业（有限合伙）	-1,333,462	1,387,817	1.81		无		其他
深圳市达晨财智创业投资管理有限公司－深圳市达晨鲲鹏二号股权投资企业（有限合伙）	-466,578	1,205,839	1.57		无		其他
元沣（深圳）资产管理有限公司－元沣顺赢 1 号私募证券投资基金	1,202,241	1,202,241	1.56		无		其他
王栋	896,754	896,754	1.17		无		境内自然人
张志龙	891,719	891,719	1.16		无		境内自然人
杨俊武	886,590	886,590	1.15		无		境内自然人
苏长君	-982,664	682,720	0.89		无		境内自然人
黄成槐	650,893	650,893	0.85		无		境内自然人
上述股东关联关系或一致行动的说明		上述股东中钟竹为石河子市崚盛股权投资合伙企业（有限合伙）执行事务合伙人，互为一致行动人，公司未知其他股东之间是否存在关联关系或一致行动关系。					
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

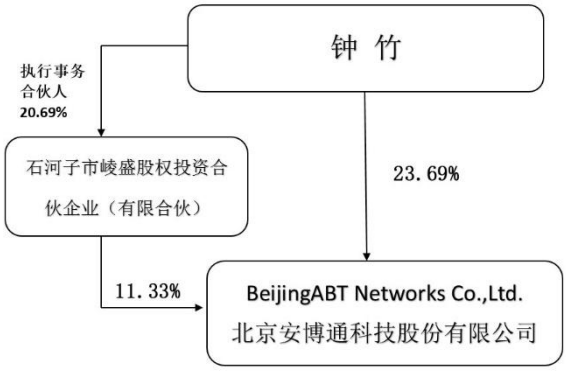
□适用 √不适用

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，公司实现营业收入 73,675.27 万元，比 2023 年同期增长 34.37%；归属于上市公司股东的净利润-11,866.72 万元，较 2023 年同期减少 1107.04%。

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