

证券代码：300379

证券简称：东方通

公告编号：2022-定-001

北京东方通科技股份有限公司 2021 年年度报告摘要

一、重要提示

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，投资者应当到证监会指定媒体仔细阅读年度报告全文。

除下列董事外，其他董事亲自出席了审议本次年报的董事会会议

未亲自出席董事姓名	未亲自出席董事职务	未亲自出席会议原因	被委托人姓名
-----------	-----------	-----------	--------

大华会计师事务所(特殊普通合伙)对本年度公司财务报告的审计意见为：标准的无保留意见。

本报告期会计师事务所变更情况：公司本年度会计师事务所由变更为大华会计师事务所(特殊普通合伙)。

非标准审计意见提示

适用 不适用

公司上市时未盈利且目前未实现盈利

适用 不适用

董事会审议的报告期普通股利润分配预案或公积金转增股本预案

适用 不适用

公司经本次董事会审议通过的普通股利润分配预案为：以本次权益分派实施公告中确定的股权登记日当日的总股本为基数，向全体股东每 10 股派发现金红利 0.90 元（含税），送红股 0 股（含税），以资本公积金向全体股东每 10 股转增 0 股。

董事会决议通过的本报告期优先股利润分配预案

适用 不适用

二、公司基本情况

1、公司简介

股票简称	东方通	股票代码	300379
股票上市交易所	深圳证券交易所		
联系人和联系方式	董事会秘书	证券事务代表	
姓名	徐少璞	韩静	
办公地址	北京市海淀区中关村南大街 2 号数码大厦 A 座 22 层		
传真	010-82652226	010-82652226	
电话	010-82652668	010-82652668	
电子信箱	tongtech@tongtech.com	tongtech@tongtech.com	

2、报告期主要业务或产品简介

（一）报告期从事的主要业务

东方通创始业务是为企业级用户提供基础软件中的中间件产品及相关技术服务。公司上市以来，一方面继续在中间件产品领域深挖市场需求，改善产品性能，提升用户体验，巩固国产中间件行业领先地位；另一方面，通过新设投资、收购等资本手段，拓展新业务，完善在网络信息安全、大数据、人工智能、5G 通信等新技术、新业态、新模式的布局，为用户提供基础软件产品及技术服务，同时继续为政府、电信运

营商等行业用户提供领先的信息安全、网络安全、数据安全、智慧应急、政企数字化转型等产品及解决方案。

东方通的产品及解决方案广泛服务于国内数千个行业及相关业务领域，拥有电信、金融、政府、能源、交通等行业领域5,000多家企业级用户和2,000多家合作伙伴。公司连续十余年被认定为“国家规划布局内重点软件企业”，是“中国软件行业最具影响力企业”、“北京软件和信息服务业综合实力百强企业”，是商务部、国资委认证的“企业信用评价AAA级信用企业”，曾荣获“国家科技进步二等奖”、“北京市科学技术进步奖二等奖”等多项荣誉。

1、基础软件中间件业务

报告期内，公司专注于基础软件Tong系列中间件的研发、销售与相关技术服务。公司中间件产品已在政府、交通、金融、电信、军工、能源、企业等行业树立了众多典型应用案例。依托信息技术应用创新产业发展带来的市场机遇，报告期内中间件业务在用户覆盖和产品应用的广度、深度均取得了一定突破性进展：继续深耕布局政务市场，进一步巩固在国内厂商的领先地位；在能源类等央企方面取得突破性进展，预期未来将在企业市场取得更多拓展机会；尤其在金融市场领域，彻底改变了以往以央行、头部大型银行机构、股份制银行、城商行用户为主的局面，市场覆盖至更多商业银行，以及证券公司、保险公司、公募基金、期货公司、各类证券或商品交易所及监管机构等多行业，并呈现出应用服务器、消息中间件、通用文件传输平台等多产品综合覆盖态势，同时应用服务器产品的应用范围也由以往的管理类系统逐渐向业务类系统逐渐深入使用，各类中间件产品在关键业务中的规模化应用逐渐显现。

通过在基础软件领域20余年的开拓，公司在中间件核心技术方面积累了较为深厚的能力和丰富经验，形成品类完善的产品体系，并在保持持续迭代升级的同时，跟踪技术发展趋势不断推出满足市场需求的新款产品，服务客户IT系统建设。报告期内，专利和软著数量保持稳步提升，生态体系建设加速推进，已与全国20余个省市的信息技术应用创新联盟、基地等开展合作。公司连任信息技术应用创新工作委员会中间件工作组组长单位，参与主导制定的6项中间件团体标准已发布，并配合金融行业权威机构参与主导制定10余项金融行业中间件验证规范。此外公司在中间件云原生、可信安全、智能运维等方向持续投入，产品在云化程度、安全防护能力及规范性、运维能力等方面均进一步增强。

2、网信安全业务

全资子公司东方通网信专注于网络安全、信息安全和通信业务安全领域的研究和应用，同时在数据安全、工业互联网等新兴领域内进行拓展。东方通网信充分发挥自身技术特长，以业内领先的网络数据采集分析能力为基础，结合网络安全新技术，深入研究网络空间中各种安全事件的特征、演变及传播形态，遵循国家有关法律法规要求，在安全事件研判、分析、预警、处置等方面积累了丰富的技术手段，形成了多样化、多场景的解决方案。

(1) 信息安全方面：目前公司具备业界领先的网络内容审计产品，已获得权威机构的检测认证，能够对5G消息、互联网流量、网站、“两微一端”中的文本、图片、视频、音频等内容，及时发现涉政、涉黑、涉黄、涉诈、商业广告、垃圾信息等非法网络信息内容，现已广泛应用在国内电信运营商，对IDC、城域网、2/3/4/5G移动互联网等网络内容进行审计，同时该产品已经已经在监管部门，电力、政府、金融、医疗等行业进行推广、试用。

(2) 网络安全方面：目前公司产品已经可以覆盖电信运营商的IDC机房、城域网、骨干网的网络攻击检测和防护、2/3/4/5G手机恶意软件的检测和治理、互联网僵尸木马病毒的检测和阻断，并应用人工智能、大数据分析技术实现网络异常的发现和处置，以及针对内网安全内审内控类产品解决方案，包括：公司持续为各企事业单位提供设计定制化网络安全解决方案，主要包括4A及IAM、安全评估与检测、数据安全管控、漏洞全生命周期管理、零信任、安全运营管理、IDCISP网安及数安升级改造等一系列网络安全解决方案。。产品同时支持运营商以外行业用户，如政府、企事业单位、金融等。

(3) 通信业务安全方面：目前公司具备业内领先的通讯信息诈骗治理系统，以“数据驱动、技管结合、以技防诈、打防结合、信息共享、综合治理”的理念，利用大数据、人工智能等技术，提供涉诈号码检测、涉诈网址分析、涉诈APP识别、涉诈短信检测、潜在受害用户提醒、深度受害用户发现等涉诈信息检测能

力，现已广发应用在国内电信运营商，并正在地方公安厅局、通信管理局等监管部门进行推广、试用。

(4) 数据安全方面：公司针对日益受到重视的数据安全保护需求，基于核心流量监测分析技术，提供各种数据安全监测和控制产品和方案，同时提供数据安全管控平台，实现数据安全的集约化管理，可有效支撑电信运营商、工业企业等的数据安全管控能力，降低数据泄露风险。

(5) 工业互联网安全方面：公司根据已有技术储备，结合工业互联网安全需求，进行了有关工业敏感数据检测方面的开发，产品已经实现现场验证和部署，为工业互联网数据安全提供有效保障。

3、智慧应急业务

全资子公司泰策科技聚焦智慧应急、工业互联网、运营商及企业DNS业务，目前主要集中在应急综合指挥调度、自然灾害、城市安全和安全生产四大领域。公司着力帮助应急管理部门全面提升信息化专业能力，从天地一体化、全时空、全要素的数据监测分析，到案例详实的知识图谱应用，为客户提供精准的综合监测预警服务，并在防灾、减灾、救灾的应急业务过程中，提供信息平台的支撑，提供可视化的一体化指挥调度，提供专业的分析研判报告，为领导提供辅助决策的科学依据。以工业互联网+安全生产为抓手，面向矿山、危化、能源、钢铁、汽车、军工等行业提供大数据平台、安全生产标准化系统、安全生产监测预警系统、工业物联网平台、工业互联网标识解析及标识应用、工业互联网+安全生产等产品和解决方案，助力企业数字化转型和智能化升级。

公司立足应急管理部应急体系整体规划内容和省级建设任务，分析现有产品、技术和外部资源条件，形成以国家应急管理框架为顶层架构的智慧应急业务产品线。报告期从事的主要业务如下：

应急行业解决方案包括监测预警和应急综合指挥调度。其中监测预警包括自然灾害综合监测预警、安全生产监测预警、城市安全风险综合监测预警、森林消防监测预警；应急综合指挥调度包括应急指挥救援、应急通信指挥和应急一张图。

自然灾害综合监测预警充分利用云计算、大数据、物联网、区块链等新技术，建设应急和常态两种模式下针对多灾种和灾害链的灾害综合风险研判评估体系，形成并完善多尺度、全方位、全过程重大自然灾害监测预警能力，提升重大灾害风险防范化解与决策支撑能力。

安全生产标准化系统遵循《企业安全生产标准化基本规范》等法规和制度，在目标职责、制度化管理、教育培训、现场管理、安全风险管控及隐患排查治理、应急管理、事故管理、持续改进8个方面提供全流程的电子化在线管控能力。

安全生产监测预警系统遵循《危险化学品企业安全风险智能化管控平台建设指南（试行）》等文件，以物联网和AI视觉识别为技术抓手，增强工业企业安全生产的5种新型能力即感知、监测、预警、应急处置和系统评估，提供全流程的智能化在线管控能力。

森林消防监测预警利用大数据、云计算、人工智能、GIS等信息技术，通过感知网络，全口径归集消防安全领域数据并深度融合，构建一张图任务部署、风险评估、调度指挥、决策支持等业务应用，实现火灾风险评估预警、火灾隐患排查整治、重大活动安保安防高效组织，安全态势智能感知，分析研判数据洞察，应急指挥“秒级”响应、高效协同，全过程精准监督，考核评估科学可靠的立体化、智能化、实战化的消防安保指挥调度体系，全面提升事前、事发、事中和事后全业务链应用支撑能力。

应急综合指挥调度纵贯部、省、市、县四级应急管理部门，横跨公安、交通、地震、水利、消防等业务部门，通过利用网络通信等基础设施和融合通信、音视频会商、GIS协同标绘、一张图可视指挥等信息系统，实现跨层级、多部门一体化应急指挥调度，全面提升应急管理抢险救援能力。

4、数字化转型业务

报告期内，公司全面布局“安全+”、“数据+”、“智慧+”战略，用安全为社会数字化转型保驾护航，用数据为政企数字化转型提供最佳路径，用AI为政企数字化转型提供智慧赋能。遵循“开放、合作、共赢”，通过与各大专院校、科研院所深入广泛合作优势互补，现已初步具备领先于业界的数字化转型前沿技术支持与应用能力。围绕主航道，加强核心技术研发，持续提升基础能力；强化员工服务意识，深入研究业务需求，增强业务沟通交流，不断迭代产品能力；广开合作渠道，发挥各自优势，共同服务客户，快速形成

能力；维护战略客户，拓展市场范围，积累客户资源，赢得发展空间，形成获客能力；引入优质资源，助力企业发展，形成高速发展能力。

(1) 在国防军工领域，在公司“安全+”、“数据+”和“智慧+”战略的基础上，综合运用大数据、云计算、物联网、区块链、人工智能、5G通信方面的积累和研发能力，探索国防及军工数字化转型的新航道。以军事数据工程为主航道，提供军事信息系统融合和业务服务支撑，业务逐步拓展至军事资源管理、军事资产管理、数字化战场等多个领域，适应军队体制改革发展，提升军队信息化管理效率，服务军队数字化转型。

在自主研发的数据中台、资源管理系统、综合信息服务、数字化战场、时空大数据、智慧探测、大数据处理与共享交换等解决方案与产品的基础上，以数据中台的数据管理能力和军事资源系统的业务能力为核心，面向军事人员管理、军事物流、作战指挥、侦察情报、数字政工的业务支撑需求，提升数字孪生、多模态数据集成、跨域交换、身份查验、知识图谱、时空大数据分析等能力，提升数据管理、业务应用与军队其他业务系统协同联动能力，提升公司产品的业务集成适配能力。主要产品包括业务领域相关数据平台、业务平台、共性组件、业务模组。具有数据采集、数据存储、数据治理、数据计算、智能分析等大数据支撑能力，满足行业信息服务、业务服务需求。此外，提供跨网跨域数据交换平台、身份认证与信息查验等配套产品。

报告期内，公司在军事资源管理、军事资产管理方面获得了多个项目，并持续跟进，获得了新的项目机会，行业地位稳定，服务范围不断扩大，发展势头良好。

(2) 在政企数字化转型领域，公司秉承“助力网络强国、服务数字中国”的理念，依托前沿技术，深度融合与挖掘业务数据效能，为政企单位和行业提供前瞻性的业务模式，构建“数据+”和“智慧+”产品体系，结合数字孪生技术，打造面向公共安全、司法、教育、数字政务“3+1”行业的“数智化”产品和整体解决方案，并在行业中得到了广泛的应用。尤其是在北京2022年冬奥会和冬残奥会中，东方通作为智慧重保解决方案提供商，深度参与各赛区相关的应急通信保障以及公共安全工作，所提供的“全天候、全场景、零中断、零故障”的智慧重保平台得到客户高度认可。

在企业方面，公司以能源电力行业为业务主航道，基于电网快速变化的需求打造组件化、嵌入式的数据能力，提供包括业务中台、技术中台、数据中台、人力外包四部分能力建设，并建立专业的劳务派遣团队支撑电网核心业务；以社会安全防控领域、制造业为辅助航道，通过数字转型解决方案交付来快速沉淀产品能力，实现其自身的数字化、智能化转型升级。

(二) 报告期内主要业绩驱动因素

报告期内公司业绩稳步持续增长，实现营业收入86,316.07万元，较上年同期增长34.80%；实现营业利润26,291.12万元，利润总额26,187.25万元，归属于上市公司股东的净利润24,810.33万元，同比增长1.53%；归属于上市公司股东的扣除非经常性损益的净利润22,122.97万元，同比增长31.89%；研发投入24,275.54万元，同比增长20.52%。

1、多举措促进主营业务竞争力持续提升

报告期通过行业深耕、平台建设、渠道拓展、生态建设、标准制定、培训赋能多种等举措，充分挖掘已有客户与合作伙伴资源，保持在传统优势市场的领先地位，同时在新兴领域市场方面实现新的突破，促进公司主营业务竞争力的持续提升。具体表现为：

(1) 持续优化完善各业务版块营销平台建设，实现营销网络全国覆盖。继续在政务、电信、交通、金融等传统优势行业深耕，巩固领先地位，积极拓展应急、军工、能源、政法及其他企业等新兴市场，实现新的突破；

(2) 以客户为中心，及时、高效的为客户提供服务，依托现有的技术优势和人才优势为用户提供全面的技术支持、咨询服务。目前已在全国30个省级地区均部署了服务网点，实现本地化服务，提升用户满意度；

(3) 进一步拓展渠道合作伙伴，与华为、阿里等头部公司开展生态合作。

东方通是华为的重要战略合作伙伴，技术创新方面：东方通多款中间件产品完成TaiShan服务器兼容

认证，基于鲲鹏平台进行深度优化，实现性能提升60%以上；生态建设方面：东方通加入openEuler、openGauss社区，与华为共建基础软件生态；市场合作方面：应用服务器TongWeb入驻华为开发者联盟市场，上架华为云市场严选商城，成为严选自营产品。

公司与阿里在市场、渠道、项目、产品等多方面展开合作。成为首批阿里云计算巢认证合作厂商，加入龙蜥社区及云峰、云原生等合作伙伴计划。应用服务器TongWeb已完成阿里专有云、PolarDB适配，实现与EDAS的产品深度融合等。

(4) 主持或参与国家相关信息安全、中间件等多项技术标准制定，作为信息技术应用创新工委会中间件工作组组长单位组织协调行业工作并取得良好成效，并与行业专业研究机构、科研院所、高校开展战略合作，扩大行业内影响力。

(5) 建立“线上+线下”的培训体系，对内加强新产品、新技术宣导，对外结合当前信创人才的现状和公司在中间件领域的技术优势，深化产学研合作，积极开展信创培训工作。2021年开展中间件认证培训班共7期，培训学员超过1500+人次。公司出版了《TongWeb中间件实用教程》一书，写作素材源于实际工程项目，有利于相关企业软件工程师、运维工程师、及高校师生学习TongWeb中间件技术。

2、受益于国家产业政策支持

2021年正处于十四五规划首年，《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》发布，我国软件业运行态势良好，业务收入保持较快增长，盈利能力稳步提升，软件业务出口保持增长，从业人员规模不断扩大，“十四五”实现良好开局。同时，伴随着我国信息技术应用创新产业的蓬勃发展，以及近年来《网络安全法》、《密码法》、《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》、《网络产品安全漏洞管理规定》、《网络安全审查办法（修订草案）》、等保 2.0 标准等多项政策法规和标准的发布与实施，为公司带来良好的发展基础。

3、加大研发投入力度，赋能公司综合竞争力

公司一直高度重视产品研发和技术进步，并致力于不断的技术创新提升公司的竞争力。报告期内公司研发投入242,755,358.60元，较上年同期增长20.52%，研发投入占营业收入比例为28.12%。除北京总部外，在成都、武汉、郑州、广州等地分别建有研发基地。公司拥有自主研发的多项软件著作权及产品证书，并取得多件国家专利授权证书，近年来多次承担国家重大科技研究课题任务，主持或参与国家技术标准制定，获得国家、北京市的成果转化、创新基金等方面的资金支持。

(三) 主要产品及其用途

东方通坚持“自主可控，安全创新”的核心发展理念，依托基础软件的技术积累，拓展政务、金融等特定行业解决方案，为用户提供基础安全产品及解决方案，同时继续为电信运营商等传统用户提供领先的信息安全、网络安全、数据安全等产品及解决方案，依托“安全+，数据+”两大产品体系，提出“智慧+”战略，开始在政企数字化转型领域进行产品布局。业务领域从政务、金融、电信、交通等传统优势客户拓展至应急管理、自然资源、教育、法检、公安、国防军工、能源电力等行业领域。

公司主要产品及用途如下：

1、“数据+”产品家族（中间件板块）

产品名称		产品用途
应用支撑	应用服务器 TongWeb	作为基础架构软件，位于操作系统与应用之间，帮助企业将业务应用集成在一个基础平台上，为应用高效、稳定、安全运行提供关键支撑，包括便捷的开发、按需应变的灵活部署、丰富的运行时监视、高效的管理等。

产品名称	产品用途	
消息中间件 TongLINK/Q	作为一个消息传递的可靠平台,应用系统可以借助于它轻松地交换和处理消息,而无需考虑消息传递的具体细节,能够大大降低开发难度,缩短开发周期,节约开发成本。	
交易中间件 TongEASY	在分布式交易处理(DistributedTransactionProcess)中负责正确传递交易,管理交易的完整性,调度系统资源和应用程序均衡负载运行,保证整个系统运行的高可靠性和高效性。使用TongEASY可以简单方便地开发出可靠、高效的分布式交易处理应用系统。	
高速传输平台 TongHTP	采用异步、松耦合来设计和实现,从技术架构上来保证产品具有高灵活性、高可用性、高效性等。不同节点之间的数据传输提供异步、可靠的数据传输服务,通过在节点之间建立传输通道,实现互联互通,应用程序只需要调用提供的API即可实现消息的可靠传输。	
分布式数据缓存中 间件 TongRDS	为信息化系统提供基于内存的数据高速缓存、分布读取功能,极大提升系统数据处理速度。通过先进的内存分配算法、高性能网络同步技术,实现了热点数据的高速读写、实时数据同步、集群化部署等关键能力,满足信息化系统的分布式与高可用使用场景。	
负载均衡软件 TongHttpServer	在应用系统集群中位于应用服务器前端,将多个应用服务器节点组成集群,内置多种负载均衡算法将请求分发到不同节点,提升应用系统的吞吐量、可伸缩性;卓越的静态文件处理能力,可作为资源服务器、动静分离服务器使用;国密和标准HTTPS自适应,可满足系统对国密和标准HTTPS同时需求的场景;支持四层反向代理和负载均衡。	
数据融合共 享	ETL工具TongETL	针对企业级用户日益增长的数据管理需求而开发的、面向数据集成领域的专业ETL工具,可以方便地将各个系统中大量的、异构的数据整合成完整的、一致的、准确的、可集中存取的数据,并解决数据准确性与有效性问题。协助用户实现数据资源的整合、数据价值的挖掘、数据服务的创新,有效促进用户数据资源的开发利用。
	通用文件传输平台 TongGTP	面向分布式应用的文件传输平台,提供满足企业级应用需要的通用文件传输功能。采用成熟的消息中间件提供底层队列传输服务,从而保证了文件传输和可靠和稳定性。同时,GTP平台提供企业大数据量传输所需要的各种管理、部署和安全功能,使其方便易用。借助此平台用户无需编码,只需进行简单的配置就可以轻松实现不同节点间的文件可靠、安全、高效的传输。
	互联网文件 传输平台TongWTP	基于互联网的文件传输平台,提供客户端到服务器之间通过Internet网络进行可靠、安全、可控、高效的文件传输。用户通过TongWTP可以实时管理和监控所有Internet客户端的传输,监控系统运行、传输状态、查询统计传输流量等。
	数据交换平台 TongDXP	公司结合近20年数据集成实践经验,抽象、归纳多种常见的数据交换的开发模式、应用模式和管理模式,为解决政府和企业多层级、跨地域、多部门间的数据资源的交换共享和业务协同支撑而研发的集数据交换共享、交换目录、统一管控于一体的专业数据交换平台软件。
	企业服务总线 TongESB	TongESB是集服务集成、数据整合、消息交换于一体,致力于为用户提供符合SOA架构的中间件运行环境和开发、管理工具,充分利用其提供的分布式企业服务总线和服务化技术,解决用户的应用集成问题,同时为用户提供集中统一的服务目录、服务生命周期、监控审计、权限及简易服务等管理功能。

产品名称	产品用途
API网关产品 TongGW	提供统一的服务生命周期管理能力,能够将所有服务统一规范,统一接入,形成统一的服务目录对外提供服务,同时统一服务调用接口和方式,建立按需服务的管理平台,真正做到可管、可监、可控、可用;同时统一对外暴露服务,实现服务路由、协议转换、服务编排、灰度发布、鉴权、流控等能力。
服务编排 TongIS	提供统一管理和服务集成的功能,通过可视化的工具实现零代码开发的服务集成功能。支持应用和数据集成、消息传输和集成安全性。为用户提供高效、灵活、安全和规模化的服务集成平台。

2、“安全+”产品家族（网信安全板块）

产品名称		产品用途
网络安全	互联网僵尸蠕虫监控系统	主要面向省网出口节点、IDC机房出口、骨干网出口、国际网出口提供全面僵尸蠕虫监测手段，通过网络数据分析和逆向工程方法，分析恶意程序的通信特征、行为特征、数据报文特征，发现僵尸网络、木马、蠕虫等网络恶意程序的源头、目的地信息，满足新时代网络安全保护工作的要求。
	违规恶意链接检测系统	通过对上网日志、实时流量、系统日志、CDN缓存等各类数据进行数据的预处理，结合“威胁情报库”对海量数据中的链接进行识别分析；构建多层的机器学习模型，实现“自更新、自学习”；通过可配置的时间区间，对黑白名单内的数据进行生命周期监控；可对重点网站、页面进行定期/不定期监控，实现“篡改发现”。
	信息安全管理系统	主要覆盖IDC/ISP、互联网专线、CDN、IRCS的互联网数据资源内容的监控，满足工信部规范的标准功能：基础数据管理（实现对机房及用户的基础信息采集、管理和上报。主要包括：基础数据的分类、基础数据本地管理、基础数据上报与核验、基础数据监测和处置）；信息安全管理（实现异常IP监测、违法违规网站管理、违法信息监测发现、违法信息处置）；访问日志管理（实现访问日志记录功能、日志记录查询方式、日志记录查询结果、日志留存时间）。
	移动互联网恶意程序监控系统	主要面向移动互联网（2/3/4/5G）进行恶意程序的监控与处置，系统主要包括：分析模块（信令面流量和用户面流量解析分析，恶意程序研判分析）；处置模块（基于五元组以及手机号码对恶意程序进行处置）；集中管理模块（获取分析模块的上报数据，并下发处置策略至处置模块，具备样本捕获以及静态和动态研判分析功能）。
	5GDPI	主要面向5GSA组网进行设计，满足运营商的核心网组网模式，提供了多种部署方式，并且满足全部信令面和用户面的数据采集和解析功能，其中，信令面包括N1、N2、N4~N8、N10~N16、N22、N26、N40、Gm等接口；用户面包括N3接口。5GDPI核心解析模块主要包括业务特征库和DPI引擎，当业务数据流经过DPI引擎模块时对其进行特征匹配处理。基于业务识别，可实现对不同业务的差异化调度，提高每比特的业务收入，并优先保证关键业务的用户感知。
	数据安全检测设备DAU	基于DPI/DFI技术解包还原网络协议（如HTTP）及携带的文件，实现文件还原、协议识别（包括VPN类、工控类）、数据资产识别分析、敏感数据主动发现、数据分级分类、数据异常访问、数据跨境传输、数据安全风险监测等功能。
	高级网络安全检测设备AU	具备扫描探测、暴力破解、漏洞利用、Web攻击等网络攻击监测、远程控制活动及恶意程序传播活动等恶意程序网络活动监测、已知恶意程序及未知恶意程序文件还原检测、常见隐蔽通信隧道及异常流量等网络异常行为检测等功能。
	IDC网络安全监测系统	在IDC机房及互联网专线机房建设网络安全监测设备，实现对各机房出口链路的流量采集、协议识别、资产识别、流量安全监测、恶意文件检测、监测结果上报、PCAP包留存、封堵处置、指令监测、设备状态上报、以及与监管部门接口功能。

产品名称	产品用途
漏洞全生命周期管理	以满足《网络产品安全漏洞管理规定》要求为基础，解决企业漏洞管理痛点为目标，打造集系统、资产、人员、漏洞为核心的多边形漏洞生命周期管理解决方案，安全策略为核心，流程为驱动，通过整合漏洞扫描工具实现安全漏洞的全生命周期闭环管理，立漏洞全生命周期的管理能力，结合企业实际业务需求，形成流程化的漏洞生命周期管理过程，规范企业安全漏洞管理过程，实现包括漏洞发现、漏洞验证、漏洞整改、漏洞归档在内的漏洞闭环生命周期管理过程，完善漏洞扫描机制，摸清资产家底，通过扫描器智能任务分发能力，结合自动化、智能化、场景化的分发机制，解决因IP范围过大、扫描器状态异常、重要场景无保障的任务执行错漏的问题，整合可视化的流程编排能力，通过对漏洞扫描节点、任务及相关参数的可视化编排，按需定制漏洞管理流程，解决因企业安全管理业务多样化、复杂化而导致的失效、失职、失能构建漏洞风险展示模型，输出可视化漏洞综合评估结果，从资产、用户、利用情况等多维度展示现网安全漏洞风险状况。帮助用户在安全管理工作实施过程中有的放矢。
数据安全管控	以国家法律法规、行业标准规范为指引，采用“管理管控双管齐下”的方式，围绕数据全生命周期，构建由内到外的主动安全纵深防御体系，从威胁防御、风险管控、数据追踪溯源、数据共享与交换等多个层面，打造数智化数据安全产品，面向多行业提供数据安全一站式全景化的解决方案，全面落实企业数据分类分级、数据对外接口管理、数据安全风险监测、数据泄露分析溯源等多方面数据安全能力，具有“能力自动化、分析智能化、交互便捷化、效果可视化”等显著特点，从而辅助用户科学规划安全体系、全面提升企业自身安全防御及风险感知能力。
零信任	以身份为认证主体，将身份数字化，持续的信任度评估，动态调整访问策略，隐藏资产及数据信息。通过终端容器实现终端与应用访问环境的微隔离，并实现轻量化的图形审计，使用基于零信任的软件定义边界模型，替代传统的VPN网络通道方式，建立应用级别的访问链接，实现业务安全访问，用户只能访问最小权限内的资源。通过可信度计算模块与策略模块联动，实现动态的策略下发，网关根据策略信息对资源的异常访问行为进行二次认证或阻断，为保障用户资源安全访问起到重要作用。
安全运营管理	以安全能力、安全数据和安全管理为核心，内聚安全能力与数据资源，实现安全功能的云化、集中化、标准化，为用户打造“集中管理、按需服务”的立体化安全防御体系。以沉淀能力、支撑发展、数智赋能为目标，聚焦“中台建设”与“中台运营”两条主线，发挥现有“安全系统能力多样、安全数据资源丰富”的优势，打破各安全系统竖井现状、消除各部门资源共享壁垒、沉淀安全创新能力、对内强化安全能力集中管理，对外提升安全公共服务水平，构建可持续运营的安全服务能力达到“数据融合、能力协同、统一指挥、联动治理、能力开放”的总体目标，从而实现传统安全运维向着更高效化的安全运营模式转变。
IDCISP数据安全监测系统	统筹整合企业内外部网络数据安全技术能力，健全完善企业网络数据资产梳理与分级分类保护技术措施，通过建设政企联动的数据安全风险监测追溯与综合管理平台，实现数据流动态监测、数据安全风险源头定位能力，实现行业数据安全风险实时监测、溯源核查、态势感知、精准定位、快速响应、高效管理能力，全面提升行业数据安全风险/事件的事前、事中、事后的技术管理水平。

产品名称		产品用途
工业互联网安全	工业互联网安全监控系统	为工业制造和智能制造提供保障体系包括政策保障、标准保障、运营保障、运维保障、安全保障等。系统主要包括智能连接层（支持多种设备连接协议，支持工业智能网关接入、适配传输介质）；智能平台层（涉及微计算服务、工作流引擎、分布式存储及大数据处理，提供各种相关服务的核心框架支撑，支撑基础云平台上各种相关的核心服务应用）；智能应用层（涉及管理应用、业务应用、分析应用及门户等，基于智能平台层开发和运行的各种制造业、服务业务应用）；
	物联网安全态势感知平台	通过采集各终端、安全设备、网络设备、中间件、数据库等网元的日志和状态信息，以及实时网络流量数据，形成安全、资产、业务等多维度整体态势视图，使用户快速直观的把握当前网络安全状态，并且为用户加固安全防护方向提供事实依据。
通信安全	DNC产品	支持INAP/SIP/ISUP/BICC/CAP/WIN等多种信令接入，适应目前中国国内三大运营商网络现状，并预留未来接入5G网络的能力。系统采用大数据分析技术，精确的算法分析处理，提供智慧数据分析管控方案系统采用在线实时采集呼叫数据以及CDR话单采集的方法，呼叫分析模块通过分析信令消息结构获取相关主被叫信息，并通过大数据分析装置进行实时分析。
	语音管控产品	实现对语音专线业务的集中化管控，包括基础信息配置管控，专线外呼管控，外呼话单审核管控机制。提供存储并管理系统级的主体库、非主体库等；疑似告警话单的审核机制，以及外呼统计分析能力等。整体平台系统分为外呼控制平台和集中管理平台，管控平台实现管控分离结构，有效的降低了专线的诈骗和骚扰案件。
	云通讯客户中心服务平台	基于开源软交换的平台，建设满足“语音、微信、微博、IM、APP、邮件、Webchat、视频”等语音话务控制、多渠道多媒体接入、统一排队、统一路由的云客服后端通讯交互平台，提升客户针对骚扰事件的防治能力。
	云通讯信息控制平台	立足于降低骚扰电话困扰，基于呼叫的情况，从通话行为、通话内容入手，采用相适应的技术手段，营造良好的绿色通话环境。一是在通话行为方面，源于xDR话单、信令、日志的基础上，建设骚扰电话分析模型，通过机器学习等检测模型对骚扰电话等进行识别发现，采用大数据分析技术和机器学习技术，包含数据采集清洗，特征构建，辅助无监督聚类分析，自动迭代等功能模块，各模块共同构成骚扰电话分析模型，构建一套可以自行迭代的，适用性强的骚扰电话分析系统；二是在通话内容方面，采用“智能+人工”双重机制，其中智能质检使用音频解析技术，根据已创建的质检规则，对通话内容进行识别、质检，然后加以人工复检的手段，进一步完善稽核流程。
	5G路测	路测产品具备5G网络的NSA和SA两种组网方式下的测试及分析能力，同时向前兼容2G/3G/4G/NB-IoT网络制式，可实现一套系统测试目前所有移动通信网络的目的。芯片方案包括当前主流的高通和海思方案，产品形态包括基于Windows的PC产品、基于Android的APP产品、以及平台类产品。系统集网络数据采集、存储、分析、定位、报告等众多功能于一身，广泛运用于网络评估、网络优化、单站验证、投诉处理、故障处理等多种场景，且贯穿移动通信网络的整个生命周期。
通信安全	通讯信息诈骗治理系统	通讯信息诈骗治理系统内聚用户基础数据资源与分析能力，有效融合多种通讯信息网络业务数据，以“数据驱动、技管结合、以技防诈、打防结合、信息共享、综合治理”的理念，指导不同业务场景下输出符合其特点的体系化、实战化的新型通信网络诈骗打击治理体系架构，提供涉诈号码检测、涉诈网址分析、涉诈APP识别、涉诈短信检测、潜在受害用户提醒、深度受害用户发现等涉诈信息检测能力。

产品名称		产品用途
安全服务云平台	网络内容风控系统	网络内容风控系统主要通过爬取、流量还原、识别内容主动送检等方式自动获取web网页、媒体客户端、社交通讯、短视频、管道流量的内容，并进行内容安全审计，及时发现可能存在的涉黄、涉暴、涉恐、违禁、涉政、商业广告、挂马、暗链等不良信息并进行处置。
	5G消息不良信息监测系统	5G消息不良信息监测系统主要对5G消息中的文本、图片、音频、视频、URL进行监测，及时发现涉政、涉黑、涉黄、涉诈、商业广告、垃圾信息等非法网络信息内容。

3、智慧应急产品线

产品名称	产品用途
自然灾害综合监测预警	<p>围绕地质、海洋、水旱、农业、气象、地震、森林草原等自然灾害，结合自然灾害风险普查和隐患排查的重大风险与隐患区域，构建起重大风险隐患全覆盖的多层级自然灾害监测预警体系，实现跨地域、跨层级、跨系统的自然灾害监测和实时预报预警，提高多灾种和灾害链综合监测、风险早期识别和预报预警能力，为及时有效防范化解自然灾害风险提供有力支撑。</p> <p>—实现感知全域覆盖。针对自然灾害重大风险和隐患区域，健全完善地质、海洋、水旱、农业、气象、地震、森林草原等灾害监测感知手段，形成空、天、地、海一体化全覆盖的自然灾害监测感知网络体系。</p> <p>—实现监测全面汇聚。通过跨部门、跨地域、跨层级的自然灾害监测预警信息共享交换机制，实现地质、海洋、水旱、农业、气象、地震、森林草原等灾害感知数据全汇聚，实现信息共享共用。</p> <p>—提高风险早期识别能力。基于空、天、地、海全覆盖高分辨率实时动态感知技术，结合大数据、云计算、神经网络、人工智能等技术，提高单一自然灾害以及多灾种、灾害链的综合监测和风险早期识别能力。</p> <p>—提升预报预警精细精准水平。提升单一自然灾害监测预警能力，构建多灾种和灾害链监测预警模型，实现对自然灾害的精确分析研判和精准预报预警。</p> <p>—实现预警靶向发布。统筹自然灾害预报预警信息发布资源，综合运用现代信息手段，拓展完善信息发布渠道，提升预警信息发布的覆盖面、精准度和时效性。</p> <p>—实现全过程监测预警。将监测预警体系从灾前防范向灾中应急、灾后处置延伸，实现对自然灾害的全过程监测预警。</p>
安全生产监测预警	<p>通过云计算、大数据、人工智能、物联网等技术在安全生产中的融合应用，创新管理，提升生产本质安全水平。</p> <p>1.在企业安全生产管理方面，建立了安全生产管理制度，通过系统能力对安全生产标准化体系和双重预防机制等制度进行安全管理。</p> <p>2.在物的不安全状态管控方面，对安全数据进行监控，DCS、有毒有害气体检测等系统能够对工艺过程和设备运行等数据进行实时监测、显示和异常数据报警。但目前与安全相关的系</p> <p>3.在人的不安全行为管控方面，建立了安防监控和生产监控视频系统，实现对生产过程视频全覆盖。</p>

产品名称	产品用途
城市安全风险综合监测预警	以“风险管理、关口前移”主动式安全保障为理念，将公司具备优势的公共安全与应急平台软件业务通过物联网技术延伸到城市安全领域，主要涉及城市生命线工程监测监管业务中的专业监测预警软件与核心监测传感装备，包括燃气、桥梁、给水、排水、热力、电信、电力、工业、道路和综合管廊安全运行监测数学物理模型、大数据监测预警系统、恶劣环境燃气探测装备等。以预防燃气爆炸、桥梁垮塌、路面坍塌、城市内涝、轨道交通事故、电梯安全事故、大面积停水停气等重大安全事故为目标，通过公共安全物联网感、传、知、用的技术架构和城市生命线公共安全科技模型，建立“城市安全监测物联网+云服务”体系，准确判断定位事故点，预先感知风险、及时预警。通过城市生命线安全运行监测系统建设，提升城市风险管理效率，降低风险应对成本，增强城市公共安全风险预警和管理能力，切实降低城市事故风险发生率。使得城市安全风险管控能力不断强化，城市应急救援机制不断完善，提升城市精细化管理水平，人民幸福感和安全感不断增强。
应急通信指挥	根据平战结合的原则，把平时、急时和战时的应急通信保障工作有机结合，真正实现“平时服务、急时应急、战时应战”的目标。平台通过整合运营商通信网络管理能力，建设“数据集中、综合监测、统一指挥、全面保障”的信息化管理平台，实现网络状态的实时监测、应急指挥、通信保障、预警预案、智能分析和扁平化管理，提升重大活动应急通信保障能力和突发事件应急处置的通信支撑能力。同时，向通信管理局、市委市政府、工信部相关管理人员提供通信网络保障的统一展示、统一调度、统一任务发放、统一信息发布的平台。 平台以国家级应急平台为中心、地方政府应急平台为节点，多级灵活建设，达到既可以完成地方本地快速综合指挥，又可以进行多级应急平台联动指挥，确保上下贯通、左右衔接、互联互通、信息共享、互有侧重、互为支撑、安全畅通。

4、政企数字化转型

(1) “数据+”产品（政务数字化转型）

产品名称	产品用途
公共安全 智安会晤系统	面向大规模、高规格、高密集的政务会议场景，提供会议全生命周期流程的一体化、智能化会议信息管理平台。
司法行业 满意度评价系统	通过科学的采集感知服务信息，分析服务质量的监督平台。
教育行业 师生一张表教综系统	以师生全生命周期数据谱系为主线，一站式展示用户所有数据信息，实现对人员数据统计、分析、对比和监测等功能。

(2) “智慧+”产品（政务数字化转型）

产品名称	产品用途
公安行业 第四代指挥中心	以数字孪生技术为依托，融合构建数、图、音、视、人、车、物、事、流程的全息模型，服务现代指挥中心的管控系统。
公安行业 智慧重保管控平台	针对重大活动安保活动中，依托大数据、人工智能等前沿技术，围绕“人、地、事、物、组织”等全要素，构建纵向到底、横向到边的网状指挥管控体系。

产品名称		产品用途
	警用数据中台	基于数据中台核心技术，结合公共安全大数据和业务特点，构建由感知、认知和服务的数据处理平台。
司法行业	智慧诉讼服务平台	以行业信息化为依托，构建全方位、网络化、智能化诉讼服务平台
	互联网法院平台	使案件审理突破时间与空间的限制，更加便捷、高效的开展庭审业务。
教育行业	教育大脑决策系统	由基础资源、一体化智能化数据平台、校园运行生命体征和应用场景等要素组成，通过数据、模型和知识逻辑，实现对校园的运行状态和质量的监管。
	高校数据中台	解决数据的“采”、“管”、“通”、“用”四类核心问题，提升教育治理能力提供辅助决策，支撑高校运营服务升级。
数字政务	百年党建	党务工作全流程管理，对党员进行能力画像，为党员干部选拔赋能，用大数据驱动党管干部。
	社会综合治理平台	基于数据识别、大数据挖掘等自主研发技术，构建贯通上下、横向协同、反应快捷、支撑有力的信息综合治理平台。
	智能视频合规审计	基于AI、目标威胁检测等前沿技术，实现审计无盲区、无死角的安全审计保障能力，打造视频堡垒审计体系。

(3) “智慧+”产品（企业数字化转型）

产品名称		产品用途
敏捷数据管理产品 DataSmart	数据敏捷集成 DS-Hub	全栈式的应用与数据集成平台，聚焦应用和数据连接，适配多种企业常见的使用场景。提供轻量级快速集成数据、服务、消息等多种集成方式配合使用，统一目录管理，统一调度监控，统一权限。
	敏捷数据计算平台 DS-Flow	简便易用的图形化数据计算流程设计平台，提供拖拽式的数据计算算子。可用于数据治理场景、数据挖掘场景、数据统计分析、数据指标计算场景下的数据计算。
	敏捷数据治理平台 DS-Gov	以数据关系探查为主的治理工具，提供个性化的数据质量管理、元数据管理、数据血缘管理基础模块，可灵活组装和修改，敏捷响应不同业务场景下的数据治理需求，可视化监控并呈现数据治理全过程。
	敏捷数据安全管控平台 DS-SM	融合数据安全治理理念与人工智能技术，以“管理+管控”相融合的技术手段，提供数据自动分类分级、数据异常访问行为自动化分析、共享数据互访基线无干预建立、敏感数据日常行为智能化审计、数据安全态势感知等核心能力，保障数据全生命周期安全防护。

(四) 经营模式

公司所处行业为软件及信息技术业，采用设计+生产（开发）+销售型经营模式。虽然没有制造业生产加工环节，但具备完整的采购、研究、开发、测试、适配、售前、销售、售后服务等能力体系。公司根据市场上客户的需求，主要自主研发相关基础软件或应用软件产品，并提供相关技术服务，同时对以往的产品进行升级迭代、改造演进，开发出来的新产品能够通过现有的资源进行复制或者有足够的资金进行新的软件产品线建设，对于自己开发的软件产品通过自建的营销平台体系建立自己的直接客户群体或是生态渠道合作伙伴。

（五）业务模式

1、研发模式

公司产品以软件为主体，网络信息安全产品会根据客户的实际要求配置一定的配套硬件为载体，产品整体仍以软件产品为核心。软件按照相关研发流程进行开发，时间周期较长。软件发布后根据项目实际要求进行硬件的装配与调试，时间周期较短。

公司设有产品决策委员会，对公司产品开发规划、产品立项及其它重大问题进行审核和决策，对于每一个产品项目的研发及发布都基于软件开发与产品质量管理标准规范，严格执行和管理每个产品项目的生命周期全过程和成果发布，确保产品从产品需求确认、产品定义、产品立项、产品设计及实现到产品发布的各个关键节点和整个流程的顺利实施。

2、采购模式

公司的软件产品以自主研发为主，其中：

中间件业务除部分售后及技术外包服务外，一般不存在规模采购的情形，因此毛利率较高；

网络信息安全、智慧应急和数字化转型业务涉及采购的存货主要包括大流量采集设备、通用服务器、网络设备、物联网感知设备等硬件，以及少量第三方软件产品和技术外包服务。

公司组织架构设立采购部，主要负责各业务板块项目存货采购及固定资产购置等工作，采购流程主要包括采购项目评审会、项目预算编制、《对外采购申请单》审批、采购询价比价及谈判、采购合同用印审批、合同归档、到货验收、付款申请等。为满足公司采购产品和服务的质量要求，公司会根据供应商提供产品的供货能力、质量、价格、付款方式、售后服务及信誉度等因素对候选供应商进行综合评定，按照对比择优的原则，选择最佳合作供应商。

3、销售模式

（1）中间件销售

公司的中间件产品销售模式可分为直接销售和系统集成商销售两种模式，具体如下：

销售模式	简介	主要面向客户
直接销售	公司直接参与最终用户的招投标，中标后与最终用户签订销售合同，直接把产品销售给最终用户。	中国移动、中国电信、中国联通、中国人民银行、中国工商银行、中国农业银行等电信、金融行业大客户
系统集成商销售	1、公司通过与规模较大系统集成商合作，进行产品绑定，共同参与最终用户的招投标，中标后与系统集成商签订销售合同，通过系统集成商把产品销售给最终用户。	财政部、人力资源和社会保障部等中央政府机关
	2、由集成商选择中间件产品，公司与系统集成商签订销售合同，通过系统集成商把产品销售给最终用户。	地方政府机关、交通、电信、金融行业的地方企业

公司拥有独立完整的销售体系，具备直接面向市场的独立经营能力，与系统集成商是合作伙伴的关系。通过系统集成商销售是中间件行业普遍采用的销售手段之一，公司与系统集成商签订的合同均明确对应最终用户的信息项目，并实现产品的最终销售。

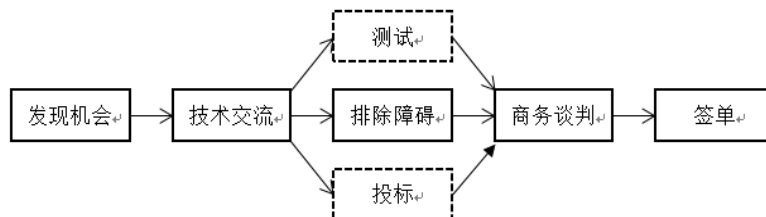
（2）网络信息安全产品销售

网络信息安全产品的客户主要分为两类：一是中国移动、中国电信、中国联通等三大电信运营商，二是广电企业、政府部门等行业客户。公司对电信运营商及行业客户的销售主要通过招投标的方式实现，并以直接销售方式为主。

三大电信运营商总公司及其省、市级分（子）公司是公司的主要客户。以中国移动为例，中国移动集团公司通常会向多家信息安全产品供应商或者技术服务商发送招标书；收到招标书后，公司经过内部研究，完成项目方案及标书，由销售部报价，将标书送至客户；客户根据标书进行综合评审确定中标名单，并分配中标额度。中标后，公司与客户直接签订销售合同。由于网络信息安全产品及服务属于运营商各级分支机构日常运营的必备产品，电信运营商各省市子公司或分公司对相关系统和服务的采购均拥有一定的独立采购决策权。

广电企业、政府部门等行业客户也是公司的重要客户，根据其各自的不同需要，行业客户通常采用招投标方式采购其所需的产品和服务。

公司的销售代表和售前服务人员通过与潜在客户的沟通、交流，经过投标、测试、试用等环节，使用户认可产品，最终形成销售。整个销售过程如下：



(3) 智慧应急产品销售：

智慧应急产品销售主要分为集成商销售和直接销售两种模式。应急安全产品主要客户包括各省、市、县地方政府客户、应急管理部门、各省通信管理局，以及大型企业。应急安全项目在政务数字化转型、城市综合治理、应急行业信息化、企业数字化转型项目中都会涉及。公司与国内大型集成商建立战略合作，形成解决方案共同面向客户，同时在国内各地发展了众多合作伙伴，共同合作拓展新兴的应急安全行业市场，实现横向覆盖和纵向深耕。对于需求明确的应急通信、应急指挥等产品更多采取直接销售模式。

应急产品销售的产品形态包括：标准产品销售，若客户有需求清晰和目前主要产品功能匹配，会按照产品授权码+维保服务周期的方式签订合作合同。待项目交付，服务期满后，为用户提供售后服务；解决方案销售，若客户需求存在大量定制开发或者个性化需求，会按照产品标准能力+扩展需求的方式签订软件开发定制服务合同。

4、服务模式

公司所提供的服务分为两类，一类是产品售后服务，一类是软件开发定制服务。

产品售后服务是指产品销售给客户后，公司提供的技术支持服务。根据公司与客户签订的销售合同，公司销售的产品一般会提供一定的服务期限，服务费用已包含于产品销售价格中。上述服务期限届满后，客户如还需公司的技术支持，需另行支付服务费用。

软件开发定制服务是指公司在产品销售过程中，如果用户对公司所提供的产品提出特定的功能需求或模块，公司可能会为满足其上述需求而进行定制化开发。

公司提供的标准服务内容主要包括：（1）电话支持服务：是指购货方（最终用户）通过电话、传真、Web或电子邮件等方式向公司咨询关于产品维护和使用等问题的服务，公司安排专门技术人员给予答复；

（2）产品安装指导服务，是指公司技术人员提供及时受理和响应客户关于产品安装及使用相关的技术支持服务，协助解决系统安装和调试过程中出现的问题；（3）故障诊断服务，是指为用户提供及时受理和响应与故障分析、诊断及解决相关的支持服务；（4）季度电话回访服务，是指每季度通过电话、电子邮件等方式对客户进行定期回访，以了解项目进展、问题处理情况、收集产品及服务建议等信息，旨在跟客户保持充分沟通，更好的服务客户；（5）产品补丁升级服务，是指为用户提供升级产品的服务。

（六）行业竞争格局和行业内主要企业

1、中间件行业竞争格局

国际中间件市场经历了长期的市场化竞争和发展，以IBM和Oracle为代表的软件行业巨头企业通过自身在软件行业的技术优势，并通过收购兼并进行产业布局，逐渐占据了国际中间件市场份额的前两位。

国内中间件行业发展初期，国外厂商IBM、Oracle等占据竞争的绝对主导地位，国产品牌处于相对弱势。随着国内中间件厂商技术水平的不断提升，以东方通为代表的国产厂商在金融、政府、电信、军工等行业客户中逐渐打破IBM和Oracle的垄断，与国外厂商之间的技术差距逐渐缩小。

从国家信息安全需求和发展信息技术应用创新产业考虑，中间件一直是国家主管部门重点发展的软件领域，在此背景下，金融、政府、电信等行业领域的国产化进程有望继续加快，虽然单一国内品牌的市场份额依然无法超过国外厂商，但是国内厂商的总体份额逐年增长。

2、网络信息安全软件行业竞争格局

网络信息安全涉及信息系统的各个层面，并且演进节奏较快，产品功能愈加专业化，行业内不断涌现出功能各异的新产品和服务，因此细分领域众多，形成了目前国内外厂商共同竞争、行业高度分散的格局。根据中国网络安全产业联盟发布的《2021年中国网络安全产业分析报告》，2020年中国网络安全市场9家主要企业的市场占有率合计为40.5%。此外，相比于其他IT细分领域，网络信息安全软件行业具有以下特点：

①国内厂商市场份额较高

由于受到政策限制、安全审查等因素制约，国外厂商无法涉足需求广阔的政府、军工等安全敏感领域，相比于IT基础设施，国外厂商在网络信息安全行业的市场份额并不具备绝对优势，甚至在部分领域落后于国内厂商。尽管在技术水平方面国内安全厂商并未完全超过国际领先安全厂商，但技术竞争力相较其他多数IT细分领域更为接近。此外，随着国家对信息安全的重视程度不断提高，国内厂商在金融、能源、电信等关系国计民生的领域将具备明显优势，有望进一步提高市场份额。

②市场集中度低，缺乏行业龙头企业

网络信息安全软件行业格局在国内外均较为分散，造成行业格局分散的重要原因是信息安全贯穿整个信息流链条，涉及几乎所有的信息设备与软件，单一信息安全企业难以掌握全部的信息安全技术，只能根据自身技术优势和渠道特点进行差异化定位，选择部分细分领域参与竞争。因此，从结果上来看，行业内难以形成绝对的龙头企业。

目前，网络信息安全行业发展越来越重视整体解决方案提供能力，显著提高了行业竞争门槛。随着我国信息安全行业的快速发展，行业内领先企业的技术创新能力、产品研发能力不断提升，以及《信息安全技术网络安全等级保护要求》等相关政策落地，市场集中度将会逐步提高。此外，云安全、工业互联网安全等新兴安全领域是未来行业发展的重点，将有利于积极布局新兴领域的头部厂商。

③网络安全产品多元化

随着网络安全威胁的日益加剧，网络安全热度不断升温，世界各国对网络安全的投入不断增加，网络安全市场需求不断被开启。网络安全投入将成为拉动网络安全产业发展的重要力量。传统的安全企业持续深耕、发展势头不减，互联网及IT企业陆续向安全领域发力，初创型企业不断在细分领域寻找突破点，网络安全产品更具创新性并且更加多元化，可以预见，未来几年我国网络安全市场规模将保持快速增长势头，网络安全市场竞争也将更加激烈。

④ 整网体系化安全成为行业发展的重要方向

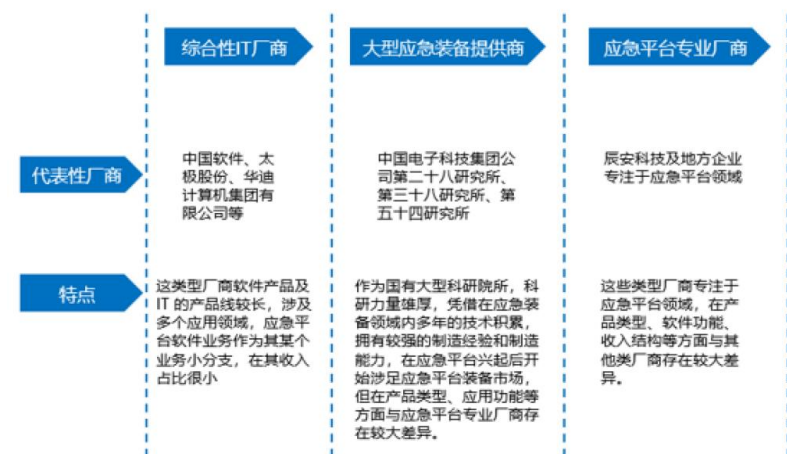
随着信息技术及其应用范围的不断发展，信息安全问题也越来越复杂，对信息安全威胁的检测和防护已很难由单个安全设备来完成。因此，由单个安全设备独立进行防护、安全设备独立于网络之外单独建设等传统模式已无法满足新的安全防护需求，将交换机、无线产品等网络设备与安全设备整合协同进行安全防护的整网体系化安全成为网络安全发展的必然趋势。

⑤ 网络安全品牌集中化趋势明显

目前，国内网络安全市场较为分散，不同细分市场领域均有其相应的优势专业厂商，却没有一个企业能掌握网络安全领域的所有技术，市场总体的品牌集中度有待提高。未来，随着市场竞争进一步加剧，具有技术、品牌、人才和资金优势的厂商将成为潜在的行业整合者，行业内的兼并收购将不可避免。缺乏技术创新、服务能力和独特商业应用模式的企业将逐步被淘汰，竞争实力较弱的中小厂商数量将大幅减少，产业趋于进一步集中。

3、智慧应急行业竞争格局

应急平台的主要构成包含应急平台软件、基础支撑系统和应急平台装备三大部分，各厂商的产品结构、收入构成、竞争优势等也各有侧重，归纳起来，主要竞争对手情况如下：



• 运营商：中国电信目前在全国应急行业基础云网市场约占据 50% 的市场份额；中国联通凭借资源优势在北方十省占据 50% 以上的市场，全国份额约 30% 左右；中国移动凭借低价优势在四川、江苏、海南等省占据了一定市场，整体份额大概 20% 左右。

• 中电科体系：中电科十五所、二十八所、五十四所等，拥有系统软件、安全软件、平台软件、各类应用软件等众多软件产品，提供从软件开发、系统集成、运营运维等全方位解决方案和服务；同时提供大型的应急救援装备如应急指挥车、方舱、移动应急平台、小型移动应急平台、各种救援装置等。

• 航天系：航天科工体系下的华迪计算机、航天科技体系下的航天四创，软件产品及 IT 的产品线较广，涉及信息安全、安监、专利、应急、电力、金融、国防、外交、工业等多个应用领域，其营业收入规模较大，拥有品牌知名度。

• 辰安科技：公共安全行业龙头企业，提供全系列的应急软件产品能力，业务已覆盖国务院、10 多个国家部委、26 个省、200 多个地市及区县，参与全国 26 个省级应急管理信息化规划设计工作。

4、政企数字化转型行业竞争格局：

数据驱动政企运营模式发生变革已经成为必然的趋势，政企数字化转型领域涉及多个行业，市场格局初显，角逐日趋白热化，新技术、新商业模式和新参赛选手不断涌现，整个行业具备以下特点：

(1) 以国内厂商为主，信息技术应用创新产业创新能力进一步提升

由于受到政策限制、安全审查、国家信创等因素制约，国外厂商无法涉足需求广阔的政府、公共安全、军工等安全敏感领域，同时我国正在加快推进自主可控、安全高效的新一代信息技术产业。据了解，随着我国信创产业的创新能力进一步提升，到2030年有望释放万亿级市场规模。国内厂商在政务、公共安全、司法、教育等关系国计民生的领域将具备明显优势，有望进一步提高市场份额。

(2) 新技术落地度不高，缺乏行业龙头企业

政企数字化转型领域市场格局在国内较为分散，其涉及信息化领域多、行业多、厂家多，单一行业缺

乏龙头企业，同时，数字孪生、人工智能、元宇宙等新技术在政企相关行业落地较少。随着我国数字化转型的快速发展，行业内领先企业的技术创新能力、产品研发能力不断提升，竞争格局的白热化，市场集中度将会逐步提高。

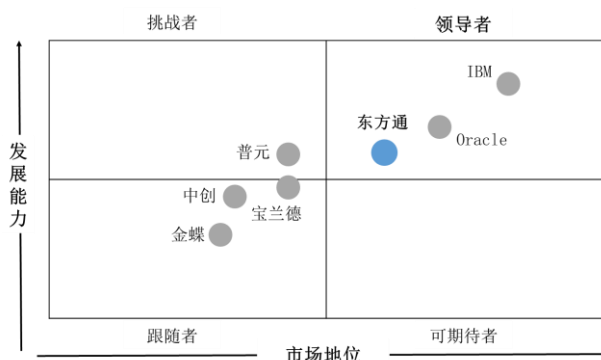
（七）公司在行业中的竞争地位

东方通是国内领先的中间件和大安全领域解决方案提供商，以“自主创新，安全创新”为核心理念，打造“数据+”和“安全+”两大产品体系，在此基础上，提出“智慧+”战略，开始在政企数字化转型领域进行全新布局，致力成为一流的智能安全行业领军企业。公司的产品及解决方案广泛服务于国内数千个行业及相关业务领域，拥有电信、金融、政府、能源、交通等行业领域5,000多家企业级用户和2,000多家合作伙伴。公司连续十余年被认定为“国家规划布局内重点软件企业”，是“中国软件行业最具影响力企业”、“北京软件和信息服务业综合实力百强企业”，是商务部、国资委认证的“企业信用评价AAA级信用企业”，曾荣获“国家科技进步二等奖”、“北京市科学技术进步奖二等奖”等多项荣誉。

1、中间件领域

东方通作为国产中间件的开拓者和领导者，不断引领中国中间件的发展与创新，承担了多项国家重大科技专项的研制任务。公司中间件产品在政府、金融、电信、交通、军工等行业树立了众多典型应用案例，始终保持在国内中间件市场的领先地位。

根据第三方机构的综合评估，从市场地位和发展能力两个维度分析，公司是唯一一家处于领导者象限的国产中间件厂商。2020年中国中间件市场厂商竞争力象限分析图如下：



数据来源：塞迪顾问

2、网络信息安全领域

全资子公司东方通网信是国内进入信息安全领域时间最早、产品线覆盖最广的厂商之一，专注于网络安全、信息安全和通信业务安全领域的研究和应用，同时在数据安全、工业互联网等新兴领域内进行拓展。东方通网信充分发挥自身技术特长，以业内领先的网络数据采集分析能力为基础，结合网络安全新技术，深入研究网络空间中各种安全事件的特征、演变及传播形态，遵循国家有关法律法规要求，在安全事件研判、分析、预警、处置等方面积累了丰富的技术手段，形成了多样化、多场景的解决方案，产品广泛应用于电信运营商及政府机关等领域。

根据《2021年嘶吼网络安全产业链图谱》发布内容，公司在数据安全与身份安全多个领域处于行业领先地位。根据中商产业研究院发布的《2021年中国网络安全行业市场回顾及2022年发展趋势预测分析》发布内容，东方通在网络安全领域是新晋的强有力的竞争者。

另外根据数世咨询及ISC相继公布《2021年度中国数字安全能力图谱（完全版）》（以下简称安全能力图谱）及2021年《网络安全行业创新技术全景图谱》（以下简称安全创新全景图谱）。东方通凭借优秀的市场表现和技术实力，入选能力图谱的内容安全领域能力者、基础设施DNS防护领域能力者；入选全景图谱的数据安全、物联网安全及零信任领域。

东方通近年来紧跟国家政策，在网络安全板块、信息安全板块积极布局，以自主研发技术为核心，专注于大数据、数据交换、数据治理、数据分析、数据服务、数据应用、数据安全、网络及信息安全、AI人

工智能等领域，沉淀下“数据+、安全+”两大产品体系，累计获得500多项软件著作权和多项专利。

在数据安全、工业互联网、物联网、车联网、移动互联网、区块链、5G等新兴领域内进行外延拓展，在新技术方面不断打造、开发新的产品，如零信任、NTA、UEBA、SOAR安全自动编排、安全中台等新产品，产品技术广泛应用于运营商、政府、公安、高校、金融、交通、能源、医疗等领域，随着产品技术的不断提升、市场占有率的不断提高，网络安全板块、信息安全板块的布局将会给公司带来新的业绩增长。

3、智慧应急领域

全资子公司泰策科技全方面推进相关的应急业务规划、产品设计、技术研发等相关工作。2021年，在多个产品线和重点领域取得突破和快速提升，业务架构和产品规划进一步明晰，相关的技术能力快速建立，多个领域具有战略意义的项目破冰落地，以“项目+产品”双轮驱动的设计思路指引各个平台的建设和完善。发挥优势，整合已有建设成果形成产品基线；把握商机，在重点领域抢占市场份额；大胆创新，引领产业改革升级趋势。

- 在自然灾害综合监测预警领域，集成自身与合作伙伴产品，形成专业性、有效性、综合性的自然灾害综合监测预警产品集，产品集各个灾种有机关联，可任意组合、拆分。

- 在城市安全综合监测预警领域，以重大项目为突破口，树立标杆。重点研发城市生命线（尤其是燃气）的监测预警产品，同时，集成已有自然灾害、安全生产相关产品，紧密跟进平台建设各个阶段，持续发掘商机。

- 在安全生产综合监测预警领域，进一步推进公司工业互联网领域能力优势，大力拓展政府侧和企业侧客户。

- 在应急通信指挥领域，整合运营商通信网络管理能力，建设“数据集中、综合监测、统一指挥、全面保障”的信息化管理平台，实现网络状态的实时监测、应急指挥、通信保障、预警预案、智能分析和扁平化管理的信息辅助平台，提升网络实时监测保障和应急通信响应支撑能力。

随着应急管理行业的高速发展以及公司对应急产业整体业务的深入研究，团队、产品、技能不断聚焦，未来将会迎来更好更快速的发展机遇。

4、数字化转型领域

公司携多年积累的大数据、人工智能、数据中台等综合技术能力，通过与各大科研院所、高校深入广泛合作发展，已初步具备领先于业界的政务、企业、国防军工数字化转型前沿技术支持与应用能力。在报告期内，公司助力2022年冬奥会和残奥会实现智慧重保，将公司大数据中台战略和“数据+”、“智慧+”实现了落地，成功的将政企数字化转型的能力应用于行业信息化项目中，同时在司法、教育、数字政务等行业具备较深的项目沉淀，并积累了丰富的数字化转型实践经验，帮助客户在转型中看懂行业未来。希望在数字化转型这样一个新兴市场取得优势竞争地位，为公司培育新的利润增长点。

3、主要会计数据和财务指标

(1) 近三年主要会计数据和财务指标

公司是否需追溯调整或重述以前年度会计数据

是 否

单位：元

	2021 年末	2020 年末	本年末比上年末增减	2019 年末
总资产	2,680,676,434.99	2,432,906,395.28	10.18%	2,156,223,097.44
归属于上市公司股东的净资产	2,265,446,014.70	2,042,155,950.08	10.93%	1,655,302,099.49
	2021 年	2020 年	本年比上年增减	2019 年
营业收入	863,160,674.61	640,337,778.89	34.80%	499,969,903.75
归属于上市公司股东的净利润	248,103,259.43	244,364,630.30	1.53%	141,291,862.35
归属于上市公司股东的扣除非经	221,229,665.56	167,738,991.63	31.89%	119,274,546.89

常性损益的净利润				
经营活动产生的现金流量净额	255,402,238.65	123,413,134.54	106.95%	87,587,633.51
基本每股收益（元/股）	0.55	0.55	0.00%	0.33
稀释每股收益（元/股）	0.54	0.54	0.00%	0.33
加权平均净资产收益率	11.45%	13.01%	-1.56%	9.37%

（2）分季度主要会计数据

单位：元

	第一季度	第二季度	第三季度	第四季度
营业收入	149,492,309.71	58,825,627.58	184,165,258.39	470,677,478.93
归属于上市公司股东的净利润	24,774,032.60	-38,855,808.89	52,282,614.50	209,902,421.22
归属于上市公司股东的扣除非经常性损益的净利润	8,561,008.62	-39,004,606.63	52,217,631.54	199,455,632.03
经营活动产生的现金流量净额	-18,141,195.10	17,790,878.14	38,611,238.84	217,141,316.77

上述财务指标或其加总数是否与公司已披露季度报告、半年度报告相关财务指标存在重大差异

□ 是 √ 否

4、股本及股东情况

（1）普通股股东和表决权恢复的优先股股东数量及前 10 名股东持股情况表

单位：股

报告期末普通股股东总数	42,665	年度报告披露日前一个月末普通股股东总数	41,142	报告期末表决权恢复的优先股股东总数	0	持有特别表决权股份的股东总数（如有）	0
前 10 名股东持股情况							
股东名称	股东性质	持股比例	持股数量	持有有限售条件的股份数量	质押、标记或冻结情况		
					股份状态	数量	
黄永军	境内自然人	7.93%	36,190,823	27,143,117			
北京东方通科技股份有限公司—第一期员工持股计划	其他	2.96%	13,533,906	0			
香港中央结算有限公司	境外法人	1.73%	7,893,998	0			
朱海东	境内自然人	1.29%	5,885,660	0			
吴志辉	境内自然人	1.26%	5,749,039	0			
李惠敏	境内自然人	1.03%	4,710,000	0			
宁波市星通投资管理有限公司	境内非国有法人	1.01%	4,600,000	0			
邓强	境内自然人	0.94%	4,270,000	0			
牛合庆	境内自然人	0.92%	4,191,988	0			
全国社保基金一一八组合	其他	0.88%	4,000,026	0			
上述股东关联关系或一致行动的说明		无					

公司是否具有表决权差异安排

□ 适用 √ 不适用

(2) 公司优先股股东总数及前 10 名优先股股东持股情况表

□ 适用 √ 不适用

公司报告期无优先股股东持股情况。

(3) 以方框图形式披露公司与实际控制人之间的产权及控制关系**5、在年度报告批准报出日存续的债券情况**

□ 适用 √ 不适用

三、重要事项

公司分别于2020年7月8日、2020年8月18日召开了第四届董事会第六次会议及2020年第一次临时股东大会，审议通过了公司2020年向特定对象发行A股股票方案的相关议案。因发行方案调整，公司分别于2021年1月27日、2021年2月25日召开第四届董事会第十三次会议及2021年第一次临时股东大会，审议通过了修订后的向特定对象发行A股股票方案的相关议案。深圳证券交易所于2021年6月22日出具《关于北京东方通科技股份有限公司申请向特定对象发行股票的审核问询函》（审核函〔2021〕020156号），公司及发行中介于2021年11月提交审核问询函回复。

2022年3月1日召开第四届董事会第二十三次会议和第四届监事会第二十次会议，审议通过了《关于终止前次向特定对象发行股票事项及撤回申请文件并重新申报的议案》，由于资本市场环境变化并综合考虑公司自身实际情况、发展规划等因素，经与相关各方充分的沟通及审慎论证，拟先向深圳证券交易所申请终止前次向特定对象发行股票事项、撤回申请文件，并将在修改和调整方案后尽快向深交所重新递交向特定对象发行的申请材料。同日，公司披露了《关于2022年向特定对象发行股票并在创业板上市预案》。

2022年3月2日，公司和保荐人第一创业证券承销保荐有限责任公司向深交所提交了《北京东方通科技股份有限公司关于撤回向特定对象发行股票的申请》和《第一创业证券承销保荐有限责任公司关于撤回北京东方通科技股份有限公司向特定对象发行股票的申请》，申请撤回申请文件。

2022年3月7日，公司收到深交所出具的《关于终止对北京东方通科技股份有限公司申请向特定对象发行股票审核的决定》（深证上审〔2022〕51号）。