证券代码:300659　　证券简称:中孚信息　　公告编号:2026-011

中孚信息股份有限公司 2025 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。

所有董事均已出席了审议本报告的董事会会议。

容诚会计师事务所(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。

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利润分配预案或公积金转增股本预案

□适用 √不适用

公司计划不派发现金红利,不送红股,不以公积金转增股本。

截至报告期末,母公司存在未弥补亏损

经容诚会计师事务所(特殊普通合伙)审计,截至 2025 年 12 月 31 日,公司母公司报表未分配利润为 -15,494,829.75 元,存在未弥补亏损。鉴于公司 2025 年度母公司未分配利润为负,在充分考虑公司正常经营和持续发展的需要后,公司 2025 年度拟不派发现金红利,不送红股,不进行公积金转增股本。敬请广大投资者注意相关投资风险。

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	中孚信息	股票代码	300659
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	张丽	刘宁	
办公地址	济南市高新区舜华路 879 号山东省大数据产业基地 A 栋 42 层	济南市高新区舜华路 879 号山东省大数据产业基地 A 栋 42 层	
传真	0531-66590077	0531-66590077	
电话	0531-66590077	0531-66590077	
电子信箱	ir@zhongfu.net	ir@zhongfu.net	

2、报告期主要业务或产品简介

(一)主要业务发展情况

报告期内,公司专注于战略和资源聚焦,深挖市场潜力,主要自主产品核心竞争力进一步加强,业务质量和盈利水平得到提升,同时持续推进降本增效工作,归属于上市公司股东的净利润亏损幅度进一步收窄。报告期内,公司实现主营业务收入 720,610,318.76 元,同比下降 8.12%;归属上市公司股东的净利润 -104,329,252.98 元,同比减亏 16.64%。

1、主营业务收入列示

单位:元

一级分类	二级分类	2025年		2024年		同比变动	
		收入	毛利率	收入	毛利率	收入变动	毛利率变动
网络安全产品	主机与网络安全产品	272,057,148.36	79.87%	211,730,357.45	77.61%	28.49%	2.26%
	数据安全产品	6,284,905.64	89.84%	11,647,118.01	79.58%	-46.04%	10.26%
	安全监管平台	63,415,378.52	72.85%	61,464,921.26	77.05%	3.17%	-4.20%
	检查检测产品	116,819,967.74	98.20%	125,132,709.80	97.83%	-6.64%	0.37%
	小 计	458,577,380.26	83.70%	409,975,106.52	83.76%	11.85%	-0.06%
密码应用产品	密码应用产品	3,535,254.35	72.64%	4,315,608.27	59.17%	-18.08%	13.47%
信息安全服务	信息安全服务	161,489,504.62	34.99%	254,889,601.29	40.77%	-36.64%	-5.78%
其他产品和服务	其他产品和服务	97,008,169.53	58.03%	115,083,311.63	55.01%	-15.71%	3.02%
合 计		720,610,318.76	69.28%	784,263,627.71	65.43%	-8.12%	3.85%

注:信息安全服务通过集成项目形式向客户交付完整解决方案,主要包含安全监管、安全服务、安全教育等解决方案的业务收入。

报告期内,由于整体网络安全市场的需求复苏不及预期,在下游客户普遍紧缩预算支出、延缓采购节奏的不利局面下,公司主营业务在阶段性市场调整中承压,收入同比出现小幅波动,公司持续深耕优势领域,积极优化业务结构,经营态势保持稳健。面对严峻的市场环境,公司聚焦重点行业,积极推动市场拓展工作,核心网络安全产品收入实现增长,持续发挥业绩引擎和支撑的作用。其中,主机与网络安全产品贡献了稳定增量,信创防护主线业务持续深化;安全监管平台与检查检测产品收入基本持平;数据安全业务通过标杆项目实现,加速打造体系化的解决方案。报告期内,公司产品业务表现突出,经营质量得到有效提升,毛利率水平显著增长,收入结构呈现积极优化趋势。

2、市场拓展情况

单位:元

客户所在行业分类	2025年		2024年		同比变动情况	
	收入	收入占比	收入	收入占比	收入变动	收入占比变动
政府及事业单位	388,732,679.64	53.94%	475,770,634.58	60.66%	-18.29%	-6.72%
特殊行业	152,177,142.45	21.12%	139,654,358.25	17.81%	8.97%	3.31%
央企集团	142,332,723.12	19.75%	113,887,004.59	14.52%	24.98%	5.23%
信息技术行业	9,155,236.39	1.27%	27,268,837.65	3.48%	-66.43%	-2.21%
其他	28,212,538.16	3.92%	27,682,792.64	3.53%	1.91%	0.39%
主营业务合计	720,610,318.76	100.00%	784,263,627.71	100.00%	-8.12%	0.00%

注:信息技术行业客户主要为整机厂商。特殊行业客户主要为国防等行业客户。

公司持续深耕党政、特殊行业、央国企三个市场领域,以公司内容感知、行为管控、风险建模的三大核心技术能力为抓手,深入业务领域打造产品矩阵,并以形成的标准化产品矩阵依托相关领域的政策和重点工程,开展体系化推广作局。从技术、产品、市场多维度全面巩固优势地位,进一步优化客户领域收入结构。报告期内,公司深化防务领域和以军工、金融为代表的央国企领域的业务拓展,实现稳健增长,收入结构进一步优化,未来将有效支撑公司总体业务收入的持续增长。

3、重要财务指标分析

报告期内,归属上市公司股东的净利润 -104,329,252.98 元,同比减亏 16.64%。公司在保障技术、产品研发紧跟行业发展趋势和客户需求的基础上,持续贯彻提质增效与精细化运营理念,全面强化管理提升工作,深入推进降本增效举措。在此带动下,期间费用得到进一步优化,盈利结构稳步改善,归属于上市公司股东的净利润亏损进一步收窄。

(二)公司主要产品及解决方案

公司以保障国家网络安全为目标,按照等级保护、分级保护、数据安全、密码安全、工作秘密、商业秘密等相关法律法规和标准要求,以合规防护为基础,实战对抗为导向,积极做深、谨慎做宽,围绕保密安全、数据安全两大业务领域,着力构建保密安全业务根基稳固、数据安全方向有效突破的新局面。

公司核心技术能力

为实现公司安全理念,通过多年技术积累,基于数据存在物理空间、数字空间、社会空间和电磁空间中的现实风险,通过抓住数据安全全生命周期的关键环节,逐步构建起“数据分析识别、数据防扩管控、数据流动检测、数据溯源、共享交换、电磁监测、密码芯片、安全教育、安全服务”等九大核心能力。全面引入 AI 技术为各类能力赋能,搭建起“人防、物防、技防”全面融合的技术能力体系,为网络安全对抗页起不强力量。

AI 应用赋能

报告期内,公司以“全面拥抱 AI”为指导思想,全力推进人工智能技术在保密安全领域落地。

通过 AI 平台化建设,为全系产品赋能。公司研制并发布天机 2.0 数据分析平台、AI 应用与服务平台,通过深度整合国产大模型与国产硬件设备、AI 应用框架、AI 基础应用和服务技术,形成为公司终端安全、网络安全、云安全等全系列产品的 AI 数据分析和 AI 应用的基础平台,为中孚全系产品注入智能基因。

模型安全与业务应用紧密结合,实现 AI 应用落地。公司推出了第三代互联网数据安全预警平台,全面引入 DeepSeek、Qwen、GLM 等国产大模型,通过融合推理模型架构、安全专用语料库构建、模型微调等技术,在内容识别、异常行为分析、攻击威胁分析、风险识别等方面能力显著提升。同时,大模型防护围栏与模型天然集成,实现模型安全与业务共生。

构建 AI 安全分析智能体,逐步扩展 AI 分析应用范围。在电磁空间安全监测领域,公司基于 DeepSeek 大模型的信号调制智能识别技术以国产大模型为基座,突破传统识别方法在复杂电磁环境中的性能天花板,创新性探索“预训练 + 轻量化微调”新范式,实现少样本、强泛化的智能识别,首次将大模型能力注入电磁安全领域,为构建“认知型”电磁防御系统提供技术雏形,实现对复杂信号调制的智能识别。

未来,公司将通过深度整合大模型技术,持续打造保密领域的智能体,为公司全系列产品注入强劲动力,推动保密与数据安全产品和技术向主动防御、智能协同的方向加速演进,在复杂多变的网络安全环境中筑牢坚实保密防线。

公司主要产品及解决方案

报告期内,公司主营业务未发生重大变化,主要产品线及服务包括:主机与网络安全、数据安全、安全监管平台、检查检测、密码应用五条产品线及信息安全服务。同时,公司基于用户典型应用场景,围绕信创安全防护、安全监测预警、零信任数据安全三大业务主线,打造面向党政、央国企、特殊行业用户的场景化解决方案,推动公司业务由产品销售向平台化、体系化解决方案营销模式演进,持续提升公司市场挖掘能力、业务布局能力,构建以产品及解决方案驱动公司业务发展和客户价值提升的良好局面。

1、主要产品体系

(1)主机与网络安全产品

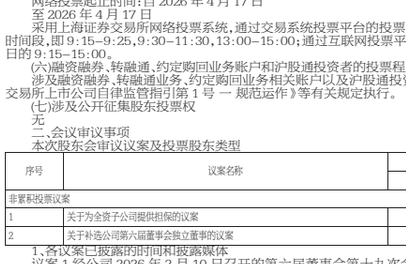
公司主机与网络安全产品线选配主流国产 CPU、操作系统、数据库及中间件,围绕主机审计、终端安全登录、打印刻录审计、网络控制与传输等方面打造了完整的产品体系。

公司主机与网络安全主要产品简介:

主机与网络安全产品	
主要产品名称	产品简介
安全保密套件管理系统	系统通过整合终端安全技术和模块,对终端提供有效的、持续的安全防护。
计算机及移动存储介质保密管理系统(三合一)	具有图断内网计算机违规外联、防止移动存储介质交叉使用、外部信息单向导入内网计算机三方面的功能,能够切实解决和防范内网计算机违规连接互联网和移动存储介质在内网计算机与外网计算机之间交叉使用引起的安全问题。
主机监控与审计系统	能够实时监控多种计算机操作行为,发现异常违规行为并产生报警,全面知悉和有效控制单位内部用户对主机资源和网络资源的使用,防止内部违规行为的发生。
终端安全登录系统	采用登录密钥(KEY)和口令(PIN 码)双因子结合的身份认证技术,实现对登录用户身份授权与鉴别管理,从而有效防止用户非授权登录,保证终端系统及数据安全。
打印刻录安全监控与审计系统	实现用户与实体打印、刻录设备的隔离,并通过入员权限管理、设备授权管理对用户行为进行实时监控,进而完成文档输出全过程的监控和管理,并且形成了完备的审计日志,方便对文件输出情况进行统计和追溯,有效解决了文件输出过程中的审核和监管难题。
网络安全隔离与信息单向导入系统	设备关键硬件采用国产自主可控的芯片,系统利用光的单向传输特性和建了一套安全、单向的传输通道,实现了外网到内网的数据传输,保证敏感数据不泄露。
网络安全隔离与信息交换系统	采用自主研发的双通道隔离交换模块,实现在网络之间双向“摆渡”数据,解决了用户在不同网络之间双向数据交换的需求,同时具有病毒检查、内容安全检查、标签检查等策略保证数据在不同网络之间安全受控传输,使不同网络之间的业务可以高速、可靠、安全的进行数据交换。
数据安全交换平台	配合网络安全隔离与信息单向导入系统或者网闸设备,实现跨边界的安全数据交换。该产品可极大拓展跨网数据交换能力,实现文件交换、数据库交换、按口服务交换、应用协议代理、音视频交换五大核心交换功能。解决多类型业务数据及海量数据共享交换难的问题,满足各领域客户对安全性、合规性、可靠性、高性能、兼容性和强审计的要求。
网络接入控制系统	以终端计算机和网络设备作为管理对象,对目标网络内终端进行合规审查、安全检查等,对不合规用户或者特定部门进行安全隔离控制。可保证合规用户的网络畅通,同时杜绝非法用户接入可能带来的安全隐患。
网络安全审计系统	通过分析网络中的通信流量,审计网络安全事件,生成安全统计报表,对重要安全事件或行为进行风险分析、追查取证,并为网络安全大数据分析系统提供有效的数据支撑。
入侵检测系统	系统能够实时高效发现网络中的异常流量,精准识别网络流量中的攻击行为,具备强大的攻击特征库,集成了海量的威胁情报库,实现对网络的实时监控,保护用户网络安全。
零信任 TNA 安全网关	不依赖 CPU、操作系统和第三方代码库的轻硬件高保障安全网关(Guarantee Advanced Trusted Network Access,TNA),基于零信任理念,以身份为基石,采用最小授权、持续信任评估、动态访问控制等机制,保障企业在互联网上的安全接入和业务访问安全。
特殊行业保密综合管理系统	依托国产化计算机软硬平台,实现对计算机设备、进程等进行精准管控审计,对电子文件的全生命周期管理,对电子文件集中存储加密,同时使用多种外设控制技术,对文件打印、复印、刻录等行为进行全方位管控审计的综合性防护系统。

(2)数据安全产品

公司数据安全产品以重要数据和敏感数据的防泄漏、防窃取、可追溯为目标,采用数据加密、数据保护、数据管控等技术,结合业务应用场景,实现对数据资产的可知、可控、可管,并且广泛适配主流国产 CPU、操作系统、数据库及中间件。



数据安全主要产品简介:

数据安全产品	
主要产品名称	产品简介
电子文件密级标志管理系统	支持办公、PDF、音频、视频等各类文件格式,满足多种工作场景需求。系统围绕电子文件的产生、存储、处理、交换、销毁等全生命周期过程,实现电子文件密级标志警示、强制访问控制和监管审计等安全目标。
电子文档安全管理系统	通过与密级标志技术结合及统一策略,对电子文档的操作行为进行安全管理、访问控制和安全审计,达到事前可定义、事中可控制、事后可审计的安全目标,从而实现对电子文档数据资产的细粒度、全方位的安全保护。
文档发文信息隐写溯源系统	采用先进图形几何变换技术,可在高式、版式文档中嵌入肉眼难以识别的信息,但通过识别软件可以恢复取证,从而定位文档的分发途径,以实现信息泄露后可追可溯的安全管理目标。
终端安全沙箱系统	采用密码技术在移动终端/PC 终端打造安全可信的隔离环境,实现个人生活区及工作区的隔离。提供周密的安全认证机制、访问控制机制,防止非法用户、未授权用户进入受保护的工作区,保证业务系统中重要数据处理安全。
API审计监测预警系统	以 API 资产为核心,通过对 API 资产的发现、检测、防护、响应,帮助组织梳理 API 资产,发现潜在的安全风险和异常行为,及时监测和应对 API 安全威胁,保护 API 资源的安全性,并提供实时预警和安全报告。
数据标识管理系统	系统提供文件的数据标识生成、脱标功能,通过基于面向切面的数据安全技术为应用系统提供透明的数据标识识别及流转管控能力,实现轻量化的数据安全访问控制和追踪溯源。
数据安全监测预警平台	针对敏感、重要数据全生命周期进行安全风险监测,可接入数据库审计、数据加密、数据脱敏、数据防泄露等防护组件,统一管理策略,掌握数据安全风险并快速响应处置,实现数据可见、可控、可管,构建体系化的数据安全防护能力,为业务的稳定、可靠运行提供保障。
数据安全态势感知系统	以数据安全全生命周期管理为核心,通过多维度量化指标,精准描述数据安全的实时风险及整体状况;利用海量数据分析引擎及模型实现对数据风险的主动发现,精准定位、智能研判、快速处置、严格审计,完成对数据安全保护工作的闭环处置流程。
大模型安全防护系统	以网关模式和 API 服务模式,提供针对 AI 推理服务、AI 应用服务、MCP 服务等大语言模型系统的安全防护服务,确保大模型输入和输出内容安全、可用和可信。产品嵌入 AI 大模型服务业务流程中,实时监控大模型的输入和输出内容,保护大模型业务不受 OWASPLLMTop10 攻击,提供包括漏洞攻击防护、提示词攻击防护、数据泄露防护、价值观过滤防护和敏感数据风险识别等防护功能。

安全监管平台主要产品简介:

安全监管平台	
主要产品名称	产品简介
互联网接入口监测平台	由互联网接入口检测器、互联网接入口监测平台等部分组成,用于检测、分析、处置网络攻击窃密及传输敏感信息行为。
政务应用安全监测系统	系统依托政务服务平台,汇聚多种政务应用数据,精准锁定及管控敏感信息在政务应用中的发布、存储、处理、传输等行为,实现政务应用数据可授入、可分析、可监测,消除政务平台敏感信息泄露的风险隐患。
互联网站内容监控系统	系统基于前沿搜索引擎、自然语言处理、智能分析等技术进行设计开发,帮助各级网络安全行政管理部门对辖区门户网站进行有效的安全检查与监控,及时发现泄密隐患,遏制敏感信息在互联网门户网站的传播。
威胁情报平台	系统专注于高精准威胁情报,为客户提供高性能、高可用、可扩展的威胁情报查询分析能力和威胁情报共享能力。
追影攻击分析系统	系统融合大数据、海量高质量威胁情报和专家知识库,有效检测并识别高级持续性威胁(APT)攻击、窃密木马等高危恶意攻击行为,做到“让安全可看见”。
互联网失泄密智能分析平台	系统运用大数据分析、人工智能和数据可视化等技术,有效整合各类监管系统的数据,实现对互联网安全态势的全面监管、融合展示、动态管理、资源共享、协同联动、快速响应,全面提升网络监管能力。
网络安全管理与运行监管平台	为用户提供资产在线动态监管、基于分级保护的动态持续合规监管、违规行为及未知风险发现三种核心能力,构建安全运行监管能力,违规行为发现能力、攻击行为发现能力和全网应急处置等核心能力,打造可视化的安全监管态势感知。
重要场所电磁环境长时监测系统	该系统能够解决重要场所中违规信号和异常无线发射信号的检测难题,通过实时采集场所内存在的无线信号,建立频谱电磁信号的实时告警,同时结合信号分析功能和后端信号特征库自动匹配功能,可实现对异常发射信号频点、带宽、调制方式及内容的识别和还原,为重要单位的电磁空间安全提供保障。
保密综合态势感知平台	系统运用深度融合监测和检查相关数据,打造数据壁垒,全面深化数据分析、提升智能辅助决策和协同作战能力。打造安全监测预警、应急响应和追踪溯源于一体的综合态势感知平台。

(4)检查检测产品

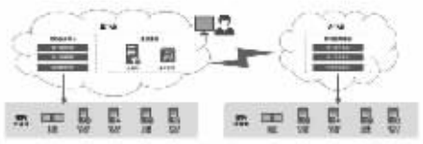
公司检查检测产品围绕主机安全、数据库安全、邮件安全、移动终端安全、云存储安全,通过构建网络化部署、自动化检查、实时化检测、便捷化整改、智能化分析于一体的检查检测系统,实现实时发现违规行为,有效提高安全能力。

检查检测主要产品简介:

检查检测产品	
主要产品名称	产品简介
密保卫士系统	实现对单位内部敏感数据存储、处理、传输过程的全生命周期管控,实现敏感数据从快速发现到安全处置的闭环管理,帮助执行管理部门及时发现处置敏感信息泄露隐患,防止敏感信息泄露事件发生,助力机关单位形成长期有效的安全管理工作机制,提高安全管理工作规范化水平。
计算机终端保密检查系统	包括单机版和网络版,通过主机检查、终端自查、违规判定等环节,及时发现违规行为、失泄密隐患和安全漏洞,做到有效防止失泄密事件发生,保障国家秘密的安全。
数据库内容保密检查系统	系统主要针对各类型数据库第口令、数据库安全策略配置、数据库敏感内容进行详细检查,及时发现违规存储行为和安全隐患,确保重要数据和敏感数据安全,支持对云存储、云数据库及主流国产数据库的检查。
电子邮件内容保密检查系统	系统实现对个人邮箱、个人邮件客户端及单位邮件服务器中存储的电子邮件的邮件头、正文、附件敏感性检查,及时发现违规传递行为和安全隐患,确保敏感信息数据安全。
移动终端保密检查系统	系统集成高效反病毒引擎及丰富病毒库,同时针对移动终端文件、图片、应用等进行检查,及时发现敏感信息、木马病毒应用,实现对移动终端的全面、高效检查。
云存储内容保密检查系统	系统通过适配各云存储官方 SDK,利用数据抽取、数据分析等技术,结合完整的数据与合规策略模型,实现对单位公有云及私有云存储中存储的文档、图片、压缩包等数据进行自动化敏感内容检查,及时发现违规存储行为和安全隐患,确保敏感信息数据安全。
网络测评管理系统	依据分级保护测评标准,面向全国测评机构,辅助进行网络保护测评、风险评估、应用系统评估,实现测评全流程信息化管理,并针对现场检测环节提供专用现场检测系统及测评工具集,有效提升测评工作效率与质量。

(5)密码应用产品

公司以国产密码算法和行业标准为基础,开发了从客户端、服务端到系统类一系列密码产品。



密码应用主要产品简介:

密码应用产品	
主要产品名称	产品简介
密码服务管理平台	密码服务管理平台是一套具备密码服务按需配置、密钥集中管理、统一提供标准化服务接口、统一设备管理能力以及密码安全态势感知能力的密码服务、管理、监控一体化平台。能够提供合规的一站式密码改造方案,兼容多种密码硬件,屏蔽底层复杂逻辑,降低应用系统改造难度,支撑密码测评改造快速落地,按需提供弹性可扩展的云密码资源池,提高设备利用率,满足未来动态扩展性需求。
服务器密码机	中孚 HSS 服务器密码机是自主研发的密码安全模块,适用于高速运算的密码安全应用场景,满足应用系统数据的签名、验证、加密、解密要求。保证传输信息的机密性、完整性、有效性,可作为数字证书管理、密钥管理、身份管理、接入认证、数据安全交换、数据存储加密、数字内容保护等系统的基础核心密码设备,支持 SM2/SM3/SM4 等国产密码算法和 RSA2048 等通用安全密码算法,可广泛应用于金融、政务、能源、工业控制、基础通信等行业。
密码卡	密码卡是包含支持 PCIe 接口和 SATA 接口的两款密码模块,具有高效密码运算能力和密钥安全管理能力,作为服务端密码应用系统核心组件,用于身份认证、通信加密、签名验证等各类应用场景。PCIe 接口密码模块的主机接口符合 PCIe2.0 工业标准,可以广泛适配各种类型的机架式服务器和桌面服务器,SATA 接口密码设备具备符合 SATARevision3.0 标准(SATA6Gbps)的 SATADevice 接口,可以广泛应用在具备 SATAHost 接口的主机或服务器中。
智能密码钥匙	基于自主知识产权的操作系统开发的多功能终端密码产品,可以支持数字证书的生成与安全存储、数字签名认证。
安全网关	一款保护网络边界、核心信息系统的软硬件结合的密码产品。它集防火墙、安全加密 VPN、用户身份核验、应用授权访问等核心能力于一体,为用户提供便捷、安全、可信的通信环境,为各类核心信息系统提供周密的安全认证和细粒度访问控制机制,可有效地防止非法用户、非法设备访问受保护的核心数据资产,保障业务数字化转型战略的顺利开展。

2、主要解决方案

围绕国家网络安全战略,公司聚焦数据安全,按照分级保护、等级保护、关基保护等法律法规,依据网信、公安、保密、密码等主管部门的相关要求,面向党政、央国企和特殊行业,构建了基于用户场景化的解决方案体系。

党政安全解决方案	
解决方案	方案简介
信创安全防护解决方案	中孚基于多年分级保护技术积累和测评经验,在统一基础平台上,打造了包含终端、网络、应用和数据防护为一体的安全解决方案,可实现信创平台与原有平台混合部署,实现统一管理、统一运维、统一审计,满足用户合规安全要求。
商用密码应用安全性解决方案	为帮助用户通过密码测评,依据商用密码应用安全性相关法律法规,为用户提供商用密码应用咨询、国密改造、系统集成和密码测评服务,确保用户系统满足商用密码测评合规性、有效性要求。
跨网数据安全交换解决方案	为解决在内网和外网、不同网域之间数据使捷、高效、稳定和安全交换的问题,基于网络安全隔离交换技术打造的跨网数据安全交换解决方案,能够提供单向、双向等多应用场景数据安全交换、敏感数据内容分析、木马检测、传输控制等能力。
安全检查整改一体化解决方案	基于智能化内容分析引擎开发的安全检查整改一体化解决方案,主要为解决机关单位安全自查手段缺乏、工作繁重、整改不彻底等问题,实现密害事件的事前预警、事中发现和事后溯源,满足机关单位日常安全自查和检查工作需求。
安全监测预警解决方案	围绕安全主管部门的管理需要,基于“统一防护、统一监管、统一运维、统一处置”理念设计的安全监管整体解决方案,能够实现对互联网、内网和电磁空间的全域全维检查监管,为用户提供便捷、易用的综合性智能分析处置平台,有效提升检查预警能力,实现“一屏观天下、一网控全局”的目标。
测评管理和风险评估解决方案	本方案可以实现测评工作规范化,减轻测评工作量,提升现场测评能力,能够为测评部门提供测评任务流程化管理、现场测评数据自动化采集、测评报告智能化生成,可有效提升测评工作效率。机关单位版可为机关单位提供预测评、风险自评估能力。

电磁空间检测解决方案	实现重要场所、公务车辆、临时会场等多业务场景下的电磁空间异常无线信号的发现识别,快速识别各类环境下的窃听、窃照、GPS 跟踪设备,并实现对异常信号的快速定位功能。
工作秘密信息防护解决方案	依据《工作秘密信息防护指南(试行)》要求,打造覆盖端、管、边、云、脑的工作秘密安全技术防护体系,强化终端信息防护、数据传输防护、应用系统防护、数据隔离交换、数据存储与备份及安全监测 6 项防护技术,确保机关、单位工作秘密处理活动的合规开展,逐步实现对工作秘密的细粒度管控。
央国企安全解决方案	
解决方案	方案简介
基于零信任的数据安全解决方案	针对全数据资产(结构化数据和非结构化数据)安全防护,融合沙箱技术与零信任理念,以密码为基石,关键业务安全为核心,全数据安全为目标,风险管理为导向,内容、行为分析为抓手,分析识别窃密、泄密、勒索三类主要安全风险,依托安全大脑,打造云、管、端、边全面防御架构,保障数据流转过程中处理、存储、传输、共享交换、服务运维等五类场景安全。
敏感信息泄漏风险预警解决方案	面向中央企业,基于多种敏感信息分析模型,通过一站式的检查方式,实现对计算机终端、数据库、云存储、移动端、电子邮件检查的全覆盖,实现检查工作态势分析,及时发现敏感数据,杜绝泄密隐患,为主管部门安全监督检查工作提供决策依据。
电网行业数据安全态势感知解决方案	数据安全防护和态势感知以数据资产动态管理、智能高效风险监控、数据安全事件响应与溯源、全生存周期策略管理为核心,以可视化为特色,以可靠服务为保障,逐步达到数据资产看得见、说得清、管的住、强审计、深溯源的目标。
中央企业商业秘密安全保护解决方案	面向中央企业,以商业秘密数据全生命周期管控为核心,全面支撑商业秘密管理、监督、检查、技术防护及培训教育等工作,提升中央企业商业秘密安全防护能力。
终端跨域安全办公解决方案	在互联网和工作网逻辑隔离要求前提下,解决办公终端安全访问互联网问题,提升工作人员上网办公与数据共享操作体验,防范工作秘密银感数据泄露
数据安全治理解决方案	通过对动静态数据资产存储、流转信息的采集分析、权益声明、分类分级,实现对数据资产底账的动态管理,识别重要资产、僵尸资产、幽灵资产,数据流向,数据热度等,为数据所有者提供数据资产权益保护支持。
特殊行业安全解决方案	
解决方案	方案简介
特殊行业综合安全防护解决方案	针对新时期特殊行业网络安全面临的新形势、新挑战,基于国产计算机软硬件平台,针对各级单位重要计算机、移动存储载体、重要文件等管理对象的新一代安全管理系统。
特殊行业网络安全监管解决方案	针对特殊行业互联网敏感信息的监测、预警、防护和应急处置的综合需求,打造全网重要信息抓取、数据高效解析、违规事件快速处置等能力,构建网络安全监测预警体系,实现“一屏观态势、一网控全局”。
安全服务解决方案	
针对当前行业发展趋势与客户安全需求的演变,构建“安全运营、安全咨询、应急响应、安全测试”梯次递进的安全服务体系,打造面向攻防实战、以对抗能力核心的服务体系,为重要客户、重要信息系统提供系列安全服务,并持续提升服务质量与价值,为客户网络提供全方位的安全保障。	
安全教育解决方案	
为客户提供线上安全可靠、内容详实的安全与保密宣教平台,提供多种形式的前台学习资源,包括手机 App、微信小程序、PC 网页等,后台管理提供资源管理、考试问卷、综合分析等。依据不同建设需求可以私有化部署和 SAAS 化服务。中孚提供平台及资源,内容的运营服务,配合线上线下活动的运推支撑。	

(三)公司经营模式

报告期内,公司继续围绕客户的安全需求,以技术为核心、市场为导向,专注于产品软硬件设计开发,通过提供高附加值的产品和服务获取利润。对部分低技术含量的生产过程公司采取外包的方式,通过营销服务网络为客户提供高质量服务。对关键核心技术和产品,公司坚持自主研发,以此内领先的具有核心技术的产品和服务满足客户安全需求,同时通过销售环节不断反馈市场的需求动态,指导公司产品研发部门进一步针对市场需求对技术进行改造和积累。

公司研发模式、采购模式、生产模式和销售模式如下:

1、研发模式

公司构建了高效、系统化的研发流程,紧抓技术研究、产品研发创新和产品开发项目管理,通过产品改进或创新,以满足市场需求或开拓新市场。此外,为有效推进产品创新,企业建立了跨部门协作机制,促进不同部门之间的沟通和合作,共同推进产品创新。同时,整合企业内部和外部资源,包括技术、人才、资金等,为产品的创新提供有力支持。

在技术研究方面,公司建立了技术研发流程,由技术立项、技术调研、方案设计、方案验证和技术移交五个阶段组成。每个阶段都有其特定的目标和任务;在产品研发创新方面,产品创新体系流程被细化为六个阶段,包括市场需求收集、制定产品路线图、产品立项、开发与验证、研发维护及管理产品生命周期;产品开发项目管理是确保产品成功开发的基础。项目管理流程包括制定项目计划、项目实施与监控、项目结项和项目变更管理四个模块。通过明确项目范围、制定项目计划、监控项目执行、及时评估和调整项目风险,确保项目按计划顺利进行。

公司建立质量持续改善机制,对质量改善方案进行流程化和标准化评审,形成案例普及推广,减少质量问题反复发生的可能性,确保输出符合市场预期、满足客户需求的产品,提高用户满意度。

2、采购模式

对于生产所需原材料,公司采取集中采购模式,由公司采购部门统一负责各类产品所需原材料的采购。公司采购的原材料主要为各类电子元器件、PCB 及 PCBA、结构及配件、整机、印刷包装材料等。公司所采购的原材料生产厂商众多,市场竞争充分。公司营销管理部门和供应链管理部门根据订单情况共同确定生产计划,根据生产计划和自主备货需求制定物料需求计划,由采购部门具体执行采购。通过市场寻源、技术认证、品质认证、商务认证、现场审核、综合评估等方式,公司将合适的原材料供应商引入合格供应商名录,对已在合格供应商名录中的企业会进行跟踪评价和例行审核,根据评价和审核结果对供应商进行相应的激励、处罚、辅导或淘汰。

3、生产模式

公司生产采取自主生产与外协加工相结合的运营模式。根据所处行业的特点,公司将主要精力集中于研发、销售、自主生产的自动化和信息化建设等高附加值环节,在加固体系化安全生产管理机制的前提下,将生产加工等低附加值环节进行外包。主要硬件产品生产以外协加工方式为主、为公司提供外协加工服务的厂商市场竞争充分,公司能够在有效控制成本、交付周期和质量的前提下满足日身对外协加工的需求。

4、销售模式

公司主要提供网络安全产品、信息安全服务及整体化解决方案。销售模式采用直销与经销相结合的方式。通过直销覆盖了关键领域、关键行业的主要客户,以更贴近市场的方式,更好地满足了其在方案、产品、技术、服务等方面的更高要求,建立良好难以复制的合作关系;通过经销进一步完善了市场及客户的覆盖,为更广泛的客户提供了产品支撑,并让公司更及时地获取了区域市场信息,为市场的深度挖掘提供了信息与服务支持。

(四)公司市场地位

公司成立于 2002 年,是国内领先的网络安全、数据安全产品研发及整体解决方案提供商,是国内最早从事保密安全业务的企业。公司作为多个标准化组织理事成员及单类头单位,参与多项国家及行业标准制定,同时公司积极推进国家网络安全强国战略,为数万家党政机关及行业用户提供安全保密产品及服务。

公司拥有百余项产品资质,包括:涉密信息系统产品检测证书、网络安全专用产品安全检测 / 认证证书、商用密码产品认证证书、信创产品兼容性认证证书等。公司各类产品和解决方案广泛应用于党政、特殊行业、央国企等各领域,积累了丰富的客户资源以及良好的市场口碑,获得了多方客户的肯定和赞扬。公司的网络安全能力得到国家相关单位的高度认可,长期为党和国家重大会议、重大赛事活动提供网络安全保障;公司多次荣获国家保密科学技术奖、国家密码科学技术奖、公安部科学技术奖及多项省级各类科学技术奖等,在业界影响深远。

报告期内,由中国信息协会信息安全专业委员会 PCSA 安全研究院 / 联盟主导,联合包括中孚信息在内的成员单位、行业用户及产业各方共同完成《数字时代:实现数据要素化安全保护象限图》正式发布。作为重要产业研究力量,公司凭借在数据安全领域的专业积淀,深度参与此次研究工作,历时半年精心打磨,为数字产业、行业用户和从业者提供了数据要素化安全保护工作的工作指引,对推动数据要素高质量发展具有非常重要的现实指导意义。

报告期内,公司荣获多项行业奖项,作为网络安全领域重点企业,凭借多年技术积累与市场表现,公司行业地位得到了不断提升。

2025 年 1 月,由山东省大数据协会与山东省数据和信息技术应用创新协会联合主办的“山东省大数据企业 50 强”评选结果正式公布,全资子公司中孚安全凭借在大数据领域的创新研发能力、核心产品以及技术方面的突出优势,成功入选。

2025 年 1 月,STIF 第五届国际科创节暨 2024 新质生产力领航者峰会于 2025 年 1 月 8 日在北京举行,公司凭借非凡的创新精神荣获“2024 年度产品创新奖”。

2025 年 1 月,工业和信息化部移动互联网 APP 产品安全漏洞专业库(CAPPVD 漏洞库)公布了 2024 年度技术支撑单位能力评定结果。公司凭借行业领先的漏洞挖掘能力、突出的漏洞报送工作表现、优质的安全服务能力再次成功入选,获评 CAPPVD 漏洞库二届级技术支撑单位。

2025 年 2 月,由灾备联盟信创工委会、安东工作室联合主办的“2024 年度十大信创安全品牌”评选结果正式揭晓,公司凭借优异成绩荣获“2024 年度十大信创安全品牌”榜单。

2025 年 3 月,公司凭借其在漏洞挖掘、检测、修复、报创漏洞支撑以及漏洞预警支撑等领域的突出贡献,顺利升至国家信息安全漏洞库(CNNVD)一级技术支撑单位,成为该领域最高等级支撑单位之一。

2025 年 5 月,由山东省委网信办公布了第二届网络安全技术支撑单位(2025-2027)遴选结果,公司凭借数据安全领域的卓越技术实力和丰富实践经验,成功入选数据