

中国网络安全行业年报

China Cybersecurity Industry Annual Report

2026-9

北京赛博英杰科技有限公司

01	2026 中国网络安全产业八大趋势 AI、地缘、合规、跨界、采购、AI原生、资本与出海八个维度
02	网信安全政策与立法动态 国家政策全景、五个专题解读、六类行业场景落地与合规影响
03	中国网络安全市场数据分析 甲方支出与厂商收入、区域与行业结构、客户与渠道分层、细分产品热度
04	国际最新动态 Gartner 年度趋势、RSAC 创新沙盒、欧盟行动计划与前沿威胁
05	2026年中国网络安全十大创新方向 从模型防护走向行动、身份、应用、供应链与基础设施
06	中国网络安全百强和新势力 百强评选方法、竞争格局与新势力30强名单
07	中国网络安全二级市场分析 上市公司横向对比、经营与战略、市值与估值
08	中国网络安全一级市场分析 投融资总量与结构、投资机构、并购与整合

技术、规则、市场与经营四个维度共同重塑产业边界



人工智能正在从单点创新能力，升级为重塑网络安全产业格局的核心变量。它不仅改变攻击方式，使社工、攻击链编排和自动化对抗更加复杂，也推动防御体系从智能助手迈向具备调查、研判和有限处置能力的安全智能体。同时，模型、数据、智能体及其权限成为新的保护对象，产品形态、服务模式和交付边界也随之重构。未来竞争壁垒将不再取决于 AI 功能数量，而在于可验证的安全效果。

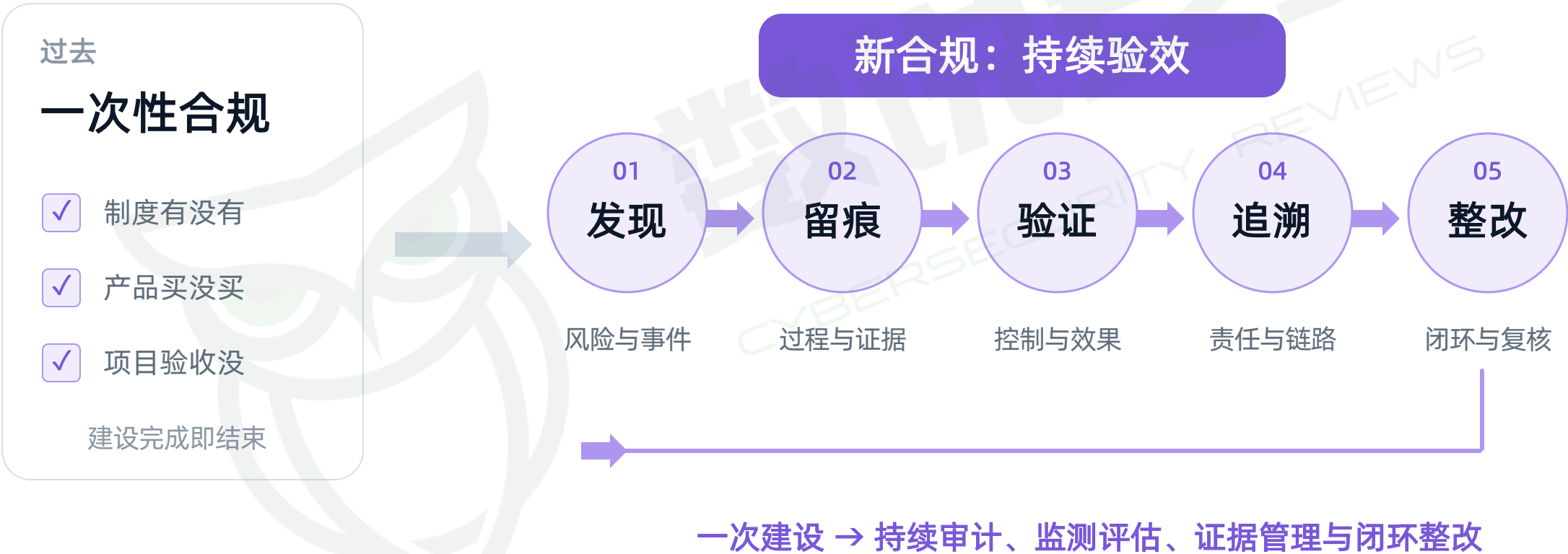
数据 × 模型 × 专家知识 × 运营能力



地缘竞争正在从网络空间攻防外溢至安全产品准入、供应链审查、可信来源认定、数据跨境和安全认证。全球网络安全市场并非全面脱钩，但统一的产品、规则和供应链体系正在分化为不同区域、不同标准和不同信任体系。安全厂商一方面面临国内自主可控和供应链安全要求，另一方面又要应对海外市场的重复认证、本地化交付和来源审查，应对地缘风险及满足各地准入要求的能力，正成为决定企业市场边界的重要因素。



网络安全合规正在从“制度有没有、产品买没买”转向“风险能否发现、过程能否留痕、效果能否验证、责任能否追溯”。个人信息保护合规审计、人工智能生成内容标识、网络安全事件报告和网络数据安全风险评估等制度陆续落地，推动需求由一次性合规建设转向持续审计、监测评估、证据管理和闭环整改。新合规不是传统合规项目的简单回归，而是推动产品能力、运营服务和交付标准升级的新动力。



运营商、央国企数字化集团和云厂商早已成为网络安全市场的重要参与者，新的变化不再是“谁在进场”，而是跨界资源能否兑现为持续收入和经营收益。中国电信2025年安全业务收入由2024年的162亿元增至166亿元，同比增长约2.5%；中国移动控股启明星辰后，启明星辰2025年收入下降29.49%，归母净亏损5.72亿元。实践表明，客户、资本、渠道和云网资源是竞争的放大器，但不能替代安全专业能力。产业关系正由简单的跨界替代转向云网安融合、专业分工和生态竞合。



客户评价安全建设的标准正在从产品数量、功能清单和项目验收，转向风险发现率、响应时间、事件闭环率、服务等级和实际风险降低。平台化是能力架构，托管运营是交付方式，订阅制是付费机制，三者共同推动网络安全收入由一次性项目向持续服务迁移。2025 年安全服务市场项目需求保持活跃。不过，订阅和托管服务能否真正形成稳定增长，仍取决于续费率、服务毛利率和结果量化能力



NO.1

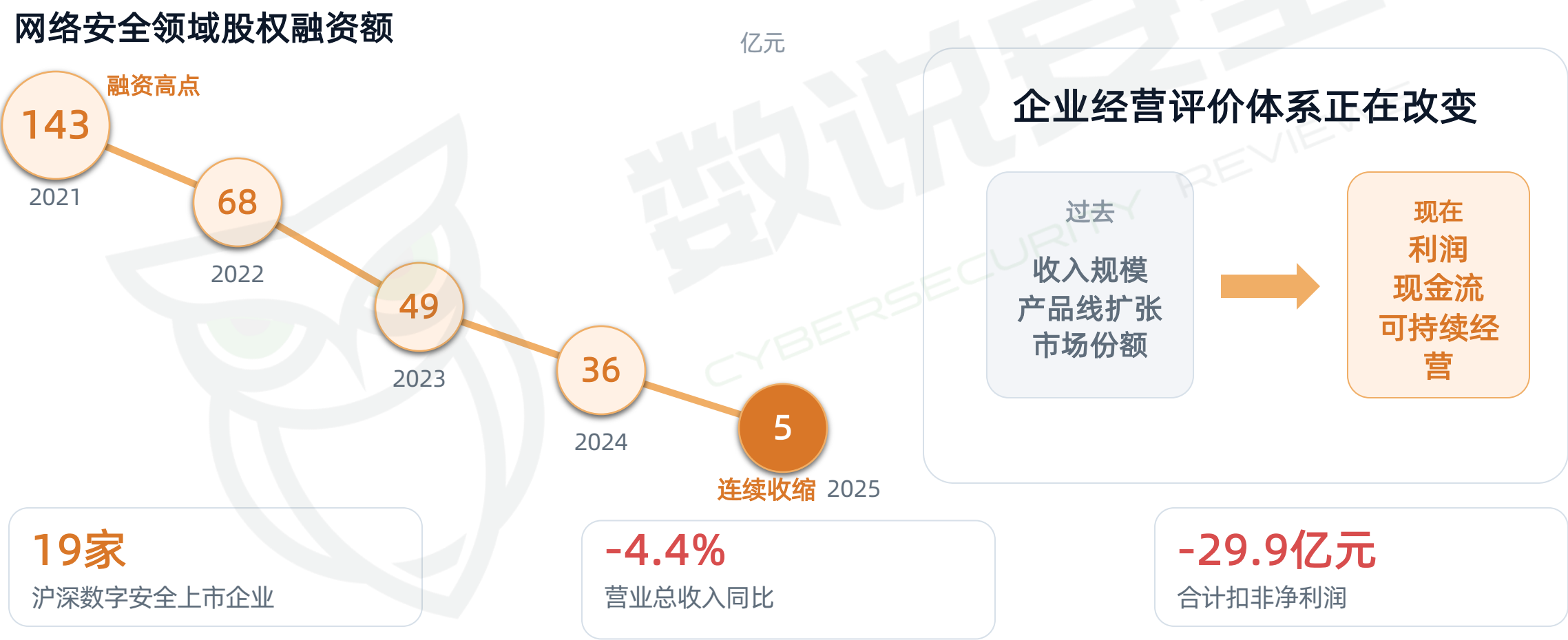
安全服务项目数量居首
2021-2025年项目热度持续上行

真正形成稳定增长，还取决于续费率、服务毛利率与结果量化能力

AI应用正在由单一模型接口演变为数据、模型、向量库、智能体、记忆、工具协议、第三方服务和算力集群共同组成的复合基础设施，传统安全边界随之从“网络—终端—身份—应用”扩展至“算力—数据—模型—智能体—工具—行动”。AI原生安全不是在传统产品中简单接入大模型，而是围绕AI系统的开发和运行方式，重新设计资产发现、身份委托、权限控制、供应链治理、运行时防护、持续测评和人工监督体系。网络安全由保护数字化基础设施，进一步走向保护智能化基础设施



资本寒冬仍在延续。2025年数字安全领域股权融资26笔，同比下降62%；融资额5.42亿元，同比下降85%，较2021年143亿元的高点大幅收缩。个别企业已经进入停摆、破产或被整合阶段。与此同时，安全企业开始压缩低毛利项目和非核心产品线，加强回款、费用控制和客户筛选。19家主要网安上市企业2025年营业总收入下降4.4%，安全业务收入下降7.11%，合计扣非净亏损29.9亿元，说明行业尚未实现整体利润修复，但经营评价体系已经从收入增长、产品线扩张和市场份额，转向利润、现金流和可持续生存能力



在国内市场增速放缓、竞争加剧的背景下，出海正由少数头部企业的战略选择转变为越来越多安全公司的共同探索方向，东南亚、中东、拉美等市场成为重点区域。但网络安全具有较强的国家信任、法规认证、渠道关系和本地服务属性，出海难度远高于一般软件产品。

目前，少数厂商已形成可以验证的海外收入，例如深信服2025年海外收入约5.99亿元，同比增长24.49%，但占总收入仍只有7.45%，且其中包含云计算和IT基础设施业务。多数专业安全厂商仍处于渠道搭建、产品适配和项目验证阶段。因此，未来出海的核心不只是产品出口，而是建立本地渠道、合规认证、交付服务和品牌信任组成的完整经营体系。



深信服 2025	5.99亿元	+24.49%	7.45%	口径含云计算及IT基础设施业务 规模突破依赖完整本地经营体系
	海外收入	同比增长	占总收入比重	

网信安全政策与立法动态

2025年1月1日—2026年9月8日 | 国家政策全景、重点制度与行业场景

国家政策全景与立法理念比较

监管义务逐步细化，数据流通和人工智能政策同步完善

主题	本期主要制度变化	关联应用场景
基础法律与监督	网络安全法修正；治安法、反不正当竞争法修订；事件报告与监督检查配套	治理责任、应急响应、数据权益保护
个人信息与数据	合规审计、负责人报送、人脸备案、风险评估、小型处理者简化措施	审计评估、分类分级、隐私管理
跨境与公共数据	出境认证、评估申报指南；公共数据登记、授权运营及政务数据共享	跨境合规、公共数据开发运营
人工智能与平台	生成内容标识、拟人化互动、智能体、未成年人保护及MCN管理	内容安全、模型治理、平台责任
行业与产品	金融、能源、交通等行业数据制度；商用密码、网络安全标识及相关标准	行业安全能力、密码应用、产品测评

资料来源：相关部门官方公开文件；

共同追求安全与发展，差别主要在制度出发点与治理方式

比较维度	中国	美国	欧盟
治理目标	统筹发展与安全；兼顾网络主权、国家安全、公共利益及个人权益	关键基础设施韧性、国家安全与消费者保护并重，侧重风险治理	基本权利保护与统一市场并行，追求共同安全水平和系统韧性
制度结构	网安法、数安法、个保法形成全国性基础制度，配套分类分级及行业监管	联邦行业规则、州法与监管执法并行，辅以NIST等风险管理框架	GDPR统一数据保护；NIS2协调成员国要求；CRA统一数字产品安全规则
合规方式	明确主体责任、等保和关基保护，落实审计、评估、报告及监督检查	强调基于风险的合理安全措施；行业强制规则与灵活实施方法结合	强调风险与比例原则、可证明的问责，并规定管理层及产品生命周期责任
跨境数据治理	数据与场景分级管理，配置安全评估、合同、认证及豁免，促进合规流动	基于国家安全，对“关注国家”等相关的特定敏感数据交易实行定向限制	重视个人数据保护水平延续，通过充分性认定、标准合同等保障跨境传输

中美差异侧重监管结构与实施方式；中欧差异侧重国家整体安全治理与基本权利、统一市场的制度组织。

注：本页为制度比较的研究归纳，含此前立法；NIST CSF为指导框架，CRA主要义务分阶段适用。

专题分析

阈值、审计周期与报送要求应分别适用

适用对象 / 场景	合规义务	依据
处理超过1000万人个人信息	至少每两年开展一次个人信息保护合规审计	合规审计管理办法 2025.05施行
处理100万人以上个人信息	设置个人信息保护负责人，向市级网信部门报送信息	审计办法及负责人信息报送公告
存储人脸信息达到10万人	向省级网信部门备案	人脸识别办法及备案公告 2025.06施行
处理未成年人个人信息	每年开展审计，次年 1 月底前报送审计结果	未成年人网络保护条例既有义务 2025年报送公告细化程序
处理不满10万人个人信息	适用简化措施，简便审计至少 5 年一次；未成年人业务不得豁免特殊义务	小型处理者简化措施规定 2026.09施行

合规审计管理办法不适用于国家机关及法律法规授权的具有管理公共事务职能的组织；

出境路径、申报材料与行业判定规则进一步细化

文件	时间	本期变化
数据出境安全评估申报指南（第三版）	2025.06.27发布	优化申报材料，并明确评估结果有效期延期的条件、流程及材料
个人信息出境认证办法	2026.01施行	落实认证路径的适用、申请、机构备案和监督；依法应开展安全评估的情形不能以认证替代
个人信息出境认证依据标准变更公告	2025.12.25公开并实施	认证依据调整为GB/T 35273与GB/T 46068；具体实施时间以相应标准公告为准
汽车数据出境安全指引（2026版）	2026.01.30印发	按汽车场景细化重要数据判定、出境管理路径及豁免条件
自贸试验区数据出境负面清单	地方配套 分地区适用	按具体地区、主体及数据场景核对适用范围；不将一地清单推定适用于全国

资料来源：相关部门官方公开文件

报告机制与执法程序进一步明确，行业要求仍需分别识别

文件与日期	适用重点	组织需要落实的工作
国家网络安全事件报告管理办法 2025.11施行	规定较大以上网络安全事件的报告范围、时限、渠道和内容	建立事件分级、首报、续报与总结流程，将法定时限落实到值班和处置机制
央行业务领域事件报告办法 2025.08施行	央行业务领域网络安全事件分级报告	将金融行业报告渠道与国家及其他主管部门要求逐项衔接
网信行政处罚裁量权基准适用规定 2025.08施行	规范网信行政处罚裁量与适用	保留履责、整改、风险处置等事实材料
公安机关网络空间安全监督检查办法 2026.10.01起施行（截至报告日尚未施行）	公安机关网络空间安全监督检查的程序及责任	按正式办法核对监督检查对象、检查事项和配合义务；截至报告日仍处实施准备期

资料来源：相关部门官方公开文件

内容可识别、用户权益和持续情感互动成为明确治理对象

规则	适用与义务	效力与时间
人工智能生成合成内容标识办法	区分显式与隐式标识，明确生产、传播及用户声明责任；特定情形按规则处理显式标识	规范性文件 2025.09施行
GB 45438-2025 标识方法	提供生成合成内容标识的技术实施要求，与管理办法衔接	强制性国家标准 2025.09实施
人工智能拟人化互动服务管理暂行办法	针对面向境内公众、模拟自然人人格特征等的持续性情感互动服务	部门规章 四章32条 2026.04.10公布，07.15施行
拟人化互动的关键要求	AI身份提示、交互数据与个人信息保护、未成年人保护、安全管理及评估	不涉及持续情感互动的智能客服、工作助手、知识问答等不适用办法

资料来源：相关部门官方公开文件

2026.08.20施行 | 重要数据年度评估与一般数据鼓励性评估分开

事项	规则要点	执行含义
重要数据处理者	每年开展评估；重要数据安全状态发生重大变化、可能造成不利影响时，及时评估变化及影响部分	数据目录和处理活动变化应接入评估触发机制
一般数据处理者	鼓励至少每三年开展一次风险评估	不应表述为所有数据处理者必须每年评估
年度评估报告	年度评估完成后20个工作日内按要求报送报告；评估报告至少保存三年	明确主管部门职责渠道，留存评估、整改与报送材料
委托评估与监管评估	可委托第三方；监管责令评估适用相应认证要求	不得将所有委托评估一概写成法定资质准入
与其他制度衔接	评估关注数据处理合法性、管理制度、安全措施及风险整改	与个人信息审计、出境评估分别判断适用，减少重复取证

资料来源：相关部门官方公开文件

行业落地

登记、授权运营、共享和披露分别建立配套规则。

环节	本期文件	安全与治理重点
资源登记	公共数据资源登记管理暂行办法 2025.03.01施行	纳入授权运营范围的资源应登记；登记机构履行数据安全保护义务
授权运营	公共数据资源授权运营实施规范（试行） 2025.03.01施行	落实分类分级、个人信息保护、安全审核及风险监测，建设可追溯的开发环境
运营约束	价格形成机制通知；2026年信息披露通知	明确收费和信息公开要求，披露运营情况；属于治理配套，不等同于安全专项规章
政务共享	政务数据共享条例 2025.08.01施行	明确数据提供、使用、平台管理等单位安全责任；国家秘密、工作秘密数据不在本条例政务数据范围内
流通利用	数据流通安全治理实施方案；合同示范文本	明确使用目的、安全保密和责任约定，推动数据合规流通

资料来源：相关部门官方公开文件

平台认定、信息分类、年申报送和内容分发责任衔接

文件	施行 / 公开时间	要点
可能影响未成年人身心健康的网络信息分类办法	2026.03.01施行	界定相关信息类别及显著提示要求，规范向未成年人呈现、推荐相关信息
未成年人重点平台认定办法（简称）	2026.04.01施行	按未成年人用户规模及显著影响认定，设置自评申报与复核程序，支撑特别保护义务
未成年人个人信息审计情况报送公告	2025.12.29公开	将既有年审义务落实为每年1月底前报送上一年度审计情况
互联网信息内容多渠道分发服务管理规定	2026.09.01施行	明确MCN机构及平台的登记、协议和内容安全管理责任，保护未成年人权益
网络交易平台规则 / 直播电商监督管理办法	均于2026.02施行	在平台经营和直播业务中落实网络数据、个人信息、信息内容及未成年人保护要求

资料来源：相关部门官方公开文件

商用密码应用、电子认证与网络安全标识分别适用

制度	日期与状态	要点
关键信息基础设施商用密码使用管理规定	2025年8月施行	细化关基商用密码使用、应用安全性评估与监督要求
电子认证服务使用密码管理办法	2026.07施行	规范电子认证服务使用密码的许可与监督；配套公告明确存量持证单位评估报送安排
商用密码产品认证目录（第三批）	2025年发布	扩大认证产品覆盖；认证目录与行政许可、应用评估分别适用
网络安全标识管理办法	2026.07.01施行	目录管理、自愿参与；按规则开展检测、备案及标识使用
第一批网络安全标识产品目录及规则	2026.06.15印发	首批为消费类网联摄像头；不能表述为所有联网产品普遍强制认证

资料来源：相关部门官方公开文件

便利身份核验的同时，明确生物识别和公共视频的使用边界

制度	主要规定	适用边界
国家网络身份认证公共服务管理办法 2025.07.15施行	网号、网证自愿申领使用；平台自愿接入，限制明文身份信息重复收集	保留其他实名核验方式，并保障用户同等服务
人脸识别技术应用安全管理办法 2025.06施行	落实必要性、告知同意、影响评估、安全措施与达到门槛后的备案	存在其他非人脸方式实现同等目的或业务要求时，不得作为唯一验证方式
公共安全视频图像信息系统管理条例 2025.04施行	规范公共安全视频系统建设、使用与管理，保护视频图像信息安全和个人权益	应按公共安全场景及法定范围判断适用，防止擅自调取、提供或传播

资料来源：相关部门官方公开文件

行业数据制度与运行安全要求持续细化

领域	本期文件	安全要求
能源电力	能源行业数据安全管理办法（试行） 2026.07施行	分类分级、重要数据目录、全生命周期管理及监测评估；用户侧涉网通知另含电力监控网络安全要求
工业	2025年护航新型工业化网络安全专项行动方案	部署工业互联网及工控网络分类分级管理、防护能力提升和风险治理
交通运输	交通运输数据安全管理办法 2026.07施行	委托及共同处理、风险评估、日志留存及AI数据合理性评估等
智能网联汽车	准入、召回及软件在线升级管理通知 2025年发布	加强OTA备案、事件事故报告与召回管理，持续符合网络、数据和个人信息保护要求
汽车数据出境	汽车数据出境安全指引（2026版）	场景化细化出境路径、豁免和重要数据判定；与汽车产品安全要求分别核对

资料来源：相关部门官方公开文件

数据使用授权、应用备案与运行管理形成具体要求

领域	本期文件	安全重点
医疗电子病历	进一步加强医疗机构电子病历信息使用管理通知 2025年6月印发	访问授权、使用留痕、外部服务商保密及授权协议、共享来源验证和定期安全评估
教育数字化	关于加快推进教育数字化的意见 2025年4月印发	包含网络安全、数据安全、个人信息保护及AI算法模型备案、安全评估等任务
政务App	政务移动互联网应用程序规范化管理办法 2026.01.25印发并施行	纳入统一备案范围的政务应用上线前备案；落实安全保密责任，关停前依法处置数据
政务App备案	备案工作指南（第一版） 2026.02.28公开	细化备案流程；纳入范围的存量应用六个月内备案，期限已届满。不承担行政职能的事业单位App不纳入
电子印章与单证	电子印章管理办法；促进和规范电子单证应用规定	分别规范印章信息保护和单证系统可靠性、等级保护、数据安全与个人信息保护

资料来源：相关部门官方公开文件

以适用义务和可核验证据组织能力建设

政策对应工作	企业应形成的履责材料	相关安全能力
分类分级与数据处理管理	数据目录、重要数据识别、处理活动记录与权限清单	数据发现分类、访问控制、日志审计
审计、评估与风险整改	评估审计报告、风险台账、整改证明、报送留痕	审计评估服务、持续监测与整改管理
事件发现与报告	分级规则、联络机制、报告模板、处置及演练记录	安全运营、应急响应、取证与报告支持
AI及平台内容治理	标识策略、服务边界、未成年人措施、内容处置和数据使用记录	内容识别、模型安全测试、隐私与权限治理
产品、密码及行业适配	适用标准清单、测试评估记录、密码应用及行业控制措施	产品测评、密码应用、行业系统安全建设

本页为对已公布文件的研究归纳，不据此推定市场规模或采购增速。

场景落地层

搭建三级标准化评判标尺，建立闭环动态监管约束机制



《网络安全标识管理办法》解读

总 则

立法目的	提升联网产品安全能力、保护消费者权益、防范物联网设备网络风险，维护网络空间公共安全中国政府网。
适用范围	全部具备联网功能软硬件产品，实行目录分批管理，暂不一次性全覆盖所有品类。
核心原则	统筹发展与安全，标识申报企业自愿，政府鼓励厂商申领、采购方优先选用带标识产品。
监管分工	三部门统筹制定产品目录、行业实施细则；委托电子标准研究院统一承担备案、公示、信息查询工作。

标识实施

三级 分级 体系	一星（基础级）	守住安全底线，禁用弱口令、建立常态化漏洞修复、保障系统持续更新；
	二星（增强级）	达到行业中上水平，强化加密、权限管控、异常行为监测；
	三星（领先级）	行业最高标准，必须通过第三方渗透测试，可用于政务、关键行业场景中国政府网。
标识统一规范	固定样式，含厂商、型号、星级、有效期、检测机构、备案二维码，扫码可查完整检测报告，全程追溯。	
申报与检测规则	企业自主委托合规实验室测评，二星可使用企业自有 CNAS 实验室，三星强制外部第三方测试。	
备案与有效期管理	检测通过后向备案机构登记，标识设置固定有效期；产品架构、安全机制重大变更需重新检测备案。	
标识使用要求	仅允许对应型号合规产品张贴、展示；不得跨型号、跨等级冒用标识，宣传不得夸大安全能力。	

监督管理

日常监管机制	三部门开展抽查、专项检查，核验检测报告真实性、产品安全能力与标识等级匹配度。	
动态 处置 措施	限期整改	产品安全不达标、未及时修复高危漏洞；
	暂停使用标识	整改期间限制对外标注宣传；
	撤销标识	伪造检测、冒用星级、出现重大安全事件拒不整改。
检测机构管控	严打出具虚假测评报告，违规机构取消资质并公示。	
信用管理	厂商、检测机构违规行为纳入行业安全信用记录，向社会公示。	
投诉渠道	面向公众开放举报通道，核查存在虚假标识、安全造假行为依法处置。	

附 则

明确术语定义	界定网络安全能力、联网产品、备案机构等概念。
配套机制授权	各品类产品配套实施规则、安全标准由三部门另行分批发布。
施行说明	明确本办法自 2026 年 7 月 1 日起正式实施。

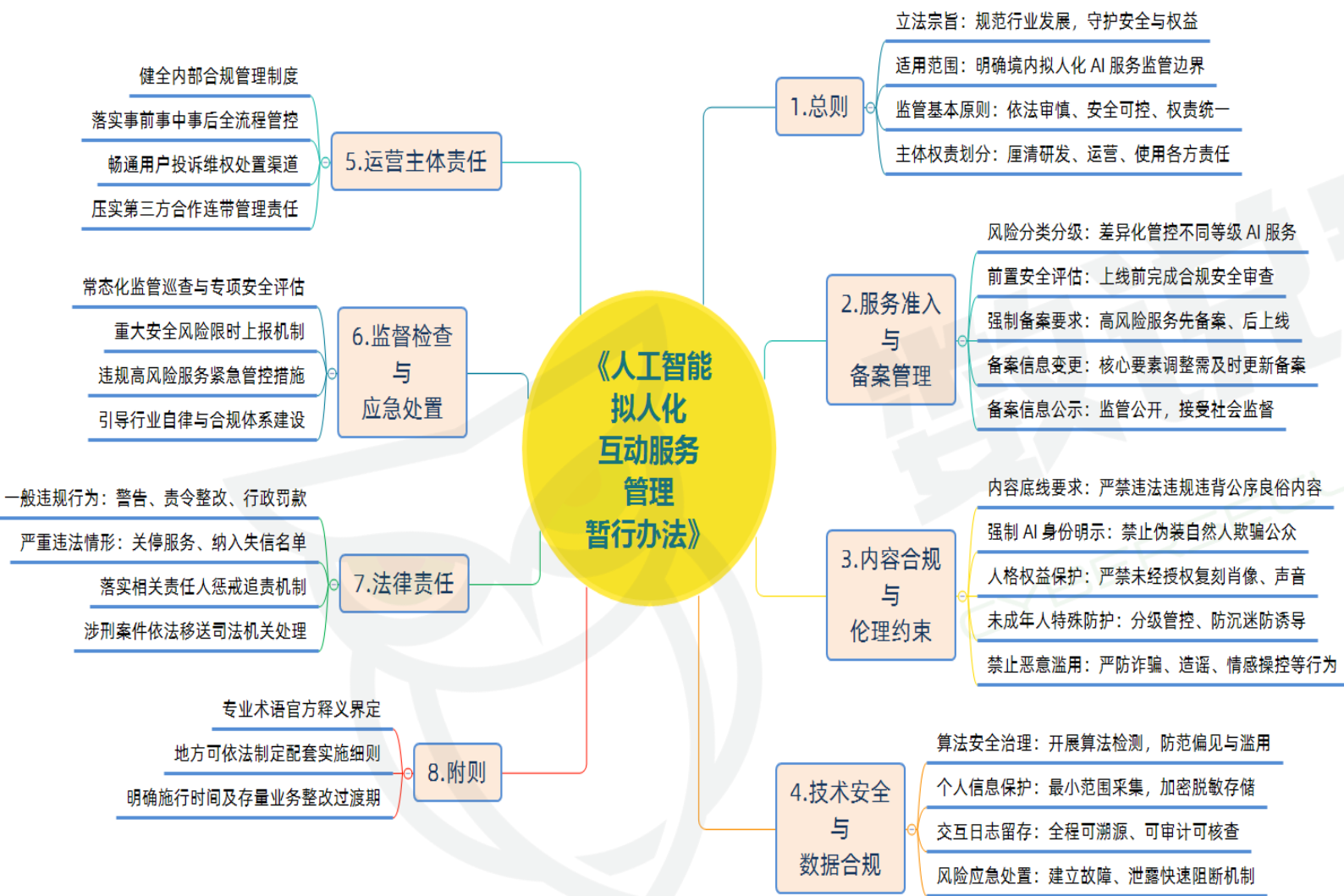
- 本办法 2026 年 4 月 2 日由网信办、工信部、公安部联合印发，7 月 1 日起实施，依据《网络安全法》《密码法》《国家安全法》制定，聚焦物联网、智能硬件安全信息不透明痛点，确立统筹发展安全、企业自愿申报、市场正向激励三大原则，由三部门统筹监管，委托电子标准院负责标识备案、公示与查询，构建政企协同治理框架。
- 办法设立了一星基础、二星增强、三星领先三级安全标识，同时统一标识外观、溯源二维码及有效期管理，规范企业检测申报、产品张贴、型号变更复检全流程，禁止冒用星级、夸大安全性能，让设备安全等级直观可辨。
- 监督管理章节监管部门常态化抽查核验产品实际安全水平，根据违规轻重采取限期整改、暂停标识、撤销公示等分级处置，从严管控第三方检测机构，虚假测评将取消资质，形成“申报 — 公示 — 抽查 — 惩戒”闭环监管，压实厂商、检测机构、采购方安全责任。
- 附则章节对联网产品、网络安全标识等专有名词作出定义，授权主管部门分品类出台配套实施细则与安全标准，衔接现有网络安全、商用密码相关法规，打通法律法规落地执行的衔接障碍。
- 办法填补了物联网设备出厂前端监管短板，借助分级标识统一行业安全评判标准，将安全管控前置至产品研发生产阶段，也倒逼企业加大安全研发投入，实现技术防护与法律监管融合，从源头防范设备入侵、数据泄露等风险，健全网络安全全链条法律体系。

2026年7月，《网络安全标识管理办法》分章节解读



2026年6月，《网络数据安全风险评估办法》分章节解读

- ❑ 《网络数据安全风险评估办法》于 2026 年 6 月 18 日由国家互联网信息办公室、工业和信息化部、公安部联合发布，2026 年 8 月 20 日起正式施行。该办法依托《网络安全法》《数据安全法》等上位法规制定，核心目标是压实数据处理主体责任，防范各类数据安全风险，维护国家安全、公共利益与公民个人合法权益。
- ❑ 办法明确了不同主体的评估频次要求，重要数据处理者每年至少开展一次全面数据安全风险评估，若业务架构、数据流转、系统环境等发生重大变化，须及时启动专项评估；仅处理一般数据的主体，建议定期开展安全评估。企业可自主评估，也可委托具备资质的第三方专业机构实施。
- ❑ 数据处理主体完成评估后需规范编制风险评估报告，明确数据处理现状、风险等级、防护措施以及整改方案，按规定报送行业主管部门与网信部门。针对评估过程中发现的安全漏洞、制度缺陷，相关单位必须落实闭环整改，从技术、管理、人员等维度完善防护手段，持续降低数据安全事件发生概率。
- ❑ 监管部门可抽查各单位风险评估工作，对敷衍评估、隐瞒风险、拒不整改企业责令重评，情节严重依法处罚。
- ❑ 最后一章统一了专业术语释义，明确各类小型内容经纪、代运营机构参照执行，理顺本规定与现有网络内容、网络表演相关法规衔接关系，对存量机构、账号设置过渡期整改要求，文件由国家网信办联合相关主管部门解释，统一于 2026 年8月20日正式落地实施。



2026 年 7 月 15 日施行的《人工智能拟人化互动服务管理暂行办法》，立足行业实际推动 AI 拟人化互动服务健康规范发展，秉持技术向善原则实施包容审慎、分类分级监管，统筹守住国家安全底线、防范各类公共与社会风险，全方位保护公民个人信息、身心健康及财产安全，规范数据采集、落实防沉迷与 AI 交互提示要求，同时针对性保护未成年人，禁止向其提供各类虚拟亲密关系类服务。

本页内容提炼了《暂行办法》的八大核心章节要点，以关键词形式呈现，便于快速聚焦法规核心框架，掌握合规关键要求。

01 第一章 总则：明确法规制定目的、适用服务范围，确立合法合规、公序良俗、以人为本的核心管理原则。

02 第二章 准入与备案：实施分类分级管理，明确服务提供者主体备案义务，强化事前准入环节规范化管控。

03 第三章 内容与伦理：规范内容生成导向，落实 AI 生成内容显著标识要求，保护用户肖像、隐私等合法权益。

04 第四章 技术与数据：保障算法安全可控，加强训练数据与用户交互数据保护，确保服务全流程可追溯。

05 第五章 运营主体责任：压实服务主体全流程管理责任，健全用户权益保障机制，及时处置用户投诉建议。

06 第六章 监督与应急：明确监管部门监督检查职责，要求服务主体制定突发事件预案，及时处置违规风险。

07 第七章 法律责任：细化违规行为的处罚种类与幅度，落实“双罚制”要求，明确直接责任人员的法律责任。

08 第八章 附则：界定“拟人化互动服务”等核心术语内涵，明确办法的施行时间及相关衔接性规定。

整套法规构建了全流程闭环监管体系，督促运营主体守牢安全底线，守护公众与国家安全，推动 AI 向善可持续发展。

2026年7月，《人工智能拟人化互动服务管理暂行办法》分章节解读

中国网络安全市场数据分析

网络安全市场项目由专项项目和网安集成类项目构成。其中专项项目专门针对网络安全产品或服务的采购而设立，能够更准确地反映网络安全市场的真实采购需求和趋势。2025年项目数量分析显示：

1

整体项目数量

2025年整体项目数量首次出现下降，但专项项目仍持续保持增长。

2

百万元以下

仍是专项项目的主要采购区间，项目数量同比增长明显。

3

百万至千万元

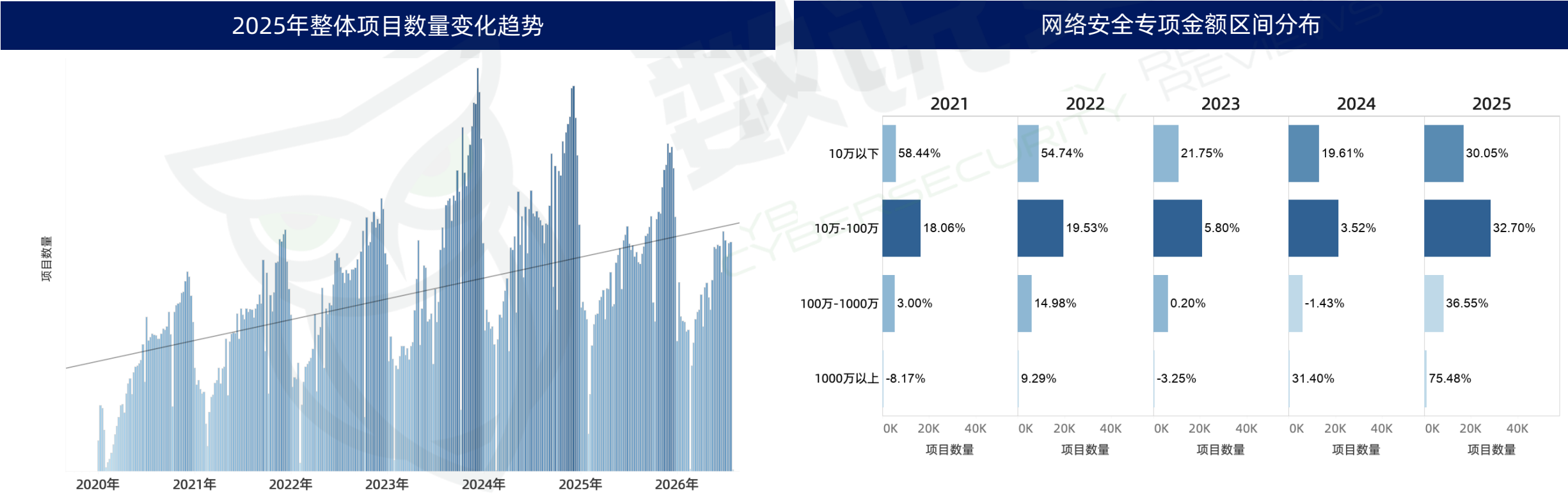
专项项目数量恢复增长，扭转了2024年的小幅下滑态势。

4

千万元以上

专项项目数量增速较高，但基数相对较小，易受单个大型项目落地节奏影响，年度波动明显。

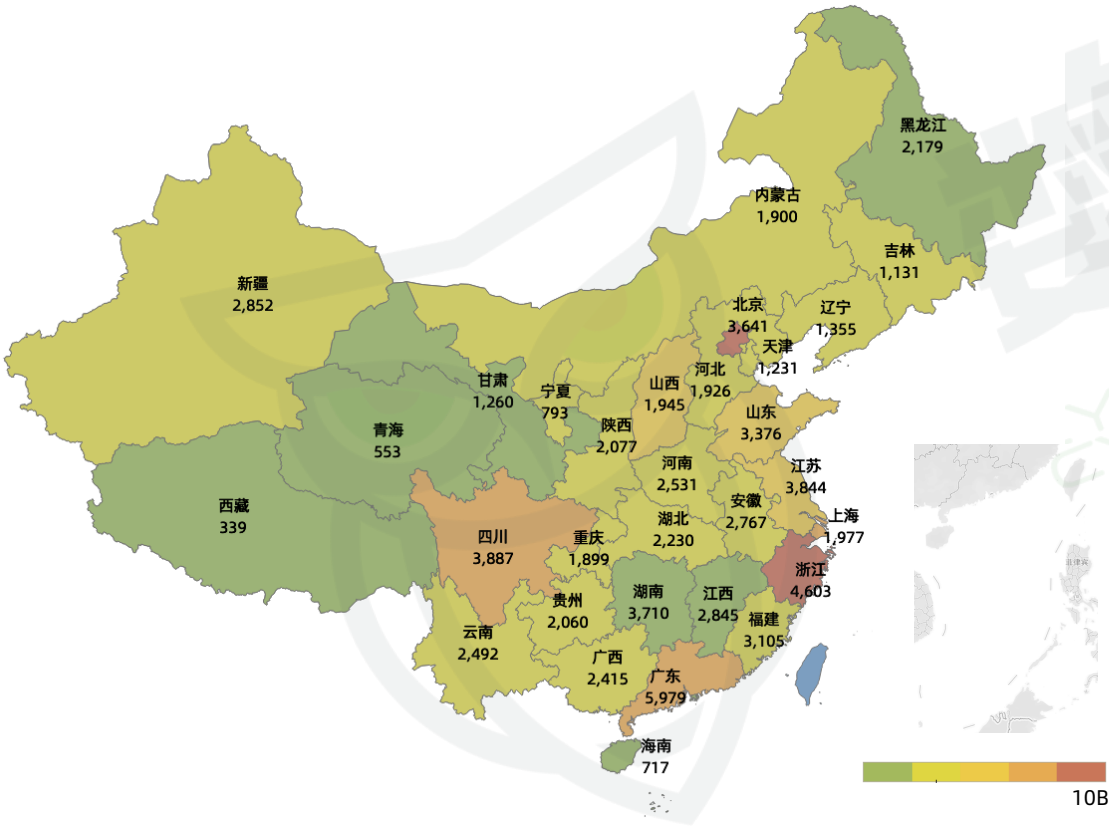
注：右图百分比表示该价格区间年同比增长率，柱状图长短表示项目数量



1 区域集聚特征

2025年中国网络安全客户数量与市场支出仍呈现较为明显的区域集聚特征，经济体量较大、数字化基础较好及重点行业集中的地区，仍是网络安全需求的重要承载地。北京、浙江、四川、广东、江苏、上海等省份客户数量和市场活跃度相对较高，区域市场梯队格局总体稳定。

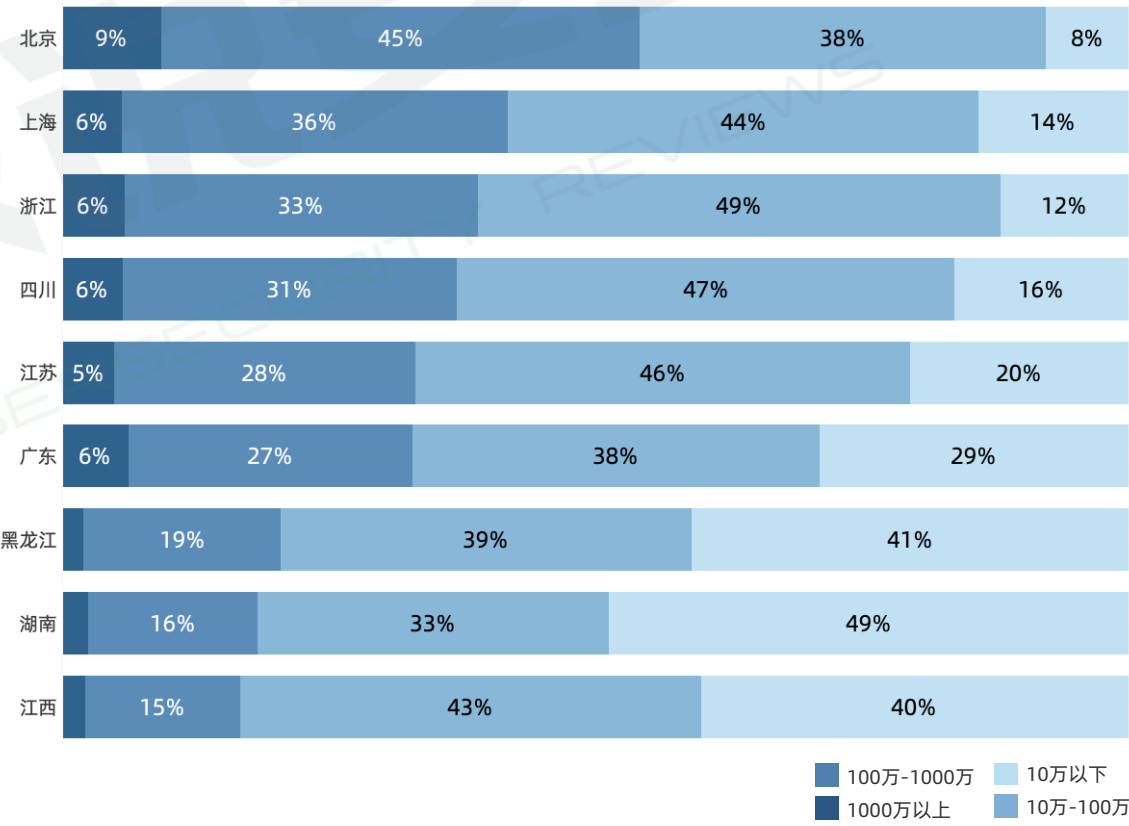
2025年网络安全市场区域客户数量与支出分析



2 项目结构分化

支出规模较大的省份项目数量较多，受政府机构、大型企业总部和重点行业客户集聚带动，百万元以上项目占比相对较高；支出规模较小的省份项目更多集中于百万元以下，黑龙江、湖南、江西等省占比超过70%。中小规模项目仍是各区域采购的基本盘，中大型项目的区域集中度更为明显。

2025年网络安全市场区域支出金额区间分布



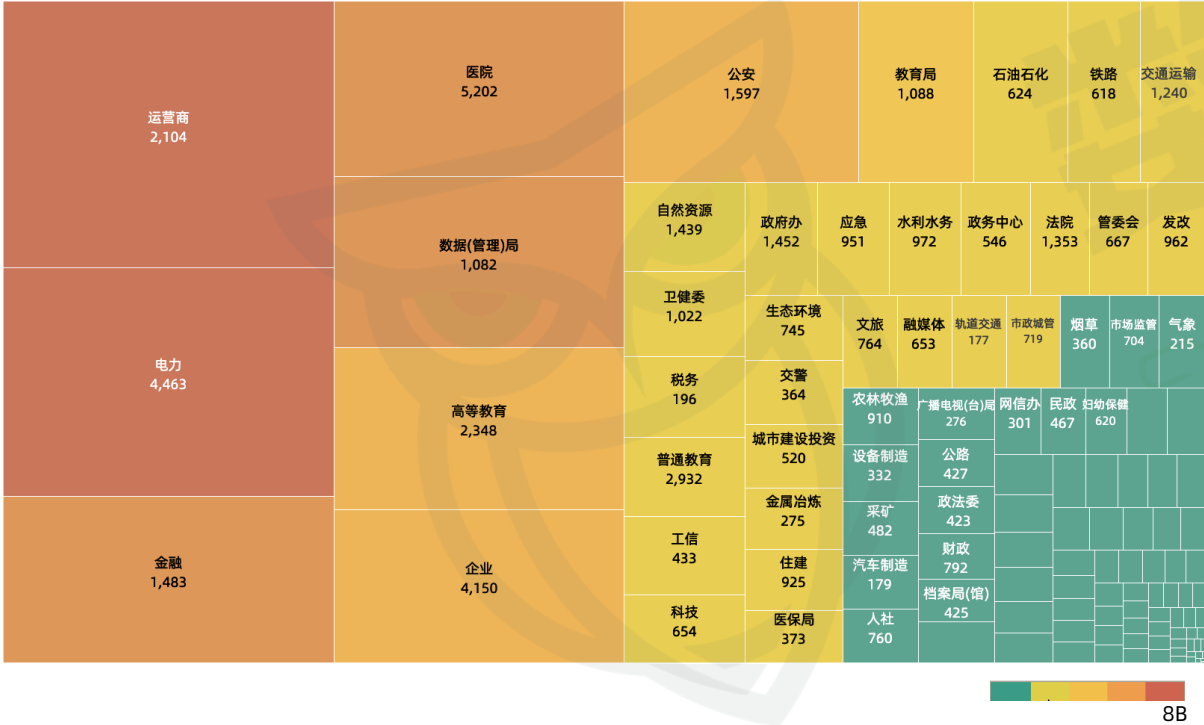
1

核心行业集中

2025年行业需求呈现“核心行业集中、投入强度分化”的特征。运营商、电力、金融、医院、数据（管理）局、高等教育、企业和公安等行业构成主要需求来源。其中运营商、电力等行业支出规模居于前列，是市场的重要支撑；医院、企业等行业客户数量较多，需求覆盖面更广。

注：左图颜色和大小表示客户支出规模，数字表示客户数量；右图气泡大小代表单客户平均网络安全支出。

2025年网络安全市场行业支出规模与客户分布

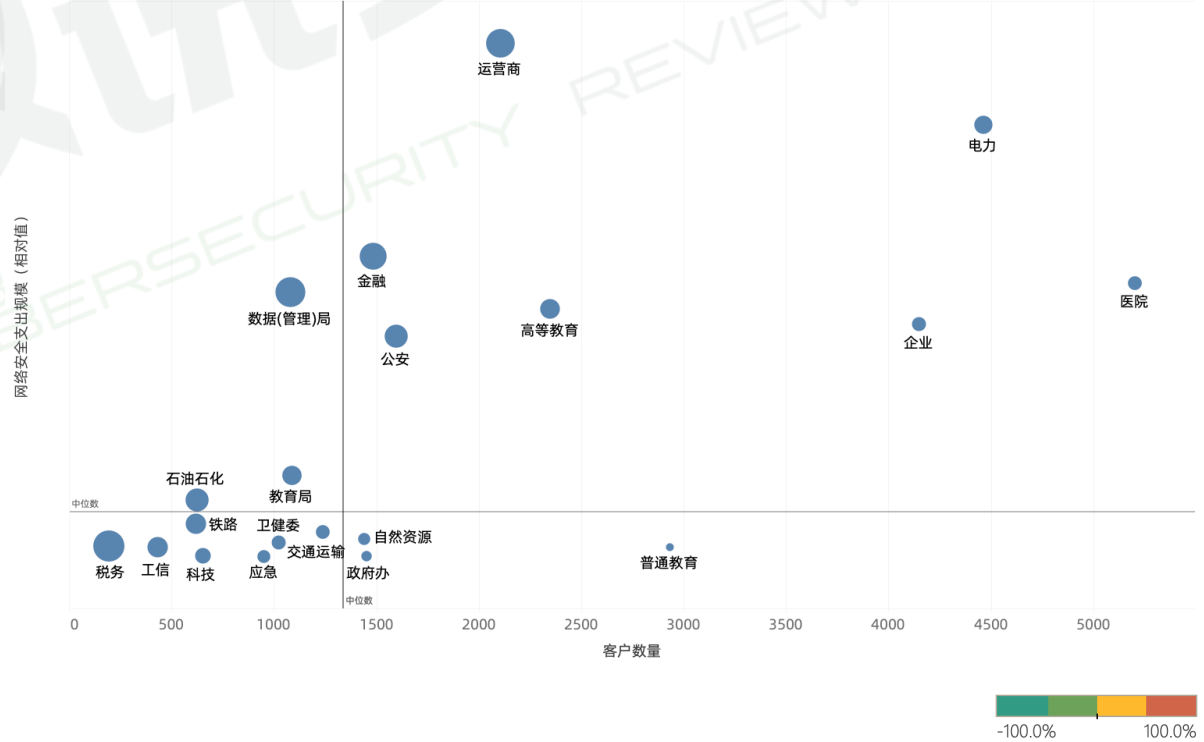


2

投入强度分化

运营商、金融、数据（管理）局等行业客户数量相对有限，但支出规模或单客户投入水平较高，体现关键业务保护、监管合规和体系化安全建设需求；医院、企业、普通教育等行业客户数量较多，但单客户投入相对分散。行业市场正由普遍建设转向结构化投入。

2025年网络安全支出规模前20行业投入特征对比



1

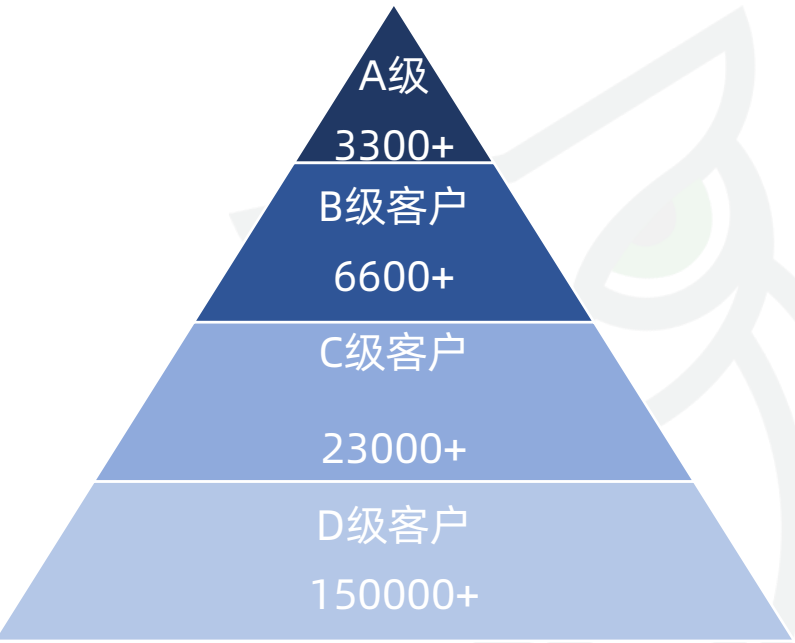
评级方法

基于近五年公开招投标项目的项目数量、项目金额及项目类型等多个维度关联分析，对网络安全客户进行综合评级，形成A、B、C、D四级客户体系。

2

分层结构

A级客户超3,300家，是采购规模大、持续活跃度高的核心客户；B级超6,600家，具备较强采购能力和市场影响力；C级超2.3万家，是支撑市场需求的重要组成；D级超15万家，构成覆盖面广泛的长尾群体。等级反映长期采购表现，年度数据变化会推动部分客户动态调整。



部分A级客户名单	
东莞市公安局	重庆银行股份有限公司
中国移动通信集团浙江有限公司	深圳市宝安区信息中心
中国联合网络通信有限公司	国家税务总局广东省税务局
天津市数据发展中心	中国联合网络通信有限公司北京市分公司
中国南方电网有限责任公司	东莞市政务服务数据管理局
杭州市数据资源管理局	深圳供电局有限公司
北京市公安局	中国联合网络通信有限公司软件研究院
广东省公安厅	中国工业互联网研究院（工业和信息化部密码应用研究中心）
中山市政务服务数据管理局	广东省政务服务和数据管理局
北京市大数据中心	广东电网有限责任公司
中山大学	内蒙古自治区大数据中心
上海市公安局	深圳市南山区政务服务和数据管理局
中国电信股份有限公司上海分公司	上海市大数据中心
国家工业信息安全发展研究中心（工业和信息化部电子第一研究所）	国家税务总局
中国信息通信研究院	成都市城市运行和政务服务管理办公室
广东电网有限责任公司广州供电局	中国移动通信集团广东有限公司
国家税务总局重庆市税务局	中央广播电视总台
清华大学	国家气象信息中心（中国气象局气象数据中心）
重庆市数字化城市运行和治理中心	杭州市地铁集团有限责任公司
汕尾市政务服务和数据管理局	中华人民共和国应急管理部

1 评级方法

基于近五年公开招投标项目中渠道商的中标及成交记录，从项目数量、项目金额及项目类型等多个维度对网络安全渠道进行综合评级，形成A、B、C、D四级渠道体系。

2 分层结构

A级渠道超3,400家，是长期参与、项目规模和市场覆盖能力较强的核心渠道；B级超6,700家，是服务与交付的重要支撑；C级超2.6万家，构成区域及细分领域的活跃力量；D级超10万家，形成长尾渠道网络。等级反映近五年持续参与度，不等同于单年收入或市场份额。



部分A级渠道名单

中科软科技股份有限公司	荣联科技集团股份有限公司
联通（浙江）产业互联网有限公司	北京银信长远科技股份有限公司
北京金信润天信息技术股份有限公司	中国软件与技术服务股份有限公司
上海仪电鑫森科技发展有限公司	北京神州新桥科技有限公司
浪潮软件集团有限公司	上海梦创双杨数据科技股份有限公司
北京华胜天成科技股份有限公司	北明软件有限公司
中通服建设有限公司	上海华讯网络系统有限公司
云南南天电子信息产业股份有限公司	中电鸿信信息科技有限公司
北京太极信息系统技术有限公司	东华软件股份公司
北京先进数通信息技术股份公司	紫光软件系统有限公司
北京奇虎科技有限公司	神州数码系统集成服务有限公司
内蒙古华强数智科技股份有限公司	建信金融科技有限责任公司
永信至诚科技集团股份有限公司	江苏天创科技有限公司
西安天泰创新科技有限公司	昆仑数智科技有限责任公司

通过对2025年部分网络安全上市公司的区域及行业项目数据跟踪，形成厂商与区域、厂商与行业的交叉分析。项目数量统计不能完全代表厂商市场份额，但能在一定程度上反映厂商的市场覆盖度、渗透率及其在不同区域与行业的表现和趋势。

2025年厂商区域项目分析

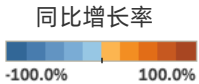
区域	安恒信息	迪普科技	绿盟科技	奇安信	启明星辰	山石网科	深信服	天融信	亚信安全
东北	159	141	396	955	362	68	604	420	94
华北	490	297	1,208	2,290	1,029	186	2,280	1,215	406
华东	1,309	612	1,594	3,704	1,777	833	5,317	2,758	521
华南	354	171	569	1,652	607	140	2,189	836	260
华中	245	148	519	1,542	489	113	1,478	729	188
西北	211	93	444	1,094	504	95	1,118	422	218
西南	412	259	658	1,648	725	147	2,008	752	210
总和	3,180	1,721	5,388	12,885	5,493	1,582	14,994	7,132	1,897

2025年厂商行业项目分析

一级行业	安恒信息	迪普科技	绿盟科技	奇安信	启明星辰	山石网科	深信服	天融信	亚信安全
电信	149	147	1,008	583	536	70	351	649	445
公检法司	271	253	408	1,502	765	77	1,153	800	92
交通	51	37	102	198	106	27	328	129	42
教育	380	178	352	1,048	305	285	2,201	558	106
金融	174	135	673	893	297	133	680	403	201
能源化工	117	77	384	662	406	123	885	441	110
其它	156	82	295	1,206	347	64	665	418	89
企业	89	73	217	424	191	51	616	264	80
医疗卫生	480	184	441	1,309	476	225	3,262	864	239
政府	1,285	543	1,397	4,997	2,007	510	4,546	2,532	447
制造业	28	19	116	171	75	26	368	118	45
总和	3,180	1,728	5,393	12,993	5,511	1,591	15,055	7,176	1,896

*以上数据基于公开数据整理，仅供参考；
厂商、区域和行业均按首字母顺序排列。

*因统计维度的不同以及数据质量原因，
区域及行业数量可能存在小幅偏差



1 结构分化

安全服务项目数量保持领先且持续增长；防火墙、安管平台、漏扫和IDPS等传统基础防护与管理类产品项目量仍相对靠前，但增速分化，市场进入存量采购、更新改造与能力优化阶段。

2 部分数据安全子方向提速

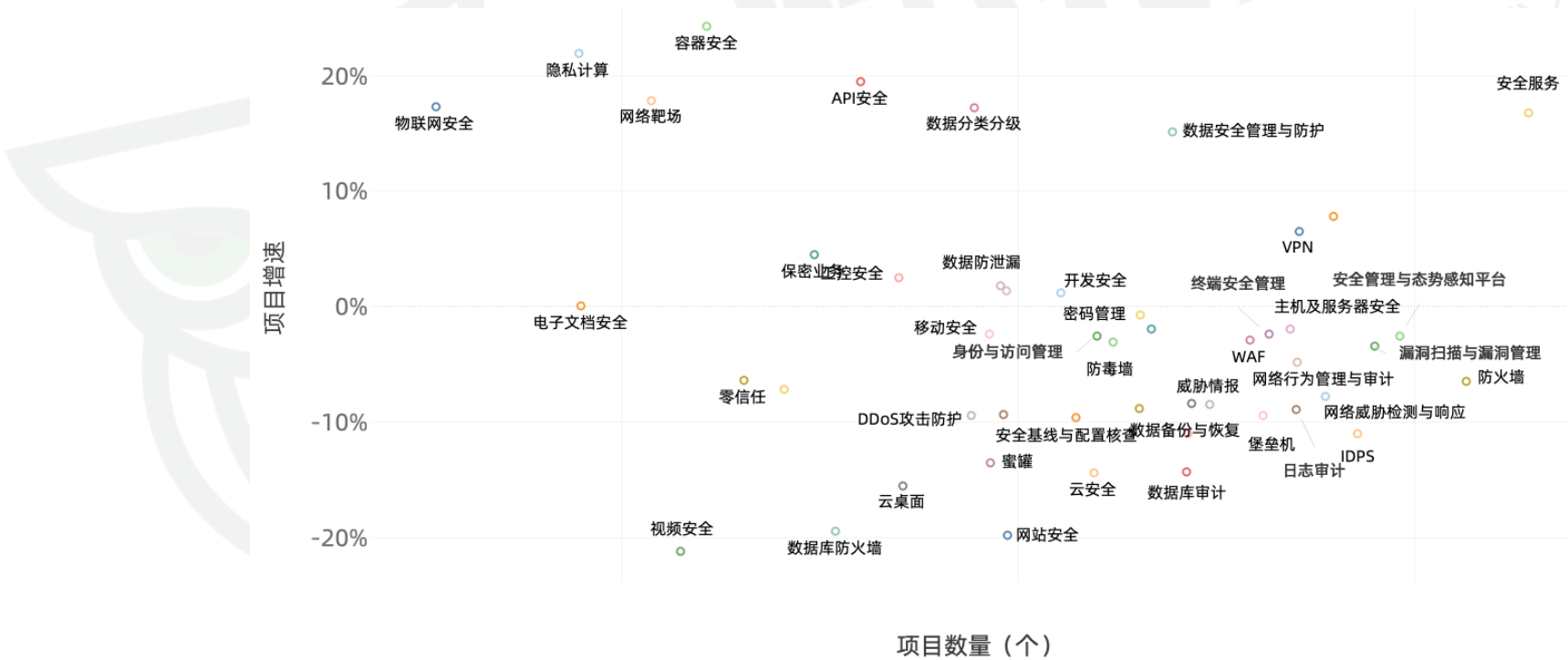
数据分类分级、数据安全管理与防护等方向项目增速较快，表明数据治理、数据资产保护和敏感数据安全管控仍是客户的重要投入方向。

3 新兴方向渗透

API安全、容器安全等方向增速居前。业务系统云化、接口开放、跨系统互联以及AI应用与智能体集成增多，推动暴露面持续扩大；但相较安全服务与传统产品，项目基数仍相对有限。

注：本图以网络安全专项项目为统计范围；横轴为各产品/服务项目数量，纵轴为项目数量同比增速。项目数据反映公开招投标市场活跃度，不等于对应细分市场的全部规模。

2025年网络安全专项项目产品需求态势



防火墙作为网络边界防护的基础产品，项目热度呈周期性波动，市场已进入常态化采购阶段。

头部品牌仍保持较强项目覆盖能力，不同品牌的项目同比增速差异明显，竞争格局持续调整。

项目价格中位数仍处于近五年低位并呈小幅波动，反映出市场价格竞争仍在持续。

医院、电力、教育、银行及运营商是主要需求来源，采购保持刚性但节奏存在差异。

2021-2025年防火墙专项项目市场热度变化趋势

2021-2025年防火墙专项项目价格变化趋势

年份	价格中位数 (¥K)
2021	128
2022	100
2023	85
2024	83
2025	88

2025年防火墙专项项目品牌热度



A word cloud visualization showing the brand popularity for firewall projects in 2025. The brands are represented by text of varying sizes and colors (blue, green, and black) on a light blue background. The largest and most prominent brand is '深信服' (SangxinFu), followed by '华为' (Huawei) and '天融信' (TianRongXin). Other visible brands include '安恒信息' (AnHengXinXi), '亚信安全' (YaxinAnquan), '山石网科' (ShanShiWangKe), '威努特' (Weinute), '迪普科技' (Diputech), '启明星辰' (QimingShichen), '绿盟科技' (LiumengTech), '新华三' (XinhuaSan), '锐捷网络' (RuigeNetwork), '奇安信' (QianAnXin), and '安博通' (AnBotong). '中科网威' (ZhongkeWangWei) is also present at the bottom.

安恒信息 亚信安全 华为 山石网科 威努特 迪普科技 深信服 天融信 启明星辰 绿盟科技 新华三 锐捷网络 奇安信 安博通 中科网威

2025年防火墙专项项目行业热度

生态环境 卫健委 幼儿园 公安 应急管理 非金属矿物 金属冶炼 化工供水住建 监狱 妇幼保健 邮政/物流公司 投资与资产管理 建筑业人社 电力 教育局 市场监管与知识产权 中国电信 检察院 医院 普通教育 高等教育 保险公司 石油石化 财政 科技 中国联通 数据(管理)局 基层医疗 统计 自然资源 船舶制造 采矿 水利水务 证券 中国人民银行 发改 交通运输 设备制造 港口/水运 公路 审计 融媒体 政府办 铁路 法院 党委办

1 热度高位回落

2021—2024年波动上行并于2024年见顶，2025年回落但仍高于2021和2023年水平。

2 四季度是主因

2025年第四季度未延续上年的高位表现，是全年项目热度较上年回落的主要原因。

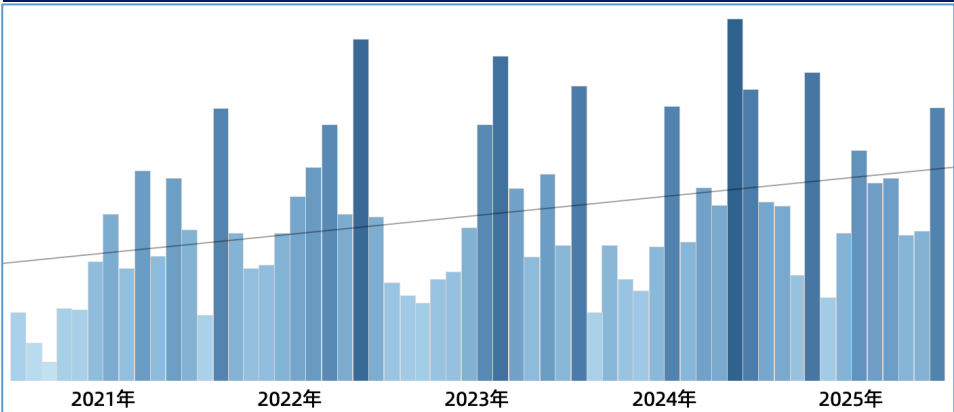
3 品牌参与度高

品牌参与度较高，头部品牌保持较强项目覆盖能力，不同品牌同比表现存在差异。

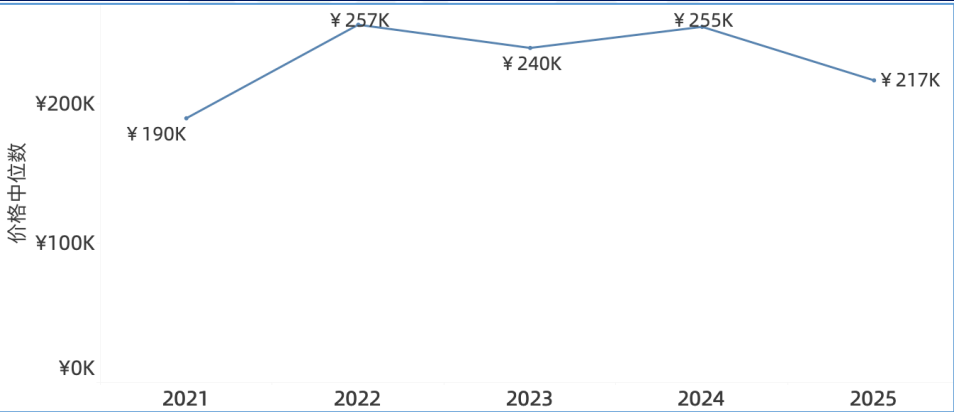
4 行业与价格

银行、高等教育、医院和运营商是主要需求来源；价格中位数较前两年有所回落。

2021-2025年WAF专项项目市场热度变化趋势



2021-2025年WAF专项项目价格变化趋势



2025年WAF专项项目品牌热度



2025年WAF专项项目行业热度



项目热度

安全运营、安全加固、渗透测试、风险评估、应急响应与重保等服务相关项目保持较高活跃度，市场项目热度总体呈上行趋势，但年度内项目释放仍存在一定波动。

行业分布

政府是安全服务采购最集中的行业，占比超过三成；电信运营商、医疗卫生、企业、能源化工和教育等行业亦构成重要需求来源。政府类项目通常围绕政务云、数据资源和公共服务系统开展。

区域对比

广东、北京、浙江、江苏等省份项目数量居前，经济发达地区及重点行业客户集聚区域仍是主要支撑；中西部部分省份也随数字化转型逐步形成新的项目需求。

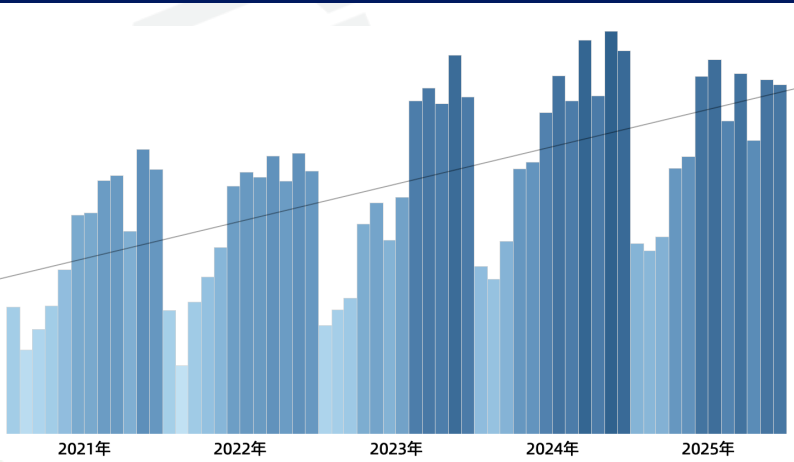
采购价格

项目价格中位数近五年整体呈下行趋势，2025年进一步走低。在客户预算约束、服务供给趋于标准化和市场竞争持续的背景下，仍面临较强价格压力。

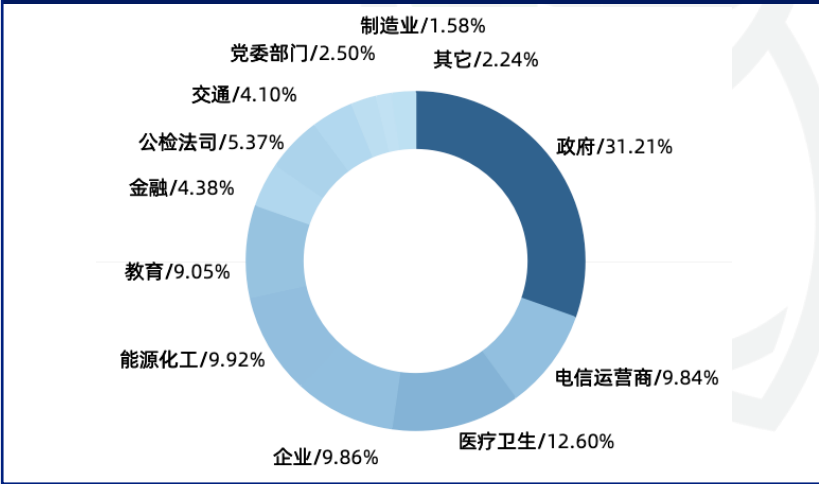
总体判断

呈现“项目需求保持活跃、采购向重点行业和区域集中、项目价格持续承压”的特征。客户对持续性服务仍有稳定需求，但采购决策更趋理性，服务商需以专业能力与交付效率构建优势。

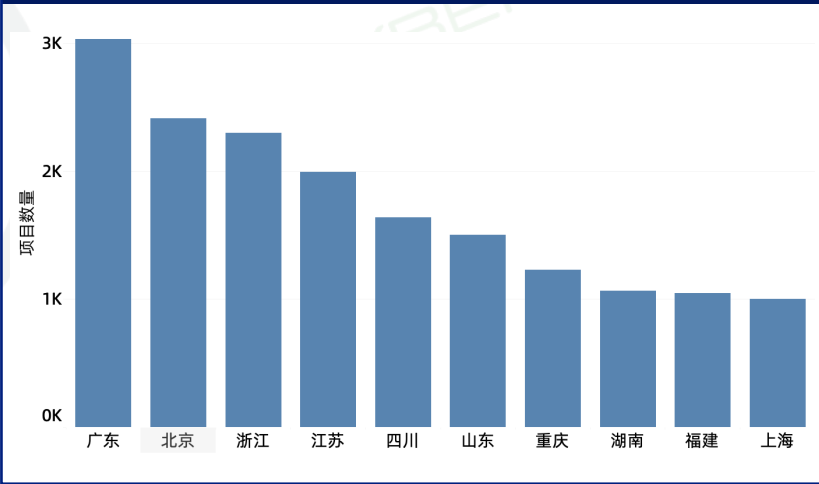
2021-2025安全服务市场项目热度指数（专项）



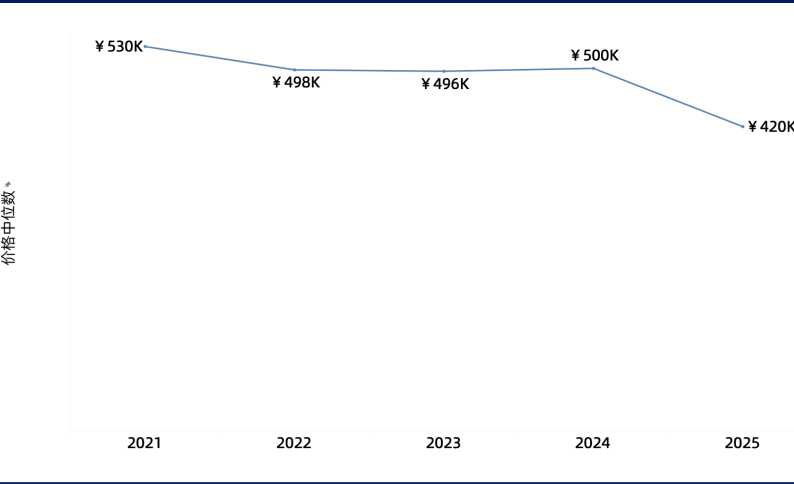
2025年安全服务市场一级行业项目数量占比



2025年安全服务市场TOP10省份项目数量对比



2025年安全服务市场价格趋势（专项）



项目热度

数据安全专项项目在2021—2024年持续提升并于2024年达到阶段高点；2025年热度有所回落，但仍高于2021和2022年水平，需求已由快速扩张转入高位调整阶段。

覆盖方向

涵盖数据安全管理与防护、数据备份与恢复、数据防泄漏、数据分类分级、数据加密与脱敏、数据库防火墙、数据库审计、隐私计算及电子文档安全等方向。

行业分布

政府是采购最集中的行业，占比超过三成；医疗卫生、教育、公检法司、企业和电信运营商亦是重要需求来源，反映监管合规、数据治理及重点数据保护仍是核心驱动。

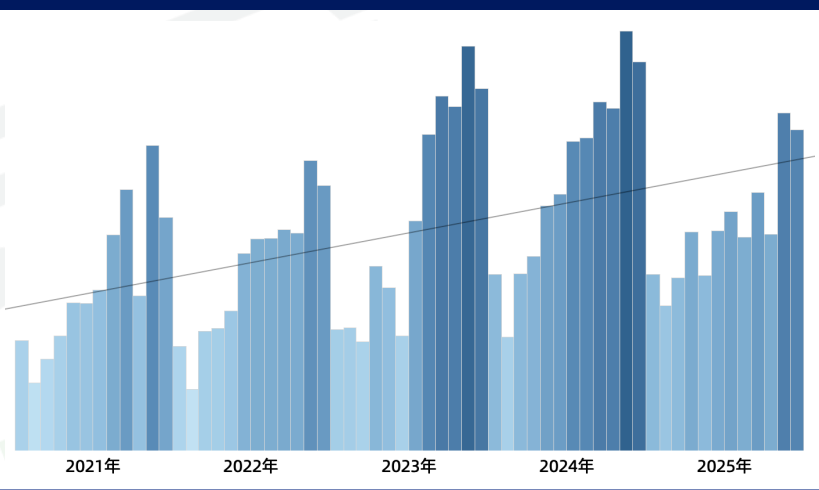
区域与价格

浙江、广东项目数量居前，四川、北京、江苏等省份保持较高活跃度。价格中位数在2023年达到阶段高点后连续回调，2025年进一步下降。

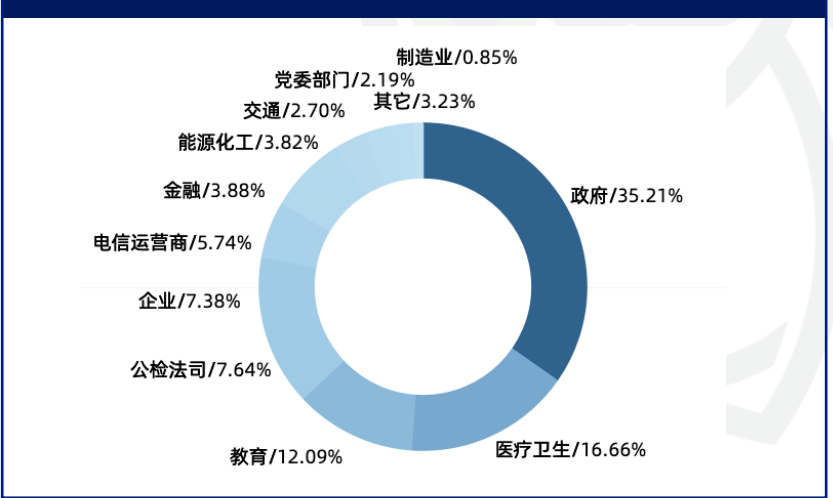
总体判断

呈现“需求热度高位调整、采购向重点行业和区域集中、项目价格回调”的特征。数据安全已由单点合规建设延伸至数据治理、分类分级、数据防护和安全运营等持续性能力建设。

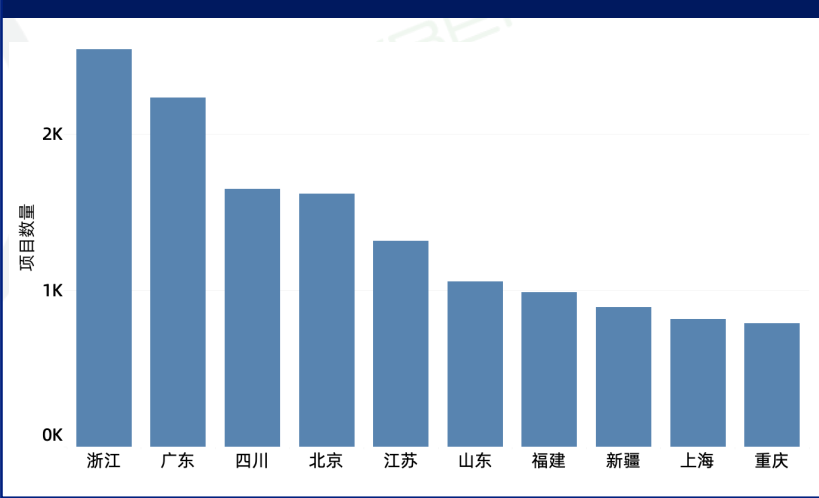
2021-2025数据安全市场项目热度指数（专项）



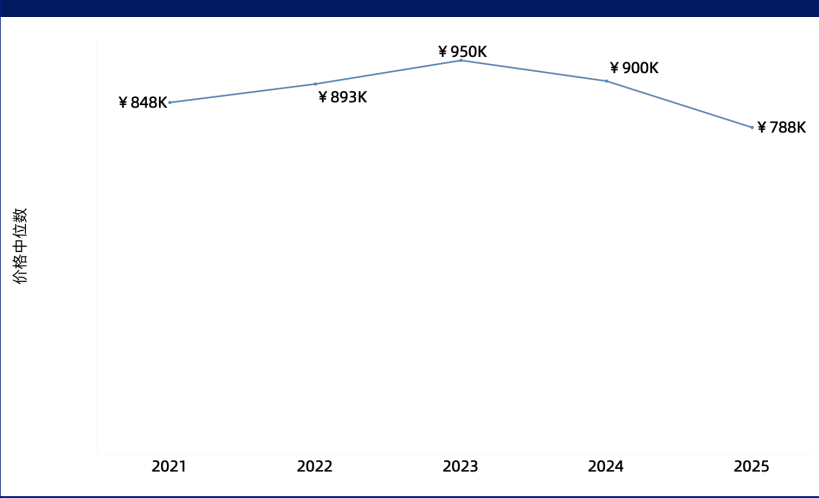
2025年数据安全市场一级行业项目数量占比



2025年数据安全市场TOP10省份项目数量对比



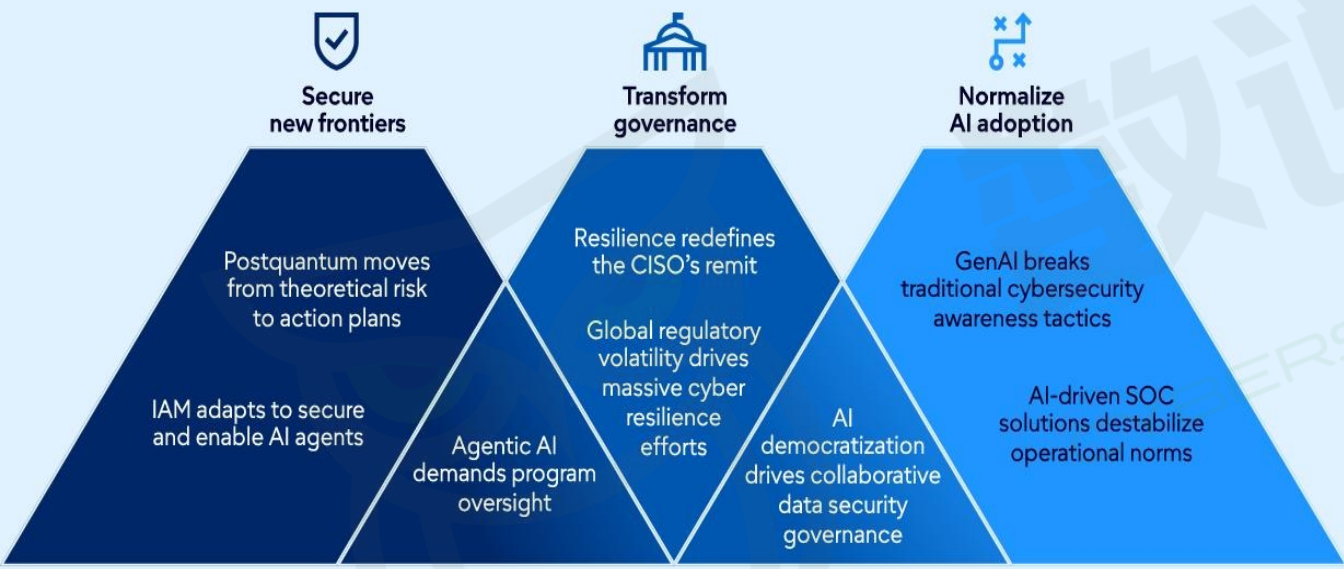
2025年数据安全市场价格趋势（专项）



国际最新动态

伴随代理型 AI 规模化落地催生海量未知攻击面，企业需健全全量 AI 智能体安全管控与应急处置机制，同时顺应全球各地日趋严苛多变的监管要求，通过跨部门协同完善合规体系、夯实网络弹性能力，规避安全违规带来的高管追责、巨额处罚与业务声誉损失。

Top cybersecurity trends for 2026



Source: Gartner
© 2026 Gartner, Inc. and/or its affiliates. All rights reserved.

- 趋势一：代理型AI要求企业必须加强网络安全监管
- 代理型AI正在员工和开发者中广泛普及，由此催生出新的攻击面。无代码/低代码平台与氛围编程进一步加速了这一趋势，导致AI智能体泛滥失控、代码安全漏洞及潜在违规风险。
- Gartner分析师表示：“对于企业而言，虽然AI智能体和自动化工具正变得越来越容易获取，实用性也不断提升，但强有力的治理措施依然必不可少。网络安全领导者必须识别获得批准与未获得批准的AI智能体、对各个智能体实施强力管控，并制定事件响应预案以应对潜在风险。”
- 趋势二：全球监管波动推动网络弹性建设
- 地缘政治格局变迁与全球法规发展使网络安全成为直接影响企业弹性的关键业务风险。随着监管机构日益加大对董事会和高管在合规失误方面的问责力度，企业一旦应对不力，就可能导致巨额罚款、业务流失和不可逆的声誉损害。
- Gartner建议，网络安全领导者应建立法律、业务与采购团队的正式协作机制，明确网络风险责任归属。保持控制框架与公认标准对齐，并妥善解决数据主权问题，将有助于缩小合规差距。

2026 年网络安全六大核心趋势【来源：Gartner】

面对未来量子计算破解传统加密的潜在威胁与 AI 智能体大规模普及带来的身份管控新挑战，企业既要提前布局后量子加密迁移、打造敏捷加密架构抵御“先窃取后解密”攻击，也要重构 IAM 体系，基于风险策略搭建人机统一的自动化身份权限治理机制，同步筑牢底层密码安全与机器身份安全两道防线。

Top cybersecurity trends for 2026



Source: Gartner
© 2026 Gartner, Inc. and/or its affiliates. All rights reserved.

趋势三：将后量子计算纳入行动计划

Gartner预测，到2030年，量子计算的发展将使企业赖以保障数据和系统安全的非对称加密技术失去效用。因此，企业当下就必须采取后量子加密替代方案，防范针对长期敏感数据的“先收集，后解密”式攻击，以此避免潜在的数据泄露、法律责任和经济损失。

Gartner分析师表示：“后量子加密正在重塑网络安全策略，促使企业识别、管理并逐步替换传统加密方法，同时优先保障加密敏捷性。通过及早投入相关技术并优先推进迁移工作，企业能在量子威胁成为现实时有效保护其资产。”

趋势四：针对AI智能体调整身份与访问管理

AI智能体的发展正在给传统身份与访问管理（IAM）策略带来新的挑战，尤其是在身份注册和治理、证书自动化，以及针对机器参与者的策略驱动授权机制等方面。随着自主智能体的日益普及，若未能妥善应对这些问题，访问相关的网络安全事件风险将显著上升。

Gartner建议，企业应采取有针对性的、基于风险的策略，在缺口和风险最大的领域重点投入，同时尽可能利用自动化技术。这对于在以AI为中心的环境中推动创新、确保合规和保护关键资产的安全至关重要。

2026 年网络安全六大核心趋势【来源：Gartner】

AI正在从运营与意识两个层面同时重塑网络安全范式——既要求安全运营中心实现人机协同的弹性进化，也迫使企业告别通用培训、转向针对生成式AI滥用风险的适应性行为治理，核心均在于以"人"为中心重构技术与组织的融合边界。

Top cybersecurity trends for 2026



Source: Gartner
© 2026 Gartner, Inc. and/or its affiliates. All rights reserved.

趋势五：AI驱动的安全运营中心解决方案打破运营常态

在成本优化实践与AI关注度持续提升的双重推动下，AI赋能的安全运营中心（SOC）应运而生，也带来了新的复杂性。尽管这些技术能优化警报分级与调查流程，但也加剧了人员配置压力、增加了技能提升需求，并会导致企业对AI工具成本的考量不断变化。

Gartner分析师表示：“为了充分发挥AI在安全运营中的潜力，网络安全领导者必须将人员放在与技术同等重要的位置上。要想在SOC演进过程中保持弹性，关键在于加强团队能力、将人机协同闭环框架嵌入AI支持的流程中，并且将落地部署与明确的战略目标对齐。”

趋势六：生成式AI打破传统网络安全意识策略

随着生成式AI的加速普及，当前的安全意识策略已无法降低网络安全风险。Gartner于2025年5月至11月对175名员工进行了调研，结果显示逾57%的受访者使用个人生成式AI处理工作事务，33%的受访者承认曾在未经授权的工具中输入敏感信息。

Gartner建议，从通用安全意识培训转向包含AI专项任务的适应性行为与培训计划。通过强化治理、嵌入安全实践和制定授权使用政策，企业将能够有效降低隐私泄露与知识产权流失风险。

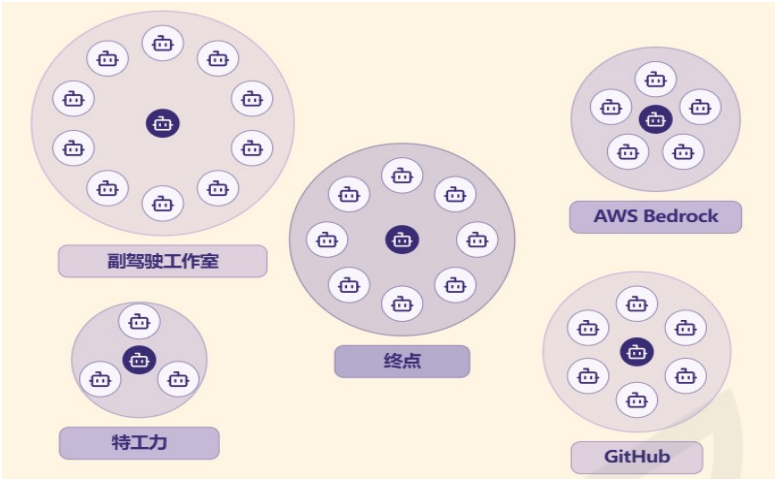
2026 年网络安全六大核心趋势【来源：Gartner】

国外最新技术动态（2020-2026 RSAC创新沙盒十强榜单）

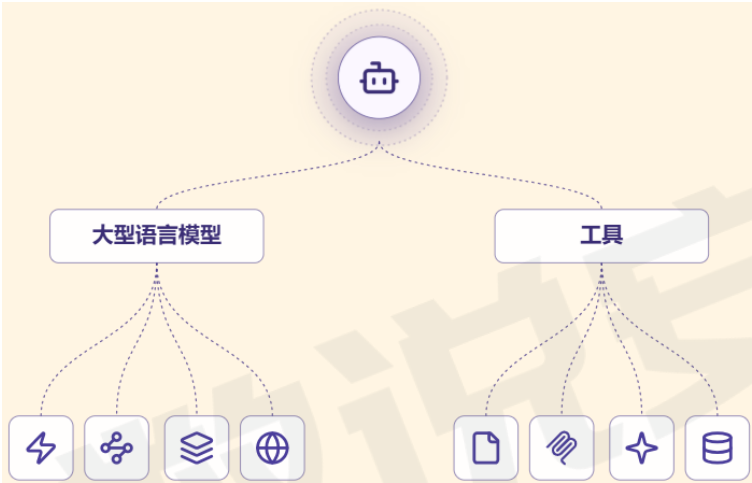


2020	2021	2022	2023	2024	2025	2026
ArmorCode [2019 美国] 应用安全漏洞治理	Abnormal Security [2018 美国] 邮件安全	Araali Networks [2018 美国] 云原生安全 / 威胁管理	AnChain.AI [2018 美国] 区块链数字资产安全	Aembit [2021 美国] 云工作负载 IAM	Aurascape [2024 美国] AI 安全防御	Charm Security [2023 美国] AI 反欺诈
BlindSpot Security [2018 以色列] 影子 IT 资产发现	Apiiro (冠军) [2019 以色列] 软件供应链安全 / 代码安全	BastionZero [2019 美国] 身份 & 访问安全 / 零信任	Astrix Security [2021 以色列] 云应用身份安全	Antimatter [2021 美国] 数据安全	CalypsoAI [2018 美国] AI 安全防御	Clearly AI [2022 美国] AI 安全评审
CloudKnox [2018 美国] 云权限治理	Axis Security [2018 美国] 身份 & 访问安全	Cado Security [2020 英国] 云原生安全 / 取证与响应	Dazz [2021 美国] 云代码安全	Bedrock Security [2022 美国] 数据安全	Command Zero [2022 美国] 零信任基础设施	Crash Override [2023 美国] 软件供应链
DeepSurface Security [2017 美国] 资产漏洞风险评估	Cape Privacy [2018 美国] 数据安全	Cycode [2019 以色列] 软件供应链安全 / 代码安全	Endor Labs [2021 美国] 开源软件供应链安全	Dropzone AI [2023 美国] 自动化安全运营	EQTY Lab AG [2022 瑞士] AI 可治理	Fig Security [2022 美国] 安全运营韧性
Guardian AI [2019 澳大利亚] AI 威胁检测	Deduce [2019 美国] 身份 & 访问安全	Dasera [2019 美国] 数据安全 / 数据治理与运维	Hidden Layer (冠军) [2022 美国] 应用算法模型保护	Harmonic Security [2023 美国] 生成式 AI 安全	Knostic [2023 美国] 数据安全与隐私保护	Geordie AI (冠军) [2025 英国] AI 代理安全
Hasura [2018 印度] 数据访问安全	Open Raven [2019 美国] 数据安全	Lightspin [2020 以色列] 云原生安全 / DevOps 安全	Pangea [2021 美国] API 交付集成的安全即服务	Mitiga [2019 美国] 云调查与响应自动化	Metalware [2023 美国] 固件与供应链安全	Glide Identity [2022 美国] 身份管理
Obsidian Security [2017 美国] SaaS 安全防护	Satori [2019 以色列] 数据安全	Neosec [2020 以色列] API 安全 / XDR	Relyance.AI [2020 美国]隐私合规	P0 Security [2022 美国] IAM 云访问治理	MIND [2024 美国] 数据安全与隐私保护	Humanix [2023 美国] AI 行为安全
Permiso Security [2019 美国] 云合规审计	Strata [2019 美国] 身份 & 访问安全	Sevco Security [2020 美国] 云原生安全 / 资产管理	SafeBase [2020 美国] 安全合规	RAD Security [2022 美国] 云原生异常行为检测 / 响应	ProjectDiscovery (冠军) [2021 美国] 漏洞发现与管理	Realm Labs [2023 美国] AI 模型审计
Secure Code Warrior [2016 澳大利亚] 安全开发培训	Wabbi [2018 美国] 软件供应链安全	Talon Cyber Security (冠军) [2021 以色列] 安全浏览器	Valence Security [2021 以色列] SaaS 安全管理	Reality Defender (冠军) [2021 美国] 深度伪造检测	Smallstep [2018 美国] 零信任基础设施	Token Security [2023 美国] AI 代理身份
Securiti.ai (冠军) [2018 美国] 隐私数据合规	WIZ [2020 以色列] 云安全	Torq [2020 美国] 安全运营无代码安全自动化	Zama [2019 法国] 基于同态加密的隐私计算	VulnCheck [2021 美国] 漏洞优先级排序	Twine Security [2021 美国] 身份安全	ZeroPath [2023 美国] AI 应用

浅金底色为本年度 RSAC 创新沙盒冠军；其余单元格为十强入围企业，信息来源：RSAC 官网（www.rsaconference.com）



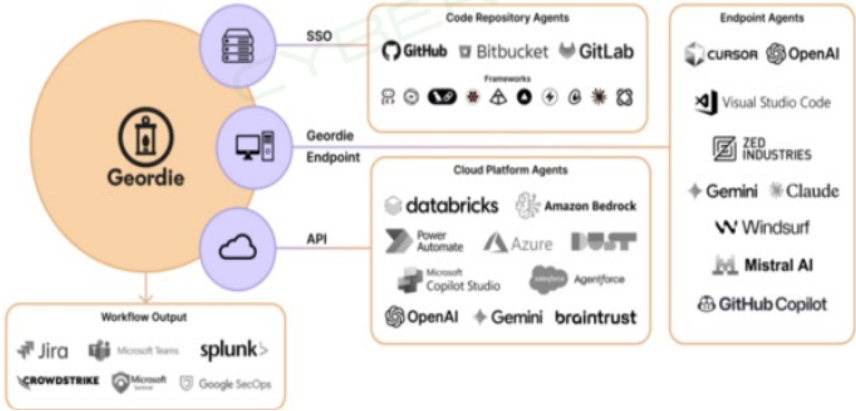
全域 AI 代理自动发现【来源：Geordie官网】



AI 代理完整姿态配置测绘【来源：Geordie官网】



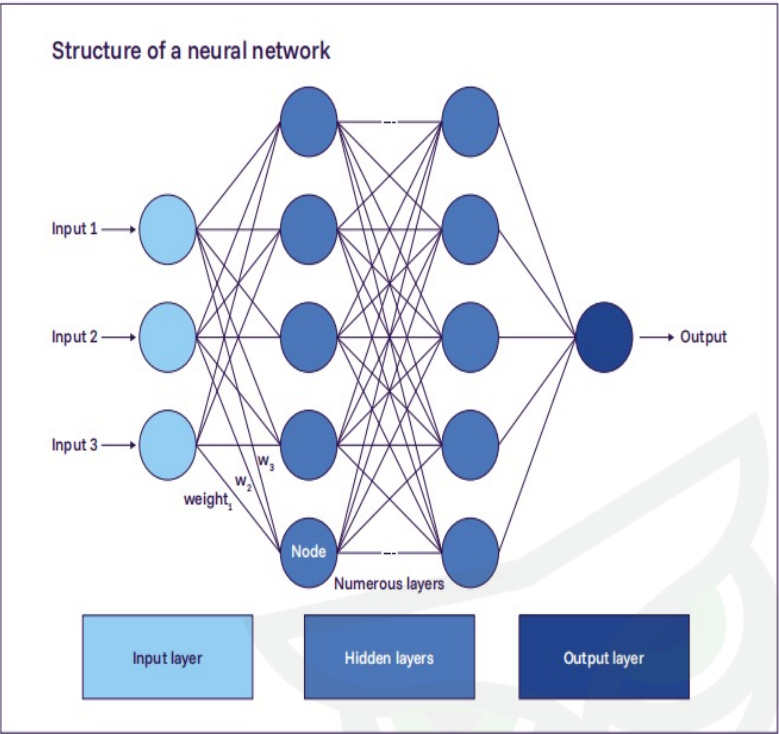
多渠道的漏洞信息【来源：Geordie官网】



Geordie架构图【来源：Geordie官网】

- 作为 2026 RSAC 创新沙盒年度总冠军，英国初创厂商 Geordie AI 主打Agent-native 原生 AI 智能体安全治理方案，凭借差异化技术路线领跑全球 AI 智能体安全赛道。该厂商的胜出并非个案，是全球网络安全行业风向转变的直观信号，标志着安全建设重心从传统数据、身份安全，转向自主化 AI 智能体安全，AI 智能体安全已成为行业确定性刚需。
- Geordie AI 核心能力亮点：
全域 AI 代理自动发现：自动发现并识别企业内所有 AI 智能体，根除“影子 AI”带来的未知风险；
AI 代理完整态势测绘：精准测绘每个 AI 代理的权限、数据交互和行为路径，实现全面风险可视；
多渠道漏洞情报赋能：汇聚并分析多渠道漏洞信息，为 AI 代理提供及时的安全加固依据。

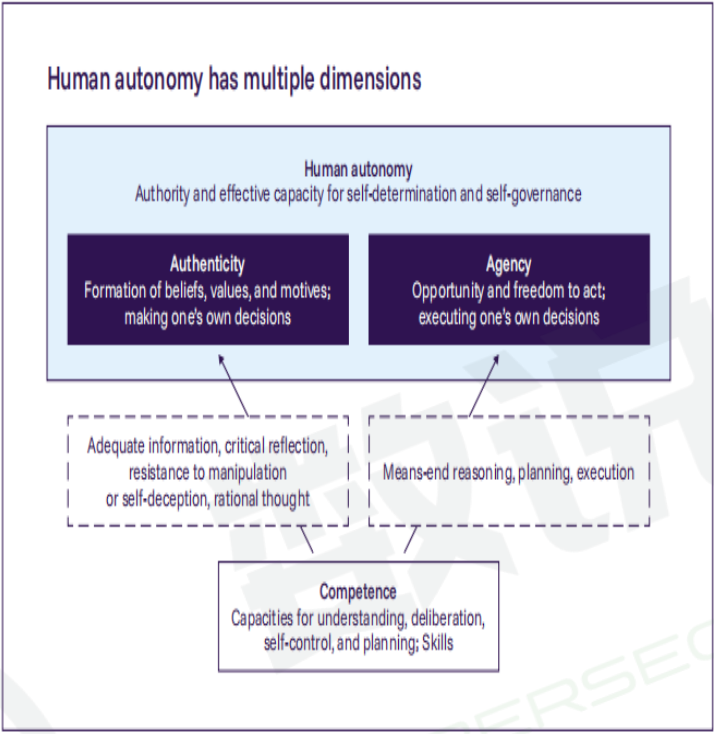
随着企业 AI 智能体逐步脱离人工值守、实现自主跨系统调度数据，传统以“人”为核心的身份认证与数据安全边界已彻底失效，而 Geordie AI 作为首个聚焦 Agent 自主行为内生风险的厂商，其夺冠正是 Gartner 2026 年代理型 AI 趋势与 RSAC 行业风向双向共振的鲜明标志——这预示着网络安全防御范式正从被动的事后补救加速转向对 AI 自主决策过程的实时、主动、全生命周期治理。



神经网络基础结构示意图

【来源：International AI Safety Report 2026】

本图解释通用 AI 底层深度学习核心架构：AI 依靠多层神经元网络处理信息，每层通过权重数值存储学习到的特征；输入原始图文数据，经隐藏层逐层提取抽象特征，最终输出结果。报告以此说明所有大模型的技术底层逻辑，是理解 AI 训练、能力涌现的基础图示，解释为何模型能自主学习海量数据中的规律。

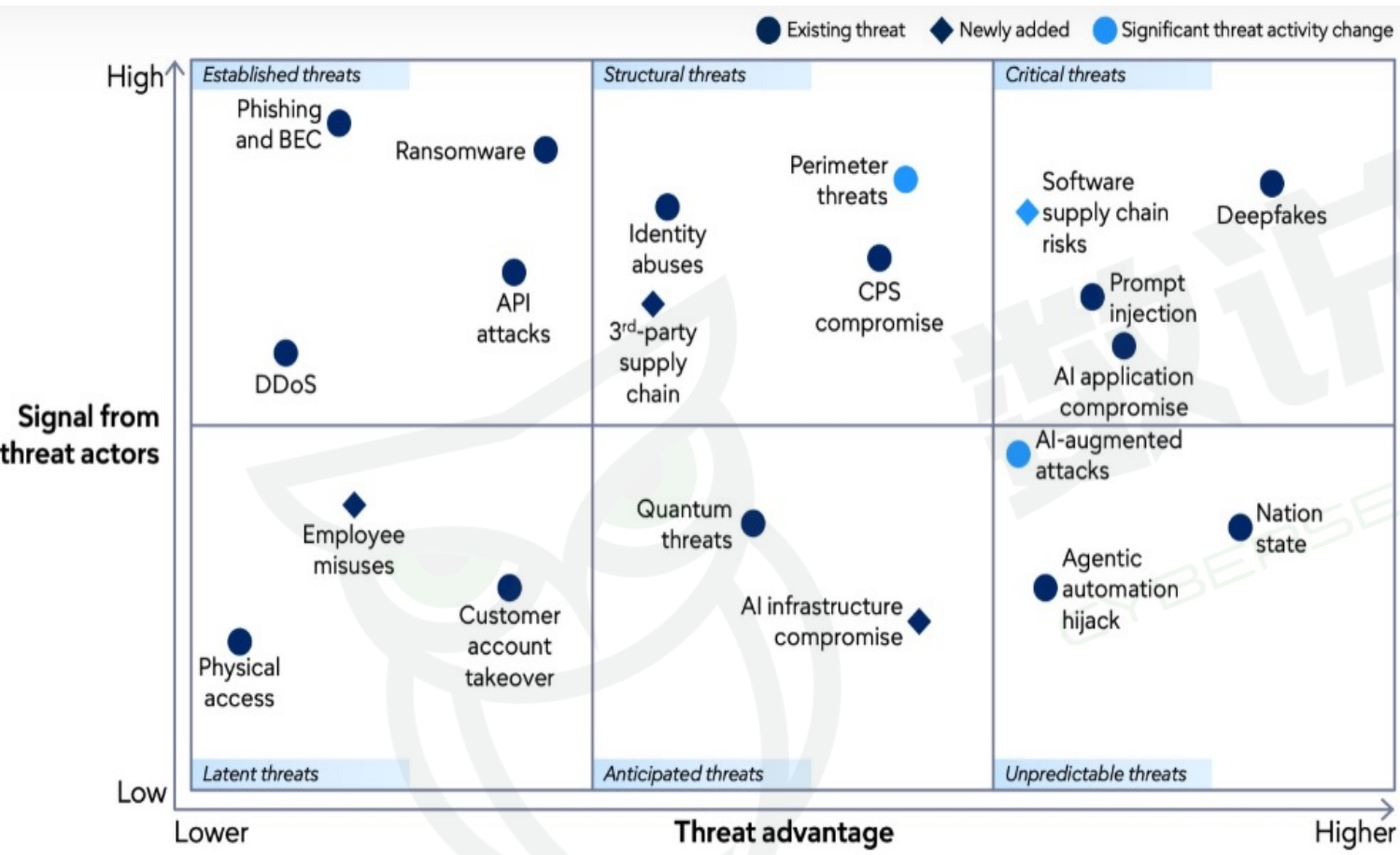


人类自主性、本真性、行动权与胜任力拆解框架示意图

【来源：International AI Safety Report 2026】

顶层总概念「人类自主能力」拆分为本真性、行动权、认知胜任力与规划执行力四个维度，四者相互关联支撑，用于清晰界定 AI 长期使用对人的伤害维度。AI 会削弱批判性思维、催生自动化偏见、造成情感依赖，分别对应破坏思辨能力、扭曲真实判断、降低自主行动意愿三大层面；框架量化区分短期工具依赖与长期心智侵蚀两类危害，支撑劳动力之外的社会宏观风险论证。

- 本报告由蒙特利尔大学 Yoshua Bengio 牵头，30 余国及国际组织专家组成顾问团，承接布莱奇利公园 AI 安全峰会研究任务，聚焦前沿通用 AI 新兴风险，删减 2025 版宽泛社会议题，结合经合组织（OECD）完成 2030 年 AI 发展情景预测，仅提供科学研判、不给出硬性政策建议。
- 第一章阐释通用 AI 定义、深度学习研发全流程，指出推理缩放、模型蒸馏是当下性能提升核心；AI 能力呈现“锯齿化”特征，擅长数理科研却存在幻觉、评估鸿沟等短板，并推演停滞、低速、持续、加速四种 2030 年发展路径，梳理算力、数据等制约因素与研究空白。
- 第二章将 AI 风险划分为三类：一是人为滥用风险，涵盖深度伪造犯罪、舆论操纵、网络攻击、生化武器研发四类现实危害；二是系统故障风险，包含幻觉、代码错误等可靠性问题，及模型欺骗、自主复制等远期失控假说；三是系统性宏观风险，既冲击脑力岗位、拉大全球就业分化，也造成人类批判性思维弱化、情感依赖等自主能力损伤，每类风险均配套实证、更新内容与缓解思路。
- 第三章构建纵深分层风险治理体系，先点明认知不足、信息不对称等四大治理难点，再介绍企业、国际通用风险管理流程与行业安全框架，列举数据筛选、水印等多层技术防护手段；专门探讨开源模型利弊，其降低研发门槛但权重不可撤回、易脱离监管；最后提出社会韧性建设作为兜底方案。
- 报告结尾综合全文，将分层防护、国际协作、缩小 AI 发展差距定为核心治理抓手，梳理待研究议题，配套术语表、参考文献，可供各国、企业作为 AI 安全决策参考。



亟需网络安全管理者加以改进的四大关键威胁
【来源：Gartner】

Gartner于2026年6月2日发布2026—2027年威胁态势分析，指出四类关键威胁中攻击者具有明显优势：AI应用受攻击、深度伪造身份冒充、软件供应链威胁和提示注入。安全团队需据此识别自身防护缺口。

AI应用受攻击：企业自建智能体、第三方集成和内部AI工具扩大了攻击面，薄弱控制可能暴露数据或凭证。应将威胁建模、安全开发、数据分类和运行时监控纳入AI应用生命周期。

深度伪造身份冒充：攻击者可利用逼真的音视频或图像干扰身份核验、在线沟通和招聘流程。防护需结合业务核验、身份认证与检测技术，不能仅依赖深伪识别工具。

软件供应链威胁：开源组件、第三方代码和AI模型等依赖项可能成为攻击入口。应建立资产和组件清单，使用可信仓库，保护构建与发布流程，并监测异常运行行为。

提示注入：恶意输入可能诱导模型泄露信息、越权操作或绕过控制。应结合输入检查、安全测试、运行时防护和异常行为监测，并将测试结果用于持续改进控制措施。

上述四类威胁分别涉及应用、身份、依赖组件和模型交互。企业应根据实际使用场景分层配置防护，并将AI相关检查纳入既有开发、身份和安全运营流程。

《网络安全与人工智能行动计划》解读	
目标一： 规范前沿AI安全使用， 筑牢AI网络风险 准入防线	1、搭建欧盟统一AI网络安全评测体系： 2027年欧盟建成AI安全评估中心，检测大模型合规与滥用风险，为《AI法案》搭建网络风险强制评估技术底座
	2、出台欧洲先进AI安全访问规范： 制定标准蓝图，明确政府、关键设施运营方合规获取前沿模型准入/审计/数据隔离规则，禁止高风险主体调用AI开发攻击工具
	3、建设AI网络安全仿真测试平台 提供免费轻量化AI安全检测工具、合规模板、线上培训，降低中小机构应对AI钓鱼、AI勒索攻击的防护成本
	4、建立AI网络安全风险分级清单： 区分通用大模型、行业高风险AI、轻量开源模型的网络安全管控梯度，统一各成员国风险判定标准，消除跨境合规差异
目标二： 强化全行业 网络韧性， 防御AI 驱动新型 网络攻击	5、关键行业AI防护普及工程： 面向NIS2指令覆盖的能源、交通、医疗、政务等主体，推广AI威胁检测自动化漏洞修复工具，强制完善AI攻击专项应急预案
	6 中小企业安全赋能计划： 提供免费轻量化AI安全检测工具、合规模板、线上培训，降低中小机构应对AI钓鱼、AI勒索攻击的防护成本
	7、开源软件安全韧性专项行动： 针对AI依赖的开源组件开展常态化漏洞扫描、安全补丁快速推送，建立开源AI供应链安全追溯机制，防范开源后门风险
	8、完善AI网络暴力、深度伪造治理技术机制： 统一深度伪造音视频识别技术标准，要求平台嵌入AI鉴伪模块，建立AI虚假信息、自动化骚扰的跨欧盟预警封堵机制
目标三： 培育 欧洲本土AI 网络安全 自主产业生态	9、发起“网络安全AI大挑战赛” 投入专项预算，资助高校、初创企业、产业联盟研发本土AI防御模型、攻击溯源系统、安全评测工具
	10、算力与基础设施自主配套： 联动《云和人工智能法案》，依托欧盟本土AI工厂、主权算力集群，为本土AI安全研发提供低成本算力，减少境外技术依赖
	11、专业人才培养体系建设： 设立AI+网络安全交叉学科专项基金，推动高校开设复合型专业，搭建跨境人才流动合作网络，缓解欧洲安全人才缺口
	12、国际协同与出口管控配套： 推动全球统一AI网络安全治理标准，配套前沿AI模型、高级安全工具出口审查机制，防止先进AI技术流向网络犯罪、敌对势力

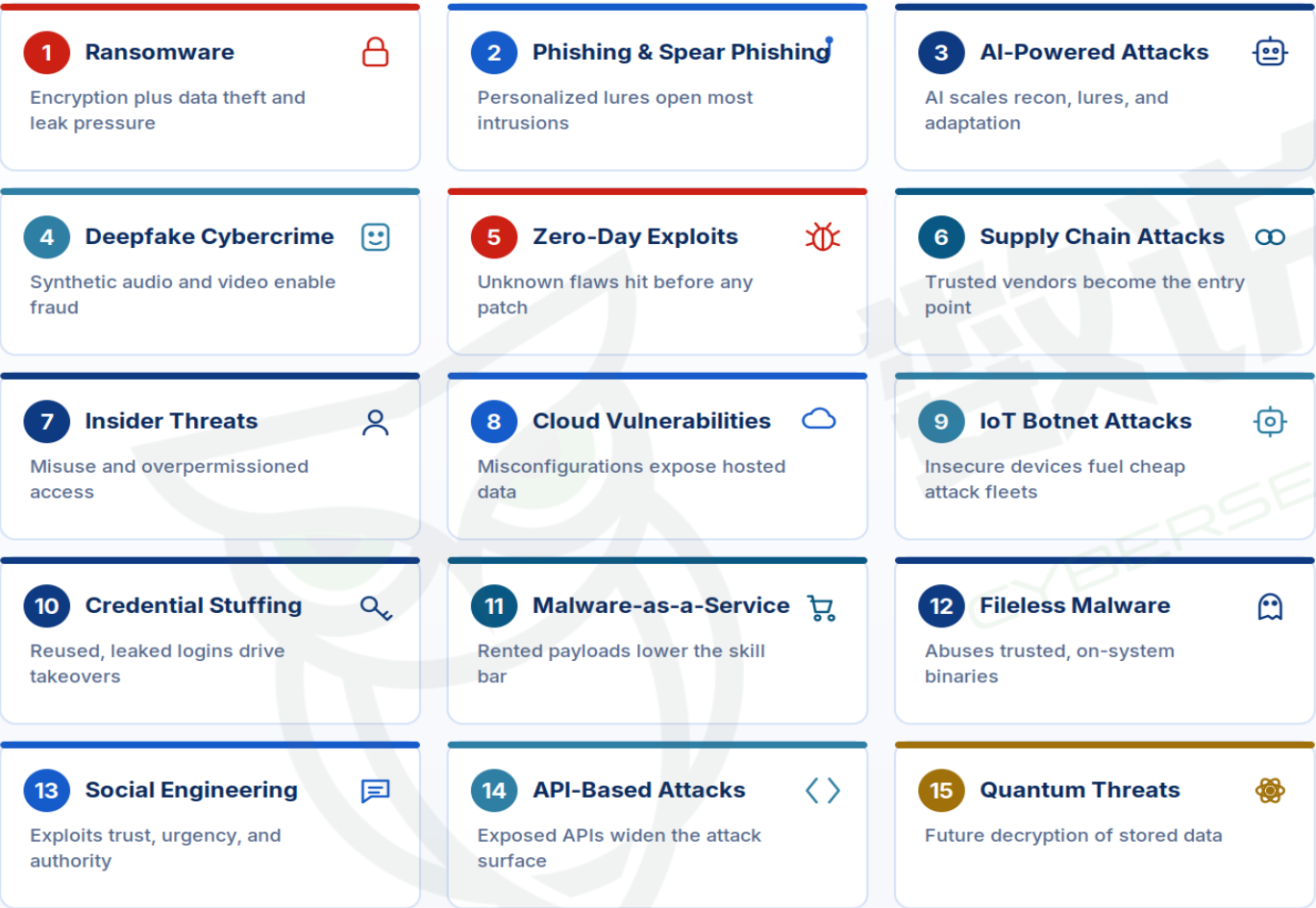
《网络安全与人工智能行动计划》

【来源：<https://digital-strategy.ec.europa.eu/en/library/>】

- 2026年7月，欧盟发布行动计划，应对AI重塑攻防的挑战，确立三大目标：推动AI安全使用、增强韧性、提升本土实力。先进AI正重新定义网络安全边界，既可助力防御，也能被攻击者用于自动化攻击。
- 人工智能正在迅速改变网络安全格局。人工智能可以帮助检测漏洞，防止网络攻击，并加强关键基础设施的保护。同时，恶意行为者也可能利用它自动化攻击、识别弱点，并以前所未有的速度和规模执行网络行动。
- 该行动计划基于欧盟现有的人工智能与网络安全法律框架，提出了协调的方法，帮助成员国、企业和公共机构利用人工智能带来的机遇，同时应对其带来的新风险。它聚焦于三个互补目标：
 - 推广先进人工智能的安全与负责任使用
 - 加强欧盟的网络安全与韧性
 - 提升欧洲人工智能在网络安全领域的能力
- 该行动计划围绕这三大目标展开。一是推动先进AI安全使用，欧盟委员会将牵头建立评估能力（预计2027年运行），强化第三方评估，并制定蓝图推进获取先进AI系统；二是增强网络安全韧性，ENISA将建设安全测试平台，在模拟环境中测试关键行业AI应用并提供指导，同时鼓励利用AI技术加快漏洞修复与应急响应；三是提升本土AI实力，启动“网络安全AI大挑战赛”等平台，联合企业与研究机构研发安全方案，依托AI工厂等基础设施撬动私人资本，推动本土产业扩张。
- 行动计划的出台将对欧盟及全球产生影响。对欧盟而言，该计划是数字主权战略的关键一环，旨在扶持本土AI产业、减少对外依赖，并通过建立统一评估与测试平台确立标准化安全合规体系，降低跨国合规成本，提升整体防御韧性。在全球层面，欧盟再次表明其AI监管态度，或为全球AI治理树立标杆，促使他国完善规范；同时，该计划将重塑全球AI产业格局，培育具有竞争力的本土企业，而在欧盟运营的跨国企业则将面对更高的合规要求与准入门槛。

Latest Cyber Threat Trends Shaping Cybersecurity

Speed, automation, and abuse of trust now define how modern attacks spread



2026 年塑造网络安全格局的 15 项新型网络威胁趋势
CloudSEK官网

cloudsek.com

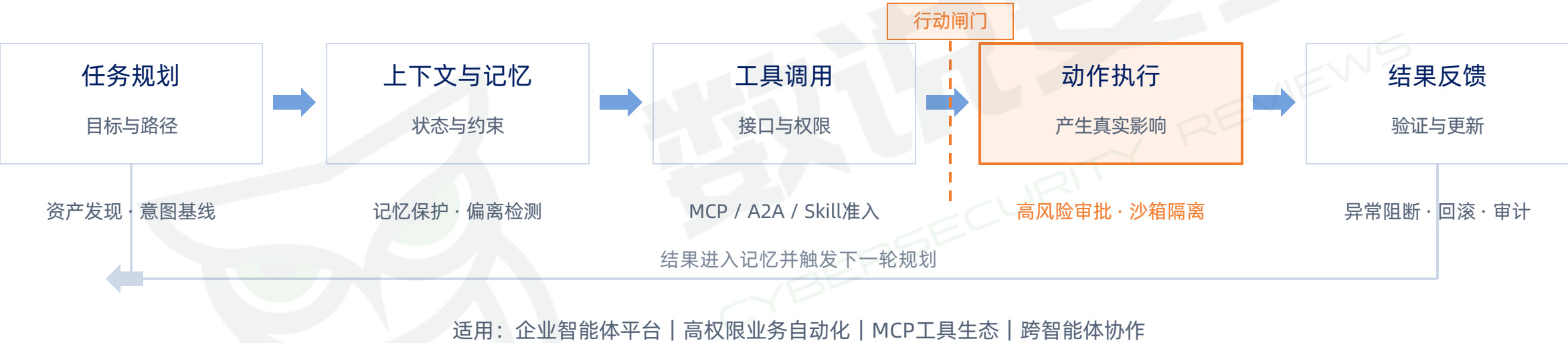
- 随着数字经济全域云化、AI 产业化、物联网规模化及远程办公常态化持续拓宽攻击面，网络威胁呈现自动化、产业化、AI 赋能与跨链路传导特征。本文基于 CloudSEK《2026 年塑造网络安全格局的 15 项新型网络威胁趋势》报告，系统拆解勒索软件、AI 攻击、深度伪造、零日漏洞、供应链渗透、云配置缺陷、API 攻击、量子前置窃取等十五类主流威胁的攻击链路、技术机理与黑产运营模式，梳理出当前防御体系在边界防护、身份管控、人工识别与第三方风险上的四大核心短板。
- 本文系统拆解了勒索软件、AI 攻击、深度伪造、零日漏洞、供应链渗透、云配置缺陷、API 攻击等新型威胁的攻击链路与技术机理，归纳出网络威胁产业化、AI 赋能、重心转向身份信任、跨场景全域传导四大演化特征。核心结论有三：一是传统静态边界防护已失效，人员操作、账号权限及第三方信任成为主要入侵入口，安全建设需转向身份管控、智能反欺诈与人员安全意识运营，多维度融合的智能反钓鱼检测系统是阻断初始入侵的关键支点；二是生成式 AI 与深度伪造大幅降低犯罪门槛，防御体系必须配套 AI 驱动的动态风险检测与实时行为分析，多特征融合评分模型可有效识别 AI 生成钓鱼内容；三是网络风险具有强传导性，需构建零信任动态安全架构，配合微分段隔离、全域监控与第三方持续风险评估，形成闭环防御，并提前布局后量子加密以应对中长期密码安全危机。
- 综上，企业安全建设亟需形成"技术工具 + 人员运营 + 第三方管控 + 长期密码规划"的一体化防护框架，平衡短期应急与长期战略升级，持续适配动态演化的威胁格局。

2026年中国网络安全十大创新方向

AI安全创新从模型防护走向行动、身份、应用、供应链与基础设施



智能体安全正在从模型输入输出防护，转向对任务规划、记忆、工具调用和动作执行的全过程控制。产品需在行动前完成动态判断，对MCP、A2A、Skill、工具权限和高风险操作实施准入、审批、阻断、回滚与审计。



核心能力

- 01 资产与行动链路发现
- 02 MCP/A2A/Skill治理
- 03 高风险动作准入审批
- 04 沙箱隔离、阻断与回滚
- 05 全过程审计

代表厂商（已具备相关产品或能力）



智能体正成为区别于自然人和普通服务账号的新型数字主体。治理需建立“用户—智能体—子智能体—工具”的动态委托链，明确代理对象、任务目的、有效时间、资源范围和责任归属，并支持短时凭证、最小权限与实时撤权。



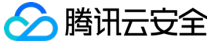
动态委托链：权限随任务创建，随任务完成或风险变化而撤销

核心能力

- 01 智能体唯一身份与责任人
- 02 短时凭证与实时撤销
- 03 任务级最小权限
- 04 权限继承与委托治理
- 05 行动签名与审计

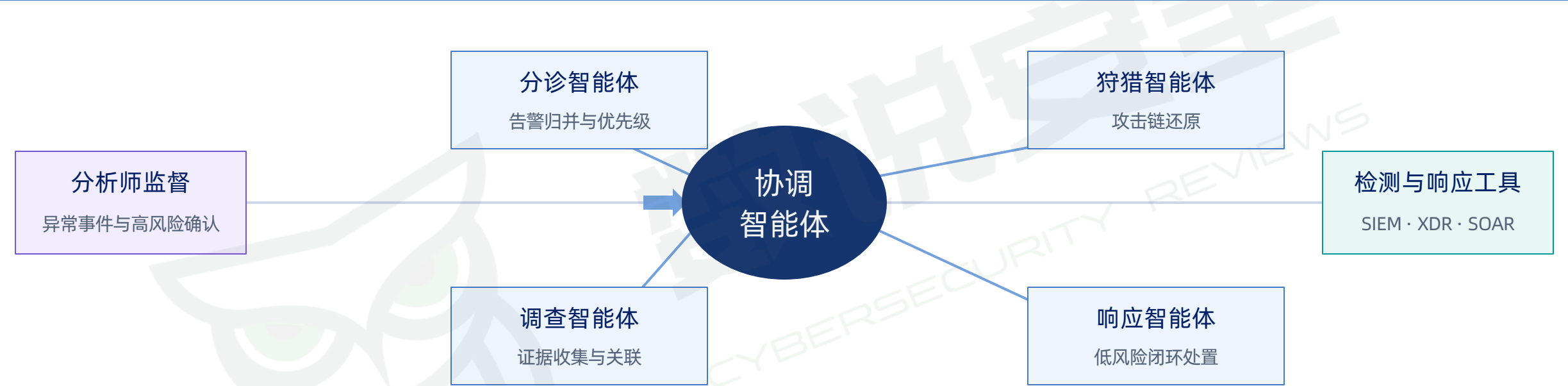
代表厂商（已具备相关产品或能力）







安全运营智能化创新不在于生成告警摘要，而在于多个专业智能体自主完成分诊、取证、关联调查、攻击链还原和部分低风险处置。安全分析师转向监督与异常事件处理，高风险动作仍保留人工确认。



区别于固定剧本：智能体可根据环境动态规划、选工具并调整调查路径

核心能力

- | | | |
|-------------|------------|------------|
| 01 多智能体任务规划 | 02 自动证据收集 | 03 攻击链关联还原 |
| 04 低风险闭环处置 | 05 高风险人工确认 | |

代表厂商（已具备相关产品或能力）



AI正在从辅助生成测试报告，走向理解代码与业务逻辑、自主构建威胁模型、生成测试路径、调用工具验证漏洞、提出修复并复验效果的安全研究系统。价值核心是发现未知缺陷，并通过动态验证降低传统扫描误报。



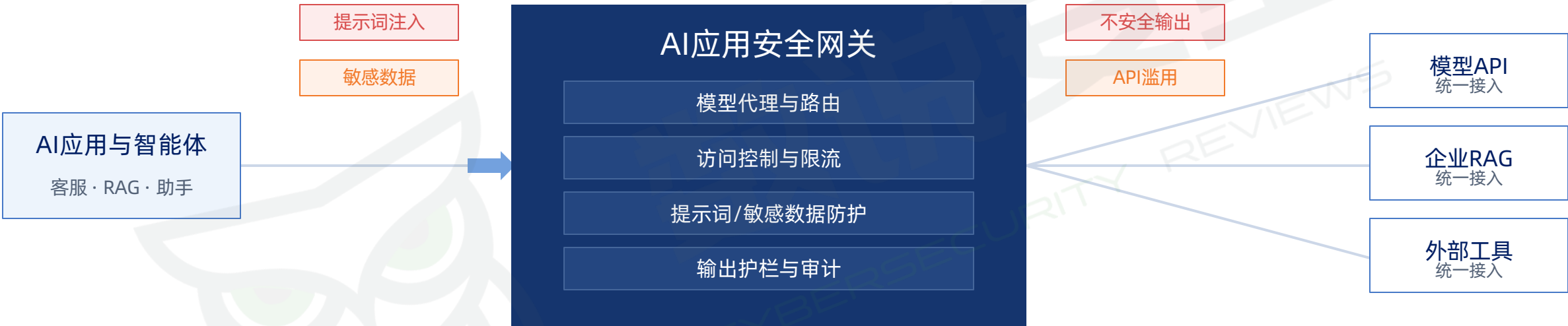
核心能力

- | | | |
|--------------|--------------|------------|
| 01 代码理解与威胁建模 | 02 测试路径与工具调用 | 03 漏洞利用性验证 |
| 04 修复建议与补丁生成 | 05 隔离复验 | |

代表厂商（已具备相关产品或能力）



企业接入多模型、智能体和外部知识后，需要在应用与模型之间建立统一安全控制面。AI安全网关将模型路由、访问控制、提示词攻击检测、敏感数据保护、输出护栏与审计整合到同一入口，并延伸到运行时防护。



统一控制面：在应用与模型之间实时检测、执行策略并留痕

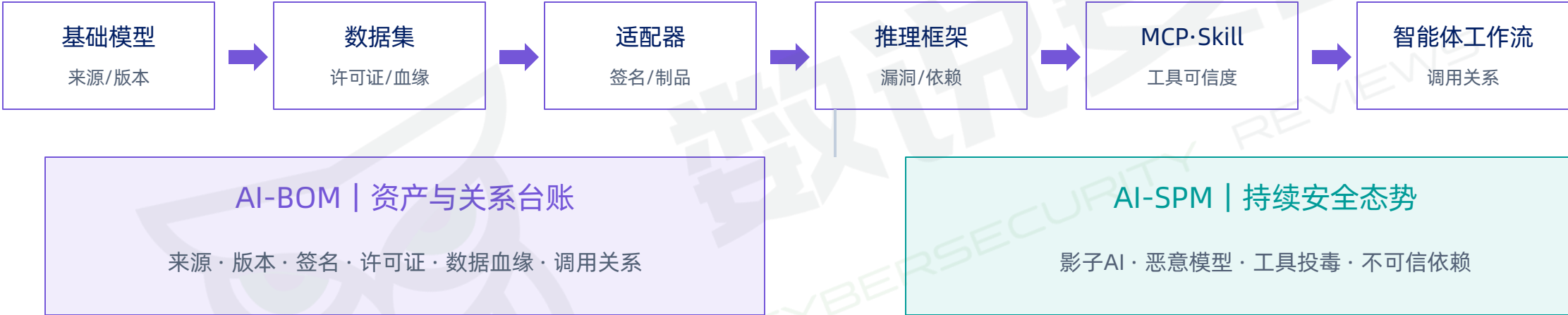
核心能力

- 01 模型代理与智能路由
- 02 提示词注入与越狱防护
- 03 敏感数据识别脱敏
- 04 输出护栏与内容安全
- 05 运行监测与审计

代表厂商（已具备相关产品或能力）



AI系统已扩展到基础模型、适配器、数据集、推理框架、MCP Server、Skill和智能体工作流。AI-BOM与AI-SPM需要持续发现这些资产，记录来源、版本、签名、许可证、血缘和调用关系，并识别影子AI与恶意依赖。



回答“企业正在使用哪些AI组件、从哪里来、是否可信”

核心能力

- 01 AI资产发现与AI-BOM
- 02 来源、签名与数据血缘
- 03 模型与制品扫描
- 04 影子AI持续发现
- 05 AI-SPM风险态势

代表厂商（已具备相关产品或能力）



大模型进入金融、医疗和企业知识库后，保护范围正从存储与传输中的数据延伸到计算使用中的提示词、响应、模型参数和知识。CPU/GPU可信执行环境、内存加密与远程证明，使用户能够验证推理是否运行在可信环境中。



从保护“存储中、传输中”延伸到保护“计算使用中”

核心能力

- | | | |
|------------------|---------------|---------|
| 01 CPU/GPU可信执行环境 | 02 使用中数据与密钥保护 | 03 远程证明 |
| 04 机密容器与推理 | 05 可信密钥释放 | |

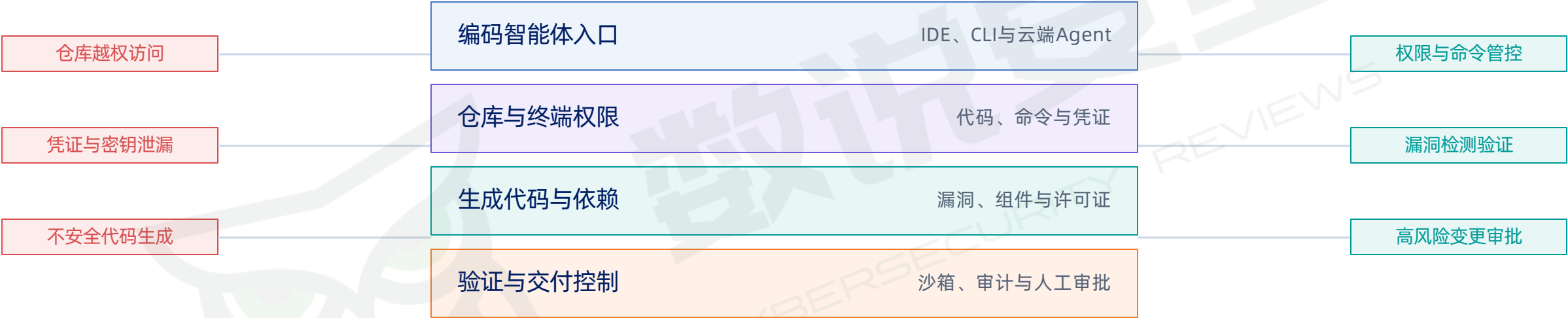
代表厂商（已具备相关产品或能力）

MISUAN
蚂蚁密算

火山引擎

荆华密算

编码智能体正在从代码补全走向读取仓库、执行终端、安装依赖和提交变更。安全控制需要同时治理“智能体如何工作”和“生成代码是否可信”，围绕仓库与终端权限、凭证保护、依赖选择、代码审计、沙箱验证和高风险变更审批形成闭环。



治理对象：编码智能体、代码仓库、终端命令、依赖组件与生成代码

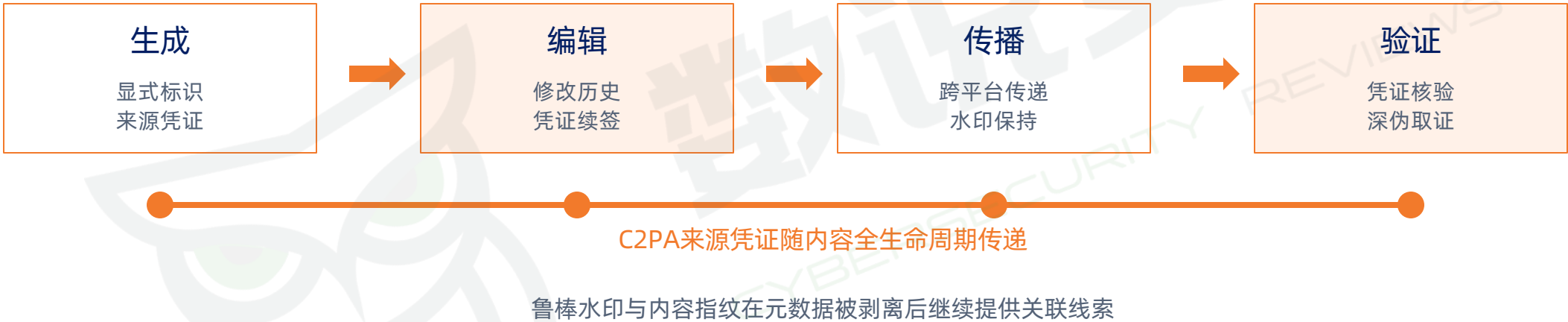
核心能力

- 01 Agent资产与权限管理
- 02 仓库/终端/MCP管控
- 03 生成代码安全审计
- 04 依赖与SBOM治理
- 05 沙箱验证与变更审批

代表厂商（已具备相关产品或能力）



生成内容治理正在从单点深伪检测，走向覆盖生成、编辑、传播和验证的真实性基础设施。显式标识、C2PA来源凭证、鲁棒水印、内容指纹和篡改检测需要协同工作，让内容来源、生成方式与修改历史可验证、可追溯。



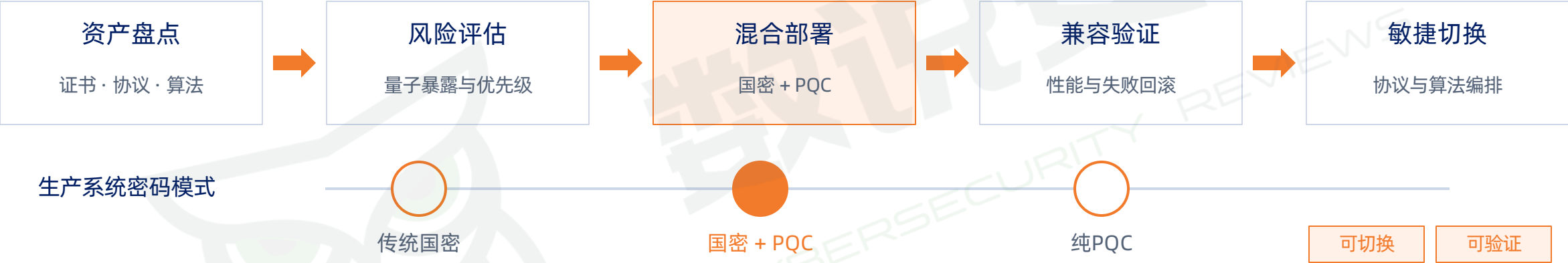
核心能力

- 01 显式标识与C2PA凭证
- 02 鲁棒水印与内容指纹
- 03 编辑传播链追踪
- 04 标识篡改检测
- 05 深伪取证与核验

代表厂商（已具备相关产品或能力）



抗量子密码的创新重点正在由算法研究转向工程迁移。企业需要先发现证书、协议、算法和密钥等密码资产，再开展风险评估、国密与PQC混合部署、协议升级、算法动态切换、兼容性验证和失败回滚。



迁移不是一次替换，而是可盘点、可编排、可验证、可回滚的多年工程

核心能力

01 密码资产发现与CBOM

02 量子风险评估

03 国密+PQC混合部署

04 协议与证书升级

05 算法编排与失败回滚

代表厂商（已具备相关产品或能力）

KOAL 格尔
股票代码：603232

sansec
三未信安

infosec
信安世纪

吉大正元

天融信
TOPSEC

中国网络安全百强和新势力

1、2026年中国网络安全100强评选紧密结合我国网络安全产业特色，以资源支撑力和市场表现力两个关键维度对参选企业进行全面评估。

【资源支撑力】：是企业所依托的人力、资本、技术及销售等关键资源的聚合，这些资源为企业的生存发展提供坚实基础和有力保障，直接影响企业在网络安全领域的稳定性与可持续性。

——资源支撑力的评定维度包括：

- (1) 人力资源：人员数量、人才质量及人才结构等；
- (2) 财务资源：营收规模、企业估值及IPO阶段等；
- (3) 技术资源：专利数量、研发人员占比及研发投入占比等；
- (4) 销售资源：营销网络覆盖度、销售模式及合作伙伴数量等。

【市场表现力】：是企业市场中展现出的综合实力与活力，涵盖品牌影响力、产品竞争力、营销成效、研发能力、服务品质以及经营效益等多个方面，反映企业将自身资源转化为市场竞争优势和经营成果的能力。**相较于2025年，2026年百强评估新增经营现金流、智能化与AI化三项考核，进一步突出经营质量与智能化转型能力。**

——市场表现力的评定维度包括：

- (1) 品牌能力：公众号影响力、官网影响力、企业品牌指数等；
- (2) 营销能力：安全营收和毛利、销售人员、客户覆盖等；
- (3) 产品能力：产品营收、产品数量、产品资质等；
- (4) 研发能力：研发人员、研发投入、研发质量等；
- (5) 服务能力：服务人员、服务收入、服务资质等；
- (6) 经营能力：安全营收增长率、毛利、净利润等；
- (7) 现金流能力：其中针对上市公司增加了经营性现金流净额、回款质量及现金流健康度等；
- (8) 智能化能力：产品与服务的智能化水平、安全运营自动化程度等；
- (9) AI化能力：大模型与AI安全方向的布局与落地，包括AI赋能安全和面向AI的安全防护等。

2、2026年中国网络安全新势力30强，主要针对创新型企业，从资源支撑力、市场表现力和创新成长力三个维度对企业综合能力进行全面评估。

【资源支撑力】和【市场表现力】：同100强评价体系一致。

【创新成长力】：是指创新型企业技术创新、商业模式、业务增长、市场拓展及人才发展等方面展现出的持续发展和进步的能力。"创新"体现了新势力厂商在技术和商业模式等方面的突破与尝试；"成长"则突出了其在业务规模、团队实力及社会影响力等方面的持续发展。

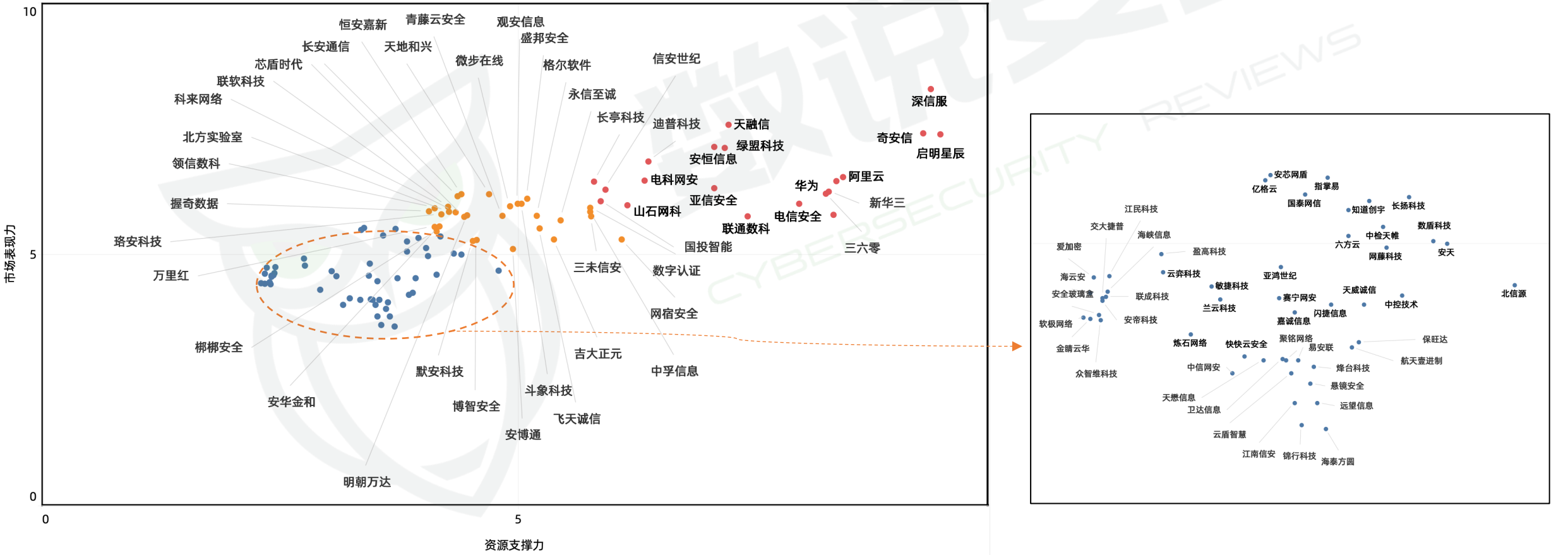
——新势力厂商的评定标准包括：

- (1) 时间规模：成立一般不超过10年，人员不超过300人等；
- (2) 业务创新：产品、技术、商业模式等创新力；
- (3) 成长发展：安全营收复合增长率、人员规模增长率、资本热度等。

2026年中国网络安全100强评选紧密结合我国网络安全产业特色，以资源支撑力和市场表现力两个关键维度对参选企业进行全面评估。

【资源支撑力】：是企业所依托的人力、资本、技术及销售等关键资源的聚合，这些资源为企业的生存发展提供坚实基础和有力保障，直接影响企业在网络安全领域的稳定性与可持续性。

【市场表现力】：是企业 在市场中展现出的综合实力与活力，涵盖品牌影响力、产品竞争力、营销成效、研发能力、服务品质以及经营效益等多个维度，**2026年评选进一步纳入经营现金流、智能化水平与AI化能力三项考核**，反映企业将自身资源转化为市场竞争优势和经营成果的能力。



排名	公司简称	公司全称
1	深信服	深信服科技股份有限公司
2	奇安信	奇安信科技集团股份有限公司
3	启明星辰	启明星辰信息技术集团股份有限公司
4	天融信	天融信科技集团股份有限公司
5	绿盟科技	绿盟科技集团股份有限公司
6	安恒信息	杭州安恒信息技术股份有限公司
7	迪普科技	杭州迪普科技股份有限公司
8	阿里云	阿里云科技有限公司
9	华为	华为技术有限公司
10	新华三	新华三信息安全技术有限公司
11	电信安全	天翼安全科技有限公司
12	腾讯云	腾讯云计算（北京）有限责任公司
13	亚信安全	亚信安全科技股份有限公司
14	电科网安	中电科网络安全科技股份有限公司
15	三六零	三六零安全科技股份有限公司
16	山石网科	山石网科通信技术股份有限公司
17	长亭科技	北京长亭科技有限公司
18	信安世纪	北京信安世纪科技股份有限公司
19	联通数科	联通数字科技有限公司
20	国投智能	国投智能信息科技股份有限公司
21	数字认证	北京数字认证股份有限公司
22	中孚信息	中孚信息股份有限公司
23	三未信安	三未信安科技股份有限公司
24	观安信息	上海观安信息技术股份有限公司
25	微步在线	北京微步在线科技有限公司
26	青藤云安全	北京升鑫网络科技有限公司
27	盛邦安全	远江盛邦安全科技集团股份有限公司
28	永信至诚	永信至诚科技集团股份有限公司
29	斗象科技	上海斗象信息科技有限公司
30	格尔软件	格尔软件股份有限公司
31	天地和兴	北京天地和兴科技有限公司
32	网宿安全	网宿科技股份有限公司
33	飞天诚信	飞天诚信科技股份有限公司
34	吉大正元	长春吉大正元信息技术股份有限公司

排名	公司简称	公司全称
35	恒安嘉新	恒安嘉新（北京）科技股份公司
36	长安通信	长安通信科技有限责任公司
37	安博通	北京安博通科技股份有限公司
38	芯盾时代	北京芯盾时代科技有限公司
39	联软科技	深圳市联软科技股份有限公司
40	明朝万达	北京明朝万达科技股份有限公司
41	科来网络	科来网络技术股份有限公司
42	北方实验室	北方实验室（沈阳）股份有限公司
43	领信数科	领信数科信息技术有限公司
44	珞安科技	北京珞安科技有限责任公司
45	握奇数据	北京握奇数据股份有限公司
46	博智安全	博智安全科技股份有限公司
47	默安科技	杭州默安科技有限公司
48	安华金和	北京安华金和科技有限公司
49	万里红	北京万里红科技有限公司
50	梆梆安全	北京梆梆安全科技有限公司
51	长扬科技	长扬科技（北京）股份有限公司
52	北信源	北京北信源软件股份有限公司
53	安天	安天科技集团股份有限公司
54	数盾科技	数盾信息科技股份有限公司
55	知道创宇	北京知道创宇信息技术股份有限公司
56	指掌易	北京指掌易科技有限公司
57	中检天帷	中检集团天帷信息技术（安徽）股份有限公司
58	竹云	深圳竹云科技股份有限公司
59	网藤科技	北京网藤科技有限公司
60	国泰网信	北京国泰网信科技股份有限公司
61	保旺达	江苏保旺达软件技术有限公司
62	赛宁网安	南京赛宁信息技术有限公司
63	六方云	北京六方云信息技术有限公司
64	天威诚信	北京天威诚信电子商务服务有限公司
65	闪捷信息	闪捷信息科技有限公司
66	中控技术	中控技术股份有限公司
67	亚鸿世纪	北京亚鸿世纪科技发展有限公司
68	亿格云	杭州亿格云科技有限公司

排名	公司简称	公司全称
69	安芯网盾	安芯网盾（北京）科技有限公司
70	悬镜安全	北京安普诺信息技术有限公司
71	锦行科技	广州锦行网络科技有限公司
72	海泰方圆	北京海泰方圆科技股份有限公司
73	聚铭网络	南京聚铭网络科技有限公司
74	云盾智慧	云盾智慧安全科技有限公司
75	海云安	深圳海云安网络安全技术有限公司
76	航天壹进制	航天壹进制（江苏）信息科技有限公司
77	联成科技	南京联成科技发展股份有限公司
78	易安联	江苏易安联网络技术有限公司
79	江民科技	北京江民新技术有限公司
80	炼石网络	北京炼石网络技术有限公司
81	快快云安全	厦门快快网络科技有限公司
82	盈高科技	杭州盈高科技有限公司
83	中信网安	福建中信网安信息科技有限公司
84	海峡信息	福建省海峡信息技术有限公司
85	天懋信息	广州天懋信息系统股份有限公司
86	江南信安	江南信安（北京）科技有限公司
87	兰云科技	北京兰云科技有限公司
88	安帝科技	北京安帝科技有限公司
89	卫达信息	北京卫达信息技术有限公司
90	嘉诚信息	长春嘉诚信息技术股份有限公司
91	烽台科技	烽台科技（北京）有限公司
92	云弈科技	北京云弈科技有限公司
93	远望信息	浙江远望信息股份有限公司
94	敏捷科技	江苏敏捷科技股份有限公司
95	爱加密	北京智游网安科技有限公司
96	众智维科技	南京众智维信息科技有限公司
97	安全玻璃盒	杭州孝道科技有限公司
98	交大捷普	西安交大捷普网络科技有限公司
99	金睛云华	北京金睛云华科技有限公司
100	软极网络	软极网络技术（北京）有限公司

序号	公司简称	公司中文全称
1	安全玻璃盒	杭州孝道科技有限公司
2	安泉数智	杭州安泉数智科技有限公司
3	持安科技	北京持安科技有限公司
4	DarkNavy	达酷诺威（上海）科技有限公司
5	方向标	北京方向标信息科技有限公司
6	观成科技	北京观成科技有限公司
7	硅基守望	北京硅基守望科技有限公司
8	画方科技	北京融汇画方科技有限公司
9	慧天云海	济南慧天云海信息技术有限公司
10	火山引擎	北京火山引擎科技有限公司
11	景安云信	北京景安云信科技有限公司
12	君同未来	杭州君同未来科技有限责任公司
13	荆华密算	荆华密算（北京）科技有限公司
14	蚂蚁密算	浙江蚂蚁密算科技有限公司
15	墨菲安全	墨菲未来科技（北京）有限公司
16	瑞莱智慧	北京瑞莱智慧科技有限公司
17	睿安致远	睿安致远（北京）信息技术有限公司
18	深依科技	深圳市深依信息科技有限公司
19	矢安科技	上海矢安科技有限公司
20	石犀科技	深圳市石犀科技有限公司
21	数安行	北京数安行科技有限公司
22	思而听	思而听（山东）网络科技有限公司
23	碳泽信息	上海碳泽信息科技有限公司
24	御安信息	浙江御安信息技术有限公司
25	元支点	北京元支点信息安全技术有限公司
26	云祺科技	成都云祺科技有限公司
27	紫讯	紫讯技术（福建）股份有限公司
28	知其安	北京知其安科技有限公司
29	中科睿鉴	中科睿鉴科技有限公司
30	众智维科技	南京众智维信息科技有限公司

*按企业简称首字母排序，排名不分先后



中国网络安全二级市场分析

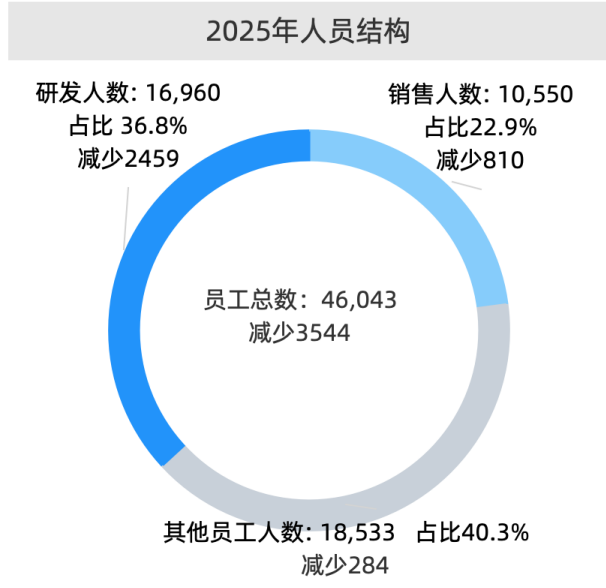
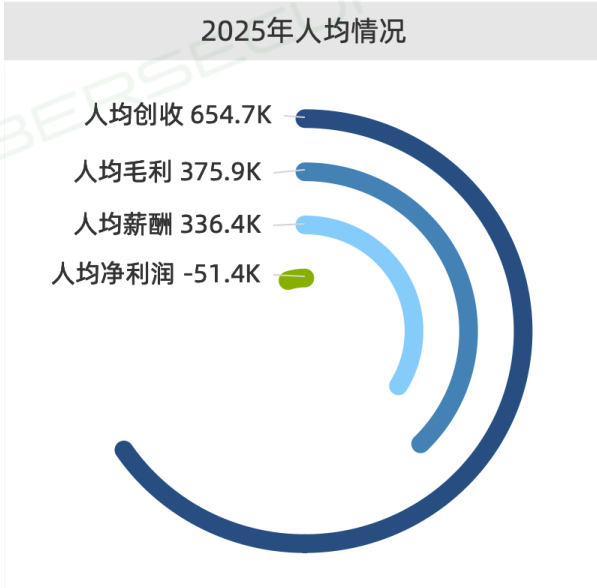
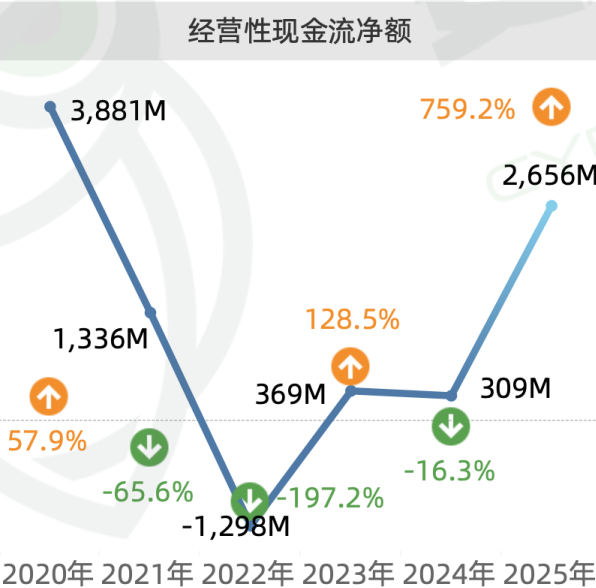
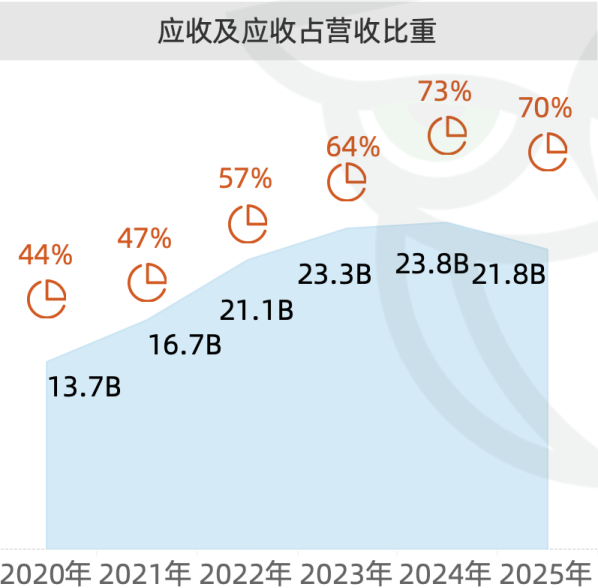
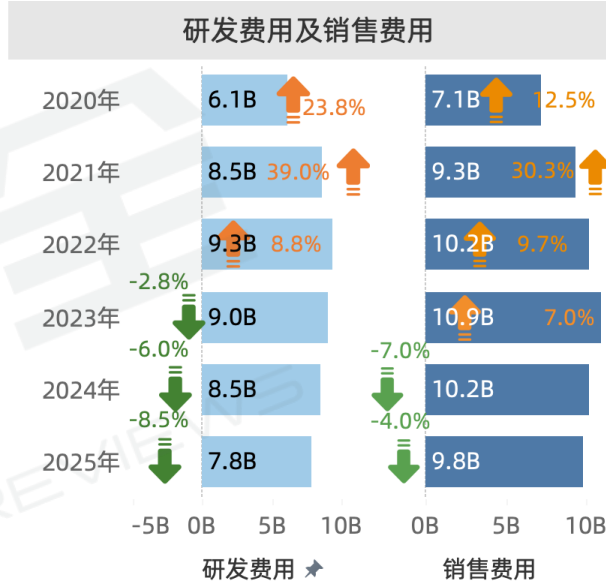
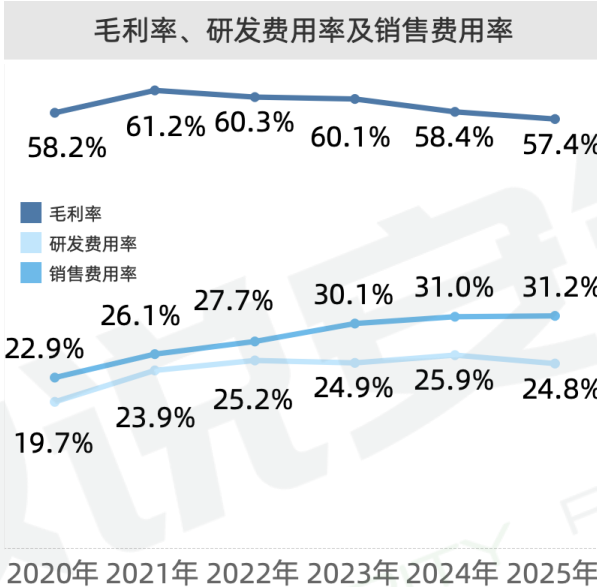
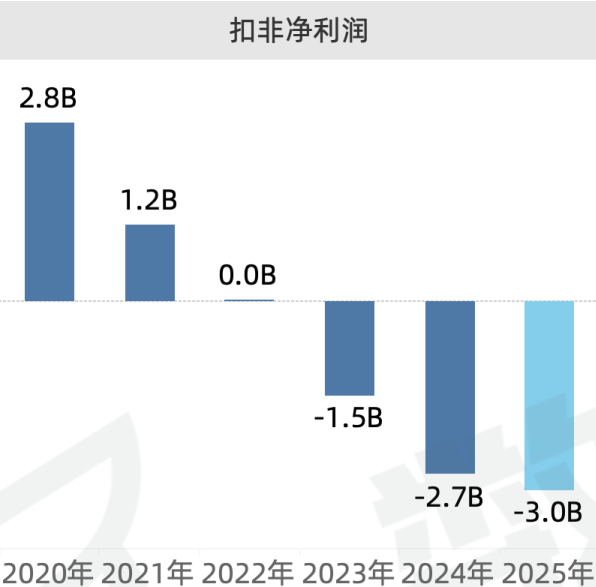
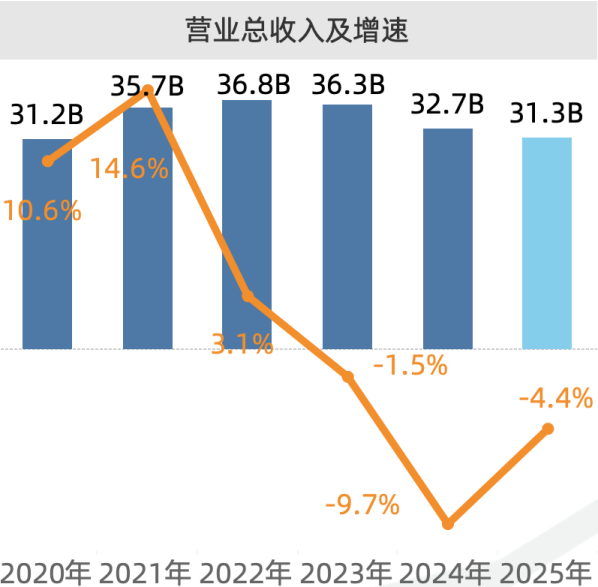
上市公司横向对比分析

本章节选取19家网络安全业务具有较强代表性的上市公司作为经营统计样本，通过比较其收入、利润、人员与现金流，观察行业经营变化。样本包括安全业务占比较高的专业厂商，以及深信服等同时经营云计算及IT基础设施业务的公司。总营收与安全业务收入分别列示，不以“安全收入占比超过50%”作为所有样本公司的统一条件。

说明：亚信安全由于并购亚信科技，收入结构和人员结构发生较大变化，因此不再纳入采样清单。

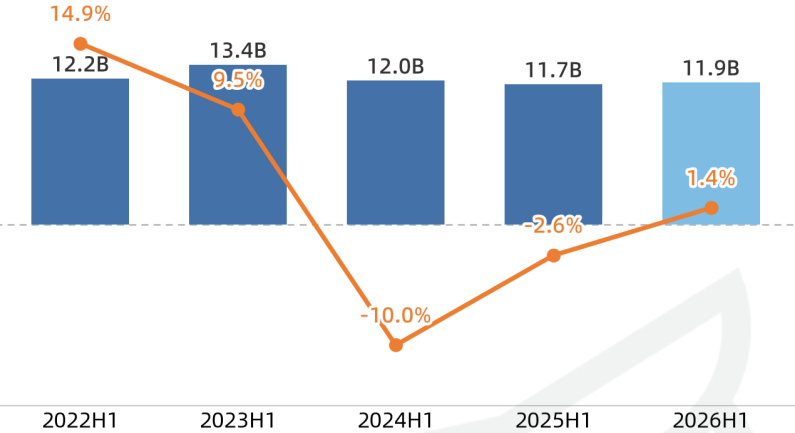


2025年网安上市公司整体经营数据

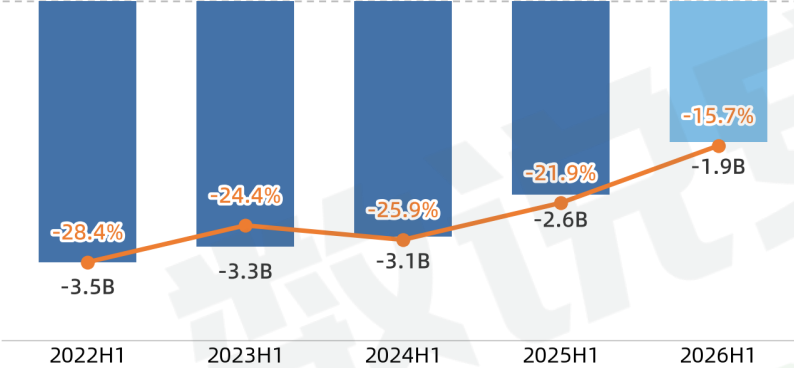


2026H1网安上市公司整体经营数据

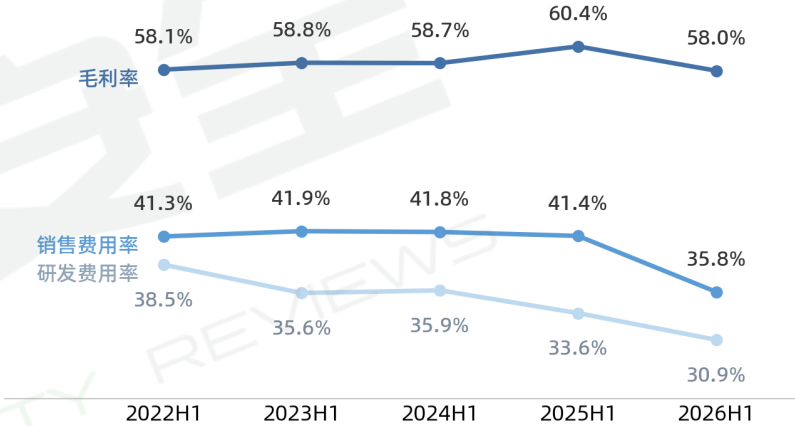
营业总收入及增速



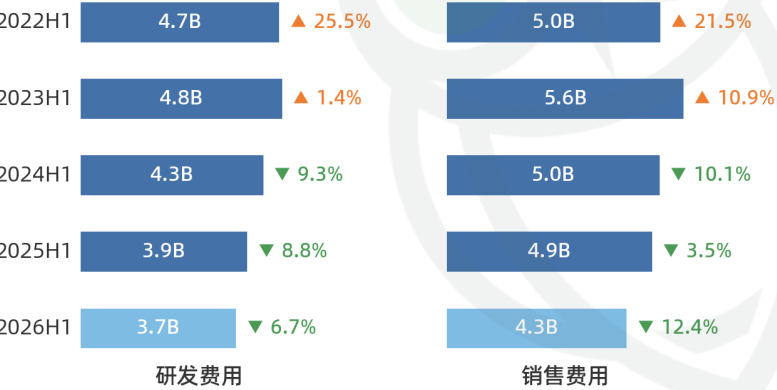
扣非净利润及扣非净利润率



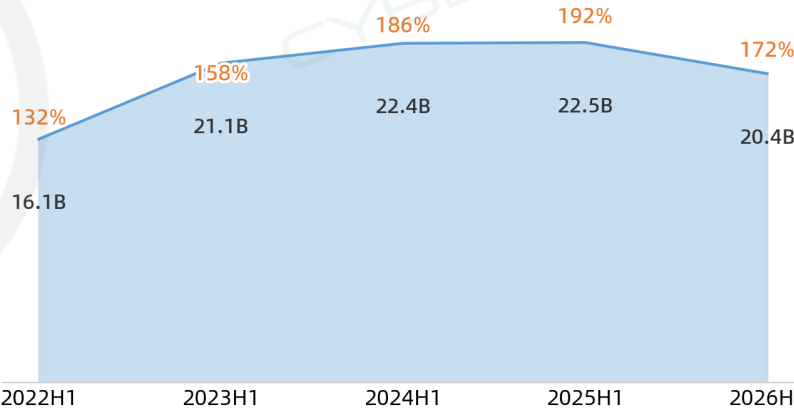
毛利率、研发费用率及销售费用率



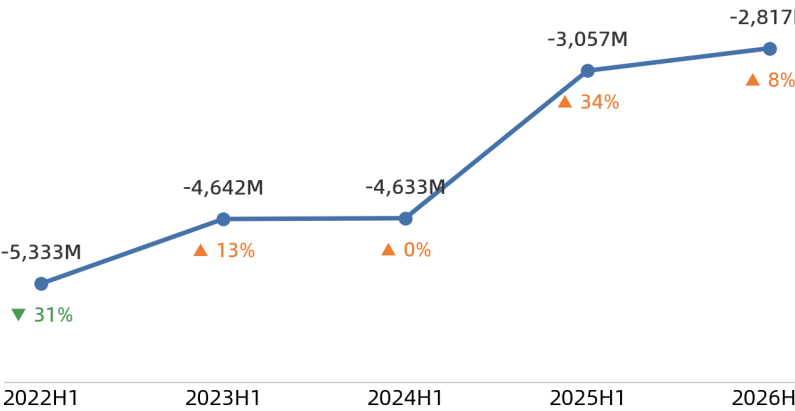
研发费用及销售费用



应收及应收占营收比重



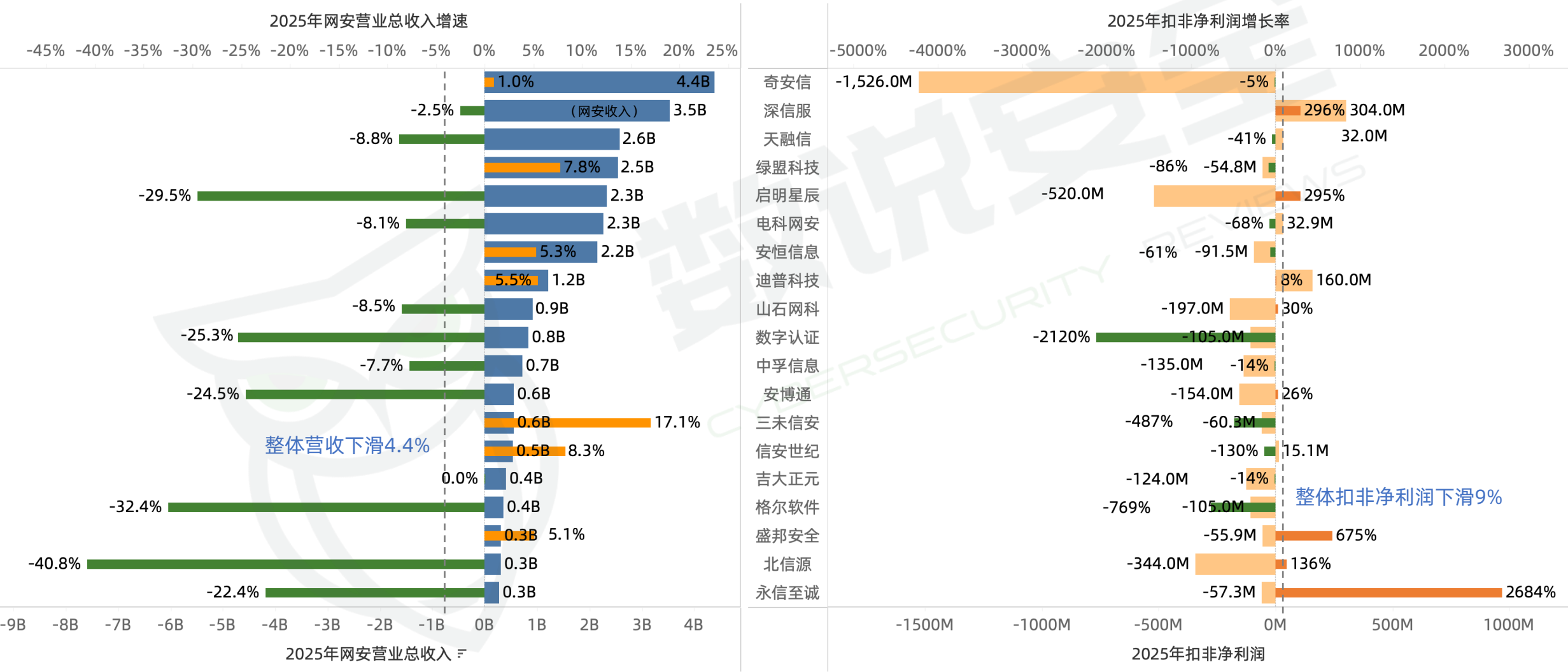
经营性现金流净额



行业整体营收降幅收窄至4.4%，扣非净利润亏损扩大至-29.9亿

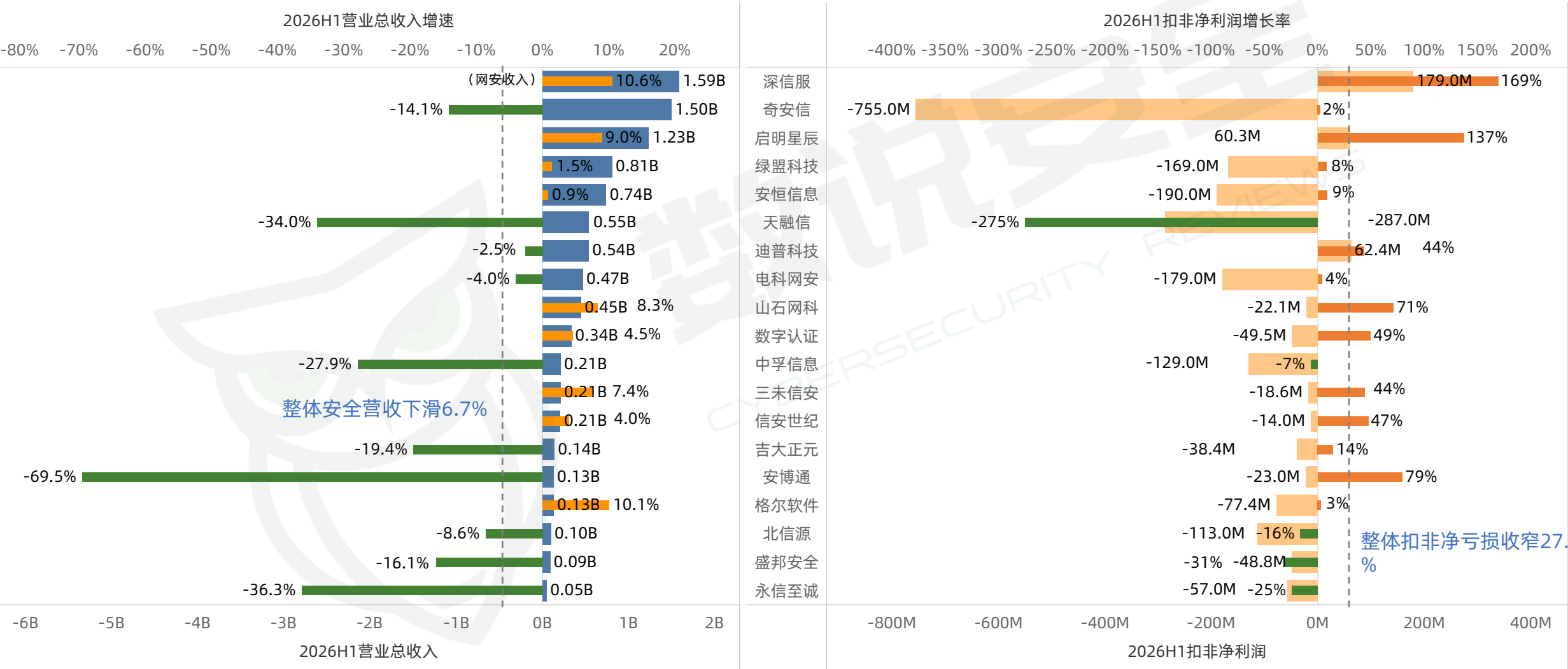


2025 年网安上市公司整体营收313亿，同比下滑4.4%，降幅较去年的9.7%明显收窄；其中安全营收 268亿，同比下滑 7.11%；19家中8家收入正增长，较去年增加3家。整体扣非净利润-29.9亿，亏损继续扩大9.05%，扣非为正的由公司由 7 家降至 5 家；其中奇安信、启明星辰两家合计亏损 20.46 亿，占整体扣非亏损的 68.5%。

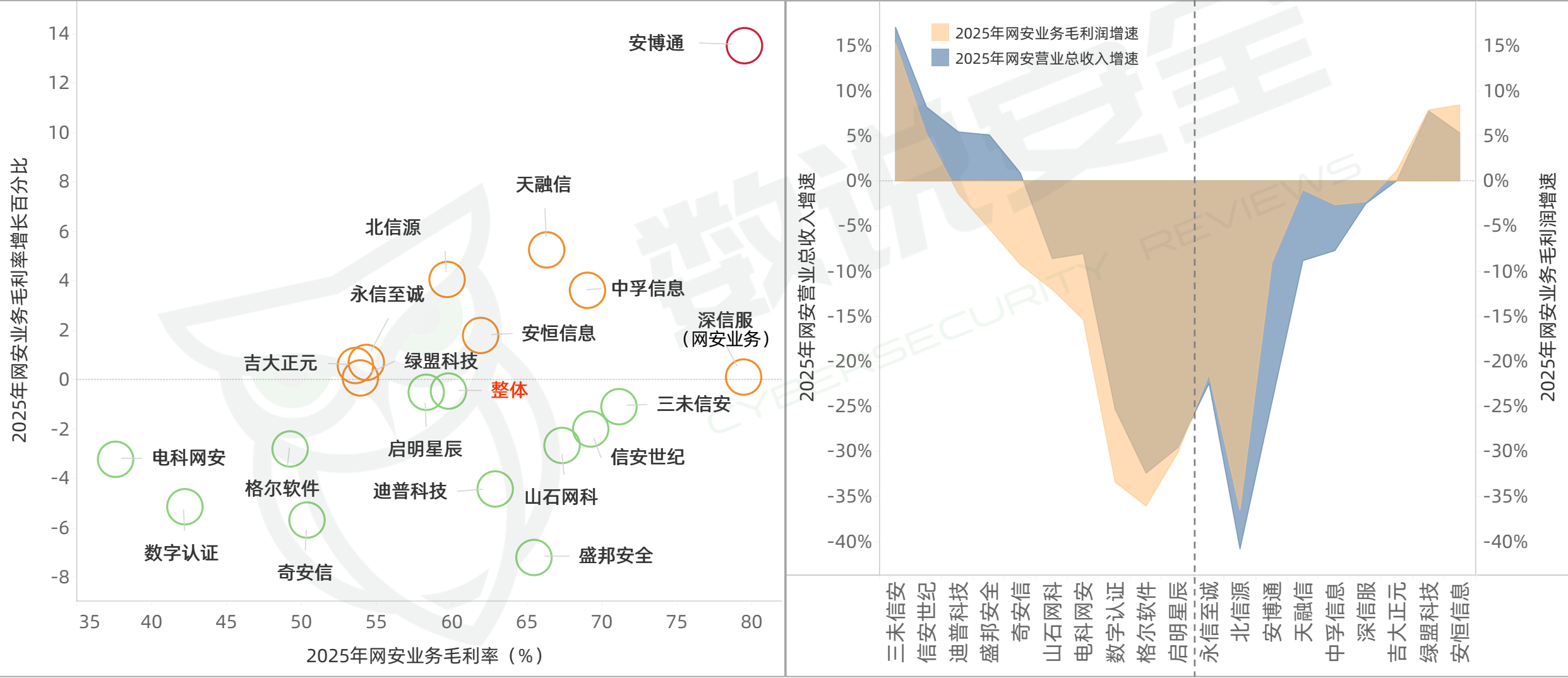


2026 年H1安全营收下滑6.7%，扣非净利润亏损收窄27.4%

2026 年上半年网安上市公司整体安全营收 94.84 亿，同比下滑 6.66%，降幅较上年同期的 5.33% 扩大；19家中9家收入正增长，较上年同期增加1家，深信服以10.6% 领跑，安博通因高基数下滑 69.5% 垫底。整体扣非净利润-18.69亿，亏损收窄27.35%；奇安信、天融信合计亏损 10.42 亿，占整体扣非亏损的 55.8%。



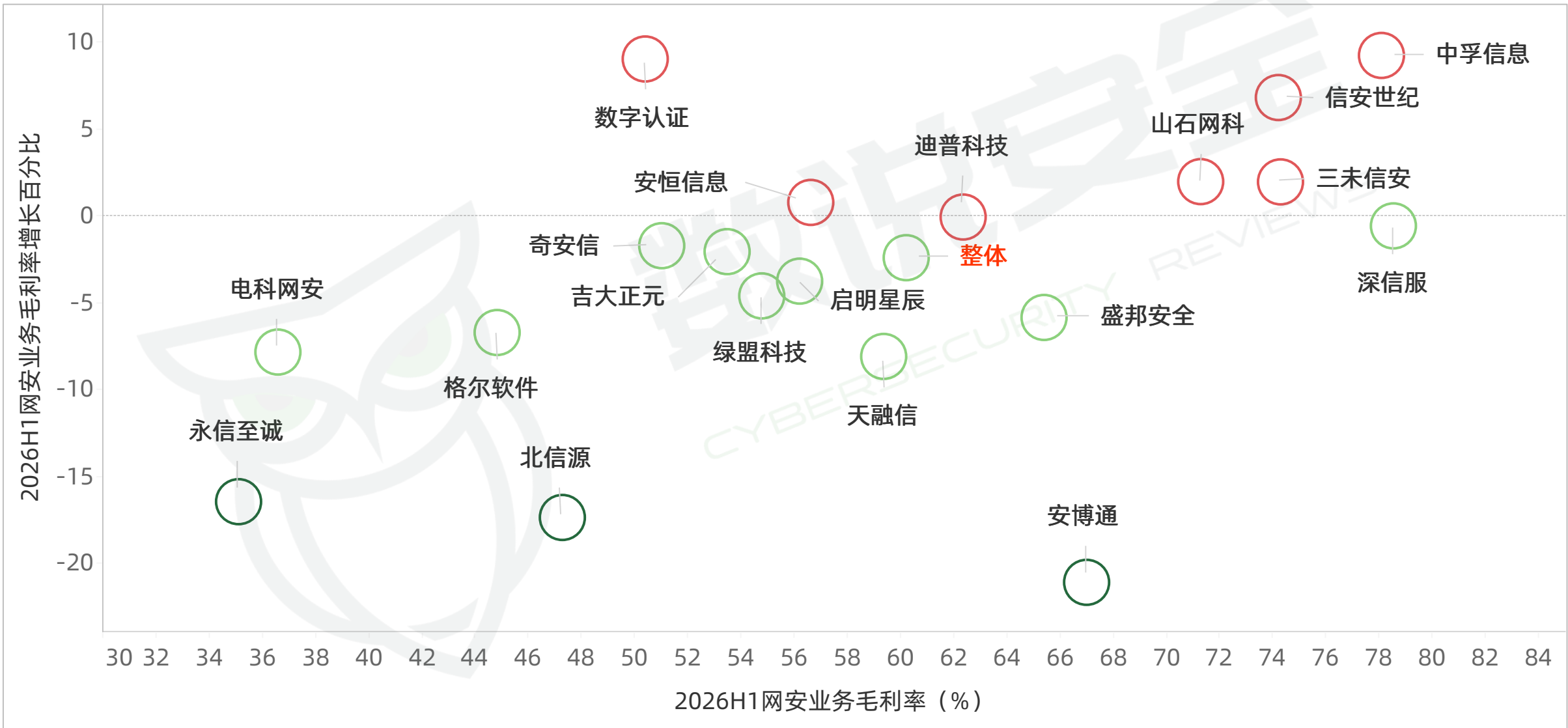
2025年网安样本公司整体毛利率57.4%，较去年同期下降1个百分点，为连续第二年低于 60%；整体毛利润 179.73 亿、下滑 5.97%，与营收降幅的差距由 3.3 个百分点收窄至 1.6 个百分点；10家公司毛利润增长 > 收入增长（深信服为安全业务毛利润）。



2026 年H1行业整体网安毛利率降至60.2%，同比下滑2.4个百分点



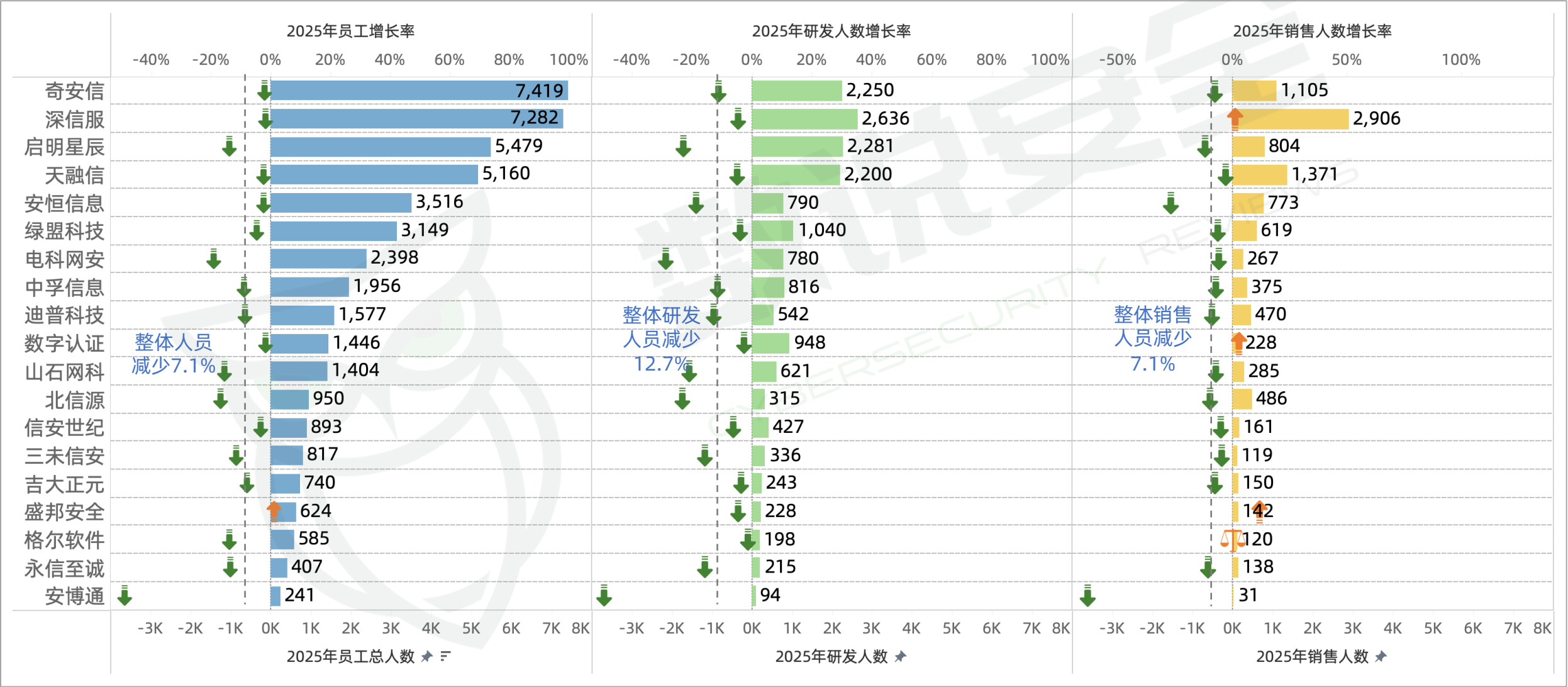
2026年上半年网安业务整体毛利率60.19%，同比下降2.37个百分点；整体网安毛利润 57.08 亿、下滑 10.20%，降幅明显大于安全营收 6.66% 的下滑；深信服78.5%、中孚信息78.1%毛利率居前，安博通降 21.1 个百分点降幅最大。



行业连续三年减员，较2022年峰值少12705人，研发仍为重点减员部门



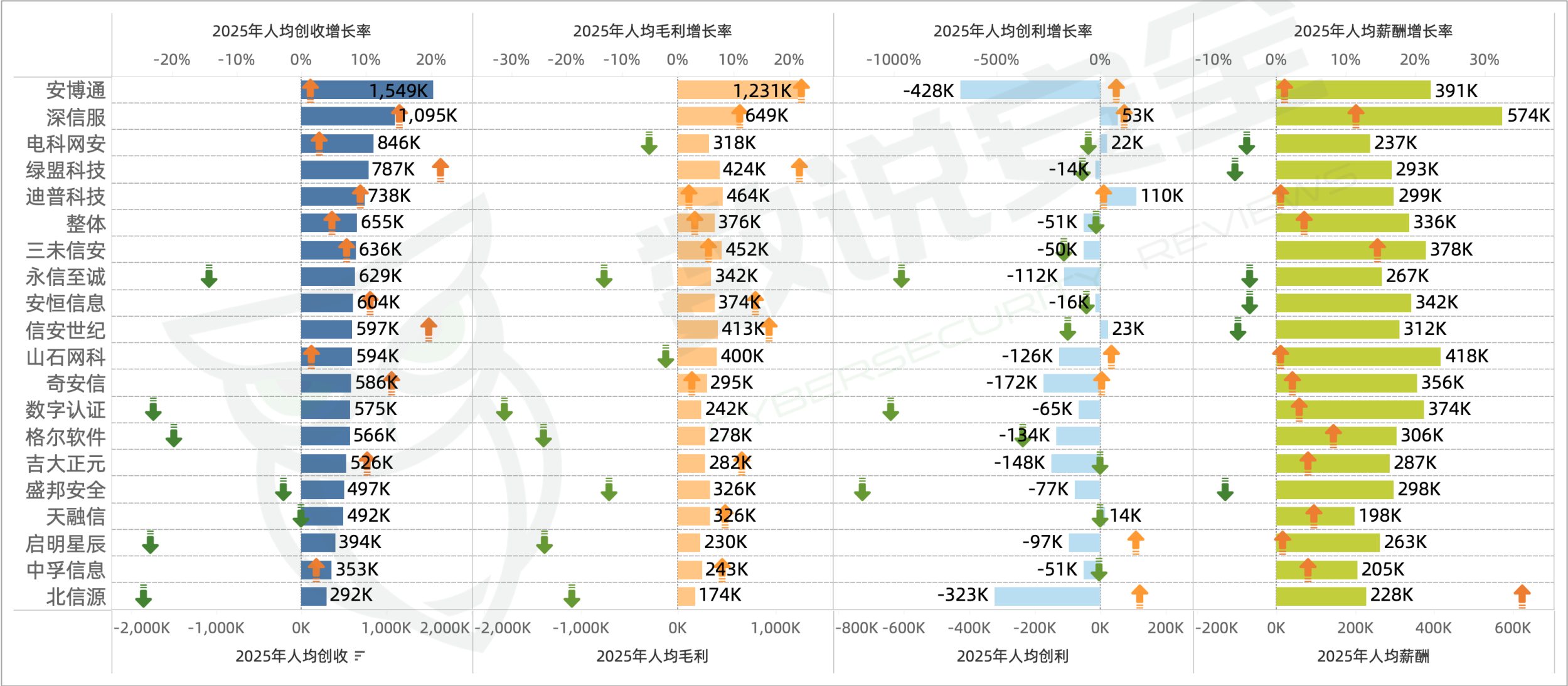
2025年18家网安上市公司进行了减员，仅盛邦安全增长 1.30%，总人数降至46043人，减员7.15%，较去年的10.1%的减员幅度下降近3个百分点；全行业连续第三年减员，累积减员12705人；研发人员是本年减员的主要对象。



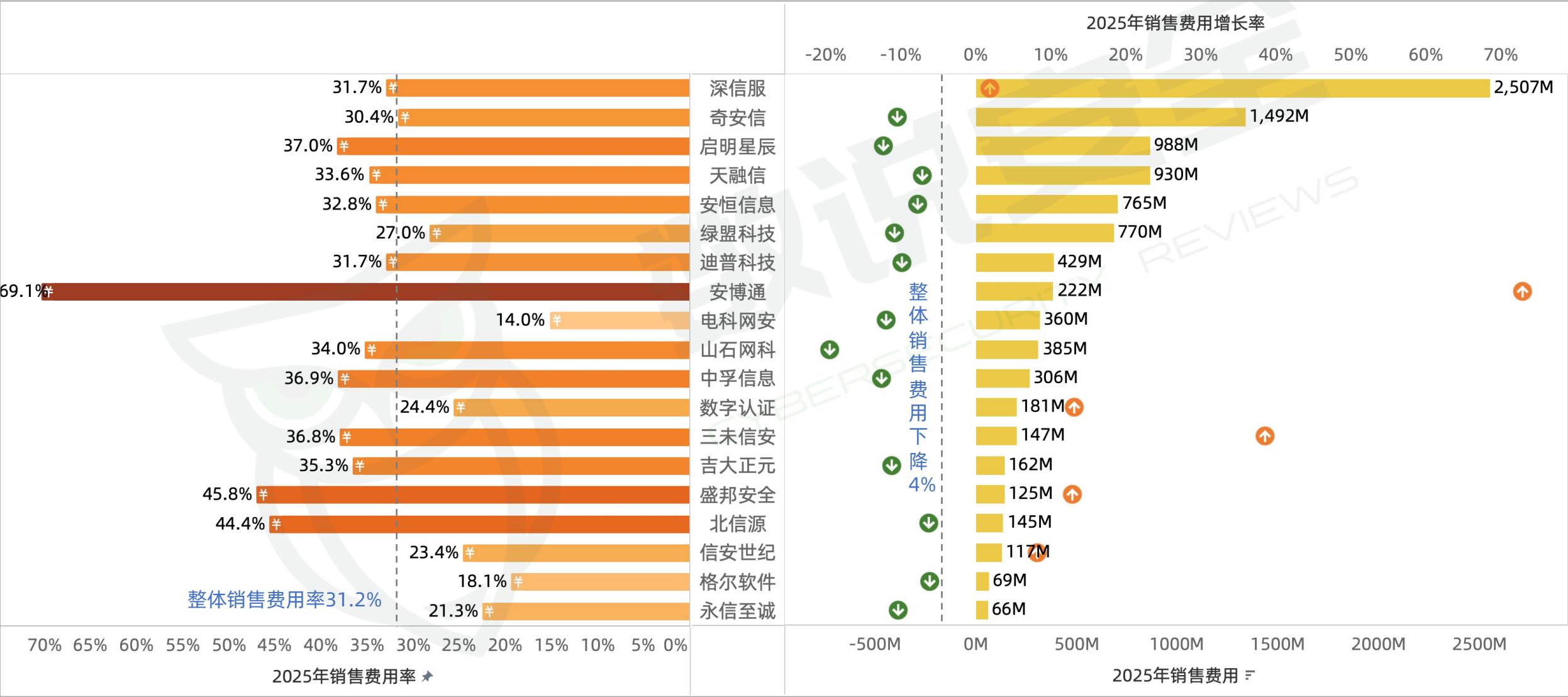
人均创收65.5万、人均毛利37.6万、人均薪酬福利33.6万、人均创利-5.1万



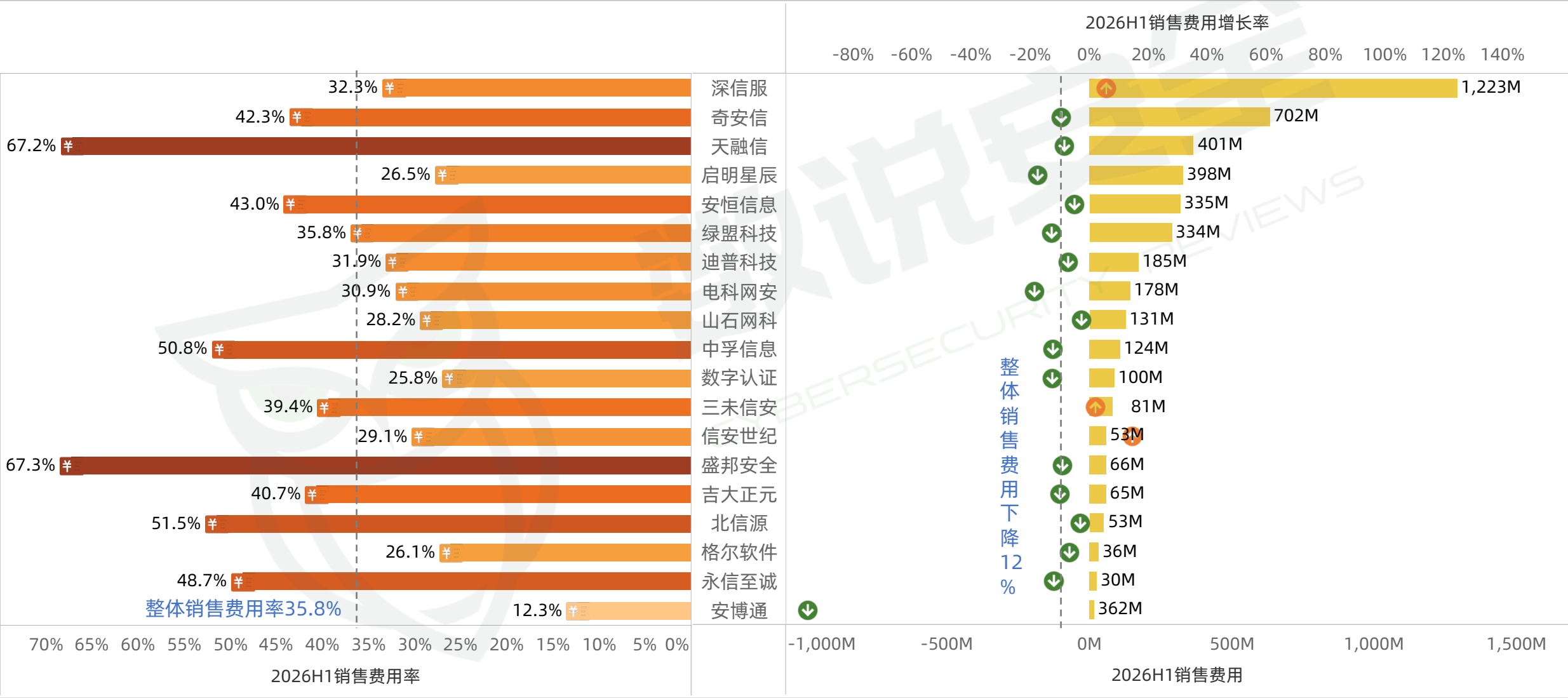
2025 年网安上市公司整体的人均指标呈现三升一降：人均创收 65.47 万、回升 4.7%，为三年来首次；人均毛利 37.59 万、提升 3.0%；人均薪酬 33.64 万、提升 4.0%；人均创利则由 -4.16 万继续恶化至 -5.14 万；三项回升均来自分母收缩——营收下滑 4.4% 而平均人数下降 8.7%；人均薪酬上升，主要因减员福利补偿所致。



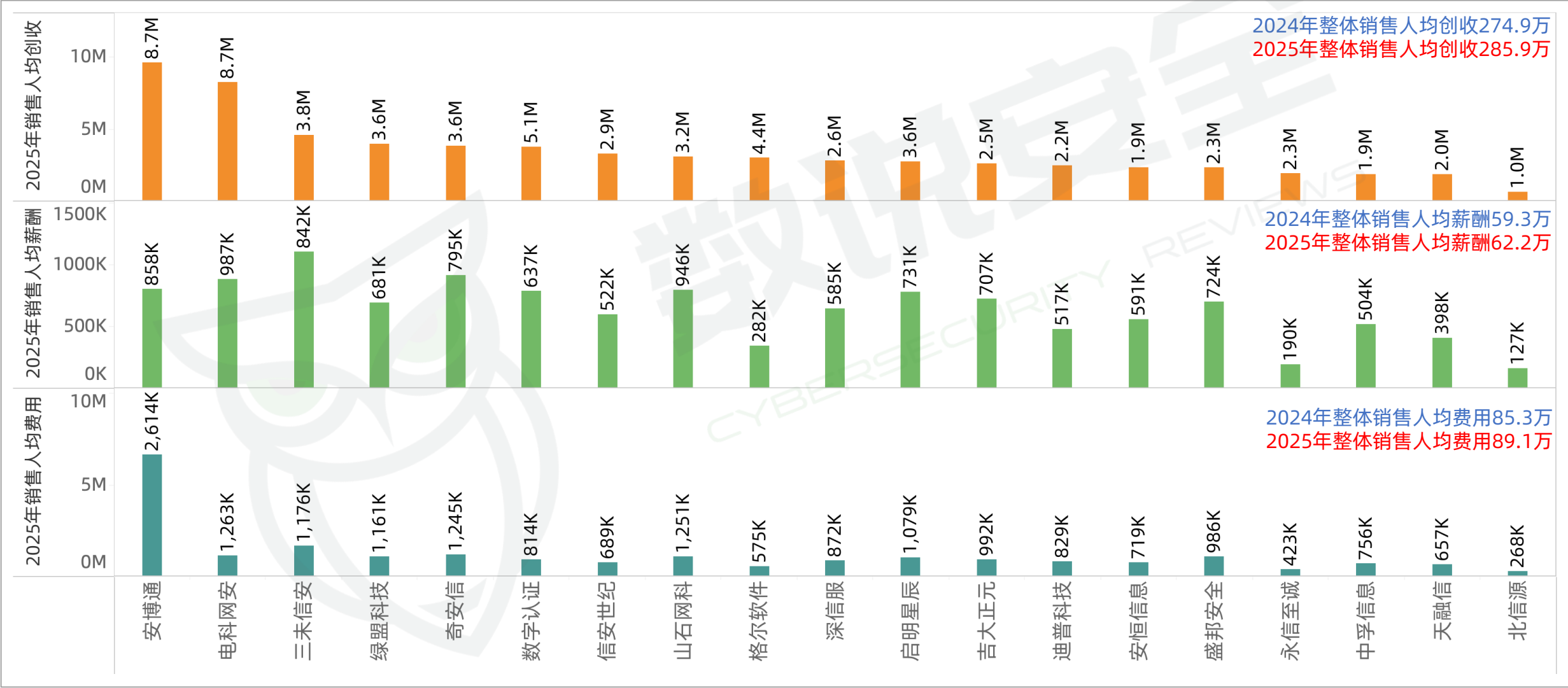
2025 年网安上市公司整体销售费用 97.54 亿，同比下降 4.05%，为连续第二年下降，但降幅较去年的 7% 收窄，略低于收入降幅；销售费用率 31.2%、连续第二年微升 0.12 个百分点。13 家公司压缩销售投入，安博通逆势增加 72.83%、三未信安增加 38.57%。



2026 年上半年网安上市公司整体销售费用 42.53 亿，同比下降 12.41%，降幅远大于上年同期的 3.47%，是本期减亏的首要来源；销售费用率 35.76%、同比回落 5.62 个百分点，上年同期仅降 0.39 个百分点。16 家公司压缩销售投入，安博通降 95.5% 力度最大，深信服逆势增加 5.5%。



2025 年网安上市公司的销售人均创收 285.9 万，较去年的 274.9 万回升 4.0%，结束连续三年下滑；但销售人均费用提升 4.4%，销售人均薪酬提升 4.8%，回升的机制仍是分母收缩：销售人员减少 7.06% 至 10550 人，而销售费用总额下降 4.05%、营业总收入下降 4.40%。



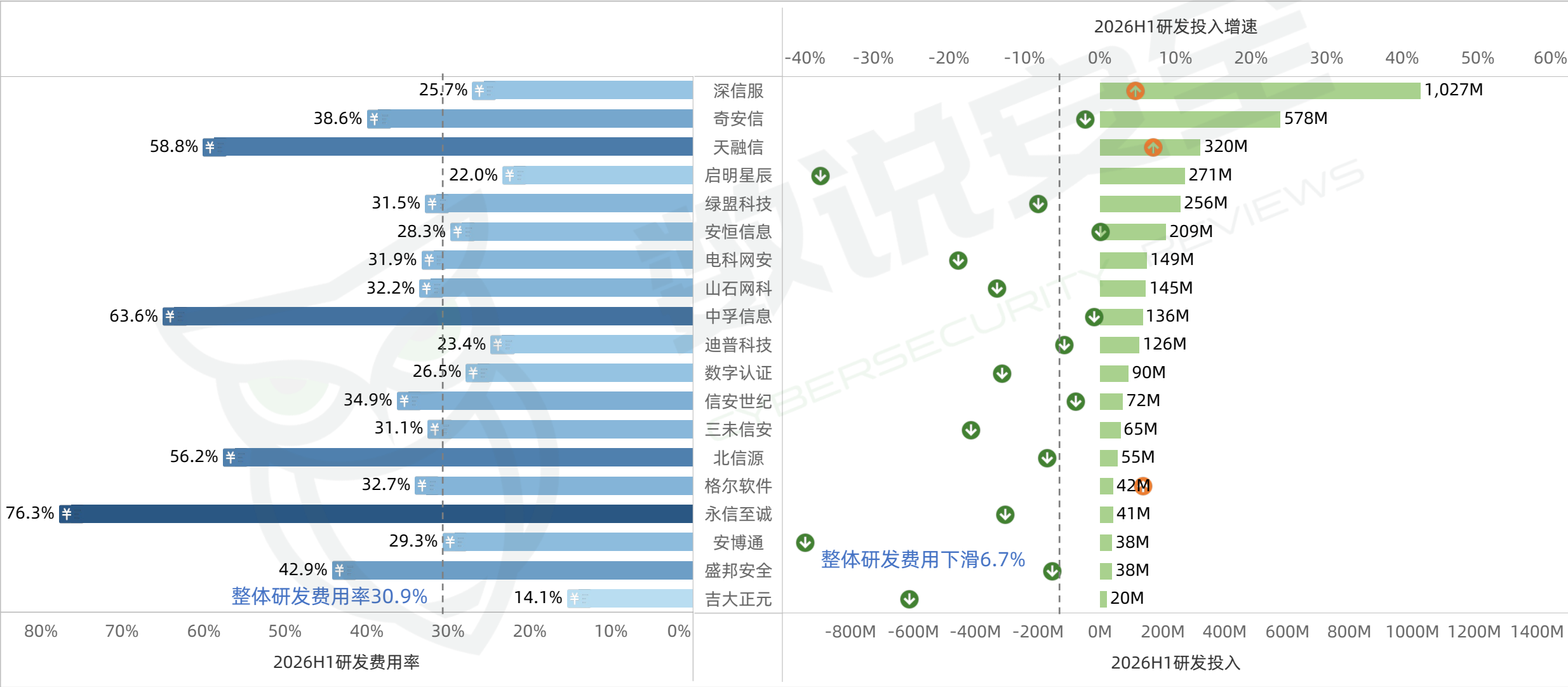
数说安全

2025年研发投入增速	
25.6%	深信服
24.8%	奇安信
31.7%	启明星辰
23.5%	天融信
21.8%	绿盟科技
20.4%	安恒信息
15.2%	电科网安
32.9%	中孚信息
37.4%	山石网科
21.7%	迪普科技
24.8%	数字认证
30.4%	三未信安
27.9%	信安世纪
44.8%	北信源
20.5%	安博通
24.2%	格尔软件
31.6%	永信至诚
27.3%	盛邦安全
12.9%	吉大正元
整体研发费用率24.8%	

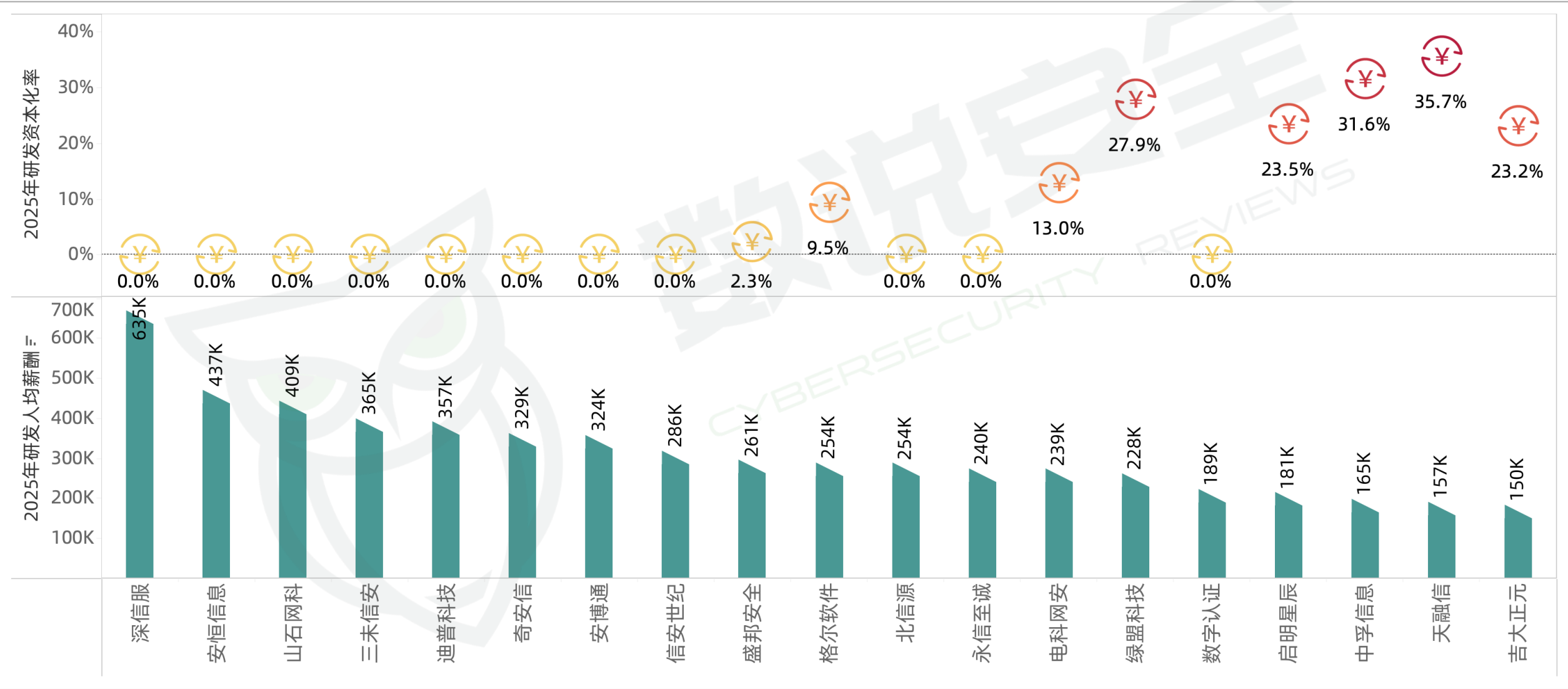
2025年研发投入	
2,055M	深信服
1,090M	奇安信
969M	启明星辰
941M	天融信
768M	绿盟科技
439M	安恒信息
396M	电科网安
349M	中孚信息
340M	山石网科
265M	迪普科技
208M	数字认证
168M	三未信安
151M	信安世纪
137M	北信源
114M	安博通
96M	格尔软件
87M	永信至诚
86M	盛邦安全
68M	吉大正元
整体研发费用下滑8.5%	

2026年H1研发费用率降至30.9%，仅3家公司增加研发费用

2026 年上半年网安上市公司整体研发费用 36.80 亿，同比下降 6.72%，降幅较上年同期的 8.77% 有所收窄；研发费用率 30.94%、同比回落 2.68 个百分点，与上年同期 2.29 个百分点的回落幅度相当。19 家中 16 家研发费用减少，仅 3 家增加；安博通降 39.1%、启明星辰降 37.1% 收缩最激进。

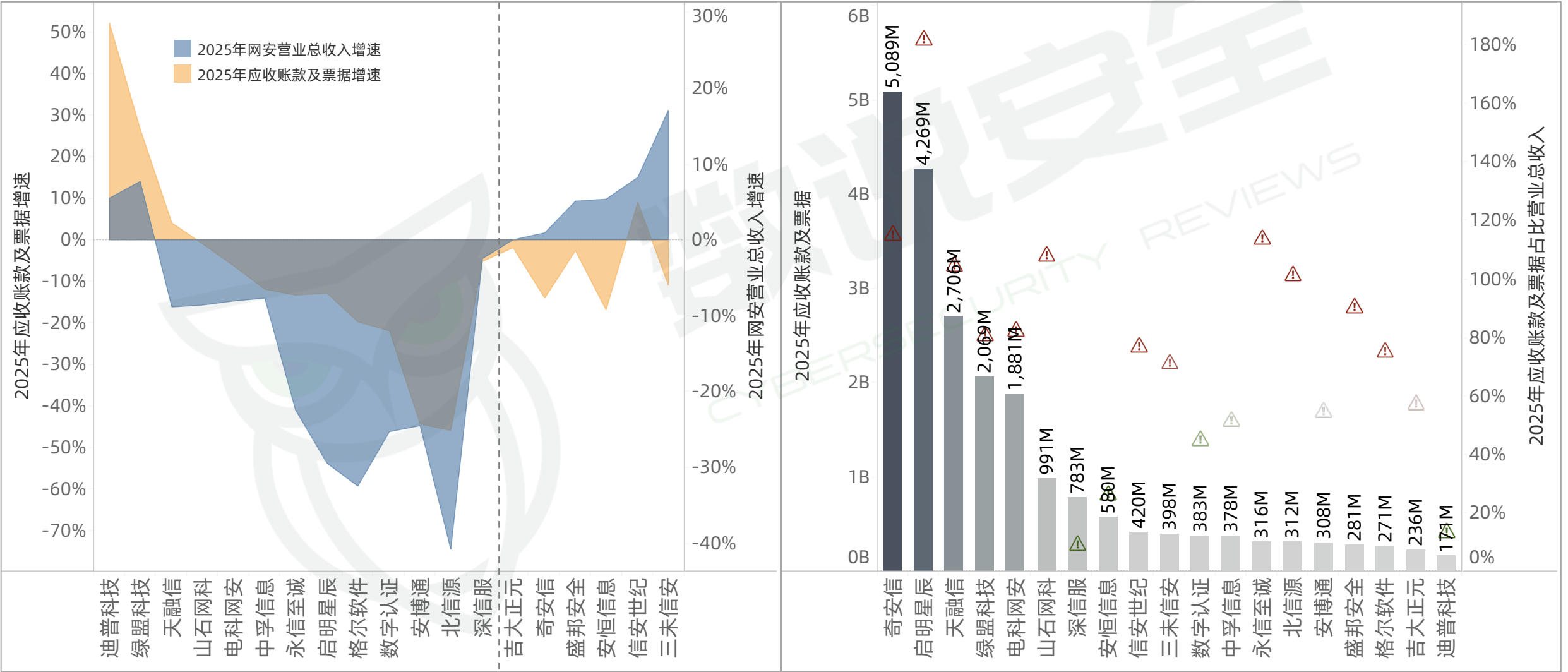


研发投入资本化率的高低可以一定程度上反映出公司利润质量的好坏，一般来讲，研发投入资本化率越高，对利润的影响越大。与2024年“公司普遍上调资本化比重”相反，2025年8家存在资本化，减少2家公司，多家公司下调资本化率，中孚信息下调 7.27 个百分点，山石网科与北信源分别由 9.09%、19.45% 直接降为零，仅三家公司上调。



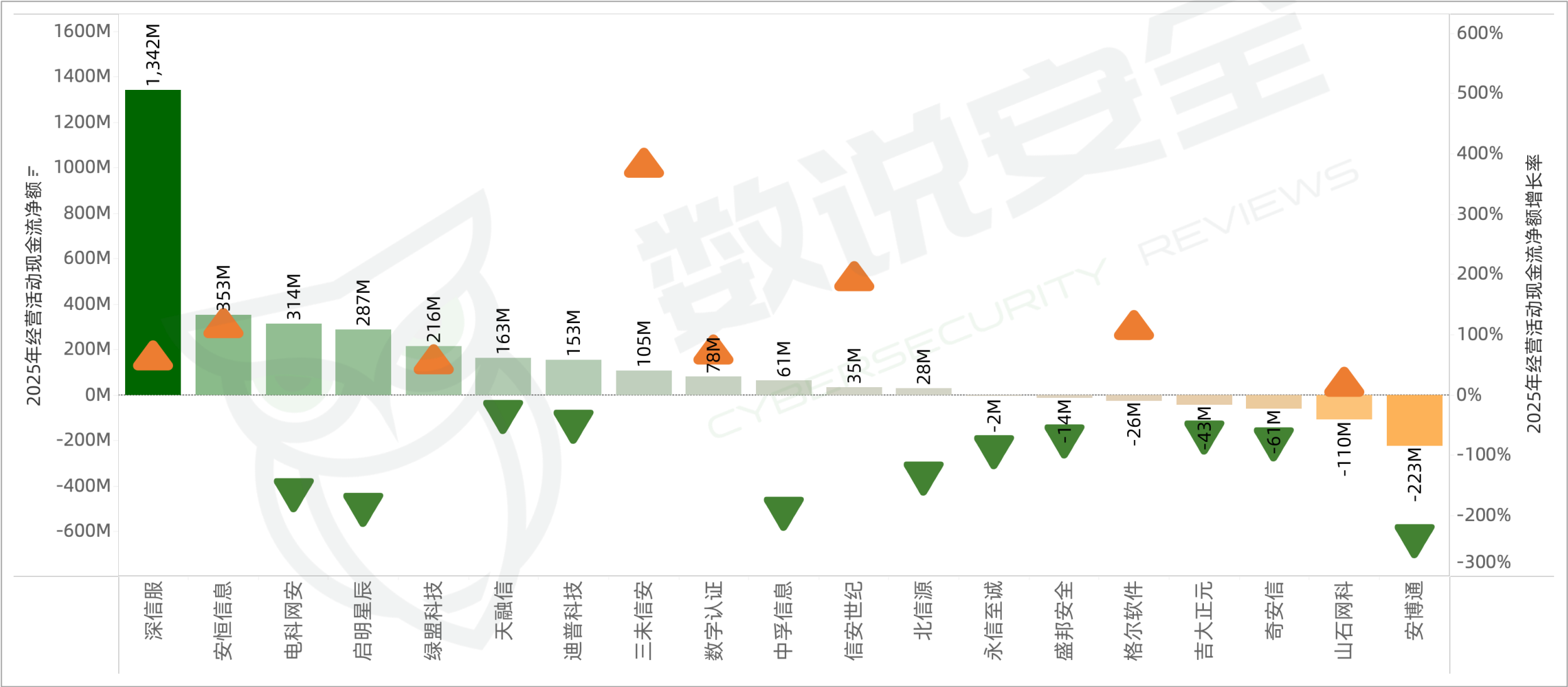
行业整体应收款首次下降 8.2%，占营收比重回落至 69.8%

2025 年网安上市公司的整体应收账款及票据 218.43 亿元，同比下降 8.20%，为近年来首次绝对额下降，去年为增长 1.9%，行业整体应收账款及票据控制效果开始显现；应收款占营业总收入比重 69.8%，较去年的 72.7% 回落 2.9 个百分点，同样是首次，其中深信服 9.7%、迪普科技 14.0% 显著低于行业水平。

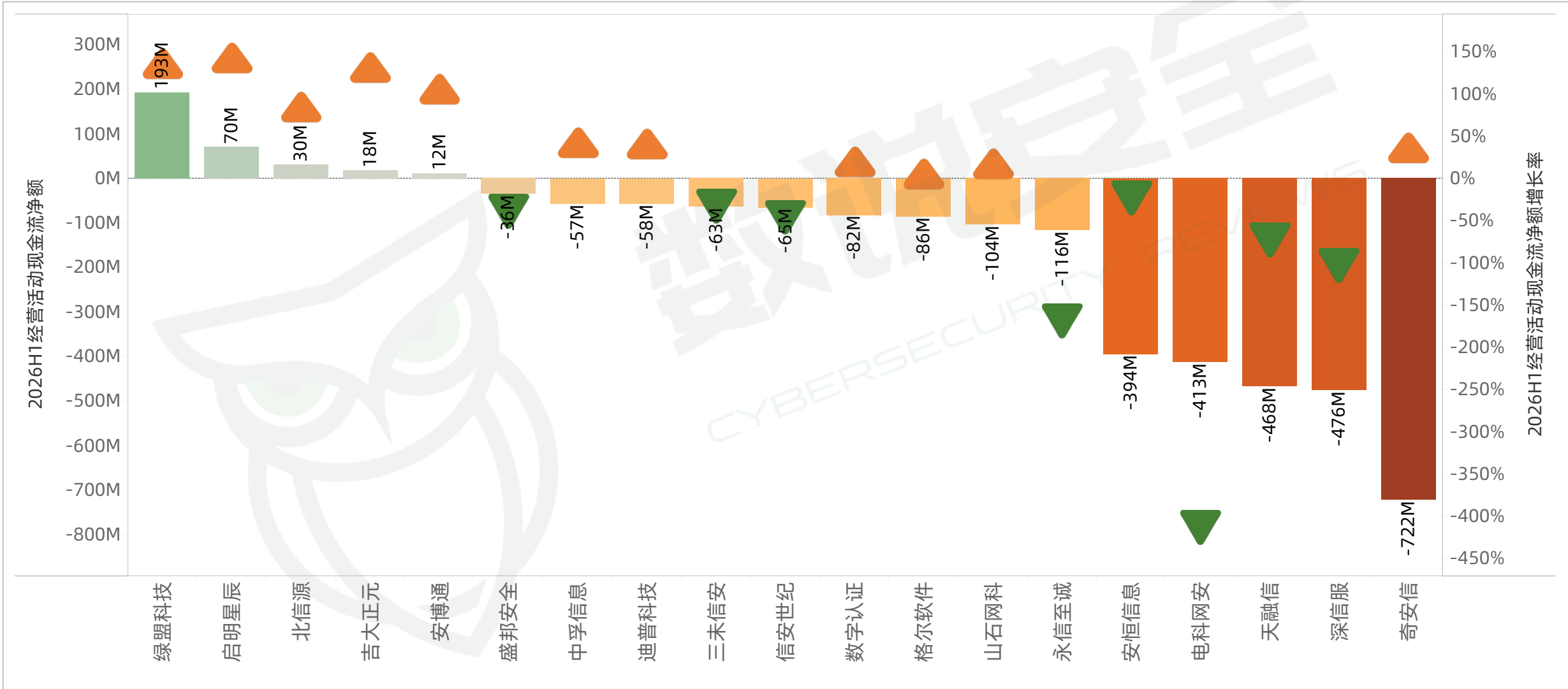


上市公司整体经营性现金流净额26.6亿，收现比升至 1.16

2025 年网安上市公司整体经营性现金流净额 26.56 亿元，较去年的 3.09 亿元增加 23.47 亿元；为正的公司由 9 家增至 12 家，仍有 7 家为负。深信服贡献 13.42 亿、占 50.5%，其余 18 家亦由净流出 5.03 亿转为净流入 13.14 亿。销售商品收到的现金 362.32 亿，收现比由 1.08 升至 1.16。

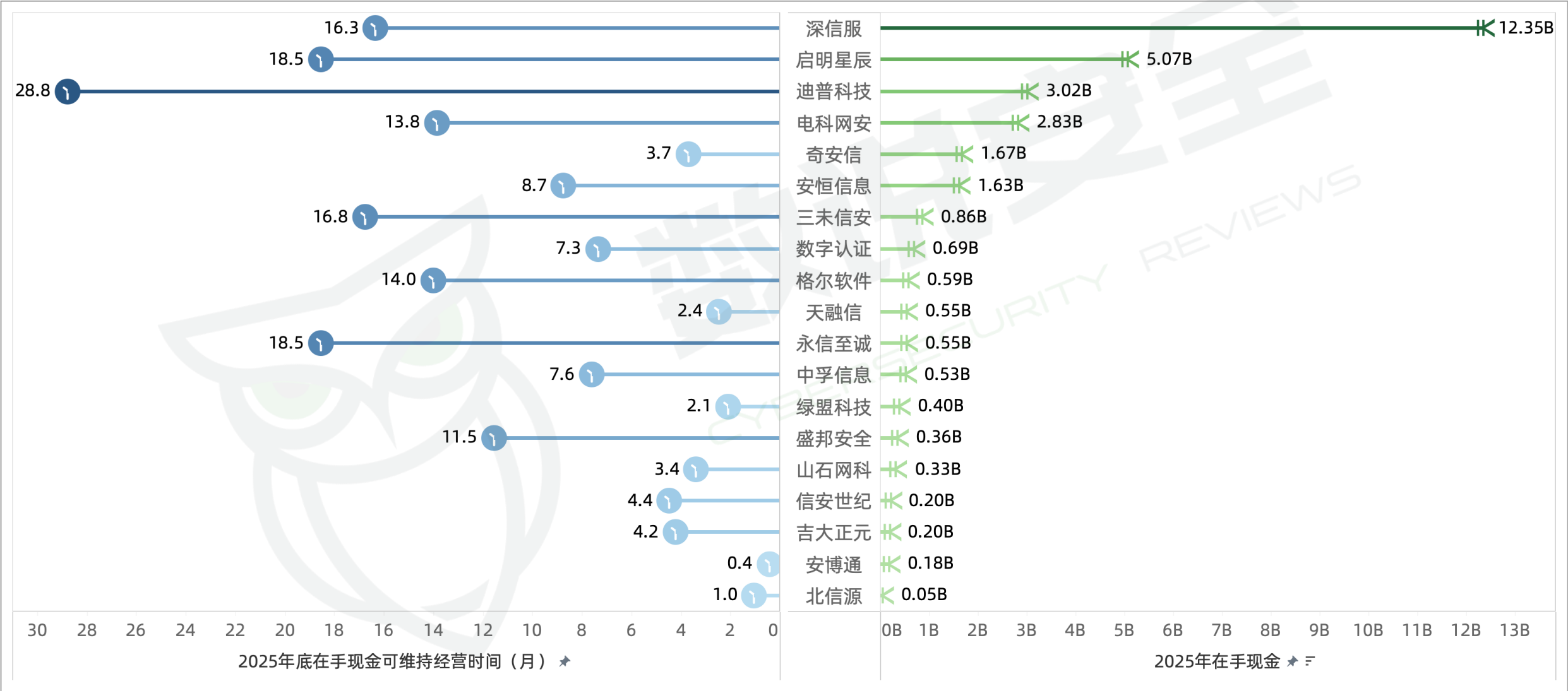


2026 年上半年网安上市公司整体经营性现金流净额 -28.17 亿元，较上年同期的 -30.57 亿元改善 2.40 亿元；为正的公司由 2 家增至 5 家，仍有 14 家为负。网安行业上半年现金流历来为季节性净流出、回款集中于下半年。



整体无收入可维持经营时间不足10个月，深信服在手现金上升至123亿

2025 年网安上市公司整体在手现金 320.57 亿元，较去年同期增长 2.25%；在无任何收入的情况下可维持 9.5 个月生产经营，与去年的 9.6 个月基本持平。深信服在手现金 123.52 亿、启明星辰 50.67 亿、迪普科技 30.23 亿、电科网安 28.26 亿，逆周期生存能力有所提升。



上市公司经营与战略分析

2025年经营情况回顾

2025年公司实现营业总收入43.92亿元，同比增长0.97%，止住了2024年-32.49%的断崖式下滑；安全产品收入27.06亿元，同比增长2.00%，毛利率64.82%、下降6.69个百分点；安全服务收入8.48亿元，同比下滑0.85%，毛利率49.41%、下降6.50个百分点；硬件及其他收入8.27亿元，同比增长0.44%，毛利率3.46%、下降2.05个百分点；公司综合毛利率下降5.67个百分点至50.32%；公司员工人数7419人，减少151人，其中研发人员2250人，减少286人、减员11.3%；销售人员1105人，减少93人、减员7.8%；公司人均创收58.6万元，较上年提升7.2万元；人均毛利29.5万元，较上年提升0.7万元。

- ◆ 2025年减亏的核心驱动是费用收缩而非业务向好——销售费用同比-10.48%、管理费用-15.75%、研发费用-22.77%，三费合计降5.59亿元、费用率同比降13.48个百分点。
- ◆ 公司持续提高现金流重视程度，2025年经营性现金流净额-0.61亿元，同比改善2.81亿元，是上市以来最好水平，距正向打平仅一步之遥。

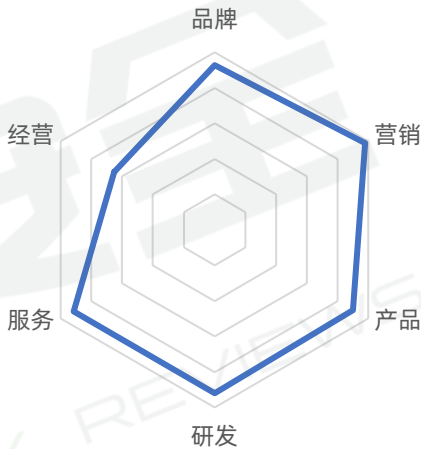
2026年发展战略

- 战略重点：
- I. 坚定“现金流优先”：聚焦核心大客户、深度改革营销体系、回款专项管理。
 - II. 全面拥抱AI：“AI for Security”和“Security for AI”双主线推进产品AI化，已从能源、汽车、有线、金融等行业头部客户实现收入转化。

总结：

2025年是公司“现金流优先”战略首年见效之年：经营性现金流净额回升至-0.61亿元、为上市以来最好水平，销售回款51.39亿元（+8.00%），三费合计压降5.59亿元。但造血改善主要靠费用压缩驱动，毛利率仍在下行说明业务结构性问题尚未解决。2026年经营重心转向“销售订单向利润回款高效转化”，关键验证点是毛利率能否稳定在50%以上，以及收入能否恢复增长。

竞争力

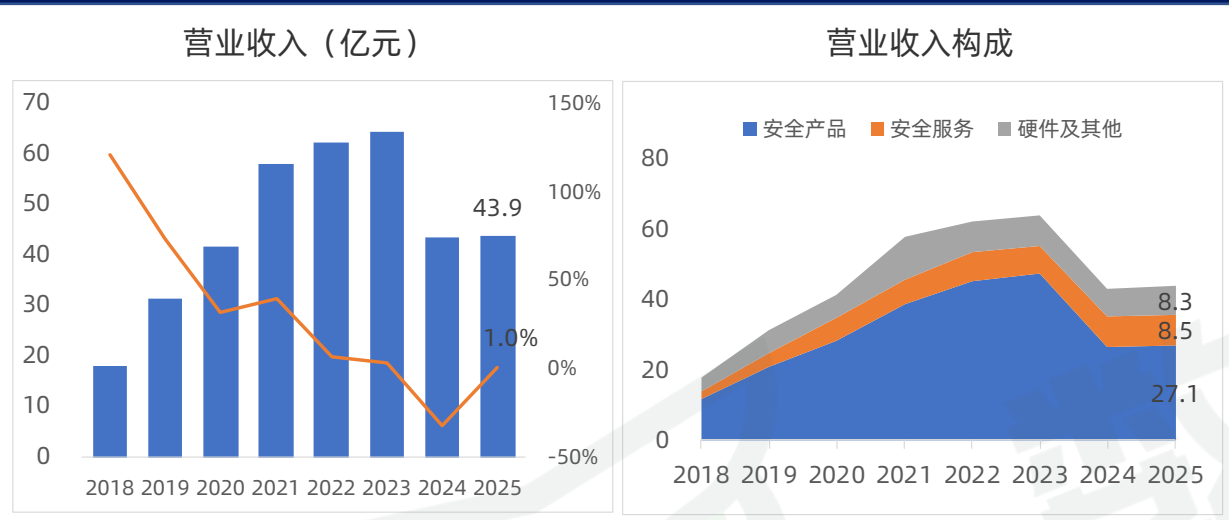


- ◆ 品牌影响力强。奇安信多次承担大型重要活动的网络安全保卫者的角色，并取得优异的成果，综合网络安全实力强劲，已经成为成长性最高，市占率最高的国内网络安全公司，在行业内具备较高的知名度。
- ◆ 产品、营销及服务体系完善。公司现已建立国内最完整的网络安全产品体系，同时也建立了覆盖全国的营销及服务网络，全面满足政企客户的网络安全需求，具备为用户提供网络安全整体解决方案及运营服务能力。
- ◆ 人才储备充沛。截至2025年末，公司员工7419人，具有较大规模的专业人才储备。在此过程中，公司不断聚集、培养大量行业内市场、研发、营销、服务等领域的中高端人才，这些人才是其未来战略成功的重要保障。

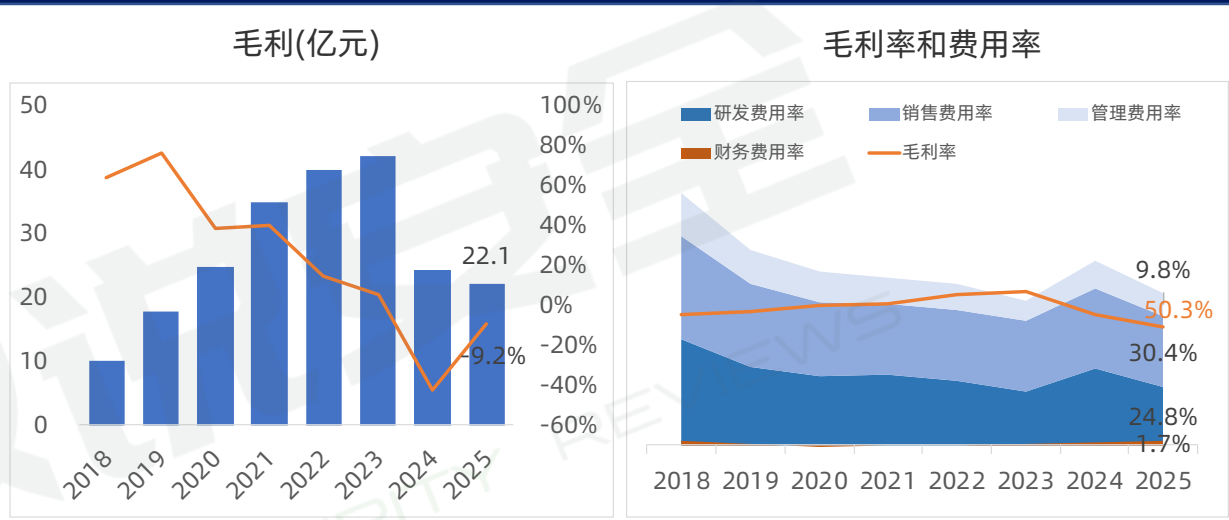
改进：

- ◆ 经营能力仍需改善。2025年营收止跌微增0.97%，但归母净利润亏损12.87亿元；经营性现金流净额创上市以来最优，但仍为-0.61亿元，离回正一步之遥；公司有息借款近18亿元，仍有一定利息费用压力；公司当前应继续加强回款管理、尽快恢复造血能力。

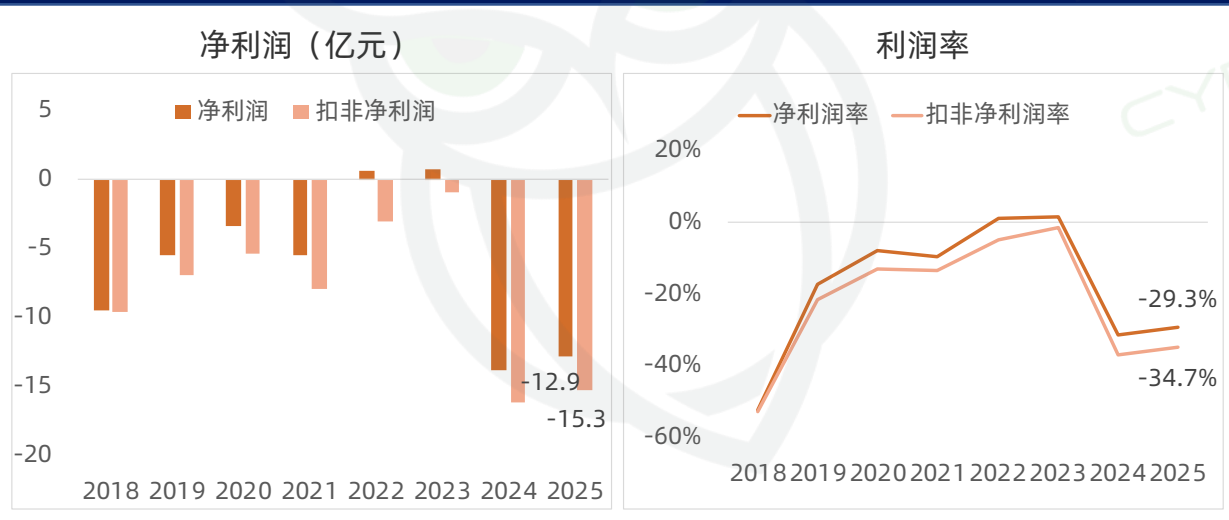
营业收入情况



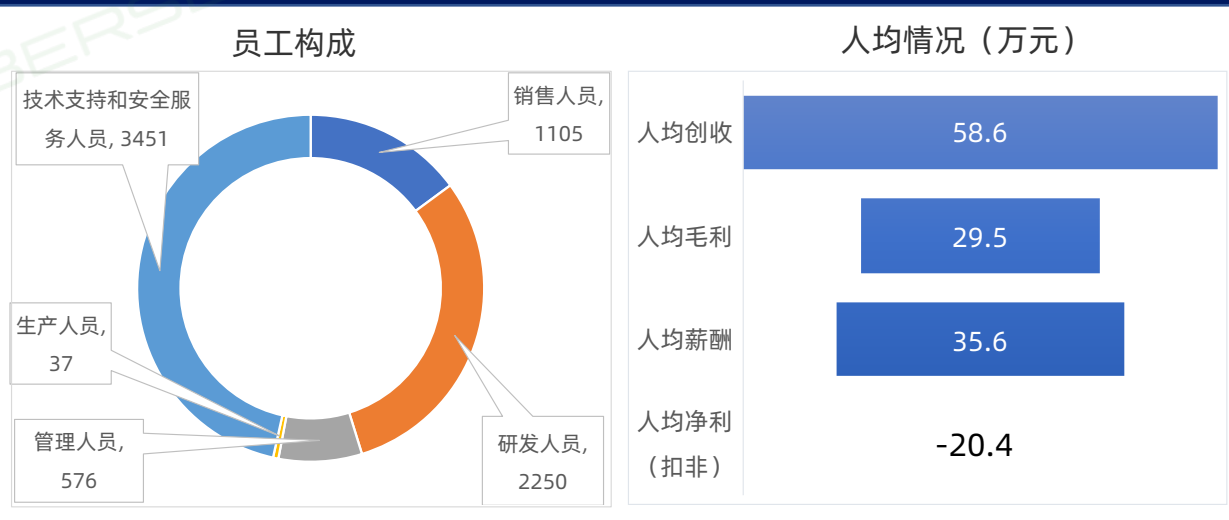
毛利情况



盈利情况

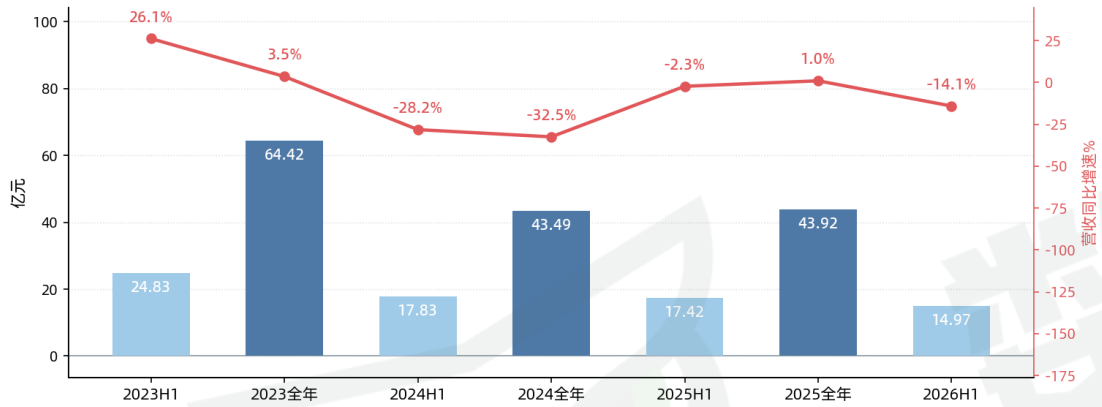


员工情况

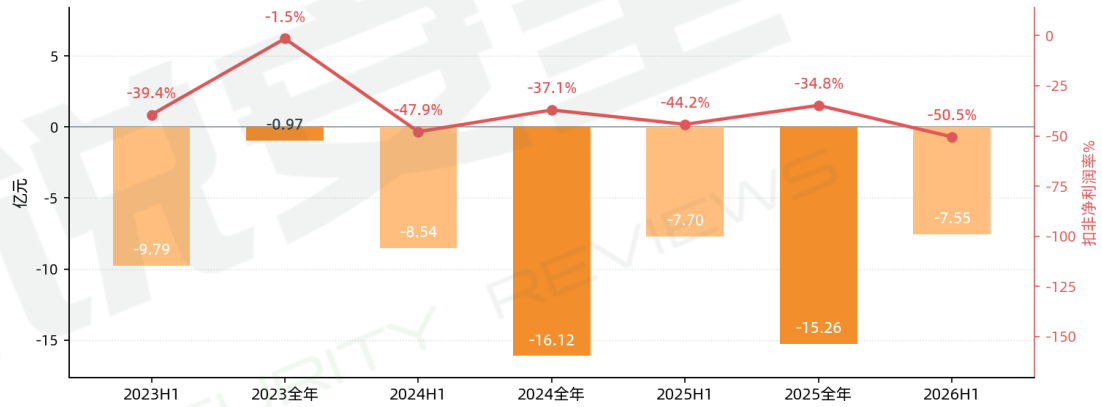


奇安信表现出“止血成功、造血未启”的状态。收入端 2023H1 的 24.83 亿一路降到 14.97 亿，三年缩掉四成；扣非净利润率从 -39.4% 走到 -50.5%，亏损占收入比重反而随规模收缩而上升，说明成本结构中的刚性部分尚未触及。真正的转折在现金：隐含下半年经营现金流由 2023 年的 6.21 亿升至 2025 年的 10.82 亿，H1 净流出也从 -11.43 亿收窄至 -7.22 亿——回款能力在改善，且改善幅度大于收入降幅。换言之公司已把“收得回来”的问题解决了大半，剩下的是“卖得出去”。

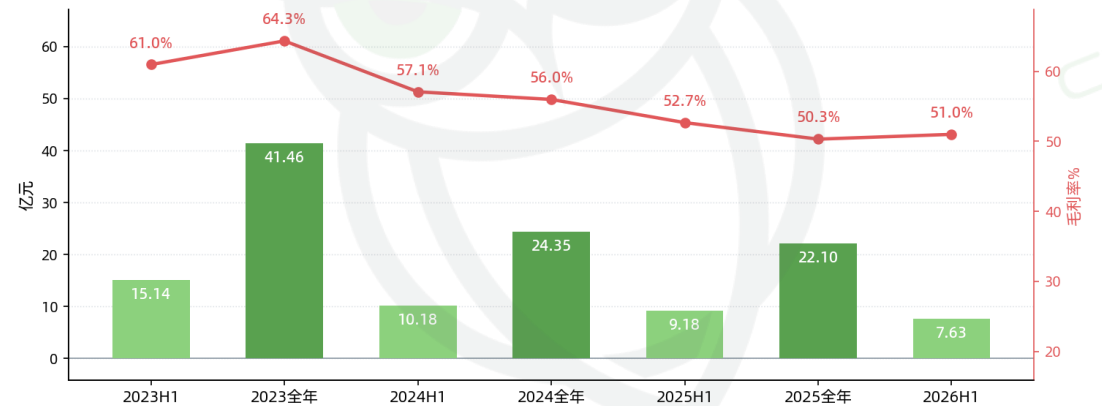
营业收入及同比增速



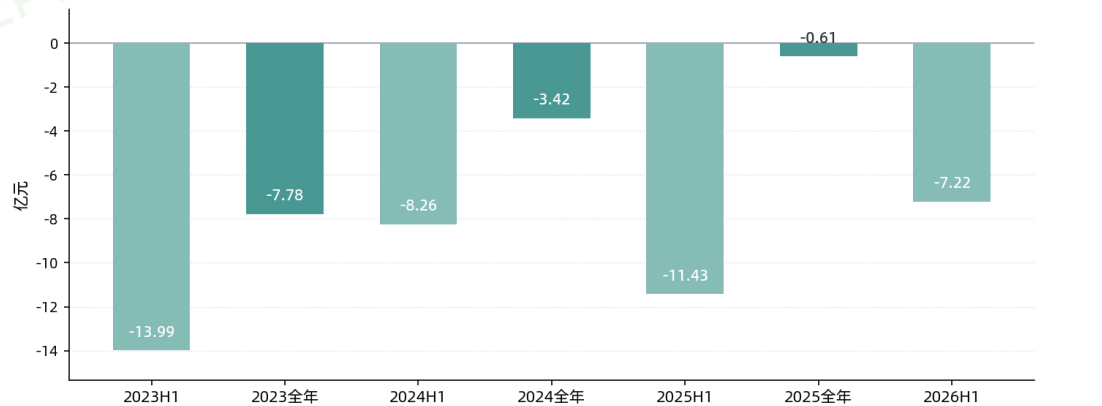
扣非净利润及扣非净利润率



毛利润及毛利率



经营活动现金流净额



浅色 = 半年度（1-6月累计） 深色 = 全年度 红色折线 = 右轴比率/增速

2025年经营情况回顾

2025年公司实现营业总收入23.38亿元，同比下滑29.49%，为连续第二年两位数下滑；安全产品收入12.67亿元，同比下滑33.5%，毛利率62.8%、提升1.96个百分点；安全运营与服务收入10.50亿元，同比下滑24.1%，毛利率53.2%、下降2.90个百分点；公司综合毛利率下降0.50个百分点至58.27%；公司员工人数5479人，减少898人，其中研发人员2281人，减少677人、减员22.9%；销售人员804人，减少111人、减员12.1%；公司人均创收39.4万元，较上年下降12.0万元；人均毛利23.0万元，较上年下降7.3万元。

- 2025年减值损失合计2.13亿元（信用减值1.25亿元+资产减值0.88亿元）叠加公允价值亏损0.85亿元，共同蚕食经营修复成果，利润底尚未到来。
- 公司积极全面融入中国移动体系，聚焦云安全、零信任+等战略型业务。
- 作为以大客户销售为典型的网安龙头企业，公司持续改善回款：2025年经营性现金流净额2.87亿元、同比+191.07%结束连续三年为负，应收账款连续8个季度压降、同比降约6.4亿元。

2026年发展战略

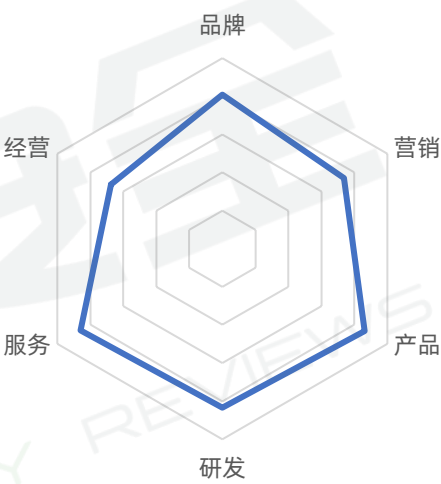
战略重点：

- I. 中移协同深化：与中国移动的中移自采业务实现同比增长，从规模扩张向质效升级转变，聚焦云安全、零信任+等战略型业务。
- II. 新赛道布局：AI+安全、专线卫士、安全云电脑三条增长曲线初具形态，专线卫士已累计服务7.2万政企客户。
- III. 降本收缩：主动压减低毛利集成业务，三费合计同比下降8.68%，精细化运营见成效。

总结：

公司已从独立安全厂商转为运营商体系内的专业子公司，2026年继续深度融入中国移动的云、网、数、DICT体系，并加大AI赋能安全投入、发挥“大模型安全大脑”核心作用。

竞争力



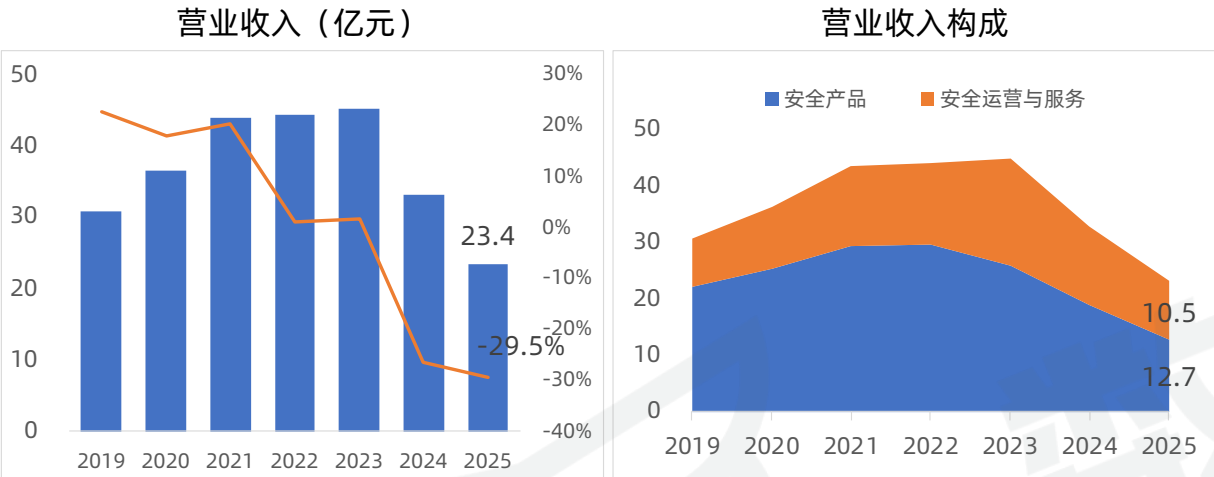
优势：

- ◆ 品牌及市场影响力。自2011年并购网御星云后，公司成为中国网络安全龙头企业，品牌得到客户广泛认可。
- ◆ 营销网络与客户积累。拥有覆盖全国的营销和技术服务体系，安全产品覆盖全面，另有较强直销能力以及中移动资源加持，大BGI市场渗透能力突出，在军工、能源、电信、金融等行业具备较为深厚的顶层客户资源能力。
- ◆ 资本市场运作能力。公司上市后连续并购多家细分领域优质企业，形成了相对完整的产业链布局。另外，中移动成为公司的实控人，国企的身份更有利于公司拓展政企、运营商等市场。

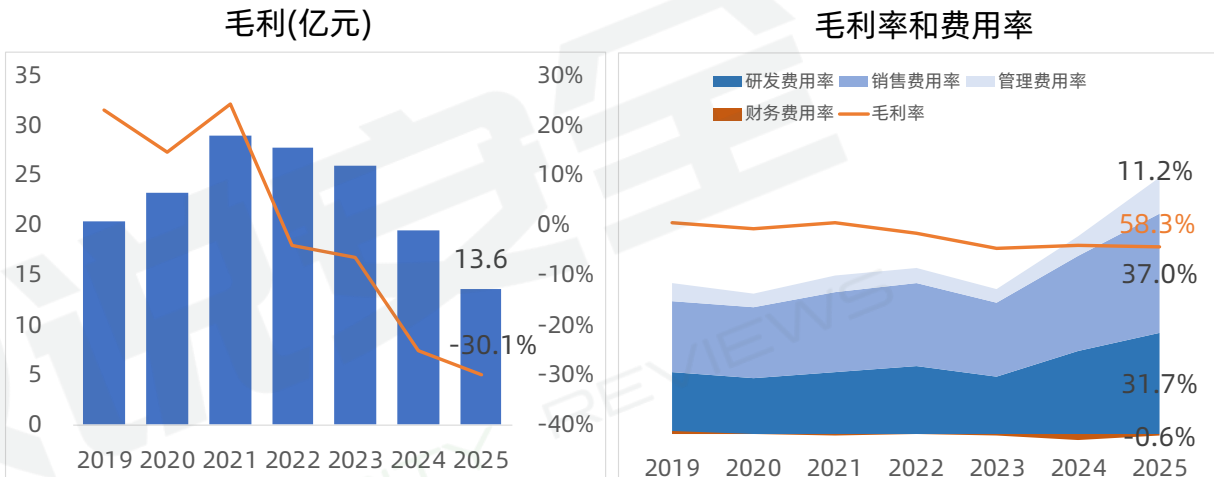
改进：

- ◆ 实控人更替过渡期的平衡与整合。中移动成为公司实控人后，公司需要对研发、产品、营销等多维度评估和整合，以确保业务流程和战略方向的一致性。以及在整合过程中，根据新的业务方向和战略目标，对组织结构进行优化，以提高运营效率和市场响应速度。

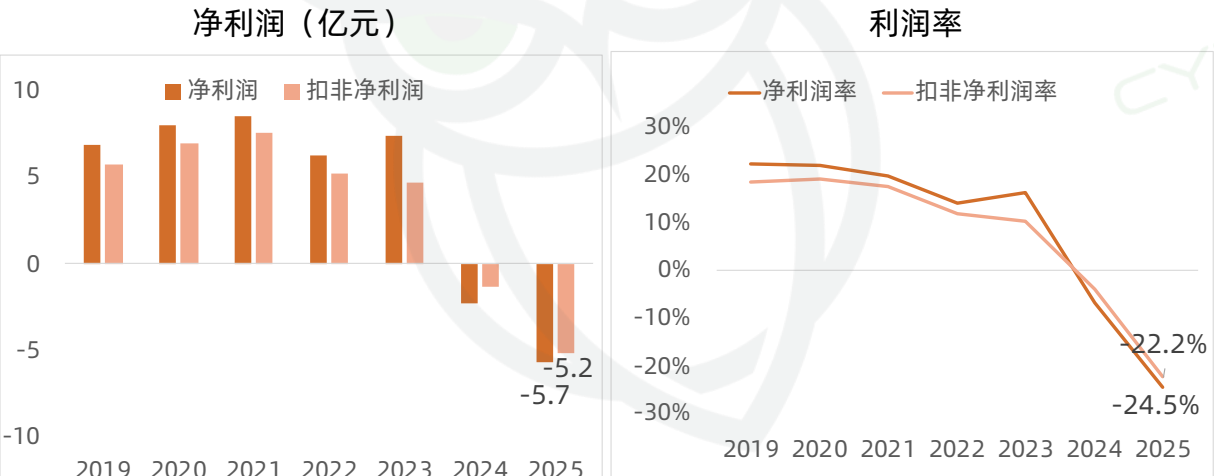
营业收入情况



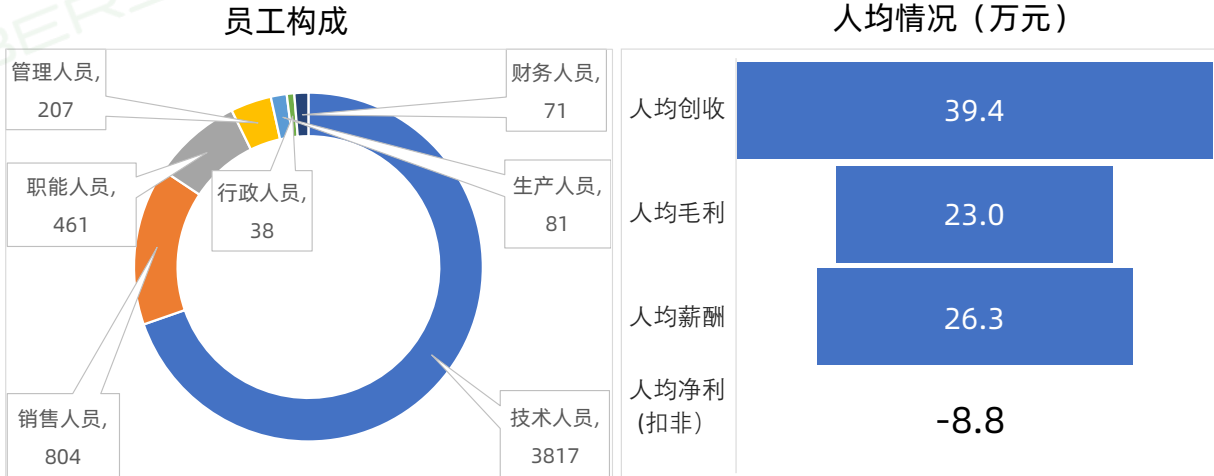
毛利情况



盈利情况

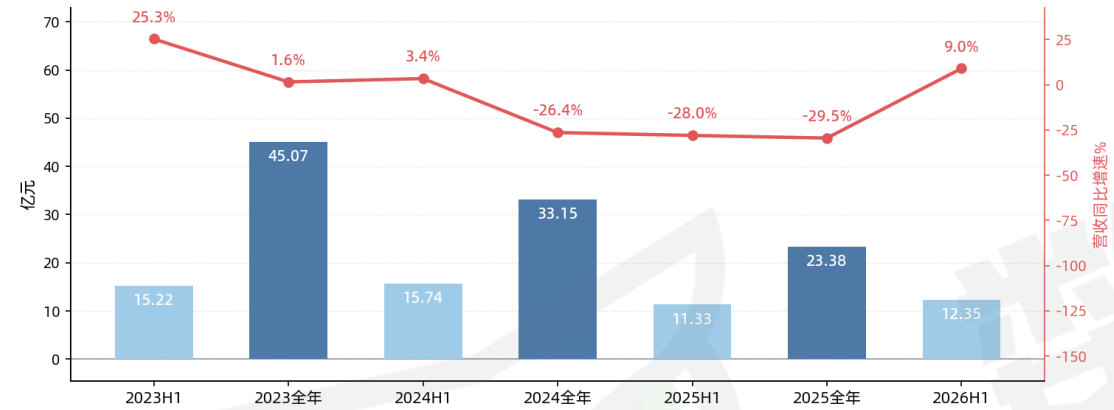


员工情况

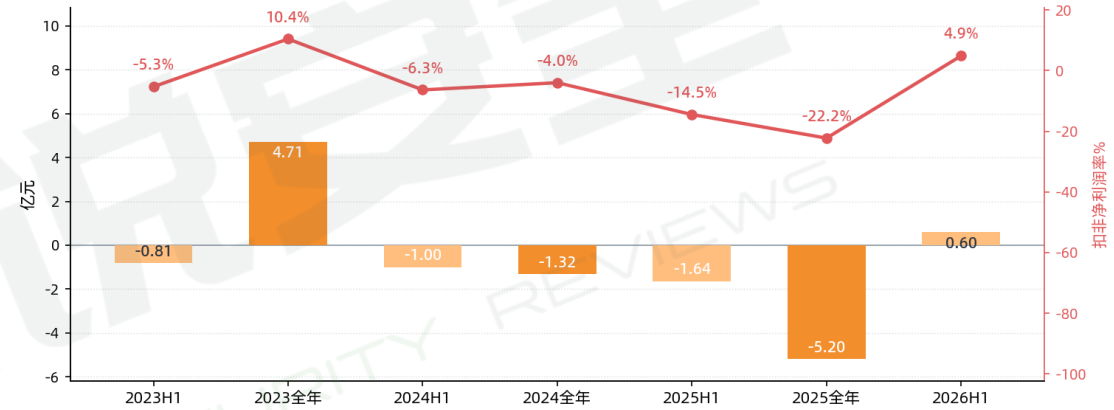


启明星辰本期扭亏值得肯定，但下半年冲量的比重正在大幅下滑，H1 收入占全年比重从 2023 年的 33.8% 跳到 2025 年的 48.5%，H2收入由 29.85 亿萎缩至 12.05 亿，两年蒸发六成。这表明下半年收入及其全年占比明显下降，传统下半年集中交付模式承压。本期 H1 收入回升 9.0%、扣非率转正至 4.9%，但毛利率同步降 3.72 个百分点，叠加研发费用砍掉 37%，这次盈利更像是把成本压到了收入曲线之下，而非需求回暖。

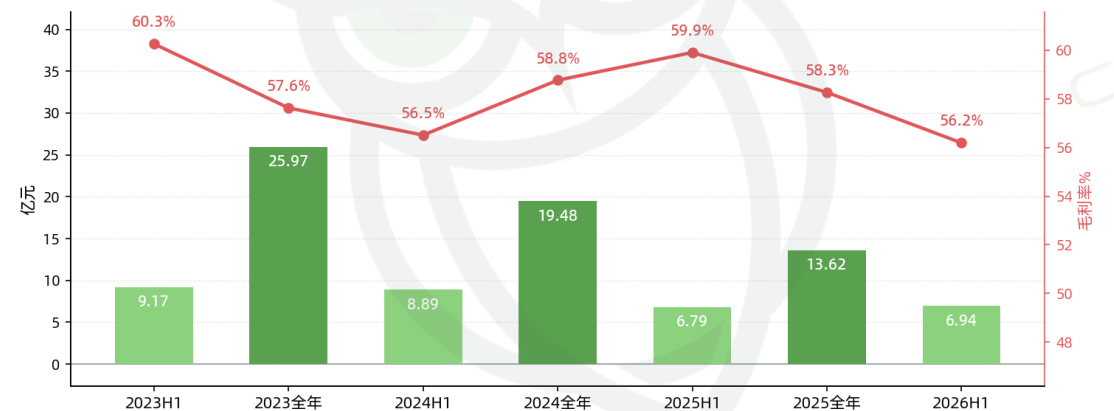
营业收入及同比增速



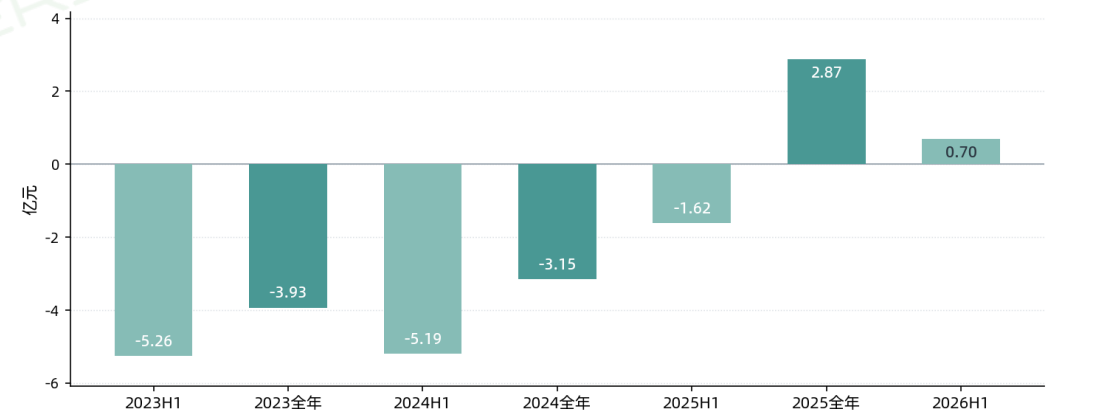
扣非净利润及扣非净利润率



毛利润及毛利率



经营活动现金流净额



浅色 = 半年度 (1-6月累计) 深色 = 全年度 右轴比率/增速

2025年经营情况回顾

2025年公司实现营业总收入80.43亿元，同比增长6.96%，创历史新高、首次突破80亿；网络安全业务收入35.40亿元，同比下滑2.46%，毛利率79.43%、提升0.12个百分点；云计算及IT基础设施业务收入40.10亿元，同比增长18.50%，毛利率42.51%、下降1.73个百分点；基础网络和物联网业务收入4.93亿元，同比下滑2.69%，毛利率51.46%、提升2.74个百分点；公司综合毛利率下降2.16个百分点至59.31%；公司员工人数7282人，减少128人，其中研发人员2636人，减少129人、减员4.7%；销售人员2906人，增加33人、增员1.1%；公司人均创收109.5万元，较上年提升14.4万元；人均毛利64.9万元，较上年提升6.5万元。

- ◆ 归母净利润3.93亿元，同比+99.52%；扣非净利润3.04亿元，同比+296.38%，利润修复显著。三费合计49.48亿元（同比-1.15%），费用率从65.57%降至61.52%，降本增效成效明显。
- ◆ 2025年经营性现金流13.42亿元，同比+65.29%，创公司上市以来最好水平。
- ◆ 2025年公司发布AI安全平台、安全GPT系列产品，推动超融合向"AI超融合"升级。

2026年发展战略

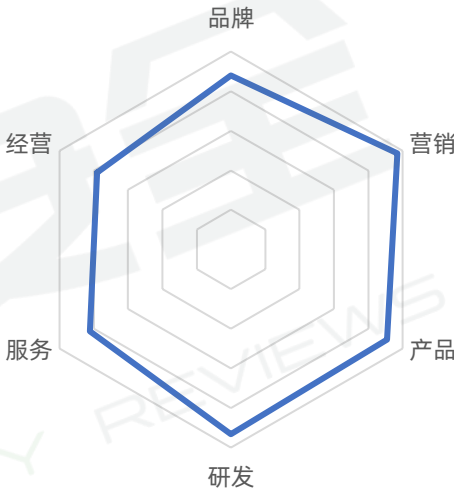
战略重点：

- I. AI重构安全业务：发布AI安全平台、安全GPT系列产品，以"开放平台+领先组件+云端服务"推动安全业务AI化。
- II. 云业务向AI Infra转型：推动超融合向"AI超融合"升级，打造统一存储、AI算力网关等适配AI时代的基础设施。
- III. 加大KA与海外投入：海外收入5.99亿元（+24.49%），KA及行业头部市场持续深耕。

总结：

深信服正在从“安全公司做云”切换为“云公司兼做安全”——云计算收入已首次超过网安业务、占比达49.86%。2026年押注两条主线：用AI重构安全业务，以XaaS交付和“开放平台+组件+云端服务”跳出传统硬件交付。

竞争力



优势：

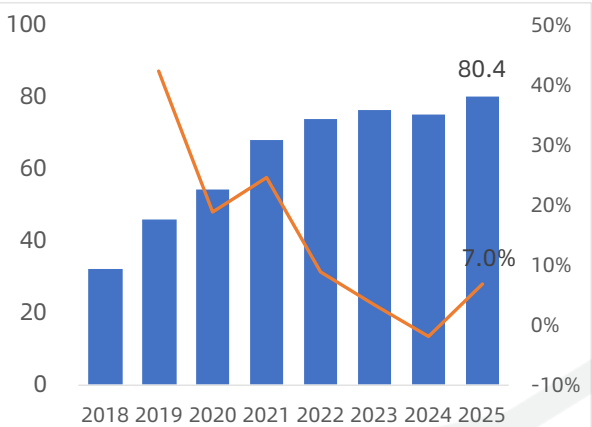
- ◆ 定位清晰，战略明确且执行能力强。公司商业价值定位清晰准确，战略布局能力突出，除安全业务外积极布局云计算领域，并实现信息安全业务与云计算业务协同发展。
- ◆ 渠道管理能力强，市场覆盖度高。国内安全公司中渠道体系最为庞大和完善的公司之一，渠道合作伙伴数量超过千家，迅速完成对小BGI的广泛覆盖，具备极强的市场渗透能力。
- ◆ 安全服务能力提升。公司近两年积极搭建服务体系及服务网络，核心安全服务能力提升。

改进：

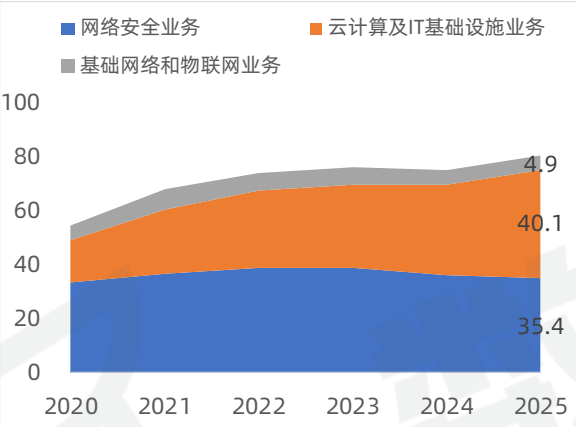
- ◆ 大客户市场亟需突破。深信服营销模式一直以渠道为主，最近几年渠道收入占比超过90%。面向高端客户采用直销模式，最近几年也在加强直销体系建设，但收效有限，面向大BGI的营销能力有待加强。
- ◆ 平衡好创新产品投入和现有产品的关系。深信服近两年来一直重点投入创新产品，但是效果不及预期，要确保资源合理的分配，加强市场导向和客户反馈，及时调整产品特性以适应市场变化。

营业收入情况

营业收入（亿元）

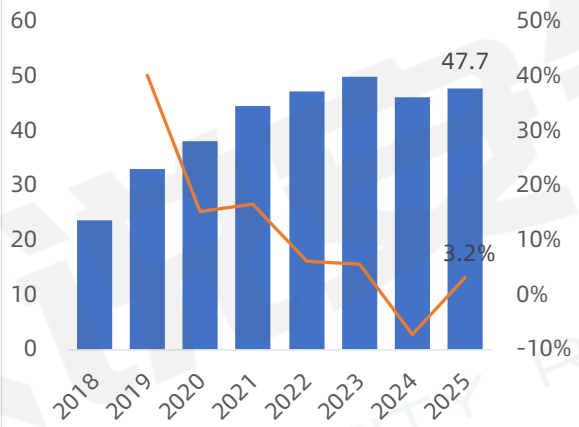


营业收入构成

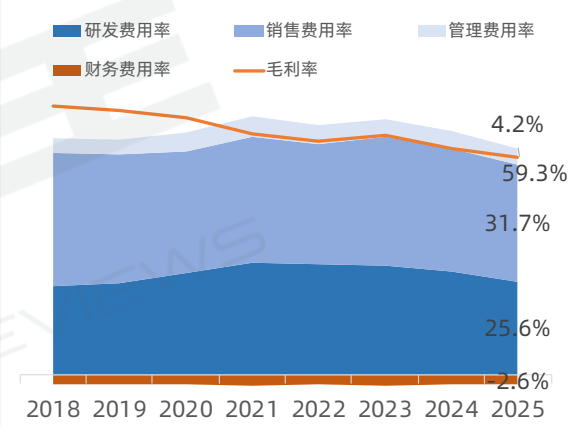


毛利情况

毛利(亿元)

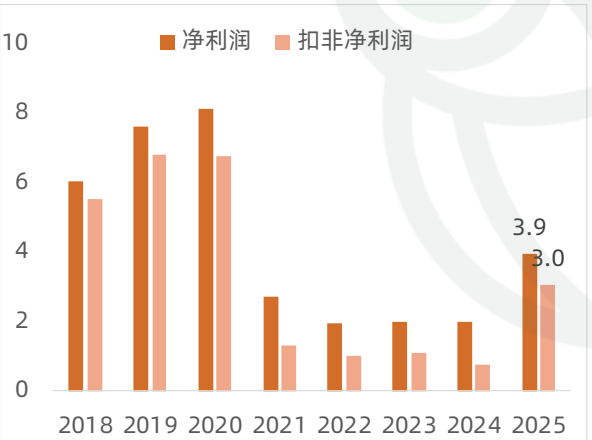


毛利率和费用率

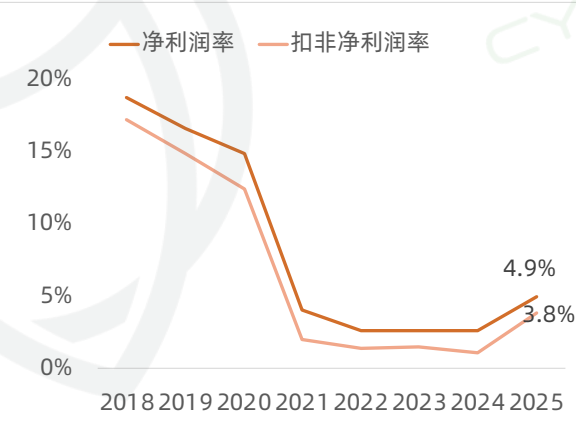


盈利情况

净利润（亿元）

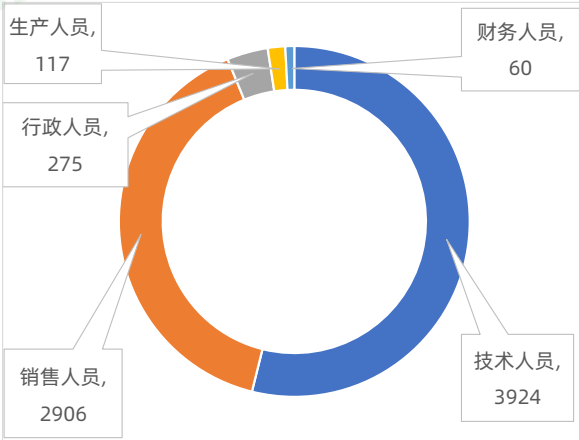


利润率

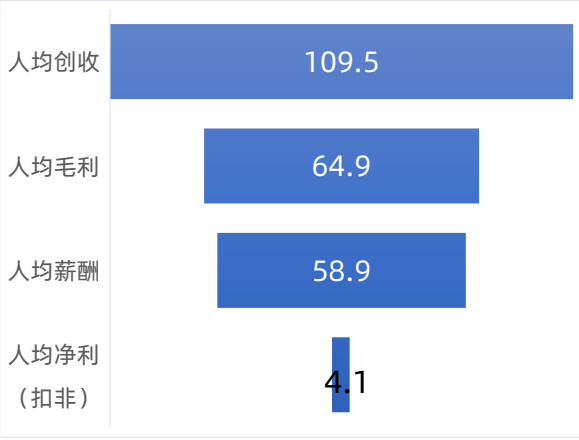


员工情况

员工构成

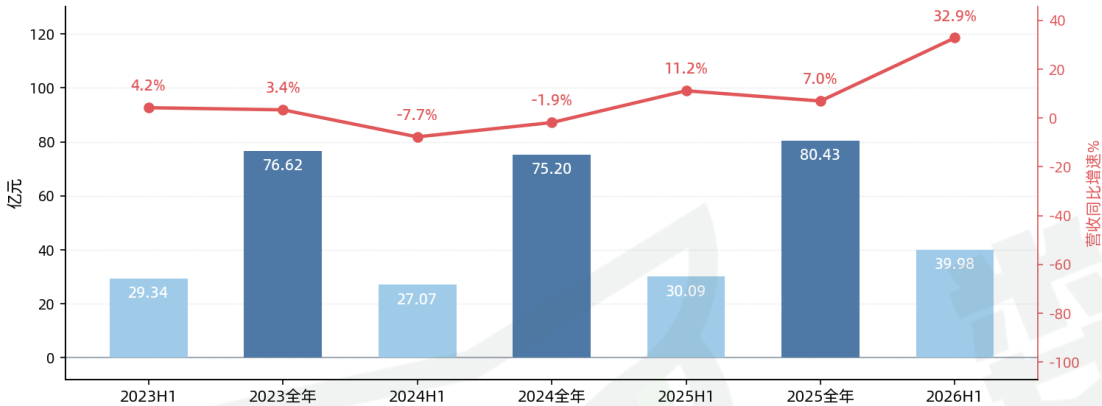


人均情况（万元）

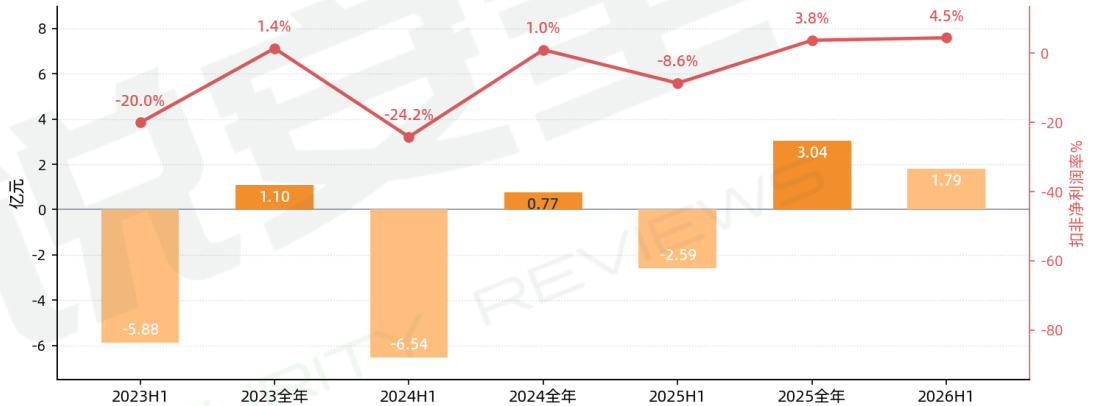


深信服2026年上半年营收39.98亿元、同比增长32.85%，为近五年最快；扣非净利润1.79亿元、扣非净利润率由-8.6%转正至4.5%。但毛利率60.89%、同比降1.20个百分点——增长由毛利率仅49%的云计算及AI基础设施业务贡献（+58.6%），高毛利网安业务仅增10.6%，收入结构向低毛利倾斜。经营性现金流净额-4.76亿元、净流出较上年同期扩大2.41亿元，规模扩张正在消耗营运资金。

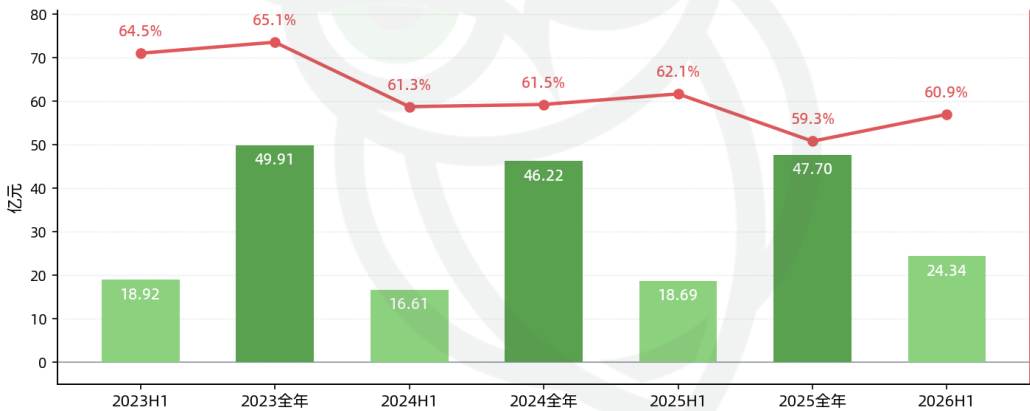
营业收入及同比增速



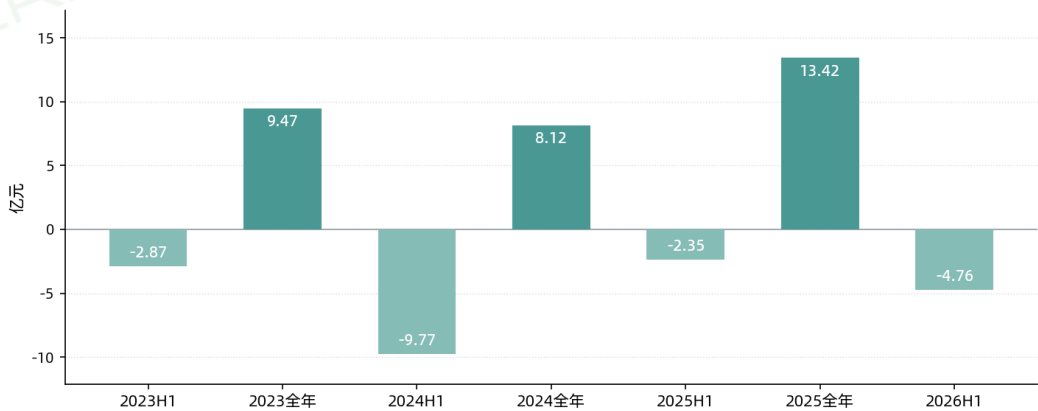
扣非净利润及扣非净利润率



毛利润及毛利率



经营活动现金流净额



浅色 = 半年度 (1-6月累计) 深色 = 全年度 右轴比率/增速

2025年经营情况回顾

2025年公司实现营业总收入25.72亿元，同比下滑8.81%，创2016年以来新低；网络安全产品收入21.52亿元，同比下滑15.62%，毛利率70.52%、提升7.57个百分点；智算云产品收入4.04亿元，同比增长57.95%，毛利率44.58%、提升2.18个百分点；公司综合毛利率提升5.27个百分点至66.30%；公司员工人数5160人，减少136人，其中研发人员2200人，减少111人、减员4.8%；销售人员1371人，减少44人、减员3.1%；公司人均创收49.2万元，较上年下降0.1万元；人均毛利32.6万元，较上年提升2.5万元。

- ◆ 利润端最大拖累是回款质量：信用减值损失8,005万元（其中应收账款坏账7,871万元）相当于全年扣非净利润的2.5倍，应收账款占营收已达105.2%，对扣非净利润形成明显拖累。
- ◆ 2025年宏观需求仍承压，但智算云成为新增长极、网络安全产品毛利率逆势升至70.52%，盈利质量改善与收入寻底并存。
- ◆ 公司持续推进提质增效，毛利率创新高，同时加强控费与回款管理，现金流净额1.63亿元。

2026年发展战略

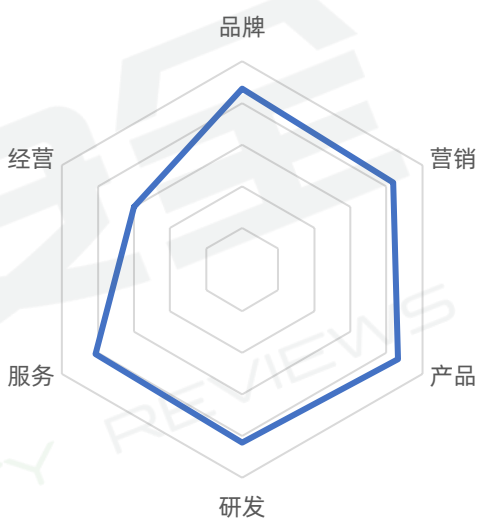
战略重点：

- I. "融智跃迁"双轮驱动：以"人工智能+"为引领，聚焦网络安全和智算云两大业务板块。
- II. AI全面内化：加速将AI内化于网络安全业务，强化AI应用安全、工业安全、数据安全、信创安全的领先优势。
- III. 智算云场景落地：以企业云、一体机、信创云核心产品的场景化适配抢占智算市场，提升市占率。

总结：

公司盈利质量正在改善，综合毛利率创历史新高，智算云成为收缩期里唯一高增长业务；但收入端尚未止跌，回款质量仍是利润最大不确定项。2026年将“继续提升销售毛利率”列入年度工作。

竞争力



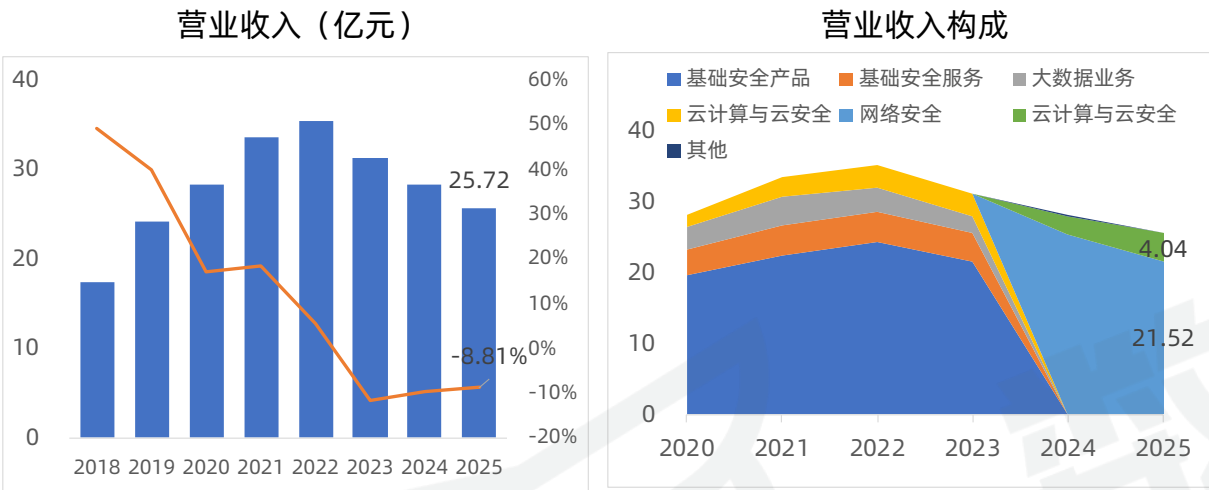
优势：

- ◆ 品牌影响力及市场占有率高。作为国内最早从事网络安全产品研发和销售企业，深耕网络安全领域20余年，积累了较为深厚的客户基础和资源，在行业内具备一定影响力和品牌号召力。
- ◆ 目前公司已构建较为成熟、可覆盖全国的营销和技术服务网络，直销销售能力出色，客户和行业覆盖能力突出，销售机会转化率高。

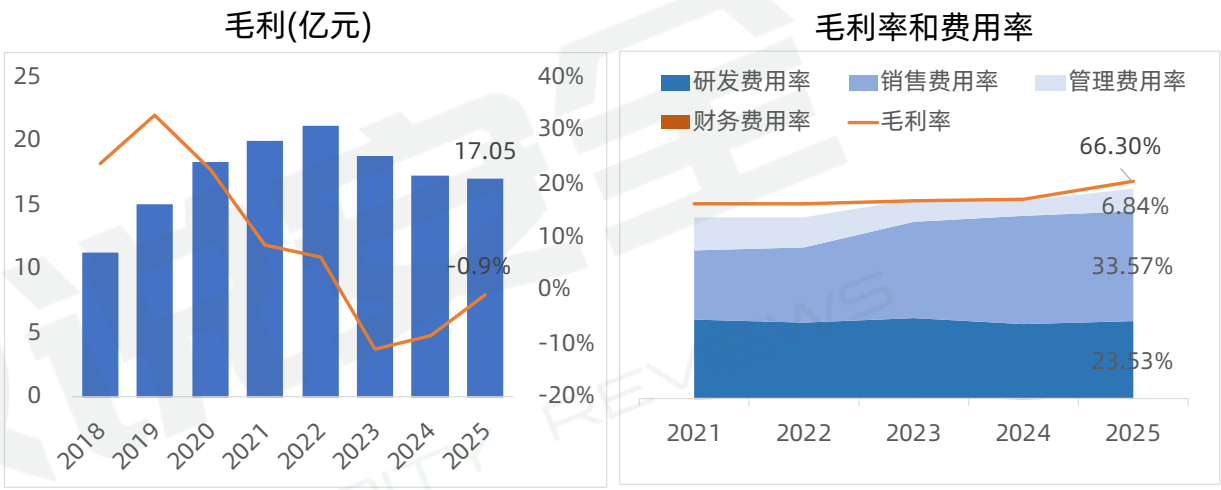
改进：

- ◆ 提升创新能力。公司应进一步加强创新投入，并提升产品创新过程中的管理能力和效率。
- ◆ 商誉余额较高。2025年天融信商誉余额为41.45亿元，若并购标的未能实现业绩预期，存在商誉减值风险，可能对公司净利润和资产进一步造成重大影响。

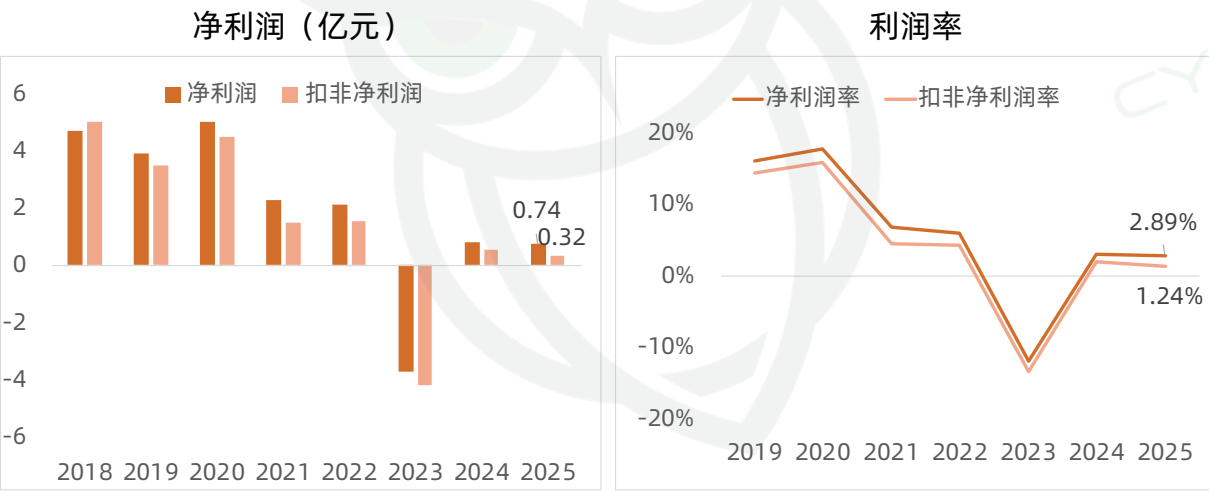
营业收入情况



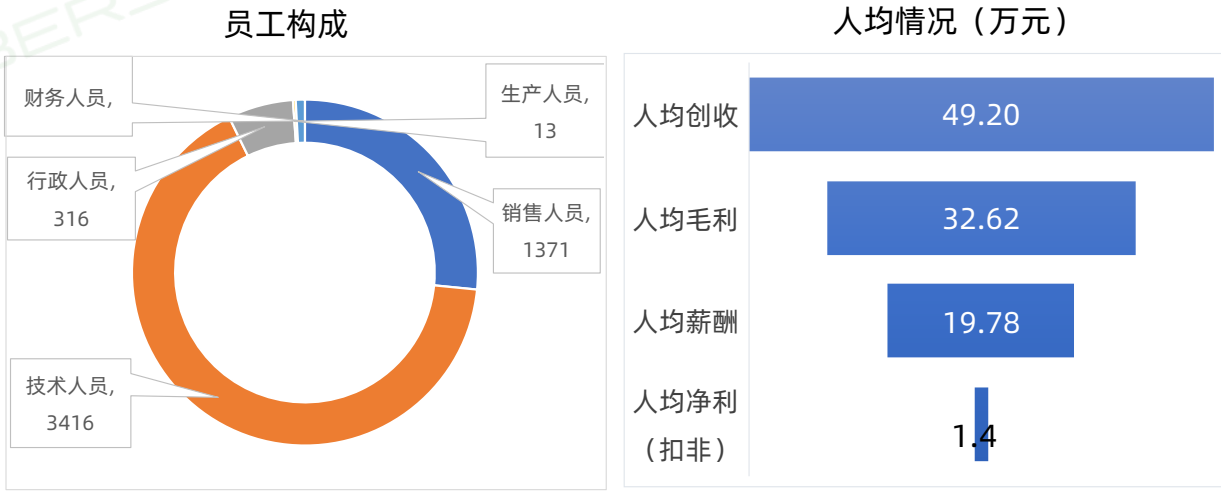
毛利情况



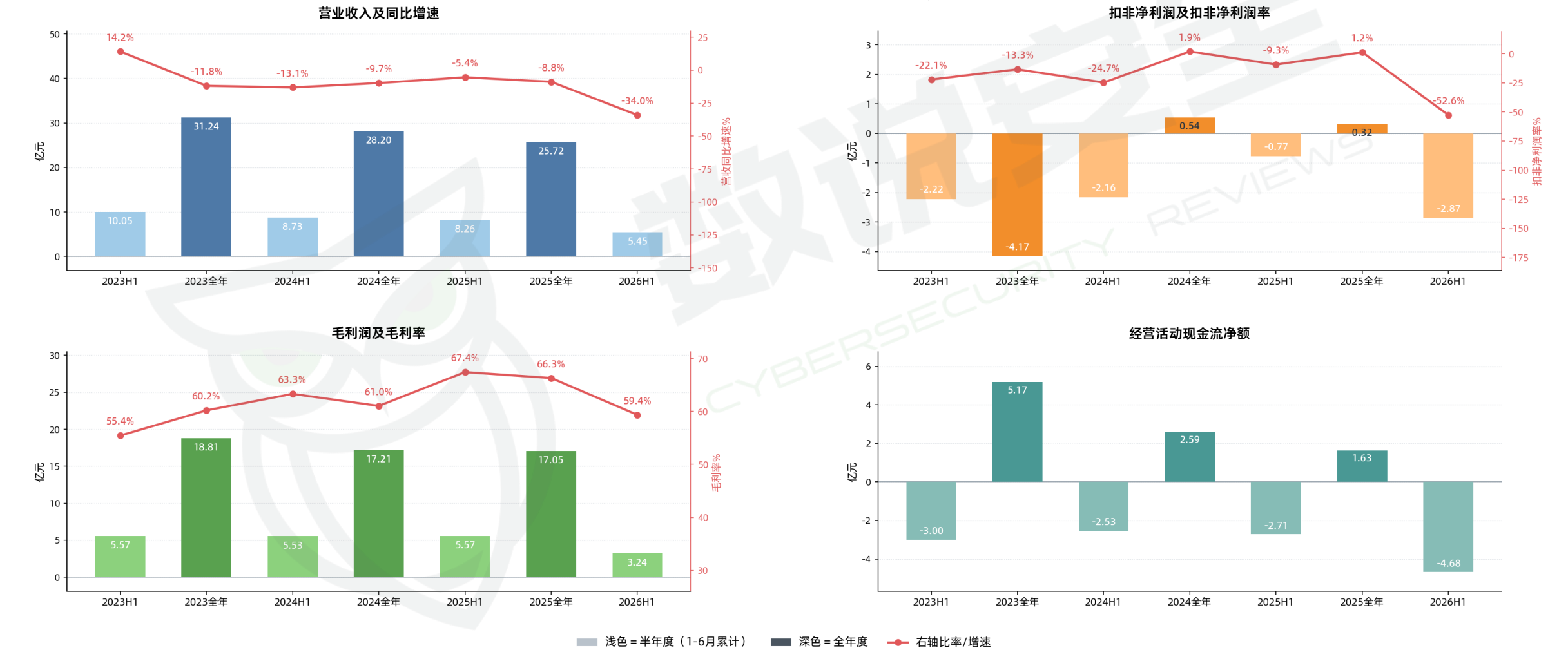
盈利情况



员工情况



天融信2026年上半年营收5.45亿元、同比下滑33.99%，降幅较大，且较上年同期的-5.38%急剧恶化。毛利率59.35%、同比降8.06个百分点；扣非净利润-2.87亿元，扣非净利润率由-9.3%骤降至-52.6%。经营性现金流净额-4.68亿元，净流出同比扩大1.97亿元。网络安全主业收入下滑43.0%是核心问题，智算云业务虽增长28.4%但仅占24%，且毛利率40.0%显著偏低，难以对冲主业收缩。



2025年经营情况回顾

2025年公司实现营业总收入22.68亿元，同比下滑8.08%，连续两年下滑；密码收入10.36亿元，同比下滑27.19%，毛利率53.04%、提升1.61个百分点；网络安全收入11.76亿元，同比增长26.18%，超越密码业务，成为收入的第一大来源，该业务毛利率24.13%、下降0.67个百分点；数据安全收入0.56亿元，同比下滑50.30%；公司综合毛利率下降3.21个百分点，达到37.56%；公司员工人数2398人，减少566人，其中研发人员780人，减少315人；销售人员267人，减少18人；公司2025年人均创收84.6万元，较上年提升2.3万元；人均毛利31.8万元，较上年下降1.8万元。

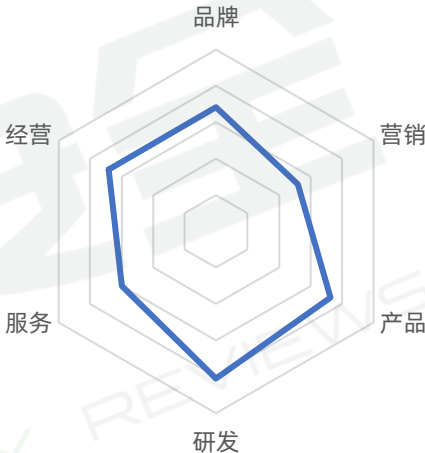
- ◆ 2025年宏观需求仍承压，密码业务收入大幅下滑27.19%，是利润端最核心的变量，但低毛利的网络安全业务+26.18%部分对冲了密码业务收缩。
- ◆ 现金流改善：经营性现金流净额3.14亿元，同比增加166.81%，由上年净流出转为净流入；扣非净利润同比下降67.64%，盈利仍承压。

2026年发展战略

- 战略重点：
- I. 密码深耕：继续巩固密码体系优势，推广云密码、行业密评密改产品，布局抗量子密码和卫星互联网密码。
 - II. 数据安全破局：聚焦纪检监察、医疗、政务等重点领域典型场景，通过标杆项目推动数据安全解决方案落地。

总结：公司定位仍是“以密码为核心的数据智能安全服务商”，但业务重心已实质切换——网络安全收入逆势增长26.18%、首次超越密码成为第一大收入来源。回款改善是真实的，经营性现金流净额同比增长166.81%，但主业盈利能力已跌至近五年谷底、综合毛利率仅37.56%。关键验证点是2026年密码业务能否企稳，这是判断公司能否真正筑底的核心。

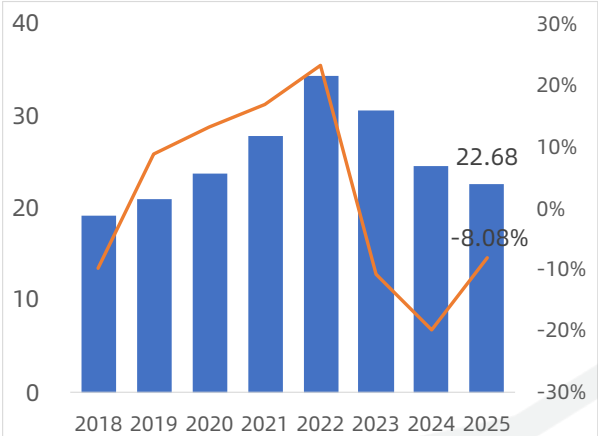
竞争力



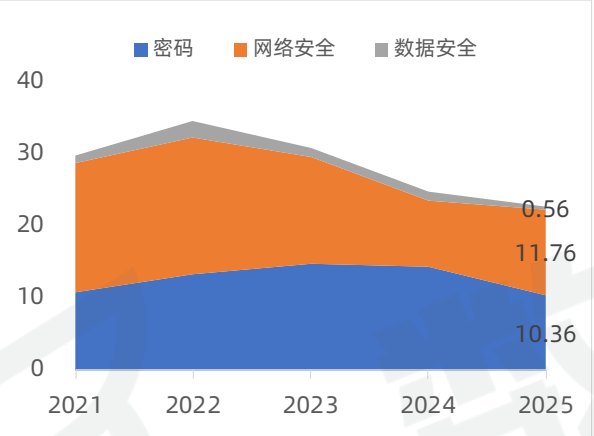
- 优势：
- ◆ 背靠电科大股东，资源优势明显。公司是中国电子科技集团有限公司旗下企业，是中国电子科技集团有限公司四大业务板块之一网络安全板块的重要资本运作平台和核心产业平台，具有值得客户信赖的央企背景，具备雄厚的技术实力、创新能力和资本运作能力，在支撑国家网络安全战略和赢得关键领域客户顶层信任方面具有天然的优势。
 - ◆ 公司拥有深厚的密码基因和能力积淀，是国内最早从事商用密码技术研究、产品研发与行业应用的企业之一。
- 改进：
- ◆ 资源与优势尚未深度挖掘。电科网安股东优势明显，公司应重新审视自身背景和资源优势，制定策略更加有效地利用这些资产，如通过市场定位、创新项目和战略合作，以进一步提升竞争力和市场影响力。

营业收入情况

营业收入 (亿元)

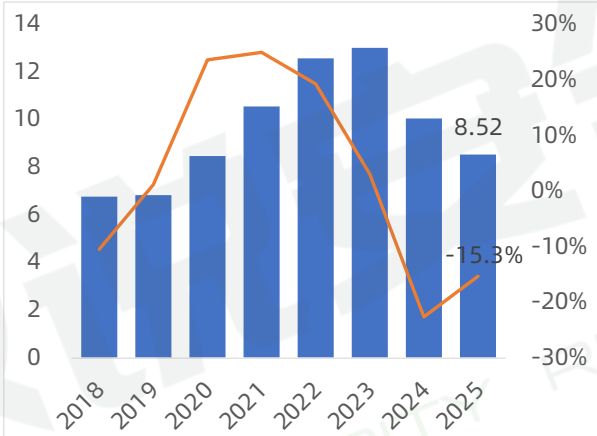


营业收入构成

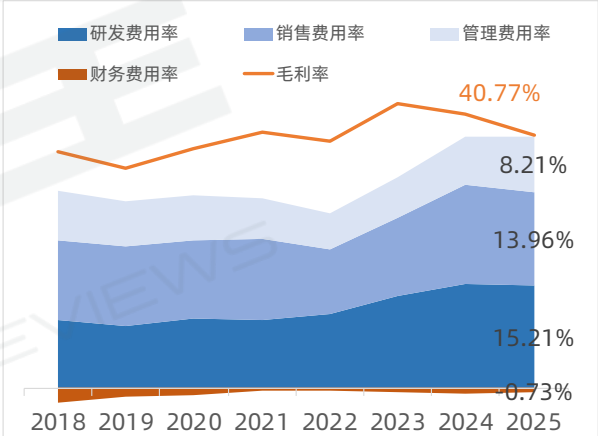


毛利情况

毛利(亿元)

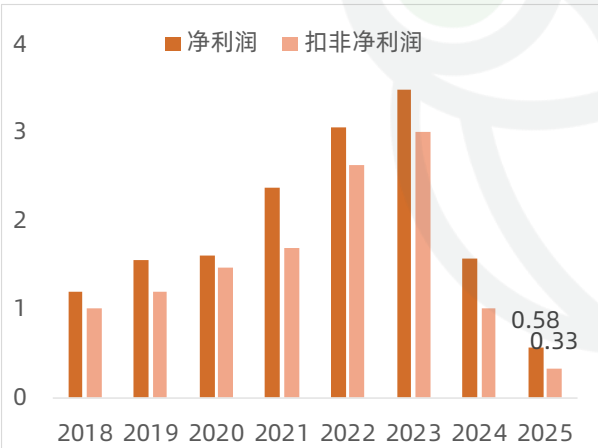


毛利率和费用率

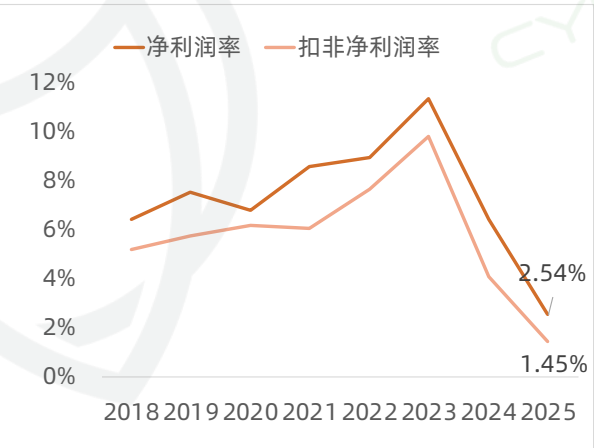


盈利情况

净利润 (亿元)

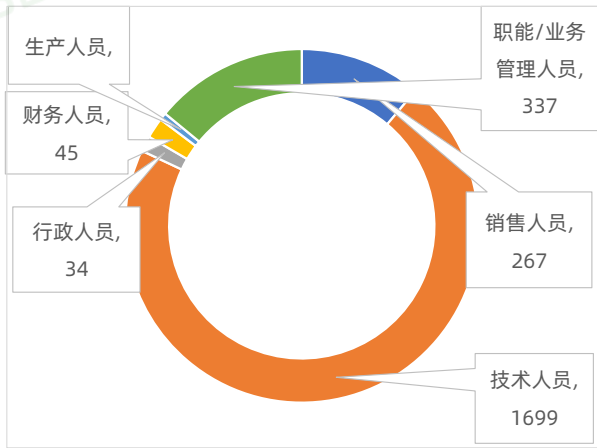


利润率

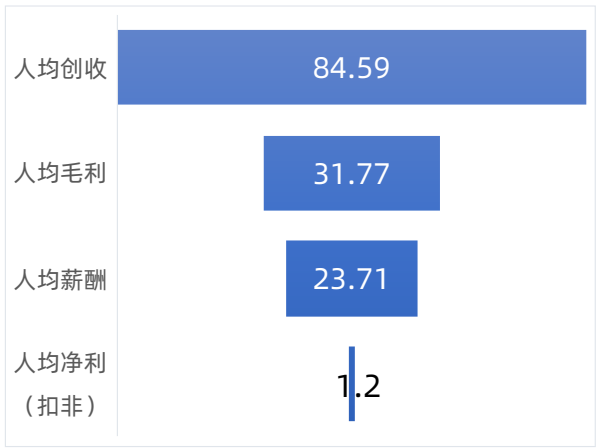


员工情况

员工构成

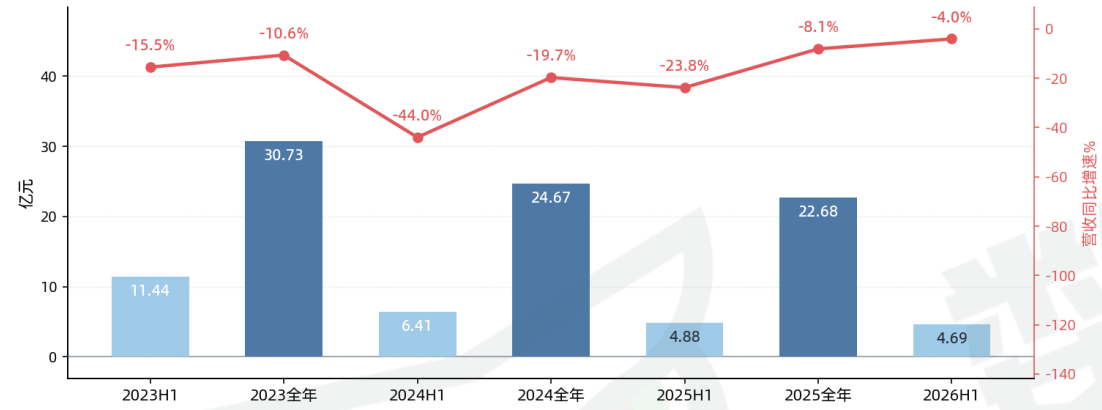


人均情况 (万元)

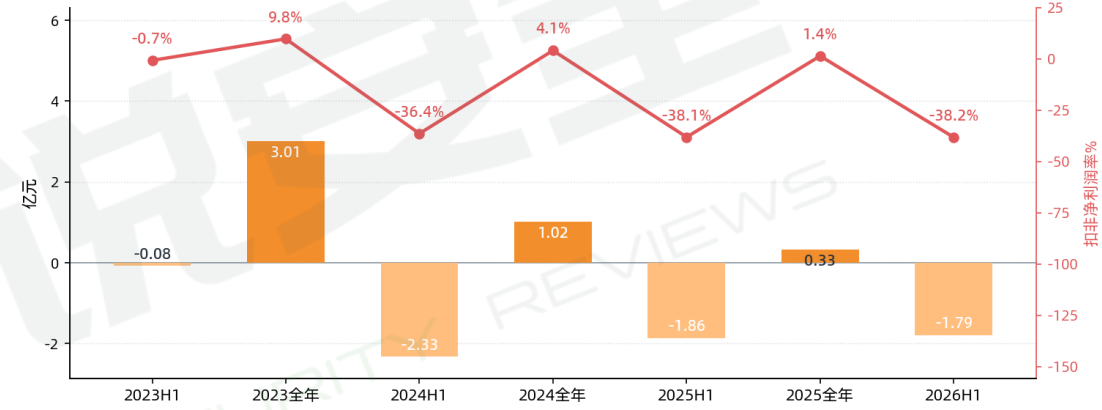


2026年上半年，电科网安营收4.69亿元，同比下降4.04%；扣非净亏损1.79亿元，同比收窄3.49%，但扣非净利润率仍约为-38.3%。毛利率由上年同期44.4%降至36.6%，收入和毛利仍承压。现金压力更为突出：经营性现金流净额-4.13亿元，较上年同期净流出0.81亿元明显扩大。当前修复重点是稳定业务毛利、改善回款，单纯减亏尚不足以说明经营已恢复。

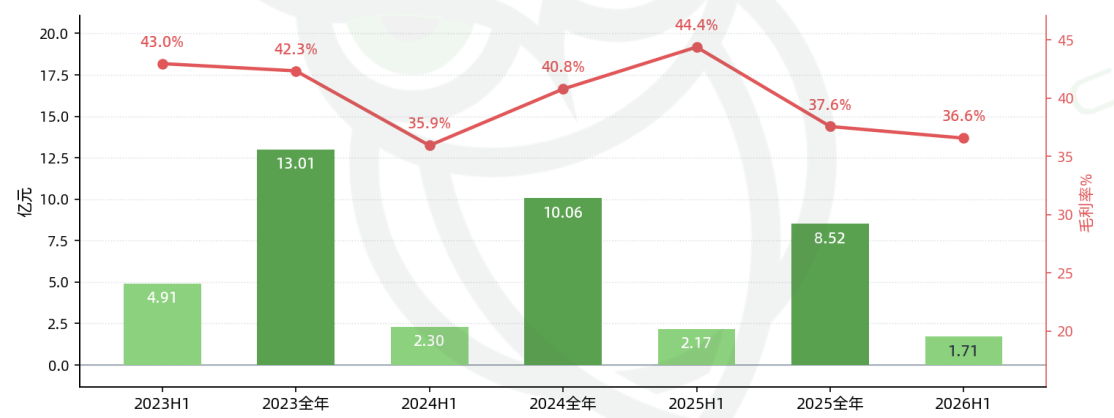
营业收入及同比增速



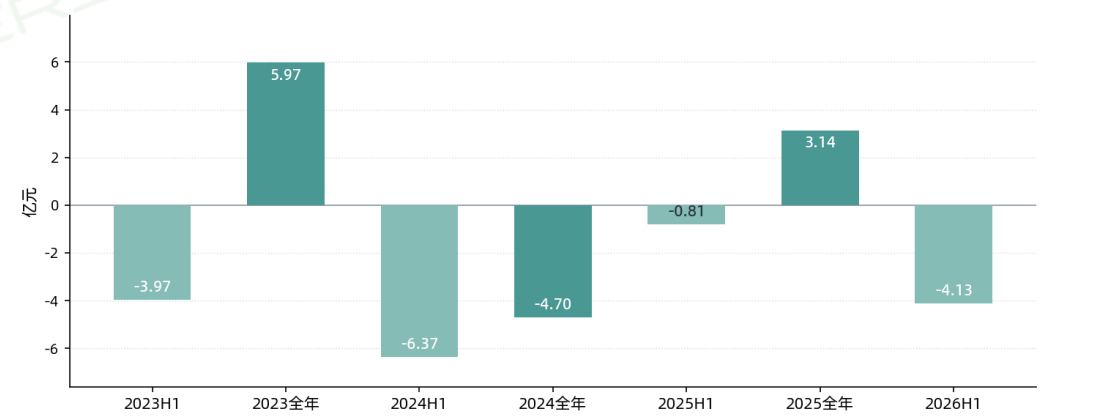
扣非净利润及扣非净利润率



毛利润及毛利率



经营活动现金流净额



浅色 = 半年度（1-6月累计） 深色 = 全年度 右轴比率/增速

2025年经营情况回顾

2025年公司实现营业总收入25.41亿元，同比增长7.78%，连续第二年回升；安全产品收入11.56亿元，同比增长1.60%，毛利率71.34%、提升3.47个百分点；安全服务收入9.97亿元，同比增长15.34%，毛利率52.37%、下降3.27个百分点；第三方产品和服务收入3.83亿元，同比增长8.06%，毛利率5.10%、提升0.64个百分点；公司综合毛利率提升0.08个百分点至53.88%；公司员工人数3149人，减少160人，其中研发人员1040人，减少42人、减员3.9%；销售人员619人，减少44人、减员6.6%；公司人均创收78.7万元，较上年提升14.0万元；人均毛利42.4万元，较上年提升7.6万元。

◆ Q4单季归母净利润+1.51亿元，相当于全年净亏损绝对额的约3倍，但全年仍亏损；四项费用合计-11.50%至14.15亿元，费用率从67.83%压至55.70%；经营现金流2.16亿元、同比+58.61%，近五年最高。AI安全相关订单额新增1.45亿元，产品订阅与软件服务化收入4.3亿元（+21%）。

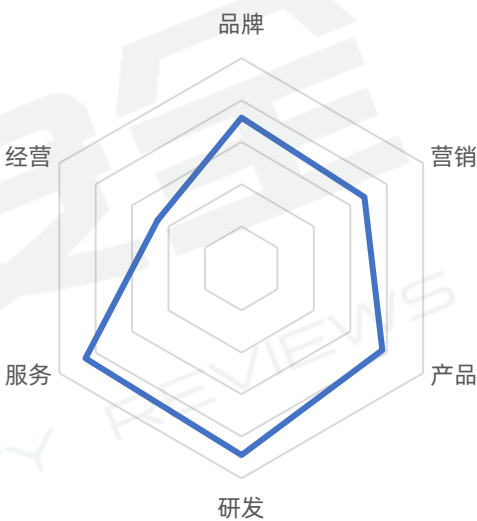
2026年发展战略

- 战略重点：
- I. "3+3+X+Y"价值客户战略：聚焦电信运营商、金融、能源三大价值行业。
 - II. AI安全双轮驱动：以"风云卫AI安全能力平台"落地智能体安全运营，MDR平台AI独立接管率已达80%；清风卫AI安全产品系列覆盖"评估-防护-响应"全链路。
 - III. 数据安全要素化：以数据保险箱和可信连接器构建数据要素安全基础设施，参与国家数据局可信数据空间试点。

总结：

2026年以实现盈利为目标，并构建营业收入、应收回款、经营现金流与利润之间的动态平衡体系。2025年已是三年亏损周期的拐点年，扣非亏损收窄86.16%，但尚未实现全年盈利，关键验证点是应收账款（已达营收49%、同比增长26.59%）能否止住上行。

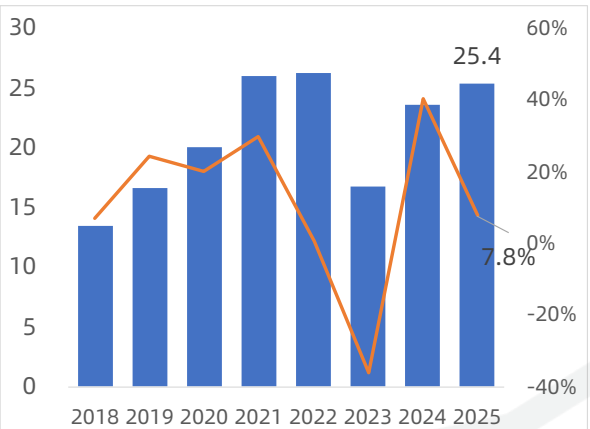
竞争力



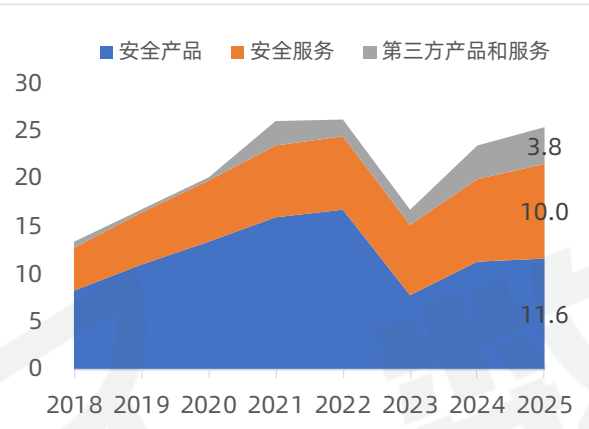
- 优势：
- ◆ 安全服务能力突出。公司服务体系及服务网络搭建完善，相继提出P2SO战略，T-ONE CLOUD 战略，发布风云卫安全大模型，提升工程交付效能，持续强化公司的安全服务能力和安全运营能力。
 - ◆ 市场认可度高。公司是国内信息安全行业的资深企业，具备深厚的历史积淀和全面的技术产品覆盖，其抗DDoS硬件安全产品和WEB应用防护系统等多款产品市占率国内领先，而且在安全服务领域也展现出强大的实力和专业性，成功为多个重大活动提供网络安全保障技术支持，凭借其卓越的技术实力和创新能力，获得了市场的高度认可和用户的深度信任。
- 改进：
- ◆ 经营的稳定性和健康性亟需加强。2025年公司经营情况明显好转，收入、现金流等指标快速恢复，但仍有一些关键指标未能真正恢复，如安全产品收入恢复较慢、综合毛利率依然较低、整体现金流情况依然紧张等，公司仍需将经营的稳定和健康作为重要的目标，从波动中尽快真正恢复至稳定增长状态。

营业收入情况

营业收入（亿元）

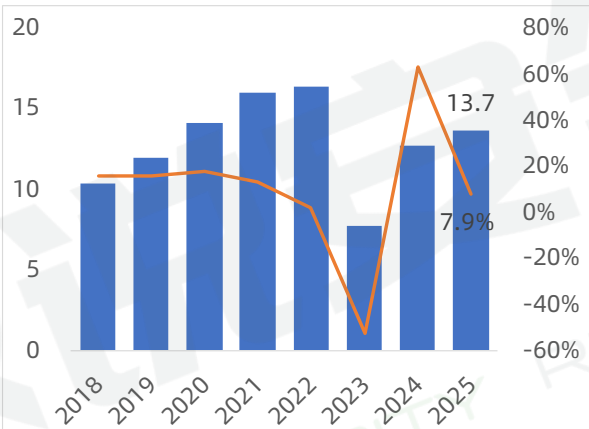


营业收入构成

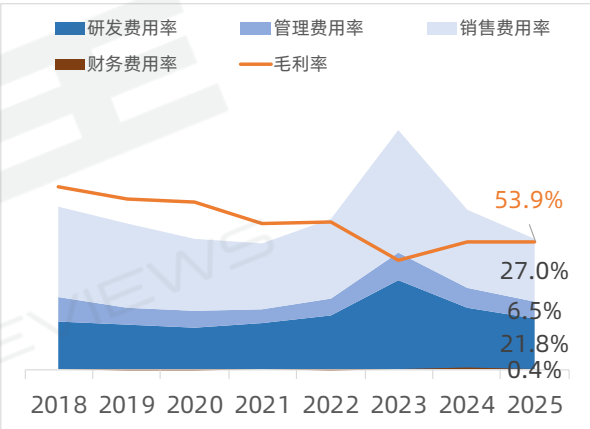


毛利情况

毛利(亿元)

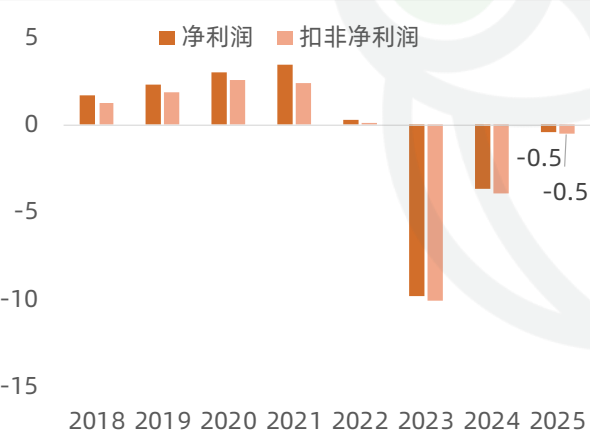


毛利率和费用率

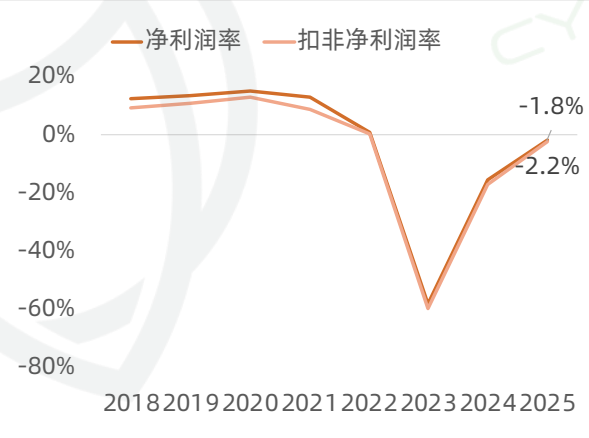


盈利情况

净利润（亿元）

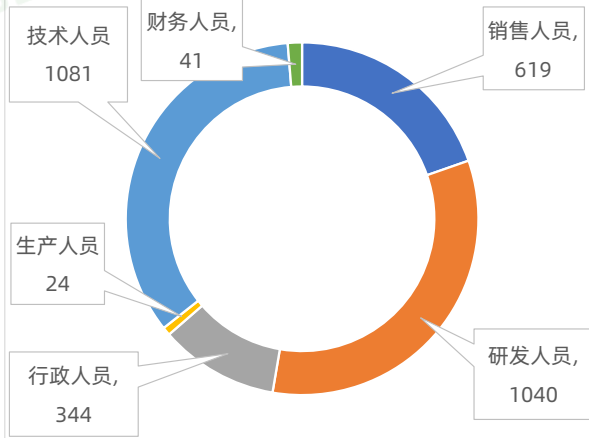


利润率

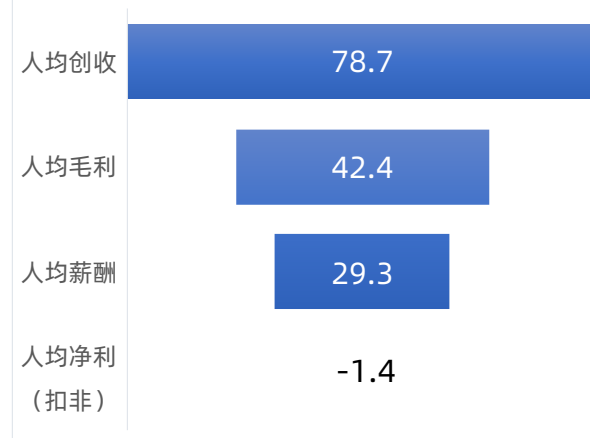


员工情况

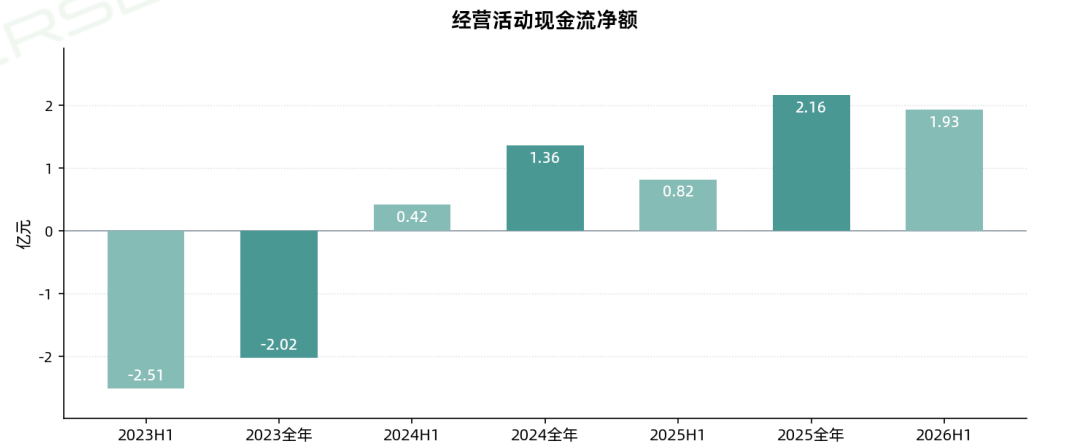
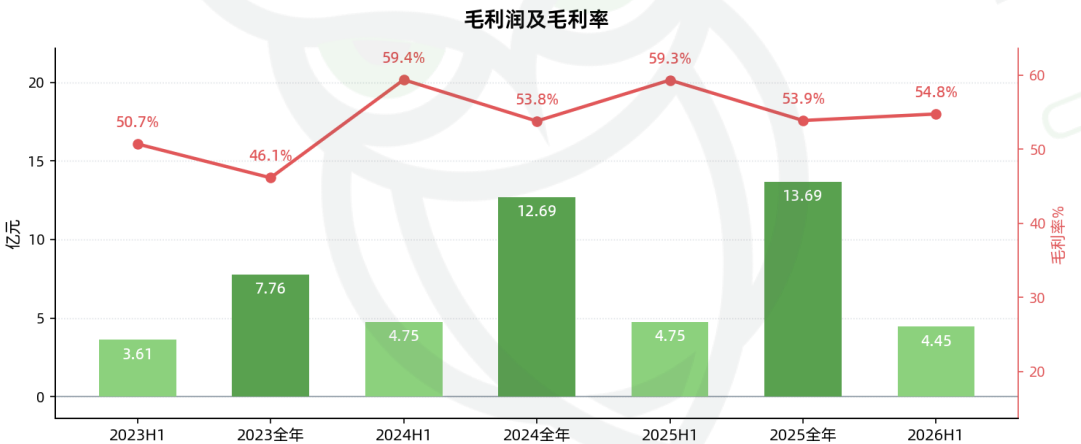
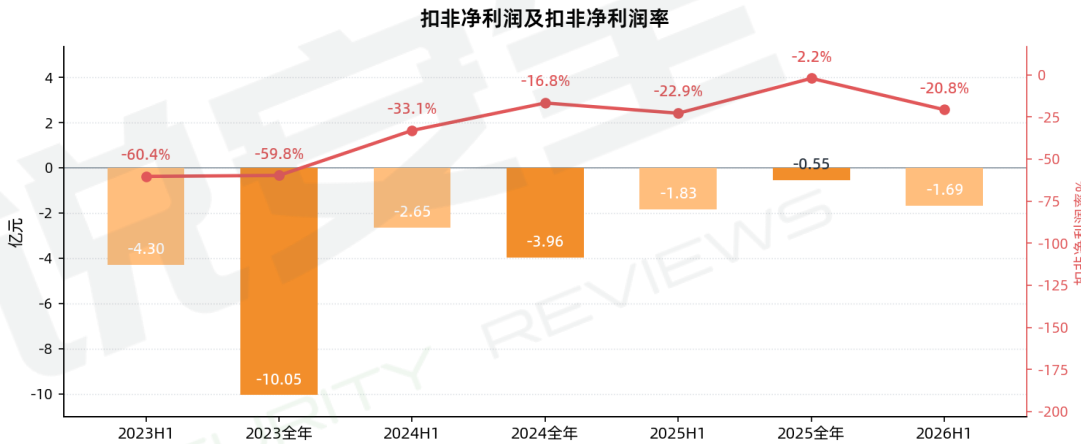
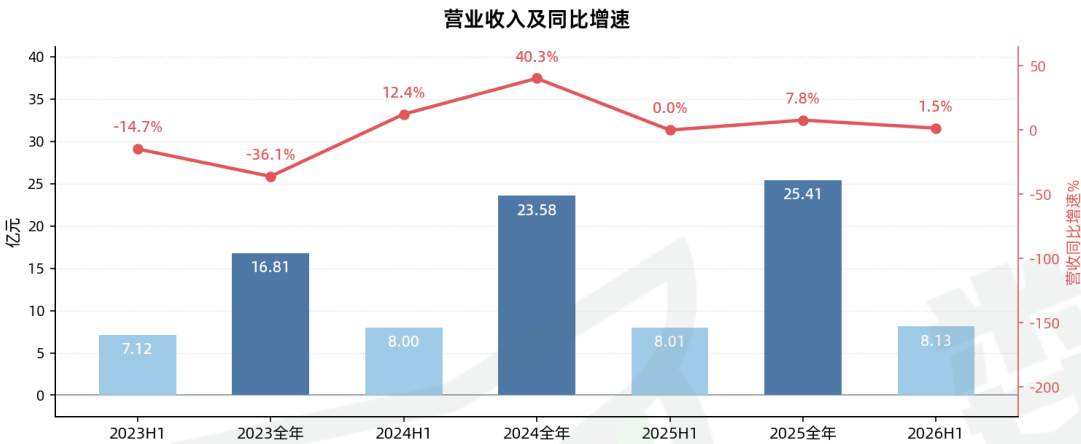
员工构成



人均情况（万元）



2026年上半年，绿盟科技营收8.13亿元，同比增长1.51%；扣非净亏损1.69亿元，同比收窄7.47%，仍未实现盈利。毛利率由上年同期59.3%降至54.8%，毛利润由4.75亿元降至4.45亿元，收入微增尚未带来毛利增长。现金流改善更明显：经营性现金流净额1.93亿元，同比增长136.05%。公司回款表现改善，但利润修复仍需毛利率企稳和费用控制共同支撑。



浅色 = 半年度（1-6月累计） 深色 = 全年度 右轴比率/增速

2025年经营情况回顾

2025年公司实现营业总收入21.51亿元，同比增长5.32%，结束2024年下滑、重回增长；网络信息安全基础产品收入3.99亿元，同比下滑4.20%，毛利率75.63%、提升2.94个百分点；网络信息安全平台收入7.68亿元，同比增长2.52%，毛利率70.75%、提升3.15个百分点；网络信息安全服务收入8.17亿元，同比增长8.68%，毛利率54.65%、提升4.27个百分点；公司综合毛利率提升1.80个百分点至61.90%；公司员工人数3516人，减少88人，其中研发人员790人，减少180人、减员18.6%；销售人员773人，减少291人、减员27.3%；公司人均创收60.4万元，较上年提升5.8万元；人均毛利37.4万元，较上年提升4.6万元。

- ◆ 四项费用合计13.26亿元，同比-8.34%，费用率从70.8%压至61.6%，销售费用率从37.46%降至32.80%、研发费用率从24.11%降至20.41%，费用压降是利润修复的核心驱动。
- ◆ 2025年经营性现金流3.53亿元，同比+119.16%，连续两年为正且创上市以来新高。但资产减值损失8,483万元是利润未能转正的主要拖累，盈利拐点尚未到来。

2026年发展战略

战略重点：

- I. AI战略全面深化：恒脑安全垂域大模型持续迭代，智能体框架和MCP协议全面接入，AI安服数字员工实现订阅化交付。
- II. 综合经营管理模式全国落地：各区域从单一业绩考核转向经营考核，大多数区域经营质量改善。
- III. 订阅化推进：MSS业务结合维保续订、威胁情报、AI智能体等，持续提高订阅式收入比例。

总结：

公司已把AI提升为公司级战略，分“AI+安全”“以AI管AI”“智能体提效”三个层次推进，商业模式上把各分公司改造为独立核算的经营单位、持续提高订阅式收入比例。

竞争力



维度	竞争力得分（0-100）
品牌	65
营销	70
产品	75
研发	90
服务	85

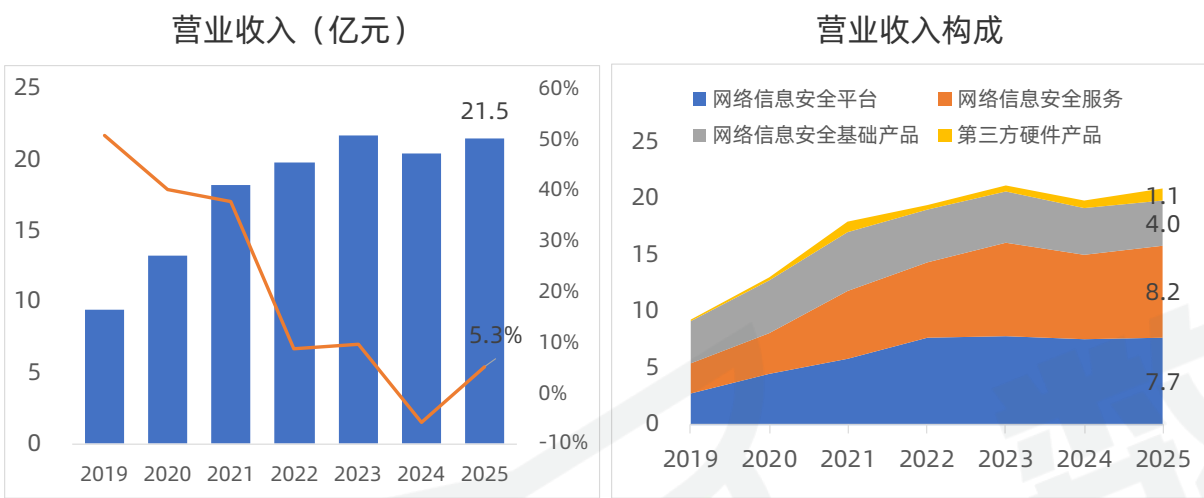
优势：

- ◆ 战略的开拓创新性强。作为新兴的网络安全企业，公司在“云、大、物、智、工”领域深耕，拓展应用场景；在数据安全、MSS、大数据态势感知、信创安全等战略新方向上加强投入，将AI提升为新的重点战略，不断完善公司产品竞争力，清晰的战略发展让公司的收入快速增长，实力迅速提升。
- ◆ 安全服务能力优异。公司安全服务占收入比重在行业中领先，并初步实现了全国网络安全运营的纵深化布局，建立四个一级安全运营能力中心和20多个二级城市级安全运营中心，并将向三四线城市拓展；公司也不断推动MSS安全托管运营服务，帮助客户构建有效闭环的安全运营体系；公司同时打造了专业的安服团队，具备为客户提供规划、建设、运维、应急响应一体化的安全服务能力。

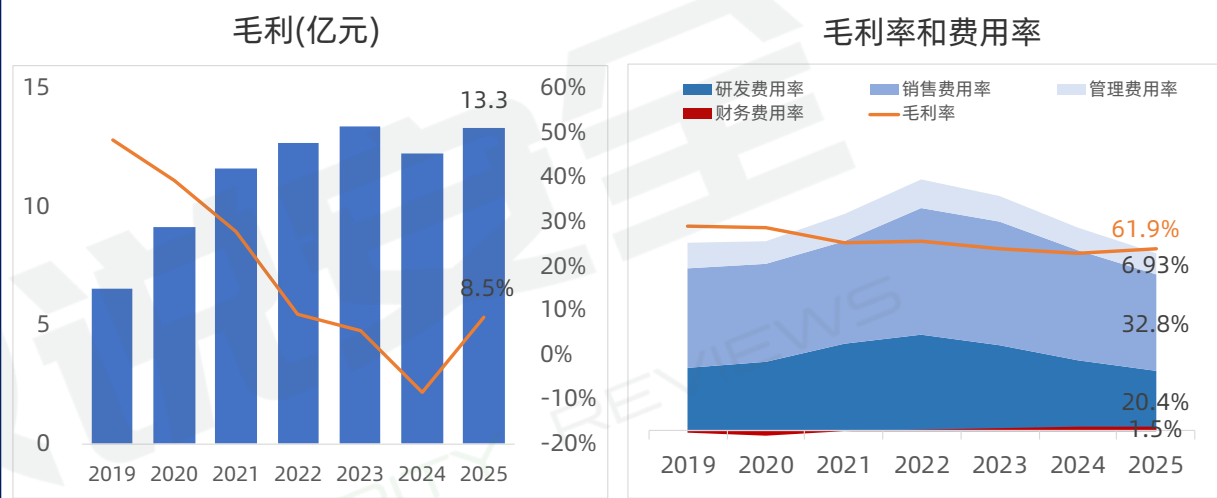
改进：

- ◆ 营销网络及策略升级调整。公司原有的营销网络和策略，无法有力支撑现有的战略发展及收入增长，亟需做出调整升级，突破路径依赖。
- ◆ 强化技术创新落地能力。公司在加大技术研发创新的同时，也需兼顾场景化开拓及市场落地，增强相关能力，以更好地适应市场的发展和需求。

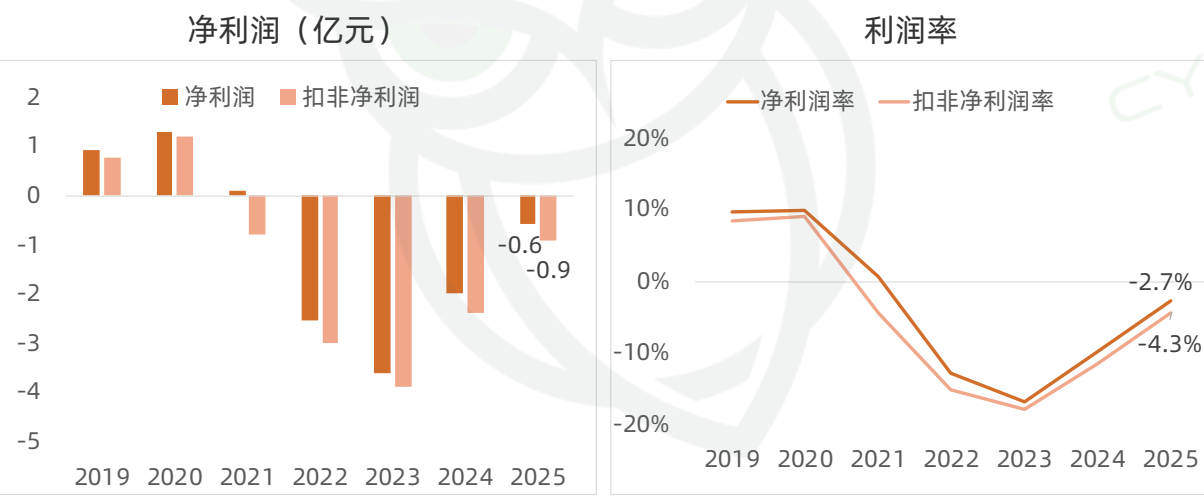
营业收入情况



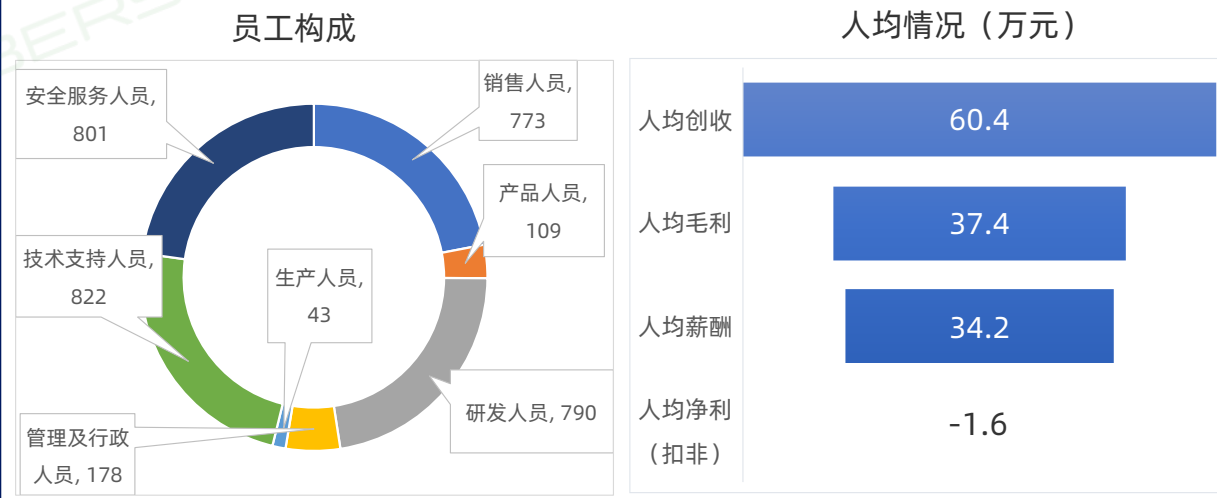
毛利情况



盈利情况

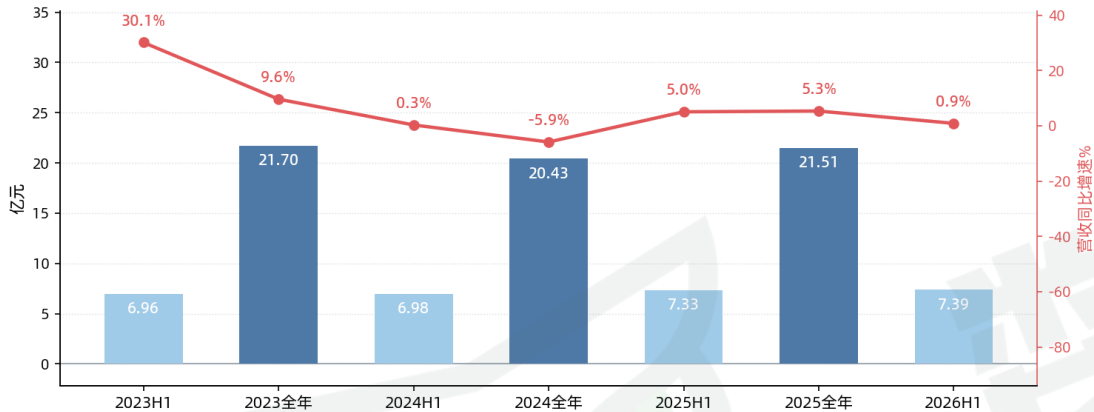


员工情况

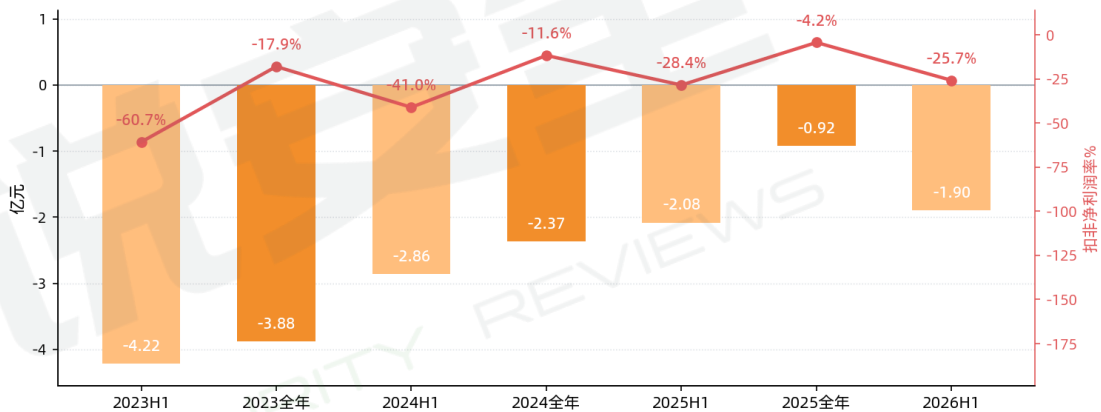


2026年上半年，安恒信息营收7.39亿元，同比增长0.86%；扣非净亏损1.90亿元，较上年同期2.08亿元收窄约8.7%，扣非净利润率由-28.4%改善至-25.8%。毛利率由55.8%升至56.6%，业务毛利有所改善，但收入增长仍较弱。经营性现金流净额-3.94亿元，较上年同期净流出3.21亿元扩大约0.73亿元。利润与现金流改善尚不同步，后续需关注收入恢复和回款节奏。

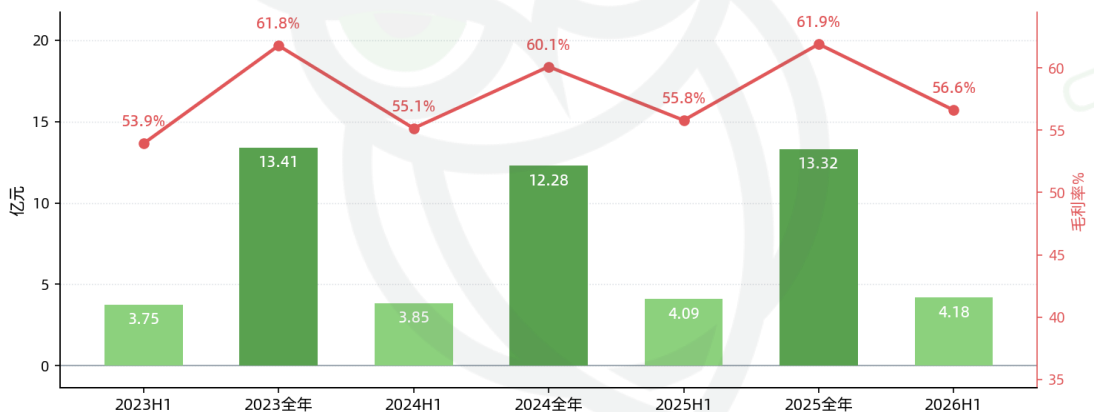
营业收入及同比增速



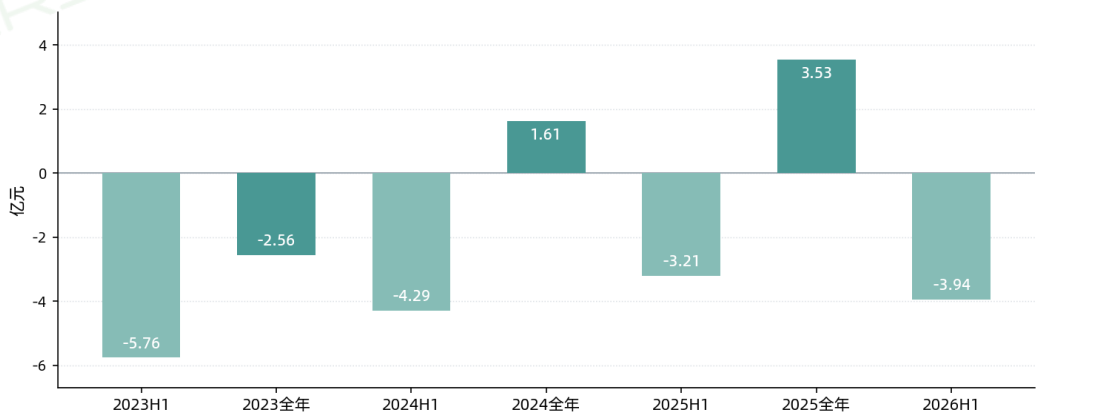
扣非净利润及扣非净利润率



毛利润及毛利率



经营活动现金流净额



浅色 = 半年度 (1-6月累计) 深色 = 全年度 右轴比率/增速

2025年经营情况回顾

2025年公司实现营业总收入12.18亿元，同比增长5.49%，连续第三年正增长、创历史新高；网络安全产品收入7.01亿元，同比下滑8.54%，毛利率68.67%、下降2.03个百分点；应用交付及网络产品收入3.95亿元，同比增长37.25%，毛利率55.59%、下降6.73个百分点；安全服务及其他服务收入1.13亿元，同比增长24.15%，毛利率50.46%、下降12.38个百分点；公司综合毛利率下降4.41个百分点至62.87%；公司员工人数1577人，减少149人，其中研发人员542人，减少80人、减员12.9%；销售人员470人，减少48人、减员9.3%；公司人均创收73.8万元，较上年提升6.2万元；人均毛利46.4万元，较上年提升0.9万元。

- ◆ 综合毛利率62.87%，同比下降4.41个百分点，是近五年最低，结构性下移（网络产品占比提升、低毛利）是主因；四项费用合计6.25亿元，同比-9.00%，费用率从59.43%降至51.27%。
- ◆ 2025年经营性现金流1.53亿元，同比-53.44%（上年3.28亿元），需关注应收回款节奏；人均营收73.76万元（同比+9.10%），连续第三年回升。

2026年发展战略

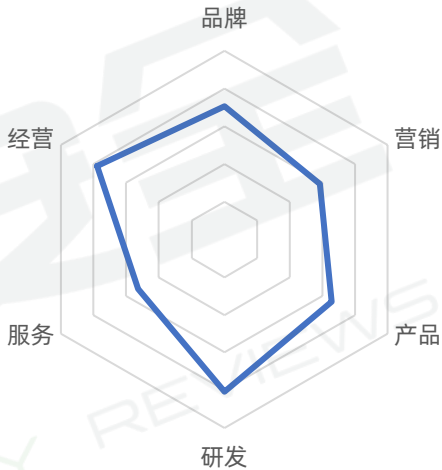
战略重点：

- I. 创新驱动与客户价值：坚持高额研发投入和自主创新，聚焦客户价值创造，持续完善产品质量管理体系。
- II. 组织优化与行业拓展：推进营销体系数字化转型，加大对运营商、电力能源、金融等高价值行业的覆盖广度与应用深度。

总结：

迪普的战略表述在同行中最为克制，核心是“有序扩张、有效增长”——不追规模扩张，靠高额研发投入维持产品竞争力，客户端集中投向运营商、电力能源、金融等高价值行业，把盈利质量放在收入增速之前。2025年收入增长5.49%、扣非增长8.11%，是行业内少数持续盈利的公司。

竞争力



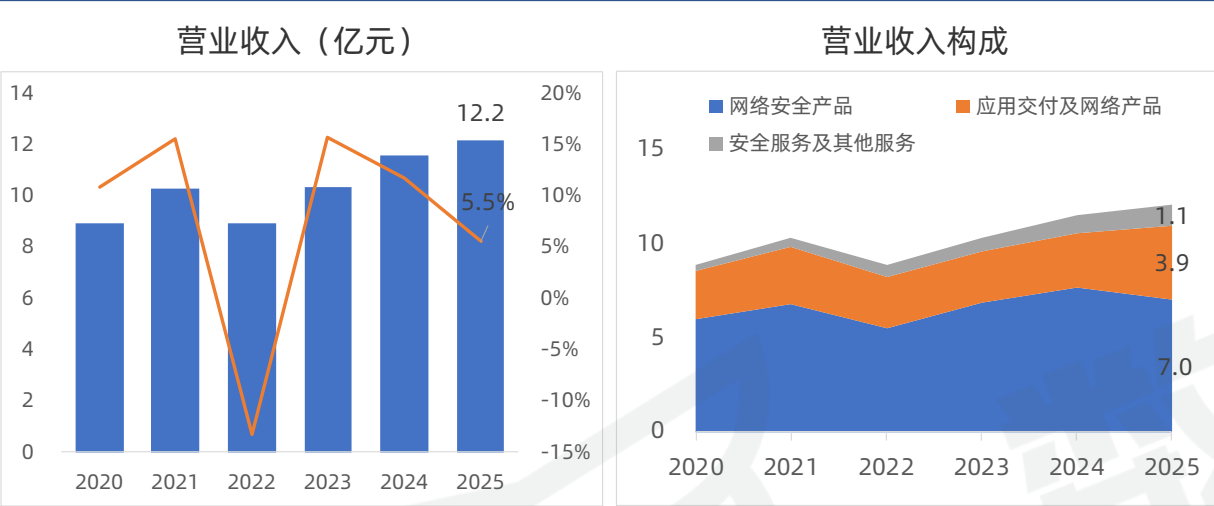
优势：

- ◆ 经营活动稳定健康。近五年来，公司的收入增速、毛利率、利润都较为稳定，应收账款金额及周转天数都维持在较低的水平，收现比维持在1以上；在2023年宏观环境的影响下，净利润和经营性现金流净额虽然出现了一定程度的下滑，但是一直为正值，并且总资产中有70%的比重都是货币资金，综合财务指标在行业中都处于领先地位，标志着经营活动一直在健康、稳定地开展。
- ◆ 营销体系不断扩充完善。公司在全国设立了28个一级办事处以及7个二级办事处，持续优化渠道管理，2019-2022年渠道合作伙伴数量从1700家提升至2500家，渠道销售收入比重维持在60%以上，不断完善的渠道帮助公司稳步扩大规模。

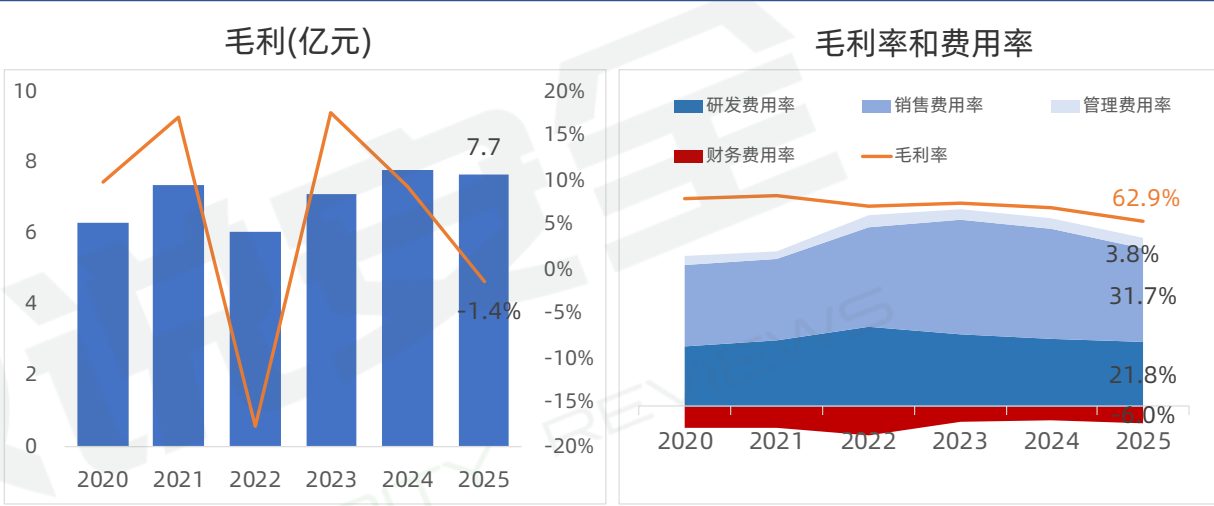
改进：

- ◆ 保持健康经营状态的前提下，有效突破收入规模及增速瓶颈。2025年收入站上12亿元，但在大环境疲软的情况下，需要进一步优化经营策略，稳住毛利率，实现收入和利润的有序增长。
- ◆ 进一步提升产品创新能力。公司需要加大新型产品和解决方案创新力度，加强研发创新投入，优化策略，寻找到新的业务增长点。

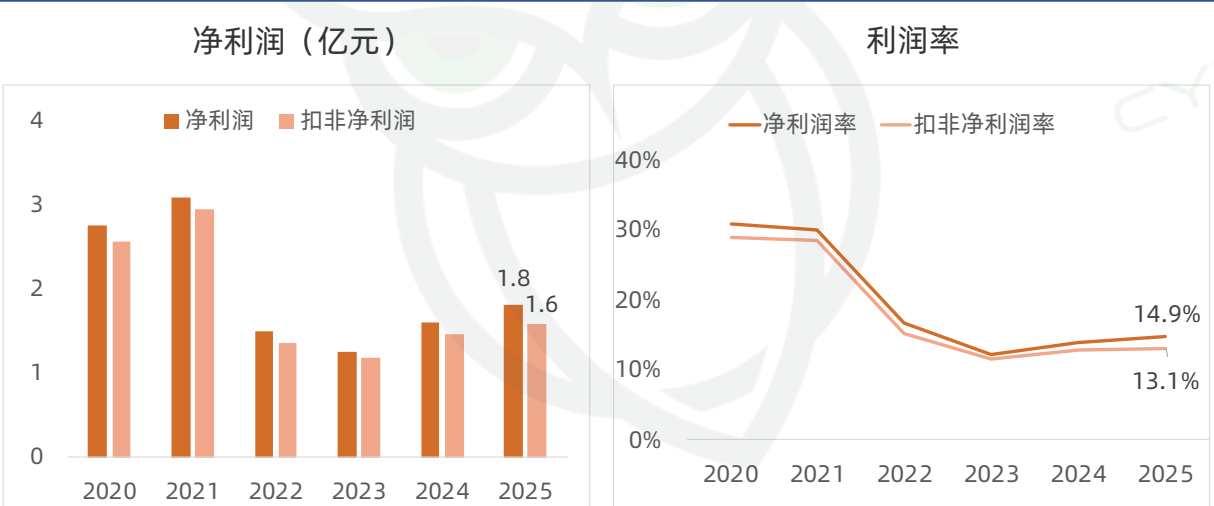
营业收入情况



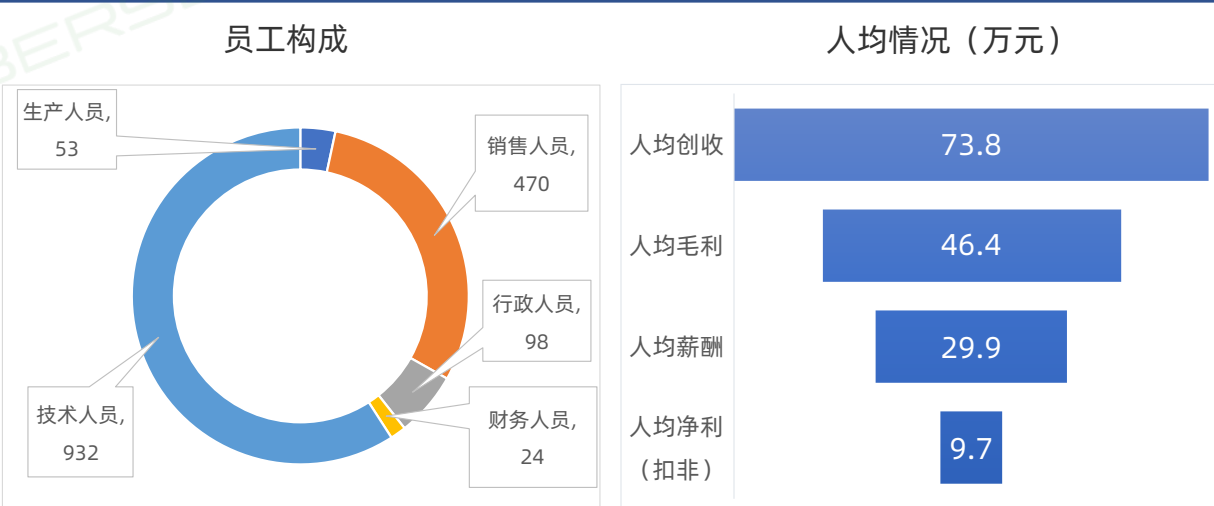
毛利情况



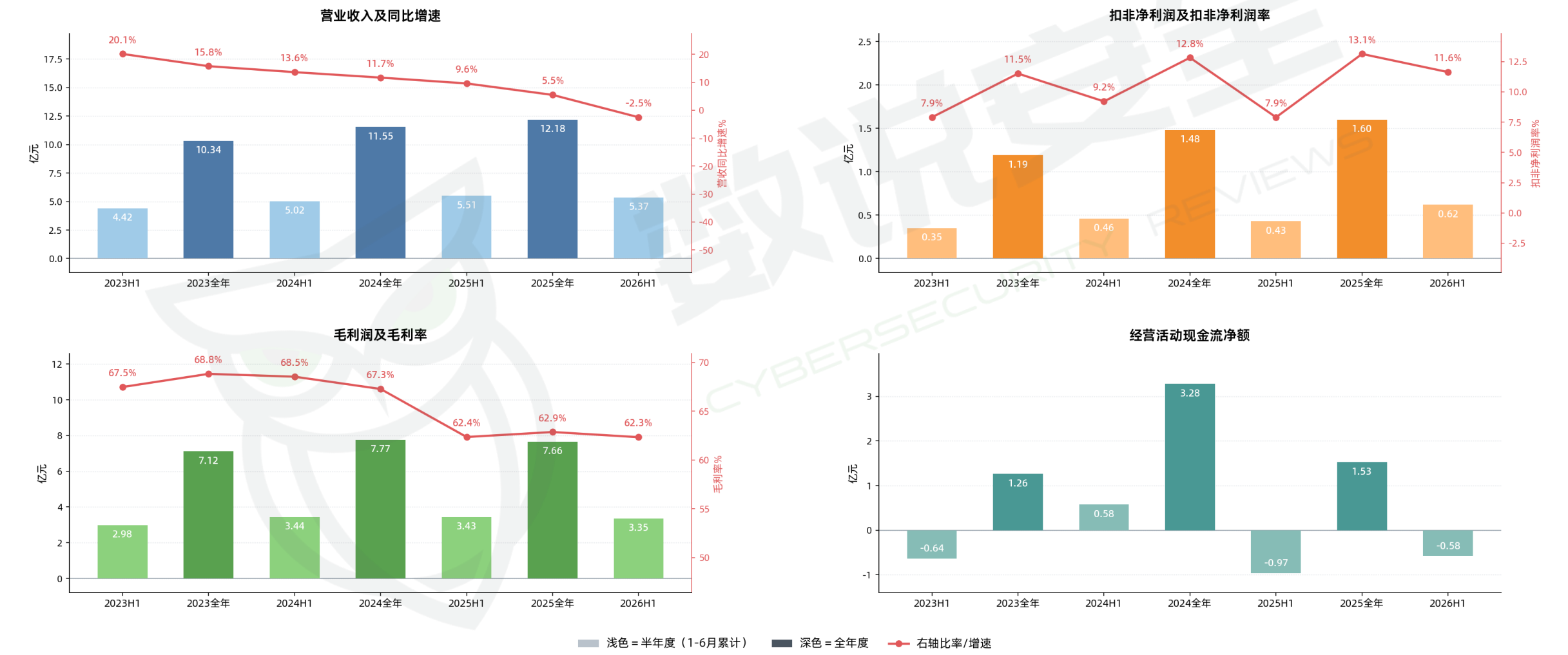
盈利情况



员工情况



2026年上半年，迪普科技营收5.37亿元，同比下降2.52%；扣非净利润0.62亿元，同比增长43.59%，扣非净利润率由7.9%升至11.6%。毛利率约62.3%，与上年同期62.4%接近，毛利润略降，说明本期利润增长并非主要来自毛利扩张。经营性现金流净额-0.58亿元，净流出同比收窄约0.40亿元。公司盈利表现改善，但收入尚未恢复增长，利润能否持续转化为现金仍需观察。



2025年经营情况回顾

2025年公司实现营业总收入9.11亿元，同比下滑8.55%，为战略调整期最后一年；边界安全产品收入6.74亿元，同比下滑9.94%，毛利率69.63%、下降2.34个百分点；云安全产品收入0.79亿元，同比增长56.56%，毛利率91.87%、提升2.21个百分点；公司综合毛利率下降2.65个百分点至67.33%；公司员工人数1404人，减少259人，其中研发人员621人；销售人员285人；公司人均创收59.4万元，较上年提升0.9万元；人均毛利40.0万元，较上年下降1.0万元。

- ◆ 2025年最大亮点不在当年财报而在硬件底座：押注三年的自研ASIC安全专用芯片实现量产落地，首批集成芯片的防火墙已发布、新品2026年初已多行业中标；云安全收入0.79亿元、同比+56.56%。
- ◆ 信用减值3,726.76万元、资产减值2,957.01万元双双扩大，综合毛利率67.33%（-2.65pct），盈利拐点仍未到来。
- ◆ 经营现金流-1.10亿元连续五年为负，短期借款增至3.95亿元，现金端仍是关键约束。

2026年发展战略

战略重点：

- I. "双A战略"贯彻：以自研ASIC芯片与AI智能技术为双引擎，推进ASIC产品规模化落地与国产替代。
- II. 出海战略：以港澳为重心拓展东南亚，长期目标海外业务收入占比提升至30%以上。

总结：

公司将2023—2025年设为战略调整期，2026—2028年设为高质量发展期。2025年处于调整期最后一年——2025年收入仍下滑8.55%、扣非亏损1.97亿元，研发资本化率由9.09%直接降为零、当期费用一次性加重。关键验证点是2026年ASIC新品能否把芯片优势转化为实际营收增量。

竞争力



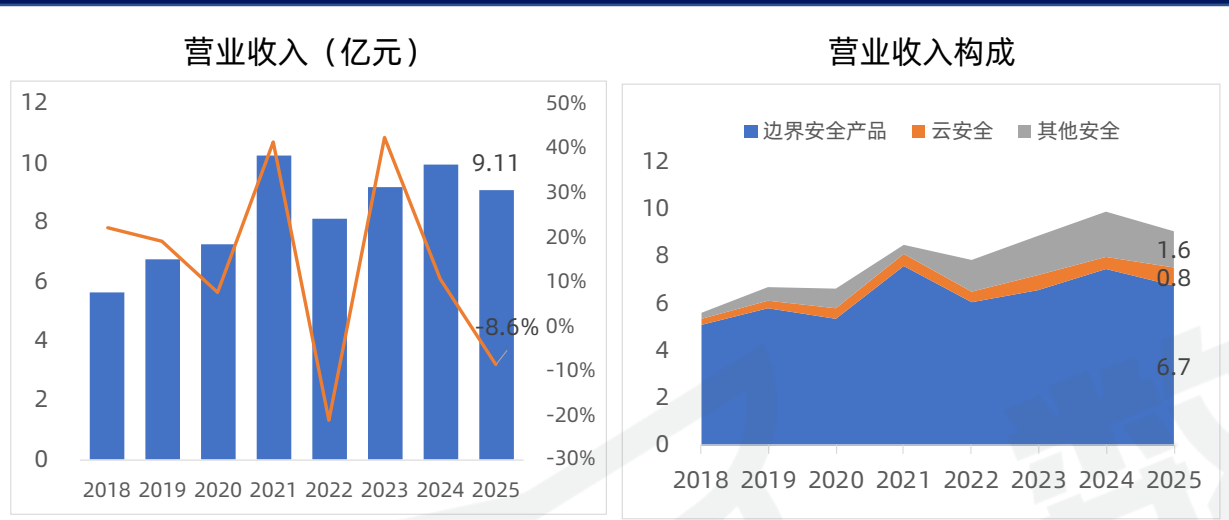
优势：

- ◆ 边界安全领域优势突出。公司在边界安全领域，产品优势突出，具有较强的产品竞争力。
- ◆ 具备国际化视野的研发体系。公司在苏州、北京、美国三地设立了研发中心，形成了具有国内外前沿洞察力的研发体系。
- ◆ 优质的客户群体。公司依赖边界安全的产品品质和研发能力在金融、政府、运营商等行业领域拥有较优质的客户群体。
- ◆ 引进神州数码为第一大股东，有望为公司带来营销能力提升。

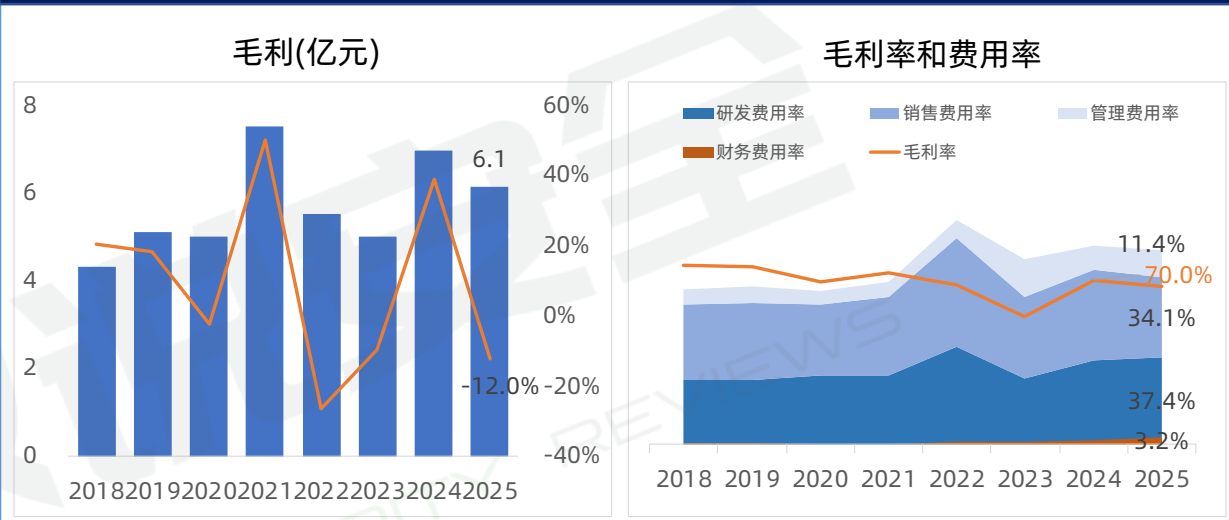
改进：

- ◆ 产品结构单一，产品线覆盖度有待提升。目前公司主要产品线依然是边界安全，云安全和其他安全业务方面拓展较慢。
- ◆ 费用结构有待优化。近三年公司的四项费用率分别为79.8%、86.6%、86%，远超过毛利率的水平。公司应严格审核各项费用支出，提高费用使用效率，推动降本增效。

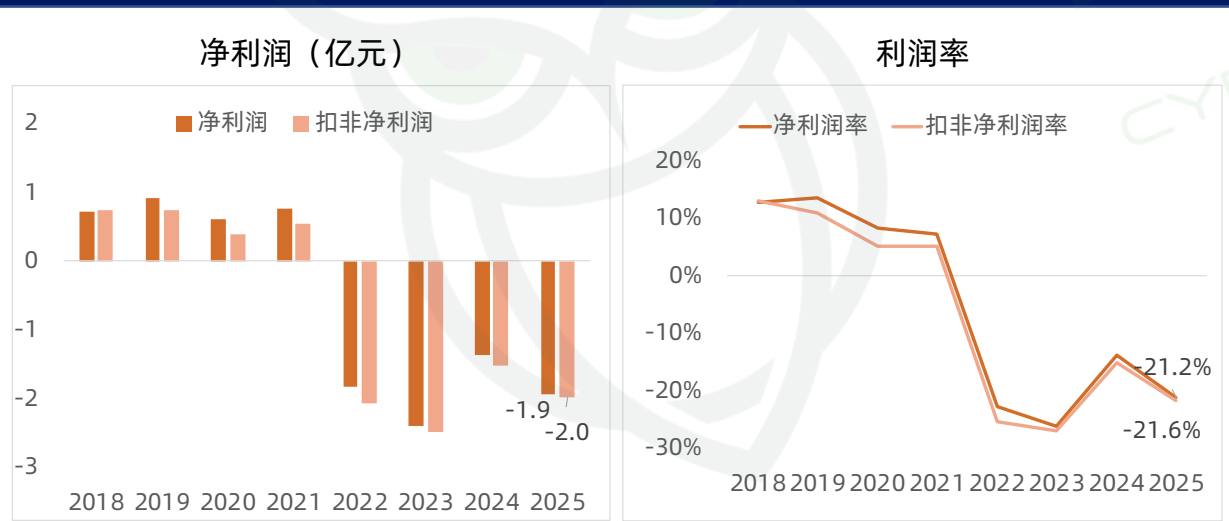
营业收入情况



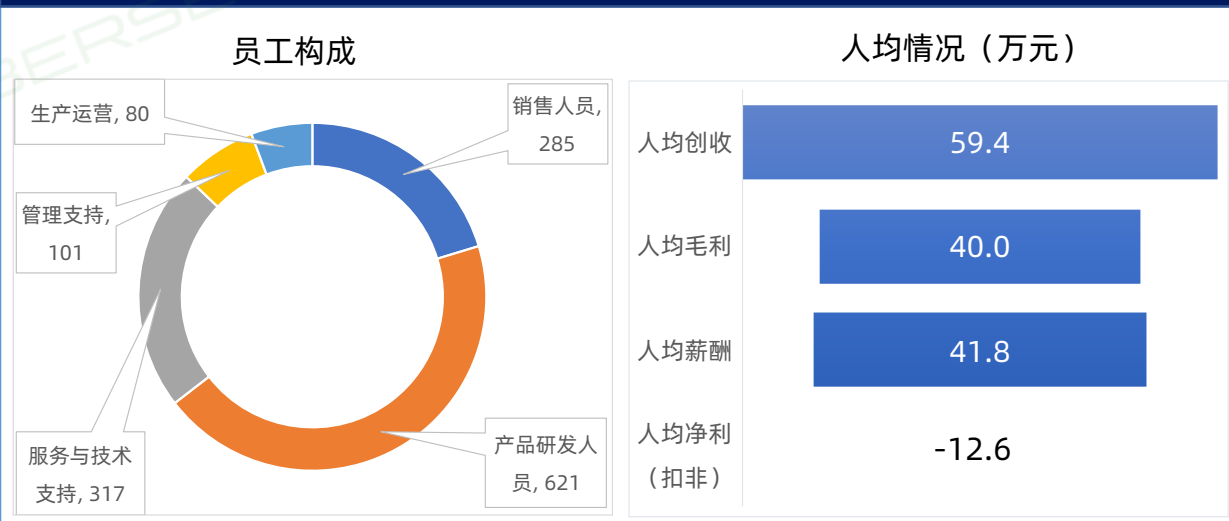
毛利情况



盈利情况

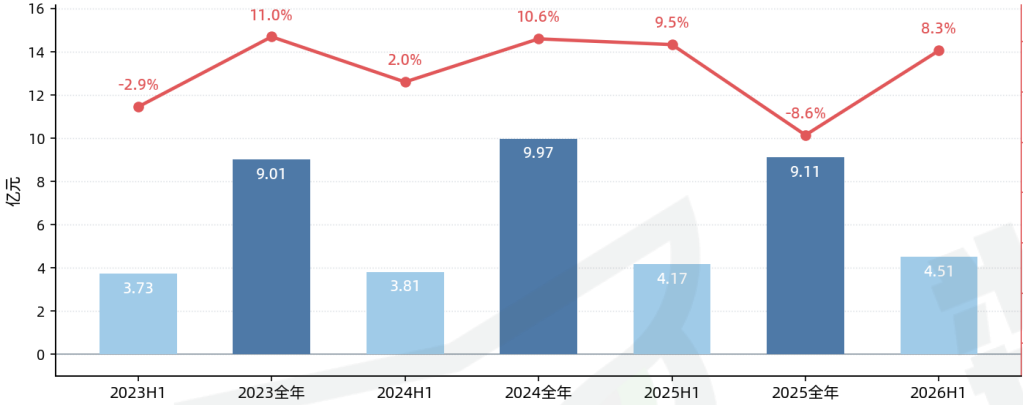


员工情况

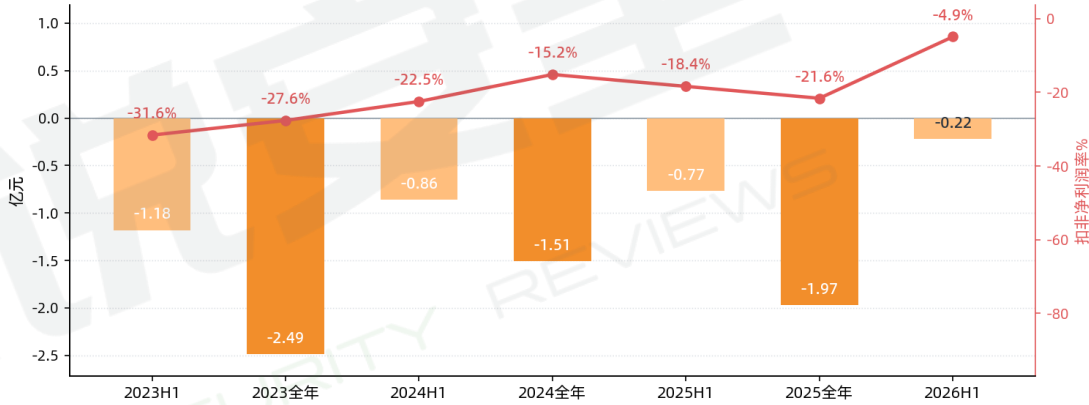


2026年上半年，山石网科营收4.51亿元，同比增长8.28%；扣非净亏损约0.22亿元，较上年同期约0.77亿元明显收窄。毛利率升至71.27%，同比提高2.01个百分点。公司披露，ASIC安全产品规模化商用、高毛利客户拓展及控费共同推动经营改善。经营性现金流净额仍为-1.04亿元，虽较上年同期-1.26亿元改善，但尚未转正。后续重点是新品放量能否延续，并带动持续盈利与回款改善。

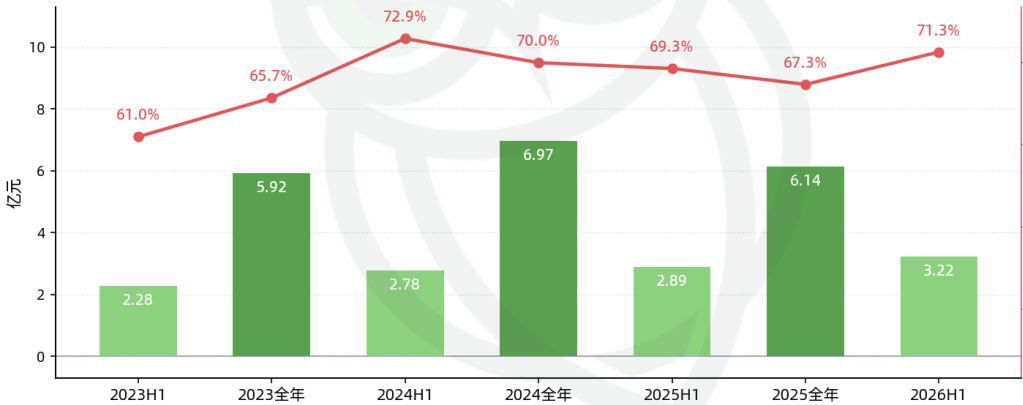
营业收入及同比增速



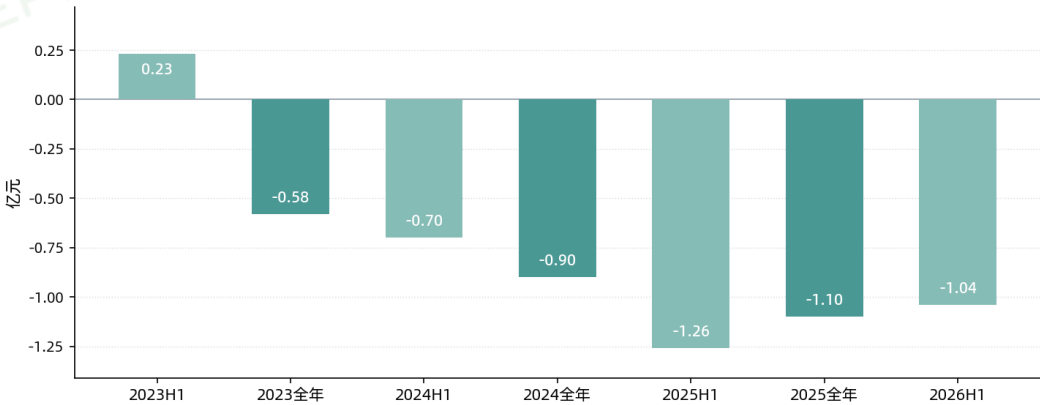
扣非净利润及扣非净利润率



毛利润及毛利率



经营活动现金流净额



浅色 = 半年度 (1-6月累计) 深色 = 全年度 折线 = 右轴比率/增速

2025年经营情况回顾

2025年公司实现营业总收入5.54亿元，同比增长17.07%；密码整机收入2.56亿元，同比增长28.93%，毛利率70.84%、下降3.42个百分点；密码系统收入1.43亿元，同比增长28.62%，毛利率77.82%、下降2.41个百分点；密码服务及其他收入1.12亿元，同比增长24.16%，毛利率70.26%、下降1.09个百分点；公司综合毛利率下降1.08个百分点至71.12%；公司员工人数817人，减少108人，其中研发人员336人；销售人员119人；公司人均创收63.6万元，较上年提升4.2万元；人均毛利45.2万元，较上年提升2.3万元。

- ◆ 利润首次转亏的核心原因是费用前置叠加减值集中计提：四项费用合计4.35亿元，同比+36.81%，增速是营收增速两倍以上，资产减值2,901万元（含商誉1,412万元）+信用减值1,730万元，合计拖累利润约4,631万元。
- ◆ 经营性现金流净额1.05亿元，同比+384.19%，创历史新高，应收账款在营收增长下反降11.06%。

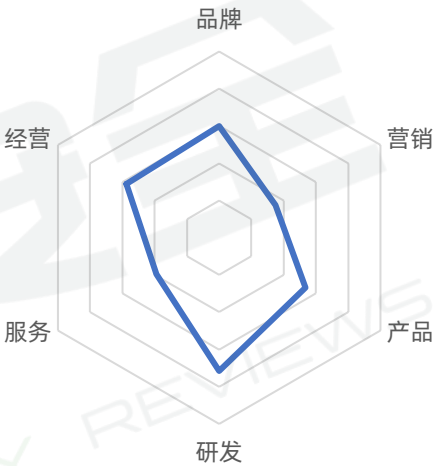
2026年发展战略

- 战略重点：
- I. 深化"云+芯"布局：推进自研密码芯片规模化商用与"密码安全芯片研发升级"募投项目，巩固云密码服务市场领先地位。
 - II. 强化并购协同：深化与江南科友（金融密码）、江南天安（云密码）的集团化融合，打造芯片到行业方案的全栈密码服务。

总结：

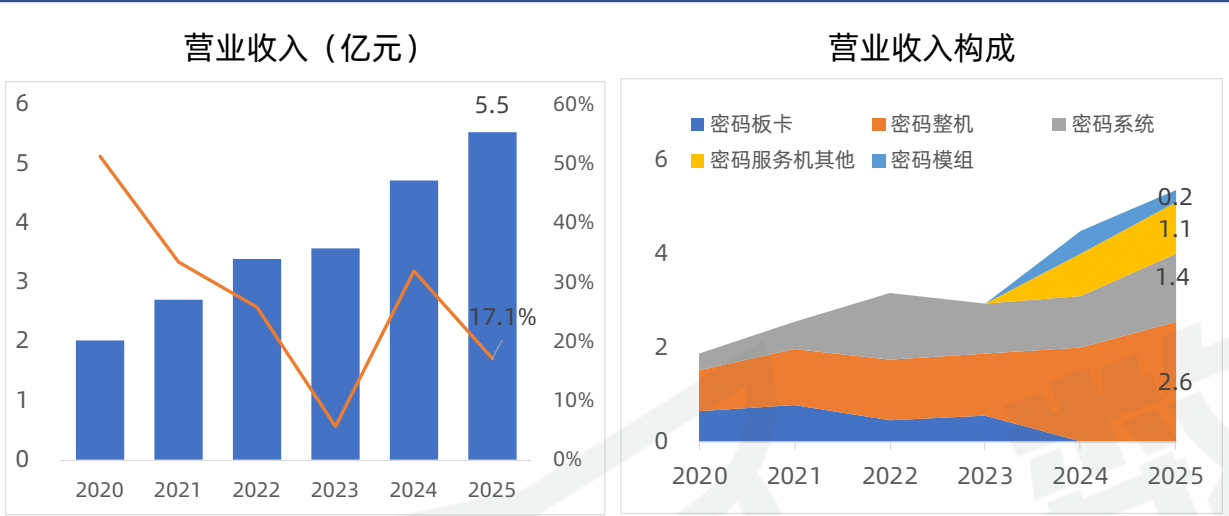
公司在收入扩张期主动加码芯片、抗量子、海外与并购整合，用当期利润换取未来的产品与渠道身位——2025年收入增长17.07%为全行业第一，但研发费用增长28.40%、销售费用增长38.57%，扣非仍亏0.60亿元。关键验证点是支出能否带来密码服务与海外收入的增长。

竞争力

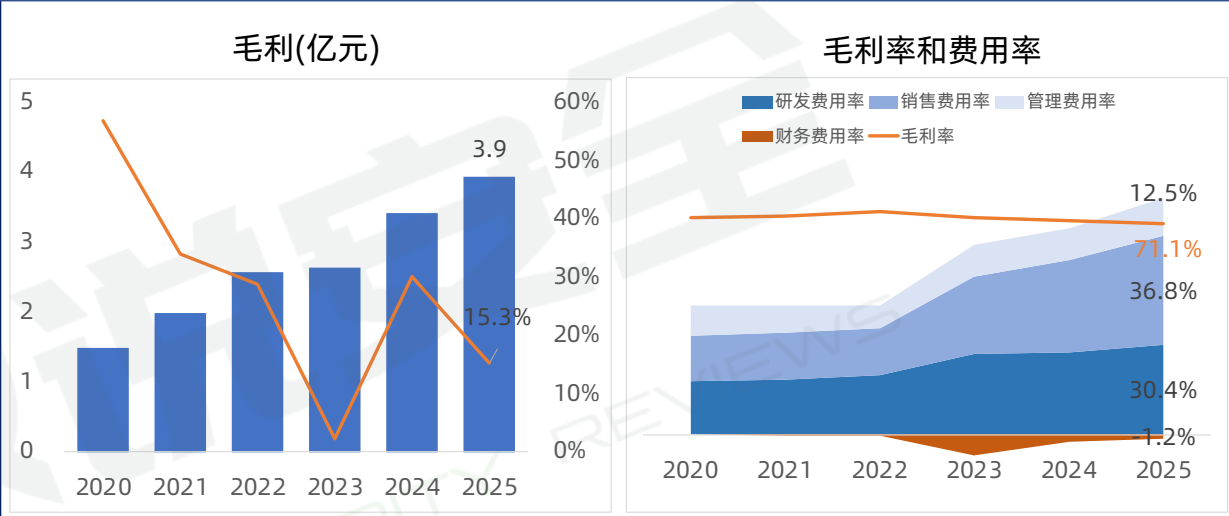


- 优势：
- ◆ 在密码领域技术优势突出。密码产品和核心部件的国产化，是当前保证产品自主可控和供应链安全的重要任务。公司聚焦商用密码技术创新和产品研发，形成了完备的拥有自主知识产权的商用密码产品体系。
 - ◆ 深耕密码领域，拥有稳定的上下游关系。三未信安作为国内主要的商用密码基础设施提供商，打造了良好的品牌效应，具备较为成熟的渠道体系，以及稳定的客户资源。
- 改进：
- ◆ 加强创新产品的投入力度。随着人工智能、数字货币、量子计算、后量子密码等新兴技术的快速突破演进，密码行业也迎来了新的发展机遇，三未信安应进一步加强创新产品的投入力度，提升公司的核心竞争力。
 - ◆ 加强销售管理能力。三未信安早期不直接面对客户，近两年来开始搭建销售体系，以拓宽市场覆盖并增强客户关系，公司应进一步增强销售管理能力，精准定位客户需求，增强市场响应速度。

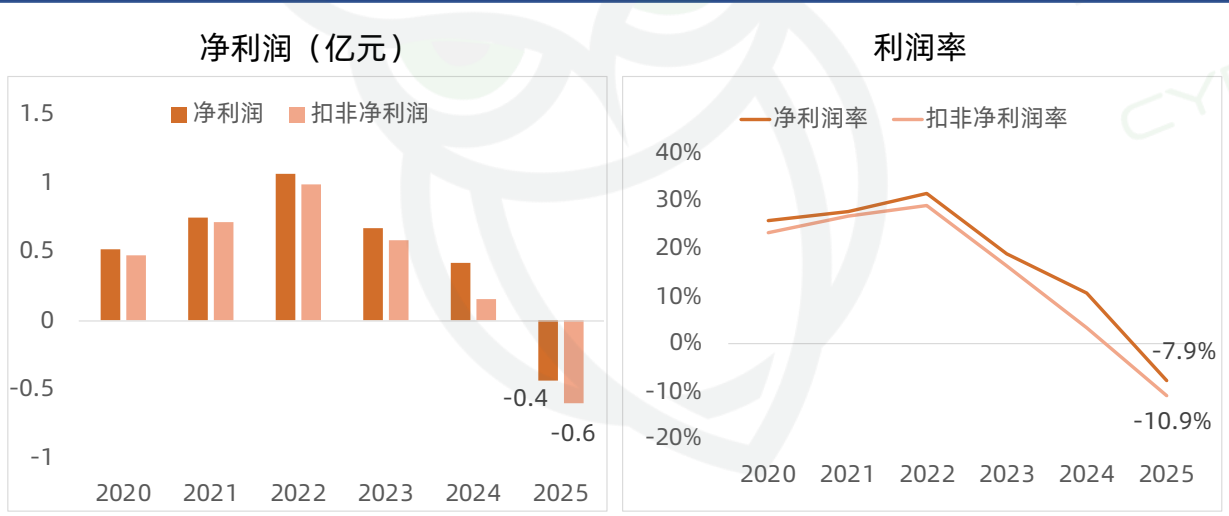
营业收入情况



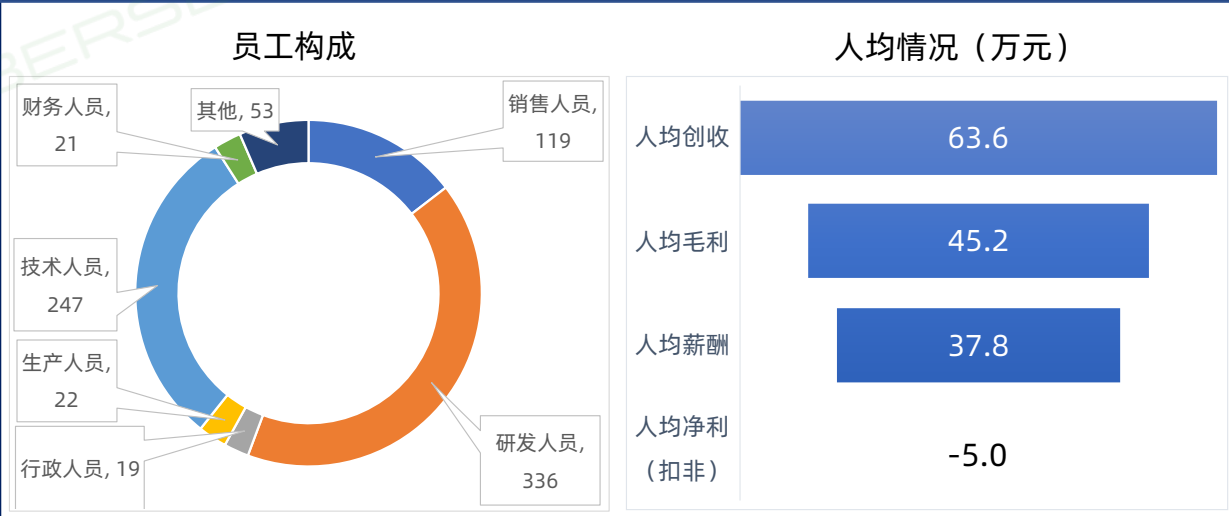
毛利情况



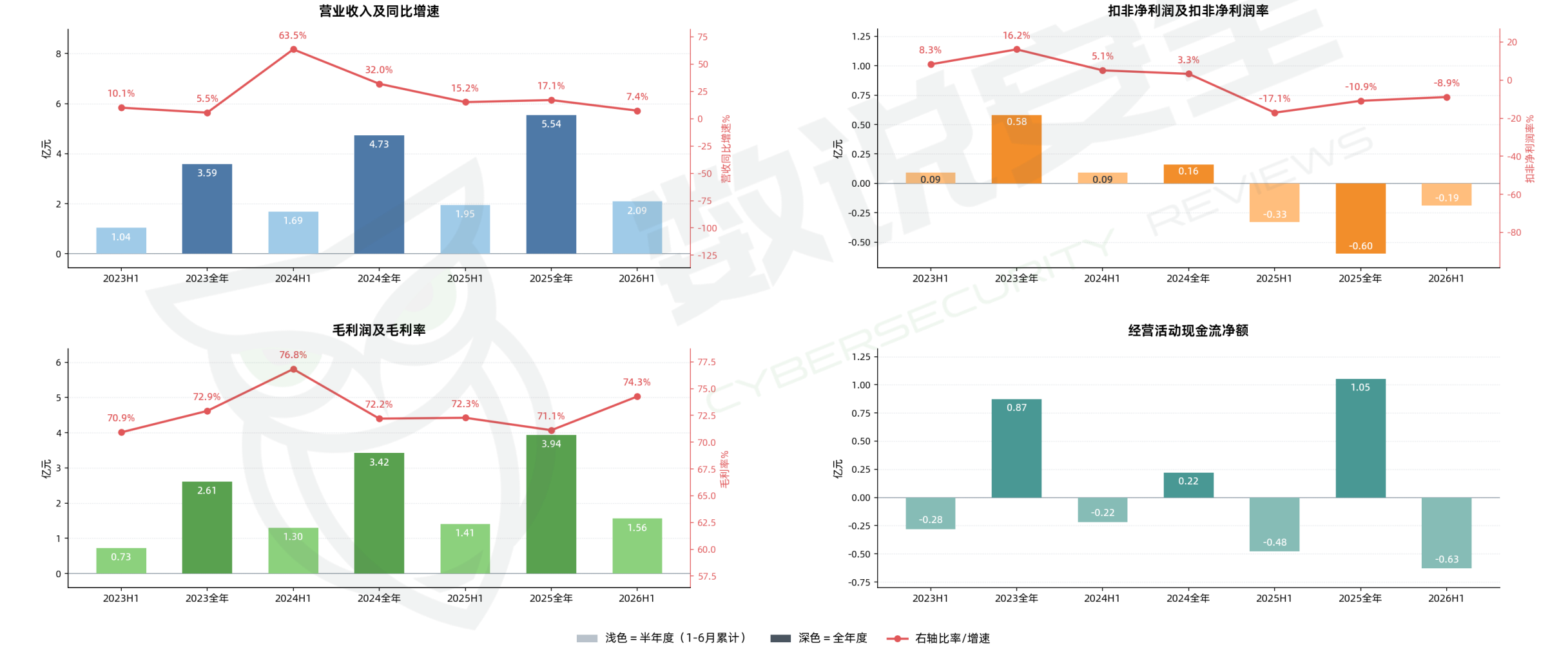
盈利情况



员工情况



2026年上半年，三未信安营收2.09亿元，同比增长7.38%；扣非净亏损0.19亿元，较上年同期约0.33亿元收窄。毛利率由72.3%升至74.3%，收入和毛利率同步改善，毛利润由1.41亿元升至1.56亿元，经营修复已有进展。但经营性现金流净额-0.63亿元，较上年同期净流出0.48亿元扩大。公司仍处于亏损状态，下一步需要把毛利增长转化为稳定盈利，并改善经营现金流。



2025年经营情况回顾

2025年公司实现营业总收入2.76亿元，同比下滑22.45%，降幅较上年扩大；数字风洞及运营收入1.75亿元，同比增长0.37%，毛利率54.03%、提升0.20个百分点；网络靶场及运营收入0.86亿元，同比下滑45.12%，毛利率53.44%、下降0.10个百分点；安全防护与管控收入0.15亿元，同比下滑39.40%，毛利率62.08%、提升10.24个百分点；公司综合毛利率提升0.71个百分点至54.28%；公司员工人数407人，减少64人，其中研发人员215人，减少40人、减员15.7%；销售人员138人，减少17人、减员11.0%；公司人均创收62.9万元，较上年下降10.6万元；人均毛利34.2万元，较上年下降5.2万元。

- ◆ 经营现金流-225万元，较上年-4,630万元收窄4,405万元，但仍未转正；应收账款及票据3.16亿元相当于全年营收的114.5%，信用减值损失3,381万元，是利润表全面承压的主因。
- ◆ 公司持续布局数字风洞和AI安全测评，2025年研发人员减少40人、销售人员减少17人。后续需在保持核心技术研发的同时，提高投入效率和产品交付能力。

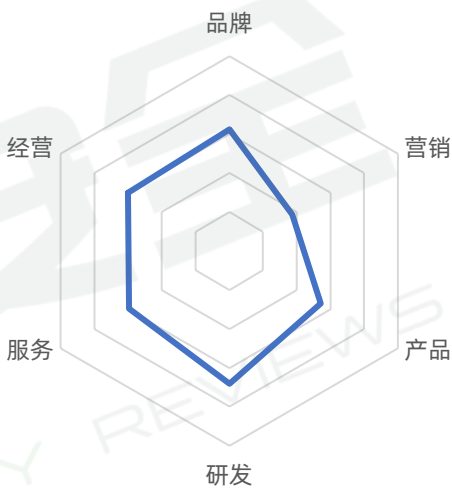
2026年发展战略

- 战略重点：
- I. 加大"数字风洞"产品体系市场开拓力度，向同行业、同类型客户做规模化推广。
 - II. 聚焦AI全生命周期安全，依托"元方"原生安全大模型与"春秋AI数字风洞"测评平台。
 - III. 持续引领网络靶场和人才建设，推进AI赋能下网络靶场智能化升级与人才培养体系。

总结：

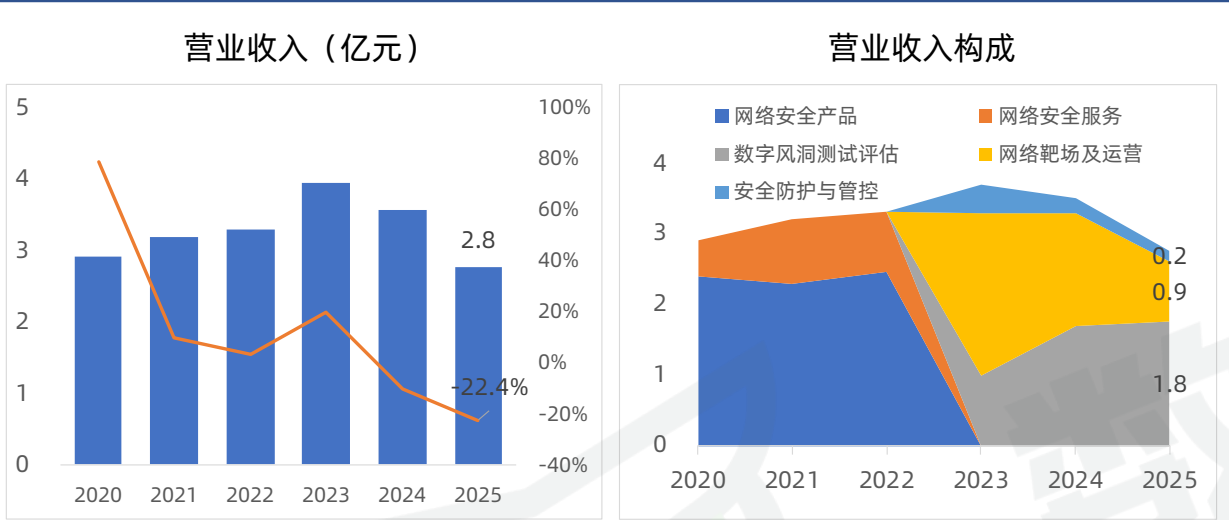
公司在收入收缩期主动保住AI大模型测评与“数字风洞”研发节奏，代价是账面利润、股权激励和分红同步让位。战略核心是把“数字健康”从理念做成可复制的交付，实质是在解决靶场类业务定制化重、规模不经济的老问题，并承接《网络安全法》AI条款2026年1月施行带来的合规需求。关键验证点是2026年AI业务能否承接网络靶场业务-45.12%腰斩留下的缺口。

竞争力

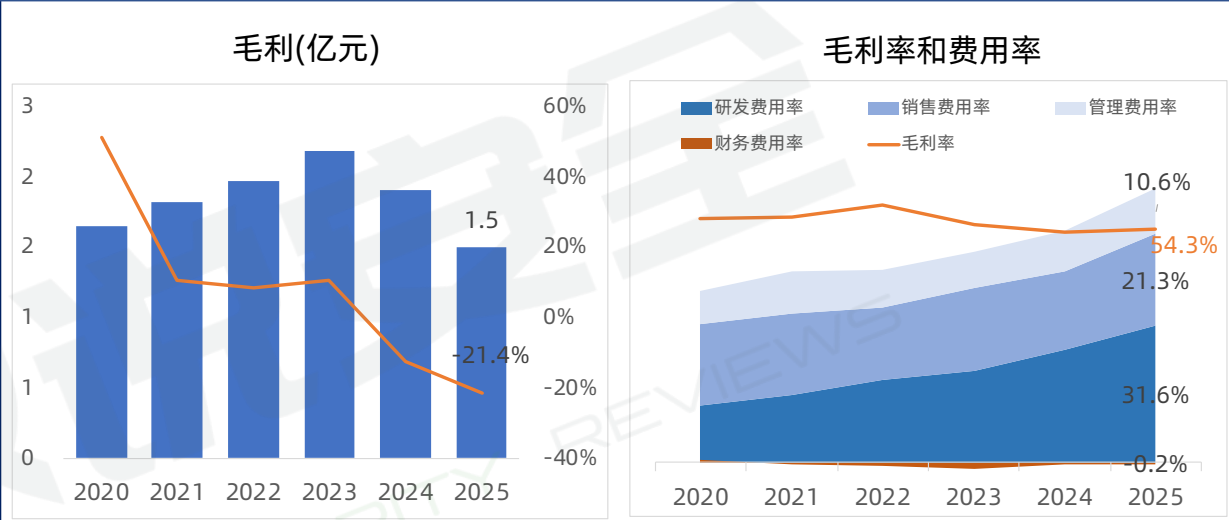


- 优势：
- ◆ 聚焦核心领域。公司专注在靶场领域，围绕网络安全靶场拓展不同行业的不同应用场景，并推出了安全测试工具、蜜罐、安全管控等一系列产品，同时开展相关安全服务、举办安全竞赛和安全培训，为客户提供围绕靶场的各种服务；公司不断积累优势，成为该领域的领先安全厂商。
 - ◆ 深耕核心能力。网络空间平行仿真技术和攻防对抗技术是公司的核心底层技术，公司持续进行核心技术的研发，形成标准化体系和功能模块，未来也将不断加大研发投入，保证技术持续领先。
 - ◆ 前瞻性的战略定位。公司在22年推出了“数字风洞”产品体系，希望将其作为网络安全基础设施，希望开拓网络安全测试评估的专业赛道；公司的战略为市场提供了新的视角，有利于公司引领市场重新审视靶场的市场地位及规模体量，同时也进一步提升了公司在该领域的领先地位。
- 改进：
- ◆ 关注经营稳定性和健康性。2025年公司收入与利润仍承压，经营现金流净流出明显收窄但尚未转正，需要公司更加关注对经营策略的调整，平滑收入结构的波动性，并尽快恢复健康的造血能力。

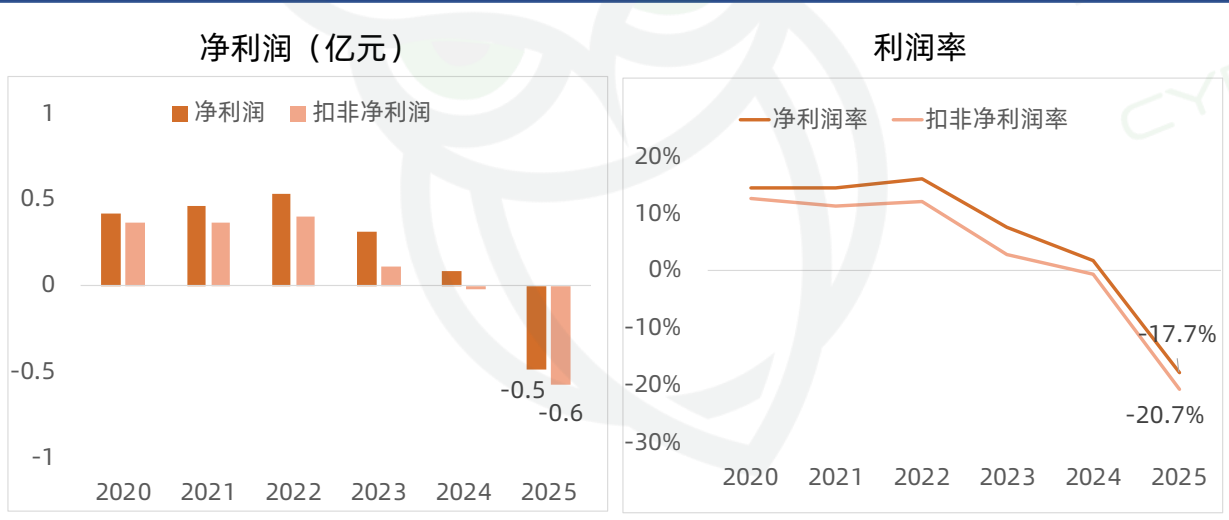
营业收入情况



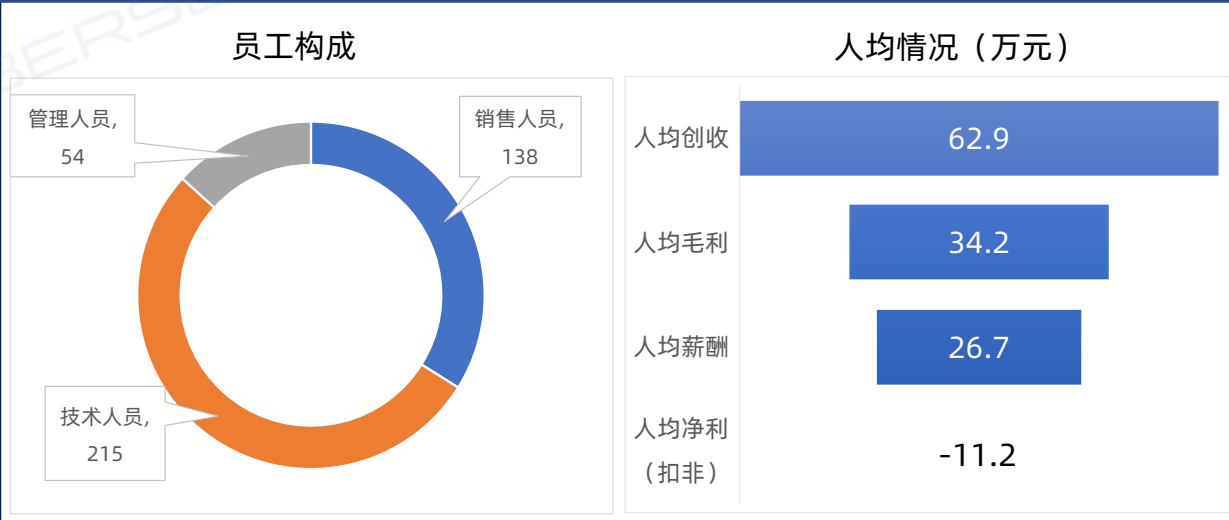
毛利情况



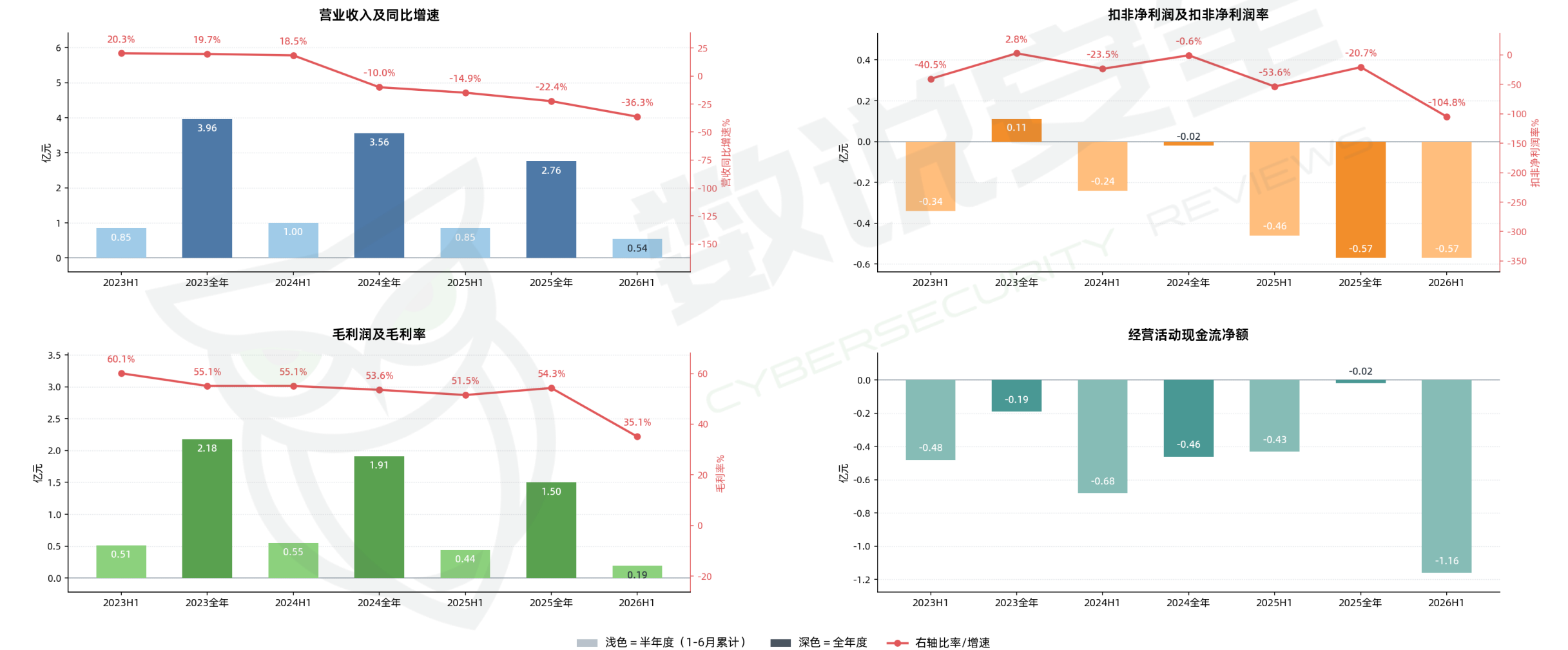
盈利情况



员工情况



2026年上半年，永信至诚营收0.54亿元，同比下降36.28%；扣非净亏损0.57亿元，较上年同期约0.46亿元扩大，亏损金额已超过同期收入。毛利率由51.5%降至35.1%，毛利润由0.44亿元降至0.19亿元，收入收缩与毛利率下滑共同压缩盈利空间。经营性现金流净额-1.16亿元，较上年同期净流出0.43亿元进一步扩大。当前经营压力集中在订单交付、毛利修复与回款，尚不能判断已出现盈利拐点。



2025年经营情况回顾

2025年公司实现营业总收入3.08亿元，同比增长5.07%，增速较上年放缓；网络安全产品与服务收入2.42亿元，同比增长6.10%，毛利率66.92%、下降4.55个百分点；网络空间地图收入0.51亿元，同比增长7.55%，毛利率62.45%、下降14.99个百分点；卫星互联网安全业务收入0.15亿元，同比下滑14.85%，毛利率52.42%、下降22.17个百分点；公司综合毛利率下降7.18个百分点至65.45%；公司员工人数624人，增加8人，其中研发人员228人，减少11人、减员4.6%；销售人员142人，增加15人、增员11.8%；公司人均创收49.7万元，较上年下降1.5万元；人均毛利32.6万元，较上年下降4.6万元。

◆ 信用减值损失2,403万元（扩大67.07%）+资产减值损失409万元，合计2,812万元，是利润由正转负的最大单一拖累项；经营现金流-1,398万元，同比改善77.94%，销售商品收到现金3.31亿元（+23.81%），回款效率边际向好。但卫星互联网安全业务收入1,528万元、同比-14.85%，前瞻布局向规模兑现的转化节奏低于预期。

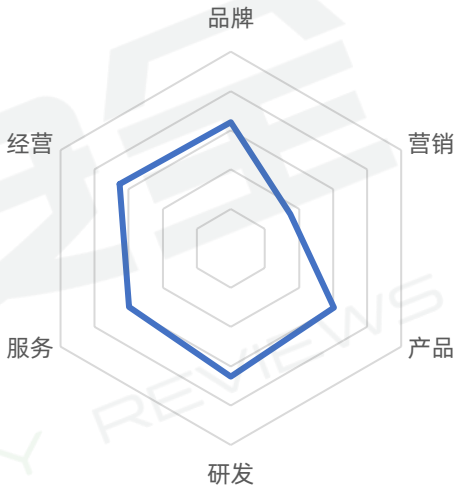
2026年发展战略

- 战略重点：
- I. 加大研发投入，持续产品、技术升级。
 - II. 坚定布局卫星互联网安全打造第二增长曲线
 - III. AI与数字化管理双轮驱动经营提效

总结：

本期亏损是“毛利率结构性下行+应收账款风险释放+卫星互联网第二曲线兑现节奏放缓”三重压力的叠加——综合毛利率同比下降7.18个百分点，降幅较大。战略上押注两个差异化资产：网络空间地图要从单点产品升级为平台化、基础设施化的数字空间底图，卫星互联网安全要从“前瞻布局”走向“持续兑现”。2026年是检验这两者能否真正承担增长引擎角色的关键验证年。

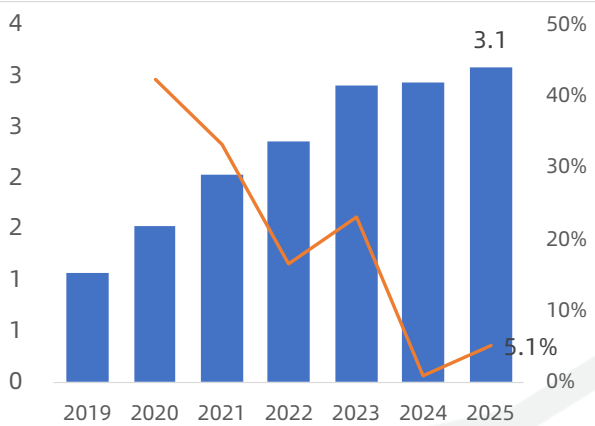
竞争力



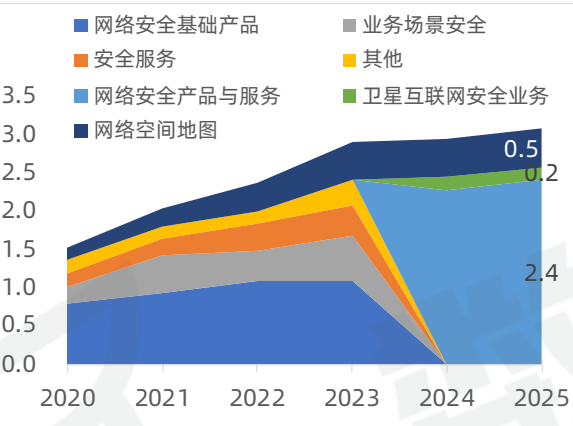
- 优势：
- ◆ 深耕核心业务领域：公司自创立起就深耕于漏洞及脆弱性检测、应用安全防护业务，并在该领域建立了一定的市场优势和品牌认知，同时，公司也拓展了网络空间地图领域，并且是国内较早关注网络空间测绘技术领域的安全厂商，相关的技术水平也达到国内领先水平，先后获得多个奖项，公司稳扎稳打，在核心业务领域不断深耕。
 - ◆ 差异化战略布局和积极的资本运作：公司在稳固核心业务的基础上，不断布局蓝海业务，较早的展开了网络空间测绘和网络空间地图领域业务，并且在不同行业（如电力、公共安全、运营商等）的业务场景安全方向进行拓展；同时，公司在2024年并购天御云安，向卫星互联网安全领域进军，并入股贝格通，通过投资并购的方式进行深层次战略布局，寻求更长远的发展路径。
- 改进：
- ◆ 协调扩张和经营平衡。公司在上市网安企业中的体量相对较小，2020-2023年收入增长迅速；近年来依然保持着费用和人员的扩张态势，但收入、毛利率、利润率、应收账款比重、经营性现金流净额等重要指标健康度明显下降，公司需要提高警惕，有序扩张，审慎投入。

营业收入情况

营业收入（亿元）

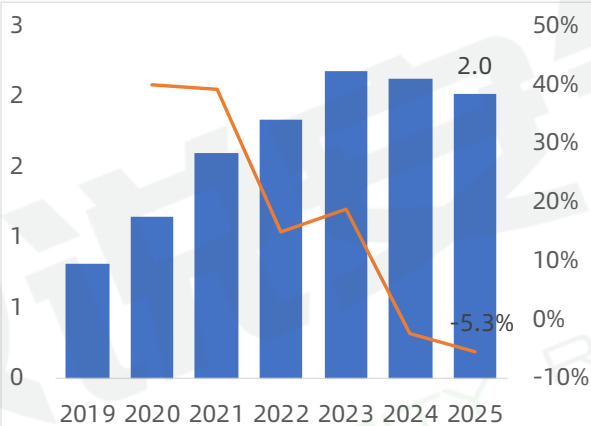


营业收入构成

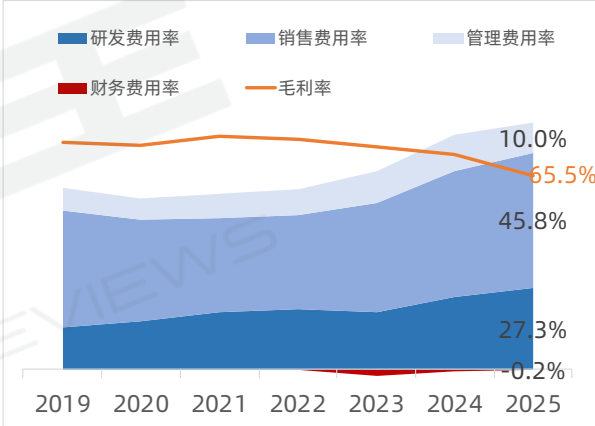


毛利情况

毛利(亿元)

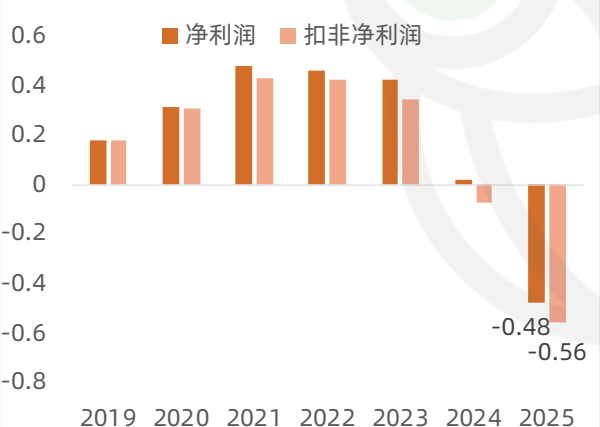


毛利率和费用率

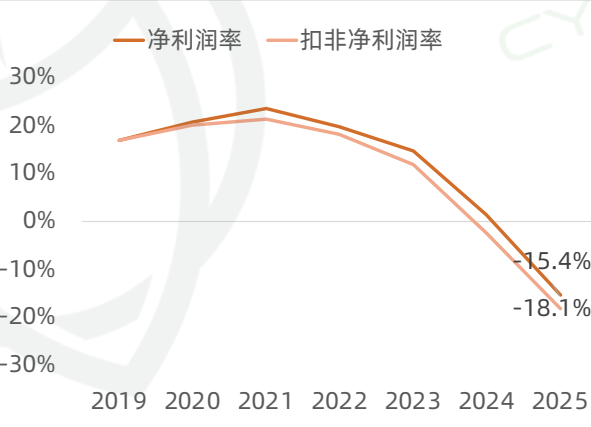


盈利情况

净利润（亿元）

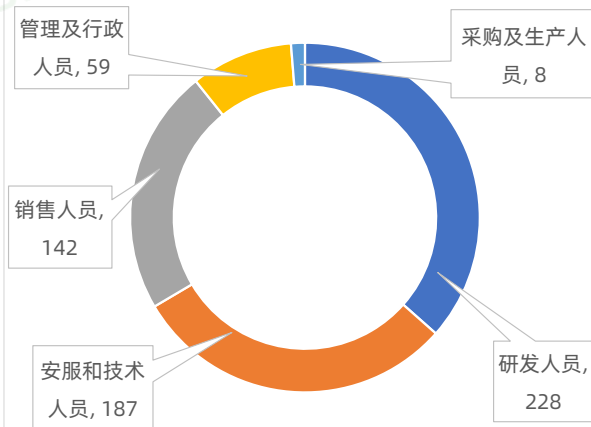


利润率

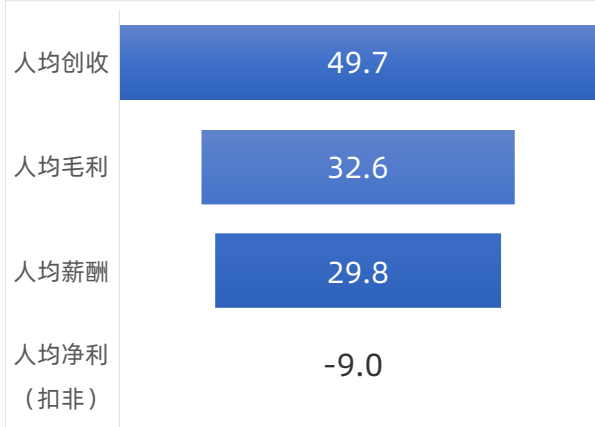


员工情况

员工构成

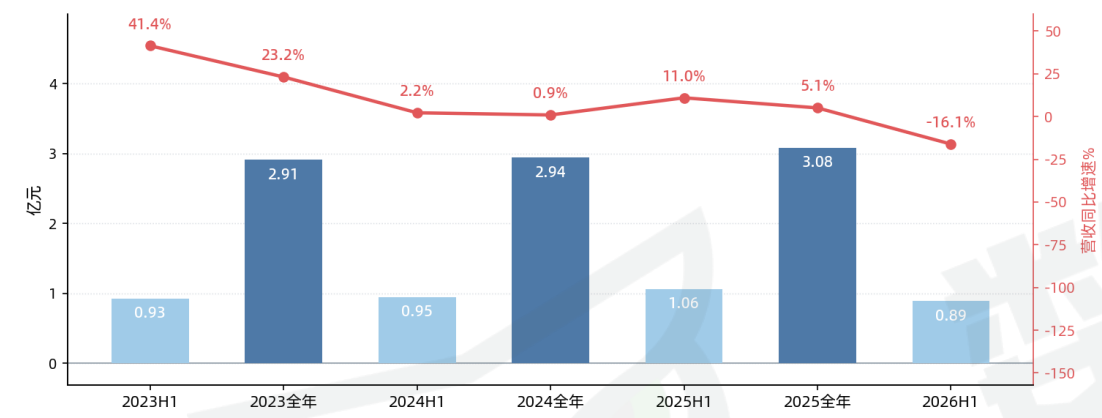


人均情况（万元）

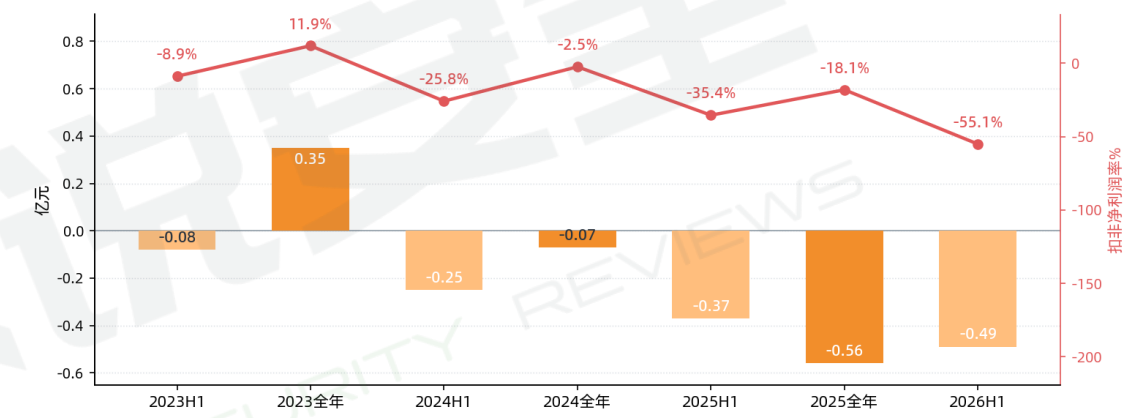


2026年上半年，盛邦安全营收0.89亿元，同比下降16.10%；扣非净亏损约0.49亿元，较上年同期约0.37亿元扩大。毛利率由71.2%降至65.4%，收入和毛利率同时下降，毛利润由0.75亿元降至0.58亿元。公司披露，收入减少主要来自网络空间地图、网络安全产品与服务。经营性现金流净额-0.36亿元，较上年同期净流出0.26亿元扩大。后续需关注核心业务恢复，以及投入能否转化为收入和现金回流。

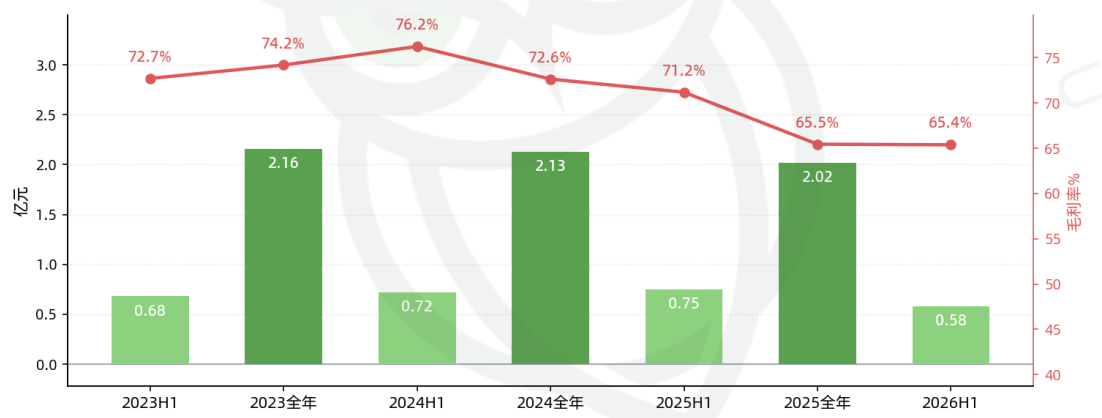
营业收入及同比增速



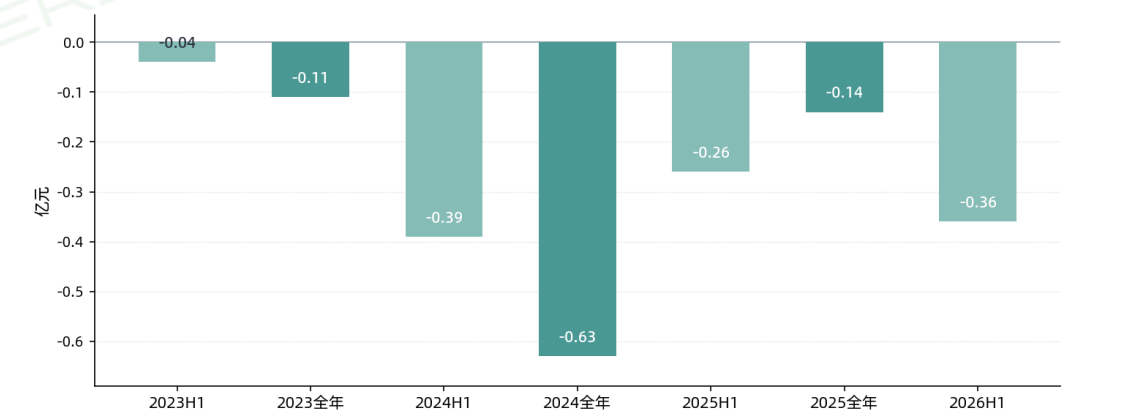
扣非净利润及扣非净利润率



毛利润及毛利率



经营活动现金流净额



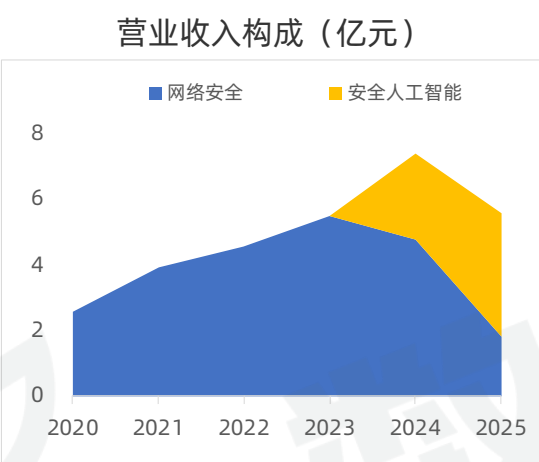
浅色 = 半年度 (1-6月累计) 深色 = 全年度 右轴比率/增速

公司介绍

北京安博通科技股份有限公司以“看透安全，体验价值”理念为核心，是可视化网络安全专用核心系统产品与安全服务提供商。其自主研发的ABT SPOS可视化网络安全系统平台，已成为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，是国内众多部委与央企安全态势感知平台的核心组件与数据引擎。2019年成为中国第一家登陆科创板的网络安全企业，2020年获评国家级专精特新“小巨人”企业，五度入选工信部网络安全技术应用试点示范项目。

使命：创造极致网络安全业务新体验

愿景：可视化网络安全技术创新者



2026年发展战略与经营计划

- 战略重点：**
- I. 战略升级：从"可视化网络安全技术创新者"全面迈向"AI时代安全算力生态构建者"，以"溢彩"AI交付架构和"鲁班"安全大模型为技术基座。
 - II. 拓展算力市场：2025年10月中标郑州人工智能计算中心（二期）项目，中标金额2.10亿元，布局推理侧算力落地。

总结：公司处于从网安可视化厂商向“AI时代安全算力生态构建者”转型的阵痛期：2025年收入下滑24.54%、员工减少49.48%，但毛利率大幅提升13.53个百分点至79.49%，是结构优化的真实信号。新增长押注推理算力（已中标郑州人工智能计算中心二期2.10亿元）与存储模组海内外市场。关键验证点是收入能否在新业务放量后止跌回升。

2025年经营情况回顾

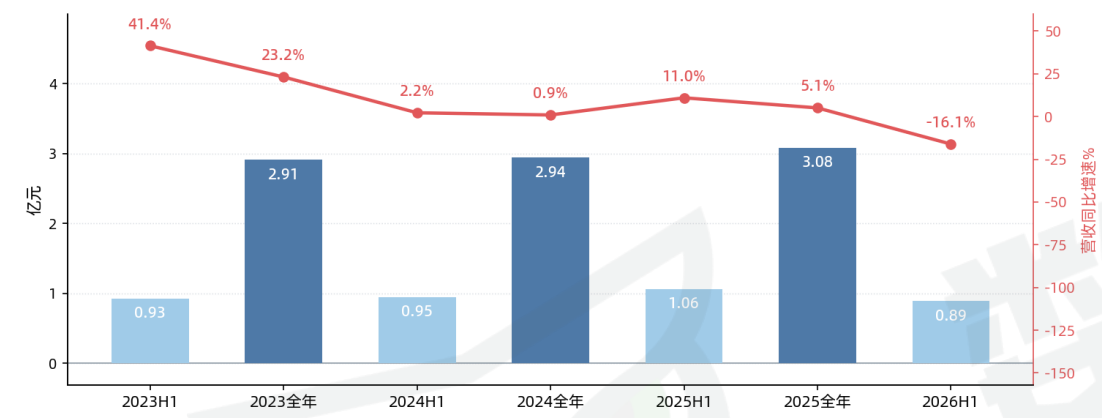
2025年公司实现营业总收入5.56亿元，同比下滑24.54%，为近五年首次负增长；安全产品收入1.80亿元，同比下滑38.28%，毛利率57.28%、提升2.13个百分点；安全人工智能收入3.75亿元，同比下滑15.71%，毛利率90.91%、提升17.88个百分点；公司综合毛利率提升13.53个百分点至79.49%；公司员工人数241人，减少236人，其中研发人员94人，减少91人、减员49.2%；销售人员31人，减少54人、减员63.5%；公司人均创收154.9万元，较上年提升2.2万元；人均毛利123.1万元，较上年提升22.4万元。

关键经营指标

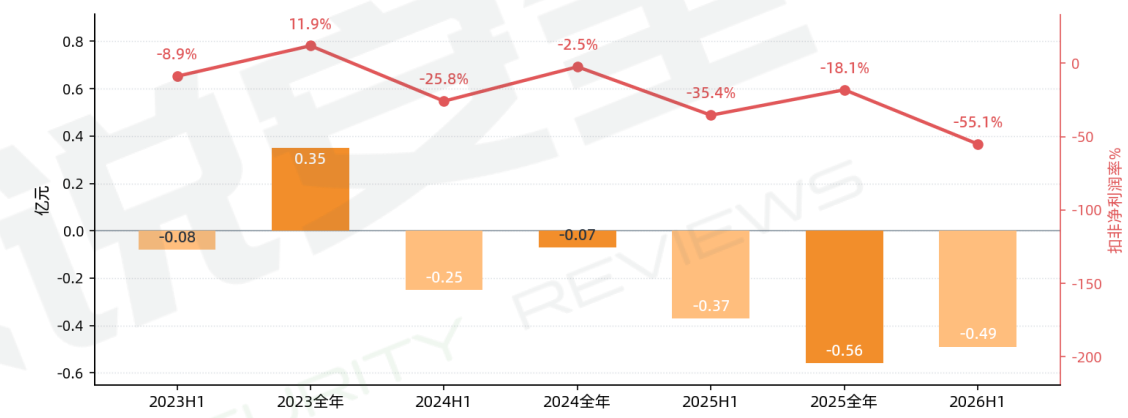
营业收入	营业收入同比增长	扣非净利润	员工人数
5.6亿元	-24.5%	-1.5亿元	241
资产总额	毛利率	经营性现金流净额	人均毛利
14.6亿元	79.5%	-2.23亿元	123万元

2026年上半年公司实现营业总收入1.31亿元，同比下滑69.46%，是由于上年同期4.29亿元基数异常偏高（占2025全年的77.2%），降幅被显著放大。综合毛利率66.98%、同比下降21.07个百分点。扣非净利润-0.23亿元，较上年同期的-1.10亿元减亏79.13%，扣非净利润率由-25.67%改善至-17.54%。经营性现金流净额0.12亿元，较上年同期的-2.06亿元转正，为近年首个半年度为正。减亏主要由费用压降驱动：销售费用同比-95.53%，研发费用-39.08%，管理费用-20.87%。

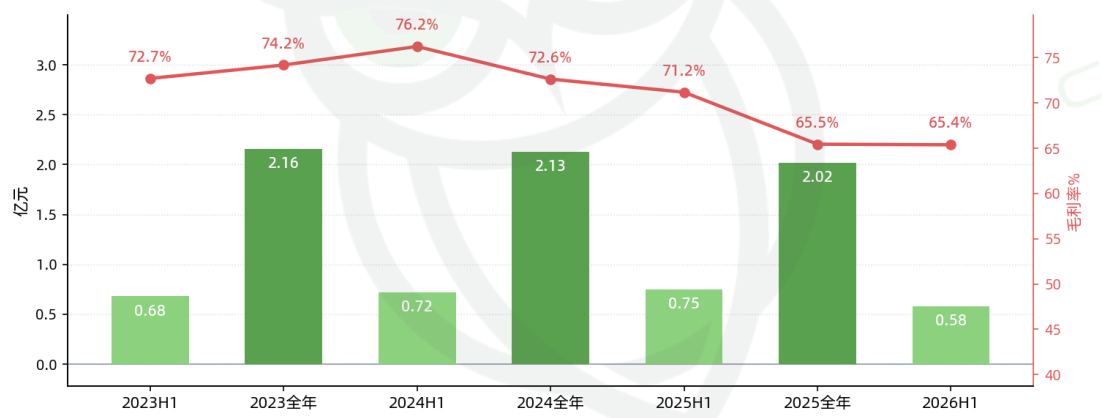
营业收入及同比增速



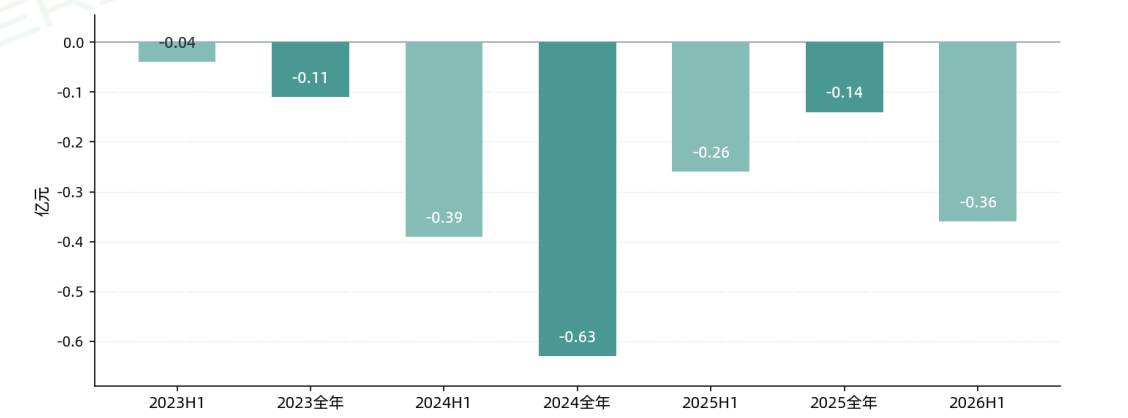
扣非净利润及扣非净利润率



毛利润及毛利率



经营活动现金流净额



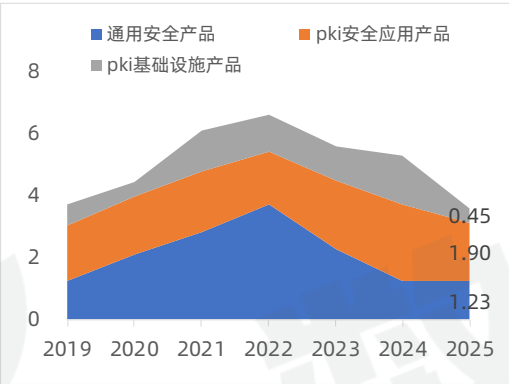
浅色 = 半年度（1-6月累计） 深色 = 全年度 右轴比率/增速

公司介绍

格尔软件是中国商用密码领域的企业，是国内较早研制和推出公钥密码基础设施（PKI）产品的厂商，是国家科技支撑计划商用密码基础设施项目的牵头单位。公司致力提供以身份治理为中心的数字经济安全整体解决方案，拥有大批政务、金融、军工等领域核心客户。面向社会数字化转型的新形势，完成了云计算、大数据环境下大规模复杂场景的安全体系建设，全力打造成为国内全栈全域的信息安全服务提供商。

使命与愿景：让互联更可信、让数据更安全。

营业收入构成（亿元）



2025年经营情况回顾

2025年公司实现营业总收入3.58亿元，同比下滑32.45%，为连续第二年大幅下滑；PKI安全应用产品收入1.90亿元，同比下滑23.38%，毛利率64.04%、提升0.96个百分点；通用安全产品收入1.23亿元，同比下滑0.67%，毛利率25.03%、下降4.43个百分点；PKI基础设施产品收入0.45亿元，同比下滑71.77%，毛利率55.47%、提升3.28个百分点；公司综合毛利率下降2.79个百分点至49.20%；公司员工人数585人，减少94人，其中研发人员198人，减少3人、减员1.5%；销售人员120人，增加0人、增员0.0%；公司人均创收56.6万元，较上年下降14.0万元；人均毛利27.8万元，较上年下降8.9万元。

2026年发展战略与经营计划

战略重点：

- I. 强化技术引领：2026年聚焦抗量子密码、AI安全、数据安全前沿领域，推进面向机器身份的证书自动化管理系统研发。
- II. 深耕重点行业：巩固党政、金融、国防军工传统优势行业，拓展教育、医疗、能源等新兴领域市场。

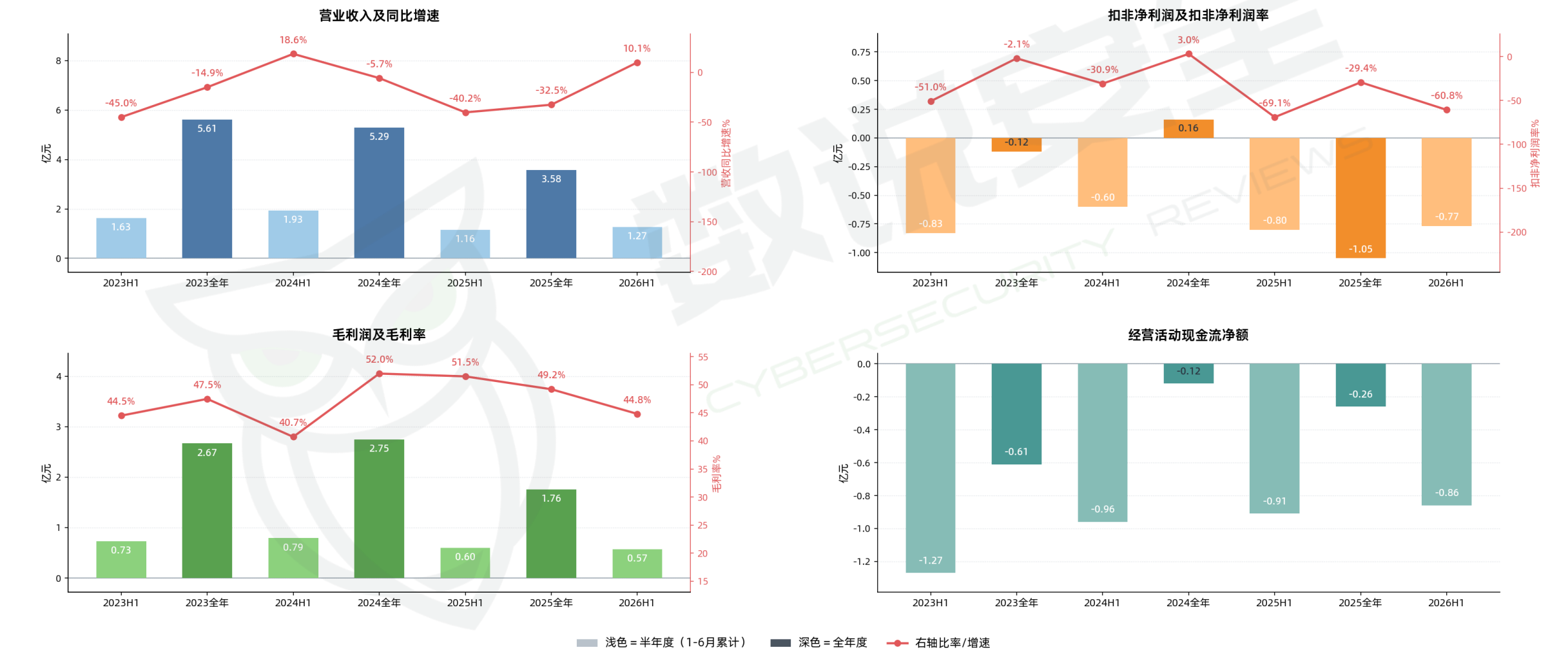
总结：

公司锚定“AI智能体时代数字信任基础设施运营商”定位，以“密码即服务+AI安全治理”双引擎完成从传统密码厂商向AI原生安全平台企业的跃迁，交付模式由“一次性交付”转向“全旅程陪伴”。2025年收入下滑32.45%，这是需求端的被动收缩而非模式失效——同赛道数字认证亦下滑25.28%。

关键经营指标

营业收入	营业收入同比增长	扣非净利润	员工人数
3.6亿元	-32.5%	-1.1亿元	585
资产总额	毛利率	经营性现金流净额	人均毛利
15.6亿元	49.2%	-0.26亿元	27.8万元

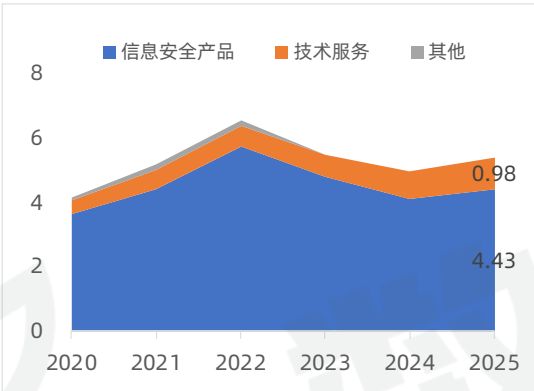
2026年上半年营收1.27亿元、同比增长10.09%，扭转上年同期-40.16%的深跌，但规模仍不足2022年同期的一半；扣非净利润-0.77亿元、扣非净利润率由-69.1%收窄至-60.8%，亏损缺口仍超过收入的六成。毛利率44.81%、同比降6.68个百分点——增长由PKI安全应用产品贡献（+43.0%），但占收入31.7%的通用安全产品毛利率从23.8%塌至7.0%，增收未能增利。经营性现金流净额-0.86亿元、净流出较上年同期收窄0.05亿元；应收账款及票据降20.4%、销售回款增24.7%，回款质量好于收入本身。



公司介绍

信安世纪是科技创新型的信息安全产品和解决方案提供商，以密码技术为基础支撑，致力于解决网络环境中的身份安全、通信安全和数据安全等基础性安全问题，在信息技术互联网化、移动化和云化等的发展趋势下，经过近二十年的自主研发和持续创新，信安世纪形成了身份安全、通信安全、数据安全、移动安全、云安全和平台安全六大产品系列。使命与愿景：公司坚持“负责任，受尊重”成为彼此最信赖的合作伙伴的合作共赢理念，与各大知名供应商、客户建立了长期稳定的合作关系，坚持“顾客至上、质量优质、不断创新”的企业使命，为客户及消费者提供安全、优质的产品和服务。

营业收入构成（亿元）



2026年发展战略与经营计划

战略重点：

- I. 更深入研究密码技术：在后量子等先进密码技术方面发挥行业领先者优势，持续加强核心技术领先性，增加产业链产品覆盖度。
- II. 拓展更宽安全领域：由商用密码横向扩张至网络安全、数据治理、保密安全，形成四个领域的更长产品链，并推广海外业务。

总结：

这是一条以密码技术为轴、逐层外扩的路径：技术上深入后量子密码保持领先，客户上从银行向泛金融及财政、交通、公安等行业延伸，边界上从商用密码拓展至网络安全、数据治理、保密安全四个领域。2025年收入增长8.26%、扣非增长130.18%，是密码赛道里少数保持增长且盈利的公司。关键验证点是横向扩张的新领域能否形成第二收入支柱。

2025年经营情况回顾

2025年公司实现营业总收入5.42亿元，同比增长8.26%，连续第二年增长；公司综合毛利率下降1.99个百分点至69.24%，仍居19家前列；公司员工人数893人，减少31人，其中研发人员427人，减少29人、减员6.4%；销售人员161人，减少9人、减员5.3%；研发费用1.51亿元、同比下降12.48%，研发费用率降至27.9%、结束连续两年30%以上的高投入；公司人均创收59.7万元，较上年提升9.9万元；人均毛利41.3万元，较上年提升5.8万元。

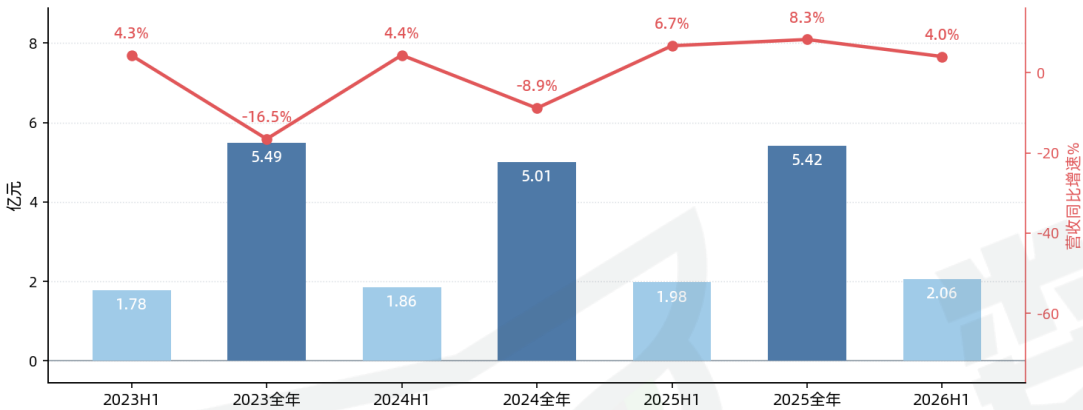
需关注：公司2025年度财务报告内部控制被出具否定意见。评估盈利修复时，应区分归母净利润、扣非净利润及非经常性损益，并结合研发支出会计处理和后续整改情况判断利润质量。

关键经营指标

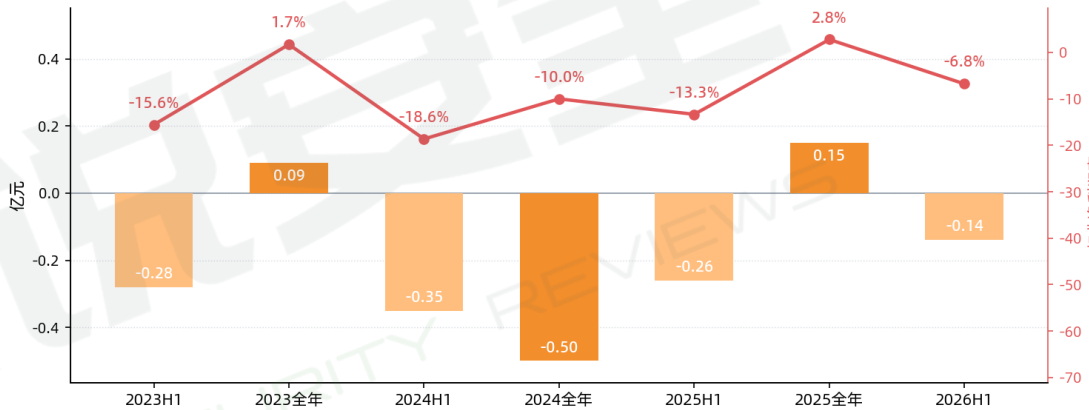
营业收入	营业收入同比增长	扣非净利润	员工人数
5.4亿元	8.3%	0.2亿元	893
资产总额	毛利率	经营性现金流净额	人均毛利
15.9亿元	69.2%	0.35亿元	41.3万元

2026年上半年营收2.06亿元、同比增长4.01%，增速为六年来最低但保持连续六年正增长；扣非净利润-0.14亿元、扣非净利润率由-13.3%收窄至-6.8%，亏损进一步收窄。毛利率74.19%、同比升6.85个百分点，为2020年以来最高——信息安全产品毛利率提升7.0个百分点至70.5%，高毛利的金融行业收入增19.8%、占比由40.5%升至46.7%，结构优化是主因。但经营性现金流净额-0.65亿元、净流出较上年同期扩大0.20亿元，销售回款仅增3.2%、慢于收入增速，利润改善尚未转化为现金。

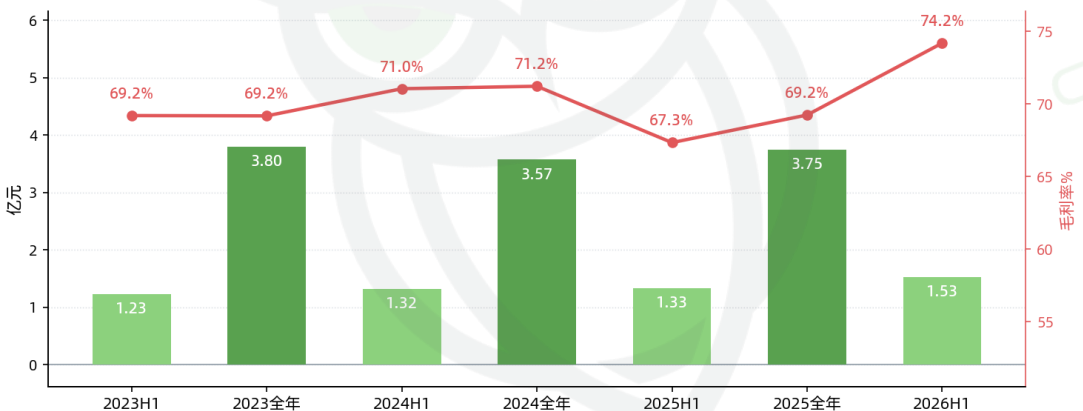
营业收入及同比增速



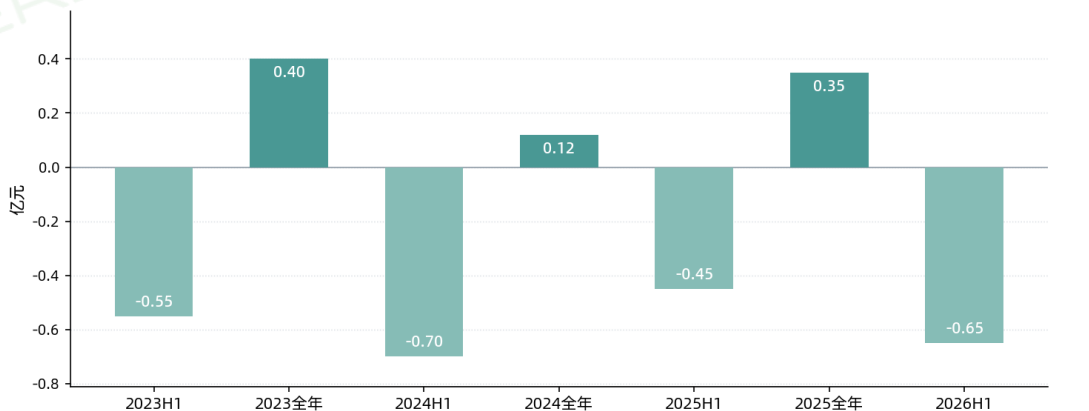
扣非净利润及扣非净利润率



毛利润及毛利率



经营活动现金流净额



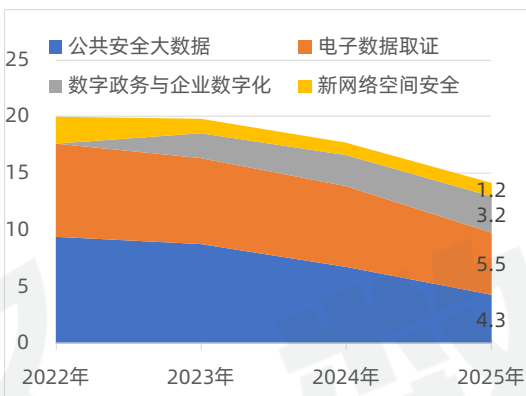
浅色 = 半年度 (1-6月累计) 深色 = 全年度 右轴比率/增速

公司介绍

国投智能是国内电子数据取证行业龙头企业、公共安全大数据领先企业、网络空间安全与社会治理 领域国家队。公司为国投集团旗下上市公司，实际控制人为国务院国资委。

使命与愿景：公司以国投集团和国投智能战略规划为指引，以服务国家数字中国、网络强国战略为己任，致力于成为国投智能数字经济产业布局的重要支撑，打造网络空间安全与社会治理的头部企业，建设世界一流大数据企业。

营业收入构成（亿元）



2026年发展战略与经营计划

战略重点：

- I. "两稳三拓一服务"战略框架：
- II. 全面深化“ALL IN AI”，瞄准具身智能全品类矩阵
- III. 国际市场与两金管控并行

总结：

公司的现金流已经先于利润触底——经营性现金流净额增长364.74%，但收现比由104.26%升至145.86%，属清收而非增收；收入端仍在寻底，基石业务的定价能力是更核心的问题，公共安全大数据毛利率已跌至8.27%。战略上以“两稳三拓一服务”重构布局，具身智能瞄准安防机器人全品类矩阵。关键验证点是2026年“三拓”新业务能否形成规模收入，以及商誉减值是否已经出清。

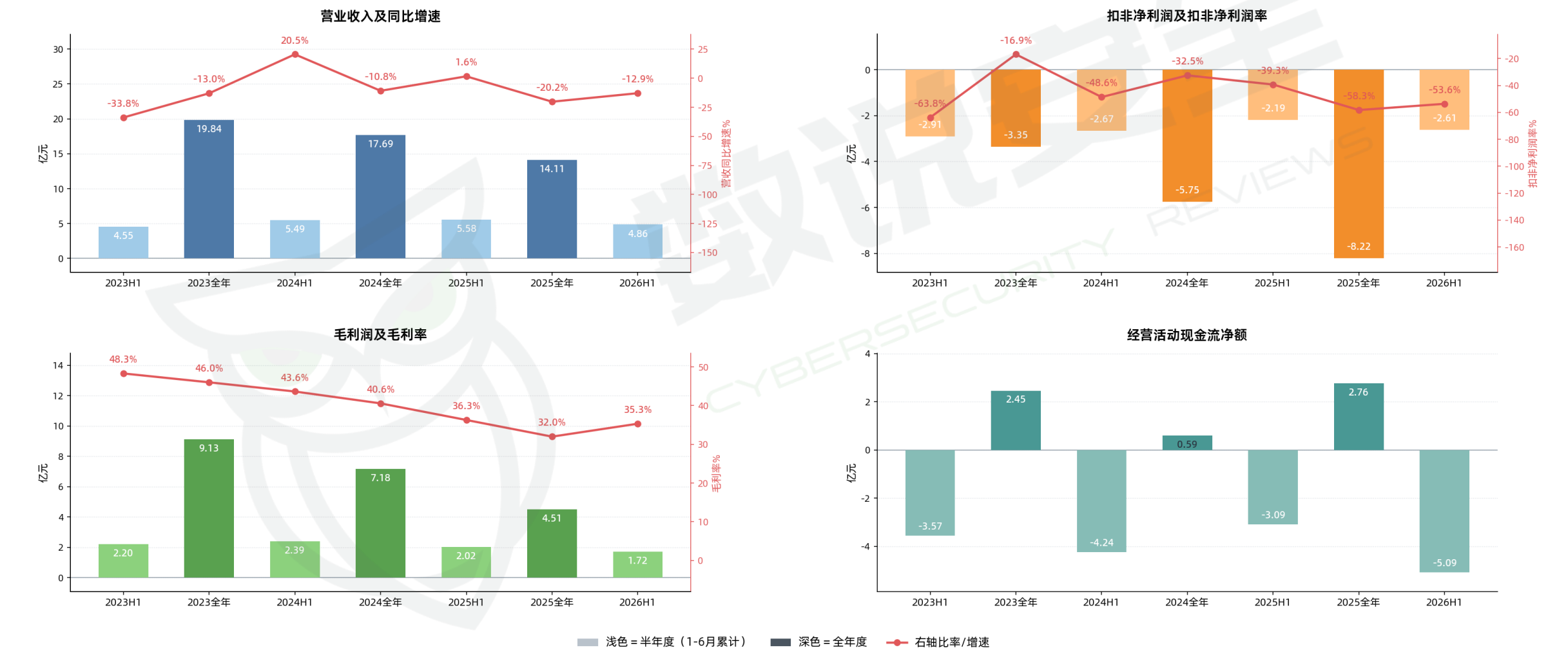
2025年经营情况回顾

2025年公司实现营业总收入14.11亿元，同比下滑20.23%；电子数据取证收入5.48亿元，同比下滑23.03%，毛利率50.17%、下降9.48个百分点；公共安全大数据收入4.26亿元，同比下滑36.66%，毛利率8.27%、下降13.22个百分点；数字政务与企业数字化收入3.20亿元，同比增长14.79%，毛利率26.45%；新网络空间安全收入1.18亿元，同比增长10.51%，毛利率48.17%；公司综合毛利率下降8.59个百分点至31.99%；公司员工人数2507人；归母净利润-7.82亿元、亏损扩大88.42%，扣非净利润-8.22亿元；经营性现金流净额2.76亿元，同比增长364.74%。传统核心业务承压，新兴业务规模尚不足以对冲。全年减值合计3.67亿元，其中商誉减值1.82亿元；期末商誉余额5.76亿元，后续仍需关注减值风险。

关键经营指标

营业收入	营业收入同比增长	扣非净利润	员工人数
14.1亿元	-20.2%	-8.2亿元	2507
资产总额	毛利率	经营性现金流净额	人均毛利
45.3亿元	32%	2.76亿元	17.9万元

2026年上半年营收4.86亿元、同比下滑12.89%；扣非净利润-2.61亿元、扣非净利润率由-39.3%恶化至-53.6%，亏损随规模收缩反而扩大。毛利率35.33%、同比降0.96个百分点，已连续五年下行（2021年同期为60.26%）——唯一增长的公共安全数智化业务毛利率仅29.15%，高毛利的电子数据取证收入降10.7%、毛利率再降7.4个百分点。费用结构剧烈重排：研发费用减0.83亿元（-53.9%）、销售费用增0.74亿元（+48.3%），一减一增几乎等额。经营性现金流净额-5.09亿元、净流出较上年同期扩大2.00亿元。

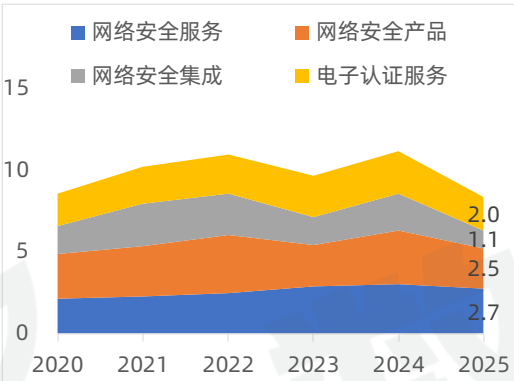


公司介绍

数字认证是领先的网络安全解决方案提供商，始终致力于保障用户网络基础设施安全可靠运行、保护用户网上业务安全可信开展、保卫用户数据安全。公司面向全国客户提供电子 认证服务、网络安全产品、网络安全集成、网络安全服务，并在政务、卫生、金融、企业、教育等领域建立领先优势。

企业使命：提供高品质的网络安全服务，帮助用户构建安全可信的网络空间
企业愿景：共建可信任的数字世界

营业收入构成（亿元）



2025年经营情况回顾

2025年公司实现营业总收入8.39亿元，同比下滑25.28%，创近五年最大降幅；网络安全服务收入2.75亿元，同比下滑9.67%，毛利率37.71%、下降10.67个百分点；网络安全产品收入2.51亿元，同比下滑24.27%，毛利率49.90%、下降4.86个百分点；电子认证服务收入2.05亿元，同比下滑21.52%，毛利率50.02%、下降11.31个百分点；公司综合毛利率下降5.13个百分点至42.18%；公司员工人数1446人，减少27人，其中研发人员948人，减少27人、减员2.8%；销售人员228人，增加6人、增员2.7%；公司人均创收57.5万元，较上年下降17.1万元；人均毛利24.2万元，较上年下降11.1万元。

2026年发展战略与经营计划

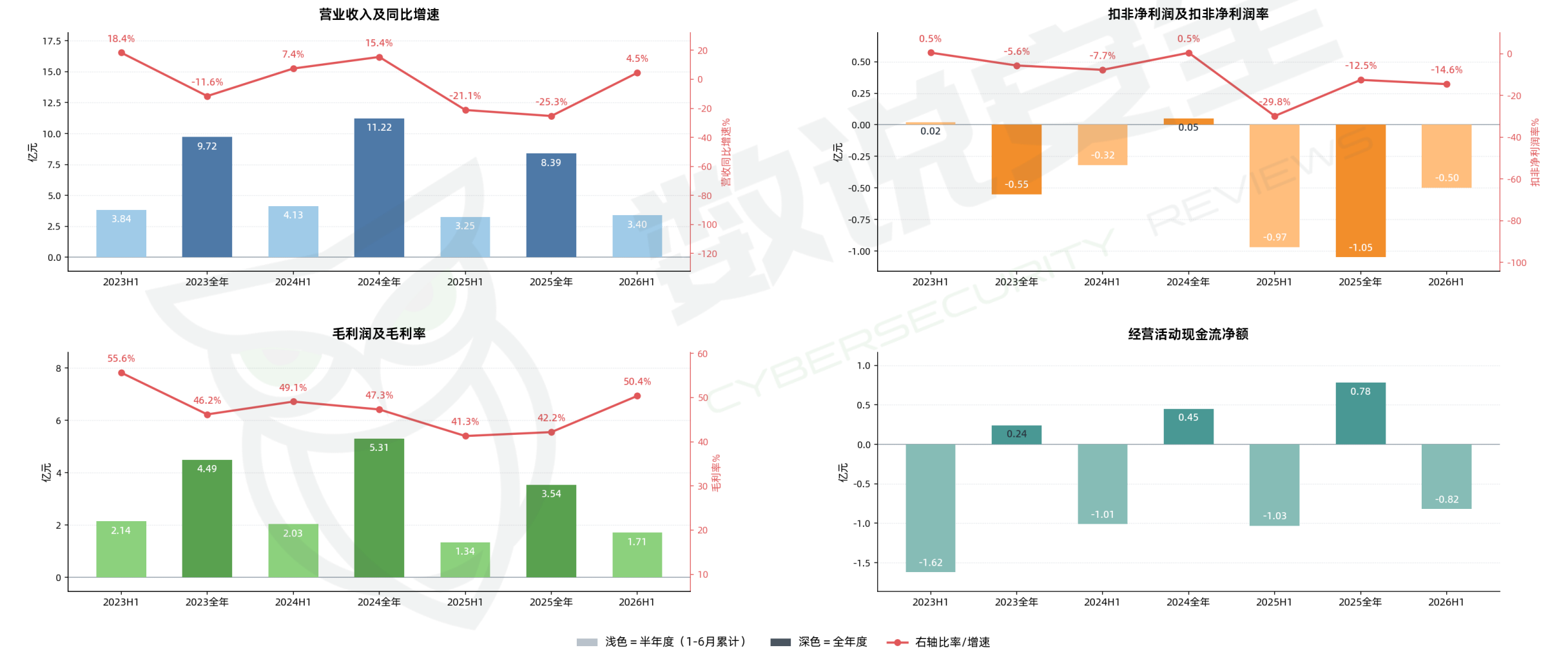
- 战略重点：**
- I. 围绕以密码为核心的技术能力，布局"网络安全基础设施""网上业务安全可信""数据资源安全可控"三条业务主航道。
 - II. 加快前沿技术攻关：推动抗量子密码、可信数据空间、人工智能安全等核心技术研发与商业化落地。

总结：
现金流改善是回款管理结果，但它掩盖不了主业的全面失速——各业务线收入均下滑，其中多条业务线降幅超过20%，综合毛利率跌至42.18%的近五年低点。战略上守住“网络安全基础设施安全可靠运行、网上业务安全可信开展、数据资源安全可控应用”三条主航道，增量指向车路云一体化、数字化健康服务与智慧教育。

关键经营指标

营业收入	营业收入同比增长	扣非净利润	员工人数
8.4亿元	-25.3%	-1.05亿元	1446
资产总额	毛利率	经营性现金流净额	人均毛利
15.1亿元	42.2%	0.78亿元	24.2万元

2026年上半年营收3.40亿元、同比增长4.52%，扭转上年同期-21.13%的下滑；扣非净利润-0.50亿元、扣非净利润率由-29.8%收窄至-14.6%，按展示值改善约15.2个百分点。毛利率50.38%、同比升9.07个百分点——主动收缩毛利率仅4.9%的网络安全集成业务（-18.0%），同时高毛利的电子认证服务增18.4%、占比升至35.4%，是典型的以规模换质量。经营性现金流净额-0.82亿元、净流出较上年同期收窄0.21亿元；合同负债增27.8%至3.98亿元，在手订单为下半年提供支撑。

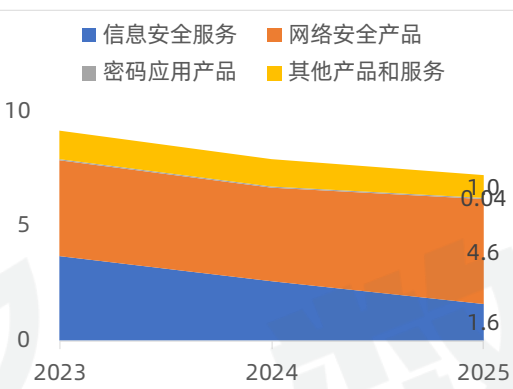


公司介绍

中孚信息以保障国家网络空间安全战略为目标，遵从等级保护、分级保护、数据安全、密码安全、商业秘密、个人信息保护等相关法律法规和标准要求，以合规防护为基础，以实战对抗为导向，聚焦数据安全，积极做深、谨慎做宽，持续推进公司从“保密安全”到“数据安全”的战略拓展。

企业使命：保障国家网络安全，创造员工幸福家园
企业愿景：构建网络空间对抗能力，让数字中国更安全

营业收入构成（亿元）



2025年经营情况回顾

2025年公司实现营业总收入7.25亿元，同比下滑7.71%，连续第三年下滑；网络安全产品收入4.59亿元，同比增长11.85%，毛利率83.70%、下降0.05个百分点；信息安全服务收入1.61亿元，同比下滑36.64%，毛利率34.99%、下降5.78个百分点；其他产品和服务收入0.97亿元，同比下滑15.71%，毛利率58.03%、提升3.02个百分点；公司综合毛利率提升3.63个百分点至69.02%；公司员工人数1956人，减少197人，其中研发人员816人，减少107人、减员11.6%；销售人员375人，减少30人、减员7.4%；公司人均创收35.3万元，较上年提升0.8万元；人均毛利24.3万元，较上年提升1.8万元。

2026年发展战略与经营计划

战略重点：

- I. AI原生平台：布局AI在保密安全与数据安全典型行业的落地应用，构建AI原生平台底座，推动AI与产品深度融合。
- II. 降本增效并举：推进标准化交付、控制安装部署与运维成本，提升精细化管理水平以改善盈利能力。

总结：

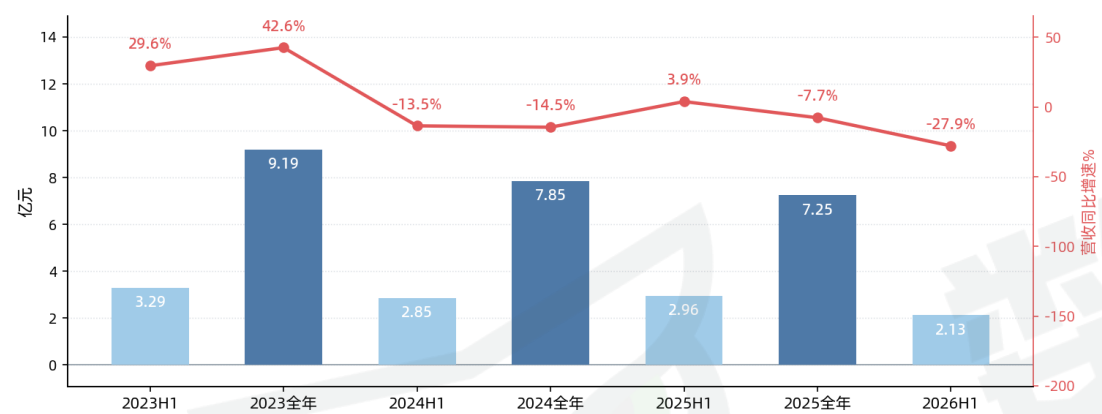
公司在党政、防务、军工三大涉密主场收缩规模、保住高毛利产品基本盘的一年，盈利拐点尚未到来，研发资本化率下调7.27个百分点，利润含金量提升。战略上最值得注意的是“形成多业务风险对冲的可持续发展能力”，关键验证点是2026年高毛利的网络安全产品能否继续逆势增长，对冲信息安全服务收入下降36.64%留下的缺口。

关键经营指标

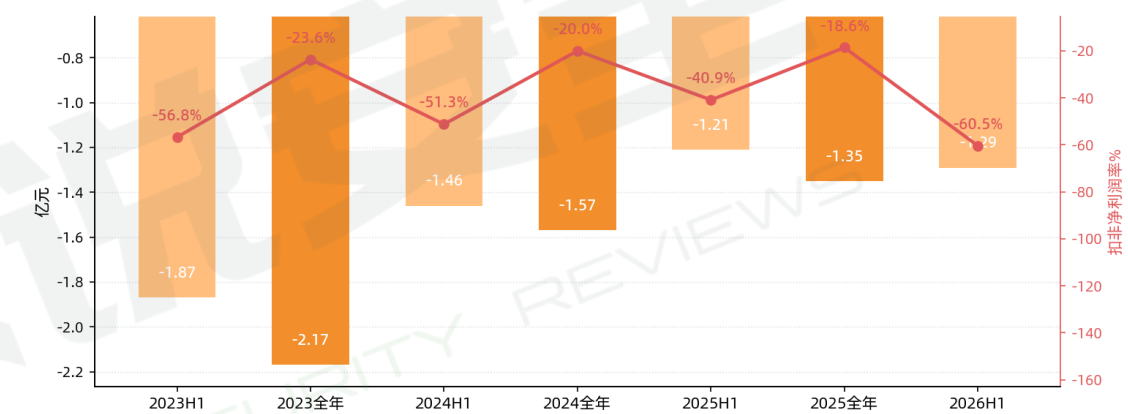
营业收入	营业收入同比增长	扣非净利润	员工人数
7.25亿元	-7.7%	-1.35亿元	1956
资产总额	毛利率	经营性现金流净额	人均毛利
18.3亿元	69%	0.61亿元	24.3万元

2026年上半年营收2.13亿元、同比下滑27.89%，降幅较大；扣非净利润-1.29亿元、扣非净利润率由-40.9%恶化至-60.5%，亏损缺口接近收入的六成。毛利率78.07%、同比升9.28个百分点看似亮眼，但成因是低毛利业务被砍——信息安全服务收入降54.2%、其他产品和服务降43.6%，高毛利网络安全产品占比由62.9%升至74.4%，毛利率提升来自结构而非定价。费用则高度刚性：研发费用几乎未动（-0.89%），研发费用率由46.3%升至63.6%。经营性现金流净额-0.57亿元、净流出较上年同期收窄0.42亿元。

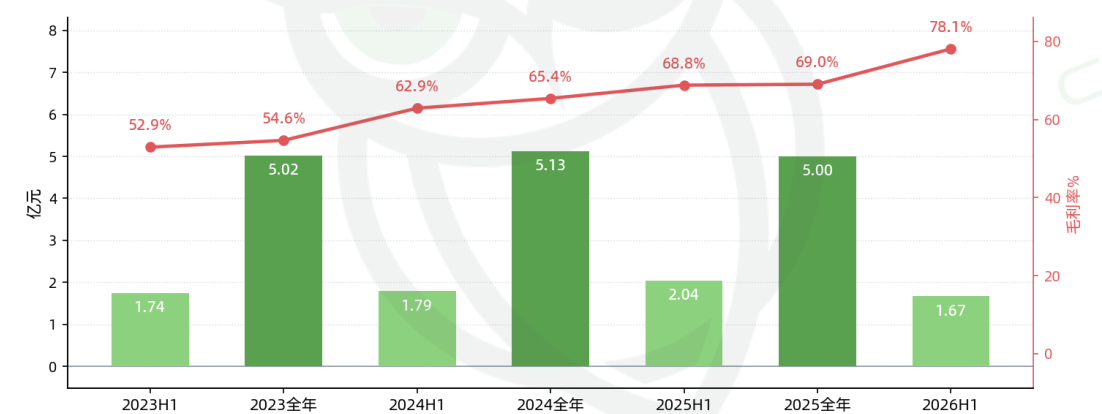
营业收入及同比增速



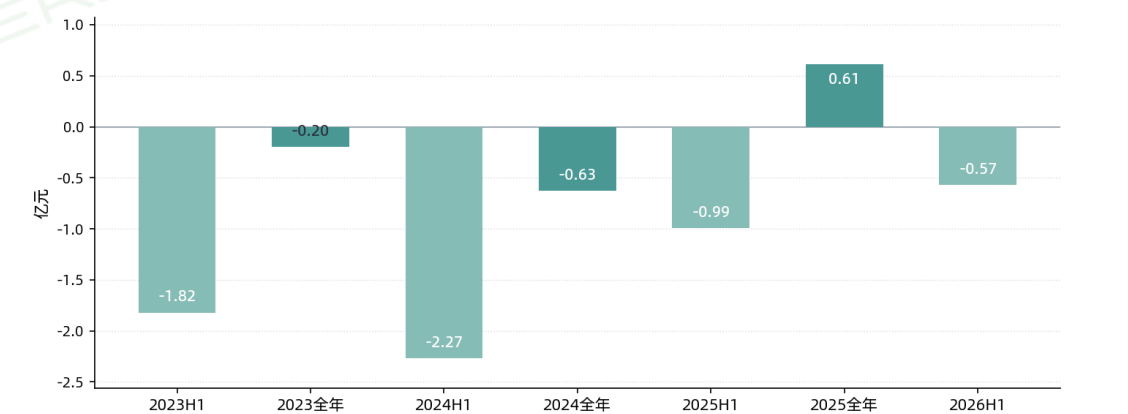
扣非净利润及扣非净利润率



毛利润及毛利率



经营活动现金流净额



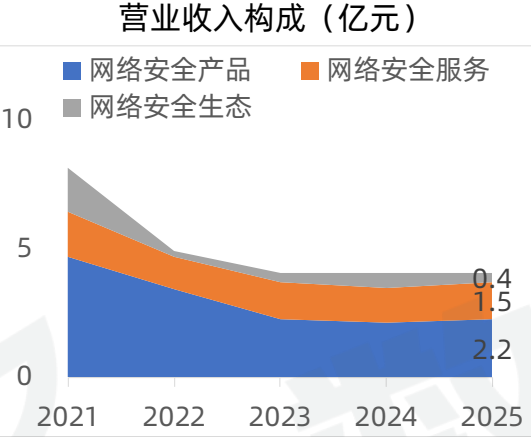
浅色 = 半年度（1-6月累计） 深色 = 全年度 右轴比率/增速

公司介绍

吉大正元以密码技术为核心，开展信息安全软件的研发、生产和销售及服务，面向政府、军工、金融、能源、电信等重点行业和领域提供基于密码的可信身份认证及可信数据保障等多层次、全方位的综合安全解决方案，为其信息系统提供关键的安全支撑与保障。

企业使命：数字世界的守护者，数字伦理的捍卫者

企业愿景：全球一流的数字安全企业



2025年经营情况回顾

2025年公司实现营业总收入4.07亿元，同比基本持平，结束2021年以来连续三年下滑；网络安全产品收入2.24亿元，同比增长5.68%，毛利率54.55%、下降1.12个百分点；网络安全服务收入1.46亿元，同比增长6.71%，毛利率58.26%、下降5.15个百分点；网络安全生态收入0.36亿元，同比下滑37.61%，毛利率28.07%、提升10.25个百分点；公司综合毛利率提升0.59个百分点至53.55%；公司员工人数740人，减少65人，其中研发人员243人，减少9人、减员3.6%；销售人员150人，减少13人、减员8.0%；公司人均创收52.6万元，较上年提升4.9万元；人均毛利28.2万元，较上年提升2.9万元。

2026年发展战略与经营计划

战略与经营重点：

- I. "密码+AI"双核驱动：构建抗量子演进的PKI产品体系，推出AI全链路防护产品，加速抗量子密码与全栈信创能力升级。
- II. 拓展泛安全新场景：聚焦卫星互联网、低空经济、算力网络安全等新兴领域规模化落地。

总结：

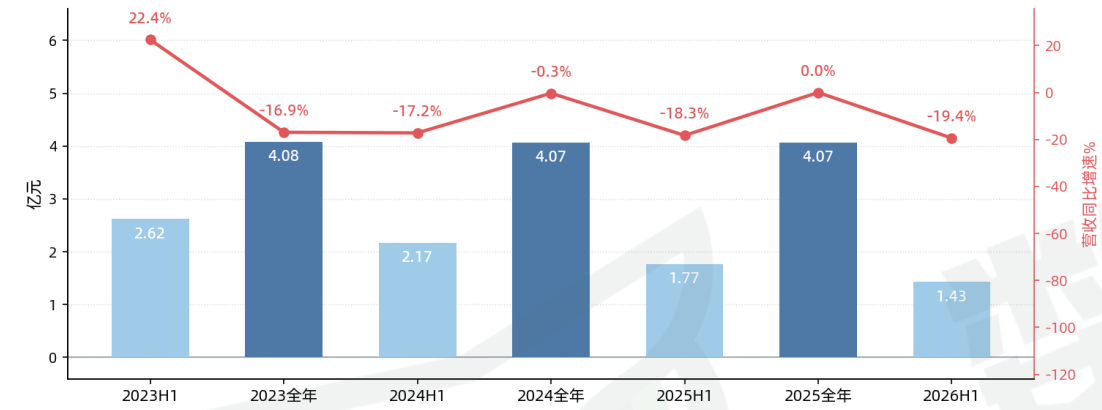
公司的收入已止跌、费用已大幅出清，但盈利尚未回到经营自造血状态——2025年收入基本持平、扣非减亏13.29%，但研发费用压缩34.00%为全行业最大降幅。战略上以“密码+AI”双核驱动，推动传统密码产品向抗量子、智能化演进并延伸至卫星、低空场景。关键验证点是2026年减值能否收窄、新业务能否把持平的收入重新推回增长。

关键经营指标

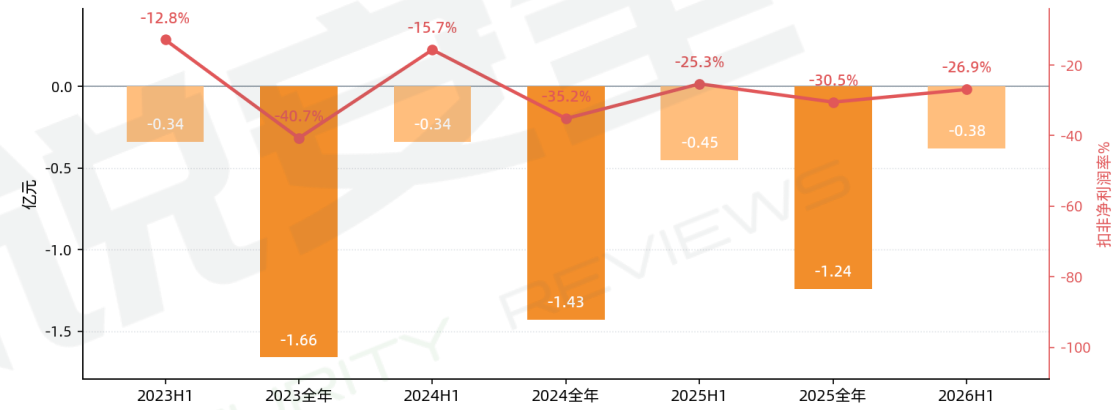
营业收入	营业收入同比增长	扣非净利润	员工人数
4.1亿元	0.0%	-1.24亿元	740
资产总额	毛利率	经营性现金流净额	人均毛利
17.2亿元	53.6%	-0.43亿元	28.2万元

2026年上半年营收1.43亿元、同比下滑19.41%，为连续第四年同期下滑，产品、服务、生态三块同步收缩约20%，无结构性亮点；扣非净利润-0.38亿元、扣非净利润率由-25.3%微降至-26.9%。毛利率53.46%、同比降2.02个百分点——网络安全产品毛利率降9.3个百分点至51.0%，网络安全生态从29.7%降至12.3%，仅服务业务升13.1个百分点对冲了一部分。亮点在现金：经营性现金流净额+0.18亿元、由上年同期的-0.58亿元转正，销售回款增36.2%、应收账款及票据降18.9%。

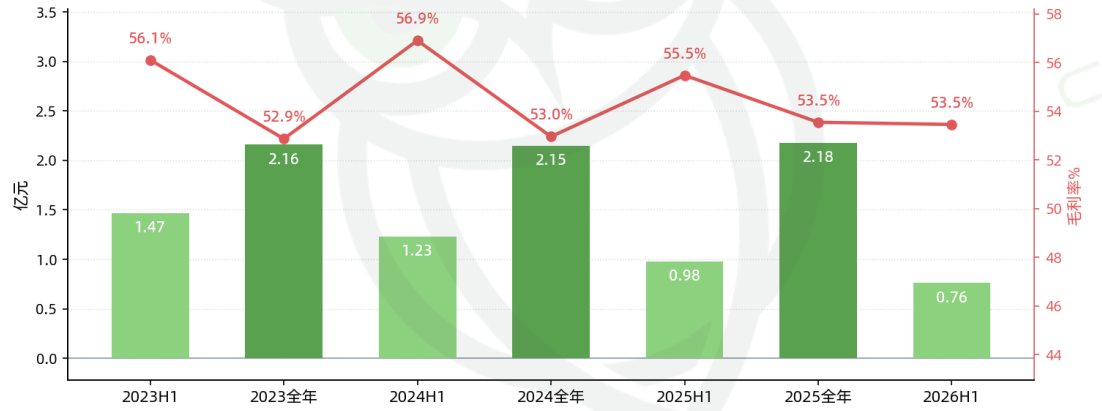
营业收入及同比增速



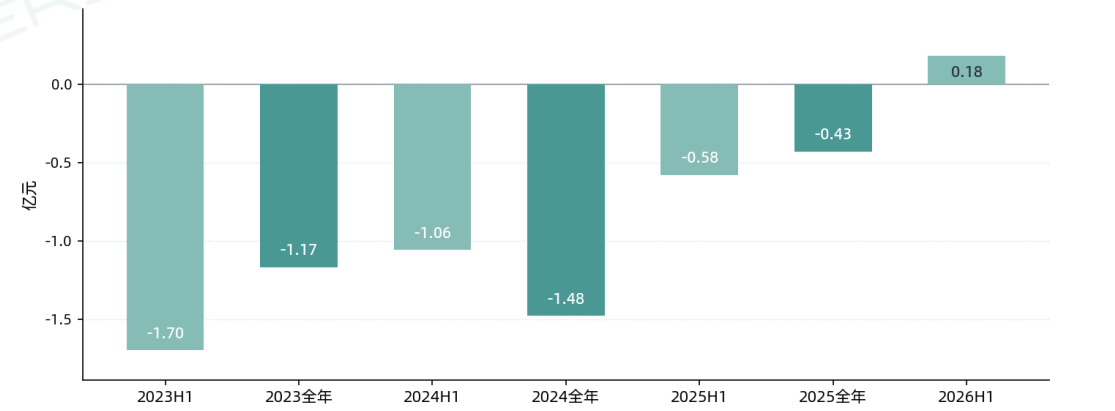
扣非净利润及扣非净利润率



毛利润及毛利率



经营活动现金流净额



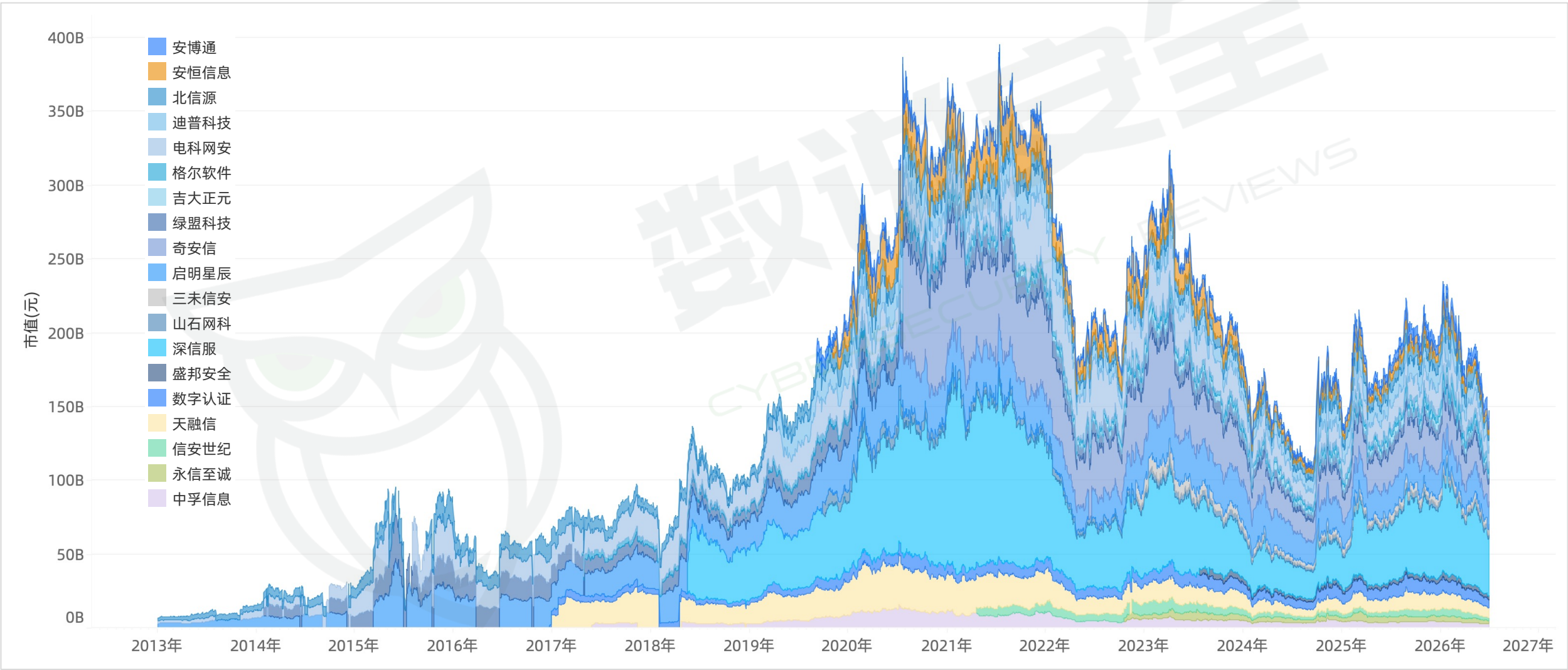
浅色 = 半年度（1-6月累计） 深色 = 全年度 右轴比率/增速

二级市场市值与估值分析

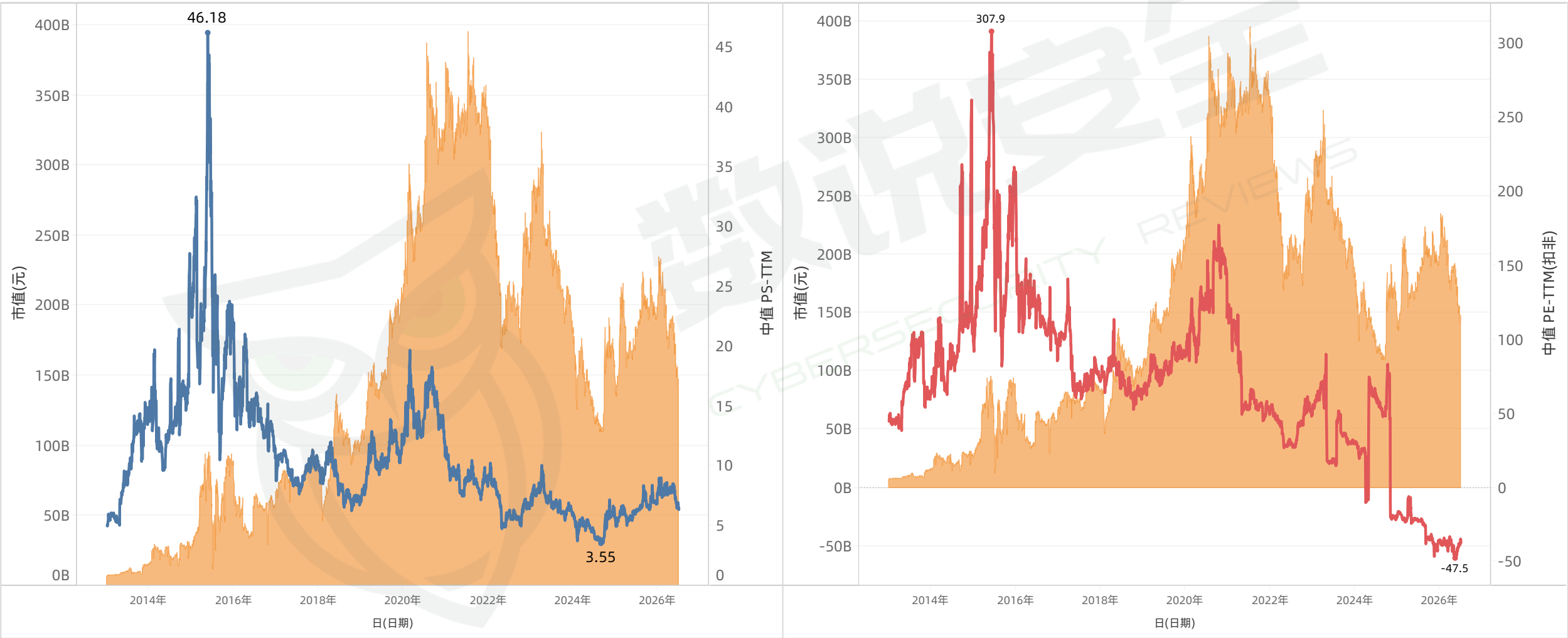
我国有网络安全相关业务的上市公司50余家。本节选取其中19家代表性公司分析市值与估值，包括专业安全厂商及部分兼营其他业务的公司。估值按上市公司整体口径计算，不等同于其安全业务单独估值。

 WebRAY 盛邦安全	 奇安信 新一代网络安全领军者	 青云 QING CLOUD	 浩瀚深度 HAOHAN Data	 亚信安全	 纬德信息 WEIDE INFO
 sansec 三未信安	 永信至诚	 UCLLOUD 优刻得	 yytek 云涌科技	 中科曙光 Sugon	 360
 信安世纪 infosec	 ABT·安博通 看透安全 体验价值	 Neusoft 东软	 中软 CS&S	 FiberHome	 亨通光电 HENG TONG OPTIC-ELECTRIC
 Hillstone 山石网科	 安恒信息 DAS-security 安全中国	 亿阳信通	 Aisino	 卓朗科技 TROILA TECHNOLOGY	 WJP 佳缘科技
 格尔软件 KOAL SOFTWARE	 DP tech 杭州迪普科技有限公司	 左江	 熙菱信息 SAILING	 飞天诚信 我们 构筑 安全	 东方通 TongTech
 中孚信息	 数字认证	 任子行 SURFILTER	 拓尔思 TRS	 美亚柏科 - MEIYA PICO -	 网宿科技 WANGSU.COM
 SANGFOR 深信服科技	 NSFOCUS	 Ultrapower 神州泰岳	 inovatio 中新赛克	 恒久 TOLDENGREEN	 通鼎互联
 北信源 VRV	 吉大正元	 榕基软件 RONGJI	 TAIJI 太极	 启明信息 QIMING INFORMATION	 unis 紫光
 启明星辰 领航信息安全	 CEIC 电科网安	 高鸿股份	 神州数码 Digital China	 GH-TECH 國華網安	
 天融信 TOPSEC					

自2023年4月起，我国网络安全上市公司的总市值经历了连续下滑，至2024年9月降至1088亿元的阶段低点，这一数值与2019年初的水平相当，较2021年接近4000亿的历史峰值相比，总市值缩水近73%；2024年9月后，随着相关政策落地，网络安全上市公司市值震荡提升，在2026年1月到达阶段高点，总市值接近2350亿元，并在之后开始回落，2026年6月底总市值接近1500亿元，较1月份高点回落约37%。



网络安全上市公司PS-TTM中位数在2024年8月底创下历史新低3.55，低于2013年和2022年约5.0的低点，2026年1月底逐渐回升至近9.0，6月底又回落至6.35；由于近年来网安上市公司的单季度扣非净利润波动较大，因此扣非PE-TTM中位数也出现较大波动，但整体呈现下移趋势。

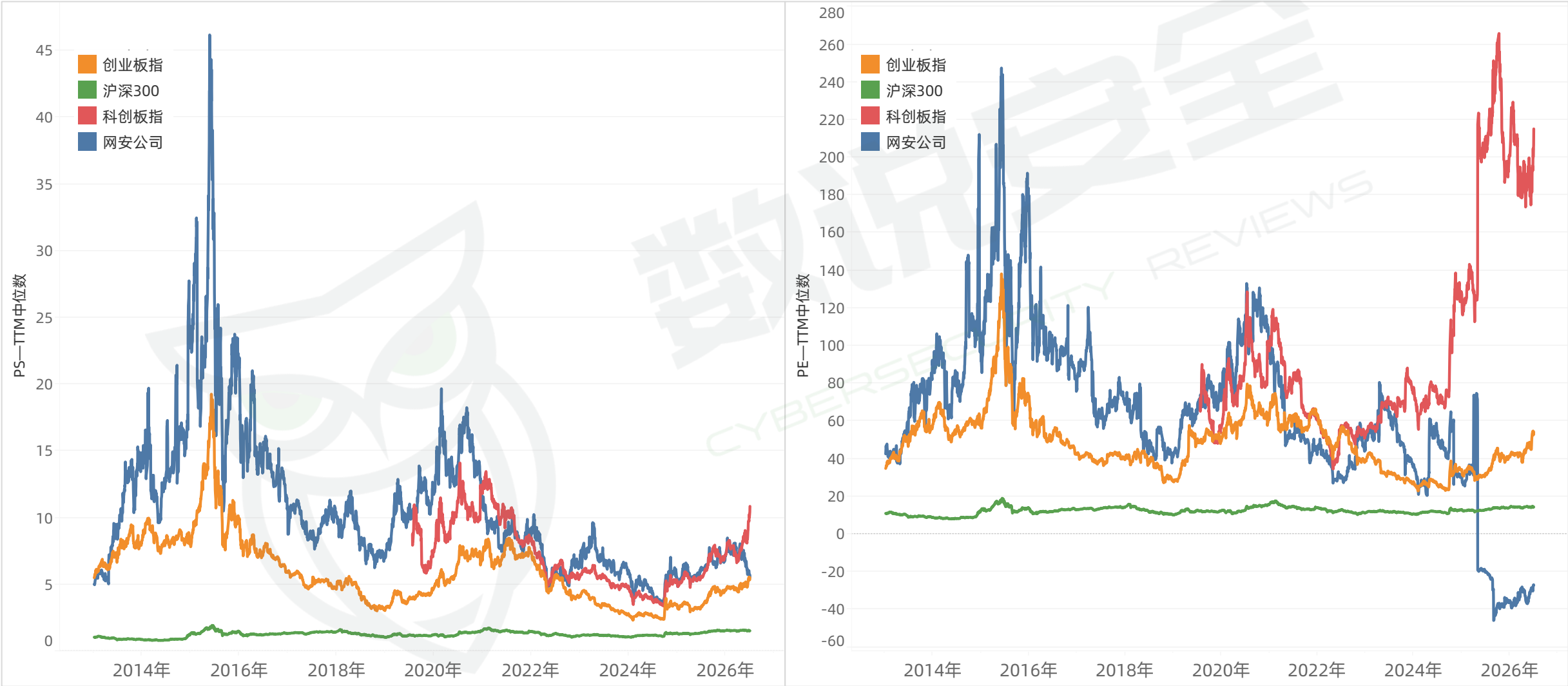


(截至2026年6月30日)

网络安全上市公司估值水平~科创板指 > 创业板指 > 沪深300

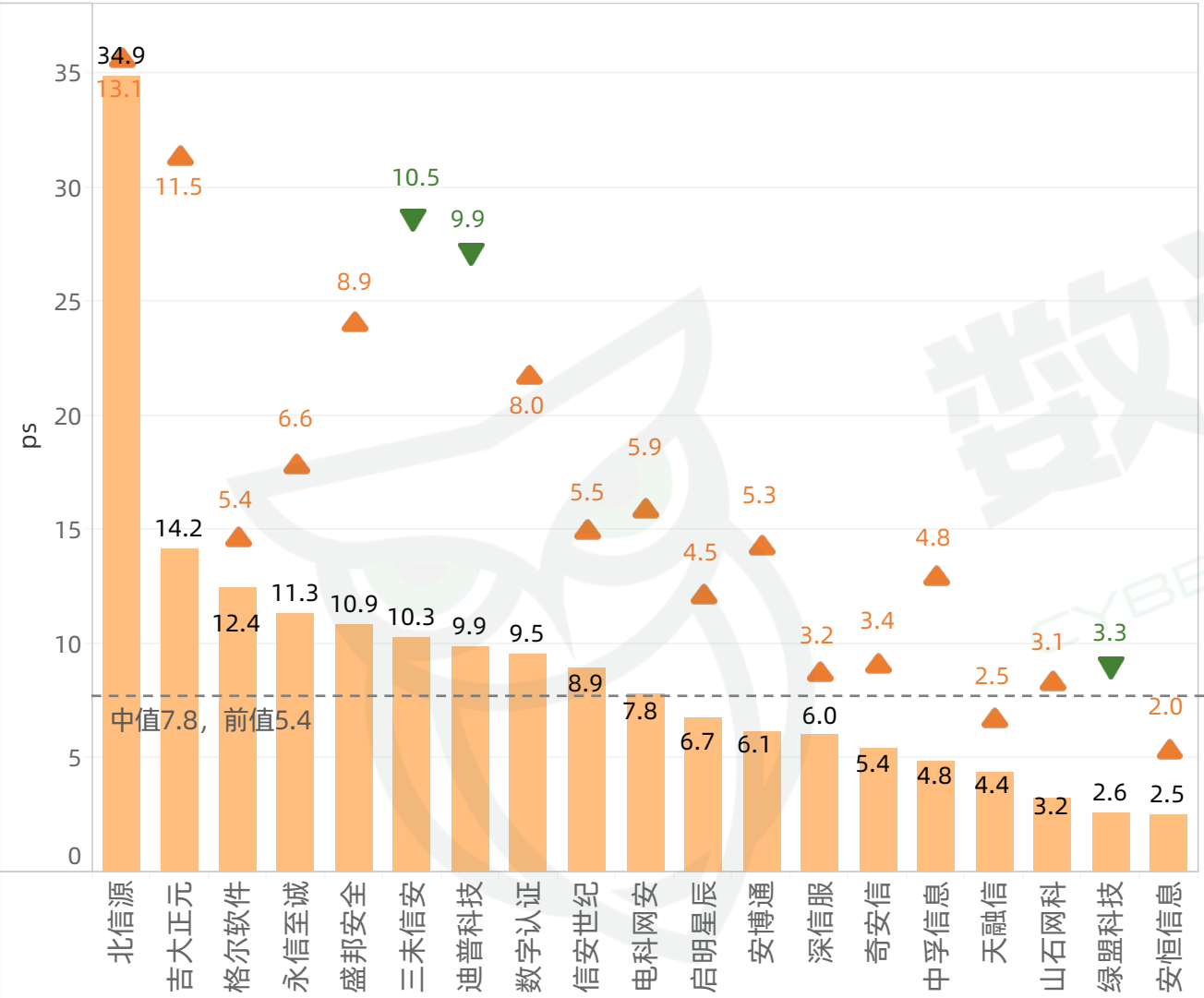


网络安全公司估值水平和科创板指数相关性较强，资本市场看好网络安全行业，愿意给出更高的估值水平，但由于AI和半导体相关公司多为科创板企业，且近年来涨幅较大，占科创板权重不断增加，因此近期估值与网络安全公司呈现背离走势。（PE-TTM中位数近期受市场波动及上市公司盈利情况影响较大，故暂时失去参照价值）

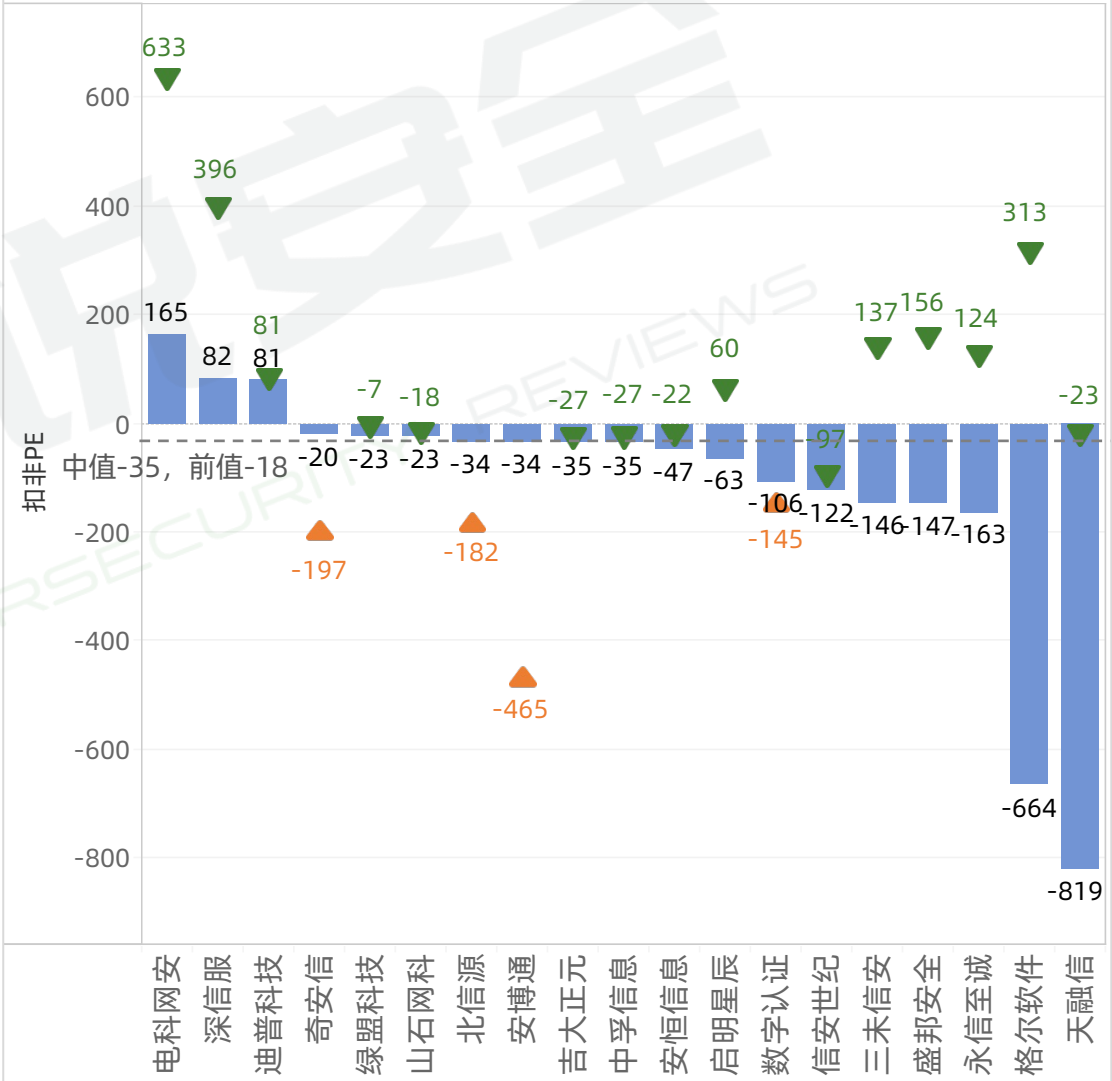


(截至2026年6月30日)

2024-2025年底PS变化

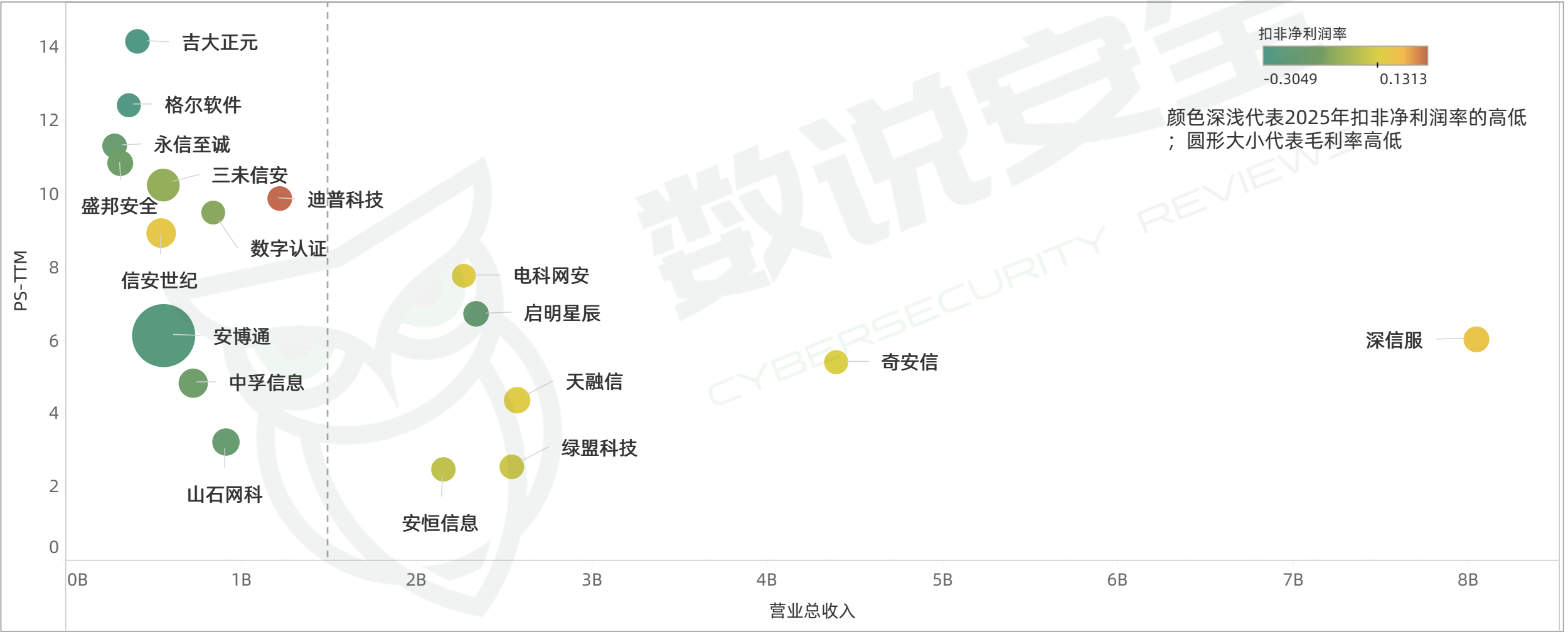


2024-2025年底扣非PE变化

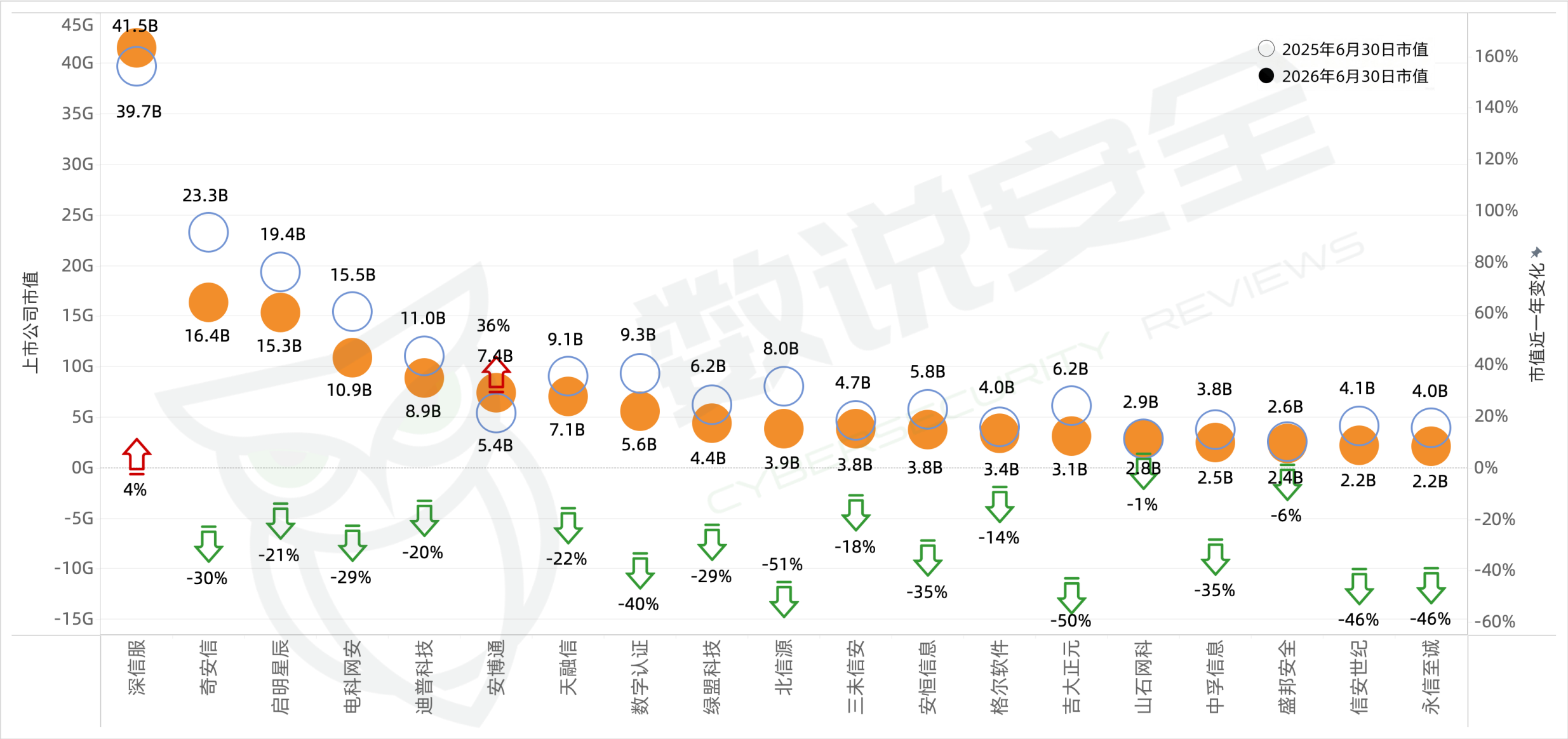


15亿收入以内的网安上市公司，估值水平与毛利率、扣非净利润率相关性较高，高毛利和高扣非净利润率的公司享有高估值；

15亿收入以上的网安上市公司，受到宏观环境和规模的影响相对较大，收入增长出现停滞，部分公司毛利率承压，企业间分化明显，估值水平定价逻辑尚不清晰。

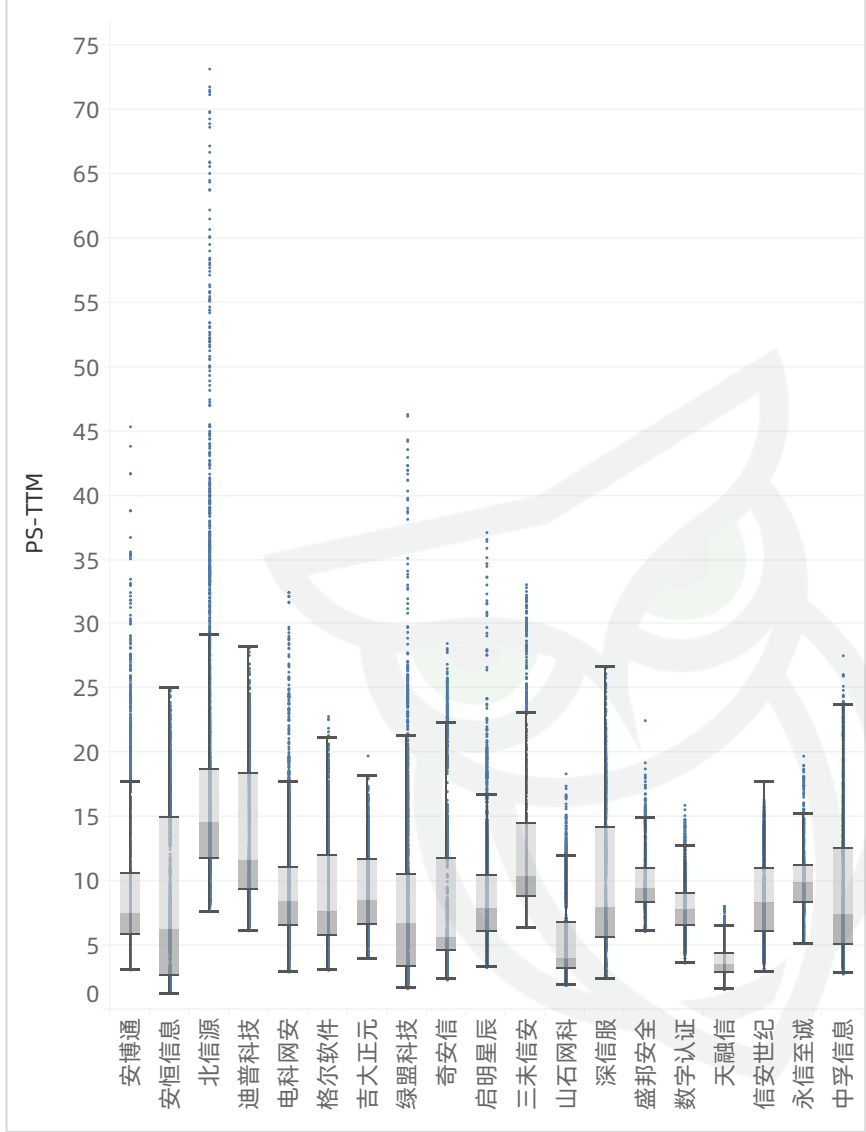


(2025年数据)



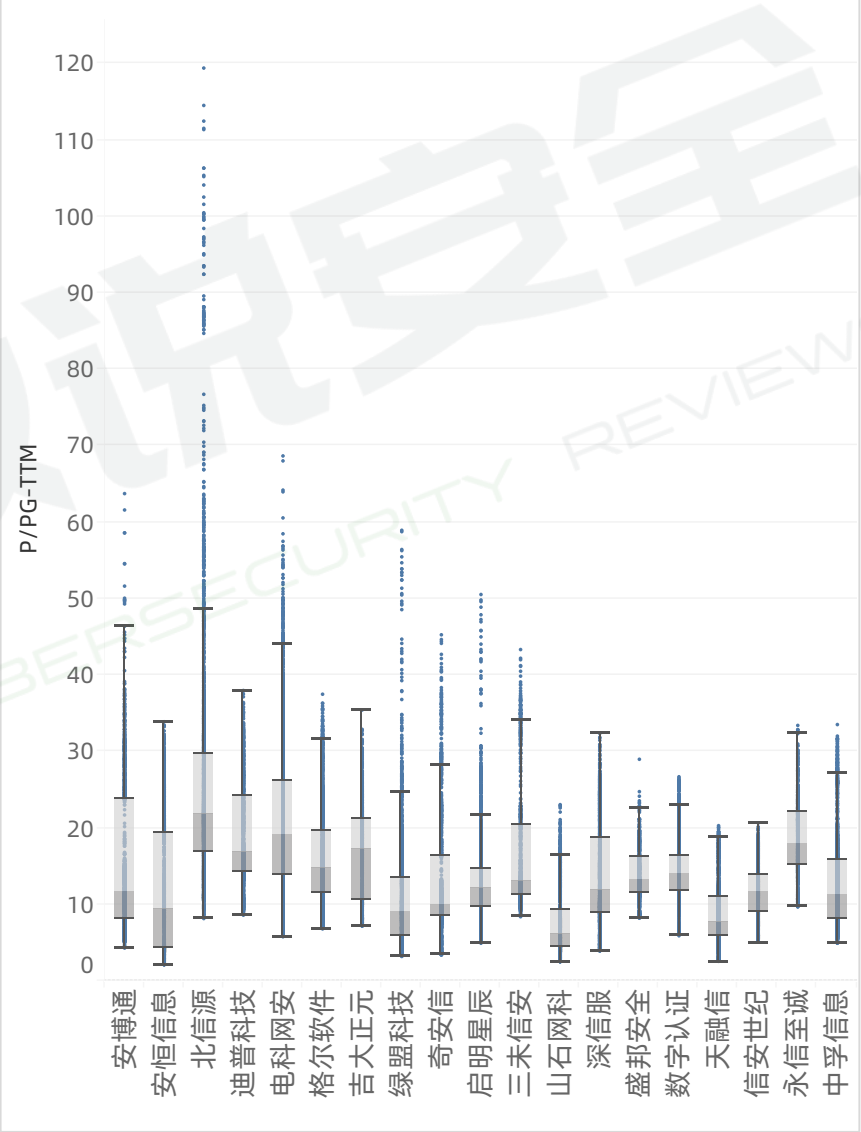
(数据区间自2025年6月30日至2026年6月30日)

上市公司PS区间



公司	PS中枢
安博通	7.5
安恒信息	6.3
北信源	14.5
迪普科技	11.6
电科网安	8.4
格尔软件	7.6
吉大正元	8.7
绿盟科技	6.7
奇安信	5.6
启明星辰	7.9
三未信安	10.4
山石网科	4.0
深信服	8.0
盛邦安全	9.4
数字认证	7.7
天融信	3.5
信安世纪	8.3
永信至诚	9.9
中孚信息	7.4

上市公司P/PG区间

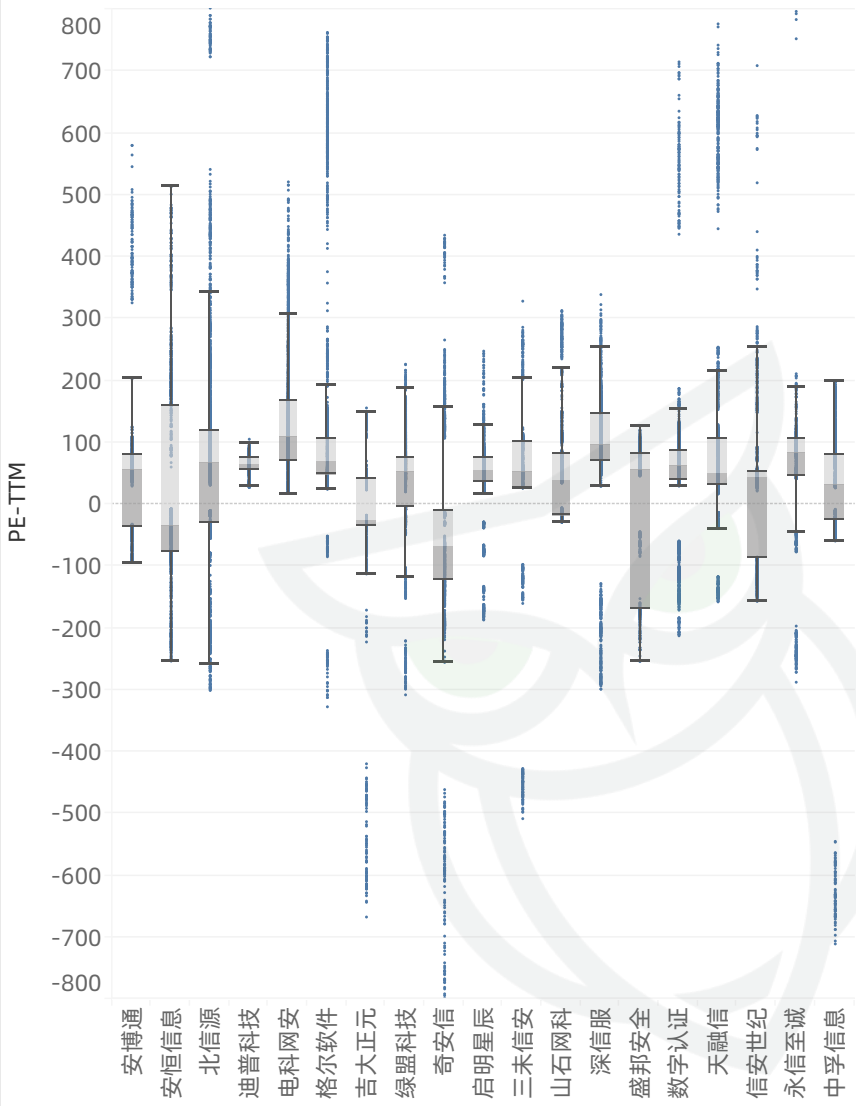


公司	P/PG中枢
安博通	11.6
安恒信息	9.4
北信源	21.8
迪普科技	16.8
电科网安	19.1
格尔软件	14.7
吉大正元	17.2
绿盟科技	9.0
奇安信	10.0
启明星辰	12.0
三未信安	13.0
山石网科	6.1
深信服	11.9
盛邦安全	13.2
数字认证	14.0
天融信	7.7
信安世纪	11.6
永信至诚	18.1
中孚信息	11.3

网络安全上市公司PE-TTM及PE-TTM（扣非）估值情况

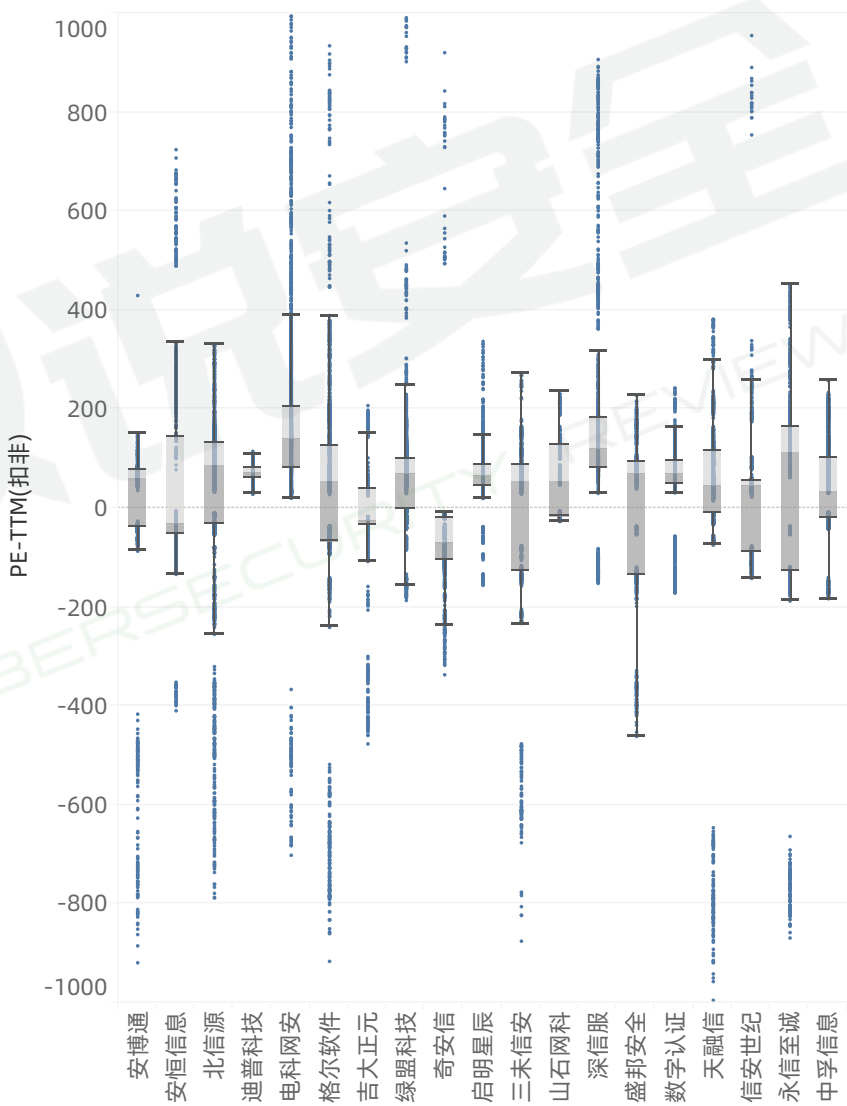


上市公司PE区间

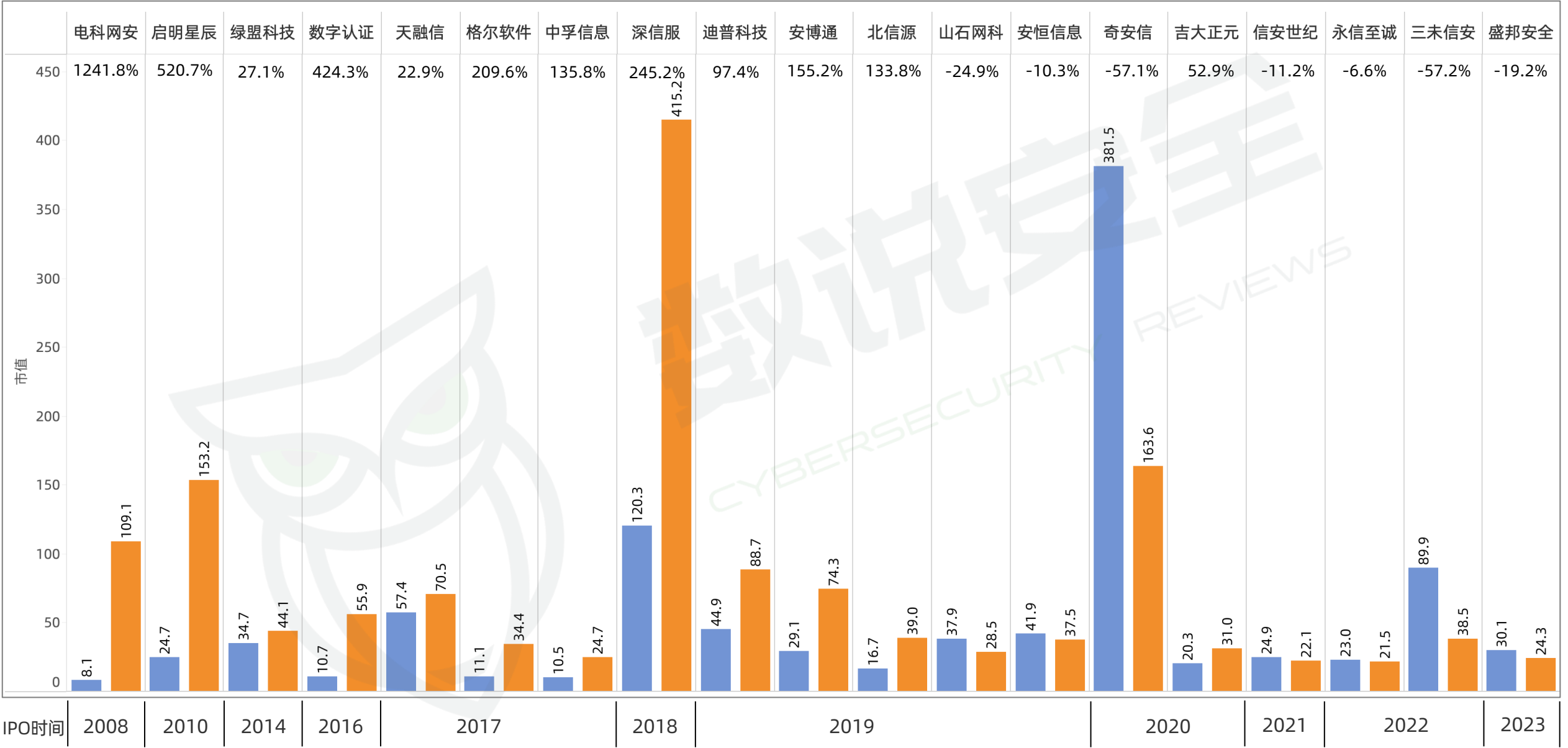


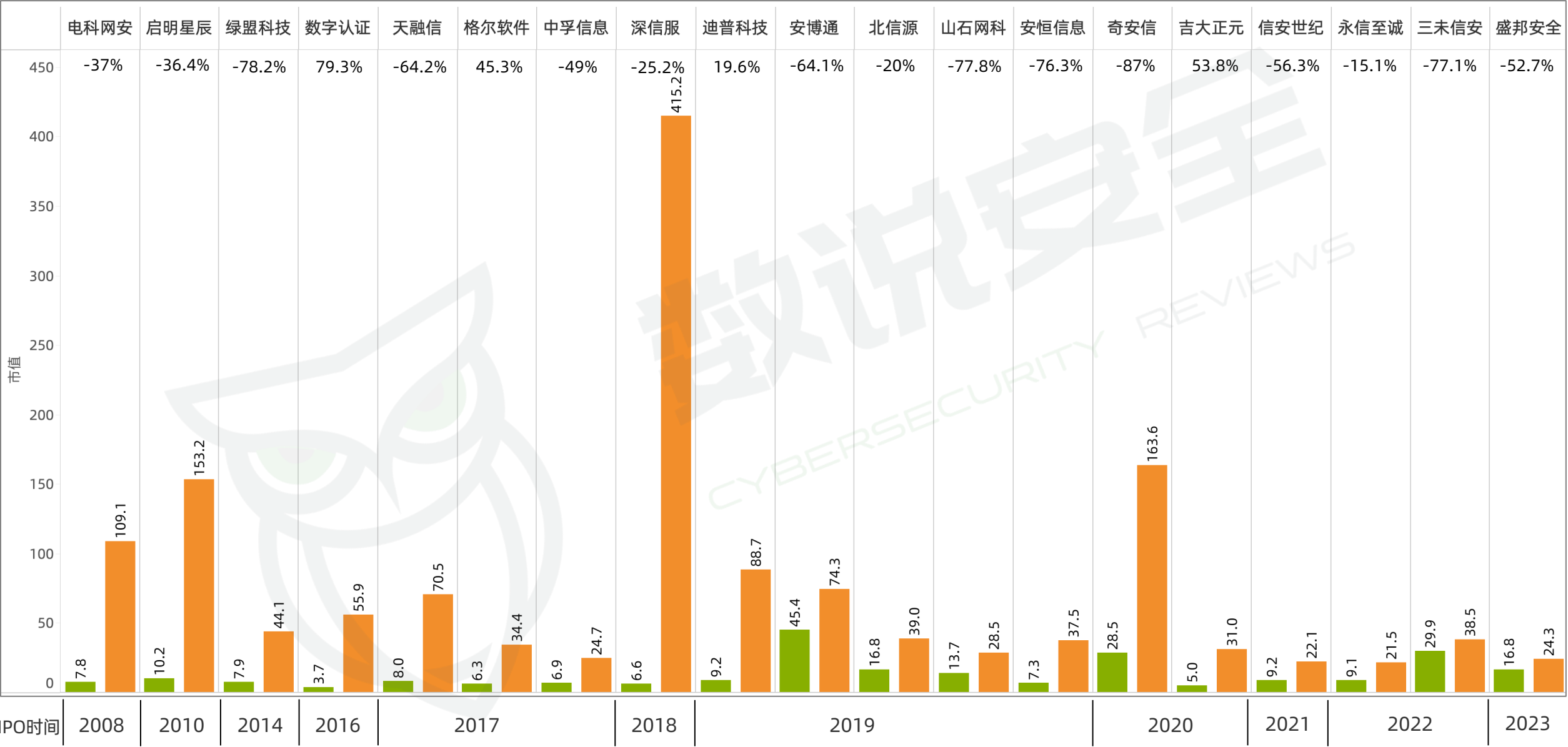
公司	PE中枢
安博通	54
安恒信息	-35
北信源	66
迪普科技	65
电科网安	109
格尔软件	70
吉大正元	-27
绿盟科技	52
奇安信	-68
启明星辰	55
三未信安	53
山石网科	39
深信服	95
盛邦安全	55
数字认证	61
天融信	50
信安世纪	42
永信至诚	83
中孚信息	30

上市公司扣非PE区间



公司	扣非PE中枢
安博通	59
安恒信息	-33
北信源	86
迪普科技	70
电科网安	139
格尔软件	54
吉大正元	-25
绿盟科技	67
奇安信	-71
启明星辰	65
三未信安	53
山石网科	53
深信服	117
盛邦安全	67
数字认证	73
天融信	69
信安世纪	45
永信至诚	113
中孚信息	33





中国网络安全一级市场分析

投融资市场概要

1 总量触底

2025年网安一级市场融资26笔、5.42亿元，较2021年高峰的197笔、142.6亿元分别下降87%和96%，为近年最低。2026年上半年10笔录得8.0亿元，已超2025年全年，但主要由长亭科技单笔5亿元交易拉动，尚不构成趋势反转。

2 资金集中

2025年各阶段同步收缩，扩张期公司以8次、2.0亿元融资相对抗跌，成长期金额仅1.1亿元回落最深。区域上北京、上海、浙江五年累计245亿元，占全国约八成。单笔大额与整体低位并存，资金正集中于少数确定性标的。

3 续轮变难

融资发生后24个月内再获下一轮的比例，由2019-2020年的71%至73%降至2024年可观察样本的约10%。拿到钱之后能否拿到下一轮，比当年融了多少笔更能说明存量项目的处境。

4 退出转向

2021年高峰期融资的150家企业中，48%未观察到后续新一轮融资；433家有融资记录的企业中最后一轮已超24个月。叠加对赌与回购条款集中进入到期窗口，被整合意愿上升；上市周期中位数14年，IPO难以承接存量。

5 资金结构

央国企出手减少，2025年投资9次、参与项目金额2.25亿元；但占全市场次数35%、金额42%，高于2021年的25%和35%，相对影响力提升。



• 行业遇冷：2025年融资26笔、5.42亿元，笔数与金额降至近年低点

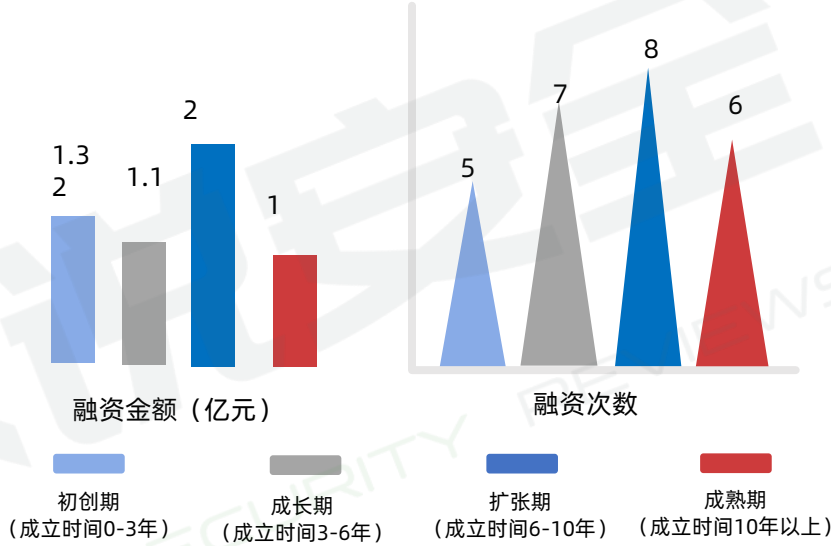


• 结构性分化：资本向少数热门赛道和优质企业集中

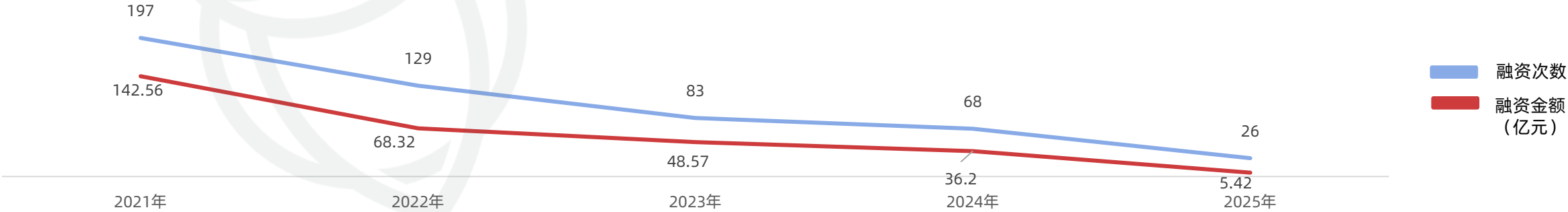


• 理性回归：投资者更加谨慎，偏好技术成熟度和商业模式相对清晰的领域

2025年中国网络安全不同阶段融资金额以及融资次数



2021年-2025年中国网络安全融资金额以及融资次数





持续收缩态势

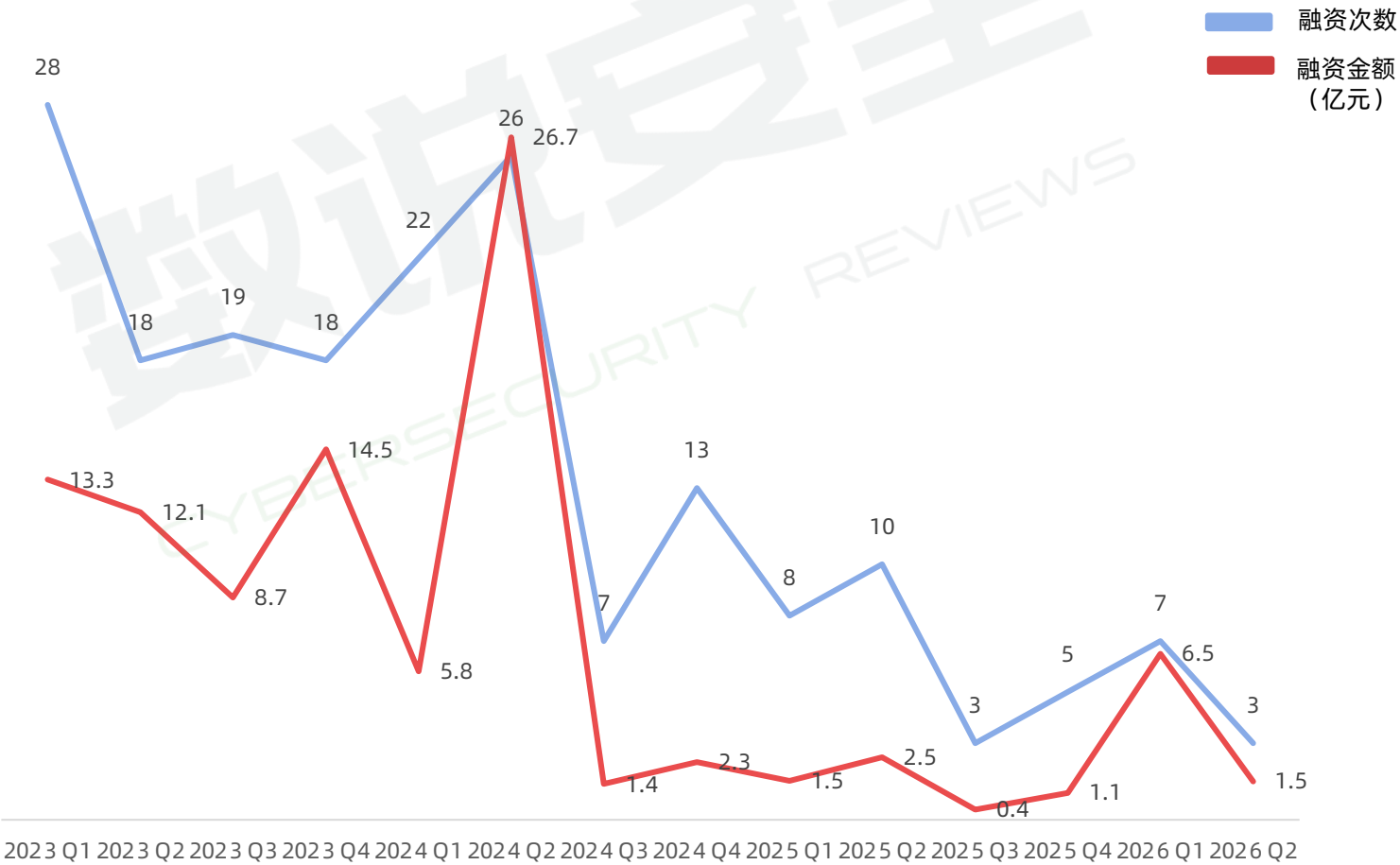
2025年融资次数与金额同步下行，2026年H1笔数仍处历史低位



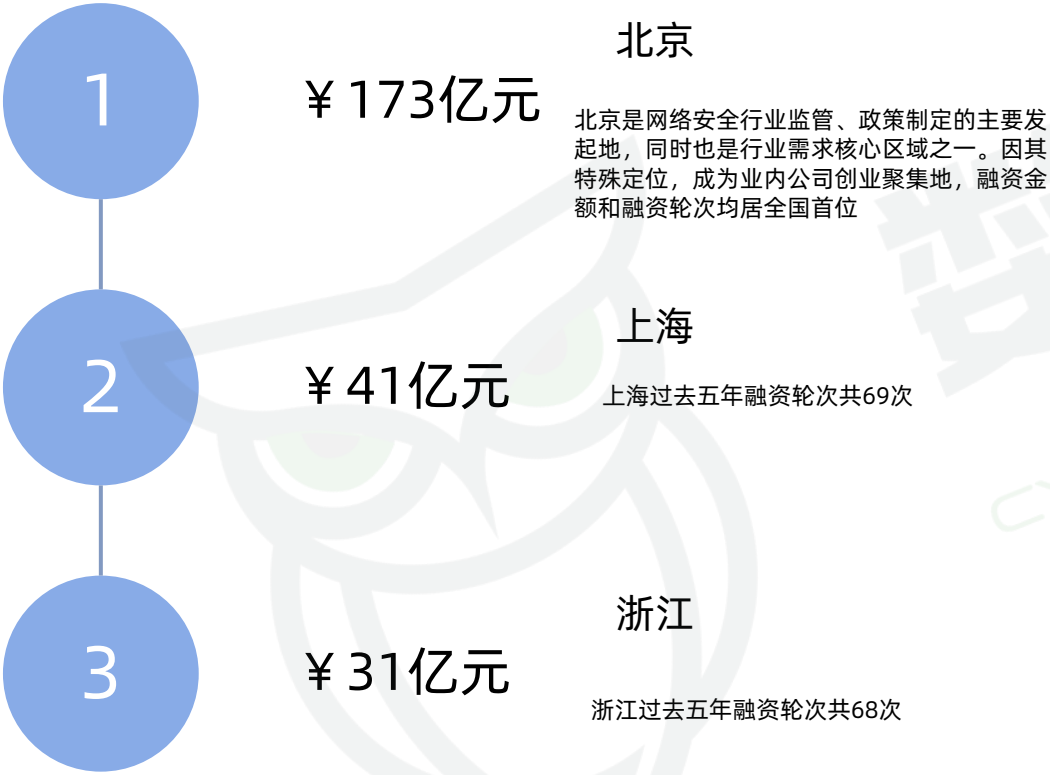
单笔大额重现

2026年Q1受长亭科技5亿元单笔交易拉动，金额短暂回升

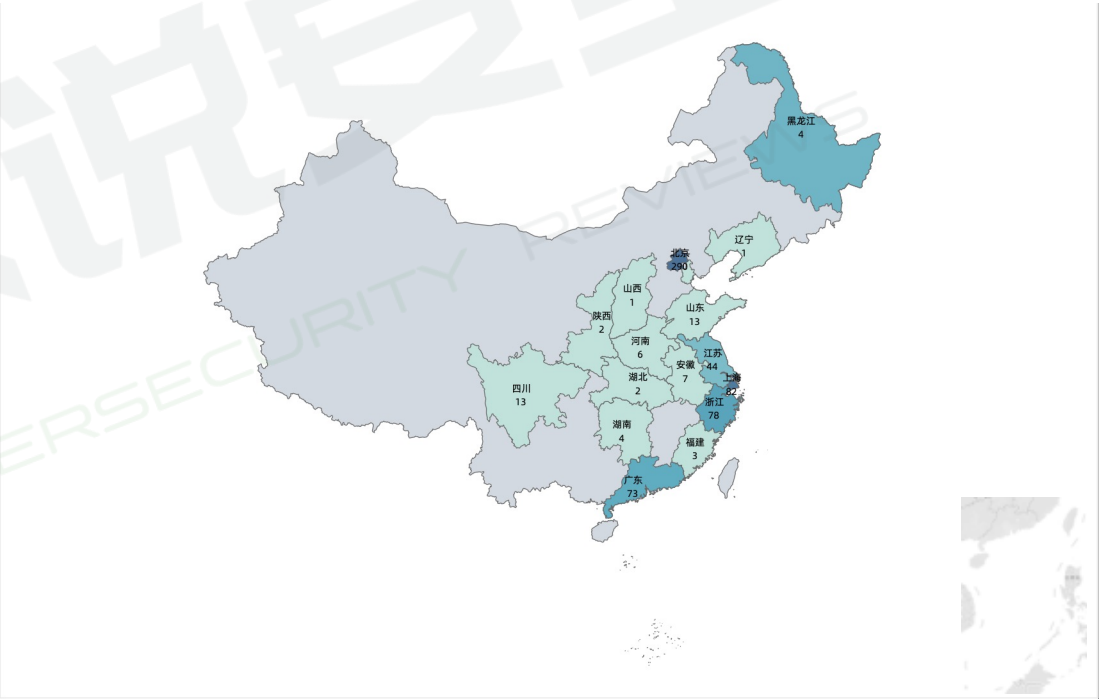
2023年-2026年Q2中国网络安全股权投资季度分布



过往五年（2021-2025）融资额TOP3省份



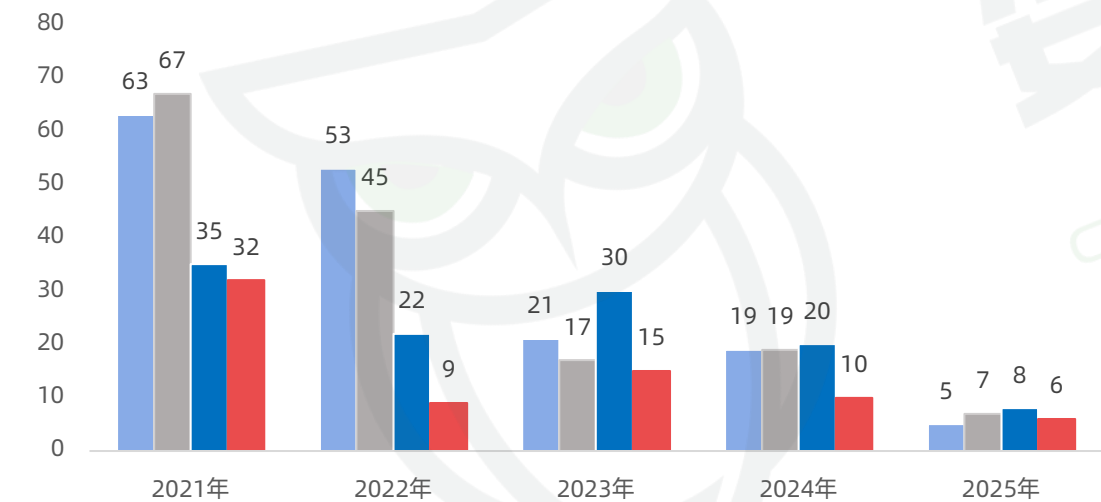
过往五年（2021-2025）省份融资分布



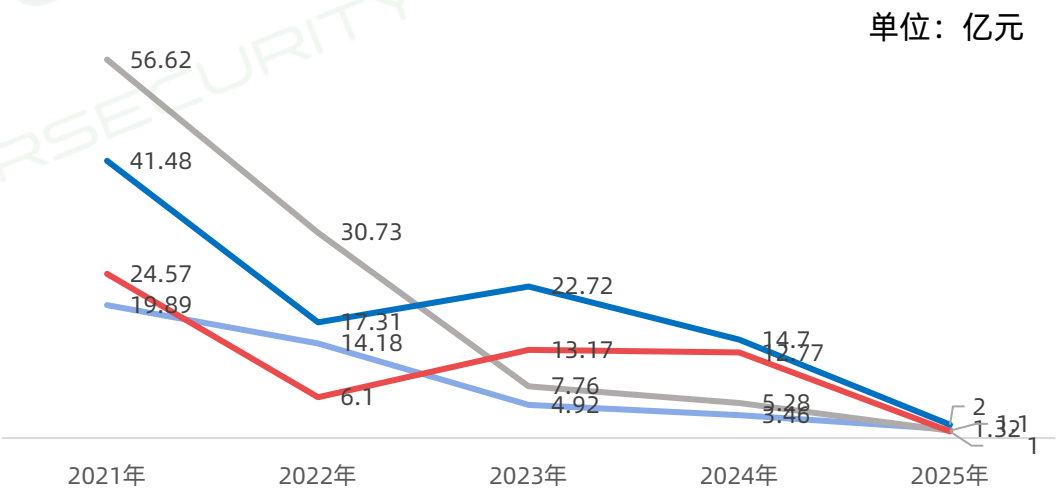
2025年各阶段融资全面收缩，扩张期项目数相对抗跌

- 2021年网络安全投融资的高点，本质上是政策红利、疫情催化、资本追逐三重因素叠加的结果。此后连续四年回落并非行业衰退，而是泡沫挤压后的价值回归。这种调整有助于淘汰概念型企业，让真正具备核心技术和商业模式的公司脱颖而出。
- 2025年各阶段同步收缩：融资次数由2024年的68次降至26次，金额由36.2亿元降至5.42亿元。其中扩张期以8次、2.0亿元位居各阶段之首，是相对抗跌的一档；成长期金额仅1.1亿元，回落最为明显。
- 在市场下行周期中，资源向头部企业集中的趋势更加明显。2026年上半年仅10笔交易却录得8.0亿元，已超过2025年全年，主要由长亭科技5亿元单笔融资拉动，说明资金正集中于少数确定性标的。
- 早期网络安全投资很大程度上依赖政策催化和合规需求，但当前的市场调整表明，单纯的政策驱动已不足以支撑高估值。未来的投资逻辑将更多转向真实的商业价值创造：包括AI安全、数据安全等新兴细分领域的技术创新。

2021-2025年融资次数分布



2021-2025年融资金额分布



初创期（成立时间0-3年）



成长期（成立时间3-6年）



扩张期（成立时间6-10年）



成熟期（成立时间10年以上）



不同发展阶段融资间隔存在差异

数据显示，各发展阶段的融资间隔存在差异，但并非逐级延长。2025年初创期约7个月、成长期22.8个月、扩张期29.0个月、成熟期22.0个月，扩张期最长。这里的间隔指前后两轮融资之间的时间，不等同于投资机构评估、尽调或谈判所用时间。



2025年成长与扩张期融资间隔拉长

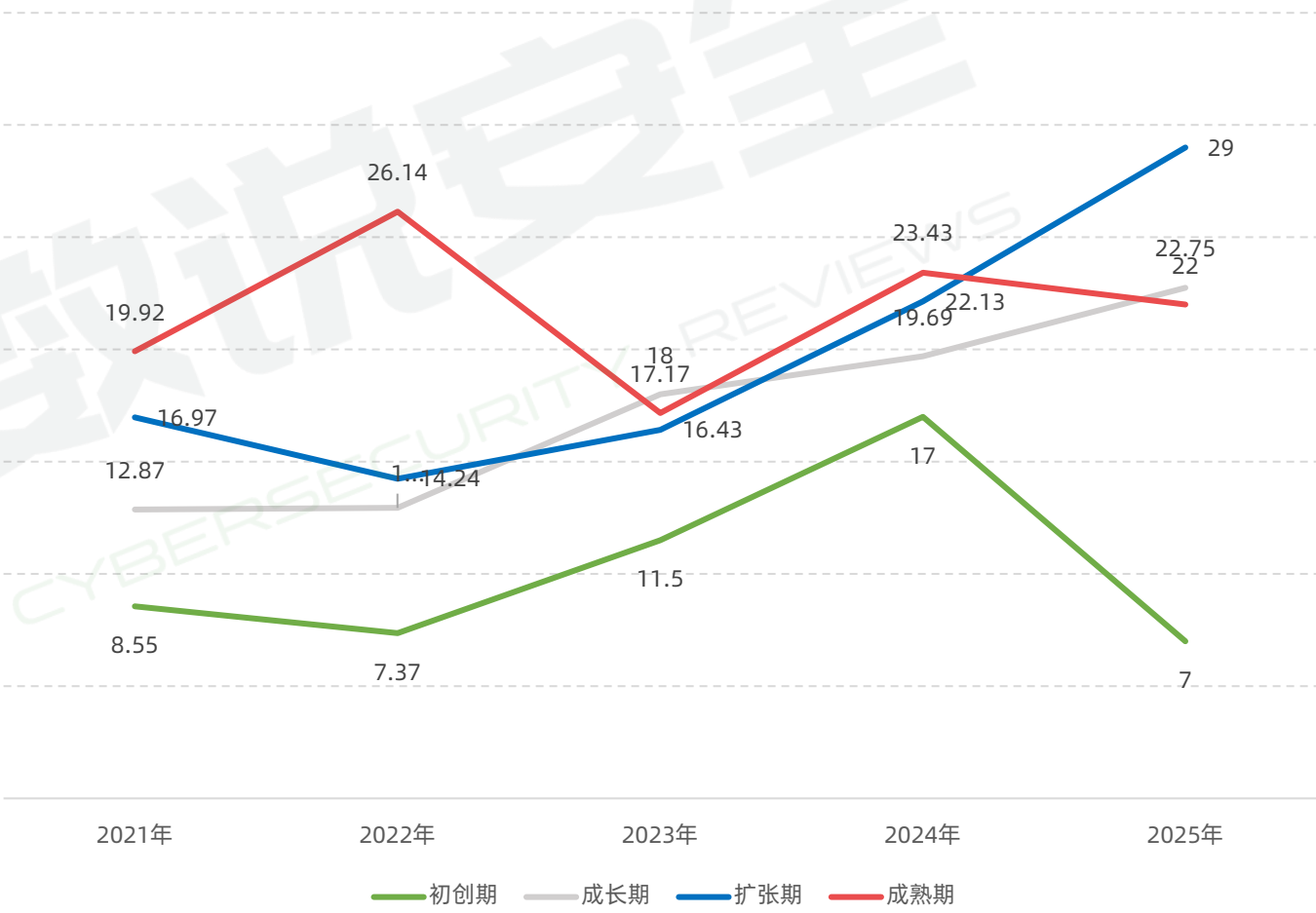
2024年各阶段融资间隔均较上年拉长。2025年成长期和扩张期进一步升至22.8个月、29.0个月，初创期和成熟期则回落至7.0个月、22.0个月。不同阶段走势分化，小样本下不宜概括为全面拉长。



样本大幅萎缩下的"幸存者效应"

2025年共26笔交易，按本报告交易名单去重涉及23家公司；融资间隔仅统计有可识别上一轮融资记录的交易，各阶段为2—4笔，周期指标的波动主要来自个案。公开交易由2021年197笔降至2025年26笔，但未融资不等于退出市场，已完成融资的企业也不能代表全部存续企业。

2021-2025年中国网络安全不同成长阶段融资周期（月）



序号	公司	成立日期	上市日期	成立到上市时间（年）
1	奇安信	2014/6/16	2020/7/22	6
2	亚信安全	2014/11/25	2022/2/9	7
3	电科网安	1998/4/23	2008/8/11	10
4	永信至诚	2010/9/2	2022/10/19	12
5	迪普科技	2008/5/28	2019/4/12	11
6	美亚柏科	1999/9/22	2011/3/16	12
7	任子行	2000/5/31	2012/4/25	12
8	安博通	2007/5/25	2019/9/6	12
9	山石网科	2007/2/16	2019/9/30	12
10	安恒信息	2007/5/15	2019/11/5	12
11	盛邦安全	2010/12/7	2023/7/26	13
12	启明星辰	1996/6/24	2010/6/23	14
13	绿盟科技	2000/4/25	2014/1/29	14
14	三未信安	2008/8/18	2022/12/2	14
15	中孚信息	2002/3/12	2017/5/26	15
16	北信源	1996/5/28	2012/9/12	16
17	飞天诚信	1998/6/16	2014/6/26	16
18	数字认证	2001/2/28	2016/12/23	16
19	深信服	2000/12/25	2018/5/16	17
20	格尔软件	1998/3/3	2017/4/21	19
21	信安世纪	2001/8/31	2021/4/21	20
22	吉大正元	1999/2/12	2020/12/24	21

从历史数据来看，我国网络安全上市公司从成立到上市经历的时间较长，最短为10年（排除情况特殊的亚信安全和奇安信），中位数约为14年，这其中的原因有：

- ◆ 网络安全是一个技术密集型行业，公司需要不断投入时间和资源进行研发，建立稳定的研发团队，实现技术的不断迭代，并形成稳定的产品线需要较长的时间来实现。
- ◆ 网络安全公司需要建立完善的销售网络，吸引客户并积累稳定的客户基础，同时不断拓展客户所处的行业和地域，获得市场的认可，这需要时间来建立信誉、培养合作伙伴关系并扩大市场份额。
- ◆ 网络安全公司的研发投入较大，一般需要进行3-4轮以上的融资，每轮融资的时间间隔在1-2年前后，不断筹集足够的资金才能支持其业务发展，并满足上市的要求。

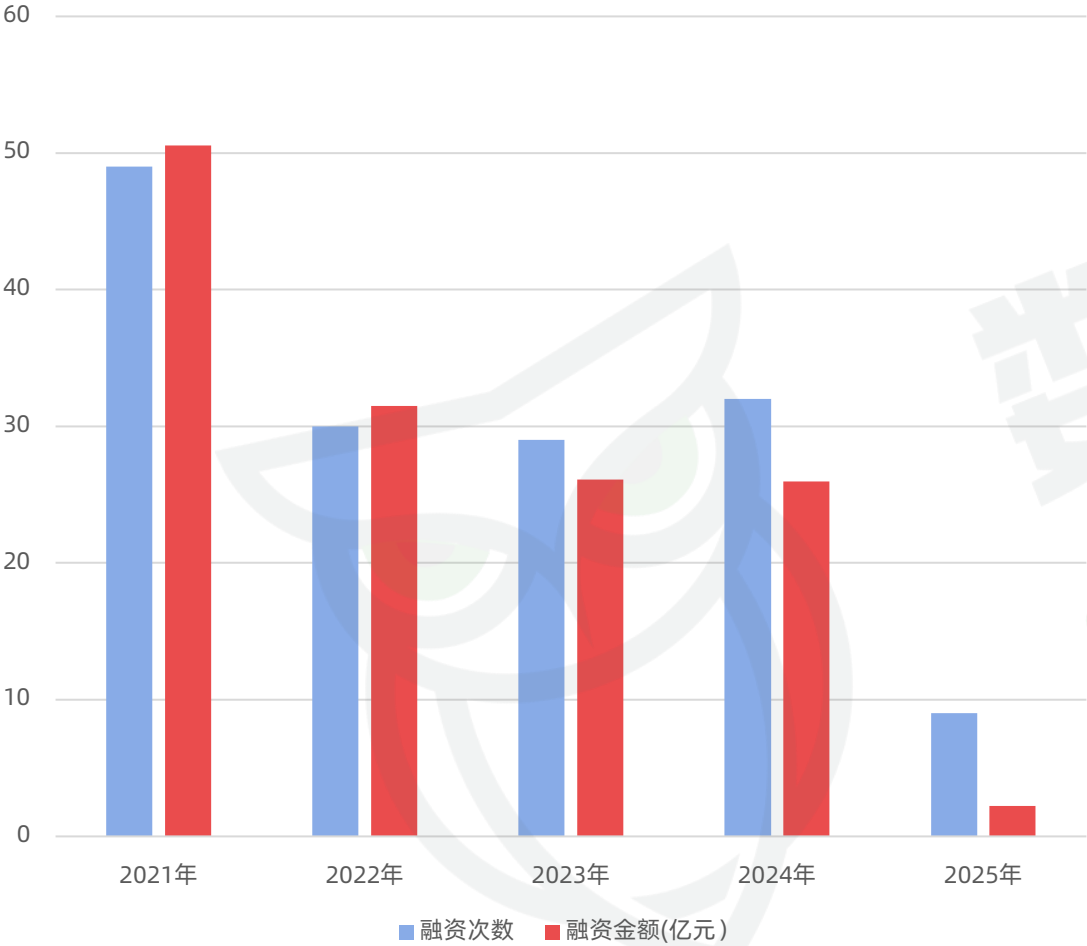
2025-2026年H1网络安全一级市场交易全名单



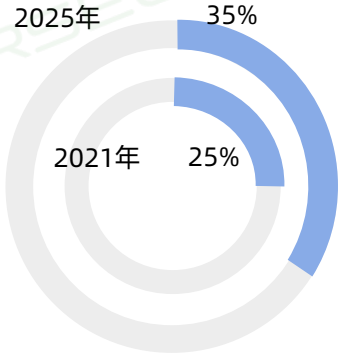
公司	时间	轮次	赛道	投资方
锐西科技	2026-05	A轮	物联网安全	智能物联、开源鸿蒙生态及数字安全领域资深产业人士
亿格云	2026-05	B轮	零信任	Monolith砺思资本、未来启创基金
锦数卫	2026-05	未披露	数据安全	成都高投、网安科技
安泉数智	2026-03	战略融资	AI安全	元起资本
炼石网络	2026-03	B轮	数据安全	元起资本
荆华密算	2026-03	天使轮	其他	盛景嘉成创投领投，国联股份、博彦科技和英诺科创基金跟投
戴猫科技	2026-03	战略融资	数据安全	长亭科技
星地探索	2026-02	天使轮	天空安全	涌铎投资
众智维科技	2026-02	B2轮	安全运营	南京扬子盛泓创业投资合伙企业（有限合伙）
长亭科技	2026-01	战略融资	AI安全	国家人工智能产业投资基金、国方创新、北京市人工智能产业投资基金
缔零科技	2025-12	天使轮	AI安全	中南创投、凯风创投、普朗克创投
安泉数智	2025-12	Pre-A轮	AI安全	英诺天使基金、杭州人才集团、杭州高新金投集团、杭实集团、杭州国有资本
汇和信安	2025-12	未披露	信息安全测评	未披露
安信与诚	2025-11	未披露	安全服务	哈创投
联盾网络	2025-11	天使轮	网安培训	复星资本
斗象科技	2025-09	未披露	资产与漏洞管理	钟鼎资本
云天安全	2025-08	A+轮	安全服务	西藏苍鹰、山东财金
无糖信息	2025-07	未披露	反欺诈	百融云创
缔零科技	2025-06	Pre-A轮	AI安全	光谷创业咖啡
华云安	2025-06	B+轮	安全运营	首发展集团
塞讯信息	2025-06	A轮	安全运营	横琴金投
亿格云	2025-06	Pre-B轮	安全SaaS服务	红杉中国，元璟资本，启创资本
一知安全	2025-06	Pre-A轮	零信任	未披露
无糖信息	2025-05	B+轮	其他	百融云创
天宽科技	2025-05	B轮	物联网安全	君澜资本
易安联	2025-05	C+轮	零信任	容亿创投、合肥包河创投
国脉信安	2025-04	A轮	商用密码	创赛创投
国腾量子	2025-04	A轮	量子网络安全	国腾量子
威努特	2025-03	战略融资	工控安全	上城资本集团
印信数安	2025-03	A轮	商用密码	四川产业振兴基金
众智维科技	2025-03	股权转让	安全运营	泓沅资本
中网云安	2025-01	A轮	边界安全	山东财金
墨菲安全	2025-01	Pre-A轮	供应链安全	恒生电子、复琢资本
铍泰克	2025-01	A轮	其他	广州盛东
安泉数智	2025-01	未披露	数据安全	赛伯乐投资、英诺天使基金
伊世智能	2025-01	A轮	车联网安全	鲁信创投

投资机构分析

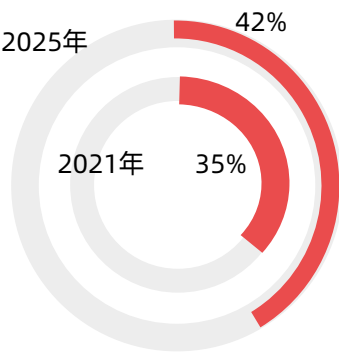
2021-2025年央国企参与投资机构投资网络安全情况



- 整体来看，央国企在网络安全领域的出手与市场同步收缩。2025年投资9次、参与项目金额合计2.25亿元，较2024年的32次、25.97亿元大幅回落。
- 但从占比看，央国企的相对影响力不降反升，2025年投资次数占全市场35%、金额占42%，高于2021年的25%和35%。



央国企投资机构投资网安项目数量占比



央国企投资机构投资网安项目金额占比

1 偏好成熟阶段

资金主要流向扩张期与成熟期企业。这类企业已完成技术验证与市场初步拓展，商业模式相对清晰，与央国资的资金性质和投资责任相匹配。

2 聚焦关键基础设施

工控安全、密码应用与管理是持续的重点投资方向，体现对国家安全战略的深度契合，也是央国资与产业协同最紧密的两条赛道。

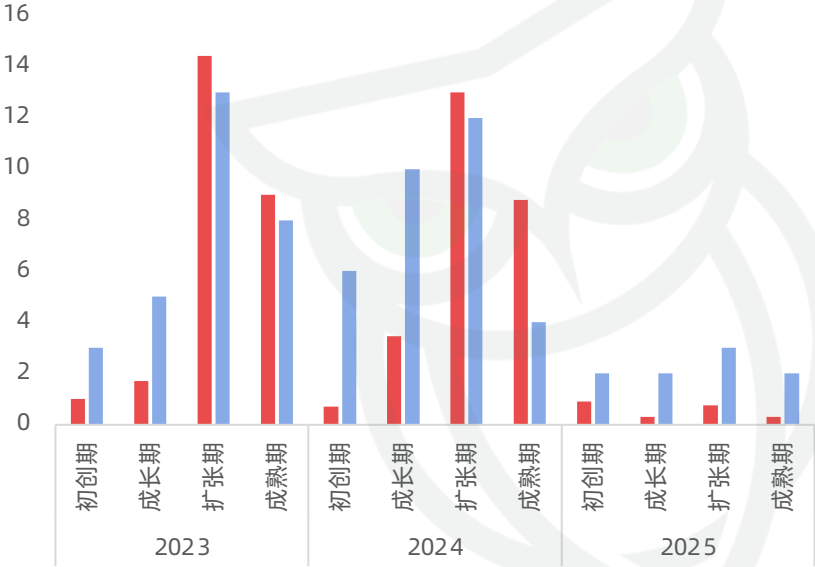
3 跟随技术趋势

2024-2025年开始在AI安全、商用密码等新兴方向布局，但单笔规模普遍在千万级，仍处于试探性配置阶段。

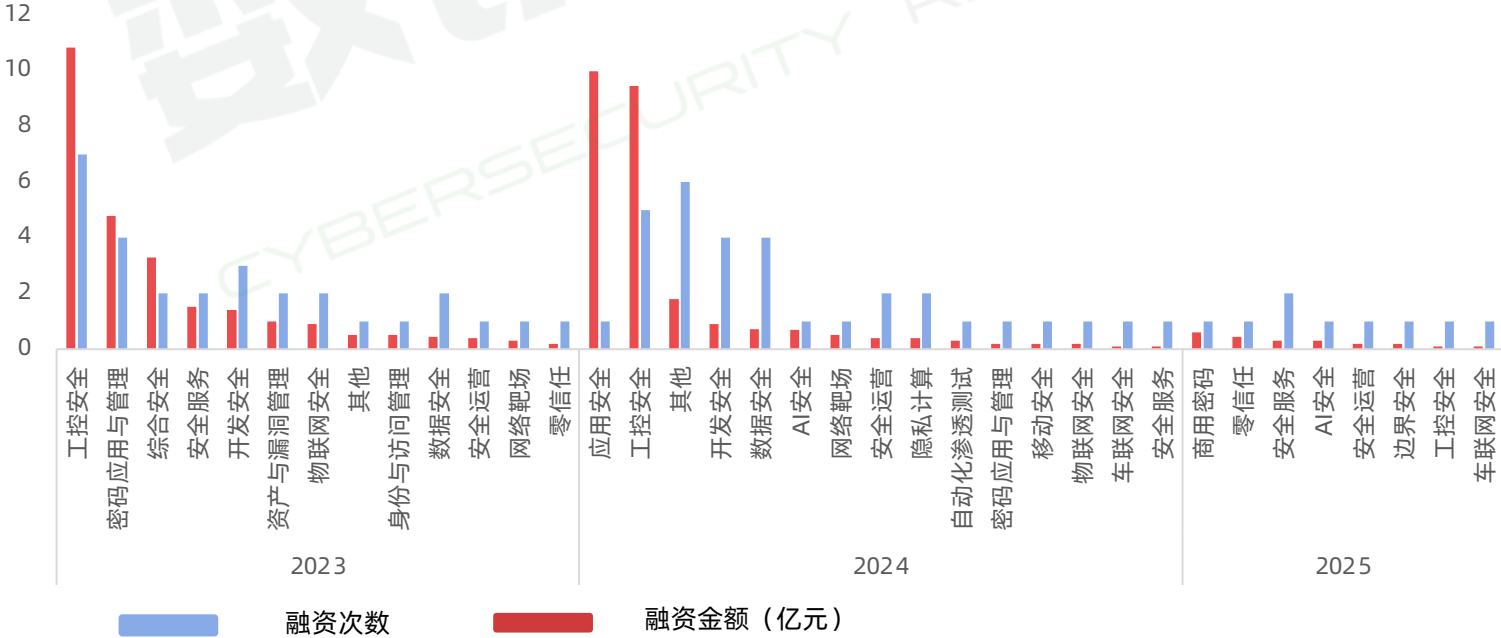
4 节奏大幅放缓

2025年仅出手9次、参与项目金额合计2.25亿元，较2023-2024年年均约30次明显收缩，与一级市场整体同步进入观望状态。

2023-2025年央国资机构不同投资阶段投资分析



2023-2025年央国资机构不同投资赛道投资分析

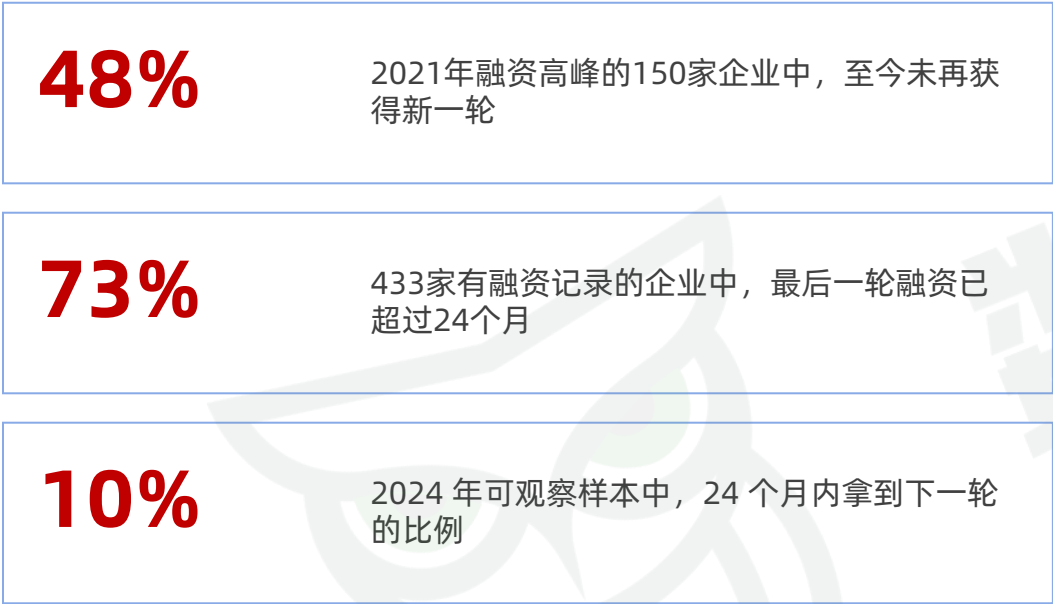


各类投资机构五年累计出手情况与近一年变化

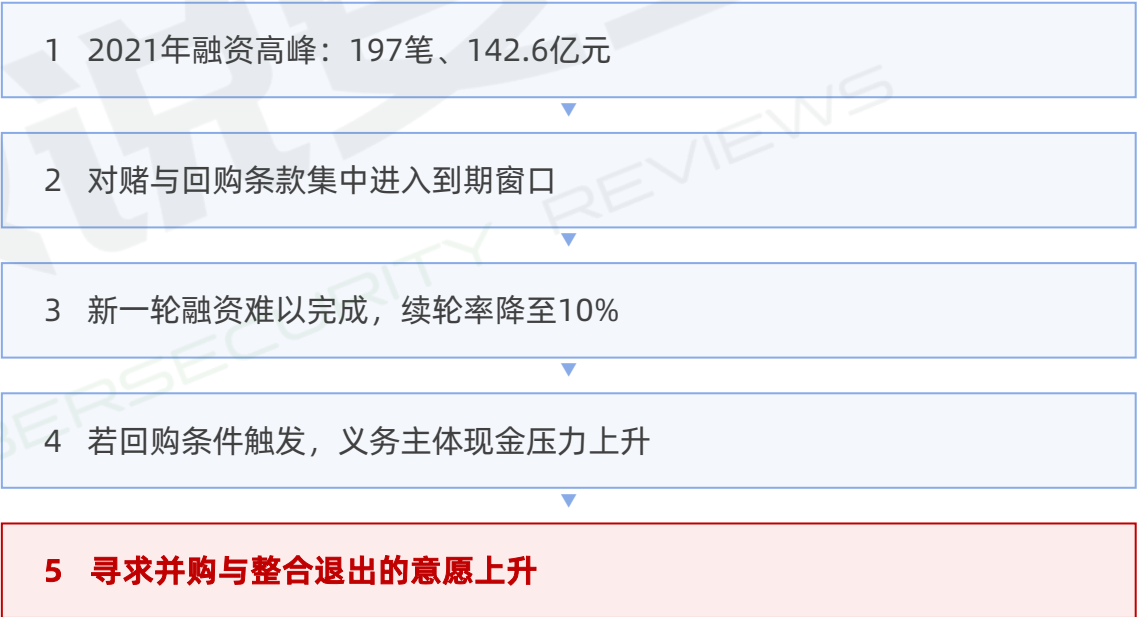
机构类别	投资机构	五年累计投资项目数	2025.7-2026.6 新增投资
国资背景基金	中电科	22	—
	国投	14	—
	深创投	19	—
	中网投	13	—
	中电子	11	—
普通风投基金	红杉	17	—
	IDG	13	—
	宽带	13	—
	金沙江创投	10	—
	方广	10	—
网安及互联网上市公司	腾讯	12	—
	阿里	6	—
	启明星辰	22	—
	奇安信（含并购）	43	—
	360	13	—
	绿盟科技	14	—
	安恒信息	15	—
	天融信	12	—
	苹果资本	16	—
	奇安创投	28	—
网安专项基金	琥珀安云	10	—
	元起资本	12	安泉数智、炼石网络
	璟泰创投	8	—
	北京星源壹号	7	—

近年典型并购/融资项目

一级市场融资连续四年收缩后，2021年融资高峰形成的存量项目正集中进入退出期。融资端断档与估值回落同时出现，承担回购义务的主体可能面临更大现金压力，部分企业寻求并购与整合退出的意愿可能上升，但实际成交仍受约束。



传导链条



交易得以发生的三重外部条件

估值差收窄

A股网安板块PS-TTM中位数由2025年底约7.8倍回落至2026年6月底约6.35倍，交易定价仍需结合标的盈利与现金流。

重组新规松绑

2025年5月证监会修订《上市公司重大资产重组管理办法》，新设简易审核程序，科创板已现首例。

退出渠道拓宽

网信办行动计划鼓励并购基金与S基金，明确拓宽IPO以外的退出渠道。

注：回购条款本身不在统计口径内，上述为基于融资断档率与单笔规模回落的推断；数据来源为公开融资信息整理。

2025年以来，全球网络安全并购由平台化整合、AI重塑产品形态与云厂商入场三条主线驱动，大额交易密集出现。本报告收录的国内案例主要集中在2023—2024年；估值变化、重组制度调整与退出需求可能为后续整合提供条件。

2025-2026年全球代表性并购交易

收购方	标的	交易金额	时间
谷歌	Wiz	320亿美元	2025-03宣布
Palo Alto Networks	CyberArk	约250亿美元	2026-02完成
三菱电机	Nozomi Networks	约10亿美元	2025-09宣布 2026-01完成
CrowdStrike	Seraphic Security	未披露	2026-01
Zscaler	SquareX	未披露	2026-02
Databricks	Panther Labs	未披露	2026-06

对照结论

全球头部厂商正用大额并购完成平台化整合，三菱电机收购Nozomi Networks更是工控安全领域史上大额交易之一，与本报告工控安全五年融资额居首的现象共同显示该领域受到资本关注。国内受估值倒挂与退出渠道限制，本报告收录的近期并购案例较少；随着估值差收窄与重组新规落地，2026年起国内更可能出现以能力互补为目标的中小额并购，而非大额平台型交易。

四点观察

- 1 全球在加速

SecurityWeek统计，仅2026年6月单月全球就宣布37笔网安并购交易。
- 2 国内样本有限

本报告收录的国内并购案例中，六个发生在2023-2024年，微步在线收购CyberStrikeAI为 2026 年新增案例
- 3 整合条件变化

2026年6月底A股网安板块PS-TTM中位数约6.35倍；重大资产重组新规新设简易审核程序；网信办明确拓宽IPO以外退出渠道。
- 4 上轮的教训

部分历史网安并购曾出现业绩承诺未达标、团队流失等整合问题，本轮买方对标的质量与整合能力的要求更高。

注：国际交易信息来自公司公告与公开报道；国内并购案例以本报告收录为准，不排除存在未公开披露的交易。

交易概述



收购

CyberStrikeAI

微步在线收购开源 AI 渗透测试平台 CyberStrikeAI。CyberStrikeAI 以 Go 语言构建，是 2026 年安全社区关注度较高的 AI 原生安全测试项目之一，以大语言模型为决策引擎、安全工具为执行单元，通过自然语言调度完成从需求描述到漏洞发现的自动化流程。

微步在线成立于 2015 年，以实战导向的 Agentic AI 与威胁情报 TI 为技术内核，提供覆盖云、网、边、端的安全体系，在本报告「Agentic SOC 安全运营自主闭环」方向中列为代表厂商。

本次收购把自主攻防验证能力并入其安全运营体系，与既有的威胁情报和智慧安全运营平台形成「以攻促防」的闭环，补齐 AI 自主安全研究与攻防验证环节。

CyberStrikeAI 核心能力简介	
自然语言调度	以大语言模型为决策引擎，通过自然语言对话调度 100 余款安全工具，完成从需求描述到漏洞发现的自动化流程，降低工具链的使用门槛。
攻击链还原	自动生成攻击链图谱，记录每一步操作及其依据，支持逐步追溯与复盘，便于在授权范围内核验测试过程。
角色化测试	内置 12 种预定义安全测试角色，覆盖渗透测试、CTF、Web 扫描与 API 安全等场景，各角色配有专属提示词与工具权限限制。

交易概述



收购



亚信科技控股有限公司始于1993年，2018年12月19日成功在香港联交所主板上市，是领先的信息技术产品及服务提供商，领先的数智化全栈能力提供商。

亚信安全于2015年收购了全球云与终端安全的领导厂商趋势科技中国业务，正式启航。为护航数智化的未来，2024年底亚信安全完成对亚信科技（股票代码01675.HK）的并购。此次亚信安全以“蛇吞象”方式完成对亚信科技的控股收购，旨在通过整合双方资源，构建“安全+数智”的云网安一体化生态体系，并强化自身“懂网、懂云、懂安全”的技术优势。

2024年11月，亚信安全计划通过设立境内外投资架构，以现金方式收购亚信科技约19-20%股份，同时通过表决权委托获得田溯宁等控制的约9.6%股份的表决权，从而获得对亚信科技的控制权。

亚信科技财务概况（单位：亿元）

	营业收入	净利润	毛利	资产总额	负债总额
2023年	78.91	5.33	29.75	112.85	46.84
2024年	66.46	5.45	24.84	105.00	38.59

交易概述



收购

北京天御云安科技有限公司成立于2018年，是一家专业的密码产品研制厂商。主要从事密码安全技术研究与产品开发、密码工程实现和方案咨询等业务。

盛邦安全成立于2010年，专注于网络安全领域，聚焦漏洞及脆弱性检测、应用安全防护、溯源管理及网络空间地图等技术领域，为客户提供网络安全基础类、业务场景安全类、网络空间地图类安全产品及服务。为了进一步打下可持续发展的基础，公司将加大对网络空间地图体系、卫星互联网安全、工业互联网安全、公共安全等现有产品线或研发项目的投入或研发力度，持续对公司产品与技术进行升级。通过对天御云安的并购，标志着盛邦的业务拓展又迈出了一大步。通过整合天御云安，盛邦正式进军卫星互联网安全领域。

2024年6月27日，公司董事会通过了收购并增资北京天御云安科技有限公司部分股份的议案，公司使用自有资金人民币3000万元收购并增资认购天御云安部分股权，本次交易完成后，公司将持有天御云安 62.5%的股权，天御云安将成为公司的控股子公司。

天御云安财务概况（单位：万元）

	营业收入	净利润	扣非净利润	资产总额	负债总额	资产净额
2023年	1458.4	212.6	252.2	1524.9	1287.4	237.5
2022年	847.8	-169.6	-420.4	752.0	927.1	-175.1

交易概述



收购



普世科技经过十多年积累的科研成果，在高效可靠的跨网数据传输技术、磁光混合数据安全归档存储与检索技术、数据安全防护技术等方面具有先发优势，普世科技一直致力于解决政府、军队和企业面临的信息安全和数据应用问题，构建了自主可控的安全体系，产品在政府、军队、军工、金融、通信、医疗等领域得到广泛应用。

信安世纪以密码技术为基础支撑，致力于解决网络环境中的身份安全、通信安全和数据安全等信息安全问题。在产品方面，双方公司的产品和解决方案均涵盖信息安全领域，彼此之间具有显著的互补性。市场层面上，信安世纪的产品和解决方案持续服务于金融、政府和企业等关键领域。而普世公司则专注于军队和军工市场，两家公司在市场定位上形成了有力的互补。这种互补性有助于更全面地满足不同行业对信息安全的需求。

信安世纪发行股份及支付现金购买北京普世时代科技有限公司 80%的股权，转让对价2.44亿元，其中发行股份方式支付2.39亿元，以现金支付0.05亿元。普世科技自 2023 年 6 月起并表至公司。2023年普世科技实现归属于母公司股东扣除非经常性损益前后孰低净利润为人民币 3,488.42 万元， 已达成当年业绩承诺数 2,950.00 万元。

普世科技财务概况 （单位：万元）

	营业收入	毛利率	净利润	净利润率	销售商品、提供劳务收到的现金	经营活动产生的现金流量净额	应收账款
2022年1-10月	6,819.51	62.17%	2,165.78	31.76%	5,844.61	1,098.63	3112.01
2021年	7,351.51	61.85%	1,966.41	26.75%	7,858.44	1,096.48	2664.46

交易概述



收购



江南科友成立于 1991 年，1998 年全面进入商用密码领域。具有完整的商用密码产品体系、完备的销售体系和覆盖全国的技术服务体系，产品包括主机安全设备、终端安全模块、密码服务基础设施、密钥管理系统、主机运维审计系统、数据库运维审计系统等。江南科友在金融等重要行业的密码应用占据优势地位，在业内享有良好声誉。

近年来，三未信安公司努力拓展商用密码产品应用场景，江南科友公司的业务、产品及下游行业与公司发展战略高度契合，并购交易有利于发挥业务协同效应，三未信安可利用自身多年来深耕商用密码行业的技术优势，共享江南科友公司的市场渠道及客户资源，形成良好的产业协同效用，实现优势互补，以提升公司整体价值。

三未信安科技股份有限公司于 2023 年 6 月 19 日召开第一届董事会第十九次会议，审议通过了《关于拟收购江南科友科技股份有限公司部分股份的议案》，拟使用自有资金人民币 15,117.2479 万元收购广州江南科友科技股份有限公司66.9349%的股份，共计 20,749,820 股。2023 年 6 月 29 日三未信安完成和江南科友的股份交割，占江南科友总股本的 66.9349%，并完成江南科友的董事会改组，取得董事会控制权，江南科友成为公司的控股子公司，纳入合并报表范围。

江南科友财务概况（金额单位：元）

	营业收入	营业成本	毛利率	净利润	净利润率	销售商品、提供劳务收到的现金	经营活动产生的现金流量净额	应收账款
2022年	117,553,998.0	21,892,986.7	81.4%	22,329,072.7	19.0%	133,237,650.1	30,119,784.7	17,010,598.4
2021年	122,974,245.2	21,704,739.6	82.4%	17,899,430.7	14.6%	138,144,061.8	31,352,474.6	20,205,168.1

交易概述



收购



领信数科认为国内信息安全产业正在经历变革期，安全产品和解决方案需要深入具体应用和场景，数字化进程的深入使用户更加关注真实需求，强调数字安全与应用、业务深度结合的市场；为了满足客户的数字化场景新需求，公司对大白互联的收购，将原有的零信任、数据安全、视频安全、大数据分析、隐私计算等方面的能力，与大白互联在数字身份认证方面多年的市场经验相结合，拓展数字安全与数字身份认证在具体业务场景中的应用。

大白互联简介		大白互联主营业务	
公司成立于2015年，是专注于数字身份应用服务的国家高新技术企业，自2016年起，大白互联先后参与“互联网+”可信身份认证体系建设、居民身份网络认证标准制定、数字身份应用推广等工作，持续为国内网络身份管理体系建设贡献力量。此外，依托卓越的技术实力与深厚的行业资源，大白互联围绕线上与线下的身份安全业务场景，持续打造数字身份应用与可信认证服务系列产品，助力客户率先实现业务数字化转型。未来，大白互联将继续深耕数字身份应用领域，以务实、诚信、进取、同心的态度，让数字身份安全惠及你我，为构建安全可信社会作出贡献。	访客云	大白互联访客云是以国家“互联网+”可信身份认证平台技术为基础打造的“1+1+N”式智慧访客管理系统解决方案，通过微信小程序（“1”）、PC端管理后台（“1”）及多种可选配智能核验设备（“N”），集成访客自主预约、快速在线审核、同步身份核验等功能，轻松实现场所出入口的统一智能管控。	
	身份云	基于国家“互联网+”可信身份认证平台，大白互联身份云对传统的匿名化、私有化单点登录与权限管理系统进行实名化、云化升级，以依托数字身份形成的新一代4A（认证Authentication、授权Authorization、账号Account、审计Audit）能力，提供覆盖多行业、全场景的标准化网络身份安全认证服务，让您的统一身份权限管理更安全、更高效、更经济。	
	物联云	大白物联云服务结合国家“互联网+”可信身份认证平台技术，将法定数字身份作为仪器、车辆、电器等各类终端设备的安全信任根，通过数字身份对物联权益进行管理，实现人与物的深度绑定，真正做到线上线下一体化的“万物互联”。	

交易概述



收购



在云计算技术快速发展，网络安全监管趋严，数据安全风险增加等综合因素影响下，各家云厂商纷纷通过自建安全团队或收购/入股专业安全公司来补充自身安全产品和能力，力争为客户提供更有力的安全保障。浪潮云致力于成为高品质云服务提供商，希望为客户提供云网边端融合、云数智融合的全栈云服务，构建零信任的云数安全体系。思福迪创立于2005年，是国内早期投入运维安全审计与防护的专业厂商，在日志审计和运维安全管理相关技术领域有深厚技术积累。浪潮云收购思福迪，既可实现安全能力的补充，同时拓展安全业务能力。

思福迪核心产品简介

堡垒机	规范操作人员行为：形成规范的运维授权管理流程，通过对运维操作内容的记录，提供指令级别控制能力，通过技术手段有效规范运维人员的操作行为，降低内部安全风险； 满足各项合规需求：自动分析运维人员操作过程，评估访问风险、并提供完整的合规审计报告，降低IT内控审计工作量； 提升企业管理效率：简化运维人员操作过程，降低账号、密码管理难度，有效提升企业IT管理效益。
日志审计	海量日志集中审计：集中采集、存储海量日志信息，保障审计数据安全，提供可视化的安全审计工具，实现日志信息集中采集、集中审计；支持不同网络环境下的实名审计； 实时分析及及时警告：对各设备、操作系统、应用的日志进行实时监测，及时发现设备运行异常情况，并第一时间通知管理员，为排查故障争取时间； 动态跟踪事件定位：通过独有的海量日志快速分析与检索系统，协助管理员快速发现、关注与定位事件。
数据库审计	详细访问审计分析：详尽记录数据库访问的登录、操作、退出过程，提供便利的审计视图和审计工具，关键信息一目了然； 规范访问权限行为：提供多角度、全方位报警策略制定与响应机制，从管理与技术上同时规范管理员行为，有效降低内部安全风险； 保护核心数据安全：提供访问、操作多层次安全控制手段，从应用层有效保障重要数据库的安全。



以数据为基础的网络安全产业研究平台

ssaq@geniuscybertech.com

2026

北京赛博英杰科技有限公司