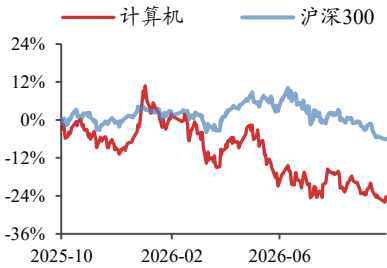


计算机

2026 年 10 月 11 日

投资评级：看好（维持）

行业走势图



数据来源：聚源

相关研究报告

《高密度算力驱动散热升级，Agent 应用持续拓展—行业周报》-2026.10.11
 《大模型系列深度（一）：国产大模型竞争重心转向效率与生态，智谱以 GLM 全栈体系卡位第一梯队—行业深度报告》-2026.10.1
 《国产算力供需持续趋紧，智能体放大 CPU 增量缺口—行业点评报告》-2026.9.23

AI 带来网络安全新变革

——行业点评报告

张越（分析师）

zhangyue1@kysec.cn

证书编号：S0790524090003

刘逍遙（分析师）

liuxiaoyao@kysec.cn

证书编号：S0790520090001

● AI 时代，网络安全进入“AI 对抗 AI”的阶段

随着人工智能技术的广泛应用，网络攻击领域迎来关键性迭代，攻击者已开始用 AI 完成目标筛选、信息整合、路径规划、实施攻击与策略调整，运用 AIAgent 发起自动化攻击，使得攻击效率与隐蔽性均实现指数级提升。网络安全攻防博弈的规则已从过去人与人的较量，进化到了“AI 对抗 AI”的阶段。同时，随着大模型与智能体等 AI 应用在政务、金融、工业、医疗及企业内部管理等场景加速落地，AI 带来安全风险随之向业务核心环节渗透，也衍生出了提示词注入、模型投毒、多智能体协同欺骗等全新系统性风险。

● Anthropic、OpenAI 推出 AI 安全防御模型，高度重视 AI 安全

（1）根据 Anthropic 披露，一个被追踪为 GTG-1002 的黑客组织，利用 Claude Code 工具对全球目标发起了高度自动化的渗透行动。攻击者没有使用任何自研恶意软件，而是组合公开的渗透测试工具，通过 Claude Code 加 MCP（Model Context Protocol）搭建了一套多代理攻击架构。他们让 Claude 相信自己是一家合法网络安全公司的员工，正在做授权的安全测试。此后，Anthropic 推出了 Claude Mythos 项目——一个专门用于安全防御的 AI 系统。它在 2026 年 4 月的测试中发现了数千个零日漏洞，覆盖所有主流操作系统和浏览器。此外，OpenAI 推出了 GPT-5.4-Cyber，作为 GPT-5.4 的专门优化版本，针对网络安全防御场景进行了特别优化。（2）8 月 27 日，OpenAI 发布了一封题为“集体行动呼吁网络防御”的公开信，获得至少 116 家企业和组织的联署，其中包括 Anthropic、Google、Microsoft、AMD、CrowdStrike、Palo Alto Networks、Okta、Fortinet、花旗银行、Capital One、Visa、万事达卡等横跨 AI、网络安全、金融和基础设施领域的重量级机构，公开信的核心警告是：AI 驱动的网络攻击将在未来数月内变得“更加广泛和复杂”。

● 随着 AI 渗透率提升，全球 AI 安全市场将实现高速增长

Gartner 预计，2027 年全球 AI 安全市场规模将较 2026 年增长 69%，达到 47.83 亿美元，并在 2028 年进一步升至约 77 亿美元。AI 安全市场高速增长主要源于企业急需保护人工智能系统、解决新兴漏洞并加强对复杂网络威胁的防御能力。2027 年，人工智能应用安全仍将是最大的支出类别，预计将达到近 8.51 亿美元，其次是 AI 使用控制，支出预计将达到 7.49 亿美元。

● 投资建议

AI 时代，网络安全进入“AI 对抗 AI”的阶段，行业也迎来新发展机遇。受益标的：深信服、绿盟科技、安恒信息、天融信、奇安信、永信至诚、盛邦安全、启明星辰、山石网科、安博通、麒麟信安等。

● 风险提示：技术进展不及预期，市场竞争加剧风险。

特别声明

《证券期货投资者适当性管理办法》、《证券经营机构投资者适当性管理实施指引（试行）》已于2017年7月1日起正式实施。根据上述规定，开源证券评定此研报的风险等级为R4（中高风险），因此通过公共平台推送的研报其适用的投资者类别仅限定为专业投资者及风险承受能力为C4、C5的普通投资者。若您并非专业投资者及风险承受能力为C4、C5的普通投资者，请取消阅读，请勿收藏、接收或使用本研报中的任何信息。因此受限于访问权限的设置，若给您造成不便，烦请见谅！感谢您给予的理解与配合。

分析师承诺

本研究报告的署名人员具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，以勤勉的职业态度，独立、客观地出具本报告，并对内容和观点负责。本报告清晰准确地反映了署名人员的研究观点，所包含的分析基于各种假设，不同假设可能导致分析结果出现重大不同。本报告采用的各种估值方法及模型均有其局限性，估值结果不保证所涉及证券能够在该价格交易。本报告署名人员保证他们报酬的任何一部分不曾与，不与，也将不会与本报告中具体的推荐意见或观点有直接或间接的联系。

股票投资评级说明

	评级	说明
证券评级	买入（Buy）	预计相对强于市场表现 20%以上；
	增持（outperform）	预计相对强于市场表现 5% ~ 20%；
	中性（Neutral）	预计相对市场表现在 - 5% ~ + 5%之间波动；
	减持（underperform）	预计相对弱于市场表现 5%以下。
行业评级	看好（overweight）	预计行业超越整体市场表现；
	中性（Neutral）	预计行业与整体市场表现基本持平；
	看淡（underperform）	预计行业弱于整体市场表现。

备注：评级标准为以报告日后的 6~12 个月内，证券相对于市场基准指数的涨跌幅表现，其中 A 股基准指数为沪深 300 指数、港股基准指数为恒生指数、新三板基准指数为三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）、美股基准指数为标普 500 或纳斯达克综合指数。我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重建议；投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者应阅读整篇报告，以获取比较完整的观点与信息，不应仅仅依靠投资评级来推断结论。

分析、估值方法的局限性说明

本报告所包含的分析基于各种假设，不同假设可能导致分析结果出现重大不同。本报告采用的各种估值方法及模型均有其局限性，估值结果不保证所涉及证券能够在该价格交易。

法律声明

开源证券股份有限公司是经中国证监会批准设立的证券经营机构，已具备证券投资咨询业务资格。

本报告仅供开源证券股份有限公司（以下简称“本公司”）的客户使用。本公司不会因接收人收到本报告而视其为客户。本报告是发送给开源证券客户的，属于商业秘密材料，只有开源证券客户才能参考或使用。

本报告是基于本公司认为可靠的已公开信息，但本公司不保证该等信息的准确性或完整性。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他金融工具的邀请或向人做出邀请。本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可能会波动，过往的业绩表现不应作为其日后表现的预示。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。客户应当考虑到本公司可能存在可能影响本报告客观性的利益冲突，不应视本报告为做出投资决策的唯一因素。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。本公司未确保本报告充分考虑到个别客户特殊的投资目标、财务状况或需要。本公司建议客户应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。若本报告的接收人非本公司的客户，应在基于本报告做出任何投资决定或就本报告要求任何解释前咨询独立投资顾问。投资者应自主作出投资决策并自行承担投资风险，任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。

开源证券在法律允许的情况下可参与、投资或持有本报告涉及的证券或进行证券交易，或向本报告涉及的公司提供或争取提供包括投资银行业务在内的服务或业务支持。开源证券可能与本报告涉及的公司之间存在业务关系，并无需事先或在获得业务关系后通知客户。

本报告的版权归本公司所有。本公司对本报告保留一切权利。未经本公司事先书面授权，本报告的任何部分均不得以任何方式制作任何形式的拷贝、复印件或复制品，或再次分发给任何其他人，或以任何侵犯本公司版权的其他方式使用。所有本报告中使用的商标、服务标记及标记均为本公司的商标、服务标记及标记。

开源证券研究所

上海

地址：上海市浦东新区世纪大道1788号陆家嘴金控广场1号楼3层
邮编：200120
邮箱：research@kysec.cn

北京

地址：北京市西城区西直门外大街18号金贸大厦C2座9层
邮编：100044
邮箱：research@kysec.cn

深圳

地址：深圳市福田区金田路2030号卓越世纪中心1号楼45层
邮编：518000
邮箱：research@kysec.cn

西安

地址：西安市高新区锦业路1号都市之门B座5层
邮编：710065
邮箱：research@kysec.cn