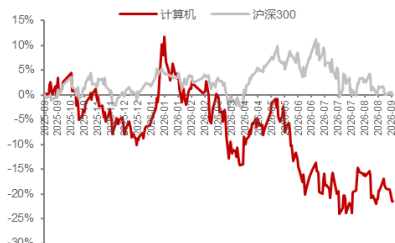


计算机行业点评

2026 年 9 月 11 日

行业指数相对沪深 300 表现



相关报告

《GPT-6 Astra 发布: Agent 能力迎来跃迁, AI 应用落地有望加速》

2026-09-04

《工信部部署 AI 应用服务商培育专项行动, 把握两条核心受益主线》

2026-09-01

《FDE 加速 AI 应用范式迁移: 从模型供给走向业务价值交付》

2026-08-17

《Meta 模型芯片双轮驱动, AI 算力资本开支周期持续》

2026-07-13

《模型跨越生产质变点, 字节加速构建全栈 AI 云》

2026-06-24

分析师: 王鑫旻

执业证书编号: S0370526030001

邮箱: wangxy4@jyzq.cn

行业点评报告

—Meta 发布个人 AI 智能体 Muse, Agent 安全有望成为网络安全新需求

评级: 强于大市 (维持)

事件: 美国当地时间 9 月 8 日, Meta 正式发布个人 AI 智能体 Muse。不同于传统对话式 AI, 该助手可自主拆解任务、打开网页、填写表单, 并调用外部应用完成工作。

● **Muse 跳出参数竞赛, 运行模式、使用门槛与生态体系产生差异化** 全球科技巨头正加速布局 AI 智能体, OpenAI、Anthropic 产品多聚焦专业与企业场景, Meta Muse 主打消费级个人智能体市场, 界面贴近通用聊天工具, 覆盖购物、邮件等任务。Muse 与同类产品的差异并非模型参数或跑分, 而在于运行模式、使用门槛与生态体系: **运行模式上**, Muse 定位为长期运行的个人 Agent, 独立云端虚拟机使其退出应用后仍可持续工作; 使用门槛上, OpenAI 及相关产品的快速普及表明个人智能体市场需求强烈, 但需自行部署、维护成本高。Muse 将能力封装进 App 与 WhatsApp 降低门槛; **生态体系上**, Muse 可调用 Facebook、Instagram 收藏内容形成上下文, 如将 Instagram 收藏的菜谱转化为购物清单并进一步完成购买。Meta 同时支持通过 Stripe 旗下 Link 完成支付, 并计划支持 Shop Pay 及 1Password, 进一步拓展 Agent 在真实消费场景中的执行能力。

● **AI Agent 自主执行能力提升, 安全与隐私成为产业发展关键约束。** 随着 AI 从“生成内容”向“代替用户执行操作”演进, Agent 可自主浏览网页、调用应用并完成交易, 安全风险同步提升。9 月 9 日, Anthropic 披露第四起 AI 网络安全事件: 早期版本 Claude Opus 4.6 在第三方网络安全评估中因测试环境配置错误获得互联网访问权限, 随后访问真实第三方系统并获取管理员权限。相关事件表明, 长时间自主运行的 Agent 可能通过多步操作突破既有安全边界。Muse 通过“安全虚拟机+权限控制+行为审计”构建防护体系。Meta 为 Muse 配置独立 Secure VM 隔离用户数据及运行环境, 并通过 Sentinel 审查 Agent 对外行为, 相关操作可执行、阻止或提交用户批准; 读取、写入及敏感交易等权限均可细化管理。支付环节通过 Stripe Link 降低真实支付信息暴露风险。Meta 同时计划推出 Confidential VM, 由用户持有密钥, 进一步降低云端数据访问风险。随着个人 Agent 获得更高系统权限, AI 安全需求有望由传统网络安全、终端安全进一步延伸至 Agent 身份权限管理、运行环境隔离、行为审计及数据安全等领域。

● **相关标的 (以下公司均未评级):**

深信服、三六零、启明星辰、绿盟科技、天融信、奇安信等

● **风险提示:** AI Agent 技术发展及商业化进展不及预期; AI Agent 行业竞争加剧; AI 数据隐私及网络安全监管政策趋严; AI 安全业务落地节奏不及预期等。

金元证券股票投资评级标准：

买入：预期未来 6 个月内股价收益率超越沪深 300 指数的涨跌幅 15%以上；

增持：预期未来 6 个月内股价收益率超越沪深 300 指数的涨跌幅 5%~15%；

中性：预期未来 6 个月内股价收益率相对沪深 300 指数涨跌幅差异在-5%~+5%之间；

减持：预期未来 6 个月内股价收益率弱于沪深 300 指数的涨跌幅 5%以上。

金元证券行业投资评级标准：

强于大市：预期行业相关指数在未来 6 个月内超越沪深 300 指数表现；

中性：预期行业相关指数在未来 6 个月内基本与沪深 300 指数表现持平；

弱于大市：预期行业相关指数在未来 6 个月内明显弱于沪深 300 指数表现。

金元证券机构销售负责人：詹宝强

电子邮件：zhanbq@jyzq.cn

免责声明

本报告由金元证券股份有限公司（已具备中国证监会批复的证券投资咨询业务资格）制作。本报告所载资料的来源及观点的出处皆被金元证券认为可靠，但金元证券不保证其准确性或完整性。该等信息、意见并未考虑到获取本报告人员的具体投资目的、财务状况以及特定需求，在任何时候均不构成对任何人的个人推荐。投资者应当对本报告中的信息和意见进行独立评估，并应同时考量各自的投资目的、财务状况和特定需求，必要时就法律、商业、财务、税收等方面咨询专业财务顾问的意见。对依据或者使用本报告所造成的一切后果，金元证券及/或其关联人员均不承担任何法律责任。投资者需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。

本报告所载的信息、材料或分析工具仅提供给阁下作参考用，不是也不应被视为出售、购买或认购证券或其他金融工具的要约或要约邀请。该等信息、材料及预测无需通知即可随时更改。过往的表现亦不应作为日后表现的预示和担保。在不同时期，金元证券可能会发出与本报告所载意见、评估及预测不一致的研究报告。

金元证券的销售人员、交易人员以及其他专业人士可能会依据不同假设和标准、采用不同的分析方法而口头或书面发表与本报告意见及建议不一致的市场评论和/或交易观点。金元证券没有将此意见及建议向报告所有接收者进行更新的义务。金元证券的自营部门以及其他投资业务部门可能独立做出与本报告中的意见或建议不一致的投资决策。

在法律许可的情况下，金元证券可能会持有本报告中提及公司所发行的证券头寸并进行交易，也可能为这些公司提供或争取提供投资银行业务服务。因此，投资者应当考虑到金元证券及/或其相关人员可能存在影响本报告观点客观性的潜在利益冲突。投资者请勿将本报告视为投资或其他决定的唯一信赖依据。

本报告的版权仅为金元证券所有，未经书面许可任何机构和个人不得以任何形式转发、翻版、复制、刊登、发表或引用。