2023 年 04 月 18 日
证券研究报告|行业研究|行业点评

计算机

投资评级 增持
维持评级

生成式 AI 快速发展，网络安全迎市场发展新契机

报告摘要

◆ 生成式 AI 快速发展带来更多潜在安全威胁

继 CHATGPT 发布以来，百度“文心一言”、谷歌 Bard、阿里“通义千问”陆续面世。CHATGPT 从根据要求生成文本、图片、视频，优化到能根据任务自主提出计划并实施的 AUTOGPT。亚马逊推出 Amazon Bedrock，意味着通过 API（应用程序编程接口）即可访问来自 AI21 Labs、Anthropic、Stability AI 和亚马逊的基础模型，并由此构建生成式 AI 驱动的应用程序。生成式 AI 技术不断进步，可以适配行业细分应用场景，赋能更多行业及企业降本增效，市场应用前景广阔。神经网络训练时使用的算法经常涉及到隐私数据，许多情况下，来自公共监控、人脸识别和指纹生物识别、以及财务和医疗应用的大量训练数据集都是隐私的，包含个人可识别信息。攻击者，无论是有组织的犯罪集团还是商业竞争对手，很可能出于经济原因或其他利益原因来利用这些信息。此外，AI 系统还面临着被注入恶意发送的伪造数据、以破坏神经网络功能的风险（例如，因面部识别图像的分类错误而导致攻击者逃脱检测）。**生成式 AI 的潜在安全风险应引起重视，安全保护需从概念生成阶段即融入到产品之中，并贯穿产品的整个生命周期。**

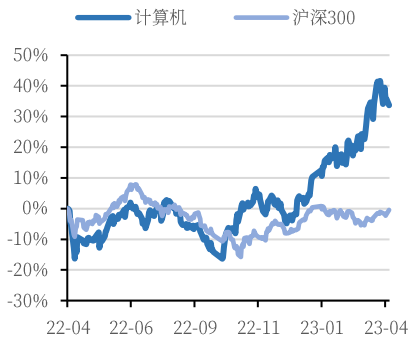
◆ 全球多个国家开始对生成式 AI 加强监管

生成式 AI 持续快速发展的同时，在信息安全、数据合规、版权保护等方面也引发了社会的关注与热议。美国商务部 4 月 11 日就人工智能问责措施正式公开征求意见，包括有潜在风险的新人工智能模型在发布前是否应该通过认证程序。英国政府于 3 月发布了第一份人工智能白皮书，概述了人工智能治理的 5 项原则。此外，3 月底，意大利政府宣布禁止使用一款人工智能聊天机器人，并限制相关公司处理意大利用户信息数据，同时对其隐私安全问题立案调查。加拿大广播公司 4 月 4 日报道称，加拿大联邦隐私监管机构宣布，已对美国人工智能研究公司 OpenAI 展开调查，因该公司涉嫌“未经同意收集、使用和披露个人信息”。**生成式 AI 潜在安全威胁较多，如信息恶意获取、篡改、伪造和乱用、数据泄漏等。安全保护在 AI 流程中不可或缺，强化 AI 监管是大势所趋。**

◆ 生成式 AI 监管意见稿发布，强监管趋势下网络安全迎市场发展新契机

4 月 11 日，国家互联网信息办公室发布《生成式人工智能服务管理办法（征求意见稿）》，向社会公开征求意见。该意见稿聚焦生成式人工智能，在算法设计、训练数据选择、模型生成和优化、提供服务、生成内容、个人信息和隐私保护方面均做出了限制。意见稿第五条指出“利用生成式人工智能产品提供聊天和文本、图像、声音生成等服务

行业走势图



作者

邹润芳 分析师
SAC 执业证书：S0640521040001
邮箱：zourf@avicsec.com

卢正羽 分析师
SAC 执业证书：S0640521060001
邮箱：luzy@avicsec.com

闫智 研究助理
SAC 执业证书：S0640122070030
邮箱：yanz@avicsec.com

相关研究报告

【中航先进制造行业周报】本周专题研究：阿里“通义千问”官宣内测，国内 AI 大模型竞相绽放 —2023-04-09

【中航先进制造行业周报】AI+应用赋能降本增效，场景不断拓展 —2023-04-02

AI 赋能，网安产业或提效优化 —2023-03-30

联系地址：北京市朝阳区望京街道望京东园四区2号楼中航产融大厦中航证券有限公司
公司网址：www.avicsec.com
联系电话：010-59219558 传真：010-59562637

的组织和个人，包括通过提供可编程接口等方式支持他人自行生成文本、图像、声音等，承担该产品生成内容生产者的责任；涉及个人信息的，承担个人信息处理者的法定责任，履行个人信息保护义务”，对人工智能产品使用过程中可能出现的问题的责任归属进行了确定。新的监管政策面对发展势头迅猛的生成式 AI，在生成内容、隐私保护、知识产权保护等方面都做出了限制。意见稿指出“利用生成式人工智能生成的内容应当真实准确，采取措施防止生成虚假信息”，“利用生成式人工智能产品向公众提供服务前，应当按照《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》向国家网信部门申报安全评估”，为生成式人工智能的产品推出设立了门槛。**《征求意见稿》强调了安全评估和算法备案的前提性和必要性；强调了确保数据安全和个人信息保护合规，尤其是隐私保护；夯实了违规责任的处罚措施，包含追究刑事责任。**

投资建议：生成式 AI 快速发展带来更多潜在安全威胁，加强监管是大势所趋。网信办发布生成式 AI 监管意见稿，网络安全市场迎来发展新契机。建议关注：奇安信、天融信、绿盟科技、启明星辰、安恒信息、美亚柏科、三未信安。

风险提示：需求释放不及预期；竞争加剧；技术进展不及预期。

公司的投资评级如下：

买入：未来六个月的投资收益相对沪深 300 指数涨幅 10%以上。
持有：未来六个月的投资收益相对沪深 300 指数涨幅-10%~10%之间。
卖出：未来六个月的投资收益相对沪深 300 指数跌幅 10%以上。

行业的投资评级如下：

增持：未来六个月行业增长水平高于同期沪深 300 指数。
中性：未来六个月行业增长水平与同期沪深 300 指数相若。
减持：未来六个月行业增长水平低于同期沪深 300 指数。

研究团队介绍汇总：

中航证券先进制造团队：研究所所长邹润芳领衔，曾获得 2012 至 2013 年新财富最佳分析师军工机械第一名，2015 至 2017 新财富最佳分析师机械行业第一名，团队在先进制造、军民融合、新能源、新材料等领域有较深的产业资源积淀，擅长自上而下的产业链研究和资源整合，着眼中国制造的转型升级，致力于探索战略产业和新兴产业的发展方向，全面服务一二级市场，拓展产融结合的深度与广度，为市场创造价值。

销售团队：

李裕淇，18674857775，liyuq@avicsec.com，S0640119010012
李友琳，18665808487，liyoul@avicsec.com，S0640521050001
曾佳辉，13764019163，zengjh@avicsec.com，S0640119020011

分析师承诺：

负责本研究报告全部或部分内容的每一位证券分析师，再次申明，本报告清晰、准确地反映了分析师本人的研究观点。本人薪酬的任何部分过去不曾与、现在不与，未来也将不会与本报告中的具体推荐或观点直接或间接相关。
风险提示：投资者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证券投资损失的书面或口头承诺均为无效。

免责声明：

联系地址：北京市朝阳区望京街道望京东园四区 2 号楼中航产融大厦中航证券有限公司
公司网址：www.avicsec.com
联系电话：010-59219558
传　　真：010-59562637