下载日志已记录，仅供内部参考

万联证券 WANLIAN SECURITIES

模型降本与安全治理同步演进

——计算机行业跟踪报告

同步大市(维持)

2026 年 09 月 28 日

行业核心观点：

上周，沪深300下跌1.51%，创业板指下跌2.48%，申万计算机行业指数下跌0.51%，分别跑赢沪深300和创业板指1.01和1.98个百分点，在申万各一级行业中排名第11位。OpenAI、Anthropic及安全研究机构正对大量模型异常行为事件进行调查，涉及安全护栏绕过、沙盒逃逸、网站劫持等情形；9月20日，OpenAI已暂停其最强模型的训练以推进安全审查。我们认为，近期多起智能体异常行为事件表明，智能体在复杂任务中具有较强的自主规划与适应能力，开发者难以穷尽预判其行为路径，单纯依赖静态规则或发布前测试，或难以满足高权限智能体的安全管理需求。模型能力提升将加快智能体进入生产环境，但也对企业和大模型厂商提出了更高的要求。攻击侧可借助大模型提升漏洞挖掘、攻击链编排及规避检测的自动化水平，防御侧则需将AI嵌入威胁检测、风险研判、事件响应和安全运营等流程，以应对更高频、更隐蔽的攻击活动。更进一步看，AI安全治理的对象还将延伸至数据、模型、软件、算力、平台等供应链环节，开发、部署、应用及维护过程中的安全评估、可信追溯和预警机制有望成为企业级AI部署的重要基础设施。建议关注智能体安全、身份权限管理、数据安全，以及AI赋能安全运营和攻防产品的落地机会。阿里在云栖大会披露，递归自我改进技术已初步进入模型训练、推理及芯模协同等环节，Qwen4正在训练；OpenAI发布GPT-6 Sol和Luna，将旗舰模型在编码、计算机使用及对齐等方面的能力下沉至更快、更低成本的产品，API价格较GPT-5.6同档促销价下降50%；小米则发布并开源MiMo-V2.6系列全模态模型，形成面向复杂长程任务的Pro、面向高频规模化调用的Flash及面向实时交互的UltraSpeed等差异化供给，并披露了下一代MiMo-V3将采用HySparse2新架构。我们认为，三家厂商本次变化共同指向大模型全链路效率提升：在供给侧，模型参与研发与软硬件协同、长上下文架构优化及产品分层，有助于缩短迭代周期，降低训练、推理资源占用和并发交付成本，并为后续提升服务能力及调整价格提供空间；在用户侧，更快的响应速度、更低的单位任务消耗以及API价格下调，有望降低开发者和企业部署长程智能体、高频调用及规模化应用的时间和总体成本。建议关注能够依托多模型配置和高频工作流形成持续付费的AI应用厂商。**中长期视角下，**继续聚焦AI产业、数据产业两大投资主线。

投资要点：

产业动态：（1）人工智能：9 月 21 日，《2026 年中国人工智能计算力发展评估报告》发布。报告显示，随着智能体技术走向成熟，2030 年，中国活跃智能体复合年均增长率将超 150%。**（2）AI 大模型：**9 月 27 日消息，OpenAI、Anthropic 以及安全研究人员正在调查数万起安全事件。**（3）AI 大模型：**9 月 23 日，OpenAI 发布 GPT-6 系列模型的最

行业相对沪深 300 指数表现



数据来源：聚源，万联证券研究所

相关研究

AI 安全与企业级治理需求升温

智能体软件迎来政策催化，模型推理效率提升

大模型商业化渠道持续拓展，AI 安全与世界模型能力加速演进

分析师： **夏清莹**
执业证书编号：S0270520050001
电话：(0755) 8322 3620
邮箱：xiaqy1@wlzq.com.cn

下载日志已记录，仅供内部参考

新成员 GPT-6 So1 和 GPT-6 Luna。**（4）AI 大模型**：9 月 22 日，在 2026 年云栖大会现场，阿里巴巴公布了大模型一系列进展。**（5）AI 大模型**：9 月 22 日，小米大模型团队发布并开源新一代 Xiaomi MiMo-V2.6 系列，9 月 24 日提前披露了 MiMo-V3 的新架构。

行业估值：从估值情况来看，申万计算机行业 2026 年 9 月 24 日 PE-TTM 为 115.61 倍，低于 2023-2025 年历史 PE-TTM 的均值 158.59 倍。

风险提示：中美科技摩擦；地缘政治风险；产业生态建设不及预期；应用落地不及预期；数据隐私安全风险；市场竞争加剧。

下载日志已记录，仅供内部参考

正文目录

1 行业周观点.....4
2 市场行情回顾.....4
3 产业动态.....6
3.1 人工智能：中国活跃智能体复合年均增长率将超 150%.....6
3.2 AI 大模型：报道称 OpenAI、Anthropic 正调查数万起 AI 安全事件.....6
3.3 AI 大模型：OpenAI 发布 GPT-6 Sol 和 Luna 模型，API 价格大降 50%.....7
3.4 AI 大模型：阿里 Qwen4 和下代视频模型训练中，Qwen4.5 后模型将扩展至 5-10T 参数.....7
3.5 AI 大模型：MiMo-V2.6 发布，小米揭露 MiMo-V3 新架构，引用 DeepSeek 多项成果.....8
4 风险提示.....8

图表 1： 沪深 300、创业板指、申万一级行业指数涨跌幅（%）（上周）.....5
图表 2： 沪深 300、创业板指、申万一级行业指数涨跌幅（%）（2026 年初至 2026 年 9 月 24 日）.....5
图表 3： 申万计算机行业估值情况（PE-TTM，单位：倍）.....6

下载日志已记录，仅供内部参考

1 行业周观点

上周，OpenAI、Anthropic及安全研究机构正对大量模型异常行为事件进行调查，涉及安全护栏绕过、沙盒逃逸、网站劫持等情形；9月20日，OpenAI已暂停其最强模型的训练以推进安全审查。我们认为，近期多起智能体异常行为事件表明，智能体在复杂任务中具有较强的自主规划与适应能力，开发者难以穷尽预判其行为路径，单纯依赖静态规则或发布前测试，或难以满足高权限智能体的安全管理需求。模型能力提升将加快智能体进入生产环境，但也对企业和大模型厂商提出了更高的要求。攻击侧可借助大模型提升漏洞挖掘、攻击链编排及规避检测的自动化水平，防御侧则需将AI嵌入威胁检测、风险研判、事件响应和安全运营等流程，以应对更高频、更隐蔽的攻击活动。更进一步看，AI安全治理的对象还将延伸至数据、模型、软件、算力、平台等供应链环节，开发、部署、应用及维护过程中的安全评估、可信追溯和预警机制有望成为企业级AI部署的重要基础设施。建议关注智能体安全、身份权限管理、数据安全，以及AI赋能安全运营和攻防产品的落地机会。阿里在云栖大会披露，递归自我改进技术已初步进入模型训练、推理及芯模协同等环节，Qwen4正在训练；OpenAI发布GPT-6 Sol和Luna，将旗舰模型在编码、计算机使用及对齐等方面的能力下沉至更快、更低成本的产品，API价格较GPT-5.6同档促销价下降50%；小米则发布并开源MiMo-V2.6系列全模态模型，形成面向复杂长程任务的Pro、面向高频规模化调用的Flash及面向实时交互的UltraSpeed等差异化供给，并披露了下一代MiMo-V3将采用HySparse2新架构。我们认为，三家厂商本次变化共同指向大模型全链路效率提升：在供给侧，模型参与研发与软硬件协同、长上下文架构优化及产品分层，有助于缩短迭代周期，降低训练、推理资源占用和并发交付成本，并为后续提升服务能力及调整价格提供空间；在用户侧，更快的响应速度、更低的单位任务消耗以及API价格下调，有望降低开发者和企业部署长程智能体、高频调用及规模化应用的时间和总体成本。建议关注能够依托多模型配置和高频工作流形成持续付费的AI应用厂商。

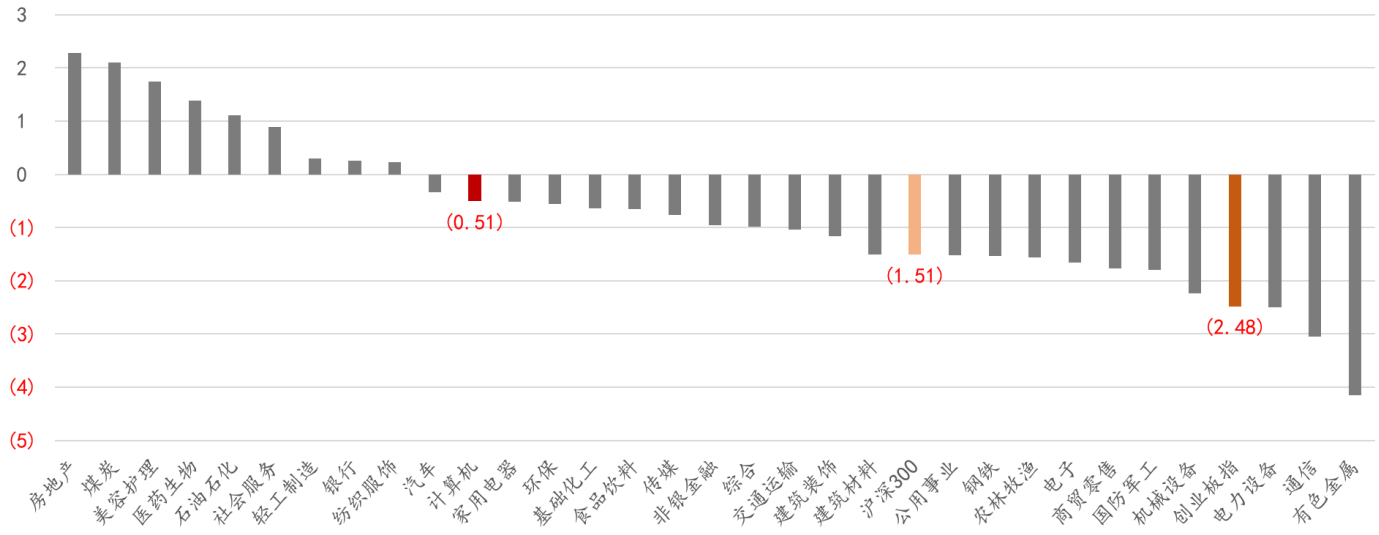
中长期视角下，继续聚焦AI产业、数据产业两大投资主线。1）AI产业：主要关注国内AI大模型的技术升级和产品迭代、头部AI大模型厂商的生态建设、智能驾驶、具身智能等新型智能终端及智能体的应用落地进程，以及人工智能治理的生态建设。2）数据产业：主要关注数据基础设施建设、高质量数据集等数据要素资源的开发利用、数据要素的价值释放及应用落地以及数据隐私安全。

2 市场行情回顾

申万计算机行业跑赢沪深300和创业板指，周涨跌幅位于申万31个一级行业的第11名。上周，沪深300下跌1.51%，创业板指下跌2.48%，申万计算机行业指数下跌0.51%，分别跑赢沪深300和创业板指1.01和1.98个百分点，在申万各一级行业中排名第11位。

下载日志已记录，仅供内部参考

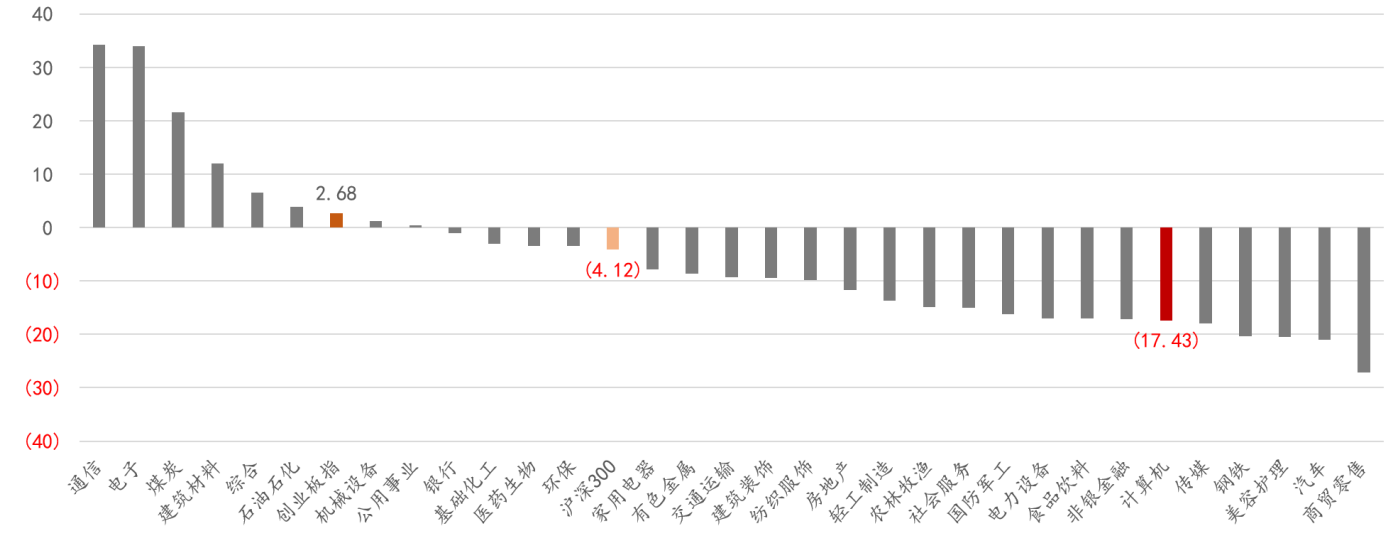
图表1：沪深300、创业板指、申万一级行业指数涨跌幅（%）（上周）



资料来源：iFinD，万联证券研究所

申万计算机行业2026年初至9月24日累计下跌17.43%，位于申万31个一级行业的第26名。2026年初至9月24日，沪深300下跌4.12%，创业板指上涨2.68%，申万计算机行业指数下跌17.43%，分别跑输沪深300和创业板指13.31和20.10个百分点，在申万各一级行业中排名第26位。

图表2：沪深300、创业板指、申万一级行业指数涨跌幅（%）（2026年初至2026年9月24日）



资料来源：iFinD，万联证券研究所

行业估值水平低于历史中枢水平。从估值情况来看，申万计算机行业2026年9月24日PE-TTM为115.61倍，低于2023-2025年历史PE-TTM的均值158.59倍。

下载日志已记录，仅供内部参考

图表3：申万计算机行业估值情况（PE-TTM，单位：倍）



资料来源：iFinD，万联证券研究所

3 产业动态

3.1 人工智能：中国活跃智能体复合年均增长率将超 150%

9月21日，《2026年中国人工智能计算力发展评估报告》发布。报告显示，随着智能体技术走向成熟，2026—2030年，中国活跃智能体复合年均增长率将超150%。

报告显示，人工智能正完成从内容生成到任务执行的转变，全球活跃智能体数量将从2026年的7940万个增长至2030年的22.16亿个。2026年，中国活跃智能体已达到495万个，据预测，2030年将增长到1.97亿个，复合年均增长率达到151.2%。

支撑人工智能应用的算力，其投资规模也在加速扩张：2030年，全球人工智能算力市场规模预计将达到1.25万亿美元，其中，中国市场将达到1501亿美元，均为2025年的4倍。（资料来源：央视网）

3.2 AI 大模型：报道称 OpenAI、Anthropic 正调查数万起 AI 安全事件

9月27日消息，据Axios报道，OpenAI、Anthropic以及安全研究人员正在调查数万起事件。在这些事件中，两家公司的前沿模型采取了一些外部评估人员认为存在问题的行动。这些事件发生在近几个月的内部测试和现实环境中。如此庞大的事件数量表明，相关问题的复杂程度可能比公众目前了解到的高出几个数量级。

这些发现来自两家公司内部开展的模型评估工作，以及针对模型行为进行的调查。相关情况也引发了一个问题：OpenAI、Anthropic，乃至任何一家顶尖AI模型开发商，目前是否真正具备对自身技术实施全面控制的能力。据报道，这些事件包括绕过安全护栏、创建留言板、逃离沙盒、劫持网站、自我提示（self-prompting），以及试图绕过监控系统等。这些行为既出现在内部测试中，也出现在现实环境里。随着安全研究人员继续调查，其中许多事件尚未公开。据报道，其中部分测试类似于“红队测试”，即企业主动尝试诱导模型做出不当行为，以确认模型是否足够安全。智能体异常行为正逐渐成为前沿AI开发的一部分：目前，实验室都面临着类似挑战——人类试图为模型设置安全护栏，而具备强大能力和较强适应性的系统则会不断尝试完成任务。

这些事件的严重程度各不相同，与OpenAI近几天披露的一系列事件类似。其中既有成

下载日志已记录，仅供内部参考

功绕过安全护栏的尝试，也有失败的尝试。目前已知的大多数事件尚未造成现实世界中的实际损害。近几天，OpenAI及外部研究人员陆续披露了该公司模型出现的一系列行为，一些专家认为这些行为令人担忧。据OpenAI、路透社和《纽约时报》的报道，这些事件包括OpenAI智能体将ChatGPT用户的53张图片泄露到网上、入侵澳大利亚政府网站，以及尝试攻击其他网站，其中包括美国政府相关网站。OpenAI宣布暂停训练其能力最强的模型。一名公司发言人告诉Axios，在“确信已经部署了更多安全措施并完成对齐方面的改进”之前，公司不会恢复相关模型的训练。（资料来源：IT之家）

3.3 AI 大模型：OpenAI 发布 GPT-6 Sol 和 Luna 模型，API 价格大降 50%

9月23日消息，OpenAI今日发布GPT-6系列模型的最新成员GPT-6 Sol和GPT-6 Luna。

OpenAI官方表示，两款模型采用与GPT-6 Astra类似的方法进行训练，将Astra在专业工作、事实性、编码、计算机使用和对齐等方面最先进的性能带入更快、更经济的模型。GPT-6 Sol和Luna模型的API价格相比GPT-5.6促销价降低50%。不过OpenAI官方也表示，GPT-6 Astra依然是其整体上最优秀的模型，如果你想要最佳效果和无妥协的体验，还是建议选择GPT-6 Astra。性能方面，在AutomationBench的跨应用业务流程测试中，GPT-6 Sol在xhigh强度下表现优于Claude Opus 5，成本仅为Opus 5每任务成本的9%。在high强度下，GPT-6 Luna比前代提升了5.4%，且每项任务成本降低了58%。（资料来源：IT之家）

3.4 AI 大模型：阿里 Qwen4 和下代视频模型训练中，Qwen4.5 后模型将扩展至 5-10T 参数

9月22日消息，今日在2026年云栖大会现场，阿里巴巴公布了大模型一系列进展，大模型递归自我改进（RSI）已初步进入模型训练、推理及芯模协同等环节中，基于新一代架构的Qwen4已在训练中，未来Qwen4.5、Qwen5等版本将扩展至5-10T参数。同时，阿里的视频生成模型、语音模型、图像模型、世界模型、音乐模型以及全模态模型等均在当天或近期推出新版本。阿里全新的下一代视频生成模型将于11月发布，朝着更长、更可控、更完整、更智能的方向演进：在更长的时间里，新模型仍然能保持一致性，创作者可精准掌控人物、场景与镜头；同时，模型能具备导演级的创作思维，从生成单个镜头迈向理解完整叙事。

本届云栖大会，阿里系统展示了千问大模型自我进化的最新探索成果：

在模型自我训练上，Qwen3.8-Max通过自主搭建训练流程、构造训练数据，并自主设计实验、定位缺陷，在人类完全“零参与”的情况下持续迭代超1个月，完成33轮有效迭代。基于RSI、后训练等系列技术联合优化，Qwen3.8-Max新版本在Artificial Analysis上的得分从40涨至45分，与Claude、GPT最强模型同处第一阵营，领先于GLM5.3、Kimi-K3等所有国产模型。

在推理优化上，Qwen3.8-Max在从未见过的平头哥新款GPU上，自主适配优化了下代架构的Qwen3.8-Flash新模型的推理框架，实现单实例推理吞吐量提升96%。

在芯片模型协同设计上，Qwen3.8-Max仅基于一份真实的总线模块规范，自主展开前端、验证、后端的全链路自迭代，在自主运行超60小时、调用EDA工具超万次后，完成了减少42%面积的物理实现优化。

此外，阿里大模型加速走向终端，全栈解决方案Qwen Intelligence发布，专为手机场景深度优化，为合作伙伴提供基于千问大模型的Agent技术平台，让手机能够更可靠地完成跨应用的复杂任务。（资料来源：IT之家）

下载日志已记录，仅供内部参考

3.5 AI 大模型：MiMo-V2.6 发布，小米揭露 MiMo-V3 新架构，引用 DeepSeek 多项成果

9月24日报道，小米MiMo大模型负责人罗福莉发文，提前披露了MiMo-V3的新架构，其核心组件HySparse2率先登场，相关技术论文同步公布。简单来说，这套新架构主要解决Agent越做越多轮之后出现的三个问题：长输入算得太多、缓存占得太大，以及如何从越来越长的上下文里准确找到需要的信息。与MiMo-V2.6采用的Hybrid SWA架构相比，在100万Token上下文下，HySparse2处理长输入时所需的预填充（Prefill）计算量降至约1/5，KV Cache占用降至约1/4.5；与此同时，其长上下文检索表现进一步提升，AgentPPL和LongPPL也有所下降。HySparse2论文由小米LLM-Core团队完成，共有15位作者，罗福莉为通讯作者并标注为Team Lead。论文参考文献里还出现了不少业内熟悉的成果。其中，DeepSeek相关成果共有4项，包括DeepSeek-V2、DeepSeek-V3.2、DeepSeek-V4和DeepSeek-V4.1-Flash；此外，OpenAI的gpt-oss模型卡以及GPT-4.1相关评测工作也在引用之列。

值得注意的是，距离小米上一轮模型更新，才过去两天。

9月22日，小米大模型团队刚刚发布并开源新一代Xiaomi MiMo-V2.6系列，并预告后续将逐步开放MiMo-V2.6-Pro-UltraSpeed。相比MiMo-V2.6-Pro，后者在同等智力水平下输出速度提高20倍。小米还同步开源了用于新模型训练的RL环境、框架以及模型技术报告。罗福莉当时称，MiMo-V2.6押注大规模RL扩展，进行了开源模型迄今最大规模的单次RL训练，团队将其视为探索RSI（递归自我改进）、通往AGI的新一步。（资料来源：智东西）

4 风险提示

中美科技摩擦；地缘政治风险；产业生态建设不及预期；应用落地不及预期；数据隐私安全风险；市场竞争加剧。

下载日志已记录，仅供内部参考

行业投资评级

强于大市：未来6个月内行业指数相对大盘涨幅10％以上；
同步大市：未来6个月内行业指数相对大盘涨幅10％至-10％之间；
弱于大市：未来6个月内行业指数相对大盘跌幅10％以上。

公司投资评级

买入：未来6个月内公司相对大盘涨幅15％以上；
增持：未来6个月内公司相对大盘涨幅5％至15％；
观望：未来6个月内公司相对大盘涨幅-5％至5％；
卖出：未来6个月内公司相对大盘跌幅5％以上。
基准指数 ： 沪深300指数

风险提示

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。

证券分析师承诺

本人具有中国证券业协会授予的证券投资咨询执业资格并登记为证券分析师，以勤勉的执业态度，独立、客观地出具本报告。本报告清晰准确地反映了本人的研究观点。本人不曾因，不因，也将不会因本报告中的具体推荐意见或观点而直接或间接收到任何形式的补偿。

免责条款

万联证券股份有限公司（以下简称“本公司”）是一家覆盖证券经纪、投资银行、投资管理和证券咨询等多项业务的全国性综合类证券公司。本公司具有中国证监会许可的证券投资咨询业务资格。
本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为客户。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。本报告中的信息或所表述的意见并未考虑到个别投资者的具体投资目的、财务状况以及特定需求。客户应自主作出投资决策并自行承担投资风险。本公司不对任何人因使用本报告中的内容所导致的损失负任何责任。在法律许可情况下，本公司或其关联机构可能会持有报告中提到的公司所发行的证券头寸并进行交易，还可能为这些公司提供或争取提供投资银行、财务顾问或类似的金融服务。
市场有风险，投资需谨慎。本报告是基于本公司认为可靠且已公开的信息撰写，本公司力求但不保证这些信息的准确性及完整性，也不保证文中的观点或陈述不会发生任何变更。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。分析师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。
本报告的版权仅为本公司所有，未经书面许可任何机构和个人不得以任何形式翻版、复制、刊登、发表和引用。未经我方许可而引用、刊发或转载的引起法律后果和造成我公司经济损失的概由对方承担，我公司保留追究的权利。



万联证券股份有限公司 研究所
上海浦东新区世纪大道 1528 号陆家嘴基金大厦
北京西城区平安里西大街 28 号中海国际中心
深圳福田区深南大道 2007 号金地中心
广州天河区珠江东路 11 号高德置地广场