下载日志已记录，仅供内部参考

万联证券 WANLIAN SECURITIES

AI 安全与企业级治理需求升温

——计算机行业跟踪报告

同步大市(维持)

2026 年 09 月 21 日

行业核心观点:

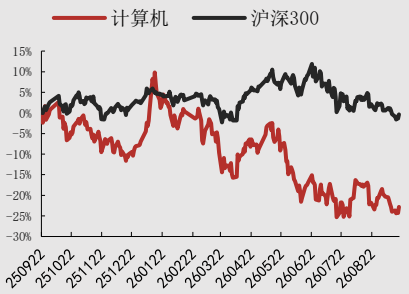
上周，沪深300下跌0.06%，创业板指上涨1.52%，申万计算机行业指数上涨1.58%，分别跑赢沪深300和创业板指1.64和0.05个百分点，在申万各一级行业中排名第10位。2026年国家网络安全宣传周聚焦人工智能对网络攻防及安全治理的影响；智谱MaaS平台宣布将上线“数据内容不留存”机制，用户申请开通后，常规模型调用的输入和输出内容仅用于完成当次请求，不再在平台侧静态保存；OpenAI发布模型失配行为报告框架，将模型训练、评估、测试及部署过程中出现的规避监督及安全措施失效等现象纳入持续跟踪、调查和披露机制，并同步披露首批6项案例，推动模型安全从发布前评测进一步向持续监测和事件披露延伸；Anthropic则从高风险能力访问和第三方评估两个方向加强安全治理。我们认为，近期国内外监管机构和头部厂商的安全部署呈现较强一致性，AI安全正由单点的模型内容治理逐步走向覆盖数据安全、模型安全、身份权限、工具调用、运行时监测和安全评测的全生命周期治理体系。其中，数据不留存、敏感信息识别与脱敏等能力，有助于降低企业将内部文档、代码及业务数据接入模型时的安全隐私顾虑；而模型获得更高的任务执行与工具调用权限后，最小权限控制、操作审计、异常拦截和人工复核将成为其进入金融、政务及研发等高价值场景的重要前提。同时，模型行为披露、持续监测和第三方评估逐步完善，有望推动企业客户由关注模型性能与价格，进一步延伸至安全能力的可验证性和全生命周期治理水平。建议关注智能体安全、数据安全及AI赋能攻防产品的落地机会。TypeSafe AI发布结构化决策模型Jev，不生成文本，直接返回结构化决策，其成本和延迟远低于大型语言模型。我们认为，Jev的产品思路并非替代通用大模型，而是针对软件自动化中的高频、低时延决策环节提供更轻量的模型能力，可用于客服工单分流、智能体工具选择及机器人动作决策等场景；若能够在真实业务中实现稳定调用，有望降低智能体在工具路由、状态判断及规则执行环节的响应时间和单位成本。建议关注具备高频自动化决策需求的智能体编排及具身智能软件方向。**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 14 日至 20 日，2026 年国家网络安全宣传周在全国范围统一开展。**（2）AI 大模型：**9 月 18 日，新一代原生全模态模型 Qwen3.8-Omni-Flash 正式上线。**（3）AI 大模型：**9 月 16 日，TypeSafe AI 发布公告，宣布推出 Jev，该 AI 模型定位为“One Model”（系统一模型）。**（4）AI 大模型：**9 月 20 日，智谱 MaaS 平台宣布，近期将上线数据内容不留存功能。

行业估值:从估值情况来看，申万计算机行业 2026 年 9 月 18 日 PE-TTM

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

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

大模型能力与成本协同优化，AI 商业化验证持续增强

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

为 116.12 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：人工智能重塑网络安全治理格局.....6
3.2 AI 大模型：Qwen3.8-Omni-Flash：从理解到交付，释放全模态 Agent 生产力.....7
3.3 AI 大模型：前 OpenAI 研究员推出首款“System One”模型引爆 AI 圈：不生成文本，专为机器做快速决策.....8
3.4 AI 大模型：智谱 MaaS 平台上线数据内容不留存机制.....8
4 风险提示.....9

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 18 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，2026年国家网络安全宣传周聚焦人工智能对网络攻防及安全治理的影响；智谱MaaS平台宣布将上线“数据内容不留存”机制，用户申请开通后，常规模型调用的输入和输出内容仅用于完成当次请求，不再在平台侧静态保存；OpenAI发布模型失配行为报告框架，将模型训练、评估、测试及部署过程中出现的规避监督及安全措施失效等现象纳入持续跟踪、调查和披露机制，并同步披露首批6项案例，推动模型安全从发布前评测进一步向持续监测和事件披露延伸；Anthropic则从高风险能力访问和第三方评估两个方向加强安全治理。我们认为，近期国内外监管机构和头部厂商的安全部署呈现较强一致性，AI安全正由单点的模型内容治理逐步走向覆盖数据安全、模型安全、身份权限、工具调用、运行时监测和安全评测的全生命周期治理体系。其中，数据不留存、敏感信息识别与脱敏等能力，有助于降低企业将内部文档、代码及业务数据接入模型时的安全隐私顾虑；而模型获得更高的任务执行与工具调用权限后，最小权限控制、操作审计、异常拦截和人工复核将成为其进入金融、政务及研发等高价值场景的重要前提。同时，模型行为披露、持续监测和第三方评估逐步完善，有望推动企业客户由关注模型性能与价格，进一步延伸至安全能力的可验证性和全生命周期治理水平。建议关注智能体安全、数据安全及AI赋能攻防产品的落地机会。TypeSafe AI发布结构化决策模型Jev，不生成文本，直接返回结构化决策，其成本和延迟远低于大型语言模型。我们认为，Jev的产品思路并非替代通用大模型，而是针对软件自动化中的高频、低时延决策环节提供更轻量的模型能力，可用于客服工单分流、智能体工具选择及机器人动作决策等场景；若能够在真实业务中实现稳定调用，有望降低智能体在工具路由、状态判断及规则执行环节的响应时间和单位成本。建议关注具备高频自动化决策需求的智能体编排及具身智能软件方向。

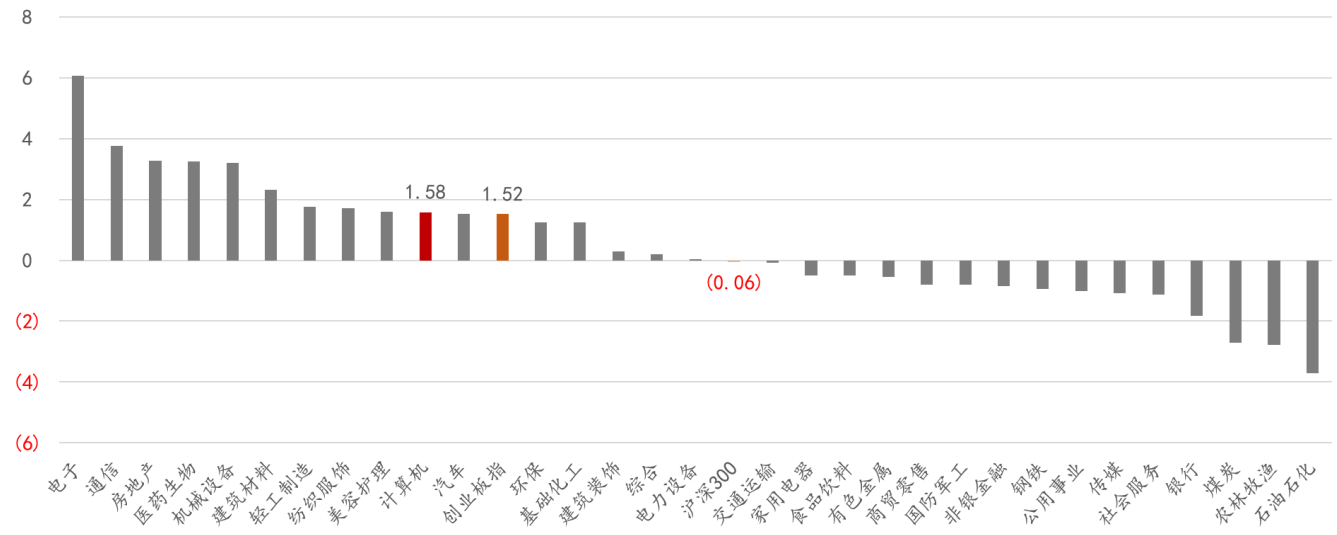
中长期视角下，继续聚焦AI产业、数据产业两大投资主线。1）AI产业：主要关注国内AI大模型的技术升级和产品迭代、头部AI大模型厂商的生态建设、智能驾驶、具身智能等新型智能终端及智能体的应用落地进程，以及人工智能治理的生态建设。2）数据产业：主要关注数据基础设施建设、高质量数据集等数据要素资源的开发利用、数据要素的价值释放及应用落地以及数据隐私安全。

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10名。上周，沪深300下跌0.06%，创业板指上涨1.52%，申万计算机行业指数上涨1.58%，分别跑赢沪深300和创业板指1.64和0.05个百分点，在申万各一级行业中排名第10位。

下载日志已记录，仅供内部参考

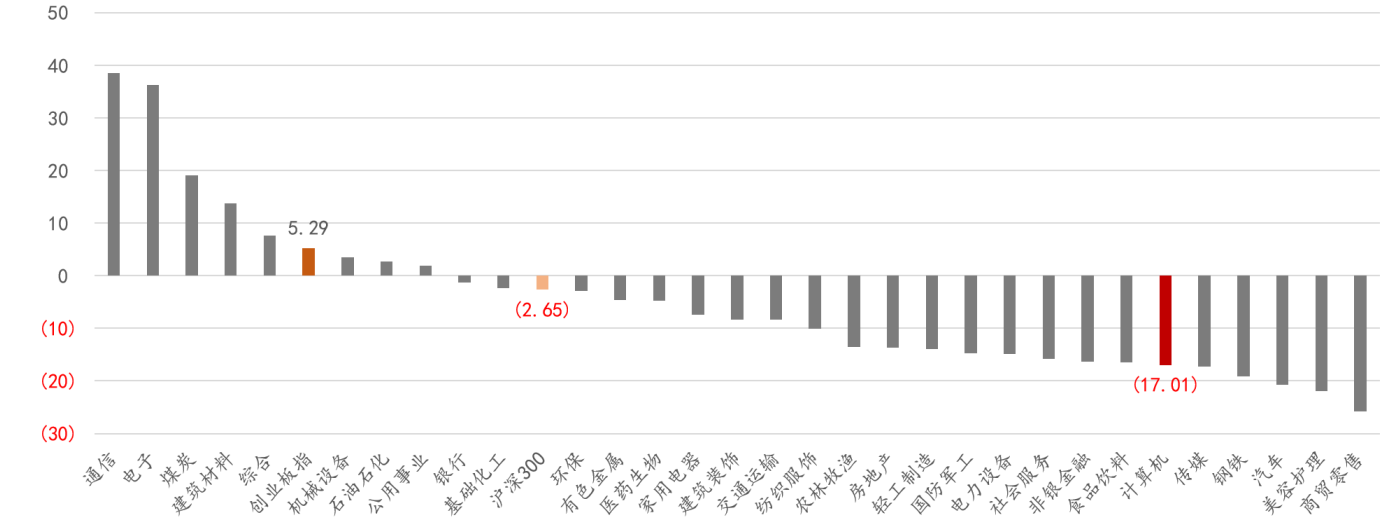
图表1：沪深300、创业板指、申万一级行业指数涨跌幅（%）（上周）



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18日累计下跌17.01%，位于申万31个一级行业的第26名。2026年初至9月18日，沪深300下跌2.65%，创业板指上涨5.29%，申万计算机行业指数下跌17.01%，分别跑输沪深300和创业板指14.36和22.30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18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18日PE-TTM为116.12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：人工智能重塑网络安全治理格局

9月14日至20日，2026年国家网络安全宣传周在全国范围统一开展，紧扣智能时代网络安全新形势、新任务，集中展示网络安全领域的发展成果，助力网络安全技术与实体经济深度融合。

人工智能的高速发展，正推动网络安全形势发生深刻变化。在网络安全技术高峰论坛上，中央网信办副主任、国家网信办副主任王京涛指出，AI驱动的网络攻击呈现出智能化、自动化、隐蔽化特征，深刻重塑网络安全保障体系和治理格局，成为影响国家网络安全的关键变量。

攻击能力在跃迁，防御也要随之应变。随着大模型能力不断突破，漏洞挖掘从人工分析逐步转向自动化，传统以被动防护为主的模式难以为继。人工智能技术可以赋能漏洞挖掘、威胁检测等环节，帮助安全人员从海量数据中更快发现异常，网络安全防御的人力和时间成本均大幅降低。

当前，技术变革已传导至产业端，网络安全企业将大模型、智能体嵌入原有产品和服务，提升风险发现、研判和处置效率。以绿盟科技集团的新一代智能渗透测试系统AI-PTS 2.0为例，该系统以AI模拟黑客攻击视角，通过以攻促防、风险前置的方式增强安全产品的防御能力，帮助企业主动挖掘系统漏洞。绿盟科技集团副总裁汤旭表示，未来网络安全需从“边界防御”走向“韧性安全”，以算力对抗算力、以AI对抗AI，构建持续进化的主动防御体系。

攻与防相互交织、动态博弈，给网络安全产业带来新的需求和发展机遇。国际数据公司（IDC）预测，中国网络安全市场规模将从2023年的110亿美元增长至2028年的171亿美元，5年复合增长率达到9.2%。

“过去更多关注服务器、终端和网络边界，现在攻击对象进一步向智能应用、数据以及模型和智能体延伸，数据流动、权限调用、智能体执行等都可能成为新的风险点。”中孚信息股份有限公司副总裁王金国表示，中孚信息不仅利用AI提升传统安全能力，也加强了AI自身的安全治理，围绕终端、网络和平台持续完善AI安全产品体系。

下载日志已记录，仅供内部参考

如今，智能体的能力边界不断拓展，除辅助生成内容外，还能规划任务、调用工具、访问数据并执行操作等，与业务流程的连接日益深入。但与此同时，其自身也成为网络攻击的目标，一旦被恶意操纵，风险将会被进一步放大。

围绕数据调用、权限管控、行为监测等环节，网络安全企业正加快布局智能体安全产品和解决方案。奇安信集团的企业级智能体安全解决方案，让多个安全控制点协同工作，由智能体安全平台统一管理，把资产、会话、模型调用、工具调用和网络行为关联起来，最终实现对企业智能体的统一发现、监测、管控、风险分析等。蚂蚁集团推出的ASL智能体安全可信互联协议，聚焦智能体之间的交互合作，为其提供共同的安全规则：确认彼此身份，通过加密通道交换信息，保护用户指令，并约束每步的操作行为。

智能体的安全运行，不仅取决于模型自身，更依赖其身后的AI供应链，网络安全防护的范围需要扩大至供应链各环节。今年5月，国家网信办、国家发展改革委、工业和信息化部联合印发《智能体规范应用与创新发展实施意见》，提出加强供应链安全，制定智能体开发、部署、应用、维护等全周期安全规范，探索建立智能体供应链安全信息共享和预警机制，并提出搭建产业协作平台，协同产业链上下游开展智能体共性技术研发、标准制定、评估认证等工作。

“AI供应链覆盖数据、模型、软件、算力、平台、工具、服务7类相互依赖的资产，任何一类资产的来源都可能改变最终模型的安全、合规和业务表现。”中关村实验室首席科学家、中国工程院院士云晓春表示，AI供应链安全，最终要证明可信依赖能够产生可信结果，需要看见完整链条，绑定可验证证据，随时准备变化与退出。

网络安全能力的构建离不开开放合作、协同共享的产业生态。在华为公司全球网络安全官杨晓宁看来，数字生态的安全单靠任何一家企业都无法独立完成，必须坚持共建共享，构建立体协同防御体系，而这需要各利益相关方尽快达成AI时代的风险共识。

“人工智能带来威胁范式的深刻变革，挑战巨大，但也带来安全能力升级的全新机遇。”杨晓宁建议，以内生安全与纵深防御筑牢根基，以网络韧性与安全运营应对不确定性风险，以立体协同防御凝聚全社会合力，真正守护数字化转型行稳致远。（资料来源：中国经济网-《经济日报》）

3.2 AI 大模型：Qwen3.8-Omni-Flash：从理解到交付，释放全模态 Agent 生产力

9月18日，新一代原生全模态模型Qwen3.8-Omni-Flash正式上线。该模型的核心目标是提升其在真实生产力场景中的Agent能力，推动全模态模型从“理解全模态内容”进一步走向“规划任务、调用工具并完成创作”。在具备编程、文本知识工作和GUI操作等通用Agentic能力的基础上，Qwen3.8-Omni-Flash进一步拓展了以音视频为核心的Agentic应用，在视频剪辑、音乐视频创作、影视制作与解说、音视频转图文摘要和音视频对话等，需要综合处理文本、图像、音频与视频的工作流中取得了显著效果。Qwen3.8-Omni-Flash支持1M长序列，在保持与同尺寸文本模型相当的文本能力的同时，全模态能力显著提升。

在累计30项评测上，相比上一代Qwen3.5-Omni-Plus，平均得分提升超过26%。

在音视频Agent、Coding和长程任务方面，模型在UniClawBench-MM上大幅提升36.5分，在AgenticVBench上提升23分，并在UniClawBench上取得69.6的高分。

基础能力方面，模型在长音频/音视频理解、音视频推理、音视频Caption和多说话人识别上均有明显提升：例如，LongAudioSpan提升8.3分，OmniVideoBench提升9.6分，

下载日志已记录，仅供内部参考

OmniCap-IF的CSR/ISR分别提升8.5/14.1分，AliMeeting的DER/cpWER从88.11/89.61降至3.35/17.18。

通过扩展数据、上下文与Agentic Environment，Qwen3.8-Omni-Flash的音视频能力接近Gemini 3.8 Flash，音频能力整体超过Gemini 3.8 Flash。

这些能力的进一步提升，也意味着音视频正在从模型的感知输入，进一步成为Agent理解环境、开展推理并执行任务的核心载体。

同时，Qwen3.8-Omni-Flash的API每小时音频输入价格降幅超过98%，每小时音视频输入价格降幅超过93%。（资料来源：“千问大模型”公众号）

3.3 AI 大模型：前 OpenAI 研究员推出首款“System One”模型引爆 AI 圈：不生成文本，专为机器做快速决策

日前，一款由美国TypeSafe AI公司发布的首款“System one”模型Jev，震动AI圈。不同于以ChatGPT为代表的大语言模型，这款由前OpenAI研究员研发的模型不生成对话、文章或代码，而是面向软件自动化场景，直接返回可以被程序调用的结构化判断及相应概率。

“System One”的名称来自心理学家丹尼尔·卡尼曼在《思考，快与慢》中提出的“系统一”概念，指快速、直觉式的判断。以ChatGPT为代表的大语言模型被纳入“系统二”，Jev则是专门做快速决策的“系统一”模型。

Jev根据TypeSafe AI的定义，开发者可以向Jev输入一段非结构化信息或程序状态，并预先设定问题与候选答案。模型目前支持Choice、Score和Noul三种问题类型，分别用于从给定选项中作出选择、按照设定标准评分，以及判断某个陈述成立的概率。

其中，Choice和Score会返回概率分布及置信度；Noul则直接返回一个介于0和1之间的数值。多个问题可以在一次调用中针对同一份状态并行、独立地处理。开发者不必再要求大模型逐个生成自然语言或JSON文本，然后对结果进行解析和校验。

例如，客服系统可以输入一段用户投诉，让Jev判断问题应该转交账单、技术支持还是销售部门，同时评估问题的紧急程度；智能体系统也可以输入当前任务与可用工具，由Jev判断下一步应该调用哪个工具。

TypeSafe AI宣称，在适合这类快速判断的“System One”任务中，Jev能够达到与部分现有大模型相近的判断水平，同时速度和效率提高两个数量级。虽然Jev不具备字符串生成功能，但它对结构化输出进行了优化，并且不会产生幻觉。（资料来源：澎湃新闻）

人在草木间

3.4 AI 大模型：智谱 MaaS 平台上线数据内容不留存机制

9月20日，智谱MaaS平台宣布，近期将上线数据内容不留存功能，为企业和开发者用户提供更严格的数据隐私保护。

数据内容不留存机制旨在减少模型调用内容在平台侧的持久化留存。任何用户均可以申请开通，生效后，智谱MaaS平台不会对用户的输入和输出进行静态存储，数据仅用于完成当次模型调用。企业和开发者可通过MaaS控制台提交开通申请，具体生效时间及适用范围以平台确认结果为准。

需要说明的是，这个功能并不意味着任何情形下都不留存数据。Batch API、File API等需要在平台侧持久化保存任务或文件的功能不在上述覆盖范围内，以及法律法规要求留存、为核查涉嫌违规或滥用行为的情况，平台可能按有关要求留存相关数据30

下载日志已记录，仅供内部参考

天及以上。（资料来源：“智谱开放平台”公众号）

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