

# 网络安全企业加速AI创新 新产品竞相落地

近日，多家网络安全上市公司公布网络安全领域AI技术应用的新进展。绿盟科技、北信源向记者透露AI创新成果,深信服、亚信安全等企业相继公布应用AI技术的网络安全产品以及市场应用。

行业专家认为,AI技术应用在带来新型安全风险的同时,也为网络安全行业提升效率、提高产品能力带来机遇。

● 本报记者 郑萃颖

## “网络安全+AI”成研发重点

9月23日,记者获悉,绿盟科技将于近期发布保护大模型自身安全的网络安全产品,包括AI安全一体机、AI安全围栏、大模型安全评估系统以及相关的服务和解决方案。

绿盟科技副总裁宫智介绍,目前绿盟科技通过深入研究AI系统的安全风险,针对客户AI系统的不同应用模式,提供场景化的产品和服务,帮助客户全面提升AI体系的整体安全防护能力,实现在线AI系统的安全合规。

北信源董事、副总裁高藏近日对记者表示,AI技术帮助企业提升开发效率,完善产品性能。公司已开发出AI能力平台,集成了大模型、开发工具和知识库,可进行私有化部署。此外,公司已在金融、能源行业等领域交付了应用AI技术的相关软件产品。

多家网络安全上市公司正在积极投入AI技术研发。深信服在投资者互动平台表示,持续将人工智能技术与能力融入网络安全和云计算各项产品与服务中,截至目前已将大模型技术应用到网络安全产品,形成安全GPT、融合AI能力的AI防火墙和其他多款安全产品,并计划未来继续加大对AI技术的研发投入。

天融信表示,公司已在AI+安全、智算云等新方向进行布局 and 投入,目前已形成“云、管、边、端”全栈安全产品体系与智算云综合解决方案,并在多行业实现规模化应用。未来将重点推动网络安全、智算云产品与人工智能等新兴场景的深度融合。

# 多家上市公司前三季度业绩预喜 绩优股获机构密集调研

● 本报记者 董添

A股三季度业绩预告陆续披露。Wind数据显示,截至9月23日19时,A股共有17家上市公司对外披露2025年前三季度业绩预告,8家预喜,预喜比例约为47.06%。长川科技、中泰股份、兄弟科技等公司前三季度净利润增幅居前。一些上市公司发布三季度业绩预告后,获机构密集调研。三季度业绩向好原因、产品价格变动、主要产品市场拓展情况等问题较受关注。

## 业绩预增推升股价

上述17家披露2025年前三季度业绩预告的上市公司中,略增4家、扭亏1家、预增3家,已披露业绩预告的上市公司整体保持了较好的业绩增长。

长川科技预计2025年前三季度实现归属于上市公司股东的净利润为8.27亿元至8.77亿元,同比增长131.39%至145.38%。报告期内,半导体市场需求持续增长,公司客户需求旺盛,产品订单充裕,销售收入同比大幅增长,使得利润同比大幅上升。

中泰股份预计2025年前三季度实现归属于上市公司股东的净利润为3.25亿元至3.55亿元,同比增长71.36%至87.19%。报告期内,公司国内外订单进入正常发货流程,海外收入占比增加,带动公司利润上升。此外,报告期内,非经常性损益对公司净利润的影响金额约1000万元。



蚂蚁集团也于近日发布了融合网络安全与AI技术的创新产品及解决方案。其中,智能眼镜可信连接技术框架gPass已与Rokid、小米、夸克、雷鸟等智能眼镜品牌合作,率先落地“看一下支付”场景。在大模型安全方面,蚂蚁集团展示了AIGC滥用检测、深度伪造防御在内的多项解决方案。

另外,启明星辰表示,其开发的安星智能体已经应用于安全运营、威胁检测、数据安全等产品或服务中,显著提升了产品的能力和服务的效率。亚信安全称,上半年,公司AI大模型应用与交付业务实现显著增长,未来公司将持续聚焦AI大模型应用与交付,5G专网与应用、数智运营三大增长引擎,加快签单节奏。

## AI应用带来安全新挑战

信息技术咨询公司Gartner的报告显示,中国网络安全的重点正逐步转向保障人工智能的安全,实现业务转型并加强企业、机构的韧性。

Gartner高级研究总监陈延全称,预计到2027年,60%的中国大型企业将在安全运营中心采用暴露面管理技术,以提升事件响应效率并减少漏洞。预计到2028年,在部署AI技术的中国企业中,60%企业将实施协作式AI防御策略,整合跨职能团队应对AI网络安全风险,而目前这一比例仅为5%。

一些公司业绩预告发布后,股价出现较为明显的上涨。以兄弟科技为例,公司9月16日晚间披露的前三季度业绩预告显示,公司预计2025年前三季度共实现归属于上市公司股东的净利润为1亿元至1.15亿元,同比增长207.32%至253.42%。其中,第三季度共实现归属于上市公司股东的净利润为3545.9万元至5045.9万元,同比增长92.49%至173.92%。业绩预告发布的次日,公司股价应声涨停。

## 机构聚焦增长逻辑

部分上市公司发布三季度业绩预告后,获机构密集调研。

以兄弟科技为例,公司9月22日披露的投资者关系活动记录表显示,公司获得上海海能投资、江苏高投创投、台州国投、胜达资本等投资机构调研。机构对公司三季度业绩向好原因、维生素产品价格变动、产品销量增加,同时部分产品成本下降,整体毛利率提升所致。对于维生素产品价格变动的主要原因,兄弟科技表示,维生素产品的价格变动主要由供需结构、成本波动、产业周期及行业竞争等多重因素综合作用,目前公司维生素B1价格相比上年同期实现增长,处稳中有升态势,其他维生素品种持平

绿盟科技副总裁曹嘉表示,企业应用AI大模型时需警惕提示词注入、模型被诱导等风险。“虽然这些风险在模型运营或开发厂商中出现的概率较低,但仍需重点关注。目前,行业主要依赖电子围栏技术来防止模型被诱导输出违规内容。”曹嘉说,另外云计算的安全问题须引起重视。

绿盟科技首席创新官刘文懋则提到工具链安全的重要性。他解释称,在企业应用AI大模型过程中,工具链漏洞和配置错误可能导致严重的数据泄露,例如智能体调用第三方工具时存在的风险。他呼吁重视软件供应链安全,采取加强版本漏洞管理、代码安全审计等基础安全措施。

360集团创始人周鸿祎近日公开表示,大模型在带来机遇的同时也带来了恶意利用、内容安全、幻觉问题、提示词攻击等风险。大模型既是生产力工具,也可能成为新的攻击载体和攻击入口,政府和企业的数字资产、商业机密面临着前所未有的暴露风险,保障AI安全是一项长期而艰巨的任务。

奇安信在投资者互动平台表示,大模型能显著提升网络安全企业的能力和效率,产生“乘数效应”。该公司认为,当前政企推广智能体应用的趋势,类似于二三十年前普及网站的浪潮。然而,智能体应用也带来了爆炸式增长的安全风险,因为它们往往拥有企业内网的超级权限。奇安信建议企业加强跨部门协作,构建动态防御体

系,特别是部署特权账号管理系统,以应对AI智能体带来的安全风险。

构建AI安全防护网

在保障AI应用安全方面,行业专家们认为,可以从大模型强制备案、构建体系化防护入手,保障企业应用AI过程中的安全。

曹嘉认为,AI大模型备案应成为强制性要求,模型厂商可以到当地网信部门进行基础评估,提前识别风险,让使用者更全面地理解其安全性与可用性。

“与传统软件和基础设施相比,AI大模型的风险更大、更泛化,必须由专业安全厂商进行持续投入。未来,大模型的检测与防御将走向一体化,客户需要从产品开发、代码审计等全流程进行规划。”曹嘉说。

此外,AI大模型的运营单位可以通过构建防护体系,保障AI应用安全。首先开展合规评估,对照监管规定、合规检查清单进行自查;其次是部署专项防护,引入AI安全围栏等技术,防御新型攻击,并确保过程可审计、可追溯;再是考虑引入第三方评估,定期进行渗透测试和安全评估,获取权威报告,降低责任风险。

刘文懋认为,AI技术应用将为各行业带来爆发式增长,但安全问题限制了数据流通。他认为,通过安全手段建立信任,推动数据流通,并将AI全面应用于各类场景,将为各行业释放巨大价值。

展望未来,公司将继续秉持创新驱动发展理念,通过强化内生增长与积极外部拓展,充分发挥遍布全球29个国家、105个生产基地的全球化制造优势,为客户提供更灵活高效的定制化服务,从而进一步巩固和拓展全球市场竞争力。同时,公司将以“智能制造升级”和“底层技术创新”为双轮驱动,全面提升全产业链的运营效率与成本管控能力。此外,公司将加速多元化业务战略布局,持续加大在AI智能终端、光电高速互联产品以及汽车智能电子电器等前沿领域的研发投入与市场渗透。

除了发布业绩预告外,近期,不少上市公司在投资者互动平台提到,三季度部分新产品业务有望实现快速增长。

星辰科技提到,公司智能机器人、车载前装等新增长曲线三季度仍可保持快速成长,同时在机器人、边缘计算、激光雷达等领域均有中高端新品推出,长期来看有利于公司整体ASP及毛利水平的提升。

一些公司提到,由于订单量较好,对全年营收增长有信心。9月23日,广电计量在深交所互动易平台提到,2025年,公司将逐步推进收入增长与精细化管理双因素驱动利润增长。今年以来,公司在汽车、集成电路、航空航天等行业继续维持高强度研发投入,订单保持较快增长。全年来看,公司预计将依托科技创新类业务的快速增长,实现全年营业收入的稳定增长,公司继续通过精细化管理,实现利润增速高于收入增速。

系,特别是部署特权账号管理系统,以应对AI智能体带来的安全风险。

## 构建AI安全防护网

在保障AI应用安全方面,行业专家们认为,可以从大模型强制备案、构建体系化防护入手,保障企业应用AI过程中的安全。

曹嘉认为,AI大模型备案应成为强制性要求,模型厂商可以到当地网信部门进行基础评估,提前识别风险,让使用者更全面地理解其安全性与可用性。

“与传统软件和基础设施相比,AI大模型的风险更大、更泛化,必须由专业安全厂商进行持续投入。未来,大模型的检测与防御将走向一体化,客户需要从产品开发、代码审计等全流程进行规划。”曹嘉说。

此外,AI大模型的运营单位可以通过构建防护体系,保障AI应用安全。首先开展合规评估,对照监管规定、合规检查清单进行自查;其次是部署专项防护,引入AI安全围栏等技术,防御新型攻击,并确保过程可审计、可追溯;再是考虑引入第三方评估,定期进行渗透测试和安全评估,获取权威报告,降低责任风险。

刘文懋认为,AI技术应用将为各行业带来爆发式增长,但安全问题限制了数据流通。他认为,通过安全手段建立信任,推动数据流通,并将AI全面应用于各类场景,将为各行业释放巨大价值。

## 友升股份： 专注轻量化汽车零部件 募资24.71亿元布局新产能

● 本报记者 王辉

9月23日,上海友升铝业股份有限公司首次公开发行A股上市仪式,在上海证券交易所举行,并在中国证劵报·中证网直播。

友升股份董事长、总经理罗世兵在致辞中表示,近年来,公司始终专注于轻量化汽车零部件领域,致力于推动新能源汽车的续航升级和燃油车的节能减排。公司将以在上交所主板上市为契机,不断加强技术创新,为客户提供优质、可靠、领先的产品和服务。以轻量化技术突破赋能汽车产业低碳转型,为我国“双碳”政策目标的实现贡献“友升力量”。同时,公司也将借力资本市场,进一步扩大经营规模,稳步实现资产增值,以高质量发展回馈广大投资者。

## 铝合金轻量化零部件的先行者

成立于1992年的友升股份,是集设计、开发、生产、销售、服务于一体的专业铝合金汽车零部件制造商,公司始终专注于轻量化汽车零部件领域,致力于推动新能源汽车的续航升级和燃油车的节能减排,也是国内新能源汽车铝合金轻量化零部件的先行者。2024年,公司获评国家级专精特新“小巨人”企业。

公司产品主要聚焦于新能源汽车领域,已经形成了门槛梁系列、电池托盘系列、保险杠系列、副车架系列等多产品体系。凭借着先进的技术工艺、强大的产品开发实力和规模化的产品交付能力,公司得到全球领先的新能源汽车整车厂商特斯拉、广汽集团、蔚来、北汽新能源、吉利集团的高度认可,形成了长期稳定的合作关系。在燃油车业务领域,公司主要客户包括凌云工业、富奥股份、华域汽车等知名一级汽车零部件厂商。

招股书相关信息显示,2022年至2024年,公司分别实现营业收入23.50亿元、29.05亿元和39.50亿元,分别实现归母净利润2.33亿元、3.21亿元和4.05亿元。根据最新财务数据,公司2025上半年实现营业收入21.76亿元,较上年同期增长30.76%;实现归母净利润2.21亿元,较上年同期增长50.07%。整体来看,近年来,公司营收、利润持续保持快速增长,在新能源汽车市场不断发展壮大的过程中,体现出了较强的经营稳健性和成长性。



友升股份董事长、总经理罗世兵在上市仪式现场致辞  
本报记者 王群 摄

## 募资投向三项目

综合公司招股书等信息,公司在本次IPO中募集资金24.71亿元,扣除发行费用后,将用于:云南友升轻量化铝合金零部件生产基地项目(一期)、年产50万台(套)电池托盘和20万套下车体制造项目、补充流动资金三个项目。

在未来发展战略规划上,一方面,公司将继续以拓展国内外高端优质客户为重点方向,扩大公司在新能源汽车零部件领域的影响力,夯实公司在新能源汽车产业链中的行业地位。另一方面,公司将不断加大研发投入和新产品开发,对新产品、新工艺、新技术进行持续投资,提升产品性能,优化生产工艺,提高生产效益。

未来,公司将积极把握新能源汽车行业快速增长带来的市场机遇,响应“碳达峰、碳中和”的号召,紧跟“十四五”规划的发展方向,大力拓展公司产品和技术在新能源汽车产业链上的应用,为提升我国新能源汽车的工业水平做出贡献。

业内人士表示,铝合金制备出的汽车零部件不仅契合新能源汽车轻量化需求,还具有可靠性高、热稳定性强等优势,是近年来应用最广泛的轻量化材料,尤其在重量占比较高的汽车的门槛梁、电池托盘、保险杠、副车架等汽车结构件领域。友升股份依托早期在铝合金材料配方的研发、挤压和机加工等领域积累的丰富工艺制造经验,逐步向后端深加工业务延伸,在门槛梁、保险杠等细分领域占据领先地位。

## 致力于成为“全球汽车工业顶级供应商”

罗世兵表示,公司目前已系统掌握高性能铝合金新材料、先进加工工艺和轻量化终端产品的设计等三大核心技术,产品质量及技术水平受到行业内一流客户的高度认可。

在战略布局上,公司深度践行国内国际双循环发展战略,已在上海、山东、重庆等地建成多座现代化制造基地。同时,公司稳步推进全球化布局,在墨西哥建设生产基地,在保加利亚设立泽升欧洲,主动融入全球汽车产业协作体系,持续提升国际竞争力与品牌影响力,致力于成为“全球汽车工业顶级供应商”。

作为保荐机构代表,国泰海通证券业务总监、投资银行业务委员会总裁郁伟君称,友升股份的成功上市,既是对过去成就的肯定,更是迈向新征程的起点。未来,国泰海通证券将继续秉承勤勉尽责的原则,切实履行保荐义务,做好上市后的持续督导和资本市场服务,助力友升股份借助资本市场实现更高质量发展。