

证券代码：688561

证券简称：奇安信

奇安信科技集团股份有限公司
投资者关系活动记录表

编号：2025-003

投资者关系活动类别	<input type="checkbox"/> 特定对象调研 <input type="checkbox"/> 分析师会议 <input type="checkbox"/> 媒体采访 <input type="checkbox"/> 现场参观 <input checked="" type="checkbox"/> 业绩说明会 <input type="checkbox"/> 路演活动 <input type="checkbox"/> 一对一沟通 <input type="checkbox"/> 新闻发布会 <input type="checkbox"/> 其他
参与单位及人员	本次参会机构共 88 家，参会人员 101 人，具体名单详见文后附录。
时间	2025 年 8 月 29 日 10 点 00 分-11 点 15 分
方式	线上会议
接待人员	董事长齐向东；董事、总裁吴云坤；董事会秘书徐文杰； 财务经理郑静；证券事务代表张腾
投资者交流主要内容介绍	<p>本次业绩说明会主要包含两部分，第一部分由公司管理层介绍公司 2025 年半年度经营情况，第二部分由公司管理层与投资者互动问答。</p> <p>第一部分由公司管理层介绍公司 2025 年半年度经营情况：</p> <p>2025 年上半年，公司整体经营质量进一步提升，实现营业收入 17.42 亿元，同比下降 2.30%，实现归母净利润-7.70 亿元，同比增长 6.16%，扣非归母净利润-7.70 亿元，同比增长 9.82%，经营性现金流净额-11.43 亿元。报告期内，公司人效指标不断提升，人均创收 24.44 万元，同比增长 14.93%；人均销售回款 23.23 万元，同比增长 6.03%。上半年，公司坚定贯彻执行年初制定的“聚焦”战略，在核心产品、核心客户、渠道改革和海外市场等方面取得了如下成绩：</p> <p>(1) 产品研发</p> <p>公司进一步聚焦核心产品，积极加强产销拉通，十余款核心产品上半年新签订单额同比增长约 6%。分产品版块看，得益于数据安全管控平台和大模型卫士等新品的驱动，以及一批核心产品在运营商行业陆续斩获大单，云与大数据安全的新签订单额同比增长超过 24%；工业互联网安全在能源和特种行业实现重要突破，新签订单额同比增长超过 61%；受实战攻防演练的推动，以及签下了多个安服大单，安全服务的新签订单额同比增长超过 24%。</p>

在聚焦 AI 场景的安全防护方面：1) DeepSeek 等大模型应用落地，触发 AI 智能体产业爆发，而 AI 智能体是政企机构内网中的“超人”，对数据拥有超级权限，将成为外部黑客和内部“内鬼”的重点攻击对象，需要进行全面的安全防护，这是传统制造业和传统服务业给安全行业提供的巨大增量市场。公司针对客户规模大小的区别，推出了“大模型安全空间”和“奇安天界大模型安全一体机”两款不同的解决方案。2) 公司自研了安全智能体框架（AI Agent），基于大模型实现自主任务规划与工具编排，可动态求解复杂安全问题，并提供可扩展的自进化方案，显著提升处理效率与准确性。创新型 AI 项目方面，应用巡检智能体在某能源单位成功实现了试点。

在聚焦安全产品 AI 化方面：1) 天眼、天擎、椒图、安全监管、防火墙、数据安全、威胁情报、盘古和工业互联网等核心产品，围绕“AI+”持续开展产品的创新升级。2) 典型客户案例方面，AISOC 新签客户和试运行客户数都呈现大幅增长趋势，告警准确率显著提升，获得行业标杆客户的认可。“AI+代码卫士”以金融行业为核心，在北京银行、人保科技等近 10 家头部客户验证成功，打造了行业标杆案例。3) 在 AI 的内部提效上，截至报告期末，公司开发人员 AI 代码助手的使用率已超过 90%，AI 生成代码量占比 5%。

在聚焦核心产品竞争力提升方面，公司从实战化、平台化、服务化等维度不断提升核心产品线的市场竞争力，推出了一批重磅新品：1) 奇安云镜（零信任 SASE），该产品首次在架构层面清晰划分“云功能”与“安全功能”的边界，解决了在云时代，包括私有云、公有云、混合云，以云公司为主提供的安全能力不能满足客户安全需求的问题。该产品将推动云安全从“混沌分工”迈向“专业司职”的新纪元，云公司负责应用功能，安全公司负责安全功能，各司其职且泾渭分明，彻底改变以往职责不清、安全无人担责的局面。2) 新一代网络资产攻击面管理系统（CAASM），该系统通过融合资产治理、风险监测与安全运营，直击企业网络资产“盘不清”、受害资产“找不到”、安全隐患“扫不着”、海量漏洞“改不完”、违规资产“管不了”等安全痛点。

能力及奖项方面，2025 年上半年，公司参与已发布的网络安全国家标准共计 7 项，行业标准 1 项，涉及数据安全、隐私计算、云安全、攻防技术、应急响应、网络安全保险等众多前沿领域。报告期内，公司成为唯一同时入选中国网络安全产业联盟（CCIA）“网安三新”的企业。在 IDC 的最新报告中，公司除了在安全软件市场三大核心领域——终端安全、数据安全、安全分析和情报，以及安全咨询服务市场蝉联份额第一以外，还凭借在大模型安全保护、安全智能体两大领域的布局，入选我国大模型安全保护市场的全部 7 个细分领域以及安全智能体市场的 5 个领域，成为“安全+AI”赛道覆盖最广的厂商，彰显了公司在 AI 领域的创新领先实力。

（2）市场销售

报告期内，公司在 1,000 家大客户的基础上，建立了大客户深挖的运营范式与机制，重点聚焦其中的 200 家超大客户。得益于对客户的进一步聚焦，上半年公司持续在金融、运营商、能源、制造、消费品、政府等行业斩获大单。

海外市场方面，报告期内，公司拿下了一批标杆客户案例：1) 中标某国有银行的最大海外分支机构项目，涉及终端安全产品及安全服务，金额超 2,000 万元。该项目是

公司在中资海外市场最大的案例标杆，也是中资网安厂商在该地区的最大单体项目。2) 拿下西亚某国轨道交通系统的网络安全项目，在海外轨道交通工控安全市场实现重要突破。

渠道发展方面，1) 在商业客户市场，公司向其释放了超过 2 万家指名客户，并推进渠道业务与省分区业务的本地化融合，通过渠道管理部统筹发展，为合作伙伴提供产品、方案、专家、商机四重精准支持。在产品供给上，推出超过 20 款渠道专属分销产品及数款限时促销爆品，以“快周转、易交付、好回款”的特点强化市场竞争力。2) 在产业渠道市场，公司全面开展与央企数科公司等渠道伙伴的合作，根据不同企业的信息化与业务发展水平，针对不同阶段分别提供安全防御体系建设、安全运营体系与安全能力输出，以及全线产品及服务的销售。

(3) 财务视角

收入结构方面，企业级客户继续成为公司收入端的主要引擎。报告期内，企业级客户、政府客户、公检法司分别占主营业务收入比为 78.74%、14.54%、6.72%。能源、金融、运营商和特种这四大行业合计占公司主营业务收入比重超过 50%。从收入的体量分布上看，百万级以上客户收入比重超过 60%，尤其是公司最坚实的“基本盘”——500 万级以上的关基行业大客户，贡献了其中主要的收入。

在费用支出方面，公司进一步执行了严格的费用管控，报告期内三费（销售费用、研发费用、管理费用）总金额较去年同期降低 2.57 亿元，三费费用率同比下降 12.38 个百分点。在现金流管理方面，公司成立了回款专项管理组织，专门运营回款，通过识别不同类型的回款问题，建立更有针对性的回款举措，以多种手段推动实现回款的“应收尽收”。Q2 单季度，公司实现销售回款 10.34 亿元，同比增长 8.00%。

第二部分由公司管理层与投资者进行问答互动：

问题一、最近关注到全球网安巨头 Palo Alto 以 250 亿美金拟收购身份安全厂商 CyberArk，之前 Google 也斥巨资以 320 亿美元收购云安全公司 Wiz。这些全球巨头都在网络安全行业频繁进行一些收购动作，请问对国内网络安全行业的发展有什么样的影响或启示？

答：影响是正面的。今天在美国网络安全行业发生的事，我们预计未来也会发生在中国。因为从全球的角度来看，各国都遭受着同样的网络攻击，网络攻击者全球化的趋势已经形成。网络安全的技术、方法和服务，无论在中国、美国还是其他国家都没有区别。

先说 Palo Alto 拟斥资 250 亿美元天价收购 CyberArk。

该收购案例证明随着智能体（AI Agent）的迅速崛起，企业面临着非常严峻的安全挑战，身份管理领域在 AI 时代的需求是十分紧迫的。在生成式人工智能技术成熟的催生下，智能体的生命力已经充分展现。政企如今做智能体与二三十年前做网站是类似的需求和发展趋势。推广使用智能体以提质增效，也是现在传统制造业和传统服务业所迫

切需要的。

但是智能体应用带来的安全风险也呈爆炸式增长。因为一个企业要用智能体，会是一类智能体为一大群员工服务，这意味着智能体在企业内网变成了一个具有超级权限（即它所服务的员工权限的大集合）的员工或者说“超人”。

威胁智能体的源头是谁呢？1）首当其冲的是黑客。对传统制造业和服务业来说，智能体基本都是委托第三方公司开发的，第三方公司规模有大有小、能力有高有低，即使他们开发出来的智能体好用，也并不代表其安全或者没有漏洞。2）内部人的威胁。比如企业内部运营智能体的员工，即管理员、程序员和操作员，通过借用智能体的权限内部作案、监守自盗，以及离职前窃取数据。

面对这种“权限雪崩”，Palo Alto 收购身份安全龙头企业 CyberArk 的目的就是解决上述问题。这次收购会产生“1+1>2”的效果——Palo Alto 提高了竞争力和市占率，同时也让 CyberArk 在智能体时代展现出了新的生命力。

在身份权限管理方面，奇安信也有一款非常优秀的产品：特权账号管理系统（PAM）。它具备三大核心技术：最小授权原则的特权管控、凭据“零存储”机制以及全链路审计。该产品在市场上受到了客户的广泛欢迎。

2025 年或成为 AI 智能体爆发元年，各行各业都在积极部署适合自身场景的 AI 智能体应用。与此同时，AI 时代的非人类身份安全威胁将持续增长，生成式 AI 和 Agentic AI 的普及将进一步放大风险。企业急需加强跨部门协作，结合 AI 技术构建动态、弹性的防御体系，尤其是通过部署特权账号管理系统，来破解 AI 智能体广泛应用带来的身份失控危机，确保 AI 技术服务于安全而非威胁。一手抓“AI 驱动安全”，一手抓“AI 应用场景”，将会是奇安信未来在 AI 智能体时代的主要发展策略。

再谈 Google 以 320 亿美元收购云安全公司 Wiz。

Wiz 是云安全领域的一家头部公司，Google 则是全球最大的云服务和人工智能服务提供商之一。因此，Google 收购 Wiz 可以给 Google 的云服务和人工智能服务打上一个更强劲的安全标签，从而带来更大的收益。

事实上，由云公司为客户包办云服务和云安全，把客户的技术服务和安全服务都“放在一个篮子里”的做法，在未来是不长久的。因为安全是一种专业的服务，它一定要和云计算体系形成对抗，由安全公司不断地发现云公司在体系建设结构设计方面的缺陷和不足，督促云公司不断加强在安全方面的投资和研发，为客户提供更安全的云服务，这才是符合趋势的。

因此，今年上半年，我们推出了一款新产品——奇安云镜（零信任 SASE），专门用于解决上述问题。该产品首次在架构层面清晰划分“云功能”与“安全功能”的边界，解决了在云时代，包括私有云、公有云、混合云，以云公司为主提供的安全能力不能满足客户安全需求的问题。该产品将推动云安全从“混沌分工”迈向“专业司职”的新纪元，云公司负责应用功能，安全公司负责安全功能，各司其职且泾渭分明，彻底改变以往职责不清、安全无人担责的局面。

与之相呼应，国际网安巨头 Palo Alto 也有类似的业务——重点投入并打造自身的 Prisma 平台。Prisma 是 Palo Alto 推出的云原生安全套件，覆盖安全访问(Prisma Access)、云安全(Prisma Cloud)和 SASE 框架(Prisma SASE)三大方向，主要解决多云和混合云安全、零信任场景下的安全需求。

最后结合海外巨头的天价并购案例，做个总结。

以 Palo Alto 为代表的网络安全巨头通过外延+内生“双轮驱动”的模式，实现业务规模的快速扩张，持续提升市场集中度。参考 Omdia 等第三方数据，Palo Alto 在美国的市场份额为 28%，与 Check Point、Fortinet 等头部厂商共同占据 60% 的市场。并且从估值水平上说，Palo Alto 的市值是 1,270 亿美元，收入 92 亿美元，净利润 11 亿美元，PS 是 14 倍，PE 是 112 倍。另一家知名公司 CrowdStrike 市值是 1,100 亿美元，收入 40 亿美元，利润亏损，PS 是 28 倍。由此可见，通过对如 CyberArk、Wiz 等专有技术公司的并购，美国的巨头们在提升技术能力、扩张市占率的同时，还形成了估值的飞轮效应。这也很好的指引了国内网络安全企业的发展路径。

问题二、海外业务是公司近年来重点开拓的一块增量，上半年成功拿下了一批标杆性的客户案例，想请教一下，公司全年以及远期来看，对海外市场的展望是什么样的？

答：海外市场是奇安信公司战略性重点布局的增量市场。

首先，在整个海外市场，奇安信有五类用户：

1) “一带一路”友好国家的网络安全监管部门。这与每个国家的发展程度有关，各国在网络体系建成以后都在参照超级大国建设网络监管部门，所以也会购买很多相应的网络安全监管工具以及平台。

2) “一带一路”国家的关键信息基础设施部门。涉及水电、油气、交通、运营商、金融、能源等领域，这部分和关键基础设施行业数字化后我们国内的情况非常类似。

3) 中资海外分支机构。我国很多央企、国企和民营企业都在出海，在去国外开展业务的整个过程中不仅需要实现本地化合规，同时也要符合国内的监管政策。

4) 我国承建的一些海外工程项目的配套。海外项目中，比较大的能源、电力、轨道交通和运营商等都有很多信息化建设的相应需求。

5) 特种行业的特种配套，包括取证过程中的一些监管工具等。

再者，从组织策略上看，我们和过去也不太一样。早些年我们处于探索过程，在东南亚以及非洲、中东地区都取得了比较好的效果。在这之后，我们一直在思考一个非常重要的问题——组织方面的保障，也就是本地化的运营。所以，我们在全球各地选取了一些重要的地点，推动代表处的建立，包括子公司和区域总部。在整个过程中，我们提供的不是简单的网络安全产品售卖，而是体系性的解决方案，既要给客户做规划，还要交付并实施安装，更重要的是确保体系运行起来。同时也要根据每个国家和区域网络安全进攻防御的威胁情报来开展运营。所以，本地化的开发和服务团队都非常重要，这也

是我们组织方面的能力。

第三，在海外市场拓展上，我们充分实施了渠道方面的策略。过去我们的渠道策略中有一条是“跟着国内的大集成商和工程建设商往外走”，未来在国际市场上，我们不仅仅是借船出海，更重要的是在海外建立自己的代理商体系。所以，我们在一些重点国家，尤其是“一带一路”友好国家，建立起了三级代理商体系，包括海外总代（T0 级别）、区域总代（T1 级别）和国家二级代理（T2 级别）。这些代理商可以提供拓展和推广的销售通道，更重要的是，在代理商体系建设的过程中还会调用当地的服务能力，与代理商联合开展市场活动，推广触达用户侧。

此外，我们还有一些比较特殊的合作伙伴，包括深耕海外的 ICT 企业、一些特种行业的贸易公司以及运营商国际公司等，我们也与他们一起开发整个市场。

最后，从“十五五”规划到未来十年的考虑来看，我们的目标是海外收入在“十五五”末占比达到 15%，到十年后的 2035 年能达到 30%。

综上，奇安信在国际市场的开拓方面是有清晰规划的，一定会将其作为重要的新兴市场来进行耕耘。

问题三、从国内情况看，公司对下游行业景气度作何展望？

答：这两年，网安行业，包括整个 ICT 领域遇到的挑战，其实是结构性问题。结合今年上半年的数据，以及下半年的预算规划、商机情况等，我们可以看到几个明显的变化：

1) 央企、国企，包括银行。因为存在内生动力，其网络安全投入明显增加，这部分也是公司收入的主要来源。所谓内生动力，就是在数字化转型过程中，需要为自己的安全托底。例如在使用大模型的时候，担心大模型的安全问题；在数据集中上云时，担心云的安全问题；在使用智能体时，要考虑身份的安全管理问题等。以上都是主要来自于内生性的安全需求。

2) 信创市场。基于国家的一系列政策指引和时间要求，信创已经逐渐由过去的办公系统向业务系统、甚至生产系统转移，而生产系统最多也最为复杂的是央企国企，如 13 个关基行业以及银行等。目前，信创已不再局限于办公市场，更大的需求来自于工业控制，包括一些复杂的交易系统，以及制造类部分生产系统的升级，所以市场空间非常大。

3) 政府市场。从上半年来看，政府在网络安全方面的投入有所上升，尤其是 2024 年一些滞后的项目开始恢复，这与化债的整个进度有很大关系，另外也和各地大数据局、大数据中心、大数据集团“三驾马车”的协同推动关系密切。在数据梳理清楚后，投资是在逐步恢复的。

4) 特种领域。国际局势发生变化以后，全球许多国家在特种领域网络安全方面都加大了投资。而我国周边环境也较为复杂，美国的贸易战主要针对我国，所以特种领域市场有比较大的增量。

5) 工业控制领域。过去我们的安全主要服务于互联网侧，而生产侧则是工控网络，

这里面有比较复杂的系统、装置，以及比较独特的协议，每个行业各有不同。在工业控制领域中，尤其是能源和特种行业，所需产品与整个装置装备相结合，如国产化替代、以及安全检测和安全防御等，都有明显的行业特征。我们把这部分叫作小批量行业专用产品，盈利能力较强且进入壁垒很高。今年上半年公司在这个领域的新签订单额同比增长超过 61%，是很好的例证。

6) AI+安全市场。在这个领域中，最直接的是 AI 如何驱动安全和赋能安全。在攻防整个链条中，对于每个细节技术点，AI 都可以实现赋能。赋能的核心可以是提高检测精度，也可以是提升覆盖率，或者降低成本。所以，我们在代码安全、安全运营、数据安全、安全攻防、安全检测形成了五大智能体，对整个产品能力进行升级，同时节省成本。以安全运营智能体 AISOC 为例，公司在 SOC 存量市场上已经是国内领先，现在只要把存量市场加入 AI，就可以形成一个新的市场增量。公司和头部客户们开展了很多实验局，今年上半年就有 20 个，普遍反馈超出预期。以全球某些高端车企为例，在真实的攻防对抗环境下，通过 AISOC 加持的智能运营模式，无论是平均威胁检测时间、研判定性时间，还是关键告警的识别率和准确率，都有了革命性的提升。在公司内部，我们也把 AI 编程训练作为长期培养的活动进行推广，在整个开发效率、代码质量以及安全性方面，都取得了非常大的进步。

另外，在 AI 应用场景侧，公司推出了“大模型安全空间”和“大模型安全卫士”，旨在保护百业千行的大模型，这是非常重要的一个领域。我们最终要实现“管得住、看得清、防得稳”。目前，公司的“大模型卫士”已通过行业主管部门的《大模型安全防护围栏（增强级）认证》，并凭借无需改造应用、低耦合、高并发的特性，在政府、央企、科技制造等行业的多家头部机构和企业中真实落地部署和应用，为客户提供了可靠的安全保障，成为“人工智能+”安全落地的坚实后盾。

问题四、想请公司自上而下地分享下关于 AI+安全的整体框架思路？

答：从 2022-2023 年生成式大模型实用化开始，公司就立刻通过奇安信人工智能研究院，在原有的深度学习小模型基础上，快速地把大模型技术应用到了网络安全产品当中，这两年多的时间里也产生了非常多的成果。尤其是在今年初，DeepSeek 免费开源后，我们在 AI+安全产品方面取得了非常大的突破，也加速了奇安信全线安全产品全面拥抱 AI 的进程。

首先，公司比较成熟的第一个代表产品是 AISOC，即通过 AI 来强化 SOC 的网络安全运营。安全产品的运营需要人力，如果有足够多的人力去运营安全产品每天产生的告警，大概率是能够把网络攻击都阻断掉的。当前网络攻击者主要从两个方向试图攻破奇安信等安全厂商构筑的防线：

一是新技术，即攻击者发明一种新的攻击方式，让安全厂商检测不出来。但事实证明，这条路随着安全防护能力的不断跃升已经越走越窄，成本也越来越高了。二则是制造“饱和式攻击”，使用低端攻击方式产生海量告警，超过安全运营人员处理能力的上限，就可能趁乱攻入系统中。“饱和式攻击”需要的是带宽资源、服务器资源、IP 地址资源、以及部署在全球的跳板、蜜罐等隐匿网络的资源。这些资源在十年前都很珍贵，

所以过去攻击者进行“饱和式攻击”很难，成本也很高。但随着近年来 5G、云计算等技术的成熟，攻击所需资源的价格大幅下降，带来了很大的威胁。以前业内没有特别好的办法应对这种“饱和式攻击”，因为加人就等于加成本，投入大量高水平的网络安全分析师将带给客户巨大的预算压力。因此，“饱和式攻击”曾经是网络安全防护体系里最大的一个漏洞，即能力的漏洞。

AISOC 用人工智能代替网络安全分析师完成对相对低端的攻击分析，虽然它对分析最高水平的网络攻击目前能力还存在一定欠缺，但对饱和式的普通攻击非常有效。我们做了统计，在应对“饱和式攻击”时，一个 AISOC 机器人智能体的效率可以相当于几十个安全分析师。目前，奇安信 AISOC 产品已在全国各个行业的多个实验局得到了大量认可。

第二个代表产品是“AI+天眼”。在网络安全行业有句广为流传的话，“无天眼，不HVV”。天眼是高级别的威胁发现系统，因此需要高级别的 AI 进行配合，我们在这方面的探索也取得了很大成果，在全国开展了主要的实验局。

第三个代表，即另一个拳头产品，是我们的“AI+代码卫士”。程序员写代码的时候不可避免地会存在一定漏洞，原来的“代码卫士”产品专门用于风险代码的检查，市场占有率很高，但其查出来的疑似风险代码需要人工的核对，对人工的消耗很大。现在我们用 AI 去分析“代码卫士”的输出结果，形成一体机，效果非常好。公司先从银行、保险、证券等对漏洞要求比较高的行业开始推广，一些典型用户已经成为了标杆案例，从而产生了显著的市场复制效应。

此外，公司还对终端安全、数据安全等产品都进行了“AI+”的升级，并且也取得了非常好的成效。

问题五、在 DeepSeek 等一些开源大模型发布后，一部分人产生了关于 AI 降低软件竞争力的担心。在这一背景下，公司的优势要如何体现出来？

答：首先，大模型现在能做到的是让企业的能力和效率在原有竞争力的基础上大幅度提升。换句话说，大模型目前还不能“无中生有”，而是产生了一个“乘数效应”。各家安全厂商原有的竞争力基础有所差异，即“被乘数”有高有低，同时使用大模型的能力也并不相同，即“乘数”也有大有小，“相乘”后的结果确实可能改变其在行业内的位置。从这个意义来说，大模型的确是能够影响网络安全行业格局的。

而相比大多数友商，奇安信的独特优势主要体现在三个方面：

1) 自身独特的数据积累优势。俗话说，“先有信息化，再有数字化，才有智能化”。以网络安全为例，我们向客户提供应急响应服务，需要撰写安全事故分析报告、处置报告和整改报告。这三份报告以往是以纸质的形式交给客户，如果只停留在纸质形式上，就无法通过人工智能进行综合运用。所以，首先要实现信息化，即为客户提供纸质报告的同时通过系统给客户发送电子邮件。但这并不够，还要对这三份报告进行结构性的分析，对它的关键词、关键环节进行加工处理，添加各种标签，补充各种属性，让报告的

特征以数字的形式显现出来，这时候才完成了数字化。

应急响应实现报告数字化之后，就可以“投喂”给大模型，帮助我们把这些报告的经验提炼出来，提升我们的能力，使得大模型成为一个大于1的“乘数”。可见，积累的报告质量和数量决定了大模型能够赋予企业的乘数大小。奇安信不仅公司规模排名第一，同时还有全国最大的网络安全应急响应体系，及服务短号95015。我们积累的数据集形成了巨大的优势，同时，这些数据集在用大模型训练的时候，还能够用来纠正大模型可能产生的一些“幻觉”。公司在这方面的能力是业内顶级的，并且不会开源，这是企业的知识产权以及核心竞争力。

2) 技术人才的优势。公司从2014年创办起，就成立了人工智能研究院，从互联网业务开始积累了一批顶尖的人工智能研究员。在大模型技术到来之前，公司没有让这些研究员散落出去，因为我们相信人工智能的时代一定会到来。人工智能研究院是我们宝贵的财富，这些研究员也没有辜负公司的期望，在大模型实用之前就通过深度学习、精准模型等方面，改进了公司的多项产品和技术，包括我们对威胁情报和开源情报的处理。在深度学习和精准模型方面，从2014年到2022年期间，公司形成了70多款专有产品和技术，来服务我们的客户。在这个过程中，这些人才也一直紧跟全球顶尖的技术，得到了持续性的成长。现在进入生成式人工智能时代，我们很高兴，因为我们手里有人才。目前，公司在AI相关领域的发明专利有200多项，技术团队在国际顶尖AI赛事中也屡获大奖。

3) 专有的AI基础设施，用于训练和微调。公司在这方面的投入和积累也是领跑行业的。目前我们拥有AI大模型算力平台、AI大模型服务平台、AI大模型安全检测平台，在此基础上我们积累了70多项的模型能力，能够广泛地服务于安全应用层。

以上三点共同构筑了公司在垂类AI领域的独特优势和领跑地位。

——结束——

附：线上参会机构名单，按所在机构拼音首字母排序。

机构名称	参会者姓名
IncTar Cap	Woiae Han
北京博润银泰投资管理有限公司	尚方建
北京和信金创投资管理有限公司	黄庆铭
北京金融街资本运营集团有限公司	管文杰
北京禹田资本管理有限公司	赵玮玮
北京泽铭投资有限公司	单河
北京致顺投资管理有限公司	朱贺凯
北京紫薇私募基金管理有限公司	李晓林
毕盛(上海)投资管理有限公司	龚昌盛
渤海创富证券投资有限公司	王洪磊
财通证券股份有限公司	罗云扬
常州投资集团有限公司	祝慧
创金合信基金管理有限公司	李晗
东北证券股份有限公司	马宗铠
东吴证券股份有限公司	戴晨

附件清单
(参会机构人员
单位、姓名)

	福建金牛投资管理股份有限公司	梁敏忠
	福建鑫诺嘉誉投资有限公司	廖勇
	福建兴合创业投资有限公司	林书顺
	富瑞金融集团香港有限公司	馬牧野
	富瑞金融集团香港有限公司	张朗铭
	富瑞金融集团香港有限公司	Annie Ping
	光大证券股份有限公司	白玥
	广东钜洲投资有限责任公司	王中胜
	广东仙津实业投资有限公司	李隆海
	国海证券股份有限公司	伍海量
	国海证券股份有限公司	刘熹
	国金证券股份有限公司	李忠宇
	国联民生证券股份有限公司	姜青山
	国联民生证券股份有限公司	黄楷
	国盛证券有限责任公司	李纯瑶
	国泰海通证券股份有限公司	楼剑雄
	国信证券股份有限公司	库宏垚
	国信证券股份有限公司	贺平鸽
	国信证券股份有限公司	云梦泽
	国元证券股份有限公司	胡爱军
	国元证券股份有限公司	耿军军
	海南鑫焱创业投资有限公司	陈洪
	杭州致道投资有限公司	刘福杰
	航天科工投资基金管理(成都)有限公司	陈鹏
	合方创新(厦门)私募基金管理有限公司	任熠
	鸿运私募基金管理(海南)有限公司	舒殷
	湖南潇湘资本投资管理有限公司	陈靓璇
	华创证券有限责任公司	胡昕安
	华福证券有限责任公司	魏征宇
	华泰证券股份有限公司	范昞蕊
	华源证券股份有限公司	董佳男
	汇丰前海证券有限责任公司	刘逸然
	汇丰前海证券有限责任公司	张恒
	金泰富资本管理有限责任公司	李云浩
	开源证券股份有限公司	刘逍遥
	美银证券	李慧群
	美银证券	庄亚林
	南京璟恒投资管理有限公司	徐冬梅
	磐厚动量(上海)资本管理有限公司	胡建芳
	青岛韬观投资管理有限公司	李佩柯
	泉果基金管理有限公司	王苏欣
	瑞银环球资产管理(中国)有限公司	丁宁
	山西证券股份有限公司	邹昕宸
	上海冰河资产管理有限公司	刘春茂
	上海贵源投资有限公司	赖正健
	上海国理投资有限公司	岳政

	上海毓盛投资管理有限公司	杨潇
	上海站观资产管理有限公司	朱戈宇
	上海加盛投资管理有限公司	陈科
	上海嘉世私募基金管理有限公司	李其东
	上海聚劲投资有限公司	张怀安
	上海联视投资管理有限公司	周申力
	上海润桂投资管理有限公司	金勇
	上海雅策投资管理有限公司	杨馥魁
	上海匀升投资管理有限公司	饶欣莹
	上海肇万资产管理有限公司	崔磊
	申万宏源证券有限公司	项敬康
	申万宏源证券有限公司	邓湘伟
	申万宏源证券有限公司	杨俊杰
	深圳丞毅投资有限公司	胡亚男
	深圳大成惠中基金管理有限公司	黄春林
	深圳前海珞珈方圆资产管理有限公司	侯海峰
	深圳前海旭鑫资产管理有限公司	李凌飞
	深圳市红方资产管理有限公司	谢登科
	深圳中天汇富基金管理有限公司	古道和
	苏州元禾重元基金管理有限公司	李喆
	泰山财产保险股份有限公司	张东华
	泰信基金管理有限公司	沈怡
	西部证券股份有限公司	周成
	溪牛投资管理(北京)有限公司	王法
	湘财证券股份有限公司	李杰
	信达证券股份有限公司	姜佳明
	信达证券股份有限公司	庞倩倩
	兴业证券股份有限公司	桂杨
	易米基金管理有限公司	赵拉
	甬兴证券有限公司	黄伯乐
	粤佛私募基金管理(武汉)有限公司	曹志平
	招商证券股份有限公司	鲍淑娴
	浙江壁虎投资管理有限公司	张小东
	中国国际金融股份有限公司	李铭娟
	中国国际金融股份有限公司	韩蕊
	中泰证券股份有限公司	余月琴
	中信证券股份有限公司	潘儒琛
	中邮证券有限责任公司	王思
	中邮资本管理有限公司	仇振洋
	珠海德若私募基金管理有限公司	罗采奕
日期	2025年8月29日	