

物理 AI 与网络安全进入新阶段 20261026

AI 安全需求确定性增强，物理 AI 数据缺口驱动 500 亿增量市场

摘要

- AI 赋能使漏洞挖掘与攻击门槛降低，驱动网络安全从“强预期”向“强现实”转型，深信服等具备云安融合能力的厂商受益于 B 端渗透率提升。
- 物理 AI 进入爆发期，英伟达、OpenAI 及特斯拉加速软硬件渗透；通用大模型如 ChatGPT-6 Astra 在机器人仿真任务中成功率已升至 58.17%。
- 高质量真机数据成为物理 AI 核心瓶颈，行业可用数据仅 50 万小时，距 GPT-3 级别通用水平存在 200 倍以上缺口，对应市场空间超 500 亿元。
- 物理 AI 数据具备产权明确、敏感度低、流转顺畅等优势，相较传统公共数据更易商业化落地，是数据要素政策体系率先兑现的领域。
- 国家数据集团成立提供产业统筹抓手，与物理 AI 数据需求形成共振，推动数据采集设备与服务环节进入确定性投资区间。
- 重点关注海天瑞声（具身智能数据业务从 0 到 1）、深信服（Q2 财报新高，云业务与安全双驱动）及首程控股、能科股份等先行布局者。

Q&A

在 AI 时代，网络安全行业呈现出哪些新的发展阶段和特征？特别是，AI 技术如何影响漏洞的挖掘与攻防格局，以及国内外市场表现有何差异？

在 AI 时代，网络安全行业已进入一个新的发展阶段。AI 能力的增强显著提升了模型挖掘漏洞的效率，例如近期利用 AI 辅助分析内存情况发现了一个长期的 PHP 漏洞。这意味着 AI 不仅能高效挖掘漏洞，也能自动进行更新和攻击，使得漏洞的利用和挖掘过程同步变得更为简单。从攻防视角看，攻击的门槛降低，使得防守的重要性进一步凸显。市场表现方面，国内外存在差异。北美市场呈现“强预期、强现实”的状态，其网络安全板块作为业绩增速最快的软件板块，IG 指数在 2026 年内创下新高。这主要得益于北美 B 端软件渗透率较高，企业采购 AI 相关安全产品的进度更快。相比之下，国内市场目前处于“强预期、弱现实”阶段。国内网络安全上市公司的客户以政企为主，其采购行为具有较强的预算性和业务进度匹配性。但随着国内 B 端 AI 软件渗透率和使用率的

提升，配套的 AI 安全产品需求预计将随之增加，市场有望从“强预期、弱现实”转向“强预期、强现实”。从历史复盘来看，网络安全板块通常以 EBITDA 的形式存在。过去五年，该板块没有新的上市公司，且单产品价格承压的影响已接近底部。2026 年部分公司已恢复增长，盈利性也有所恢复。在 AI 需求上升的背景下，无论是 AI 赋能传统安全还是 AI 安全本身，其后续需求的确定性都相对较高。考虑到板块的贝塔属性以及各公司覆盖领域和产品的相似性，整个网络安全板块值得重点关注。

AI 与网络安全的结合具体体现在哪些方面？深信服作为推荐标的，其业务结构和增长逻辑是怎样的？

AI 与网络安全的结合主要体现在两个层面。第一是“AI 赋能传统安全”，即利用 AI 提升传统安全产品的效率和能力。例如，在漏洞挖掘和威胁识别过程中，AI 能带来更高的效率和识别准确性；在 XDR 产品中，AI XDR 能够显著提升效率并扩展防御和搜索的范围。第二是“AI 安全”，这部分是伴随企业内部 AI 应用而生的新需求。随着企业内部 Agent 使用频率增高，相关的安全产品需求也会持续增长，具体包括 Agent 的权限管理、全生命周期管理、模型 Skills 检查以及模型本身的安全负荷等。海外如 OpenAI 也已提出对 AI 整体执行环境的安全需求，表明 AI 安全是整个 AI 产业长远发展的基石，它能让 AI 的应用范围和时长更具确定性和可靠性。深信服的核心业务包括网络安全和以超融合为代表的云业务。其增长逻辑在于，随着企业尤其是中小企业对私有云需求的增加，对网络安全和算力的支持需求也同步上升。深信服的产品能够同时满足这两方面需求，因此采购需求度预计会持续上升。从财务数据看，公司在 2026 年第二季度的财报已创历史新高，其云业务的增速和网络安全业务的恢复预计将延续 Q2 的良好态势。

近期物理 AI 领域进入新阶段的主要催化因素有哪些？通用大模型在该领域的进展如何？

近期物理 AI 领域进入新阶段，主要由多层次因素催化。首先，通用大模型正加速向物理 AI 领域衍生。以 ChatGPT-6 Astra 模型为例，其在物理 AI 领域的进展显著。根据 9 月发布的 RoboDog 官方评测，Astra 在 42 项机器人仿真任务中完成了 2,100 次实验，平均成功率为 22.48%，得分 28.97 分，已超过报告中收录的 4 个机器人公开策略。尽管当时数据不算特别亮眼，在精细动作方面仍有卡点，但 10 月份披露的两套新方案——Hexa-shell 和 WorkScapes，极大地提升了 Astra 的能力。Hexa-shell 方案通过将任务决策、几何测量、轨迹生成等与可迭代的代码工具结合，让 Astra 专注于其擅长的部分；WorkScapes 方案则强调通过执行反馈进行自我迭代和更新，强化规划与执行的协同。这两套方案在 RoboDog-9 仿真评测中的进度分别达到了 58.17% 和 46.58%，实现了重大进展。此外，10 月 22 日，宇树科技展示了使用 ChatGPT-6 完成绘画、换颜料、洗笔、围棋等操作，整个过程未使用专门的物理 AI 数据进行专项训练，也未单独编写程序。尽管过程中存在传感误差，但这恰恰证明了高质量、高精度的物

理 AI 数据目前仍然是行业发展的堵点。同时，10 月 24 日发布的 Kimi 3.1 Pro 在百川的评测中也取得了接近 Astra 的成绩。市场正在寻找继 AI for Coding 之后的下一个重要方向，物理 AI 因其在场景规模化落地后对算力有巨大需求，被认为是潜力极高的领域，这也是市场形成共识的基础。

除了通用大模型的进展，还有哪些科技巨头的布局推动了物理 AI 进入新阶段？

除了通用大模型的技术突破，头部科技巨头在机器人本体及相关生态的布局也是推动物理 AI 进入新阶段的关键催化剂。具体体现在以下几个方面：首先，OpenAI 于 10 月 19 日官方宣布招聘 19 个与机器人相关的岗位，涵盖控制系统、电气工程、执行器、电机设计、制造及数据系统等领域，这标志着其战略从软件向硬件延伸。其次，英伟达在 10 月 20 日至 22 日于柏林举行的 GTC 大会上，将物理 AI 列为业务发展主线，这是驱动本轮行情的一個关键事件。10 月 21 日，英伟达进一步发布了 Cosmos 世界基础模型、人形机器人模型以及覆盖采集、仿真、运行的全套技术栈，并推出了基于 Groot 的最新款参考人形机器人。此外，特斯拉也强调了后续将实现批量级的、高质量的具身智能机器人出库。这些头部企业的动向共同表明，物理 AI 产业链正进入一个新的发展阶段。

如何看待当前物理 AI 产业的整体发展趋势，特别是从模型、算力和本体等不同参与方的角度来看？

当前物理 AI 产业呈现出几个显著趋势。首先，以英伟达为代表的头部公司正在从其具备优势的世界模型和算力领域，向机器人本体或硬件方面进行考量与布局，这一点在其最新的 GTC 大会上发布的机器人产品中有所体现。其次，通用大模型公司和芯片公司也在加速向机器人本体侧延伸，形成了模型、算力与本体之间的相互渗透。例如，模型公司开始布局机器人本体，而本体公司则在自研世界 AI 模型和构建超大规模算力集群。最后，头部厂商已进入产能建设期，例如特斯拉已启动早期量产，并计划在未来一年左右达到每周 2 万台的设计节奏；同时，宇树科技也提出正在持续提升大规模产能，以适配千万级乃至亿级的市场需求，并自建物理 AI 模型和超大规模算力集群。

物理 AI 发展当前面临的关键瓶颈是什么？从数据供需角度看，这个瓶颈的具体表现和市场规模如何？

当前物理 AI 发展最关键的瓶颈在于高质量、有效性的数据。从需求侧看，尽管通用模型在向物理 AI 大脑的训练中取得了进展，但在触觉、高精度轨迹和时序等方面仍存在难点，需要大量高精度数据来弥补。行业共识认为，要使具身智能机器人达到可用阶段，至少需要 1,000 万小时的真机数据；若要达到 GPT-3 级别的通用水平，则需要 1 亿甚至数亿小时的真机数据。以每小时 500 元人民币的中间价格估算，达到 GPT-3 水平所需的数据市场空间将超过 500 亿元人民币，并且随着新场景的挖掘，这一空间还会持续扩大。从供给侧看，目前行业

内真正高质量的有效真机数据可能仅有约 50 万小时，与 1,000 万小时的目标相比存在 20 倍的缺口，与 GPT-3 级别的需求差距则更大。这种巨大的供需缺口使得数据环节成为物理 AI 产业中确定性最高、而非主题性的投资领域。

针对物理 AI 的数据瓶颈，目前行业内有哪些解决方案及其发展现状？

行业内主要有三种解决方案来应对数据瓶颈。第一种是真机数据采集，主要通过机器人本体获取，这涉及数据服务公司与本体公司之间的商业合作，合作模式包括本体的购买、租用等多种形式并行。然而，真机数据采集存在成本高、效率低的问题。第二种是异构与众包模式，这被认为是一种较为理想化的解决方案，旨在通过多样化的设备和众包方式来扩充数据来源。目前，多数布局数据业务的公司在提供数据服务的同时，也在部署相关的异构采集设备。第三种是仿真与合成数据，得益于大模型（如 Sora、Kimi 3.0 Pro 等）的快速发展，这一领域进展显著，被认为是中长期的主流趋势。不过，在当前节点，仿真合成数据在产业中的实际应用占比较少。因此，现阶段能够解决燃眉之急的最佳方案组合是真机数据与异构众包数据的结合。

国家数据集团的成立对数据要素市场有何重要意义？它与物理 AI 数据的发展之间存在怎样的关联？

国家数据集团的成立是中国数据要素发展历程中的一个重要里程碑。此前，地方虽成立了众多数据集团，但规格、任务各不相同，国家层面缺乏统一的产业抓手。国家数据局虽在政策层面发挥作用，但在产业统筹上需要一个实体抓手，国家数据集团便扮演了这一角色。其强大的股东背景（包括国资委、河北国资委、三大运营商和两网）和可观的注册资本，预示其未来将在推动数据要素市场发展中发挥核心作用。国家数据集团的成立与物理 AI 数据的发展形成了强烈的共振。传统数据要素市场的发展，尤其在公共数据和企业数据领域，长期受制于数据价值与隐私性的高度挂钩、产权归属不明确以及数据敏感性高等问题，导致商业化进展缓慢。相比之下，物理 AI 数据具有产权明确（采集方所有）、敏感性低（不涉及个人隐私或商业机密）、流转顺畅等特点。因此，过去几年国家在数据要素领域构建的政策体系、标准规范以及数据空间等基础设施，其早期愿景很有可能在物理 AI 数据这个更易于商业化的领域率先实现和落地。

在物理 AI 数据这一关键环节，有哪些值得关注的投资方向和相关公司？

在物理 AI 数据环节，值得关注的投资方向主要包括数据采集设备和数据服务两大类。在这一领域，海天瑞声是重点关注的公司之一。该公司从 2025 年开始布局具身智能数据业务，经历了从 0 到 1 的发展阶段，包括成立子公司、获取订单等，并与国家数据集团在数据标注基地、高质量数据等方面保持着合作。除了海天瑞声，其他在物理 AI 领域布局较早的公司也值得关注，例如首程控股、

能科股份以及汇程科技。