紧跟热点前沿赋能本地发展

数据集团多举措助力AI场景应用与创新

> 今年春节以来，一股来自东方的“神秘力量”——国产AI大模型DeepSeek，以其强大的智能交互能力迅速风靡全球。其背后的DeepSeek-R1模型凭借卓越的性能和创新性，展现了中国人工智能技术的巨大潜力，引发全球AI领域关注。全民AI的时代要来了！

多平台迅速接入DeepSeek模型能力

作为国产开源大模型DeepSeek“朋友圈”的一员，数据集团凭借在人工智能产业建设方面的积淀和准备，联合太初元碁、燧原科技等无锡本地具有显著竞争优势的国产算力合作伙伴完成DeepSeek-R1系列模型的适配工作，于无锡“算力超市”（无锡算力公共服务平台）快速上线包括DeepSeek-R1-671B在内的多款大模型服务，实现“锡产锡用”。

由新基建公司建设运营的无锡“算力超市”还特别开放DeepSeek技术服务入口，为企业提供覆盖前后端、数据库、运维等全栈技术解决方案，推动DeepSeek全栈技术能力输出，助力无锡本土企业创新与应用开发，赋能城市数字化发展。

“灵锡”App作为政务与城市服务的移动端总入口，在中国电信的技术支持下，迅速上线了DeepSeek大模型，为用户提供更智能的服务体验。

锡企服务平台也同步接入DeepSeek模型能力，借助大模型的语义识别和逻辑推理能力，打造企业服务AI助手，为锡企提供专属智能管家，为企业带来更高效、更便捷、更贴心的体验。

由锡数交开发运营的服务全市个体工商户的小程序“锡小服”也已上线DeepSeek大模型，完成本地化部署和调用。“锡小服”部署的DeepSeek-R1-Distill-Qwen-14B模型，使用包含《中华人民共和国民法典》《中华人民共和国市场主体登记管理条例》《中华人民共和国劳动法》《中华人民共和国个人独资企业法》《中华人民共和国食品安全法》等多部法律条文语料训练，基本涵盖个体工商户生产经营所依赖的法律法规内容。个体工商户和小微企业可以在“锡小服AI”模块中免费体验使用。

推出一体化训练推理资源

为高效服务不同场景需求，在上线DeepSeek大模型后，无锡“算力超市”很快又推出了针对DeepSeek的一体化训练推理资源池，为DeepSeek快速赋能无锡人工智能产业发展筑牢坚实算力底座。

一体化训练推理资源池聚焦无锡本市政府侧及企业端DeepSeek部署及微调需求，依托运营商、无锡尚航、宏芯港湾、摩尔线程、燧原科技等生态合作伙伴，通过对全市闲散算力资源进行梳理、归集高性能算卡及国产算卡资源，旨在满足包括训练、推理、数据分析等不同类型的算力需求，为企业提供高效、便捷、低成本的算力服务，提高企业的市场竞争力。

在一体化训练推理资源池高性能算力资源的助力下，市城运中心实现全省首个政务信创环境下DeepSeek R1 671B全尺寸模型部署，通过融合通用大模型的泛化能力与政务数据集专精优势，为“城市大脑”注入更强大的AI动能。目前，“小城”“小运”也已于政务服务大厅正式上岗，基于DeepSeek的深度学习框架，它们的咨询响应准确率、问题解决率都将有明显提升，极大改变传统智能客服“不解人意”“答非所问”等难题。

推出AI原生安全解决方案

数据集团下属锡数安联合启明星辰，正式携手DeepSeek大模型，推出面向AI原生的安全解决方案——面向AI原生安全的大模型应用安全“新三件套”，开启智能化安全防护的新篇章。

大模型应用安全“新三件套”包括MAF大模型应用防火墙、MASB大模型访问安全代理、MAVAS大模型安全评估系统，面向使用大模型的用户，保障大模型本身的安全性。

MAF（大模型应用防火墙，Model Application Firewall）产品承继了WAF产品的基本形态，针对DeepSeek大模型和其他语言大模型所面临的特有威胁进行专项防护，主要针对大模型的越狱、提示词注入攻击防护、大模型软件供应链漏洞防护、应用层DDos拒绝服务攻击缓解、不安全输出过滤、敏感信息防泄露等进行防护。基于MAF外挂式防护来降低大模型自身的安全训练成本，更灵活规避大模型上的安全风险。

MASB（大模型访问安全代理，Model Access Security Broker）是聚焦在大模型企业级场景下用户交互访问场景下数据防泄露、权限管控、合法合规安全需求。MASB解决了大模型使用过程中防数据泄露、企业AI访问权限管控问题。

MAVAS（大模型安全评估系统Model Application Vulnerability Assessment System），接入DeepSeek通过“以大模型对抗大模型”的创新方式，通过识别并防范模型在伦理、价值观及对抗攻击方面的潜在风险，帮助用户实现合规运营、规避内容失控风险，保障生成内容的安全性。

除了推出了针对大模型本身的防护方案，锡数安还利用DeepSeek对传统安全产品进行了史诗级加强，推出全智能安全运营模式、高级威胁检测分析响应系统等多款AI安全产品，并同步升级了安全服务能力。