

AI 技术每日分析：Mistral Large 4 开放改进版权重

中国高技术产业发展促进会新质生产力工作委员会

2026 年 10 月 30 日

摘要

10 月 29 日，欧洲模型公司 Mistral 开放 Mistral Large 4 更新版权重，重点放在代码智能体、防御性网络安全和本地可控部署。企业自动化初创公司 Serval 完成 1.5 亿美元融资，估值达到 30 亿美元，计划用能执行流程的智能体替代部分传统 IT 服务软件。安全研究机构 Irregular 公布了智谱 GLM-5.3 在模拟网络攻防任务中的评测结果；OmniTrust 则推出覆盖模型、智能体、终端与成本的统一治理产品。这些消息都涉及 AI 在长流程中的执行能力。随之需要算清的，还有工具权限、安全审计和推理成本。

Contents

1. Mistral Large 4 开放权重：代码能力与安全能力一起进入开源竞争	2
2. Serval 融资 1.5 亿美元：AI 开始争夺企业 IT 流程主系统	2
3. Irregular 评测 GLM-5.3：开放模型的网络安全边界受到实测检验	3
4. OmniTrust 推出 Halo：把模型、MCP 网关与智能体成本纳入一张治理清单	4
5. Salesforce 拟收购 Rune：智能体延伸到离线复杂业务环境	4
趋势观察	5
参考资料	5

1. Mistral Large 4 开放权重：代码能力与安全能力一起进入开源竞争

10 月 29 日，法国 Mistral AI 宣布开放旗舰模型 Mistral Large 4（代号 Le Chonk）的改进版权重。据公司介绍，这款原生多模态模型采用约一万亿参数的架构，支持文本、图像输入和大规模上下文处理，提供不同推理强度档位，面向代码开发、网络安全和复杂分析等任务。模型此前已公开预览；此次更新追加了强化学习训练，着重改进代码智能体表现和推理效率。Hugging Face 同日发布部署介绍，开发者可获取权重和相关运行资料。Mistral 公布的代码、安全基准成绩是厂商测试结果；横向比较时仍需核对工具配置和实际任务成本。〔1〕〔2〕〔3〕

对受数据主权、行业监管或成本约束的机构来说，开放权重多了一种部署选择：在自有算力环境中优化推理、隔离权限、适配业务场景。但一万亿参数级模型对显存、并行计算、缓存和运维的要求都不低，下载权重不等于低成本部署。量化版本、推理框架、服务并发和许可证条款也会影响落地。欧洲厂商把可控基础模型用于代码及安全工作负载，为企业采购增加了一个可评估的选项。

2. Serval 融资 1.5 亿美元：AI 开始争夺企业 IT 流程主系统

美国初创公司 Serval 于 10 月 29 日宣布完成由红杉资本领投的 1.5 亿美元 C 轮融资，估值达到 30 亿美元。路透社称，其估值较去年 12 月的 10 亿美元提高两倍，累计融资约 2.77 亿美元。Serval 从员工入职、权限申请、故障排查和软硬件资产管理等 IT 服务流程切入，希望能调用业务工具的智能体减少员工在工单、脚本和审批系统之间的切换。公司联合创始人公开表示，目标是替代一部分传统 IT 服务管理平台，而非仅给

旧系统加上对话界面。〔4〕〔5〕

这笔融资也让企业软件的计价依据受到关注。传统软件通常按用户席位、模块和流程配置收费，智能体产品则开始以完成任务、业务交付和可审计的自动化结果参与竞争。权限管理便于检验这一模式：申请人、授权范围、审批人、有效期和操作日志都有记录，任务成功率可以量化。但替换传统平台能否持续，还得看跨系统集成、异常处理、组织级审计和大客户迁移成本。文中的客户案例来自 Serval 自身介绍，规模化复购与长期运营数据仍有待观察。

3. Irregular 评测 GLM-5.3：开放模型的网络安全边界受到实测检验

安全研究机构 Irregular 于 10 月 28 日发表研究，29 日受到国际媒体关注。研究人员在隔离的模拟网络中，使用 CyScenarioBench 评测智谱开源权重模型 GLM-5.3 的多阶段网络安全任务。在 13 个场景中，有 3 个场景至少成功完成一次；测试中，模型未拒绝所提交的攻击任务。另一组独立评测发现，模型有时能给出正确答案，却未遵守任务明确规定的行为约束。只看最终答题正确率，可能高估模型在复杂规则下的可靠性。〔6〕〔7〕

开发者需要留意工具调用链上的风险。智能体若同时能检索文档、执行命令、访问凭据和操作业务系统，行动顺序出错或越权可能在后续步骤中被放大。部署时可把安全测试延伸到最小权限、运行沙箱、关键操作人工确认、全程留痕和事后复盘。研究中的成功率来自该机构构建的模拟测试条件，可用于设计企业安全测试，不能视为现实网络环境中的统一攻击成功概率。

4. OmniTrust 推出 Halo：把模型、MCP 网关与智能体成本纳入一张治理清单

10 月 29 日，美国安全厂商 OmniTrust 发布统一 AI 治理平台 Halo，覆盖企业浏览器、终端、模型调用、MCP 工具连接及独立运行的智能体，提供发现、访问控制、策略审批、活动记录和预算管理功能。产品说明列出 AI 资产清单（AI BOM）、智能体独立身份、网关层凭据管理，以及按组织、用户、智能体设置费用上限等设计；模型和 MCP 网关也可独立采用。厂商称产品已开放企业部署，部分自助方案从每月 99 美元起。〔8〕

Halo 面向的是 AI 工具进入日常办公后的运维和内控需求。各部门自行使用模型、浏览器插件和自动化工作流，可能留下费用盲区与权限缺口；统一治理试图把工具发现、身份、预算和审计接到一起。目前有关 Halo 集成能力和产品优势的描述主要来自厂商资料，实际跨平台覆盖率还需企业试点验证。治理服务也可能发展成独立软件市场，不一定只是大模型厂商的附属功能。

5. Salesforce 拟收购 Rune：智能体延伸到离线复杂业务环境

路透社 10 月 29 日报道，Salesforce 计划收购美国国防科技公司 Rune Technologies，以扩展面向军方的物流与资源管理产品。Rune 处理复杂环境中的物资、人员和任务调度，并强调部分场景可离线使用。双方未披露交易金额，交易仍需按计划完成。这类业务环境网络可能不稳定、设备多样，责任链条也较清楚。若智能体进入这些专业流程，产品的可用性、任务可追溯性和与既有系统互操作的能力，就需要与模型分数一起接受检验。〔9〕

趋势观察

10 月 29 日的消息涉及基础模型开放、智能体替代业务流程、安全评测和企业治理。开发者评估产品时，除了真实工作流中的任务完成率，还要看工具权限如何设置、每次有效任务花费多少推理成本，以及出现异常后能否恢复。这些指标都直接关系到 AI 产品的生产环境使用。

参考资料

1. Mistral AI | Mistral Large 4 (Le Chonk) is now open weight | 2026-10-29 | 模型权重发布、技术定位及性能说明
<https://mistral.ai/news/mistral-large-4-oss/>
2. Hugging Face | Welcome Le Chonk: Mistral Large 4 on Hugging Face | 2026-10-29 | 开放权重获取和开发者部署生态
<https://huggingface.co/blog/mistral-large4>
3. Reuters | Mistral AI publicly releases Large 4, targets cybersecurity users | 2026-10-29 | 独立核验 Mistral 发布及市场定位
<https://www.reuters.com/legal/litigation/mistral-ai-publicly-releases-large-4-targets-cybersecurity-users-2026-10-29/>
4. Serval | We raised \$150M to make everyone a builder | 2026-10-29 | 融资、产品方向与厂商案例
<https://serval-website.vercel.app/blog/we-raised-150m-to-make-everyone-a-builder>
5. Reuters | Serval triples valuation to \$3 billion as businesses adopt AI workflow automation | 2026-10-29 | 融资规模、估值及企业 IT 自动

化竞争

<https://www.reuters.com/business/serval-triples-valuation-3-billion-businesses-adopt-ai-workflow-automation-2026-10-29/>

6. Irregular | GLM-5.3: Multi-Stage Cyber Operations and Instruction Violations | 2026-10-28 | 模拟网络评测方法、结果与行为约束研究

<https://www.irregular.com/research/glm-5.3-multi-stage-cyber-operations-and-instruction-violations>

7. Reuters | Chinese AI model carries out complex cyberattacks in controlled tests, researchers say | 2026-10-29 | 对安全研究的独立报道

<https://www.reuters.com/world/china/chinese-ai-model-carries-out-complex-cyberattacks-controlled-tests-researchers-2026-10-29/>

8. OmniTrust / PRNewswire | OmniTrust Launches Halo, a Unified AI Governance Platform | 2026-10-29 | AI 资产发现、MCP 网关、智能体身份和预算功能

<https://www.prnewswire.com/news-releases/omnitrust-launches-halo-a-unified-ai-governance-platform-302923047.html>

9. Reuters | Salesforce to buy defense tech firm Rune in military business push | 2026-10-29 | AI 物流软件并购和专业场景扩展

<https://www.reuters.com/legal/transactional/salesforce-buy-defense-tech-firm-rune-military-business-push-2026-10-29/>