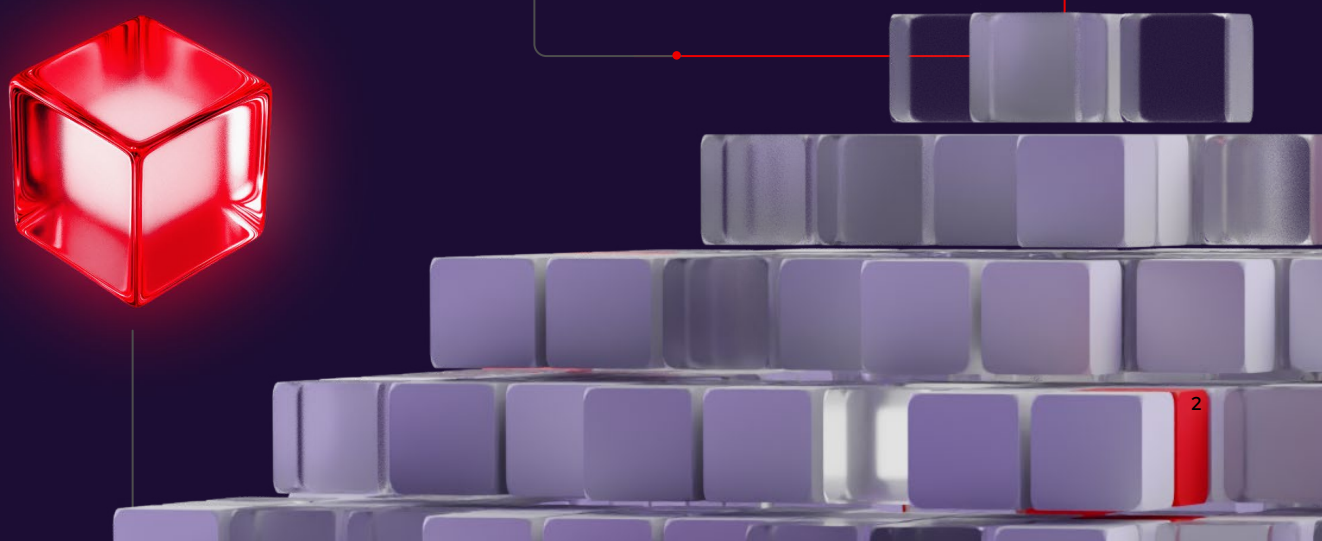
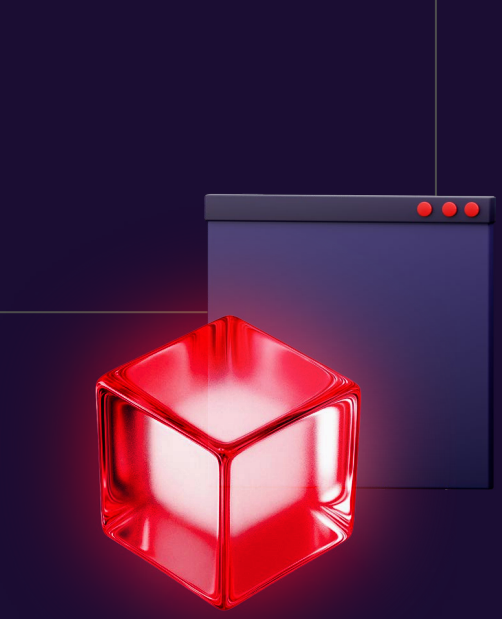
释放代理式 AI 的力量

关于 AI 下一阶段演进的高管指南

Red Hat

目录





简介

代理式 AI 带来的机遇

如今，高管们正处于技术演进的关键时刻。尽管 AI 已重新定义我们与数据交互、实现任务自动化以及服务客户的方式，但 AI 的下一阶段发展已悄然来临，其应用场景正突破内容生成与预测性分析的范畴。

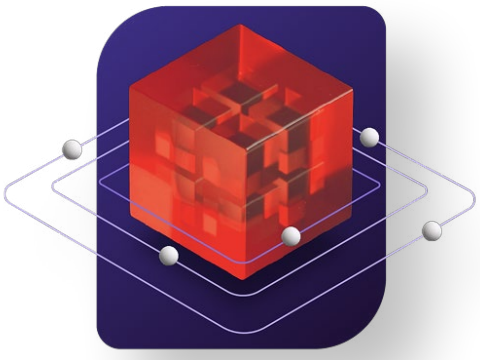
代理式 AI 是从生成式模型演进而来的自主系统，具备更强的适应性和持续学习能力。代理式 AI 可以是一种物理结构、一个软件程序，或二者的结合体。这使得代理能够在几乎所有业务环节中，于预定义参数范围内进行感知、决策和行动。不同于响应提示的模式，代理式 AI 可主动发起多步骤任务、访问工具和应用编程接口（API），并随着时间的推移不断改进。其应用场景包括跨多个平台处理客户服务问题、自动执行 IT 修复步骤，或实时管理供应链运营。

对于高层领导者而言，洞悉这一变革趋势是在未来保持竞争力的战略要务。

代理式 AI 的工作原理

代理式 AI 对于需要持续监控或快速决策的任务最为有用。您可以将其视作自动化与大语言模型（LLM）的推理、决策和创造能力相结合的产物。要将代理式 AI 应用于日常运维，企业组织必须首先创建一个系统，使 LLM 能够调用外部工具和算法，以此为依托于其他软件工具并对其进行操控的 AI 代理提供指令。

随后，AI 代理可以根据所采用的框架，与工作流编排工具进行交互。这种模式能够支持 LLM 进行推理，进而确定解答问题的最佳方式。



到 2029 年，代理式 AI 将可在无需人工干预的情况下，自主解决 80% 的常见客户服务问题，从而使运维成本降低 30%。[1]

代理式 AI 的优势包括：

提高运维效率：通过自主工作流减少对人工干预的需求。

降低成本：最大限度地减少人工干预并提高生产力。

加速决策制定和执行：凭借实时数据和情境洞察，推动各业务部门快速决策与高效执行。

打造差异化竞争优势：助力企业组织编排和监管 AI 代理，以提高投资回报率（ROI）。

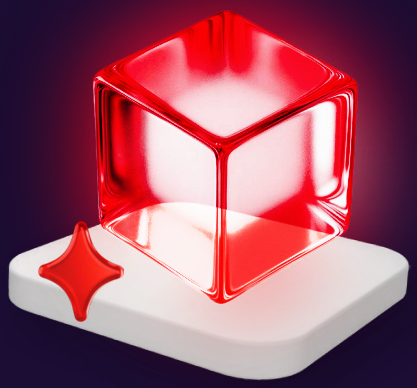
在这个持续变革的时代，代理式 AI 可助力企业组织预判趋势、灵活应变并引领发展。

采用方面的挑战

从编排复杂的代理工作流，到维持信任和可靠性，再到在整个企业内高效推广这些创新成果，将代理式 AI 融入企业组织必将面临诸多挑战。然而，随着商业环境以前所未有的速度演变，对于志在保持竞争优势的企业组织而言，采用代理式 AI 已不再是可有可无的选择。

本电子书将深入探讨这些挑战及其应对方案，解析代理式 AI 带来的业务优势，并提供切实可行的战略，助力企业组织运用代理式 AI 提高效率和促进创新。

[1] Gartner，“Gartner Predicts Agentic AI Will Autonomously Resolve 80% of Common Customer Service Issues Without Human Intervention by 2029”（Gartner 预测，到 2029 年，代理式 AI 将可在无需人工干预的情况下自主解决 80% 的常见客户服务问题）。2025 年 3 月 5 日。



第 1 章

企业面临的代理式 AI 挑战

企业对 AI 的认知与运用正迅速拓展，随着这一进程的推进，其发展成熟度也日益提升，越来越多的企业组织开始意识到 AI 所带来的深远商业价值。

事实上，随着对 AI 的投资持续增加，依托 AI 的工作流（其中许多由代理式 AI 提供支持）预计将从 2024 年的 3% 攀升至 2026 年的 25%。[2]

然而，转型之路绝非坦途。任何企业组织要想大规模且自信地部署智能代理，都必须攻克诸多切实存在的挑战。

尽早洞悉这些挑战有助于领导者提出精准问题，高效设计试点项目，并选择有助于取得成功的技术。

挑战 1：编排复杂的代理工作流

相较于生成式 AI 等其他形式的 AI，代理式 AI 系统的一个关键区别在于，它并非单点解决方案。

AI 系统可以理解各类工具、API、通信协议、数据源、机器学习（ML）模型、LLM 和 AI 代理。虽然 AI 代理承担最终决策职能，但这需要对其他各组成部分进行统筹编排。

[2] “From AI projects to profits: How agentic AI can sustain financial returns”（从 AI 项目到盈利变现：代理式 AI 如何实现可持续财务回报），IBM，2025 年 6 月 9 日。

这种级别的编排带来了新的复杂性，包括需要：

跨系统管理

代理式 AI 必须管理不同系统间的依赖关系，而这些系统往往具有不同的协议、安全模型和性能参数。

跨代理协调

必须谨慎同步多代理协作，以避免出现重复或相互冲突的操作。

为团队提供合适的工具

开发人员和 IT 团队需要新的工具来快速设计、测试和迭代这些工作流，以免每次都从头开始构建。

若缺乏统一的框架及将代理式 AI 融入现有工作流的战略，这项技术将可能沦为看似不断扩张的数字工具箱中又一普通工具。

挑战 2：确保可信度与代理行为可靠性

企业组织若要放心地允许代理自主行动，必须先建立信任。与自动化等只需极少人工干预、结果可预测且已预先设定的技术不同，AI 代理涉及动态推理与决策。核心区别在于，代理可以模仿人类行为自主做出决策，而这也引发了人们对可靠性、透明度及合规性的合理担忧。

需要考虑的关键问题：

如何实时监控和管理代理行为？

能否确保代理始终遵循业务策略和监管要求？

已建立哪些问责机制，用以管理和解释代理的决策？

可观测性、监督机制以及恰当的防护措施，都是让各利益相关者采纳代理式 AI 所需满足的技术要求。

挑战 3：高效扩展代理式 AI 应用

即便是效果极佳的试点项目，也可能在规模化推广阶段遭遇失败。代理式 AI 的实施，尤其是由 LLM 提供支持的场景，需要大量的计算资源作为支撑。试想当数十乃至数百个代理同时运行时，IT 基础架构将承受何等巨大的压力。每个代理可能都在同步查询模型、访问数据并调用工具。

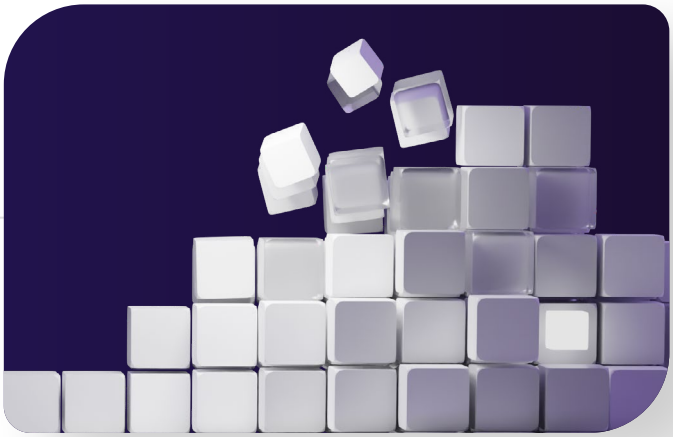
为了以可持续的方式扩展代理式 AI，企业组织必须确保：

其基础架构能够有效地扩展或缩减，并且已建立完善的成本管控方法。

能够灵活部署于混合云与多云环境，并且更贴近数据源或应用。

监管机制、安全防护和性能表现均保持一致。

采用平台方法可以应对这些挑战，助力企业组织在创新与运维最佳实践之间取得平衡。

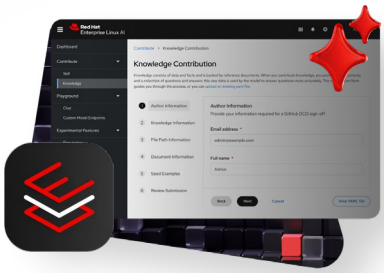


第 2 章

以开放平台策略助力成功实施代理

要充分利用代理式工作流，有赖于可靠的基础架构、运维可见性、安全至上的部署，以及跨环境的灵活性。而这正是平台化方法的价值所在。

红帽® AI 依托数十年来在企业级开源领域的领先积淀，专为从实验到生产级编排的智能代理式工作流提供支持。这使得企业组织能够开发、部署和维护代理式 AI 系统，包括 AI 代理。



红帽企业 Linux® AI，
适用于独立 Linux 服务器环境。

红帽 OpenShift® AI，
适用于分布式 Kubernetes 平台环境。

红帽 AI 推理服务器，
用于优化 LLM 的推理。

这些解决方案将开源技术的强大功能与领先的开源模型相结合，共同助力企业组织加快探索步伐，并让新兴工具和技术得到更广泛的普及应用。

简化代理工作流构建

代理式 AI 的成功取决于规划算法、记忆存储、工具编排以及学习反馈循环的协调运作。红帽通过提供以下优势，降低了此类堆栈的构建难度：

统一的 API 体验

通过标准化 LLM、开放代理框架和检索增强生成（RAG）管道的交互方式，企业组织可实现跨不同模型提供商和框架的互操作性。

专属 AI 体验

改进的用户体验为工程师提供了统一的环境，用于管理 AI 资产、代理和应用并进行原型设计。

生态系统支持

原生兼容领先的 LLM 框架（包括 LlamaStack），且支持兼容 OpenAI 的 API，让开发人员能够选择合适的模型架构，包括具有复杂集成开销的开放权重模型和微调模型选项。

适应性强且受管控的代理部署

随着企业组织不断增强 AI 代理的自主性，全面的监管、可观测性和可说明性变得至关重要。

红帽 AI 采取了一系列功能来应对这些挑战，助力实现负责任的部署：

上下文感知执行

模型上下文协议（MCP）支持代理访问语义相关的运维数据，并执行与意图一致的边界限制，从而提升决策的可说明性和可控性。

集成可观测性与策略执行

借助红帽监控工具和基于角色的访问控制，团队可以设定行为边界，并将决策追溯到源模型或数据。

兼容现有企业及合规性策略

该兼容性可确保代理活动在受监管的环境中遵循企业组织的安全策略要求。

红帽 AI 可助力企业构建强大且可预测的自主代理，并确保其始终符合企业目标与合规要求。

可扩展且经济高效的 AI 平台

要扩展代理式 AI，仅依赖大模型远远不够。企业组织需要搭建一个智能基础架构。该基础架构还必须能够适应不断变化的工作负载需求，实现成本与性能的平衡优化，同时持续提供支持并保持安全态势。

红帽 AI 提供的方法具备以下优势：

跨环境灵活部署

跨数据中心、云环境、集群和边缘节点运行代理。

优化的计算编排

借助红帽 AI 推理服务器降低推理成本，并通过红帽 OpenShift AI 跨云和本地资源重新平衡任务来支持智能自动扩展，从而降低总体拥有成本。

安全至上的扩展

获得对于在金融、医疗和政府等行业部署 AI 至关重要的支持、安全补丁和连续性保障。

红帽 AI 平台是一款集工具、监管与可扩展性于一体的统一平台。无论您是在为 IT 运维、客户服务，还是行业特定任务协调自主代理，红帽都能在您应用代理的各个阶段提供支持，让您自信前行，无需面对复杂难题。

第 3 章

基于红帽 AI 规划代理式 AI 战略

有了合适的基础，代理式 AI 便可以加速交付、降低成本并提高投资回报率。然而，转型并非一蹴而就；需始于一种与业务优先事项、技术就绪度及监管要求保持一致的战略方法。

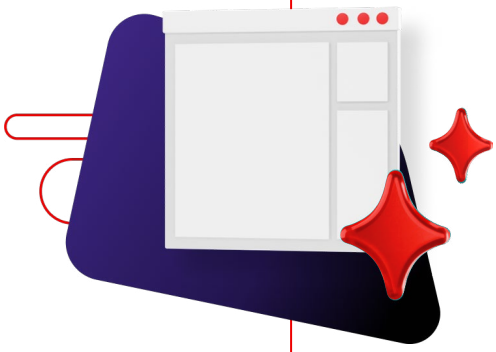
红帽 AI 旨在为企业组织在这一历程的各个阶段提供支持，涵盖从初步探索到企业级全面部署。无论您是刚刚开始评估代理式工作流，还是已经在扩展 AI 计划，周密的战略规划都将确保您的努力与投资集中在创造切实的商业价值上。

从何处着手

自主运维之路无需从全面部署开始。分阶段采用策略往往更为有效，首先关注高价值、边界清晰且能快速获得见解的用例开始。

- **客户支持工单分类与处理。**
- **自动化 IT 修复或 DevOps 事件响应。**
- **跨业务部门生成合规性报告。**
- **内部知识库检索代理。**

这些初步举措提供了一个理想的试验环境，可用于评估代理的行为表现、与利益相关者建立信任关系，并验证 IT 基础架构的性能。



如何评估企业组织的就绪度

要更深入地了解企业组织的环境状况以及采用代理的准备情况，请考虑以下方面：

1

在哪些方面，重复性或基于规则的决策拖慢了团队效率？

2

代理需要访问哪些系统、API 或数据源？

3

现有 IT 基础架构能否大规模支持基于模型的低延迟工作流？

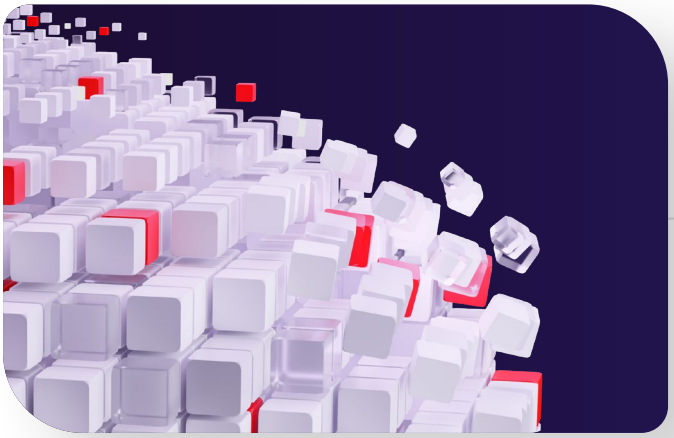
4

需要制定哪些策略和防护措施来监管自主操作？

5

如何衡量成功与否？（需综合考虑成本节约、速度提升、准确性改进及自动化错误减少等维度。）

尽管这并非一份详尽的清单，但这些问题是极佳的切入点，可助力企业组织锁定早期成果，并确保 IT、运维与业务领导者之间保持一致。



战略考量

为助力企业组织取得成功，在制定代理式 AI 策略时，请考虑以下要素：

互操作性

选择一个开放、模块化的平台，避免受限于单一模型、云服务或工具集，这将帮助您在技术演进过程中保持灵活性。

在设计阶段融入监管机制

从初始阶段就建立政策规范、监控机制与可说明性框架，以保持合规性与可信度。例如，确保符合《健康保险流通与责任法案》（HIPAA）的要求。

将 AI 融入 IT 战略

将 AI 代理视为更广泛的数字化和自动化策略的一部分，而不是孤立的实验。

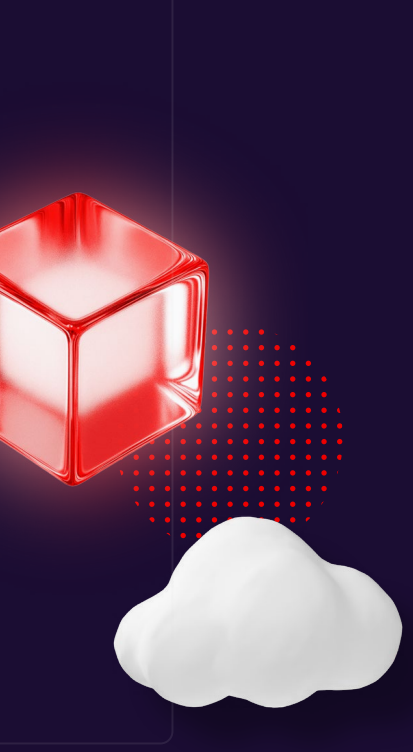
技能培养

新技术的应用需要新技能。应通过培训与激励，赋能工程、运维及业务部门的团队，使其能够高效运用智能代理。

代理式 AI 就绪度检查清单

鉴于涉及环节众多，制定一份内部检查清单以评估企业组织在代理式 AI 之旅中所处的阶段将大有裨益。

- **我们是否已确定至少一个可从自主代理中受益的业务职能？**
- **我们是否了解代理需要与哪些系统和 API 进行交互？**
- **我们的 IT 基础架构能否在满足必要监管与安全防护要求的前提下，支持模型推理工作负载？**
- **关键利益相关者是否支持我们的试点代理式工作流？**
- **我们是否制定了衡量成功和推广成熟用例的计划？**



了解更多

企业自动化的未来在于自主化

企业组织需要重新审视自动化的未来，它不仅是替代人工操作的工具，更是赋能系统自主决策、适应变化并追求持续改进的核心引擎。

代理可以承担复杂的任务，并以快速、准确和自主的方式推动业务目标的实现。

对于高管而言，这种转变标志着一种新的竞争格局。积极采用代理式 AI 的企业组织，有望实现运维敏捷性、创新能力与投资回报率的全新跃升。而且，对于这一采用过程，不必望而生畏。

红帽 AI 提供开放的混合基础，助力企业组织成功采用。从简化代理工作流到监管自主行为，再到跨环境优化基础架构，红帽可以帮助具有前瞻性的领导者以实用、可扩展且值得信赖的方式实施代理式 AI。

准备好带领您的企业组织迈入 AI 之旅的下一阶段了吗？

进一步了解红帽 AI 赋能代理式 AI，或联系红帽代表以了解更多信息。