DELL Technologies | NVIDIA

利用代理式 AI 重新定义工作、决策和创新

引领组织迈向 AI 新时代

代理式 AI 是生成式 AI 的进化形态，可为业务运营和未来工作模式带来自主性、适应性和目标驱动型智能。随着组织应对日益复杂的数字环境，能够部署按照意图执行行动、从环境中学习并持续优化流程的 AI 已成为颠覆性优势。

代理式 AI 有望赋能每位员工、优化每项流程，并为工作流带来深远影响。随着目标驱动型 AI 代理的出现，未来员工需具备调度与协同各种 AI 代理的能力，以应对多应用场景和多工作流的需求。代理式 AI 可以加快明智的决策，自动执行低风险任务和流程，并开始以令人信服的全新方式弥合人类专业知识与机器智能之间的差距。

通过制定合适的战略和规划，组织可以有效地实施代理式 AI，而不会带来不必要的风险。携手戴尔和 NVIDIA，组织将获得合适的基础架构、数据转型服务和平台，从而充分利用代理式 AI 的优势。

对 CEO 而言，代理式 AI 不仅仅代表了更高的效率，更标志着企业在竞争、运营和交付价值方面发生了根本性转变。[1]

1.Forrester Trends 报告，《Agentic AI Is Rising And Will Reforge Businesses That Embrace it》，2025 年 3 月 7 日。

将 AI 代理转化为您的竞争优势

什么是智能体式 AI?

代理式 AI 让组织有机会将大量宝贵数据、最佳实践和程序与自主智能系统相结合。传统 AI 会被动处理输入以产生固定的输出，而代理式 AI 的功能更像是一个智能协作者，可在业务环境中积极努力实现目标，而不仅仅是遵循指令。

这种协作功能使组织及其员工能够以前所未有的效率和创造力开展运营，同时确保与组织目标和期望保持一致。通过赋予推理、环境感知、学习和适应能力，代理可以在获得一个目标后独立执行复杂的任务并解决问题以实现该目标，而无需人工干预。

生成式 AI 的演变

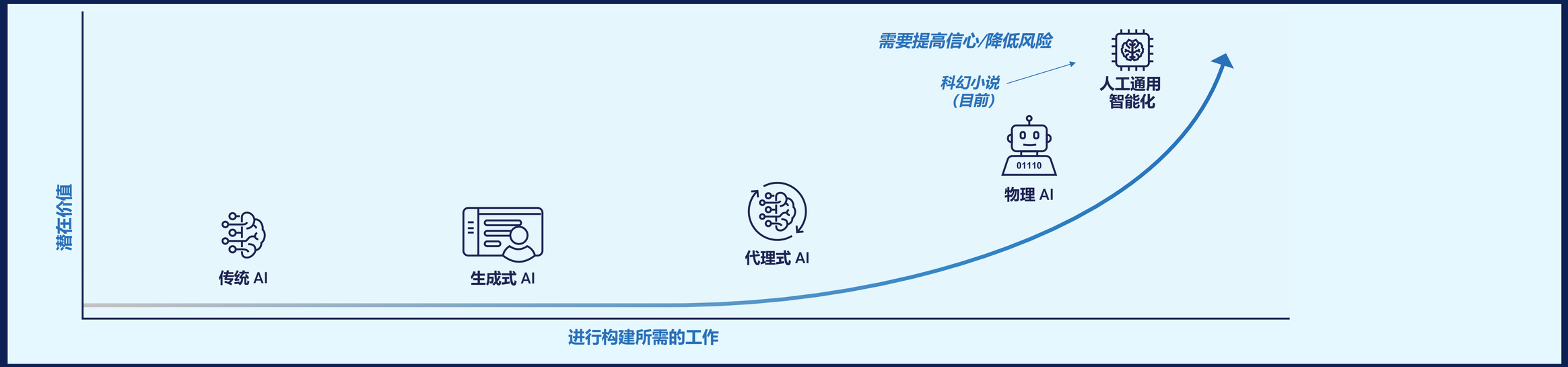
聊天机器人
通过提示词与用户交互，以回答问题或引导操作。

数字助手
在特定领域内处理专项任务问题。

代理式 AI
自主管理各种任务，并根据需求变化进行调整。

AI 层级

通过人工智能的整体发展脉络，可以更好地理解代理式 AI。随着 AI 演进至不同阶段，各阶段均赋予了新的能力。具体演进路径如以下类别所示：



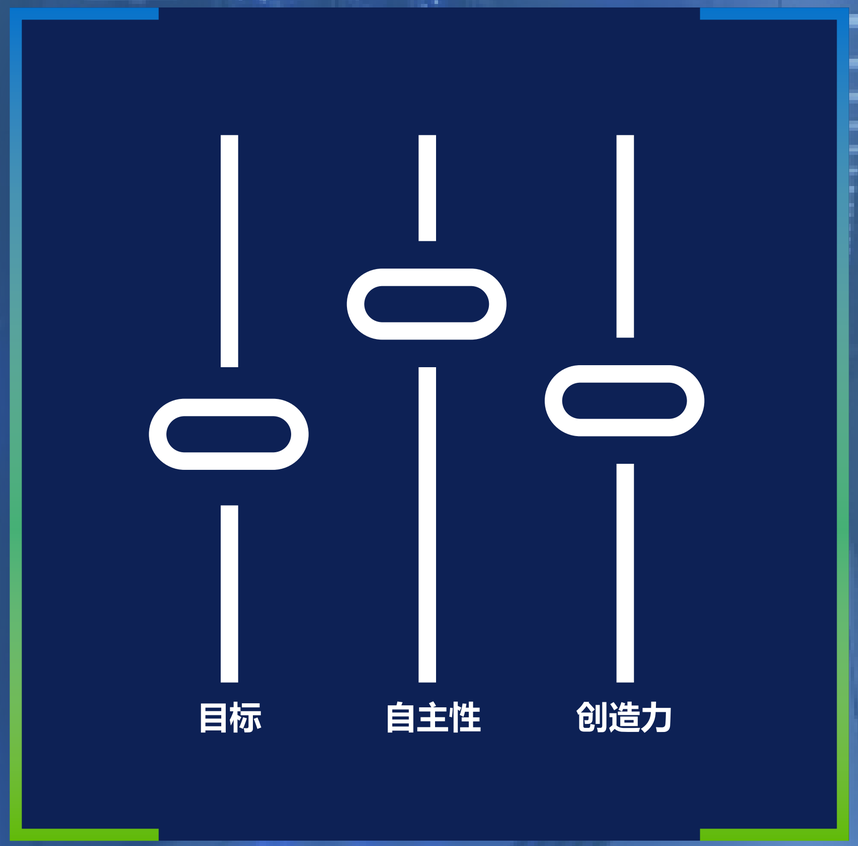
传统 AI
基于规则的系统依赖于预编程逻辑，需要人工干预进行调整。对于重复的结构化任务有效，但缺乏灵活性。

生成式 AI
基于现有的数据和用户驱动的提示输入，运用深度学习模型，生成文本、图像、代码及其他内容。

代理式 AI
AI 代理具备推理、环境感知、学习和适应能力。在设定目标后，代理能够以极少或无需人工干预的方式解决复杂问题。

物理 AI
将智能性体现在与物理世界交互的机器人系统中，例如机器人、传感器及其他设备。

人工通用智能 (AGI)
代表 AI 开发人员、研究人员和科幻迷们所追求的愿景，即拥有与人类认知能力相似的机器。AGI 仍处于理论阶段。



AI 层级为何至关重要

企业领导者必须了解 AI 各个阶段之间的区别，以便进行战略投资，并评估不同 AI 实施或应用场景的复杂性。代理式 AI 尤其带来了前所未有的复杂性和精密性，需要与业务流程、商业逻辑深度契合，并具备跨场景自主行动能力。

此外，如果已投资传统 AI 和生成式 AI 的组织想要采用代理式 AI 解决方案，则必须实施强健的防护机制、人工监督体系及更严密的安全措施，以确保安全、可靠的成果。

目标、自主性和创造力不仅仅是代理式 AI 的特征，也可以由组织积极定义。设定明确的目标可验证 AI 从一开始就与业务优先事项保持一致。界定自主权限范围，使系统在限定框架内独立运作。通过约束条件、上下文或优选方法引导 AI 行为，可确保解决方案始终支持战略意图。

风险和回报：人类影响

代理式 AI 正在重塑工作场所、深刻改变任务完成方式、决策制定过程以及团队协作方式。这种转变带来了巨大的回报，但也伴随需审慎管理的新复杂性。组织需要一个明确的战略，在自动化与监督之间实现平衡，确保系统在性能和问责制方面都经过校准。

向代理式 AI 推进，就是迈向更智能、更具适应性和更具弹性的企业。实现这一目标意味着领导者必须确定哪些职能最适合自主性、哪些环节仍需以人类判断为核心，以及如何确保 AI 驱动型决策的透明度和信任机制。

风险：自动化与监督需要并行

代理式 AI 虽具备强大能力，但若缺乏适当监督，可能引发透明度、责任归属与判断力方面的挑战。

回报：AI 成为效能倍增器

通过战略性部署，代理式 AI 可成为效能倍增器，依托数据驱动洞察激发员工潜能、加速决策速度、优化业务成果。

探索核心特征

用于定义代理的核心特质

代理式 AI 将自主性、适应性和目标驱动型智能相结合，赋予 IT 系统主动驱动结果、优化流程和实时学习的能力，从而创造变革性商业价值。代理式 AI 的以下核心特征可帮助组织提高运营速度、精度和可扩展性，从而在 AI 驱动型经济中创造可重复、可持续的竞争优势。

通过这些核心特质，代理式 AI 能够提供可扩展的智能系统，从而能够提高效率、优化决策并减少工作流之间的摩擦。通过利用这些能力，组织可以在 AI 驱动性不断增长的经济中获得更强敏捷性、创新力和弹性。

自主运营，无需人工干预即可执行任务。

与系统交互，以便在数字环境中采取有意义的操作。

追求定义的目标，而无需详细的执行说明。

根据上下文理解和可用数据进行分析、推理和采取行动。

通过数据输入，传感器和模型感知环境，提供交互信息，以感知环境。

通过持续分析与经验积累，实现行为模式的迭代优化。

为什么代理代表 AI 的下一阶段

自主运营的影响

与需要频繁人工干预的 AI 模型不同，代理式 AI 能根据实时数据和组织目标持续优化流程，实现独立运作。下面的关键功能定义了代理式 AI 如何增强业务运营。

被动监控

代理式 AI 可以扫描数字和物理环境，以识别相关数据点或异常情况，并根据定义的规则和流程以及决策做出智能反应

主动查询响应

传统 AI 系统通常需要结构化输入，但代理式 AI 可以动态响应复杂的非结构化查询，以解释上下文并检索相关信息。

事件驱动触发

代理式 AI 可以在满足特定条件时执行预定义的操作，从而缩短响应时间，并在关键场景中及时采取行动。

计划任务

代理式 AI 可以通过智能管理时间敏感型工作流和调整时间表来优化效率。这有助于增强合规性报告、预测性维护和库存补货流程。

有序的工作流集成

要充分发挥代理式 AI 的潜力，必须将其无缝集成到现有的工作流、数据源、平台或基础架构中。代理式 AI 不是作为独立系统运行，而是通过增强员工能力、改善决策和主动消除低效环节，实现技术生态系统的升级。

当考虑如何部署 AI 代理时，确定特定应用场景对底层 IT 体系结构和平台的影响至关重要。例如，纯数字化 AI 系统与需物理组件的 AI 系统所需的基础架构截然不同。

例如：

信息系统

商用系统
代理式 AI 使 CRM、HR 和 ERP 系统能够自主适应和行动，实现客户互动个性化、简化员工队伍规划并自动执行供应链运营。

IT 操作
AI 代理可以主动监控 IT 系统、识别威胁并自动响应，有效保障安全、满足 SLA 协议并减少停机时间。

运营系统

店内或实时客户交互
运用情绪分析和计算机视觉，实时监控和响应店内客户交互，以提供个性化客户服务。

工厂、仓库、物流
将计算机视觉与 IoT 设备和代理式 AI 相结合，可管理复杂的物理操作，例如自主视觉设备检查。

治理和风险规避

确保数据隐私和合规性是负责任采用 AI 的基石。组织必须实施治理和多层安全措施，以保护敏感信息，同时使 AI 系统能够有效运行。相关战略包括：

受控访问
将 AI 访问限制为仅限必要的数据集，确保信息受到保护和保密。

加密
利用高级加密方法来保护静态和传输中的数据，从而降低网络威胁的风险。

AI 决策过程中的透明度
记录 AI 模型如何做出决策，并向利益相关方及监管机构提供可追溯的决策依据。

定义并强制实施防护边界
限制功能范围、明确定义用途，并为代理设定严格的操作窗口。

风险监控和衡量
使用定义的指标来评估风险并及时通知响应行动，持续监控 AI 系统的漏洞和性能偏差。

通过将强大的治理、安全性和隐私措施嵌入到代理式 AI 部署中，组织可以自信地发挥 AI 的潜力，同时保持道德诚信和法规合规性。

代理式 AI 应用场景示例

代理式 AI 通过自动执行决策、优化工作流和提高效率来实现行业转型。代理式 AI 应用程序可能因行业而异，以下精选应用场景展示了 AI 的广泛影响。

客户服务
代理式 AI 可以部署代理，以自动解决询问、个性化交互和实时分析情绪，从而改变客户服务。与 CRM 系统集成，可缩短客户等待时间、提高满意度，并自动处理常规客户支持请求。

网络安全
代理式 AI 可以自主监控 IT 环境、检测异常情况并根据预先建立的安全协议执行响应，从而增强网络安全。这种主动式方法可降低风险、缩短事件响应时间，并确保大规模持续保护。

智能城市和数字孪生模型
代理式 AI 可通过分析实时传感器数据、优化交通流量及预测维护需求，赋能更智能的城市基础架构。当集成到数字孪生环境时，它能模拟城市运营，从而实现主动的城市规划和危机防范。

运营和物流
代理式 AI 可以通过预测需求、管理库存水平和精确协调物流，实现全供应链优化。根据实时状态动态调整：智能改派运输路线、优化排程，并通过持续不断地学习提升效率。

财务
在金融领域，代理式 AI 可以识别可疑交易、分析复杂的风险模式，并实时防止欺诈。通过不断更新的情报，增强合规性、减少手动监管，并支持更精准的财务决策。

持续预测和规划
代理式 AI 可以根据不断变化的内部和外部数据不断优化预测，从而促进动态预测。它能自动调整计划、探测新兴趋势，并为跨业务职能提供更精准敏捷的决策支持。

代理式 AI 应用场景的优先级排序

成功落地实施需要采用结构化方法，确定 AI 驱动的自动化能创造最大价值的场景。通常情况下，企业领导者应根据部署代理式 AI 所需的工作、成本和复杂性来评估潜在的 AI 应用场景的可行性。该计划涵盖了系统集成、数据准备、模型训练以及持续维护等多个方面。优先考虑能匹配现有工作流且干扰最小的解决方案。

缩略词 **LEARNS** 可用于识别能够带来价值的合适类型的代理式 AI 任务和活动。它可以帮助决策者从以下标准的角度查看应用场景，从而帮助决策者了解 AI 解决方案的商业价值：

低风险
自动化或 AI 出错时，对任务产生极小的负面影响。

新兴
在特定领域，AI 驱动型自动化仍在不断发展且潜力显著。

艰巨
重复且耗时的流程，这些流程可以从自动化中受益。

补救
容易出错的任务，通过 AI 可以进行优化并增强准确性。

不值得
对于特定职能，AI 使员工能专注于其他更多更有价值的工作，从而实现额外价值。

速度
在特定流程中，AI 能以超越员工的速度完成任务。

通过应用这种方法，组织可以战略性地确定哪些活动最适合代理式 AI，从而在自动化和人工监督之间建立平衡。

如何构建代理式 AI

核心组件

构建强大的代理式 AI 系统需要基础 AI 技术、可扩展基础架构和战略实施相结合。
下面的关键组件使代理式 AI 能够有效运行：

数据访问
要使代理式 AI 有效运行，IT 必须能够无缝获取及时、相关且富含上下文的数据，并嵌入现有的业务流程和逻辑。通过这种访问权限，AI 代理能够做出明智的决策、适应不断变化的环境，并根据可用的最新信息持续优化性能。

基础架构
大规模部署代理式 AI 需要强大且可扩展的基础架构，并与支持云和边缘计算环境的现有工具集成。某些应用场景可能依赖于云，而边缘计算支持在行动点进行实时处理，从而减少延迟。

大型语言模型 (LLM)
LLM 是原型 AI 的核心，可提供处理、理解和生成类人文本的能力。通过这些模型，AI 系统能够理解和处理复杂的查询、整合信息，并提供根据业务需求定制的上下文洞察。

多代理系统
多代理系统不是依赖单一 AI 模型，而是涉及多个任务专用 AI 实体协同工作，以实现复杂目标。在初始代理式 AI 部署中投资于数据访问、基础架构和 LLM，将为未来的多代理系统奠定基础。

分阶段（爬行、行走、奔跑）方法

成功实施 AI 和生成式 AI 需要采用分阶段方法，以确保与业务目标和风险管理保持一致。组织可以采用“爬行、行走、奔跑”方法来逐步扩展 AI 功能。

爬行阶段
专注于小规模传统 AI 和生成式 AI 项目，重点关注低风险、高价值应用场景。识别 AI 驱动的自动化能够迅速取得成果的领域，以便在全面部署之前验证 AI 的有效性。

行走阶段
从试点小规模代理项目开始，将 AI 驱动的决策集成到关键工作流、治理框架和模型中。

在该节点上运行
在整个组织内部署和集成代理式 AI，作为业务流程的核心组件，以满足您最关键的需求。

戴尔和 NVIDIA：值得信赖的 AI 创新合作伙伴

Dell AI Factory with NVIDIA

代理式 AI 需要现代化 IT 和可扩展的基础架构，以支持大规模自动化。如需加速采用 AI，组织可以利用 Dell AI Factory with NVIDIA — 一款集服务、AI 软件和基础架构于一体的端到端框架。

Dell AI Factory with NVIDIA 可通过预构建的体系结构、高性能系统和 AI 优化的集成软件堆栈，帮助加快 AI 的采用速度，从而高效且可扩展地部署代理式 AI 模型。

戴尔和 NVIDIA 提供创新、可靠性和深厚的行业专业知识的独特组合，包括：

可扩展的 AI 基础架构
戴尔的 AI 就绪型服务器和存储由 NVIDIA GPU 提供支持，可提供大规模训练和部署代理式 AI 所需的性能，无论工作负载是在本地、云中还是在边缘。

无缝集成 AI
AI 部署需要与业务流程和运营无缝集成。戴尔和 NVIDIA 提供预先验证的框架、容器化部署和自动化工具，以将 AI 嵌入到工作流中。

成熟的AI专业知识
戴尔和 NVIDIA 以数十年的 AI 和技术专业知识为后盾，提供可加快实现价值、提高性能并简化 AI 实施的解决方案。

充分释放代理式 AI 的潜力

与戴尔和 NVIDIA 合作，您可以放心地实施代理式 AI，将效率、自动化和业务智能提升到新的水平，同时确保 AI 基础架构始终安全、可扩展且面向未来。

为了优化您的成果，请参加免费的 Dell Accelerator Workshop、量身定制符合您目标的 AI 战略，并深入了解戴尔和 NVIDIA 的解决方案组合及框架。

开启 AI 之旅

探索 Accelerator Workshop

Dell **AI Factory** WITH NVIDIA

DELL Technologies | NVIDIA