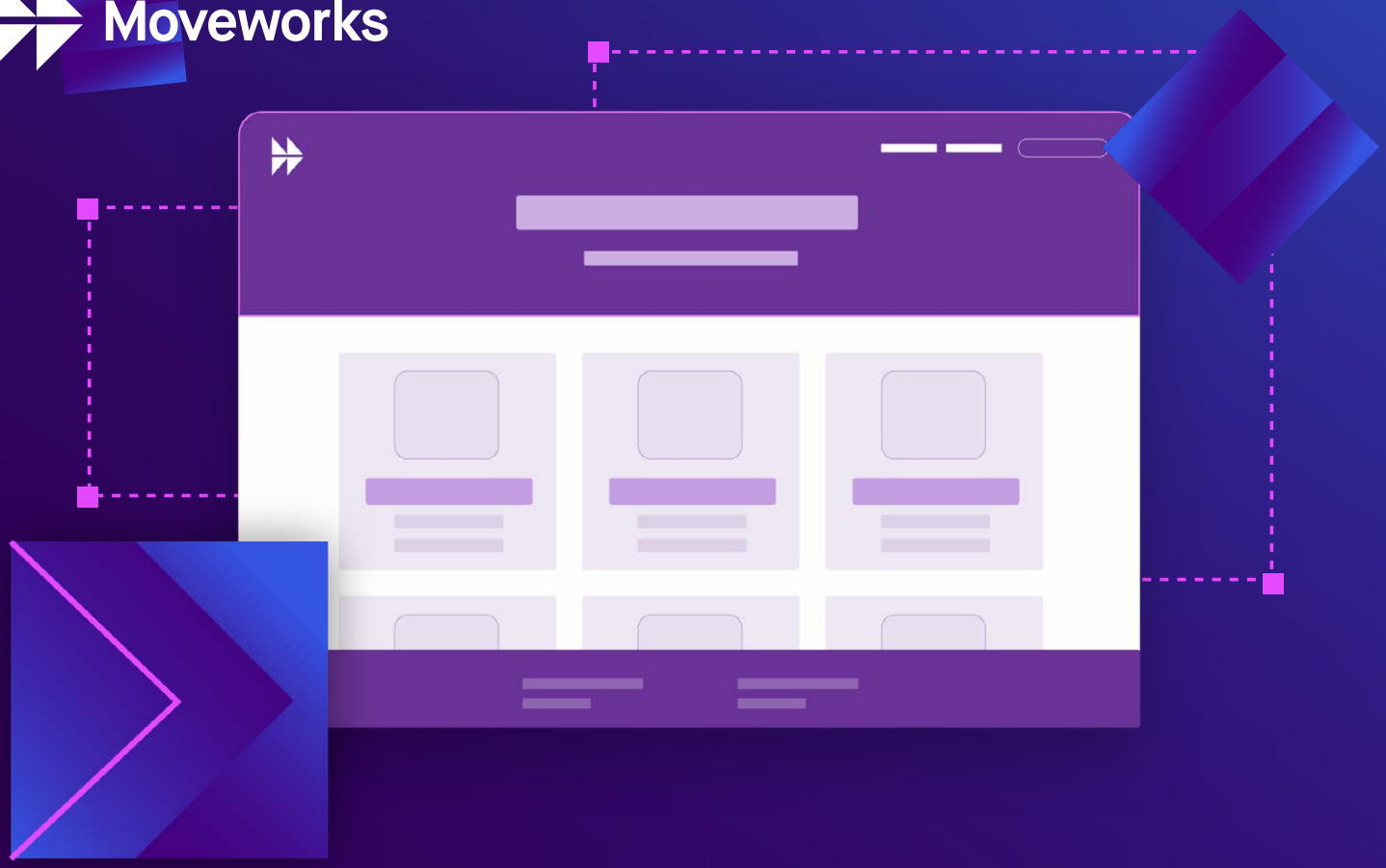
Moveworks



AI 代理的终极指南

简介

AI 代理是未来

自动化正在经历一场根本性的变革。传统的系统曾经能够轻松处理预定义的业务流程，但现在在面对更为复杂、基于推理的操作时却面临局限性。进入AI代理——由高级大型语言模型（LLMs）驱动的新一代自动化时代。

“AI 代理 ” 是一个由 LLM 驱动的自治系统 ， 它是

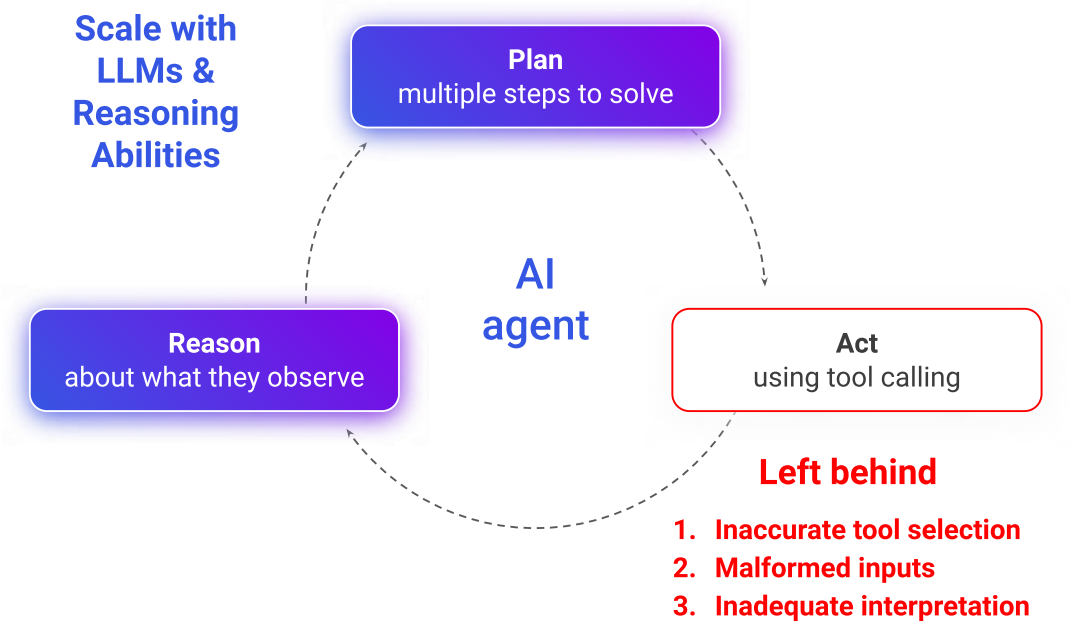
能够代表用户完成任务。

AI代理拥有独特的自然语言解释能力、制定行动计划以及在最少人工干预的情况下执行任务的能力。通过使用AI代理，企业现在有机会实现前所未有的效率提升，使员工能够专注于高层次的思考，而自动化则处理琐碎的工作。

什么是 AI 特工 ？

“代理人 ” 是代表另一个人或团体行事的实体 (牛津英语词典 y)

一个“AI代理”是由大型语言模型驱动的自主系统，能够代表用户完成任务。



想象一下AI代理的强大功能，能够迅速加速并简化您的自动化开发过程，将所有自动化任务集中到一个平台上，并提供内置合规性，因为代理被编程遵守公司政策。

但是 ， 尽管有了早期的承诺 ， 但大多数 Agentic AI 系统还没有完全辜负这种炒作。

我们旨在帮助您理解代理自动化（Agentic Automation），探索Moveworks代理自动化的动力，以及展示它如何使您的开发比以往任何时候。 这是因为Moveworks的代理自动化不仅仅是连接API——，它还利用大型语言模型（LLMs）进行推理、解释和决策，从而采取智能行动，使得开发过程更快捷、更轻松。

让我们探讨Agentic自动化如何赋能开发者轻松构建和使用AI代理，以弥合人类语言与结构化系统API之间的差距。

亲身体验Moveworks Agentic Automation Engine如何无缝集成到各种系统中，帮助您的AI代理理解复杂请求、做出明智决策，并自动化广泛的任务。继续阅读，准备好充分释放Agentic Automation的全部潜力并加速您的开发项目。

目录

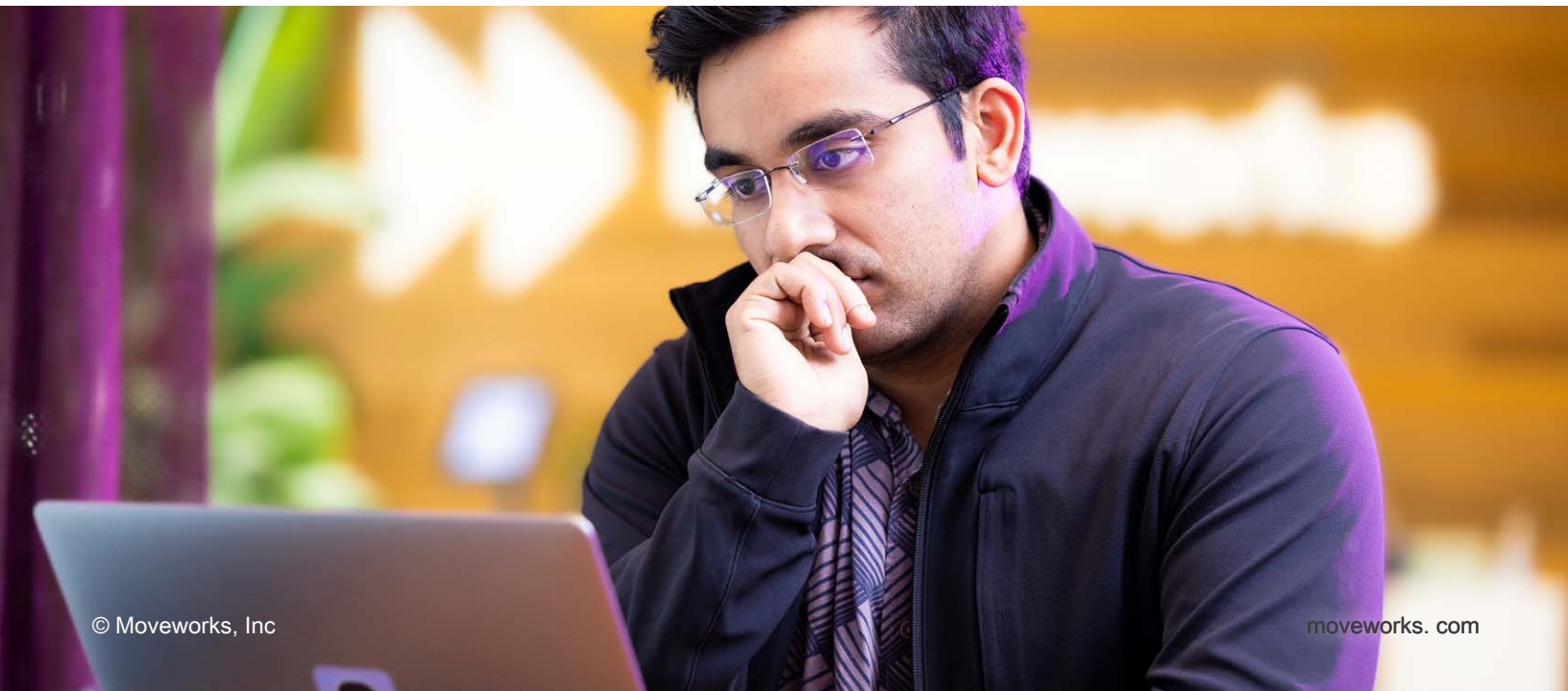
01

传统自动化平台的挑战

厌倦了无尽的自动化构建和管理循环以及对开发者造成的巨大压力吗？随着您的组织SaaS场景的发展超过1000个应用甚至更多，技术团队构建高效集成的压力正在不断加大。

因此，您的业务依赖后办公室专家来重新启动流程，并依靠开发者通过构建无数自动化功能来填补空白。然而，使用传统的API驱动方法和iPaaS平台来构建自动化功能是耗时且繁琐的，根本不够用。

今天的自动化工具高度依赖基于API的过程。虽然这种方法对于可预测且结构化的任务非常有效，但在处理人类语言的动态性质时可能会遇到困难。传统的企业集成平台（iPaaS）在配置预定义的工作流方面表现出色，但在AI代理的时代，它们可能显得力不从心。简而言之，这些传统的自动化方法效率低、复杂度高，并且往往更为耗时。



人工智能的崛起

在这方面 ， AI 代理提出了一种新的

自动化范式。 与传统的SaaS应用期望用户发现和导航界面不同，AI代理使用大型语言模型（LLM）为用户执行自动化操作。

理解目标，制定计划，并进行相关的工具调用（即函数调用）以完成用户任务。这类系统通常被称为代理型AI系统——正如这些系统所展现的推理、规划和工具调用能力所定义的那样。

如果成功，代理型AI系统能够使企业显著提高效率并提升员工的工作 productivity。

用户简单地描述了他们想要完成的任务 ，
而 AI 代理能够

Traditional Applications	Agentic Applications	Business Outcomes
Developers build portals & hope employees find intake forms.	AI agents find the right automation based on the user's need.	Downsize support staff required to navigate employees to resources
Employees have to go to sift through emails & portals to find pending tasks	AI agents aggregate a single view of all tasks	Fewer tasks are dropped or ignored
Developers build a user interface for every type of task	AI agents can dynamically generate the perfect interface for each task	Higher quality, more informed decisions are made
Developers pre-build & maintain static workflows.	AI agents combine smaller automations to fit user needs on-the-fly	Less developer time spent on editing workflows.

然而 ， 尽管推理的进步
LLM 的能力 ， **我们还没有看到 agentic**
AI 违背了这一愿景。

02

机构自动化 - 一类新的工具

代理自动化带来了革命性的工具集，使AI代理能够弥合人类语言与结构化系统API之间的差距。该平台允许开发者创建能够理解模糊指令并将其转换为更精确操作的AI代理。

AI 代理需要能够推理、计划和行动。

世界领先的大型语言模型（LLMs）如OpenAI的o1、Anthropic的Claude 3.5以及Google的Gemini Pro 1.5越来越强大（更大的上下文窗口、更好的推理能力、更多的模态）。这使得推理和规划能够扩展，但 还有更多的建立 AI 代理。

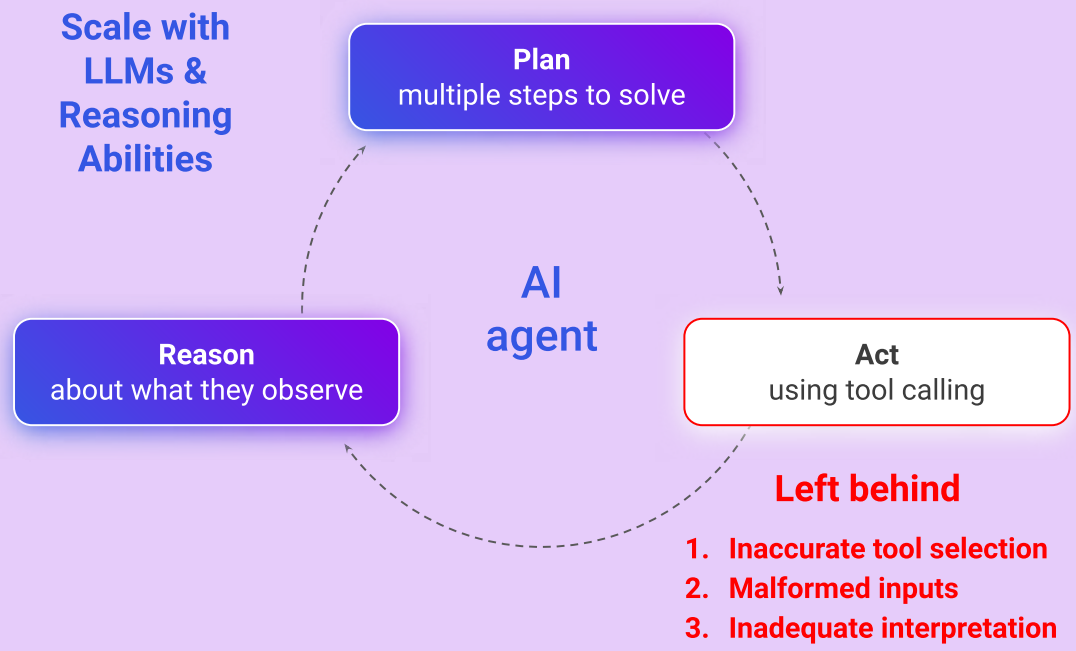
一些开发者错误地认为，大型语言模型（LLMs）可以直接通过与其他系统相同的API与业务系统进行交互。虽然API允许您与业务系统交互并使这些系统能够通信，但它们本身并不是一种集成。每一个曾经通过API进行过集成的开发人员可能都能理解，集成不仅仅是使用API——还需要编写代码。

集成平台即服务（iPaaS）行业应运而生以解决这一问题。当前的iPaaS工具（如Zapier、Workato、Microsoft Power Automate、ServiceNow Flow Designer、Salesforce Flow Builder、Mulesoft等）允许开发者编写代码来连接不同业务系统的API。

现实情况是 ， 现有的 API 和集成平台很难设计为基于 LLM 的 AI 代理使用。

iPaaS和中间件旨在连接API（这些API精确且确定）到其他API。然而，AI代理需要将人类语言（这一语言模糊且多义）连接至API。

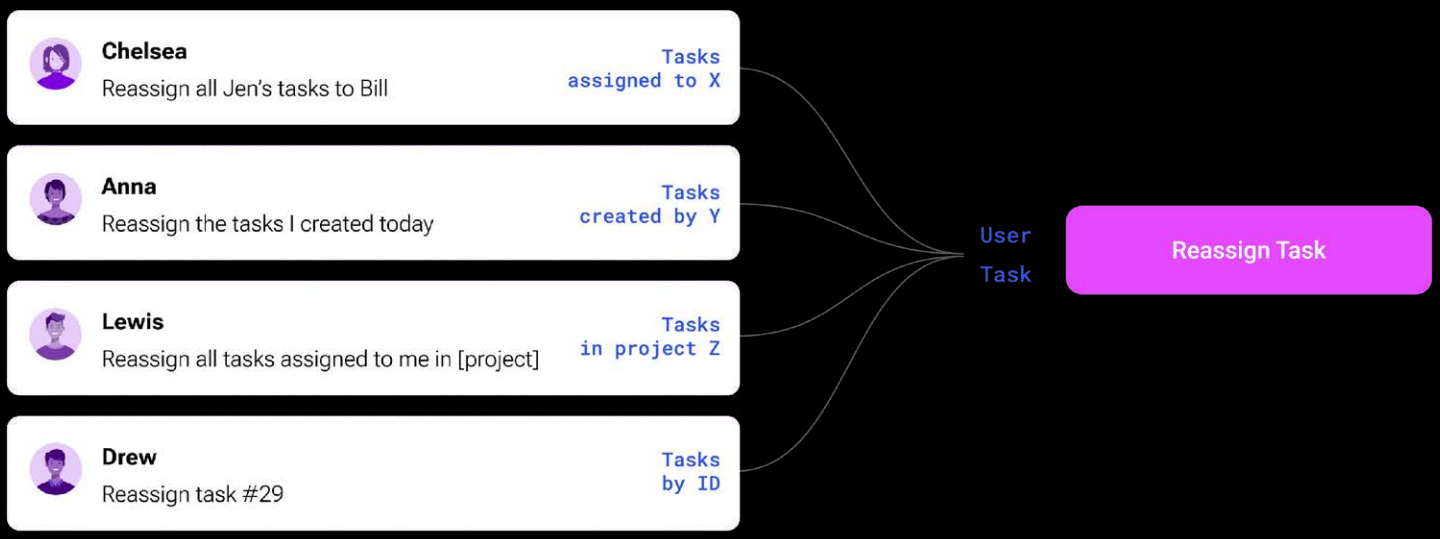
如何 AI 代理工作



让我们举一个简单的例子。

假设我想要一个能够帮助我管理任务（创建新任务、更新现有任务、重新分配任务等）的代理。为了构建这样一个代理，我们可以设想我们需要提供一系列功能以实现这一目标。 **重新分配任务 API** 。它需要(1) 任务 ID 和(2) 用户 ID 来分配给它。

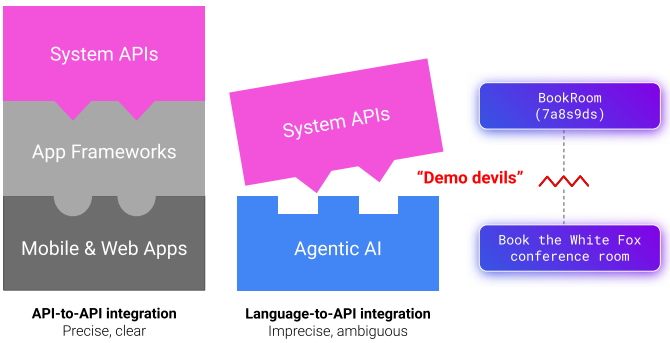
但是人类语言是混乱的。您的用户可能会通过数十种方式指定这些输入 ：



这些限制正是为什么REST APIs和传统自动化平台不适合由AI代理使用的原因。它们往往缺乏关键的能力，以克服因工具选择不准确、输入错误以及不连贯响应所带来的挑战。

系统API与代理AI系统之间的空白空间代表了当前开发AI代理的“尚未准备好”的现实。这里就是“Demo魔鬼”存在的地方。

没有合适的底层工具，开发者被迫让iPaaS的圆枘塞入代理AI的方孔中。因此，开发者可能会尝试用大量的难以维护、无法扩展的代码（技术债务）来填补差距，仅仅只是为了产出次级的结果。



当企业需要将AI代理部署到成百上千的员工中时，“在我的沙盒里有效”在出现问题时不是一个合理的回答。企业为AI代理所作出的投资往往难以见到成效——它们经常被困于科学项目和演示阶段，因为这些投资缺乏足够的稳健性和成熟度以在整个企业范围内可靠地部署。

简而言之，使用iPaas工具构建有agency的AI系统往往无法实现预期的有agency的能力。此外，这一开发过程甚至可能挑战高级技术团队，并消耗大量资源，从而偏离您的战略目标。

超越iPaaS的限制涉及采用专门设计以应对代理AI复杂需求的平台。这意味著优先考虑赋予开发人员自由的工具 到错综复杂的设计 与先进的逻辑和自主性性相结合，优化和完善AI系统。当前的空白正是AI代理尚未广泛普及的原因所在。在AI代理受限于传统自动化平台的情况下，它们可能无法充分发挥其潜力。

机构 AI 自动化 ： 前进的道路

代理自动化是一种创建AI代理的方法，旨在实现业务平台与企业副驾之间的无缝集成，克服传统自动化工具的局限性。它支持直接将对话转换为API，利用先进的推理引擎，并访问关键数据，从而为更智能、更具响应性的AI系统的开发铺平道路。

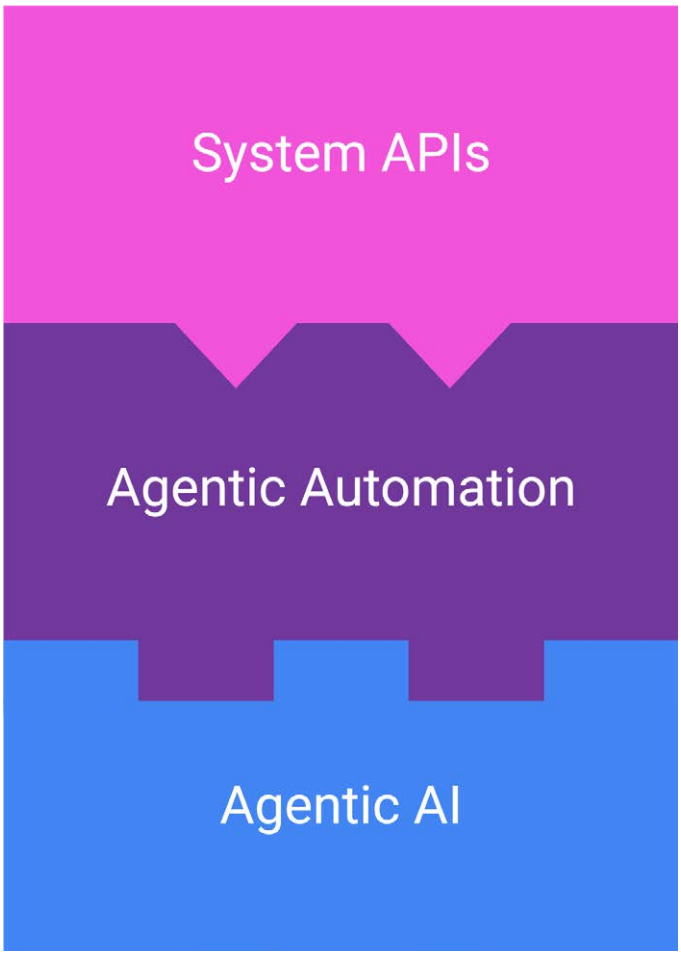
03

使用 Moveworks 机构自动化引擎释放 AI 代理

为了赋能开发者突破传统自动化平台的局限性，Moveworks设计了一款全新的代理自动化引擎。通过使开发者能够用极少的代码构建强大的AI代理，此引擎解锁了更高的效率层级，彻底改变了企业自动化复杂工作流程的方式。

The Agentic Automation Engine 从核心设计出发，旨在构建能够连接代理型AI语言和业务系统结构化数据的自动化流程。这一Agentic Automation Engine 成为了新的核心。Creator Studio ，开发人员在 Moveworks 平台上构建 AI 代理。

借助此技术，开发者能够构建强大的AI代理，这些代理能够处理传统自动化引擎驱动的AI代理无法处理的更复杂任务。与传统方法相比，开发者能够使用不到十分之一的代码更快地构建AI代理。最理想的是，开发者能够在单个平台上集中所有开发工作，消除代码蔓延并简化部署实践。

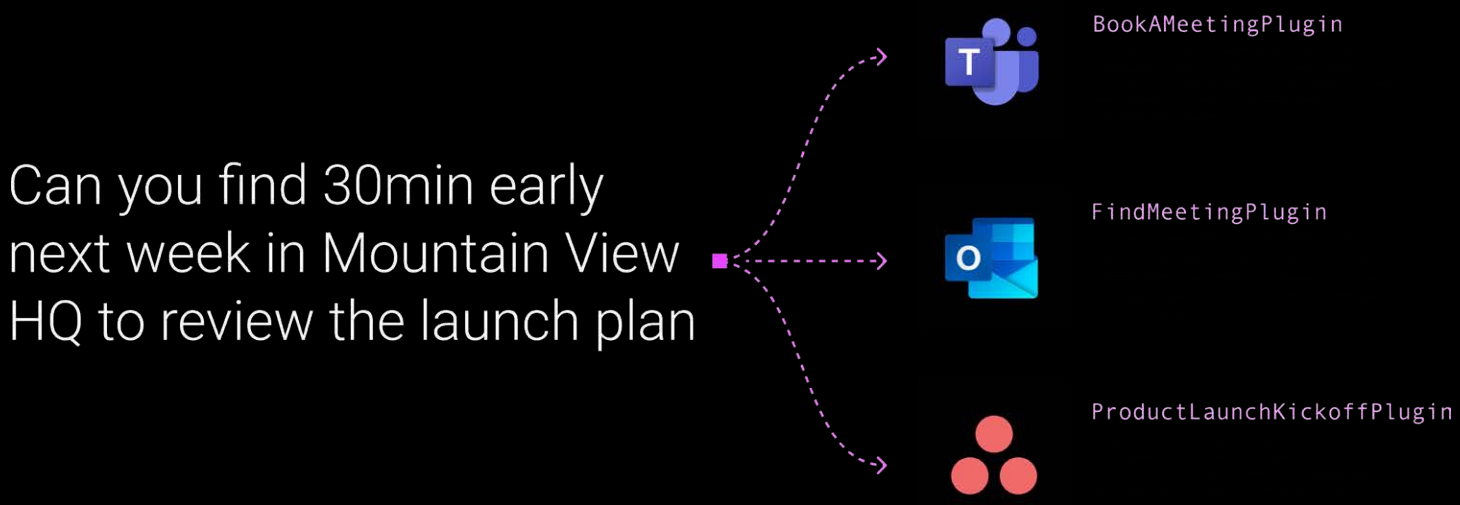


由Agentic自动化引擎驱动，开发者能够构建插件，这些插件被Moveworks Copilot使用。Agentic自动化引擎具备一些关键功能：

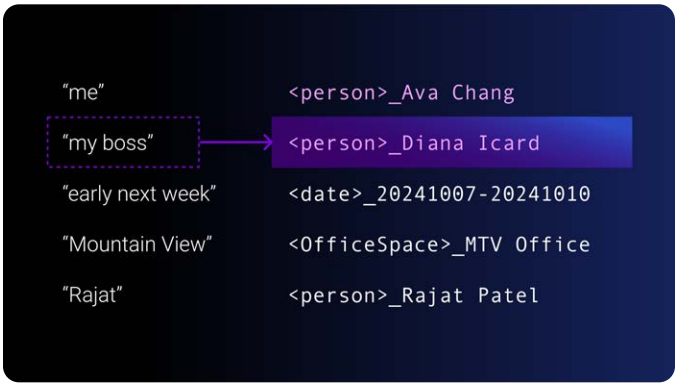
清单生成器

一种超越 mere 提示和语句的与大语言模型（LLMs）交互的新方法。它分析插件（代理自动化），生成精确的插件清单，并动态调整提示以帮助AI代理更好地理解插件之间的细微差别，并更有效地将它们映射到用户请求。

在此之前 ，开发人员必须学习如何进行提示工程和提示调优以获得所需的行为。



一种新的技术，使自主AI系统能够将自然语言转换为可靠且API友好的标识符。例如，它可以将“ACME账户”转换为其Salesforce标识符“00ORd0000040V9ZMAU”。这使得AI代理能够正确识别商业对象并成功执行任务。



在此之前，开发人员必须尝试解析文本并在iPaaS内部操作字符串，这可靠性差且会导致意外结果。

Policy Validators

大型语言模型（LLMs）能够很好地处理不确定性，但其指令可能被误解，甚至可能被破解。商业规则是不可违背的规定。你不希望有人为仅有两人的会议预订一个可容纳20人的房间，也不希望员工提交超过100美元的报销而没有合理的商业理由。我们的政策验证器能够在推理引擎中增加一层额外的约束，以确保这些政策得到执行——无论你添加多少条政策。

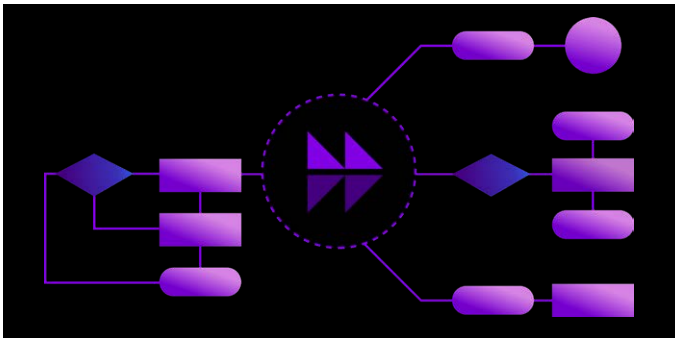
在此之前，开发人员会尝试添加自然语言指令，但模型往往会误解这些指令或无法正确执行。

策略验证器有助于实施您的特定策略

一种高度集成的技术，能够将计划中的、进行中的和已完成的动作通知给推理引擎。这种方法让开发者能够专注于构建工作原型，而我们的推理引擎则负责所有对话生成、边缘情况处理以及故障处理。

为了了解更多这些令人惊叹的技术及其它们与传统自动化同类产品之间的独特之处， 在这里阅读我们的白皮书。

在此之前 ， 开发人员必须构建所有的错误处理逻辑 ， 并为每个场景提供自定义的 dia - logs 。



04

Moveworks 推理引擎如何通过机构 AI 提高生产率

人工智能领域长久以来一直在探讨一个基本问题：机器能否真正进行推理？近期，自主智能AI的发展为这一问题提供了令人信服的答案。与遵循预定义规则的传统AI系统不同，自主智能AI旨在自主思考和行动。这一方法的核心是推理引擎——一种超越数据处理、通过逻辑分析解决复杂挑战的高级AI系统。

推理引擎使AI能够独立理解问题、制定策略并执行解决方案，这一能力正在改变企业处理任务自动化和解决问题的方式。本文将探讨推理引擎的工作原理、它们在自主AI中的角色以及它们如何改变企业运营的格局。

什么是推理引擎 ？

一个推理引擎是一种AI系统，它理解用户的目标，制定实现目标的计划，根据计划执行函数调用，评估执行的成功与否，迭代改进计划，直至成功实现原始目标。在某种程度上，它试图模仿人类解决问题的方式。

在实际应用中，推理引擎使系统能够动态地确定如何帮助用户，而不是遵循一套预先定义的规则或决策树。它充当人工智能助手的大脑。

理解代理推理

代理型AI是一种可以通过自主“代理”来实现复杂目标的AI系统，以代表用户采取行动。在这种框架中，结合使用多种机器学习模型，以创建一个可以独立制定和执行基于推理的计划的AI，该计划能够实现用户的目标，而不仅仅局限于遵循预编程的逻辑或对话流程。

具备推理能力的代理AI副驾更能全天候帮助员工应对各种任务。类似于个人助理的角色，这种AI同样能够理解挑战并替您解决问题。提出您面临的难题，Copilot将进行深入研究并提出最佳解决方案——这就是推理在行动的价值。

Moveworks 推理引擎

推理引擎使 AI 能够有意义地实现员工的目标。它具有以下能力 ：

- 了解用户的目标

制定实现这一目标的计划

- 根据其计划执行函数调用

- 评估此执行的成功

- Iterate on the plan until it successfully achieves its original objective

重要的是，推理引擎能够在必要时回访用户以获取关于目标的额外上下文信息、确认其方向，并实时接收用户输入以适应计划。

在某些方面 ， 它试图模仿人类如何解决问题 ， 这就是为什么
推理 Copilot 是如此强大。

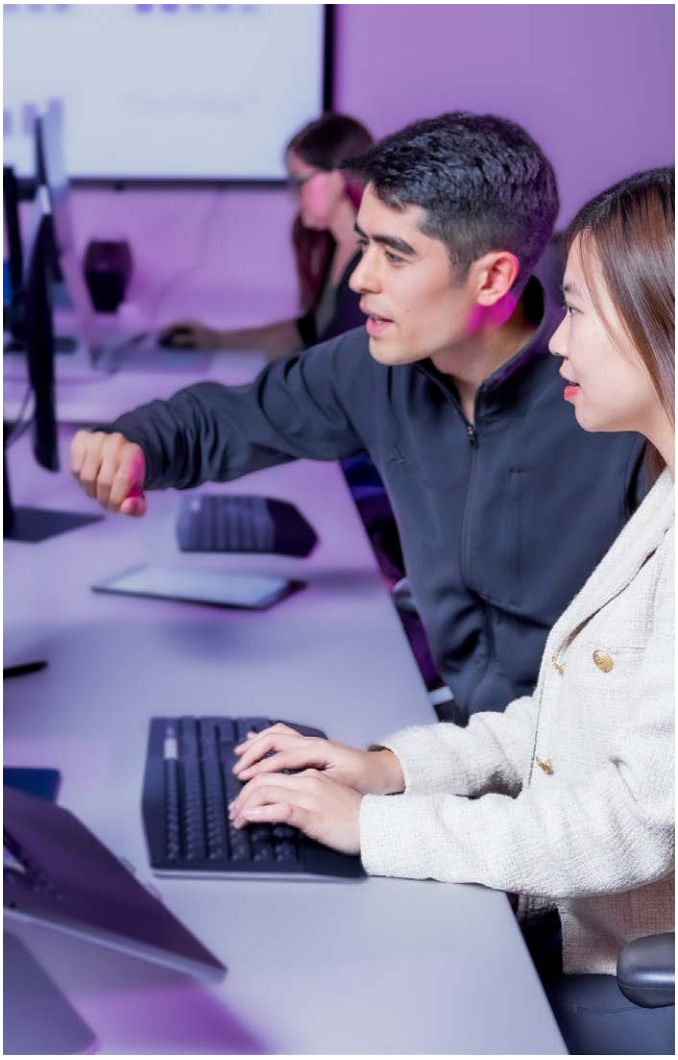
Moveworks Copilot 的推理引擎是一个
基于代理的人工智能系统 展示了诸多类似人类的问题解决能力。我们的引擎利用了多个语言模型的推理、决策和插件调用能力，以完成我们之前提到的要点中的特定元素。

从通用支持的角度来看，我们的推理引擎能够可靠地运行于任何客户独特环境的具体细节中（即系统集成、可用插件、业务逻辑、流程等）。

Moveworks Copilot的成功意味着我们的推理引擎能够利用一组独特可用的工具和流程来创建针对特定业务的计划，并以目标导向的方式一致地执行任何任务，为全球数百万用户实时完成。让我们进一步探讨这一过程是如何发生的。

当用户与Copilot互动时，他们的查询、问题或对话会被送入一个推理过程，该过程会指导Copilot如何回应他们。为了便于理解，我们可以将这一过程视为三个distinct步骤依次展开：理解、规划和执行。

在每一步中，我们不断调整Reasoning Engine的各种LLM，以应用最佳的推理和决策技术。这种方法旨在使每位员工的互动都能得到深思熟虑且高质量的回应。



了解用户需求

第一阶段，理解阶段，在接收到查询请求时即开始。首先是对查询文本进行丰富处理，加入提取的元数据，这些元数据作为推理过程中至关重要的信号。推理引擎利用包括大型语言模型（LLMs）在内的机器学习模型集合，来确定语句的属性，如主题、意图、情感、领域和语言。

接下来，通过利用Moveworks知识图谱将用户提及的实体映射到其标准或规范形式，该过程在客户的具体业务背景下确立查询。这确保了Moveworks Copilot的所有组件能够理解实体引用的各种方式，包括那些仅存在于客户环境中的非常独特且特定于组织的实体。在此阶段，推理引擎还会检查查询是否具有毒性或冒犯性，并防止此类请求被处理并进入系统。

理解的关键要素之一是对话背景。推理引擎整合了用户与聊天机器人之间的先前交互，提供了丰富的上下文信息，以帮助识别最有效的解决方案。这包括识别用户是否开始新的主题还是继续之前的讨论，解析诸如“它”、“那个”等隐含参考等内容。

了解后续问题 ， 并检查以前向用户提供了哪些其他资源和选项。

从所有这些输入的结合中，推理引擎重新编写用户的查询，并能够构建一个完整且明确的问题陈述以解决问题。

规划成功

下一步是规划行动方案。这一阶段是推理引擎将对问题及其先前上下文的理解映射到选择最适合的插件或工具以满足请求。可以将插件视为专门针对特定应用场景定制构建的专用工具，并与某些系统进行集成。

例如，插件可能在Okta中重置密码、在Google Workspace中配置用户、在BambooHR中入职员工、在AccessHub中管理访问权限、部署服务器、更新Salesforce、从分析平台获取报告，以及在ERP系统之间同步产品数据。

列表不胜枚举。每个组织都有一套独特的插件，基于它们选择的配置以及使用Creator Studio扩展平台开发的自定义插件。

推理引擎审查可用插件列表，并迅速根据先前提取的信息过滤插件目录，筛选出最相关的选择。