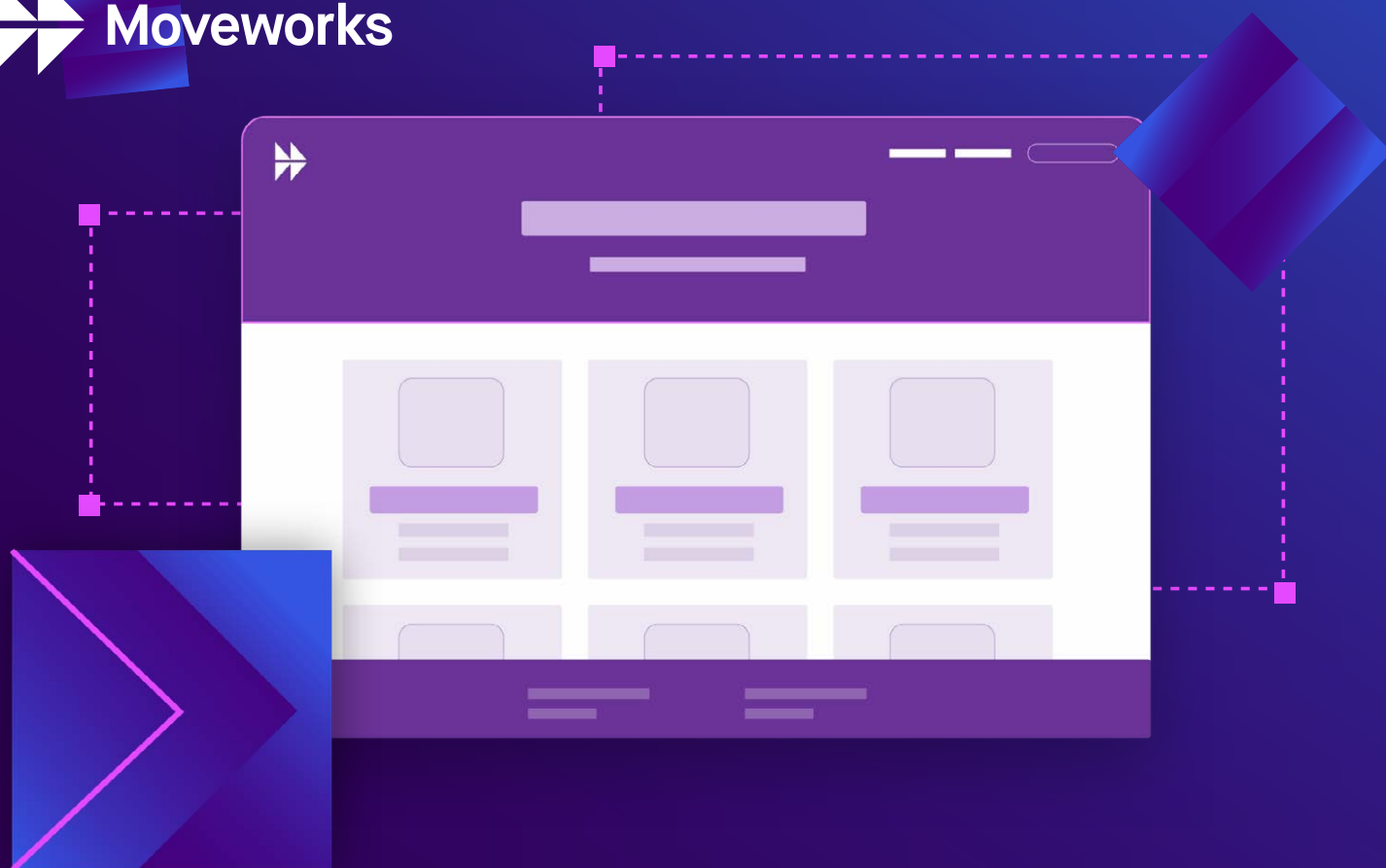




AI 代理的终极指南

简介

AI 代理是未来

自动化正在经历一场根本性的变革。传统系统曾轻松处理预定义的业务流程，但在面对更为复杂、基于推理的操作时却面临局限。进入AI代理——由先进的大语言模型（LLMs）驱动的新一代自动化时代。

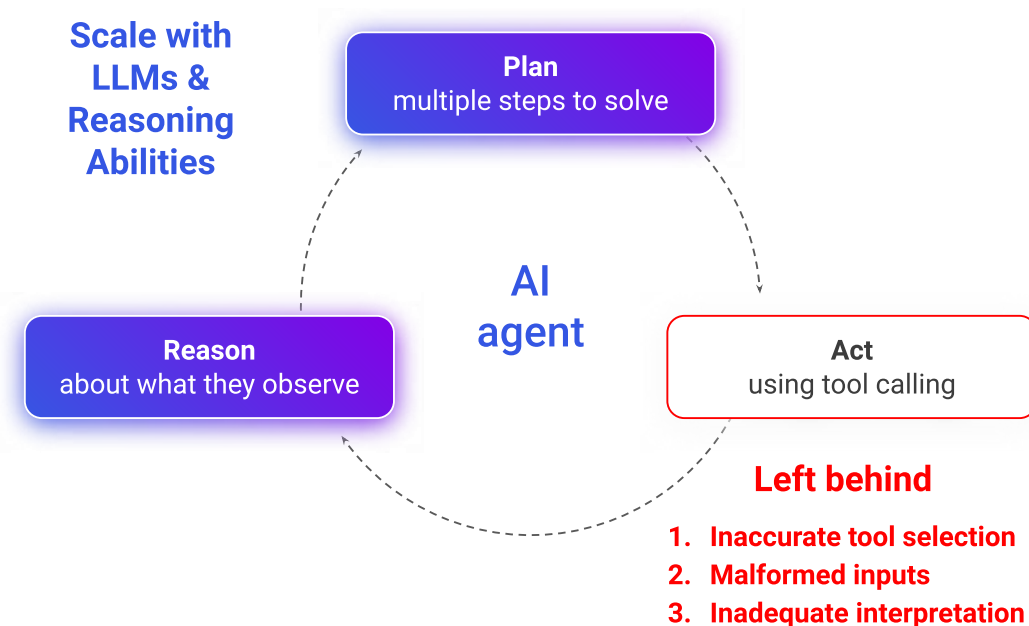
“AI 代理”是一个由 LLM 驱动的自治系统，它能够代表用户完成任务。

人工智能代理具有独特的能力来解读自然语言、制定行动计划并以最少的人工干预执行任务。利用人工智能代理，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思考，而自动化则处理那些繁琐的任务。

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。



just想象人工智能代理的强大功能，以快速加速和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。

我们希望帮助您了解Agentic自动化、Moveworks Agentic自动化引擎的强大功能，并展示它是如何使您的开发变得更加快速和简便。这是因为Moveworks Agentic自动化不仅连接API，还能够进行推理、解释和决策，利用大型语言模型 (LLMs) 采取智能行动。

让我们探索Agentic Automation如何赋能开发人员轻松构建和使用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的代理自动化引擎如何无缝集成到各种系统中，帮助AI代理理解复杂请求、做出明智决策，并自动执行一系列任务。继续阅读，准备好释放代理自动化的全部潜力并加速您的开发项目。

目录

简介

AI 代理是未来

04

Moveworks 推理引擎如何通过
机构 AI 提高生产率

01

传统自动化平台的挑战

02

机构自动化 - 一类新的
工具

03

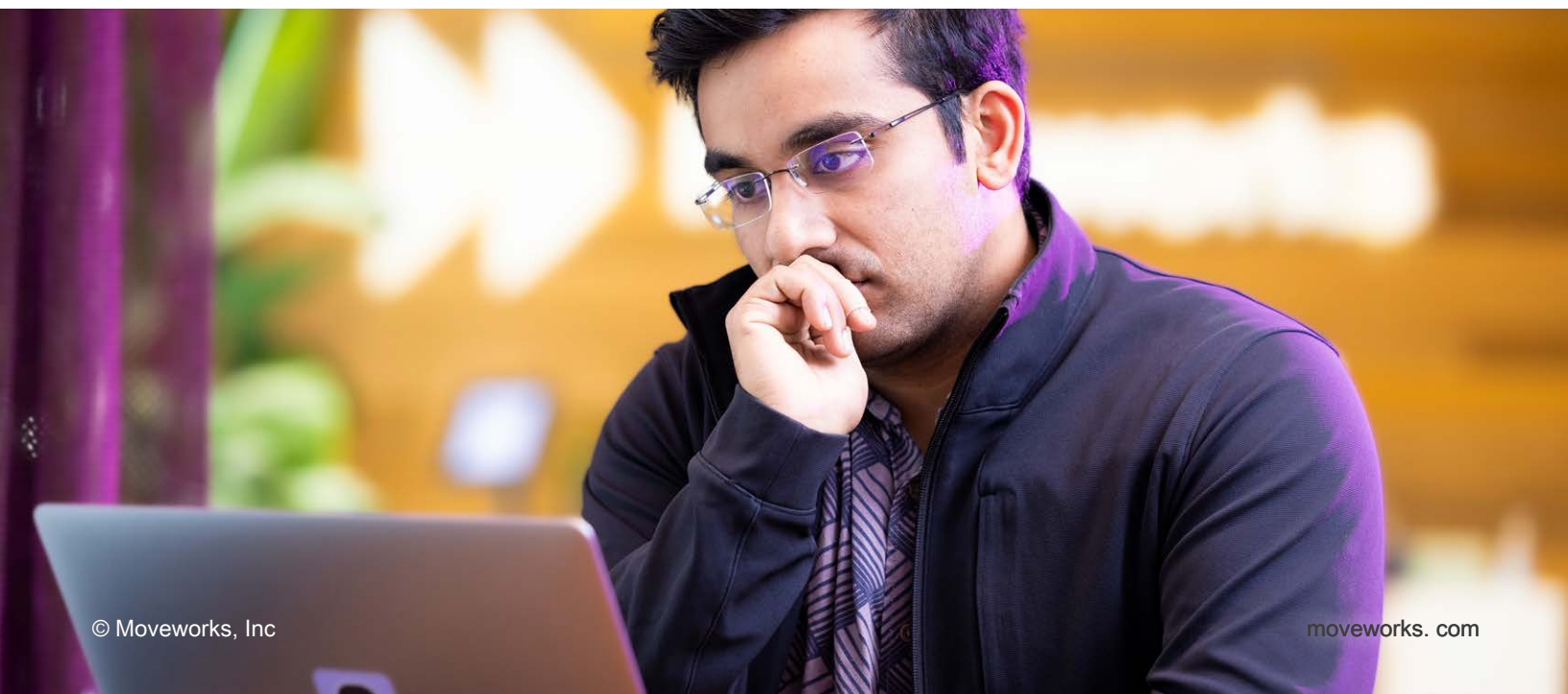
使用 Moveworks 机构自动化引擎
释放 AI 代理

传统自动化平台的挑战

厌倦了无尽的构建和管理复杂自动化过程以及令开发人员感到压倒的任务循环吗？随着您组织的SaaS景观扩展至1000多个应用程序甚至更多，对技术团队构建高效集成的压力只会越来越大。

因此，您的业务在后台雇佣专家以重新启动流程，并依赖开发人员通过构建无数自动化来填补空白。然而，使用传统的API驱动方法和iPaaS平台来构建自动化效率低下、繁琐且无法满足需求。

今天的自动化工具高度依赖基于API的过程。虽然这在处理可预测和结构化任务时效果良好，但在应对人类语言的动态特性时可能会遇到困难。传统iPaaS平台在配置预定义的工作流程方面表现出色，但在AI代理的时代可能力不从心。简而言之，这些传统的自动化方法效率低、复杂且往往耗时较长。



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。 不同于传统的SaaS应用程序依赖用户发现和导航界面，AI代理使用大型语言模型 (LLMs) 为用户提供自动化服务。

理解目标，制定计划，并执行相关的工具调用（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系统能够显著提高企业的效率并提升员工的 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

代理自动化提供了一组革命性的工具，赋予AI代理能力，以弥合人类语言与结构化系统API之间的差距。该平台使开发者能够创建能够理解模糊指令并将其转化为更精确行动的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Open AI的o1、Anthropic的Claude 3.5以及Google的Gemini Pro 1.5，日益强大 (更大的上下文窗口、更好的推理能力、更多的模态)。这使得推理和规划的能力得以扩展，但 **还有更多的建立 AI 代理。**

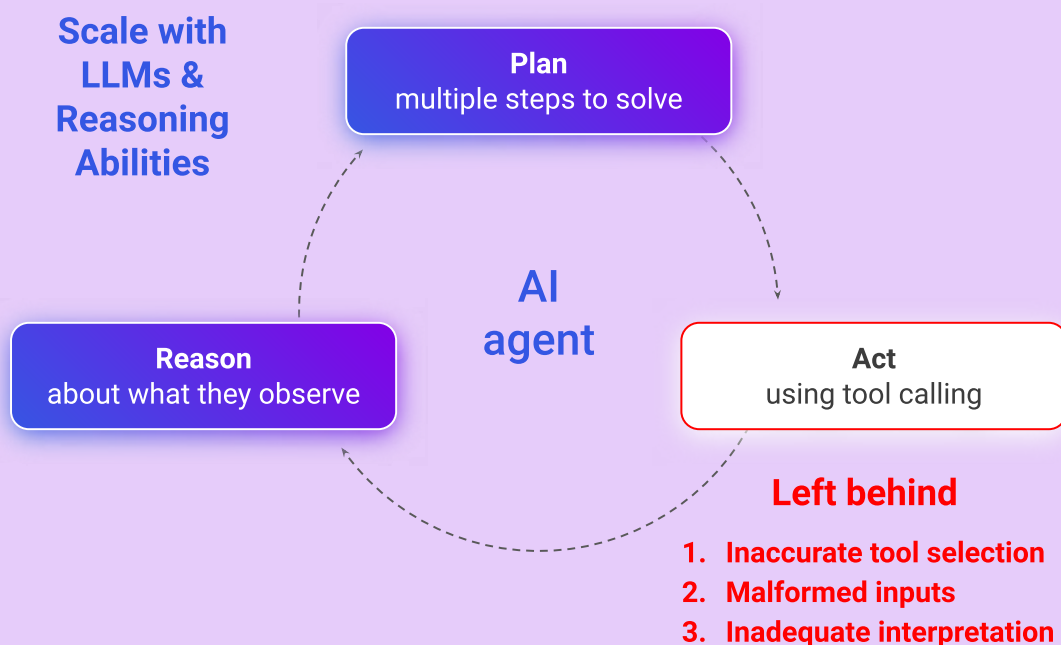
一些开发者可能错误地认为，LLMs可以直接通过与其他系统相同的API与业务系统进行交互。尽管API允许你与业务系统互动并使这些系统进行通信，但它们本身并不构成集成。每个之前使用过API的开发人员可能都能理解，集成需要的不仅仅是API——需要在某个地方编写代码。

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、Wor kato、Microsoft Power Automate、ServiceNow Flow Designer、Salesforce Flow Builder、Mulesoft等) 允许开发人员编写代码以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和中间件旨在连接精确且确定性的API到其他API。但AI代理需要将模糊且含糊的人类语言连接到API。

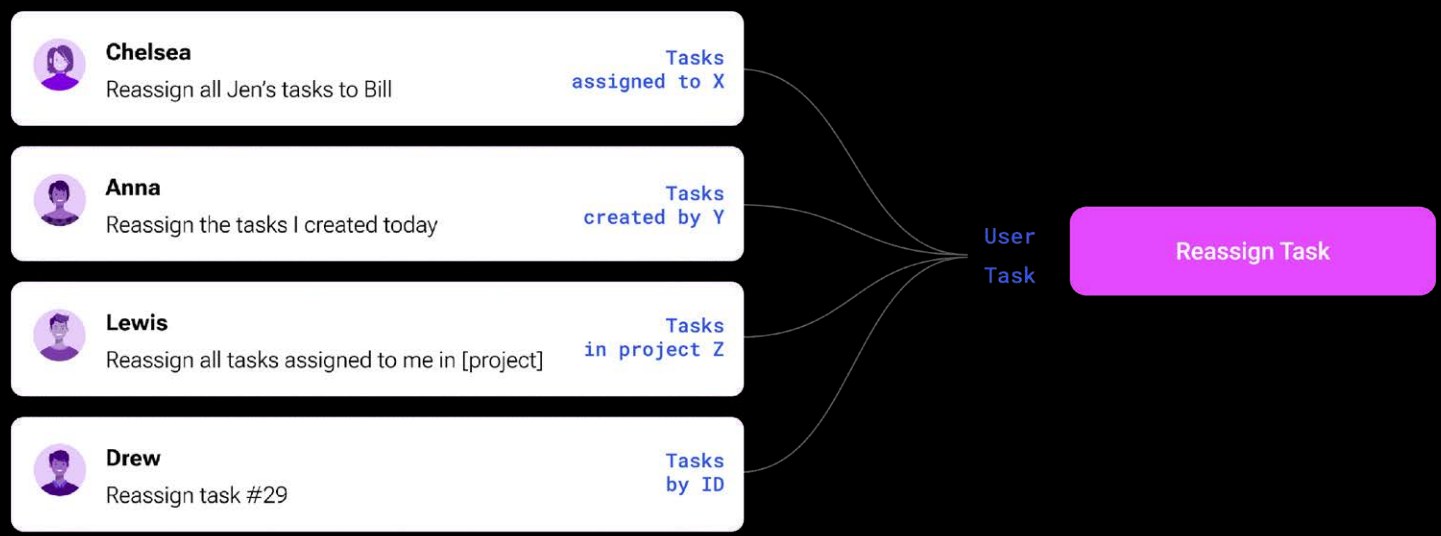
如何 AI 代理工作



让我们举一个简单的例子。

说我想拥有一个能够帮助我管理任务（创建新任务、更新现有任务、重新指派任务等）的代理。为了构建这样的代理，我们可以想象我们需要暴露一个 **重新分配任务 API**。它需要(1) 任务 ID 和(2) 用户 ID 来分配给它。

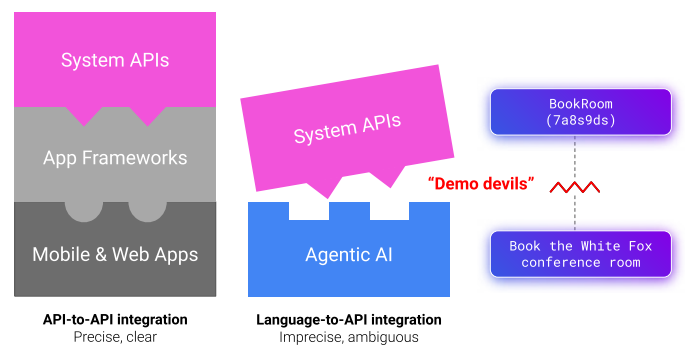
但是人类语言是混乱的。您的用户可能会通过数十种方式指定这些输入：



这些限制正是为什么REST API和传统自动化平台并非为AI代理设计的原因。它们往往缺乏关键能力，无法克服由于不准确的工具选择、不正确的输入以及不连贯的响应所带来的挑战。

系统API与代理AI系统之间的那片空白地带代表了当前开发AI代理的“尚未完全准备就绪”的现实。这就是Demo恶魔们生活的地方。

缺乏合适的底层工具，开发者被迫让iPaaS的圆钉塞入代理AI的方孔中。因此，开发者可能会试图通过大量无法维护、不可扩展的代码（技术债务）来弥补差距，从而仅能产生劣质的结果。



当企业需要将AI代理部署到成百上千名员工时，“在我的沙盒中有效”在出现问题时不是一个合理的回答。企业对AI代理的投资往往难以得到实际应用——它们经常被困于作为科研项目和演示阶段，因为这些投资缺乏足够的稳健性和成熟度，无法在全业务范围内可靠地部署。

优先考虑赋予开发人员自由的工具 到错综复杂的设计 并且通过高级逻辑和自主性来优化AI系统。空白空间是导致AI代理尚未普及的原因。在传统自动化平台的限制下，AI代理可能无法充分发挥其潜力。

简而言之，使用iPaas工具构建代理型AI系统往往无法实现预期的代理能力。此外，这一开发过程甚至可能对高级技术团队构成挑战，并消耗大量资源，从而分散对战略举措的关注。

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，旨在促进企业平台与企业副驾之间的无缝集成，超越传统自动化工具的局限。它允许直接将对话转化为API，利用高级推理引擎，并访问关键数据，为开发更智能、反应更灵敏的AI系统铺平道路。

导航超越iPaaS的限制涉及采用旨在解决代理AI复杂需求的平台。这意味著



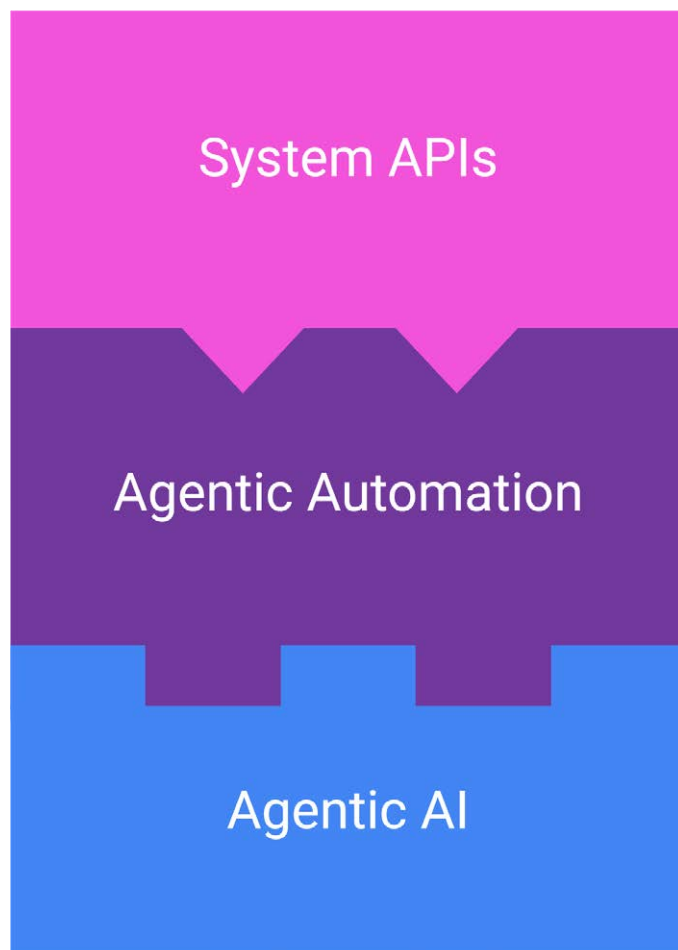
使用 Moveworks 机构自动化引擎释放 AI 代理

为了赋能开发者突破传统自动化平台的限制，Moveworks 设计了一种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，这一引擎解锁了更高的效率，从而变革了企业自动化复杂工作流的方式。

代理自动化引擎从其核心被设计为构建能够连接代理AI的语言和商业系统结构化数据的自动化。这个代理自动化引擎成为了新的核心动力。

Creator Studio，开发人员在 Moveworks 平台上构建 AI 代理。

通过这种方式，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，开发者能够将所有开发集中到一个平台上，消除代码蔓延并简化部署实践。

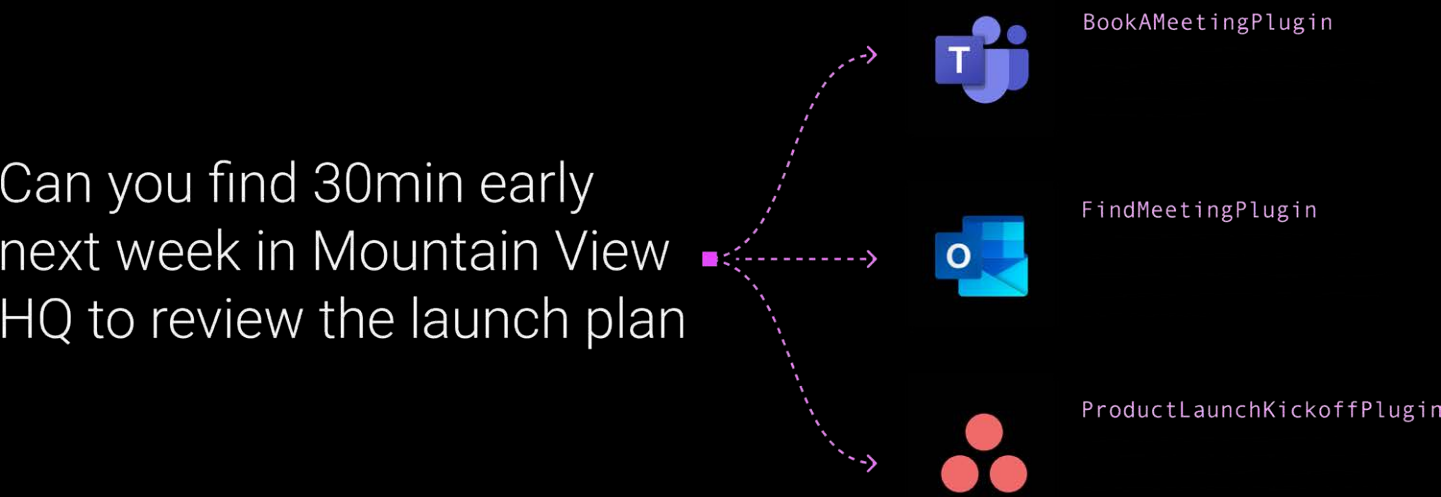


由Agentic自动化引擎驱动，开发者能够构建插件，这些插件被Moveworks Copilot使用。Agentic自动化引擎具备以下关键功能：

清单生成器

一种超越 mere 提示和语音命令的与大语言模型（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以及如何更有效地将它们映射到用户需求。

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ID。例如，它可以将“AC ME账户”转换为其Salesforce ID“00ORd0000040V9ZMAU”。这使得AI代理能够正确识别业务对象并成功执行任务。

"me"	<person>_Ava Chang
"my boss"	<person>_Diana Icard
"early next week"	<date>_20241007-20241010
"Mountain View"	<OfficeSpace>_MTV Office
"Rajat"	<person>_Rajat Patel

在此之前，开发者需要尝试解析文本并在他们的iPaaS内部操作字符串，这不可靠且导致了出乎意料的结果。

Policy Validators

大语言模型（LLMs）能够很好地处理不确定性，但其指令可能存在被误解的风险，甚至可能被破解。商业规则是不可违背的规定。你不希望有人为两人会议预订了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。我们的策略验证器能够在推理引擎中增加额外的一层，以确保这些政策得到严格执行——无论你添加多少条政策。

在此之前，开发者尝试在自然语言中添加指令，但模型往往会误解这些指令，或者无法正确执行。

策略验证器有助于
实施您的特定策略

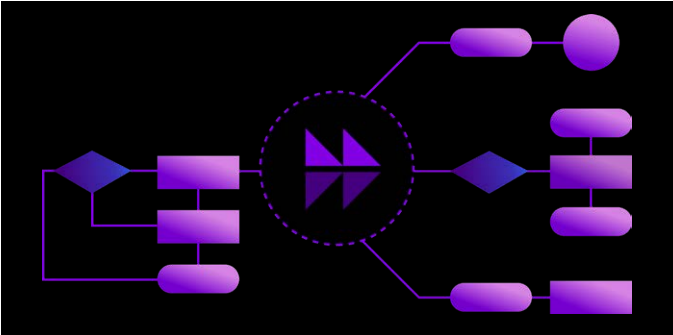


Meetings with execs require a meeting agenda	✓
Exec meetings must be scheduled 4 hours in advance	✓
Special rooms can not be reserved for more than 2 hours	✓
Meetings with virtual employees need a room with working VC	✗

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。这种方法使开发人员能够专注于构建工作原型，并让我们的推理引擎处理所有对话生成、边缘情况和失败情况。

要了解这些令人惊叹的技术及其与传统自动化技术的区别，请参阅更多信息。[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 dialogs。



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，自主人工智能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，自主人工智能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。

什么是推理引擎？

一个推理引擎是一种人工智能系统，能够理解用户的目标，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，直到成功实现原始目标。在某种程度上，它试图模仿人类解决问题的方式。

一个推理引擎使AI能够理解问题、制定策略并独立执行解决方案。这一能力正在改变企业在任务自动化和问题解决方面的Approach。在这篇博客中，我们将探讨推理引擎的工作原理、它们在自主AI中的作用以及它们如何改变企业运营的格局。

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，而非遵循预设规则或决策树。它充当人工智能助手的大脑。

```
raise Exception("Input language could not be determined")
return None
parsedInput = self.parseInputToLanguageModel(inputString, inputLanguage, context)
if not parsedInput or not self.model:
    return None
context.append(parsedInput) # Add new conversation entry to context
return (self.model.generateLLMOutput(parsedInput), context)

def parseInputToLanguageModel(inputString, inputLanguage, context):
    if self.model is None or self.model.language != inputLanguage:
        # LLM is not initialised or has wrong language, load LLM
        self.model = self.loadAILanguageModelFromDatabase(inputLanguage)
    if self.model is None or self.model.language != inputLanguage:
```



理解代理推理

代理型AI是一种可以通过自主“代理”来实现复杂目标的人工智能系统。在这种框架下，结合使用多种机器学习模型，以创建一种能够独立制定和执行基于推理的计划的人工智能，该计划可以实现用户的目标，而不仅仅局限于遵循预编程的逻辑或对话流程。

一种能够进行推理的代理型AI副驾更能全天候帮助员工处理各种任务。类似个人助理的角色，这种AI同样具备理解挑战并代为解决问题的能力。当你遇到挑战时，Copilot可以进行详尽的研究，并提出最佳解决方案——这就是推理在行动的价值所在。

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，reasoning引擎能够在必要时回溯到用户处寻求额外背景信息，确认其方向，并根据用户输入即时调整计划。

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。

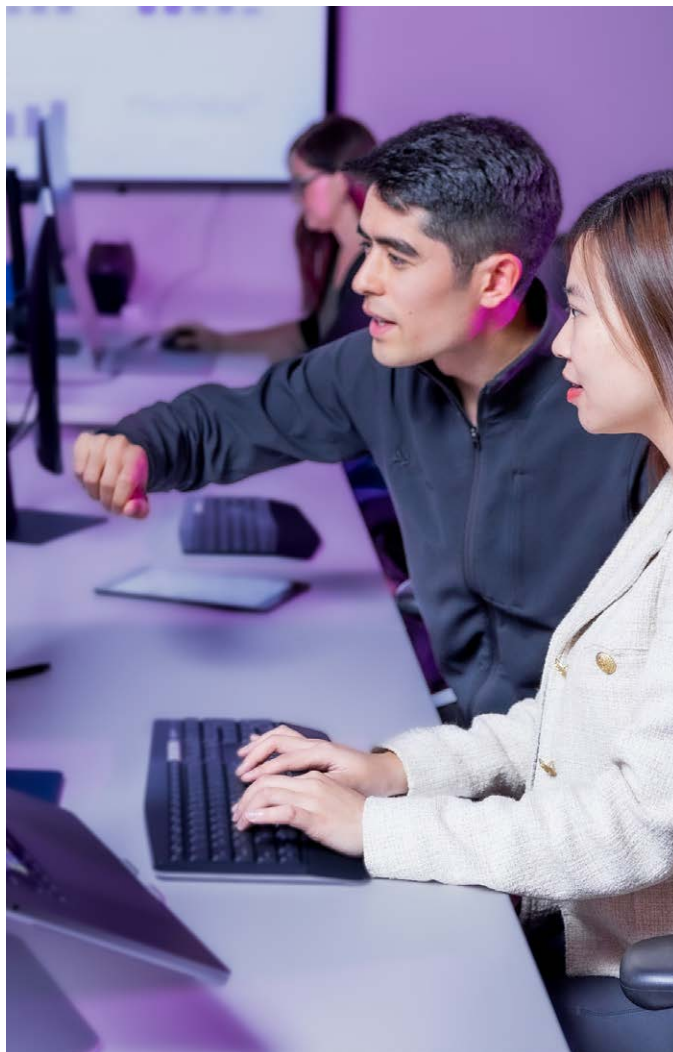
Moveworks Copilot 的推理引擎是一个基于代理的人工智能系统，展示了诸多类似人类的问题解决能力。我们的引擎利用了多个LLM的推理、决策和插件调用能力，以完成我们之前提到的各项要点中的特定元素。

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使用一套独特的工具和流程来创建特定于业务的计划，并以目标导向的方式一致地执行任何任务——这适用于全球数百万用户，且全部实时进行。让我们进一步探讨这一过程是如何实现的。

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，该过程决定了Copilot是如何回应他们的。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。

在每一阶段，我们都对Reasoning Engine的各种大型语言模型（LLMs）进行了精细调整，以应用最佳的推理和决策技巧。这一方法旨在确保每位员工的互动都能得到深思熟虑、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。第一步是通过提取元数据来丰富查询文本，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规模语言模型（LLM）在内的机器学习模型集合，以确定语句的属性，如主题、意图、情感、领域和语言。

接着，它通过利用Moveworks知识图谱将用户提及的实体映射到其标准或规范化形式，在特定客户业务背景下建立查询。这确保了Moveworks Copilot的所有组件能够理解实体引用的各种方式，包括仅存在于客户环境中的独特且具有组织特定性的实体。在此阶段，推理引擎还会检查查询是否具有毒性或冒犯性，并阻止此类请求被提供并进入系统。

下一个重要的理解要素是对话上下文。推理引擎整合了用户与机器人的先前交互，提供了丰富的背景信息，有助于识别最有效的解决方案。这包括确定用户是否开始新的话题或继续之前的话题，并解析隐含的引用，如“它”、“那”等。

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，并能够拼凑出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。这一阶段是由推理引擎将其对问题的理解和先前上下文映射到选择最适合的插件或工具以满足需求。可以将插件视为为特定用例量身定制的专业工具，并与某些系统集成。

例如，插件可以在Okta重置密码、在Google Workspace中分配用户、在BambooHR中上线员工、在AccessHub中管理访问权限、部署服务器、更新Salesforce、从分析平台拉取报告，以及在ERP系统之间同步产品数据。

列表不断延续。每个组织都拥有独一无二的一组插件，基于它们所选择的配置以及使用Creator Studio扩展平台自主研发的定制插件。

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

它随后进入一个计划-评估循环。在这个循环中，推理引擎利用其规划模块与自主评估模块相结合进行操作。

规划者和评估器迅速迭代方法，利用Chain-of-Thought分解问题并利用可用插件。这种独立的迭代过程产生了一个高质量的初步结果，消除了不必要的努力和对用户的额外负担，以引导推理引擎。从性能角度来看，我们还对此进行了优化，以确保延迟非常低，从而确保计划能够快速制定。

但我们如何知道某个特定计划在业务背景下是否合理？这通过推理引擎中的政策来实现，这些政策提供了在员工支持背景下思考问题的指导，并列出了员工支持助手应遵循的标准目标和最佳原则。这种做法赋予了推理一种立足于实际的形态，专注于具体的应用场景。

解决方案空间，并允许计划者和评估者确定候选计划的质量和有效性。

有目的地执行

推理引擎现已准备好开始执行其识别的计划。就像人类问题解决者一样，它能够应对问题，但会密切关注每一步的输出，以便如果需要，可以调整计划。

它会调用插件执行器组件，该组件负责对计划中选定的每个插件进行适当的函数调用，并监控返回的响应。当插件执行其特定任务时，它们会返回结果或错误消息，插件执行器分析这些结果和错误消息并将其发送给推理引擎，以确定下一步该做什么。

在每一个关节点，Copilot都会分析最新的可用信息，并决定是将输出总结为最终答复，还是要求用户提供更多信息，或是尝试其他方法。



另一种方法是调用其他插件。这种迭代方法确保推理引擎能够在没有人类干预的情况下，动态地尝试通过多种方式解决问题。这种灵活性内置在其核心推理方法中，模拟了人类处理类似情况的方式。

作为示例，在处理复杂的IT故障排除场景时，计划可以涉及使用搜索插件来搜索知识库文章或文件，或者提供相关的支持表单或工作流程，以引导用户通过设计的解决方案过程。因此，我们可以看出，推理和规划过程紧密配合，始终专注于用户的目标，并找到最快的有效解决方案的途径。

所有这些步骤均由推理引擎和插件以无缝、自主的方式在几秒钟内完成。推理引擎生成面向用户的响应，并附上最相关的发现的简洁、参考性摘要。更重要的是，在每一步中，推理引擎继续为可解释性提供推理步骤，这也有助于用户理解它尝试了哪些步骤以及响应是如何生成的。

如果现有的插件都无法帮助用户，Copilot将使用户能够轻松地寻求-human-支持，方式包括提交工单或与在线代理交谈。



Moveworks Copilot将强大的AI直接置于员工的指尖，帮助他们在日常工作中解决问题。推理引擎在理解用户的问题、制定解决方案以及执行相应的行动以达到相同的成功程度时，能够与人类代理进行相似的细致工作；只有AI能以更快的速度、更低的成本，全天候地完成这些任务。

机构自动化：自动化的未来

所有 Moveworks 客户都可以使用这些功能，无需额外费用。

本发布推进了我们对于Moveworks作为AI代理平台愿景的实现。当与行业领先的代理推理引擎结合使用时，新的代理自动化引擎极大地增强了开发人员构建新AI代理的能力。每一个角色、每一个SaaS应用、每一项业务都应该拥有由Moveworks驱动的AI代理。此外，使用Moveworks构建AI代理时，此发布消除了传统自动化平台的需求。

代理自动化不僅是一種新的工具——它代表了企業與技術交互方式的根本轉變。通過利用人工智能代理的先進推理能力，企業可以實現此前無法想象的效率和準確性水平。

Moveworks 的代理自动化引擎使开发人员能够以最少的努力和最大的灵活性创造出强大的复杂AI代理。随着更多企业采用这项技术，我们正见证着自动化新时代的到来——在这个时代，企业不再需要导航僵化的系统，而是能够将其需求转化为现实。

在未来展望中，我们期待开发者生态系统能够成倍增长，并真正为企业提供最需要的东西：每个业务系统都拥有一个AI代理。

了解机构自动化如何彻底改变您的业务运营

下载我们的白皮书或观看我们预先录制的网络研讨会，[了解更多信息](#)：

Agentic Automation 如何利用 AI 代理实现前所未有的效率和准确性。

- 为什么传统集成工具在构建智能，适应性强的 AI 代理方面不足。
- Moveworks 机构自动化引擎的关键组件。
- 如何在企业应用程序中构建和部署强大的 AI 代理。

不要错过这个处于自动化革命前沿的机会。

