



AI 融于人类奋斗潮流之中

IT 领导者指南之满怀信心地规模化采用 AI

如何为安全的 AI 应用、智能体的就绪状态以及可衡量的业务影响奠定基础。

面向在企业范围内扩展 AI 的 IT 和安全领导者 - 以 Microsoft 365 为基础平台，并具备针对每种场景选择合适模型的灵活性。



简介

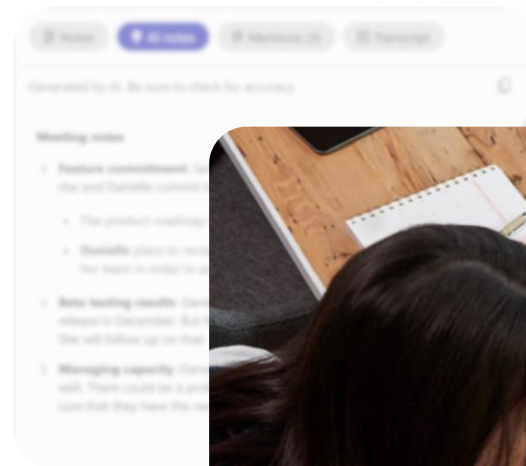
大多数企业不再纠结是否采用 AI。他们发现自己其实已经拥有了 - 数十种互不相连的工具，由不同的团队购买，并且没有特定的人进行管理。



独立企业监测显示，组织内部的大多数 AI 使用仍然通过个人、非托管帐户运行，难以被 IT 部门监控。

NETSKOPE, 2025

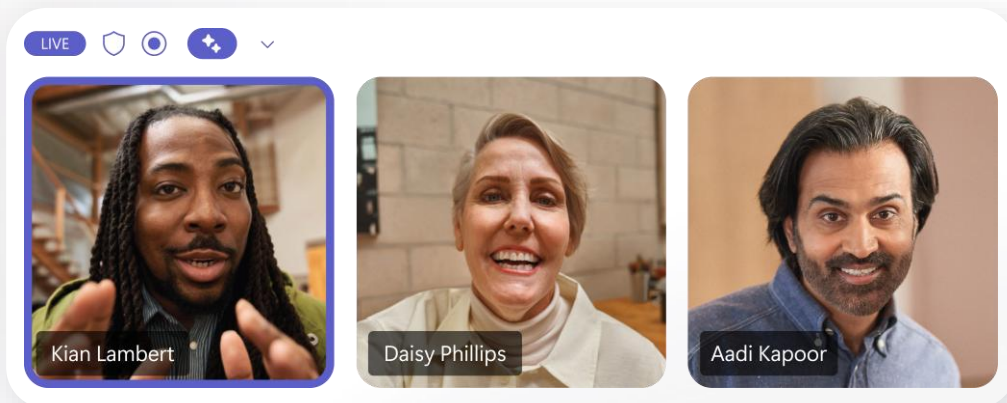
对于 IT 和安全领导者来说，这才是当下真正的挑战。你的员工已经在使用 AI 来撰写内容、分析信息、自动化重复性工作和加快决策速度。现在授权范围更广：将分散的势头转化为安全、受控的企业级能力，从而带来可衡量的业务价值，而无需搭建另一个堆栈来运行。



How can I help?

出错的代价正在不断攀升如果不加以管理，独立部署会导致数据碎片化、治理不一致、重复支出和安全盲点，而这恰恰发生在智能体开始在你的系统中执行多步骤操作的时候。现在的风险不再是错失生产力提升的机会；而是在这两者最为关键的时刻，失去可视性和控制力。

卓越的组织都采取了一项共同的举措：他们没有构建并行的 AI 技术栈，而是扩展了他们已经信任的平台。本指南阐述了 Microsoft 365 如何以及在何处作为基础发挥作用。



扩展 AI 规模不仅仅是添加工具那么简单。
它由两根相连的柱子支撑：

智能

它将人员、数据、工作流程和智能体汇聚在一起。

信任

在这些方面一致地应用安全、身份、治理和管理。

对于许多组织而言，Microsoft 365 已经具备了这样的基础 - Copilot 将 AI 引入工作流程，而更广泛的平台则提供了负责任地扩展的控制功能。而且由于 AI 本身也在不断变化，因此该基础必须保持模型灵活性 - 能够将新的和不断发展的模型引入同一个受控平台，这样你就可以为每个场景匹配最佳模型，而无需每次都重新构建安全性和治理。

本指南

01

为什么 AI 规模化现在不仅是生产力问题，而是控制问题

02

阻碍试点项目推进的技术和运营障碍

03

安全扩展 AI 的五部分模型 - 本指南的核心

04

模型选择如何在不增加风险的情况下保持灵活性

05

一份评分式自我评估，用于衡量你的智能体准备度

06

从何处着手以及 Microsoft 如何提供帮助

为什么 AI 试点项目在规模化之前会遇到阻碍

你很可能已经在 AI 试点方面投入大量资源，并见证了真实成效：节省日常任务时间，更快地获得见解，提高工作流程效率。将这些成效扩展到单个团队之外时，推进速度会变慢。



Gartner 预测，至少有 30% 的生成式 AI 项目在概念验证后被放弃，原因包括数据质量差、风险控制不足、成本不断攀升以及商业价值不明确。

GARTNER, 2024



IT 领导者在尝试扩展规模时遇到的四个障碍

01

工具的无序扩展导致复杂性

随着团队采用不同的工具，你会积累重叠的功能、重复的支出、碎片化的体验，以及控制不一致。最初的实验逐渐转变为运营负担，使成本、安全性和价值变得更难管理。

02

价值变得难以衡量

早期试点项目侧重于个人生产力，但最终需要展示更广泛的业务影响 - 更优化的流程、更快的决策、持续的采用，以及对哪些投资真正创造价值的清晰认识。

03

治理滞后于采用

业务团队希望能够立即获得新功能；安全与合规负责人则需要确信各项控制措施已到位。平衡这两者已成为企业 AI 的决定性挑战。

04

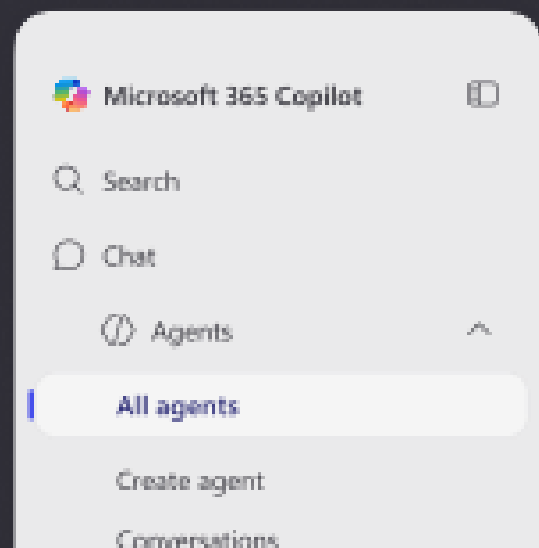
智能体式转变提升了要求

随着智能体开始执行多步骤任务，它们对身份、访问、权限、监控和生命周期管理提出了新的要求。你需要确信，今天的平台决策能够支持未来的智能体，而不会在可见性或控制方面产生新的缺口。

一种全新 AI 规模化模型

五大基础因素

第一波 AI 浪潮以实验为主。接下来是关于如何实现大规模运营 - 在保持可见性、控制力和灵活性的同时，从你已有的投资中获得更多价值。五大基础因素始终区分着那些从试点阶段迈向企业价值的组织。它们是本指南后续所有内容的基石。





在规模化环境中最大化 AI 价值

模型建立之后，下一个问题是 AI 在哪些方面能创造可衡量的价值。普遍存在一种误解，认为价值来源于技术本身。价值来源于 AI 与你已经依赖的工作、数据、安全和管理实践的深度整合 - AI 只有在扩展你现有系统而非孤立运行时，才能发挥最大效能。

组织通常从个人生产力入手 - 总结、起草、调研、创作。这些都是很有价值的切入点。当 AI 推动工作流程和业务流程转型时，更广阔的机遇将呈现。

以下三个问题有助于确定 AI 和智能体能够产生最大影响的领域：

1. 知识在不同系统中的分散程度体现在哪里？

重要信息常常分布在各个应用程序、文档和团队之间，造成执行上的延迟和不一致性。

2. 工作流程在人员和系统之间的哪些地方出现中断？

智能体可以协调任务、触发操作并连接系统，使流程推进更加顺畅。

3. 变革是否仅限于可见的工作，而不是其背后的流程？

许多组织只关注表层的生产力提升，而最大的影响则来自于重新审视决定结果的后端流程。



实际落地架构如下

在 Forrester 对智能 Microsoft 365 Copilot 副驾驶® 的研究中，受访者表示，会后总结的完成时间由 30 分钟缩短至约 5 分钟；一家专业服务公司每月提交的销售提案数量增加了 10%，且成交周期由 30 天缩短至 20 天。

一项由 MICROSOFT 委托开展的 FORRESTER TOTAL ECONOMIC IMPACT™ 研究。



这种价值可以从 Copilot 中由 Microsoft 及其可信赖的合作伙伴构建的现成智能体开始，然后通过由你团队基于自身知识来源、数据、系统和流程创建的自定义智能体进一步扩展。目标并不是单纯追求自动化。它旨在帮助人们在他们已经使用的 Microsoft 365 应用中，花更多时间发挥专业能力、做出决策并创造价值。



优化成本，简化增长

随着应用范围的扩大，你将面临一个新的运营问题：
AI 实际应用在哪些领域？哪些投资创造了价值？成本如何变化？以及哪些功能存在重叠？缺乏这样的可视性，AI 的发展速度将超过你管理支出和将投资与成果关联的能力。

平台方法通过将 AI 的采用与你已有的生产力、安全性、管理和治理投资相连接，从而简化这些决策。整合降低了运营复杂性，并为员工提供了更一致、更熟悉的体验。它还能让你以真正的可见性来管理 AI 支出 - 将投资与可衡量的结果联系起来，了解哪些能力能够创造价值，并决定在哪些方面扩大自动化规模，在哪些方面人类的专业知识仍然至关重要，以及如何平衡这两者。

交流内容从

我们有多少 AI 工具？

↓ 转变为

我们的 AI 投资是否有效地推动了业务目标？

在面向未来的平台上自信创新

创新和控制常常被视为相互冲突的优先事项。实际上，你需要两者，既要让员工有探索的自由，也要有创新能够以负责任方式规模化的信心。这种信心正是信任支柱的体现。



以下是在实际应用中的具体体现

身份和访问

随着 AI 更深入地连接到业务数据和工作流程，扩展你现有的身份和访问控制至关重要，以确保每一次体验都建立在正确的权限、用户和上下文之上。

智能体治理

随着智能体承担更多任务，你需要能够了解它们如何运作、采取了哪些行动，以及这些行动如何与政策保持一致，从而在可追责的前提下实现创新。

数据保护

AI 的成效取决于可信数据。内置保护有助于保持对 AI 体验中信息访问、使用和共享方式的信心。

可应对未来的平台

随着 AI 的发展，平台也随之演变，包括新模型、多模型灵活性、持续创新，以及如 Cowork（新智能体体验名称）和 Scout（新智能体体验名称）等新的智能体体验。这种适应能力让你能够在不重建基础或中断工作的情况下采纳下一步发展。

上下文与智能

AI 的价值取决于其所理解的背景。借助 Work IQ，Copilot 可以利用贵组织的数据、内容和工作方式，因此提示都基于相关的背景，可以产生更有用、更个性化、更可操作的结果。



评估智能体准备度

利用此自我评估，将指南中的原则转化为企业、IT、安全和转型领导者之间切实可行的准备对话。
对每项陈述进行 1 到 3 分的评分，然后将你的分数相加，并在下方查看你的分数等级。

	1	2	3
准备度陈述	未启动	进行中	已建立
战略与领导力			
已确立高层支持和清晰的 AI 愿景。			
AI 和智能体相关举措与可衡量的业务成果对齐。			
业务流程准备度			
已确定 AI 和智能体的高价值工作流程和用例。			
关键业务流程、依赖关系和成功指标已被理解。			
技术和数据准备度			
员工可以在需要时访问可信信息。			
已确定高价值知识来源和商业数据。			
安全性和治理准备度			
已建立明确的数据访问、保护和合规控制措施。			
治理策略可以在 AI 和智能体相关场景中一致地应用。			
存在用于管理智能体生命周期、监控和监督的流程。			
组织准备和采用			
员工已做好有效使用 AI 的准备，并制定了持续采用和变更管理的计划。			
利益相关者了解 AI 和智能体将如何支持工作方式的开展。			

准备度评分

将你在所有 11 项陈述中的得分相加（最高 33 分），然后查找你的分数段：

你的分数	范围	接下来要关注的内容
随需而扩	27–33	基础稳固。优先考虑你的第一个启用智能体的场景，并锁定价值指标 - 从步骤 4 开始。
初出茅庐	18–26	地基正在形成。在扩大规模之前，先弥合治理、数据访问和成功衡量标准方面的差距 - 从第 2 步开始。
早期	11–17	从战略、高管支持和确定高价值工作流程开始 - 从第 1 步开始。

着手点

评估准备度之后，下一步是将理解转化为计划。AI 规模化通常并不是从购买更多工具开始。首先要找到 AI 能够产生最大影响的领域，以及你准备好以负责的方式进行规模扩展的领域。

一个实用的初步流程：

01

挖掘高价值工作流程。

02

评估组织内当前 AI 的使用情况。

03

利用你已运行的平台评估治理和安全准备度。

04

优先考虑首批启用智能体的场景。

05

定义采纳率和价值指标。

06

制定实现长期扩展的路线图。

有意识地采用平台驱动方式的组织更能平衡创新、治理和商业价值。

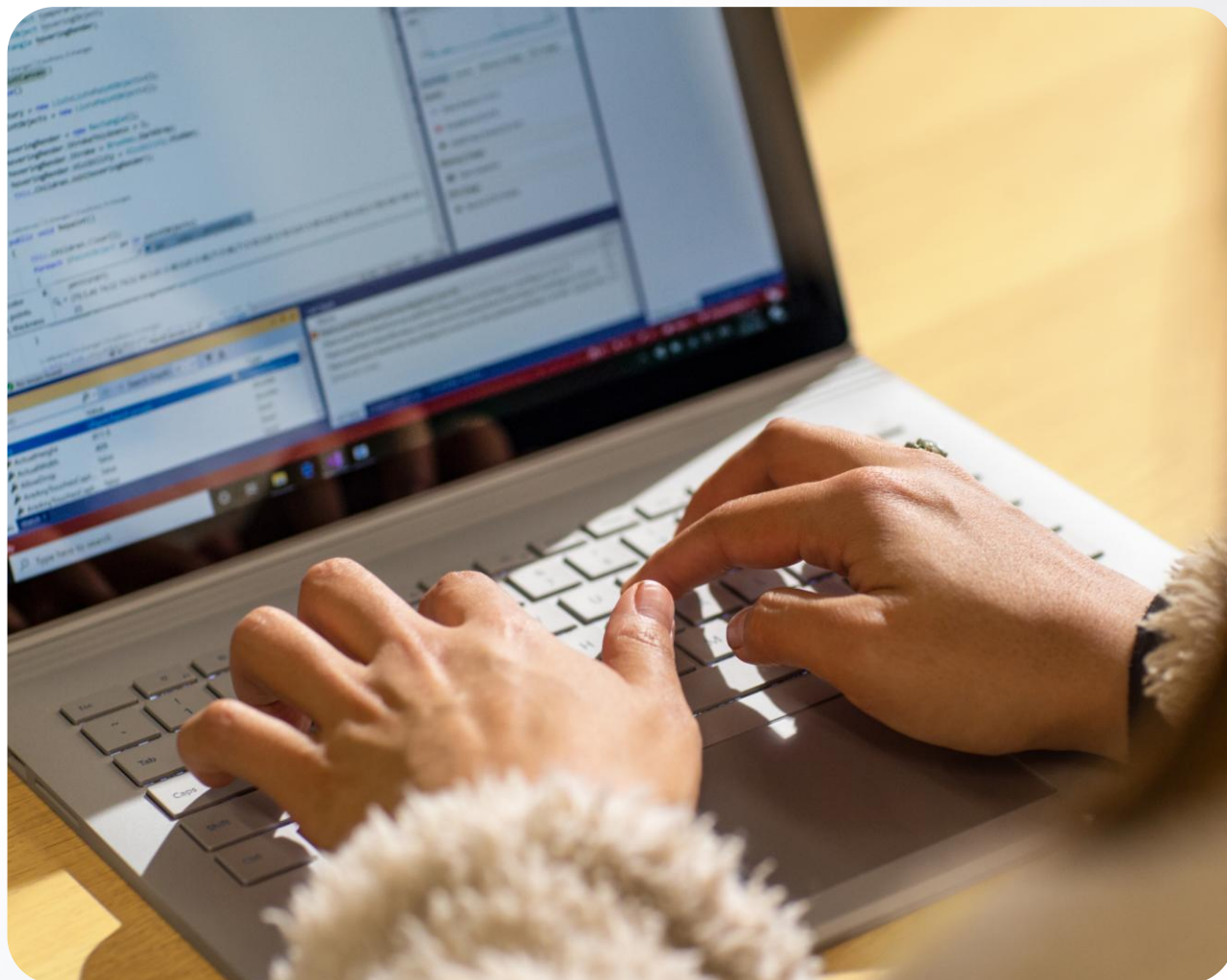
Microsoft 如何提供帮助

本指南中的选择都指向一个结论：下一代工作需要的不仅仅是独立的 AI 工具。它需要一个集成平台，将生产力、业务数据、安全、身份、治理、管理和 AI 汇聚在同一个基础平台之上。

Microsoft 365 E7 正是单一集成解决方案的基础。它由四个基本组成部分构成：

- Microsoft 365 E5 用于提高生产力、安全性和管理；
- 工作流中适用于 AI 的智能 Microsoft 365 Copilot 副驾驶®；
- Microsoft Agent 365 用于智能体管理；以及
- Microsoft Entra 套件用于高级身份和访问控制。

简而言之：E7 是 E5 加上扩展所需的 AI、智能体和身份层 - 作为一个整体进行治理。





只要基础打好，就能获得实实在在的回报。



在 Microsoft 委托 Forrester Total Economic Impact™ 研究中，一个拥有 25,000 名员工的综合型组织模拟了其对于智能 Microsoft 365 Copilot 副驾驶® 的投资在三年内实现 116% 的回报，投资回收期不到 11 个月，且每位用户每月平均节省约 9 小时。

FORRESTER, 2025

值得注意的是，该综合组织在部署前首先投入了数据清理和权限管理工作 - 这提醒我们，AI 的价值依赖于受监管、权限良好的数据，而这正是平台方法旨在提供的。

随着模型选择逐渐丰富，Microsoft 的优势不仅仅体现在可以获取更多的模型。它能够在同一个可信平台上采用模型多样性，该平台用于管理人员、数据、应用和智能体，而无需在评估、调整和维护方面重复投入精力。

不是将各自独立的 AI、身份、安全、治理和智能体管理工具拼接在一起，E7 而是将它们连接起来，使人们在 AI 推动工作前进的同时保持控制权。对于想要更进一步的团队，Copilot Studio 让他们能够根据自身流程、知识和系统来构建和管理专属智能体。

通过 Microsoft 365，让智能与信任融入工作流程。你可以评估并使用合适的模型，安全合规地进行管理，并在模型和智能体持续演进的过程中自信地扩展 AI，无需为每个模型和智能体单独制定运营模式。这就是将 AI 融入人类雄心壮志的意义所在：以人为本，以人的抱负为工作发展的核心。



采取后续行动

Netskope, Cloud and Threat Report:Shadow AI and Agentic AI, 2025 年 - 企业 AI 的使用大多通过个人、非托管帐户进行

Gartner, 《Gartner 预测到 2025 年底, 30% 的生成式 AI 项目将在概念验证后被放弃》, 2024 年 7 月。

Forrester Consulting, The Total Economic Impact™ of Microsoft 365 Copilot, 受 Microsoft 委托, 2025 年 (116% 的三年投资回报率; 投资回收期不到 11 个月; 每位用户每月节约约 9 小时); 以及 New Technology:The Projected Total Economic Impact™ of Microsoft Copilot for Microsoft 365, 受 Microsoft 委托, 2024 年 4 月 (会议回顾和销售提案示例)。

注意: 发布前, 应根据 CELA 的首选引用列表对外部 (非 Microsoft) 数据进行确认。可以用具名的 ME7 客户案例替换实践示例。



立即试用 智能 Microsoft 365 Copilot 副驾驶®

了解 AI 如何在工作流程中帮助你的团队创造、协作, 并以更多背景信息和控制权更快推进工作 - 立即启动 Copilot 对话助手, 并将其应用于实际任务中。



借助 Microsoft 365 E7, 自信地扩展 AI 规模

将生产力、安全性、身份、AI 和智能体管理整合到一个整合解决方案中, 旨在帮助你以更高的信心、更强的控制力和更大的业务价值扩展 AI。

