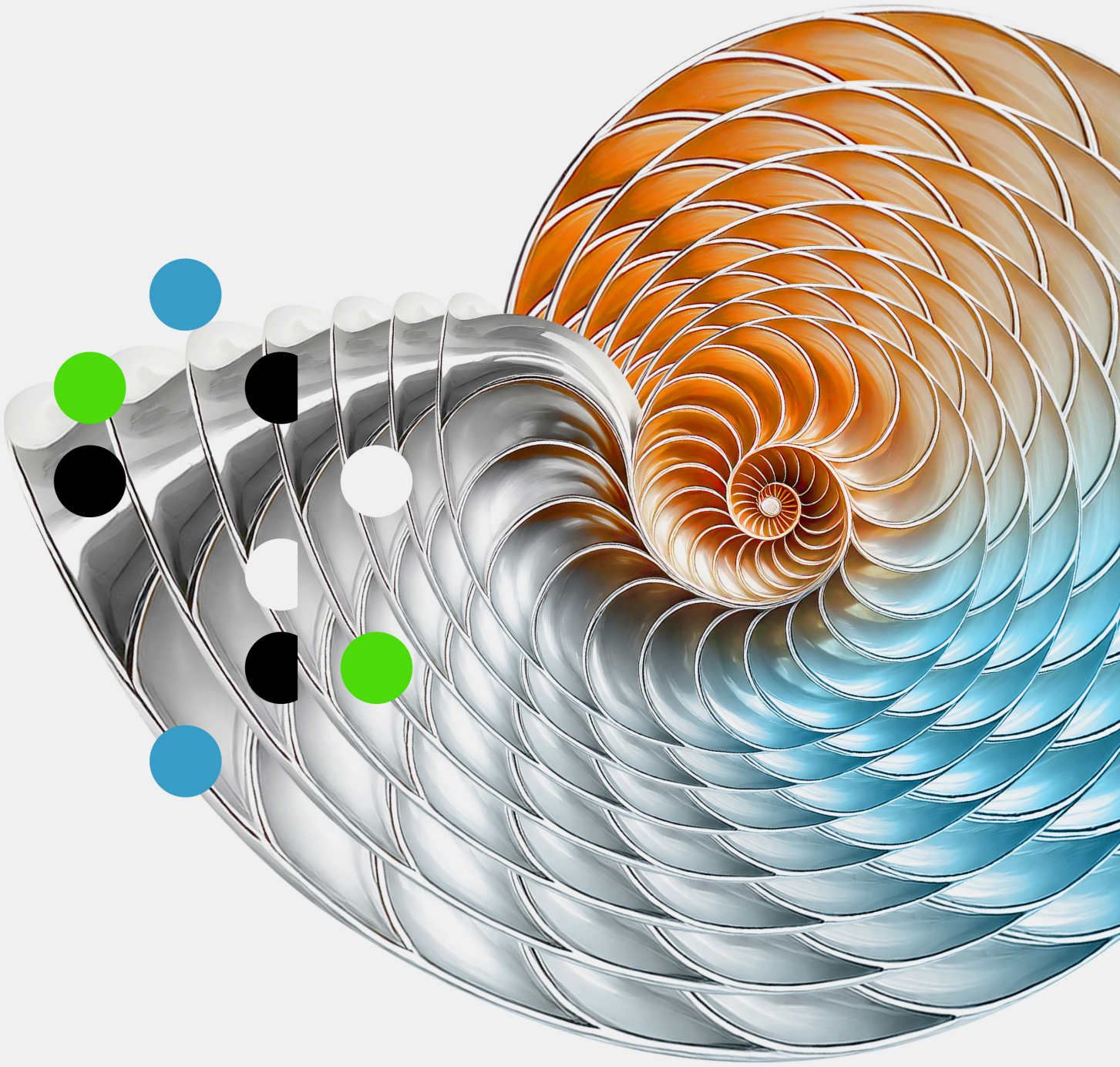
# 技术趋势2026



Deloitte.
Insights

# 目录

# 执行摘要

去年的《技术趋势》报告预测，AI将如同电力一般，成为一种基础要素，无缝融入各类产品和服务之中。今年这份《技术趋势》报告（第17版年度报告）印证了这一假设。如今，企业技术的各个领域都受到AI的影响，对智能运营的需求影响着从计算硬件到实体机器人技术等方方面面的决策。去年，企业的重点在于开展概念验证项目和探索技术的潜在可能，而今年则完全聚焦于技术的规模化应用。各行各业的企业都在将AI驱动的流程投入实际运营。原因很简单：企业领导者已经意识到，要实现差异化竞争优势，关键在于运用AI推动自动化、创新和业务增速提升。

## 创新的复合效应

技术领导者正面临从AI试验阶段向可衡量价值创造阶段的关键转变。如今，创新呈现出指数级的复合增长态势：生成式AI仅用两个月就吸引了约1亿用户，而电话达到5000万用户则用了50年。这种增长形成了一个不断加速的飞轮效应——技术、数据、投资和基础设施方面的进步相互促进，共同加速发展。传统的基础设施和循序渐进的改进流程已难以跟上这一速度。要取得成功，仅依靠先进技术是不够的，企业必须重新设计业务流程，而非仅仅对现有流程进行自动化改造；要将投资与业务成果紧密关联，并快速执行相关举措。

## 物理AI：探索AI与机器人的融合

物理AI正推动机器人技术发生变革，使其从预先编程的机器转变为能够在复杂环境中自主感知、学习和运行的自适应系统。这些能力已在工业机器人、自动驾驶汽车、无人机以及其他各类系统中得到应用。目前，该领域面临着培训缺口、安全隐患和网络安全风险等挑战，但成本的下降正推动其应用范围从智能仓储和供应链运营向更广泛的主流领域拓展。人形机器人将成为下一个前沿领域，预计到2035年，工作场所的人形机器人数量将达到200万台。未来，生物混合机器人和量子机器人技术也可能成为新的发展方向。

## 未雨绸缪：为数字员工做好准备

尽管人们最初对智能体AI充满热情，但许多企业在应用智能体后，尚未实现显著的业务变革。这是因为大多数企业只是对现有流程进行自动化处理，而没有从根本上重新设计业务运营模式。在接受调查的企业中，仅有11%已将智能体系统投入实际生产应用，面临的挑战包括遗留系统整合难题、数据架构限制以及治理框架不完善等。领先企业正在采取以智能体为核心的流程重构方式，利用新兴协议实现多智能体协同调度，并将智能体视为需要专门管理框架的硅基劳动力。这其中涵盖以智能体为代表的数字员工入职管理、绩效跟踪以及成本管控等方面。未来，智能体的自主程度将逐步提升，人机混合劳动力模式将成为主流，同时企业还将利用智能体生成的数据实现持续学习，这些变化将彻底改变企业的运营和竞争方式。

## 积极反思：优化AI基础设施策略

随着AI从试验阶段迈向实际生产应用，企业在基础设施建设方面面临着难题。尽管成本大幅下降，但由于使用量激增，企业在AI方面的总体支出仍在急剧增加。许多企业正面临一个临界点：对于大规模使用量而言，云服务的成本已高得难以承受，部分企业每月的云服务账单金额高达数千万美元。领先企业正在采用战略性的混合架构：将云服务用于处理可变工作量，本地部署用于稳定的生产任务，边缘计算则用于低延迟需求的应用场景。这种架构可能需要专门构建的AI数据中心，配备针对图形处理器（GPU）优化的硬件、先进的网络系统以及专门的冷却设备。未来面临的挑战包括员工技能重塑、利用AI智能体管理基础设施，以及推动可持续计算创新（如采用可再生能源供电的数据中心，甚至可能出现轨道数据中心）。

## 脱胎换骨：重构一个AI原生技术组织

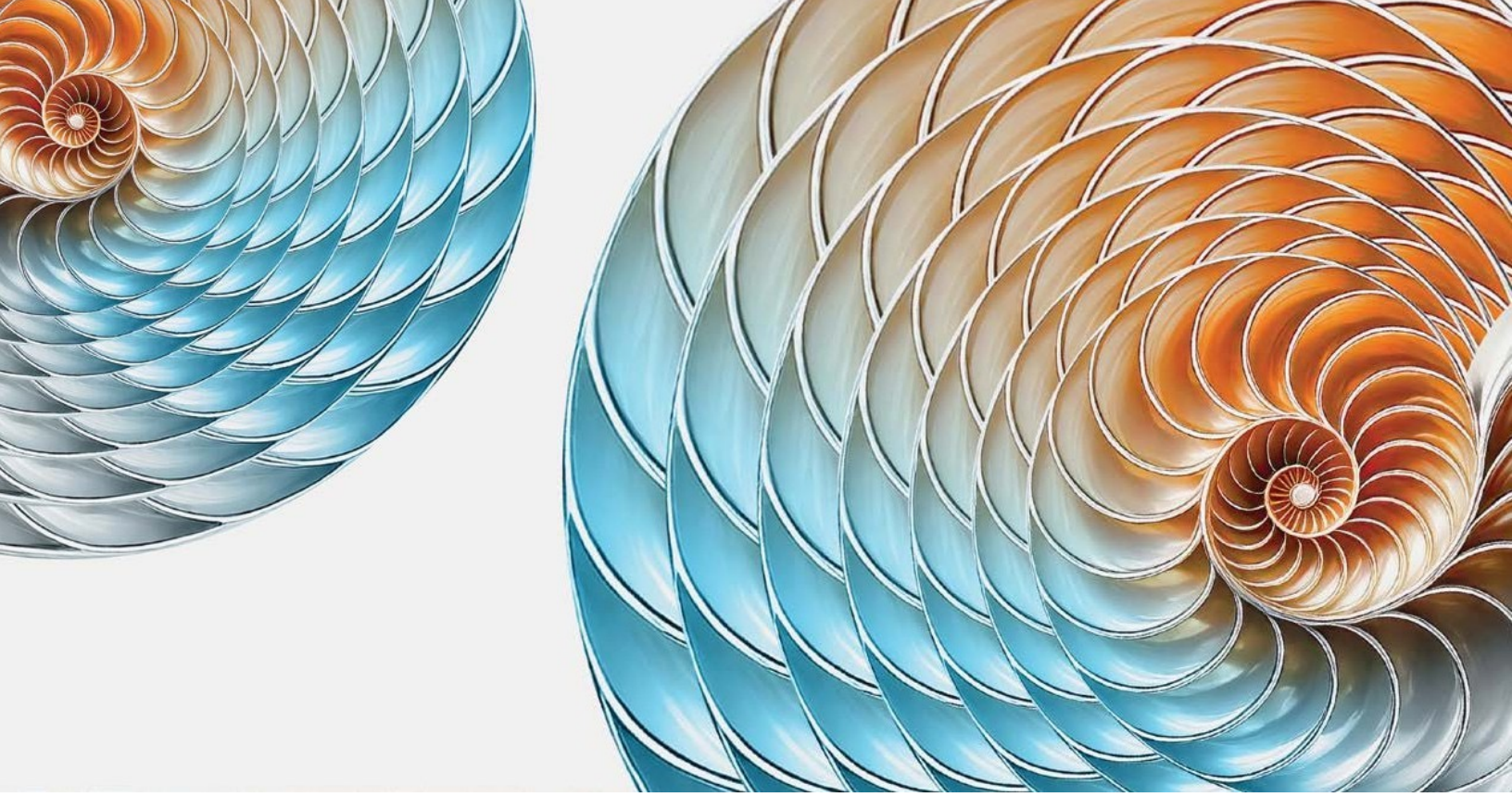
AI正在从根本上重构技术组织，其影响远超简单的自动化改造。64%的企业正在增加AI领域的投资，AI相关的技术预算也在不断上升，企业的工作重点正从基础设施维护转向战略引领。领先企业将AI计划与可衡量的业务成果相结合，设计具备灵活性的模块化架构，并围绕人机协作重新制定人才战略。新的职业角色不断涌现，如AI协作设计师、边缘AI工程师和提示工程师等。同时，首席信息官（CIO）的角色也在转变，从技术战略制定者逐渐成为AI推广者和协调者。未来的技术组织将具备智能体架构、以产品为导向的精简团队、人机混合劳动力模式、自适应治理机制以及面向生态系统的创新模式。要取得成功，企业必须勇于持续变革，大胆重新规划业务运营模式，而非局限于渐进式的微小改进。

## 走出困境：使用AI进行网络防御

AI在网络安全领域引发了一个悖论：推动业务创新的技术能力，同时也带来了新的安全风险。企业面临着来自影子AI部署（未经授权的AI应用）、对抗性攻击以及AI系统固有漏洞等方面的威胁，这些威胁涉及数据、模型、应用程序和基础设施四个领域。企业可以调整现有的安全措施，通过健全的访问控制、模型隔离和安全的部署架构，应对AI特有的安全风险。与此同时，AI也为解决其自身带来的安全漏洞提供了强大的新能力。领先企业正以防御为目的运用AI技术，例如利用AI智能体开展红队测试、进行对抗性训练，以及以机器速度实现自动化威胁检测。未来的挑战将包括AI与实体基础设施融合带来的风险、自主网络战，以及量子计算和太空安全威胁等。要在这一领域取得成功，企业必须从AI项目启动之初就将安全理念融入其中，将安全视为推动创新的助力，而非制约创新的因素。

## 拨开迷雾：AI进阶过程中值得追踪的技术趋势

《技术趋势》报告深入探讨了五种正在重塑企业运营方式的技术发展趋势，但在任何时期，影响企业的趋势都远不止这五种。另有八个相关的“信号”同样值得关注，包括基础AI模型是否可能进入发展平台期、合成数据对模型的影响、神经形态计算的发展、边缘AI的新兴应用场景、AI可穿戴设备的增长、生物识别认证的发展机遇、AI智能体对隐私的影响，以及生成式引擎优化技术的兴起。这些信号中，有些可能会发展成为具有主导性的技术力量，有些则可能逐渐淡出人们的视野。但所有这些信号都反映出一个共同的核心现实：技术变革的速度已发生根本性转变，那些能够及早识别这些趋势模式的企业，将有更充足的时间进行调整和适应。



# 创新的复合效应

## 随着技术创新和采用的加速，五个趋势揭示了成功的组织是如何从试验阶段迈向实际价值创造阶段

*Kelly Raskovich*

我一年中的大部分时间都在与技术领导者交谈，询问他们哪些做法是有效的，哪些做法是无效的，以及有哪些事会让他们彻夜难眠。最近，这些对话有了新的特征及含义。

过去，大家常问的是“我们能用人工智能做什么？”，而现在问题变成了“我们如何从人工智能试验阶段迈向实际价值创造阶段？”。关注点已从无休止的试点项目转向获取实实在在的业务价值，而且所有人都感受到了紧迫感。这种紧迫感并非仅仅因为技术在不断进步（尽管技术确实在进步），更重要的是技术变革的速度本身已大幅加快。

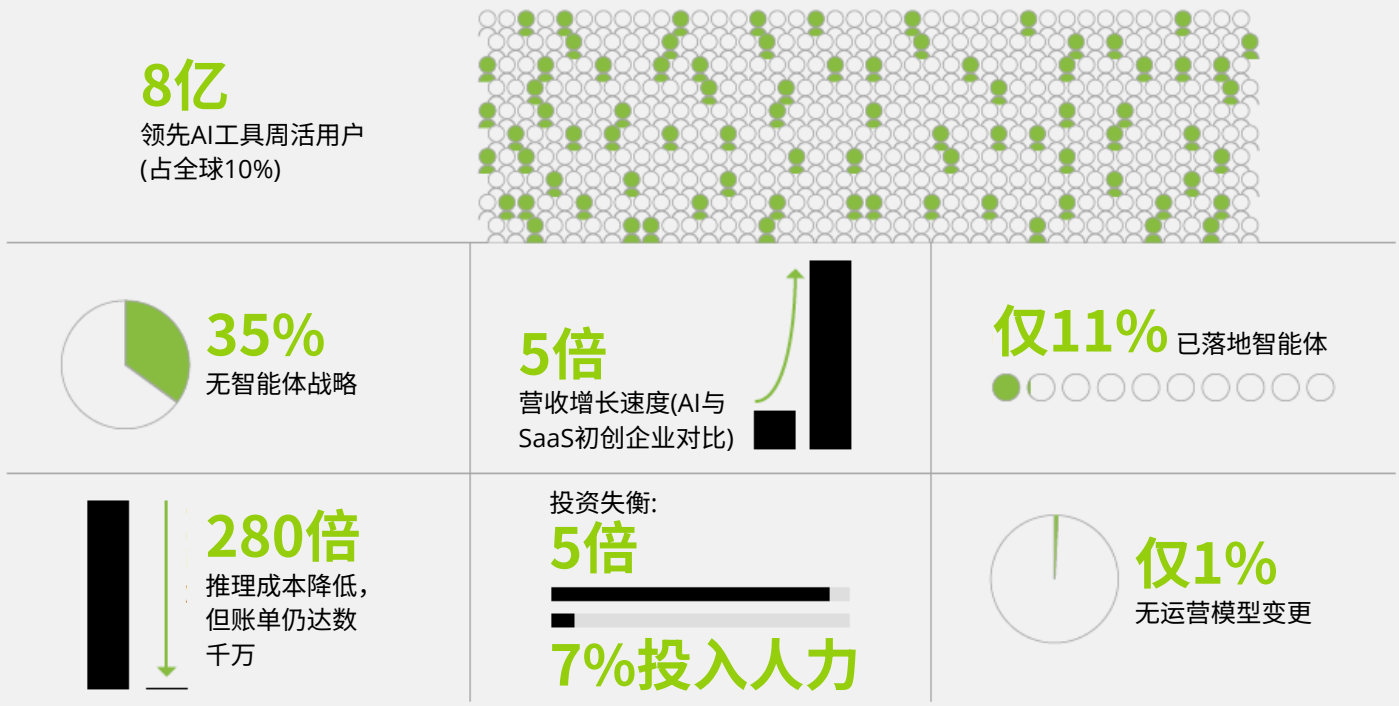
数字说明了问题（图1）。电话用了50年才达到5000万用户。互联网花了七年时间。一款领先的生成式AI工具在两个月内达到了这一数字的两倍。[1]截至本文撰写之时，该工具每周拥有超过8亿用户，约占全球人口的10%。[2]

然而，用户的快速增长只是表面现象。创新正呈现出复合增长的态势，各种推动创新的力量并非简单叠加，而是相互作用、产生倍增效应。可以将其比作一个飞轮：更先进的技术催生出更多应用场景；更多的应用场景产生更海量的数据；更海量的数据吸引更多投资；更多的投资打造更完善的基础设施；更完善的基础设施降低技术应用成本；更低的成本推动更多试验探索。每一项进步都会同时加速其他方面的发展。

这也解释了为何人工智能初创企业实现营收从100万美元增长到3000万美元的速度，是SaaS企业的5倍[3]；为何人工智能领域知识的半衰期从数年缩短至数月[4]；以及为何一位首席信息官（CIO）告诉我：“如今，我们研究一项新技术所花费的时间，甚至超过了这项技术的有效生命周期。”

图表1

## AI变革数据洞察




数据来源:Rebecca Bellan,“Sam Altman移ChatGPT周活用户达8亿”,TechCrunch,2025年10月6d,TechCrunch,2025年10月6日;德勤<<企业新兴技术趋势调查>>;WingVenture Capital,“AI增长快建于SaaS”;斯坦福以人为本人工智能能研究所，“2025年AI指数报告”;德勤2025年AI投资分配模式研究;德勤2025年技术支出展望。

**我们研究的每个组织都发现了同样的真理：过往的成功模式已不可复制于未来。**

为“云优先”战略构建的基础设施，难以满足人工智能时代的经济成本需求；为人类员工设计的业务流程，无法适配以智能体为代表的数字员工的运行模式；基于边界防御理念构建的安全模型，难以抵御以机器速度发起的安全威胁；为服务交付而建立的IT运营模式，无法推动业务变革。

**这不仅仅是对现有体系的优化升级，更是一场全面的重构。**

17年来，《技术趋势》报告始终致力于探索未来18至24个月内可能重塑商业格局的新兴技术。我们的研究基于两方面：一是与德勤领域专家及外部技术领导者交流获取的趋势洞察，二是德勤针对新兴技术开展的专业研究。今年的数据揭示了五个相互关联的关键趋势。

## 物理AI：探索AI与机器人的融合

亚马逊已部署了第100万台机器人，其DeepFleet AI系统负责协调整个机器人车队，使仓库内的运输效率提升了10%[5]。宝马的工厂中，汽车能够自主完成长达数公里的生产运输路线[6]。如今，智能不再局限于屏幕之上，而是具备了实体形态，能够自主运行，并在现实世界中解决实际问题。

## 未雨绸缪：为数字员工做好准备

尽管有38%的组织进行了试点，但只有11%的组织在生产中使用智能体。从试验到落地的差距揭露了一切， 42%的人仍在制定战略，而35%的人根本没有战略。[7] Gartner预测，到2027 [8] 年，40%的智能体项目将失败。这不是因为该技术不起作用，而是因为组织只有碎片化的自动流程，而不是重新设计运营。HPE的首席财务官认为有效的方法是：“我们希望选择一个端到端的流程，在那里我们可以真正转型，而不仅仅是解决一个痛点。”[9] 重新设计，不仅仅是自动化改造。这就是区分成功和失败的模式。

## 积极反思：优化AI基础设施策略

两年间，令牌成本下降了280倍 [10] ，但部分企业每月的AI相关支出仍高达数千万美元。这是因为使用量的增长速度远超成本下降速度。企业逐渐发现，现有的基础设施战略无法支撑AI技术实现规模化生产部署。于是，它们开始从“云优先”战略转向战略性混合架构：利用云服务应对波动性工作负载，通过本地部署保障稳定的生产推理需求，借助边缘计算满足低延迟应用场景。

## 脱胎换骨：重构一个AI原生技术组织

人工智能正在重构技术组织，使其更精简、更高效、更具战略性。在德勤的调查中，仅有1%的IT领导者表示企业没有正在推进的重大运营模式变革[11]。领导者们正从渐进式的IT管理模式，转向协调人机协作团队的模式，首席信息官（CIO）也在逐渐转变为人工智能的推广者。要取得成功，企业必须大胆重塑业务模式：采用模块化架构、嵌入治理机制，并将持续变革作为核心能力。

## 走出困境：使用AI进行网络防御

本应助力企业获得竞争优势的技术，如今却成为了攻击者针对企业的工具。美国电话电报公司（AT&T）的首席信息安全官这样描述所面临的挑战：“我们如今面临的情况，与过去并无本质区别。人工智能带来的唯一不同，在于威胁的速度和影响程度。”[12] 企业必须在数据、模型、应用程序和基础设施这四个领域保障人工智能的安全，同时也有机会利用人工智能驱动的防御手段，对抗以机器速度发起的安全威胁。

在今年的报告中，你将看到一些技术领导者成功应对这场变革的案例。他们并非掌握了所有答案，但在引领变革的过程中，已展现出一些明显的成功模式。

- 他们以问题而非技术为导向。博通首席信息官：“如果不聚焦于特定的业务问题以及期望获取的价值，企业很容易在人工智能领域投入资金，却得不到任何回报。”[13]
- 这里所说的问题，特指企业面临的重大问题。UiPath的首席执行官认为：“与其陷入无休止的概念验证循环，不如聚焦企业面临的最大问题，努力实现重大突破。”[14]
- 他们优先追求速度，而非追求完美。西部数据（Western Digital）的首席信息官表示：“我们宁愿在小型试点项目中快速试错，也不愿完全错失技术发展的机遇。”[15]
- 他们在设计过程中注重以人为本，而非仅仅为用户设计产品。沃尔玛在开发排班应用程序时，充分征求了门店员工的意见，加入了换班、排班可视化和员工自主掌控排班等功能。结果显示：排班时间从90分钟缩短至30分钟，而且员工确实愿意使用这款应用[16]。
- 他们将变革视为一个持续的过程。可口可乐的首席信息官将企业的人工智能发展历程描述为从“我们能做什么？”到“我们应该做什么？”的转变[17]。这种从“能力优先”到“需求优先”的转变，正是区分富有成效的试验和陷入试点困境的关键所在。

长期追踪技术发展趋势的经验让我能够敏锐地识别其中的规律。互联网改变了一切，移动技术重塑了消费者行为，云计算带来了颠覆性变革。

但当下这个时代却有所不同。

这不仅仅是因为人工智能功能强大，更重要的是技术发展的S曲线（增长曲线）正不断压缩，新兴技术从出现到成为主流的时间间隔越来越短。

那些依赖循序渐进改进模式的企业，已难以与处于持续学习循环中的企业竞争。传统的发展策略假定企业有足够的时间去完善各项举措，但这种假设如今已不再成立。

未来取得成功的企业，未必是拥有最先进技术的企业。而是那些有勇气重新设计业务模式而非仅仅进行自动化改造的企业；那些能够将每一项投资与业务成果紧密关联的企业；那些能够在机遇窗口关闭之前快速行动的企业。

创新具有复合效应，落后者与领先者之间的差距正以指数级速度扩大。企业如何应对，将决定其最终处于差距的哪一侧。

不过，你不必独自应对这场变革。我们希望今年的报告能让你明白，所有企业都在面临这种快速变革，只要携手合作，我们就能共同塑造未来。

**Kelly Raskovich**
《技术趋势》报告执行主编

# 尾注

1. Jeff Desjardins，“在争夺5000万用户的竞赛中，有一个明显的赢家，这可能会让你感到惊讶，”世界经济论坛，2018年6月 26日；Alexandra Garfinkle，“ChatGPT有望比TikTok或Instagram更快地超过1亿用户：瑞银，”雅虎财经，2023年2月2日。
2. Rebecca Bellan，“Sam Altman说ChatGPT已经达到8亿。每周活跃用户，”TechCrunch，2025年10月6日。
3. Zach DeWitt，“AI比SaaS增长更快”，Wing Venture Capital，2024年11月7日。
4. 基于德勤对技术采用周期和AI能力演变时间表的分析。
5. Scott Dresser，“亚马逊部署了100多万个机器人，并推出了新的AI基础模型”，亚马逊，2025年7月1日。
6. Brad Anderson，“当汽车在宝马工厂自动驾驶时，谁需要工厂司机”，CarScoop，2024年11月26日。
7. 德勤2025年企业新兴技术趋势调查。从2025年6月到7月，德勤对500名美国技术领导者进行了一项在线调查，以量化各行业采用新兴技术的普遍性、参与度和看法。
8. Gartner，“Gartner预测，到2027年底，超过40%的智能体AI项目将被取消”，新闻稿，2025年6月25日。
9. 玛丽·迈尔斯（HPE执行副总裁兼首席财务官），对德勤的采访，2025年3月1日。
10. 斯坦福大学以人为本的AI研究所，“2025年AI指数报告”，于2025年11月12日访问。
11. 德勤2025年技术支出展望。从2025年6月到7月，德勤对302名IT采购负责人、IT主管和负责技术支出监督的非IT高管进行了在线调查，以了解关键行业的美国企业如何管理技术预算。
12. “一种在at&T确保AI启用的严肃方法，”Deloitte Insights，2025年11月21日。
13. Katherine Noyes，“博通首席信息官：‘现代化应该由业务驱动’，”《首席信息官杂志》、《华尔街日报》和德勤，2025年9月10日。
14. Katherine Noyes，“UiPath首席执行官：智能体自动化将‘迎来一个新的工作时代’”，《首席信息官杂志》、《华尔街日报》和德勤，2025年2月21日。
15. Katherine Noyes，“西部数据首席信息官：在AI时代，‘要么进攻，要么落后’”，《首席信息官杂志》、《华尔街日报》和德勤，2025年9月6日。
16. 沃尔玛，“沃尔玛推出新的AI工具来增强 150万名员工，”2025年6月24日。
17. Katherine Noyes，“可口可乐首席信息官关于扩大AI：从‘我们能做什么？’到‘我们应该做什么’”，《首席信息官杂 志》、《华尔街日报》和德勤，2025年1月18日。

# 物理AI：探索AI和机器人的融合

在AI的推动下，传统机器人正逐步转变为能够在复杂环境中运行并从中学习的自适应机器，进而在安全性和精准度方面实现突破。

*Jim Rowan、Tim Gaus、Franz Gilbert和Caroline Brown*

物理AI是指使机器能够实时自主感知、理解、推理并与物理世界交互的AI系统。这些能力出现在机器人、车辆、仿真和传感器系统中。与遵循预编程指令的传统机器人不同，物理AI系统能够感知环境，从经验中学习，并根据实时数据调整行为。仅靠自动化并不能使它们具有革命性；相反，这是他们弥合数字智能和现实世界之间差距的能力。

在机器人这一新兴且发展迅速的领域，物理AI使机器人转变为具备自适应能力的学习型机器，能够在复杂且不可预测的环境中运行。人工智能、移动技术和物理智能体的结合，让机器人能够在环境中移动、执行任务并与世界互动，其方式与功能增强型设备有着本质区别。物理AI融入机器人系统后，确实正在不断的进步中。

如今，配备人工智能的无人机、自动驾驶汽车和其他类型的机器人正日益普及，在智能仓储和供应链运营领域的应用尤为广泛。行业内部、监管机构以及潜在的应用企业正共同推动这项技术从原型阶段走向实际生产应用。

## 从原型到生产

与传统仅运行于数字环境的AI系统不同，物理AI系统整合了感官输入、空间理解与决策能力，使机器能够适应并响应三维环境与物理动态。这类系统依赖于神经图形学、合成数据生成、基于物理的仿真以及先进AI推理技术的融合。通过强化学习、模仿学习等训练方法，这些系统能够在部署到现实世界之前，先在虚拟环境中掌握重力、摩擦等物理原理。

机器人仅是物理AI的一种体现形式。它同样涵盖利用固定摄像头与计算机视觉优化工厂及仓库运营的智能空间、支持物理系统虚拟测试与优化的数字孪生仿真，以及基于传感器的AI系统——这类系统无需机器人介入，即可帮助人类团队管理复杂的物理环境。

传统机器人遵循既定指令运行，而物理AI系统能够感知环境、从经验中学习，并根据实时数据和不断变化的环境条件调整行为。

它们能够操控物体、在不可预测的空间中自主移动，并做出影响现实世界的瞬间决策。

机器狗通过分析声学特征，在设备故障变成灾难之前检测到故障。机器狗能够通过分析声音特征，在设备发生严重故障前检测出问题；工厂机器人在生产计划中途调整时，能够重新规划运行路线；自动驾驶汽车借助传感器数据，比人类驾驶员更早发现骑行者；配送无人机能根据风向变化调整飞行路径。这些系统之所以具有革命性，不仅仅在于它们能实现任务自动化，更在于它们具备感知、推理和自适应能力，正是这些能力架起了数字智能与物理世界之间的桥梁[1]。

### 技术进步推动物理AI与机器人融合

物理AI之所以为大规模部署做好了准备，得益于多项技术的融合——这些技术深刻影响了机器人感知环境、处理信息以及实时执行动作的方式。

**视觉-语言-动作模型。**物理AI借鉴了大语言模型（LLM）的训练方法，同时融入了描述物理世界的数据。多模态视觉-语言-动作（VLA）模型整合了计算机视觉、自然语言处理和运动控制技术。[2]如同人类大脑一样，VLA模型帮助机器人理解周围环境并选择适当的动作（图1）。

**机载计算与处理能力。**神经处理单元（NPU）是专为边缘计算优化的专用处理器，能够让机器人实现低延迟、高能效的实时人工智能处理。机载计算能力使实体人工智能系统能够运行大语言模型和视觉-语言-动作模型，处理高速传感器数据，并在无需依赖云服务的情况下做出关乎安全的瞬间决策——这对于自动驾驶汽车、工业机器人和远程手术等应用场景至关重要[3]。此外，它还能将机器人从孤立的机器转变为可自主共享知识、协同行动的智能网络系统。

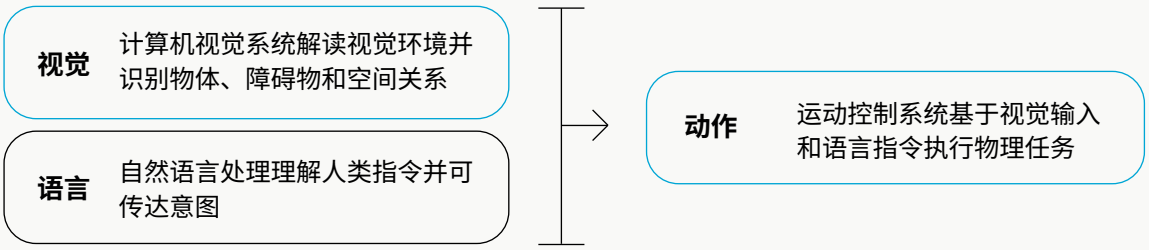
**机器人技术的进步。**机器人技术的发展让机器人变得更易获取且功能更强大[4]，主要体现在以下几个方面：

- 用于“观察”和理解周围环境的计算机视觉
- 用于捕捉声音、光线、温度和触觉等信息的传感器
- 受人体肌肉启发，用于实现运动的执行器
- 用于在三维环境中导航的空间计算技术
- 改进的电池技术，实现更长运行时间且无需频繁充电

**培训和学习。**在强化学习中，机器人通过不断尝试与纠错（根据行为结果获得奖励或惩罚），逐步形成复杂的行为模式。

图表1

## 视觉-语言-动作模型的工作原理




数据来源：德勤分析

在模仿学习中，机器人则通过模仿专家示范来学习，这两种方法都可以应用于模拟环境或具有真实硬件的物理世界。[5] 将这些技术的结合运用，从基于模拟的强化训练开始，再通过有针对性的物理演示进行微调，可以创建持续的学习循环。这有助于机器人通过将现实世界的数据反馈回其训练策略和模拟空间，从而实现继续改进。[6]

**显著的经济效益推动工业应用**

随着技术的进步，相关成本持续下降，许多实际应用场景已不断涌现。

如今，先进的制造基础设施能够支持复杂机器人及物理AI系统实现企业级规模的生产。这意味着，物理AI机器人如今能以智能手机或汽车般的可靠性及质量控制标准进行制造，从而使其适用于日常工业场景。

组件商品化和开源开发正在降低物理AI系统的入门成本。然而，由于这些机器人需要先进的AI芯片和处理器，

它们仍然比传统的工业机器人更昂贵。目前，即使整体价格逐渐下降，这种成本差距也可能持续存在。

因此这些经济因素正在推动物理AI和机器人在特定用例中的应用。自动驾驶汽车和无人机是最具代表性的机器人形态（图2）。Waymo的无人出租车服务已完成逾千万次付费乘坐，而Aurora Innovation则率先推出了商业化自动驾驶卡车服务，在达拉斯和休斯顿之间实现定期货运配送。[7]

AI无人机从根本上改变了消费者对速度和便利性的期望，同时也成为强大的商业工具。无人机配备了先进的摄像头和传感器，如今可以通过在货架间自主导航，并用条形码和二维码扫描仪识别商品，以自主管理仓库库存。[8]

在企业中，仓储和供应链运营是最早应用物理AI机器人系统的领域，这很可能源于劳动力市场的压力。[9]

许多组织现在大规模使用这些系统。例如，亚马逊最近部署了第一百万个机器人，作为一支与人类协同工作的多样化车队的一部分。[10] 其DeepFleetAI模型负责协调这支庞大机器人军团在整个履约网络中的移动，据亚马逊称，该系统将使机器人车队的运行效率提升10%。[11]

图表2

## 机器人和物理AI的六个关键形态


资料来源：MarkOsis，Raquel Buscaino和Caroline Browm，“机器人与物理AI”，Deloitte，2025年。

同样，宝马正在将AI自动化整合到其全球工厂中。在一次创新部署中，宝马利用自动驾驶技术——借助传感器、数字地图和运动规划器——使新制造的汽车能够从装配线自动驶向测试区，再驶向工厂的最终处理区，全程无需人工协助。[12]

## 物理AI的转折点

随着技术进步与融合、成本下降及可行应用场景涌现，物理AI驱动的机器人正蓄势从细分市场迈向主流应用——前提是能够克服技术、运营及社会层面的挑战。

### 突破实施障碍

随着组织机构寻求扩展物理AI的应用规模，它们正面临一系列复杂且相互关联的实施挑战。该技术本身可行，但要实现大规模应用，必须解决技术、运营和监管领域的多重难题。那些直面这些挑战的组织将引领下一波部署浪潮。

**训练和学习。**模拟环境在速度、安全性和可扩展性方面具有关键优势，但由于近似的物理模型，模拟与现实表现之间始终存在差距。[13] 俄亥俄州立大学工程学院院长Ayanna Howard说：“模拟环境的视觉效果相当逼真，但现实世界存在难以复现的细微差异。”俄亥俄州立大学工程学院院长艾安娜·霍华德指出，“机器人可能在模拟中学会抓取物体，但进入物理空间后，实际操作与模拟环境并非完全对应。”[14]（完整问答详见侧栏）

### 人为因素：Ayanna Howard谈物理AI与机器人技术的未来

Ayanna Howard现任俄亥俄州立大学工程学院院长，是知名机器人学家及AI安全与协调倡导者。此前她曾任美国宇航局喷气推进实验室高级机器人研究员，后担任佐治亚理工学院交互计算学院院长并创立人机协同系统实验室。

**Q： 哪些技术挑战阻碍了物理AI和机器人技术的进步？**

**A：**核心挑战在于物理世界本质上充满动态变化。我每天走进办公室时，总有一些不同—— 也许有人吸过地、挪过物品，或者我的电脑无法启动。关键在于如何模拟所有这些变量，让机器人能够像人类一样学习适应、行走、举起物品并应对不确定性？你无法在现实世界中无限次练习，否则会破坏物品。

还有一个硬件限制，我将其解释为“操纵能力与身体比例”。 人类能举起自身体重甚至更重的物体，但传统的机器人——即使是重型机器人——常因驱动器限制连自身半数重量都举不起。它们没有像我们这样的肌肉来缓冲刚性驱动，这限制了它们与物体交互及移动的能力。

最后，还有实时处理的挑战。大型语言模型和视觉语言模型通常运行在所谓“人类时间”中：我们能接受一两秒的响应延迟。但是，如果行走中的机器人需要决策，一两秒钟的延迟可能导致它会掉东西、撞车或可能伤害到某人。我们在实时处理方面做得越来越好，但尚未完全成熟。

**Q： 你对AI系统中的信任和过度信任进行了深入研究。你能解释一下这两个极端是如何构成挑战的吗？**

**A：**事实证明，言语信任与行为信任之间存在显著差异。换句话说，人们经常说他们不信任AI，但若询问他们是否使用手机电脑，甚至是否出门，你猜怎么着？他们其实都在使用AI。

我对过度信任的研究侧重于行为，而不是人们说的话我们设计实验让受试者与会犯错的机器人系统互动。在接受调查时，参与者表示他们不信任这些系统，因为他们看到它们犯了错误。但行为分析却揭示了另一面：他们的实际行为表明他们确实信任机器人。

当AI具备实体形态时，这种行为过度信任变得危险，因为这些机器人会在环境中施加物理影响。它们的行动可能造成不可逆的后果。有了今天的AI，你仍然需要人类。

**人为因素：Ayanna Howard谈物理AI和机器人的未来（续）**

驱动大多数任务，尽管智能体AI正在开始改变这一格局。

**Q： 当前最需要投入的关键研究领域是什么?**

**A：** 在物理空间中实现学习，同时避免发生伤害事故。我们仍然需要弄清楚如何将模拟安全地转化到物理世界。模拟环境中的视觉图像相当逼真，但现实世界中存在微妙差异。机器人可能会在模拟中学会抓取东西，但当它进入物理空间时，两者并非完全对应。研究表明，机器人在从模拟环境转移到物理环境后确实能适应，但它们学习的是具体任务而非整体环境交互。他们可能会学会在摩擦系数不同的表面上抓取球体。却无法基于模拟社交互动来学习在商场或校园里如何在抛接球时与人群保持安全距离。这种全面的环境适应还不存在。

**Q： 您是否有任何与传统智慧相悖的观点?**

**A：** 我坚信人类必须始终参与决策链。永远如此。作为机器人学家，我强调这一点并非保证百分百安全，而是为了避免过度信任。或许需要由CEO每年对机器人进行评估。若缺乏这种反馈机制，技术将脱离人类掌控。

技术突破方向。物理引擎、合成数据生成以及将虚拟训练与现实世界应用相结合的方法的进步，应该有助于组织在模拟的规模和安全性方面实现物理训练的质量。

**可信赖的AI与安全保障。**物理系统中微小的错误率可能引发连锁反应，可能导致生产浪费、产品缺陷、设备损坏或安全事故。如果AI系统出现幻觉，错误可能会在整个生产过程中持续扩散，对成本和运营产生累积性影响。

即使经过全面安全测试，AI驱动的机器也可能表现出不可预测的行为。在公共空间中，自主系统必须应对不可预测的人类行为，风险显著升高。要在不同行业大规模部署物理AI系统，需要综合监管合规风险评估和持续监控的全面安全策略。[15]

**监管环境。**企业需应对不同司法管辖区间相互重叠且有时相互矛盾的要求。[16] 随着机器人从受控的工厂环境进入公共空间，监管机构可能会制定新的安全认证、责任归属和运营监督框架。

**数据管理。**企业需采集并管理大量的传感器数据、3D环境模型和实时信息。物理资产的高保真数字孪生体对于有效的培训和部署至关重要，这要求获取大量关于物理特性、物体属性和交互数据。组织还需要整合来自不同来源的多模式数据，保障数据安全，并管理数据基础设施成本。

**人类接受度。**尽管多数员工普遍接受可预测的规则型机器人，但具备学习适应能力的物理AI系统会引入新不确定性，尤其引发就业替代担忧。不过专家预测多数岗位将演变为协作而非替代关系。[17] 目标是构建机器人处理重复性或危险任务、人类专注创造性问题解决与复杂决策的环境。

**网络安全漏洞。**正如在“AI困境”物理AI系统在数字与物理领域之间创造了新的攻击面。联网车队加剧了网络风险，漏洞可能导致未经授权的访问、数据泄露甚至恶意机器人控制。当安全漏洞可能影响物理安全和运营连续性时，风险甚至更高。

机器人车队协调。随着物理AI系统的成熟，企业将越来越多地部署来自多个供应商的异构机器人、自动驾驶汽车和AI智能体车队，每种设备都有专有协议。这带来了互操作性挑战，可能导致事故、停机、系统拥塞和运营效率低下。[18] 自主车队管理和协调系统可以帮助解决这些问题。

在未来18到24个月内，解决这些基础问题可能会使物理AI和机器人技术突破传统产业边界。仓储和物流可能是物理AI的试验田，但技术边界远不止于此。

**正在瓦解的行业边界**

随着公共和私营部门的领先组织正在为大规模部署物理AI奠定基础，其应用率正呈指数级增长。凡实体AI能解决实际问题的领域，创新应用便应运而生。

在面临全球人员短缺的医疗保健领域，医疗技术公司正在开发AI驱动的机器人手术和数字成像设备通用电气医疗保健公司正在利用机械臂和机器视觉技术打造自主X射线和超声波系统。其他医疗科技公司正在设计智能机器人助手，既能辅助患者护理，又能实现手术任务自动化。[19]

餐饮业也在部署机器人来帮助解决劳动力短缺问题。人行道配送机器人以步行速度行驶；在餐馆里，机器人负责翻煎汉堡和准备沙拉等任务，而服务机器人则引导就座并上菜。

西班牙跨国天然气和电力公用事业公司Naturey Energy Group目前使用无人机进行设备巡检。Naturey的首席数据官拉斐尔·布莱萨设想，随着技术成熟，物理AI将发挥更大的作用，特别是在涉及高电压或开放式天然气管道的危险现场作业中。他解释说：“从长远来看，许多与电网维护相关的操作都可以由机器人完成。” 他解释道，“我预计三到四年内，机器人将执行物理性操作，这可能挽救生命。”[20]

同样，辛辛那提市正在使用AI驱动的无人机自主检查桥梁结构和路面状况，既降低了成本，又避免了人工检查员暴露在危险环境中，还将数月的分析工作压缩至数分钟完成。辛辛那提市长阿夫塔布·普雷瓦尔表示：“这种技术将成为支撑市长们高效履职的核心要素，为选民提供更优质的信息、决策和成本效益。”

2024年，底特律市推出了一项免费自动驾驶接驳服务，专为行动能力受到传统交通系统严重限制的老年人和残障人士而设计。被称为“无障碍底特律”的自动驾驶汽车配备了轮椅无障碍设施和训练有素的安全操作员。三辆自动驾驶汽车在底特律11平方英里的区域内行驶，覆盖110个不同的停车点。[22]

无论应用于哪个领域，这些部署都有一个共同的特点：它们在安全、精准度或可及性至关重要的场景中，增强了人类的能力。

## 人形机器人及其发展前景

我们都看过广为流传的人形机器人的视频，它们动作流畅，虽非完全拟人却已相当逼真。这种形态最具吸引力，不是因为它们具有最高效的设计，而是因为我们的世界是为人体建造的。这意味着他们可以畅行于现有的基础设施（门廊、楼梯、工厂车间乃至家庭厨房），而无需耗资改造来适应专门的机器人系统。[23]

俄勒冈州立大学机器人研究员、敏捷机器人公司联合创始人Jonathan Hurst说：“人类与环境的交互极具适应性，时刻保持着与周遭的接触。这对商业机器人来说极具挑战。”。“通常机器人是高度位置控制的设备。它们适用于数控加工（需要精确、可重复定位的精密制造）或点焊等任务，但在非结构化空间中进行装配、操作或移动则表现欠佳。”[24]（完整的问答请参见侧栏。）

多家公司已经开发并持续改进具有更精确手指控制能力的双足机器人。随着近期引入可比拟人类认知的链式思维推理能力，技术基础不断进步。[25]
在未来十年里，AI智能体系统与物理AI系统的融合，将催生以自主AI为“大脑”的机器人。各种形态的机器人将日益具备适应新环境、规划多步骤任务、从故障中恢复以及在不确定性条件下运作的能力。这种技术融合对人形机器人的影响将尤为深远。

未来或将不再为每个领域定制专用机器人，而是通过通用智能模块实现跨领域复用——无论是仓库、家庭、医疗、农业还是其他场景。具备智能体功能的人形机器人终将作为助手、同事或医疗护理员投入使用，其交互、推理与协商能力将更趋直观。

大规模普及人形机器人可能还需要几年时间。尽管如此，瑞银估计，到2035年，工作场所将部署200万类人机器人，预计到2050年，这一数字将增加到3亿。该公司预测，这些机器人的潜在市场总量到2035年将达到300亿至500亿美元，并于2050年攀升至1.4万亿至1.7万亿美元。[26]

由于劳动力短缺，仓储和物流等企业应用领域仍然是人形机器人部署的试验场。宝马公司正在其南卡罗来纳州的工厂测试人形机器人，用于执行传统工业机器人无法胜任的精细操作：精确操控、复杂抓握和双手协同作业。[27] 出于类似的需求，人形机器人可以在医疗领域发挥作用。一家医疗保健公司正在康复中心测试人形机器人，通过指导患者进行锻炼和提供体重支持来辅助治疗师开展工作。[28]

更广阔的长期机会在于消费市场，其愿景涵盖全面家务劳动，包括老年及残障护理、清洁维护、膳食准备和洗衣服务。美国银行研究所预测，在未来十年，人形机器人的材料成本将从2025年的约35000美元降至每台 13000 至 17000 美元， 高盛报告称， 2023 年至 2024年间，人形机器人制造成本下降了40%。[29]

## 从实验室到现实世界：Jonathan Hurst谈人形机器人

Jonathan Hurst是俄勒冈州立大学的机器人学教授也是该校机器人研究所的联合创始人，他的研究重点是腿部运动学。他也是敏捷机器人公司的联合创始人兼首席机器人官，该公司致力于开发和部署人形机器人，使其能在商业应用中与人类工人协同作业。

**Q： 你是否试图打造人形机器人来解决一个特定的问题?**

**A：** 我们希望制造出能像动物或人类般行动、同时适应人类生活空间的机器。人类与环境互动时具有高度适应性，时刻与外界保持接触。这对商用机器人来说极具挑战。传统机器人多采用位置控制装置，它们适用于数控加工（需要精确、可重复定位的精密制造）或点焊，但不适用于非结构化空间中行装配、操作或移动。

我们的机器人已相当接近正常人类腿部构造——双足直立、躯干挺拔、双手操作。最重要的是，这些特征皆有其功能意义。我们正在捕捉这种形式背后的功能本质。

**Q： 你是怎么确定人形机器人能做什么的?**

**A：** 从项目伊始，我们就致力于打造以人为本的多功能机器人。我们研究了数百个应用场景。事实证明搬运箱子和托盘这类简单任务与该技术高度契合。这项任务需要机器人具备窄足迹特性，才能在走廊中作业、穿过门洞并融入人类活动空间。它还需具备举重能力——例如将25公斤重的物品搬运至两米高的货架顶部。

为此机器人必须具备动态稳定性——即机器人在移动中保持平衡。若采用静态稳定底盘，在搬运重物时极易倾覆。因此，双足行走结构是实现动态稳定、避免跌倒的最有效方案。

## 从实验室到现实世界：Jonathan Hurst谈人形机器人（续）

这就是设计起点。随后我们赋予其双臂功能，因为搬运大型物品需要两侧同时抓握。同时必须具备可达工作空间，才能从地面拾取物品并举高，需要具备直立躯干，因此这项技术与人形机器人堪称绝配。

这对于现有的自动化来说很难实现。由于所有工作流程都具有独特性，因此需要相当大的灵活性。例如，不同类型的托盘需要运往不同地点。你需要堆叠托盘、进行托盘化处理、将其放置在传送带上，或从自主移动机器人（AMR）上取下。这种多样性使传统的自动化变得困难，但它仍然具有相当的结构化特征。或许可称之为半结构化。该工业环境具备高度可控性与流程自动化特征，这为人形机器人提供了绝佳的切入点。

**Q： 人形机器人如何实现规模化应用？**

**A：** 未来25年内，人形机器人市场的规模将是汽车行业的两倍。要达到这一目标，需要大规模扩展，因为这意味着数百万台机器人的部署，而当前全球仅有数百台机器人投入使用。

功能安全型人形机器人有着巨大的市场，这种机器人无需局限于独立工作单元。

届时，才能实现数千台机器人的规模化部署。你如何保障现场运维？你如何让机器人车队管理软件突破所有独特的带宽限制及其他障碍？在机器人领域中，这很难做到，但并非不可实现。Waymo已经在道路上部署了基本上是机器人的自动驾驶车辆，所以这绝对是可行的。这并不是说需要发明新事物，但组织必须具备极强的执行力。这就是我们正在践行的道路，一旦机器人足够安全，足以支撑规模化应用。

### 人形机器人之外的未来？

人形机器人以其熟悉的两足形态俘获公众想象。接下来更前沿的未来科技该是怎样的？

在物理形态方面，突破边界的工程师越来越多地尝试模糊生物界限的机器。试想由活体蘑菇组织驱动的机器人，借助鼠类肌肉组织模拟动作的机械，或者可以使用磁场在固态和液态之间转换的装置。在当今的创新实验室中，科学家们正在将生物体整合到机械系统中，开发能够通过多种移动模式穿越复杂环境的机器人，并创造能根据任务调整物理形态的机器。[30]

量子机器人——量子计算和AI机器人的结合——同样前景广阔，尽管它还处于非常早期的阶段。叠加态、纠缠态、量子算法和其他量子计算原理可能使机器人以当今二进制计算机无法企及的运行速度。[31]量子算法有望改善处理、导航、决策和编队协调能力，而量子传感器将增强感知和交互功能。[32]

实用型量子机器人尚需数十年发展。硬件不成熟、集成难题和量子态的极端敏感性只是量子计算广泛部署前需攻克的若干挑战。[33]

人形管家至少还有十年的时间才能问世，奇特的外形和量子能力仍主要停留在实验阶段。但这些突破标志着机器人技术思维的根本性转变。随着这些突破性技术从实验室走向企业再进入家庭，机器人技术领域正正从单纯自动化人类任务，迈向创造全新类别机器的进阶阶段。

# 尾注


1. Nvidia，“什么是物理AI？”访问日期为2025年11月6日
2. Anony，“具身AI的视觉语言动作模型：调查概述”， Medium，2025年5月12日。
3. Josh Schneider和Ian Smalley，“什么是神经处理单元（NPU）？”IBM，访问日期为2025年11月6日。
4. 王洁飞和达米斯·赫拉特，“是什么造就了机器人？传感器、执行器和算法”，《机器人基础》（新加坡：施普林格， 2022）；美国银行研究所，“人形机器人101”，2025年4月29日。
5. 麻省理工学院技术评论，“在AI驱动的工业元宇宙中训练机器人”，2025年1月14日。
6. 自动化，“NVIDIA关于物理AI对机器人意味着什么”，2025年8月5日。
7. Mark Osis、Raquel Buscaino和Caroline Brown，“机器人 和物理AI：运动中的智能”，德勤，2025年10月17日。
8. 同前
9. 同前
10. Michael Grothaus，“什么是物理AI和实体AI？机器人知道”，《快公司》，2025年7月19日。
11. Scott Dresser，“亚马逊推出了一种新的AI基础模型，为其机器人车队提供动力，并部署了第100万个机器人，”亚马逊，2025年7月1日。
12. Brad Anderson，“当汽车在宝马工厂自动驾驶时，谁需要工厂司机”，Carsoples，2024年11月26日。
13. Erica Salvato、Gianfranco Fenu、Eric Medvet和Felice Andrea Pellegrino，“跨越现实差距：强化学习中机器人控制器从模拟到真实可转移性的调查”，IEEE Access 42016。
14. Ayanna Howard，《德勤访谈》，2025年9月18日。
15. 标准机器人，“工业机器人安全标准：你需要知道什么”，2025年4月23日。
16. Jacob Otasowie、Alexander Blum、Mohamed El Sayed Ahmed和Mathias Brandstötter，《机器人中AI的危险：对伦理、监管和经济挑战的系统分析》，施普林格， 2025年9月2日。
17. Osis、Buscaino和Brown，“机器人和物理AI”
18. 力士乐，“高效车队管理：如何成功协调异构车队”，2024年8月30日。
19. Conor Hale，“英伟达概述了机器人手术、自主成像领域的新AI项目，”Fierce Biotech，2025年3月21日。
20. 拉斐尔·布莱萨，德勤访谈，2025年5月22日。
21. 德勤美国，“锈带复兴：辛辛那提的OptoAI故事”，YouTube视频，2023年9月15日。
22. 德勤美国，“底特律在自动驾驶汽车方面取得进展”，访问日期为2025年11月6日。
23. 人形机器人技术，“2025年12大人形机器人”，2025年2月。
24. Jonathan Hurst，德勤访谈，2025年10月6日。
25. Anabelle Yearsdon，“人形机器人指南（2025）：类型、历史、最佳模型、解剖结构和应用”，Top 3D Shop，2025年4月 28日。
26. 史蒂夫·戈尔茨坦，“3亿人形机器人即将到来，以下是将受益的公司，”晨星公司，2025年6月18日。
27. 宝马集团，“宝马集团斯巴达堡工厂的仿人机器人”，2024年11月9日。
28. News.am，“仿人机器人傅里叶GR-1已经推出：它的用途是什么？”2023年7月14日。
29. 高盛，“到2035年，全球人形机器人市场可能达到380亿美元”，2024年2月27日；美国银行研究所，“人形机器人101”
30. Future Today Strategy Group，“2025年技术趋势”，访问日期为2025年11月6日。
31. Matt Swayne，“什么是量子机器人？研究人员报告称，量子计 算和AI的融合可能会导致量子机器人”，《量子内幕》， 2025年5月9日。
32. Fei Yan， Abdullah M.Iliyasu， Nianciao Li， Ahmed S.Salama和Kaoru Hirota，“量子机器人： 新兴趋势综述”，量子机器智能6，第86期（2024）。
33. Swayne，“什么是量子机器人？”

# 作者简介

**Jim Rowan**
jimrowan@deloitte.com

Jim Rowan是德勤美国AI主管，与外部技术组织、客户和德勤的商业领袖合作，帮助我们的客户实现他们的AI抱负。除了他的客户工作，Rowan还是德勤咨询公司的负责人。他的经验涵盖了生命科学、医疗保健和电信行业，重点是应用分析、规划、预测和数字化转型来增强财务职能。

**Tim Gaus**
tgaus@deloitte.com

Tim Gaus是德勤咨询公司的负责人和智能制造业务负责人。他拥有超过25年的供应链经验，专注于利用新兴技术进行价值链优化。他领导了多个供应链转型，涵盖供应链战略、制造优化、供应链规划、库存优化、运营模式设计以及国内和跨国公司的卓越运营。

**Franz Gilbert**
frgilbert@deloitte.com

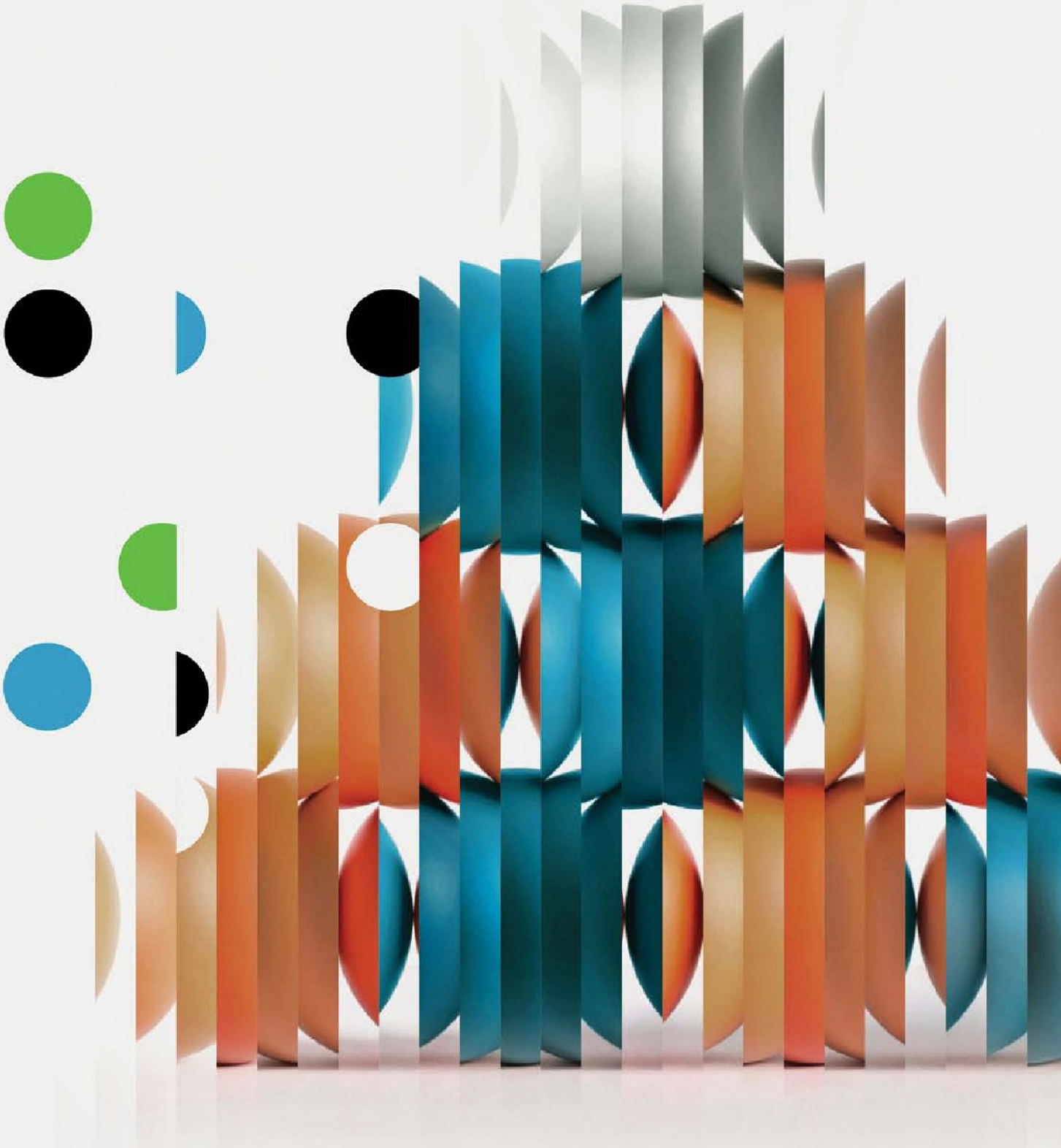
Franz Gilbert是德勤咨询公司的董事总经理，担任人力资本战略和创新负责人，并在人力资本管理委员会任职。他和他的团队负责制定和推动人力资本增长战略，孵化新兴企业，并管理联盟，为客户带来创新的解决方案和更有价值的成果。Gilbert是人力资源认证协会的董事会成员。

**Caroline Brown**
carolbrown@deloitte.com

Caroline Brown是德勤首席技术官办公室的高级经理。她领导着一个跨职能的编辑和设计制作团队，培养思想领导力。她担任德勤旗舰技术报告《技术趋势》的编辑。作为一名作家和研究员，Brown在北卡罗来纳大学教堂山分校获得了英语和新闻学的本科和研究生学位。

# 致谢

衷心感谢德勤的众多专业领域负责人为本章研究提供的贡献：
Mahesh Chandramouli和Ryan Kaiser。



# 未雨绸缪：为数字员工做好准备

尽管前景可观，但很多智能体的实施却失败了。然而，那些正在重构运营并将智能体视为员工的领先组织正在取得成功。

*Jim Rowan、Nitin Mittal、Parth Patwari和Ed Burns*

企业正在迅速向智能体应用迈进，但许多企业都遭遇了瓶颈。他们正试图自动化现有的流程——由人类员工设计并专为人类员工设计的任务——而不重新思考这些工作实际应该如何开展。

领先的组织正在发现一些不同的东西：真正的价值来自运营的精简优化，而不仅仅是将智能体叠加到原有的工作流程中。这意味着要构建与智能体兼容的架构，实施稳健的编排框架，并为数字工作者开发新的管理方法。

这也意味着重新思考工作本身。随着组织充分发挥智能体的潜力，不仅他们的流程可能会发生变化，他们对员工的定义也会发生变化。智能体式AI可能被视为一种硅基劳动力，对人力劳动力起到补充和增强作用。正确掌握基本要素——从基于微服务的智能体架构到硅劳动力管理——可以让企业为工作流自动化的未来做好准备，并使其具备在智能体原生商业环境中有效竞争的能力。

亨利·福特（Henry Ford）曾精辟地指出这一点：“许多人正忙于寻找更好的方法来做那些根本不应该做的事情。仅仅找到一种更好的方法去做一件无用的事情是不能带来任何进步的。”[1] 他在1922年写这段话是关于制造汽车，但也同样适用于描述2025年的企业AI。

## 未雨绸缪

智能体以其令人信服的自主操作和智能执行的前景，吸引了企业的广泛关注。这一变化势不可挡：Gartner预测，到2028年，15%的日常工作决策将通过智能体自主处理，而2024年这一比例还是零，而同期33%的企业软件应用程序将集成智能体，而目前这一比例不足1%（图1）。[2]

然而，尽管管理者抱有热情，企业在将智能体试点项目转化为可投入生产的解决方案时却遇到了重大障碍。德勤的《2025年企业新兴技术趋势》研究指出，有30%的受访组织正在探索智能体式解决方案，38%的组织正在试行相关方案，但仅有14%的组织拥有已就绪可部署的解决方案，仅有11%的组织将这些系统投入实际生产应用。此外，有42%的组织表示他们仍在制定自身的智能体式AI战略路线图，而35%的组织甚至尚未制定任何正式的战略。[3]

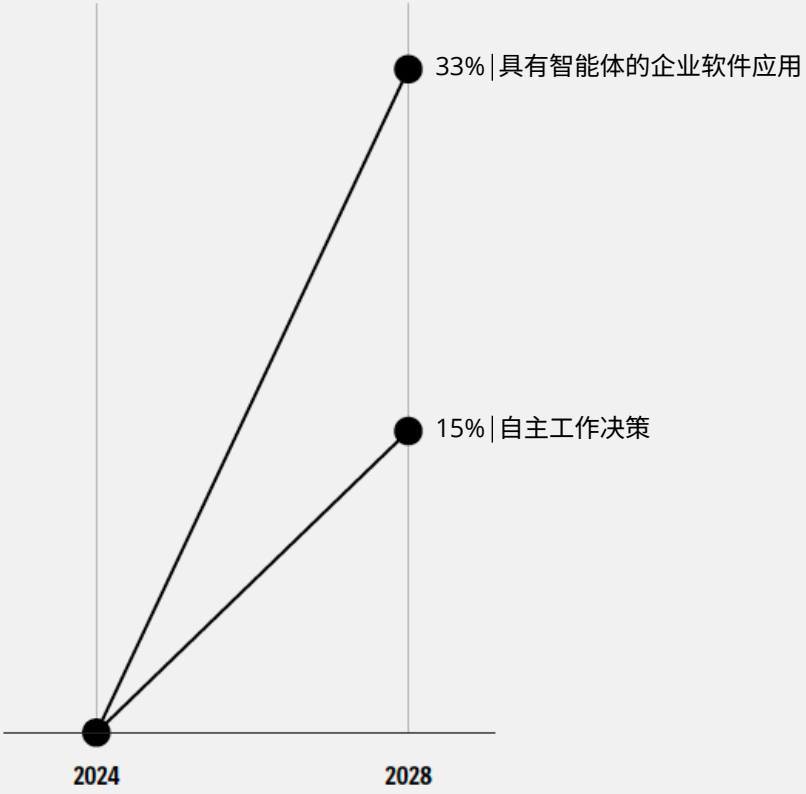
### 智能体现实差距

三个基本的基础设施障碍可能阻碍组织充分发挥智能体的潜力。

**旧有系统集成：**传统的企业系统并非为智能体式交互而设计的。大多数智能体仍然依赖于应用程序编程接口（API）和传统数据管道来访问企业系统，这造成了瓶颈并限制了它们的自主能力。Gartner预测超过40%的系统存在此类问题。

图表1

## 智能体应用情况预测




来源:Gartner分析。2025年1月，Gartner对3412名网络研讨会参与者进行了调查，了解他们公司实施智能体的计划。

到2027年，大量基于智能体的项目将遭遇挫折和失败，因为传统系统无法满足现代AI的执行需求。这些系统缺乏真正实现智能体式集成所需的实时执行能力、现代API、模块化架构和安全身份管理等能力要求。[4]

**数据架构限制：**当前的企业数据架构以提取、转换、加载（ETL）流程和数据仓库为核心，这给智能体的部署带来了诸多不便。最根本的问题是，大多数组织数据都未被设计成可供需要了解业务环境并做出决策的智能体使用。在德勤2025年的一项调查中，近一半的组织将数据的可搜索性（48%）和数据的可重用性（47%）列为影响其AI自动化战略的挑战。[5]

该解决方案涉及一种范式转换，即从传统数据处理流程转变为“企业搜索和索引”的模式，类似于谷歌使万维网可被检索的方式。这种方法涉及通过基于知识图谱的内容和索引存储将企业数据情境化，使得信息得以被检索，而不需要大量的ETL处理过程。

**治理和控制框架：**企业很难为那些旨在自主运行的系统建立适当的监督机制。传统的IT治理模型并未考虑到能够做出独立决策和采取行动的AI系统。这一挑战不仅涉及技术层面的控制，还触及到流程重新设计的根本性问题：许多组织尝试自动化当前流程，而非为智能体式环境重新设计工作流。

此外，许多所谓的智能体式举措实际上不过是伪装的自动化用例。企业往往在原本只需要简单工具就可解决的问题上应用智能体式技术，导致投资回报率低下。这种“智能体洗白”加剧了这个问题的复杂性，供应商将现有的自动化功能重新包装为“智能体”服务。[6]此外设计不当的智能体式应用实际上会给流程增加工作量，一些企业发现智能体式“冗余工作”会降低流程的效率。[7]

从本质上讲，智能体代表了一种全新范式，但如今大多数企业并未具备利用智能体蕴含的自动化机遇的条件。然而，我们已开始在领先的组织中看到一些迹象，表明通过战略性流程重新设计、架构现代化以及新型治理框架的构建，这些挑战是可以被克服的。

## 自主运营的架构

具有前瞻性思维的组织正逐渐超越试点项目阶段，转而实施系统化策略，推动智能体应用转型。他们的成功源于认识到有效的智能体应用需要的不仅仅是部署单个智能体。相反，它需要采取深思熟虑的策略，将智能体集成到系统和工作流程中，并在智能体投入应用后对其进行精细化管理。

### 重新设计流程使其成为智能体原生流程

领先的企业不会简单地将智能体叠加到现有的工作流程中。相反，他们会重新设计流程，以利用智能体的独特优势。这要求我们退后一步，审视整个端到端流程，而不仅仅是在当前运营中寻找自动化机会。智能体可以处理一系列事务、相互通信和协作以实现商业目标，但前提是底层流程必须经过结构化设计以支持这些功能。

英特尔全球战略联盟负责人、前人工智能战略副总裁布伦特·柯林斯表示：“现在是进行价值流映射的理想时机，以了解工作流应有的运行方式与实际运行方式之间的差距。

不要只是在现有基础上修修补补，而应利用这次人工智能变革的机遇，重新思考智能体如何才能最好地协作、支持和优化企业运营。”[8]

大多数企业现有的流程都是围绕员工设计的。智能体的运作方式则有所不同。他们不需要休息或周末。他们可以连续完成大量任务。当组织意识到这一点时，重新设计流程的机会就变得极具吸引力。这就是为什么在智能体方面取得成功的企业正在从始至终审视自身的流程。

企业软件和服务公司HPE正在开发一种智能体，正是考虑到了这种流程的重新设计。执行副总裁兼首席财务官Marie Myers表示：“我们希望选择一个端到端流程，在那里我们可以真正实现转型，而不仅仅是解决一个痛点。我们希望以不同的方式运营。”[9]

她的团队率先创建了一个名为Alfred的智能体，帮助完成内部运营绩效评估。Myers说，进行此类评估的过程非常耗时，但这也是从大型数据集发展而来的，这为智能体自动化提供了成熟条件。该团队开发的智能体由一个智能体前台用户界面组成，该界面与四个独立的底层智能体协同工作。这些智能体将查询分解为多个元素进行处理，对SQL数据进行数据分析，构建图表和图形来呈现数据，并将AI洞察转化为用户友好的结构化报告。智能体从公司的数据仓库中提取数据，该数据仓库位于其企业资源规划和客户关系管理系统之上。

Myers表示，她相信该项目为团队之外甚至HPE之外的人都有借鉴意义：“这正是我们选择这个用例的原因，因为它适用于不同的职能和行业。我们希望能够推动组织各个层面的变革。”

## 规模化数字化技能：John Roese谈使用智能体重塑业务流程

John Roese是戴尔科技公司的全球首席技术官兼首席AI官，负责领导公司的全球技术战略和AI转型计划。凭借数十年的企业技术经验，他专注于推动实用的AI实施，在保持严格的治理和安全标准的同时提供可衡量的商业价值。

**Q： 企业在AI 智能体方面缺少什么？**

**A：** 如果我们将智能体视为数字技能，那么当他们开始作为一个集体运作时，他们的真正价值就会显现出来。第一代AI工具，如聊天机器人和编码助手，非常擅长处理一维流程，如展示销售信息或编写代码。但是，当你进入一个复合的过程时——这个过程并不完全存在于一个域中——智能体是更好的工具。智能体能够在彼此之间传递上下文，跨边界推理，并通过智能体到智能体等协议进行交互。

大多数复合流程不仅仅存在于企业内部。第三方、软件供应商和SaaS提供商是该工作流程的一部分。智能体之间值得信赖、安全的互通至关重要。否则，我们永远无法将这些跨边界的过程数字化。大多数企业几乎没有将AI应用于单一流程。想象一下，如果你将AI应用于运行组织的复合流程，生产力会有多高。

**Q： 你是如何在内部付诸实践的？**

**A：** 我们现在有十几种智能体概念验证方案，都是致力于解决复杂性问题，如跨域的客户问题的报价或端到端补救，包括权利、计费和物流。我们非常关注投资回报率。我们不做科学项目。我们的智能体技术出现在销售、服务、供应链和工程领域，这些领域对公司的财务业绩有重大影响。

我们可能已经触及了20个数字化的企业流程。在2025年底之前，我们将拥有实时的自主系统，这些系统很可能作为第一代工具跨领域工作，这为我们明年大幅扩大智能体的使用奠定了良好的基础。

**Q： 您如何帮助组织考虑所需的成本和基础设施投资？**

**A：** 在我们流程的前端阶段，我们要求财务合作伙伴及相关业务部门负责人对重大投资回报率进行确认。该规定确保了实验性得以保持，只有在有可靠的投资回报率的情况下才能进行生产。

我们还意识到，你是将AI应用于流程，而不是个人、组织或公司。我们希望您非常清楚您正在改进的流程。

随着我们不断改进，我们在工作流程中已变得极为严谨。因此，我们不再允许个人设计自己的AI解决方案，而是创建了一个架构审查委员会来评估和批准AI投资和解决方案。

**Q： 您是否已经记录和衡量了现有的业务流程？**

**A：** AI是一种流程改进技术，所以如果你没有坚实的流程，你就不应该继续推进。首先要弄清楚这一点，否则你将会猜测该技术的应用切入点和情况。

我们清理了数据，并明确了现有流程。如果没有这一点，我们就会试图将AI应用于无法量化且可能不准确的事情上。

秉持这一理念，我们的服务部门已经将所有流程进行了数字化。我们将他们的所有数据整合到一个智能助手中，该助手分布于各个数字和人工渠道中，以预测下一步的最佳行动。其结果是，在成本和客户满意度方面，每个指标都有两位数的改善。[10]

### 旧有系统更换

当一个组织审视其端到端流程时，它可能会发现跨越多个系统的工作流，包括遗留软件。这对核心现代化战略产生一定影响。正如我们在去年讨论的《技术趋势》报告中所探讨的，AI越来越具备学习和理解定义企业运营的基本业务规则和工作流程的能力。各组织应该仔细思考什么构成了其真正的核心系统。

当智能体能够有效地弥合遗留系统的差距时，确定是否使用传统的应用程序现代化。

在丰田，团队正在使用一种智能体工具来更好地了解车辆到达经销商的估计时间，并将很快开始使用智能体来解决供应问题。该流程过去涉及50到100个主机屏幕和供应链团队成员的大量亲历亲为的工作。现在，则由一个智能体来完成相关工作。

从预制造到交付给经销商，向员工提供车辆的实时信息，所有这些都无需任何人与主机交互。

展望未来，该团队计划赋予智能体识别车辆运输延误的能力，并起草电子邮件以尝试解决该问题。

杰森·巴拉德说：“智能体可以在团队成员早上进来之前完成所有这些工作。”，丰田数字创新副总裁“我们已经做出了关键的决定，继续在这一领域进行更深入的投资。我们觉得这就是未来的差异化关键所在。”[11]

**管理硅基和碳基混合劳动力**

在实施智能体时，最重要的转变或许在于认识到智能体代表了一种新型劳动力，这种劳动力可能与人类（或碳基）劳动力有一些相似之处。一些组织开始超越将智能体作为简单的自动化工具的阶段，转而探索将其与自身的人力资源优化整合的方法。

这一变革代表了对工作内涵、工作方式以及工作执行者身份的根本性重新构想。这一转变的核心在于认识到智能体和人类工作者具有不同的技能组合。虽然智能体在特定流程方面表现出色，但人类对于应对不断变化的商业需求和复杂的问题解决场景仍然至关重要。

这种转型催生了人类员工正在走向的两个主要领域。

- 合规与治理：人类越来越关注验证、监督以及为智能体构筑护栏
- 增长与创新：他们还专注于重新构想运营并识别来自智能体的新机遇。

在保险公司Mapfre内部，智能体被广泛应用于各个部门，包括索赔管理领域。在这些部门中，智能体负责处理日常行政任务，如损害评估等。当涉及到更敏感的任务时就像客户沟通一样，一个人总是处于信息的循环中。Mapfre集团首席数据官Maribel Solanas Gonzalez表示，她会仔细斟酌将哪些任务委托给智能体，确保智能体能够安全、高效地完成这些任务。任何可能带来风险的内容仍需通过人类员工处理。这正开始改变工作的性质。该公司发布了一份《AI宣言》，强调优先发展治理良好、尊重人性且安全的AI技术。

“它是一款精心设计的混合体，”她说。“随着这些智能体的高度自治，它并不会取代人类，但它会改变（人类员工）目前的工作方式，让他们把时间投入到更有价值的工作中。”[12]

其他企业走得更远。生物技术公司Moderna最近任命了第一位首席人事和数字技术官，这实质上是将其技术和人力资源职能合二为一。此举是通过整合人员和技术来加速工作完成方式，从而推动公司运营模式的战略变革。

Moderna.[13]的首席人力资源和数字技术官Tracey Franklin表示：“人力资源部门在员工规划方面做得很好，IT部门在技术规划方面做的也很好。我们都需要考虑工作规划，无论是人还是技术。”

**专业型自动化与广义自动化**

成功的部署策略侧重于特定的、定义明确的领域，而非试图实现企业层面的自动化。广泛的自动化仍然是可能的，但需要多个专业智能体以协同方式共同运作，而非依赖单一的、整体式的解决方案。

组织面临着关键的构建还是购买的决策，这些决策通常取决于技术成熟度和特定的用例要求。研究表明，通过战略合作伙伴关系建立的试点项目实现全面部署的可能性是内部构建的试点的两倍，外部构建工具的员工使用率几乎翻了一番。[14]

**多智能体编排**

企业中的第一波生成式AI主要由通用聊天机器人组成，尽管这些机器人作为生产力工具很有用，但往往不能提供企业提高效率所需的自动化机会。借助

智能体技术，组织可以开发高度专业化的工具，自动执行特定任务。当这些“专家”以协同方式有组织地部署时，它们可以自动化整个工作流程。这一方法的实现得益于一系列促进智能体间交互的标准和协议。

模型上下文协议（MCP）：由Anthropic公司开发，MCP标准化了AI系统如何连接到数据源和工具，，为智能体访问企业资源提供了一个通用接口。[15] 虽然前景广阔，但MCP在处理复杂的企业安全要求和集成遗留系统方面存在局限性。

智能体间协议（A2A）：谷歌的协议允许跨平台的不同智能体之间直接通信，处理智能体发现、任务委托和协作工作流。[16]

智能体通信协议（ACP）：这是一个开放的协议，使智能体能够通过RESTful API 相互通信，允许智能体进行协作，而无论它们是在什么环境中构建的。[17] 由于可以在单个网络中协调的智能体数量的限制以及与现有企业工具集成的复杂性，ACP可能面临障碍。[18]

这些协议代表了专家所说的“AI微服务方法”的基础层：即在更接近工作流指令和数据所在位置的各种平台上部署大量规模较小、功能专一的智能体。这种方法具有诸多优势，例如降低了复杂性（因为较小的智能体更容易调试、测试和维护）；可扩展的编排，即其中可以组合多个专门的智能体来执行复杂的任务；以及平台灵活性，允许智能体在不同系统上运行，同时保持互操作性。

### 智能体的FinOps

随着智能体的持续运行，配置不当的智能体交互可能会触发级联操作，如不可预测的资源消耗和不断膨胀的成本，使成本管理变得至关重要。组织需要专门的财务运营框架（或FinOps）来监控以及控制智能体驱动的费用开支，并考虑基于代币的定价模型。这些框架通过资源标记、实时监控、自动资源管理（包括自动扩展和合理配置）以及强大的治理框架，有助于详细跟踪各项成本，[19] 实现对AI相关支出的有效管理。

### 推动智能体实施的五个问题

当组织开始他们的智能体之旅时，他们可以考虑五个战略问题，以帮助和推动现在和未来的应用。

- 将部署哪些智能体，它们将执行哪些功能?
- 与人类员工相比，成本情况如何?
- 哪些流程将实现自动化，效率达到什么水平?
- 未来四年，人类员工和数字员工的最佳组合是什么?
- 智能体最终会在五年后接管整个运营领域吗?

如今，大多数准备实施智能体的企业可能已经为前三个问题准备好了答案。然而，当他们考虑后两者时，情况变得更加模糊。这在很大程度上取决于智能体技术和底层生成式AI模型在未来的发展，以及这一发展如何推动劳动力构成和运营优先事项的变化。

## 人机协作推动差异化

未来的企业可能会经历工作基本性质的显著变化，这一变化将超越传统的碳基劳动力范畴，延伸至包括自主处理整个工作职能的数字智能体。正如我们所讨论的，公司已经开始开发混合型人类-数字劳动力模式。如果组织能够正确地把握这种平衡，它可能会成为未来大多数行业的主要竞争差异化优势所在。

### 自治频谱

组织应通过分级自治级别为智能体决策制定明确的界限，并辅以适当的人工监督触发机制。自主性谱系经历了三个不同的阶段。

- 增强：一种当今现实，智能体增强人类员工能力
- 自动化：一种新兴能力，智能体在人类定义的流程内自动执行任务
- 真自主：一种未来状态，通用AI使智能体能够在最小监督下工作

智能体实施的成功需要部署“智能体监督员”——主动地设计环节让人类员工进入工作流以处理需要智能体判断的异常。这不仅仅是检查智能体的工作，而是在关键决策点进行战略性的工作交接。在未来几年，随着AI技术的进步，可能达到通用AI，组织应该能够让智能体更独立地工作。领导者应该不断评估AI能力的状态，以确保他们正在将适合智能体处理的职责进行授权。

**智能体人力资源管理**

随着智能体在工作职能中的逐渐成熟，组织将需要同样成熟的方法来对其进行管理。这可能需要一个全新的智能体管理框架，该框架不仅依赖于传统的人力资源管理理念来处理在智能体与人类员工有相似之处的领域，同时考虑其独特的特点还要有所区别。人力资源管理的一些重点领域，如工作场所文化、员工忠诚度和员工激励等，将不适用于智能体，但仍将是组织管理人类员工的关键支柱。人类员工管理的其他功能可扩展到应用于智能体，即使它们在外表上略有不同。

**入职培训流程：**与人类员工一样，智能体也需要入职培训流程，在企业独特的数据和操作方面对它们进行培训的同时，智能体的人力主管也应接受相应的培训以及如何利用新智能体的教育。这将需要一种新的双管齐下的入职方法来引入数字员工，使智能体和人类员工都能为协作做好准备。

**绩效管理：**这可能是管理智能体与传统人力资源管理差异最大的领域之一。组织将需要系统来证明智能体做了什么，为什么他们做出了具体的决定，以及他们在谁的授权下行事。这需要数字身份系统、交易的加密收据以及每个智能体操作的不可变日志。随着智能体在企业运营中的推广，它们将创建生成大量的数据，超出人类管理者的评估能力范围，这可能会推动对管理绩效的额外智能体的需求。

**生命周期管理：**智能体将需要持续接受培训更新、调配部署到优先领域，甚至可能需要退休计划。各组织开始为智能体人分配个人名字以跟踪生产力贡献，同时意识到数字工作者最终可能会像人类员工一样纳税。[20]

**零信任架构：**实施临时身份验证系统可确保智能体操作得到持续验证和授权，就像人类员工必须定期完成身份验证任务才能访问企业资源一样。[21]

经过正确校准后，管理智能体的框架将推动人类和数字员工之间的强有力协作。然而，将智能体比作数字员工可能会限制智能体的潜力。若将其置于旨在衡量人类绩效的标准之下，则有可能导致其活动与更适合由人类员工承担的职能产生偏差。

**作为数字废气的数据**

在智能体驱动的环境中，系统生成大量描述所采取行动和结果的数据。今天，大多数智能体都不会根据自己的输出数据进行训练，但在未来，硅基员工的这种数字废气可以成为有价值的知识宝库，使智能体能够从中学习并提升自身能力。展望未来，关键的区别在于组织如何引导利用这些副产品来加强智能体学习和能力提升。

这代表了一种根本的思维方式转变。智能体的每一个推理行为都会生成令牌，这些令牌构成了可以强化学习系统的数据。未来最有可能产生重大影响的，将是对这些持续数据流的高级、复杂应用。

**智能体原生的未来**

审视系统现代化的未来时，初步迹象显示，混合式方法最有可能占据主导地位。这种方法中，智能体延长了旧有系统的使用寿命，而组织则致力于对关键业务流程进行有选择性的现代化改造。这种方法使组织能够从智能体能力中实现即时价值，同时又能保持对未来技术决策的战略灵活性。

向智能体的过渡不仅仅关乎技术层面的演进，它更是一场组织层面的变革转型，可能会从根本上重塑企业的运营模式、竞争策略以及价值创造的方式。

那些掌握了智能体原生流程设计、多智能体编排以及硅基员工管理等这些基本要素的组织，将具备在日益自动化、现代化的商业环境中蓬勃发展的能力。

成功的关键在于认识到AI和智能体转型并非要用机器取代人类，而是通过创造新型人类与AI协作模式，充分发挥人类和基于硅基员工的独特优势。那些能够找到有效推动这种协作模式的组织，将重新定义工作本身的未来。

## 崎岖的前沿：Ethan Mollick谈AI在职场中的作用

Ethan Mollick是宾夕法尼亚大学沃顿商学院的教授，著有《协同智能：与AI共同生活与工作》。他是AI在商业和教育领域实际应用的领军人物，以研究组织如何有效地采用AI并将其整合到运营中而闻名。

**Q： 从AI作为工具到AI作为劳动力的过渡在实践中是什么样子的?**

**A：** 许多组织的领导者并不清楚这意味着什么。通常会有大量含糊其辞的情况，比如“AI会做一些事情”或“你会管理一堆智能体”。但如果不重新思考和重新设计组织的运作方式，这一切便无从实现。

我发现这实际上并非一个技术问题，而是流程上的问题。这意味着你必须应对那些参差不齐的边界。AI已经非常擅长数学和编码，这对数学和编码任务有明显的影响，但也带来了一些不太明显的影响诸如在分析或与人会面等任务上。人类员工将不得不调整工作时间安排，以从事不同的工作内容。这并不是说智能体会包揽所有事物；它们主要负责基础性的繁重工作，所以我可以打电话给更多的组织来面试和访谈。领导者必须能够清晰阐述这一未来趋势。

**Q： 在智能体优先流程重新设计方面，组织需要考虑什么?**

**A：** 做AI工作需要三件事：领导力、实验室和群众基础。首先，你需要群众基础：组织中使用这些系统的每个人。其次，你需要一个实验室，它正在积极地进行全天候的实验，从群众中汲取想法和创意，并将其转化为真正的产品。最后，你需要具备协调一致的领导力。领导者必须考虑组织设计的问题。例如，如果你的代码编写速度比以前快 10倍或100倍，你还在做敏捷开发吗？敏捷没有那么快的速度，因此你便无需继续如此行事。

**Q： 哪些劳动力技能最重要?**

**A：** 有一种“使用AI”的技能，我们还不知道如何对其进行衡量或训练。这可能涉及主动性、勇于尝试的意愿、恰当的激励措施，以及成为所在专业领域专家的能力。

**Q： 你预计智能体何时接管运营?**

**A：** 我不知道，但智能体已经比人们想象的要好了。

真正的智能体已经来了，你只是没有使用它们，你必须构建它们，但这在今天是可行的，虽然没有未来的时间表。因为你现在完全可以利用当前的技术构建具有经济价值的智能体，而且企业正在构建以高精度自主完成大量工作的智能体工作流程。它们是否已经取代了所有的工作？不，我也不希望他们这样做。但如果你等到技术更成熟时再行动，那你就会遇到麻烦，因为这项技术已经存在了。[22]

# 尾注


1. 《亨利·福特语录》于2025年11月6日发布。
2. Gartner，股份有限公司，“Gartner预测，到2027年底，超过40%的智能体项目将被取消，”新闻稿，2025年6月25日。
3. 《2025年德勤企业新兴技术趋势调查》，正在出版中。
4. Gartner，股份有限公司，“Gartner预测，到2027年底，超过 40%的智能体项目将被取消。”
5. 德勤综合研究中心于2025年6月进行的2025年技术价值调查。
6. Gartner，股份有限公司，“Gartner预测，到2027年底，超过 40%的智能体项目将被取消。”
7. Bruce Gil，“‘Works’：AI生成的工作内容正在减缓一切，”Gizmodo，2025年9月23日。
8. 德勤云播客对英特尔AI战略副总裁Brent Collins的采访，2025年8月27日。
9. Marie Myers，HPE执行副总裁兼首席财务官，德勤访谈，2025年3月1日。
10. John Roese（戴尔科技公司首席技术官兼首席AI官），2025年9月29日对德勤的采访。
11. “用丰田的智能体重新构想运营”，Deloitte Insights，2025年12月3日。
12. Maribel Solanas Gonzalez，Mapfre Insurance集团首席数据官，德勤采访，2024年6月18日。
13. Tracey Franklin（莫德纳首席人事和数字技术官），2025年9月26日对德勤的采访。
14. Aditya Challapally、Chris Pease、Ramesh Raskar和 Pradyumna Chari，“AI鸿沟：2025年AI商业状况”，2025年7月。
15. Anthropic，PBC，“介绍模型上下文协议”，2024年11月25日。
16. Rao Surapanini 、 Miku Jha 、 Michael Vakoc 和 Todd Segal，“宣布智能体协议（A2A）”，谷歌开发者版，2025年 4月9日。
17. AgentCommunicationProtocol.dev，“欢迎”，访问日期为2025年11月6日。
18. Saad Merchant，“ACP：离线AI智能体协作的未来”，Alumio，2025年10月24日。
19. Kearney，“FinOps for AI和AI for FinOps”，2025年1月28日。
20. Jake Latimer，“AI会被征税吗？关于AI驱动企业的争论：2025年的技术税收之争”，Medium，2025年3月13日。
21. 黄，“智能体身份管理方法”，云安全联盟，2025年3月11日。
22. Ethan Mollick（宾夕法尼亚大学沃顿商学院教授），德勤访谈，2025年1月1日。

# 作者简介

**Jim Rowan**
jimrowan@deloitte.com

Jim Rowan是德勤美国AI主管，与外部技术组织、客户和德勤的商业领袖合作，帮助我们的客户实现他们的AI抱负。除了他的客户工作，Rowan还是德勤咨询公司的负责人。他的经验涵盖了生命科学、医疗保健和电信行业，重点是应用分析、规划、预测和数字化转型来增强财务职能。

**Nitin Mittal**
nmittal@deloitte.com

Nitin Mittal是德勤的负责人，领导德勤的全球AI项目。他就AI应用以及新兴技术对企业战略和竞争定位的影响向组织提供建议。在德勤，米塔尔负责塑造AI市场，并通过利用新兴技术创造新的商机。他还领导德勤自己努力成为一个全球AI驱动的组织，并改变他们提供专业服务的方式。

**Parth Patwari**
ppatwari@deloitte.com

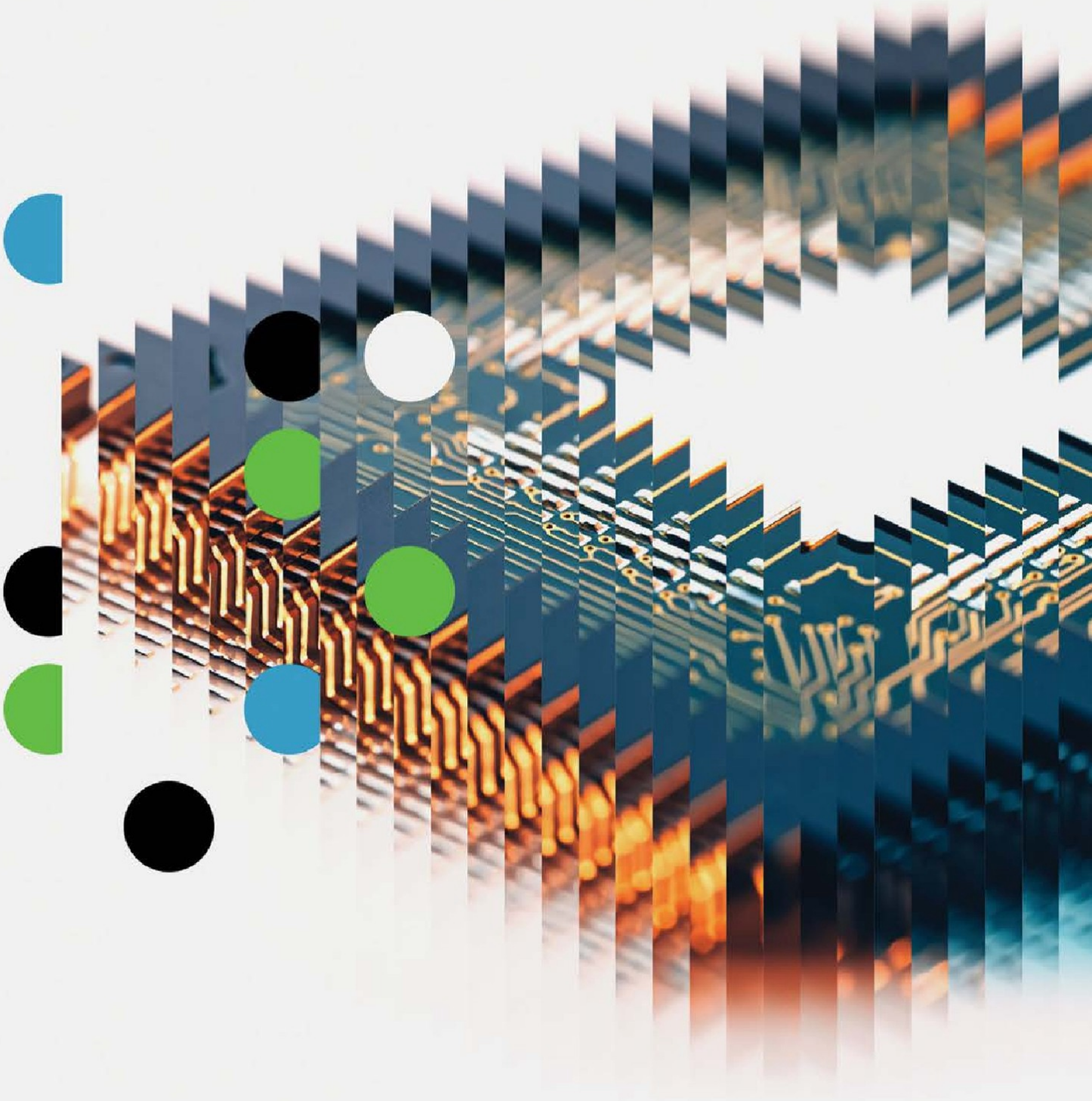
Parth Patwari领导德勤在美国所有行业的AI和数据实践。他在与资本市场和支付机构合作方面拥有丰富的经验，能够构建、设计和实施支持关键任务客户、财务、风险、监管和合规职能的大型系统。Patwari利用AI、分析和数据管理功能推动效率议程。

**Ed Burns**
edburns@deloitte.com

Ed Burns在CTO办公室领导客户故事倡议，该倡议被称为趋势线。该项目是对《技术趋势》和其他知名企业的重要研究投入。在担 任现职之前，他领导了一家科技新闻出版物，涵盖了AI、分析和数据管理的所有内容。

# 致谢

非常感谢德勤的许多主题负责人，他们为本章的研究做出了贡献：Jinlei Liu、Baris Sarer、Kate Fusillo Schmidt、Prakul Sharma、 Akash Tayal和 Ashish Verma。



# 积极反思：优化AI基础设施策略

随着AI从概念验证迈向生产规模部署，企业发现其现有的基础设施可能与这项技术的独特需求不相匹配

*Nicholas Merizzi、Chris Thomas和Ed Burns*

当生成式人工智能崭露头角时，企业纷纷开始构想下一代产品与服务。如今，人工智能已日趋成熟。然而，在其从概念验证阶段向规模化生产部署转型的过程中，企业却发现，现有基础设施策略根本无法满足人工智能的需求。

重复的AI工作负载意味着近乎持续的推理——即在实际业务流程中使用AI模型的过程。当采用基于云的AI服务时，这可能导致频繁调用API并进而推高成本。因此，一些组织开始重新审视用于运行AI工作负载的计算资源。然而，问题不仅仅在于成本，还涉及数据主权、延迟要求、知识产权保护和系统弹性。解决方案并非简单将工作负载从云端迁移到本地，反之亦然。关键在于构建能够针对各项工作负载灵活选用计算资源的基础设施。

在探索AI优化的基础设施时，各个组织都会发现，芯片组、网络和工作负载编排领域的进步能够满足企业各方面的关键需求。那些现在就采取了行动，同步推进基础设施现代化和员工能力提升问题的组织，将能够引领未来计算复兴的竞争格局。

## 推理经济学的警钟

AI消费的数学规律正迫使企业以前所未有的速度重新规划其基础设施。尽管推理成本大幅下降，在过去两年内降幅高达280倍，[1] 但企业的整体AI支出却呈现爆炸式增长。[2] 原因很简单：推理形式出现的的AI使用增量远远超过了成本降低的速度。

基于应用程序接口（API）的大语言模型（LLM）工具适用于概念验证项目，但一旦部署到企业运营中去时，成本便会高得难以承受。[3] 一些企业已经开始看到，每月用于AI的费用高达数千万美元。其中，成本最高的当属智能体型AI，这种技术涉及连续推理，这可能会使Token费用急剧攀升。

### 为什么组织正在重新思考计算

不断上涨的账单正迫使组织重新考虑其AI工作负载的部署方式和部署地点，但还有其他因素需要一并思考。

**成本管理：**各组织正迎来一个临界点，此时对于持续且高容量的工作负载而言，本地部署的成本可能开始低于云服务。当云服务成本占购置同等配置本地系统总成本的比例开始超过60%至70%时，这种情况便可能发生，从而使得资本支出变得更具经济性。

对于可预测的AI工作负载，投资比运营费用更具吸引力。[4]

**数据主权：**监管要求和地缘政治考量正推动一些企业将计算服务迁回本地，各组织不愿完全依赖位于本地管辖范围之外的服务提供商来处理关键的数据和提供AI能力。这一趋势在美国以外地区尤为明显，在那里的主权AI倡议正加速其基础设施投资。[5]

**延迟敏感性：**实时AI工作负载要求靠近数据源，尤其是在制造工厂、石油钻井平台和自主系统中，网络延迟将可能妨碍实时决策。对于响应时间要求在10毫秒或以下应用，系统无法容忍基于云的处理的固有延迟。

**弹性要求：**不可中断的关键任务需要本地基础设施作为主计算或备份系统，以防与云端的连接中断。

**知识产权保护：**由于大多数企业的数据仍然存储在本地，组织越来越倾向于将AI能力引入其自身数据中，而非将敏感信息转移到外部AI服务。这使他们能够保持对知识产权的控制，并满足合规性要求。部分由于这些因素，许多国家的公司正在以前所未有的速度扩充其新的数据中心能力。丹麦物业管理公司Thylander正在北欧建立新的数据中心托管设施，为AI工作负载中使用的尖端图形处理器（GPU）及其他硬件提供机柜空间、网络连接、电力和冷却支持。

Thylander数据中心首席执行官Anders Mathiesen表示，目前丹麦境内所有超大规模数据中心均归外国公司所有。然而，企业界日益呼吁提供更多选择，以便其数据能够由本国拥有并运营的公司进行存储和处理M “从数据主权的角度出发，思考究竟谁才是数据中心的所有者，这促使我们萌生了这样一个想法：我们希望为丹麦企业做些丹麦特色的事情，同时也为那些认为丹麦市场颇具价值的外部企业服务。”Mathiesen表示。[6]

### 基础设施不匹配

尽管企业可以利用这些因素来指导未来的举措，但其基础设施的现状可能会带来其他阻碍。现有的数据中心普遍采用架空地板、标准冷却系统、基于私有云虚拟化的编排方式和传统的工作负载管理模式，所有这些设计均针对机架式风冷服务器所进行的设计。而AI基础设施的技术规范——从GPU之间的网络需求，到InfiniBand等先进的互连技术——都要求采用传统企业环境中所不具备的架构方案。

## AI优化的数据中心

与云端或本地基础设施之间二选一不同，领先企业正在构建混合架构，充分利用每种平台的独特优势。这种做法标志着一种转变——告别过去十年占据主导地位的非此即彼的云端或本地化思维模式。

这种物理基础设施的不匹配可能成为企业扩大AI应用时的主要瓶颈。不过，具有前瞻性的组织正在开始探索未来数据中心的轮廓。

### 三层混合方法

领先组织正在实施三层混合架构，充分利用所有可用基础设施选项的优势。

**云服务助力弹性扩展：**公共云能够应对可变的训练工作负载、突发的容量需求、实验阶段以及现有数据集中化导致云端部署成为明智之选的各类场景。超大规模云服务商提供前沿的AI服务，简化了对快速演进的模型架构的管理。

**本地部署，确保一致性：**私有基础设施以可预测的成本运行生产推理高容量、连续性的工作负载。组织在构建内部AI基础设施管理专长的同时，能够更好地掌控性能、安全性和成本管理。

**边缘计算，实现即时响应：**本地处理以极低延迟快速应对时间敏感型决策，这一点这对于制造业和自动驾驶系统尤为重要——在这些领域，分秒必争的响应时间决定了运营的成败。

“云端在某些场景下确实很有意义，它就像是AI领域的‘一键启动’按钮，”AI领域思想领袖David Linthicum表示，“但关键在于为每项工作选择合适的工具。企业正在构建跨多种异构平台的系统，根据成本最优化来决定采用何种方案。有时用云端，有时用本地部署，有时则选择边缘计算。”[7]（完整问答内容请参见侧栏。）

## 混合现实检验：Dave Linthicum谈如何合理配置AI基础设施

Dave Linthicum是全球公认的AI、云计算和网络安全领域的思想领袖、创新者和影响力人物。他为全球2000强公司、新兴创新公司和政府机构提供思想领导力、架构和技术指导。

**问： 随着企业从以云为先的模式向混合模式演进，它们将面临哪些挑战？又有哪些解决方案？**

**答：** 最大的挑战是复杂性。当你采用异构平台时，你突然需要同时管理各种不同的平台，还要确保一切都能可靠运行。我们在多云采用过程中就看到了这种情况：企业一夜之间从管理5000个云服务猛增至管理10000个服务，而且必须在不同的平台上运行和运维所有这些服务。

企业无需再单独管理每个平台，而是需要采用统一的管理方法。我的移动平台与云端环境或桌面端的数据存储方式有何不同。您应当将所有这些复杂性下沉到另一个抽象层，在那里，你可以以组或集群为单位进行管理，而无需关心它们实际运行在何处。

否则，企业通过雇佣专业团队和购买特定平台的工具来应对复杂性。这种方式既昂贵又低效，还会侵蚀业务价值，因为你在不断放大复杂性通过临时流程而不是战略性思维进行管理。这实际上是为了减轻运营上的困扰，以便您能专注于真正关乎企业发展的关键事项。

**问： 德勤的研究表明，当云服务成本达到同等硬件成本的60%至70%时，企业应认真评估其他替代方案。在考虑从“云优先”转向混合模式时，企业还应关注哪些临界点？**

**答：** 在本地基础设施和公共云之间的各项条件均等的情况下，我每次都会选择公共云，因为它更简便，而且能为我提供可扩展性和弹性。不过，当云端成本达到同等硬件成本的60%至70%时，您就应该评估其他替代方案，如托管数据中心供应商和托管服务供应商商。这是一个切实可行、可量化的关键指标，有助于您基于数据做出关于基础设施部署的明智决策，不再一味采取“云优先”策略而无视经济因素。

**问：数据中心的可持续性问题如何解决？**

**答：** 归根结底，我们不可能阻止数据中心的发展，因为市场需求巨大。我住在弗吉尼亚州北部，在我此刻所处位置的10英里范围内就有100个数据中心。所以，如果我们确实要朝着这个方向发展，不如通过使用清洁能源来尽量减少对环境的破坏清洁能源的来源有多种，核能就是其中之一。这对很多人来说很可怕，但别无选择。

我认为，我在数据中心密集的地区，我们会看到小型核电站的出现。届时，大家都会像现在一样，直接从这些核电站获取电力。我附近就有一座核电站，专门服务于数据中心，但遗憾的是，它并非清洁能源。要想在保持业务可持续发展的同时，转向更环保的能源选择，这恐怕是我们唯一能接受的权衡。除非我们找到某种新型能源，否则电网根本无法以任何值得投入的速度扩容。

**问： 你对这个话题有什么独到见解，或者认为哪条传统观点是错误的？**

**答：** 这很简单。并非所有任务都必须跑在GPU上，我们得摆脱这种思维定式。几年前那种疯狂囤积GPU的现象简直荒谬至极。现实情况是，大多数真正能为企业创造价值的AI工作负载并不需要专门的GPU处理器，它们完全可以在CPU上顺畅运行。当然，如果我正在训练大语言模型，而且需要进行海量数据训练，那确实需要专用处理器，否则这项工作可能需要花上10年而不是短短几个月时间。不过，这类应用场景少之又少，绝大多数企业根本不会涉足如此高难度的AI项目。

### 计算基础设施部署的决策框架

制定计算基础设施决策的框架（图1）看似简单明了，但实际操作中，这类选择却很少能轻易做出。每个人都希望采用速度最快的硬件，运行最新的模型，并且项目启动和运行的障碍最少，然而这样做往往成本高昂。

正因如此，戴尔公司最近成立了一个架构评审委员会。该委员会负责评估新的AI项目，确保他们采用一致的工具，并基于成本、性能、治理和风险等因素，选择最优的基础设施。目前，戴尔正在四大核心领域内开发AI智能体用例，相关负责人正着眼于在这些高投资回报率的领域进一步拓展用例。随着项目数量不断增长，负责人表示，确保项目运行在适当的基础设施上至关重要。有时，这可能意味着要调用AI服务提供商的API；而在其他情况下，这意味着要完全使用本地部署的资源。

“如今，这些系统的资源密集度如此之高具备这种严谨的架构设计能力显得尤为重要。” 戴尔全球首席技术官兼首席AI官John Roese表示，“当你开始谈论推理模型和智能体这类技术，以及与之相关的成本时，拥有这样的架构规范就变得至关重要。”[8]（完整问答内容请参见侧栏。）

### 硬件架构革命

这一刻为企业提供了前所未有的机遇，使其能够摆脱以中央处理器（CPU）为中心的思维模式，转向专为AI优化的硬件架构。各组织正就处理器部署做出审慎决策，从通用计算逐步过渡到针对特定工作负载的优化。

这一演进涉及在单个系统中集成多种处理器类型：采用GPU进行AI处理、采用CPU进行编排及传统工作负载处理。

用于高效推理的神经处理单元，以及用于特定机器学习任务的张量处理单元。现在，服务器更新已涵盖混合CPU/GPU配置。过去，服务器机架上每个托盘可能配置四到八个GPU，并由一个 CPU协调器管理，而如今，我们越来越多地看到一个CPU配备两个GPU的配置模式。

图表1

## 算力负载部署决策框架


来源：德勤分析

定制化AI数据中心：这些趋势正汇聚成所谓的AI数据中心，这种数据中心的GPU数量相对CPU更多；采用新型服务器机型与编排，以应对混合工作负载；数据中心规制不断演变，以便于快速部署；处理器之间采用光网络连接，以降低延迟；同时，工作负载正逐步迁移并重构成适合利用GPU功能的模式。

**AI工厂的兴起**

AI工作负载正推动“AI工厂”的兴起：这是一种专为AI处理而设计的集成式基础设施生态系统。这些环境将多个专用组件整合到一个单一解决方案中：

- **AI 专用处理器：**GPU与高带宽内存共同封装，并经过特殊设计CPU针对AI编排而非一般计算任务进行了优化；
- **高级数据管道：**专门用于收集、清洗和准备数据的系统用于AI模型消费，消除传统的提取、转换、加载瓶颈；
- **高性能网络：**先进的互连技术，以最大限度地减少数据传输延迟包括光网络技术的进步以及专用的GPU到GPU通信协议；
- **算法库：**预先优化的软件框架，可将AI功能与特定业务相匹配目标是缩短开发时间并提升性能；
- **编排平台：**能够处理多模态AI工作的统一管理系统跨不同计算类型加载，实现各种AI技术之间的无缝集成。

这些AI工厂还可以通过服务模式提供多余的计算能力，使组织能够在保持对关键工作负载战略控制的同时，将未使用的处理能力转化为收益。

**绿地优势：John Roese谈有目的的AI基础设施**

John Roese是戴尔公司的全球首席技术官兼首席AI官，负责领导公司的全球技术战略和AI转型举措。他拥有数十年的企业技术从业经验，专注于推动AI的实践落地，在严格遵从治理和安全标准的同时实现可衡量的业务价值。

**问： 与AI基础设施相关的最大瓶颈和挑战是什么?**

**答：** 如今许多企业所拥有的基础设施，是为AI出现之前的时代所设计的，其架构巨册源自多云时代刚刚兴起之时，这些决策是由企业自身做出的：比如该用哪朵云、采用何种拓扑结构、以及在本地部署还是云端部署——这大概都发生在疫情之前。没人会那么聪明或幸运，能在设计架构时就考虑到后来根本不存在的东西。

很快，大部分基础设施能力都将服务于AI系统，而非传统的工作负载。AI工作负载需要加速计算，它们需要的不仅是数据，更需要一个知识层。这些工作负载具备可分布式的特点，且所处行业熵值较高，具有众多不同的实现路径。这在最基础的基础设施层面，是一种截然不同的工作负载。

**问： AI工厂的概念如何融入其中?**

**答：** AI工厂是专为AI打造的全新环境。要将原本专为传统企业应用和服务设计的旧有环境改造为能够顺畅运行AI的环境，难度很大。你需要一种加速计算架构，往往不仅限于CPU（中央处理器）。从网络角度来看，这种架构的拓扑结构虽然简化了，但速度却极快。存储环境实际上构成了一个知识层：向量数据库、图数据库、知识图谱、情境感知聊天机器人以及数据管道等。而实际的AI应用及其运行环境，则大多极为前沿和现代。

**绿地优势：John Roese谈有目的的AI基础设施（续）**

**问： 通常需要多长时间才能将其启动起来?**

**答：** 实际上，这比改造现有设施更快。我们已经建立了并行环境， 其中配置了GPU，并将知识层和其他基础设施无缝连接。数据网格将所有 数据整合在一起。AI工具与传统工具所使用的正是同一数据网格，但其实际物理拓扑结构——即它们所依托的基础设施——则由加速服务器、知识层数据管理、AI工作负载、可观测性以及控制机制组成。

将它作为一个独立实体来搭建，比试图改造现有环境要快得多。你可以购买一种设备，它基本上就是预先组装好的存储、计算和网络功能的集合开箱即用即可运行整套智能体AI系统。通过将其部署在现有设施之外，您可以将其与许多复杂性隔离开来，从而快速移动。
这听起来似乎会增加一笔额外成本，但实际上并非如此。试图将AI功能融入您现有传统环境所涉及的运营成本，很可能高于构建一套全新的专用基础设施。

**问： 可持续性如何融入基础设施决策过程?**

**答：** 能源效率是规划过程中的一个关键考量因素。先进冷却系统、热管理解决方案和服务器领域的创新，可以在最大限度地提高每瓦能耗性能的同时，助力组织监测并降低其能源消耗。

您面临的最大的选择之一，就是何时使用液冷方案。例如，直接液冷冷却效率至少可比自然风冷高出一倍，因此采用直接液冷的单个机架有助于降低成本并缩小占地面积。

其次，重点关注您的传统基础设施。IT资产利用率低下是数据中心能源浪费的最主要原因。如果您能优化传统基础设施，以减少浪费并提高效率，或许就能降低AI扩展带来的额外环境影响。

最后，AI的大部分工作负载都可以转移到客户端设备上。一台AI PC是一种极为节能的分布式计算环境。它早已融入能源网络，也存在于您的碳足迹中。相当一部分计算任务可以从数据中心转移至这些设备上。根据工作负载的需求，如果将部分功能分散到给这些高效能的AI PC上，您就能大幅降低整体碳足迹。

## 数据中心的新前沿

当前AI基础设施的变革仅仅标志着一场更广泛计算革命的开始。在未来的五到二十年时间里，随着新兴计算范式的逐步成熟，数据中心需要持续演进，以适应针对特定应用日益专业化的工具需求。

### 基础设施持续演进

定制硅集成正加速从通用芯片向为特定AI任务设计的专用处理器迈进，这包括用于模式识别应用的神经形态计算[9]，以及旨在实现更节能数据处理的光学计算——后者正日益成为AI领域的关注焦点。[10]

一旦量子计算技术实现规模化，其与生俱来的特性可能会从根本上改变数据中心的设计需求。[11] 量子系统需要专门的基础设施，包括冷却系统、先进的外形规格，以及对噪音和温度敏感度的极致控制，这些都与当前AI基础设施的需求截然不同。

管理这种混合架构需要全新的专业知识和管理工具。未来的编排层可能会用专门为AI工作负载设计的平台来取代传统解决方案。这些系统不仅能够管理传统的虚拟机和容器，还能够管理量子处理器、神经形态芯片以及光计算阵列。

### 劳动力转型要求

基础设施转型可能需要整个IT组织进行技能再培训。数据中心团队很可能需要从传统的服务器管理转型为面向AI优化的基础设施运营、GPU集群管理、高带宽网络以及专用冷却系统管理。

网络架构师面临这样的挑战：需要针对以AI为优先的流量模式和高吞吐量需求进行设计，而这些需求与传统的企业网络有着根本性的差异。AI带来的网络需求——包括GPU之间的通信、海量数据传输需求以及超低延迟需求——需要具备许多组织所欠缺的专业技能。

造价工程师需要在混合计算组合优化领域培养专业知识，不仅需要了解云端经济性，还需要深入把握不同基础设施方案之间的复杂权衡。这包括熟练掌握新的财务模型，这些模型能够充分考虑GPU利用率、推理经济性以及混合成本结构。

经过多年的云迁移，许多组织内部的数据中心专业技能已经不复存在，导致它们难以找到精通AI基础设施要求的专业人才。这种人才缺口既是一个挑战——尤其是对于那些已经完全转向云端的企业而言——同时也为愿意投资于员工发展的组织提供了机遇。

**AI智能体管理AI基础设施**

随着AI基础设施的日益复杂，传统的IT操作手册可能难以满足AI工作负载所需的动态优化需求，从而催生了专为IT运维设计的AI协同助手，这些协同助手能够汇总告警信息、提出根因分析并给出修复建议[12]

这些智能体正逐步扩展到容量规划和供应商选择领域，例如亚马逊云服务推出了一系列AI模式应用，可自动分析容量预留情况，并通过Amazon Bedrock智能体推荐相应操作方案。[13]这标志着迈向完全自主智能体的前兆——未来的智能体应能动态地统筹模型选择、实例类型优化、按需与预留定价的权衡，以及多云环境下的成本和碳排放优化。

采购正逐渐从周期性、手动的方式转向算法化和持续化的模式。各组织可能会越来越多地依赖AI智能体，根据工作负载需求、成本波动和性能要求，实时做出基础设施决策。

**可持续数据中心创新**

AI基础设施对环境的影响正推动可持续计算方法的创新。政府与私营部门的多项举措正在探索以核能为数据中心供电、实现零碳排放的技术，不过目前这一技术的实施实施仍仅限于超大规模云服务商以及拥有雄厚资本实力的机构与组织。

微软的Natick项目证明，水下数据中心容器能够以海水作为散热介质，提供实用可靠的计算服务。不过，该公司在完成概念阶段后已终止了这一研究计划。[14] 与此形成鲜明对比的是，中国海兰信Highlander已部署了商用水下数据中心模块，并正在获得政府正式支持的情况下扩大业务规模。[15]

可再生能源的融合正在加速，例如德克萨斯州数据城项目，该项目计划在未来实现完全由可再生能源驱动的数据中心运营，并具备未来整合氢能源的能力。[16]这些举措正指向可持续计算基础设施更广泛的发展趋势。

新兴概念包括利用太阳能运行并直接向太空辐射热量散热的轨道数据中心，从而 完全无需冷却水。像Sophia Space和Lonestar这样的公司正在开发在轨计算能力，其中一些公司已经实现了月球数据中心有效载荷的初步飞行测试，但实际应用仍需数年时间。[17]

## 计算领域的复兴：AI基础设施作为战略差异化优势

成功驾驭这一基础设施转型的组织，有望在AI部署与运营种获得可持续的竞争优势。而那些未能及时适应的组织，则很可能面临成本攀升、性能受限以及战略脆弱性加剧等问题，因为AI正日益成为企业运营的核心要素。

这场AI基础设施的转型，不仅仅是一次临时的市场调整；它标志着企业对待计算资源方式的根本性转变。正如过去十年云计算重塑了IT战略一样，混合AI基础设施很可能将定义未来十年的技术决策方向。

计算领域的复兴已然开启，其成果将决定哪些组织能在AI驱动的商业环境中蓬勃发展。

# 尾注


1. 斯坦福大学人类中心AI研究所，“2025年AI指数报告”，斯坦福大学，访问日期为2025年11月12日。
2. Sarah Wang、Shangda Xu、Justin Kahl和Tugce Erten，“2025年100名企业首席信息官如何构建和购买AI”，Andreessen Horowitz，2025年6月10日。
3. Chris Thomas、Akash Tayal、Duncan Stewart、Diana Kearns Manolatos和Iram Parveen，“贵组织的基础设施是否已为新的混合云做好准备？”Deloitte Insights，2025年6月30日。
4. Thomas、Tayal、Stewart、Kearns Manolatos和Parveen，“贵组织的基础设施是否已为新的混合云做好准备？”
5. Exasol，“云遣返的兴起”，2024年11月6日。
6. “丹麦可再生能源投资公司的新资产类别：AI就绪、可持续的数据中心”，Deloitte Insights，2025年12月5日。
7. David Linthicum（德勤前首席云战略官）于2025年9月8日接受德勤采访。
8. John Roese（戴尔科技公司首席技术官兼首席AI官），2025年9月29日对德勤的采访。
9. 美国国家标准与技术研究所，“神经形态计算导论，为什么它对模式识别如此有效，为什么它需要纳米技术”，2025年 11月12日访问。
10. Kazuhiro Gomi，“光学计算：它是什么，为什么重要”，《福布斯》，2024年9月10日。
11. Christopher Tozzi，“评估量子数据中心的状态：承诺与现实”，《数据中心知识》，2024年2月8日。
12. ServiceNow，“现在协助IT运营管理（ITOM）”，2025年1月30日。
13. Ankush Goyal、Salman Ahmed、Sergio Barraza和Ravi Kumar，“通过AI驱动的容量洞察优化ODCR使用”，亚马逊网络服务，2025年6月5日。
14. Sebastian Moss，“微软确认Natick项目水下数据中心已不复存在”，数据中心动态，2024年6月17日。
15. Peter Judge，《数据中心动态》，2023年4月4日，“中国汉兰达完成首个商业水下数据中心，寻求出口”。
16. 燃料电池工作，”能源丰度公布数据城，得克萨斯州一世界上最大的24/7绿色动力数据中心枢纽，具有未来的氢气集成，”2025年3月24日。
17. Mandala Space Ventures于2025年5月19日发布了“Sophia Space：世界上第一个可扩展的太空数据中心”；Lonestar Data Holdings，“月球数据中心在登月途中首次取得成功”，美通社，2025年3月5日。

# 作者简介

**Nicholas Merizzi**
nmerizzi@deloitte.com

Nicholas Merizzi是德勤咨询公司的负责人，也是公认的数字化转型领导者。他是德勤Silicon2Service和AI基础设施的负责人，在那里他与组织合作，加速技术现代化，释放云潜力，并整合AI驱动的解决方案。Merizzi将深厚的基础设施经验与战略愿景和云创新相结合，引导客户应对数字化变革的复杂性，以实现他们的技术目标。

**Chris Thomas**
chrthomas@deloitte.com

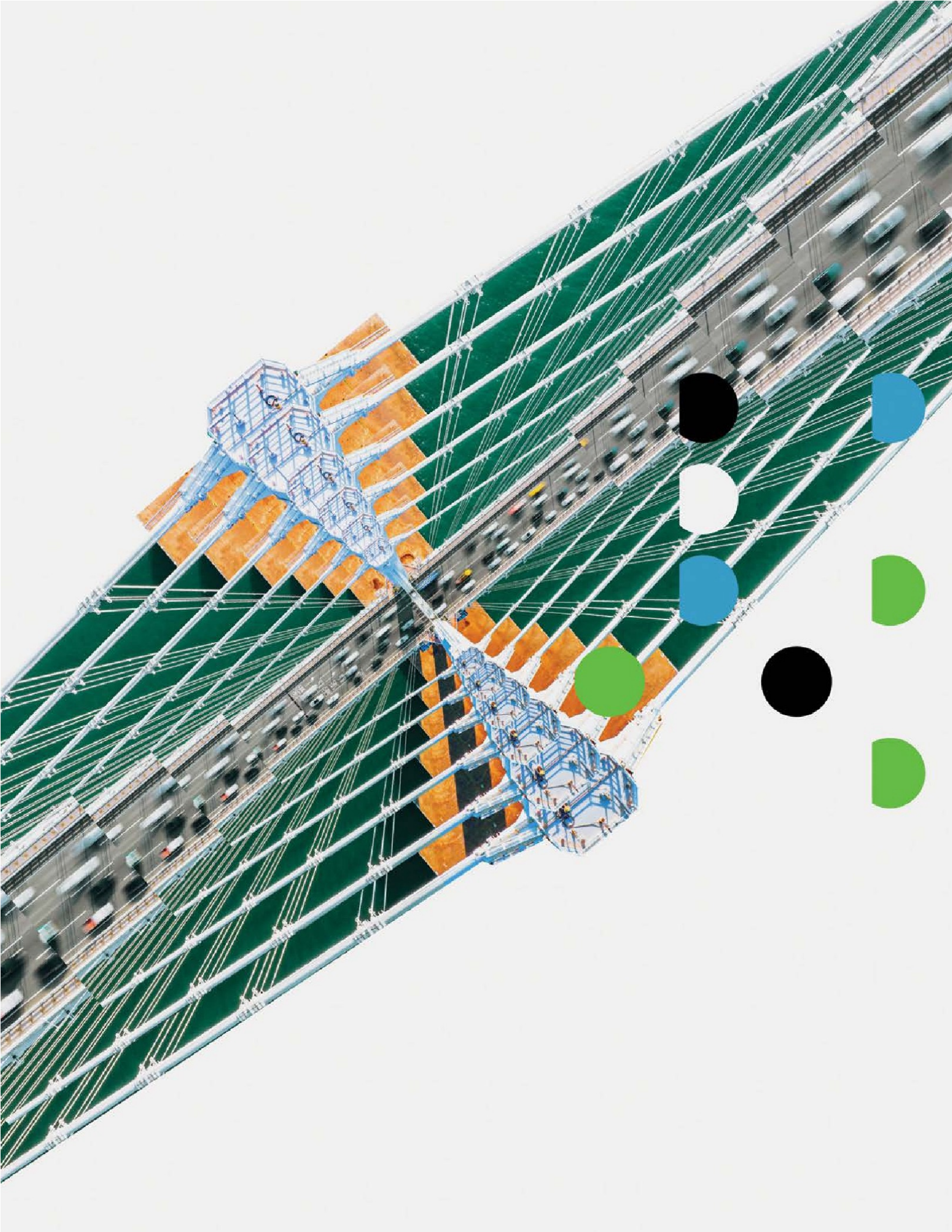
Chris Thomas是德勤咨询公司的负责人，也是美国混合云基础设施的领导者。他拥有超过25年的跨行业战略咨询和实践云转型经验，领导德勤美国AI与工程业务，为混合云基础设施提供服务，帮助客户优化混合云战略，建立面向未来的组织。他拥有与高级管理人员合作的丰富经验，通过以云为中心的运营模式、大规模技术转型、战略成本优化、全球外包计划和未来计划的劳动力来实现业务成果。

**Ed Burns**
edburns@deloitte.com

Ed Burns在CTO办公室领导客户故事倡议，该倡议被称为趋势线。该项目是对《技术趋势》和其他知名企业的重要研究投入。在担 任现职之前，他领导了一家科技新闻出版物，涵盖了AI、分析和数据管理的所有内容。

# 致谢

非常感谢德勤的许多主题负责人，他们为本章的研究做出了贡献：
Bernhard Lorentz、Baris Sarer、Duncan Stewart和Rohit Tandon。



# 脱胎换骨：重塑一个AI原生技术组织

## 定义未来技术组织的关键是什么？领导者该如何开始着手构建？

*Lou DiLorenzo，Jr.、Anjali Shaikh、Michael Caplan和Erika Maguire*

渐进式技术变革的时代已经落幕。在短短几年内，AI已经从工作流自动化跃升为重塑技术组织的核心架构和能力。[1]

根据德勤《技术架构展望2025》调查，78%的技术领导者预计在未来五年内AI智能体将广泛、有针对性或变革性地融入到技术架构重塑工作中。[2]

然而，这将不仅仅是工具和员工配置的变化。AI也会重塑技术团队的结构、治理和领导方式。未来的模式将会更精简、高效，并把AI融入到架构到交付的每一层中，将技术组织从“成本中心”转变为持续学习和不断优化的创新进化引擎。

莫德纳首席人才和技术官Tracey Franklin表示 “智能体和人类员工在工作方式上深度融合将很快实现，而且这一切会来得非常快，快过大多数公司准备的速度。” “企业需要更擅长快速迭代AI创新计划，因为 ‘一劳永逸’ 的时代已经结束。”[3]

虽然对于如何构建一个适应AI时代驱动的技术组织，并没有一个确切的、明确的蓝图，但前进的道路正在逐渐清晰，未来的高绩效者不仅会跟上AI的步伐，还会借助它开拓全新的领域。如今，每位领导者面临的问题不是AI是否会改变技术组织，而是他们能多快地释放其全部潜力。

## AI如何重塑技术组织

德勤的技术支出展望发现，64%的受访企业组织计划在未来两年内增加AI投资[4]，这清楚地表明，领导者认识到AI可以在整个企业中带来巨大的价值和变革潜力。虽然大多数人承认他们仍处于生成和智能体的探索阶段（图1），但数据显示，AI正从优先事项、人员到目标等多个方面重塑技术组织。

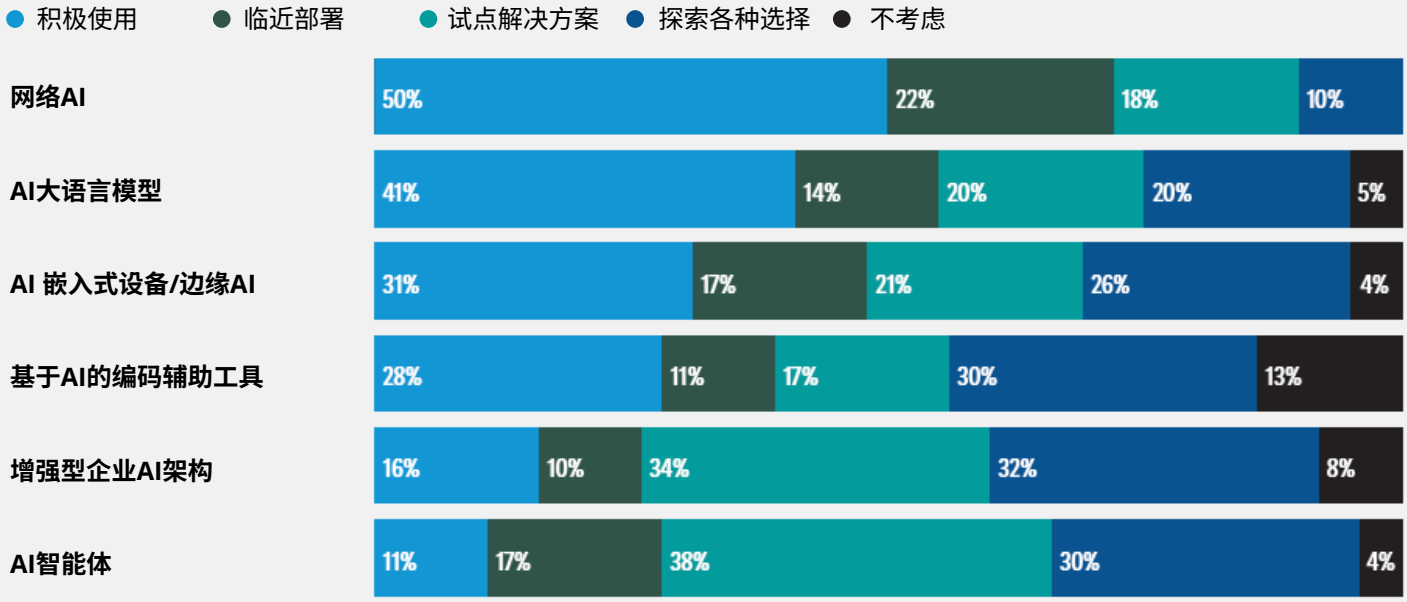
**优先事项。**德勤2025年技术高管调查中的首席信息官（CIOs）特别指出，利用AI、数据和分析的全部潜力，列为他们投入最多时间和精力的领域。[5] AI已经成为许多高管的首要考虑因素，其中，生成式和代理式AI也已位于技术组织首要议程，企业在大规模的投资。未来两年，分配给AI的技术预算比例预计将大幅上升，平均从8%上升到 13%，突显出AI正从实验创新转向核心战略。[6]

**人员。**在同一项调查中，近70%的技术领导者计划针对AI直接[7]扩大团队，这清晰体现出AI应用从“对失业的担忧”到“员工增强与协同”的转变。AI的持续发展势头也在创造新的角色，如莫德纳的首席人才和技术官，以及一线工程师和其他岗位。[8] 例如，AI架构师角色的数量预计将几乎翻倍，从现在的30%增加到未来两年的58%。[9] AI正在推动工作方式变革，不再是一种“即插即用”的工具，而是一种需要深思熟虑的设计、集成和治理的技术——这些任务需要专业知识。

图表1

## 虽然组织仍在试行AI技术，但广泛的实验趋势表明，重新构建技术职能的势头强劲

Q： “贵组织目前采用以下每项技术的阶段是什么？”




**目标。**随着AI在CEO当前和未来的战略中发挥着关键作用，[10] 技术组织的职责正在发生变化。如今首席执行官们希望技术领导者推动业务战略实现，而不仅仅是运营IT。大多数大型企业（德勤技术高管调查中66%）将他们的技术组织视为收入创造者，而不是服务中心，当被问及技术组织在塑造业务方面的作用时，德勤技术支出展望报告中的最主要的回答是“战略领导者：以技术为重点，推动整体业务战略实现”。[11] 越来越多的首席信息官直接向首席执行官报告（2025年[12]为65%， 2015年[13]为41%），这进步表明技术和AI不仅仅是运营问题，它们已成为增长、创新和竞争定位的核心能力。技术组织使命正从 “维持运营” 转向 “引领未来”。

## 为AI驱动的未来做准备的策略

随着AI技术的持续演进，组织也正在积极评估他们的技术运营模式。事实上，当被问及如何调整技术运营模式以满足不断变化的业务需求时，只有1%的受访IT决策者表示他们没有进行重大变革。[14]

为AI驱动的未来旅程做好准备将取决于组织的成熟度和优先事项等因素，并可能从增加AI和自动化的应用开始。除此之外，以下是当今组织如何规划AI驱动的未来。

### 系统现代化始于业务而非技术

71%的受访组织目前正在对核心基础设施进行现代化改造，以支持AI的实施，23%的组织将年收入的6%至10%投资于核心企业系统的现代化改造。[15] 但是认知还不够，关键是解决真正的业务问题，而不仅仅是技术升级。

博通首席信息官Alan Davidson表示：“现代化不是为了技术而技术，它是为了解决成本、产品销售等基本业务问题”。“AI是一个很好的例子。AI技术的发展速度如此之快，以至于今天关于AI的讨论与六个月前已大不相同，因此制定一个战术计划非常重要。如果不聚焦于解决具体的业务问题，确定想要获得的业务价值，投资AI很可能就没有回报。”[16]

### 面向模块化和可视化的架构

AI驱动的、面向未来的企业架构不能建立在“为维持运作而拼凑起来的传统平台”上，这或许解释了为什么 66%的受访组织正在试行或探索围绕AI增强型企业架构的相关方案。[17] 当新兴技术与端到端的企业系统融合使用时，它们可以带来更多的价值。新的架构要高度模块化和高度可视化 [18] 其核心，是赋能企业通过分析系统的外部输出不断观察、理解和优化系统。

西部数据首席信息官Sesh Tirumala表示：“在西部数据，我们正在开发一个高度可视化架构，以帮助我们采取整体方法来管理我们的技术环境”。“我们不是在等待完美的AI解决方案，我们宁愿在小型试点中快速失败，也不愿错过整个浪潮。”[19]

可口可乐公司也在优先采用模块化方法。 高级副总裁 兼首席信息官Neeraj Tolmare表示：“对于全球性组织来说，单一方案很难通用于所有情况。世界各地的工作方式并不相同。我们的做法是构建一个模块化架构和一套指导性核心原则，并由一个敏捷团队提供支持，该团队能够根据需要快速运营并进行本地化。”[20]

### 人机协作是技术人才战略的核心

德勤最近的研究突显了科技人才格局的快速演变。随着组织采用新兴技术，最受期待的新岗位包括：

- 人机协作设计师，负责设计人与智能系统之间的无缝交互；
- 边缘AI和嵌入式系统工程师，将AI能力直接带到设备和互联基础设施上；
- 合成数据的数据质量专家，确保为AI系统提供训练数据的可信度、价值和代表性；
- AI提示工程师和模型训练师，优化AI输出并定制模型以满足特定业务需求 。[21]

为了让AI在实践中发挥作用，考虑一下它如何既能成为技能提升引擎，又能成为弥合知识差距的工具。“即使你不是JavaScript专家或产品经理专家，AI也可以帮助弥合这一差距，甚至填补这一差距。”《凤凰项目》合著者和新出版的《Vibe Coding》一书的作者Gene Kim表示。[22] 他补充道，随着组织重新考虑他们的技术人才战略，考虑到AI可以做什么，他们需要在团队中拥有多大程度的功能专业知识是有帮助的。这有助于明确哪些领域应优先投入技能提升或再培训。（完整问答请参见侧栏。）

虽然AI可以普及能力和专业知识，但未来的竞争优势可能不仅仅来自采用AI工具，还来自建立能够设计、管理和优化人机协同工作方式。

未来不是人类或机器，而是人类和机器的结合。[23]

### 通过治理提升变革速度并管理风险

虽然这并非易事，但航空航天和国防公司RTX的首席数字官兼企业服务部门负责人Vince Campisi分享了他在AI时代调整治理的策略：“将治理分为三个维度：地图、衡量和监控。这意味着团队可以绘制行动地图以跟踪进度，衡量结果以查看是否实现了他们想要的结果，并监控质量以确保实现最初的目标。接下来，在战略指引下专注于战术落地。随着AI变得越来越具有自主性，组织可首先基于领导目标建立可解释性和可审计性治理机制，以便人类可以验证和信任其结果。[24]

## VIBE转变：Gene Kim论企业IT中AI驱动编码

Gene Kim是一位研究高绩效技术组织的研究员和《华尔街日报》畅销书作者。他曾任首席技术官(CTO)，并组织年度企业技术领导力峰会，他的书已售出100多万册。他的最新著作《Vibe Coding》是与Steve Yegge合著的（请参阅侧栏“从作家到导演：软件开发人员的转变”）。

**Q： AI编码工具如何改变企业格局？**

**A：** AI正在创建我所说的“自主”团队，在那里你不一定需要在每个领域都有深厚的功能专业知识，因为AI可以帮助弥合或填补这些空白。你可能不是数据库专家、业务专家或产品经理，但AI可以帮助你在这些领域更独立地工作。

任何业务领域的专家，无论是销售、营销还是客户支持方面的专家，再加上开发人员，现在都可以在没有太多监督的情况下完成伟大的事情。一位高级技术负责人对我说：“在我职业生涯的20年里，我一直听说我交付不足、迟到、无法兑现承诺。现在情况正好相反——我总是被告知我走得太快，需要放慢速度。”这就是我们所有人都向往的状态。

**Q： IT领导者应该如何让他们的团队做好准备，而不仅仅是说“去学习用AI编程”？**

**A：** 取得最大成功的人往往是更资深、技术头脑更敏锐的领导者，他们了解局限性，但也看到了潜力。作为一名领导者，你需要设定一个基调，即时间既不能被储存也不能被创造，所以如果有什么东西可以节省我们的时间，我们就需要利用它。

有趣的是，许多高级工程师实际上正在抵制AI编码工具。这项技术仍然是笨拙和不可预测的，所以许多受过传统训练的程序员都很抗拒，认为他们的训练方式更好。正是因为工具简陋，才需要培训。你不能只尝试一两次就放弃，你需要了解一些理论以及它们在内部是如何运作的。

最近一份关于AI辅助软件开发状况的报告中的一个关键见解让我印象深刻：对AI的信任与使用频率和持续时间直接相关。你使用这些工具越多，就越能理解它们的特性和局限性。你开始给他们看到更多更大的问题，这也将就是你看到巨大回报的地方。

**Q： 对于面临这一转变的首席信息官和IT领导者，您有什么建议？**

**A：** 领导力对于帮助那些不愿看到价值并冒着被甩在后面风险的高级工程师至关重要。虽然招聘总体上有所下降，但正在发生的招聘可能会有利于使用AI的开发人员，从这个角度来看，你会选择一个利用AI来加速工作的人，而不是一个坚持手写每一行代码的人。

领导者在决定谁获得生产率盈余方面也发挥着至关重要的作用。如果不公开讨论AI，人们可能会在一小时内完成一天的工作，而不会告诉任何人。但在一种共享AI实践的文化中，这位工程师可能会说，“我在一小时内完成了五天的工作——这就是方法。”这种知识共享的价值远远超过节省的时间，组织也从中获益。

**Q： 你对AI在企业IT中的发展有什么看法吗？**

**A：** 有两个可能不被主流认可的观点。首先，我相信手工编码的时代即将结束。没有人能说服我相反的观点。

其次，我真的不在乎AI是否会变得更好。即使AI的效用停留在目前的水平，我也会非常感激，现有的AI的作用已堪称奇迹。我们并不需要取得重大进展才能让它变得有用，它已经有用了。这意味着任何软件工程师或领导者都没有理由等待。现在加入吧！

### 大胆创新：重塑而非渐进式变革

转变技术组织需要的不仅仅是一系列小而安全的步骤——它需要一个大胆的的愿景，重新构想可能的事情。那些具有雄心勃勃目标的组织，利用AI的应用远远超出了战术性的自动化，而是彻底重塑技术、人才和战略的融合方式。

UiPath首席执行官兼执行董事长Daniel Dines表示："与其陷入概念验证的循环，不如考虑解决你最大的问题，争取重大的成果。""一旦有了显著的成功，你就可以证明，不仅有机会重新思考业务流程，还有提升生产力和挖掘新收入来源的潜力。越早开始，你在通往这些目标的旅程中就越能占据有利位置。"[25]

### 重新定义首席信息官(CIO)的角色

随着AI的普及，首席信息官（CIO）的职责正从技术战略家扩展到AI布道者。事实上，在技术高管调查中，70%的首席信息官表示，他们在组织中与AI时代的主要角色要么是在整个企业中实施AI，要么是作为布道者，帮助团队看到技术的潜力。[26] 随着AI应用渗透到企业内部各个组织，IT的中心化程度降低，首席信息官从基础设施的所有者转变为了协调者和集成者。事实上，近三分之一的首席信息官表示，在未来18个月内，协调其他技术领导者至关重要。[27] 现在，这一角色要求更深度地融入业务战略和企业转型，使首席信息官既是变革的推动者也是负责任的看门人。

西部数据的Tirumala补充道："首席信息官们更像首席集成官，因为他们的很大程度职责是确保 SaaS 和其他应用程序有效地协同工作。今天，我认为我的角色是传统首席信息官加上首席数据官、首席AI官和首席数字官的结合。""这个时代是技术领导者站出来的机会。我们了解技术、数据和流程。不要等待授权——要作为合作伙伴积极参与，要能阐明进取的数字蓝图并制定路线图。实现收入增长和商业模式转变，以及管理风险的战略，专注于速度、敏捷性、结果和价值，如果方法正确， 以后就不需要后悔了。"[28]

## AI驱动的技术组织特征

每个企业的AI之旅都各不相同，但成功的AI技术组织有着共同的特征。这些特征代表了在AI驱动的世界中蓬勃发展的技术组织的新标准。

### AI作为核心合作者

未来的技术运营模式将AI从附加工具或效率提升到企业各个领域的嵌入式能力升级——从决策、运营到产品开发。作为共同创造者，AI可以加速路线图绘制，自动化反馈循环，并实时重新确定工作的优先级。就像之前的云和移动革命一样，这一转变将AI定位为竞争优势的下一个核心能力。

实现这一愿景需要云原生、平台驱动的基础。在德勤技术支出展望中接受调查的48%的组织表示，他们目前正在扩展云原生和DevOps实践，以更好地将技术与业务需求相结合。[29] 云不再只是基础设施，它是速度、灵活性和创新的引擎。模块化、API优先的自助服务平台实现了快速扩展，同时减少了基础设施开销；平台工程和编排确保了跨产品线的一致性、治理和重用。在这种模式下，技术组织成为企业AI的架构师，提供标准化、安全和可扩展的构建模块，使团队能够自信、一致地采用AI。

### 为速度而重新设计的产品

在未来的几年里，传统的项目团队可能会转变为精简、跨职能的团队，围绕产品和价值流协同，从而缩短从概念到客户的闭环，并固化对成果的责任。57% 的组织报告称，他们已经从项目模式转向产品模式，以使业务和IT更紧密地联系在一起。[30] 在这种模式下，产品路线通过共享的面向客户的平台提供以用户为中心的功能，敏捷小组负责工作方式和工具选择，一线工程师与产品或客户团队一起工作，缩短价值实现的速度。[31] 其结果是更强大的责任感、更快的迭代和更清晰的业务价值。

AI、认知工具和机器人技术可以通过将持续的规划、交付和实验嵌入日常工作中来增强这一结构。预测模型和智能自动化可以取代人人协作，而AIOps领导等角色出现了，传统的项目管理逐渐淡出。组织敏捷性可以扩展到IT之外，创建一种运营模式，持续适应不断变化的优先事项，同时在团队层面保持速度和问责制。

**人机团队规模化**

未来的劳动力将人类的聪明才智与机器智能融合在一起，三分之二的组织正在试点、积极使用或接近部署智能体。[32] 这些未来的团队可能是人类、AI智能体和协同工具的无缝融合，人类贡献创造力、监督和道德判断，AI带来速度、精度和模式识别，这种模式将推动跨产品、服务和运营的持续实验、快速原型设计和可扩展创新。随着智能体承担更复杂的任务，AI技能运用能力成为每个角色的核心技能。技术组织未来的成功可能取决于协调这种人机合作模式，确保人类和智能体一起学习和进化。

**嵌入式治理**

现代科技组织正在用适应性治理周期取代缓慢、一次性事后监督：持续的AI辅助机制，在不牺牲安全的情况下保障了速度。预测模型和实时信号正在将决策从主观的、基于意见的猜测转变为客观的、基于事实的选择，在风险升级之前将其揭示，并在环境变化时指导优先级。政策、流程和控制措施成为有生命的资产——被编码、自动监控，并在短周期内迭代，以跟上新兴技术的步伐，从而确保合规，安全和道德是嵌入到工作流程中的，而不是附加的。

规模化实现这一目标需要领导者之间的强有力合作，AI成果不会从孤立的创新中产生，当首席信息官（CIO）、首席财务官（CFO）和首席战略官（CSO）作为一个有凝聚力的三驾马车协同运作，平衡愿景、执行和价值实现时，这些成果才会被释放。在这种动态中，首席信息官（CIO）推动技术整合，首席财务官（CFO）确保投资带来可衡量的投资回报率，首席战略官（CSO）使战略与企业优先事项保持一致。[33] 它们共同构建了创新和业务成果之间的连接纽带，表明AI的成功不仅依赖于先进技术，更依赖于共同领导。

**生态系统协调者**

技术组织可能会从服务提供商演变为生态系统协调者，链接初创公司、超大规模企业、监管机构和学术界以加速创新。随着数字能力在企业中广泛培训与应用，具备技术能力的岗位在企业成为新常态，IT和业务之间的界限会逐渐消融。在未来几年，企业可能会在灵活的创新网络中运作，进行一系列试验性项目，并不断强化行之有效的做法。成功将不再取决于拥有所有的技术，而更多地取决于构建一个适应性强的生态系统——该系统持续验证并拥抱“快速失败，快速学习”文化。

**持续演进：持续设计与创新**

未来科技组织的标志性特征是持续演进，在此过程中，变革成为一项核心能力，而不是一次性工作。将适应性和持续测试与创新心态嵌入到结构、文化和战略中，将打造出能够与所驾驭技术同步学习的组织。

Kim说：“你一直以来做事的方式，并不一定成为你明天继续做事的方式。”“利用你现在可以从AI中获得的能力，因为即使性能水平停滞不前，AI如今能为你的组织和团队带来的帮助依然令人惊叹。没有时间等待，立即行动。”

## 从作家到导演：Steve Yegge谈软件开发者的转型

Steve Yegge是一名拥有30多年行业经验的软件工程师，是《Vibe Coding》一书的合著者（与Gene Kim合著；见前面的侧栏“Vibe转变：Gene Kim谈企业IT中的AI驱动编码”）。Yegge用十几种语言编写了超过一百万行生产代码，并领导过多个多达150人员的团队。他目前是Sourcegraph的一名工程师，从事AI编码助理的工作。

**Q： AI 编码如何影响技术职能?**

**A：** IT是一项分层活动。我们正在失去底层代码生成环节。任务或角色不断地被推到硬件或软件中，而人类负责的工作涉及设计、整合工作流和领导团队。因为AI正在编写代码，每个人都在向这个方向发展。
这也意味着非程序员正进入IT职能领域。产品经理、用户体验设计师等角色开始参与编码工作，因为我们正在使用AI来生成这些共享工件。如今在业务和IT之间有一个我们以前从未有过的转译层。我们看到小团队，可能是工程师、财务分析师和营销人员正在打造以往从未有过的软件。

**Q： 这将如何改变软件工程师的角色?**

**A：** 你不能把一切都交给AI，最终，人类需要审核。这就像传统的的技术项目经理，过去管理工程师团队，但现在你正在管理的是AI智能体。但智能体不能解决所有问题，它们的工作速度远超人类，但我们的抱负会变得更大。过去我们想做的所有项目，现在都可以实现了，但这需要持续的调整、看护和引导AI。

随着AI（工具）变得越来越智能，未来几年将有更多的非程序员能够做到这一点（监督）。但现在这一切都与程序员及其可塑性能力有关，以适应这种全新的工作方式，他们本质上是在指导AI。

**Q： 在这种环境下，你如何衡量开发人员的生产力?**

**A：** 自2022年AI驱动的代码完成出现以来公司一直在努力解决这个问题。通过代码补全，AI会自动完成你正在编写的代码行，你可以接受或忽略它，这时生产率指标是接受率。

当基于聊天的编码工具出现时，这种生产力指标几乎在一夜之间消失了，因为现在你所做的就是在聊天中发出请求，AI编写代码然后你复制粘贴。很难找到好的指标，因为这些改进比简单的接受率更具多样性和上下文依赖性。

现在我们有了编码智能体，AI可以使用工具来运行代码本身，查看结果，并迭代，而无需手动复制粘贴和来回传递信息。根据你选择的任何衡量标准：代码行数、提交、实际业务成果，使用编码智能体的人的生产力是不使用的人员的10倍。这显然比没有使用编码智能体的人大一个数量级，以至于公司甚至没有尝试衡量它。然后，当你试图比较比同龄人效率高10倍的人时，讨论就变成了在绩效评估时该怎么做。

**Q： 在AI时代，你对招聘开发人员有什么看法?**

**A：** 对于新进入该领域的人来说，这是一个艰难的时期，但我的观点是，人们过于谨慎、招聘不足。他们阻碍了一群才华横溢的初级程序员构建下一代产品，使公司成为同类产品中的佼佼者。
具备适应性强和思维可塑性强的人员一直都是需要的，但现在他们比以往任何时候都更重要。雇佣那些没有太多包袱的人，而不是那些说 “我不会做X，我不会做Y”的人。投资他们，培训他们，让他们有犯错的灵活性，并作为一个组织从中吸取教训，这样做的公司将会非常成功。[34]

# 尾注


1. Kelly Raskovich等人，“IT，放大：AI提升了技术功能的覆盖范围（和职权范围），”Deloitte Insights，2024年12月11日。
2. 德勤2025架构展望调查。从2025年6月到7月，德勤对250名美国各行各业的技术领导者进行了一项在线调查，以了解当今的技术架构状况以及不同的方法如何推动商业价值。所有受访者都是他们内部的领导者。该组织的IT职能部门（董事级及以上）来自年收入10亿美元或以上的商业公司。
3. Tracey Franklin（莫德纳首席人才和数字技术官），2025年9月26日对德勤的采访。
4. 德勤技术支出展望。从2025年6月到7月，德勤对302名IT采购负责人、IT主管和负责技术支出监督的非IT高管进行了一项在线调查，以了解关键行业的美国企业如何管理技术预算、做出支出决策、衡量技术投资带来的价值，以及根据市场动态规划情景。所有受访者都来自年收入10亿美元或以上的组织；66%的受访组织为公有制，34%为私有制。
5. 德勤美国，“新的德勤科技高管调查突显了科技高管重塑的时刻，因为对AI技能和跨职能协作的需求变得至关重 要，”2025年6月17日。从2025年3月到4月，德勤对美国各行各业的622名技术领导者进行了一项在线调查，以了解高级技术领导角色和职责的演变情况，以及2025年及以后的主要挑战和优先事项。受访者的头衔包括首席信息官（33%）、首席技术官（18%）、首席数据分析官（25%）和首席信息安全官或同等职位（24%）。
6. 德勤技术支出展望。
7. 德勤2025技术高管调查。
8. Isabelle Bousquette，“为什么莫德纳合并了技术和人力资源部门”，《华尔街日报》，2025年5月12日；Lee Chong-Ming，“OpenAI的一位高管表示，该公司正在利用新的工程角色来让大客户的项目快速进行，”Business Insider，2025年7月23日。
9. 德勤2025架构展望调查。
10. 本杰明·芬齐、布雷特·温伯格和伊丽莎白·莫拉切克，“2025年春季财富/德勤首席执行官调查”，德勤，2025年5月15日。
11. 德勤美国，“新的德勤调查显示，科技高管推动增长，制定战略，并关注首席执行官席位；”德勤技术支出展望。
12. 德勤2025技术高管调查。
13. 德勤首席信息官项目，“许多技术领导者在德勤最新研究表明，高管层正在壮大，”德勤见解，2024年9月26日。
14. 德勤技术支出展望。
15. 2025年德勤企业新兴技术趋势调查。
16. Katherine Noyes，“博通首席信息官：‘现代化应该由业务驱动’”，《华尔街日报》，2025年9月10日。
17. 2025年德勤企业新兴技术趋势调查。
18. Michael Caplan等人，“未来的技术运营模式：代理企业的崛起”，《华尔街日报》，2025年8月23日。
19. Katherine Noyes，“西部数据首席信息官：在AI时代，‘要么进攻，要么落后’”，《华尔街日报》，2025年9月6日。
20. Katherine Noyes，“可口可乐首席信息官关于扩大AI：从'我们能做什么'到'我们应该做什么'”，《华尔街日报》， 2025年1月18日。
21. 2025年德勤企业新兴技术趋势调查。
22. Gene Kim（凤凰计划和新出版的书《Vibe Coding》的研究员和合著者），2025年9月15日对德勤的采访。
23. Kyle Forrest、Brad Kreit、Abha Kulkarni、Roxana Corduneanu和Sue Cantrell，“AI、人口结构变化和敏捷性：为下一次劳动力发展做准备”，Deloitte Insights，2025年8月25日。
24. Katherine Noyes，“RTXAICDO：‘价值总是胜过数量’”，《华尔街日报》，2025年9月13日。
25. Katherine Noyes，“UiPath首席执行官：代理自动化将‘迎来一个新的工作时代’”，《华尔街日报》，2025年2月22日。
26. 德勤2025技术高管调查。
27. 同前
28. 不/是，“西部数据首席信息官：在AI时代，‘主动出击，否则落后。’”
29. 德勤技术支出展望。
30. 同前
31. Gergely Orosz，“什么是前沿部署的工程师，为什么他们如此受欢迎？”《务实工程师》，2025年8月12日。
32. 2025年德勤企业新兴技术趋势调查。
33. Lou DiLorenzo等人，“AI的投资回报率三巨头：首席信息官、首席财务官和首席战略官”，《华尔街日报》， 2025年5月10日。
34. Steve Yegge（Vibe Coding的合著者和Sourcegraph的软件工程师），2025年10月1日对德勤的采访。

# 作者简介

**Lou DiLorenzo Jr.**
ldilorenzojr@deloitte.com

Lou DiLorenzo Jr.领导Monitor Deloitte的美国技术、AI和数据战略实践。DiLorenzo在各个领域拥有超过25年的经验擅长将关键利益相关者聚集在一起，推动变革，开发新能力，并为大公司和初创公司实现积极的财务业绩。DiLorenzo是科技界的一位杰出人物，经常被《福布斯》、《财富》和《华尔街日报等领先出版物引用。

**Michael Caplan**
mcaplan@deloitte.com

Michael Caplan是德勤咨询公司战略实践的负责人，也是德勤技术运营模型设计和实现能力的领导者。Caplan拥有20多年的经验在复杂的技术和商业模式转型方面为公司提供咨询，重点是将技术与更广泛的企业相结合，以制定面向未来的技术战略、运营模式和工作方式，从而提升价值并推动组织增长。

**Anj al i Shai kh**
anjalishaikh@deloitte.com

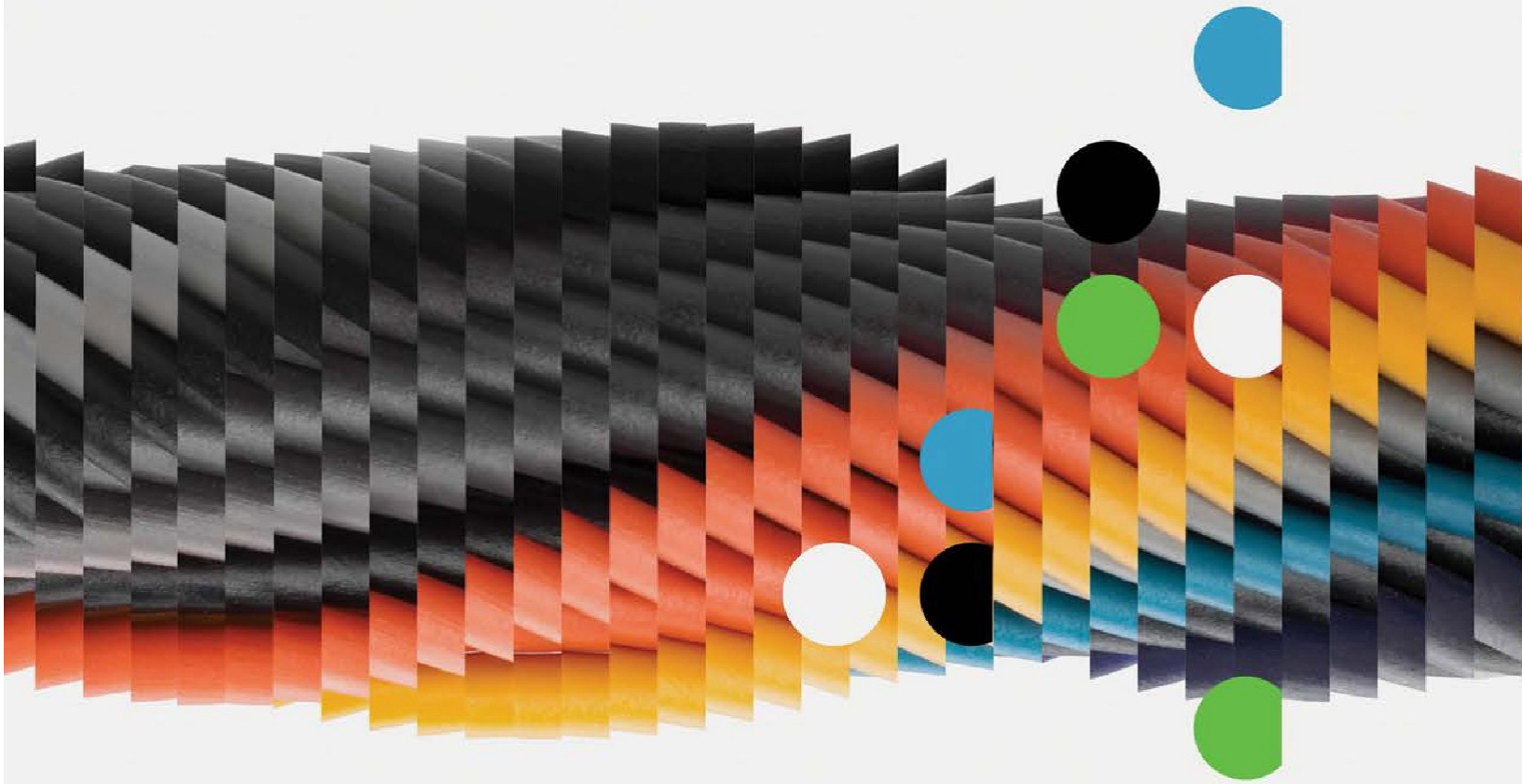
Anjali Shaikh领导德勤的技术高管项目，担任首席信息官、首席数据官和技术领导者的顾问，并为项目开发提供战略指导。Shaikh领导着一个由熟练从业者组成的团队，负责创建定制体验，并开发有价值的见解，帮助高管应对复杂的挑战；制定技术议程；建立和领导有效的团队；并在职业生涯中脱颖而出。

**Erika Maguire**
ermaguire@deloitte.com

Erika Maguire是一名研究员和编辑，专注于揭示科技领域的新事物和下一步发展。作为德勤首席信息官计划的一部分，她领导了关键的思想领导力倡议，包括德勤的全球技术领导力研究，并为客户提供可操作的见解，以建立更好的团队和更好的业务。她之前在福布斯工作了九年，为当今最大的品牌创建数据驱动的内容。

# 致谢

非常感谢德勤的许多主题负责人，他们为本章的研究做出了贡献：Ryan Casden、Nate Paynter、Tarun Sharma、Tim Smith和Michael Wilson。



# 走出困境：使用AI进行网络防御

## 组织如何应对网络安全悖论——在应对面临AI带来的威胁之前，认知并利用其强大的防御能力？

*Sunny Aziz、Adnan Amjad、Naresh Persaud、Mark Nicholson和Ed Burns*

大规模部署AI的组织正在发现其悖论：帮助他们更具竞争力的AI能力同时也可能带来新的安全风险。然而同时，他们也认识到AI提供了强大的新能力来应对它所造成的漏洞。

企业面临着与AI相关的多种威胁，包括影子AI部署、AI驱动的攻击加速和AI系统的内生风险。[1] 然而，即使AI驱动了新的威胁因素传统的网络安全原则仍然有效，并启用具备机器速度的自主学习、适应和运行的智能系统。其中许多技术都需要进行重大调整，因为大多数网络安全架构的设计都不依赖于数字智能。

响应式网络安全应对方法的窗口正在关闭。去年，许多组织专注于调动并探索AI的可能性。现在，随着他们意识到AI未经检查便被采用的风险，他们正在对新出现的威胁进行分类，并实施有针对性的治理框架，以帮助平衡创新速度和安全性。

## 内在的敌人

外部威胁依然存在。正如我们在《技术趋势2024》，中讨论的，深度伪造，虚拟身份以及AI驱动的社交工程持续升级。但当今许多最紧迫的AI相关风险都源于组织内部。其中两个相关风险是影子AI和对AI智能体治理的控制不足。

影子AI是由企业中的各个团队实施的未经批准的AI部署，它造成了治理盲点，并引入了可以访问敏感数据、做出相应选择并与其他系统交互的自主决策系统。[2] 每次部署都可能造成潜在的数据泄露、模型操控、模型漂移或未经授权访问的潜在来源。在过去几年中，企业为应对影子IT部署制定了很多方法，包括监控企业网络以发现所有AI应用设施，并制定策略以确保新的部署符合隐私和安全标准。[3]

在过去的一年里，企业一直专注于将AI有效地整合到业务流程工作流中。现在，随着AI用例场景在企业运营中的扩展，他们发现AI的应用也会产生一系列新的风险，并且这些风险需要相应的缓解策略。

### 从风险识别到风险缓解

AI安全风险体现在四个领域：数据、AI模型、应用和基础设施。随着组织逐步发现威胁的全部范围，被动应对方式的可行窗口正在收窄。采用许多现有的安全实践都可以应对这些特定于AI的风险。

**数据安全风险：**大语言模型（LLM）和其他AI系统集中使用了大量敏感数据，因此需要额外的保护。数据安全关注包括AI模型部署后在开展训练、测试、验证和推理过程中处理的信息（图1）。

**AI模型安全风险：**模型安全包括模型的架构和 独特的训练参数以及训练、测试和验证过程（图2）。透明度要求通常因模型类型而异，这带来了重要的监管考量。

图表1

## AI相关的数据安全风险及相关缓解策略

| 风险 | 缓解策略 |
| --- | --- |
| **机密性和数据隐私：**:AI工具可能会无意中暴露敏感数据。<br>**训练数据投毒：**对手可以篡改训练数据，从而损害输出的准确性和实用性。<br>**模型偏差：**这包括故意操控训练数据以创建后门或系统性偏差。 | **数据安全管理实践：**盘点AI数据源目录，维护高质量的人工生成训练数据，并仔细管理合成数据。<br>**数据完整性监控：**持续监控数据，以确保其不被操控并监测异常。<br>**强大的访问控制：**只向授权人员提供访问训练数据或相关服务的权限，实施最小授权原则。 |

图表2

## A模型安全风险及相关缓解策略

| 风险 | 缓解策略 |
| --- | --- |
| **模型崩溃：**在合成数据上训练的AI模型会随着时间的推移逐渐退化。<br>**模型窃取：**未经授权访问专有模型使对手能够识别漏洞并复制能力。<br>**模型反演：**模型输出可用于重建和暴露敏感的训练数据。<br>过度滥用智能体：生成型AI应用程序获得并使用过多的权限来执行例外的操作。 | **模型隔离：**在培训和部署过程中实现数据和环境分隔。<br>特权访问管理：通过全面的身份和访问管理来控制和监控对训练模型的访问。 |

**应用安全风险：**这类风险涉及托管模型的外层与AI基础能力，具体表现为用户或系统通过用户界面与AI功能交互时可能产生的安全隐患（图3）。

**基础设施安全风险：**基础设施安全涵盖AI系统开发与托管所依赖的硬件及网络组件，是支撑AI功能稳定运行的基础层级（图4）。

图表3

## AI应用安全风险及相关缓解策略

| 风险 | 缓解策略 |
| --- | --- |
| **伦理使用问题：**模型镜像了人类行为，使AI决策容易受到不准确或偏见的影响。<br>**输入注入：**恶意输入会覆盖控制或改变模型行为。<br>未经授权访问：未经授权的用户访问AI应用程序或数据。 | **网络和用户访问管理：**大语言模型需要只有授权用户才能访问的安全飞地。<br>**全面的访问控制：**控制和监控对训练数据、训练模型或支持服务的访问。<br>**第三方服务提供商评估：**识别潜在的合作伙伴风险，并通过供应商生态系统扩展安全要求。 |

图表4

## AI相关基础设施安全风险及相关缓解策略

| 风险 | 缓解策略 |
| --- | --- |
| **不安全的接口和API：**可以利用漏洞攻击模型或获取有关系统和数据的信息。<br>**模型拒绝服务：**精心设计的输入会触发资源密集型操作，使系统不可用或增加成本。<br>**供应链漏洞：**使用第三方数据集、预训练模型和框架可能会引入在整个AI系统中传播的风险。<br>**部署配置错误：**托管环境中的配置错误可能导致未经授权的访问、数据泄露或系统受损。<br>**横向移动攻击：**横向攻击利用相邻服务或受控帐户来访问AI系统。 | **利用虚拟网络强化AI部署：**利用安全沙箱在测试期间将AI工作负载与生产环境隔离开来。<br>**外围和工作负载加固：**通过防火墙、网络隔离和流量检查等严格控制来降低违规风险。<br>**保护机器学习运行集成环境：**将安全性集成到机器学习运行中。 |

## AI的安全性：Sanmi Koyejo谈AI系统的基本安全挑战

Sanmi Koyejo是斯坦福大学的助理教授， 也是 Virtue AI的联合创始人，该公司为AI安全开发企业解决方案。他对AI评估、对抗鲁棒性和安全评估的研究已在大型科技公司的生产系统中实施。

**Q： 与传统计算系统相比，为什么AI系统难以保护?**

**A：** AI系统的行为、用例和范围与我们过去看到的许多计算基础设施截然不同。

最大的区别在于，与经典计算系统相比，AI的灵活性和情境性要高得多。这意味着，许多为传统安全开发和完善的工具集在应用于AI系统时效果不佳，在应用于智能体等新兴框架时效果更差。

此外，在经典计算系统中，数据和计算是孤立的，因此您可以使用传统的网络安全技术将攻击数据的内容与攻击基础设施的内容分开。但在AI系统中，数据和计算是结合在一起的，因此攻击一个通常意味着攻击所有。新兴的AI用例和威胁面的复杂性要求重新思考保护计算系统意味着什么。

当前，AI系统已经能够与标准数据集高度融合，但这也带来了新的安全挑战。例如，在流量和内容层面，大量“看似人类生成的信息”正使许多传统检测策略失效。为了应对这一问题，我们需要构建更适应AI特性的、动态的安全防护体系。

从语言到视觉、音频和其他多模态系统，有很多令人兴奋的地方。相较于文本，人们对音视频的互动要频繁得多，因此也更容易相信这些内容。由于模态集的扩大以及不同模式交互能力的增强，利益相关者及计算系统基础设施所面临的风险也随之增长。

**Q： 在AI的安全方面，有哪些新兴的方法?**

**A：** 在生态系统方面，一些非常有趣的事情正在发生。我们看到了两大类公司。他们正在采取高度互补但不同的方法。

首先，有一些经典的网络安全公司在AI安全加固领域（security-for-ai）和安全赋能AI领域（AI-for-security）都加入了AI。他们一直在投资AI来帮助解决传统的安全问题，但最有趣的是，他们正在为AI功能增加安全性，如数据清洗、安全护栏和AI防火墙，以防止提示注入和其他智能体部署问题。

在探讨AI安全问题时，一个惊奇的对比体现在两种不同的思维路径上：一种路径是从安全专业本身出发，思考如何为AI系统搭建外部“脚手架”来应对威胁。另一种路径则始于对原生AI基础设施的深入理解——当您已经亲手构建了这些系统，洞悉其内在机制与潜在漏洞，并基于这些知识来设计安全基础设施时，方法看起来便全然不同。前者是在既有的安全范式上延伸，后者则是从AI系统的本质中生长出安全逻辑。这种视角的差异，深刻影响着防护策略的设计与实施。

认为AI原生方法可能对AI应用程序的安全性更有效。原生AI公司有一个特殊的优势因为他们比传统的安全公司更了解系统，也更有针对性。

**Q: 展望未来两到四年，我们还会面临哪些其他类型的攻击，或可预见的攻击维度，还是说因为形势发展太快，根本无法预测?**

**A：** 根据我的经验和广泛的参考框架，风险和能力往往是密切相关的。系统能做的越多，我们给予它的访问和接口就越多，我们需要覆盖的新型安全范围就越大。所以，若你想看看风险在哪里，就看看功能在哪里——人们试图用它做什么，人们对什么用例感到兴奋，以及未来的投资在哪里。

有了AI，对这项技术的兴奋使我们忽视了安全问题，专注在能力上，然后意识到我们留下了一个空白。我们应该重新审视，找出可能出现的安全风险，并将安全视为模型能力。[4]

### 引入创新思维

保护AI设施所需的大多数做法并不新鲜；他们只是在升级更新后以应对AI风险。AT&T高级副总裁兼首席信息安全官Rich Baich表示，他降低AI风险的方法严重依赖现有的网络安全领先实践。特别是，他专注于实施强有力的软件开发生命周期方法。无论工具是自制的还是供应商支持的，都应该经过测试和红队攻击检测，以满足安全架构和访问控制的要求。

Baich表示，这种方法使他的团队能够引入创新和推进运营所需的AI工具，同时确保不会产生新的问题。

“我们今天所经历的与过去没有太大不同，”Baich说。

“与AI的唯一区别是速度和影响力。”[5]

不断加速的攻击时间轴、影子AI以及管理自主智能体的复杂性，使得从数据分类到智能体监控的基础安全工作变得尤为迫切。

然而，正如我们将在后续章节中阐述的那样，AI在网络、风险与合规团队中也正发挥着更重要的作用，助力他们更有效地应对这些新出现的挑战。

## AI军备竞赛升级

AI引入了新的风险，但它也提供了强大的防御能力。领先的组织正在探索AI如何帮助他们以机器速度运行，并实时适应不断变化的威胁。基于AI的网络安全解决方案有助于识别人为遗漏的模式，监控整个环境，加快威胁响应，预测攻击者的行动，并自动化重复任务，这些能力正在改变组织进行网络风险管理的方式。

### 先进的AI原生防御策略

网络安全团队利用AI的其中一个领域是红队攻击检测(red teaming)。这涉及严格的持续测试，并通过模拟对抗性攻击来挑战AI系统，以在对手利用它们之前识别漏洞和弱点，这种主动的方法有助于组织了解其AI系统的失误模式和安全边界。

巴西金融服务公司Itau Unibanco已为其红队演习招募了智能体。它采用了一种老练的方法，在整个公司部署了人类专家和AI测试智能体。这些“红队智能体”使用迭代过程来识别和消减道德、偏见和不当内容等风险。

Itau Unibanco，新兴技术主管Roberto Frossard表示 “ 作为一个受监管的行业，信任是我们最关心的问题。” “所以这是我们花了很多时间做的事情之一即测试、重新测试，并试图模拟攻破模型的不同方式。”

AI在对抗训练中也发挥着作用。该技术通过在对抗性示例上训练模型——即专门设计用于欺骗或攻击模型的输入——帮助系统识别和抵抗恶意操纵，从而显著提升其对攻击的鲁棒性。[6]

### 治理、风险和合规性演变

使用AI的企业面临着新的合规要求，特别是在医疗健康和金融服务领域，他们经常需要解释决策过程。[7] 虽然这个过程通常很难解读，但某些策略可以帮助确保AI的部署是合规的。

一些组织正在重新评估谁来监督AI的部署。虽然传统上由董事会管理这一领域，但越来越多的趋势是将责任分配给审计委员会，该委员会有能力不断审查和评估与AI相关的活动。[8]

管理跨境AI实施仍然很重要。这种情况可能需要关注数据主权，以确保数据按照适当的规则在本地处理。

### 高级智能体治理

智能体在设计上具有高度的自主性。随着智能体在整个组织中的激增，企业将需要复杂的智能体监控来实时分析其决策模式以及智能体之间的通信，并自动检测除基本活动记录之外的异常智能体行为。这种监控使安全团队能够在受到攻击或行为不端的智能体造成重大损害之前识别出他们。

动态权限管理是智能体治理的另一个方面。这种方法允许团队按用户管理数百甚至数千个智能体，以保持安全边界。特权管理策略应平衡智能体自主性与安全要求，根据上下文和行为调整授权。

治理政策应纳入生命周期管理，控制智能体的创建、修改、停用和继任计划——类似于对人类员工的人力资源管理，但适用于数字员工这将有助于限制那些孤立智能体的问题，防止机器人即使在被关闭后仍可以持有对关键系统的访问权限。

随着AI智能体被授权自行开发智能体，治理对企业来说将变得更加紧迫。这种能力引发了关于管理隐私和安全的重大问题，因为智能体可能成为攻击者的主要目标，特别是如果企业缺乏对这些智能体正在做什么以及他们可以访问哪些系统的可见性。

### 力量倍增效应

许多网络组织正在使用AI作为克服复杂威胁的力量倍增器。AI模型可以作为增强的防御机制叠加在当前的安全工作之上。

AI可以帮助进行风险评分和优先级排序、第三方风险管理、自动化政策审查和编排、网络安全成熟度评估以及监管合规支持。当部署在这些领域时，AI功能使安全团队能够就资源分配做出更快、更明智的决策。

AI还在控制测试和自动化、安全代码生成、漏洞扫描能力、系统设计优化和模型代码审查过程中发挥作用。这加速了安全漏洞的识别和修复。

### 对AI蓝图的需求

网络安全团队的运营不是为AI而设计的，但在整个组织中推进实施AI商业变现将为重构安全运营创造了机会。随着企业在其运营中推出AI（特别是智能体），许多企业选择彻底重塑劳动力、运营模式、治理模式和技术架构。在重构运营以利用AI智能体的同时，组织应该将安全考虑纳入基础设计，而不是将其列入后期设计。这种预防新兴网络风险的积极方法可以使企业为当今的威胁做好准备，并使其能够很好地应对未来两到五年可能发生的危险，这将是下一节的主题。

## AI网络风险将继续发展，但解决方案也将继续发展

展望未来，新兴趋势可能会挑战有关网络安全、物理安全甚至地缘政治稳定的基本假设。虽然有些场景仍然是推测性的，但了解潜在的未来使组织可以准备能够随着威胁的发展而适应的架构和治理框架。

### 当一切都是武器：AI-物理现实融合

随着AI在诸多领域日益普及，并与电网、水处理设施、交通网络、供应链、医疗系统等物理基础设施深度融合，由此带来的物理风险也呈指数级增长。AI与物理系统的结合，正创造出可能引发前所未有破坏性攻击的潜在入口。

未来可能出现的威胁，将不再局限于单一系统，而是能通过一次攻击同时瘫痪交通、医疗、公用事业等多个部门的AI系统。一旦攻击者获得这些互连互通的智能系统访问权限，就有可能策划一场波及多个关键基础设施的连锁故障，造成系统性崩溃。

复杂的攻击可能会采用“煮青蛙”策略，AI系统 会在几个月内微妙地降低系统性能，使监测变得困难，直到累积成重大损害。

组织可以通过多种方法为AI物理融合风险做好准备。

- **自动化集成漏洞检测：**
  组织应部署监控工具持续检查集成风险，实施入侵指标预警系统。
- **物理系统弹性：**组织应为关键物理系统建立备用的手动控制系统，确保人类操作员在必要时可以覆盖自动决策。
- **级联预防架构：**面对问题，组织应建立已连接系统的传播屏障并及时熔断，实现故障边界的隔离。

### 自主网络战

向自主网络战的演变——即AI驱动的全自动攻击与防御系统在无人类干预的情况下，以机器速度运行的AI作战形式——代表了网络安全的范式转变。

未来的攻击能力可能包括：

- **群体攻击协作：**AI系统可以通过协调来压倒防御系统-实时适应防御反应的行动。
- **适应性持续威胁：**攻击可以根据防御措施进行演变，从每种措施中学习防御行动，以识别弱点并不断调整战术。
- **地缘政治维度：**AI在网络战中的武器化带来了新的地缘政治风险，包括通过篡改或完全捏造的媒体操纵公众舆论，如在《技术趋势2024》中描述的。
- **经济战风险：**股市越来越依赖AI进行交易、风险评估和市场分析。一些专家认为，下一次金融危机可能是由AI而不是传统经济因素驱动的。[9]

### 新兴前沿：太空和量子安全

随着AI安全的发展，尽管这两个新兴领域刚刚发展起来，但它们仍然需要得到紧急关注：太空基础设施和量子计算。

**太空基础设施脆弱性：**商业航天工业开辟了新的攻击面；每颗卫星本质上都是一台容易被利用的计算机。随着对手发展渗透卫星的能力，破坏的可能性延伸到GPS、通信、天气监测和国家安全系统。

**量子通信信道：**量子通信承诺理论上不可破解的加密，而且有可能使当前的加密方法过时。如《技术趋势2025》所述，组织应该为这一转变做好准备，同时保护量子通信基础设施免受寻求妥协入侵或控制这些能力的对手的攻击。

## 平衡创新的必要性

组织应该通过从一开始就将安全嵌入AI计划的战略框架，同时追求创新和安全。

企业可以从实施基本的安全控制开始：数据安全、访问管理、模型保护和基础设施强化。为了追求快速的AI部署而忽略这些基本原则可能会产生漏洞，最终可能会危害他们的竞争地位。

由此，企业可能会考虑投资于先进的AI以加持防御能力。对抗AI威胁需要AI驱动的安全体系，以机器速度运行，识别微妙的攻击模式，并适应不断发展的对手战术。将AI安全视为力量倍增器而非成本中心的组织有希望建立持久的防御优势。

最后，为新出现的威胁准备安全架构和治理框架将在未来几年变得更加重要。虽然自主网络战和AI物理融合似乎很遥远，但随着威胁格局的演变，今天构建适应性强的安全架构有助于明天的弹性扩展。

AI困境最终根本不是困境，这是一个行动的号召。从战略上接近AI安全、在快速创新的同时实施多个防御层的组织可以更好地保护其资产，并可能通过领先的风险管理能力建立竞争差异化。未来属于掌握这种平衡的企业，将安全视为AI采用的推动者，而不是限制因素。

# 尾注


1. Gartner，“Gartner调查显示，AI攻击正在上升”，新闻稿，2025年9月22日。
2. CybSafe，“研究：近40%的员工在雇主不知情的情况下与AI工具共享敏感信息”，新闻稿，2024年9月26日。
3. Dana Raveh，“什么是影子IT？”CrowdStrike，2024年7月10日。
4. Sanmi Koyejo（斯坦福大学助理教授），对德勤的采访，2025年9月26日。
5. “一种在at&T确保AI启用的严肃方法，”
6. Deloitte Insights，2025年11月21日。Roberto Frossard（Itau Unibanco新兴技术主管），对德勤的采访，2025年9月17日。
7. Pat Niemann，“网络和AI监管披露：2025年公司共 享的内容”，哈佛法学院公司治理论坛，2025年10月28日。
8. 德勤美国，“AI：审计委员会的新兴监督责任？”，访问日期为2025年11月11日。
9. John Divine，“AI如何引发下一场金融危机”，《美国新闻与世界报道》，2023年6月30日。

# 作者简介

**Sunny Aziz**
saziz@deloitte.com

Sunny Aziz是德勤网络和战略风险服务的负责人，在帮助客户管理、实施和运营复杂的网络项目方面拥有超过25年的经验。他为客户提供网络战略和执行大型网络转型计划方面的建议。Aziz还担任德勤金融服务业保险部门的网络主管，专门从事管理安全服务、网络战略和评估、身份和访问管理等。

**Adnan Amjad**
aamjad@deloitte.com

Adnan Amjad担任德勤美国网络主管，负责监督德勤网络产品的增长和战略，包括网络防御和弹性、网络运营、网络战略和转型数字信任和隐私以及企业安全。在此职位上，Amjad为客户提供建议，通过强大的网络解决方案和托管服务来应对不断变化的威胁形势，这些解决方案和服务旨在简化复杂性，保护和使企业取得成功，建立弹性，并加速转型，帮助他们保护未来的企业。

**Naresh Persaud**
napersaud@deloitte.com

Naresh Persaud是德勤风险与财务咨询公司的负责人，专注于跨行业的网络风险。他在身份和访问管理方面拥有20多年的经验，担任过多个职位。Persaud在身份管理和关系数据库安全方面拥有深厚的领域知识，并在跨部门领导大型安全实施和运营方面拥有丰富的经验。

**Mark Nicholson**
manicholson@deloitte.com

Mark Nicholson是德勤咨询公司的负责人，拥有25年的网络安全 经验。在被德勤收购之前，Nicholson是网络安全公司Vigilant，股份有限公司的联合创始人。他目前是德勤网络的AI领导者。

**Ed Burns**
edburns@deloitte.com

Ed Burns在CTO办公室领导客户故事倡议，该倡议被称为趋势线。该项目是对《技术趋势》和其他知名企业的重要研究投入。在担 任现职之前，他领导了一家科技新闻出版物，涵盖了AI、分析和数据管理的所有内容。

# 致谢

非常感谢德勤的许多主题负责人，他们为本章的研究做出了贡献：
Gi ri Saravanan Chandramohan、Edward Guerrero、Ki eran Norton和Abhi shek Sekhri 。

# 拨开迷雾：AI进阶过程中值得追踪的技术趋势

那些微小的技术趋势——是否预示着颠覆性变革即将到来？从类脑计算到边缘AI，这些领域都值得关注。

*Kelly Raskovich、Bill Briggs和Caroline Brown*

在通信理论中，信号是滤除噪声后信息：是系统传输内容中的真正蕴含意义的内容。在技术领域，信号则是方向变化的早期征兆——犹如地震前的微颤，预示着即将发生的剧烈变动。信号并非预测，而是对已然启动力量的观察，是本报告先前所述复合效应所催生的种种规律与趋势。

它们将在未来18至24个月内重塑各组织：物理AI与机器人技术、AI智能体、AI基础设施、技术组织转型以及AI时代的网络安全。前文探讨了将在未来18至24个月内重塑组织的五项新兴技术趋势：物理AI、数字员工、AI基础设施、AI原生技术组织和AI网络安全。

但新兴技术领域远不止上述五个趋势。决定将哪些趋势应纳入我们的主题报告，既是一门科学，也是一门艺术，更少不了些许直觉。

随之而来的信号——一些与我们的核心趋势直接相关，另一些则以并行方式运行——这些都是技术领导者应密切关注的新兴动向。它们没有以完整的章节入选，并非因为它们重要性不足，而是因为它们尚处于发展之中。所以，这些信号都值得关注。

其中大多数都是当下正在发生的，而非虚幻的未来。有些已开始重塑行业，而另一些则刚刚展现出可衡量的影响。在“新兴”与“主流”之间距离正在日益拉近。

领导者需要明确将注意力和资源投向何处——哪些技术趋势亟需当下投资，哪些需要持续监测，以及哪些依赖关系如果被忽视可能会带来风险。

**基础模型是否已经触及发展瓶颈？**这些基于海量数据训练而成的大型AI系统正面临一个关键问题：它们能否继续呈指数级地提升，抑或其能力将趋于平稳？尽管新模型仍在进步，但一些指标显示，它们并未实现像早期版本那样呈现出显著的性能飞跃。[1] 此外，模型规模越大，能耗和计算成本也越高。新的扩展方式，比如让模型有更多时间处理复杂问题的技术，[2] 或许能帮助我们摆脱“更大的模型=更好的性能”的传统思维。这意味着，当前的模型完全可以通过优化提示词设计与实施策略来实现性能提升。企业如何部署、微调和将AI整合到重新设计的流程中，其重要性很可能将超过单纯拥有最新一代的基础模型。

**新数据>合成数据>旧数据。**随着基础模型在类似的公开数据集上进行训练，数据本身已不再构成竞争优势。随着世界不断变化，旧数据的价值也在逐渐降低。合成数据——即由AI生成并用于训练其他AI的内容——有助于填补数据空白，据预测，到2028年，AI工具所用数据中将有80%为合成数据，而这一比例在2024年仅为20%。[3] 然而，合成数据的性能存在上限，通常只能达到真实数据质量的90%至95%。[4] 更糟糕的是，如果AI主要基于AI生成的内容进行训练，可能会导致模型崩溃——这是一种退化过程：模型会逐渐丧失对罕见模式的识别能力，混淆概念，并最终产生平淡乏味、重复单调的输出。[5] 因此，那些能够获取最新信息（包括实时用户交互、专有业务数据以及前沿研究发现）的企业将占据优势。换句话说，掌控交互层（搜索引擎、社交平台、AI助手、智能设备）的公司必将胜出。

**神经形态芯片为计算注入强大动力。**神经形态芯片是受大脑启发的处理器，在某些AI任务中，其能效高于传统的图形处理单元（GPU）。GPU有独立的存储和处理区域，而神经形态芯片将两者结合在同一个地方。神经形态芯片采用事件驱动模式——只在事件发生时处理信息——而GPU则是始终全速运行。这意味着，对于涉及偶发信号的AI任务（例如分析传感器数据或处理自动驾驶汽车中的信息），神经形态芯片的能效比可达到传统芯片的80到100倍。尽管 GPU在连续、高通量计算方面仍然具有优势。[6] 但随着AI从数据中心走向数十亿个边缘设备（见下一条信号），其能效优势变得至关重要。[7] 预计到2030年，神经形态计算将得到广泛应用。

**边缘AI和设备端处理的兴起。**与以往将数据发送至遥远的云端服务器不同，边缘AI直接在设备上运行——无论是你的手机、智能手表、安防摄像头、还是工业机器人。这一趋势之所以重要，是因为：延迟问题（自动驾驶汽车无法等待服务器响应）、隐私保护（数据始终留在本地设备上）、成本激增（云端账单每月高达数千万美元），以及对互联网的依赖。 边缘AI的潜力已体现在具备生成式AI功能的智能手机市场上：2024年，这类智能手机的销量同比增长近364%，达到每年2.342亿部，并有望在2028年攀升至9.12亿部。[8] 在现实生活中，边缘AI的应用包括：智能摄像头在本地实时进行识别、工业传感器预测设备故障，以及健康可穿戴设备在不传输医疗数据的情况下监测生命体征。这是一场正在悄然发生的根本性变革。

**AI原生的个人设备与可穿戴设备会成为主流吗？**企业正纷纷试水智能手机之外的AI原生可穿戴设备，诸如能记录并转录对话的吊坠、具备实时翻译功能的智能眼镜，以及支持语音交互且无需屏幕的袖珍式设备。据预测，全球可穿戴技术市场到2026年将达2654亿美元，科技巨头们正在大力投资下一代形态的可穿戴设备。[9] 然而，市场的实际接受度仍充满不确定性，市场上充斥着不少失败的智能眼镜、别针及其他可穿戴或袖珍形态的设备。[10] 消费者究竟是否真的需要独立的AI设备，抑或更倾向于将AI直接集成到他们已有的手机和耳机中，这一问题依然悬而未决。如果真有某种形态最终胜出（即便这种形态真的出现的话），其成功与否仍将取决于能否妥善解决隐私顾虑，并提供足以证明额外携带一款设备的合理优势。

**生物识别认证是下一级网络安全技术。**由于AI可以复制声音、伪造文件和模仿行为模式，所以生物识别认证是验证物理存在和身份的关键手段。随着深度伪造和AI欺诈变得越来越复杂，各组织正在迅速采用生物识别系统：在一项针对首席信息安全官的研究中，92%的受访者表示他们已经实施、正在实施或计划实施无密码身份验证。[11] 然而，生物识别技术并不是唯一的解决方案。一旦生物特征数据被泄露，便无法像密码一样轻松更换，并且隐私问题依然不容忽视。未来的发展方向将是混合型方案，即生物识别技术将成为主要但并非唯一的验证方法。

**AI助理的隐私权衡。**真正具备强大功能的个人AI助理需要前所未有的个人数据访问权限，而这种访问权限如今已经被默认授予。为了高效的预订餐厅、管理日程或过滤电子邮件，个人AI代理必须掌握用户多年的消息记录、日历条目、浏览数据、存储的密码、信用卡信息、以及私密的个人偏好。[12] 然而，这一权衡极为严峻：一旦个人数据被纳入AI模型，用户便几乎无法再行使删除的权利。[13] 当然，安全问题令人深感忧虑。公众对此的反应已然出现分歧：一些人热切地同意授权以获取更多功能，而另一些人则坚决抵制。但这个悖论始终存在：用户不得不授予广泛的权限，才能让AI助手真正发挥作用，然而大多数人并不完全理解自己所同意分享内容的具体范围及其持续性。

**GEO超越SEO**。用户正越来越多地转向AI聊天机器人，而非传统的搜索引擎。一场争夺AI生成答案排名的竞赛已然打响——这标志着从搜索引擎优化（SEO）向生成式引擎优化（GEO）的转变。目前，AI生成的答案已主导各大搜索引擎的搜索结果，使用户点击传统网站的几率降低了三分之一以上。[14] 人如今，AI平台已驱动了6.5%的自然流量，预计一年内这一比例将攀升至14.5%。[15] GEO与SEOG有着根本性差异：它更注重语义丰富性而非关键词，更看重作者的专业知识而非反向链接，更青睐在AI回答中被引用而非页面浏览量。[16] 正如付费搜索定义了2000年代、社交媒体广告主导了2010年代，AI生成的回答正日益成为2020年代最关键的营销渠道。

其中一些信号可能会逐渐演变为主导力量，而另一些则可能逐渐消退。但所有这些信号都反映着同一个潜在的现实：技术变革的步伐已发生根本性转变。然而，适应的速度比预测的准确性更为重要。那些真正蓬勃发展的组织，并非那些能够准确预测哪些信号会成为趋势的组织；而是那些具备能力，能够敏锐感知、审慎评估并迅速应对新生事物的组织。那些一味等待清晰信号的组织，最终将发现自己不得不去适应竞争对手早已掌握并加以应用的尴尬现实。

# 尾注


1. Casey Newton，“AI公司遇到了一堵扩展墙”， Platformer，2024年11月14日。
2. Anthropic联合创始人Matthias Bastian在2024年12月25日的《解码器》一书中说：“2025年的AI进步将“更加显著”。
3. Grant Gross，“合成数据旨在应对AI培训挑战”，《首席信息官杂志》，2025年2月19日。
4. Emmett Fear，“合成数据生成：为AI模型开发创建高质量的训练数据集”，RunPod股份有限公司，2025年7月31日。
5. IBM，“检查合成数据：前景、风险和现实”，访问日期为2025年11月11日。
6. TokenRing AI，“神经形态计算：重塑下一代AI硬件的大脑革命”，WRAL News，2025年10月7日。
7. 研究与市场，“2025-2030年神经形态计算的增长机会：神经形态技术蓄势待发。到2030年，市场将激增45倍以上，实现超高速增长”，新闻稿，环球通讯社，2025年4月18日。
8. IDC研究，“根据IDC的数据，到2028年，全球生成AI智能智能手机的出货量预计将达到70%的市场份额，2024年的增长率将超过360%”，新闻稿，2024-7-30。
9. 美通社，“AI驱动的可穿戴设备改变了消费者与日常技术的互动方式”，2025年9月15日。
10. Amanda Yeo，“2024年失败的三种产品”，Mashable，2024年11月28日。
11. Janna Bureson，“无密码技术达到了企业安全的临界点”，Portnox，2025年10月20日。
12. Mark McCarthy，“新兴个性化AI服务的隐私挑战”，技术政策出版社，2025年5月28日。
13. Zack Whittaker，“为了隐私和安全，在授予AI访问您的个人数据之前要三思而后行”，TechCrunch，2025年7月19日。
14. Ryan Law和Xibeijia Guan，“AI概述使点击量减少了34.5%”，Ahrefs，2025年4月17日。
15. Jake Stainer，“生成式发动机优化（GEO）：2025年完整指南”，Skale，2025年9月30日。
16. Leigh McKenzie，“生成引擎优化（GEO）：如何在AI搜索中获胜”，Backlinko，2025年10月23日。


# 作者简介


**Kelly Raskovich**
kraskovich@deloitte.com

Kelly Raskovich是德勤CTO办公室 (OCTO) 的高级经理及负责人，并担任德勤旗舰技术趋势报告《技术趋势》的执行主编，该报告专注于新型技术领域。她的职责在于引导客户，塑造德勤技术品牌的未来方向与服务内容，培养专业人才，助力企业实现未来增长。她肩负着技术影响力的提升、深化客户合作以及推动市场营销与公共关系的任务。

**Bill Briggs**
wbriggs@deloitte.com

作为德勤的CTO，Bill Briggs致力于帮助客户预见新兴技术可能对其未来业务带来的影响，并提供从当下实际情况到未来愿景的实施路径。他负责对客户业务产生影响的新兴技术的研究、影响力推广和孵化工作，并为德勤管理咨询技术相关服务与解决方案的未来发展提供指导。Briggs同时担任德勤CIO计划的执行发起人。

**Caroline Brown**
carolbrown@deloitte.com

Caroline Brown是德勤CTO办公室的高级经理。她领导着一个跨职能的编辑和设计制作团队，培养思想领导力。她担任德勤旗舰技术趋势报告《技术趋势》的编辑。作为一名作家和研究员，布朗在北卡罗来纳大学教堂山分校获得了英语和新闻学的本科和研究生学位。

# 致谢

## 特别鸣谢

Ed Burns、Preetha Devan、Makarand Kukade、Erika Maguire、Heidi Morrow和Sarah Mortier成为推动技术趋势的引擎。Ed，你对卓越编辑的持续奉献以及将研究和见解巧妙地融入引人入胜的叙事中的能力，确实提升了我们的工作。Erika，这是第一次做出的巨大努力——我们非常感谢你的研究和写作技巧、商业直觉、幽默感以及应对挑战的能力。Heidi ，你在设计和创意视觉方面的领导力为视觉卓越树立了标准，以吸引和激励的方式将我们的想法变为现实。Makarand，感谢您在第一年加入《技术趋势》，为我们的补充资产和视觉材料带来了新的视角。Sarah，你在管理生产过程中的领导力对我们保持正轨起到了重要作用。你的组织能力、对细节的关注和协作精神带领我们度过了挑战，并使社论不断向前发展。Preetha，我们感谢您今年将您的出版专业知识带到Tech Trends，并帮助我们改进我们的流程和工作流程。我们很幸运，也很感激你们六个人是团队的一员。

**Caroline Brown，**以稳定的指导、战略眼光和坚定不移的支持领导《技术趋势》的编辑和制作。您的领导在应对今年报告的复杂性方面发挥了至关重要的作用，我们感谢您在将技术趋势变为现实方面的合作。

**Catarina Pires**和**Haley Gove Lamb**支持技术趋势并提供卓越的客户体验。您致力于为我们的客户带来技术趋势，并创造有意义的参与，确保报告能够触及最需要它的受众并引起他们的共鸣。感谢您成为我们工作的有效大使。

**Katarina Alaupovic、Alison Cizowski、Deanna Gorecki 、Ben Hebbe、Bri Henley、Abria Perry、Mikaeli Robinson和Madelyn Scott**感谢您在推广技术趋势方面的不懈奉献和创新策略。您在营销、沟通和外联方面的创造力年复一年地显著扩大了我们的影响力。感谢您对广泛传播技术趋势价值的热情和承诺。

**Amanpreet Arora**和**Nidhi John**感谢您通过研究、数据和见解为技术趋势过程带来的新鲜空气。我们感谢您在报告的整个生命周期内，从确定趋势到为我们的工作提供支持的数字，热情而愉快地处理任何问题。

**Raquel Buscaino**和**Mark Osis**是我们的合作者，因为我们发现了趋势和信号，并帮助我们完善了我们的研究工艺。感谢您慷慨地与我们分享您的知识和专业知识。

感谢**Diana Kearns-Manolatos** 和 **Duncan Stewart** 的专业知识和跨团队分享知识的意愿。您的合作丰富了我们的工作，加强了我们研究工作之间的联系。感谢您的慷慨和合作。

**Hannah Bachman、Aditi Rao、Elisabeth Sullivan**和整个**Deloitte Insights团队**，感谢您在我们共同发展技术趋势的过程中继续提供合作和支持。随着我们的合作不断深化，我们的业务不断发展，我们感谢您的灵活性、战略指导和对卓越的承诺。

**Sylvia Chang、Jim Slatton、Manya Kuzemchenko、Melissa O' Brien、Molly Piersol 、Natalie Pffaf 、Harry Wedel 、Jaime Austin、Govindh Raj 、Megha Priya和Naveen Bhusare，**感谢您在开发将技术趋势变为现实的视觉资产方面的创造力和奉献精神。您的艺术眼光和对细节的关注创造了迷人的图像和图形，使我们的报告不仅信息丰富，而且真正引人入胜。我们感谢您对合作和卓越创意的承诺。

# 持续对话

我们的洞察可以帮助您把握新兴趋势的机遇。如果您在寻找应对挑战的灵感，欢迎与我们共叙。

## CTO办公室

德勤美国CTO办公室是一个专注于工程技术未来的团队。我们识别、研究和孵化新兴技术解决方案，以塑造未来市场的需求，培育人才，并赋能企业实现增长。

如果您想联系德勤美国CTO办公室作进一步探讨，请随时通过OCTO@deloitte.com与我们联系。

## 德勤中国

如果您想联系德勤中国作进一步探讨，请参考文末“德勤中国业务联系人”随时与我们联系。