Microsoft 365

从监督到洞察：应对影子 AI 风险

目录

引言

在近期发布的工作趋势指数报告中，对 31 个国家/地的知识型工作者区（包括普通员工及领导层）展开的调查显示，超过 80% 的受访者表示感觉自己缺乏时间或精力来完成工作。此外，超过 50% 的受访企业领导者表示，需要提高工作效率才能实现目标[1]。根据 2024 年 Microsoft 工作趋势指数报告，许多员工正在主动寻找生成式 AI 工具来弥补这一差距，并且在开始使用这些工具时并不会等待 IT 部门的正式批准。

当工具在 IT 部门的监管范围之外运行时，可能会给组织带来安全和合规风险。而“影子 AI”（即未经 IT 批准便使用的 AI 工具）正成为当前工作场所中影子 IT 的最新存在形式。

随着 AI 采用进程的加速推进，企业领导者正努力抢占先机，并降低这些工具可能带来的潜在风险在最近开展的 iSMG 研究中，超过 70% 的受访企业领导者表示，确保数据隐私和安全是将生成式 AI 与现有 IT 基础结构集成过程中面临的主要挑战[2]。此外，超过 90% 的受访 CIO 和 CTO 表示，生成式 AI 已经或将会推动其组织加大网络安全方面的投资[3]。

在本电子书中，你将了解影子 AI 的常见应用场景，明确其给组织带来的潜在风险，掌握应对这些风险的五种方法，并了解 Microsoft 365 E3 如何提供支持。

[1] **2025 年工作趋势指数年度报告，** Microsoft, Inc.，2025 年 4 月。Microsoft 分析了 2025 年 2 月 6 日至 2025 年 3 月 24 日期间，来自 31 个国家/地区的 31,000 名全职受雇或自雇知识工作者的调查数据、领英劳动力市场趋势，以及 Microsoft 365 中的数万亿个高效工作信号。

[2] **“iSMG Second Annual Generative AI Study:Business Rewards vs. Security Risks”，** 基于第三季度对 6 个地区（北美、欧洲、亚洲、南美洲、澳大利亚和非洲）360 多名商业和网络安全专业人士的调查反馈。

[3] **“The AI Security Balancing Act:From Risk to Innovation”，NTT DATA，2025 年 6 月，** 基于 NTT DATA 对 2,300 多名 GenAI 资深决策者的调研数据，其中包括来自 34 个国家/地区的 1,500 名高层领导者。

什么是影子 AI？为何可见性至关重要？

影子 AI 是指员工在未经 IT 部门明确批准或监督的情况下使用人工智能工具和应用程序，而且这类使用行为通常不受官方安全与合规框架的监控。随着员工寻求提升工作效率、应对日益繁重工作需求的方法，他们可能会借助这些未经授权的解决方案，以简化任务流程、开展协作或生成新内容，且往往并未意识到其中潜藏的风险。由于影子 AI 处于 IT 部门的监控范围之外，组织难以掌握员工正在使用哪些应用程序，以及哪些应用程序存在重大风险。

为何影子 AI 的可见性至关重要

当 IT 未知晓某个应用程序或服务时，就无法对其进行安全防护或提供支持。这一*可见性缺口* 导致难以准确识别、管理或降低与敏感数据泄露、监管合规性不足及对专有信息失去控制相关的潜在威胁。IT 部门和业务负责人需要洞察其组织正在使用的影子 AI，应对 AI 应用带来的新兴风险，并确定哪些工具应在适当的管控框架下获准使用。对于组织而言，机遇在于将影子 AI 从风险转变为安全推动工作方式创新的契机。要实现这一目标，就需要达成更好的平衡：让员工能够在受管控、安全的框架内利用实用的 AI 工具，同时降低潜在风险。

见解

*你无法防护看不到的东西。*当 IT 部门不知晓正在使用的应用程序或服务时，就无法对其进行安全防护。这正是将影子 AI 问题的关键所在，也凸显了为何需要采取新的应对方法。如果员工认为这些 AI 工具对实现目标至关重要，那么直接禁止所有外部工具并不现实。相反，组织需要让影子 AI “浮出水面”，了解员工正在使用的工具，实施适当的管控措施，并提供安全、经批准且符合组织需求的替代方案。简而言之，挑战在于在*不*牺牲安全性的前提下，让团队能够借助 AI 提升能力。

工作场所中的影子 AI：示例场景与潜在风险

影子 AI 通常源于员工希望提升工作效率、扩大影响力或尝试新技术的需求。以下为几个虚构案例，用以说明未经许可的 AI 工具可能的使用场景及其潜在风险：

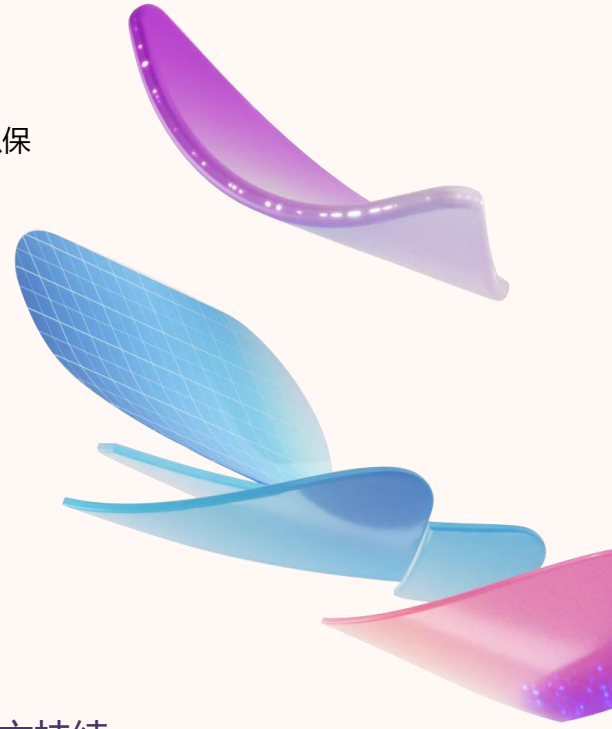
角色	示例场景	未经授权工具带来的潜在风险
市场营销	使用生成式 AI 工具，基于公司品牌数据制作营销文案或设计。	泄露敏感品牌或产品信息；无法控制外部 AI 服务如何存储或使用公司的创意资产。
财务	将公司财务数据上传到 AI 驱动的分析或可视化服务，以快速获得见解。	机密财务数据（如预算、预测）泄露给第三方；如果包含客户或员工数据且未有妥善保护，可能会违反合规要求（例如 GDPR）。
客户支持	将客户数据或支持聊天记录导入 AI 工具，以撰写回复或总结案例。	违反隐私和数据处理规定：敏感客户信息可能存储在公司系统之外；无法保证 AI 提供商会妥善保留或删除数据。
一线零售	门店经理在手机上使用 AI 排班应用，以优化员工轮班安排。	公司员工数据（姓名、排班表）被上传到未经批准的应用，存在隐私泄露问题。如果 AI 给出的排班建议不符合劳动法规，可能会出现排班冲突或违反政策的情况。
一线医疗	护士或医生利用 AI 聊天机器人辅助撰写患者护理记录或解答医疗问题。	患者健康信息(PHI) 可能会在毫无防护措施的情况下泄露给外部服务，导致违反合规与保密要求AI 提供的医疗建议也可能未经核实，存在安全风险。

在上述每种情况下，员工个人均出于良好意愿，期望提升工作效率，但由此可能给组织带来风险。

公司信息最终可能会分散在未经授权的各个平台上，造成*数据治理难题*。未经审查的应用程序可能会引入恶意软件或安全漏洞，将攻击面扩大至 IT 部门监管范围之外。此外，也可能带来合规方面的影响。从 IT 支持的角度来看，如果影子 AI 工具出现问题，服务台可能无法帮助最终用户，因为他们对该工具没有任何了解，也无法进行控制。

应对影子 AI 风险的五大方法

凭借正确的策略和工具，可以将影子 AI 从潜在威胁转变为促进安全创新文化的机会。利用 AI 高效办公工具赋能你的团队，*同时*保持必要的监督，以保护你的业务。这意味着不再一味拒绝，而是有条件地接受，关键在于设定适当的防护措施。以下五项建议可以帮助你管理并掌控组织中的影子 AI：



01 明确影子 AI 的应用范围，评估风险并划分优先级

你无法保护看不到的东西。通过活动日志洞察你组织正在使用的 AI 应用程序。一旦了解了正在使用的应用程序，你就可以甄别处理敏感数据的合适工具，并记录不符合安全性与合规性策略的应用程序。借助这些洞察，你可以更明智地决定允许、监控或限制哪些应用程序，从而降低潜在风险。

02 实施安全与合规政策，快速取得成效

启用或应用策略调整，以更好地缓解使用影子 AI 所带来的潜在风险。你可以利用条件访问策略来管控高风险应用的使用；利用数据丢失防护策略来保护敏感信息，防止过度共享和数据泄露；并对所有用户强制推行基础的多重身份验证和设备合规要求。即使尚未全面掌握正在使用的 AI 应用程序，这些措施也能迅速降低最突出的风险。

03 对员工开展关于影子 AI 潜在风险的培训

员工往往不清楚使用未经授权的 AI 工具可能给组织带来的风险。通过合理的数据丢失防护警示、公司政策提醒和简短培训，频繁传达影子 AI 的风险，引导用户转向更安全的操作方式，而非采取强硬手段强制执行。

04 提供经批准的 AI 工具，以进一步降低风险

在条件允许的情况下，为员工提供经批准的 AI 工具，作为未经授权工具的替代方案。减少影子 AI 的一个有效方法是，使用经认可的解决方案来满足组织内的常见使用场景需求。这样一来，IT 部门既能保持可见性和控制权，又能在出现问题时为用户提供支持。

05 建立持续治理机制

将检查工作融入日常 IT 治理中，定期审查活动日志和报告，及时根据新的 AI 服务更新策略，并向领导层通报进展（比如未经授权应用程序的使用量下降或已防范的事件）。这将帮助你在当前以及未来环境不断变化的情况下，降低潜在风险。

通过采取上述措施，你可以同时增强创新能力和安全性。

员工能够在工作中使用经批准的 AI 解决方案，IT 部门则可以对这些工具保持控制并确保合规。

借助 Microsoft 365 E3 发现并应对影子 AI 风险

Microsoft 365 E3 为组织提供了发现影子 IT、评估潜在风险以及实施安全性与合规性策略的能力，并且*不会*抑制创新。这套集成的高效办公、安全防护和管理功能可以帮助你直接应对影子 AI 挑战。

Microsoft 365 E3 解决方案	如何助力应对潜在的影子 AI 风险
Cloud App Discovery	**发现未经许可的应用程序并采取行动。**借助 Cloud App Discovery，你可以上传活动日志并生成快照报告，从而掌握超过 31,000 款云应用的使用情况，包括 400 多款生成式 AI 应用程序。通过该工具，你可以了解组织内正在使用哪些应用程序、由谁使用以及使用频率。这些信息有助于你做出明智决策，确定允许或限制使用哪些应用程序。
Microsoft Purview 数据丢失防护 (DLP)	**降低敏感数据泄露风险。**借助 Microsoft Purview DLP，你可以制定并应用策略，以检测敏感信息，并防止或限制通过 Microsoft 365 服务在电子邮件和文件中共享这些信息。例如，你可以设置规则，以监控、审核或阻止用户通过电子邮件或文件共享敏感信息，并及时提醒用户。
Microsoft Entra ID P1	**管理对云应用的访问权限。**Microsoft Entra ID P1 支持通过条件访问策略，控制谁可以在什么条件下访问哪些应用程序。例如，你可以选择要求进行多重身份验证，或限制使用企业凭据登录认定为高风险的应用程序。Microsoft Entra ID P1 可在合规设备和批准条件下，为合适人员提供对云资源的访问，同时限制对未经批准应用的访问。
Microsoft Intune P1	**执行设备和应用程序使用策略。**借助 Microsoft Intune P1，你可以允许将受管理且合规的设备用于工作，它还会为你提供管理这些设备的工具。例如，它可以禁止在公司电脑上安装未经批准的软件，或推送限制访问特定网站或服务的配置。
Microsoft Defender for Endpoint P1	**限制对未经批准 URL 的访问。**Microsoft Defender for Endpoint P1 可通过阻止受管理设备访问未经批准的 URL，帮助降低来自高风险网站的风险。例如，员工在公司笔记本电脑上尝试访问已知的高风险 AI 网站时，将被阻止访问。

采取后续行动，推进你的 AI 采用之旅 →

一切始于认知、合适的工具和积极主动的计划。Microsoft 365 E3 提供一系列工具，帮助你的组织为 AI 解决方案建立强大的安全基础和治理框架。你将能够洞察未获批准的工具，启用保护敏感数据的策略，并持续管控用户访问和设备安全性。做好准备，从被动应对（在影子 AI 出现后才发现并阻止）转向更积极主动的方式，引导通过安全且受管理的渠道来应用 AI。参与 AI 安全评估，了解如何提高你组织的 AI 安全状况。详细了解 Microsoft 365 企业版所包含的功能。