

在安全基础之上 释放 AI 潜力



目录

- 01 AI 机遇与安全要务
- 02 善意举措可能带来的风险：AI 示例场景
- 03 使用 Microsoft 365 E3 构建安全、AI 就绪的基础
- 04 继续 AI 采用之旅



引言

AI 机遇与安全要务

当今劳动力的生产力差距日益扩大。在近期发布的《工作趋势指数》报告中，对 31 个国家/地区的知识型工作者区（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¹。与此同时，**超过 50%** 的受访企业领导者表示，需要提高生产力才能实现目标¹。这为我们提供了一个契机，以审视当前的工作方式，并探索有助于弥合这一差距的潜在解决方案。AI，包括智能体在内，作为一种解决方案具有很大的潜力。**超过 80%** 的受访领导者表示，他们有信心在未来 12 到 18 个月内，所在组织将开始使用 AI 智能体来扩展劳动力规模¹。

这种对 AI 的快速推进存在一个需要注意的问题：创新应与强大的安全保障和数据保护相结合，以降低潜在风险。iSMG 最近发布的研究报告表明，**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。领导者面临双重使命：加快 AI 的采用以提升生产力，以及在这个新时代保护数据。

本电子书将解析可能带来潜在风险的 AI 场景示例，分享使用 Microsoft 365 E3 降低这些风险的技巧，并附上一份检查清单，帮助组织开始或继续为大规模采用 AI 做好准备。准备好充满信心地接纳 AI 吧，让你的组织能够在遵守安全或合规标准的前提下，利用 AI 实现创新。





善意举措可能带来的风险：AI 示例场景

在 AI 的使用和采用过程中，最大的风险往往源于善意地履行职责、希望产生更大影响的员工。在追求提高生产力的过程中，团队成员可能会无意中与 AI 工具过度共享敏感信息，或者使用尚未获得 IT 部门批准的应用程序。这可能会带来风险，并可能使组织面临新的威胁。

让我们通过两个示例场景来说明这一点：一个是办公室信息工作者，另一个是一线员工。

在这些虚构的场景中，你将了解到：1) 即使是出于好意的 AI 使用，如果缺乏有效管控，也可能引发安全问题；2) 这些潜在风险可以通过强健的安全基础加以防范。



在安全基础之上释放 AI 潜力

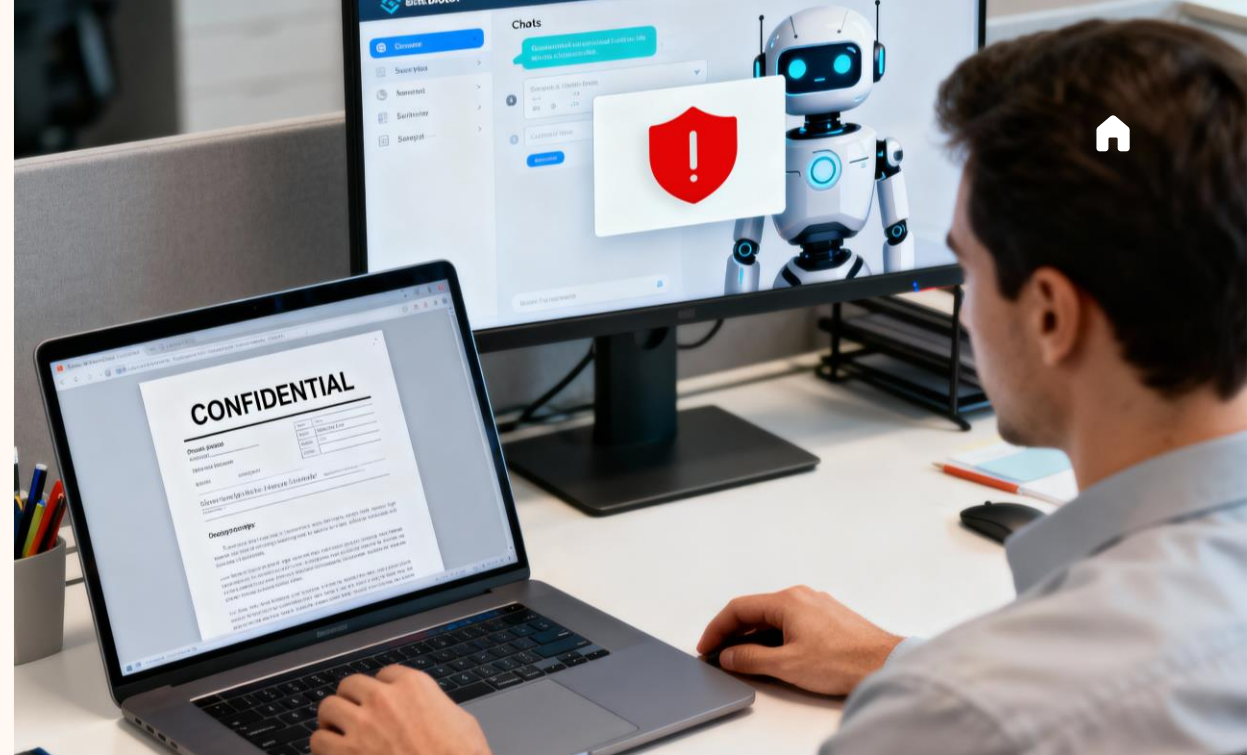
示例场景 14

产品营销经理借助 AI 工具起草新闻稿

一家制造公司的产品营销经理需要在紧迫的时间内撰写一篇关于未来几个月即将推出的新产品的新闻稿。为了头脑风暴并提高写作效率，这位员工将机密产品路线图和内部财务预测中的摘录复制粘贴到免费的在线 AI 写作助手。AI 工具迅速生成了一些精炼的段落，员工随后将这些段落用于新闻稿草稿中。不过，该工具尚未经过他们组织的审查或批准。

潜在风险：

通过使用这个外部 AI 服务，员工将敏感的公司数据（产品计划和财务信息）上传到了 IT 团队无法查看、管理或控制的第三方系统。一旦数据被共享给 AI 工具，公司就会失去对数据的控制权，因为这已经超出了授权范围。组织现在无法知道数据被存储了多长时间、谁可以访问这些数据，以及第三方如何使用这些数据。原本旨在快速提高工作效率的行动，却演变成了一起数据泄露事件。这种情况反映了潜在的内部风险，即出于好意的员工与未批准的 AI 工具共享敏感数据，从而给组织造成漏洞。



使用 Microsoft 365 E3 降低风险：

Microsoft 365 E3 包含多项功能和特性，可以帮助防止此类情况发生。**Microsoft Purview 信息保护计划 1** 可让你为产品路线图和财务预测等文档应用敏感度标签和加密。如果这些文档已被归类并加密，同时贴上具有加密属性的 *机密* 等敏感度标签，那么只有授权用户具有对这些文档的访问权限。此外，**Cloud App Discovery** 可以帮助识别正在使用的生成式 AI 云应用（来自云应用目录中的众多应用），包括具体哪些用户在使用，以及使用频率。IT 部门本可以发现员工正在使用这款特定的 AI 工具，并采取措施，通过 **Microsoft Defender for Endpoint P1** 限制其使用，或提供经批准的替代方案。Microsoft 365 E3 提供各种工具和功能，帮助组织提高可见性并降低风险。

在安全基础之上释放 AI 潜力

示例场景 2⁴

一家零售店的经理使用 AI 起草员工排班表和绩效记录

一家大型零售连锁店的门店经理因繁重的行政类任务感到压力巨大，发现了一款免费的 AI 高效办公应用，该应用承诺可以帮助他进行排班和文档处理。为了节省时间，该经理将包含员工姓名、电话号码、时薪、工作时间偏好和最近绩效记录的电子表格上传到 AI 工具中。他们要求该 AI 应用创建优化的排班，并协助起草即将举行的一对一会议所需的绩效评估总结。

潜在风险：

通过将这些员工数据上传到未经审查的 AI 应用，该经理将员工的敏感个人信息暴露给了公司无法控制和监督的第三方系统。这可能会造成潜在的隐私侵犯和劳动法合规性问题。公司的人力资源 and IT 部门无法掌握员工数据目前的存储位置、存储时长，以及可访问人员。原本旨在提高效率的行动，最后却带来了严重的法律、隐私和员工信任问题。



使用 Microsoft 365 E3 降低风险：

Microsoft 365 E3 的设备和应用程序管理功能有助于降低此类一线场景风险。借助 **Microsoft Intune P1**，零售商的 IT 团队可以实施应用程序保护策略，将规则应用于访问工作数据的应用程序，比如限制将复制和粘贴及数据传输到非托管应用。如果零售商通过 **Microsoft Entra ID P1** 创建条件访问策略，则可以阻止来自非托管应用或设备对企业帐户的登录尝试。在此场景下，如果经理的手机不合规或应用未受管理，这些策略可帮助阻止它们访问受限的公司文件或将这些文件上传至影子 AI 应用程序。

关键见解：在这两种场景下，员工的目标都是积极的，即利用 AI 提升工作效率。不过，如果没有适当的保护机制和策略，结果可能会是负面的。这些例子凸显了在没有安全保障的情况下采用 AI，可能会为组织带来新的、额外的风险。我们的目标不是阻止 AI 的使用，而是以负责任的方式加以应用。下一节将探讨在评估可能提升工作效率的解决方案时应考虑的基本功能，并介绍 Microsoft 365 E3 提供的相关功能，这些功能可帮助组织设置防护措施，确保敏感数据保留在经批准的安全渠道中。

使用 Microsoft 365 E3 构建安全、AI 就绪的基础

组织是否已做好实现 AI 规模化应用的准备？请查看以下检查清单，了解 Microsoft 365 E3 如何为组织提供助力。

随着 AI 采用加速，在扩大 AI 采用的规模之前，评估贵组织的安全状况并识别潜在风险变得尤为重要。Microsoft 365 E3 致力于打造一个 AI 就绪的高效办公和安全基础，结合了广泛的身份、安全、合规和管理工具，这些工具协同工作，可帮助你自信地扩大 AI 采用的规模。

将以下检查清单作为起点，了解贵组织目前的状况。如果任何项目尚未完全实施，组织都可能面临不必要的风险。



强制执行严格的身份认证和访问管理策略，例如多重身份验证 (MFA) 和条件访问。

Microsoft 365 E3 包含 **Microsoft Entra ID P1**，能够在云端和本地环境中强制实施强大的身份认证和访问管理。MFA 和条件访问策略等解决方案可验证每次登录，并根据比如用户角色、设备健康状况和位置等标准限制或允许访问，从而有助于减少未经授权的访问和数据过度共享。例如，你可以将 AI 应用程序的访问权限限制为特定员工群体，并要求登录时使用多重身份验证，从而降低帐户被盗用的风险。条件访问策略可以进一步保护敏感数据，阻止员工使用公司凭据访问未批准的应用程序，共享设备还可以强制执行注销规则，以防止未经授权的会话使用。



支持在托管终结点和设备之间安全协作。

Microsoft 365 E3 通过 **Intune P1**、**Defender for Endpoint P1** 和 **Windows E3** 等解决方案确保智能的终结点安全性。这些工具可以帮助管理和提高 PC、移动设备和应用的安全性。组织可以强制实施 Web 筛选来阻止高风险网站（包括未批准的 AI 工具），并利用 **Windows 自动更新** 和 **Windows Autopilot** 及时为设备安装最新的安全修补程序。这些控制措施有助于保持设备健康、受管控，并及时更新安全修补程序，从而减少攻击面。统一的终结点和设备管理使组织能够保障工作设备安全，并确保应用程序合规，无论员工使用的是个人设备还是公司配发的设备。



通过使用敏感度标签和数据丢失防护策略等功能来保护数据。

Microsoft 365 E3 提供核心 **Purview** 功能，即敏感度标签、加密和数据丢失防护 (DLP)，以保护文档和电子邮件中的敏感信息。一旦标签策略发布，员工即可对包含财务数据、个人信息或知识产权的文件进行分类（例如，使用“机密”敏感度标签），并对其进行加密和设置访问控制。DLP 策略可能会检测并限制在 **Exchange Online 和 SharePoint Online/OneDrive for Business** 内的未经授权的共享。即使在使用**智能 Microsoft 365 Copilot 副驾驶®** 时，这些保护措施仍然有效：Copilot 遵循最高敏感度标签，并防止未经授权的用户访问或处理受保护的内容。



洞察未批准 AI 工具的使用情况，并采取有信息依据的行动。

Microsoft 365 E3 包含 **Cloud App Discovery**，可帮助你了解哪些 AI 应用程序正在使用（来自云应用目录）、由谁使用，以及相关的风险评分，从而据此采取行动。如被认定风险过高，IT 可以使用 **Defender for Endpoint P1** 来限制个人在受管理的 Windows 11 设备上访问该 URL 的能力。例如，如果你发现有 100 名用户正在使用某个未经 IT 部门审核或批准的 AI 图像生成工具，IT 可以根据组织的安全与合规标准对此进行调查。如果认为存在风险，IT 部门可以建议一个经批准的替代方案。有了这些功能，你可以降低影子 AI 的风险，并就 AI 的使用做出适合组织的合理决定。



提供经批准的 AI 应用，例如智能 Microsoft 365 Copilot 副驾驶®。

提供经批准的 AI 应用程序能够为员工提供符合组织安全与合规标准的强大工具，从而带来显著价值。例如，员工无需使用未经审核的 AI 图像生成器或聊天机器人，IT 部门可以提供经批准的替代方案，比如**智能 Microsoft 365 Copilot 副驾驶®**，这些方案会受到监控、支持，并集成到公司现有的政策中。**智能 Microsoft 365 Copilot 副驾驶®** 提供安全、企业级的 AI 解决方案，并深度集成到 Microsoft 365 高效办公套件中。**Copilot** 让员工能够更智能地开展工作、自动执行例行任务并生成洞察，同时遵守身份和数据保护政策。这种方法可以减少影子 IT，有助于限制数据泄露，并使组织能够洞察和管控 AI 的使用方式。



这些功能并不是各自孤立运行的，它们协同作用，形成集成化的多层防御体系。身份、设备和数据保护策略协同作用，帮助你缓解威胁。当安全团队确信此类管控措施已到位时，安全便能成为推动创新的助力，而非阻碍。

Microsoft 365 E3 使你能够建立合适的防护措施，确保贵组织在不危害安全性的前提下利用 AI 实现创新。



继续 AI 采用之旅

每个组织都在探索如何更好地利用 AI 来实现其目标。AI 的前景令人向往，但在采用 AI 的同时，必须同时实施强有力的安全防护。使用 Microsoft 365 E3，你无需在两者之间做出选择。这一强大套件可帮助你提升安全性和合规性，让你安心无忧地采用 AI。

评估 AI 安全就绪性。



Microsoft 提供 **AI 安全评估**³。此[在线评估](https://security-for-ai-assessment.microsoft.com)（地址：security-for-ai-assessment.microsoft.com）会根据你提供的信息，为你提供提升 AI 安全性的建议。它帮助你从**准备**、**发现**、**保护**，以及**治理**这四个关键支柱的角度评估当前的 AI 安全状况，并提供切实可行的建议。

了解更多信息并与 Microsoft 联系。



深入了解 Microsoft 365 E3 的强大功能，以及它们如何帮助你安心采用 AI。
www.microsoft.com/en-us/microsoft-365/enterprise/e3?activetab=pivot:overviewtab。你也可以联系 Microsoft 客户团队或合作伙伴。

- ¹ [工作趋势指数年度报告，《2025：前沿企业诞生之年》](#)，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 [“Second Annual Generative AI Study: Business Rewards vs. Security Risks”](#)，ISMG, Inc.，2025 年 2 月，基于 2024 年第 3 季度对 360 多名商业和网络安全专业人士的调查反馈。
- ³ AI 安全评估：security-for-ai-assessment.microsoft.com/ 结果的准确性取决于输入的准确性。报告仅供信息参考，不对性能或结果作出保证。这不应被解读为 Microsoft 的承诺。实际结果可能因地点、购买方式和使用情况等因素而异。Microsoft 对本报告或网站的内容不作任何明示或默示保证。
- ⁴ 文中所述场景均为虚构，仅用于说明用途。

