# 安全的基础

## 从零信任到 AI 驱动的高效

Microsoft 365

# 目录

## 2018 至 2022 年平均每月身份攻击次数的增加幅度[1]

**+1,329%**
密码喷射攻击

**+26%**
密码攻击

**+35%**
网络钓鱼攻击

如今，人们可以随处办公。无论是在办公室、在家还是在通勤途中，员工都希望能够随时随地开展工作，不会被中断。许多组织通过混合解决方案来满足这种随处办公的需求。但创造合适的环境就意味着需要面对一系列不断变化的挑战。

对许多组织来说，远程办公需要连接员工自有设备来完成工作，其他组织则会提供额外的设备供远程使用。这两种情况都可能导致不受管理的终结点和身份增多。已经忙于现有日常工作的 IT 工作者通常没有时间或工具来安全地管理所有这些工作。

过去几年网络攻击次数显著增加，单个不受管理的设备可能会使整个组织面临风险。

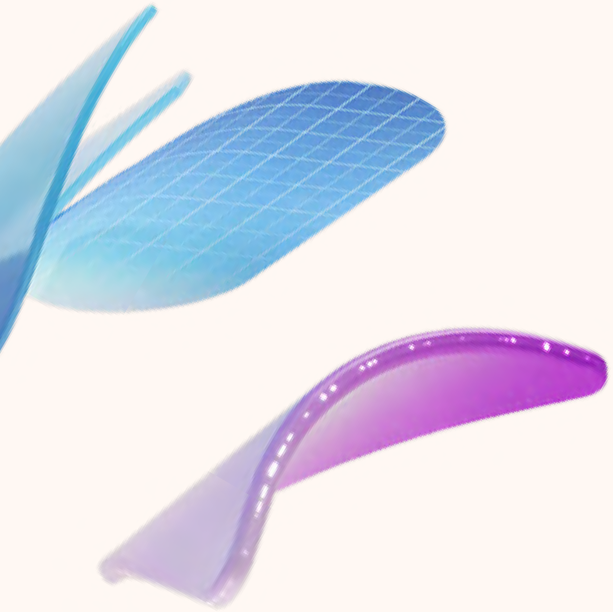
要实现新的工作方式，需要在整个企业范围内采用以零信任为基础的技术，以实现灵活、高效办公。专为集中管理安全性而构建的工具至关重要。但这些工具必须为员工提供所需的立足点，让他们能够高效地工作，从而随时随地展开协作并发挥创意。

零信任是一种安全模型，该模型假定对任何内部或外部实体都不存在隐式信任，并且需要持续验证身份、设备、数据和网络。

本电子书探讨了现今的混合工作环境如何产生风险、为什么会产生风险，以及组织可以使用哪些工具来确保其技术的安全，从而实现随时随地高效工作。

# 当今工作环境中的安全风险

虽然组织希望改进其工作方式，但 68% 的组织经历过一次或多次终结点攻击，导致他们的数据和 / 或 IT 基础结构遭到入侵。[2] 一个安全漏洞就可能会削弱客户未来几年对组织的信心，平均损失达 445 万美元。[3] 如果没有适当的安全性，组织面临的风险将不仅仅是停机。也许更重要的是，他们将面临长期声誉受损的风险。



## 灵活的工作场所中不受管理的设备和身份增加

虽然员工已做好随处办公的准备，但其组织的安全性可能尚未准备充分。超过一半的组织对其至少四分之一的终结点没有可见性或控制权。[4] 随着可以完成工作的地点增多，不受管理的设备和身份的数量也可能会增加。

当员工在混合环境中工作和协作时，他们可能会发现现有工具存在不足。如果没有经过优化的应用，远程协作可能会很困难，而且台式机、笔记本电脑和移动设备之间的软件界面可能会有很大差异。这导致一些员工转而使用影子 IT，据报告，80% 的员工会使用未经审核和批准的应用和设备。[5]

由于 IT 团队需要手动发现和限制访问大量不受管理的终结点，近 70% 的 IT 人员报告称，他们在尝试管理远程工作时感到力不从心。[7]

**3,500**

连接到企业的不受管理、不受保护的平均设备数量 [6]

**+71%**

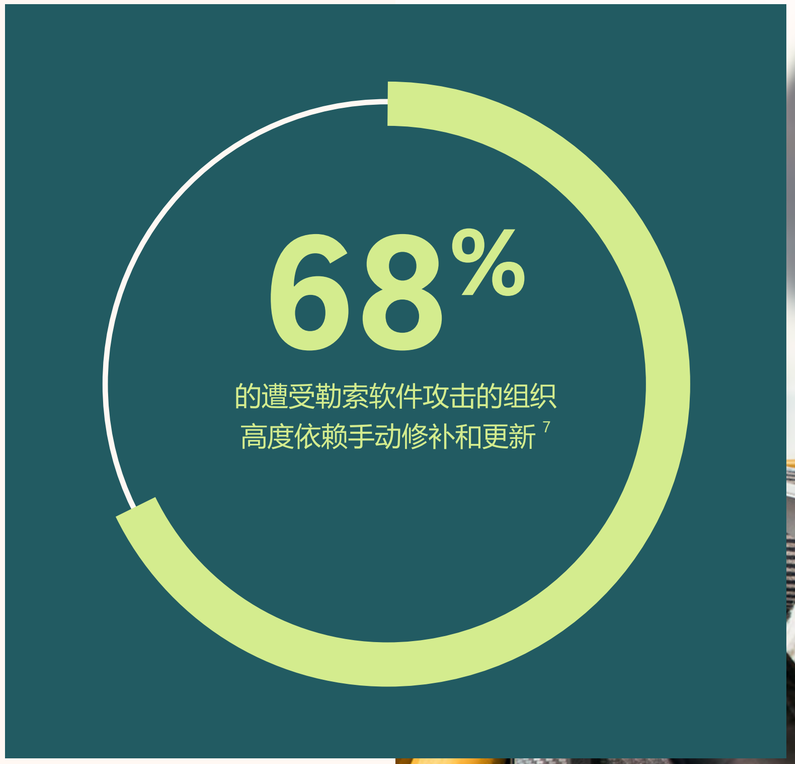
在不受管理的设备上，感染的可能性的增加幅度 [6]

# 过时的手动终结点和应用管理

要以适当的方式保护大量增加的员工所有设备以及员工随处办公所需的应用和工具，组织必须解决其旧式终结点、软件和应用问题。近 90% 的安全领导者同意，过时的 PC 硬件让组织容易受到攻击，但报告显示，大多数组织都有三分之一的硬件已经过时。[8] 不到一半的组织每两年更新一次计算机。[8]

依赖手动修补和更新的设备存在相当大的风险。从更新或修补程序可用到实施，这之间会产生安全缺口，让组织容易受到攻击。此外，手动更新设备所需的时间可能会延迟更重要的战略性 IT 工作。报告显示，超过一半的 IT 团队没有在战略性工作上投入足够的时间，例如抵御日益复杂的网络攻击技术。相反，他们的时间通常被软件和固件修补程序等日常问题所占据。[7]

当组织实施新技术时，他们必须确保停用冗余解决方案。72% 的组织报告称，过去两年其 IT 环境的复杂性有所增加。[9] 这种复杂性不仅是指计算环境的复杂性，还表示 IT 团队工作日益增加的复杂性。



# 打造零信任基础

要将组织转变为现代化环境，让员工可以按需随处办公，这可能是一项重大的任务，而安全性必须放在首位。如果不解决安全问题或解决程度不足，组织可能会面临巨大的损失风险。为了让组织的安全状况保持不变，你的 IT 团队可能已经管理了许多不同的小规模问题。他们需要相应的解决方案来专注处理更紧要的安全风险，以应对不断增加的攻击。这款合适的解决方案必须提供内置安全性的高效办公工具。

## 来自 Microsoft 的安全解决方案

Microsoft 365 E3 是一款全面的、基于云的工作效率和安全性解决方案，可为现代化办公构建强大的零信任基础。通过身份管理、威胁防护和数据安全措施，Microsoft 365 E3 可以确保企业的安全性，同时帮助团队进行有效协作并消除冗余解决方案。

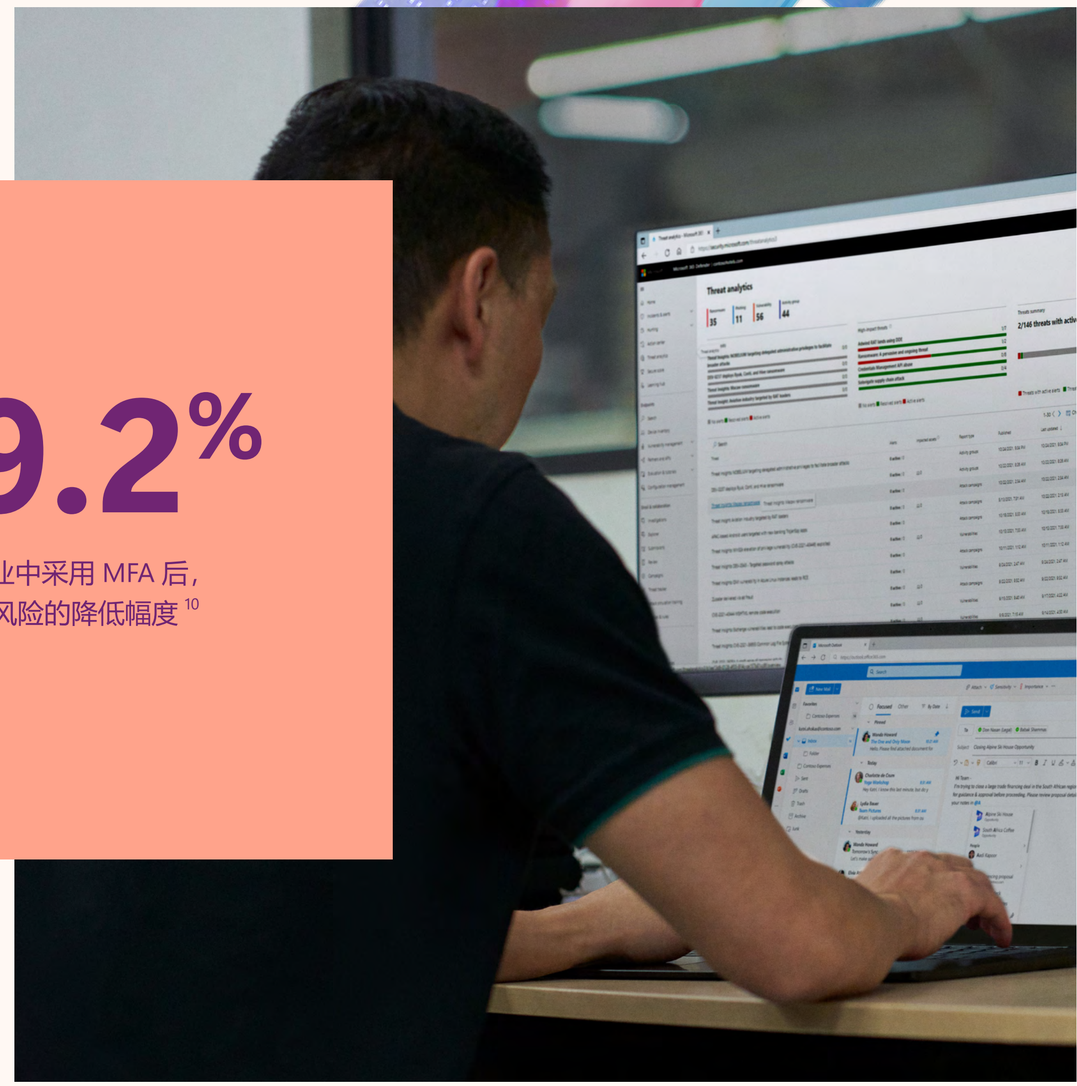
# 保护组织的所有身份

借助 Microsoft 365 E3，你可以大规模实施简单有效的身份安全措施。

通过在整个组织中采用多重身份验证 (MFA) 和无密码登录方法，可以显著降低入侵风险。结合持续访问评估，你可以确保所有登录尝试都在正常的地理区域和工作时间内进行。这将创建一个受到高度保护且易于员工使用的登录流程。

一旦有身份登录到组织，Microsoft 365 E3 就会以 Microsoft Intune 的形式提供强大的基于风险的条件访问管理工具。

借助 Intune，IT 团队可以按角色设置应用和工具的访问权限，员工则可以使用自助服务选项来解决密码重置等常见问题。这样一来，员工问题能够更快地得到解决，因此组织可以在三年内 * 在每位用户身上节省高达 79 美元的成本。[11]



**99.2%**

在整个企业中采用 MFA 后，
身份泄露风险的降低幅度 [10]

组织每个月可在每位用户 * 身上节省

**55 美元**

（整合供应商与
Microsoft 365 后）[11]

**97%**

的受访者报告称，IT 团队在部署
终结点更新方面实现了效率提升 *[11]

## 显著降低终结点管理复杂性并防范威胁

借助 Microsoft 365 E3，组织可以实现现代化的统一终结点管理，并获得所有终结点的可见性。作为单一解决方案，Microsoft 365 还可以减少组织中专用解决方案和企业设备的数量，从而节省资金，并让 IT 团队能够专注于完成规模更大的任务，例如战略性安全规划和更新设备资产。

Microsoft 365 E3 中还包含安全、部署和软件更新自动化功能，可减轻忙碌的 IT 员工的负担，并让企业终结点保持最新状态。

云终结点部署意味着员工可以安全地将 Windows 桌面、应用、设置和内容从 Microsoft 云流式传输到云电脑。组织无需花费资金实施辅助解决方案，即可快速为员工完成设置，让他们能够随处办公。除此以外，部署方面也节省了大量时间，相当于三年内平均节省 1,500 万美元。*[11]

跨所有应用和环境实现自动威胁防护和修复，让 IT 团队能够针对常见网络威胁配置条件响应。如果没有自动化功能，这些工作将占用 IT 员工宝贵的时间。此外，自动软件更新可让员工从 Microsoft 云快速安全地流式传输最新版本的应用、设置和内容。

## 管理和保护组织的敏感信息

Microsoft 365 E3 是一款完全集成的解决方案，可让 IT 团队大规模发现敏感信息并进行分类。信息保护甚至可以在 Microsoft 和非 Microsoft 应用之间扩展。借助敏感数据标记和丢失防护、端到端加密、电子数据展示以及合规管理器等功能，IT 团队可以对传输中的数据和静态数据进行分类、监控和控制。

借助 Microsoft 365，
组织预计可节省高达

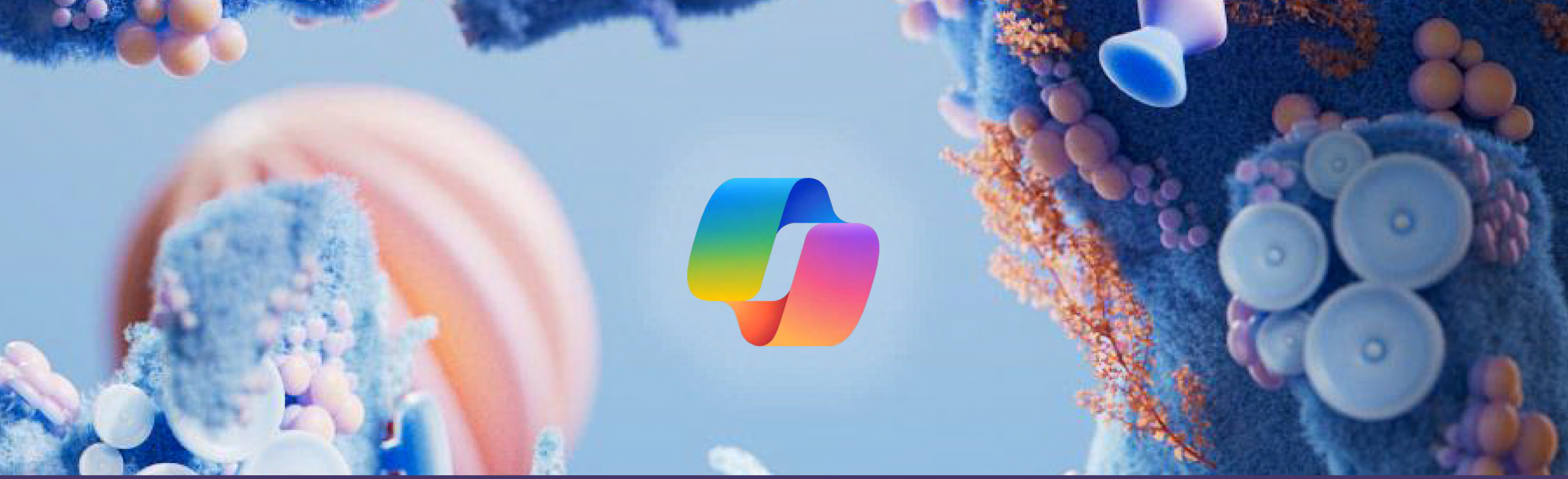
# 120 万美元

这是三年内数据泄露风险降低
带来的成本节省[11]

# 具有安全基础的现代化办公

当组织的基础得到保护、数据实现连接并且团队保持联系后，Microsoft 365 E3 可以实现高工作效率，从而满足新的工作时代的需求。借助 Microsoft 365，员工可以随时随地安全地访问完成工作所需的应用、工具和数据。

Microsoft 365 E3 可以帮助组织实现其数字化转型目标，并让员工能够协同工作。通过出色的高效办公应用建立联系后，员工无论身在何处，都可以协力工作并提高工作效率。



# 借助强大的 AI 工具提高工作效率

Microsoft Copilot for Microsoft 365 可进一步提高工作效率，充当敏捷的助理来帮助员工精简工作，每天完成更多任务。Copilot 与组织的数据集成，并与 Microsoft 365 应用程序协同工作，可实现常规流程的自动化、创建演示文稿、设计数据可视化效果、编写文档等。Copilot 为员工提供了 AI 工具，能够将他们的想法转化为世界上最强大的高效办公工具之一。

Copilot 以三种不同的方式工作。第一，通过创建供员工完善的初稿、生成专业的数据可视化效果以及分析趋势，激发员工的创造力。第二，通过总结电子邮件、消息和待办事项来智能地减少繁琐的工作，从而提高工作效率。第三，通过数千个自然语言 AI 命令来帮助员工更轻松地完成工作，同时提升员工的技能。

# Microsoft 365 企业版

借助 Microsoft 365 E3 构建安全的基础
以实现灵活办公。

了解更多信息 >

# 来源：


[1] “Microsoft Entra：2023 年关于身份的 5 大优先事项”，Microsoft 安全博客，2023 年 1 月 9 日。
https://www.microsoft.com/en-us/security/blog/2023/01/09/microsoft-entra-5-identity-priorities-for-2023/

[2] “The 3rd Annual Study on the State of Endpoint Security Risk”，Ponemon，2020 年 1 月。

[3] Cost of a Data Breach Report 2023，IBM，2023 年 7 月。
https://www.ibm.com/reports/data-breach

[4] Dave Gruber 和 Gabe Knuth，“Managing the Endpoint Vulnerability Gap: The Convergence of It and Security to Reduce Exposure”，Enterprise Strategy Group，2023 年 2 月。
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWXwKT

[5] “发现和管理影子 IT - Microsoft Defender for Cloud Apps”，Microsoft Learn，2023 年 5 月 24 日。
https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-shadow-it

[6] “现代攻击面剖析”，Microsoft Security Insider，2023 年 5 月 2 日。
https://www.microsoft.com/en-us/security/business/security-insider/threat-briefs/anatomy-of-a-modern-attack-surface/

[7] Microsoft，“2022 年 Microsoft 数字防御报告：阐明威胁格局，加强数字防御”。
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

[8] “安全信号助力 SDM 研究学习”，Microsoft 安全，2021 年 9 月。
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWP0mz

[9] Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022，新闻稿，2022 年 9 月。
https://www.gartner.com/en/newsroom/press-releases/2022-09-12-gartner-survey-shows-seventy-five-percent-of-organizations-are-pursuing-security-vendor-consolidation-in-2022

[10] “Microsoft 数字防御报告：构建和提升网络复原能力”，Microsoft 威胁情报，2023 年 10 月。
https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

[11] The Total Economic Impact ™ of Microsoft 365 E3，一项由 Forrester Consulting 进行的委托研究，2022 年 10 月。结果基于美国的一家在全球开展业务、拥有 30,000 名员工且使用 Microsoft 365 E3 的复合型组织。
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5970p


Microsoft 365