

# 确保混合办公的五项建议

随着全球更持久地转向混合办公，这种灵活性在给雇主和员工带来前所未有的益处的同时，也引发了一些挑战。无论您的团队是现场、远程办公，还是移动办公，您都不必为了提高灵活性而牺牲安全性。为此，我们精心准备了五项简单易行的建议，旨在帮助您为打造混合办公文化提供有力支撑，同时有效保护您的员工和公司资产。



## 1 培训员工，确保他们遵循安全办公原则

员工希望无论在哪里办公，技术都能“如影随形”。但是，灵活选择办公地点又会让它们（和您的组织）面临新的威胁。因此，IT 和安全团队需要让用户了解安全实践和潜在危险，以确保用户在每部终端上都能畅享安全可靠的混合办公体验。



2

## 2 验证用户的真实身份

多因素身份验证 (MFA) 简单易用，是所有企业在授予公司资产访问权限之前不可或缺的第一层安全保护。简而言之，MFA 就是使用您知道的信息（您的用户名/密码）和您拥有的设备（您的电话）来验证您的身份和设备运行状况。



## 3 确保随时随地安全访问

VPN 在用户和应用程序之间提供了一个安全隧道，使员工在出差或在家办公时仍能保持连接和高效工作。它可以在不影响用户体验的情况下提供适当级别的安全保护，帮助确保只有经过批准的用户才能访问公司网络。



4

## 4 在任何入口点防御安全威胁

大多数安全漏洞都以终端用户为攻击目标，因此需要在 DNS 层设置第一道防线，并针对越过防线的威胁设置最后一道防线。第一层安全防护可屏蔽与恶意行为关联的域，防止恶意软件侵入您的网络，或者遏制已经侵入的恶意软件，而最后一层则用来防御更高级的威胁。



## 5 通过简单省心的集成平台提供一致的安全保护

避免使用东拼西凑起来的安全解决方案，这会让用户无法获得一致的体验。借助 SecureX 可轻松高效地为用户提供安全保护。SecureX 是一个内置的无缝集成平台，可将您的各种 Cisco Secure 产品与基础设施连接在一起。



Cisco Secure 混合办公解决方案是一款简单省心、统一一致的解决方案，可提供无处不在的安全保护，并助力员工随时随地办公。它可以确保无论您的员工在哪里工作，数据始终安全无虞。

详情请访问 [cisco.com/go/securehybridwork](https://cisco.com/go/securehybridwork)。