

保护远程团队的 8 个关键点



现代远程团队是由可以在线工作以及可以完成工作的人员构成。这就意味着各种不同类型的用户在相同的工具上一起工作—全职员工、承包商、自由职业者、供应商和合作伙伴。您如何才能在不降低数据速率的情况下随时随地保护公司的数据？以下是在不降低数据速率的情况下保护现代远程团队的 8 个最佳实践。



1、安全访问内部管理的应用程序

您可能正在使用传统 VPN 保护企业的内部应用程序—不过这种模式可能会在员工大规模远程连接时发生故障。更有甚者，VPN 过度许可，信任所有可以让其访问的东西。

现代解决方案依赖于零信任模型：在不影响或降低 VPN 性能的情况下查询所有数据包。



2、保护您的团队免遭互联网威胁

如果使用 SaaS 应用程序，您的团队将有暴露于互联网威胁的风险。从历史上来说，企业已将外向互联网请求路由至总部进行威胁扫描—但这样做速度很慢，且在规模较大时显得不稳定。

您需要一种在不干扰团队的情况下识别和停止最新威胁的方法。



3、随时随地保护您的企业数据安全

您的企业最宝贵的数据可能横跨 SaaS 供应商、内部应用程序、公共云等等。确保本数据只用于为本地和云服务支持提供保护。

保护远程团队的 8 个关键点



4、使用所有人都可以使用的工具。

如果您的安全态势让您的团队感到头疼，您的 IT 员工就会感到很大的压力。员工可能会放弃使用内部工具（更有甚者：视图寻找应变之法）。

为什么不选择一种他们熟悉的系统——一种使用他们习惯使用的 Google 或 OKta 登录呢？



5、快速跟踪您的承包商

现代劳动力是流动的。由于承包商和其他外部合作伙伴与您的团队合作，因此从一开始就为他们提供他们所需的一切就显得十分重要——不过仅此一次。工作完成后，您需要确保已撤销他们的授权。

现代身份验证解决方案将与各种识别提供商无缝衔接，包括您的承包商很可能已经在使用的免费服务。



6、使工具易于查找。

高效率的远程团队可以让员工很轻松就能找到他们需要的合适工具。应用启动台是工具汪洋中的救生筏，可以让每个应用程序用户都能访问简单易用的图形化仪表盘。

某些启动台要优于其他同类产品：确保您的启动台支持粒度许可，确保员工只能看到他们能够访问的工具。



7、考虑用新的解决方案解决老问题

如果您已陷于老应用程序的泥沼之中，现在正是您考虑众多成熟 SaaS 解决方案的时候了。如果您有合适的工具保护他们的安全，SaaS 应用可以提供高功能性、连续更新以及众多企业长期时间内比一次性预付更易处理的订阅模式。



8、遇到问题时获取预警

办公室内的仪表盘可能会出现故障，但那并不意味着您毫无所觉。确保您使用了支持密集登录和请求审核的解决方案——并具有导出至安全信息和事件管理 (SIEM) 平台的灵活性。

立即为您的团队解锁更安全、更快速的远程办公解决方案：
teams.cloudflare.com