开发人访问的 Zero Trust 指南

更安全、更快地访问关键工具和基础设施，减轻技术团队的负担

工程师需要对基础设施的特权访问，以维持业务正常运转，他们不希望被拖慢速度。ZTNA 允许拥有特权的技术用户从任何地方访问您的关键基础设施，不会像使用企业 VPN 那样牺牲性能。了解 Zero Trust 安全如何提高技术团队的工作效率，同时增强构建环境的安全性。

在 Cloudflare 近期委托 Forrester 进行的一项研究中，83% 的安全决策者计划今年专注于为开发者提供更安全、更快的访问。[1]

使用 Zero Trust 访问加速技术团队的三种方法

保护构建环境

将开发人员连接到应用程序，但不会让他们暴露到公共互联网。利用安全隧道软件来创建到 Cloudflare 网络的专用隧道，并使用我们的策略引擎来实施多因素身份验证策略。

减少对 VPN 的依赖

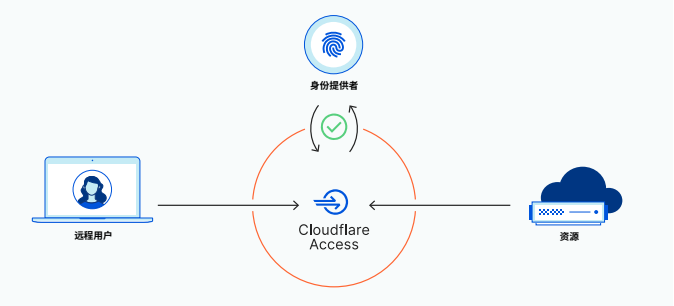
通过 VPN 隧道来连接到基础设施可能会增加延迟，对分布在全球的团队而言更是如此。用户通过 Cloudflare 分布在世界 250+ 地点的数据中心之一连接到您的工具，体验快如闪电的性能。

记录一切

记录受保护的应用程序中发出的任何请求——而不仅限于进入和退出。在 Cloudflare 中汇总活动日志，或将其导出到您的 SIEM 提供商以供分析。

了解详情

Cloudflare 的全球边缘网络分布在世界各地 250+ 地点；始终接近您的用户及其所需的应用程序。在您的基础设施前部署 Cloudflare Access 后，您就不再需要使用 VPN 隧道和回传了。无论身在何处，开发人员都能享受快速、可靠的性能。



Cloudflare Access 可以为您保护什么

SSH 连接

安全外壳 (SSH) 协议允许用户连接到基础设施以进行各种活动，例如远程命令执行。Cloudflare Access 可以保护通过安全外壳 (SSH) 建立的连接。当用户尝试从命令行访问资源时，Access 会启动浏览器窗口，提示他们登录其身份提供商。

Web 和 SaaS 应用程序

使用 Access 保护内部管理的应用程序（例如 Jira、WordPress、GitLab 和 SAP），以便用户无需 VPN 即可登录以访问它们。Cloudflare Access 评估对应用程序发出的请求，并根据您定义的策略确定访问者是否具备授权。

远程桌面

远程桌面协议 (RDP) 允许用户从另一台计算机连接到桌面。Cloudflare Access 使最终用户可以通过其单点登录 (SSO) 提供商进行身份验证，并通过 RDP 连接到共享文件，无需使用 VPN。

其他协议

您可以使用 Cloudflare Access 将身份验证添加到使用任意 TCP 或 UDP 的安全消息块 (SMB) 文件共享或应用程序中。

有意进一步了解？
请访问
cloudflare.com/zh-cn/products/zero-trust/access

1. Forrester 机会快照：Zero Trust，2020 年 10 月

“ Discord 就是世界建立关系之处。Cloudflare 将我们内部工程团队与所需的工具相衔接，帮助我们达成这一使命。有了 Cloudflare，我们知道对关键应用的每个请求都已经过身份和上下文评估——这是一种真正的 Zero Trust 方法，因而我们能够安枕无忧。”

Mark Smith
基础设施总监，Discord

DISCORD

“OneTrust 依托 Cloudflare 来维护我们的网络边界，我们可以专心致志地交付技术产品，帮助我们的客户变得更受信赖。借助 Cloudflare，我们可以轻松构建上下文感知 Zero Trust 策略，以安全地访问我们的开发者工具。员工可以轻松连接到需要的工具，团队甚至不知道是 Cloudflare 在幕后提供支持。这种方法确实有效。”

Blake Brannon
CTO，OneTrust

OneTrust