CLOUDFLARE

解决方案简述

保护分布式办公场所

通过单个统一控制平面对来自任何办公地点的所有请求实施一致的控制

将安全转移到云端

通过 Cloudflare 降低办公室的复杂性和风险

鉴于员工同时在办公室和远程工作，很多组织正在重新评估如何确保办公室安全——无论是依赖于数据中心的设备，还是允许直接、不安全的互联网访问。

他们的新重点是为网络内外的用户提供一致的保护和体验。大多数情况下，这意味着将控制从各种不同的工具(例如 VPN、Web 代理和防火墙)转移到单一云交付安全平台。

Cloudflare 支持企业通过两个常见的用例来实现办公室安全的现代化。

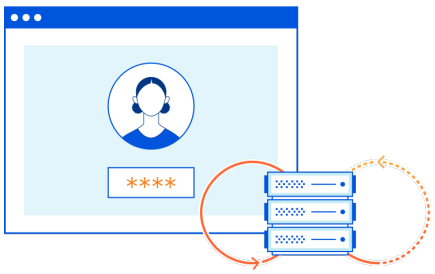
> “通过单一实施将分支机构和远程访问融为一体，确保一致的策略并最大程度减少所需供应商数量。部署 ZTNA 来增强或取代传统 VPN，以限制对传统技术的投资。”[1]
>
> Gartner

推荐用例：

用 Zero Trust 取代 VPN 以保护应用访问

对每个应用执行细粒度的身份感知策略，防止公司网络内部的横向移动。

- **第一步：** 与您的身份提供商集成
- **第二步：** 通过浏览器保护任何 Web 应用
- **第二步：** 通过浏览器保护 SSH、VNC 和 RDP 环境

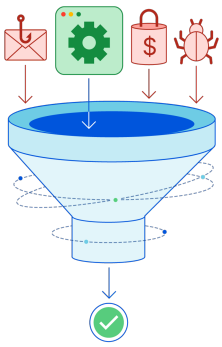


推荐用例：

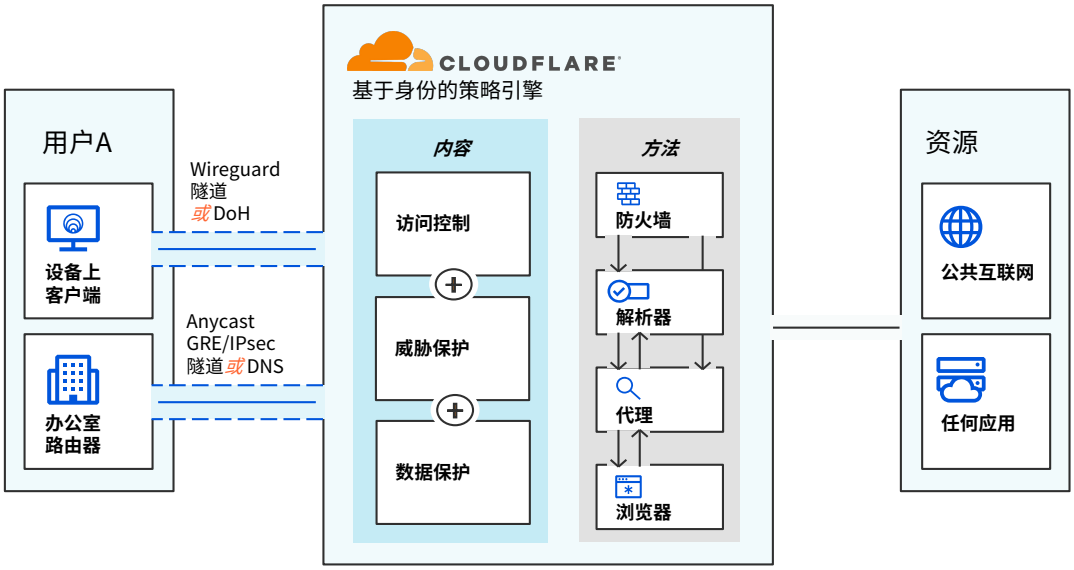
过滤互联网访问，实现一致的安全性，快速实现价值

首先通过 DNS 过滤保护办公室用户，然后在所有地点执行更全面的检查。不再需要回传流量以通过数据中心的本地安全设备。

- **第一步：** 将 DNS 流量指向 Cloudflare 的全球网络
- **第二步：** 设置基于位置的 DNS 过滤，以防止勒索软件、网络钓鱼和其他互联网威胁
- **第三步：** 通过执行无限 TLS 1.3 检查的 HTTP、网络和浏览器隔离规则来控制数据流



工作方式



无客户端部署，以验证访问并过滤来自办公地点的 DNS 查询。

通过 Cloudflare 的设备客户端部署，以增强针对每个用户和设备的可见性和管控。

图： 使用 Cloudflare Zero Trust 一次性验证、过滤、隔离和检查办公室流量

适用于任何来源的灵活入口

首先使用 Cloudflare 处理经网络路由器的 DNS 解析。随着时间的推移，通过您的 GRE 或 IPsec 隧道，或使用您现有的 SD-WAN 路由方法，将 L3 流量发送到我们的全球网络。

或者部署 Cloudflare 的客户端以在托管设备上执行 DNS 和 HTTP 过滤和检查。

快速执行策略，原生全球扩展

所有安全、性能和可靠性功能都被设计为在我们遍布全球 100+ 国家/地区 275+ 数据中心的每台服务器上运行。

我们的网络规模意味着，始终可在靠近办公室和最终用户的地方一次性高速执行保护措施。

探索未来 6-12 个月内的其他用例

重获对 SaaS 应用的控制

发现并降低员工在办公室和家中使用影子 IT 的风险。

从相同的单一 Cloudflare 仪表板启用 CASB 策略，防止数据泄露和违规行为。了解详情。

卸载 MPLS 流量

取代昂贵、老化、缓慢的专用 MPLS 连接。

通过使用 Cloudflare 的全球网络来管理分支机构、数据中心和公有云服务之间的流量，简化传统的 WAN 架构。了解详情。

[1] *Gartner Hype Cycle for Network Security, 2021* | GARTNER 和 HYPE CYCLE 是 Gartner，Inc. 和/或其附属公司在美国和国际上的注册商标和服务标志，在此经许可使用。保留一切权利。