Zero Trust 网络访问（集成专用路由）

防止横向移动，减少对 VPN 的依赖

信任基于网络的应用程序访问控制（如 VPN 和 IP 位置限制）会增加您的攻击面，限制可见性，并让最终用户感到沮丧。Cloudflare 的 Zero Trust 与身份提供商和端点保护平台协同工作，实施默认拒绝的 Zero Trust 规则，限制对企业应用程序、内部 IP 空间和主机名的访问。在 Cloudflare 庞大且性能卓越的 Anycast 网络支持下，用户连接速度比VPN 更快。

自从在内部部署 Zero Trust 网络访问以来，Cloudflare 已经取得了如下效益：

- 攻击面减少 91%[1]
- 通过减少 IT 工作量节省 2 倍的成本。
- 在 VPN 相关工单支持上所花费的时间缩短约 80%
- 支持工单数量减少约 70%
- 每年新员工入职节省 300 多个工时

Access 能为您做什么

保护任何应用程序

Cloudflare Access 与身份和应用程序无关，让您能够保护任何应用程序，无论是 SaaS、云还是本地应用程序。

灵活地连接用户，有无客户端均可

简化 web 应用程序和 SSH 连接，无需客户端软件或终端用户配置。对于非 web 应用、RDP 连接和专用路由，利用一个覆盖各种互联网和应用访问用例的综合性客户端。

实现跨多个身份提供者的身份联合

集成所有企业身份提供者（Okta、Azure AD 等），实现更安全的迁移、收购和第三方用户访问。启用临时访问的一次性代码，或集成领英和 GitHub 等社交身份来源。

限制企业资源之间的横向移动

通过 IP 防火墙和 Zero Trust 规则，甚至对传统应用程序也能实施严格、一致的身份认证方法。

启用设备感知访问

在授予对某个资源的访问权限前，对设备态势进行评估，包括网关客户端的存在、序列号和 mTLS 证书，确保只有安全、已知的设备才能连接到您的资源。整合来自端点保护平台（EPP）提供商的设备态势，包括 Crowdstrike、Carbon Black、Sentinel One 和 Tanium。

记录跨越任何应用的用户活动

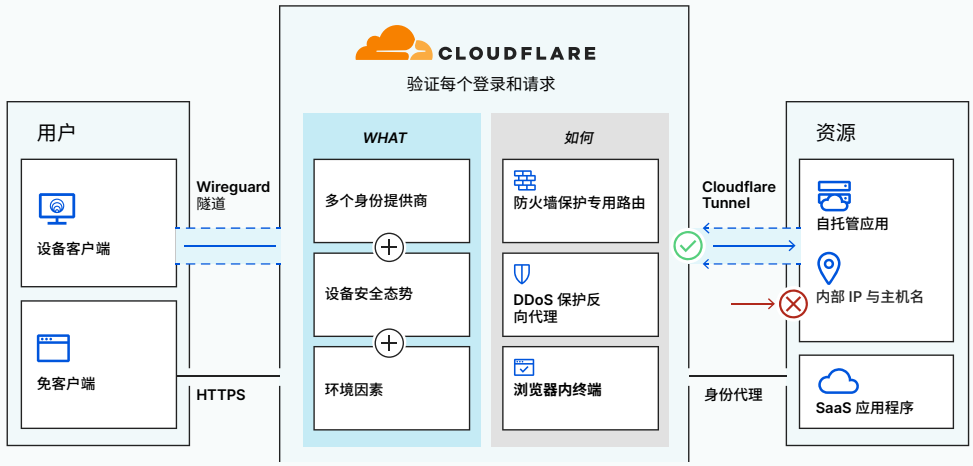
记录在受保护应用程序中发出的任何请求， 不仅仅是登录和登出。在 Cloudflare 中汇总活动日志，或将其导出到您的 SIEM 提供商。

[1]当 Zero Trust 网络访问与互联网浏览相结合时

Cloudflare 的不同之处

- **性能卓越**通过使用 Cloudflare Anycast 网络上经过优化、情报驱动的路由，更快地路由请求。平均而言，web 应用访问速度提高 30%，TCP 连接往返时间缩短 17%。我们的情报基于对每秒 2500 万次 HTTP 请求和每秒 3.9 万个新 TCP 连接的数据所进行的分析。
- **管理简单**将 Zero Trust 网络访问、安全 Web 网关、远程浏览器隔离等整合到一个控制平面中，具备从零开始构建的管理体验，绝非由来自多个供应商的产品拼凑而成的大杂烩。
- **一次性检查**由于每一项 Cloudflare 服务都部署到全球 250 多个地点的每一个数据中心，可在全球各地快速、一致地验证、过滤、隔离和检查流量。

了解详情



用户通过客户端或 web 浏览器连接到企业资源，无需使用 VPN。当请求通过我们的网络进行路由和加速时，它们将被根据 Zero Trust 规则进行评估，这些规则包含来自集成其身份提供者、设备和其他上下文的信号。过去，RDP 软件、SMB 文件查看器和其他胖客户端程序需要 VPN 来实现专用网络连接，而现在，团队可以通过 Cloudflare 的网络私密地路由任何 TCP 或 UDP 流量，并对流量进行加速、验证和过滤，提高性能和安全性。

“Cloudflare Access 让我们无需自行开发身份和访问管理 (IAM) 系统。我们不需要将用户权限功能内置到由 Access 保护的应用程序中。我们已全身心投入；公司每个人都获得了一个席位。”

Jim Tyrrell
基础设施主管，Canva

“Delivery Hero 始终致力于为客户提供出色的体验。Cloudflare Access 可以帮助我们让内部团队享受同样的体验：拥有安全的工作环境，而且无需 VPN 就能从全球各地访问我们的所有应用程序。”

William Carminato
高级总监，工程，Delivery Hero

身份和访问管理 (IAM) 集成

Active Directory · okta · Google Workspace · PingIdentity · CITRIX · Centrify · onelogin · SAML OIDC

端点保护平台 (EPP) 集成

CROWDSTRIKE · vmware Carbon Black · SentinelOne · TANIUM

主要特色

统一策略	
定制应用程序、专用网络和互联网访问策略	**无限制**
企业和社交媒体 idP 身份验证	✓
使用第三方集成和 Cloudflare 的设备态势	✓
CSV格式批量导入企业设备序列号列表	✓

增加可见性	
活动日志保留	**6 个月**
基于身份的国家/地区、州/省和设备详细信息视图	✓
将日志推送至云存储或 SIEM	✓

安全连接	
基于客户端加密的互联网连接（WARP 客户端）	**Win, Mac, iOS, Android**
对自托管和 SaaS 应用程序的无客户端安全访问	✓
面向自托管应用和内部 IP、主机名的专用连接（Cloudflare Tunnel）	✓

简易的互操作性	
端点和移动管理集成	✓
面向本地或 VPN 连接性的隧道拆分	✓
非受管设备的客户端自助注册	✓
可定制的应用程序启动器	✓
同时支持多身份提供者的验证	✓
用于支持 SAML 和 OIDC 的通用和自定义连接器	✓
用于自动设备的基于令牌的验证	✓
面向 IoT 和其他 mTLS 用例的基于证书的授权	✓

性能毫发无损	
正常运行时间 SLA	**100%**
最快的网络之一（与 250+ PoP 延时< 50 ms）	✓
速度最快、隐私第一的 DNS 解析器（通过 250+ PoP 延时 7-31 ms）	✓
闪电般快速的策略更新（到 250+ PoP < 500 ms）	✓
闪电般快速的远程浏览器（不推送像素——运行于我们的网络上；非第三方云）	**附加服务**

有意了解更多?

请访问www.cloudflare.com/zh-cn/products/zero-trust/access/ t以注册一个帐户，50 席位免费。