保护混合办公

为所有用户——无论在网内还是网外——降低风险并增加可见性

保护来自任何用户、任何设备、任何位置的任何连接

我们的随处办公未来：全球疫情已经持续多年，经济衰退即将到来，混合办公看来将成为常态。IT 和安全团队必须为所有用户和设备提供一致的保护和体验，无论是在远程还是在办公室，而传统的以位置为中心的工具（如 VPN 和基于 IP 的控制）无法胜任。

适用于现代劳动力的现代安全保护：作为回应，很多组织正在重新构想其 IT 和安全架构，采用云交付的安全，根据分布式劳动力的需求扩展，并遵循最佳 Zero Trust 实践。

Cloudflare 使保护任何连接变得易如反掌，让使用任何设备或身处任何位置的用户在访问应用程序或互联网时均保持安全、高效。

Gartner® 称：

> *到 2026年，75% 的员工将继续在家庭和传统办公地点之间分配时间，略低于疫情最严重时的 77%。*[1]

> *基于边界安全设备集合的网络安全设计不适合满足现代数字商业及其混合数字劳动力随时随地的动态需求。*[2]

目录

安全现代化机会

在不使用 VPN 的情况下保护应用程式访问

由于用户高度分散，通过 VPN 等本地设备回传流量减慢性能，造成威胁在企业网络内部横向移动的风险。

取而代之，企业应该重获对所有请求的可见性，并在更接近用户的地方执行基于身份的控制，以维持生产效率。无需进行任何回传。

简化 SaaS 安全

现在的员工比以往任何时候都更加依赖传统企业网络控制之外的 SaaS 应用程序。

因此，组织需要对其 SaaS 应用程序获得更全面的可见性和管控，以设置访问策略、应用数据保护控制、缓解影子 IT ，并扫描应用程序的错误配置。

保护用户和数据免受来自互联网的威胁

与此同时，勒索软件、网络钓鱼和其他基于互联网的威胁继续存在，而且越来越复杂。

对传出流量实施基于云的检测和隔离，使用户免受恶意软件的侵害。此外，管理员可以应用控制来防止敏感数据到达本地的非受管设备。

成熟企业：需要现代化安全以实现信心十足的混合办公

挑战：复杂的传统环境

一些企业正在试验办公室内工作的模式。但在这些混合场景中，维持一致的保护和用户体验是并非易事。

这些公司往往更为成熟，已经在本地和传统网络上进行了更大规模（也常常是复杂的）的投资。在经济衰退的背景下启动新的安全项目可能让人感到太危险、太困难。

机会：更简单的现代化路线

企业应该按照自己的节奏进行数字化转型，不需无限的预算、昂贵的“概念验证”、复杂的实施阶段或菊式连接的服务。

为帮助这些成熟的企业满足混合办公需求，Cloudflare 被设计成比其他 Zero Trust 服务提供商（例如 Zscaler）更容易、更快地部署。

示范用例

电信

情景： 一家年营收超过 200 亿美元、拥有 100 多年历史的欧洲电信公司需要一家供应商来部署互联网过滤，并对最近迁移到多个云环境的传统应用程序实施基于身份验证的访问。

解决方案： 该公司选择 Cloudflare 来整合服务，并使用统一平台来确保其 10 万多名员工的应用程序和互联网访问安全。

联邦政府

情景： 美国国土安全部（DHS）正在领导对各联邦办公室、地点和基础设施的互联网威胁防护投资。

解决方案： DHS 选择 Cloudflare 和埃森哲联邦服务公司（Accenture Federal Services）开发一种联合解决方案，以过滤到恶意和有风险目的地的 DNS 查询。这个解决方案将在各联邦机构使用。

媒体与广告

情景： 某媒体集团（全球收入超过 100 亿美元，员工超过 10 万）面临针对内部基础设施的网络攻击，包括一封勒索信。

解决方案： Cloudflare 使用基于身份的 Zero Trust 规则保护数百个网络和非网络应用程序。该公司在三个月内为 5 万员工提供保护，并计划在 9 个月内扩大到所有员工。

能源

情景： 某《财富》500 强天然气供应商寻求为其分布式数据中心和 1500 多名员工加强保护，以应对针对该行业的日益增长的网络威胁。

解决方案： 该公司选择 Cloudflare 来取代 Zscaler，理由是在保护应用程序和互联网访问方面具备更佳的可靠性和一致性，同时长期内更容易采用集成远程浏览器隔离的高级控制。

客户感言

> *Cloudflare 是我们 Zero Trust 之旅的力量倍增器。*
>
> **John McLeod**
> **首席信息官**
> **National Oilwell Varco**

> *Cloudflare Access 让 Ziff Media Group 能够无缝、安全地向员工交付我们的内部工具套件，无需复杂的网络配置，他们就能从全球任何地方通过任何设备使用这些工具。*
>
> **Josh Butts**
> **高级副总裁，产品与技术**
> **Ziff Media Group**

> *通过 Cloudflare，我们得以减少了对 VPN 和 IP 允许列表的依赖。*
>
> **Alexandre Papadopoulos**
> **网络安全总监**
> **INSEAD**

数字原生企业远程办公优先的劳动力队伍

数字原生企业：优先考虑敏捷安全以支持远程办公的灵活性

挑战：扩展和自动化云安全

许多组织都开始接受远程优先招聘。它们往往是更年轻的早期云采用者，基础设施有限，业务模式基于安全、快速和可靠的数字服务。

实现随处办公的灵活性可能成为差异化因素，但要求在用户移动和依赖个人设备时同样灵活的安全工具。

机会：可组合的安全适合于扩展

由于需要弃用的传统 IT 设施较少，这些数字原生企业可以利用我们的互联网原生架构和部署灵活性，从而在其安全现代化中保持敏捷。

我们的可组合服务、API 优先设计和单面板管理易于启用并实现安全。我们全球网络的速度、规模和可靠性满足完全远程劳动力队伍的需求。

示范用例

B2B SaaS

情景： 澳大利亚平面设计平台 Canva（2021 年估值 4 亿美元）在疫情大流行前部署了 Cloudflare，以优化第三方用户访问并避免实施 VPN 的麻烦。

解决方案： 随着时间的推移，Canva 在其不断增长的员工队伍中推出了 Zero Trust 应用程序访问策略，并扩展了互联网过滤和检查。

金融科技与区块链

情景： BlockFi 是一家由区块链技术驱动的 D 系列财富管理平台，随着其管理的资产不断增长和远程优先的劳动力队伍面临网络威胁，该公司需要提高安全性。

解决方案： Cloudflare 使 BlockFi 能够过渡到基于身份的应用程序访问认证，远离耗时的基于 IP 的控制。

社交媒体

情景： 某全球社交媒体平台遭遇了一次利用其内部应用访问和 VPN 配置的高调入侵。

解决方案： 作为回应，该公司决定全面改革其远程访问方式，为 1.3 万名员工和承包商采用 Cloudflare 的 Zero Trust 网络访问(ZTNA)解决方案，并退役其 VPN 部署。

电子商务

情景： 某全球电子商务平台（40 亿+美元收入，1.5 万员工）寻求为远程用户在网外浏览互联网和访问敏感的 SaaS 应用程序时提供更好的保护。

解决方案： 该公司部署了 Cloudflare，叠加 DNS 过滤等威胁保护功能，同时提供对 SaaS 应用程序使用情况的增强可见性。

客户感言

> *Delivery Hero 始终致力于为客户提供卓越的体验。Cloudflare Access 帮助我们让内部团队享受同样的体验：在全球范围内为他们提供安全的工作环境，并以一种简单的方式构建快速、可靠和尊重隐私的应用程序。*

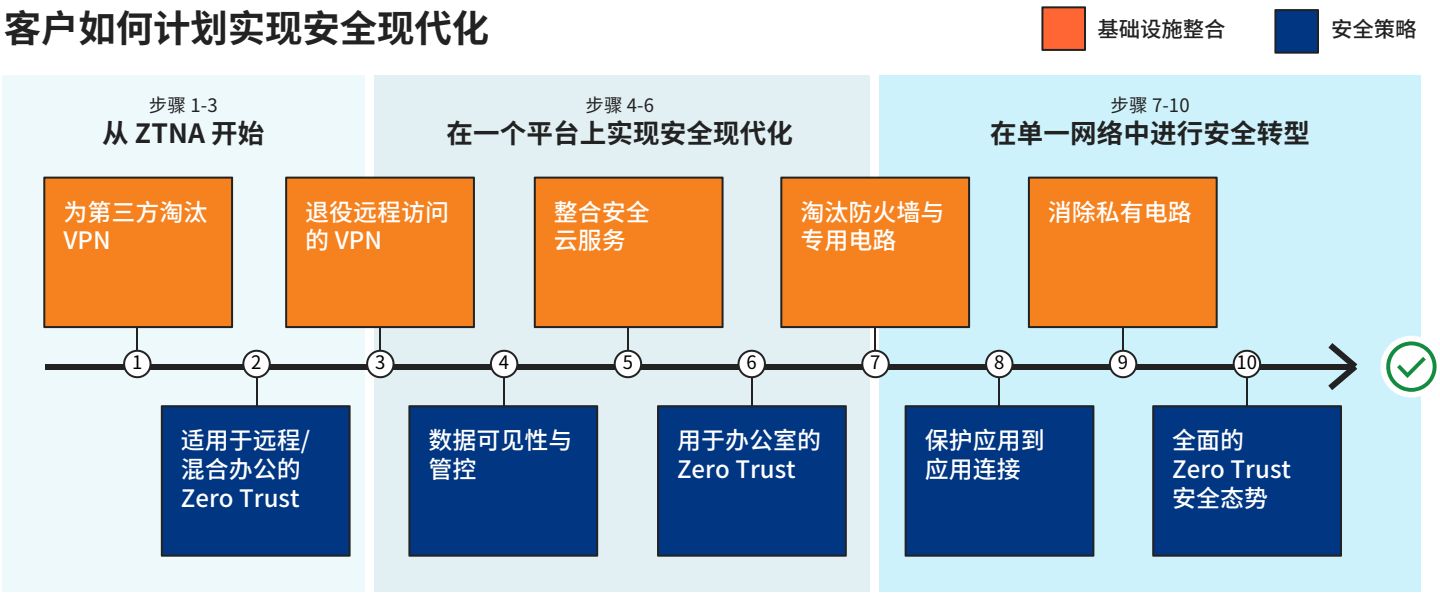
Christina von Hardenberg
首席技术官，Delivery Hero

> *Cloudflare 对于保护我们快速增长的远程员工至关重要。对应用程序访问采用 Zero Trust 为我们的管理员提供了增强的可见性和细粒度控制，这是以往的传统工具无法实现的。*

Marccio Alcaide
IT 安全主管，Facily

混合办公路线图

客户如何计划实现安全现代化



安全现代化路线图

上面的路线图说明了我们看到组织在现代化其安全性以适应混合办公时所采取的方法。这个路线图有两个主要目标：

1) **第一行（橙色）：** 将连接性和安全性基础设施从独立产品和硬件整合到一个云原生平台。
2) **第二行（蓝色）：** 为了获得可见性和控制，在任何位置、使用任何设备的用户和资源之间采用 Zero Trust 安全。

阶段 1-5：保护应用和互联网访问

对许多组织而言，采用混合办公首先意味着使劳动力队伍访问公司资源的方式现代化。

阶段 1： 这些组织的第一步是开始卸载 VPN 流量，并将特定用户（如承包商、开发人员、合作伙伴或新收购的团队）过渡到互联网原生的控制。Cloudflare 使得通过浏览器访问自托管应用程序变得特别容易，而不需要在端点上部署任何软件。

阶段 2： 这种现代工具支持基于角色、MFA 和硬件密钥要求、身份和设备态势构建针对每个应用程序的策略所需的可见性。

阶段 3： 随着团队对这种方法建立起信心，他们开始完全放弃 VPN，并使用 Zero Trust 保护非 Web 的传统专用网络。

阶段 4： 随后重点转向改善 SaaS 应用的可见性和管控，包括缓解影子 IT、管理租户和防止数据泄露。

阶段 5： 随着内部和 SaaS 应用程序现在受到单一平台管理，企业希望扩大对出站互联网访问的控制，并整合威胁防护工具，如 DNS 过滤器和安全 Web 网关。

阶段 6-10：将连接转移到云

路线图的余下阶段在大多数组织的规划中，但它们的愿望是将所有的网络连接和安全转移到一个统一的云网络上。

阶段 6： 在这个阶段，组织寻求将一致的 Zero Trust 扩展到任何网络位置，如总部、分支机构、数据中心和卫星办公室，以支持混合工作。

阶段 7： 随着越来越多的办公室流量被发送到 Cloudflare 以确保安全，企业可以逐步淘汰传统的本地防火墙和其他专用网络设备。

阶段 8： 这些高级用例的重点是确保跨混合多云环境的应用程序到应用程序的连接，这为网络基础设施团队在**阶段 9** 终止电信 MPLS 合同做好准备。

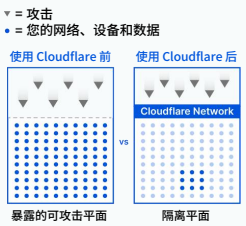
阶段 10： 尽管现代化永远不会真正结束，但我们期望 Zero Trust 现已扩展到所有用户、设备、数据、应用程序和环境。

商业和安全成果

Zero Trust 为企业节省时间与金钱的五种方法

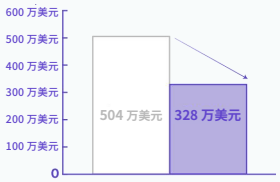
减少攻击面

91%↓



减少入侵成本

35%↓



加快速度员工入职

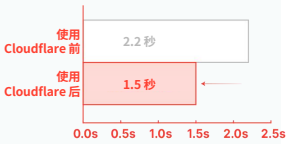
60%↑

减少IT 工单负担

80%↓

减少用户延迟

39%↓



其他商业驱动因素

释放员工生产力

管理员

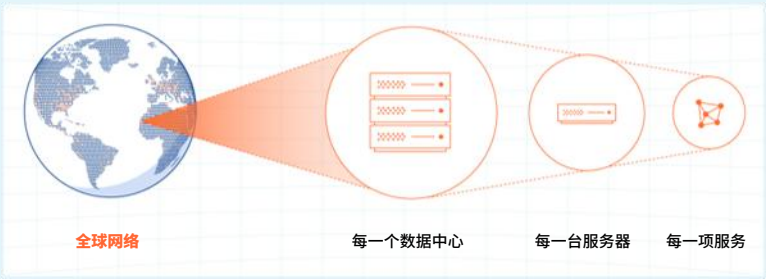
- 通过单一的管理接口简化配置，设置跨应用程序和互联网访问的策略
- 从同一管理界面配置与身份提供商、端点保护、云提供商和网络接入的所有集成

最终用户

- 无摩擦的身份验证和原生浏览体验，安全不会造成问题

降低传统服务的成本

- 更换或增强企业虚拟专用网络（VPN）设备，采用 Zero Trust 网络访问（ZTNA）
- 从本地 Web 代理或防火墙过渡到云原生的 L3-L7 安全服务
- 使用远程浏览器隔离（RBI）将用例从虚拟桌面基础设施转移出来
- 用现代云电子邮件安全取代传统的安全邮件网关



提供一致的速度和规模，保护所有远程和办公室用户

所有安全、性能和可靠性功能都设计为运行于 Cloudflare 现已遍布全球 275+ 城市的每一个数据中心的每一台服务器上。

加速您的 Zero Trust 路线图

马上试试吧

联系我们

010 8524 1783 | enterprise@cloudflare.com | www.cloudflare.com

REV: PMM-2022JJUL

[1] *支持混合工作的最主要网络实践（Top Network Practices to Support Hybrid Work）*，Gartner，作者：Karen Brown、Andrew Lerner 和 Mike Toussaint，04/08/2022
[2] *2022 年 SASE 融合战略路线图（Strategic Roadmap for SASE Convergence）*，Gartner，作者：Neil MacDonald、Andrew Lerner 和 John Watts，06/24/2022