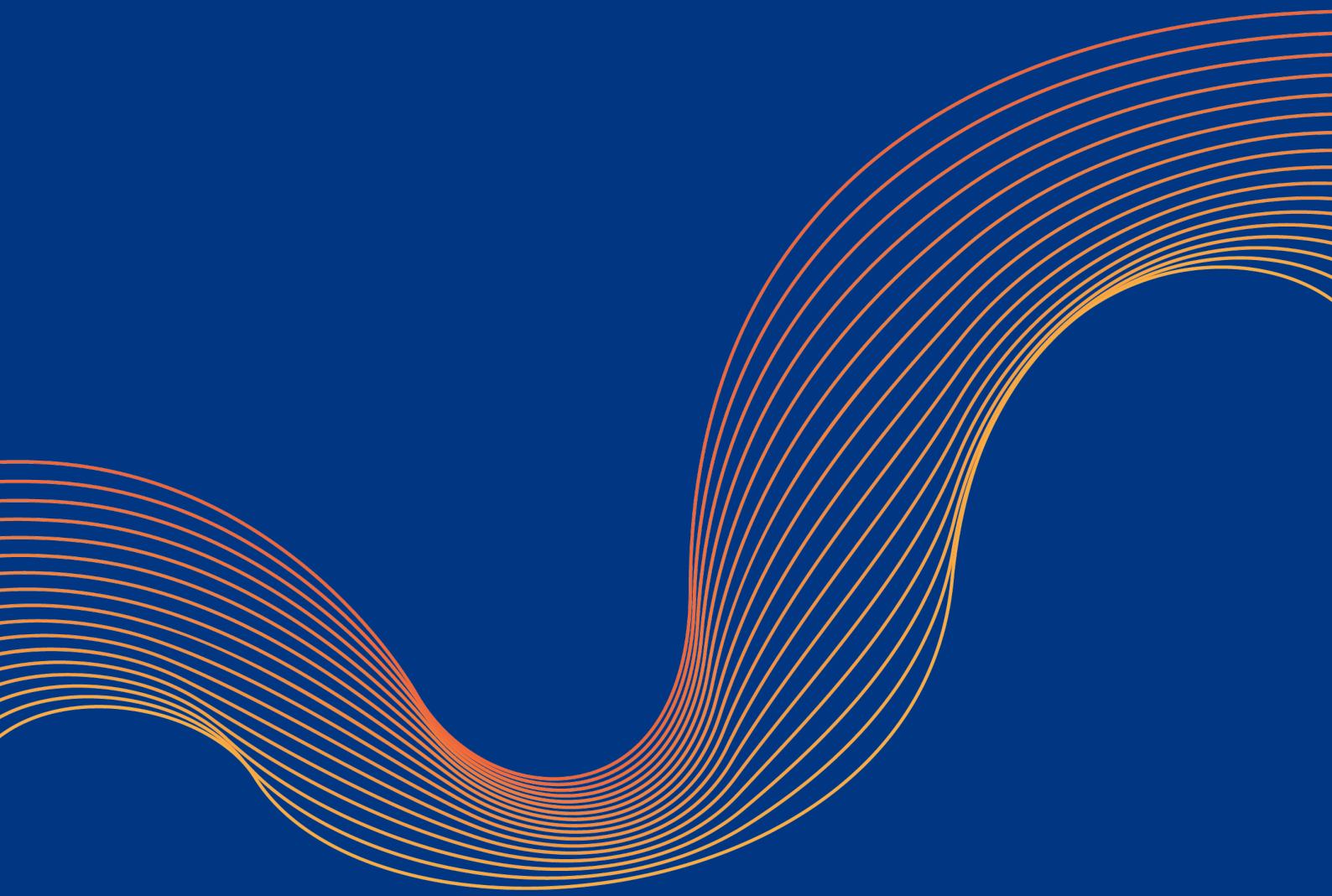
白皮书

CLOUDFLARE

ZTNA 能取代您的 VPN 吗？三种远程访问方式的比较



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

索引

简介1

安全、无缝的远程访问是业务助推器——可提高远程用户的工作效率，减少 IT 团队花费在员工入职上的时间，并敏捷、灵活地维护用户到应用程序的连接。尽管如此，远程访问对很多组织而言依然不是易事。

曾几何时，VPN 提供了将少数远程用户短时间内连接到企业网络的简单方法。然而，随着员工变得更加分散，组织需要在更长时间内维持远程用户的安全连接——这种方法的缺陷变得明显起来，性能缓慢，安全风险增加，还带来了可扩展性问题。

随着远程访问需求增加，组织日益从传统的 VPN 转向更安全、性能更佳的远程访问解决方案。Zero Trust 网络访问（ZTNA）在特定的应用程序、私有 IP 和主机名周围创建安全边界，将默认允许的 VPN 连接替换为默认拒绝、根据身份和上下文授予访问权限的策略。

2020年，约 5% 的远程访问主要使用 ZTNA 服务。由于传统 VPN 访问的局限性，加上需要提供更精确的访问和会话控制，到2024年，这一数字预计将跃升至 40%。[1]

相比 VPN，ZTNA 为企业提供了若干显而易见的优势，以及扩展的功能，但很多组织发现它无法完全取代 VPN 基础设施。但随着 ZTNA 变得更健壮，而 VPN 问题越来越多，这种情况正迅速改变。本文对 VPN 和 ZTNA 远程访问解决方案进行对比，说明各自的优点和局限性，以及迁移项目最重要的考虑因素。本文解释 Cloudflare 如何提供 ZTNA，并推荐一整套操作步骤，为远程用户从传统 VPN 基础设施过渡到更快、更安全的 Zero Trust 连接。

[1] Riley, Steve, MacDonald, Neil, and Orans, Lawrence. 《Zero Trust 网络访问市场南》（“Market Guide for Zero Trust Network Access.”）Gartner Research, https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access. 2021 年 6 月 21 日访问。详情参见表 1。

方式 #1：传统 VPN

数十年来，VPN 帮助组织将远程用户连接到企业网络，提供一定程度的隐私和安全保护。VPN 允许用户通过加密连接安全地访问内部资源，而非在公共互联网上访问敏感信息，以防攻击者窥探或盗窃数据。

VPN 实施的两个最常见模式是基于客户端的 VPN 和无客户端的 SSL-VPN。每种都有其自身的优点和挑战：

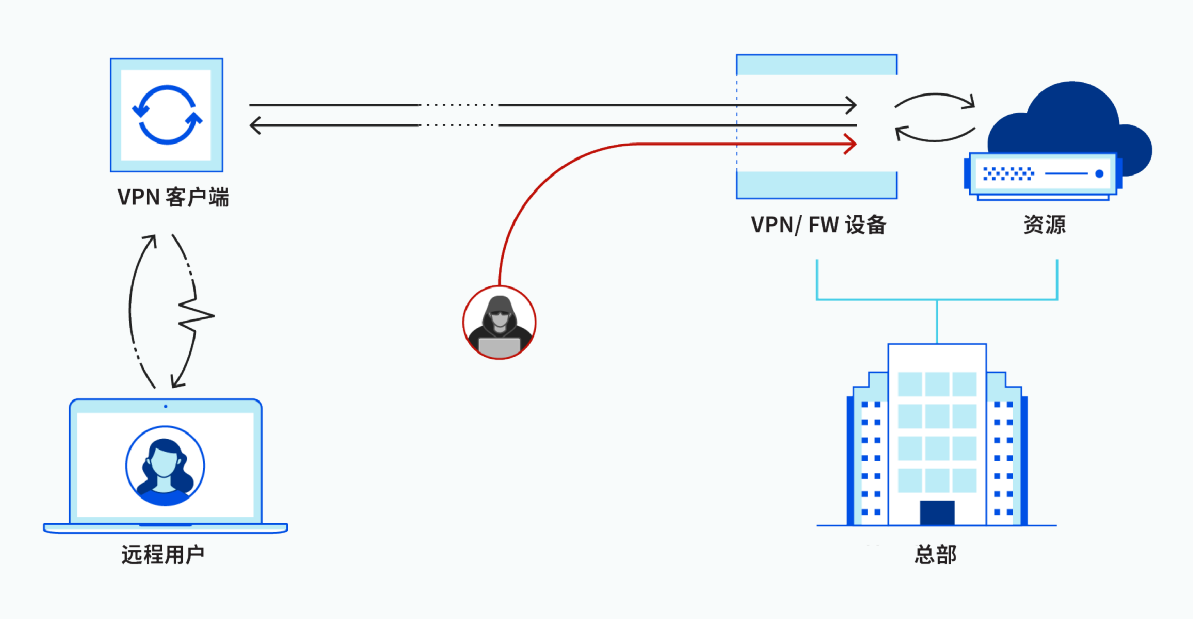
基于客户端的 VPN 通过加密隧道将远程用户连接到一个专用网络。这个连接是通过软件应用程序（即客户端）建立的，后者要求用户使用用户名和密码进行一次验证，以获得对该网络中任何资源的持久访问权限。	**优点：**一旦连接，用户就能自由横向移动，通过访问应用程序和连接到内部主机来迅速访问多个资源。 **挑战：** • **非为漫游用户和移动设备设计。**在用户四处漫游时，随着无线网络从一个地点更换到另一个地点，其笔记本电脑和移动设备会无缝重连。然而，VPN 客户端并不擅长流畅地处理重新连接，要求用户反复强制客户端重启和重新验证——导致工作效率下降和产生 IT 支持需求。 • **可见性低。**使用这种方法时，VPN 基础设施在数据中心内部防火墙后的 VPN 客户端终止加密隧道。尽管这些连接被记录到日志中，但没有特定于应用程序的集中式日志来揭示用户访问了哪些应用程序，或他们在应用程序内进行了什么操作。

无客户端 SSL-VPN 门户允许少数远程用户连接到专用网络内的少数基于浏览器的应用程序。这个连接是通过使用运行 VPN 服务的网络设备内置的 web 服务器来建立的。

优点： 无需使用设备上的客户端，任何 web 浏览器都可以使用门户的 SSL 证书来建立一个加密的 HTTPS 连接，以支持非受管设备上的承包商。

挑战：

- **安全问题。**数据中心中的大多 VPN 配置都向用户授予完全访问权，如果组织不希望非员工（例如承包商）获得对敏感资源和应用程序的无限制访问权限，这种方式就会造成问题。
- **不支持大量并发用户。**不同于现代云服务，该门户的 web 服务器不能弹性地扩展以满足更高需求。相反，必须安装更多网络设备以平衡负载来扩展门户，这种做法往往成本高昂、复杂且效果欠佳，因为这些设备的其他功能有可能得不到充分利用。
- **无客户端的 SSL-VPN 门户将防火墙端口和 web 服务器暴露在攻击面前。**为了允许托管门户的 web 服务器访问内部应用程序，管理员必须打开传入防火墙端口，使其暴露在外部攻击面前。开放的端口和 web 服务器本身都必须受到保护，以防御 DDoS 和 web 应用程序攻击，这要求更复杂的配置和更高的成本，以保护这种链接方法。



虽然 VPN 为远程用户提供基本的隐私保护，但其设计并没有考虑安全性和可扩展性。传统上，组织使用 VPN 在短时间内将少数远程用户连接到企业网络。然而，随着远程办公越来越普遍，VPN 的问题开始成本增加：

- **用户体验到缓慢的性能。**如果 VPN 基础设施无法处理员工带来的流量和并发连接，用户就会体验到互联网连接变慢。此外，当 VPN 同时远离用户和他们试图访问的应用程序服务器时，所需的传输时间就会造成延迟。
- **企业网络易受攻击。**VPN 通常使用城堡加护城河模型，一旦连接到某个网络，用户就能获得对所有企业资源的无限制访问。由于没有内置的方法来限制对关键基础设施和数据的访问，组织被迫配置成本高昂、复杂的安全服务——例如下一代防火墙和网络访问控制——否则就会容易受到恶意横向移动的破坏，导致更大的数据泄露。

托管 VPN 服务的挑战

一些厂商将运行 VPN 服务的网络设备转移到公有云中，在一个或多个数据中心上作为虚拟机运行。这种 VPN 会或不会绑定（或菊式链接到）额外的安全服务。

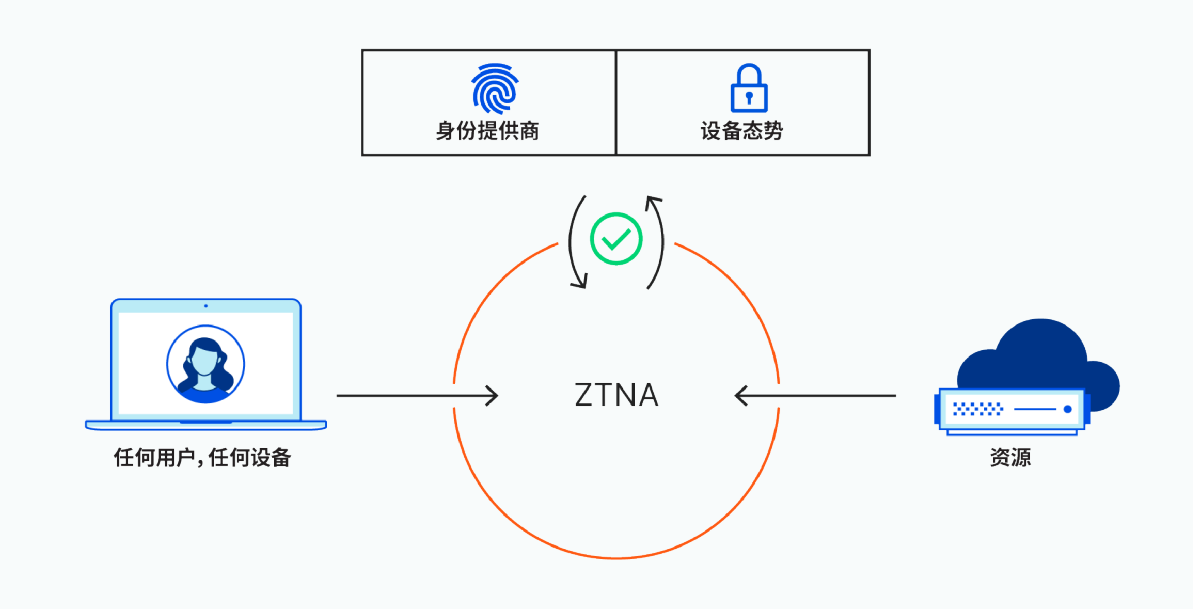
将 VPN 放到云端似乎一定程度上解决了硬件 VPN 设备固有的可扩展性问题。然而，这样做也带来一些重大的安全性和可扩展性挑战。

例如，假设某个组织托管一个完整的下一代防火墙（NGFW），将 VPN 与防火墙和额外安全功能结合在一起。由于下一代防火墙作为捆绑服务提供，无法按需独立扩展任何特定功能。扩展一项功能需要扩展整个服务；要做到这一点，就必须启动更多虚拟机来平衡每个虚拟机执行的少量计算。这种解决方案不切实际且难以处理，随着组织的访问需求继续扩大，还有可能造成高昂成本。

方式 #2：ZERO TRUST 网络访问

Zero Trust 安全规避了 VPN 固有的众多挑战。它基于这样一种原则：某个网络内部和外部的任何用户或设备默认都不能被信任。为了降低数据泄露、内部攻击和其他威胁的风险和影响，Zero Trust 方式……

- 验证、记录每一个登录和请求，
- 要求对所有用户和设备进行严格验证，
- 根据身份和上下文限制每个用户和设备能访问的信息，
- 增加端到端加密，以隔离网络中的应用程序和数据。



与 VPN 一样，有几种配置 ZTNA 的方法：

1. **无客户端（即服务启动的）ZTNA** 使用现有浏览器而非客户端来创建安全连接和验证用户设备。一直以来，无客户端 ZTNA 局限于使用 HTTP/HTTPS 协议的应用程序，但兼容性正在迅速发展。[2]
   - **优点：**无客户端 ZTNA 使用反向代理来防止对应用程序的直接访问，防止用户访问他们可能无权查看的应用程序或数据，在管理上为管理员提供更大的控制和灵活性。
2. **基于客户端的（即端点启动的）ZTNA** 在用户设备上安装软件，以便在控制代理和授权应用程序之间建立加密连接。
   - **优点：**客户端的 ZTNA 让管理员更深入地掌握访问应用程序的用户设备态势、位置和风险上下文，从而创建和实施更细粒度的策略。而且，由于这种方法不限于 HTTP/HTTPS，它可用于访问广泛的非 HTTP 应用程序 — 例如依赖于 SSH、RDP、VNC、SMB 和其他 TCP 连接者。

[2] 截至 2021 年 6 月，Cloudflare 的 ZTNA 支持对 SSH 和 VNC 应用程序的无客户端访问，并计划在日后支持 RDP。

ZTNA 实施的挑战

虽然 ZTNA 与传统 VPN 相比具备显著优势，它并非保护远程用户网络访问的完美方法。企业在权衡 Zero Trust 采用的利与弊时，有可能遇到如下一个或多个挑战：

解决方案并非真正云原生的。

如果某个供应商不提供基于云的 ZTNA——意味着其客户需要在其自己的数据中心部署软件——那么用户就会失去一些关键优势，例如即时扩展性和无限吞吐量。

厂商可能不提供基于客户端或无客户端 ZTNA 选项。

对于需要将用户连接到非 HTTP 应用程序（如远程桌面、SSH 应用程序或文件共享）的组织而言，价值受到了限制。

配置过程既复杂又耗时。

如果供应商不提供对策略编排和自动化（如通过 Terraform 等工具）的支持，那么除了对身份提供商已有的配置外，管理员还要执行更多手动工作。

CLOUDFLARE 的远程访问方式

保护和扩展远程访问应当是一个无缝的过程，无需叠加笨拙的安全解决方案，造成性能折衷，或产生不必要的成本。Cloudflare 使团队能够处理所有远程访问用例，具备如下优势：

- **用户和管理员上手简单、零风险。**Cloudflare 与原有身份提供商和端点保护平台轻松集成，实施 Zero Trust 策略，限制对企业应用程序和资源的访问。
- **客户端和无客户端 ZTNA 部署的灵活性。**Cloudflare 提供对 web、SSH、VNC、（以及即将推出的 RDP）应用程序的无客户端支持，对非 HTTP 应用程序的客户端支持和到内部 IP 的专用路由。

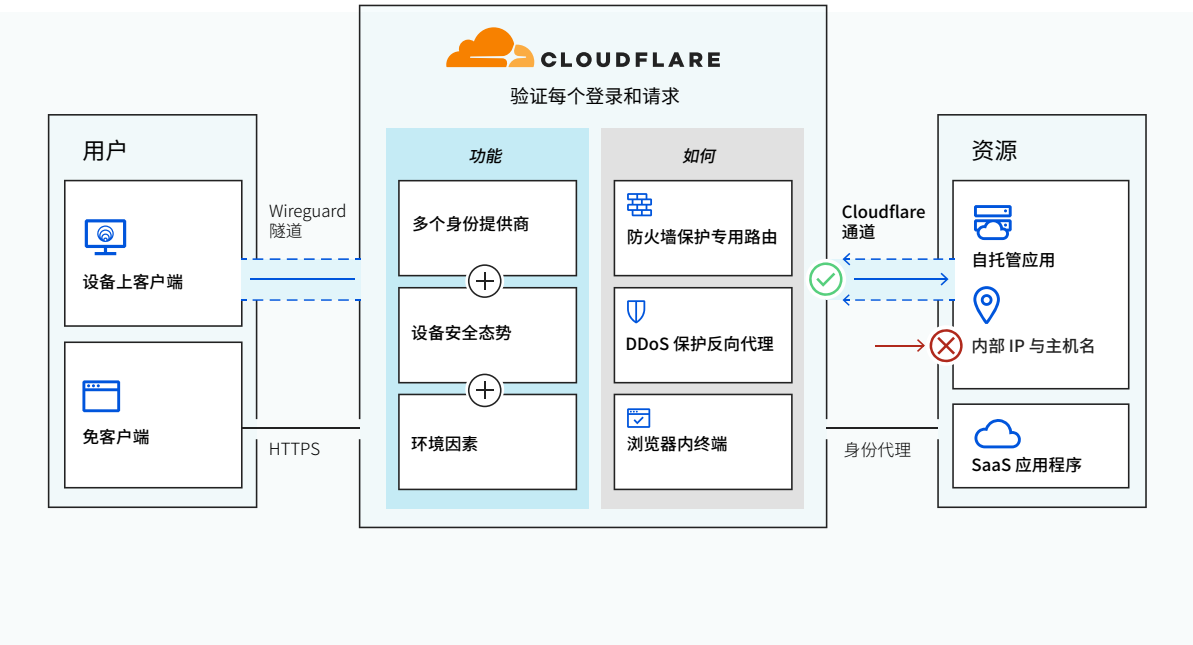


表 1：Cloudflare 如何解决远程访问挑战

⚠ 问题	✓ 解决方案	⚙ Cloudflare 实施
难以扩展	全球边缘网络	VPN 和 ZTNA 服务均存在可扩展性问题，使远程用户难以访问应用程序和数据。 Cloudflare 的全球 Anycast 网络不仅使用户连接比 VPN 更快，也确保任何大小的远程员工队伍都能根据需要安全、快速地连接到企业资源——无需管理员进行额外的耗时配置。
移动设备兼容性欠佳	轻量客户端	使用 IPSec 和 SSL 协议的 VPN 和 ZTNA 解决方案在移动或漫游设备上往往性能糟糕。 Cloudflare WARP 客户端使用更现代的 Wireguard 协议，在用户空间中运行，支持更广泛的操作系统，提供比传统选项更快的用户体验。Cloudflare 的 WARP 客户端可在 Windows、MacOS、iOS 和 Android 上配置，并即将支持 Linux 设备。
无集成 DDoS 防御或较弱	内置行业领先的 DDoS 防御	如果没有集成的 DDoS 防御，组织尝尝被迫串联额外安全服务，这会造成配置麻烦、可扩展性问题和安全挑战。 Cloudflare 容量高达 67+ Tbps 的网络为任何 ZTNA 模式提供内置 DDoS 保护，防御最大规模的容量耗尽型攻击。
协议限制	非 web 应用支持	✓ 模式兼容性：适用于 SSH/VNC 应用程序的无客户端 ZTNA；适用于所有其他非 web 应用程序的客户端 ZTNA
无集成网络防火墙	内置网络防火墙	随着企业网络发展，组织必须平衡的安全硬件堆栈数量也在增加——导致成本、性能和安全之间的权衡。 Cloudflare 让管理员能够在边缘实施网络防火墙规则，精细化地控制哪些数据能进出其网络，并改善对流量如何流经网络的可见性。 ✓ 模式兼容性：基于客户端的 ZTNA
缺乏细粒度控制	内置安全 web 网关（SWG）	未经批准使用应用程序可能会给组织带来重大的安全问题；如果实施没有严格的策略，用户可访问和篡改敏感数据和其他公司资源。 通过结合 ZTNA 和 SWG，Cloudflare 允许管理员对应用程序内的用户和设备访问权限进行更细粒度的管控，以便用户和基于角色的组仅能访问其所需的资源。 ✓ 模式兼容性：基于客户端的 ZTNA

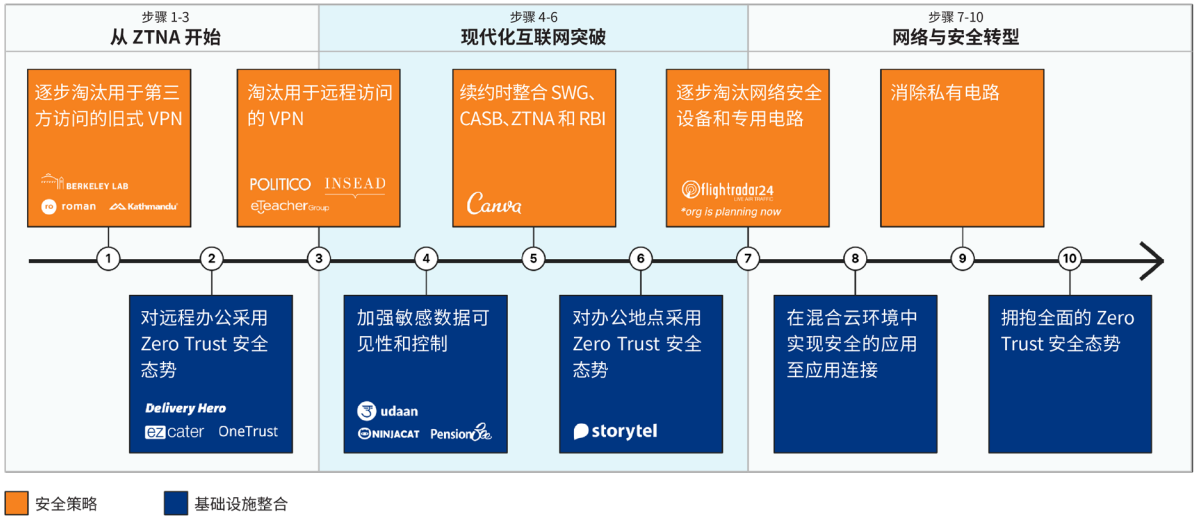
用 ZERO TRUST 网络访问取代您的传统 VPN

在向没有 VPN 的安全过渡这一漫长、痛苦的过程中，Zero Trust 的承诺对 IT 主管而言可能显得很空洞。然而，无需在协议支持或功能方面进行权衡，就有可能用 Zero Trust 网络访问替代您的 VPN。

根据驱动您项目的业务优先事项，推荐的迁移路径会存在差异：

- 如果您的优先考虑是更快的应用程序连接速度，那么应该首先部署**适用于非 web 应用程序的 ZTNA**。
- 如果增强应用程序访问规则的安全性更加重要，那么应当从**web 应用程序开始**。

替代您的 VPN 只是全面网络转型的第一步。由于过渡到 SASE 模型可能非常困难，根据客户所采取的方法，我们拆分出一条实现 Zero Trust 安全的通用路径：



进一步了解 Cloudflare 的Zero Trust 能如何帮助您降低对 VPN 的依赖并最终取而代之。

了解更多

查看 VPN 与 ZTNA 在现实世界中的比较，以及Cloudflare Access 如何增强应用程序访问的安全性。

观看演示

附录

现代化您的互联网突破

实施 ZTNA 是部署安全访问服务边缘（SASE）模型的重要一步。**Cloudflare One** 是综合性的网络即服务（NaaS）解决方案，它为各种规模的团队简化和保护企业网络。通过 Cloudflare One，组织能够：

- **拥抱 Zero Trust 访问。**将宽泛的安全边界替换为对每个资源的每个请求进行一对一验证。对企业应用程序的每个连接执行 Zero Trust 规则，无论用户是谁和在哪里。
- **保护互联网流量。**当互联网上的威胁快速行动时，您的防御措施也需要更加主动。Cloudflare One 保护远程员工免受互联网威胁侵害，通过在任何站点实施 Zero Trust 浏览器隔离，执行各种策略来防止宝贵的数据从组织中泄露出去，并提供流畅、快速的用户体验。
- **保护并连接办公室和数据中心**企业网络变得过度复杂，意味着用户流量往往需要经过多个跃点才能到达目的地。通过 Cloudflare One，企业能利用一个一致、统一的云平台来保护办公室和数据中心。

若要进一步了解 Cloudflare One，请观看这个时长 10 分钟的介绍和演示短片。

改造您的网络

不久后，Cloudflare 的 Zero Trust 和 WAN 即服务产品就会合二而一，使您的员工无论身在何处，都能以一致的方式访问企业资源。

今天，您的 VPN 和 WAN 产品让您的员工能访问位于私有企业网络内的资源，但它们迫使您以不同的方式来管理连接和安全策略。

现在，Cloudflare 提供一个统一的控制面，为您提供更大的灵活性，对您的整个员工队伍和工作场所应用相同的 Zero Trust 安全策略，无需切换多个独立产品。

若要了解详情，请访问 https://www.cloudflare.com/cloudflare-one/。

文档类型