Zero Trust 网络访问

Cloudflare Zero Trust，具体而言是 Access，让所有用户无需使用 VPN 即可访问企业的自托管、SaaS 或非 Web 应用，从而提高团队生产力并降低风险。

为混合办公提供简单、安全的访问

互联网原生的 Zero Trust 网络访问 (ZTNA)
今天的分布式办公环境要求分布式的安全方法。“边界”不再存在，传统的远程访问解决方案（如 VPN）无法满足现代的安全性和性能期望。

ZTNA 持续检查基于每个资源的细粒度上下文信息（例如身份和设备态势），简化和保护任何用户对任何应用的访问，无论使用什么设备，无论身处何地。使用一种全新的方法，无需在安全性和用户体验之间“权衡取舍”。ZTNA 同时提升两者，让企业如虎添翼。

它还使组织更加敏捷，能够更好地应对变化，无论是进行云迁移、并购活动，还是快速创新和扩展。Cloudflare 是一个 Zero Trust 或安全现代化战略的核心，通过我们可编程的全球连通云交付 ZTNA。

80% 使用 VPN 相关的远程访问支持工单解决时间平均减少 80%[1]

72% 相比以前的供应商，每月策略配置时间减少 72%[1]

68% 68% 用户发现简化员工和承包商的身份验证体验产生重大影响[1]

为您的企业提供现代访问方式

增强用户体验

利用现代化安全工具，让本地应用程序使用起来就像 SaaS 应用程序一样，从而提高团队生产力。不再依赖缓慢、笨重的 VPN，不再有员工抱怨。

杜绝横向移动

为每种资源授予基于上下文的最低特权访问，而非网络级访问权限，从而降低网络风险，缩小攻击面。

轻松扩展 Zero Trust

通过保护关键应用程序或最高风险的用户群来改善技术效率，然后扩展互联网原生的 ZTNA 以保护整体业务。

Access 主要用例

安全混合办公

- ★ **VPN 增强与替代** — 访问比传统 VPN 更快、更安全。开始卸载关键应用，以提升安全性和最终用户体验。
- ★ **承包商访问** — 通过无客户端选项、社交 IdP 等方式验证第三方用户的身份。
- **开发人员访问** — 让特权技术用户安全访问关键基础设施，而无需牺牲性能。

支持数字现代化

- **加速并购** — 完全避免传统的网络合并。集成多个 IdP 的访问，在并购过程中提供基于应用的内部访问。
- **云迁移** — 确保在应用或身份目录迁移到云端之类的转型期间维持业务连续性。
- **防钓鱼的 MFA** — 在每一个地方推出强身份验证，例如符合 FIDO2 标准的安全密钥。

开始进行 VPN 增强和替代

对于增强 VPN 的 ZTNA 试点，优先考虑关键应用或高风险的用户。使用无客户端方式访问 Web 应用或基于浏览器的 SSH，以便加快测试。随着时间的推移，采用高级功能来全面替代 VPN，并在网络变化时维持动态可见性。

开始使用承包商（第三方）访问

提供流畅的用户体验，同时减轻来自非受管设备的风险。为承包商配置简单的身份验证选项 —— 无需安装最终用户软件。随着时间的推移，采用高级功能来应用更进一步的数据保护。

** 使用 Zero Trust 平台其他部分的功能*

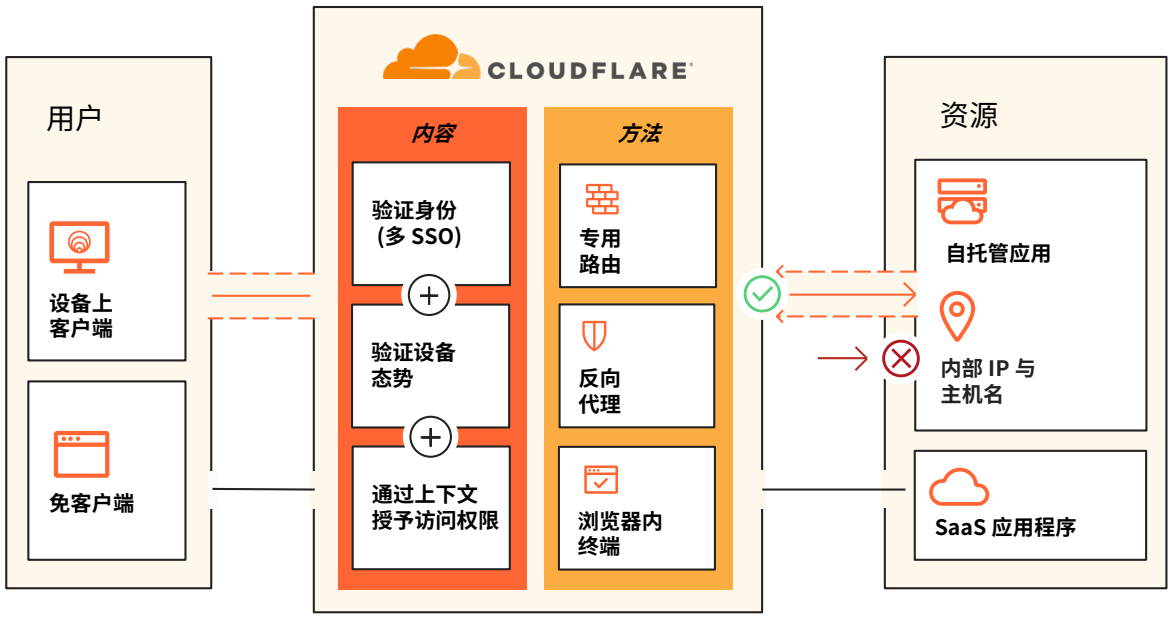
Access 的工作方式

Cloudflare Access 是一个灵活的聚合层，它可以不断地验证细粒度上下文，例如身份和设备态势，提供针对组织所有资源的简单、安全的访问，创建一个软件定义的边界。当用户进行身份验证并满足所有访问策略条件时，Access 会发放一个经过签名的 JSON Web Token，在特定会话期间有效。所有用户请求通过我们的可组合平台时，我们将执行一次性检查；凭借我们独特的 Anycast 网络架构，我们的集中式策略管理体验可在数秒内将策略更改传播到全球。

无客户端和客户端双管齐下，可处理所有设备类型。所有 Zero Trust 服务使用单一设备客户端，加密到达我们网络的流量，维持客户数据的隐私。我们还通过我们的无客户端设置为企业外部的设备提供简单、安全的访问。我们的 ZTNA、DNS、以及市场领先的 WAF 和 DDoS 保护服务协同工作，创建和保护公共主机名，以便第三方用户和混合办公人员通过任何设备访问。我们的无用户身份验证选项（令牌或 mTLS 证书）还可以解决自动化服务和物联网设备用例。

对于 Zero Trust 控制，资源使用公共主机名作为反向代理，以访问自托管应用程序（云端/本地）或基于浏览器的 SSH/VNC，使用身份代理访问 SaaS 应用，或者使用基于客户端/隧道的专用路由通过 L4-7 前向代理以访问专用子网内的任何 Web 或非 Web （例如任意 TCP/UDP）资源。我们的全球网络和应用连接器软件相结合，可支持任何计算环境，包括公共云（包括 Kubernetes 和容器）或传统的本地网络资源，无需虚拟机基础设施，也没有类似其他 Zero Trust 供应商的吞吐量限制。

第三方身份、端点、网络入口、日志/分析和 SIEM 工具集成到我们的仪表板中，还提供我们设备客户端的原生选项和分析，让管理员能够保持敏捷，利用已经使用的工具进行构建。



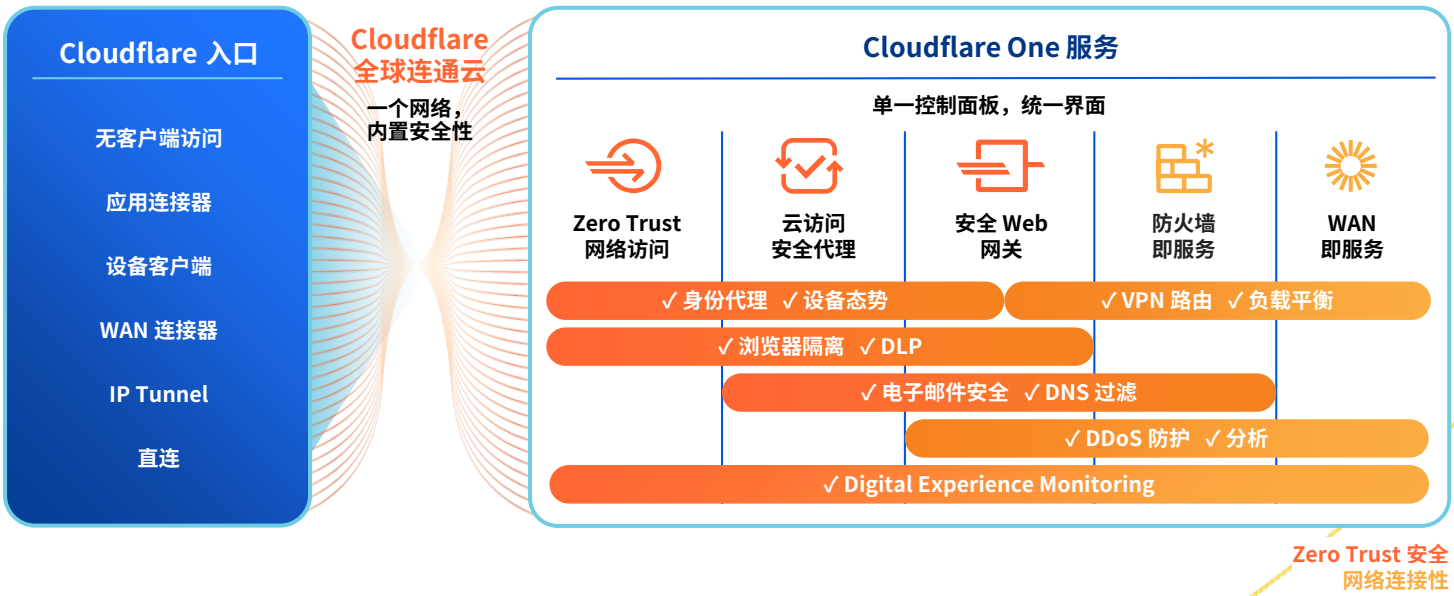
Access 是 Cloudflare SSE 和 SASE 平台的一部分

虽然 SSE 和 SASE 往往是一个多年的战略过程，但 Cloudflare 经常看到组织从 ZTNA 开始，因为它为 IT 团队提供了可操作和可实现的步骤，同时展示显著的短期业务价值。IT 领导者寻求在整合过程中保护混合办公、抵御威胁并保障数据安全，并越来越多地选择 Cloudflare 作为他们值得信赖的合作伙伴。

Cloudflare 的部署灵活性和可组合架构使任何组织都能够保护和加速设备、应用和整个网络的性能，以保持混合办公的安全性和生产力。为此，我们支持最终用户的无代理接入，无客户端 Web 隔离以限制不安全的流量，并使用统一的管理仪表板，以便查看所有安全和网络服务，无论管理员或用户从何处连接。Cloudflare 全球网络的广度使安全措施在更接近最终用户的位置之星，最大限度地减少延迟，并提供流畅的员工体验。我们的 Anycast 架构有助于绕过互联网中断，让团队保持在线并帮助确保业务连续性。

通过我们统一的 SSE 和 SASE 平台，ZTNA、CASB、DLP 和 SWG 策略之间共享的上下文有助于增强安全态势，并通过一致的管理员工作流程简化实施。相同的身份和设备态势属性为 ZTNA 和 CASB 访问策略以及 SWG 策略提供信息，从而简化跨组织的策略管理。

ZTNA、RBI 和电子邮件安全也可以一起使用，以便为用户提供对资源的有条件访问，同时将用户与电子邮件和协作工具中的恶意内容（链接、附件）隔离开来。为承包商和使用非受管设备的用户提供对企业资源的有限访问权限，并禁用用户交互（例如上传/下载、复制/粘贴、键盘输入）以防止数据泄露，并可应用其他 L7 DLP 策略来检测敏感数据。



客户感言

“Cloudflare Access 是传统 VPN 的绝佳替代方案。用户只需打开浏览器并登录，无需下载和配置任何额外软件。”

— **Platzi**，云工程主管

“在限制对内部资源的访问方面，Access 比 VPN 简单得多，也更安全。我们只需激活它并添加用户。它就能工作了。”

— **Bitpanda**，联合创始人兼 CTO

“Cloudflare Access 及时到位，让我们避免了部署 VPN 的麻烦。这对我们来说是一个容易的选择，而且它的部署非常简单。”

— **ezCater**，安全主管

“在使用 Cloudflare 之前，安全部署一个应用需要进行为期两到四周的准备工作。利用 Cloudflare Zero Trust，我们将以上时间缩短了接近 90%。”

— **Creditas**，网络工程团队主管

分析师评价

Cloudflare 被 2023 年 IDC MarketScape Zero Trust 网络访问报告评为 “领导者”

IDC 指出 Cloudflare 以“积极进取的产品战略来支持企业安全需求。”我们相信，这一认可证实了我们的方法，即帮助任何规模的企业开始采用 Zero Trust，保护任何用户安全对任何资源的访问，无需 VPN。

Cloudflare 被 2022 年 KuppingerCole ZTNA 领导力指南针评为“领导者”

KuppingerCole Analysts AG 的 2022 年度 ZTNA 市场分析列举了 Cloudflare 的数项优势，例如：全面集成、有机开发的安全和访问管理平台，最大的全球云基础设施，以及庞大的市场份额。

Access 的功能

创建/编辑 Zero Trust 以实现安全访问	
细粒度、自定义的访问策略	集中式策略管理体验。L7 应用在子域和路径级别受到保护，支持通配符和多主机名，并支持 CORS 请求。策略变化数秒即可传播到全球。包括策略测试器。
资源广度： 我们可保护什么，如何保护	资源使用公共主机名作为反向代理，以访问自托管应用（云端/本地）或基于浏览器的 SSH/VNC，使用身份代理访问 SaaS 应用，或者使用基于客户端/隧道的专用路由通过 L4-7 前向代理*以访问专用子网内的任何 Web 或非 Web （例如任意 TCP/UDP）资源。
身份	通过所有主流企业和社交 身份提供商 (IdPs)进行身份验证，包括同时使用多个 IdP。也可使用 SAML 和 OIDC 连接器。支持（并可执行）任何 IdP 提供的 AuthN 方法、 临时 AuthN、 目的证明、全局或每个应用会话的 re-AuthN 间隔，以及每个应用或每个用户的即时会话撤销选项。
设备态势	使用设备客户端和第三方端点保护平台(EPP)集成验证 设备态势。使用服务对服务集成拉取 EPP 风险评分到 Zero Trust 策略中。
用于策略的上下文信号	配置各种信号，例如电子邮件群组，IP 范围，地理位置，登录方法(例如，MFA 类型，IdP 类型)，有效的 mTLS 或 SSH 证书，服务令牌，序列号列表，设备态势属性，设备客户端安装，会话持续时间，SWG 规则实施或来自外部 API 调用的信号。也可直接引用 Microsoft Entra ID (Azure AD) 有条件访问策略。
其他相关支持	• **SCIM：** 为自托管和 SaaS 应用自动配置/移除用户（ Okta 和 Azure AD 的示例） • **内部 DNS：** 配置本地域回退并解析专用网络请求 • **拆分隧道：** 包括/排除用于专用网络或 VPN 运行的 IP • **mTLS 身份验证：** 基于证书的身份验证，针对对物联网和其他 mTLS 用例 • **应用隔离：** 勾选单选框，即可将应用隔离在我们超低延迟的远程浏览器中*
网络	
应用连接器	简单编排我们的轻量级应用连接器 (Cloudflare Tunnel) 即可加快资源接入 Cloudflare 的速度，无需使用虚拟机基础设施，也没有吞吐量限制。包括监控、 虚拟网络 （用于 IP 重叠）及冗余和故障转移能力。
设备客户端： 何时使用	• **无客户端：** 将 Zero Trust 策略扩展到非受管设备上的第三方用户；也可与无客户端 RBI 和 L7 DLP 策略很好地搭配使用*。无客户端访问支持 Web 应用和基于浏览器的 SSH/VNC。 • **客户端：** 我们的设备客户端 (Cloudflare WARP) 将安全访问扩展到专用网络，支付服务对服务的设备姿态集成，具有位置感知能力，可为本地用户应用量身定制的策略。还可以连接任何两个或更多运行 WARP 的设备，以创建专用网络。用户可自行注册或通过 MDM 部署。
可扩展性和可见性	
页面自定义	上传自定义 HTML 块和应用启动屏幕，以适应您的品牌或传达特定的访问说明，从而优化最终用户体验。
日志记录	全面记录所有请求、用户和设备的日志。可使用 logpush 或 API 与现有的 SIEM、编排和分析工具集成。对于未知资产，我们用于内部基础设施的影子 IT 发现被动编目来自所有源的独特流量。
自动化	直观的 API 和 Terraform 提供商用于以编程方式管理 Zero Trust 实现的所有方面。也提供无用户的服务令牌以支持自动化服务。

** 使用 Zero Trust 平台其他部分的功能*

为什么选择 Cloudflare?

易于设置和管理

通过应用连接器软件和隧道编排，从根本上简化私有资源入口流量的设置和操作。

无缝连接，永远在线

利用 Cloudflare 的全球 Anycast 技术实现最终用户的峰值性能，有足够的韧性来应对网络中断，确保网络稳健可靠。

早期采用者的快速创新

携手积极创新、超越同行的 Zero Trust 提供商，跟上互联网自身的发展步伐，使应用访问更快、更安全。

让我们讨论一下如何为您的组织实现安全、简单的访问

申请研讨会

CLOUDFLARE

还未准备好进行实时对话?

进一步了解 **Cloudflare 的 SSE & SASE 平台**

1. 2023 年调查： techvalidate.com/product-research/cloudflare/charts