CLOUDFLARE

产品简介

Cloudflare 浏览器隔离
互联网的内置 Zero Trust

将 Zero Trust 扩展到互联网

攻击面很大，控制措施有限

如今，Web 浏览器是使用最广泛的企业应用程序，它代表了很大的攻击面。

然而一直以来，保护用户免受基于浏览器的威胁的举措都不够理想。而且，应用控制措施来保护用户与敏感数据的交互方式也更加困难。

完善 Zero Trust

在浏览中应用 Zero Trust 是指默认不信任设备上运行的任何代码或交互。

Cloudflare 浏览器隔离在边缘运行所有代码 — 将用户与不受信任的 Web 内容隔离，防止不受信任的用户和设备访问浏览器交互中的数据。

不再使用您的普通远程浏览器

- 兼容性原生适用于任何浏览器中的任何网页。
- 性能以低延迟方式传输网页数据流。

保护使用中的数据，避免不可信用户和设备访问，并保护设备和用户免受勒索软件和网络钓鱼甚至是零日攻击。

立即试用，无需安装

内置而非附加的安全性

在 Cloudflare 上构建

我们的浏览器隔离是借助我们网络上的其他 Zero Trust 服务从零开始搭建起来的，专为在超过 275 个地点运行而设计。

Web 浏览会话会在尽可能靠近用户的地方提供，确保闪电般快速的体验。

原生集成

与其他提供商不同，Cloudflare 通过本地集成的浏览器隔离提供我们所有的 Zero Trust 服务。

将统一管理界面用于：

- 安全 web 网关（SWG）
- 零信任网络访问（ZTNA）
- 云访问安全代理 (CASB)
- 云电子邮件安全（在路线图上）
- ……还有更多

缩小攻击面
Zero Trust 浏览可以阻止未分类、有风险甚至低风险网站上的恶意代码感染用户的设备。

简化部署
可在管理应用程序访问的相同地方设置 Zero Trust 浏览策略。

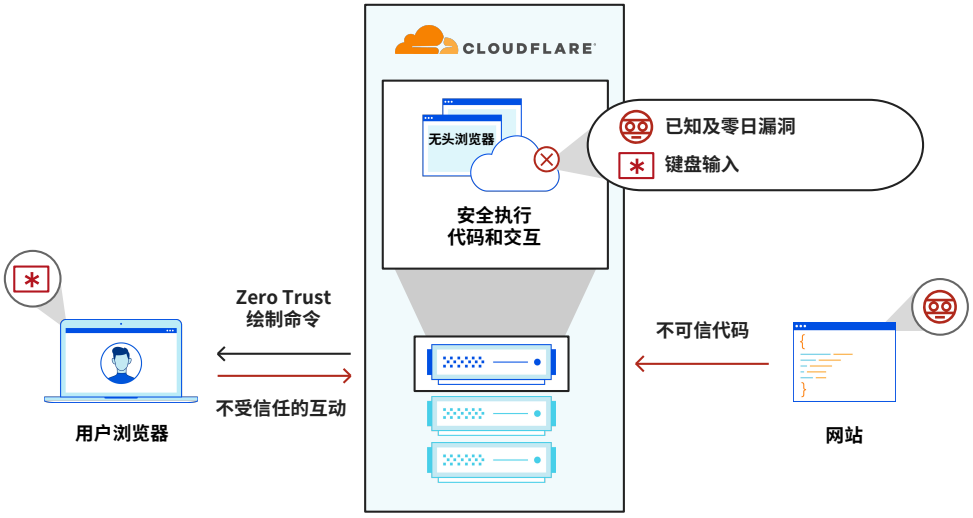
保护数据
通过控制用户在应用程序或有风险站点内的操作（如键盘输入、复制、打印、上传/下载）来阻止数据丢失和网络钓鱼。

最大限度减少攻击面而不影响用户体验

挑战：
没有任何 IT 团队能针对已知漏洞为每一个浏览器打上补丁。而且，现实情况是，即使拥有最佳的情报，过滤和检查并不能预防或检测出所有的威胁。拦截每个站点也不是解决之道：过多限制会导致用户工作效率下降，带来更多损害。

解决方案：
浏览器隔离在无头版本的 Chromium 浏览器上运行，该浏览器在我们的边缘而非您的端点呈现所有浏览器代码，从而遏制恶意软件等已知和未知威胁。最终用户感受不到低延迟体验，使用感受与本地浏览器相似。

工作方式



使用设备客户端*进行的*部署
将来自设备的用户流量发送到 Cloudflare 的全球网络，进行完整的 L4-7 过滤和检查。

无客户端部署
将用户发送到隔离的超链接，而不将其公共 IP 或设备暴露给站点上潜在的恶意代码。

关键用例

勒索软件

隔离能有效预防感染勒索软件。但是，即使是未隔离的站点，这种防御也得到了在本地集成的服务的支持，例如我们的 SWG 可以阻止有风险的站点和域，还有我们的 ZTNA 可以减少威胁的横向移动。

网络钓鱼与电子邮件安全

隔离不仅防止在本地执行网络钓鱼链接中的有害代码，还防止用键盘输入敏感个人信息。此外，不久后，管理员将能一键启用由 Area 1 提供支持的电子邮件过滤功能。

零日攻击

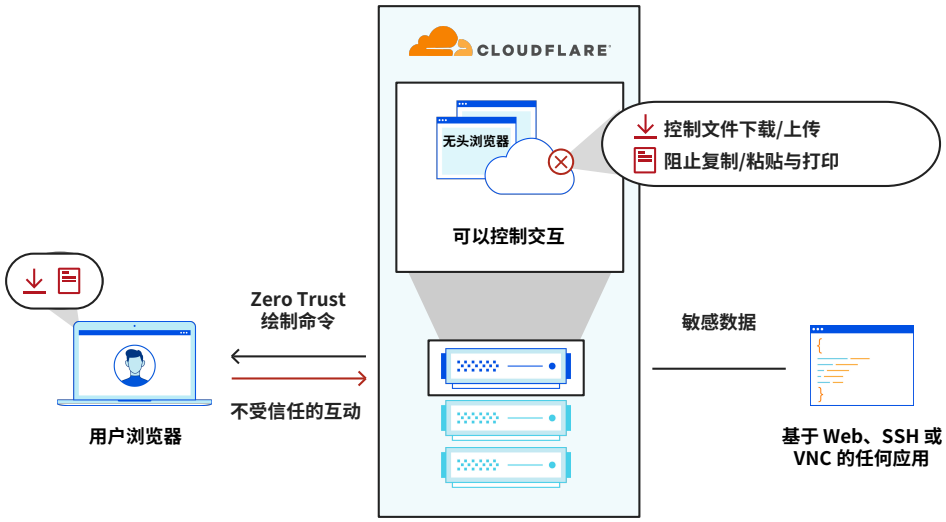
只要有零日漏洞的补丁，Cloudflare 就会自动将补丁部署到我们网络上的所有远程浏览器。这意味着管理员既可以保护设备，还能避免中断，不需要中断用户的工作，也能强制执行更新。

保护 Web 浏览器中使用的数据

挑战：
随着 SaaS 软件的兴起，Web 浏览器成为用户访问数据的主要方式。但传统上，管理员对于数据交付到浏览器的方式的控制很有限。用户通常可以将敏感数据或 PII 复制、粘贴或打印到其他网站、应用或位置。这些常见操作会增加数据泄露的风险。

解决方案：
在隔离的浏览器上运行能让管理员收复控制权，保护任何网站或 SaaS 应用程序上的敏感数据。只需点击几下鼠标，管理员就可以建立粒度规则，预防用户在浏览器上发起有风险的操作。这包括限制使用下载、上传、复制粘贴、键盘输入和打印功能。

工作原理



使用设备客户端*进行的*部署
针对托管设备上用户与数据交互的方式，获得完全可视性并创建设备态势感知策略。

无客户端部署
将应用与未托管设备上的用户最有可能经常访问的敏感数据（如 CRM）隔离开。

关键用例

安全的承包商访问

隔离指向特定超链接的连接 — 无需在用户设备上安装任何软件。

使用此无客户端模式保护承包商在未托管设备上与之交互的数据而不增加配置开销。

控制可疑站点上的输入

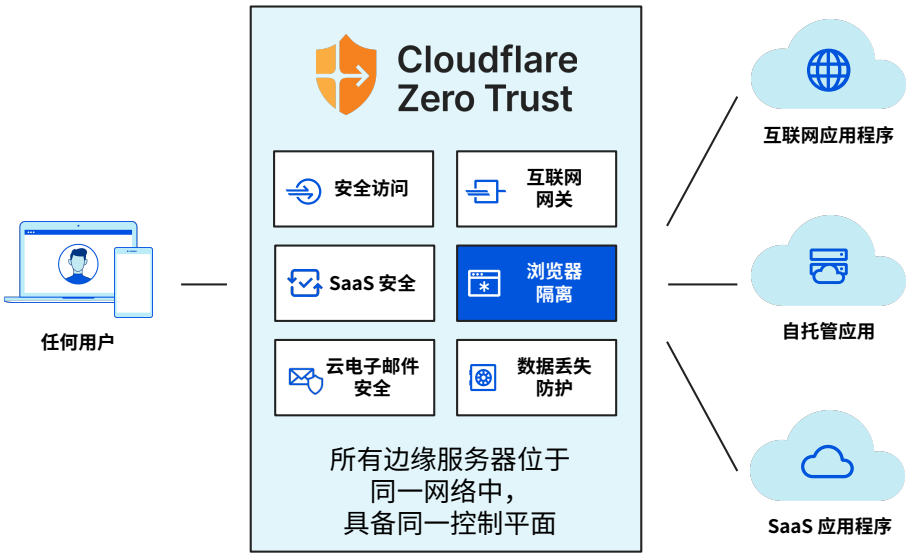
管理员通过隔离“误植域名”和“域”等网络钓鱼常用的高风险网站，保护团队的安全。Cloudflare 提供只读模式的站点，且禁止上传、下载和用键盘输入文件。

与第三方解决方案集成

通过我们的无客户端部署，管理员可以使用现有的 Web 或电子邮件网关集成 Cloudflare，从旧有的服务逐渐过渡。将高风险点击发送到远程浏览器，并应用自定义阻止页面或其他保护措施。

浏览器隔离：对于 Zero Trust 至关重要

隔离是 Zero Trust 的核心原则。只需在 Cloudflare 的 Zero Trust 平台中点击几下，即可轻松扩展浏览器的可视性和控件。



隔离更加便利
在过去，浏览器隔离是独立的解决方案，成本高昂而又复杂，只有大型企业才买得起。

自从 Cloudflare 推出与 ZTNA、SWG 和其他 SSE 服务的原生集成，就可以在合适的地方轻松开始您的现代化之旅，然后再使用浏览器隔离进一步扩展 Zero Trust。

本地与远程浏览

本地浏览
不受信任的网页代码和网络钓鱼网站会在端点设备上本地执行。用户可在钓鱼网站自由输入敏感数据，他们的设备和数据直接暴露在未打补丁的漏洞或零日威胁之下。

远程浏览
未过滤的代码或站点可在持续修补漏洞的远程浏览器中执行。用户交互受到控制，以防止恶意软件和网络钓鱼攻击，并将零日攻击与最终用户的设备隔离开来。

Cloudflare 的方法

网络矢量渲染 (NVR)
不同于占用大量带宽的像素推送或脆弱的内容解除和重建技术，NVR 流式传输安全的绘制指令至设备，但不会发送任何恶意网页代码，也不会影响最终用户的体验。

我们的全球网络
其他提供商在公有云中托管远程浏览器。Cloudflare 的浏览器更接近您的用户，让用户在任何地方都能获得与本地浏览一样的体验。

关键功能

- 在远离用户的云中执行所有浏览器代码
- 无像素推送
- 极速网络（对于全球 95% 的互联网用户只需约 50 毫秒）
- 兼容所有现代浏览器
- 使用/不使用设备客户端部署
- 阻止数据离开企业应用，并获得对“影子 IT”的可见性
- 通过来自我们网络防火墙的情报和 Zero Trust 规则，阻止威胁
- 100% 正常运行时间 SLA

立即自行体验更快速、更安全的浏览

立即试用浏览器隔离