CLOUDFLARE®

SaaS 提供商生存指南

适用于在线应用程序的性能、安全和加密基础知识

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

摘要

SaaS 市场从 2016 年到 2020 年预计将增长 196%。[1] 随着 SaaS 市场持续膨胀并成为业务基础结构的整体组成部分，安全和性能依旧是 SaaS 提供商及其客户最为关注的事项。随着此市场的持续增长，SaaS 提供商在向客户交付最安全和性能最高的应用程序方面将面临日益激烈的竞争。性能不佳和易受攻击的应用程序难免会给收益、终端用户使用、品牌声誉和客户流失带来负面影响。对于一部分重要的 SaaS 提供商而言，要求加密品牌虚名客户域意味着需要手动管理 SSL 生命周期，这需要较长的部署时间和一定的开销成本。或者，可以构建复杂的内部自动化解决方案，此方法将减少专注核心竞争力所需的工程资源。

Cloudflare 适用于 SaaS 提供商的性能和安全解决方案可以保护并加速 SaaS 提供商、终端客户和终端访问者的体验。Cloudflare 的 10 Tbps 全局内容交付网络 (CDN) 结合 Argo 智能路由、负载平衡和性能优化，能够将访问者延迟缩短最多 2 倍。Cloudflare 的高级 DDoS 防护结合 Rate Limiting 和 Web 应用程序防火墙 (WAF)，能够缓解面向网络、传输和应用程序层的大规模攻击和复杂攻击。此外，SaaS 提供商可以选择使用自定义虚名域的便于实施和完全代管的 SSL 解决方案，以保护客户数据的传输。

延迟和安全不足带来的业务影响

任何形式的 SaaS 应用程序延迟和安全不足都将导致客户体验不佳、转换率和搜索引擎排名降低，还将导致收益减少和客户流失增加。

对 SaaS 应用程序使用的性能和可用性影响

在使用网站、应用程序和 API 时，客户需要快速且高度可用的体验。如果在线资源延迟或不可用，SaaS 应用程序使用和转换率将受到显著的负面影响。

例如，Google 曾报告称，站点延迟增加 100 - 400 毫秒这样小的幅度就会对客户行为造成重大影响[1]；Walmart 发现，站点加载时间增加不过几秒，转换率即急剧下降[2]；同样地，Amazon 发现，站点延迟每减少 100 毫秒，收益就会增加 1%。[3]

典型的 SaaS 应用程序性能问题与阻碍 SaaS 提供商的共享托管基础结构或应用程序设置的内部因素有关。这些因素之一是访问者和 SaaS 应用程序原始服务器位置之间的地理距离；据预计，每 100 英里的距离，延迟增加 0.82 毫秒。[4] 距离加上大量未优化的静态内容将增加访问者的延迟时间。

但是，性能并不仅仅由服务器、网络和应用程序决定，它也取决于峰值或季节性流量，这些因素会在共享的基础结构上过度加载，导致应用程序延迟或完全不可用。

加载缓慢和不可用的 SaaS 应用程序对收益、转换率、跳出率、搜索引擎 (SEO) 排名、品牌声誉、客户满意度和服务级别协议 (SLA) 都有巨大影响。

[1] http://www.sfgate.com/business/article/Google-s-speed-need-instantaneous-Internet-3251049.php
[2] https://www.slideshare.net/devonauerswald/walmart-pagespeedslide
[3] https://blog.gigaspaces.com/amazon-found-every-100ms-of-latency-cost-them-1-in-sales/
[4] http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

定向 SaaS 应用程序攻击的影响

无论是进入市场的新 SaaS 提供商，还是将原本在本地的应用程序迁移到云端的现有软件公司，始终在线的应用程序的安全隐患必须考虑在内。

SaaS 应用程序和服务的攻击面变得更为广阔，因为它们暴露于公共 Internet，并且在许多情况下在共享基础结构上跨越多个工作负载。针对 SaaS 提供商的示例攻击矢量包括登录门户、共享 DNS 和托管，以及复杂的应用程序漏洞。请务必注意，许多 SaaS 提供商在共享基础结构中托管多个客户端应用程序，针对该共享基础结构的任何数据泄露、可靠性事件或攻击都可能为其他客户带来负面影响。

以上述矢量为目标的特定攻击包括大规模且复杂的 DDoS 攻击、暴力登录尝试、应用程序漏洞利用以及在许多设备上拦截所有目标网站、应用程序和 API 的未加密客户数据。成功执行攻击所带来的业务影响包括服务中断、品牌劣化、客户流失以及收益严重降低和损失控制开销。

在 2013 年，黑客侵入 Adobe，获取了该公司 290 万客户的信用卡信息和其他个人数据。[5] Adobe 首席安全官 Brad Arkin 坦承在线业务存在风险，并称“网络攻击是当今运营业务所面临的不幸现实之一”。

在 2016 年 10 月 16 日，由于受到臭名昭著的 Mirai 僵尸网络攻击，Airbnb、Amazon.com、Netflix、The New York Times、Paypal、Pinterest、Reddit、Tumblr、Twitter、Verizon、Visa、The Wall Street Journal、Yelp、Zillow 及许多其他网站和应用程序均停止运行很长时间。直接目标不包括应用程序本身，但包括在这些网站和应用程序之间共享的 DNS 服务提供商 Dyn。Dyn 在 11 小时后得以解决问题，所有受影响网站的服务重回正轨。[6]

在加密域和自定义虚名域之间做出选择

由于受到大型科技公司努力构建更安全的 Internet 的压力，在线组织采用 SSL/TLS 加密已成为安全最佳做法，并日益成为一项要求。例如，在 2016 年年末，Google Chrome Web 浏览器开始为用户将不使用 HTTPS 的网站明显标记为“不安全”。[7] 此外，Apple 现在要求所有 iOS 应用程序在提交到应用商店前拥有 HTTPS 连接。[8]

在 SSL 开始兴起的时候，在线组织必须在通过 HTTPS 加密流量或向访问者提供满足性能预期的体验这二者之间做出选择。直到几年前，SSL 协议导致延迟增加，同时也降低了网站和应用程序的性能。另外，即使组织决定牺牲性能以提高安全性，但当时实施 SSL 的操作难度也限制了它的广泛采用。凭借现代的 SSL 改进内容，例如开发了 HTTP/2（HTTP 1.1 的增强版），现在与未加密 HTTP 的性能相比，使用 SSL 保护 HTTPS 上的流量更具优势。

与组织在过去只能在加密和性能之间二选一一样，现在部分重要的 SaaS 提供商必须在加密客户流量和允许这些客户使用自己的品牌虚名域之间做出选择。这两项内容都对合适的品牌代表、安全性、搜索引擎排名和最佳可用性能的组合优势至关重要。

[5] http://www.nytimes.com/2013/10/04/technology/adobe-announces-security-breach.html
[6] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[7] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/
[8] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/

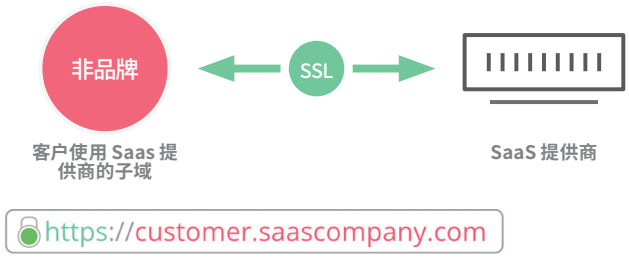
这部分 SaaS 提供商通常向客户提供创建面向公众的在线资源的功能，例如登录页面、网站、支持门户等。SaaS 提供商通常在其主要域的子域上托管这些新创建的客户资源，例如某个 SaaS 提供商的客户创建的资源的 URL 可能读作 **customercompany.saasprovider.com**，而非 **customercompany.com** 或 **support.customercompany.com** 等品牌虚名 URL。这对客户而言是一项挑战，因为没有品牌虚名域，品牌认知、SEO 排名和访问者信任度都会降低。

SaaS 提供商及其客户通过将 customercompany.com 或 support.customercompany.com URL 进行 CNAME 别名解析来转换为 customercompany.saasprovider.com，从而克服了域品牌挑战。这样一来，客户能够使用自己的品牌虚名域；但是 SaaS 提供商将无法轻易启用 SSL，并且难以管理整个 SSL 生命周期过程。手动管理 SSL 生命周期过程或尝试为终端客户构建内部解决方案将导致庞大的时间投入、人力和成本。

在克服上述挑战时，SaaS 提供商可以采用三种方案：

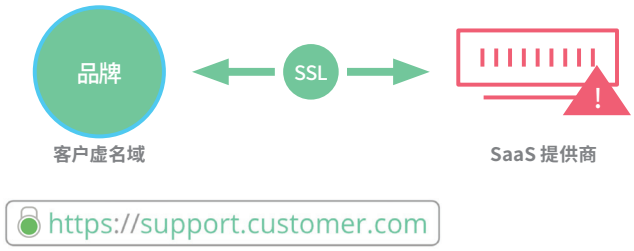
未加密的品牌虚名域

不包含 SSL 的自定义虚名域缺少 SSL 和安全数据传输的性能优势，导致它们易受侦听，并且内容在呈现给访问者之前会被修改或注入。



加密的非品牌域

通过 SaaS 提供商启用 SSL 的域缺少自定义虚名域，导致品牌劣化和 SEO 排名较低。

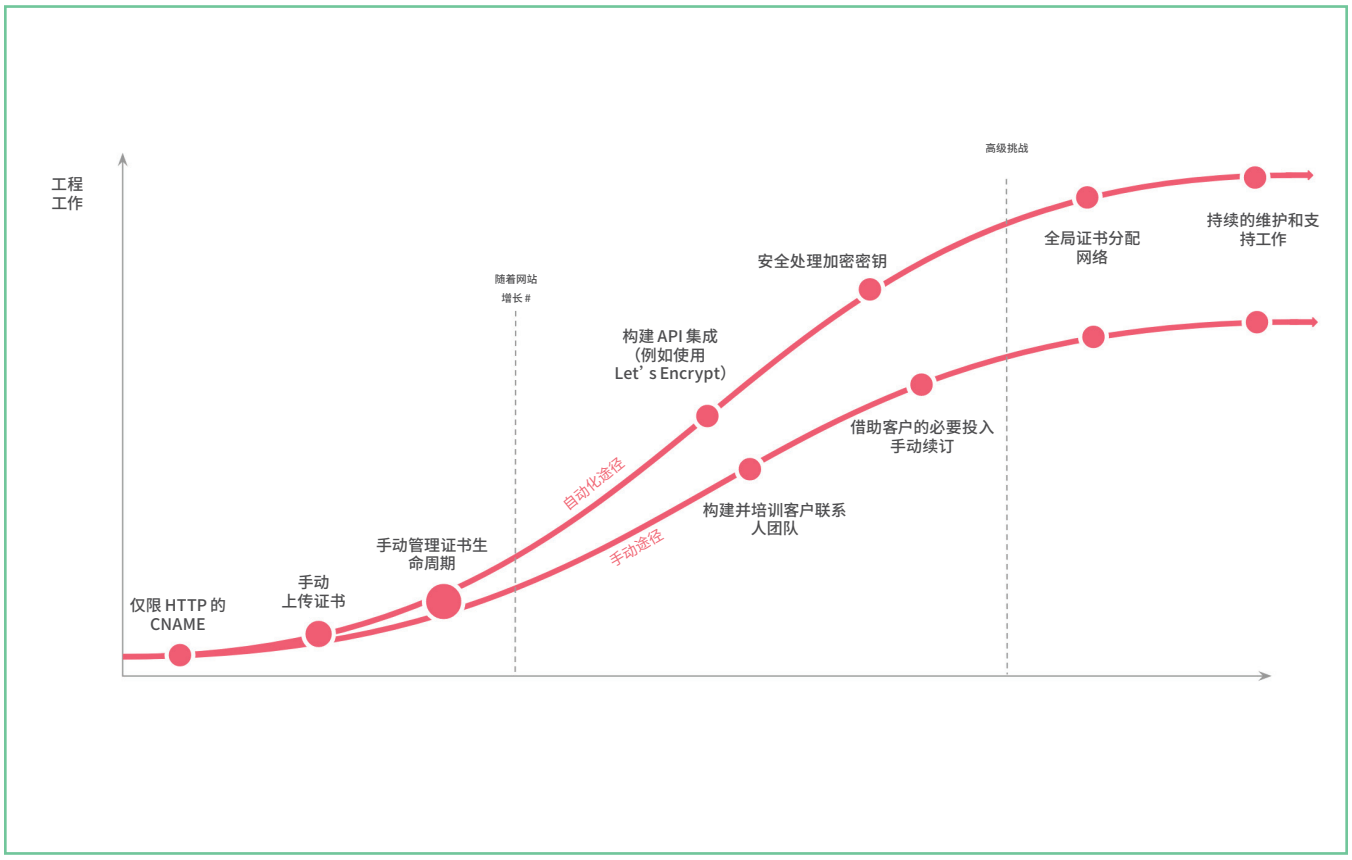


有挑战性的内部方法

想要已加密品牌虚名域的 SaaS 提供商可以手动管理 SSL 生命周期（这需要较长的部署时间和一定的开销成本），或者构建复杂的内部自动化解决方案。

在 SaaS 提供商构建自己的解决方案以为客户域管理 SSL 时，要注意他们面临的技术挑战，这很重要。下图描绘了尝试构建内部自动化 SSL 解决方案的 SaaS 提供商列出的典型路线图。

构建内部解决方案时可以采用两种途径，但这两种途径都不理想。第一种（上方）途径实现 SSL 过程的自动化，但需要大量的工程工作并且带有多个复杂挑战；第二种途径要求 SaaS 提供商和终端客户都付出适当的人力。



Cloudflare 提供的 SaaS 应用程序安全、性能和可用性

Cloudflare 通过减少延迟和优化内容交付性能，同时将这些优势扩展到终端客户的 Internet 资源，提升 SaaS 提供商网站、应用程序和 API 的终端用户体验。

全局可用

Cloudflare 解决方案的核心是由分布在 57 个国家/地区的 117+5 个数据中心组成的全局任播内容交付网络 (CDN)，在每个地区都拉近了 SaaS 应用程序内容与访问者的距离。Cloudflare 还支持超过 38% 的代管 DNS 域，运行着世界上最大的权威 DNS 网络之一。凭借平均几毫秒的查询速度，Cloudflare 与任何代管 DNS 提供商相比，都具有最快的全局性能速度。

规模化应用程序可用性

通过在 Cloudflare 高度可用的 DNS 基础结构和全局 Anycast™ 网络的基础上扩展，Cloudflare Load Balancing 通过跨多台服务器负载平衡流量并将流量路由到最近的地理区域来减少延迟。Load Balancing 包括运行状况检查和快速故障转移，可快速将访问者从故障中路由出来。此外，Load Balancing 可在多个云提供商或本地基础结构上使用，以缓解由单个提供商或服务器导致的中断的影响，同时避免云供应商锁定。

更快的访问者体验

Cloudflare 的 CDN 采用高级优化内容构建，包括 HTML、CSS 和 JavaScript 的自动最小化以及 Gzip 压缩，这可节省最多 20% 的文件和资源大小。此外，专用的图像和移动优化内容可进一步提升 SaaS 应用程序的性能。

虽然 Cloudflare 交付超过世界上 10% 的 Internet 流量，它还实时分析网络路径的真实运行状况和可靠性。Cloudflare 的 Argo 智能路由算法使用这些收集的信息在最快的可用路径上路由流量，同时保留开放的安全连接，以消除连接设置带来的延迟。Argo 智能路由将 Internet 延迟平均降低 35%，并减少 27% 的连接错误。

> “Cloudflare 为 Crisp 将服务质量提升到最高，并将服务响应时间缩短至最低。它为大众将昂贵的网络基础结构商品化。我们非常依赖它。”
>
> crisp™ | Valérian Saliou
> Crisp 首席技术官

保护 SaaS 应用程序和客户数据

Cloudflare 的基于云的安全解决方案保护 SaaS 提供商网站、应用程序和 API，同时将这些优势扩展到终端客户的 Internet 资源。

Cloudflare 的超过 117 个总计 10 Tbps 吞吐量的数据中心任播网络是有史以来最大 DDoS 攻击的 10 倍，可防护针对 OSI 模型第 3、4 和 7 层的攻击。当与 Rate Limiting 和 Web 应用程序防火墙 (WAF) 结合时，Cloudflare 的安全解决方案还可缓解针对应用程序层的复杂攻击。并且借助适用于 SaaS 的 Cloudflare SSL，SaaS 提供商和终端客户可以期望使用加密通信以防御数据拦截和恶意内容注入，同时继续使用自定义虚名域。

保护敏感的客户数据

随着 SaaS 应用程序逐渐保留更多私人和商业敏感型数据，确保防御暴力登录尝试、数据泄露和中间人攻击至关重要。

防御这些类型的攻击可首先通过 Cloudflare 的 Web 应用程序防火墙 (WAF) 实现，它可以缓解针对应用程序层的复杂攻击。Cloudflare 的 WAF 默认包括对 OWASP 前 10 大漏洞的防御，并且包括特定于应用程序的漏洞（针对常见集成和语言）的防御，例如：PHP、Magento、WordPress、Drupal、Atlassian 等。Cloudflare 的 WAF 支持 SaaS 提供商即时创建自定义规则集以防御新发现的攻击矢量和漏洞，并在不到 30 秒内将这些规则传播到 Cloudflare 网络。

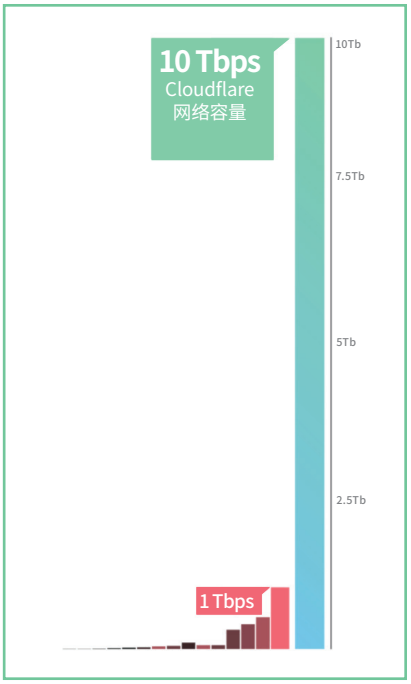
通过与 Cloudflare 的 DDoS 防护合作，Rate Limiting 实现精细控制，以阻止带有可疑请求率的访问者。配备 Rate Limiting 是为了缓解暴力登录尝试，这些尝试寻求访问应用程序或网站的未经授权区域；Rate Limiting 在指定时间内将从特定 IP 地址提出的请求数量限制到特定端点。

> “Cloudflare 的解决方案非常有效。他们的团队几乎立即满足了我们传达的所有要求和自定义项。”
>
> zendesk | **Amanda Kleha GM**
> Zendesk 在线业务单元

适用于 SaaS 的 Cloudflare SSL 提供最高效的方法以自动化管理自定义 CNAME 虚名域的 SSL/TLS 证书，从而确保防御由于未加密连接导致的中间人攻击产生的数据拦截或流量侦听。

阻止恶意流量，确保可用性

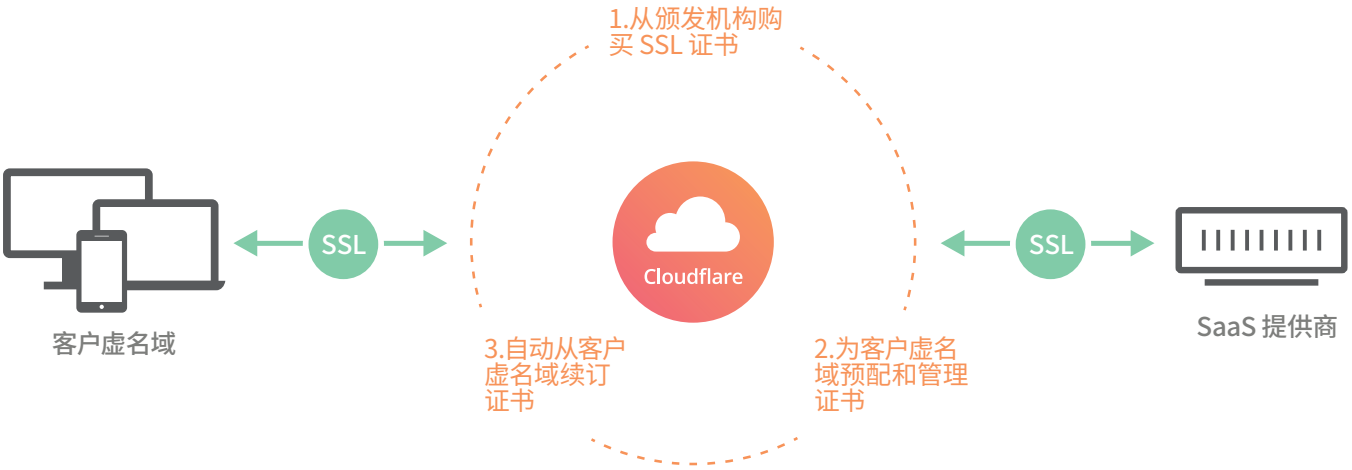
虽然敏感客户数据失窃或丢失可能是灾难性的，但受到尝试中断服务可用性的成功攻击将同样具有破坏性。Cloudflare 的主干是由分布在 57 个国家/地区的超过 117 个数据中心组成的全局内容交付网络 (CDN)。Cloudflare 的总网络吞吐量超过 10 Tbps，这大概是有史以来最大 DDoS 攻击的 10 倍大小。任何针对第 3、4 和 7 层的大规模 DDoS 攻击的尝试都可吸收，并平均分配到 Cloudflare 网络，防止出现停机并向 SaaS 客户保证最高可用性。Cloudflare 的 Rate Limiting 解决方案与 DDoS 防护协同运行，支持精细控制以阻止带有可疑请求的访问者。当特定 IP 超过定义的阈值时，它们在规定时间内将无法进一步向特定端点提出请求。



适用于 SaaS 提供商的自动化 SSL 解决方案

适用于 SaaS 的 SSL 向 SaaS 提供商提供将 Cloudflare 网络的安全和性能优势扩展到终端客户的能力，这些客户将创建自己的自定义虚名域。适用于 SaaS 的 Cloudflare SSL 解决方案支持

客户继续对他们的虚名域进行 CNAME 别名解析来转换为 SaaS 提供商的子域，从而提供品牌 URL 的优势；同时，Cloudflare 为 SaaS 提供商及其客户支持和管理整个 SSL 生命周期。在客户域上支持 SSL 可向访问者提供额外信任、提升 SEO 搜索排名，并解锁现代 HTTP/2 协议，从而更大幅度地提升速度。



品牌访问者体验

可以选择创建自定义品牌虚名域的 SaaS 提供商的客户可以继续这样做，同时也可以享受完全代管的 SSL 证书带来的附加优势。自定义 CNAME 虚名域为 SaaS 客户提供更好的品牌可见性和 SEO 排名，同时确保在网站或应用程序访问者中产生更强的信任感。

安全和高性能的客户资源

适用于 SaaS 的 SSL 可以将专用 SSL/TLS 证书无缝添加到 CNAME 自定义虚名域。通过 HTTPS 传输数据可确保安全传输敏感型客户数据，从而防御中间人攻击和网络侦听。启用 SSL 后，可使用提高速度的 HTTP/2 协议。

自动化生命周期管理和快速 SSL 部署

Cloudflare 管理 SaaS 提供商的 CNAME 客户虚名域的整个 SSL 生命周期，范围从私钥颁发/保护到域验证、颁发、续订和重新颁发。这样就解除了 SaaS 提供商和终端客户处理 SSL 生命周期的重担。在 SSL 颁发过程中，Cloudflare 在几分钟内传输新证书请求并使 HTTPS 上线。

“作为一个工程师，使用 Cloudflare 令我最快乐。”

UDACITY

Paul Bauer
Udacity 平台工程师

附赠

注册 Cloudflare 以提升 SaaS 应用程序的性能和安全，同时为终端客户 CNAME 虚名 URL 轻松部署 SSL。设置很简单，通常不到 5 分钟即可快速上手。请通过 www.cloudflare.com/plans/ 查看从免费版到企业版的各个套餐，并通过 www.cloudflare.com/saas/ 了解关于适用于 SaaS 提供商的 Cloudflare 的详细信息。

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com