CLOUDFLARE®

保持领先

为移动消费者提升电子商务站点性能和安全性

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

摘要

移动商务正处于成为最重要的电子商务战略渠道的临界点。在美国，排名前 25% 的零售商在这场赢家通吃的竞争中早已知晓如何提高移动转换率，以抢占超比例潜在市场份额。他们通过提供快速可用的移动站点和应用，更好地留住用户并吸引用户查看产品。Cloudflare 提供以下优势，可帮助满足这些关键要求：

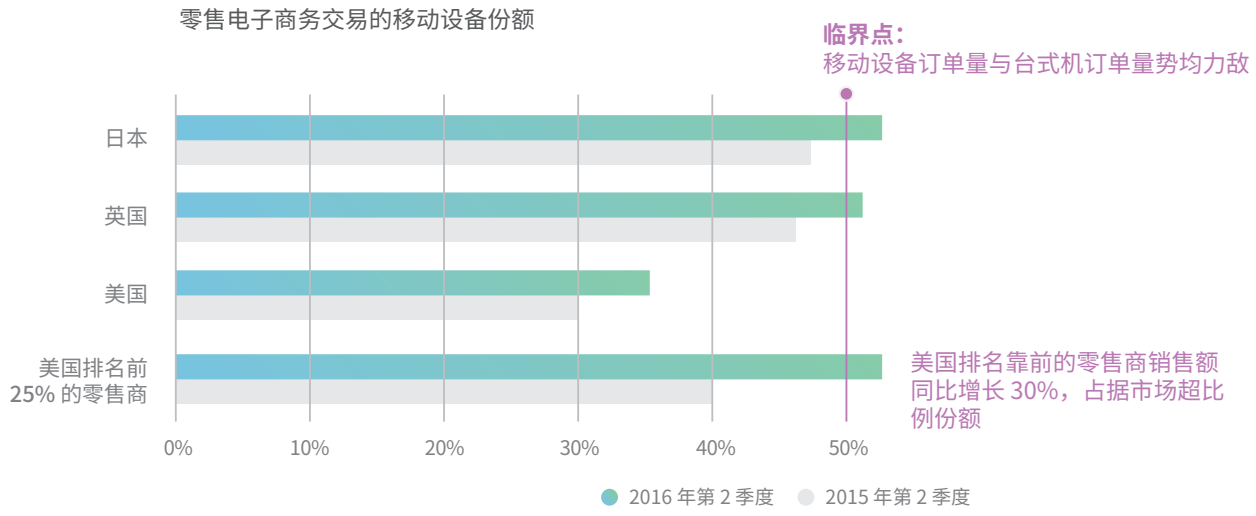
- 最快的内容交付网络之一，基于任播路由，并能缓存空间上接近消费者的内容以降低延迟
- 可预测的统一定价
- 移动图像和代码优化以及 IPv6 支持，来降低移动设备延迟
- 抵御第 3、4 和 7 层 DDOS 攻击并防范第 7 层应用程序漏洞，从而延长正常运行时间
- 凭借高性能妥当加密

设置 Cloudflare 以获上述功能是电子商务供应商为主动保障其站点全年快速安全运行而向前迈出的一大步。

移动商务正处于突破的临界点

电子商务取得的成绩令人兴奋不已：2015 年同比增长 14.6%，而 2015 年美国零售销售额增长就高达 36.2%，其增长速度远远超过了实体零售的增长速度。更令人兴奋的是移动商务，它的增长速度更快。移动商务正处于突破的临界点：2016 年第 2 季度，日本和英国的移动电子商务零售交易份额有史以来首次超过 50%，由此可知其份额大于桌面交易份额。在美国，电子商务交易移动份额以 17% 的同比增速迅速增长。虽然美国电子商务交易移动份额仍低于 35%，但其有望赶超领先的国家。

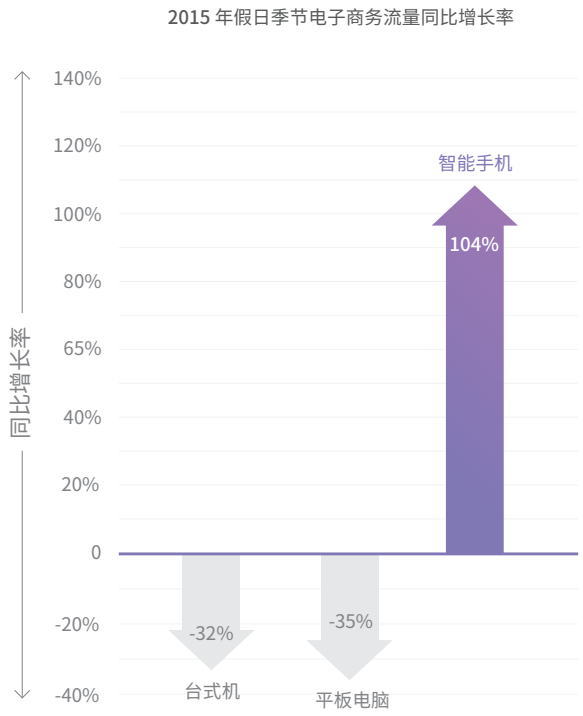
美国排名前四分之一的零售商已经通过提供最佳移动站点和应用来把握住这股趋势。与普通新兴零售商相比，他们能够更好地留住用户并吸引用户查看产品，从而可以将转换率最高提升至 90%。这样一来，他们凭借移动商务带来的 52% 的电子商务销售额占据了超比例移动份额，同比增长达到了惊人的 30%。

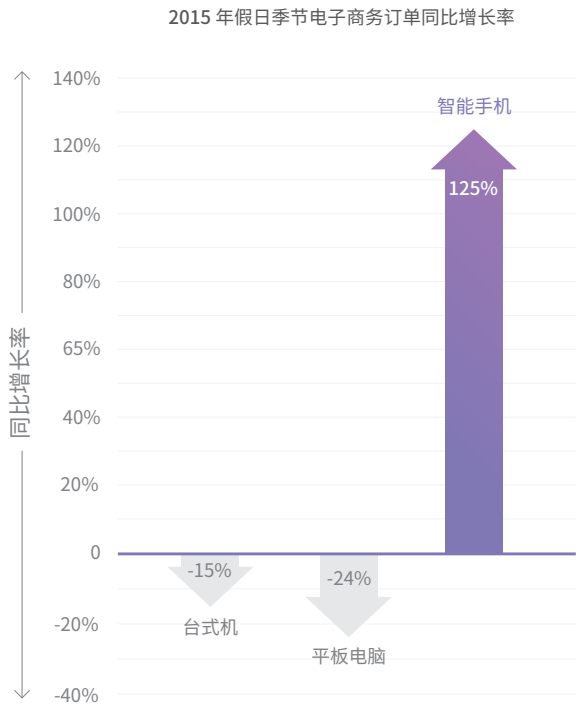


移动商务无疑已发展为关键的销售和营销渠道。能提供最佳移动体验的零售商将成为赢家，他们所拥有的有效市场份额将继续占据主导地位。

移动商务对于假日购物季极其重要

2015 年假日在线购物 (Cyber 5) 打破记录，网购星期一也成为美国历史上在线消费最多的一天。智能手机发挥了相当重要的作用，占用了 49% 的流量并完成了 27% 的订单。智能手机的流量和订单量增长率惊人，而台式机和平板电脑的流量/订单量则有所下降。

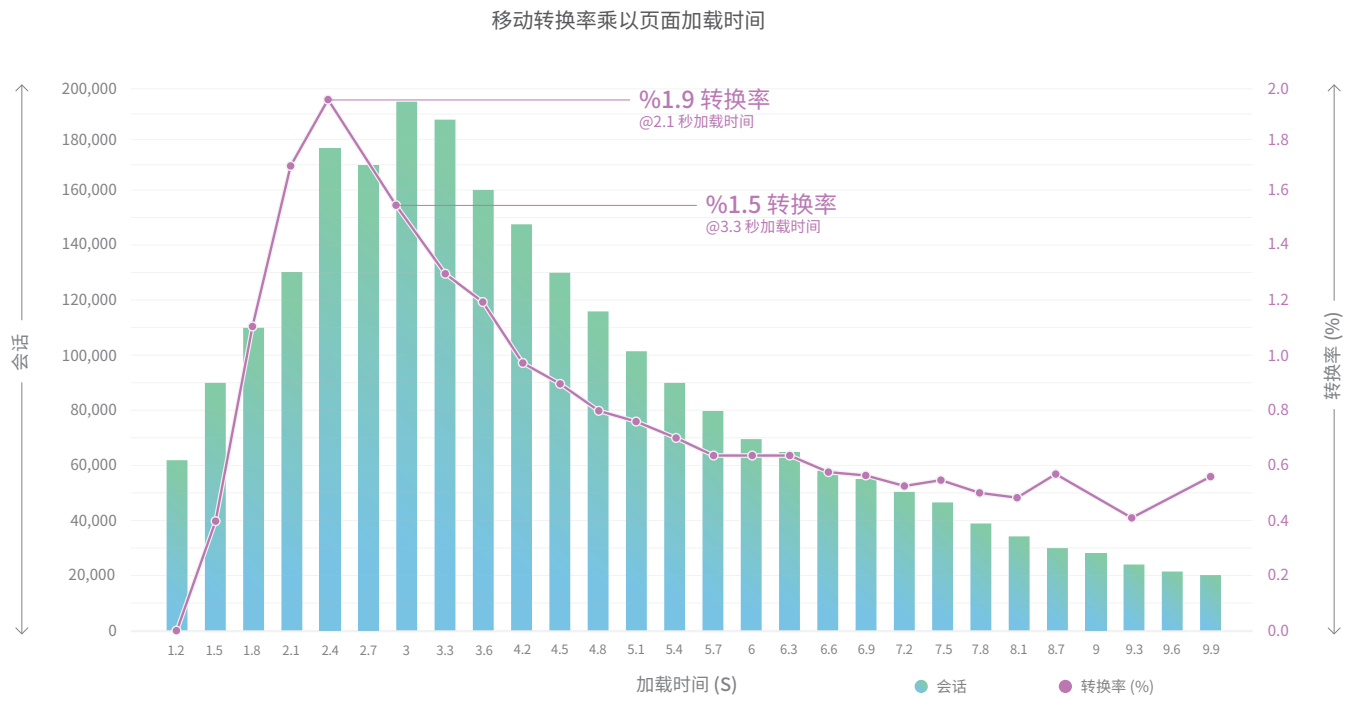




2015 年的 Cyber 5 购物季再次证明，能提供最佳移动体验的零售商将成为最大赢家。例如，Amazon 在 2015 年 Cyber 5 购物季的销售额相较于 2014 年同比增长了 24.1%。在即将到来的假日季，实体零售商与网络零售商将可能迎来线上流量超过店内客流量这一局面，从而彰显出移动购物体验对增长的重要性。

延迟和可用性对转换率的影响

是什么让领先者脱颖而出？领先的电子商务零售商提供最佳移动站点和应用来提升转换率。移动转换率依旧很低，它们直接关乎移动站点/应用的性能和可用性。例如，当平均页面加载时间为 2.4 秒时，某领先在线零售商的转换率可达到 1.9% 的峰值。平均页面加载时间仅慢一秒（即时间为 3.3 秒）会导致转换率下降 27%。

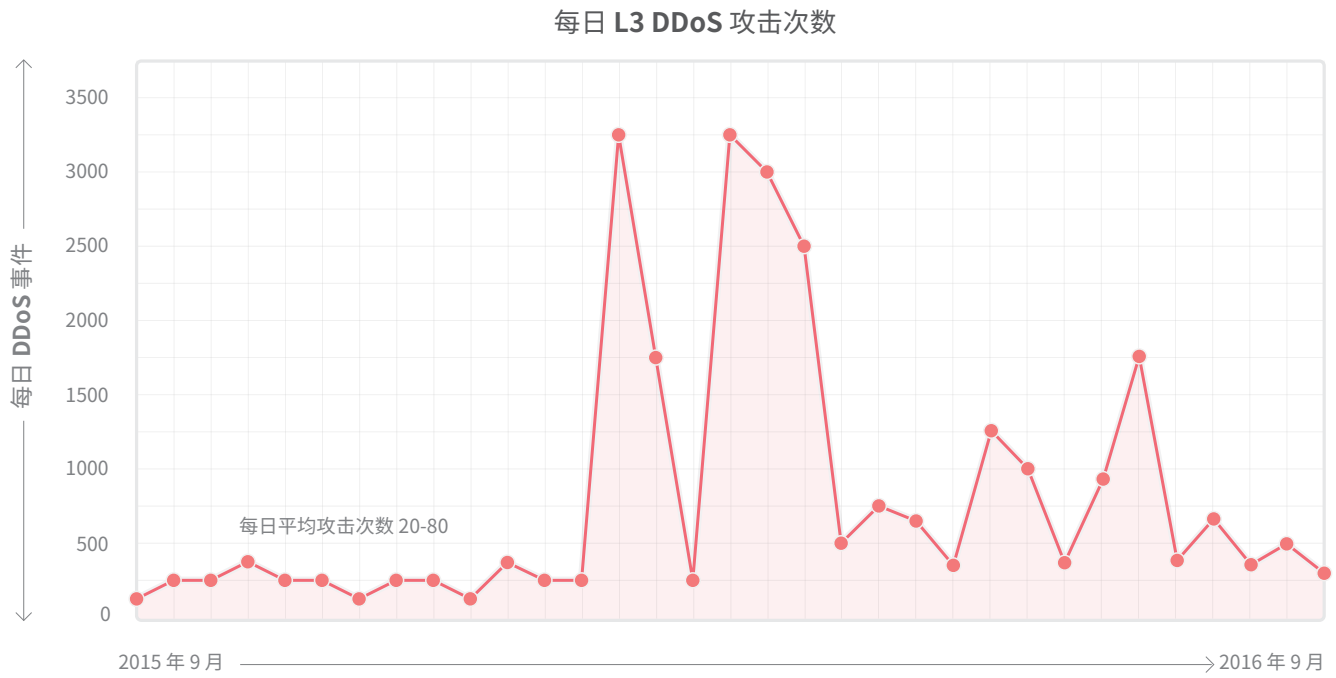


说明站点性能和转换率之间的关系的行业示例有很多

- 站点延迟每降低 100 毫秒，Amazon 增加 1% 的收益
- 站点延迟每降低 400 毫秒，Yahoo 增加 9% 的流量
- 当平均站点加载时间从 1 秒增加到 4 秒时，Walmart 的转换率急剧下降

Google 报告称，一般而言，100 到 400 毫秒的站点延迟会对消费者行为造成重大影响，而对于一个比竞争对手的站点慢 250 毫秒的站点，其访问量通常很少。

除站点/应用本身引起的延迟外，分布式拒绝服务 (DDOS) 攻击还可能会使站点完全不可用。Cloudflare 的网络流入将近 10% 的世界 Internet 流量，可过滤并精确衡量攻击数量。在过去的一年内，Cloudflare 看到攻击数量和强度不断增加，每天最多发生 1,400 起 DDOS 事件，每秒产生 400Gbps 聚合传入流量和包含 2 亿数据包的攻击。



攻击通常不是一次性事件，受害者一般会在一年中多次成为目标。根据 Cloudflare 的经历，任何规模的组织都可能会成为目标。尽管很多行政辖区都有关于 DDOS 攻击属非法行为的规定，但仍有 DDOS 即服务提供商提供订阅，部分起始价格低至 5 到 10 美元/月。

即使是 Amazon 网站（2015 年零售收益 990 亿美元）也在过去多次被攻陷，具体原因尚不清楚。例如，在 2013 年，Amazon.com 被攻陷，持续了大约 15 到 45 分钟，致使公司销售额损失 180 万到 530 万美元（根据该公司每分钟平均销售额 117,882 美元计算得出）。由于是业务旺季，故障带给电子商务供应商的损失在假日季可能会更大（Amazon 在 2015 年第四季度实现了 33% 的年度收益）。系统故障带来的其他负面影响包括对客户满意度、搜索引擎排名和投资者关系的影响。

总之，对于想要提升转换率（特别是在假日季期间）的电子商务供应商来说，提供能够抵御 DDOS 攻击的便捷站点/应用来增加正常运行时间很重要。

实现快捷安全的移动站点的关键技术

Cloudflare 可帮助您加快移动商务站点和应用的速度并提供保护，而无需添加硬件、安装软件或更改任意一行代码。

首先使用 Cloudflare 的内容交付网络 (CDN)，这是世界上最大的网络之一，可支持每月超过 10 万亿次的请求。此数字接近世界上 25 亿多人提出的全部 Internet 请求数的 10%。据 Cedexis 称，Cloudflare 的 CDN 凭借平均响应时间 34 毫秒（在美国）连续被评为最快 CDN 之一。其部分关键功能如下:

基于任播的路由

虽然 Cloudflare 的 CDN 使用名为“任播”的路由方案，但目前多数 Internet 仍使用名为“单播”的机制。在单播下，网络上的每个节点都将获取唯一 IP 地址。路由器将保留全球 IP 地址图，方便找到各跃点之间的最短路径，从而找到最终目标。但是，最终目标可能是在大陆上的某个位置或者是在世界上的其他位置，找到它需要其他跃点，而每个跃点都将增加延迟。在 Cloudflare 使用的路由方案“任播”下，CDN 网络中的多台计算机共享同一 IP 地址，路由器借此可以将请求直接发送到空间上距离最近的服务器，从而降低延迟。

内容缓存

Cloudflare 的任播网络与内容缓存一同运行。在任播将请求路由到空间上距离最近的服务器后，可在此服务器上访问缓存内容副本。缓存的优势在于可以将对象移至更加靠近请求它们的访问者所在位置，从而加快交付速度，并缩短在源 Web 服务器上加载的时间。Cloudflare 提供自动缓存静态内容的功能，并借助 Railgun 来提供缓存动态内容的机制。

Cloudflare 会分析通过 CDN 中的服务器传回的流量，找到原始站点的静态内容部分。然后，静态内容将在短时间内缓存在 CDN 中。通常 66% 的 Web 内容可缓存（通过“自动缓存静态内容”功能），剩余 34% 的内容不可缓存，而且必须从源 Web 服务器获取。Railgun 旨在加快无法缓存内容的交付速度，从而使整个 Web 基本上都可以缓存。其工作原理是认识到无法缓存的网页不会很快更改，而且 Cloudflare 的 CDN 服务器可以识别不同网页版本之间非常细微的差异。随后 Cloudflare 将压缩这些更改（压缩率高达 99.6%），并跨链路发送它们，从而使性能提升了高达 700%。Railgun 需要在源服务器端安装软件组件。

> “随着带宽成本的持续上升，使用类似 Cloudflare 的 CDN 在边缘向用户提供图像既可以节省成本，又能为移动客户降低延迟”
>
> Big 5 Sporting Goods 电子商务总监 Chris Smith

统一定价

为成为 Internet 的一部分，Cloudflare 向许多不同的提供商购买带宽（称为“传输”）。Cloudflare 根据任意给定月份的容量大规模购买传输，来支付某个时间段的最大利用率。虽然 Cloudflare 支付的费率在全球不同地区之间变化很大，但为了使定价简单，Cloudflare 向客户统一收费，无论是在世界上的哪些地方提供流量都是如此。与一些针对在某个网络上提供的个别比特计费的云服务不同，Cloudflare 让月度帐单可预测。Cloudflare 一直致力于降低传输定价和提高对等性，以便可以尽可能低的价格提供最好的服务。

图像和代码优化

Cloudflare 使用 Polish、Mirage 和 Auto-Minify 这“三把利剑”来降低延迟。这些功能对移动设备尤为重要，因为它们的带宽都很有限。

Polish 通过删除元数据并压缩图像来缩小图像大小。Polish 可以在无失真模式下运行，这样可在不删除任何图像数据的情况下从图像标题和元数据中删除多余膨胀项。平均文件大小减少 21%。除了在无失真模式下运行外，Polish 也可以在失真模式下运行，此时会将压缩算法应用到合适的图像。显示的图像将与之前的完全一样，肉眼无法看出任何差别，但平均文件大小减少 48%。在构成常规网站的数据中，图像占比超过 50%。

Mirage 管理图像在移动设备上的加载方式。它将快速生成可用页面的外观以供用户交互，同时在不干扰用户体验的情况下填充页面的其余部分。

- Mirage 使用延迟加载来设置图像在视口中加载时的优先级，即浏览器实际显示的图像。对于浏览器未显示的其他图像，当需要它们或者有备用网络资源可用时，将在页面上加载它们。
- 移动设备由于屏幕尺寸较小而要求使用较小的图像。Mirage 可在服务器上调整图像大小，通常将图像调整至完整分辨率图像的 1%，并先发送缩小的图像。在缩小的图像呈现在页面上后，它们将替换为完整分辨率版本的图像。图像开始先显示为低质量图像，然后转为呈现清晰聚焦版。
- Mirage 通过单个请求从 Cloudflare 网络流式传输全部图像，无需为每个图像发起新请求。这意味着，即使是一个包含数百个图像的页面，也可以通过至多两个请求开始在浏览器中呈现。甚至是使用慢速移动连接的用户也可以立即开始与页面交互，无需等候加载全部的完整分辨率图像

Auto Minify 会从 HTML、JavaScript 和 CSS 文件中即时删除所有不需要的字符（即“空白”），可节省 20% 的文件大小，而且不会更改任何功能。Cloudflare Auto Minify 的实现速度要比排在其后的方法快 100 倍。

支持 IPv6

据 Facebook 和 Linkedin 提供的真实用户监控测量数据显示，美国前 4 大移动网络通过 IPv6 加载移动页面的时间要比通过 IPv4 加载的时间快 10%。虽然推出 IPv6 耗费了数十年时间，而且它也饱受慢速质疑，但美国前 4 大移动网络约 60% 的 Android 和超过 20% 的 iPhone 请求仍在双栈站点上使用 IPv6（数据截止至 2016 年 5 月 4 日）。Cloudflare 不仅从 2012 年以来就提供完整的 IPv6 支持和 IPv6 转 IPv4 网关，而且还让客户通过“简单的单击”即可启用此服务。如果源服务器支持 IPv6，则抵达 IPv6 连接的访问者将通过端到端协议进行传输。如果源服务器仅支持 IPv4，Cloudflare 将通过 IPv6 接受访问者，然后无缝通过 IPv4 向服务器提出请求。此外，如果在源服务器上运行的应用程序有要在 IPv4 上运行的硬性要求，Cloudflare 可提供伪 IPv4。无论何时通过 IPv6 建立连接，此选项都会将 HTTP 标题添加到包含“伪”IPv4 地址的请求中。

第 3 层和第 4 层 DDOS 保护 - 借助自动学习平台实现任播网络弹性

除使用 Cloudflare 的内容交付网络 (CDN) 外，下一步是保护站点/应用免遭恶意攻击，以保证正常运行时间。Cloudflare 的高级 DDoS 保护已配置为网络边缘的一项服务，能够与威胁的复杂性和规模相匹配，并可用于缓解各种形式和规模的 DDoS 攻击。Cloudflare 已阻止多起最大的 DDOS 攻击，包括超过 400Gbps 的攻击。

第 3 层和第 4 层 DDOS 攻击通常是批量攻击，例如 DDOS 放大攻击、DDOS 洪水攻击和 DDOS SYN 洪水攻击。虽然这些攻击可以摧毁典型的基于单播的网络，但 Cloudflare 基于任播的网络通过将攻击流量散布到 100 多个 Cloudflare 数据中心和一组其他网络的多样化高带宽互联上，从本质上扩大表面，以轻松吸收攻击流量。此外，Cloudflare 还提供自动学习平台来实时分析网络流量，以确定异常或恶意请求。确定新攻击后，Cloudflare 将自动开始为特定网站和整个社区阻止该攻击类型。

即使从成本角度来看，攻击通常也不会对 Cloudflare 造成影响：Cloudflare 会大规模购买大量带宽，并支付一个月内平均较高的入口（入站）流量或出口（出站）流量的费用。由于 Cloudflare 充当缓存代理，因此在正常情况下，出口流量总是会超过入口流量，通常大约 4 到 5 倍。当有攻击时，这两条线将靠得很近，但很少有攻击能大到增加 Cloudflare 的整体带宽成本。Cloudflare 将此优势传递给客户，而且客户无需支付因 DDOS 攻击引起的增加的网络流量费用。

随着 Cloudflare 持续壮大其网络和社区，发动对任何 Cloudflare 用户的有效 DDoS 攻击将变得越来越难。

第 7 层 DDOS 保护 - 包含 IP 信誉数据库的评分限制器

与第 3 层和第 4 层批量攻击一样，第 7 层拒绝服务攻击使用大批量请求以阻止真实用户访问网站。在第 7 层拒绝服务攻击中，单个 IP 地址可提出许多与无恶意的正常流量模式相似的请求，因此难以防御。

Cloudflare 的流量保护器（当前可通过早期访问计划获取）将跟踪从每个 IP 地址发出并到达某个站点的请求数，然后识别每分钟发出过多请求的站点。识别可疑 IP 地址后，将向从此 IP 地址发出的流量呈现约 5 秒的间隙页面，以解决一系列数学难题。如果请求无法解决该难题，流量保护器将降低该 IP 信誉的级别，并且来自此地址的流量在每次尝试访问时，都将显示 CAPTCHA 页面。

当 Cloudflare 识别某个 IP 地址疑似发出恶意请求时，该地址将存储在 Cloudflare IP 信誉数据库中。根据威胁得分，某项请求可得以通过或显示 CAPTCHA。如果 CAPTCHA 无效，并且该 IP 地址被确认为恶意地址，则将针对整个网络在 Cloudflare 边缘拦截该请求，使整个 Cloudflare 社区受益。

第 7 层非 DDOS 应用程序漏洞攻击 - Web 应用程序防火墙

第 7 层应用程序层攻击是最复杂也是最先进的攻击类型。通过模仿应用程序的正常使用方式，它们能够躲过多数 DDoS 缓解设备和漏洞防护服务。常见的攻击类型包括 SQL 注入和跨站点脚本 (XSS)，这可能会允许攻击者访问并篡改客户数据或其他任何类型的应用程序数据。

Cloudflare 通过 Web 应用程序防火墙 (WAF) 应对这些威胁。WAF 实现 OWASP 核心规则集（Cloudflare 提供的即时可用规则）以及社区/客户创建的自定义规则。Cloudflare 发布的新规则将在 30 秒内传播到所有 Cloudflare 服务器节点，并且 WAF 本身对每个请求增加不到 1 毫秒的延迟，由此可在不损失任何性能的情况提供安全性。如此一来，Cloudflare 能够保护客户不受重大零日漏洞（包括 Shellshock 漏洞或 Heartbleed Bug）的影响。

> “我们非常认真地对待 DDOS 攻击的影响。即使在我们的域面对 DDOS 攻击时，Cloudflare 仍能快速提供保护，从而为我们的客户提供无缝体验。Cloudflare 带给我们的一项最大优势是内心得以平静，因为我们知道有人正在监控网络，并能缓解任何攻击”
>
> Big 5 Sporting Goods 电子商务总监 Chris Smith

TLS 1.3 和包含服务器推送的 HTTP/2

加密对于提供可信赖的购物体验至关重要，而最新的 SSL 增强功能可用于妥善加密和提升性能。传输层安全性 1.3 (TLS) 不仅删除了早期 TLS 版本的不安全功能，还通过减少一半的协议往返降低了延迟。Cloudflare 最先部署了 TLS 1.3，并对制定标准作出重大贡献。Cloudflare 也最先部署了仅可与 TLS 一起使用的 HTTP/2。终端用户在使用浏览器时认为 HTTP/2 提升了性能，特别是降低了延迟。HTTP/2 与服务器推送一同运行，由此服务器可发送客户端尚未请求的资源，以大幅提升所需性能。Cloudflare 正致力于将新兴技术整合到其网络，TLS 1.3 和包含服务器推送的 HTTP/2 仅是其中的两个示例。

要点

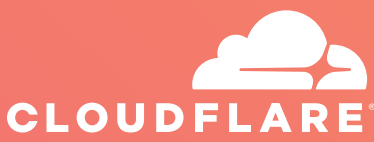
注册 Cloudflare 以提升移动站点和应用的性能，同时保护它们不受 DDOS 攻击和应用程序漏洞的影响。设置过程很简单，通常只需不到 5 分钟的时间便可设置完并运行。请查看从免费版到企业版的各项计划，网址是 www.cloudflare.com。

要了解有关 Cloudflare 的详细信息，请联系我们。

www.cloudflare.com

enterprise@cloudflare.com

1 888 99 FLARE



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