

保护云端应用程序

快速、易于部署且可扩展的分层防御，
用于防范 DDoS、数据威胁和恶意僵尸

保护云端应用程序

快速且易于部署的分层防御, 可防范 DDoS、数据威胁和恶意僵尸

公司在增强安全态势方面所面临的压力正与日俱增。造成安全压力的三个作用力如下:

- 攻击者实力更强、手段更先进且动机极强
- 由于应用程序面临更多公开的 API、更高的 SaaS 采用率以及与更多第三方应用程序集成, 所以攻击表面区域不断增加
- 公众和政府对于数据、隐私和安全性的审查更严格

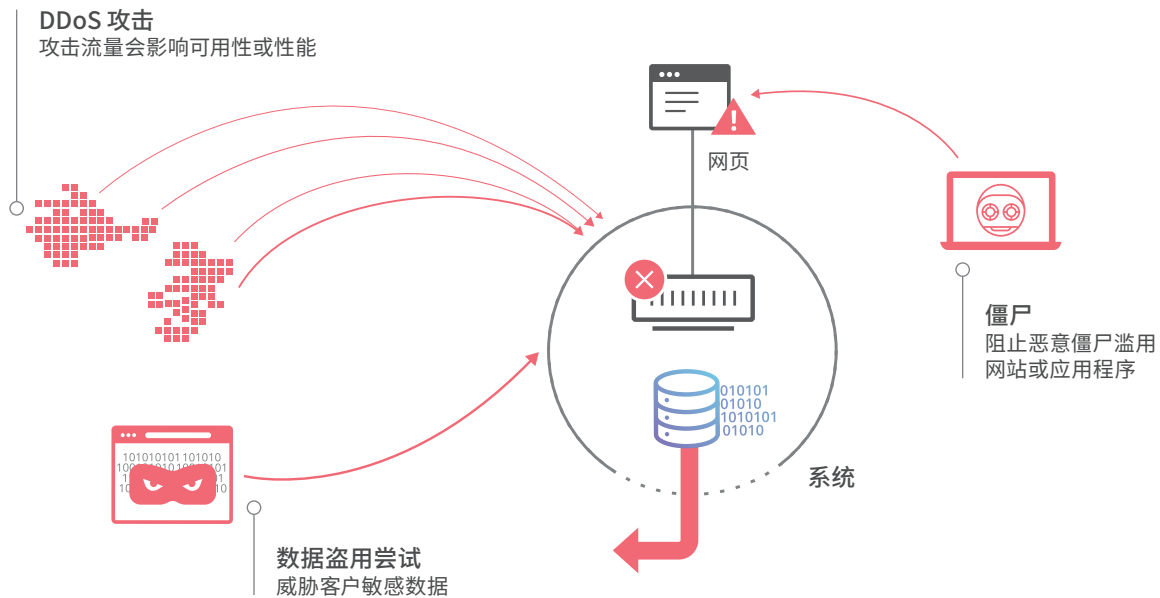
攻击者发起分布式拒绝服务 (DDoS) 攻击的频率和规模正在不断增加。通过联机利用僵尸网络和数百万台物联网 (IoT) 设备, 他们能更加轻松地发动高度分布式大规模攻击且影响力巨大。

除了发起更大规模的攻击外, 攻击者还将注意力从网络层转移到应用程序层。应用程序层攻击或“第 7 层”攻击检测起来愈发困难, 此类攻击通常需要更少的资源即可攻陷某一网站或应用程序, 并中断运营。

攻击者能够通过试图攻陷网站或盗取敏感数据来获利, 例如通过劫持网站进行勒索。这样一来, 由于成功通过勒索从企业目标对象那里获利, 攻击者的动机更强、更具组织性且愈发普遍。

随着公开程度的增强, 公司需要加强抵御以下三种主要问题和风险的能力:

- 针对应用程序、网站和 API 的 DDoS 攻击不断削弱可用性或性能, 使得收益减少、运营成本增加、品牌退化
- 对敏感客户和业务数据 (如个人身份识别信息 (PII) 或知识产权) 的威胁, 造成客户流失和客户信任的丢失
- 恶意僵尸通过内容剽窃、帐户盗用和欺诈性付款滥用客户应用程序



尽管 DDoS 会造成经济上的损失，但数据外泄或恶意僵尸可能因公司规模或行业而异，企业影响的严重性正在各类企业中不断增长。

根据 2015 年的 IDC 报告，基础设施停工的平均成本为每小时 10 万美元。¹

数据威胁可能是泄露的用户信息或者敏感客户数据的渗漏，如应用程序数据存储中的信用卡和密码。据记载，在 2017 年按丢失或被盗计算数据外泄的全球平均成本为 141 美元，而数据外泄的平均总成本为 362 万美元。² 随着政府和媒体的审查越来越严格，无论是从经济代价还是从公众信任丢失的角度来看，甚至最小数据威胁给公司带来的影响也越来越大。

恶意僵尸不仅可以盗用用户帐户，而且还能进行欺诈性付款和内容剽窃。来自僵尸的付款欺诈（即自动以有限供应量反复购入库存）可能会损害商店的品牌影响力，造成以后的客户不再光顾，进而导致未来销售量走低，甚至破坏与供应商之间的关系。内容剽窃可能直接导致收益下降（尤其是广告驱动型企业），具体表现在 SEO 排名下降、每千人成本印象 (CPM) 降低或者广告商流失。

优势

为了应对频现的泄露和严峻的企业影响，公司不仅要处理具体的策略问题，而且还需要在不断变化的威胁环境中先于敌人抢占先机。

三个重要的区别之处在于扩展、性能和易用性。

扩展方面

Cloudflare 在网络规模和用于数据分析的流量变化上具有优势。凭借对 600 万客户网站提供保护，Cloudflare 对新生的全球威胁有进一步了解。因此，Cloudflare 的 DDoS 保护和 Web 应用程序防火墙主动保护客户免遭引发停机和收益损失的攻击。

Cloudflare 网络专为扩展而设计，既能实现速度又具有弹性。为了每天针对超过 3,000 亿个请求提供其所有服务，在每个数据中心的各服务器上运行的服务（如 DNS、加密和 WAF）可通过低延迟和高可靠性处理巨大的流量负载。

随着 DDoS 攻击规模的不断扩大，网络的规模和弹性可以给客户带来益处。通过与任播网络相结合，Cloudflare 基于超过 116 个数据中心进行扩展，从而甚至能抵御最大的分布式攻击。

提高性能的同时保护应用程序

过去，客户不得不在安全性和性能之间权衡取舍。TLS 和 WAF 解决方案通常会降低网站的性能。例如，用于加密连接的协议 TLS 最多可以引入四个来回，而这一切仅仅是为了启动单个安全会话。这些额外的来回引入可能会增加延迟。类似地，由于 WAF 会串联检查每个请求，因此会带来额外的延迟。

Cloudflare 既能提供安全性，又能保持高性能。由于低延迟安全性服务与流量加速服务的集成，Cloudflare 的安全功能可提高应用程序性能，而不会降低性能。对 TLS 1.3 的支持和全球会话恢复可以减少来回次数，而允许多路复用下载的 HTTP/2 可缩短页面加载时间。因为 Cloudflare 安全服务与流量加速服务（如缓存和智能路由）集成，所以相较于在不使用 Cloudflare 的情况下不安全地运行而言，应用程序可以体验更快的性能。

¹ IDC, DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified, Stephen Elliot, 2015 年 3 月

² Ponemon Institute, 2017 Cost of Data Breach Study, 2017 年 6 月

通过缓存, 网站访问者可以更快访问静态内容。这不仅减轻了源服务器上的负载, 而且还加快了应用程序的响应速度。智能路由可确定从 Cloudflare 到源服务器的最快路径, 从而加快动态和静态内容的呈现。



扩展

从头开始针对弹性进行构建



易用性

直观 UI 和 API, 实现灵活的配置和管理



速度

高性能安全性与流量加速集成

易用性可提高安全态势

对用户和管理员来说, 安全解决方案的易用性不仅仅是漂亮的界面, 还需要有助于提高公司的安全态势。Gartner 的研究表明, 到 2020 年, 99% 的防火墙违规将由简单的防火墙配置错误 (而不是缺陷) 造成。³

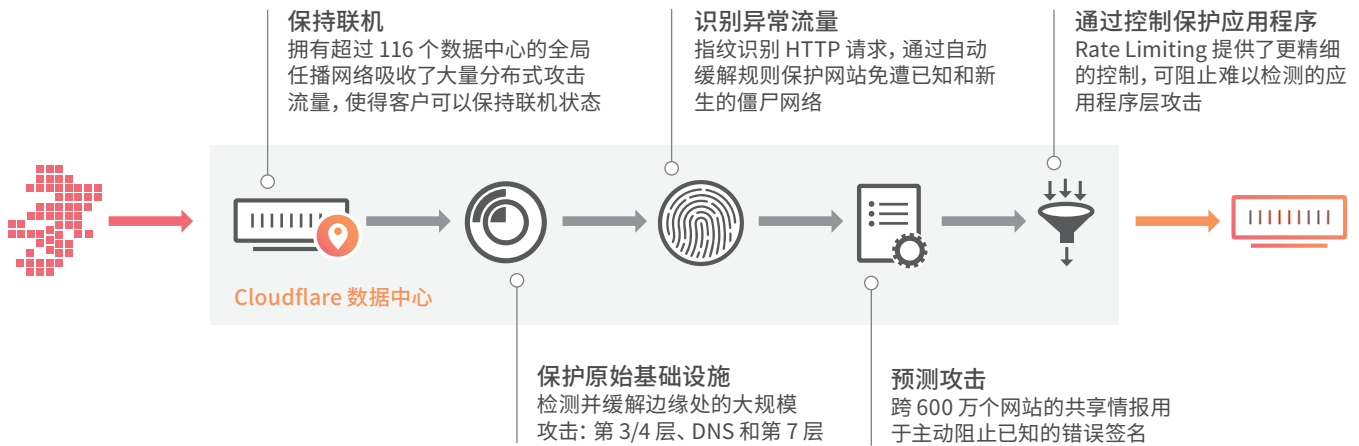
良好的用户体验 (UX) 可以降低因配置错误引起的安全风险, 还可以提高在不断变化的威胁环境中的敏捷性。设置 Cloudflare 可能需要不到 5 分钟的时间。这种易用性使公司能够面向更多非安全专家的员工扩展安全策略管理, 减少更改和部署新策略的时间, 并提高对复杂应用程序安全态势作适时调整的力度。

Cloudflare 运用了这些优势来保护客户免遭以下三项主要挑战的威胁: 可能会降低应用程序性能和可用性的 DDoS 攻击、来自多方位攻击的客户数据威胁, 以及滥用网站的恶意僵尸。

保护应用程序免遭 DDoS

DDoS 攻击会发送大量流量, 试图攻陷某个网站或服务。这种恶意流量通过使源服务器过载, 使目标应用程序运行缓慢或者不提供给终端用户。Cloudflare 提供多层防御。

³Gartner, Inc., [One Brand of Firewall Is a Best Practice for Most Enterprises](#), Adam Hills and Rajpreet Kaur, 2017 年 6 月 5 日



全局任播网络

超过 116 个数据中心的任播网络扩大了表面区域, 使得 Cloudflare 可以将 DDoS 攻击分散开来。借助任播, 多台计算机可以共享同一 IP 地址。当某一请求发往任播 IP 地址时, 路由器会将其引导至网络上距离其最近的计算机。这样就缓解了僵尸网络发起的高度分布式攻击, 因为一部分 DDoS 流量已被各数据中心吸收, 而非集中在单个点上。

边缘处的智能和自动缓解

由于 Cloudflare 在其 600 万个网站上提供可见性, 因此 DDoS 保护服务可基于一个网站的攻击采用启发式方法来保护许多其他网站。

自动缓解通过指纹识别网络流和 HTTP 攻击流量, 以便在对客户网站造成不利影响前主动识别并停止攻击流量。

通过在网络边缘处消除这些大量攻击, 客户的源服务器可保持受保护和联机状态。

DNS、网络和第 7 层保护的集成堆栈

由于每个边缘服务器都有一个集成的安全服务堆栈 (如 DNS、防火墙、Rate Limiting 和 WAF), 因此 Cloudflare 不仅可以提供分布式保护, 而且还能提供分层防御以抵抗不同类型的 DDoS 攻击, 特别是 DNS、网络和应用程序层 DDoS。

Cloudflare 的分布式 DNS 服务可以抵御针对域名服务器的直接攻击。诸如第 3 层和第 4 层等网络攻击不仅自动被阻止, 而且可以由客户进行配置, 以便通过 IP 防火墙按 IP、来源国家/地区或 ASN 阻止恶意源。安全设置可以利用 Cloudflare 对其 600 万个网站上的任意 IP 地址信誉的可见性, 主动阻止标识的恶意流量。

我们喜欢以平和的心态知道自己可以设置 Cloudflare，
无需考虑，坚信不会受到任何恶意 DDoS 攻击的影响。

BUYCRAFT

LEE MCNEIL
CTO

基于速率的可配置缓解

尽管 Cloudflare 的 DDoS 解决方案可自动保护客户免遭大规模网络和应用程序攻击，但部分客户需要可配置的控制来保护自身免遭规模虽小但仍在恶意之列的流量攻击。

凭借自定义请求速率阈值、目标 URI 和请求属性（如方法和响应代码）的功能，让客户可灵活地基于其应用程序和流量配置文件调整其防御。

通过分层防御降低数据威胁的风险

攻击者在试图破坏客户数据时通常会使用多种攻击手段。公司需要分层防御来保护自己。



攻击



Cloudflare 解决方案

1. 通过各种形式和 API 注入
恶意负载



通过 WAF 阻止热门 OWASP 和新生的
应用程序级攻击

2. 窥探客户输入的未经加密的
敏感数据



通过 SSL/TLS 进行加密来阻止窥探

3. 以暴力方式攻破登录页面



通过 Rate Limiting 提供登录保护

4. 攻击者试着伪造 DNS 信息
来拦截客户凭据



弹性 DNS 和 DNSSEC 可阻止伪造的信息

通过安全的 DNS 减少欺诈

缓存中毒或“欺骗”诱使让毫无戒心的网站访问者在受到攻击的网站上输入信用卡号等敏感数据。在攻击者使用错误的记录来损害 DNS 域名服务器的缓存时，会发生此类攻击。在缓存条目失效前，该域名服务器将返回假的 DNS 记录。访问者将路由到攻击者的网站而非正确的网站，致使攻击者可以盗取敏感数据。

DNSSEC 使用加密签名验证 DNS 记录。通过检查与记录关联的签名，DNS 解析器可以验证请求的信息来自其认证的域名服务器，而不是中间人攻击者。

通过加密减少欺诈

攻击者可能会拦截或“窥探”客户会话以盗取客户敏感数据，包括诸如密码或信用卡号等凭据。当出现“中间人”攻击时，浏览器会认为它正在与加密通道上的服务器通信，服务器则认为它正在与浏览器通信，但它们都在与位于两者中间的攻击者通信。所有流量均流经此中间人，该中间人能够读取和修改任何数据。

通过快速加密/终止、简单证书管理和最新的安全标准支持，确保客户安全传输用户数据。

通过自动更新的可扩展 WAF 阻止恶意负载

攻击者通过提交恶意负载利用应用程序漏洞，从而从数据库或用户浏览器中提取敏感数据，或者通过注入可破坏目标系统的恶意软件来提取敏感数据。

Web 应用程序防火墙 (WAF) 会检查网络流量以寻找可疑流量；它可以自动根据您要求应用的规则集过滤掉非法请求。它会查看基于 GET 和 POST 的 HTTP 请求并应用规则集（如涵盖 OWASP 排名前 10 的漏洞的 ModSecurity 核心规则集），确定阻止、质询或予以通过的流量。它可以阻止垃圾评论、跨站点脚本攻击和 SQL 注入。

Cloudflare WAF 会基于 600 万个客户识别的威胁更新规则，并且可以在不影响应用程序性能的情况下保护客户，这归因于其低延迟检查和与流量加速的集成。

通过登录保护降低帐户盗用几率

攻击者通过采用转储凭据自动化登录，以“暴力”方式攻破受登录保护的页面，从而发动“字典攻击”。Cloudflare 使用户能够自定义速率限制规则来识别和阻止边缘处的这些难以检测的攻击。

通过监控和评分提供保护

Cloudflare 的第三方应用通过监控网站是否存在漏洞、对公司的安全成熟度进行评分并将其集成到开发过程中，提供额外的主动保护层。

Cloudflare 的安全功能让我们的开发人员不必再担心网站是否保持联机状态, 让他们可以专注于其他网站的改进工作。

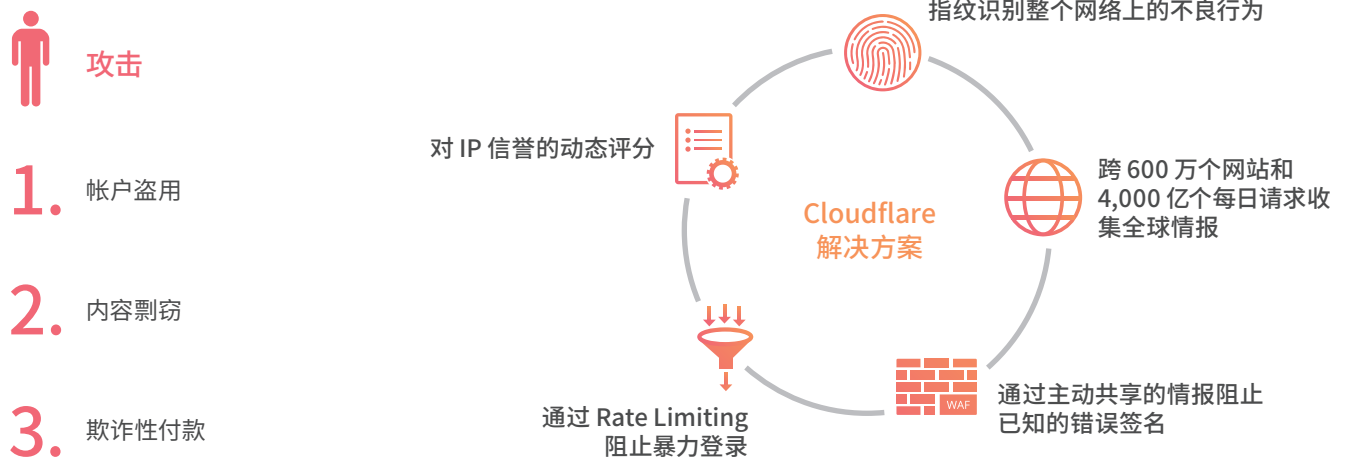


DAVID VERZOLLA
技术主管

防止滥用僵尸

三种滥用僵尸形式正在不断增长, 不仅频繁出现, 手段极其先进, 而且还给客户带来了不利影响。因此, 僵尸防御性解决方案需要不同的元素来解决不同的潜在攻击模式。

最常见的攻击是帐户盗用、内容剽窃和欺诈性付款。这三种形式可以使用不同的僵尸“样式”, 每种样式可使用不同的方法进行检测和缓解。



基于速率的检测和缓解

因为一些僵尸是自动攻击型, 需要以高速率攻击网站才能实现其目标, 使得基于速率的自动化可以检测和缓解这类攻击。例如, 相较于普通用户而言, 暴力登录在通过单个 IP 地址登录失败时会以更高的速率进行登录。基于速率的阈值可以检测这些类型的帐户盗用尝试操作。类似地, 攻击不再存在的页面 (404 错误) 的内容剽窃者也会出现速率高于普通用户的现象。

基于已知的错误签名阻止

Cloudflare 通过为 600 万个网站提供保护, 可以在一个网站上检测到滥用僵尸的已知错误签名, 随后可以在其他所有网站上对其进行阻止。

总结

为了在不断变化的威胁环境中保持安全和“始终可用”，企业需要良好性能、大规模的智能安全性和分层防御，以便抵御拒绝服务、数据盗用和恶意僵尸。

由于人类一直关注着取舍平衡，通过减少“胖手指”并允许更多的员工在没有风险或不必要摩擦的情况下应对各种变化，使得部署、配置和调整安全策略方面的易用性影响着整体安全态势。

Cloudflare 的云安全性可抵御日益复杂的 DDoS 攻击，并抵御攻击者和恶意僵尸对数据造成威胁的尝试操作。



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

© 2017 Cloudflare Inc. 保留所有权利。
Cloudflare 徽标是 Cloudflare 的商标。所有其他公司和产品名称分别是与其关联的各自公司的商标。