CLOUDFLARE

电子书

预防宕机：DDoS 防御模型指南

内容

点击跳至章节

前言：混合办公环境中的 DDoS 防御

随着对更好、更快的应用程序和客户体验的需求日益增加，目前平均每家企业使用超过 1400 种不同的云服务 [1]。然而，云转型的副作用是攻击面不断扩大：数字服务越多，可供攻击者利用的“入口点”就越多。因多年全球疫情大流行而变得必要的混合办公（办公室和远程办公的结合）也是导致攻击面扩大的一个因素。

所有这些因素都在给资源紧张的企业带来更大压力。IT 和安全团队不仅需要提供更有韧性的应用程序和网络，他们还需要保护用户和设备，无论它们位于何处，以防御不断演变的威胁。

其中一些威胁包括更频繁、更长时间、更大规模的分布式拒绝服务（DDoS）攻击。2023 年 2 月，Cloudflare 检测并缓解了有记录以来[最大的 HTTPS DDoS 攻击](#)（71 Mrps）。我们的数据还显示，在 2022年，超大容量的 DDoS 攻击（超过 100 Gbps的攻击）每个季度都在[增长](#)。

在今天的经济状况和混合办公的现实背景下，企业需要重新评估自身的 DDoS 防御措施：
宕机、数据盗窃、网络渗透和财务损失的风险非常巨大。

研究表明，超过 60% 的宕机成本超过 10 万美元，15% 的成本超过 100 万美元 [2]。例如，由于一系列 DDoS 攻击导致的宕机，一家公司损失接近 1200 万美元 [3]。

这些现实使得 DDoS 防御对于各种规模的组织都至关重要。而且过去的人工方法已经不再足够。攻击可能是由人类发动的，但它们是由机器人执行的——要打赢这场战役，您必须用机器人对抗机器人。检测和缓解必须尽可能自动化。

本电子书探讨如下问题：

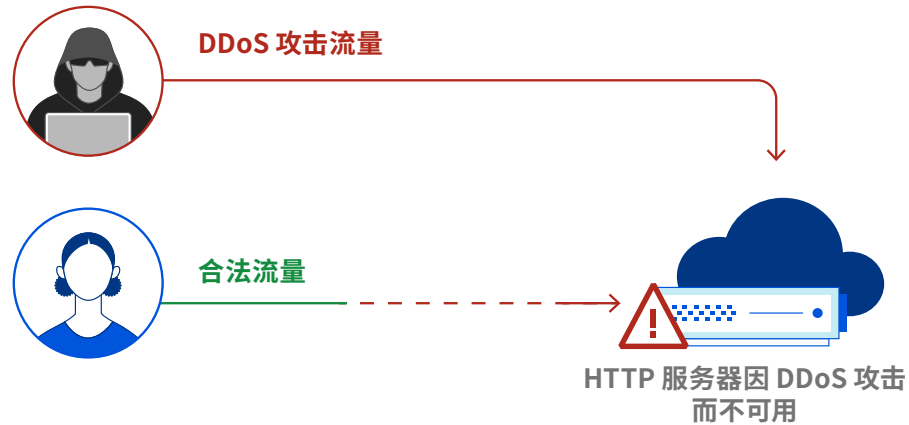
- 云 DDoS 防护的不同模式
- 克服始终开启云清洗的限制
- 一家财富世界 500 强公司如何利用 Cloudflare 挫败勒索 DDoS 攻击

了解基于云的 DDoS 缓解方法

DDoS 攻击是一种恶意的企图，旨在利用大量互联网流量淹没目标或其周围的基础设施，以破坏目标服务器、服务或网络的正常流量。一个有效的 DDoS 解决方案将准确地告诉您这个“交通堵塞”发生的时间、地点和方式——同时吸收和重新分配恶意流量，使其不会干扰合法流量。高流量的站点，以及不受保护的互联网资产和网络，都是常见的目标。

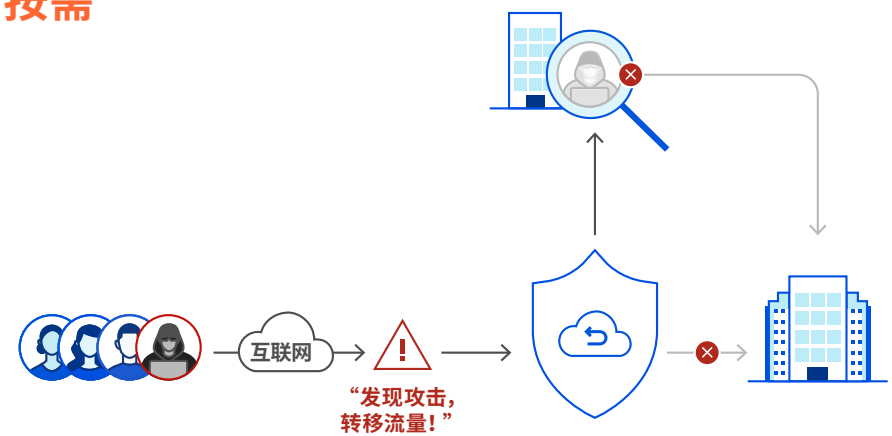
虽然 DDoS 攻击并不是新事物，但阻止它们需要新的方法。随着应用程序迁移到云端，本地 DDoS 解决方案的市场已经萎缩[4]——取而代之，更多的组织正在转向基于云的 DDoS 保护解决方案。

有多种基于云的保护方案，云提供商位于组织的应用程序和基础设施前面，将所有流量重定向到清洗中心以进行“清洗”。只有合法的流量才会发送回客户端。这种“云清洗”操作可以通过两种方式激活：***按需***或***始终开启***。



图：应用层 DDoS 攻击导致对合法用户的服务被拒绝

按需

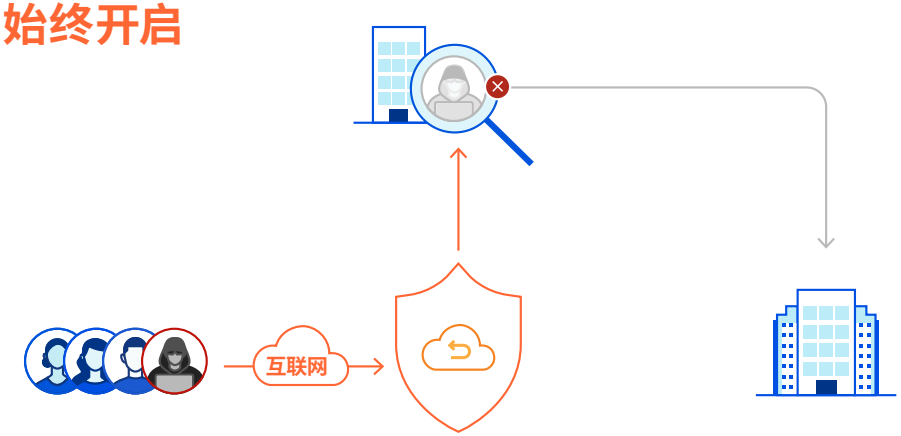


在“和平时期”，按需进行的云清洗确保所有流量都能到达应用程序和基础设施，而不进行任何重定向。只有在受到 DDoS 攻击的情况下，流量才会被转移到云清洗提供商。

如果入站流量超过预先配置的阈值（例如链路容量的 70%），或者检测到大规模攻击，那么按需云缓解模式就会被激活，流量会被转移到最近的清洗中心进行处理。

对比

始终开启



这种基本上不需要动手的云清洗方法总是将流量通过云提供商的数据中心以进行威胁检查——即使在和平时期。

始终开启模型有助于最大限度地减少从检测到缓解的时间，而不会出现任何服务中断。

虽然按需和始终开启技术都提供了不同的好处，
但它们在不同的情况下都会存在限制——如下节所述。

云清洗方法的常见限制

按需云清洗的挑战

攻击响应延迟：

- 按需模式是在发生 DDoS 时将流量重新路由到云提供商。除了手动响应攻击（例如告知提供商开启服务）的时间外，完成切换也可能需要几分钟的时间。如果没有及时开启按需保护，则有可能造成重大影响。

长期成本增加：

- 按需云保护供应商通常按攻击流量的字节数收费。虽然您仅为使用的服务付费，但如果组织遭到更频繁的 DDoS 攻击，最终可能导致更高的费用。

可能错过攻击：

- 未超过利用率阈值的 DDoS 攻击可能不被发现，导致网络链路拥堵，影响合法流量。
- 网络链路也不监测 SSL 和应用层的更高层协议攻击。

始终开启云清洗的挑战

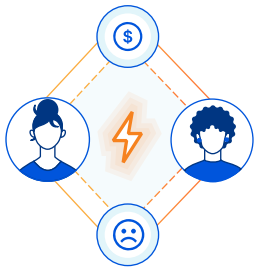
延迟问题导致了负面的用户体验：

- 许多云 DDoS 缓解提供商拥有一组专用于清洗网络流量的远程数据中心，这些数据中心远离攻击流量的源头。较少清洗中心通常造成较大的延迟。这种流量回传也会造成明显的延迟。
- 专门用于 DDoS 清洗的数据中心往往也只检查网络层。对于位于其他层的功能，例如 Web 应用程序防火墙或内容缓存，流量通常在另一个数据中心处理，因而导致更大延迟。

总拥有成本较高：

- 一些始终开启的云清洗解决方案网络容量有限，可能会以提高定价的形式将其带宽限制转嫁给客户。提供商还可能收取专业服务费。

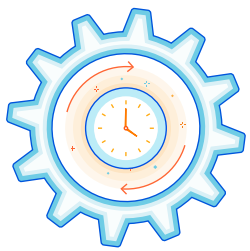
时间就是金钱：宕机和延迟对企业有何影响



91% 的组织表示，**宕机成本高达 30 万美元/小时**，包括业务损失、生产力中断和修复工作 [5]

44% 的游戏玩家遇到延迟时的反应是**退出正在玩的游戏**并稍后再试，**24% 的人将退出并玩其他游戏** [8]

对于知名电子商务公司，宕机成本可能高达 **22 万美元**/分钟 [6]



64%的 IT 决策者表示，提供更快、更方便的客户体验的需求**“对其技术基础设施而言是一个重大或主要的负担”** [9]

90% 的购物者会放弃一个不能在“合理时间内”加载的**网站，57% 的人将离开并从一个类似的零售商处购买** [7]

实现云 DDoS 防御的全部承诺——并防止因宕机而导致的收入损失

我们提供由智能全球网络驱动的统一云平台，防御 DDoS 威胁的方式如下：

按需进行的云清洗依赖于人工干预，增加了缓解响应的时间。相比之下，始终开启的云 DDoS 保护更全面，但许多始终开启的云 DDoS 保护提供商依赖于遥远的清洗中心，这会增加用户体验的延迟。

Cloudflare 通过一个统一的安全平台来解决这些限制——平台包括三层 DDoS 防护（第 3、4 和 7 层），以及对本地、云托管和混合网络的流量加速。攻击流量在靠近源头处缓解，从而为最终用户提供无缝、高性能的体验。

网络驱动的安全

Cloudflare **在超过 285 个城市拥有数据中心，网络容量达到 197 Tbps**（相比之下，一款知名的始终开启 DDoS 缓解服务仅有不到 40 个清洗中心和 20 Tbps 的网络容量）。攻击在到达您的网络之前就会被我们的网络自动吸收，大多数恶意流量在**不到 3 秒**的时间内被阻止。不需要进行回传。

可用性、可见性和自助服务

Cloudflare DDoS 保护是以服务形式提供的，这意味着不需要资本支出投资或硬件生命周期管理。

此外，它是**可自助服务的，通过单一仪表板**提供自定义配置能力。

大规模威胁情报

看到更多，保护更多：近 20% 的 Web 在 Cloudflare 上运行。客户受益于我们全球网络的规模和情报，我们的网络**每天阻止超过 1120 亿次网络威胁**。

先进的机器学习模型不断提高我们的防御能力，让我们代表您领先于新兴威胁。

业内认可的 DDoS 防御

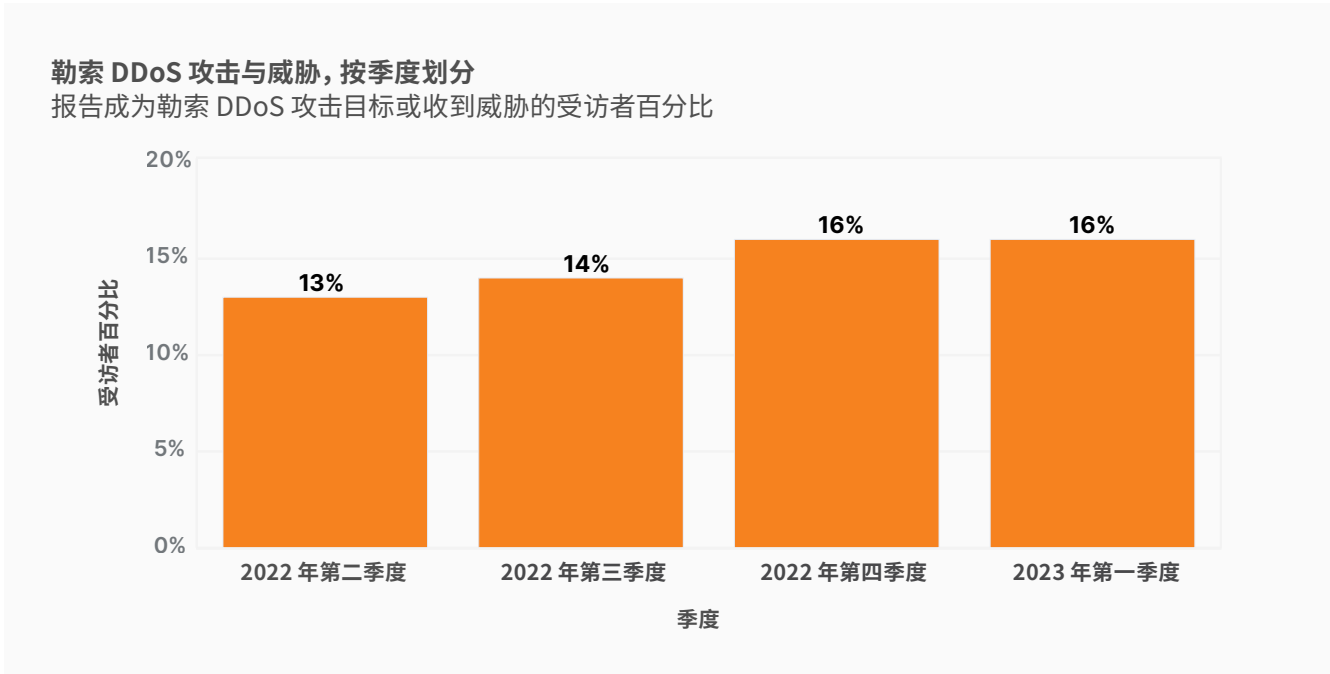
Cloudflare **在 2022 年 GigaOm Radar 的 DDoS 保护报告中被评为领导者**。报告评估了九家不同的提供商，其中 Cloudflare 的综合排名最高。Cloudflare 还在 **The Forrester Wave™：DDoS 缓解解决方案（2021 年第一季度）报告中被评为“领导者”**。

Cloudflare 在包括安全运营中心、响应自动化、性能等的 15 项标准中获得了最高分数。

案例研究：某《财富》世界 500 强公司成为勒索 DDoS 攻击的目标

勒索 DDoS（RDDoS）攻击，也称为勒索敲诈，是恶意行为人试图通过威胁要对个人或组织发动 DDoS 攻击的方式来勒索钱财。在 2022 年，勒索 DDoS 尝试的数量稳步增加，而在 2023 年第一季度，超过 16% 的 Cloudflare 客户在 DDoS 攻击中收到了威胁或勒索要求。

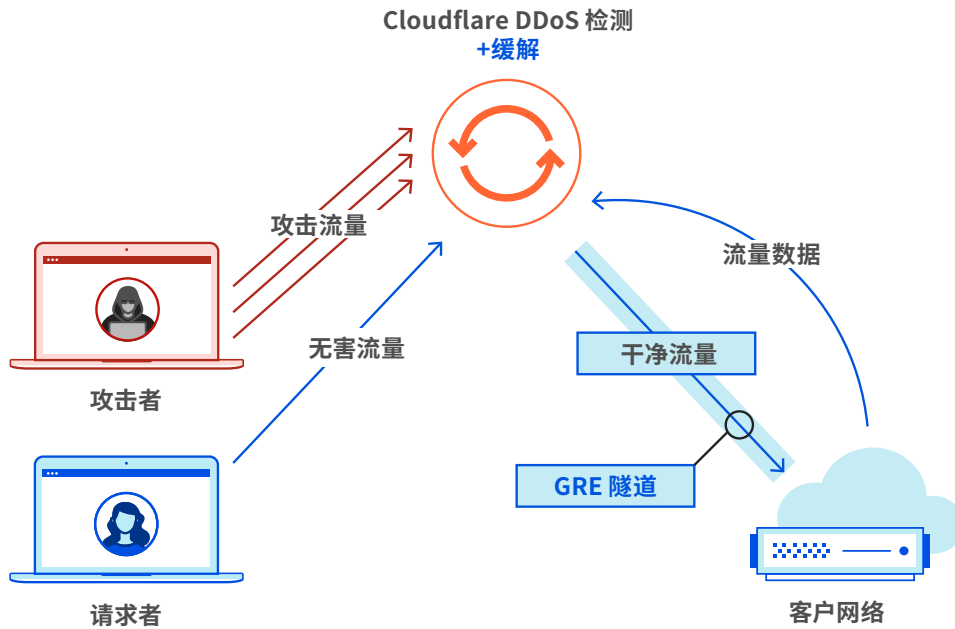
尽管常常与勒索软件攻击混淆，但勒索 DDoS 攻击的工作方式不同，而且更容易执行：它们不需要欺骗受害者打开电子邮件或点击链接，也不需要入侵网络或在企业资产中取得立足点。勒索软件即服务的日益普及也使得勒索 DDoS 成为攻击者一个低成本、低风险的选择。



2020 年底，在使用 Cloudflare 进行 DDoS 缓解之前，一家《财富》世界 500 强公司 被自称是 Lazarus Group（据称是由朝鲜政府运作的网络犯罪集团）发动了一次 RDDoS 攻击。攻击者最初发送了一封电子邮件，要求以比特币支付赎金，并给出一周“支付期限”，否则将发动第二次更大的攻击，而且赎金会增加。

在收到勒索信并发现对其全球数据中心之一的流量显著增加后，该公司联系了自己的按需清洗中心服务。该公司花了 30 多分钟来激活提供商的服务，并将流量重定向到清洗中心。激活该按需服务也造成了网络故障，导致多起事件。

在经历了初次攻击和面临按需服务提供商的挑战后，该公司决定采用 Cloudflare Magic Transit——Cloudflare 针对网络层 DDoS 攻击的始终开启保护。尽管攻击者承诺要发动第二次大规模攻击，但其始终未发生。



Cloudflare Magic Transit 提供网络层 DDoS 保护

“关键区别之一是，我们所看到的攻击和流量分析是原有提供商无法提供的。我们看到从未被发现的攻击被自动缓解。”

事件响应和取证团队
某财富世界 500 强公司

总结

后疫情时代， DDoS 攻击的频率和复杂性不断增加，维持合法流量的正常流动对于保护企业收入非常重要。Cloudflare 能够快速、轻松地防御攻击，而不会出现其他供应商常见的延迟问题或高成本，让始终开启的云防御成为轻松的选择。

要进一步了解利用 Cloudflare 防御网络 DDoS 攻击， 欢迎申请演示。

要进一步了解这个内置 Zero Trust 功能、DDoS 缓解、网络防火墙和流量加速的单一全球网络， 请点击这里。

来源

1 Sam Langrock。“云计算使攻击面管理复杂化”。Recorded Future，2023 年 4 月 3 日，
https://www.recordedfuture.com/the-cloud-has-complicated-attack-surface-management

2 “Uptime Institute 的 2022 年宕机分析发现，由于行业遏制宕机的努力不足，宕机成本和后果不断恶化。” Uptime Institute，2022 年 6 月 8 日，https://uptimeinstitute.com/about-ui/press-releases/2022-outage-analysis-finds-downtime-costs-and-consequences-worsening

3 Catalin Cimpanu，“遭遇 DDoS 勒索企图之后，Bandwidth.com 预计将损失高达 1200 万美元”。The Record，2021 年 11 月 1 日，
https://therecord.media/bandwidth-com-expects-to-lose-up-to-12m-following-ddos-extortion-attempt

4 David Holmes 和 Joseph Blankenship 等人，“The Forrester Wave™: DDoS 缓解解决方案，2021 年第一季度”，Forrester，2021 年 3 月 3 日

5 Laura Didio，“企业宕机的成本”，TechChannel，2021 年 9 月 30 日。
https://techchannel.com/IT-Stratgy/09/2021/cost-enterprise-downtime

6 “美国顶级电子商务网站的宕机成本”，Gremlin，2023 年 5 月 8 日访问，
https://www.gremlin.com/ecommerce-cost-of-downtime

7 Stephanie Crets，“大多消费者会放弃加载缓慢的电子商务网站”，DigitalCommerce360，2020 年 8 月 1 日。https://www.digitalcommerce360.com/2020/08/21/most-consumers-abandon-a-slow-loading-ecommerce-site

8 Mathieu Duperre。“44% 的玩家对延迟的反应是退出游戏——我们能做什么来阻止这种情况？”，PocketGamer.biz，2022 年 10 月 24 日，https://www.pocketgamer.biz/asia/comment-and-opinion/79974/44-per-cent-of-gamers-respond-to-latency-by-quitting-their-games-what-can-we-do-to-stop-this

9 “Infinity Data 和征服延迟的战斗”。Hazelcast 和英特尔，2019 年 11 月。https://hazelcast.com/resources/infinity-data-report

010 8524 1783 | enterprise@cloudflare.com | www.cloudflare.com

CLOUDFLARE