CLOUDFLARE®

如何构建基础设施以提供卓越的网络体验

010 8524 1783 | enterprise@cloudflare.com | www.cloudflare.com/zh-cn/

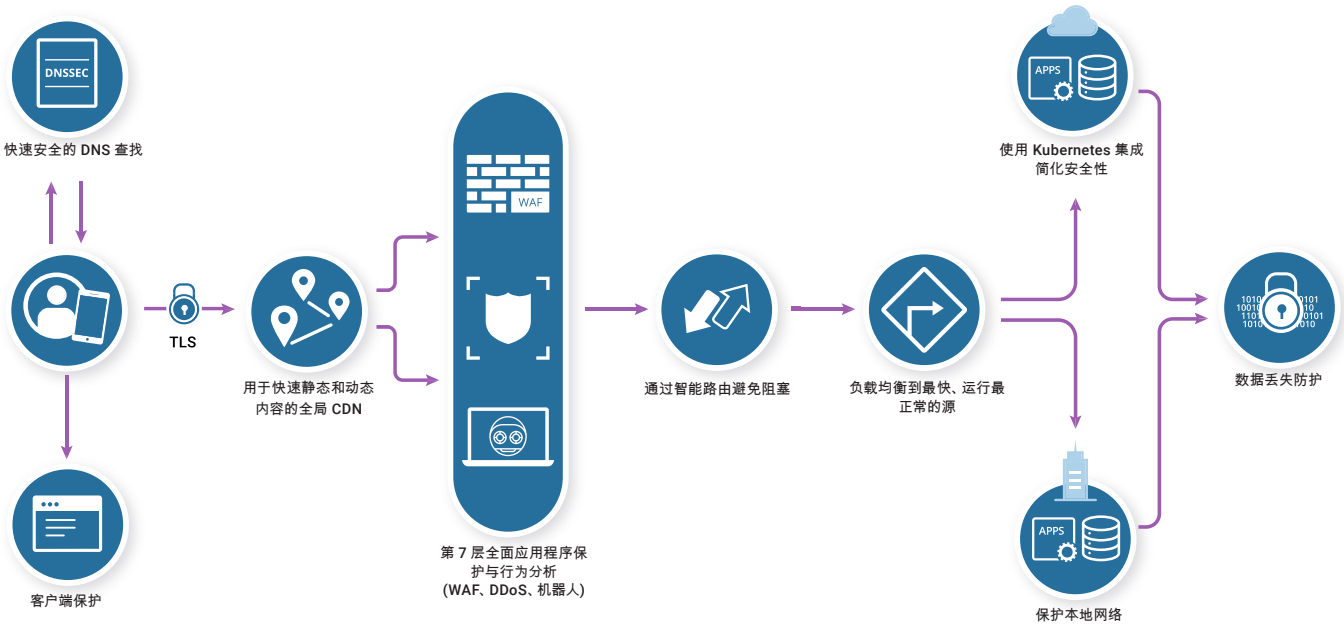
目录

简介

向全球客户群提供卓越的网络体验，不再是一个可有可无的选项。随着对 Web 服务和应用程序的需求增加，企业既要满足客户的需求，也要确保网站和应用程序尽可能安全、快速、可靠。

在这个转变中，企业面临着新的挑战和增长机遇——从预测和满足客户的数字需求，到针对基于 Web 的攻击建立强大的防御能力、克服延迟问题、防止站点中断以及维护网络连接和性能。

构建卓越的网络体验不能仅依靠单一工具或产品套件，还需要集成全方位的安全态势和性能特征，以便降低延迟和提高网络可靠性，如下图所示：

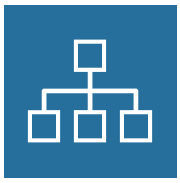


要满足客户需求并提供安全无缝的用户体验，现代企业需要采取这五个重要步骤：

.

第一步：

确保客户连接安全、快速、可靠



DNS

对每一个基于互联网的业务而言，DNS 都是重要组成部分，但其往往会被忽略，直到出现问题才会受到关注。随着 DNS 攻击日益普遍，企业开始意识到，缺少富有弹性的 DNS 在其整体安全策略中造成一个薄弱环节。如果企业的应用不可用，无法被客户找到，那么为构建和保护 Web 资产而投入的数百万美元变得毫无价值。

DNS 挑战：

高延迟：当企业的网页频繁从多个域加载资源时，解析每个被请求域的时间将增加，企业就会面临 Web 性能问题。

自有 **DNS** 基础设施：自有 DNS 维护成本高昂，可能会因全球分布的客户群解析较慢而增加延迟，不能全面防御复杂高级的 DNS 攻击。

小型网络 **DNS** 提供商：在选择 DNS 解决方案时，企业往往会错误地选择一个并不拥有大型网络、不能在所有数据中心执行 DNS 解析的提供商。此举可能会限制性能和可靠性，对需要接触全球多个地区客户的企业尤甚。

DNS 提供商必备要素

集成安全解决方案：鉴于 DNS 威胁复杂多样，要有效缓解 DNS 攻击，企业需要一个集成安全策略，其中包括 DNSSEC、DDoS 攻击缓解和 DNS 防火墙。对于希望维护自有 DNS 基础设施的大型企业，可部署 DNS 防火墙并同时使用辅助 DNS。这种配置能为本地 DNS 基础设施增加一个安全层，有助确保整体 DNS 冗余。

快速 **DNS** 解析：有些企业考虑基于云的托管 DNS 提供商，那么所选择的供应商必须能实现快速 DNS 解析以及基于位置的路由或动态路由，从而最大化性能和可用性。

冗余：一些企业选择通过单一提供商托管 DNS 记录，由于依赖于单点故障，更容易发生中断。为了最大化弹性，企业不仅需要借助多个独立的托管 DNS 提供商，还要确保这些提供商使用不同的名称服务器设施。

客户端安全

目前在用户浏览器上执行和渲染的代码中，多达 70%[1] 来自外部不受监控的 JavaScript 集成，为各种客户端攻击开辟了新的广阔通道，例如 Magecart、跨站点脚本（XSS）、信用卡盗刷（skimming）、网站污损和其他更恶劣的手段。

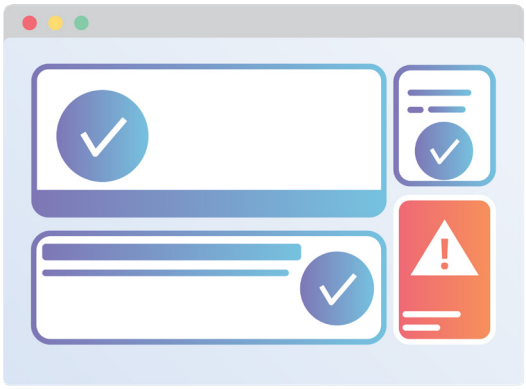
对客户端威胁，服务器端安全工具的能见度有限，无法阻止攻击或修补这些漏洞。对于拥有 Web 站点的公司而言，至关重要的是，能够部署和维护专门的客户端保护措施，以便确保其网站免受这些常见并快速演变的威胁侵害。

客户端攻击

跨站点脚本**(XSS)**： XSS 攻击者向合法网站中附加或插入恶意代码，通常是为了窃取用户登录凭证，获得其他敏感信息，或控制用户的浏览器。

Magecart 攻击：Magecart 攻击属于“数据盗刷（skimming）”，攻击者将恶意代码插入网站中，从网络支付表单中窃取机密用户数据（例如信用卡号码、密码等）。对于企业而言，这种攻击可能更难检测，因为攻击者可将恶意代码隐藏在无害代码中，或者对被盗的数据进行编码，以便不知不觉地将其返回给攻击者。

欺骗：欺骗是指假冒可信来源以掩盖恶意通信的手段，让攻击者得以窃取敏感的用户数据，重路由流量以发动 DDoS 攻击，或在未经授权的情况下访问某个组织的系统或网络。



[1] 马克·伯明翰（Mark Bermingham）。“通过 NGINX Plus 的 Tala 安全认证模块重新定义客户端安全”，NGINX，https://www.nginx.com/blog/redefining-client-side-security-tala-certified-module-nginx-plus/

客户端安全解决方案的必备要素

端对端保护：企业需要同时保护后端基础设施以及前端流程，而非锁定任何一种客户端威胁。

尽可能减少对性能的影响：部署和管理严格的安全协议是许多企业最关心的问题，但很重要的一点是，这些安全产品不能破坏 Web 性能，因为反应迟钝的网站会赶走潜在客户，导致跳出率增加和转化率下降。

TLS

存储和传输敏感数据的企业必须设法保护数据，以防泄漏、滥用和失窃。TLS 网络协议（亦称“SSL”）通过加密公共网络上的通信和验证受信任方的身份来帮助实现这一点。这些协议旨在维护客户的隐私，保护数据以防第三方监视和篡改。

TLS 挑战:

管理 **SSL/TLS** 证书: 尽管 SSL/TLS 证书旨在验证受信任方的身份，但这些证书可能会被恶意行为者破坏和操纵。由于通常任何人都能买到这些证书，攻击者可使用证书来假冒某一个受信任方，绕过安全程序，并访问到机密数据。

保持最新状态：SSL/TLS 的每一个后续版本都试图修补已知的漏洞，并帮助加强网站防御攻击的能力。如果企业使用这些加密协议的过时版本——如 TLS 1.1 或 1.2——企业可能会无意中允许恶意行为者利用现有漏洞发动攻击。今天，Alexa 排名前 1000 个网站中仅 22% 使用最新版本的 TLS。[2]

[2] 拉尔夫·霍尔兹（Ralph Holz），Johanna Amann（约翰娜·阿曼），Abbas Razaghpanah（阿巴斯·拉扎帕纳）和纳塞奥·瓦利纳-罗德里格斯（Narseo Vallina-Rodriguez）。“TLS 1.3 时代：通过主动和被动方法衡量部署和使用”，悉尼大学，https://arxiv.org/pdf/1907.12762.pdf

确保遵守法规和标准：很多企业必须遵守《通用数据保护条例》(GDPR) 和《加州消费者隐私法》(CCPA) 制定的标准，两者都规定了帮助保护客户数据免遭窃取或滥用的准则。如果企业未能妥善加密客户数据流量，有可能面临恶意软件和数据泄露等潜在威胁。

TLS 解决方案必备要素

轻松部署：对于需要手动配置 SSL/TLS 协议的企业，意外的错误配置可能会阻止客户访问这些企业的网站。提供商应能简化 SSL/TLS 部署，实现轻松检测和回滚（以防出现错误），并自动更新 TLS 协议到最新版本，以便修补最新的已知漏洞。

灵活性：随着企业的安全需求发展，企业可能需要一个能提供多种类型证书配置的 SSL/TLS 提供商，从证书权威机构颁发的证书到自签名证书。

合规满足：全方位的 SSL/TLS 检查允许企业识别可能隐藏在加密数据流量中的潜在威胁。通过快速定位和抗击这些威胁，它们能保护客户数据，免遭篡改和窃取，同时确保遵守 GDPR 和 CCPA 等法规。

第二步

加速用户体验

全局 CDN

对于那些正在寻找简单而有效的方法来扩大其影响力的全球企业来说，比起投资于远程托管设施，CDN 是一个合理的替代方案。借助 CDN，企业不必在全球构建昂贵且难以管理和维护的庞大基础设施，就能触及广大分散的消费者群体。

CDN 挑战

安全与性能之间的权衡：虽然 CDN 应该在面对网络问题时具有韧性，并保护敏感数据免遭窃取和丢失，但集成安全特性带来额外的延迟，会导致性能折衷。

缺乏实时分析：实时分析要么难以获得，要么明显滞后，影响到企业洞察其 Web 资产性能的能力。

一体化架构：传统 CDN 使用一体化架构，配置改变往往需要一段时间才能传播到整个网络。此类延迟会让开发人员感到沮丧，因为他们需要快速实现和迭代这些策略更改。

CDN 提供商必备要素

性能提升：在评估一个 CDN 时，企业应首先运行测试，以确定在关键市场的性能具有可比性。每一个 CDN 提供商会给出好坏参半的结果——某些在其他地区性能更佳。完成初步测试后，企业应进行评估，考虑到在其他地区的提升，任何性能下降是否可以接受或忽略。

实时分析：是否能轻松收集分析和数据，了解企业 Web 域在世界各地的使用情况和用户体验。以及获得这些信息的延迟。

开发人员友好度：在决定 CDN 在数字基础设施建设中所起的作用时，开发人员和工程人员拥有话语权。企业应寻找提供无缝 API 集成，且定制配置不需外部供应商专业服务的提供商。

更快的路由

拥有全球客户群的企业需要确保其 Web 应用程序的性能。导致延迟的因素很多，从繁琐的安全协议到世界各地用户的网络条件欠佳。

智能路由根据网络阻塞情况和可靠性来选择路由，从而帮助缓解这些问题。它在 BGP 之上运行，测试可用路径，以确定哪一个路径提供卓越性能。通过避免不可靠的网络连接，它也能避免丢包，后者通常会导致服务缓慢和网络中断。

路由挑战

网络阻塞：网络阻塞可能局限于某些缺乏足够基础设施的地区，也会影响 ISP 的整个网络。在公众假期或全球性灾难等大流量事件中，更多用户涌向互联网以进行通讯或使用服务，从而增加阻塞。

网络延迟增加：较高的网络延迟会直接影响网站的速度和性能，继而降低整体用户体验，导致转化率减少和收入下降。

成本过高的解决方案：可从大型服务提供商购买私有租用线路和 MPLS（多协议标签交换）网络，为企业通信获得专用路由。虽然租用私有线路具备一定的优点，但其实施成本往往越来越昂贵，可能影响到盈利能力和其他业务关键服务的预算资源。

如何选择网络路径优化工具

资产性能提升：凭借合适的提供商，企业应能通过可用的最快链路交付 Web 流量，从而显著提升资产速度和性能，并改善最终用户的体验。

实时指标和分析：企业应当能通过实时指标和分析来评估任何潜在的路由问题，从而避免阻塞，优化路由，衡量全局性能提升，并增加正常运行时间——不管用户身处何地，使用何种设备，以及当前网络状况如何。

网络监测工具：为了降低延迟和绕过网络阻塞，企业可部署网络检测工具来识别潜在阻塞点并帮助对流量进行优先排序，确保最关键的负载到达预定目的地，并防止单一应用程序占用过多带宽。

移动优化

与使用台式电脑浏览网站的人一样，移动用户希望其移动设备上的页面加载时间不超过 3 秒，因此，任何基于 Web 的业务要取得成功，移动优化都必不可少。如果企业不能通过快速无缝的移动体验满足用户的期望，客户会转向其他地方。

移动优化挑战

图像优化欠佳：没有为小尺寸移动设备屏幕设置正确尺寸和格式的图像会导致页面视图扭曲并导致页面难以浏览，从而降低用户体验。图像尺寸越大，下载时间越长。因此，用户可能会发现页面加载时间增长，因为很多设备的屏幕分辨率不够高，或屏幕尺寸不够大，没有必要使用超高分辨率图像。

提高带宽利用率：文件越大消耗带宽越多，就要向托管服务提供商支付更多数据费用。如果企业不能为其移动资产应用适当的图像优化解决方案，可能会面临大量风险，从带宽成本增加到客户失去兴趣、转化率下降和收入减少。

繁琐的内部开发：Web 开发人员常常被要求协助为移动设备优化资源。这可能涉及为各种设备类型创建图像副本的人工过程。这不是一个理想的解决方案，因其会成为另一个需要随着时间推移而管理和维护的系统或过程。替代方案——部署专门的第三方图像优化解决方案——往往成本高昂，并可能降低功能利用方面的投资回报率。

移动优化解决方案必备要素

CDN 集成：移动优化应当与现有 CDN 服务无缝集成，允许企业利用缓存效益，并减少通过该服务获得冗余图像文件的依赖。正确的 CDN 能检测用户设备要求，“虚拟化”图像以缩小文件大小，并在尽可能接近移动用户的位置缓存图像，从而帮助提升移动性能。

内部维护对比第三方维护：考虑移动优化解决方案时，与可在内部构建和管理的解决方案相比，仔细考虑需要怎样的长期维护和更新。企业也应当考虑，这些优化解决方案是否能加以扩展，以便支持企业域以外的第三方存储地点。

第三步

增强基础设施的安全态势

Web 应用程序防火墙

即使对于积极努力保护其基础设施和数据的企业来说，有效实施安全措施也有可能极其困难——在如今每一个安全漏洞都可能造成攻击机会的情况下尤其如此。

拥有基于云的 Web 应用程序防火墙（WAF）后，企业能抵御零日攻击，并保护应用程序以防御常见威胁，如跨站点请求伪造（CSRF）、跨站点脚本（XSS）和 SQL 注入攻击。WAF 还允许企业通过设置规则来维持对其安全策略的精细控制，这些规则可以保护应用程序中的漏洞，并防御新出现的威胁。

WAF 挑战

启用和管理需要大量资源：对于开发良好的网络安全和保护业务关键应用程序，对基础设施应用最新修补至关重要。然而，由于来自无数供应商的修补数量庞大且推出速度极快，即使最大的安全团队往往也无法对整个基础设施进行修补。虽然 WAF 解决方案有助缓解这个问题，由于今天的 WAF 需要大量高水平的安全专业人员来处理这个过程，上手和管理往往需要投入大量时间和资源。

缺乏灵活性：在当今的威胁环境中，基于设备的硬件 WAF 是一种严重过时的安全解决方案。由于应用程序和数据大多驻留在混合环境中——包括本地基础设施和云——基于云的 WAF 已成为任何企业分层防御策略的关键组成部分。与硬件 WAF 设备不同，不管应用程序和基础设施托管在何处，基于云的 WAF 都能提供保护，防御基于漏洞的攻击。

敏捷性：当今世界，保护资产和数据成为安全团队和恶意行为者之间的持续竞赛，敏捷性是关键所在。基于硬件的 WAF 无法提供一种敏捷的机制，以便创建规则并快速传播到所有基础设施。从某个漏洞被公布到应用补丁以防御尝试利用这个漏洞发动的攻击，两者之间的时间非常关键。

WAF 解决方案必备要素

易用性：在选择、启用和管理 WAF 时，可用性至关重要。启用一个 WAF 不应耗费数周乃至数月，管理不应需要一群专业人员。此外，企业可能需要考虑提供无缝 API 集成的 WAF 提供商。

实时威胁情报：对于基于硬件的 WAF，主要缺点之一是缺乏有关威胁和攻击的实时上下文。企业也许能将威胁情报源与基于硬件的 WAF 集成在一起，但这样做只能提供一个被动——而非主动——的解决方案。鉴于威胁环境快速演变，实时威胁情报对于帮助企业掌握最新威胁至关重要。WAF 应当包括有关全球和多种威胁的实时上下文，不仅注意威胁情报数据集的规模，也要注意数据的多样性。

全面覆盖：虽然攻击者常常试图利用包括 OWASP 前十在内的常见漏洞，他们对关键漏洞和零日漏洞的兴趣日益浓厚。全面的 WAF 解决方案应当包括定期更新的托管规则集，以便自动阻止试图利用零日漏洞或其他关键漏洞的攻击。

机器人缓解

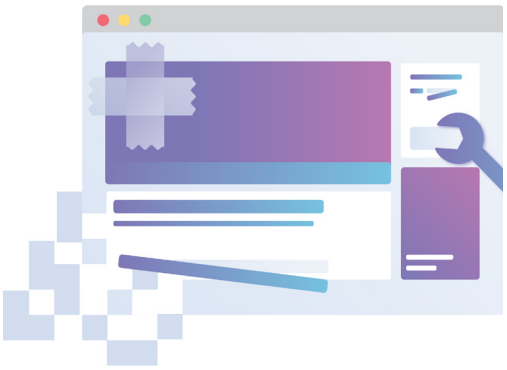
恶意机器人会对基于 Web 的业务造成严重破坏，不仅会危及敏感数据并破坏整体客户体验，还会直接影响企业的运营成本。随着机器人攻击日益复杂，区分真正的用户活动和自动化的机器人活动变得越来越困难，这使企业面临比以往更大的风险。恶意机器人活动会对网站产生威胁，压垮 Web 服务器、扭曲分析数据、阻止用户访问网页、窃取用户数据、发送垃圾信息、破坏品牌诚信并影响到客户留存和收入。

然而，并非所有机器人都是有害的。实施机器人管理解决方案后，企业能区分有用和有害的机器人活动，防止恶意行为影响用户体验。

机器人挑战

基础设施成本高企：任何 Web 流量都是企业的有形成本，因为企业需要托管内容、部署服务器并支付存储和计算费用。不幸的是，在 Web 资产成为恶意机器人活动的目标时，这些成本就会增加。对于 SEO、客户支持和其他有用任务，善意机器人不可或缺，但恶意机器人会抓取内容和破坏服务，从而导致过高的带宽费用。

用户体验欠佳：客户会强烈感受到恶意机器人对企业的影响。他们的帐户可能会被锁定，被指控进行欺诈交易，或者完全不能访问某个企业的网站。因机器人活动而过载后，服务器将无法向合法用户提供快速的页面加载，导致虚拟购物车放弃率提高，跳出率增加，转化率下降，以及客户参与度、留存和收入的整体损失。



分析失实：除了降低用户体验和导致基础设施成本飙升外，恶意机器人还会扭曲分析数据，掩盖有关企业 Web 性能的真实情况。 恶意机器人活动往往是低质量的，会对企业的综合分析数据造成负面影响（例如，人为夸大页面浏览量），阻止企业就流量模式和性能指标获得有价值的洞察。

机器人缓解解决方案必备要素

准确检测：要抗击恶意机器人，企业需要能够准确识别出其 Web 资产上的机器人活动。一些最准确的检测方法将威胁情报与行为分析、指纹识别和机器学习结合起来，能在不干涉真正用户活动或破坏用户体验的情况下帮助企业监测恶意机器人活动。

无缝集成：如果需要冗长而复杂的配置，即使是全面的机器人缓解策略也会变得毫无用处。机器人缓解解决方案应能轻松、快速地与任何技术栈、安全策略（包括 DDoS 攻击缓解）和 CDN 集成在一起，以便客户在不明显影响用户体验的情况下获得升级攻击保护带来的益处。

多样化缓解方法：随着恶意机器人行为者变得日益复杂和精密，企业需要调整缓解策略，以确保尽快检测和阻止机器人活动。由于没有任何一种策略能阻止所有类型的恶意机器人行为，有必要实施广泛的检测和缓解方法，包括如下一种或多种：阻止所有机器人流量，将善意机器人列入白名单，以 CAPTCHA 验证码挑战疑似机器人，维护所有站点流量的日志，对所有用户实施额外验证，将机器人重定向到替代内容。

DDoS 攻击防护

DDoS 攻击会消耗目标设备和互联网之间的所有可用带宽，不仅会导致严重的服务中断，还会使客户无法访问企业的资源，从而对企业造成明显的负面影响。

为保护 Web 服务器，反向代理帮助阻止攻击者识别并锁定服务器的 IP 地址。对于更复杂的第 7 层 DDoS 攻击，Web 应用程序防火墙（WAF）能充当反向代理，保护目标服务器免受某些类型的恶意流量攻击。

一些公司创建或部署自己的反向代理，但这要求密集的软件和工程资源，以及对物理硬件的大量投资。要获得反向代理的益处，一个更轻松、更经济的方式是使用提供全局服务器负载均衡的 CDN，企业可在不影响性能的情况下缓解较接近来源的 DDoS 攻击。

当然，只是保护 Web 服务器免遭 DDoS 攻击并不足够。企业往往会在公有或私有数据中心托管本地网络基础设施，这些基础设施也要受到保护以免受威胁。

DDoS 缓解的传统方式

清洗：清洗要求重新路由网络流量到位于指定地理位置的集中清洗服务器，试图从非恶意流量中过滤或“清除”出恶意流量。将所有流量重新路由到距离遥远的清洗中心会导致延迟明显增加，这对于大多数应用程序而言常常是不可接受的。

本地硬件设备：另一种 DDoS 缓解技术使用本地硬件设备来扫描流量并过滤出恶意请求。由于重新路由网络流量以通过设备来完成扫描过程的瓶颈，扫描硬件也会造成网络延迟并抑制性能。默认情况下，基于企业网络容量和设备硬件容量的组合，反 DDoS 设备常常会有带宽限制。

DDoS 缓解解决方案必备要素

缓解能力和缓解时间企业应当评估在不影响站点性能的情况下缓解 DDoS 攻击的现有能力。要吸收 DDoS 攻击产生的流量峰值，传统方式是构建昂贵的本地服务器群，但这些服务器易被大量攻击压垮。更有效的方式是部署基于云的缓解解决方案，此类解决方案提供抵御 DDoS 的无限容量，并能在网络边缘提供服务。

全程保护对比按需保护：使用按需缓解服务时，每当检测到潜在 DDoS 攻击，流量都必须重新路由到云缓解服务，用户仅在需要时为 DDoS 缓解支付费用。阻止 DDoS 攻击可能需要更长时间，因为流量峰值必须达到特定阈值，服务才会开始分析并由人工启用缓解服务。

相比之下，全程缓解持续路由和过滤所有站点流量，因此在任何时候都只有清洁流量到达用户的服务器。虽然成本高于按需服务，但全程缓解提供自动、不间断的保护，带来更快的响应时间。对于面临持续攻击的企业而言，全程缓解可能比按需保护更具成本效益。

一体化安全和性能：DDoS 攻击造成迟缓和中断，不仅会降低性能，还会破坏企业实现可持续增长的能力。企业需要考虑一体化安全和性能解决方案，这些解决方案能强有力地防御 DDoS 攻击，而不影响站点性能或消费者体验。

第四步

构建韧性基础设施，确保应用程序的高可用性

负载均衡

最大化服务器资源和效率需要微妙的平衡。服务器发生过载，或地理位置与最终用户距离太远，都可能对业务产生不利影响，因为延迟增加和服务器故障可导致收入损失、客户信任受损和品牌退化。

基于云的负载均衡将请求分配到多个服务器，以便处理流量峰值。负载均衡决策发生在网络边缘，更接近用户——以便企业提高响应时间和有效优化其基础设施，同时最小化服务故障风险。即使有一台服务器发生故障，负载均衡器会在其余服务器中重定向和重新分配流量，确保客户不会察觉到明显延迟或发现站点中断。负载平衡器还允许进行主动运行状况检查，从而识别性能不佳的服务器，并在故障实际发生前采取预防措施。

负载均衡挑战

应用程序运行中断和延迟：即使短暂的延迟都会明显影响参与度和转化率。延迟达到 30 毫秒左右，用户就会察觉到，即使短至 100 至 400 毫秒的延迟都会对消费者行为产生不利影响。[3]如果企业没有使用有效的负载均衡解决方案，当 Web 资产不可避免地遇到性能问题时，转化率和收入就有可能下降。

成本高企且灵活性有限：硬件负载均衡器价格昂贵且结构复杂，无法随业务增长而扩展。企业必须通过估计其 Web 资产将接收的流量来提前购买硬件设备。这意味着，企业常常需要为未使用的能力付费，或者被迫忍受加载时间和 Web 性能欠佳的状况，直至能增加在用设备数量为止。

复杂的流量管理：对于寻求最大化 Web 性能和可靠性的企业而言，获得对流量模式的可见性、管理区域流量和监测源服务器的运行状况至关重要。如果缺乏上述可见性，在工作异常的负载均衡解决方案无意中将流量路由到存在问题的服务器时，企业可能无法检测到，从而导致用户侧的严重延迟和中断。

[3] Brutlag, Jake。 “速度很重要”，Google AI 博客, https://ai.googleblog.com/2009/06/speed-matters.html

负载均衡器必备要素

与供应商无关的解决方案：提供多云和混合云支持的负载均衡器能帮助企业避免供应商锁定和复杂配置。基于云的独立解决方案可与云供应商的原生负载均衡器或传统硬件设备相结合，而非取代原有负载均衡服务，从而最大化灵活性，尽可能避免错误配置。本质上，这个解决方案应能让企业在其基础设施中动态分配流量——不管其源服务器位于本地，还是托管于多云或混合云环境。

主动运行状况检查和详细分析：在选择负载均衡解决方案时，可见性是关键所在——不仅能使企业确保服务器和应用程序运行正常，也能预防潜在延迟和中断。通过对流量模式和源服务器运行状况的详细分析，企业应能识别性能欠佳的服务器，优化其基础设施，实现高可用性和增加正常运行时间。

CDN 集成：在理想配置中，负载均衡解决方案与 CDN 协同工作，最小化延迟和带宽消耗。通过在网络边缘缓存静态内容，CDN 可从距离最终用户最近的服务器交付内容，既提高了整体 Web 性能，也减少了发送到源服务器的总请求数量。

第五步

检测异常行为并保护网络边缘的 Web 资产

数据丢失防护 (DLP)

随着云计算的出现，数据泄露已经成为现代企业最严重的威胁之一。数据泄露通常由有针对性的攻击、内部系统故障和简单的人为错误造成，可能会暴露敏感的客户数据、违反数据隐私法规并招致高达数百万美元的罚款和收入损失。

为了预防潜在敏感数据的潜在泄露和丢失，企业可部署一系列网络安全策略和产品。数据丢失防护（DLP）解决方案也能协助企业遵守 GDPR 和 CCPA ，以及其他旨在执行数据隐私政策和保护用户数据免遭未授权使用的法规。

DLP 挑战

部署复杂：传统 DLP 解决方案功能强大，但设置过程可能既复杂又耗时。企业需要定制 DLP 策略以适应特定用户群组和业务用例，这可能是一个痛苦的过程，需要大量外部支持和管理。此外，DLP 规则预防用户将数据传输到严格定义的边界以外，有可能在无意中阻止对必要数据的访问，从而影响员工生产力和协作。

缺乏全面的数据保护：DLP 策略需要同时涵盖受监管数据（应该保持机密的敏感数据）和不受监管数据（所有公开信息，可能包括部分保密数据）。然而，很多传统 DLP 产品没有考虑对不受监管的知识产权数据进行保护，导致企业在发生入侵时容易遭受重大损失。

可见性有限：为了确保机密数据得到全面保护，预防内部威胁，并遵守当地隐私法规，企业需要了解其数据被访问和传输的方式。如果过于关注现有或预期威胁，企业可能无法防范意料之外的恶意行为。

DLP 解决方案必备要素

简化部署和管理：基于硬件的 DLP 系统不但设置复杂，管理笨拙，还需要不断更新以应对持续演变的威胁。基于云的解决方案能帮助降低部署成本，并在应对新的数据威胁时保持灵活性，让企业更加了解其数据的使用和管理。

灵活性：企业采用的 DLP 解决方案应具有足够灵活性，可容纳各种用户群组和用例，同时易于部署、管理和维护。企业不应依赖于基于硬件的传统 DLP 解决方案，而应该考虑基于云的替代方案，后者能够提供更大的灵活性，并能更好地控制旨在保护公司和客户机密数据的策略和手段。

保护对比预防：尽管传统 DLP 系统专注于数据丢失防护，这些系统无法保护公司的机密数据免遭每一个外部和内部威胁破坏。下一代解决方案使企业不仅能缓解这些威胁，还能以更快、更有效的方式从数据泄露中恢复过来。

边缘可编程性

边缘计算使企业能将应用程序开发转移到网络边缘，使计算尽可能接近最终用户，最小化延迟、服务器资源和带宽使用。借助无服务器架构，企业可将基础设施配置和管理工作转移给第三方，从而使开发人员得以将精力集中于构建和部署应用程序、为现有应用程序启用自定义配置及帮助优化应用程序的开发和安全性。

边缘可编程性挑战

延迟和冷启动：由于无服务器计算以按需方式运行函数，启动某个函数可能需要数秒钟。这些“冷启动”可能造成不必要的延迟，要求企业采取积极的措施——例如找到变通方法来最小化冷启动的时间和频率——以免用户察觉到 Web 性能明显下降。

缺乏全球规模：如果基于 Web 的业务拥有广泛分布的用户群，应用程序必须在全球范围内部署。将应用程序转移到网络边缘有助企业更有效地触及用户，同时改善应用程序性能和交付。

资源应用不足：构建应用程序和自定义编程是复杂的过程，要求专门的内部资源，来自中央云提供商的适当服务器能力，以及测试时间。如果完成得不理想，就可能增加原型设计成本，导致企业无法将应用程序快速推出市场。

边缘计算解决方案必备要素

简化的可扩展性：边缘计算旨在通过从网络边缘交付资源来为最终用户最小化延迟，因此企业选择拥有全球网络的供应商变得至关重要。这不仅使企业能够扩大业务范围，提供更快的用户体验，还能简化部署过程，通过在边缘运行代码来触及所有位置的客户，而非逐个地区进行。

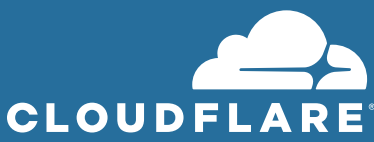
改善开发人员体验：开发新应用程序和增强现有应用程序应当是一个简单流畅的过程，允许开发人员快速而轻松地部署代码，而无需依赖于技术运营团队。

降低基础设施成本：凭借无服务器架构，企业不需再为未使用的服务器空间或空闲的 CPU 时间付费。取而代之，企业可将更多请求处理转移到这个网络，仅为所需的资源付费，从而能够显著降低基础设施成本。

Cloudflare 如何帮助企业提供卓越的网络体验

创建卓越的网络体验要求正确的安全和性能策略——这种策略不仅使企业能够加速内容交付，也能确保网络可靠性并保护其 Web 资产免受站点停机、数据失窃、网络漏洞和其他严重攻击影响。

Cloudflare 的网络遍布全球超过 90 个国家的 200 多个城市，提供一个可扩展的一体化全球云平台，帮助企业为其本地、云和 SaaS 应用程序提供安全性、性能和可靠性。要了解 Cloudflare 如何帮助保护您的网络业务，请访问 Cloudflare.com。



010 8524 1783 | enterprise@cloudflare.com | www.cloudflare.com/zh-cn/

REV: 200408