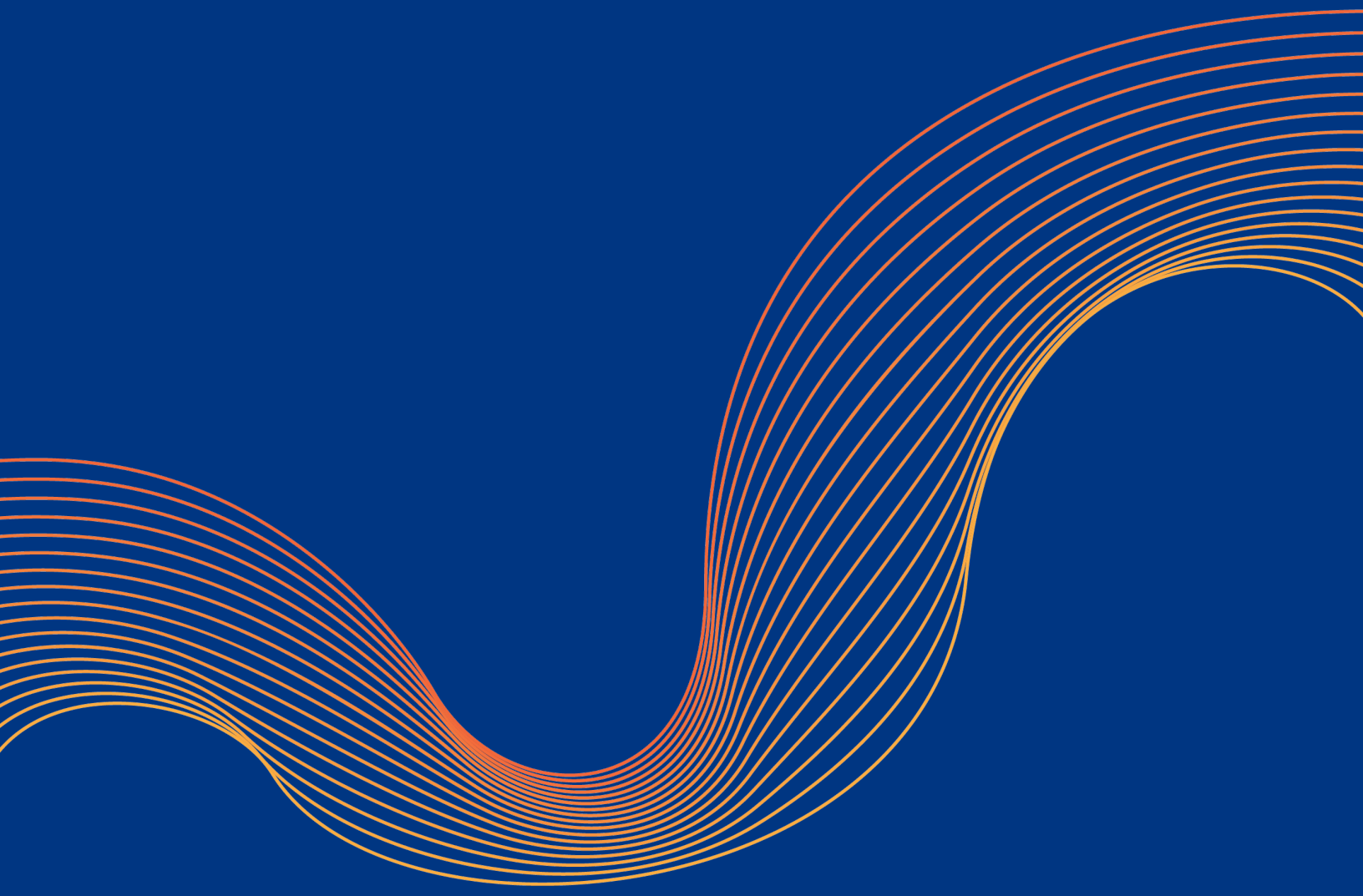
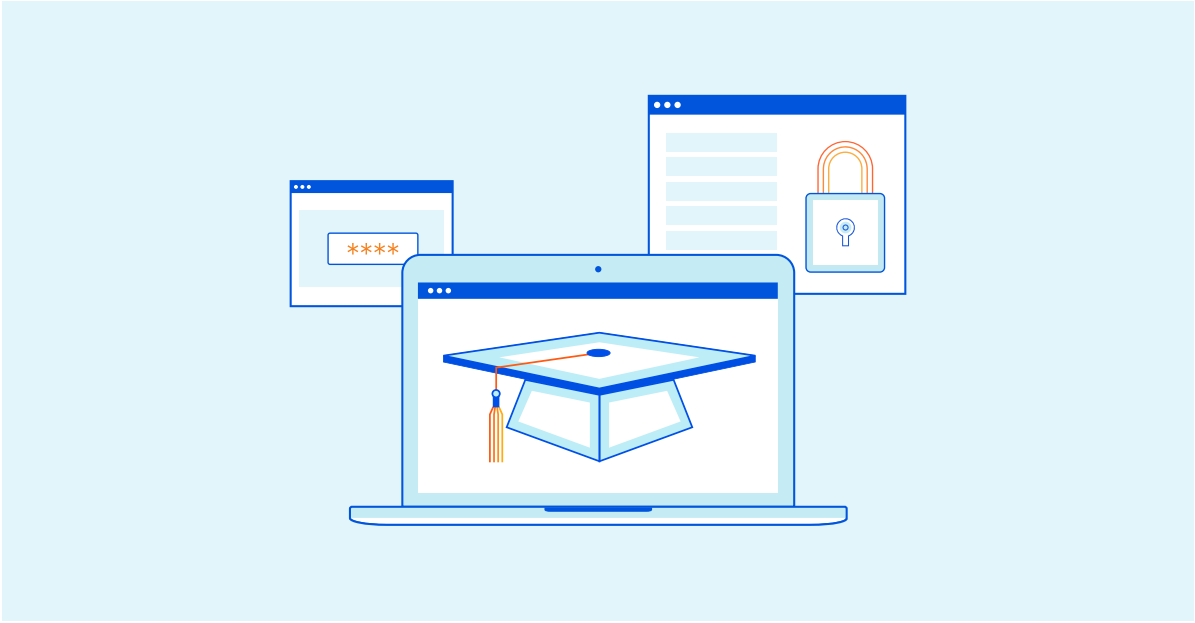
白皮书

CLOUDFLARE

设计安全且可扩展的远程教育基础设施



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



简介

近年来，远程教学已成为日益流行的教育模式。受新冠肺炎 (COVID-19) 疫情影响，许多教育机构被迫转移到远程教学模式，以确保学生和教育工作者免遭病毒伤害，这加快了向混合式和全面远程教学模式的转变。

远程教学需要一种与传统面对面授课截然不同的方法。教育工作者必须能够胜任各类教学方式和教学内容，包括讲座、视频、互动内容等。在远程教学模式下，课堂上的所有学生都需要能够快速并同时获得共享内容。

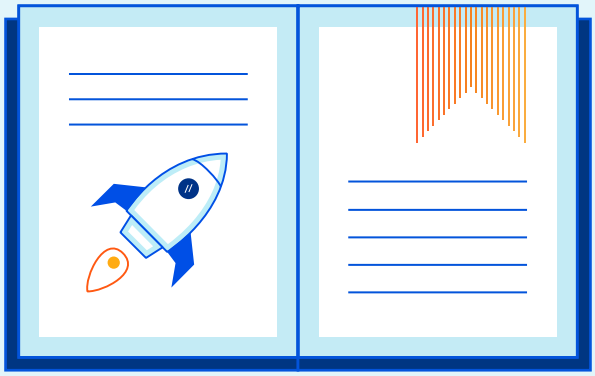
在技术方面，教育机构需要能够为各类内容提供支持，确保系统能在学生需要时正常运行。这需要应对一系列挑战，包括：

- 大规模交付内容
- 缓解分布式拒绝服务攻击
- 防止帐户盗用
- 阻止恶意内容和恶意软件

大规模交付内容

对于远程教学而言，学校的 IT 基础设施是其运营能力的重要组成部分。教育工作者需要能够同时向众多学生投放内容，确保延迟最低。

教育工作者需要能够向学生交付各类内容，包括从静态网页到动态内容（例如互动式在线学习工具和流式传输视频）的各类内容。教育机构的 IT 基础设施需要能够以高效且可扩展的方式将这类内容远程交付给学生。



静态内容

教育工作者需要向学生提供的内容中有一部分是静态的。这包括其中信息不会发生变化且不需要频繁更新的网页。

对于这类内容，IT 方面的主要挑战在于可扩展性和延迟。如果许多学生同时尝试访问相同的内容，Web 服务器能否正常工作？此外，Web 服务器所在位置也会对远程教学效果产生巨大影响。学生距离服务器所在地越远，交付内容的延迟就越久。

对于静态内容，创建本地缓存的能力有助于缓解这些挑战。如果学生经常访问某个页面，该页面的副本将可能保存在本地，以便学生在需要时快速访问。

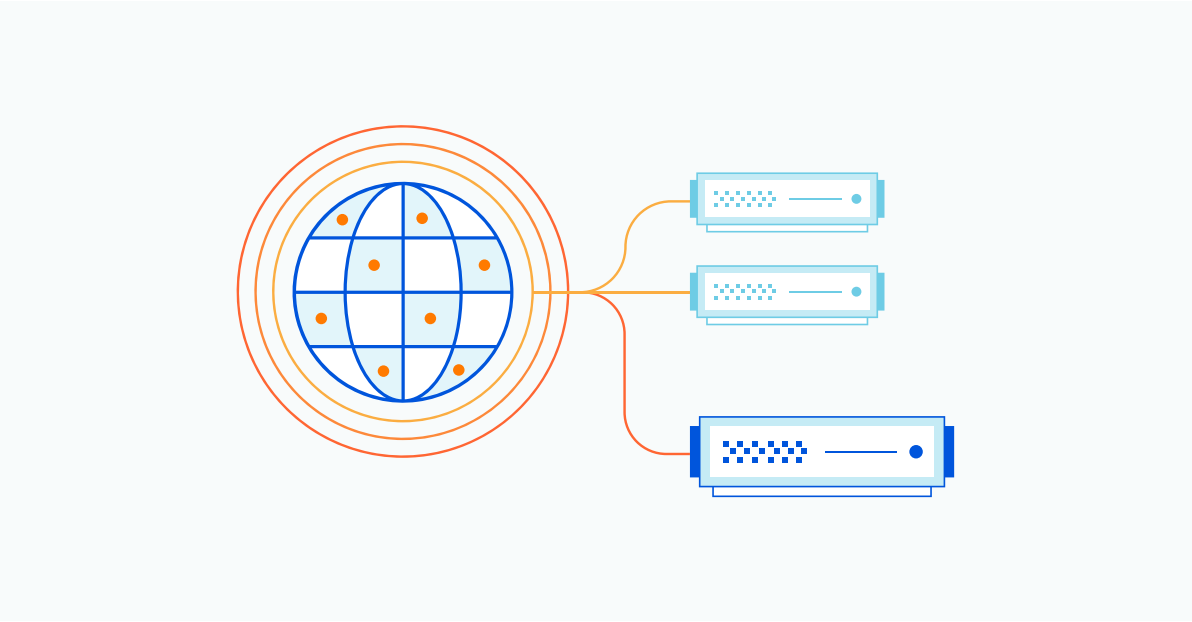
利用内容分发网络（CDN）可以规模化地实现缓存创建。
CDN 网络中的节点存储静态内容的本地副本，并定期检查更新。覆盖全球的 CDN 可以提供高效远程教学所需的可扩展性和低延迟。

动态和互动式内容

与静态内容一样，互动式在线学习和其他内容也可能存在扩展性问题。不过，CDN 节点网络不适合处理这类内容。如果内容需要频繁或接近持续的更新，那么 CDN 节点就会不断向主 Web 服务器查询更新版本。这样会增加用户的延迟，造成主 Web 服务器超负荷。

动态内容可扩展性问题可以通过负载平衡技术来解决。这时不会使用单个服务器来处理学生请求，而是使用多个服务器并在它们之间分配流量。这样就不会造成单个服务器超负荷，将延迟降至最低。

为确保高效，负载平衡服务器需要能够完全独立运行，或仅依靠其他负载平衡设备来运行。如果所有服务器都设置为使用同一个数据库服务器，那么该数据库服务器很可能成为瓶颈，额外的负载平衡服务器将几乎毫无用武之地。远程教学解决方案必须精心设计，确保能在需要时提供所需的规模，系统的架构方式能够提供负载平衡的全部优势。

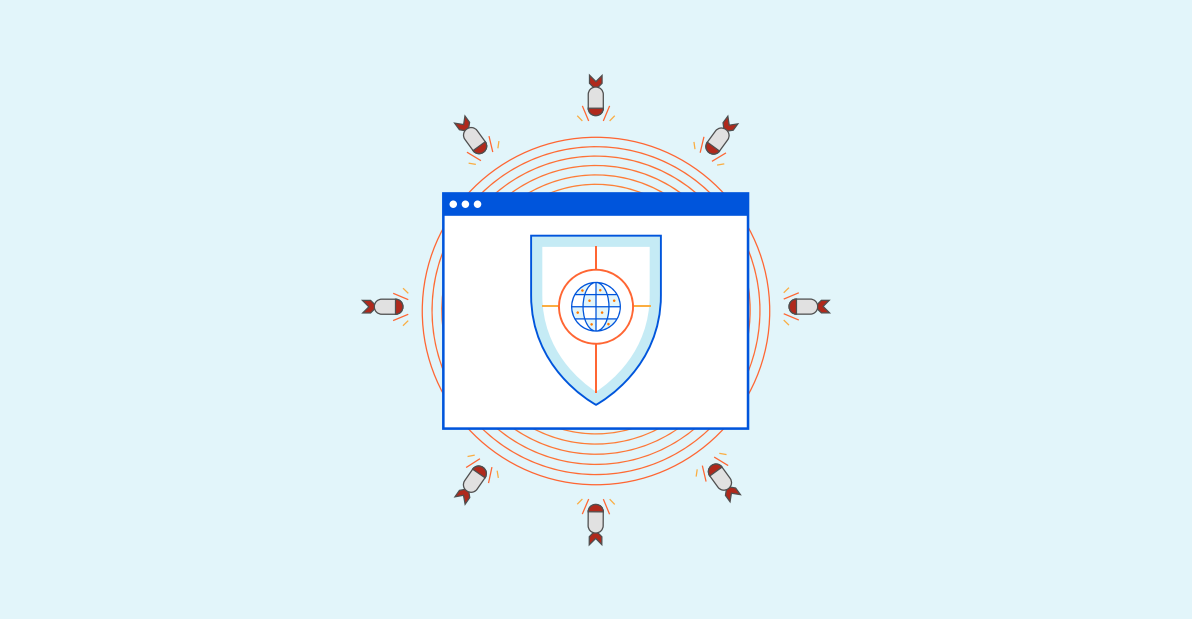


分布式拒绝服务攻击

当用户访问 web 资产时，其设备向一个映射相应资产所在域的 DNS 解析器发出查询请求。分布式拒绝服务（DDoS）攻击正变得日益普遍。随着物联网（IoT）和云计算的发展，攻击者获取联网计算能力的难度和成本越来越低。然后，这些遭到破坏的设备会被用于向服务器发送恶意流量，使其难以响应合法的请求。

在远程教育中，DDoS 攻击对提供服务的能力构成重大风险。在 2020 年上半年，许多教育机构改为采用远程教学模式，在线教育资源遭受的 DDoS 攻击数量增长了 350%[1]。

此外，一些 DDoS 攻击行为经过演变，已经包含了勒索元素。
攻击者可能威胁对机构发起 DDoS 攻击，并要求以支付赎金为条件停止攻击。虽然很多威胁都是无稽之谈，但教育机构如果没有 DDos 保护机制，就会觉得他们的基础设施面临着不容忽视的风险。

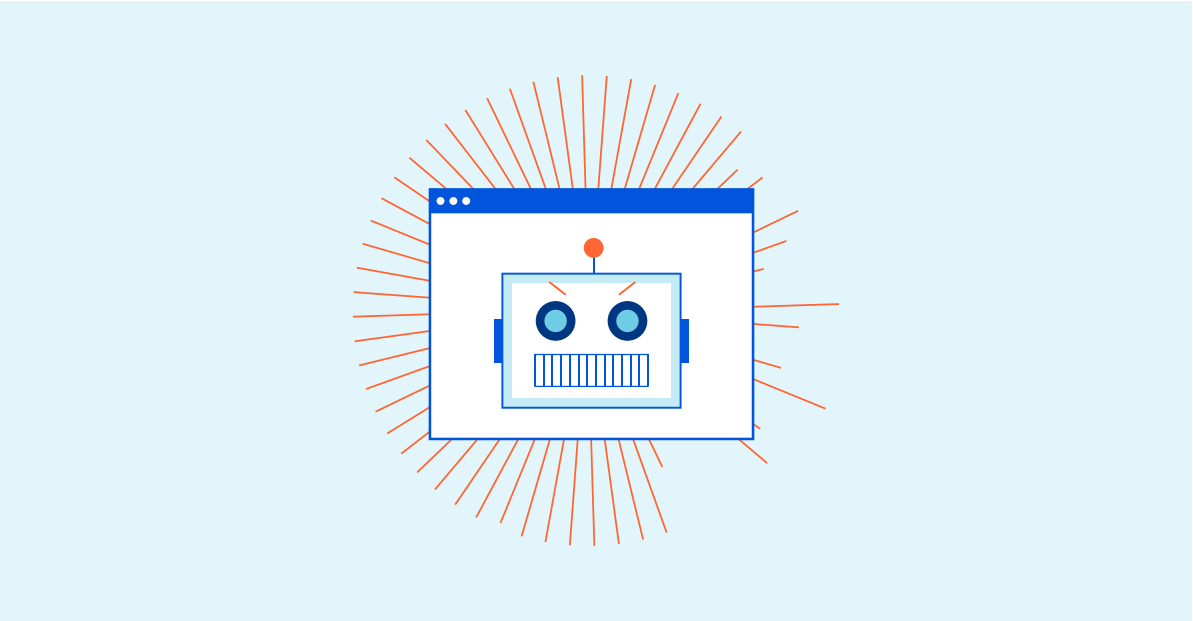


幸运的是，即使是经费预算相对紧张的教育机构，也有许多有效的 DDoS 缓解策略可供选用。组织应该考虑：

- 强大的缓解能力：虽然贵组织希望只为所需的保护付费，但如果发生意料之外的大规模攻击行为，升级服务所需的时间会造成额外的停机时间。
- 分布式缓解模式：DDoS 流量清洗应该是分布式的，因为将组织的所有流量通过单个中央端点进行路由和过滤可能不可扩展，而且会增加网络延迟。
- 按需保护与不间断保护：对于按需 DDoS 缓解，流量通常会从公共互联网流向组织的服务器或网络基础设施，直到检测到潜在的攻击行为才对流量进行更彻底的检查和过滤。而不间断保护会持续过滤所有流量。尽管不间断保护比按需服务更加昂贵，但不间断缓解可以提供连续的保护，而且由于不需要手动启动服务，所以响应时间会更快。

要详细了解 DDoS 缓解策略，请阅读 Cloudflare 资源中心中的文章《缓解 DDoS 攻击的五种最佳实践》。

[1] *https://www.infosecurity-magazine.com/news/ddos-attacks-on-virtual-education/*



帐户盗用

很多网络攻击行为从盗用合法用户的系统帐户入手。帐户盗用攻击包括破解合法用户用于登录网络、应用程序或其他系统的凭据。攻击者可以通过多种方式获取帐户凭据，包括网络钓鱼攻击和凭据填充。

攻击者利用这些凭据伪装成合法用户，在目标系统上植入恶意软件、窃取数据或实现其他目的。通过这个方式，攻击者可以获取受《儿童在线隐私权保护法》(COPPA)和《家庭教育权和隐私权法》(FERPA)等法规所保护的数据。攻击者也能删除重要的学生记录，或利用勒索软件锁定资料以勒索赎金。

教育机构应部署一种网络钓鱼缓解方案，能够基于已知恶意内容和使用机器学习来检测可疑语言和其他未知威胁，从而发现攻击行为。电子邮件扫描就是这样一种方法；另一种方法是使用安全 Web 网关，以屏蔽已知的恶意网站并阻止用户下载特定类型的文件。

凭证填充

攻击者也可能会利用机构的公开登录系统(如虚拟专用网络(VPN)、远程桌面协议(RDP)或 web 访问门户)来破解用户凭据。普通人一般会为 13 个在线帐户使用相同的登录凭据[2]，而且人们往往会使用安全系数低、容易猜出的密码。凭据填充攻击会使用自动机器人程序来尝试猜出用户用于这类身份验证门户的密码。成功猜出密码后，攻击者就掌握了合法的登录凭据，因此能够访问合法用户的帐户。凭据填充攻击利用自动化程序。防范这

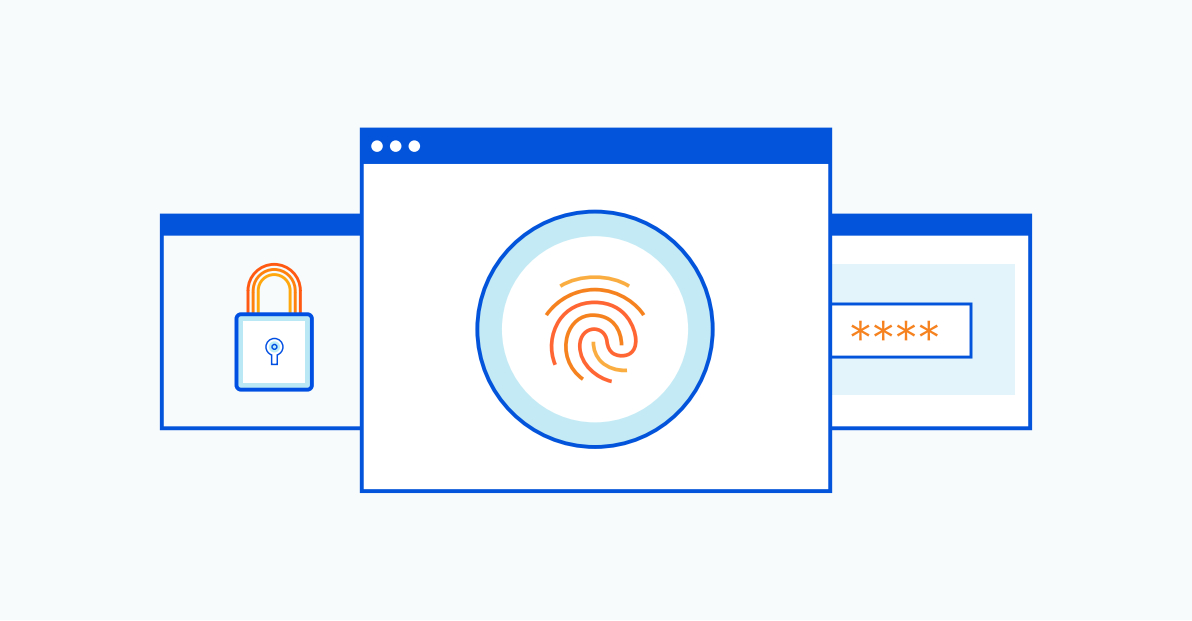
[2] *https://www.lastpass.com/state-of-the-password/global-password-security-report-2019*

类攻击行为需要用到机器人程序检测解决方案，不过，区分良性和恶意的机器人程序也非常重要。

有各种方法检测和阻止机器人程序。恶意机器人程序缓解策略的基本要素包括：

- **速率限制：**限制 IP 地址向您的网站或网络提交请求的次数。这是应对简单暴力型机器人程序攻击的最有效方法。
- **CAPTCHA 和双因素身份验证：**这两种方法都可以彻底阻止很多机器人程序访问登录页面，但会给用户体验带来不利影响。
- **维护机器人程序阻止列表和允许列表：**跟踪已知的恶意机器人程序，确保搜索引擎爬虫程序和其他良性机器人程序仍能执行其任务。

不过，这些方法可能无法有效应对更高级、更专门的机器人程序。要详细了解机器人程序缓解策略，请查看 Cloudflare 资源中心内的《恶意机器人程序应对手册》。

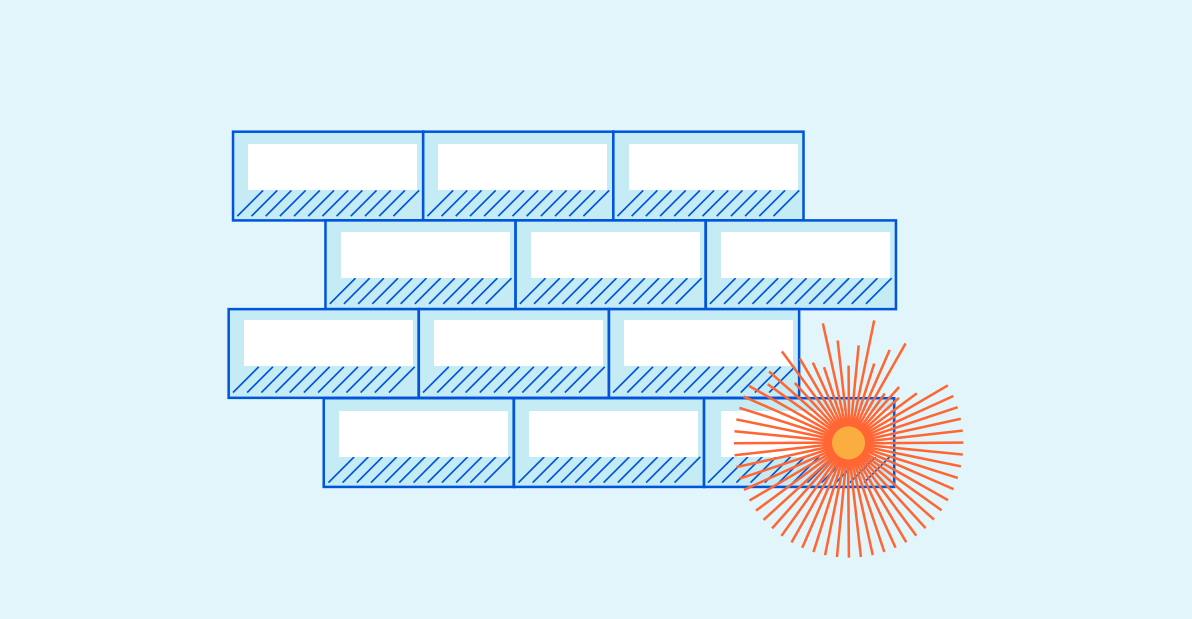


恶意内容和恶意软件

随着教育工作者采用远程教学模式，越来越多系统接入公共互联网。学生可利用 web 应用程序进行在线学习。远程学生和教育工作者可能通过 VPN、RDP 或类似解决方案访问远程网络和计算机。这些系统也必须受到保护以防御网络威胁。

Web 应用程序安全

教育 web 应用程序可能有权访问各类敏感数据。受 COPPA、FERPA 和类似法规保护的学生数据可能存储在这类平台上，因此教育机构必须对其进行有效保护。



由于这些应用程序属于软件，所以可能存在容易被利用的漏洞。要想保护这些应用程序以防范网络攻击，需要检查网络流量，检测和阻止试图利用软件漏洞的行为。

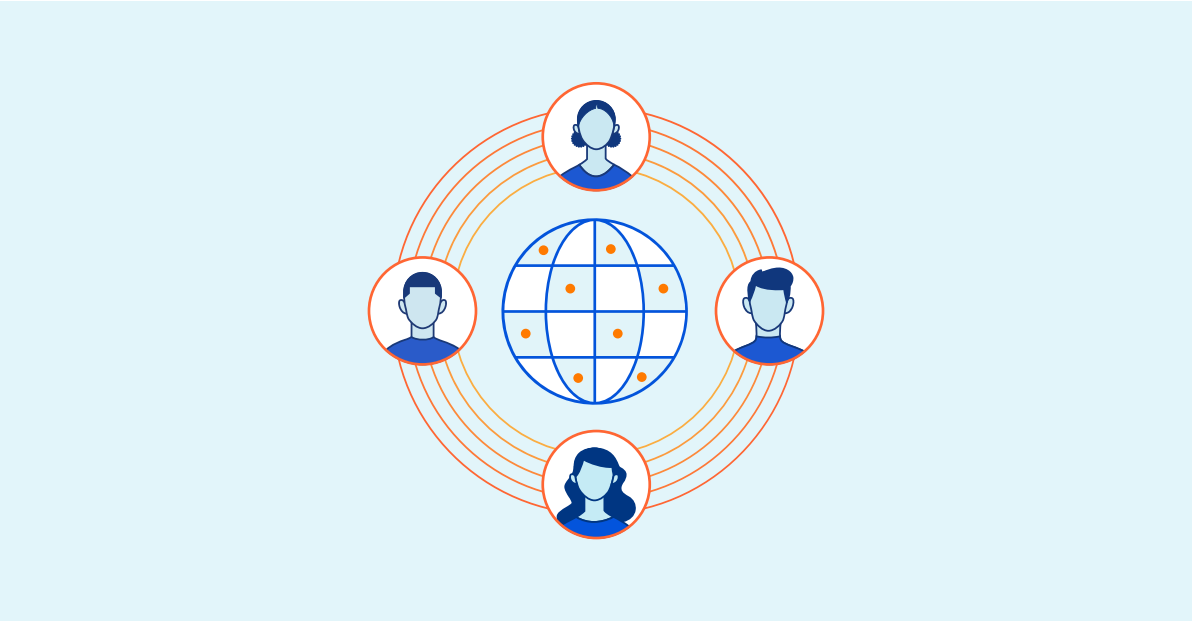
Web 应用程序防火墙（WAF）提供针对各种应用程序漏洞的防护。WAF 可以结合使用基于签名的检测技术和机器学习来识别已知和新型攻击。这样甚至可以防御针对组织 web 基础设施的零日攻击。

反勒索软件保护

勒索软件是增长最快的恶意软件之一。一旦勒索软件获得计算机的访问权限，就会对其中存储的文件进行加密，并以恢复文件访问权限为条件勒索金钱。即便学校能立即支付赎金，恢复受影响的系统也需要大量时间和费用。

VPN 和 RDP 等远程访问技术正日益成为投放勒索软件的主要方式。攻击者获取合法登录凭据后，会利用它们登录计算机并安装恶意软件。进入机构的内部网络后，恶意软件通常会进行传播，感染网络上的其他计算机。

教育机构需要一种防火墙解决方案，对所有业务网络流量进行检查，以便检测到传入的恶意内容（如勒索软件），防止机构中的计算机遭受感染，同时阻止数据（包括学生的受保护个人数据）外泄行为。



利用 Cloudflare 为远程教学保驾护航

新冠肺炎疫情终会过去，但轻松过渡至远程教学模式的能力对教育机构很有价值。在线学习资源也是课堂学习的宝贵资产，有了必要的远程教学基础设施，教育机构就能妥善应对恶劣天气等意外事件所造成的教学中断。

Cloudflare 提供便于用户使用的集成式平台，包含适用于各类教学机构的解决方案，应对最常见的 IT 和安全性挑战。借助 Cloudflare 这样的单一集成解决方案，教育机构能避免不必要的复杂性，能更灵活自如地应对意外情况。Cloudflare 提供：

- 全球性的内容交付网络，在世界各地超过 200 座城市拥有数据中心。
- 47 Tbps 的 DDoS 缓解能力，在网络边缘实施不间断缓解。
- Web 应用程序防火墙，从 Cloudflare 网络上约 2500 万互联网资产持续收集威胁情报。
- 高级机器人程序缓解，利用机器学习和指纹识别来分析网络中的流量模式并检测最高级的机器人程序。
- 安全 Web 网关，运行于网络边缘，降低将流量回传到偏远数据中心造成的延迟。

有关详情，请访问 www.cloudflare.com。