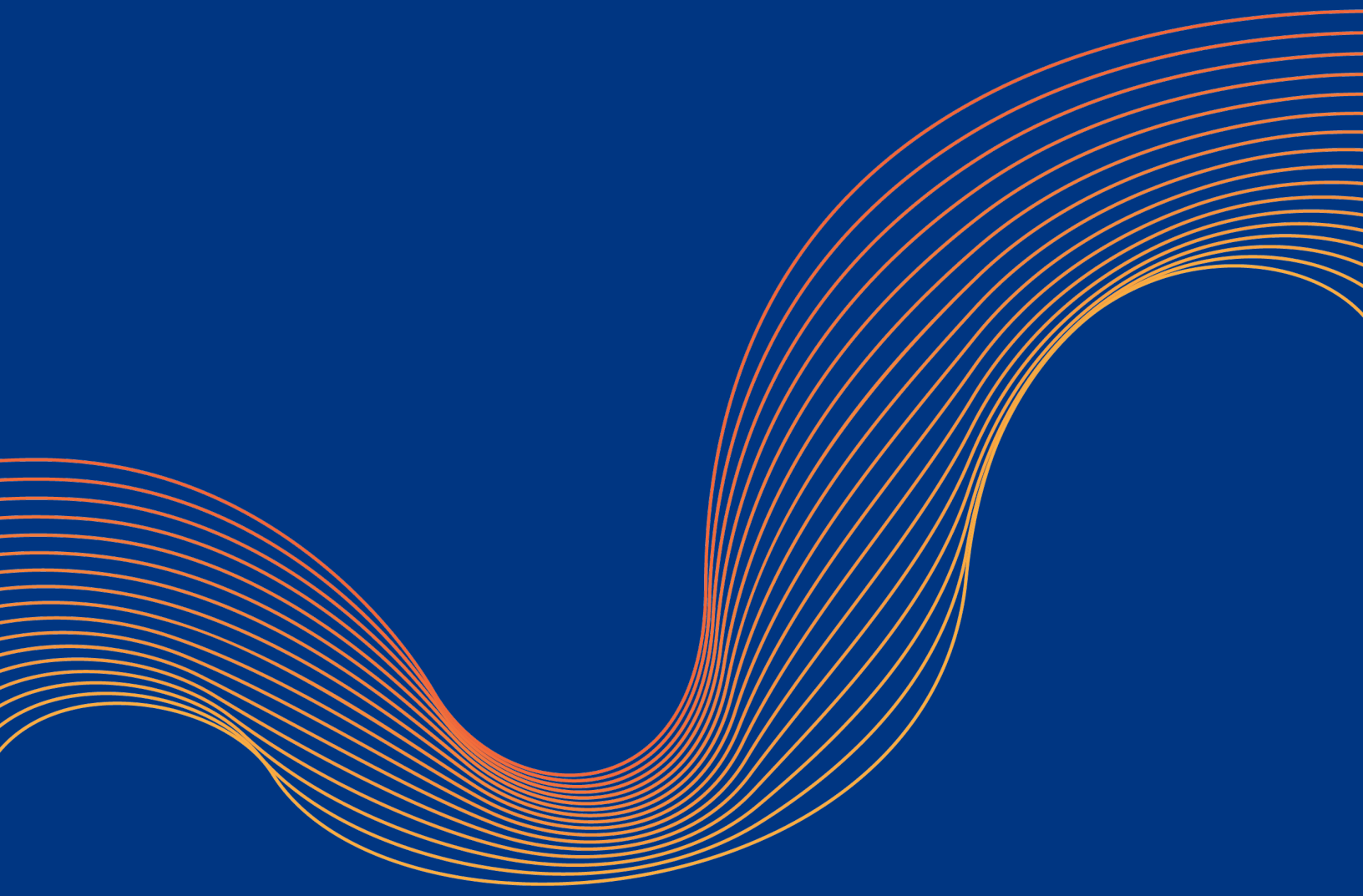
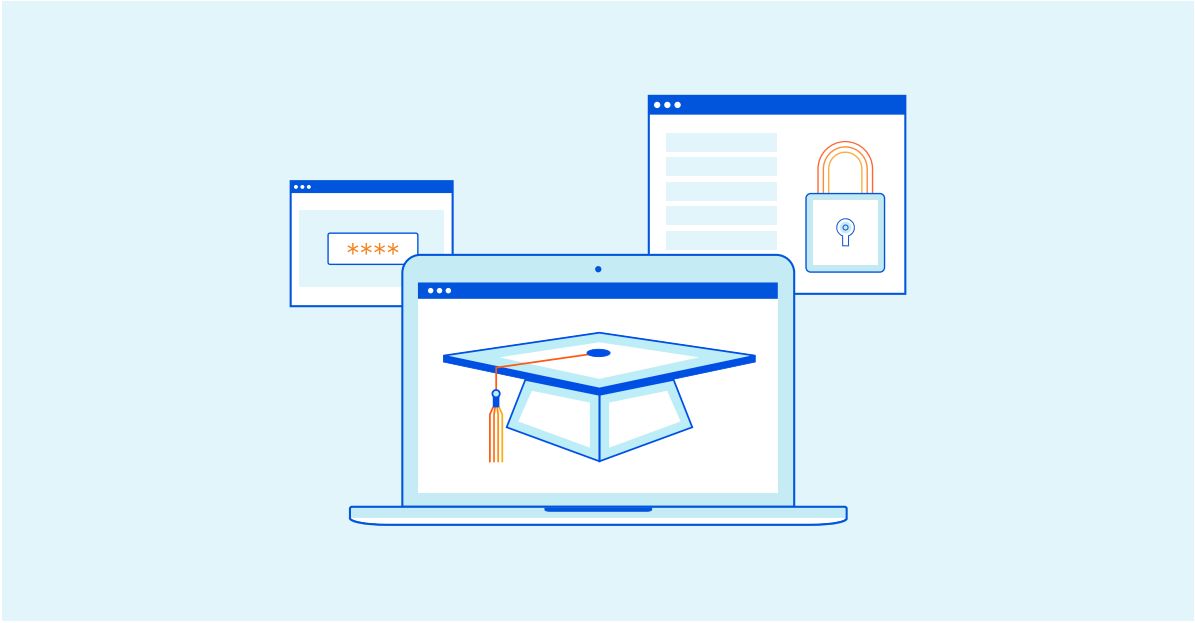
白皮書

CLOUDFLARE

設計安全且可擴充的遠端教學基礎結構



+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com/zh-tw/



介紹

近年來，遠端教學已成為日益流行的教學模式。受 COVID-19 疫情影響，許多教育機構被迫採用遠端教學模式，確保學生和教育工作者免遭疫情感染，這加快了混合式和全面遠端教學模式的轉型速度。

遠端教學的方法完全不同於傳統的面對面授課。教育工作者必須能夠勝任各類教學方式和教學內容，包括講座、視訊、互動內容等。在遠端教學模式下，課堂中的所有學生都需要具備快速並可以同時獲取共用內容的能力。

在技術方面，教育機構需要能為各類內容提供支援，確保學生能在需要時使用系統。為此，需要解決一系列難題包括：

- 大規模傳遞內容
- 緩解分散式阻斷服務攻擊
- 防止帳戶盜用
- 阻止惡意內容和惡意軟體

大規模傳遞內容

對於遠端教學而言，學校的 IT 基礎結構是其營運能力的重要組成部分。教育工作者需要能夠同時向眾多學生投放內容，並確保將延遲降到最低。

教育工作者需要能夠向學生傳遞各類內容，包括從靜態網頁到動態內容 (互動式線上學習工具和串流視訊) 的各類內容。教育機構的 IT 基礎結構需要能夠以高效率且可擴充的方式將這類內容遠端傳遞給學生。

靜態內容

教育工作者需要向學生提供的內容中有一部分是靜態的，包括特定的網頁，其中的資訊不會發生變化，而且不需要頻繁更新。

對於這類內容，主要 IT 難題在於可擴充性和延遲。如果許多學生同時嘗試存取同一個內容，網頁伺服器能否正常運作？此外，網頁伺服器的地點也會對遠端教學效果產生巨大影響。學生距離伺服器所在地越遠，傳遞內容的延遲就越久。

對於靜態內容，如果能夠建立本機快取，則有助於解決這些難題。如果學生經常存取某個頁面，則可以將該頁面副本儲存在本機，以便學生在需要時快速進行存取。

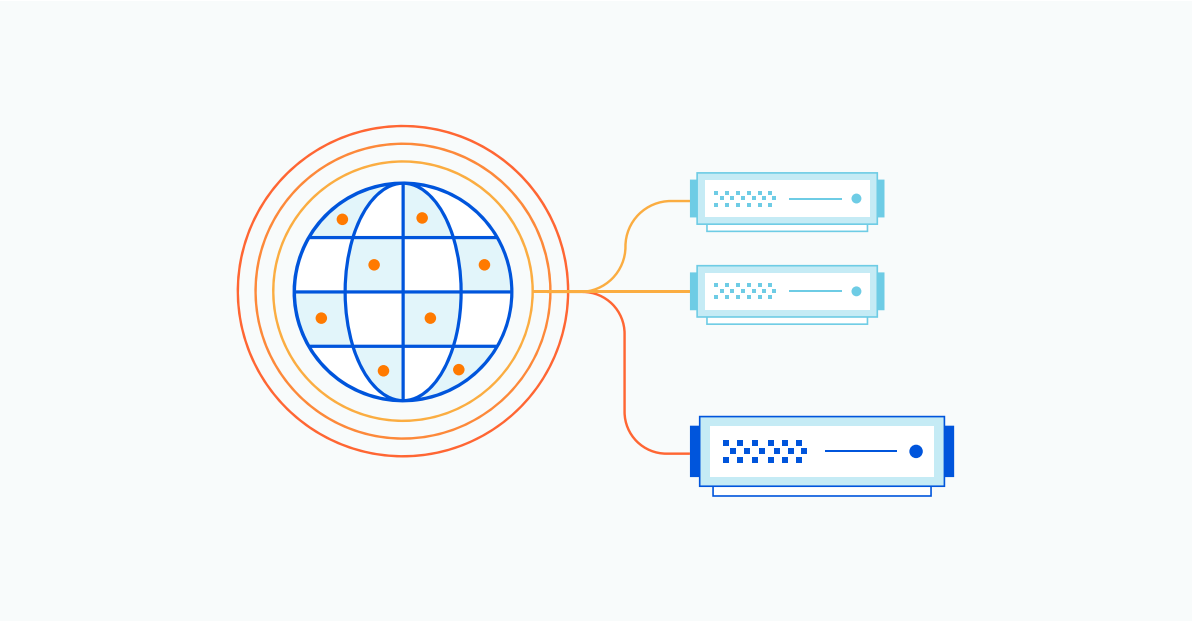
利用內容發佈網路 (CDN) 可以規模化地實現快取處理。CDN 由網路節點構成，可以儲存靜態內容的本機副本，並定期檢查更新。覆蓋全球的 CDN 可以提供所需的可擴充性和低延遲，實現高效率的遠端教學。

動態和互動式內容

就像靜態內容一樣，互動式線上學習和其他內容也可能存在可擴充性方面的問題。不過，CDN 節點網路不適合用於處理這類內容。如果內容需要經常更新或一直更新，那麼 CDN 節點就會不斷向主網頁伺服器查詢更新版本。這樣會增加使用者的延遲，造成主網頁伺服器超過負荷。

動態內容可擴充性問題可以透過負載平衡技術來解決。這時不會使用單個伺服器來處理學生請求，而是使用多個伺服器並在之間分配流量。這樣就不會造成單個伺服器超過負荷，將延遲降至最低。

為確保高效率，負載平衡伺服器需要能夠完全獨立執行，或僅依靠其他負載平衡裝置來執行。如果所有伺服器都設定為使用同一個資料庫伺服器，那麼該資料庫伺服器很可能成為制約因素，其他伺服器則無法或幾乎無法帶來任何好處。遠端教學解決方案必須精心設計，確保能在需要時提供所需的規模，所建置的系統能夠提供負載平衡的全部優勢。

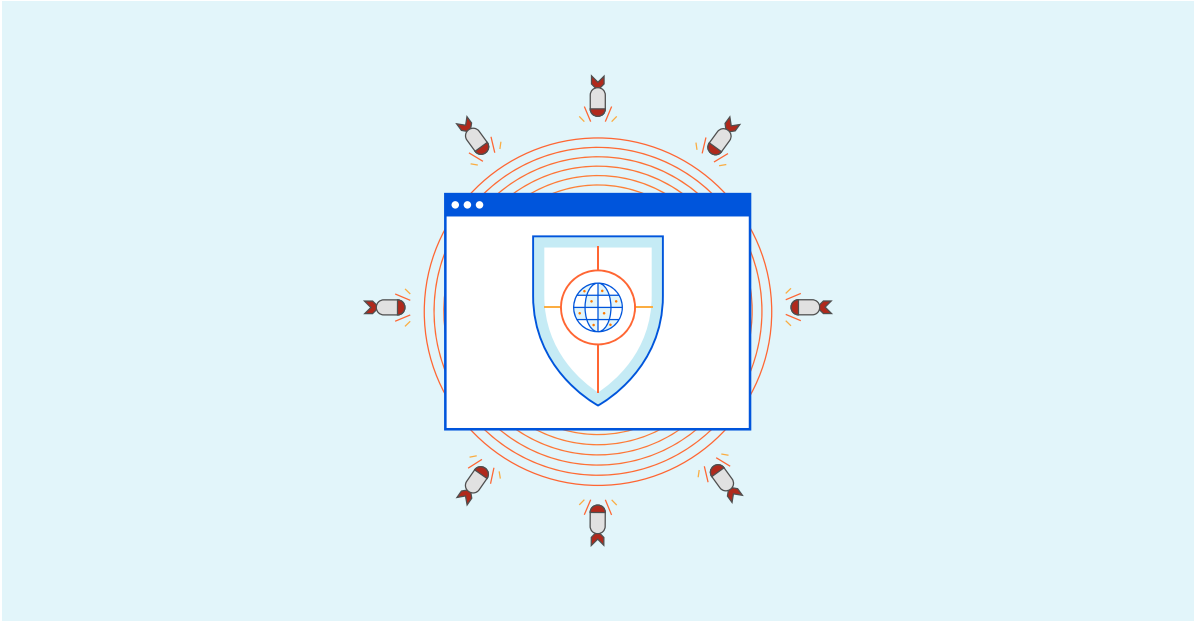


分散式阻斷服務攻擊

當使用者存取網頁資產時，其裝置所查詢的 DNS 解析器對應了相應資產的網域分散式阻斷服務 (DDoS) 攻擊，這種情況日益普遍。隨著物聯網 (IoT) 和雲端運算的發展，攻擊者獲取連網運算能力的難度和成本越來越低。然後，這些遭到破壞的裝置會用於向伺服器傳送惡意流量，使伺服器難以回應合法的請求。

在遠端教學模式下，DDoS 攻擊會對服務提供能力帶來嚴重風險。在 2020 年上半年，許多教育機構改為採用遠端教學模式，線上教育資源遭受的 DDoS 攻擊數量增長了 350%[1]。

此外，一些 DDoS 攻擊行為經過演變，已經包含了勒索元素。攻擊者可能威脅對機構發起 DDoS 攻擊，並要求以支付贖金為條件停止攻擊。雖然很多威脅都是無稽之談，但教育機構如果沒有 DDos 保護機制，就會覺得他們的基礎結構面臨著不容忽視的風險。

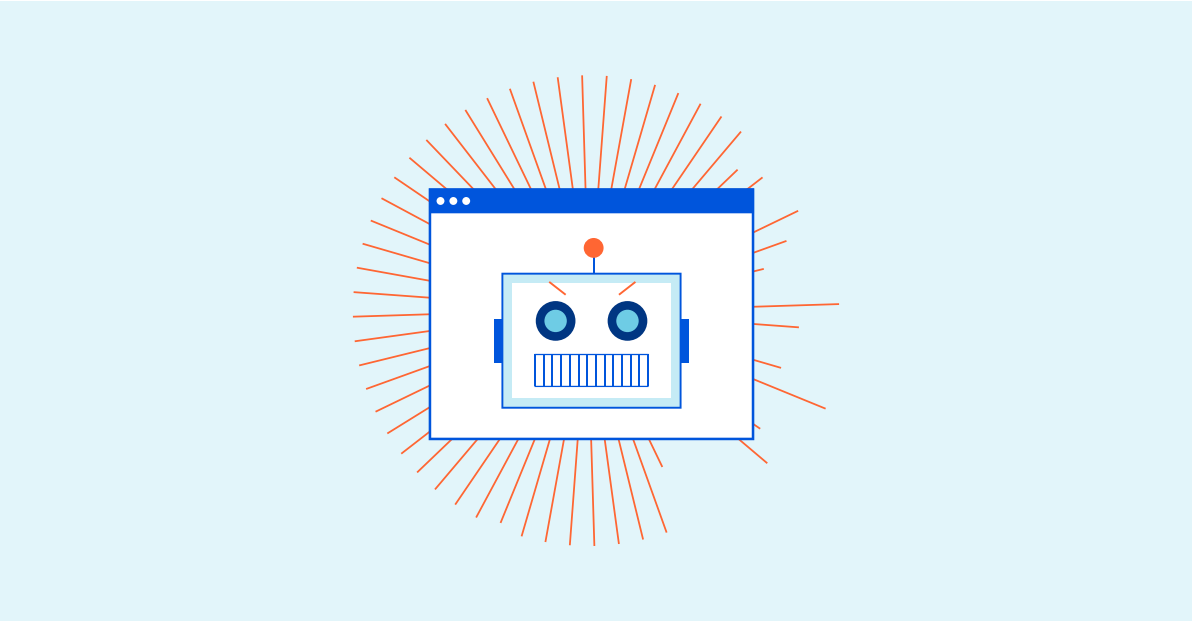


幸運的是，即使教育機構的經費預算相對緊張，也有許多有效的 DDoS 緩解策略可供選用。組織應當作何考量：

- 強大的緩解能力：雖然對各類機構而言，僅付費購買所需的保護機制是個吸引人的方法，但如果發生意外的大規模攻擊行為，升級服務就會消耗時間，造成停機時間增加。
- 分散式緩解模式：DDos 流量清理系統應該是分散式，因為將機構的所有流量透過單個中央端點進行路由和篩選可能不具擴充性，而且會增加網路延遲。
- 視需求保護與不間斷保護：對於視需求的 DDoS 緩解，流量通常會從公開的網際網路流向機構的伺服器或網路基礎結構，直到偵測到潛在的攻擊行為，這時會對攻擊行為進行更全面的檢查和篩選。而不間斷保護機制會持續篩選所有流量。儘管不間斷保護機制比視需求的服務更加昂貴，但不間斷緩解可以提供連續的保護，而且由於不需要手動啟動服務，所以回應時間會更快。

若要詳細瞭解 DDoS 緩解策略，請閱讀 Cloudflare 資源中心中的文章《緩解 DDoS 攻擊的五種最佳實踐》。

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



帳戶盜用

很多網上攻擊行為從盜用合法使用者的系統帳戶入手。帳戶盜用攻擊包括破解合法使用者用於登入網路、應用程式或其他系統的憑證。攻擊者可以透過多種方式獲取帳戶憑證，包括網路釣魚攻擊和憑證填充。

攻擊者利用這些憑證偽裝成合法使用者，在目標系統上植入惡意軟體、竊取資料或實現其他目的。這樣一來，攻擊者就可以獲取受《兒童線上隱私權保護法案》(COPPA) 和《家庭教育權和隱私權法案》(FERPA) 等法規所保護的資料。攻擊者也可能會刪除重要的學生記錄，或利用勒索軟體以此勒索贖金。

教育機構應部署網路釣魚緩解解決方案，基於已知惡意內容和使用機器學習來偵測可疑語言和其他未知威脅，藉此發現攻擊行為。電子郵件掃描就是這類方法之一，還有一種方法是使用安全 Web 閘道，以封鎖已知的惡意網站並防止使用者下載特定類型的檔案。

憑證填充

攻擊者也可能會利用機構的公開登入系統 (如虛擬私人網路 (VPN)、遠端桌面通訊協定 (RDP) 或網頁存取入口網站) 來破解使用者憑證。普通人一般會為 13 個線上帳戶使用相同的登入憑證[2]，而且人們往往會使用安全係數低、容易猜出的密碼。憑證填充攻擊會使用機器人來嘗試猜出使用者用於這類身分驗證入口網站的密碼。成功猜出密碼後，攻擊者就掌握了合法的登入憑證，因此能夠存取合法使用者的帳戶。憑證填充攻擊利用自動

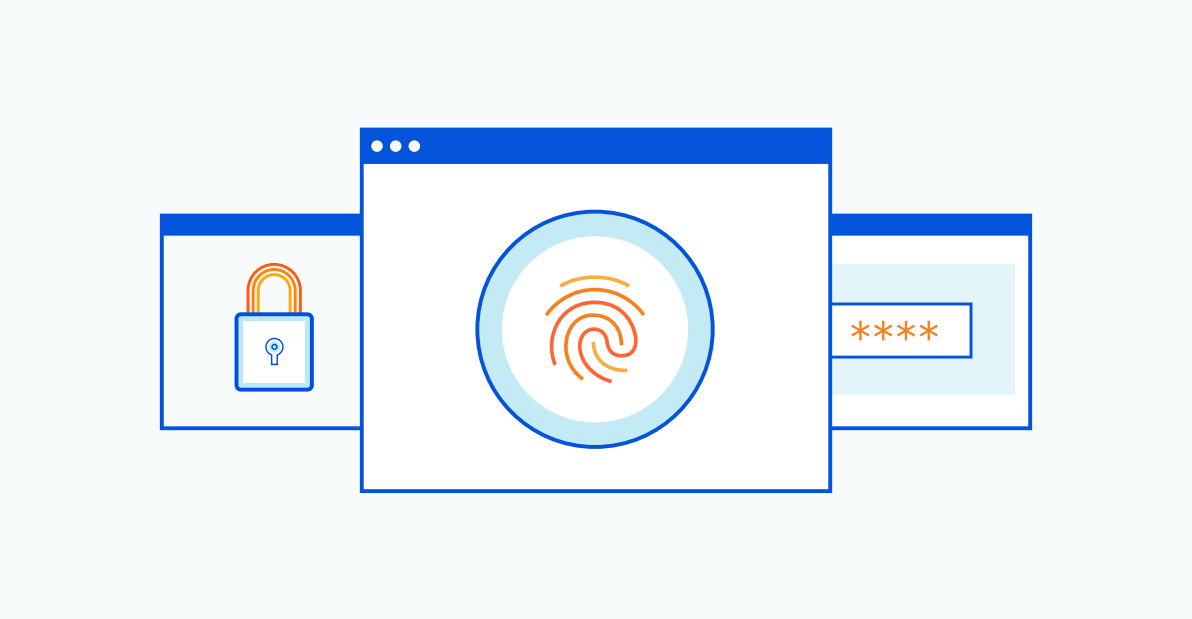
[2] *https://www.lastpass.com/state-of-the-password/global-password-security-report-2019*

手段。防範這類攻擊行為需要用到機器人偵測解決方案，不過，區分有益的和惡意的機器人非常重要。

偵測和封鎖機器人的方法有很多種。惡意機器人緩解策略的基本要素包括：

- **速率限制：**限制 IP 位址向您網站或網路提交請求的次數。這是因應簡單的暴力破解機器人攻擊的最有效方法。
- **CAPTCHA 和雙重驗證：**這兩種方法都可以徹底阻止機器人存取登入頁面，但會對使用者體驗帶來不利影響。
- **維護機器人封鎖清單和允許清單：**追蹤已知的惡意機器人，確保搜尋引擎網路爬蟲和其他有益的機器人仍能執行其任務。

不過，這些方法可能無法有效因應更加進階的專業化機器人。若要詳細瞭解機器人緩解策略，請查看 Cloudflare 資源中心內的《惡意機器人應對手冊》。

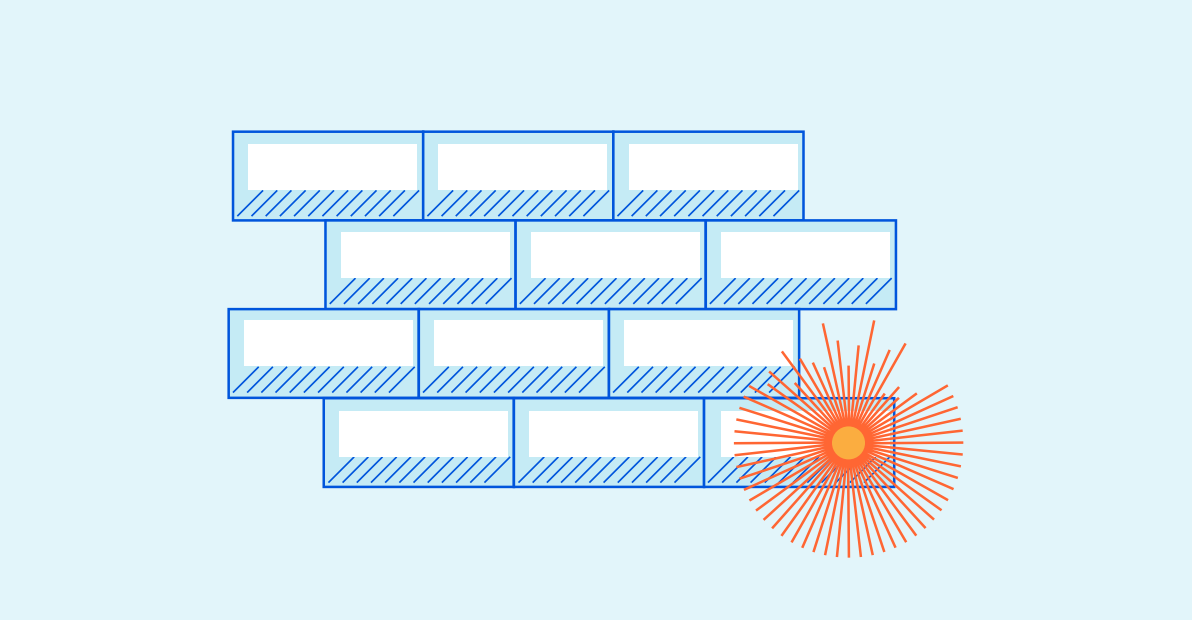


惡意內容和惡意軟體

隨著教育工作者採用遠端教學模式，會有越來越多的系統接入公共網際網路。學生可利用網頁應用程式進行線上學習。遠端的學生和教育工作者可能透過 VPN、RDP 或類似解決方案存取遠端網路和電腦。這些系統也必須受到保護，防範網路威脅。

Web 應用程式安全性

教育網頁應用程式可能有權存取各類敏感性資料。受 COPPA、FERPA 和類似法規保護的學生資料可能儲存在這類平台上，因此教育機構必須對其進行有效保護。



由於這些應用程式屬於軟體，所以可能存在容易被利用的漏洞。若想保護這些應用程式防範網路攻擊，就需要檢查網路流量，偵測和封鎖試圖利用軟體漏洞的行為。

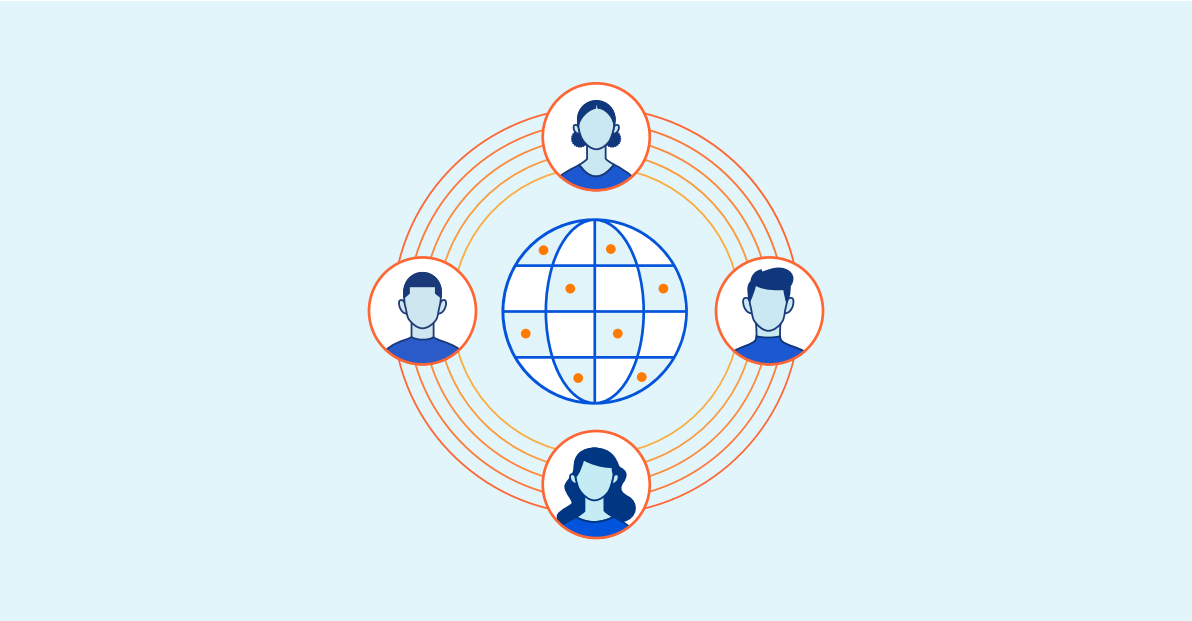
Web 應用程式防火牆 (WAF) 可以為各類應用程式漏洞提供防護。WAF 可以結合使用基於簽名的偵測技術和機器學習來識別已知和新型攻擊。這樣就可以抵禦針對機構網頁基礎結構的零日攻擊。

反勒索軟體保護

勒索軟體是增長速度最快的惡意軟體類型。一旦勒索軟體獲得電腦的存取權限，就會對其中儲存的檔案進行加密，並以恢復檔案存取權限為條件勒索金錢。即便學校能立即支付贖金，恢復受影響的系統也需要大量時間和成本。

VPN 和 RDP 等遠端存取技術正日益成為投放勒索軟體的主要方式。攻擊者獲取合法登入憑證後，會利用它們登入電腦並安裝惡意軟體。進入機構的內部網路後，惡意軟體通常會進行傳播，感染網路上的其他電腦。

教育機構需要防火牆解決方案，對所有業務網路流量進行檢查，以便偵測到傳入的惡意內容 (如勒索軟體)，防止機構中的電腦遭受感染，同時封鎖嘗試外洩資料 (包括學生的受保護個人資料) 的行為。



利用 Cloudflare 為遠端教學保駕護航

COVID-19 疫情終有平息的一天，但對於教育機構而言，能夠輕鬆過渡至遠端教學模式仍十分重要。線上學習資源也可以為課堂學習帶來優勢，有了必要的遠端教學基礎結構，機構就能妥善因應惡劣天氣等意外事件所造成的教學中斷。

Cloudflare 提供便於使用者使用的整合式平台，包含適用於各類教學機構的解決方案，能夠解決最常見的 IT 和安全性難題。藉由 Cloudflare 的一體化解決方案，教育機構可以避免不必要的複雜性，更靈活地因應意外情況。Cloudflare 能夠提供：

- 遍布全球的內容傳遞網路，在世界各地超過 200 座城市建立資料中心。
- 47 Tbps 的 DDoS 緩解能力，在網路邊緣實施不間斷緩解。
- Web 應用程式防火牆，從 Cloudflare 網路上的近 2500 萬網際網路設備持續收集威脅情報。
- 進階機器人緩解，利用機器學習和指紋識別來分析網路中的流量模式並偵測最進階的機器人。
- 安全 Web 閘道，在網路邊緣執行，降低將流量回傳到地理位置偏僻的資料中心時的延遲。

如需更多資訊，請造訪 www.cloudflare.com。