CLOUDFLARE®

SaaS 提供者生存指南

適用於線上應用程式效能、
安全性與加密的基本解決方案

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

報告摘要

SaaS 市場預期將在 2016 到 2020 之間成長 196%。[1] 隨著 SaaS 市場持續成長並成為商業基礎結構不可或缺的一部分，安全性與效能一直是 SaaS 提供者與其客戶最關心的一件事。由於此持續成長，SaaS 提供者在提供最安全且最具效能的應用程式給客戶時，將會面臨越來越多的競爭。效能不佳與易遭受攻擊的應用程式將會對營收、使用者參與、品牌商譽與客戶忠誠度造成負面影響。針對 SaaS 提供者的重要子集，品牌化自訂客戶網域加密需求表示必須手動管理 SSL 生命週期，進而造成較長的部署時間與額外成本。或者，建置複雜的自動化內部解決方案會使得工程師無法著重於核心優勢。

Cloudflare 為 SaaS 提供者提供效能與安全性解決方案，不僅可以保護 SaaS 提供者、客戶與訪客，更可為其提供快速的使用體驗。Cloudflare 每秒 10 Tb 的全球內容提供網路 (CDN) 結合了 Argo 智慧型路由、負載平衡與效能最佳化，可將訪客所感受到的延遲縮短一半。Cloudflare 的進階 DDoS 保護結合了 Rate Limiting 與 Web 應用程式防火牆 (WAF)，可同時防堵以網路層、傳輸層與應用程式層為目標的大型體積型與複雜攻擊。此外，SaaS 提供者能以易於實作且完全受管理的 SSL 解決方案來保護客戶自訂網域的客戶資料傳輸。

延遲與不當安全性的商業影響

任何形式的 SaaS 應用程式延遲與不當安全性都會導致客戶體驗、轉換率與搜尋引擎排名變差，而且會導致營收減少與客戶流失。

對 SaaS 應用程式存取的效能與可用性影響

客戶在存取網站、應用程式與 API 時，會想要獲得快速且高度可用的體驗。當線上資產回應速度變慢或無法使用時，SaaS 應用程式存取與轉換率會降低並大幅受影響。

例如，Google 報告指出即使網站延遲只小幅增加 100 - 400 毫秒，也會對客戶行為造成可觀的影響 [1]；Walmart 發現即使網站載入時間只增加數秒，轉換率也會大幅降低 [2]，同樣地，Amazon 發現每當其網站延遲降低 100 毫秒，其營收就會增加 1%。[3]

傳統 SaaS 應用程式與效能問題與內部因素和 SaaS 提供者的共用託管基礎結構或應用程式設定有關。其中一個因素是訪客與 SaaS 應用程式來源伺服器之間的地理距離；距離每增加 100 英哩，延遲就會增加大約 0.82 毫秒。[4] 距離加上龐大的未最佳化靜態內容，導致訪客感受到的延遲更為長。

然而，效能不止是由伺服器、網路與應用程式所決定；它可能也取決於尖峰或季節性流量，這可能造成共用基礎結構超載，進而使得應用程式回應速度變慢或完全無法使用。

載入速度極慢與無法使用的 SaaS 應用程式會對營收、轉換率、跳離率、搜尋引擎 (SEO) 排名、品牌商譽、客戶滿意度與服務層級協定 (SLA) 造成大幅影響。

[1] http://www.sfgate.com/business/article/Google-s-speed-need-instantaneous-Internet-3251049.php
[2] https://www.slideshare.net/devonauerswald/walmart-pagespeedslide
[3] https://blog.gigaspaces.com/amazon-found-every-100ms-of-latency-cost-them-1-in-sales/
[4] http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

目標式 SaaS 應用程式攻擊的影響

不論是剛進入市場的新 SaaS 提供者或經營已久的軟體公司，想要將本機應用程式移轉到雲端時，都必須將一律在線上執行之應用程式的安全性納入考量。

由於 SaaS 應用程式與服務公開到公用網際網路，而且在許多情況下工作負載跨越多個共用基礎結構，因此受攻擊面越來越大。SaaS 提供者的攻擊媒介範例包括登入入口網站、共用 DNS 與代管，以及複雜的應用程式弱點。請務必注意，許多 SaaS 提供者都在共用基礎結構中裝載多個用戶端應用程式，因此任何資料外洩、可靠性事件或對共用基礎結構的攻擊，都會對其他客戶造成負面影響。

以上述媒介為目標的特定攻擊包括體積型與複雜 DDoS 攻擊、暴力登入嘗試、應用程式弱點探測，以及對跨各種裝置之所有目標網站、應用程式與 API 的未加密客戶資料攔截。成功遂行攻擊的商業影響從服務中斷、品牌商譽變差與客戶流失，到營收大幅損失與損害控制成本。

在 2013 年，駭客滲透 Adobe，並取得 290 萬個客戶的信用卡資訊與其他個人資料。[5] Adobe 的首席保安官 Brad Arkin 確認了線上商務風險，他引用了「網路攻擊是現今商業必須面臨的其中一個殘酷現實，」。

在 2016 年 10 月 16 日，Airbnb、Amazon.com、Netflix、The New York Times、Paypal、Pinterest、Reddit、Tumblr、Twitter、Verizon、Visa、The Wall Street Journal、Yelp、Zillow 與許多其他公司都因為來自惡名昭彰的 Mirai 殭屍網路的攻擊而斷線一段不短的時間。直接目標並非應用程式本身，而是這些網站與應用程式所使用的 Dyn 這家 DNS 服務提供者。Dyn 在 11 個小時後成功解除了此事件，讓所有受影響網站的服務恢復正常。[6]

在加密與自訂網域之間做選擇

由於大型科技公司企盼打造更安全的網際網路的壓力，線上組織採用 SSL / TLS 加密已成為安全性最佳實作並逐漸成為要求。例如，Google Chrome 網頁瀏覽器在 2017 年以後開始以可見的方式將未使用 HTTPS 的網站標示為「不安全」。[7] 此外，Apple 現在要求所有 iOS 應用程式都必須使用 HTTPS 連線，才能提交到 App Store。[8]

在 SSL 發展初期，線上組織必須選擇透過 HTTPS 將網路流量加密，或為訪客提供符合效能預期的體驗。直到幾年前，SSL 通訊協定仍會導致延遲增加，並使得網站與應用程式效能降低。再者，即使組織選擇放棄效能來提高安全性，當時實作 SSL 的操作困難度限制了廣泛的採用。隨著近期的 SSL 改進 (例如 HTTP/2 (HTTP 1.1 的後繼者) 的發展)，現今使用 SSL 透過 HTTPS 來保護流量已超過未加密之 HTTP 的效能。

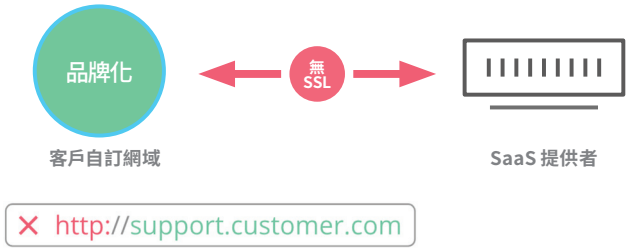
就像組織過去必須在加密或效能之間做出選擇一樣，現今 有一部分的 SaaS 提供者必須選擇將其客戶流量加密並讓那些客戶使用他們自己的品牌化自訂網域。這兩者對於結合適當品牌呈現、安全性、搜尋引擎排名與最佳效能優勢方面都非常重要。

[5] http://www.nytimes.com/2013/10/04/technology/adobe-announces-security-breach.html
[6] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[7] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/
[8] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/

此類 SaaS 提供者通常可讓其客戶建立公開到網際網路的資產，例如登錄頁面、網站、支援入口網站等。SaaS 提供者通常在其主要網域的子網域代管這些新建立的客戶資產；例如，由 SaaS 提供者的客戶所建立之資產的 URL 可能是 **customercompany.saasprovider.com**，而非品牌化自訂 URL (例如 **customercompany.com** 或 **support.customercompany.com**)。這對客戶而言是一個挑戰，因為若沒有品牌化自訂網域，可能會造成品牌認知、SEO 排名與客戶信任降低。

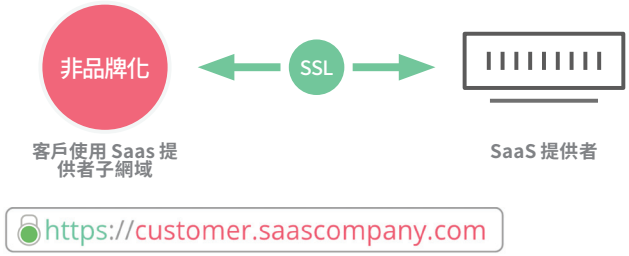
SaaS 提供者與其客戶透過為 customercompany.com 或 support.customercompany.com URL 進行 CNAME 處理以導向 customercompany.saasprovider.com 來克服網域品牌化挑戰。這樣一來，客戶就能使用其自有品牌化自訂網域；然而，SaaS 提供者將無法輕鬆地啟用 SSL，而且會發現管理整個 SSL 生命週期程序十分困難。針對客戶手動管理 SSL 生命週期程序或嘗試建置內部解決方案不僅耗時，而且必須耗費許多人力與成本。

在處理上述挑戰時，SaaS 提供者可以發現他們屬於三種情節的其中一種：



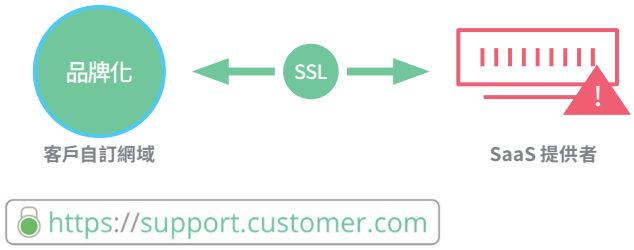
未加密但品牌化的自訂網域

無 SSL 的自訂網域缺少 SSL 的效能與安全資料傳輸優勢，因此內容在傳遞給訪客前易被窺探，且可能被竄改或插入惡意程式碼。



加密但未品牌化的網域

透過 SaaS 提供者啟用 SSL 的網域缺少自訂網域，因此會使得品牌認知度與 SEO 排名下降。

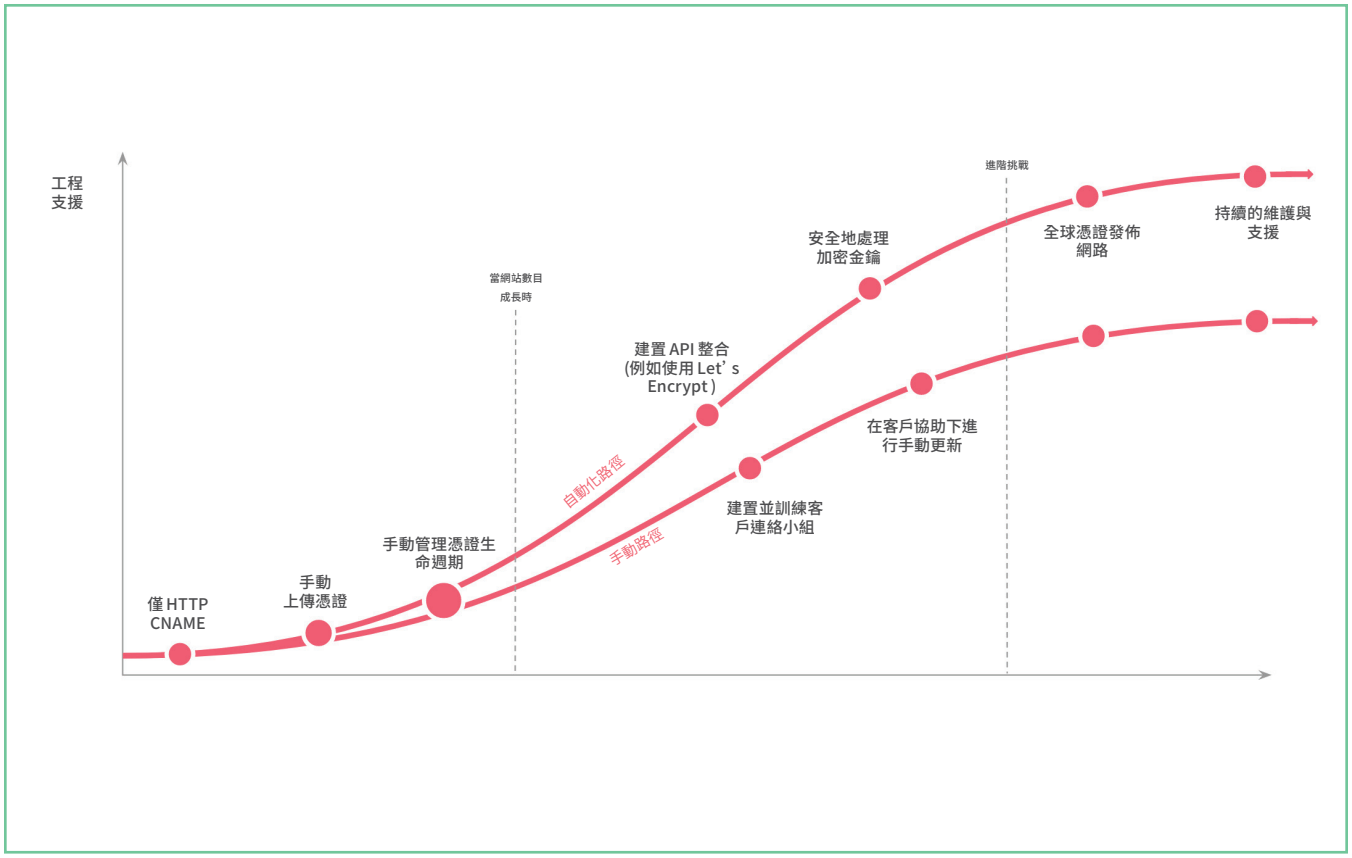


內部方法的挑戰

想要加密品牌化自訂網域的 SaaS 提供者可以手動管理 SSL 生命週期 (但這樣會導致部署時間變長且成本過高)，或建置複雜的自動化內部解決方案。

請務必注意當 SaaS 提供者建置自有解決方案以管理客戶網域的 SSL 時所面臨的技術挑戰。下圖顯示 SaaS 提供者所描繪的傳統藍圖，此提供者嘗試建置自動化內部 SSL 解決方案。

建置內部解決方案時有兩個路徑可採用，但兩者都不理想。第一個 (上方) 路徑會將 SSL 程序自動化，但需要充足的工程支援，而且會面臨複雜的挑戰；第二個路徑則需要同時由 SaaS 提供者與客戶提供的手動支援。



Cloudflare 可滿足 SaaS 應用程式安全性、效能與可用性需求

Cloudflare 可透過降低延遲並將內容傳遞效能最佳化，同時將這些優勢延伸到客戶網際網路資產，來改進 SaaS 提供者網站、應用程式與 API 的使用者體驗。

全球可用

Cloudflare 解決方案的核心是全球任一傳播內容傳遞網路 (CDN)，由位在超過 57 個國家/地區的 117+5 個資料中心所組成，可為任何地區的訪客提供提供最接近的 SaaS 應用程式內容。Cloudflare 也為超過 38% 的受管理DNS 網域提供服務，並執行全球最大的權威 DNS 網路。由於平均查詢速度只有幾毫秒，Cloudflare 擁有任何受管理 DNS 提供者難以望其項背的最快全球效能。

可調整規模的應用程式可用性

Cloudflare 負載平衡是以 Cloudflare 高度可用 DNS 基礎結構與全球 Anycast™ 網路為基礎而延伸，可以跨多部伺服器進行流量負載平衡並將流量路由傳送到最接近的地理區域，以降低延遲。負載平衡包括具備快速容錯移轉的健康情況檢查，可迅速將訪客從有問題的伺服器導向健康情況正常的伺服器。此外，負載平衡可以跨多個雲端提供者或內部部署基礎結構使用，以減輕由單一提供者或伺服器所造成之服務中斷的影響，同時避免雲端廠商鎖定。

更快的訪客體驗

Cloudflare 的 CDN 是以進階最佳化為目標所建置，包括自動縮減 HTML、CSS 與 JavaScript 大小，以及可節省 20% 檔案與資源大小的 Gzip 壓縮。此外，專有格式影像與行動最佳化讓您的 SaaS 應用程式效能更棒。

Cloudflare 提供超過全球 10% 的網際網路流量，這足以讓其即時分析網路路徑的健康情況與可靠性。Cloudflare 的 Argo 智慧型路由演算法使用這個收集的資訊來跨可用的最快路徑路由傳送流量，同時維持開放式安全連線來減少連線設定所加諸的延遲。Argo 智慧型路由平均可額外減少網際網路延遲 35%，並減少 27% 的連線錯誤。

「Cloudflare 為 Crisp 提供最佳服務品質，並減少服務回應時間。他們成功地將昂貴的網路基礎結構商品化，讓一般公司都能使用。我們不能沒有它。」

crisp™ | **Valérian Saliou**
Crisp 資訊長

保護 SaaS 應用程式與客戶資料

Cloudflare 的雲端型安全性解決方案可保護 SaaS 提供者網站、應用程式與 API，同時將優勢延伸到客戶網際網路資產。

Cloudflare 超過 117 個資料中心的任一傳播網路輸送量是每秒 10 Tb，這是有史以來曾記載之最大 DDoS 攻擊的 10 倍以上，可有效防堵針對 OSI 模型第 3、4 與 7 層的攻擊。結合 Rate Limiting 與 Web 應用程式防火牆 (WAF) 之後，Cloudflare 的安全性解決方案也能減緩以應用程式層為目標之複雜攻擊的影響。此外，搭配適用於 SaaS 的 Cloudflare SSL，SaaS 提供者與客戶可以預期通訊會受保護，以免資料被攔截或插入惡意內容，同時繼續使用自訂網域。

保護並保全機密客戶資料

由於 SaaS 應用程式已逐漸持有更多的私密與商業機密資料，因此請務必確保您的資產受到保護，以免遭受暴力登入嘗試、資料外洩與攔截式攻擊的威脅。

這些類型攻擊的防護可先透過 Cloudflare 的 Web 應用程式防火牆 (WAF) 來達成，它可以減緩以應用程式層為目標的複雜攻擊。Cloudflare 的 WAF 依預設可保護系統不受 OWASP 前 10 大弱點的威脅，也可防衛以常見整合與語言為目標的應用程式特定弱點，例如：PHP、Magento、ordPress、Drupal、Atlassian 等。Cloudflare 的 WAF 可讓 SaaS 提供者即時建立自訂規則集以保護系統不受新發現之攻擊媒介與弱點的威脅，同時在不超過 30 秒的時間內跨 Cloudflare 的網路傳播規則。

搭配 Cloudflare 的 DDoS 保護使用時，Rate Limiting 可達成更精細的控制，以封鎖具有可疑要求速率的訪客。Rate Limiting 可減緩暴力登入嘗試，這種類型的攻擊會企圖存取應用程式或網站的未授權區域；Rate Limiting 會限制一段指定時間內來自特定 IP 位址與傳送到特定端點的要求數目。

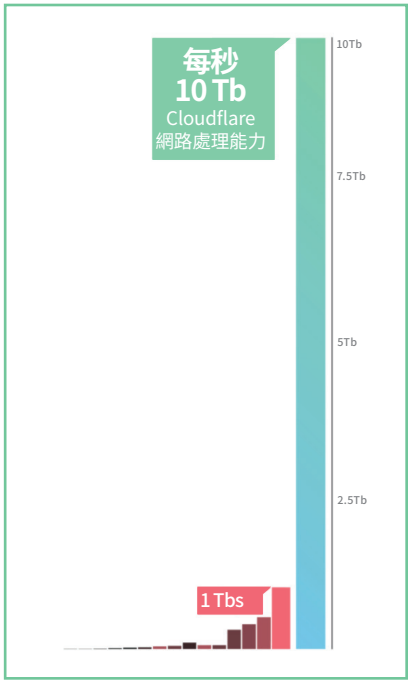
「Cloudflare 的解決方案確實有效。他們的小組完成我們的所有要求，
而且自訂的設定幾乎可立即傳播。」

zendesk | **Amanda Kleha 總經理**
Zendesk Online Business Unit

適用於 SaaS 的 Cloudflare SSL 提供最有效的方式讓您可以將自訂 CNAME 網域的 SSL / TLS 憑證管理作業自動化，進而確保不會遭受從半途攔截資料的攔截式攻擊或因為連線未加密而使得流量遭窺探。

透過封鎖惡意流量來確保可用性

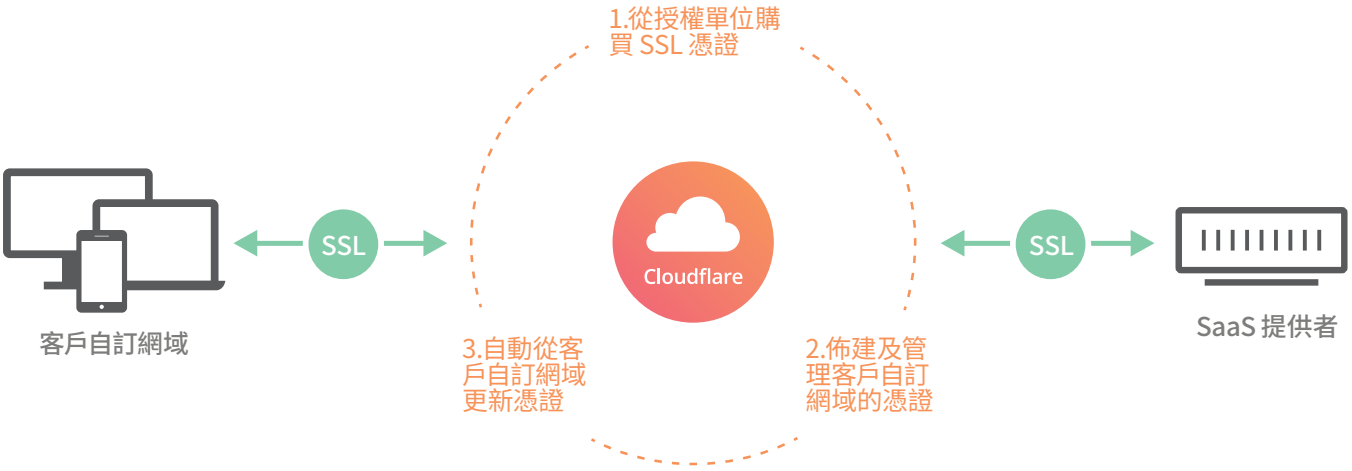
如果說客戶機密資料遭竊或遺失可能造成嚴重災難，一場成功的中斷服務可用性攻擊也可能造成同樣慘重的後果。Cloudflare 的骨幹是其全球內容傳遞網路 (CDN)，由跨 57 個國家/地區、超過 117+ 個資料中心所組成。Cloudflare 的網路輸送量總計超過每秒 10 Tb，這大約是有史以來曾記載之最大 DDoS 攻擊的 10 倍。任何以第 3、4 與 7 層為目標的體積型 DDoS 攻擊都會被吸收並平均分散到 Cloudflare 的網路中，進而協助 SaaS 客戶防止停機並確保高可用性。Cloudflare 的 Rate Limiting 解決方案搭配 DDoS 保護運作，達成更精細的控制，以封鎖具有可疑要求的訪客。當特定 IP 超過已定義的閾值時，系統會封鎖它，使其在一段已配置的時間內無法再傳送任何要求到特定端點。



適用於 SaaS 提供者的自動化 SSL 解決方案

適用於 SaaS 的 SSL 讓 SaaS 提供者可以將 Cloudflare 網路的安全性與效能優勢延伸到客戶端，並讓客戶可以使用自訂網域。適用於 SaaS 的 Cloudflare SSL 解決方案允許

客戶繼續使用 CNAME 方式將其自訂網域導向 SaaS 提供者子網域，提供品牌化 URL 的優勢，而 Cloudflare 可啟用及管理 SaaS 提供者與其客戶的整個 SSL 生命週期。在客戶網域上啟用 SSL 可提高訪客信任度、改善 SEO 搜尋排名並使用現代化 HTTP/2 通訊協定的完整功能，進而提高速度：



品牌化訪客體驗

SaaS 提供者的客戶若可以使用其自有品牌化自訂網域，則可以繼續那樣做，同時享受完全受管理之 SSL 憑證的額外優勢。以 CNAME 方式處理的自訂網域為 SaaS 客戶提供更好的品牌可見度與 SEO 排名，同時確保提高網站或應用程式訪客的信任度。

有效率地保護客戶資產

適用於 SaaS 的 SSL 可讓您以無接縫方式新增專屬 SSL / TLS 憑證到進行 CNAME 處理的自訂網域。透過 HTTPS 傳輸資料可確保安全地傳輸機密客戶資料，以免遭受攔截式攻擊與網路窺探。在已啟用 SSL 的情況下，就能使用可提供較快速度的 HTTP/2 通訊協定。

自動化生命週期管理與快速 SSL 部署

Cloudflare 會管理 SaaS 提供者以 CNAME 方式處理的客戶自訂網域的整個 SSL 生命週期，從私密金鑰簽發/保護到網域驗證、簽發、更新與重新簽發。SaaS 提供者與客戶就不需要再負責管理 SSL 生命週期。在 SSL 簽發程序期間，Cloudflare 會傳輸新的憑證要求並在數分鐘內讓 HTTPS 上線。

「身為工程師，我覺得沒有比與 Cloudflare 合作更愉快的事了。」

UDACITY

Paul Bauer
Udacity 平台工程師

重點

註冊 Cloudflare 服務以改進您 SaaS 應用程式的效能與安全性，同時輕鬆地為客戶以 CNAME 方式處理的自訂 URL 部署 SSL。設定方式非常簡單，而且通常只需要不到 5 分鐘的時間就能讓功能順利運作。在 www.cloudflare.com/plans/ 查看我們從 Free 到 Enterprise 的方案，並在 www.cloudflare.com/saas/ 深入了解 Cloudflare 為 SaaS 提供者推出的解決方案。

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