CLOUDFLARE

白皮書

事半功倍

7 間公司具有成本效益的應用程式安全性及效能策略。

報告摘要

保護 Web 應用程式和 API 免遭惡意傀儡程式、DDoS 攻擊、資料隱碼攻擊和其他漏洞是組織的一項重要工作。然而，實作可靠的安全性策略難度很大，特別是在面對預算限制和團隊發展受限的情況下。

本白皮書分享了公司使用應用程式安全性策略，成功提升效率和削減成本的真實案例。透過學習這些成功案例，企業在對使用應用程式安全性做法來精簡支出方面取得了寶貴的深入見解。

網路安全和 IT 團隊何時必須做到事半功倍

當組織面臨預算限制時，沒有團隊能夠完全不受影響。無論是因為廣泛的經濟不確定性、銷售下降、組織結構調整，還是一大堆其他理由，網路安全和 IT 團隊通常都被迫在預算未按預期增加的情況下改善營運，甚至更糟糕的是，被迫在成本大幅削減的同時這樣做。

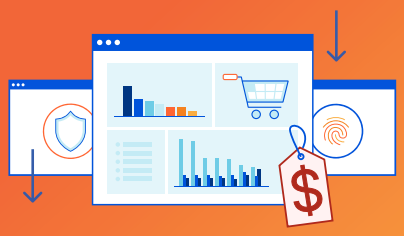
然而，在應用程式安全性和效能方面都不允許下降。在安全性方面，保護應用程式一年比一年複雜。攻擊規模和複雜度日益增長，隨著組織規模的擴大，其受攻擊面也在擴大。據估計，CVE 計畫報告稱，新漏洞數量從 2021 年到 2022 年增長了 25%，2022 年，已確認記錄總數達到了 25,059 個。

在效能方面，消費者希望每次數位體驗都是快速、可靠和個人化的。即便是很小的減速也會對參與度和轉換率產生重大的影響，如果公司不能滿足客戶的期望，就會陷入困境。

當面對預算限制和預期上升的雙重壓力時，網路安全和 IT 團隊必須想方設法做到事半功倍。本白皮書將討論在不犧牲結果的情況下，有效建立具有成本效益的安全性及效能做法的公司案例。

在應用程式安全性做法中削減成本的方式

在保護 Web 應用程式和 API 免受現代威脅時，最佳防禦不僅會提供分層安全服務，還可讓組織削減不必要的支出。為了實現這一點，組織可能會使用若干主要策略，包括廠商整合、精簡憑證管理、為免受提高流量成本的攻擊提供專門保護以及輸出費用減免。



透過安全廠商整合降低成本

透過自動化憑證管理精簡人力和基礎架構成本

封鎖提高流量成本的攻擊

消除非預期費用和成本，如頻寬、雲端和輸出費用

透過安全廠商整合降低成本

Gartner 最近的一項調查表明，75% 的公司正在安全性做法中探索廠商整合。透過減少所依賴的廠商數，組織可以最佳化供應鏈流程並實現更高的效率，進而降低成本。

Chrono24 是一間全球領先的線上豪華手錶賣場，透過與 Cloudflare 整合減少了對多個廠商的依賴。

在轉換之前，Chrono24 使用 EdgeCast 的 CDN 解決方案以及其他數個廠商的 DDoS 緩解和 WAF。混合使用多個解決方案會導致效能較差，不僅延遲明顯、網路安全效能較低，也浪費了廠商支出。

在與 Cloudflare 的解決方案（包括 CDN、WAF 和 DDoS 緩解）整合之後，Chrono24 的網站安全性及效能成本下降了 67%。

技術總監 Sven Ferber 表示：「現在，我們將效能和安全性整合到一位提供者中，因此大大降低了基本成本。」「我估計，我們現在的支出大約只佔原來的三分之一。」

廠商整合是一種極為高效的策略，可幫助企業精簡購買和管理支出。當您尋求整合廠商時，可以使用以下三個簡單問題：

1. 您的廠商是否提供威脅保護並提高應用程式效能？
2. 您能否透過一個主控台管理應用程式和 API？
3. 您組織中的多個團隊能否利用同一廠商來提高預算效率？

透過遵循上述整合技巧，組織能夠降低成本、簡化供應鏈管理，並強化與主要廠商的關係。

chrono24
The World's Watch Market

重點

75% 的公司正在探索廠商整合

Chrono24 在與 Cloudflare 整合後，網站安全性和 IT 成本下降了 **67%**

透過減少廠商數量以及整合服務，公司可以**降低成本**並簡化供應鏈管理

透過自動化憑證管理精簡人力和基礎架構成本

對於 IT 團隊而言，在多個網域和地理區域部署網路安全設定的過程不僅成本高昂，而且非常耗時。而隱藏成本可能會為其支援的組織帶來額外的麻煩，特別是那些面臨預算限制的組織。

這些隱藏成本通常隱藏在憑證管理中。SSL/TLS 憑證構成了網路的數位身分。平均而言，一個企業的 Web 空間可能需要數百個甚至數千個憑證。但是隨著人力和基礎架構支出的積累，管理這些憑證的成本可能極為高昂，更不用說非預期憑證服務中斷造成的虧損了。

電子商務平台 SHOPYY 使用 Cloudflare 自動管理 SSL 憑證，包括私密金鑰建立、保護、網域驗證、發行、續訂和重新發行。

起初，SHOPYY 使用的是一款免費的憑證管理工具，所提供的憑證不僅不可靠，有效期也很短。因此，SHOPYY 不得不雇佣更多的員工來監督憑證管理和續訂過程。

使用 Cloudflare SSL for SaaS，SHOPYY 將憑證管理流程委託給 Cloudflare，只需一名內部員工即可維護整個流程。

「使用 Cloudflare 產品後，僅在營運和維護方面，成本就降低了 60%，」創辦人暨技術長 Yuanming Chen 說道。

無效的憑證管理做法還會因為憑證過期而影響收益。線上借貸市場 LendingTree 使用 Cloudflare 的 TLS 憑證來節省資金和防止服務中斷。

「我們擁有數千種不同的資產。在如此大的規模下，錯過憑證續訂只是時間問題，」應用程式安全性主管 John Turner 說。「利用 Cloudflare 可自動續訂的 TLS 憑證，**我們一年可節省大約 50,000 美元，這包括管理成本以及因憑證過期導致服務中斷而造成的虧損**。」

內建一個有效的憑證管理系統也有助於適當地重新分配資源。成立於德國的 mogenius 是一個部署基於雲端的應用程式的自動化平台，它藉助 Cloudflare 自動執行憑證管理做法，讓公司能夠將更多的時間用於發展核心業務。

「在內部管理 Cloudflare 為我們所做的一切會佔用我們至少 20% 的時間。」共同創辦人暨 CPO Jan Lepsky 說。「**有了 Cloudflare，我們可以專注於為客戶最佳化雲端開發和部署管線。**」

如果企業尋求避免隱藏成本和確保業務順利營運，則卸下憑證管理工作至關重要。低效、手動或拼湊式憑證做法會導致高昂的人力和基礎架構支出，因憑證過期中斷而造成虧損，以及資源分配浪費。

透過使用 SSL for SaaS 或 TLS 憑證等功能實作憑證管理，企業能夠節省大量成本並提高盈利。

SHOPYY

lendingtree

mogenius®

重點

使用 Cloudflare SSL for SaaS，SHOPYY 的營運和維護成本降低了 60%

Cloudflare TLS 幫助 LendingTree 在管理成本和虧損方面一年節省了 50,000 美元

Cloudflare 讓 mogenius 能夠自動執行憑證管理做法——騰出 20% 的時間專注於核心業務

封鎖提高流量成本的攻擊

隨著 API 使用的增加，受攻擊的面積也在擴大。惡意傀儡程式、DDoS 攻擊和其他威脅可能會入侵應用程式和 API，而行政主管和技術領導者特別清楚這些攻擊可能會對企業造成的重大影響。

據估計，API 不安全導致企業每年損失最多 7500 萬美元。

這些攻擊會導致憑證填充和 DDoS 攻擊，不僅會中斷合法使用者的服務，還會迫使組織不得不承擔攻擊流量導致的流量激增的成本。

LendingTree 在先前的安全廠商花費了大量資金，該廠商在 DDoS 攻擊期間向他們收取了激增定價。這種模式不僅產生了巨大的超額成本，而且還封鎖了合法流量。

「每當我們播放新的電視廣告或推出新的社交媒體活動時，要求即會暴增並超過廠商讓我們指定的任意限制，這表示廠商會將暴增情況視為 DDoS 攻擊並封鎖合法流量，」應用程式安全性負責人 John Turner 回憶道。**「我們不但損失了那些潛在客戶，也損失了我們用於讓他們造訪網站的成本，而且廠商還會向我們收取『DDoS 保護』的費用。」**

為了解決這些低效的問題，LendingTree 開始採用 Cloudflare 的 Bot Management 和 Rate Limiting 功能。**在 48 小時內，對特定 API 端點的攻擊下降了 70%，而在不到 5 個月的時間，LendingTree 透過阻止 API 端點濫用節省了 250,000 美元。**

當線上遊戲控股公司 Flutter Entertainment 意識到，將近 70-90% 的流量是惡意流量時，他們需要一個解決方案來篩選和封鎖惡意傀儡程式。在實作 Cloudflare Bot Management 後，**Flutter 的惡意流量減少了 90%，每年可節省 200 多萬英鎊。**

使用傀儡程式管理和 DDoS 保護，組織可防止攻擊和 API 濫用，並減少與攻擊相關的支出。當探索安全廠商時，組織應尋找以下廠商：

- 使用機器學習根據觀察到的流量資料設定速率限制
- 超出基於地理和 IP 位置的速率限制，因為現代攻擊可以輕鬆繞過 IP 限制
- 確保開發人員透過 WAF 和 API 閘道路由傳送所有 Web 應用程式和公用 API 流量
- 整合 DDoS、WAF 和 API 閘道工具，進一步增強分層威脅防禦
- 確保在企業處理流量的位置部署保護措施來減少延遲
- 提供非計量 DDoS 緩解來消除支付的超額費用

透過實作正確的廠商/安全性策略，每年可節省數千甚至數百萬美元。

Flutter™

重點

據估計，API 不安全會導致企業**每年損失最多 7500 萬美元**

實作正確的應用程式安全性工具，**每年可節省數千甚至數百萬美元**

採用 DDoS 保護，LendingTree 在 48 小時內遭受的特定 API 攻擊下降了 70%，而在不到 5 個月的時間，透過阻止攻擊節省了 250,000 美元

Cloudflare Bot Management 幫助 Flutter 將惡意流量減少了 90%，並且每年節省 200 多萬英鎊

消除非預期費用和成本，如頻寬、雲端和輸出費用

許多網路安全服務都依賴於雲端，而多個雲端提供者都向企業收取儲存和計算費用。此外，他們通常還要求企業支付資料輸出費用，這是從儲存空間傳輸資料的關聯支出。

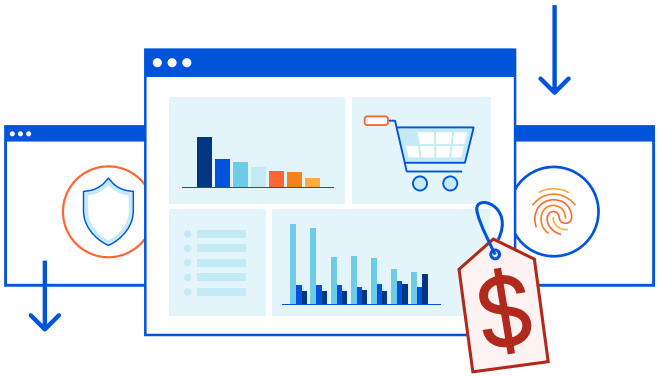
輸出費用是根據多種因素計算的，例如，客戶層級、訂閱類型和傳輸的資料量。基於上述原因，這些費用往往很難預測 — 當它們開始不斷積累時，可能會對組織造成很大的損失。實際上，IDC 估計輸出費用金額至少佔雲端儲存成本的 6%。

考慮到這一點，歐洲數位目錄和區域搜尋服務 PagesJaunes 決定實作 Cloudflare CDN 來幫助減少頻寬費用，並改進快取和 DNS 管理。

「我們很快注意到，Cloudflare CDN 吸收的流量意味著，我們的基礎架構壓力更小，更具彈性，」架構、效能和網路安全主管 Loïc Troquet 強調道。「**70% 的頻寬不再需要由 Solocal 的基礎架構提供服務。**」

而頻寬節省也會帶來成本節省。採用 Cloudflare 的 CDN、DNS、WAF 和 DDoS 緩解服務後，線上學習工具 **Quizlet 每天節省了總計 10 TB 的頻寬，並將 Google Cloud Services 網路輸出帳單降低了 50% 以上。**

實作應用程式安全性策略和做法可消除非預期的輸出費用。



PagesJaunes

Quizlet

重點

實作應用程式安全性策略（例如，選擇正確的 CDN 廠商）可以消除非預期的輸出費用

使用 Cloudflare CDN，PagesJaunes 的頻寬減少了 70%

Quizlet 使用 Cloudflare **每天節省了總計超過 10 TB 的頻寬**，並將 Google Cloud Services 網路輸出帳單降低了 50% 以上，因此，每月可節省數千美元

使用 Cloudflare 精簡應用程式安全性和削減成本

使用 Cloudflare，組織可以內建應用程式安全性策略來提高效率並精簡支出。Cloudflare 的整合式應用程式安全性產品組合匯集了一流的非計量 DDoS 保護、可阻止最進階攻擊的 Web 應用程式防火牆、主動 API 安全性、由威脅情報提供支援的傀儡程式管理以及進階用戶端攻擊偵測。

有興趣嗎？

立即連絡 Cloudflare

CLOUDFLARE

+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES/4588.2023JUN05