CLOUDFLARE

白皮書

維持 PCI DSS 4.0 合規性的戰略方法

目錄

概觀

處理信用卡、轉帳卡或預付卡的所有組織都必須遵循支付卡產業資料安全標準 (PCI DSS)。這包括小型商家、零售商、電子商務網站、銀行和大型企業。然而，由於向雲端和混合式工作的遷移，以及標準的不斷演變（如 PCI DSS 4.0 的推出），導致很難有效遵循該標準。

對於這個數位現代化的世界，需要採用一種全新的方法，透過一種可擴展的方式來簡化合規流程，從而讓組織能夠跟上與企業數位現代化保持同步的動態監管環境。

當今組織面臨的 PCI DSS 合規性挑戰

PCI 合規性至關重要，違規者會面臨罰款、訴訟和政府調查。然而，合規性為金融機構、電子商務商家以及其他受其監管的組織帶來了一些挑戰。

由於越來越依賴於雲端運算和遠距工作，IT 團隊失去了對數位環境的控制，而解決這些挑戰的過程也變得更為複雜。

時間和資源配置：53% 的組織表示，技術隱私職務人手不足，導致合規性面臨嚴峻的挑戰[1]。

技術堆疊整合的複雜性：透過整合並維護必要的技術來滿足合規性標準（例如，加密和防火牆設定）往往是很複雜的。而對於使用傳統系統的組織或正在進行數位化轉型的組織而言，這一挑戰就更複雜了。

廠商合規性：確保第三方服務提供者和廠商遵循 PCI 標準進一步加劇了複雜性。

不同環境中的資料安全性：隨著雲端運算和行動支付的興起，在通常受到較少控制的各種不同環境中確保合規性越來越困難。

稽核：IT 團隊必須在所有的基礎架構和系統中維護最新的稽核記錄，以確保合規性。

使用 PCI DSS 4.0 應對複雜的網路威脅

PCI DSS 4.0 於 2022 年 3 月 31 日發佈，並於 2024 年 3 月 31 日生效，其他要求將於 2025 年 3 月 31 日生效。PCI DSS 4.0 的目標是[2]：

1. 繼續滿足支付產業的安全性需求

- **增強驗證要求：**更加強調驗證，特別是對進入持卡人資料環境 (CDE) 的所有存取的多重要素驗證。密碼要求也更嚴格，從最少 8 個字元增加到了 12 個。
- **增強加密要求：**PCI DSS 4.0 要求針對持卡人資料的儲存和傳輸使用「增強式」加密，例如，不易受已知漏洞利用的 TLS。
- **用於應對持續威脅的全新電子商務和網路釣魚要求：**為了實現用戶端安全性以及抵禦網路釣魚和社交工程攻擊，PCI 4.0 新增了更多要求。

2. 持續不斷地提升安全性

- **更加注重風險分析和管理：**鼓勵組織實施持續的風險分析和管理流程，以便立即識別並解決漏洞。
- **更加重視問責和控管：**新版本更注重對持卡人資料的控管以及對維護安全控制的問責。
- **為實施和滿足安全性要求提供更多指導：**PCI 4.0 闡明了該標準的目的以及所使用的時間範圍。

3. 增加對不同方法的靈活性

- **整合新技術：**PCI DSS 4.0 解決了雲端和行動支付系統等新興技術的安全性問題。
- **為組織實現安全目標提供更多的靈活性：**組織可以使用「自訂方法」（更多樣的方法）來滿足要求。而 PCI 4.0 提供了更多的靈活性，根據針對性的風險分析來確定他們執行動作的頻率。

4. 增強驗證方法

- **連續監控和測試：**新標準鼓勵從年度合規性驗證轉向連續的安全性與合規性監控。
- **增強合規性評估與證明之間的一致性：**合規性自我評估問卷或報告中的資訊與合規證明中總結的資訊更加一致。

解決方案：透過 Cloudflare 的全球連通雲，採用一種全新的方法來滿足 PCI 要求

安全與 IT 團隊需要透過一種簡單且可程式設計的方式來滿足 PCI 要求，這種方式不僅可與目前的安全和技術堆疊輕鬆整合，還要隨著基礎架構和 PCI DSS 的演變而保持這種狀態。

答案並不是將很多傳統和單點安全解決方案混合起來。相反，團隊需要一個統一的雲端原生安全和網路服務平台，專門設計用於幫助企業重新控制 IT 環境，並滿足包括 PCI 在內的各種合規性要求。我們將這樣的統一平台稱為全球連通雲。

Cloudflare 全球連通雲可提供：

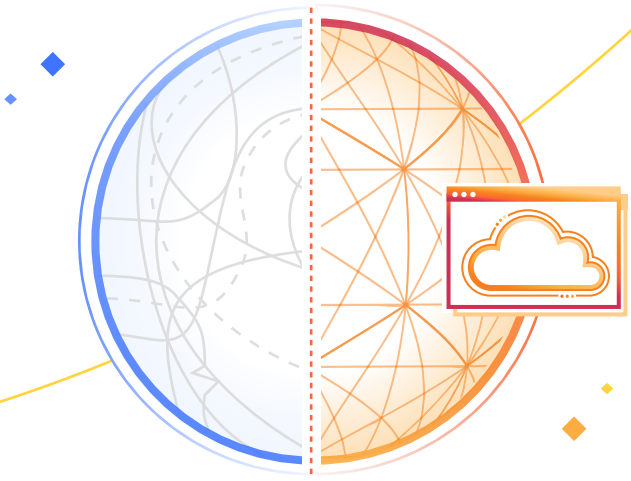
- 一個專為滿足資料合規性而設計的平台
- 一個統一的原則引擎
- 毫不妥協的資料主權
- 用於滿足稽核要求的智慧型報告

使用 Cloudflare，IT 團隊可以在不同的位置套用一致的控制，使用單一控制平面隨時隨地啟用控制。

團隊可將記錄從 Cloudflare 邊緣直接傳送至偏好的 SIEM 或雲端目的地進行稽核。此外，Cloudflare 對網際網路流量的大規模洞察還意味著，Cloudflare 可以自動識別並抵禦新型威脅。

Cloudflare 本身符合 PCI 標準，並且原生支援 PCI DSS 4.0 要求。例如，藉助 Cloudflare，IT 團隊能夠輕鬆實施多重要素驗證，而這正是 PCI DSS 4.0 的一大重點。此外，Cloudflare 也支援最新的加密標準，並經常為其增添內容，從而幫助客戶滿足 PCI DSS 4.0 對敏感性資訊加密的要求。

PCI DSS 要求與 Cloudflare 全球連通雲功能的對應摘要請見下一頁：



Cloudflare 有助於滿足 PCI 要求的關鍵領域*

PCI 要求	Cloudflare 功能
1. 安裝和維護網路安全控制項（以前稱為「安裝和維護防火牆」）。	Cloudflare 可保護網路、應用程式和雲端部署都免受惡意網路流量的影響。Cloudflare 使用來自每日數千億個威脅的威脅情報，保護網站和 Web 應用程式免遭基於 Web 的威脅，包括 OWASP 十大攻擊和 zero-day 攻擊。它的安全平台是雲端原生的，幾分鐘內即可完成部署，並可讓使用者在數秒鐘內推出全球原則變更。
2. 對所有系統元件套用安全設定。	位於 Cloudflare 背後的使用者、裝置和應用程式經過增強加密，可以免遭 Web 上潛在攻擊者的威脅。Cloudflare 的 API 護盾可讓使用者透過識別序列並強制執行有關 API 交易的原則，針對 API 中的漏洞建立防禦。
3. 透過加密或其他資料保護方法保護儲存的資料。	Cloudflare 不僅可以識別待用個人識別資訊，還可滿足持卡人記錄保留時間的要求。
4. 在開放的公用網路上加密持卡人資料。	在 Cloudflare 全球網路中傳送的流量滿足在此要求中指定的加密標準，而 Cloudflare 可以封鎖使用者進行識別所需的個人識別資訊的傳輸。
5. 保護所有系統和網路免遭惡意軟體的攻擊。	Cloudflare 每秒處理超過 5,500 萬個 HTTP 請求，為我們提供了一個廣泛且獨特的最新攻擊視角。Cloudflare 為使用者提供了一個反惡意程式碼保護套件，包括防病毒、雲端電子郵件安全性和遠端瀏覽器隔離。
6. 開發並維護安全的系統和軟體。	Cloudflare 可以對使用者的安全違規行為以及在 SaaS 應用程式內偵測到的設定錯誤進行排名和加權。Cloudflare 的安全服務可以保護所有面向 Web 的公共應用程式免遭已知攻擊和漏洞利用。
7. 在「需要知道」的基礎上限制持卡人資料存取。	無論使用者位於何處或資料儲存於何處，Cloudflare 都可以強制執行最低權限的精細存取控制。
8. 識別使用者並驗證對系統元件的存取。	Cloudflare 可以針對流經其全球網路的任何流量，實施基於身分的原則和安全狀態檢查（例如，是否使用了 MFA）。
10. 記錄並監控對系統元件和持卡人資料的所有存取。	Cloudflare 在其平台的所有產品中提供精細的稽核記錄，並與大多數主要 SIEM 整合。
11. 定期測試系統和網路的安全性。	除了針對所有主要產品提供深度記錄以外，Cloudflare 還提供有限存取原則測試和入侵偵測服務功能。

*Cloudflare 不支援 PCI DSS 4.0 要求的第 9 條和第 12 條，它們與實體安全和組織結構有關。

總結：依賴 Cloudflare 幫助滿足 PCI 合規性要求

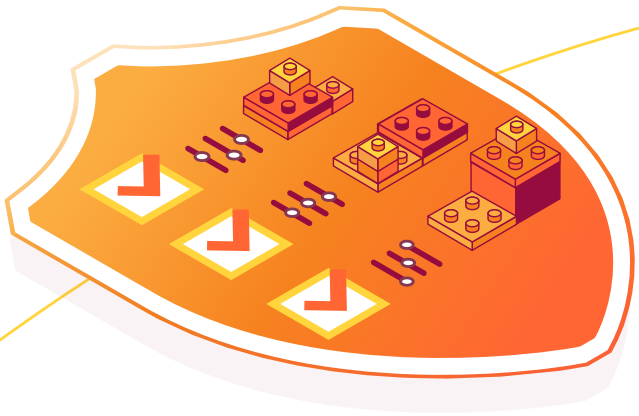
Cloudflare 符合 PCI 標準，無論客戶採用何種基礎架構，都能夠幫助他們自行滿足合規性要求。

實際上，使用 Cloudflare 可將資料外洩可能性降低 65%[3]，年度網路保險費降低 24%[4]，在管理系統和流程方面花費的時間減少 59%[4]。

我們的企業客戶根據合約規定要求 Stax 滿足非常具體的合規性標準。這導致我們必須在基礎架構中實施 Zero Trust 等安全控制……Cloudflare 依照我們的需求，絲毫不差地完成了工作。它既保護了我們的端點，也保障了我們的安全性[5]。」

Troy Ridgewell
Stax 網路安全主管

STAX



立即瞭解 Cloudflare 資料合規性解決方案。
與專家討論以開始使用。

參考文獻

1. https://www.isaca.org/about-us/newsroom/press-releases/2023/privacy-staff-shortages-continue-amid-increasing-demand-for-these-roles
2. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4-0-At-A-Glance.pdf
3. IBM 2022 年外洩成本報告
4. 2023 年 Cloudflare TechValidate 對 Cloudflare 應用程式服務客戶的調查
5. https://www.cloudflare.com/case-studies/stax/

CLOUDFLARE

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

REV:BDES-5776.2024APR09