

支付卡產業 (PCI) 法規遵循

PCI 法規遵循

PCI 組織創立於西元 2004 年，目的是為了建立支付卡產業的共同安全需求－資料安全標準(DSS)，期望被所有的信用卡組織所接受。這些信用卡組織包括：American Express、Discover Financial Services、JCB、MasterCard Worldwide 和 Visa International。這個標準主要是定義持卡人與卡片上的資料如何安全地儲存、管理與處理。

PCI 如何影響客製化的應用程式？

PCI 具體規定－信用卡某些類型的資料應該永遠不會被儲存，不應該出現在資料庫，也不應該出現在交易記錄中，即使資料加密。我們商業應用軟體（嵌入式 POS 設備、電子商務網站）如何處理敏感性資料？在應用軟體的其它地方儲存該資料？或許在除錯的記錄中？應用軟體有試著去徹底清除記憶體內的敏感性資料來確保惡意使用者無法去利用軟體弱點來揭露非授權的資訊？

在 PCI 規範下，組織必需保護持卡人資料，這些包括：

- 所有個人識別(ID)資訊
- 主要帳號資訊(PAN)
- 服務代碼
- 到期日
- 社會安全碼
- 會員資料號
- 其他廠商搜集的電子資料，這些包括：信用卡錄音檔(.wav, .mpg)，例如：訂房或是訂票。
- 針對持卡人的個人見解資訊
- 住址與電話號碼

誰必須遵守？

西元 2006 年成立的 PCI Security Standard Council 組織負責發展與維持 PCI DSS 標準。違反該標準的組織將遭受高達每次\$50 萬的罰款。只要有儲存、處理或傳輸持卡人資料的所有的商家和服務提供商都必須遵守。本標準適用於所有支付通道，包括零售業（實體商店），郵遞/電話訂購和電子商務。

Fortify 如何協助 PCI 法規遵循？

PCI 法規遵循	Fortify 可以協助
6.5 節：發展安全的系統與應用程式 - 開發的 Web 應用程式應該依據安全編碼原則，例如：OWASP Top 10 - 重新檢視客製化的程式碼，以識別程式碼弱點 - 必須考慮一般弱點的防護	Fortify SCA 是原始碼分析工具，可用來協助開發安全的應用程式 - 擁有最全面的安全編碼的規則知識庫，這些包含： - OWASP Top 10 - PCI 相關的規則，例如：把信用卡的卡號寫至 log 檔 - 能夠掃描百萬行原始碼大型的專案 - 低誤報率 - 可擴展以滿足獨特的源碼庫
6.6 節：確保公眾 Web 應用程式能抵擋一般常見的攻擊 - 在 Web 應用程式前端安裝應用層防火牆 - 所有客製化程式碼必須經由應用程式安全領域專家審查一般的弱點	Fortify Defender(RTA)提供最準備確與有效的應用程式防火牆 - 尖端的防火牆技術來保護 Web 應用程式 - 詳細的應用程式攻擊鑑識駭客資訊：何時與如何 - 利用應用程式的語意方式比其它技術擁有更深入與精確地識別全面的弱點。
6.7 節：能夠提供溝通法規遵循狀態的詳細報表 - 弱點稽核報告 - 應用程式防火牆狀態	Fortify Manager 可產生 PCI 法規遵循的詳細活動與狀態之報表 - 弱點稽核報表 - 應用程式防火牆報告將說明：誰正在攻擊、使用什麼技術在攻擊、攻擊的頻率以及其它更多的資訊 - 以 Report Card 的方式呈現每一類重要的法規遵循的類別的安全狀態 - 詳細的未遵循法規的稽核結果 - 可提供下拉式程式碼的方式來檢視

- 除了 OWASP Top 10 報表外，還包含了全面性的安全範本。完整的弱點清單在 Fortify 網站上的 <http://www.fortifysoftware.com/vulncat/>

Fortify 如何展現 PCI 法規遵循？

案例 1：利用 Fortify Defender(RTA)佈署應用程式防火牆

有一間未通過 PCI 法規的大型的電子商務網站。他們要保護網路的安全時，由於缺乏適當的應用程式層保護而失敗了。愈來愈多的應用程式層的攻擊，Fortify 的客戶意識到有必要加強其應用程式防護—不僅僅是 PCI 法規遵從—還有確保私密資料不被駭。藉由 Fortify RTA—強大的應用程式防火牆，同時也有準確的攻擊度量後，可以進一步了解攻擊取證，因此客戶可受到強力的保護。

案例 2：使用 Fortify SCA 來提升與滿足源碼稽核的要求

這個案例是一家頂尖的線上零售業，利用 Fortify SCA 來識別與修復任何在原始碼發現的弱點問題。由於這家公司是大型的商業公司，常遭受外來的攻擊。他們需要導入原始碼檢核，也知道手動檢視原始碼曠日廢時。自從使用了 Fortify SCA 後，可以藉由快速地掃描所有的程式碼而加快審核流程，並且識別弱點與產生問題清單以及修復建議的圖示報告。