imperva

# Imperva On-Premise WAF
# 網頁應用程式防火牆

**Imperva網頁應用程式防火牆是唯一連續9年位於 Gartner WAF/WAAP 領導象限的廠商**

Imperva 目前於全球超過70個國家有使用客戶，已有超過2600家客戶使用，各個產業皆有採用Imperva解決方案之客戶，如政府、電信、金融、電子商務、製造業等領域。台灣也已有超過130家客戶使用，且使用客戶持續快速增加中。

## 特色

- 自動學習：自動且動態白名單學習機制及政策調整，大幅減少維運人力及時間
- 彈性佈建：用戶可彈性選擇Inline或sniffing方式，不須更動現有架構及程式，並具有集中控管機制
- 使用者追蹤分析技術：讓事後的應變追查更加快速有效
- 操作簡便：不需要專業能力及可操作使用，功能分類清楚，內容詳盡
- 報表系統：內建符合國際法規的報表範本
- 分權控管：權限控管系統，各司其職
- 即時更新：由原廠維護，每周更新報表範本、政策定義、黑名單...等
- 整合弱點掃描：可匯入網頁弱點掃描報告，並提供資料庫弱點評估功能
- Threat Radar：結合第三方專業機構，及時防護最新攻擊事件
- 服務：原廠支援團隊分布兩地，真正做到跨時區，提供7x24小時專業服務

## 法規遵循

- Imperva 系列產品可滿足個資法施行細則第9條-要成立管理組織及投入適當資源保護個人資料之規定。
- Imperva WAF 可滿足政府資安等級A、B級單位對網頁應用程式防火牆的部署要求。
- Imperva 網頁應用程式防火牆可幫助企業滿足支付卡產業資料安全標準(PCI-DSS) 6.6的要求，並防護OWASP Top 10及新興威脅的攻擊。
- 符合上市櫃公司資通安全控管指引.第十八條.第五項，如有對外服務之核心系統，具備應用程式防火牆規範

# 特色一覽表

## 精確監控和保護網頁應用程式

Imperva 網頁應用程式防火牆採用多層檢查和多重安全防護來提供最安全的保護。

- **HTTP(S)協定驗證**

  HTTP(S)協定驗證可以防止包括緩衝區溢位、惡意編碼、HTTP 偽裝以及非法伺服器操作在內的協定濫用。 彈性的規則讓使用者可以嚴格遵守 RFC 標準，同時支援各種靈活多變的應用程式。

- **防止資料洩漏**

  Imperva 檢查伺服器回應資訊以識別潛在的敏感資料(如持卡人資料和身份證字號)洩漏。除了報告還在應用程式中何處發現了敏感資料外，還可以選擇讓Imperva 阻止這些資訊從企業網站洩漏。

- **網路及平台防護**

  Imperva 針對網頁伺服器弱點、中繼軟體弱點和平台弱點中的已知攻擊提供廣泛的保護，這些已知攻擊的資訊來源是 Imperva 應用防禦中心(ADC)提供的超過6,500個特徵碼。ADC 特徵碼不僅包括Bugtraq、CVE®和Snort®來源發現的攻擊，還包括透過ADC研究發現的威脅。Imperva還可透過檢測和識別網頁爬蟲獨特的特性組合來抵禦零時差的新爬蟲攻擊。

- **無與倫比的準確度**

  Imperva 獨特的關聯攻擊驗證技術，可準確識別最複雜的攻擊。

- **網頁服務保護**

  Imperva 透過動態學習網頁服務的行為來保護這些應用，包括 XML檔、元件、屬性、架構、變數和簡單物件連結協定(SOAP)。Imperva將識別並阻止任何嘗試竄改正常網頁服務的行為，還會抵禦應用程式中常見的威脅，如SQL注入、XSS、CSRF等。

## 自動化安全操作

- **自動應用學習**

  Imperva 獨特的動態建模技術可自動學習被保護 網頁應用的結構、元件和預期使用模式。動態建模持續自動檢測有效的應用模型中。透過對比Web請求與行為模型，Imperva WAF能夠精細的檢測不可接受的行為，並防止惡意活動。

- **網頁應用程式使用者追蹤**

  Imperva 使用動態建模技術自動獲取Web應用的使用者名稱並將後續所有會話活動與這個使用者名稱的關係連接在一起。因此 Imperva WAF 能夠依使用者進行監控、實行策略和稽核。

- **來自ADC的最新安全解決方案**

  Imperva ADC 是國際知名的安全研究機構，持續調查全球各地的漏洞，分析來自眾多不同網站的非法探測流量，並進行根本性漏洞研究來識別最新威脅。研究的結果就是提Imperva各設備的最新防護措施，包括特徵碼更新，協定驗證規則和關係連接規則。

## 使用非入侵式的部署

- **不需要更改網路或應用程式**，Imperva在業界所有網頁應用防火牆中提供的建置部署選項最多，包括不需要更改任何網路應用程式的透通橋接建部署項目。

  Imperva 提供每秒數 GB的傳輸量、數萬次的交易處理量，同時還能將延遲時間保持在低於毫秒的等級。

## 提供企業級的集中管理

- **支援分散式部署**

  Imperva 可作為獨立設備進行部署，也可進行擴展以保護大型或分散式資料中心。Imperva MX 管理伺服器提供集中式配置、監控和報表基礎架構，以便從單一控制台管理多個設備和安全政策規則。

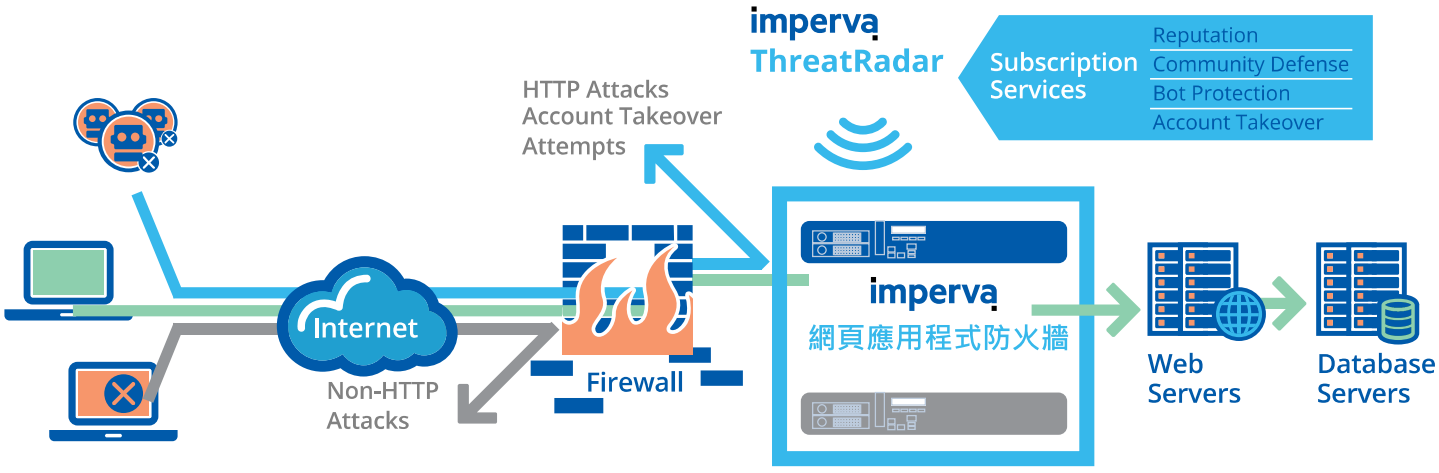
- **同等級產品最佳監控和報表功能**

  即時集中展示頁面提供一個高階的系統狀態與安全事件圖形，可以很方便地對告警進行搜尋、排序，還可以直接將其連結到相對應的安全規則。

  Imperva提供豐富的圖形報表功能，使客戶能輕鬆地瞭解安全狀態並符合法規要求。Imperva 提供預設的報表，也提供基於Web應用的客製化報表。可以按需求查看報表，也可以每日、每週或每月透過電子郵件發送。

## 整合第三方應用程式

Imperva 整合大型企業Web應用程式防火牆的整體安全活動，包括 SIEM 和日誌管理的領導解決方案、基於角色進行身份驗證和用於弱點評估的網頁應用掃描解決方案。



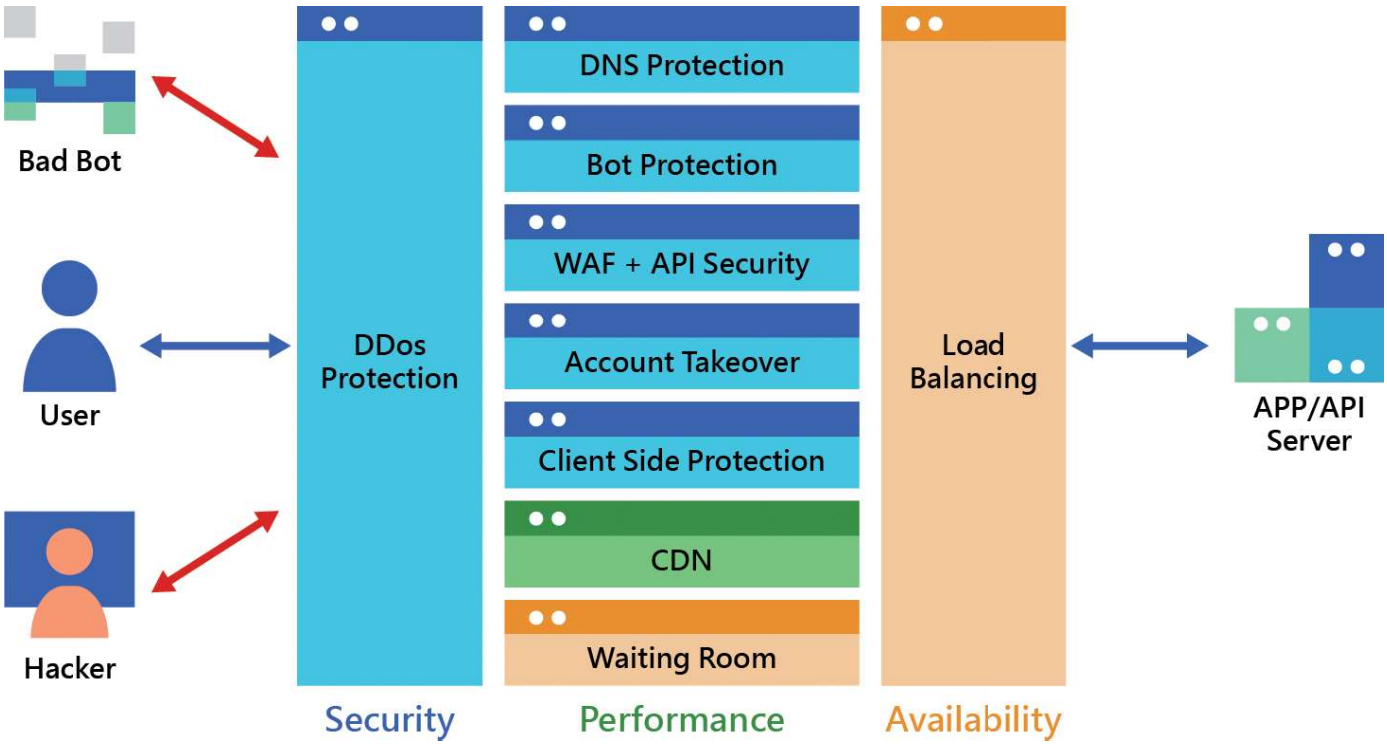

Imperva 可支援多種部署設定選項，包括Layer2 Bridge、Proxy和Non-Inline方式。

imperva

# Imperva Application Protect
# 將安全整合一體

Imperva Application Security 防護技術，是 100% 基於雲端的安全解決方案，提供不同等級的服務內容，能同時滿足各種客戶的需要， Imperva 的防護功能有 CDN、WAF、DDoS、API 安全、ATO 帳戶竊取和 Advanced Bot Protection 進階機器人檢測保護，產品獲得 PCI 認證，可用於保護網站和應用程式免受外部威脅，包括：OWASP 十大威脅、駭客攻擊、惡意機器人、漏洞掃描、DDoS緩解、SQL Injection 、XSS (Cross-Site Scripting)、撞庫攻擊等各種惡意攻擊。

Imperva 防護的核心是透過客戶執行簡單的 DNS 變更，將所有網站流量導向部署在全球的 Imperva 雲端處理中心，透過獨特的檢查技術，將發送到網站的每個請求都進行過濾，處理任何類型的惡意活動，保護網站免受已知和未知的威脅。Imperva 以接近零的誤報率來阻擋這些惡意攻擊行為，確保您的設備在受到攻擊後的幾分鐘內就能受到完整防護。




Imperva Application Security 完整保護解決方案

## 高可用性的全球的雲端處理中心

Imperva 為安全而建立的全球雲端處理中心，包含台灣在內，共有 51 個雲端處理中心 (PoP)，每個處理中心都具備 Application Security 全部功能，確保您的網路流量可以從最近的雲端處理中心進行清洗，不必從一個 PoP 跳到另一個。

鄰近的日、韓、新加坡、香港與泰國都有設置處理中心，Imperva 透過先進的軟體開發技術創建了一個 DDoS 清理中心虛擬池，可以在需要時進行全自動分配流量，並相互調用資源來應對惡意流量攻擊。

**Imperva 全球雲端處理中心**

○Operational ○Planned

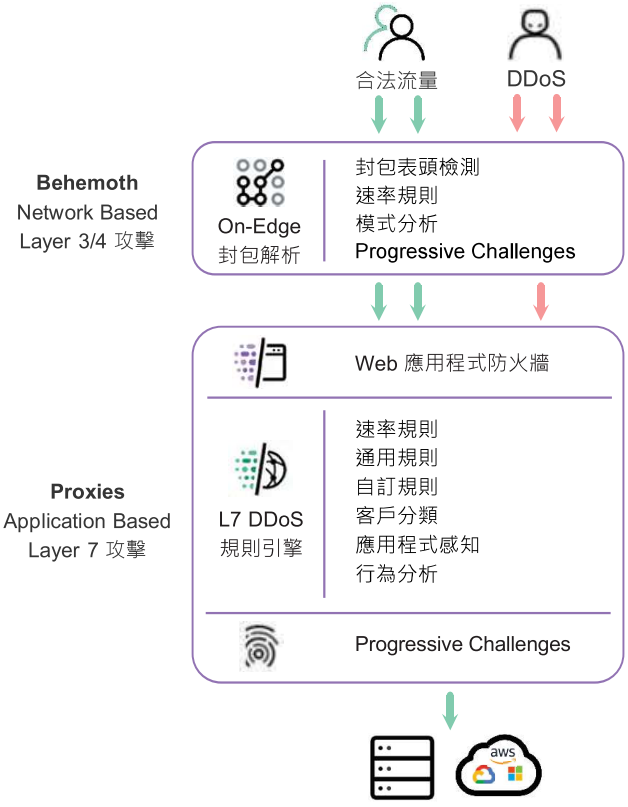
- 99.999% 的正常運行時間
- 全球 95% 區域存取低於 50 毫秒延遲
- DDoS 提供 SLA 保證 3 秒內完成清洗
- 每分鐘阻擋 25,00,000 個惡意請求

## 3 秒內完成各種 DDoS 清洗處理的信譽保證

Imperva DDoS 透明緩解防護技術，可以讓使用者免受任何類型的 DDoS 攻擊，不論是網路第 3 層、第 4 層或是應用程式第 7 層的攻擊行為，都能保證您的網路存取者和您的設備在DDoS 攻擊中永遠不會受到影響，不論主機是設置在地端或是雲端，都只有合法的連線能被轉發到服務主機。

防護的目標可以是網站、DNS、網段，甚至單一IP，並支援多種網路協定和部署方式，包括 GRE 路由、Cross Connect和 Equinix Cloud Exchange 等。Imperva 提供每秒 9+ Tbps 和 650億個封包的清理能力，並使用先進的來源識別技術，以保證3秒內啟動防護，完成任何攻擊行為的阻擋。

Imperva 有經驗豐富的網路維運中心（NOC），工程師團隊也提供 7x24 的技術支援，能不間斷進行實時監控與策略調整。



## 針對最複雜的安全威脅提供企業級保護

Imperva Cloud WAF 提供業界領先的 Web 應用程式安全防火牆，針對最複雜的安全威脅提供企業級保護。作為基於雲的 WAF，無論您的網站及應用程式是託管在公有雲還是本地端，Imperva Cloud WAF 都能確保您的關鍵資產一直受到保護，免於各種應用程式層的駭客攻擊。Imperva Cloud WAF 是 Imperva 全方位應用程式安全與服務交付解決方案的關鍵要素，可將企業組織的縱深防禦提升到新的水平。

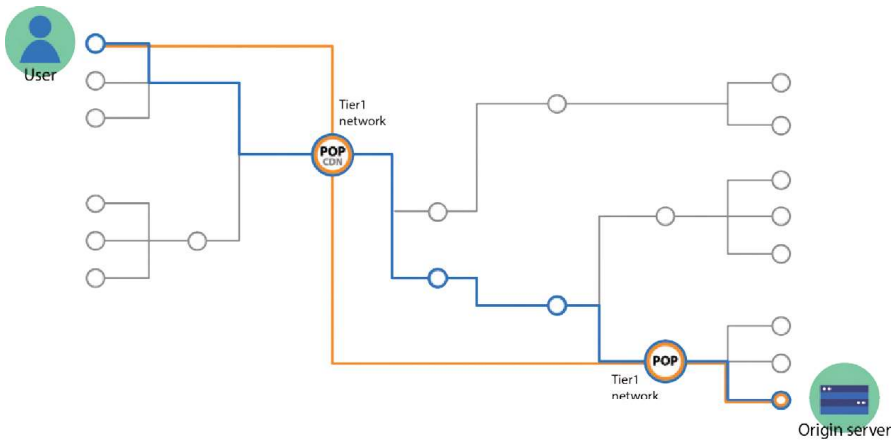
Imperva 數據整合平台的分析內容覆蓋範圍超越 OWASP Top 10 ，提供最好的網站防護，將網站風險從邊緣網路開始進行緩解，因此您的網站只會接收到安全的存取流量。

您可以透過 Imperva 保護最新的服務，無論是舊版應用程式、第三方應用程式、微服務 API、雲端應用程式、容器 (Container) 及虛擬機 ((Virtual Machine) 等，都能以接近零的誤報率和全球 SOC 阻擋這些攻擊，確保您的組織在受到攻擊後的幾分鐘內就能受到保護，並符合 PCI 6.6 的規範。

## 完整的邊緣網路安全 CDN 解決方案

安全 CDN 會自動快取一份網站內容在各地的節點上，當不同區域的用戶向網站發出請求時，使用者可以就近取得服務，提升服務遞送速度及品質，提高網站效能並降低頻寬用量，最大程度地減少將內容下載到存取者瀏覽器所需的時間，並預防頻寬濫用可能導致的停機風險。

**使用 Imperva 的網站平均速度能提高 50%，頻寬消耗減少 60%。**




Imperva CDN 提升網站和應用程式效能，進而為您的客戶提供更好的體驗，包括更快的載入時間、更好的內容交付和更低的頻寬成本。

- 進階快取，提升網站速度
- 降低延遲、自動故障移轉
- 自訂快取規則，降低延遲並改善效能
- 基於雲端技術的網路第 7 層服務和數據中心負載平衡
- 傳輸內容和連線優化技術
- 支援 IPV6 和 HTTP/2 效能強化
- 與 ISP、雲端託管供應商、一級網路供應商為合作夥伴關係
- 提供流量監控與即時分析

## 更好的網路流量控管，更好的客戶體驗

網站存取量在尖峰或特殊期間可能忽然大增，除了讓主機花費變高外，IT人員也很難評估網站所需的硬體需求。網站效能中斷不僅會影響客戶體驗，並可能導致客戶流失並損害企業品牌聲譽。

Imperva Waiting Room 功能可讓您為網站預設一個最大存取值，當訪客數超過該數量時，客戶將被導向虛擬等候室中的排隊系統，以先進先出的方式進行處理，直到客戶最終存取網站。這意味著網站可以保持在線狀態，不會讓客戶收到”無法存取”的訊息，相反地，客戶可以在 Waiting Room 的虛擬等候室內持續更新預計等候時間，藉此獲得更令人滿意且無縫的使用者體驗，降低離開網站的機率。

## 超越涵蓋 OWASP API 十大資安威脅範疇

Imperva API Security 雲端應用程式安全套件的預設的安全規則，涵蓋 OWASP API Top 10 攻擊手法，並使用自動化的積極安全模型，同時採用 API Discovery 持續學習機制，會在 API 更新時不斷學習它們的結構，透過檢測應用程式並阻止漏洞利用來保護您的 API 免遭利用。

在新的應用程式的開發架構裡、自動化 B2B 的運用流程、物聯網設備連接等系統架構都廣泛被使用，隨著API使用激增，對 API 的攻擊也呈現上升趨勢，需將您的防禦縱深提升到一個新的水準。

## 卓越的自動化爬蟲檢測技術

唯一擁有全球最大的已知違規者設備指紋實時更新資料庫，讓您由全球主動防禦態勢實時分析的機器學習基礎設施，主動防禦特定領域風險並快速進行更深度的生物特徵檢測分析，使您的用戶能進行有效的搜索並找到您提供的內容。

有效識別任何惡意行為並提供最深入的進階爬蟲機器人洞察力，包含通過 IP 、用戶代理、載入JavaScript，支援 cookie、移動鼠標和改變頁面時間 100 多個數據維度的分析，在機器人爬蟲的戰爭中最大程度地控制您的惡意流量，將駭客工具、帳戶接管、密碼撞庫、漏洞掃描等機器人惡意行為屏除在流量之外。

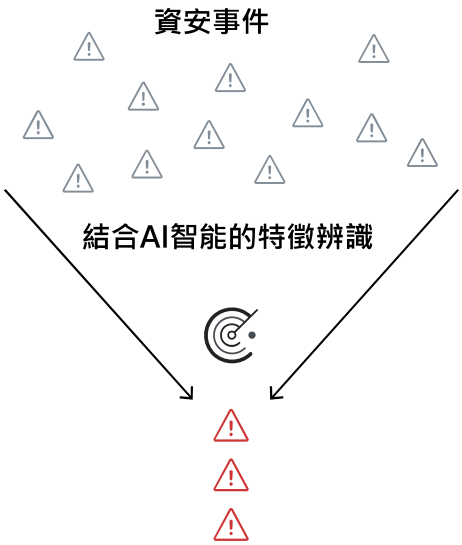
Imperva 優異的爬蟲檢測能力也榮獲 Forrester 自動化爬蟲解決方案評估報告中的領導者品牌 。

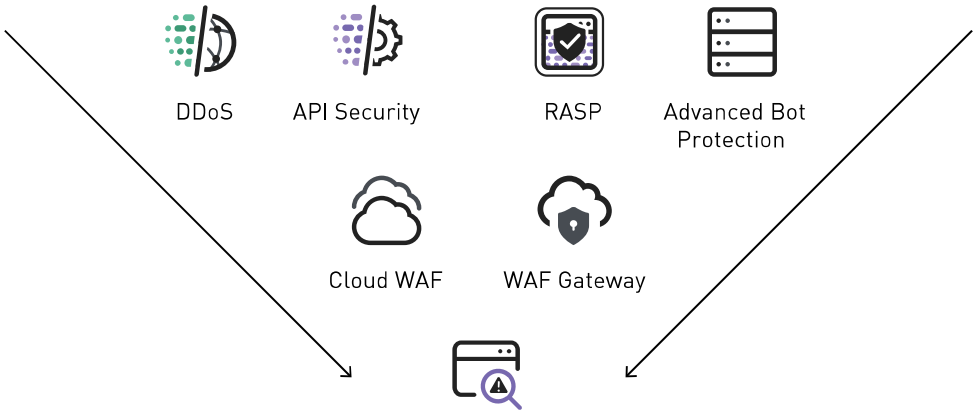
## 雲端AI告警分析系統 - 在眾多告警事件裡找出真正的危脅

Imperva 雲端AI告警分析系統 (Attack Analytics) 是 Imperva Application Security 解決方案之一，透過機器學習和領域專業知識來檢測應用程式攻擊，將大量資安事件分類和分組呈現去蕪存菁的結果，並為每個事件分配一個嚴重級別並提供額外的聲譽情報，提供資安事件所需的統一監控及統整分析。這讓資安團隊可以用簡單的方式，專注在少數幾個真正重要的事件分析上，而不必在成千上萬的事件告警裡大海撈針。

Imperva解決方案整合各大 SIEM 系統，並藉由 Attack Analytics 的AI人工智慧過濾告警資訊，降低隱藏在大量告警事件下的威脅風險，實現完整的可見性，減少資安事件分析所需的時間，進而顯著提升安全營運中心 (SOC) 的效率。

Attack Analytics 是基於雲的解決方案，可一鍵部署，因此具備無限的可擴充性和企業所需的大量事件處理能力。




Attack Analytics 分析、過濾 Imperva 多項解決方案中成千上萬的告警事件訊

## 高智能全自動撞庫防護

Account Takeover(ATO) 為暴力帳密填充技術，非法獲得的帳號密碼被用於未經授權存取的線上帳戶，攻擊者可以從中執行惡意操作，例如資料竊取、身份盜用或執行詐欺性電子商務交易。

Imperva 的核心 ATO 檢測機制使用其風險引擎中定義的因素（例如每台設備的登錄率、用戶名和登錄失敗的數量）來識別攻擊，根據攻擊的嚴重性和客戶定義的政策採取相對應的緩解措施。

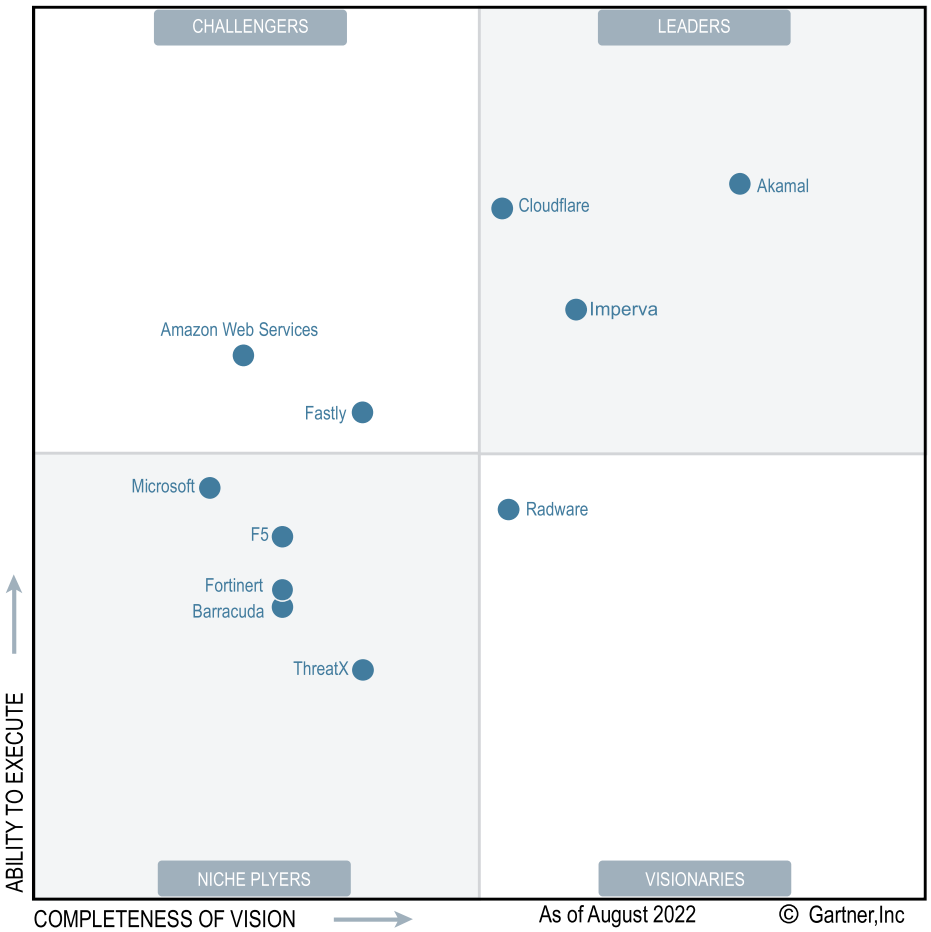
## 實時的洞察分析第三方 JavaScript 套件

JavaScript 服務在 Web 應用程式上呈現爆炸式成長，並廣泛被嵌入使用，當第三方套件在不知情的情形下被更新或劫持，將導致客戶在不知情的狀態下成為表單劫持攻擊的受害者，對於企業造成的嚴重的影響。

Imperva Client-Side Protection 讓您在不需要更改套件或增加延遲的情形下，即可查看、控制嵌入在 Web 應用程式中的所有第三方 JavaScript 套件，並持續監控所有 JavaScript 服務。Client-Side Protection 只允許執行預先批准的服務，這意味著在網站中任何 JavaScript 服務在套件被劫持或獲得授權前將數據發送到其他地方都會被阻擋。

## 多重榮譽的安全解決方案領導品牌

Gartner 將 WAAP（Web應用程式和API保護）定義為 WAF 的進化，並將原本 WAF 的功用擴展至 4 個面向：WAF、DDoS 防禦、機器人管理、API 保護。在 Gartner WAAP Report中，Imperva 是唯一連續9年位於領導象限的品牌，除了提供強大的混合雲資安防護功能：包括資料安全產品、RASP、實體或虛擬設備的 WAAP (Imperva WAF Gateway)，以及雲端 WAAP 服務 (Imperva Cloud WAF) 等，近期更收購 API 資安公司 CloudVector ，進一步拓展 API Security 領域的資安防護。




Imperva 是業界專家認可的網路安全領導品牌，致力於提供資料和應用程式所需的各種保護，無論是地端、雲端或是混合架構環境

imperva

# Imperva Data Security
# 資料庫安控稽核系統

- » 取得完整的資料庫活動細節(5W)留存存取資料庫的行為軌跡
- » 利用靈活的視圖和稽核分析使稽核資料容易取得
- » 產生對資料庫攻擊和欺騙性活動的即時警告，以善盡保護資料庫重要資料(如個資)的責任
- » 建立資料安全、遵守法規週期
- » 自動化與集中化的資料庫稽核與報告
- » 加密與加註簽章的稽核資料，具有資料不可被竄改與不可被否認性

## 特色

- 持續稽核與分析所有資料庫流量：詳細稽核與持續監控所有資料庫的操作，提供每筆事件的稽核紀錄，包含：「何人、何時、何處、如何連線資料庫及做什麼(5W)」。同時能擷取所有資料庫活動，包括 DML、DDL和DCL活動、查詢活動(SELECT)、對儲存程序、觸發程序和資料庫物件的修改及SQL錯誤的資料庫登入活動，並監控(可選擇稽核)資料庫回應以確保不會洩漏敏感資料。
- 驗證及控制特權資料庫活動：Imperva 利用閘道設備來監控網路流量，利用輕量化 Imperva Agent 來擷取本機活動並消除問題點。確保全面瞭解和保護所有網路與本機特權使用者的操作，包括資料定義語言(DDL)命令、資料控制語言(DCL)命令、資料操作語言(DML)命令和SEELECT。
- 防止竄改的稽核紀錄：監控詳細的稽核資料會儲存在安全的外部硬體處存設備中，可透過唯讀方式存取。該儲存設備中使用以角色為基礎的存取控制(RBAC)，為了確保稽核資料的完整性，還可以對其進行加密。
- 即時資料庫保護（※僅適用DBF/Bridge）：監視即時資料庫活動時會於作業系統、通訊協定及SQL活動層檢查各種資料庫攻擊，以提供準確的即時保護。未授權更改、欺騙性活動以及資料庫攻擊可以在到達受保護系統之前從網路上阻擋或在系統自身上阻擋。
- 靈活的部署與集中管理架構：提供包括通透網路監視、輕巧的Agent監視、自身稽核收集或混合模式。這種非入侵性的體系結構使企業能以任一方式混合部署，以滿足客戶特有的拓樸與需求。集中管理伺服器可對多 Gateway 及 Agents 進行統一管理。

## 法規遵循

- Imperva DAM 可滿足新版個資法施行細則第5條 - 要對個人資料之處理留有軌跡紀錄之規定，且提供稽核資料具有不可被竄改、不可否認性，可滿足個資法採舉證責任倒置原則。
- Imperva DAM 提供資料庫加密的補償性控制（PCI-DSS 3）。它還啟用關鍵性對存取持卡人資料的監控和跟蹤（PCI-DSS 10）。其它 PCI-DSS 要求符合以下措施：1.內建評估工具確保不使用廠商提供的帳號和密碼 2.對非法存取持卡人資料進行智慧型告警 3.使用內建和客制報表來衡量控制的有效性。 12項 PCI-DSS 要求中共有7項可由 Imperva DAM 來完成。
- Imperva 使企業能夠保持獨立的稽核線索，該稽核線索中包括與財務資料相關活動中的「何人、何時、在哪裡、如何及做什麼?」詳細資料，符合沙賓法案（SOK）要求實施適當的步驟和控制以確保可靠財務資訊的一致性(第302條)以及內部控制的可靠性(第404條)。

# 特色一覽表

## 探索和弱點管理

**• 資料庫探索和分類**

Imperva 可確保企業能夠保護所有敏感資料並區分其優先順序。基於整個網路的探索可了解資料庫伺服器間的資料。基於資料庫中包含的資料類型對資料庫進行分類可幫助企業對應所發現的伺服器並區分其優先順序，從根本瞭解哪些伺服器屬於法規監管的範圍。

### 廣泛的弱點評估

Imperva RDBMS 弱點評估和最佳作法有助於企業修正、控制其資料庫的設定配置並實現整體弱點管理策略。這些評估測試會與Imperva應用防護中心(ACD)研究小組的最新研究保持即時更新。

## 自動稽核和安全保護

Imperva 包含一套完整的預設稽核與安全政策，可以迅速監測任何資料庫的環境。這些規則基於＂黑名單＂和＂白名單＂安全模組，這些模組可透過Imperva 已申請專利的動態建模技術以及Imperva ADC 不斷更新的研究成果得以持續更新。動態建模技術(Dynamic-Profiling)可持續自動檢測並納入有效的更改，使管理員不必再手動新增和更新包含了成百上千個資料庫物件、使用者和SQL查詢的冗長白名單。

## 持續稽核與分析所有資料庫流量

詳細稽核並持續監控所有資料庫操作，提供每筆事件的詳細稽核紀錄，包含：「何人、何時、何處和如何連線資料庫及做什麼(5W)」。

Imperva 擷取所有資料庫活動，包括DML、DDL和DCL活動、查詢活動、對儲存程序、觸發程序和資料庫物件修改以及SQL錯誤和資料庫登錄活動。

Imperva 並監控(可選擇稽核)資料庫回應以確保不會洩漏敏感資料。

### 管理安全對策和更改

Imperva 即時監控資料庫活動並檢查各種作業系統、協定層級SQL層的資料庫攻擊。透過詳細的行為更改稽核可以準確地針對欺騙性活動、資料庫修改和攻擊進行告警、發送即時告警、分配後續任務以及確保變更的控制。

### 原始資料保存與回復

資料庫稽核軌跡原始資料(Raw Data)，可透過加密、數位簽章等方式，安全備份存放於本機硬碟，或搭配外部儲存空間，以NFS、FTP、Mount Point等方式，備份存放於指定外部儲存空間，避免歷史紀錄遭受竄改或刪除。

Imperva 操作介面提供匯入功能，可將歷史紀錄匯入回復，以供查詢、產製報表等作業。

### 加密解析

若資料庫本身啟用如SSL加密傳輸等機制，僅須利用安裝Agent或匯入憑證等方式解析出資料庫帳號，不影響稽核紀錄完整性。

## 簡化工作流程，並符合法規要求

**• 互動式稽核分析**

Imperva 提供圖表及統計數據列表兩種分析，透過互動式稽核分析可以全面瞭解所有稽核活動，這讓不瞭解技術的資料庫稽核人員只需點幾下滑鼠即可從多個角度深度分析、關聯和查看資料庫活動、從而簡易識別可能隱藏了安全風險或法規問題的趨勢和模式。

### 同級產品最佳報表功能

Imperva 提供內建的圖形報表，可以圖形、統計數據列表方式，呈現完整資料庫存取紀錄，並支援UTF8、BIG5等中文編碼，可正確呈現中文內容。排程自動產生報表，發送PDF或CSV格式的結果，以及與SIEM、問題處理系統和其他第三方解決方案的整合，提供相關稽核及告警訊息。

## 靈活的部署、較低的建置成本

靈活的部署模式：網路、Agent、內建稽核或混合模式

Imperva 提供最簡單的部署選項，包括透通的網路監視、輕巧的Agent監視、自身稽核收集或混合模式。這種非侵入性的體系結構使企業能夠以任意方式混合部署，以滿足客戶特有的拓樸和需求。

Agent可在下列情況下獨立運作：

(1)不使用資料庫帳號安裝

(2)不啟動資料庫內建之稽核日誌功能

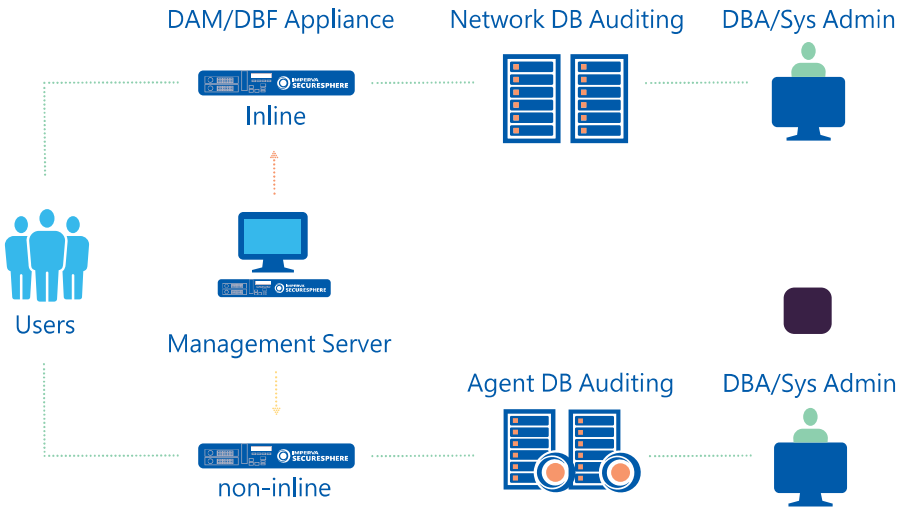
(3)不更動資料庫設定

(4)Agent故障不影響資料庫運作

(5)可調整占用之系統資源

### 效能和可擴展性

Imperva 提供即時的保護和完備的稽核功能，可以很容易地支援任何環境，從中小企業到大型企業，這是其它資料庫防火牆解決方案無法與之相比的。




Imperva 可部署在inline或non-inline網路監控環境，控管特權及使用者帳戶的資料庫行為