Websense® Data Security Gateway

資料外洩的法規和閘道
資料竊取防護

今日的業務環境暴露在許多進階威脅和資料竊取行為中，還必須遵循各種法令規範的管制。您的難題是必須防範上述威脅，避免敏感資料離開組織並遵循相關法規。**Websense® Data Security Gateway** 可對電子郵件和網頁管道提供超越傳統網路防護的即時資料竊取分析，還有超過 **1,700** 個政策和範本以供遵循法規之用。

為什麼 **Websense** 是最佳選擇？

Data Security Gateway 是全方位的網路資料外洩防護 (DLP) 解決方案，可避免敏感資料無意或蓄意傳送到網路之外。其由 Websense DICE (資料識別和分類引擎) 所支援，將多個資料分類器與使用者和目的地感知能力結合，以獲得準確性和完整性。Data Security Gateway 會監控一般的網路通訊管道，如網頁、電子郵件、FTP 和行動電子郵件的 ActiveSync 等。當發現敏感資料時，Data Security Gateway 會阻擋傳輸動作並記錄該事件，或是自動採取如進行加密、隔離電子郵件或執行自訂指令檔等修補動作。

領先產業的 **DLP** 防禦能力

- Data Security Gateway 業界第一個 (也是唯一) 使用光學字元識別 (OCR) 功能識別圖片中文字的產品。
- 為了對付隱匿且滴漏式的資料外洩攻擊，Drip DLP 會對事件進行長時間的觀察，以偵測出滴漏式的緩慢資料外洩情形。
- 利用地理位置感知能力，透過擷取鑑識資料和利用網頁分類功能判斷資料傳送地，以便瞭解敏感資料的去向及原因。
- Data Security 是健全的資料對外傳送防禦策略的一部份，能偵測經過犯罪意圖加密的上傳檔案和竊取密碼檔案的行為。

精細化的政策和社交媒體管制

- Data Security Gateway 可對社交媒體應用程式提供無與倫比的可見度，包含即時目的地感知能力，可掌握資料的傳送目的地和傳送者是誰。
- Data Security Gateway 提供自動化的政策執行選項：包括即時阻擋、隔離、加密、稽核/記錄與通知使用者。
- 您可以容易地在統一式 TRITON 架構下，由 Data Security Gateway 擴充到 Websense Data Endpoint 和完整的 Websense Data Security Suite。DICE 被用於所有解決方案中，並可由單一主控台進行管理。

保護對象

WEB☑ 電子郵件☑ 資料☑

平台

軟體☑ 設備☑ 雲端☐ 混合☐

進階 **DLP** 防禦功能

- Drip DLP 功能可觀察累積的事件
- 對圖片中的文字進行 OCR
- 地理位置目的地感知能力
- 偵測自定加密和密碼檔案資料竊取的資料竊取防護政策
- 自動化事件更新作業

降低複雜性

- 可容易地與現有的網路基礎結構整合
- 單一主控台管理資料、Web、電子郵件和行動安全性

輕鬆進行部署和管理

- 一組全方位的資料識別技術，保護包括政策範本、指紋檔案和機器學習的資料，再加上資料竊取防護
- 超過 1,700 個政策和範本以為遵循法規用途，並由 Websense 研究人員維護與更新
- 對獨特、特別業務的敏感資料進行文件指紋處理
- 進階機器學習功能可以填補指紋檔案和政策範本之間的不足，以提升準確性和效率
- 容易客製化、產生和派送報表

「由於只有被許可的重要資料可以離開組織，我們相信採用 **Websense** 可以為我們的業務做出龐大的貢獻。」

Murli Nambiar
Reliance Capital 資訊安全副總裁

websense®

Websense® Data Security Gateway

Websense 的優勢：DICE (資料識別和分類引擎)

Websense DICE 結合多種分類器和即時的使用者、資料和目標相關內容感知能力，可對整個 TRITON 架構提供非常準確且一致的資料外洩防護能力。DICE 支援三種資料分類：描述式、註冊式和學習式。描述式資料包括正規表示式、字典和自然語言分類器，有包含超過 1700 個政策和範本可供使用；註冊式資料包含文件及資料庫指紋資訊，同時也可以經過壓縮並保存在端點，以供端點電腦於網路離線防護之用；學習式資料是進階的機器學習技術，利用演算法分析小量的資料，以填補描述式和註冊式資料間的缺口，提供更高的準確性和效率。資料竊取防護功能包含對圖片文字進行 OCR、偵測客製化加密檔案和密碼檔案竊取、偵測滴漏式資料外洩和地理位置感知能力。DICE 可用於搜尋作業、閘道和端點，並從單一主控台進行管理。

Websense Data Security Gateway 使用 **DICE**，以相關內容感知的方式分類資料

您的需求	Websense 解決方案
保護資料免於複雜、緩慢的資料外洩攻擊	Websense 提供另一個業界首創 Drip DLP，可以監控累積事件中的資料外洩行為，避免重要資料外洩。
保護儲存在圖片中的資料	只有 Websense 提供對圖片內文字進行 OCR 的功能，以進行搜尋、監控和防禦。
深入瞭解離開貴組織網路的資料	來源和目的地感知能力，再與 Websense 分類器結合，能讓您瞭解誰正在存取哪些資料、如何使用資料以及資料會傳送到什麼地方，藉此您的組織可以即時制定更周延的政策，並可於未來進行調整。
進階資料竊取防護政策	Websense 有能力偵測自定的加密檔案，以及密碼檔案資料竊取行為，這是電腦犯罪份子佔領第一個攻擊跳板時常用的手法。
輕鬆進行部署和管理	Websense 提供一個集中主控台，可以輕鬆管理閘道、端點和搜尋的 DLP 政策、事件和報告產生作業。
易於管理	可利用自動事件更新的自我發佈機制，容易地更新事件。
集中式事件管理和報表	派送摘要或詳細的報表，顯示裝置/應用程式管道、使用者群組、政策、規章、採取的實施動作等資訊。可顯示合規性的狀態。

websense®

行動、社交和雲端技術都能帶來生產力，但是這些管道也為資料竊取和更先進的攻擊敞開了大門。防毒、URL 篩選和防火牆防線對這些威脅都無能為力。Websense® TRITON™ 解決方案結合了共用架構的 Web、電子郵件、資料和行動安全解決方案 (可同時或個別購買)，能讓您領先威脅一步。Websense ACE (進階分類引擎) 的即時防禦，再加上彈性的部署選項和一個統一式的管理主控台，使 TRITON 成為今日動態環境中不可或缺的解決方案。

欲瞭解更多資訊，請造訪 **www.websense.com**

Websense代理商 docutek 達友科技 **服務專線**：02-2658-8970 | **http://www.docutek.com.tw**

websense® TRITON™