Websense® Data Security Suite

閘道、端點和資料搜尋的統一式資料外洩防護

從商譽受損到被科以罰款，外洩資料所造成的嚴重影響顯而易見。只要發生一件資料外洩事件，就足以讓企業的競爭優勢消失殆盡，失去客戶的信心，並會受到執法單位處以罰款或刑責。但是因為行動裝置快速成長、周邊裝置廣泛使用、可輕易取得的檔案分享應用程式不斷出現，使資料外洩和被竊的機會大幅增加，導致這個問題更加惡化。

為什麼 **Websense** 是最佳選擇？

Websense® Data Security Suite 可防範各種資料外洩的情形。其為網路與端點資料外洩防護 (DLP) 與機密資料搜尋提供了同一個政策架構。

- 輕鬆採用一個可擴充的解決方案來防止入埠 (inbound) 的威脅，並且管理與資料外洩和法令規範相關的離埠風險。
- 超過 1700 個預設政策和範本，並依國家地區和產業進行分類，可減化政策制定的工作。
- Websense 資料識別和分類引擎 (DICE) 同時也內建在 Web 和電子郵件閘道解決方案中，是集中式 Websense TRITON™ 架構的基礎。

Data Security Suite 由以下模組組成，可彈性依部署架構個別購買：

- **Websense Data Security Gateway**：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，或是自動採取修補動作。
- **Websense Data Endpoint**：會監控即時流量，並擴大對機密資料的管控能力，包含允許傳輸的機密資料在什麼地方、誰使用這些資料、如何使用、傳輸的目的地為何，以及要採取什麼即時動作來防止資料在端點外洩。
- **Websense Data Discover**：能利用 DICE 的三種資料識別分類器 (描述式、註冊式、學習式) 識別機密資料，提供最深入的資料資訊。

保護對象
WEB☑ 電子郵件☑ 資料☑

平台
軟體☑ 設備☑ 雲端☐ 混合☐

進階防禦

- 全文識別的 DICE 政策引擎內建於整個 TRITON 架構
- 可對圖片內文字進行影像文字辨識 (OCR)，以執行資料搜尋、監控和防護
- 依時間自動加總事件以偵測滴漏式資料外洩的情形
- 偵測客製化加密和竊取密碼檔案的行為
- 資料傳送目的地具地理位置和網頁分類感知能力
- 進階機器學習功能可填補描述式與註冊式資料比對的缺口
- 離線的端點電腦也能提供指紋比對 (finger-printed) 的偵測防護技術

降低成本與複雜度

- 可容易地與現有的網路基礎結構整合
- 單一主控台集中管理資料、Web、電子郵件和 DLP 安全政策
- 超過 1700 個預設政策和範本，並依國家地區和產業進行分類
- 利用先進的資料分類器和自然語言處理保護智慧財產權
- 利用電子郵件進行事件流程管理

「**Websense Data Security Suite** 讓我們可以深入掌握組織中資訊的使用情形，藉此我們可以對敏感和受管制的資料採用正確的防護政策。」

Matt Tucker
OmniAmerican 銀行 IT 副總裁

競爭廠商警示
資料：PCI & PII
來源：10.14.222.21
管道：Web
目的地：10.14.222.21

- 內容資訊有限
- **IT** 系統管理員工作增加

VS

Websense 警示
資料：PCI & PII, customer database
來源：Joe User x1234
juser@company.com
職稱：助理
管理者：Jane Manager x2345
jmanager@company.com
管道：Web
目的地：mail.google.com
類型：個人 webmail 站台
地點：Mountain View, CA

- 使用者與目的端感知
- 加速修補時間

Websense® Data Security Suite

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 Suite 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
一致的政策制定作業	超過 1700 個預定義政策和範本，經由產業和區域分類，讓您可以對端點、網路和資料存儲快速制定和套用新政策。範本會由專屬 Websense 研究人員定期更新和檢視。
保護存在圖片中的資料	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。
經過簡化和統一式的架構，簡單易用並可降低 TCO	Data Security Suite 已經完全和 TRITON 架構整合。DICE 可用於所有 DLP 功能，並在所有 TRITON 解決方案中都是一致的。Data Endpoint、Data Security Gateway 和 Data Discover 共用同一個管理介面。
簡化的工作流程	Websense 能讓主管回覆電子郵件通知以管理事件，簡化工作流程。
統一式事件管理和報告	分發摘要或詳細的報告，顯示裝置/應用程式管道、使用者群組、政策、法規、採取動作等資訊。可顯示合規性的狀態。
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。
保護資料免於精心計畫、持續的微量資料外洩攻擊	Websense 提供另一個業界首創滴漏式資料外洩防護 (Drip DLP)，可以依定義的時間區間監控及累積事件中的資料外洩行為，並主動告警與阻擋，避免重要資料外洩。
輕鬆進行部署和管理	Websense 提供一個統一主控台，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。

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™

© 2013 Websense Inc. 保留一切權利。Websense 與 ThreatSeeker 是 Websense, Inc. 在美國與某些國際市場中的註冊商標。TRITON、X-Series、X10G 和 Websense Security Labs 是 Websense, Inc. 在美國和其他國家的商標。Websense 在美國與國際上有許多其他註冊和未註冊的商標。所有其他商標是各自擁有者的資產。規格得遵自變更而不另行通知。01-10-2013 EN