



SPAM SQR

全方位郵件過濾平台

Anti-Spam 產品 第一品牌

領先 No.1 郵件過濾產品第一品牌
口碑 No.1 擁有全國最多使用客戶數
創新 No.1 榮獲資訊研發多項大獎

SPAM SQR

全方位郵件過濾平台

新一代郵件過濾平台，獨家分離垃圾與威脅郵件，提供差異行為管理功能，既可彈性開放使用者自主管理放行郵件，亦可控管惡意郵件任意流竄。

垃圾郵件與威脅郵件雙核過濾技術，擁有完善的特徵庫、指紋庫和惡意網址資料庫雲端差分更新技術，搭載流量控制防禦引擎、社交工程偵測引擎、附件檔案分析引擎，有效縮短零時差攻擊的風險，提昇系統整體攔截效能。架構於企業郵件伺服器前，有效降低各式郵件攻擊的風險，如垃圾/廣告郵件、釣魚郵件(社交工程)、偽造攻擊郵件、病毒郵件、夾帶惡意檔案郵件等。

另外可掛載防毒模組和ADM (Advanced Defense Module) 進階防禦模組。程式會自動解封裝檔案進行掃描，可發掘潛在代碼、隱藏的邏輯路徑及反組譯程式碼，以利進行深層惡意程式比對。可進階防禦魚叉式攻擊、匯款詐騙、APT 攻擊郵件、勒索病毒以及新形態攻擊等郵件。

電子郵件指紋碼擷取及垃圾郵件辨識方法、電子郵件分析及管理技術已申請專利獲准，專利字號為【發明 第I 429238號、439096號、472192號、441496號、435572號、443526號】

多層次過濾圖



產品特色



N-Tier多重防禦，層層篩選過濾更透澈

- 連線層阻擋：阻擋瞬間大量郵件攻擊，節省頻寬、降低郵件伺服器負載。
- 惡意郵件隔離：將隱藏惡意行為及特徵郵件進行隔離，能效降低使用者接觸到惡意郵件的風險。
- 垃圾郵件攔截：如垃圾/廣告信件等不具威脅性之郵件，可選擇發送明細給使用者自行定義接收與否。
- 詐騙郵件示警：檢查郵件偽造痕跡並分析來源，當此類郵件放行至使用者端時加強警示，藉以提高使用者警覺。



內控管理，掌握內部風險

- 外寄郵件過濾，防止內部濫發惡意郵件，導致列入RBL。
- 外寄帳號速率控制，防止內部中毒亂發垃圾郵件，造成公司信譽受損。
- 密碼防猜機制，降低密碼被竊取風險。(建議搭配密碼強度檢測模組，以提昇密碼強度。)



個人化管理，接收查信更便利

- 可依個人需求定時發送攔截明細，方便使用者接收或回報案件。
- 提供使用者 MySPAM 個人化管理介面，自我管理郵件，如系統自動回覆、自動密件副本給自己與個人黑白名單等功能。可透過攔截明細郵件、QRCode 或 APP 連結。

標準功能

郵件過濾/防禦功能

DoS防禦 針對瞬間大量郵件攻擊或連線數進行管控及阻絕，可避免郵件主機因遭受攻擊而癱瘓服務

流量控制 檢查企業內部合法收信帳號，以灰名單機制來控制流量，能防禦字典檔的試發帳號攻擊

RBL 支援外部資料庫名單和自訂名單，並提供自動判斷機器人發信機制

DKIM 阻擋或攔截濫發垃圾郵件的人假造郵件中的地址

SPF 檢查郵件是否由經過授權的郵件伺服器發出，阻擋偽裝網域對內發送的假冒郵件

DMARC 運用SPF和DKIM機制驗證郵件寄件者是否來自合法網域，有效識別偽造郵件，避免遭受詐騙攻擊

黑白名單 提供系統/群組/個人黑白名單設定，系統白名單還附加防偽檢查功能，提供安全的防禦機制

ASRC 指紋辨識 完整拆分垃圾和威脅指紋庫，其自動收集機制，佈點更全面。啟用雲端指紋差分更新機制，更新更快速

ASRC 特徵分析 結合產官學研究分析，針對郵件行為、標頭、以及來源及內容等複合型條件，發展持久長效之特徵

ASRC 附件辨識 針對附件檔案進行指紋萃取分析，綜合檔案分析引擎進行分類，提升垃圾郵件和威脅郵件的辨識能力

內容關鍵字過濾 提供多國語系關鍵字過濾資料庫，並可彈性調整過濾類別開關以及自建過濾類別

自動學習過濾 自動學習過濾引擎可在學習垃圾郵件及正常郵件後，自動分離垃圾郵件及正常郵件

管理性功能

政策管理 提供瀏覽及調整各群組的過濾類別設定，並可設定類別明細派送之原則

過濾條件 管理者可根據企業內部電子郵件管理原則，設定放行、攔截、審核或延遲寄送等條件

群組設定 提供企業內群組人員的帳號設定，並能依群組內成員的管理需要，進行個人化服務開關設定

統計報表 提供多元且易讀的統計資訊—包括各項流量、攔截、排名、郵件、寄件來源、IP來源、連線阻擋、病毒等各種統計輔助圖表，並可提供報表匯出及列印

標準LDAP帳號整合 可整合標準LDAP通訊協定，自動同步電子郵件帳號，並支援SMTP認證

分權管理功能 依照公司部門分權分責政策，可定義管理者登入管理者介面權限，包含郵件記錄、群組設定及統計報表等

郵件攔截/標記服務 提供分級標記傳送模式、垃圾郵件攔截模式等多元化服務

個人化管理

攔截明細 彈性寄發攔截郵件明細，可直接透過明細閱覽或放行郵件

MySPAM 透過個人化MySPAM介面，除可查看攔截郵件記錄，亦可針對個人郵件進行查詢、轉寄或回覆。另外個人化管理功能有自動休假回覆及自動密件副本

手持裝置APP 提供iOS/Android手持裝置APP，可記憶登入帳號資訊，並可符合手持裝置瀏覽，提供快速查信閱信功能。可做為企業商務人士的信件處理平台

選購模組

郵件管理

遠端調閱模組 提供介面作即時調閱查詢已備份的遠端郵件

附件稽核模組 針對附件內容關鍵字進行審核控管，並可定時發送明細方便主管閱覽。含個資特徵套版，提供8種預設特徵套版，並提供自訂特徵套版功能，可將符合個資法保護的資料，分別計算次數，重新組合使用。設定後的套版，可應用在過濾條件及郵件查詢

威脅防禦

防毒模組 提供郵件雙向（inbound/outbound）病毒掃描過濾，包含防毒資訊及設定、病毒隔離、病毒統計報告..等功能，可以防堵病毒、蠕蟲..等惡意程式擴散，更可提升至多層防毒引擎架構

進階防禦模組
Advanced
Defense Module

可進階防禦魚叉式攻擊、詐騙及APT攻擊郵件。其運用雲端沙盒技術，模擬產出靜態特徵，攔截附件及檔案夾帶零時差（Zero-day）惡意程式、APT攻擊工具、含有文件漏洞的攻擊附件及利用 Drive by download 等攻擊手法的威脅郵件。並提供攔截統計，揭露漏洞編碼和攻擊工具及攻擊族群等細部資訊，供管理者作為內部資安強化的資訊

HA備援

Multi-way 模組 包含分流備援、異地備援、分散式系統分工及運作服務

弱點偵測

密碼強度檢測模組 符合ISO27001定時檢測密碼強度之規定，同時具有自動通知和統計報表功能。提供企業防堵資安漏洞，有效降低駭客入侵企業的危機

防偽認證模組 防止認證通過帳號，利用他人名義發信。以降低偽造企業人員發送黑函的風險

產品規格

50U 型
100U 型
200U 型

- 處理流量：2G 以內
- 1U 可上 19 吋標準機架
- 尺寸 (D x W x H)：43.5x43x4.6cm

300U 型
500U 型

- 處理流量：2~5G
- 1U 可上 19 吋標準機架
- 尺寸 (D x W x H)：62x48.4x4.3cm

1000U 型

- 處理流量：5~10G
- 1U 可上 19 吋標準機架
- 尺寸 (D x W x H)：75.3x48.5x4.5cm

2000U 型

- 處理流量：10G
- 2U 可上 19 吋標準機架
- 尺寸 (D x W x H)：70.5x48.5x8.8cm

提供上述搭配硬體的 Appliance 授權版，含一年系統維護、版本更新、硬體保固