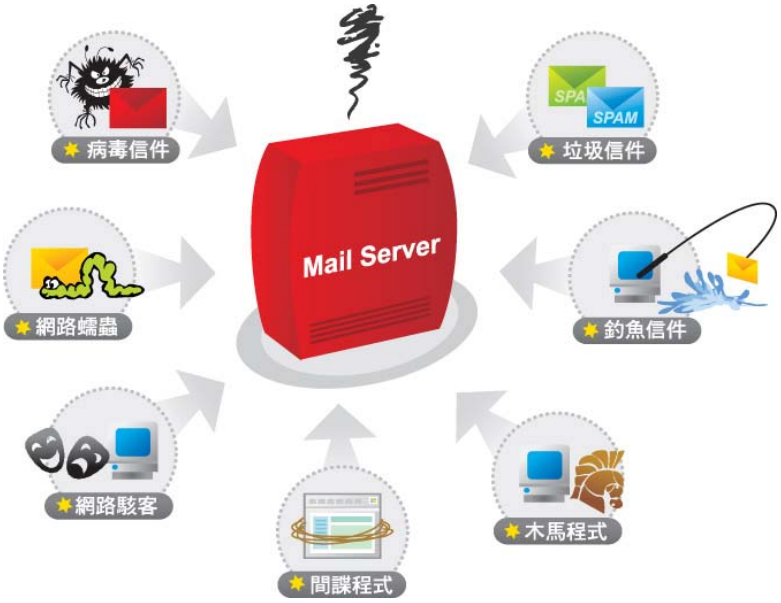
新一代郵件安全防護趨勢

正視垃圾郵件新威脅-混合式攻擊不容忽視

根據 2006 年 IDC「企業安全調查」指出，包含病毒、垃圾郵件等安全內容管理(SCM)，仍是企業認為最嚴重的資安威脅。這聽起來像是平常的消息報導卻正是全球所有企業主在 2007 年所必須正視的挑戰，且比以往更加險峻。這不僅侷限於垃圾郵件，包含釣魚郵件、木馬、蠕蟲、間諜程式、網路型病毒、網路駭客的威脅等也都變本加厲不斷變形為更難辨識的樣貌，其中以結合病毒的垃圾郵件變形影響最為全面。垃圾郵件發送者不再只是單純的發送文字或圖片化的垃圾郵件，反之發送帶有間諜僵屍程式的垃圾郵件，利用被病毒控制的僵屍電腦網路來當作攻擊或發送垃圾郵件的中繼站，這意味有許多垃圾郵件是由許多不知情的用戶電腦所發送的，目前全球正以每日 25 萬台的速度再增加。



雖然比爾蓋茲在 2004 年一場訪問中大膽預言了「兩年後垃圾郵件問題將得到徹底解決。」但兩年後的今天，從 Ferris Research 最新的報告顯示 2007 年垃圾郵件總量將持續高昇，而因為圖片型垃圾郵件的崛起，所有的企業主必須準備較去年更多的資源以因應這樣的挑戰。這樣的成長歸因於垃圾郵件發送者不斷的找尋新的方法與日益精進的技術，驅使垃圾郵件總量反增不減，造就垃圾郵件在 2007 年達到成長的高峰。

郵件發送者之風雲再起-圖片型垃圾郵件

2006年12月由一群抵抗垃圾郵件氾濫所組成的Open Relay DataBase (ORDB) 非政府組織宣布將關閉該收集全球黑名單的網站，意味著過去透過開放轉寄黑名單的垃圾郵件攔截技術已經不再有效防阻新興而起的垃圾郵件發送技術，垃圾郵件的偵測攔截技術正式進入下一個世代。

面對圖片型垃圾郵件的猖獗與氾濫，現有常見的攔截技術大多與光學字元辨識(OCR)方式做搭配，由 OCR 先做第一階段圖片的解析，之後再將辨識出來的內容透過既有的文字過濾方式作篩選與判斷。這樣的方式雖然可以解決掉圖像無法辨識的問題，但當垃圾郵件量大幅增長時，這樣的兩階段判斷方式可能容易拖慢整個過濾比對流程。根據 Openfind 統計顯示，圖片型垃圾郵件佔所有垃圾郵件量的30%，若一家100人的企業來推測，每日信件流量若有15萬封，圖片型垃圾郵件就佔了45,000封，硬體空間每日就佔用了1.4 GB (目前圖片型垃圾郵件平均一封信件大小為25~30KB)，這還只是單純計算圖片型垃圾郵件的量而已，尚未計算其他攻擊行為所造成的系統損失。此時，若在收件時還要將圖片型垃圾郵件一封一封的通過OCR掃瞄後，再開始進行垃圾郵件的篩選，就大幅考驗著企業系統效能與頻寬的運用了。

除了搭配OCR光學辨識的攔截方式外，另一種常見的攔截方式即為針對圖片型垃圾郵件的特徵去作分析。廠商透過收集大量圖片型垃圾郵件，將特定常見的特徵予以解析與辨識。常見的垃圾郵件圖檔格式如JPG, GIF, PNG等都早已經納入各家防護廠商的解決方案，但比較不同的是「圖片特徵解析技術」可以解決垃圾郵件發送者為破除OCR光學字元辨識技術所發明的變種圖片型垃圾郵件，此種郵件乍看下為一般圖片，但經分析解讀後，可以發現圖片內容含有許多不規則大小的黑點以及切割的圖樣，讓OCR無從辨識起。而透過「圖片特徵解析技術」，反而可將這些多重特徵作為辨識的參考方向，結合其原本的多層式過濾技術，方可有效阻擋圖片型垃圾郵件的攻擊。

全方位郵件防護-導入郵件監察為首要任務

雖然目前有關圖片式垃圾郵件的話題不斷，但必須注意的是這股熱潮僅是眾多混合式攻擊的其中一種。面對郵件安全層出不窮的資訊威脅和翻成出新的發送技術，企業主必須更全面的思考導入方案的防護效能。根據Forrester Research調查報告指出，35%的企業懷疑員工會透過電子郵件洩漏機密資料，其中外寄郵件中有高達 25%的信件帶有財務或法律性的管理風險。由此可見，郵件安全僅單單被動防護外對內(Incoming) 資訊傳遞所造成的可能威脅是不夠的，更應主動控管來自於內對外 (Outgoing) 訊息往來的潛藏危機。同時，企業在考量郵件防護

安全架構時，也需評估郵件監察(Email Supervision)的應用概念，同時結合郵件主動防護(Email Active Protection)、郵件政策執行(Mail Policy Enforcement)與郵件稽核(Mail Audit)，才能有效達到全方位郵件防護的目的。

- **郵件主動防護加強過濾效果**

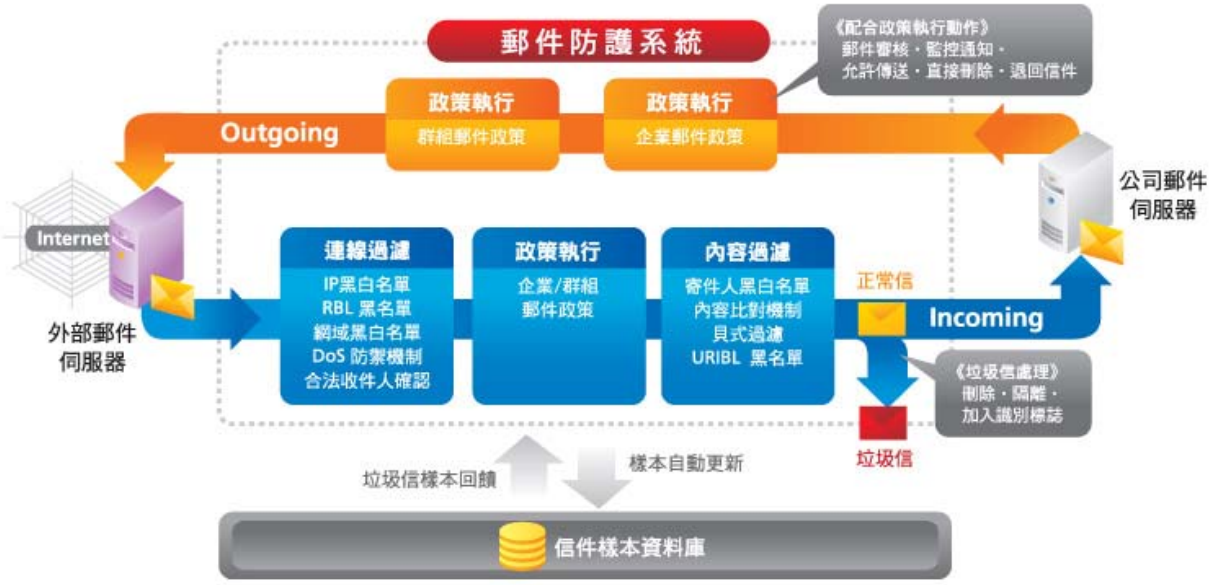
  為降低企業整體管理成本(TCO)，郵件防護的架構需能同時協助企業做好從 IP 連線到內容階段的郵件過濾動作，並且結合主動郵件行為分析與威脅樣本線上自動更新，以防制各式新資安威脅。對於電子郵件系統經常遇到的惡意 SMTP 連線，例如 DoS 攻擊或是垃圾郵件業者的字典攻擊，郵件防護系統更需能提供動態的即時防護，當在 SMTP 端發現有不當信件時，能立即阻絕異常連線，無須等到郵件完全進入系統後，才進行內容分析與判斷。在現今越來越多圖片型垃圾郵件的攻擊下，更可協助企業大幅節省硬體與頻寬成本。

- **郵件政策執行防止洩密與預先防範**

  郵件政策執行是郵件過濾的其中一環，主要在於預防企業內部不當、威脅或機密信件的進出，事前預防以降低可能帶來的損害，並滿足各部門規劃各自郵件管理政策的需求，提供符合企業組織行為的階層式管理(Hierarchical Management)架構。企業可針對組織內部運作流程，制定郵件政策，針對寄件者、收件者(含副本、密件副本)、信件主旨與內文、信件大小、附檔名稱和內文等設定多重過濾條件，將符合條件的對內、外郵件，留置在隔離區或是進入內部審查流程，以確保機密資料不外洩、威脅不進來。

- **郵件稽核事後追蹤與情報掌握**

  郵件稽核重點在於讓稽核人員與管理者掌握系統情報，進而清楚瞭解郵件防護與政策遵循狀況。因此系統需能提供各式系統紀錄與詳盡的圖像化統計報表以供監察，而不只是郵件紀錄(Mail Log)。郵件稽核也需能配合群組管理功能，進行郵件紀錄的調閱與郵件過濾政策的調整，並可結合郵件系統後端的郵件歸檔系統成為一個完整的郵件治理監察架構，協助企業有效管理政策，提昇營運競爭力。



打造完善防護系統-獨立架構強化防護效能

建構一套完善的郵件防護系統，除了應導入「郵件監察」(Email Supervision) 概念以進一步評估系統的運作效能外，更建議此一防護系統的建置，必須透過單一專屬的郵件防護閘道，僅放行安全可靠的訊息進出企業的郵件系統，才能徹底阻絕安全威脅。環顧坊間大多數的訊息安全管理解決方案，多半採取二合一或是三合一的架構設計，將「郵件＋過濾」或是「過濾＋備份」規劃在同一部主機。然而，這樣的部署方式僅適合信件量不大或是對於郵件系統風險容忍度較高的企業；對於十分重視郵件系統安全的企業而言，建議應將防護及備份系統各自獨立運作，以保障最佳的系統效能與穩定性，更可避免郵件備份資料庫曝露在高風險的對外網路環境，確保郵件系統的安全性。

整合式郵件防護系統 VS. 獨立式郵件防護系統

	整合式郵件防護系統	獨立式郵件防護系統比較表
系統架構	將所有系統安裝在同一台機器	個別系統獨立安裝於不同的機器
優點	導入快速	獨立運作，將各別系統發揮最大效能
	單一操作介面管理方便	系統各自獨立互不影響、風險大幅降低
缺點	系統效能堪慮	硬體成本較高
	系統風險較高，任一系統出問題都有可能導致郵件收發停擺	需維護不同的系統
適用客戶	中小型企業 簡單易用的整合性產品，鎖定信件量不大、對於資安要求較不嚴格的中小型企業	中大型企業 適合郵件量較大、需要彈性擴充整合內部軟硬體資源、並且重視資安的中大型企業