新一代訊息安全管理解決方案

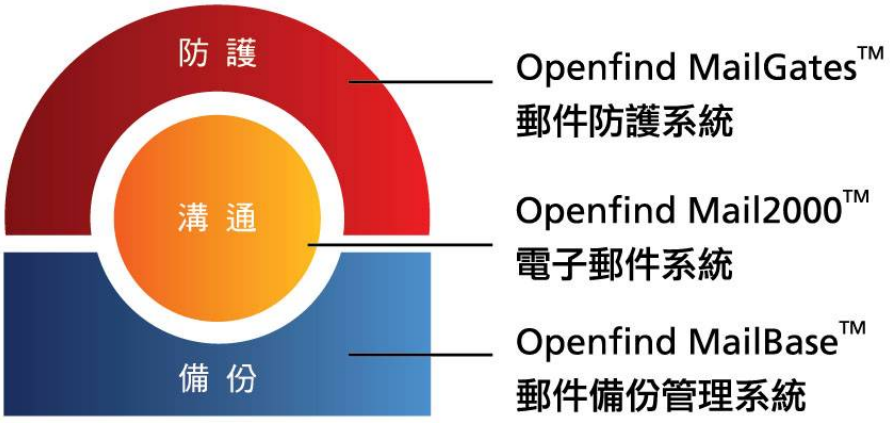
郵件訊息管理三部曲：「防護、溝通、備份」

根據 IDC 報告指出，未來電子郵件的安全管理將會成爲企業最頭痛的問題。企業首先要做的就是釐清應用需求並制訂郵件政策，再進一步落實政策執行(Policy Enforcement)，每一步都需要謹慎的審核與評估，以杜絕不當的使用行爲與衍生的風險。建構健全的郵件系統可以保障訊息安全、提高企業生產力與溝通時效，讓郵件不僅傳遞訊息，更可以將累積的郵件資訊轉化成爲企業知識資產，落實知識管理。

全方位訊息安全解決方案

以傳統資訊安全的觀點來說，只要安裝防毒軟體、防火牆、入侵偵測系統即已足夠。但隨著企業資訊環境的快速變遷，幾年來資訊安全事件卻層出不窮，並多集中在企業內部的郵件訊息安全，這也讓資安關注的焦點由過去只是被動防禦外部的惡意連線攻擊，轉向主動重視內部應用程式與資料安全的控管。根據 Forrester Research 2005 年調查報告指出，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，企業除了被動防護外對內(Incoming) 資訊傳遞造成的威脅以外，更應主動控管來自於內對外 (Outgoing) 訊息往來的潛藏危機。

因此該如何有效管理郵件訊息安全? 制定完善的公司郵件政策，加上資訊安全方案的配合，方能達成全面、完整的資訊安全系統環境。以目前企業訊息環境所面臨的複雜度來說，除了一般軟硬體設備、網路環境等因素外，應該由**「安全防護、溝通應用、資料保存」**三個角度來檢視企業郵件訊息環境，確保溝通競爭力並妥善管理使用行爲。透過在郵件收發流程中三個系統的獨立運作，才能將各自效能發揮到最大，以確保郵件訊息系統安全性，不因和其他過濾或備份系統的共存，導致爭搶系統資源進而影響系統穩定性的問題產生。



安全防護- 郵件防護閘道打造資訊安全

企業每天透過大量郵件往來對內外溝通，雖然加速了資訊的流通，但也帶來各種資訊安全上的威脅。此時，位於戰略地位的第一線郵件防護系統也就格外的重要。郵件防護系統需承受的不只是外部垃圾郵件、病毒信件、惡意連線、弱點掃描以及阻斷攻擊，還需監控內部員工的郵件使用行爲，稽核是否有對公司不利的信件。此一防護系統的建置，必須透過單一專屬的郵件防護閘道 (Email Protection Gateway)，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。因此在實務上，建議採取實體主機分離的佈署架構，搭配防火牆設定以提升郵件使用安全，讓內部系統可在不受干擾的環境中，提供高效能的郵件服務。

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，郵件防護閘道更需能提供動態的即時防護，避免後方重要的郵件主機受到干擾。以維護上的考量來看，即使郵件防護閘道持續進行更新升級，內部郵件系統亦可安心處理郵件收發，彼此各司其職、互不影響。

溝通應用- 多台主機共同提供企業良好溝通平台

根據 Enterprise Strategy Group 調查：E-mail 已經成爲商務溝通最常使用的工具，企業員工每年平均會收到 25,000 封的電子郵件，而企業的智慧資產有 75% 都存在電子郵件媒介中，每天來往的業務與訊息都需倚賴電子郵件傳遞。因此，一個兼顧穩定與效率的訊息平台，已成爲企業維持競爭力的關鍵因素。

爲了能因應各種突發狀況，以確保重要的電子郵件系統長期穩定運作，除了導入相關防護、備份機制之外，建議企業可採用多台郵件主機的架構，各郵件主機共同分擔流量，且彼此互爲備援。郵件系統中不論是任何主機發生狀況，都不應該影響到電子郵件的收發。若將所有郵件功能全部整合在單一郵件主機之上，不但運作效率不佳，管理者也很難釐清問題，更可能因爲單一功能發生狀況，導致電子郵件系統全面停擺。

資料保存- 郵件備份需有效降低系統風險

在網路 e 化的世代，有越來越多的重要資訊是透過電子郵件傳遞，其中不乏寶貴的企業知識、機密資訊以及商業交易文件，導致企業對於郵件備份系統的日益重視。但除了加速落實郵件備份系統的建置之外，對於備份系統導入後對於既有郵件系統造成的衝擊，企業更不能等閒視之。

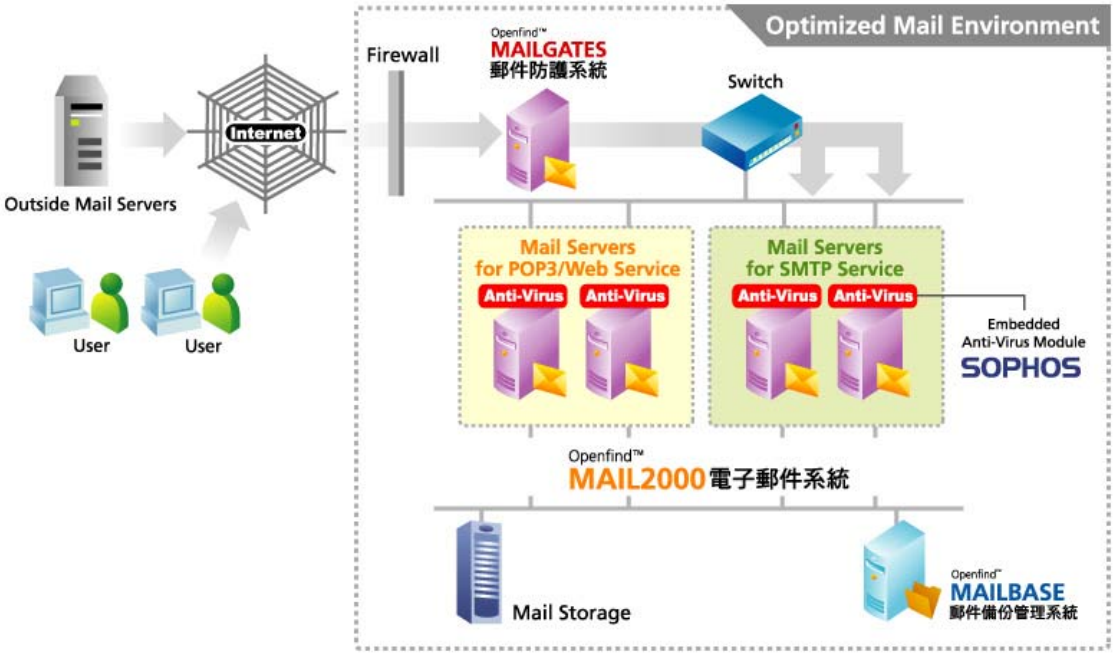
爲了確保信件備份系統的效能與安全性，筆者建議不要將備份與防護系統安裝在 Gateway 的同一台主機上，而是提供獨立主機讓備份系統單獨運作。相關的理由如下：

1. 郵件備份主機若與 Gateway 主機整合，等於是將備份信件暴露在高風險的對外網

路環境中。若稍有閃失，公司重要的機密郵件資料等於是任人魚肉。

2. 郵件備份系統應以不影響郵件收發流程爲最高原則。若與防護系統整合在同一台 Gateway 主機上，不但會影響彼此的運作效率，而且只要任何一個系統出了問題，都會造成收發信流程的停擺。

3. 郵件備份若採用 Gateway 的架構，將無法備份到內部互寄的 Webmail 信件。一旦被有心人士知悉，很可能會利用這個漏洞散發惡意郵件，造成企業有形無形的損失。



獨立架構發揮系統最高防護效能

環顧坊間大多數的訊息安全管理解決方案，多半採取 2 合 1 或是 3 合 1 的架構設計，將「郵件＋過濾」或是「過濾＋備份」規劃在同一部主機。這樣的部署方式僅適合信件量不大、對郵件系統風險容忍度較高的企業。反之，如果企業重視郵件系統安全，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。

	All in one	Independent
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	需維護三套系統
適用客戶	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	適合郵件量較大、需要彈性擴充整合內部軟硬體資源、並且非常重視資安的中大型企業

打造完善訊息安全管理平台-「防護、溝通、備份」

面對龐大的郵件訊息管理，企業應根據郵件政策重新檢視郵件訊息環境，進行整體性規劃後，再思考採購的需求與步驟。由於郵件系統需求與資安問題快速演變，計畫導入時應採取整體性規劃，以郵件系統的「防護、溝通、備份」三大系統爲主軸，爲企業描繪出完整的系統藍圖，再依據資訊預算決定進行多次或一次建置。妥善的郵件訊息規劃與保存，不但幫助企業善用與管理日益龐大的郵件訊息資產，更可有效提昇企業競爭力，降低資訊不當外洩的風險。