# 雲端技術對郵件威脅防護產業的影響

Openfind 產品經理 廖享進

隨著雲端世代來臨，許多資安產業也紛紛將自己的資安防護技術升級，霎那間許多冠著「雲端防護技術」的詞語，紛紛出現在許多防火牆、防毒軟體、防垃圾郵件系統、甚至入侵偵測系統 ( IDS、IDP ) 的技術規格上；尤其針對網際網路應用排名前三名的電子郵件，許多電子郵件威脅防護的廠商，也紛紛在自己的行銷資訊中揭露自家雲端防護技術的細節說明，令人目不暇給。到底現在所謂的雲端防護技術，跟以前的垃圾郵件威脅防護技術有什麼差別？現在又應該要怎麼挑選最好的雲端郵件威脅防護技術解決方案？這是許多企業組織的 IT 管理人員心中幾個最大的問題。

事實上，雲端技術這個名詞雖然在近幾年開始發酵，但其特質中的「即時性」、「隨選即用」的特質，早已存在於過往的郵件威脅防護技術中。郵件威脅防護是一門需要「快速反應」全球郵件威脅走向和趨勢的技術，因此許多廠商說明的「雲端防護」機制，其實也是新瓶裝舊酒，將以往早已具備這些特質的技術重新說明、包裝，進而讓使用者認為自己的郵件威脅防護方案，已具備先進的雲端防護特質而安心。這篇文章在此也將把這些「新瓶舊酒」的技術描述出來，讓郵件系統的管理者在如迷霧般的技術規格中，能清晰地辨別藏在行銷用語背後的真實內涵。

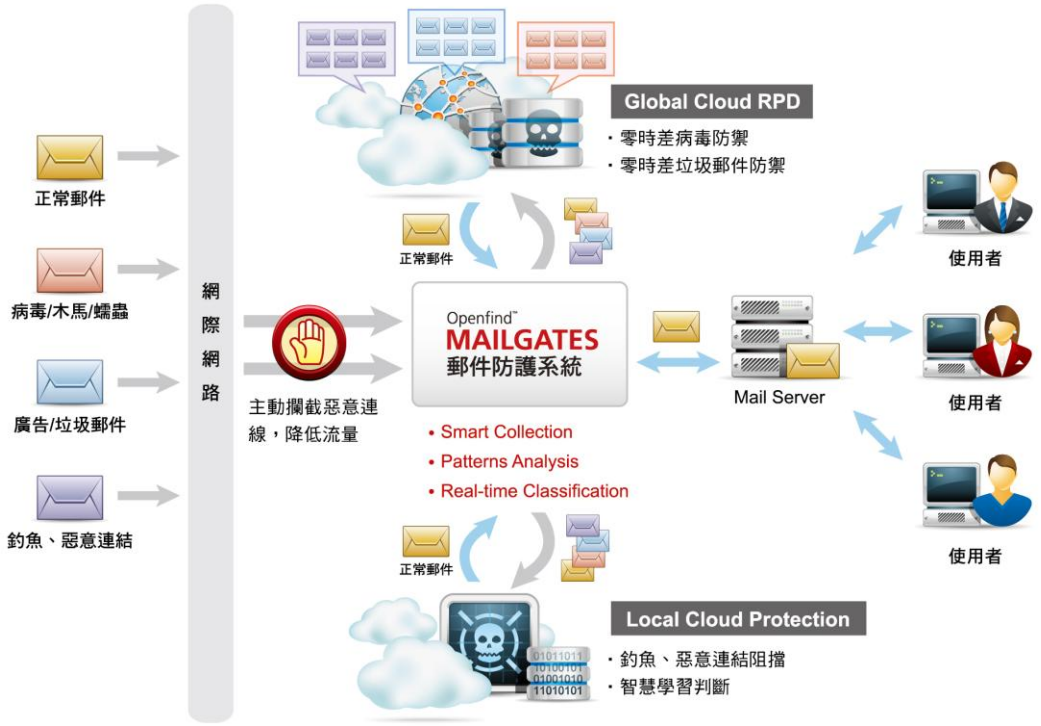
在以往的垃圾郵件防護技術中，最常被廠商包裝成現在雲端防護的項目就是 RBL ( Realtime Blackhole List )，也有人稱為 DNSBL。RBL 技術是透過郵件伺服系統在接收到郵件傳遞連線的同時，將對方 IP 位置利用 DNS 查詢的方式，快速的向 RBL 服務的提供者進行查詢，一旦發現這個 IP 位置已經被服務提供者或者相關的協力社群節點回報為黑名單，便阻擋這個 IP 連線，進而達到拒絕對方送信的防護效果。由於該技術具備「即時查詢」、「更新快速」的防護特質，因此最常被廠商包裝為雲端防護技術，例如趨勢科技的 ERS ( Email Reputation Service )、Barracuda 的 cloud-based email security service 等等。

除了 RBL 外，還有部份具備類似特質的舊技術，都會被包裝成現在的雲端防護技術，例如使用誘捕方式蒐集樣本，進而更新防護特徵碼機制的 Honeypot System、或者部份使用開放原始碼方案中的 SpamAssassin 協力社群提供的垃圾信特徵更新檔案等，都很容易包裝成雲端防護技術。事實上，這些技術也的確或多或少具備部份雲端技術的特質，如果不仔細挑剔「雲端防護」這四個字的嚴格定義，稱之為雲端防護也不為過，不過以下介紹幾個新興的雲端防護技術，則是可以讓企業組織的 IT 人員，作為郵件威脅防護解決方案選購時的參考。

在許多興起的雲端防護技術中，RPD 技術是很特別的一種混合式雲端防護技術，透過結合 Honeypot System 和郵件特徵分析，往往能精準地快速反應瞬間大量發信的垃圾郵件發送行為。RPD 技術的原理是使用一連串特殊的演算法，在各個 Honeypot System 的子節點中，將

郵件的內容計算出一個獨一無二的特徵值，並且反應回 RPD 服務提供者的資料中心，當郵件威脅的發送者瞬間大量發出垃圾郵件的同時，RPD 服務提供者的雲端資料中心，也能瞬間偵測到該封信件不合理的大量發送行為，進而通知所有服務的使用者，立刻阻擋該封郵件。RPD 技術的特色是從郵件內容的分析出發，進而延展到郵件發送行為的分析、判定，因此能作到「以行為判定」但「以內容為阻擋準則」的雙重效果。

另外一種混合式雲端防護技術，則是結合傳統垃圾信特徵碼與雲端即時查詢特質兩種優點，將傳統透過類似病毒碼更新特徵程序來防護垃圾郵件的方式進化，直接改將這些特徵值放置於防護技術提供者的雲端資料中心，並且直接透過網路線上即時查詢的方式，迅速阻擋這些郵件威脅。此一技術的特點是可以預防傳統下載等待特徵碼更新的防護空窗期，同時防護技術提供者也可以快速地反應許多處於爆發期（Outbreak）的郵件威脅，讓所有使用此類混合式雲端防護技術的客戶，在不需要更新系統的狀況下，立刻具備防護能力。




雲端環境的快速部署、強大運算能力等特性，將會使郵件威脅的風險以數百倍甚至數千倍的速度成長，近期許多駭客或惡意攻擊者也將 Botnet 視為強大的雲端服務，利用 Botnet 來達到「隨選即用」、「快速大量發送」、「用完即關」的郵件威脅發送行為，甚而演化成一門產值上千億的地下獨門生意。這都代表郵件威脅防護技術的反應速度週期，將從過去的「天」、「小時」，演化到「分鐘」甚至到「秒」，因此雲端技術的使用也將會是郵件威脅防護解決方案必須面對的課題。如何在眾多解決方案的廠商中，辨別雲端技術的新舊方式和效果，將是精挑細選過程中的關鍵。