金融客戶案例分享 | 導入產品 Openfind™ MailAudit

一分鐘聊案例

Openfind™
網擎資訊軟體股份有限公司
詳細資訊請查閱
http://www.openfind.com
聯絡電話
(02) 2553-2000 分機 888 業務部

客戶痛點

某大型商業銀行在臺灣有 150 家以上分行，海外亦有 100 多個服務據點，企業郵件系統使用人數高達上萬人，龐大的信件量加上往來郵件容易夾帶機敏資料，因此極度仰賴系統的自動化判斷及處理。金融單位基於業務需求往往保存了大量民眾機敏資料，包含個人資料、身分認證資料、信用卡、卡號等，而該銀行使用者卻反映原先既有的 DLP 系統一旦偵測到機敏資料，即全面阻擋郵件外寄，反而造成了資料交換困難；但若由使用者自行加密檔案夾帶寄出，雖然可解決資料交換問題，企業卻又擔心遭到有心人士利用，造成惡意外洩資料的可能。

導入效益

- 加密機敏郵件，收件人需使用正確密碼才能解開郵件，防止有心人士不當竊取
- 加密、解密、政策管理面都能依企業需求彈性設定
- 多主機可同時處理信件達到雙倍成效及服務不中斷目標
- 系統進行郵件全文偵測與保護，避免惡意加密或繞過稽核系統而外洩機敏資料
- 保存完整的原始郵件，需要調閱歷史信件時，不會因為原信或原始附檔被加密而無法確認內容，完整解決企業郵件外寄問題

網擎資訊協助金融單位利用郵件加密降低機敏資料外洩風險

某商業銀行是臺灣的大型商業銀行之一，臺灣有 150 個以上分行據點，海外各國亦有 100 多個服務據點，企業郵件系統使用人數達萬人，信件量多加上往來郵件容易夾帶機敏資料，因此需要依賴系統自動化判斷及處理郵件。

金融單位基於業務需求往往保存了大量民眾機敏資料，包含個人資料、身分認證資料、信用卡、卡號等，該銀行遵循個資法防範員工外洩機敏資料，原先已導入他牌 DLP 系統，但卻常聽到使用者反映業務往來有時需夾帶部分機敏資料，既有的 DLP 系統全面阻擋郵件外寄，反而造成資料交換困難；但若由使用者自行加密檔案夾帶寄出，雖然可解決資料交換問題，企業卻也無法掌握檔案原始內容，擔心遭到有心人士利用，增加惡意外洩資料的機率。

Openfind MailAudit 協助銀行客戶加密郵件，防範企業機密不當外流

衡量金融法規機敏資料於網際網路傳輸時應全程加密及業務需求，該銀行決定導入網擎 MailAudit 郵件稽核系統，利用 MailAudit 加密功能設定加密機敏郵件，收件人需使用正確密碼才能解開郵件，防止有心人士不當竊取。

1. 加密功能為客戶首要的評估重點

該銀行先與各單位討論郵件加密需求，歸納出兩種使用情境，情境一：郵件夾帶企業認定的機敏資料，先由稽核系統檢查，確認夾帶機敏資料後再進行加密外寄。情境二：郵件雖未夾帶企業認定的機敏資料，但使用者認為郵件需要受到保護，便主動觸發加密功能，由加密系統進行加密再外寄。以上兩種情境還可以延伸不少加密設定的細節，例如：觸發「主動加密」的方法、加密目標（郵件全文加密或是郵件附件加密）、郵件加密方式、密碼複雜度要求、密碼管理彈性、密碼傳輸對象控制等，這都是企業常一併評估加密系統的項目。

2. 其次就是系統處理效能

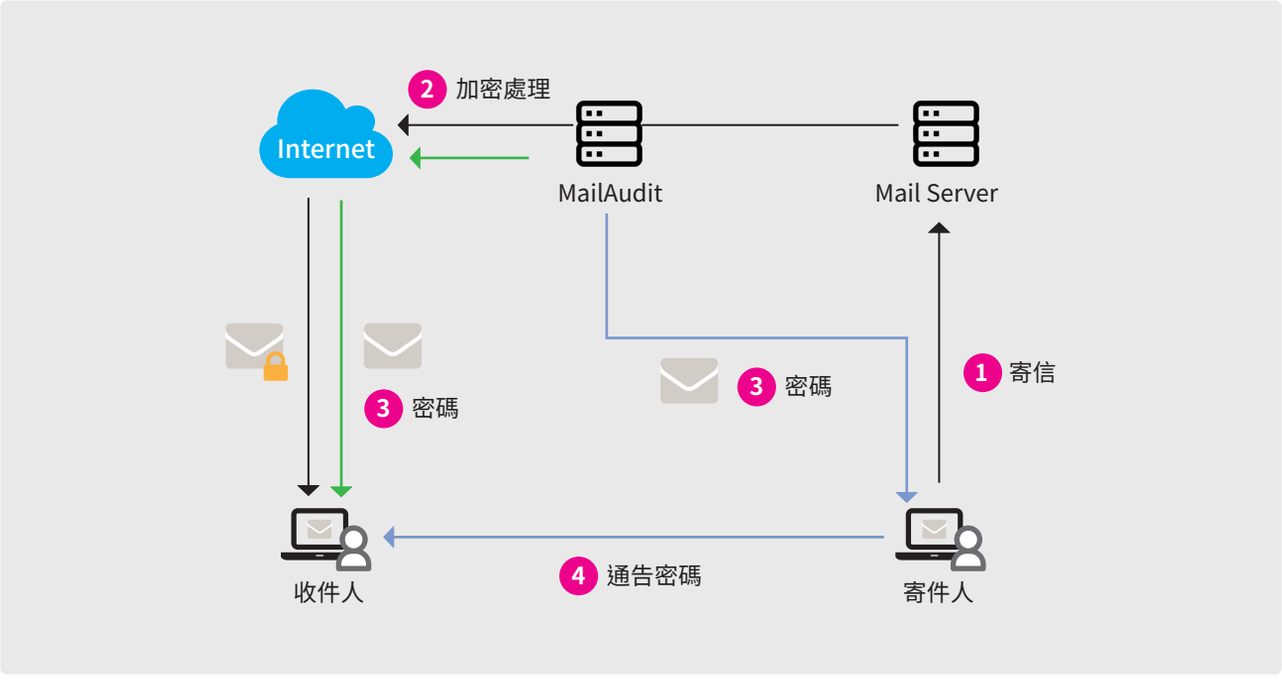
一來該客戶郵件量龐大，二來金融業往來郵件大部分都包括機敏資料，若因加密功能造成郵件堵塞或延遲寄達，將造成業務單位使用困擾，甚至產生損失與服務糾紛，因此系統效能評估也是相當重要的一環。網擎 MailAudit 完全符合企業所提需求，除了加密功能相當成熟，高效能也是 MailAudit 特點：單機一小時可處理並加密 90,000 封 50 KB 信件，另外企業也橫向擴充為多主機架構，由多台 MailAudit 主機同時處理信件，達到雙倍成效及服務不中斷目標。

加密功能可依需求彈性調整，由系統自動進行郵件全文偵測與保護

MailAudit 加密功能相當完整，不但能選擇對郵件全文或只針對郵件附檔進行加密，全文加密還可以選擇使用 ZIP 加密或 PDF 加密，企業能依單位需求設定切合收件者環境的加密方法，不需擔心收件者的電腦環境支援度，例如：A 單位使用 ZIP 加密，解密後的郵件為 HTML 檔案，收件者透過瀏覽器就能瀏覽信件；B 單位使用 PDF 加密，解密後的郵件為 PDF 檔案，PDF 背景附加企業 Logo 顯得更為正式，也能限制郵件資訊被列印及複製。

大部分郵件都直接採用 MailAudit 自動加密，由系統判斷是否執行加密程序，過程不需要人為介入或管理，MailAudit 也能依照郵件標題關鍵字進行加密，企業導入 MailAudit 時會向使用者宣導加密關鍵字；以 [請加密] 舉例來說，當使用者認為郵件需要被保護時，只要在郵件標題加上 [請加密] 字串，MailAudit 偵測到便會移除 [請加密] 字串再進行郵件加密，達到使用者主動觸發郵件加密的目標。

MailAudit 郵件加密後會產生一封加密信及一封對應的密碼信，加密信直接外寄給收件人，密碼信企業則選擇寄予寄件人，由寄件人另外進行密碼的通告；而加密用的密碼依企業規範產出高度複雜的組合（包含最小為 8 碼的英數字及特殊符號），不需擔心加密信件輕易被破解。企業也開放使用者使用「約定密碼」：使用者自行設定固定往來對象的解密密碼，當郵件收件人為約定密碼設定對象時，MailAudit 便改用當組約定密碼進行加密，大幅簡化使用者重複通告密碼流程。



因為導入 MailAudit 加密功能，由系統進行郵件全文偵測與保護，使用者不再需要自己加密重要信件或附件，除了增加工作效率，對企業來說更能掌握每一封外寄郵件的資訊是否合法，無須擔憂有心人士惡意加密、繞過稽核系統散發機敏資料；企業既有的備份系統也能保存完整的原始郵件，未來稽核單位或法務單位需要調閱歷史信件時，不會遭遇因為原信或原始附檔被加密而無法確認內容的窘境，完整解決企業郵件外寄問題。

加密同時效能表現毫不遜色 郵件防偽更大幅提升系統安全

雖然郵件加密能解決企業困擾，但同時也擔心加密程序造成郵件壅塞而得不償失，因此效能處理評測也是該銀行選用加密系統的重點。MailAudit 分別進行了兩次實測：測試 10 分鐘收到 34,000 封信件，並完成所有信件 ZIP 加密的處理時效。第一次測試每封信檔案大小為 50K，MailAudit 於 22 分鐘完成 34,000 封信件處理，推估 1 小時可處理 90,000 封信流量；第二次測試每封信檔案大小為 10M，MailAudit 於 9 小時 26 分鐘完成 34,000 封信件處理，推估 1 小時可處理 3,600 封信流量。MailAudit 1 小時處理的郵件封數皆高於企業壓測標準，都一再證明 MailAudit 對信件的優異加密處理能力。

MailAudit 作為郵件外寄最後一站，用於郵件防偽的 DKIM (DomainKeys Identified Mail) 機制也是極為重要且必要的功能之一。DKIM 是一種以數位簽章為基礎的電子郵件認證標準，企業透過 MailAudit 產生 DKIM 公鑰，並將其加入企業 DNS 主機，而所有外寄信件則由 MailAudit 自動加簽 DKIM 私鑰，收件者端的電子郵件服務便能比對來信私鑰與 DNS 公鑰是否相符，以此過濾信任企業的來信、避免被判定為垃圾信件，提升郵件傳遞之安全性與信賴感。

未來計畫分階段導入完整稽核機制，確保商業機密寄送無虞

因為加密設定僅是 MailAudit 郵件稽核系統的功能之一，而金融單位往往因為擁有大量機敏個資，主管機關對其資安要求更為嚴苛，所以對於此金融客戶而言，即使已導入 DLP 系統，但被動預防資料外洩是遠遠不夠的。有鑑於此，該銀行未來也計畫分階段擴充導入完整稽核機制，藉由徹查郵件及附件是否帶有機敏資料或個資，其中更包含滴漏式個資稽核，依企業規則檢核銀行帳號、保單帳號，與現有 DLP 系統共同佈署多重檢核關卡，準確攔截異常郵件、確保機密商業文件使用加密方法安全寄出，準確遞送給指定收件人。