

以私有企業個人雲支援法規遵循及跨平台協同

網際網路、雲端應用、智慧型手機的出現，企業成為跨應用、跨（公、私）網路、跨裝置的環境。對企業員工來說，跨平台、跨雲的協同行為再尋常不過。然而這也意謂著安全風險及法規遵循的責任隨之升高。

現今企業生產力和協同密不可分。為了提升生產力及業務運作，企業員工以電子郵件交換機密資訊、用網路芳鄰或 Dropbox 分享檔案、用 FTP 上傳客戶或其他工作上的資料，再尋常不過了。市場分析機構 Gartner 預估，到 2022 年全球 80% 的中大型企業會部署內容協同平台(Content Collaboration Platform)。



（Openfind 行銷處協理林家正）

然而，各種企業資料分享管道都有不足，像是電子郵件拒收太大檔案、FTP 和 NAS 系統分享無法追蹤資料流向有資料外洩可能。雲端化的 Dropbox 十分方便，但是公司 IT 部門無法有效管理、USB 隨身碟容量有限，而且容易掉，還可能夾帶病毒。檔案伺服器現在仍有許多企業使用，但是從外部網路需要建立 VPN 才能下載檔案，不利於在外作業的員工，如支援工程師或業務人員存取，而且檔案伺服器缺乏存取控管、紀錄、備份機制，可能置重要資料於竄改、破壞及被惡意程式感染的風險，更別提企業資產被勒索軟體加密，必須破財消災的威脅。

上面還只是企業部門考驗的一部份。另一個更大的挑戰來自法規遵循。從《個人資料保護法》、《營業秘密法》，今年還多了《資通安全管理法》，以及歐盟推動的《歐盟通用資料保護規則》(EU General Data Protection Regulation, 簡稱 GDPR)。以國內銀行業為例，主管機關金管就有嚴格規範，並不時提出糾舉，像是要求圖片稽核、往來電子郵件要備存 7 年、客戶個資需加密儲存，以及外部網路不得下載檔案的資料不落地限制，而且受到新興的勒索軟體威脅影響，現在連企業常用的網路芳鄰，也被限制要求資料傳輸處理需做好認證及軌跡紀錄。

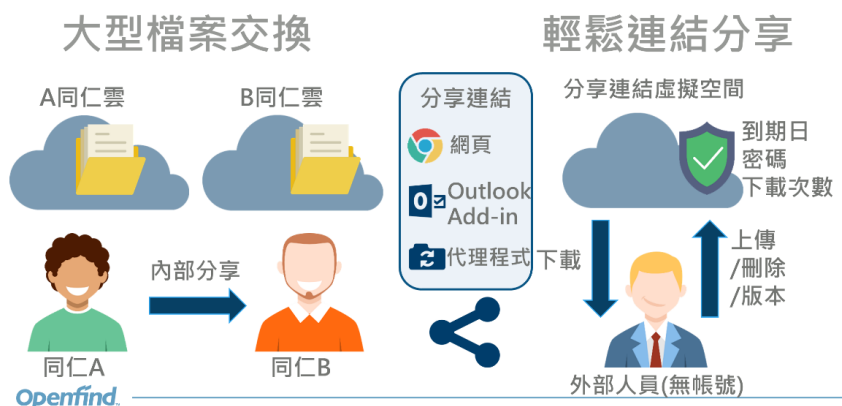
那麼，要如何在現在跨平台、跨網路協同環境中，確保生產力與法規遵循的平衡呢？網擎資訊從郵件歸檔產品起家，之後日漸擴大產品線到郵件資安、防詐騙沙箱技術，去年收購和沛科技的私有企業個人雲產品 ArkEase Pro(以下簡稱 AEP)後，則積極整合為串連企業內網、外網及雲端的資料協同安全產品。



（AEP 可確保企業員工、外部人員在私有企業個人雲上方便而安全的協同。）

AEP 可以跨平台、跨裝置提供員工重要資料同步與備份，而且確保權限控管與存取安全，並能防禦勒索軟體損害。在 AEP 平台的多人協作空間，專案團隊管理員可針對不同職務角色（或是公司內、外部人員）設定存取權限、或是設定容量上限。它對內網允許大型檔案交換、對外網支援網頁、Outlook add-on 及代理程式分享連結，而不同人的文件更動、上傳、下載、刪除在系統上都有軌跡紀錄，以便於管控究責。此外，所有文件也都有檔案版本控制及註解、備份，方便資料的回溯及復原。當團隊中有員工離職，管理員只要移除帳號，就能關閉所有存取權限，還能將資料指定給接班人。

分享檔案再也不用擔心檔案量大小



（ AEP 對內部員工允許大型檔案交換、對外部人員或外網存取支援網頁、Outlook add-on 及代理程式分享連結）

AEP 還提供以 AI 為基礎的惡意軟體防護。例如，AEP 若透過文件中的誘餌代理程式偵測到文件於異常時間加密，就會緩步或停止上傳到雲端，如果真的偵測是遭勒索軟體加密時還能以備份版本還原文件。

秉持產品雲端化、資安在地化及溝通協同化精神，結合網擎 AEP 及其資安與郵件管理產品，將可協助企業在多平台協同環境中，確保兼顧法規遵循、安全及生產力。