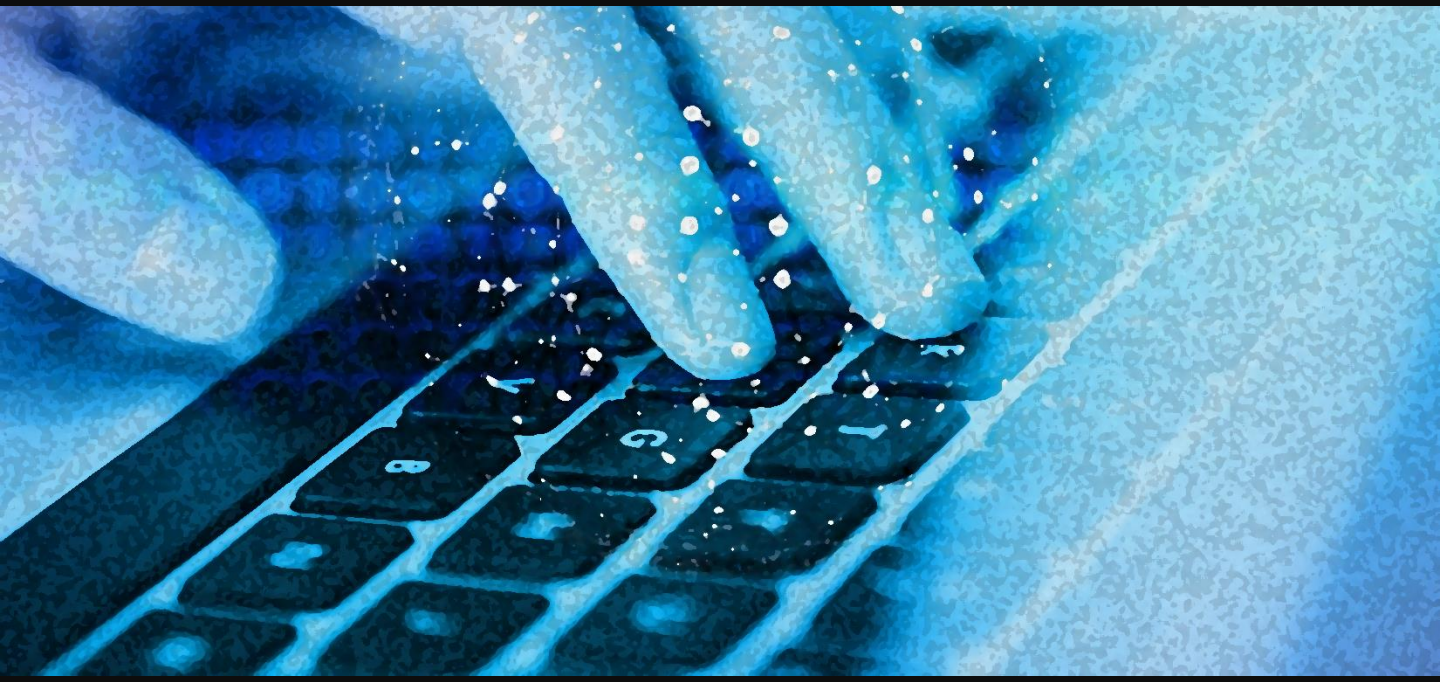
2020

高科技機密智財防洩
關鍵祕笈

看 OmniStor 數位應用如何強化企業資安防禦



asusCLOUD

引言

高科技製造業因其複雜的產業鏈關係，在推動新市場與發展新科技的過程中，有許多機密的資料與檔案需要被保護，這些資料包含客戶保密協議、執行專案內容、產品規格文件、研發專利、製程文件與設計圖稿等；與供應鏈合作，需要交換和營業機密與研發技術相關的資訊，都需要嚴密的方式防堵外洩。高科技業常見離職員工因競業祭出高薪誘因，竊取公司專利、製程等營業機密，再透過 Email、個人雲、隨身硬碟等方式外流，協助對手超前開發，破壞市場布局，當事人及竊密之公司除了嚴重違反《營業秘密法》，面臨法律責任及賠償，對原公司更造成龐大營業損傷，影響企業與客戶及供應鏈間的合作信賴關係。

中美貿易掀起一波科技戰，加深了外商客戶對於合作企業專案機密保護的資安意識提升，亦不乏客戶要求高科技業遵循國際標準原則強化資安防禦。此外，隨著 COVID 19 驅動數位轉型加速，企業面臨首當其衝的問題，即是在佈署數位及遠距辦公應用，必須同時兼顧安全與便捷。也因為存取裝置愈來愈多元、駭客攻擊事件層出不窮，資安已成為大企業 IT 首要投資的關鍵。值得重視的是，從多項報告分析指出，內部員工威脅，相較於外部駭客攻擊，更是影響公司信譽的一大潛在風險。

由 Cybersecurity Insiders 發表的一份《2020 內部威脅報告》[註] 中，揭露大企業在新環境下，面臨的潛在內部威脅來源及挑戰。幾個關鍵的發現如下：

內部員工威脅帶來更難偵防的資安風險

內部威脅對企業造成的影響，從有形至無形都動搖著企業未來的發展。前三大最常見的影響為：營運中斷 (50%)、關鍵資料遺失 (48%) 以及品牌危機 (37%)。此外，其他主要影響還包含企業營收損失、失去競爭優勢、連帶的法律責任以及補救支出。有近 6 成的企業認為來自內部的威脅相較於外部威脅，更難偵測與防護，原因包含：

- 內部員工通常已有敏感資料及應用程式的存取權限，使得可疑的活動較難被發現 (61%)
- 內部員工對於網路郵件、公有雲及社群的仰賴，讓資料更容易被流出 (52%)
- 有愈來愈多的內部員工資料不在企業的控制與安全防護範圍內 (45%)

此外，內部員工分享資料常用的電子郵件、通訊及溝通軟體 (42%)、個人雲、公有雲如 Dropbox、OneDrive (39%) 等，被視為竊取機密的主要途徑。這些外在因素實際也反映了潛在的內部問題，包含：員工欠缺資安意識及訓練 (58%)、企業針對資料保護的政策與方案不足 (51%)，再者，在 BYOD (Bring your own device) 趨勢下，有愈來愈多的個人裝置，可以存取公司重要的資料 (51%)，也對關鍵資料的保護形成威脅。

複雜的非結構化資料與缺乏維護人力影響政策推行

對任何一家企業而言，資料是企業的核心資產，而某些特定的資料類型，非常容易遭到內部威脅的覬覦，這些資料分別是：客戶資料 (61%)、財務資料 (54%) 以及智慧財產 (IP，53%)，其他包含員工資料、公司資料、業務與行銷資料等都被視為企業主要受保護的關鍵內容。而在資料的保護上，超過半數 (52%) 的企業認為非結構化的資料，如文件、產品規格、簡報、工程圖等，相較於資料庫型態的結構化資料 (12%)，是更難被保護的。亦有將近 8 成的企業認為，追蹤檔案的歷程對於資安政策的實施與稽核非常重要。

超過 6 成的企業雖然知道坊間有合適的工具可用來追蹤敏感資料與保護內部威脅，但還未正式採用的瓶頸包含：缺乏導入的人力 (42%)、類似 DLP 的工具價格太高昂 (37%)、缺乏維護工具的人力 (32%)；而已經採用 DLP 等工具的企業 IT，也反映了實際面臨的挑戰：資安政策與業務需求齊行困難度高 (27%)、對於資料或檔案只有受限的可視度 (25%) 以及採用的工具有太多誤判的結果 (23%)。

[註] 資料來源：Cybersecurity Insiders 《2020 Insider Threat Report》

面對內部威脅，企業如何保護關鍵智財

企業面對資安事件與內部威脅，需要檢視與盤點是否做足了以下準備：

- 有效控管資料帳戶驗證與檔案類型，並可追蹤使用者動態與異常檔案行為
- 依據最小權限原則，給予企業成員執行任務和完成工作所必需的存取權限
- 無論是內部或外部資料交換，都需建立安全性原則以保障關鍵資料內容
- 能夠辨識與控管企業內部存在的風險檔案，並設立安全性政策掌控流向
- 關鍵資料的協作與攜出，都需在授權核可的情況下進行，確實掌握使用動態

OmniStor 企業儲存雲

ASUS OmniStor (以下簡稱 OmniStor) 為企業級檔案儲存管理與內容協作平台，以資料應用為核心，具備多層式彈性佈署模式，滿足企業高資安防禦要求。透過單一平台集中企業檔案，強化企業內部授權管理、存取安全性防護及外部分享風險控管。原生高可用架構，提供檔案異常威脅阻斷與復原機制，降低 IT 管理成本，保障企業營運持續性。整合內網共同編輯應用，友善使用者體驗，滿足遠距辦公安全協作需求，使用無學習門檻，加速企業數位轉型。

輔助企業從日常建立多層式防禦堡壘

在檔案的管理與應用，不犧牲使用彈性同時擁有存取安全性，是許多企業的必備需求，OmniStor 的多層式防禦特質，為高科技業在關鍵資料保護上提供一個兼具可靠、可用、彈性與安全優勢的平台，讓企業所有機密文件與敏感資訊都能在高度管控的協作環境下，嚴密保護。

第一、從網路層級建立多層式的防護架構

多層式元件佈署

OmniStor 提供元件佈署的彈性，可拆式的元件，為企業的資料防禦設下一道強化的關卡，從網路層級佈建多層式架構，在使用者登入服務、驗證帳戶到進入服務享受到分享便利前，透過企業防火牆、白名單及傳輸加密等機制，阻斷可能的風險。

高可用架構

OmniStor 原生 Active-Active HA 架構，透過成對架構實現檔案及時備援，遇到單點伺服器失效，系統將立即啟動備援機制，保障服務不中斷，資料不遺失。

第二、從身份層級建立存取權限控管

白名單控管 (AD / IP)

系統管理者可設置 AD 白名單，控管可登入 OmniStor 企業儲存雲的成員清單，不明 IP 的成員帳號，將多一層圖形驗證機制始可登入，僅有經授權白名單內的 IP 始可下載使用檔案。在遠端辦公需求下，同樣達成嚴防資料外流之效。

群組權限控管

平台管理者可針對群組成員(通常為單位或部門別)設置成員的分享、編輯、下載、全文檢索等權限，給予成員符合其職務最小化的權限以確保資料安全。

第三、從資料層級建立資料交換的安全原則

內部分享資料安全性原則

OmniStor 提供企業成員間分享的安全性原則，可依資料夾成員職務定義其檢視或編輯權限，並可指定特定成員為代理人，協助資料夾擁有者新增、刪除與管理其他成員的權限，多階式授權降低管理負擔。

外部分享資料安全性原則

提供外部單位或廠商分享的安全性原則，可設定廠商存取資料截止日、存取連結密碼，廠商提交檔案，亦可設定檔案上傳可用空間，便利大檔傳輸應用情境。

第四、從風險檔案層辨識與控管可能的風險

風險檔案控管

企業檔案上傳，無論來自內部成員或外部廠商，皆可透過 OmniStor 的防毒與 DLP 整合應用掃描，篩選具有中毒檔案或敏感資料的風險檔案，並可依據企業需求自訂風險檔案安全性原則，可依據風險等級設定放行及審核機制，或嚴禁風險檔案進一步分享，保障敏感資訊受控管。

第五、從整合層建立安全的協作與攜出機制

建立檔案安全攜出機制

在面對企業內部機密文件或敏感資料，無論是內部成員於非公司以外的場域需要使用檔案，或者需要將檔案提交給第三方的廠商或外部單位，都可藉由整合企業內部審核系統，建立完善攜出審核機制，為企業資料於外部使用的安全多一層防護。

落實資料不落地應用

從群組的職務需求，企業可規範群組成員可使用檔案的存取範圍，如線上預覽、編輯與下載，或可透過 IP 白名單的設定，控管成員可以下載檔案的場域。針對機密文件，除了上述的存取控管，更可透過預覽及編輯套入浮水印防護機制，嚇阻內部員工進行不當的資訊外流。

總結

企業面對重要資產外洩的風險與威脅，透過 OmniStor 企業儲存雲輔助，除了能加速企業數位轉型、滿足遠距辦公需求、解決 IT 管理負擔、不改變使用者日常習慣，更讓企業內部及外部的成員都能在高強度的資安防禦架構下，輕鬆享受協作的便利性，提升生產與企業競爭力。

了解更多

想了解更多 OmniStor 於高科技製造業應用情境與商用解決方案，歡迎與華碩雲端銷售團隊聯繫。

官方網站

www.asuscloud.com/contact.html

電子郵件

solution@asuscloud.com