DLP 解決方案的優點

DLP 的第一項優勢是可以對資料進行分類和監控，同時提升整體的可見度和控制能力。

分類和監控敏感性資料

了解自身持有哪些資料以及這些資料在數位資產中的使用方式，可讓組織更輕鬆地識別未經授權存取資料的行為，並避免資料遭人不當使用。分類是指套用規則來識別敏感性資料和保持符合規範的資料安全性策略。

自動化資料分類

自動化分類會收集相關資訊 (例如文件建立的時間、儲存的位置以及共用的方式) 來提升組織資料分類的品質。DLP 解決方案會運用這類資訊來強制執行 DLP 原則，而這有助於防止與未經授權的使用者分享敏感性資料。

監控資料存取和使用情況

為了防患未然，您需要監控誰能存取什麼內容，以及他們會利用這項存取權做什麼。在所有網路、應用程式和裝置上管理員工、廠商、承包商和合作夥伴的數位身分識別，藉此防範內部漏洞和詐騙。 角色型存取控制是其中一種方式，僅會將存取權提供給需要權限完成工作的人員。

偵測和封鎖可疑活動

自訂 DLP 解決方案，以便掃描所有經過您網路的資料，並阻止資料透過電子郵件、複製到 USB 隨身碟或其他方式離開網路。

維持法規合規性

各組織皆必須遵守資料保護標準、相關法律及規定，例如健康保險流通與責任法案 (HIPAA)、沙賓 (SOX) 法案以及聯邦資訊安全管理法案 (FISMA)。DLP 解決方案會提供完成合規性稽核所需的報告功能，其中還可能包含為員工制定資料保留計劃和訓練計畫。

提升可見度和控管力

DLP 解決方案能為您提供組織內敏感性資料的可見度，並協助您探查有可能將敏感性資料傳送給未授權使用者的人員。決定實際和潛在問題的範圍後，您可以進一步自訂設定以分析資料和內容，藉此強化網路安全性措施和 DLP 投入量。

Office 365 + Office 365 DLP

Office 365 資料遺失防護 (DLP) 幫助組織通過深入的內容分析來識別、監控和保護敏感信息。它允許您設置規則和政策，以確定數據應如何保護、處理，以及如果數據在違反這些規則的情況下被共享，應通知誰。

資料外洩防護結合相關人員、程序及技術，來偵測和防止敏感性資料外洩。DLP 解決方案使用像是防毒軟體、AI 和機器學習等技術來比對內容與組織的 DLP 原則，藉此偵測可疑的活動。這些原則會定義組織如何標記、共享和保護資料，同時避免將資料暴露給未經授權的使用者。