檢查清單：需要將 DLP 新增至 MSP 實務的五個標誌

為什麼服務供應商應該關心資料外洩防護（DLP）？

多年來，組織在保護敏感資料免遭透過外部攻擊或內部風險（如 IT 設定錯誤和人為錯誤）造成未經授權的存取和外洩方面成效甚微。這讓其不得不面臨令人難堪的頭條新聞、客戶和合作夥伴信任受損、股權損失及法規制裁等後果。

隨著行為式資料外洩防護（DLP）技術的興起，MSP 現在可以毫不費力地啟動和管理 DLP 服務，盡可能降低客戶的資料外洩風險。

現在正是利用這一趨勢的大好時機，可讓客戶資料安全无虞，其法規遵循完好無損，從而確保客戶高枕無憂。

「80% 的全球組織報告稱在未來 12 個月內，他們可能會遇到影響客戶資料的資料外洩。」

來源：Ponemon Institute 2021 年網路風險指數報告

檢查需要將 DLP 新增至實務的五個標誌

1 客戶的員工可以透過其端點存取敏感資料（如受法規管制的資料）

無論客戶的資料是否儲存在雲端，或者是否可以透過員工的工作站進行存取，這些資料都很容易透過週邊裝置或網路通道（如電子郵件和即時訊息）洩漏出去。

根據《2022 年 Verizon 資料外洩調查報告》，80% 以上的資料外洩皆出於財務動機。因此，如受法規管制的資料、商業秘密或可用於財務收益的智慧財產資料等攻擊目標的主要資料往往具有較高價值。

如果客戶的員工在其端點上建立、儲存或使用此類資料，您需要確保這些資料不會洩漏給未經授權者，以避免他們面臨嚴重的財務、法規及信譽風險。

2 您正在尋找新的收入來源以壯大業務

在 MSP 2021 報告的 Acronis 脈動中，我們可以看到 MSP 預計其未來幾年的主要收入來自網路資安。然而，隨著大多數服務供應商提供某些形式的受管安全性服務，競爭正成為該產業的主要挑戰。

行為式 DLP 技術的興起讓您能夠將產品組合與一些 DLP 服務區分開來，這些 DLP 服務先前不適用於 MSP 和較小組織，因為其複雜性高、服務交付成本高，而且由於需要將原則對應至特定於每個客戶的不斷變化的業務流程，實現價值時間亦較慢。

藉由行為式 DLP 技術，您可以找到新的收入來源，為各種規模的組織提供具吸引力的 DLP 服務產品，從而降低客戶資料最終落入未經授權者的風險。

3 您的客戶身居受嚴格監管的產業 (如醫療健康、BFSI、政府部門)

如果您的客戶使用或儲存個人可識別資訊 (PII)、病患醫療資訊 (PHI)、持卡人資料或受嚴格監管的產業中任何其他形式的敏感資料，則他們需要比備份更高層級的資料保護。

在發生敏感資料外洩時，大多數法規 (如 GDPR、HIPAA 和 PCI-DSS) 皆要求在嚴格時間範圍內報告資料外洩和資料洩漏情況，可能會導致客戶受到重罰。

資料外洩防護解決方案是唯一能夠監控組織內部資料流並防止資料外洩的技術，同時還能夠提高 DLP 事件的可見性並啟用調查。

4 您的客戶較容易遭受攻擊和資料外洩風險

從過往經驗來看，有一些產業存在較大安全性漏洞且同時還儲存珍貴的敏感資料，從而成為網路攻擊的高價值目標。這類產業包括教育、醫療保健及其他需要資料可存取性的公共部門，但與此同時，您需要對這些資料進行有效保護，使其不會洩漏給未經授權者。

行為式 DLP 技術讓您能夠以經濟實惠的價格提供具有較高競爭力的 DLP 服務，以保護此類組織抵禦不符規範和資料外洩風險。

5 您的客戶正考慮/支付網路保險以減輕責任

面對現實吧 – 網路保險是近年來網路資安領域最熱門的話題之一。客戶紛紛轉向網路保險公司，以限定發生資料外洩時企業的責任。

網路保險的成本取決於幾個因素，包括企業的年收入、產業、所持有資料的類型和數量以及安全性等級。您應考慮將 DLP 新增到您的服務堆疊中，以滿足網路保險的資料安全防護需求，同時將客戶成本降至最低。

Advanced DLP

Acronis Cyber Protect Cloud 的 Advanced DLP 可協助客戶高枕無憂，因為其敏感資料會受到保護，不會洩漏給未經授權者。其獨特的行為式技術支援根據每個客戶的具體情況建立和持續延伸 DLP 原則，並以前所未見的簡單、便捷性簡化服務啟動。