Acronis

白皮書

啟動和擴展 DLP 服務：MSP 指南

近年來，儘管意識、安全性通訊協定和法規皆有所提升，但各種規模的組織仍無法應對資料外洩風險。事實上，它們實際在不斷攀升：根據 Risk Based Security 的《2021 年終報告：資料外洩快速檢視》，該年暴露的記錄超過 220 億條，達到2005年以來機密資料遭入侵數量第二高。這些記錄中絕大多數都是由於資料外洩而暴露。資料外洩定義為安全性破壞，指機密、敏感或受保護資料意外或刻意洩漏給不受信任的環境或組織外部或內部未經授權的使用者。

那麼，是什麼導致資料外洩？有兩個主要原因：

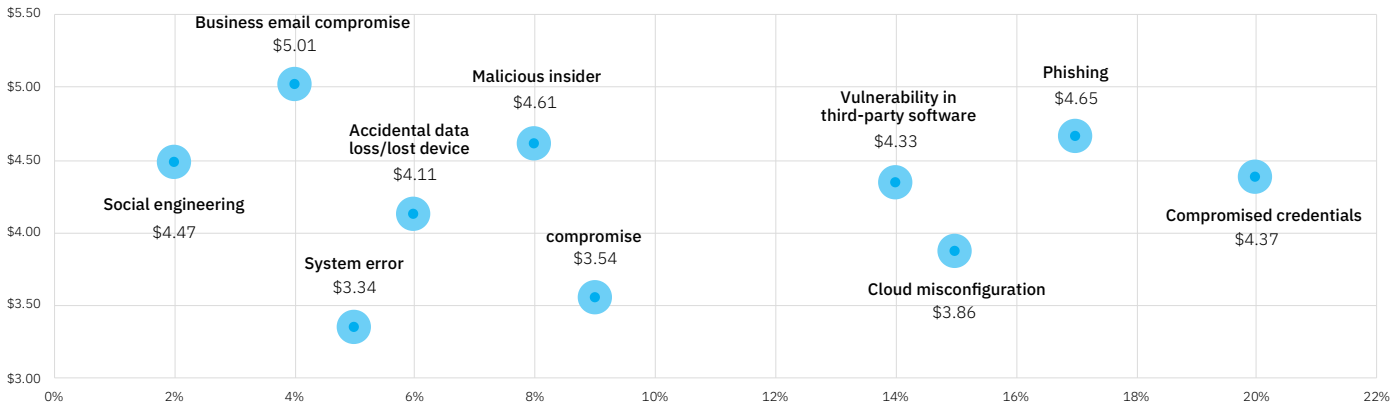
1.外部網路威脅

根據 MITRE ATT&CK 架構的定義，資料外洩是惡意對手在攻擊期間採取的最後手法之一。根據 Verizon 2022 年資料外洩調查報告，80% 以上資料外洩行為發動者的動機是牟取經濟利益。

這就是敏感資料成為大多數攻擊的主要目標的原因所在。惡意對手一旦建立對公司環境的存取，他們就可能嘗試透過各種通道來外洩資料。隨著攻擊的複雜性不斷增加，越來越能夠避開安全防護關卡，組織資料的風險呈現指數性成長。

2.內部風險

雖然防惡意軟體和其他端點安全技術能夠偵測和阻止外部攻擊，但組織資料的其他風險 (與內部相關的風險) 卻不斷增長。一個常見的例子是終端使用者在不知情的情況下將資料洩漏給未經授權者 (如透過轉寄電子郵件)。發生這種情況的原因可能是偶然的員工錯誤、IT 設定錯誤或惡意內部人員所為，所有這些都可能對組織構成嚴重威脅，進而導致代價慘重的資料外洩。



值得注意的是，儘管部分組織低估了內部風險的影響，但 Ponemon Institute 的《2021 年資料外洩成本報告》明確指出大約三分之一的資料外洩牽涉到內部人員。

資料外洩對企業有什麼影響？

資料外洩會給企業帶來嚴重風險。將敏感資料外洩給未經授權者會導致：

- **不符合法規** – 儲存、存取和保護諸如員工和客戶個人可識別資訊 (PII) 、受保護的醫療資訊 (PHI) 或持卡人資料的敏感資料受當地和國際法規 (包括 GDPR、CCPA、HIPAA、PCI-DSS 等) 的嚴格監管。一些法規 (如 GDPR) 甚至要求在嚴格的時間範圍內報告外洩情況。如果受監管資料外洩報告延遲，組織可能會面臨巨額罰款，甚至可能會失去其合規性認證。
- **財務損失** – 資料一旦外洩，除了 MSP 客戶可能面臨的違規罰款外，服務供應商也可能因對客戶的安全責任而面臨財務損失威脅，這可能會導致訴訟。此外，洩漏商業秘密或智慧財產還可能會給公司造成額外的財務損失，甚至動搖其市場地位。
- **信譽風險** – 最終成為令人難堪的資料外洩頭條新聞可能會對企業不利。這不僅會導致客戶的客戶流失，還可能會損害現有合作夥伴並削弱開拓新客源能力。客戶發生資料外洩也可能會影響您的聲譽和業務。

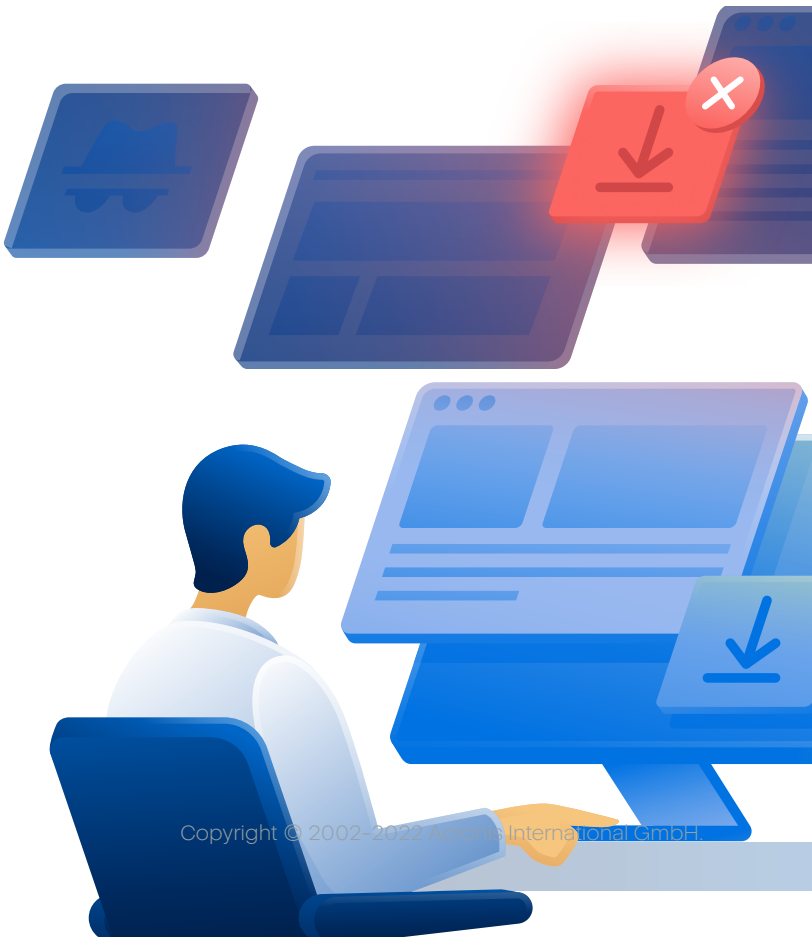
什麼是資料外洩防護？

資料外洩防護是一種早就建立的安全性解決方案類別，代表可偵測和防止未經授權的使用、傳輸和儲存機密、敏感資料的整合式資訊安全性技術系統。

DLP 解決方案透過套用資料流控制和內容分析方法的組合來實現這一點。此類技術會在整個組織中實施業務可接受的資料使用和處理原則，防止將敏感資料洩漏給未經授權的收件者 (內部和外部)。

雖然資料防護主要與備份和災難復原相關，但還有諸如 DLP、公證和加密等其他重要技術，可保護敏感資訊免遭各種不同的威脅 (如資料外洩)。

DLP 是唯一一項能夠提供整個組織內敏感資料流動和儲存可見性和控制的技術，可防止這些資料洩漏給未經授權的實體。



資料狀態和不同的功能性 DLP 如何保護它們

資料可以存在於組織內的**主要狀態有三種**：

- **使用中資料：**正在本機通道 (如週邊設備、卸除式儲存裝置) 中或透過端點電腦上的應用程式使用或傳輸的資料。此類資料的一個例子是正從端點電腦傳輸到 USB 磁碟機的檔案。
- **傳輸中資料：**此術語指正在電腦系統之間移動或傳輸的資料。例如正從本機檔案儲存傳輸至雲端儲存的資料，或透過即時訊息或電子郵件從一個端點電腦傳輸至另一個端點的資料也視為傳輸中的資料。
- **靜置資料：**這說明的是儲存在本機或網路中且目前未被存取或傳輸的資料。靜置資料的一個例子是儲存在網路共用或地端部署伺服器中的資料。

必須注意的是，資料會頻繁並持續地變更其狀態 (儘管有些資料可能在端點的整個生命週期中都保持單一狀態)。瞭解資料的不同狀態、其具體情況和差異，可以協助客戶更安全地處理其組織資料和防止資料外洩。

分別有三種主要「功能性」DLP 類型專用於保護每種狀態的資料：

- **使用中資料 DLP**
- **傳輸中資料 DLP**
- **靜置資料 DLP**

值得一提的是，還有其他可以應對不同資料風險 (如可存取性，隱私風險) 的技術，如身分管理或加密。但是，DLP 是唯一能夠跨多種狀態保護資料的技術，其正式目的是防止資料外洩，同時提供資料流的可見性。

DLP 控制：內容與上下文

組織中的每個資料流都有其上下文和內容。上下文指的是環境因素，如資料流中涉及的使用者、所使用的通道、流的方向等。內容說明的是所傳輸資訊的實際類型/類別，如病患醫療記錄、員工 PII 等。

高效的 DLP 解決方案應根據資料流的上下文和內容對其實作控制：

- **上下文感知 DLP 控制** – 根據作業的上下文，透過使用一些屬性 (如相關的使用者、使用的通道、傳輸的資料方向、目的地、時間等) 來控制資料傳輸作業。

範例：允許使用者 (身分) 將資料 (內容) 複製到加密的 USB 裝置 (地點) 並阻止將資料複製到未加密 USB 裝置的原則。

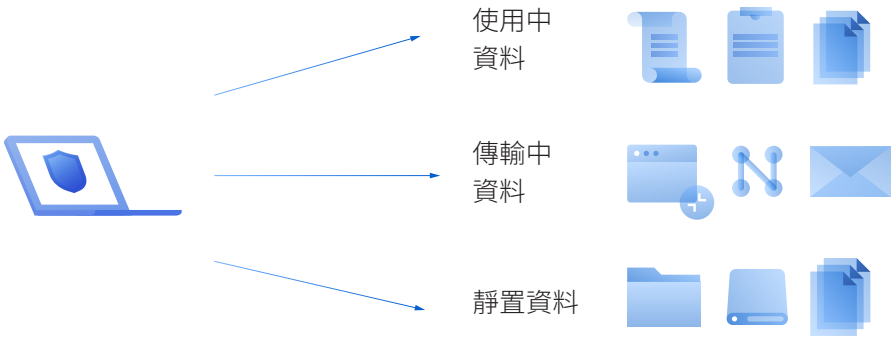
- **內容感知控制 DLP 控制** – 對資料流的更深入控制基於所傳輸的實際資訊 (內容) 的類型和敏感性。

範例：禁止將包含 HIPAA 相關的資訊 (資訊內容) 的文件複製到任何 USB 裝置。

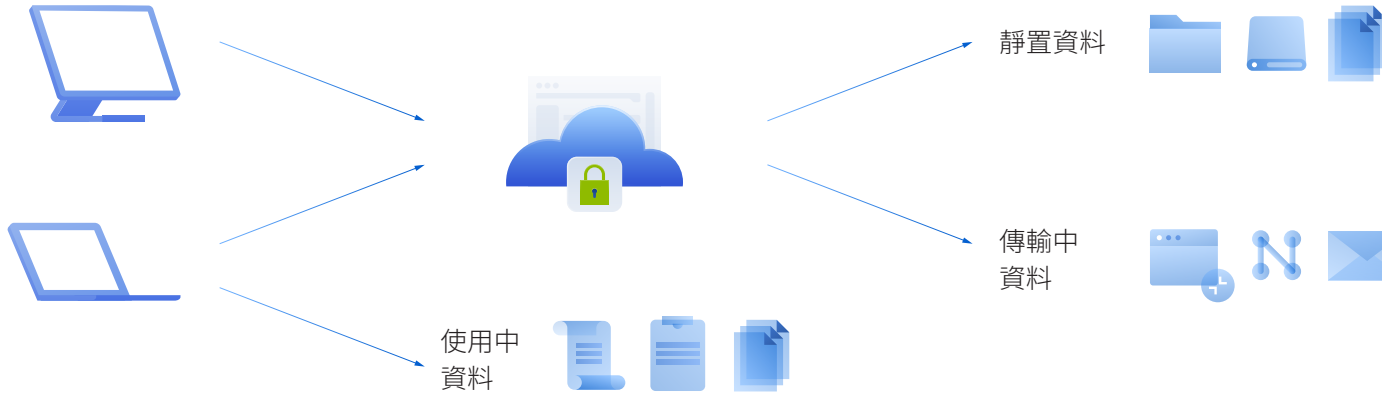
DLP 架構類型

根據 DLP 的部署和運作方式，主要有三種 DLP 類型：

- **端點 DLP** – 這類解決方案會在端點電腦上使用 DLP 代理程式，並防止使用中資料、傳輸中資料及靜置資料從這些電腦洩漏，無論這些電腦是在公司網路內部還是網際網路上使用。



- **網路/雲端 DLP** – 這些解決方案僅使用網路駐留元件，包括可保護公司網路中電腦上的傳輸中資料或靜置資料的硬體/虛擬 DLP 閘道和伺服器，從而防止資料洩漏給未經授權的收件者和公司網路外部的目的地。



- **混合式 DLP** – 此類解決方案利用網路和端點 DLP 元件，來執行端點和網路 DLP 架構的所有功能。

值得記住的是，網路 DLP 由於其架構而無法保護使用中資料，且只能控制向公司網路外部的未經授權者洩漏的資料，而端點和混合式 DLP 可以保護所有狀態下的資料，並防止洩漏給內部和外部的未經授權者。

在本指南中，我們將重點關注基於端點 DLP 架構之 DLP 服務的啟動、執行和擴展。

為何客戶需要 DLP

根據 Ponemon Institute 的《2021 年資料外洩報告》，資料外洩的全球平均總成本為424萬美元，相較於2020年高出10%。如我們所見，資料外洩的成本在攀升，識別和遏制外洩的實際平均時間為287天，這表示您的客戶在外洩得到遏制之前會面臨巨大風險。這些風險可能會導致財務、名譽損失和合規成本。

您能夠使用 DLP 服務來降低客戶風險的主要方式為：

- **協助遵循法規**和保護監管資訊 – PII (GDPR、CCPA)、PHI (HIPAA)、支付卡資訊 (PCI DSS) 等
- **保護客戶的**智慧財產和商業機密
- **將惡意軟體和**社交工程所致攻擊所造成的資料外洩風險降至最低
- **加強遠端工作**和 BYOD 安全性，防止敏感資料傳輸至私有雲端型儲存
- **防止員工**因意外錯誤、疏失、不當行為導致的資料外洩
- **透過對 DLP 事件的持續監視**，實現對資料外洩事件和違規後調查的快速回應

DLP 服務交付流程

在深入瞭解如何啟動、執行和擴展 DLP 服務的細節之前，首先要注意的是由於其他詳細規格，DLP 服務具有具體的交付流程，其中包括下列步驟：

- **部署 DLP 代理程式：** 決定應該佈建 DLP 服務的端點 (旨在確保對公司資料的徹底防護) 並在這些端點上部署 DLP 代理程式是服務交付程序的第一步。請記住，建議對建立、儲存或使用敏感資料的所有工作負載佈建 DLP 代理程式。如果此類工作負載仍不受保護，則會在公司 IT 安全性系統中造成潛在的資料外洩漏洞。

- **建立 DLP 原則：**另一個初始步驟是建立可確保正確資料使用和處理原則以防止資料外洩的 DLP 原則。請記住，根據所使用的 DLP 技術，此步驟可以在部署之前。**需要注意的是**，DLP 原則並非通用，它們始終是客戶特定的，因為不同的組織有不同的內部程序，隸屬不同的法規，並且具有不同的資料存取和共用需求。由於建立 DLP 原則的這些具體情況，需要手動管理原則的傳統 DLP 解決方案給服務供應商建置 DLP 服務帶來相當大的複雜性和成本障礙。
- **驗證 DLP 原則**：建立初始 DLP 原則後的一個重要步驟是和客戶一起進行驗證，以確保這些原則符合業務需求，因為 MSP 無法獲得對每位客戶業務細節的深入瞭解。原則的視覺表現愈複雜和「具技術性」，客戶驗證它所需的時間和專業知識愈多。
- **強制執行和管理 DLP 原則：**客戶對 DLP 原則進行驗證後，即可強制執行這些原則，以開始保護敏感業務資料免遭外洩。請記住，DLP 技術會控制組織的敏感資料流，從而阻止任何未經授權者。然而，隨著業務的不斷發展，引入了新的程序，出現新的資料法規，舊的可能會有所變化。因此，必須根據不斷變化的業務需求持續調整初始 DLP 原則，以確保不攔截新的基本資料流，同時防止所有資料外洩企圖。這可以透過手動原則微調或適應性原則調整的自動方法來達成。
- **報告 DLP 服務價值：**持續報告攔截的敏感資料傳輸和與 DLP 相關的終端使用者動作以展示 DLP 服務的價值，有助於提升客戶留存率和向未意識到其資料外洩問題的客戶說明風險降低。

MSP 對目前 DLP 解決方案面臨的挑戰

DLP 是一個成熟的、以企業為中心的市場，擁有建立長久關係的參與者，但由於需要持續深入地瞭解和將業務細節對應至 DLP 控制、知道法規要求及熟悉運作此類技術所需的資料合規性，所以一直難以被更廣泛的市場 (如服務供應商和其 SMB 客戶) 採用。這導致 DLP 產業主要集中於能夠承擔 DLP 管理專用的昂貴內部專業技能的大型組織。

MSP 在實作和執行 DLP 服務時面臨的主要挑戰為：

- **執行 DLP 服務昂貴且複雜** – 由於傳統 DLP 解決方案需要複雜的手動程序來建立初始原則和後續調整，因此在客戶間實作高效 DLP 所需的時間和和精力使服務成本過高。此外，這種複雜性需要僱用 DLP 專家，這項工作比僱用一般 IT 安全專家更困難，也更為昂貴。

- **高效 DLP 需要客戶特定的原則** -如上所述，任何組織的業務流程和資料敏感性都是獨一無二的且不斷變化，這就需要不斷調整 DLP 原則以適應業務細節。但是，MSP 缺乏且無法獲得並持續保持對每位客戶業務流程的深入瞭解。這成為一個障礙，對採用傳統 DLP 技術的 MSP 構成重大的可擴展性挑戰。
- **設定錯誤的 DLP 原則會中斷業務續航力** - 一方面，由於複雜性和精細度，手動建立和設定 DLP 原則很容易出錯。另一方面，DLP 技術會攔截任何未經授權的資料流。如果 DLP 原則設定錯誤或新的業務流程未一致地對應至這些原則，則這種複雜性和 DLP 預防功能的融合可能會錯誤地攔截業務所需的資料流，從而破壞基本業務流程。
- **員工是客戶最薄弱的環節** - 無論 MSP 及其客戶多難存取 DLP 技術，人為錯誤和針對員工的攻擊都是造成資料外洩的主要原因。即使服務供應商能夠透過其他端點防護層來限制外部威脅的風險，但如果使用者在不知情的情況下釋放敏感資料而導致資料外洩，他們也要承擔責任。
- **客戶可能並不知道資料外洩問題** - 由於以往客戶難以接近 DLP，可能並不一定知道資料外洩問題。推出 DLP 服務意味著服務供應商還需要向客戶介紹他們所面臨的資料外洩風險，以及 DLP 是唯一能夠化解對任何規模組織構成重大威脅之風險的技術。

市面上的最新趨勢和技術 (自動行為式 DLP 原則建立、延伸和監控) 正在應對快速變化的 DLP 原則的挑戰，以適當不斷演進的業務程序以及法規要求。這些新功能有力地讓 DLP 市場大眾化，使其可供服務供應商和其客戶使用。現在是考慮透過 DLP 服務擴展產品組合的大好時機。

規劃和啟動 DLP 服務

規劃和啟動 DLP 服務的第一步是確認您的客戶是否確實需要 DLP。

如果客戶佔有下列部分或全部指標，則需要 DLP 服務來降低其資料外洩風險：

- 使用受法規管制的資料建立、儲存或處理其工作負載
- 有商業機密或智慧財產需要保護以防洩漏
- 在受嚴格監管的產業中營運
- 曾遭資料外洩，希望保護其環境安全並降低風險
- 擁有/需要合規性認證
- 正要支付/考慮網路保險以減少其責任
- 缺少專門的安全人員或專業知識

此外，以往下列產業的客戶會對 DLP 表現出更大興趣：

- 銀行和金融服務
- 醫療保健
- 法律
- IT 和電信
- 政府和公共部門
- 製造
- 零售和物流
- 教育
- 能量學

如果您的客戶顯示出這些指標或在上述產業中營運，那麼現在正是考慮將 DLP 新增到您的服務產品的大好機會，以滿足他們在降低資料外洩和加強法規合規性方面迅速增長的需求。

規則服務和成本估算

決定服務價格的三個主要因素是人力成本、產品成本和期望的利潤。以下是每種因素影響報價的方式：

- **人力成本：**所選解決方案的複雜性將決定服務技術人員在佈建和管理服務上所花費的時間，以及他們所需的 IT 安全專業知識水平。
- **產品成本：**DLP 以往被大型企業採用，成本較高，使中小型企業負擔不起。如果您的客戶主要是 SMB，則需要選擇一種不會使服務成本過高的解決方案。
- **期望的利潤：**在經常性收益模式下銷售的遠端交付服務，MSP 帶來的平均毛利高達 50%。

透過 Acronis Advanced DLP 套件執行 DLP 服務

Acronis 提供了可自動建立和持續維護客戶特定原則一致性的行為式DLP，無需數個月的部署，維護團隊或隱私法博士學位即可瞭解。

使用 Acronis Advanced DLP 套件，您可以為客戶提供全方位 DLP 防護，以前所未見的簡單性保護傳輸中資料和使用中資料，讓您能夠：

- **解鎖新的獲利商機**，方式是擴展產品組合，藉由先前僅對企業提供的 DLP 服務來吸引更多客戶，從而增加每位客戶的收入。
- **最大限度地減少工作**，可將 DLP 輕鬆新增至您的實務，無需增加管理複雜性、成本和員工人數。
- **減輕客戶安全性風險**，方式是防止敏感資料外洩。
- **強化客戶的法規遵循**，藉由使用通用法規架構 (包括 GDPR、HIPAA 和 PCI DSS) 的現成資料分類範本實現。
- **簡化服務佈建和管理**，方式是自動化 DLP 服務佈建、初始原則設定以及後續調整。
- **確保客戶特定的 DLP 原則在任何範圍內有效**，方式是將 DLP 原則與不斷變化的業務細節和行為式技術自動調整，從而確保在實施之前與客戶進行簡單的原則驗證。
- **更快對 DLP 事件做出回應**並簡化 DLP 服務作業、原則維護、IT 安全性稽核、事件調查，這一切透過集中式原則型稽核記錄和安全性警示實現。