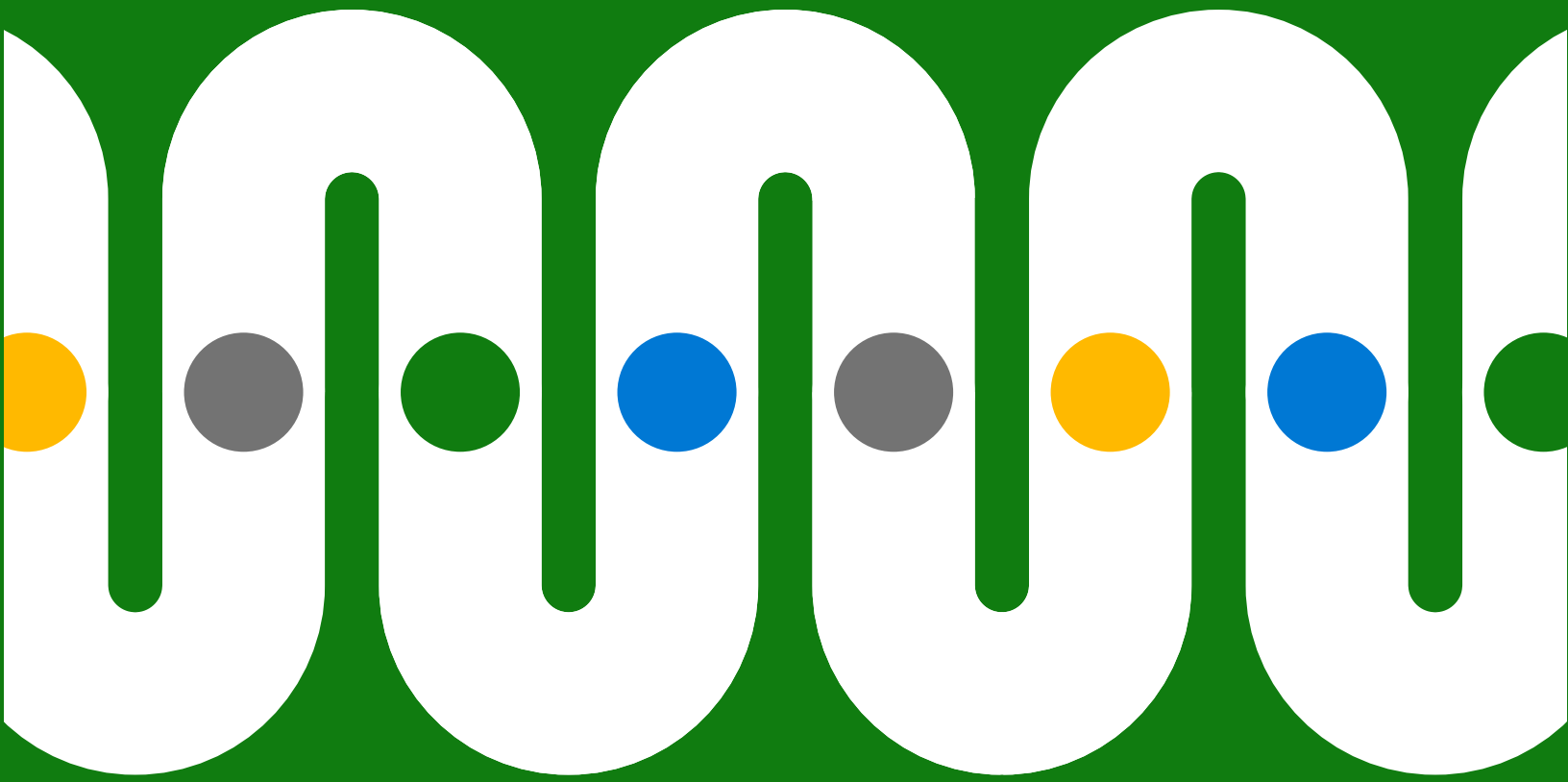
Microsoft Security

端對端保護資料的 3 個步驟



目錄

針對合規性決策者所進行的調查指出，有 95% 的受訪者對資料保護的難題表示擔憂。[2]

前言

組織的數位足跡已隨著混合式辦公而大幅擴展，遠遠超出了傳統辦公室的界限。

這衍生出更多的資料分散和外流問題，而大量應用程式、裝置和位置的快速成長更讓一切雪上加霜、更加複雜。此外，許多工作者也在尋求更大程度充實感或彈性的過程中切換角色，讓上述挑戰加劇，在不斷增長的資料資產中造成新的盲點。[1]

所有這些因素都讓資訊長和資安長重新思考他們的資訊保護措施。根據對 500 多名美國合規性決策者進行的追蹤調查，我們發現幾乎所有受訪者 (95%) 都對資料保護的難題表示擔憂。[2]

[1] Microsoft 如何協助降低「大洗牌」期間的內部風險（英文），Alym Rayani，Microsoft 安全性。2022 年 2 月 28 日。

[2] 2021 年 9 月對 512 名美國合規性決策者進行的調查（英文），由 Microsoft 委託 Vital Findings 進行。

IT 和安全性團隊正在尋求更好的方法來跨多雲端、混合雲和內部佈署環境管理整個資料生命週期。此端對端方法涉及三個關鍵步驟：

第 1 步：識別資料

確定資料的所在位置、種類以及使用或共用方式

第 2 步：將資料分類

將資料分類並加以標記，以找出適當的原則和降低風險的做法，並加以套用

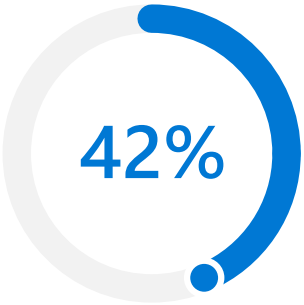
第 3 步：預防資料外洩

採取智慧型偵測和控制，在降低風險及確保員工彈性之間取得平衡

此方式的目標是什麼？弭平缺口並將風險降到最低，而不犧牲生產力。

第 1 步

識別資料



當問及組織有多少資料為「暗資料」時，有 42% 的組織表示至少一半以上。[3]

這種「隱藏」的資料可能會以多種形式存在，像是電子郵件附件、客戶通話記錄、機器記錄和影片片段。

如果您無法識別資料的所在位置、種類以及使用或共用方式，就不可能能夠套用適當的原則或保護措施。

現代組織會持續產生大量的資料。不只文件、電子郵件和訊息，還有安全監控影片到地理定位資料等內容，所有一切再加上內部佈署和雲端中的應用程式、裝置和儲存設備增長，讓局勢更加嚴峻。

要識別所有資料可不是件容易的事，有 42% 的組織表示，他們至少有一半的資料是「暗資料」。[3] 換句話說，這些資料雖然是收集到的資訊，但在業務用途上卻為未知或未使用狀態。有時候，當建立資料的工作者轉換專案或角色後，資料就會變成「暗資料」；甚至在資料建立或修改時，通常也都沒有備妥可識別資料的系統。

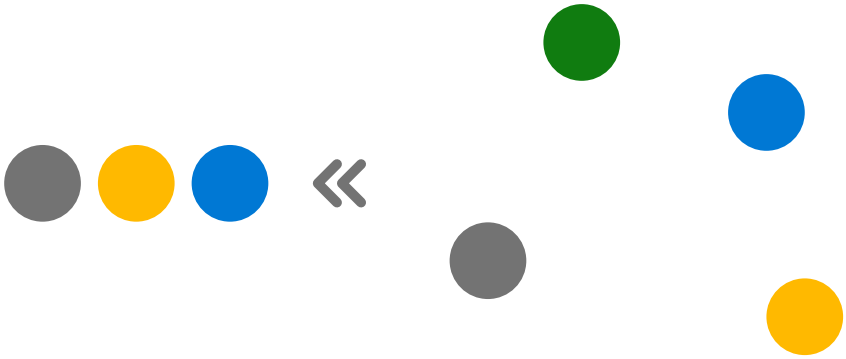
[3] "2022 State of Data Governance and Empowerment Report"，Enterprise Strategy Group。2022 年 7 月。

想要在單一平台上建置端對端探索工作流程嗎？

您可以前往 **Microsoft.com** 了 解 Microsoft Purview 中的資料探索。

這個難題只會日益艱困。到了 2026 年，建立、擷取、複製和取用的新資料數量預計將會超過兩倍以上，且企業資料的增長速度會比消費者資料快兩倍以上。[4]

人工智慧 (AI) 和機器學習 (ML) 在此時便可派上用場，例如辨識敏感性資料 (像是電子郵件地址、健康資料、信用卡號碼或智慧財產權)，並自動加以分類。AI 和 ML 還可以提高分類的準確性，並追溯檢閱資料。這些識別流程可以橫跨您的整個資料資產，無論內容位於任何位置，皆可跨雲端保存、收集、分析、檢閱及匯出內容。



[4] "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth"，John Rydning，IDC。2022 年 5 月。

第 2 步

將資料分類

分類和原則兩者都必須隨著資料移動。

舉例來說，當有員工將信用卡號碼從 Microsoft Word 文件複製到 Excel 時，分類和原則都應該自動套用至這兩個文件。

對資料進行適當分類有助您判斷正確的原則和風險降低措施，確保不同類型的資料不會在未經授權的情況下，意外或無意遭到誤用或存取。加密和浮水印則可進一步保護資料，無論資料狀態是待用、傳輸中或使用中。

然而，當資料在組織內移動時，分類及原則也必須隨之移動。標記和保護原則不能只侷限在離散文件，而必須跨越整個數位資產：包含從內部佈署到雲端式存放庫，以及從軟體即服務 (SaaS) 應用程式到 OS 原生應用程式。

傳統分類方法涉及大量手動工作，進而導致發生錯誤或不小心忽略關鍵資料的風險。內建的分類器可進行訓練，有助於將此流程自動化，而整合式解決方案則可讓系統管理員跨所有系統集中管理這些原則。

想要更有效地管理及保護整個環境中的敏感性資料嗎？

您可以前往 **Microsoft.com** 了解 Microsoft Purview 中的資料分類和保護。

第 3 步

預防資料外洩

DLP 原則可禁止不符合規範的動作。

例如，如果有員工嘗試將含有信用卡號碼的試算表下載至快閃磁碟機，或將其上傳到雲端儲存空間，DLP 原則即可將此活動識別為不符合規範，並加以禁止。

一旦識別資料並加以分類後，資料外洩防護 (DLP) 解決方案即可強制執行端對端保護原則，以降低暗資料和資料外流等威脅，如此一來便可確保在職員工和離職員工不會在未經授權的情況下，有意或無意地共用、公開或傳輸敏感性資料。

智慧型 DLP 解決方案會根據情境，在提供彈性與封鎖高風險動作之間找到平衡。例如，個人可以在收到有關潛在風險和適用原則的提醒之後仍繼續動作。這種做法有助於保護敏感性資料，同時也可訓練使用者更加了解風險。

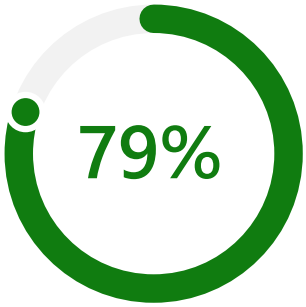
DLP 解決方案有助於保護智慧財產權和其他關鍵業務資料，也有助於提升法規的合規性，例如一般資料保護規定 (GDPR)、健康保險流通與責任法案 (HIPAA) 和加州消費者隱私保護法 (CCPA)。

DLP 的全方位做法會以一致方式在整個組織強制執行原則，並會保護資料生命週期中「最脆弱的環節」部分。

想要對敏感性資訊採取智慧型偵測和控制嗎？

您可以前往 **Microsoft.com** 了解 Microsoft Purview 中的資料外洩防護。

別把資料保護當成附帶機制，而應由內而外構築而起。



針對合規性決策者進行的調查指出，有 79% 的受訪者已購買多種合規性和資料保護產品。

大多數受訪者都購買了三種以上。[5]

許多組織都嘗試過以「附加型」方法來進行資訊保護，使用多種解決方案來管理資料生命週期的離散部分。但這種做法會迫使您的安全性、資料治理、合規性和法務團隊將解決方案拼湊在一起，通常效率不彰且耗損資源。

「內建」方法可以弭平缺口，將資料識別、資料分類和 DLP 結合在一起。有了整合式解決方案後，就能更簡便地集中管理和強制執行原則，並同時縮短使用者的訓練時間，因為使用者可以透過熟悉的方式，在應用程式內原生接收原則通知。

[5] 2022 年 2 月對 200 名美國合規性決策者進行的調查 - (n=100 599-999 名員工，n=100 1000+ 名員工)（英文），由 Microsoft 委託 MDC Research 進行。

內建的整合式解決方案：Microsoft Purview

Microsoft Purview 可提供一套全方位的解決方案，協助您治理、保護及管理整個資料資產，以應對目前因工作場所分散且有大量資料而帶來的挑戰。

超越治理。

了解更多如何使用 Microsoft Purview 來保護您資料的相關資訊 >

對資料保護的特定領域感興趣嗎？深入了解 Microsoft Purview 如何協助您進行：

資料探索 >

資料分類和保護 >

資料外洩防護 >

Microsoft Security