Netskope One 資料外洩防護 (DLP)

資料表

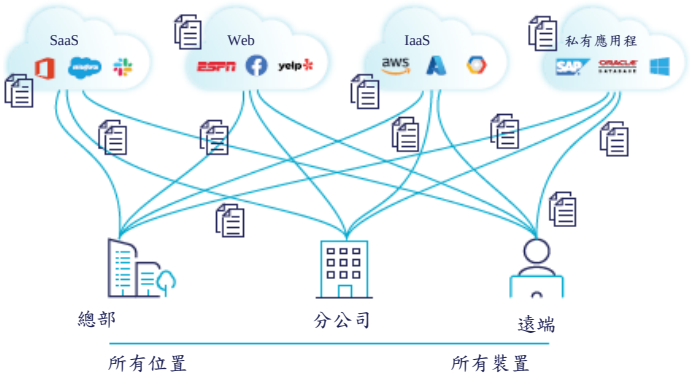
為現代企業提供資料保護

全面且先進的雲端交付 DLP 解決方案保護所有位置的敏感資料，包括雲端、網路、電子郵件服務、端點和使用者。

更新資料保護方法的必要性

保護敏感資料（例如個人可識別資訊 (PII)、商業機密、財務文件及其他智慧財產 (IP)）是現今所有組織的首要之務。現代商業趨勢以前所未有的方式洩露資料：

- **混合工作導致資料超出傳統邊界**，遍及雲端服務，以及使用者要連線的任何位置，包括內部和外部。
- **資料被儲存和分享至越來越多 SaaS 應用程式**，任何使用者和任何裝置都可直接存取。
- **資料數量、種類和速度爆炸性成長。**因此，越來越難識別和保護敏感資料。



傳統的 DLP 解決方案無法適應雲端、混合工作和指數級資料蔓延。它們複雜、受限於地端基礎架構、耗費資源，並採用成本高昂的附加式擴充方法。

由於資料外洩層出不窮、合規性要求（GDPR、PCI、HIPAA、GLBA 等）更加嚴格以及必須節省成本，組織迫切需要新的資料保護方法。組織需要可靠的解決方案以保護敏感資料，無論資料儲存於或流向何處，包括雲端、Web、電子郵件、私有應用程式或裝置。

Netskope One DLP 提供全面的覆蓋範圍、無與倫比的偵測準確度和簡易的管理，適合任何規模的現代組織。

主要效益和能力

全面

實現全面的資料保護範圍：探索、監測和保護所有網路、雲端、端點、電子郵件服務和使用者的敏感資料。

精準

透過機器學習和人工智慧驅動最準確的資料偵測和分類功能，達到最高資料保護效力。

簡易

確保最簡單、最具成本效益的企業 DLP 部署，並利用統一原則和單一管理主控台。

情境和風險感知

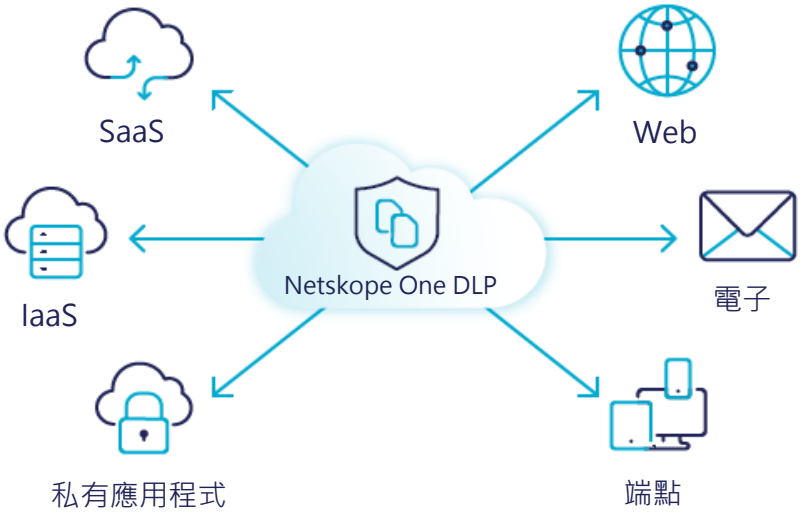
自動適應不斷變化的風險、行為和組織情境，遵循零信任原則妥善保護資料。

「移轉至雲端時，尋找最佳 DLP 解決方案是我們的首要任務。Netskope 在各方面都超乎我們的預期。」

– 資安架構師，Fortune 100 製造業

從雲端將 Netskope 資料保護延伸至各個位置

Netskope One DLP 是業界最全面、最先進的雲端資料外洩防護解決方案，隨時隨地保護雲端、網路、電子郵件服務、端點和使用者的敏感資料。Netskope One DLP 提供零信任資料保護，因為它具備風險感知和情境感知能力，並原生整合於 Netskope 領先市場的安全服務邊緣解決方案中。

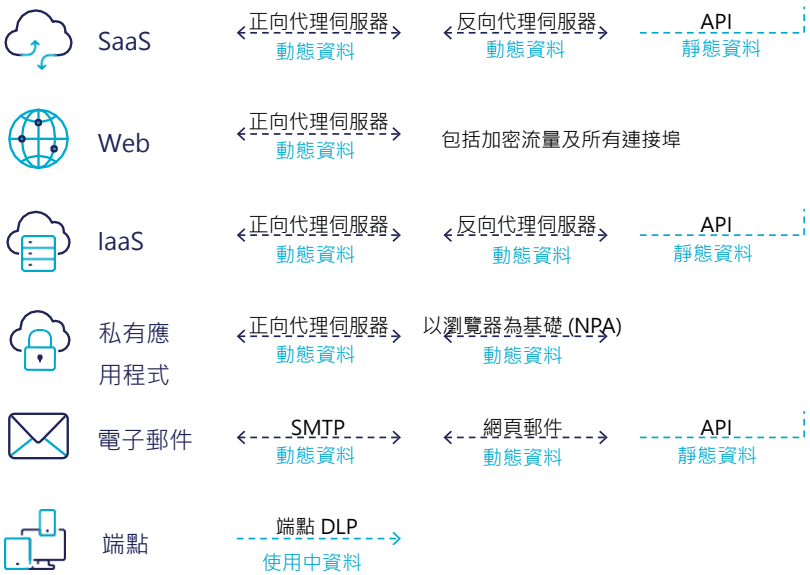


能力

以統一原則全面涵蓋所有關鍵通道

在傳統企業邊界之外四處移動的敏感資料變得更難以追蹤和保護，也更容易被有意或無意洩露。

Netskope One 雲端 DLP 持續探索、監測和保護 SaaS 應用程式、IaaS、企業網路和分公司、行動工作者、電子郵件服務以及員工端點上的動態、靜態和使用中敏感資料。它為所有儲存、使用或從集中式雲端服務傳輸和交付資料的位置提供統一的資料保護原則。單一主控台採用以角色為基礎的存取控制，確保所有通道的原則配置、監測、報告和事件應變全都由從業人員透過單一窗格管理。



以無與倫比的準確度偵測和分類所有敏感資料

資料量持續增加，且變得比以往更加多樣化。Netskope One DLP 以最低錯誤率準確、可靠地偵測和分類任何形式的所有敏感資料，將誤報和違規分類疲勞最小化。這是透過多種偵測技術和先進的分類演算法自動完成。

1. 描述內容比對使用 3,000 多個預先定義的資料識別碼和針對 133 個國家的個人識別碼，包括正規表示式 (regex)、姓名、數字、財務資料、醫療資料、生物資料、不當用語和產業相關資訊，以及在地化語言和完全可自訂識別碼。也可以組合資料識別碼，並透過鄰近關鍵字、表示式、布林邏輯、嚴重性等級、閾值和鄰近範圍對規則進行精細自訂和微調。解決方案包含各種預先定義的資料設定檔，支援多種使用案例與合規性要求，例如 GDPR、CCPA、PCI-DSS、HIPAA 和 GLBA。

2. 精確資料比對 (EDM) 用來對實際資料集（例如客戶清單、財務資料、合約等）和範本進行指紋辨識。這是幾乎萬無一失的方法，可偵測來自結構化資料來源的特定資訊，例如個人的全名、社會安全號碼、地址、身分證字號、信用卡號碼和銀行帳戶。Netskope One DLP 可對超過二十億筆紀錄及其多種組合進行指紋辨識。隨後會在雲端儲存庫以及任何將發生資料流動的位置自動探索和保護這些已建立索引的資訊。

3. 在現今的世界，使用者可輕鬆拍攝文件、表單、證件、白板的照片，甚至照片的照片。光學字元辨識 (OCR) 是整體資料保護策略的重要部分。透過 OCR，Netskope One DLP 可從圖片和 PDF 文件中擷取文字資訊，隨後根據分類演算法和建立的偵測原則自動尋找敏感資料。

4. 手動定義的規則是資料偵測的基礎，但自動化引擎提供寶貴的輔助，使敏感資料偵測變得非常準確。Netskope One DLP 提供以人工智慧 (AI) 和機器學習 (ML) 為基礎的影像分類，以獨特能力辨識敏感檔案和文件類型而不必擷取此類資產包含的內容，即使影像和文件部分毀損、有皺摺、模糊且整體清晰度不佳也不成問題。內建的 ML 分類器可偵測信用卡、履歷、專利、M&A 文件、螢幕截圖、護照、照片證件、稅務表單、醫療卡、原始碼等。Netskope One DLP 也提供建立自訂 ML 分類器的功能。

5. 就某些任務關鍵性文件和高度機密的檔案而言，必須不惜代價防止全部或部分外洩以及複製。檔案和文件指紋辨識可為整份文件建立索引，隨後如果在不同環境和傳輸通道中發現其中包含的資訊，即可偵測完全相同或具有一定相似度的部分內容。

6. Netskope One DLP 可掃描超過 2,000 種不同的檔案類型，例如文字格式、簡報、電子郵件、圖片、試算表、設計、通訊、資料庫、封存檔、壓縮檔等類型。偵測以真實檔案類型為根據，以防止混淆和試圖規避偵測，並包含以裝置、應用程式、位置、使用者活動等為根據的組織情境感知。

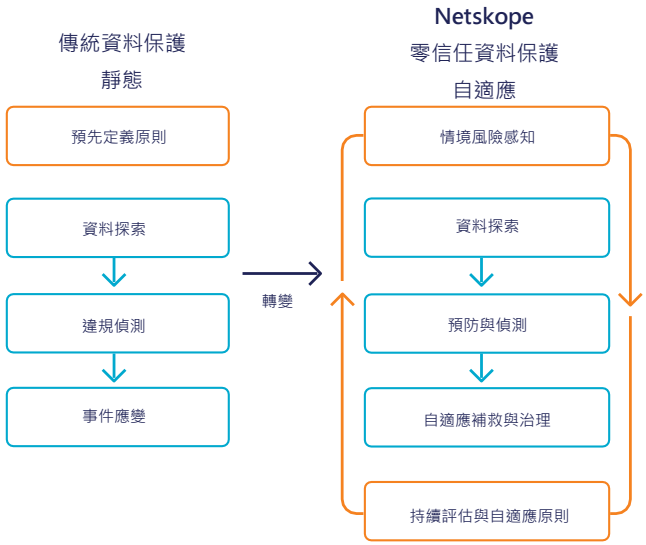
7. Netskope One DLP 與第三方資料分類技術整合。除了內容掃描之外，也能讀取中繼資料和標籤，將保護原則延伸至被商務使用者標記為敏感的資料。

整合式風險感知資料保護

誤報、事件應變疲勞和業務中斷是與傳統 DLP 解決方案相關的問題。是時候該讓 DLP 從由固定原則構成的靜態保護模型轉變為動態自適應零信任方法。Netskope One DLP 是唯一超越單純探索敏感資訊和應對預先定義違規的解決方案，將組織情境和安全風險納入考量，以根據不斷變化的條件自動動態啟用適當的保護。

Netskope One DLP 原生內建於 Netskope 的智慧安全服務邊緣 (SSE) 解決方案，後者將 SWG、CASB、ZTNA、UEBA 等基本安全服務整合在 Netskope One 平台的完全融合單一介面中。此方法消除安全盲點、確保原則一致性，並大幅降低成本和複雜性。

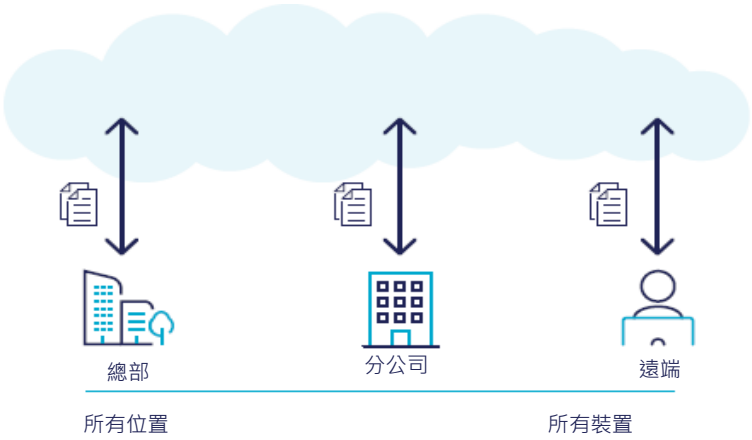
平台持續感知使用者行為、地理位置、安全態勢、裝置風險、應用程式風險和信譽、個人應用程式執行個體等，並允許 DLP 針對真實的資料安全事件調整事件應變，將誤報、事件分類和業務中斷最小化。



Web

為所有網路和隨處工作提供 Web 資料保護

現今的企業通訊透過比以往更多樣化的網路連線有效地進行。事實上，在混合工作模式下，除了企業網路之外，使用者從遠端位置存取網路時也會洩露敏感資料。此外，企業資料可能被受管理和未受管理端點存取、上傳和下載，而 Netskope One DLP 可確保敏感資料不會透過不受信任的高風險 Web 流量（包括加密流量）外洩。



可偵測、監控和保護敏感的企業資料，防止資料透過各種網路連線外洩和暴露，包括居家辦公室、公用 Wi-Fi 地點和蜂巢式網路，以及公司園區網路、資料中心和分公司。它可掃描所有企業 HTTP 和 HTTPS Web 流量、識別內嵌敏感資訊，以及選擇性移除敏感的 HTML 內容或封鎖要求。Netskope 針對 Web、應用程式和非 Web 流量有效提供保護與存取控制，此外，也確保持續驗證從未受管理裝置對企業資產的存取並根據原則掃描其流量，同時正確驗證遠端使用者。也可防止資料外洩至未受管理或個人裝置，並在使用者進行高風險活動時根據安全性原則予以提醒和指導。DLP 以雲端為基礎並與 Netskope SWG 原生整合，不需要 ICAP、SPAN、額外的地端基礎架構、網路配置和流量引導。

保護	動態資料
模式	以用戶端為基礎、顯式代理伺服器、代理伺服器鏈接
類別	120+
連接埠	所有連接埠
原則操作	警報、允許、繞過、封鎖、轉送、指導等
管理	統一主控台、原則和事件管理，涵蓋整個 DLP 平台

SaaS

跨 SaaS 應用程式保護雲端資料

軟體即服務 (SaaS) 應用程式是現今的企業賦能工具，讓所有員工無論在何處工作都能輕鬆連線，並且方便地存取資料。但便利性伴隨著風險，因為資料暴露於新型雲端威脅、過度分享權限，可能透過數千個未經授權的應用程式傳輸，甚至被上傳至企業 SaaS 應用程式的個人執行個體。根據 Netskope 2022 年雲端和威脅報告，83% 的使用者在受管理裝置上使用個人應用程式執行個體，平均每月進行 20 次檔案上傳。

全面性 Netskope One DLP 是 Netskope 多模式雲端存取安全代理 (CASB) 的核心功能，將資料保護原則無縫延伸至 SaaS 應用程式，包括內嵌以及透過 API。此解決方案可探索、監測和保護企業授權 SaaS 應用程式（例如 Microsoft 365、Salesforce、Google Workspace 和 Slack）的動態和靜態敏感資料。此外，也可探索並保護超過 100,000 個 SaaS 應用程式的動態敏感資料，包括傳輸至個人應用程式執行個體（例如從企業 OneDrive 到個人 OneDrive）和高風險應用程式的資料。探索的敏感資訊涵蓋 1,900 多種檔案類型，包含在 Slack、Teams、Zoom 等協作應用程式的貼文和非同步通訊以及電子郵件中。

此解決方案利用情境和風險感知，根據可能隨時間變化的條件（例如透過 Cloud Confidence Index (CCI) 確定的應用程式風險評分、安全態勢、使用者行為、地理位置等）採取適當的保護措施以保護敏感資料。保護措施包括取消檔案共用、隔離檔案、阻止檔案離開應用程式、對使用者發出違規警報，以及對與外部共用的資料套用強加密或數位版權管理。Netskope 也透過原生控制措施（例如 SaaS 安全態勢管理、威脅預防和行為分析）降低資料遺失的風險。

保護	動態和靜態資料
模式	多模式：內嵌和以 API 為基礎
類別	經授權和未經授權的 SaaS 應用程式，以及 IaaS
原則操作	警報、封鎖、變更所有權、限制存取、加密、刪除、隔離、法律保留、限制共用、資料分類、停用列印和下載、IRM 保護、指導等
管理	統一主控台和原則，涵蓋整個 DLP 平台

IaaS

保護 IaaS/PaaS 公用雲端資料

由於收集和處理的資料量增加，加上在雲端執行資料密集型應用程式的便利性，現代組織普遍採用基礎架構即服務 (IaaS) 資料儲存。企業資料的雲端原生服務具有高擴充性、可用性和耐久性，但若未受到妥善保護和監測，可能會以新的方式暴露敏感資料，超出資安團隊的管轄和控制範圍。

Netskope One DLP 將探索、監測和保護延伸至在公用雲端服務（包括 Amazon S3 儲存貯體、Azure Blob 和 Google Cloud Storage）中儲存和共用的敏感資料。領先業界且經過機器學習強化的分類功能可準確辨識敏感資料，例如 PII、原始碼和存取金鑰。在公用雲端服務中一致執行資料保護、合規性和資料隱私原則，並在整個 Netskope One DLP 平台（包括 SaaS 應用程式、網路、電子郵件和使用者端點）上自動同步。

Netskope 統一 DLP 解決方案以服務形式整合於 Netskope 公用雲端安全平台中，以提供資料保護、威脅預防、雲端安全態勢管理和行為分析，建立統一的安全策略。

保護	動態和靜態資料
模式	內嵌和儲存空間掃描
雲端覆蓋範圍	Amazon Web Services、Microsoft Azure、Google Cloud Platform
原則操作	警報、允許、繞過、封鎖、轉送、指導等
管理	統一主控台和原則，涵蓋整個 DLP 平台

端點

端點資料外洩防護

端點裝置是使用者存取企業資源和連接網路的途徑。尤其是現在，可攜式運算裝置使隨處工作成為可能。基本上，端點可讓使用者完成工作，包括建立敏感的企業資料並與他人共用。因此，端點也成為重大資料外洩的管道，通常是惡意使用者行為所導致。

Netskope 端點 DLP 可偵測、監控並保護員工端點上的使用中敏感資料以防止資料遺失和遭竊，無論裝置處於上線或離線狀態，也無論裝置位於何處。Netskope 端點 DLP 整合於單一 Netskope 用戶端中，不必部署額外的代理程式。有別於傳統解決方案，Netskope 端點 DLP 將資源利用最小化，同時具備全套功能，包括以 ML 為基礎的分類器、OCR、檔案指紋辨識、EDM 等。事實上，它利用雲端 DLP 服務，包括來自整個 DLP 平台的情報，以避免在資料源自雲端的情況下重複掃描。此方法造就無摩擦使用者體驗和更強的保護效果。端點 DLP 可讓您：

- 利用 Netskope 的全套 DLP 功能，包括 ML 分類器、資料指紋辨識和 OCR。
- 執行 DLP 檢查，以偵測並防止透過 USB、印表機或藍牙進行敏感資料傳輸。
- 啟用 USB 裝置和印表機保護，以防止未經授權使用。
- 配置裝置控制原則，管理 USB 大量儲存裝置、印表機、藍牙和網路共用在端點上的運作方式。
- 將在 Netskope One DLP 平台中的其他位置使用的預先定義和自訂設定檔無縫延伸至與端點相關的內容檢查。
- 根據歷史掃描，利用現有掃描結果涵蓋所有控制點，例如內嵌和雲端應用程式。
- 使用新的檔案來源功能，在檔案源自特定企業雲端應用程式（例如 Salesforce、OneDrive、GDrive 及其他 SaaS 應用程式）的情況下自動保護端點上的使用中檔案。
- 透過使用者和使用者群組定義實現精細原則控制。
- 解讀使用 Azure 資訊保護套用至敏感資料的分類標籤。
- 利用裝置分類狀態判斷裝置處於受管理或未受管理狀態。

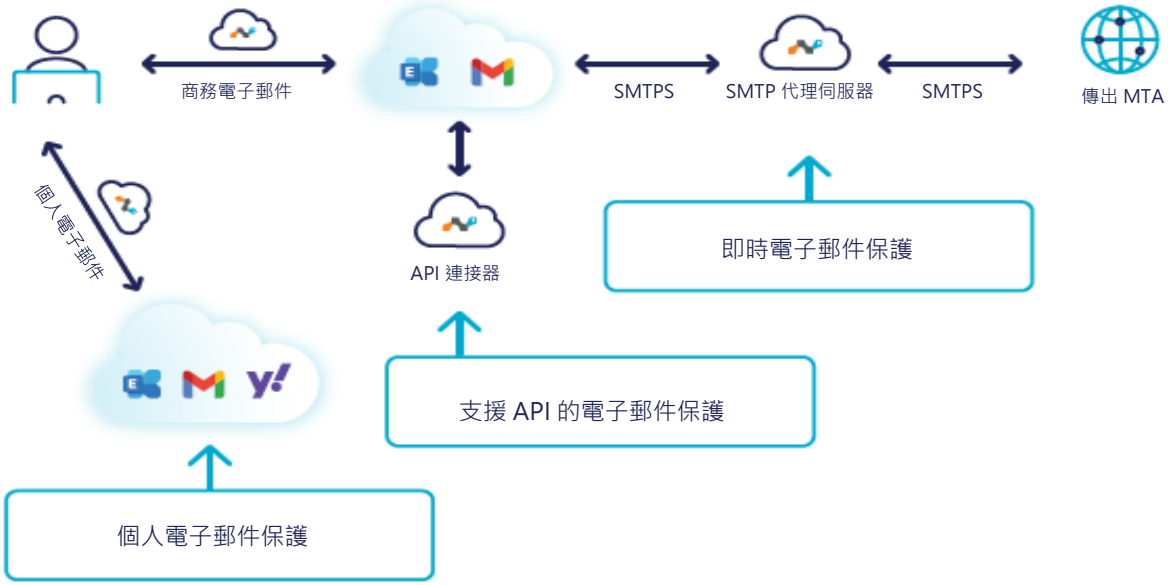
裝置	USB 儲存裝置、區域網路印表機、藍牙和網路儲存
保護	使用中資料
代理程式	Netskope Client 單一代理程式的一部分
原則操作	允許、封鎖、警報、使用者警報（指導）
OS 支援	Windows 10 x64、Windows 11 x64、macOS 支援（Ventura、Sonoma 和 Sequoia）
管理	統一主控台和原則，涵蓋整個 DLP 平台

電子郵件

電子郵件資料保護

由於現在的商務使用者不再定期進辦公室，透過電子郵件和協作應用程式進行的虛擬通訊將增加。電子郵件在組織內部和外部被使用，仍然是與客戶、合作夥伴及員工溝通的主要方式。

Netskope 為電子郵件（例如 Microsoft 365、Gmail、地端）提供全面的 DLP 解決方案，涵蓋動態和靜態資料。解決方案包含：



- 針對透過企業電子郵件帳戶經由 SMTP 代理伺服器和網頁郵件傳出的敏感電子郵件提供內嵌即時電子郵件保護。
- 以內嵌模式監測並防止敏感資料透過個人帳戶（例如企業 Gmail 與個人 Gmail）或私人電子郵件服務（例如 Yahoo）外洩。
- 支援 API 的電子郵件保護，偵測並回應透過企業電子郵件服務傳送的敏感電子郵件。
- 支援所有電子郵件部署，包括雲端電子郵件服務、網頁郵件和地端郵件傳輸代理程式 (MTA)。
- 以相同的 DLP 規則掃描附件、內文、主旨和標題。
- 全套偵測功能，包括檔案指紋辨識、EDM、OCR 和以 ML 為基礎的分類。
- 將 DLP 僅限於特定群組、使用者，或延伸至所有使用者。

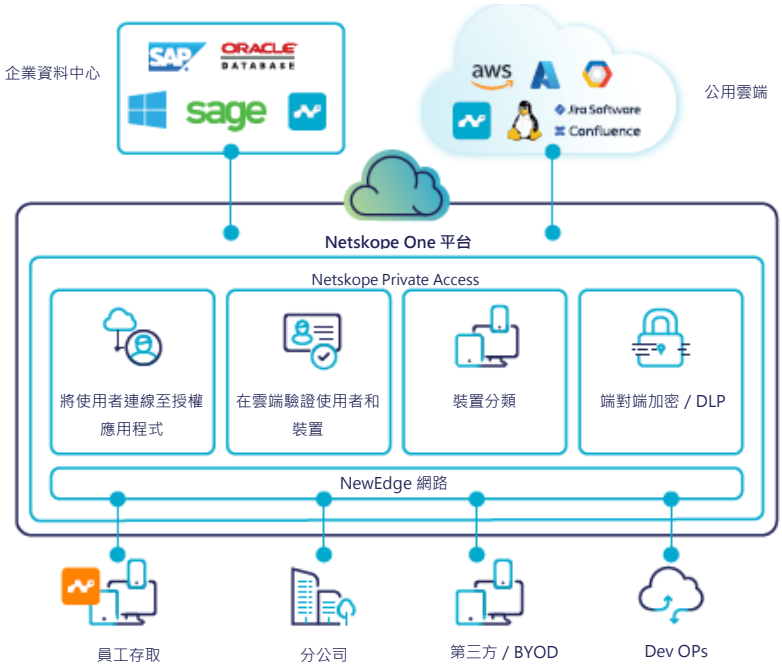
Netskope 的單通道 DLP 方法直接將統一 DLP 原則延伸至電子郵件流量，並在單一 DLP 主控台下為整個解決方案傳達原則定義、事件管理和報告。

保護	動態和靜態資料
模式	多模式：內嵌和以 API 為基礎
覆蓋範圍	經授權和未經授權的電子郵件服務
原則操作	警報、封鎖、限制存取、加密、刪除、隔離、法律保留、限制共用、資料分類、停用列印和下載、IRM 保護、指導等

私有應用程式

保護在私有應用程式上存取的資料

託管於資料中心和公用雲端環境的私有資源承載敏感資料，對企業而言極為重要。無論使用者從何處連線，都必須確保安全地存取私有應用程式，以及監測敏感資料移動，並防止資料外洩。



透過 Netskope Private Access (NPA) 遠端存取解決方案提供 Netskope One DLP，以防止資料中心和公用雲端環境中的私有資源內的資料遺失和外洩。Netskope One DLP 與 NPA 可檢查 HTTP 和加密流量，並自動探索、監測和保護動態敏感資料，在使用者從任何位置透過瀏覽器存取私有應用程式時提供資料保護。此解決方案也以零信任網路存取 (ZTNA) 原則為基礎，將位於任何位置的使用者連線至私有資源，提供驗證和安全存取。

保護	動態資料
模式	內嵌
存取方法	瀏覽器
原則操作	允許、封鎖等
管理	統一主控台和原則，涵蓋整個 DLP 平台

立即使用 Netskope One DLP 保護敏感資料

92%

的 IT 組織表示，與過去使用的解決方案相比，
Netskope 改善其資料保護

欲深入瞭解，請造訪 https://www.netskope.com/products/data-loss-prevention