

SYMANTEC

by Broadcom

企業資料外洩防護(Enterprise DLP)

在雲端與 AI 時代，保護您最寶貴的資產

高階主管專屬手冊

董事長 | 總經理 | 資訊安全長(CISO)

資訊安全維運經理與工程師 | 財務長(CFO)

Broadcom Inc.

2026 年 7 月

目錄

摘要.....	3
策略當務之急：董事長與總經理.....	3
財務論證：財務長.....	4
建構可禁得起檢驗的資安架構：資訊安全長.....	5
運作高效能專案：資安維運經理.....	6
深入探討偵測與部署：資安維運工程師.....	7
涵蓋所有通訊管道的全方位保護.....	9
資料保護實務：常見使用案例.....	9
產品組合：DLP Core 與 DLP Cloud	10
擴充平台功能：DSPM、進階威脅防護及其他	12
符合全球法規遵循與監管要求.....	12
確保 AI 時代之安全	13
部署彈性與系統需求.....	14
常見問題.....	14
為何選擇 Symantec DLP：真正重要的差異化優勢	15
實務部署路徑.....	16
產業別考量.....	17
附錄 A：端點與儲存庫涵蓋範圍詳情.....	18
附錄 B：關鍵術語詞彙表.....	19
關於 Broadcom 旗下之 Symantec 資料外洩防護	19
立即開始保護您的資訊.....	20

摘要

資料已成為現代企業最寶貴、同時也是最容易外洩的資產。它存在於員工攜帶穿越機場的筆記型電腦中、公司防火牆後方的資料庫中、與承包商共用的 SharePoint 網站中、Office 365 信箱中、Box 與 Google Workspace 資料夾中，並且日益出現於員工輸入至 ChatGPT 等生成式 AI 工具的提示詞（Prompt）當中。上述每一個接觸點，都可能成為攸關企業競爭地位之智慧財產、受監管記錄及策略規劃外洩的出口。

Broadcom 旗下之 Symantec 資料外洩防護 (Data Loss Prevention, DLP)，正是為了在不拖累業務運作的前提下，弭平此一風險缺口而生。它是一套單一整合平台，能夠探索機敏資料所在位置、監控其移動方式，並防止其遺失、遭竊或外洩——涵蓋端點、網路、儲存庫及雲端應用程式，全數由單一政策引擎與單一管理主控台統一治理。

本手冊係為肩負此一決策重任之各方人士所撰寫：必須守護企業價值與品牌聲譽的董事長與總經理；必須以資料外洩成本為依據、為投資提出正當理由的財務長；必須建構可禁得起檢驗之資安態勢的資訊安全長；必須以低誤報、高效率方式運作事件應變專案的資訊安全維運經理；以及必須精準實施並調校偵測機制的資安維運工程師。以下各節將分別直接回應該等角色最可能提出之問題，而底層平台則始終如一：單一DLP引擎，部署於資料所至之每一處。

訊息很單純：Symantec DLP 不會要求您在防護與生產力、地端掌控與雲端靈活性、或昨日的法規遵循要求與明日的AI驅動風險之間做出取舍。它透過單一整合介面，為您同時提供這一切，並以數十年來在資料保護領域的市場領導地位為後盾。

策略當務之急：致董事長與總經理

對於位居組織最高層的領導者而言，資料外洩鮮少被視為技術問題，而是被視為一則新聞頭條、一封股東質詢函、一封監管機關來函，或是一位不再信任貴公司保管其資訊的客戶。一次嚴重的資料外洩事件，足以抹煞多年累積的品牌價值、觸發契約違約罰則、招致訴訟，並在受監管產業中，危及營運執照。董事會無須理解「描述內容比對」或「索引文件比對」等技術細節，也能切身感受資料外洩所造成的後果；他們需要的，是對組織就「這種事有可能發生在我們身上嗎？」這個問題，具備可信賴、企業等級答案的信心。

三股力量正在匯聚，使這個問題比兩年前更加迫切。首先，企業邊界已實質上瓦解。員工在家中、機場及客戶所在地辦公，使用筆記型電腦、行動裝置，以及一份日益增長、且 IT 部門未必正式核准的雲端應用程式清單。其次，生成式 AI 已成為日常工作的一部分。員工基於提升生產力之名，將合約、原始程式碼、財務模型及客戶記錄貼入公開的AI工具，往往完全未受資安團隊掌握。第三，監管要求持續擴大——新的隱私法規、新的產業別要求，以及不僅要「宣稱」、更須「證明」機敏資料已受保護之新義務。

Symantec DLP以單一、連貫的策略，同時因應此三股力量，而非仰賴零散拼湊的單點工具。它為組織提供一套政策，可隨資料移動至任何地方而如影隨形：筆記型電腦、公司網路、檔案共用區與資料庫，以及包括員工已在使用之生成式 AI 平台在內的已核准與未核准雲端應用程式。這種一致性，對領導階層而言意義重大，因為它能將一項龐雜難以治理的風險，轉化為單一專案——具備單一負責人、單一主控台，以及單一、可供彙報之指標體系。

對董事長或總經理而言，此項投資的價值，最適合以「從未登上新聞版面的事件」來衡量：從未外洩給競爭對手的合約、從未出現在黑市待售的客戶資料庫、從未隨離職員工一同流失的商業機密、未發現任何缺失即順利結案的法規稽核。Symantec DLP 正是讓這些「未發生的事件」成為常態的基礎建設，同時讓企業得以持續使用驅動其生產力的雲端應用程式、AI 工具及遠距辦公模式。保護組織最機敏的資訊，並非對成長的限制；若處理得當，反而是成長的助力之一，因為客戶、合作夥伴及監管機關，都會對能夠證明自身認真看待資料治理的組織給予正面評價。

歸根究柢，這既是一項技術決策，同時也是一項治理決策。核准建置企業級DLP專案，等同向市場、稽核人員及貴公司員工傳遞明確訊息：資料保護是董事會層級的優先要務，並由一套經過驗證的平台做為後盾，而非長期以來東拼西湊、彼此獨立的工具集合。

財務論證：致財務長

每一項資安投資，都必須與具有更明確、更立即營收效益的方案相互競爭資本。若要以財務語言為 Symantec DLP 之投資提出論證，將討論拆解為財務長自然會提出的三個問題會有所助益：不採取行動的代價為何、此平台的持有成本為何，以及其總持有成本與拼湊多套單點產品之替代方案相比，情況如何。

不採取行動的代價為何？資料外洩事件所付出之代價，遠遠超出事件本身：鑑識調查、法律顧問費用、監管罰款、客戶通知作業、受影響個人之信用監控服務、來自合作夥伴之違約罰則、網路保險保費上升，以及往後數年間，透過客戶流失與商機流失緩慢顯現之聲譽損害成本。上述多數成本，皆是資料原本就不應外流之直接後果——郵件誤寄至錯誤信箱、資料庫匯出至未經核准之雲端硬碟、機密文件貼入公開 AI 工具。DLP 正是專為防範此類情境而設計，因此其投資報酬，最適合以「降低大規模、未編列預算損失之發生機率與嚴重程度」來評估，而非單純以生產力提升衡量。

此平台的持有成本為何？Symantec DLP之設計，旨在相較於零散拼湊之替代方案，降低總持有成本。由於 DLP Core 與 DLP Cloud共用單一偵測引擎及單一管理主控台——即 DLP Enforce Platform——貴公司資安團隊只需撰寫一套政策，即可於各處統一執行：端點、網路、儲存庫及雲端。此舉可消除因分別部署端點防護、網路監控及雲端存取安全等獨立單點解決方案所產生之重複授權、重複管理及重複訓練成本。部署彈性亦進一步保障預算：此解決方案可採地端軟體、虛擬或實體設備，以及公有、私有或混合雲端服務等形式提供，使組織不致受限於單一基礎架構模式，並能採用最符合其現有資本支出與營運支出組合之部署方式。

與零散拼湊之替代方案相比又是如何？整合本身即是一項降低成本之槓桿。超過70套預建政策範本，以及超過130項現成資料識別器，可大幅縮短為PII、PCI及PHI等常見監管類別建立偵測機制所需之專業服務時間。自動化事件修復——包括一鍵式 SmartResponse 及加密、隔離、重新導向或封鎖等以規則為基礎之動作——可降低分流處理事件佇列所需之人力配置，而此類人力往往是資安專案中最龐大之經常性營運成本。此外，由於此平台已獲驗證可擴展至數十萬名使用者規模，成本曲線將隨組織成長而趨於平緩，無須在每個擴張階段皆重新建置架構。

對財務長而言，其財務論述十分明確：Symantec DLP 能將一項開放式、難以量化的風險——喪失對組織最機敏資料掌控權之風險——轉化為固定、可編列預算之營運成本，僅需維繫單一供應商關係、採用整合式授權模式，並可實證降低事件應變之人力負擔。這是以企業規模採購之防護方案，其定價設計正是為了避免單點產品氾濫所帶來之疊加成本。

建構可禁得起檢驗的資安架構：致資訊安全長

資訊安全長的職責，在於設計一套禁得起檢驗的資安架構——無論是面對董事會、監管機關、稽核人員，或是在事件發生時面對資訊安全長自身的團隊，皆須經得起檢驗。這不僅需要優異的偵測技術，更需要一套連貫的架構，使政策、可視性與執行力，無論資料位於何處皆保持一致。Symantec DLP 正是圍繞此一原則所打造。

此架構之核心為 DLP Enforce Platform，是一套單一整合管理主控台，用於政策管理、事件應變、報告及管理作業。貴團隊無須為端點、網路出口、儲存庫及雲端應用程式，各自維護獨立的政策集，只須撰寫一套政策，即可於各處統一執行。這是資訊安全長在此領域中，所能做出最重要的架構決策，因為彼此獨立工具間的政策漂移 (Policy Drift)，正是合規缺口與漏報事件(False-Negative)——亦即因無任何單一工具掌握完整資料路徑之可視性、而從未觸發警示之外洩事件——最常見的根本原因之一。

從此主控台出發，其涵蓋範圍可延伸至四大領域，共同構成機敏資料的完整生命週期：

- 端點(Endpoints)——筆記型電腦與桌上型電腦：DLP Endpoint Discover掃描本機儲存空間，建立機敏檔案之基準盤點清單；DLP Endpoint Prevent 則監控使用者於各應用程式、裝置及平台之活動，涵蓋可移除式儲存裝置、虛擬桌面、瀏覽器、列印、傳真及剪貼簿。
- 網路(Network)——DLP Network Monitor於網路出口點，對外傳流量執行深度、零封包遺失之內容檢測；DLP Network Prevent for Email 與 DLP Network Prevent for Web 則針對違反政策之郵件與網頁流量，執行修改、重新導向或封鎖，並可在與安全網頁閘道整合後，涵蓋加密流量。
- 儲存(Storage)——DLP Network Discover 掃描 Windows、Linux、AIX 及 Solaris 環境中之檔案伺服器、資料庫、SharePoint 及其他儲存庫，可辨識超過 330 種檔案類型；DLP Network Protect 則針對 Discover 所發現之項目，透過隔離、加密或數位版權管理(DRM)進行修復處理。
- 雲端(Cloud)——由 Symantec CloudSOC 驅動之 DLP Cloud，將相同之偵測技術與政策集，延伸至超過 100 個已核准與未核准之雲端應用程式，包括 Office 365、Google Workspace、Box、Dropbox 及 Salesforce，並即時檢測流向生成式 AI 應用程式之資料。

在此管道涵蓋範圍之下，真正決定此架構能否禁得起稽核檢驗的是其偵測技術本身。SymantecDLP結合描述內容比對(Described Content Matching，內建超過 130 項資料識別器，用以偵測帳號、政府核發證號及信用卡號等模式)、針對資料庫與目錄伺服器已建立指紋之結構化來源進行的精確資料比對(Exact Data Matching)、適用於 Office 文件、PDF 甚至檔案間複製之衍生內容等非結構化內容的索引文件比對(Indexed Document Matching)、運用 OCR 與表單辨識之機敏影像辨識，以及針對財務模型、原始程式碼等關鍵字規則經常漏判之細膩、難以描述之智慧財產所採用的向量機器學習(Vector Machine Learning)。將此等技術結合複合式比對條件與基於群組之例外規則，於單一政策內分層運用，正是將誤報率控制在企業實際能夠容忍之範圍內的關鍵所在。

就治理與稽核目的而言，此平台之設計本就以「可禁得起檢驗」為出發點。系統內建超過70套與主要監管框架 (PII、PCI、HIPAA及其他區域性與產業別標準) 相符之預建政策範本，且每一起事件均附帶完整脈絡：所違反之政策、已採取之應變動作、偵測到之確切比對內容、自訂屬性，以及關聯歷程，全數皆可自單一主控台直接查詢調閱，無須事後自多個彼此獨立之記錄重新拼湊還原。Symantec Information Centric Analytics更在此原始遙測資料之上，加入已取得專利之使用者與實體行為分析(UEBA)，針對正常行為建立基準，並就資料、身分及威脅訊號進行風險評分，讓貴團隊得以優先處理少數真正屬於惡意或高風險活動之事件，而非以相同急迫程度追蹤每一筆政策比對結果。

最後，此架構之設計理念，是與貴公司既有系統整合，而非取而代之。Symantec DLP與Microsoft Purview Information Protection完全整合，可用於分類、加密及權限管理；並與 Symantec 安全網頁閘道(ProxySG與Web Security Service) 連接，以檢測加密網頁流量；同時運用Symantec VIP身分與存取管理，於資料與外部合作夥伴共用時強化驗證機制；並開放完整之 API 介面——DLP REST API、FlexResponse API、Content Extraction API、Incident Reporting and Update API，以及 API Detection 虛擬設備——使其得以融入 SOAR 劇本、自訂修復流程及第三方資安工具。這正是「可禁得起檢驗之架構」的定義：一致的政策、分層式偵測、完整的稽核軌跡，以及開放式整合，全數出自單一平台。

運作高效能專案：致資訊安全維運經理

若您負責資料保護專案之日常維運，您所面臨的主要限制，往往不在於某項控管機制是否存在，而在於貴團隊能否以具規模的方式運作該控管機制，同時不被警示淹沒、不惹惱業務單位，也不需要每一起事件都仰賴資深分析師逐一手動釐清。Symantec DLP 正是針對此類維運壓力所打造。

首先談事件量與分流處理。Symantec DLP 所偵測到之每一起事件，抵達主控台時皆已附帶完整資訊：所違反之政策、已採取之應變動作、確切比對之內容、關聯之自訂屬性，以及該使用者或資產之完整事件歷程。這意味著貴公司分析師的時間，花費在決定「下一步該怎么做」，而非重新拼湊「發生了什麼事」——當貴團隊須同時處理來自端點、網路、儲存及雲端等多個管道之事件時，此差異對平均處理時間而言意義重大。

並非每一起事件都需要人工介入。自動化與人工修復選項，可讓您依違規之嚴重程度校準應變方式。風險較低、信心水準較高之事件，可透過升級通報、通知、重新導向、隔離與還原，或直接封鎖等方式自動處理，無須分析師介入。嚴重程度較高或情況不明確之事件，則可升級通報至貴團隊，此時一鍵式 SmartResponse 可讓分析師立即採取行動，無須經歷多步驟工作流程；事件亦可直接分派給業務單位之資料負責人，由其自行審查並做出處置——在不增加資安團隊人力的情況下，擴大事件應變能量。

防範僅是維運工作的一半；另一半則是改變行為模式，避免同類事件再次發生。Symantec DLP 之即時教育提示通知，會在員工嘗試進行風險行為之當下立即發出警示，說明適用之政策內容，並於適當情形下，讓員工自行提供業務正當理由，或於誤判情況下自行取消該動作。此舉將相當比例之政策教育宣導，由正式訓練課程轉移至風險實際發生之當下，其成效不僅更佳，執行成本也低於定期舉辦之教室型法規遵循訓練。

在幕後，做為本平台使用者與實體行為分析引擎的 Information Centric Analytics，會持續針對每位使用者與每項資產建立正常活動之基準，並關聯資料外洩遙測資料、身分與存取遙測資料，以及來自其他資安系統之威脅遙測資料。其結果是一套可自我調整之風險評分機制，以及可自訂之儀表板，讓貴團隊得以將注意力集中於真正代表內部風險或帳號遭入侵活動之使用者與事件，而非以同等急迫程度看待每一筆政策比對結果。對於須在固定分析師人力下、因應日益增加之受監控管道數量的經理人而言，此優先排序機制，往往正是「可持續運作之專案」與「持續疲於奔命救火」之間的關鍵差異。

向上彙報功能亦內建其中。Symantec IT Analytics for DLP 提供進階報告與臨機分析功能，讓您得以向領導階層呈現事件量、修復時間、政策成效，以及依事業單位劃分之風險集中度等趨勢走向——此即支持預算申請、以及本手冊前文所述董事會層級信心保證所需之維運佐證。簡言之，此平台之設計，讓一支精簡的維運團隊，即可涵蓋企業內每一個資料管道，而無須隨每新增一個管道，即線性增加人力配置。

深入探討偵測與部署：致資安維運工程師

對於負責日常組態設定、調校及維護本平台之工程師而言，所面對的問題十分具體：有哪些偵測方法可供使用、這些方法如何在單一政策內相互組合、實際支援哪些管道與協定，以及在大規模分散式環境中，部署拓撲究竟是何種樣貌。本節即以此等細節層級撰寫。

偵測技術。Symantec DLP 之內容感知偵測技術，係由五項互補技術所構成，可於單一政策內組合運用：

- 描述內容比對(Described Content Matching, DCM)——透過關鍵字、正規表示式、模式及檔案屬性辨識內容，並運用超過 130 項現成資料識別器，結合模式比對與內建智慧邏輯以抑制誤報。最適合用於無法建立索引之資料，例如：以自由格式描述之機敏類別內容。
- 精確資料比對(Exact Data Matching, EDM)——針對資料庫、目錄伺服器及結構化資料檔案等結構化資料來源，建立指紋或索引，最適合用於帳號、信用卡號及政府核發證號等事先已知確切數值之情境。
- 索引文件比對(Indexed Document Matching, IDM)——針對非結構化文件(包括 Microsoft Office 檔案、PDF，以及 JPEG、CAD 檔案、多媒體等二進位格式) 建立指紋，並偵測衍生內容——亦即自來源文件複製至另一檔案之文字——此為僅依賴關鍵字比對之工具經常無法察覺之常見規避手法。
- 向量機器學習(Vector Machine Learning, VML)——保護具細膩特徵、難以描述或建立指紋之智慧財產，例如財務報表與專有原始程式碼，無須事先定位、描述或建立索引。
- 機敏影像辨識(Sensitive Image Recognition)——隨 DLP Core 提供，結合專有之表單辨識(Form Recognition)技術與內建之光學文字辨識(OCR)引擎，偵測嵌入於掃描表單、螢幕截圖及以影像為主的 PDF 中之機敏文字。

此平台亦支援針對表格式資料格式之結構化資料比對，並開放完整之 API 介面以供擴充：DLP REST API、用於建置自訂修復動作並與第三方檔案安全解決方案完成整合之 FlexResponse API、Content Extraction API、Incident Reporting and Update API，以及可將偵測功能嵌入自訂或專屬應用程式之 DLP API Detection 虛擬設備。

端點涵蓋範圍。單一輕量化端點代理程式，即可啟用兩項模組。DLP Endpoint Discover 掃描本機硬碟，建立靜態機敏資料之基準盤點清單，並透過 Endpoint FlexResponse API，支援本機與遠端檔案隔離、以政策為基礎之加密，以及數位版權管理等應變作為。DLP Endpoint Prevent 則即時監控使用者活動，支援針對複製至 USB 之檔案採用基於身分之加密與數位版權管理、螢幕或郵件警示，並允許使用者於疑似誤判情況下，自行提供業務正當理由或取消該動作。端點涵蓋範圍延伸至 Chrome、Safari、Firefox、IE 及 Edge 瀏覽器；Box、Dropbox、Google Drive 及 Microsoft OneDrive 等雲端應用程式；Outlook 及 Lotus Notes 等電子郵件用戶端；HTTP、HTTPS 及 FTP 等網路協定；MSC 與 MTP 可移除式儲存裝置；Citrix、Microsoft Hyper-V 及 VMware 虛擬桌面；以及列印、傳真、網路共用區及剪貼簿等操作行為。

網路涵蓋範圍。DLP Network Monitor 以零封包遺失之方式，擷取並分析對外傳輸之網路流量——有別於在尖峰負載下抽樣封包、進而導致漏報之解決方案——並可跨標準、非標準及專屬通訊協定，偵測機敏內容與中繼資料。此模組部署於網路出口點，並與網路分接器(Network Tap)或交換式連接埠分析器(Switched Port Analyzer, SPAN)整合。DLP Network Prevent for Email 與郵件傳輸代理程式及雲端郵件(包括 Microsoft Office 365 Exchange)整合，可採軟體或虛擬設備形式提供，並依機敏內容或郵件屬性，執行郵件修改、重新導向或封鎖。DLP Network Prevent for Web 則透過網際網路內容調適協定(Internet Content Adaptation Protocol, ICAP)，與 HTTP、HTTPS 或 FTP 代理伺服器整合，可採軟體、硬體設備或虛擬設備形式提供，並視需要移除機敏 HTML 內容或封鎖請求。

儲存涵蓋範圍。DLP Network Discover 掃描 Windows、Linux、AIX 及 Solaris 伺服器上之本機檔案系統、Lotus Notes 與 SQL 資料庫，以及 Microsoft Exchange 與 SharePoint 伺服器，並可依二進位簽章辨識超過 330 種檔案類型——包括自訂檔案類型——並針對大規模分散式環境，最佳化高速掃描效能，僅處理新增或已修改之檔案。DLP Network Protect 則在此基礎上疊加修復功能：隔離或移動檔案、將檔案複製至隔離區、套用以政策為基礎之加密或數位版權管理，並於原始位置留下說明性標記檔案，讓業務使用者瞭解該檔案遭隔離之原因。

雲端涵蓋範圍。DLP Cloud Detection Service 檢測自雲端應用程式及網頁流量中擷取之內容，並透過與 Symantec CloudSOC 之雲端對雲端整合，於超過 100 個已核准與未核准之應用程式(包括 Office 365、Google Workspace、Box、Dropbox 及 Salesforce)中執行機敏資料政策，同步保護傳輸中與靜態儲存之資料。與 Symantec Web Security Service 整合，可將監控範圍延伸至漫遊及行動使用者之加密網頁流量。CloudSOC 本身則疊加了用於探索影子 IT 之 CASB Audit、用於活動監控與控管之 CASB for SaaS and IaaS，以及運用 ThreatScore 風險分析異常使用者行為、進行即時內嵌式執行之 CASB Gateway。DLP Cloud Detection Service for Email 支援 Gmail for Work、Microsoft 365 Exchange Online 及 Microsoft Exchange Server，並於資料與第三方共用時，提供即時封鎖、郵件修改，以及自動化基於身分之加密或數位版權功能。

部署拓撲。此平台支援地端軟體、虛擬及實體設備，以及公有、私有或混合雲端服務，並可透過 Symantec 合作夥伴提供之代管服務交付——讓工程團隊得以彈性選擇最符合既有基礎架構與法規遵循要求之部署方式。此架構已獲大規模驗證，可於單一整合管理平台之下，支援涵蓋數十萬名使用者之高度分散式環境。

涵蓋所有通訊管道的全方位保護

資料保護領域中最常見的失效模式之一，即是涵蓋範圍不完整：擁有強大端點代理程式、卻對雲端儲存毫無可視性；或是網路監控工具，卻無法察覺透過個人裝置流出之資料。Symantec DLP之架構圍繞四大涵蓋領域建構，並由單一政策引擎與工作流程統一整合，使同一條保護檔案共用區內社會安全碼的規則，同樣適用於電子郵件附件、USB 複製檔案，以及上傳至雲端硬碟之情境。

涵蓋領域與代表性管道

領域	代表性管道
網路	電子郵件、網頁、FTP、即時通訊（IM）、IPv6
儲存	檔案伺服器、資料庫、Exchange、SharePoint、NAS 檔案伺服器
端點	可移除式儲存裝置、桌面電子郵件、網頁應用程式、虛擬桌面
雲端	雲端應用程式、Office 365 Exchange、Gmail、Box、Google Workspace、Salesforce

這不僅僅是一張行銷用示意圖，更真實反映資料在實際組織中的移動方式。一份在筆記型電腦上草擬的合約(端點)，可能透過電子郵件寄送給外部律師(網路)、儲存於公司 SharePoint 網站(儲存)，並在稍後透過合作夥伴的 Box 帳戶共用出去(雲端)。由於Symantec DLP在上述每一個環節，皆套用相同的政策邏輯與偵測技術，組織無須寄望四套不同的工具，恰好對「何謂機敏資料」達成一致認定——組織可以確知它們的認定必然一致，因為其底層正是同一套引擎。

此一整合式作法，也直接因應了資安團隊當前面臨、成長最快速的風險類別之一：生成式 AI。由於 DLP Cloud 針對流向 AI 應用程式之傳輸中資料，採用與其他各處相同之內容感知偵測技術，組織無須在「全面禁止生成式 AI（因而喪失生產力效益）」與「放任不受監控地使用」之間二選一。機敏內容可即時被辨識並攔截、阻止其送達公開 AI 工具，而非機敏內容之使用則可暢行無阻、不受影響。

此設計所帶來的實際效益，同時展現在三個層面：攻擊者或疏忽的員工能夠找到的涵蓋缺口更少；資安團隊須維護的獨立政策集更少；一旦發生問題，調查人員也能取得單一、完整的事件時間軸可供追查。全方位管道涵蓋範圍，並非單純的功能清單——它是讓本手冊中所述其他每一項能力(從自動化修復到高階主管報告)真正值得信賴的基礎。

資料保護實務：常見使用案例

抽象的功能，最容易透過具體情境加以評估。以下使用案例，代表部署 Symantec DLP 之組織最常提及的情境，且每一項皆可直接對應至本手冊其他章節所述之功能。

「在撰寫第一條政策之前，先取得可視性。」許多組織在啟用探索掃描後才發現，自己其實並不清楚機敏資料究竟存放於何處。DLP Network Discover 與 DLP Endpoint Discover，可針對檔案伺服器、資料庫、SharePoint 網站及筆記型電腦，建立基準盤點清單，經常因此發現多年累積、存放於無人記得曾經建立之位置的受監管資料。此一基準清單，將成為後續每一項政策決策的基礎，也往往是組織在承諾展開更大規模部署之前，所要求提供的第一項交付項目。

「阻止善意員工造成的意外外洩。」絕大多數資料外洩事件並非出於惡意；而是員工郵件誤附錯誤檔案、共用資料夾的範圍超出原本預期，或是為了在家工作而將客戶名單複製至個人雲端硬碟等情況所致。由於 Symantec DLP 在電子郵件、網頁、雲端應用程式及端點各處，均套用相同的偵測邏輯，此類意外外洩事件，可於發生的當下即被攔截，並透過即時教育提示，說明所違反之政策，並於適當情形下，讓員工得以自行更正。

「偵測內部風險與遭入侵帳號。」即將離職的員工，開始下載異常大量的原始程式碼；或是某個遭入侵的帳號，突然出現與其歷史基準不符的存取模式——此類情境，代表與意外外洩截然不同的風險類別。Information Centric Analytics 與 Symantec CloudSOC UEBA，正是專為此類情境而打造，透過關聯資料外洩遙測資料與身分及威脅訊號，在人工分析師從原始事件佇列中察覺異常之前，及早標記行為異常。

「在不造成政策脫節的前提下，將治理有序的資料保護延伸至雲端。」多年前即建立完善地端 DLP 實務的組織，經常發現其政策未能跟上關鍵工作負載遷移至 Office 365、Google Workspace、Salesforce 及數十種其他 SaaS 應用程式的腳步。DLP Cloud 無須為雲端另行建立第二套獨立政策集，而是將既有、已於地端獲得驗證之政策與偵測技術，直接延伸適用，使得一條規則只需撰寫一次，即可隨資料遷移至已核准雲端服務內部及各服務之間，持續發揮效用。

「在不全面禁止的前提下，治理生成式 AI 的使用。」如本手冊 AI 時代章節所述，組織日益傾向選擇「允許」而非「禁止」員工使用 AI 工具，同時仰賴即時內容檢測，防止機敏資料實際送達該等工具。此一使用案例，在短短約兩年間，已從邊緣案例，躍升為新建 DLP 部署案中最常被要求之功能之一。

「以可實證、持續性的控管機制，滿足稽核人員或監管機關之要求。」組織無須僅在事件發生後才提出合規證據，而是運用平台內建之政策範本、完整事件脈絡及 IT Analytics 報告功能，產生一份持續性的控管成效記錄——此記錄經常直接納入董事會及稽核委員會之例行報告週期當中。

「支援企業併購及其他高機敏交易案。」在盡職調查與整合期間，高度機密之財務、法律及策略資訊之流通量，會大幅增加，且經常涉及一組暫時擴大之外部顧問及交易對手。Symantec DLP 能夠針對特定交易相關文件，套用精確資料比對與索引文件比對，並搭配對外共用資料時之基於身分加密機制，讓交易團隊得以快速推進，同時在組織風險暴露程度最高的這段期間，不致喪失對最關鍵資訊的掌控。

產品組合：DLP Core 與 DLP Cloud

Symantec DLP 透過兩套互補的解決方案組合交付，兩者共用單一政策引擎、單一主控台及單一事件處理工作流程。組織可選擇由其中一套著手，日後再擴充至另一套，無須重新規劃整體架構。

DLP Core提供地端及混合式部署之基礎：涵蓋端點、網路及儲存之防護，並加入機敏影像辨識與Information Centric Analytics（使用者與實體行為分析）。對於著重受管理環境內靜態及傳輸中資料（例如筆記型電腦、檔案伺服器、資料庫、SharePoint 及對外傳輸流量）之組織而言，這是理想的起點。

- DLP for Endpoints——透過單一輕量化代理程式提供 Endpoint Discover 與 Endpoint Prevent，針對電子郵件、雲端應用程式、網路協定、外部儲存裝置，以及虛擬桌面與伺服器中使用中之資料，提供探索、監控及防護功能。
- DLP for Network——包含 Network Monitor、Network Prevent for Email 及 Network Prevent for Web，以零封包遺失之檢測方式，保護透過公司網路出口點傳輸中之資料。
- DLP for Storage——包含 Network Discover 與 Network Protect，於檔案共用區、資料庫及企業儲存庫中，尋找並修復靜態機密資料。
- Information Centric Analytics——已取得專利之使用者與實體行為分析，關聯資料、身分及威脅遙測資料，優先處理風險最高之使用者與事件。
- 機敏影像辨識（Sensitive Image Recognition）——結合光學文字辨識（OCR）與表單辨識技術，擷取並偵測嵌入於掃描文件、螢幕截圖及以影像為主之 PDF 中的機敏文字。

DLP Cloud 將相同的偵測技術與政策集延伸至雲端，結合業界領先之企業級 DLP，與 Symantec 旗下之雲端存取安全代理（Cloud Access Security Broker，CASB）——CloudSOC。若說 DLP Core 保護的是貴公司受管理環境內部所發生之一切，DLP Cloud 保護的，則是資料一旦跨越至 SaaS 應用程式、未經核准之影子 IT，以及生成式 AI 平台之後所發生之一切。

- CASB Audit——探索並監控組織內正在使用之每一項雲端應用程式，揭露影子IT，並可封鎖對未經核准服務之存取。
- CASB for SaaS and IaaS——雲端式服務，針對 Office 365、Google Workspace、Box、Salesforce 及 ServiceNow 等已核准平台上之使用者活動，提供可視性與控管能力。
- CASB Gateway——持續監控並控管雲端應用程式之使用情形，以執行政策、辨識惡意或不當共用行為、發出惡意軟體威脅警示，並自動化升級通報流程。
- DLP Cloud Detection Service for CASB——檢測自雲端應用程式及網頁流量中擷取之內容，將既有地端 DLP 政策延伸至超過 100 個已核准與未核准之雲端應用程式，並可直接自 DLP 主控台進行事件管理。
- DLP Cloud Detection Service for Cloud SWG——與 Symantec 雲端安全網頁閘道整合，即便是漫遊及行動使用者之加密網頁流量，亦能加以監控。
- DLP for Office 365 and Gmail——運用內建智慧邏輯與進階偵測技術，持續監控公司電子郵件流量，並透過自動化郵件修改、封鎖、隔離，或針對共用附件套用下游加密及數位版權管理，即時防範資料外洩。

DLP Core 與 DLP Cloud 兩者結合，共同實現此平台所稱之「單一整合介面」：單一主控台即可完成政策管理、事件應變、報告及管理作業，並以單一政策與工作流程集，涵蓋雲端、電子郵件、網頁、端點及儲存。組織無須在地端嚴謹性與雲端靈活性之間二選一——兩者兼具，正是此架構設計之核心理念。

擴充平台功能：DSPM、進階威脅防護及其他

除了 DLP Core 與 DLP Cloud 核心套件之外，另有多項附加功能，可進一步擴充可視性、威脅防護及資料治理能力。

Symantec 資料安全態勢管理 (Data Security Posture Management, DSPM)，為 DLP Cloud 之附加功能，提供單一整合式儀表板，讓組織對其環境內所有資料及其相關風險，掌握完整全貌——協助資安及資料治理團隊，辨識並分析異常活動，並在風險演變為事件之前，及早採取行動加以化解。對於承受壓力、須向稽核人員及監管機關展現主動資料治理成效之組織而言，DSPM 可將一次性的 DLP 部署，轉化為持續性、可量化衡量之資料風險管理專案。

CloudSOC進階威脅防護，運用檔案信譽情資、防毒掃描及沙盒分析技術，保護雲端帳號與交易免受惡意軟體侵害——將平台之防護範圍，由資料外洩本身，延伸至日益伴隨而生的雲端威脅，例如：上傳至已核准 SaaS 平台之惡意檔案。

此平台亦與周邊資安及身分基礎架構原生整合，組織無須另行汰換既有系統。與Microsoft Purview Information Protection 整合，可延伸 DLP 之能力，使其得以偵測並讀取已透過 Microsoft 自有資訊保護框架完成分類及加密之文件與郵件。與 Symantec VIP 身分與存取管理整合，可於機敏資料與外部業務合作夥伴共用時，強化驗證機制。而與 Symantec 安全網頁閘道(ProxySG 與 Web Security Service)整合，則可確保機敏資料不致透過不受信任之網頁流量外洩，即便該流量已加密亦然。上述每一項整合，皆能減少與貴公司既有資安技術堆疊之重複建置，而非又新增一套彼此獨立、需要貴團隊額外監控之主控台。

符合全球法規遵循與監管要求

圍繞資料保護之監管義務，鮮少單獨出現，也鮮少維持不變。單一跨國組織，可能同時須就支付卡資料展現PCI DSS 合規性、就受保護健康資訊展現HIPAA合規性，並因應日益增長之各國及區域性個人身分識別資訊隱私法規清單——每一項規範，皆各自定義範疇、各自要求控管措施、各自訂有稽核期待。將此一拼湊式的規範體系，轉化為具體的技術控管措施與組織性措施，是當今資安與法規遵循團隊所面臨最持續存在的負擔之一。

Symantec DLP 將法規對應(Regulatory Alignment)視為首要設計目標，而非事後才考量之附加項目。平台內建涵蓋 PII、PCI、HIPAA 及其他監管要求之政策，並由超過 70 套預建政策範本及超過 130 項現成資料識別器提供支援，直接對應帳號、政府核發識別證號、信用卡號及受保護健康資訊等常見受監管資料類別。對多數組織而言，此舉可大幅縮短自採購此平台至建立起可禁得起檢驗、且能實際運作之合規專案之間的時間——您只需針對經驗證之範本進行組態設定與調校，而無須從零開始建置偵測邏輯。

合規執行不僅止於偵測層面，更延伸至自動化保護行動。一旦於雲端儲存或傳輸過程中發現受監管資料，平台即可自動套用整合式加密，並要求使用者完成多因子驗證，同時滿足眾多監管框架之明文規定與立法精神——此類框架所要求者，不僅是監控，更是對受監管資料採取積極保護措施。針對透過電子郵件與第三方共用之資料，可自動對郵件內文及附件套用基於身分之加密及數位版權管理，將保護範圍延伸至組織直接掌控範疇之外。

就稽核作業本身而言，此平台所提供之完整事件脈絡——所違反之政策、已採取之應變動作、偵測到之確切比對內容、自訂屬性、屬性關聯，以及事件歷程——意味著貴公司之法規遵循與資安團隊，得以直接自主控制台調取佐證，回應監管機關或稽核人員之提問，無須事後自散落各處之記錄重新拼湊。搭配 Symantec IT Analytics for DLP 之進階報告與臨機分析能力，可讓法規遵循主管取得一份持續性、可實證之控管成效記錄——此類佐證，如今不僅在資料外洩調查發生時才被要求提出，更日益成為例行性監管監督作業之一部分。

隨著監管版圖持續擴展至資料落地要求、AI 治理義務，以及尚未定案之產業別要求等新類別，單一、可擴充政策引擎之價值，也將隨之持續提升。運用 Symantec DLP 之組織，無須為每一項新要求部署新工具，而是可延伸既有政策、新增資料識別器，並將相同、經驗證之偵測技術，套用於未來任何一項監管要求之上。

確保 AI 時代之安全

生成式 AI 在企業內部的快速普及，創造出一項數年前並不存在的資料外洩管道，而在多數組織中，此管道至今幾乎完全未受監控。員工將原始程式碼貼入 AI 程式撰寫助理、將財務模型上傳至 AI 驅動之試算表工具，並要求公開聊天機器人摘要機密合約——所有這些行為，皆是出於追求正當生產力提升之目的，且除非事先部署專屬控管機制，否則資安團隊完全無從察覺。

Symantec DLP 直接因應此一風險，而非將其視為未來才須處理的路線圖項目。此平台監控並檢測流向生成式 AI 應用程式之傳輸中資料，運用與環境中其他各處相同之內容感知偵測技術——描述內容比對、精確資料比對、索引文件比對及向量機器學習——在機敏內容送達公開 AI 服務之前，即予以辨識。資安團隊無須採取全面禁止、進而促使員工轉向未經核准之個人帳號及影子 AI 使用之作法，而是可以允許具生產力之 AI 使用行為，同時防止受監管資料、智慧財產或機密商業資訊透過此管道外流。

此項功能，與平台既有之影子 IT 探索功能相輔相成。正如 CASB Audit 可辨識組織內正在運作之未經核准雲端應用程式，相同的探索方式，亦可延伸用於辨識實際在使用之生成式 AI 應用程式——該清單往往比資安團隊預期得更長、也更令人意外——使組織得以逐一針對各應用程式評估風險並套用適當控管措施，而非採取「全有或全無」的政策，導致不是扼殺生產力，就是忽視風險。

對資安領導者而言，此項功能之策略價值，在於組織無須為此另行建立一套全新的專業領域。由於 AI 監控功能，運作於與其他所有管道相同之 DLP 引擎、相同之政策及相同之主控台之上，組織不必另外維護一套擁有獨立偵測邏輯、也存在獨立盲點的 AI 治理工具。隨著生成式 AI 使用持續擴大，以及新的 AI 專屬監管義務持續浮現，此一共同基礎，意味著組織得以循序漸進地擴充涵蓋範圍，而無須從零開始重新建置。

部署彈性與系統需求

沒有任何兩個組織的基礎架構完全相同，而 Symantec DLP 之設計，正是刻意為了因應此一現實，而非強制套用單一部署模式。此解決方案由單一整合管理平台、輕量化端點代理程式，以及強大之內容感知偵測產品所構成，並提供企業 IT 環境可能需要之各種部署形式：地端軟體、虛擬及實體設備、公有、私有及混合雲端服務，以及針對希望委外處理日常維運之組織，透過 Symantec 合作夥伴提供之代管服務。

此項彈性，在組織雲端旅程的每一個階段皆具有其意義。對於仍在整併地端基礎架構之組織而言，地端軟體與實體設備可直接與既有網路分接器、郵件傳輸代理程式及代理伺服器整合。對於正積極遷移至雲端之組織而言，虛擬設備及雲端交付服務，可延伸相同政策，無須另行並行建置地端環境。而對於正將部分工作負載自雲端遷回客戶自行管理環境之組織——此一模式日益普遍——相同之統一政策集，無論資料移動方向為何，皆可持續適用。

其規模擴充能力已獲驗證，並非停留於理論層次。Symantec DLP 之設計，可於高度分散式環境中運作，並擴充至數十萬名使用者規模，這對負責尖峰負載效能表現之資安維運工程師而言，具有直接意義：以 DLP Network Monitor 為例，其對所有網路通訊執行深度內容檢測，且零封包遺失，相較之下，部分解決方案於高流量期間抽樣封包，恰好在組織最無法承受的時刻，導致漏報情形發生。

各平台之詳細系統需求——包括支援之作業系統、資料庫版本及設備規格——均維護於 Broadcom 支援入口網站，貴公司工程團隊應於進行任何部署規劃作業前先行查閱確認。就架構層面而言，本手冊可確認的是：某一管道所選用之部署模式，並不會限制另一管道可採用之部署模式——組織可將 Network Prevent for Email 以虛擬設備形式運作，同時將 Endpoint Prevent 以裝置端輕量化代理程式形式運作，並將 DLP Cloud 以完全雲端交付服務形式運作，三者皆由同一主控台、依循相同政策統一治理。

常見問題

問：DLP Cloud 是否要求我們汰換既有的地端 DLP 投資？

答：不需要。DLP Core與DLP Cloud之設計理念，是彼此結合運用，而非二選一。單一政策即可對儲存於端點、伺服器、檔案共用區、資料庫及 SharePoint 上之資料套用控管措施，同時該政策亦可同步治理透過Office 365、Box、Google Workspace 及其他雲端應用程式流動之資料。已具備地端部署之組織，通常會將 DLP Cloud 做為既有投資之延伸，而非取而代之。

問：典型的導入過程，對終端使用者的干擾程度有多大？

答：此平台之設計，旨在透過分層式應變選項，將干擾程度降至最低。多數組織並非一開始即封鎖每一筆政策比對結果，而是先從監控與即時教育提示通知著手，於警示使用者的同時，並於適當情形下，允許其提供業務正當理由或自行更正。封鎖與隔離動作，通常僅保留給信心水準最高、嚴重程度最高之政策違規情形，且僅於組織已針對真實流量驗證政策準確性後，才予以導入。

問：此平台如何在企業級規模下，將誤報率控制在可管理的範圍內？

答：其作法是在單一政策內，結合多項偵測技術——描述內容比對、精確資料比對、索引文件比對、機敏影像辨識及向量機器學習——而非僅依賴關鍵字或正規表示式比對。複合式比對條件，以及基於群組之規則與例外設定，可讓政策針對個別事業單位、使用者群組或資料類型進行調校，這正是組織通常用以將誤報率降至維運團隊可長期負荷水準的方式。

問：此平台能否監控加密流量？

答：可以。透過與 Symantec 安全網頁閘道（ProxySG 與 Web Security Service）及 DLP Cloud Detection Service for Cloud SWG 整合，此平台可檢測加密網頁流量——鑒於如今無論是合法業務流量，或是潛在外洩流量，多半皆預設透過 HTTPS 傳輸，此項能力至關重要。

問：當員工使用生成式 AI 工具時，會發生什麼情況？

答：提交至生成式 AI 應用程式之資料，會運用與其他所有管道相同之內容感知偵測技術，進行即時檢測。非機敏用途可暢行無阻、不受干擾；符合已定義政策之內容——例：如客戶記錄、原始程式碼、機密財務文件——則可依政策組態設定，被標記、攔截，或轉交審查。

問：此平台是否適合擁有數十萬名使用者規模的組織？

答：適合。Symantec DLP 已獲驗證，可於高度分散式環境中運作，並可擴充至數十萬名使用者規模，同時支援地端、虛擬及實體設備，以及公有、私有或混合雲端等部署模式，使組織得以在不受單一架構限制點束縛的情況下，達成規模化擴充。

問：我們多快能向董事會或稽核人員展現成效？

答：由於此平台內建超過 70 套預建政策範本，以及超過 130 項涵蓋常見監管類別之現成資料識別器，多數組織能夠及早展開基準探索掃描與第一批政策運作，其所需時間遠短於從零開始建置自訂偵測專案之時程。完整的事件脈絡及 IT Analytics 報告功能，讓組織能夠輕鬆將早期成果，轉化為董事會或稽核委員會期待看到的佐證資料。

問：此平台是否能與我們現有的工具整合？

答：可以。此平台可與 Microsoft Purview Information Protection 整合，用於分類、加密及權限管理；可與 Symantec VIP 身分與存取管理整合，於對外共用資料時提供強式驗證；可與 Symantec 安全網頁閘道整合，用於檢測加密網頁流量；並開放完整之 API 介面——包括 REST API、FlexResponse API、Content Extraction API 及 Incident Reporting and Update API——供希望將 DLP 偵測與修復功能，嵌入自身 SOAR 劇本或第三方工具之組織使用。

為何選擇 Symantec DLP：真正重要的差異化優勢

在本手冊所述及之每一種讀者群體中，皆一再出現若干共通的差異化優勢，因為這些正是使其他一切成為可能的結構性決策。

- 單一整合政策引擎。一套政策，撰寫一次，即可於端點、網路、儲存及雲端統一執行——消除彼此獨立單點工具所造成之涵蓋缺口與管理負擔。

- 業界最廣泛的內容感知偵測技術。描述內容比對、精確資料比對、索引文件比對、機敏影像辨識及向量機器學習，皆可於單一政策內組合運用，兼顧精準度與低誤報率。
- 全方位管道涵蓋範圍。雲端應用程式、電子郵件、網頁、端點、儲存，以及生成式 AI 應用程式——涵蓋機敏資料自產生、儲存、共用，乃至可能外洩之完整生命週期。
- 內建使用者與實體行為分析。Information Centric Analytics 與 Symantec CloudSOC UEBA，關聯資料、身分及威脅遙測資料，優先處理真實風險，而非以相同標準看待每一筆政策比對結果。
- 自動化、可擴充之事件修復機制。以規則為基礎之自動化動作，以及一鍵式 SmartResponse，可在受監控管道及資料量成長之同時，降低分析師之工作負擔。
- 部署彈性。地端、虛擬及實體設備，以及公有、私有或混合雲端，皆已獲驗證可規模化擴充至數十萬名使用者。
- 深度、開放式整合。整合 Microsoft Purview Information Protection、Symantec 安全網頁閘道、Symantec VIP 身分與存取管理，並提供完整之 REST、FlexResponse、Content Extraction 及 Incident Reporting API 介面。
- 為 AI 時代量身打造。即時檢測流向生成式 AI 應用程式之資料，採用與其他所有管道相同之偵測引擎與政策。

上述任何一項差異化優勢，皆非孤立存在。正是此等優勢之組合——單一引擎、全方位管道、分層式偵測、內建分析、自動化應變、彈性部署、開放式整合，以及對 AI 時代之充分準備——使 Symantec DLP 得以透過單一投資，滿足本手冊所述及之每一位利害關係人，而無須為每一位利害關係人之關切事項，分別採購獨立產品因應。

實務部署路徑

評估 Symantec DLP 之組織，經常詢問實際的導入過程究竟是何種樣貌——並非行銷語言層面的描述，而是專案在第一年間所歷經的決策順序與里程碑。儘管每個環境皆有所不同，成功的部署案例，往往傾向遵循類似的四階段模式；事先瞭解此一模式，有助於本手冊所述及之每一位利害關係人，對成效開始顯現的時間點，建立務實的期待。

第一階段：探索與建立基準。在撰寫任何一條執行性政策之前，多數組織會先以純監控模式，針對最優先之儲存庫及端點群體——通常涵蓋財務、法務、人力資源及工程部門，因為此等部門集中了大量受監管及高價值智慧財產——運行 DLP Network Discover 及 DLP Endpoint Discover。此階段之目標，是針對「我們的機敏資料究竟存放於何處」此一問題，取得可禁得起檢驗的答案，而此答案往往與組織原先的假設有所出入。此階段也讓資安維運團隊，在任何政策設定為封鎖之前，取得關於事件量與誤報率的第一批真實資料。

第二階段：政策調校與監控。以預建政策範本及現成資料識別器為起點，資安團隊逐步加入複合式比對條件、基於群組之規則，以及針對組織自身資料與工作流程之例外設定。此階段之政策，通常運行於監控與通知模式——針對違規事件發出警示，並即時提供使用者教育提示，但尚未執行封鎖或隔離——讓團隊得以在不干擾業務運作的前提下，依真實流量驗證政策準確性。此階段亦是 Information Centric Analytics 開始建立基準之時期，因為使用者與實體行為分析，須經過一段正常活動期間，才能為特定群體確立「正常」樣貌之基準。

第三階段：執行與自動化。一旦政策準確性經過驗證，信心水準最高、嚴重程度最高之政策，即轉為自動化執行——封鎖、隔離、重新導向或加密——而信心水準較低之政策，則維持於教育提示或人工審查狀態。此時亦是設定自動化事件修復及 SmartResponse 之時機，將維運團隊之日常工作，由被動式分流處理，轉向例外狀況處理及持續性政策精進。許多組織亦於此階段，將涵蓋範圍延伸至 DLP Cloud，將已於地端驗證之相同政策，套用於其已核准之雲端應用程式，並視情況延伸至生成式 AI 使用行為。

第四階段：持續改善與報告。在核心涵蓋範圍到位後，專案將轉為穩定的運作節奏：隨業務變化定期審查政策、於新監管要求出現時將其納入、運用 DSPM 及基於 CloudSOC 之可視性，將涵蓋範圍擴展至新採用之雲端應用程式，並運用 Symantec IT Analytics for DLP，定期向資安領導階層、法規遵循單位及董事會進行報告。此階段也是本手冊前文所述之財務論證與風險降低效益，開始變得可量化衡量之時期——事件量、修復時間及政策成效之趨勢走向，為組織提供該專案投資報酬率之具體佐證。

由於DLP Core與DLP Cloud在上述四個階段中，皆共用相同之政策引擎與主控台，隨著涵蓋範圍由端點擴展至網路、儲存乃至雲端，上述工作皆無須重複進行。於第二階段調校完成之政策，在第三階段延伸至新管道時，其底層邏輯維持不變、持續適用——這正是單一整合平台旨在提供之維運槓桿效益。

產業別考量

儘管核心平台在各產業間皆維持一致，形塑部署方式之優先考量，卻往往因產業別而有所不同。以下考量事項，可做為產業別規劃討論之起點。

金融服務業。銀行、保險及資本市場相關組織，通常優先著重於帳號、支付卡資料，以及交易與案件資訊之保護，並須遵循嚴格之監管報告義務。針對核心銀行系統及客戶資料庫套用精確資料比對，搭配內建 PCI 政策範本，以及與交易對手共用資料時採用之基於身分加密機制，往往是建立可禁得起檢驗之控管體系最快速的途徑。本手冊前文所述之併購及交易團隊使用案例，在此產業中尤其攸關重大，因為機密交易資訊在此產業中持續不斷流通。

醫療照護與生命科學業。受保護健康資訊，是所有資料類別中受監管義務最嚴格的類別之一；醫療照護機構，經常將針對病患記錄系統之結構化EDM，與機敏影像辨識技術結合運用，以攔截嵌入於掃描表單、傳真及轉診文件中之受保護健康資訊——儘管數位化程度日益提升，此一管道在臨床環境中，仍出乎意料地活躍。符合 HIPAA 規範之政策範本，以及平台針對受監管資料內建之合規執行機制，可減輕將 HIPAA 要求轉化為具體技術控管措施之負擔。

製造業與工業技術業。對於主要風險並非受監管個人資料、而是工程設計、專有配方及原始程式碼流失之組織而言，向量機器學習與索引文件比對，通常是最具相關性之偵測技術，因為此類智慧財產，經常難以用關鍵字或正規表示式加以描述，卻能夠直接自組織自身之機密檔案（包括 CAD 設計檔及其他二進位格式）建立指紋或建模。

科技、媒體與專業服務業。以智慧財產為核心之組織——軟體原始程式碼、尚未發布之產品規劃、客戶機密交付項目——所面臨之風險型態，具有其獨特性，集中於員工離職、承包商存取權限，以及為提升生產力而使用生成式AI程式撰寫及寫作助理所帶來之壓力。Information Centric Analytics 與CloudSOC UEBA，在此產業中特別具有價值，可在員工離職之前，及早標記異常資料移動情形；而平台之生成式 AI 監控功能，則因應原始程式碼或客戶資料遭貼入公開 AI 工具此一較新興之風險。

無論在哪一個產業，底層架構皆維持不變——單一政策引擎、分層式偵測，以及涵蓋端點、網路、儲存與雲端之保護範圍。真正因產業而異的，是組織選擇優先採用之偵測技術、政策範本及整合方式；而 Symantec DLP 廣泛之內建功能，意味著此優先順序可隨時間演進調整，無須為未來浮現之新優先事項，另行採購新平台。

附錄 A：端點與儲存庫涵蓋範圍詳情

對於負責規劃部署範圍之工程團隊而言，下表彙整了本手冊其他章節所提及、已記錄之管道與儲存庫涵蓋範圍。

端點管道可用性

端點管道	可用性
瀏覽器	Chrome、Safari、Firefox、Internet Explorer、Edge
雲端應用程式	Box、Dropbox、Google Drive、Microsoft OneDrive
電子郵件應用程式	Outlook、Lotus Notes
網路協定	HTTP、HTTPS、FTP
可移除式儲存裝置	MSC 裝置、MTP 裝置
虛擬桌面	Citrix、Microsoft Hyper-V、VMware
其他管道	列印、傳真、網路共用區、剪貼簿

儲存庫可用性

儲存庫	可用性
檔案伺服器	Windows（透過 CIFS 及 DFS）、Unix（透過 NFS）、本機 Windows、Linux、NAS 檔案伺服器
分散式主機	筆記型電腦、桌上型電腦
電子郵件應用程式	SharePoint、Lotus Notes、Microsoft Exchange、PST
網頁內容與應用程式	公司網站、內部網路（Intranet）、外部網路（Extranet）、自訂應用程式
資料庫	Oracle、Microsoft SQL Server、IBM DB2

上述表格僅供參考，並非詳盡完整清單；完整且最新之系統需求與支援平台版本，均維護於 Broadcom 支援入口網站，並應於正式擬定部署計畫前，與貴公司之客戶經理確認。

附錄 B：關鍵術語詞彙表

- CASB(雲端存取安全代理，Cloud Access Security Broker)——位於使用者與雲端服務供應商之間、用以執行資安、法規遵循及治理政策之控管節點；於本平台中，透過 Symantec CloudSOC 交付。
- DCM(描述內容比對，Described Content Matching)——透過關鍵字、正規表示式、模式及檔案屬性，辨識機敏內容之偵測技術。
- EDM(精確資料比對，Exact Data Matching)——針對資料庫等結構化資料來源建立指紋或索引，以偵測與已知機敏記錄完全相符內容之偵測技術。
- IDM(索引文件比對，Indexed Document Matching)——針對非結構化文件建立指紋，以偵測原始檔案或自其衍生之內容之偵測技術。
- VML(向量機器學習，Vector Machine Learning)——針對財務報表或原始程式碼等事先難以描述或建立指紋之內容，採用機器學習為基礎之偵測技術。
- UEBA(使用者與實體行為分析，User and Entity Behavior Analytics)——針對使用者與系統之正常行為建立基準，並將具統計顯著性之偏差標記為潛在風險指標之分析技術。
- DSPM(資料安全態勢管理，Data Security Posture Management)——以儀表板為核心之功能，提供環境內資料所在位置及其相關風險之整合式檢視。
- ICAP(網際網路內容調適協定，Internet Content Adaptation Protocol)——用於將DLP Network Prevent for Web 與 HTTP、HTTPS 或 FTP 代理伺服器整合之通訊協定。
- SmartResponse——供分析師快速執行人工事件應變之一鍵式、預先設定修復動作。
- 影子 IT(Shadow IT)——組織內未經 IT 或資安團隊正式核准、掌握可視性或治理之雲端應用程式或服務。
- FlexResponse API——一套 API 平台，讓組織得以建置自訂檔案修復動作，並將 DLP 與第三方檔案安全解決方案進行整合。

關於 Broadcom 旗下之 Symantec 資料外洩防護

Symantec 資料外洩防護，是 Broadcom 旗下 Symantec Enterprise Cloud 產品組合的一部分，支持現代企業以資料為核心、支援混合式部署之安全存取服務邊緣（Secure Access Service Edge，SASE）願景。它反映了數十年來，於內容感知偵測、事件管理及雲端資料安全領域持續投入之成果，並整合為單一平台，而非事後鬆散整合、透過併購取得之單點產品集合。

在一個資料保護供應商來來去去、且於合規專案推行數年後才更換平台將帶來實質成本與風險之市場中，此一發展歷程意義重大。選擇企業級DLP平台之組織，所選擇的不僅是今日可用之一系列功能；更是選擇一家預期將持續投資於偵測準確度、管道涵蓋範圍，以及包括生成式 AI 在內之新興風險類別的供應商，且此投資須延續多年。Symantec 對此平台之持續擴充——從最初之端點與網路 DLP 基礎，延伸至 CloudSOC CASB、Information Centric Analytics，乃至如今之資料安全態勢管理與生成式 AI 監控——正是此種持續性投資之最佳寫照。

對於正將本手冊與其他競爭提案一併評估之組織而言，值得向任何供應商提出的問題，正是本手冊嘗試直接回答的那些問題：其偵測準確度是否足以避免以大量誤報淹沒貴公司之維運團隊？其涵蓋範圍是否確實涵蓋貴公司資料所在及移動之每一個管道，包括貴公司員工已在使用之雲端及生成式 AI 應用程式？是否能以貴組織實際運作之規模，自動化修復事件？其部署方式是否足夠彈性，能同時符合貴公司今日與五年後之基礎架構？以及其總持有成本，反映的是一套整合式平台，還是拼湊多項彼此獨立工具所隱藏之授權、整合及管理成本倍增效應？Symantec DLP 之建置與持續擴充，正是圍繞著對上述每一個問題給予肯定答案而展開。

立即開始保護您的資訊

Symantec 解決方案，將資安與法規遵循政策，延伸至防火牆邊界之外，讓貴組織得以比一套零散拼湊之單點工具，更全面、更有效地探索、監控並保護其最機敏的資訊。Symantec DLP 建構於經驗證之部署方法論、直覺易用之政策與事件管理主控台，以及涵蓋每一項高風險管道（包括正在重塑員工工作方式之生成式 AI 應用程式）之全方位保護範圍之上，其設計目標，是在同類企業資料保護策略中，實現最低的總持有成本。

無論貴公司當前的優先要務，是彌補特定的合規缺口、整合一套零散的舊有工具、將既有地端DLP投資延伸至雲端，抑或及早因應生成式 AI 所帶來之風險，起點皆相同：單一平台、單一政策引擎，以及一套能隨貴組織成長、而非限制貴組織發展的主控台。

如欲討論針對貴公司環境量身打造之部署方案，或為貴公司之資安與法規遵循利害關係人安排 DLP Enforce Platform 產品展示，請聯繫保安資訊業務，或造訪 <https://www.savetime.com.tw/>。



關於賽門鐵克

賽門鐵克是資安業界的長青樹，品牌享譽至今超過四十年。賽門鐵克(Symantec)已於2019/11併入全球網通晶片巨擘-博通(Broadcom，美國股市代號AVGO，全世界網際網路流量有99.9%經過博通的網通晶片)軟體事業部的企業安全部門(SEO)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系統整合性，有著脫胎換骨並超越業界的長足進步。博通(Broadcom)是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec持續創新的技術能為日新月異的資安問題提供更好的解決方案，近年來Symantec很少出現在由公關機制產生的頭版文章中，而且在全球前南千大企業的市佔率及營收成長均遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦(CA Technologies)以及雲端運算及「硬體虛擬化」的領導廠商-VMware，也是博通軟體事業部的成員)。2021年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署(CISA)宣布聯合民間科技公司，發展全國性聯合防禦計畫JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵召的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技术型領導廠商，被業界公認為賽門鐵克解決方案專家。自1995年起就全心全力於賽門鐵克資訊安全解決方案的技术支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業IT專業人員的知識傳承(Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更熟悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。

免責宣言:本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2026/7