FORCEPOINT 資料外洩防護

在無邊界世界的資料保護

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

Forcepoint DLP

以人為中心的安全防護

資料安全是一場永無止境的挑戰。一方面IT組織需要遵循法規並保護智慧財產免於目標式攻擊(APT)以及意外洩漏，另方面他們也需因應宏觀IT的變化，如雲端應用程式的應用、混合雲環境以及BYOD趨勢，而這些都增加了組織外洩資料的機會。

這使得被攻擊的機會大幅度增加，如何有效保護重要資料成為重大的挑戰。資料安全團隊採用看似合乎邏輯的方法來追查資料：找到資料、將之分類並控制資料。然而這種傳統的方法對防止資料外洩已不再有效，因為它忽略了資料安全中最大的變數——你的員工。

不再只關注資料，安全的起點與終點都在於人，關鍵就是要了解使用者與資料和應用程式的互動情形。一旦達成，您便可以根據特定使用者的風險以及資料的機敏度或價值來採用不同程度的控制。

組織的資料保護計劃必須考慮以人為中心——也就是使用者、資料和網路的交集處。此外，企業必須對資料在企業中的傳輸保持警覺，並特別關注產生資料、存取資料和傳輸資料的人員。

資料保護必須做到：

- 透過單點控制所有員工用來產生資料、儲存資料和搬移資料的應用程式，以**保護需受監管的資料**。
- 透過能分析員工如何使用資料的先進DLP系統以**保護智慧財產**，引導您的員工依據資料機敏性正確的處理資料，並依據風險決定事件的優先順序。

任何地方都能掌握能見度並加以控制您的員工工作及資料所在地

- 雲端應用程式(透過Forcepoint CASB提供保護)
- 端點
- 網路
- 資料盤點

Forcepoint DLP解決了以人為中心的風險，在您的員工工作及資料所在的任何地方提供可視性和控制。安全團隊可應用使用者風險評分來關注最重要的事件，並加速遵守全球資料法規。

加速符合規範

現代IT環境對於以遵守繁複的全球資料安全法規為目標的企業來說是一項艱鉅的挑戰，特別是當他們朝向雲端應用和行動工作方式時。許多安全解決方案提供某種形式的整合式DLP，例如整合在雲端應用程式中。然而，在跨端點、雲端應用程式和網路去部署管理各別且不一致的政策時，安全團隊將面臨額外的複雜性並增加成本。

Forcepoint DLP透過結合內建完整的全球法規範本與整個IT環境的集中控制功能，來加速合規性相關工作。Forcepoint DLP可以有效地保護機敏的客戶資訊和受監管的資料，因此您可放心地證明現況符合規範。

- **法規涵蓋度**完整，可快速滿足並保持符合適用於83個國家監管要求的370多項政策。
- 使用網路、雲端和端點資料盤點功能來**查找和保護受監管資料**。
- 跨整個IT環境**使用集中控制與一致的政策**。

引導員工保護資料

僅具有阻止控制功能的DLP將使那些真正想完成工作的使用者感到不便，而用各種方法去規避DLP。一旦成功繞過安全控管會導致不必要的風險和非故意的資料外洩

Forcepoint DLP將您的員工視為當今網路威脅的第一線。

- 無論是在雲端還是在網路上的資料，可透過電子郵件和端點來**盤點和控制資料。**
- **教導員工做出明智的決策，**運用能指導使用者操作的訊息、教育員工了解政策並在與機敏資料互動接觸時確認使用意圖。
- 使用以政策為基礎的自動加密技術**與受信任的夥伴安全地協同合作，**使資料在傳出組織外時受到保護。
- 透過與領先的第三方資料分類解決方案整合（例如，Microsoft Azure Information Protection、Bolden James、Titus），以**進行資料分類和標記。**

先進的資料偵測和控制

惡意和意外的資料外洩是複雜的事件，而不是單一事件。Forcepoint DLP是一個經過驗證的解決方案，包括Gartner、Forrester和其他調研分析公司都認同為產業領先者。Forcepoint的DLP產品提供2個版本：『DLP for Compliance』與『DLP for IP Protection』。

『Forcepoint DLP for Compliance』法規遵循版本提供關鍵功能以滿足合規性要求，特色功能如下：

- **OCR光學辨識技術**可找出在存放或傳輸中被嵌入在圖像中的文字資料（傳輸中辨識功能僅Forcepoint DLP – Network模組提供）。
- **強化個人資料（PII）**的識別提供資料驗證檢查、實名偵測、相似分析和情境辨識。
- **自訂加密格式識別功能**可找出企圖規避DLP管控與盤點的資料。
- **累積分析**可偵測滴漏式DLP（例如以長時間且緩慢方式一點一滴外洩資料）。
- **與Microsoft Azure Information Protection整合**可分析加密文件並將相對應的DLP控制動作套用於資料上。

『Forcepoint DLP for IP Protection』智慧財產保護版本採用最先進的潛在資料外洩偵測和控制功能，特色如下：

- **機器學習**允許使用者訓練系統來識別同類型、而從未見過的資料，使用者為引擎提供正面與負面樣本來學習，從而辨識類似的業務文件、程式碼等。
- **結構化和非結構化資料的指紋識別**可允許資料擁有者定義資料類型，並識別各類文件（如業務文件、設計計劃和資料庫）中完全和部分符合的資料，然後將正確的控制功能或政策應用在這些符合的資料上。
- **分析功能可識別使用者行為的改變，**因為它與資料的使用互動有關，例如更頻繁使用個人電子郵件。

應變與降低風險

傳統的DLP方法因為太多誤判而增加使用者工作負擔，同時造成資料遺失風險。Forcepoint DLP應用先進分析可關聯看似無關的DLP事件為有優先次序的事件。Forcepoint DLP提供的事件風險等級（IRR）將不同的DLP指標融合到貝氏定理框架中，以評估資料風險情境的可能性，例如資料竊取和業務流程瑕疵。

- 透過凸顯高風險使用者、有風險的關鍵資料與使用者的常見行為模式來排定事件優先次序，**藉此應變團隊可專注在最高的風險上。**
- 藉由連接不同的事件、顯示風險資料的情境脈絡，並為分析師提供他們需要的訊息以採取行動來做到**調查與應變。**
- 透過使用者匿名功能和分權存取控制來**保護使用者隱私。**
- 透過與Forcepoint Insider Threat和Forcepoint UEBA的深度整合，將資料的情境脈絡**加入更廣泛的使用者分析中。**

在您員工工作的任何地方掌握能見度，控制在任何地點的資料

Forcepoint DLP提供所有防護部署的單點控制，其中包含各種先進分析功能與法規遵循政策範本。企業可根據其IT環境選擇部署方案。

附錄A：DLP解決方案組成元件概觀

Forcepoint DLP Endpoint	Forcepoint DLP - Endpoint端點模組保護你在Windows及Mac上的關鍵資料，不論是否在企業網路中它包含對靜態資料(資料盤點)、傳輸中及使用中資料的進階保護與控制，能與Microsoft Azure Information Protection整合以分析加密資料並施以適當DLP控制措施。解決方案能監控網頁上傳的資料，包括以HTTPS，以及上傳到如Office 365及Box企業版的雲端服務。能與Outlook、Notes及電子郵件用戶端完整整合。
Forcepoint DLP – Cloud Applications	透過Forcepoint CASB 防護，Forcepoint DLP – Cloud Applications雲端應用程式模組將Forcepoint DLP的先進分析及單一控制能力延伸到關鍵雲端應用程式，如Office 365、Salesforce、Google Apps、Box等。
Forcepoint DLP – Discovery	Forcepoint DLP – Discovery 資料盤點模組能找出你網路中的機敏資料並加以保護，也包括儲存在Office 365及Box企業版中的資料。先進的指紋識別技術可辨識出儲存中的監管資料和智慧財產，並透過套用適當的加密和控制措施來保護資料。
Forcepoint DLP – Network	Forcepoint DLP – Network 網路模組提供關鍵閘道端的防護，以阻擋透過電子郵件與網頁通道傳輸竊取資料。該解決方案有助於識別和防止來自外部攻擊或不斷增長的內部威脅所造成的惡意和意外資料外洩。OCR(光學字元辨識)能識別在圖像中的文字資料。 DLP分析功能可阻擋資料竊取及其他高風險的使用者行為。

附錄B：DLP解決方案組成元件細節

	FORCEPOINT DLP – ENDPOINT	FORCEPOINT DLP – CLOUD APPLICATIONS	FORCEPOINT DLP – DISCOVER	FORCEPOINT DLP – NETWORK
如何部署？	Endpoint Agent	Forcepoint Cloud	由IT管理盤點伺服器	本地設備 或公有雲
主要功能是甚麼？	蒐集使用者端點的資訊	在雲端或雲端應用程式中盤點資料或執行政策	資料盤點、掃描及保護在資料中心的靜態資料	提供透過網頁及電郵傳輸的動態資料能見度，並加以控管
可以盤點／保護何處的資料？	Windows endpoints MacOS endpoints Linux endpoints	Exchange Online Sharepoint Online Box	本地檔案伺服器與網路儲存設備 Sharepoint伺服器 Exchange伺服器	
在哪裡的傳輸中資料受到保護？	電子郵件 網頁HTTP(S) 印表機 可移動儲存設備 行動裝置 檔案伺服器／NAS	上傳及與Google Apps分享 上傳及與Office 365／OneDrive分享 Salesforce.com 與 Box		電子郵件／行動裝置郵件／ActiveSync代理伺服器 網頁HTTP(S) ICAP
使用中的資料在哪裡受到保護？	即時通訊、VOIP檔案分享、應用程式(雲端儲存的用戶端)、作業系統裡的剪貼簿	使用雲端應用程式的協同合作活動		
事件風險評級*	內含	內含		內含
光學字元辨識			內含	內含
資料分類整合	Microsoft Azure Information Protection, Bolden James, Titus			
哪些資料可做指紋識別？*	結構化(資料庫)、非結構化(文件)、二進位資料(非文字檔案)			

*此功能在IP保護版本提供更多細節請見附錄C

關於FORCEPOINT

Forcepoint正透過關注最重要的事情來改變網路安全：理解人們在與各地關鍵資料及智慧財產權互動使用時的意圖我們功能強大的系統讓公司能讓員工無障礙地存取機密資料，同時保護智慧財產權並簡化合規性。總部位在德州奧斯丁的Forcepoint已支援全球超過20,000個組織。如需了解更多Forcepoint資訊，請上www.forcepoint.com，及在Twitter追蹤我們：@ForcepointSec

與我們聯繫

886-2-8758-2970 fkuo@forcepoint.com

www.forcepoint.com/contact

[BROCHURE_FORCEPOINT_DATA_LOSS_PREVENTION_EN] 400026.112917