Forcepoint DLP and Forcepoint DLP Endpoint

取得資料安全防護的能見度和控管度

FORCEPOINT
POWERED BY Raytheon

Forcepoint DLP and Forcepoint DLP Endpoint

無論是在辦公室、行動中或雲端，都具備無與倫比的關鍵資料能見度和控管度

為鼓勵全球協作，您的關鍵資料儲存在類似 Office 365 和 Box 的雲端服務中，方便在行動中存取。Forcepoint DLP 是領先業界的資料外洩防護 (DLP) 解決方案。無論資料是儲存並透過類似 Windows 和 Apple 筆記型電腦存取，或透過電子郵件和 IM 共用，它都具備無與倫比的能見度和控管度，以有效保護您的資料安全。

無論敏感資料處於端點、雲端或辦公場所內，Forcepoint DLP 都能妥善進行防護。

Forcepoint DLP 提升您組織的防護能力

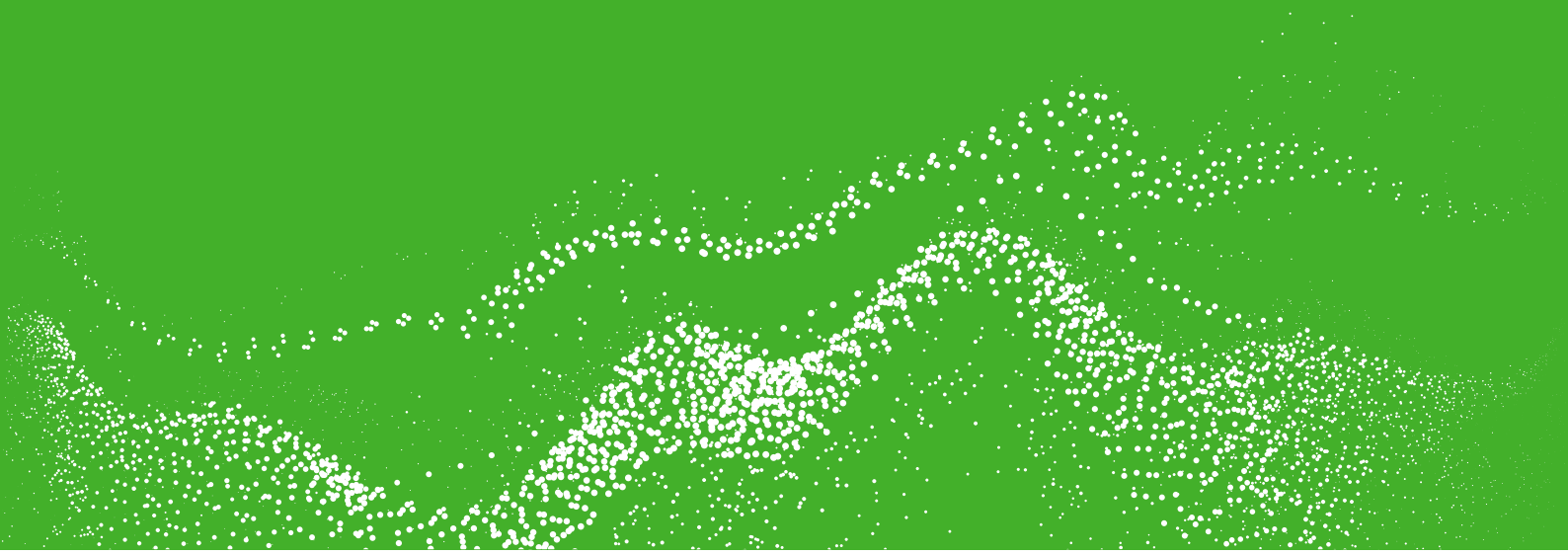
- 運用 Forcepoint 專屬研究團隊提供的維護和更新的預先定義政策，快速處理全球和產業的特定法規遵循的要求。
- 借助資料分類工具，辨識並保護儲存於各處的智慧財產。
- 行為規範政策結合內容和情境感知的功能，能自動辨識使用者的高風險行為，例如：轉寄電子郵件至個人帳戶，或使用加密方式封裝資料，以達成資料外洩的目的。
- 輕鬆盤點儲存在 Mac、Windows 和 Linux 端點裝置上的機敏檔案，並確保其安全。
- 辨識和避免儲存在類似 Office 365 和 Box 等雲端服務中的資料遺失。
- 有效實行基於職務的存取控管及全面稽核，以符合內部和外部的法規遵循要求。
- 無縫整合 Microsoft、HP、Splunk、IBM、Titus、Boldon James 和 Citrix 等第三方的資料安全解決方案。
- 使用資料模組和統計資料分析的 DLP 資料分析作業，能自動辨識極具資料遺失或竊盜風險的使用者行為，促使您的安全作業團隊能充分借助 Forcepoint 的研究專長。
- Forcepoint 的 TRITON 架構能讓您整合安全解決方案、協調防禦政策、跨平台情資共用，並具有資料安全集中化管理的便利性。

主要特色

- **事件風險排行**使用先進的資料分析作業，為您的安全團隊提供大量排名報告，讓您知道組織內排名在前的資料安全風險有那些。
- **整合式光學字元識別（OCR）**辨識類似 CAD 設計圖、掃描文件、MRI 和截圖等圖片內的敏感資料和 IP 標記。
- **防止分批資料外洩行為**會監控一段期間內所累積的資料傳輸活動，以查出少量持續的資料外洩行為。
- **基於安全行為的政策**結合了內容和情境感知功能，自動辨識使用者將敏感資料置於風險中的行為。
- **無論員工是在辦公室內或離開企業網路工作，我們獨特的 PreciseID 指紋辨識**能偵測到 Mac 和 Windows 端點上的結構（資料庫記錄）或非結構資料（文件）的部份指紋。
- **自動加密**傳送至移動裝置的資料，確保與合作夥伴共用的資料安全。
- **基於電子郵件事件的工作流程**，讓您能輕鬆將須檢閱和補救的事件分發至資料擁有者及與該業務利益相關的人士，而無須提供 DLP 管理系統的存取權限。
- **偵測並預防**敏感資料被他人透過電子郵件、網路上傳、IM 和雲端服務客戶端（其中包括：網路流量和端點上的 Native SSL 解密），傳送至組織外。
- **在 Microsoft 部署 DLP 元件**，將 DLP 原則套用至 Microsoft Office 365。

「Forcepoint 資料安全是我們找到能阻止和預防資料外洩的最強效解決方案。」

— Amir Shahar， Cellcom Israel Ltd. 資訊安全經理。



FORCEPOINT DLP 的優異功能

自信地運用創新技術

要滿足客戶需求並永保市場競爭力，您需要推動創新，並讓您的員工採用新的技術。Forcepoint 的 DLP 解決方案 Forcepoint DLP，將資料安全控管延伸至企業雲端應用程式和您的端點。此舉有助於您安全採用強效的雲端服務，例如：Microsoft Office 365、Google for Work 和 SalesForce.com，以及保護您存儲於 Windows 和 Mac 筆記型電腦的敏感資料和智慧財產，無論是在連網時或下線時。

Forcepoint 為促進組織內和與信賴的合作夥伴能安全共用和融合資料，在基於安全政策的情況下，加密傳送至移動儲存裝置的敏感資料，這些資料在執行 AP-ENDPOINT 的端點上能夠自動解密。

減緩部署和管理的負擔

我們提供最精確和正確的企業 DLP 安全政策，並且政策的部署在 DLP 廠商中是最簡易的。我們的「可立即實施政策」文件庫和易用型精靈以地區和產業作為篩選條件，建議一組 DLP 政策，並在單一範本內，快速維護您的智慧財產和法規資料的安全。Forcepoint 也是第一位 DLP 供應商，可提供您結合內容和情境感知之行為基礎政策的功能，自動辨識出使用者將敏感資料置於風險中的行為。基於電子郵件事件的工作流程，讓您能輕鬆將須檢閱和補救的事件分發至資料擁有者及與該業務有利益關係的人士，而無須提供 DLP 管理系統的存取。利用標準化的報告，滿足稽核人員的要求，您也能視需要而客製化專屬報告。

利用業界最先進技術，全面保護資料安全

傳統 DLP 解決方案無法辨識儲存為 .jpeg 格式的惡意螢幕截圖、或掃描並儲存為圖片的醫療圖像、銀行圖像或舊記錄，但這對 Forcepoint DLP 而言並非難事。

有了 Forcepoint 的光學字元識別 (OCR) 分析技術，您就能可靠地辨識出圖片中的敏感資料，並確保其安全。這項特有的功能，讓您可有效避免敏感資訊透過螢幕截圖、傳真頁面、智慧型手機與平板電腦內的相片，以及支票、收據與掃描的舊檔案等文件而外洩，保護企業免於進階攻擊與內部資料竊取之苦。

取得更高的能見度以監測進階的資料竊取策略，例如：自訂加密模式以模糊處理資料，或透過少量分批傳送資料來躲避偵測。

將資料移動和使用者行為互為連結，全面保護資料安全

Forcepoint 是第一家整合先進的 DLP 解決方案和 Forcepoint Insider Threat 的廠商，提供違反安全政策事件的脈絡及記錄用戶使用資料的企圖等風險情境感知的能力。這套領先業界的應用程式組合，為您提供使用者嘗試傳送敏感資料的情境。「全面的威脅感知能力」透過DVR 擷取和播放的檢視功能，提供掌握使用者活動和您資料移動時的情境，能辨識出系統被挾制、憑證遭竊、惡意內部人員或員工犯錯的早期警告訊號。

Forcepoint DLP 和 Forcepoint DLP Endpoint 的元件

結合 Forcepoint DLP（AP DATA DISCOVER 和 AP-GATEWAY）和 Forcepoint DLP Endpoint，能將 Forcepoint 的企業級 DLP 控管延伸至資料風險性最高的管道，分別是：網路、電子郵件、雲端應用程式和端點。Forcepoint 是唯一提供企業級安全政策和技術的廠商，以維護整合式管道的安全（網路和電子郵件），並將這些政策和報告引進企業 DLP 解決方案中，同時為您提供產業最先進的技術，維護關鍵資料之安全。PreciseID 指紋辨識能偵測處於辦公場所、雲端、Windows 或 Mac 端點或網路外的非結構或結構資料的片斷。

FORCEPOINT DLP ENDPOINT	Forcepoint DLP Endpoint 保護您在 Windows 和 Mac 端點上，以及企業網路以外的關鍵資料。PreciseID 指紋辨識甚至能讓您偵測網路外端點的非結構或結構資料的片斷。同時，它也能監控包括 HTTPS 在內的 Web 上傳，以及 Office 365 和 Box Enterprise 等雲端服務的上傳。與 Outlook、Notes 和電子郵件客戶端全面整合，同時使用與 Forcepoint 的各資料、網頁、電子郵件、端點解決方案同樣的使用者介面。
FORCEPOINT DLP	Forcepoint DLP Endpoint 能辨識並保護存在貴公司網路環境中的敏感資料，以及儲存於 Office 365 和 Box Enterprise 等雲端服務上的機密資料。加上 Forcepoint DLP Endpoint 的功能後，Forcepoint DLP 的強大技術即可延伸至線上和離線的 Mac OS X 與 Windows 端點，以保障資料不管在何處皆能受到完整的保護。藉著產業最先進的指紋辨識技術，確保敏感資料不會外洩。
FORCEPOINT DLP NETWORK	終止透過電子郵件和網路而發生的資料竊盜很重要。Forcepoint DLP Network 能幫助您辨識並預防來自外部的惡意程式攻擊及資料竊取事件，甚或防禦逐漸增多的內部威脅。藉由功能強大的光學字元識別 (OCR) 分析技術，能有效辨識出藏於圖片內的敏感資料，以防止這種被很多進階威脅攻擊用來躲避偵測的手法。此外，透過 Drip DLP 技術，能阻擋資料被持續緩慢少量外洩，同時也可用於辨識高風險使用者的行為監控。

「知道 Forcepoint 正在保護我們的資料安全，晚上睡得更安穩。」

—Ahmet Taskeser，Finansbank 資深 SIMM 主管

Forcepoint 解決方案的獨特功能

ACE（先進分類引擎）

Forcepoint ACE 採取綜合風險評分技術以及預測分析方式，針對 Web、電子郵件、資料以及行動安全，提供即時性的內聯式情境防護措施，發揮市面上最有效的安全防護。同時，擁有業界領先的資料感知防護功能，可分析企業內外網的進出流量，有效的阻擋威脅與攻擊。ACE 技術是多年研發的心血結晶，其即時安全、資料與內容分析的分類器，即是為何 ACE 能夠每天偵測出比傳統防毒引擎更多威脅的重大功臣（更多威脅分析資訊，請參考 http://securitylabs.forcepoint.com）。ACE 由 Forcepoint 全球智能網路威脅情資 (Forcepoint ThreatSeeker Intelligence) 提供支援，是所有 Forcepoint 解決方案的重要防護。

整合 8 大先進安全防護分析技術

- 提供 10,000 種安全分析檢查，可深入剖析安全威脅。
- 預測性安全引擎，可預知威脅變化。
- Inline 防護能力使您不僅能夠監控，還能**阻斷**威脅。

Forcepoint ThreatSeeker Intelligence

由 Forcepoint Security Labs 管理的全球智能網路威脅情資 (Forcepoint ThreatSeeker Intelligence)，替所有 Forcepoint 的安全解決方案匯整了全球的資安情報。彙集超過 9 億個端點，包含來自 Facebook 的大量網頁分析請求，並結合先進分類引擎 (Forcepoint ACE) 的安全防護，每天可分析多達 50 億個網頁請求。憑藉如此龐大的資安威脅偵測資料庫，全球智能網路威脅情資 (Forcepoint ThreatSeeker Intelligence) 可提供即時更新阻斷進階威脅、惡意程式、網路釣魚攻擊、蠕蟲和詐騙病毒等的資安防禦情報，以及提供最新的 Web 安全評析。全球智能網路威脅情資 (Forcepoint ThreatSeeker Intelligence) 具有業界最充足的網路威脅資料，藉由 ACE 引擎即時分析龐大網頁樣本請求，其價值及效果無人能出其右。當您使用 Websense Web Security 防護模組時，Forcepoint ThreatSeeker Intelligence 全球智能網路威脅情資，將能有效降低企業面臨 Web 威脅與資料竊取的風險。

TRITON 架構

Forcepoint TRITON 擁有來自 Forcepoint ACE 的 Inline 即時安全分析技術，在任何時候使用者點擊瀏覽網頁時，可得到即時的安全防護效果。透過 Forcepoint 全球智能網路威脅情資 (Forcepoint ThreatSeeker Intelligence) 的豐富資料，以及 Forcepoint Security Labs 研究人員的專業支援，讓 Forcepoint TRITON 防護能力發揮到極致。它統一的使用者介面及架構平台，讓其成為市場上最優異的安全防護解決方案。

聯絡方式

www.forcepoint.com/contact

[BROCHURE_FORCEPOINT_DLP_TCH] 400004.031517

FORCEPOINT

POWERED BY Raytheon