



內部威脅資料防護

取得無與倫比的使用者行為分析和資料移動擴散的能見度



內部威脅資料防護

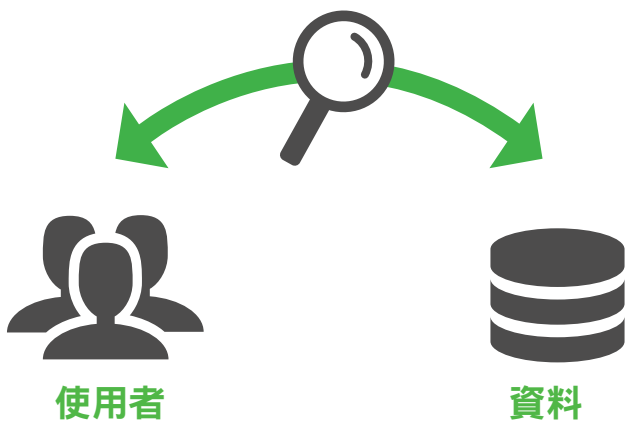
無與倫比的使用者行為分析和資料移動擴散的能見度，帶來領先業界的安全防護

FORCEPOINT「從內到外」法則

Forcepoint 創新的網路安全「從內到外」法則，全面改革關鍵資料防護之道。無論使用者身在何處，我們的「內部威脅資料防護」都能從內到外，將資料移動和他們的行為互為連結，分析彼此的關聯。

內部威脅早期警告系統

使用者一產生風險行為，系統會即早警告您發生在組織內部的資料威脅事件。阻止關鍵資料從組織內外洩出去，辨識惡意和粗心大意的使用者，將威脅風險降至最低。



您為什麼要在意此事？

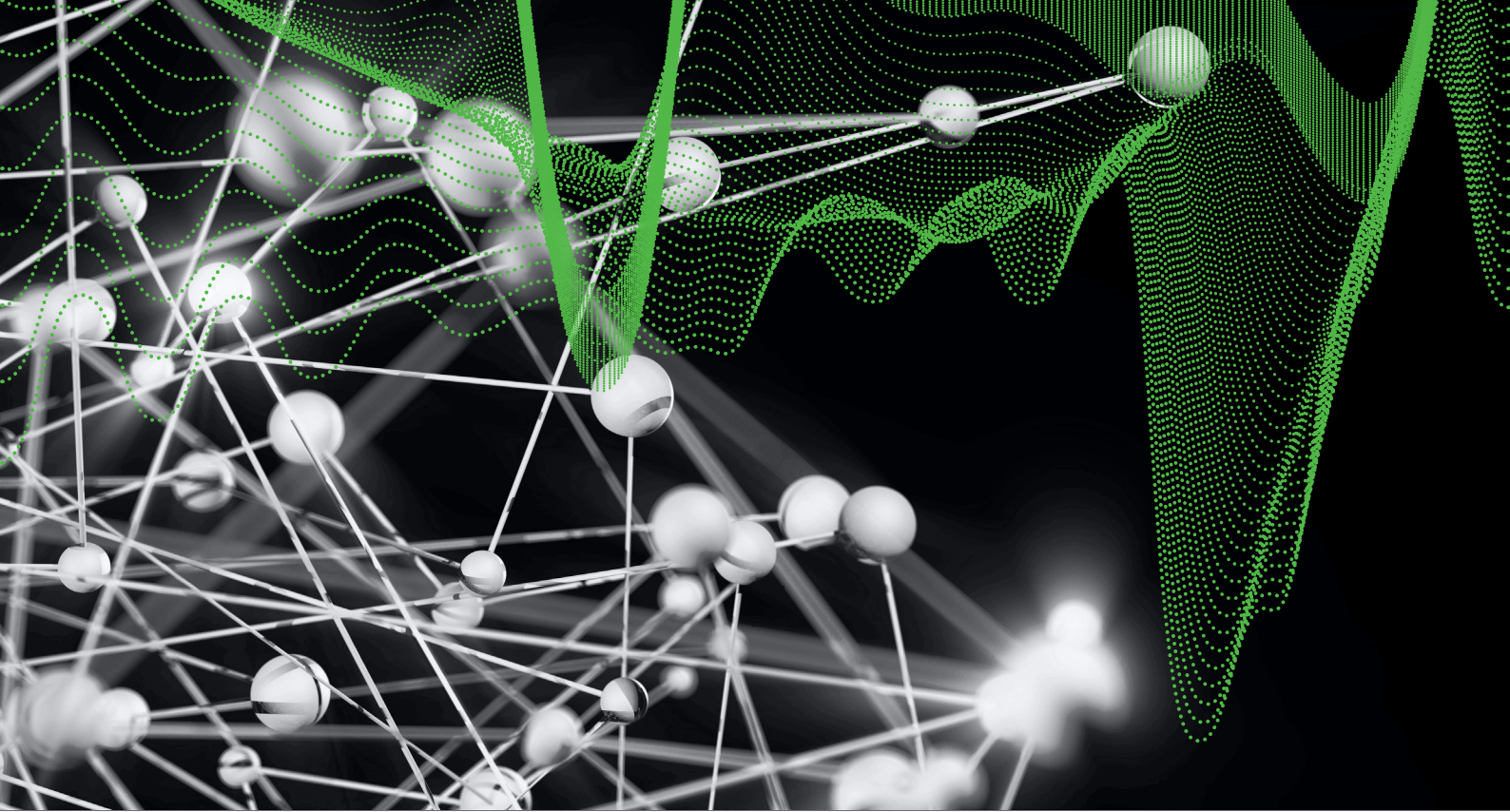


在 2015 年，最常外洩的三種資料分別是：可辨識個人身份的資訊 (PII)、驗證憑證，以及智慧財產 (IP) 資訊。此外，37% 的外洩資料都是因內部有意或無意行為¹而起。

如何妥善確保您的團隊能存取所需資料，同時保護資料安全？

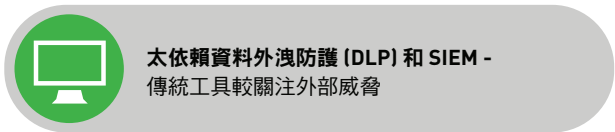
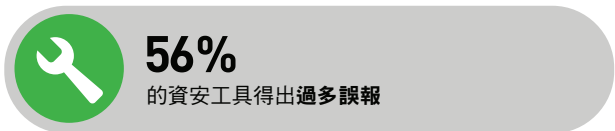
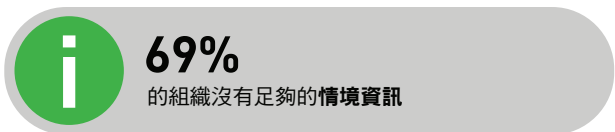
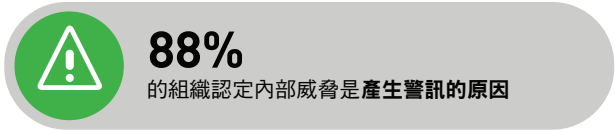
Forcepoint™ 提供唯一的早期警告系統，防範可能導致威脅的內部風險行為。

¹ Forrester：市場總覽 - 資料外洩防護，2016 年 5 月



為解決問題而須面對的挑戰

來自內部的威脅



能見度



預算



40% 以下
針對內部威脅防護備妥
專用預算

72% 表示他們使用驗證和身份管理工具，以管理特殊權限使用者的濫用行為；其中大部份人使用未能防範內部威脅的現有網路安全工具。





取得無與倫比的使用者行為分析和資料的能見度

我們的解決方案- Forcepoint™ Insider Threat Data Protection

Forcepoint 的 Insider Threat and Data Protection 是業界第一套能針對內部威脅發出早期警告的解決方案，預防您的智慧財產和法規資料外洩。它能提供使用者和資料的能見度，將資料移動擴散和使用者行為互為連結，全面保護資料安全。Forcepoint 保護貴組織免於因系統被挾制憑證遭竊、惡意的內部人員威脅，以及意外的資料遺失。業界公認「內部威脅資料防護」的高度可擴充性和可信賴性，無論是在辦公室、行動中或雲端，都能為您帶來所需的資料能見度，全面掌握員工正在如何使用敏感資料。



Forcepoint 的 Insider Data Protection 結合業界領先的企業 DLP 解決方案，以及無與倫比的 SureView Insider Threat 解決方案，前者為您帶來資料移動時的能見度和控管能力，後者則套用行為分析的資料和取證功能，進一步辨識具風險的使用者行為。與市面上任何其他解決方案相比，我們強效的組合能更早偵測到更多內部威脅。

業界最穩定且可擴充的解決方案，與組織同步成長



資料移動



使用者行為



全面性的資料保護

Forcepoint DLP 的優勢 (TRITON AP-DATA 和 TRITON AP-ENDPOINT)

業界最先進的指紋辨識功能

- ▶ **PreciseID 指紋辨識**能偵測辦公室、行動中或雲端的非結構或結構資料片斷。
- ▶ **業界一流的端點代理程式**，為安裝 Windows 和 Mac 作業系統的筆記型電腦，提供無與倫比的敏感資料能見度和控管。

先進的敏感資料防護技術

- ▶ **「光學字元識別」(OCR)** 辨識隱藏於圖形中文字。保護隱藏於傳統掃描文件、.jpegs 檔案、CAD 設計圖、MRI 和截圖中的機敏資料。
- ▶ **Forcepoint 的「機器學習」** 功能在設置過程中無誤判的需求，可減少機器學習的入門障礙。
- ▶ **緩慢分批資料外洩行為** 對抗緩慢分批攻擊，也就是為避免偵測而將資料以少量分批方式對外傳送資料的行為。
- ▶ **一次性安全政策制定和部署**，將企業 DLP 控管延伸至常見的外洩管道，例如網路和電子郵件。

Forcepoint SureView® Insider Threat 的優勢

資料移動和使用者行為互為連結

- ▶ **早在發生 DLP 事件之前就能偵測到違規行為**，例如：員工儲存大量資料，或建立後門。
- ▶ **偵測到高風險使用者行為後**，快速驅動更明智的補救決策。

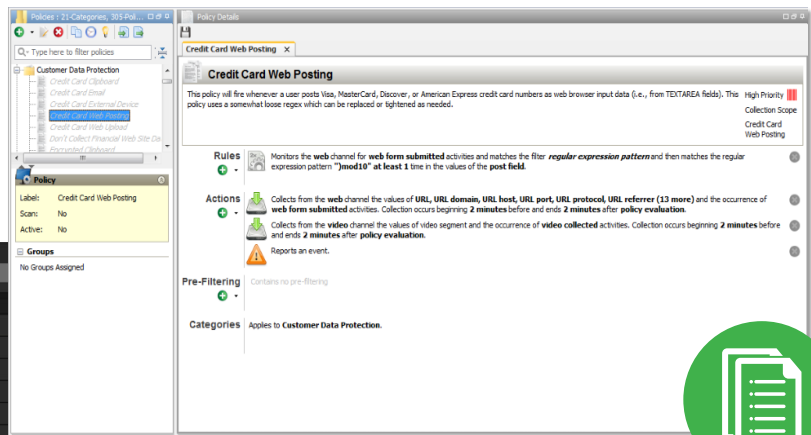
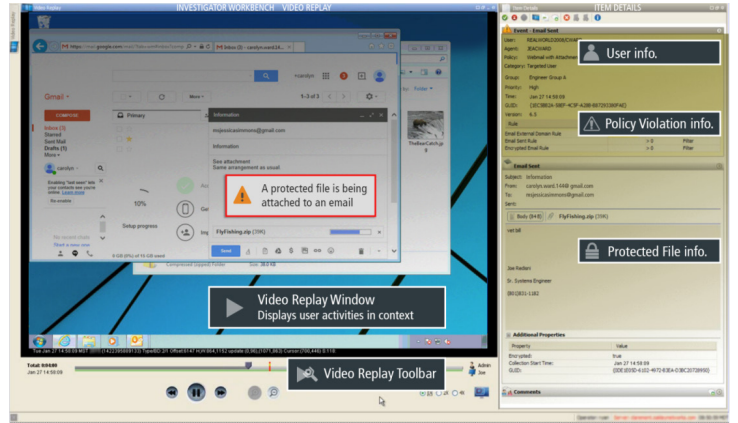
使用者行為風險分析評級引擎

- ▶ **早在敏感資料外洩或遭竊之前**，Forcepoint 就能即早針對被挾制的系統、憑證遭竊、惡意內部人員或員工犯錯提出警告的訊號。
- ▶ **省時省力**，能自動計分，為您找到風險最高的使用者，而不必從上千個警示中費力尋找關鍵風險。
- ▶ **跨單位建立個人和組織行為規範的基本線**，以辨識風險行為。
- ▶ **每天為每位使用者提供綜合性風險分數**，並迅速突顯 30 天的風險趨勢。




搭配取證功能的螢幕截圖擷取和播放功能

- ▶ 螢幕截圖的擷取和播放能提供完整風險情境感知能力，讓您以無與倫比的能見度洞察可疑的行為以免其演變成實際問題。
- ▶ 取得佐證，確定攻擊的是來自被挾制的系統、憑證遭竊、惡意內部人員或無知的犯錯。
- ▶ 若有必要，SVIT 取證是法院受理的證據。
- ▶ SVIT「命令中心」自動依照風險排定使用者次序，而不必從上千個警示中費力尋找關鍵風險。
- ▶ 輕鬆追溯具風險的使用者行為，以及可擴展的時間表，進而顯示員工之所以成為高風險使用者的活動。



過去 15 年以來，Forcepoint 一直竭誠保護全球商務企業、及高度注重安全防護的政府、軍事和情報組織之敏感資訊。



**保護全球最敏感的組織超過 15 年的
經驗，備受各界信賴。**

聯絡方式

www.forcepoint.com/contact

Forcepoint™ 是 Forcepoint LLC 的商標。SureView®、ThreatSeeker® 與 TRITON® 是 Forcepoint LLC 的註冊商標。Raytheon 是 Raytheon Company 的註冊商標。所有其他商標和註冊商標均歸其各自所有者所擁有。

[BROCHURE_INSIDER_THREAT_DATA_PROTECTION_TW]
400012.062916

