Proofpoint ITM
內部威脅管理

專為當代企業設計、以人為本的內部威脅管理

關鍵優勢

- 偵測內部風險活動並防止資料從端點外洩
- 簡化內部威脅和資料外洩事件之回應流程
- 雲端原生、架構彈性的「軟體即服務」（SaaS），能夠快速部署，為您節省大量時間
- 以輕量的 Agent 端點程式維持員工的工作效率

ITM 重要功能

- 識別使用者風險
- 防止資料從端點外洩
- 對人為事件加速回應
- 發展內部威脅應對方案

Proofpoint 內部威脅管理（Insider Threat Management，ITM），採用了以人為本的策略保護您的組織對抗資料外洩事件，防止由內部引發的惡意行為及品牌形象損傷。我們能讓您避免因為已授權使用者的惡意、疏忽或不知情行為而蒙受損失。透過關聯化使用者活動與資料動向，將協助您預防內部導致的資料外洩。此外，我們即時偵測具風險的使用行為，讓您輕鬆掌握違規行為的證據。

即時偵測並防止風險行為

藉由 ITM，您可以在風險行為發生的第一時間關聯化與之相關的應用程式、檔案、桌上型電腦、伺服器以及虛擬環境。這些資訊與使用者的操作同步生成，而非只在事件發生後才有所反應。我們對於事件即時的可視性，讓您能透過全新有效的方法來找出關聯性、偵測並解決內部威脅事件。

來源全面的真實威脅情境

您將能即時偵測風險行為，其中包括：

- 資料外洩
- 風險性的資料橫向移動
- 特權濫用
- 應用程式濫用
- 未經授權的存取
- 風險性的意外行為

透過我們以布林邏輯為基礎的規則管理工具，您將能依照企業環境量身打造，輕鬆創建所需的規則與觸發條件。除了從內建好的威脅情境著手，更改既有的情境設定，您亦可從零開始，自行創建所需規則與觸發條件。我們提供多樣的內部威脅規則適用廣泛的使用情境，匯集了從卡內基梅隆大學計算機緊急回應小組（Carnegie Mellon, CERT Division）、美國國家內部威脅專責小組（NITTF）、美國國家標準技術研究院（NIST），以及我們與客戶累積的知識。

操作簡單且直觀的威脅獵捕

威脅獵捕不只需要防範來自外部的風險。有了 ITM，就能識別內部人員是否承受著不必要或刻意的風險。可透過簡單直觀的使用者介面讓您輕鬆地主動探索並搜尋異常行為。

有了操作簡單且直觀的威脅獵捕功能，您就可以：

- 根據企業目前的環境設定，審查其中的風險行為與活動
- 使用智慧分組機制，過濾數以千計的行為紀錄，聚焦於事件相關的使用活動
- 透過時間軸和截圖留存的證據，釐清異常行為的完整脈絡

支援資料分類

我們的 ITM 可與微軟資訊保護模組 (Microsoft Information Protection，MIP) 整合。當使用者存取檔案時，ITM 的 Agent 會即時讀取其上的機敏性標籤。您可根據標記在檔案上 MIP 定義的機敏性程度、檔案來源、檔案類型及檔案目的地，設立對應的偵測和預防規則。

資料外洩防護 (Data loss prevention，DLP)

ITM 可防止機敏資料透過從端點的常見管道外洩，像是 USB 連接的設備，包含了本地同步資料夾、網路儲存裝置 (NAS)、隨身碟、多媒體裝置和電話等。就算您的員工離線作業，內部威脅管理功能也會正常運作。

您可按使用者、組織部門單位和主機，管理以下的 USB 相關活動：

- 封鎖資料寫入到 USB
- 建立可放行的 USB 裝置列表
- 封鎖特定檔名特徵的檔案
- 封鎖特定檔案類型
- 封鎖特定檔案來源
- 執行全球通用的預防規則

若使用 Proofpoint 資料外洩防護企業版 (Proofpoint Enterprise DLP) 套組，還可以將保護範圍延伸至電子郵件和雲端應用程式。

加速事件回應

許多組織在資安事件發生後才對內部威脅展開準備，而且大多數組織因此發現原有資安工具的工作流程無力應對內部威脅。內部資料的處理通常是企業敏感議題，且需要與非資訊安全的團隊更深入地協同合作。

即時情境脈絡和無可辯駁的證據

我們的系統流程是針對使用者導向的事件所設計。可使用關鍵字和篩選功能，在所有已收集的 metadata 和螢幕截圖中，搜尋資安事件，換而言之，您無須學習額外的查詢語法。此外，您還可儲存篩選條件，用來進行主動威脅獵捕或作為未來調查的參考依據。

當您發現與當前調查相關的重要事件或告警時，您可製作標記並進行分類。當需要分享這些證據時，您可透過這些標記找到這些相關的事件和告警，將它們導出爲通用的檔案格式，像是 PDF等。報告內容可包括螢幕截圖證據以及相關的完整脈絡，包含使用者、事件內容、地點和時間等。如此不只能讓資安團隊管控上變得更加便利，對人力資源、法律、合規等部門的團隊和調查人員而言也更容易解讀。

ITM 架構的優勢

為了達成規模化、易用性、安全性以及可擴充性，我們使用了雲端架構，並透過我們領先業界的輕量化 agent 端點程式來收集活動資料，能在不妨礙使用者操作且不受應用程式限制的情況下，讓您清楚洞悉使用者在系統上的行為。

純粹「軟體即服務」(SaaS) 佈署

Proofpoint 端點資料外洩防護 (Proofpoint Endpoint DLP) 作為一個先進的「軟體即服務」(SaaS) 平台，專門為規模化、數據分析、資訊安全、隱私和可擴展性而打造。不只減少在系統後端建置的時間和成本，亦簡化了安全管理員對整個組織規則管理的複雜程序，能夠即時、全面地掌握資料活動。

用一個輕量級方案解決兩個問題

端點 DLP 和 ITM 共同使用一個輕量級的 agent 代理程式以及先進的「軟體即服務」(SaaS) 架構。當您將二者搭配使用，端點 DLP 可防止使用者日常的資料外洩風險，而 ITM 則會擴展這項保護，應用在惡意或高風險使用者的任何風險行為。

瞭解更多

如需更多詳細資訊，歡迎瀏覽 **proofpoint.com**。