Proofpoint Insider Threat Management

使用以人為本的策略管理內部威脅

關鍵優勢

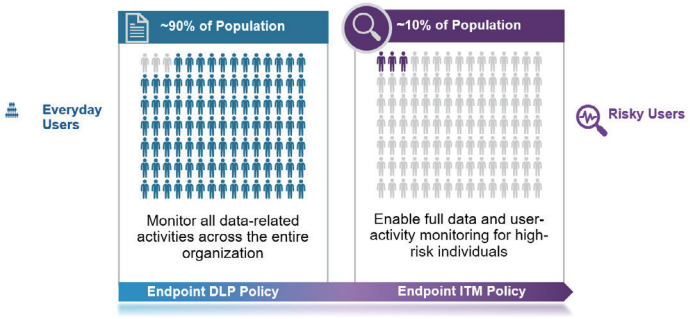
- 偵測企業內部風險活動，防止端點資料外洩
- 加快針對『內部威脅』和『資料外洩』事件之回應速度
- 輕量化端點代理程式，兼顧使用者工作效率和安全性
- 可透過現代化雲端平台，建置高度可擴充的SaaS，加快價值實現。

Proofpoint 內部威脅管理 (Insider Threat Management, ITM) 是『以人為本』的解決方案，協助降低內部威脅及端點資料外洩的風險，以有效防護重要機敏資料。透過綜觀分析使用者行為、資料內容與威脅等資訊的關聯脈絡，讓您深入洞察使用者活動。

ITM 能協助資安團隊因應偵測、預防內部威脅的挑戰，簡化內部人員資安事件的回應流程，並提供能防止後續損害的處理建議。ITM 解決方案也能找出使用者活動和機敏資料移動之間的相關性，您的團隊能藉此辨別使用者風險、偵測內部人員引發的資料外洩事件並加速調查。ITM 是 Proofpoint 資訊防護系列產品，建構於資訊防護及雲端安全平台內。

Gain Visibility and Context Into User Activity
使用者行為及事件脈絡洞察

Proofpoint ITM 協助您了解使用者觸發事件的完整脈絡。如日常風險較低的使用者，您可能只需要觀察他們與資料的互動情形；然而對於高風險使用者（例如高階主管或即將離職的員工），您應該蒐集這些使用者的行為或活動資訊，以更深入、全面地把關。Proofpoint ITM 可讓您透過一致、輕量代理程式，同時管控日常與高風險的使用者。



圖一: 使用單一 、輕量化代理程式，依使用者類型啟用不同功能來降低內部風險

Proofpoint ITM 可讓您建立觀察清單以監測高風險使用者。 這份名單可依據多種條件加以設定，例如：使用者身分與互動的資料類型、 員工對於網路釣魚或各類社交工程的弱點，或是涵蓋就業狀況、 人力資源、 法律等相關因素的變化。

Detect and Prevent Risky User Behavior In Real Time
即時偵測並預防具風險的使用行為

Proofpoint ITM 可讓您快速建立自定義偵測規則。根據資料外洩、可接受的使用情境和內部威脅等企業定義的資安策略，量身打造屬於企業的控管規則。『彈性的規則引擎』可依照實際環境中的使用者、資料、 日期/時間、 應用程式、端點以及內容機敏度、來源和目的地等資訊調整告警，以契合企業的環境。

Proofpoint ITM也內建『預設的告警模板資料庫』，易於設定且能快速佈署。 讓您可以即時掌握端點上高風險的資料移動和互動，包括：未經授權的存取、資料外洩和使用未經授權的軟體等操作行為。

移動中的機敏資料往往具備較高的風險。 ITM 可結合 Proofpoint Endpoint DLP模組透過掃描內容、 比對分類標籤 (如微軟資訊防護模組，MIP) 等方式，辨識移動中的資料是否屬於機敏資訊。 此功能僅在觸發特定規則時啟用，能避免佔用過多端點設備的系統資源，確保使用者安全的同時也維持工作效率。

Proofpoint ITM 可即時防止資料外洩，避免使用者對機敏資料進行違規的操作，像是上傳至網路、複製到 USB、 複製到雲端、 資料夾同步和列印等。 您也可以設定使用者辯護功能，啟用後，使用者須提供存取這些資料的理由並提交給安全團隊參考。

Accelerate Incident Response
加速事件回應

Proofpoint ITM 透過單一介面即可掌握事件狀態和歷史記錄，監測使用者活動、 分析告警關聯性並管理事件調查，以協助您完整了解事件全貌、 鎖定威脅並進行有效回應。 您也可以對告警進行標記和分類，以利其他安全分析師加入協作。

Proofpoint ITM 提供強大的搜索和篩選功能協助您獵捕威脅。 您可使用預設的威脅探索腳本，或透過自定義的資料探索，找出對企業有風險的特定活動，或是對新的風險進行回應。

在使用者時間軸上詳細記錄了告警觸發的事前、 事中和事後的活動資料，包括事件的相關人員、 事件描述、 位址和時間等資訊。 您還可以取得使用者活動的螢幕截圖，以更明確且不容置疑的證據協助調查進行。

Proofpoint ITM 從端點收遙測資料 (Telemetry)，並使用 Webhook 輕鬆將 ITM 平台的告警導入企業 SIEM 和 SOAR 等工具，助您更快識別、 分類事件。

Achieve Rapid Time To Value
快速實現價值

Proofpoint ITM 專為大規模資料的分析、 安全、隱私和擴展性而打造，同時提供一個彈性的佈署模式，適用多種企業應用情境。 減少系統後端建置的時間和成本，藉由單一管理平台簡化安全團隊對端點與存取的管理程序；透過調整配置滿足您對企業資安的特權設置及管理需求，並能佈署細緻的安全與存取政策以防護資料隱私，創建符合企業需求的工作流程

瞭解更多

如需更多詳細資訊，歡迎瀏覽 **proofpoint.com**.