

「人」是最寶貴的資產，也是最佳的防護

滿足以人為本的所有安全需求

駭客攻擊的目標已從網路節點逐步轉向「人」。資料外洩的主因是人，隨處可見的帳戶與應用程式也是「人」所建立的。因此，「以人為本」的資安不僅重要，更是關鍵所在。不同於網路或主機，人無法完全被阻擋在外，人們在不同的地方，用不同的工具、不同的方式工作，並仰賴電子郵件、協作工具及不斷增加的應用程式與雲端服務。與此同時，駭客也不斷開發新技術，瞄準人性弱點發動攻擊。

Proofpoint 以核心技術打造的模組與 App，聚焦於四大主要領域，提供完整的解決方案：

- 阻擋複雜的鎖定式攻擊
- 預防資料外洩，主動遏阻內部威脅
- 帳號接管 (ATO) 及安全態勢防護
- 提供即時指引，協助每位用戶在需要時採取正確行動

Proofpoint 「以人為本」安全平台讓客戶可以靈活選擇所需的模組/App，同時共享統一的技術平台。不僅協助企業全面防禦所有針對人的威脅，涵蓋各種用戶可能遭遇的情境，更能降低成本與導入時間，簡化了整體解決方案的操作流程，使企業更輕鬆地實現其資安目標。

Proofpoint 安全平台的強大功能來自兩大核心技術 — Nexus 與 Zen，兩者在對稱架構中協作，並結合強大的 AI 智慧模型，為終端用戶工作的每個環節把關，包括：電子郵件、網頁、協作、應用程式與雲端服務。

以人為本的安全平台架構



Proofpoint Nexus®

以人為本的安全，背後的核心偵測技術

在以人為本的安全策略中，偵測技術是核心支柱之一。除了識別威脅，更能透過深入分析人員行為、資料流動和網路活動，提前發現各種潛在的風險。

為什麼偵測技術對以人為本的安全至關重要？

- 「人」是主要攻擊目標：超過 90% 的資安事件都源於針對「人」的社交工程攻擊，如釣魚郵件或惡意附件。
- 行為驅動的威脅：內部威脅和帳戶劫持往往會先透過異常行為表現出來，需要先進的偵測技術才能及時發現。
- 數據驅動的決策：藉由整合、分析大量數據，偵測技術能提供可操作的洞察，幫助資安團隊快速回應威脅。

以人為本的安全策略，其核心在於保護「人」——無論是員工、客戶還是合作夥伴。Proofpoint 結合先進的偵測技術和人員行為分析，讓企業能夠更有效地識別、應對威脅，進而建立更強大的安全防線。

Proofpoint Nexus®：AI 驅動的全方位威脅情資平台

Proofpoint Nexus® 是一個強大的威脅情資平台，專為解決以人為目標的複雜威脅而設計。透過 **AI**、**機器學習**、**行為分析**、**威脅情資** 和 **威脅偵測** 的整合，提供強大、自適應的防禦，可動態應對新興威脅，使企業在不斷變化的威脅環境中保持韌性。Proofpoint Nexus 能保護企業的最脆弱的破口——人，無論是釣魚攻擊、內部威脅或是惡意軟體，Nexus 都能提供企業以人為本的關鍵防護。

核心功能

阻止以人為目標的攻擊	即時威脅情資整合	多層次威脅偵測	自適應威脅防禦	無縫整合日常工具
• Nexus 利用多種 AI 驅動模型，識別並應對複雜的社交工程、釣魚郵件和惡意軟體，進而有效阻擋針對人的攻擊。 • Nexus 透過用戶行為和威脅模式分析，可提前發現潛在的攻擊，並採取預防措施。	• Nexus 整合全球威脅情資，確保對最新攻擊手法和惡意軟體的掌握與偵測。透過與外部威脅情資來源的實時同步。 • Nexus 可快速回應各種新興威脅。	• 電子郵件安全：深度掃描電子郵件內容、附件和連結，有效識別釣魚攻擊和惡意軟體。 • 雲端安全：監控雲端應用與協作工具中的異常活動，防止未授權的資料共享或帳戶劫持。 • 網路安全：分析網路流量，精準識別潛在惡意行為和資料外洩風險。	• Nexus 的 AI 驅動模型不斷從實際威脅研究中學習，並能根據最新攻擊手法調整防禦策略。這種自適應能力使 Nexus 始終領先於不斷演變的網路犯罪戰術。	• Nexus 無縫整合企業所依賴的日常工具，例如電子郵件、協作平台（如 Microsoft 365、Google Work space）和雲端應用程式，確保威脅偵測和回應的完整性，同時將對業務流程的干擾降至最低。

全方位的的安全防護

透過進階語言分析技術 深入發掘各種潛藏威脅

Nexus 語言模型 (Language Model, LM) 利用先進的 AI 語言模型的強大功能來防範商業電子郵件詐騙 (BEC)。它能仔細分析電子郵件內容，偵測 BEC 攻擊中常見的特徵，例如交易相關的用語和緊迫性。透過識別細微的語言模式與行為線索，Nexus LM for BEC 能在可疑郵件造成損害前就預先識別。這個尖端解決方案為企業提供了關鍵的防護層，能有效抵禦複雜的電子郵件攻擊，確保更高層級的安全保護。

自動執行複雜數據分析 簡化威脅偵測流程

生成式人工智慧 (Generative AI) 透過先進的生成式演算法，自動執行跨電子郵件、雲端平台及網路的複雜數據分析。生成式 AI 不依靠預設的規則，而是識別模式、連結和內容中的細微變化，進而偵測到傳統系統難以察覺的複雜威脅，例如：網路釣魚意圖和未經授權的資料外洩。以資料外洩防護 (DLP) 為例，生成式 AI 能處理大量的即時與歷史數據，偵測並防止敏感資料外洩。隨著技術不斷進化，生成式 AI 加速了決策過程，並有效防範新興威脅，提升整體安全防護效能，讓資安團隊能更有效率地應對進階網路攻擊。

整合全球即時威脅情資 領先網路犯罪分子一步

Nexus 威脅情資 (Threat Intelligence, TI) 整合了大量威脅數據，以提升 Proofpoint 各項產品的偵測能力。Nexus TI 提供即時更新，涵蓋新興威脅、攻擊者策略以及系統漏洞等資訊。Nexus TI 專注於進階威脅情資，確保 Proofpoint 解決方案能持續領先不斷演變的網路威脅，並提供主動偵測與防禦。Nexus TI 是維持堅韌安全防護態勢的關鍵，能有效幫助企業對抗各種現代網路威脅。

識別異常用戶行為 偵測內部威脅及遭駭帳戶

Nexus 關係拓模圖 (Relationship Graph, RG) 利用 AI 監控、評估用戶行為，進一步強化網路安全防禦。透過行為分析、機器學習和異常偵測技術，Nexus RG 能發現用戶行為中可能是潛在威脅的異常偏差。Nexus RG 與 Proofpoint 的整體威脅偵測系統無縫整合，強化用戶即時防禦能力，提供全面保護，有效應對行為驅動的網路風險。

自適應機器學習強化防護 力，抵禦日新月異的威脅

Nexus 機器學習 (Machine Learning, ML) 運用先進的機器學習技術，強化 Proofpoint 威脅偵測能力。透過監督式學習、非監督式學習及整合學習法 (Ensemble Method) 等技術，Nexus ML 提供了可擴展且強大的安全解決方案。這項核心 AI 技術確保 Proofpoint 能夠偵測並緩解各種不斷演變的威脅，提供跨資安領域的全面保護。

運用進階視覺 AI 技術 (Vision AI) 消除視覺 欺騙攻擊

Nexus 電腦視覺 (Computer Vision, CV) 是一個 AI 驅動的模組，專門用於識別並消除以視覺為主的威脅。透過先進的電腦視覺技術，Nexus CV 能夠偵測隱藏在視覺元素中的威脅，例如網路釣魚網站、QR Code、惡意附件，以及偽造的電子郵件。Nexus CV 專注於視覺威脅向量，並透過強大的因應能力來增強安全性，有效打擊涉及嵌入圖像及其他圖形內容的攻擊。

制定整體安全措施以保護人員和資料

Proofpoint Nexus 威脅情資平台無縫整合各種現代化安全技術，藉此實現其真正的價值。Proofpoint Nexus 提供強大的自適應防禦力，將 AI、機器學習、行為分析、威脅情資和視覺威脅偵測等技術整合到單一、具統整性的系統中，因此可動態應對各種新興威脅。

Proofpoint Nexus 確保攻擊的每個階段都能被即時監控、分析和消除，進而提供用戶無與倫比的保護。Proofpoint Nexus 的核心價值在於多種技術模組的協同運作，並將個別洞察轉化為統一、多層次的策略，協助客戶用宏觀的角度採取所需的行動，以在不斷變化的威脅態勢中保持韌性。

Proofpoint Zen™

將禪學精神的簡單、便利融入安全防護中

資安長期以來一直是一個複雜且要求嚴格的領域。

資安人員必須隨時保持警惕，而終端用戶則承受著持續審視每次互動，以發現潛在威脅的壓力。但一切可以更簡單。

Proofpoint 開發了全方位的網路安全技術來因對這些挑戰。Proofpoint Zen™ 是一套控管終端用戶使用工具的技術，無論工作在哪裡進行，都能保護企業的人員和資料；同時也蒐集正確情資，支援 Nexus 模型所需的分析數據，並做為引導用戶行為或執行政策的控制點。

一個完整的技術生態系統，為以人為本的安全平台提供現代化且統一的體驗

ZenWeb

確保所有裝置都能安全瀏覽

Proofpoint ZenWeb™ 於 2025 年第一季推出，是一款可嵌入基於 Chromium 瀏覽器的擴充功能，適用於各種裝置。無論是協作、檔案共享工具，還是生成式 AI 應用程式，ZenWeb 都能全面保護用戶安全。

- 保護用戶工作環境

ZenWeb 能有效防禦惡意連結、憑證竊取和資料外洩，無論用戶在哪裡工作，都能獲得完善的保護。

- 提前應對威脅

透過即時的威脅偵測與防護，確保企業的連網活動安全無虞，且不影響工作效率。

Zen for Outlook

阻擋電子郵件威脅與資料外洩

- 保護通訊管道

電子郵件始仍然是網路攻擊的主要途徑。Zen for Outlook 不僅能提醒員工注意可疑郵件，還能輕鬆加以舉報，即使是透過行動裝置也能簡單操作。

- 透過智能干預強化郵件的資料防護

Zen for Outlook 的主動防護機制能防止機敏資料誤傳給錯誤的收件人，避免人為失誤，確保重要資訊安全無虞。

ZenConnectors

無縫的安全整合

ZenConnectors™ 能無縫整合 Microsoft 365 及其他關鍵應用程式，將 Proofpoint 的安全防護擴展至整個數位工作環境。

- 安全工作無處不在

無論是電子郵件、協作工具還是資料儲存，ZenConnectors 都持續提供防護，確保安全涵蓋團隊工作的每一個環節。

- 輕鬆整合

ZenConnectors 能快速、簡便地部署，不影響既有工作流程或生產運作。

Email Security and Protection 電子郵件安全與保護

電子郵件是第一大威脅媒介，網路釣魚和電子郵件詐騙等社交活動 96% 都是透過電子郵件進行，且方式不斷在演變。Proofpoint 提供最有效的解決方案，保護您的員工和機敏資料免於進階電子郵件威脅。Proofpoint 完整且可擴充的電子郵件安全平台提供進階 BEC 防禦功能，可阻擋惡意和非惡意軟體的電子郵件威脅，讓您掌握最大的風險來源 — 您的員工，更全面了解所面臨的風險並快速回應各項威脅。

防止電子郵件詐騙 防範 BEC 威脅

您可以透過 Proofpoint 先進的機器學習技術 NexusAI 對 BEC 和網路釣魚電子郵件、惡意軟體、垃圾郵件等威脅進行準確分類，並對所有寄件者進行身份驗證，讓合法電子郵件正常傳遞，以確保您的組織在電子郵件詐騙攻擊中的商譽。Proofpoint 電子郵件安全解決方案可自動識別您的供應商及其對企業組織的風險。

進階 BEC 防禦 防範電子郵件和 供應商詐騙

保護您的電子郵件免於各式各樣的詐騙，例如付款時遭重新導向至惡意網站，或是供應商發票詐騙等。面對這些威脅，您需要更精細的檢測技術。進階 BEC 防禦所運用的檢測引擎結合 AI 和機器學習，是專為發現、阻擋 BEC 攻擊而設計，能夠分析多種訊息屬性，藉此確認該訊息是否為 BEC 威脅。分析內容包括：

- 訊息標頭資料
- 寄件者的 IP 位址 (x-originating IP 和商譽)
- 緊急郵件內容和文字、句子等訊息

進階 BEC 防禦還可檢測各種攻擊者策略，例如回覆地址不一致 (reply-to pivots)、使用惡意 IP 或類似供應商網域，並且可以讓您詳細了解 BEC 威脅資訊、提供 BEC 主題 (例如，供應商發票、禮品卡、變更薪資轉帳帳戶等)、訊息相關的可疑原因觀察及訊息範例。這些詳細資訊可協助資安團隊更了解攻擊並進行因應。

威脅防護 檢測並阻擋進階 惡意軟體

Proofpoint 電子郵件安全解決方案透過多層次內容分析、信譽分析和 Sandbox 分析來分析電子郵件，可檢測帶有惡意 URL 或附件的電子郵件，並阻擋勒索軟體和多種型態的惡意軟體。重寫 URL 可以保護所有網路和裝置上的用戶，並協助檢測訊息在發送後是否已被武裝化。

修補措施 一鍵自動收回 惡意郵件

您可以刪除寄送後中毒的 URL 網路釣魚電子郵件或被駭者不需要的電子郵件。即使電子郵件被其他使用者轉發或接收，也可以一鍵自動執行。

| Proofpoint 電子郵件安全產品

電子郵件保護 Email Protection

Proofpoint 電子郵件保護 (EP) 是業界領先的電子郵件安全閘道，允許您保護、控制您的收信和發信。Proofpoint 特有的機器學習和多層次檢測技術有助於動態識別並阻止網路釣魚和 BEC 威脅。

針對性攻擊防護 Targeted Attack Protection

針對性攻擊防護 (TAP) 可協助您領先攻擊者。它為您提供一種創新方法，可以在進階威脅到達您的收件匣前對其進行檢測、分析和阻擋，進而保護您的電子郵件。TAP 可顯示重點受攻擊人員的可見性，並提供可行的建議和攻擊活動的詳細取證資訊。

電子郵件詐騙防禦 Email Fraud Defense

超越電子郵件身份驗證，掌握供應商詐騙行為。透過電子郵件詐騙防禦，您可以簡化 DMARC 實施。Proofpoint 為您提供工作流程指導及顧問支援，全面保護您的組織在電子郵件詐騙攻擊中的信譽。

威脅回應自動收回 Threat Response Auto-Pull

透過威脅回應自動收回，使您的訊息傳遞和安全管理人員能夠分析電子郵件，並在寄送後將惡意或不需要的電子郵件移至隔離區。

內部郵件防禦 Internal Mail Defense

擴展您的電子郵件安全解決方案，協助內部郵件防禦檢測出遭盜用的帳號。IMD 自動掃描所有內部電子郵件流量，提供一種多層次方法來識別透過遭盜用帳戶所發送的垃圾郵件、惡意軟體或網路釣魚攻擊，刪除這些電子郵件並提供報告以顯示哪些帳戶已遭盜用。

電子郵件持續性 Email Continuity

電子郵件系統停機可能會嚴重影響員工的工作效率。借助企業持續性，即使電子郵件系統停擺，仍可確保電子郵件始終可用。它透過 Outlook 整合、Web 入口網站或本機行動支援為您的使用者提供完全存取權限，EC 會在斷線時自動啟動，並於上線時自動回復。

Security Awareness Training 資安意識培訓

現今駭客比以往任何時候都更直接地以人為目標，95% 的網路安全問題都可以追溯到人為錯誤。透過為用戶提供具目標性、以威脅為導向的教育，可確保您的用戶知道在面臨真正威脅時該怎麼做。Proofpoint 資安意識培訓使您的員工能透過完整解決方案保護您的組織，進而有效減少 30% 現實世界的惡意連結的點擊次數。

Proofpoint 資安意識培訓方案採用整合性方法進行資安教育和意識培訓，提供經過驗證的框架，推動行為改變和真正的安全成果，因此連續 6 年在 Gartner 魔力象限中被評為領導者。透過 Proofpoint 資安意識培訓，您可以針對使用者弱點、角色和能力客製資安教育，實施簡短且聚焦的課程，進而持續讓員工培養習慣，確保在面臨複雜的攻擊時能做出正確回應，同時也提供 CISO 所需要追蹤的各項指標。



評估

第一步是建立組織的基準並了解使用者網路安全知識和計畫間的差距。Proofpoint 資安意識透過威脅情資驅動的知識評估、文化評估和網路釣魚模擬測試，幫助您了解計畫重點，並可與 Proofpoint TAP 針對性攻擊防護平台整合，讓您掌握實際攻擊中的經常點擊者和 VAP 重點受攻擊人員。Proofpoint 協助您確認使用者面臨威脅時會做什麼以及對安全的認知，進而調整培訓計畫，滿足使用者的個別需求。

- 基於實際威脅的網路釣魚、USB 模擬
- 知識評估
- 文化評估
- 識別組織內的 VAP 和點擊次數最多的項目/用戶報告

改變行為

提高資安意識的下一步是改變不安全的行為。借助 Proofpoint 獨特的自適應學習框架，您可以為使用者分配具針對性、威脅驅動的培訓。這種量身定製的線上資安教育可著重用戶需求及其薄弱環節來幫助企業推動行為改變，建立資安意識的知識基礎。Proofpoint 支援 40 多種語言的用戶培訓教材，減少語言障礙，並能與電子郵件安全解決方案整合。您可以提供上下文提示，提醒使用者有問題的電子郵件，並允許他們使用電子郵件警告標籤提報可疑訊息，透過自訂報告統整用戶回饋的可疑訊息，強化積極回報行為。

- 微學習內容
- 自適應學習框架
- 威脅導向的教育訓練
- 電子郵件警告標籤
- 閉環電子郵件分析和回應 (CLEAR) 流程

評鑑

最後，您可以衡量您的安全意識培訓計畫績效，了解使用者的電子郵件準確率、點擊率和模擬 / 真實攻擊的報告資訊，並透過擷取重要指標來與產業同行比較。資安意識培訓可以提高安全計畫的可見性，以便更好地展現成效，並幫助您專注於須改進的地方。

- 使用 CISO 儀表板進行基準測試和其他關鍵指標確認
- 即時報告
- VAP 重點受攻擊人員的可見性

擴充和規模

Proofpoint 資安意識培訓為您提供靈活的導入方式，甚至應用至全球規模。您可以依計畫職責進行委派，同時監督整個計畫，並透過 Proofpoint 的多租戶管理做出集團規模的決策。

- 適用於具有全球或分散式的大型組織
- 了解全公司內的教育活動
- 針對在地用戶和客製化培訓需求
- 打造您的資安意識品牌內容
- 可支援擴充至 40 多種語言

ITM & Endpoint DLP 內部威脅管理與端點資料外洩防護

遠距辦公的形成讓員工、第三方廠商及供應商可以存取比以往更多的資料，因此資料遺失的風險也隨之增加。然而，資料遺失往往都是「人」所造成的；而資料外洩又分為三種類型：粗心、惡意或遭駭。在制訂策略之前，必須先了解使用者背後的行為，這將有助於在內部事件發生時以更好的方式回應。

Proofpoint ITM 內部威脅管理和 DLP 端點資料外洩防護，用「以人為本」的方法來管理內部威脅並防止端點資料外洩。

- 識別具風險的使用者行為和機敏資料的相互影響
- 檢測並防止內部人員的資安事件和端點資料外洩
- 快速回應使用者引起的事件

Proofpoint DLP 端點資料外洩防護和 ITM 內部威脅管理都能防止用戶資料外洩，並透過對使用者活動的深度分析來防禦高風險用戶的威脅。這兩個解決方案隸屬於 Proofpoint 資訊保護和雲端安全平台 - 一個全面、情境化的雲端原生平台。它允許您從中控台設定策略、分類告警、尋找威脅並回應事件，協助您快速有效地阻止資料外洩並調查內部違規行為。

監控日常用戶和潛在風險用戶

Proofpoint 開發了輕量的端點 agent，可以防止資料外洩並提供對使用者活動的深入分析。透過簡單變更策略配置，就能以自適應方式依個別使用者或群組設定所需收集的資料量和類型，更有效地調查、回應告警，且無須收集大量資料。一般用戶通常風險較低，可以用 Proofpoint DLP 端點資料外洩防護對其進行監控，以深入了解資料活動及關聯性。對於高階管理者或具有風險的用戶，則需要更深入了解他們的動機和意圖，監控他們的行為或情境。Proofpoint ITM 內部威脅管理收集關於這些使用者活動的深入分析資料，提供在事件發生的前、中、後，用戶的意圖關聯分析。

提供使用者資料活動的可見性和關聯性

Proofpoint DLP 端點資料外洩防護收集使用者與端點互動的資訊，包括使用者何時操作檔案或重新命名機敏資料檔案，以及嘗試移動機敏資料時的記錄。Proofpoint ITM 解決方案提供基於端點活動的完整視圖，以便監控具風險的使用者。它收集 Proofpoint 端點 DLP 的資料，提供應用程式使用的可見性、端點活動的截圖和其他風險行為，包括安裝、執行未經授權的工具。ITM 有助於掌握風險事件相關的人員、內容、地點和時間，藉由上下文的分析洞察，您可以在資料外洩或不符合規範的行為發生時，更快辨別使用者的意圖。

即時檢測有風險的用戶行為和資料的相互影響

您可以從頭開始建立適合您的環境規則和觸發設定，或者調整 Proofpoint 預設的威脅腳本。依使用者群組、應用程式和日期/時間以及資料敏感度、分類標動、來源和目的地、移動路徑和類型進行腳本修改。

Proofpoint 端點 DLP 和 Proofpoint ITM 包含預設的告警庫，可以輕鬆設定並快速執行。Proofpoint 端點 DLP 和 Proofpoint ITM 都能提醒端點上具風險的資料移動及使用；Proofpoint ITM 還能針對更廣泛的內部威脅危險行為進行告警。

端點 DLP 和 ITM 告警庫

資料活動		使用者活動(僅限 ITM)	
資料使用及外洩相關告警，包括 (超過 40 個警報)：		全方位端點用戶活動相關告警 (超過 100 個警報)：	
• File upload to web • File copy to USB • File copy to local cloud sync • File printing • File activities (rename, move, delete) • File tracking (web to USB, web to web, etc.)	• File download from web • File sent as email attachment • File downloaded from email/endpoint	• Hiding information • Unauthorized access • Bypassing security control • Careless behavior • Creating a backdoor • Copyright infringement • Unauthorized comm tools • Unauthorized admin task	• Unauthorized DBA activity • Preparing an attack • IT sabotage • Privilege elevation • Identity theft • Suspicious GIT activity • Unacceptable use

防止未經授權的資料從端點外洩

只檢測具風險的用戶和資料活動是不夠的，您還必須主動阻止資料外洩。透過 Proofpoint 平台，您可以防止使用者與機敏資料進行不當的行動。這些行動包括：

- 與 USB 裝置之間的傳輸
- 上傳到未經授權的網站
- 將檔案同步到雲端資料夾
- 文件列印

可依據使用者、使用者群組、端點群組、程式名稱、USB 裝置/序號/供應商、資料分類標籤、來源 URL 和內容掃描等項目自訂防護。

Identity Threat Detection and Response 身份威脅檢測及回應

檢測、預防身分風險，以阻止橫向移動和權限提升

身分竊取是現今數位環境中日益嚴重的威脅。駭客能突破既有防禦，在幾天內完成攻擊。Proofpoint ITDR 解決方案，可提供防禦攻擊時所需的身分威脅防護及回應。即使駭客正在行動並在環境中橫向移動，ITDR 解決方案也能持續發現並修復您的即時漏洞。

ITDR 解決方案可發現並消除的特權身分風險如右圖所示：



- ← 服務帳號
- ← 舊版應用程式帳號
- ← 影子管理者帳號
- ← Kerberoastable 憑證
- ← 快取憑證 (Windows、瀏覽器等)
- ← 未正確斷開的 RDP session
- ← 雲端服務 Token

Spotlight - 透過自動修復預防身分風險，並檢測橫向移動與即時威脅

當駭客第一次入侵時，很少直接執行他們的最終目標，這意味著他們需要提升權限並透過橫向移動來實現目標。駭客快速、輕鬆且有效地利用特權帳號，組織也很難檢測到。透過 Proofpoint Spotlight，您可以檢測環境中的權限提升和橫向移動。

發現並修復特權身分漏洞和政策違規行為

AD 持續發現和檢查	自動風險修復	準確檢測並回應
Spotlight 會持續檢查 Enterprise AD、Azure AD 和 PAM，以發現組織的身分漏洞並確定其優先順序。Spotlight 可檢測： ■ Enterprise AD 與 Azure AD 設定錯誤 ■ 特權存取管理 (PAM) 漏洞 ■ 端點暴露 (Exposure) ■ 權限提升和橫向移動	簡化身份漏洞修復： ■ 自動修復端點和伺服器風險 ■ 提供身份風險儀表板，完整了解自動修復的風險及告警 ■ 輕鬆強化組織的身分安全態勢 ■ 有效評估新環境風險	檢測規避防禦的身份威脅： ■ 用於部署失效安全 (Failsafe) 對入侵者的檢測誘捕 ■ 超過 75 種誘捕技術用於無代理檢測和保護 ■ 從攻擊者角度提供攻擊的可見性 ■ 針對不同端點客製化的自動誘捕 ■ 在攻擊鏈中自動收集證據以進行稽核和合規

Shadow - 透過誘捕技術，在駭客意識到前進行阻擋

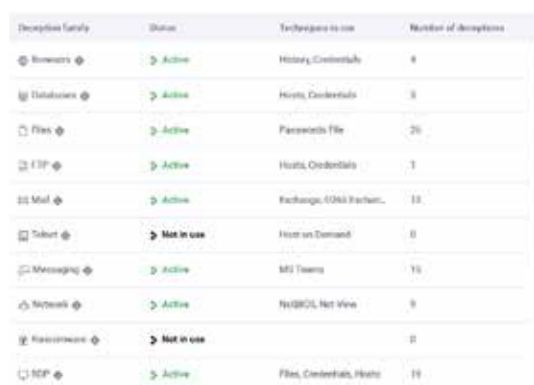
用傳統特徵碼或行為分析進行檢測，很容易讓資安團隊因為誤報和告警疲勞而不知所措。為了持續檢測新形態的網路攻擊，您需要誘捕技術來提供對權限提升和橫向移動的實際檢測。Proofpoint Shadow 與傳統方法不同，以無代理方式 (Agentless) 在您的正式環境中主動吸引攻擊者，並檢測出他們的存在。

將每個端點變成誘捕網，阻止攻擊者橫向移動

無代理檢測及保護	超過 75 種誘捕技術	自動誘捕	從攻擊者角度出發	自建誘捕文件檔案
Shadow 獨特的無代理方式建立在智慧自動化的基礎上，減少營運足跡，最大限度地降低對 IT 的影響，且無法像基於代理的解決方案那樣被攻擊者停用或規避。	Shadow 提供主動誘捕技術來模擬對攻擊者有用的憑證、連接、資料、系統和其他文件。無論從何處開始被駭，組織都能在最短時間內發現內外部攻擊者。	Shadow 智能自動化系統可建立高度真實的誘捕環境，並隨時間進行擴充和改變，而且幾乎不需要人為操作。Shadow 分析端點情況並為每台機器量身定製誘捕技術。可一鍵進行流程部署，並持續自動調整、管理誘捕的過程。	透過 Shadow 中控台，您可以了解攻擊者與關鍵資產的距離，一旦發生誘捕，就能取得攻擊活動的完整時間軸，還能了解攻擊者如何取得誘捕資料，以及更多與攻擊活動有關的情報。	透過 Shadow，您可以自建數十萬個誘捕用的 MS Word 和 Excel 檔案。這些檔案與真實檔案沒有差別，甚至連公司商標和信箋都一樣。這些仿真檔案會載入假數據，一旦駭客試圖用這些資訊來獲取存取權限，系統就會立即發出告警。



Spotlight 身分風險儀表板



Shadow 誘捕狀態