Proofpoint Identity Threat Defense Platform

阻斷非法提權與橫向移動

產品

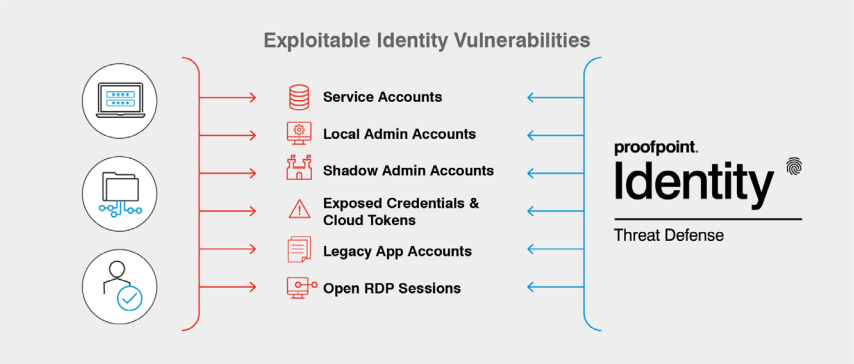
- Proofpoint Shadow
- Proofpoint Spotlight

關鍵優勢

- 發掘、優先處理並修復身份安全漏洞
- 了解企業環境中的特權身份風險或潛在入侵管道
- 提升身份漏洞細部觀察能力，涵蓋 Active Directory、Entra ID、AWS Identity Center、Okta、特權帳號管理 PAM、端點和 LAPS
- 自動修復端點中已知的身份安全漏洞
- 確保及早發現攻擊者並加快威脅調查
- 使用無代理程式 (Agentless) 技術防止被攻擊者規避偵測
- 彌補特徵比對和威脅行為偵測技術無法顧及的安全缺口
- 與Proofpoint TAP、TAP ATO以及NPRE整合，將威脅、風險及身分安全漏洞串聯起來

攻擊手法日趨複雜且具高針對性，而對應的威脅防禦解決方案卻未趕上威脅的步伐。根據趨勢顯示[1]，攻擊者已針對身份漏洞，標準化其策略、技術和攻擊程序，但企業尚未找到打破其攻擊鏈的可靠方式。在企業環境，身份 (Identity) 是攻擊面的關鍵環節，應加強予以關注。

Proofpoint 身份威脅防護平台 (Identity Threat Defense Platform, ITD) 提供點對點的身份威脅保護，平台包含 Proofpoint Shadow 和 Proofpoint Spotlight 兩大產品，具備發現與修復身份漏洞、無代理程式的誘捕偵測與鑑識資料收集功能，協助您發現、確定其優先度並修復易受攻擊的身份漏洞。



圖一: Proofpoint 身份威脅防護和易受攻擊的身份安全漏洞

Proofpoint『以人為本』安全平台降低基於『人』的風險，並將風險區分為四大領域，ITD為其中的『身分』安全領域

1 這些解決方案包括身分識別與存取管理 (IAM)、多因素身份驗證 (MFA)、端點偵測與回應 (EDR)、安全資訊和事件管理 (SIEM) 以及擴展偵測與回應 (XDR) 等

身份危機

大多數企業都有佈署 Active Directory（AD），不幸的是，在過去兩年中，有 79% 的企業曾經歷過身份相關外洩事件。根據 Verizon DBIR 報告，94% 成功的攻擊都使用 AD 和特權身份來提升其權限。攻擊者會使用各式各樣的工具，如 Bloodhound、Cobalt Strike、Mimikatz 和 ADFind 等，幫助他們更快盜取特權身份，也讓攻擊變得更難以偵測。

Proofpoint 調查發現，即便企業已佈署傳統的身份識別與存取管理（IAM）解決方案，平均每六個企業端點中（包括使用者端及伺服器）仍有一個存在身份安全漏洞，而攻擊者可以利用這些漏洞獲取管理者權限。駭客通常不會將第一次登陸的主機作為最終目的，而會在企業網路內橫向移動，以找到企業中最關鍵或 Tier 0 的資產。一旦抓到目標，他們即可以竊取資料，並同時發動勒索軟體攻擊。

Figure 2: Proofpoint Identity Threat Defense platform.

許多身份安全漏洞源於正常的業務和 IT 操作流程，如：

- **使用者名稱和密碼**：使用者的應用程式通常會將這些資訊快取暫存於瀏覽器、SSH、FTP、PuTTY 和資料庫等端點，這些憑證不受特權存取管理（PAM）保護。
- **域名（Domain）管理者憑證**：有時在遠端支援工作結束後，憑證仍會繼續留存在系統記憶體中，或暫存於未受保護的服務帳戶內。
- **影子特權（Shadow privileges）**：在 Active Directory 中設定身份目錄物件（Object）和群組可能非常複雜，因此某些使用者可能被不當分配過多的影子特權。

點對點視角的身份安全

成功的攻擊會利用管理和防護的漏洞，Proofpoint 身份威脅防護平台可協助資安團隊識別並防堵這些破口，讓您可以：

1. **發現風險**：持續發現並檢查在AD、EntraID、AWS Identity Center、Okta和端點上的身份安全漏洞。
2. **優先排序及自動修復**：根據優先度清單確認須優先關注的漏洞（會將所有發現到的漏洞依緊迫程度進行排序），啟用 Proofpoint平台的身份安全漏洞自動修復功能，客戶可設置例外規則以符合您的企業安全政策。
3. **偵測與回應**：藉由無代理程式的欺敵技術，偵測攻擊者在客戶環境的活動，諸如 Kerberoasting、密碼噴灑（Password Spraying）、特權帳號濫用等，並藉由自動取證資料收集，協助企業因應運作中的威脅。

了解更多

如需更多詳細資訊，歡迎瀏覽 **proofpoint.com**.