Proofpoint Email Security
郵件安全

獲得進階威脅防護與深度解析

關鍵優勢

- 在郵件送達前阻止商業郵件入侵 (Business Email Compromise，BEC) 詐騙、網路釣魚及進階惡意軟體攻擊
- 讓您的員工能透過郵件警告標籤 (Email Warning Tag) 來提高警覺
- 透過快速郵件追蹤和維護郵件衛生，提升企業運作效率
- 在先進式威脅進入收件匣前，即先偵測、分析並阻擋這些威脅
- 深入與獨到的剖析，能識別出企業中的重點受擊人員 (Very Attacked People™) 以及整體的安全風險
- 運用 Proofpoint 威脅情資 (Proofpoint Threat Intelligence) 防範威脅，並取得詳細的威脅鑑識報告

有高達百分之九十以上的攻擊是藉由郵件發起[1]，而這些威脅仍不斷地進化和演變。

Proofpoint 能協助保護與控管企業收發的電子郵件，利用機器學習和多層偵測技術，識別並阻止惡意郵件，其中包括偽冒郵件 Imposter、釣魚郵件 Phishing 、惡意軟體 Malware、垃圾信件 Spam、大量投寄郵件 Bulk 等。而在自定義安全政策和郵件發送規則的設定上，也具備極大的彈性，再加上 Proofpoint 對郵件威脅的深入洞察，協助您找出企業最佳化的應對策略。

攔截新興威脅，阻絕一切漏網之魚

通常商業郵件入侵 BEC 和供應鏈帳戶入侵威脅不會帶有明顯的惡意內容，若要識別這些威脅，須要使用比沙箱掃描更細緻的偵測技術。由 NexusAI 驅動的 Proofpoint 進階 BEC 防護 (Proofpoint Advanced BEC Defense)，就是為了能有效阻止五花八門的郵件詐騙所設計，能偵測像是透過遭入侵的帳戶，向您發送轉帳付款要求，或是假冒請款收據等郵件詐騙行為。由於這類社交工程的威脅通常不含一般系統可偵測到的惡意內容與指令，唯有更精密的偵測技術才能抵禦。

我們透過獨特的郵件判定機制，動態分類多種郵件類型，將您收到的惡意電子郵件進行分類隔離。Proofpoint Nexus 威脅圖表 (Proofpoint Nexus Threat Graph) 和進階 BEC 防禦 (Advanced BEC Defense) 引擎，乃是根據豐富的威脅資料構建和訓練而成，它們能即時學習，快速響應威脅形勢的變化。這些功能合力保護您的系統，能第一時間阻擋惡意活動的入侵。我們的技術不僅偵測威脅，也會應用機器學習來觀察每次駭客攻擊的模式、行為和技術。透過如此的洞察力，「針對性攻擊防護模組」(Targeted Attack Protection，TAP) 持續學習並適應新局勢，以便更迅速地攔截未知多變的先進式攻擊。

URL 防禦

我們的 TAP URL 防禦 (TAP URL Defense)，可防範像是惡意軟體和憑證釣魚等基於 URL 傳遞的郵件威脅。我們提供獨特的預測分析功能，能根據郵件傳輸模式識別可疑的 URL，並在沙箱進行測試。

1 Verizon, "Cost of a Data Breach Investigations Report." July 2019.

郵件附件防禦

TAP 郵件附件防禦 (TAP Attachment Defense) 能支援多種檔案類型偵測，可檢查受密碼保護的檔案、內嵌 URL 連結的附件和 Zip 壓縮檔案等，防範隱藏在檔案中的惡意威脅。

針對重點受擊人員 (VAP) 的瀏覽隔離策略

提供給重點受擊人員的 URL 隔離策略 (TAP URL Isolation for VAP)，主要目的是為了保護您的「重點受擊人員」(Very Attacked People™，VAP) 免受來自 URL 和網頁的攻擊。運用我們的瀏覽器隔離解決方案 (RBI)，VAPs 能在不危害公司資訊安全的環境中，安心地訪問從公司郵件導向的其他網站。

*此產品僅適用已獲得 P-bundles 軟體授權的客戶。

快速追蹤任何郵件

您可以藉由 Proofpoint 的智慧搜尋功能獲得詳盡的搜尋結果，像是超過 100 種控制條件的 metadata，此外還有內建多種即時報告，能讓您詳細洞察郵件的動向與攻擊趨勢。

提高使用者警覺

郵件警告標籤 (Email Warning Tag) 可以指出特定郵件的相關風險，提供使用者能輕易理解的簡短說明。您的員工將因此對可疑的郵件更加地謹慎，從而降低威脅入侵的潛在風險。

深入洞察並解析威脅與被鎖定的目標

利用平台提供的資訊，您可同時了解廣灑型與針對性的駭客攻擊。在平台上都能輕易取得各種威脅的詳細資訊，如受影響的使用者、觸發攻擊時的截圖、深度鑑識分析等資料。

重點受擊人員 (VAP)

Proofpoint 攻擊指數 (Proofpoint Attack Index) 能幫助識別組織中的 VAPs，讓您的資訊安全團隊鎖定出最優先的防護對象。透過更加瞭解 VAPs，您可找出最有效阻止威脅的關鍵策略。

企業層面的攻擊指數 (Company-level Attack Index)

從企業層面上能透過攻擊指數 (Attack Index)，幫助您的資安長和資訊安全團隊理解公司所正遭受的攻擊類型，以及與產業中其他同儕的差異。您將可根據自身企業遭遇的攻擊樣態，擬訂安全控制措施的優先順序。

洞察網路威脅集團

多年來，我們的威脅研究人員持續蒐集網路威脅集團的相關情資，而這集大成的智慧結晶，就在TAP管理介面 (TAP Dashboard) 上清楚呈現。透過管理介面，客戶能清楚明白攻擊來自哪些駭客組織、誰是攻擊目標、這些威脅團體隨時間推進而改變的攻擊策略和技術TTP，以及攻擊趨勢。這些資訊有助於您的組織決定優先要採取的額外安全與補救控制措施，以更完善地保護組織中最有價值的資產—您的員工。

瞭解更多

如需更多詳細資訊，歡迎瀏覽 **proofpoint.com**。