Proofpoint Email Security

偵測、阻止郵件威脅並獲得深度解析

關鍵優勢

- 在郵件進入時，封阻商業郵件詐騙 (Business Email Compromise, BEC)、釣魚 (Phishing) 攻擊及進階惡意軟體攻擊
- 透過郵件警告標籤 (Email Warning Tag) 讓員工提高警覺
- 快速追蹤郵件和維護郵件衛生，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，能識別出企業中的最受攻擊人員 (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
- 以雲端佈署實現行業領先的SLA：
  - 99.999% 的服務可用性
  - 近乎 100% 的病毒防護
  - 不到一分鐘的電子郵件延遲
  - 阻擋或重新導向 99% 的垃圾郵件

電子郵件是排名第一的威脅媒介，高達 96%的『可疑社交行為』都是通過電子郵件送達[1]。 Proofpoint是《Fortune》百大、千大企業中佈署最廣泛的電子郵件安全解決方案，其中也包括全球最大規模的企業。 Proofpoint 每天處理數十億封郵件，能看到更多威脅，藉由更快、更好地偵測，協助您對抗如偽冒郵件等難以偵測的無惡意檔案之電子郵件威脅。 再加上Proofpoint 對郵件威脅的深入洞察，幫助您找出企業最佳的應對策略。

Catch Emerging Threats That Others Miss
攔截新興威脅，阻絕一切漏網之魚

偵測釣魚、偽冒和詐騙電子郵件

搭載 NexusAI 的 Proofpoint Advanced BEC Defense 功能旨在有效阻止廣泛、多變的電子郵件詐騙，包括由已遭入侵之郵件帳戶發動的薪資轉移攻擊和供應鏈發票……等詐騙攻擊。 因為通常沒有惡意負載 (malicious payload) 可以偵測，這些類型的威脅往往需要更複雜的偵測技術。

Proofpoint 郵件防護還能讓您了解 BEC 威脅的詳細資訊，包括 BEC 利用的主題 (禮品卡、薪資轉移、發票、誘餌或工作任務)。 完整提供郵件被視為可疑的原因、和該威脅郵件的攻擊樣本，以便於您的安全團隊能夠更深入的瞭解攻擊並溝通。 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，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。

1 Data Breach Investigations Report, Verizon, 2020

URL 防禦

URL防禦(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。

郵件附件防禦

郵件附件防禦 (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。

針對最受攻擊人員 (VAP) * 的瀏覽隔離策略

提供給最受攻擊人員的URL隔離策略 (URL Isolation for VAP)，主要目的是為了保護您的「最受攻擊人員」(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。

Track Down Any Email in Seconds
快速追蹤任何郵件

您可以藉由 Proofpoint 的智慧搜尋 (Smart Search) 功能獲得詳盡的搜尋結果，包含超過100種屬性的 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。

Raise User Security Awareness
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。提醒您的員工將對可疑的郵件更加地謹慎，從而降低威脅入侵的潛在風險。

Gain Deep Insight and Visibility Into Threats and Targets
深入洞察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。 在平台上都能輕鬆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。

最受攻擊人員(VAP)

Proofpoint 攻擊指數 (Proofpoint Attack Index) 能幫助識別企業中的 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正遭受攻擊的類型，以及與產業中其他同儕的差異。 可根據企業遭遇的攻擊樣態，擬訂安全控制措施的優先順序。

洞悉網路威脅團體

多年來，Proofpoint 威脅研究人員持續蒐集駭客組織的相關情資，透過管理介面，您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，與攻擊趨勢。這些資訊有助於企業決定優先要採取的額外安全與補救控制措施，以更完善地保護企業中最有價值的資產— 人。

* 此產品僅適用已獲得 P-bundles 軟體授權的客戶

瞭解更多

如需更多詳細資訊，歡迎瀏覽 **proofpoint.com**.