Harmony Email & Collaboration

完善防護雲端電子郵件與協作套裝軟體

防護 Office 365 和 Google Workspace 應用程式

主要功能

- **防網路釣魚：**封鎖網路釣魚攻擊，如身分偽裝、商務電子郵件詐騙 (BEC)，防堵惡意攻擊進入收件匣
- **防堵惡意軟體：**防堵規避軟體和勒索軟體，數秒內即可提供清消過後的檔案
- **防止資料遺失：**設定自訂政策，維護資料安全與合規性
- **防止帳戶接管：**使用事件分析演算法，辨識惡意行為跡象，封鎖可疑登入維護資料安全與合規性

主要優勢

- **完善防護：**保護所有溝通管道，電子郵件到協作平台滴水不漏
- **防彈等級安全性：**攔截最複雜的規避技術攻擊，他牌難望項背
- **迅速有效：**適用電子郵件與協作套裝軟體的單一解決方案，高效能、符合成本效益

雲端電子信箱是您的資安弱點

超過 90% 的企業組織攻擊始於惡意電子郵件，也有 75% 的勒索軟體攻擊來自電子郵件。電子郵件攻擊通常牽涉人為因素，因此 Microsoft 365 和 Google Workspace 工作環境將會是您的企業資安弱點。網路釣魚和勒索軟體攻擊一旦得逞，將會造成重大的財務損失。為了弭平安全性落差，您需要防護多種威脅媒介，才能有效防堵網路釣魚、惡意軟體、資料竊盜與帳戶接管。

運作原理

完善的電子郵件與協作安全性

1. **封鎖複雜的社交工程攻擊，如身分偽裝、零時差網路釣魚，以及使用 AI 訓練引擎進行商務電子郵件詐騙 (BEC)**

   內建安全性並不足以阻止進階網路釣魚攻擊，如涉及細膩的社交工程技術，專門設計用來欺騙並操縱終端使用者。Harmony Email & Collaboration 是您電子郵件最後一道防線，保護收發信和內部郵件不受網路釣魚攻擊，這類攻擊往往能夠規避平台資安防護。這項解決方案會檢查傳輸的 Metadata、附件、連結和語言，並與歷史傳輸資料比對，以判定發送者和接送者之間的過往信任關係，可有效提升辨識使用者身分偽裝或詐騙訊息的機率。方案亦會即時檢查內部傳輸，以預防橫向攻擊與內部威脅。

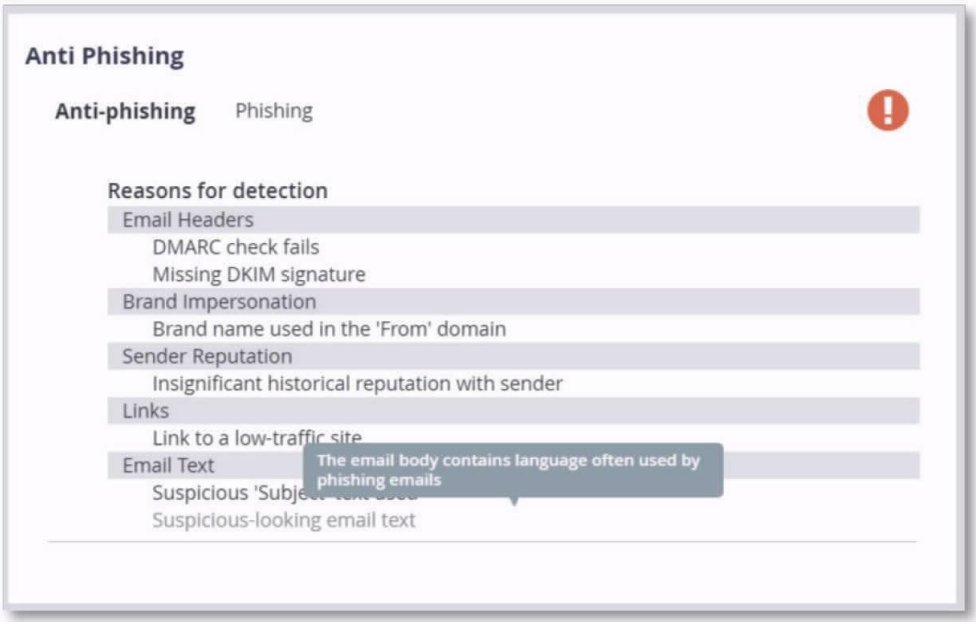

圖 1：往下追朔釣魚郵件

2. 封鎖惡意附件，阻止攻擊觸及使用者信箱，同時不會影響業務生產力

Harmony Email & Collaboration 使用 Check Point 的 SandBlast 技術，此技術受到 NSS Labs 認可，最有效地防止資料外洩，包含下列功能：

- 威脅模擬事件：CPU 層級防規避沙箱，能夠封鎖首次出現的惡意軟體，並維持防護能力，阻擋最進階的網路威脅。
- 主動式威脅萃取：檔案消毒並排除潛在威脅，迅速將安全檔案版本交付到使用者手中，全程僅需不到兩秒
- 「威脅萃取」可維持業務不中斷，同時沙箱亦在背景繼續運作。「威脅萃取」採用業界唯一完全整合的文件與圖像消毒解決方案，能夠排除傳統威脅模擬事件所造成的延遲問題，同時立即消毒檔案內所有主動式內容

3. 進階資料外洩防護 (DLP)，保護敏感性業務資料，並維持監管合規性

Harmony Email & Collaboration 可偵測電子郵件和其他協作應用程式內的敏感性資料共享，並立即限制資料外洩。它能讓您根據公司需求執行資料外洩政策，提供數百種預定義及自訂資料類型。當員工透過電子郵件或其他協作套裝應用程式分享資料時，Harmony Email & Collaboration 即會檢驗主旨、內文與附件，若有敏感性資料共享，如信用卡詳細資訊、個人資料或競爭情報，即會封鎖傳輸內容，或是採行「未共享」模式，以預防資料外洩。

4. 增強驗證流程，預防進階帳戶接管攻擊

Harmony Email & Collaboration 使用專利申請中技術，預防未授權使用者與遭到入侵的裝置存取您的雲端電子郵件或應用程式，因此可減少帳戶接管攻擊的風險。Harmony Email & Collaboration 使用 SaaS 原生 API 與 Check Point ThreatCloud 功能，加上機器學習演算法攔截攻擊，它能分析使用者行為，並運用行動及終端裝置來源偵測作業系統是否存在漏洞、惡意軟體與網路攻擊。

Harmony Email & Collaboration 可為身分識別資訊系統的驗證流程提供額外資料，立即拒絕封鎖可疑登入 (例如：登入活動出現在不同位置、IP 曾有不良活動記錄)。

**NSS Labs 報告：https://www.nsslabs.com/tested-technologies/advanced-endpoint-protection/*

防彈等級安全性，攔截他牌無法阻擋的進階攻擊

1. **Inline-API 防護，有效保障電子郵件收發和內部郵件傳輸**

   API 式整合可讓 Harmony Email & Collaboration 即時掃描電子郵件發信和內部郵件傳輸，預防組織內的橫向攻擊、內部威脅以及資料外洩。此外不需要變更 MX 紀錄，攻擊者因此無法查看活動。Harmony Email & Collaboration 作為您的最後一道防線，訓練人工智慧攔截他牌無法阻擋的規避沙箱攻擊，有效減少 99.2% 網路釣魚電子郵件進入收件匣。

2. **服務整併至 Check Point Infinity 架構，並由世界最強大的威脅智慧技術驅動**

   Harmony Email & Collaboration 可以整合 Check Point Infinity 架構，Check Point Infinity 是整併式安全性架構的一環，跨越網路、雲端、端點、行動裝置與物聯網實現一致高效的安全性，並由世界最強大的威脅智慧資料庫 ThreatCloud 所驅動。

3. **NSS Labs 唯一測試實證的安全性解決方案，惡意軟體攔截率 (99.91%) 為業界最佳**

   Harmony Email & Collaboration 運用 NSS Labs 認可為防止資料外洩最有效的 SandBlast 技術，100% 封鎖率、規避測試最高得分，提供您多層保護。

迅速有效的安全性

1. **數分鐘即可完成部署，數小時可見成效，包括針對既有的惡意電子郵件進行回溯式掃描**

   Harmony Email & Collaboration 可在五分鐘內完成安裝，安全性管理人員可立即部署。Harmony 即可立時攔截惡意活動。部署當天，解決方案即會執行回溯式掃描，尋找組織內部是否存在既有威脅，確保方案啟始時便有最佳保護。

2. **單一授權即可涵括所有安全性功能，電子郵件與生產力應用程式皆適用**

   Harmony Email & Collaboration 僅需單一授權即可提供雲端電郵和協作應用程式的所有安全性功能，減少購買支出與管理開銷，提供企業組織一站式的全方位解決方案，真正降低總體擁有成本 (TCO)。

3. **僅需單一儀表板即可監控深度解析與報告，並執行操作**

   Harmony Email & Collaboration提供安全性事件的精細等級能見度，僅需單一儀表板即可使用所有安全性功能。Harmony 提供可執行操作的深度見解與報告，減少管理開銷並改善生產力。

檔案共享安全性

1. **Harmony Email & Collaboration 保障重要檔案共享服務的安全——Google Drive、ShareFile、OneDrive、Sharepoint、Box、Dropbox，免受惡意軟體、勒索軟體、伺服器間的東西向流量攻擊 (east-west attack)，並預防意外或惡意事件導致的資料遺失**

   透過可擴充的雲端式虛擬環境進行動態分析，所有附件皆會接受測試執行，以確保未含惡意內容。Harmony 可直接偵測惡意行為，並在檔案散播威脅之前加以隔離。用戶可依據組織規劃自訂政策篩選操作。Harmony 會掃描並分析每一個檔案，若有惡意連結，將會立即封鎖惡意檔案。Harmony 運用多項主要資料源查詢 URL 封鎖名單，將每一個檔案內的連結皆會逐條衡量，包含網域與其頁面。

協作安全性

1. **Harmony 電子郵件協作為 Slack 和 Microsoft Teams 等協作應用程式新增安全防護層，以防堵惡意連結與訊息。**

   Slack 和 Microsoft Teams 等協作工具本質上並無安全防護，企業組織與資料因而曝於風險之中。Harmony 能夠控制機密資料存取權限、隔離惡意內容，並通知使用者安全性事件。與此同時，更具備詳盡的儀表板，針對安全性問題更新管理，且可於應用程式內使用。Harmony 會記錄使用者總數量、檔案、資料分享、連結、登入資料、渠道來源與威脅偵測。

總結

電子郵件是攻擊鏈目標的第一個環節，隨著遠端工作日益興盛，雲端信箱與協作應用程式的使用亦呈現指數型成長。Harmony Email & Collaboration 提供企業組織完善的全方位保護，與時俱進，因應大環境威脅演變而進化，同時提供安全人員部署管理簡便的平台，讓您輕鬆擁有高效安全防護。

與 Check Point 台灣銷售團隊聯繫
電話：+886-2-2719-9030 | Email：info@checkpoint.com
www.checkpoint.com