電子郵件安全購買者指南

電子郵件：網路攻擊的主要攻擊向量

現今的網路犯罪越來越常從電子郵件下手，並提供以威脅為中心的內容，然後再利用電子郵件將惡意軟體引進公司系統、竊取資料和勒索金錢。由於雲端信箱服務（如 Office 365）的使用率越來越高，導致混合式攻擊可從多個端點鎖定組織。

雖然現在持續對公司電子郵件發動攻擊的威脅類型五花八門，但其中有三種造成的問題最堪慮。

- **勒索軟體：**惡意軟體的一種，可阻擋受攻擊的公司存取自己的資料；勒索軟體 2016 年造成的損失高達 $10 億美元 (csoonline.com)。
- **公司電子郵件入侵 (BEC)：**這類網路犯罪可不當獲取大量現金，其造成的威脅甚至比勒索軟體更嚴重，BEC 攻擊會要求高價值的目標人士向不肖人士提供資金或敏感資訊。網際網路犯罪申訴中心 (IC3) 指出，在 2013 年 10 月到 2016 年 12 月之間發生的 BEC 詐欺事件中，就有 53 億美元遭竊 (ic3.gov)。
- **網路釣魚：**向來都是最有效果的攻擊方式，利用精巧的社交工程和鎖定魚叉式網路釣魚，誘騙使用者掉入陷阱，進而入侵整個組織。2017 年第二季期間，入侵組織的惡意軟體中有 67% 是透過網路釣魚攻擊達成目標 (nttcomsecurity.com)。

網路犯罪可利用以下三個部分的訊息入侵電子郵件。

- 電子郵件內文
- 附件
- 電子郵件內的 URL

勒索軟體造成
$10 億美元損失[2]

$53 億美元：
遭入侵的公司電子郵件
付出的成本代價[3]

67% 的惡意軟體
是透過網路釣魚入侵組織[4]

1 《思科 2017 年中網路安全報告》，思科（2017 年）。https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

2 Maria Korolov《勒索軟體 2016 年進帳 $10 億美元：改善防禦措施並不足以力挽狂瀾》(Ransomware Took In $1 Billion in 2016—Improved Defenses May Not Be Enough to Stem the Tide)，CSOonline.com（2017 年 1 月 5 日）。https://www.csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html

3 《公司電子郵件入侵、電子郵件帳戶入侵：50 億美元詐騙案》(Business E-mail Compromise, E-Mail Account Compromise: The 5 Billion Dollar Scam)，網際網路犯罪申訴中心 (IC3) 和聯邦調查局（2017 年 5 月 4 日）。https://www.ic3.gov/media/2017/170504.aspx

4 《GTIC 2017 年第 2 季威脅情報報告》，NTT Security（2017 年 8 月 8 日）。https://www.nttcomsecurity.com/en/gtic-2017-q2-threat-intelligence-report/

給電子郵件安全防護購買者的參考準則

思科安全研究部門[5] 指出，組織採用的電子郵件解決方案必須符合五大關鍵要求，才能確保企業現在和未來都能獲得需要的深入多層級防護。

1. 對於整個安全態勢能提供有效的情報、分析和回應
2. 快速追溯修復
3. 公司電子郵件入侵 (BEC) 防護
4. 防止資料外洩及來自輸出電子郵件的風險
5. 加密敏感的業務資訊

要求 1：對於整個安全態勢能提供有效的情報、分析和回應

網路攻擊越來越複雜，因此部署的安全防護也要跟著升級；網路犯罪現在發動的威脅相當廣泛，已非傳統資安防護所能抵擋。若想發揮抵禦作用，電子郵件安全解決方案必須超越及時單點檢查電子郵件的基本周邊工具。除了涵蓋基本工具，還要透過更全面的方式整合多層安全防護，以持續分析威脅和監控流量趨勢。

透過此方式，您的解決方案才能根據最適當的情報，對威脅指標快速作出反應。您的資安團隊也可藉此取得必要的深入能見度和控制能力，以降低攻擊的偵測用時 (TTD)[6]，並確認事件影響範圍，然後在惡意軟體造成傷害之前加以遏止。

思科如何針對多個向量提供有效的安全防護

思科透過多種方式建立多層必要的安全性，以抵禦多種攻擊類型。

- 以地理位置為基礎的篩選功能可根據寄件者的位置快速控制電子郵件內容，進而抵禦複雜的魚叉式網路釣魚攻擊。
- 思科®內容自適掃描引擎 (CASE) 提供超過 99% 的垃圾郵件擷取率，以及不到百萬分之一的業界超低誤判率。
- 思科 Talos™ 擷取的威脅資料可加快識別威脅，並縮短 TTD，甚至可找出最新型的零日攻擊。
- 進階惡意程式防護 (AMP) 解決方案提供全域能見度和持續分析能力，範圍涵蓋端點和行動裝置，以及雲端和網路中的所有 AMP 架構元件，能根據惡意軟體的行為進行辨識，而無需識別其型態。
- AMP 亦可藉由即時分析潛在的惡意連結，持續抵禦以 URL 為基礎的威脅。

更快偵測到威脅能降低潛在的傷害

思科已將 TTD 中位數從 2015 年 11 月（公司初次記錄）的超過 39 小時銳減至 2016 年 11 月到 2017 年 5 月期間的大約 3.5 小時。

資料來源：《思科 2017 年中網路安全報告》，思科（2017 年 7 月）。

威脅情報

Talos 是由超過 250 名思科全職威脅研究人員組成的團隊，負責追蹤新興威脅，其收集的情報取自思科安全產品等各種資料來源；接著 Talos 會這些情報與思科電子郵件安全客戶分享，以確保更完善的防護。Talos 提供同級最佳的防護，一旦發現威脅，便會在所有地方封鎖該威脅，可抵禦新興的混合式攻擊並予以封鎖。

5 《思科 2017 年中網路安全報告》，思科（2017 年 7 月）。https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html
6 思科將偵測用時 (TTD) 定義為從威脅入侵到系統偵測到該威脅所經歷的時間。

Office 365 可追溯的安全

AMP 使用自動可追溯的安全功能，針對 Office 365 客戶受感染的輸入和輸出電子郵件採取行動，可協助客戶更輕鬆、更快地修復漏洞。

假如看似正常的附件稍後被系統發現可能帶有惡意檔案，則系統會自動向 Azure 發出 API 呼叫，然後檔案就會轉寄或刪除。

要求 2：快速追溯修復

一旦惡意軟體、網路釣魚攻擊或惡意 URL 突破您的前線防禦，您的企業必須具備持續監控威脅和評估的能力，以隨時偵測出問題，並快速掌握事件的影響或潛在影響，然後再以最快的速度進行修復。

思科如何提供自動可追溯的修復

思科會持續檢查您的資安環境內是否有躲過防護機制或突然改變處置方式的惡意檔案或 URL。

- 進階疫情擴散過濾器可讓您持續深入檢查 URL。透過即時分析，您只要按幾下滑鼠，原本正常的網站出現惡意行為時，便可快速加以封鎖。
- AMP 可持續運用 Talos 的即時監控和分析資料，以及思科 Thread Grid 情報，找出先前不明的威脅或突然改變處置方式的檔案。
- AMP 也會採取修復行動，包括自動觸發動態信譽分析，並提供惡意軟體來源能見度、指出受影響的系統及惡意軟體正在進行的活動。自動排定修復優先順序後，AMP 接著會根據取得的情報，對輸入和輸出電子郵件採取行動。

要求 3：公司電子郵件入侵 (BEC) 防護

公司電子郵件入侵 (BEC) 又稱詐欺電子郵件，屬於網路釣魚攻擊，網路罪犯會假冒為高級主管（通常是執行長），嘗試要求員工、客戶或廠商匯錢或提供敏感資訊給網路釣魚者。

BEC 攻擊高度集中，並利用社交工程技術抓取入侵電子郵件的收件匣、研讀公司新聞並研究員工在社交媒體上的動態，以確保電子郵件內容的可信度。由於 BEC 攻擊不會利用惡意軟體或惡意 URL 威脅組織，因此十分難以偵測。

跨多個攻擊向量的全方位防護

進階惡意程式防護 (AMP) 除了利用傳統型時間點偵測技術，同時也為您的資安環境提供持續分析及可追溯的安全。

思科如何抵禦 BEC

思科對於 BEC 採用多層級安全策略，利用精密的網路信譽過濾器和進階電子郵件驗證技術，監控來自全球的電子郵件和網路流量，進而識別出網路釣魚嘗試。

- 假造電子郵件偵測 (FED) 功能可檢視 SMTP 操縱訊息的一或多個部分，包括「實際寄件者」、「收件者」或「寄件者」標題，輕鬆偵測出魚叉式網路釣魚攻擊。目前有一套驗證工具提供特定防護：發送器政策框架 (SPF) 可用於驗證寄件者，而域名金鑰識別郵件 (DKIM) 和網域訊息驗證、報告及符合性 (DMARC) 則用於驗證網域。
- 可深入檢視電子郵件寄件者及其網域，有助授權合法寄件者，並在封鎖詐欺電子郵件傳到員工、業務合作夥伴和客戶之前予以封鎖。

要求 4：避免資料外洩和輸出電子郵件的風險

電子郵件安全解決方案必須偵測、封鎖和管理輸出電子郵件的風險；包括避免惡意內容傳送給客戶和業務合作夥伴，並防止敏感資料意外或刻意流出網路。除了重要的智慧財產遭竊，遭入侵的電子郵件帳戶內若包含惡意軟體，則可能藉由突然製造大量輸出垃圾郵件散播病毒。即使電子郵件通過簽署，但這仍會導致組織的電子郵件網域遭列入黑名單。

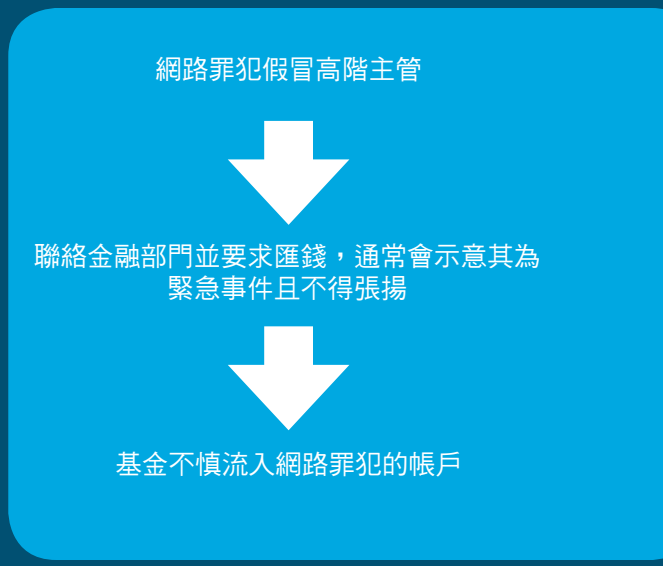
思科如何防止資料外洩和輸出威脅的風險

- AMP 提供適用於輸出電子郵件的安全性層級，包括用來偵測遭入侵帳戶的行為監控、輸出流量速率限制、防垃圾郵件和防毒掃描；此可避免入侵電腦或帳戶讓您的公司列入電子郵件黑名單。
- 思科 DLP 技術提供內容、背景及目的地資訊，避免意外遺失或惡意竊取資料、強制法規遵循並保護您的品牌和信譽。您可控制寄件者、資訊內容，以及傳送位置和方式。
- 超過 100 項最新的預先定義政策，有助於防止資料遺失，並支援適用政府、私人部門及自訂公司專用規範的安全性和隱私權標準。例如：「HIPAA」、「GLBA」或「DSS」等過濾器可根據政策自動掃描和加密裝載，防止資料遺失。修復選擇包括新增頁尾和免責聲明、密件副本、通知、隔離、加密等等。
- 此外，傳輸層安全性 (TLS) 數位憑證可驗證使用者及網路，確保寄件者和收件人之間的隱私和資料完整性，進而提供完善的通訊防護。

預先定義的法規遵循政策

思科電子郵件安全有助組織遵守這些隱私權和安全標準。

- 支付卡產業資料安全標準 (PCI DSS)
- 健康保險可攜性和責任法案 (HIPAA)
- 沙賓法案 (SOX)
- 美國金融隱私保護法案 (GLBA)
- 美國與歐洲隱私權指令及規範



思科電子郵件安全結合多層安全性，能降低輸出威脅的風險。

要求 5：加密敏感的業務資訊

公司執行公司業務活動時應採用安全無虞的通訊，以免遭到入侵。加密是其中一個重要的安全層級，用來保護離開您網路的資料。無論遇到惡意或意外情況，加密功能皆可避免財務及個人資訊、競爭對手情報和智慧財產等敏感資料外洩。

思科如何加密資料

思科採用現今市場上最先進的加密金鑰服務，可管理電子郵件收件人註冊、驗證及按郵件/按收件人的加密金鑰。

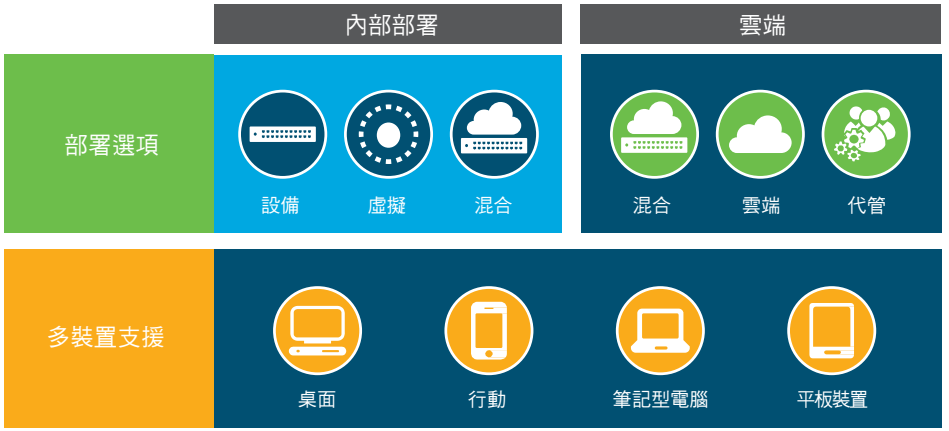
- 優異的 TLS 支援有助於設定最適合的交付方式。閘道也為法規遵循和資安人員提供控制力與能見度，可掌握交付敏感資料的方式。
- 可自訂的報告控制面板能讓您即時存取加密電子郵件流量資訊，包括使用的交付方式及主要寄件者和收件者。

思科電子郵件安全解決方案提供功能

思科電子郵件安全解決方案提供高適用層級的電子郵件防護，能有效因應現今不斷快速演化並影響組織的威脅。我們具有獨一無二的因應策略，運用業界最大的資安研究組織 Talos 提供的情報，通常能搶先競爭對手數小時甚至數天提供防禦。

簡單的設定及自動化功能，數分鐘內輕鬆完成防護工作。我們的解決方案符合成本效益、隨時警戒並採用最新技術。訂閱人數最低要求只要 100 位使用者，且各種規模的客戶皆可選擇所有可用的功能和部署項目。

靈活的部署選項包括內部部署或雲端部署（其中採用混合模式及支援各種端點裝置的代管服務）。無論您選擇哪一種部署方式，程式碼基底皆相同，因此可使用同一套功能。這表示如果您現在的安全防護採用內部部署，日後也可移轉到混合式環境，甚至按階段完全部署到雲端，同時在所有環境中皆保有相同的政策和相似的使用者介面。



彈性的電子郵件安全部署選項。

為何選擇思科電子郵件安全解決方案？

現在的組織需要多層級電子郵件資安模式，以防禦複雜的多向量新興威脅，例如：BEC、勒索軟體和以 URL 為基礎的攻擊。思科的安全架構策略整合多項產品，可讓您在不同產品組合之間共用有效情報。如此可使多個安全層級的回應更快速並保持同步。

- 我們的電子郵件安全解決方案在共用情報的支援下，除了具備單點及時掃描功能，還能提供：
- 來自思科 Talos 最完善的全球預測情報，能在您的系統受到影響之前找出攻擊。
- 無論有風險的檔案何時出現惡意行為，持續予以監控，並在發生感染時減輕傷害；採用與 Office 365 電子郵件使用者相同的安全防護。
- 深入的即時 URL 掃描、分析及封鎖功能，只要按幾下滑鼠即可掌握惡意變動情況。
- 防止敏感資訊不慎外洩，協助您確遵循產業及政府規範。
- 完整的即時報告功能，縮短調查及回應時間。
- 彈性部署選項讓您無論採用內部部署或雲端環境，皆可享有同樣完善的電子郵件防護，讓您放心進行移轉。
- 佔用空間小、實作簡單、自動化管理，長時間下來可節省成本並降低整體擁有成本。

立即免費試用 45 天

若想瞭解思科電子郵件安全防護的優點，最好的方式就是立即使用 45 天免費試用版親自體驗。我們的試用版易於使用，其中提供最受歡迎的電子郵件安全附加元件，包括適用電子郵件的進階惡意程式防護和 ThreatGrid。

如需其他資訊，請造訪：
www.cisco.com/go/emailfreetrial