

電子書

紅色警戒： 別成為下一個 數位人質

勒索軟體預防與緩解最佳實務

勒索軟體之殤

儘管近期執法機關持續打擊，勒索軟體依然是重大威脅。

勒索軟體是一種惡意軟體，會加密檔案或鎖定使用者，使其無法存取裝置與系統，意圖迫使企業付款後才恢復存取權限。根據 Chain Analysis 統計，2023 年勒索軟體贖金總額已超過 10 億美元。此外，《2024 年 Verizon 資料外洩調查報告》指出，「約三分之一的資料外洩事件涉及勒索軟體或其他勒索手法……勒索軟體更是 92% 產業所面臨的首要威脅。」

近幾個月來，多個執法機關聯手行動，成功逮捕了主要勒索軟體集團 LockBit 的多名成員。然而，這些行動並未對攻擊數量帶來實質影響，勒索軟體威脅依然存在。但請不必恐慌！本電子書將為您說明幾項可用來保護企業的最佳實務作法。

勒索軟體是日益嚴重的威脅。但請不必恐慌！本電子書將為您說明幾項可用來保護企業的最佳實務作法。



根據 2024 年 Astra Blog 統計
，92% 的惡意軟體透過電子郵件
散布。

勒索軟體帶來的挑戰

身為惡意軟體的一種，勒索軟體可透過多種方式散布，常見的攻擊途徑包括網路釣魚郵件、惡意下載檔案，以及不安全的網站。

根據 2024 年 Astra Blog 的統計，92% 的惡意軟體透過電子郵件散布。此外，《2024 年 IBM 資料外洩成本報告》指出，「由勒索軟體引發的資料外洩事件占比在過去一年成長了 41%，且平均比其他事件多花 49 天才能識別並圍堵。」不僅如此，我們也觀察到勒索軟體攻擊逐漸出現直接鎖定伺服器的趨勢，因此曝險的不只是端點而已！

勒索軟體的主要挑戰包括：

- 特徵碼式工具難以偵測新型威脅與攻擊手法。
- 機器學習與信譽評等式工具，對於「就地取材(Living off the Land)」攻擊手法的防禦成效不佳。
- 端點偵測與回應(EDR)工具仍需投入人力進行事件分診研判。

儘管上述工具皆實用且不可或缺，但仍須搭配其他技術，才能全面因應勒索軟體威脅。本電子書將進一步介紹這些輔助技術。

破解枷鎖

對抗勒索軟體攻擊並沒有萬靈丹，唯有整合多種資安技術與策略協同運作，才能有效預防並緩解此威脅。

以下六項要訣可納入貴組織的資安策略，協助抵禦勒索軟體及其他電子郵件型攻擊。

- 1.即時阻斷攻擊。導入全方位電子郵件安全防護，檢查並阻擋可疑郵件與連結，防止其進入使用者的收件匣。
- 2.最好的攻擊就是堅實的防禦。安裝具備即時防護能力、信譽良好的防毒軟體，攔截漏過電子郵件安全防護的惡意郵件。
- 3.每日一「蘋果」，駭客遠離我。持續更新並修補端點系統。許多攻擊者正是利用已知弱點入侵桌機、工作站、筆電與伺服器。
- 4.留存副本，有備無患。定期將檔案備份至雲端或外接儲存裝置，確保資料一旦遭到破壞也能迅速復原。
- 5.將零信任延伸至核心層級。針對擁有較高權限或特權的使用者、帳號與系統，建立並落實原則控管。
- 6.把「真心」鎖起來。將所有機敏資料加密，防止駭客存取竊取，並導入遠端清除機制，銷毀任何落入駭客手中的資料。

以下六項要訣可納入貴組織的資安策略，協助抵禦勒索軟體及其他電子郵件型攻擊。



智慧型的全方位電子郵件安全防護平台，運用信譽分析、防毒引擎與反垃圾郵件特徵碼等技術，**攔截垃圾郵件與惡意軟體。**

即時阻斷攻擊

電子郵件是網路犯罪者發動並散布威脅時最常使用的途徑。

進階電子郵件威脅(例如：魚叉式網路釣魚、勒索軟體、商務電子郵件詐騙(BEC)等)如今已成為攻擊者偏好的手法，因為這類攻擊會利用網域偽冒與混淆技術隱藏惡意連結，比傳統惡意軟體更難以偵測與阻擋。因此，標準的特徵碼式防惡意軟體工具，對這類攻擊的防禦成效普遍不佳。

Symantec® Email Security.cloud 強化電子郵件系統原生的安全防護，能以極低的誤判率有效防範惡意軟體與電子郵件威脅。此外，Symantec Email Threat Detection Response and Isolation 進一步擴充相關能力，整合雲端沙箱分析、點擊時網址防護、Office 365 郵件收回(clawback)，以及結合Symantec 全球情資網路(GIN)遙測資料的網頁瀏覽器隔離等進階技術，藉此阻擋勒索軟體、魚叉式網路釣魚與商務電子郵件詐騙(BEC)等精密攻擊。這些雲端服務相輔相成，共同打造出智慧、全方位的電子郵件安全防護平台。

最好的攻擊就是堅實的防禦

端點安全防護(Endpoint Security)依然是防止網路攻擊入侵裝置最關鍵的防線之一。

由於全球網路威脅比以往更為兇猛，對企業造成的衝擊也可能相當驚人，因此事前預防至關重要。及早阻止攻擊尤其關鍵，因為現代攻擊留給企業偵測與反應的時間窗口非常短。全方位且整合式的端點安全防護解決方案，能同時保護傳統端點與行動裝置，並在裝置、應用程式與網路等層級提供層層相扣的防禦。

Symantec Endpoint Security採用創新的自適應防護方式，協助企業將防護重心前移(shift left)，強化整條攻擊鏈的防禦能力，並著重於預防以達到快速圍堵。除了防毒、垃圾郵件與惡意軟體防護等基本功能外，此解決方案還運用人工智慧(AI)最佳化資安決策判斷，並透過沙箱分析偵測隱藏於自訂封包中的惡意軟體。

及早阻止攻擊至關重要，因為現代攻擊留給企業偵測與反應的時間窗口非常短。



Astra Security 的調查發現，「近半數企業並未建置弱點管理計畫，無法在弱點遭利用前及早識別並修復。」

每日一「蘋果」，駭客遠離我

截至 2024年1月24日，由美國國家標準與技術研究院(NIST)維護的國家弱點資料庫(NVD)已收錄 236,489 個弱點。

最容易成功的攻擊，往往是利用組態設定不當或未修補的端點上之已知弱點。這類弱點之所以存在，是因為許多企業缺乏即時掌握自身端點狀態的能力。事實上，Astra Security的調查發現，「近半數企業並未建置弱點管理計畫，無法在弱點遭利用前及早識別並修復。」

Symantec IT Management Suite 能協助企業因應此挑戰，安全地管理防護邊界內外的所有裝置。此解決方案可讓您全面掌握環境中的軟硬體現況，藉此強化整體資安態勢，並透過強大的修補程式管理能力，針對各類端點識別並修復弱點。



留存副本，有備無患

只要事先備妥遭竊或遭加密資料的副本，即可大幅縮短勒索軟體攻擊發生後的復原時間。

勒索軟體真正的威脅在於加密檔案及／或封鎖對裝置與系統的存取權限，而攻擊者所要求的贖金，正是建立在企業急需恢復存取的需求之上。然而，只要企業定期將檔案備份至雲端或外接儲存裝置，即使資料遭駭客加密，也能輕鬆復原，無需支付任何贖金給犯罪者。

同樣地，企業也能將遭勒索軟體攻擊入侵的系統復原。VMware Live Cyber Recovery 提供專為勒索軟體復原打造的服務型解決方案，協助企業克服勒索軟體復原過程中最常見的五大挑戰。

VMware Live Cyber Recovery™ 提供專為勒索軟體復原打造的服務型解決方案，協助企業克服勒索軟體復原過程中最常見的五大挑戰。

Symantec PAM 提供伺服器控制代理程式，協助企業集中管理主機伺服器安全的所有面向。

將零信任延伸至核心層級

在核心層級落實精細化存取控制，可有效防範利用「就地取材」工具鎖定伺服器的勒索軟體攻擊。

勒索軟體攻擊者正逐漸轉向鎖定面向網際網路的伺服器與裝置弱點，導致潛伏時間縮短，也使得企業更需要採取主動預防措施，而非僅依賴事後偵測與回應。然而，雙重用途工具與「就地取材」工具的使用，使識別與預防變得更加困難。在核心層級實施精細化存取控制，可有效阻斷此類攻擊途徑。

Symantec PAM是一套完整的解決方案，透過強大的特權存取管理(PAM)能力防範資安入侵事件。為協助企業因應直接鎖定伺服器的勒索軟體攻擊，Symantec PAM提供伺服器控制代理程式，可集中管理主機伺服器安全的所有面向。這些代理程式運作於核心層級，即使攻擊者取得root層級存取權限，仍能強制執行嚴格的控管。透過這些原則落實點，Symantec PAM得以限制勒索軟體攻擊者經常從事的惡意行為，例如：存取機敏檔案、執行未經授權的指令、安裝程式、竄改日誌檔案，或建立未經授權的網路通訊。

把「真心」鎖起來

完善的資料加密策略，有助於符合資料隱私法規遵循要求，並取得安全港豁免資格。

這或許令人難以置信，但犯罪者本來就不值得信任——真是令人震驚！駭客在要求贖金以歸還資料的同時，往往也會存取並竊取這些資料，轉手在公開市場上販售。若能在勒索軟體成功得逞之前，就將所有資料加密，即可有效防範此風險。

Symantec Encryption 可針對終端使用者裝置、內部伺服器與第三方雲端環境，提供彈性的靜態資料保護。此能力能讓資料對犯罪者而言形同無法存取，藉此防範勒索軟體攻擊所引發的資料竊取。此外，還可搭配遠端清除功能進一步強化防護，讓資安管理人員只需按下按鈕，即可清除遭入侵端點上的所有資料，徹底終結駭客對該資料的掌控。

完善的加密解決方案，可針對終端使用者裝置、內部伺服器與第三方雲端環境，**提供彈性的靜態資料保護**。

Broadcom 為整體企業提供
全方位的勒索軟體防護。

Symantec 產品組合

隆重介紹 Symantec 勒索軟體資安產品組合。



電子郵件安全防護

保護電子郵件訊息免受威脅、使用者疏失與資料外洩之害



端點安全防護

運用創新技術，全面守護傳統裝置與行動裝置



端點管理

透過自動化修補程式管理，修復系統弱點



特權存取管理

落實系統層級存取與特權使用者行為之控管



PGP 加密

加密機敏資料，防止竊取並符合法規遵循要求

您為防範勒索軟體、保護資料所做的努力，真的足夠嗎？

Broadcom提供以下競爭優勢，協助您全面保護資料安全。

為什麼選擇 Broadcom

與我們攜手合作的三大理由

在評選能協助保護資料的資安廠商時，Broadcom 相較於競爭對手，提供以下三大差異化優勢。

最全面的安全防護



Broadcom 資安解決方案在資料生命週期的每個階段，都提供完整防護。

最廣泛的涵蓋範圍



Broadcom 資安解決方案橫跨混合式環境，隨處守護您的資料。

最值得信賴的夥伴



Broadcom 資安解決方案已守護全球最大型企業客戶超過 50 年。



如需更多資訊，請造訪我們的網站：<https://www.savetime.com.tw/>

關於賽門鐵克

賽門鐵克(Symantec)已於2019/11併入全球網通晶片巨擘--博通(BroadCom, 美國股市代號AVGO, 全世界網際網路流量有99.9%經過博通的網通晶片)軟體事業部的企業安全部門(SED), 特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系, 讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性, 有著脫胎換骨並超越業界的長足進步。博通(Broadcom)是務實的完美主義者, 致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝, 同時也大大降低交易複雜性。Symantec持續創新的技術能為日新月異的資安問題提供更好的解決方案, 近三年Symantec很少出現在由公關機制產生的頭版文章中, 而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前, 增長幅度也領先其他競爭對手, 是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證, 也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司, 組合國際電腦(CA Technologies)以及雲端運算及「硬體虛擬化」的領導廠商--VMware, 也是博通軟體事業部的成員)。2021年8月, 因應國外發動的針對性攻擊日益嚴重, 美國網路安全暨基礎架構安全管理署(CISA)宣布聯合民間科技公司, 發展全國性聯合防禦計畫JCDC(Joint Cyber Defense Collaborative), 而博通賽門鐵克是首輪被徵招的一線廠商, 如就地緣政治考量, Symantec也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商, 被業界公認為賽門鐵克解決方案專家。自1995年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務, 特別是提供企業IT專業人員的知識傳承(Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上, 以及基於比原廠更熟悉用戶使用情境的優勢能提供更快速有效的技術支援回應, 深獲許多中大型企業與組織的信賴, 長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼, 把我們當成可信任的資安建議者、可以提供良好諮詢的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

免責宣言: 本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準, 請知悉。2025/1/28