電子書

從全新的視角看待終端安全性
利用縱深防禦策略防制勒索軟體

前言：重新審視終端

以往清晰明確的網路邊界因雲端興起而模糊，令您的企業面臨日益複雜且破壞性極大的網路攻擊威脅。未獲得充份保護的桌上型電腦、筆電及伺服器都會為攻擊者提供竊取資料及造成破壞的切入點。最終用戶分佈於多個（住家）辦公室及地區並使用各式各樣的裝置及雲端應用程式來完成其工作，使情況變得更為複雜。

勒索軟體的攻擊手法層出不窮，也比以往更頻繁，不僅直接造成業務中斷，媒體的大肆報道更會令企業名譽掃地。再加上訴訟及罰款成本，終端攻擊可讓大型企業蒙受超過 900 萬美元的損失。在 CyberArk 最近對 1,000 名 IT 安全決策者所做的調查中，59% 的受訪者將勒索軟體列入其最大安全風險清單[2]。

縱深防禦方法

我們應當重新審視終端，採用縱深防禦方法保護終端安全，並建立各種安全控制措施防制勒索軟體。縱深防禦方法的構想最初來自美國國家安全局，採用多層次的安全措施消弭漏洞、減少攻擊面及遏制風險。

本電子書將重新探討全方位終端安全策略的五個基本要素。多層終端安全計劃可協助您補強安全漏洞、改善安全態勢並降低風險。

一次終端攻擊造成的平均經濟損失超過 900 萬美元[1]

[1] 2019 年 Ponemon Institute 終端安全風險現狀
[2] CyberArk 全球進階威脅形勢報告

勒索軟體縱深防禦策略

終端安全策略的五個基本要素

- 終端偵測及回應 (EDR)
- 防病毒及下一代防病毒
- 特權管理
- CDR - 電子郵件安全
- 應用程式及作業系統修補

要素一

終端偵測及回應 (EDR)

終端偵測及回應工具可讓您主動識別及調查終端上的可疑活動。起源於 2013 年的 EDR 解決方案最初是一個額外的防護層，持續監控、記錄及分析終端活動，協助 IT 和專業安全人員有效發現及減少進階威脅。

許多 EDR 解決方案使用進階分析技術分析終端事件，以偵測可能未被察覺的惡意活動。EDR 工具可即時檢視可疑終端的行為，協助您在威脅紮根並傳播至整個企業之前攔阻下來。

擴充偵測及回應 (XDR)

為發現更多威脅並為其分析提供更多背景情報，經過進化升級的工具已擴充至網路、雲端及終端並具備更進階的分析及自動功能。

終端偵測及回應

偵測及回應終端上的
進階主動攻擊

防病毒/下一代防病毒

運用多種技術
防止惡意軟體感染

要素二

防病毒及下一代防病毒

防病毒（AV）及下一代防病毒（NGAV）保護工具可協助您偵測及移除各種形式的惡意軟體。傳統的防病毒解決方案透過檢查檔案及尋找已知病毒的特徵碼來識別及防堵惡意程式。傳統防病毒工具雖然在引入初時很有效，卻無法偵測到更新型的威脅，例如無檔案惡意軟體和零時差攻擊等。事實上，一項 Ponemon Institute 的調查顯示，62% 的受訪者表示他們的傳統防病毒解決方案只能減少最多 50% 的攻擊[3]。

下一代防病毒工具利用預測分析、人工智慧（AI）及機器學習（ML）來防禦現代攻擊，例如可躲避傳統防病毒程式的勒索軟體和進階網路釣魚。不同於透過掃描檔案尋找已知特徵碼的傳統防病毒解決方案，下一代防病毒解決方案採用全觀式做法，檢查每一個在終端上運作的流程，並利用 AI 和 ML 智慧化偵測及主動防堵以往未知的惡意軟體形式。

[3] 2018 年 Ponemon Institute 終端安全風險現狀

要素三
特權管理

終端特權管理解決方案可幫助您解決與特權帳號（例如 Windows 或 Mac 管理員帳號）相關的風險。特權帳號用於控制檔案、目錄、服務及用戶存取權限。如果落入不法之徒手中，就可能被用來竊取資料或破壞系統。

攻擊者經常試圖透過終端上的惡意軟體或網路釣魚攻擊，獲取權限擅自存取特權帳號。一旦取得立足點，他們便可橫越網路尋找高價值的目標，並使用升級的特權竊取機密資訊或破壞關鍵應用程式。Forrester 估計至少有 80% 的資料外洩與特權憑證遭竊取有關[5]。

終端特權管理解決方案透過移除本機管理權限及根據政策嚴格控制用戶與應用程式許可來幫助降低暴露風險。執行最小特權原則（授予用戶執行其工作所需的最小特權組合），可防止橫向移動並改善您的安全態勢，而又不會降低用戶的生產力或影響業務績效。

以特權為核心的防勒索軟體保護

建立應用程式控制，可防止已知惡意應用程式執行並限制未經批准的應用程式運作，從而大大降低風險與不確定性。擴充的功能包括偵測政策（尚）未涵蓋支援的應用程式內的勒索軟體、防堵竊取憑證嘗試及主動阻斷透過特權詐欺組件（例如本機管理員詐欺帳號或假密碼誘餌）進行中的攻擊。

[5] The Forrester Wave™：特權身份管理，2018 年第 4 季

CDR - 電子郵件安全

保護電子郵件帳號
免遭擅自存取、
遺失或滲透

要素四

CDR - 電子郵件安全

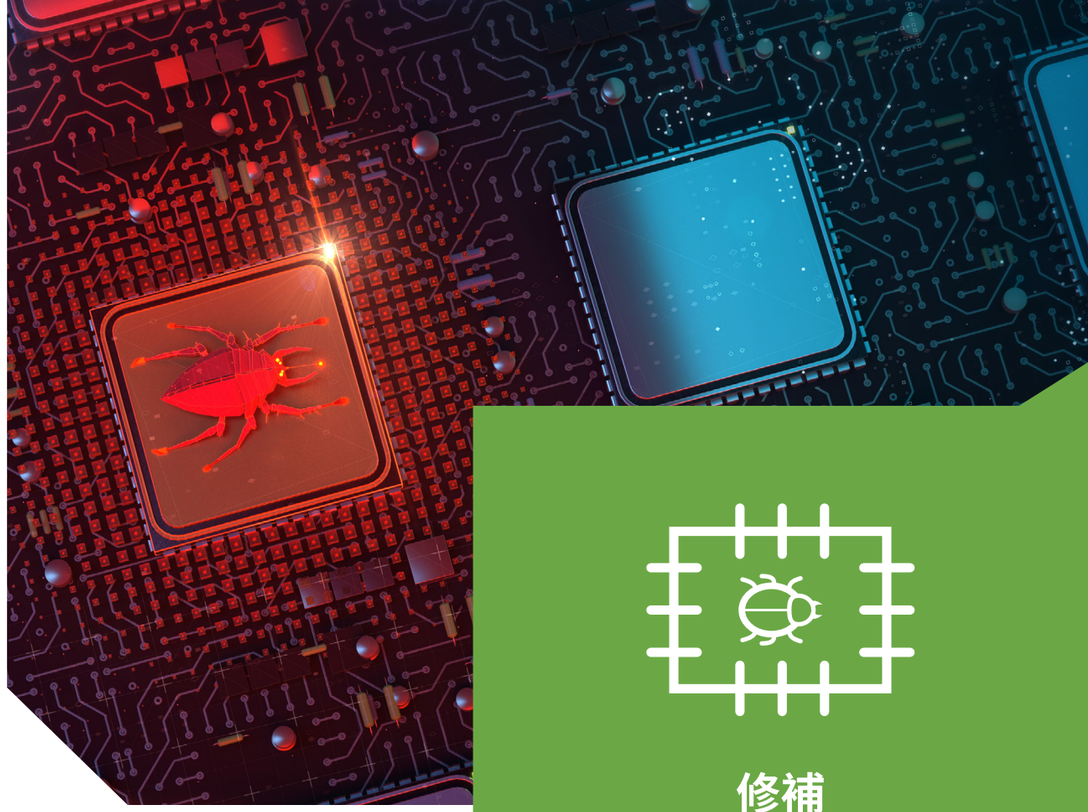
94% 的惡意軟體透過電子郵件傳遞，而通報的社交工程事件有 80% 以上涉及網路釣魚[4]。除了最終用戶認知訓練可對解決這類問題起著重要作用之外，CDR（內容威脅解除與重組）工具可提供多一層保護。與傳統的終端偵測及回應（EDR）不同的是，CDR 無法偵測惡意檔案，而是允許您刪除各種來源（包括電子郵件）中未通過既定規則與政策批准的組件。

除了封存及備份之外，電子郵件安全功能還包括防垃圾郵件、URL 分析、附件沙盒模擬分析、動態內容過濾及加密等。一些更進階的解決方案還可利用人工智慧和即時最終用戶情報辨識及刪除惡意電子郵件。您可使用管理主控台為用戶、網域及網域群組制訂政策，使用允許/拒絕清單及自訂資料遺失防護（DLP）規則。

[4] Verizon 2019 年資料外洩調查報告

要素五

修補工具



修補工具可協助您有效追蹤及實施終端軟體更新，以加強您的安全態勢。精明的攻擊者及網路犯罪份子不斷探求可利用的應用程式和作業系統安全漏洞。軟體供應商則持續發佈修補程式來解決已知漏洞[6]。在這場持久的貓鼠遊戲中，應用程式和作業系統必須保持最新狀態，才能永遠領先惡人一步。

應用程式修補

對許多組織而言，管理應用程式更新是一項挑戰。一項研究指出，一般 IT 組織平均需要 34 天修補高嚴重性的安全漏洞。應用程式修補解決方案可幫助您摒除人工密集、易出錯且耗時的修補程式管理流程並加強網路安防準備。

大多數應用程式修補程序解決方案提供：

- 庫存掃描程式以發現分散於整個企業的所有應用程式
- 狀態儀表板及報告以識別已修補且易受攻擊的應用程式
- 自動執行修補程式批准、分發及安裝程序的工具

修補

套用更新以解決安全問題及修正錯誤

[6] 生產環境網路應用程式安全報告，tCell by Rapid7

要素五

作業系統修補

就像應用程式更新一樣，您需要隨時留意終端作業系統更新。您可設定作業系統自動更新或實施其他系統與方法來減少安全漏洞，確保所有公司桌上型電腦、筆電和伺服器均執行最新版本的作業系統。

每家供應商都有各自發佈作業系統修補程式的做法，因此必須個別考量。Microsoft 在每月第二個星期二發佈 Windows 伺服器及 Windows 桌上型電腦的**安全更新**。您可使用 Windows Update 自動安裝這些修補程式。將更新部署至生產環境之前，如果您想要先進行測試，則可使用 Windows Server Update Services（WSUS）或第三方應用程式修補工具按照自己的時程表發佈及實施作業系統更新。

Apple 會定期發佈 macOS 軟體（可能包括安全更新）。您可以**設定 Mac** 以手動或自動安裝 macOS 更新。

總結

終端可能帶來重大安全風險。精明的攻擊者可利用終端的安全漏洞竊取機密資訊或干擾 IT 服務，進而造成收益損失及高額的監管罰款及法律和解金。針對勒索軟體採取縱深防禦方法（建立廣泛的終端安全控制措施），可增強您的安全態勢及降低暴露風險。

特權管理是有效終端安全策略的關鍵，但卻常被輕忽。惡意內部人員或外部攻擊者經常利用終端管理員帳號取得網路上的立足點，然後橫向移動以滲透或破壞更高價值的目標。

特權管理解決方案可限制特權存取及執行應用程式控制，授予用戶執行其工作所需的最小權限組合，增強安全性而不削弱用戶生產力。這可減少入口終端處的威脅，防止橫向移動及惡意軟體散播，進而協助您降低曝露風險及防止勒索軟體加密。

關於 CyberArk

CyberArk 是特權存取管理領域公認的領導者，提供最完整、靈活的身份安全功能組合，針對任何位置、任何裝置適時執行特權及啟用存取。在人工智慧行為與風險分析的支援下，CyberArk 身份安全平台可隨著您支援分散式工作團隊、登上雲端及採用新雲端技術，以及發展以信任為基礎的客戶體驗時，為任何人類或機器身份提供持續保護及即時存取。

利用 CyberArk，您可刪除本機管理員權限並在需要時提供即時的特權存取，增加多一道抵禦勒索軟體攻擊的重要防線。CyberArk 結合應用程式控制、防止憑證竊盜及特權詐欺功能，提供全方位的勒索軟體防禦解決方案。

透過 CyberArk 市場取得的預建整合及整合可加強我們的縱深防禦做法。擴充的功能包括威脅情報、資產資料及其他終端安全健康指標。

詳細瞭解資訊