DELL Technologies

提升您的網路安全性與零信任成熟度

別讓安全風險成為創新的阻礙

瞭解您的網路安全強度

瞭解其需要達到什麼程度

在現今複雜且快速演進的威脅態勢中，組織在維護健全的網路安全實務方面，經常面臨資源和知識的限制。提升網路安全和零信任成熟度，在對抗不斷演變的網路威脅方面至關重要，可在確保環境安全的同時，又不阻礙創新。

使用這些檢查清單，評估您網路安全成熟度的目前狀態。瞭解貴組織的優勢和弱點，有助於採取正確的後續步驟，以提升網路安全成熟度。

目錄

深入瞭解

深入瞭解如何提升網路安全和零信任成熟度

檢查清單：

減少攻擊面

攻擊面是指環境中所有可能成為網路攻擊者的目標，或遭利用的點或區域。這些點可能包括軟體漏洞、組態錯誤、認證機制薄弱、未修補的系統、過度的使用者權限、開放的網路連接埠、不良的實體安全性等。這些問題有助於決定，如何盡可能減少惡意行為者可能入侵的漏洞和進入點。

是	否	
☐	☐	您的組織是否執行定期評估、滲透測試或入侵攻擊模擬，以識別系統和網路中的漏洞和弱點，以便及時補救和改進？
☐	☐	您的組織是否定期為員工提供安全性訓練？
☐	☐	您的組織是否使用多因素驗證 (MFA) 和角色型存取控制 (RBAC)？
☐	☐	您的組織是否已實施網路切分，以隔離關鍵資產，並限制網路不同部分之間的存取？
☐	☐	您的組織是否已實作安全編碼實務、定期進行安全性測試和程式碼審查，以及使用 Web 應用程式防火牆 (WAF)，以協助防範常見的應用程式層級攻擊，同時減少 Web 應用程式的攻擊面？
☐	☐	您的組織選擇的 IT 供應商，是否能夠證明其流程和程序可確保其供應鏈安全無虞？
☐	☐	您的組織是否正在實施零信任原則，來取代傳統的邊界型安全機制？
☐	☐	您的組織是否利用最低權限原則，將使用者和系統帳戶限制為僅具有執行工作所需的最低存取權？
☐	☐	您的組織是否定期修補系統和軟體？
☐	☐	您的組織的安全性工具是否運用 AI/ML 功能，以協助主動識別漏洞？

檢查清單：

偵測及因應威脅

偵測及因應網路威脅，是任何安全性策略的基本要素。這涉及監控和分析網路流量、系統記錄和其他區域，以及安全資料，以識別未經授權的存取、入侵、惡意軟體感染、資料違規或其他網路威脅的跡象。這些問題有助於決定組織如何主動識別，並主動解決電腦網路、系統或組織中的潛在安全性事件和惡意活動。

是	否	
☐	☐	您的組織是否使用安全性工具和技術，例如擴展偵測和回應 (XDR)、入侵偵測系統 (IDS)、入侵防禦系統 (IPS)、SIEM 和記錄分析，來持續監控網路和系統活動？
☐	☐	您的組織是否分析收集到的資料，以識別可能表示潛在網路威脅的模式、異常狀況以及入侵指標 (IoC) 和/或攻擊指標 (IOA)？
☐	☐	您的組織是否已部署最新的可見度和監控工具，以快速偵測並警示潛在威脅？
☐	☐	您的組織是否會監控網路流量中，可能表示有進行中的網路攻擊的異常模式或可疑活動？
☐	☐	您的組織是否已導入任何 AI/ML 工具，透過即時分析異常資料模式或行為，協助偵測網路威脅？
☐	☐	您的組織是否考慮實施新一代 SIEM 解決方案，以更有效管理安全警示，並開始將整個 IT 生態系統中的安全性事件資料建立關聯？
☐	☐	您的組織是否實行漏洞測試和管理，以排定優先順序並解決現有漏洞，同時有效率地因應新的漏洞？
☐	☐	您的組織是否制定了事件應變計畫，來調查和緩解已確認的安全性事件？
☐	☐	您的組織是否整合了安全性協調流程、自動化和回應 (SOAR) 工具，以加速事件因應動作，進而幫助減少網路攻擊的傳播？
☐	☐	您組織的事件應變計畫是否考量到遏止原則、通訊計畫、合規要求、鑑識分析和復原程序？

檢查清單：

從網路攻擊中復原

從網路攻擊中復原，是指在發生資安事件之後，將受影響的系統、網路及資料還原至安全且可運作狀態的過程。這涉及採取行動以減輕攻擊造成的損害，重新建置遭入侵或中斷的服務和裝置，分析事件以防止將來的攻擊，以及讓組織恢復營運正常。這些問題有助於判斷，您的組織是否有效地從網路攻擊中復原。

是	否	
☐	☐	您的組織是否已實施任何事件遏止措施，來隔離和遏止網路攻擊？
☐	☐	在事件得到控制後，您的組織是否制定了還原系統和/或裝置的程序？
☐	☐	在保護資料時，您的組織是否使用資料隔離、不變性或網路存放庫？
☐	☐	您的組織是否已建立程序，以便在資料遭到入侵、加密或刪除時，徹底地還原資料？
☐	☐	您的組織是否使用 AI/ML 技術，協助自動化或加快從網路攻擊中復原的速度？
☐	☐	在遭受攻擊和復原後，您的組織是否持續評估事件，並找出需要改善的領域？
☐	☐	您的組織是否已執行鑑識分析，以瞭解攻擊方法、判斷外洩程度、識別受影響的系統和資料，並收集證據，以協助您提高安全性並採取法律或懲戒行動？
☐	☐	您的組織是否知道要通知相關方 (如客戶、合作夥伴和廠商) 有關此網路攻擊，以及可能對其資料或營運造成的影響？
☐	☐	您的組織是否每年多次實踐您的復原策略，以獲得復原業務的信心並滿足 SLA？
☐	☐	您的組織是否與服務供應商協同合作，以協助組織復原？

進階網路安全與零信任成熟度

在網路安全方面，IT 組織必須為最糟的情況做規劃，並具備多層防禦機制。在瞬息萬變的網路安全威脅情境中，持續推廣安全性實務並接受零信任原則，至關重要。這包括：

減少攻擊面

徹底減少可能用來入侵環境的漏洞和進入點。

偵測及因應網路威脅

主動識別並解決潛在的資安事件和惡意活動。

從網路攻擊中復原

在安全事件後，幫助組織恢復至先前已知可正常運作的安全狀態。

透過運用專業服務的專業知識，並與值得信賴的業務合作夥伴協同合作，Dell 可協助組織建立全方位的安全狀態，防範不斷演變的網路威脅。隨著技術的不斷進步，我們的網路安全方法也必須如此，以保護我們的數位基礎結構，並維持對數位領域的信任。

DELL Technologies

關於 Dell Technologies

Dell Technologies 協助組織與個人建構數位未來，並改變他們工作、生活和娛樂的方式。該公司為客戶提供業界最廣泛且最創新性的技術和服務產品組合，以因應資料時代的需求。

如需深入瞭解，請前往
www.dell.com/securitysolutions