DELL Technologies

5 解決零信任需求的建議

1	2	3	4	5
規劃將典範轉變為「絕不信任，一律驗證」	**確定所需的路徑**	**是組織推動零信任環境，而不是反過來**	**著重於資料**	**在整個 IT 生態系統中落實「絕不信任，一律驗證」**
在風險緩解和業務影響之間，決定可接受的取捨結果	遞增的安全性強化功能	根據業務需求建立控制措施	確保持續記錄所有網路、裝置和使用者活動	必須普遍套用多因素驗證和身分識別管理等零信任活動，以避免出現重大漏洞
考慮成本、對營運和利益關係人的影響，以及法規遵循和法規要求	超大規模使用者	記錄流程、角色、職責和資料分類	利用 AI 和 ML 分析資料，並識別可能象徵威脅的異常狀況	在零信任框架中，納入第三方實體和數位供應鏈
從以邊界為基礎的安全性，發展為以資料為中心的微切分模式	專屬環境	使用者經驗依然至關重要	請記住，保護資料和應用程式是零信任架構的關鍵角色	
視需要利用外部協助	身分識別是新的邊界	零信任等安全性強化功能，不能以犧牲可用性為代價		
		成長和創新等組織目標依然是重中之重		

人們普遍認為零信任是安全性架構的最佳實務做法。

資料顯示，大多數組織已開始考慮或正在實施零信任[1]。雖然轉變為零信任很重要，但有一些實際的考量將有助於引導這一過程。

Dell Technologies 主題專家 Project Fort Zero 解決方案採用主管 Tracy Emmersen 和首席安全性工程師 Justin Vogt，與安全服務產品經理 Ash Lakshmanan 分享了他們的建議與見解。他們的關鍵建議總結如下，或者您可以在 dell.com/cybersecuritymonth 觀看他們的完整對談。

> 「當我們退後一步，從整體的觀點來看零信任時，就會發現一切都與資料有關。」
>
> ***Tracy Emmersen***
> *Dell Technologies Project Fort Zero 解決方案採用主管*

規劃將 (重大) 典範轉變為「絕不信任，一律驗證」

從根本上說，邁向零信任環境代表重大轉變，從歷史安全模式邁向以「絕不信任，一律驗證」和最低權限存取為基礎的原則。Emmersen 指出：「我們需要以不同於過去的方式，看待我們的安全狀態，擺脫傳統以邊界為基礎的網路安全解決方案，更傾向以資料為中心的微切分架構。」

確定所需的路徑

Emmersen 說明了實現零信任優勢的三種截然不同的路徑：

- **遞增：**為當前環境帶來關鍵零信任原則的迭代方法
- **超大規模使用者：**利用主要雲端提供商的零信任功能
- **完全合規的專屬環境：**從頭開始組建的私人內部部署環境，嚴格遵守零信任標準

除了這三條路徑之外，虛擬化的中小型企業還可以採取一種稱為「身分識別是新的邊界」的方法。此方法側重於身分識別和存取管理，並利用 SaaS 工具實現以零信任為基礎的保護。此方法的一個關鍵要素是在每個地方實施多因素驗證 (MFA)，這也說明了零信任功能的影響。

超大規模使用者和身分識別方法的成本通常較低，而遞增和專屬環境則需要更多投資。

是組織推動採用零信任環境，而不是反過來

從根本上說，零信任架構旨在管理和保護組織的工作流程、使用者角色和相關權限、裝置、資料、應用程式和網路。實作的第一部分需要這些方面的可靠記錄，然後控制平面和基礎結構則是專為強制執行治理原則所設計。

如果零信任環境抑制或顯著改變業務營運，從而損害組織利益，那麼無論實現什麼強化的安全性，都可能不值得。正如 Vogt 指出：「如果 [安全性] .....妨礙了組織的核心使命.....我們真的不比我們試圖中斷的攻擊者更好。我們只是自行停止服務。」

著重於資料

正如 Emmersen 指出：「當我們退後一步，從整體的觀點來看零信任時，就會發現一切都與資料有關。」保護組織資料是轉換為零信任最有價值的優勢之一，而持續驗證和分段等原則，則可防止威脅在網路內橫向移動，以保護資料和應用程式。

記錄和持續監控是零信任的關鍵要素，會分析資料和遙測，以識別可能表示存在風險或威脅的異常情況。例如，資料使用模式的改變，可以指出潛在的外流或勒索軟體攻擊。

1. 摘自 Dell 委託企業策略集團進行的研究，《Assessing Organizations' Security Journeys: Insights Spanning the Attack Surface, Threat Detection and Response, Attack Recovery, and Zero Trust》(評估組織的安全性歷程：涵蓋攻擊面、威脅偵測與應變、攻擊復原及零信任等層面的深入解析)，2023 年 11 月

DELL Technologies

有鑑於記錄所有活動會產生大量資料，現代分析工具必須使用 AI 和機器學習才能具有實效。

必須貫徹套用「絕不信任，一律驗證」

雖然資料、應用程式、使用者和裝置大部分是內部的焦點，但零信任架構固有的審查必須套用至整個 IT 生命週期。否則可能會留下嚴重的安全漏洞。

供應鏈就是一個很好的例子，Vogt 建議詢問有關第三方硬體和軟體的重要問題：

- 「還有誰能存取？
- 由什麼組成？
- 背後還有什麼在執行？
- 即使我們正在使用的技術屬於技術供應鏈的上游，我們要如何才能對這些技術，套用這些不信任的原則 [和] 某種驗證程序，以及某種最低權限狀態？」

邁向零信任架構或實施其原則，是提升網路安全成熟度的當前最佳實務做法。有幾種路徑代表了成本、風險和安全性強化層級之間的不同取捨。第一步應該是確定組織的獨特定位，並據此引導技術決策。

造訪 **dell.com/cybersecuritymonth**，瞭解如何解決當今一些主要的網路安全挑戰