使用零信任擁抱主動式安全性

實際部署和攻擊正在形塑零信任的未來。我們的架構、關鍵趨勢和成熟度模型可加速您的旅程。

取得技術白皮書

選擇零信任的原因

現今的組織需要新的資訊安全模型，能更有效地適應現代化環境的複雜性，採用混合式工作場所，以及保護任何位置的人員、裝置、應用程式和資料。

隨時隨地保持生產力

讓使用者可以隨時隨地在任何裝置上更安全地工作。

雲端移轉

為現今複雜的環境啟用具有智慧型安全性的數位轉型。

風險降低

封閉安全性缺口，並將橫向移動的風險降到最低。

取得零信任商務方案 >

零信任原則

明確地驗證

一律根據所有可用的資料點進行驗證和授權，包括使用者識別、位置、裝置健康情況、服務或工作負載、資料分類和異常。

使用最低的特殊權限存取

使用即時且足夠的存取權 (JIT/JEA)、以風險為基礎的適性原則以及資料保護來限制使用者存取，以協助保護資料和生產力。

假設有缺口

將波及範圍縮到最小並區隔存取權。驗證端對端加密並使用分析功能，取得可見度、驅動威脅偵測和改善防禦能力。

零信任旅程的下一步是什麼？

評定貴組織的零信任成熟度階段並獲得目標里程碑指導方針，外加精選的資源和解決方案清單，以在全方位安全性態勢中向前邁進。

進行評定 >

零信任定義

零信任模型並不認為公司防火牆後的全部內容都是安全的，而是假設有缺口並驗證每個要求，就像它是來自開放網路一樣。無論要求來自何處或存取什麼資源，零信任教導我們「絕不相信，一律驗證。」每個存取要求都必須經過完整驗證、授權並加密之後，才會授與存取權。套用微區隔方法和最低特殊權限存取原則以最小化橫向移動。豐富的情報和分析功能可用於即時偵測和回應異常狀況。