

Workspace ONE 的零信任安全性

問：零信任是什麼？

答：零信任是條件式存取控制模式，需要持續驗證信任，才能允許最低權限存取應用程式和資料。零信任背後的策略歸結為遠離傳統的安全性方法；傳統方式視網路週邊內的所有資源為可信任，零信任則改為採用「永不信任，一律驗證」。與傳統的安全性方法相比較，零信任有動態的決策點，會驗證信任並影響對企業應用程式和資料的存取層級。

問：零信任為一想法、功能或產品嗎？

答：零信任為一安全性模式，有一套指南，目標在於提供企業端對端安全性，即使在 IT 擁抱行動化和雲端等新技术時亦然。此模式的概念仰賴持續驗證裝置合規和使用者身分識別，之後才能以最低要求的權限授予對企業應用程式和資料的存取權。

問：為什麼需要零信任？

答：傳統的安全性方法是根據週邊有界限的環境進行開發，同時針對組織網路內部的每個人採用隱含信任。這類似於「城堡與護城河」方法，重點幾乎都是在透過 VPN 和網路存取控制等技術建立「護城河」。不過，隨著行動化和雲端等技術的出現，我們所知的網路週邊今日已不復存在。我們需要新的安全性方法，這個方法仰賴持續驗證合規，並可保護應用程式和資料，不論是從何處存取以及存取的裝置為何。這正是零信任採取的方法。

問：為什麼零信任現在關係重大？

答：零信任由 Forrester 的 John Kindervag 在 2010 年創造，是一個仰賴「永不信任，一律驗證」概念的安全性方法。這所強調的是信任的概念，以及受惠的惡意源起方如何滲透似乎是受信任但實際上已遭入侵的裝置（例如透過網路釣魚攻擊、惡意軟體等）。隨著組織擁抱數位工作區，諸如裝置選擇（行動、桌面、物聯網）、彈性的工作型態（在網路內部和外部）以及應用程式異質性（軟體即服務、網路、原生、虛擬）的概念已成為真實並共同存在。在如此動態的環境中，使用者會從任何裝置存取任何應用程式，我們需要一種同樣也有動態特性的安全性方法來持續驗證信任，才能允許存取機密資訊。安全性缺口的案例不斷增加，最近的缺口問題是由公司過期的安全性原則所造成。零信任方法的相關性更甚於以往。

問：零信任的主要宗旨為何？

答：雖然有多個由不同公司和組織定義的零信任存取模式（Google 的 BeyondCorp、Forrester 的 Zero Trust eXtended、Gartner 的 CARTA 等），VMware 的 Zero Trust Architecture 指定五個主要宗旨：

- 裝置管理和合規 - 確保裝置的合規狀態
- 條件式存取 - 可使用升級驗證功能來確認使用者身分識別
- 應用程式通道和 Proxy - 保護到資料中心的路徑和虛擬桌面的安全性，並部署減少攻擊表面的技術
- 風險分析 - 透過增加能見度與行為分析來提升安全性
- 修復和協調作業 - 運用自動修復和協調作業來強化安全性及經驗

問：客戶是否必須遵守所有原則才能擁有零信任 IT 環境？

答：遵守零信任旅程所有原則，可在持續演進的 IT 環境中提供企業端對端的安全性存取控制，包括提供對雲端或內部部署中的應用程式存取權。不過，對大部分組織來說，在公司重新思考及投資於能為他們提供完整零信任環境的技術時，零信任將會是一趟持續多年的旅程。此外，每個組織將會有自己的旅程，端視他們想要保護的應用程式以及他們如何加入數位化轉型而定。

問：我的客戶已有其他安全性解決方案。零信任會如何影響這些投資？

答：VMware 適用於數位工作區的零信任方法不會限制特定廠商。此方法的主要宗旨基礎為向企業提供最佳安全性，同時與「永不信任，一律驗證」的零信任原則保持一致。Workspace ONE 提供跨平台、彈性的端對端零信任安全性，並支援所有應用程式。除了保持彈性並可擴充之外，Workspace ONE 也可輕鬆整合其他協力廠商的威脅擷取解決方案或協調作業，讓客戶能夠運用其現有投資，同時仍能達成其零信任目標。

問：客戶能以購買產品的方式來購買零信任嗎？

答：否。客戶必須判斷其需求，並將其對應至適當的 Workspace ONE SKU。如需關於 Workspace ONE SKU 的詳細資訊，請於此處取得。

問：VMware 收購 Carbon Black 會如何影響 VMware 的零信任定位？

答：Carbon Black 是業界在端點和工作負載安全性方面的領導者之一，為 VMware 的零信任安全性方案帶來極大價值。透過新的 Workspace Security 套件，Workspace ONE Advanced 客戶可以利用 Workspace ONE Intelligence 和現有的信任網路整合來擷取從 Carbon 的 Black Next-Gen

Antivirus (NGAV) 和端點偵測與回應 (EDR) 產品 CB

Defense 偵測到的即時威脅資料，來計算風險分數並評估合規狀態。這有助於持續驗證信任並增強 VMware 的數位工作區零信任方案。

問：從何處可以更進一步瞭解零信任？

答：任何人士若想要深入瞭解 VMware 對於將零信任運用到數位工作區的定位，請在此處造訪數位工作區的安全性網站，取得詳細資訊。您也可以在此處的技術區網站上取得深入的技術資訊

問：專業服務是否能協助為客戶執行零信任方案？

答：是。現已推出專業服務方案，協助您啟用不同的服務，以開始零信任旅程。如需如何開始使用的詳細資訊，請聯絡您的業務專員

問：客戶可以如何開始其零信任旅程？

答：客戶可以造訪 TechZone 取得詳細的技術說明文件和以使用情境為基礎的實作指引以開始使用。請聯絡您的業務專員以深入瞭解不同的 Workspace ONE 解決方案，協助展開您的旅程 A。VMware Solution Exchange，網址：
<https://marketplace.vmware.com/vsx/>，可提供合作夥伴解決方案的更多資訊。

