後疫時代全球零信任網路發展趨勢

台灣亞太產業分析專業協進會 106 年認證資深產業分析師 徐富桂

雖然全球已從全面封鎖到逐漸解封，但是在歐美仍然建議員工大部分繼續採用居家上班 WFH(Work From Home) ，已成為後疫時期的新常態。而隨之帶來的新一波遠端接入需求以及資安的問題，不僅讓 VPN 在全球性大規模遠端辦公巨變中大幅成長，同時也因網路資源消耗、連網速度卡頓影響辦公效率而備受批評，進而讓全球企業思考更好更安全的網路安全架構，而讓實施零信任網路架構迎來最佳發展時機。雖然「零信任」一詞已被提出 10 年，然而，COVID-19 疫情加速了因應遠端工作帶來了的網路威脅解決方案的殷切需求。依麻省理工學院及斯坦福大學在 5 月進行的一項調查發現，在美國已超過 50%的人員在家工作，而之前大約只有 15%。而另一項調查發現，與 2020 年 1 月相比，在 6 月份，員工點擊到惡意 URL 的風險提高 49%。整體而言許多公司在尋求營運數位轉型過程中，已讓「零信任」技術在過去兩年中贏得了不少擁護者，只是新常態經濟讓它一夜成為新寵。

一、 零信任網路技術簡介

(一) 網路安全的新挑戰

網網相連的 Internet 開始運轉之後，為了保障企業內部的安全，築起網路邊界，區隔內、外網，並將防火牆放置在重要的網路節點上，將外部網路威脅阻隔在外，只信任網內的使用者與設備成為標準架構。但是隨著雲端服務、行動上網與物聯網的蓬勃發展，網路安全也面臨了巨大的轉變。過去的網路安全部署是將重要的資料、伺服器保護在一個集中的網路高牆內，只要在出入閘道執行好的安全保護策略就可高枕無憂；而現在情形更複雜了，包括

1. 企業內部網路上增加了各式不同類型的使用者，包括承包商、第三方供應商和連接到公司網路的遠端工作人員等。

2. 越來越多的使用者使用自己的設備，比如智慧型手機、平板電腦等都可以連接型企業內部網路。

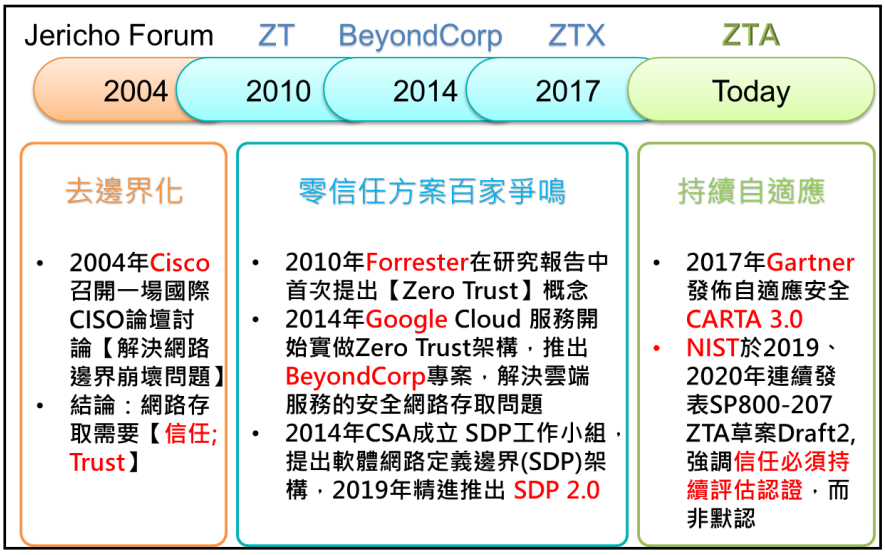
3. 全球化的營運，讓企業採用雲端服務、雲端儲存、資料中心等將重要資料放在外部公有雲的情形逐漸增加。

4. 物聯網裝置連接至公司專用服務也成為存取公司內部網路的另一個重要入口。

使用者、設備和雲服務的交互聯接，複雜度不斷增加，使得傳統網路定義的「網路邊界」早已成為不復存在的界線，造成網路安全防護新的挑戰。

(二) 何謂零信任網路安全架構

針對網路安全面臨的挑戰，2004 年 Cisco 召開一場國際 CISO (首席資安官)論壇，討論網路邊界崩壞，唯有建立起一個「可信任」的安全管理模型，才能夠讓使用者的認證及授權可信、資訊流及資安風險能夠可見可視及可控可管。尤其是傳統網路安全模型認為組織內部網路的人、物均應是可以信任的，但真實的世界不是這樣運行的。太多的信任就是一個漏洞，尤其是進入內部網路後，使用者(包括威脅行為者和惡意內部人員)可以自由地橫向移動並存取或洩露不屬於他們必要知道的任何數據，這就存在極大的風險。因此，Forrester Research 前副總裁 John Kindervag 提出了【Zero Trust】概念，認為應預設任何的網路存取要求均不可信任，唯有經過認證之後，才可以依政策權限存取。



資料來源：工研院產科國際所 ITIS 研究團隊(2020/09)

圖一 零信任網路概念發展歷史

支援零信任網路概念的安全技術近年來迅速發展，為零信任的實踐提供了豐富而實用的工具、框架和方法。而且實踐零信任網路架構也不是只有唯一的標準答案，可謂條條大路通羅馬。可以將各種網路安全技術模組、方法整合在一起，確保【只有經過安全驗證的使用者和設備才能有最小的權限去存取目標應用程式和資料】。

例如，最小化存取權限原則，就是僅為使用者提供完成工作所需的最少資料和許可權。這包括實施【限期特權】和【一次性憑證】等，這些存取憑證在不需要後會自動作廢。此外，還需實施連續檢查和流量記錄，並限制網路存取範圍，以防止資料在系統和網路之間未經授權的橫向移動。

若以產品與服務角度，Zero Trust 零信任網路安全架構涉及身份認證、網路安全、資料安全、端點安全、安全分析、資安營運自動化響應(SOAR)及資安策略管理等眾多產品與服務。

二、全球零信任網路發展現況

(一) CSA 訂定軟體定義網路邊界 SDP 架構

2014 年 CSA(雲端安全聯盟；Cloud Security Alliance)有鑑於新型態的數據中心、混合雲等應用的興起，造成網路邊界的不斷變化，不論是有多個網路分段或不同權限的遠端存取等，都對防火牆(甚至新世代防火牆 NGFW)、VPN 等帶來極大的挑戰。CSA 啟動了軟體定義網路邊界(SDP；Software Defined Perimeter)的架構及研究，即推出 SDP 1.0 的架構指南，利用實現有效的身份驗證和授權之後，才可以存取當次的網路服務，以實現零信任網路的概念。

CSA 並在 2019 年 5 月再度精進推出 SDP 架構指南 2.0 版，在美國國土安全部的支持下，建立開源的實作參考(http://sdpcenter.com/test-sdp/)，利用經過驗證的標準組件來阻止針對雲端應用程式的網絡攻擊，幫助企業依照指南即可成功部署 SDP 解決方案。

(二) NIST 發佈零信任架構 ZTA

美國國家標準技術研究所(NIST)發佈的零信任架構(ZTA；Zero Trust Architecture)，是美國政府採用零信任架構的指南，目標是希望可以讓更多的組織/機構能夠受益於零信任架構的好處。NIST 更提供多種實施零信任架構的示範建議，希望 ZTA 不僅能在大型企業

落地，同時在小型企業中也能發揮作用。並認為不管採用何種實做方式(包括增強身份治理、網路微分段、以及基於網路基礎架構和 SDP 等)，ZTA 應該圍繞著企業本身的數位資產防護且遵守零信任原則宗旨進行，而具體的實現方式應結合企業現狀，而不是照本宣科直接援用。另外，風險評估也成為零信任的重要內容之一，企業如果希望向 ZTA 遷移，在考慮技術替代的同時，應該重視風險評估工作。NIST 在 2020 年 2 月公佈的 ZTA Draft 2 (SP800-207)標準草案第 2 版中再次強調【零信任是一種以資源保護為核心的網路安全示範，其前提是信任從來不是隱藏式默認的，而是必須進行持續評估認證】。NIST 更重新定義認為，零信任(Zero trust, ZT)是一種不斷發展的網路安全示範術語，將網路安全防禦政策從靜態的網路邊界防護改為關注使用者、數位資產及關鍵資料及資源的動態防護。

(三) 主要國際大廠在零信任框架的發展

因為零信任架構並不是指特定的技術，而是多種技術的應用整合，只要供應商的產品、服務或產品組合，可以協助實現零信任目標，就算是零信任架構下的供應商了。目前各家廠商的零信任框架，也都使用了多種安全技術來增加對機敏性資料和系統的存取進行細微化控制。例如使用者身份和訪問管理(IAM)、基於角色的存取控制(RBAC)、統一管理策略的網路存取控制(NAC)、多因素身份驗證(MFA)、加密、存取策略編排、日誌記錄、分析以及風險評分和檔案系統許可權等各式產品。

因此，最早提出零信任架構的研究機構 Forrester research 在 2019 年底選出了 14 家提供零信任網路安全架構產品的主要廠商，並依相關的評估指標，認為思科、Illumio、Palo Alto Networks、Akamai Technologies 和 Okta 等公司位於市場領先地位。不過 Cyxtera Technologies、MobileIron、賽門鐵克、Unisys、Forcepoint、Google、Check Point 和 Forescout 等廠商的表現也很出色；Proofpoint 則是未來的競爭者。

三、 結論：零信任網路未來動向

Zero Trust 零信任網路安全架構將成為未來十年主流的網路安全架構之一。根據 MRFR(Market Research Future)在 2020 年 5 月報告，全球零信任網路安全架構相關市場成長快速，預測 2019-2025 的年複合成長率達 15.4%，預計在 2025 年將達約 320 億美元。其中北美

市場因數位化程度以及法規需求對於零信任網路安全架構解決方案的需求最高。此外，由於雲端服務帶來的大量網路存取風險，亞太區將成為全球零信任網路安全市場中增長最快市場。

觀察成功實施零信任網路的最重要決定因素，是網路存取策略的動態授權管理。因此在零信任架構中，必須有一個可以收集檢查內、外部網路流量日誌，對於使用者的存取行為分析、應用存取進行動態授權，持續優化安全策略的「智慧中心」，而各大廠商莫不大量投入於建立以 AI 為中心的零信任大腦，針對網路安全性政策以及應用服務、使用者、設備、數位資產等的信任狀態主動決策推斷進行研發。

展望未來，以【人】為中心的「零信任 Zero Trust」網路架構成為未來企業安全存取的必然發展，搭配實體、安全的硬體密鑰取代不安全的人工密碼已箭在弦上，加以隨著 5G 時代的來臨，不論是開發安全網路存取代理及控制引擎，或是發展以 AI 為中心的網路存取分析策略中心等網路安全設備，都是臺灣資安產業可以發揮的地方。

(本文作者為工研院產科國際所執行產業技術基盤研究與知識服務計畫產業分析師)

原文出處：ITIS 智網 http://www.itis.org.tw/