駭客終結者 2.0 登場！打破舊有資安概念，零信任架構 (ZTA) 引領資安新風潮

110/09/07 17582

簡如茵 | 科技大觀園特約編輯

台科大教授兼資通安全研究與教學中心查士朝主任專訪

> 現今，人們對於網路的依賴性大，尤其是疫情影響下的社會，各家企業紛紛採取居家辦公，此外，日常中的網路銀行轉帳、購買日用品、電子信箱等功能均需利用網路。但網路便利的同時，伴隨而來的就是，個資外洩、網路上的購賣身分遭到惡意人士盜用，魔鬼藏匿於網路的角落，緊盯著各個使用者的活動，看看誰是下一個受害者。為了層層把關網路上的潛在危機，零信任架構 (Zero Trust Architecture，ZTA) 出現了！ZTA 是一種資安防護的新概念，打破了傳統以邊界（例如防火牆）區分內網及外網的資安型態。今天，想長點 ZTA 的新知識嗎？跟著查士朝教授的腳步來探索一下這個酷東西吧！

查士朝教授小簡介

查教授是台灣大學資訊管理博士，曾任職於意藍科技資深技術顧問，於資誠企業擔任資深經理。現為台灣科技大學資訊管理系教授，同時也身兼資通安全研究與教學中心主任。查教授獲得許多國際資安認證，近年致力於資訊安全相關研究，參與多項產學合作計畫，並協助政府建立資訊安全管理制度，並發掘系統資安漏洞以研擬推動智慧型手機應用程式安全與物聯網裝置安全檢測標準。

跳到主要內容

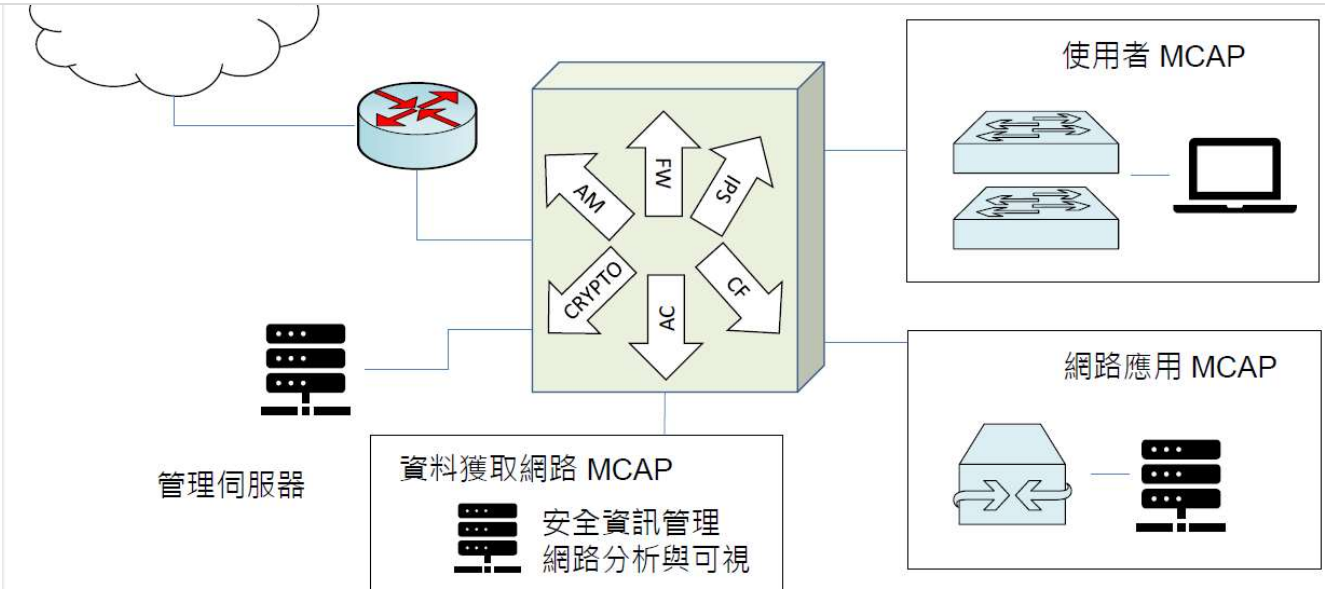
查士朝教授近幾年於資訊安全制度訂定及設計發想貢獻良多。圖 / 查士朗教授提供

ZTA 的誕生與發展

2003 及 2004 年間，傑里科論壇 (Jericho Forum) 為了達到網路資源於企業間共享的目的，因此想出了消除企業與企業間的網路邊界，但這個做法也造成了網路安全的漏洞，而解決這個漏洞的技術性方案就是 ZTA 的最初架構。可以說是無心插柳，柳成 ZTA 阿！但是，這個論壇當初提及的 ZTA 概念還是滿抽象的，因此，Forrester Research 前副總裁 John Kindervag 於 2010 年提出了具體的概念，他提出了三大核心理念：（一）裝置不再有信賴與不信賴的邊界，（二）不再有信賴與不信賴的網路，（三）不再有信賴與不信賴的使用者。而實際上的做法需要四大核心元件：

1. 網路分區閘道 (Network Segmentation Gateway)：當前的網路需要透過許多安全設備來保護其整體環境及數據，例如我們最常見的就是防火牆，還有為取得公司或機構內部存取權所需要用到的工具 VPN 。而 John Kindervag 想要開發出一個結合所有安全設備特性及功能的網路分區閘道（最強守衛者的概念），並將安全性構建到網路的架構當中，以安全的方式正確分割網路資源。
2. 創建平行且安全的網路分區：打破以往防火牆只一分為二，阻隔外界及保護內部的功能。這裡運用的是微核心邊界 (Microcore and perimeter, MCAP)（圖二），你可以把它想像為「保護套」，將你想保護的資料都個別套起來，像是使用者端、網路應用、資料獲取網路都自己有一層保護套。如此一來，將資安防護不再單單只靠一層防火牆，而是個個資料、系統都有盾牌可以做自我保護。
3. 網路後臺集中管理：承第 2 點提及的「保護套」，網路後臺是擔任管理這些微核心邊界 (MCAP) 的角色，增加操作上的便利性。
4. 建立數據蒐集網路以掌控網路整體狀況：對於修繕故障網路的人來說，要能有效取得數據包是件非常困難的事，但在零信任網路中採用數據蒐集網路 (data acquisition network, DAN)，此種方法結合網路分區閘道，能有效採集各個微核心的數據，加速數據取得以便E

跳到主要內容

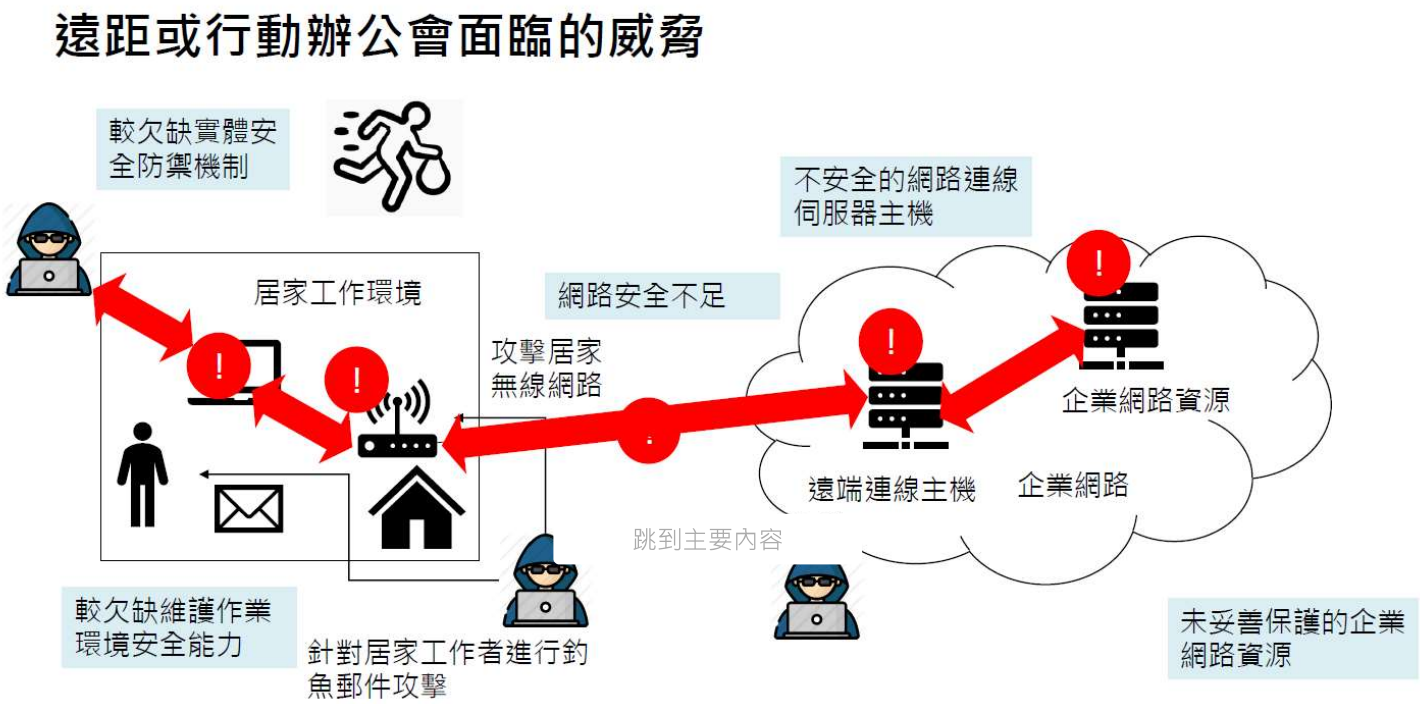


微核心邊界 (Microcore and perimeter, MCAP) 使整體網路環境又多一層保障。圖 / 查士朝教授提供

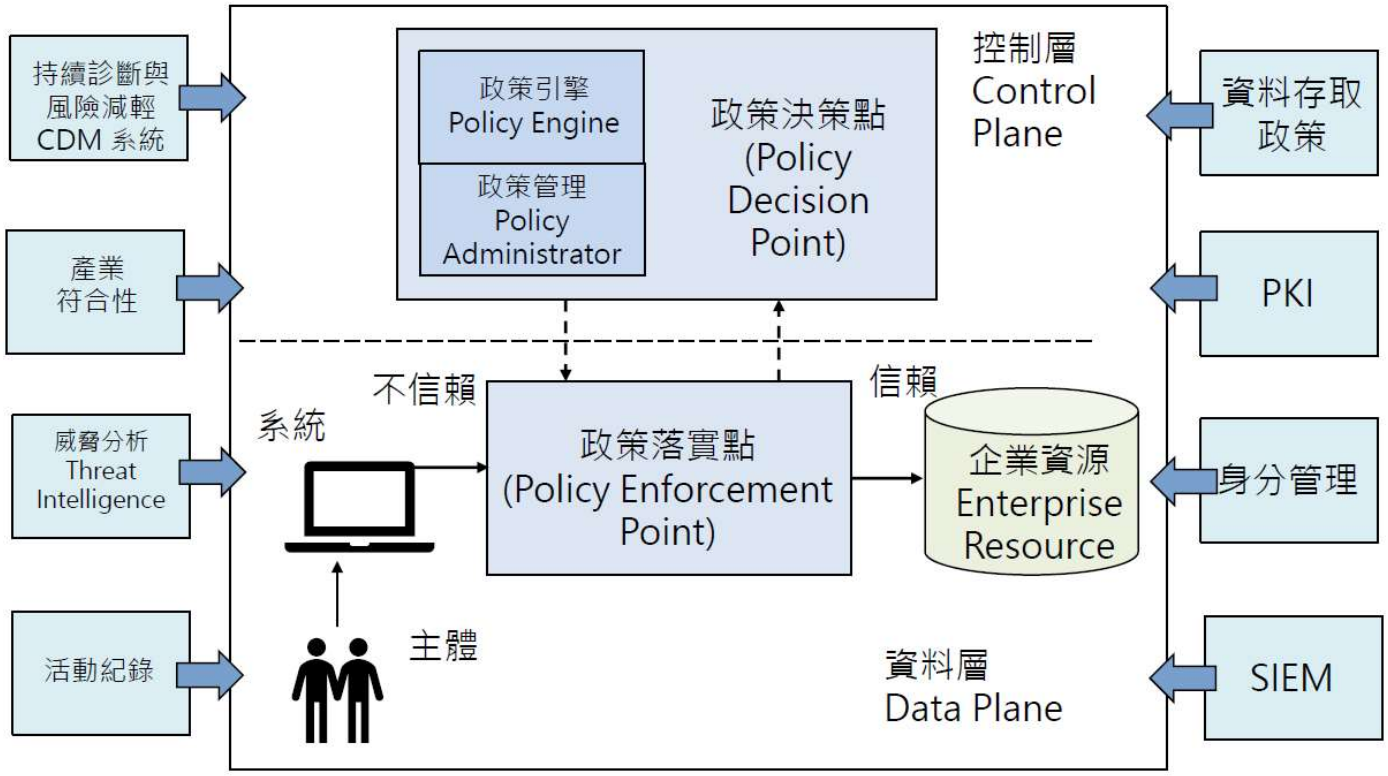
此外，美國國家標準技術研究院 (NIST) 也量身打造 ZTA 的標準指南 SP 800-207，時至今年美國政府所公布的網路安全策略中也包含了零信任架構，甚至要求美國聯邦政府網路導入零信任架構的網路安全策略，足見零信任網路架構在整體資安領域上佔有一席之地。當中，SP 800-207 講究七大原則：(1) 識別可存取資源；(2) 確保連線安全；(3)妥善存取控制；(4)考量存取者狀態；(5)了解資源狀態；(6)監控裝置與資源風險；(7)持續收集資訊與改善。

現今資訊安全防護存在什麼樣的漏洞？ZTA 如何防範的資安危機？

新聞報導資安危機事件層出不窮，於個人，個人資料被盜用、信用卡被盜刷；於企業，美國淨水廠系統及最大燃油管系統、銀行 ATM、國內科技大廠都曾遭受駭客及勒索軟體襲擊；於國家，國安危機更是重大事件。查教授講道過去的資安架構，往往只是透過防火牆等相關架構，將安全與不安全網域劃清界線，並且只注重防範邊界，無法防止內部橫向擴散。然現今惡意駭客早已能夠輕鬆越過此界線，橫行於安全網域之中。



「手」，政策落實點 (Policy Enforcement Point，PEP) 是 ZTA 的手，當使用者發出存取公司內網資源的要求時，PEP 會先接收到這個訊息，並將此訊息傳遞給政策決策點 (Policy decision point，PDP)（也就是 ZTA 的大腦）決定是否允許這位使用者的要求，在 PDP 下達決定後，PEP 便會聽從這個決定做出相應的舉動。而 PDP 內部則是仰賴所謂的信賴演算法，它會考慮存取要求、主體資料庫及歷史、資產資料庫、資源政策要求、威脅情資與紀錄來做訓練，當然現今的 ZTA 架構會依照各個企業或機關的需求而有客製化的調整。



政策落實點 (PEP)及政策決策點 (PDP)是 ZTA 的核心機制之一。圖 / 查士朗教授提供

ZTA的迷思

迷思一：零信任架構 = 完全不信任任何使用者？

ZTA 是為了防止有心人士在進入企業內網後就能肆意做出任何惡意行動，但如果你是一個正常的使用者，只要通過認證，ZTA 還是會信任你的。

迷思二：ZTA 真的方便用嗎？會不會一直需要驗證？

查教授回答道 ZTA 通常會以連線為基礎做出行動，若是新建立連線必然要經過一次驗證，之後便會自動存取使用者驗證，並依照各家企業規定設定間隔多久需再驗證一次，所以不見得都要一直驗證。

迷思三：ZTA 在驗證、授權的過程中，均需要取得使用者和其使用裝置的相關資訊，是否會引發隱私權益問題？

跳到主要內容

查教授仔細講道，若是疫情下在家工作，使用[illegible]內網，ZTA 確實有可能會看見私人電腦上的隱私資料。但是最簡單的解決方法，就是使用公發電腦或設備，這樣就不怕自己電腦的東西被看光光囉！

迷思四：ZTA 可以完全取代 VPN？

ZTA 的未來展望及挑戰

查教授認為目前主要有兩項挑戰：一、要達到零信任架構的整合，以現在的設備發展，不太可能把所有的設備都換掉，因此如何將既有設備整合到零信任架構、達到相關要求是一個重點。二、上述所提及的信賴演算法訓練程度也是一大重點，它是 ZTA 的核心，假使訓練得宜，安全防護加倍，反之，問題可就大囉～另外，ZTA 在台灣可說是百家廠商爭鳴的主推架構，但查教授認為更重要的是，普及 ZTA 的概念宣導讓社會大眾理解其運作模式，如此，對於個人，能免於受到財務或個資損失；對於企業，能成為永續運作的一環，免於資安問題而殃及利害關係人權益；對於國家，不但能領先於資訊戰，更能提供民眾穩定、信賴的服務，維護公有設施系統的穩定性。ZTA 是新型態的保護概念，不單單只局限於個人研發上的努力，更需整體社會、企業、政府的致力推動方能共創榮景。

查教授給有志投入資安產業者的勉勵

查教授真切地說道資安的領域很廣，涵蓋了技術、管理、稽核層面，當然甲方和乙方的需求也不一樣，若想知道自己適合哪個領域、哪個職位，首先必須清楚自己的個性，究竟是穩定型，還是喜歡探索開發型。但無論如何，做資安產業的人個性都要正直，並把基本功打好。

結語

很榮幸這次邀請到查士朝教授探討關於 ZTA 的概念，透過教授清楚仔細的講解，想必讀到這邊的讀者們已經收穫滿滿，ZTA 雖然起初設計的基礎是建立在企業上，但查教授認為未來也可能透過多因素身分認證 (Multi-factor authentication, MFA) 廣泛運用於個人資訊系統。ZTA 的發展指日可待！

資料來源

[Build Security Into Your Network's DNA: The Zero Trust Network Architecture]
[Forrester Pushes 'Zero Trust' Model For Security]
[IMPLEMENTING A ZERO TRUST ARCHITECTURE]
[Zero Trust Architecture]
[SP 800-207, Zero Trust Architecture | CSRC]
[從內到外全面保護你的公司 | CIO Taiwan-台灣唯一專屬於企業資訊長的CIO媒體]
[思科、VMware、微軟競相打造，近年最火爆的資安議題Zero Trust 究竟是什麼]
[【網路世界徹底提升資安的自保之道】防護無邊界，零信任才能夠真安全]
[【搞懂零信任，從理解NIST SP 800-207著手】打造以零信任原則的企業網路安全環境]
[從企業資安直通國安的零信任架構]
[【臺灣資安大會直擊】看懂零信任架構 跳到主要內容 的3大迷思]
查士朝教授所提供的採訪資料

相關文章