不買新產品，你要怎麼做到零信任架構？

魔法師 駭客花生醬
發佈於 駭客花生醬

2023/05/15 閱讀時間約 14 分鐘

(Zero Trust Architecture) 一詞在臺灣風靡一時，各家資安廠商也搭上了這股風潮，什麼產品都要「零信
」「零信任」的產品就是資安萬靈丹嗎？

麼？

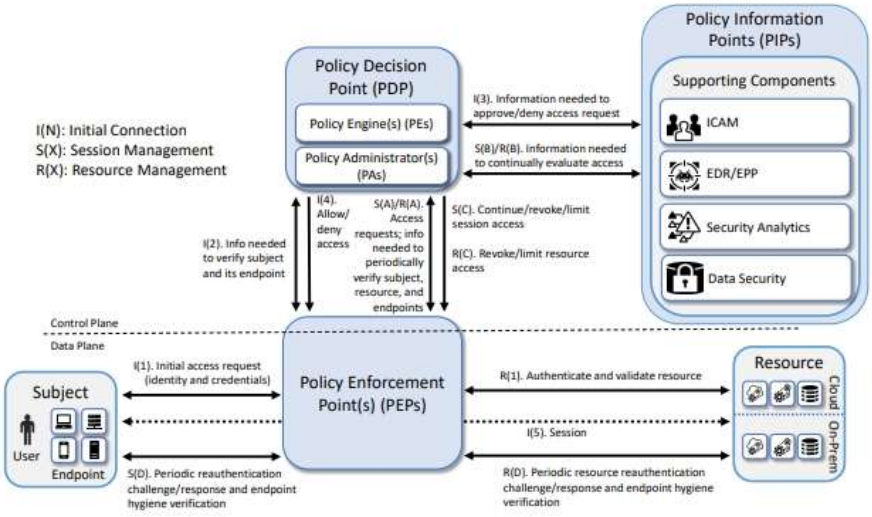
存取資料，首先要驗證使用者身份（例如生物識別＋密碼），接著又要同時驗證使用的裝置是否安全，
本次存取行為是否正常，才會被放行讓你存取資料。這樣的流程是不是聽起來很安全呢?

全的話，那你可以了解一下零信任架構。上述流程只是零信任架構中的一種情境，順帶一
的零信任網路也都只是零信任架構中的一環。

構 (Zero Trust Architecture, ZTA) 是一種資安策略和架構，其基本原則是**不信任任何用
，直到其經過驗證和授權。**

的核心概念為「不要有任何隱式的信任。」

：



以美國 NIST Zero Trust Policy 舉例

其中，有三個重要的名詞概念需要了解：

- PIP (Policy Information Point)：用於收集與分析所有可用的安全策略和資訊，例如身份

取路徑基本上是任重而道遠，不太可能一次到位。

因此，接下來本篇文章會分享我對於零信任架構的一些觀察與實作建議。對零信任架構的基礎概念尚不清楚的，可以閱讀 iThome 整理的〈ZTA 101〉，一般民眾也可以聽聽資安解壓縮的podcast〈EP51 - 別相信任，以對零信任架構有一些基礎認識。

前提：

一種產品。

之後，我們看到無數標榜零信任 OO 的各類產品在仿間大肆宣傳，但零信任不等於：

- 特權管理系統 (Privileged Access Management, PAM)
- 多重要素驗證 (Multi-factor authentication, MFA)
- 微切分架構 (Micro-Segmentation)
- 安全存取服務邊界 (Secure Access Service Edge, SASE)
- 虛擬私人網路 (Virtual Private Network, VPN)

等等等.....

了這套產品就可以「完全」實踐零信任，請多想想，我們要保護的資產千千萬萬種，不可以一體適用所有資產、所有產業、所有情境。零信任只是一種概念，而不是一顆萬靈丹。

上諸多產品分類，都只是零信任架構在實作時的**「子集合」**。在不考慮成本的情況下，這不錯的保護效果。舉例來說，Cloudflare 的 SASE 類型服務，每月 USD$ 7 元 / User，還是地端的 VPN 與網路分隔，價格也許可以更低一些。

零信任架構」，你也許可以導入上述產品分類。但就算不用——你也有機會做到。

不買新產品，你要怎麼做到零信任架構？

實施零信任架構需要進行裝置盤點、應用程式和服務的分類、控制更新管道、確認供應商對資安的掌控等。零信任不是不信任任何人，而是**沒有隱式信任**。在零信任架構下，環境中的所有東西，從裝置、應用，到網路都應該做到同樣的驗證，而不是預設相信他們都是安全的。

若是不看各種解決方案，針對零信任架構，我們如何將零信任的概念內化，實踐於企業的安全防護中？

以下將分為裝置、應用程式或服務、網路、身份進行說明。

置、或是沒有續約的老舊裝置等等，企業中可能存在這些敏感性高且資安風險等級高的防護漏洞。進行裝置的分類有助於確保我們能夠更好地管理和保護這些資產。

此外，確保裝置都安裝了最新的安全更新和修補程序也是十分重要的。如果企業自身對於己身的資產毫無概念、無法掌握。我認為比起購買解決方案，企業更應該優先解決這些基本問題。

主：以上所述的資產盤點與分類並非只限於 OA 區或部分敏感範圍，而是包含整個企業領域，像是那些常常被忽略的舊伺服器區。

服務全都是在雲端上，我相信你要實施一些零信任架構的措施是相較簡單的，但如果你的呢？

用程式或服務分為兩種類型：第三方、自主開發。

的零信任架構實作差異。

身無法掌握其核心技術的應用程式或服務。例如：企業資源規劃系統 (Enterprise , ERP)、員工系統、文件儲存裝置……等等。對於這些第三方的應用程式或服務，實施零信於：

更新管道：對於這類應用程式與服務，除了老生常談的保持更新，企業最好還要掌控更新管道。例如，Windows Update 獨立安裝程式 (Wusa.exe) 可以限制更新來源以及要更新的項目。此外，有些第三方的 IT 管理工具也可以管理端點軟體的更新。畢竟，來自第三方的應用程式與服務有可能因為其軟體供應商被攻擊，導致更新之中反而被塞入惡意程式，例如最新的 3cxDesktopApp 事件還有之前的 SolarWinds 事件，都是經典的供應鏈攻擊案例，因此，如果在第一時間就可以知道受害範圍或是控制更新範圍，便可以快速地進行資安事件處置。

2. 確認供應商對於資安的掌控度：雖然不是每個企業都有足夠大的體量和能力強制要求供應商遵守一定的資安標準，但常見的做法是要求供應商出示安全合格認證（包含但不限於 ISO27001、Common Criteria...）。除此之外，稽核團隊應該注意的是安全合格認證的「**範圍**」。臺灣最常見的情況是通過 ISO27001 的範圍只有機房，但開發人員或是存取資料的人員並沒有納入管理範圍。
3. 服務或應用程式的開發安全性：在採購時，供應商有責任提供安全評估報告（包含但不限於軟體弱點掃描報告、第三方測試報告...），並擁有安全的軟體開發流程（包含但不限於 SSDLC）。其中經常被忽略的是，供應商通常沒對軟體或服務使用的第三方函式庫進行盤點與版本控管。
4. 限制服務的網路：這在後面的「網路」章節也會再次提到。實施零信任架構前，肯定會

2. 程式庫管理：對於開發中使用的第三方程式庫，追蹤版本和確保安全性。例如定期檢查相關的漏洞和安全風險，並在必要時進行更新或替換。許多現今企業的開發工具或是版本控制軟體都是使用第三方的系統，而許多駭客會偽造類似名稱的程式庫讓開發人員不小心引用。

主：除了上述做法，應用程式應確保更新管道與使用套件根據最小權限原則，永遠認定是可能被攻擊的。

然是基本中的基本，但也是最難做好的。有些企業甚至連自己的網路拓撲圖都拿不出來。個面向都非常值得企業投資。

NS、HTTP、Email ，不要讓這些服務繼續裸奔了。DNS 應該是被很多企業遺忘的部分，不被竄改，或是防止被駭客偷看上什麼網站，都是很基本的措施。

與網段的管理。無論是微分段，還是傳統的網路分段，不同做法其實都有同樣的目標，那基於身份的隔離環境，防止攻擊者進入後能夠輕易地在網路中橫向移動，攻擊其他電腦。

信任架構並不代表完全沒有內外網，隔離環境需要根據企業的需求和風險進行調整，並且措施相互配合，才能真正實現網路的安全防護。而且一般來說，當企業有意識地去做網路消除」隱式信任更靠近一步了。

們加密各種流量，如何在監控網路封包與分析封包內容之間取得平衡就很重要了。檢查並流量是零信任架構的一個重要原則，但許多深度封包檢測 (Deep Packet Inspection, DPI) ecure Sockets Layer, SSL) 分析的產品，並沒有好好實作，導致可能有被中間人攻擊的風〈HTTPS Interception Weakens TLS Security〉）。另一方面，對網路全面執行 DPI 也，針對存放敏感數據並具有可預測性的來源和目的地的應用程式做封包深度檢測，其他的則是保留 Metadata 以進行異常分析。

身份

最後來到最多人討論的身份。這邊就不再說明 MFA 了，由於其十分重要，MFA 也是所有人在談零信任架構時最常說到的概念。那麼，除了 MFA 之外，還有哪些措施可以實踐身份上的零信任架構？

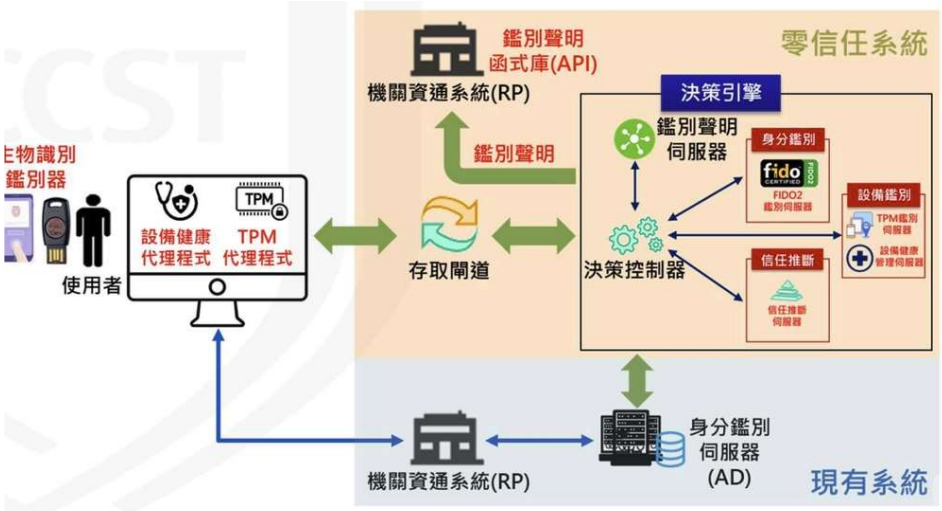
- **單一身份識別來源：** 盡可能地減少身份識別的來源並統一管道。想像一下，一個人要記 5~10 種帳號和密碼，哪天可能就忘記了。做好單一身份識別來源，能夠有效盤點使用者方面的風險。同時，當人員異動時也能快速進行反應，避免人員離職後卻因為過多身份沒有完整停用權限，使之還能違規存取。
- **權限盤點**：還沒盤點好權限的企業都應該格外注意。很多人看到權限盤點，第一時間會想到 PAM 這種解決方案，但這種解決方案的使用前提是你要知道帳號或是服務的存在才

的。

為什麼我會這樣認為呢？

零信任網路是一種保護網路安全的方法，它假設所有人都不可信，必須驗證身份和權限才能存取資源。然而，，沒有考慮到應用程式的安全性。

構」是一種更完整的安全方法，考慮了網路和應用程式的安全性，以及人和電腦之間的信的隱式信任盡可能地帶入架構中討論。



NCCST 政府零信任網路說明 - 截圖

說明 - 截圖

不難看出有借鑑許多美國 NIST 的零信任架構部分內容。所謂的存取閘道相當於 PEP，讓存通過它進行限制。而決策控制器相當於 PDP，作為決策的大腦根據各單位的政策去允許或拒絕存取，而各種身份與設備的代理程式相當於 PIP，用以輸入供決策的資訊。

然而，這樣的架構僅針對網路，無法等同於零信任架構。畢竟，被保護的資源或應用程式本身也可能存在問題，且資料的回傳也沒有必須經過決策系統。因此，僅透過零信任「網路」的保護方式，並不能完全保證資源或應用程式的安全性，必須透過零信任「架構」，綜合考量人、設備、應用程式之間的互動和信任關係，才能更全面地保障資訊安全。

總結來說，零信任架構並不僅僅是透過限制網路連線就可以解決的，它是整個資安策略的核心思想。因此，在制定資安策略時，必須將零信任的概念內化，從多個角度考量和防範潛在風險。

不買新產品，也有機會做到零信任架構。

參考資料

〈面圖片〉

〈人｜零信任原則〉

〈on Weakens TLS Security〉

時，我稍微收集並參考了一些有關零信任架構的資料，並附上了我自己的見解，歡迎大家

JIST SP 800-207：最多人講到零信任架構時會提到它，我想應該也是最早出現在大眾良前的白皮書。如果你想深入了解完整的零信任架構理論，這會是很好的參考，但這份文件並沒有提供明確的實踐指南。

JIST SP 1800-35 (Draft)：由於零信任架構被提出來後，許多美國聯邦單位也被要求實下，因此 NIST NCCoE 找了廠商來做示範組，詳盡解釋了零信任架構的執行概念、策各、評估、實作功能。最貼心的是，這份文件還針對不同層級的管理人員分成四份文卡，讓每一個層級的管理者都能夠有所依據。這份文件目前還在草稿階段，並持續更新中。

美國聯邦政府 ZTA 指南：這份文件主要是讓聯邦政府人員有概念怎麼採購與實施零信任架構，非常簡短但有效，還很貼心地在結尾提供了 memo 資訊的整理，讓美國的聯邦政守人員能大概了解跟零信任架構有關的政府命令。

英國 NCSC ZTA 指南：與美國聯邦政府的 ZTA 指南類似，但英國的 ZTA 指南更加淺顯易懂，並涵蓋比較多的常見問題 Q&A。

- CIS Controls v8 mapping ZTA：為了讓企業有明確的提升與改善目標，CIS 把自己列的安全控制項 (Controls) 對應到零信任架構的概念中，雖然無法全部涵蓋，但對企業而言總是個起頭。

企業 # 管理 # 資安 # 零信任網絡 # security

在這裡尋找共鳴，與方格子的 46 萬格友分享觀點與生活。

| 2023年 | 挑戰一整年不買新衣服 |

台灣太太在北京

特權存取管理 (PAM) 解決方案之優點與不足

駭客花生醬

19 追蹤者　6 內容數

贊助

駭客花生醬

分享對於資訊安全的分析和評（吐）論（嘈），趨勢觀察、技術分析、觀點評論、科普教育，除了特別專業的網路...

＋ 追蹤

0

查看全部

發表第一個留言支持創作者！

可能也想看

商品販售功能隆重登場！全新變現管道降臨

s 正式推出數位商品販售功能囉！ 恭喜各位創作者，除了原有的訂閱、廣贊助外，又多了全新的變現方式可供選擇。內容創作不止於文字形式，內...

方格子 vocus 發佈於 方格誌　♡ 68

2023-10-25

公告　# 數位商品　# 新功能

該不該買新上市的ETF？

常常有人問我，某某新上市的ETF可不可以買？因為我從來沒有代言過，我真的很難回答，所以只能請他自己要好好研究，不要因為有知名的投資達人推薦，...

施昇輝 發佈於 小資幸福講堂　♡ 60

2022-12-09

生活哲學 # 閱讀筆記 # 書籍分享

DIY動手換掉行李箱輪子，不用買新的，也不製造垃圾！

現在很多東西修都比買新的還貴，有時候心裡都覺得對不起地球，於是就試著自己改裝了。

換日線 發佈於 線線的生活日常 ♡ 5

)-06-10

垃圾減量 # 動手作 # DIY

後悔新聞】那些不買可惜的分紅保單

升學制度的重視，進入職場的時間被延後，退休年齡也隨之提高，對沒有存款的人來說是有「經濟」的心理負擔，而多數人在面對生活的劇烈變化...

小新臟 實習心理師 ♡ 4

)-05-14

儲蓄 # 分紅 # 富邦

百五新聞週報】烏俄戰事延燒，全球經濟動盪！全球通膨，美國不起房改買「迷你屋」？

二百五新聞週報，婊姐將透過七則感興趣的新聞事件分享個人觀點，只攻事要塞？烏克蘭城市馬立波婦幼醫院遭俄軍砲擊！不要免費做自己在行的...

聲歷其境 All Around You ♡ 0

)-03-29

買中古屋要如何殺價？　TODY陶迪：2步驟+良好心態

財經專家TODY分享買中古屋的議價技巧。影片來源：TODY陶迪YouTube台灣現階段的預售屋價格下不來，消費者又有承擔一定風險，不少民眾...

E. Grey ♡ 2

2023-03-17

中古屋 # 實價登錄 # 房子

個人觀點 | 喜歡借書買書卻不看書，這是什麼心態？

前幾天，我走進住家附近的圖書館。原本只是打算借用飲水機，裝瓶水就離開，但我還是逗留了一陣子。我隨手抓了一些書，每一本看沒幾眼就放回書架...

Z先生 ♡ 0

2021-09-12

福箱 # 福袋 # 買起來