



零信任架構下，如何實現組織內使用者安全登入

Passkey與特權帳號管理系統整合

技術經理 沈泓智

Agenda

- uniXecure介紹
- 密碼的問題與常見建議
- 我們如何處理
- Q&A

公司簡介

智慧資安科技致力成為亞洲資通安全服務暨代理
領導廠商。

有鑒於全球企業急速數位轉型的需求，新科技演進
延伸更多未知潛藏的資安疑慮，智慧資安科技率先
針對國內外資安規範，提供「**事前預防、事中偵測、
事後應處**」一站式資安服務，整合人員、技術與程
序，解決資安合規性與資安人才缺乏的窘境，並提
出 **MSSP 託管式資安服務**，推出**零信任、
DevSecOps、OT 資安及雲端合規四大解決方案**，
與企業攜手因應日益嚴峻的資安挑戰，協助企業無
後顧之憂發展組織核心業務。



自有產品-強化資安效度、維度 提升防禦深度

零信任架構

- 身分鑑別
- 設備鑑別
- 信任推斷

DevSecOps

- 自動化測試
- 持續集成/持續部署
- 安全敏捷開發
- 容器化和微服務架構

OT 資安

- 資安檢測與服務
- 資產盤點與漏洞管理
- 端點防護與監控
- OT 法規遵循

雲資安合規

- 數據加密與保全
- 日誌管理與監控
- 可視化分析
- 異地備份/備援

MOC
監控維運中心

跨境跨域 MSSP

SRMAS
資源監控

GCB
組態設定

EDR
端點偵測

LUCAS
記錄管理

SIVAS
弱點通報

SSC
端點監管

打造全面可靠、高效的全域式資安聯防



效益化企業成本



智能監控維運



顧問級服務團隊



全方位資安防護

代理產品 ZTA 解決方案



密碼的問題與常見 建議



定義與現實

密碼為資訊系統用戶識別與驗證身分的重要機制，其設計應具備**唯一性**、**機密性**與**足夠強度**，並搭配密碼政策進行管理，以降低未經授權存取之風險。

一串夠亂夠長的字串，例如

WtswVOmygYJ2hj(\$yCAX7bV*S1DZ6b

除了極少數**天賦異稟**者外，多數的人都沒有辦法處理這樣的要求.....

不管是**產生**還是**記憶**



幾個問題

使用者會擁有N個帳號或一個帳號用於N個系統

這代表攻擊方的靶子變大了或更有價值

如何處理人性？

你相信你的使用者能夠按照『違反人性』的規範妥善管理密碼？

分散或集中？密碼該如何保存

現代的系統多數採集中式保存管理，但這也代表雞蛋放在同一個籃子



一把鎖不夠，那就再加一把

MFA (Multi-Factor Authentication) 是一種強化使用者身份驗證安全性的機制，要求使用者在登入或存取系統時，提供兩種或以上的不同類型驗證因子，以降低帳號被盜用的風險。

可以增加安全，但更加**違反人性**

只適用於給『人類』使用的系統，對於**背景系統沒有保護能力**



一個簡單的歸納

現代多數的方案嘗試在安全性及人性中選擇一種作為處理目標，但常落入局部最佳解的迷思

透過各種設定限制使用者對於密碼變更的要求，當要求違反人性時，注定會出現問題

MFA強化了認證，但沒有處理密碼先天問題，反而產生更多運作成本



傳說中的銀子彈 (Silver Bullet)

Passkey/FIDO2

由 FIDO (Fast Identity Online) 聯盟推動的無密碼身份驗證方式，以公開金鑰加密為基礎，讓用戶透過生物辨識 (指紋、臉部) 或 PIN 驗證，不使用傳統密碼、去中心化保存。

多數系統並不支援，有支援的系統採並行制度運作 (密碼還是存在)

我們如何處理



將目標拆解

如何讓認證機制簡單化，同時又能符合安全規範

使用Passkey，作為使用者認證方式

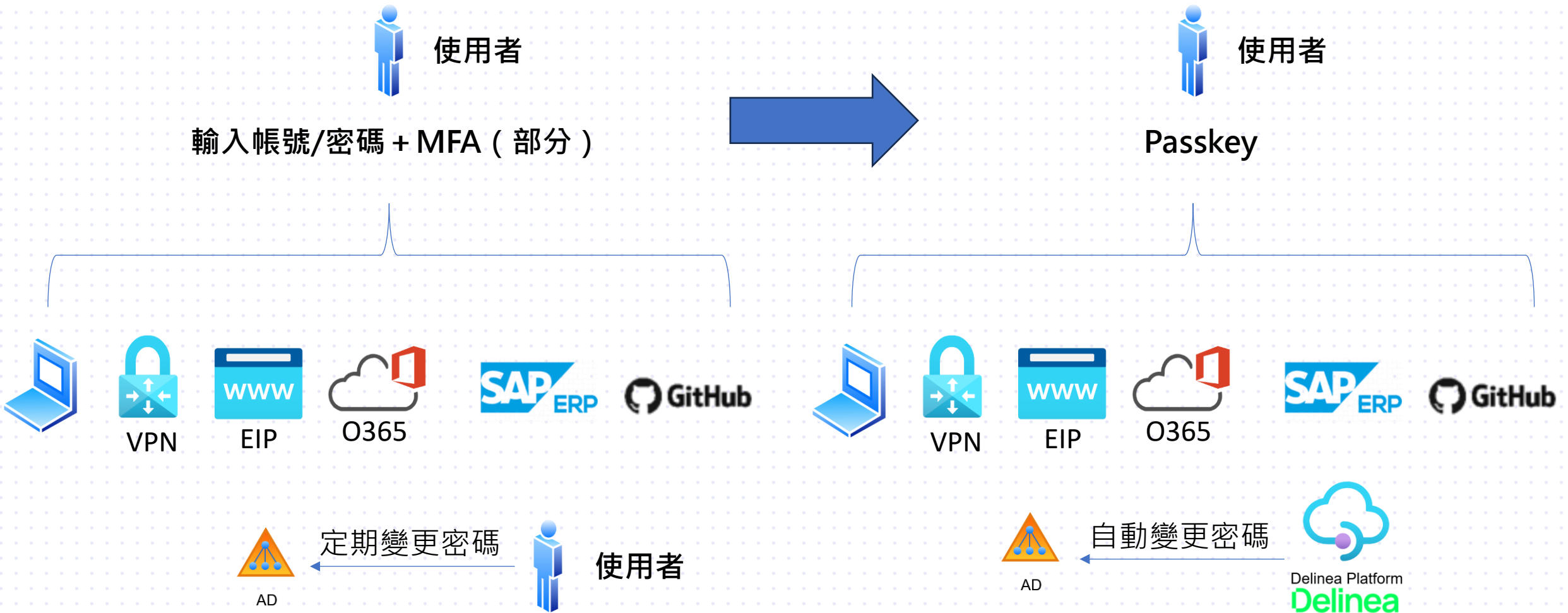
如何有效管理密碼

管理密碼交給特權帳號管理系統處理

如何讓上述模式可以盡可能適用於日常作業

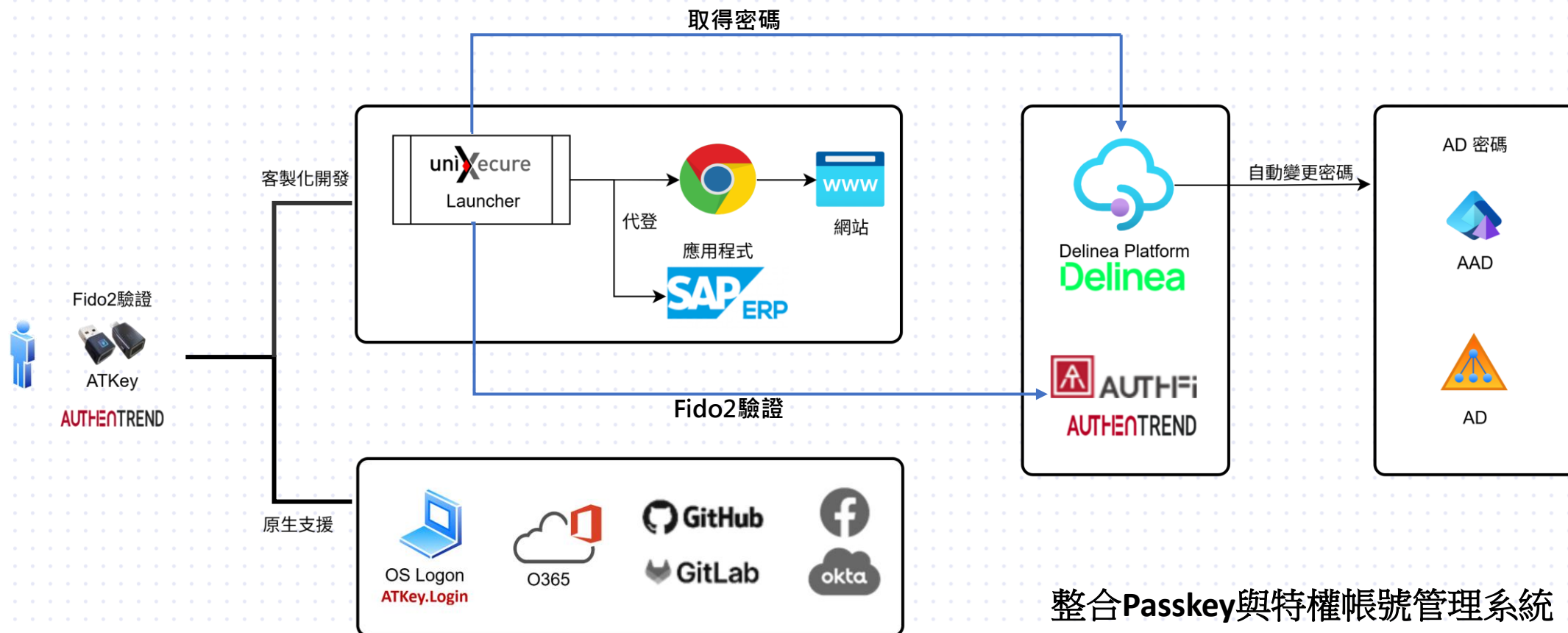
整合Passkey與特權帳號管理系統

一個簡單情境





Architecture





效益

- 讓使用者免除密碼管理負擔，透過Passkey達成單一驗證
- 傳統密碼管理交由Delinea Platform處理，實現高強度、密集密碼變更目標

在既有系統未能支援Passkey的過渡期間，藉由Authentrend、Delinea及uniXecure的組合，提供一個低維護成本的解決方案



常見問題

和MFA、Passkey方案有什麼不同？

- MFA目標在於強化驗證，並不處理密碼變更
- Passkey有支援度問題，實務使用上還是會遭遇到需要使用密碼情境

那為何不直接用PAM去管理使用者密碼就好？

- 當沒有其他機制輔助下，使用者無法知道目前密碼，進而無法使用
- 使用者操作複雜度會大幅提高

有無系統支援限制？

- 目前階段僅支援Windows系統應用，MAC及Mobile裝置會在下一階段支援
- 若遇到不支援情境，提供一次性密碼供使用者手動使用

Passkey 與特權帳號管理系統整合 -
零信任架構下，如何實現組織內使用

填寫問卷送好禮





uniXecure

Thank You

