

GO PASSWORDLESS WITH ZERO TRUST

GoTrust 建構零信任的 第一道防線

保護全球 360 萬用戶的身分安全領導者

IT 的真實噩夢：破碎的防線



30%

IT 時間耗費在處理密碼重設工單

81%

資料外洩源於弱密碼或憑證遭竊

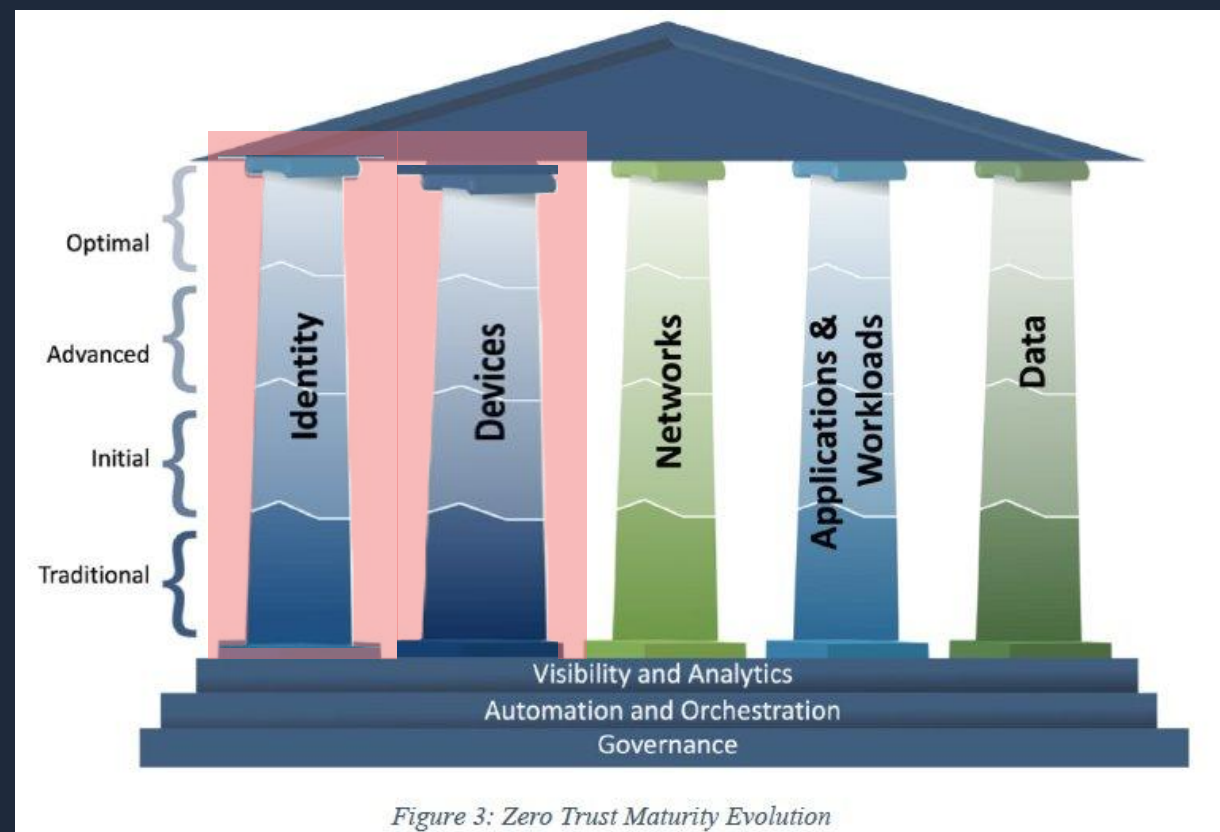
釣魚郵件 (Phishing) 防不勝防，傳統邊界已然失效。

回歸根本：CISA ZTMM 2.0 模型

根據美國 CISA 零信任成熟度模型，所有安全策略的起點在於：

- ✓ **身份 (Identity)**：確認「你是誰？」
- ✓ **裝置 (Devices)**：確認「你的設備安全嗎？」

核心論點：若無法確保用戶與設備的合法性，任何防火牆與 VPN 部署都將功虧一簣。



全方位零信任防護平台



GoTrust ID

軟體解決方案

手機即憑證
無縫登入 Windows/Mac



Idem Key

硬體解決方案

FIPS 140-2 Level 3
軍規級實體防護

從一般員工到特權管理者，提供一致性的免密碼安全體驗。

資安第一道防線 - 免密碼認證



GO PASSWORDLESS WITH ZERO TRUST

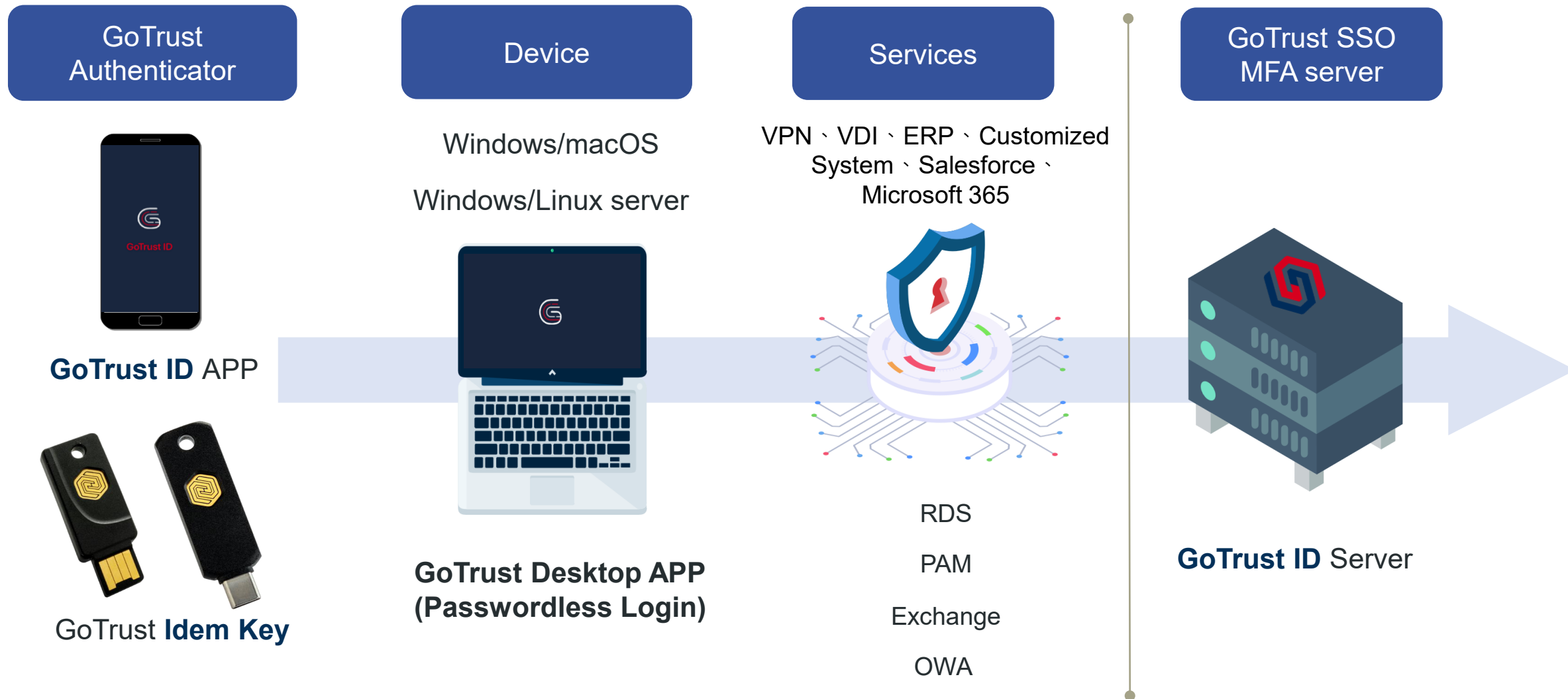
我們專注於免密碼身分認證、零信任資安防護
從辦公室到遠端工作，一致性的免密碼安全體驗

打造端點零信任端點防護

阻擋橫向滲透

一個平台，實現全方位零信任防護

Authentication for Desktop Login and Services



SOFTWARE: GoTrust ID

專利「離線免密碼登入」技術

- ✔ **斷網也能用**：獨家專利技術，員工出差或網路不穩時，依然能透過手機藍牙解鎖電腦。
- ✔ **無密碼體驗**：支援 FaceID / TouchID 生物辨識，手機就是身分證。
- ✔ **廣泛支援**：完美整合 Windows 10/11, macOS, AD Domain。

解決 IT 最擔心的：「沒有網路怎麼驗證？」



HARDWARE: Idem Key

堅若磐石的物理防禦

- ✓ **全球首創**：同時具備 IP68 防水防塵 與 FIDO2 Level 2 認證。
- ✓ **FIPS 140-2 Level 3**：內建軍規安全晶片，私鑰永不出金鑰。
- ✓ **多合一功能**：整合 FIDO2, U2F, OTP, PIV，一支抵多支。



「Build to Endure, Crafted to Resist」

GoTrust ID



兩大產品線



- Authentication for Desktop Login and Services
- 零信任免密碼身份認證解決方案 (軟體)
- 兩項美國及台灣發明專利
- 通過台灣資安院認證, 美國FIDO Alliance 認證, 微軟認證
- 包含Server, Windows, Mac, iPhone and Android 五套軟體組成

Idem Key



- FIDO2 L2 & IP68 防水認證 (全球首款), 微軟認證, 台灣資安院認證, 符合台灣銀行公會載具規範
- 可隨插即用於Apple ID, AWS, Google Workplace, Microsoft Windows, Azure AD, Office 365, Salesforce, Okta, DUO 等數百種大型雲端應用.
- 美國及台灣發明專利
- 台灣, 奧地利, 捷克, 市占第一, 美國加州市占第二



GO PASSWORDLESS WITH ZERO TRUST

涵蓋數位生態系的全面防護



免密碼電腦登入

- Windows 10/11
- MacOS



- Windows Server
- Linux Server



- PAM
- 地端應用
- 雲端應用
- 郵件

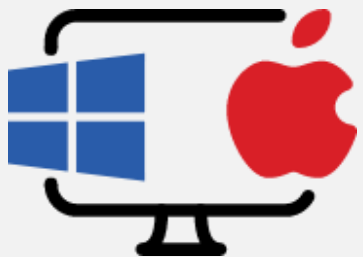


- VPN
- VDI
- SASE
- WiFi



- 支援各式認證協議
- SDK

端點



免密碼電腦登入
Windows 10/11
MacOS

- Domain & Local 使用者
- 單一使用者模式
- 共用電腦多人使用模式
- IT 登入口多因子驗證

伺服器



Windows Server
Linux Server

- RDP and RDS
- Internet Information Services (IIS) based application
- Admin 於 SSO portal 中註冊，即可登入授權之伺服器
- Linux Ubuntu, Debian, Fedora, RHEL, CentOS

應用



PAM
地端應用
雲端應用
郵件

- CyberArk
- Onedidentity
- Delinea
- Outlook Web Access (OWA)
- M365
- Google Workspace

網路



VPN
VDI
SASE
WiFi

- Check Point
- FortiGate
- Palo Alto
- Pulse Secure
- F5
- Array Networks AG
- VMware (VDI)
- Palo Alto SASE
- EnGenius

第三方應用接口



支援各式認證協議
SDK

- Open ID Connect (OIDC)
- Radius
- SAML2
- IIS Adapter
- LDAP Proxy
- SDK

GoTrust ID

超越傳統的零信任身分與存取控管平台
六大核心優勢解析

為什麼選擇 GoTrust ID ?

從高延展性架構到全方位的稽核控管，打破傳統單一平台密碼登入的限制，真正實現企業級零信任安全。

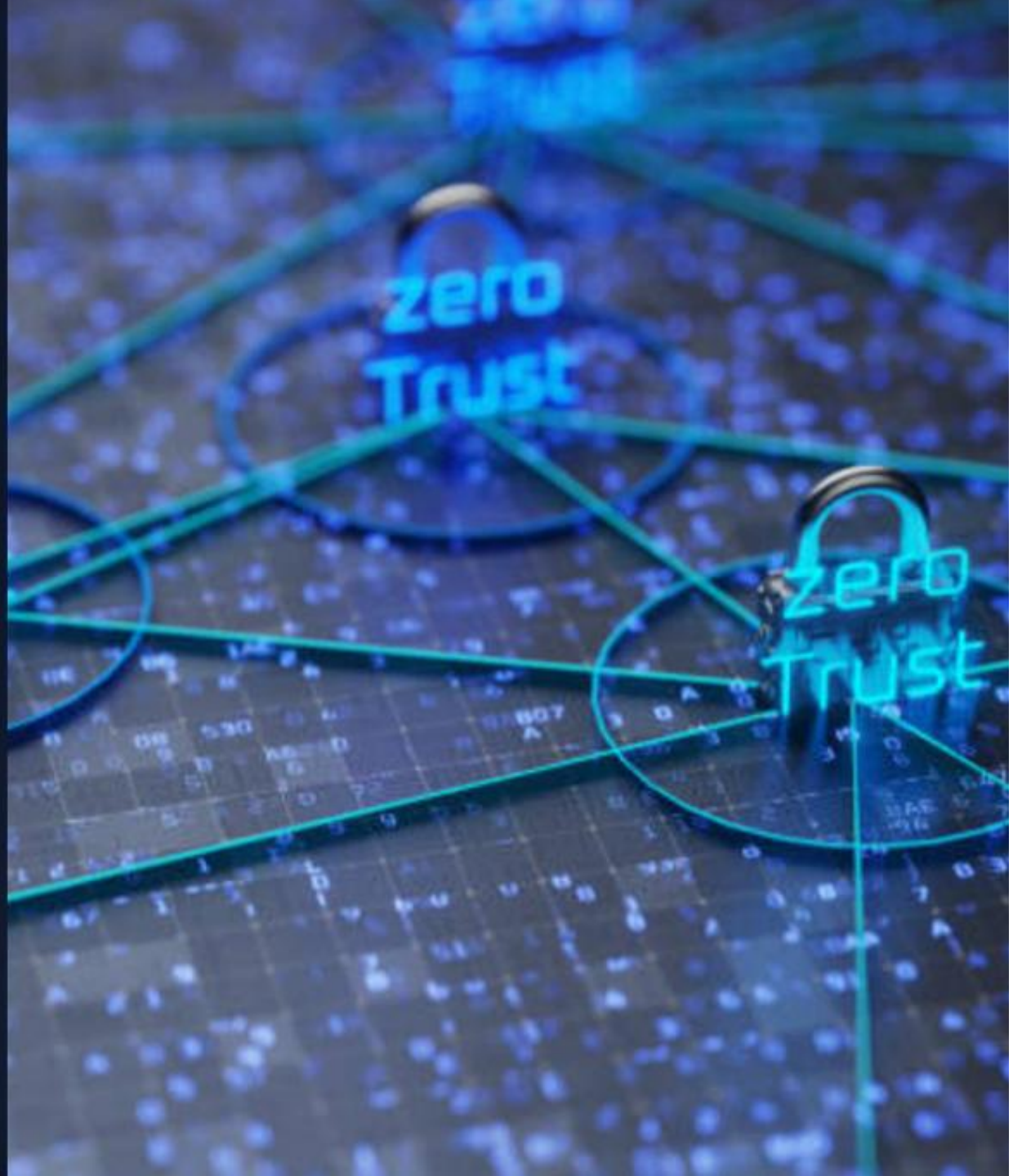
1. 高延展性架構

不受限於單一電腦登入

GoTrust 零信任身分與存取控管平台，不僅適用於個人電腦與作業系統登入，更能無縫介接企業內部多種關鍵系統。

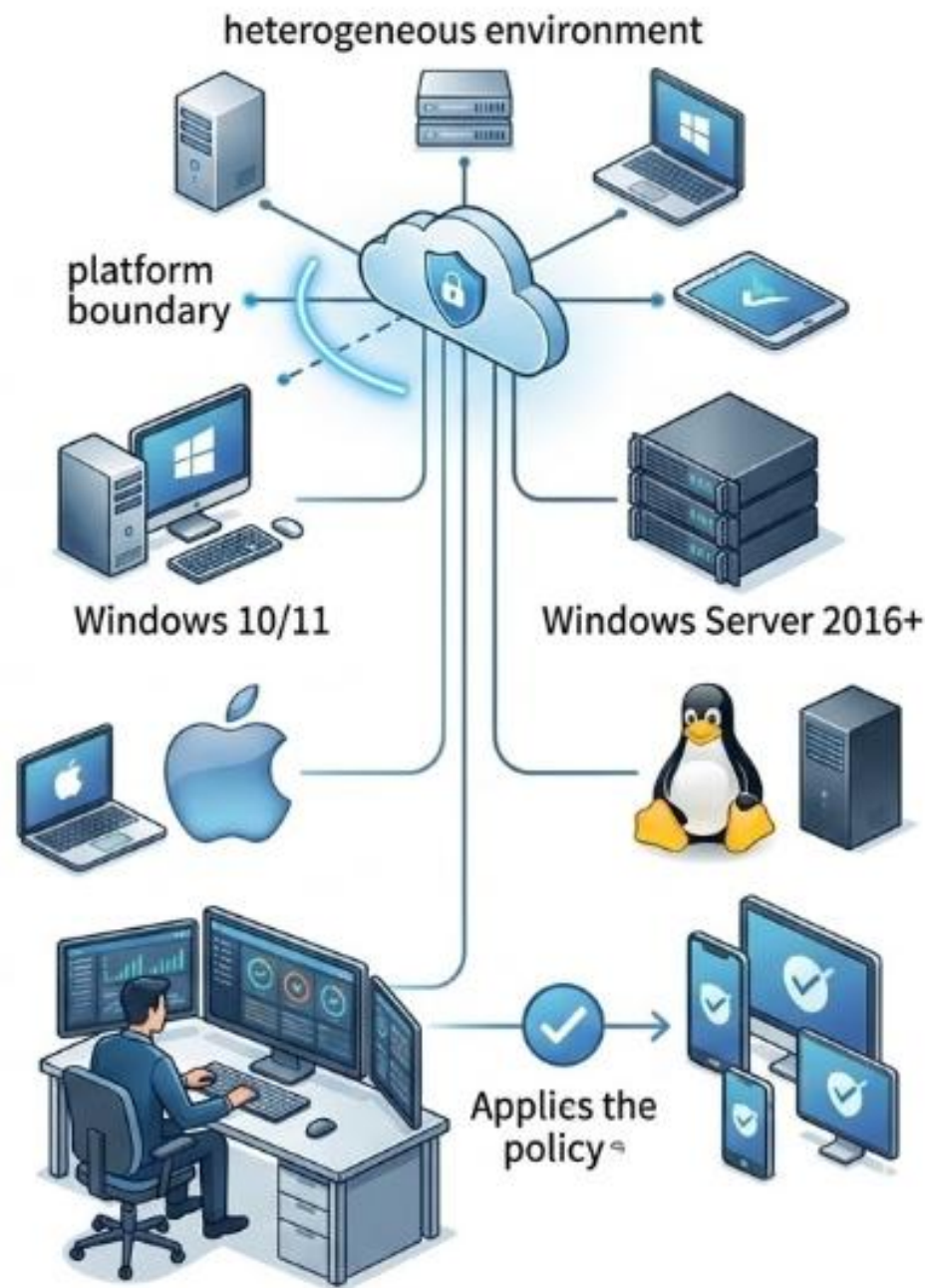
完美支援伺服器、VPN、CyberArk 及各式自開發業務系統。未來若企業導入新系統，只要具備 AD, RADIUS, OIDC, SAML, IIS, LDAP 等標準介接能力，皆可迅速納入集中管控架構。

優勢：統一身分驗證與存取控管，徹底擺脫傳統密碼登入機制的限制與外洩風險。



2. 跨作業系統的登入支援

- ✔ **打破平台限制**：完美解決 Windows Hello 僅能用於單一微軟平台的侷限，讓企業在異質環境中統一管理終端設備。
- ✔ **全面涵蓋主流系統**：完美支援 Windows 10/11 以及 Windows Server 2016 以上版本。
- ✔ **無縫接軌多樣生態**：完整支援 macOS 以及 Linux 等開源作業系統。
- ✔ **統一管理體驗**：無論員工使用何種裝置，IT 部門皆能實施一致且強大的安全登入策略，大幅降低維運成本。



3. 完整的登入控管與稽核能力

集中管理與即時阻斷

企業管理者擁有系統最高權限，可集中管理全域安全策略。若發現異常情況，管理者能隨時強制撤銷特定使用者的登入驗證器。

系統亦支援即時暫停或永久停用特定帳號的登入權限，為企業提供比單純本機登入機制更強大、更即時的安全防護網。

全面行為稽核與調查

系統會詳細且不可篡改地記錄所有使用者的登入與登出日誌。全面支援企業內部的資安稽核、異常行為調查及資安事故應變處置。

讓每一次的系統存取皆有跡可循，輕鬆滿足金融、醫療、政府等高機密產業最嚴格的合規與內部稽核要求。

4. 支援 Windows RDP



將多因子驗證 (MFA) 延伸至遠端桌面

遠端桌面協定 (RDP) 一直是企業內網遭駭客入侵的常見破口。GoTrust ID 創新地將高強度的無密碼 MFA 完美延伸至遠端桌面情境。

核心目的：大幅降低帳號密碼遭到外洩，或是遭受暴力破解時，攻擊者透過 RDP 入侵企業核心內網的嚴重風險，為遠端辦公提供堅實防禦盾牌。

5. 多元驗證器選擇

行動裝置 App 驗證

透過員工自身手機內建的生物辨識機制即可完成 MFA 驗證。無須額外攜帶實體硬體設備，最適用於筆電使用者、遠距辦公及業務人員等高機動性情境。



GoTrust Idem Key 金鑰




具備 FIDO 國際認證的 USB 安全硬體金鑰，提供最高標準的防護等級。特別適用於共用電腦、機房主機、受管控終端及高度機密且不允許使用智慧型手機的特殊環境。



6. 專為「共用電腦」優化

完美支援多使用者場景

針對櫃檯、產線、倉儲、客服中心等多位使用者輪班共用同一台設備的特殊企業情境，提供無縫且安全的登入體驗。

-  **極速切換：**人員可使用各自專屬的驗證器在同一台電腦極速完成登入與登出。
-  **明確權責：**稽核日誌會精準區分「人、機、時」，徹底避免帳號共用致使資安責任不清。
-  **簡化管理：**無需逐一註冊多組生物特徵，完美解決 Windows Hello 在多人共用情境下的管理痛點。



GoTrust Idem Key

如何抵禦中間人攻擊

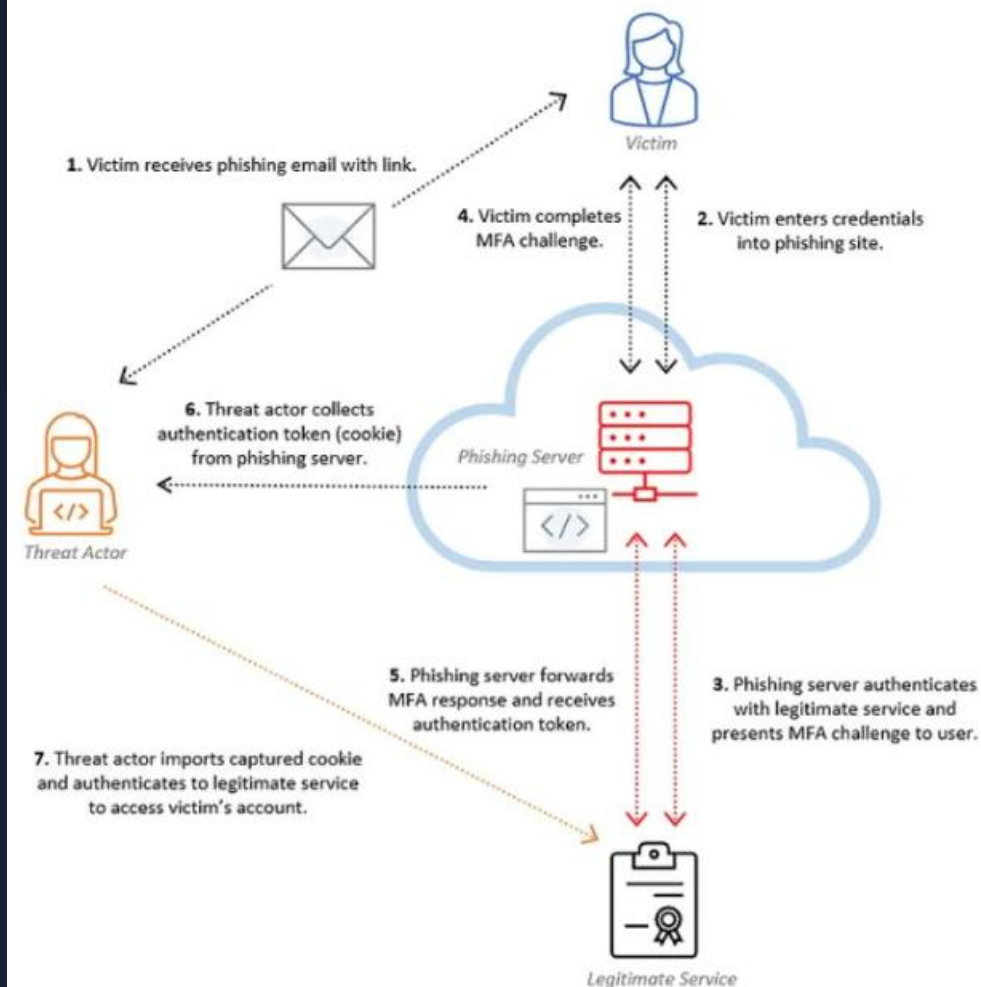
(Adversary-in-the-Middle, AitM)

Evilginx：隱形的中間人 (AitM)





不僅是釣魚，是「代理」

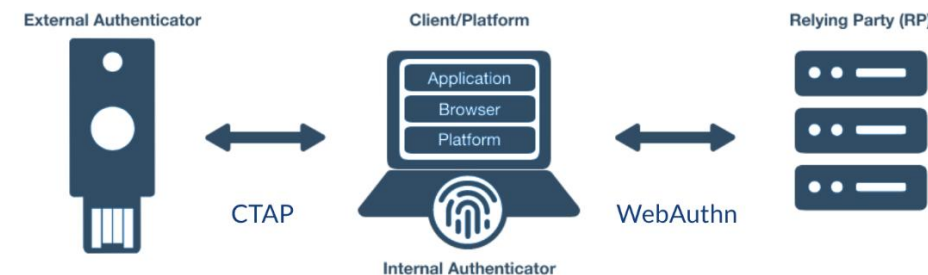
Evilginx 扮演反向代理，它不複製頁面，而是直接傳輸真實服務器的流量。

- 即時攔截帳號與密碼
- 同步轉發二階段驗證 (2FA)
- 最終目標：盜取 Session Cookies (憑證)



技術細節: 為什麼Evilginx無法成功?

- 
網域捕捉: 瀏覽器自動抓取當前網址 (Evilginx 偽造網域)。
- 
挑戰傳遞: 將網域作為 FIDO2 Challenge 資訊傳給 Idem Key。
- 
硬體核對: 金鑰內核偵測到「請求網域」與「原始註冊網域」不匹配。
- 
拒絕簽署: Idem Key 網域綁定與硬體層級簽名，釣魚網域無法獲得有效回應。



1. 網域強制驗證 (Origin Check)

當使用 Idem Key 進行驗證時，瀏覽器會自動抓取當前網站的網域（如釣魚網站）並傳送給硬體金鑰。

關鍵點：Idem Key 內存儲的私鑰是與「真正的網域」（如 microsoft.com）綁定的。

防禦機制：當金鑰發現瀏覽器傳來的網域與當初註冊的網域不符時，金鑰會**拒絕簽署**驗證請求。Evilginx 拿不到任何有效的簽章，攻擊宣告失敗。

2. 加密綁定與私鑰不出金鑰

不可複製性：Evilginx 只能代理流量，但它無法從 Idem Key 中提取私鑰。

抗中間攻擊：FIDO2 協議包含一個由金鑰簽名的「挑戰值 (Challenge)」，這個簽名是針對**特定網域**生成的。即使 Evilginx 攔截了這個簽名，也無法將其用於真正的 microsoft.com 登入，因為網域資訊不匹配。

終結釣魚攻擊的利器

專為企業設計的防線

基於 FIDO2 / WebAuthn 標準，Idem Key 將身分驗證從「知識」轉向「硬體持有」。

- 支援 USB-A, USB-C, NFC
- 相容 Windows, macOS, iOS, Android
- 軍規級非對稱加密技術



戰略結論

Evilginx 欺騙的是人的視覺，而 Idem Key 依賴的是不可偽造的硬體數學。這是將防禦從「事後補救」轉向「本質安全」的關鍵投資。



GO PASSWORDLESS WITH ZERO TRUST

GoTrust Idem Key

長得就像 USB！小小「硬體密鑰」為何能完全阻擋網路、軟體漏洞？

- 硬體密鑰是一種**物理硬體**，用於儲存密鑰和進行加密操作。
- **FIPS140-2 Level 3**安全晶片+加密演算法以提供更高的安全性。
- 使用硬體密鑰時，用戶需要將其插入電腦，然後輸入一個**PIN**來解鎖它，才能進行操作。言下之意，攻擊者需要直接接觸該裝置才能進行攻擊，這代表硬體密鑰**完全阻擋**針對網路、軟體漏洞的遠程駭客攻擊。



GoTrust Idem Key

Build to Endure, Crafted to Resist
堅若磐石, 匠心獨運

- ❑ 支援 FIDO + PKI + PIV + OTP 多應用
- ❑ 全球首款, IP68 防水防塵 & FIDO2 L2 的安全金鑰 (USB Security Key)
- ❑ FIPS 140-2 Level 3 認證 Secure Element
- ❑ 符合台灣資安院零信任身份鑑別器
- ❑ 微軟認證, 可隨插即用微軟生態鏈 (免密碼登入Windows , Microsoft Entra ID and Microsoft 365)
- ❑ 符合台灣銀行公會憑證載具規範, 台灣唯一可用於行動企業網銀的合規載具



140-2 Level 3 certified
Secure Element



Idem Key 優異的全球銷售

- 市佔：
 - 市佔第一：捷克、奧地利、台灣
 - 市佔第二：美國中小學USB Key
- 全球代理商：美國、加拿大、捷克、奧地利、德國、加保利亞、日本、台灣
- 特殊事蹟：第一支捷克MojelD及奧地利ID認證的USB Key



名列奥地利 ID 认证名单第一位

Welche FIDO-Sicherheitsschlüssel sind mit ID Austria kompatibel und wo sind sie erhältlich?

Token, die FIDO2 Level 2 zertifiziert mit [WebAuthn](#) unterstützen, können mit ID Austria verwendet werden. Dies erfüllen derzeit:

- GoTrust Idem Key FIDO2
- Trustkey G310H
- Yubico Security Key NFC in **schwarz** (USB-A + NFC, USB-C + NFC)
- Yubico YubiKey FIPS Series (5 NFC FIPS, 5C NFC FIPS, 5C FIPS, 5 Nano FIPS, 5C Nano FIPS, 5Ci FIPS)

Gängige Modelle bieten meist Verbindung via USB oder NFC zu Ihrem Computer an. Sie können im Handel erworben werden und können je nach Ausführung zwischen 30 Euro und 70 Euro kosten.

Wir empfehlen die Nutzung am Betriebssystem Windows und die Verwendung von gängigen Browsern wie Chrome oder Firefox, um einen reibungslosen Ablauf sicherzustellen. Eine Übersicht über die Unterstützung von FIDO2 auf Betriebssystemen und Browsern finden Sie auf <https://fidoalliance.org/expanded-support-for-fido-authentication-in-ios-and-macos/>.

Welche Funktionen erfüllen die Apps „Digitales Amt“ und „Handy-Signatur“ mit der ID Austria mit Vollfunktion?

Wie funktioniert die Umstellung von Bürgerkarten auf ID Austria?

Nach der Umstellung meiner Bürgerkarte habe ich eine ID Austria mit Basisfunktion erhalten. Wie kann ich diese auf eine Vollfunktion aufwerten?

- GoTrust Idem Key FIDO2

領先市場的獎項及認證

- ❑ 市場先驅，提供適用於電腦與雲端登入的無密碼多因素驗證（MFA）
- ❑ 全球首款通過 FIDO2 Level 2 認證的 USB/NFC 安全金鑰，適用於所有 PC 和行動裝置
- ❑ 唯一通過 FIDO2 認證的 BLE 智慧識別證
- ❑ 微軟 Azure 認證的無密碼身份驗證產品
- ❑ 擁有 17 項國際專利，其中包含 8 項美國專利
- ❑ 榮獲全球最具權威的數位安全大獎——法國巴黎 Sesames Award



TOP 10 Multifactor Authentication
Solution Provider for 2019



Winner of the Digital Security
Award Sesames Award, in Paris



FIDO2 Level 2 Certification



Level 3





GoTrust

GO PASSWORDLESS WITH ZERO TRUST

部署需求

部署需求



GoTrust ID Server

Respective VM System Resource Requirements

- CPU Core: 2 cores and above
- Memory: 8GB RAM and above
- Image Disk Size: 50 GB and above



GoTrust ID Mobile Application

iOS :

- iOS 10 and above

Android :

- Android 6 and above



GoTrust ID Windows/Mac Application

Windows :

- Windows 10/11
- Windows server 2016 and above

Mac :

- macOS 11.4 and above



GoTrust Idem Key (optional)

- Windows 10 version 1903 and above
- macOS 10.13 and above
- Linux (UDEV 188 and above)
- Chrome OS 76 and above
- Android 7 and above
- iOS 13.3 and above

Thank
You



GO PASSWORDLESS WITH ZERO TRUST