HYPR 解決方案介紹

防網路釣魚的 MFA，能夠讓員工及客戶更快、更輕鬆及更安全的登入帳戶。

日辰資訊

保護存取也降低成本

現代企業都需要消除身份驗證所帶來的威脅，同時也要提供最佳的用戶體驗，不論任何平台或地點。HYPR 是公認的 Passwordless (無密碼)、防網路釣魚、多因素身份驗證領域的領導者，已經在很多大規模且最複雜的環境中，全面部署驗證過。

傳統 MFA 失效

絕大多數的資安事件，如果追溯到源頭都會是身份驗證的弱點所造成。傳統的多因素認證(MFA) 已經被證明無法保護企業，很容易受到推送轟炸、中間人竊取、網路釣魚、網路詐騙、密碼填充和其他憑證攻擊。此外，傳統的身分驗證技術迫使企業需要在安全性和可用性之間做出選擇，選擇更安全的選項可能會帶來成本及管理工作增加，將對用戶滿意度和工作效率產生負面影響。除非企業做出改變，否則就很容易受到攻擊。Passwordless(無密碼) MFA 是打破這種循環的唯一途徑。

HYPR — 改變這個世界的登入方式

HYPR 提供最強大的身份驗證，並簡化用戶體驗，提供解決方案可以加快業務大幅的增長。HYPR 的容易使用、防網路釣魚 MFA ，已經通過 FIDO 認證，這是美國網路安全暨基礎設施安全局 (CISA) 視為零信任身份驗證的黃金標準。透過部署 HYPR，企業可以將身份驗證與身份提供商脫鉤，以確保採用最佳的技術和一致的登入體驗。

HYPR 身分驗證的運作方式

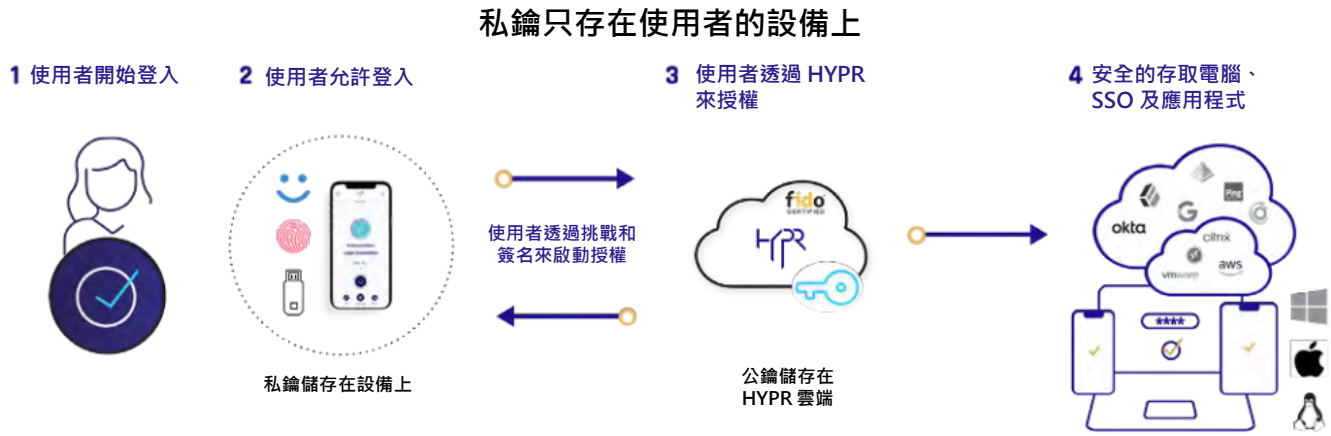
HYPR 的身分驗證，是以 FIDO 金鑰為標準的強大公鑰加密方式，來取代密碼、PIN 碼、 簡訊驗證碼和一次性密碼(OTP)等共享機密方式。生物識別感測器如 Apple Touch ID、Face ID、 以及安卓和 Windows 系統中同類的產品，在經過身份驗證伺服器使用公鑰加密技術進行驗證過後，即可用來解鎖憑證。

HYPR 主要優點

- 解決電腦上 MFA 的不足。
- 透過更安全、最新的 FIDO 密鑰標準為基礎的認證方式，防止憑證網絡釣魚，欺詐和賬戶接管。
- 提高工作效率，將密碼重置的 IT 服務降低 95% 。
- 快速的整合現有系統、IdP 和應用程式。
- 透過使用功能齊備且經過企業驗證過的 Passwordless MFA，將帶來 324% 的 ROI [1]。

1 The Total Economic Impact™ Of HYPR True Passwordless MFA, Forrester Research, July 2023

在登錄時，HYPR 會安全的生成一對加密密鑰，私鑰存儲在用戶的手機設備內安全、隔離的信任執行環境 (TEE) 硬體層之中，公鑰存儲在 HYPR 伺服器上。 簡而言之，這就像把智能手機變成 FIDO2 認證 token。 HYPR 還可以與任何其他 FIDO 認證的身份驗證器（例如硬件密鑰和智能卡）配合使用，為無法使用或選擇不使用智能手機的用戶提供靈活性和選擇。



HYPR 解決方案的內容

HYPR 身分驗證應用程式 App

HYPR 提供了一款輕量級手機應用程式，以密鑰為基礎的身份驗證方式取代了密碼，比傳統 MFA 快了 300%。HYPR 應用程式可以在多個用戶設備上運行，提供隨時隨地的安全登入，而且可以離線登入。

HYPR 電腦用戶端程式

HYPR 電腦用戶端程式解決了一個嚴重但很常見，在身份驗證上的不足，消除了 Windows、MacOS 和 Linux 工作站（包含共享工作站和控制台）上的密碼和共享機密。遵守電腦上 MFA 的監管要求和安全框架指南， 用戶能夠從電腦到 SSO 和雲端應用程序有統一的登入體驗，包括虛擬桌面、VPN 和 RDP。

HYPR 控制中心

HYPR 控制中心能對數百萬用戶進行管理、配置和部署以密鑰為基礎的身份驗證規則。HYPR 讓您能夠大規模管理 FIDO 身份驗證硬體、輕鬆自行定義註冊方式和創建身份驗證規則，以及即時監控用戶和系統分析以及審核日誌。

HYPR SDK

利用 HYPR SDK 將無障礙、安全且符合法規的身份驗證嵌入到手機和網路應用程式中，為用戶提供最快速的登入體驗，並在任何設備上實現最大的安全性，以加快部署和上市時間來獲得商業競爭上的優勢。HYPR 的 SDK 支援同步密鑰和設備綁定密鑰。

提供員工和客戶用的 Passwordless 無密碼身份驗證，是以 FIDO 密鑰標準為基礎

HYPR 可以確保所有用戶群體都獲得最高級別的網路釣魚的安全防護，包括您的員工和客戶。現在的 CISO、CIO、COO、IAM、IS 和 IT 領導者都期望 HYPR 能夠降低他們的身份和訪問管理的總體擁有成本，讓他們的安全性、可用性和效率性目標趨於一致。 事實證明，HYPR 可以帶來 324% 的投資回報率。[2]

2 Forrester Research

HYPR 功能與益處

消滅了攻擊目標

有了 HYPR，就沒有會被駭客攻擊的集中密碼的數據庫。憑證以私鑰的形式存儲並一直保存在用戶設備最安全的區域。這種組合改變了駭客攻擊能獲得經濟上的好處，讓攻擊目標變得毫無吸引力，駭客都不會想去攻擊。

部署端到端的身份驗證黃金標準

HYPR 解決方案端到端都獲得了 FIDO2® 認證。FIDO 被 CISA、NYDFS、OMB 等管理機構視為是，防範網路釣魚密鑰為基礎的身份驗證的黃金標準。 許多其他的解決方案聲稱有“支援 FIDO”和“符合 FIDO 規範”，這僅表示有基本的互通性。 其他解決方案僅在單個組件（例如伺服器）有獲得 FIDO 認證。 HYPR 的所有組件均經過認證，以確保企業遵守最新的 FIDO 規範。

電腦到雲端都能安全登入

用戶首次登入設備時使用 HYPR 進行身份驗證，而且 HYPR 會引導他們完成所有登入步驟。 經過一次身份驗證之後，用戶即可獲得防網絡釣魚、使用密鑰的 MFA，就能存取其設備、資料、本地和雲端應用程式。 每個人每天平均登入次數為 26 次， HYPR 將登入簡化為單個步驟， 不再需要記住密碼，不再因為無法登入而不能工作，也無需打電話給 IT 服務台要求密碼重置。

完全的整合現有及未來的需求

消除 Windows、MacOS 和 Linux 平台上以及虛擬桌面 (VDI) 和虛擬專用網絡 (VPN) 上的密碼。 許多企業使用多種 SSO 和身份提供商，例如 Okta、Ping 和 Azure AD。 HYPR 能與所有主要提供商整合，將身份驗證流程分離，這樣就不會被供應商綁住，用戶也能有一致的身份驗證體驗。選擇部署最好的技術並對現有基礎設施加碼投資。

將傳統應用登入方式帶進無密碼時代

傳統的專屬應用程式在更新到目前的身份驗證標準時，通常會提出個身分驗證挑戰。 HYPR 與身份協調的供商合作，因此即使是最古早的應用程式和最客製化的安全堆疊，也可以無縫接軌使用 Passwordless (無密碼) MFA。

無所不在的 Passwordless，包括離線狀態

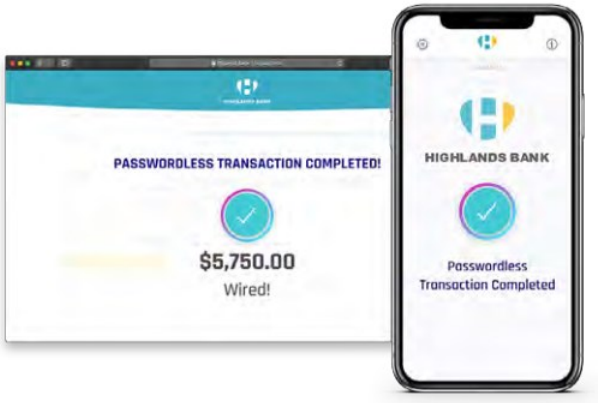
HYPR 離線模式可以確保即使在無法連線的情況下，也可以使用 Passwordless(無密碼) MFA。 離線模式利用安全的分散式 PIN 碼，讓外出的員工可以從任何地方安全登入。 PIN 碼存儲在設備安全元件中，並且只能使用一次。 管理員能管理此功能的啟用以及 PIN 碼定義、可用的 PIN 碼數量和有效期。每次用戶成功連線驗證後，都會生成新的 PIN 碼，並移除所有之前的 PIN 碼。

不再有一次性密碼(OTP)

用戶在其移動設備上安全地使用身份驗證； HYPR 的身份驗證過程中從不使用 OTP。 借助 HYPR，可以消除 MFA 攻擊和違規行為，包括推送攻擊（MFA 轟炸）、OTP 攔截、中間人竊取、重放攻擊、憑證填充和社交工程。 這也意味著無需浪費時間輸入密碼、token、OTP 或其他繁瑣的傳統 MFA 方法。

客戶身份驗證的安全

HYPR 的安全無密碼客戶身份驗證，為使用者提供一致的移動到網路的登入體驗，並通過無密碼交易批准加快交易速度。 HYPR 可擴展至每分鐘數百萬筆交易，並滿足 PSD2 SCA 要求，包括每筆交易的加密簽名和獨特的動態鏈接。 HYPR 可在高壓下運行，因此您可以應對使用率高峰和不斷增長的需求。



符合法規要求

HYPR 不使用可能違反數據安全規定的密碼、PIN 或共享機秘。 每個用戶的加密資料，包括身份驗證密鑰和生物識別訊息，都存儲在其設備上的可信賴平台模組 (TPM) 中。 HYPR 能幫助您符合防網絡釣魚 MFA 的官方業界指南，還滿足並超越紐約州金融服務委員會(NYDFS)、美國聯邦金融情報委員會 (FFIEC) 和其他監管機構制定的 MFA 要求。

Why HYPR

HYPR 結合了開放標準、最佳安全性和快速一致的用戶體驗，為您的員工和客戶提供經過驗證的、完全可擴展的身份驗證解決方案。 HYPR 可以保護您的用戶、服務和品牌聲譽，並具有靈活性和兼容性，可以滿足未來不斷變化的環境條件。

HYPR 在很多最複雜和要求最嚴苛的環境中進行過部署驗證過，包括美國四大銀行中的兩家、指標性的關鍵基礎設施公司和其他技術領先企業，這些出色的記錄在全世界確保了企業的安全。 經過獨立的驗證，HYPR 的解決方案投資回報率高達 324%。

THE PASSWORDLESS COMPANY

www.hypr.com

日 辰 資 訊

您的最佳 IT + OT 服務夥伴

www.ausenior.com.tw

service@ausenior.com.tw

02-26597886