威雲科技
WeiCloudTech

onelogin
by ONE IDENTITY

解碼雲端
SaaS 服務的管理之道

威雲科技資安顧問 張元朋

Agenda

- 多雲時代的來臨
- 零信任框架的推行
- 零信任概念的導入
- 登入流程展示

多雲時代的來臨

onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

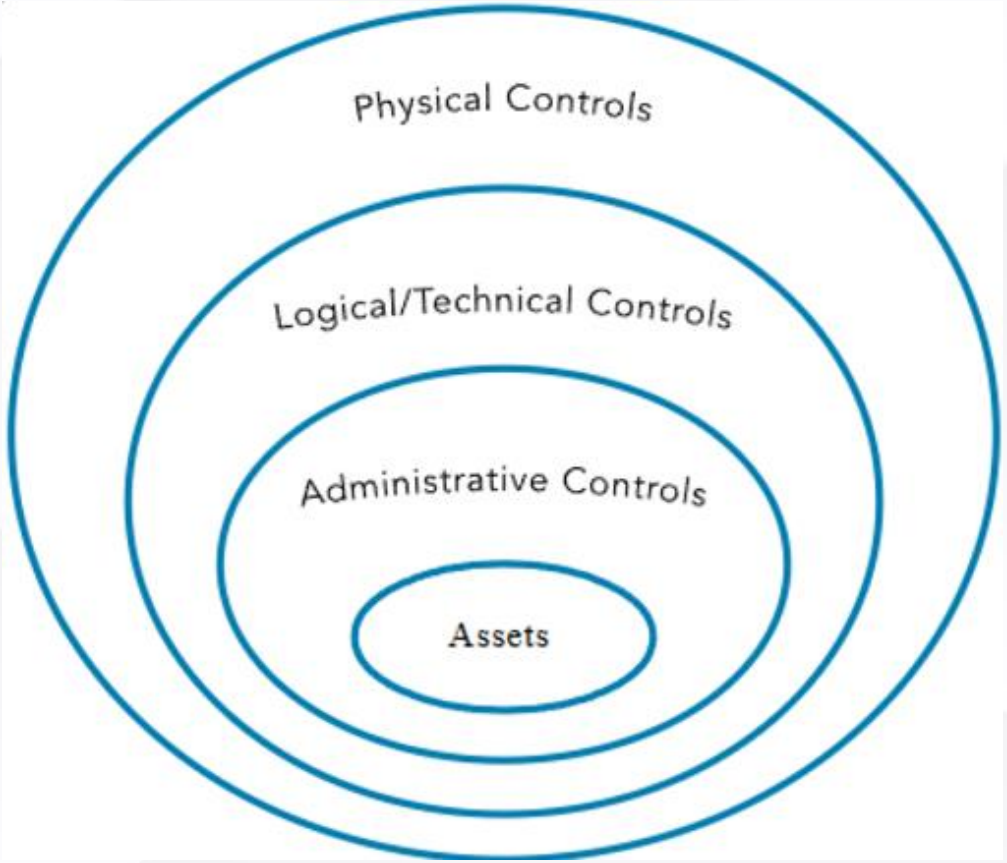
多雲時代衍生的問題

- 邊界模糊
- 密碼重設成本高昂
- 多雲數位身分管理不易
- 難以鑑別登入者是否為本人

邊界模糊 – 傳統的防禦邊界

- 縱深防禦為一種資訊安全策略，已在組織中多個層次建立可變的屏障，以分層的方式來進行防禦。

- 抵禦外部攻擊
- 延緩攻擊



邊界模糊 – 雲服務時代來臨

onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

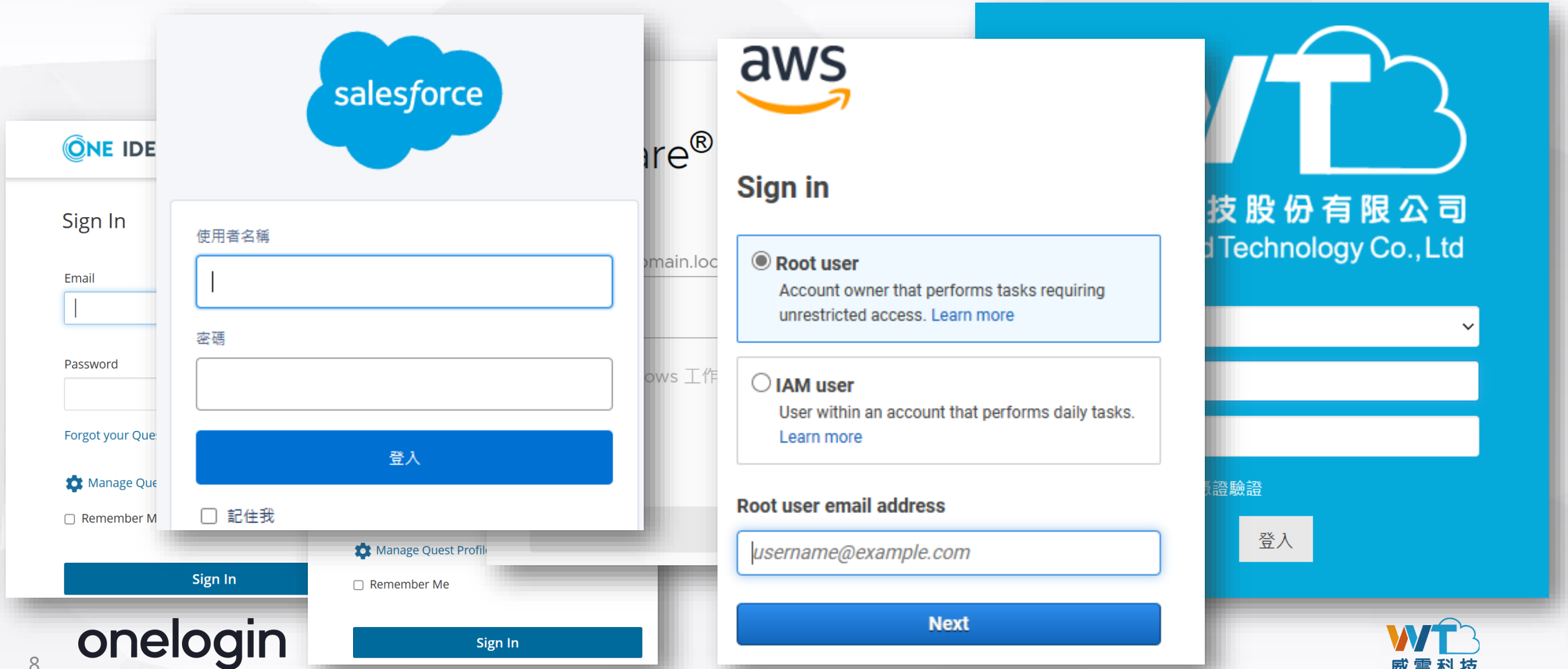
密碼重設成本高昂

- Help Desk 無法及時處理密碼問題
- Forrester Research 統計平均重設密碼的成本為70美金

onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

多雲數位身分管理不易 – 地雲服務的登入問題



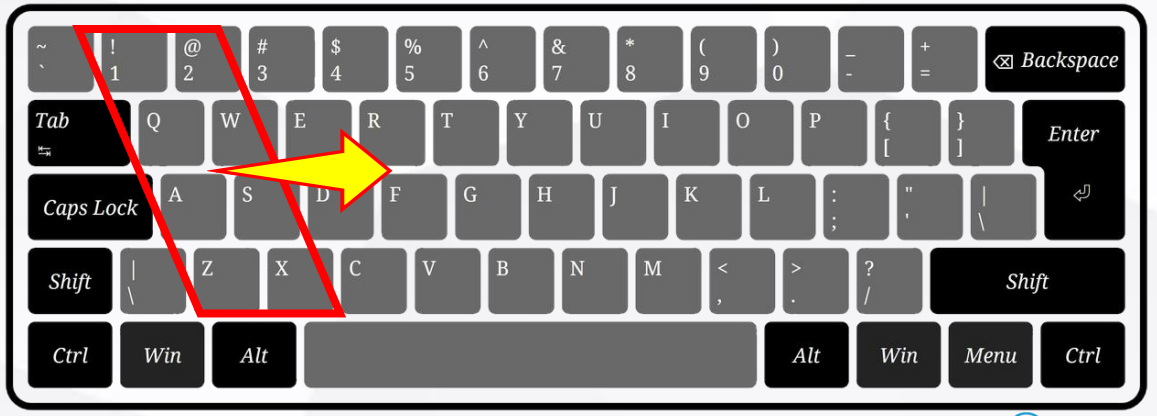
onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

多雲數位身分管理不易 - 多帳號/多密碼問題

- 一個服務一組帳號密碼
  - 多次錯誤帳號密碼遭鎖定
  - 密碼原則的不同 (複雜度、週期)
- 都設同一組密碼
  - 密碼遭竊，駭客暢行無阻
  - 換密碼換到發瘋

導入	服務	帳號	密碼
2004	App1	TW009	ji32k7au4a83
2006	App2	Charlie.Wang	P@ssw0rd
2008	App3	Charlie@wt.com	$RFV5tgb
2012	App5	Charlie_Wang	#EDC4rfv
2015	App6	Charlie@wt.com	1qaz@WSX3edc
2016	App7	TW0009	1qaz@WSX3edc



onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

難以鑑別登入者是否為本人 - SSO 衍伸問題

LOGIN SUCCESSFUL

這真的是你本人嗎?

onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

難以鑑別登入者是否為本人 – 帳行無阻

零信任框架的推行

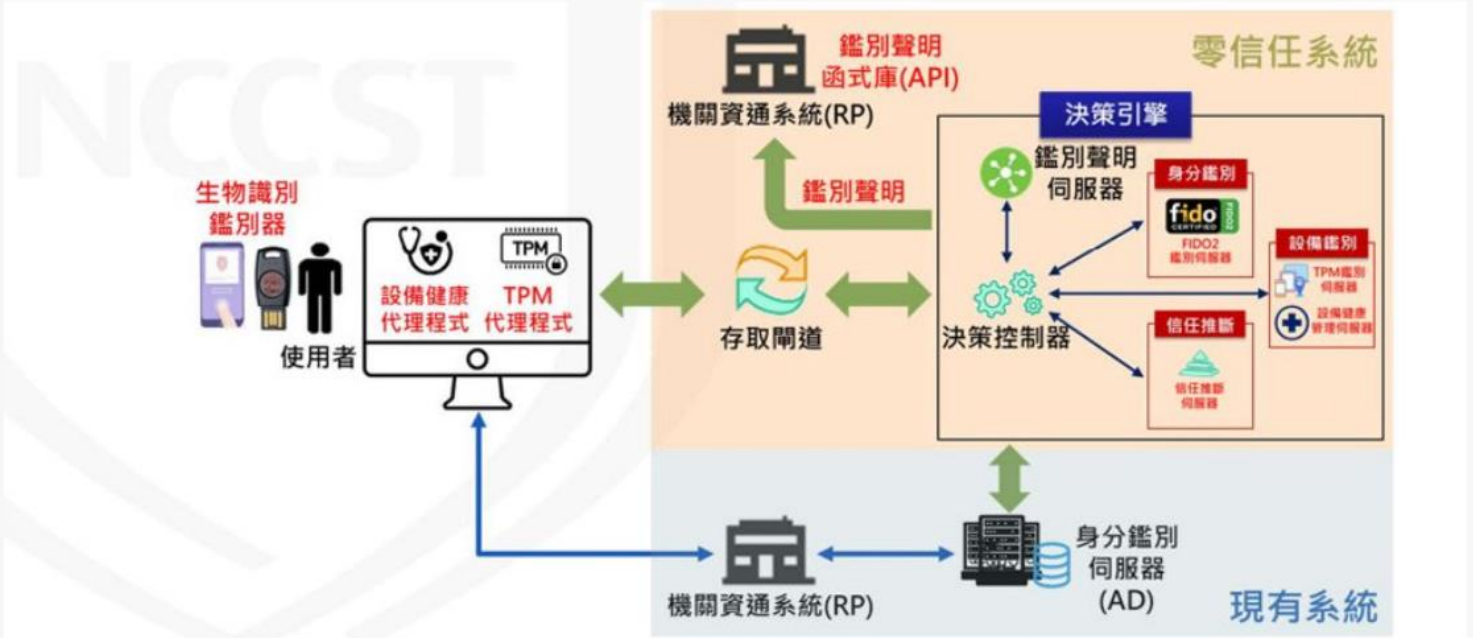
新聞

臺灣政府零信任網路戰略成形，優先推動A級公務機關逐步導入，身分鑑別先行

全球都在關注的網路安全零信任轉型，臺灣政府也要開始行動了！目前我國最新規畫出爐，現階段2022年8月正遴選導入試行的機關，後續將優先推動A級公務機關逐步導入，同時也將促進國內資安業者發展相關產業鏈

文/ 羅正漢 | 2022-08-17 發表

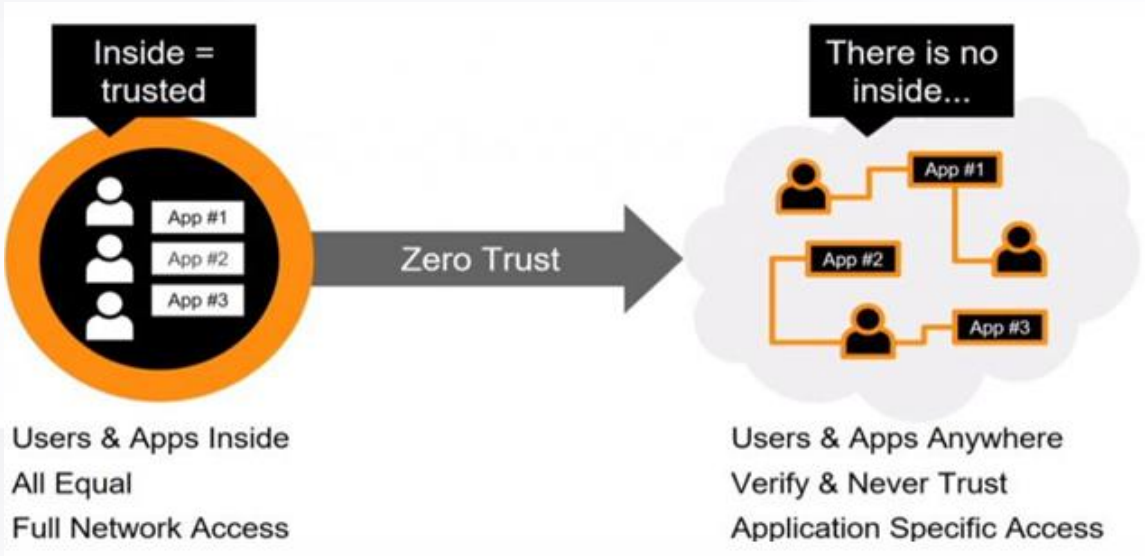
讚 160 分享



在2022年7月，行政院國家資通安全會報技術服務中心說明政府推動零信任網路的計畫，將採門戶部署方式，逐年導入零信任網路的3大核心機制：身分鑑別、設備鑑別，以及信任推斷。（圖片來源／擷取自行政院國家資通安全會報技術服務中心）

零信任概念

- 補強傳統的資安邊界防禦概念，保護資產存取
  - 除了保護網路存取，更著重於保護或應用程式的存取
  - 邊界模糊化，設備、應用程式、資料無所不在



Never trust.

Always verify.

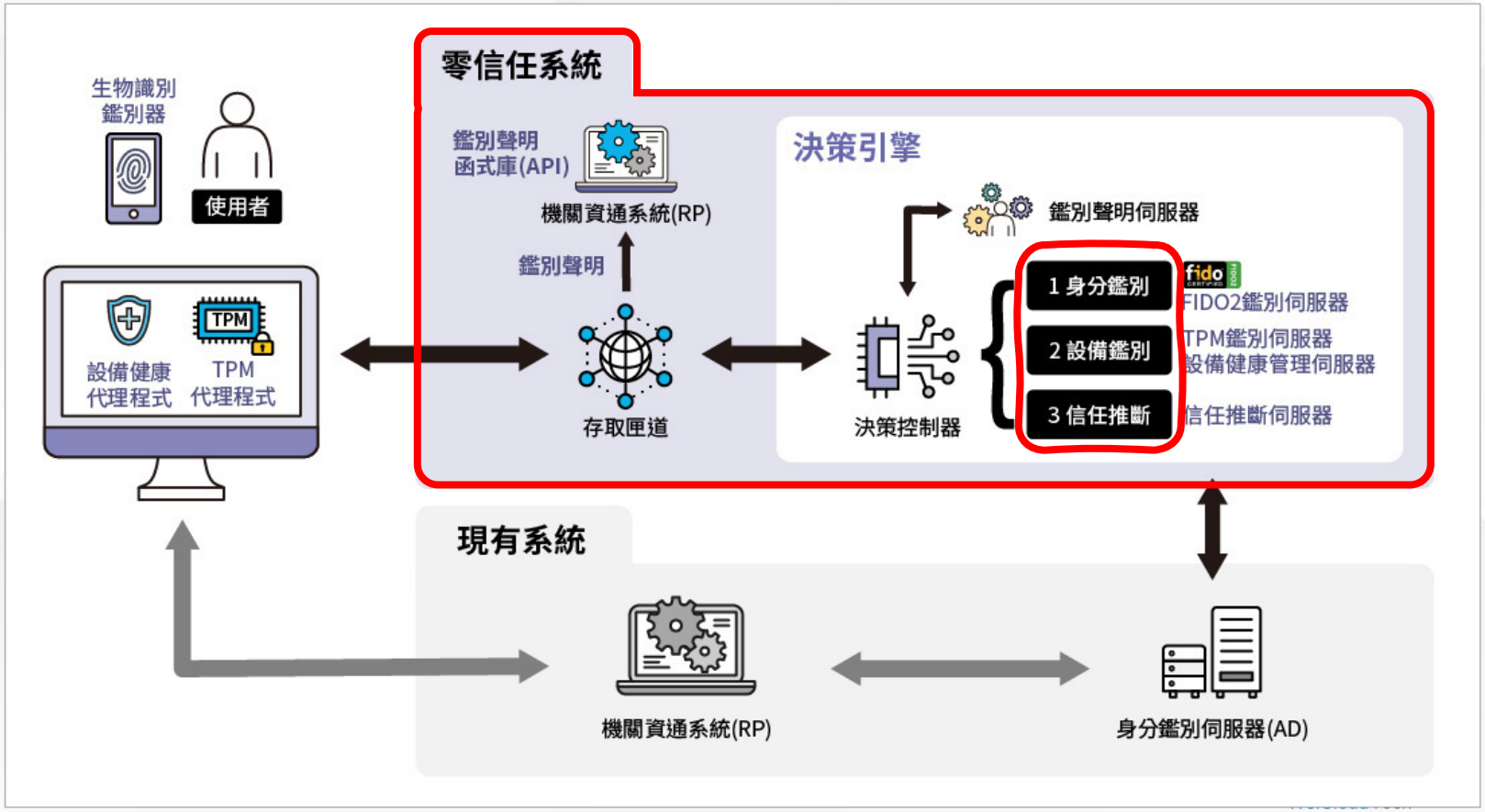
onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

資安院-零信任導入建議

國家資通安全研究院
National Institute of Cyber Security

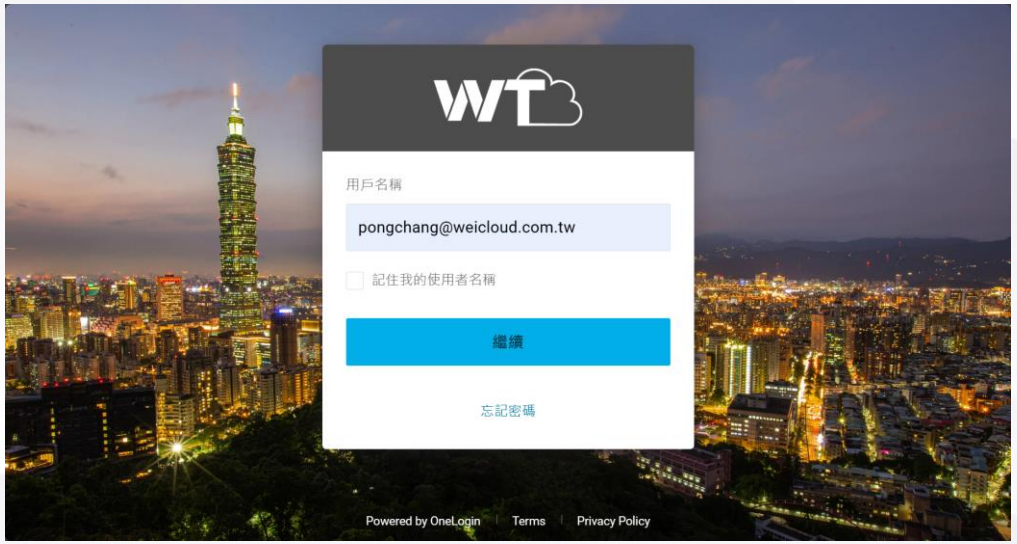
- 由決策引擎為核心包含以下三大技術
  - 身分鑑別
  - 設備鑑別
  - 信任推斷



onelogin by ONE IDENTITY

身分鑑別

- 利用 FIDO2 的相關技術來鑑別使用者的身份，透過**公開金鑰加密**（Public Key Cryptography）的架構進行**多重因素驗證（MFA）**以及**生物辨識**登入來加強身分。



onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

FIDO2

- FIDO2 在原有的 FIDO 標準中加入了 WebAuthn 這個規範，強調 Passkey 的使用來實現 FIDO 聯盟最初的免密碼(Passwordless)目標

- 多因子驗證 MFA 中強調的三個因子為
  - ~~Something you know~~
  - Something you have
  - Something you are

onelogin by ONE IDENTITY

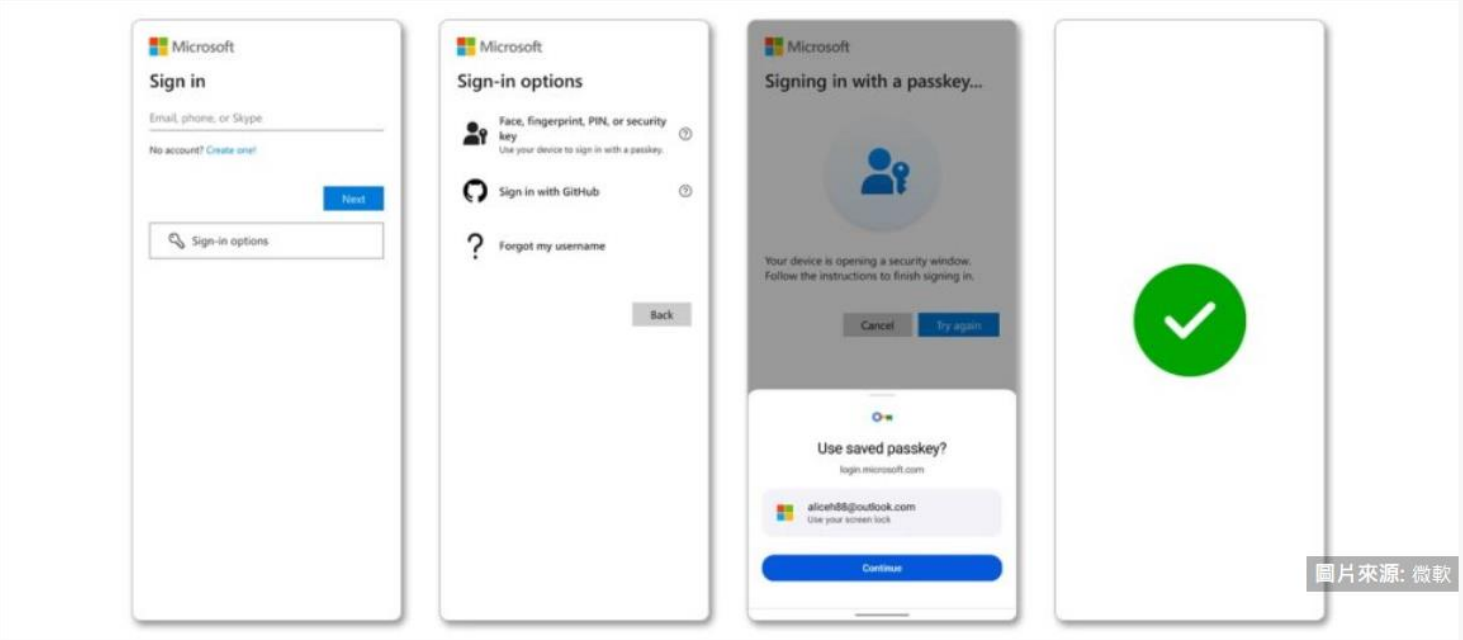
威雲科技 WeiCloudTech

微軟通行密鑰開始支援消費者帳戶

在5月2日、2024世界密碼日這天，微軟宣布開始支援微軟消費者帳戶的通行密鑰

文/ 陳曉莉 | 2024-05-03 發表

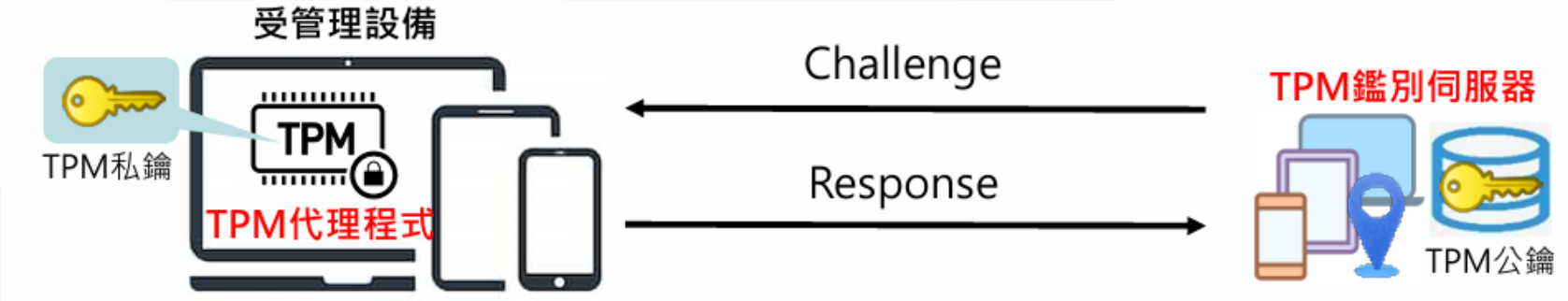
讚 146 分享



每年5月的第一個周四（5/2）為世界密碼日（World Password Day），微軟與Google都在當天發表雙方在推動通行密鑰（Passkey）上的成果。其中，微軟宣布開始支援微軟消費者帳戶的通行密鑰，而Google則說，迄今已有4億個Google帳戶執行逾10億次的通行密鑰身分驗證。

設備鑑別

- 基於軟體憑證或 TPM 的公開金鑰密碼系統鑑別協議，以確認使用者端點設備是受到機關管理
  - 註冊階段：於 TPM 鑑別伺服器註冊受管理設備之 TPM 公鑰
  - 鑑別階段：代理程式進行私鑰運算，並與鑑別伺服器完成鑑別協議

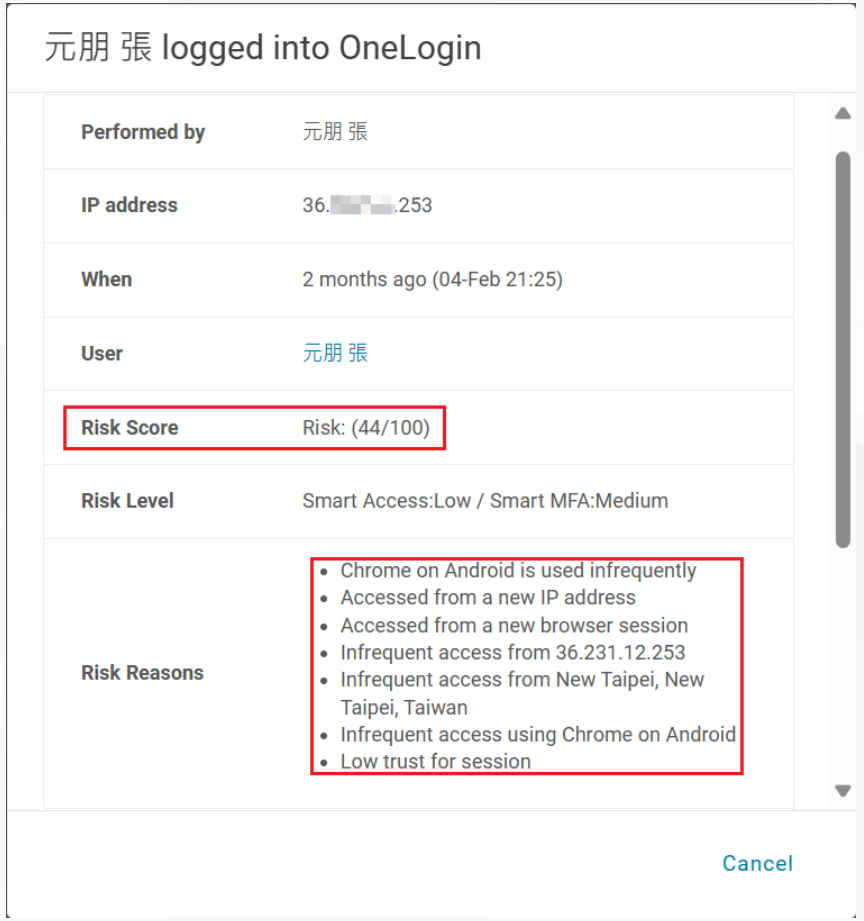


onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

信任推斷

- 依使用情境計算每次存取之信任分數作為判斷依據 (Score)
  - 登入時間
  - 登入地點
  - 登入的裝置
  - 登入的來源 IP
  - 登入使用的瀏覽器



onelogin by ONE IDENTITY

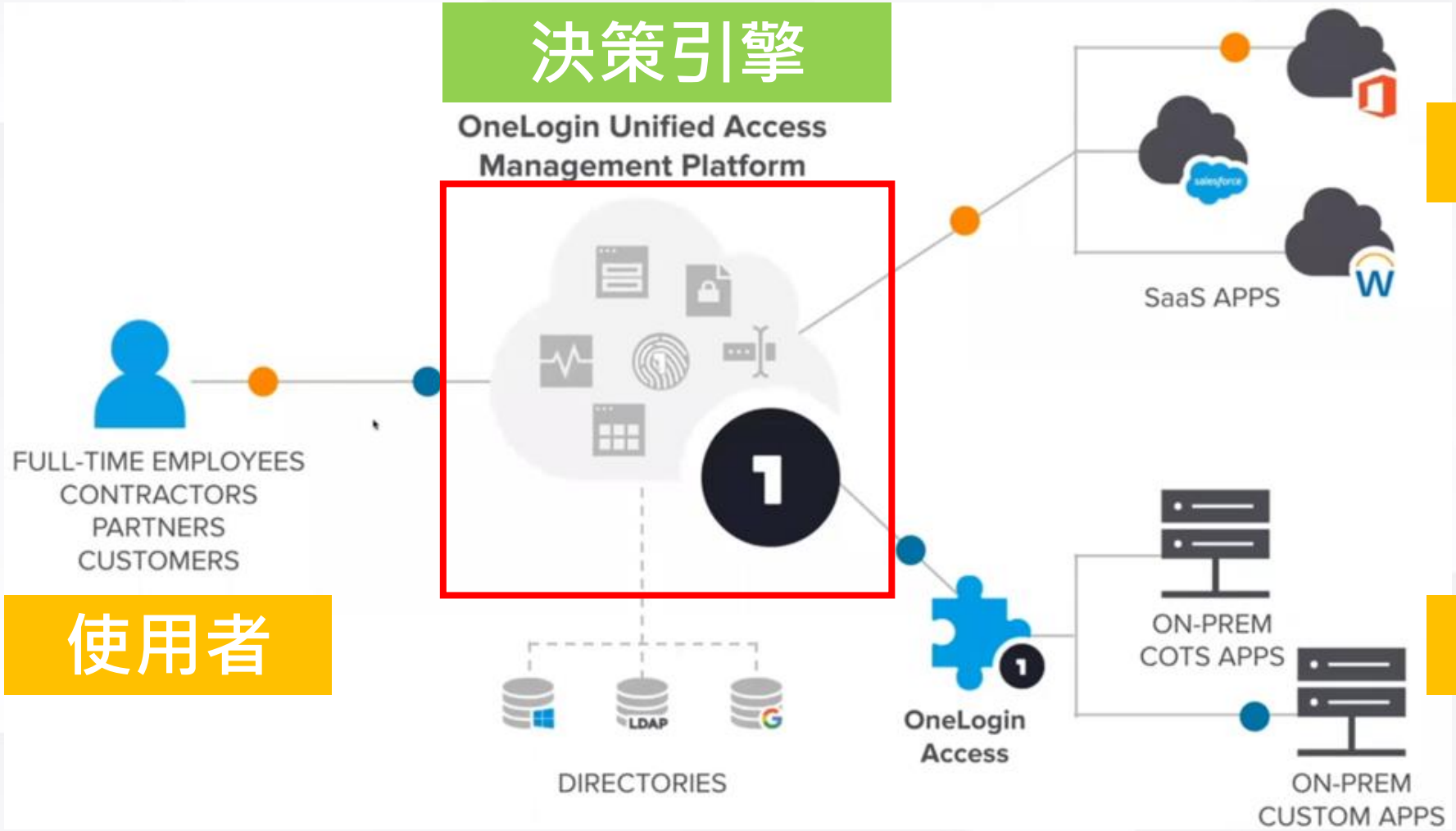
威雲科技 WeiCloudTech

零信任概念的導入

onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

導入架構

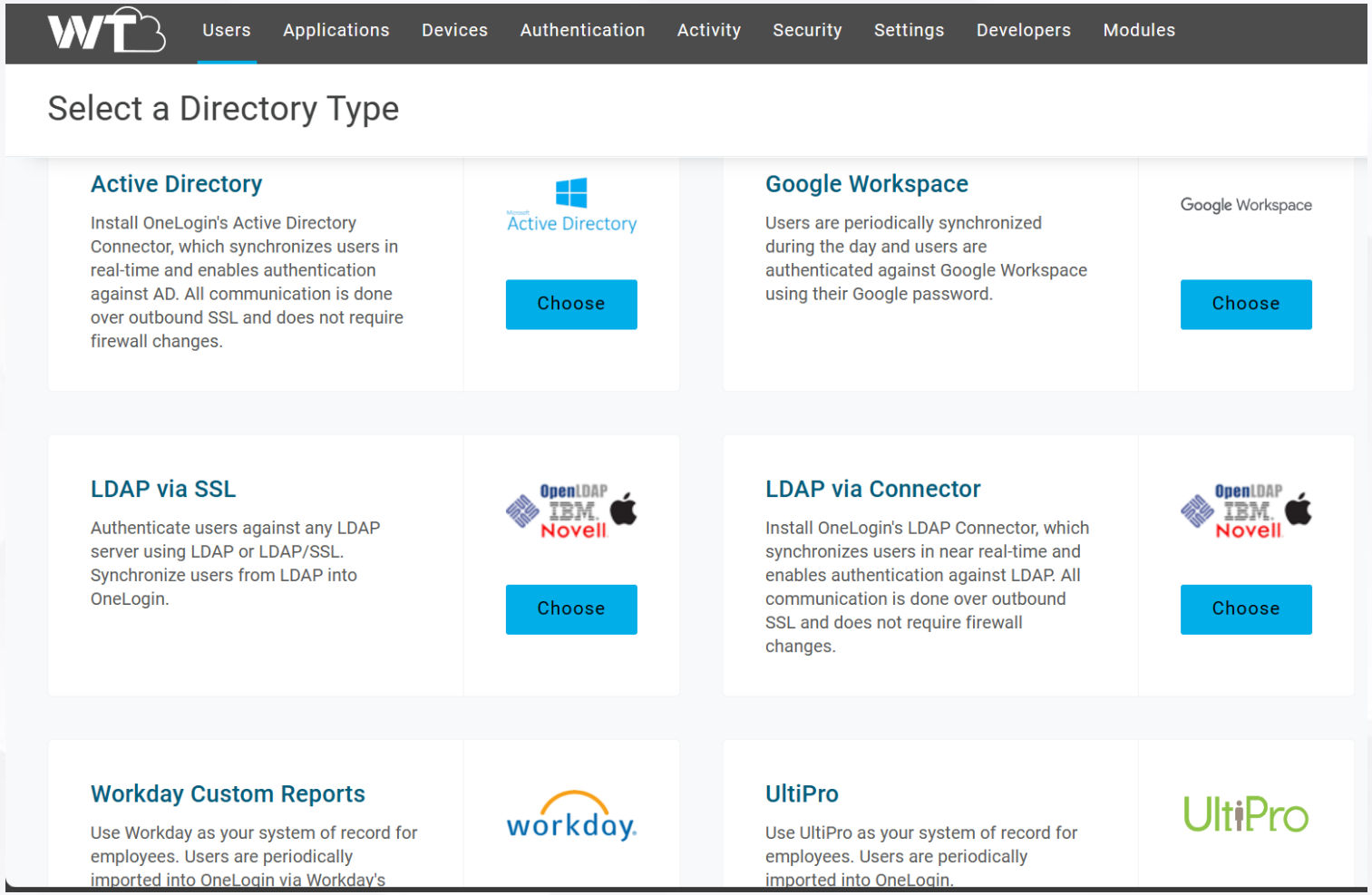


onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

多帳號源整合 (OneLogin 做為 IdP)

- 帳號源：
  - AD
  - Entra ID (AAD)
  - G-Suite
  - LDAP
  - 部分SaaS HR 系統



onelogin by ONE IDENTITY

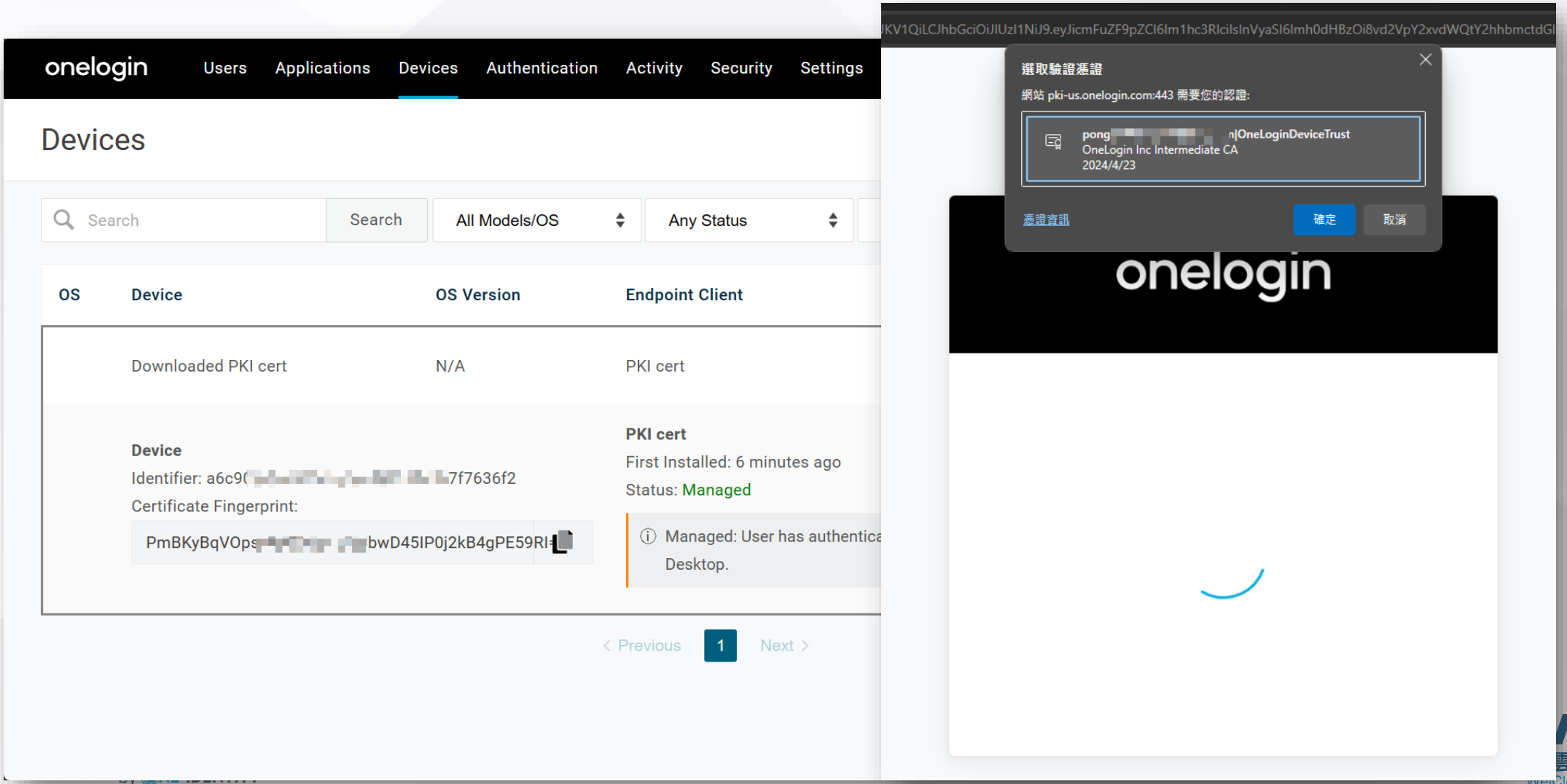
威雲科技 WeiCloudTech

多種因子驗證 (身分鑑別)

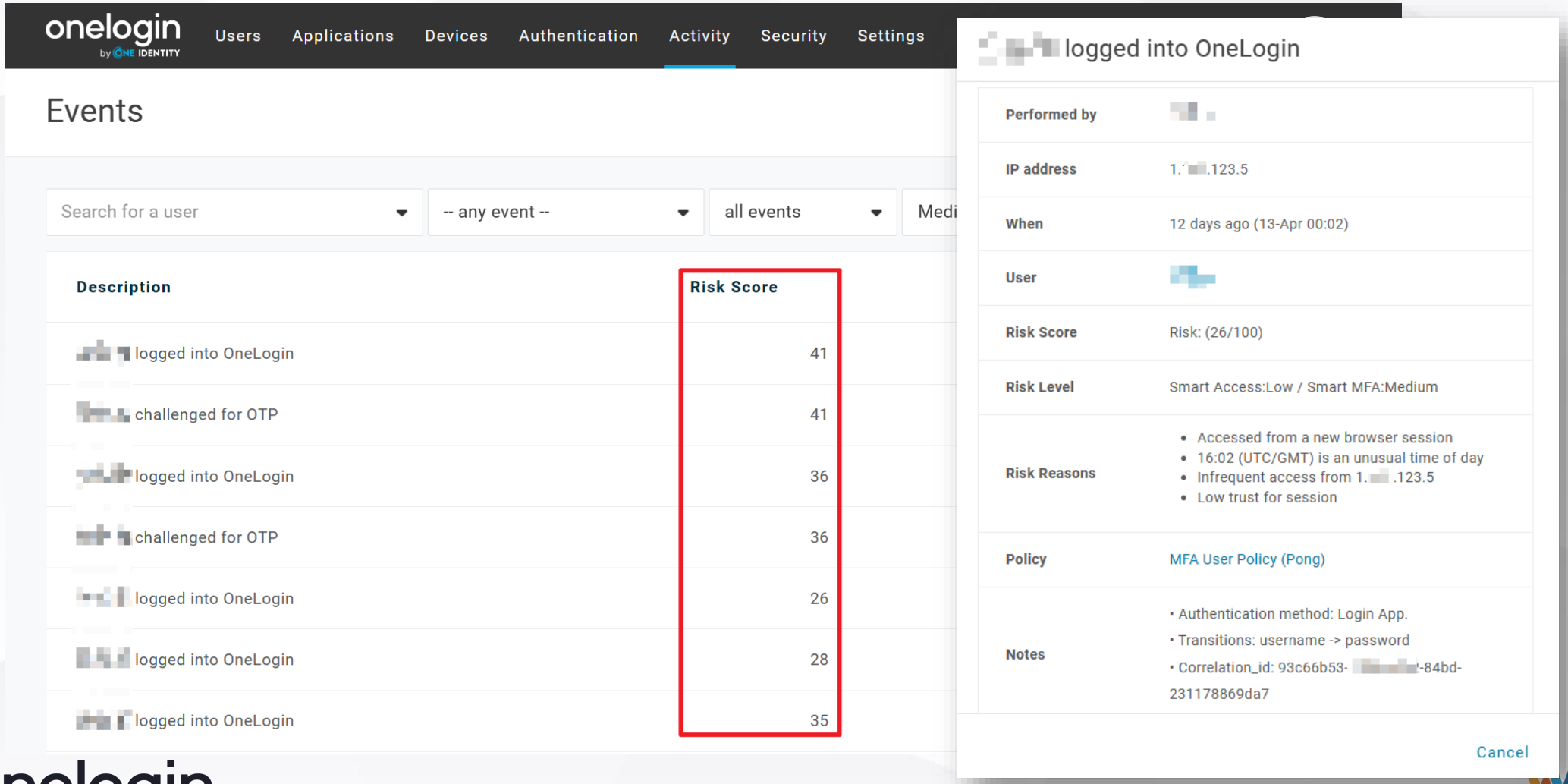
onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

PKI Cert 裝置綁定 (設備鑑別)



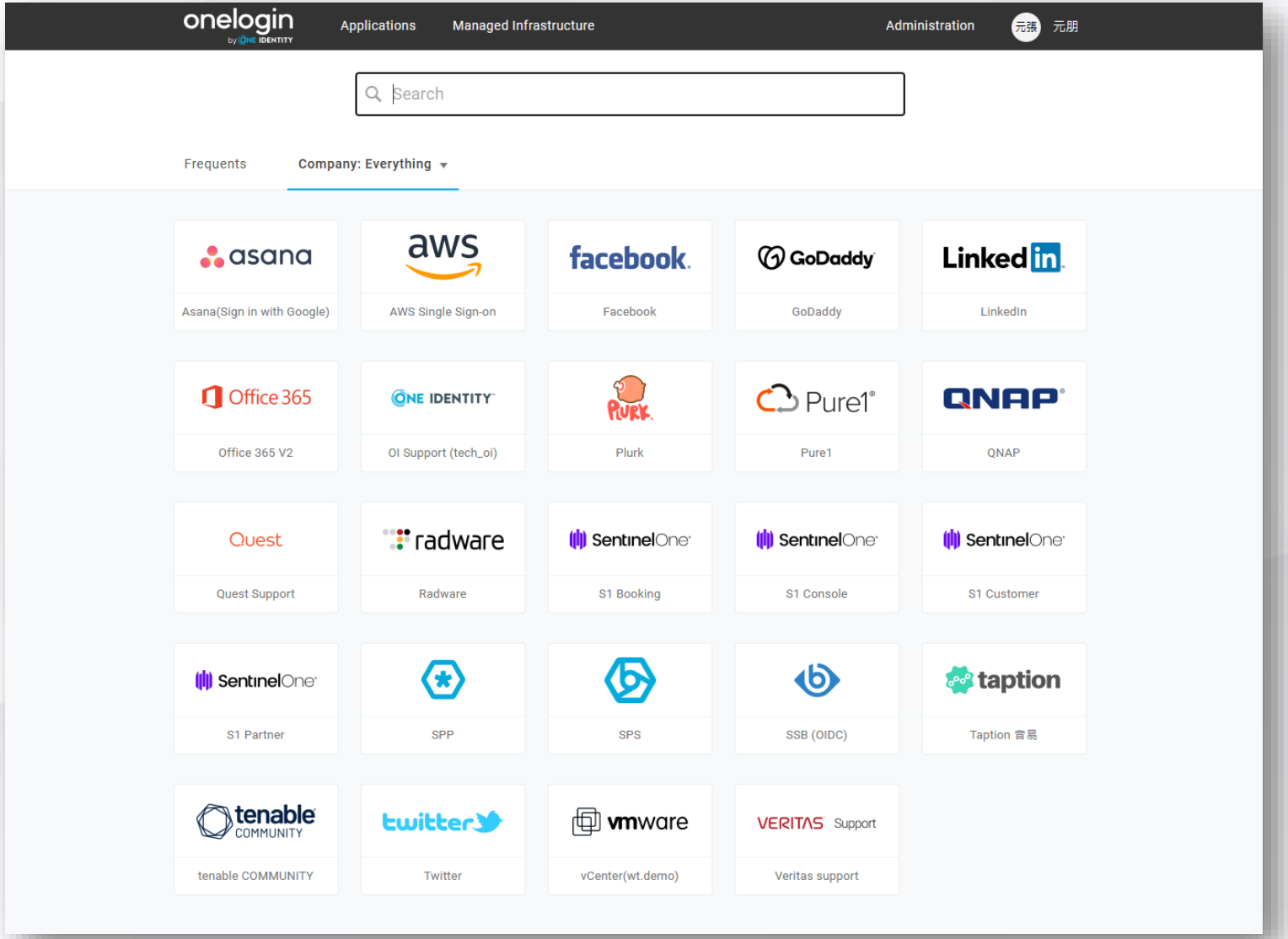
使用者登入的風險分數 (信任推斷)



onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

單一介面多服務整合 (Single Sign-On)



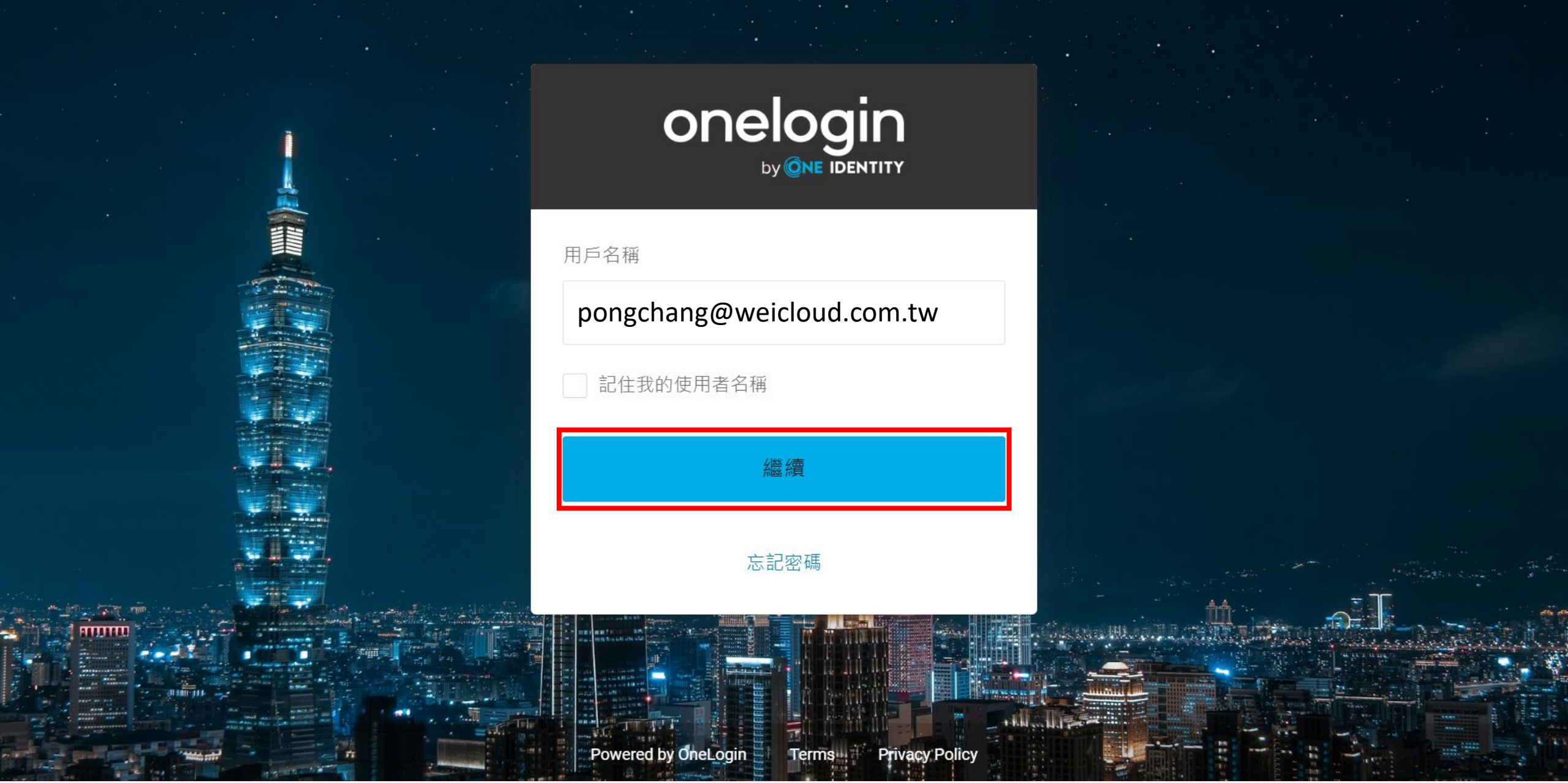
onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

登入流程展示

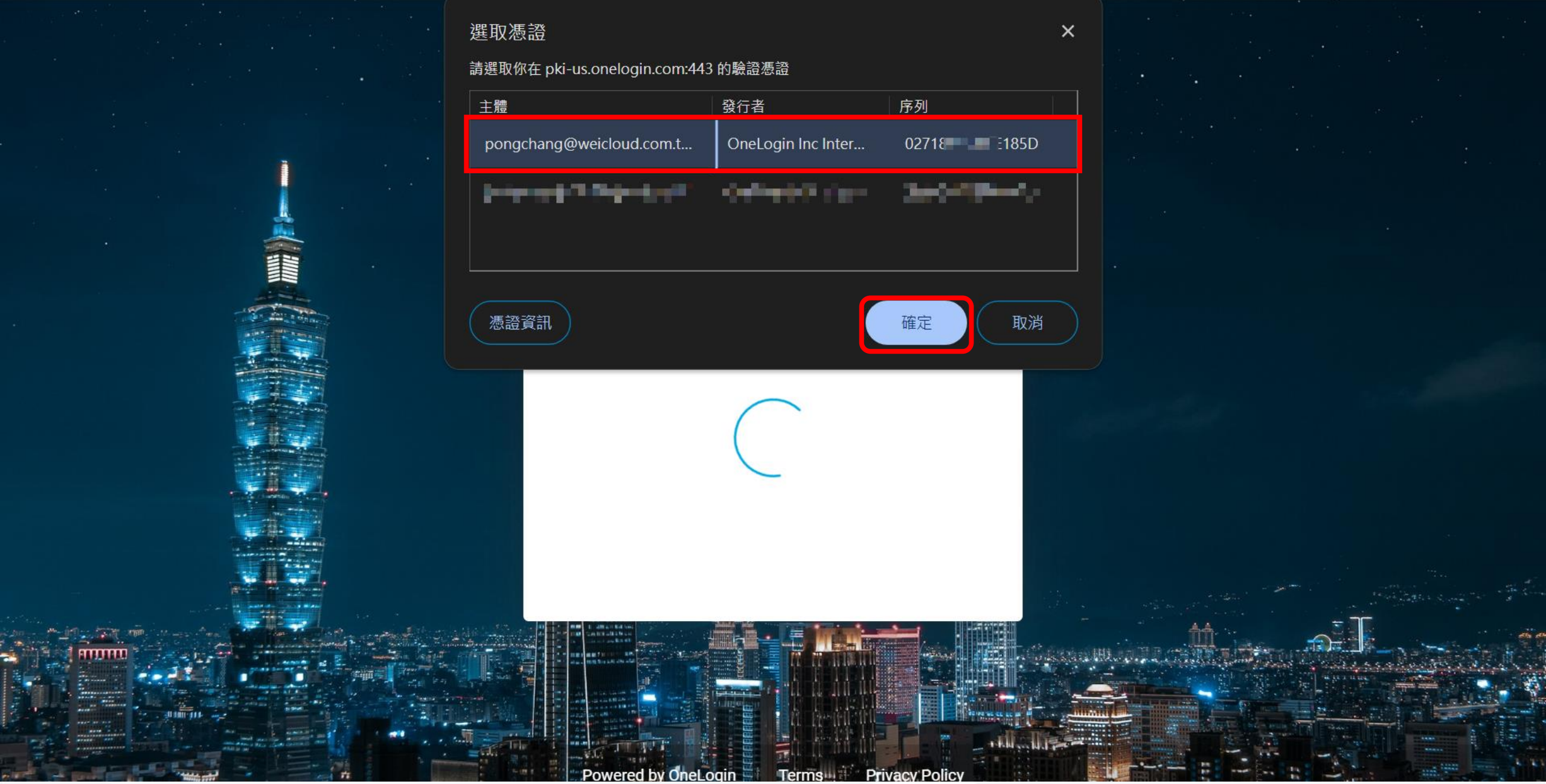
onelogin by ONE IDENTITY

威雲科技 WeiCloudTech



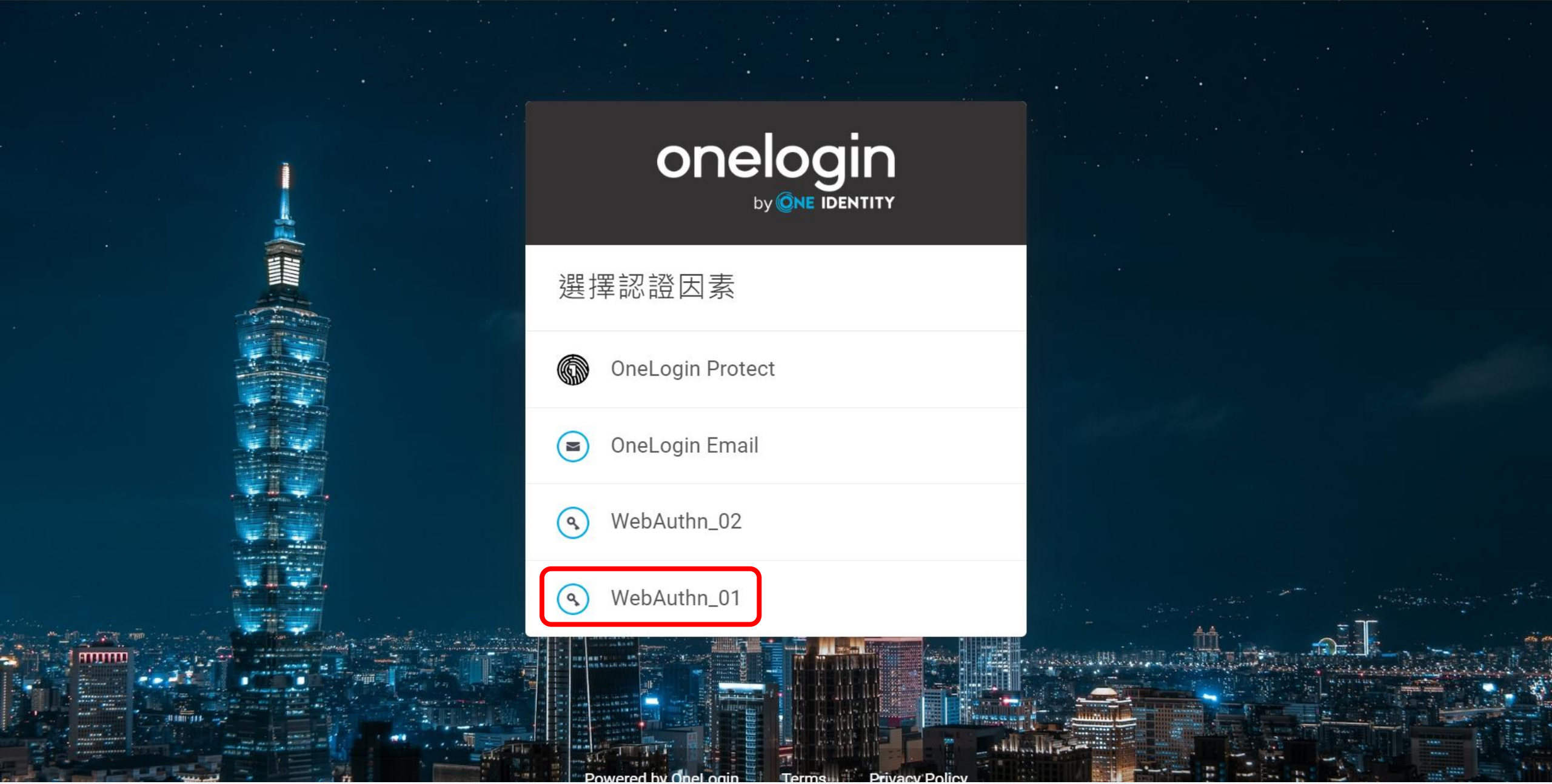
onelogin by ONE IDENTITY

威雲科技 WeiCloudTech



onelogin by ONE IDENTITY

威雲科技 WeiCloudTech



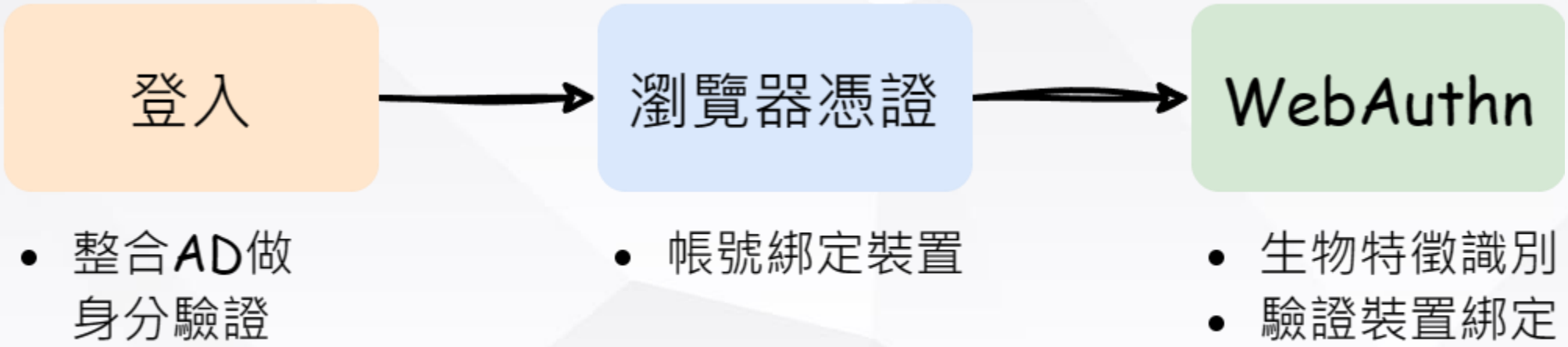
onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

onelogin by ONE IDENTITY

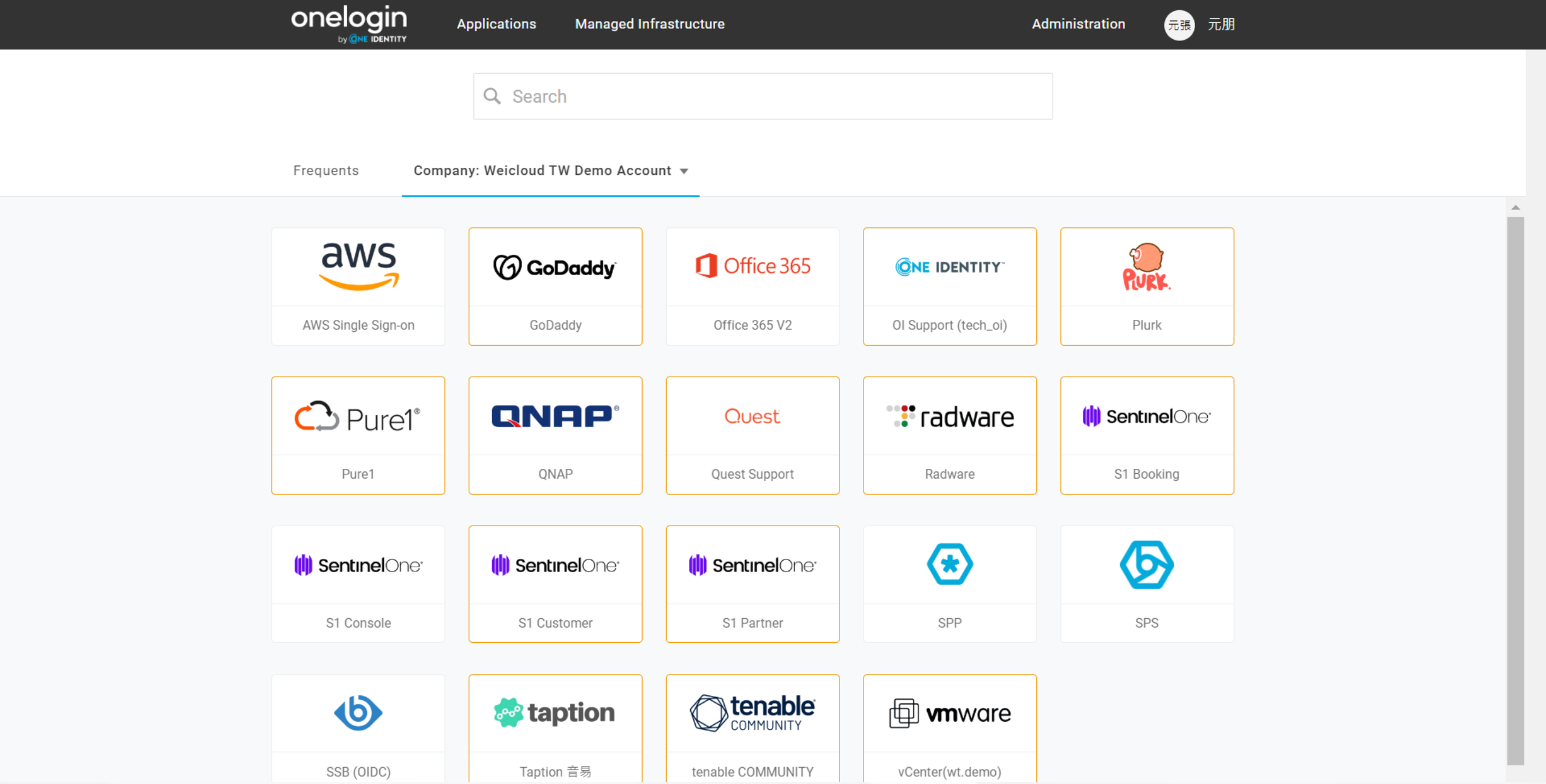
威雲科技 WeiCloudTech

登入驗證流程



onelogin by ONE IDENTITY

威雲科技 WeiCloudTech



onelogin by ONE IDENTITY

威雲科技 WeiCloudTech

Applications

Download JSON | Add App

Search | Search

Total apps 30

App	Authorization Type	Users	Provisioning	Last Updated	Visible in Portal
Office 365 V2	WS-Federation with SAML 1.1	6	Available	about 1 month ago	✓
AWS Single Sign-on	SAML2.0	3	Enabled	6 months ago	✓
S1 Console	SAML2.0	5	Not Available	3 months ago	✓
SPP	SAML2.0	5	Not Available	6 months ago	✓
SPS	SAML2.0	5	Not Available	6 months ago	✓
SPP (test)	SAML2.0	1	Not Available	5 months ago	✓
syslog-ng StoreBox (OIDC)	OpenID Connect	0	Not Available	6 months ago	✓
PAM Essentials Portal	OpenID Connect	4	Not Available	26 days ago	
One Identity Cloud	OpenID Connect	4	Not Available	26 days ago	

TAKEAWAY

- **邊界模糊**
  - 加強身分管理與存取治理
- **密碼重設成本高昂**
  - 透過身分存取管理(IAM)密碼自助服務降低人力及時間成本
- **多雲數位身分管理不易**
  - 透過 SAML、OIDC 串接多雲服務身分驗證
- **難以鑑別登入者是否為本人**
  - 透過 FIDO2 搭配生物辨識(Biometric)

Thanks

onelogin by ONE IDENTITY

威雲科技股份有限公司
Weicloud technology Co., Ltd