



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

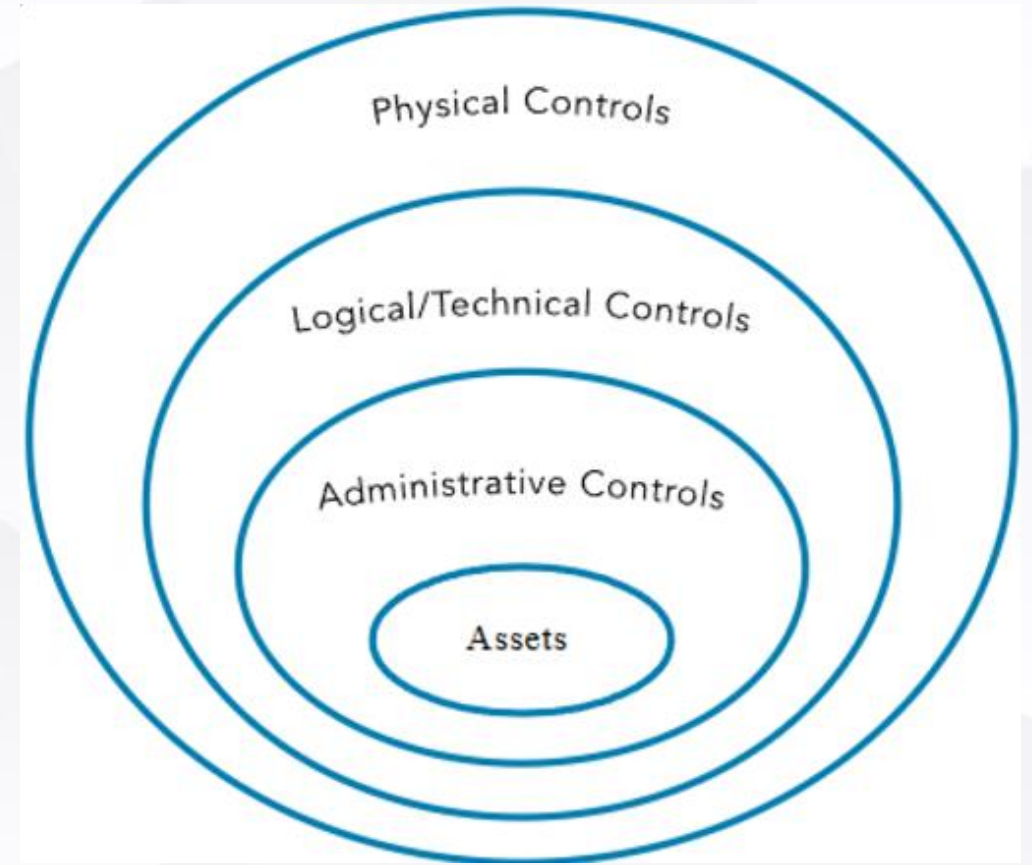
多雲時代衍生的問題

- 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

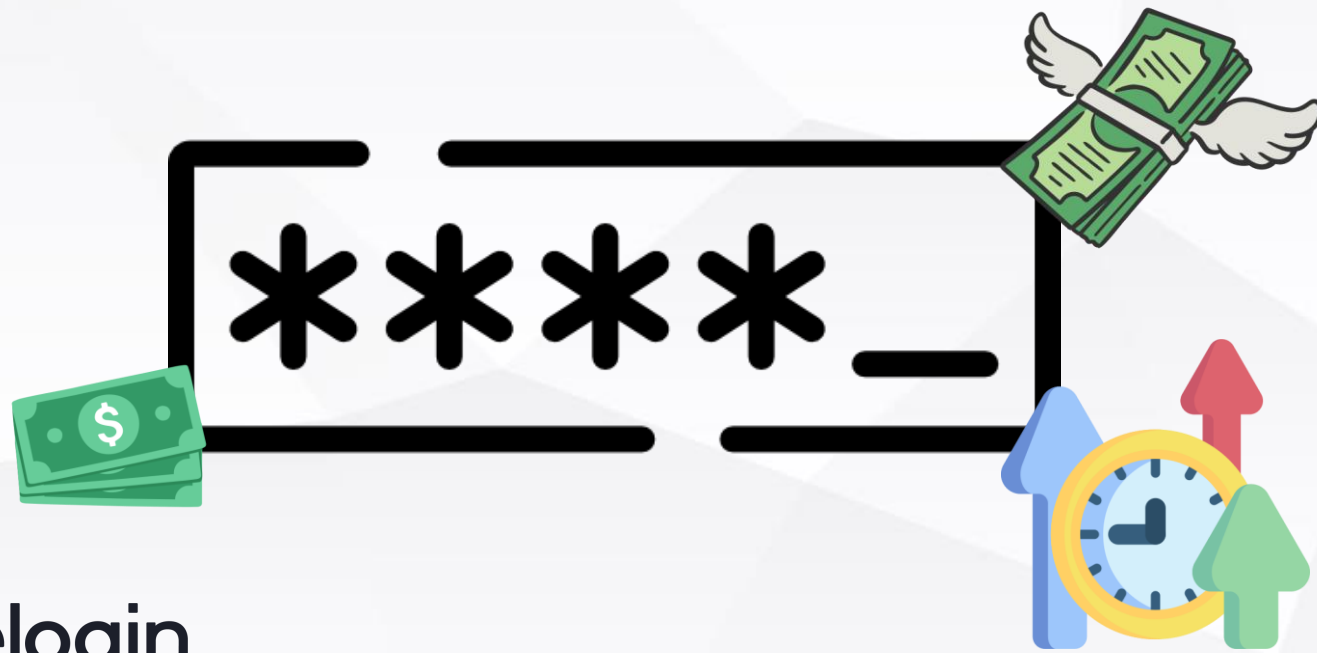


邊界模糊 – 雲服務時代來臨



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



70 \$

多雲數位身分管理不易 — 地雲服務的登入問題

The image displays three overlapping login screens:

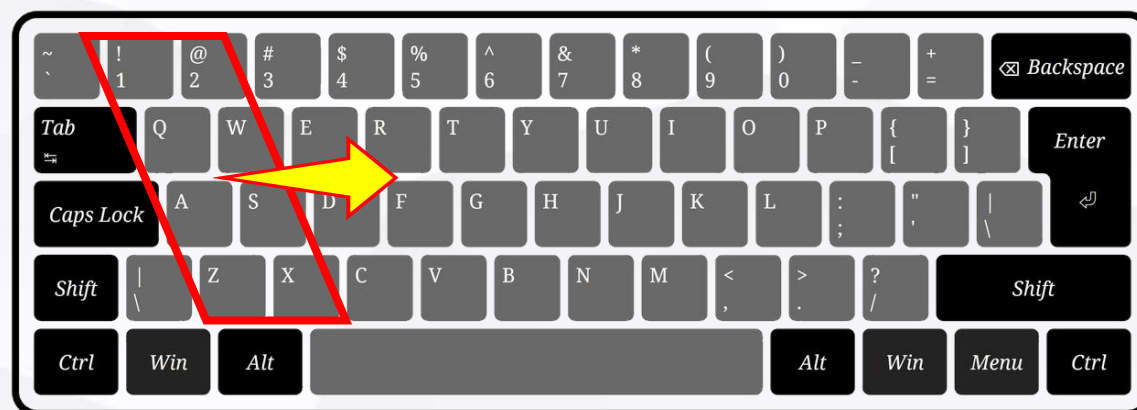
- Left (One Identity):** A 'Sign In' form with fields for 'Email' and 'Password', a 'Remember Me' checkbox, and a 'Sign In' button.
- Middle (Salesforce):** A 'Sign In' form with a 'salesforce' logo, a '使用者名稱' (Username) field, a '密碼' (Password) field, a '登入' (Sign In) button, and a '記住我' (Remember Me) checkbox.
- Right (AWS):** An 'aws Sign in' form with radio buttons for 'Root user' (selected) and 'IAM user', a 'Root user email address' field containing 'username@example.com', and a 'Next' button.

On the far right, a blue banner for 'WeiCloudTech' (威雲科技) is partially visible, featuring a large 'WT' logo and the text '技股份有限公司' and 'Technology Co., Ltd'. Below the banner, there are input fields and a '登入' (Sign In) button.

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 |



難以鑑別登入者是否為本人 - SSO 衍伸問題

LOGIN SUCCESSFUL

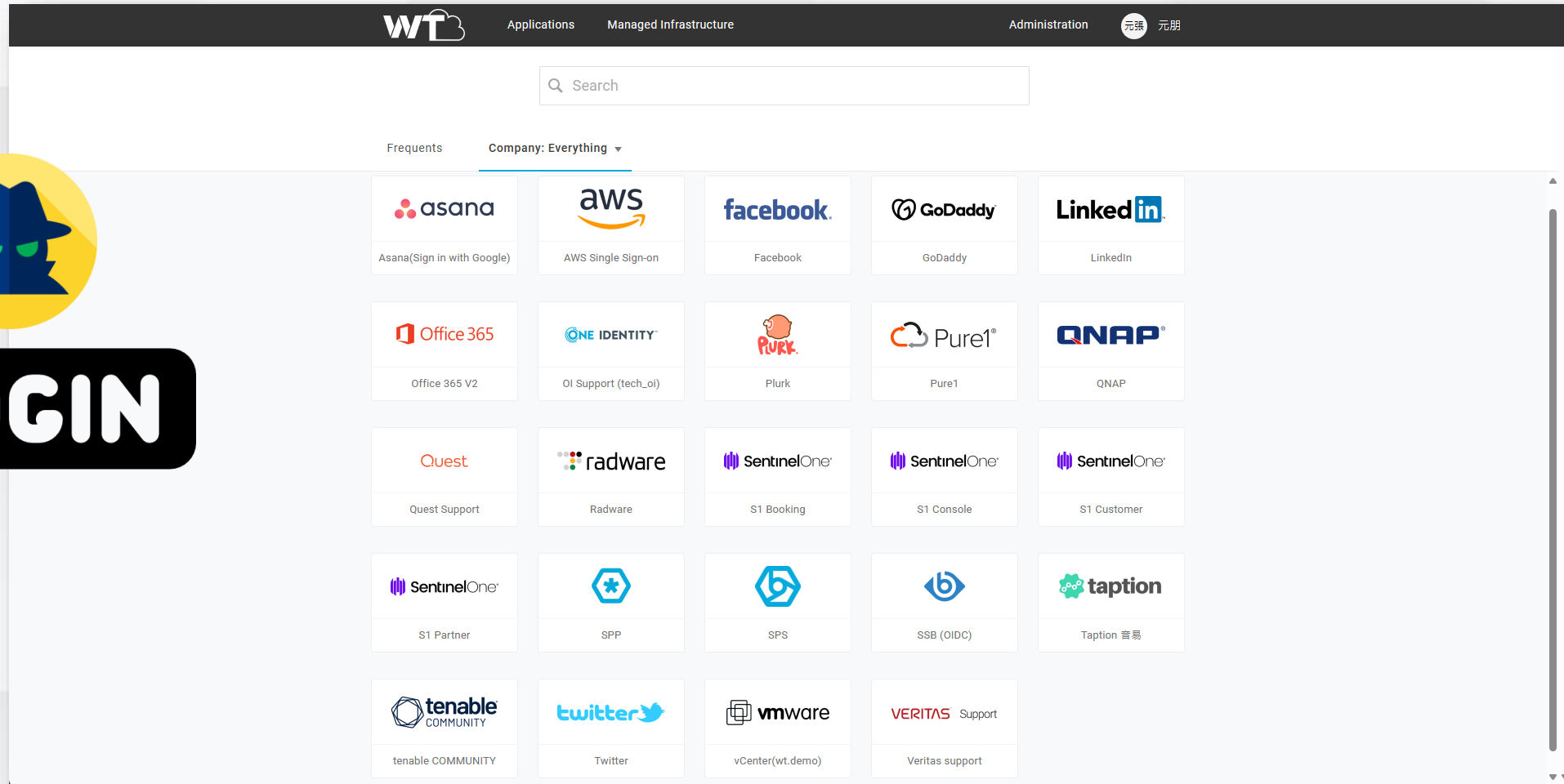


這真的是你本人嗎？

難以鑑別登入者是否為本人 – 帳行無阻



LOGIN



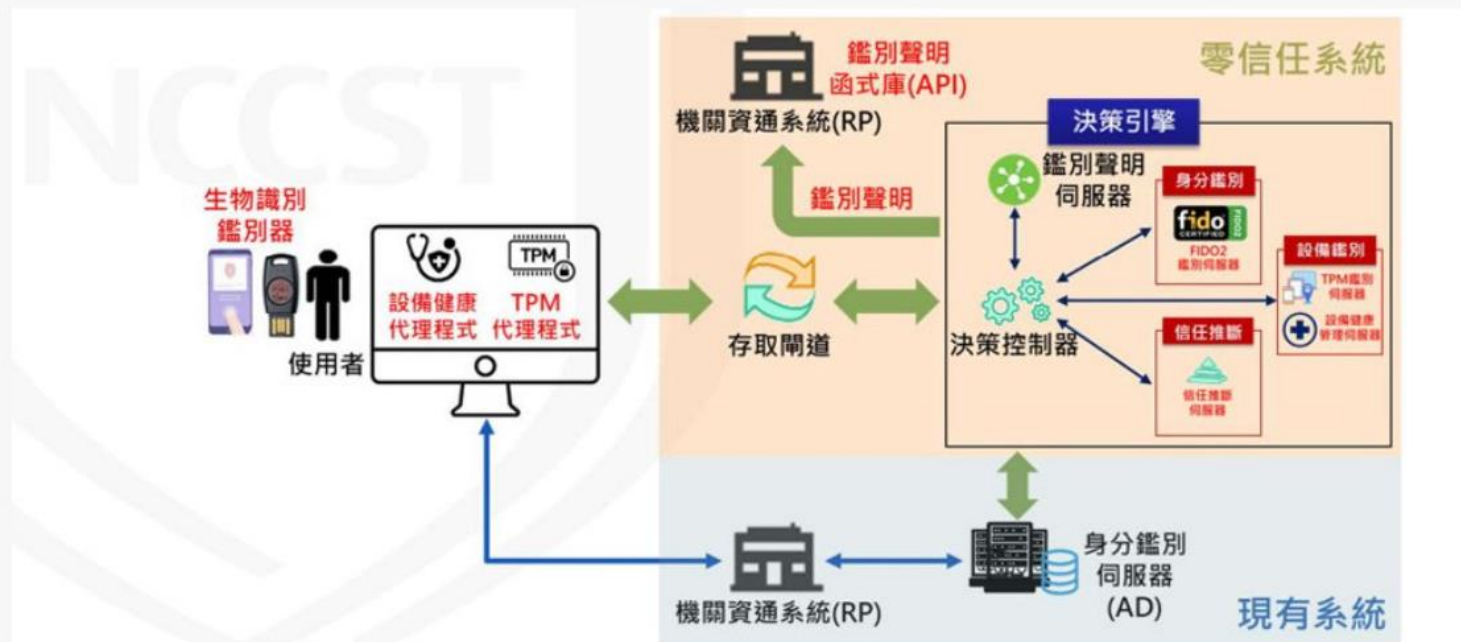
零信任框架的推行

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

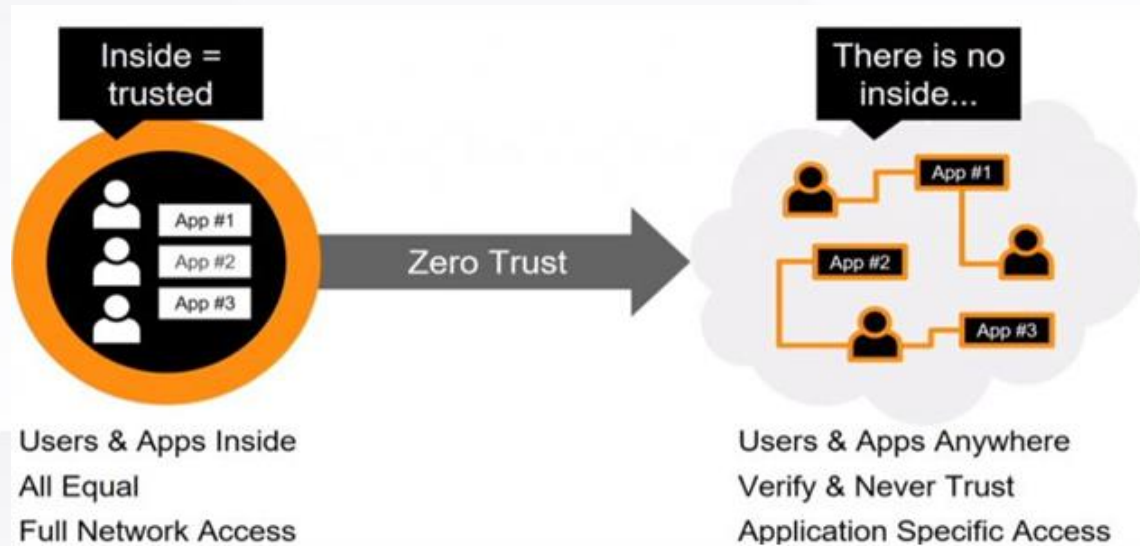
讚 160 分享



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.

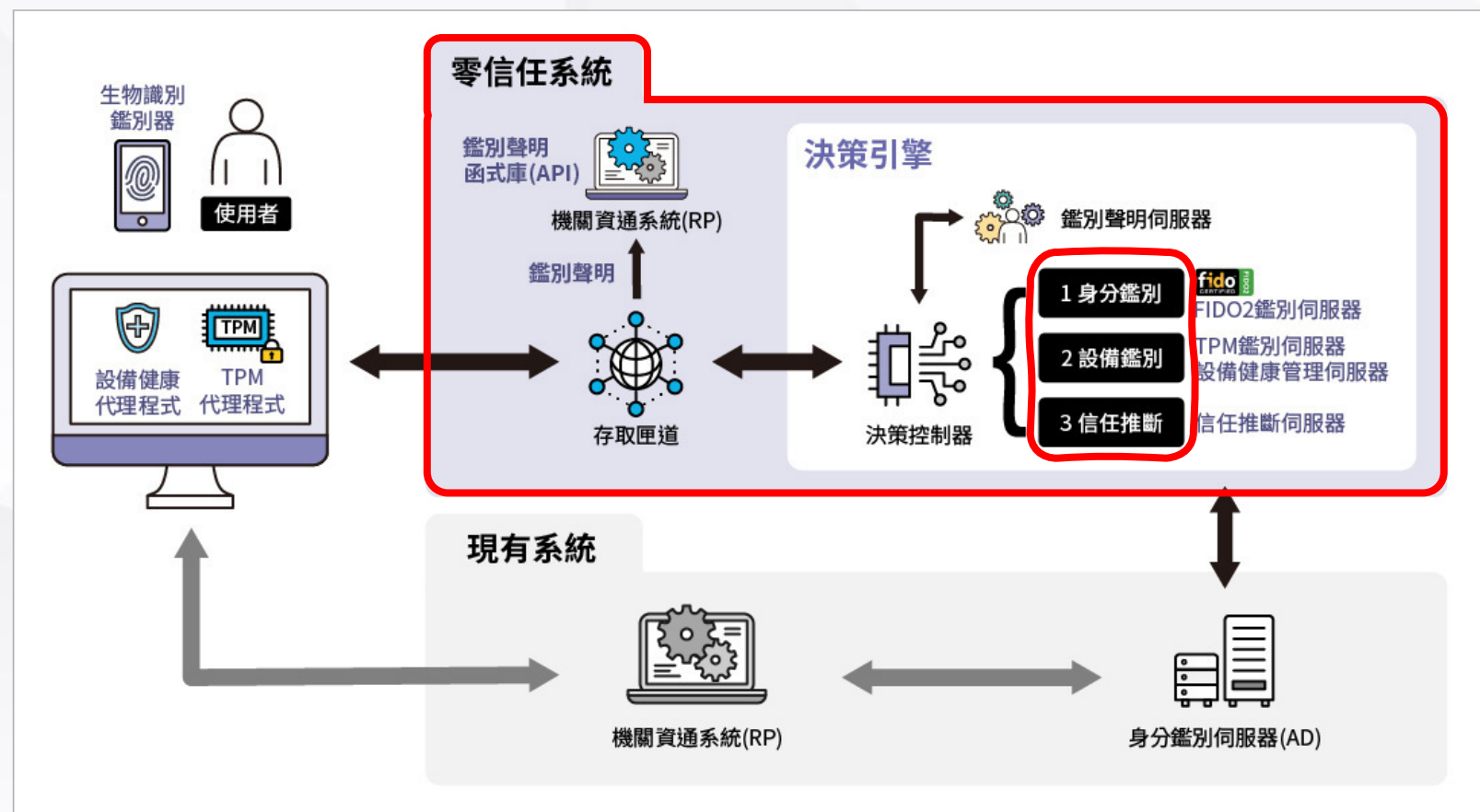
資安院-零信任導入建議



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

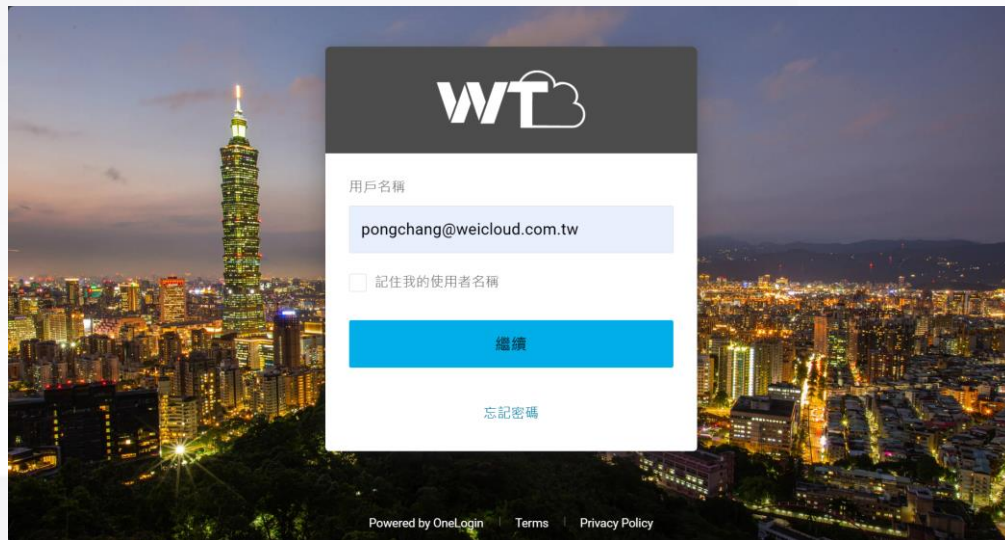
➤ 由決策引擎為核心包含以下三大技術

- 身分鑑別
- 設備鑑別
- 信任推斷



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。



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



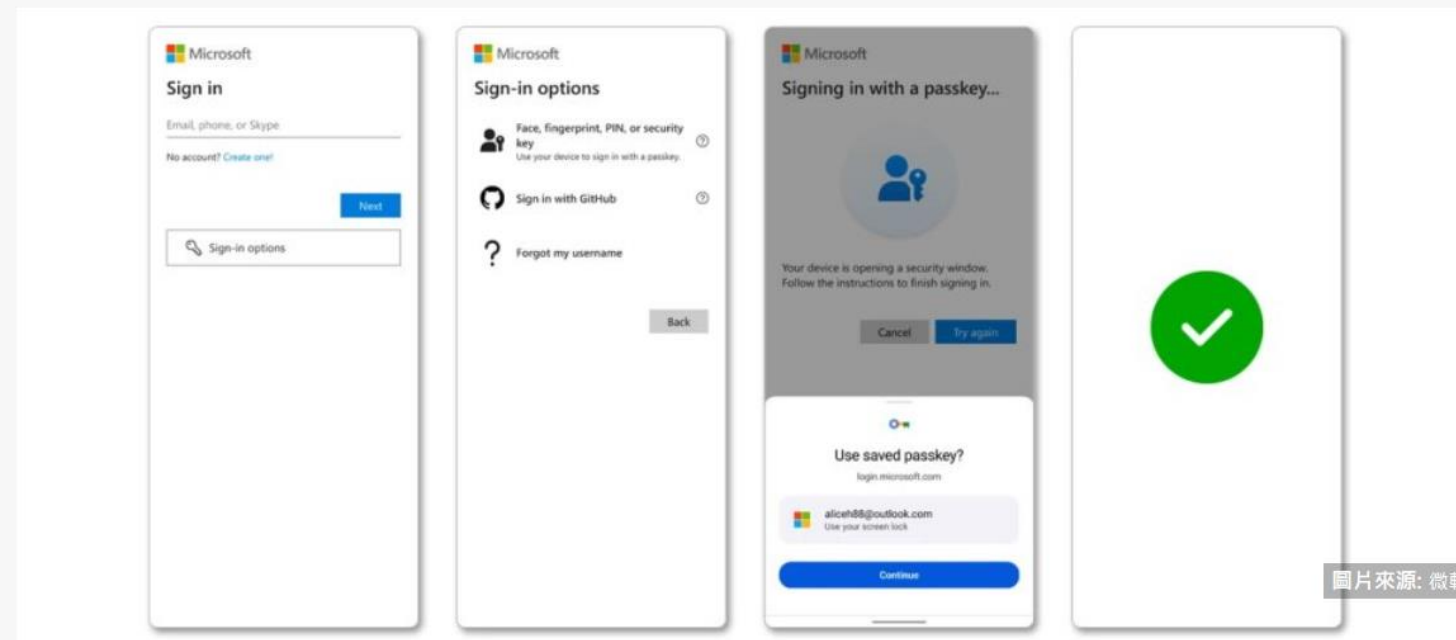
微軟通行密鑰開始支援消費者帳戶

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

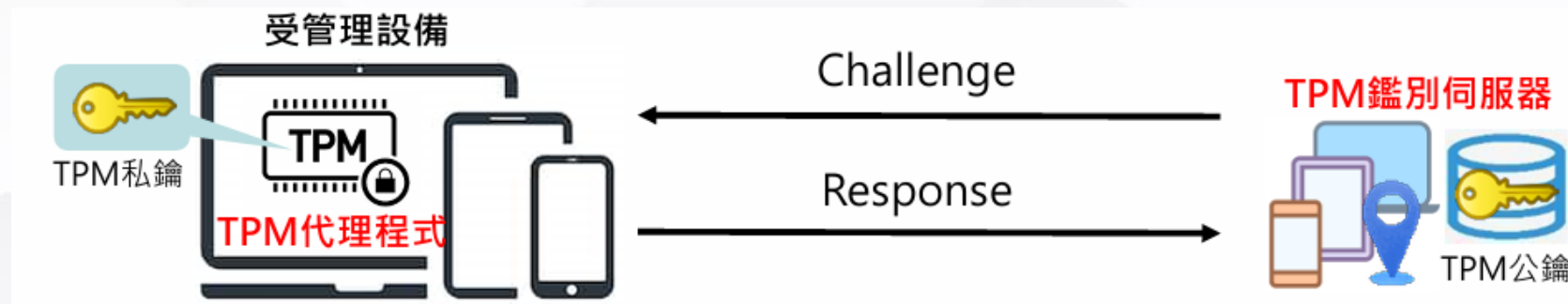
分享



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



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

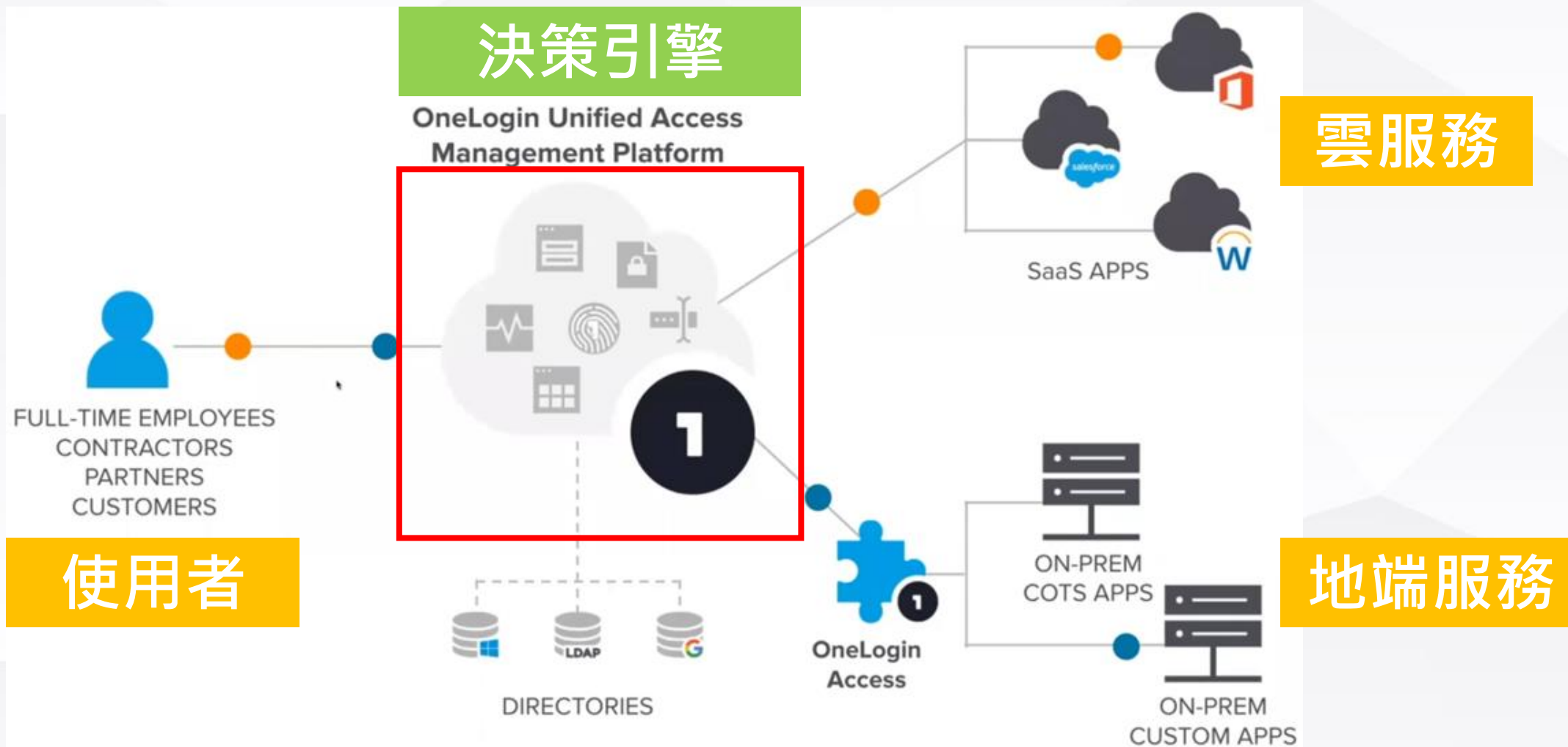
元朋 張 logged into OneLogin

| | |
|--------------|--|
| Performed by | 元朋 張 |
| IP address | 36.██████.253 |
| When | 2 months ago (04-Feb 21:25) |
| User | 元朋 張 |
| Risk Score | Risk: (44/100) |
| Risk Level | Smart Access:Low / Smart MFA:Medium |
| Risk Reasons | <ul style="list-style-type: none">• Chrome on Android is used infrequently• Accessed from a new IP address• Accessed from a new browser session• Infrequent access from 36.231.12.253• Infrequent access from New Taipei, New Taipei, Taiwan• Infrequent access using Chrome on Android• Low trust for session |

Cancel

零信任概念的導入

導入架構



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

The screenshot displays the OneLogin console interface for selecting a directory type. The navigation bar includes: WT, Users, Applications, Devices, Authentication, Activity, Security, Settings, Developers, and Modules. The main heading is "Select a Directory Type".

| Directory Type | Description | Choose Button |
|------------------------|--|---------------|
| Active Directory | Install OneLogin's Active Directory Connector, which synchronizes users in real-time and enables authentication against AD. All communication is done over outbound SSL and does not require firewall changes. | Choose |
| Google Workspace | Users are periodically synchronized during the day and users are authenticated against Google Workspace using their Google password. | Choose |
| LDAP via SSL | Authenticate users against any LDAP server using LDAP or LDAP/SSL. Synchronize users from LDAP into OneLogin. | Choose |
| LDAP via Connector | Install OneLogin's LDAP Connector, which synchronizes users in near real-time and enables authentication against LDAP. All communication is done over outbound SSL and does not require firewall changes. | Choose |
| Workday Custom Reports | Use Workday as your system of record for employees. Users are periodically imported into OneLogin via Workday's | Choose |
| UltiPro | Use UltiPro as your system of record for employees. Users are periodically imported into OneLogin. | Choose |

多種因子驗證 (身分鑑別)

The image shows a screenshot of the OneLogin console interface. The top navigation bar includes 'Users', 'Applications', 'Devices', 'Authentication', 'Activity', 'Security', 'Settings', 'Developers', and 'Modules'. The main content area is titled 'Authentication Factors / Select a Strong Authentication Factor'. It lists several authentication factors:

- OneLogin Protect**: OneLogin, Inc. Free mobile solution that allows users to submit their one-time password by pressing a button. Available on iPhone and Android.
- WebAuthn**: OneLogin, Inc. WebAuthn allows users to register and authenticate using an 'authenticator' such as a fingerprint, face scan and USB key.
- OneLogin Email**: OneLogin, Inc. OneLogin sends a challenge question to the user's email address.
- WebAuthn_02**: Authenticator is a software based two-step authentication token developed by Google, and used by Microsoft as well.
- WebAuthn_01**: Authenticator is a software based two-step authentication token developed by Google, and used by Microsoft as well.

A Windows security dialog box is overlaid on the right side of the console, titled 'Windows 安全性' and '繼續設定'. It contains the text '請將安全性金鑰插入 USB 連接埠。' (Please insert the security key into the USB port.) and a '取消' (Cancel) button. Below the dialog box, a photograph shows a YubiKey USB security key plugged into a laptop's USB port next to a keyboard.

PKI Cert 裝置綁定 (設備鑑別)

onelogin Users Applications Devices Authentication Activity Security Settings

Devices

Search [] Search All Models/OS Any Status

| OS | Device | OS Version | Endpoint Client |
|----|---------------------|------------|-----------------|
| | Downloaded PKI cert | N/A | PKI cert |

Device
Identifier: a6c9[]7f7636f2
Certificate Fingerprint:
PmBKyBqVops[]bWD45IP0j2kB4gPE59RI[]

PKI cert
First Installed: 6 minutes ago
Status: **Managed**

Managed: User has authenticated Desktop.

< Previous 1 Next >

選擇驗證憑證
網站 pki-us.onelogin.com:443 需要您的認證:

pong []OneLoginDeviceTrust
OneLogin Inc Intermediate CA
2024/4/23

憑證資訊 確定 取消

onelogin

使用者登入的風險分數 (信任推斷)

The screenshot shows the OneLogin interface. At the top, there is a navigation bar with the OneLogin logo and menu items: Users, Applications, Devices, Authentication, Activity, Security, and Settings. Below the navigation bar is the 'Events' section. It features a search bar for users, a dropdown for event types (currently set to '-- any event --'), and a dropdown for event filters (currently set to 'all events'). A table lists several events, with the 'Risk Score' column highlighted by a red box. The events and their risk scores are:

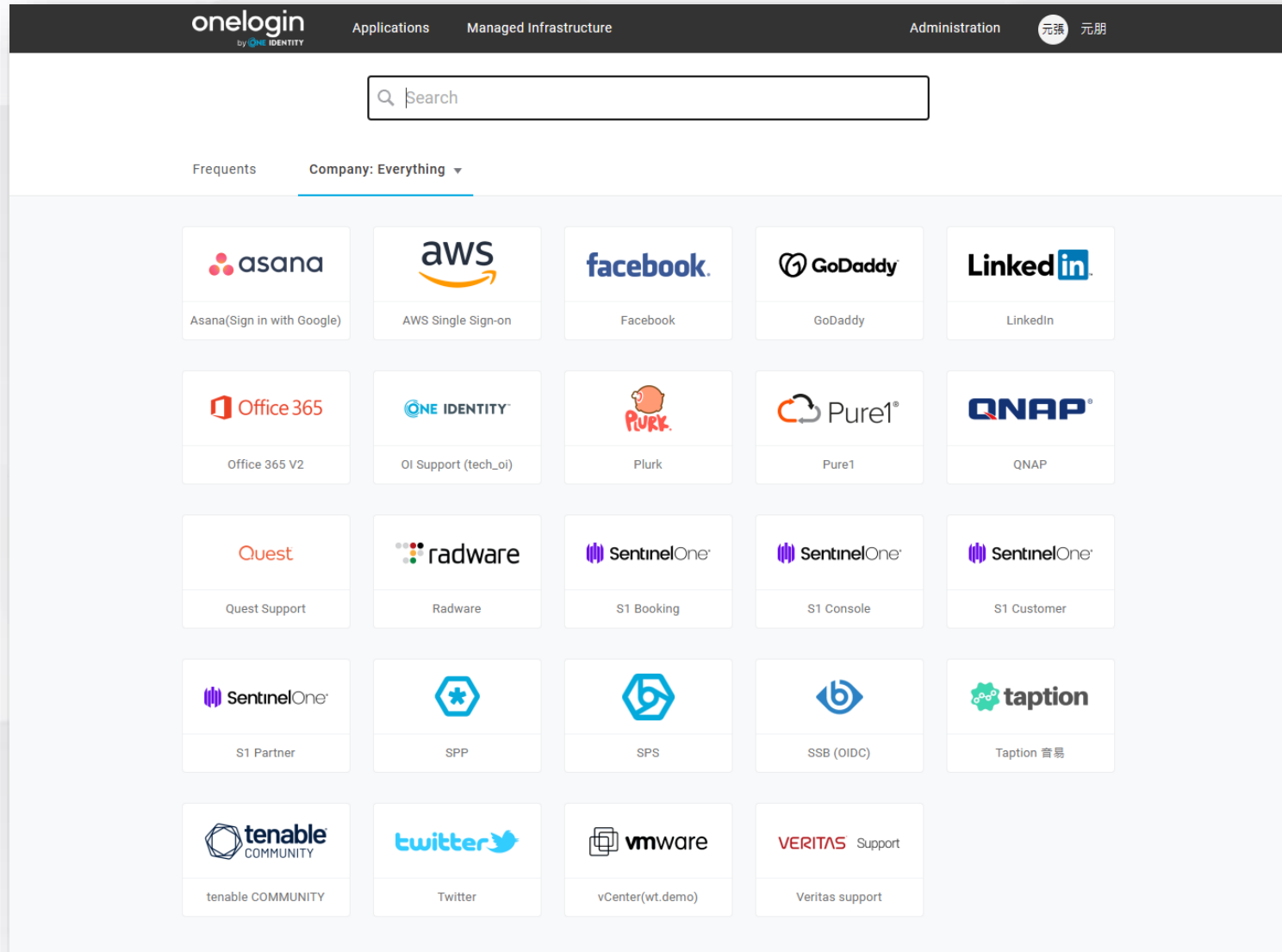
| Description | Risk Score |
|----------------------|------------|
| logged into OneLogin | 41 |
| challenged for OTP | 41 |
| logged into OneLogin | 36 |
| challenged for OTP | 36 |
| logged into OneLogin | 26 |
| logged into OneLogin | 28 |
| logged into OneLogin | 35 |

To the right of the table is a detailed view of a specific event titled 'logged into OneLogin'. This view includes the following information:

- Performed by:** [User Avatar]
- IP address:** 1. [Redacted].123.5
- When:** 12 days ago (13-Apr 00:02)
- User:** [User Avatar]
- Risk Score:** Risk: (26/100)
- Risk Level:** Smart Access:Low / Smart MFA:Medium
- Risk Reasons:**
 - Accessed from a new browser session
 - 16:02 (UTC/GMT) is an unusual time of day
 - Infrequent access from 1. [Redacted].123.5
 - Low trust for session
- Policy:** MFA User Policy (Pong)
- Notes:**
 - Authentication method: Login App.
 - Transitions: username -> password
 - Correlation_id: 93c66b53- [Redacted]-84bd-231178869da7

A 'Cancel' button is located at the bottom right of the detailed view.

單一介面多服務整合 (Single Sign-On)



登入流程展示



用戶名稱

pongchang@weicloud.com.tw

記住我的使用者名稱

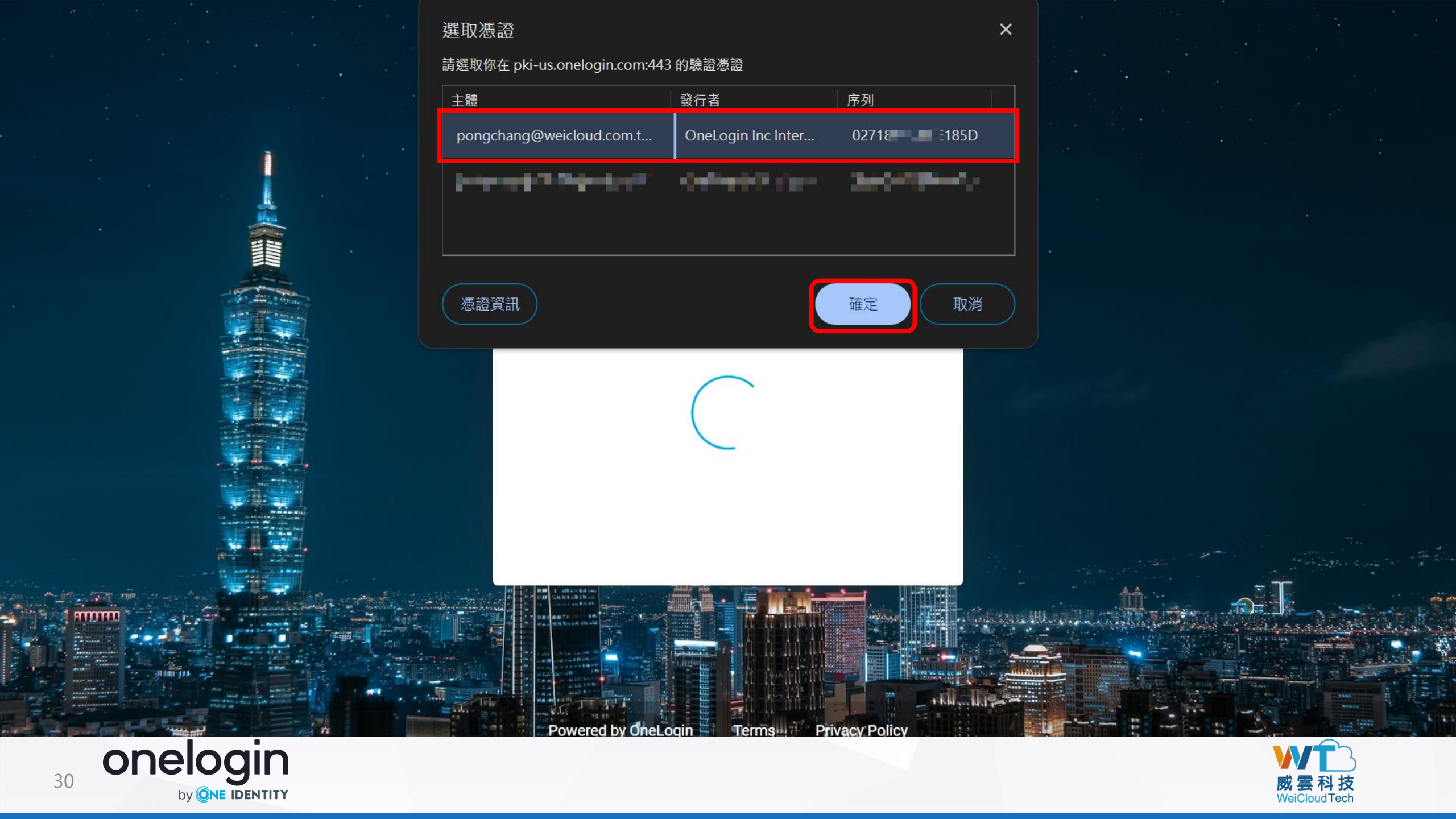
繼續

[忘記密碼](#)

Powered by OneLogin

[Terms](#)

[Privacy Policy](#)

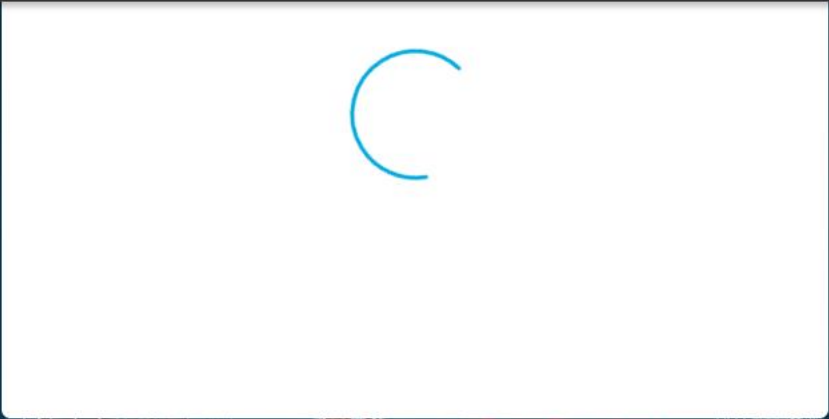


選取憑證 ✕

請選取你在 pki-us.onelogin.com:443 的驗證憑證

| 主體 | 發行者 | 序列 |
|-----------------------------|-----------------------|---------------|
| pongchang@weicloud.com.t... | OneLogin Inc Inter... | 02718...E185D |
| [blurred] | [blurred] | [blurred] |

憑證資訊 確定 取消





選擇認證因素

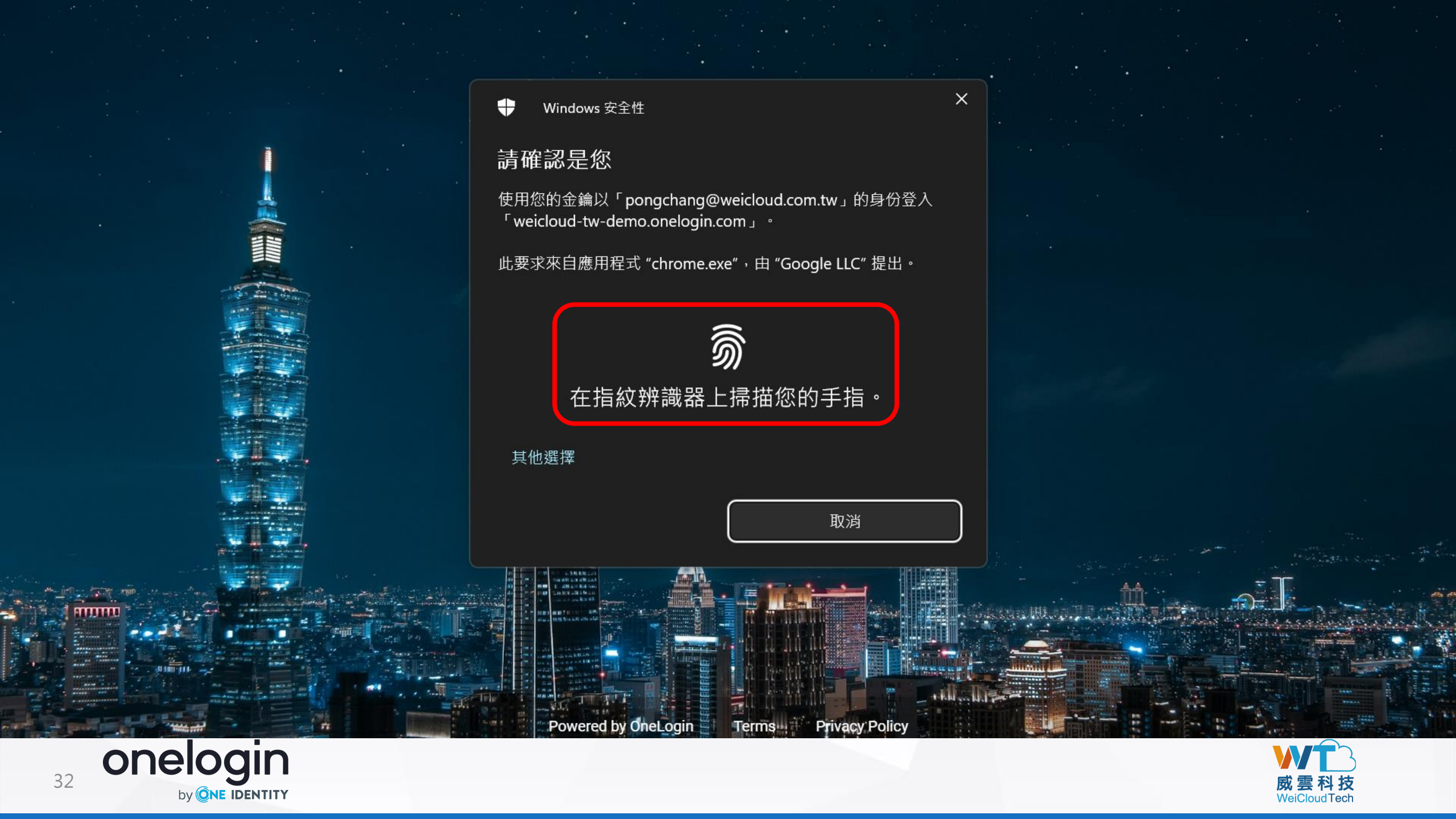
 OneLogin Protect

 OneLogin Email

 WebAuthn_02

 WebAuthn_01

Powered by OneLogin | [Terms](#) | [Privacy Policy](#)



Windows 安全性



請確認是您

使用您的金鑰以「pongchang@weicloud.com.tw」的身份登入
「weicloud-tw-demo.onelogin.com」。

此要求來自應用程式“chrome.exe”，由“Google LLC”提出。



在指紋辨識器上掃描您的手指。

其他選擇

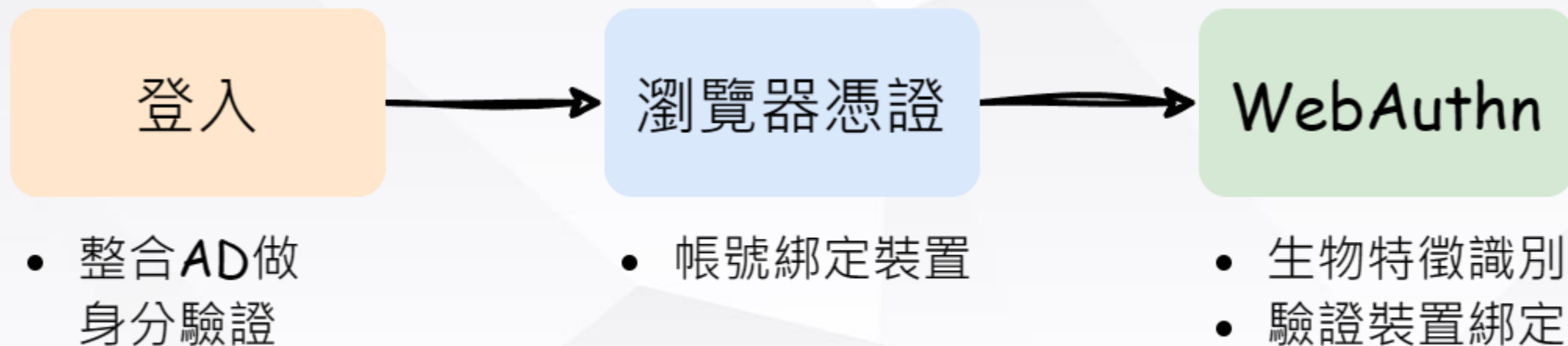
取消

Powered by OneLogin

[Terms](#)

[Privacy Policy](#)




















登入驗證流程



Search

Frequents

Company: Weicloud TW Demo Account

| | | | | |
|---|--|--|---|---|
|  AWS Single Sign-on |  GoDaddy |  Office 365 V2 |  OI Support (tech_oi) |  Plurk |
|  Pure1 |  QNAP |  Quest Support |  Radware |  S1 Booking |
|  S1 Console |  S1 Customer |  S1 Partner |  SPP |  SPS |
|  SSB (OIDC) |  Taption 音易 |  tenable COMMUNITY |  vCenter(wt.demo) | |

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