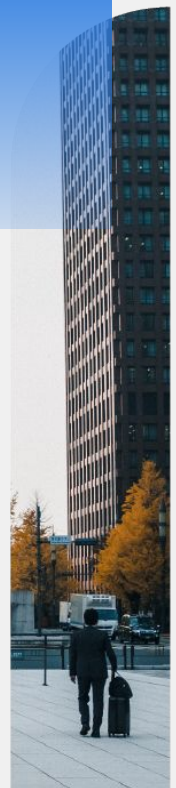
身分識別與網路存取管理

IDENTITY AND ACCESS MANAGEMENT (IAM)

FortiAuthenticator / FortiToken

張益盛-Marty Chang
Technical
Consultant
mchang@fortinet.com

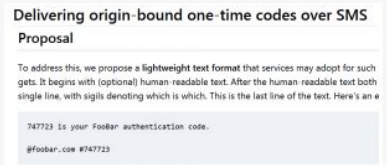


密碼災難 ...

iThome 新聞 產品&技術 專題

IT EXPLAINED 全新企劃 Webinar

網釣



雙因素驗證 | 動態密碼 | 2FA | 一次性密碼 | OTP | OTP簡訊 | 網釣 | 資安 | 身分驗證 | 身分認證

蘋果提出OTP簡訊格式草案，獲Google支持

為了提高以簡訊傳送動態密碼的安全性，蘋果提出改良版一次性密碼（OTP）簡訊格式，以避免使用者遭遇網釣攻擊

2020-02-04

資安 | 伊朗 | 網軍 | 網路攻擊 | 關鍵基礎設施 | 網釣 | 工控

美國土安全部警告企業，伊朗可能發動網路攻擊

因美國在中東發動空襲炸死伊朗重要軍事將領，美方對內發出警告，留意伊朗網軍針對關鍵基礎設施業者以及各類組織發動

iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 科技防疫情

IT EXPLAINED 全新企劃 Webinar 搶先體驗AWS年度雲端峰會 ModernWeb' 21

新聞

國發基金系統遭中國駭客

國發基金執行秘書蘇來守表示，遭駭創業投資電腦系統於6月28
備份，沒有企業營運機敏資料；經數位鑑識發現3個惡意程式和
階段，沒有發現資料竄改、外洩的跡象

文/ 黃彥棻 | 2021-07-23 發表

行政院國家發展基金管理會 關於本會 主

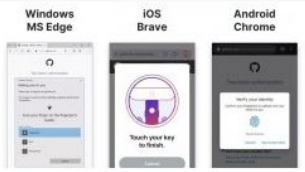
假冒國泰世華網路銀行傳簡訊盜

刑事局今天表示，有民眾接獲「假冒國
等字詞，經統計，3天內21人帳戶遭盜
求證。

警政署刑事警察局透過新聞資料指出
「假冒國泰世華網路銀行」詐騙簡訊，
騙簡訊內的連結網址，恐被盜領。

刑事局表示，詐騙簡訊內容為「您的銀
則帳戶會被凍結無法使用」，若被害人
網路銀行。

雙因素驗證



GitHub | WebAuthn | 雙因素驗證

GitHub使用者現可在更多平臺使用實體安全金鑰，作為第二身份驗證因素

GitHub服務擴大實體安全金鑰支援，在Windows、macOS和Linux上的Firefox和Chrome瀏覽器都能使用

2019-08-22

Android手機 | 雙因素驗證 | iPhone | 2FA | 2SV

Android的2FA金鑰功能延伸到iOS裝置

Android 7以上手機也可用來驗證用戶在iPhone、iPad上的Google帳號登入，只要使用者同時擁有Android手機和

2019-06-13

雙因素驗證 | 2FA | 安全金鑰 | google | 身分驗證

Google將讓Android 7以上手機當2FA安全金鑰

搭載Android 7.0以上系統的手機，在更新後都將可當成FIDO 2/WebAuthn標準的安全金鑰，不再需要額外購買硬體金鑰

2019-04-11

臉書 | 雙因素驗證 | 2FA | 個資

臉書2fA手機號碼可能讓用戶被任何人搜出來，而且關不掉

繼去年被發現將用戶在雙因素驗證頁面（2fA）輸入的電話號碼，提供給外部廣告主之後，又有研究人員揭發臉書用戶在

釣魚郵件 | 駭客 | 2FA | 雙因素驗證 | Gmail | Yahoo

中東、北非人權人士也遭駭客網釣信件鎖定，連雙因素驗證機制也被突破

駭客用兩種方法繞過驗證，第一種是偷App密碼。某些信箱服務提供app密碼，

釣魚郵件 | 雙因素驗證 | 2FA

伊朗駭客假冒Gmail和Yahoo Mail遭駭通知信來發送釣魚郵件，專門鎖定記者、社運人士和官員

釣魚信件會將受害者導向假的Gmail或Yahoo Mail網頁，要求用戶驗證帳號、

強化帳號密碼安全的必要性

iThome 新聞 產品&技術 專題 AI Cloud DevOps 資

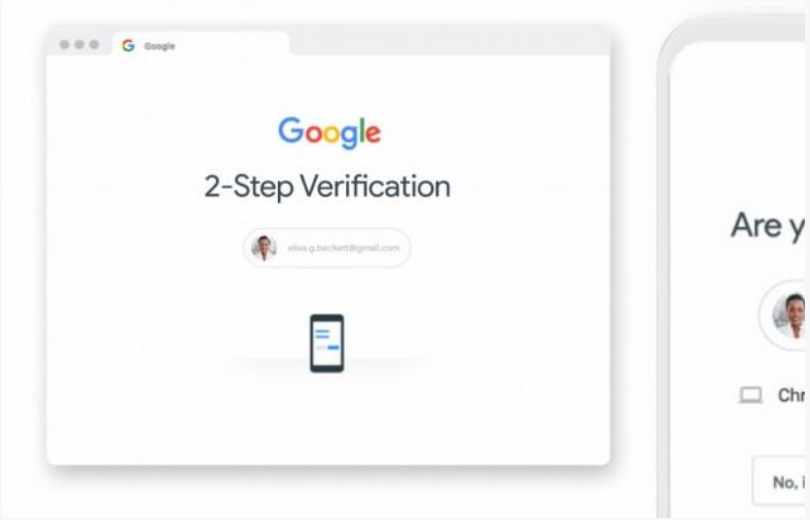
新聞

Google將強制用戶啟動帳號雙因

Google將全面要求所有用戶透過Authenticator App、Google Titan以及Google Sr
登入Google帳號的第二層驗證機制

文/ 林妍溱 | 2021-05-07 發表

讚 6.6 萬



雖然Google提供雙因素驗證（2
驟驗證（two-step verification，
但目前仍允許用戶自行選擇，不
Google帳號用戶啟用2SV。

Google身份與用戶安全產品管理

iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 科技防疫情報站 搜尋

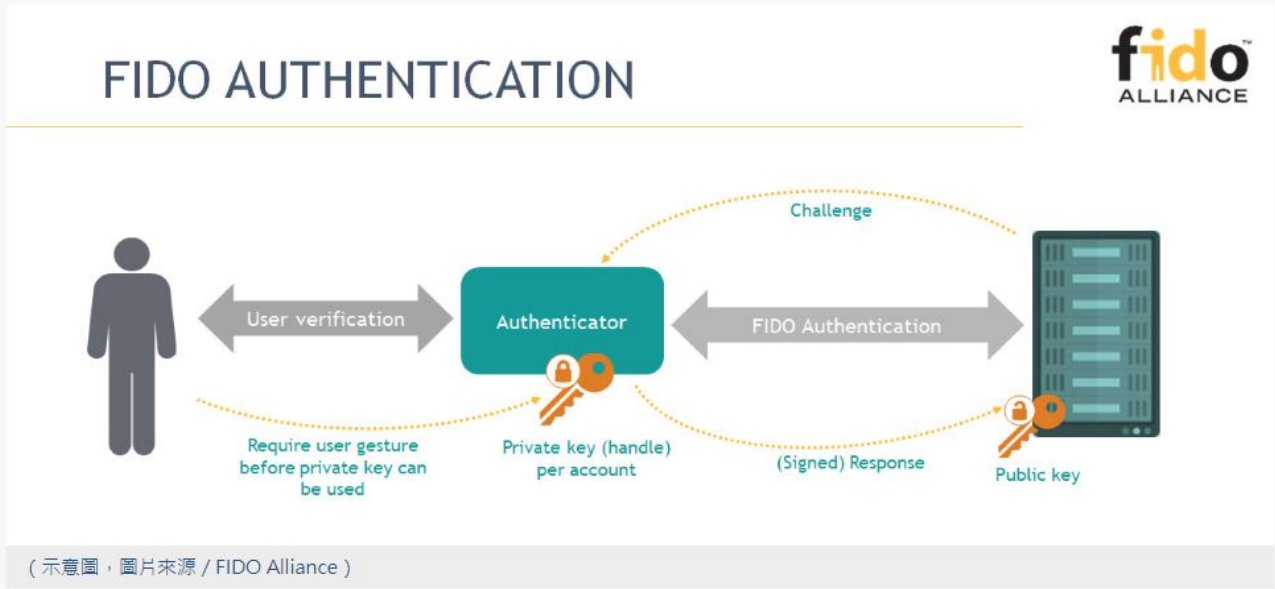
新聞

金融FIDO今年Q4啟動試辦，先從銀行業跨機構身分識別開始

金融行動身分識別標準化機制（金融FIDO）在今年Q4要啟動試辦，將採取集中式開發手機身分識別App，導入FIDO標準，綁定實體卡片，以提供跨機構身分識別功能。金管會也表示，要採用哪種實體卡片如自然人憑證、晶片金融卡等來開通金融FIDO，則還在討論中。

文/ 李靜宜 | 2021-06-15 發表

讚 6.6 萬 按讚加入iThome粉絲團 讚 180 分享



（示意圖，圖片來源 / FIDO Alliance）

去年8月，金管會所發布的金融科技發展路徑圖中，有一大重點是要研究發展金融行動身分識別標準化機制（簡稱金融FIDO）。金管會在今天（6/15）宣布金融FIDO最新進展。

存取權限管理不當引發企業機密外洩風險

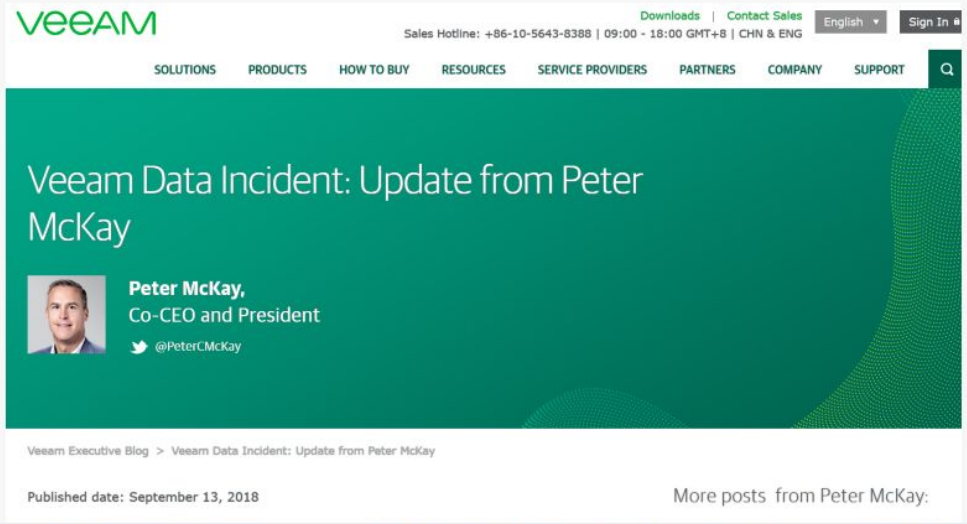
iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 科技防疫情報站

【機敏資料不當存取權限指派已成為企業雲上的未爆彈 存不設防，成重大資訊治理隱憂

近期研究人員不斷發現多起雲端曝露企業重要資料情事，導致任何人都能隨意存取，而造成的原因，竟多半來自於員工無心將企業機密檔案存放在雲端公開資料夾

文/ 周峻佑 | 2018-11-23 發表

讚 6.6 萬 按讚加入iThome粉絲團 讚 126 分享



專門開發備份、災難復原與智慧資料管理軟體的Veeam在9月傳出重大資料外洩事件，遭人揭露其放置在AWS的MongoDB資料庫因配置錯誤，而讓200GB的客戶資料暴露在外。

以往提及資料外洩的防範，多半不是從內部竊取，就是駭客由外部發動攻擊的角度探討。而這兩種型態的事件，都是屬於帶有特定意圖的攻擊為出發點，像是可能因同業挖角等原因，即將離職的員工，從而竊取公司的重要機密。

3C科技 影音專區 智慧手機 實用秘技 電腦應用 網路社群 好攝相機 家電娛樂 科技趣

HP 調查顯示：存取權限管理不當引發企業機密外洩風險

2011/12/19 19:23
HP

HP 調查顯示: 存取權限管理不當引發企業機密外洩風險

安全智能科技解決方案有效輔助資安政策的執行

HP 日前發布一項新的全球調查報告指出，由於企業對於資料庫管理者、網路工程師及 IT 資安人員等特殊權限使用者的監管不甚周延，導致企業機密資料外洩風險持續增加(１)。

由 Ponemon Institute 組織所進行的「不安全的特殊權限使用者」的研究中，幾項主要重點如下:

- 52 %受訪者表示，特殊權限使用者可以取得高於本身權限許可的機密資料。
- 60 %受訪者表示，特殊權限使用者經常很容易取得與其工作職掌無關的機密資料。
- 顧客個資與企業業務資料所面臨的安全風險最高，特別是相關應用軟體存取企業內部系統、行動通訊、社群網路..等系統時。

許多受訪者表示，他們清楚了解進入公司特殊 IT 系統的權限規範。然而，仍有將近四成的受訪者表示，他們對於公司存取資訊權限的規定並非全盤了解，特別是不確定現行特殊權限使用者的行為是否合乎規範。

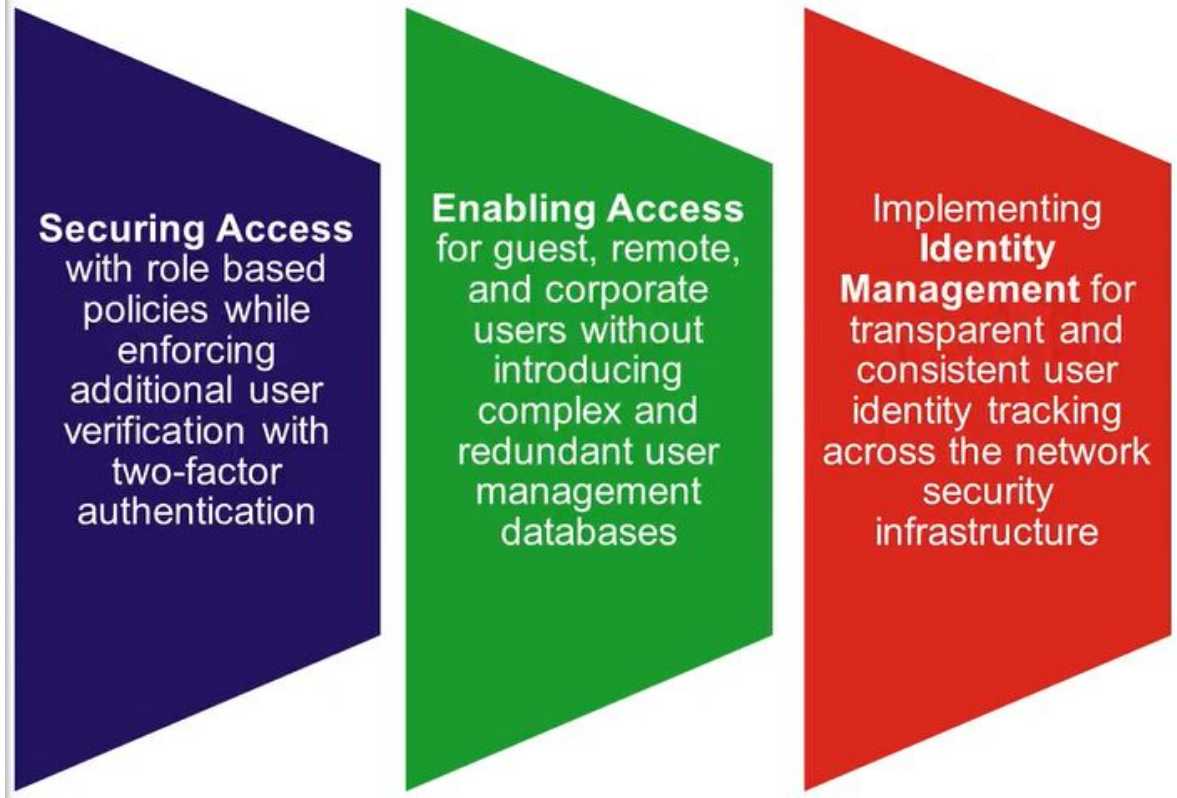
企業試圖以不同的方式掌控這樣的狀況， 27 %受訪者表示，公司現行以身分確認系統與存取控管方式，來管控資料管理系統的相關人員。 24 %受訪者表示同時公司也制定相關作業程序來管控資料。但仍有 15 %的受訪者認為公司對資料取得的權限掌控不佳，也有將近 11 %的受訪者認為取得資料的權限實際上無法被有效辨識。

如何維持企業的運作?

企業成長 -- 業務力

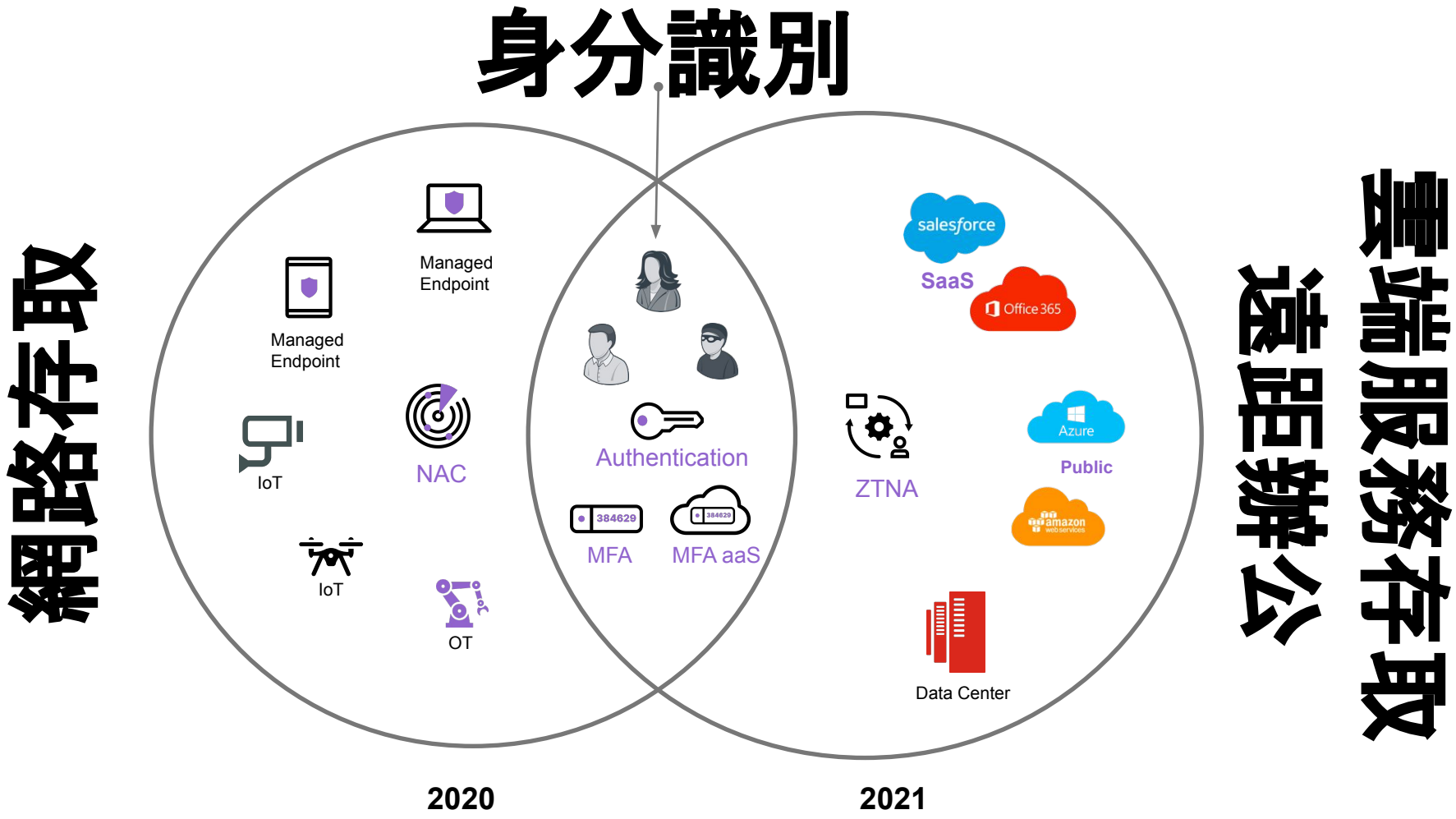
企業資產 -- 人力資源、硬體

企業命脈 -- 資料可以幫助我們深入洞悉市場、快速精準地找出應對策略，甚至為企業帶來更大商業價值的創新驅動力。



零信任的存取

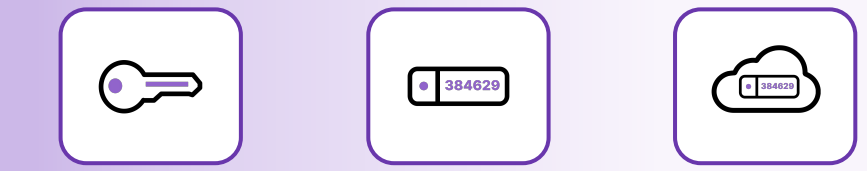
- Convergence of networking and security across all edges and users

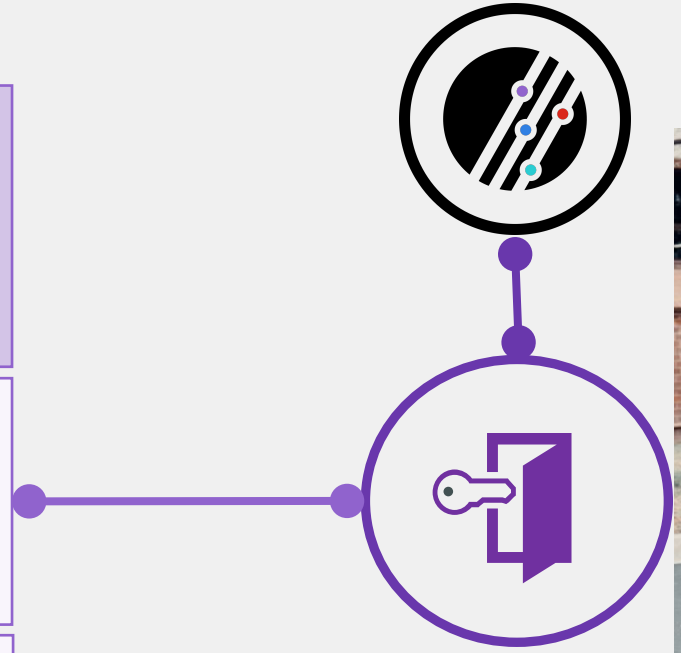


Fortinet身分識別與網路存取管理(IAM)

確保使用者在任何地方都是一致的存取權限

集中式的管理系統,省去跨不同
系統身分驗證時的困難度與繁雜度

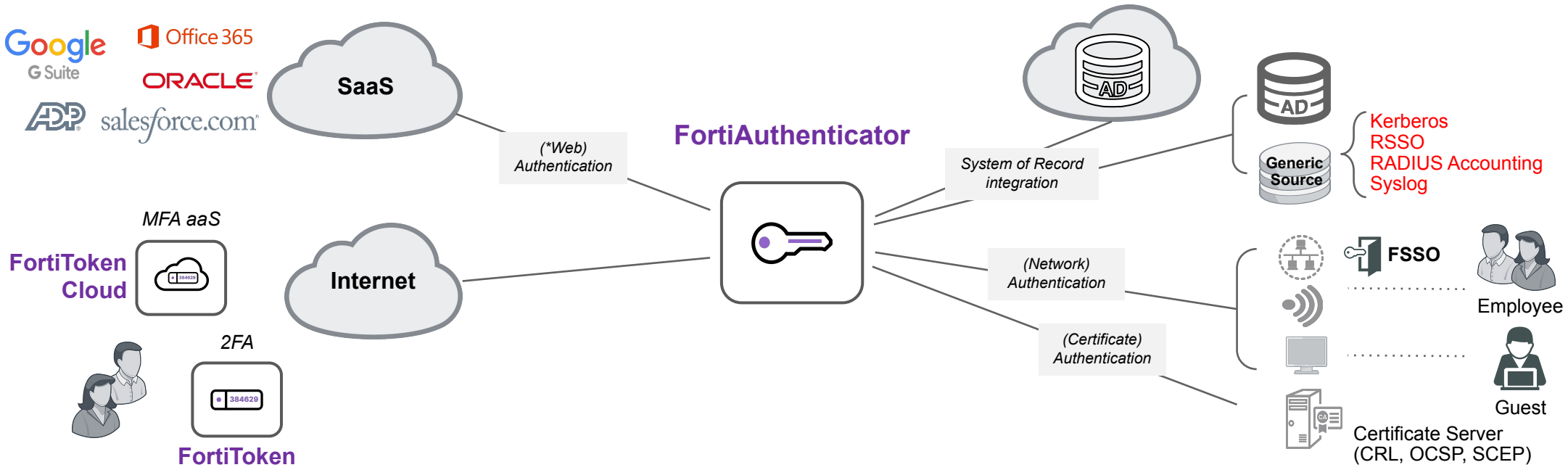




Forti保全

- 存取權限一致
- 多樣化的密碼保護機制、雙因子驗證
- 方便的單一登入系統、免除多次登入的手續、訪客自我註冊系統

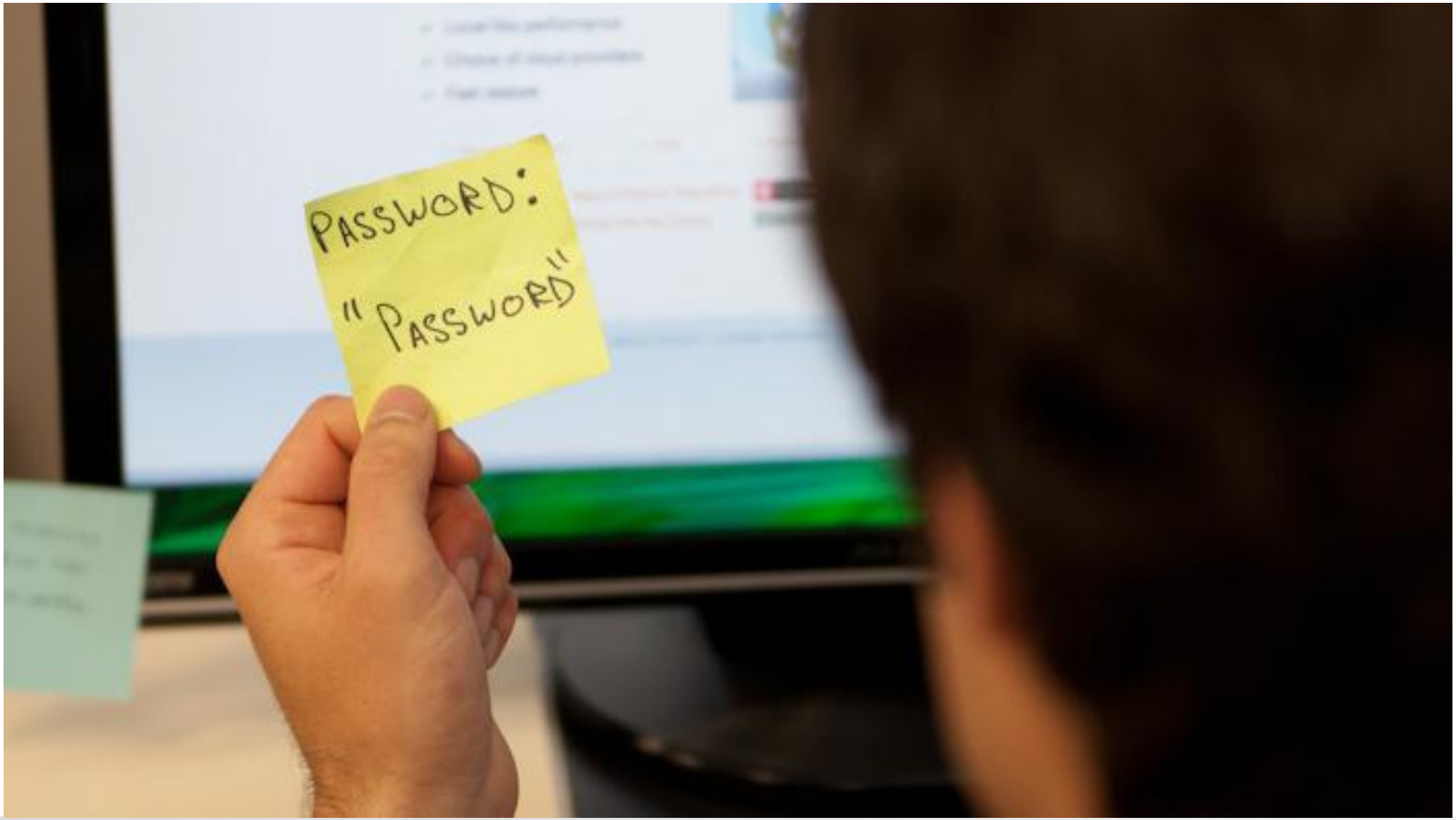
集中管理、安全存取



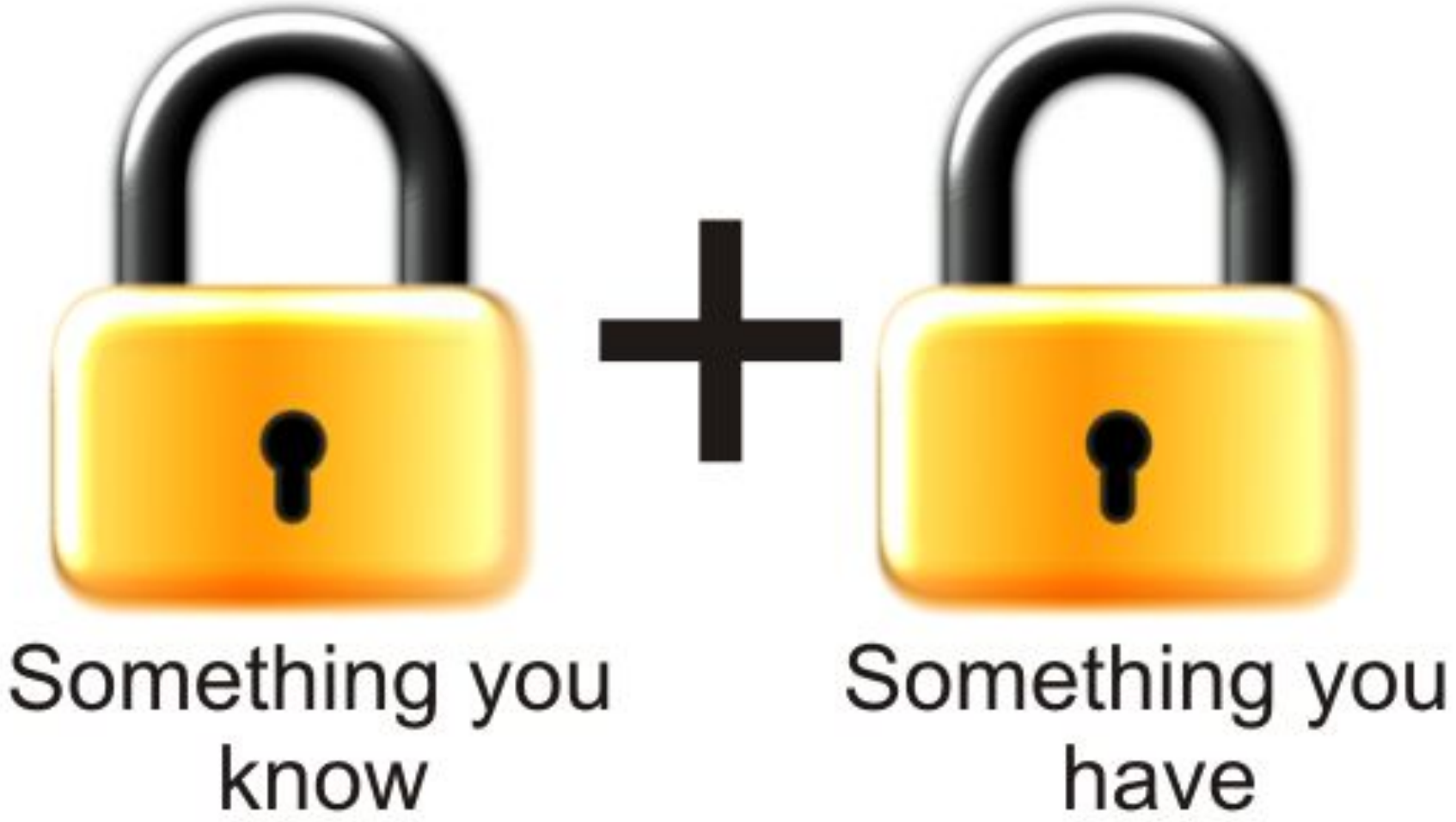
帳號密碼強化	權限控管	單一登入
Establish identity through user log-in, adaptive, certificate, and/or multifactor input	Provide information from authentication source for use in privileged access	Improve security with improved user experience, i.e. reduce user login fatigue

*(Web) Authentication: SAML2, oAUTH2, OIDC, RestAPI

用戶的密碼強度.....？



何謂 雙因子認證（Two factor Authentication）



FortiToken Current Portfolio

FortiToken Mobile

Multi platform OATH OTP application with push notification of login attempts and one tap approval

FortiToken 300

Driverless USB Device
FIPS-140 compliant
Economical PKI authentication

FortiToken 220

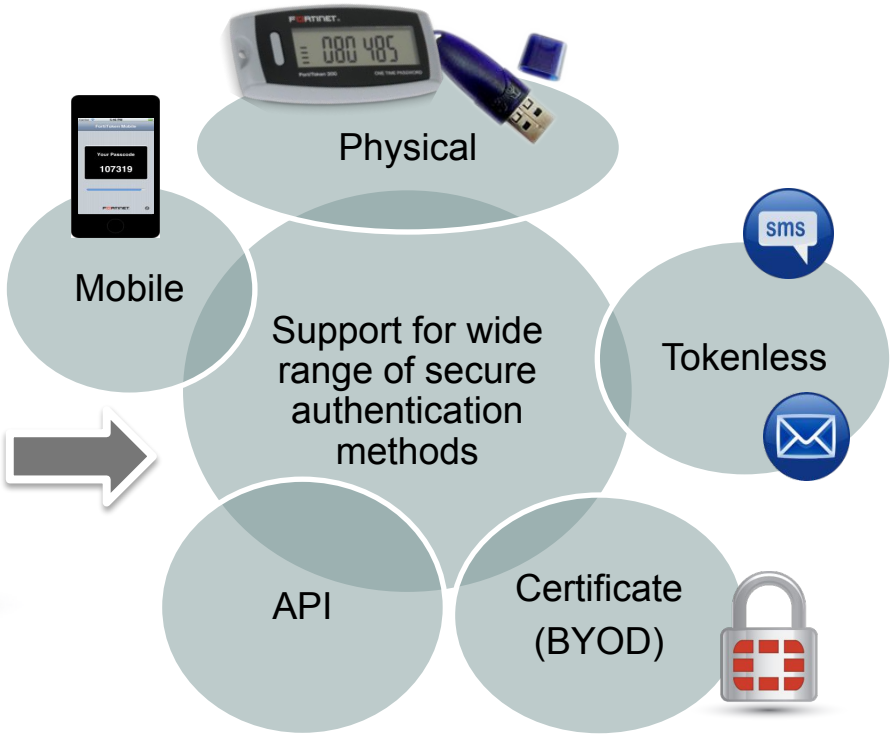
The FortiToken 220 OTP token is a mini credit card form factor token. There is also a companion tool for Android devices on Google Play that allows users to reprogram the token seed*.

FortiToken 200/200CD

Durable, large display, OATH OTP token with FortiGuard activation or optional encrypted activation file.

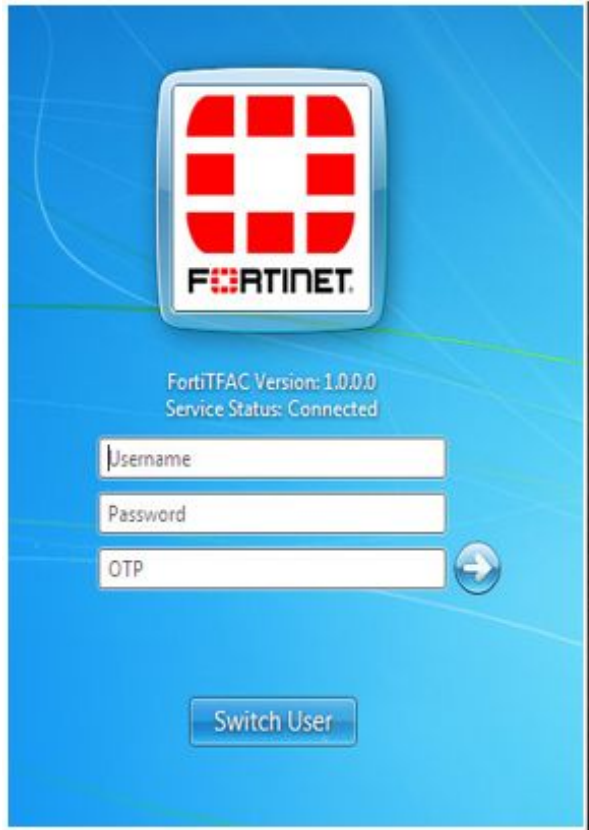
雙因子認證應用介紹

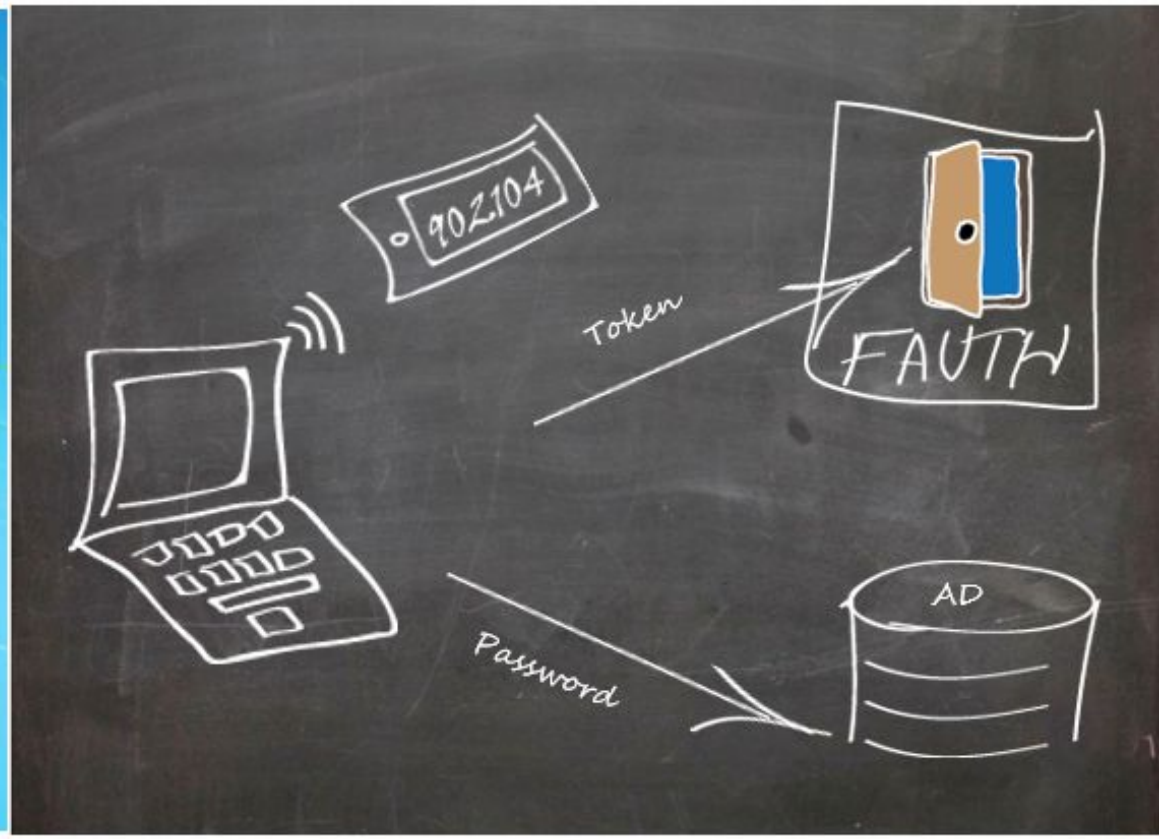
- 多樣化的 token 種類，適應不同的應用需求
  - 相容 OATH 協定 TOTP (time) based tokens (FTK200)
  - USB certificate tokens (FTK300)
  - 適用 Android, iOS and Windows Mobile的 FortiToken Mobile
  - SMS 與 Email 動態密碼.
- 應用範圍
  - Windows/Linux 伺服器或個人電腦的登入
  - 任何可以透過Radius 通訊協定做身分驗證的設備
  - Fortinet設備的管理登入驗證
  - VPN連線的使用者登入驗證



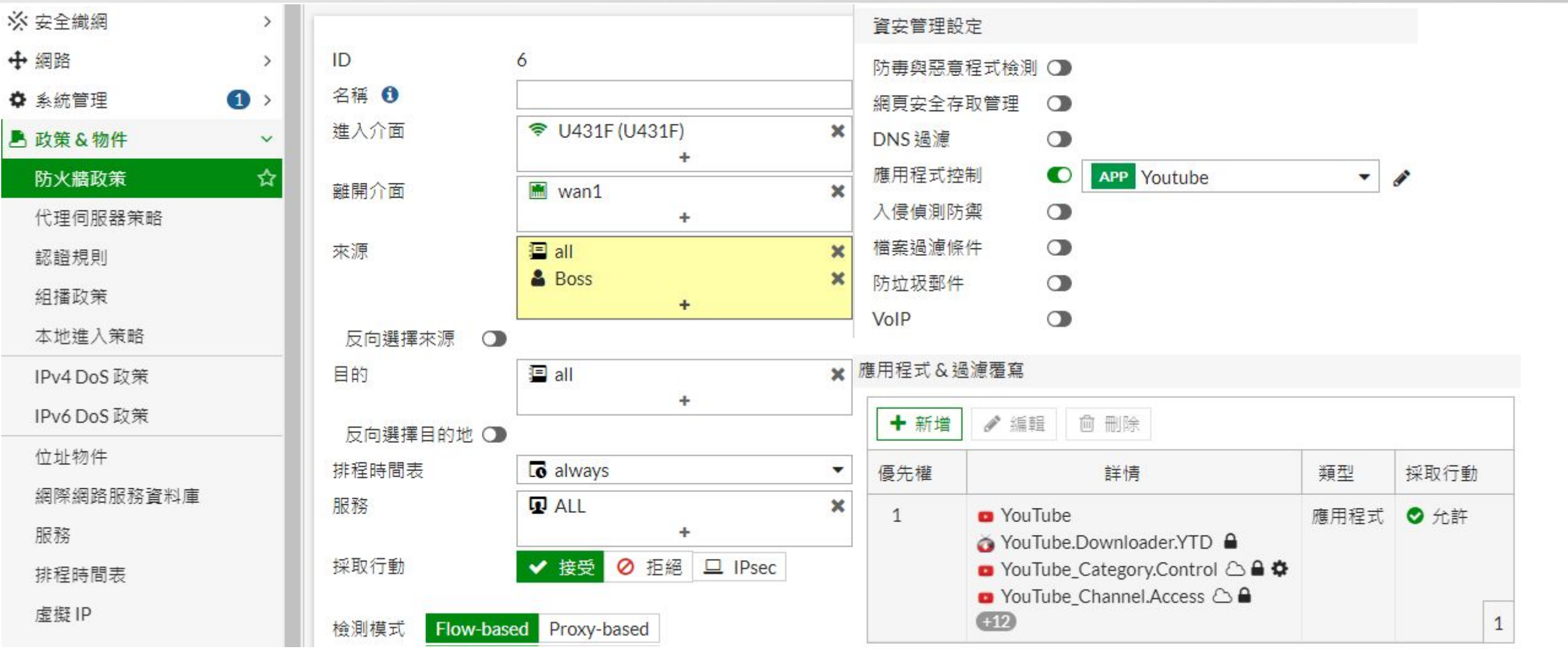
強化微軟作業系統的身分驗證

- 強化作業系統登入使用雙因子驗證
  - » Credential Provider Plugin Installed in the Client PC
  - » Split Authentication Process:
    - Token Authentication to the FAC
    - Password Authentication to DC
    - Protects PC from brute forcing
    - Utilizes SSL API rather than RADIUS





使用者權限控管

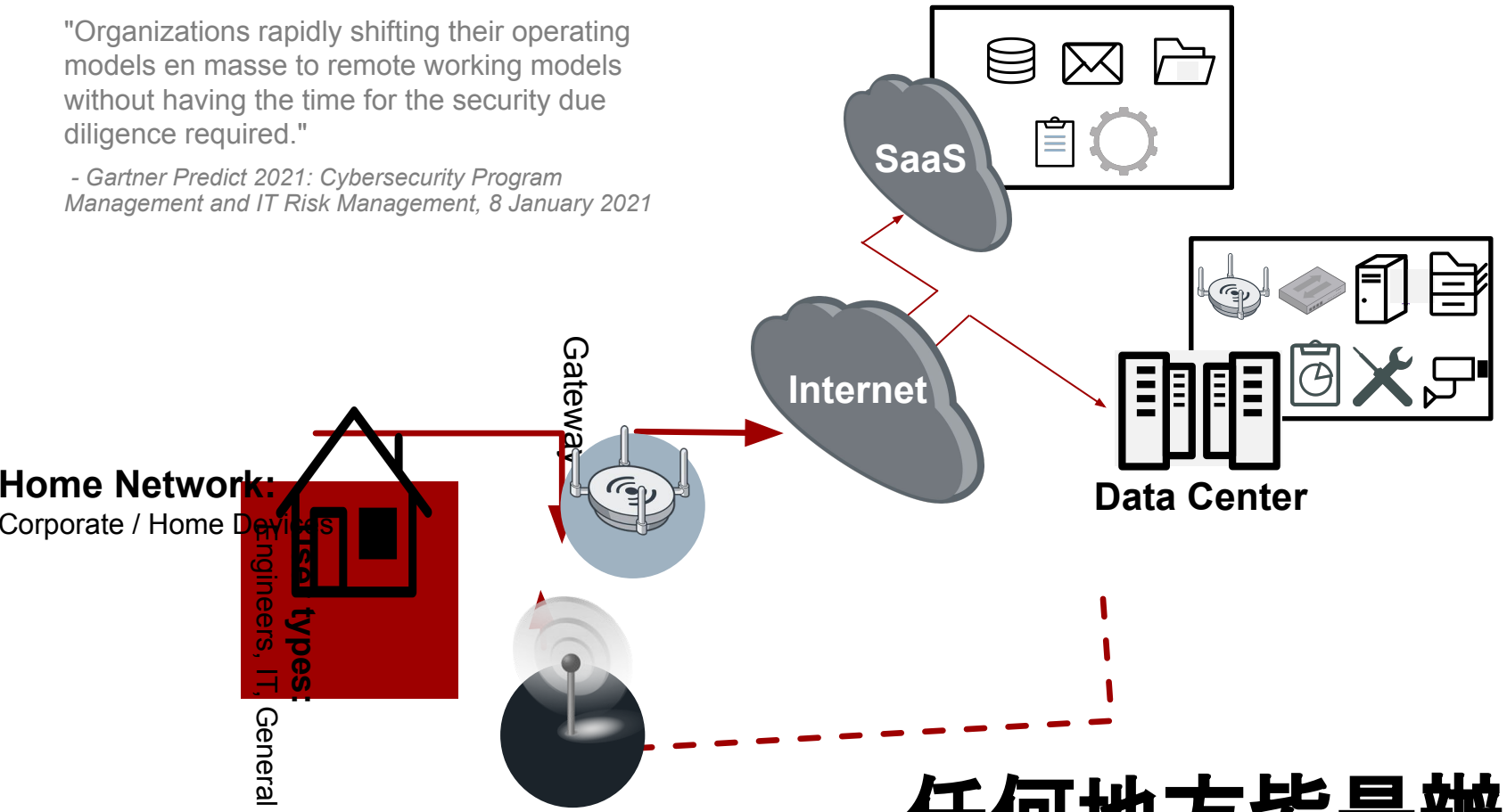

安全織網
網路
系統管理 1
政策 & 物件
防火牆政策
代理伺服器策略
認證規則
組播政策
本地進入策略
IPv4 DoS 政策
IPv6 DoS 政策
位址物件
網際網路服務資料庫
服務
排程時間表
虛擬 IP
ID 6
名稱
進入介面 U431F (U431F)
離開介面 wan1
來源 all Boss
反向選擇來源
目的 all
反向選擇目的地
排程時間表 always
服務 ALL
採取行動 接受 拒絕 IPsec
檢測模式 Flow-based Proxy-based
資安管理設定
防毒與惡意程式檢測
網頁安全存取管理
DNS 過濾
應用程式控制 APP Youtube
入侵偵測防禦
檔案過濾條件
防垃圾郵件
VoIP
應用程式 & 過濾覆寫
新增 編輯 刪除
優先權 詳情 類型 採取行動
1 YouTube YouTube.Downloader.YTD YouTube_Category.Control YouTube_Channel.Access +12 應用程式 允許
1

使用情境 – 遠距辦公

IAM will continue to become even more important, fostering growth for the organizations

"Organizations rapidly shifting their operating models en masse to remote working models without having the time for the security due diligence required."

- Gartner Predict 2021: Cybersecurity Program Management and IT Risk Management, 8 January 2021



雙因子認證—強化密碼安全

安全的連線加密—資料不外露

單一登入窗口—簡化登入手續

自我註冊機制—減低IT人員工作量

任何地方皆是辦公室

使用情境 – 單一登入加上雙因子驗證

標準化的單一登入機制

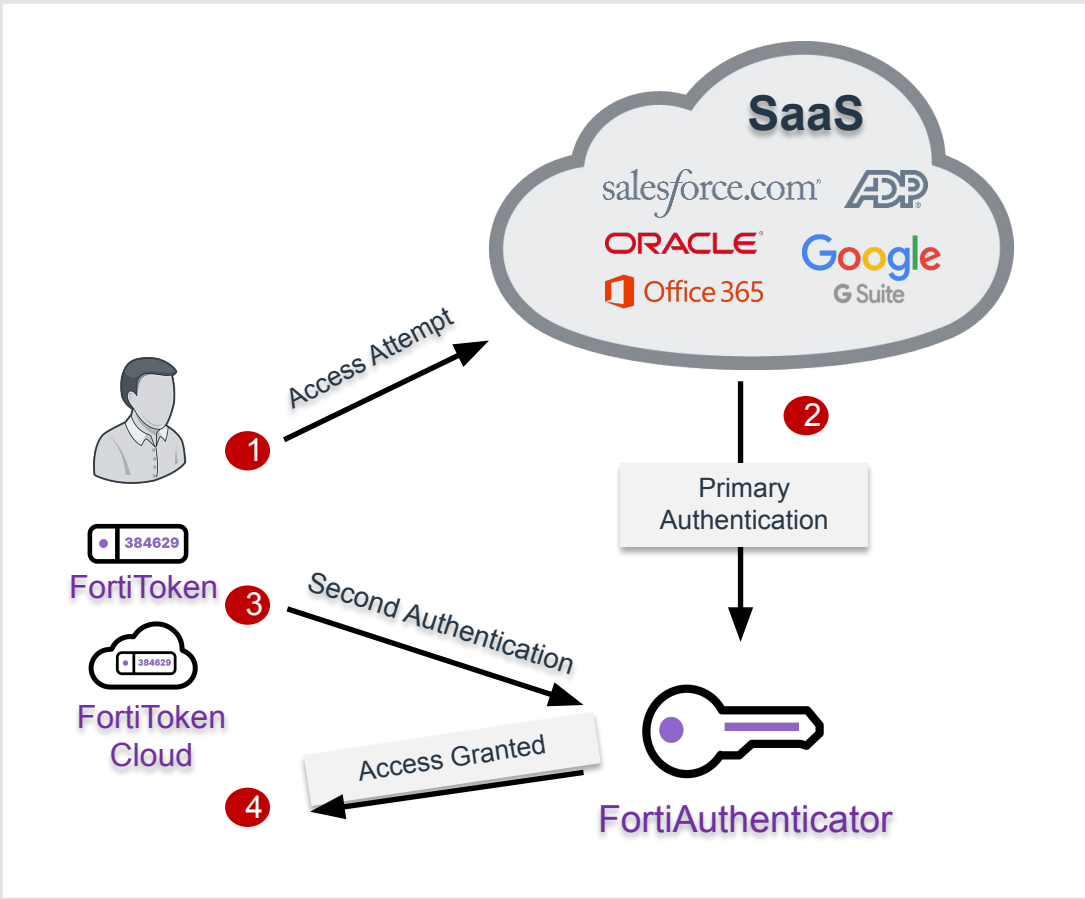
Provides Seamless Cloud Authentication.
Supports SAML 2.0 IdP-Initiated, SP-Initiated and IdP Proxy flows

提供使用者方便性

Users sign-in Once, No further Authentication required to use other cloud apps

增加安全性—降低密碼被竊的機率

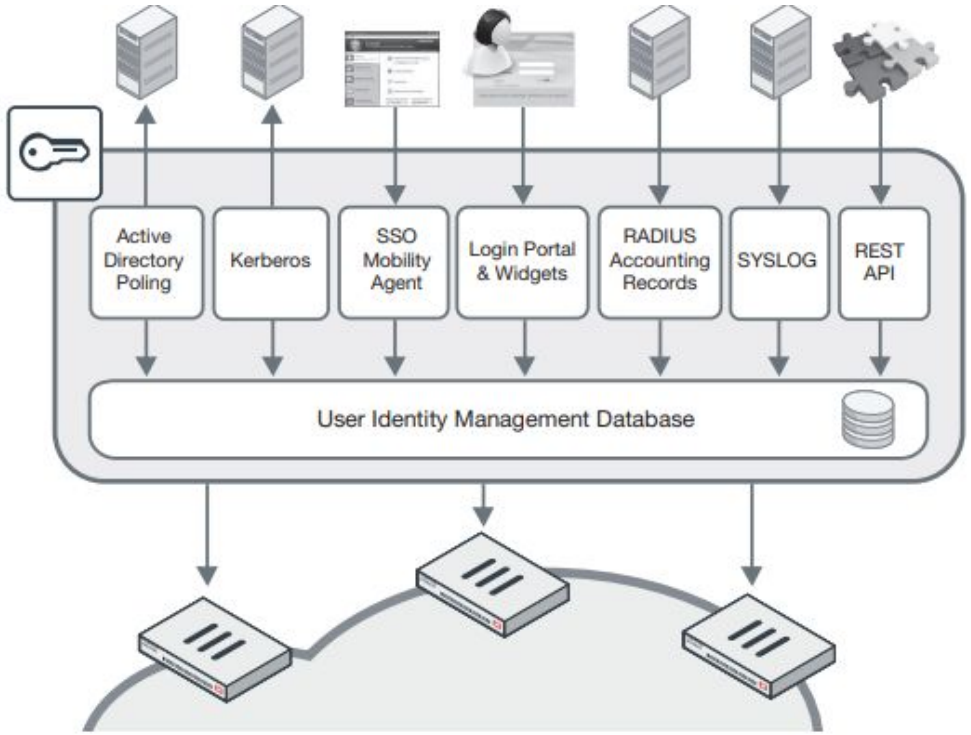
A single point of strong authentication, minimizing the overwhelming password syndrome



Fortinet身分識別與網路存取管理

FortiAuthenticator 具備以下特點

- 使用者身分的驗證以及使用者權限的控管
- 結合 FortiToken，強化密碼的安全性
- 單一登入功能,整合網路與不同系統服務的繁瑣登入步驟
- 提供有線與無線網路及 VPN 使用時的身分驗證與憑證管理
- 提供訪客管理功能，保障有線和無線網路的安全



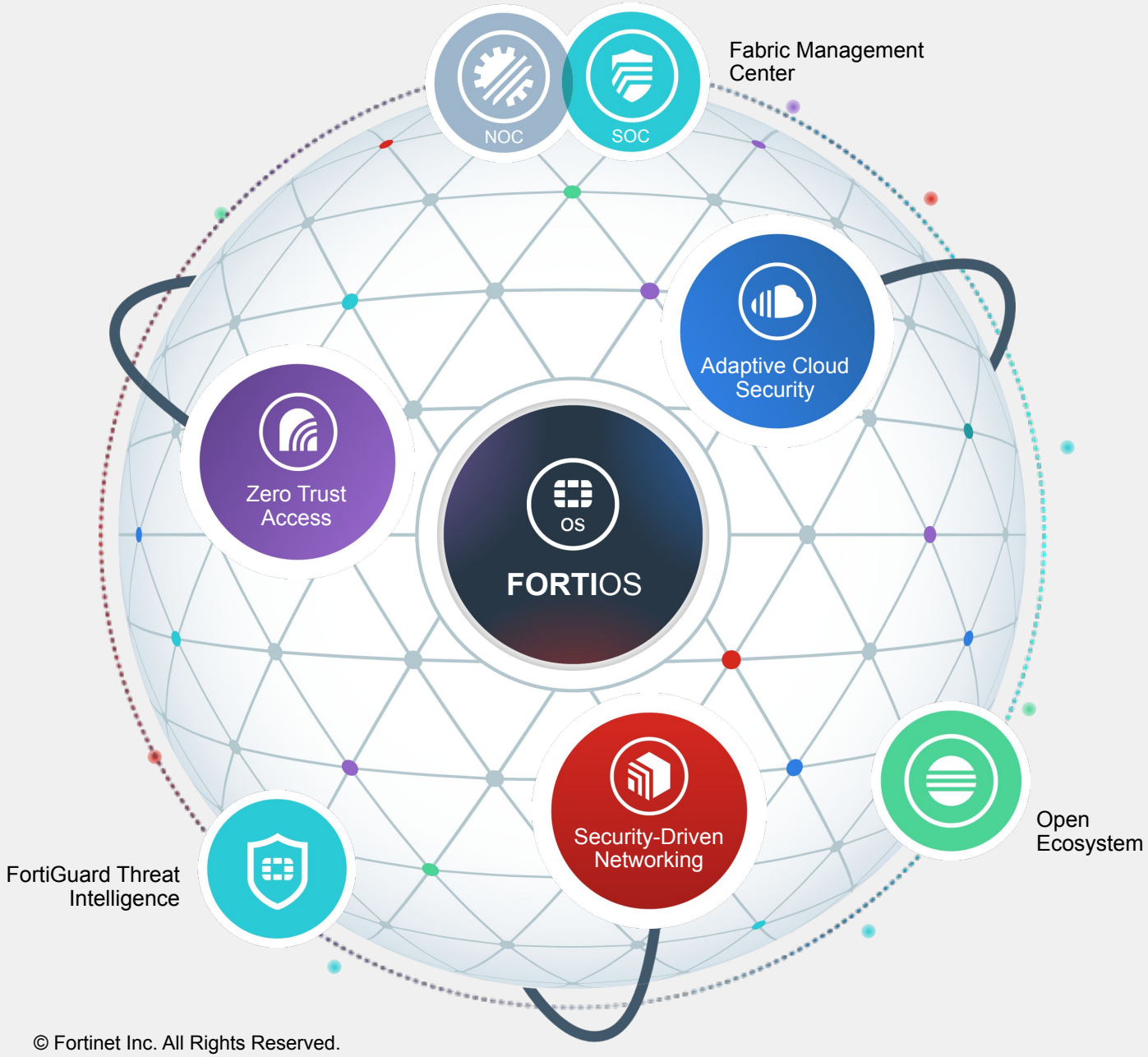

FORTINET

Fortinet
安全織網

廣度與深度
資訊可視性與資訊安全的全面化 ,有效保護公司運作的命脈

全面性整合
資安訊息共享,降低建置的複雜度,建立資安快打部隊

自動化佈署
透過AI –人工智慧達到全面防禦,提升防護力,築起堅不可破的防護牆



開放式的整合生態 – 單一身分識別

Technology Partners

PRE-VALIDATED. DOCUMENTED.

- *Fabric API integrations with FortiAuthenticator and FortiToken to comprehensively secure your attack surface*