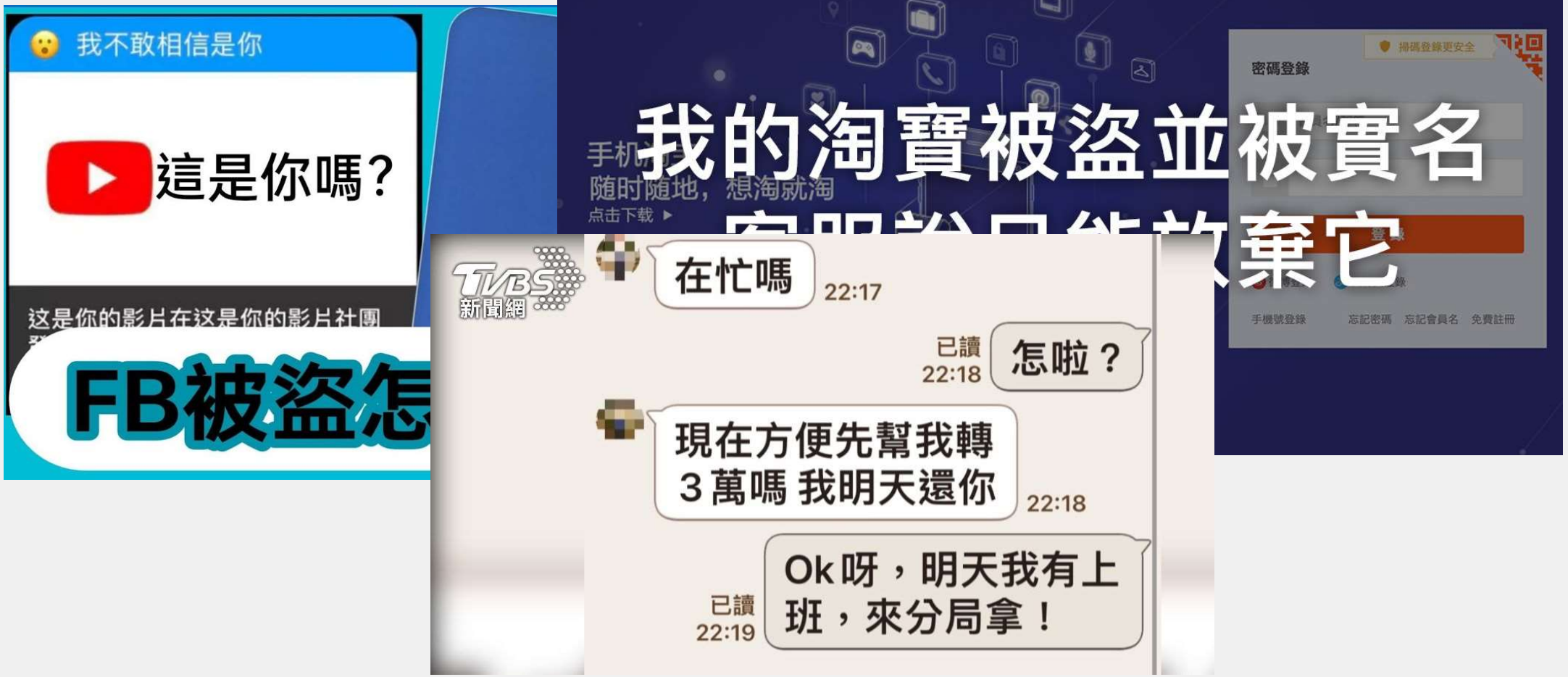
FORTINET

搞資安~
身分認證與特權管理落實了嗎？

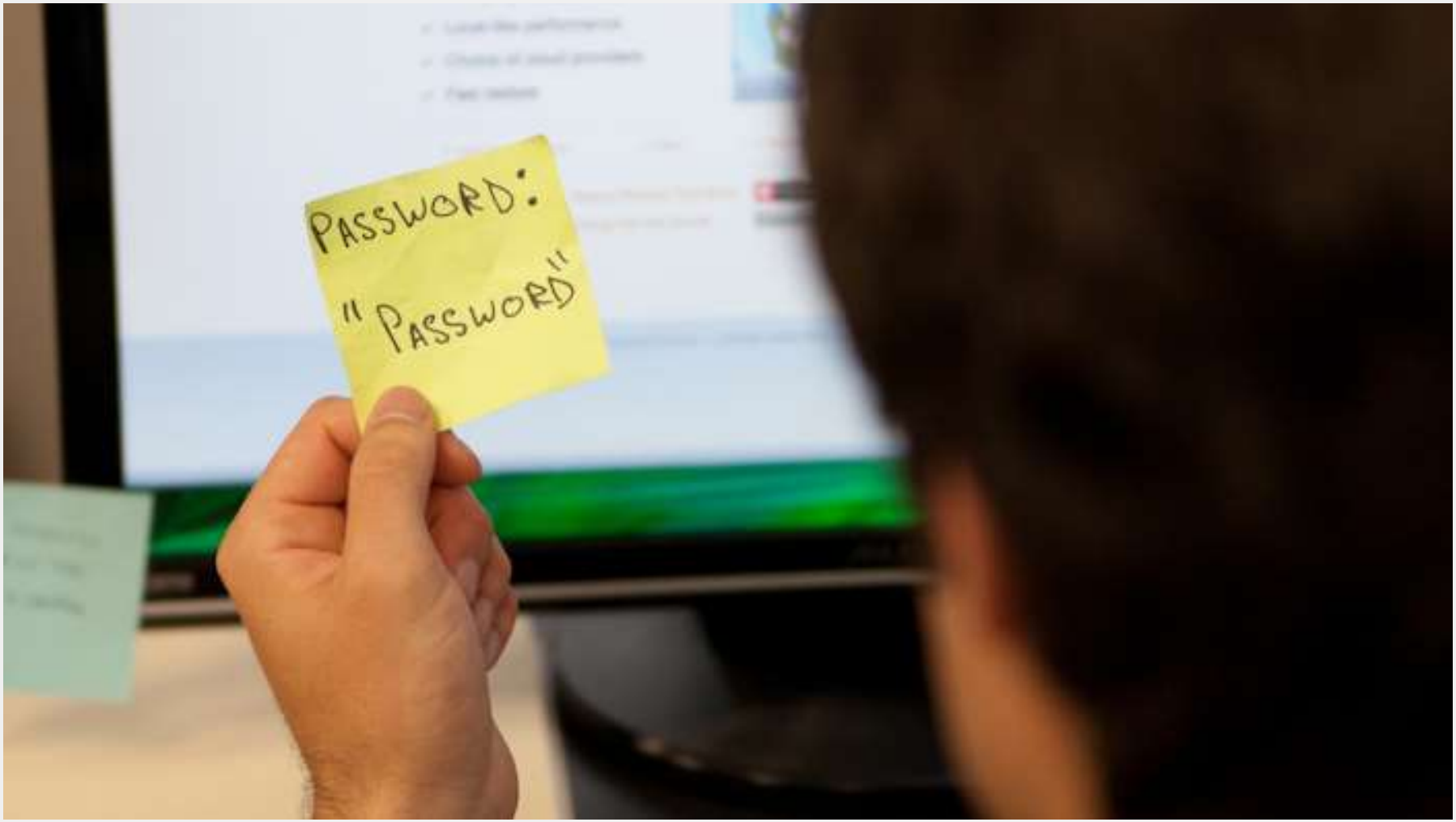
Fortinet 業務協理

洪一民 Keith Hung

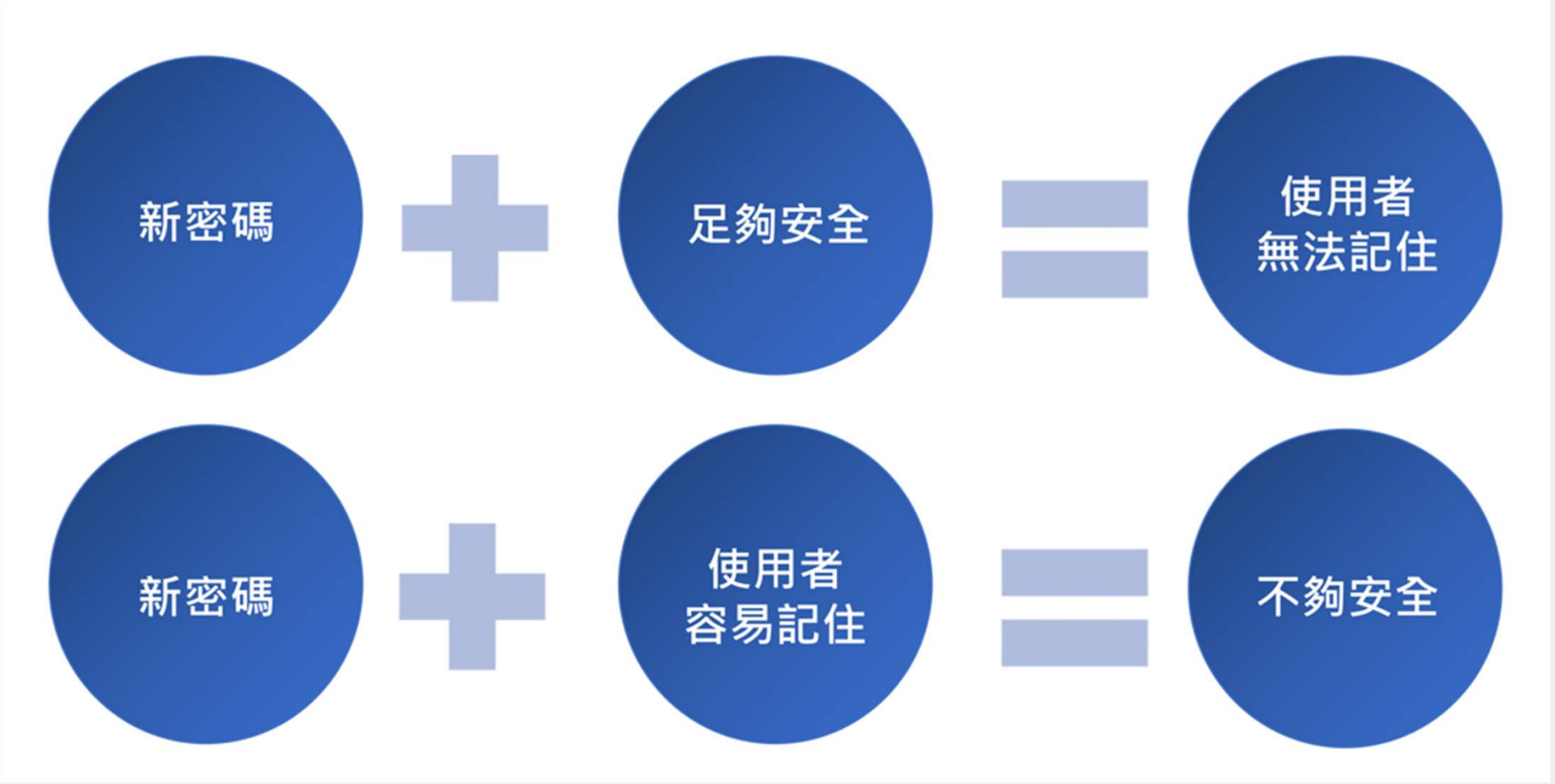
帳密外洩後的風險...



用戶的密碼強度.....？

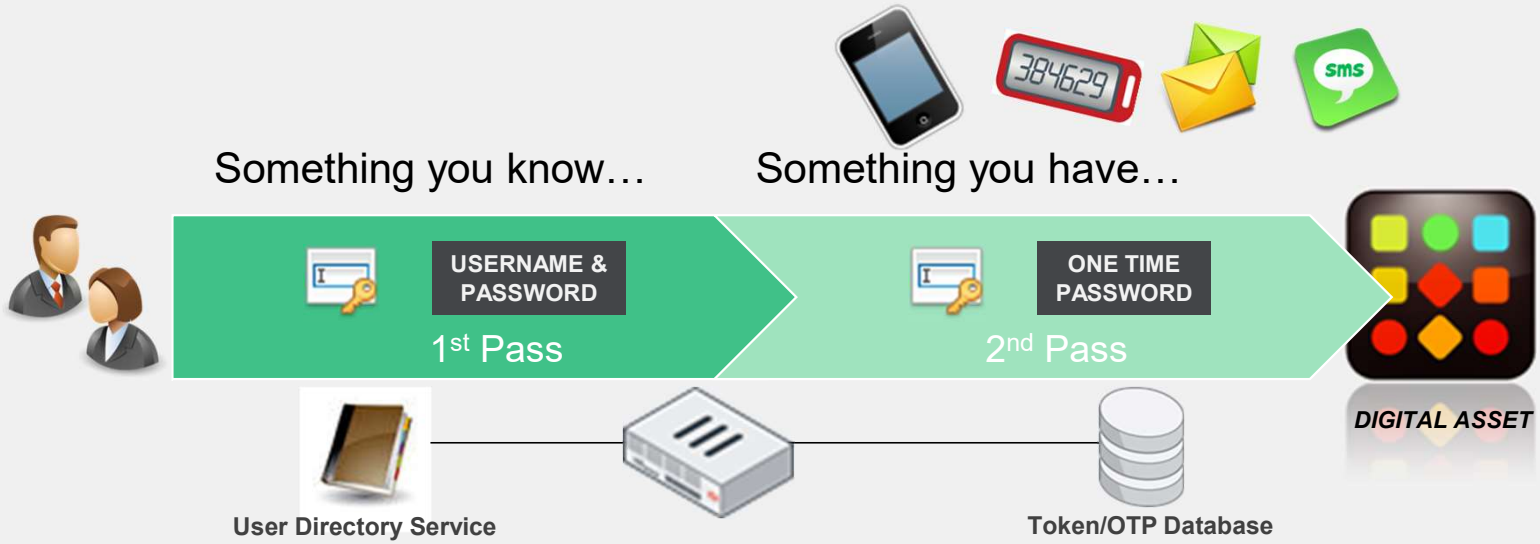


夠安全又能記住的密碼是一項挑戰...



強化身分認證的兩道關卡機制

何謂 雙因子認證 （Two factor Authentication）



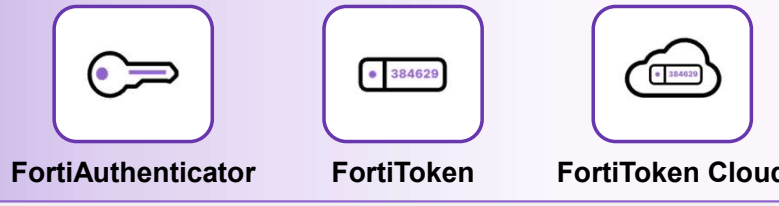
Stronger authentication

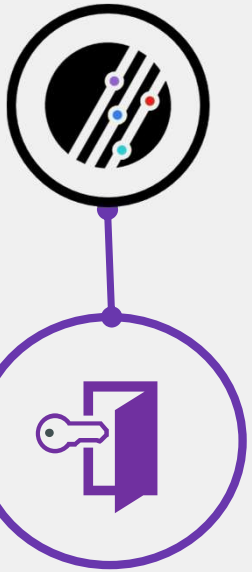
- Password maybe compromised (stolen, hacked, shared)
- Stronger authentication is achieved by requiring additional One-Time Password

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登入管控

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

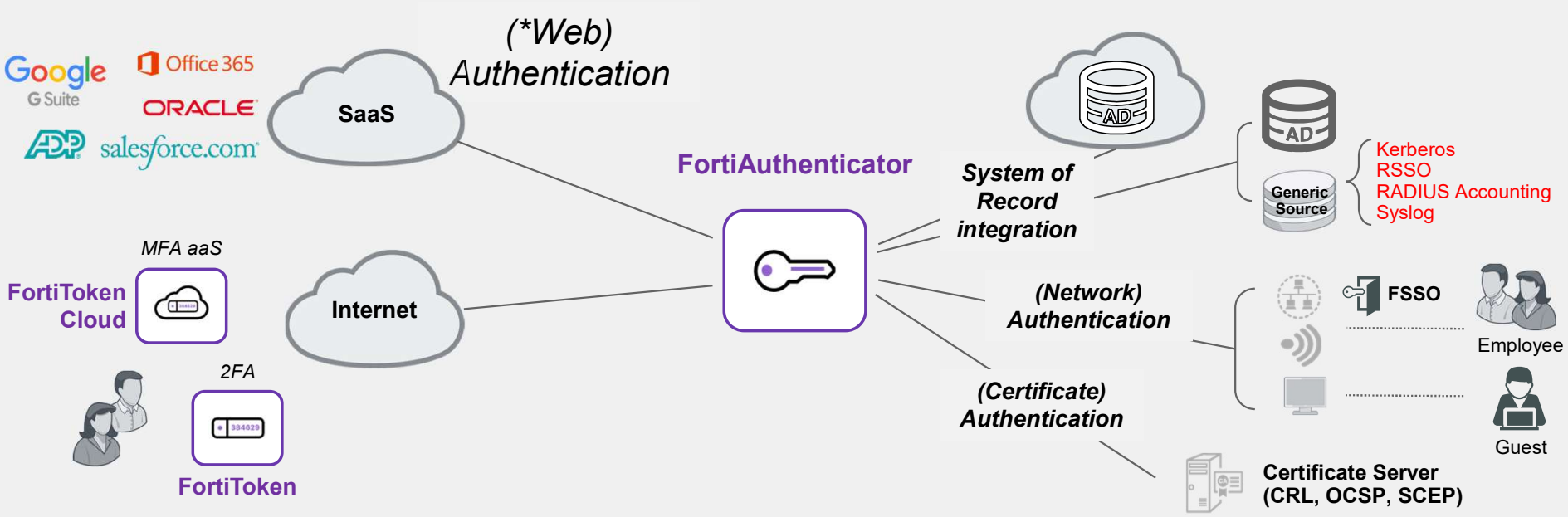




Forti保全

- 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

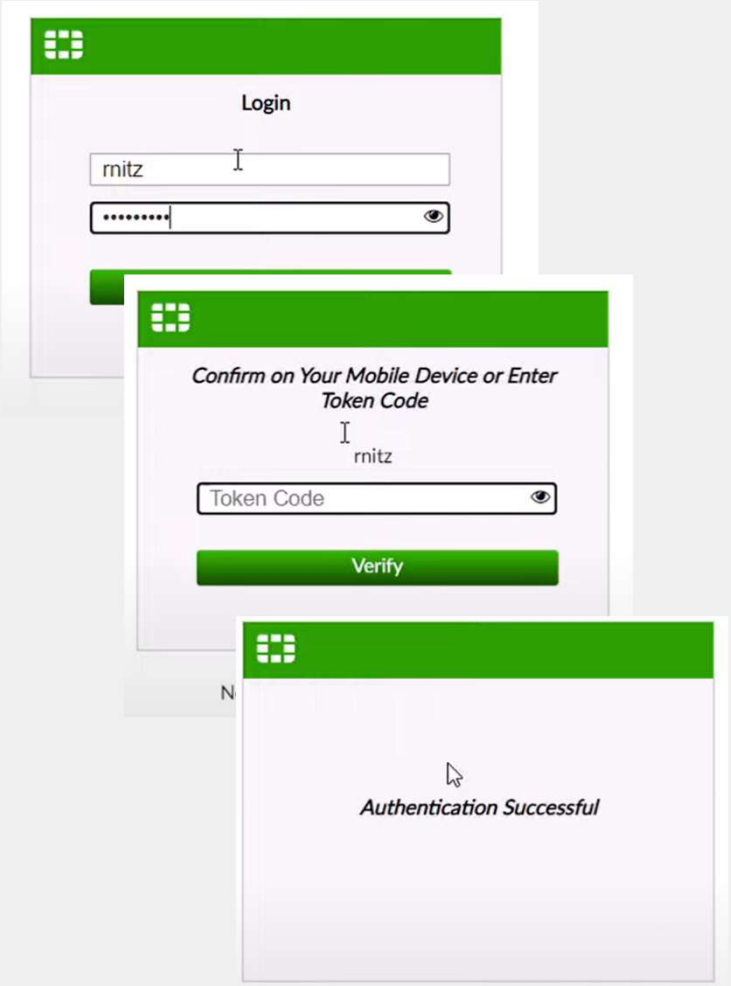
集中管理 安全存取

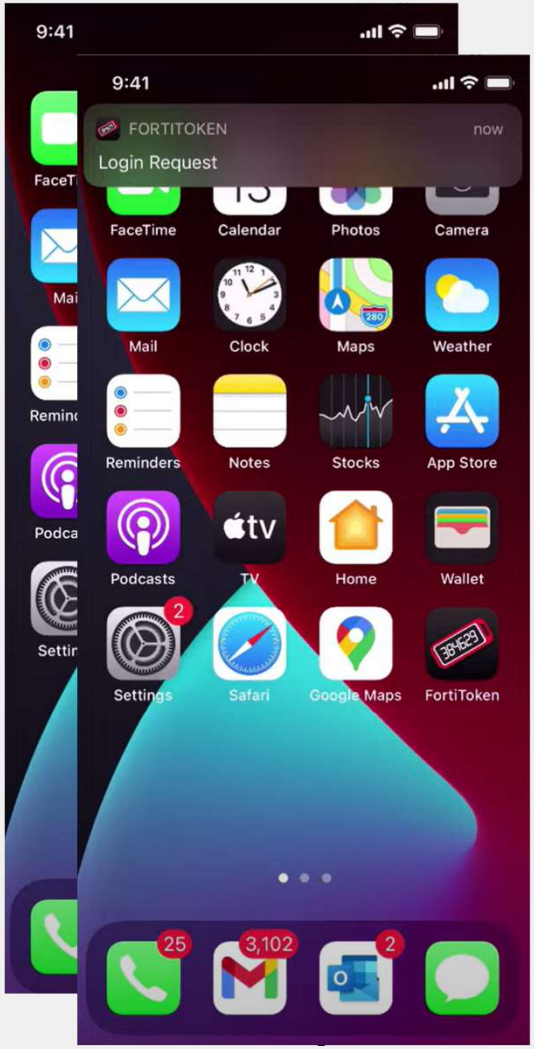


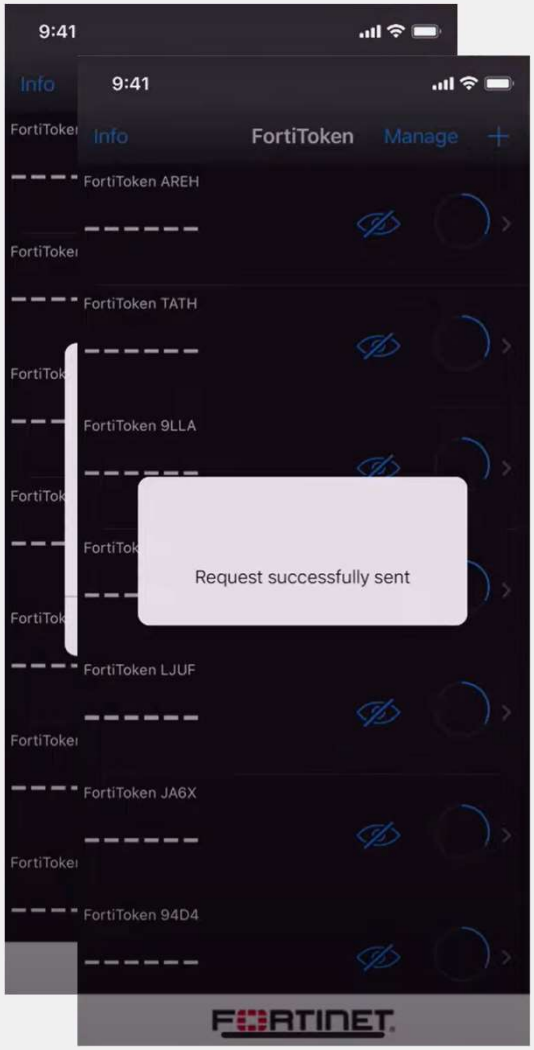
帳號密碼強化	權限控管	單一登入
Establish identity through user log-in, adaptive, certificate, and/or multifactor input	Provide information from authentication source for use in privileged access	Improve security with improved user experience, i.e. reduce user login fatigue

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

雙因子認證無腦操作


Login
rnitz
Confirm on Your Mobile Device or Enter Token Code
rnitz
Token Code
Verify
Authentication Successful


9:41
FORTITOKEN
now
Login Request
FaceTime
Calendar
Photos
Camera
Mail
Clock
Maps
Weather
Reminders
Notes
Stocks
App Store
Podcasts
TV
Home
Wallet
Settings
Safari
Google Maps
FortiToken


9:41
Info
FortiToken
Manage
FortiToken AREH
FortiToken TATH
FortiToken 9LLA
FortiToken LJUF
FortiToken JA6X
FortiToken 94D4
Request successfully sent
FORTINET

FortiToken – Two-Factor Authentication

Multiple Token Options, Easy to Use and Deploy

Perpetual License

FortiToken Mobile App Simplifies User Input to "Click to Accept"

Hardware Tokens Available – to Suit All Use Cases

Self-Service Portal for Guest Access and BYOD

Simple **Deployment** options

Perpetual Licensing – No Ongoing Fees for Locally Managed FortiToken

FortiToken Mobile

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

FortiToken 200B / 200BCD

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

FortiToken 220

A mini credit form factor OTP token

FortiToken 300

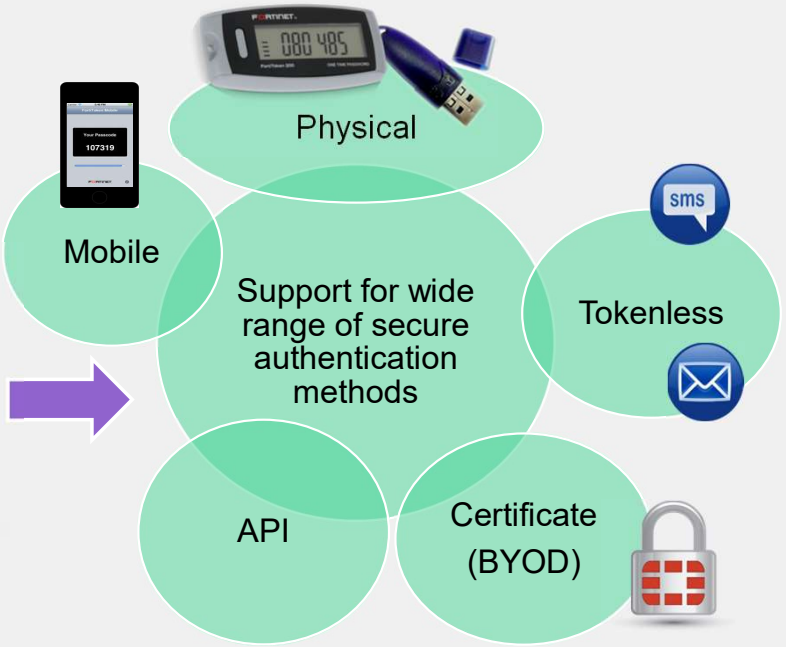
- Driverless USB Device
- FIPS-140 compliant
- Economical PKI authentication. Use with cryptography apps, VPN, web-based apps

FortiToken 400

- FIDO certified
- Passwordless security key
- Use with SSL/VPN, SaaS, or FIDO2 supported browsers

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



FortiToken Mobile

- Two-factor Authentication

From 頴長生
Subject **FortiToken 行動密碼 FTKMOB390A5B9C34 啟用程序 Fortinet Taiwan**
To 頴長生

歡迎使用 FortiToken Mobile - 動態密碼啟用程序

動態密碼啟用碼如下 **FTKMOB390A5B9C34**, 你可以手動輸入啟用碼

"DEYMJYFM6WEUG4NA"

或是透過附件的 QR code 圖片啟用動態密碼 "Scan Barcode"

你必須在下列時間內啟用完成: Thursday, March 03, 2016 17:28 CST (UTC +0800) 如果超過時間尚未啟用,請聯繫 資訊部 重新發送啟用碼

資訊部 Fortinet Taiwan

ftm_qr_FTKMOB390A5B9C34_DEYMJYFM6WEUG4NA.png

1 attachment: ftm_qr_FTKMOB390A5B9C34_DEYMJYFM6WEUG4NA.png 2.8 KB

ANDROID APP ON Google play

Download on the App Store

Download from Windows Store

FortiToken Mobile

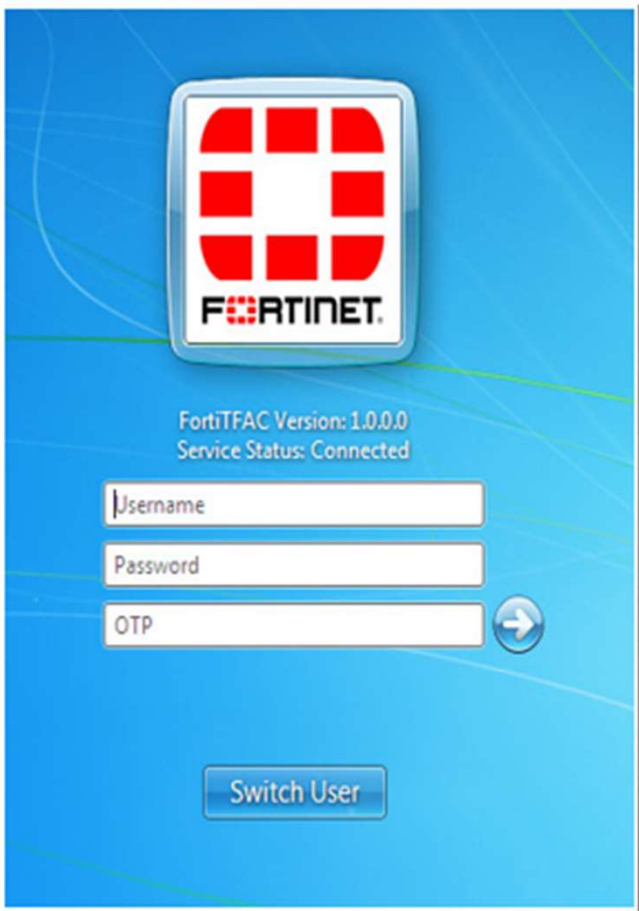
- FortiToken Mobile: 支援 Android, iOS 與 Windows Mobile
  - 6 或 8 驗證碼, 30 或 60秒的更新週期
  - 免費下載安裝, 支援其他 TOTP & HOTP OATH tokens 例如. Google, Dropbox, Amazon
  - 可以透過 QR Code 快速驗證啟用
  - 透過 FAC 可以強制啟用 PIN 碼保護機制
- 永久性授權使用
  - 用戶端載具遺失，可注銷重新發放
  - 用戶離職或調任，可以回收授權重新啟用

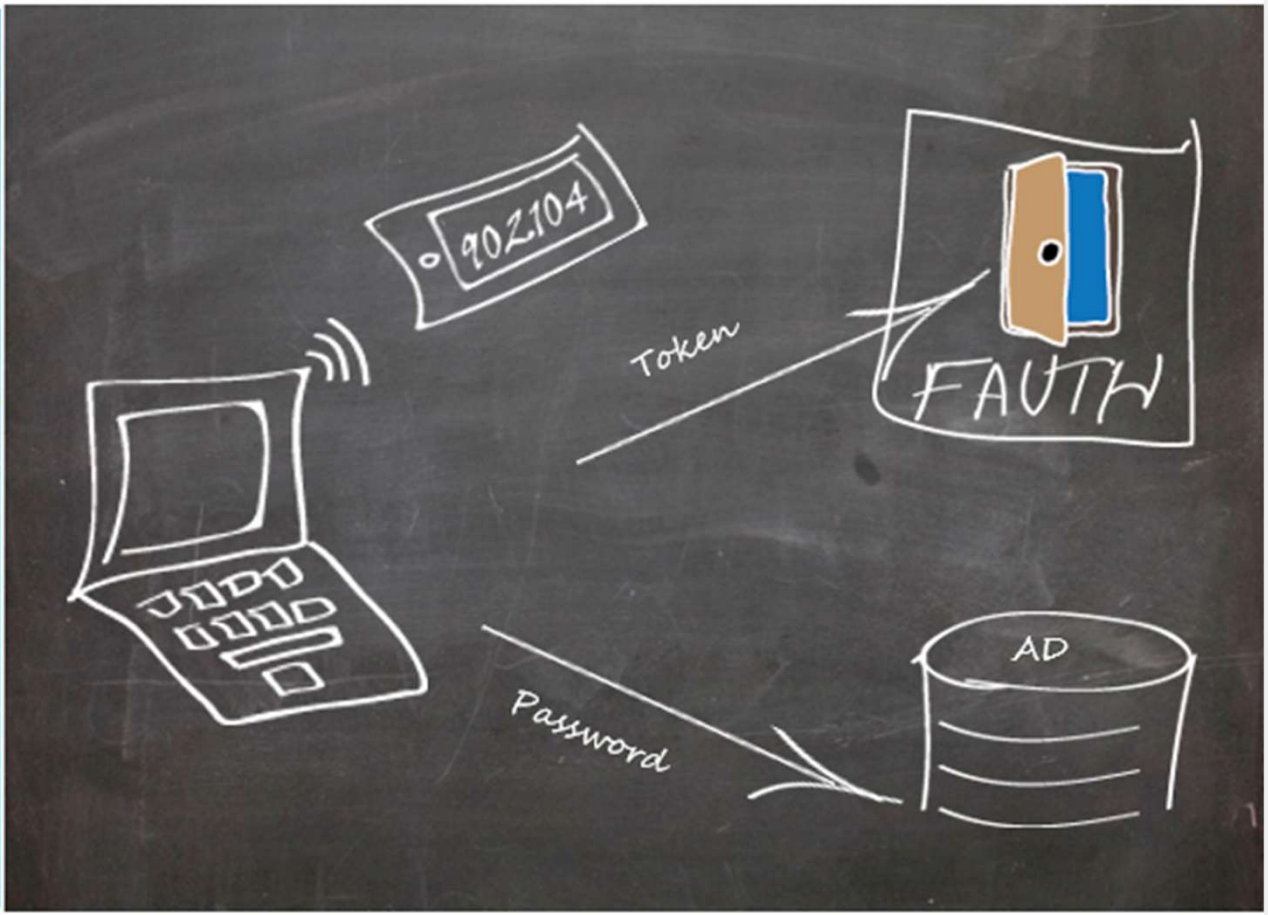
ANDROID APP ON Google play

Download on the App Store

Download from Windows Store

強化微軟作業系統的身分驗證

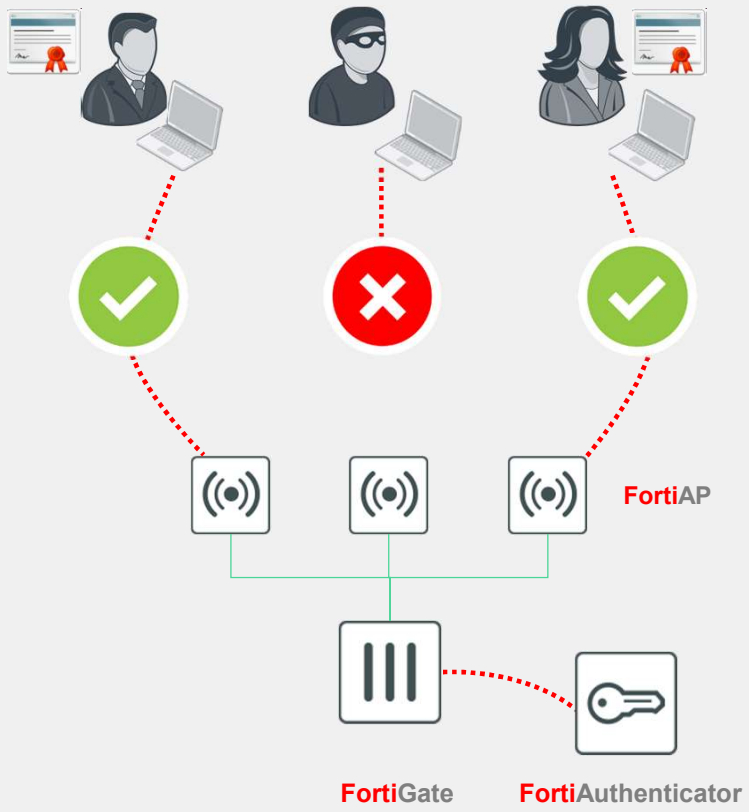




802.1X Port Access Control

有線 / 無線網路認證

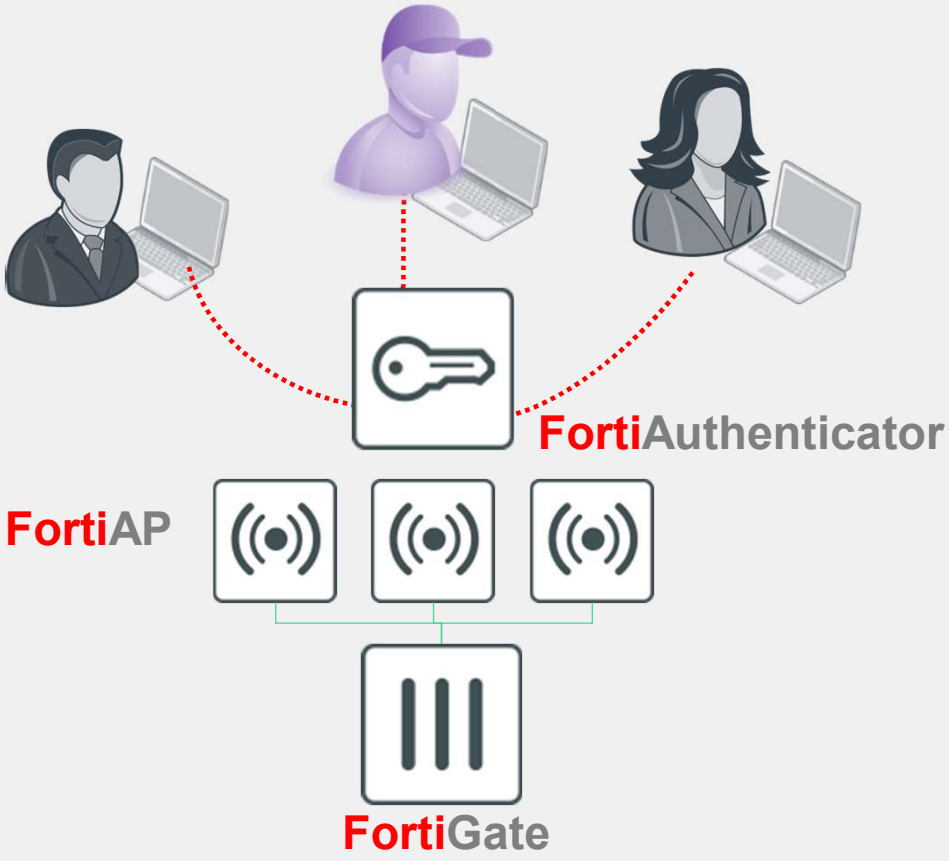
- 集中式 有線網路認證
- 集中式 WiFi 認證
- 支援 (PEAP, EAP-TTLS) 認證協定
- 支援透過憑證基礎的認證方式
- 支援網頁認證，可提供靜態密碼、動態密碼、雙因數認證



Wi-Fi Access Control – 訪客管理系統

訪客認證管理

- 用戶自行註冊
- 簡訊或郵件認證碼
- 用戶資訊欄位選擇與記錄
- 帳號時效管控
- 過期帳號自動清除
- 社交通訊網站身分授權認證
  - Facebook / Google
  - Twitter / LinkedIn



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*

Fortinet 身分識別與網路存取管理系統

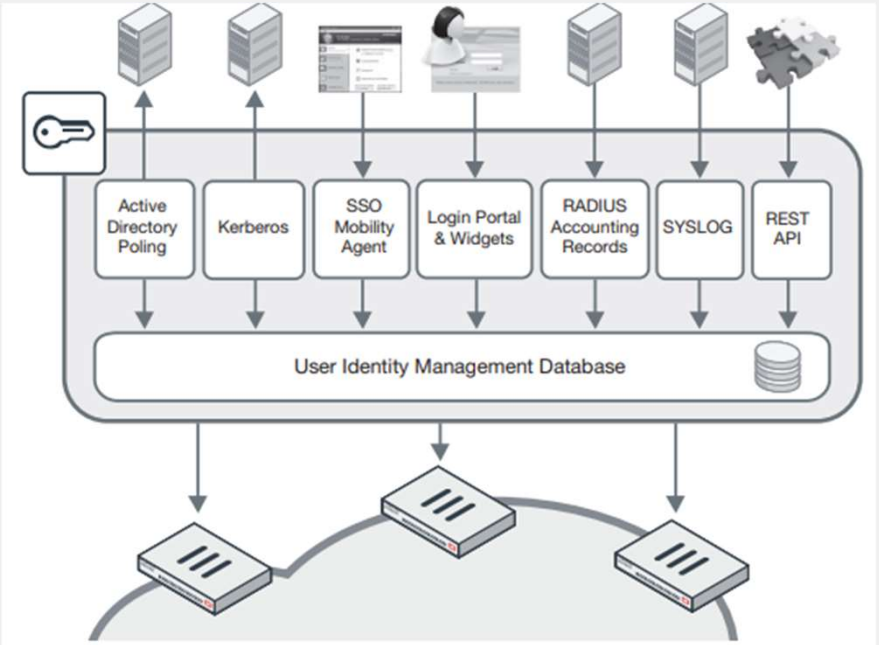
使用者身分的驗證以及使用者權限的控管

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



系統管理權限失守

Uber遭駭，內部多項系統權限被竊，資安業者指出事件嚴重性不應低估

網路叫車平臺大廠Uber在9月中旬，發生約聘員工帳號遭駭，竟致多種系統與內網管理權限遭奪的事件，儘管Uber已經調查並因應，調此事件的嚴重性

文/ 羅正漢 | 2022-09-29 發表

Security upda

Written by Uber Team

September 19, 10:45am PT

While our investigation is still ong
security incident.

What happened?

An Uber EXT contractor had their

豐田供應商系統漏洞 駭客獲取管理權限

2023-02-08

編譯／鄭智懷

化名Eaton Works的白帽駭客在本周發表有關汽車大廠豐田（TOYOTA）公司資訊安全的研究報告，指出其全球供應商管理系統（GSPIMS）存有安全漏洞，任何人可以使用有效的電子郵件地址登入系統，甚至取得系統管理

的時間就找出豐田四個歸類資安漏洞，尤其以
全球供應商管理系統的問題最為嚴重。

MGM Resorts遭網路攻擊，賭場與飯店電腦系統停擺

米高梅國際酒店集團（MGM Resorts International）9月11日對外公告發生網路攻擊事件，旗下飯店與賭場官網停止服務，相關報導則指出MGM在9月10日晚上系統便陸續出現故障，從支付系統、數位房卡到賭場設施無一倖免。

文/ 陳曉莉 | 2023-09-12 發表

圖片來源: MGM Resorts International

資料出處:https://www.ithome.com.tw/news/

如何保護您的財產

常見權限帳戶使用與管理痛點

一個共享的管理員帳戶

無法進行有效稽核，究竟是誰? 人是誰殺的？

管理員帳戶與個人帳戶綁定

傳統常用的方法，安全風險大，
個人帳號失守，整體安全失效。

拆分管理帳號與工作帳號

實務上，難以實踐，並且會導致漏洞。

特權帳號管理 - 1H、2W、3Safe

Who
帳號是誰要用

驗證使用者身分為合法

How
用多久、能用什麼

分級審核制度
最小權使用權限範圍

What
帳號做了什麼

活動監控、記錄、監測

FortiPAM - 用戶管理 (Who)

用戶認證管理

- 本地帳戶
- 遠端帳戶：RADIUS
- 遠端帳戶：AD/LDAP
- 遠端帳戶：SAML IdP

彈性的多因子密碼機制

- 多因子驗證機制(MFA)
  - Email OTP
  - FortiToken
  - FortiToken Mobile

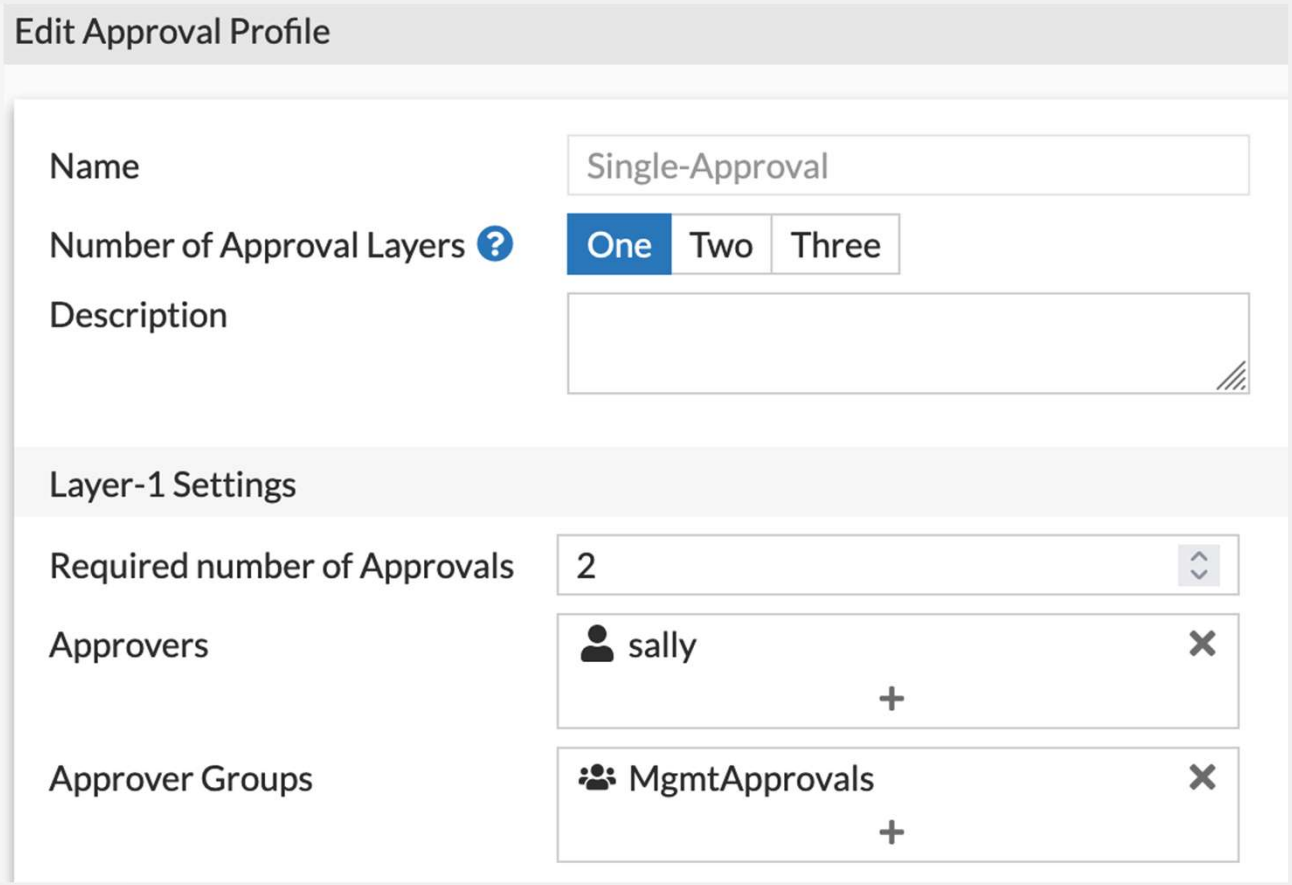
進階的安全強化機制

- 來源位址確認
- 連線時間限制
- 零信任存取架構

FortiPAM - 審核與控管 (How)

存取憑證流程審核

- 組織可依需求決定審核流程。
- 啟用後，使用的用戶，要獲得授權後才能連線主機。
- **存取流程審核流程最多 3 層。**
- **每一層至少一位授權者。**
- 核決授權者角色 ，可為 User 或 Group成員。



FortiPAM - 審核與控管（How）

權限控制 - 誰可以連線

管控政策

- Inherit Policy - **Enabled**:

  由上至下層群組套用一致的權限原則

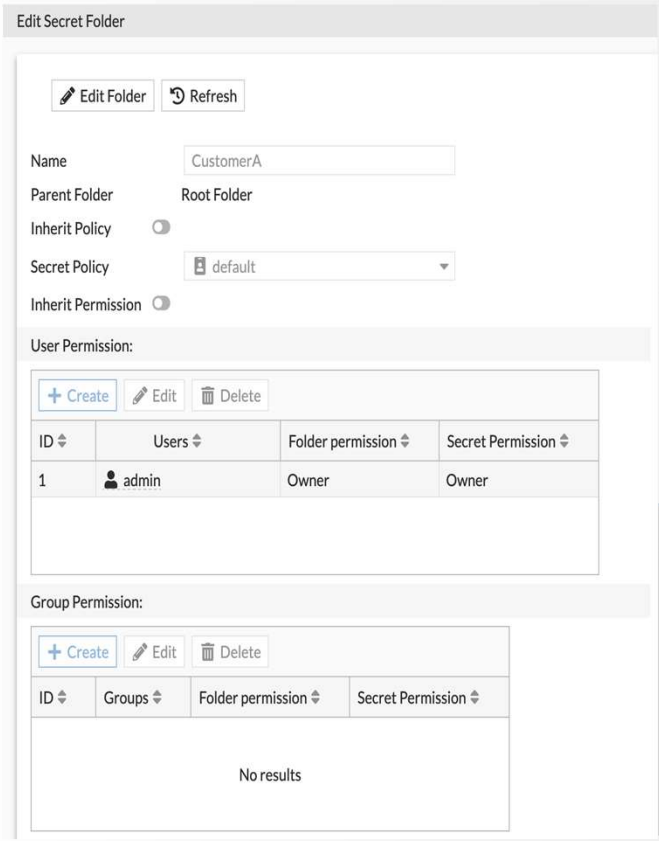
- Inherit Policy - **Disabled:**

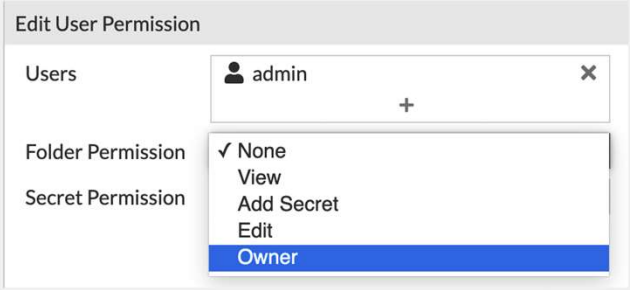
  可透過自訂套用至不同的子群組。

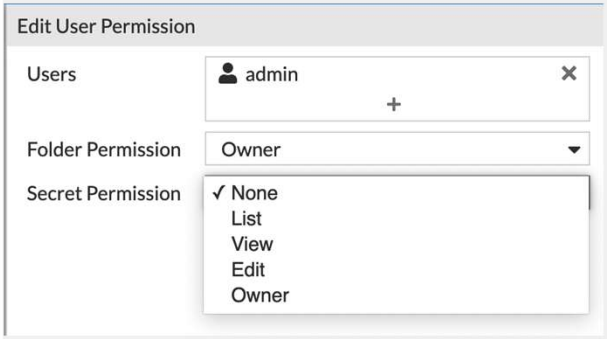
使用權限

- 可套用至使用者及群組。
- 可細緻設定連權限：

  - view, list, add, edit, owner







FortiPAM - 監控與紀錄(What)

凡走過必留下足跡

會話錄影紀錄

- **支援全會話錄影 。**
- **會話使用期間滑鼠點擊、鍵盤活動紀錄。**
- **影像保留紀錄政策。**
  - 可自定義會話錄影保留政策。

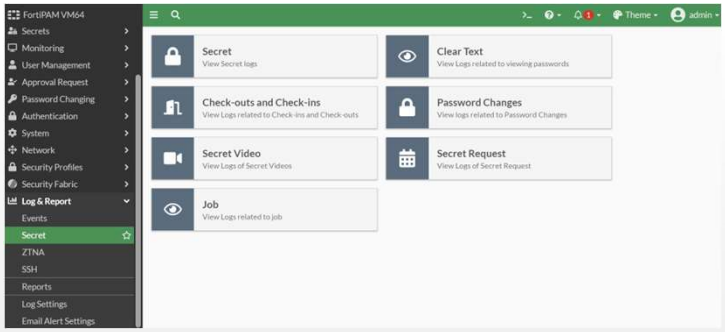
紀錄

Events

- 系統紀錄。
- 使用者活動紀錄。

Logs

- 存取紀錄。
- 簽出、簽入紀錄。
- 操作紀錄。



FortiPAM - 安全強化 (Safe)

Secure File Transfer, Securing Secrets and Monitoring

檔案安全傳遞

檔案交換惡意威脅偵測

- 可聯動 FortiSandbox、FortiNDR 偵測已知、未知 Zero-day 惡意程式。
- 支援 WinSCP、WinSMB。

系統資料安全保護

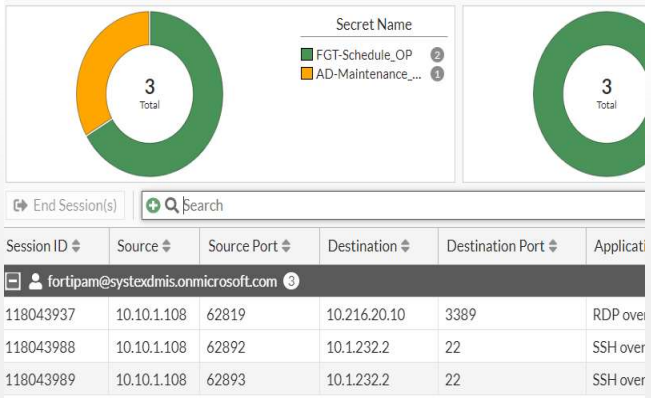
TPM 加密機制

- TPM in Hardware Models 。
- vTPM in Virtual Machine。

Trusted Platform Module

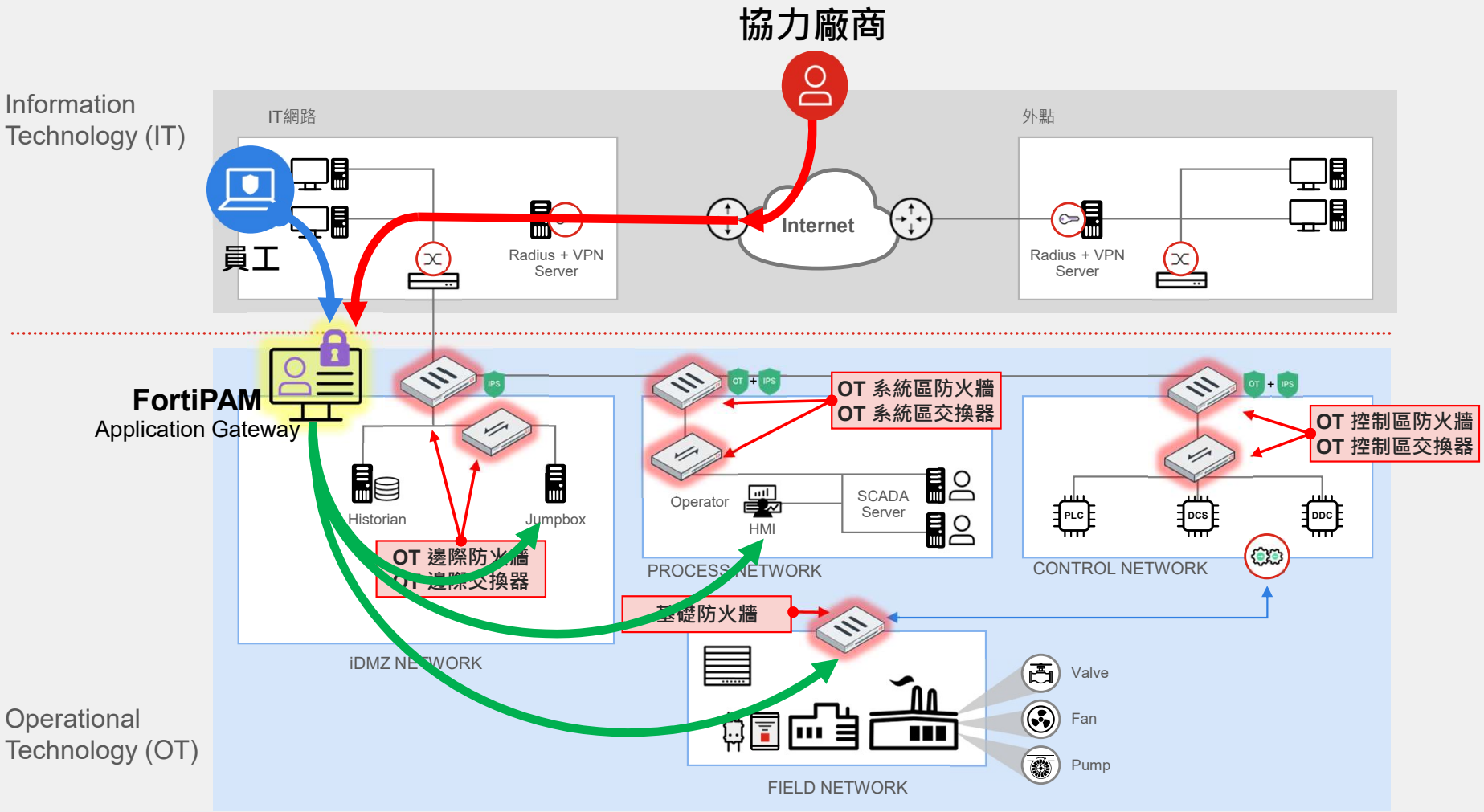
監督

- **SSH 風險性指令控制。**
- **使用者及連線監控。**



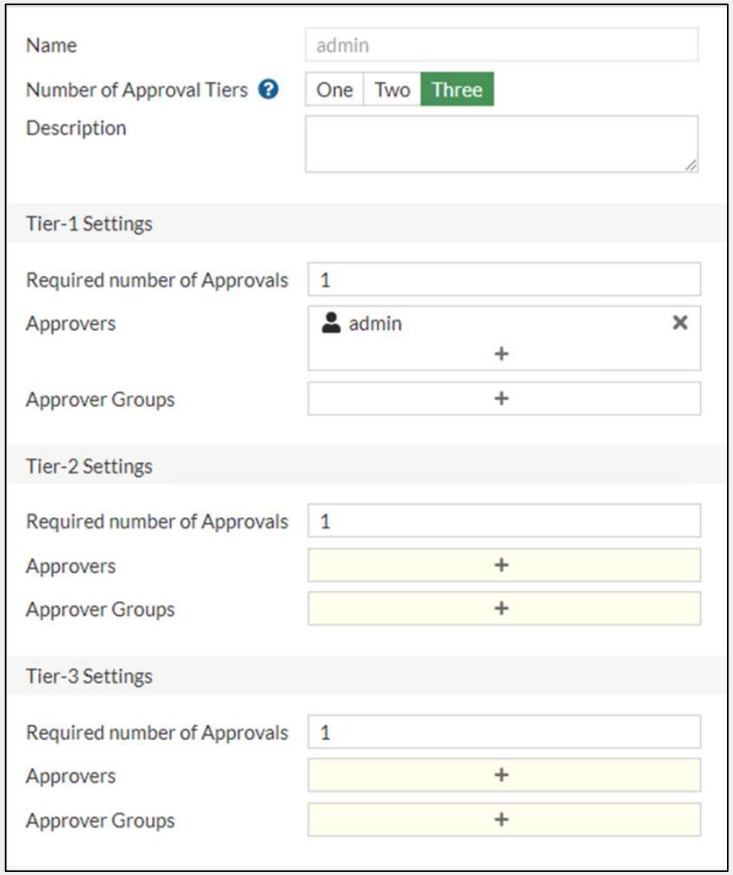
應用情境

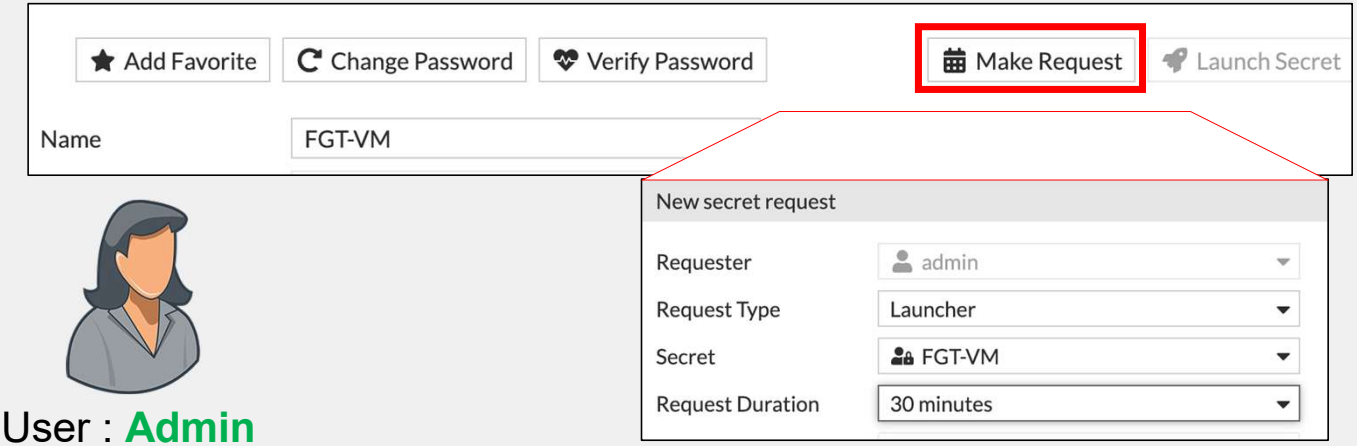
安全的使用接入點



使用管控 - 審核授權

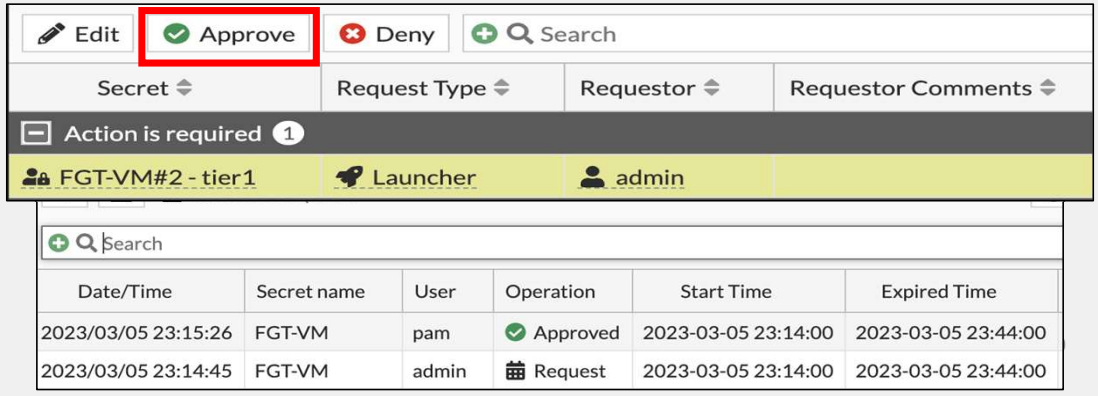
最多可以設定3階審核



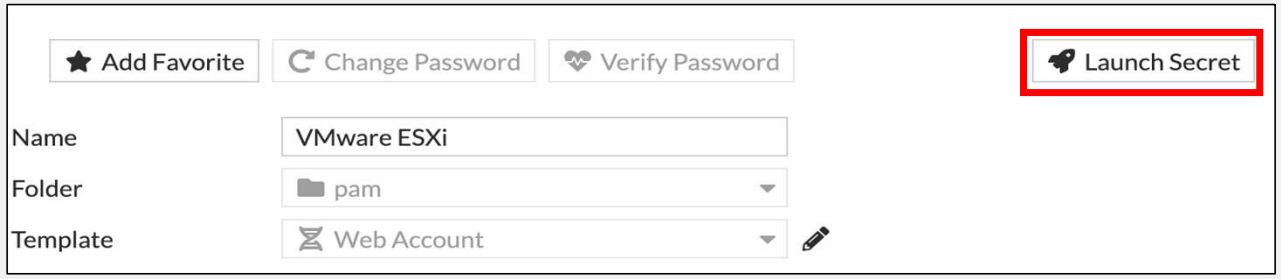


User : **Admin**

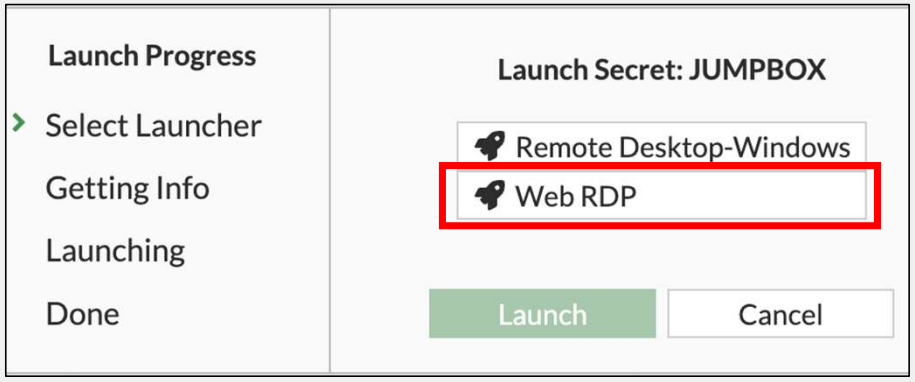
User : **Pam**

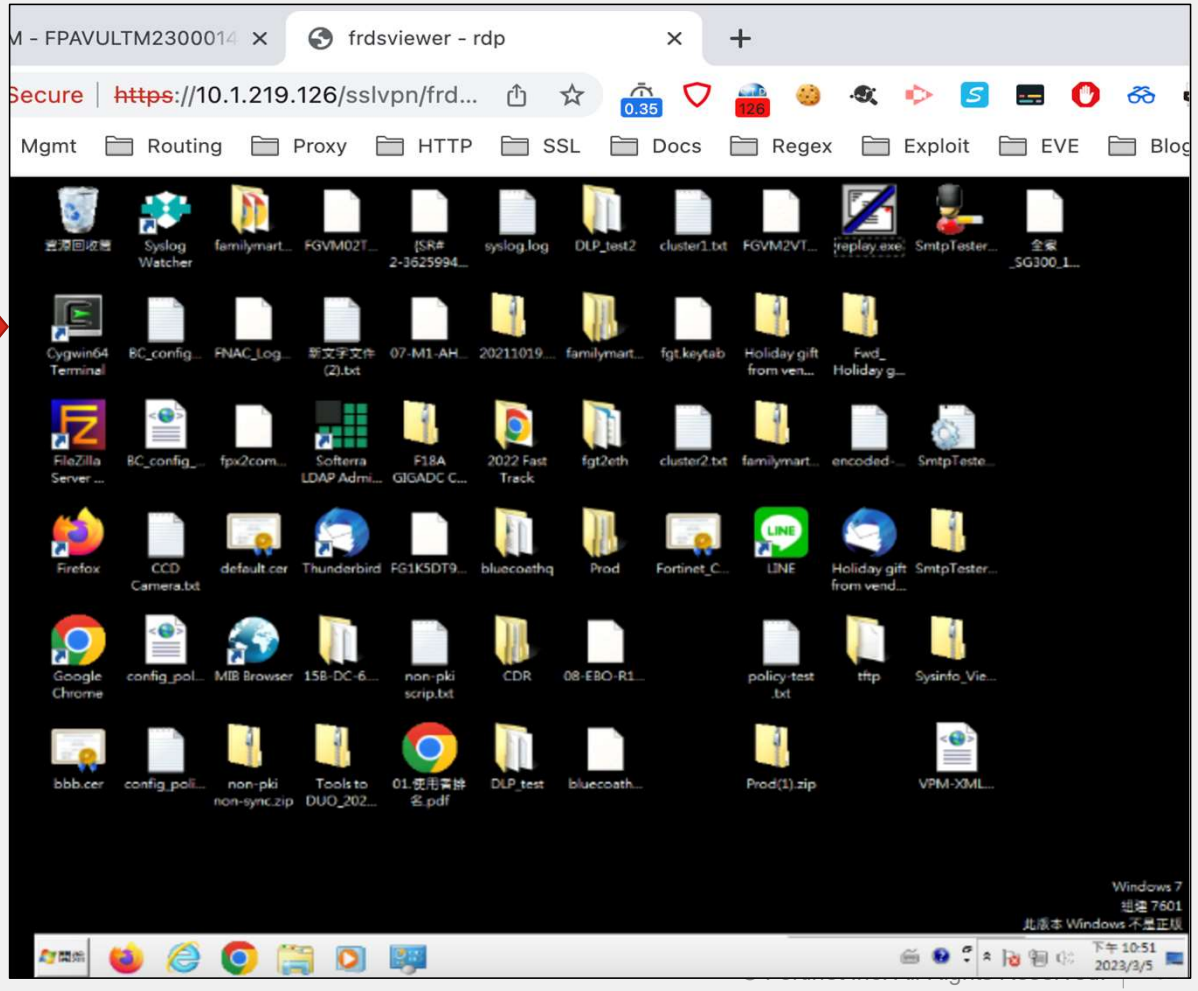


虛擬環境管理強化： ESXi Mgmt



安全協定保護 - Web RDP



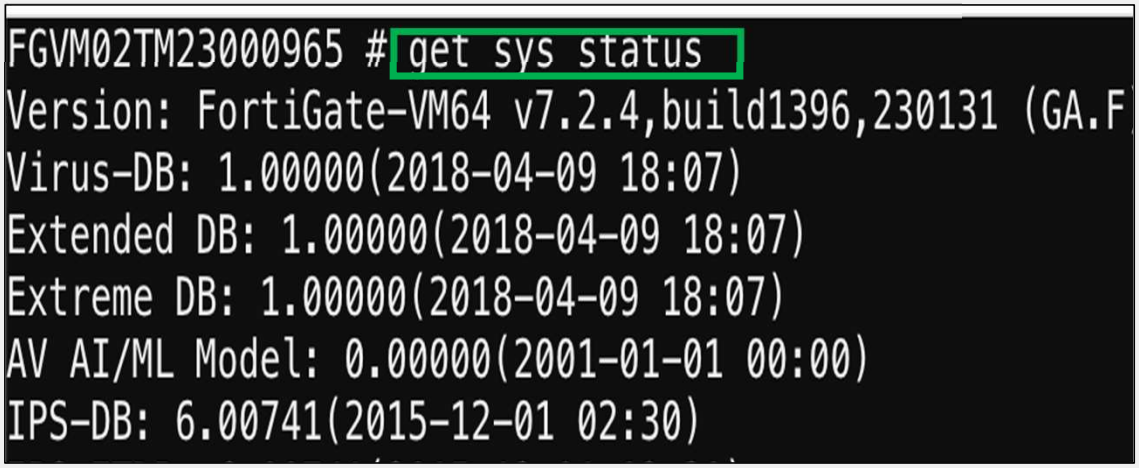


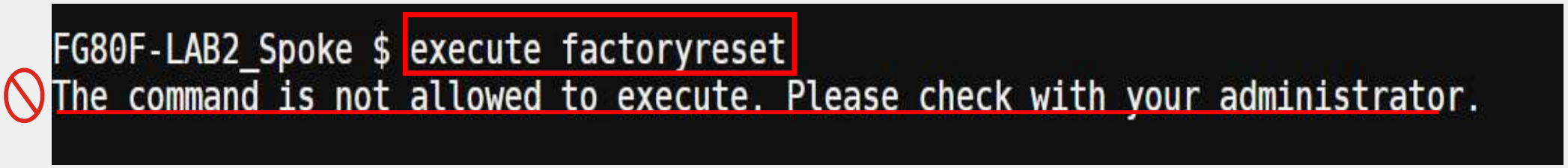
保護 RDP 協定

“避免直接暴露”

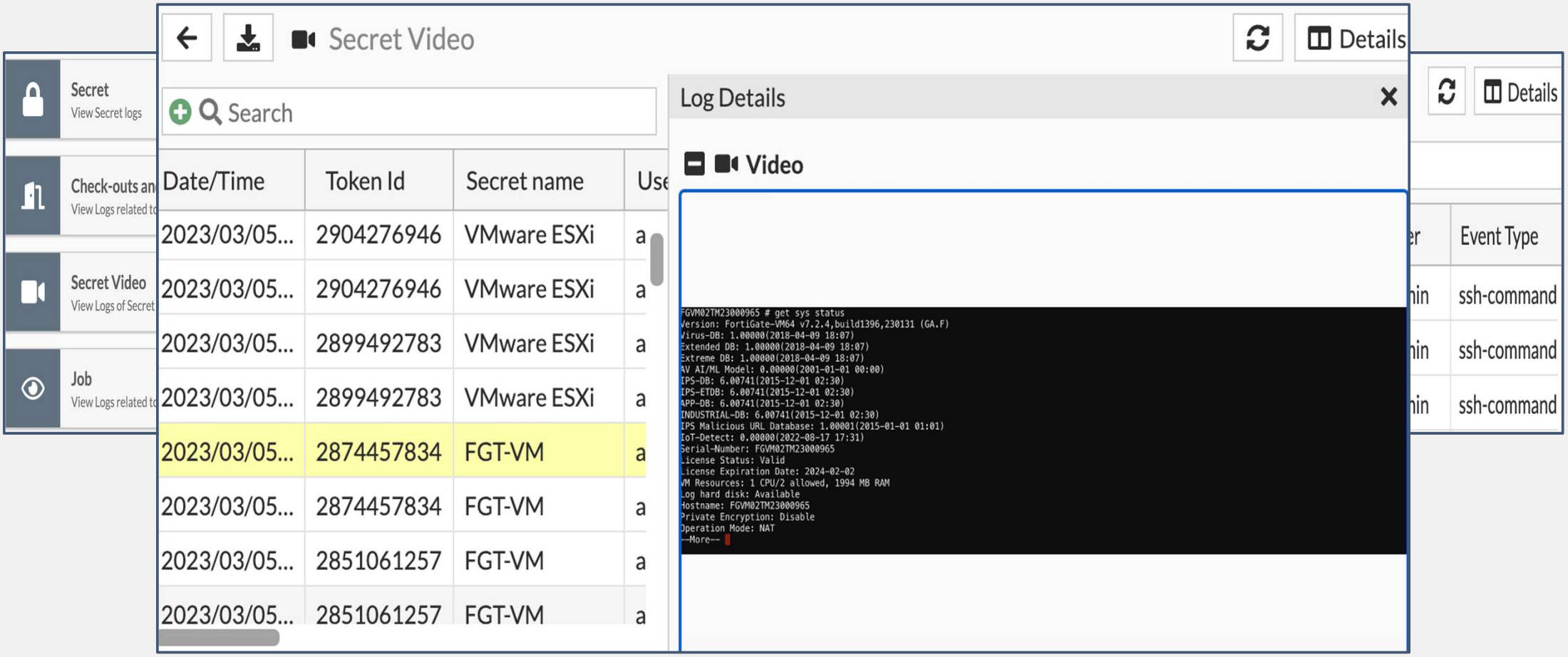
操作的安全性 - 指令過濾器

保護系統操作 “避免無意或蓄意的指令”





紀錄資料



Daily Report

每日報表整理連線的時間、次數與人員的連線紀錄

Top Failed Password Verification by Secret Name and Reason

#	Secret Name	Reason	Totals
1	RDP250 (*a32761)	connection-error	5
2	FTP (*5c7249)	connection-error	1
3	RDP250 (*a32761)	login-auth-error	1

Top Failed Password Verification by Secret Name, User and Reason

#	Secret Name	User Name	Reason	Totals
1	RDP250 (*a32761)	admin	connection-error	5
2	FTP (*5c7249)	admin	connection-error	1
3	RDP250 (*a32761)	admin	login-auth-error	1

Clear Text View

Summary	Stats
Total # of Views	14

Top Clear Text View by Secret Name

#	Secret Name	Total # of Views
1	RDP250 (*a32761)	6
2	SMB (*37315b)	5
3	FTP (*5c7249)	2
4	RDP (*e88a77)	1

Top Clear Text View by Secret Name and User

#	Secret Name	User Name	Total # of Views
1	RDP250 (*a32761)	admin	6
2	SMB (*37315b)	admin	5
3	FTP (*5c7249)	admin	2
4	RDP (*e88a77)	admin	1

Schedule-default-2023-05-17-000100

5 of 7

Secret

Secret Launch Success

Summary	Stats
Total # of Launches	39
Total Duration	02h 12m 22s

Top Secret Launch Success by Secret Name

#	Secret Name	Total # of Launches	Total Duration
1	FTP (*4597ed)	9	02h 01m 48s
2	7.4_SSH (*36ab5c)	8	06m 29s
3	FTP (*5c7249)	6	01m 23s
4	FTP (*45ba47)	4	55s
5	FTP (*c1a03f)	4	16s
6	RDP250 (*a32761)	3	55s
7	SMB (*5c7831)	2	11s
8	RDP (*e88a77)	2	07s
9	FTP (*3999bb)	1	18s

Top Secret Launch Success by Secret Name and User

#	Secret Name	User Name	Total # of Launches	Total Duration
1	FTP (*4597ed)	admin	9	02h 01m 48s
2	7.4_SSH (*36ab5c)	admin	8	06m 29s
3	FTP (*5c7249)	admin	6	01m 23s
4	FTP (*45ba47)	admin	4	55s
5	FTP (*c1a03f)	admin	4	16s
6	RDP250 (*a32761)	admin	3	55s
7	SMB (*5c7831)	admin	2	11s
8	RDP (*e88a77)	admin	2	07s
9	FTP (*3999bb)	admin	1	18s

Password Change

Summary	Stats

Easy To Security

特權帳號不外露，降低數據洩露風險

提高資安防護。

Easy To Manager

使用者認證與連線授權，**落實資安控管**

Easy To Tracking

活動監控、記錄，**強化資安合規與追蹤**

Fortinet Security Fabric

安全織網 **全面-整合-自動**

防護點線面，整合不落單

FORTINET

感謝您的聆聽


FORTINET