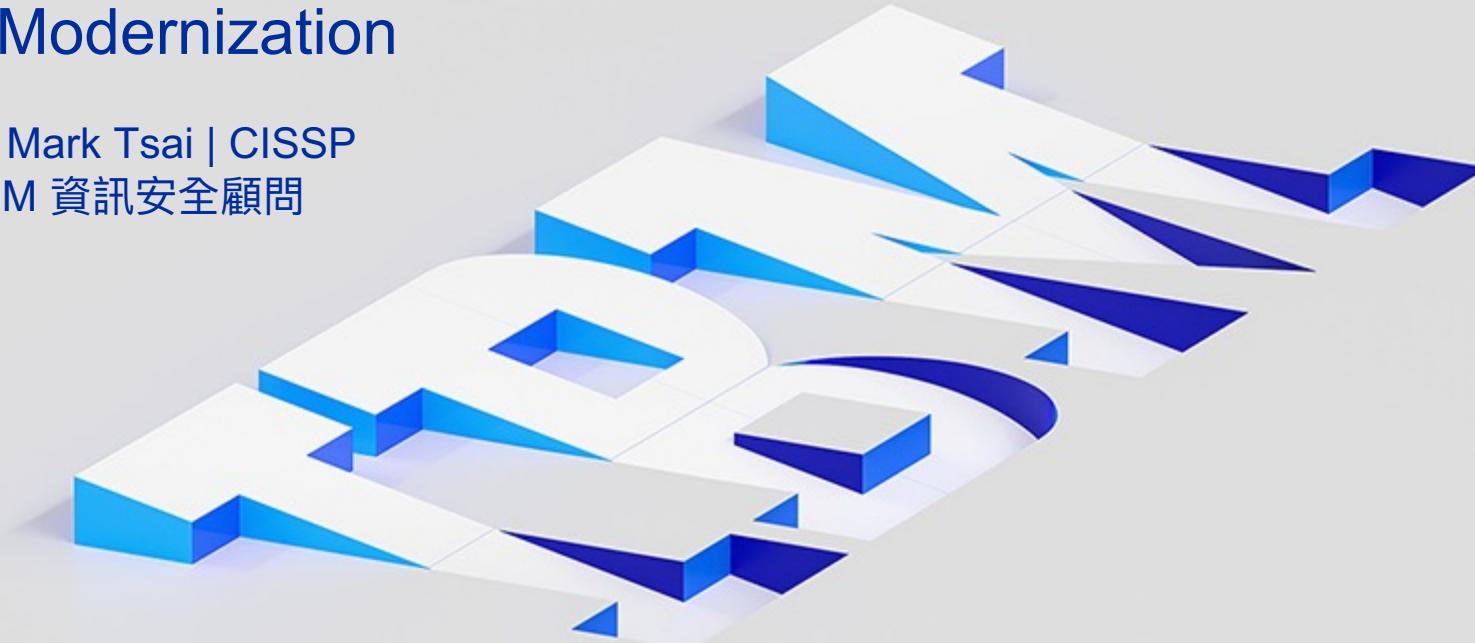


# IBM Security™ with TSMC

## 身份存取與管理的現代化轉型

### IAM Modernization

—  
蔡睿誠 Mark Tsai | CISSP  
臺灣 IBM 資訊安全顧問



# 網路釣魚和漏洞利用 是最重要的資安攻擊感染媒介

41%

## 網路釣魚事件的威脅佔比

網路釣魚是 2021 年最流行的初始感染媒介，佔 IBM Security X-Force 觀測的所有事件中 41%，高於 2020 年的 33%。

33%

## 漏洞利用攻擊增加

儘管在 2021 年下降到第二大最常見的初始感染媒介，僅次於網路釣魚，但由漏洞利用引起的事件數量比 2020 年增加了 33%。

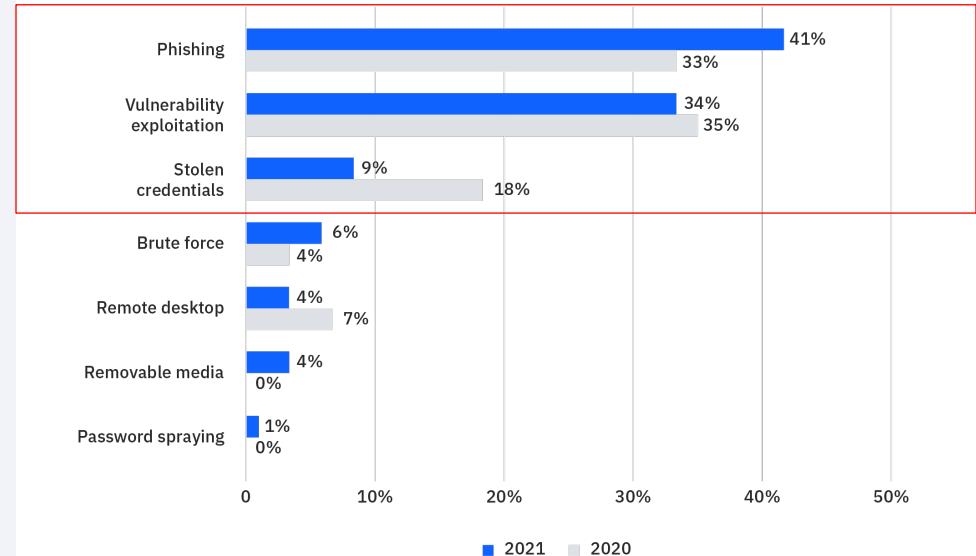
## Log4j

### 在 10 大漏洞列表中排名第二

接近 2021 年底，對 Log4j 漏洞 CVE-2021-44228 的廣泛利用使該漏洞進入 X-Force 2021 年的前 10 名名單。

## Top infection vectors, 2021 vs. 2020

Breakdown of infection vectors observed by X-Force Incident Response, 2020-2021 (Source: IBM Security X-Force)



# 產業趨勢 Trends

**Breakdown of attacks on the top 10 industries, 2021 vs. 2020**  
(Source: IBM Security X-Force)

## 製造業 Manufacturing #1

### 所有產業裡遭受最多的攻擊

自 2016 年以來，金融和保險首次不是受攻擊最嚴重的行業，在2022年製造業是成為被攻擊的第一大產業，從去年的第二位和三年前的第八位攀升，主要是勒索軟件和 BEC 對製造業的衝擊促成了這一轉變。

## 金融和保險 Finance and Insurance #2

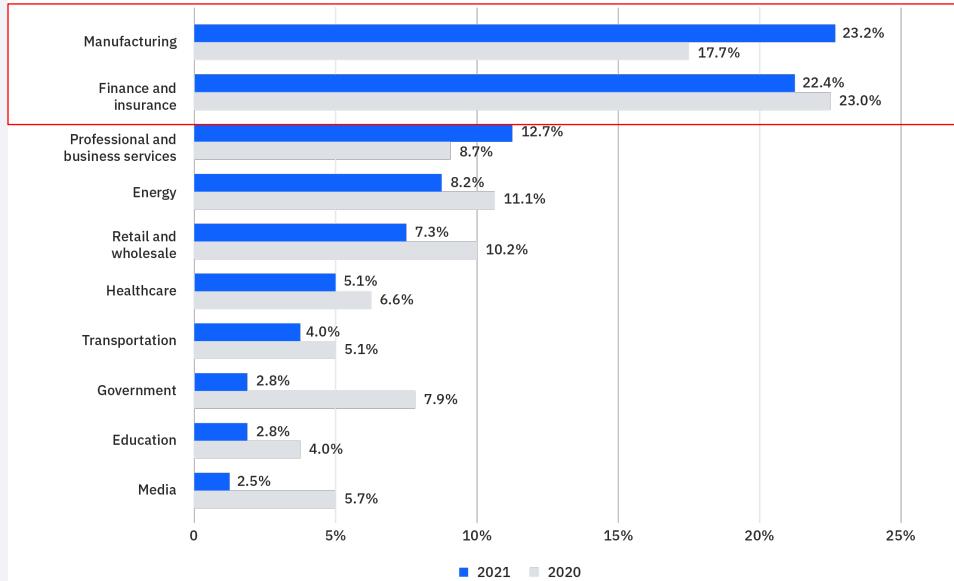
### 部署對的資安防護方案

金融業從首位下降表明金融服務業正在對的資安防護策略。此外，混合雲環境在金融服務體系中占主導地位，使可以更好地了解和管理敏感數據。

## 批發業 wholesale 遭受重點攻擊

### 批發業去年受到的攻擊比零售還多

這些行業在 X-Force 的 2022 年排名中排名第五。在這些攻擊中，35% 是針對零售的，65% 是針對批發的，這凸顯了威脅行為者對批發組織的高度重視，這可能是由於它們在供應鏈中發揮的關鍵作用。



# 製造業 Manufacturing

#1

23.2%

製造業從 2020 年的第二位上升為  
2021 年受攻擊最多的行業。

對前 10 大行業的所有攻擊，  
高於 2020 年的 17.7%。

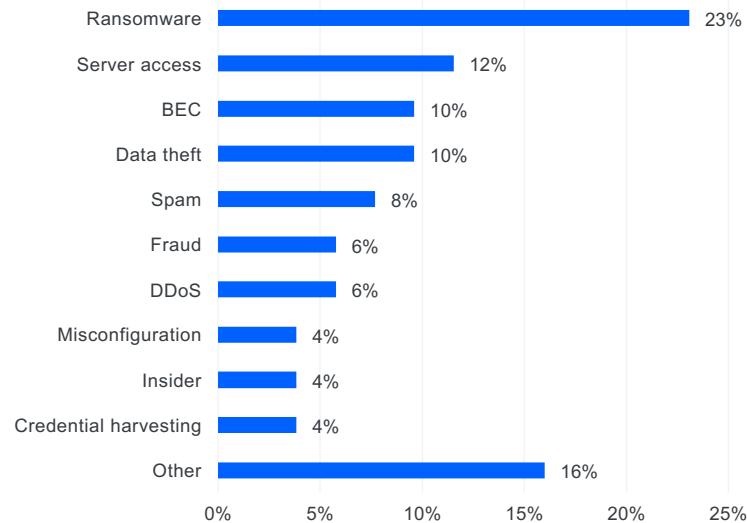
## 威脅觀測洞察 Threat intelligence

- 該部門對停機時間的低容忍度可能是對威脅參與者的高盈利能力的一個促成因素。
- 勒索軟件是最主要的攻擊類型，佔針對製造組織的攻擊的 23%，突顯了勒索軟件攻擊者對製造業的高度關注。
- 服務器訪問攻擊以 12% 位居第二，可能代表了一些失敗的攻擊操作。BEC 和數據盜竊並列第三，各佔 10%。BEC 攻擊者可能正在尋求利用製造組織發展的許多供應商和批發運輸關係，並試圖將合作夥伴之間的付款重定向到 BEC 攻擊者控制的賬戶。

## 受到攻擊的地區 Geographies attacked

製造業面臨的攻擊最多 Asia (32%),  
North America (27%), and Europe (26%)

**Top attack types in manufacturing**  
(Source: IBM Security X-Force)



# IBM Security 威脅對策

- 1 制定勒索軟體的威脅響應計劃
- 2 在網路中的每個接入點上實施多因素身份驗證
- 3 採用分層防禦方法來打擊網絡釣魚
- 4 完善和成熟化您的漏洞管理系統
- 5 採用零信任原則來幫助降低進階威脅攻擊風險
- 6 使用資訊安全作業自動化來增強事件響應
- 7 使用擴展的偵測與響應功能以獲得優於攻擊者的優勢



# IBM採用現代化數位身份解決方案提供內部員工與外部客戶統一性身份認證與管理

透過 IBM Verify 身份認證  
與管理解決方案，提供超過：

# 270 萬+

使用無密碼方式 QR 和 FIDO2 等  
高級身份驗證機制進行內、外部資源存取



“With IBM Security Verify, to anyone who interacts with IBM, we can now provide frictionless, secure, state of the art access to information resources.”

Gary Schmader, Sr. Manager, Assured Identity and Security Operations, IBM



# IBM採用現代化數位身份解決方案提供內部員工與外部客戶統一性身份認證與管理

w3id on IBM Security Verify

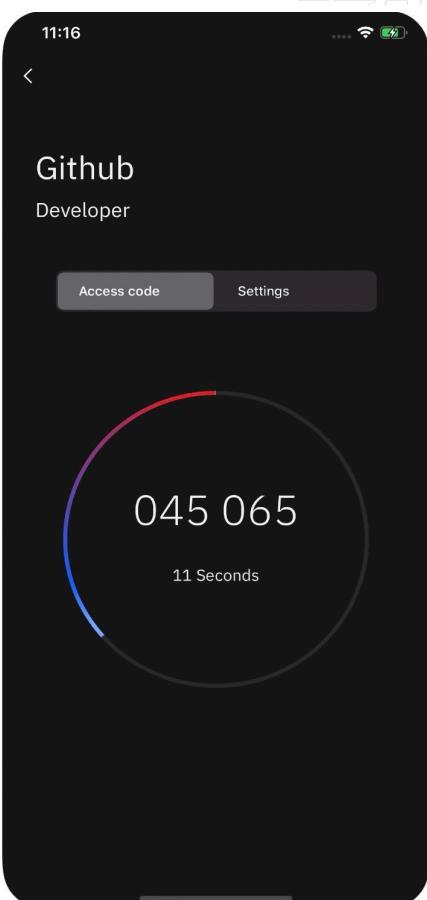
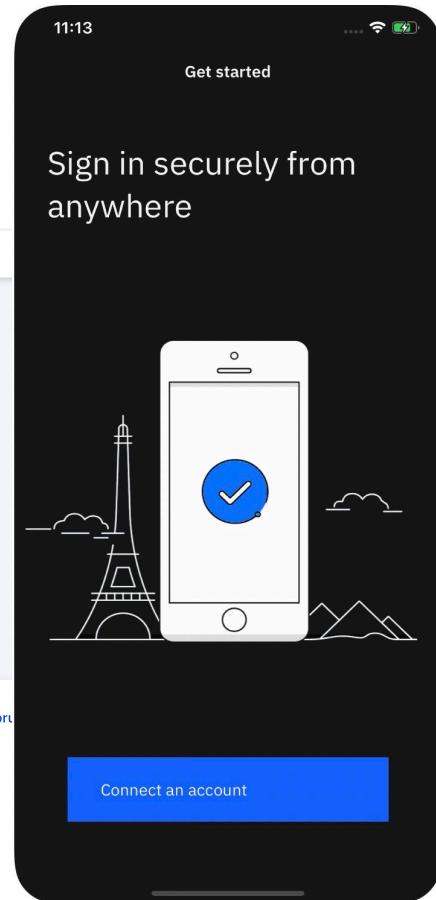
≡ IBM AccessHub | Home

Hi Ruei Cheng (Mark) Tsai  
You are logged in as : ZZC

Overview  
Certifications Pending for My Action  
0

Tiles

- Request New Access  
This is place to start a request for New Access for Self
- Requests History
- Pending Approvals



# 遠傳電信採用適合雲地的身份安全方案 打造電信客戶門號與隨選服務身份認證



透過 IBM Verify 身份認證  
與管理解決方案，提供超過：

## 10 萬+

使用身份聯合 (Identity Federation) 機制串連客戶門號帳戶資訊實現單一登入機制 SSO

### 遠傳 frid<sup>ay</sup> 影音

### 隨時隨地 盡享影音樂趣

全球潮流影劇每日更新、隨選隨看

- 全館影劇無限看 (單片除外)
- 每月送2張看片券
- 周周看片送點數
- 支援跨裝置使用



# 現代化大型企業組織身份安全管理

## 高科技製造業的身份存取與管理的威脅挑戰

### 傳統機制現代化的挑戰

高科業製造業普遍採用 Active Directory 機制實現身份集中化控管，但隨著混合辦公、供應鏈管理與應用程式微服務化等異質環境的新興需求，傳統身份管理機制逐漸無法滿足企業成長實需。

### 身份蔓延的內部威脅風險

製造業因產業特性，內部常因業務需求而建立許多獨立、互不兼容的身份管理系統，隨著帳號數量增加，身份憑證資訊開始無法避免地在組織傳播、分散或蔓延，可能遭駭客鎖定利用，進而成為組織內部潛藏的安全風險。



### 帳號授權與生命週期管理

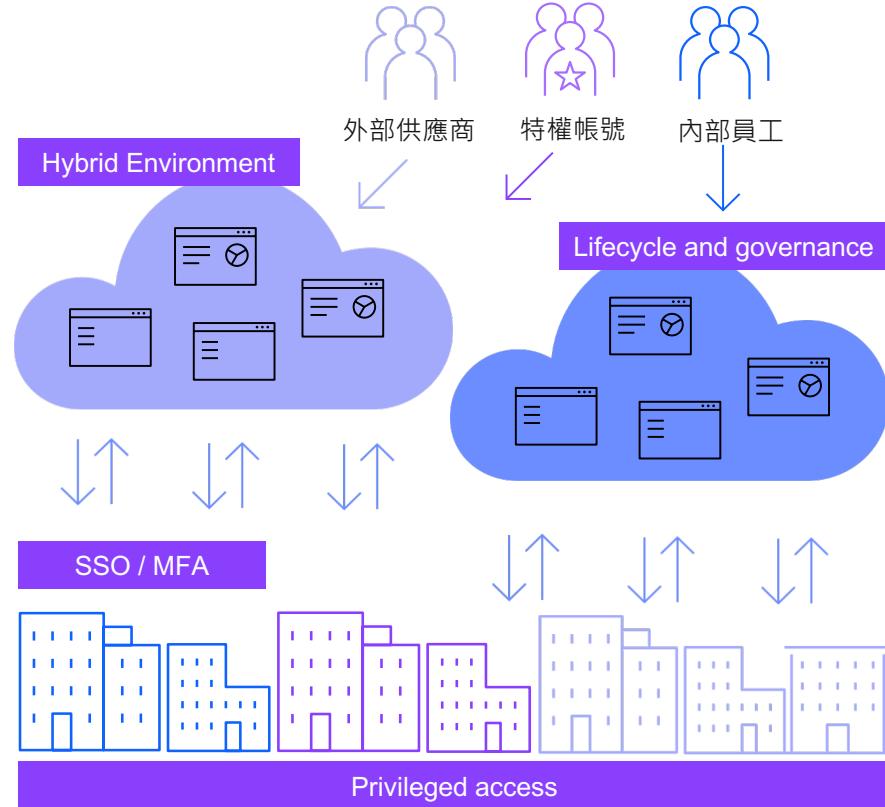
當製造業開始與時俱進引入新興科技，加上各自獨立的身份管理系統，常造成組織無法有效根據用戶、角色與職掌授予或撤銷相應權限，導致整體人員到職、調職或離職程序等員工身份帳號活動無法與企業整體身份安全管控方案相整合。

### SSO與MFA的部署挑戰

現今高科技製造業均逐漸接受並實施企業單一登入 (SSO) 與雙因子認證機制 (MFA)，來強化身份存取安全，但常因組織各自獨立的應用系統，無法有效統一部署實施，導致企業需反覆投入重複資源建立個別、不連貫的身份安全管理機制。

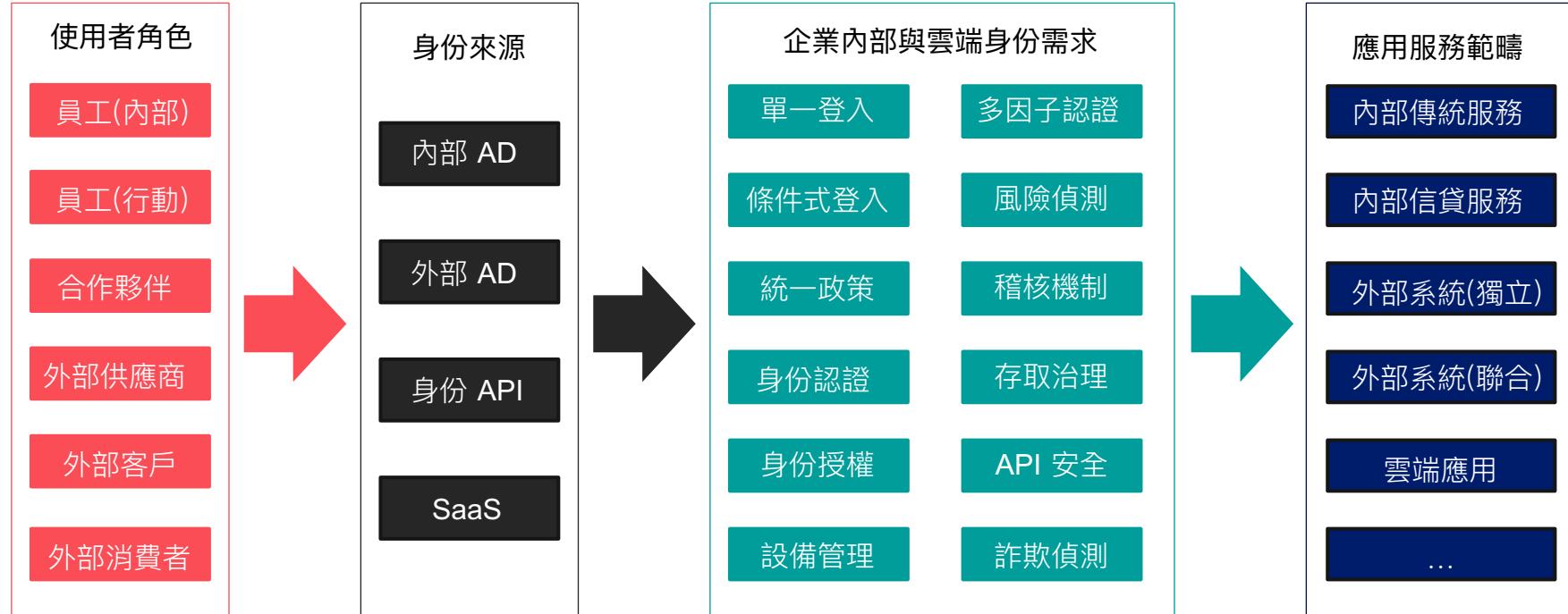
# 現代化大型企業組織身份安全管理 高科技製造業的身份存取與管理的威脅挑戰

如何透過整體化身份  
管理解決方案於地端  
、雲端環境實現單一  
登入、雙因子登入、  
特權帳號控管，以及  
帳號生命週期管理？



# 現代化大型企業組織身份安全管理

## 高科技製造業的身份存取與管理的威脅挑戰



現代化身份安全管理解決方案需針對所有類型的用戶、企業內、外部系統與雲端服務整體考量

# 現代化大型企業組織身份安全管理 端到端 (End-to-End) 一站式的身份管理解決方案



## 持續性的登入存取管控 (Access Control)



單一登入與多因子認證  
Single Sign-On and MFA



帳號生命週期管理  
Lifecycle management



條件式存取  
Adaptive access



特權帳號存取管理  
Privileged access



無密碼式認證機制  
Passwordless authentication



隱私權與同意資料管理  
Privacy and consent management



## 企業內部身份管理 Workforce Identity

推動 IT 身份管理現代化、  
技術敏捷性和用戶生產力



## 外部客戶身份管理 Consumer Identity

提供客製化、個性化和  
值得信賴的操作與登入體驗

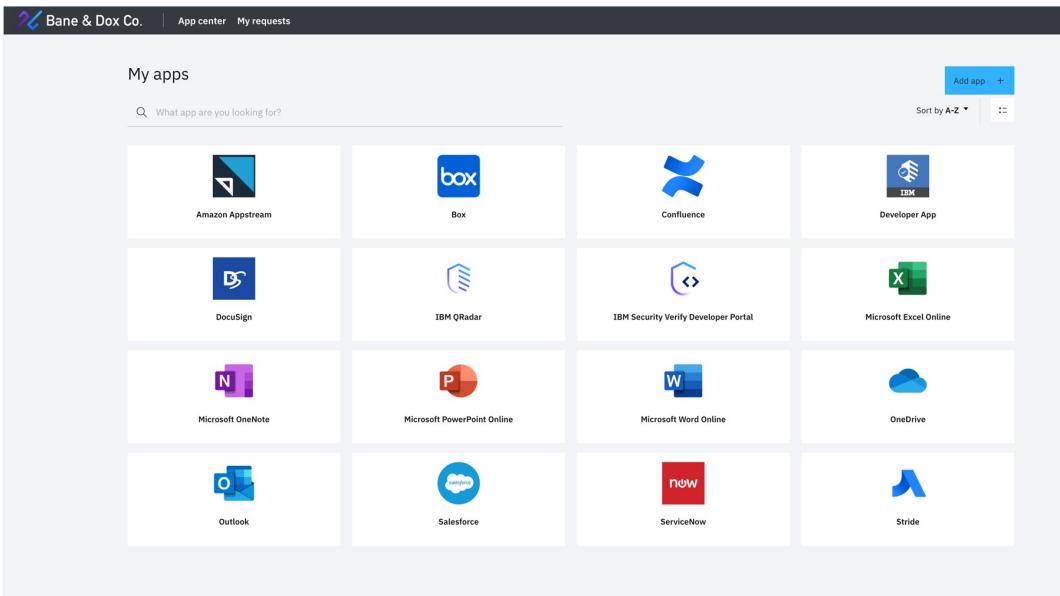
## 地端、雲端內、外部應用程式資源 (Hybrid Cloud Resources)

Cloud Apps | On-Prem Apps | Mobile Apps | Data

VPNs | Servers | Databases | Mainframes



# 現代化大型企業組織身份安全管理 端到端 (End-to-End) 一站式的身份管理解決方案



## IBM Security Verify SSO Launch Pad

讓員工輕鬆存取和授權企業組織內、  
外部工作所需的應用程序服務。

- 訪問 SaaS 或自行開發的應用服務
- 搜索與檢視企業應用服務
- 請求訪問企業應用服務
- 管理設置個人身份資料
- 註冊與啟用 MFA 設備
- 更改用戶名和密碼

# 現代化大型企業組織身份安全管理 端到端 (End-to-End) 一站式的身份管理解決方案



Two-step verification

## Choose a method

How would you like to verify it's you?

Authenticator app

TOTP

Enter code

IBM Verify app

Jessica's iPhone (Fingerprint Approval)

Jessica's iPhone (Touch Approval)

Send push

Send push

Email

Email jes\*\*\*\*\*@banedox.com

Send code

FIDO2 authenticator

Macbook Pro

Verify

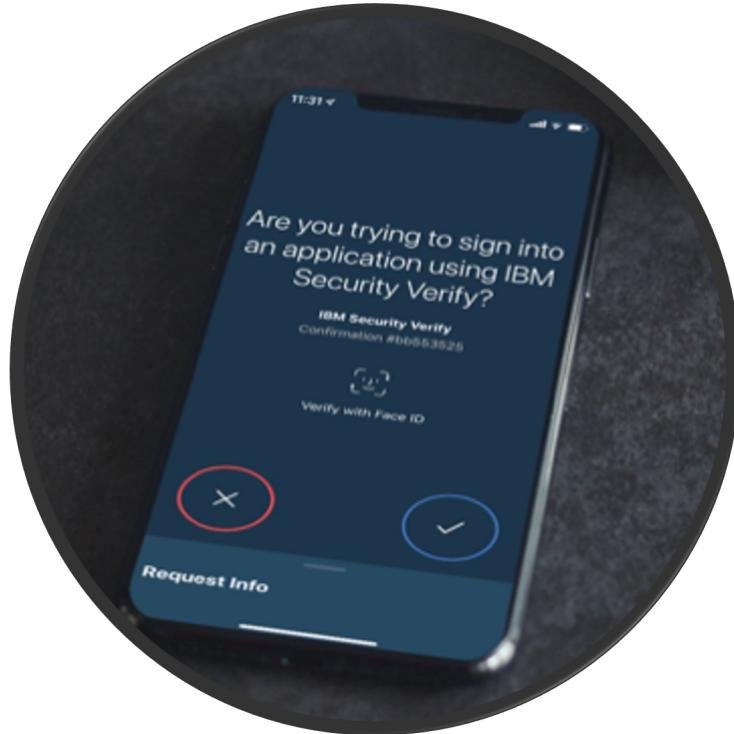
Can't use any of these verification methods? [Get help](#)

## IBM Security Verify MFA Options

提供企業組織或員工 MFA 的適用選項，例如 SMS OTP 或是 FIDO2

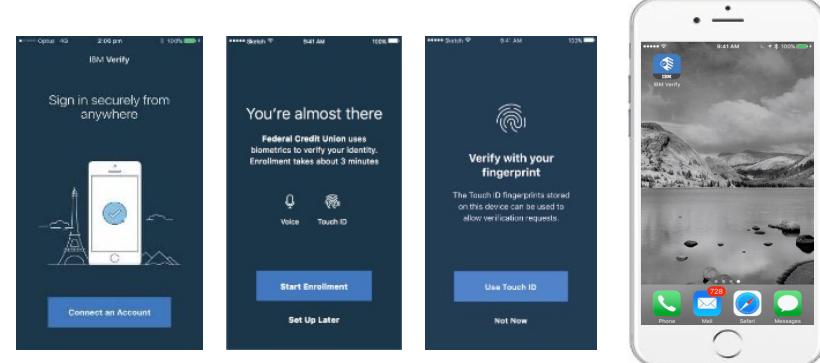
- 整合行動裝置應用程序推送基於時間的 TOTP 進行雙因子認證
- 二維碼、指紋、面部識別和 FIDO2 身份驗證器等無密碼選項 (Passwordless)
- 使用簡單、開箱即用的訪問策略或基於每個應用服務進行服務存取的政策定義
- 僅在必要時或偵測為高風險訪問時，要求用戶進行 MFA 機制認證 (條件式認證)

# 現代化大型企業組織身份安全管理 端到端 (End-to-End) 一站式的身份管理解決方案

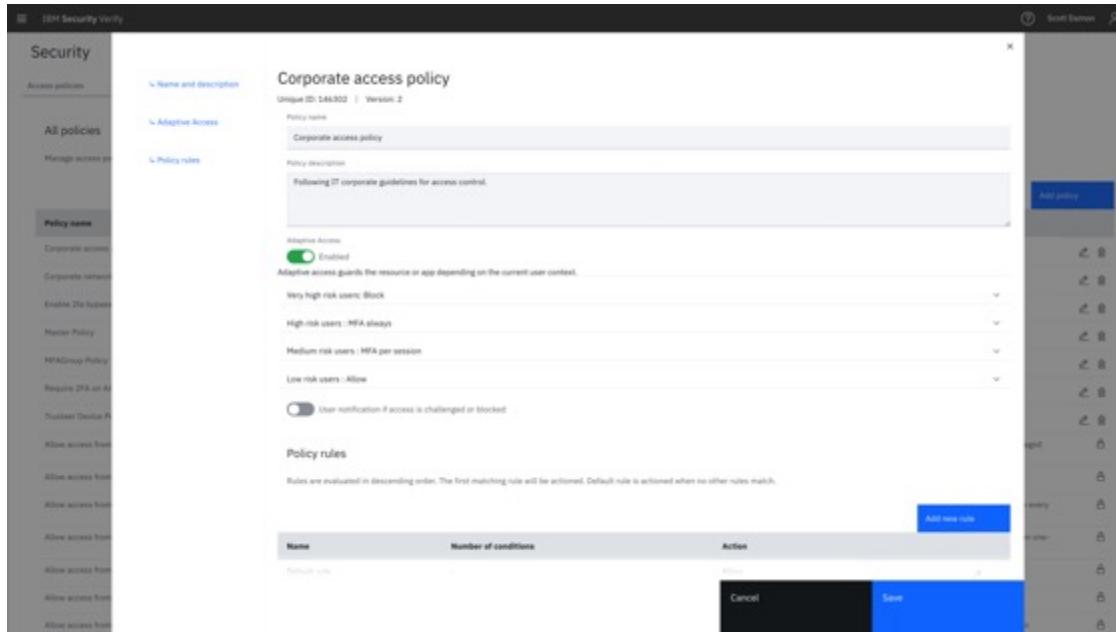


## IBM Security Verify MFA Across Resources

- 在一般性平台上利用其他 MFA 方法
- 對本地或雲端應用程序進行身份驗證
- 擴展到 VPN、Linux、AIX、Windows 桌面、Windows 服務器、IBM z 等整合 MFA



# 現代化大型企業組織身份安全管理 端到端 (End-to-End) 一站式的身份管理解決方案



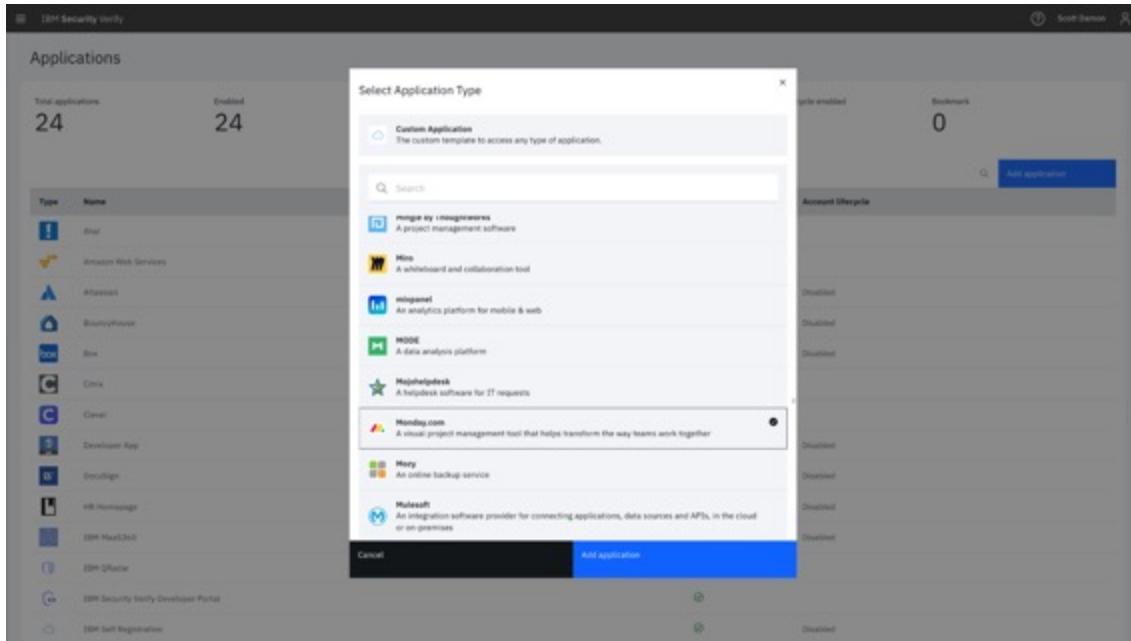
## IBM Security Verify Adaptive Access

基於風險的身份驗證的訪問策略

- 身份詐欺風險偵測保護機制和身份存取管理技術的整合。
- 深入結合用戶、設備和環境情境
- 人工智能驅動的整體風險評分
- 為低風險用戶提供無障礙訪問，同時防範高風險身份存取場景
- 僅需簡單的配置即可完成設定

# 現代化大型企業組織身份安全管理

## 端到端 (End-to-End) 一站式的身份管理解決方案



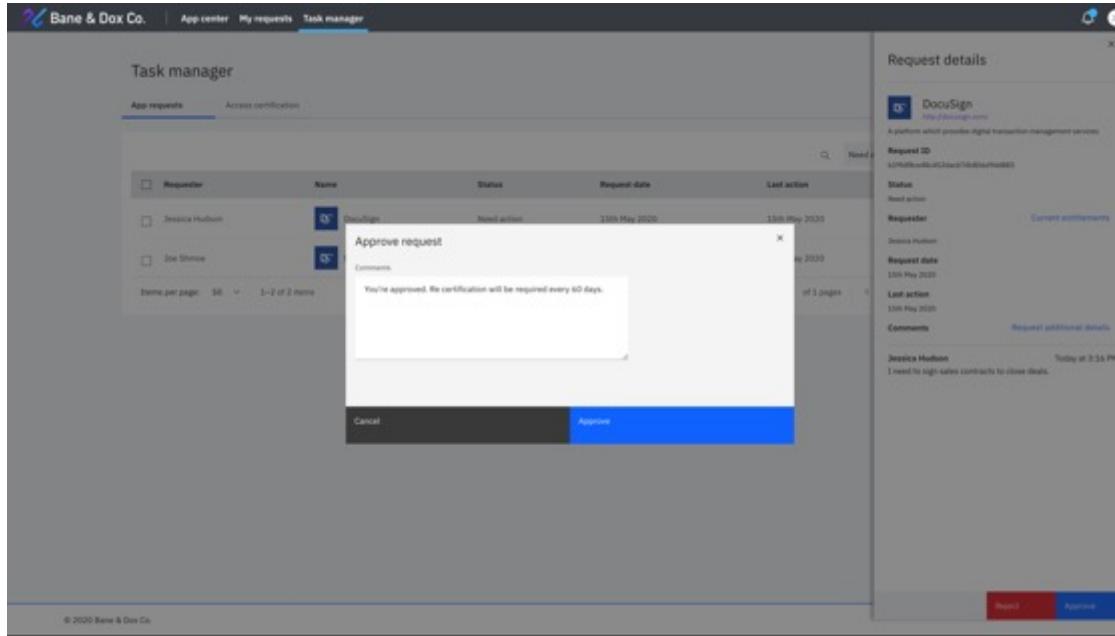
# IBM Security Verify

## Application Onboarding

在短時間內在整體身份安全  
管控系統內整合新的應用服務

- 內建支援數百個常見的 SaaS 應用快速連接器
  - 按步驟式的整合步驟與指導
  - 整合應用服務的進階屬性
  - 支援各式共通的認識協定 OAuth2、OIDC 或 SAML 2.0

# 現代化大型企業組織身份安全管理 端到端 (End-to-End) 一站式的身份管理解決方案



## IBM Security Verify Delegated Administration

釋放 IT 身份管理資源與簡化  
企業組織業務認證與授權流程

- 指定業務單位管理者或所有權者來管理特定應用服務的訪問權限
- 使管理人員能夠快速啟用人員加入應用系統團隊，而無需呼叫外部 IT 單位完成簡單的授權任務
- 加速新應用程序的採用與納管

# 現代化大型企業組織身份安全管理 端到端 (End-to-End) 一站式的身份管理解決方案

The screenshot shows the IBM Security Verify interface. On the left, a summary dashboard displays 'Total invitations' (19), a risk level distribution (Very High: 0, High: 5, Medium: 8, Low: 6), and a line chart showing the number of invitations over time. Below this are filters for Identity (User Name, Result), Source (Client IP, Location: United States, Canada, Brazil), and Event details (Risk level: Medium, Low, High). A table lists recent adaptive access events:

Time stamp	User	Risk level	Reason	Policy action	Client IP
May 12, 2022 9:27:52 AM CDT	michael.duglas.cloudIdentityrealm	High	Access with a change in device attributes	MFA always	24.28.106.72
May 12, 2022 9:27:27 AM CDT	michael.duglas.cloudIdentityrealm	Low	Access with a user behavior change	Allow	34.73.14.191.44
May 12, 2022 9:22:43 AM CDT	michael.duglas.cloudIdentityrealm	Low	Access from a known and trusted device	Allow	79.120.202.199
May 08, 2022 8:31:49 AM CDT	jia.zhishuo.cloudIdentityrealm	Low	Access from a known and trusted device	Allow	79.121.203.199
May 07, 2022 2:07:13 PM CDT	michael.duglas.cloudIdentityrealm	Low	Access from a known and trusted device	Allow	79.121.203.199
May 07, 2022 1:52:24 PM CDT	michael.duglas.cloudIdentityrealm	Low	Access from a known and trusted device	Allow	79.121.203.199

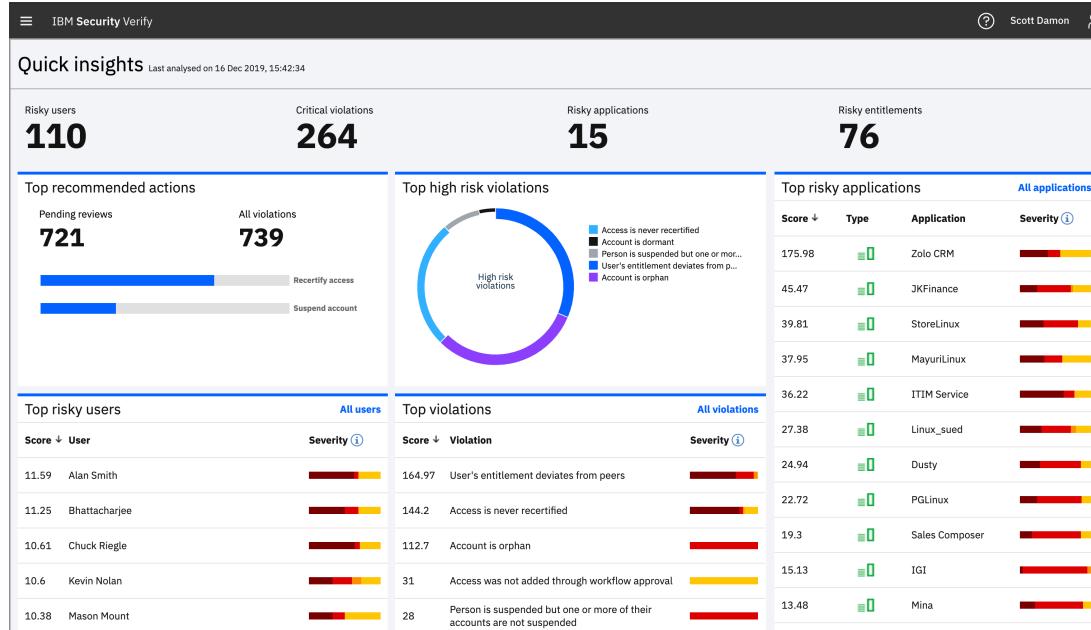
On the right, a detailed view of an 'Adaptive access event' for May 12, 2022, at 9:27:52 AM CDT, showing the identity (michael.duglas), source (Client IP: 24.28.106.72, Device details: Chrome 82.0.4064.122, Windows 10, Device type unknown, Share user agent, United States), and event details (Event type: Adaptive risk, Application name: IBMISV121205763056, Policy name: S4T40, Rule name: S4T40, Risk level: High, Policy action: Present, Reason: MFA always, Adaptive details: Reference anomaly: False, New device: True, Risky device: False, Risky connection: True, Intercept provider: Standard, Location: Austin, New location: False).

## IBM Security Verify Reporting

針對身份存取風險即時過濾、診斷與調查

- 認證活動 Authentication Activity
- 自適應訪問 Adaptive Access
- 應用程序使用 Application Usage
- 管理員活動 Admin Activity
- MFA 活動 MFA Activity
- 身份認證活動 Fulfillment activity

# 現代化大型企業組織身份安全管理 端到端 (End-to-End) 一站式的身份管理解決方案



## IBM Security Verify Identity Analytics

查看企業組織 IAM 整體運行狀況

- 使用 360 度視角掃描與身份相關的存取風險
- 同儕或同團體成員的群體分析
- 通過 AI 驅動的風險和可信度評分以挖掘潛藏風險異常情況
- 採取建議的緩解措施，例如重新檢查訪問權限或暫停特定帳戶活動

# 身份安全管控方案的導入效益

有效控管企業整體身份安全風險與強化 IT 效率

透過全面化身份安全管理降低資料外洩與資安事件發生風險

## 降低網路攻擊面

藉由實現 SSO 作為員工、外部供應商與合作夥伴存取企業內、外部資源的單一登入途徑。

## 促進企業組織資安保護

整合企業內部應用程式 MFA 機制提供第二層資訊安全保護效益。

## 降低用戶身份帳號風險

自動化執行身份帳號風險偵測，協助偵測或阻絕高風險帳號存取

節省與降低 IT 執行身份帳號日常管理操作與維護成本

## 提供身份自助管理服務

讓員工透過一定程度的自助服務解決常見的憑證管理問題，例如忘記或重置密碼，或是申請特定服務的權限開放，釋放 IT 部門日常維運。

## 分層授權身份存取申請

分層授權由相關部門經理批准員工特定層級的訪問請求，以加速整體身份授權流程、提升組織身份安全管理生產力。



# Let IBM help you accelerate

- 借助專業資安顧問和經驗豐富的技術專家加速 IAM 計劃
- 解決方案已跟數以千計的合作夥伴整合擁有良善的技術聯盟
- 20 多年 IAM 解決方案專業知識，適合大型企業部署實施

IBM Identity as a Service  
**LEADER**  
KuppingerCole's  
Leadership Compass

## IBM 身份認證與管理資安服務 (IBM Security IAM Services)

### 策略規劃與設計

#### Strategy & Design

Plan | Define | Design

### 開發合適的身份管理框架

- 使用企業營運思維設計以用戶為中心的解決方案與務實可行的遷移計劃
- 確定要配置的企業應用服務與身份功能
- 評估現有基礎設施和 IAM 流程的整合
- 使用行業最佳實務導入標準化 IAM 流程

### 部署實施與執行

#### Transformation

Build | Test | Enable

### 確保 IAM 專案成功實施

- IAM 技術與專案的快速部署
- 適配企業組織的商業與工作流程
- 使用敏捷方法快速測試、雛形化和迭代
- 降低基礎設施管理成本以建立管理階層或利益相關者投資信心
- 整合企業應用服務、配置認證與授權功能和最終用戶身份安全意識教育訓練
- 分階段實施、遷移以最大程度避免用戶服務存取中斷或遭受干擾

### 持續最佳化調適

#### Optimization

Operate | Enhance | Expand

### 提升整體投資效益

- 將熟練的商業部門成員重新引用至企業更關鍵的營運任務中導入 IAM 專案
- 完善整合員工入職、調職與申請程序
- 通過自動化 IAM 身份安全提升管理效率
- 持續收集用戶使用反饋與持續改進
- 與時俱進支援新安全技術整合

A successful IAM program requires a security strategy that combines people, process and technology.



# The Forrester Wave™: Risk-Based Authentication, Q2 2020



Forrester, The Forrester Wave™: Risk-Based Authentication, Q2 2020, Andras Cser, Merritt Maxim, Matthew Flug, and Peggy Dostie, May 2020

Disclaimer: The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™.

Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.



# Magic Quadrant for Access Management (AM), Q4 2021

Gartner®

“ Access management (AM) has become the source of trust for identity-first security. Increased dependence on identities for access anywhere, anytime, requires AM to be more reliable and easier to adopt. Identity orchestration, IAM convergence and SaaS resilience importance will increase during 2022 ”

“ IBM is a Challenger in this Magic Quadrant. Its product is offered as software (IBM Security Verify Access) and SaaS-delivered (IBM Security Verify) options, focused on a converged approach for AM and other IBM Security products. Its operations are geographically diversified, and its clients tend to be large organizations, mostly in the banking and public sector industries, looking for on-premises and hybrid deployments. ”

