# 雲端數據安全與韌性：從威脅防禦到災後復原的全面戰略

探索雲端安全風險、關鍵防禦策略與最佳復原實踐，打造穩健的數位防線


- 台灣二版　高級產品經理　盧 惠 光 (Kenneth Lo)


# 全球雲端趨勢數據 (2023-2025)

- 全球雲端市場規模 ( 2023 年：5,930 億美元 → 2025 年：7,250 億美元 )
- SaaS 市場 ( 2023: 1,952 億 → 2025: 2,500 億美元, CAGR: 13% )
- PaaS 市場 ( 2023: 1,364 億 → 2025: 1,980 億美元, CAGR: 18% )
- IaaS 市場 ( 2023: 1,503 億 → 2025: 2,190 億美元, CAGR: 24% )
- 企業雲採用率 ( 2023: 64% → 2025: 78% )
- 雲端安全投資年成長率 ( 約 15.1% )
- AI 與大語言模型在數位轉型中的關鍵作用

# 2024 重大資安事件分析

事件名稱：

## 2024 年 KADOKAWA 與 Niconico 動畫遭受網路攻擊事件

- 發生時間：2024 年 6 月 8 日 – 8 月 5 日
- 影響範圍：KADOKAWA 官方網站、Niconico 動畫平台及相關服務
- 攻擊手法：勒索軟體攻擊，攻擊者聲稱竊取 1.5TB 的商業夥伴和用戶資訊
- 影響：服務中斷、經濟損失、品牌信任受損
- 事後應對措施：企業如何復原，法規與標準的變更

# 雲端數據安全的挑戰與趨勢

- 雲端攻擊手法演進：勒索軟體即服務 (RaaS)、零信任繞過技術
- 企業雲端架構日趨複雜，資安管理難度增加
- 法規合規壓力（如 GDPR、CISA、NIS2）
- 供應鏈攻擊成為資安防禦的弱點

# 雲端安全架構概述

雲端服務分為 SaaS、PaaS、IaaS，各有不同的安全風險

企業需根據雲端架構設計適合的資安方案

需確保身份管理、資料保護、應用安全、災難復原全面覆蓋

# SaaS, PaaS, IaaS 的用戶責任與風險

| | 供應商負責 | 使用者負責 | 常見誤解 |
|---|---|---|---|
| SaaS | 基礎設施與應用 | 存取與數據安全 | 供應商負責所有安全 |
| PaaS | 運行環境 | 應用與數據 | 忽略 API 安全 |
| IaaS | 基礎架構 | 作業系統 | 未設置異地備份 |
| 所有 | 保障運行穩定性 | 合規性、存取管理 | 防火牆足夠防禦所有攻擊 |

# 從威脅防禦到災後復原的全面戰略

- **預防 ( Prevent )**
  - 透過強化身份管理 ( IAM )
  - 零信任架構 ( Zero Trust )
  - 端點防護 ( Endpoint Protection ) 來降低攻擊風險
  - 企業應實施存取控制、多因素驗證 ( MFA )、應用程式安全測試及攻擊面減少策略
- **偵測與回應 ( Detect & Respond )**
  - 建立即時監控系統，如 SIEM ( Security Information and Event Management ) 和 XDR ( Extended Detection and Response )，及早發現異常行為並快速應對 ，結合自動化與 AI 分析技術
  - 事件回應計畫 ( Incident Response Plan ) 可確保組織能夠及時處理攻擊，減少影響範圍
- **備份與復原 ( Backup & Recovery )**
  - 為關鍵數據建立異地備份與多層次備份策略，確保即使遭遇勒索軟體攻擊或硬體故障，仍可快速恢復營運
  - 企業應定期測試災難復原計畫 ( DRP ) 以確保可行性
- **解決方案與產品參考**
  - **預防 ( Prevent ) ：ESET、Penta Security、OpenLogic**
  - **偵測與回應 ( Detect & Respond ) ：JumpCloud、Senhasegura**
  - **備份與復原 ( Backup & Recovery ) ：Storware、CloudCasa、Keepit**

# 雲端安全市場趨勢與增長率

- 全球資訊安全市場規模 年增長 15.1%
  ( 2023: 1,620 億美元 → 2025: 2,120 億美元, 年增長 15.1% )
- SaaS/PaaS/IaaS 資安支出增長年增長 13-24%
  ( SaaS: 13%, PaaS: 18%, IaaS: 24% )
- 企業資安預算與投資持續增長
  ( 83% 企業計畫 2024 年增加資安預算 )
- 安全產品與解決方案正快速整合 AI 與大語言模型技術

# SaaS ( Software as a Service ) 的安全風險與應對

## 帳號外洩與未授權存取

- 風險：
憑證洩露可能導致駭客獲取企業機密數據

- 解決方案：
  - 啟用 **多因素驗證 ( MFA )**
  - 使用 **身份存取管理 ( IAM )** 來控制權限 ( JumpCloud, Senhasegura )

## 數據丟失與不可逆刪除

- 風險：
內部員工錯誤刪除數據或 SaaS 提供商故障可能導致數據遺失

- 解決方案：
  - 建立 **定期備份策略**，使用 **異地備份** ( Keepit )
  - 啟用版本控制與回溯機制，確保數據

## API 安全風險

- 風險：

不安全的 API 可能成為駭客攻擊的入口，
允許未授權存取數據

- 解決方案：
  - 限制 API 權限，採用 **零信任原則 ( Zero Trust )**
  - 使用 **API 安全防護** ( Penta Security )

## 合規與法規挑戰

- 風險：

不同區域的 SaaS 法規 ( 如 GDPR、CCPA )
可能對數據存儲與傳輸有不同要求

- 解決方案：
  - 確保 SaaS 供應商符合 **ISO 27001、SOC 2** 等標準
  - 使用加密技術保護數據隱私

# PaaS (Platform as a Service) 的開發與部署安全

## 應用程式漏洞

- 風險：
未經安全測試的應用可能含有漏洞，成為駭客攻擊的目標

- 解決方案：
  - **安全程式開發生命周期 ( SDLC )**：落實 DevSecOps，確保每個開發階段都進行安全測試
  - 使用 **自動化安全掃描工具** ( 如 SAST、DAST ) 來檢測漏洞

## 開源庫與依賴風險

- 風險：
使用過時或含有已知漏洞的開源庫可能引入安全風險

- 解決方案：
  - 建立 **軟體組成分析 ( SCA )**，定期審查開源庫的安全性
  - 使用 **開源安全管理工具** ( OpenLogic ) 來確保依賴組件安全

## API 存取風險

- 風險：
未受保護的 API 可能被駭客利用進行攻擊，如 API 濫用或數據竊取

- 解決方案：
  - 實施 **API 限流 ( Rate Limiting )** 來防止濫用
  - 使用 **身份驗證與授權機制** ( 如 OAuth 2.0、JWT ) 來限制 API 存取
  - 採用 **API 安全防護技術** ( Penta Security ) 來強化 API 安全

## 運行環境錯誤配置

- 風險：
雲端環境中的錯誤配置 ( 如公開儲存桶、過寬的權限 ) 可能導致數據外洩

- 解決方案：
  - 定期審查 **雲端資源設定 ( Cloud Security Posture Management, CSPM )** 使用 **基於角色的存取控制 ( RBAC )** 來限制權限
  - 自動檢測與修復錯誤配置，確保符合安全標準

## 供應鏈安全風險

- 風險：
開發流程中可能受到供應鏈攻擊，如惡意程式碼注入或 CI/CD 流程中的安全漏洞

- 解決方案：
  - 建立 **零信任架構 Zero Trust ( JumpCloud )**，確保所有開發環境均受到監控
  - 使用 **代碼簽名 ( Code Signing )** 來驗證應用程式的完整性
  - 採用 **CI/CD 安全工具** 來監測與防禦供應鏈攻擊

# IaaS (Infrastructure as a Service) 的基礎架構安全

## 錯誤配置 (Misconfiguration)

- 風險：
公開存儲桶、過度開放的安全群組 ( Security Groups )、未加密的數據存儲

- 解決方案：
  - 使用 **基礎架構即代碼 ( IaC ) 安全策略** 確保配置標準化
  - 部署 **Cloud Security Posture Management ( CSPM )** 來自動檢測並修復錯誤配置
  - 啟用 **數據加密 ( Encryption at Rest & in Transit )** 確保數據機密性

## DDoS 攻擊 (Distributed Denial-of-Service)

- 風險：
攻擊者發送大量流量導致 IaaS 服務癱瘓，影響業務運營

- 解決方案：
  - 啟用 **DDoS 防護服務** (如 AWS Shield, Cloudflare, Azure DDoS Protection)
  - 設定 **速率限制 ( Rate Limiting )**，防止惡意流量淹沒伺服器
  - 使用 **WAF ( Penta Security )** 來過濾異常流量

## 雲端監控與威脅偵測不足

- 風險：

企業缺乏對 IaaS 環境的即時監控，導致攻擊或異常行為無法被及時發現

- 解決方案：
  - 部署 **SIEM ( Graylog )** 進行日誌監控與異常偵測
    使用 **威脅檢測與回應工具 XDR, EDR ( ESET )**來分析並回應潛在威脅
  - 建立 **自動警報機制**，確保安全團隊能即時應對異常事件

## 運行環境錯誤配置

- 風險：

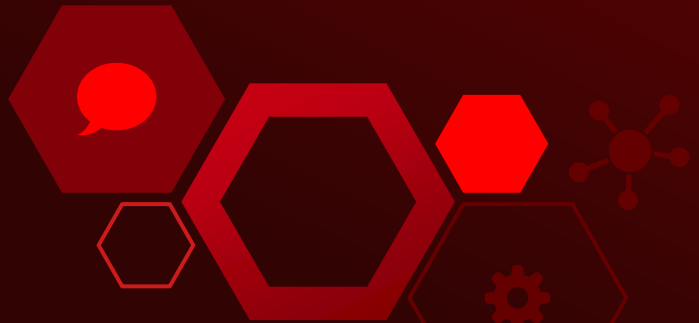
未加密的數據存儲、未設置適當的存取控制，可能導致數據外洩

- 解決方案：
  - 使用 **端到端數據加密 ( End-to-End Encryption )** 來確保數據安全
  - 啟用 **自動化備份策略 ( Storware , CloudCasa )** 來確保數據可恢復
  - 設定 **對象存儲 (Object Storage) 的存取權限**，確保數據僅授權人員可讀取

# 雲端安全策略的整合與協同防禦

- 如何將 SaaS、PaaS、IaaS 安全防禦結合，形成完整防護
- 強化零信任架構，確保存取控制與身份驗證
- 多層次備份與災難復原計畫，確保業務不中斷

# 產品展示與實際案例分析



- 產品展示與實際案例分析

# ESET 企業資安解決方案

## 端點防護

- 利用 AI 驅動的行為監控，快速偵測並攔截異常進程
- 自動化反應機制，有效防禦勒索軟體與零日攻擊

## 勒索軟體防禦

- 實時攔截可疑行為，縮短威脅暴露時間
- 定期更新病毒庫與威脅情報，確保防護措施及時升級

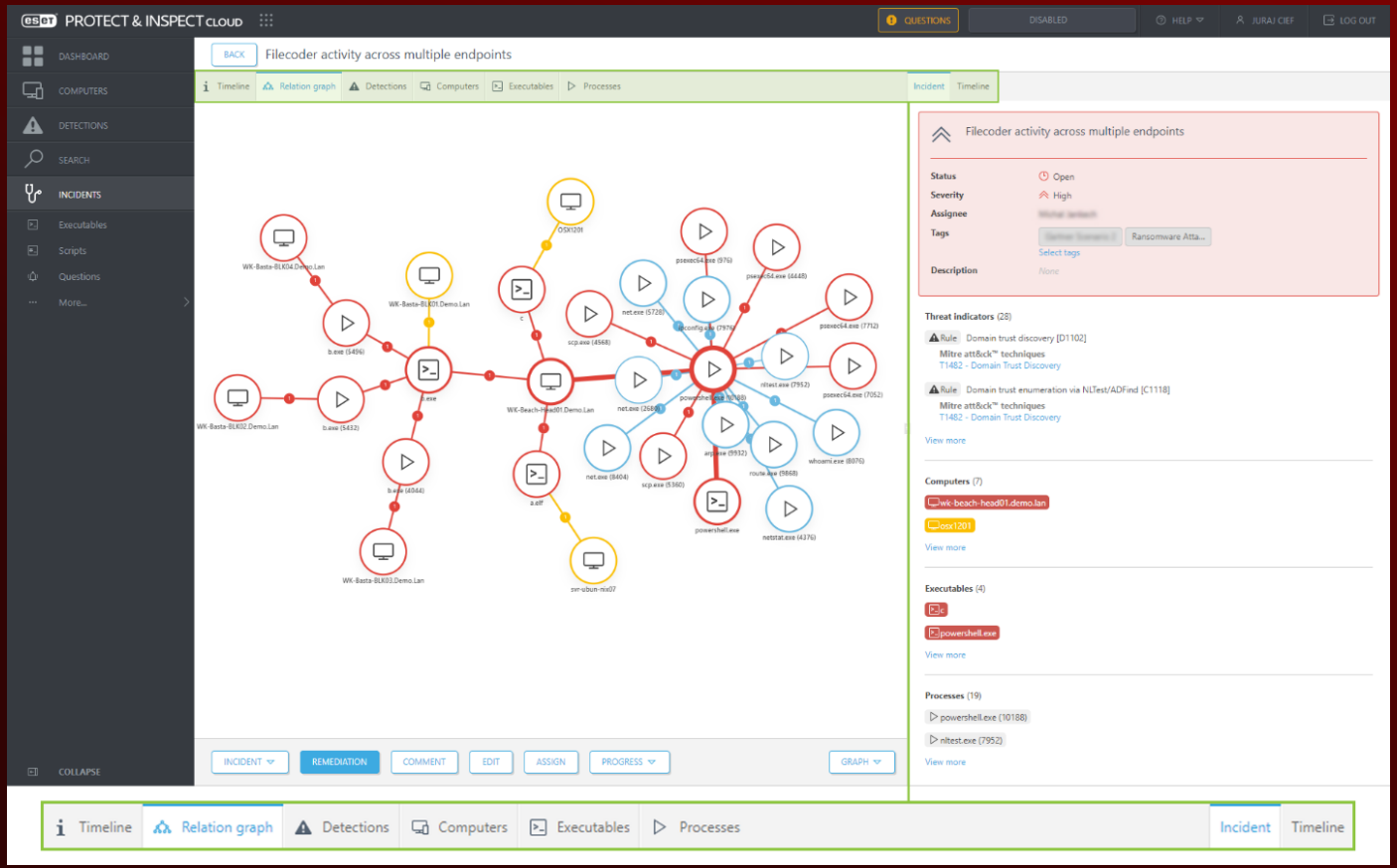
## 企業端點管理

- 集中管理所有端點，統一部署安全策略
- 透過定期審計與監控，確保各項安全配置符合標準

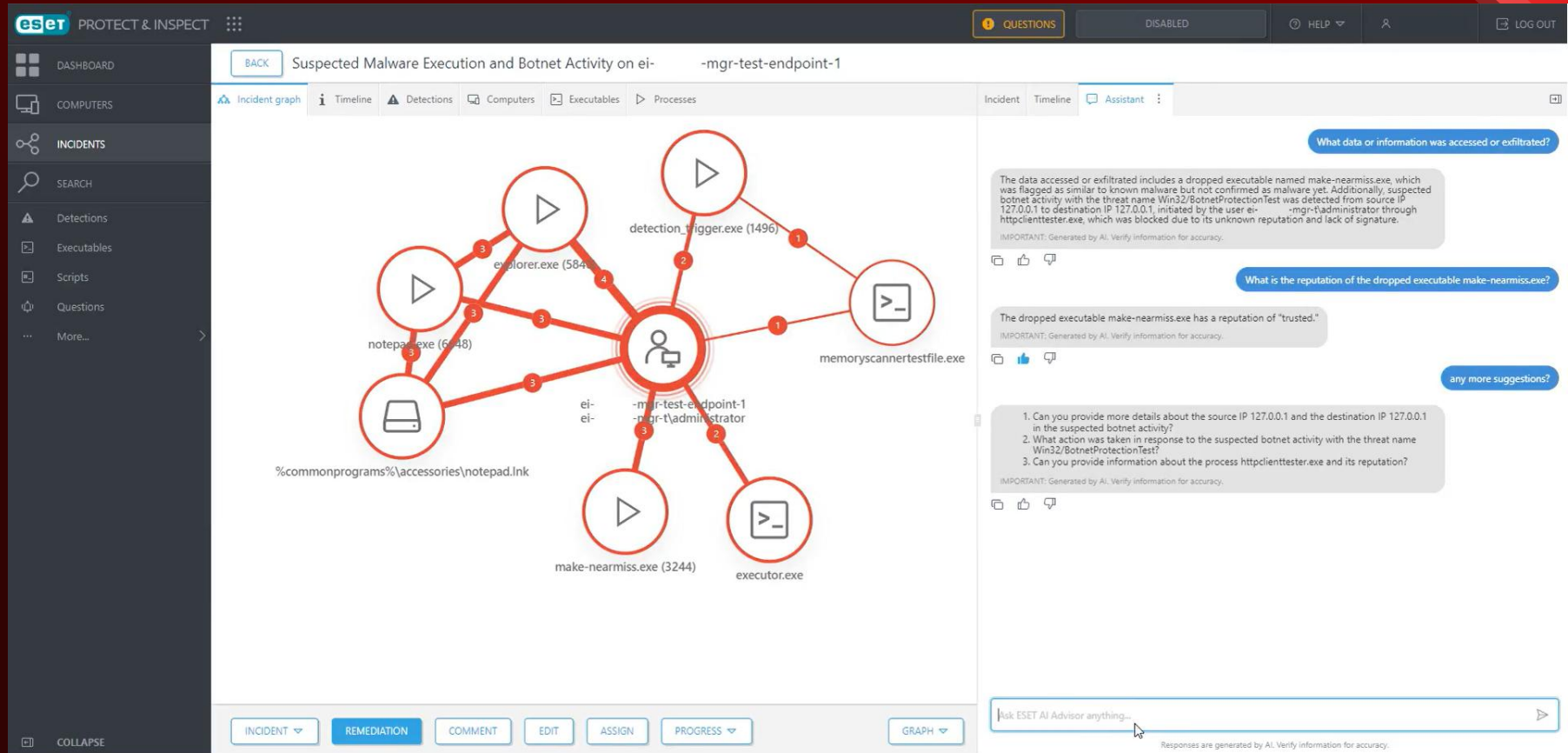
## 雲端資安整合

- 與其他安全工具無縫連接，形成全方位防護體系
- 整合身份管理、數據保護與配置審查，降低跨平台風險

# ESET 企業資安解決方案



# ESET 企業資安解決方案



- 產品展示與實際案例分析

# Penta Security


## WAF 防禦

- 高效流量過濾，實時監控並攔截惡意攻擊（如 DDoS、應用層攻擊）
- 自動化規則更新，應對最新攻擊手法

## 應用程式與 API 安全

- 實加強 API 管控，防止未授權存取與數據洩露
- 整合自動化漏洞掃描工具，及時發現與修補安全漏洞

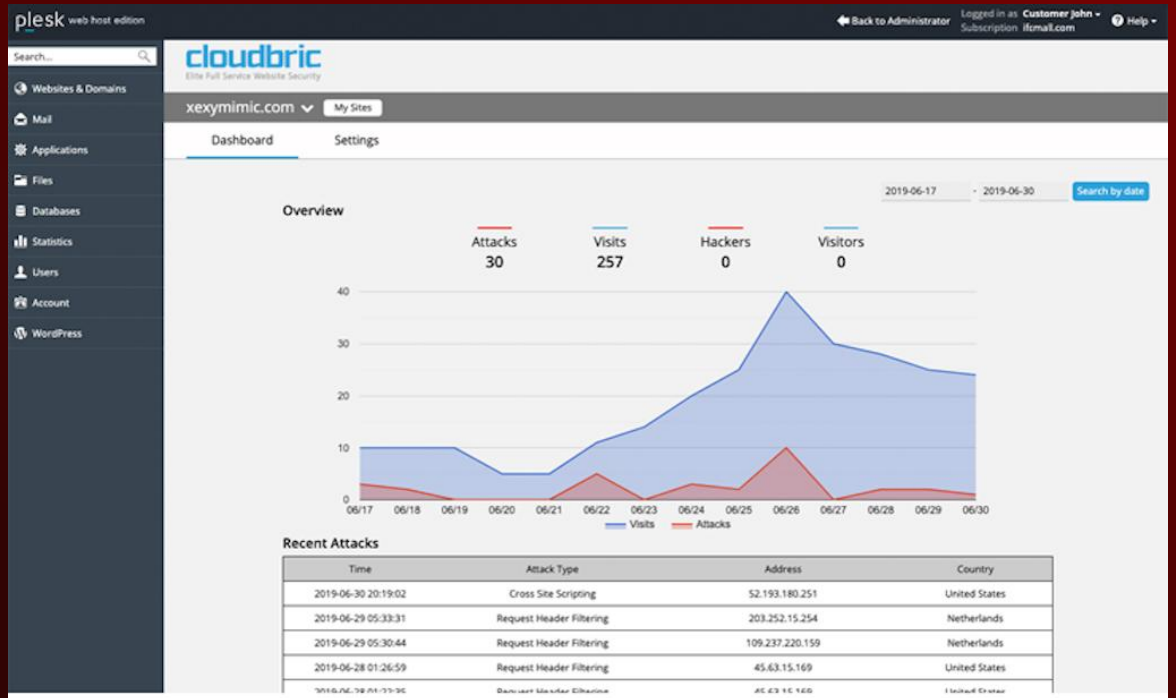
## 資料庫加密技術

- 採用先進加密技術保護靜態與傳輸中的數據
- 自動化密鑰管理機制，降低人為操作風險

## 雲端資安整合

- 強化 API 安全與數據保護，降低錯誤配置與資料洩露風險
- 持續監控與安全掃描確保系統始終處於最新防護狀態

# Penta Security – CloudBric 雲端防護解決方案




See detailed attack information from
our intuitive dashboard as and when they happen.

- 產品展示與實際案例分析

# JumpCloud 雲端身份驗證目錄解決方案


## IAM 與設備信任管理

- 集中管理身份認證，實現自動化角色與權限分配
- 定期評估設備信任狀況，確保連接端點安全

## 多因素驗證 (MFA)

- 增加登入安全層級，有效降低帳號外洩與未授權存取風險
- 支援多種驗證方式，靈活適應各種業務場景

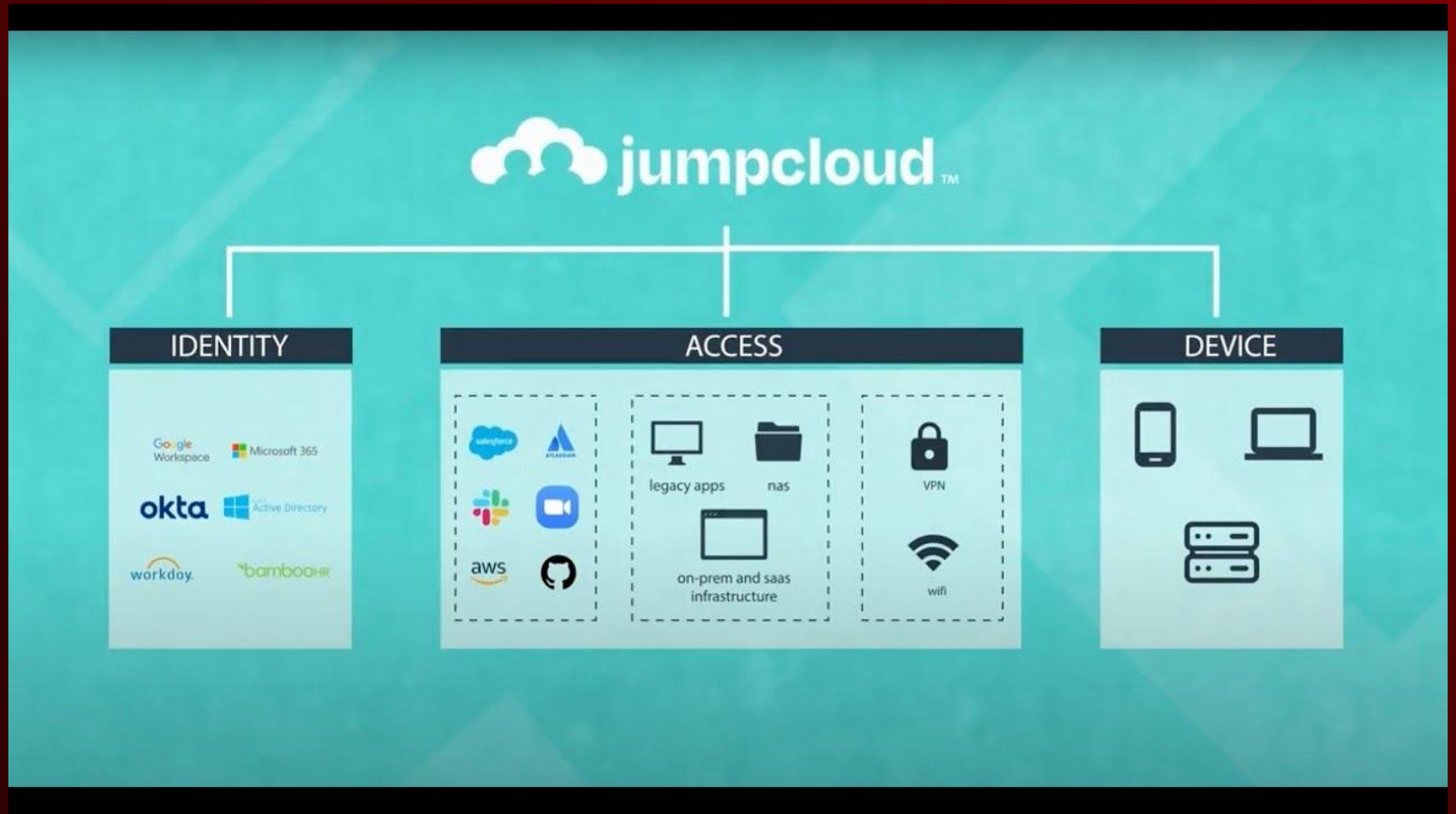
## 企業身份存取管理

- 實施最小權限原則，防止過度開放的存取權限
- 實時監控與審計，迅速發現異常行為並啟動應急預案

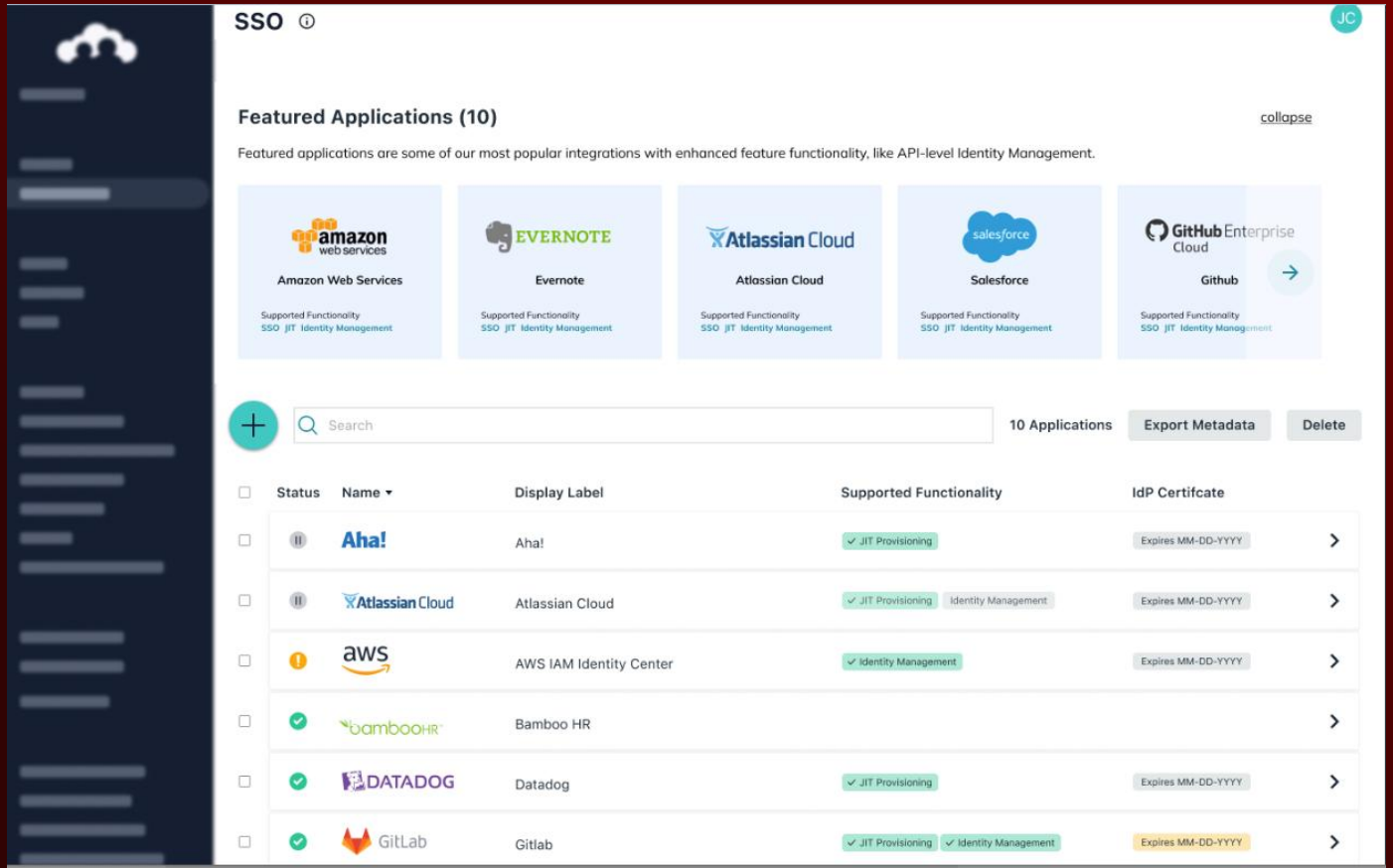
## 風險與解決回饋

- 有效應對身份與存取管理風險，確保用戶與設備安全
- 透過自動化監控及時調整安全策略，降低內部威脅發生率

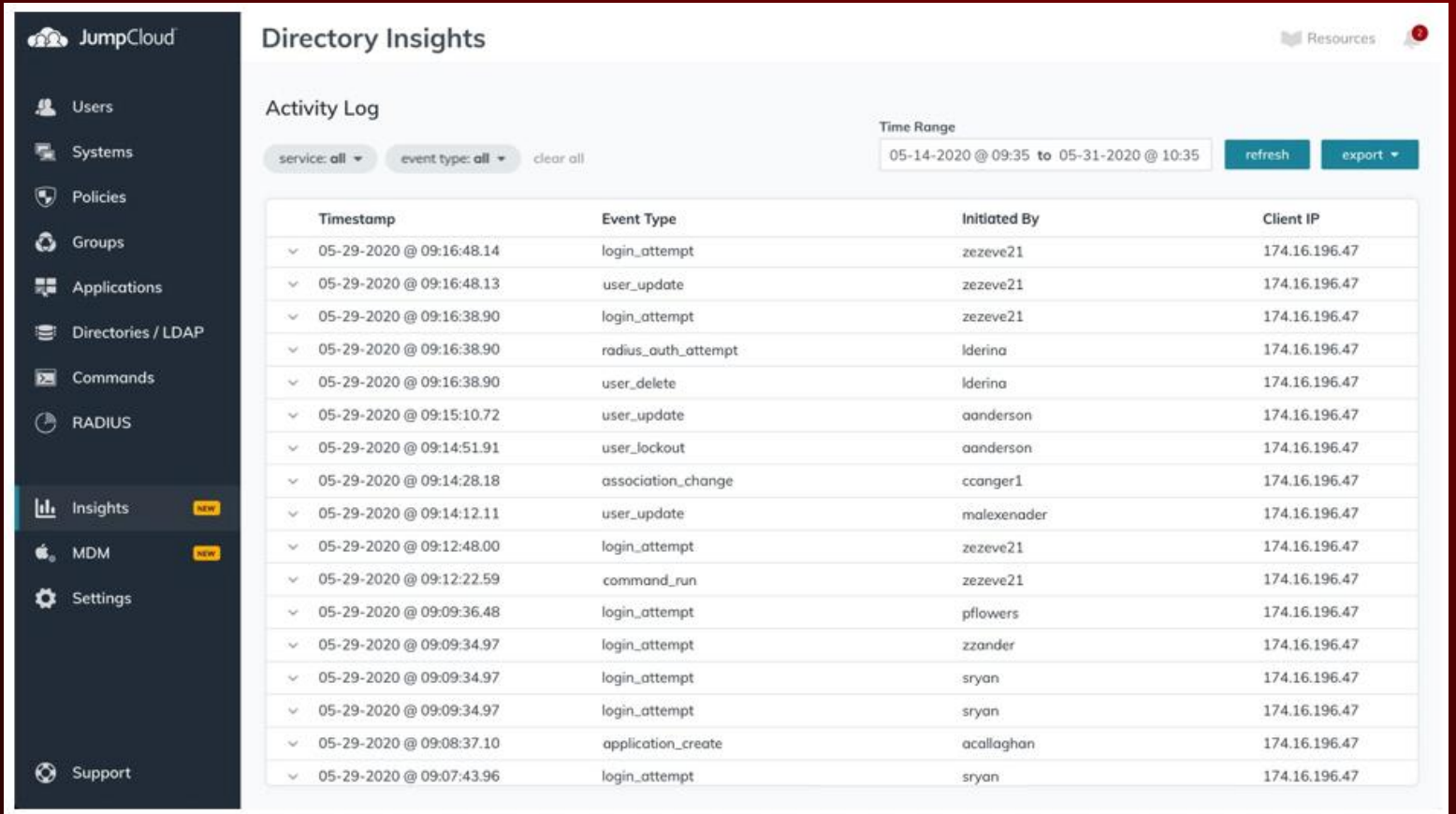
# JumpCloud 雲端身份驗證目錄解決方案



# JumpCloud 雲端身份驗證目錄解決方案



# JumpCloud 雲端身份驗證目錄解決方案



- 產品展示與實際案例分析

# Storware 數據備份&還原解決方案

## 企業級多雲備份與即時災難復原解決方案

### ◇ 雲端備份與復原

- 自動化備份策略：支持無代理與代理式備份，滿足不同虛擬化環境需求
- 增量備份與資料去重技術：降低存儲成本，縮短恢復時間
- 高效加密與壓縮：保護數據安全，同時優化備份存儲空間

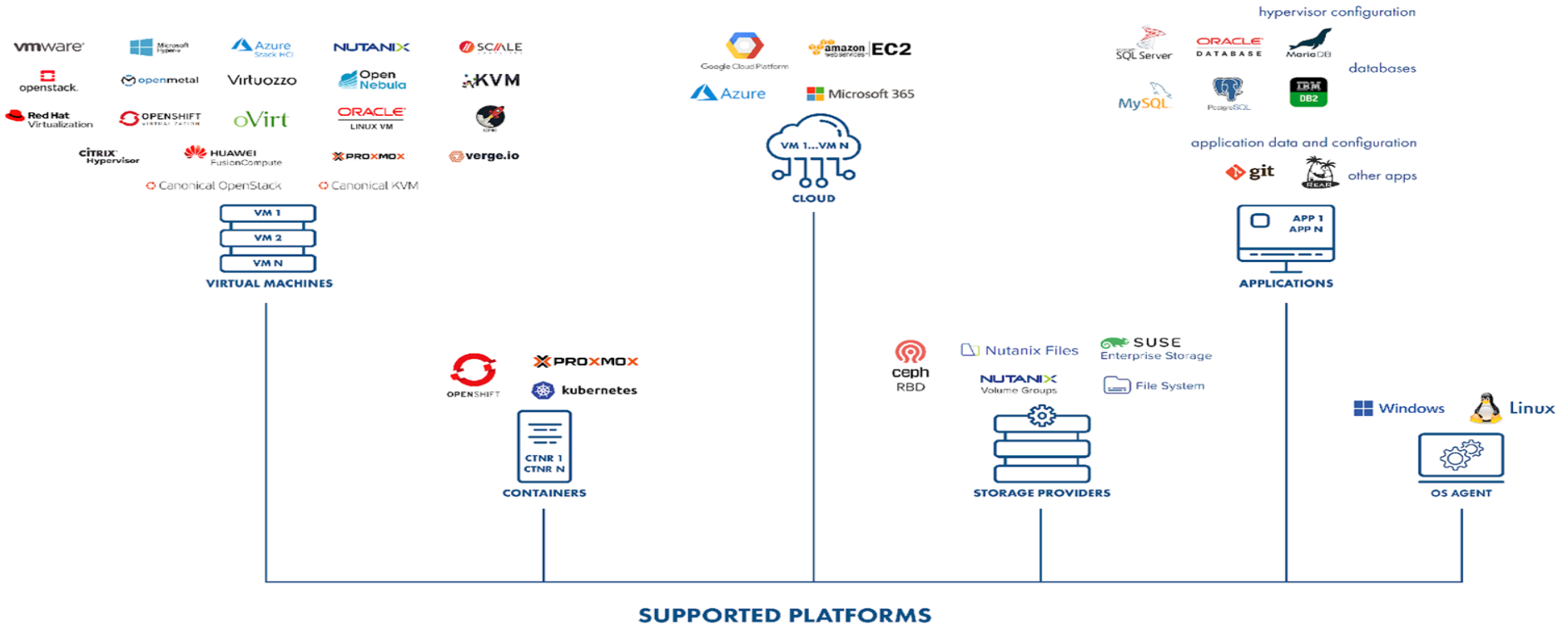
### ◇ 異地備份與災難復原

- 多雲環境整合：支持 AWS S3、Azure Blob、私有雲與本地存儲的無縫連接
- 自動化災難復原演練：縮短 RTO 與 RPO，確保業務持續運作

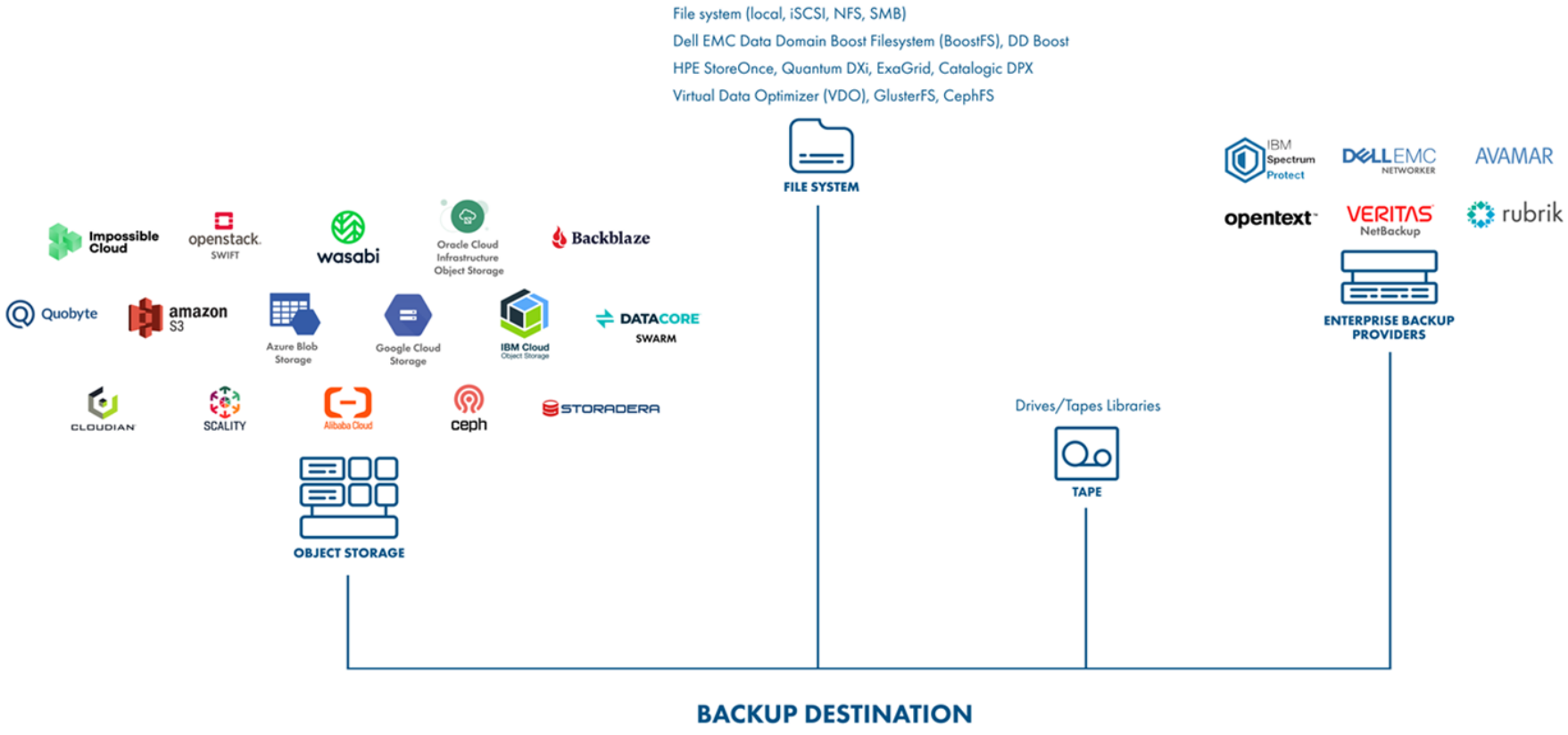
### ◇ 產品特色回饋風險與解決方案

- 統一管理平台：實時監控與報告，便於合規審計，降低配置錯誤風險
- 多種虛擬化支持：適用於 VMware、Hyper-V、KVM 等，保障各類工作負載數據安全
- API 整合能力：方便與其他資安工具和自動化系統無縫連接，提升整體防禦效率實施最小權限原則，防止過度開放的存取權限

# Storware 數據備份&還原解決方案



# Storware 數據備份&還原解決方案



- 產品展示與實際案例分析

# CloudCasa 備份&還原解決方案

## 容器化環境與雲原生應用數據保護平台

### ◇ 雲端備份與復原策略

- 策略驅動自動化：簡化備份流程，確保關鍵數據定時、完整保存
- 高頻率備份與快速恢復：縮短業務中斷時間，滿足即時恢復需求
- 內建加密保護：確保數據在傳輸與存儲過程中的安全性

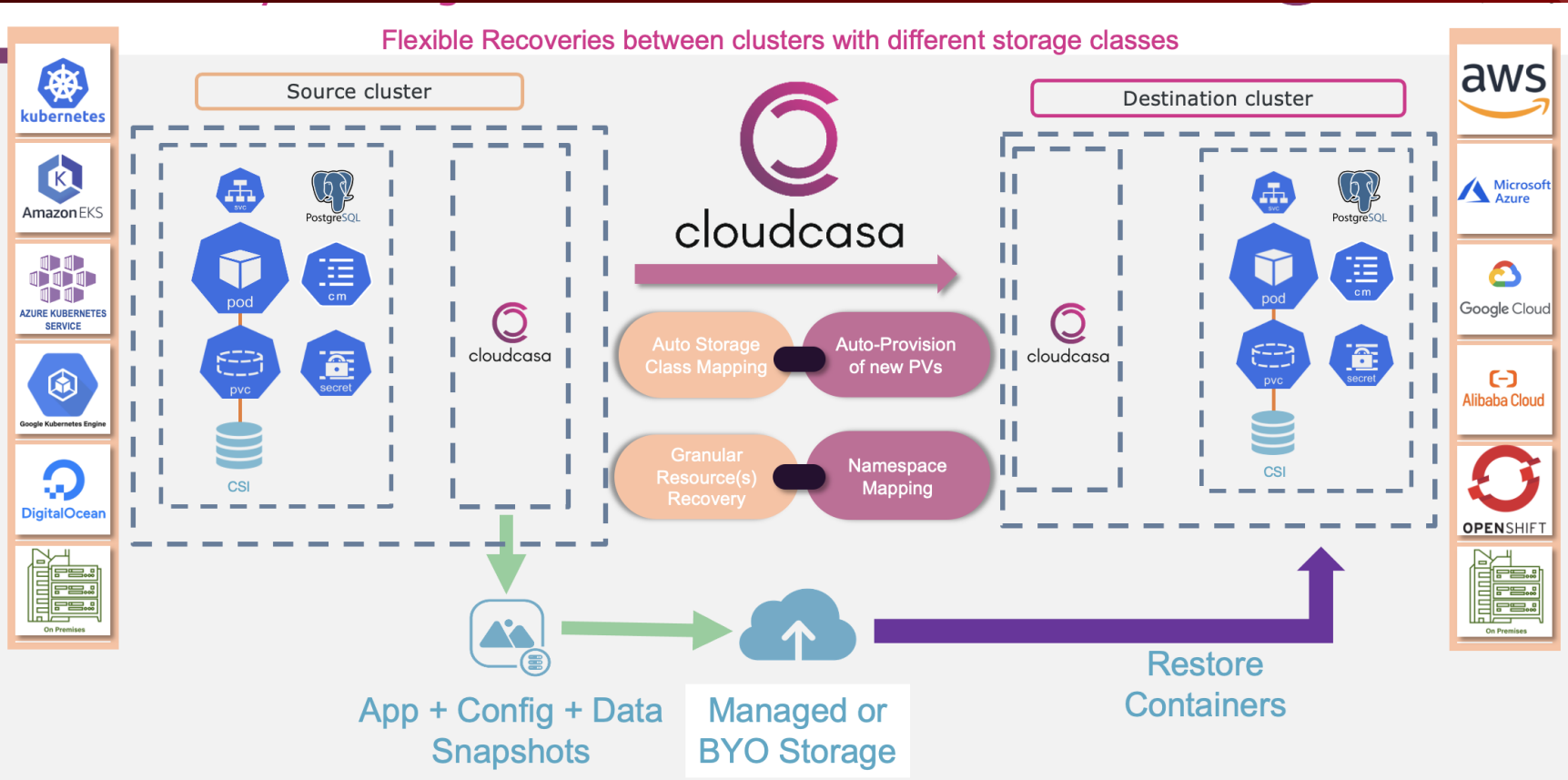
### ◇ Kubernetes 企業級保護

- 原生支持 Kubernetes：專為容器化設計，確保容器內應用數據一致性
- 跨雲平台支持：整合 AWS、Azure、GCP 等主要平台，實現跨平台備份
- 應用感知功能：自動識別關鍵應用，保障數據完整性與連續性

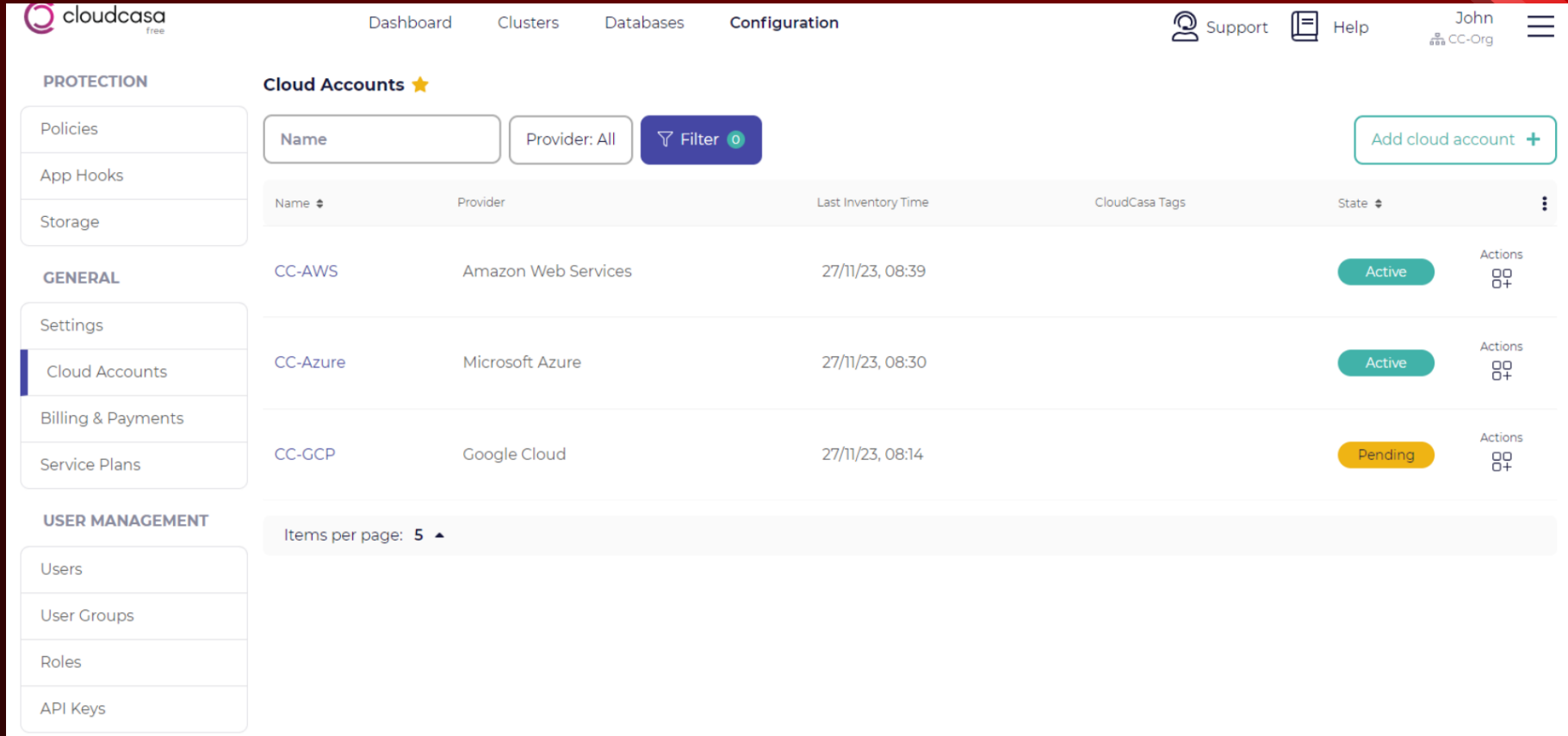
### ◇ 產品特色與安全防護回饋

- 易用網頁儀表板：提供實時監控、報告與預警，便於管理與決策
- API 接口整合：方便與現有安全監控與管理系統連結，提升自動化程度
- 完整恢復流程：支持細粒度與全系統恢復，降低數據丟失風險

# CloudCasa 備份&還原解決方案



# CloudCasa 備份&還原解決方案



# 結論與 Q&A

- 雲端安全與韌性是企業數據保護的核心
- 需要端到端整合防禦策略與自動化應對方案
- 選擇適合的工具與技術，提升企業應對能力

Version 2 台灣二版
www.version-2.com.tw

展攤號碼：
1F / Q304

V2資源中心 QRcode

# 台灣總代理-台灣二版
# 資安解決方案

| | | | |
|---|---|---|---|
| cloudcasa by Catalogic | 雲端備份&還原解決方案 | OpenLogic by Perforce | 開源資安諮詢服務 |
| eset | ESET企業資安解決方案 | Penta SECURITY | 網路應用防火牆解決方案 |
| jumpcloud | 雲端身份驗證目錄解決方案 | senhasegura | 特權帳號管理解決方案 |
| keepit | 雲端備份&還原解決方案 | storware | 數據備份&還原解決方案 |