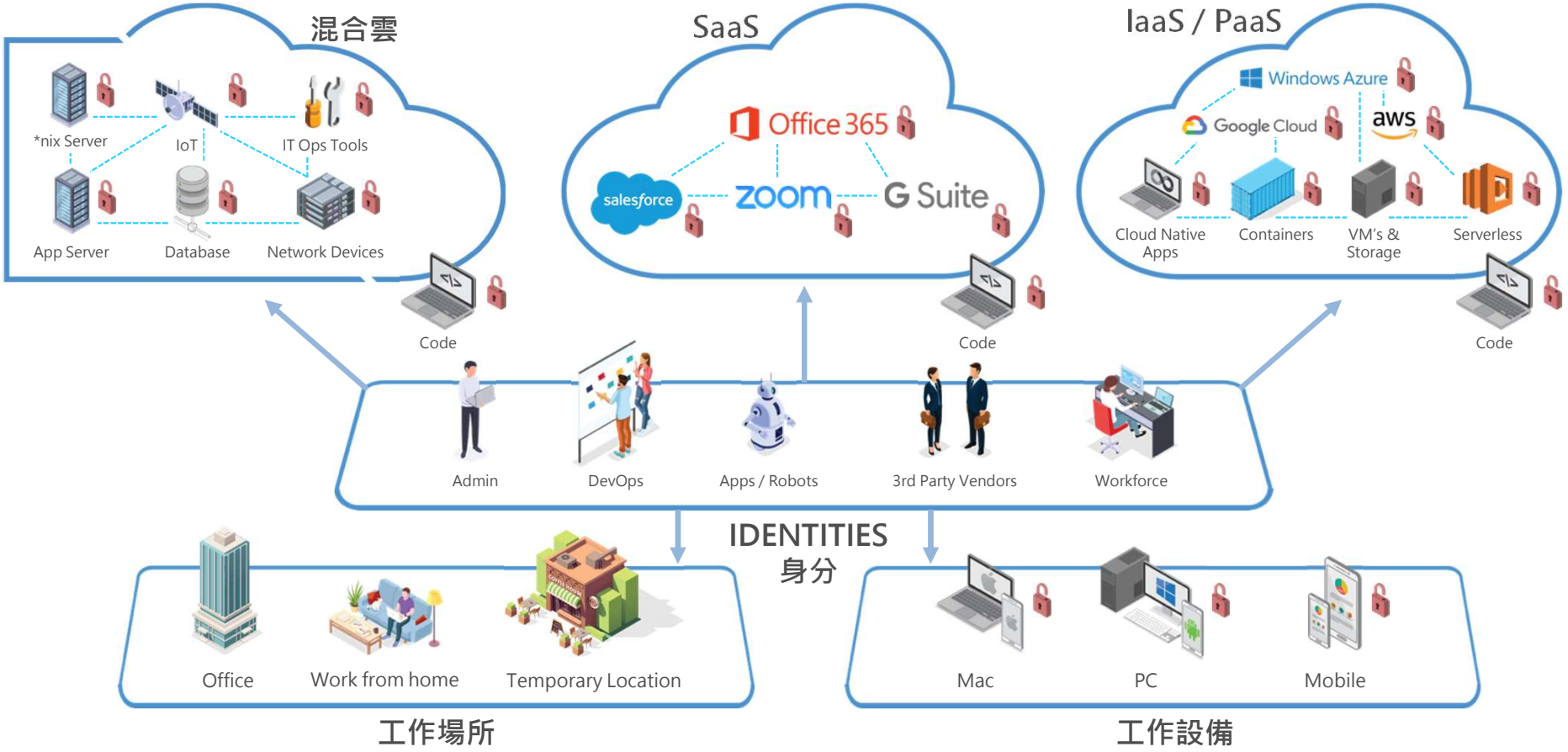
CYBERARK®

建構一致性雲平台與DevOps的身分安全環境

陳鳴豪 Bryant Chan
技術顧問

Nov 2021

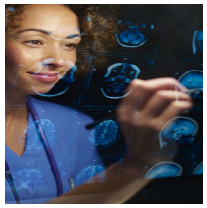
現代企業與身分關聯


混合雲
*nix Server
IoT
IT Ops Tools
App Server
Database
Network Devices
Code
SaaS
Office 365
salesforce
zoom
G Suite
Code
IaaS / PaaS
Windows Azure
Google Cloud
aws
Cloud Native Apps
Containers
VM's & Storage
Serverless
Code
Admin
DevOps
Apps / Robots
3rd Party Vendors
Workforce
IDENTITIES
身分
Office
Work from home
Temporary Location
工作場所
Mac
PC
Mobile
工作設備

CyberArk's Mission

Provide a modern approach to **IDENTITY SECURITY** anchored on privilege to protect against advanced cyber threats

無邊界成為身分已成為挑戰

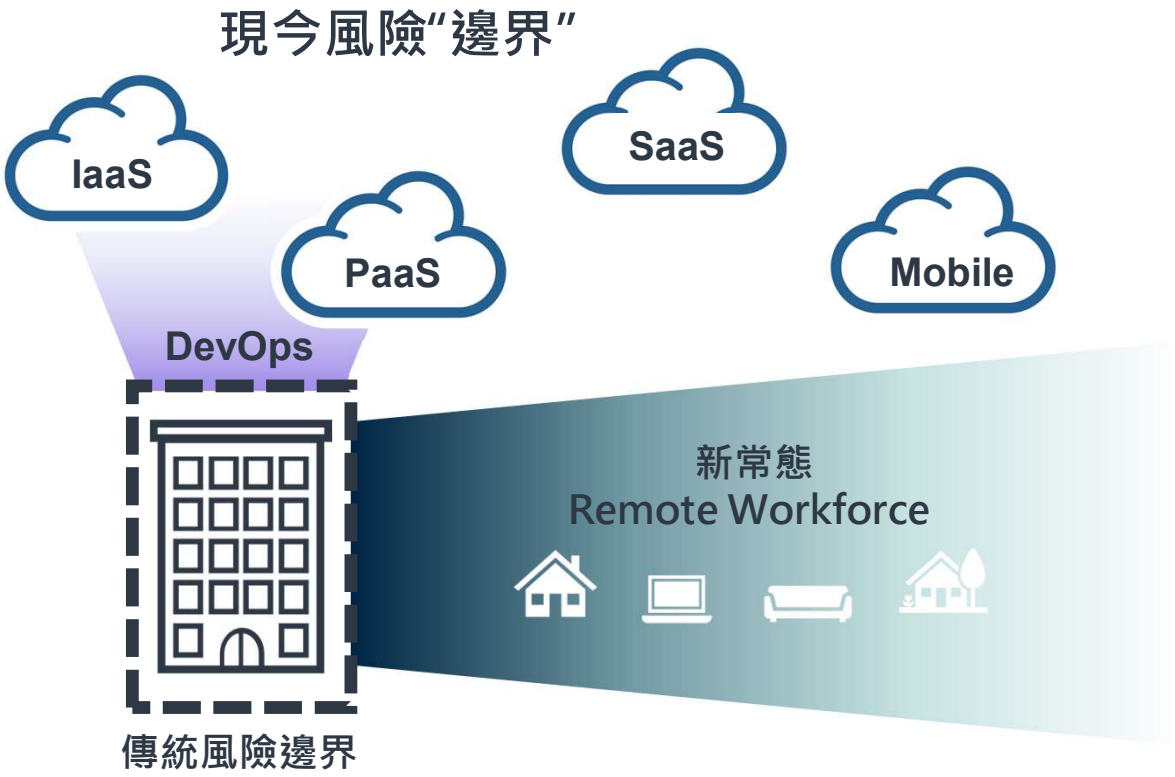


數位轉型正在加速進行中

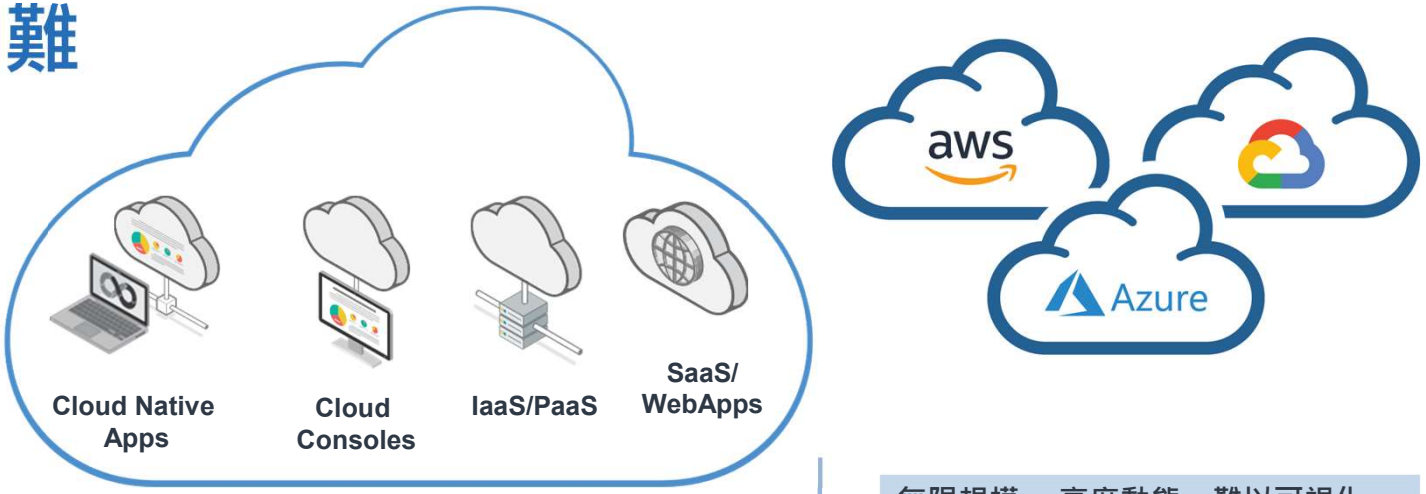
運營效率: 遠程勞動力和第三方協同合作者成長

合規和稽核的要求及新標準

風險的降低



雲服務資安的困難



無限規模； 高度動態，難以可視化、追蹤和管理

CLOUD SECURITY

ENTITLEMENTS

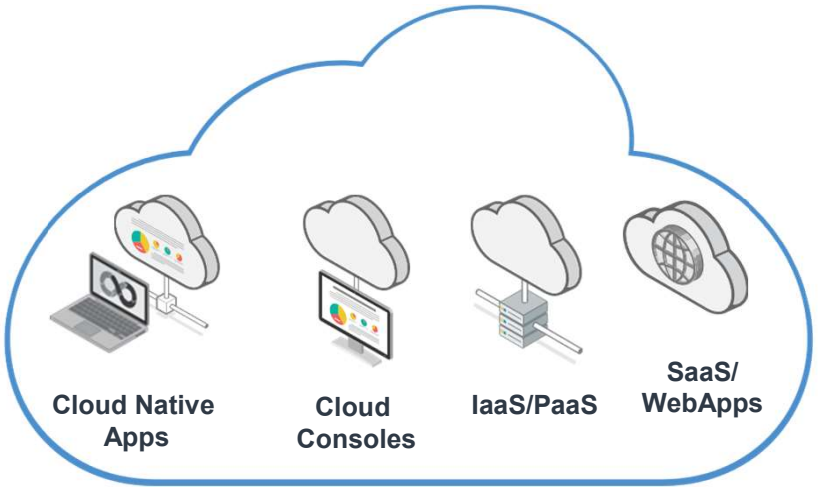
各雲平台擁有成千上萬的權限；難以可視化和管理。

DevOps 團隊跑得很快，很難實施資訊安全。

如何對身分管理能提供一致性及驅動的跨雲存取

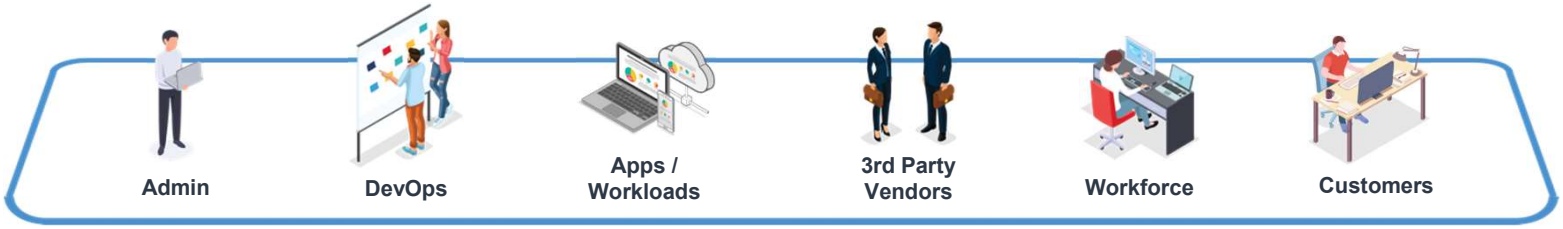
IDENTITIES IN THE CLOUD AND ON-PREM

“雲”重道遠



TO-DO LIST

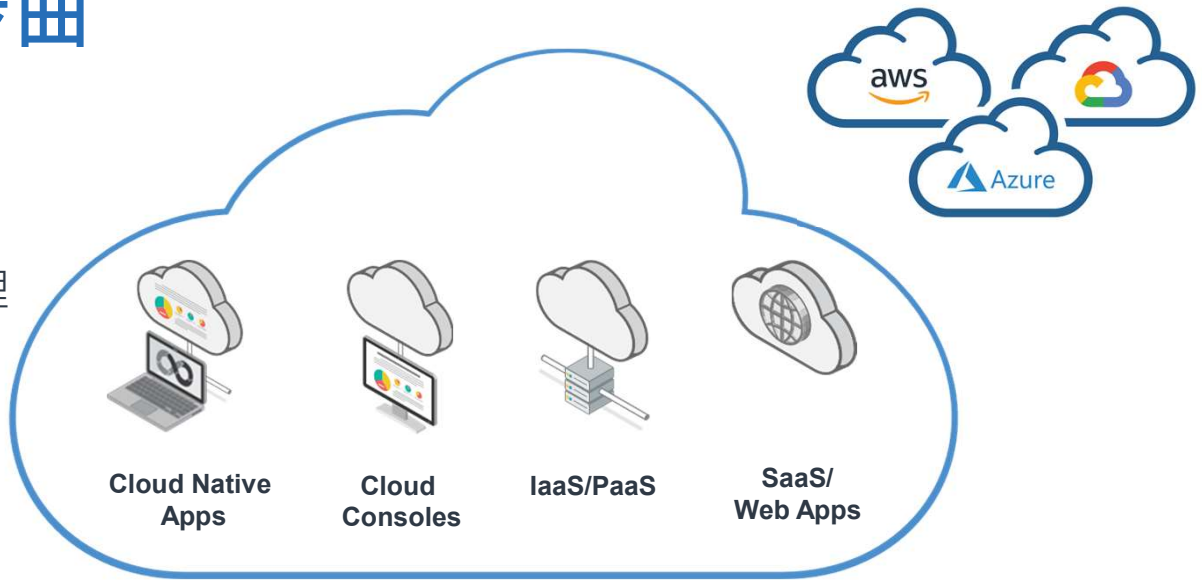
- 保持雲一致安全態勢
- 管理、審核權限以確保最少權限
- 保障的雲操作安全和控制台存取
- 確保雲虛擬機安全存取
- 保護應用程式和DevOps 中使用的秘密資訊如憑據/API Key
- 保護 SaaS 應用服務



IDENTITIES – IN THE CLOUD AND ON-PREM

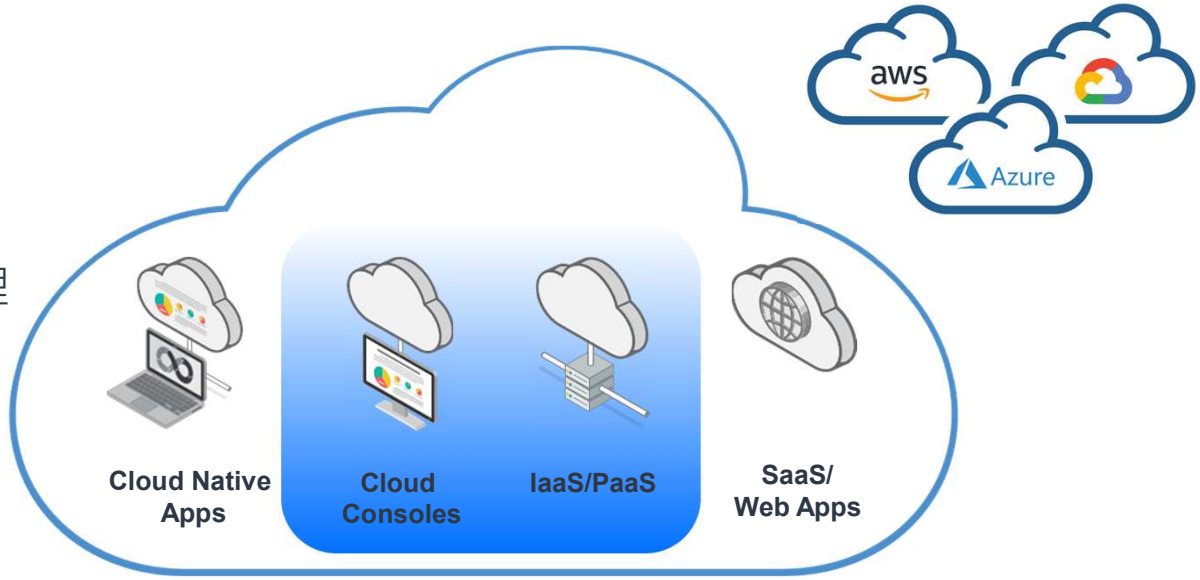
雲世界的身分安全五步曲

1) 實施 IAM 最少權限
2) 保護雲服務控制台存取安全
    1) root and super admin特權管理
    2) 聯合身分存取
3) 雲虛擬機的安全存取
4) 雲原生應用的秘密資訊管理
5) SaaS應用服務存取安全



實施 IAM 最少權限

1) 實施 IAM 最少權限
2) 保護雲服務控制台存取安全
    1) root and super admin特權管理
    2) 聯合身分存取
3) 雲虛擬機的安全存取
4) 雲原生應用的秘密資訊管理
5) SaaS應用服務存取安全



AWS, Azure 及 GCP
平台上超過25k+ Permissions

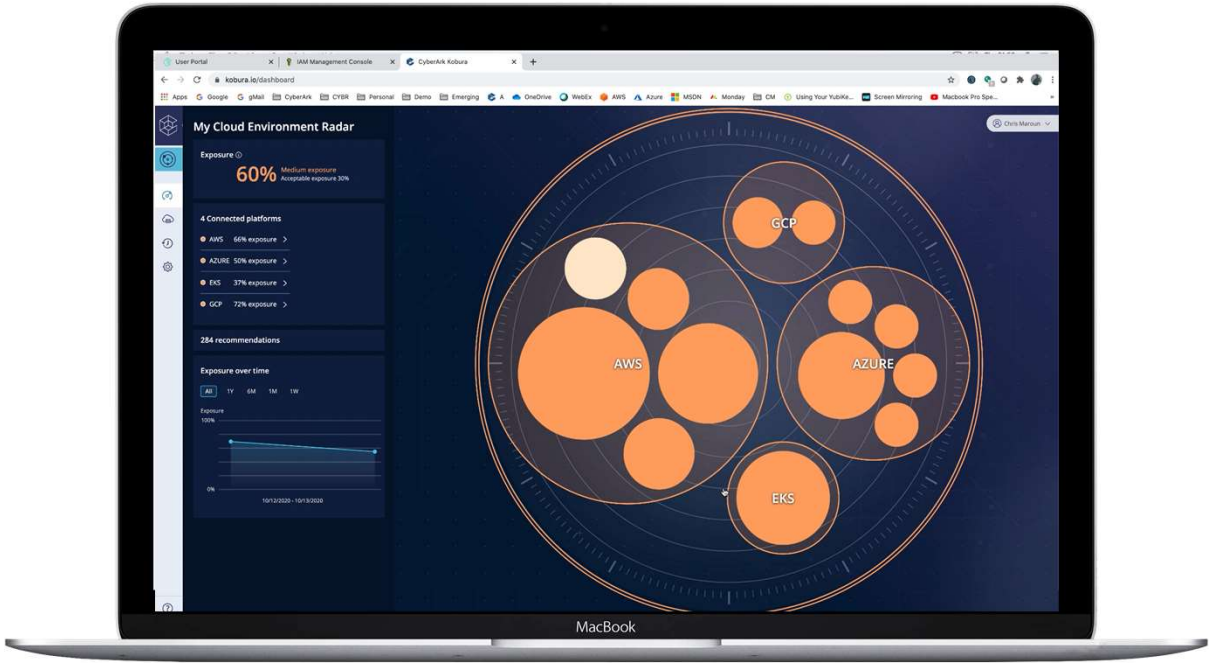
Cloud Entitlements Manager

偵測及移除過多權限

AI-powered SaaS 解決方案
落實跨雲端環境的最小授權資安原則

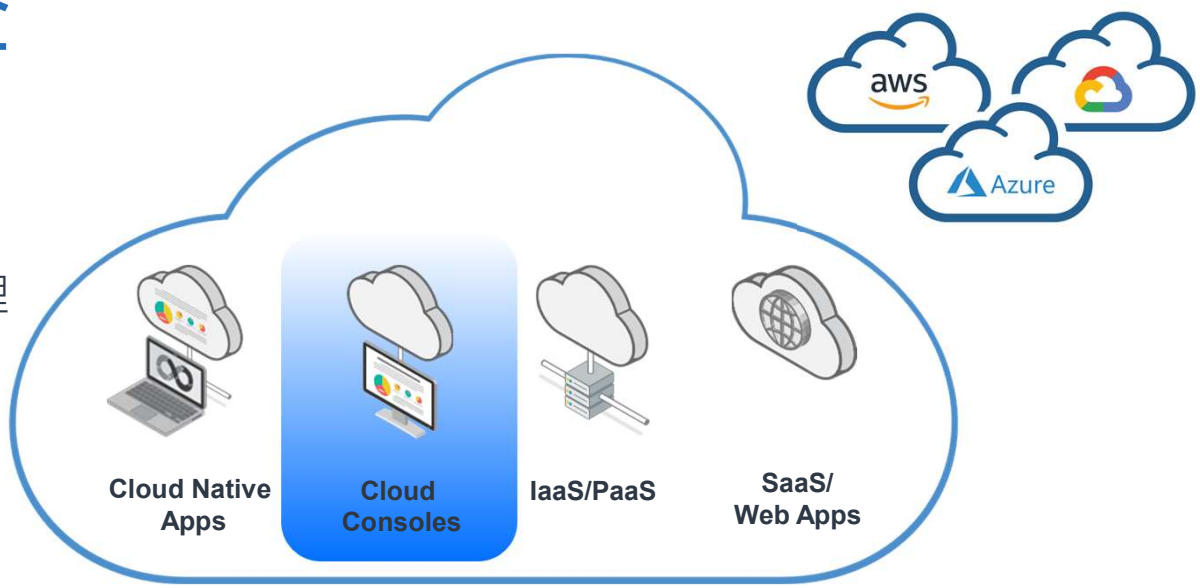
中央控制及能見度:

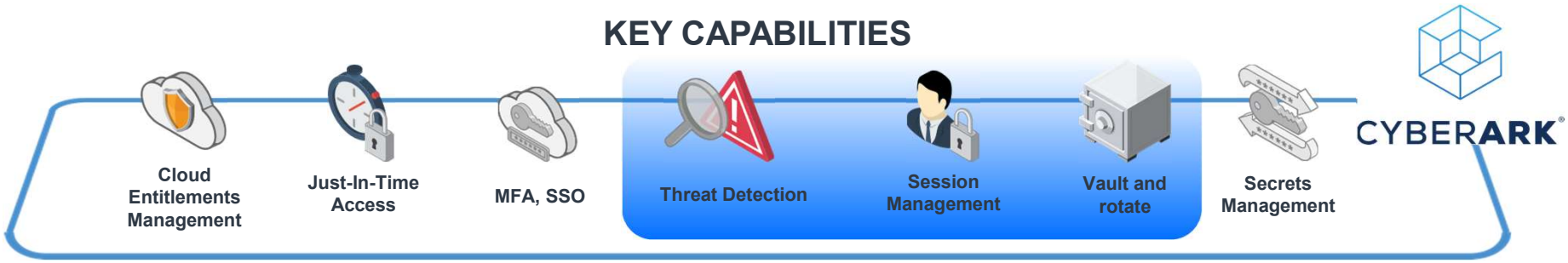
- 分析細微的存取權限
- 辨識未使用及過度的權限
- 模型畫暴露等級
- 提供行動方案建議
- 提供可佈署的補救措施



保護雲控制台訪問安全

1) 實施 IAM 最少權限
2) **保護雲服務控制台存取安全**
   - root and super admin特權管理
   - 聯合身分訪問
3) 雲虛擬機的安全存取
4) 雲原生應用的秘密資訊管理
5) SaaS應用服務存取安全

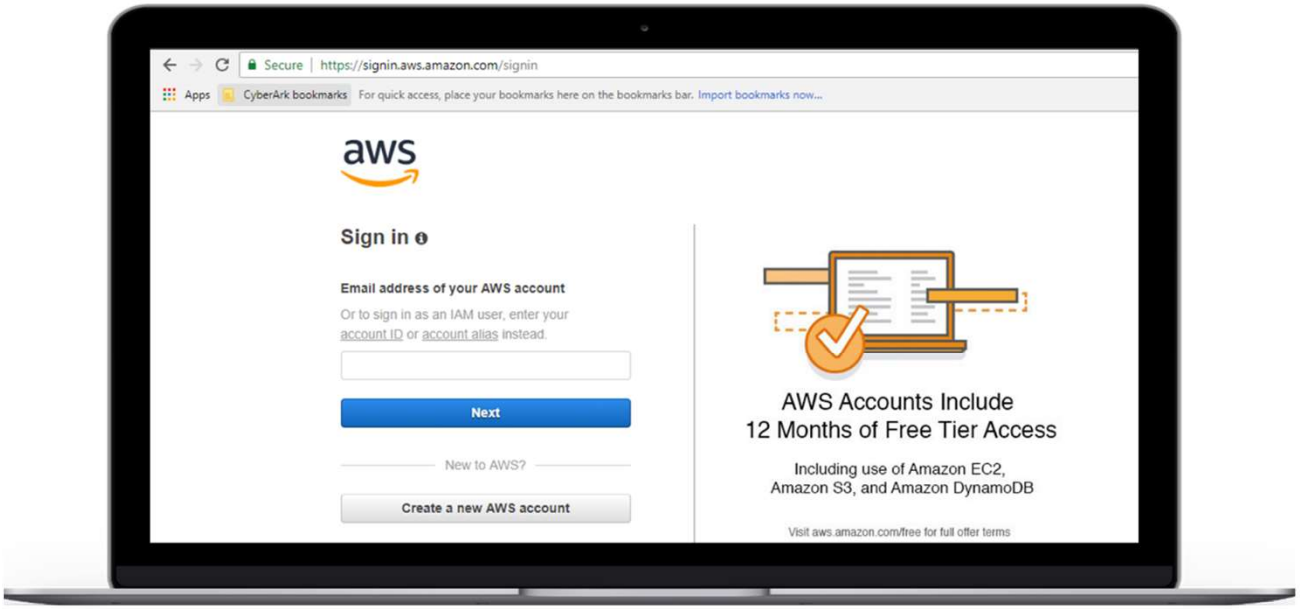




Root and Super Admin特權管理

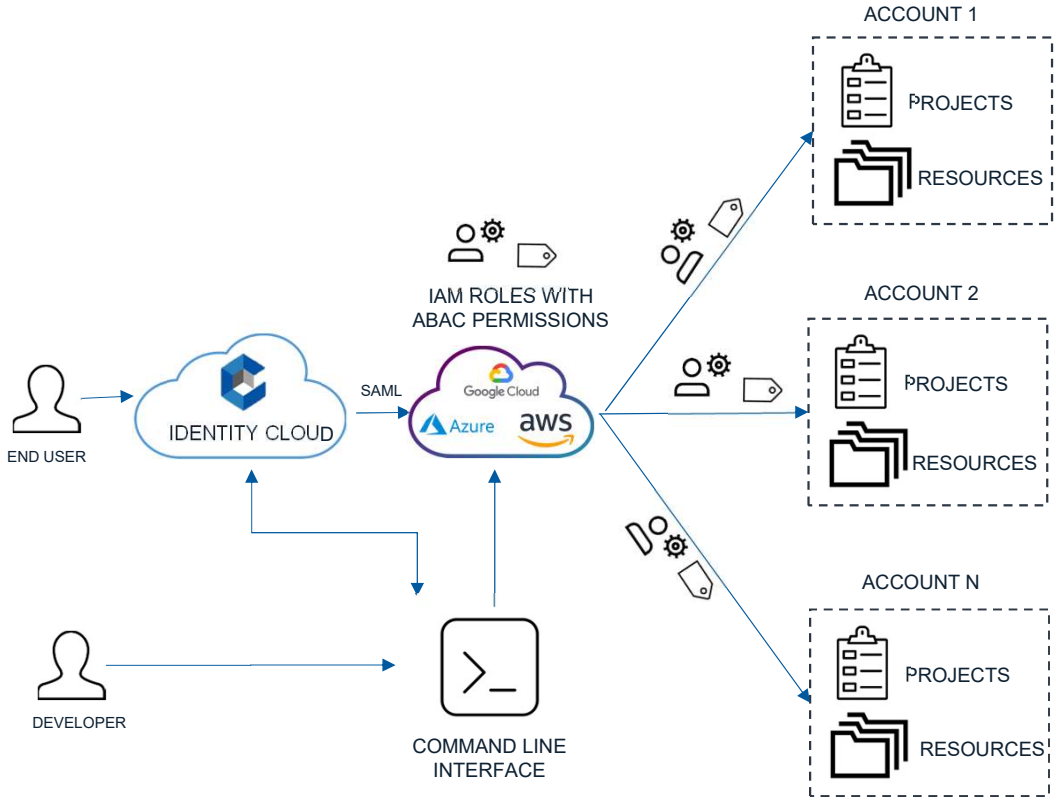
PRIVILEGED AND SHARED USERS

- 發掘特權 IAM 用戶並修復未受管理帳戶
- 保管和輪換特權帳戶憑據
- 隔離和記錄連線
- 監控和風險雲連線
- 檢測繞過保管庫的特權雲活動

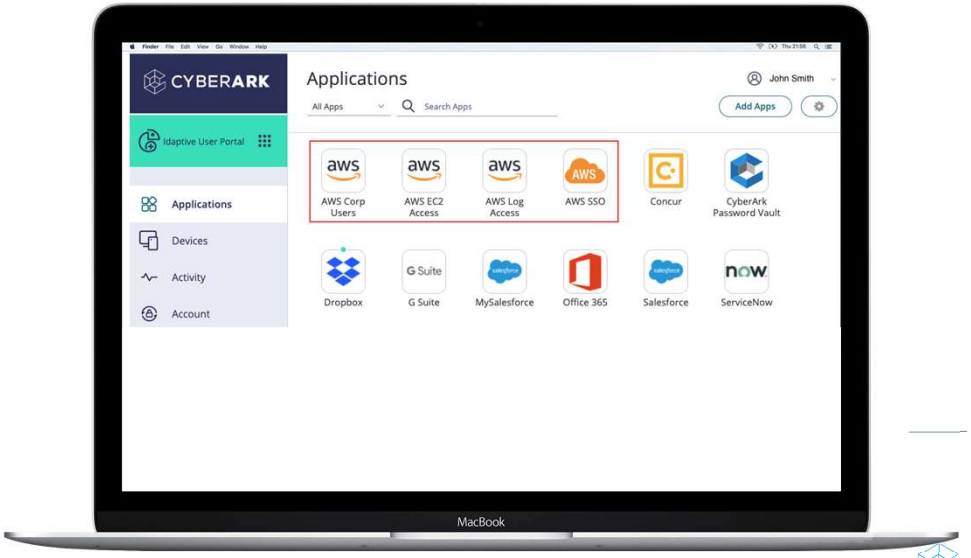


> *CyberArk is the standard for securing break glass console access to AWS*

聯合身分存取

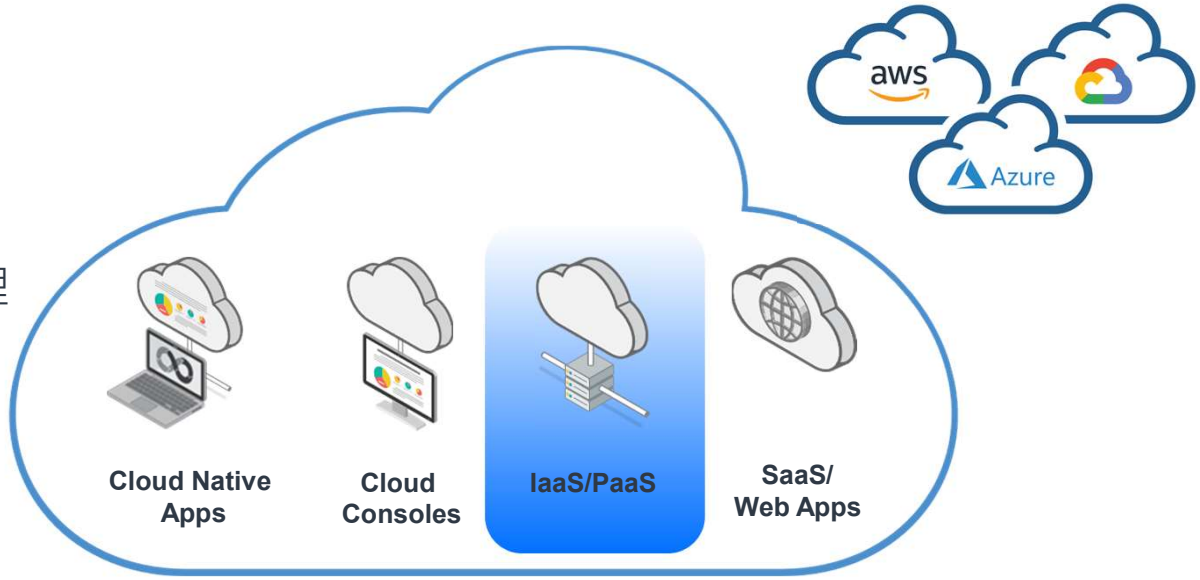


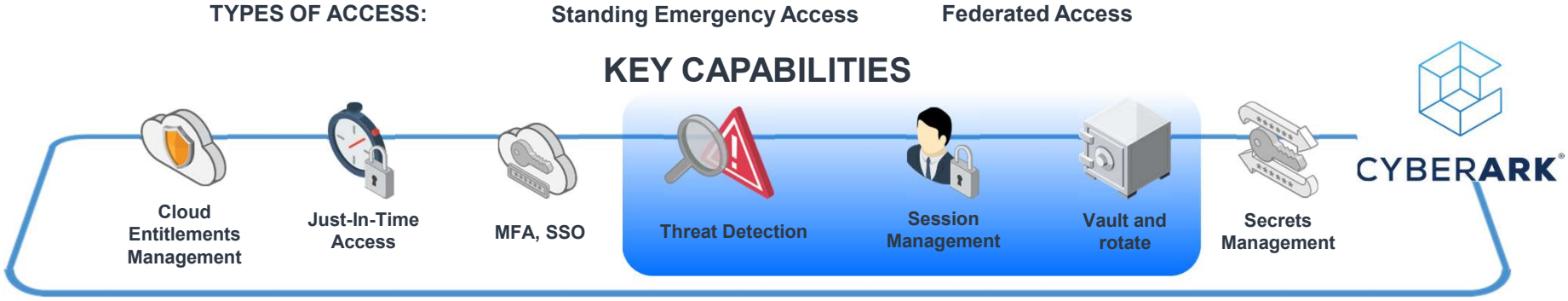
- 聯合安全存取雲服務控制台(SAML/oAuth)
- 使用自適應 MFA 安全存取雲服務控制台(SMS/Mobile Auth)



雲虛擬機的安全存取

1) 實施 IAM 最少權限
2) 保護雲服務控制台存取安全
    1) root and super admin特權管理
    2) 聯合身分存取
3) **雲虛擬機的安全存取**
4) 雲原生應用的秘密資訊管理
5) SaaS應用服務存取安全

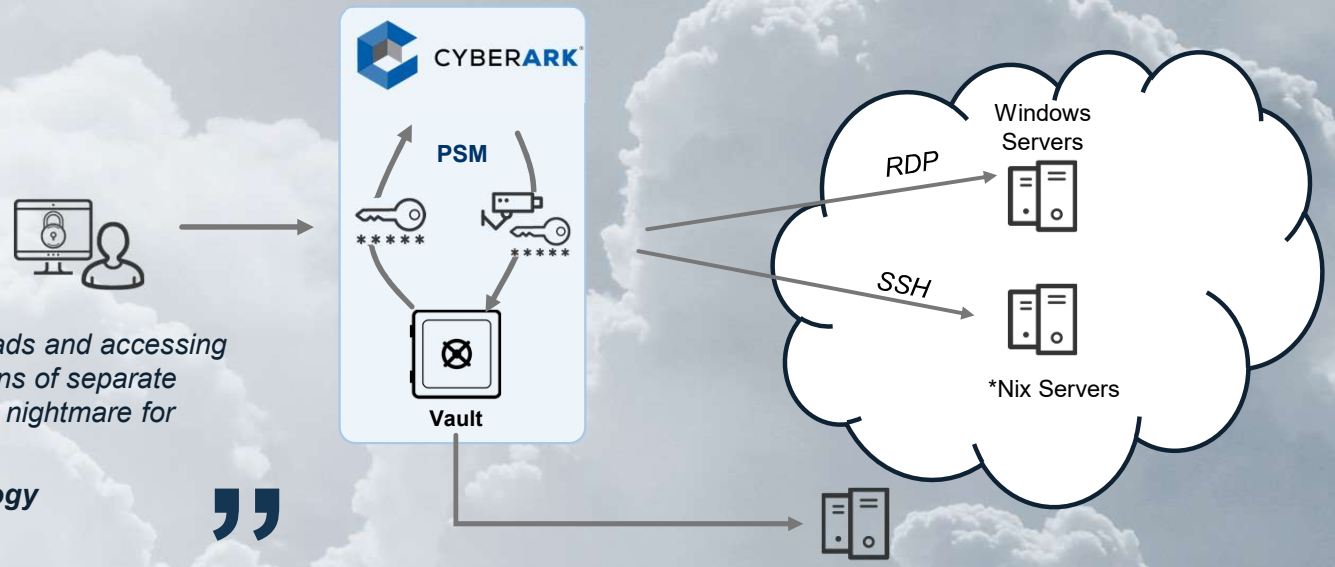




安全訪問雲基礎架構

- AWS、Azure 和 GCP 上實現虛擬機帳戶/密鑰的保管和輪換
- 使用短期證書身份驗證、輕鬆安全地存取 Linux 和 Windows 雲虛擬機
- 隔離和監控到雲虛擬機的特權存取

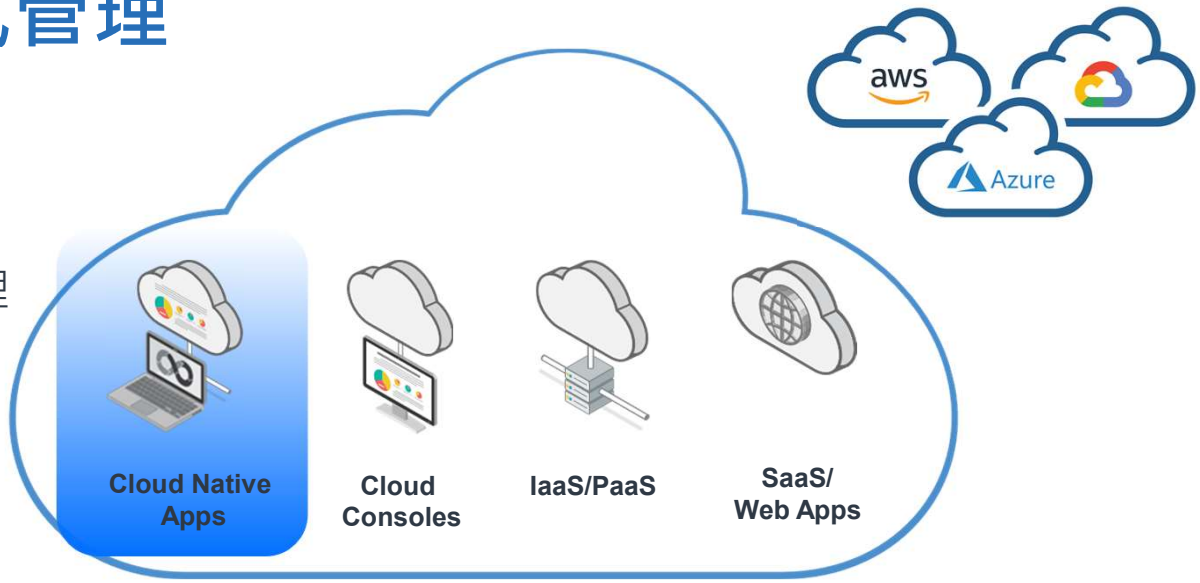
LINUX AND WINDOWS VM ACCESS WITH SHORT-LIVED CERTIFICATE AUTHENTICATION



> *For our operational teams logging into workloads and accessing servers and admin and SSH keys, we have tons of separate keys. That's where we have difficulties… it's a nightmare for operations"*
>
> ***- Global Leader in Connected Car Technology***

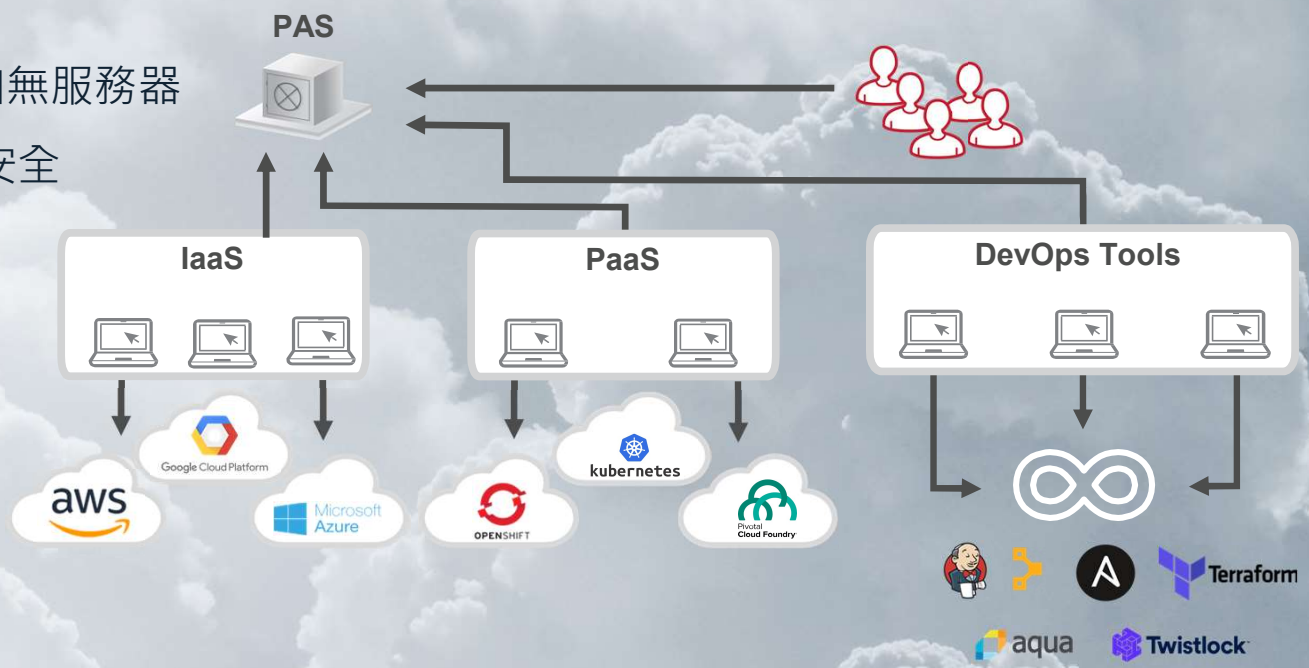
雲原生應用的秘密資訊管理

1) 實施 IAM 最少權限
2) 保護雲服務控制台存取安全
    1) root and super admin特權管理
    2) 聯合身分存取
3) 雲虛擬機的安全存取
4) **雲原生應用的秘密資訊管理**
5) SaaS應用服務存取安全



安全的雲原生應用程序和 DevOps Pipeline

- 從應用程序、腳本、自動化工具等中刪除嵌入式 API 密鑰和機密資訊。
- 以身分角度驗證應用程序安全
- 跨混合雲單一身分維護
- 整合到 DevOps Pipeline、容器化和無服務器
- 集中管理機密並附合以下機密資訊安全
  - Policy
  - Authorization
  - Rotation
  - audit



CYBERARK

C³ Alliance

150+ CERTIFIED PARTNERS

250+ CERTIFIED JOINT SOLUTIONS

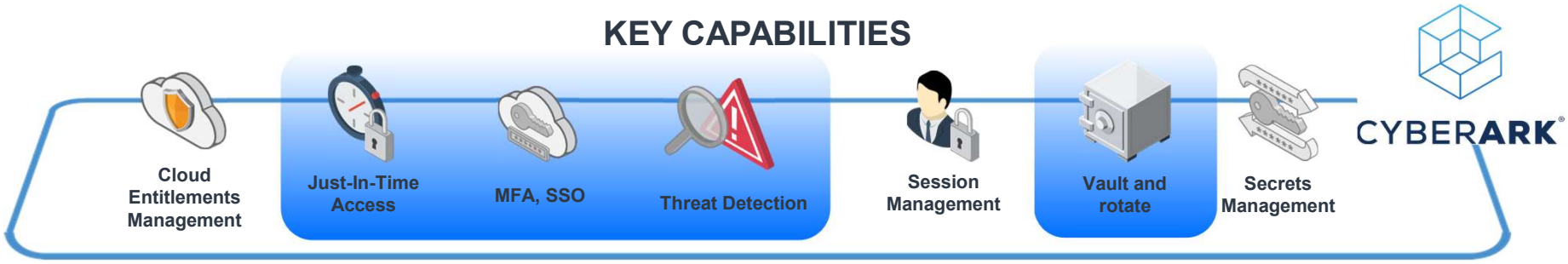
- Analytics
- ICS
- Identity & Access Management
- Authentic ation
- ITSM
- Detection
- Orchestration & Response
- DevOps
- Robotic Process Automation
- Discovery
- SIEM
- Governance
- HSM
- Vulnerability Management

200+ PLUG-INS

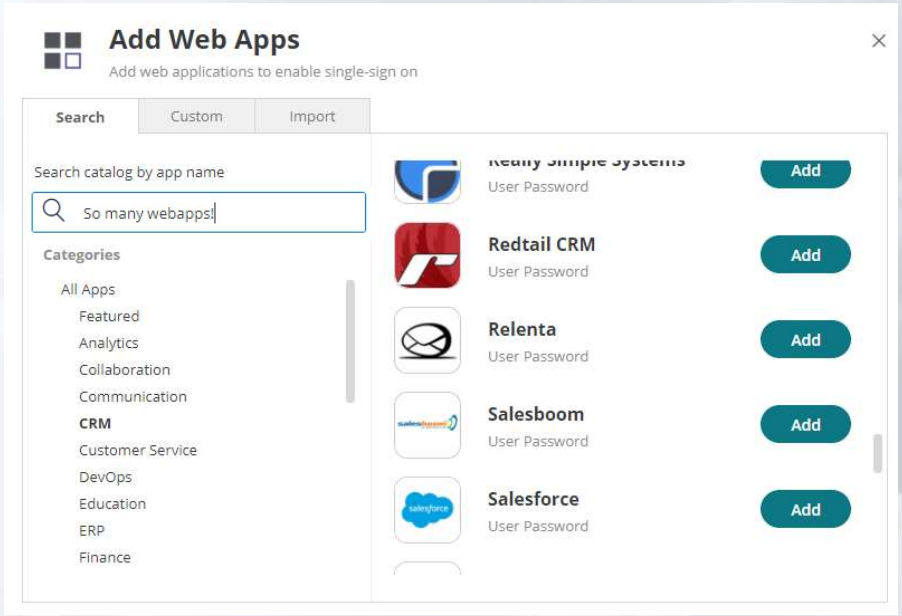
- CPM Plug-ins
- PSM Plug-ins

SaaS應用服務存取安全

1) 實施 IAM 最少權限
2) 保護雲服務控制台存取安全
    1) root and super admin特權管理
    2) 聯合身分存取
3) 雲虛擬機的安全存取
4) 雲原生應用的秘密資訊管理
5) **SaaS應用服務存取安全**



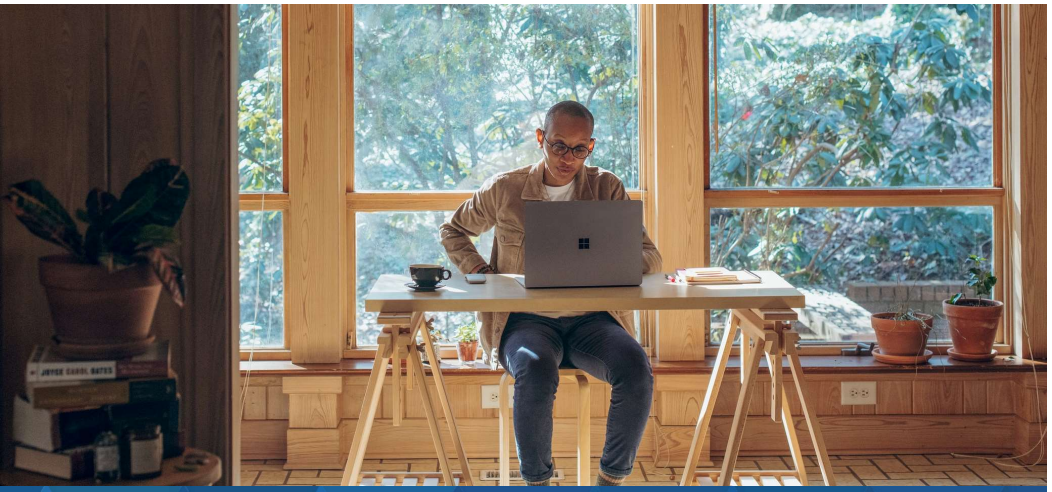
保護SaaS及網頁應用服務



- 支援大部份以SAML, UserName/Password為方式入方式的SSO的網頁應用
  - 提供InfiniteApps,能快速設定的SSO設定流程
- 支援自適應 MFA
- 用戶行為分析 (UBA) 和風險評分技術
- 具備簡單及易上手的網頁應用服務Onboard,解決設定的困難及大幅減少上線所需時間

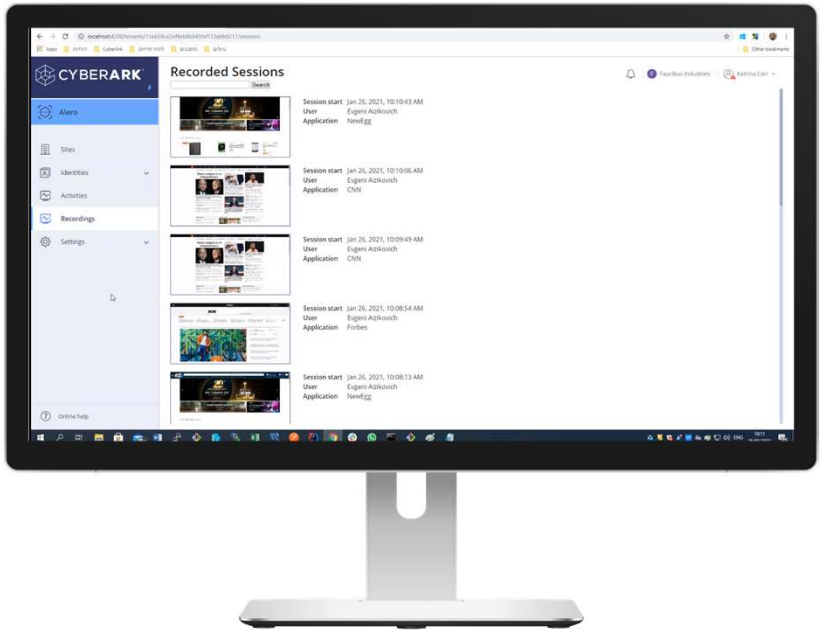
Major American Bank

Leverages Idaptive for MFA and SSO to a large number of webapps. Remote Access a CorePAS customer!



CyberArk Identity Secure Web Sessions

CyberArk Secure Web Sessions 雲服務，可讓您記錄和審核受 CyberArk Identity 保護的 Web 應用程式中的用戶活動。



REC

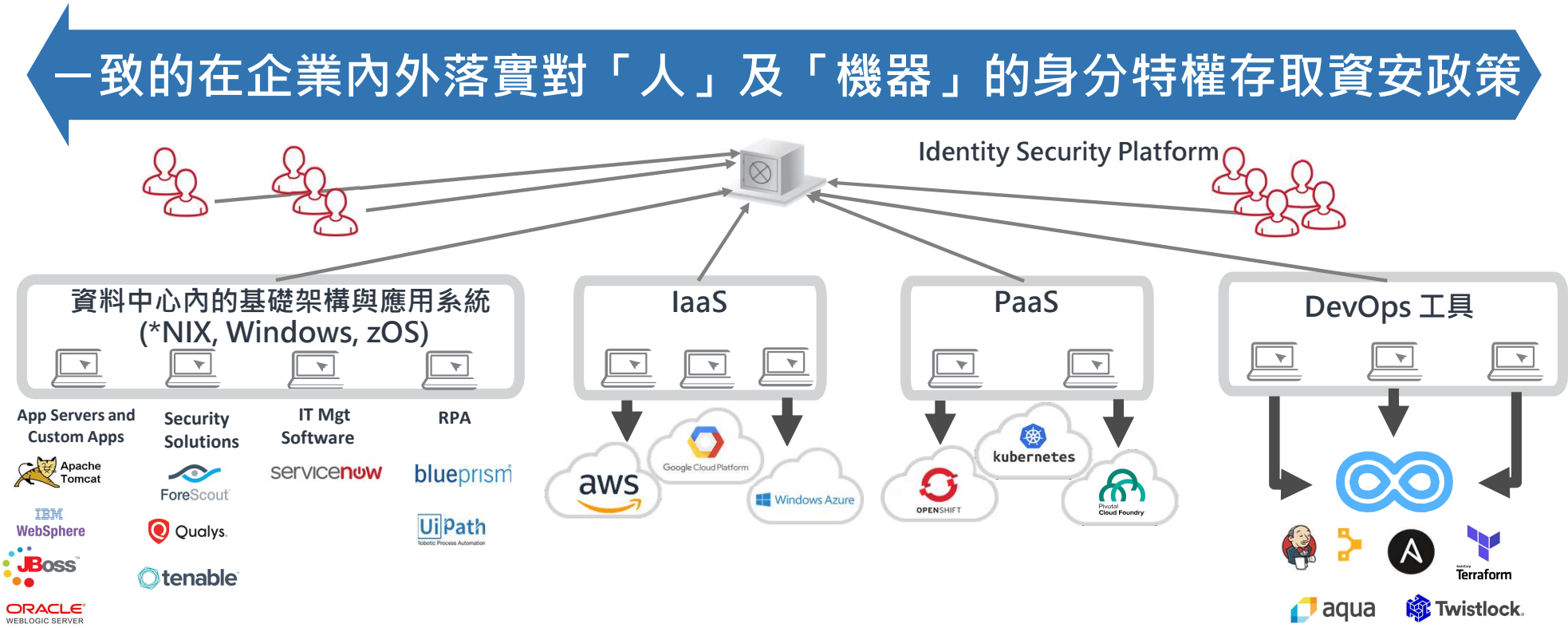
Record Activity

Create Audit Trail

Continuously Authenticate

Protect Sessions

一致的特權存取資安政策



身分安全商業價值

抵禦攻擊:
安全

- 基礎的、基於風險的 PAM 管控
- 適應性、依場景的存取控制
- 最小授權, JIT 存取
- 人及機器的身份管理
- 支援廣泛、混合的平台
- 受信賴的夥伴、CyberArk Labs研究團隊

維運效率提升:
簡化

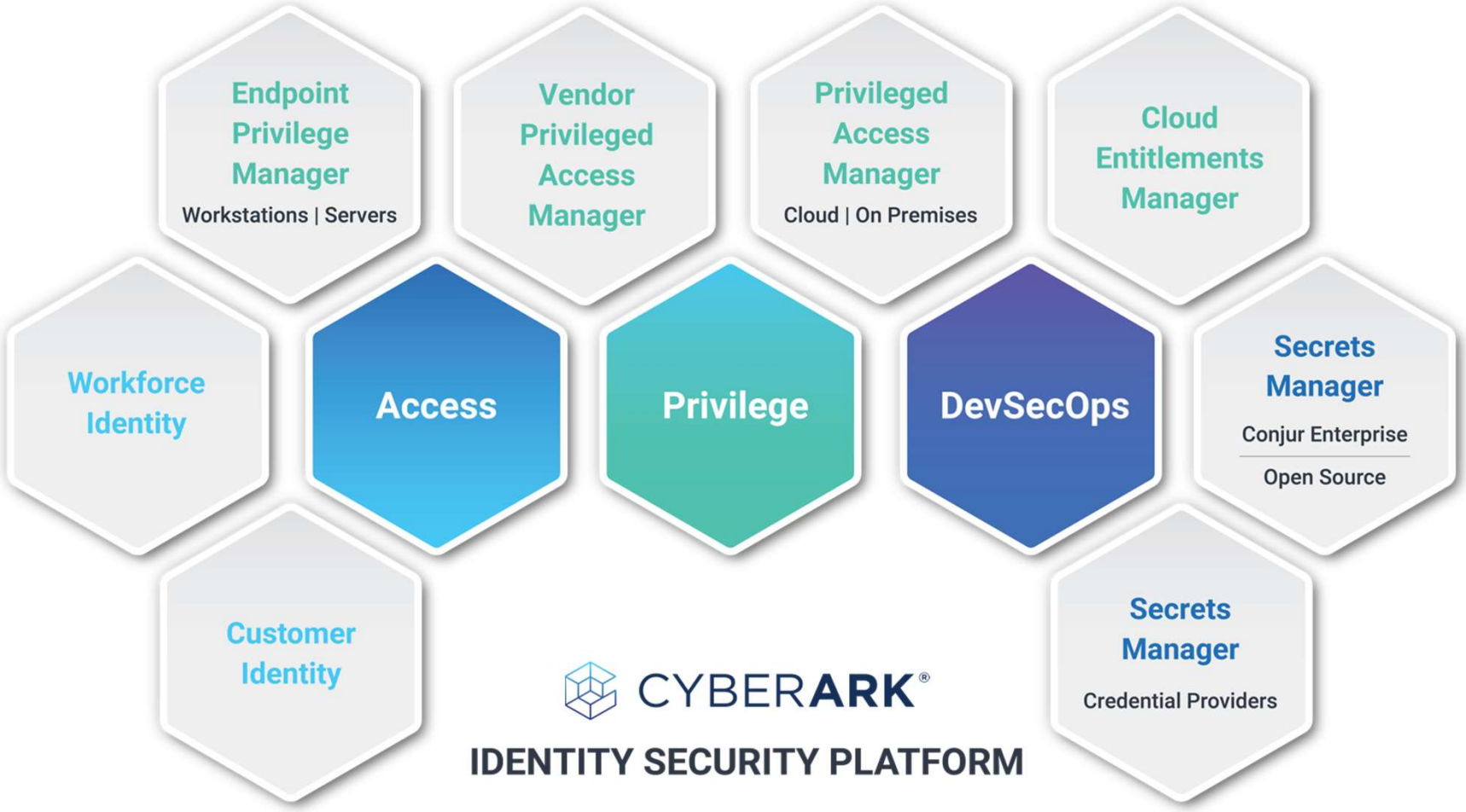
- 特權用戶有一致性的操作方式
- 集中化的能見度與管控
- 自助服務
- 原生存取方式
- SaaS 訂閱服務
- 資安合作夥伴聯防
- CyberArk 導入藍圖

啟動數位轉型:
加速

- 值得信賴的客戶導入經驗
- 保障現在及未來IT環境
- 最廣的設備、服務、平台預先整合
- 速度及靈活度
- API 優先策略
- 高可用度設計
- 支援各大雲端平台

滿足稽核與合規性:
標準化

- 品牌信譽
- 財務健全
- 看齊業界標準風險框架與規章
- 集中化完整的稽核軌跡
- 卸除符規壓力
- 持續合規



Security First Approach | AI Powered | Frictionless Experience | Everywhere

資安優先 • 人工智慧(AI)驅動 • 流暢體驗 • 任何地方

謝謝指導

THANK YOU