數位轉型及大規模自動化的特權存取管理

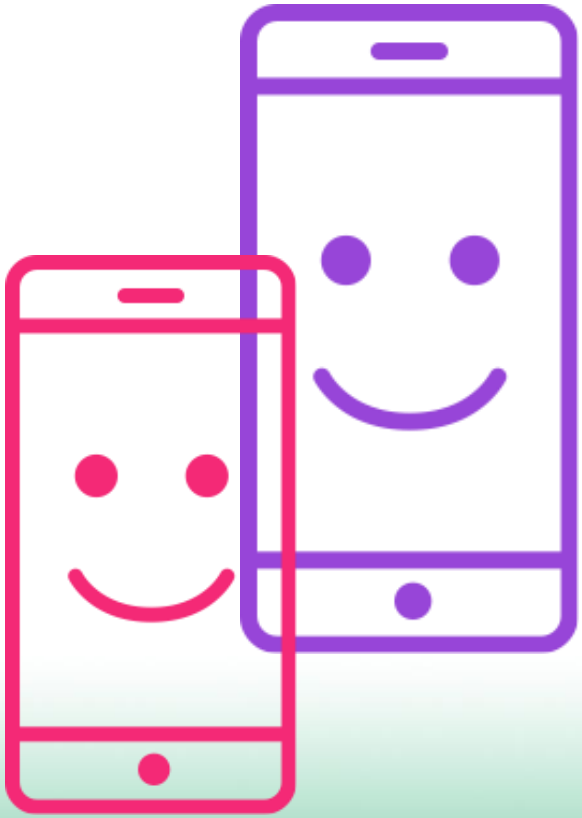
主講人：CA Technologies
大中華區首席資安顧問
凌尊豪 Joseph Ling

我們的使命：

消弭創意與成果之間的阻礙

現今所有業務都是軟體業務

在軟體業務中，體驗決定一切



事實：

53% 的使用者在瀏覽行動網站時，如果頁面載入時間超過三秒就會放棄使用[1]

[1]https://www.doubleclickbygoogle.com/articles/mobile-speed-matters/ Google Data, Aggregated, anonymized Google Analytics data from a sample of mWeb sites opted into sharing benchmark data, n=3.7K, Global, March 2016

我們知道

成功的公司專注於四個主要準則

安全性
降低風險，並提供安全且順暢的存取。

自動化
提升速度與品質。

洞察力
持續改進並洞見商機。

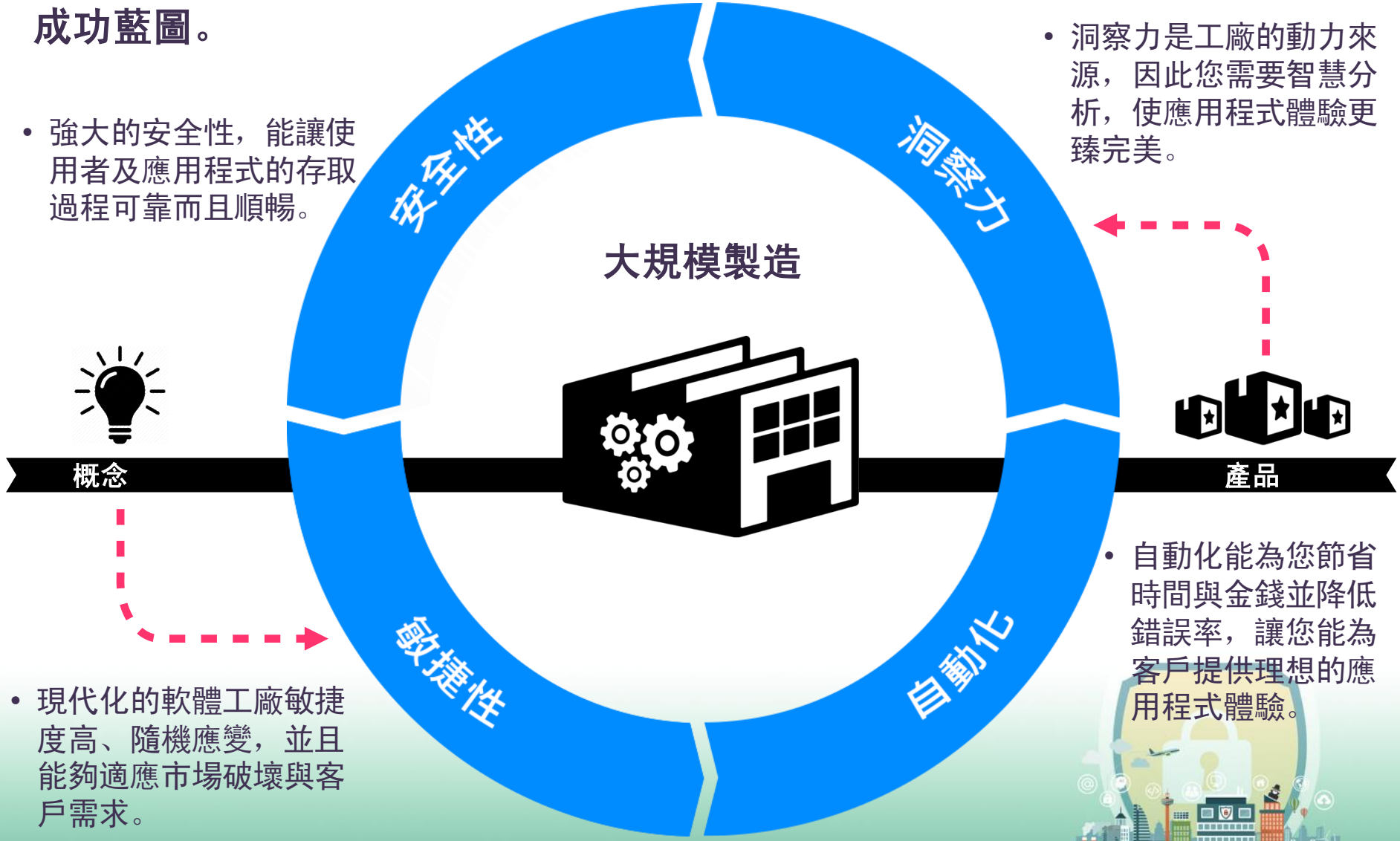
敏捷性
加速上架時程。

現代化的軟體工廠

成功藍圖。

- 強大的安全性，能讓使用者及應用程式的存取過程可靠而且順暢。

- 洞察力是工廠的動力來源，因此您需要智慧分析，使應用程式體驗更臻完美。



- 現代化的軟體工廠敏捷度高、隨機應變，並且能夠適應市場破壞與客戶需求。

- 自動化能為您節省時間與金錢並降低錯誤率，讓您能為客戶提供理想的應用程式體驗。

讓安全性成為競爭優勢

保護應用程式、資料和基礎結構
Identity Management + Privileged Access Management + Threat Analytics

保護資料隱私權
Test Data Manager + Privileged Access Management + Data Content Discovery + Project & Portfolio Management

提供風險型行動存取
API Lifecycle Management + Privileged Access Management + Advanced Authentication + Single Sign On

CA Privileged Access Manager

SYSTEX A DATA COMPANY

特權帳戶究竟有多少

找不到就保護不到

管理員
AWS/Office 365

外包商
系統/網路/資料庫/應用管理員

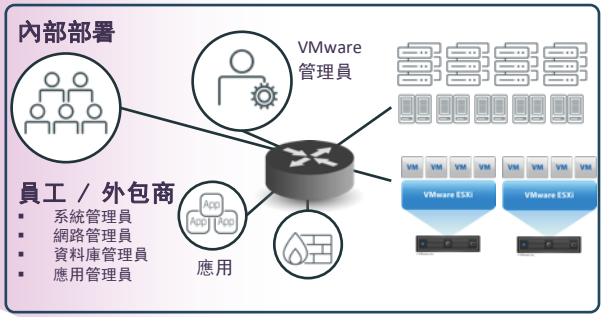
應用/服務帳戶

員工
系統/網路/資料庫/應用管理員

互聯網

Office 365
salesforce
amazon web services

雲端服務



企業特權帳號存在現況分析表

帳號 屬性	範圍	使用人員	使用用途
特權個人帳號	如同Super User權限的個人帳號 jSmith_admin	• IT人員	• 執行特殊操作與存取 • 可存取敏感資料
特權共用帳號	最高權限使用帳號 Administrator UNIX root Cisco Enable Oracle SYS MSSQL sa Local Administrator	• IT人員 • 系統管理者 • 網管工程師 • 資料庫管理者 • 外包廠商 • 程式開發人員 • 傳統應用程式	• 特殊操作 • 緊急狀況 • 災難復原 • 可存取敏感資料
應用程式帳號 (App to App , AP to DB)	內嵌或固字在程式中的帳號及密碼 系統服務啟動帳號	• 應用程式 • Script • Windows服務 • 排程工作 • 批次工作 • 程式開發人員	• 線上資料庫存取 • 批次資料處理 • 應用程式連接到伺服器 • 應用程式連接到資料庫

如何消除風險的源頭？

透過保護管理員帳戶，控制特權用戶使用，和管控記錄特權用戶的活動三管齊下**防止漏洞**

透過特權帳戶管理從攻擊的源頭阻止意外發生

防止非授權帳戶使用

- 「強驗證」
- 登錄控制
- 自動的行為分析和風險偵測

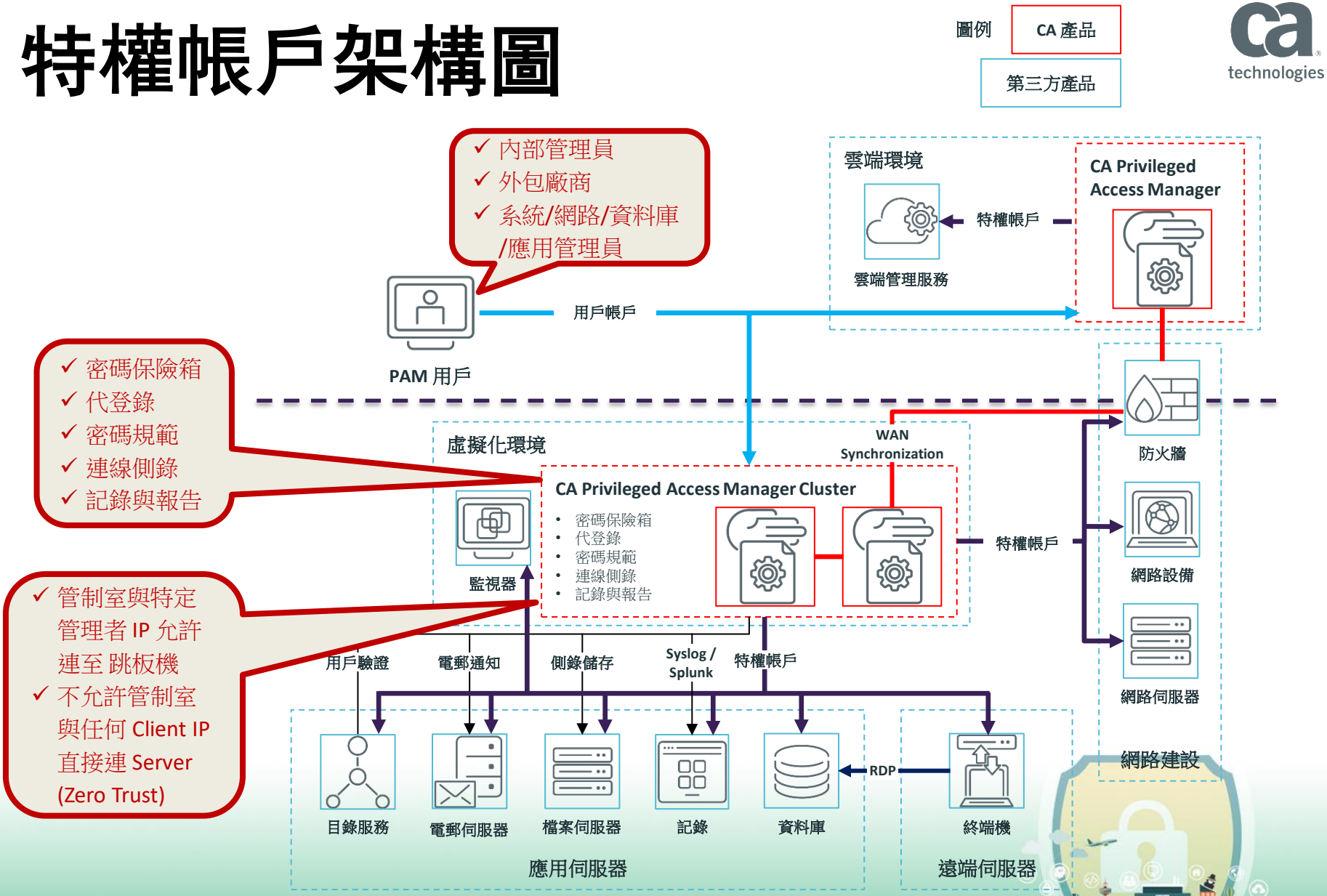
防止特權提升

- 指令過濾/防蛙跳
- 零信任 - 通過認證後還是不信任，必須通過明確的許可，否則拒絕
- 主動式細部管理

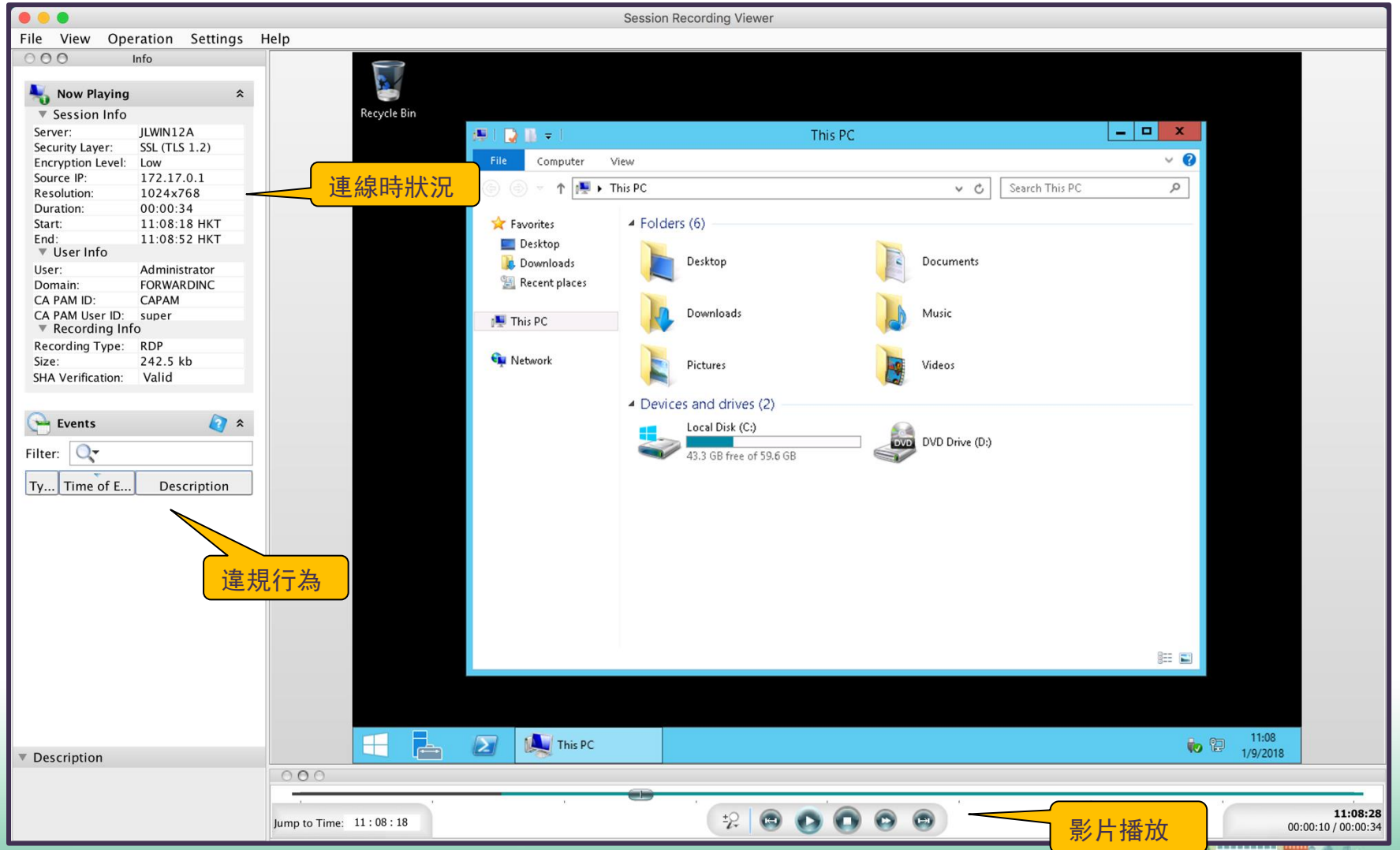
記錄與稽徵

- 連線錄影和管控
- 活動記錄和稽徵
- SIEM 整合

特權帳戶架構圖



連線側錄



特權用戶/共用帳號
是資訊安全威脅最大的問題與挑戰

- 各個系統上都有特權帳號，對資源具有強大的存取權限，行為無法控管，能對系統產生破壞性，包含
  - 新增另一個有權限的使用者
  - 變更其他使用者的權限
  - 存取敏感的資訊（copy, modify, delete)
  - 變更或刪除稽核記錄
  - 停止系統運作
  - 擁有一個系統
- 通常會被共用(Shared) – 缺乏帳號的有責任性(Accountability)，無法區隔權責
- 缺少存取的透明度及稽核記錄的完整性
- 法規的要求（金管會, ISO27001, PCI-DSS, SOX..)

Superuser (Administrator/root) 遏制與權限限制

- Administrator/root 帳戶是重大的漏洞來源，因為可能讓應用程式或使用者取得超出需求的強大特殊權限等級。
- CA PAM Server Control 會在系統層次上檢查所有相關的送入要求，然後根據已定義的規則和原則來實施授權。即使特殊權限的 administrator/root 帳戶也需通過 CA PAM Server Control 這一層管制。因此，所有授權使用者都會變成受管理使用者，必須對他們在系統上的活動負起責任。

最低權限控管

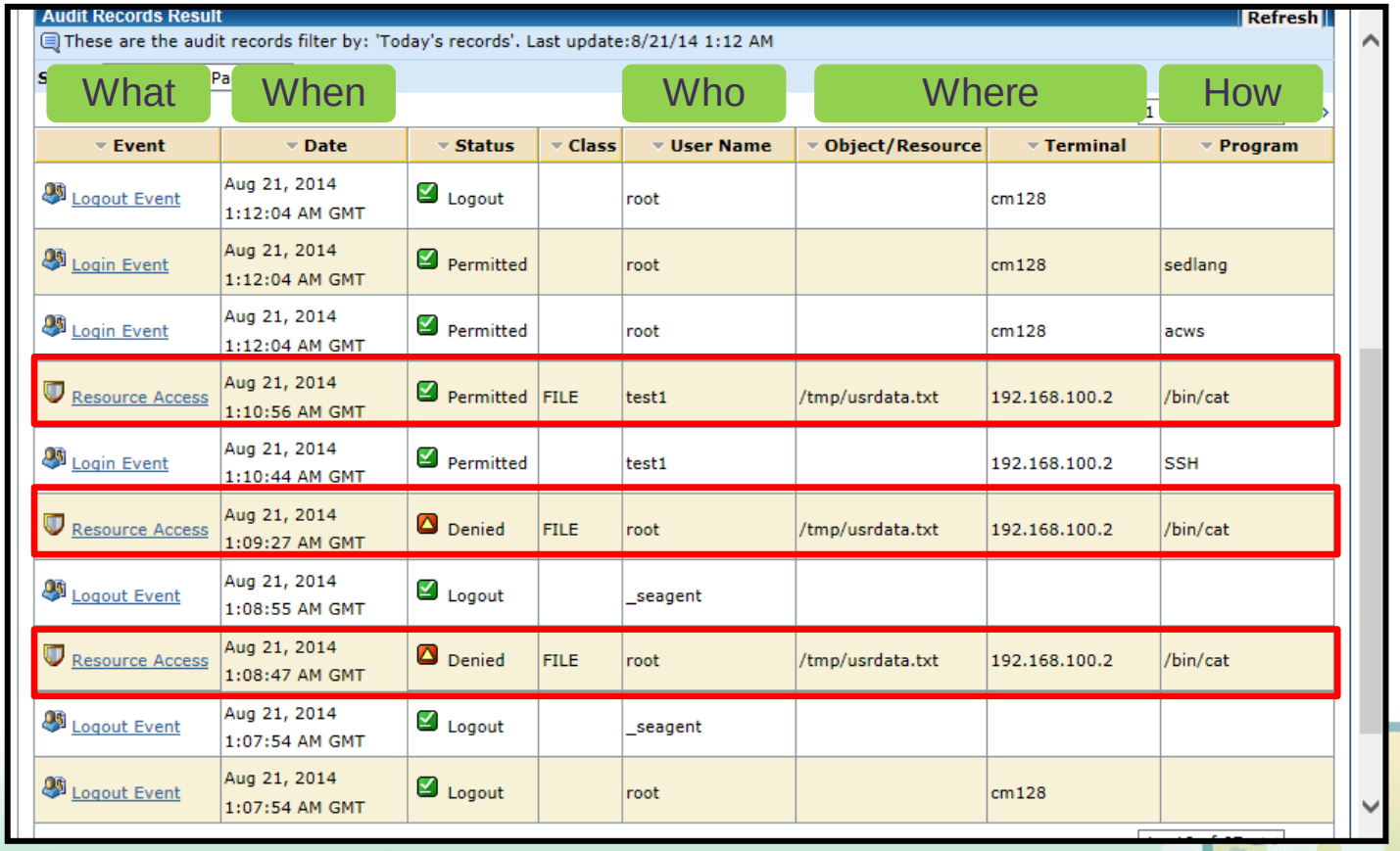
即便切換成 root，仍不能存取重要檔案

```
oracle_operator@aclinux:/home/oracle_operator
[oracle_operator@aclinux ~]$ su root
Please enter your password:
[root@aclinux oracle_operator]# cat /etc/hosts
cat: /etc/hosts: Permission denied
[root@aclinux oracle_operator]#
```

su/sudo 控制 (UNIX/Linux 主機)

- 管理員可以偽裝另一人的身分資料來變更檔案的存取控制清單屬性，而不對他們的行動負起任何責任。
- CA PAM Server Control 可以控制代理使用者委派功能，避免未獲授權使用者以加強的特殊權限來執行應用程式，達到共用帳戶活動的責任歸屬。
- 即使在代理動作之後，CA PAM Server Control 也會保留原始使用者 ID，以確保稽核記錄中的使用者存取記錄顯示原始帳戶。這樣可讓使用者以自己的 ID 登入，安全地將設定檔變更為特殊權限的帳戶，而不會失去責任歸屬。

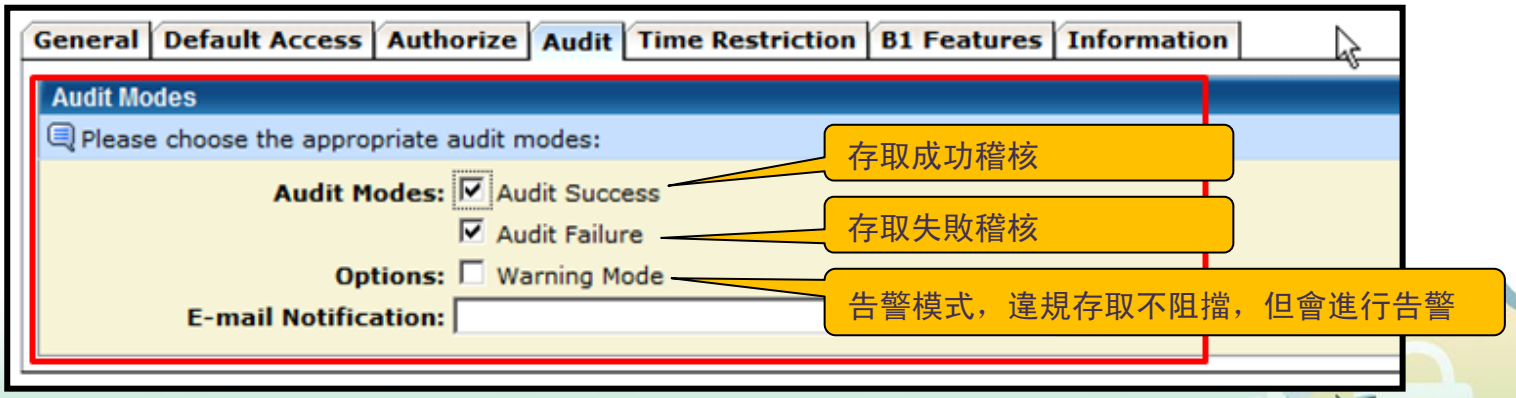
稽核記錄



Event	Date	Status	Class	User Name	Object/Resource	Terminal	Program
Logout Event	Aug 21, 2014 1:12:04 AM GMT	Logout		root		cm128	
Login Event	Aug 21, 2014 1:12:04 AM GMT	Permitted		root		cm128	sedlang
Login Event	Aug 21, 2014 1:12:04 AM GMT	Permitted		root		cm128	acws
Resource Access	Aug 21, 2014 1:10:56 AM GMT	Permitted	FILE	test1	/tmp/usrdata.txt	192.168.100.2	/bin/cat
Login Event	Aug 21, 2014 1:10:44 AM GMT	Permitted		test1		192.168.100.2	SSH
Resource Access	Aug 21, 2014 1:09:27 AM GMT	Denied	FILE	root	/tmp/usrdata.txt	192.168.100.2	/bin/cat
Logout Event	Aug 21, 2014 1:08:55 AM GMT	Logout		_seagent			
Resource Access	Aug 21, 2014 1:08:47 AM GMT	Denied	FILE	root	/tmp/usrdata.txt	192.168.100.2	/bin/cat
Logout Event	Aug 21, 2014 1:07:54 AM GMT	Logout		_seagent			
Logout Event	Aug 21, 2014 1:07:54 AM GMT	Logout		root		cm128	

稽核與警告模式 (Warning mode)

- CA PAM Server Control 可以針對所行為之存取成功或存取失敗進行稽核，而不需藉助作業系統本身的稽核機制。
- 企業可透過「警告模式 Warning Mode」來判斷提議的安全原則是否太嚴格或太寬鬆，據以適當地修改。



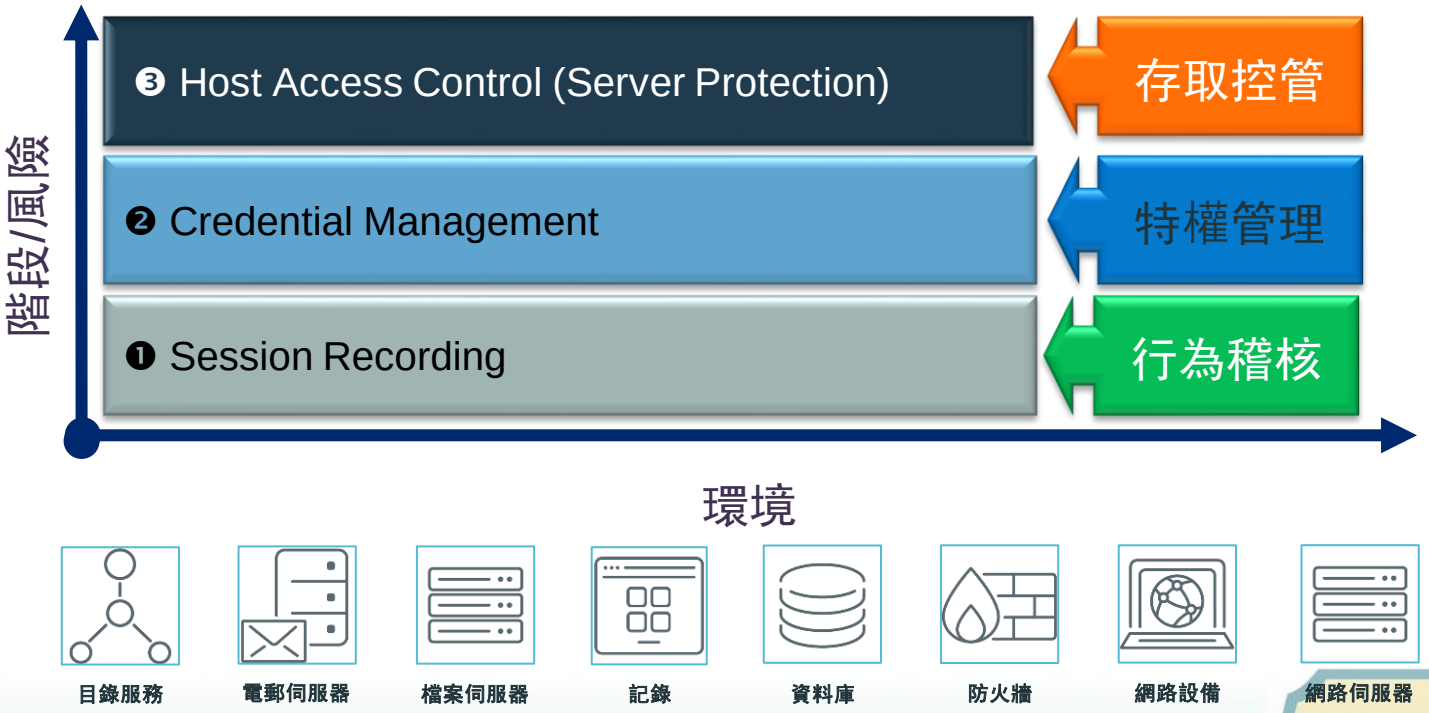
跨平台集中式
作業系統存取控管與稽核

主機管控

Windows Server	Linux/UNIX Server	
程序 (Program) 執行管控	程序 (Program) 執行管控	防止外洩
鎖定的ports/services	鎖定的ports/services	
網路TCP/IP 進入與流出保護	網路TCP/IP 進入與流出保護	
檔案(Files)和目錄(dirs)的存取控制	檔案(Files)和目錄(dirs)的存取控制	防止非法提權，避免存取敏感機密資料
Administrator 帳號的權限分割	root 帳號的權限分割	
Windows 註冊碼保護	sudo / su 保護	
Windows 服務保護	登入方式保護	
上述所有活動稽核報表(成功/失敗)	上述所有活動稽核報表(成功/失敗)	稽核與監管
集中管理所有系統的存取政策	集中管理所有系統的存取政策	

主機/特權帳戶管理與使用者軌跡稽核方案

保護眾多異構主機系統(實體機/虛擬機器),提供特權使用者訪問及許可權管理



完整特權帳戶管理方案

CA 身份管理

- 帳戶活動提請
- 符合安全規定
- 風險分析

CA Privileged Access Manager

- 強認證，包括雙因子認證
- 帳戶密碼管理
- 細部管控，把特權收到最小
- 指令過濾
- 連線側錄
- 應用上的帳戶密碼管理
- 完整的企業保護
- 完全加密的封閉系統

網路為本的保護

CA Privileged Access Manager Server Control

- 針對重要伺服器的深入保護
- 仔細準確的帳戶行動控制
- 分散特權
- 控制系統資源如檔案，資料夾，系統程序和系統登錄檔的存取
- Unix 驗證橋接
- 安全工作代理(sudo)
- 建立信用操作平台

主機為本的保護

深入防護

精明的選擇

低成本

CA PAM 不會按帳戶數量跟使用流量計價

快達標

簡單的架構、完整的功能、快速的建構

高效率

每一台 CA PAM 可以同時處理一千個特權帳戶的連接

靈活架構

一台 CA PAM 可以處理主機、虛擬機器、桌上型電腦，跟雲端服務

Thank You!