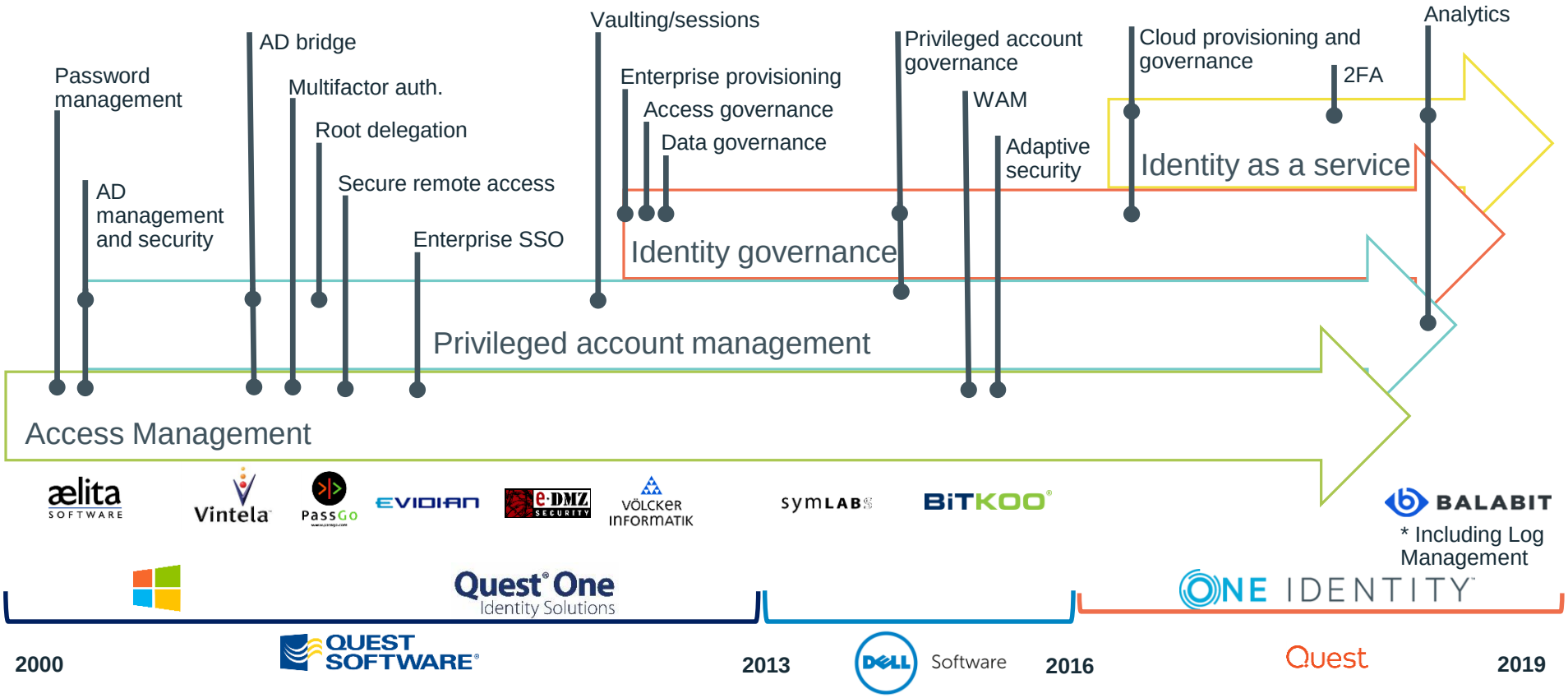
缺乏治理的特權帳號系統，才是最大的資安漏洞

亞太區高級架構師

龐祥雲 James

ONE IDENTITY

History



ONE IDENTITY

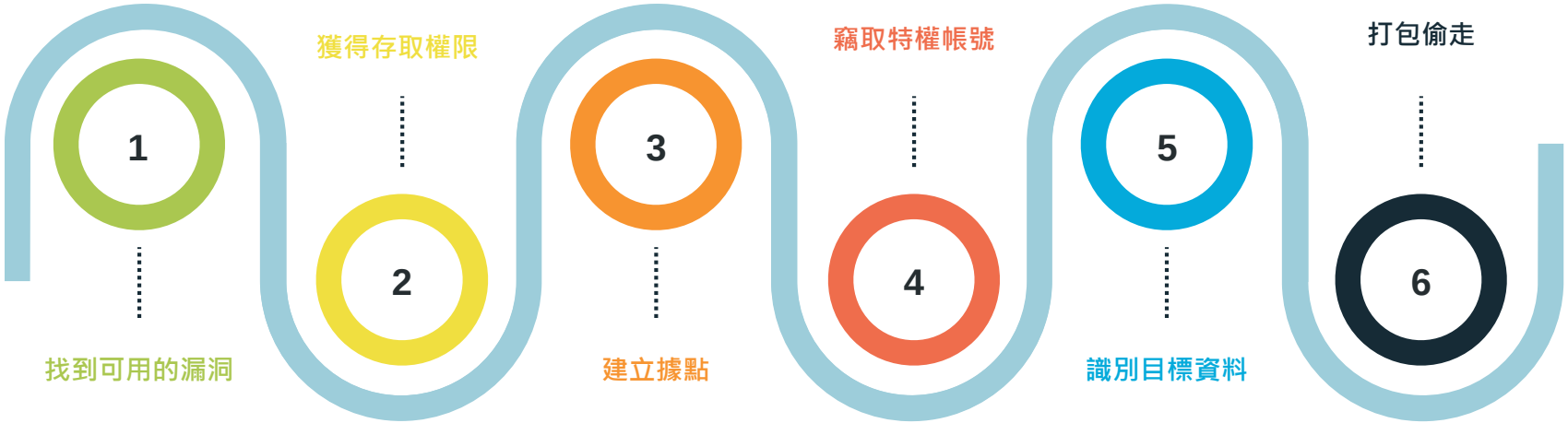
身分治理 Gartner Report

Figure 1. Magic Quadrant for Identity Governance and Administration

Source: Gartner (February 2018)

ONE IDENTITY

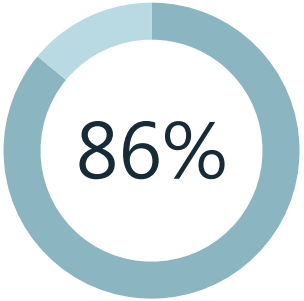
Cyber Attack Lifecycle



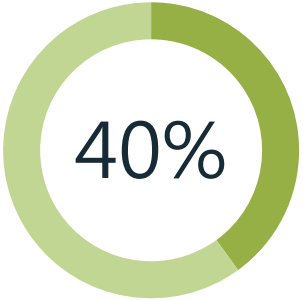
- Global Average to detect cyber incident is 78 days*
- 204 days for APAC based organization*

Source : FireEye M-Trends 2019

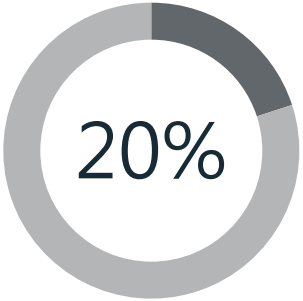
密碼使用行為統計



每次使用特權帳號不會變更密碼



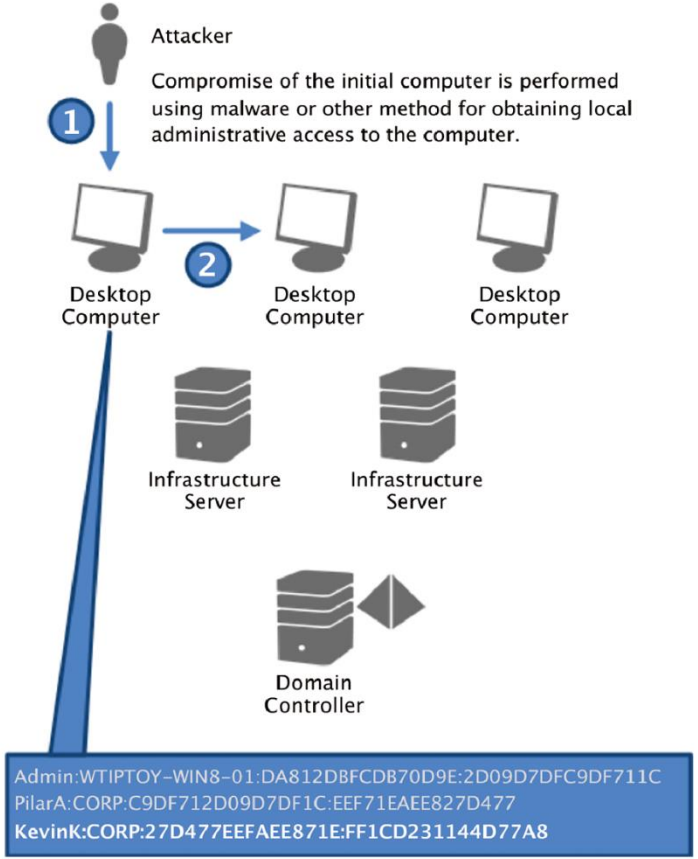
重要系統沒有變更admin的預設密碼

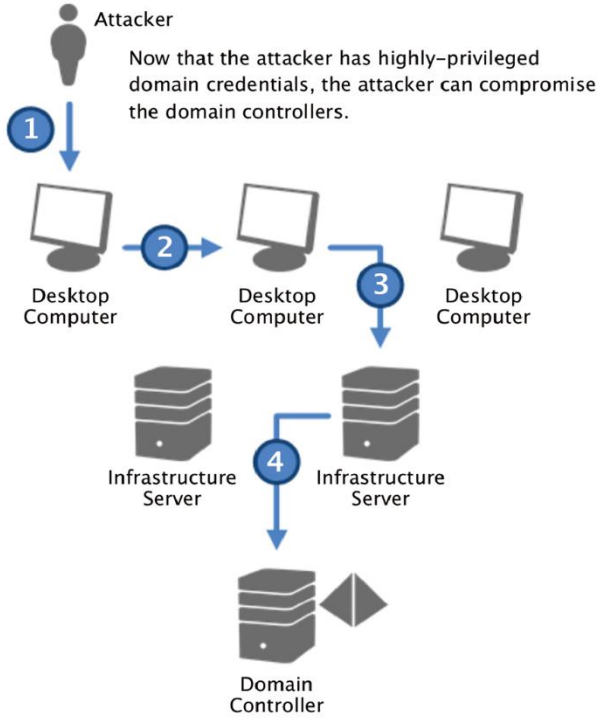


使用紙紀錄特權帳號密碼

Source: One Identity Global Survey

Pass-the-Hash (PtH) Attacks





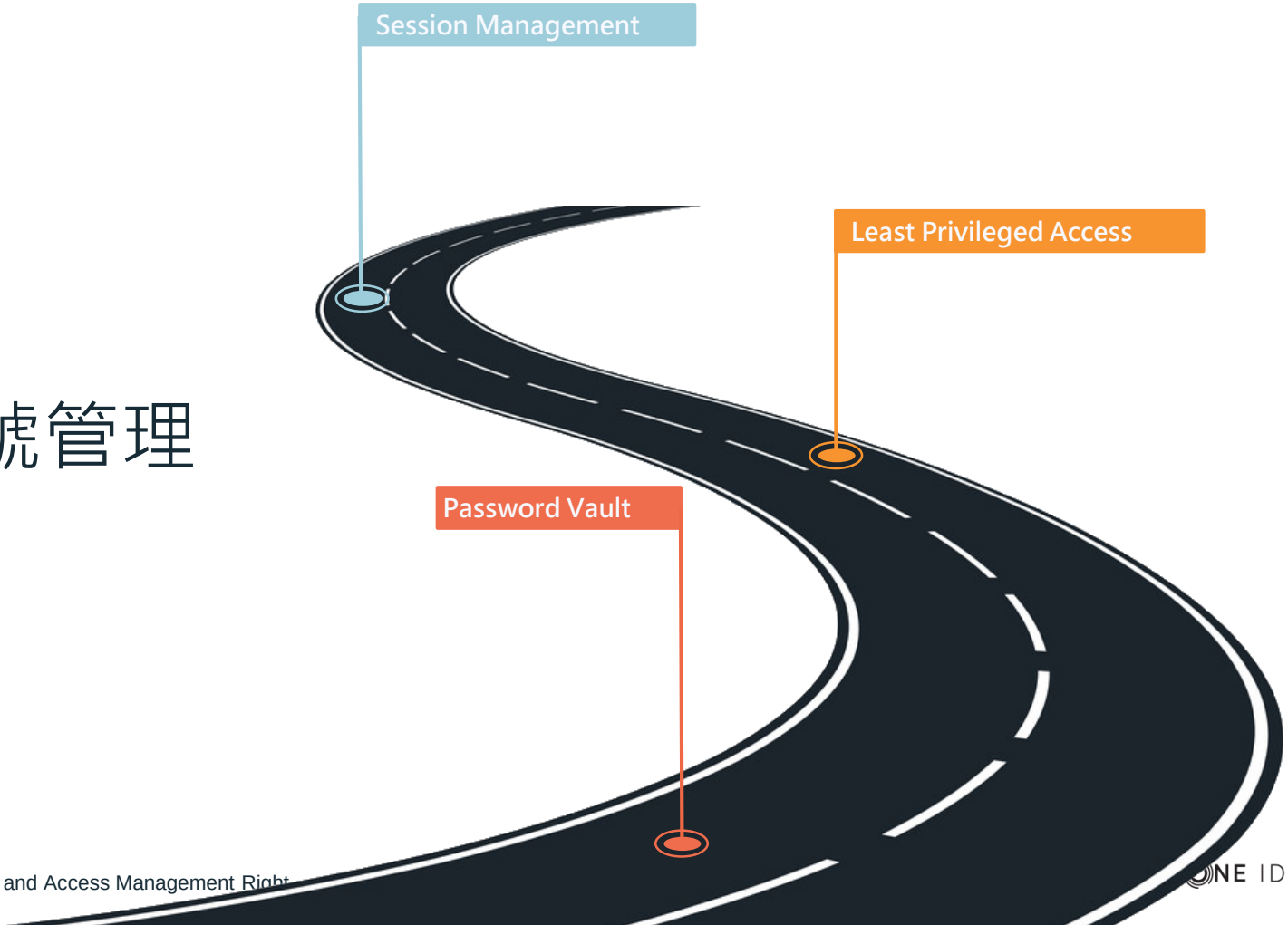
Source : Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques

ONE IDENTITY

特權帳號挑戰

- 共用帳號的問題：帳號多個人使用，帳號不具有唯一性，如果出現操作錯誤或者惡意操作，無法追查到當事者。
- 協力廠商操作的問題：如何監控委外人員和設備廠商的操作行為是企業面臨的一個關鍵問題。
- 特權帳號濫用：防火牆、入侵偵測系統等安全產品可以解決外部安全問題，但對於內部人員的違規操作卻無能為力。
- 密碼回收問題：人事異動時，特權帳號密碼難以回收或忘了回收。
- 密碼保管問題：密碼規則越來越複雜，記不住只好抄在紙上。
- 密碼變更問題：三個月須要換密碼一次，有200台主機需要換....。
- APT威脅：駭客會長期潛伏於內部，伺機取得特權帳號的密碼。

特權帳號管理


Session Management
Least Privileged Access
Password Vault

用治理角度看特權帳號管理系統：

治理是個重要議題，其主要目的乃透過管控制度的設計與執行，強化企業內部控制、有效監督，以健全企業組織的運作(Shleifer & Vishny, 1997；OECD, 2004)。

三個面向：

1. 特權帳號的登入機制
2. 特權帳號的規則設定
3. 發覺異常行為

強化系統的登入

確保登錄到系統人員的真實身份

- 實施密碼策略，將身份驗證強度調整？
- 在系統上實施雙因子驗證？
- 使用Federated Authentication?

特權帳號的規則設定

規則是以人作為出發點 -> 系統 -> 帳號

- 誰來設這個規則?
- 有沒有設錯?
- 誰同意這個規則?
- 多久稽核這個規則?
- 符合公司權責畫分(Segregation of Duties)的要求?

PAM 規則設定

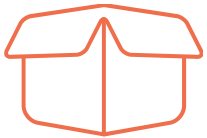
申請人	系統	帳號	審核者
James	Windows01	Administrator	Jim
James	Linux01	root	Dama
James	SQL01	sa	Jim
James	SQL02	sa	Jim

設定錯誤

自動核可
全選一次核可

規則盤點

Right individuals



Right resources

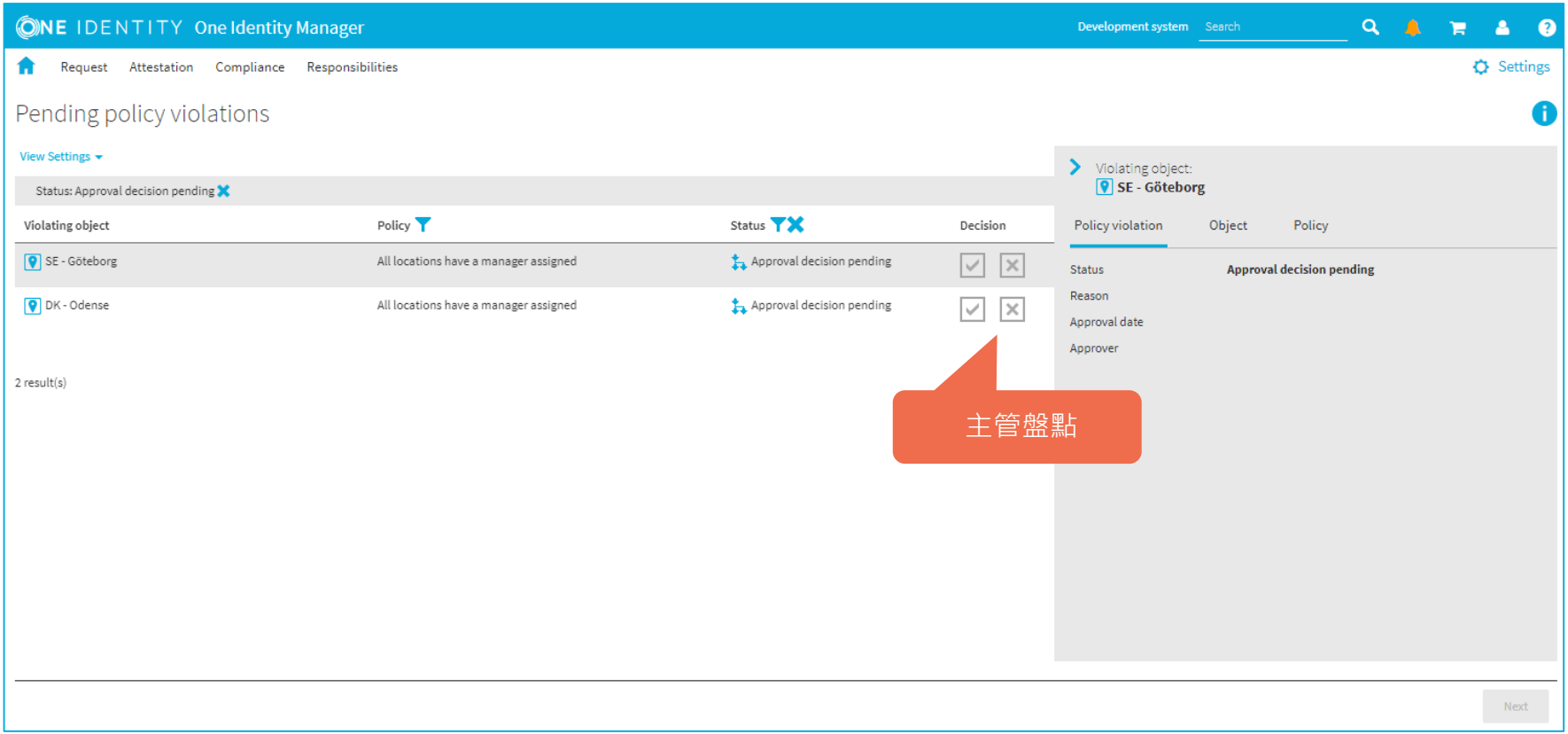
Right time

Right Approve

確保規則設定正確

- 每半年盤點規則一次？
- 使用身份治理工具？

帳號盤點


ONE IDENTITY One Identity Manager
Development system
Search
Request
Attestation
Compliance
Responsibilities
Settings
Pending policy violations
View Settings
Status: Approval decision pending
Violating object
Policy
Status
Decision
SE - Göteborg
All locations have a manager assigned
Approval decision pending
DK - Odense
All locations have a manager assigned
Approval decision pending
2 result(s)
Violating object:
SE - Göteborg
Policy violation
Object
Policy
Status
Approval decision pending
Reason
Approval date
Approver
主管盤點
Next

PAM 規則設定

申請人	系統	帳號	審核者
James	Windows01	Administrator	Jim
James	Linux01	root	Dama
James	SQL01	sa	Jim
James	SQL02	sa	Jim

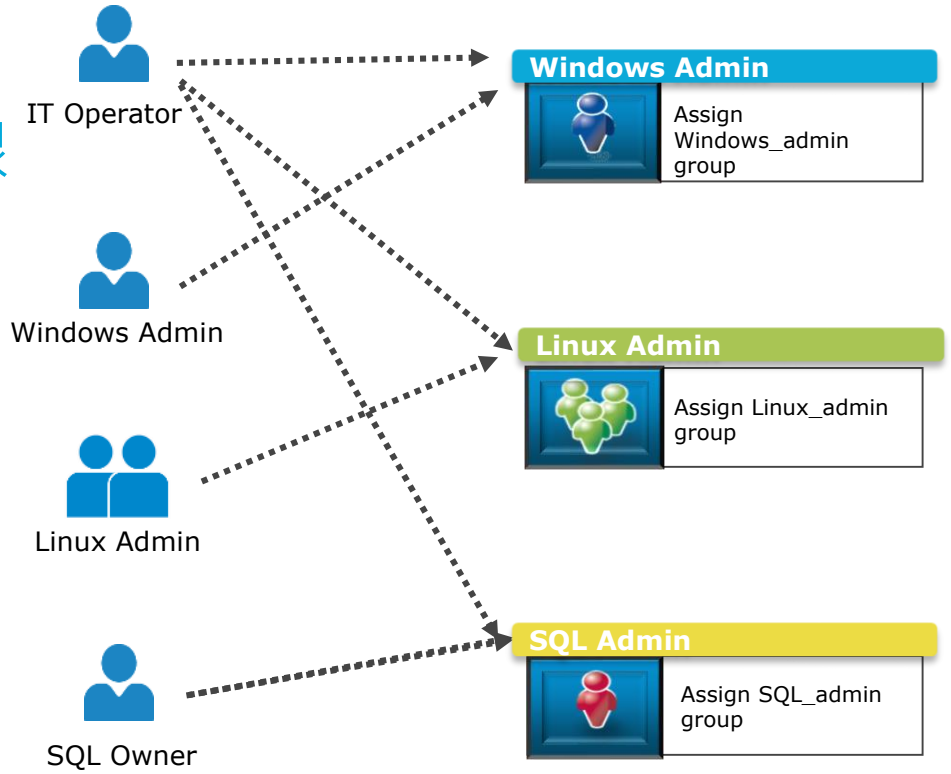
PAM 規則設定

申請群組	系統	帳號	審核者
Windows_Admin	Windows01	Administrator	Jim
Linux_Admin	Linux01	root	Dama
SQL_Admin	SQL01	sa	Jim
	SQL02	sa	Jim

規則授權管理

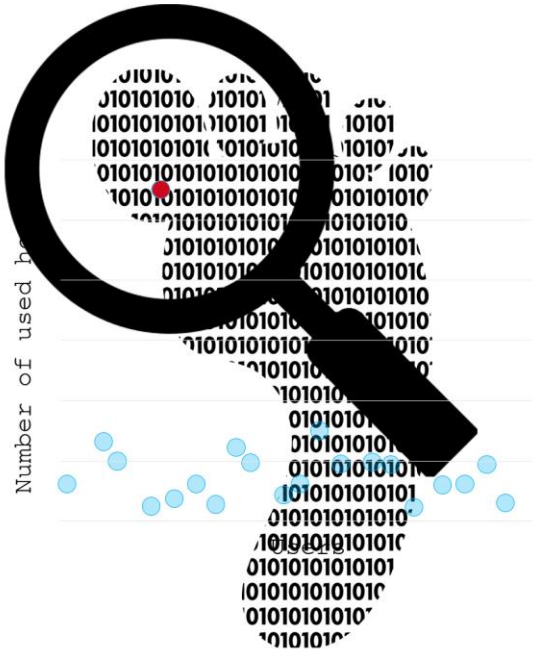
管理方法

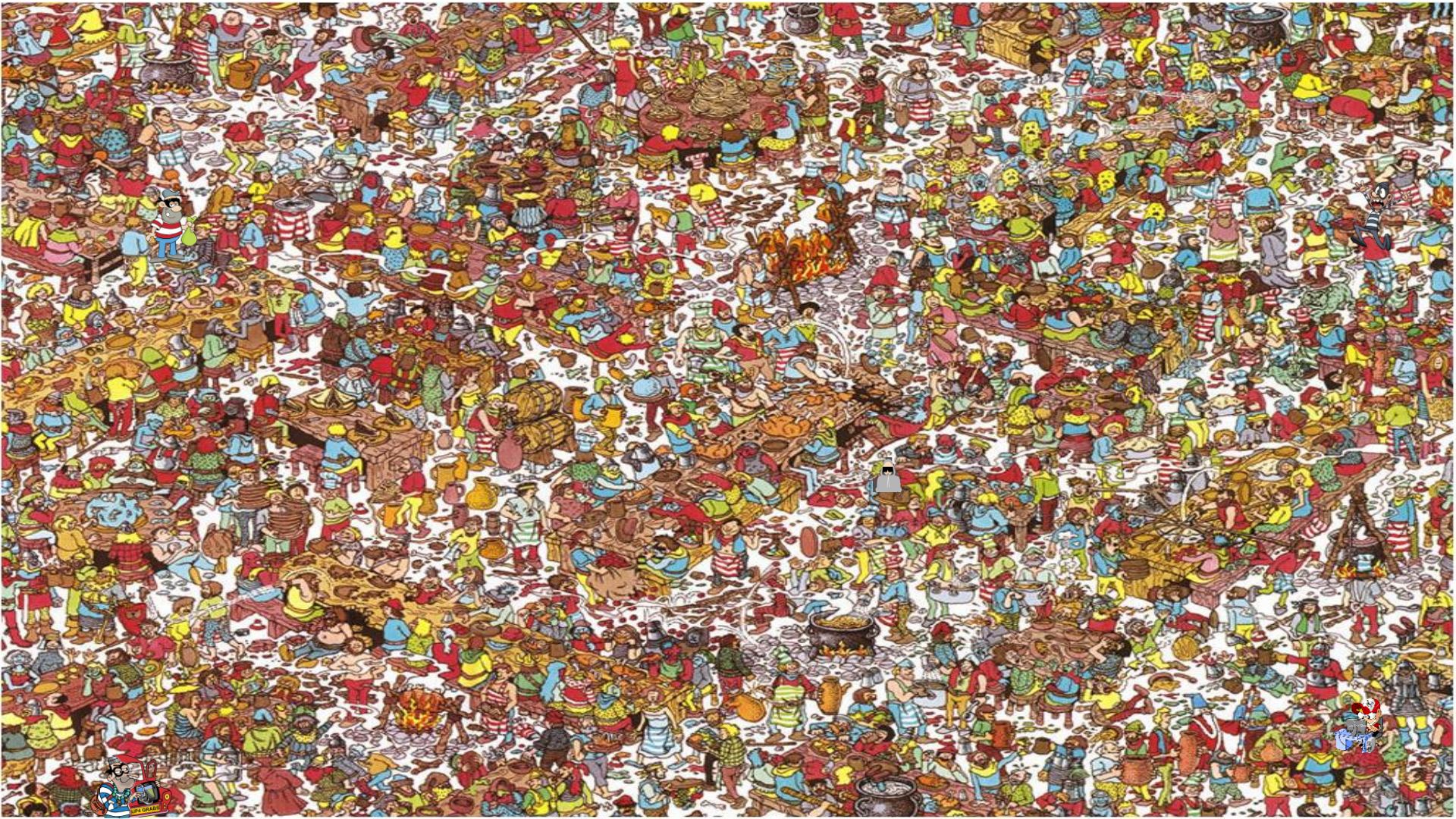
- 回收Domain Admin權限
- 建立分層授權
- 建立授權流程
- 保留授權紀錄



發覺異常行為

錄影持續在運作，但是那些有異常行為?

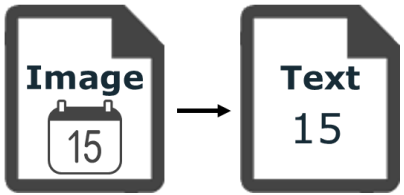




關鍵字搜尋 - OCR技術

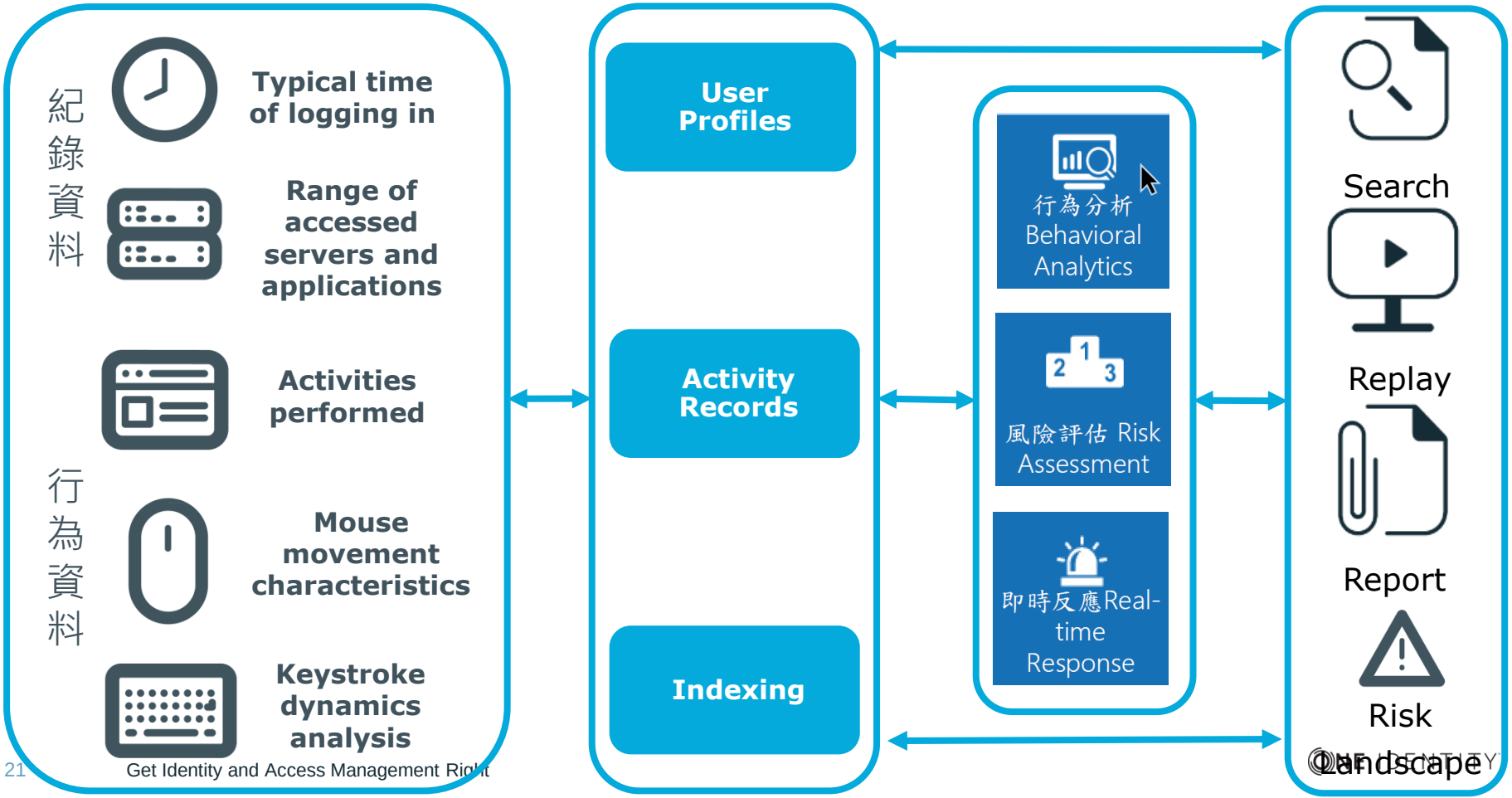
文字搜索

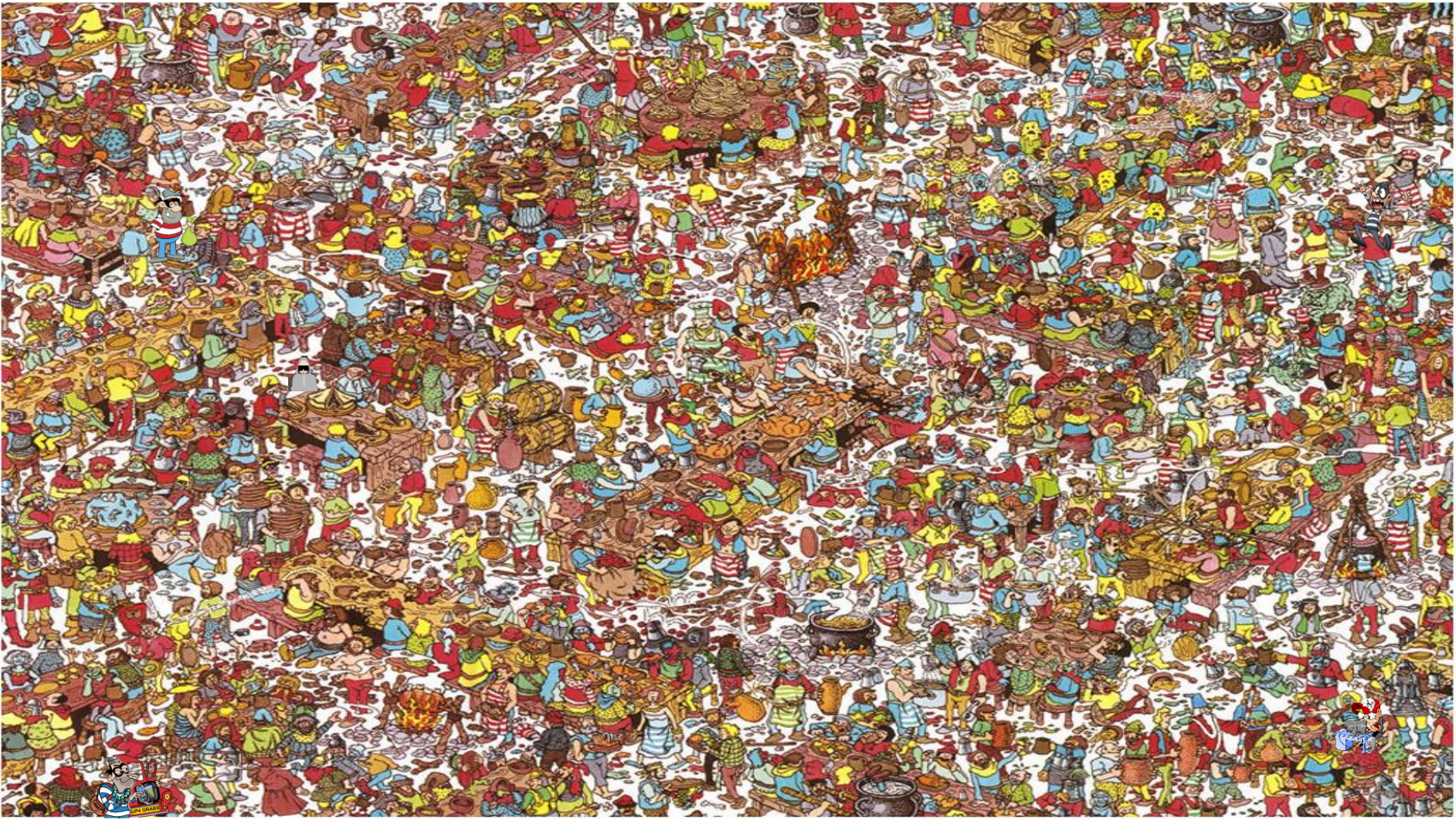
圖片-光學辨視



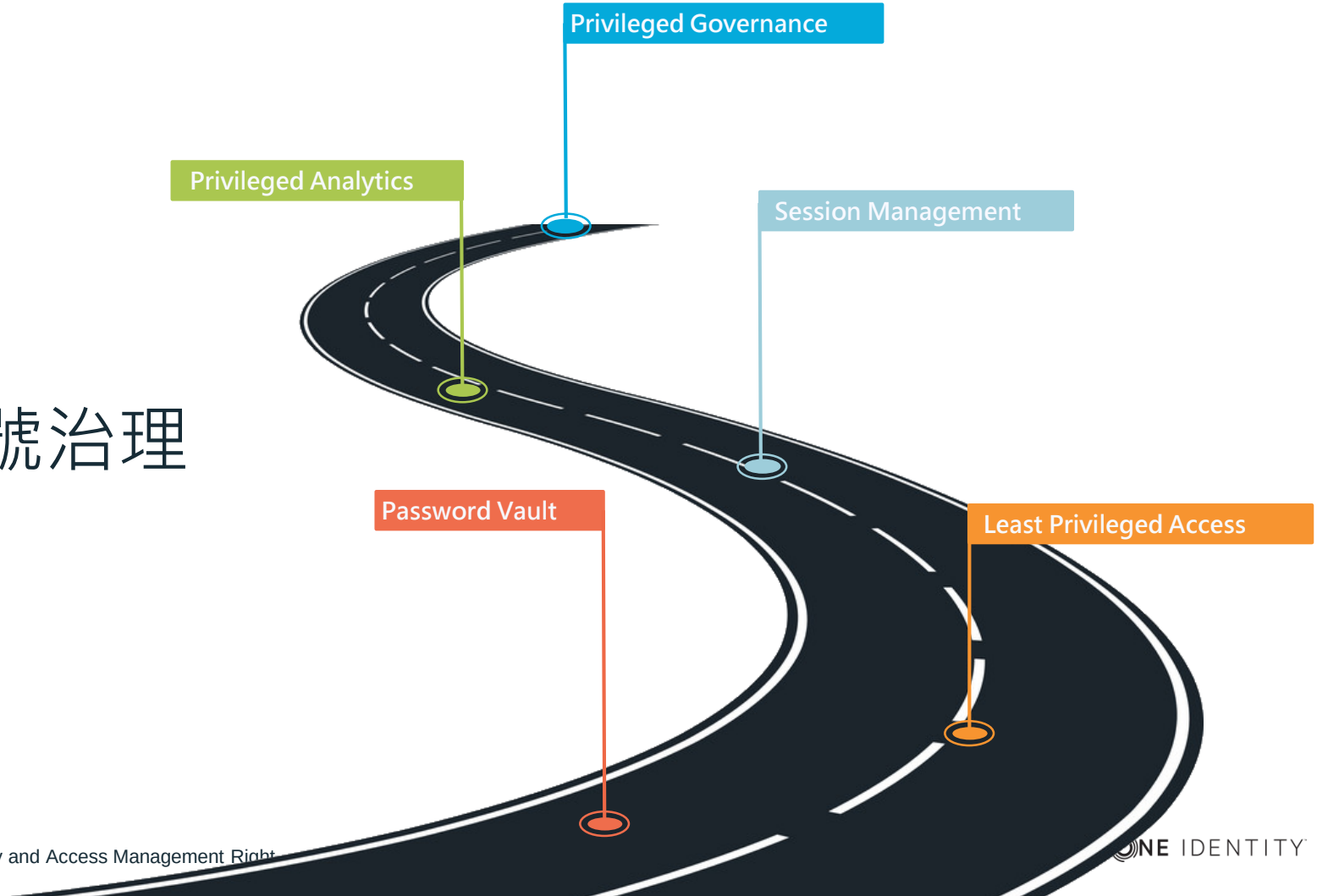
ONE IDENTITY

行為分析 - 平台架構

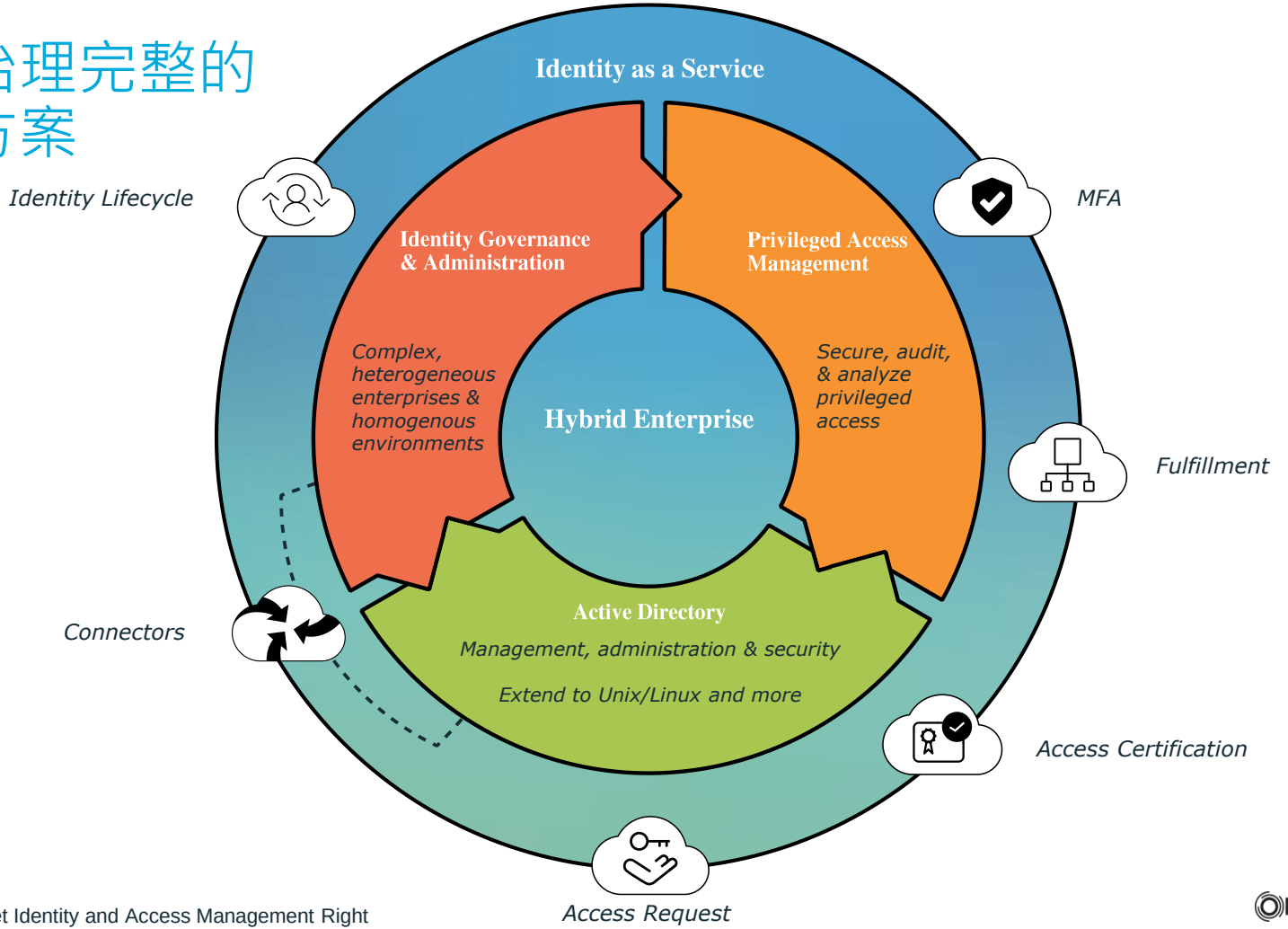

紀錄資料
Typical time of logging in
Range of accessed servers and applications
Activities performed
行為資料
Mouse movement characteristics
Keystroke dynamics analysis
User Profiles
Activity Records
Indexing
行為分析 Behavioral Analytics
風險評估 Risk Assessment
即時反應Real-time Response
Search
Replay
Report
Risk
Landscape



特權帳號治理

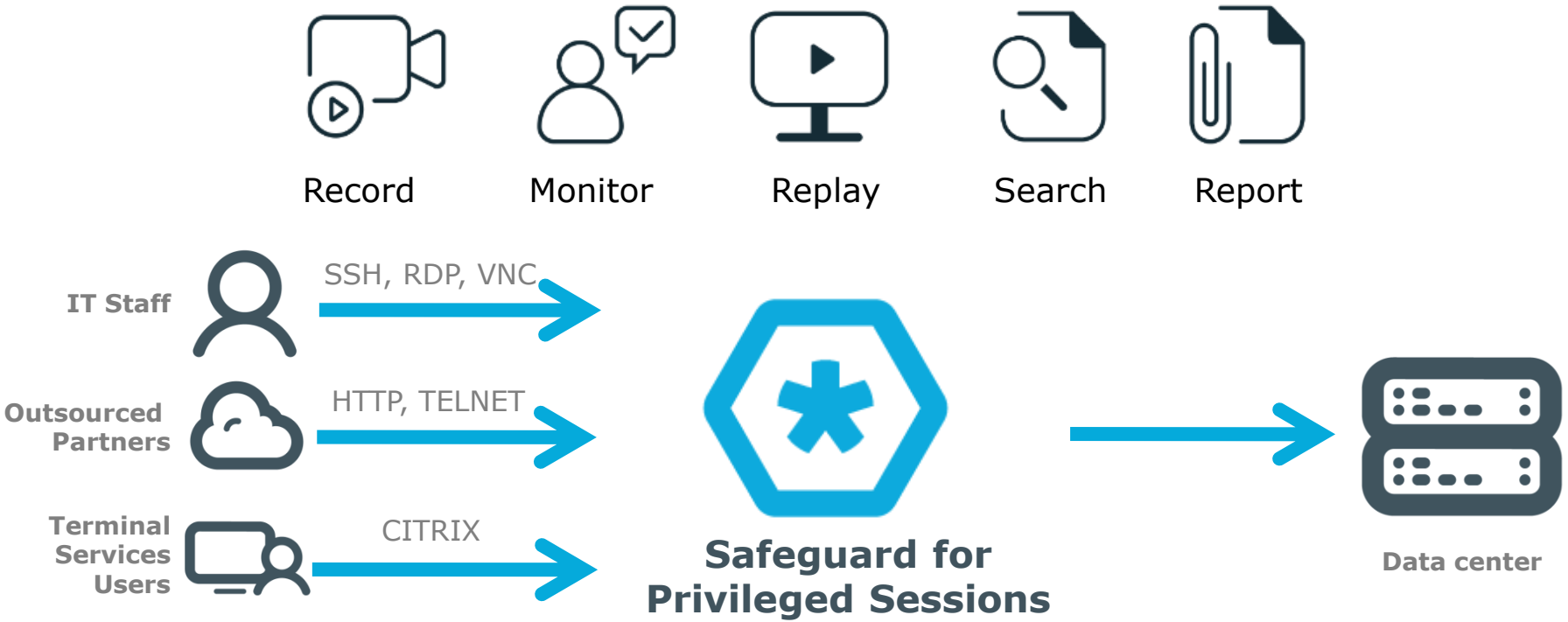

Privileged Governance
Privileged Analytics
Session Management
Password Vault
Least Privileged Access

身分治理完整的解決方案



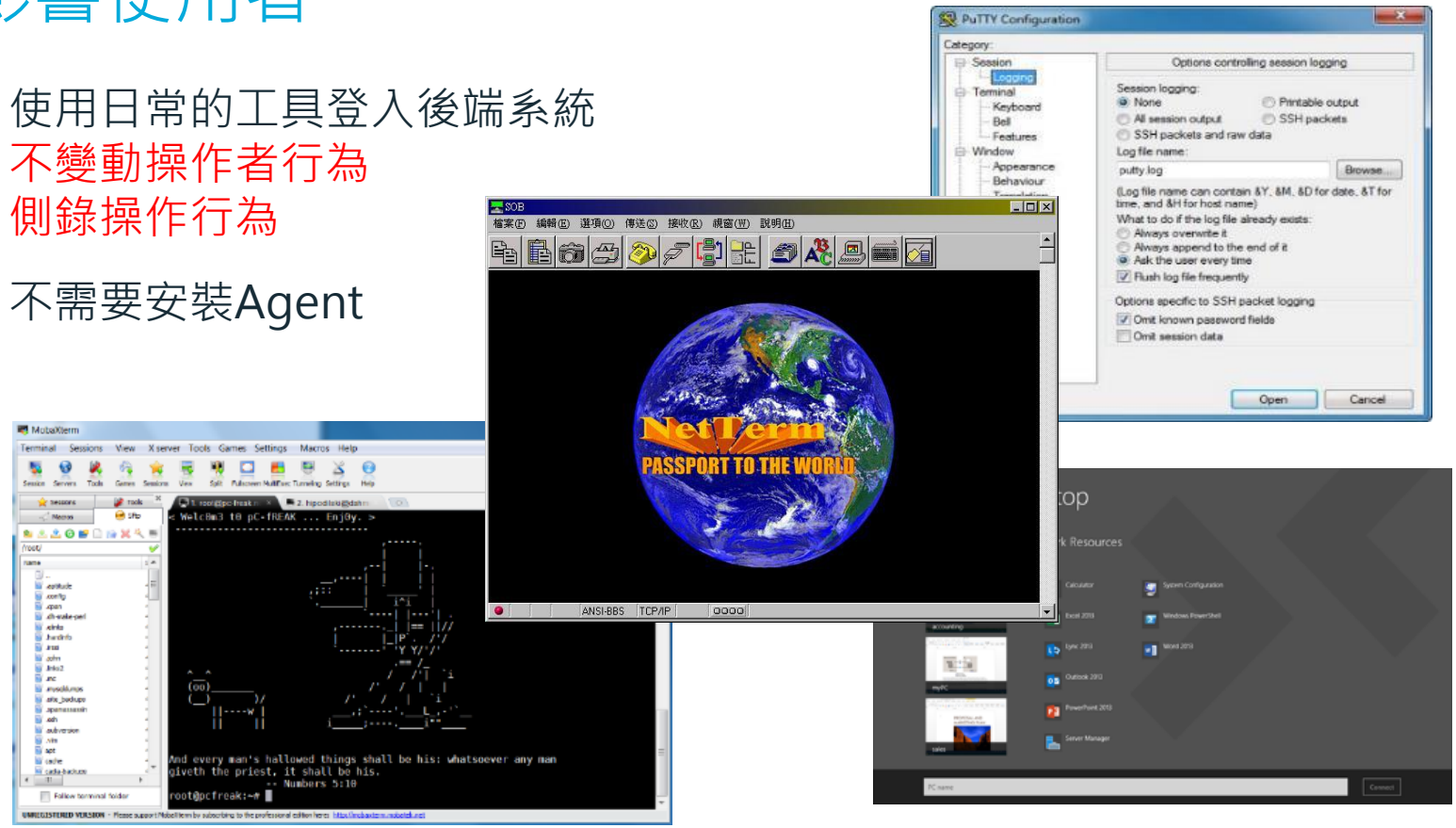
ONE IDENTITY

側錄功能 – 保護重要資產


Record
Monitor
Replay
Search
Report
IT Staff
SSH, RDP, VNC
Outsourced Partners
HTTP, TELNET
Terminal Services Users
CITRIX
Safeguard for Privileged Sessions
Data center

不影響使用者

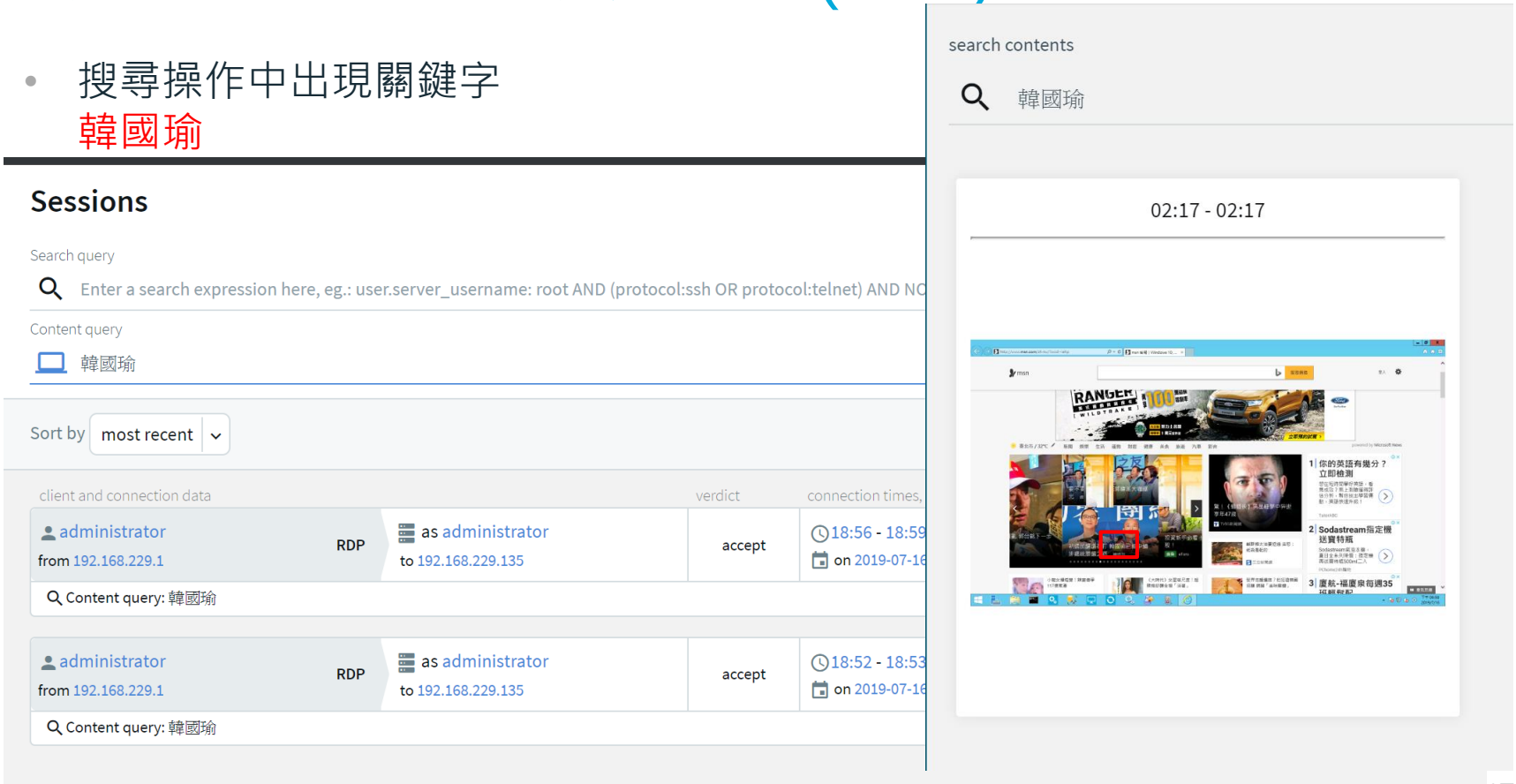
- 使用日常的工具登入後端系統
  不變動操作者行為
  側錄操作行為
- 不需要安裝Agent



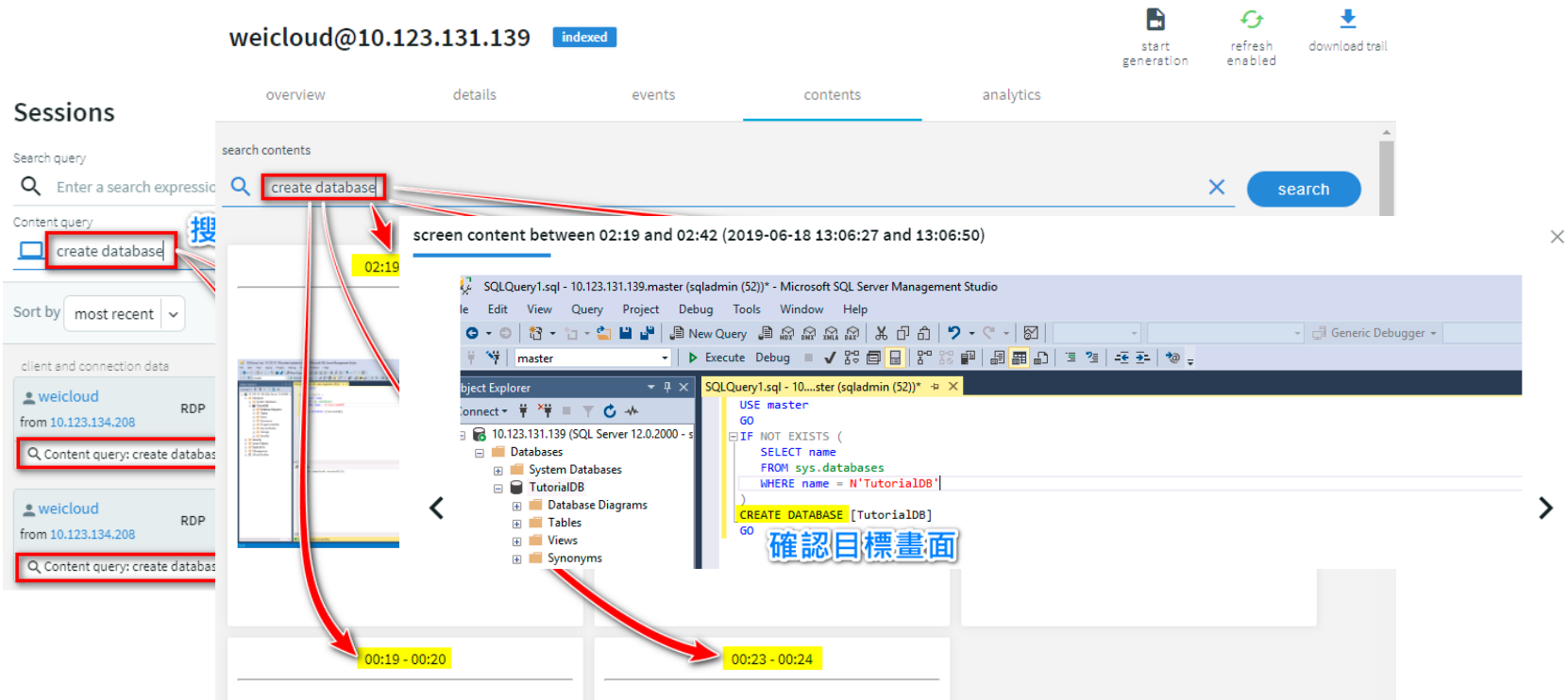
ONE IDENTITY

自動建立索引 - 影像文字辨識(繁中)

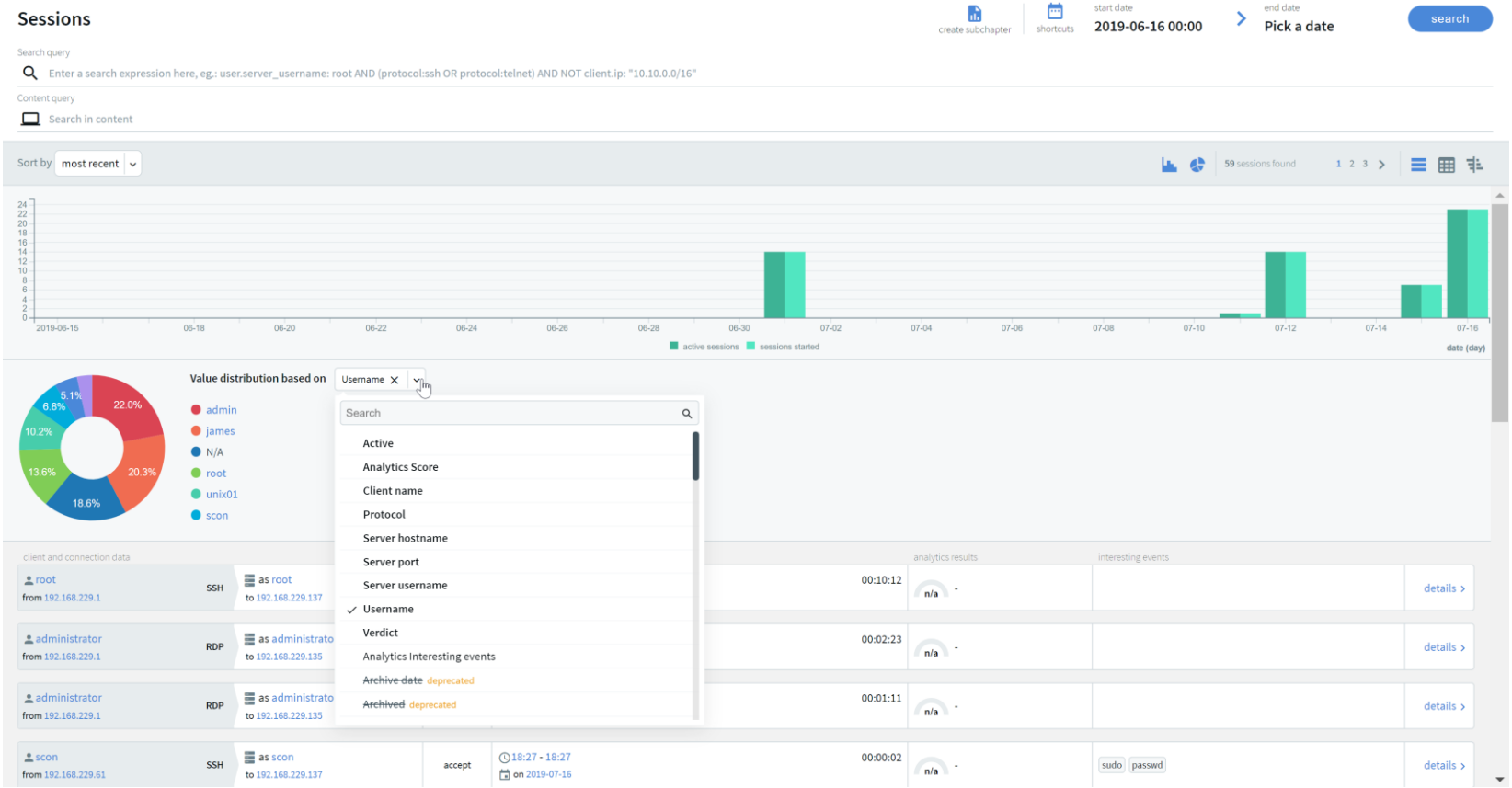
- 搜尋操作中出現關鍵字
  韓國瑜



自動建立索引 - 影像文字辨識

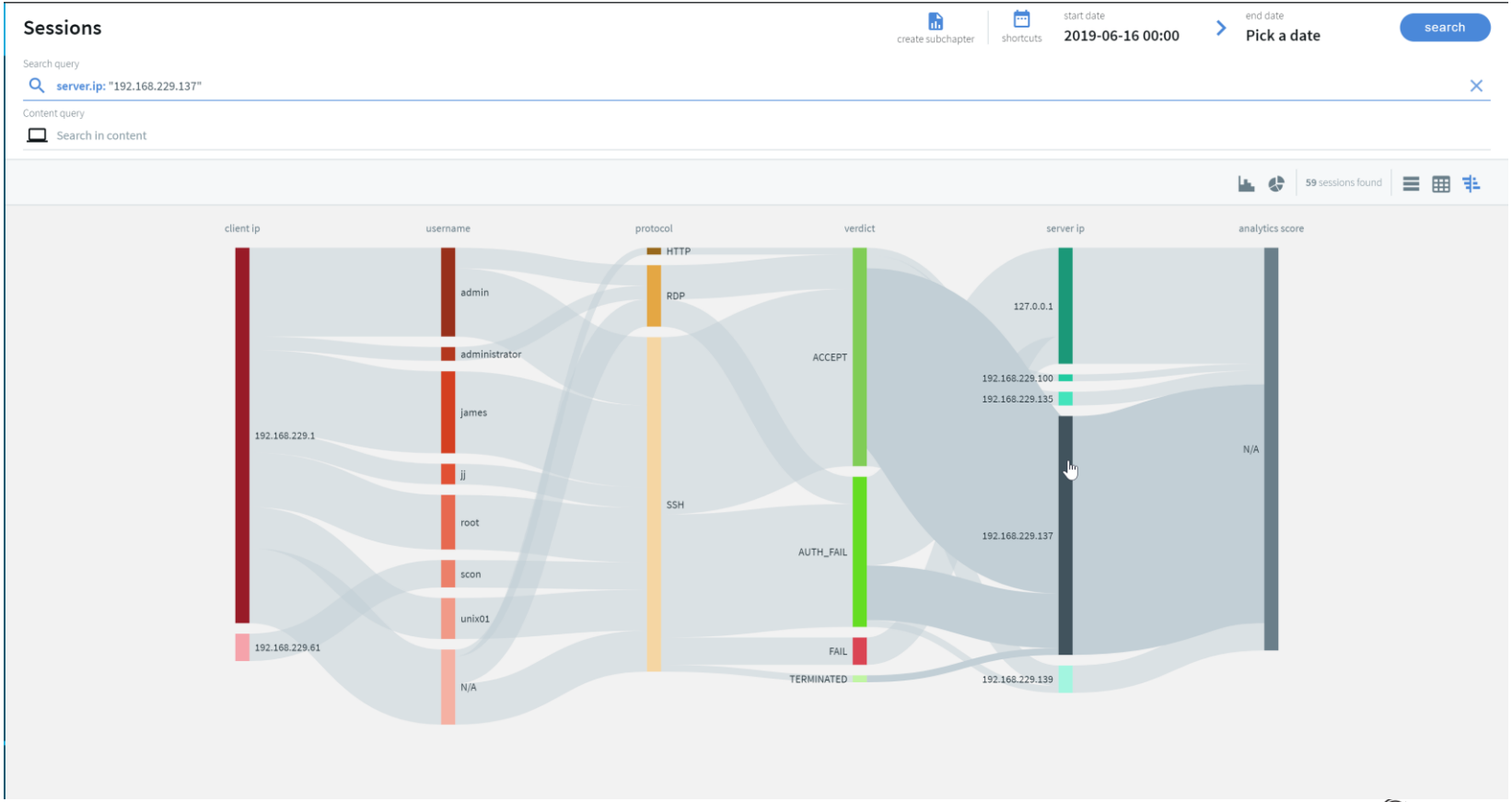


多樣性的分析

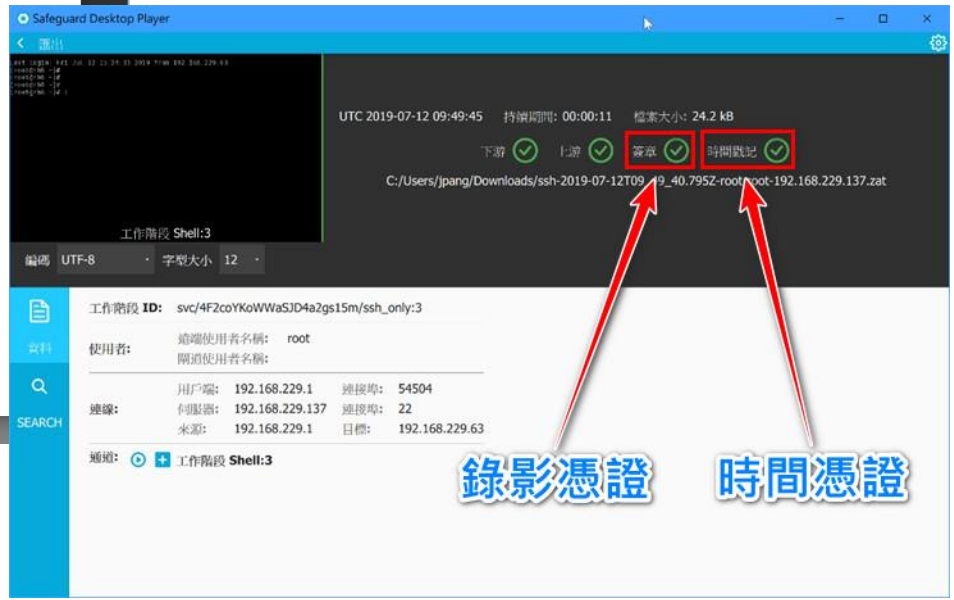


ONE IDENTITY

多樣性的分析



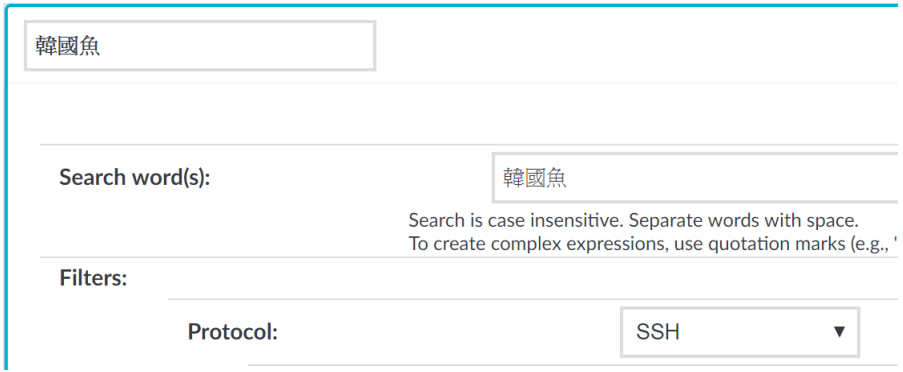
紀錄不可竄改 - 不可否認

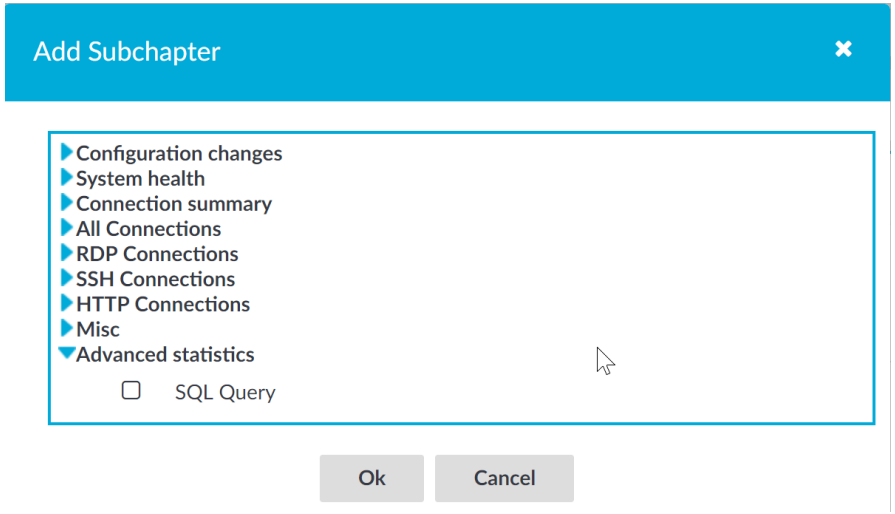


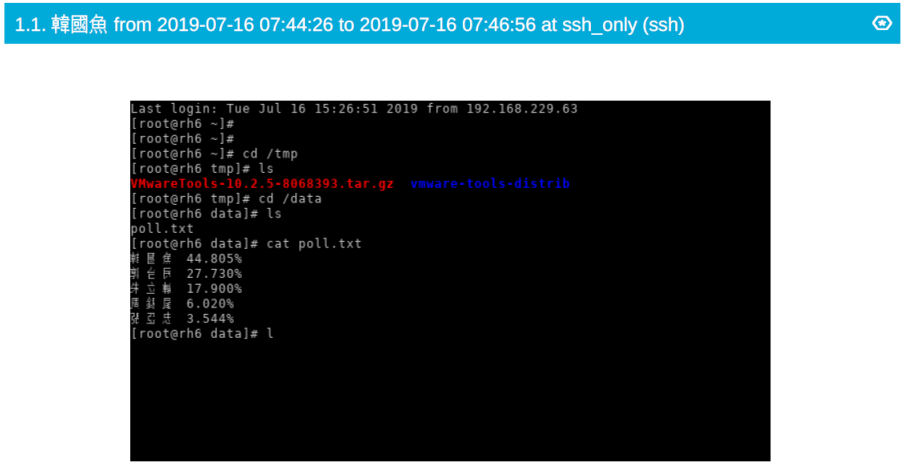
ONE IDENTITY

報表

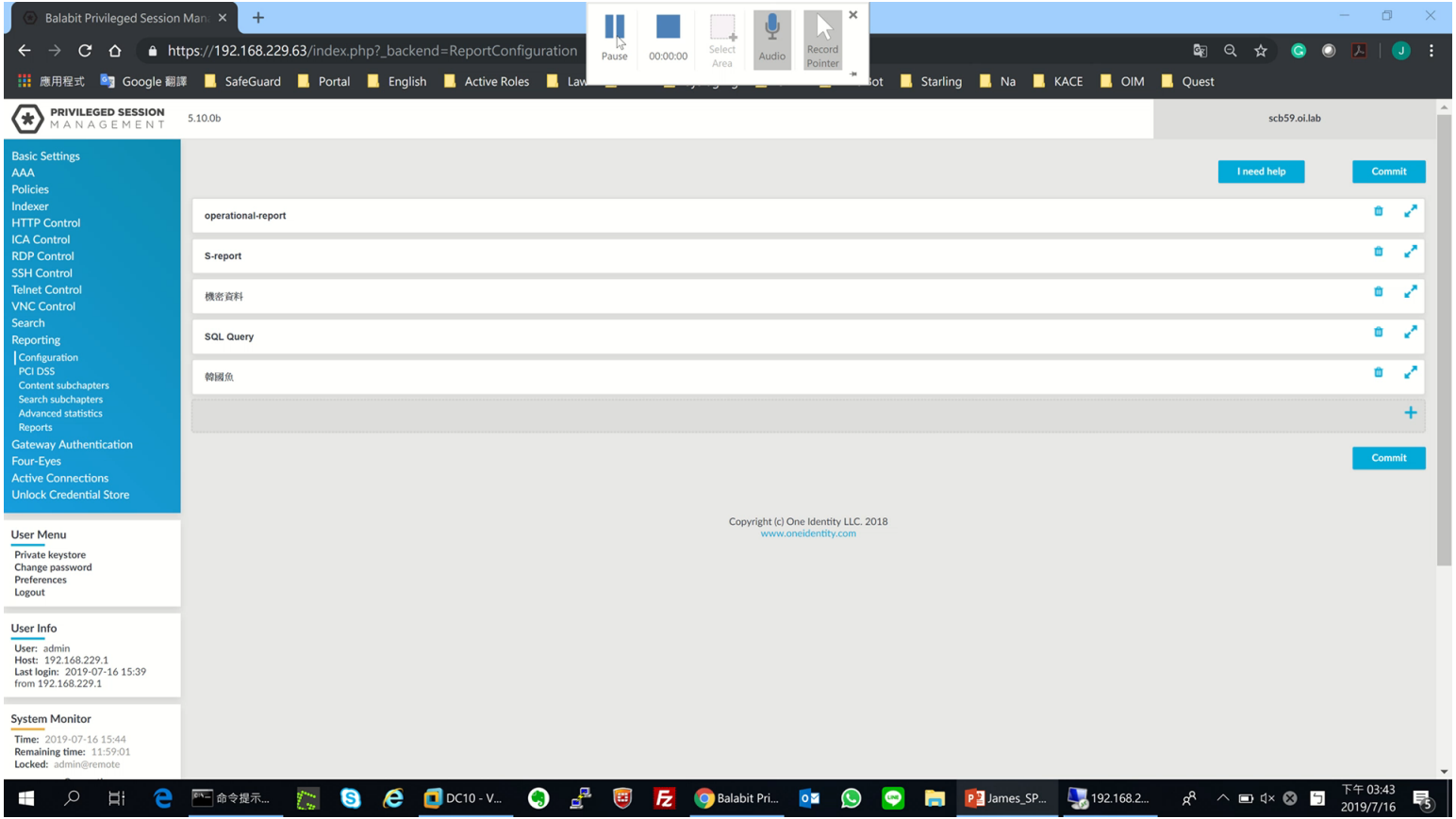
- 操作中出現關鍵字，可設定直接轉成報表輸出。
- 可設定排程，定時發送給管理者。
- 提供API。



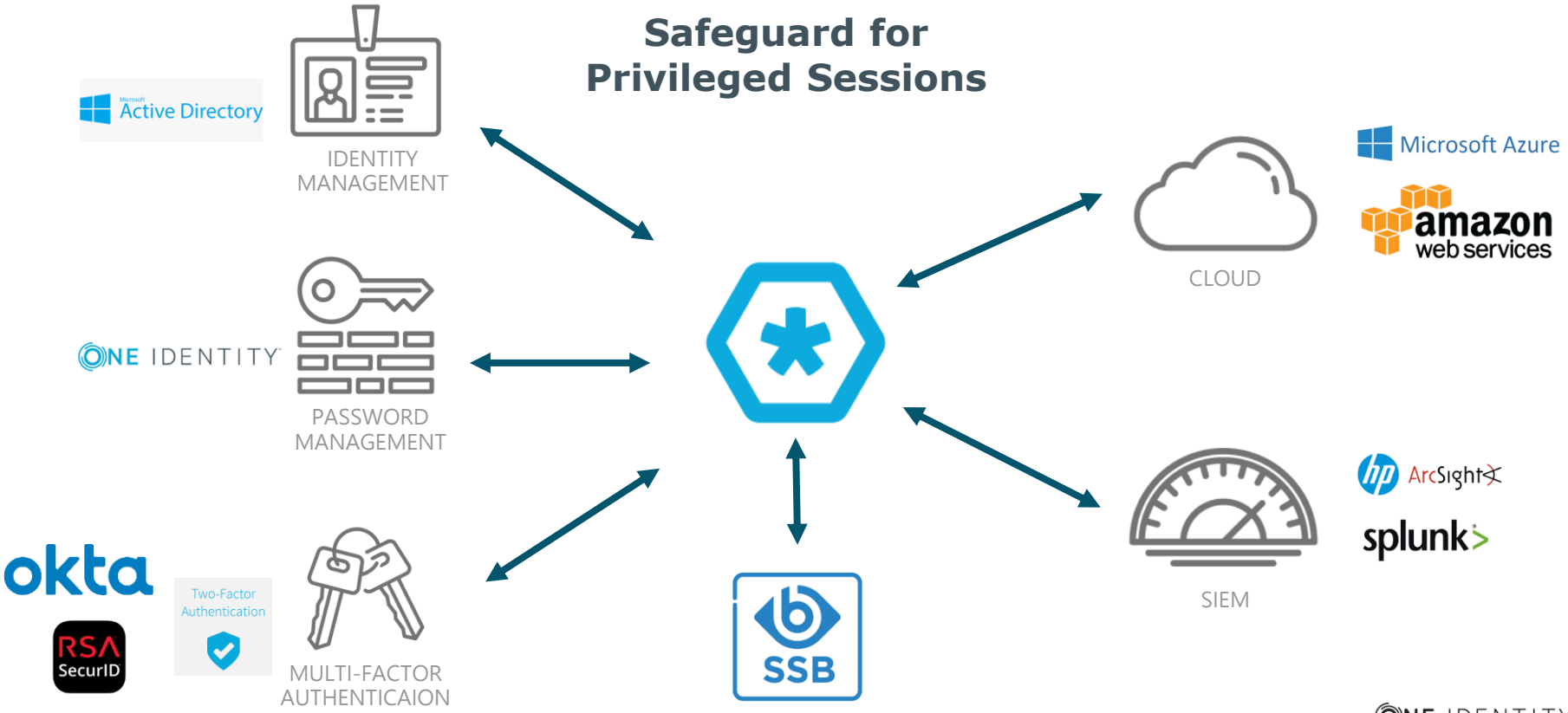




Demo

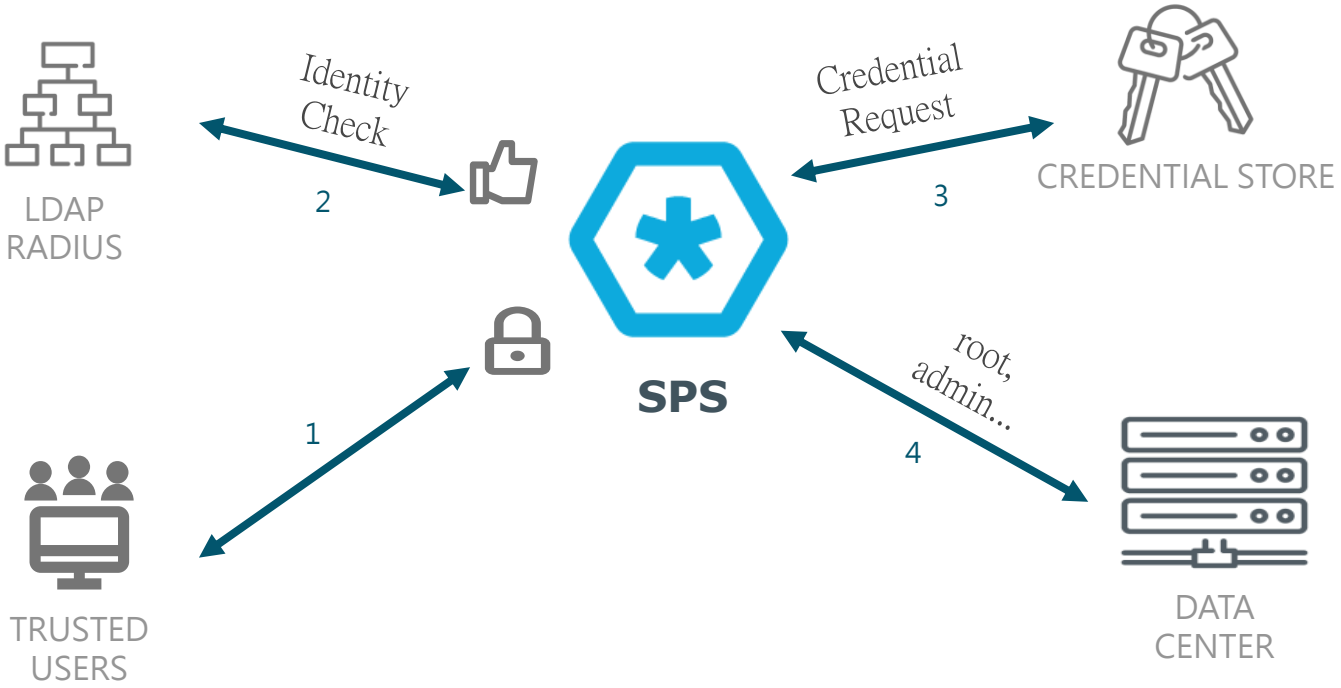

Balabit Privileged Session Man
https://192.168.229.63/index.php?_backend=ReportConfiguration
Pause
00:00:00
Select Area
Audio
Record Pointer
PRIVILEGED SESSION MANAGEMENT
5.10.0b
scb59.oi.lab
Basic Settings
AAA
Policies
Indexer
HTTP Control
ICA Control
RDP Control
SSH Control
Telnet Control
VNC Control
Search
Reporting
Configuration
PCI DSS
Content subchapters
Search subchapters
Advanced statistics
Reports
Gateway Authentication
Four-Eyes
Active Connections
Unlock Credential Store
I need help
Commit
operational-report
S-report
機密資料
SQL Query
韓國魚
Commit
Copyright (c) One Identity LLC. 2018
www.oneidentity.com
User Menu
Private keystore
Change password
Preferences
Logout
User Info
User: admin
Host: 192.168.229.1
Last login: 2019-07-16 15:39
from 192.168.229.1
System Monitor
Time: 2019-07-16 15:44
Remaining time: 11:59:01
Locked: admin@remote

整合

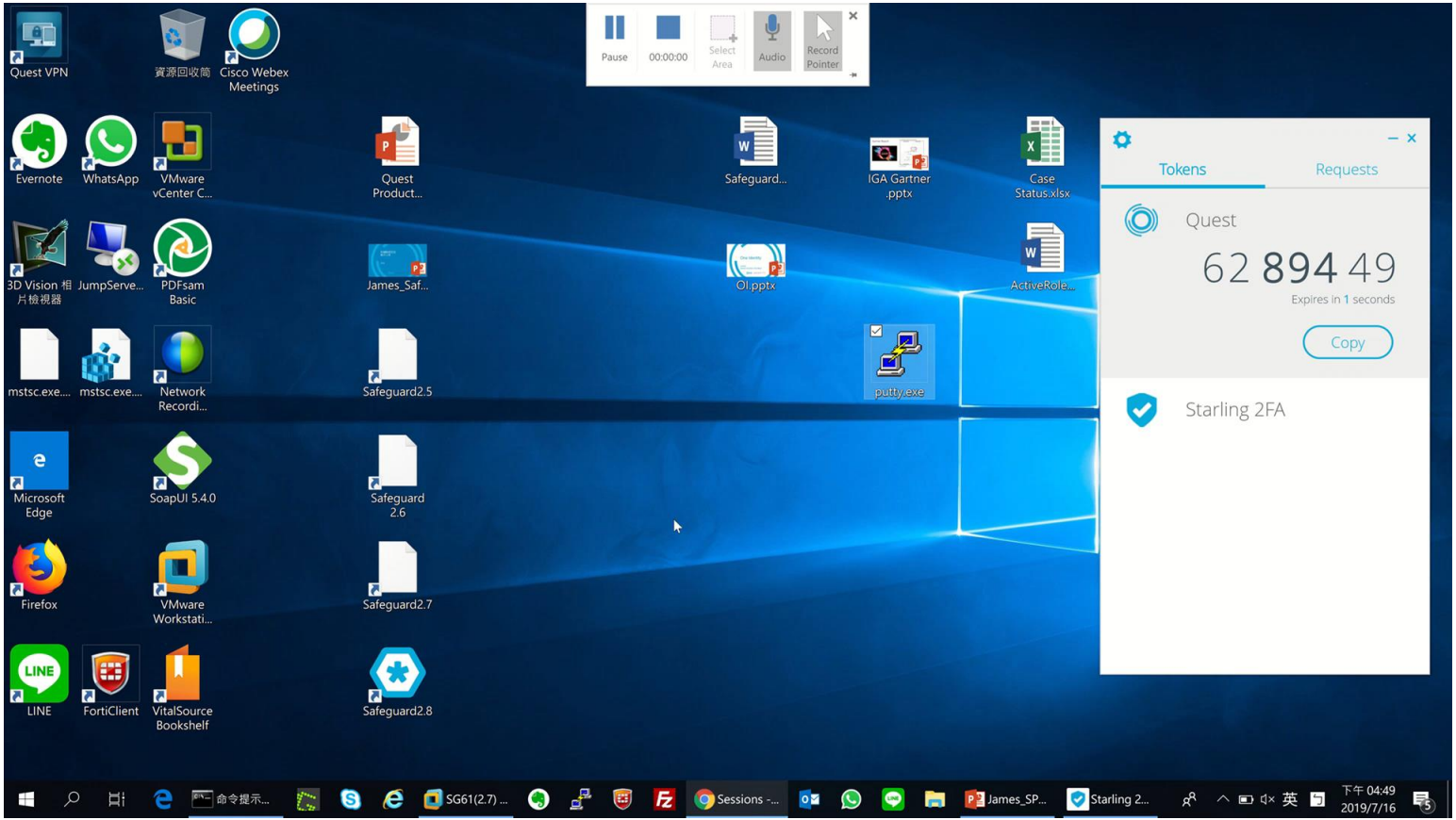


ONE IDENTITY

應用情境分享 – 認證後，自動代登



Demo



ONE IDENTITY

Thank You!
Questions?


ONE IDENTITY™