

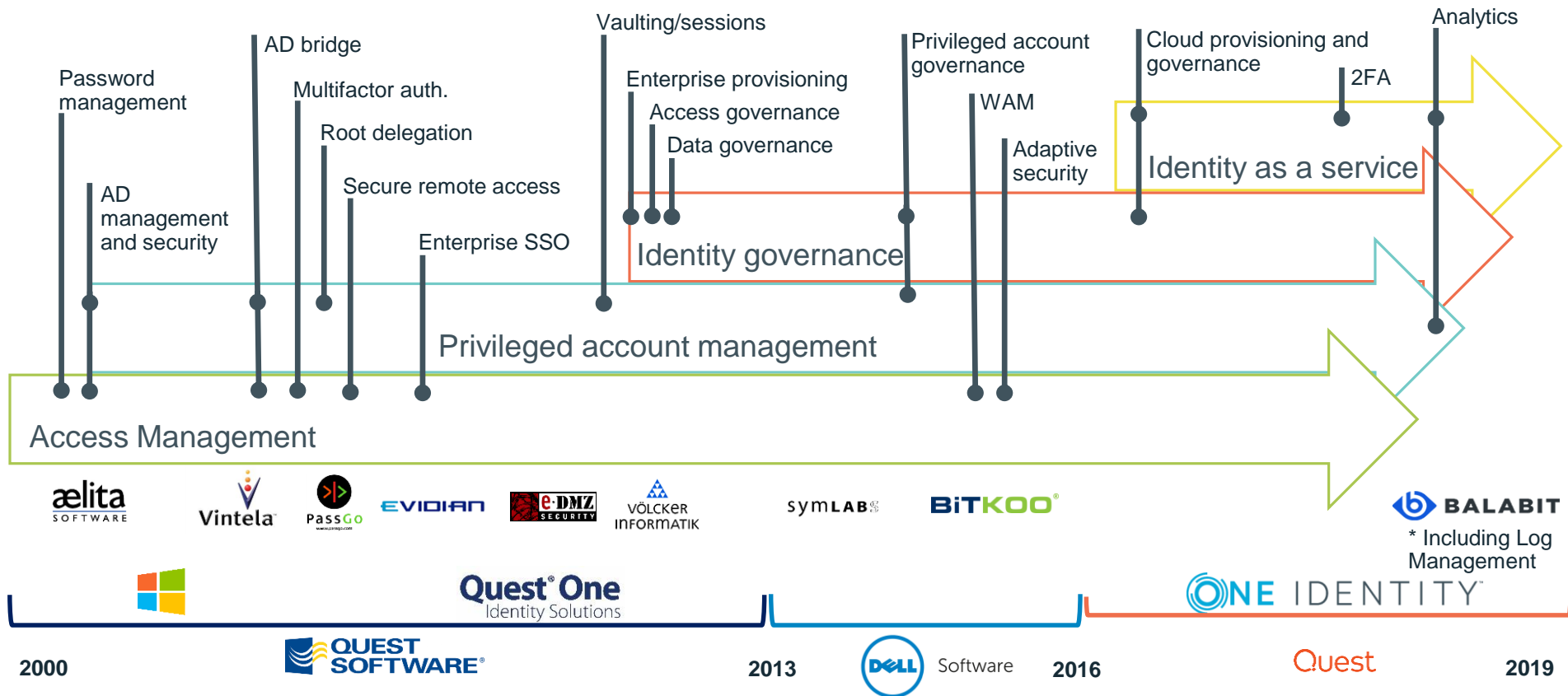
# 缺乏治理的特權帳號系統， 才是最大的資安漏洞

亞太區高級架構師

龐祥雲 James



# History



# 身分治理 Gartner Report

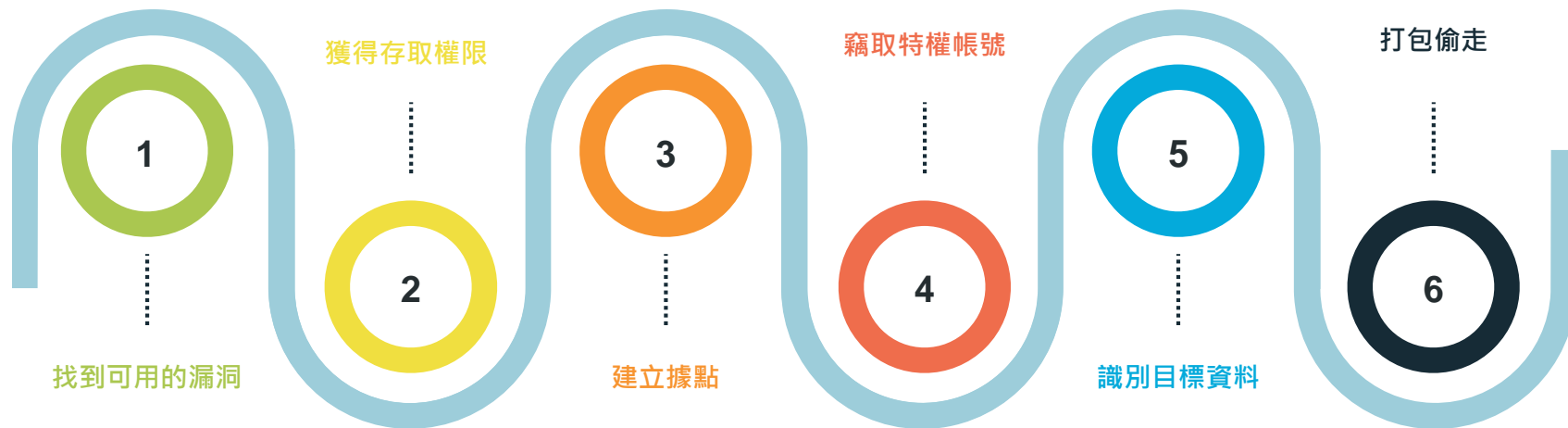


Figure 1. Magic Quadrant for Identity Governance and Administration



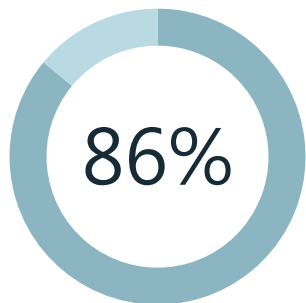
Source: Gartner (February 2018)

# Cyber Attack Lifecycle

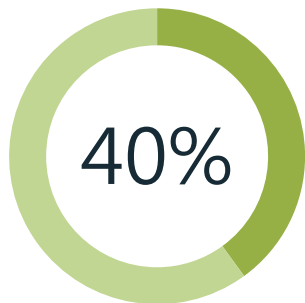


- Global Average to detect cyber incident is 78 days\*
- 204 days for APAC based organization\*

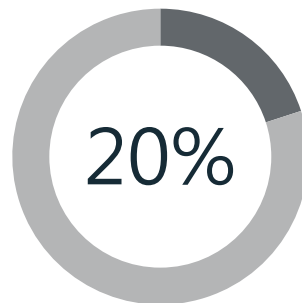
# 密碼使用行為統計



每次使用特權帳號不會變更密碼

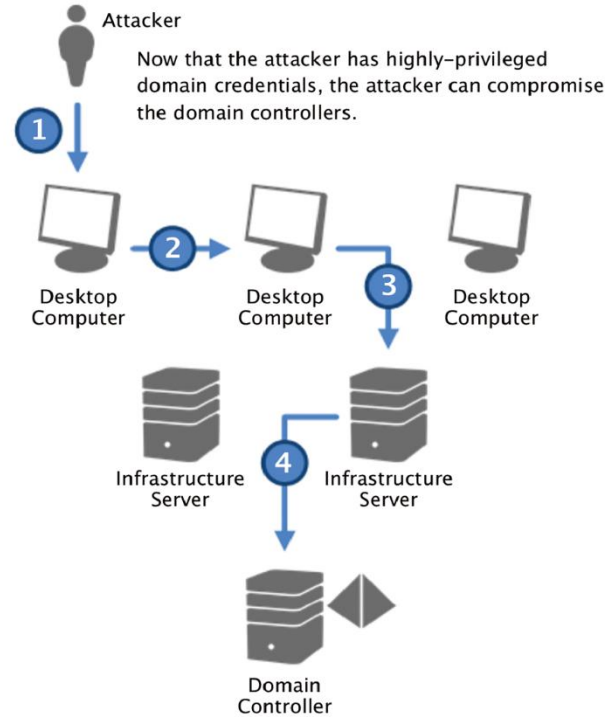
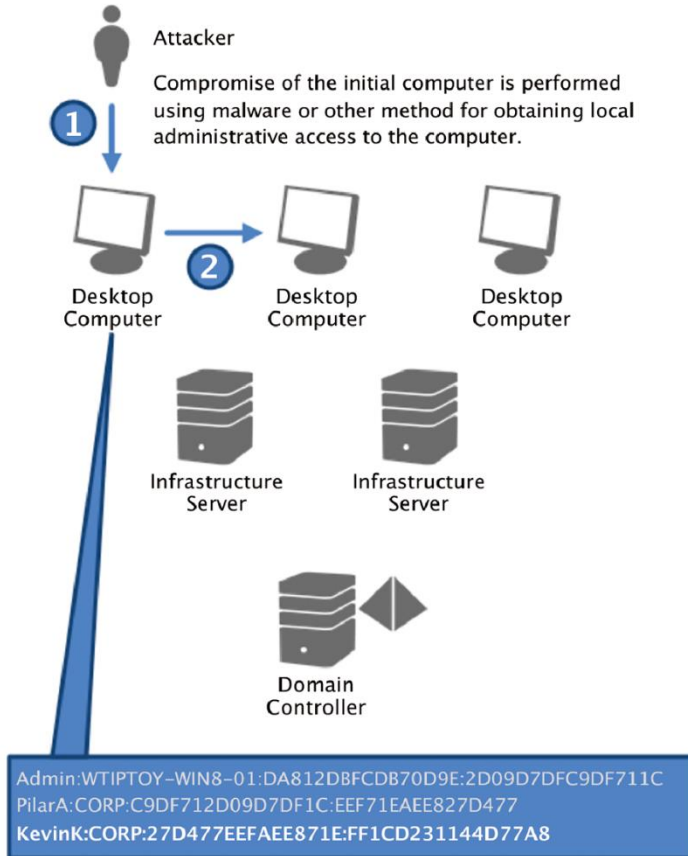


重要系統沒有變更admin的預設密碼



使用紙紀錄特權帳號密碼

# Pass-the-Hash (PtH) Attacks

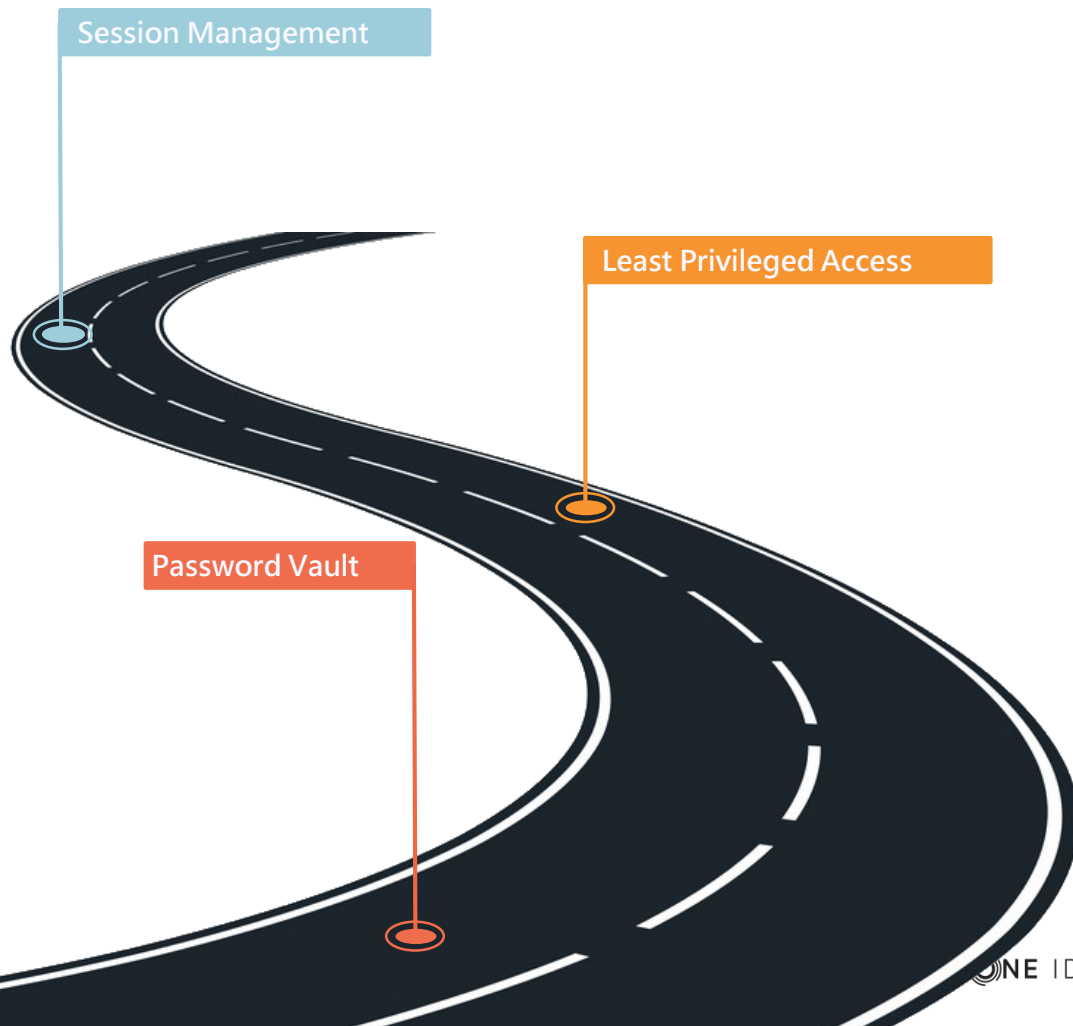


Source : Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques

# 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





## 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?



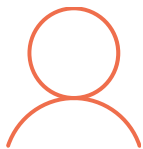
# PAM 規則設定

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

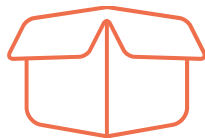
設定錯誤

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

## 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	<input checked="" type="checkbox"/> <input type="checkbox"/>
DK - Odense	All locations have a manager assigned	Approval decision pending	<input checked="" type="checkbox"/> <input type="checkbox"/>

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

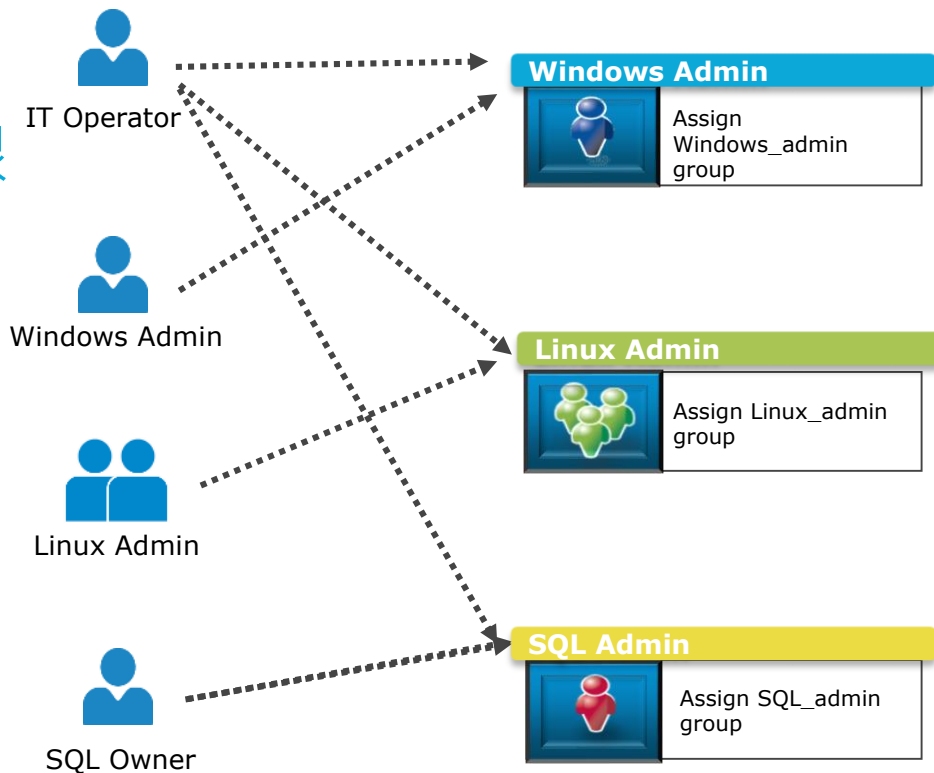
- 
1. 群組
  2. 授權交給  
AD



# 規則授權管理

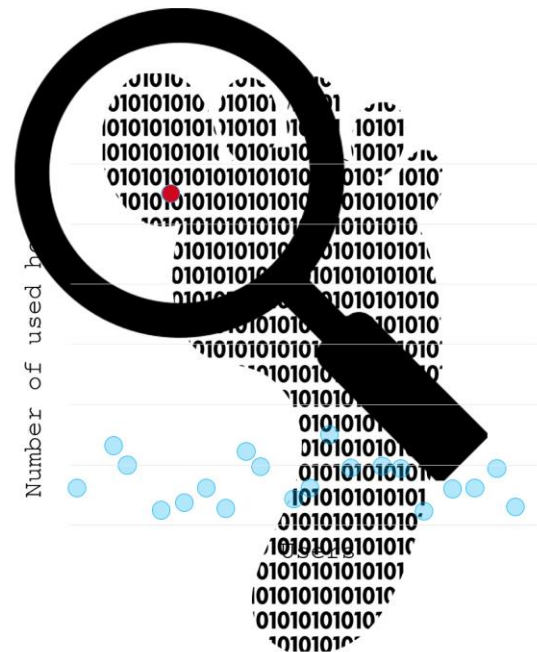
## 管理方法

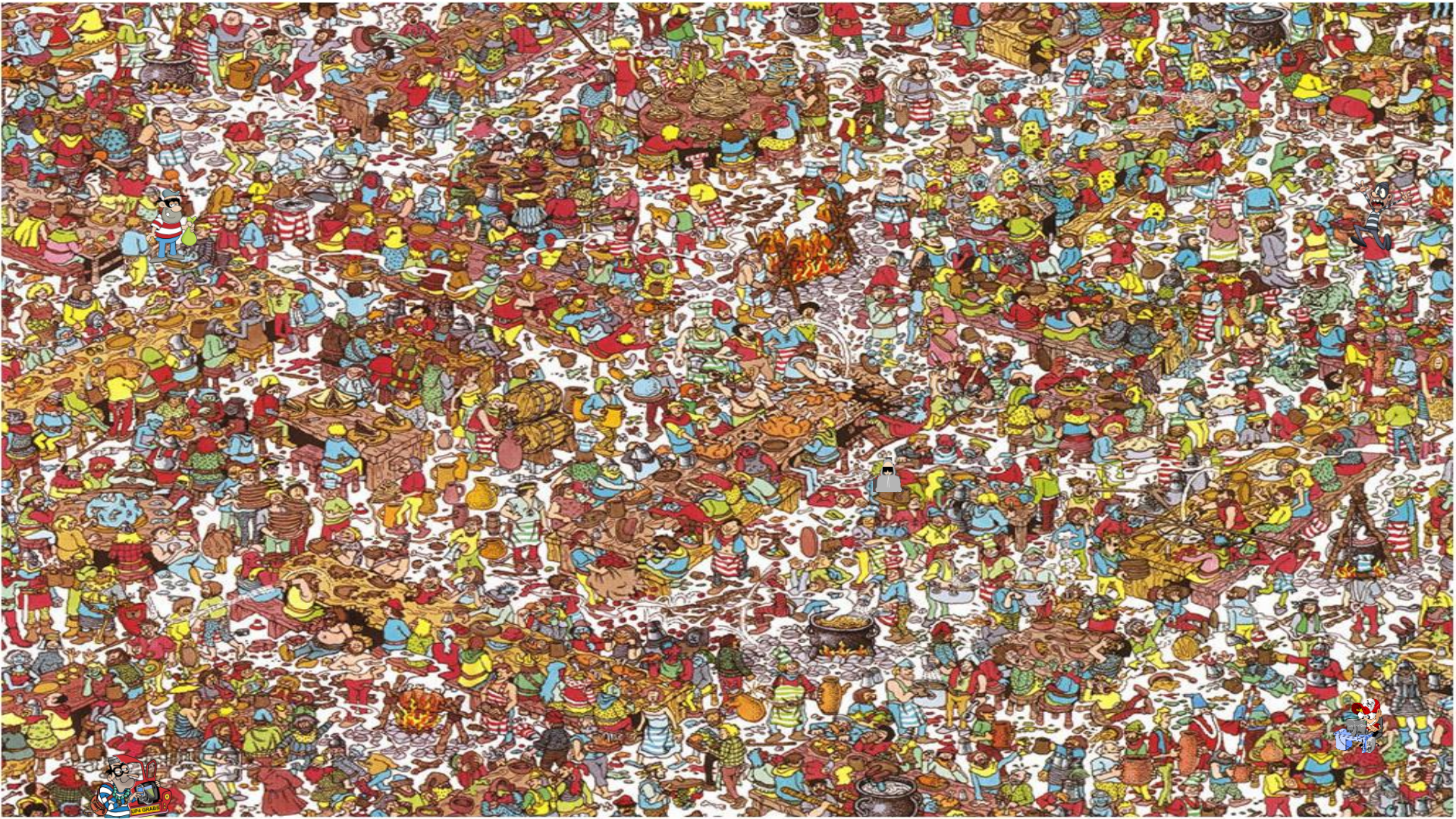
- 回收Domain Admin權限
- 建立分層授權
- 建立授權流程
- 保留授權紀錄



# 發覺異常行為

錄影持續在運作，但是那些有異常行為？



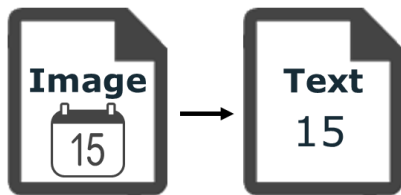


# 關鍵字搜尋 - OCR技術

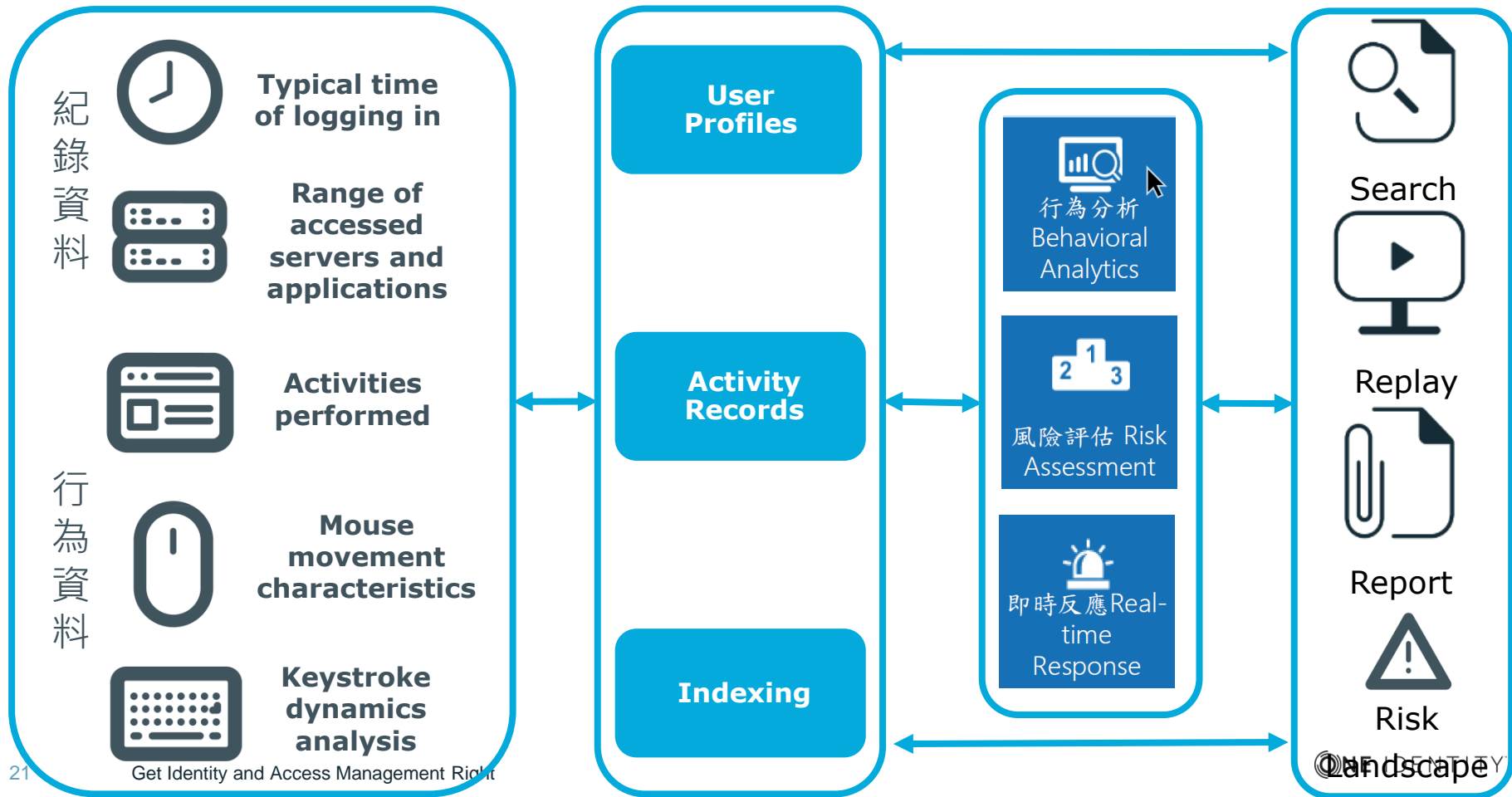
文字搜索

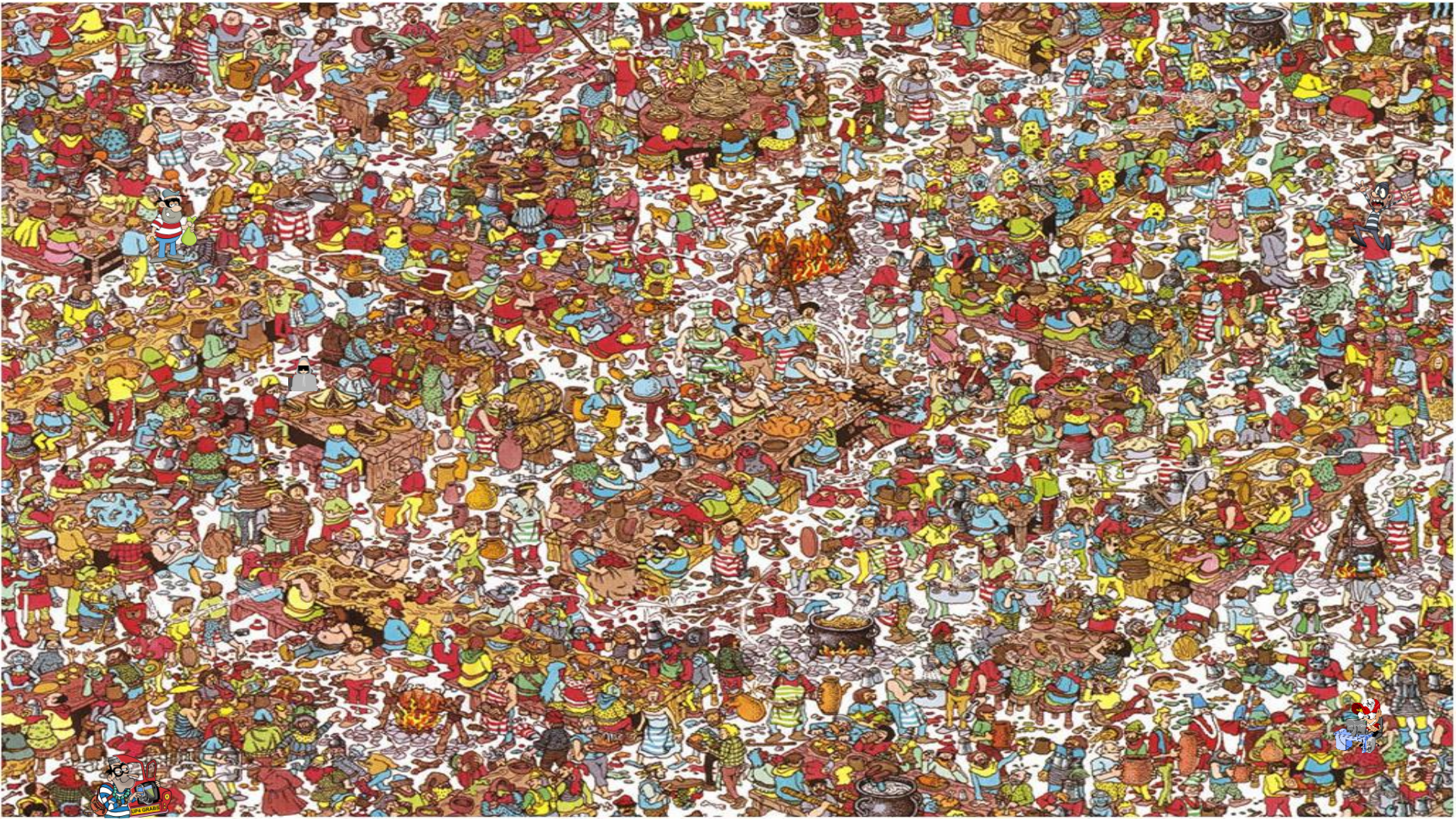


圖片-光學辨視

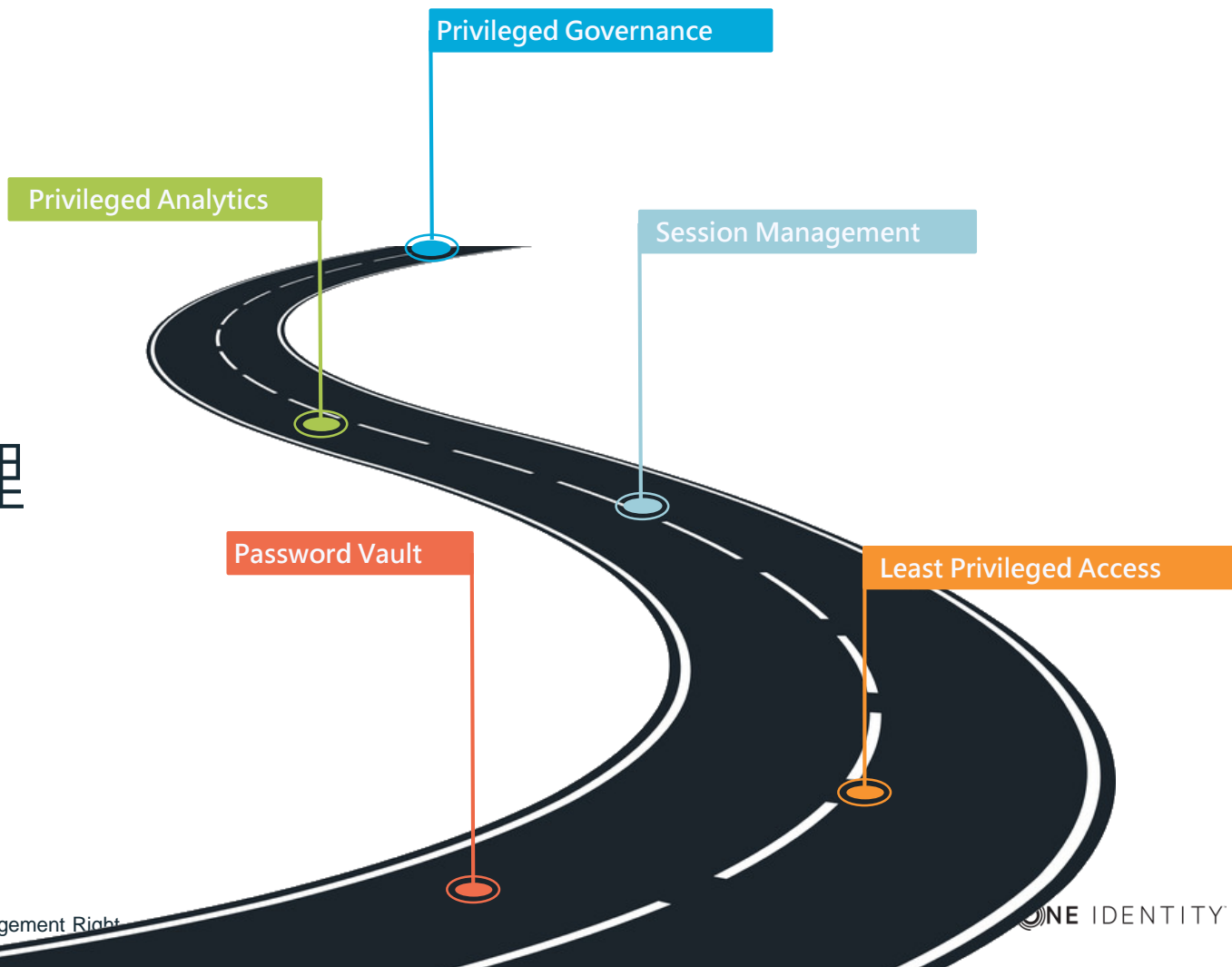


# 行為分析 - 平台架構





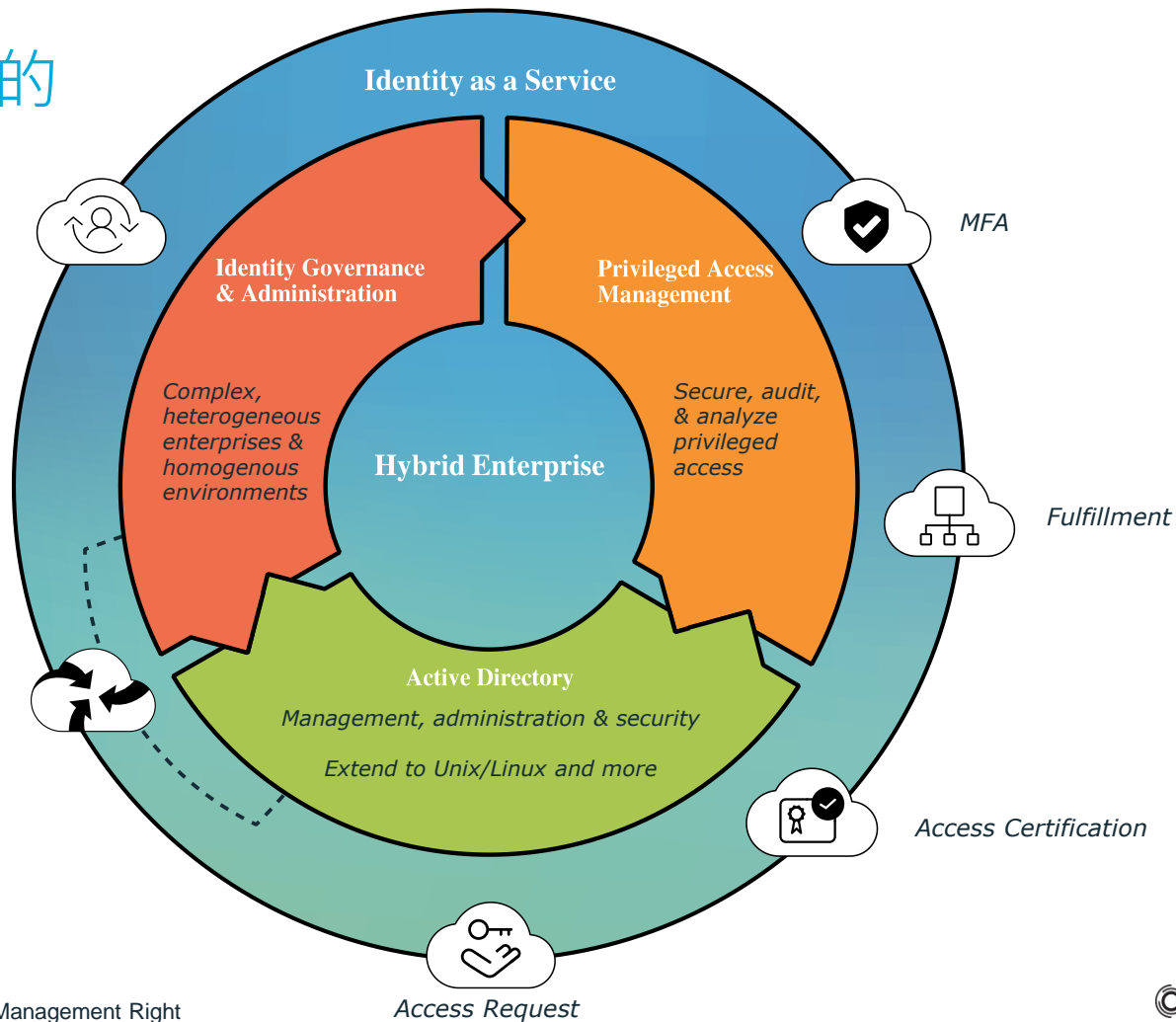
# 特權帳號治理



# 身分治理完整的 解決方案

Identity Lifecycle

Connectors





# 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



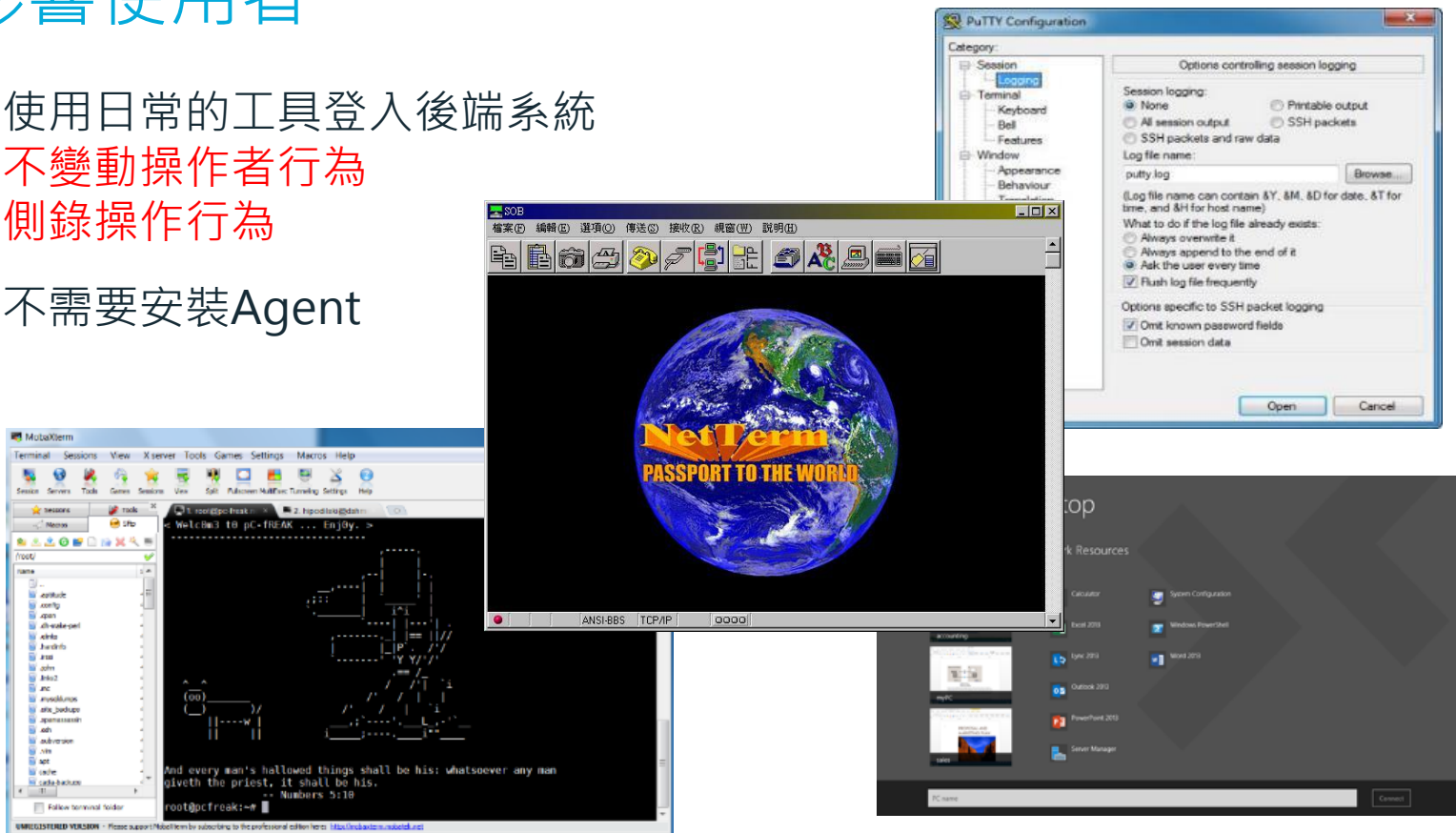
**Safeguard for Privileged Sessions**



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



# 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**

## Sessions

Search query

🔍 Enter a search expression here, eg.: user.server\_username: root AND (protocol:ssh OR protocol:telnet) AND NO

Content query

🖥️ 韓國瑜

Sort by **most recent** ▾

client and connection data

verdict

connection times,

<b>administrator</b> from 192.168.229.1	RDP	as administrator to 192.168.229.135	accept	🕒 18:56 - 18:59 📅 on 2019-07-16
--	-----	--	--------	------------------------------------

🔍 Content query: 韓國瑜

<b>administrator</b> from 192.168.229.1	RDP	as administrator to 192.168.229.135	accept	🕒 18:52 - 18:53 📅 on 2019-07-16
--	-----	--	--------	------------------------------------

🔍 Content query: 韓國瑜

search contents

🔍 韓國瑜

02:17 - 02:17



# 自動建立索引 - 影像文字辨識

weicloud@10.123.131.139 indexed

start generation refresh enabled download trail

overview details events contents analytics

Sessions

Search query

Enter a search expression

Content query

create database 搜

Sort by most recent

client and connection data

weicloud RDP from 10.123.134.208

Content query: create databas

weicloud RDP from 10.123.134.208

Content query: create databas

search contents

create database search

screen content between 02:19 and 02:42 (2019-06-18 13:06:27 and 13:06:50)

02:19

Microsoft SQL Server Management Studio

```
USE master
GO
IF NOT EXISTS (
  SELECT name
  FROM sys.databases
  WHERE name = N'TutorialDB'
)
CREATE DATABASE [TutorialDB]
GO
```

確認目標畫面

00:19 - 00:20

00:23 - 00:24

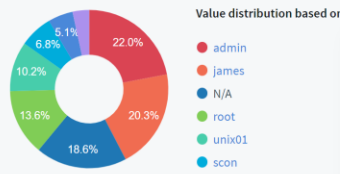
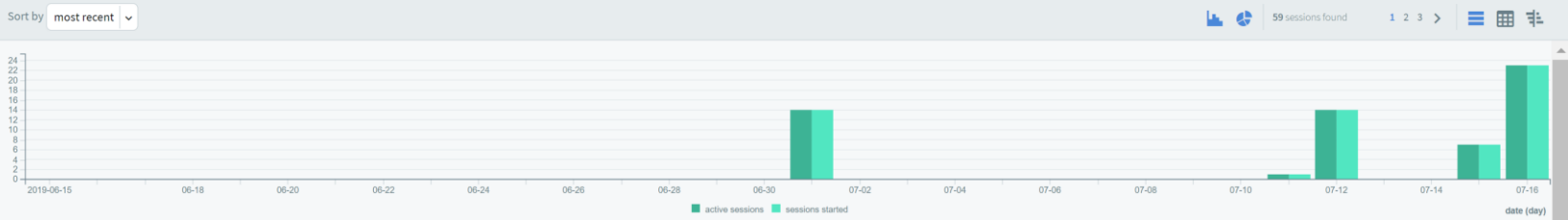
# 多樣性的分析

## Sessions

create subchapter | shortcuts | start date **2019-06-16 00:00** > end date **Pick a date**

Search query  
Q Enter a search expression here, eg.: user.server\_username: root AND (protocol:ssh OR protocol:telnet) AND NOT client.ip: "10.10.0.0/16"

Content query  
🔍 Search in content



Username X ▾

Search

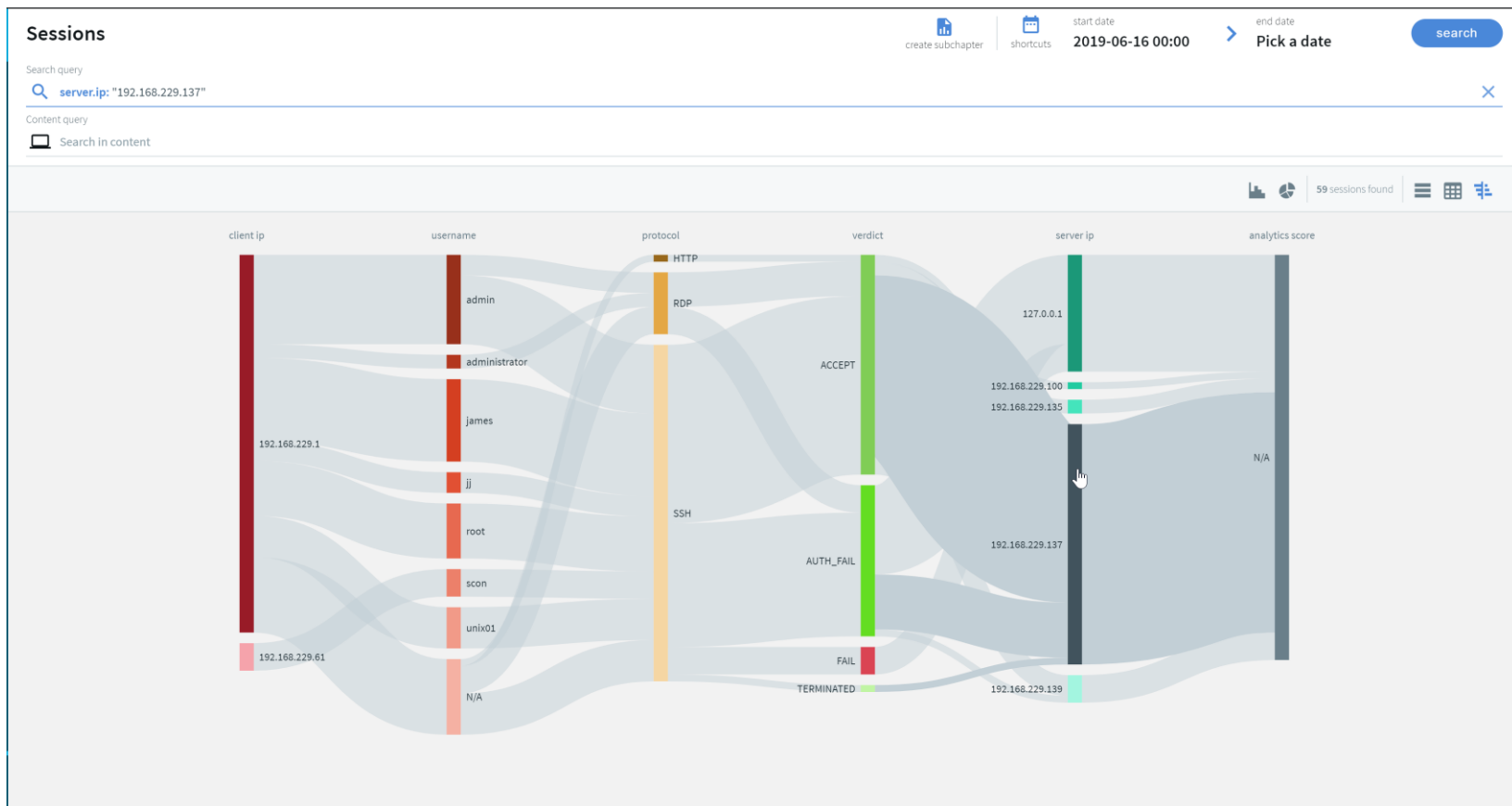
- Active
- Analytics Score
- Client name
- Protocol
- Server hostname
- Server port
- Server username
- ✓ Username
- Verdict
- Analytics Interesting events
- Archive date deprecated
- Archived deprecated

client and connection data

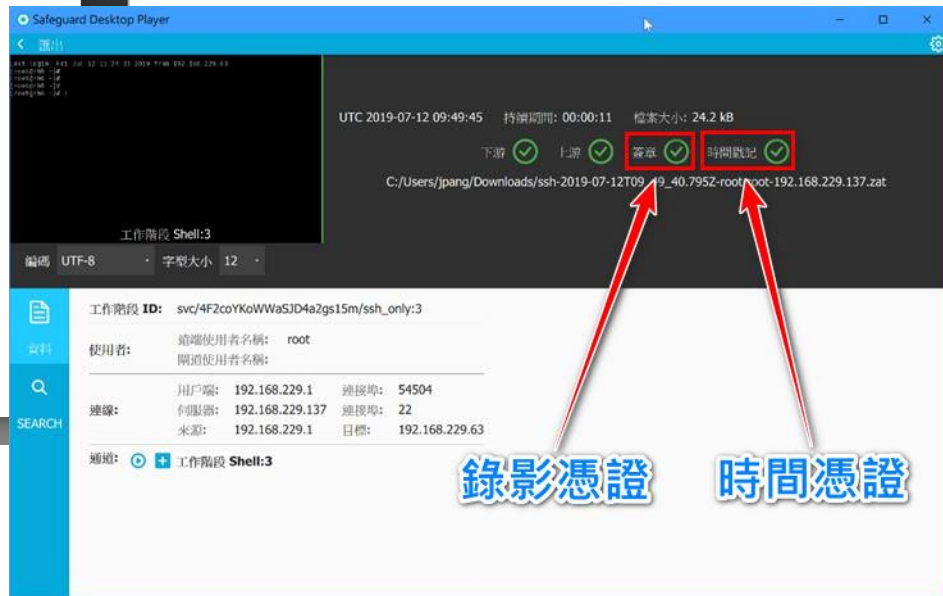
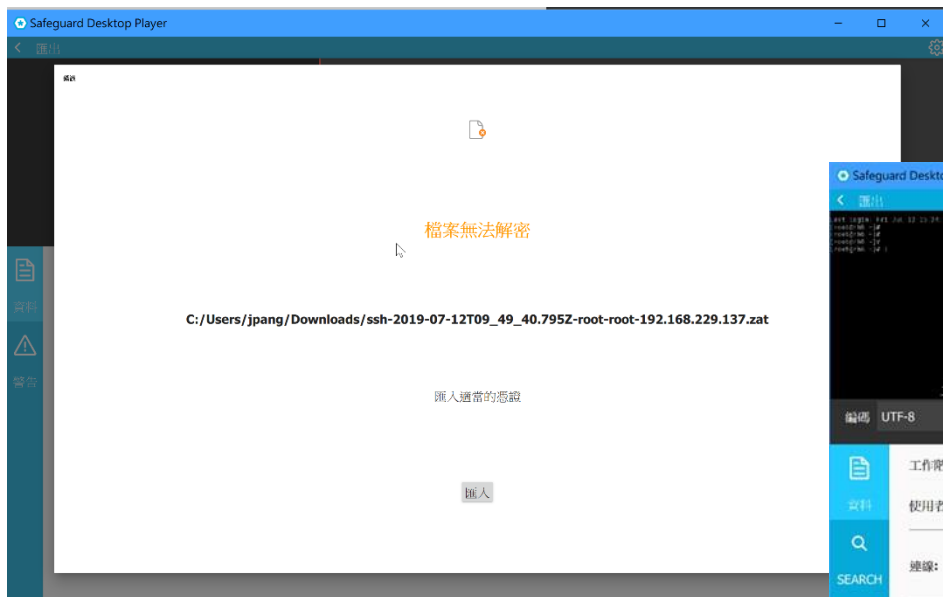
root from 192.168.229.1	SSH	as root to 192.168.229.137
administrator from 192.168.229.1	RDP	as administrator to 192.168.229.135
administrator from 192.168.229.1	RDP	as administrator to 192.168.229.135
scon from 192.168.229.61	SSH	as scon to 192.168.229.137

	analytics results	interesting events	
00:10:12	n/a	-	<a href="#">details &gt;</a>
00:02:23	n/a	-	<a href="#">details &gt;</a>
00:01:11	n/a	-	<a href="#">details &gt;</a>
00:00:02	n/a	-	<a href="#">details &gt;</a>

# 多樣性的分析



# 紀錄不可竄改 - 不可否認



# 報表

- 操作中出现關鍵字，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。

韓國魚

---

Search word(s):

Search is case insensitive. Separate words with space.  
To create complex expressions, use quotation marks (e.g., '...')

Filters:

Protocol:

## Add Subchapter



- ▶ Configuration changes
- ▶ System health
- ▶ Connection summary
- ▶ All Connections
- ▶ RDP Connections
- ▶ SSH Connections
- ▶ HTTP Connections
- ▶ Misc
- ▼ Advanced statistics

SQL Query



Ok

Cancel

1.1. 韓國魚 from 2019-07-16 07:44:26 to 2019-07-16 07:46:56 at ssh\_only (ssh)



```
Last login: Tue Jul 16 15:26:51 2019 from 192.168.229.63
[root@rh6 ~]#
[root@rh6 ~]#
[root@rh6 ~]# cd /tmp
[root@rh6 tmp]# ls
VMwareTools-10.2.5-8068393.tar.gz  vmware-tools-distrib
[root@rh6 tmp]# cd /data
[root@rh6 data]# ls
poll.txt
[root@rh6 data]# cat poll.txt
# 匿名 44.805%
# 匿名 27.730%
# 匿名 17.900%
# 匿名 6.020%
# 匿名 3.544%
[root@rh6 data]# l
```



# Demo

Browser address bar: [https://192.168.229.63/index.php?\\_backend=ReportConfiguration](https://192.168.229.63/index.php?_backend=ReportConfiguration)

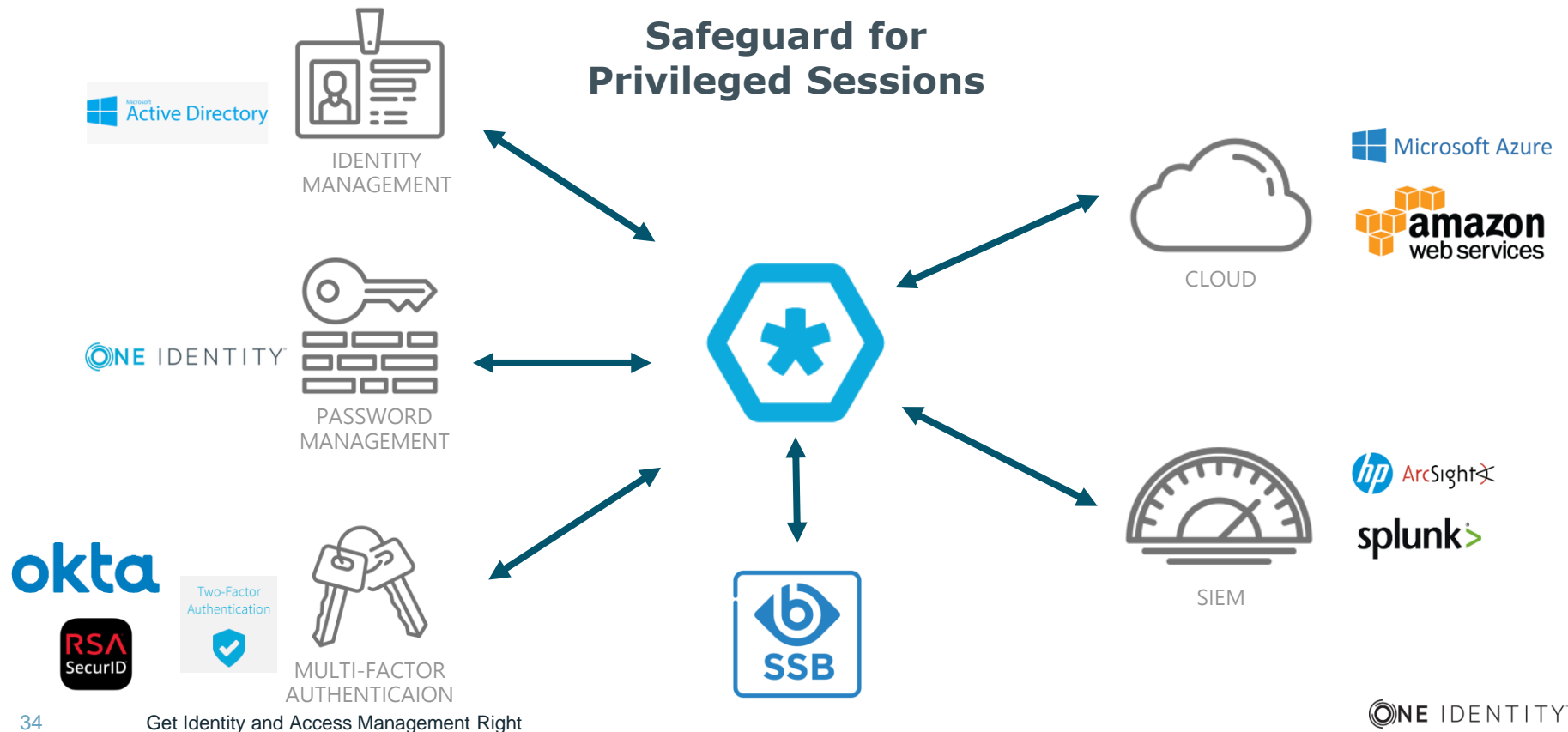
Page Title: PRIVILEGED SESSION MANAGEMENT 5.10.0b

Page Content:

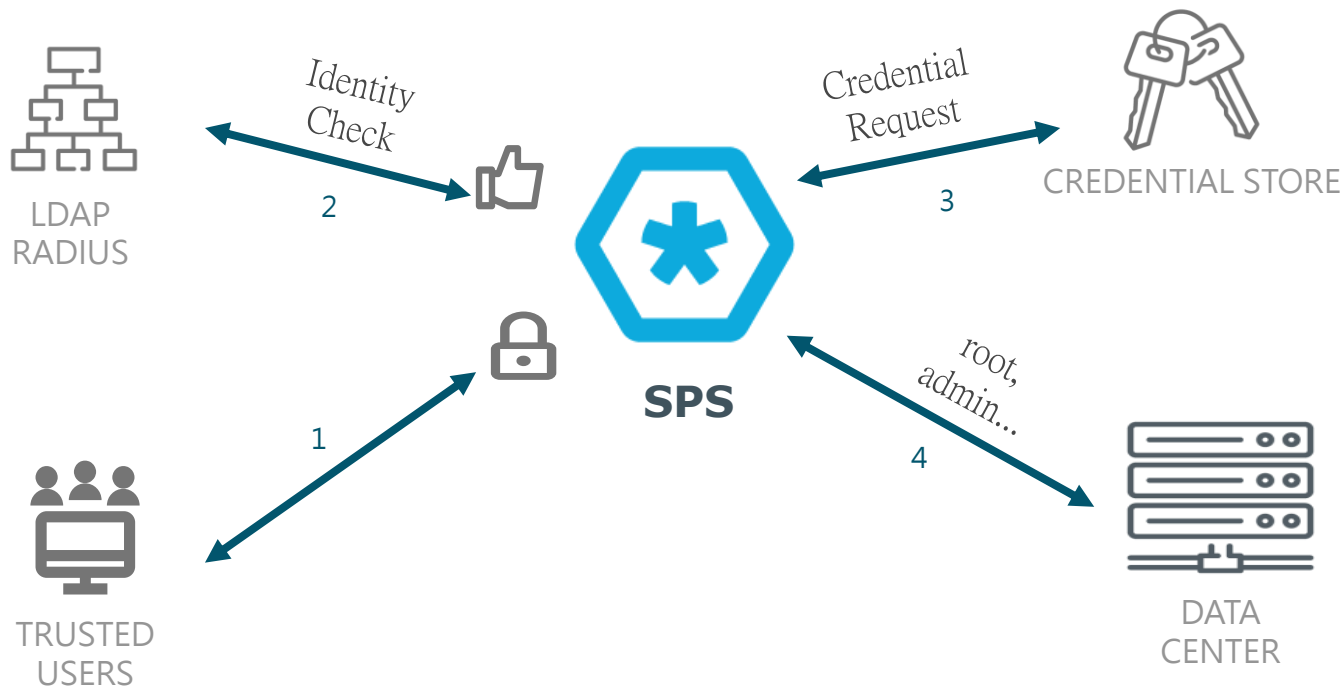
- operational-report [I need help] [Commit]
- S-report [I need help] [Commit]
- 機密資料 [I need help] [Commit]
- SQL Query [I need help] [Commit]
- 韓國魚 [I need help] [Commit]

Footer: Copyright (c) One Identity LLC. 2018 [www.oneidentity.com](http://www.oneidentity.com)

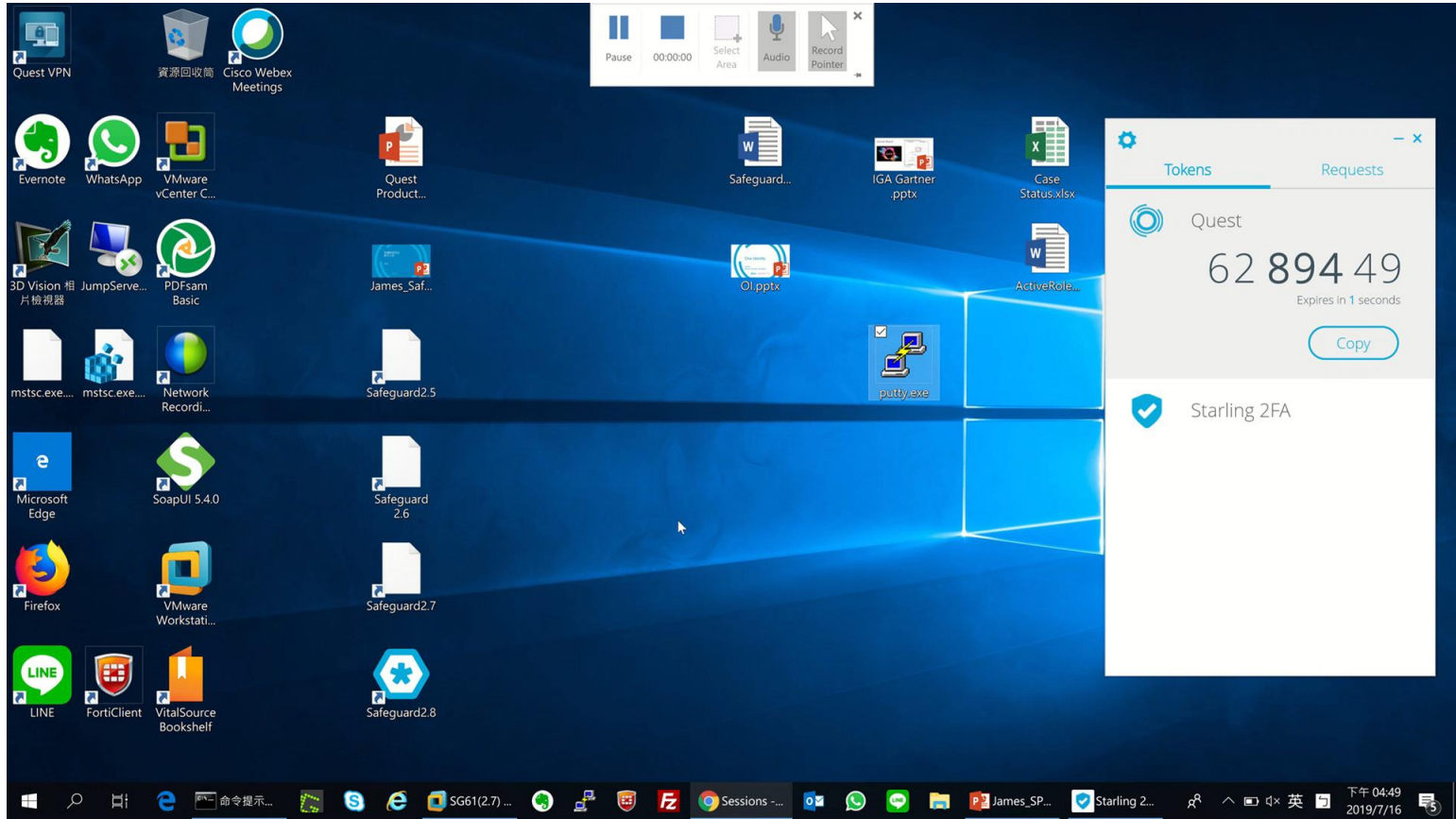
# 整合



# 應用情境分享 – 認證後，自動代登



# Demo



Thank You!  
Questions?

 ONE IDENTITY™