運用零信任策略落實身份治理與單一簽入整合

鋐迪資訊資深技術顧問
Andy Chung

鍾迪 Andy Chung

- 現職：
  - 鋐迪資訊股份有限公司-資深技術顧問
- 學歷：
  - 加州長堤大學 CSULB 碩士
- 專案建置經歷：
  - 政府、電信、航空、學校、海外：40個專案
- 專業能力：
  - 身份管理系統規劃與建置
  - 帳號整合同步規劃與建置
  - 單一簽入系統規劃與建置
  - 特權管理系統規劃與建置
  - 多因素認證系統規劃與建置
  - Java / Linux Shell / VBscript / SQL 開發
- 專業證照：
  - Access Manager Certified Professional Exam
  - Certified NetIQ Identity Manager Administrator (CNIMA)
  - Micro Focus Access Manager Specialization
  - IBM DB2 UDB Family Fundamentals
  - CompTIA LINUX+
  - Novell Certify Engineer (CLE)
  - Novell Certify Linux Professional (NCLP)
  - Security and Identity Management Technical Specialist
  - Novell Certify Linux Administrator (NCLA)
  - Access Management Technical Certification
  - Identity and Access Management Knowledge Check
  - Security Operations Knowledge Check

零信任策略

零信任的重要性

當前組織面臨的挑戰

威脅在不斷變化的環境中增加

28%

勒索病毒

Sophos 2020

34%

惡意軟件

Sophos 2020

76%

COVID-19 導致企業變化

Spiceworks Ziff Davis 2020

22%

2025 年，遠端作業

Upwork 2020

77%

數位轉型將佔據預算最大塊

subex 2021

Only 16%

企業聲稱有能力阻擋攻擊

Forrester 2021

36%

釣魚網站將使資料外洩

Verizon DBIR 2021

85%

個人因素導致資料外洩

Verizon DBIR 2021

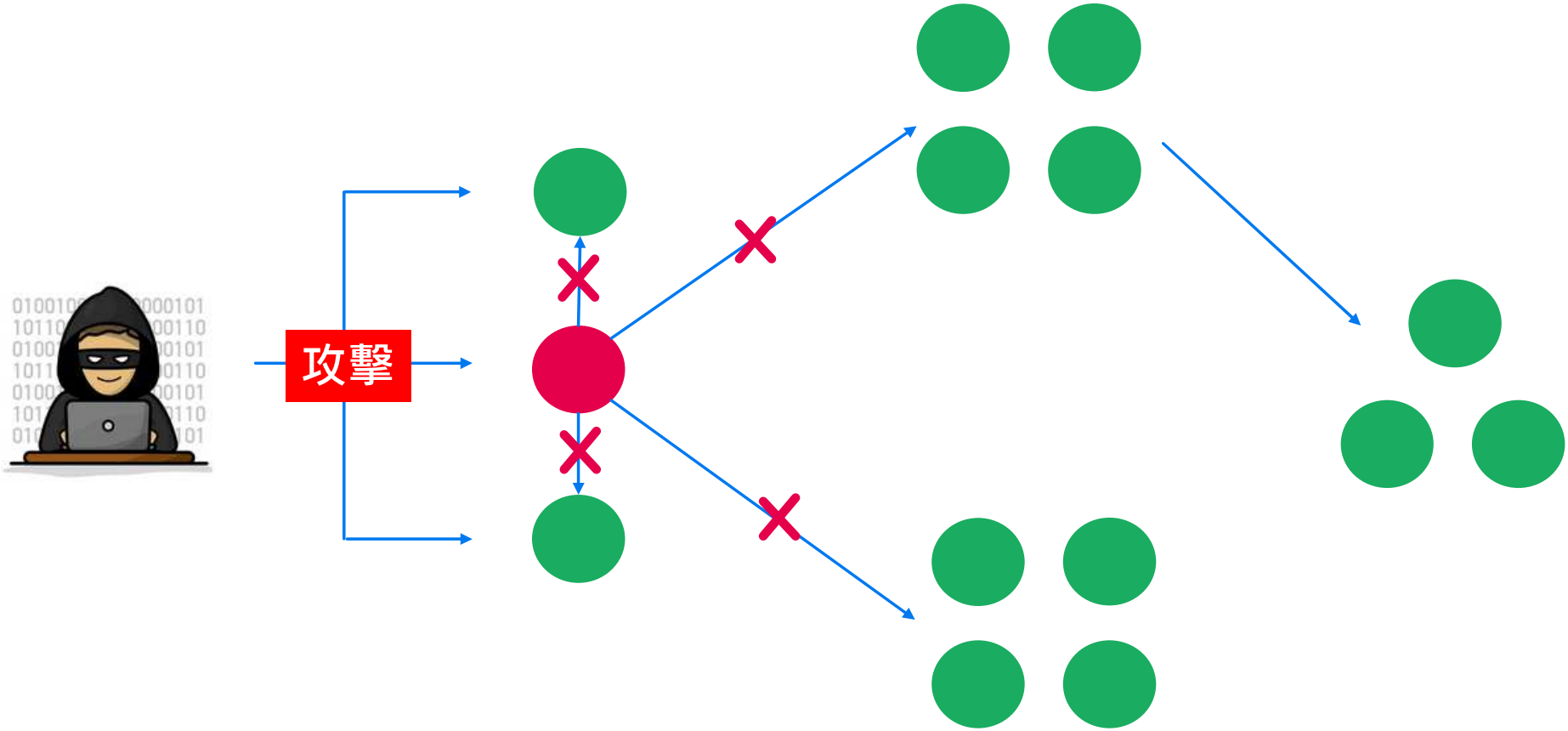
在不斷受到攻擊的情況下
需要有顛覆性創新的資源管理

網際網路彈性的需求

- 如果一個組織成為攻擊目標，最終它會受到損害
- 組織必須能夠抵禦攻擊並繼續提供關鍵功能
- 必須建立彈性 - 不增加

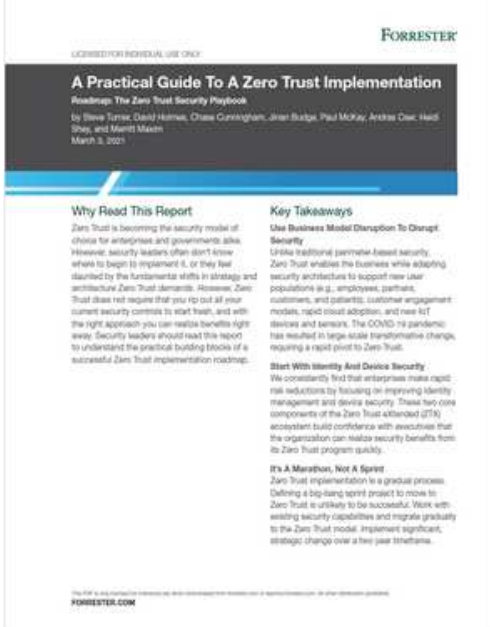
零信任主要概念

零信任安全框架背後的關鍵思想是，使攻擊者難以到處攻擊。



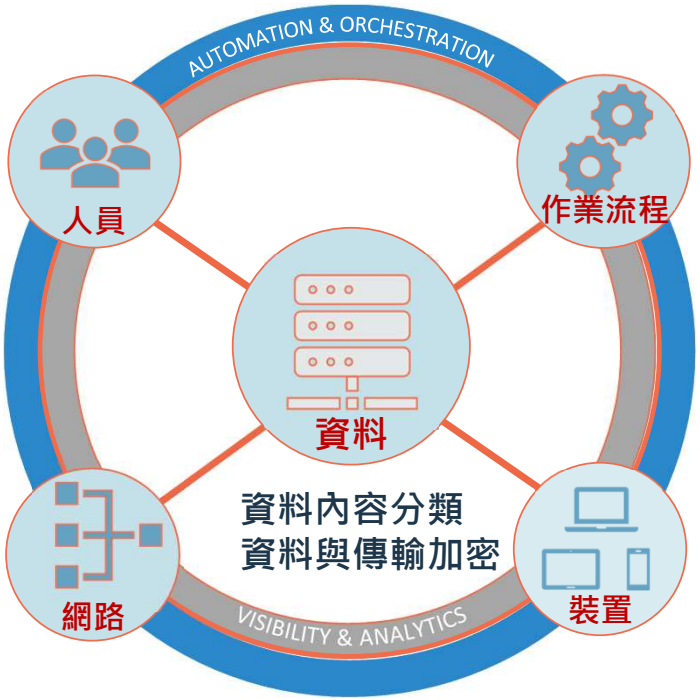
什麼是零信任

- 零信任架構是一種持續演進的資源保護和信任前提下的網絡安全架構概念，目前尚無任何認證或實際的標準可供遵循。
- 零信任只是一套方法，它可以使用現有或新開發的產品或服務，來落實零信任架構。
- 雖然零信任是一種概念，但 National Institute of Standards and Technology，簡稱 NIST （美國國家標準與技術局 ） 和 Forrester、IDC 等研究機構，都對零信任框架的基本元素提出了他們的定義。



零信任的面向

認證、驗證及管理使用者為零信任策略的第一個基礎



應用程式和組件都視為威脅向量，必須經過認可及驗證

安全分區、網路隔離技術和控制網路的使用及存取能力

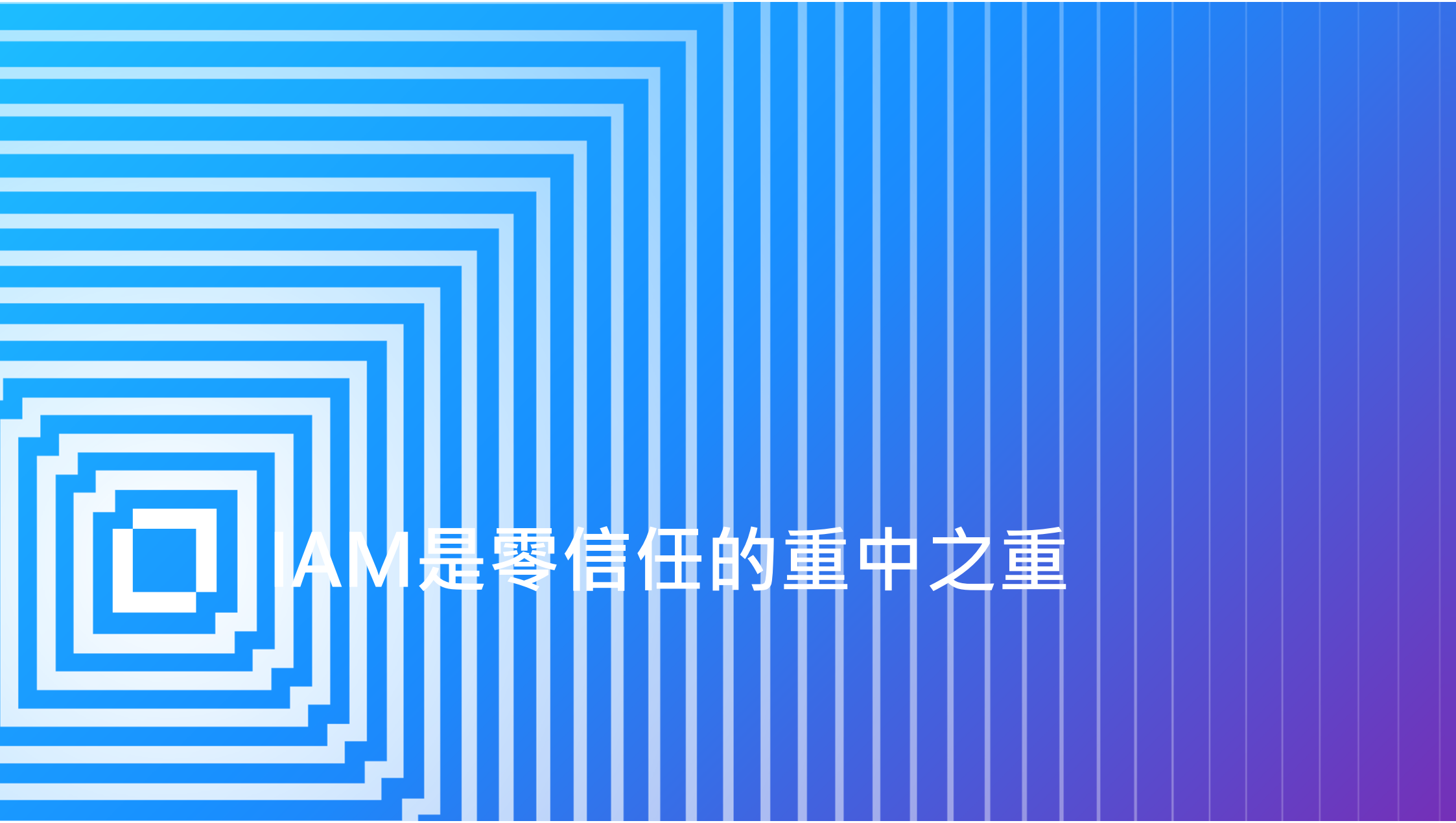
在任何基礎架構中必須能夠控制連網的每個設備

透過認證、軌跡、稽核紀錄的資訊可見度完成、自動化和協調流程

零信任基本原則

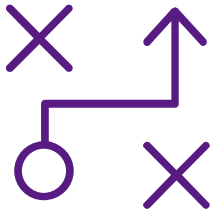
1. 所有資料與服務都視為資源
2. 不論在何處所有連線必須是安全保護的
3. 當下的連線階段授予最低必要權限
4. 依據動態政策來提供存取支援
5. 沒有任何設備或資產是可信任的
6. 嚴格執行認證與授權與不斷重複驗證
7. 盡可能的收集資訊

1. 資料是資源
2. 安全連線
3. 低權限
4. 政策存取
5. 資產不安全
6. 重複驗證
7. 收集資訊


IAM是零信任的重中之重

企業對零信任的看法

Top reasons for considering/implementing Zero Trust Security



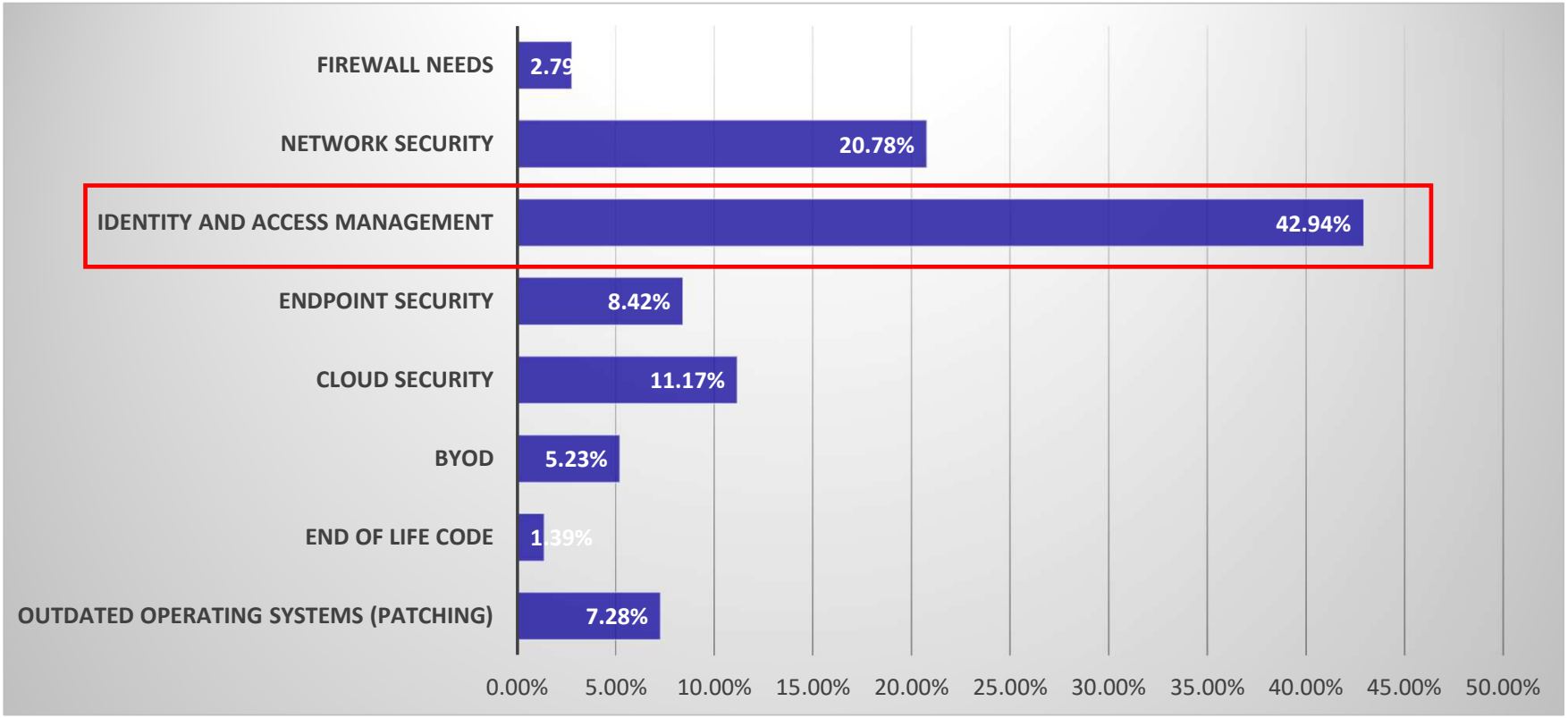
52.5% 零信任方式比傳統方式更主動

32.7% 零信任是對抗複雜攻擊的唯一方法

Source: Ericom 2021 Zero Trust Market Dynamics Survey

企業對零信任的感受

在零信任架構中, 什麼是必須優先重視與改善的?



來源: Ericom 2021 Zero Trust Market Dynamics Survey

為何IAM是重要的

- 登入系統需要帳號密碼。
- 帳號裡的資訊可當作權限的判斷。
- 單一簽入的效益。
- 帳號密碼作為認證已不夠安全。
- 登入系統後的控管或是操作軌跡。
- 地端與雲端的整合。

驗證且永不信任

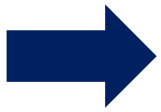
最低權限的授與策略

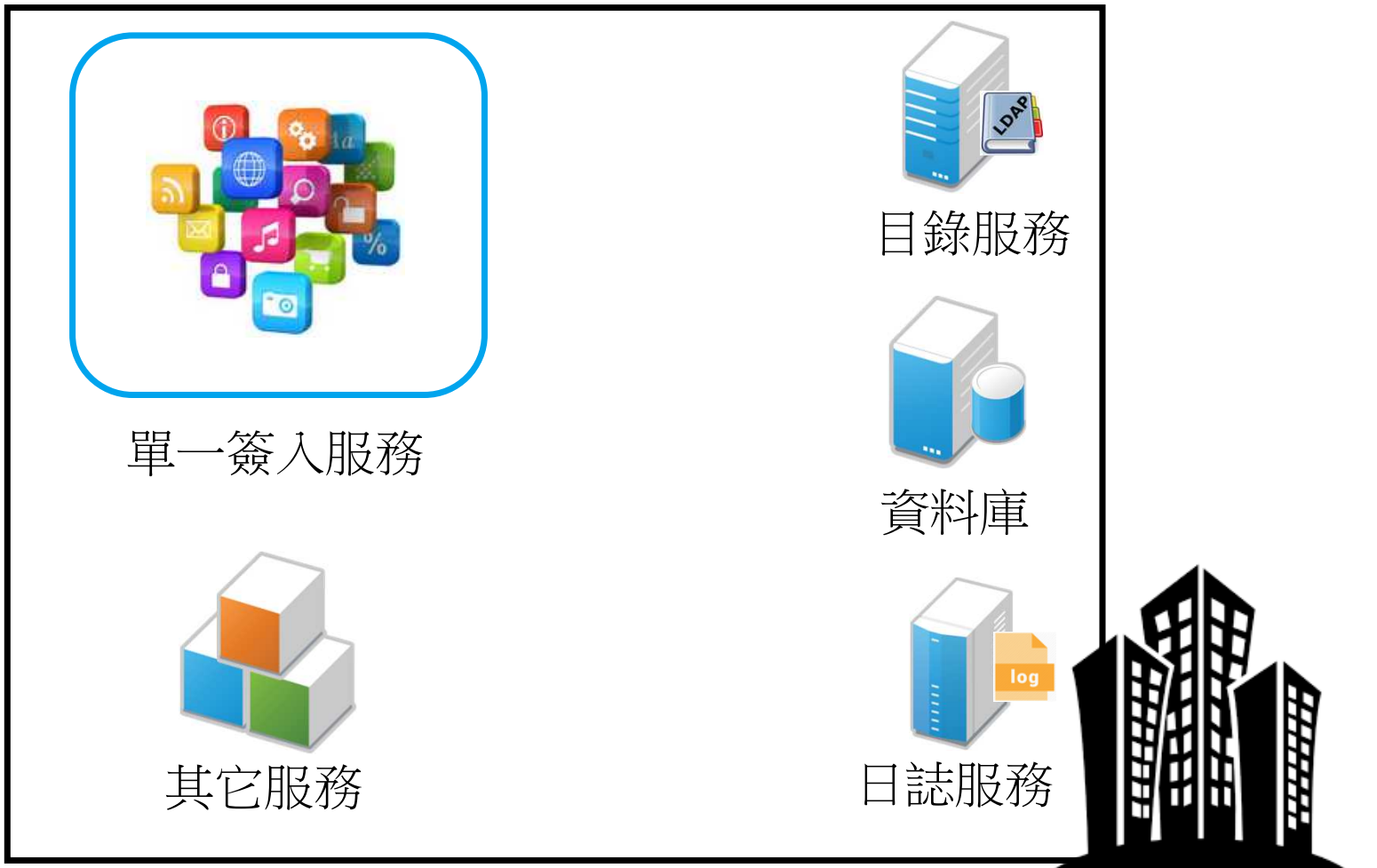
集中管理

檢測與記錄所有的流量

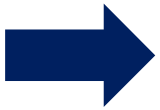
四種IAM架構

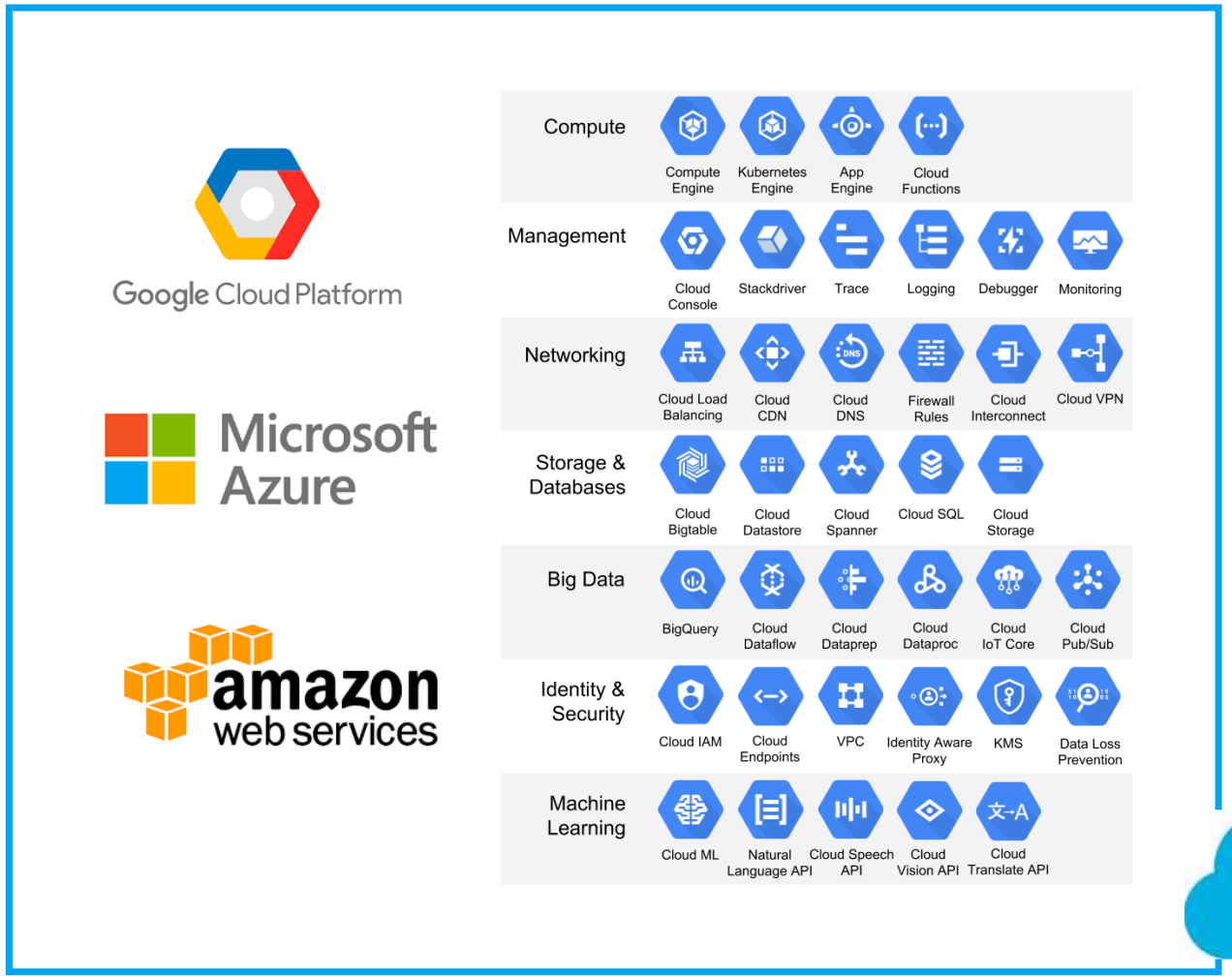
地端IAM





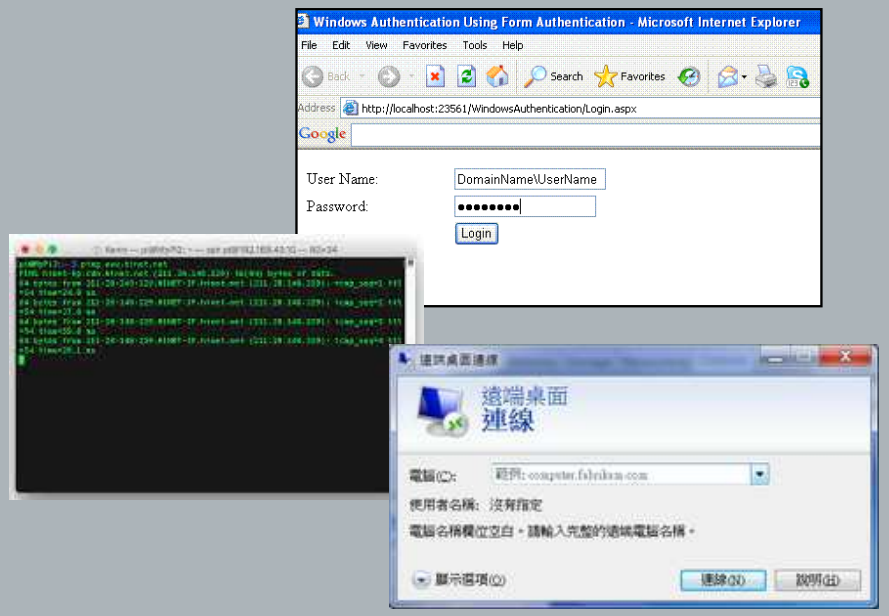
雲端IAM



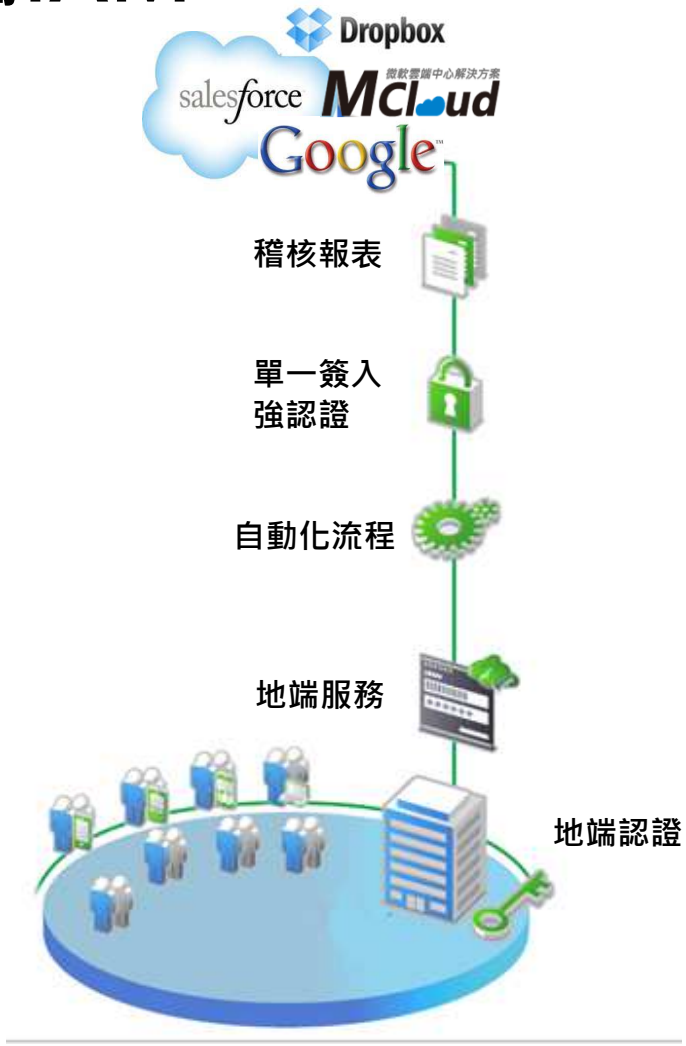

Google Cloud Platform
Microsoft Azure
amazon web services
Compute
Compute Engine
Kubernetes Engine
App Engine
Cloud Functions
Management
Cloud Console
Stackdriver
Trace
Logging
Debugger
Monitoring
Networking
Cloud Load Balancing
Cloud CDN
Cloud DNS
Firewall Rules
Cloud Interconnect
Cloud VPN
Storage & Databases
Cloud Bigtable
Cloud Datastore
Cloud Spanner
Cloud SQL
Cloud Storage
Big Data
BigQuery
Cloud Dataflow
Cloud Dataprep
Cloud Dataproc
Cloud IoT Core
Cloud Pub/Sub
Identity & Security
Cloud IAM
Cloud Endpoints
VPC
Identity Aware Proxy
KMS
Data Loss Prevention
Machine Learning
Cloud ML
Natural Language API
Cloud Speech API
Cloud Vision API
Cloud Translate API

雲端與地端IAM

地端	雲服端



混合式雲端與地端IAM




IAM元件

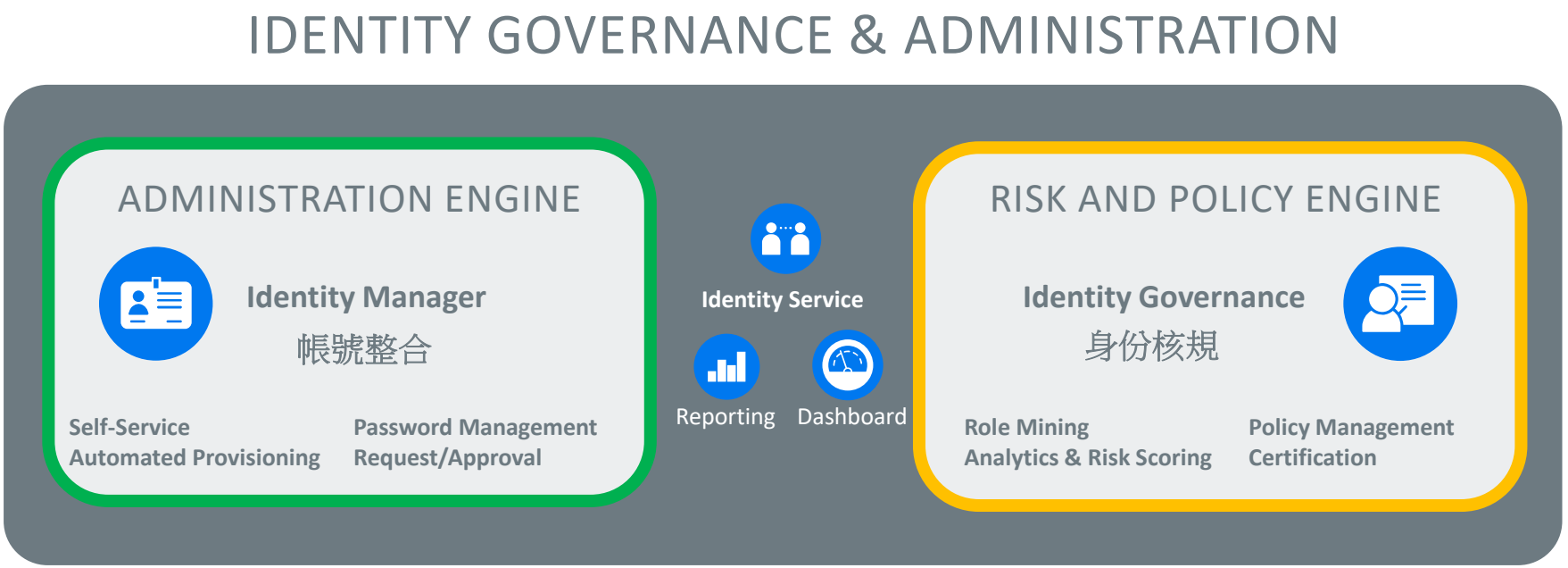
身份治理

身份治理功能概要

1. 管控帳號與權限的生命週期
2. 帳號權限集中
3. 提供認證使用
4. 可快速簡單的整合其它系統
5. 自我服務
6. 內建核規檢查
7. 提供稽核紀錄與報表

1. 資料是資源
2. 安全連線
3. 低權限
4. 政策存取
5. 資產不安全
6. 重複驗證
7. 收集資訊

身份治理管理


IDENTITY GOVERNANCE & ADMINISTRATION
ADMINISTRATION ENGINE
Identity Manager
帳號整合
Self-Service
Automated Provisioning
Password Management
Request/Approval
Identity Service
Reporting
Dashboard
RISK AND POLICY ENGINE
Identity Governance
身份核規
Role Mining
Analytics & Risk Scoring
Policy Management
Certification

帳號暨存取管理

整個用戶生命週期

身份整合

身份整合介接支援清單

Database
* MSSQL
* ORACLE
* support JDBC or ODBC

LDAP Directory Driver
* Active Directory
* eDirectory
* LDAP

Scripting
* Script Command

Linux Unix
* RedHat
* SuSE
* AIX

Mainframe
* ACFS
* RACF
* Top Secret

Microsoft Enterprise
* Azure Active Directory
* Mutli-Domain Active Directory
* Office 365
* SharePoint

Oracle Enterprise
* Oracle E-Business Suite HR
* Oracle E-Business Suite TCA
* Oracle E-Business Suite User Management
* PeopleSoft

SAP Enterprise
* SAP HR
* SAP Portal
* SAP User Management
* SAP User Management Fanout

Tools
* Restful
* CSV
* SOAP
* SCIM

Email Server Driver
* Exchange
* Lotus
* Postfix
* Zimbra

GoogleApps
* GoogleApps

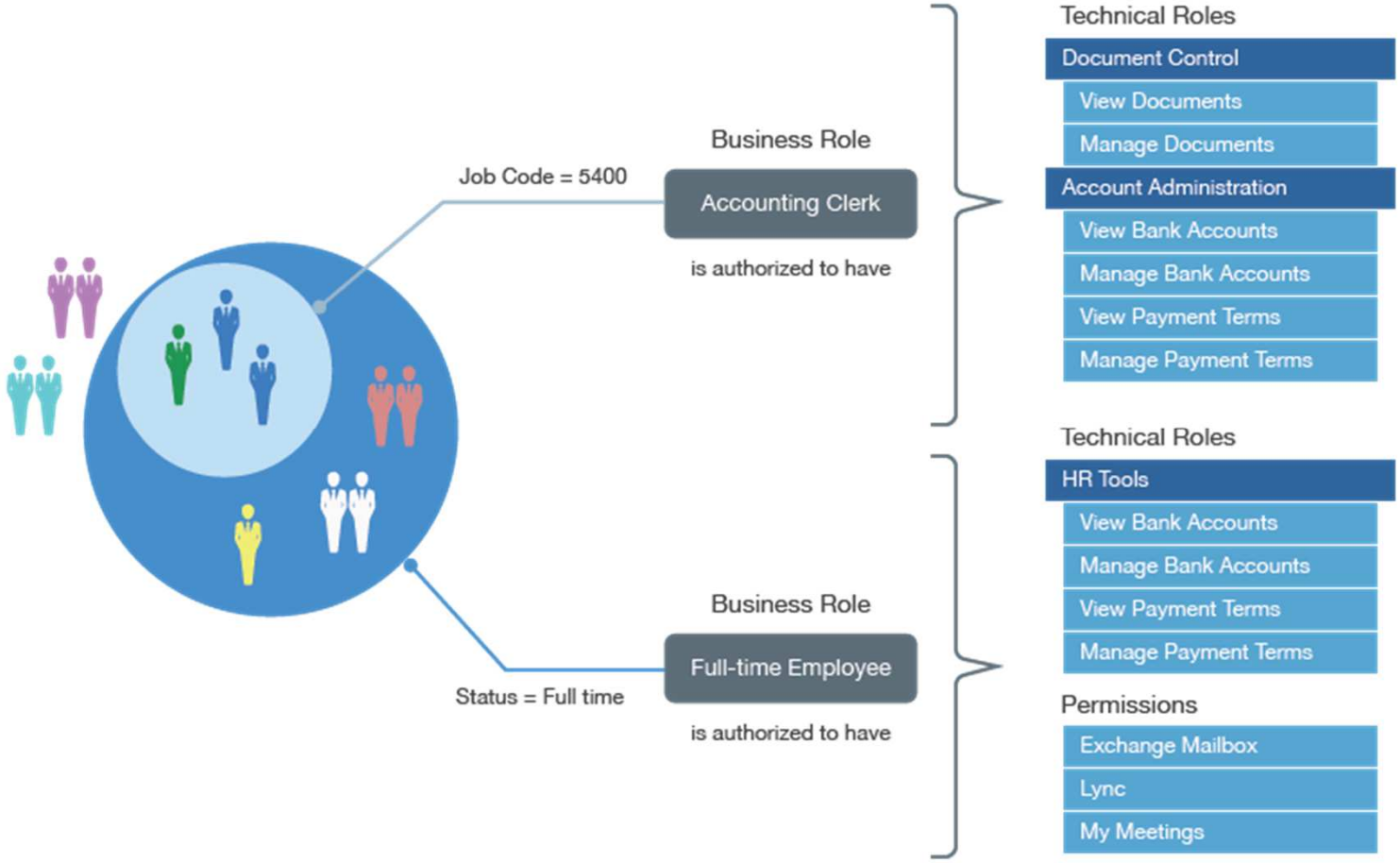
Salesforce
* SalesForce

ServiceNow
* ServiceNow

Messaging
* JMS

Developing
* IDM API

角色管理

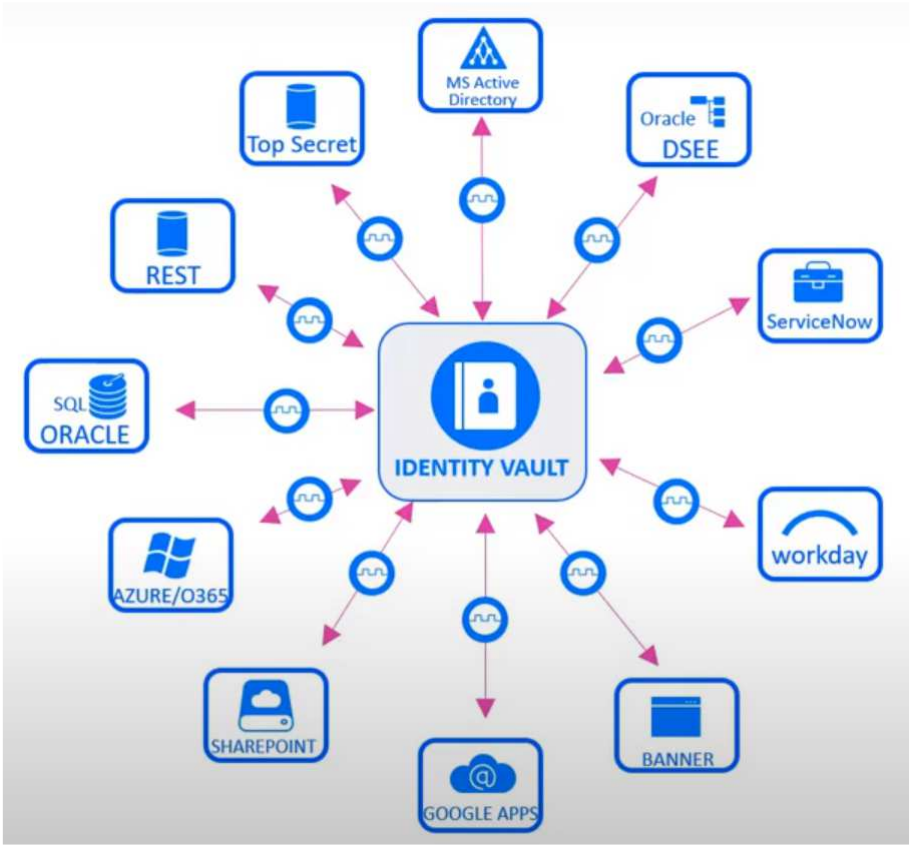

Technical Roles
Document Control
View Documents
Manage Documents
Account Administration
View Bank Accounts
Manage Bank Accounts
View Payment Terms
Manage Payment Terms
Business Role
Job Code = 5400
Accounting Clerk
is authorized to have
Technical Roles
HR Tools
View Bank Accounts
Manage Bank Accounts
View Payment Terms
Manage Payment Terms
Permissions
Exchange Mailbox
Lync
My Meetings
Business Role
Full-time Employee
Status = Full time
is authorized to have

自我服務網頁

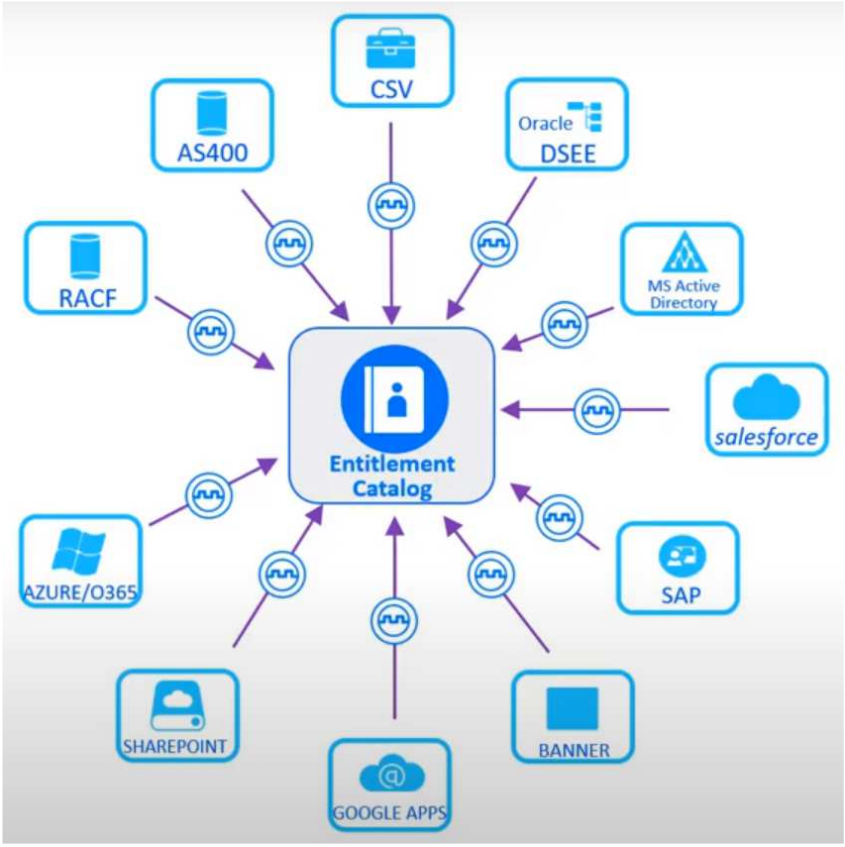

鍾迪
儀表板
應用程式
任務
存取權
人員
管理
組態
應用程式
依名稱或描述搜尋
首頁項目
服務台票證
服務台票證建立表單
申請存取
申請許可權及其他資源
儀表板
導覽至 IDM 儀表板
我的核准
檢視我的 0 Identity Manager 核准任務
我的申請歷程
檢視我的申請歷程
我的存取權
檢視我的存取權限
我的設定檔
更新個人資訊
變更我的密碼
建立新密碼
搜尋使用者
搜尋使用者
組織圖
瀏覽組織
管理
資料收集服務
從受管理系統收集資料
管理團隊
在 Identity Manager 系統中建立、更新和刪除團隊
建立使用者
在 Identity Manager 系統中建立使用者
導覽及存取
管理對使用者應用程式管理的存取權
Identity Reporting
建立、排程和檢視身分報告

自我服務

身份治理架構

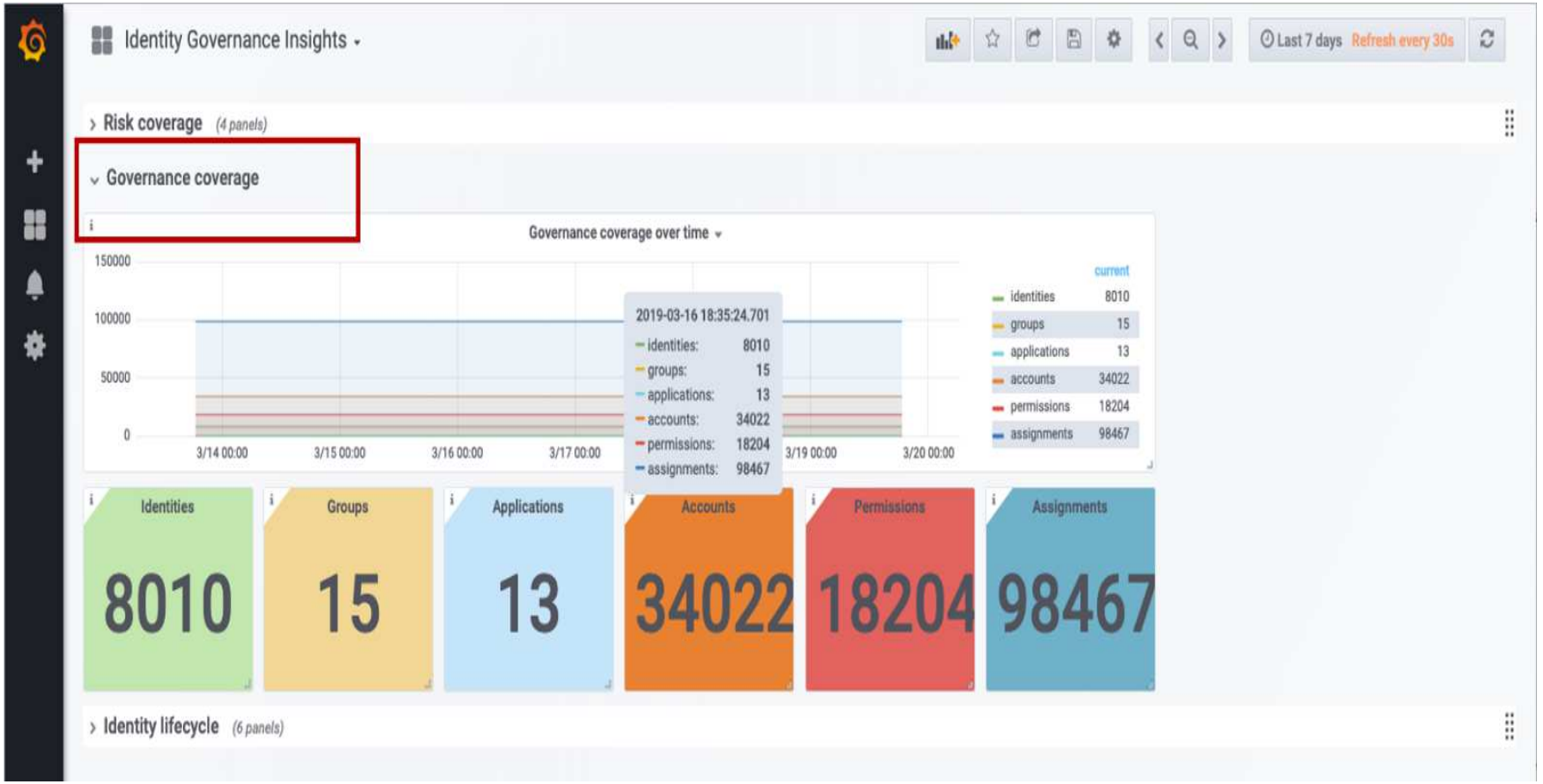


帳號整合



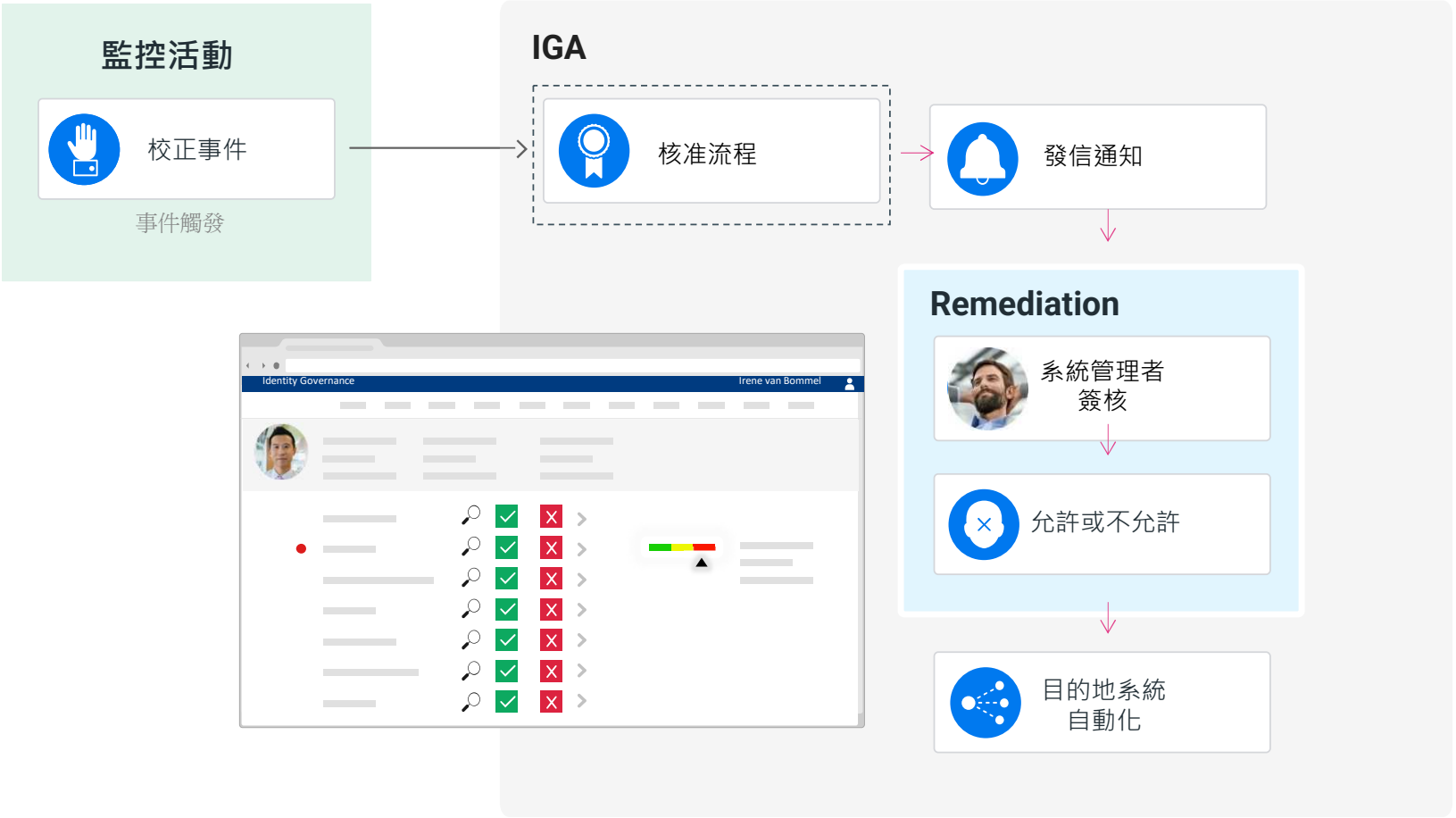
身份核規

帳號與權限盤點



盤點統計

校正核對

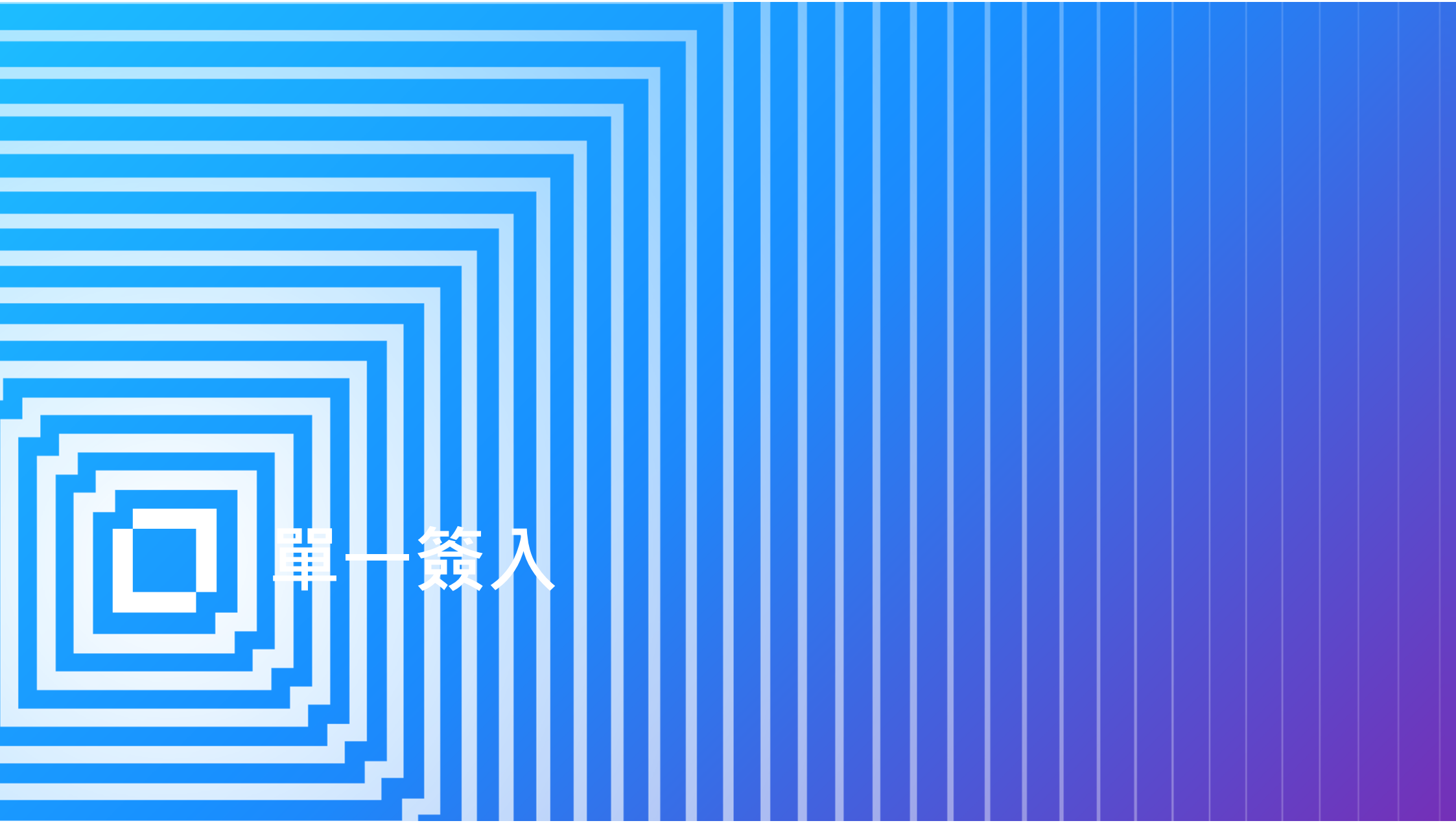

監控活動
校正事件
事件觸發
IGA
核准流程
發信通知
Identity Governance
Irene van Bommel
Remediation
系統管理者
簽核
允許或不允許
目的地系統
自動化

校正核對

報表功能


RPT
Identity Reporting
綜覽
儲存庫
輸入
行事曆
報告
設定
資料來源
下載
報告定義和排程的儲存庫
批量動作
套用
報告定義名稱
描述
標籤
Application Delta - CSV
This report lists changes to an application over a specified date range
Identity Governance
Identity Governance 的資料庫統計資料
此報告顯示選定資料來源的 Identity Governance 資料庫統計資料。若要從 Identity Governance 資料庫擷取統計資料，需要對資料庫具有管理員層級的存取權限。
Identity Governance
使用者做出的授權變更
此報告顯示個別業務角色導致的使用者授權變更。
Identity Governance
使用者設定檔檢閱
此報告列出所有使用者設定檔並顯示相關詳細資料，例如檢閱者、檢閱狀態以及每個檢閱的最終決策。
Identity Governance
使用者設定檔變更
此報告依集合和編輯列出對使用者設定檔屬性所做的變更。
Identity Governance
使用者許可權快照
此報告顯示有關選定日期指定使用者的許可權資訊。適用於 NetIQ Identity Governance。
Identity Governance
使用者許可權指定 - CSV
此報告提供許可權指定的摘要。此報告中的某些欄 (包括開始時間和結束時間) 可能並非從所有資料來源收集而來。
Identity Governance
依使用者列出的許可權差異
此報告顯示給定日期範圍內指定使用者擁有之許可權發生的變更。許可權依應用程式分類。
Identity Governance

報表功能


單一簽入

單一簽入功能概要

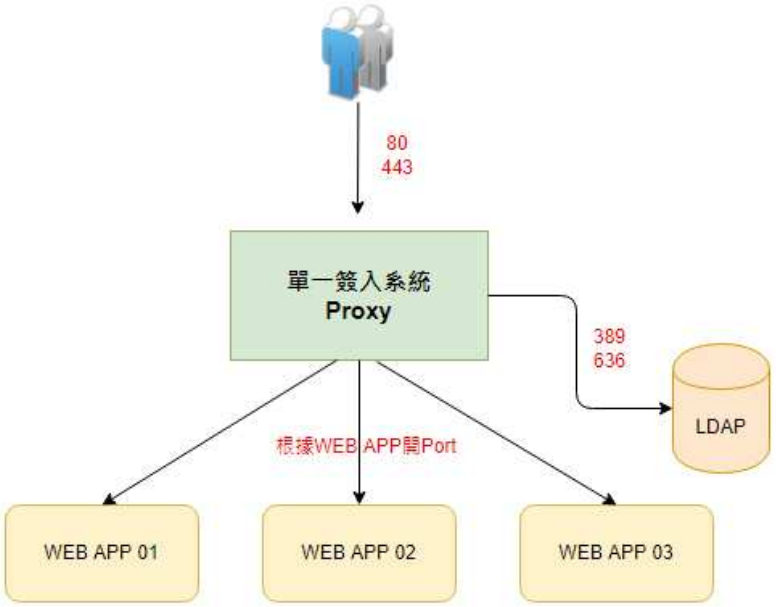
1. 單一簽入功能
2. 集中管控應用系統
3. 角色存取控管
4. 多因素認證結合
5. 提供API呼叫
6. 提供稽核紀錄
7. 內建OAuth 、OpenID與 SAML認證
8. 支援情境感知認證(context-aware authentication)
9. 支援持續認證與授權 (Continue Authentication and Authorization)

1. 資料是資源
2. 安全連線
3. 低權限
4. 政策存取
5. 資產不安全
6. 重複驗證
7. 收集資訊

Proxy功能

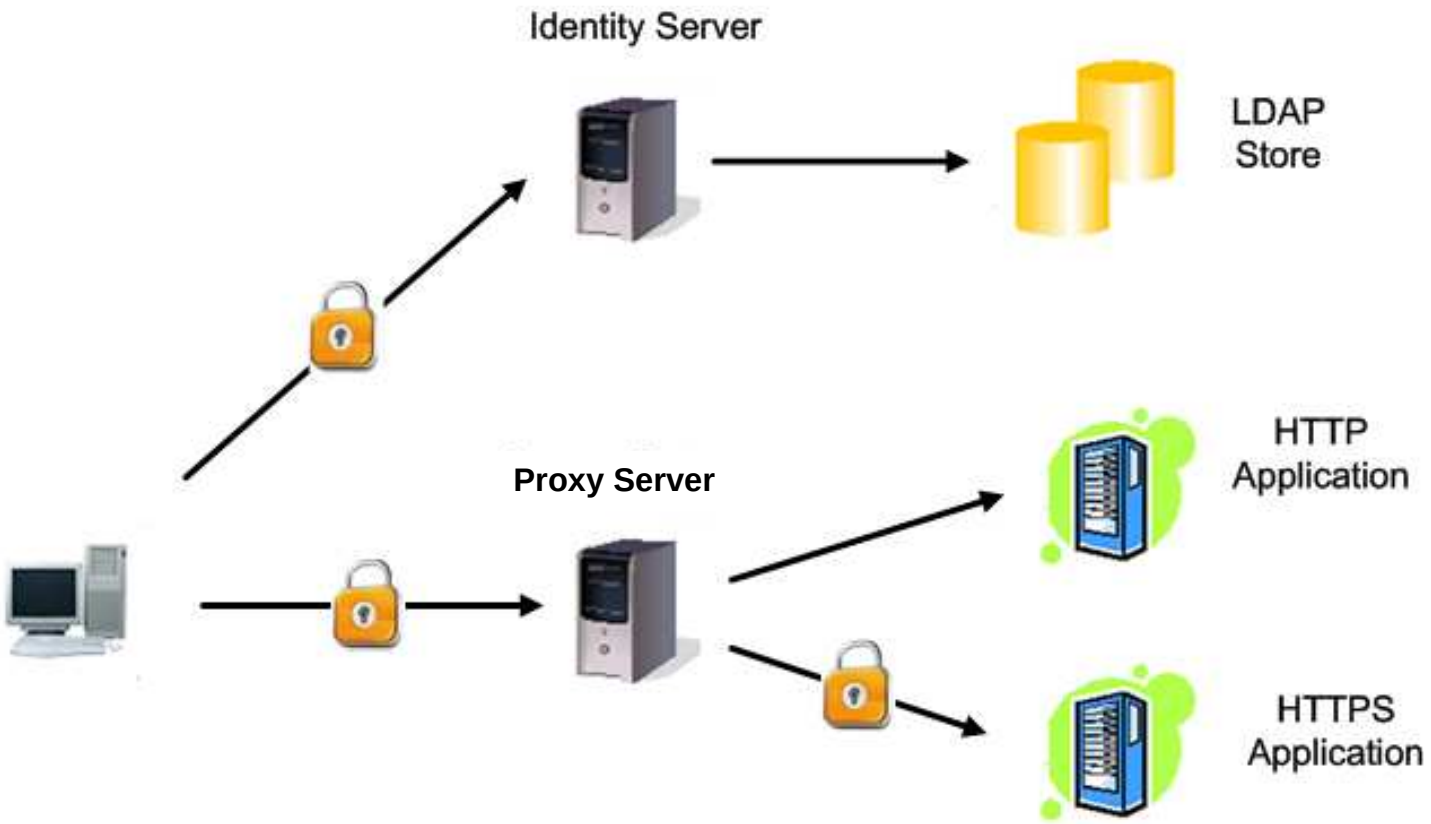
Reverse Proxy：

1. 區隔內部與外部網路，外部主機無法直接連到該 Web Server，保護內部 **Web Server** ，阻擋外部攻擊
2. 因為 Proxy 代理架構，所以瀏覽網站的資料都會透過 Proxy Server 進行代理與快取，所以若是要瀏覽抓取的資料已經存在於 Proxy Server 主機時時就不需要再次連結到實際的 Web Server，如此可以減少 **Web Server** 的負擔
3. 可管控連線**session**。可跟風險控管機制整合大幅提昇安全性。

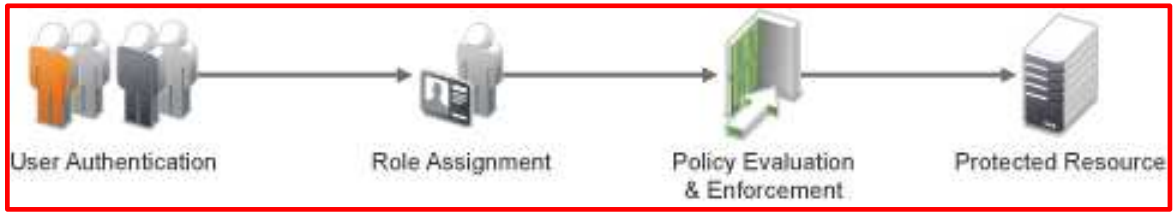


Proxy會保護與管控介接網頁

Secure Access to HTTP Apps



Role Base Access Control (RBAC)



Edit Policy: Auth_For_Sales_Dept

Type: Access Gateway: Authorization

Description: Sales Department

Rule List

New | Delete | Copy | Enable | Disable

	Rule	Priority	Enabled	Action	Description
☐	1	1	✓	Permit	Sales Representative
☐	2	2	✓	Permit	Sales Manager
☐	3	3	✓	Permit	Sales President
☐	4	10	✓	Deny	Deny

Changes made on this panel must be applied from the Policies Panel.

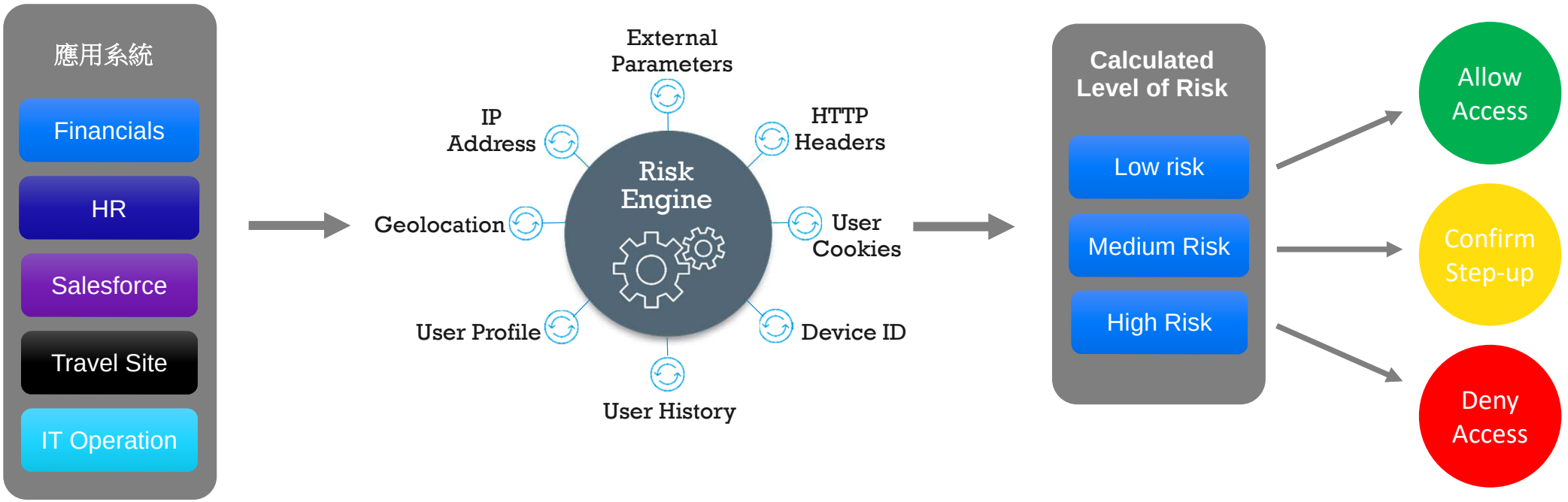
OK Cancel

判斷條件

- Authentication Contract
- Client IP
- Credential Profile
- Current Date
- Day of Week
- Current Day of Month
- Current Time Of Day
- HTTP Request Method
- LDAP Attribute
- LDAP OU
- Liberty User Profile
- Roles
- Risk Score
- OAuth Scopes
- OAuth Claims
- URL
- URL Scheme
- URL Host
- URL Path
- URL File Name
- URL File Extension
- Virtual Attribute
- X-Forwarded-For IP

風控管理認證

- 可依據使用者”所在地域”、”IP Address”、”設備”、”個人屬性”、”存取歷史習性”、”時間”...等自動控制使用者登入認證的方式或直接拒絕存取。



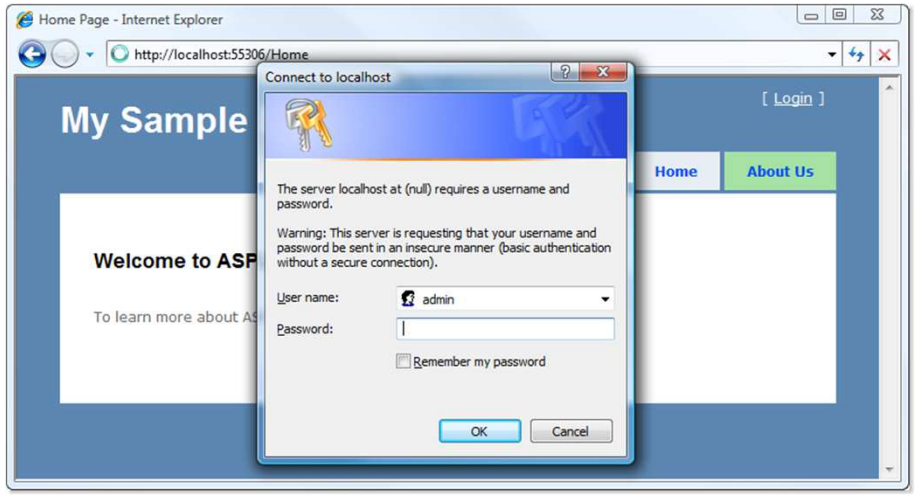
Web SSO整合技術

1. Authentication Header
2. Custom Header
3. Query String
4. Cookie Header
5. Kerberos Ticket
6. OAuth Token

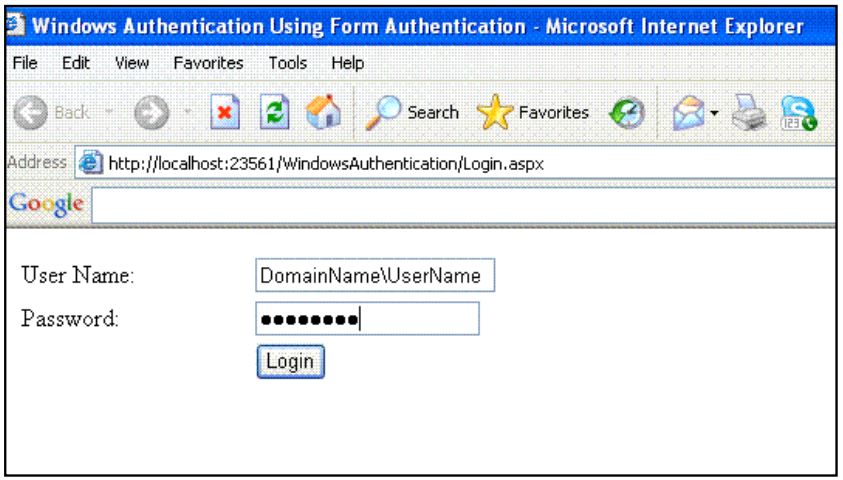
```
GET /private/index.html HTTP/1.0
Host: localhost
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

```
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
```

Web Form Post SSO 整合技術



Windows Popup 401 Authentication



Form Authentication

強認證整合

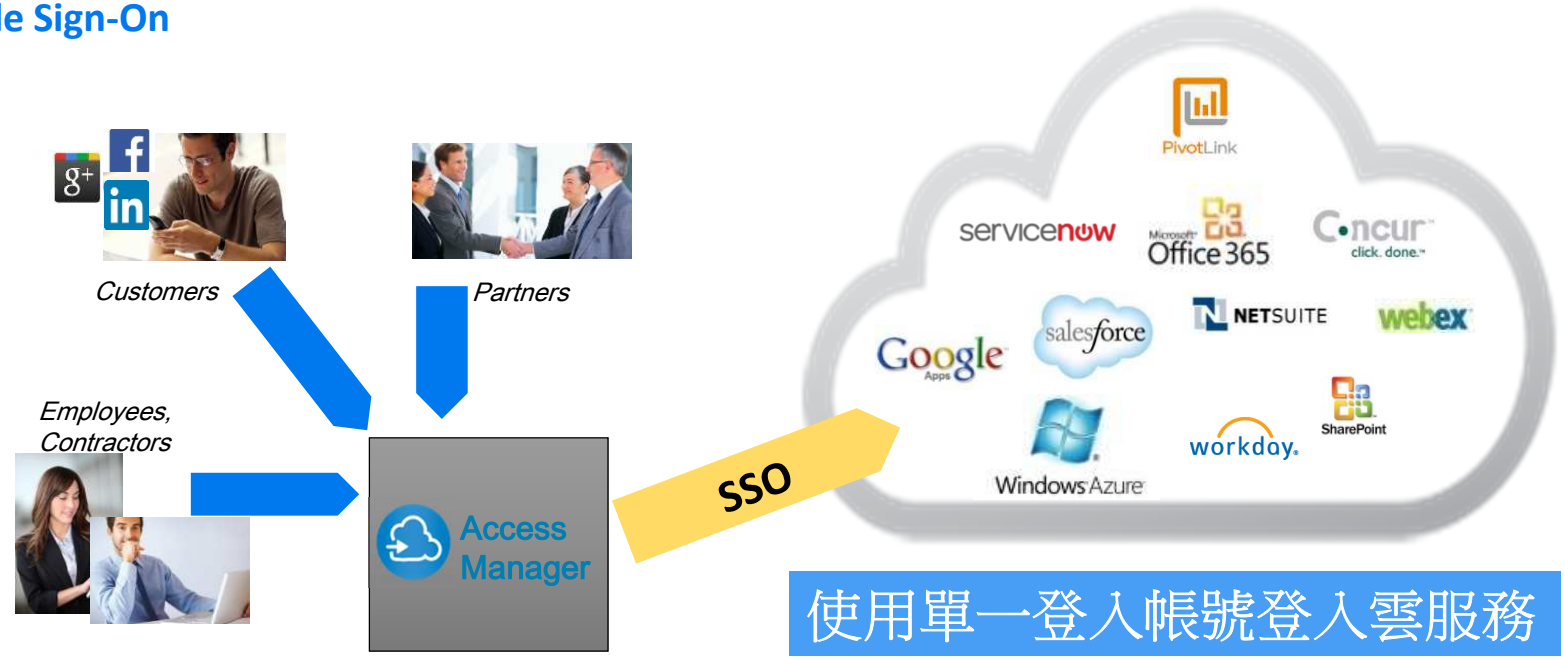
RADIUS

X509

Advanced Authentication

雲端服務

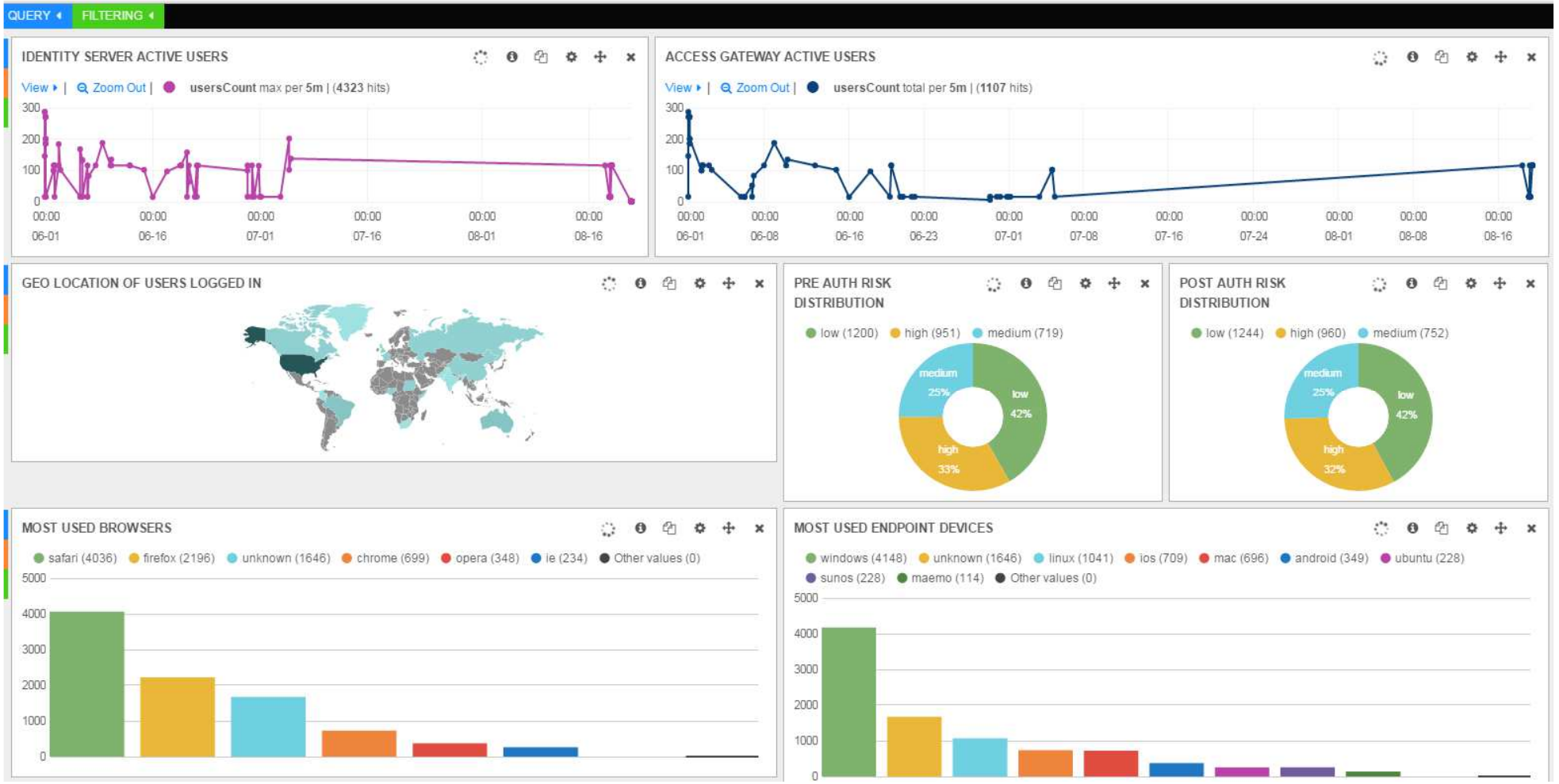
Federated Single Sign-On



使用單一登入帳號登入雲服務

- 遵循國際雲端認證整合規範
- SAML、ADFS、WS-Federation、WS-Trust、Liberty、OAuth2 + OpenID connect
- Identity Provider initiated and Service Provider initiated SSO
- Just-In-Time (JIT) Provisioning

分析與報表


QUERY
FILTERING
IDENTITY SERVER ACTIVE USERS
View | Zoom Out | usersCount max per 5m | (4323 hits)
300
200
100
0
00:00 06-01
00:00 06-16
00:00 07-01
00:00 07-16
00:00 08-01
00:00 08-16
ACCESS GATEWAY ACTIVE USERS
View | Zoom Out | usersCount total per 5m | (1107 hits)
300
200
100
0
00:00 06-01
00:00 06-08
00:00 06-16
00:00 06-23
00:00 07-01
00:00 07-08
00:00 07-16
00:00 07-24
00:00 08-01
00:00 08-08
00:00 08-16
GEO LOCATION OF USERS LOGGED IN
PRE AUTH RISK DISTRIBUTION
low (1200) high (951) medium (719)
medium 25%
low 42%
high 33%
POST AUTH RISK DISTRIBUTION
low (1244) high (960) medium (752)
medium 25%
low 42%
high 32%
MOST USED BROWSERS
safari (4036) firefox (2196) unknown (1646) chrome (699) opera (348) ie (234) Other values (0)
5000
4000
3000
2000
1000
0
MOST USED ENDPOINT DEVICES
windows (4148) unknown (1646) linux (1041) ios (709) mac (696) android (349) ubuntu (228)
sunos (228) maemo (114) Other values (0)
5000
4000
3000
2000
1000
0

特權管理

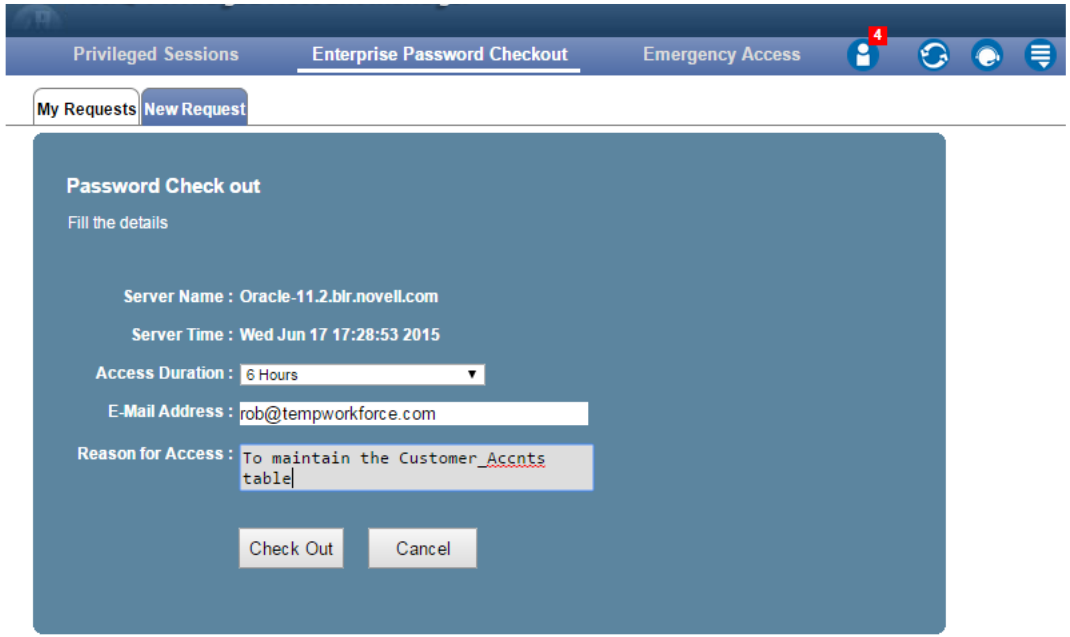
特權管理功能

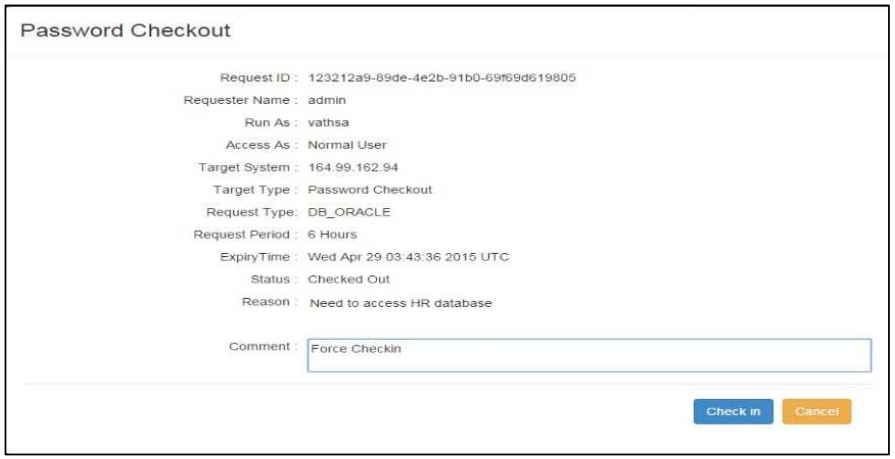
1. 可管控Linux, UNIX, Windows, Databases 等伺服器帳號
2. 特權帳號代登入
3. 特權帳號密碼函
4. 即時監控
5. 行為側錄或敲鍵播放
6. 多因素認證整合
7. 提供API呼叫
8. 提供稽核紀錄與報表

1. 資料是資源
2. 安全連線
3. 低權限
4. 政策存取
5. 資產不安全
6. 重複驗證
7. 收集資訊

簽核流程與Portal

密碼箱與密碼借出機制



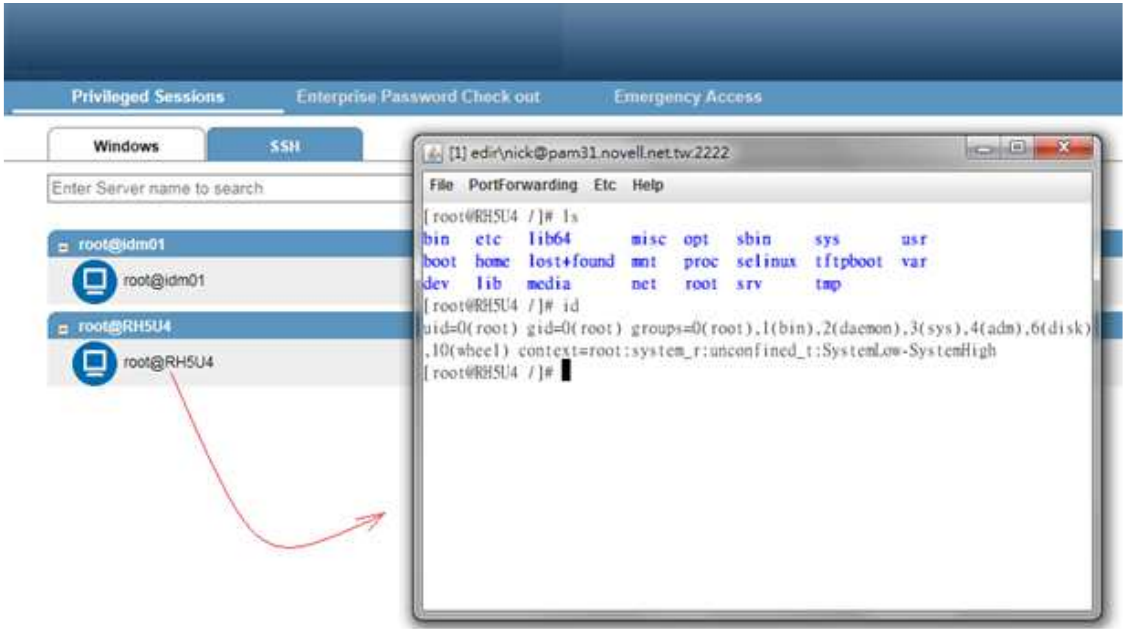


可申請特權帳號的密碼與使用期限，到期後自動回收重置密碼

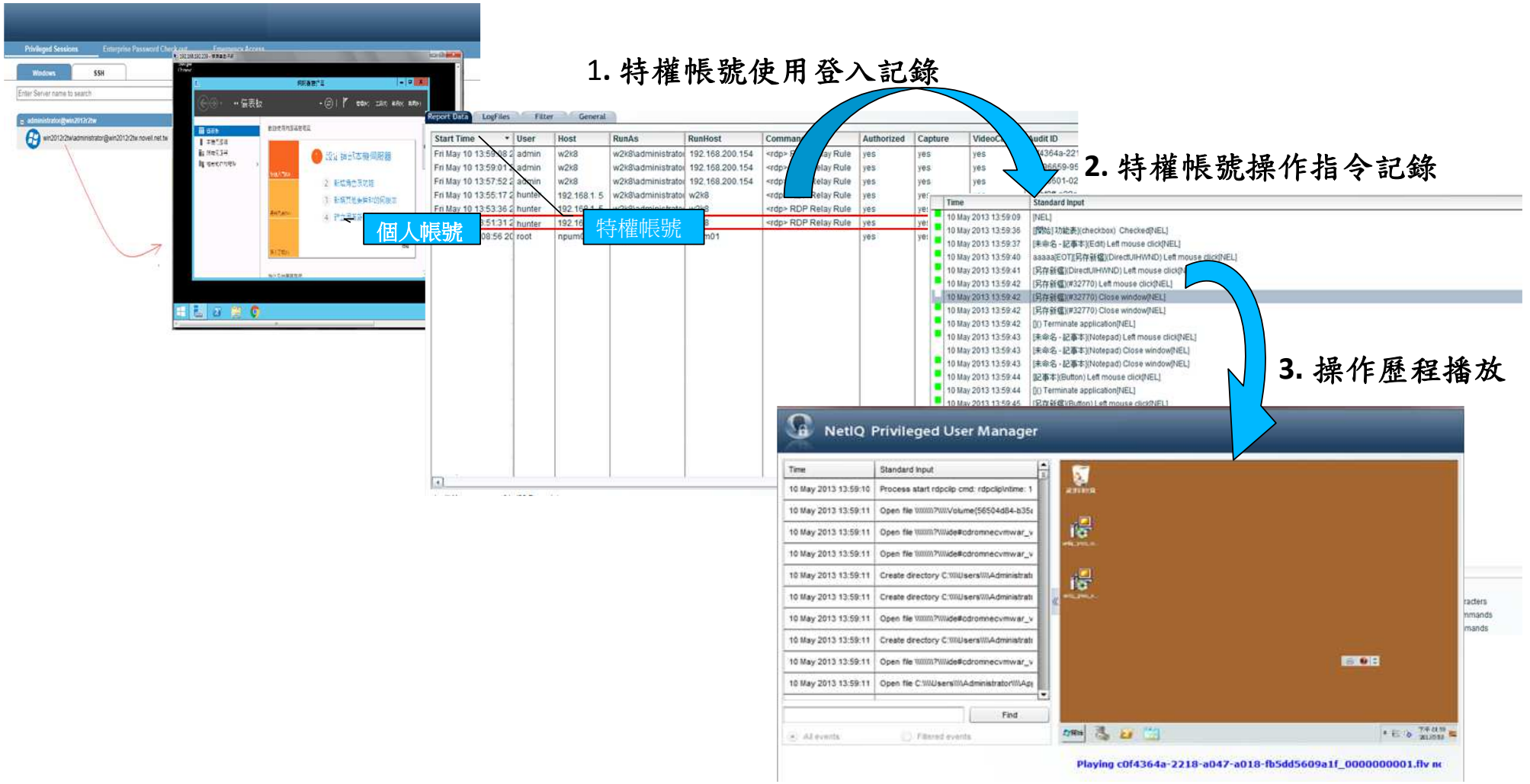
Web中央管控

Windows RDP

Unix/Linux SSH

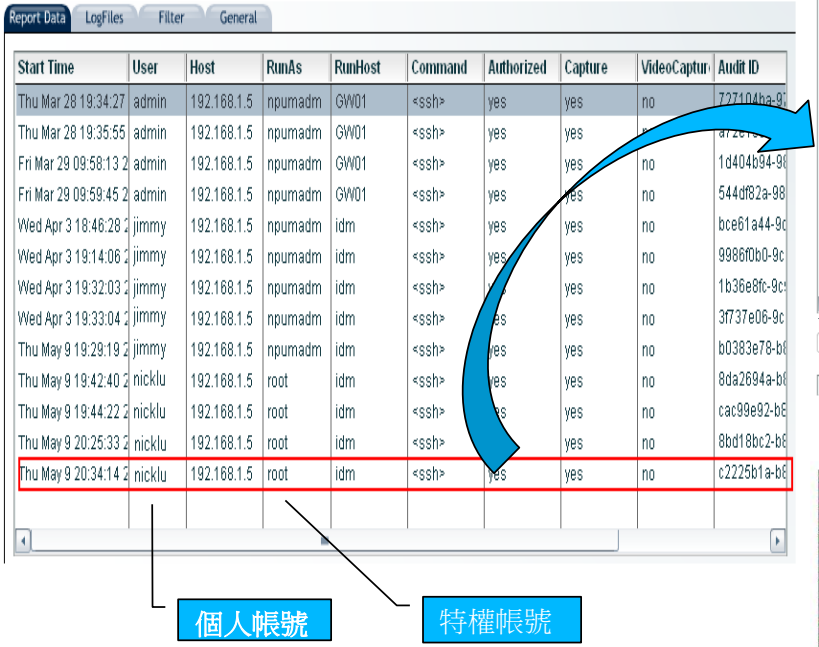


Windows操作使用歷程記錄

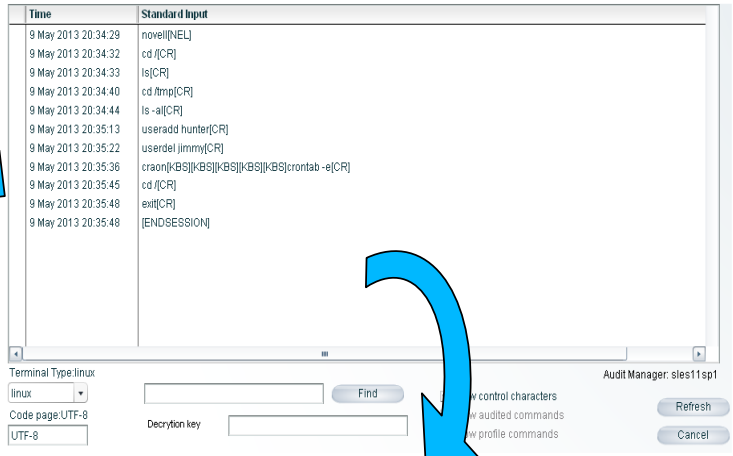


SSH操作使用歷程記錄

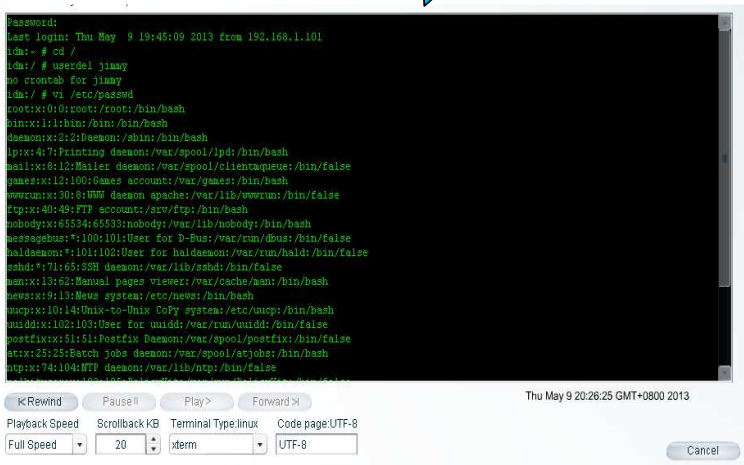
1. 特權帳號使用登入記錄



2. 特權帳號操作指令記錄

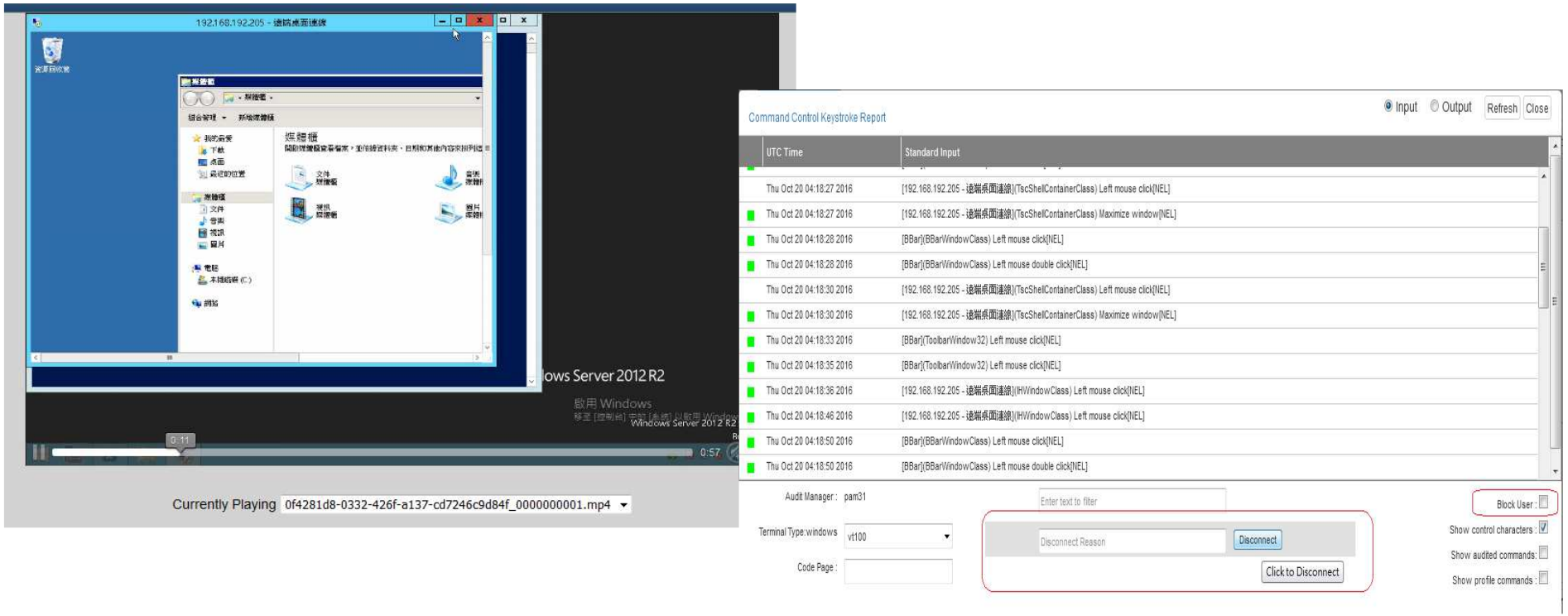


3. 操作歷程播放



- 可查詢的鍵盤指令操作紀錄

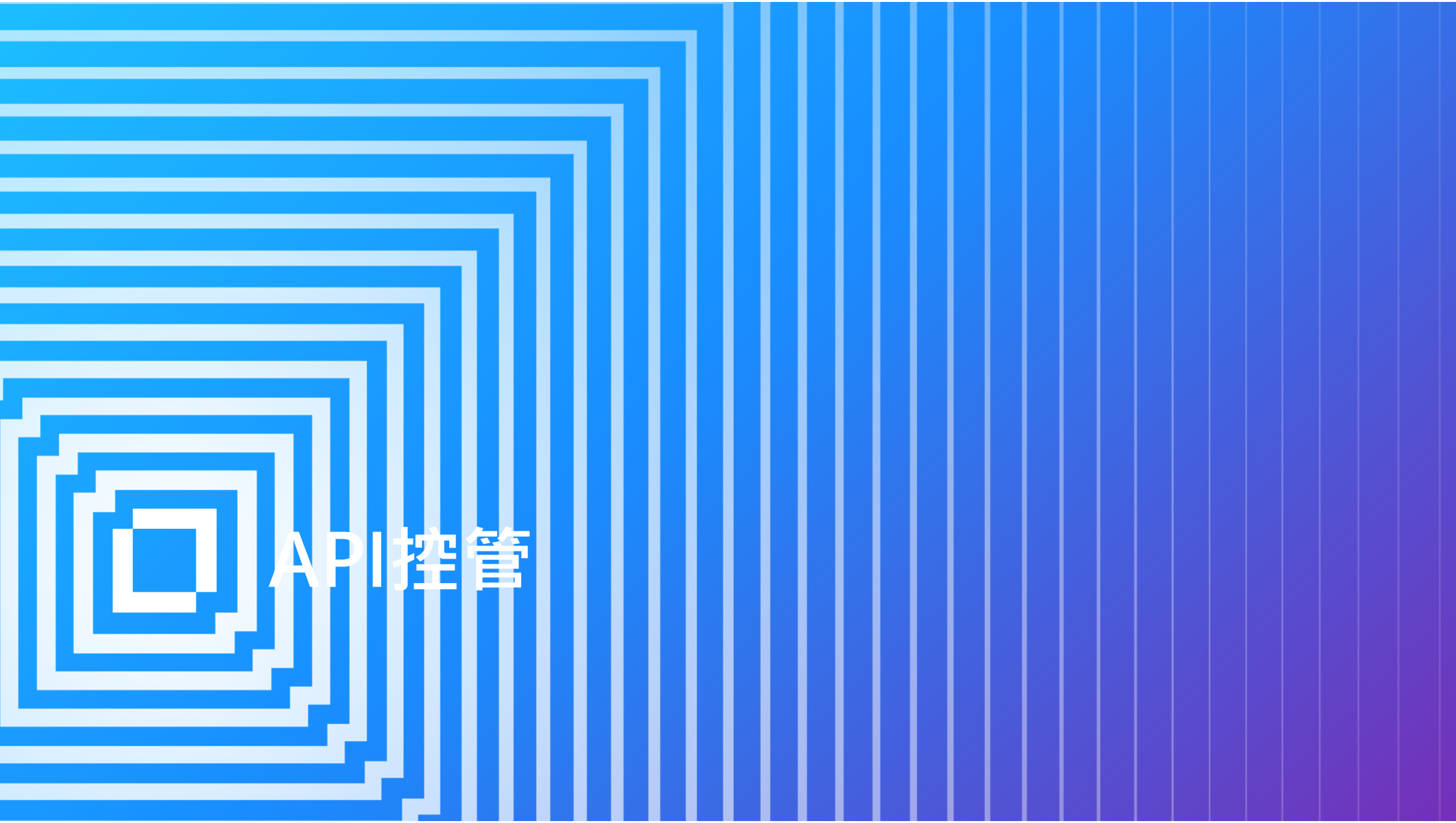
連線監控與管控



即時監控使用者在Unix/Linux/Windows系統上的行為

支援多因子認證


HID
ProxCard II
AUTHASAS
956534
RSA
SecurID
1684 314
VASCO
USB
自然人憑證
Citizen Digital Certificate
甄 美 麗
使用期限：2015/01/01
TP03 0000 0123 4567
經濟部 工商憑證

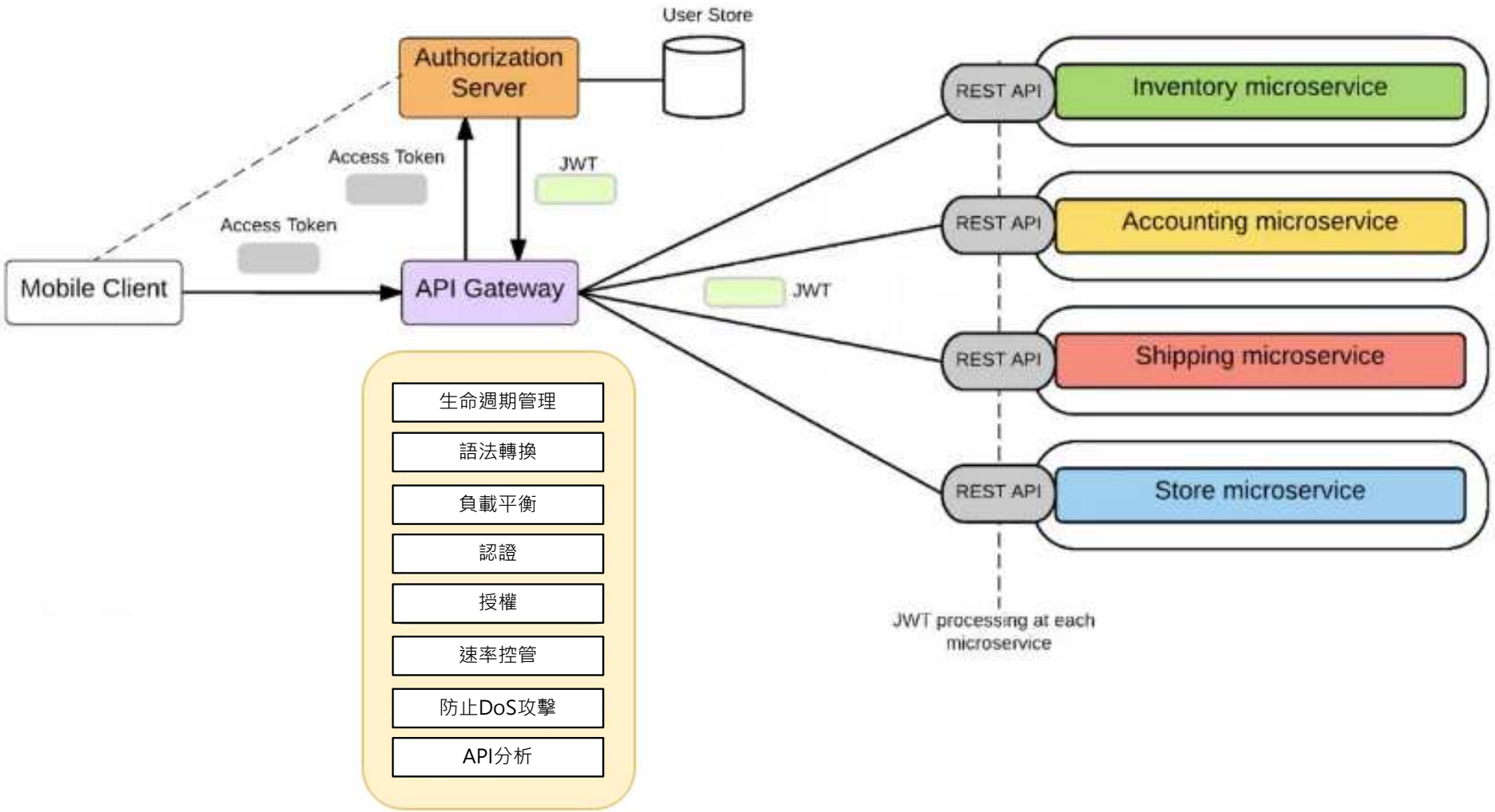

API控管

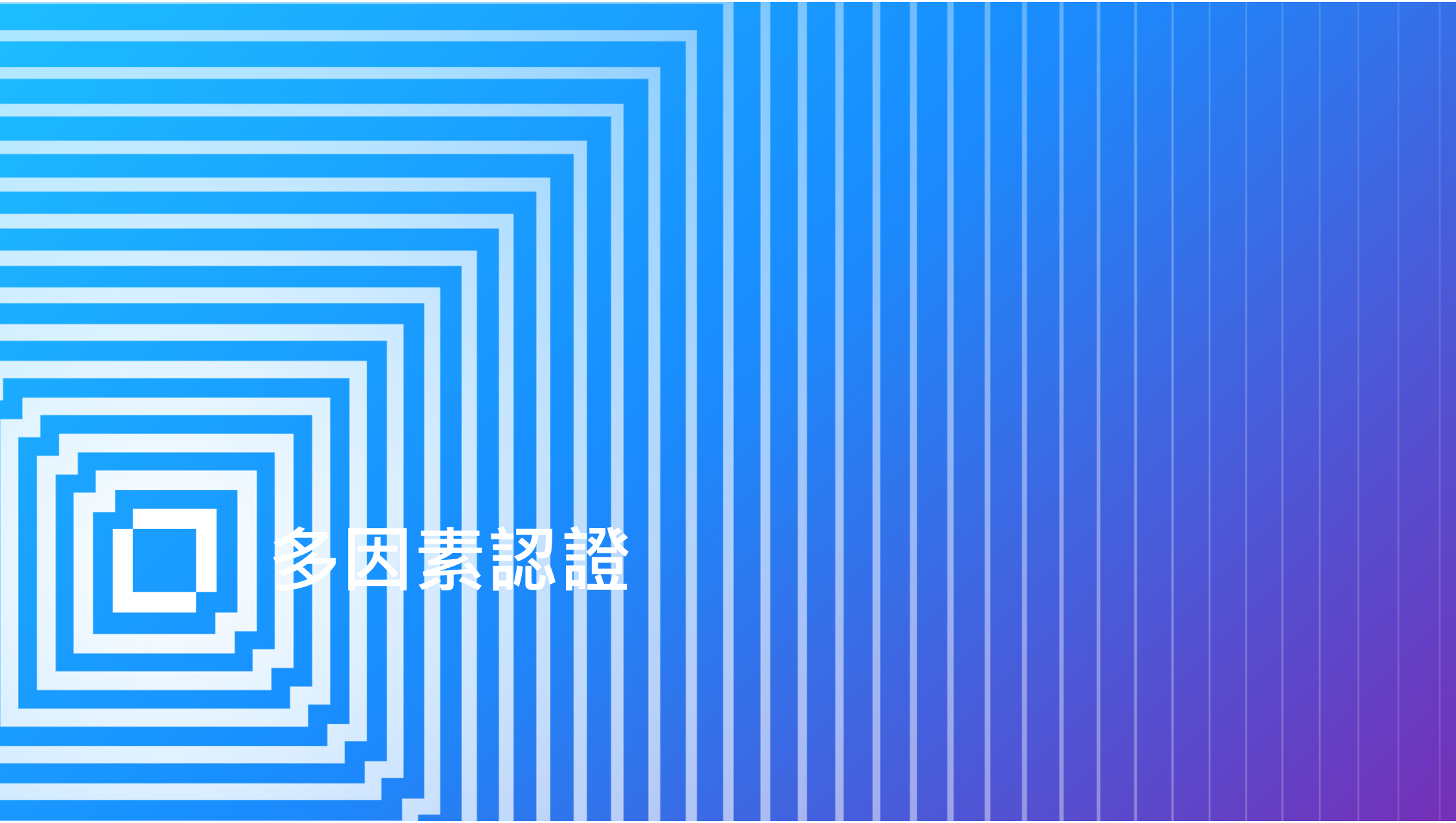
API管控功能

1. 單點管控所有API
2. API 生命週期管控
3. 管控API認證與授權
4. 速率控管 (Rate Limiting Control)
5. 風險管制執行
6. 多因素認證 for API clients
7. 防制DoS攻擊
8. 提供稽核紀錄與報表

1. 資料是資源
2. 安全連線
3. 低權限
4. 政策存取
5. 資產不安全
6. 重複驗證
7. 收集資訊

API Gateway


User Store
Authorization Server
Access Token
JWT
Access Token
Mobile Client
API Gateway
JWT
REST API
Inventory microservice
REST API
Accounting microservice
REST API
Shipping microservice
REST API
Store microservice
JWT processing at each microservice
生命週期管理
語法轉換
負載平衡
認證
授權
速率控管
防止DoS攻擊
API分析

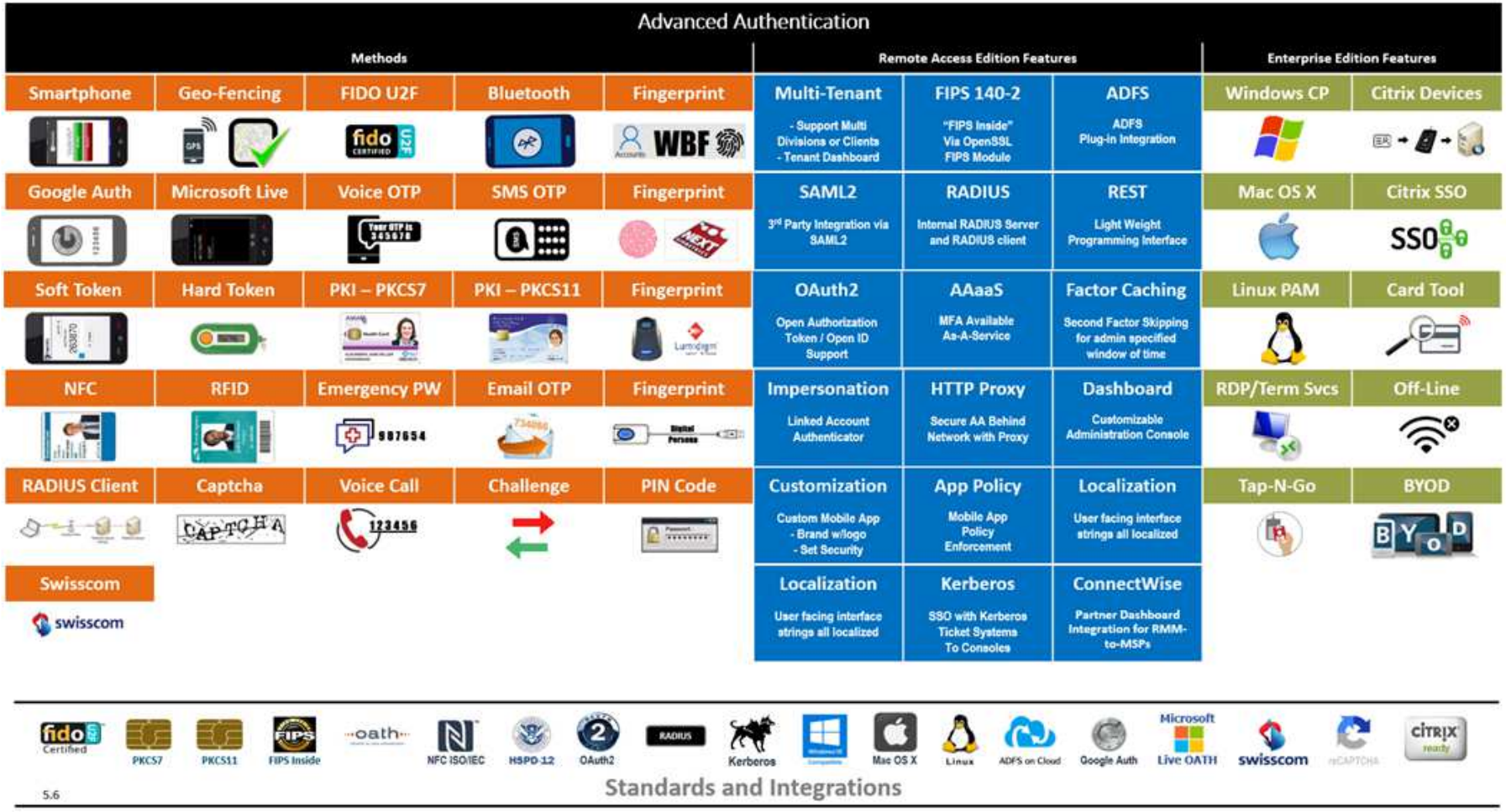

多因素認證

多因素認證功能

1. 支援多種認證(Multi-Factor)
2. 支援叢集架構
3. 提供API、OAuth 2.0 與 SAML 2.0認證
4. 提供二次認證設備註冊機制
5. 稽核紀錄與報表

1. 資料是資源
2. 安全連線
3. 低權限
4. 政策存取
5. 資產不安全
6. 重複驗證
7. 收集資訊

多種認證方式


Advanced Authentication
Methods
Remote Access Edition Features
Enterprise Edition Features
Smartphone
Geo-Fencing
FIDO U2F
Bluetooth
Fingerprint
Multi-Tenant
- Support Multi Divisions or Clients
- Tenant Dashboard
FIPS 140-2
"FIPS Inside" Via OpenSSL FIPS Module
ADFS
ADFS Plug-in Integration
Windows CP
Citrix Devices
Google Auth
Microsoft Live
Voice OTP
SMS OTP
Fingerprint
SAML2
3rd Party Integration via SAML2
RADIUS
Internal RADIUS Server and RADIUS client
REST
Light Weight Programming Interface
Mac OS X
Citrix SSO
Soft Token
Hard Token
PKI – PKCS7
PKI – PKCS11
Fingerprint
OAuth2
Open Authorization Token / Open ID Support
AAaaS
MFA Available As-A-Service
Factor Caching
Second Factor Skipping for admin specified window of time
Linux PAM
Card Tool
NFC
RFID
Emergency PW
Email OTP
Fingerprint
Impersonation
Linked Account Authenticator
HTTP Proxy
Secure AA Behind Network with Proxy
Dashboard
Customizable Administration Console
RDP/Term Svcs
Off-Line
RADIUS Client
Captcha
Voice Call
Challenge
PIN Code
Customization
Custom Mobile App
- Brand w/logo
- Set Security
App Policy
Mobile App Policy Enforcement
Localization
User facing interface strings all localized
Tap-N-Go
BYOD
Swisscom
Localization
User facing interface strings all localized
Kerberos
SSO with Kerberos Ticket Systems To Consoles
ConnectWise
Partner Dashboard Integration for RMM-to-MSPs
fido Certified
PKCS7
PKCS11
FIPS Inside
oath
NFC ISO/IEC
HSPD-12
OAuth2
RADIUS
Kerberos
Mac OS X
Linux
ADFS on Cloud
Google Auth
Microsoft Live OATH
swisscom
citrix ready
Standards and Integrations

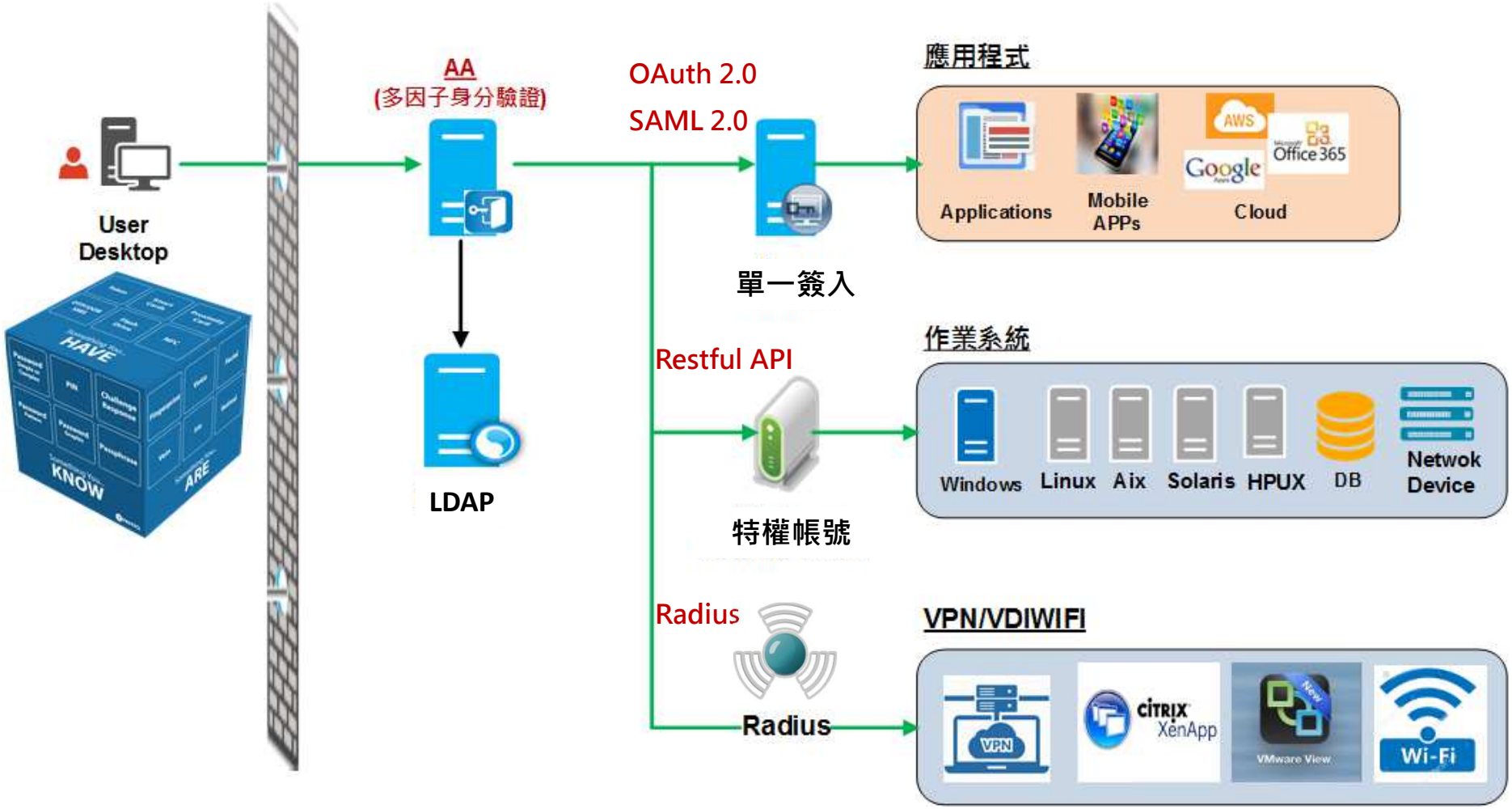
設備註冊機制


新增 FIDO 2.0 驗證程式
備註
Yubikey
類別
<預設>
按一下 "儲存" 以開始註冊
儲存
取消

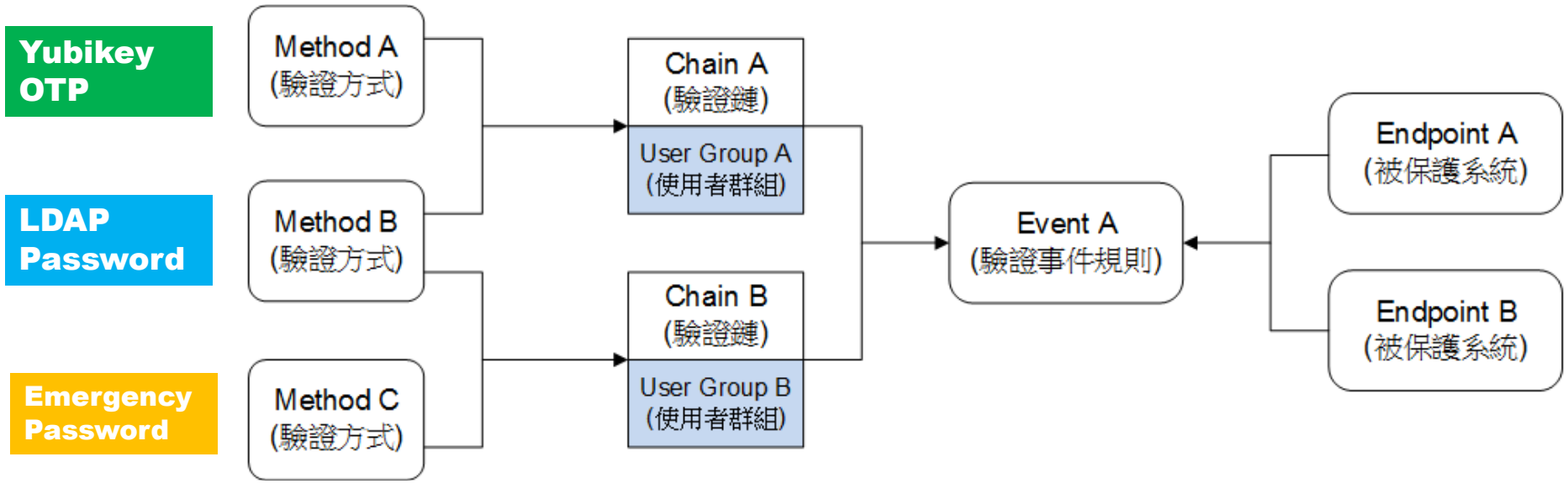

驗證有效時間：02:55
重新產生
取消驗證
請以行動身分識別APP掃描QRcode進行驗證
QRcode有效期限3分鐘，逾時請重新產生


已註冊的驗證程式
FIDO 2.0
Yubikey
LDAP 密碼
已自動建立
新增驗證程式
FIDO 2.0
新增更多
LDAP 密碼
新增更多
密碼

介接通訊協定


AA
(多因子身分驗證)
OAuth 2.0
SAML 2.0
應用程式
User
Desktop
HAVE
KNOW
ARE
LDAP
單一簽入
Applications
Mobile
APPs
AWS
Google
Office 365
Cloud
Restful API
作業系統
特權帳號
Windows
Linux
Aix
Solaris
HPUX
DB
Netwok
Device
Radius
VPN/VDIWIFI
Radius
VPN
CITRIX
XenApp
VMware View
Wi-Fi

多因子驗證規則套用



可設定身分驗證規則，配置下列使用者身分安全驗證方式：

- 雙因子驗證
- 多因子驗證
- 無密碼驗證
- 多選一驗證

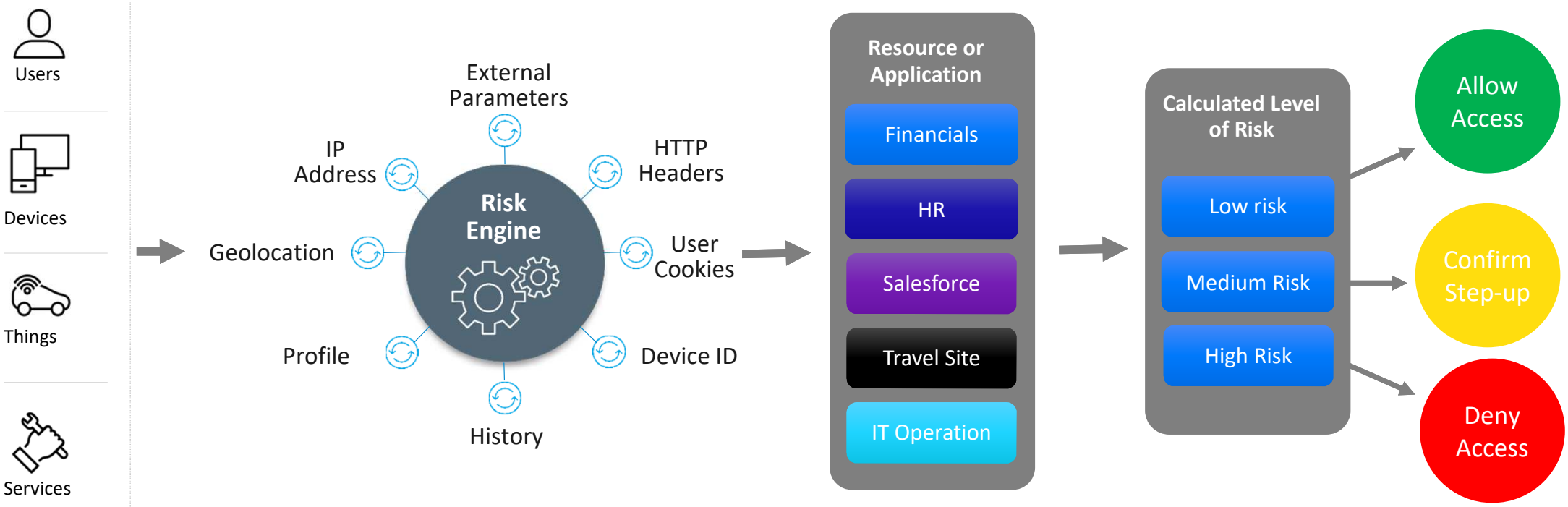
風險控管

風險控管

1. 行為分析
2. 計算風險
3. 學習行為與預測潛在風險
4. 可整合第三方服務來取得分析風險所需資料
5. 認證前評估與降低風險
6. 稽核紀錄與報表

1. 資料是資源
2. 安全連線
3. 低權限
4. 政策存取
5. 資產不安全
6. 重複驗證
7. 收集資訊

風險控管系統


Users
Devices
Things
Services
External Parameters
IP Address
HTTP Headers
Geolocation
Risk Engine
User Cookies
Profile
Device ID
History
Resource or Application
Financials
HR
Salesforce
Travel Site
IT Operation
Calculated Level of Risk
Low risk
Medium Risk
High Risk
Allow Access
Confirm Step-up
Deny Access

風險控管規則設定

Risk-based Policies

Add Risk Policy

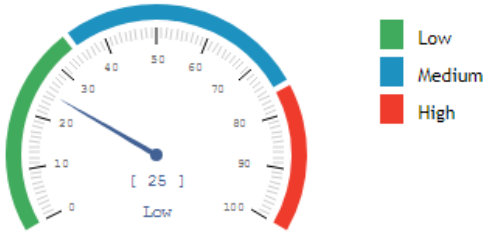
Policy Name: My Risk Rule
Description: For Testing
Assign Policy To: IDP-Cluster

Policy Rules Actions

Risk Rule	Action (when rule condition is met)	Risk Score (when rule condition is *not* met)
DemoRule_InternalNetwork	Allow Access	25

Risk Levels Actions

Total Risk Score	Risk Level	Action	Share	Reduce Score
Less than 35	Low	Allow Access		0
Between 35 and 75	Medium	Authenticate using Smartphone		0
Greater than 75	High	Deny Access		0



安全資訊與事件管理

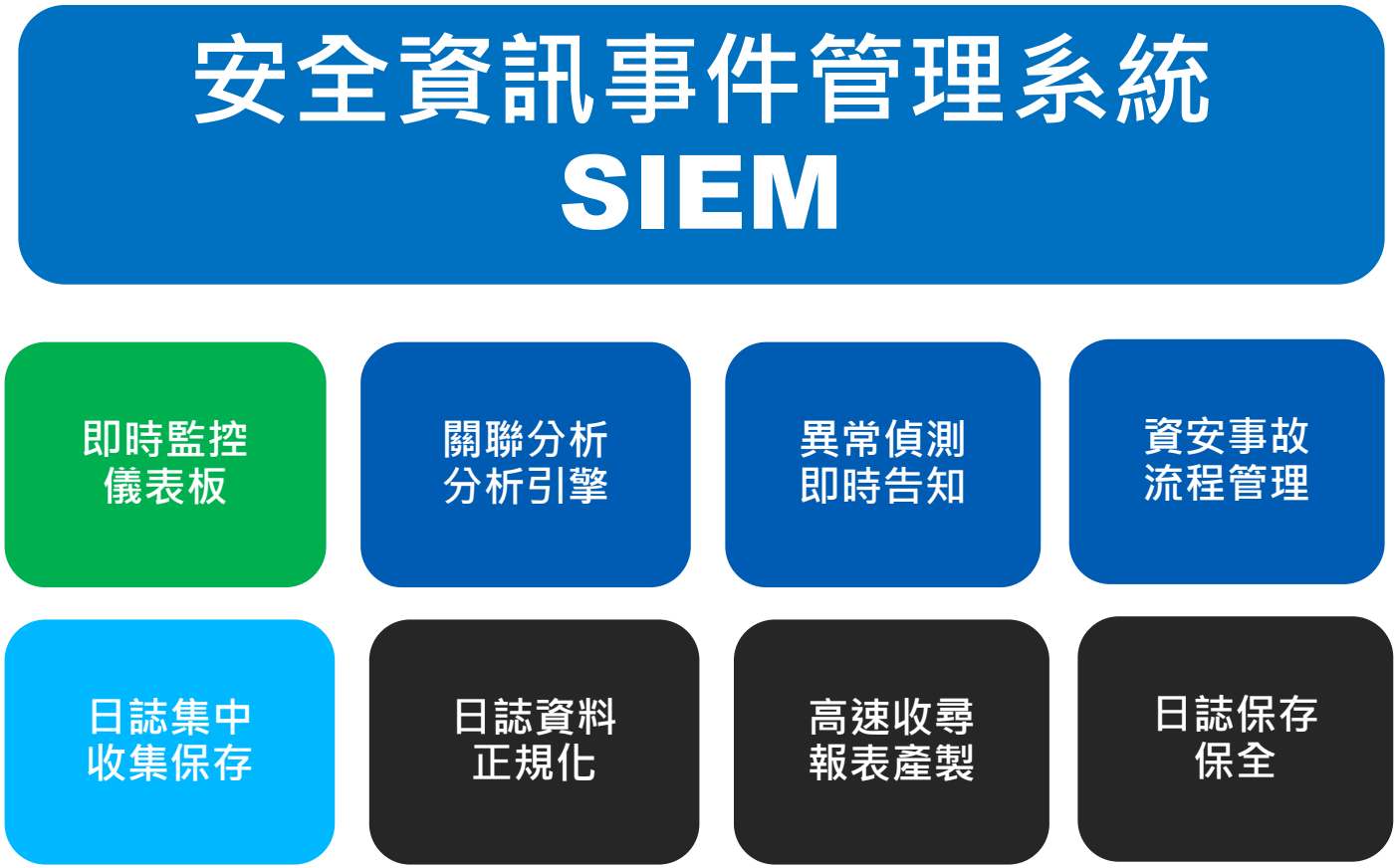
安全資訊與事件管理

1. 收集稽核資料。
2. 將不同的資料標準化到統一稽核資料格式。
3. 將事件對應至標準法規。
4. 整合稽核資料。
5. 分析稽核資料。
6. 比對多個系統間的事件以判斷是否有安全問題。
7. 當資料未遵循規範時傳送通知。
8. 針對通知採取動作，以遵守公司規則。
9. 產生報告以證明遵循法規。

1. **資料是資源**
2. **安全連線**
3. **低權限**
4. **政策存取**
5. **資產不安全**
6. **重複驗證**
7. **收集資訊**

日誌管理系統

安全資訊事件管理系統

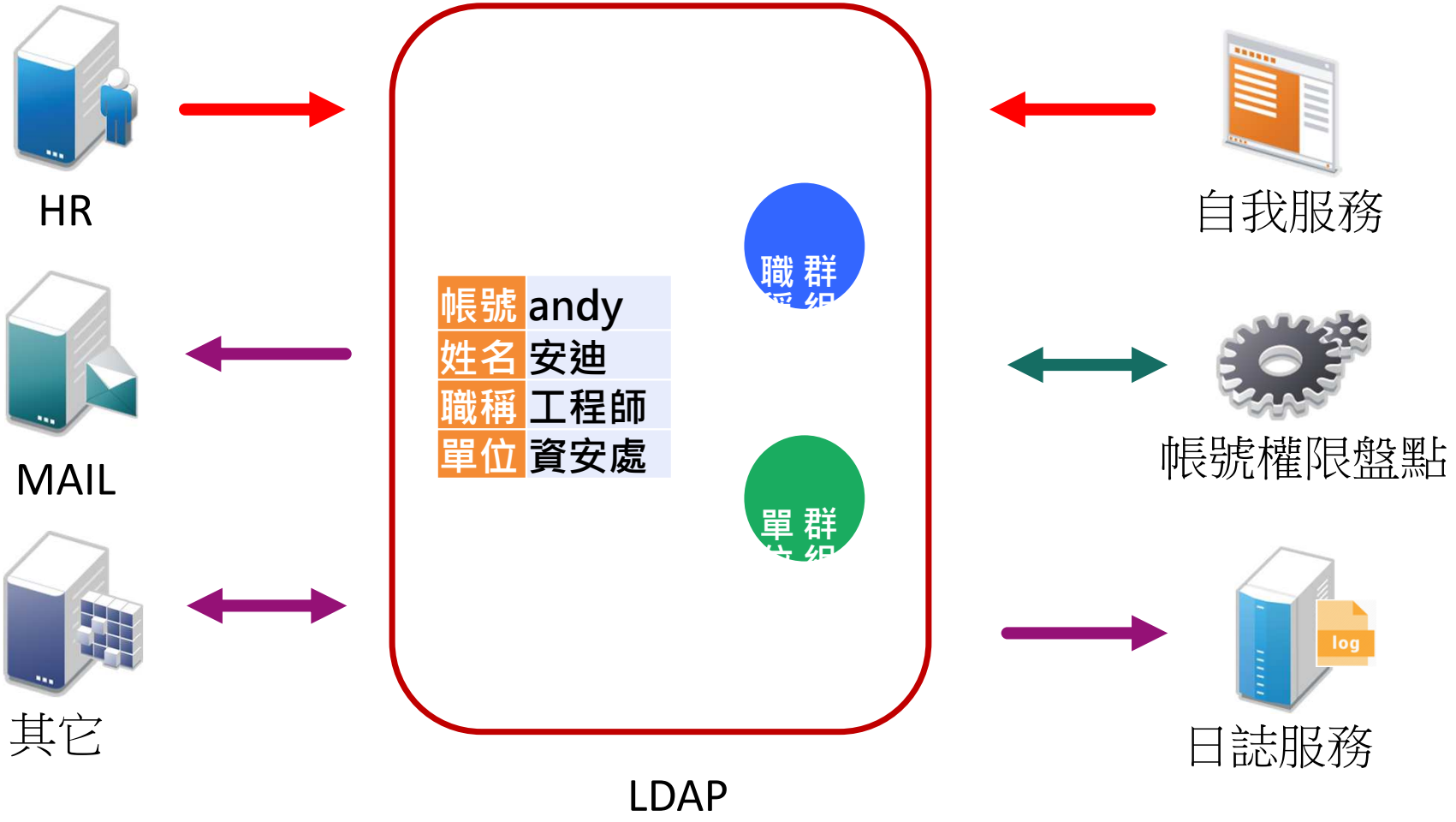

安全資訊事件管理系統
SIEM
即時監控
儀表板
關聯分析
分析引擎
異常偵測
即時告知
資安事故
流程管理
日誌集中
收集保存
日誌資料
正規化
高速收尋
報表產製
日誌保存
保全


零信任原則與IAM規劃
設計

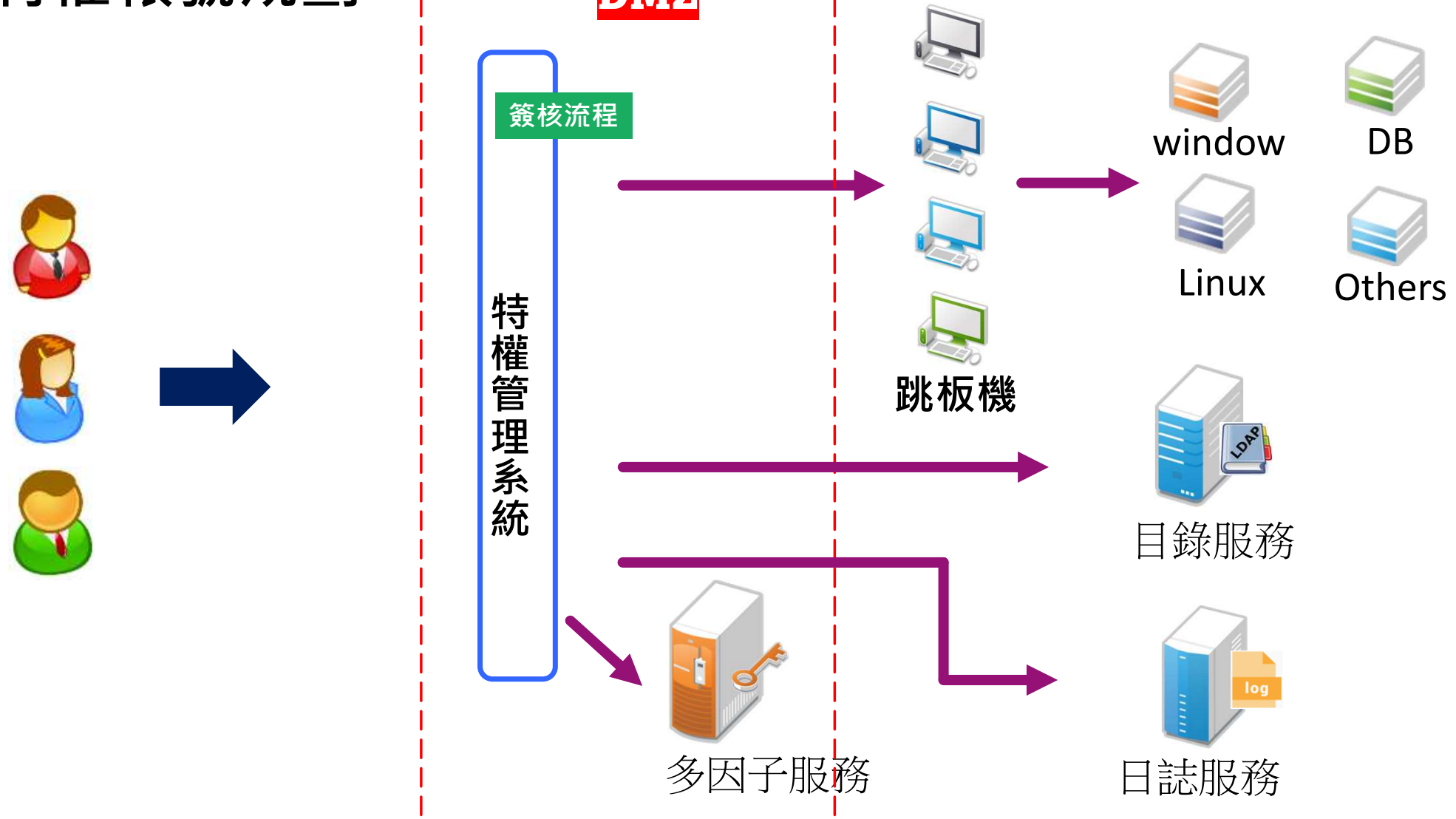
身份治理建置規劃順序

1. 建置目錄服務，並且資料來源為人資系統、校務系統、差勤系統。
2. 至少建立二種群組：單位群組與職稱群組。
3. 日誌服務整合。
4. 設備與AP整合。
5. 自我服務系統整合。
6. 帳號權限盤點與身份核規。

身份治理規劃


HR
MAIL
其它
帳號 andy
姓名 安迪
職稱 工程師
單位 資安處
職 群
單 群
LDAP
自我服務
帳號權限盤點
log
日誌服務

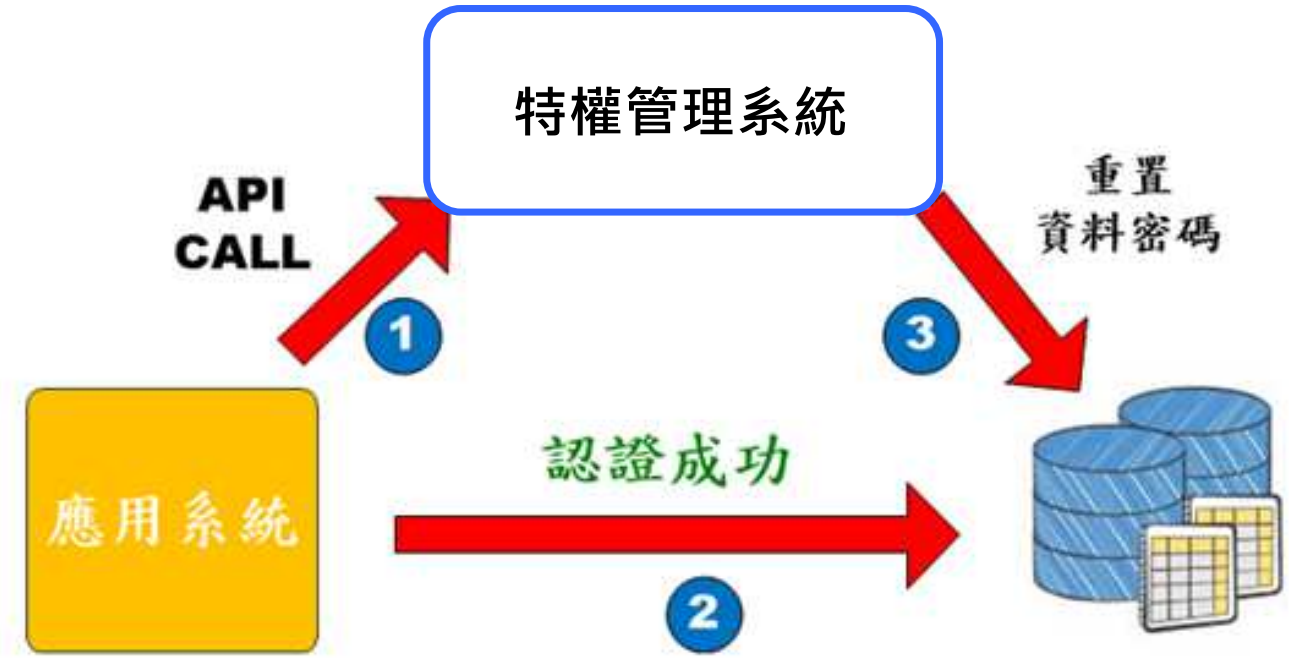
特權帳號規劃


DMZ
簽核流程
特權管理系統
跳板機
window
DB
Linux
Others
目錄服務
LDAP
多因子服務
日誌服務
log

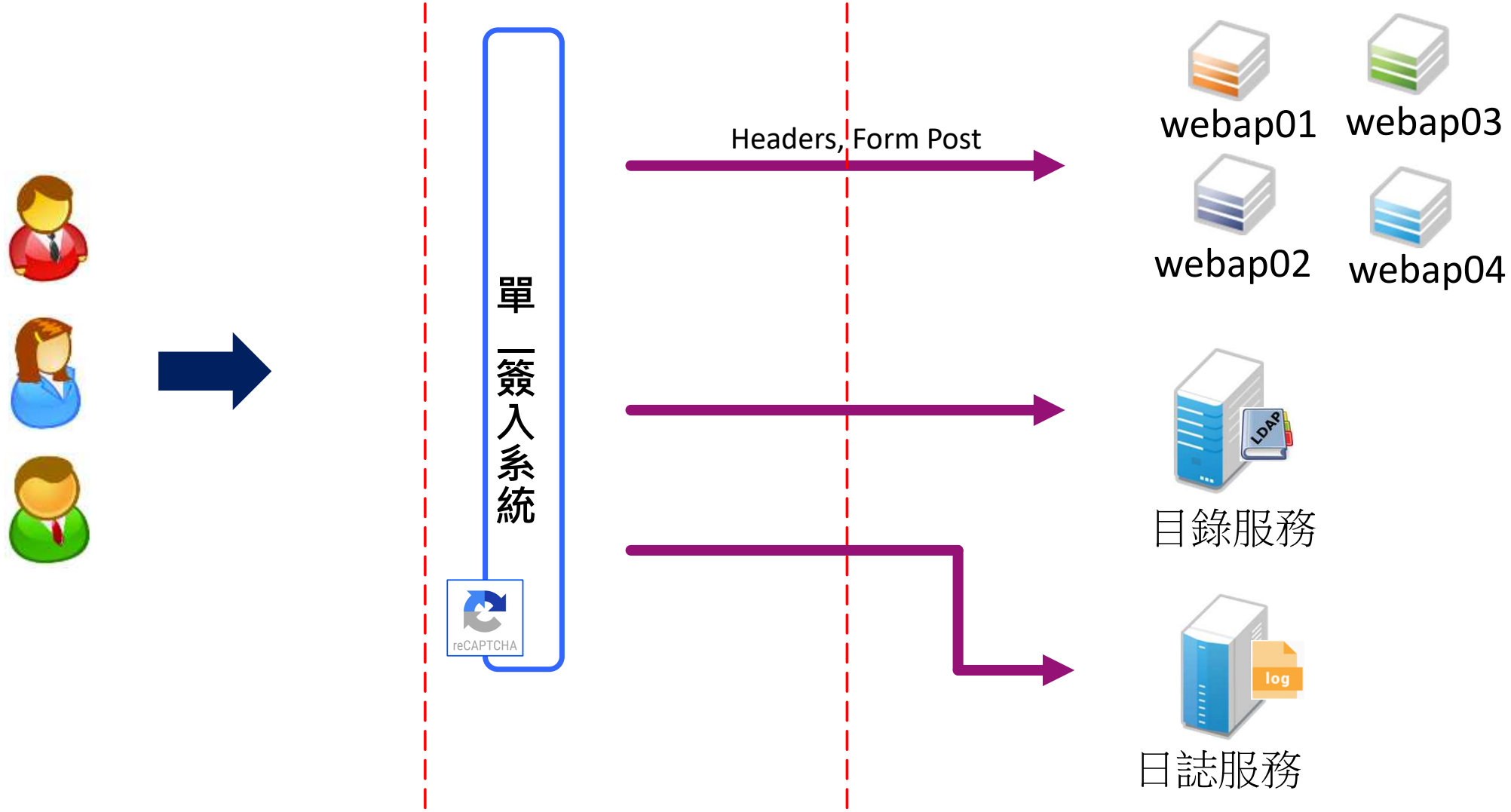
特權帳號規劃

解決在程式碼裡

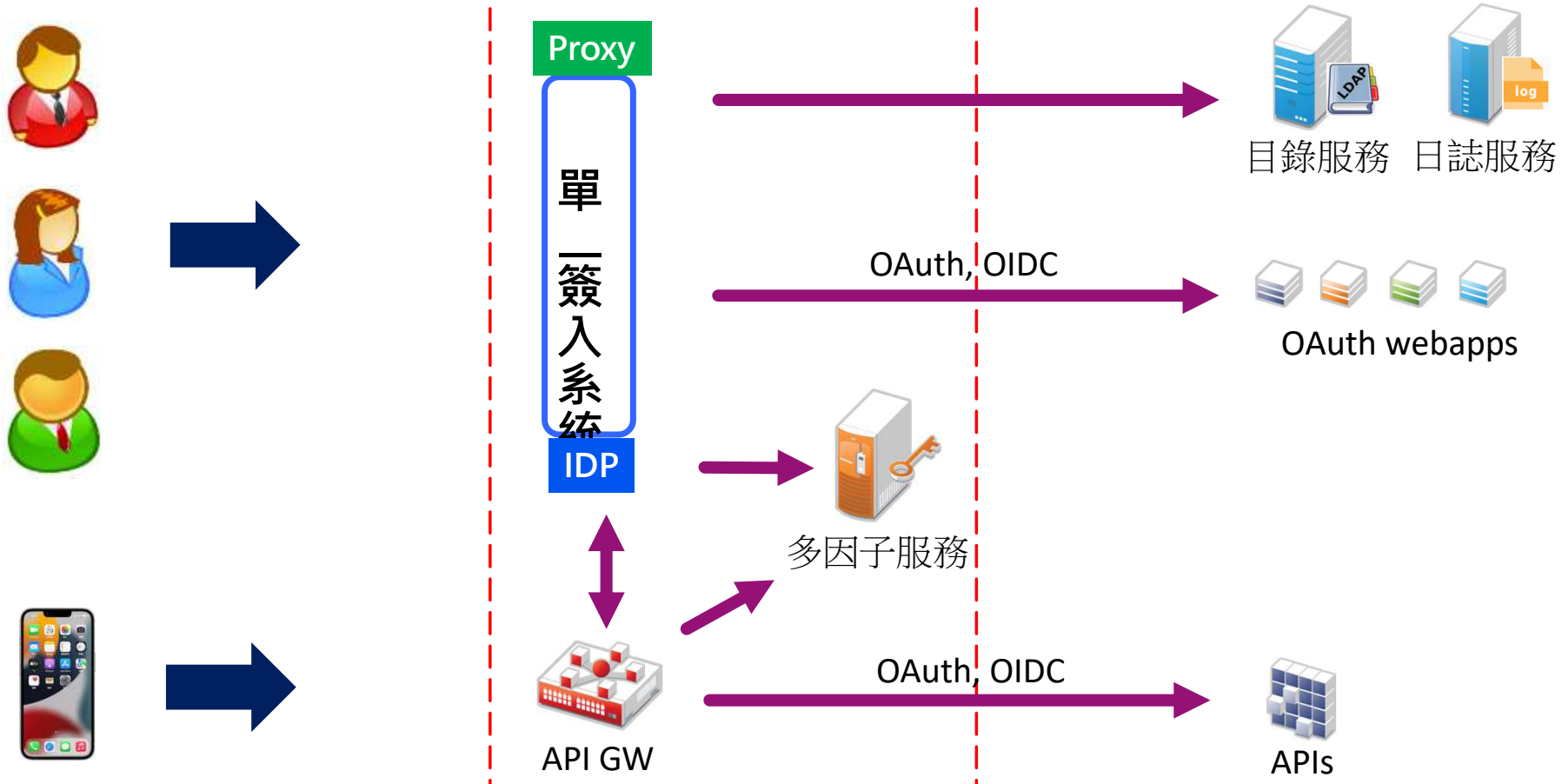
萬年不變的AP連線密碼



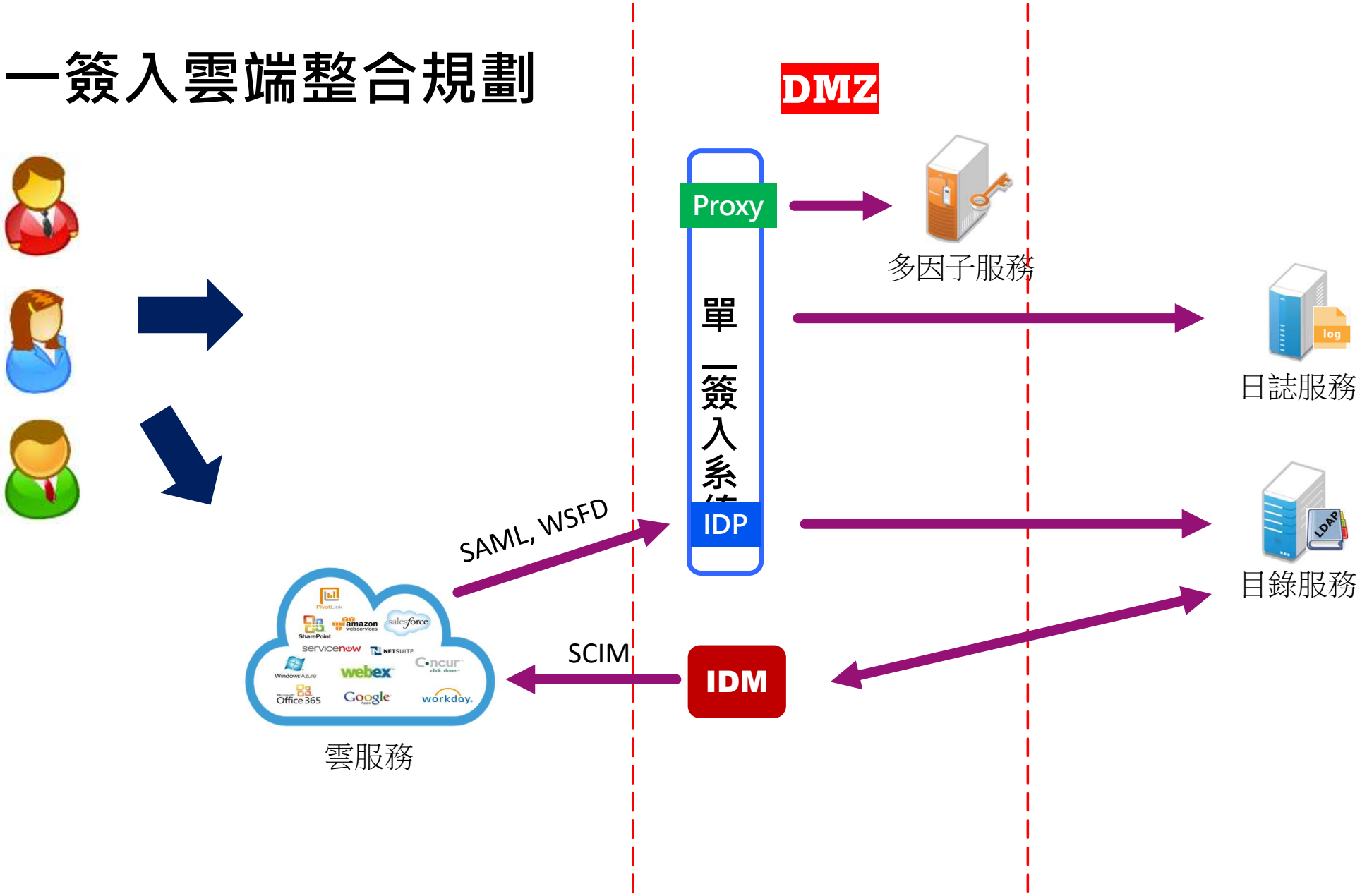
傳統單一簽入規劃


DMZ
單一簽入系統
reCAPTCHA
Headers, Form Post
webap01
webap03
webap02
webap04
LDAP
目錄服務
log
日誌服務

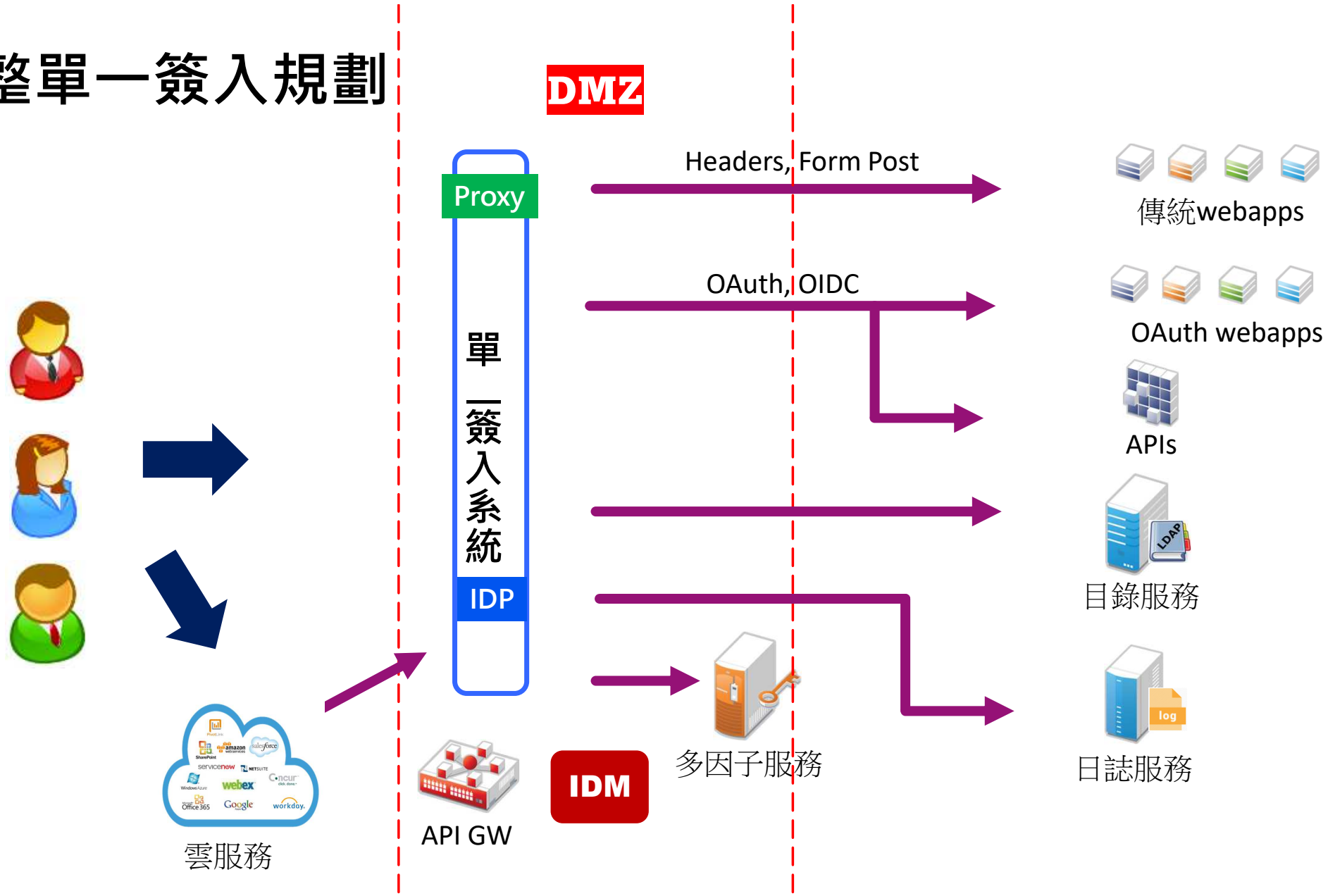
單一簽入Token認證規劃



單一簽入雲端整合規劃

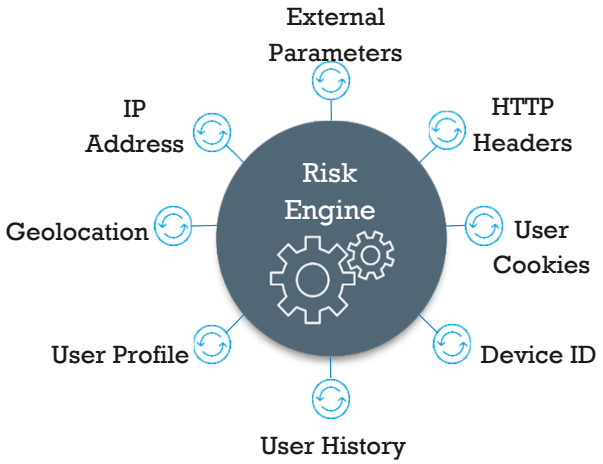


完整單一簽入規劃


DMZ
Proxy
單一簽入系統
IDP
Headers, Form Post
OAuth, OIDC
傳統webapps
OAuth webapps
APIs
目錄服務
日誌服務
多因子服務
IDM
API GW
雲服務

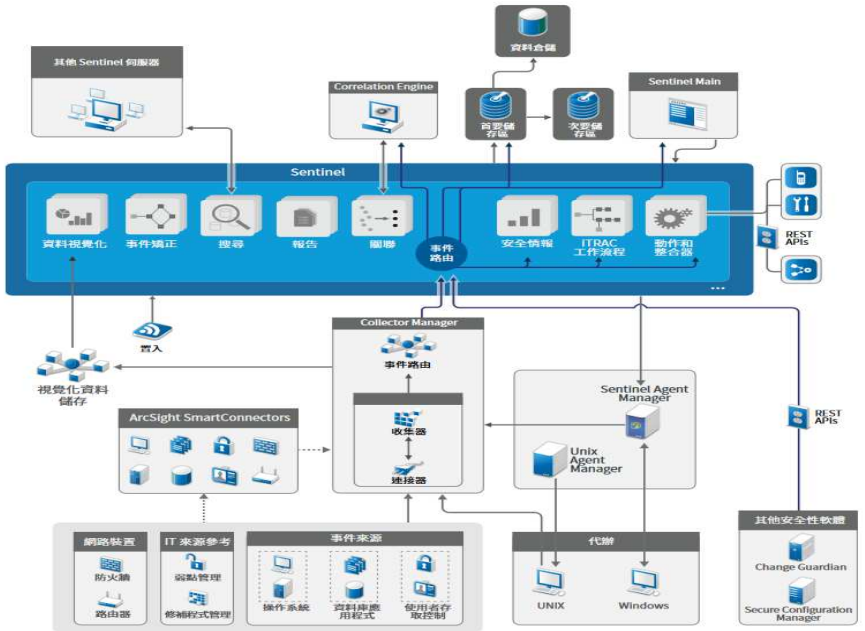
單一簽入+多因子認證+風險控管使用案例

	認證規則
1	登入時每一個人都須提供帳號密碼 + OTP
2	內部網斷 帳號密碼 登入 外部網斷 帳號密碼 + FIDO U2F
3	08:00 – 12:00 帳號密碼 登入 12:01 – 12:59 帳號密碼 + OTP 13:00 – 18:00 帳號密碼 + FIDO U2F 登入 18:01 – 07:59 禁止登入
4	帳號隸屬FIDO群組成員，帳號密碼 + FIDO U2F登入。 不是FIDO群組成員，帳號密碼 + OTP登入。
5	限定只能使用Chrome，其餘的Browser.都不能用



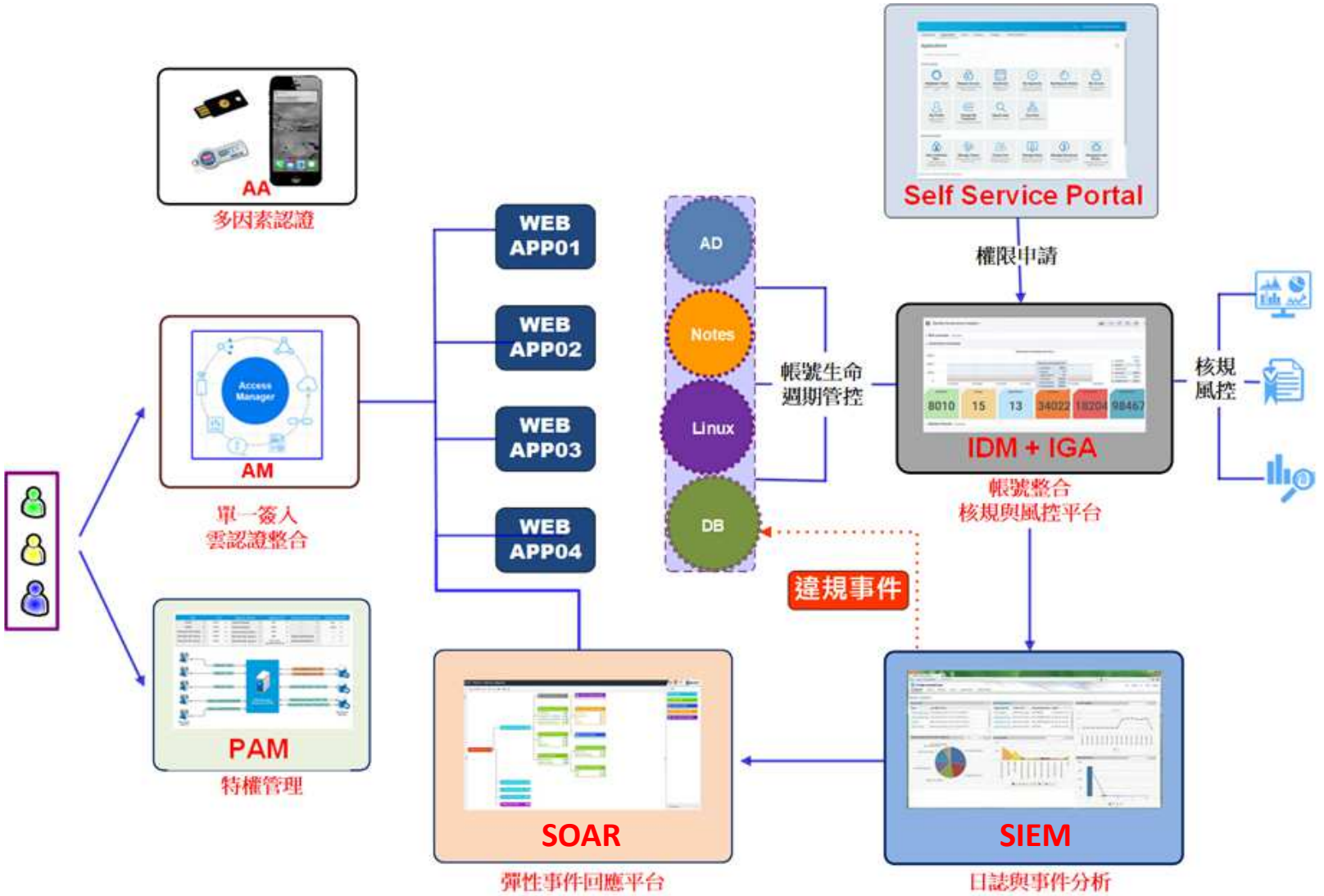
安全資訊事件管理系統

	事件規則	行為
1	一分鐘內登入五次失敗	帳號鎖定
2	一分鐘內帳號從不同IP登入	發信告知使用者
3	一分鐘內十次拒絕存取	發信告知管理者
4	不恰當時間登入高等級系統	發信告知管理者 鎖定執行帳號
5	外部IP存取高等級系統	鎖定執行帳號 API Call 調整防火牆規則



基於零信任概念的完整IAM架構

1. 資料是資源
2. 安全連線
3. 低權限
4. 政策存取
5. 資產不安全
6. 重複驗證
7. 收集資訊




THANKS!