深入剖析特權帳號管理

與居家辦公的資安控管

特權帳號在世界未來的發展趨勢

台灣資安館T23

大會展場S21

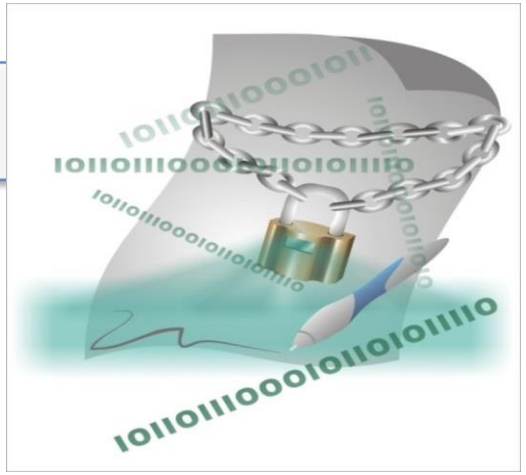
CTO Edward Li

智弘軟體科技

State-of-the-art PAM Product

大綱

- 特權帳號管理的風起雲湧(2018~2025)
- 特權帳號管理的背景知識
- ANCHOR特權帳號管理平台
- 特權帳號管理的未來



特權帳號管理的風起雲湧
(2018~2025)

台灣資安館T23

大會展場S21

智弘軟體科技

State-of-the-art PAM Product

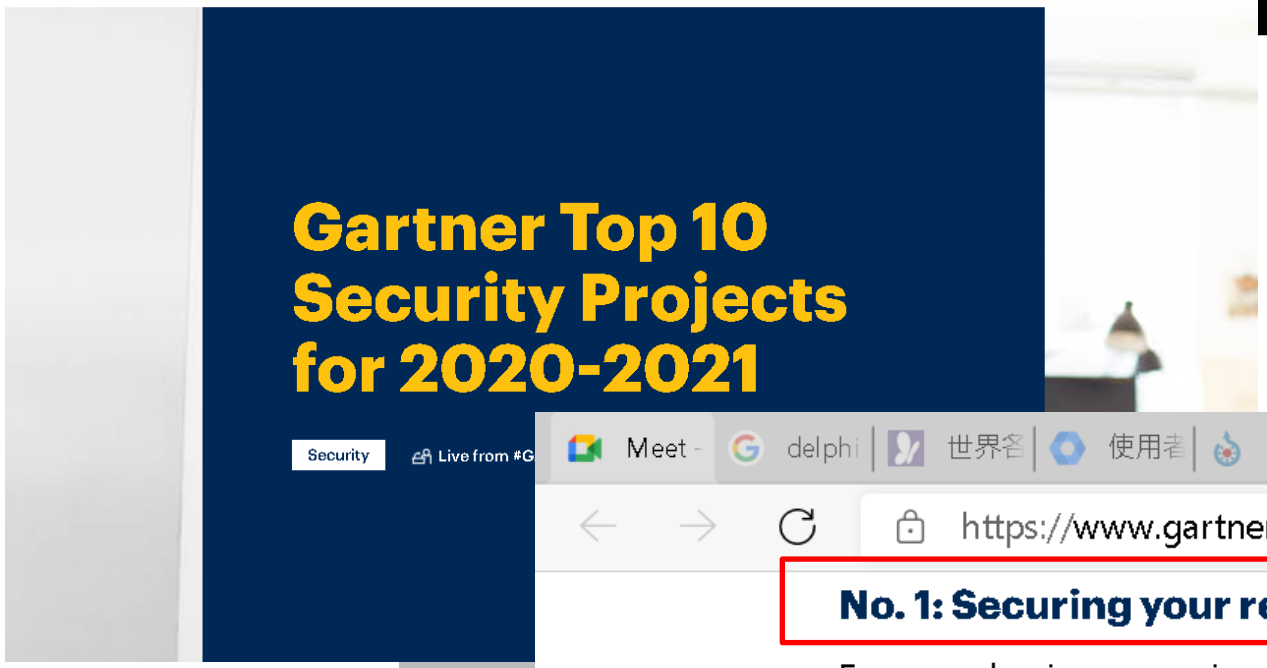
特權帳號管理- Gartner十大安全項目的第一名

State-of-the-art PAM Product

https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020-2021/

Smarter With Gartner Subscribe Search

COVID-19 Executive Finance Human Resources IT Legal & Compliance Marketing Sales Service Suppl



"Focus on
have the l
and distin
2018 Gart
National H

No.
This
acc
mor
shou
all administrat
for third-party access, such as contractors.

Top 10 Security Projects for 201

projects-

site. To learn more, visit our Privacy Policy.
ur use of cookies.

Call +1 855-515-4486 or co
to become a Gartner clien

Insights About Search

SIGN IN
Forgot username or password?

The failure to manage your digital risks is likely to sabotage your digital

Meet - delphi 世界客 使用者 File:C 亞洲走 定居在 美洲原 商朝人 隱私權 gartne G

https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020-2021/

No. 1: Securing your remote workforce

Focus on business requirements and understand how users and groups access data and applications. Now that a few months have passed since the initial remote push, it's time for a needs assessment and review of what has changed to determine if access levels are correct and whether any security measures are actually impeding work.

R

1.

居家辦公對「特權帳號管理」的挑戰

當「系統管理員」在家辦公...

- 如何確保維運可行性，需要時仍能安全且有效率連接設備進行作業? 。

當「維運廠商人員」在家辦公...

- 如何保障維運安全，設備密碼與重要資料仍能防止外流至公司外部?

當「管理/稽核人員」在家辦公...

- 如何掌握維運管理，不在同一辦公室，維運管理與稽核仍全面可控?

當在家辦公使用「家用電腦」...

- 家用電腦可能已中駭客木馬或病毒，維運過程如何確保不波及公司內部?

特權帳號管理- Gartner未來的戰略規劃設想(2022~2025)

Gartner

Critical Capabilities for Privileged Access Management

Published: 4 August 2020

By 2022, 40% of privileged access activity will leverage ZSP through JIT privilege elevation, effectively eliminating standing privileges, up from just 10% today.

By 2025, up to 84% of all organizations will have adopted SaaS-based PAM tools in their PAM practice.

Gartner

Magic Quadrant for Privileged Access Management

Published 4 August 2020

By 2024, 50% of organizations will have implemented a just in time (JIT) privileged access model, which eliminates standing privileges, experiencing 80% fewer privileged breaches than those that don't.

By 2024, 65% of organizations that use privileged task automation features will save 40% on staff costs for IT operations for IaaS and PaaS, and will experience 70% fewer breaches than those that don't.

特權帳號管理的背景知識

台灣資安館T23

大會展場S21

智弘軟體科技

State-of-the-art PAM Product

特權帳號管理的背景知識- 風險在那裏?

維運人員

合作廠商

作業系統

資料庫

檔案伺服器

網路設備

資安設備

駭客

虛擬化平台

中大型主機

應用系統

其它設備

特權帳號管理的背景知識- 頭痛的問題

內部員工　駐外員工　臨時雇員　合作伙伴　外包廠商　離職人員　駭客

- 密碼規則不同且越來越複雜，記憶或輸入都是問題。
- 人事異動時，密碼難以回收或忘了回收。
- 太多人共同擁有特權帳號，查問題時無法確認使用者是誰?
- 每年花很大力氣作帳號清查，但是否真的能確保沒有幽靈帳號?
- 數量眾多的電腦/筆電的administrator要如何管理?
- 法規要求要如何達成? – GDPR：72小時通報；ISO ：說、寫、作一致。
- APT攻擊/資安事件不斷爆發，身為負責部門的我該如何因應?
- 居家辦公，如何有效且安全地進行特權帳號管理?

服務網站　作業系統　資料庫　網路設備　虛擬化　資安設備　外點/分公司系統

特權帳號管理的背景知識- 現況我在那裏？

成熟度

完全不管/各自保管
寫在紙上/固定幾組
石器時代

記在Excel/文字檔
共享負責部門人員
無法歸責

鎖保險箱/兩人分持
人工流程嚴格控管
難以落實

自動化特權管理
電子化生命周期管理
自然符規

演進

ANCHOR特權帳號管理平台

台灣資安館T23

大會展場S21

智弘軟體科技

State-of-the-art PAM Product

ANCHOR- 國內自主研發的特權帳號管理系統

State-of-the-art PAM Product

資通安全自主產品在臺附加價值率認定表

公司名稱：智弘軟體科技股份有限公司	
產品類型： 資通安全軟體產品	2.1 ● 能量登錄項目：：3.2.5 人員身份與存取控制產品 ● 產品名稱：ANCHOR 特權帳號管理與稽核平台

行政院資安處認證國產軟體

項次	品名	型號
1	ANCHOR 特權帳號管理平台	APETP-P-10100
2	同時上線人數模組	ANCHORP-CU-0005
3	被管理端設備側錄授權模組	ANCHORP-H-0025

計算 側錄設備數 與 同時上線人數，節約導入成本

國內自主研發
特權帳號管理系統

課程項目	課程項目	課程時數
		小時
02		小時
		小時
04		小時
05	維運相關支援文件使用說明	1 小時

台灣資安館T23
大會展場S21

國內技術支援/課程

國內廣泛採用並行銷世界(如美、澳、中、港...)

- 個人帳號維護：減少個人帳號逐一維護成本
- 輕鬆訪問設備：HTML5 Ready 一鍵部署/零部署
- 工具特性保留：保留功能鍵/熱鍵 Copy/Paste...等
- 批次設備指令：多部同類型設備執行相同指令
- 多層備份/移轉：系統資料與錄影自動備份移轉
- 緊急申請審核：審核人員不打開電腦也能授權
- 定義式稽核流程：設備訪問結束主動提醒關卡執行
- 線上工作報告：線上寫工作報告保留修改歷程
- 可訂閱式報表：訂閱日/週/月周期自動寄送報表
- 支援個人語系：支持繁中、簡中、英文、日文

十大特色，符合國內國情與使用習慣

ANCHOR代表客戶

State-of-the-art PAM Product

政府

- 行政院 主計處、人事行政總處。
- 衛生福利部 本部、健保署。
- 勞動部 勞保局、勞發署。
- 內政部 營建署、移民署、墾管處。
- 經濟部 水利署。
- 交通部 台鐵局、高公局、航港局。
- 銓敘部。
- 退輔會、農委會、林務局。
- 新北市 稅捐稽徵處。

金融業

- 合作金庫銀行(台灣、海外)。
- 國泰世華銀行。
- 陽信商業銀行。
- 三信商業銀行。
- 玉山綜合證券公司。
- 台灣產物保險公司。
- 華南產物保險公司。
- 和泰產物保險公司。
- 宏泰人壽保險公司
- 兆豐銀行(@海外)。
- 玉山銀行(@海外)。
- 台灣中小企銀 (@海外)。
- 合作金庫銀行(@海外)。

醫院/財團法人

- 署立台北醫院。
- 綠色基金會。

電信/製造

- 亞太電信公司。
- 啟碁科技公司。
- 臺灣菸酒公司。
- 富台工程公司。
- 日商中鹿營造公司。

ANCHOR的十大特色

緊急連線需求

用OTP緊急審核，不須網路連線或打開電腦審核

終端連線設備

任意HTML5終端，連線授控設備，零部署

駭客入侵防禦

駭客透過特權帳號進行入侵，進行四部曲防禦

批次設備指令

多部同類型設備，執行一系統相同指令，節約處理時效

安全性/可用性

導入後，不用擔心設備密碼保存安全性或服務可用性

指令即時阻斷

未授權Telnet/SSH指令即時阻斷 ，可以防患未然

生命周期管理

申請審核、代登入、監控、撥放，含工作報告與稽核流程

A2A不改程式

應用系統使用密碼之特權帳號，不須修改應用系統程式

端點管理監控

在家辦公端點軌跡管理，遠端即時監控與操作軌跡稽核

輕量化部署

上述全部功能，僅須部署一部主機，達最低資源需求

ANCHOR模組結構圖

State-of-the-art PAM Product

Privileged Security Goals

- 帳號生命周期
- 駭客入侵防禦
- 風險威脅警示

Definable Role Functions

雙重認證	存取管制	連線申請	連線審核
連線開通	單一簽入	軌跡紀錄	即時監控
連線回收	密碼變更	工作報告	稽核流程
密碼存取	帳號清查	密碼檢查	報表訂閱

Shared Infra-mods

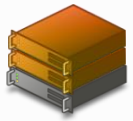
- OTP
- SSO
- Credential Vault
- SR
- A2A
- AM
- IDM
- BPM
- VDI

Adapter Framework


作業系統


資料庫


虛擬化


網路/資安

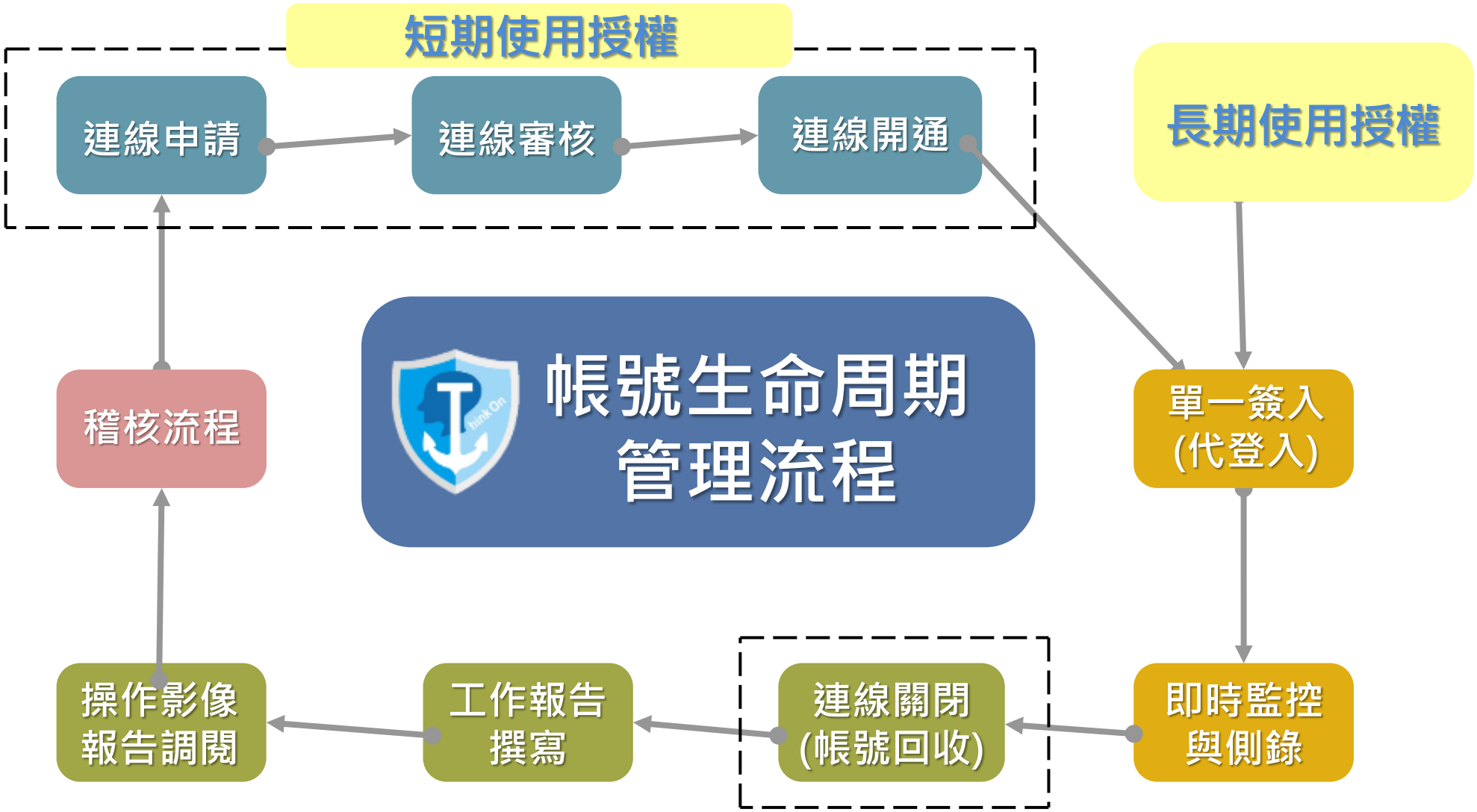

雲端服務


郵件


AD/目錄


SIEM

帳號生命周期管理



外包廠商作業情境展示：「https://www.globalwisdom.com.tw/參考情境展示.html」

駭客APT入侵防禦

中招

- 開源連線工具管控
- 桌面連線(VDI)

竊取密碼

- 集中進行密碼保管
- 自動定期密碼檢查
- 指定使用者來源IP

橫向移動

- 代登入/帳號密碼不落地
- 連線結束立即變更密碼

偷建帳號

- 自動排程帳號盤點

駭客入侵防禦情境展示：「https://www.globalwisdom.com.tw/參考情境展示.html」

風險威脅警示

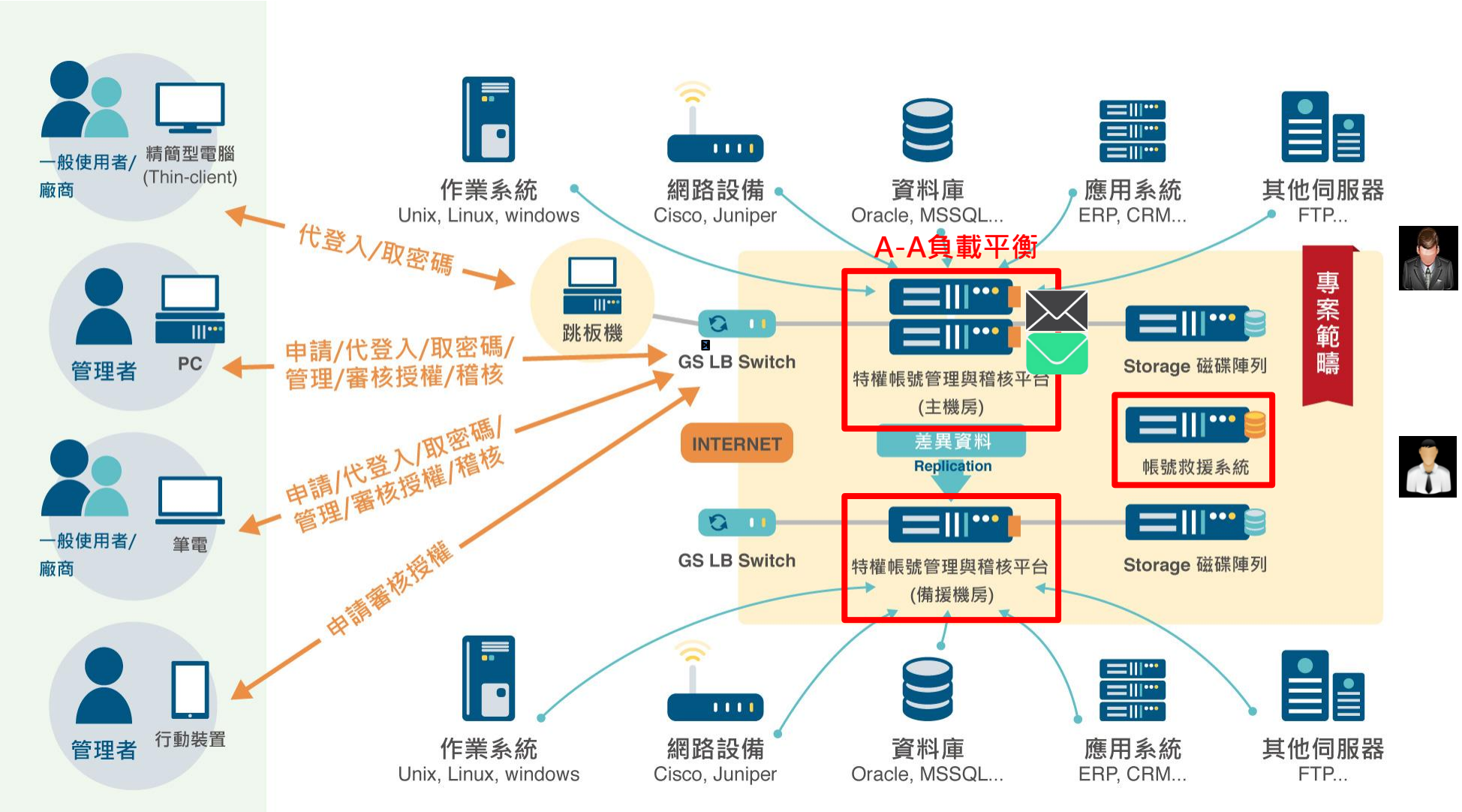
異常帳號警示

密碼異常警示

登入失敗警示

違規指令警示

ANCHOR架構與可用性



Design for User Experience-方便性設計

個人帳號維護

減少個人帳號
逐一維護成本

輕鬆訪問設備

HTML5 Ready
一鍵部署/零部署

工具特性保留

保留功能鍵/熱鍵
Copy/Paste…等

批次設備指令

多部同類型設備
執行相同指令

多層備份/移轉

系統資料與錄影
自動備份移轉

緊急申請審核

審核人員不打開
電腦也能授權

定義式稽核流程

設備訪問結束主
動提醒關卡執行

線上工作報告

線上寫工作報告
保留修改歷程

可訂閱式報表

訂閱日/週/月周期
自動寄送報表

支援個人語系

支持繁中、簡中、
英文、日文

特權帳號管理的未來

台灣資安館T23

大會展場S21

智弘軟體科技

State-of-the-art PAM Product

特權帳號管理的未來

「更安全」的特權帳號管理

- 駭客的挑戰- 80%的駭客入侵透過先竊取特權帳號；安全的規範- 日趨嚴格的資訊安全規範。

「更精確」的特權帳號管理

- JIT(Just-In-Time) Privileged Access Management、ZSP(Zero Standing Privileges)。

「更自動化」的特權帳號管理

- 透過自動化的特權帳號管理，節約時間與管理成本。

謝 謝 您 的 參 與 ！

Thank You！

台灣資安館T23

大會展場S21

智弘軟體科技

State-of-the-art PAM Product