ManageEngine

PAM360

整合式特權存取管理方案

bluechip infotech

藍籌科技
張慶振
Kerry Chang

Helping your business grow

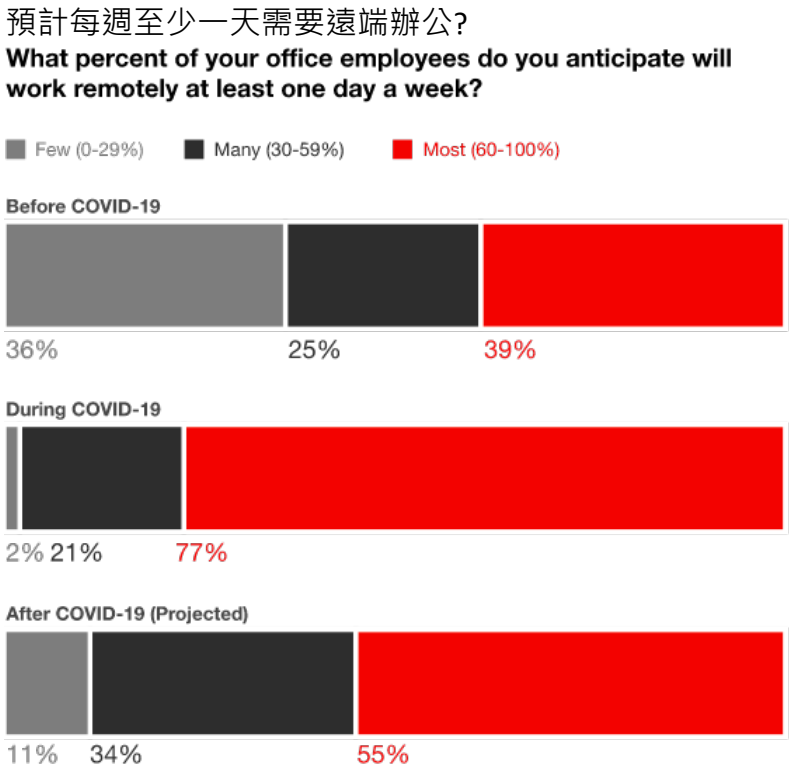
資安趨勢分享

Infosec trends

後疫情時代，遠端辦公需求大增

- 需要遠端辦公人員
  - 疫情期間高達77%
  - 後疫情時期也有55%
- 研究更指出
  - 高達72%希望
    一週兩天能遠端辦公

#以上皆已除去必須遠端作業人員



Source: PwC US Remote Work Survey
June 25, 2020. Base: 120 US executives.

https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html

疫情加速了新時代轉變，帳號管理任務更加艱鉅

- 77% 人員使用未經管理的設備登入公司存取資源。
- 大量新增帳號，提供外部存取，大幅增加監控與管理壓力。
- 相較傳統網路分隔，現今無法控制人員在哪裡工作。

https://www.businesswire.com/news/home/20200603005158/en/Remote-Work-Study-How-Cyber-Habits-at-Home-Threaten-Corporate-Network-Security

遠端辦公需求大增，相對資安風險急遽升高


新聞

【2020十大資安趨勢1：資料外洩】管理不周導致資料外流事件頻傳，企業、雲端業者、政府均應強化管理

2019年的資料外洩事件，有不少是發生在外部廠商，或者是已經下線的系統，徹底盤點和控管，成為企業資安需要加強的面向

讚 6.3 萬 按讚加入iThome粉絲團 讚 165 分享

文/ 周峻佑 | 2020-01-09 發表


新聞

國內人力銀行傳有592萬筆求職個資外洩，104公告說明，遭公布35筆是2013年舊資料

104資訊科技於今日10月4日（週日）接近深夜時分正式在其官方網站發出關於遭駭一事的聲明，指出駭客所公開的35筆資料，都是2013年的舊資料。

讚 6.3 萬 按讚加入iThome粉絲團 讚 1,020 分享


新聞

Amazon用戶資料再遭員工外洩

Amazon近日通知某些用戶其個資被自家員工洩露出去，涉案者已遭開除

讚 6.3 萬 按讚加入iThome粉絲團 讚 127 分享

文/ 林妍溱 | 2020-10-28 發表


新聞

臺灣戶政資料傳出外洩疑雲，行政院資安處揭露更多細節，強調與戶政單位無關

之前有資安公司宣稱，臺灣2千多萬筆戶政資料在暗網流傳。對此，行政院資通安全處接連發出兩次公告，並指出他們的發現，表示這些資料與臺灣戶政資料無關

讚 6.3 萬 按讚加入iThome粉絲團 讚 176 分享

文/ 周峻佑 | 2020-06-01 發表


新聞

Zoom又傳資料外洩，53萬筆帳密流入暗網

這批Zoom用戶個資包含電子郵件、密碼、Meeting URL及主持人密鑰等，受害者遍及摩根大通、花旗銀行及學校等機構

讚 6.3 萬 按讚加入iThome粉絲團 讚 1,485 分享

文/ 林妍溱 | 2020-04-14 發表


新聞

全球最大眼鏡集團Luxottica外洩病患資料，面臨集體訴訟

Luxottica提交給美國衛生及公共服務部的資料顯示，此一資料外洩事件總計影響了82萬多名病患

讚 6.3 萬 按讚加入iThome粉絲團 讚 15 分享

文/ 陳曉莉 | 2020-11-13 發表


新聞

萬豪國際再爆資料外洩，520萬人受害

全球最大飯店集團萬豪國際在今年2月底發現員工帳密被駭，導致顧客管理系統遭非法存取，500多萬筆客戶資訊可能因此外洩

讚 6.3 萬 按讚加入iThome粉絲團 讚 273 分享

文/ 林妍溱 | 2020-04-01 發表


新聞

美國大型醫療網路U.S. Fertility遭勒索軟體攻擊，病患資料外洩

U.S. Fertility在今年的9月遭到勒索軟體攻擊，導致為數不詳的病患個資外流

讚 6.3 萬 按讚加入iThome粉絲團 讚 48 分享

文/ 陳曉莉 | 2020-11-27 發表

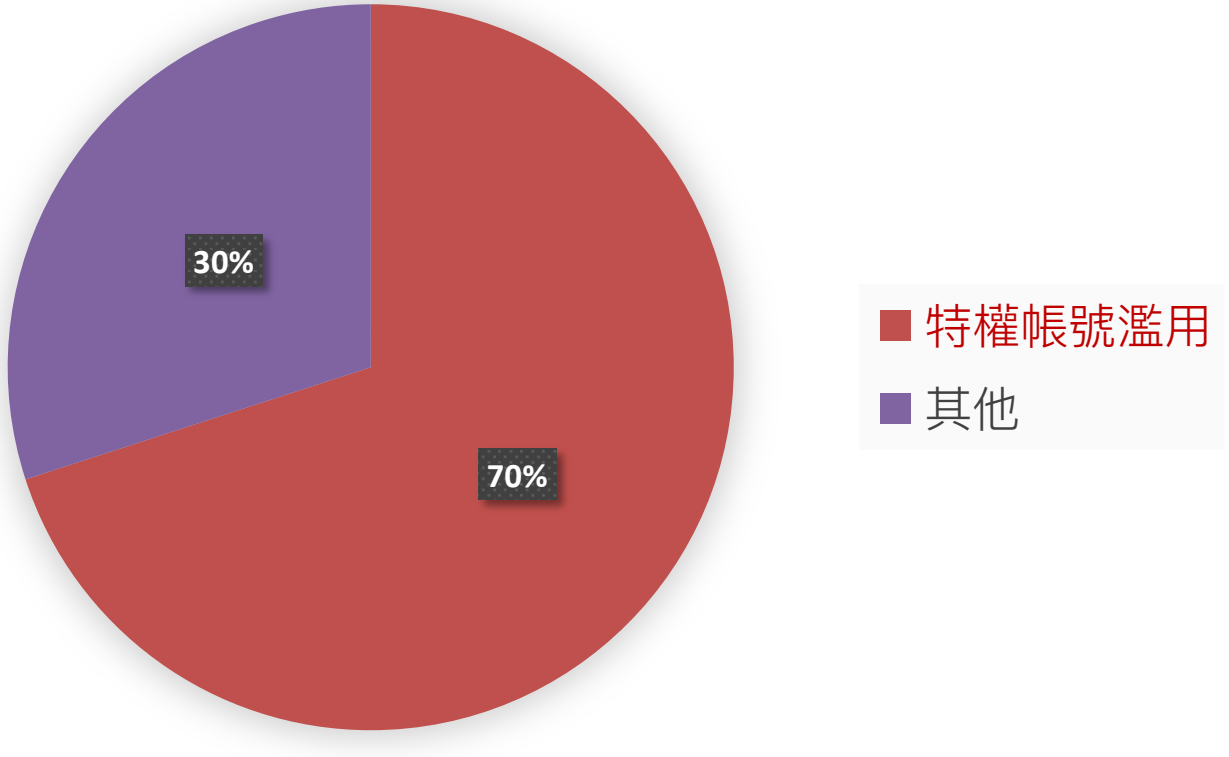

新聞

又傳出335萬求職個資被出售於暗網論壇，1111人力銀行表示已是9年前舊案

繼昨日104人力銀行傳出求職個資在暗網論壇出售，今日（10月5日）同個論壇、同個發文者，又聲稱將出售1111人力銀行大量用戶個資。對此，1111表示經比對釐清後，販售內容是2011年舊資料。

讚 6.3 萬 按讚加入iThome粉絲團 讚 396 分享

資料外洩事件

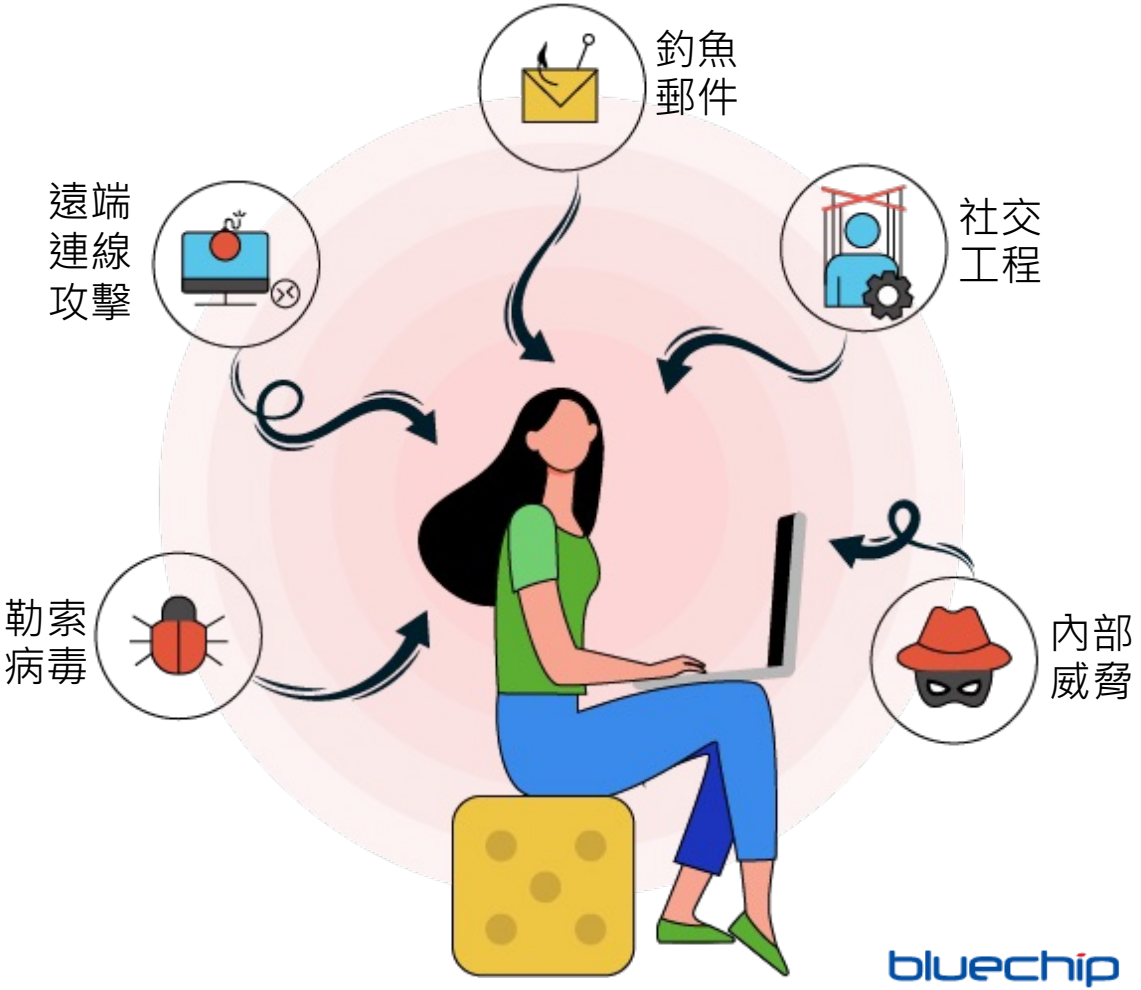


Source: The Data Breach Investigations Report 2021

什麼是特權帳號濫用？

What is Privilege abuse?

無論內部/外部
未經管理的
常設特權帳號
是攻擊者的最愛



權限越大，風險越大

從未監控或定期審視

可透過多台設備，永久性存取機敏資料

網路內無法檢測到的橫向存取行為

被惡意內部人員或前僱員所利用


PAM360能幫助您什麼？
Privileged Access Management 360 degree solution

核心功能

特權帳號掃描、
納管與存取管理

具安全性的遠端存取

SSH 金鑰與憑證
生命週期管理

特權連線存取管理

特權使用者行為分析、
稽核與合規報表
(須整合Log360)

有效強化特權帳號存取安全

- 即時權限提升
  - 在有限的時間裡提升權限，過期即收回

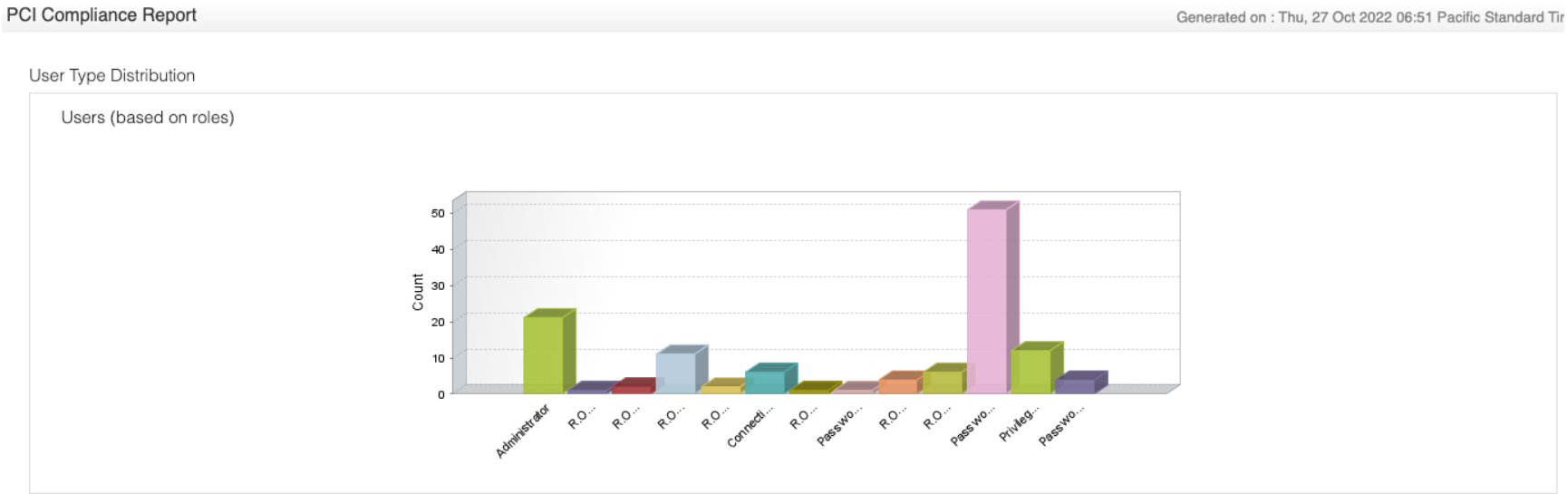
- 具安全性的遠端存取
  - 一鍵登入機敏系統，過程中加密與錄影

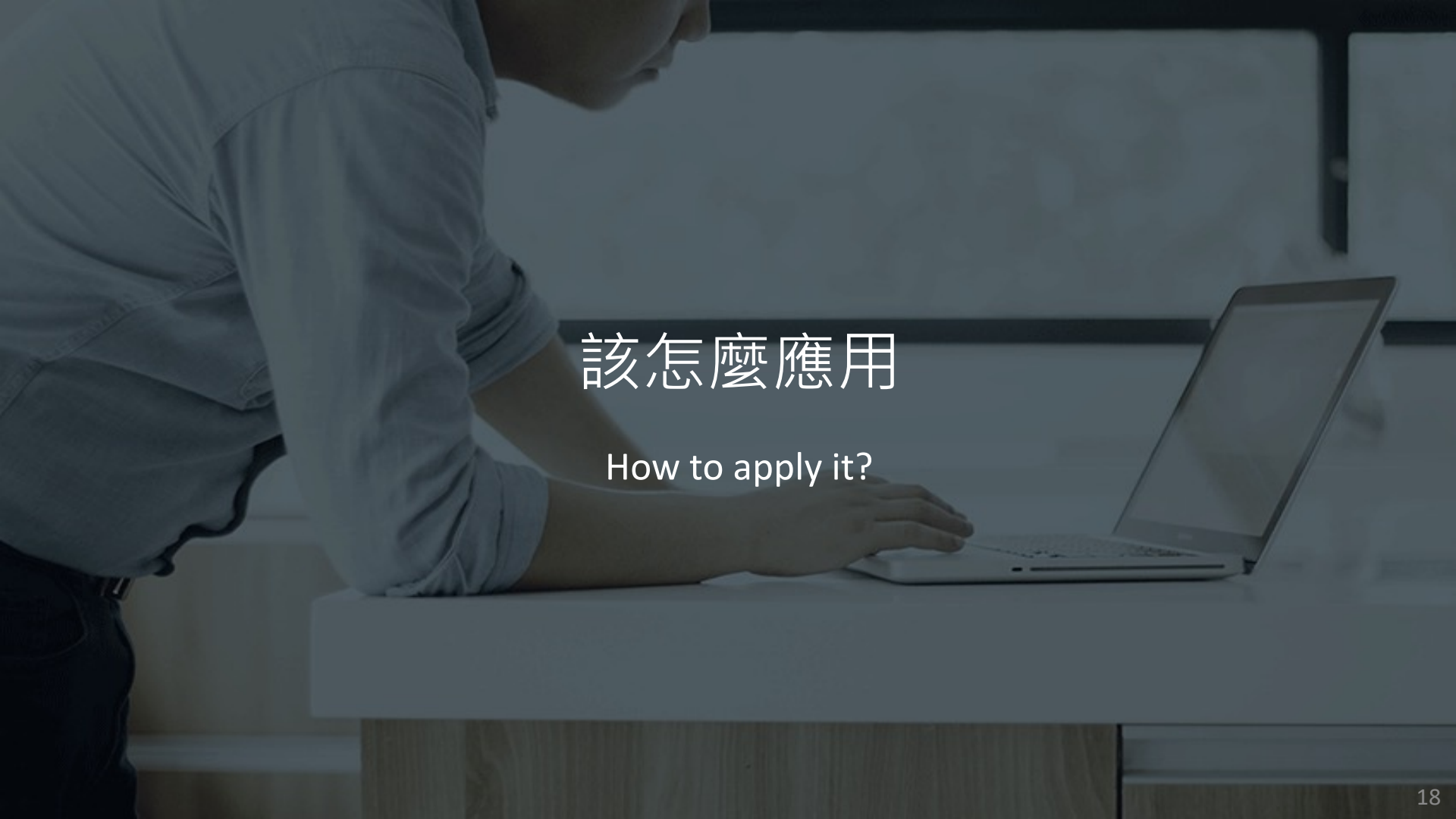
- 智慧型存取控制工作流程
  - 角色等級的權限授予與智慧工作流程

- 特權使用者行為分析 (須整合Log360)
  - 透過機械學習偵測異常行為並即時中斷

輕鬆滿足特權帳號管理的合規需求

- 依法令遵循，產出相關報表
  - PCI DSS / NERC-CIP / ISO/IEC 27001 / GDPR





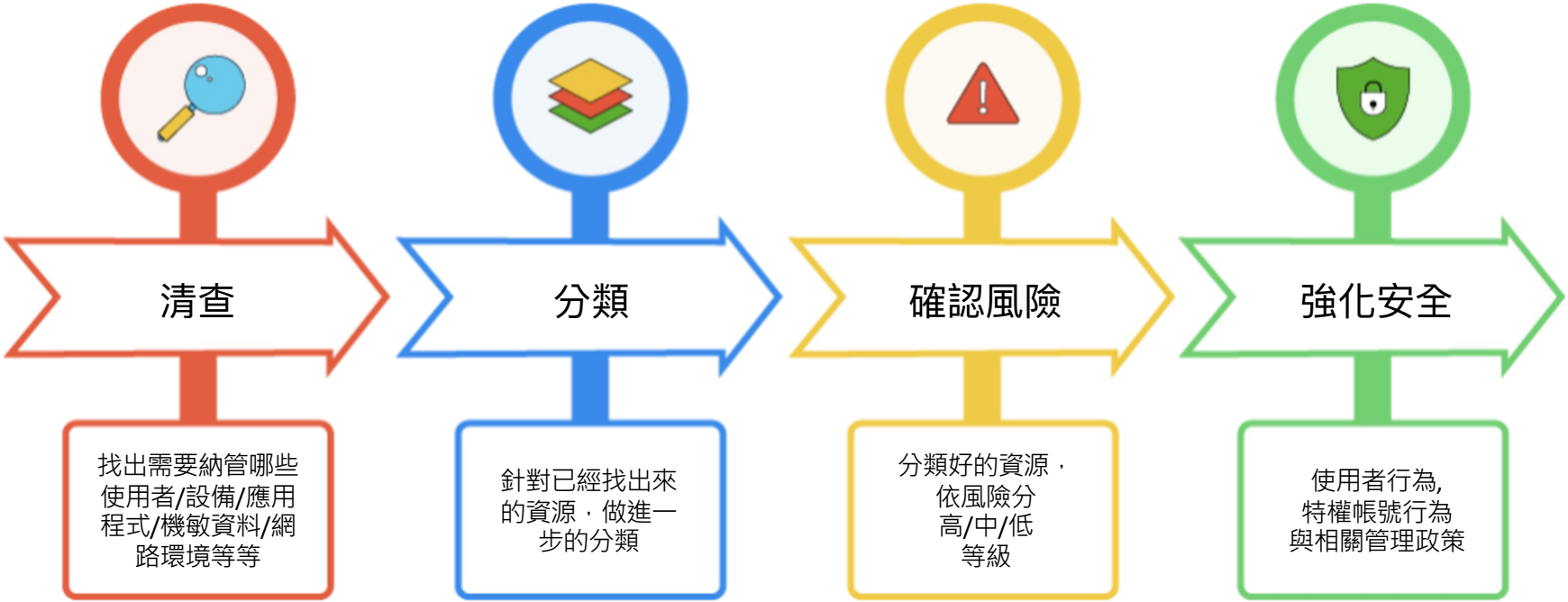
該怎麼應用

How to apply it?

協助您達到

1.最低需求授權

最低需求權限存取(Just-in-time privileges)



六個步驟達到最低需求權限管理

- 清查：檢視所有特權帳戶與權限
- 限縮：盡可能分配最低權限
- 授權：即時授與權限提升
- 釋權：刪除沒有根據且多餘的權限
- 清除：透過API取代寫死在AP上的密碼
- 控管：有效控管特權執行應用程式與指令

資源清查面向

協助您達到

2.零信任

透過零信任，增強資訊安全性

授權之前，先驗證
是否為合法使用者

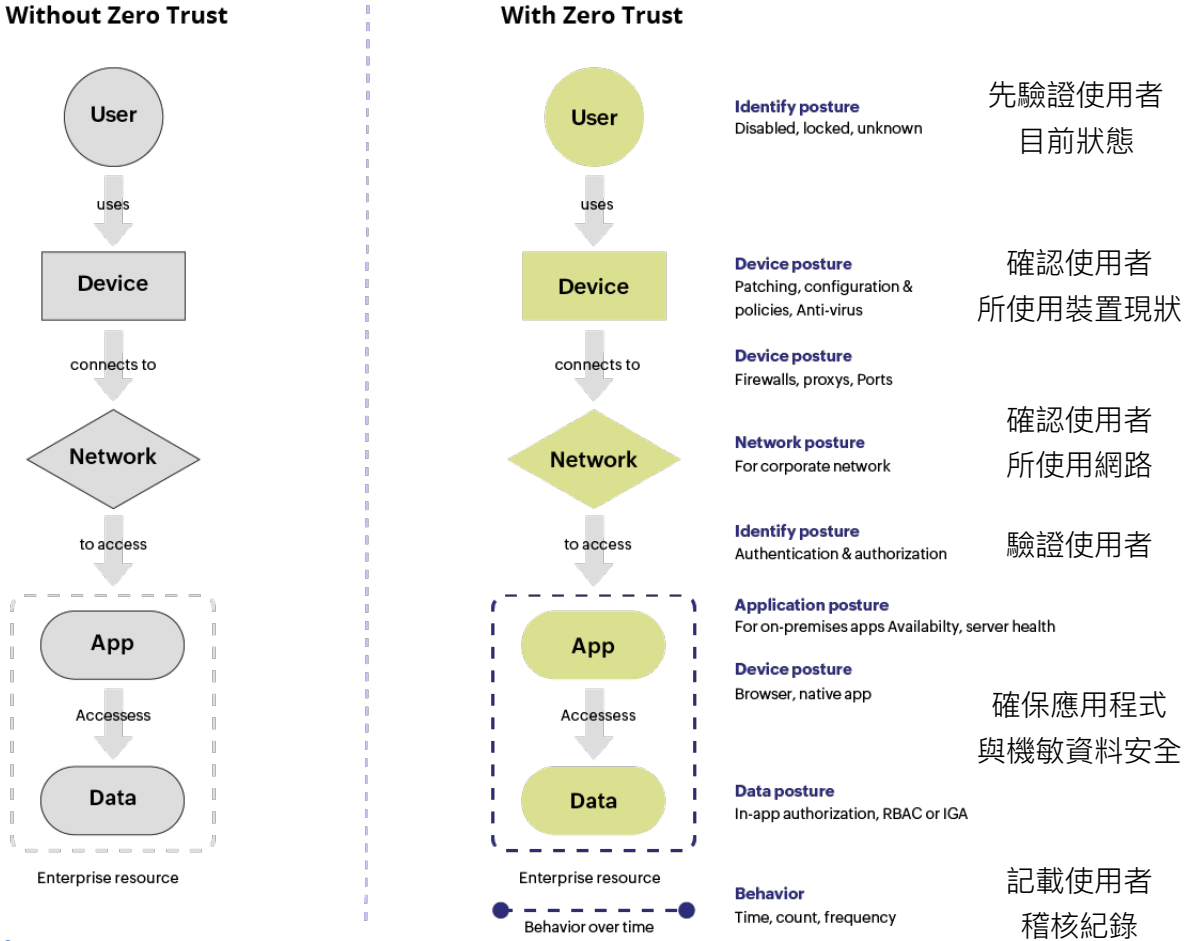
利用風險與信任度
評比

根據不同資源，
授予應得的
存取權限

根據不同的使用者
與管理行為放行

導入多因素驗證

導入後


Without Zero Trust
User
uses
Device
connects to
Network
to access
App
Accessess
Data
Enterprise resource
With Zero Trust
User
uses
Device
connects to
Network
to access
App
Accessess
Data
Enterprise resource
Behavior over time
Identify posture
Disabled, locked, unknown
先驗證使用者
目前狀態
Device posture
Patching, configuration & policies, Anti-virus
確認使用者
所使用裝置現狀
Device posture
Firewalls, proxys, Ports
Network posture
For corporate network
確認使用者
所使用網路
Identify posture
Authentication & authorization
驗證使用者
Application posture
For on-premises apps Availabilty, server health
Device posture
Browser, native app
確保應用程式
與機敏資料安全
Data posture
In-app authorization, RBAC or IGA
Behavior
Time, count, frequency
記載使用者
稽核紀錄

六個步驟達到零信任

- 清查：找出並清除常駐特權帳號
- 審查：定期審查權限並封阻弱項
- 更換：定期更換密碼/金鑰/憑證
- 強化：管理者應該依不同角色/時間點/需求來授予使用者存取權限
- 稽核：針對特權管理錄影與軌跡留存
- 多因素驗證：強化登入安全性

使用情境

Scenarios

情境一：放長假中的網路工程師

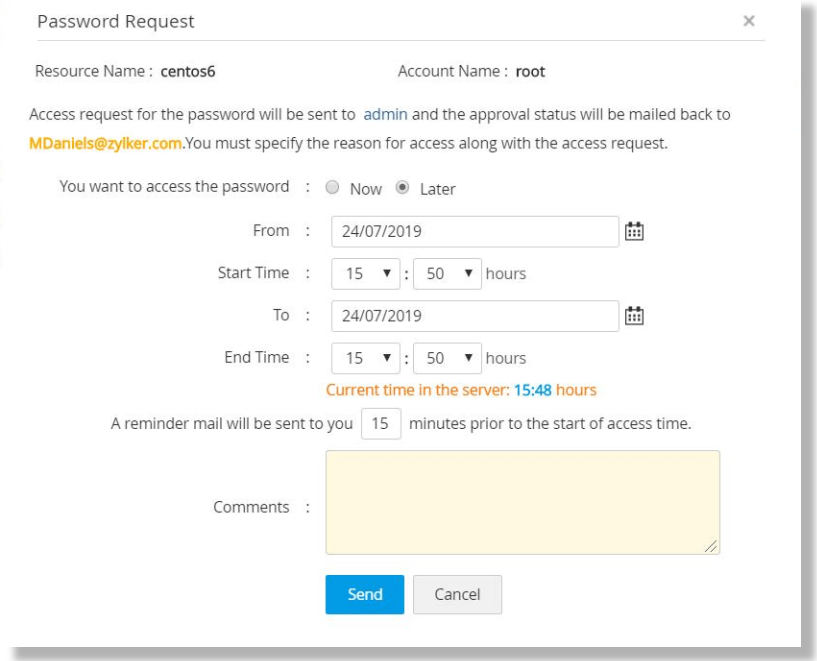
- 在墾丁大街吹著海風，吃著火鍋唱著歌，突然一通電話打來！
- 需要臨時連回公司，調整防火牆上的規則，提供系統工程師臨時上系統的需求
- 只好跟女朋友說聲：抱歉!
- 回到飯店，使用自己的筆電，以及飯店的WIFI網路。

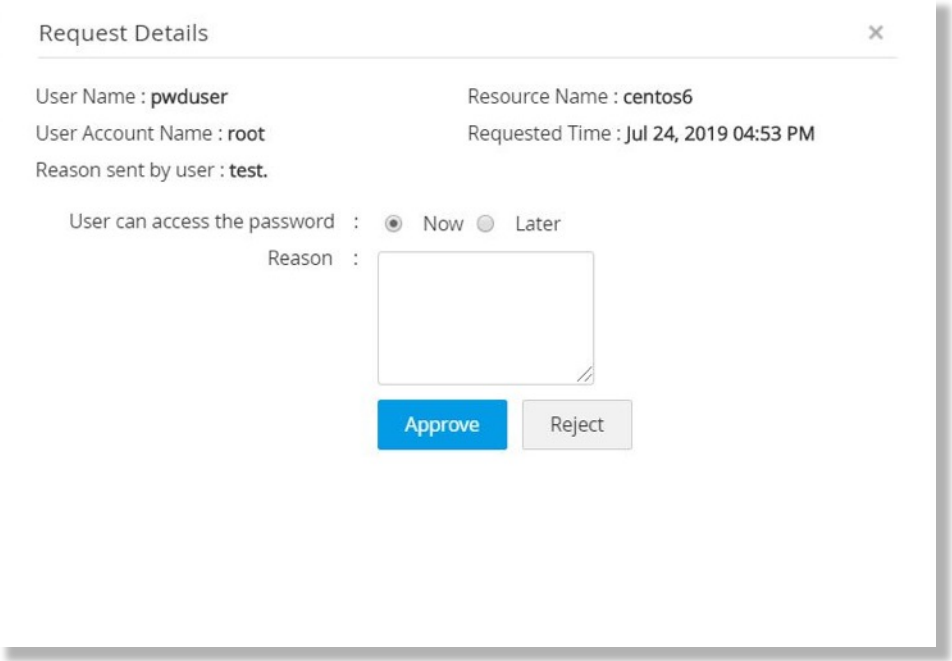
導入PAM360後，增強安全性流程

- 在登入頁面，通過MFA的即時身份認證
- 向經理提出防火牆存取的請求，且得到批准
- 經理授予了30分鐘的存取權限，時間到立即撤銷阻斷
- 透過PAM360遠端控制，並錄影留存

即時授權

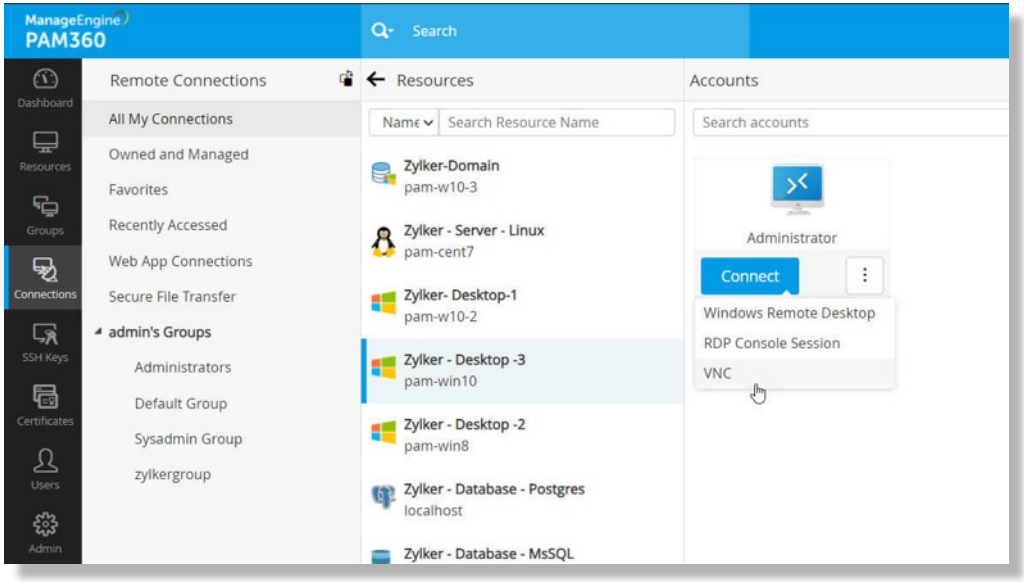
- 針對特定機敏設備，即時授予，有限的時間內的較高權限





遠端控制並錄影

- 直接透過PAM360達到
  - RDP/VNC
  - SSH/Telnet
  - SQL
- 可開放雙向檔案傳輸
- 在Windows平台可支援RemoteApp.




為何選擇PAM360
Why PAM360?

連續三屆！Gartner 特權存取管理魔術象限

Figure 1. Magic Quadrant for Privileged Access Management

Source: Gartner (August 2020)

2020 PAM

Figure 1: Magic Quadrant for Privileged Access Management

Source: Gartner (July 2022)

2022 PAM

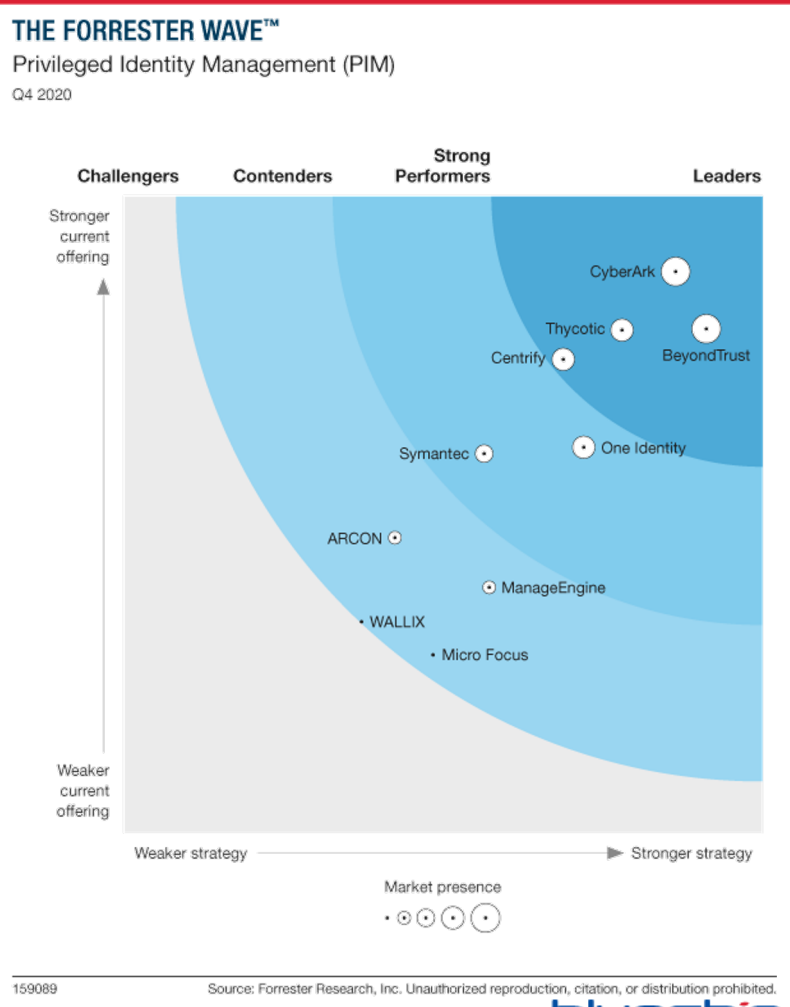
入圍 The Forrester Wave™: PIM, Q4 2020

PAM360 提供了整合統一性且集大成的管理介面，快速簡易的部署，並能有效整合多元系統和應用程式。

客戶對於 ManageEngine 提供優質使用者體驗，給予高度肯定與滿意度。

ManageEngine也因易於使用，具有專業迅速的售後服務品質，而建立聲譽 。

The Forrester Wave™: Privileged Identity Management (PIM), Q4 2020



選擇PAM360

- 簡單安裝，簡單管理
- 功能涵蓋所有特權存取管理需求
- 極具競爭力的價格
  - 只計費管理者(Administrators)數量與SSL金鑰數量
  - 不計算遠端使用者與資源

為你呈現

ManageEngine

Introduing **Manage**Engine

全方位IT管理解決方案

- IT多維方案，整合管理
  - 提供 90 多種，價格合理，滿足您的所有 IT 管理需求之產品。
- IT簡單易用，快速上手
  - 易於下載、安裝、設定和部署，無需第三方支援服務或幫助。
- IT計費親民，價格實惠
  - 更高的價格並不始終意味著更好的產品

180,000+
家全球企業

9/10
財富 100 強公司

3,000,000+
管理者

..信任 ManageEngine 來管理其 IT。

ManageEngine 主打星

基礎架構管理

基礎架構監控管理整合方案

OpManager Plus

AD稽核管理整合方案

AD360

IT治理

ServiceDesk Plus

資訊安全

整合式日誌管理SIEM

Log360

特權管理

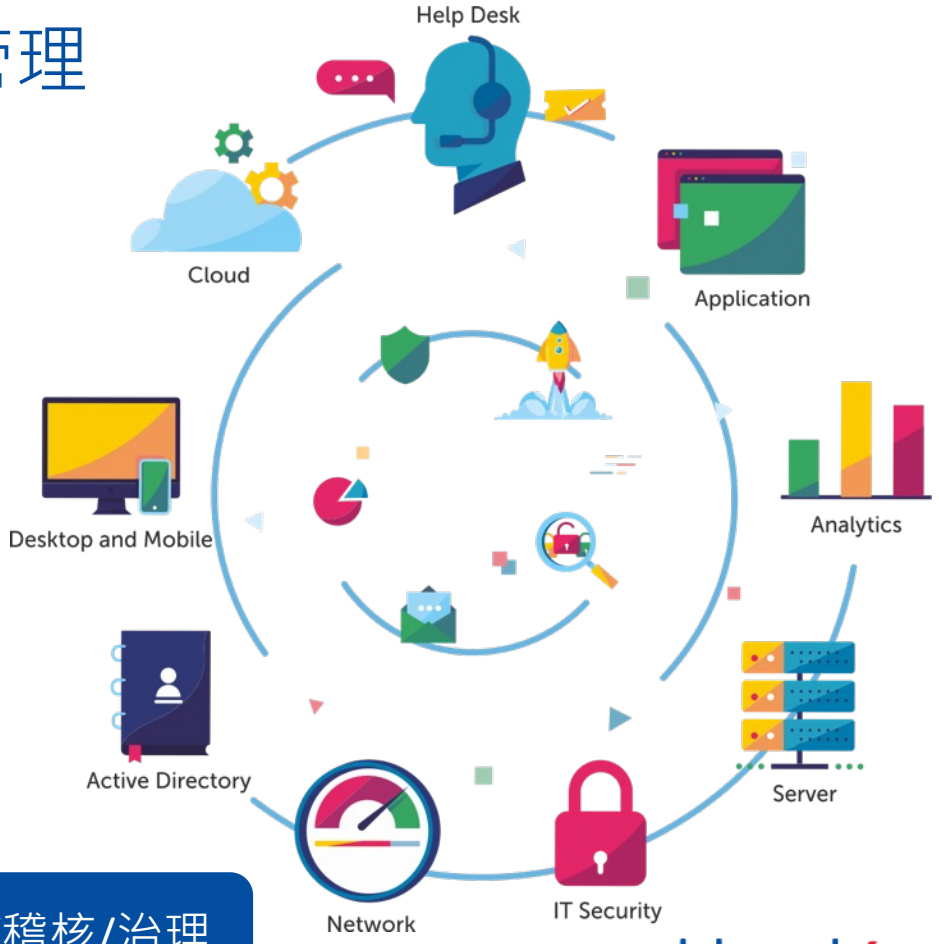
PAM360

端點管理

Endpoint Central

ManageEngine 涵蓋各項管理

- 資訊安全
  - SIEM
  - 特權管理
  - 檔案管理
- IT治理
  - ITIL 4
- AD管理
- IT監控
  - Infra
  - App
- 端點管理
- 雲端管理



ME三支箭: 監控/稽核/治理

20 YEARS 2020

Celebrating 20 Years with Bluechip

PLATINUM SPONSORS

acer CyberPower LogMeIn SOPHOS

GOLD SPONSORS

EATON hp

bluechip 與您的企業一起成長

- 總部位於澳洲雪梨，與其他據點
  - 墨爾本
  - 布里斯本
  - 阿得雷德
  - 伯斯
  - 台北
- 超過150名員工，提供您最佳服務
- 2020上半年營收突破14億台幣(71M AUD)

THANK YOU

Any Questions?