ManageEngine

ADAudit Plus

稽核視覺化的IT好幫手

bluechip infotech

藍籌科技
張慶振
Kerry Chang

Helping your business grow

原生AD管理就夠了嗎？

Native ADUC is not good enough ?

AD管理是一門藝術

- 您是否遇到這些狀況？
  - Windows 日誌量太多
  - 一份報表需要花很多時間整理
  - 該如何分析這些資料？
  - 不知使用者到底做了些什麼
  - 也無法即時得知環境變化

花費許多心力與成本，卻常常事倍功半

網路攻擊手法日漸複雜

- 從之前的DDoS大量存取阻斷攻擊
  - 某些公司，網站掛掉也無所謂
- 到現在轉由內部攻擊
  - 資料外洩、勒索病毒攻擊
  - 各種公司都遭殃

都與使用者帳戶行為有關

後疫情時期，資料外洩風險急遽升高

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

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

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

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

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

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

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

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

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

IT管理員的責任日漸加重

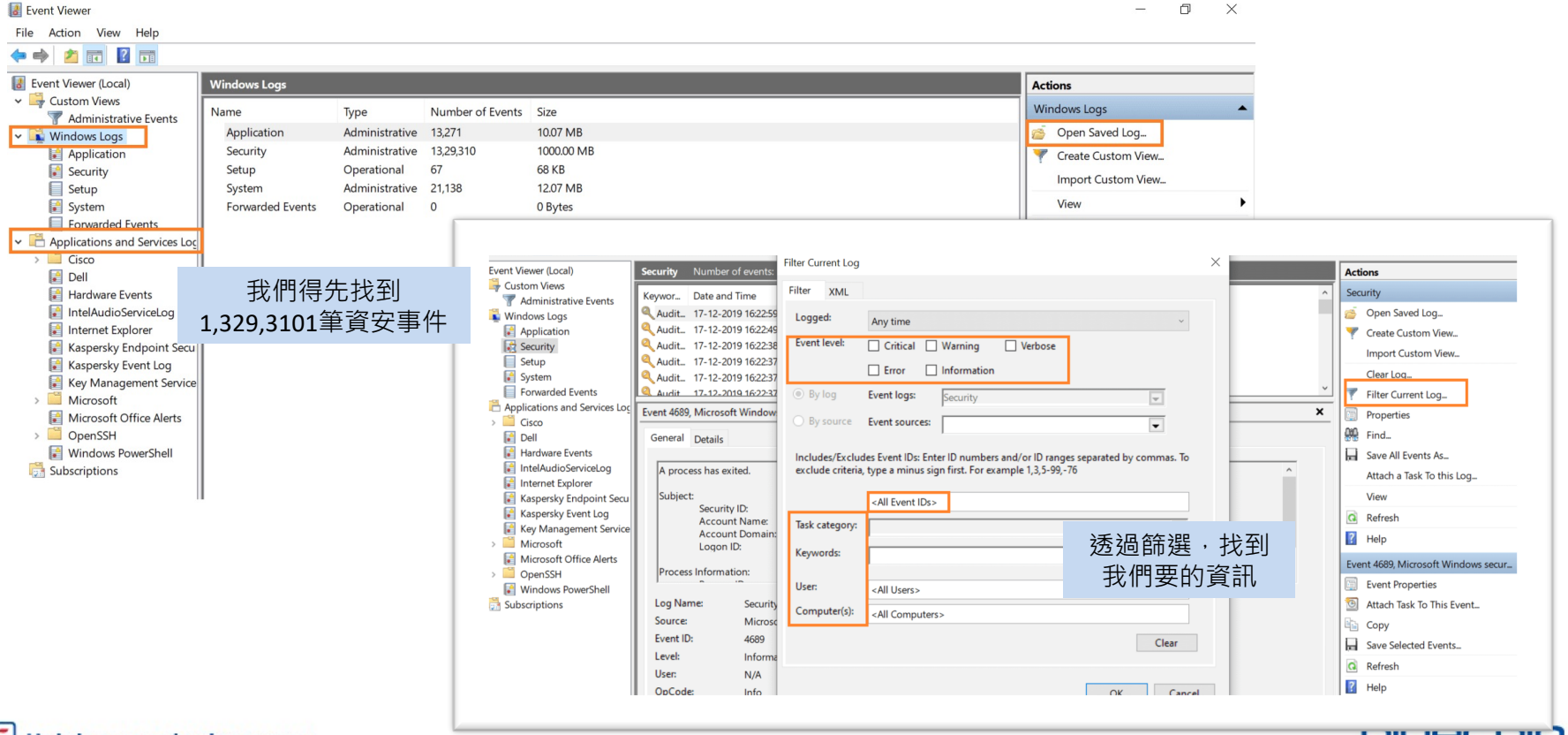
- 主管想要看各種AD的報表
- 稽核單位想要看使用者行為軌跡
- 保護好機敏資料
- 帳號鎖住了，需要幫忙
- 要想辦法符合規範

AD管理員也是需要被服務的

- 你需要的是：
  - 輕鬆寫意的簡單日常維運
  - 即時有效的狀況預防與感知
  - 更有效率的資安事件處理
  - 節省管理成本

功能介紹

如何在傳統內建的AD事件管理介面大海撈針？



使用者導向的IT稽核工具

- 透過行為分析，ADAudit Plus讓你的IT環境安全與合規

AD/Azure AD

File Server

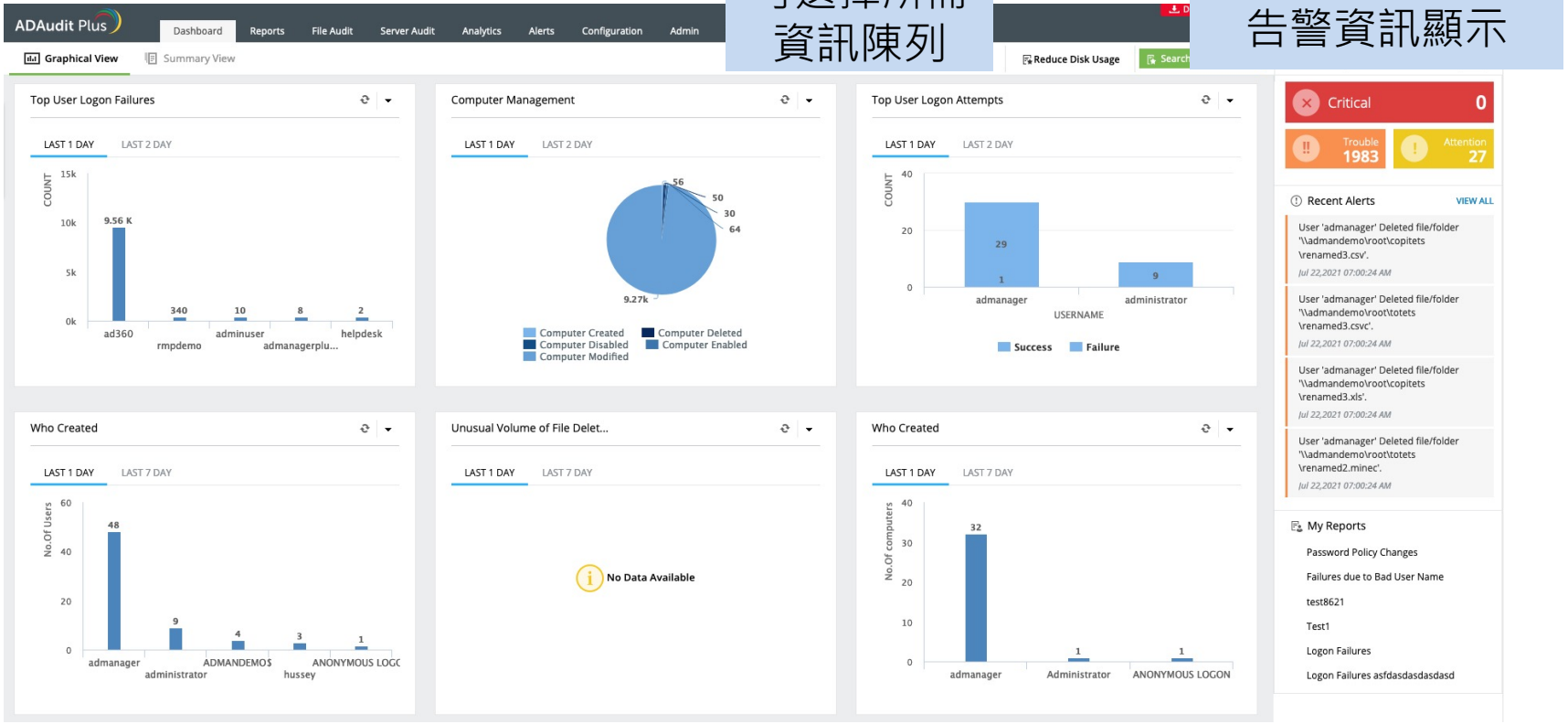
Windows Server

Workstations

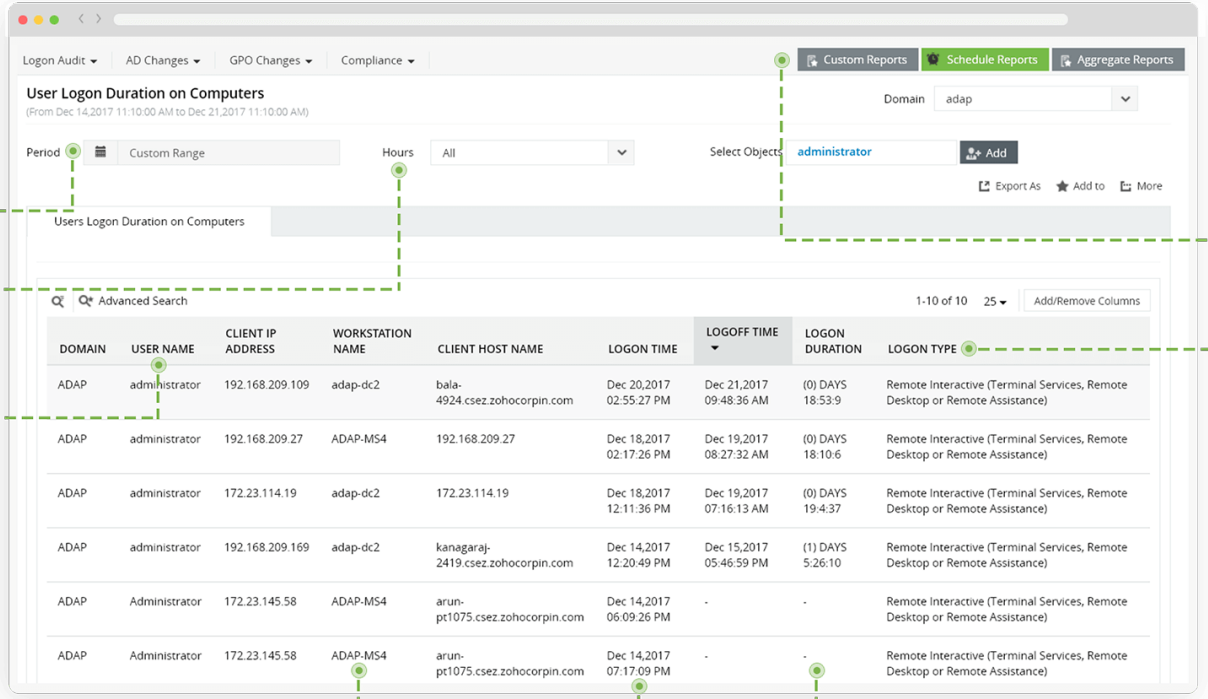
可自定義儀表板

可選擇所需資訊陳列

告警資訊顯示



Windows登入監控



設定時間區間

設定上下班時間

誰登入的？

自訂報表，定期產出

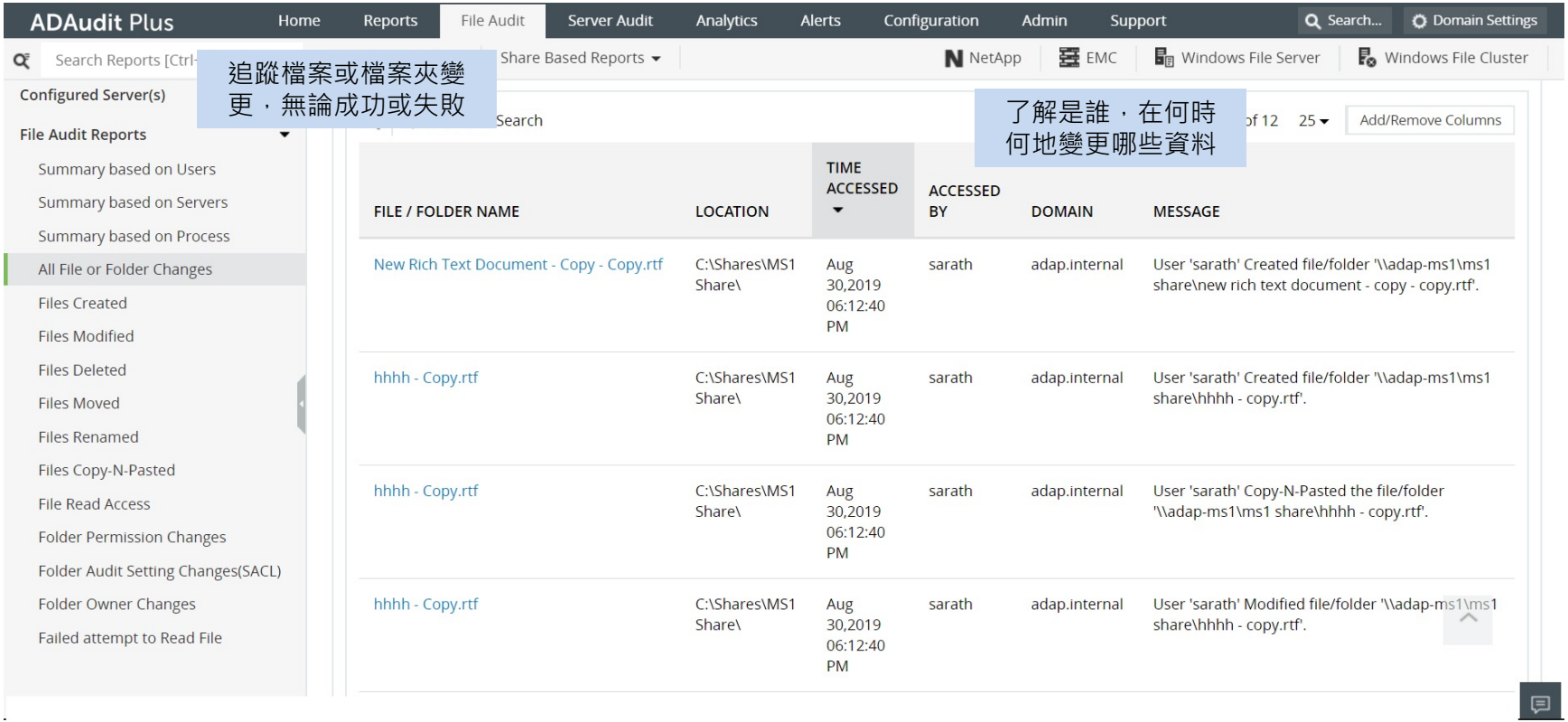
如何登入的？

登入到哪一台電腦？

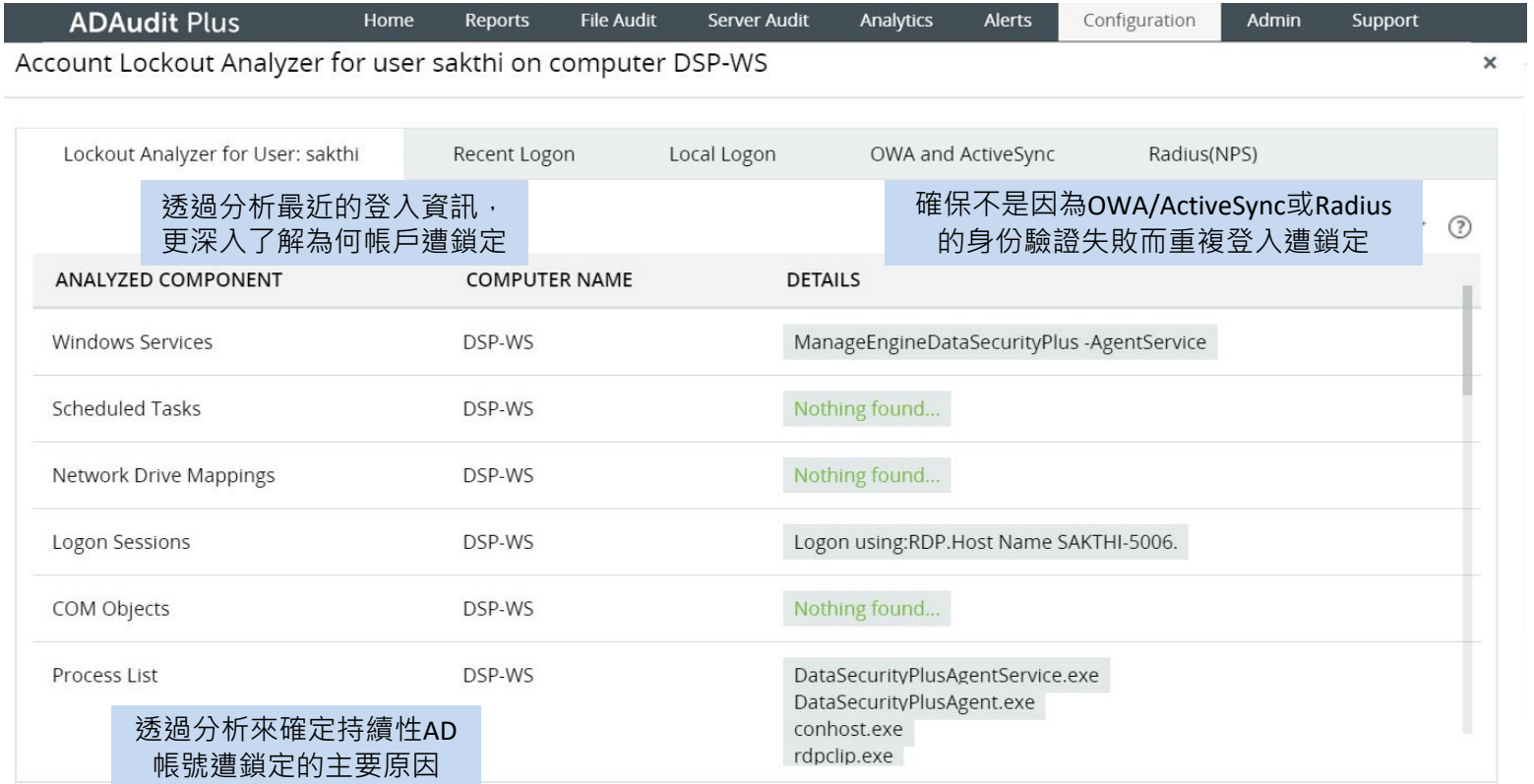
何時登入?

登入了多久？

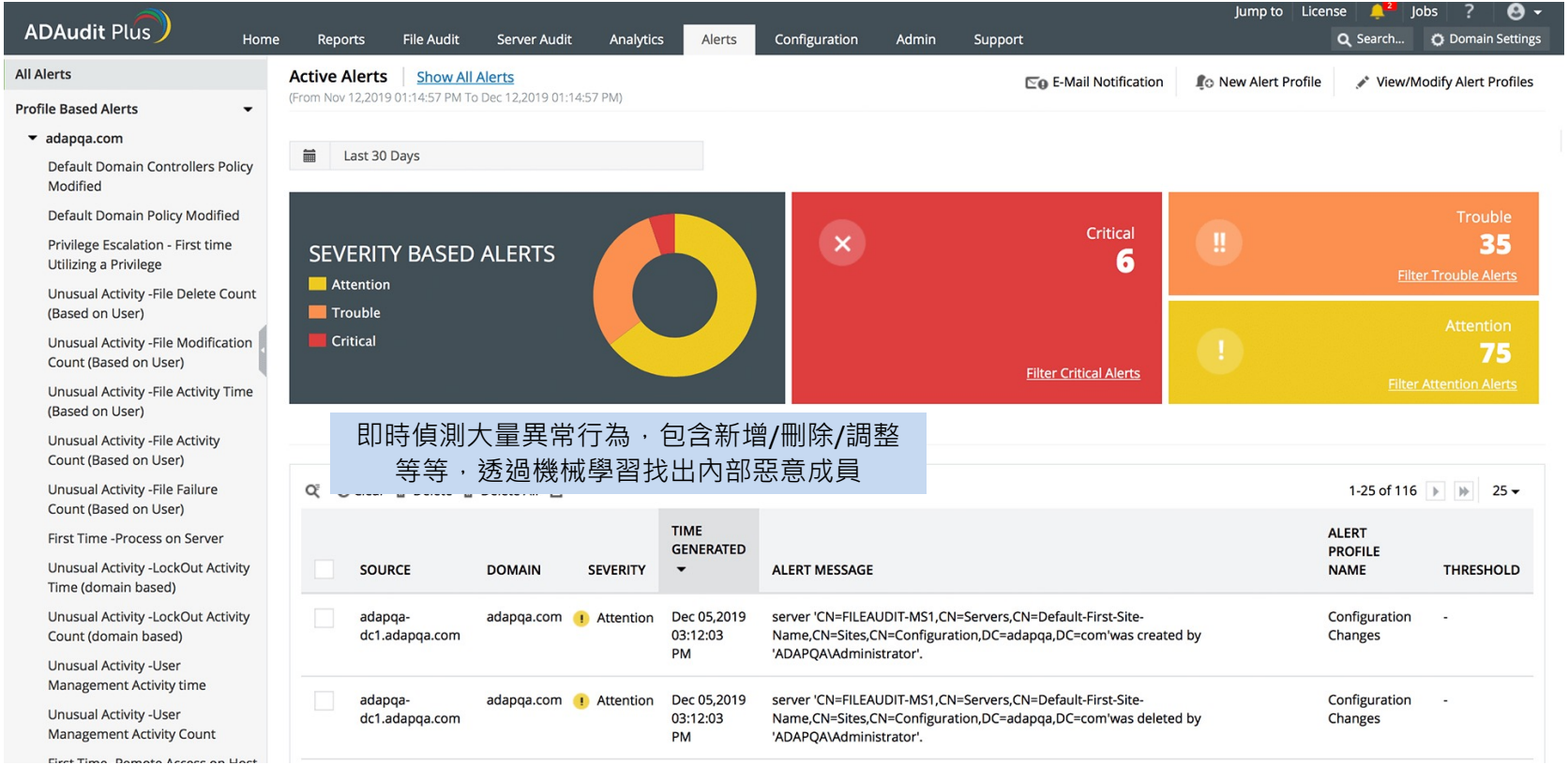
機敏資料變更監控


ADAudit Plus
Home
Reports
File Audit
Server Audit
Analytics
Alerts
Configuration
Admin
Support
Search...
Domain Settings
Search Reports [Ctrl-
Share Based Reports
NetApp
EMC
Windows File Server
Windows File Cluster
追蹤檔案或檔案夾變更，無論成功或失敗
了解是誰，在何時何地變更哪些資料
Configured Server(s)
File Audit Reports
Summary based on Users
Summary based on Servers
Summary based on Process
All File or Folder Changes
Files Created
Files Modified
Files Deleted
Files Moved
Files Renamed
Files Copy-N-Pasted
File Read Access
Folder Permission Changes
Folder Audit Setting Changes(SACL)
Folder Owner Changes
Failed attempt to Read File
Search
of 12
25
Add/Remove Columns
FILE / FOLDER NAME
LOCATION
TIME ACCESSED
ACCESSED BY
DOMAIN
MESSAGE
New Rich Text Document - Copy - Copy.rtf
C:\Shares\MS1 Share\
Aug 30,2019 06:12:40 PM
sarath
adap.internal
User 'sarath' Created file/folder '\\adap-ms1\ms1 share\new rich text document - copy - copy.rtf'.
hhhh - Copy.rtf
C:\Shares\MS1 Share\
Aug 30,2019 06:12:40 PM
sarath
adap.internal
User 'sarath' Created file/folder '\\adap-ms1\ms1 share\hhhh - copy.rtf'.
hhhh - Copy.rtf
C:\Shares\MS1 Share\
Aug 30,2019 06:12:40 PM
sarath
adap.internal
User 'sarath' Copy-N-Pasted the file/folder '\\adap-ms1\ms1 share\hhhh - copy.rtf'.
hhhh - Copy.rtf
C:\Shares\MS1 Share\
Aug 30,2019 06:12:40 PM
sarath
adap.internal
User 'sarath' Modified file/folder '\\adap-ms1\ms1 share\hhhh - copy.rtf'.

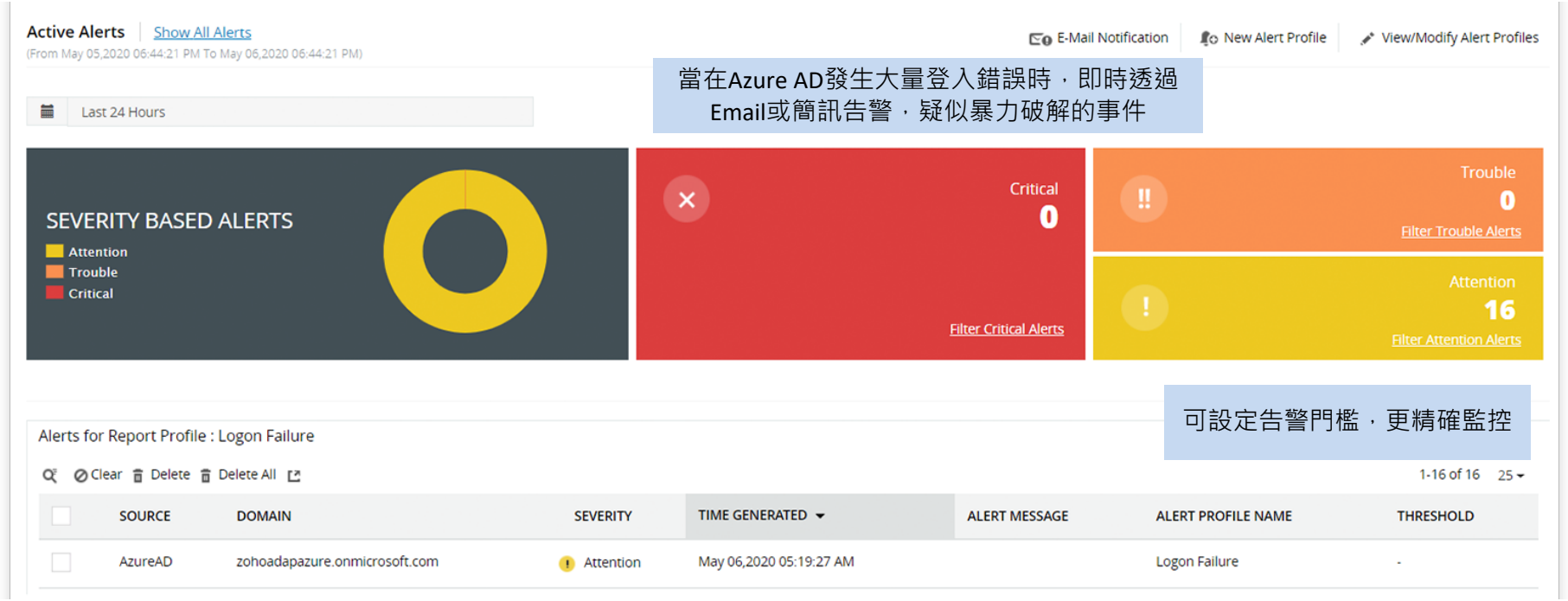
帳號鎖定分析


ADAudit Plus
Home
Reports
File Audit
Server Audit
Analytics
Alerts
Configuration
Admin
Support
Account Lockout Analyzer for user sakthi on computer DSP-WS
Lockout Analyzer for User: sakthi
Recent Logon
Local Logon
OWA and ActiveSync
Radius(NPS)
透過分析最近的登入資訊，
更深入了解為何帳戶遭鎖定
確保不是因為OWA/ActiveSync或Radius
的身份驗證失敗而重複登入遭鎖定
ANALYZED COMPONENT
COMPUTER NAME
DETAILS
Windows Services
DSP-WS
ManageEngineDataSecurityPlus -AgentService
Scheduled Tasks
DSP-WS
Nothing found...
Network Drive Mappings
DSP-WS
Nothing found...
Logon Sessions
DSP-WS
Logon using:RDP.Host Name SAKTHI-5006.
COM Objects
DSP-WS
Nothing found...
Process List
DSP-WS
DataSecurityPlusAgentService.exe
DataSecurityPlusAgent.exe
conhost.exe
rdpclip.exe
透過分析來確定持續性AD
帳號遭鎖定的主要原因

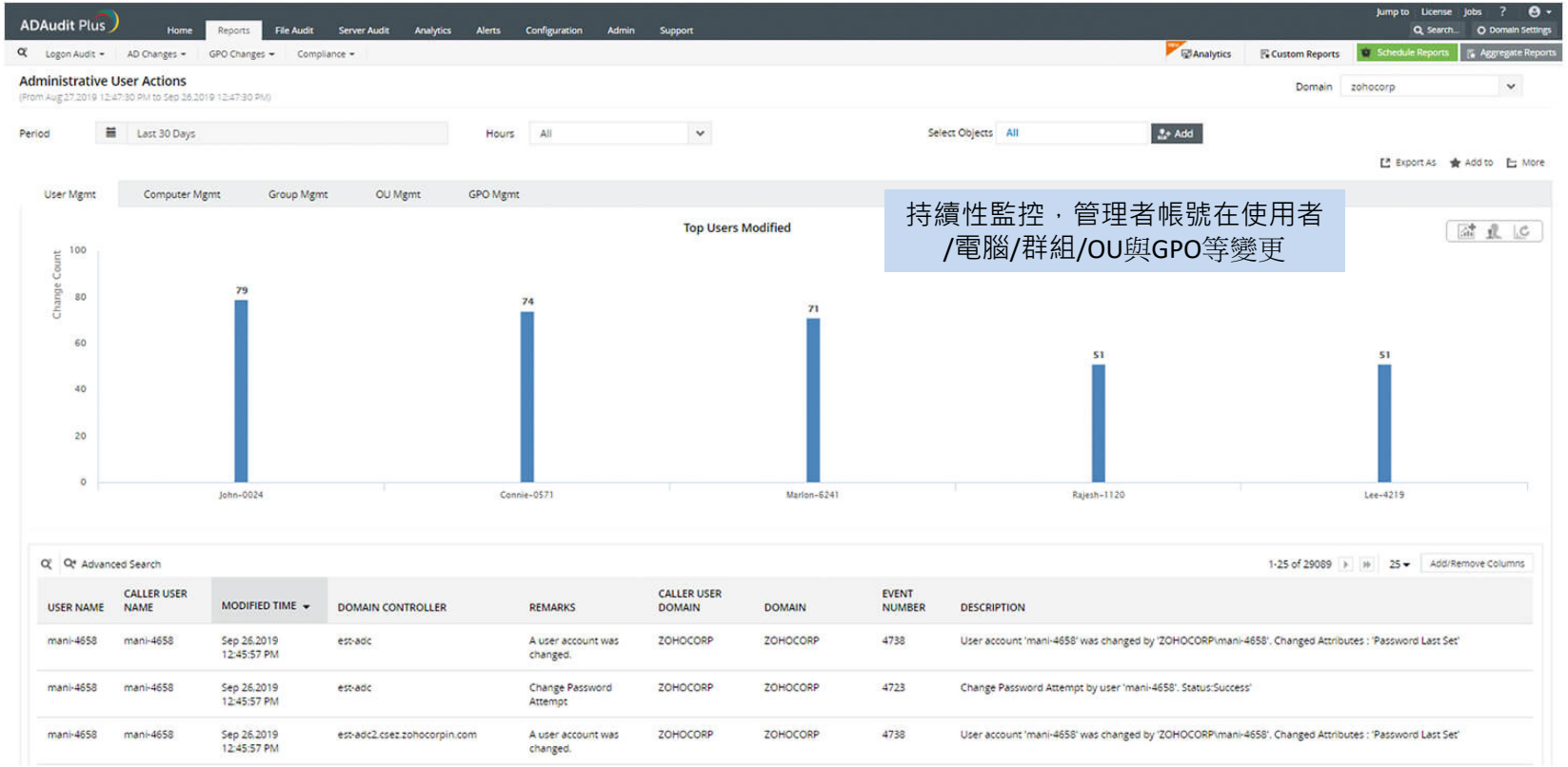
即時變更告警


ADAudit Plus
Home
Reports
File Audit
Server Audit
Analytics
Alerts
Configuration
Admin
Support
Jump to
License
Jobs
Search...
Domain Settings
All Alerts
Profile Based Alerts
adapqa.com
Default Domain Controllers Policy Modified
Default Domain Policy Modified
Privilege Escalation - First time Utilizing a Privilege
Unusual Activity -File Delete Count (Based on User)
Unusual Activity -File Modification Count (Based on User)
Unusual Activity -File Activity Time (Based on User)
Unusual Activity -File Activity Count (Based on User)
Unusual Activity -File Failure Count (Based on User)
First Time -Process on Server
Unusual Activity -LockOut Activity Time (domain based)
Unusual Activity -LockOut Activity Count (domain based)
Unusual Activity -User Management Activity time
Unusual Activity -User Management Activity Count
Active Alerts
Show All Alerts
(From Nov 12,2019 01:14:57 PM To Dec 12,2019 01:14:57 PM)
E-Mail Notification
New Alert Profile
View/Modify Alert Profiles
Last 30 Days
SEVERITY BASED ALERTS
Attention
Trouble
Critical
Critical
6
Filter Critical Alerts
Trouble
35
Filter Trouble Alerts
Attention
75
Filter Attention Alerts
即時偵測大量異常行為，包含新增/刪除/調整等等，透過機械學習找出內部惡意成員
1-25 of 116
25
SOURCE
DOMAIN
SEVERITY
TIME GENERATED
ALERT MESSAGE
ALERT PROFILE NAME
THRESHOLD
adapqa-dc1.adapqa.com
adapqa.com
Attention
Dec 05,2019 03:12:03 PM
server 'CN=FILEAUDIT-MS1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=adapqa,DC=com'was created by 'ADAPQA\Administrator'.
Configuration Changes
-
adapqa-dc1.adapqa.com
adapqa.com
Attention
Dec 05,2019 03:12:03 PM
server 'CN=FILEAUDIT-MS1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=adapqa,DC=com'was deleted by 'ADAPQA\Administrator'.
Configuration Changes
-

支援Azure AD稽核

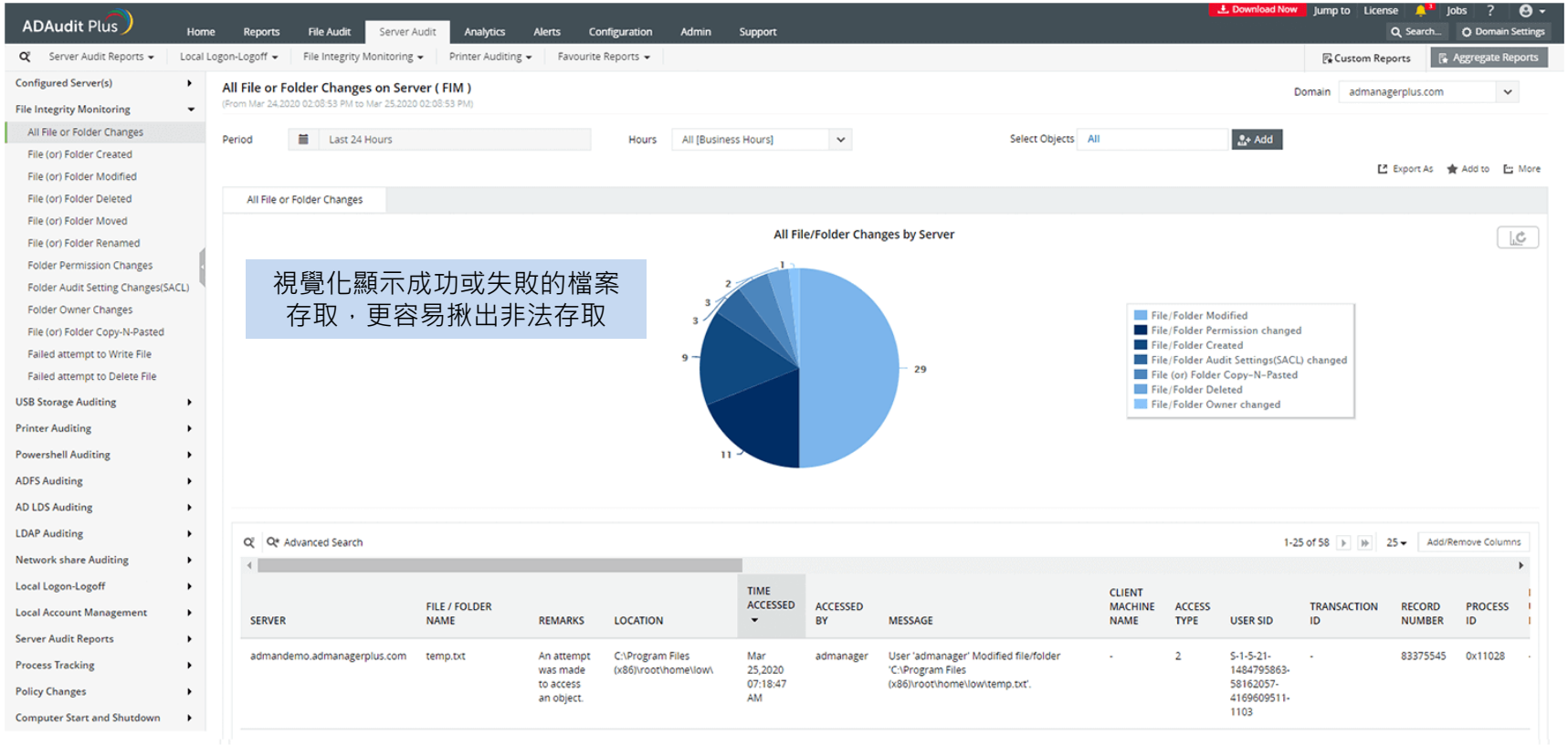


特權帳號監控

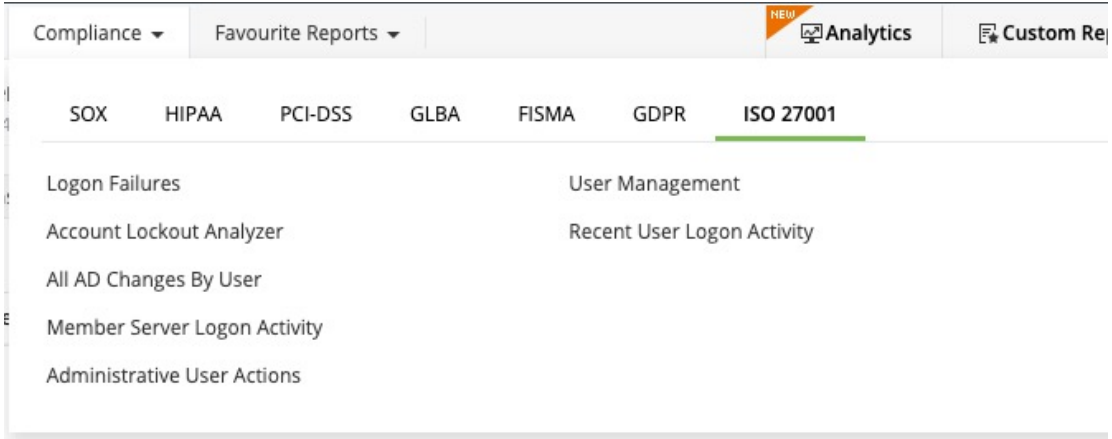


持續性監控，管理者帳號在使用者/電腦/群組/OU與GPO等變更

檔案完整性監控


ADAudit Plus
Home
Reports
File Audit
Server Audit
Analytics
Alerts
Configuration
Admin
Support
Download Now
Jump to
License
Jobs
Search...
Domain Settings
Server Audit Reports
Local Logon-Logoff
File Integrity Monitoring
Printer Auditing
Favourite Reports
Custom Reports
Aggregate Reports
Configured Server(s)
File Integrity Monitoring
All File or Folder Changes
File (or) Folder Created
File (or) Folder Modified
File (or) Folder Deleted
File (or) Folder Moved
File (or) Folder Renamed
Folder Permission Changes
Folder Audit Setting Changes(SACL)
Folder Owner Changes
File (or) Folder Copy-N-Pasted
Failed attempt to Write File
Failed attempt to Delete File
USB Storage Auditing
Printer Auditing
Powershell Auditing
ADFS Auditing
AD LDS Auditing
LDAP Auditing
Network share Auditing
Local Logon-Logoff
Local Account Management
Server Audit Reports
Process Tracking
Policy Changes
Computer Start and Shutdown
All File or Folder Changes on Server (FIM)
(From Mar 24,2020 02:08:53 PM to Mar 25,2020 02:08:53 PM)
Domain
admanagerplus.com
Period
Last 24 Hours
Hours
All [Business Hours]
Select Objects
All
Add
Export As
Add to
More
All File or Folder Changes
All File/Folder Changes by Server
視覺化顯示成功或失敗的檔案存取，更容易揪出非法存取
29
11
9
3
3
2
1
File/Folder Modified
File/Folder Permission changed
File/Folder Created
File/Folder Audit Settings(SACL) changed
File (or) Folder Copy-N-Pasted
File/Folder Deleted
File/Folder Owner changed
Advanced Search
1-25 of 58
25
Add/Remove Columns
SERVER
FILE / FOLDER NAME
REMARKS
LOCATION
TIME ACCESSED
ACCESSED BY
MESSAGE
CLIENT MACHINE NAME
ACCESS TYPE
USER SID
TRANSACTION ID
RECORD NUMBER
PROCESS ID
admandemo.admanagerplus.com
temp.txt
An attempt was made to access an object.
C:\Program Files (x86)\root\home\low\
Mar 25,2020 07:18:47 AM
admanager
User 'admanager' Modified file/folder 'C:\Program Files (x86)\root\home\low\temp.txt'.
-
2
S-1-5-21-1484795863-58162057-4169609511-1103
-
83375545
0x11028

輕鬆符合規範要求

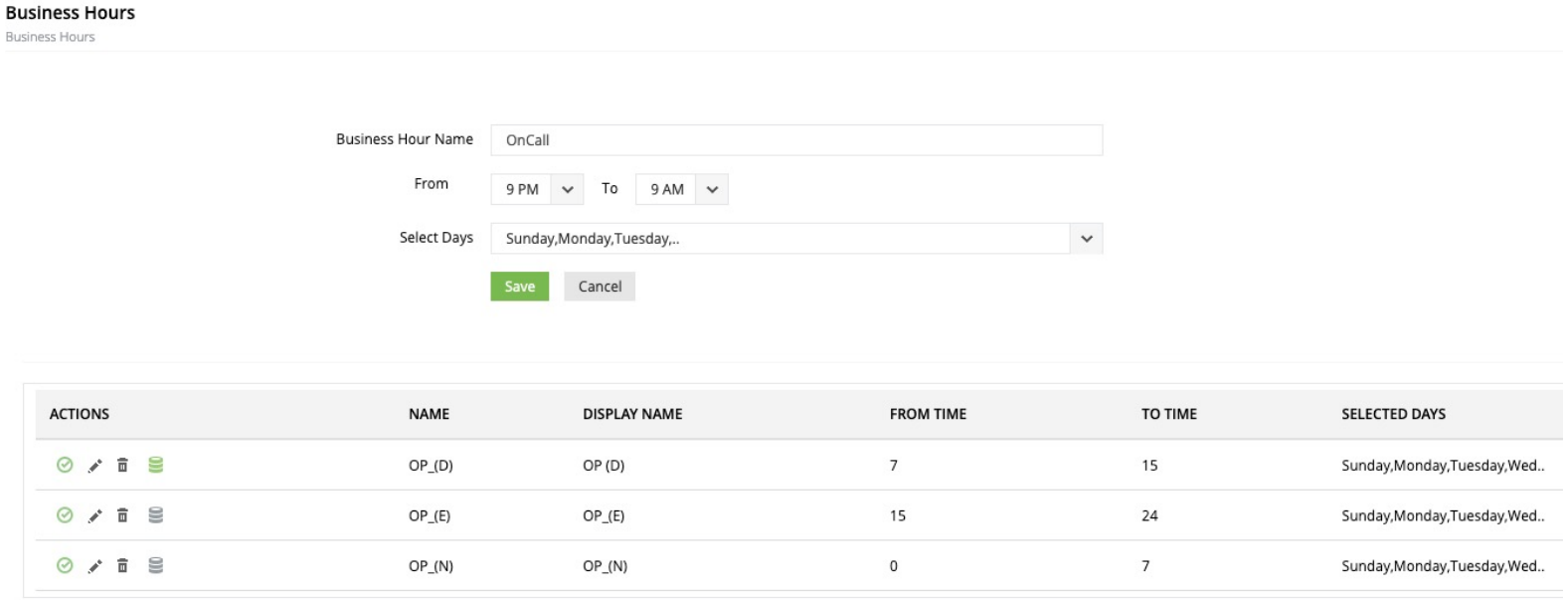

Compliance
Favourite Reports
NEW
Analytics
Custom Re
SOX
HIPAA
PCI-DSS
GLBA
FISMA
GDPR
ISO 27001
Logon Failures
Account Lockout Analyzer
All AD Changes By User
Member Server Logon Activity
Administrative User Actions
User Management
Recent User Logon Activity


SOX
HIPAA
PCI
FISMA
GLBA

實際應用

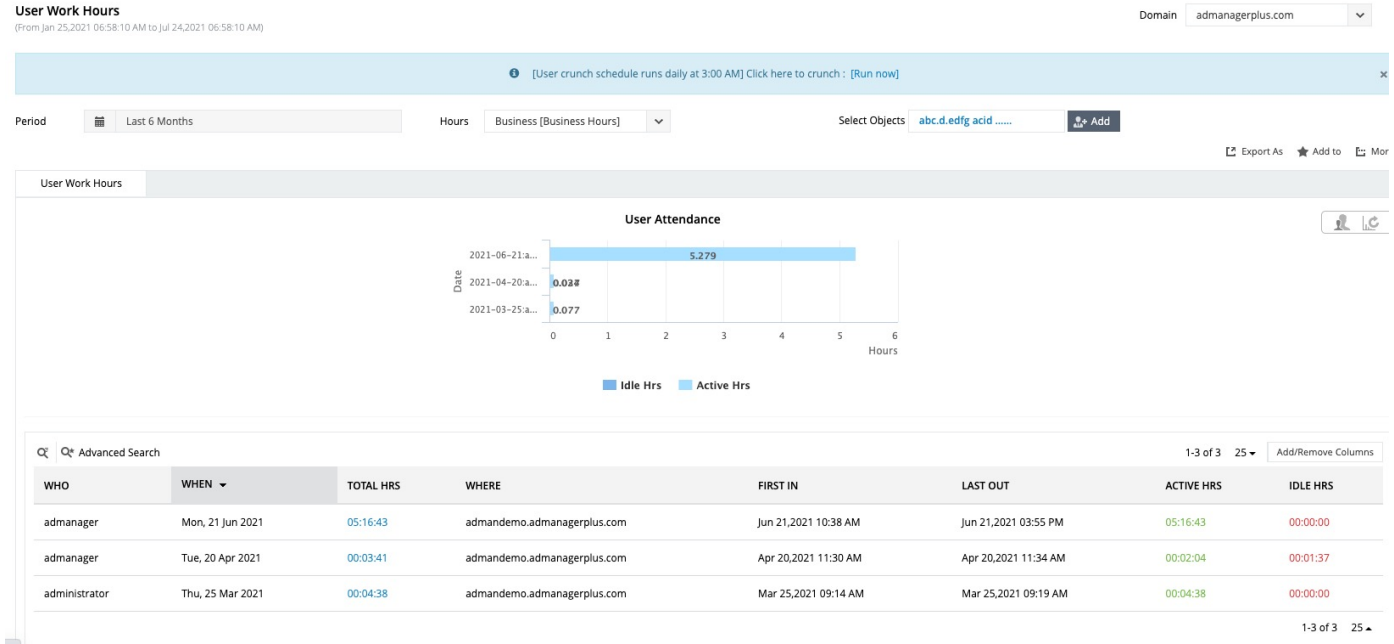
人員登入登出工時記載

- 設定多組上下班時間



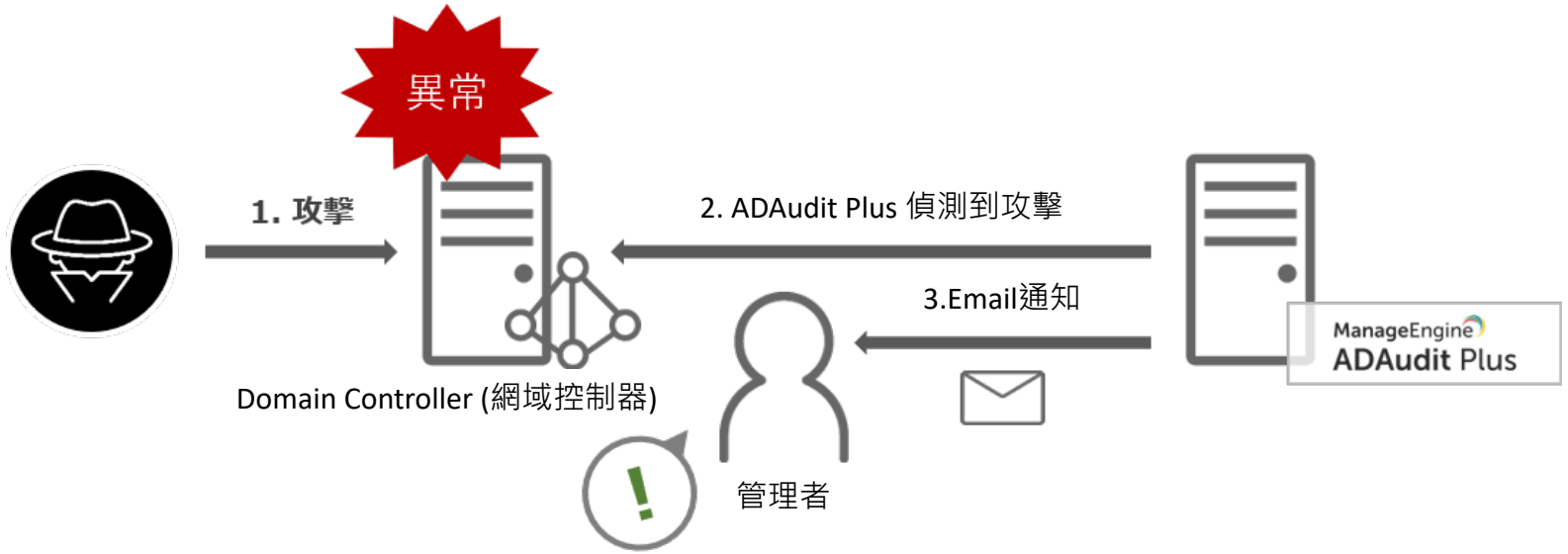
人員登入登出工時記載(續)

- 勞檢時立刻提出佐證，WFH也不需要登入點名了。



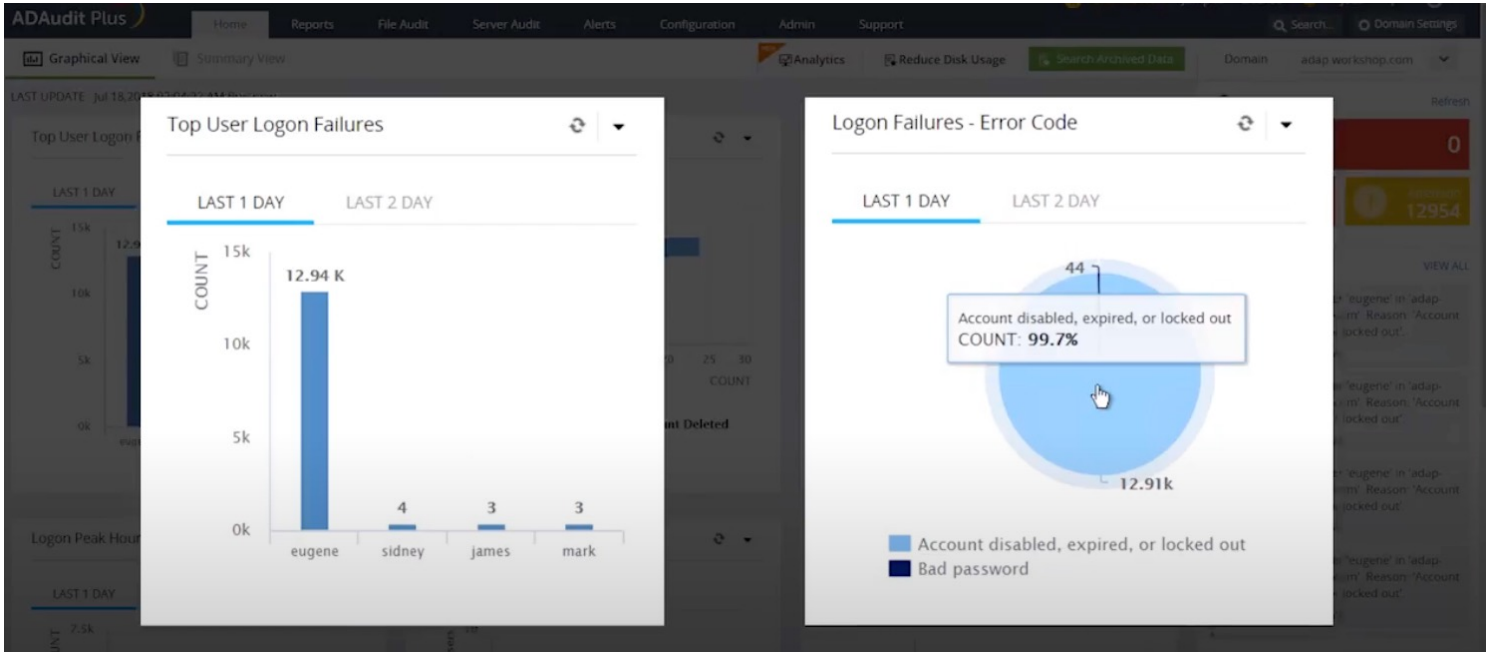
監控AD是否遭到攻擊

- 下班時間，嚴密監控是否遭大量登入且告警



監控AD是否遭到攻擊

- 揪出大量登入失敗帳號，疑似暴力破解




案例分享

連續四年榮獲
Gartner Peer Insights Customer's Choice for SIEM

Our customers have spoken! We're thrilled to be named a **Gartner Peer Insights Customers' Choice** for SIEM once again!

為你呈現

ManageEngine

Introduing ManageEngine

ManageEngine的概念就是

- 花更少的預算
- 得到相同的功能
- 甚至更多!

全方位IT管理解決方案

- IT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簡化管理
  - 易於下載、安裝、設定和部署，無需第三方支援服務或幫助。
- IT實惠管理
  - 更高的價格並不始終意味著更好的產品

180,000+
家全球企業

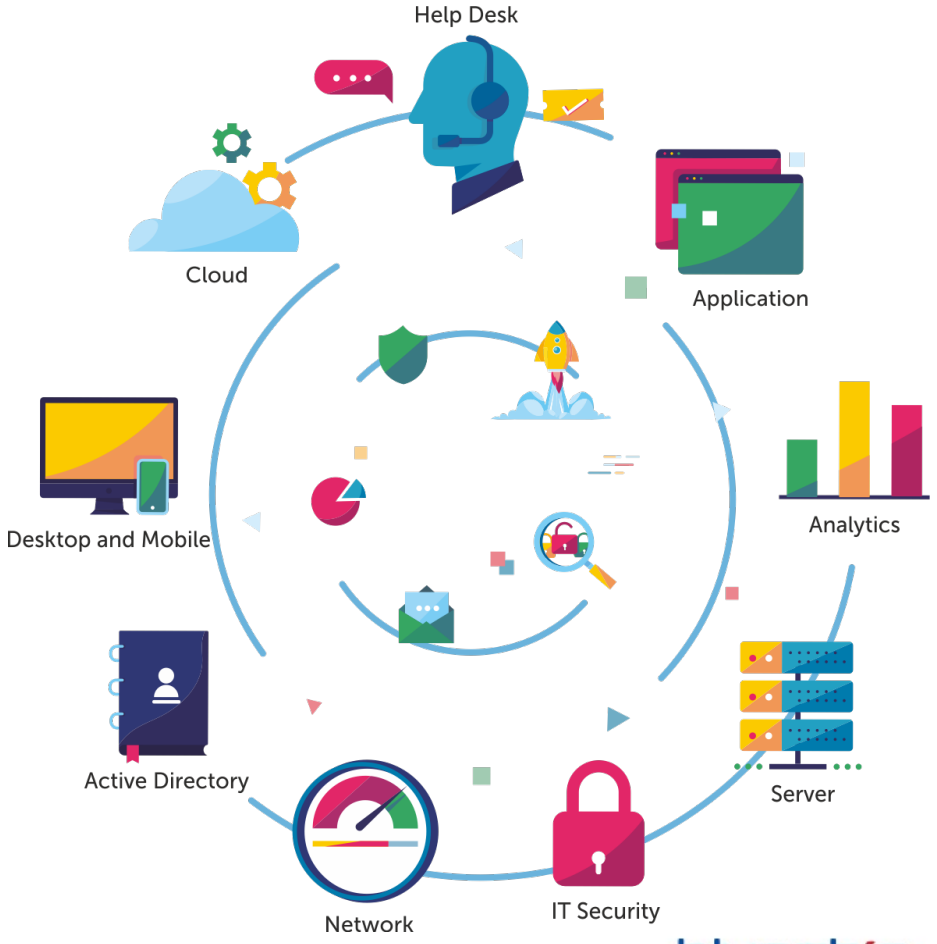
9/10
財富 100 強公司

3,000,000+
管理者

..信任 ManageEngine 來管理其 IT。

ManageEngine 協助您

- ITIL整合式資產和服務管理
- 更有效的管理雲平台
- 比讓微軟更實用的AD管理
- 大量端末設備
- 複雜的基礎設施
- 符合資安需求的稽核
- 可滿足所有IT管理需求



選擇ManageEngine

- 易於安裝、易於操作、易於管理
- 與企業一同成長，彈性增長規格
- 極具競爭力的價格

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
- 超過101名員工，提供您最佳服務

THANK YOU

Any Questions?

Or

Contact Kerry