EMS/ATA/OMS/System Center

資安相關方案

Enterprise Mobility Suite (EMS)

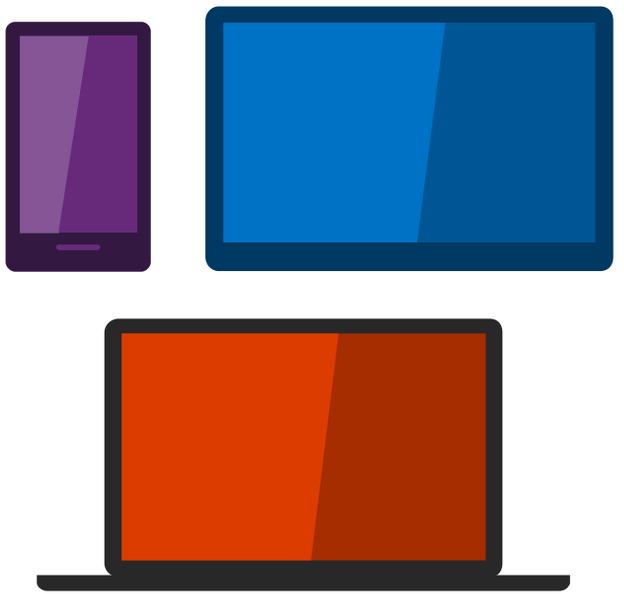
跨平台裝置管理解決方案

Microsoft Intune
行動裝置管理

Azure AD Premium
行動裝置上的使用者身分識別

Azure RMS
行動裝置上的檔案加密

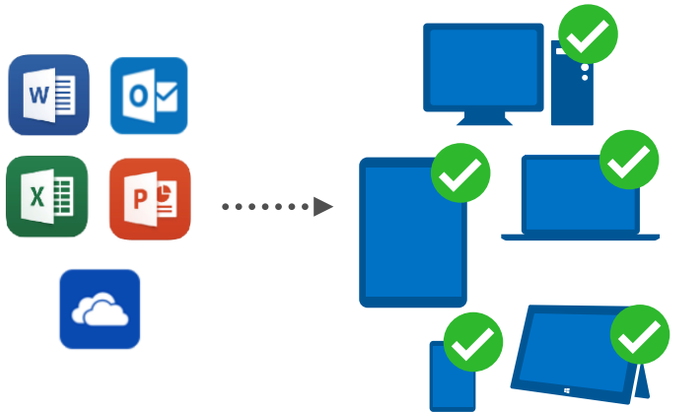
Microsoft ATA
進階式威脅分析與偵測



http://www.microsoft.com/zh-tw/server-cloud/enterprise-mobility/Overview.aspx

Why EMS ?

適合於企業使用的跨平台行動裝置管理解決方案

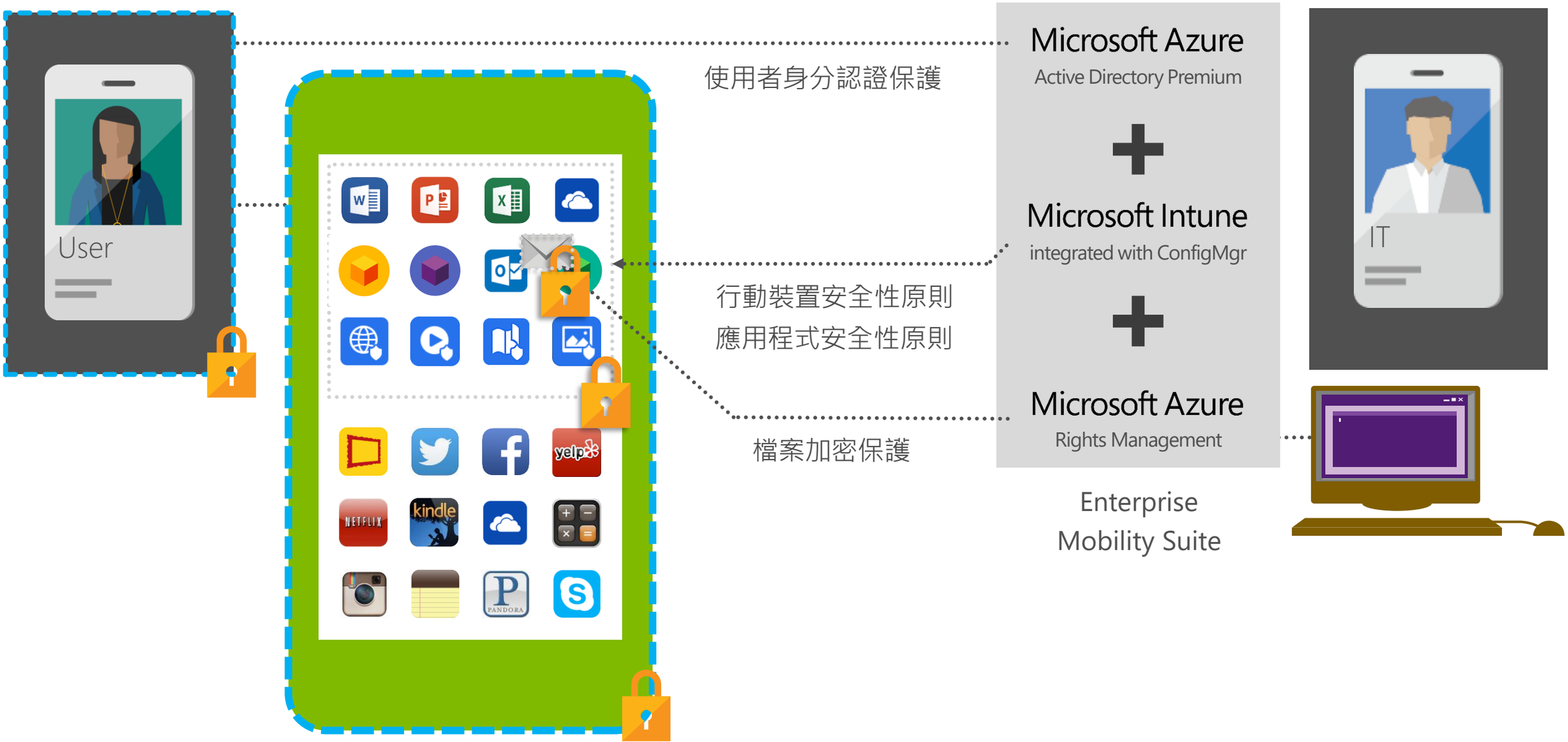


整合
應用程式跨平台部署

管理
跨平台行動裝置

轉型
改變商業模式降低IT成本

從上到下，安全加密滴水不漏



Managing Mobile Productivity

with Enterprise Mobility Suite

Future IT

Office 365 + EMS: 一次擁有行動生產力與安全性

安全無疑的行動平台

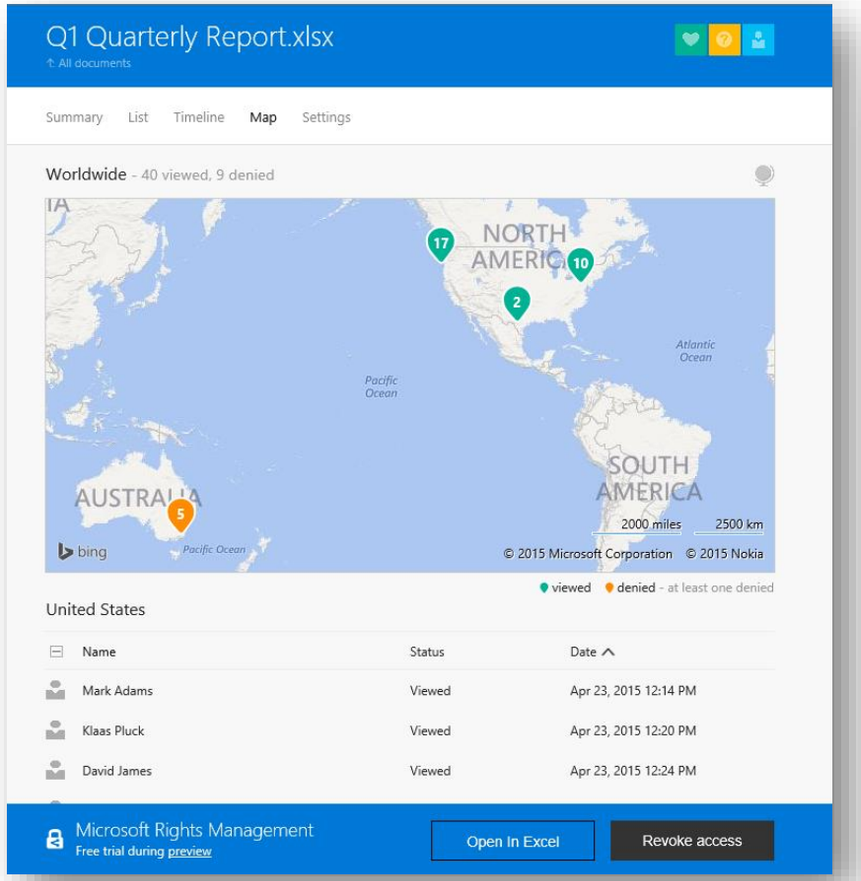
- IT 可自行定義企業安全法規,禁止未授權之應用程式存取商業資料藉此保護機敏資料不因為應用程式轉換而外洩
- 除了支援管理 iOS, Android 行動 Office apps, 更重要的是企業自行開發之應用程式也能同時受 Intune 的管控

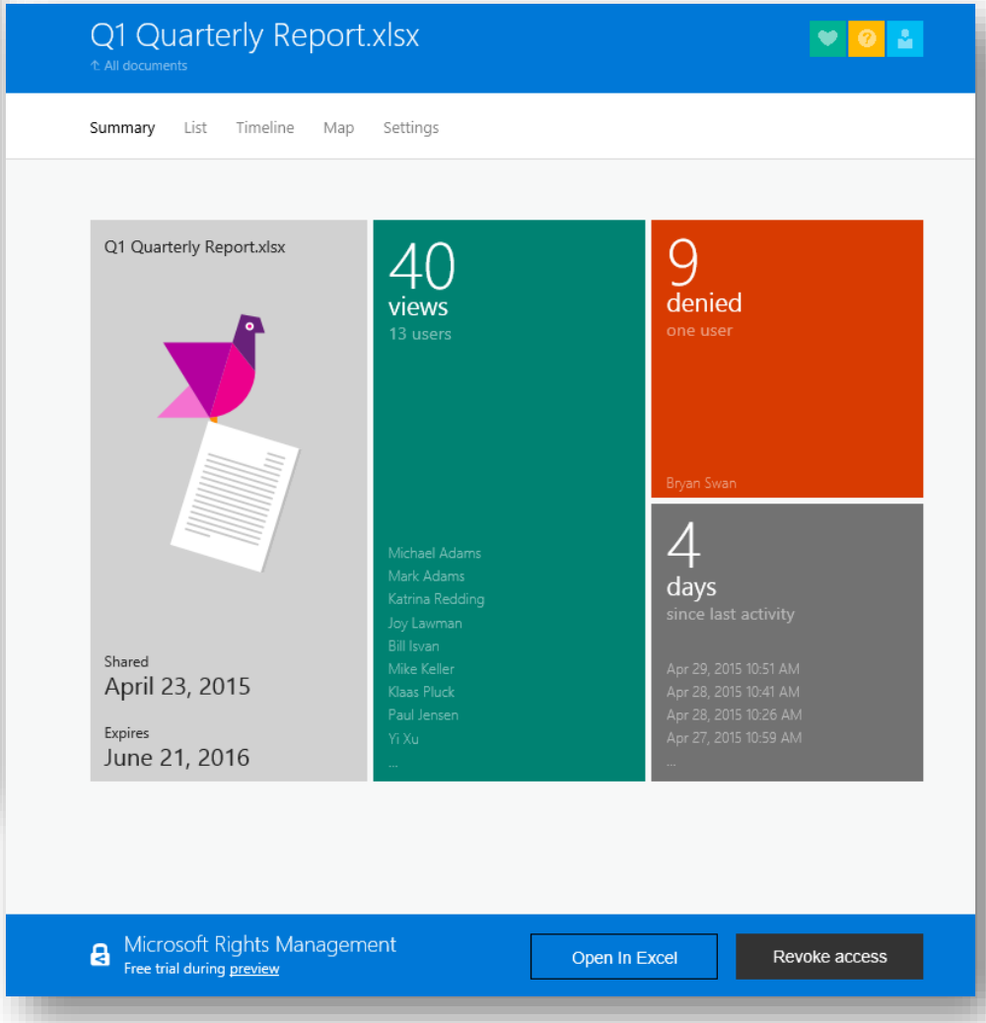
就如坐在辦公室一樣輕鬆自在

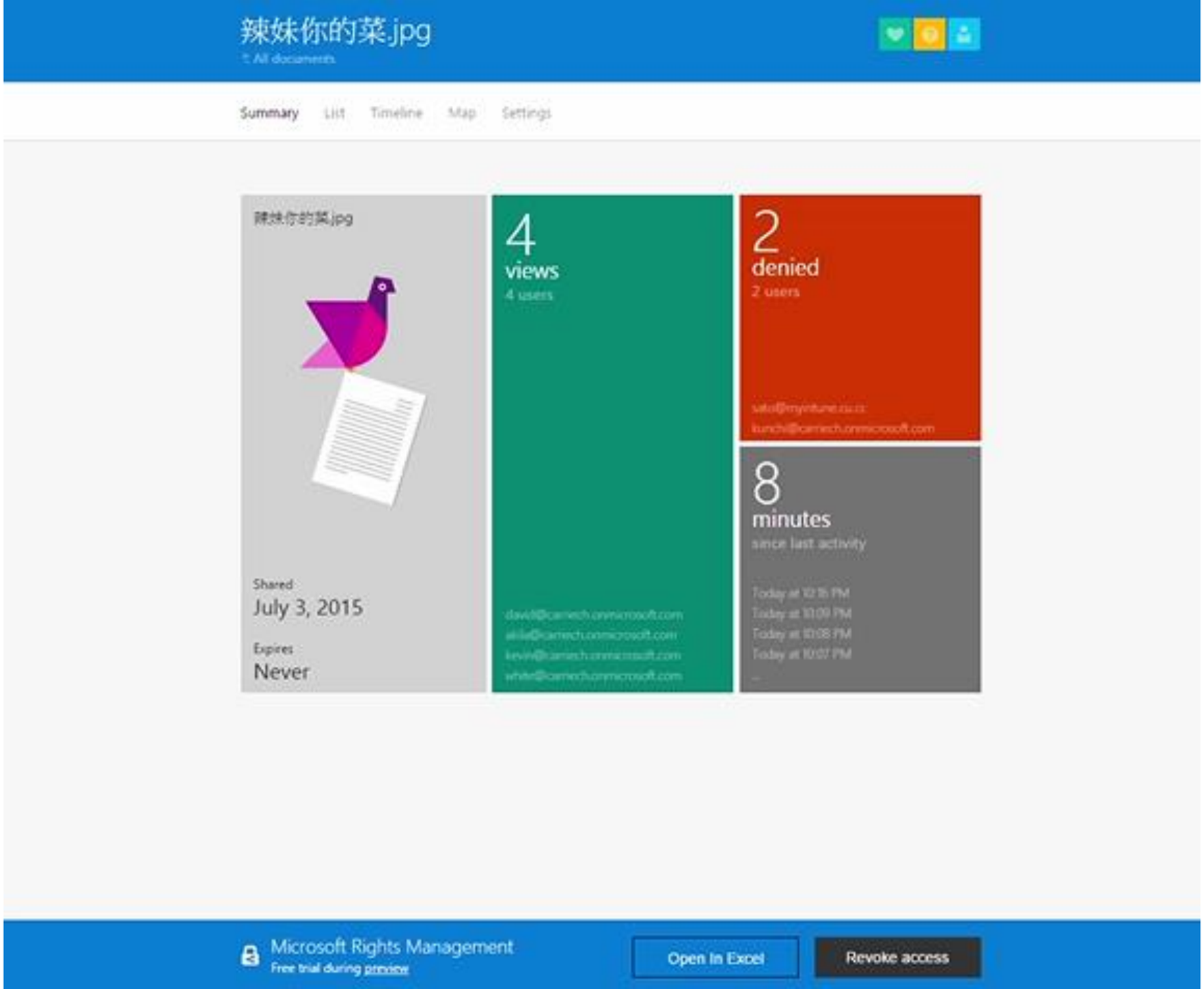
- 提供使用者介面熟悉, 功能齊全的 Office 應用程式
- 輕鬆管理與傳輸跨平台文件, 不必擔心格式問題
- 透過 OneDrive for Business 安全地保存, 同步與分享商業資料

Document Tracking
文件追蹤與加密 (2015下半年)

- Email 通知加密文件開起狀態
- 遠端回收檔案權限
- 自助式服務入口網站
- 地圖模式瀏覽加密文件開啟位置
- 自動分析使用流量

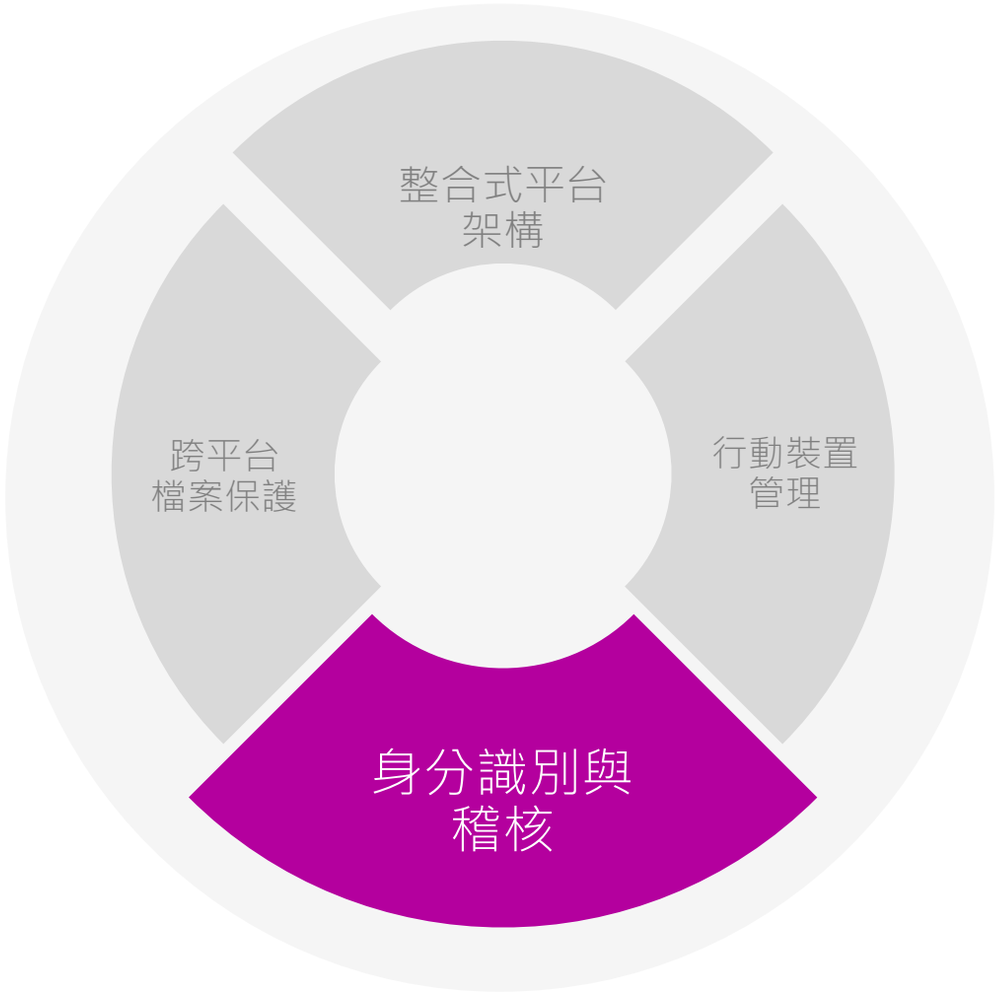





辣妹你的菜.jpg
All documents
Summary
List
Timeline
Map
Settings
辣妹你的菜.jpg
Shared
July 3, 2015
Expires
Never
4
views
4 users
2
denied
2 users
8
minutes
since last activity
Microsoft Rights Management
Free trial during preview
Open in Excel
Revoke access

Azure AD Premium

身分識別與稽核



- 多因素驗證 Multi-Factor Authentication
- 單一登入 Single Sign On
- 自助式服務使用者密碼重設 Self-Service Portal
- 安全性稽核報告 Reporting Service

WINDOWS 10

EMS 和 Windows 10 裝置可無縫式整合

- **Self-provisioning of corporate owned devices ->** 使用者自助式服務平台
- **Use existing organizational accounts ->** 無須更改現有管理模式
- **Automatic MDM enrollment ->**自動管理, 輕鬆無負擔
- **Single Sign-on on-premises ->** 單一登入, 內外皆通
- **Enterprise-ready Windows store ->** 專屬企業內部市集
- **Support for modern form factors ->** 即使沒加入網域, 也可以存取內部資源
- **OS State Roaming ->** 換機免煩惱, 設定跟著跑

正在改變的網路攻擊型態

現今的網路攻擊

- 取得使用者身分認證
- 以合法的軟體工具作為掩護，使得惡意攻擊更難追蹤
- 可隱匿、不被偵測到長達八個月
- 造成財物損失、品牌形象損毀、機密資料被竊取與相關的業務歸屬

正在改變的網路攻擊型態

現今的網路攻擊

- 取得使用者身分認證
- 以合法的軟體工具作為掩護，使得惡意攻擊更難追蹤
- 可隱匿、不被偵測到長達八個月
- 造成財物損失、品牌形象損毀、機密資料被竊取與相關的業務歸屬

正在改變的網路攻擊型態

現今的網路攻擊

- 取得使用者身分認證
- 以合法的軟體工具作為掩護，使得惡意攻擊更難追蹤
- 可隱匿、不被偵測到長達八個月
- 造成財物損失、品牌形象損毀、機密資料被竊取與相關的業務歸屬

正在改變的網路攻擊型態

現今的網路攻擊

- 取得使用者身分認證
- 以合法的軟體工具作為掩護，使得惡意攻擊更難追蹤
- 可隱匿、不被偵測到長達八個月
- 造成財物損失、品牌形象損毀、機密資料被竊取與相關的業務歸屬

面臨的挑戰

傳統資訊安全解決方案

複雜

初始設定、微 調以及設立規範以及準則

容易偵測錯誤

偵測的錯誤佔據使用者的寶貴時間

防護措施未到位

當使用者機密被竊取、攻擊者在網路活動，防範軟體並無相關因應措施與辦法

微軟Advanced Threat Analytics

具有預防能力的全方位資安守門員

使用行為分析

資安風險偵測

Advanced Threat Detection
ATD

微軟Advanced Threat Analytics的優勢

快速

不須新增規範、篩選機制或準則。
ATA 利用Active Directory 和 SIEM 瀏覽歷史資料，快速的偵測可疑行為。

自主學習

自主的分析、辨識出異常行為。

一目了然的報告

即時的回報攻擊發生的時間、位置與方式。

正確率高的警示

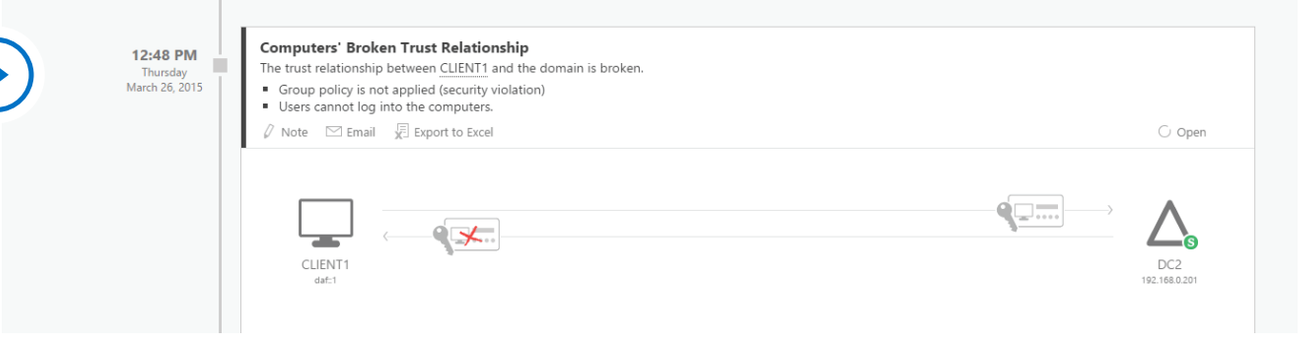
ATA 不僅將異常活動與使用者的例行活動比較，也會和其他使用者的活動紀錄對比，以確保警示提醒的正確率。

現今企業員工使用多種裝置

Microsoft Advanced Threat Analytics 運作方式

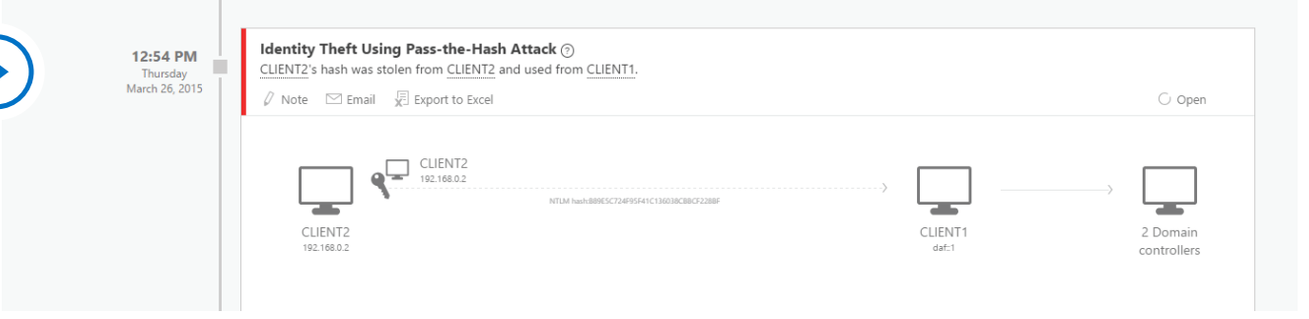
安全問題和風險

- 不受信任
- 薄弱通訊協定
- 已知通訊協定弱點



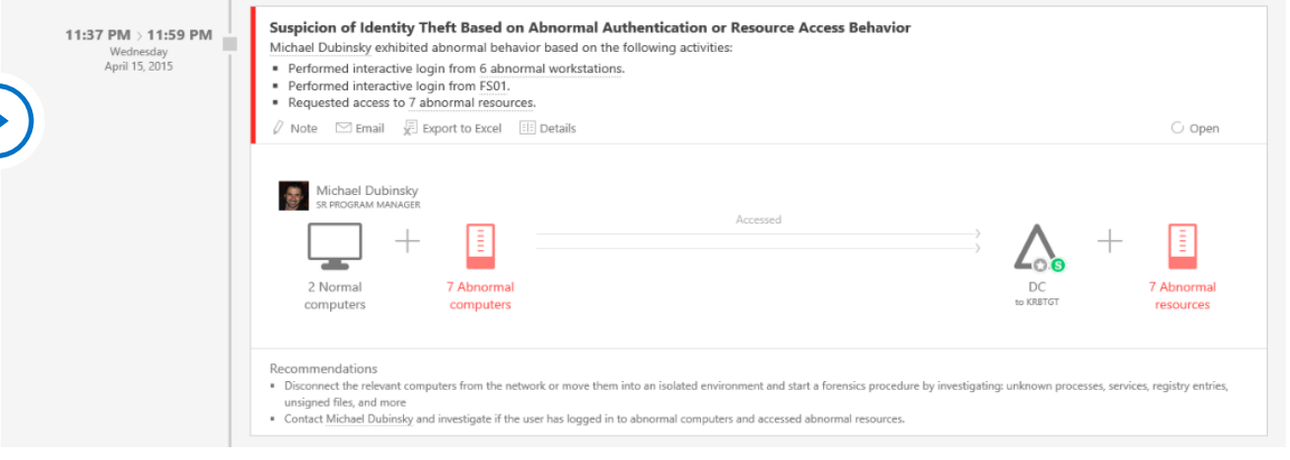
惡意攻擊

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Skeleton key malware
- Reconnaissance
- BruteForce

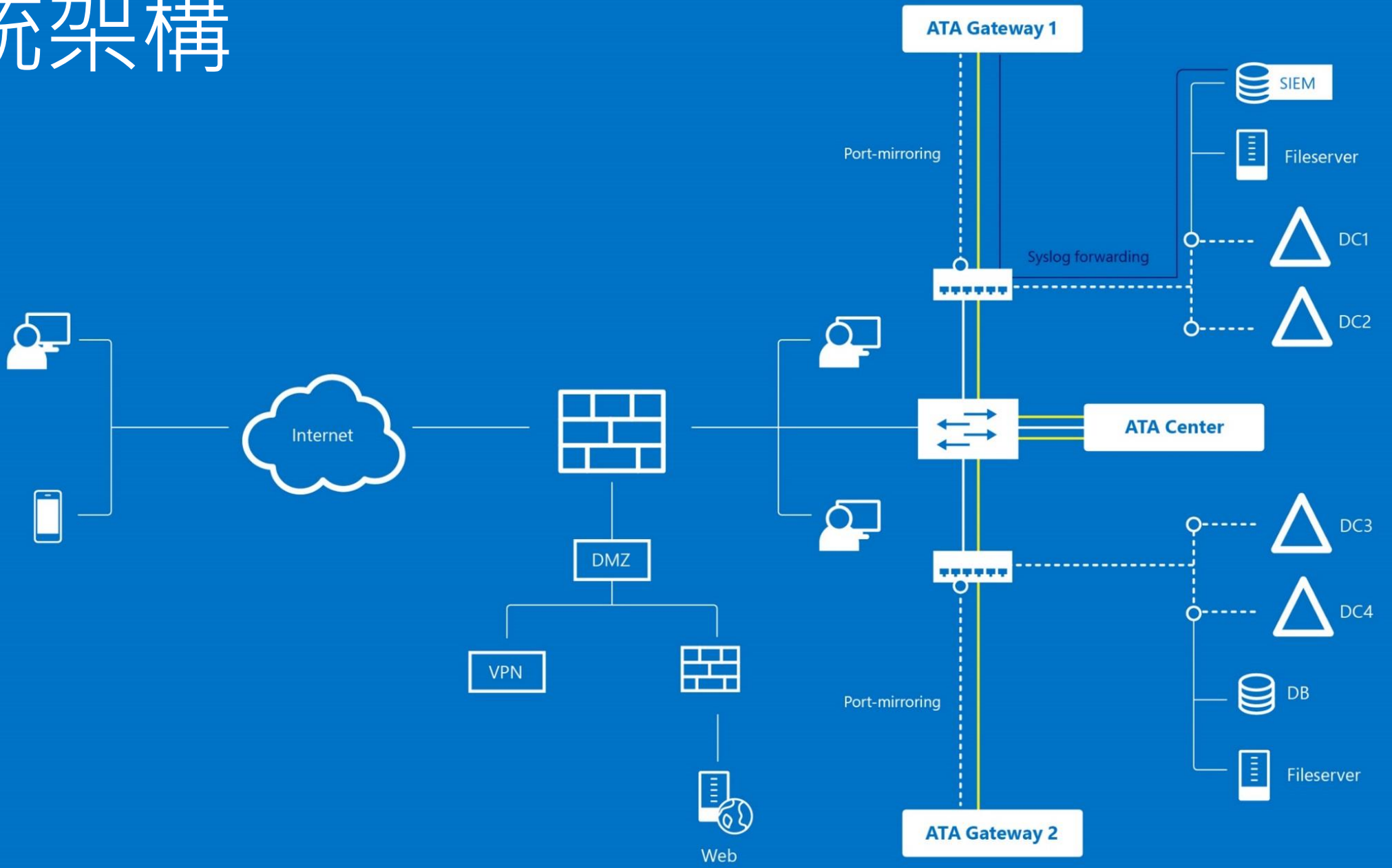


異常行為

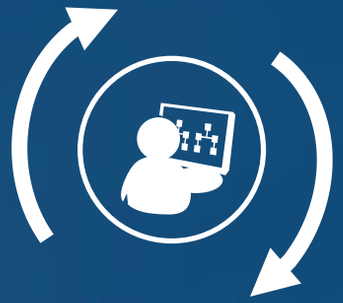
- 異常登入
- 遠端程式碼執行
- 可疑活動
- 未知威脅
- 分享密碼
- 水平擴散

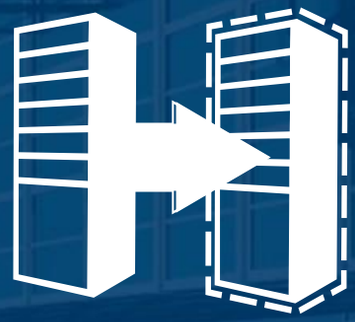


系統架構


ATA Gateway 1
SIEM
Fileserver
Port-mirroring
DC1
Syslog forwarding
DC2
Internet
ATA Center
DMZ
DC3
DC4
VPN
DB
Port-mirroring
Fileserver
Web
ATA Gateway 2

OMS 解決方案





記錄分析	自動化	可用性	安全性
收集並分析公有雲與私有雲的資料	自動化複雜與高重覆性的工作	增加資料保護與提高應用程式可用性	協助加強工作、伺服器、使用者的安全性

http://www.microsoft.com/oms

Overview

Log Search

My Dashboard

Solutions Gallery

2.7GB
Servers and Usage

AD Assessment

4
Servers Assessed

3
High Priority Recommendations

6
Low Priority Recommendations

72
Passed Checks

Malware Assessment

1
Servers with Active Threats

38
Servers with Inadequate Protection

Capacity Planning

23.6 %
Available Cores

62.3 %
Available Memory

42.5 %
Available Storage

Backup

ITPRodBackup

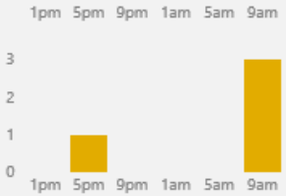
13
Servers backed up

3 TB
Backup data

Alert Management

0
Active critical alerts in the last 24 hours

4
Active warning alerts in the last 24 hours



Automation

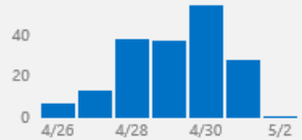
ITAutomation

9
Runbooks

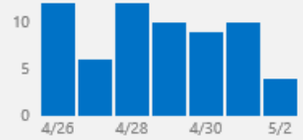
15
Jobs in the last 7 days

Change Tracking

20
Software changes in the last 24 hours



6
Windows service changes in the last 24 hours (excludes Status)



Security and Audit

95 ↘ 1
Active Computers in the last 24 hours

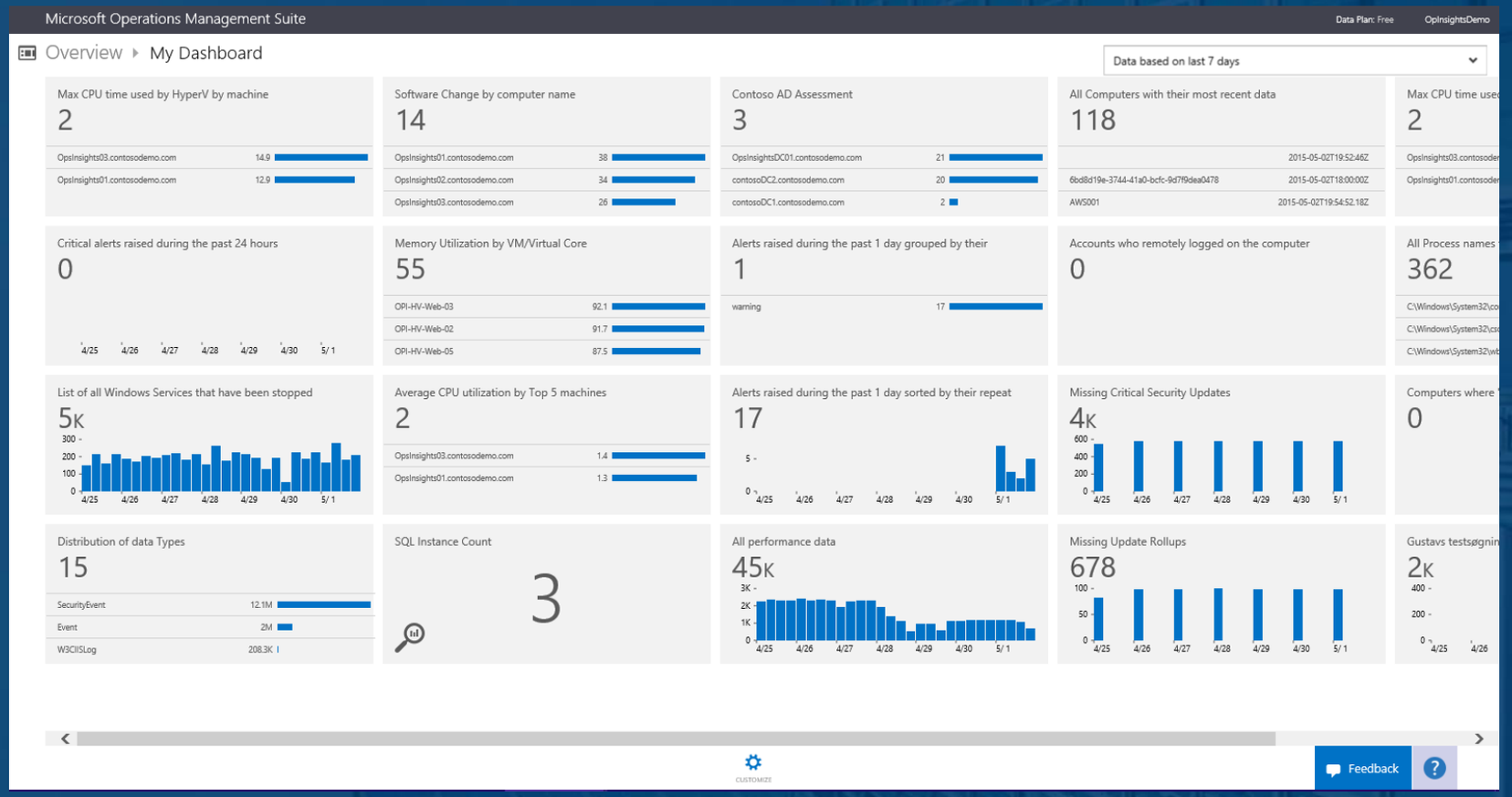
64 ↗ 1
Accounts Authenticated in the last 24 hours

Feedback

自訂儀表板

將多個自訂搜尋結果，視覺化整合到同一個介面上，提供一個 IT 環境狀態的概觀

- 使用內建或自訂的搜尋條件
- 可自行調整的視覺化介面呈現
- 跨小組與工作區搜尋結果整合



方案套件 Solution Packs

類似 SCOM 的管理組件 (Management Pack, MP)，定義了資料收集規則、視覺化介面、程式邏輯

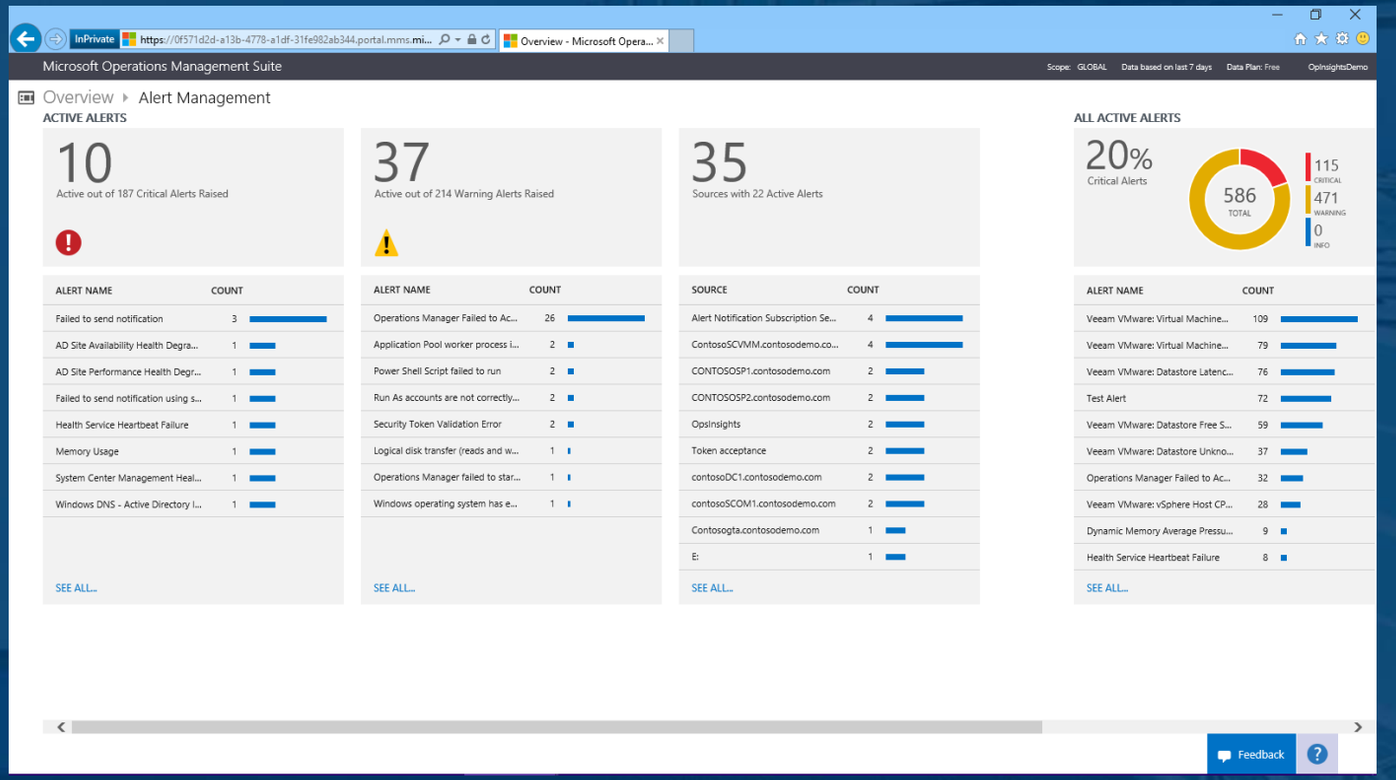
- 整合原本強大的搜尋能力
- 針對特定領域進行資料收集與分析
- 協助調查與解決該領域所面臨的問題
- 可以隨時新增到與移除自管理介面

方案套件

Alert Management

整合並呈現 System Center Operations Manager 的警示資訊

- Web 介面的視覺化警示呈現
- 整合搜尋功能，進行深入警示分析
- 內建常用的警示查詢條件

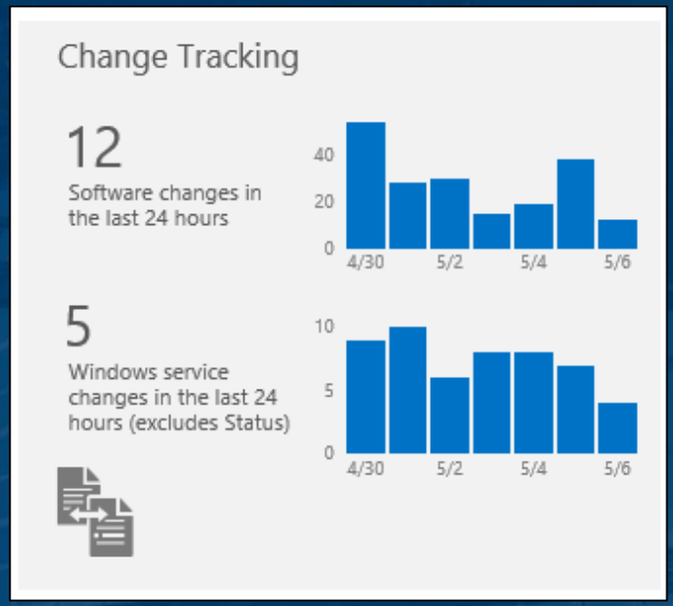


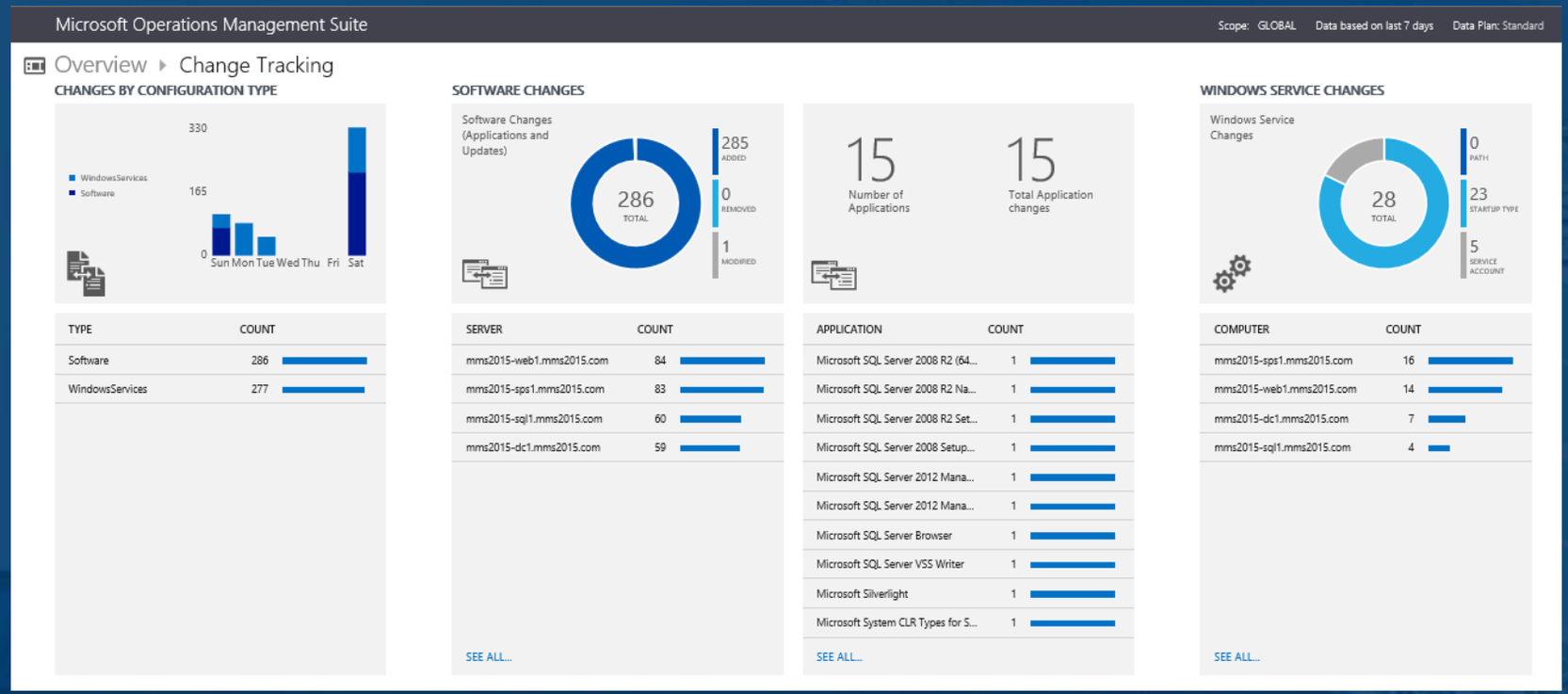
方案套件

Change tracking

跨環境追蹤系統變更

- 系統變更統計 (依類型)
- 伺服器軟體變更
- 應用程式變更
- Windows 務變更



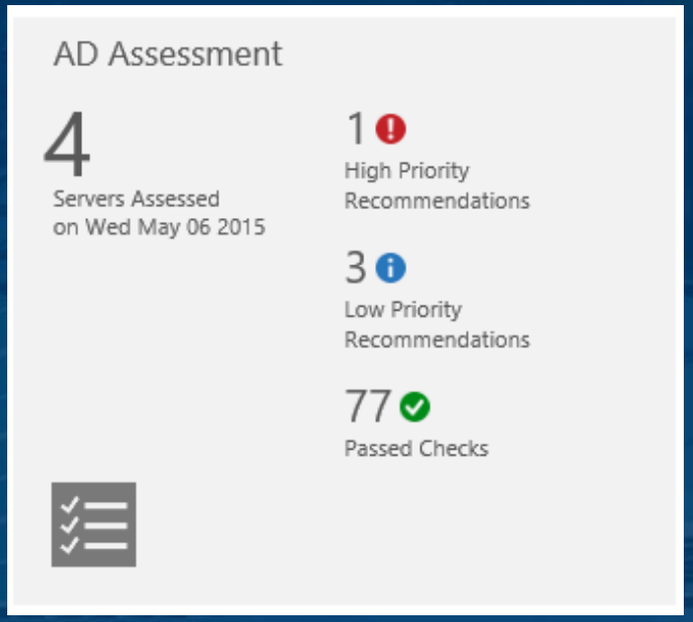


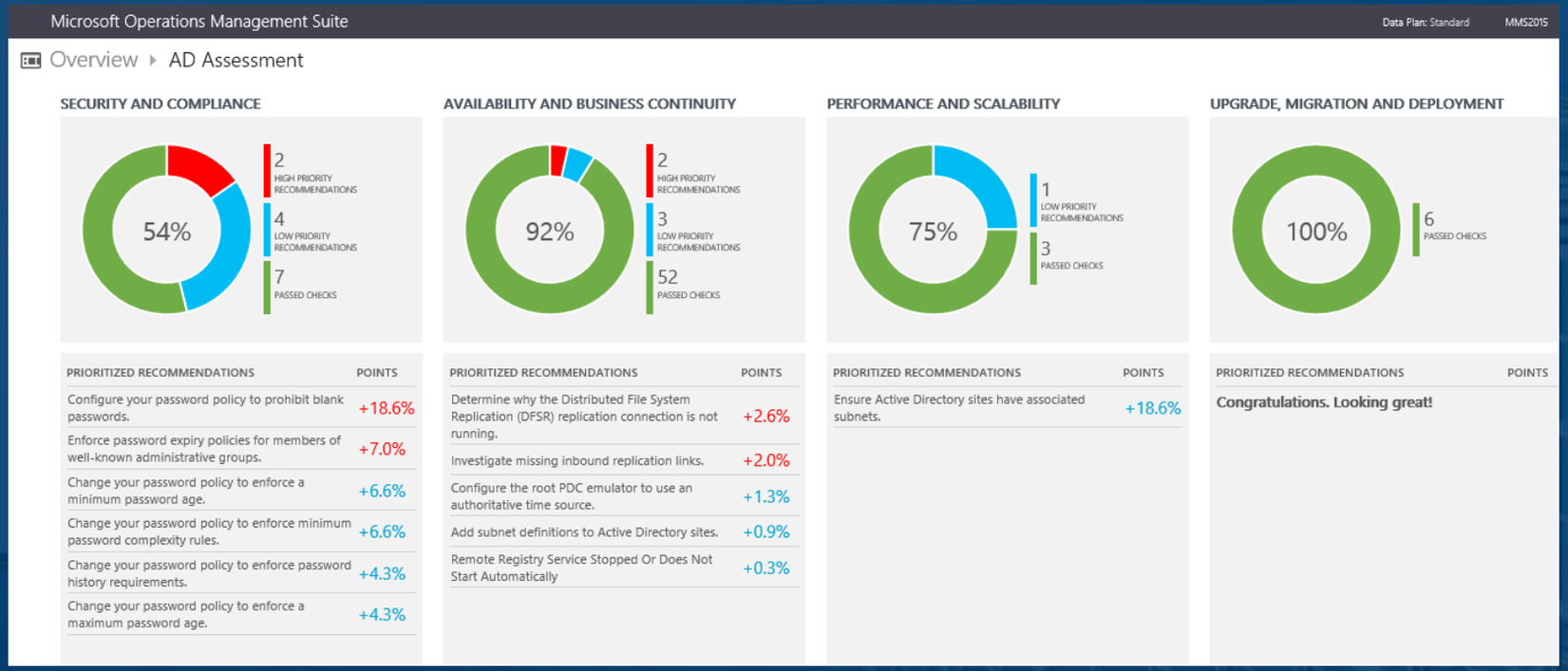
方案套件

Active Directory Assessment

使用最佳實作與所收集到的資料
進行比對，找出 AD 潛在的問題

- 安全與規則符合
- 可用性與企業永續性
- 效能與擴展性
- 升級、移轉與部署



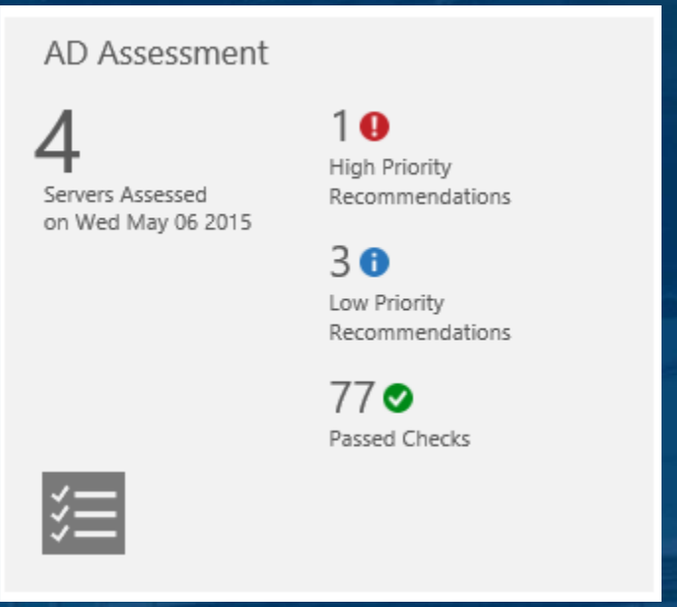


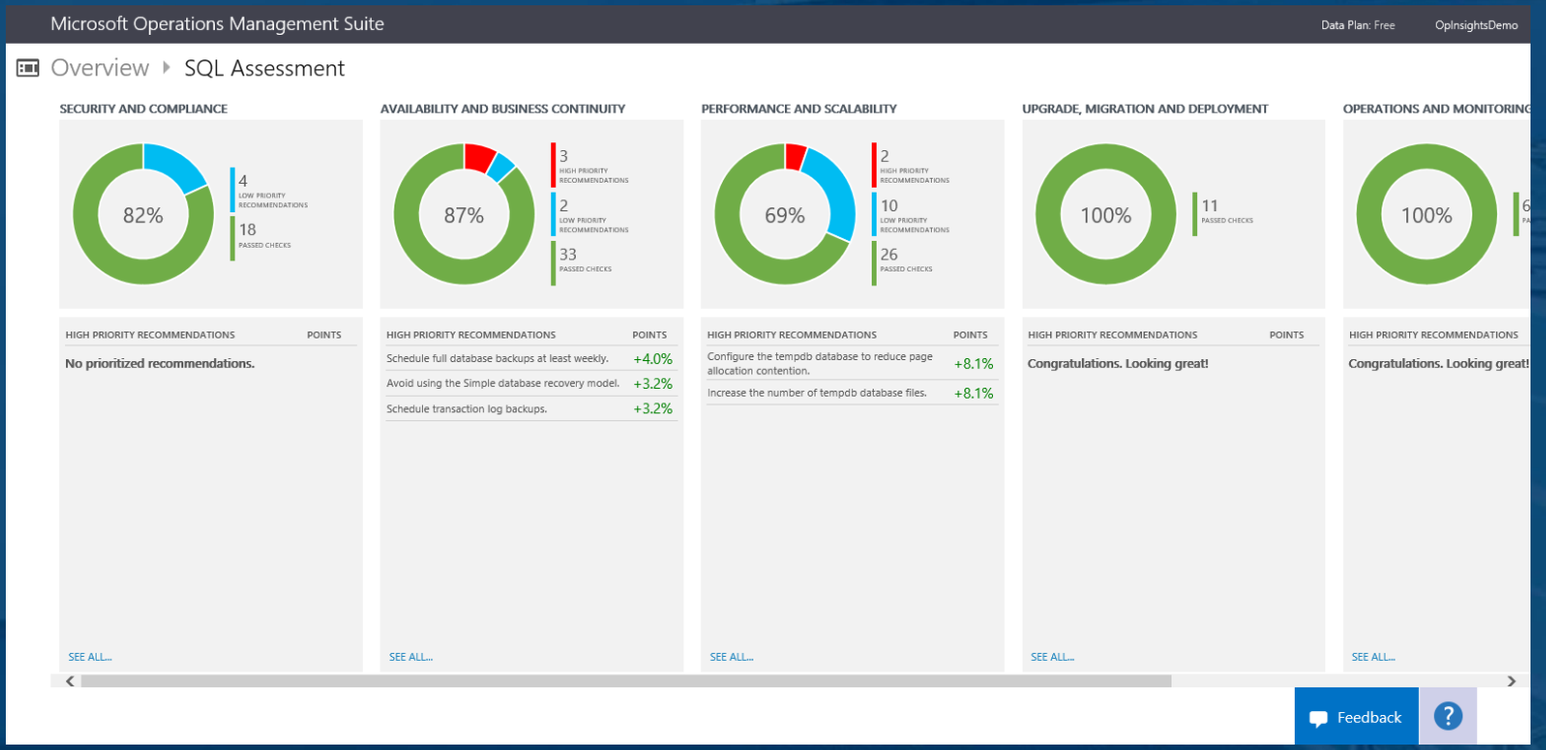
方案套件

SQL Server Assessment

使用最佳實作與所收集到的資料進行比對，找出 SQL Server 潛在的問題

- 安全與規則符合
- 可用性與企業永續性
- 效能與擴展性
- 升級、移轉與部署
- 作業與監控
- 變動與組態管理



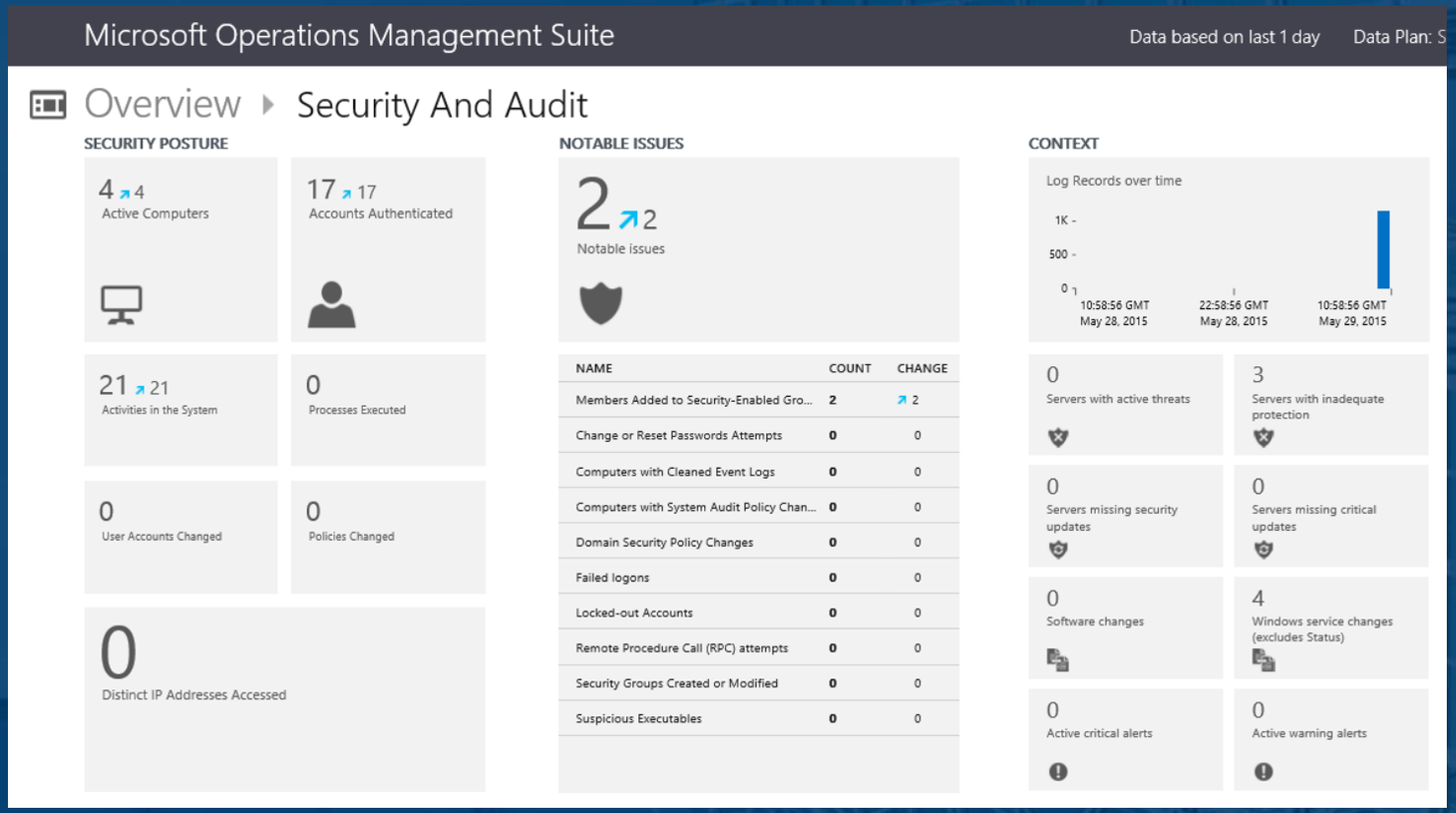


方案套件

Security and Audit

提供安全與稽核相關的統計

- 安全性資訊統計
- 已知問題通知
- 安全事件統計

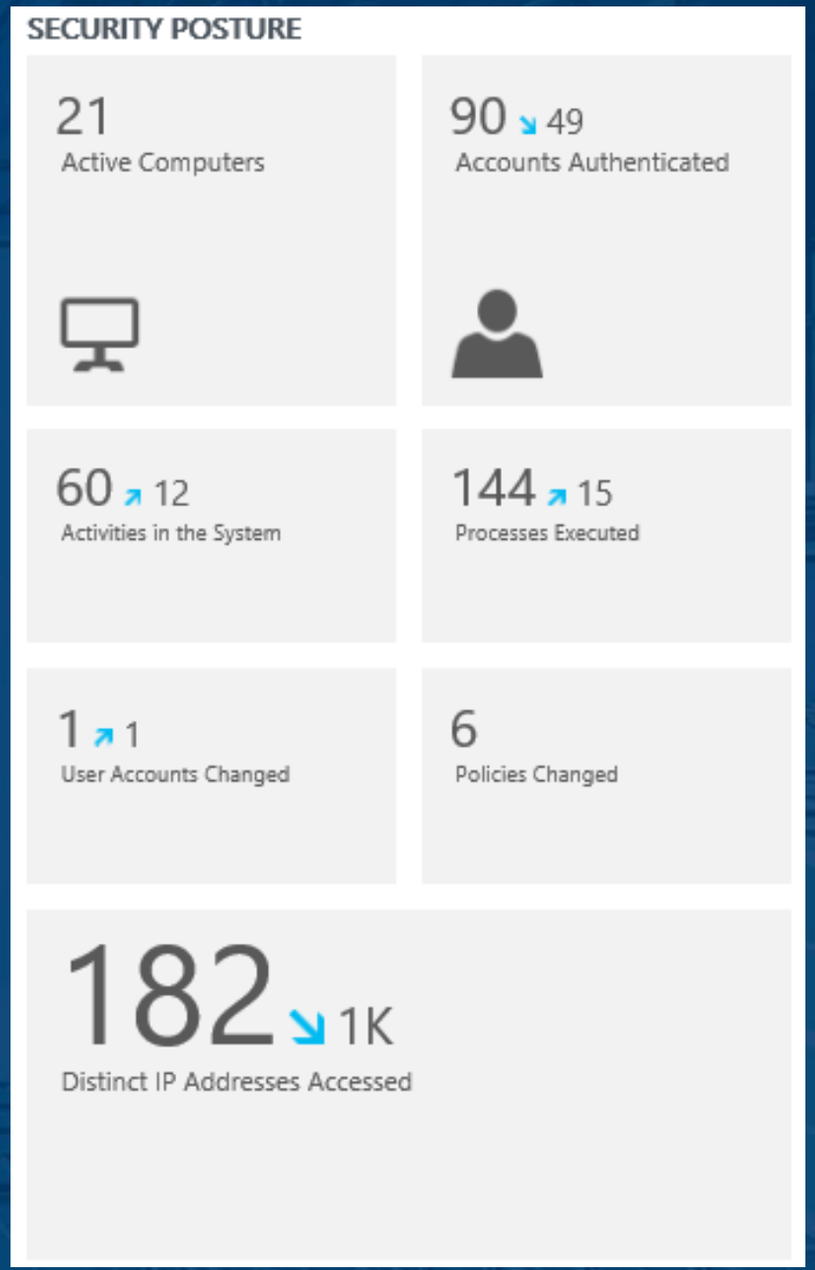


方案套件 – Security and Audit

Security Posture

快速瀏覽伺服器的各項工作量
與安全威脅

- 電腦數量增減
- 帳戶驗證次數變化
- 系統活動統計
- 程式執行統計
- 系統原則變動
- IP 位址統計

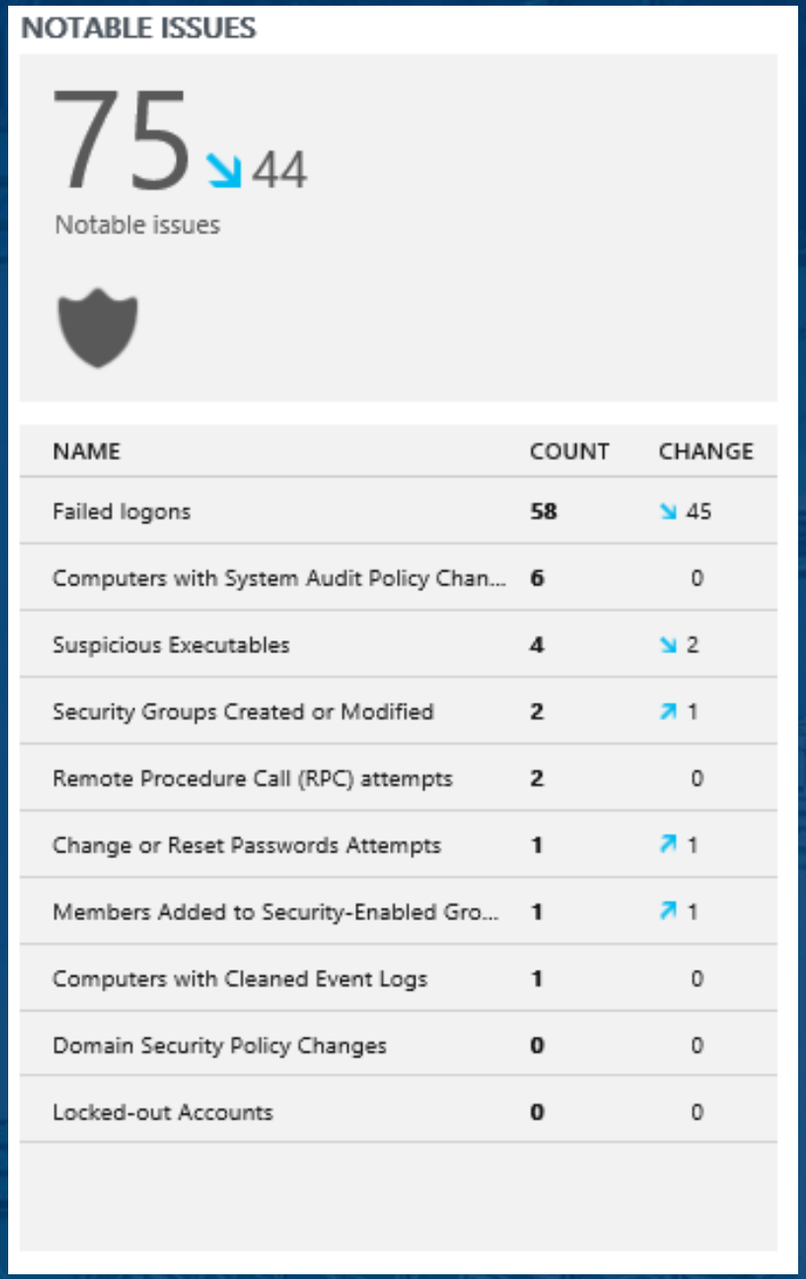


方案套件 – Security and Audit

Notable issues

顯示已收到的安全問題統計，
以及變動狀況

- 帳戶登入失敗
- 安全原則與群組變動
- 密碼重設
- 事件記錄清除
- 帳戶鎖定

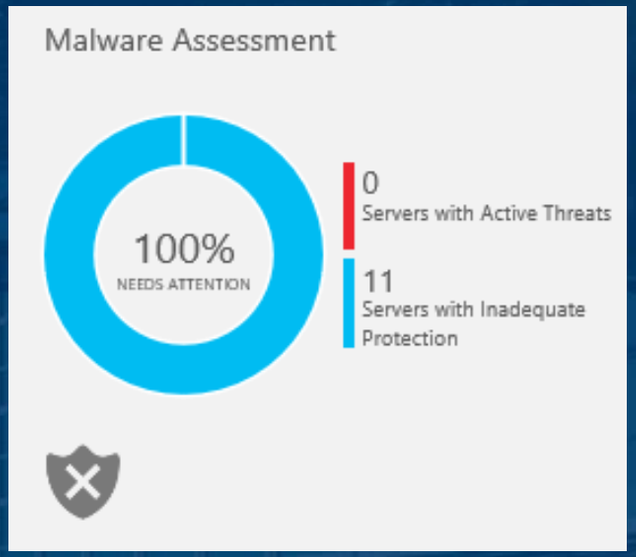


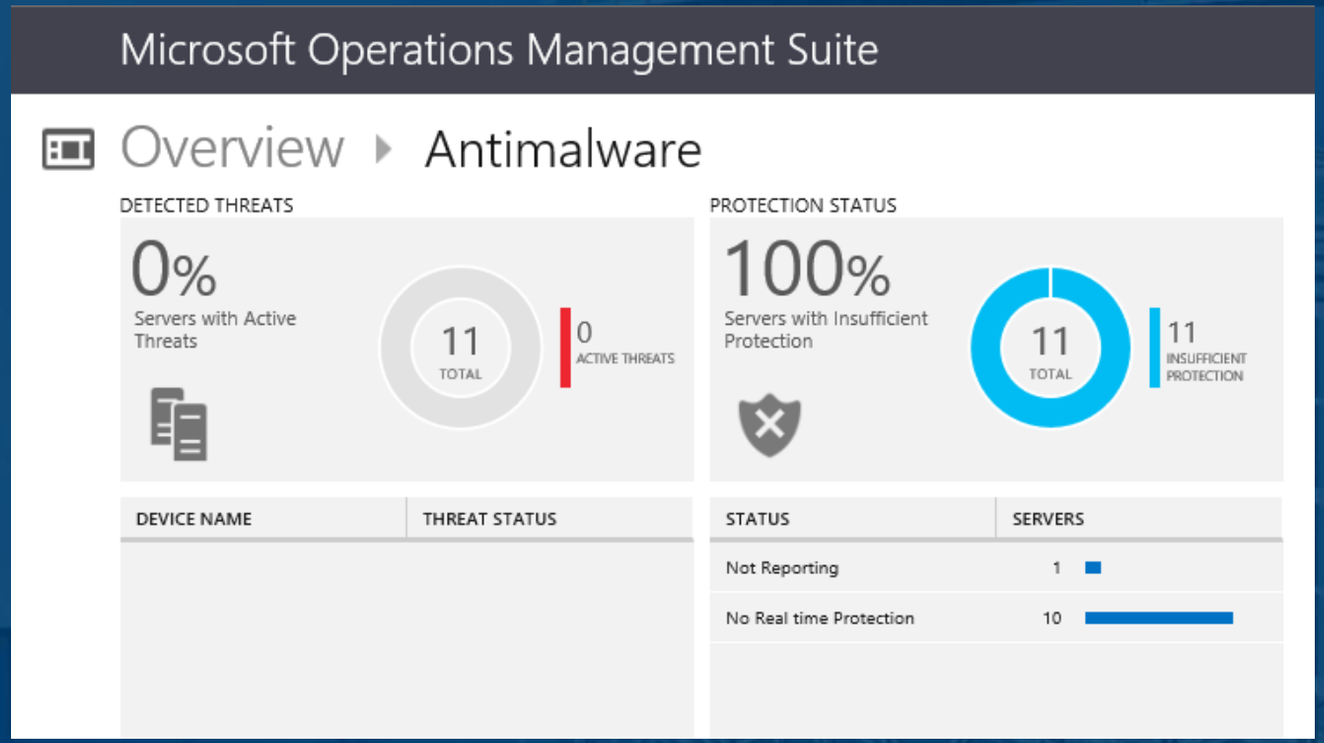
方案套件

Malware Management

收集受惡意程式感染或有高感染風險的伺服器資訊

- 已偵測到的威脅
- 系統保護狀態





方案套件

System Update Assessment

評估伺服器更新狀態

- 缺少更新的伺服器
- 最近未更新的伺服器
- 更新的套用與未套用統計
- 缺少的更新類型