技能解封初始篇章-非法隱身存取(Cloud App Security)

前言

<https://ithelp.ithome.com.tw/articles/10213972>

成本評估

**Cloud App Security 依下列定價面向計費：**

Azure Active Directory 共有四種版本：Free、Office 365 應用程式版本、Premium P1 及 Premium P2。Azure 訂用帳戶即包含免費版。您可以透過 [Microsoft Enterprise 合約](https://www.microsoft.com/en-us/licensing/licensing-programs/enterprise.aspx)、[開放大量授權計劃](https://www.microsoft.com/en-us/licensing/licensing-programs/open-license.aspx)與[雲端方案提供者](https://go.microsoft.com/fwlink/?LinkId=614968&clcid=0x404)計劃取得 Premium 版本。

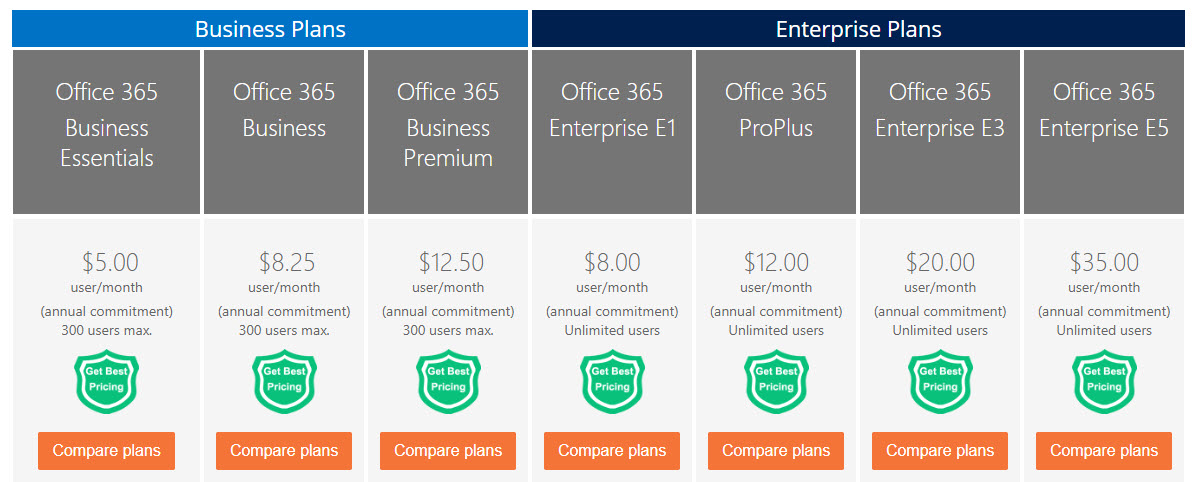
Azure 及 Office 365 訂閱者也可以線上購買 Azure Active Directory Premium P1 與 P2。於此處[登入](https://portal.office.com/Commerce/Catalog.aspx)購買。

一張含有 文字 的圖片

自動產生的描述

To **enable Cloud App Security**, you must have an **E5 license** or purchase the **Cloud App Security** add-on. To enable the alerts and monitoring capabilities, log onto the **Office 365 Security** and Compliance portal or the Microsoft **Cloud App Security** website.

**企業版本類型一次滿足**



常見E1 / E3 / E5 功能比較(本次驗證為 E5 約NT$1,135.00 每個用戶/月)

一張含有 文字 的圖片

自動產生的描述

Cloud App Security Q&A

**需要有何種權限才能存取 Cloud App Security？**

須在 Azure Active Directory 中為全域系統管理員、合規性系統管理員或安全性系統管理員。 僅有 Office 365 安全性與合規性中心具這些角色仍不具權限。

**PowerShell**

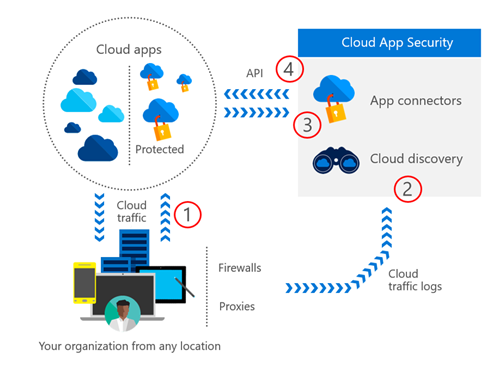
$cred = Get-Credential  
Connect-MsolService -credential $cred  
Add-MsolRoleMember -RoleName “Compliance Administrator" -RoleMemberEmailAddress “XX@XX.XX"

or

Add-MsolRoleMember -RoleName “Security Administrator" -RoleMemberEmailAddress “XX@XX.XX”

服務架構

1. 用戶正進行平日工作使用雲端應用系統。
2. Cloud App Security 分析來致用戶端的存取其雲端之間的流量確保正常使用應用程式之行為。
3. 管理者審核應用程序，可選擇放行或限制。
4. 利用雲端上的應用程序 API界接來持續監控來實現合規和威脅分析。



**前置作業**

測試可以透過免費 90 天的管道自行依條件申請即可．(此申請帳戶需要在AAD為全域管理員權限)

簡易環境示範

圖1. O365 E5已經有授權後就需要指派指定的用戶可以擁有此功能

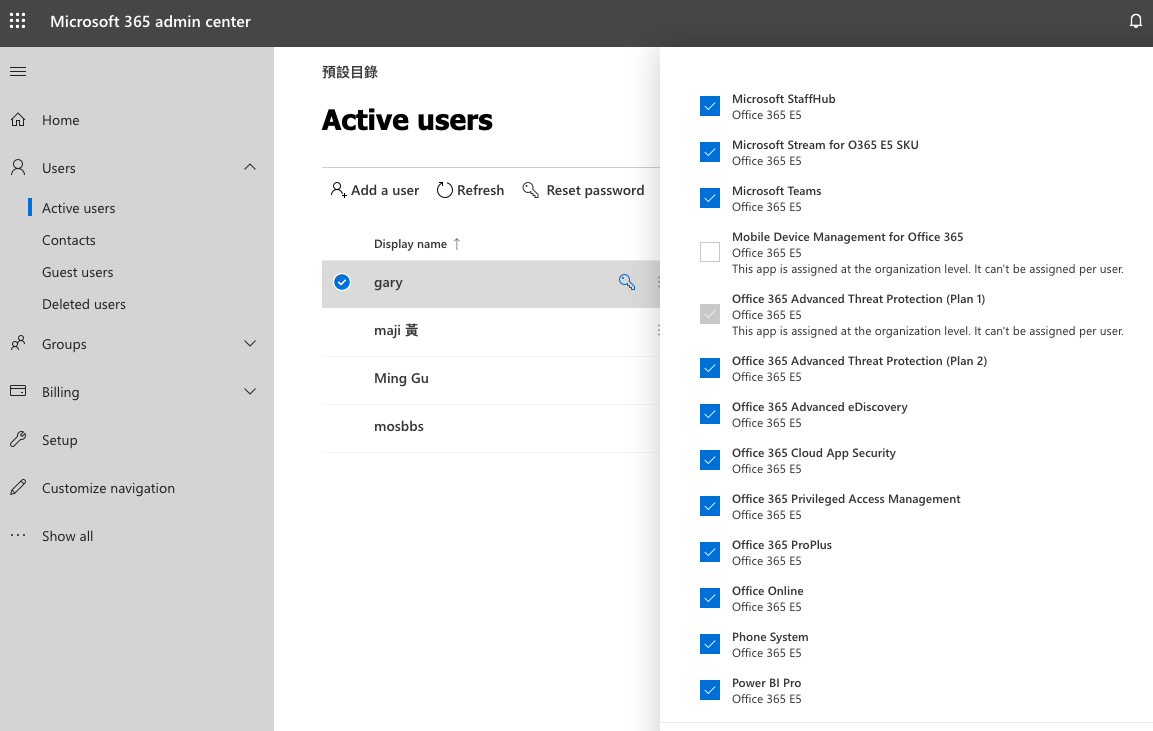


圖2. 回到O365找到Security功能並點擊

一張含有 文字 的圖片

自動產生的描述

圖3. 新的畫面出現了，在官方文件上根本就還沒更新．．直接進入新頁面

一張含有 文字 的圖片

自動產生的描述

圖4. 關鍵啟用畫面在此，已經被放到進階警示的功能之下，花了好一會功夫才找到．．(其實有問我朋友)

一張含有 文字 的圖片

自動產生的描述

圖5. 回到 Azure 找到剛剛申請的授權清單已經有一包O365 E5的授權

一張含有 桌 的圖片

自動產生的描述

圖6. 針對群組指定所附有的授權後就可以為後續的帳戶方便給此群組即可

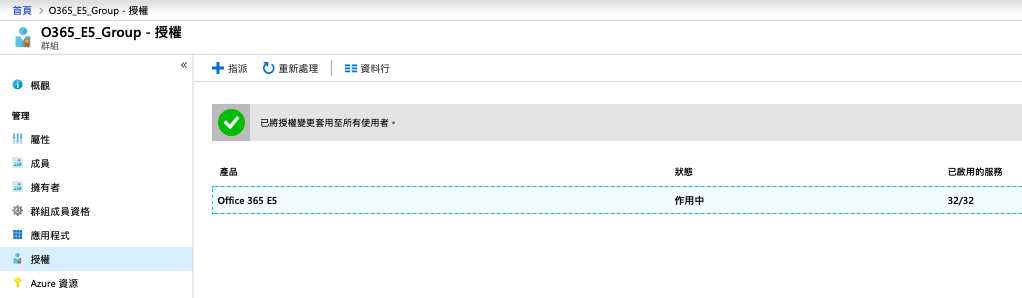


圖6. 一開始其實時麼都沒有登入進去Cloud App Security 功能最有感的就只有規則與政策

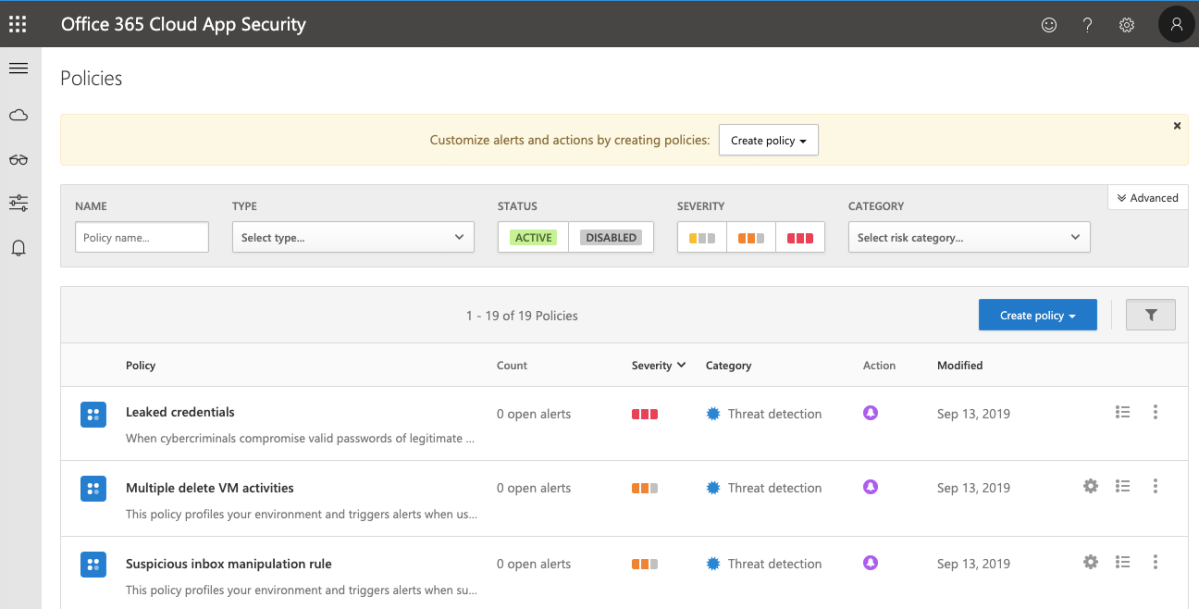


圖7. 主要能透過既有的原則與範本來最選擇設置你想監視的標的上一張含有 文字, 螢幕擷取畫面, 室內 的圖片

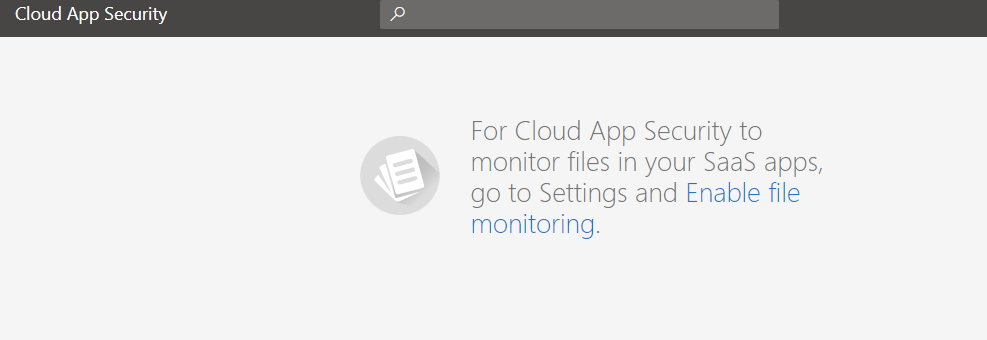
自動產生的描述

圖8. 建立規則時就會發現…..

一張含有 文字 的圖片

自動產生的描述

圖9. 針對每種規則監視的AP類型不同都有特別需要啟用

圖10. 啟用檔案監視並完成存檔

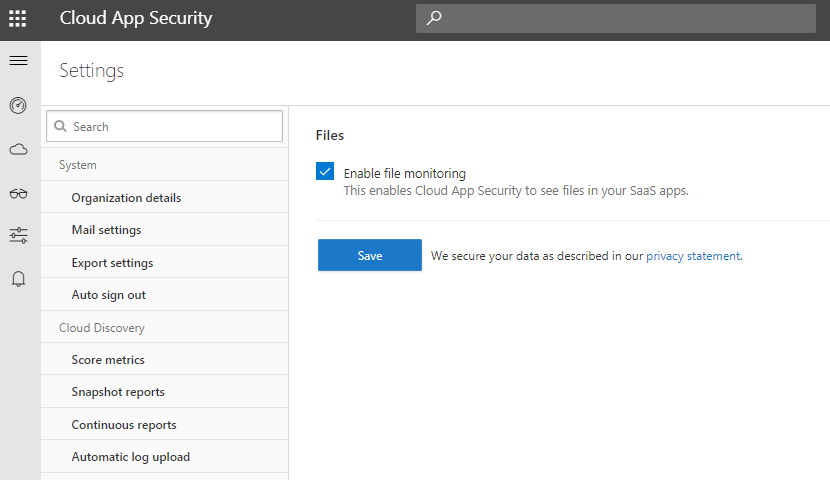


圖11. 舉例針對OneDrive及Sharepoint針對隨意分享檔案的行為進行警示通知

一張含有 文字, 螢幕擷取畫面, 膝上型電腦 的圖片

自動產生的描述

圖12. 先以傳送警示郵件為主

一張含有 文字 的圖片

自動產生的描述

圖13. 回頭看儀表板有抓出各種資源包含應用程式,帳號與檔案等(應該是需要同步時間故一開始時沒有任何資源的)

一張含有 文字 的圖片

自動產生的描述

圖14. 以自己為例就看到有在登入執行的歷程

一張含有 文字, 螢幕擷取畫面, 室內 的圖片

自動產生的描述

圖15. 沒錯，我剛剛真的有進入到Onedrive做檔案分享…

一張含有 文字 的圖片

自動產生的描述圖16. 同時連結到Azure訂閱中資源檢視安全性

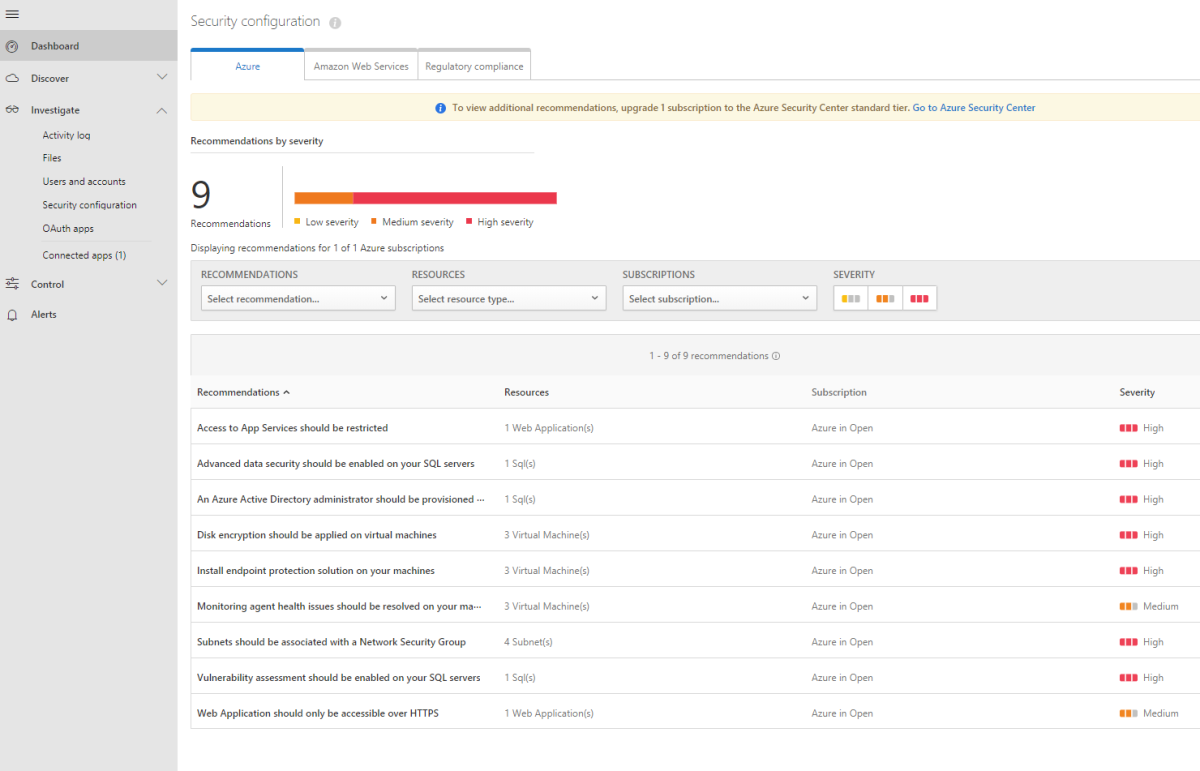
圖17. 比對Azure 資訊安全中心是一致的

圖18. 透過OAuth驗證的網站

一張含有 文字, 螢幕擷取畫面, 室內, 數個 的圖片

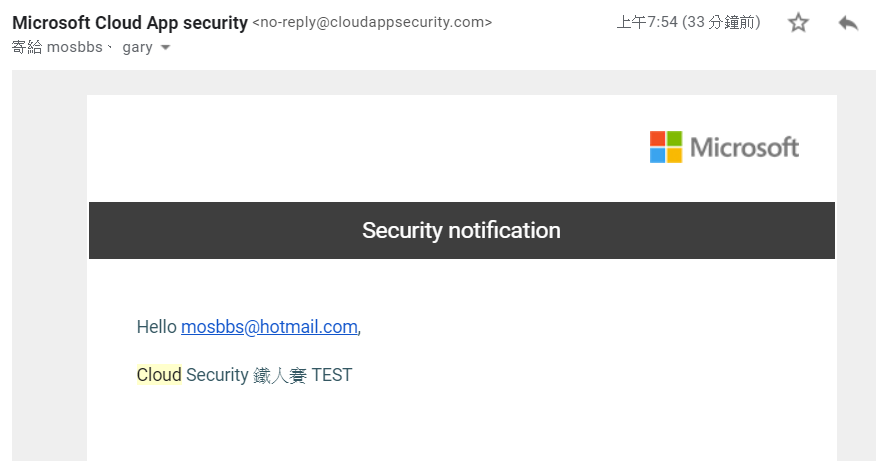
自動產生的描述

圖19.包含外部的AP真的非常多元就視需求來做進一步監視

一張含有 文字 的圖片

自動產生的描述

先前建立的規則觸發收到警示通知



一張含有 文字 的圖片

自動產生的描述