

Find, prioritize, fix, and enforce
Microsoft 365 security controls.

Microsoft 365 安全協作



全面查找 & 優先處理

彙整整個Microsoft 365的存取、敏感性和活動資料。根據您對風險的定義自動對問題進行優先排序並符合相關法規和安全政策規定。Insights洞察出您最關心的問題，無論是過度分享、匿名連結甚至是影子帳號。



時時監控 & 自動修復

安全儀表板突顯出危險的匿名連結、過度暴露的敏感內容等等。深入瞭解已知和潛在的問題。自動修復權限和分享設定的問題。

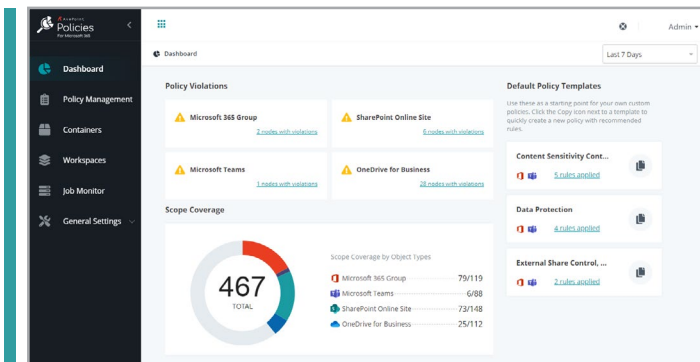


強制執行 & 事先預防

使用自動化政策來防止配置漂移。政策觸發警報或回復未經授權的更改和風險操作。隨時間推移追蹤改進，實現安全協作。

嚴密安全政策成就協作佳話

PI使您生成整個租戶的安全報告變得容易，但您又如何得知是否存在問題呢？PI透過加入前後文理解的機制改變了傳統的安全報告。橫跨Microsoft Teams、Groups、SharePoint和OneDrive收集敏感資訊和活動資料，確保優先處理您最首要的問題。最後，自動化的權限和設置修復，政策強制執行，將全面保護您的數位工作區。



INSIGHTS

- 彙總Microsoft 365權限和安全資料，包含活動和敏感資訊類型。
- 報告租戶內的權限資料，或深入到Teams、Groups、SharePoint和OneDrive以監視特定的服務或使用者。
- 根據您對風險的定義對關鍵問題進行優先順序——基於Microsoft 365敏感資訊類型、敏感度標籤以及您對風險定義的方式。
- 從Microsoft的敏感資訊範本中選擇符合您的行業或地區的範本，或在Microsoft 365安全與合規中心裡建立您自己的範本。
- 使用我們建議的暴露定義，或調整大型團隊和外部使用者設置。
- 風險評分突出高優先順序的問題，如過度暴露的敏感內容或不過期的匿名連結。
- 深入瞭解已知或潛在的問題，並利用內容活動歷史和內容敏感性的完整背景，直接從報告中進行編輯。
- 單一或整批執行終止、刪除或編輯已授予給外部使用者、影子帳號或透過匿名連結存取的權限。
- 獲取文件的風險級別、暴露程度、存取權限和使用者活動等詳情訊息。
- 將特定範圍內的管理權限委託給一組特定的專用帳號。
- 安全儀表板顯示了匿名連結、外部使用者存取和影子帳號的風險遞減趨勢及進展情況。

POLICIES

- 根據洞察力或公司的準則來制定自動執行的政策。
- 應用預設範本快速建立應用推薦規則的政策來管理敏感內容、外部分享和資料保護。
- 應用政策至Microsoft Teams、Microsoft 365 Groups、SharePoint及OneDrive，以確保協作安全。
- 監督違反既定政策的行為，確保持續執行。
- 防止過度外部分享和未經授權的對權限和安全設置的更改。
- 每2小時提醒或恢復違反政策的更改。
- 基於Microsoft活動資料觸發政策執行。
- 輕鬆點選即可存取和修復違規操作。
- 30+ 現成政策可供選擇，根據情境需求選擇性地將規則應用到數位工作區，例如metadata或敏感資訊類型：

For your SharePoint Online, OneDrive, Groups, and Teams:

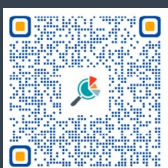
- 分類變更限制
- 外部分享設置
- 刪除影子帳號
- 存取要求設定
- 掃描外部使用者
- Teams設定強制執行

[完整清單 \(英文\)](#)

For Your Entire Tenant:

- 幽靈使用者偵測
- Tenant-Level網站內容外部分享設定
- 國際垃圾郵件防範
- 惡意軟件防範
- 匿名日曆共用控制
- Exchange Online PowerShell存取規則
- 信箱審核

[完整清單 \(英文\)](#)



••• 瞭解更多 •••

AvePoint Taiwan

- Sales_tw@avepoint.com
- www.avepoint.com/tw
- www.facebook.com/AvePointTW

Partner