Acronis 安克諾斯 Cyber Backup

請立即啟動 Acronis Active Protection
安克諾斯主動防禦勒索軟體

設定說明

湛揚科技總代理
www.t-tech.com.tw

親愛的安克諾斯用戶，您好!!

請立即啟動 "Acronis Active Protection" 安克諾斯獨家功能，有效遏止加密勒索攻擊，提升資安層級，保護貴重資料安全。

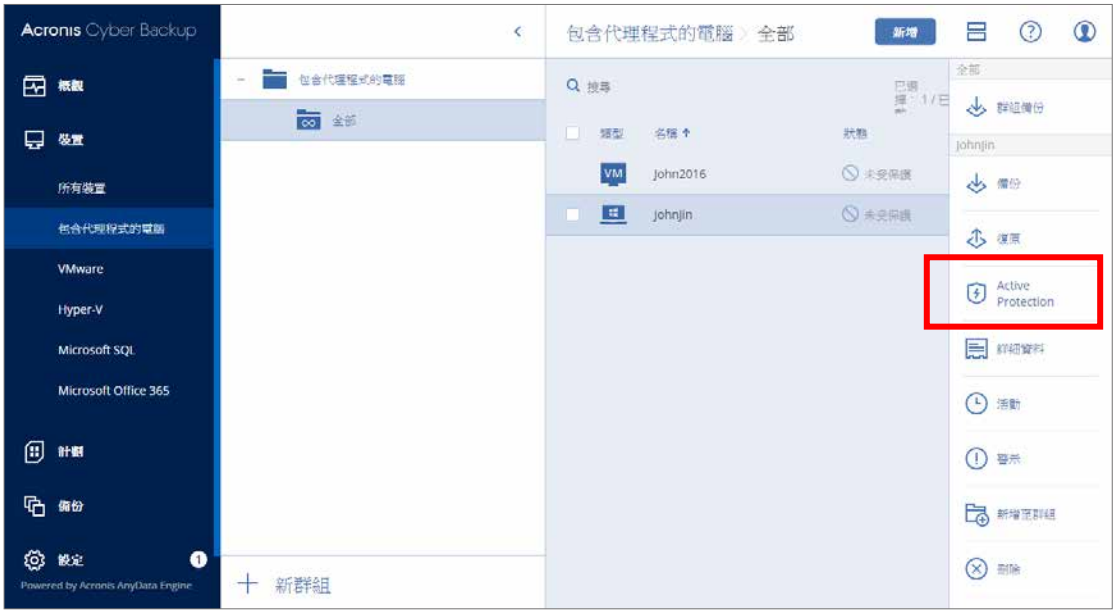
啟動 Acronis Active Protection 的功能，可有效防止端點和伺服器的檔案被加密(需安裝安克諾斯代理程式)，也可以有效防止端點和伺服器的電腦被當成挖礦電腦使用。

建議 Acronis Cyber Backup 的用戶，版本為下表所列之客戶 (Update 1 Ver.7970，Update 2 Ver.9010，Update 3 Ver.10130)，提醒您盡早升級至最新版本(目前官方最新版本為 Update 5 Ver.16180)，且檢查 "主動防禦" 的功能是否已開啟，如未開啟，請依照下列步驟設定。

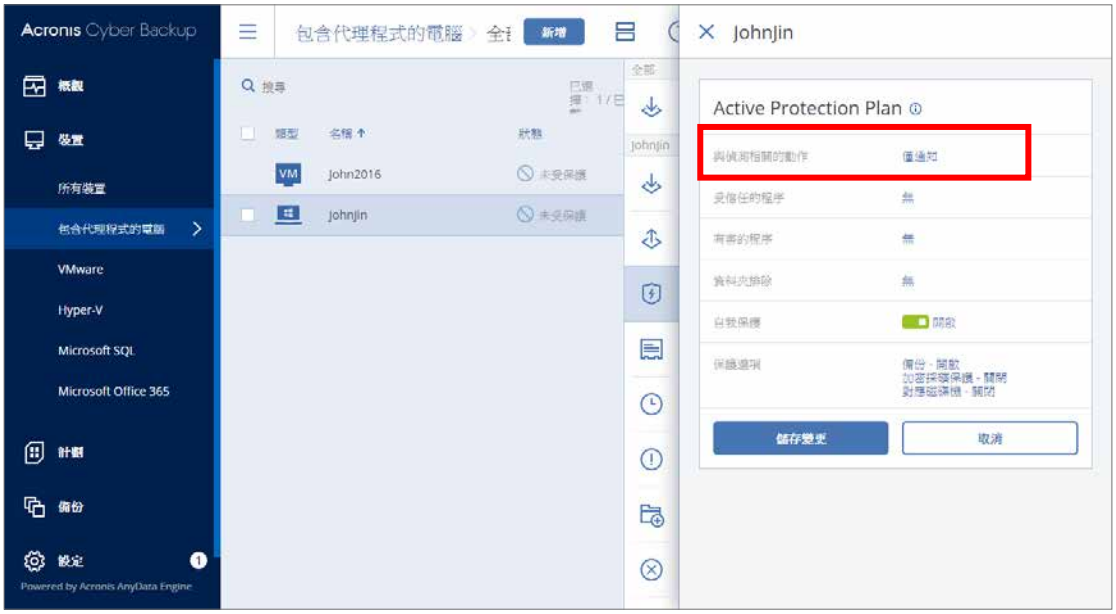
近期因加密勒索猖獗，災情頻傳，湛揚科技貼心提醒您，安克諾斯具有主動防禦加密勒索的功能，於偵測到大量檔案竄改行為時，系統發出警告訊息，阻斷加密攻擊程序以及復原被加密檔案之行為，具有復原檔案之功能。湛揚科技與您一同加強資安防禦，降低被加密之風險。

如有其他相關問題，請電洽湛揚科技技術服務中心(02)7718-5588

1. 請點選裝置>包含代理程式的電腦，再點選【Active Protection】

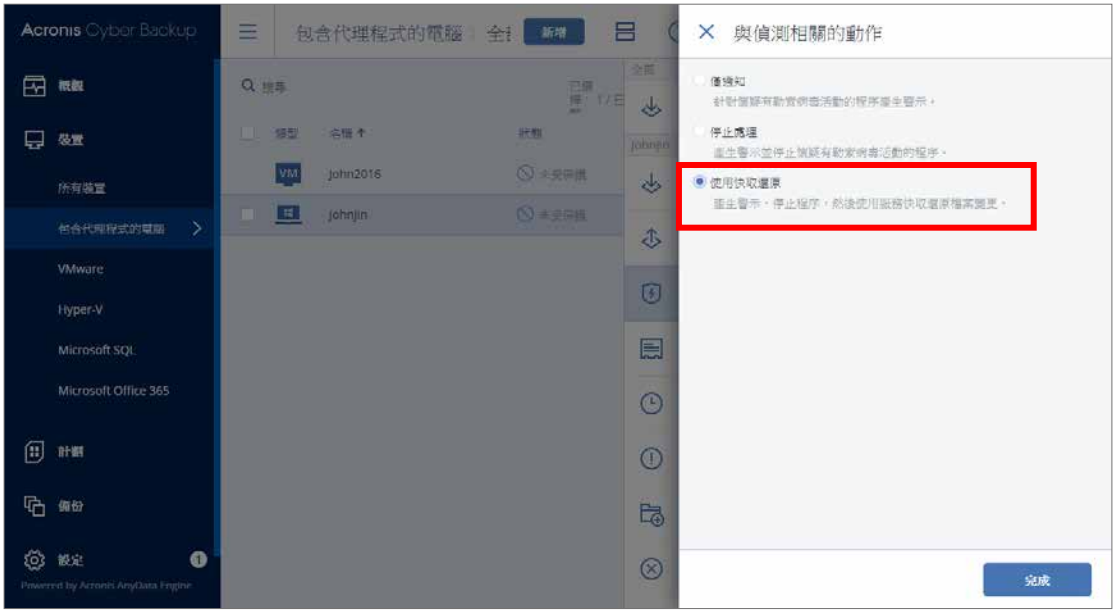


2. 請確認【與偵測相關的動作】，若是顯示【僅通知】，請點選該選項進行修改

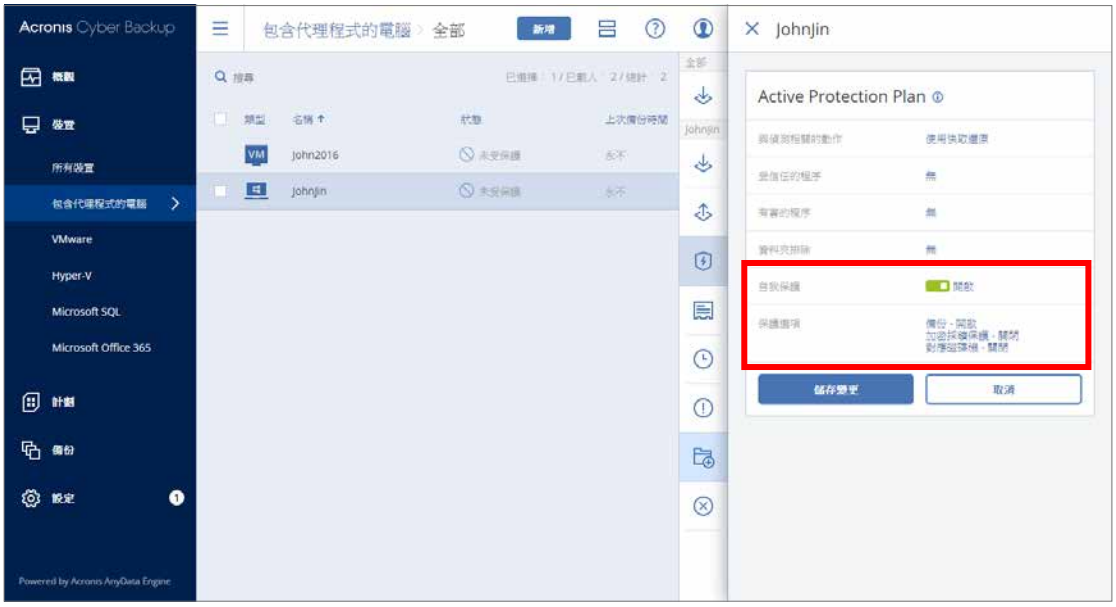


3. 以下為【與偵測相關的動作】的行為說明

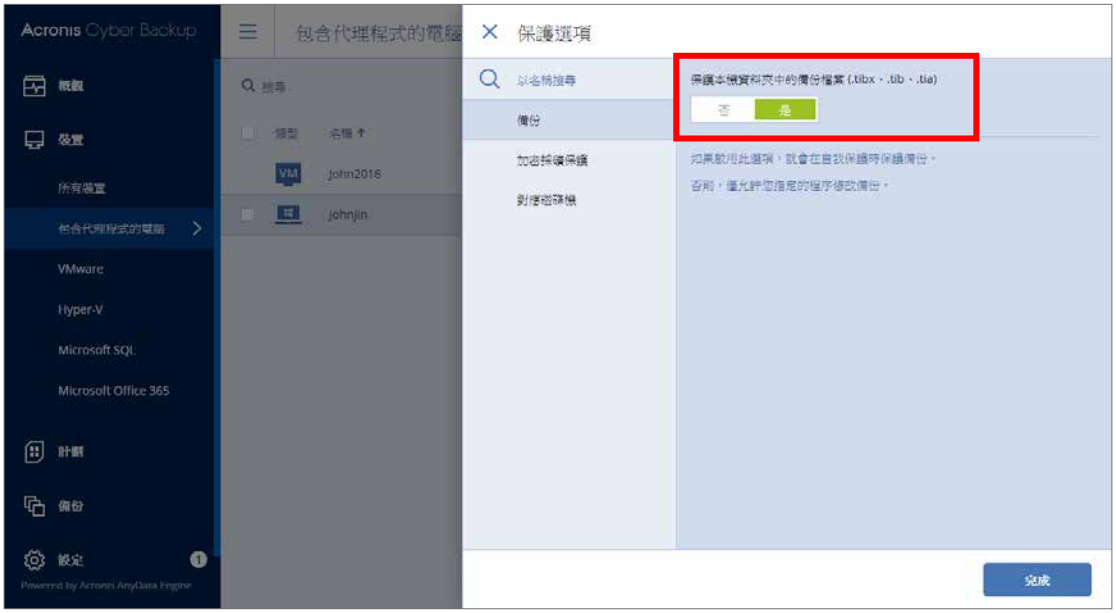
【僅通知】在中控台產生勒索病毒的警示
【停止處理】在中控台產生勒索病毒的警示，同時阻止勒索軟體的程序。
【使用快取復原】在中控台產生勒索病毒的警示，阻止勒索軟體的程序，同時可以透過快取還原被勒索軟體加密的檔案，建議選擇此選項。



4. 設定完成後，請檢查【自我保護】功能是否在開啟狀態，請點選【保護選項】。

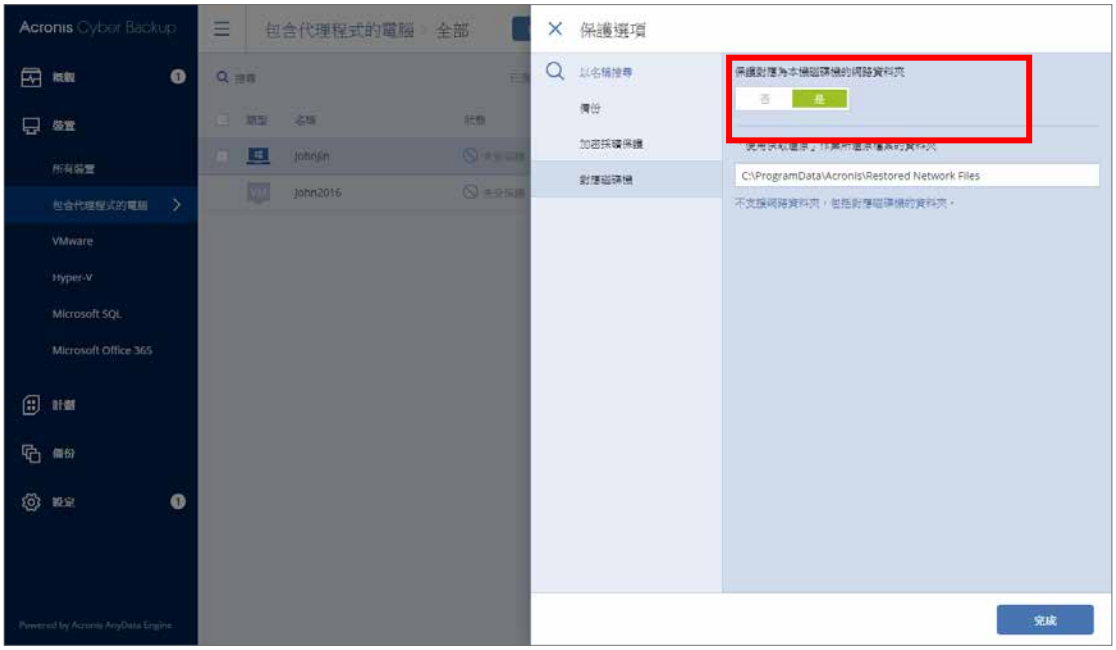


5. 在【備份】的選項請選擇【是】，以保護該台裝置內的備份存檔

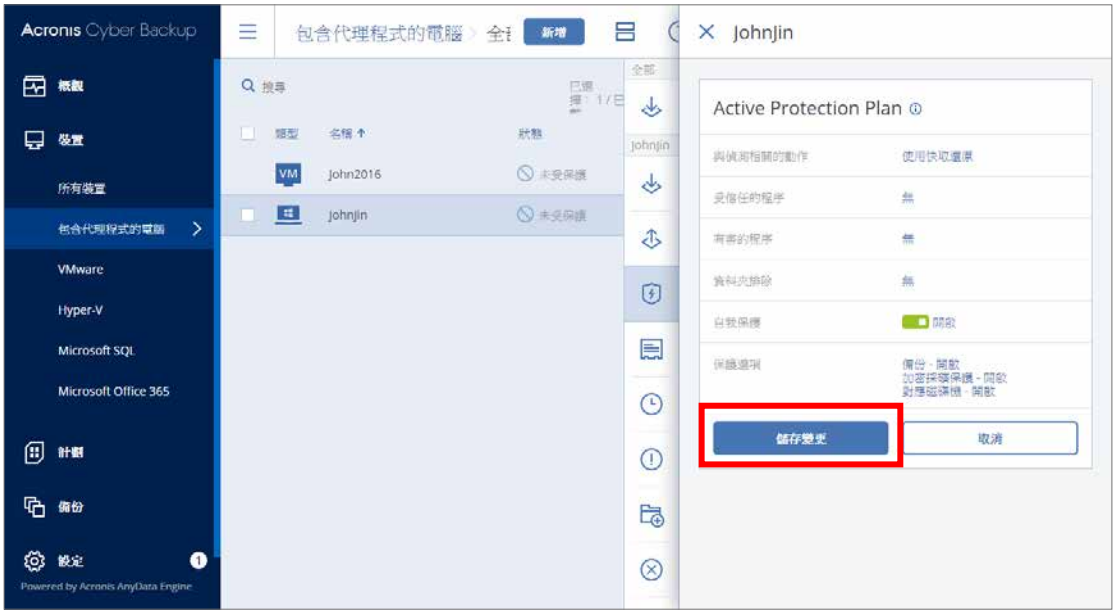


6. 若要開啟挖礦保護，請點選【是】

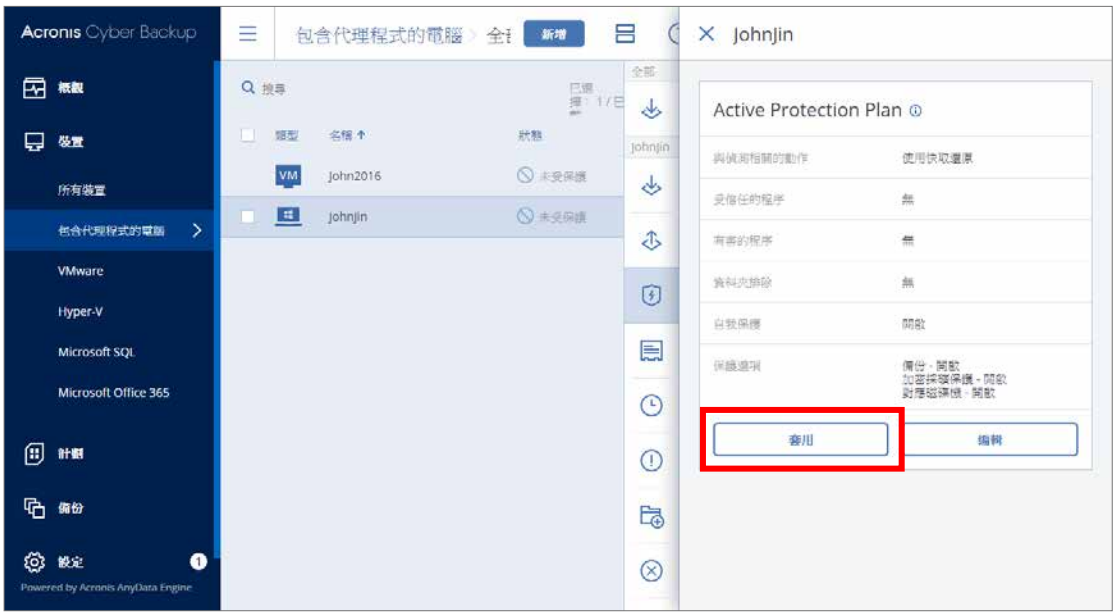
7. 對應磁碟機的功能請點選【是】。



8. 完成後請點選【儲存變更】。

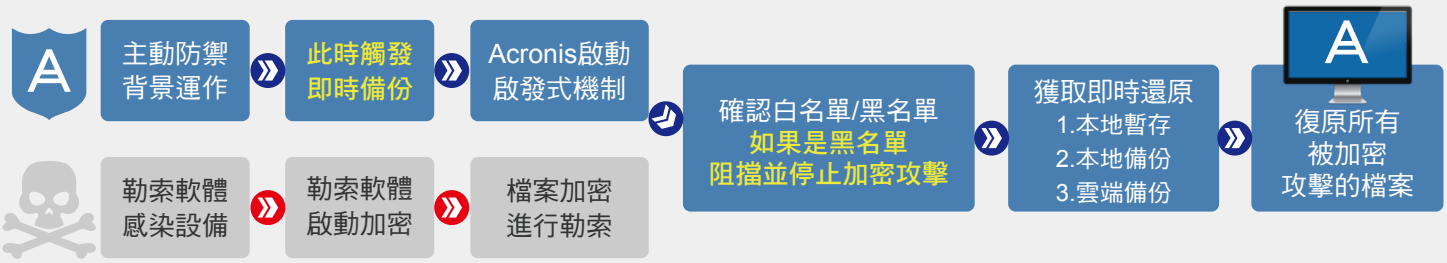


9. 請再點選【套用】，完成主動防禦功能的設定。



Acronis Active Protection™ 主動防禦技術 獨家

保護資料免受勒索軟體威脅



Acronis Active Protection™ 是一種先進的勒索軟體防護技術，主動保護電腦上的所有資料，包含文件、所有類型的資料和您的Acronis備份檔案，其運作方式如下：

- 智能檢測模式：智能檢測惡意行為，即便是來自從未被發現的勒索病毒變種也無法閃避。
- 白名單和黑名單：建立黑白名單，防止授權活動被誤標為未授權。
- 備份檔案的自我防衛：自我防禦機制，不讓犯罪分子干擾Acronis 程式執行與備份檔案內容。
- 檔案復原：Acronis Active Protection™ 可檢測、比對和復原任何大小的檔案！

安克諾斯 Acronis 是唯一經過 AV-TEST 測試並被證實可以主動防範勒索軟體的備份產品。Acronis Active Protection™主動防護勒索軟體技術已運用於Acronis True Image 2020與Acronis Cyber Backup 12.5。更多關於Acronis Active Protection™ 請參閱 https://www.t-tech.com.tw/ActiveProtection.php

經AV-TEST認證可主動
防禦勒索軟體攻擊的備份軟體

若您對產品有任何疑問，歡迎洽詢安克諾斯 Acronis 台灣總代理 湛揚科技

湛揚科技 Acronis 總代理 www.t-tech.com.tw
台北：(02)2735-3512 技服電話：(02)7718-5588
高雄：(07)972-7388 技服信箱：support@t-tech.com.tw