

# 用ASUSTOR NAS全面防範！ 擊退Ransomware的加密勒索 與網路攻擊



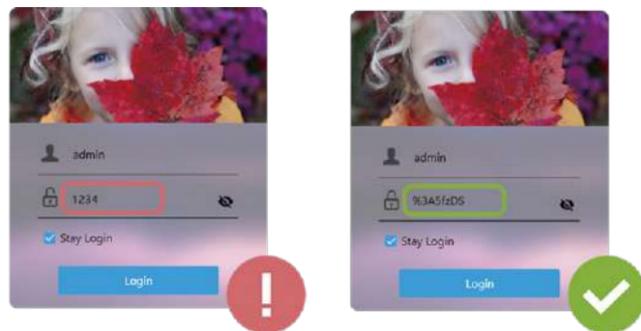
或許你對Ransomware這個名字很陌生，不過只要提到「病毒」兩個字，相信你一定膽顫心驚，知道防範它有多重要了！Ransomware是一種特殊的惡意軟體，又稱勒索病毒，它會惡意加密你的檔案與文件，使你的檔案無法開啟，進而失去對自己系統或資料的控制，甚至遭到機密資訊外洩的風險。在這個情況下，你的系統或資料等於成為了「人質」，而你必須支付「贖金」給綁架資料的駭客，以取回對自己系

統、文件的控制權。

從今年初到現在，國際間已有多家知名企業及政府機關遭到Ransomware的勒索攻擊，進而導致必須停工的情況發生。而面對這樣代價不小的惡意攻擊，相較於其他繁複的防毒措施，完善的備份作業絕對是最簡單又有效的不二法門，而ASUSTOR NAS全方位的備份功能，正是抵禦勒索軟體的最佳利器！

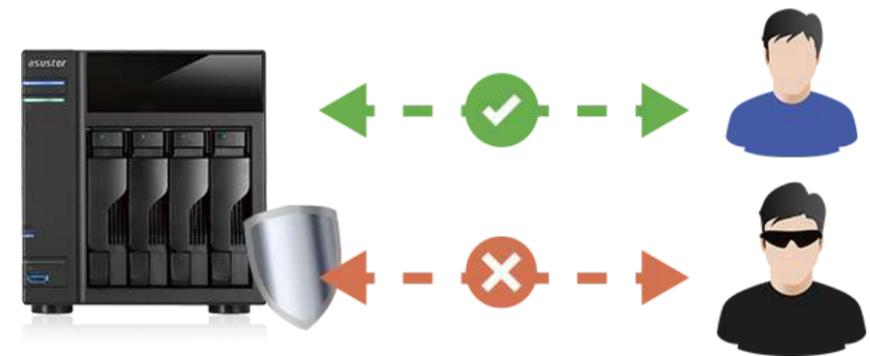
## 1 建立防毒正確觀念，從更新密碼及在安全環境下存取資料開始

許多人設定密碼時，都會為了方便而設定簡單的組合，但這會讓駭客很輕易的就猜到並且竊取資訊。因此設定密碼時，必須謹記使用「8位數以上、大小寫字元、數字符號混和」的原則，並定期更新密碼，才能有效避免駭客入侵。除此之外，也要避免在公共電腦上面或是使用免費的WiFi，或是瀏覽不安全的網站與隨意下載來路不明的檔案影片，因為這些都會讓病毒輕易的進入到電腦裡。



## 2 使用ASUSTOR NAS的五大必要防護措施，缺一不可！

1. 隨時將ADM更新至最新版本：面對駭客針對漏洞層出不窮的攻擊，ASUSTOR ADM作業系統會持續修改可能出現的漏洞，以確保資料的安全性，因此時時更新ADM到最新版本十分重要。
2. 建立擁有管理權限的新帳號：預設帳號「admin」過於簡短，很容易被猜到，加上如果使用簡易的密碼，很輕易就會被駭客入侵，因此設立新的使用者帳號及高強度的密碼可有效預防。
3. 開啟ADM Defender防火牆及網路防護 (Firewall and Network Defender)：至Network Defender啟用自動黑名單以防止惡意網路攻擊及嘗試登入，
4. 不須使用SSH及SFTP服務時將其停用：如果你沒有使用SSH及SFTP服務，需先將其長時間停用。等到需要使用的時候再啟用，並養成使用完停用的習慣。
5. 避免使用8000及8001等預設連接埠：使用預設的連接埠8000及8001，有機會被駭客猜到，建議自行設定不一樣的連接埠。



## 3 牢記備份321原則，建立萬無一失的檔案備份

只要謹記備份321原則：「至少製作3份備份+將備份分別存放在2種不同儲存媒體+至少1份放在異地保存」，就能建立有效的備份策略。而建立多種備份，更可以在不幸遭遇勒索病毒或駭客入侵之時，也能快速將資料復原。在ASUSTOR NAS上，有多種的基本備份組合可以讓使用者選擇來達到備份321的原則：

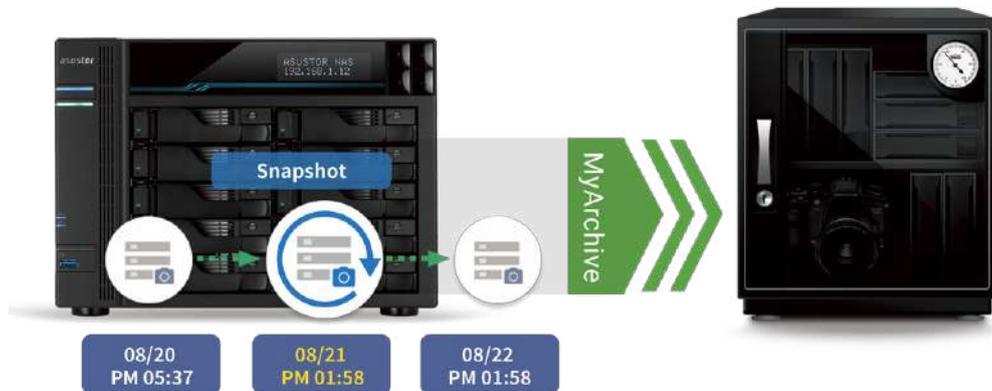
- 備份至公有雲如Dropbox、Google Drive、Microsoft OneDrive等等
- 備份至MyArchive硬碟
- 備份至本地端電腦
- 備份至遠端NAS
- 備份至外接式儲存裝置
- Btrfs快照中心



## 4 利用MyArchive和Btrfs快照，強化保護已備份的資料

透過ASUSTOR的特色功能——MyArchive進行離線備份，使用者可以將重要資料儲存在MyArchive硬碟並置於獨立於NAS的不同環境，也將不同屬性檔案進行分類，同時進行硬碟加密，增加其安全性。除此之外，ASUSTOR快照中心可設定排

程定時或手動即時建立快照，協助用戶在資料毀損或是遇到勒索軟體等意外狀況時，快速還原重要檔案到過去的版本與時間，同時整合Btrfs快照及iSCSI LUN快照兩種功能，將所有快照檔案集中管理、讓資料還原更加便利。



## 5 若真的被勒索軟體感染，可以透過Snapshot Center協助還原檔案

如果發現自己的NAS不幸被勒索攻擊，千萬不要慌張！首先該做的事情是先停用WiFi或拔掉網路線，確認已無網路連線。接著，徹底清空NAS上所有內容及文件，但注意千萬不要誤刪備份檔案。最後，在確認NAS已無感染疑慮後，可透過ASUSTOR的Snapshot Center備份功能將事先備份的檔案還原至未感染前的版本。



只要建立好正確觀念並搭配ASUSTOR NAS的防護措施，即不必再擔心勒索病毒或是駭客入侵對我們造成影響，也能免去付出不必要的金錢與時間。有關防範Ransomware的詳細資訊，都可以在ASUSTOR官網上找到：<https://www.asustor.com/>。

