

QNAP

Security Counselor 讓你遠離資安風險

QNAP NAS 的安全評估中心



存放在 NAS 的資料，是重要的數位資產，常成為駭客覬覦的目標！

加密勒索是
一門好生意

明槍易躲
暗箭難防

職業

大學資管教授

狀況

某日發現共用資料夾無法使用。

作為

聯絡技術支援後，發現該 NAS firmware 為三年前的版本，已被新病毒入侵。

解法

更新 firmware 後才解決問題。以前他從來沒想到要更新。

真實案例一



職業

科技公司產品經理

狀況

在家裡安裝一台 NAS 存放照片，由於工作忙碌，很少連線到 NAS 的介面。

作為

有一天看到官網宣傳，得知有 Malware Remover 可以使用。掃描 NAS 後發現已被病毒入侵。

解法

執行 Malware Remover 後，成功將病毒移除。

真實案例二



從上述案例可以得知，資安風險跟用戶是否擁有技術背景無關，隨時保持警覺與擁有謹慎的網路使用習慣才是重點！

別讓人為疏失，成為資安防範的漏洞。



這樣的行為最危險！

- 管理者的權限遭到濫用
- 使用預設密碼及連接埠
- 系統及應用程式有漏洞
- 使用外網，但沒有安全配套措施
- 未即時發現系統感染病毒

Security Counselor 是什麼？

你是否擔心，在不知不覺的情況下讓 NAS 暴露於危機之中？

該如何發現危機？化險為夷

Security Counselor 幫你找出風險，確保 NAS 環境安全無虞。

避險

檢查 NAS
有哪些風險。

排除

直接幫您套
用好安全的
設定。

防毒

集結病毒防
護和反惡意
軟體工具。

修補

軟體漏洞的
資安公告通
知服務。



為什麼要使用 Security Counselor ?

2018 年 7 月 NAS 用戶的資安事件應變調查

調查來源：台灣駭客年會HITCON Community 2018

當您懷疑帳號密碼被入侵

134 則回應

當您一直收到來路不明的 IP 試圖登入您的裝置

134 則回應

當您發現使用的軟體存在資安漏洞時

134 則回應

● 依照軟體開發商的資安公告，將軟體

74.6%

Security Counselor 協助您找出風險並設立安全機制，防範未然。

如果置之不理，受害者得付出龐大的代價.....

53%

的受害者本身沒有
察覺到安全漏洞

191

從病毒入侵到真正
察覺問題平均要花
上 191 天

66

從識別資安問題到
遏制平均又得再花
上66天

115^億美元

每年損失的成本

資料來源：2018 ixia 年度安全報告

使用 Security Counselor , 您每天平均所需的成本...



安全性檢查：3 步驟， 讓您的 NAS 變安全了！



Security
Counselor
如何使用？

1

執行檢查



2

查看報告



3

修正風險



安全性檢查範疇：

軟體更新
檢查



網路安全
檢查



帳號安全
檢查



存取權限
檢查



掃毒工具
檢查



認證安全
檢查



問題一

經常使用檔案傳輸服務、打開共享權限、忘記更改密碼或通訊埠預設值.....每天去注意這些行為，好麻煩！



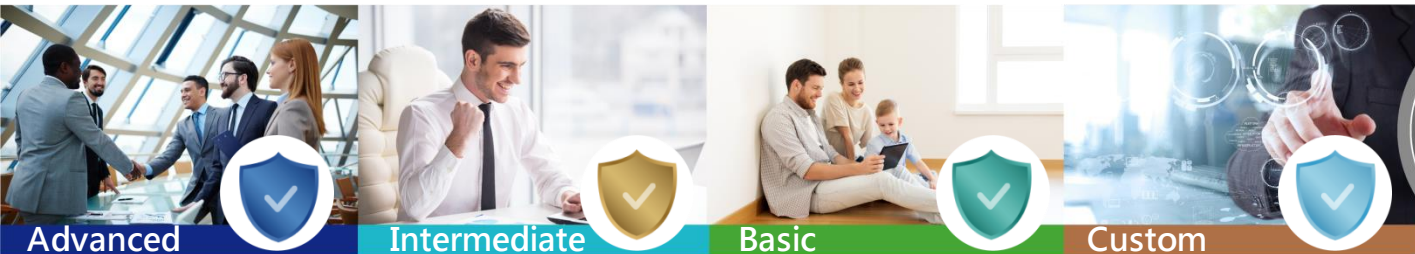
安全性等級： 提供不同需求的保護

NAS使用習慣百百種，對於安全性的要求也有所不同。

因此，Security Counselor 提供**基本**、**中階**、**高階**三種等級的保護，可依照您的使用需求，選擇最適合自己的安全性等級，讓您在受到保護之下，使用某些網路服務時能保有彈性，盡情發揮 NAS 的使用效益。

問題二

我時常要使用SSH, SAMBA/AFP 等服務，關閉相關設定雖能提高安全性，但卻也間接限縮了使用彈性！



一鍵設定： 系統幫您套用建議設定

有哪些服務用不到要關閉比較好？有什麼安全性方案可以使用？在什麼情況下做哪些設定，才不會讓 NAS 處於不安全的環境？

Security Counselor 都幫您規劃好了，除了引導您做最佳的設定，還能選擇系統直接幫您套用好建議設定，讓 NAS 處於較安全的環境。



問題三

NAS 的功能這麼多，該去哪裡調整相對應的安全性設定？該怎麼設定才安全？



集結掃毒工具： 安全管理，全盤掌握

- 病毒防護
- Malware Remover
- 安全性設定管理介面



問題四

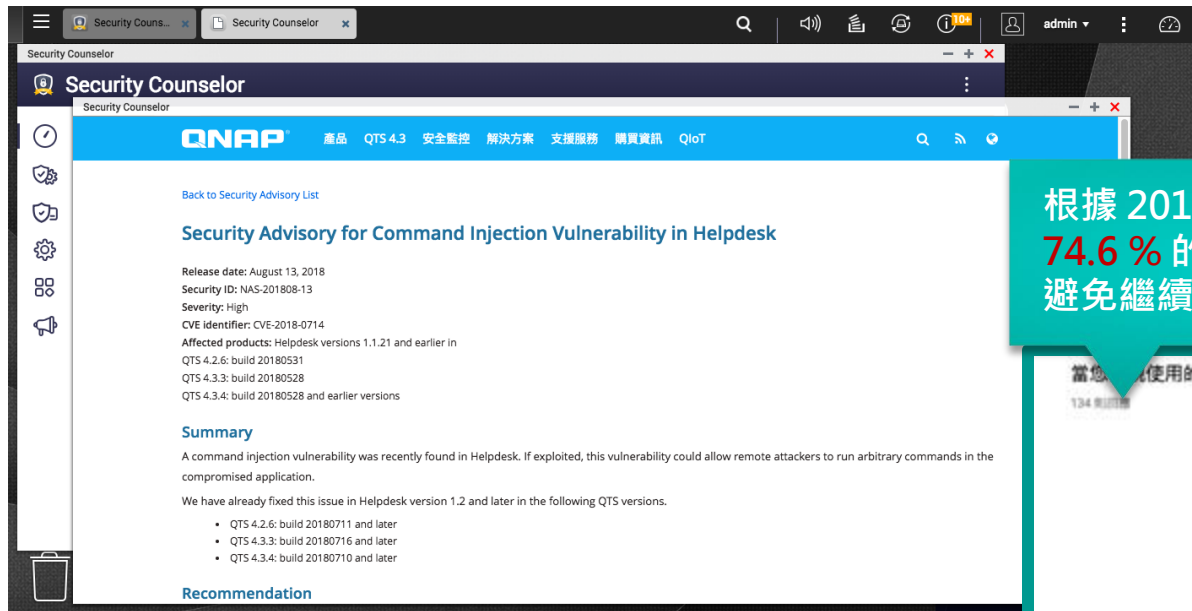
每週固定掃描、還要注意病毒碼是否有更新，正在掃毒的工具又有哪些？



資安公告通知：揭露存在漏洞軟體，以即時修正危機

問題五

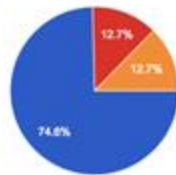
駭客及惡意軟體的威脅日益漸增，深怕有一天我也中標，到底該如何預防？



根據 2018 駭客年會調查，有 **74.6%** 的民眾仰賴資安公告，以避免繼續使用存在漏洞的軟體。

當您使用的軟體存在資安漏洞時

134 票選擇



- 依照軟體開發商的資安公告，將軟體更新至最新版本。
- 使用可防護漏洞的防火牆，例如：Virtual Patching (虛擬補丁)。
- 刪除此軟體。

你可以事先排除的風險

- 避免資料外洩
- 阻止可疑的登入
- 避免帳號密碼被駭客入侵
- 避免使用存在漏洞的軟體



Security Counselor
排除四面埋伏的風險，
讓你的 NAS 變得更
安全。



下載資訊：
請至 App Center 下載 **Security Counselor**

用戶回饋：
security_counselor@qnap.com



QNAP

