

Synology®

S Y N O L O G Y
2 0 2 0

迎接未來，相片管理的全新蛻變

滿足所有影像應用的管理工具



產品經理

Demi Chen

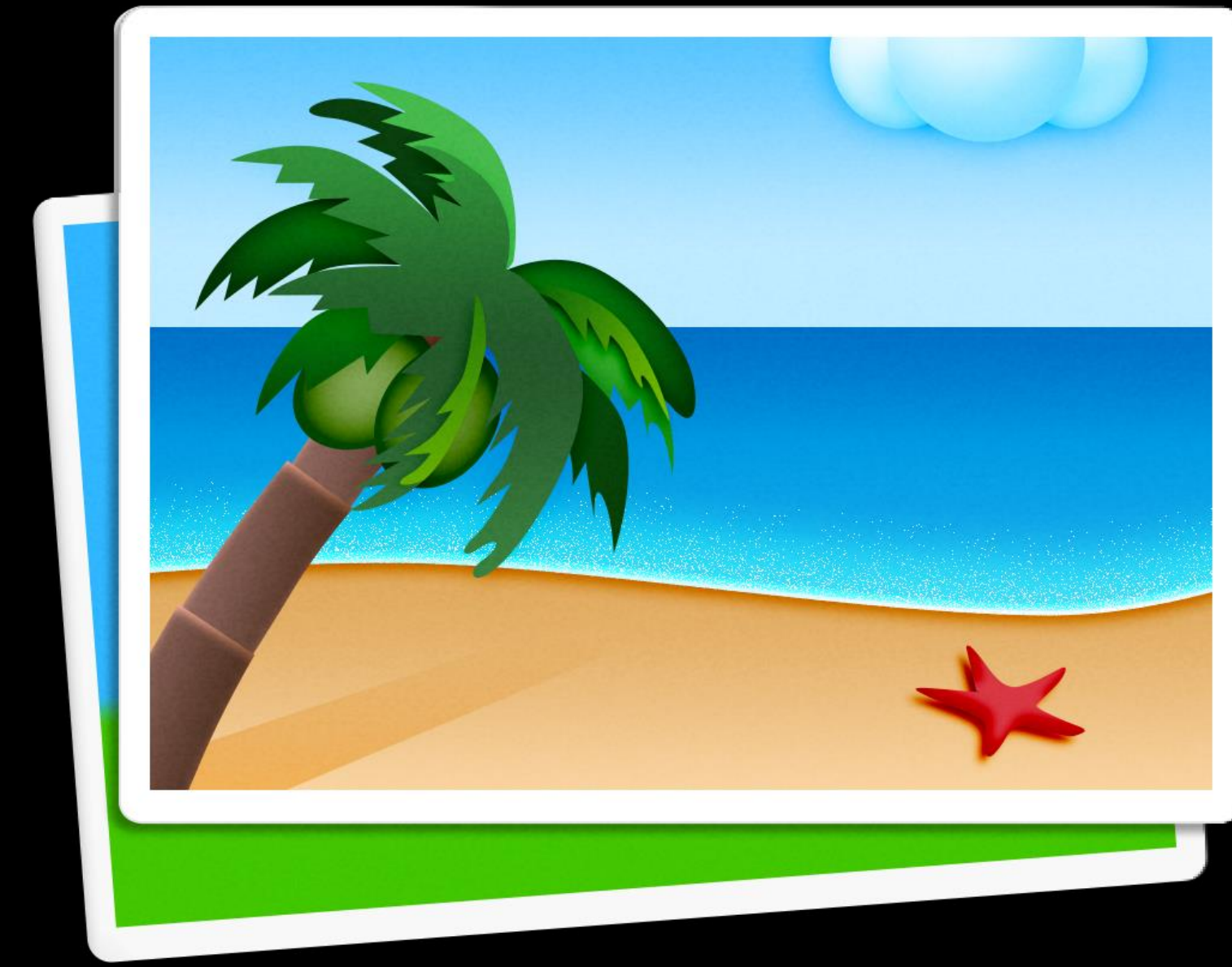


Photo Station



Moments

超過一半的 Synology 用戶
正在使用 Photo Station / Moments

全球共有 446 億 張照片存在於 Synology NAS 中
相較於 2017，相片總數量成長了 17.6 %



Photo Station



Moments



更人性化的時間軸檢視模式
自動建立人臉、地點相簿



實體資料夾的管理功能

純手機使用者

攝影愛好者

專業攝影師



上傳

整理

分享

瀏覽

搜尋

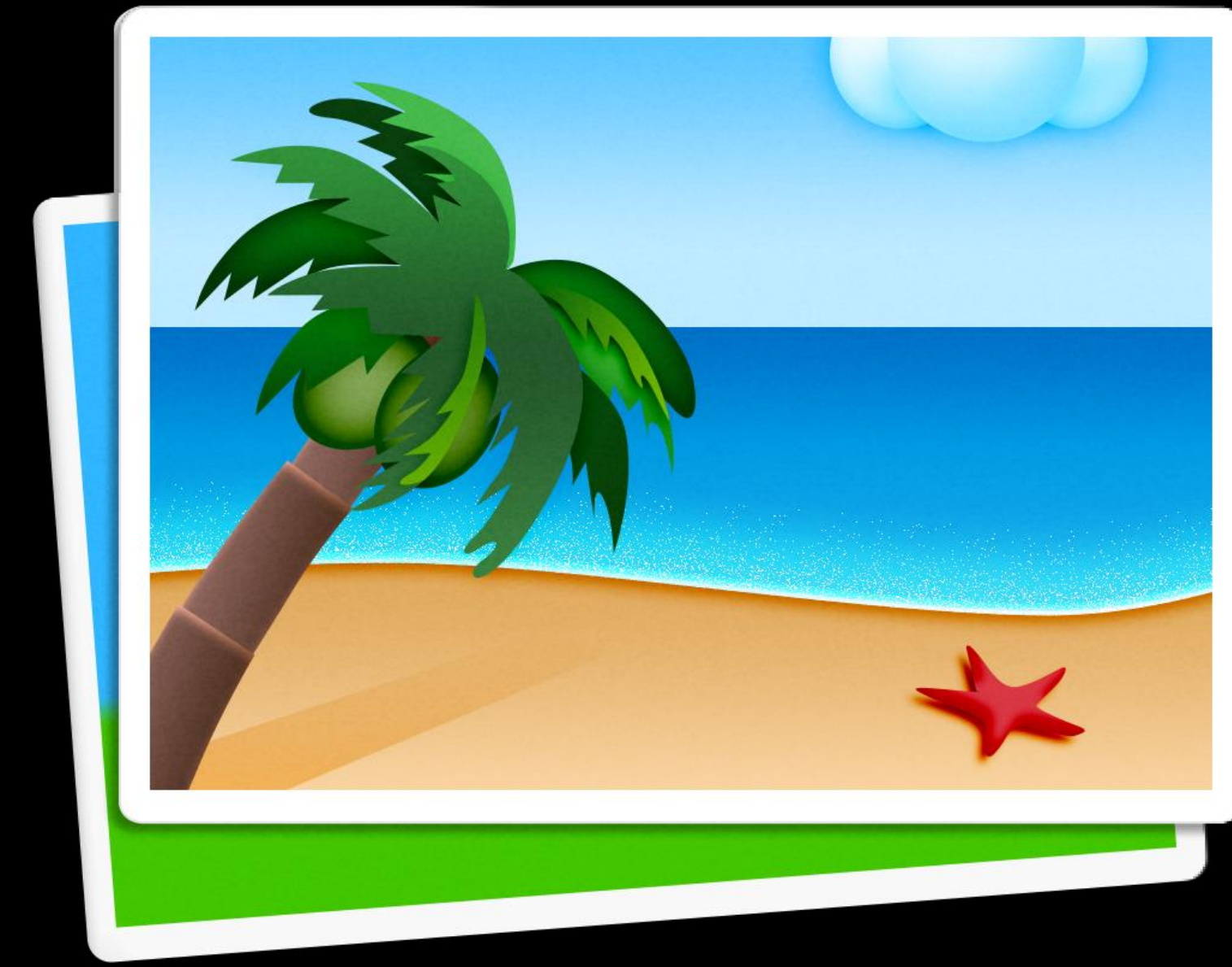
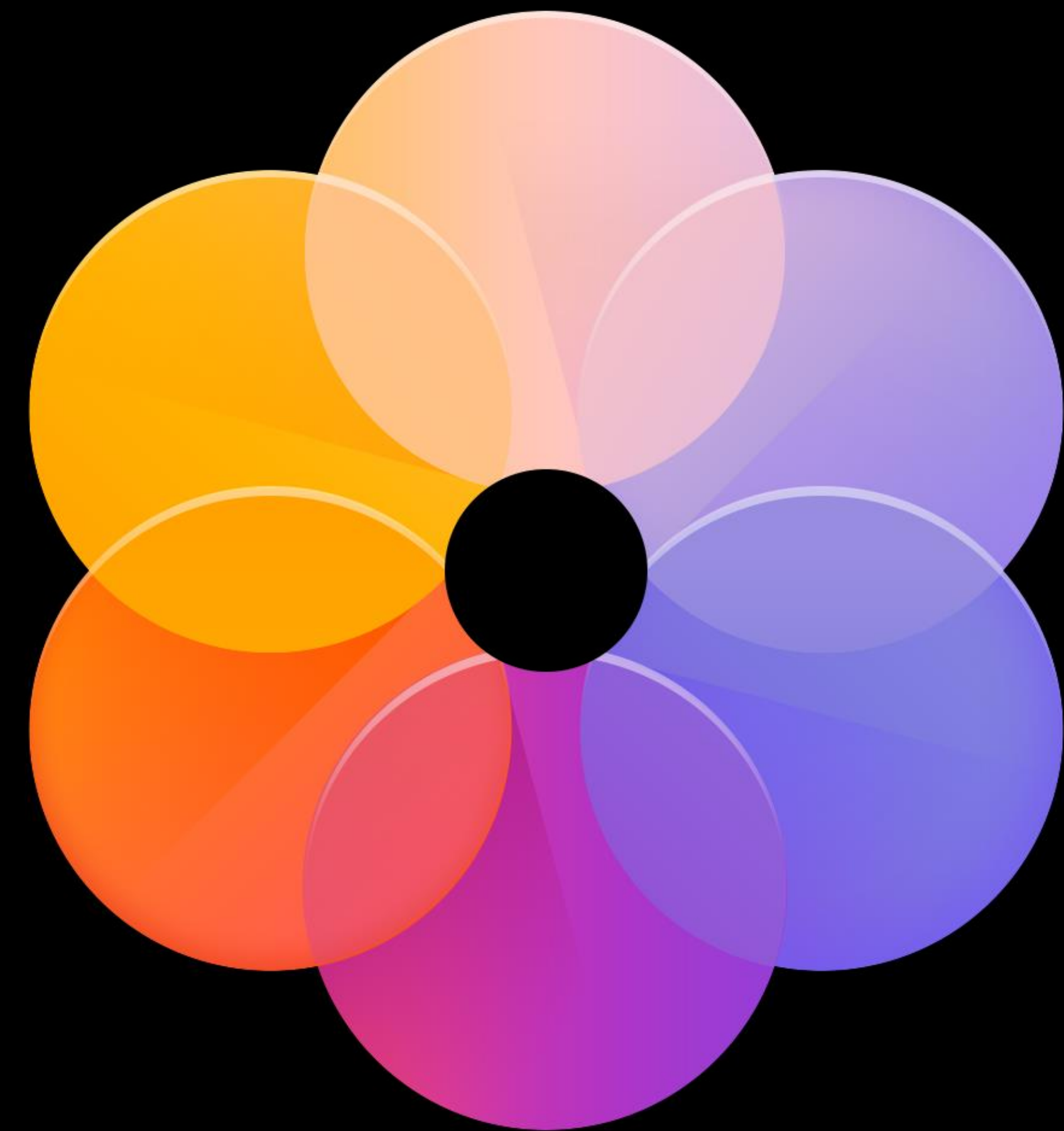


Photo Station



Moments



Synology Photos

快

狠

準

上傳照片
疾速顯示

索引含轉縮圖

透過 SMB 上傳 1000 張
JPG 照片所需時間

3 hrs → 1 hrs



轉縮圖

處理 3MB 的照片

478 ms → 160 ms

Test models : J series

疾速顯示

> 300%

手機備份
SMB 上傳
瀏覽器上傳

整理照片

狠彈性、狠智慧、狠方便

分享照片 快速收集

公開收集

收集親友
旅遊照片

攝影課程
學員分享

分享照片
快速收录
即時互動



瀏覽照片

極流暢、零阻礙



尋找照片 精準篩選



升級是否能無痛移轉？

快速顯示

狠彈性
狠智慧
狠方便

精準搜尋



相片

Metadata



資料夾結構

標籤



分享連結

Synology®

S Y N O L O G Y
2 0 2 0

與時俱進，守護資產安全

從實體到虛擬，三個面向實現完整防護



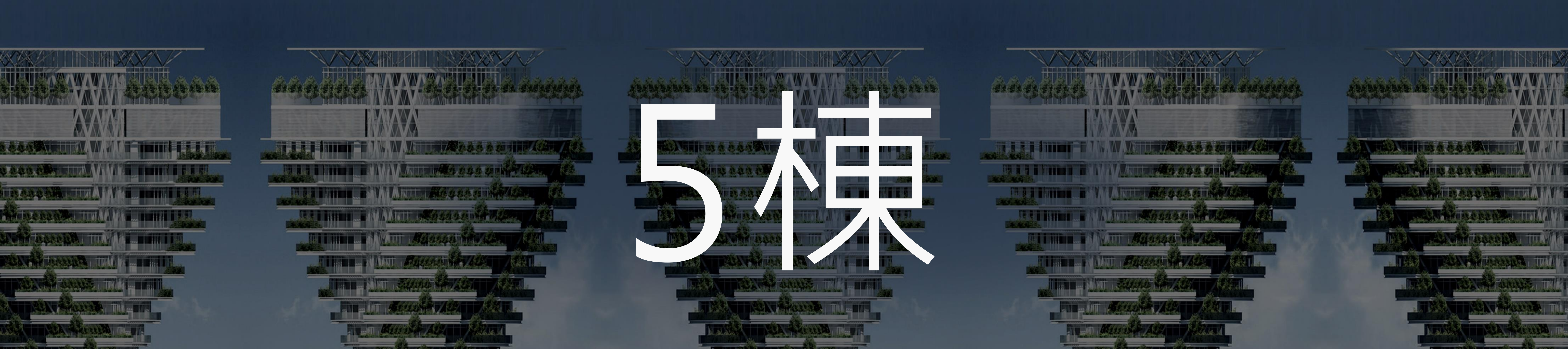


勒索軟體

115億美元 = 3565億台幣

陶朱隱園





5棟




如何保護數位資產



事前防護

事件察覺

事後修復



事前防護

新聞

資安一周第53期：勒索軟體威脅再度成為關注焦點，近期不僅傳出NAS設備用戶遭鎖定，南非也有電力公司遇害

文/ 羅正漢 | 2019-07-31 發表

讚 5.6 萬 按讚加入iThome粉絲團

讚 84 分享



擁抱Kubernetes
讓你的企業基礎設施
來一次華麗轉身

企業團購正優惠

Kubernetes Summit
9/11 ▶ 臺北文創大樓

iThome Security 2019 最大資安展會
擴大首辦臺灣資安週
說這專頁讚 1萬按讚次數
台北國際會議中心 & 台北世貿一館 2F

成為朋友中第一個說這讚的人

iThome Security
約 1 小時前
這些帳號張貼了針對香港群眾運動的負
面言論訊息，但除盡你帳號裡有這些

Current					
Clear		Export		Connection	
				admin	
Level	Log	Date & Time	User	Event	
Warning	Connection	2019-07-19 07:09:53	system	User [admin] from [188.166.2.191] failed to log in via [DSM] due ...	
Warning	Connection	2019-07-19 07:09:48	admin	User [admin] from [188.166.2.191] failed to log in via [DSM] due ...	
Warning	Connection	2019-07-19 07:08:28	system	User [admin] from [165.22.82.115] failed to log in via [DSM] due ...	
Warning	Connection	2019-07-19 07:08:23	admin	User [admin] from [165.22.82.115] failed to log in via [DSM] due ...	
Warning	Connection	2019-07-19 07:07:01	system	User [admin] from [35.192.145.110] failed to log in via [DSM] due...	
Warning	Connection	2019-07-19 07:06:56	admin	User [admin] from [35.192.145.110] failed to log in via [DSM] due...	

群暉科技 Synology® 及 TWCERT/CC 與國際資安組織展開協作，阻止全球 NAS 勒索事件擴散

台北台灣—2019 年 8 月 8 日—群暉科技 Synology® 與台灣電腦網路危機處理暨協調中心（Taiwan Computer Emergency Response Team / Coordination Center, TWCERT/CC）共同宣布，日前全球多個品牌 NAS（Network Attached Storage）遭駭客暴力破解管理員密碼加密資料勒索的攻擊事件，已透過與國際資安組織之協作，於 7 月 26 日撤下駭客用以執行攻擊的主機，並控制住災情擴散。Synology 與 TWCERT/CC 同時呼籲全球 NAS 用戶加強系統安全設定，以確保資料安全無虞。

Synology 產品安全事件應變團隊經理李宜謙表示，Synology 一直將保護用戶資料安全視為最重要的任務，藉由長期積極參與國際資安社群互動，Synology 得以串聯台灣與全球資安社群的網絡，在事件發生時快速與全球資安組織展開協作，讓災情不致全面性爆發。

Synology 於 7 月 19 日開始陸續接獲用戶回報 NAS 資料遭到加密勒索，分析樣本後排除駭客利用 DSM 系統漏洞進行攻擊，而是針對使用預設 Admin 帳戶及弱密碼的用戶進行密碼組暴力破解取得管理員權限後，加密檔案再對受害者勒索贖金。7 月 22 日，Synology 透過全球技術支援部門統計回報受影響的 Synology 用戶達數十位，並評估全球有上萬台不同品牌的 NAS 可能暴露在風險中，為此次事件潛在受攻擊對象。是日，Synology 追蹤並連回駭客執行攻擊控制與命令的伺服器，同時通報 TWCERT/CC 啟動國際協作，並於 7 月 26 日透過丹麥的 CFCS-DK 根據 IP 位置找到攻擊來源的主機，撤下駭客用以執行攻擊的主機。

TWCERT/CC 負責人丁綺萍表示：「此次事件有賴於良好的合作關係才能快速反應、讓 TWCERT/CC 取得樣本進一步啟動跨國資安組織協作，及早掌握並控制住災情。我們期待看到更多品牌參考 Synology 的作法建置產品安全團隊，並積極與資安組織互動。」

儘管事件已獲控制，Synology 仍建議無論是 Synology 或其它品牌 NAS 用戶參考以下步驟，強化資料安全性：

- 啟用防火牆功能，僅在必要的時候開啟對外網路埠

群暉科技 Synology® 及 TWCERT/CC 與國際資安組織展開 協作，阻止全球 NAS 勒索事件擴散

台北台灣—2019 年 8 月 8 日—群暉科技 Synology® 與台灣電腦網路危機處理暨協調中心 (Coordination Center, TWCERT/CC) 共同宣布，日前全球多個品牌 NAS (Network Attached Storage) 攻擊事件，已透過與國際資安組織之協作，於 7 月 26 日撤下駭客用以執行攻擊的主機，並建議 NAS 用戶加強系統安全設定，以確保資料安全無虞。

Synology 產品安全事件應變團隊經理李宜謙表示，Synology 一直將保護用戶資料安全視為首要任務。Synology 得以串聯台灣與全球資安社群的網絡，在事件發生時快速與全球資安組織展開協作，以確保用戶資料安全。

Synology 於 7 月 19 日開始陸續接獲用戶回報 NAS 資料遭到加密勒索，分析樣本後排除駭客利用弱密碼的用戶進行密碼組暴力破解取得管理員權限後，加密檔案再對受害者勒索贖金。受影響的 Synology 用戶達數十位，並評估全球有上萬台不同品牌的 NAS 可能暴露在風險中，執行攻擊控制與命令的伺服器，同時通報 TWCERT/CC 啟動國際協作，並於 7 月 26 日透過國際資安組織撤下用以執行攻擊的主機。

TWCERT/CC 負責人丁綺萍表示：「此次事件有賴於良好的合作關係才能快速反應、讓台灣電腦網路穩定運作並控制住災情。我們期待看到更多品牌參考 Synology 的作法建置產品安全團隊，並積極與國際資安組織合作，以確保用戶資料安全。」

儘管事件已獲控制，Synology 仍建議無論是 Synology 或其它品牌 NAS 用戶參考以下步驟，以確保資料安全無虞：

- 啟用防火牆功能，僅在必要的時候開啟對外網路埠

妥善管理帳號與網路設定
防範惡意攻擊

Synology

Synology 群暉科技

7月23日 · 🌐

【Synology 建議您立即檢查網路與帳號安全設定，防範惡意攻擊】

近期傳出市面上各種 NAS 品牌與型號遭駭客以暴力破解密碼，並對檔案進行加密。Synology 經調查發現，此事件是採用字典攻擊獲取密碼，而非利用特定系統安全性漏洞。為確保您存放於 NAS 中的檔案安全無虞，我們建議用戶立即採取以下行動：

1. 使用強度較強的密碼，並在控制台啟用密碼強度限制規則
2. 新增一組具管理員權限的帳號，並停用系統預設的「admin」帳號
3. 啟用自動封鎖來阻擋嘗試登入次數過多的 IP
4. 執行安全性諮詢中心為系統進行完整安全性評估

👉 詳細資訊點此了解 <http://sy.to/4e5ef>

👍👎👤 153

👍 讚

💬 留言

➦ 分享

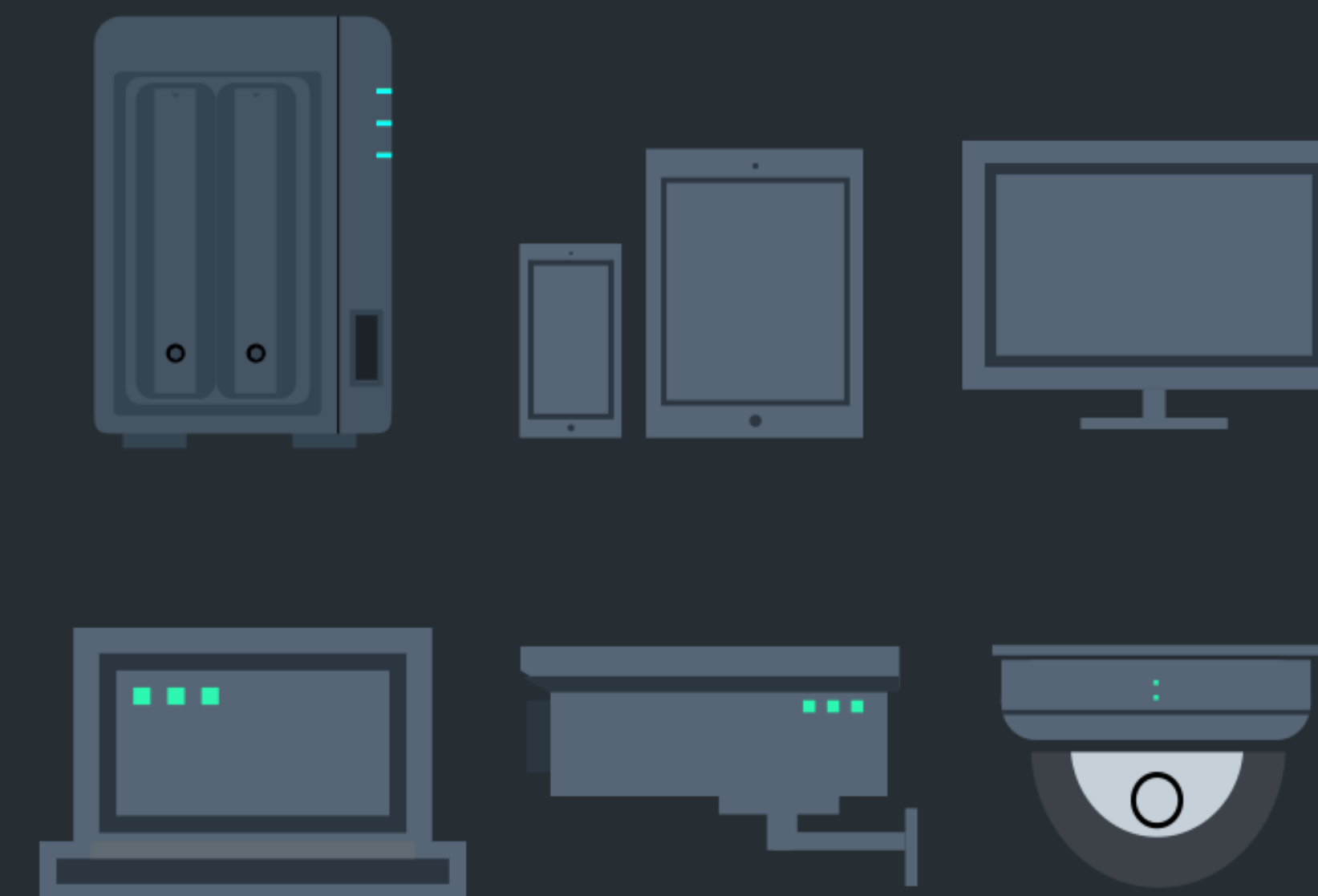
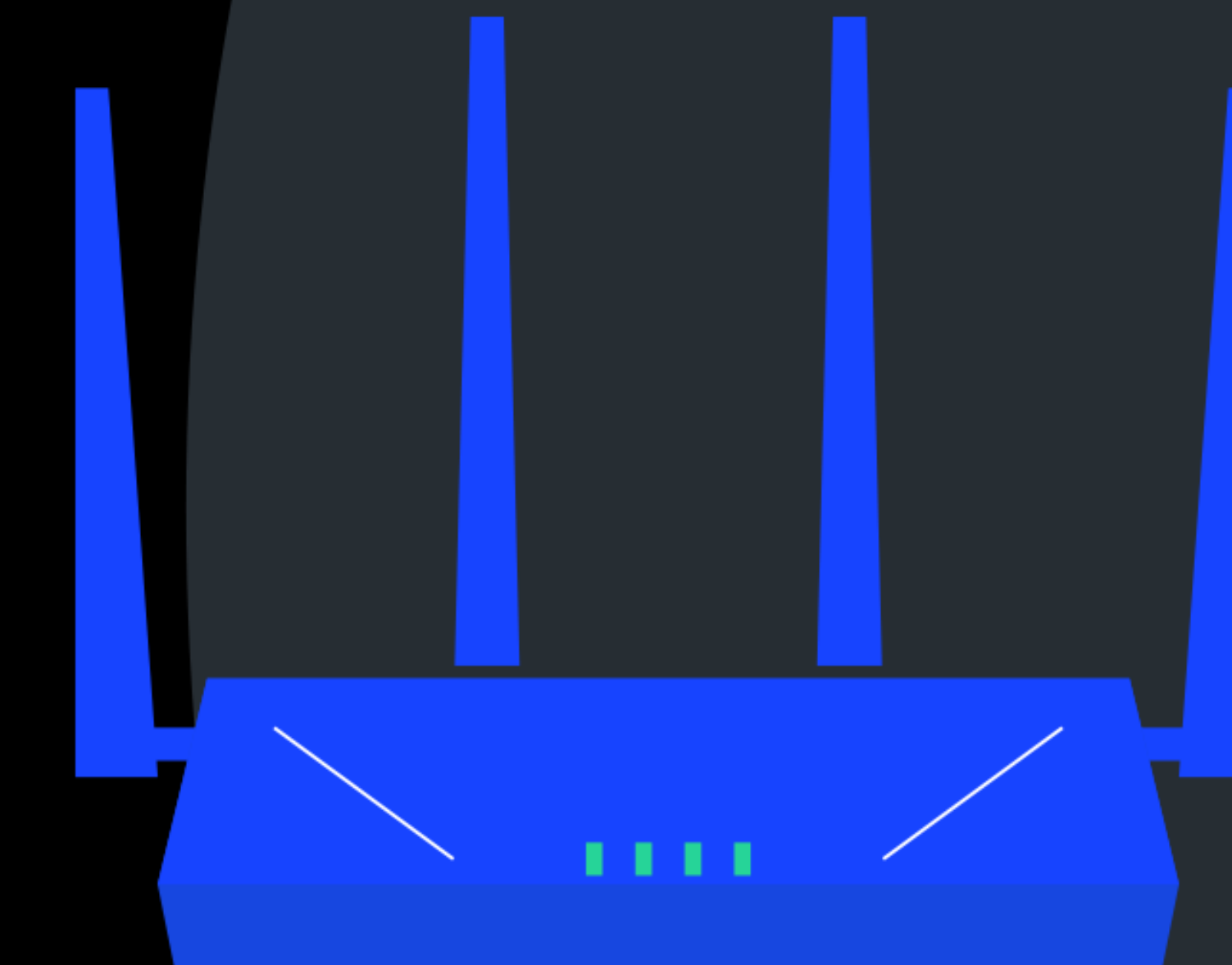
🌐

第一步：周界安全

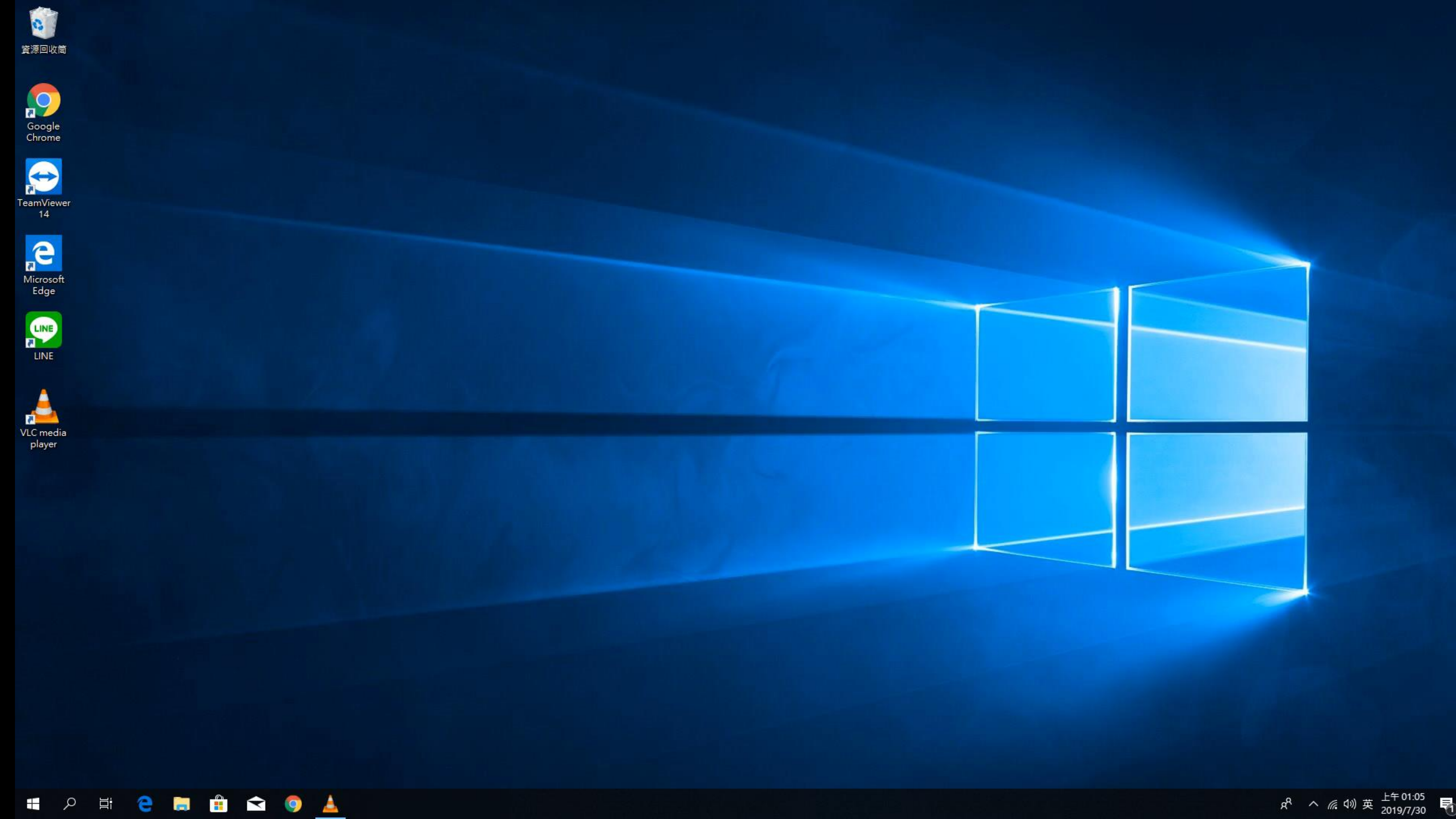
除了路由器，其他一律不對外開 port



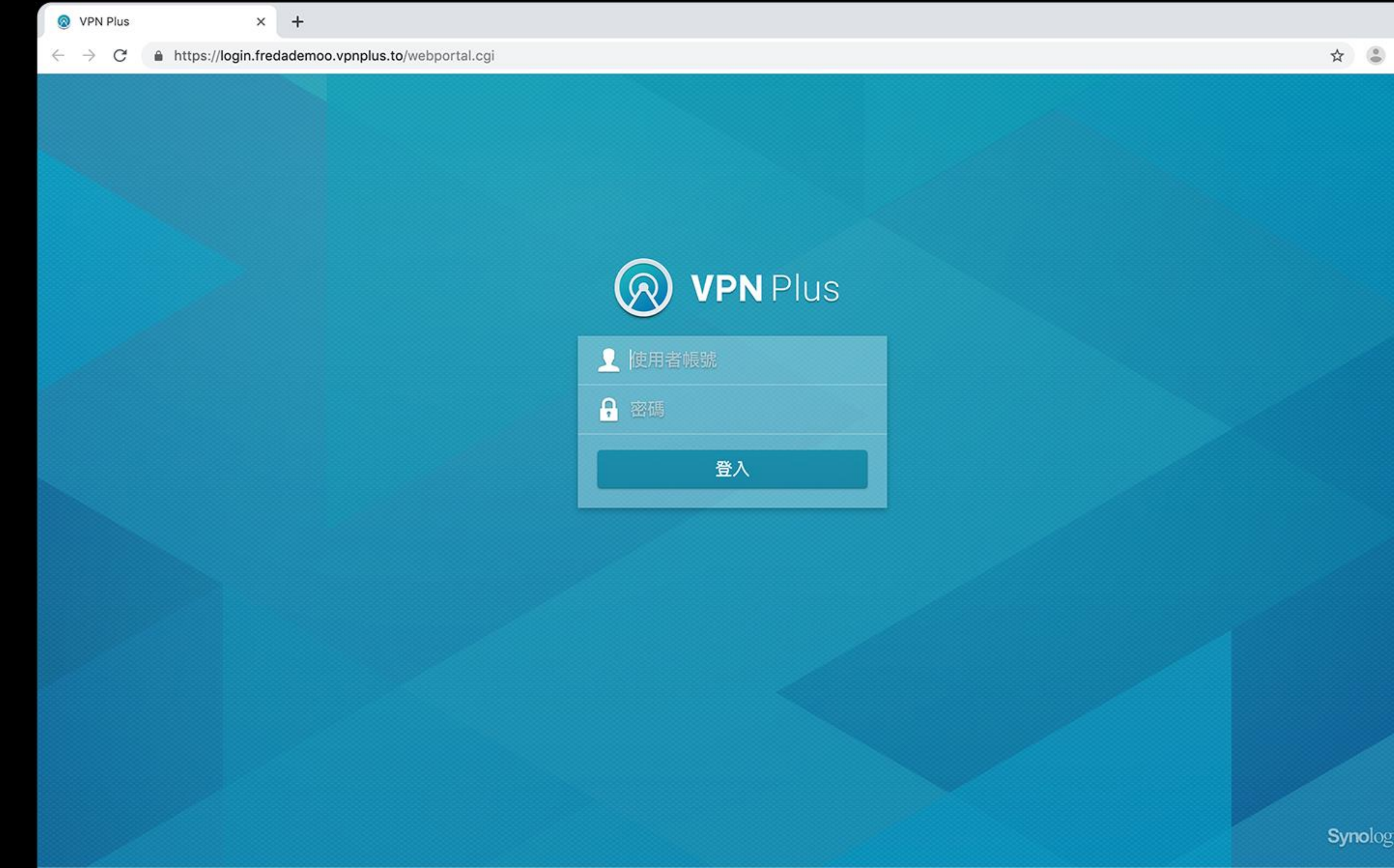
1



VPN



VPN Plus



免費的最貴



「祝賀！您被Google隨機選中」跳出中獎視窗 當心挨詐



2019-06-20 17:40

〔記者林嘉東 / 基隆報導〕「祝賀！您被Google隨機選中」當心挨詐！

使用手機、電腦、接收EMAIL時，瀏覽器
機會贏得 iPhone 或其他Google獎品」等

iPhone用戶小心！出現「恭喜Google用戶！贏得iPhone」是詐 詐騙惡意彈跳視窗

2018-03-27 • by 瘋先生



最近看見不少使用 iPhone或iPad 用戶在反應瀏覽網頁到一半，總是會跳出「恭喜Google用戶～贏得iPhone一台」的彈跳訊息，有些都會以為自己所用的 Safari 或 Chrome 遭網頁綁架了，但其實這個是很常見的抽獎詐騙網頁惡意彈跳視窗，不管是在 Android 系統或

新一波透過感染行動裝置,進一步取得家用路由器控制權的攻擊事件

針對家用路由器的攻擊已經出現好幾年了，從操縱路由器的惡意軟體到DNS重新綁定攻擊及後門程式等。就在去年，趨勢科技的研究人員曾發現網域名稱系統 (DNS) 變更惡意軟體會將瀏覽特定網站的使用者重新導到惡意網頁。使得受害者的網路憑證，例如密碼和PIN碼陷入險境。





Safe Access

自動阻擋惡意網站





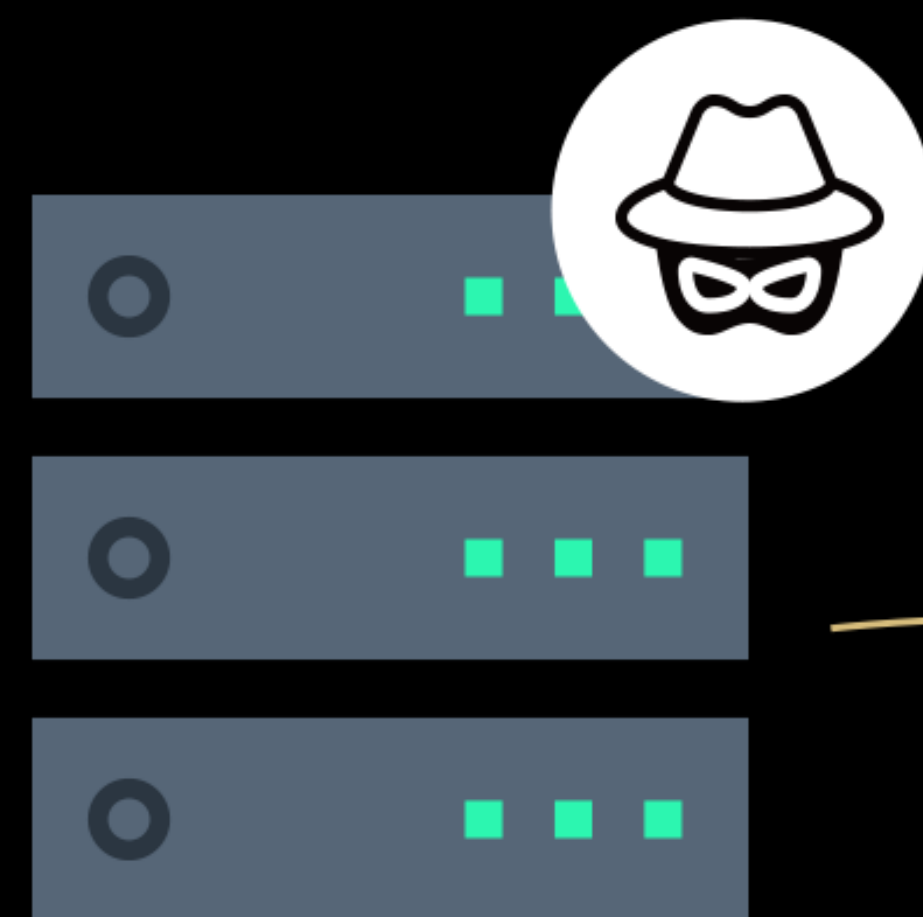
Threat Prevention

企業級入侵防禦系統
深度封包檢測



第二步：網路安全

阻擋惡意網站惡意封包
雙重保護



2



新聞

英國發布DNS挾持攻擊警告

今年DNS挾持攻擊活動持續在各地升溫，英國國家網路安全中心呼籲各大組織應謹慎應對

文/ [陳曉莉](#) | 2019-07-15 發表

👍 讚 5.6 萬 按讚加入iThome粉絲團

👍 讚 344

分享



Advisory: Ongoing DNS
hijacking and advice on how
to mitigate



怎麼去 www.pchome.com.tw

一般 DNS



PChome



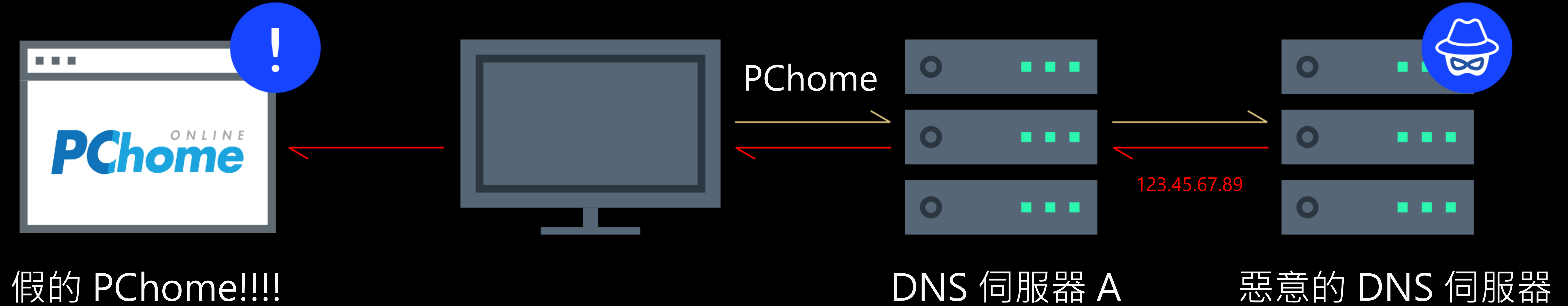
DNS 伺服器 A



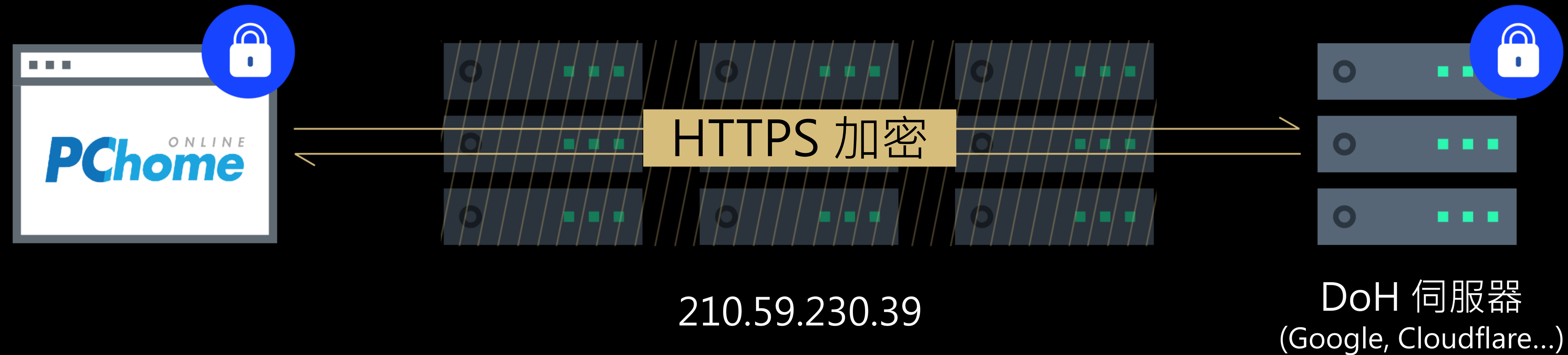
DNS 伺服器 B

210.59.230.39

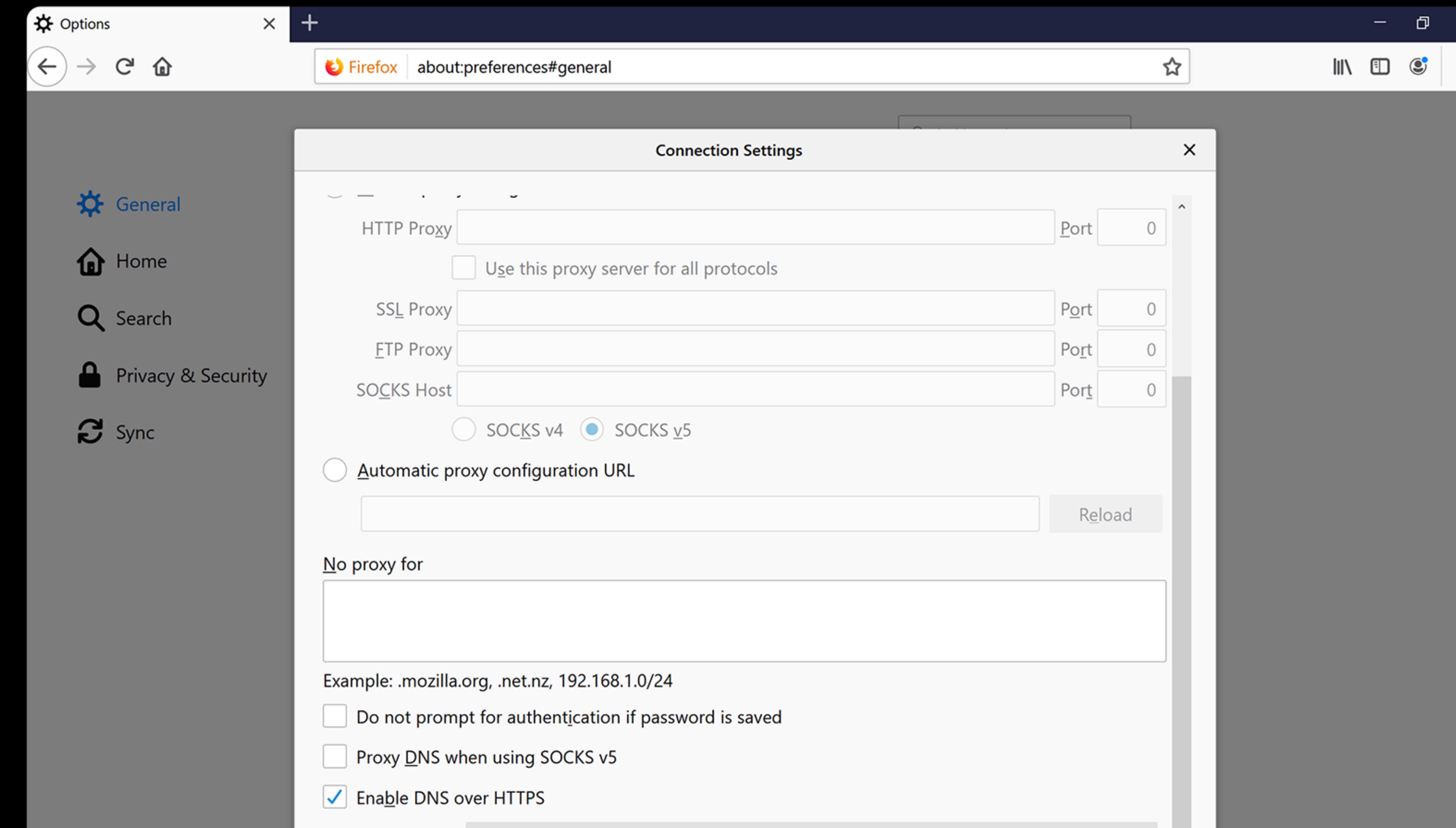
DNS 挾持



DNS over HTTPS (DoH)

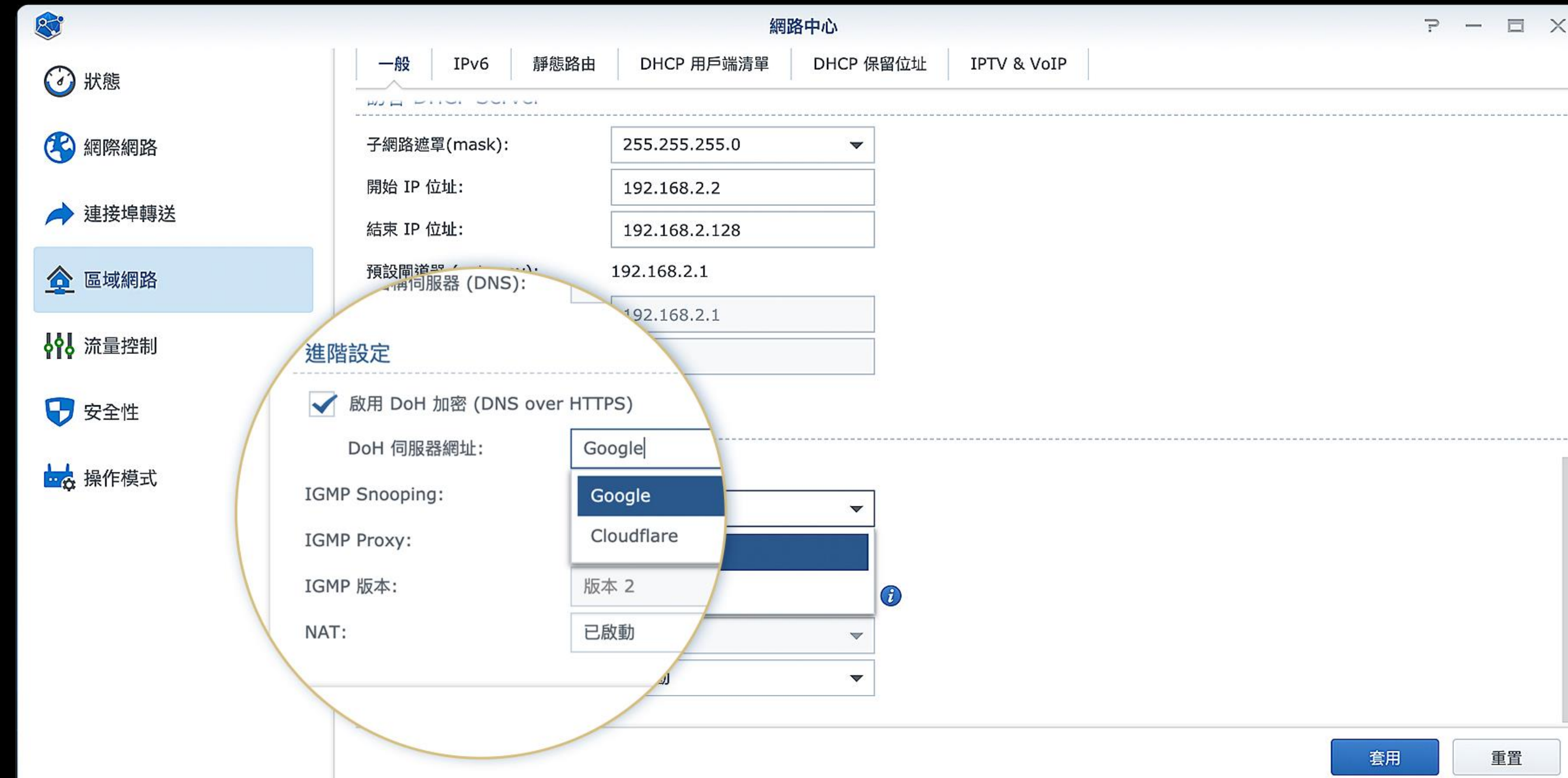


部分瀏覽器 已開始支援



一鍵啟用

為所有裝置啟用 DoH 加密



第三步： 開啟 DoH 加密

防止中間人攻擊



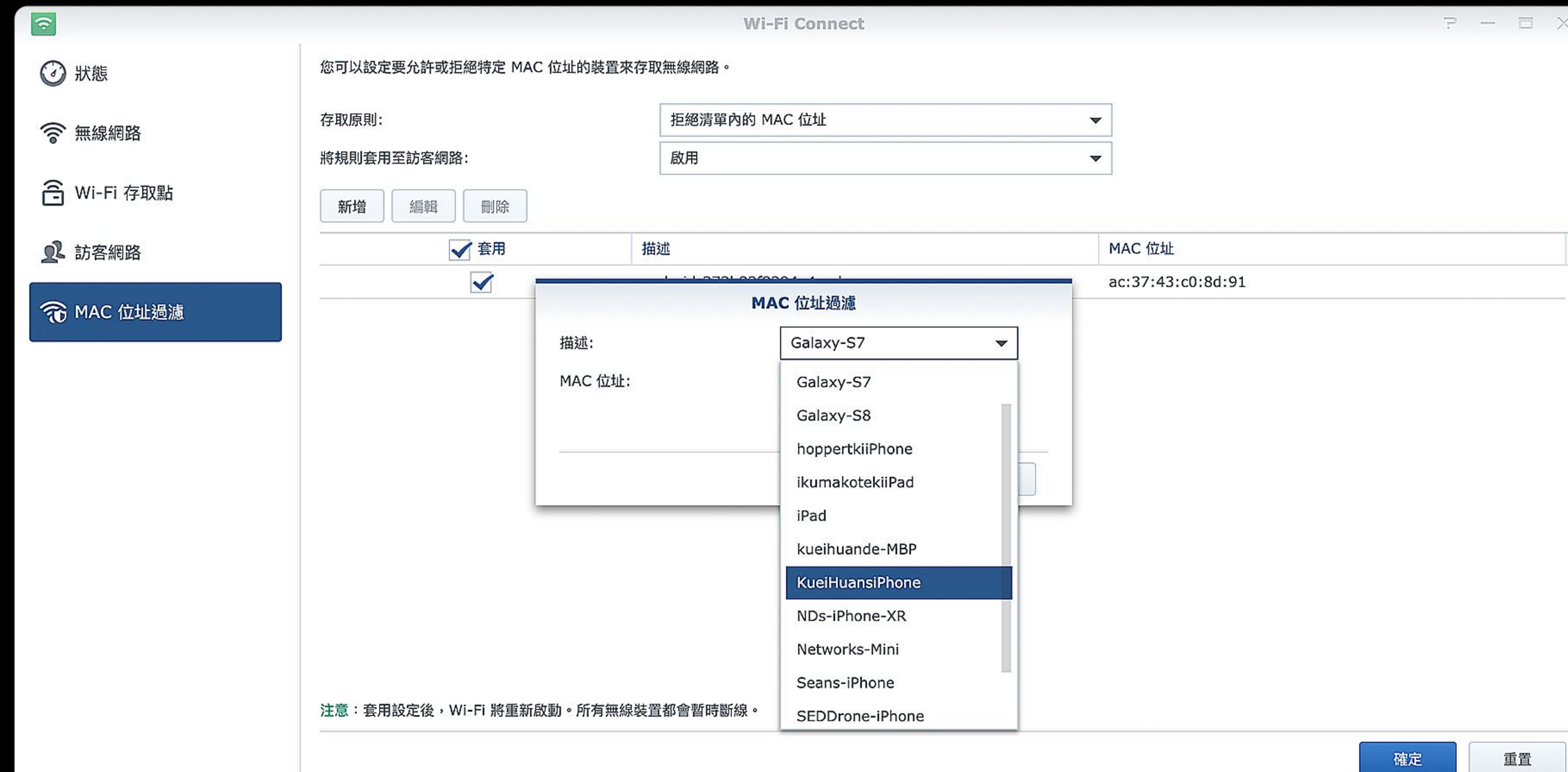




Wi-Fi 密碼外流或被破解

MAC 位址過濾

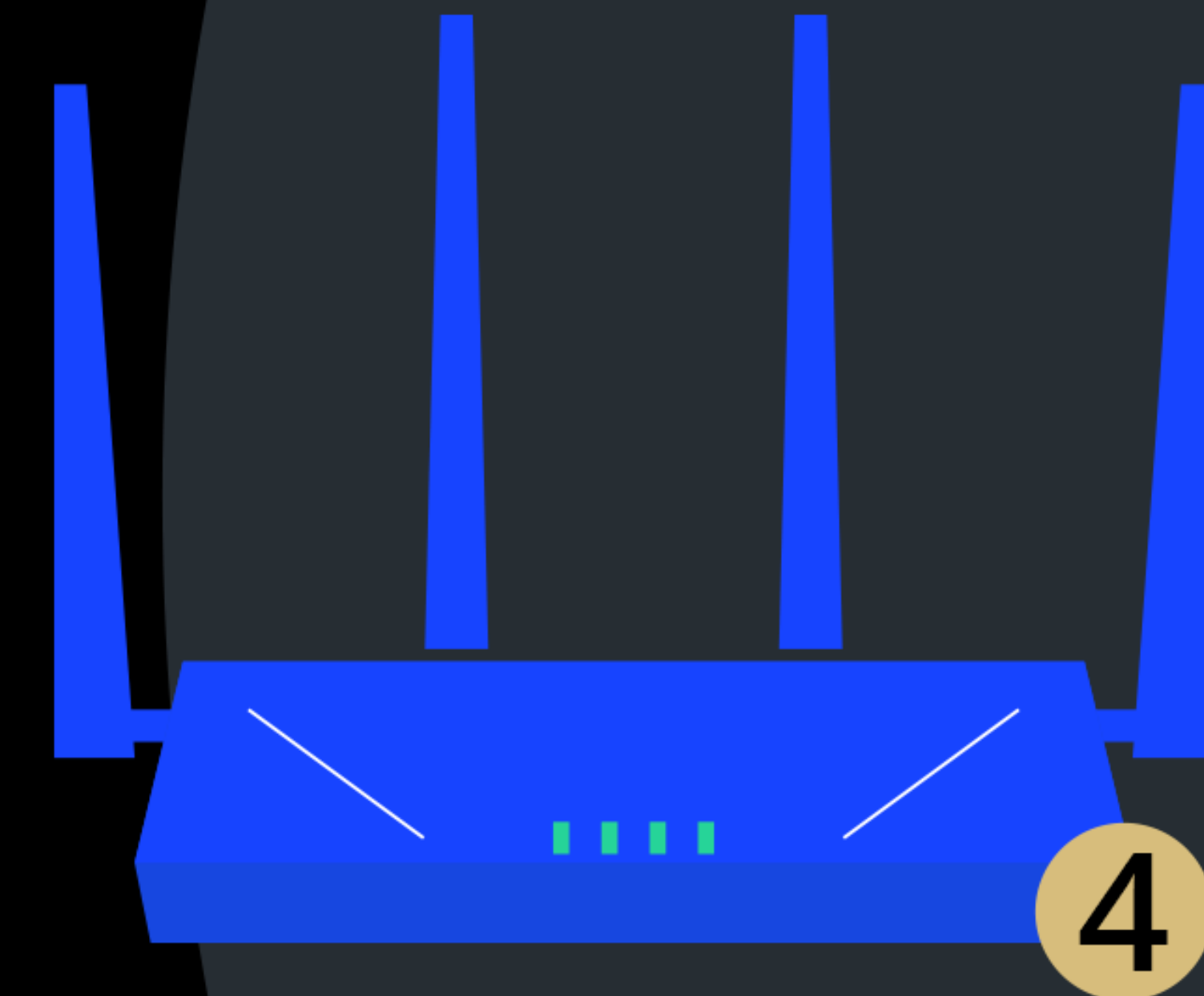
僅允許已知裝置連上 Wi-Fi



第四步： 允許連線清單



✗
Wi-Fi 密碼外流
或被破解



事前防護 四部曲

周界安全

網路安全

開啟
DoH 加密

允許
連線清單



事件察覺

IoT裝置數量愈多 成為攻擊跳板的工具可能性愈高

作者：編輯部 -2019 / 07 / 17



產業研究報告預測明年2020，全球IoT裝置，全部的IoT裝置數量已經設備，不過，這種新型應用環境也險的曝露。

隨著這幾年物聯網世代的快速發展中，工業製造產業的腳步亦趨跟上在工業環境下，企業的製造與營運

【再也沒有 123456 了】加州立法禁用「預設密碼」，IoT 產品全得強制改密碼

2018/12/12 讚 339 分享



楊采翎

IoT殭屍網路引爆危機 未設防節點淪為攻擊跳板

2017-12-27 David Holmes

誘人的利益下總是潛藏危險，很多消費者將會震驚的發現他們的一些物聯網裝置（IP網路攝影機、DVR和家用路由器）或許已遭入侵，甚至可能已變成傀儡被使用於大型的殭屍網路。

物聯網（Internet of Things，IoT）安全威脅，特別是具有安全弱點的物聯網裝置遭駭客利用作為攻擊工具所引發的問題，已成為F5 Labs一年多來的主要研究領域。

物聯網裝置逐漸成為今天傀儡殭屍網路攻擊者的最佳「網路武器投射系統」。理由其實很簡單，世界上有數十億物聯網裝置，而且大多可以輕易存取（藉由Telnet）和駭入（因為欠缺安全管控）。當有那麼多裝置可以免費利用時，攻擊者何以需要投入昂貴的資源去構築他們自己的殭屍網路？



別再用「Admin」作密碼！近萬台Router等IoT裝置密碼被公開

呀粗

2017-08-29

你家的 Router 帳號及密碼依然是「Admin、Admin」嗎？沒改過預設密碼的話，真的要當心了！因為網上流傳一份載有全球 8,000 多台 IoT 物聯網裝置之 IP 位址及帳號密碼名單，並有過萬人存取過，恐怕已被駭客入侵裝置，令它們成為殭屍網絡的一部分，利用裝置發動 DDoS 攻擊！

裝置異常徵兆

流量激增

先斷網再重置

裝置

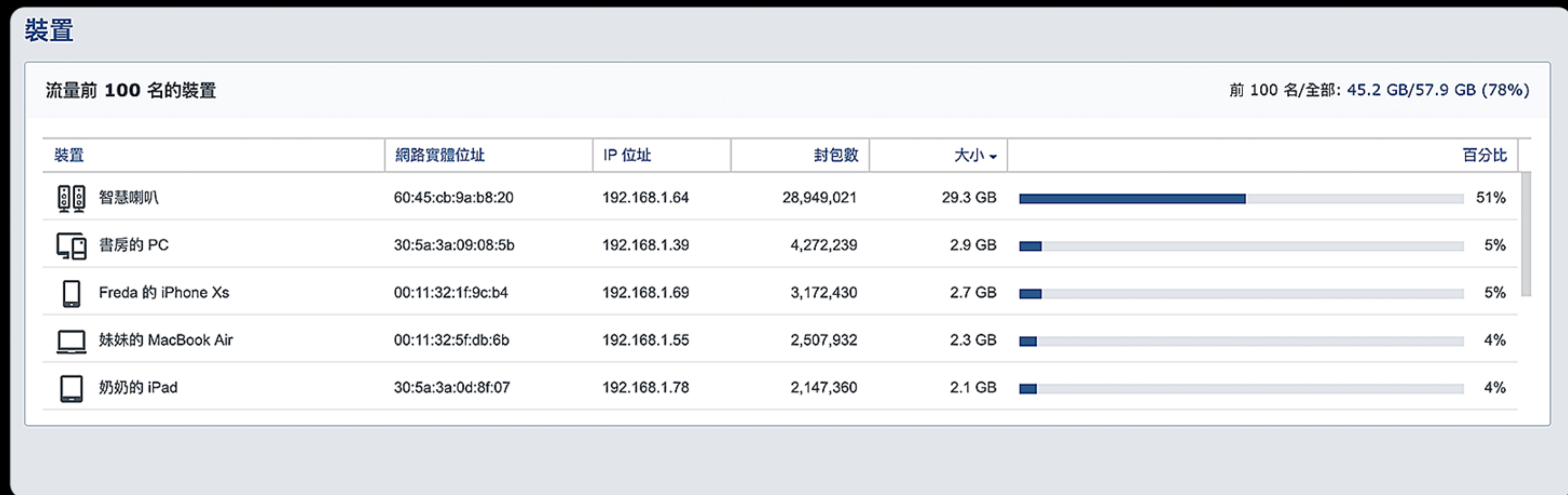
流量前 **100** 名的裝置

前 100 名/全部: 45.2 GB/57.9 GB (78%)

裝置	網路實體位址	IP 位址	封包數	大小 ▾	百分比
 智慧喇叭	60:45:cb:9a:b8:20	192.168.1.64	28,949,021	29.3 GB	<div><div></div></div> 51%
 書房的 PC	30:5a:3a:09:08:5b	192.168.1.39	4,272,239	2.9 GB	<div><div></div></div> 5%
 Freda 的 iPhone Xs	00:11:32:1f:9c:b4	192.168.1.69	3,172,430	2.7 GB	<div><div></div></div> 5%
 妹妹的 MacBook Air	00:11:32:5f:db:6b	192.168.1.55	2,507,932	2.3 GB	<div><div></div></div> 4%
 奶奶的 iPad	30:5a:3a:0d:8f:07	192.168.1.78	2,147,360	2.1 GB	<div><div></div></div> 4%

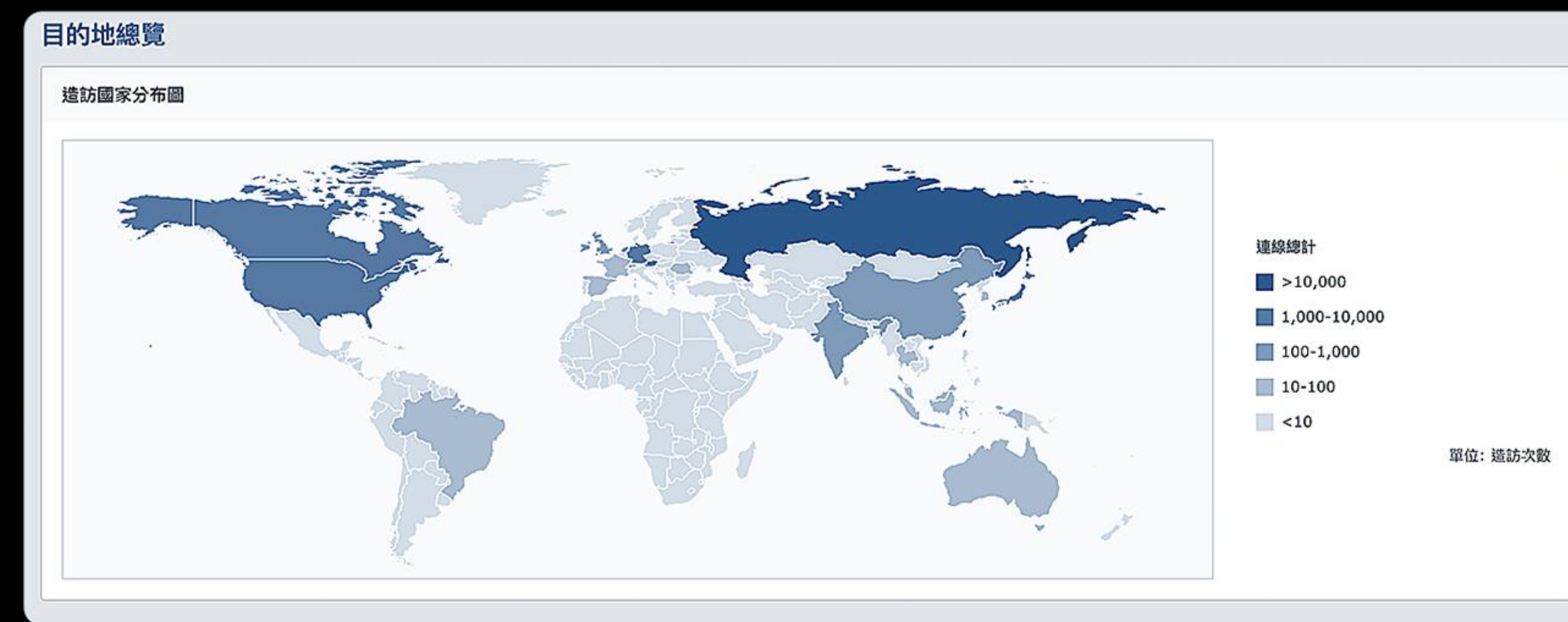
流量激增

先斷網再重置



大量連往特定區域

開啟 Geo-IP 進行過濾阻擋





事後修復

零時差攻擊

USB

公用 Wi-Fi



付還是不付



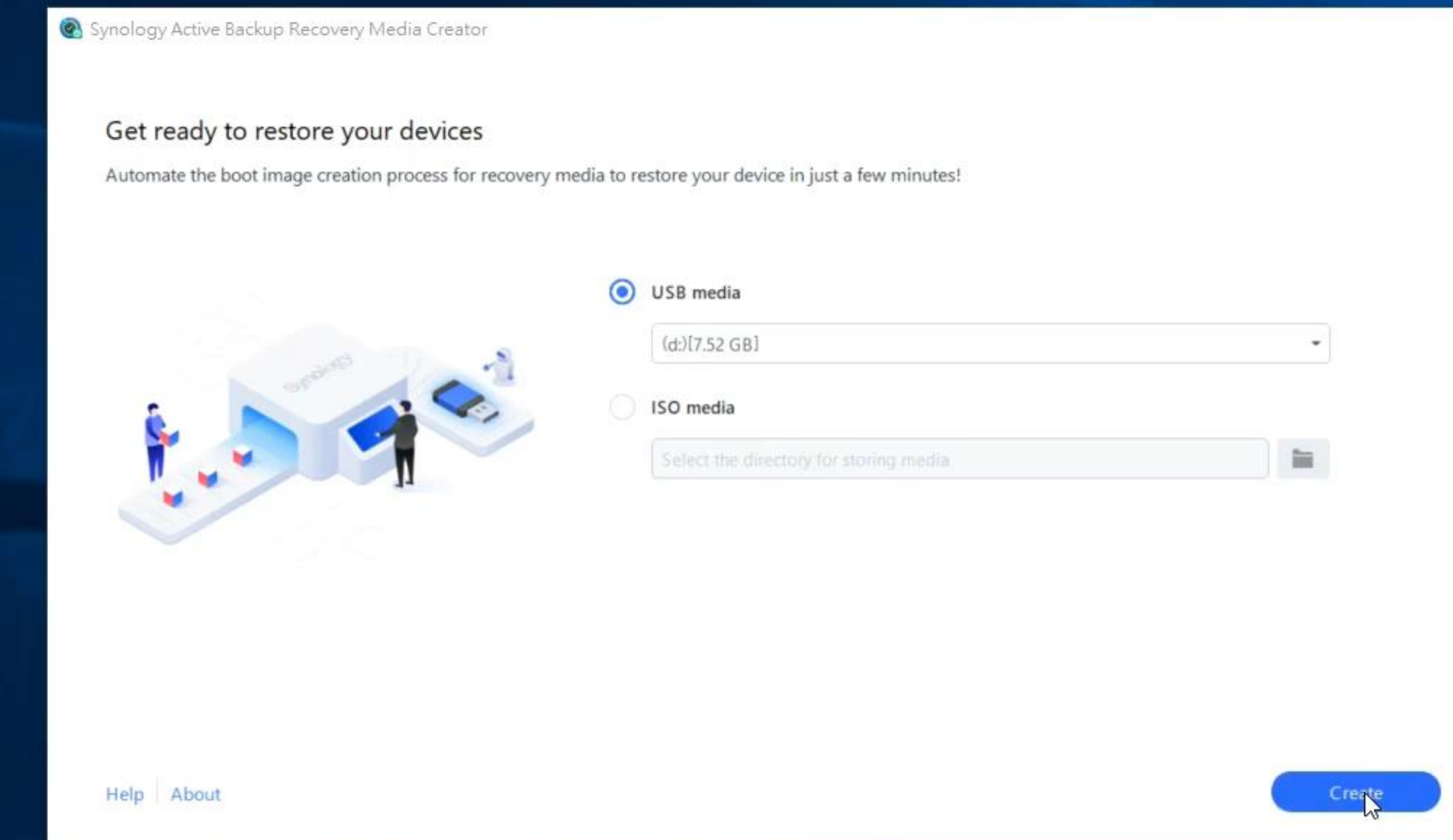


Active Backup
for Business

快速建立 備份



整機還原



Active Backup for Business

- 整機備份 / 整機還原
- 單一檔案快速還原
- 增量備份

Synology Active Backup for Business 代理程式



已完成

上次備份時間:
2019-08-21 03:02

下次備份時間:
2019-08-22 02:59



伺服器資訊

伺服器位址:
10.17.60.182

使用者帳號:
admin

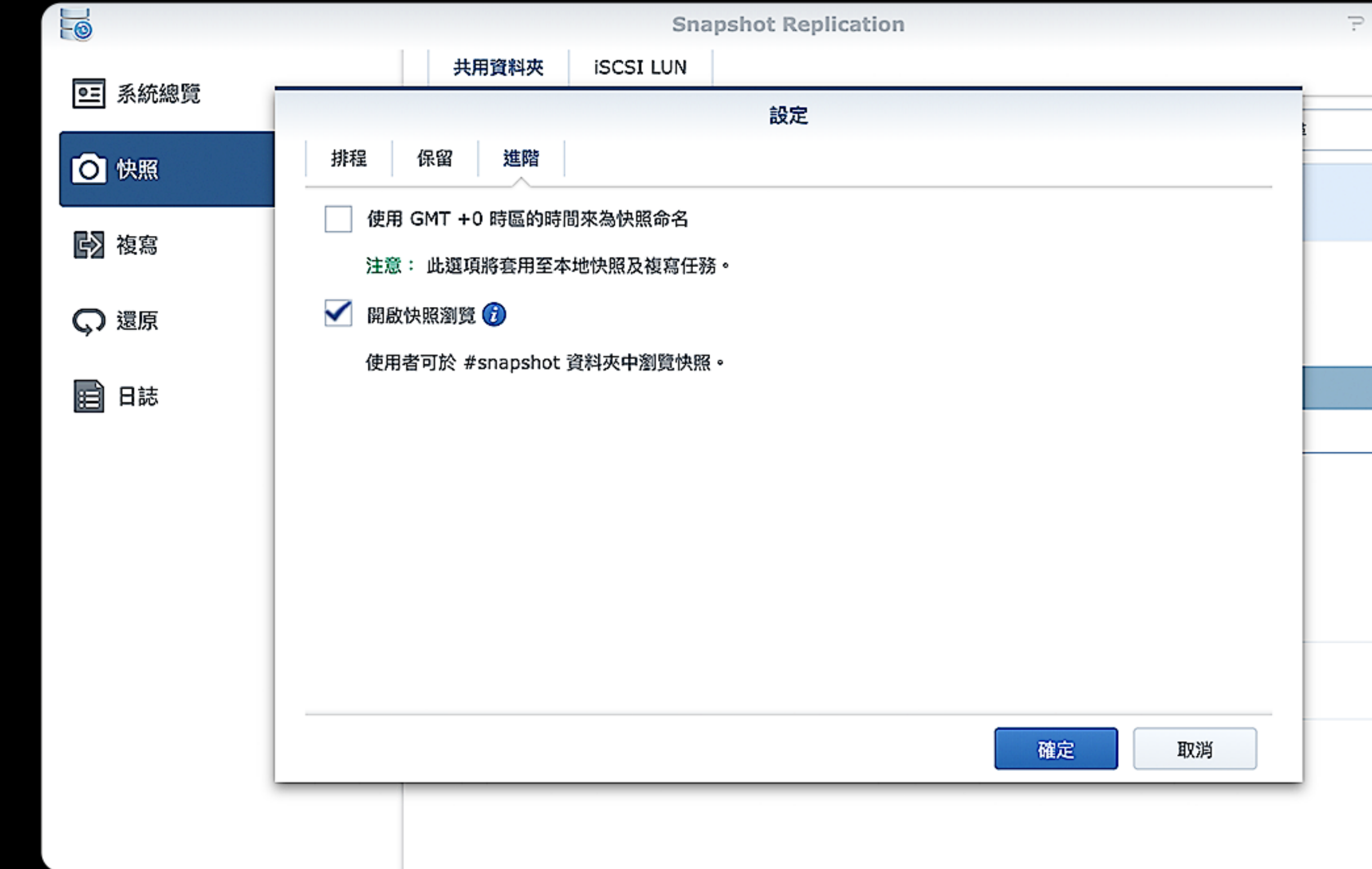
還原入口

最近事件

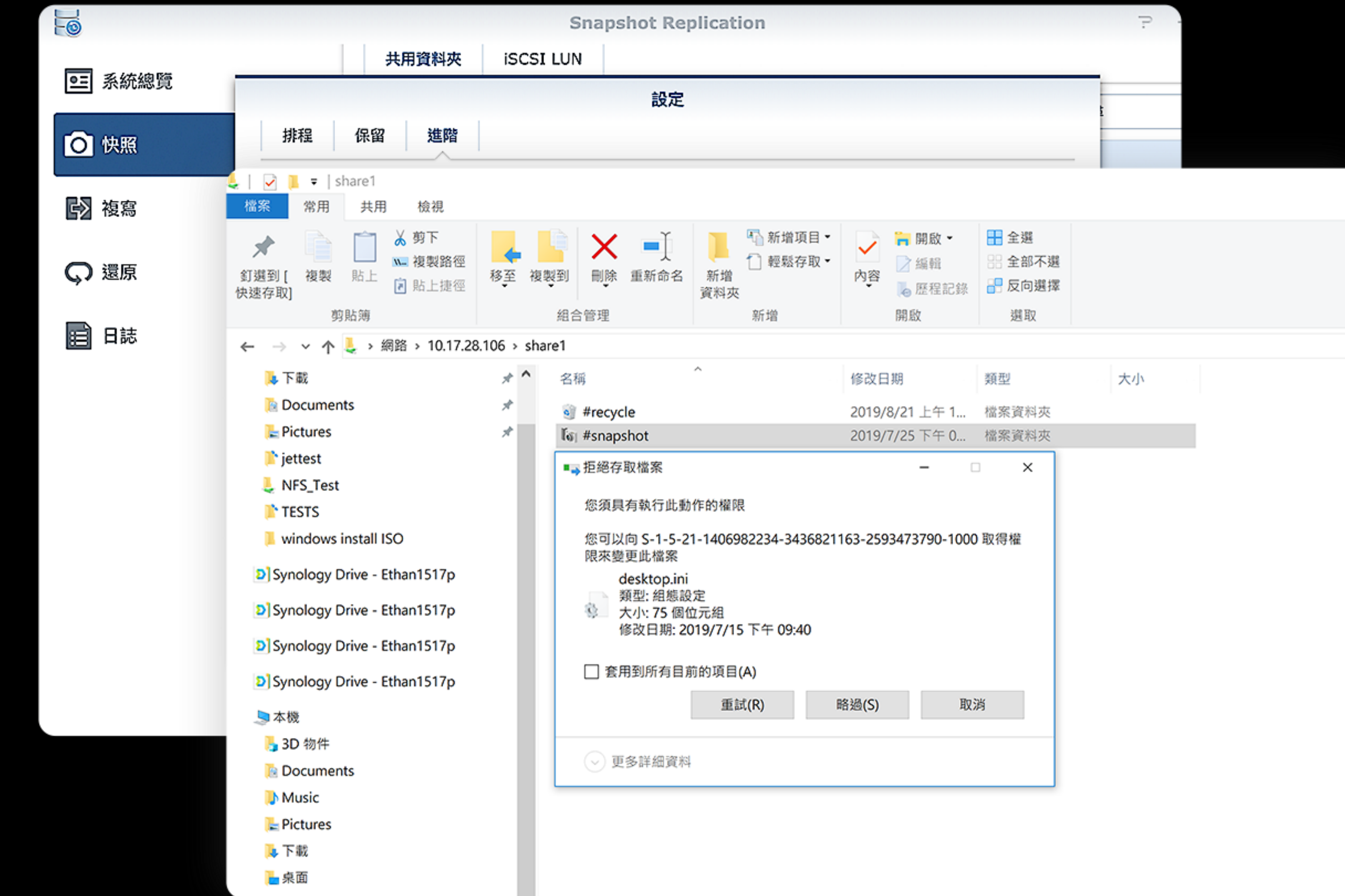
事件	日期及時間
備份任務 admin-Default 成功完成。	2019-08-21 03:02:26
SystemVolume2 儲存空間內的資料已成功讀取並上傳。	2019-08-21 03:02:20
正在準備讀取並上傳 SystemVolume2 儲存空間內的資料。[CBT]	2019-08-21 03:02:20
D:\ 儲存空間內的資料已成功讀取並上傳。	2019-08-21 03:02:18
正在準備讀取並上傳 D:\ 儲存空間內的資料。[CBT]	2019-08-21 03:02:18
SystemVolume5 儲存空間內的資料已成功讀取並上傳。	2019-08-21 03:02:17
正在準備讀取並上傳 SystemVolume5 儲存空間內的資料。[CBT]	2019-08-21 03:02:17
C:\ 儲存空間內的資料已成功讀取並上傳。	2019-08-21 03:02:17
正在準備讀取並上傳 C:\ 儲存空間內的資料。[CBT]	2019-08-21 03:00:19

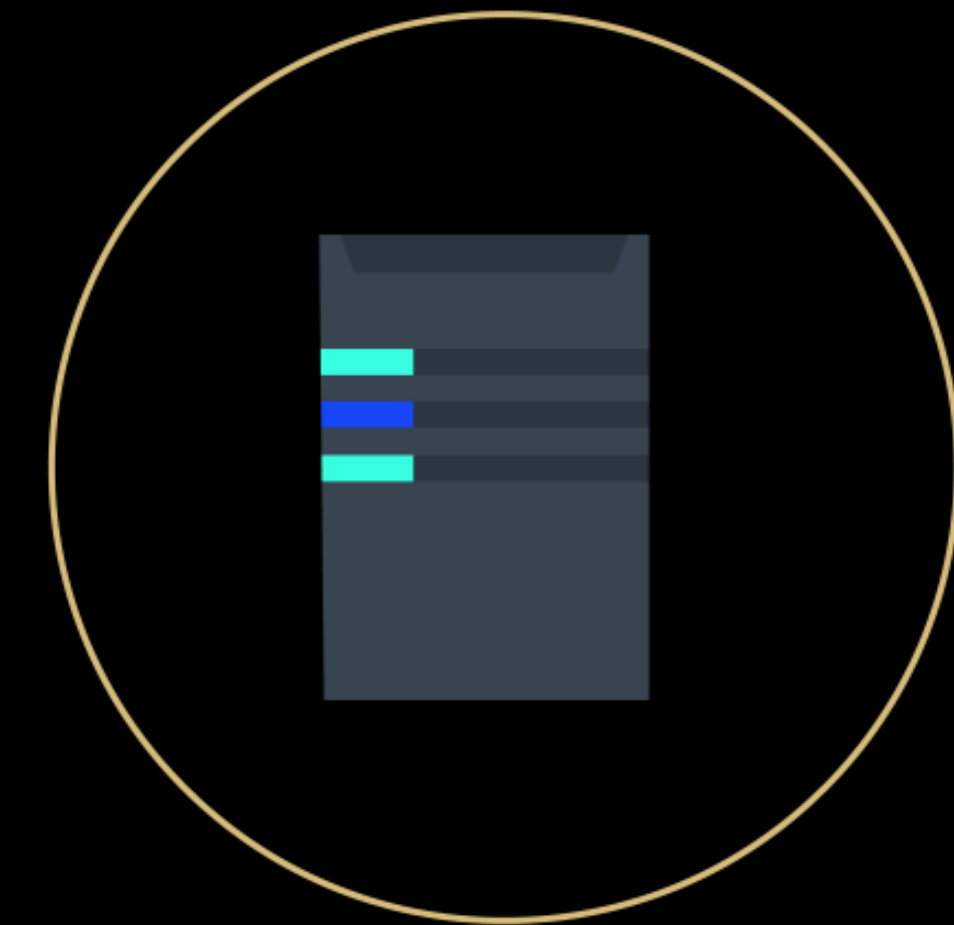


Snapshot



Snapshot

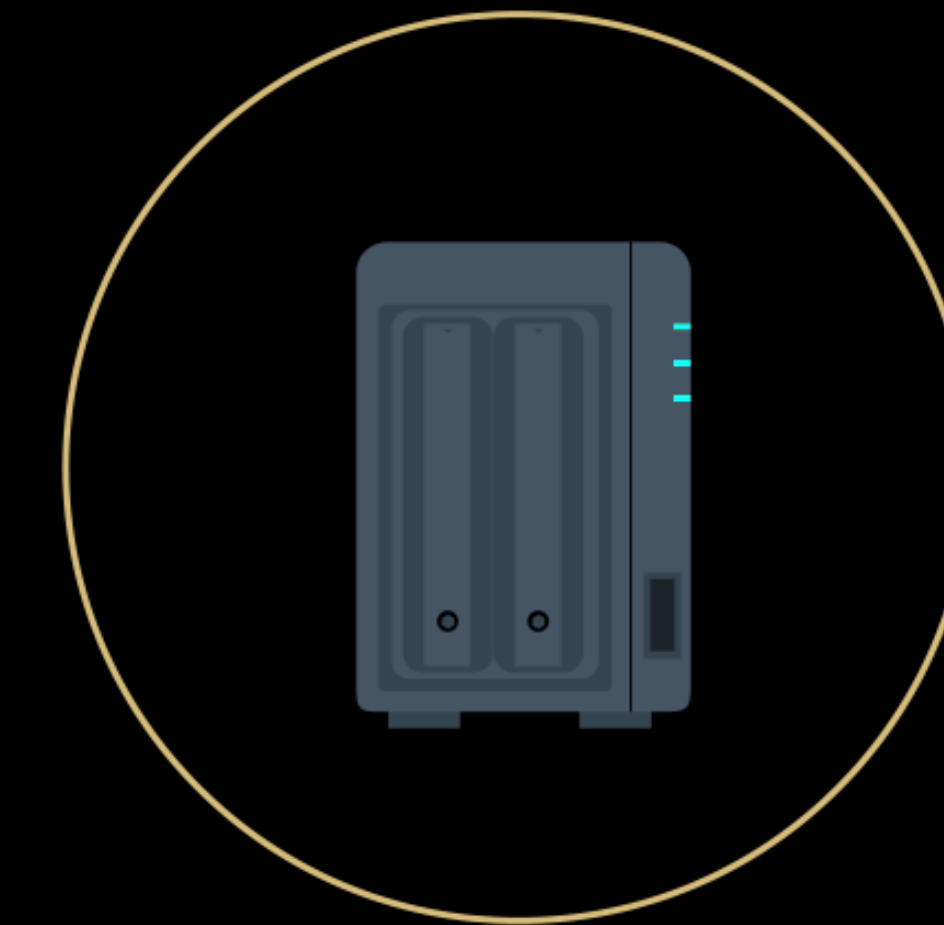




Rsync Server 外部裝置



公有雲



Synology NAS



Hyper Backup支援各種備份架構



事後修復 三選擇

Active Backup
for Business

整機還原 / 單檔還原

Snapshot

更高防護 / 秒級還原

Hyper Backup

備份目的地更彈性



實體資產



Surveillance Station

自動化守護你的實體資產



四大影像分析

人流計數

入侵偵測

禁止逗留區

深度動作偵測

四大影像分析

人流計數

入侵偵測

禁止逗留區

深度動作偵測



行動規則

符合預設條件時
立刻觸發一系列動作

新增行動規則精靈

事件

新增 刪除

設定

邏輯設定: AND

間隔 (秒鐘): 10

事件 1

事件來源: 攝影機

設備: D-Link - DCS-5222

事件: 偵測到動作

觸發類型: 偵測到動作

數位輸入已觸發

數位輸入未觸發

偵測到 PIR 動作

偵測到即時影像分析

連線中斷

連線正常

攝影機已啟動

上一步

取消



行動規則

符合預設條件觸發一系列動作

事件

新增 刪除

設定

邏輯設定:

間隔 (秒鐘):

事件 1

事件來源:

設備:

事件:

觸發類型:

上一步

新增行動規則精靈

新增 刪除

行動

行動 1

行動設備:

設備:

行動:

攝影機

D-Link - DCS-5222

啟動攝影機

開始行動規則錄影

停止行動規則錄影

拍攝快照

移動至預設點

巡邏

音訊輸出

啟動攝影機

停用攝影機

彈出影像視窗

上一步

取消



精準偵測入侵事件



觸發任務



手機即時推播

An abstract digital network background featuring a complex web of white lines and dots on a dark background, suggesting a digital or data-driven environment.

數位

A close-up, black and white photograph of a computer keyboard, showing the keys and the texture of the keyboard surface.

實體

Synology®

S Y N O L O G Y

2 0 2 0