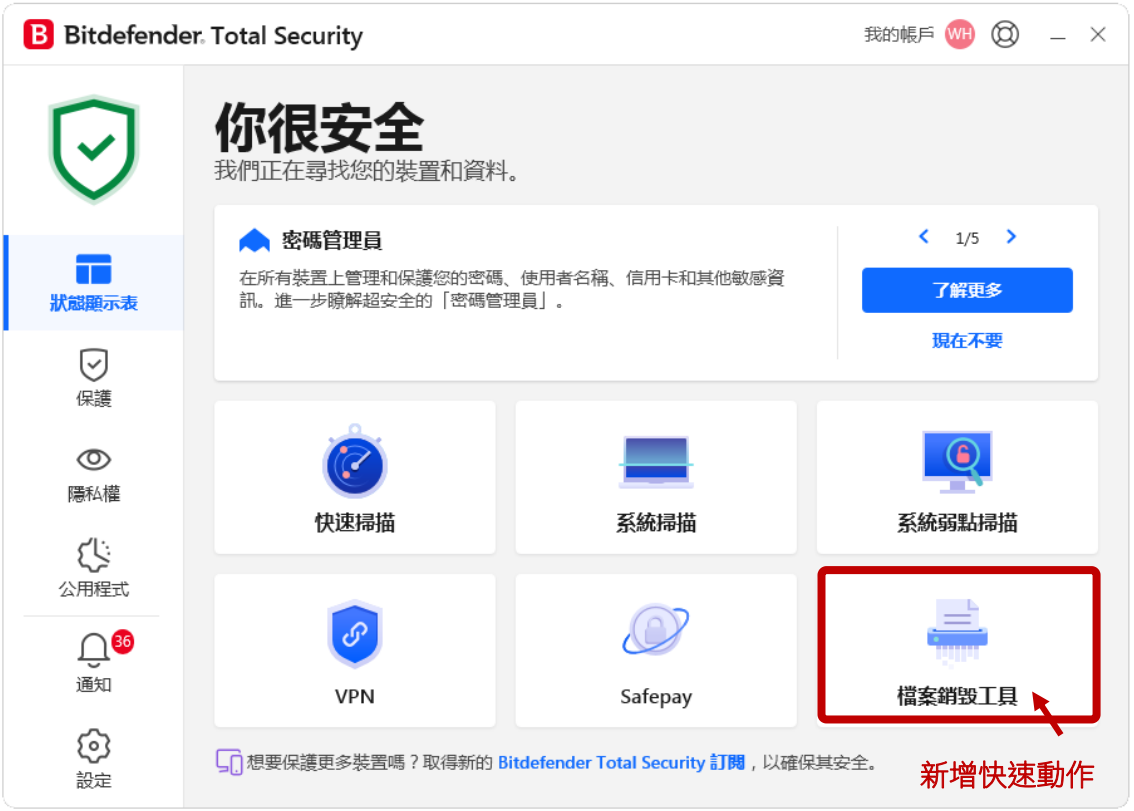
Bitdefender Total Security

功能操作說明

目錄

功能說明

狀態顯示表



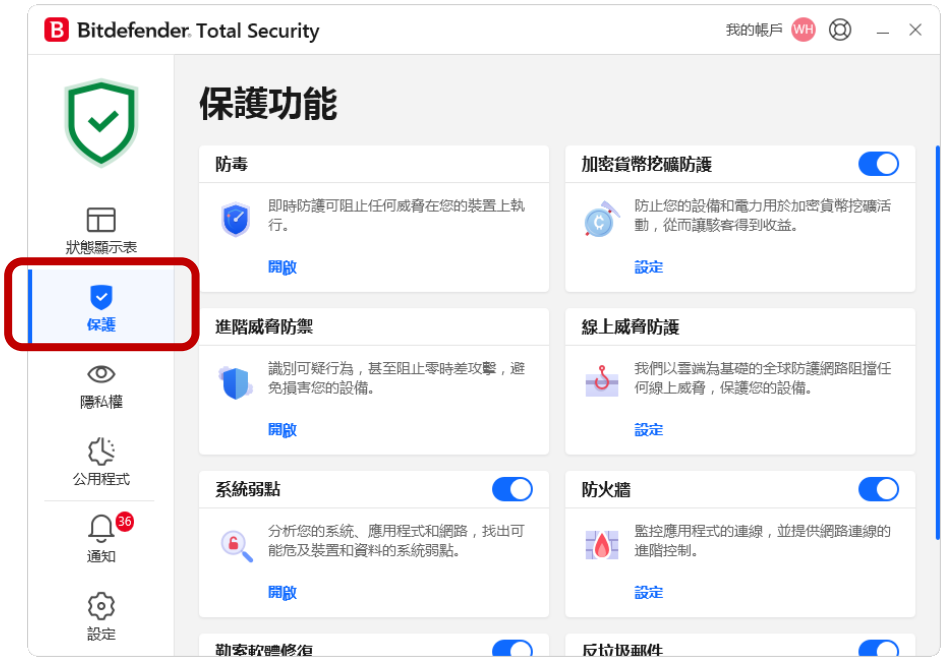
1. **快速掃描：**啟動快速掃描，僅針對檔案、軟體及部分系統檔案進行掃描。
2. **系統掃描：**啟動完整掃描，針對檔案、軟體及所有系統檔案進行掃描。
3. **系統弱點掃描：**啟動系統弱點掃描，來檢測是否有作業系統的更新未進行、設定存在虛弱性以及應用程式未更新…等，相關存在可能被駭客利用來進行攻擊的弱點。
4. **VPN：**Bitdefedner Total Seciurity 具備有 VPN 功能，並提供 200 MB/每天/每裝置，在進行需要登入帳號密碼或者金融支付等具備個人帳號或個資服務時可以使用。(註：因 Safepay 也是使用 VPN 通道，故也會計算在流量內)

5. **Safepay：**Safepay 是一個受保護的瀏覽器，存在於封閉的環境，**請注意：系統將跳出全新的背景桌面以及獨立瀏覽器，讓您搜尋支付網頁，** 旨在確保您的網路銀行、電子購物和任何其他類型的線上交易的隱私和安全性。駭客會不遺餘力地竊取個人訊息，Safepay 可防範所有針對您的銀行資料的威脅，例如駭客攻擊、網路釣魚、封包分析、「瀏覽器中間人」和「中間人」攻擊、特洛伊木馬、系統變更等。會面臨被監視或密碼被竊的風險。惡意鍵盤側錄程式無法記錄您在鍵盤上輸入的內容並透過 Internet 將報告傳送給駭客。Safepay 還可以防止惡意軟體截取螢幕截圖並偵測詐騙網站。網頁過濾技術可確保您永遠不會造訪有害網站。 Safepay 還內建了VPN，即使在公共 Wi-Fi 網路上也能保護您的機密資料。

   在啟動後於 Safepay 瀏覽器的網址列中輸入您要造訪的網站網址，便可以受到保護。更可將需要在保護狀態下的常用網站 URL 新增於書籤中，讓之後使用可以更方便。於瀏覽器右上方的功能列進入設定，可針對虛擬鍵盤及列印等功能進一步開放或限制。

6. **新增快速動作：**可將需要加入快速啟用的功能新增至此。

保護



1. **防毒：**即時檢測、防護病毒及惡意軟體的功能，預設為開啟且不可關閉。
   a. 掃描：執行、管理掃瞄作業。
   b. 設定：設定 IO 裝置是否掃描、管理例外及隔離的威脅。
   c. 進階：進階掃描功能設定。
2. **加密貨幣挖礦防護：**即時檢測設備是否有被惡意利用來進行挖礦，**預設為關閉。可於『加密貨幣挖礦防護』的設定中**
   a. 若選擇『阻止所有加密貨幣挖礦活動』，會即時檢測並且在檢測到威脅的當下立即將其阻止。並可於下方選單中選擇是否每一次阻擋都要進行阻止亦或者僅發送摘要。
   b. 若選擇『**檢測加密貨幣挖礦活動**』，則會在檢測到威脅的當下發送通知但不進行阻止，將由設備用戶自行採取適當的措施。

   或有實際的挖礦需求，也可於『**管理例外**』中將其排除於掃瞄範圍之外。
3. **進階威脅防禦：**抵禦可疑連線行為、零時差攻擊，避免設備及資料遭受損害。
   a. 威脅防禦：列出 90 天內遭受到的威脅紀錄。
   b. 設定：啟用或停用進階威脅防禦及應用程式漏洞檢測，管理例外及隔離威脅。
4. **線上威脅防護：**阻擋來自於網路及電子郵件的威脅。可依照需求設定防護範圍及內容，基本全部為啟用。
5. **系統弱點：**分析系統及應用程式，還有網路找出可能威脅到此裝置資料及系統的弱點。

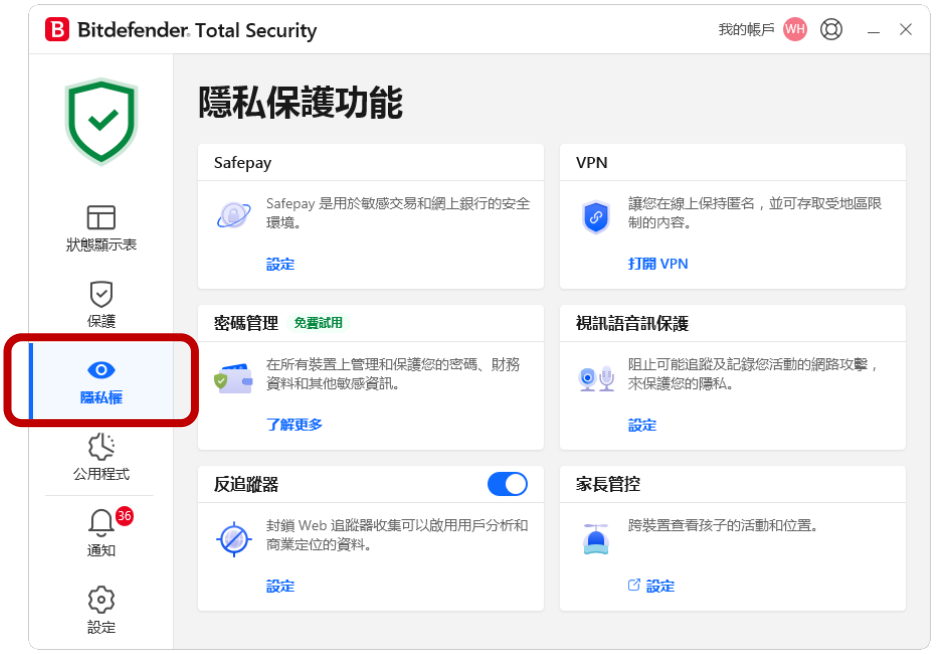
a. 系統弱點掃描：掃瞄系統並分析可能存在的弱點及漏洞。
b. Wi-Fi 安全顧問：評估無線網路的安全性。
c. 設定：設定分析的範圍及深度。

6. **防火牆：**監控應用程式的網路連線行為，並提供網路連線的進階控制。
   a. 存取應用程式：列出目前有網路連線行為的應用程式及使用的網卡。
   b. 規則：針對個別應用程式設定防火牆規則。
   c. 網路介面卡：設定及管理網卡的網路組態類型。
   d. 設定：進階設定，可針對 Port Scan 類型的網路行為進行防禦。提供網卡隱匿功能，亦可針對個別網卡設定行為。

7. **勒索軟體修復：**還原被勒索軟體加密的檔案。
   a. 例外：將特定程式設定成例外。
   b. 設定：自動還原勒索軟體加密的檔案。

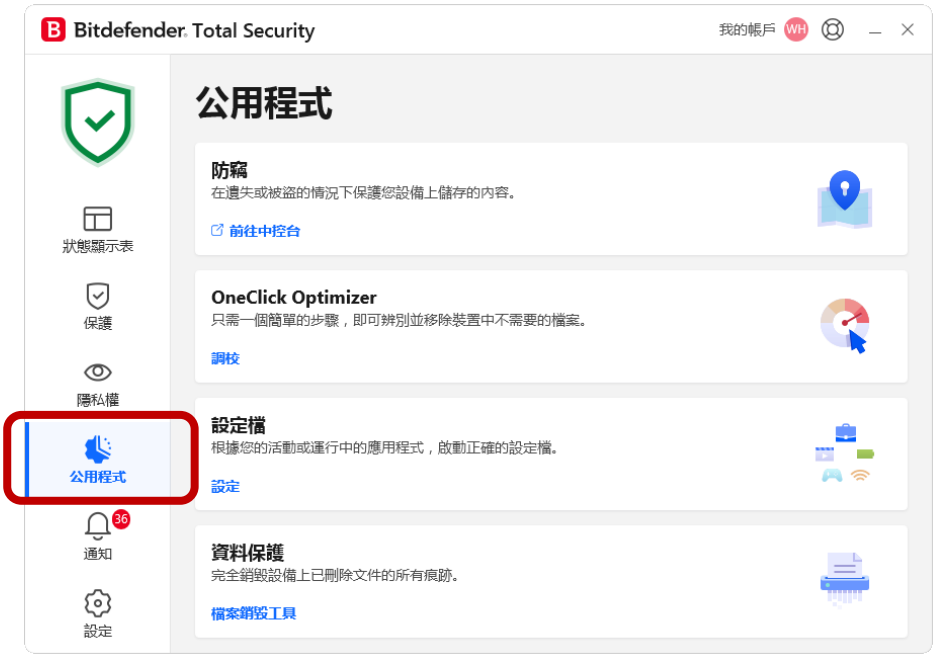
8. **反垃圾郵件：**可幫助郵件本地用戶端(例 outlook、Thunderbird 等)，過濾掉不相關的郵件。
   a. 管理朋友：將朋友的電子郵件地址或域名加入變成為白名單，不在過濾範疇內。
   b. 管理垃圾郵件來源：將電子郵件地址或域名加入變成為黑名單，將不會再收到來自此名單的郵件。
   c. 設定：可以設定來自亞洲區域語標及斯拉夫文字的電子郵件，並可設定是否提交信件樣本給原廠進行分析以改善產品。

隱私權



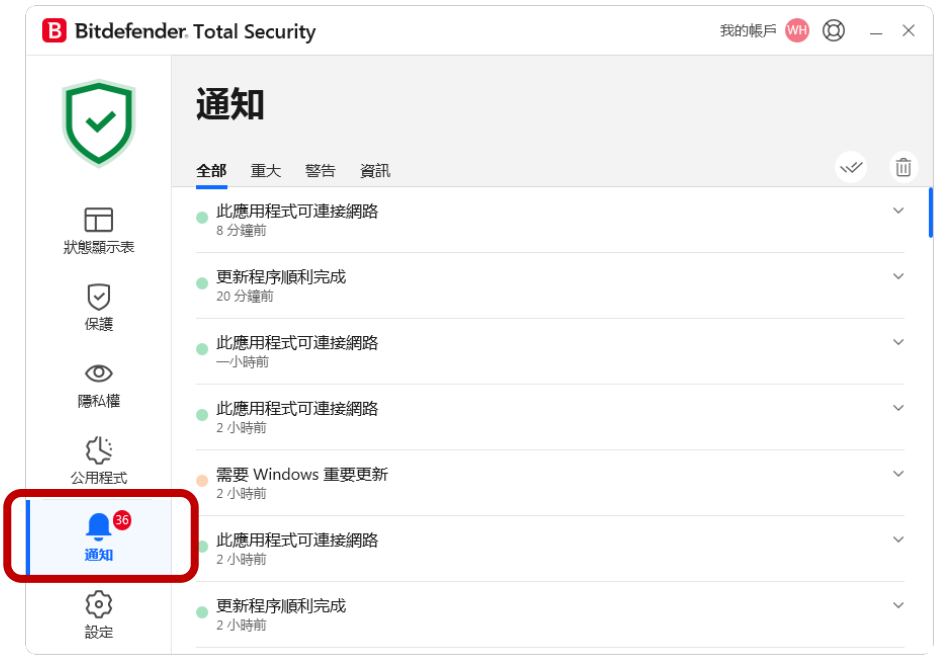
1. Safepay
   a. Safepay：啟動 Safepay。
   b. 設定：可以設定在使用銀行頁面時使用 Safepay, 使用 Safepay 將 自動啟用 VPN 獨立系統畫面。
2. **VPN：**點擊打開 VPN 便可以使用 Total Security 提供的免費 VPN 通道及每天每台裝置 200MB 的流量。
3. **視訊語音訊保護**
   a. 網路攝影機保護：本頁面設定可使用網路攝影機的應用程式清單，非在清單內的應用程式則無法使用。
   b. 音訊保護：本頁面設定可使用麥克風的應用程式清單，非在清單內的應用程式則無法使用。
   c. 設定：可針對網路攝影機及麥克風設定存取權限。
4. **反追蹤器：**封鎖瀏覽器蒐集用戶使用資料。
5. **家長管控：**可以跨裝置監控裝置的使用情況。註：此功能需於 Bitdefender Central 上使用。

公用程式



1. **防竊：** 本功能預設為啟用且不可關閉。若端點裝置失竊時， 便可透過 Bitdefender Central 中尋找裝置定位、鎖定裝置或抹除裝置上的資料。
   註：本項功能需該遺失裝置有連上網路才可以實現。
2. OneClick Optimizer：一鍵優化器，本項功能主要檢測設備中有無不需要的檔案並提供移除之功能。包含『磁碟清理』、『登入檔清除』及『隱私清理』三大功能。
   a. 磁碟清理：檢測並清理 Windows 中的垃圾檔案、暫存檔案及偵錯檔案。
   b. 登入檔清除：檢測並清理可疑及不需要的軟體登入檔、共用的 DLL 檔案。
   c. 隱私清理：檢測並清理設備的應用程式中的隱私權問題。
3. **設定檔：**Total Security 提供適用於 5 個不同情境下的設定模板給用戶使用，分別是工作、電影、遊戲、公用 Wi-Fi 環境、電池模式下，可以依照使用情境不同來進行切換，切換方式是需要先將『自動啟動設定檔』的選項關閉後，再點選下方欲套用的類型即可。
4. **資料保護：**本功能為檔案徹底刪除之功能，可避免被有心人士透過資料復原軟體將硬碟當中已經刪除的檔案還原。使用方式點選『檔案刪除工具』後，透過新增項目選擇欲永久刪除的檔案即可。
   註：檔案透過此功能刪除後便無法再回復，請謹慎使用。

通知



1. **全部：**於此頁面列出 Total Security 執行過程所有發生事件的訊息。
2. **重大：**於此頁面 Total Security 執行過程發生的高風險事件的訊息，並可以進一步展開了解詳細事件原因及建議。
3. **警告：**於此頁面列出 Total Security 執行過程中的錯誤訊息。
4. **資訊：**於此頁面列出 Total Security 執行過程的資訊。

設定

1. 一般

a. 以透過自定義的密碼來管制是否可以變更 Total Security 的設定。預設為關閉，**建議開啟以避免端點用戶隨意關閉防護功能。**開啟即未來需要變更設定就需要輸入管理員自定義的密碼。

b. 管理密碼：系統設定保護密碼。

c. 安全小工具：於作業系統畫面上顯示即時設備安全狀態的小工具。綠色為正常，紅色則需要查看『通知』中的資訊進一步釐清原因並排除。

d. 特別優惠：開啟或關閉產品優惠通知。**註：台灣地區建議至官網商店選購 https://bhv.com.tw/ ，才能享有台灣獨家18個月(一年送半年)**

e. 推薦通知：於『狀態顯示表』中顯示安全性功能的相關建議。

f. 產品語言：產品介面語系設定。

g. 深色模式：產品介面深色主題，開啟則為深色主題，關閉則為淺色主題。

2. 進階

a. Proxy 伺服器：若網路架構上有管制，需要透過代理伺服器才可連上網路，則可於此啟用代理伺服器之功能。

b. 管理代理伺服器：若啟用前一項的代理伺服器功能，則需將代理伺服器的資訊設定於此項中。

c. 產品報告：是否提供產品使用過程中遭遇到的網路威脅及攻擊情資給必特官方，以利產品改善。**預設為開啟，並且建議開啟。**

3. 更新

a. 自動更新：是否自動更新 Total Security 的端點代理程式、病毒碼以及威脅情資。**預設為開啟，並且建議開啟。**

b. 更新檢查區隔：設定前一項次中自動更新的時間區隔，**預設為 8 小時，建議可調整為 6 小時。**

c. 隱匿更新：此項主要設定更新過程是否於背景中執行，**預設為開啟，並且建議開啟**，因背景執行更新不影響端點用戶的使用體驗。