

測試與評估表	
VeraCrypt	
1. 工具概述	
姓名：	VeraCrypt
類別：	加密
目的：	VeraCrypt 是一款免費的開源磁碟加密軟體，它使用強大的加密技術來保護單一檔案、資料夾和整個磁碟機。
測試日期	2025年4月22日
文件翻譯日期：	2025年8月17日
地位：	已部署 <input checked="" type="checkbox"/> 營運中 - 積極運作/維護 <input type="checkbox"/> 測試中 - 目前正在評估或試行 <input type="checkbox"/> 不活躍/棄用 - 不再維護或運行
部署架構：	<input checked="" type="checkbox"/> 獨立軟體 - 完全在本地運行(例如, 在電腦上運行並且不依賴外部伺服器) <input type="checkbox"/> 具有獨立伺服器和用戶端元件的本機主機服務 - 自行執行後端/前端(例如, 後端可以在本機網路上, 也可以在雲端自行託管) <input type="checkbox"/> 由第三方託管的本機用戶端服務 - 您在裝置上安裝用戶端, 但它連接並依賴遠端伺服器(例如, Signal : 安裝應用程式(用戶端), 但 Signal 的伺服器處理訊息中繼等) <input type="checkbox"/> 由第三方託管但也可以自行託管的服務
版本：	2020年1月26日
2. 安裝和設定	
作業系統相容性	Windows、macOS (Monterey 12 及更高版本)、Linux、FreeBSD
安裝手冊：	Yes
安裝步驟：	<ul style="list-style-type: none"> ● 從下載安裝程式VeraCrypt 官方網站。 ● 執行安裝程式並依照 GUI 提示進行操作。 ● 可選: 如果需要安裝驅動程序, 請重新啟動 (Windows)。

	<ul style="list-style-type: none"> ● 啟動 VeraCrypt。
提及是否需要命令列設定或特殊配置	無需命令列設定或特殊配置(可以使用命令列代替 GUI, 並且具有 文件 但更複雜且不太直觀)。
常見安裝問題及修復:	<ul style="list-style-type: none"> ● 驅動程式簽署錯誤 (Windows): 停用安全啟動或手動允許驅動程式。 ● 缺少依賴項 (Linux): 使用官方軟體包安裝或安裝所需的庫 (例如, wxWidgets)。 ● macOS 權限問題: 在系統偏好設定 > 安全性和隱私權下授予 VeraCrypt 完全磁碟存取權限。 ● 更多的限制/問題
使用者文件:	是(全面的使用者指南和常見問題解答可在 官方網站)
所需的技術知識	中級(設定簡單, 但可能需要了解不同加密方法的技術知識, 但有一些相關文件)

3. 測試與評估

<u>類別</u>	<u>細節</u>	<u>分數</u>
操作功能:	<p>功能</p> <ul style="list-style-type: none"> ● 測試步驟: 使用所有主要功能驗證工具的核心功能, 追蹤任何故障或錯誤。 <p><input type="checkbox"/> 該工具基本上無法使用, 存在許多損壞的功能和缺陷。</p> <p><input type="checkbox"/> 一些功能損壞或出現錯誤</p> <p><input type="checkbox"/> 小錯誤或問題</p> <p><input type="checkbox"/> 基本功能正常, 幾乎沒有錯誤或沒有錯誤</p> <p><input checked="" type="checkbox"/> 功能齊全, 無任何錯誤</p> <p>網路依賴:</p> <ul style="list-style-type: none"> ● 安裝後無需連網。完全離線工具。 <p>在地化和語言支持</p> <ul style="list-style-type: none"> ● 支援 40 多種語言, 包括簡體中文、繁體中文、日文、韓文。並提供社群翻譯支援。 <p>移動無障礙</p> <ul style="list-style-type: none"> ● VeraCrypt 無法透過行動裝置訪問, 而且他們也不打算讓它可以訪問。 ● 他們確實在其文件中提供了適用於 iOS 和 Android 的其他選項。 	4.3

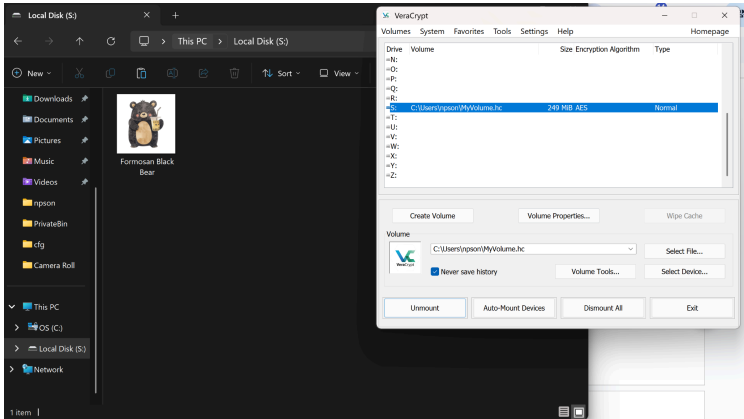
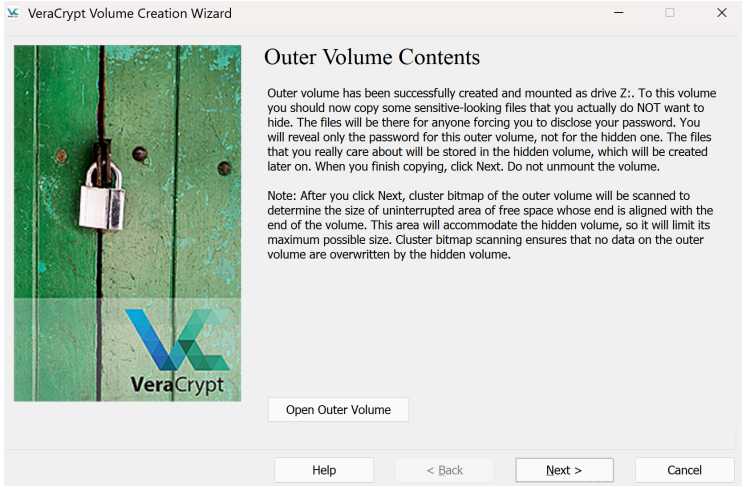
非技術用戶的可用性	<p>易於安裝和部署</p> <ul style="list-style-type: none"> ● 安裝時間為 5-10 分鐘。提供 GUI 安裝程式。根據設備規格，下載時間可能更長（僅限桌面版） ● 設定複雜性：不是一鍵安裝，而是最少的設定過程。 ● 文件：可用且經常更新。所有安全和加密功能均有詳盡的文件。 <p>使用者入門體驗</p> <ul style="list-style-type: none"> ● 擁有整個專門的初學者教學，包含豐富的 VeraCrypt 使用教學。下載 VeraCrypt 後，它會提示您閱讀教學，並直接連結到教學。 <p>所需的技術經驗水平</p> <ul style="list-style-type: none"> ● 中級 – GUI 使用者友好，但可能需要對加密、磁碟區和金鑰檔案的概念有所了解。 	4.7
安全和隱私強度	<p>加密標準</p> <ul style="list-style-type: none"> ● 包含多種加密演算法： <ul style="list-style-type: none"> ○ AES、Camellia、Kuznyechik、Serpent、Twofish、密碼級聯（其他加密演算法的不同組合） ● 儲存區資料的端對端加密 <p>哈希演算法：</p> <ul style="list-style-type: none"> ● BLAKE2s-256 ● SHA-256 ● SHA-512 ● Whirlpool ● Streebog ● 雜湊演算法用於 VeraCrypt 的隨機數產生器（用於安全加密資料的不可預測且安全的金鑰）和標頭金鑰派生（將密碼轉換為可以解密這些安全金鑰的金鑰） <p>已知強度彈性</p> <ul style="list-style-type: none"> ● 該加密軟體可以在審查和監視嚴格的地區（如中國）使用，因為它完全離線運行並且無法被檢測到。 ● 所使用的加密演算法具有極強的抗暴力破解能力，即使是強大的國家行為者也需要花費大量時間才能破解，而且難度極高。 ● 一個非常好的功能是隱藏捲和隱藏作業系統，支援“合理的否認”（在壓力下不放棄一切而透露某事的方式） <ul style="list-style-type: none"> ○ 隱藏儲存區： <ul style="list-style-type: none"> ■ 可以在定期加密的磁碟區中建立隱藏儲存區 	5.0

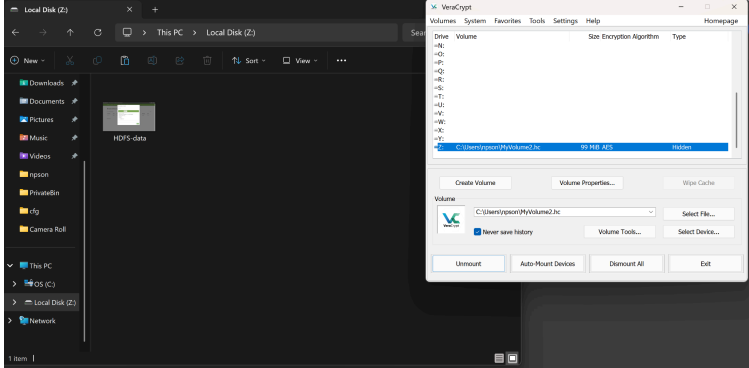
	<ul style="list-style-type: none"> ■ 可以設定具有兩個密碼的儲存區，其中一個是誘餌儲存區，另一個是包含敏感資料的隱藏儲存區 ■ 無法判斷隱藏儲存區是否存在 ○ 隱藏的作業系統(OS)： <ul style="list-style-type: none"> ■ 與隱藏磁碟區的想法相同，但作用於整個作業系統 ■ Decoy OS 的密碼不同，前者包含無害文件，後者包含真正的工作 ■ 只有你知道哪一個是真的。 <p>弱點：</p> <ul style="list-style-type: none"> ● 無檔案級加密(加密整個資料夾、分割區或虛擬設備，而不是單一檔案) <ul style="list-style-type: none"> ○ 要加密單一文件，您需要掛載整個磁碟區；要解鎖，您需要解鎖整個保險庫(不太方便) ● 沒有檔案共享或同步功能 <ul style="list-style-type: none"> ○ 加密儲存區可儲存在 Dropbox/Google Drive 中，但不會自動同步/更新 ○ 跨裝置協作困難 ● 如果有人訪問您的電腦並安裝鍵盤記錄器或監視您的設備，他們可能會懷疑某些事情並採取相應的行動。 <p>與已知標準的比較</p> <ul style="list-style-type: none"> ● 超越了許多隱私工具標準。 ● 它被許多安全專業人士使用和信任。 ● 目前最好的加密工具之一。 <p>資料最小化</p> <ul style="list-style-type: none"> ● 由於完全離線，因此不會收集任何用戶資料(不存在透過網路/互聯網追蹤任何資料的風險)。 <p>隱私權政策</p> <ul style="list-style-type: none"> ● 沒有明確的隱私權政策，但它是透明和開源的(不收集資料，因此在這方面沒有風險) 	
維護/永續性	<p>社群支持</p> <ul style="list-style-type: none"> ● 公共論壇和 GitHub 上的活躍社群。 ● 有超過 100 位貢獻者。 ● 如果有人對貢獻有疑問，可以透過網站上的聯絡資訊聯絡開發團隊。 <p>開發活躍狀態</p> <ul style="list-style-type: none"> ● 它幾乎每個月都會頻繁更新。 ● 開發團隊反應迅速，能夠清楚地查看新的貢獻並批准是否可以接受。 	4.3

	<p>資金和贊助</p> <ul style="list-style-type: none"> ● 融資金額尚未公開。 ● 無主要贊助商的獨立項目。 ● VeraCrypt 積極參與資助活動和其他支援計劃。 ● 用戶將在網站上看到捐款請求，以幫助維護該項目。 	
性能/有效性和可靠性	<p>測試環境設定：</p> <ul style="list-style-type: none"> ● 裝置：戴爾 XPS 15 ● 作業系統：Windows ● 網路：不需要（離線） <p>使用者體驗觀察</p> <ul style="list-style-type: none"> ● 從使用者的角度來看，該工具使用起來非常流暢。 ● VeraCrypt 在測試時反應非常靈敏。 ● 許多步驟都非常直觀，因為會彈出包含重要資訊和步驟的訊息。 <p>速度和反應能力：</p> <ul style="list-style-type: none"> ● 即使加密量很大，延遲也最小。 ● 安裝和卸載磁碟區時會有輕微延遲，這是可以預料的。 <ul style="list-style-type: none"> ○ 極大容量：測試了 100GB 容量，大約需要 1 分鐘來收集隨機滑鼠資料（格式化容量），然後以大約 800MB/s-1GB/s 的速度實際創建它（大約 2 分鐘）。 <p>資源使用：</p> <ul style="list-style-type: none"> ● 儲存區安裝期間的使用率較低（因磁碟區大小而異，但無論如何都相對較低）。 ● 即使對於大容量（~15MB），RAM 使用率也很低 ● 格式化磁碟區時磁碟使用率約為 800MB/s。 <p>網路效能：</p> <ul style="list-style-type: none"> ● 不適用－工具完全離線（優勢） <p>可靠性</p> <ul style="list-style-type: none"> ● 2016年奧迪OSTIF 和 Quarkslab 發現並幫助修補了幾個問題，大大提高了可靠性。 ● 在加密設計中沒有發現後門或致命缺陷。 ● 特別是在優先考慮隱私的社會中，VeraCrypt 在安全性和功能性方面都被認為極為可靠。 ● 如果使用得當，很少會失敗。 	5.0
部署注意事項：	<p>開源與透明度：</p> <ul style="list-style-type: none"> ● 原始碼可供獨立驗證。 <p>雲端部署與本地部署：</p> <ul style="list-style-type: none"> ● 完全在地化 <p>依賴項：</p>	

	<ul style="list-style-type: none">● 需要少量依賴項(如果有)—安裝程式幾乎可以處理所有依賴項。在 Linux 上, 一些 GUI 可能需要依賴項, 例如libwxgtk。 <p>部署後維護</p> <ul style="list-style-type: none">● 在潛在部署之後, 該工具易於維護(部署它可能非常複雜且沒有必要, 因為有經過審核的發布版本可用)。 <p>合併/可持續性:</p> <ul style="list-style-type: none">● 積極接受拉取請求和改進, 同時在貢獻標準上列出 README 第四部分。	
--	---	--

4. 測試場景

<ul style="list-style-type: none">● 場景 1 建立並掛載標準加密儲存區	 <ul style="list-style-type: none">●● 按照 VeraCrypt 網站上的初學者教學, 建立和安裝標準加密磁碟區非常簡單。● 有時可能會出現作業系統權限錯誤。這僅僅意味著儲存區宗無法位於某個目錄中。	
<ul style="list-style-type: none">● 場景 2 建立並掛載隱藏加密儲存區	 <ul style="list-style-type: none">●	

	 <ul style="list-style-type: none"> ● 此場景也很簡單，步驟與標準加密磁碟區非常相似。但是，請務必閱讀此文件關於如何在對外部磁碟區進行更改時保護隱藏磁碟區。 ● 這對於合理否認來說是一個非常好的功能，因為個人可以在必要時「放棄」誘餌儲存區，同時確保真實資訊的安全。此外，隱藏儲存區的存在也無法得知。
<h2>5. 見解和建議</h2>	
<p>主要發現</p>	<p>優勢：</p> <ul style="list-style-type: none"> ● VeraCrypt 使用強大的加密標準，例如 AES256、Serpent 和 Twofish。它們甚至可以防禦高級取證級攻擊。 ● 該工具是開源的，並且已經經過獨立的安全審核，以使其更加安全並在解決漏洞的同時改進其他功能。 ● VeraCrypt 完全在本地運行，不需要互聯網連接，它可以與隔離的電腦一起使用，並消除了透過線上服務洩露資料的可能性。 ● 支援隱藏捲和隱藏作業系統，允許使用者在脅迫或審訊下否認加密資料的存在。 <p>弱點：</p> <ul style="list-style-type: none"> ● VeraCrypt 目前不支援 iOS 和 Android 系統，這限制了高度依賴行動裝置的用戶的使用。解決方法是使用第三方工具，但這可能會帶來安全風險。 ● VeraCrypt 不會加密單一文件，而是加密整個磁碟或分割區。即使是小文件，使用者也必須維護容器，並且文件必須在磁碟區內傳輸才能確保安全。在掛載整個容器之前，無法即時加密單一檔案。 ● 每次需要使用時都必須手動安裝磁碟區（可能不太無縫）。
<p>建議的改進</p>	<ul style="list-style-type: none"> ● 開發行動相容版本（已經聲明他們沒有這個計劃） ● 新增檔案級加密
<p>替代工具：</p>	<p>Cryptomator、GnuPG (GPG)、Age</p>

授權	Apache License 2.0
成本/資源影響	<p>總成本：</p> <ul style="list-style-type: none"> ● 該工具完全免費使用。 ● 使用者可以捐款(如果願意/非必要)以幫助改善和維護 VeraCrypt ● 維護、第三方整合或更新無隱藏成本。
為什麼這對威權環境中的公民社會有用？	<p>VeraCrypt 對威權環境下的公民社會組織和人權捍衛者極為有用。這得歸功於其先進的加密和雜湊演算法，可以保護記者、活動家、舉報人等敏感資料的安全。此外，其最佳功能之一是合理的否認性。即使在強制解密或檢查的情況下，您也可以合理地否認隱藏作業系統或磁碟區的存在，因為它在磁碟上不可見。</p> <p>例如，我如果記者正在報導一個非常危險的政治話題，並且擁有敏感資料，他們可以創建一個隱藏儲存區並將其儲存在那裡。記者也會將真實的文件加入外部磁碟區。如果這名記者隨後被中國官員攔下並被迫交出密碼(例如，在邊境檢查站或接受訊問時)，他們可以提供密碼A(外部儲存區的密碼)。官員可以打開它，查看“無辜”的資料，而無法知道還有更多內容。由於 VeraCrypt 的隱藏磁碟區加密於主磁碟區的可用空間內，並以隨機資料的形式顯示，因此如果沒有正確的密碼，隱藏磁碟區將無法被偵測到。即使檢查了主磁碟，隱藏儲存區的存在也具有合理的可否認性。這確保瞭如果沒有隱藏儲存區的密碼，就無法證明其存在。</p> <p>注意：務必確保無人時刻監視您的電腦，或安裝鍵盤記錄器之類的程式。在這種監控環境下，這些人可以追蹤檔案更改或查看您輸入的密碼，這可能會讓他們誤以為您隱藏了某些內容或發現了隱藏儲存區。除此之外，隱藏儲存區將無法存取。</p>