Synology

保護您的組織，不受勒索軟體攻擊

根據預測，光 2023 年，勒索軟體攻擊就可能對組織造成總共 8 兆美元的損失。[1] 具有快速還原選項的資料保護計畫，對於減輕勒索軟體及其他形式的網路犯罪影響至關重要。

Date 2023年10月13日

備份：災害來臨時的最後一道防線

事前備份可幫您即時還原關鍵任務資料，避免資料遭惡意刪除或竄改而蒙受損失，也能有效縮減服務停機時間。Synology 更提供多元資料保護解決方案，能協助您輕鬆規劃並落實完整 IT 基礎架構的備份策略。

面面俱到的保護

保護端點和主要服務，為您的資料建構層層安全網。

快速復原

透過即時復原選項，最小化災害發生時的停機中斷時間。

不可變儲存空間

能防止他人未經授權而擅自更改資料和快照。

免授權備份

無隱藏費用，只要您的 Synology 伺服器容量足夠，即可無上限備份所有裝置或平台資料。

集中防範勒索軟體

集中備份四散於工作站、伺服器、虛擬機器和雲端應用程式的重要資料，並支援去重複技術和增量備份，可達到儲存空間的最佳消耗，消除頻寬瓶頸。
https://www.synology.com/dsm/solution/infrastructure

實體工作負載

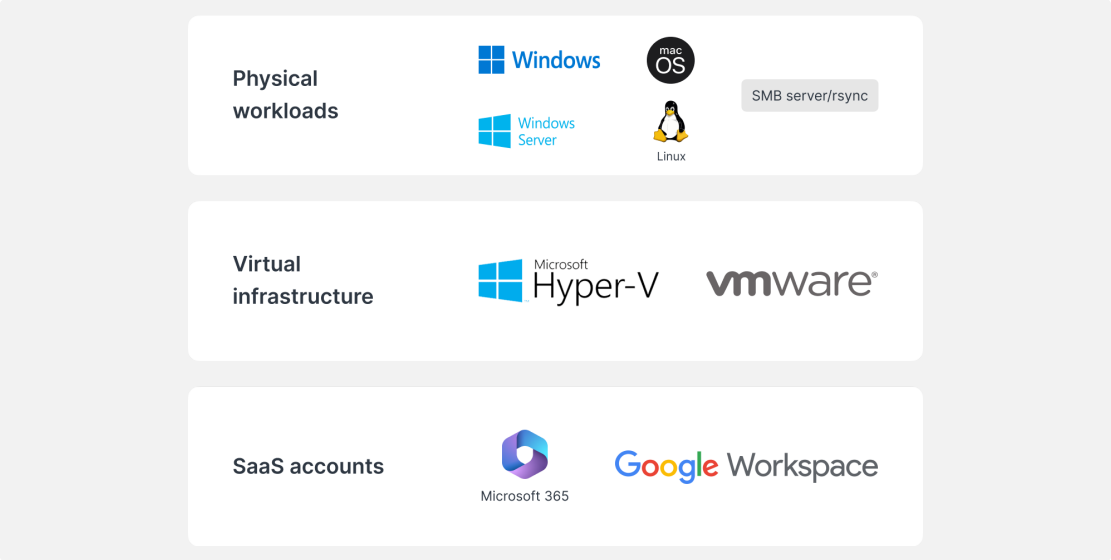
全面的裸機備份和靈活的精細檔案復原可以在發生惡意攻擊時，有效保護端點。

虛擬基礎架構

採用強大的資料減量技術，備份 VMware® vSphere™、Microsoft® Hyper-V® VM 和 LUN。

公有雲服務帳號

系統將自動偵測新增的帳號，確保所有雲端資料持續受到保護。



高效率復原

從本地或異地 Synology 伺服器快速還原，大幅節省關鍵服務的停機時間。

RTO 近乎為零

將備份映像檔裝載在 VMware®、Hyper-V® 或 Synology Virtual Machine Manager 上，加速讓系統恢復運作，將 VM 還原到替代 Hypervisor 則可避免服務中斷。

大幅降低 RPO

您可以自訂備份頻率，大幅降低遭受攻擊時，可能影響到的資料量。並透過增量備份和重複資料刪除技術，確保系統能快速獲得保護，同時節省儲存空間。

直覺化操作

讓員工透過便利的入口，先預覽電子郵件、聯絡人和檔案，再進行還原，不但讓使用體驗更人性化，還可減輕 IT 團隊的工作負擔。

增添多一層的保護

謹守 3-2-1 備份策略，將第三份資料儲存在異地或雲端，這可以防止您的資料因火災、自然災害或竊盜而遭受損失。

備份到異地伺服器

將備份儲存到次要位置的 Synology 伺服器，抵禦物理災害的影響，同時複寫不可變快照，以增強勒索軟體保護。

備份到雲端

備份到任何主要雲端儲存供應商，並透過用戶端 AES-256 加密保護您的資料，避免他人未經授權擅自存取。 https://c2.synology.com/storage/nas

贏得各行各業的信賴

「Synology [...] 讓我們減少了伺服器硬體支出 [...] 同時讓基礎架構與工作站備份、系統日誌和檔案管理更加輕鬆。」
https://www.synology.com/company/case_study/Investortools

「有了 Active Backup for Business，我們所有的備份現在全都集中處理，並且全天候隨時可用，這有助於我們將停機時間降到最低，並確保遵循 FERPA 法規。」
https://www.synology.com/company/case_study/University_of_Washington

「[...] 經過測試後，我們發現 Active Backup for Business 的備份速度驚人，刪除重複資料的工作表現更讓人嘖嘖稱奇，在總共 58 TB 的伺服器上只占用 28 TB。[...]」
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

「[...] Active Backup for Business [...] 讓我們在單一主控台集中管理所有備份任務。復原既快速又可靠，也確保讓營運不中斷。」
https://www.synology.com/company/case_study/UNESCO

常見問題

什麼是勒索軟體？

勒索軟體是一種惡意軟體，會將受害者的檔案予以加密。接著，攻擊者會要求受害者支付贖金，才能取回資料，常會威脅受害者，如果拒不配合，資料將會被永久銷毀。勒索軟體攻擊可能具有高度破壞性，並對個人和組織造成重大經濟損失。所以，保護您自己和您的裝置免於勒索軟體的侵害非常重要，例如您可以確保軟體保持最新狀態並定期備份檔案。

勒索軟體有哪幾種？

勒索軟體有許多類型，並且還不斷有新的變種出現。幾個最常見的勒索軟體類型包括：

- **加密型勒索軟體** — 這是最常見的勒索軟體類型，會加密受害者的檔案，沒有解密金鑰就無法存取這些檔案。攻擊者接著會要求受害者支付贖金以換取金鑰。
- **Locker 勒索軟體** — 這種類型的勒索軟體會更改登入憑證或顯示一則訊息來阻止受害者存取他們的系統，把受害者鎖在電腦之外。接著，攻擊者會要求支付贖金，才會解鎖電腦。
- **勒索軟體即服務 (RaaS)** — 這是一種商業模式，攻擊者提供勒索軟體給其他個人或團體以執行攻擊。通常是前者提供勒索軟體並處理付款，而後者則從中收取一定比例的贖金。
- **恐嚇軟體** — 這類的勒索軟體旨在恐嚇受害者支付贖金，典型的手法是顯示假的安全警告或訊息，聲稱受害者的電腦已中毒。接著，攻擊者會要求支付贖金以將其移除。

勒索軟體如何散播？

勒索軟體通常透過網路釣魚電子郵件或利用電腦系統漏洞進行散播。網路釣魚的攻擊者寄來的電子郵件，可以偽裝成來自法來源 (例如銀行或知名公司)。該電子郵件通常含有一個連結或附件，點選後就會在受害者的電腦上安裝勒索軟體。利用系統漏洞也是類似手法，只是攻擊者是利用系統安全漏洞，在受害者不知情的情況下安裝勒索軟體。不論是以上哪一種情況，勒索軟體一旦安裝，便會迅速散播到同一網路上的其他電腦。

典型的勒索軟體攻擊過程是如何進行的？

勒索軟體攻擊的過程通常是按照以下步驟進行的：

1. 攻擊者寄出網路釣魚電子郵件或利用系統漏洞，取得對受害者電腦的存取權限。
2. 攻擊者一旦可以存取受害者的電腦，就會在系統上安裝勒索軟體。
3. 勒索軟體接著將受害者的檔案加密，讓使用者無法存取檔案。
4. 接下來，攻擊者向受害者索討贖金 (通常要求以比特幣等虛擬貨幣支付)，以換取解鎖加密檔案的解密金鑰。
5. 如果受害者支付贖金，攻擊者將提供解密金鑰，讓受害者能再次存取他們的檔案。但是，不保證攻擊者會真的提供金鑰，即使提供了，受害者的檔案也可能因加密過程而遭受破壞或損毀。

請務必注意，攻擊過程千變萬化，並非所有勒索軟體都完全按照這些步驟進行。例如，有些攻擊可能根本不需要加密檔案，有些攻擊可能另外要執行其他形式的敲詐或勒索。

哪些行為容易感染勒索軟體？

感染勒索軟體有幾種侵入管道。最常見的一種方式是點選網路釣魚電子郵件中的惡意連結或附件。這種類型的電子郵件貌似合法電子郵件地址，常常看起來像是來自知名公司或組織。當您點選信中的連結或附件，勒索軟體就會安裝到您的電腦上。 可能感染勒索軟體的另一種方式，是透過中毒網站。網站已遭到攻擊者駭入，並插入了程式碼，如果您進入這個網站，這些程式碼會自動在您的電腦上安裝勒索軟體。 此外，您也可能從網路下載了中毒檔案，並因此感染勒索軟體。從可疑網站下載檔案，或是下載不認識的人分享的檔案，都可能會發生感染情況。 簡單說，瀏覽網站時務必謹慎小心，應避免點選連結或從不熟悉的來源下載檔案。這樣做能有助於防止感染勒索軟體及其他類型的惡意軟體。

誰是勒索軟體的目標？

使用電腦或其他裝置連接網路的任何人，都可能成為勒索軟體攻擊的目標。不過，某些團體比別的團體更容易成為攻擊目標。舉例來說，勒索軟體攻擊通常以企業為目標，因為企業常擁有更有價值的資料，並且可能更願意支付贖金來取回這些資料。醫院、學校、其他提供緊急服務的組織也是常見的目標，因為勒索軟體攻擊可能會破壞他們的營運，令人們的生命面臨危險。 個體也可能成為勒索軟體攻擊的目標。此時，攻擊者可能試圖威脅刪除受害者的個人檔案或公開敏感資訊來勒索錢財，除非受害者支付贖金。 勒索軟體通常是根據資料的價值，以及支付贖金以取回資料的意願來選擇攻擊的目標。

支付贖金給勒索軟體會有哪些風險？

向勒索軟體攻擊者支付贖金，似乎是取回檔案的最簡單方法，但這可能其實是一個非常冒險的決定。支付贖金風險不少，包括：

- 不保證攻擊者真的會提供解密金鑰。很多情況是，受害者已支付贖金，卻永遠沒收到金鑰，仍然無法取得他們的檔案。
- 支付贖金可能會鼓勵攻擊者，助長攻擊的氣焰。當攻擊者知道受害者願意支付贖金，未來就可能會發動更多的攻擊。
- 支付贖金可能會使你被標記為未來攻擊的目標。當攻擊者知道你願意支付贖金，未來很可能繼續對你發動攻擊。
- 支付贖金可能會成為非法行為。某些情況下，向犯罪組織支付贖金可能被視為資助恐怖主義或其他非法活動的一種形式。

雖然支付贖金似乎是取回檔案的最簡單方法，但這可能其實是一個非常冒險的決定。所以務必審慎評估風險，再做決定。

勒索軟體的代價是多少？

勒索軟體攻擊的代價可能會因多種因素而有很大差異，例如，所使用的勒索軟體類型、加密檔案的數量以及攻擊的有效性。在某些情況下，勒索軟體攻擊的代價可能相對較低，攻擊者只索討幾百美元的贖金。在某些情況下，代價可能會高出許多，攻擊者要求支付數千美元、甚至更高，才願意還回受害者的檔案。 除了與支付贖金相關的直接成本外，勒索軟體攻擊還可能產生高昂的間接成本。例如，勒索軟體攻擊可能導致停機和產能損失，進而導致損失營收和收入。不僅如此，也會損害公司商譽和客戶信任，對營運帶來長期負面影響。這些間接成本常常遠高過贖金本身。

勒索軟體的感染症狀有哪些？

勒索軟體攻擊的感染症狀會因所使用的勒索軟體不同而異。但是一些常見症狀包括：

- 檔案已加密，無法存取。
- 收到攻擊者的勒索訊息，須支付贖金來換取解密金鑰。
- 看到不熟悉的程式或處理程序在電腦上執行。
- 電腦變得很慢或無回應
- 電腦顯示不正常的錯誤訊息或快顯視窗

如果懷疑自己的電腦中了勒索軟體，務必馬上採取行動。立即中斷電腦的網路連線，防止勒索軟體擴散。

如何預防勒索軟體攻擊？

您可以採取幾項行動來防止勒索軟體攻擊，包括：

- 使用信譽良好又知名的防毒軟體或資安軟體，並讓軟體保持在最新狀態。這樣做能有助於保護電腦，遏止勒索軟體及其他類型的惡意軟體入侵。
- 打開電子郵件附件或連結的時候，請務必小心看清楚。勒索軟體常透過網路釣魚電子郵件散播，因此請務必注意所要點選的內容。
- 讓您的作業系統及其他軟體保持在最新狀態。軟體更新項目經常包括安全修補程式，有助於保護您的電腦，免於勒索軟體和其他威脅。
- 定期執行檔案備份，一旦電腦不幸遭受勒索軟體入侵，備份有助於找回資料。記得要遵循建議的備份策略，像是 3-2-1 備份策略。
- 掌握勒索軟體的風險，並讓組織中的其他人了解這類的安全威脅，這樣做能有助於防止勒索軟體攻擊，萬一感染也更容易偵測出來，並做出應變。

防止勒索軟體攻擊的最佳方法，就是保持警惕，並採取相關措施來保護電腦和資料。這樣將有助於降低勒索軟體攻擊的風險，不幸感染勒索軟體時，也更容易恢復正常。

Synology 如何保護我免於勒索軟體攻擊？

為了防止成為勒索軟體的受害者，積極的預防措施有其必要。您可以使用 Synology 解決方案，再搭配自選的防病毒軟體，即可達到保護相輔相成效果：

- **阻止存取** — 用 Secure SignIn 和 C2 Password 設定檔案、應用程式和存取權限，以及設定安全登入憑證，將可減少勒索軟體的散播。
- **保護裝置** — 過時的系統有更大的風險。透過 Synology Central Management System (CMS) 可以一次更新所有 NAS，使用 Synology Directory Server 和 C2 Identity 中的群組原則可保護其他裝置。
- **避開可疑檔案** — 含有可疑檔案的垃圾郵件和網路釣魚電子郵件是常見的勒索軟體手法。Synology MailPlus 提供強大的反惡意軟體防護和垃圾郵件防範功能。
- **檢查漏洞** — 您可以使用 Synology Security Advisor 定期掃描惡意軟體、漏洞和異常登入活動，並實施建議的處理行動，以提高您的 NAS 安全性。
  https://www.synology.com/dsm/overview/security

更多保護資料的方法

管理您的機組

利用廣泛多樣的功能，集中管理資料存取權限、軟體狀態、系統健康度等。
https://www.synology.com/dsm/overview/administration

監控您的所有系統

無論您的裝置位於何處，都能偵測到可疑的登入活動、管理更新並監控裝置健全狀況。
https://www.synology.com/dsm/feature/active-insight

為資料提供安全保障

遵循 3-2-1 備份規則，保護您的資料免於任何意外或惡意的修改或刪除。
https://www.synology.com/dsm/solution/data_backup

開始使用

聯繫我們

詳情請洽各地業務單位
https://www.synology.com/form/inquiry/sales

經銷資訊

尋找您所在地區的 Synology 合作夥伴
https://www.synology.com/wheretobuy

注意事項：

1. eSentire，2022 年官方網路犯罪報告 https://www.esentire.com/resources/library/2022-official-cybercrime-report

保護您的組織，不受勒索軟體攻擊

https://www.synology.com/zh-hk/dsm/solution/ransomware

Synology 官網

https://www.synology.com/

聯繫我們

https://www.synology.com/company/contact_us