Acronis

白皮書

Acronis 掃描備份中有無惡意軟體

在不犧牲安全性或可用性的情況下以非破壞性的方式執行

備份和防惡意軟體是現代端點安全性態勢的兩個重要部分。在備份之前，通常會掃描有無惡意軟體，已經發生過多次惡意軟體一路長驅直入地入侵備份映像了。這樣的事通常發生在兩個情況，一個是由於使用的一般防惡意軟體解決方案僅提供有限的偵測功能，另一個是在進行防惡意軟體掃描前就已完成備份。

為偵測惡意軟體而完整掃描大型封存檔 (包含備份)，需要相當多的時間和運算資源。結果，這些都在浪費時間和資源。話雖如此，如果封存檔不是儲存在本機，而是在雲端的話，掃描封存檔就變得格外重要了，因為存取雲端的封存檔的速度可能遠比存取本機儲存裝置還要來得慢 (端看所使用網路或通訊的速度，和/或通道的負載程度而定)。此外，如果封存檔中發現病毒和/或惡意檔案，該封存檔就被視為已損毀或遭感染，可能無法當作系統復原或檔案及資料擷取之用。

往常的作法是，封存檔在儲存期間，若要新增切片至封存檔時和/或在復原資料前，會定期以防毒掃描程式進行掃描，以避免復原的遭到感染的檔案。然後，現在已經沒有解決方案會允許自訂封存檔的掃描時機或範圍了。反之，解決方案都被迫要掃描整個封存檔。而且也無法修復封存檔中的已損毀或遭到感染的資料。

Acronis 技術正是一切問題的解答

典型的系統管理員必須管理一堆機器和對應的備份機器。處理上述機器的所有問題並隨時面對其他難題是他們工作的一環。例如，備份的系統磁碟機並不是唯一一個容易遭受惡意軟體攻擊的部分。裝置的作業系統和第三方應用程式也可能成為感染的閘道。

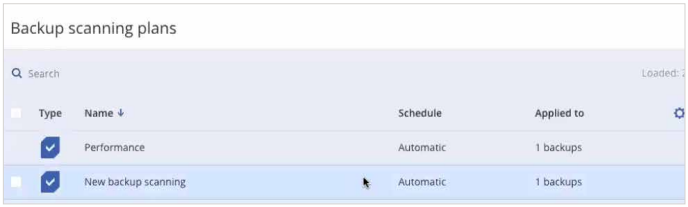
修補機器及套用最新的防惡意軟體定義碼，可讓系統管理員復原能抵擋週期性感染的作業系統映像。在集中位置正確且有效地掃描備份中有無惡意軟體，是另一個確保安全復原和安全資料儲存的必要步驟。這正是 Acronis Cyber Protect 所帶來的強大功能。

透過 Acronis Cyber Protect，使用者能在集中位置 (Acronis Cloud 或未來能將支援擴大至 Amazon、Google、Microsoft 或其他常用的雲端儲存空間環境的地端部署伺服器) 掃描完整磁碟備份，以找出潛在的弱點和惡意軟體感染，進而確保可以使用不含惡意軟體的備份來進行不含惡意軟體的復原 (若將來有此必要的話)。

Acronis 的工程師讓您除了能檢查大型的備份，也能檢查封存的切片，以找出惡意軟體。我們能將備份封存檔裡的多個切片中的第一個切片掛接到磁碟上，其中第一個切片是首次作為使用者資料的映像。Acronis 技術可以偵測掛接切片的修改區塊、識別對應偵測修改區塊的第一個掛接切片中的檔案，並掃描特定檔案中有無病毒或其他惡意軟體。這個方法還可以讓 Acronis 產生入侵第一個掛接切片使用者資料的修復切片，而不包含惡意檔案。藉由掃描集中位置，Acronis Cyber Protect 可以讓使用者執行以下動作：

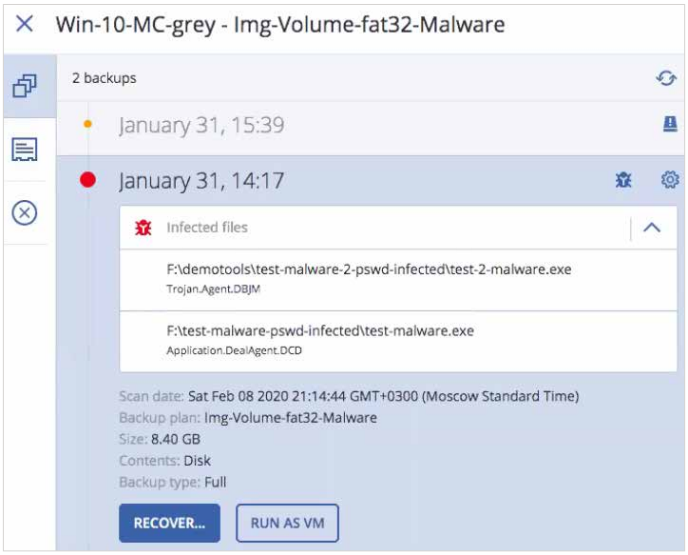
- **降低用戶端端點的負載**
- **僅還原無害資料**
- **提升根目錄套件和開機套件偵測的可能性 (在第一次即時監視或隨選掃描期間難以偵測)**

這表示管理員能定期執行備份掃描，而且能掃描集中位置裡每個用戶端的備份增量中有無惡意軟體。第一版的 Acronis Cyber Protect 僅會將 Acronis Cloud 儲存空間視為集中位置並進行支援。在未來的反覆項目中，支援將擴大至 Amazon、Google、Microsoft 或其他常用的雲端儲存空間環境。



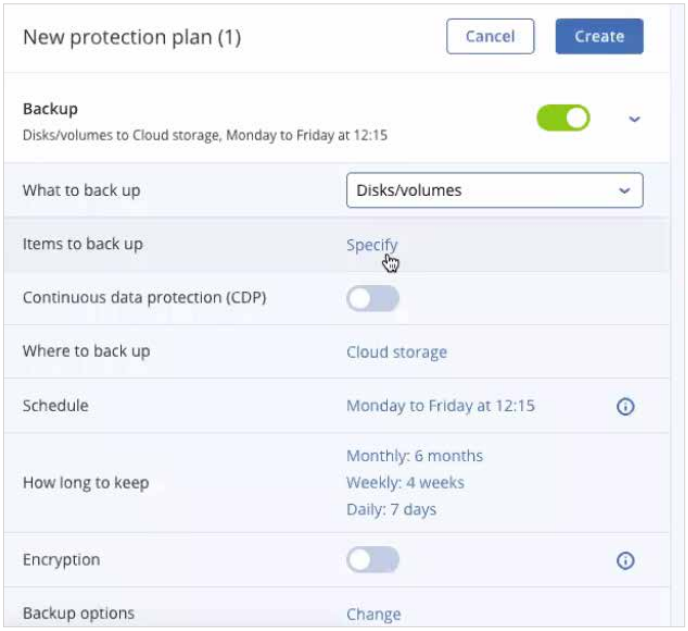
一旦完成，管理員不只會有復原點，還有標示的「安全復原點」，這裡沒有偵測到惡意軟體。

管理員可以使用 Acronis Cyber Protect 管理主控台詳細查看已發現哪些受到感染的檔案和出現的時間。他們可以從該處清除備份切片中的惡意軟體，並復原無害的資料副本。所有透過 Acronis Cyber Protect 執行的備份掃描會使用最新的惡意軟體定義碼，所以即使最初沒有偵測到未知的惡意軟體，也會在下次完整備份掃描中識別出來。



目前，Acronis 技術支援完整磁碟或含增量選項的磁碟區備份，但不支援檔案備份。

當其他產品還只處於掛接並掃描整個映像的階段，Acronis 能在掃描初始切片後快速掃描新的切片，同時兼顧彈性與效率。這表示速度將比完整掃描快上數倍 (實際的結果端看磁碟區映像的大小及競爭對手掃描引擎的效能而定)。Acronis 技術使用其 Archive 3 儲存格式 API 的進階功能和 NTFS 檔案系統功能，這也是另一個運作能發揮超高效能的原因。



如有必要，備份也能在本機上進行掃描。例如，小型企業會在儲存備份磁碟區時使用網路共用。您不需要 Acronis Cyber Protect 代理程式即可涵蓋檔案儲存空間。在這個情況下，您可以從網路中能存取儲存空間並已安裝 Acronis Cyber Protect 代理程式的任何機器執行掃描工作。

下一步是清除完整磁碟/磁碟區備份中的潛在弱點。惡意軟體透過本機網路散播並利用單一未經修補的弱點感染機器的實際案例比比皆是。機器在復原後再次受到感染，只因惡意軟體在作業系統運作環境恢復上線時再度迅速感染。為避免這類危險的情況，您可以在完整機器復原作業期間修補軟體，以排除惡意軟體入侵弱點的可能性。Acronis Cyber Protect 很快就會推出這項功能，這項功能目前處於開發階段，接下來便會進行測試和品質保證。

入侵止步：
完全交給頂級的防惡意軟體防護

備份時常受到惡意軟體感染。有些企業會掃描集中位置中的備份，但連續執行定期掃描需要耗費很多時間。使用中的惡意軟體也會一再感染未經修補的磁碟映像。每日或甚至是每週的完整磁碟隨需掃描工作相當費時，且往往無法在非工作時間進行，這表示掃描會不斷打亂員工的工作，使其失去生產力。

但現在有更好的防惡意軟體防護方式：快速掃描端點，並在備份後於集中位置執行剩餘的掃描。使用 Acronis Cyber Protect，您就不需要在效能與安全性之間糾結了。

這項 Acronis 的全新產品將網路資安與頂級的備份技術整合到一個代理程式中。我們因此得以涵蓋網路資安防護的兩大基本層面，並清除現代威脅。相較於其他解決方案，管理員也能更快地掃描備份，並能確信可在沒有任何惡意軟體或回報的弱點下復原系統。