Acronis

白皮書

多層次網路資安：現代網路資安防護的一部分

整合各項技術
以提升防禦能力

資料是最重要的企業資產。隨著世界逐漸轉型成為數位化，資料在質與量方面跟著提升。事實上，這項現代社會最重要的資源，每年的數量都會倍增，而該成長率很可能會更往上飆升。當然，這也帶來了挑戰：您是否以安全的方式儲存資料，而您又要如何確保您對資料進行的每項操作都受到保護？如今，資料外洩等於搞丟一切，包括業務、身分識別、未來，在某些情況還可能丟了性命。

一般來說，您這樣的企業會有兩套方法處理這個挑戰。防毒和防惡意軟體控制的系統安全性，可提供安全的環境，另一個則是備份解決方案管理的資料，可確保能隨時取得資料的副本。雖然防惡意軟體和備份代理程式通常安裝在相同的端點，卻不會互相聯繫，無法保證在事件發生時能快速復原資料。

Acronis Cyber Protect 克服了這項挑戰，同時在新建的網路資安防護空間中，新增了其他必要的功能。

為什麼要加強網路資安？

現代網路攻擊、資料洩漏和勒索軟體爆發都表明了同一件事：網路資安是失敗的。出現此失敗狀況的原因是，技術薄弱和聰明的社交工程導致人為錯誤。在備份解決方案運作良好且未被盜用的情況下，通常需要幾小時和幾天的時間來將系統 (含資料) 還原至運作狀態。網路資安解決方案失敗時備份是必要的，但同時備份解決方案可能會被盜用、停用，緩慢地執行，導致企業因停機時間而損失大量的資金。

為了解決這些問題，Acronis 開發了 Acronis Cyber Protect：這個網路資安防護解決方案將防惡意軟體和備份程式整合到一系列 Windows 作業系統底下執行的單一代理程式。此整合可讓您維持最佳的效能、消除相容性問題，及確保快速地復原。如果在資料改動期間未發現或偵測到威脅，則會立即從備份還原該資料，因為它的一個代理程式，知道資料已遺失且需要還原。

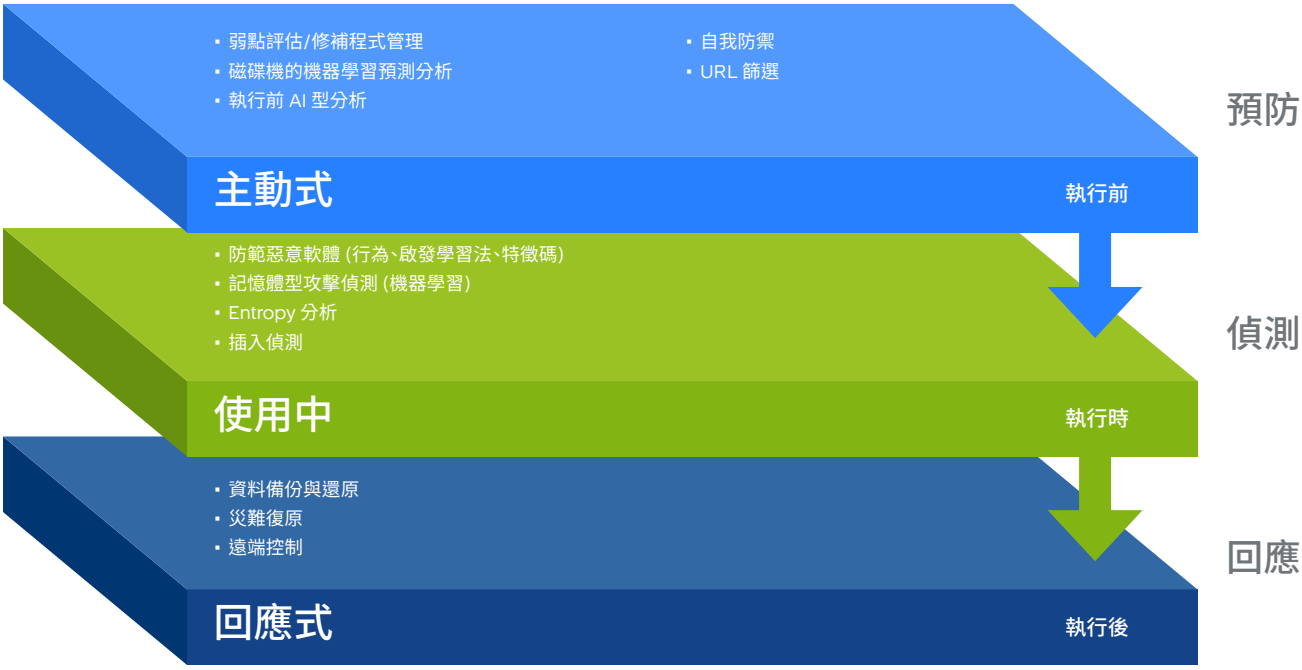
當防惡意軟體代理程式與擁有自己的代理程式的備份產品分開時，這一點無法實現。您的防惡意軟體解決方案可能會停止威脅，但部分資料可能已經遺失。備份代理程式不會自動辨識出威脅，而在最好的情況下，會緩慢地還原資料 (如果有的話)。

當然，Acronis Cyber Protect 會在威脅危害環境之前偵測並消除它們，努力讓資料復原不需要進行。這會透過我們增強的多層網路資安功能實現，我們將在本白皮書中深入探究這點。

面對新興威脅

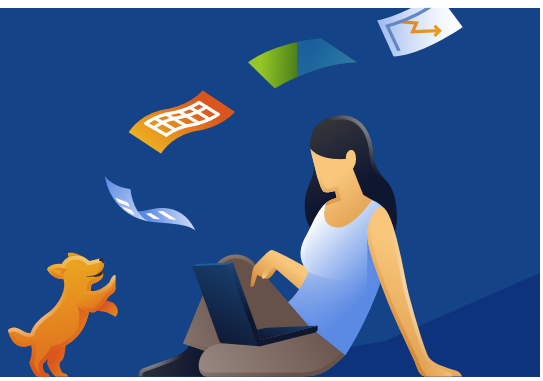
目前，適當的網路資安解決方案需要多層次威脅防護。這一點可透過一套智慧整合的技術解決，當中的每項技術都會在特定的威脅防護階段各司其職。例如，如果安全性產品使用特徵碼型的偵測引擎，就無法對包含零時差惡意軟體攻擊在內的新興危險威脅做出反應。

當前的網路資安或防惡意軟體解決方案都能提供紮實的即時防護。這包括偵測入侵並嘗試破壞端點的當前、新型或未知威脅的能力。在一個典型的端點安全性解決方案中，這個能力將包含在所謂的「存取時」或「執行時」偵測方法之中，當然這些方法會在 Acronis Cyber Protect 中實作。此外，系統管理員也可以執行隨需掃描：比方說，使用者機器上出現的新軟體可以在執行前進行掃描。若以 Acronis Cyber Protect 為例，這些即時偵測可以透過內含的多項技術達成。



我們將特別檢閱以下的偵測技術。誠摯邀請您透過討論以下主題的專用白皮書來進行瞭解：

- 弱點評估和修補程式管理
- Acronis Active Protection
- Acronis AnyData Engine
- Acronis AI 型磁碟機健全狀況分析
- 無檔案型攻擊



ACRONIS CLOUD BRAIN

佈局全球的 Acronis 資料中心的這項技術提供雲端偵測功能。端點上的 Acronis Cyber Protect 代理程式偵測到可疑情況時，會將中繼資料傳送至雲端以進一步分析和研究，包括沙箱處理和 AI 型處理等等。此外，專家也會在必要時親自分析威脅。接著 Acronis 會建立偵測記錄，供所有其他連線至 Acronis Cloud 的端點即時存取。如此就能比需要花上數小時才能發佈的代理程式特徵碼資料庫和啟發學習法規則更新搶先一步提供更完善的防護。

行為型引擎 (加上 ACRONIS ACTIVE PROTECTION)

要避開特徵碼等靜態偵測方式相當容易。網路罪犯只需打包並混淆惡意檔案，特徵碼偵測就派不上用場。這也是引入行為型引擎的原因。這類引擎通常是一套行為規則，會從已知的良好處理程序中對已知的惡意行為或異常行為做出回應。例如，嘗試惡意編輯登錄、刪除檔案、嘗試常駐於系統資料夾，或是插入其他處理程序的程式很可能就是惡意程式。

行為型引擎會偵測並停止顯示出這類行為的處理程序。Acronis 行為型引擎會分析可疑的核心層級事件以及來自 Windows 作業系統的事件。這些啟發學習法規則可輕鬆更新，並可讓 Acronis 的安全專家快速回應這些全新開發的威脅。此外，Acronis 行為型引擎也具有偵測記憶體或指令碼型攻擊等無檔案型威脅的強大功能。藉由分析記憶體中的特定處理程序行為，Acronis 也能判斷其是否為威脅。例如，如果惡意程式碼透過弱點，感染或建立惡意網站的方式，在網頁瀏覽器中執行，Acronis 行為偵測引擎便能藉由分析瀏覽器的執行緒行為來加以識別、封鎖並回報給系統管理員。

2017 年引入的 Acronis Active Protection，是透過人工智慧強化的個別行為型引擎。能偵測任何形式的威脅，並已針對 Acronis Cyber Protect 進行完整內部開發的全新一般用途 Acronis 行為型引擎密切合作，共同抵禦威脅入侵。若要檢閱 Acronis Active Protection 中所有實作的創新功能，如堆疊追蹤分析和偵測合法處理程序的插入行為，請詳閱本白皮書。

機器學習和人工智慧

Acronis 在 2018 年結合機器學習技術，做為 Acronis Active Protection 防勒索軟體技術的一部分。在機器學習模型和人工智慧決策的協助下，我們針對 Windows 可執行檔堆疊追蹤進行分析，並讓我們對 Acronis Active Protection 行為啟發學習法增添不少信心。

Acronis 在 2019 年於 VirusTotal 上啟用了靜態 AI 型偵測引擎。這個引擎能處理 Windows 可執行檔和動態連結程式庫 (DLL)，透過一組獨特的參數判斷處理程序是否為惡意。Acronis Cloud Brain 處理過幾千萬個檔案 (詳實記錄這類詳細資料，以做為數位憑證的目前狀態與效力)，機器學習模型會在其中針對各種惡意和無害檔案進行訓練。Acronis Cloud Brain 會持續分析檔案，其中的模型也會透過沙箱和其他安全性工具不斷進行訓練。根據遭遇過的各類狀況和惡意行為的模式，我們使用一套經過監督的訓練方法和包含各種決策樹的梯度提升技術。

Acronis 引擎會不斷最佳化這個模型，並可以從雲端的每個端點上輕鬆更新。因此，只有相關參數會加入訓練之中，協助取得最佳可行的結果。如果在偵測後還是無法判斷處理程序的行為，其他的模型會自動接手進行分析，我們會在之後檢閱這些結果，並視情況調整偵測模型。對於主要的惡意軟體及系列，我們有個別對應的模型，可以取得最佳的偵測結果。

好的機器學習模型不需要大量的資料，相關且優質的資料才是必要的。這也就是訓練模型以掌握常見威脅功能與特徵為何扮演著重要角色的原因。例如，勒索軟體的主要特徵是能對資料進行加密，並與命令和控制中心連線。

目前一堂 Acronis 靜態偵測模型的訓練課程僅費時 20 秒，而我們每天有一萬多個資料更新，可以專門用來反覆訓練模型。這意味著，我們能夠持續加強模型防禦全新和新興威脅的效率。目前 Acronis Cyber Protect 能夠對 Windows、macOS 和 Linux 作業系統進行分析。

白名單資料庫

白名單是包含無害/非惡意應用程式資訊的龐大資料庫。雲端和本機都存有這份名單，其中本機版本的回應更為迅速，對於需要封閉環境，並且只想接收資料而不想在全球網路分享資料的企業來說，更是必要的元件。政府和軍方通常會有這類需求，考量到他們處理的資料性質，這是合理的限制。

如果是雲端實作，再次強調，這是 Acronis Cloud Brain 的一部分，位於 Acronis 資料中心。更有趣的是，如果您有自訂軟體，Acronis 的網路資安防護產品也可以從備份植入白名單，這是個相當獨特又實用的功能。想像您使用的是自家開發人員所開發的應用程式。這個應用程式允許部分的系統存取，所以公司中只有少數人員可以使用。傳統的白名單系統遭遇到這類應用程式，會以旗標標出，並標示為可疑。清理該檔案的唯一方式就是下載並分析檔案，但這方式不見得永遠可行。在此同時，您的系統管理員還得應付誤判以及時間的浪費和生產力的下降。

現在想像您使用這個應用程式在網路中註冊新機器。我們會為您執行完整的備份 (如果您有 Acronis Cyber Protect)，並使用不同的防惡意軟體引擎進行掃描。當 Acronis Cyber Protect 發現備份中的新應用程式不在目前的白名單時，就會立刻進行分析，並在必要時進行沙箱處理，且花 24 小時或更久的時間 (視 Acronis 工程師設定的組態而定) 加以清除。之後，您註冊的新機器上的白名單就會在遭遇此應用程式時正確回應。

這個方式會將誤判情況降到最低，並讓 Acronis 的專家建立更精確、更強化的啟發學習法偵測規則，藉以提升整體的偵測率和防護率。

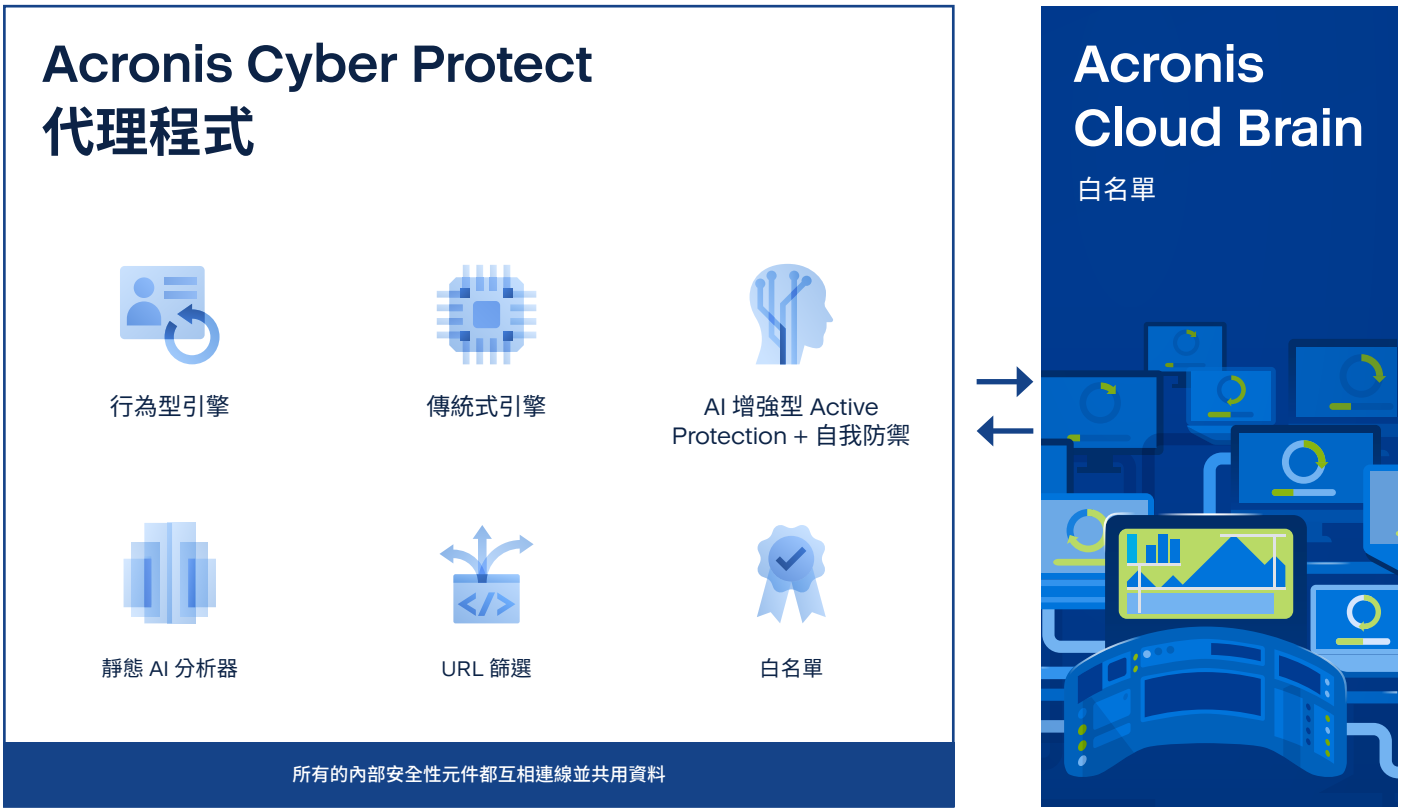
URL 篩選

篩選和辨識網路釣魚意圖和惡意 URL 的能力也是任何現代安全解決方案不可或缺的一部分。由於當前大部分的威脅都來自網際網路，適當控制對已知不安全的特定網站的網際網路存取權是相當重要的。此外，合法的網站也可能遭到入侵，在修復完成之前，它們也會遭到 URL 篩選或網路篩選封鎖。

一般來說，URL 篩選功能是由雲端信譽庫所提供，若為 Acronis，Acronis Cloud Brain 則會使用以下方式偵測並封鎖惡意 URL：

- **Acronis 的特徵碼**
- **Acronis AI 型偵測技術**
- **來自包含 Anti-Phishing Working Group 等業界合作夥伴的情報**

為避免網際網路連線中斷而保留惡意與網路釣魚 URL 的本機偵測規則是很明智的，我們的網路資安防護解決方案都包含這項功能。Acronis URL 篩選可透過由分析連結與網頁結構 (標頭、內容等) 所建置的機器學習模式加以強化。

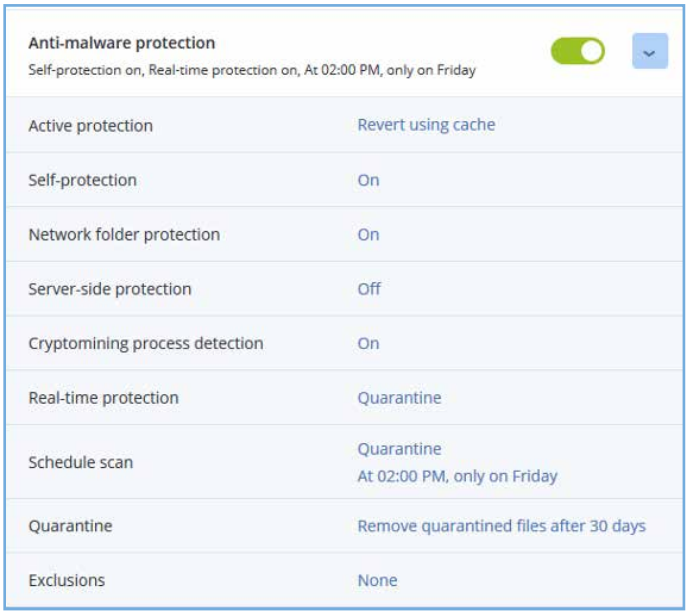


針對已知威脅的傳統式特徵碼型防惡意軟體引擎

重點鎖定在攔截零時差威脅的主動技術固然重要，但把特徵碼型引擎當成安全解決方案的一部分也有其必要性，原因就在其迅速的回應速度。它會將位元組序列與端點代理程式上的本機資料庫進行比對，這個處理程序會比其他向雲端提出要求的偵測技術快上許多。特徵碼型的偵測也會進一步防護所有會造成問題的已知威脅。大部分的雲端、行為型和 AI 產生的偵測方式最終也會走向特徵碼，以加快偵測處理程序的速度。

然後，各個特徵碼型引擎的效率可能會有所差異。想像您手邊的記錄很多都已過時、錯誤或損毀。這可能會導致掃描引擎的效能下降。當企業對威脅一無所知，僅建立了部分的特徵碼，導致引擎只能識別有限範圍，您也可以想像會發生什麼情況。Acronis Cyber Protection 產品授權市場上其中一個最出色的引擎，以確保取得最佳的效能和涵蓋範圍。

此外，了解防惡意軟體記錄在這些引擎的更新方式也很重要。Acronis 採用了有效的分散式點對點型更新，如此就不會因為仰賴單一伺服器 (來源) 將更新發佈至網路中的數百台機器而導致堵塞。有了 P2P 更新，只要有一台機器取得新的資料庫，另一台也會隨之取得，無須等候更新伺服器。



完整 Microsoft Windows 相容性

身為 Microsoft Virus Initiative，Acronis 為 Windows 提供備受好評且獲得認證的防惡意軟體解決方案，其強大的功能足以取代 Windows Defender。Acronis 遵循所有 Microsoft 的建議，並針對其產品建立了一套完整的 ELAM 相容驅動程式。開機初期啟動的防惡意軟體 (ELAM) 是一項 Windows 8 (與更高版本) 的安全技術，可以評估非 Microsoft Windows 開機時間裝置/應用程式驅動程式是否帶有惡意程式碼。這是第一個以 Windows 作業模式啟動的系統核心驅動程式，領先所有第三方軟體或驅動程式。在 Acronis Cyber Protect 中，Windows 資訊安全中心整合由「受保護的程序輕型」(PPL 是一項 ELAM 型的技術，能確保作業系統只會載入受信任的服務和處理程序) 提供完整的保護。Acronis Cyber Protect 也與 PPL 一同防護主要的防惡意軟體服務。這讓 Acronis 軟體達到最高等級的自我防護，涵蓋了不在其他解決方案範圍的核心防惡意軟體模組。

在 Acronis Cyber Protect 管理主控台中，系統管理員可以：

- **在多部電腦上強制套用設定**
- **確認所有機器上的防惡意軟體資料庫均為最新**
- **查看所有 Windows Defender 偵測事件**

確認網路資安防護是否正常運作

很多資安公司都聲稱其產品能夠保護您的資料和環境，實際上並非所有公司都能勝任這項工作。我們建議您在挑選網路資安解決方案時，要先從設定優先順序做起。每家企業的最終目標就是要獲利。任何形式的業務中斷或有損信譽的情事都會造成大量的財物損失。

既然沒有任何解決方案能夠保證 100% 的安全性，您會需要挑選一個能在事件發生後能快速恢復運作的解決方案。多層次網路資安解決方案應該能偵測到最多的威脅，並提供評估其偵測能力的機會。查看 AV-Test 或 AV-Comparatives 等企業提供的各種獨立測試便能進行評估。

如果可行，建議您針對偵測能力加以測試。如果遺漏了威脅，您應該確認多快可以復原遭刪除或損毀的檔案，或多快可以讓使用者的機器能再度恢復運作。這是因為與惡意資料外洩事件相關的成本終究會比因惡意軟體本身造成的當下損失高上許多。

掃描備份中有無惡意軟體

防惡意軟體掃描通常會在端點或伺服器上執行。然而，如果這些機器已經完整備份 （已製作磁碟映像），則掃描儲存於集中式位置的完整磁碟映像也說得過去。這個做法可以降低端點或伺服器的負載。我們也有好方法可以檢查不是經常出現在企業網路內部部署上的筆記型電腦或其他機器。

Acronis 能夠掃描位於集中式位置 (不論是在雲端還是地端部署) 的備份檔案。但 Acronis 能做的不只是掃描這些完整映像，還能檢查每個新切片中是否有惡意軟體。相關做法，請參閱本白皮書。