

Acronis Cyber Security with web console Standard

資安防毒勒索軟體防護標準版

將資料防護和下一代 AI 型反惡意軟體、防毒軟體和設備防護管理集結在一個解決方案中。整合與自動化功能在減少複雜性的同時還提高生產力並減少運營成本，為服務供應商提供了無與倫比的舒適性。



已透過基本網路防護免費增強

採用 AI 技術的先進行為偵測引擎可防止客戶的工作負載遭受惡意軟體、勒索軟體和零時差攻擊所侵擾。

使用下一代網路防護來保護所有客戶工作負載的安全

藉由涵蓋客戶 100% 工作負載的整合式網路防護，將客戶面臨的安全風險降至最低，並率先享有當前安全防護廠商未提供的獨特功能。迎接 2021 年網路威脅的挑戰，大幅減少安全事件和漏洞。運用獨立測試領域領先的解決方案 (VB100、AV Test、AV-Comparatives、ICSA 實驗室)。

弱點評估

識別並彌補客戶系統中的安全漏洞。您可以掃描客戶電腦的弱點，確保所有應用程式和作業系統均處於最新狀態，不讓網路罪犯有機可乘。

保護遠端工作的員工

借助多項保護功能，最大限度降低遠端工作者面臨的日益增多的網路攻擊的風險，這些功能包括針對關鍵任務遠距離工作應用程式 (Zoom、Webex、MS Teams、Slack、Skype、TeamViewer) 的優先修補和保護、遠端裝置抹除和安全的桌面遠端連線。

裝置與連接埠控制

對使用者存取本機連接的裝置與連接埠以及相關的資料作業進行精細、內容感知的控制 (即使是虛擬的工作階段也如此)，以此強化資料安全性並預防經由本機通路出現敏感資訊洩漏情況。

剪貼簿控制

控制應用程式與文件之間的資料傳輸，及早預防資料洩漏。允許或封鎖使用者對於複製到剪貼簿的不同資料類型的物件的存取，即使是對虛擬工作階段中的重新導向的 BYOD 裝置也如此。

裝置控制：支援加密卸除式媒體與螢幕截圖擷取存取

透過加密卸除式媒體與螢幕截圖擷取控制功能，消除資料外洩的風險。如此一來，使用者即可在卸除式裝置落入惡意人士手裡時，確保組織的機密資料不會外洩，同時也能防止有人將螢幕截圖複製到剪貼簿。確保您客戶的機密資料安全無虞。

報告排程

將採用所需格式與語言的排程報告傳送給列出的收件者，以此功能來提升資訊安全的可見性並簡化 IT 安全性稽核。

集中式防護計畫和群組管理

利用分組管理多項工作負載和集中式防護計畫，讓管理工作變得輕鬆。其中包含的所有安全性組態可以套用至客戶組織中的多個端點。

預先定義的防護計畫

從三個預先設定的防護計畫中選擇一個，就能快速且輕鬆地保護客戶的遠端和辦公室員工。這些選項能為您節省時間，同時確保您客戶的工作負載與環境受到妥善保護。

遠端桌面協助

藉由內建的遠端桌面功能，讓使用者能安全地異地存取機器，從而方便遠端辦公或者向客戶提供技術協助。

硬體庫存收集

借助最新的硬體庫存，節省時間和精力。透過自動掃描與隨需掃描，探索所有硬體資產。建立硬體庫存報告、瀏覽並篩選依多項條件劃分的記錄，並在機器或租用戶移除後自動將其刪除。

不可變儲存

設定應保留刪除資料的天數，透過管理主控台輕鬆復原刪除的備份，防範意外或惡意刪除客戶備份，並加強遵循法規。

鑑定備份

遵守法規要求及實施內部調查這個流程可能所費不貲。有了 Acronis Cyber Protect Cloud 的鑑定模式，您可從磁碟層級備份中收集數位證據 (例如記憶體傾印和處理程序資訊) 以簡化任何未來的分析過程。

防止入侵

使用專注於弱點攻擊的行為型偵測啟發學習法來預防包括零時差攻擊和無檔案型攻擊在內的進階攻擊技術。Acronis 的防止入侵技術專門偵測利用軟體弱點的惡意軟體。

增強的簽名型偵測

使用增強的惡意軟體簽章資料庫來提高偵測率和速度，確保在數秒內無縫偵測所有已知威脅，同時將代理程式對於效能的影響降至最低。

增強型 URL 篩選功能

防範惡意網站攻擊，協助客戶滿足法規要求及提高生產力。藉由 Acronis URL 篩選功能，您可以利用 HTTP/HTTPS 攔截器控制網站存取、管理 URL 例外並執行承載分析。

安全復原

藉由 Acronis 的特有安全復原技術，防止發生反覆危險感染。在復原過程中，整合式解決方案會掃描備份有無惡意軟體，安裝最新的安全性修補程式，並更新其防毒資料庫。

遠端裝置抹除

從遠端清除遭入侵或遺失的 Windows 裝置，防止業務關鍵資料落入不肖人士手中。您可以保護資料不被心懷不滿的員工刪除，也可避免有心人士從遺失或遭竊的裝置存取資料。

全域和本機允許清單

透過更積極的行為啟發學習法，達到零誤判水準。您可以建立客戶最常用應用程式 (包括自訂應用程式) 的自動允許清單，節省時間並避免耗盡資源的誤判。還支援手動設定允許清單。

Acronis Cyber Security with web console Enterprise

資安防毒勒索軟體防護 企業版

憑藉防故障修補技術、磁碟機健全狀態監控、軟體庫存收集和無縫報告排程，利用修補程式管理更好地控制 IT 資產和安全性。

修補程式管理

軟體修補程式是保護企業環境不可或缺的環節，同時也能在已知弱點演變成棘手問題之前先行修正。我們的修補程式管理 Microsoft 和 Windows 上的第三方軟體，因此您可以輕鬆地排定修補時間或手動部署修補程式，保護客戶安全。

磁碟機健全狀態監控

預防意外遺失資料，以及藉由監控磁碟機的健康狀況，主動改善正常運作時間。使用機器學習技術，Acronis Cyber Protect Cloud 可以預測磁碟問題並提醒您採取必要的預防措施來保護客戶的資料。

軟體庫存收集

獲取深入的軟體庫存能見度並節省時間。自動掃描或隨需掃描客戶機器，探索所有已安裝的軟體。瀏覽並篩選依多項條件劃分的軟體、產生報告，或者在機器被移除後刪除記錄。

網路指令碼

自動處理諸如佈建與維護等日常工作，並以事半功倍的效果管理更多工作負載。利用您可以輕鬆自訂、測試、執行與排程的立即可用且經過 Acronis 驗證的指令碼，簡化作業。

防故障修補

有問題的系統修補程式會導致系統不安全。在實作最新版本的修補程式前，已自動建立映像備份。一旦發生問題，您可以輕易地還原及復原回工作狀態。

合作夥伴級別的指令碼管理

透過集中管理指令碼並跨所有終端用戶端、專屬終端用戶端、個別工作負載以及靜態或動態工作負載群組執行這些指令碼，簡化作業。



支援平台：Workstation / Server / VM



Acronis

OFFICIAL CYBER PROTECTION PARTNER

Acronis 台灣總代理

北祥資訊股份有限公司

台北市內湖區文湖街 20 號 2 樓



pdcmarketing@pershingdata.com.tw



www.pershingdata.com.tw