

Advanced Security

探索可抵禦現今網路威脅的全方位防禦機制

以更少的資源，為用戶抵禦更多的資安威脅。Advanced Security 附加元件延伸 Acronis Cyber Protect 的端點防護功能，讓您透過增強的反惡意軟體防護和修復服務減少對客戶造成的風險。進階整合與自動化簡化了部署、設定和管理工作。

讓 Advance Security 增強您的資訊安全服務



進階端點防護

已透過攻擊預防增強的 Acronis Active Protection、URL 篩選、已備份資料的反惡意軟體偵測，以及提高的偵測率以便更快地揪出更多威脅。

安全性自動化

智慧簡單的防護政策管理、自動允許清單、自訂應用程式、自動惡意軟體掃描和 AV 定義更新，作為復原流程一部分以更輕鬆地提供服務。

高效鑑定

收集數位證據並將其儲存在一個安全的集中式存放庫，以進行全面的事後調查和正確的修復，同時壓低成本。

快速輕鬆地進階您的安全服務	提高效率，減少人力投入	實現更高效、更快速、成本更低的回復
- 提高防護能力—使用與數據保護和安全集成管理的全堆疊反惡意軟體，降低用戶風險 - 覆蓋更多攻擊向量—阻止基於Web的攻擊和漏洞 - 提高檢測率和速度 - 防止威脅再次發生	- 管理單一的整合解決方案—減少提供服務所需的資源 - 通過解決方案整合降低成本 - 通過安全自動化改善反應時間 - 減少用戶端點上的負載—掃描Acronis雲中的惡意軟體 - 減少誤判	- 確保通過法規見解對違規行為進行充分調整，降低補救成本並簡化流程—通過收集的數位鑑識簡化安全調查 - 將威脅復發的風險降至最低 - 安心還原過程 - 將數位證據存儲在安全的中央存儲庫中

以採用 AI 技術的下一代備份防護為基礎打造

單一視窗管理防護解決方案 Acronis Cyber Protect 將用戶的風險降至最低。該解決方案兼備同類型最佳的備份和復原、端點防護管理和資訊安全防護，並整合可抵禦勒索軟體和零時差攻擊的反惡意軟體技術，能與客戶目前的防毒軟體相輔相成。透過 Advanced Security 的完整堆疊反惡意軟體強化用戶的防護措施，以我們經過實證的整合式網路防護取代其防毒軟體。

Acronis Cyber Protection :	Advance Security Add-on :
Acronis Active Protection：新一代的行為式技術，旨在主動阻止網路威脅，重點關注勒索軟體和零時差攻擊	進階端點防護增強您的安全性服務，整合了資料防護的完整端點安全防護，取代非整合式防毒工具及備份，讓您在更少的管理負擔之下提供更多資料安全防護。
- 主動防護：下一代基於行為的技術旨在主動阻止網路威脅，重點是勒索軟體和零時差攻擊 - 弱點評估 - 透過裝置控制進行資料遺失防護 (DLP) - 備份和復原 - 在勒索軟體攻擊後自動復原資料 - 採用 #CyberFit Score 進行安全漏洞識別	- 完整堆疊的反惡意軟體防護：採用多個防禦層的即時防護，涵蓋多個攻擊媒介 - URL 篩選：封鎖惡意 URL、Web 型攻擊和 COVID-19 詐騙 - 防止入侵：基於行為的偵測啟發學習法可預防未知弱點的入侵，包括記憶體入侵和插入 - 對 Acronis 雲中的數據進行反惡意軟體掃描：卸載用戶端點，實現更積極的掃描並確保無惡意軟體備份 - 對 Acronis Cloud 中的資料進行反惡意軟體掃描：卸載用戶端點以啟用更積極的掃描，從而確保無惡意軟體的備份 - 備份中的鑑定資料：收集數位證據以加快修復速度並降低其成本 - CIOC 威脅動態：更快速地回應新出現的威脅並獲取修復建議 - 遠端裝置擦除：防止數據洩漏通過丟失的設備 - 惡意軟體再次感染防護：在復原期間掃描惡意軟體並更新 AV 定義，預防威脅再次發生 - 自動設定允許清單：減少誤判並實現更積極的掃描

提供久經考驗、屢獲殊榮的端點保護



獨立測試的領導者

Acronis Cyber Protect Add-on License

Advanced Security 附加元件延伸 Acronis Cyber Protect 的端點防護功能，憑藉改進的偵測率和速度、智慧防護計畫、對於備份與復原的其他防護以及鑑定功能，新一代的網路防護技術可應對更廣泛的威脅。

立即嘗試