

# Acronis SP Protection

(需成為授權夥伴)

## 服務供應商是主要的網路攻擊目標

對於鎖定目標來存取客戶的端點和寶貴資料的網路攻擊而言，MSP 是這些網路攻擊的一大目標。服務供應商仰賴的平台越來越常淪為供應鏈攻擊入侵的目標，例如 [SolarWinds](#)、[ConnectWise](#) 和 [Kaseya](#) 缺口。

Acronis 全心投入服務供應商合作夥伴的支援，不僅提升了實務做法，也把企業的網路攻擊與停機時間風險降到最低。Acronis 提供合作夥伴免費的 SP Protect 計畫，其中包括能協助自行防護的 Acronis Cyber Protect Cloud NFR 授權、我們以安全性為主軸的開發實務做法，以及網路資安訓練模組，藉以提升服務技術人員的效率。Acronis 能協助您更妥善地做好防範，以抵禦威脅和供應鏈攻擊的入侵。



## 有 81% 的 SP

擔心他們組織的網路資安缺口可能會導致客戶的 IT 系統遭到入侵\*

## 管理網路風險所需的全套工具 - 免費

軟體： 強化您自身資產的安全性狀態	訓練： 提升您團隊的網路資安專業知識	方法： 選擇經證實且以安全性為主軸的合作夥伴
<ul style="list-style-type: none"> <li>使用 Acronis Cyber Protect Cloud NFR 計畫<b>保護您的企業</b>，無需負擔額外成本</li> <li>在現代威脅危害您的企業或橫向攻擊客戶前，<b>自動做好防護措施</b></li> <li><b>降低資料外洩風險並對</b>漫布在基礎架構中的<b>漏洞加以解決</b></li> <li><b>進行安全性調查與稽核</b></li> </ul>	<ul style="list-style-type: none"> <li>充分利用 Acronis #CyberFit 學苑提供的<b>安全意識與網路防護訓練模組</b>，培養強調<b>安全第一思維的文化</b></li> <li>提供內容專為 SP 量身打造的<b>優質服務</b></li> <li>提升專業知識，輕鬆完成網路資安服務的<b>銷售工作</b></li> </ul>	<ul style="list-style-type: none"> <li>確保您提供的服務能獲得保護，免受入侵，<b>以避免攻擊經由您滲透到客戶的防禦系統</b></li> <li>確保在任何時刻只有您才能存取您自己和客戶的資料</li> <li>選擇經過證實且能提供以<b>安全性為主軸方法</b>的 MSP 合作夥伴</li> </ul>

## 客戶不是唯一處於風險之中的人 - 保護您自己的端點不會遭受他人失誤的攻擊

透過我們的 [NFR 計畫](#)，免費利用 Acronis Cyber Protect Cloud 以保護您的基礎架構。我們的多合一網路防護可讓您的企業更靈活面對現代網路威脅，同時減少缺口和技術問題造成的影響。

\*資料來源“MSPs Speak: Cybersecurity and the Future Role of MSPs”  
(MSP 主講：網路資安和 MSP 的未來角色)，2021 年，Acronis 與 Vanson Bourne。

抵禦現代威脅	範圍有限的受攻擊面	降低資料外洩和停機風險
使用下一代的防惡意軟體、URL 篩選和電子郵件安全性，以防範包含零時差攻擊在內的現代惡意軟體和勒索軟體。使用內建的防護功能降低供應鏈風險。	使用多達 270 個應用程式的自動化修補程式管理，以識別並解決漫布在組織中尚未解決的安全漏洞。	透過下列方式，降低安全事件與技術問題對您企業的影響，以減輕財務及商譽的損害： <ul style="list-style-type: none"> <li>同業最佳的備份與災難復原</li> <li>自動勒索軟體回復</li> <li>HDD 健康狀態監控</li> <li>防故障修補</li> </ul>

開始著手保護您的服務

[提出申請](#)


## 提供您的客戶更完整豐富的網路資安專業知識

高效防護如今的威脅需要的不僅是技術，還需要豐富的人力專業經驗。為了讓合作夥伴能提供更卓越的服務，Acronis #CyberFit 學苑持續更新以 SP 為主的安全訓練模組，重點鎖定網路資安防護、威脅態勢、合規性以及必要的網路資安實務做法，其中包括：

- 惡意軟體和防範攻擊並從缺口復原的方式
- 行動安全性
- 多重要素驗證 (MFA)
- 密碼安全性
- 隱私權和個人識別資訊 (PII)
- 雲端安全性
- 實體安全性
- 遠端監控與管理 (RMM)
- 資料外洩防護 (DLP)
- 無線安全性
- 權限提升
- 網路釣魚
- 分散式阻絕服務 (DDoS) 攻擊
- 社交工程
- 以及更多...

開始著手進行您的教育訓練

[開始訓練](#)


## Acronis 對合作夥伴採用安全性為主軸的方法



Acronis 的產品在各個階段皆確保所有資料的端對端加密，所以只有您才能存取。我們採用透明、以安全性為主軸的開發做法並確保工程師接受定期安全訓練，以此保護客戶資料不受現代威脅的侵害。Acronis 借助獨立的測試實驗室 (例如 VB100、SE Labs、AV Test 和 AV Comparatives) 來測試其代理程式。自從 2018 以來，我們在 HackerOne 上執行了一個漏洞回報獎勵計畫來確保我們的產品採用最高等級的安全性。

- 針對客戶資料實行 AES-256 加密
- 以安全性為主軸的開發
- 獨立評估技術
- 漏洞回報獎勵計畫