

Acronis Security Services 適用於服務供應商

抵禦現代網路威脅

資料供現代的組織達成目標，進而成為世界上最珍貴的資源。這便是網路犯罪分子鎖定以資料為目標、攻擊的頻率不斷攀升且手法更趨複雜的原因。

遺憾的是，技術已不足以保護客戶免受資料外洩之災：

- 防毒軟體會漏阻 57% 的攻擊 (*Ponemon Institute*)
- 依據高層主管們的說法，有 47% 的漏洞是因人為錯誤而起 (*Shred-it*)
- 74% 的公司尚未準備好應對網路攻擊 (*Hiscox*)

採行包含技術、人員和程序的整體性安全策略已臨當務之急。為了保護資料與端點不受現代網路的威脅，組織不僅需要使用中 (active) 安全技術，也同時需要主動式 (proactive) 和回應式防護方案。

服務供應商面臨的挑戰

更全面的安全策略需求，為服務供應商帶來前所未有的挑戰：

- **提供完整的安全性：**SMB 現在期望每個 MSP 都能提供減輕風險與網路資安服務 (*MSSP 警示*)
- **IT 人員配置：**網路資安人才短缺已逾 4 百萬人 (*ISC*)
- **可擴縮性的成本：**72% 全球性公司的 IT 成本皆在疫情期間增長 (*Acronis*)
- **複雜性：**平均而言，中型 MSP 需與 7 個或更多供應商經營關係，而大型 MSP 則經營 10 個或更多供應商。 (*Auvik*)
- **法規遵循：**54% 的 SMB 表示，「需要遵循法規、法律和其他授權」是考量 IT 投資決策的一個關鍵 (*Gartner*)

優點

安全評估

- 提升客戶的安全狀態
- 將修復成本降至最低
- 符合法規要求
- 維持網路資安策略暨藍圖與業務目標一致
- 制定明確的 IT 投資決策
- 藉由修復計劃降低風險

安全意識

- 提升員工應對網路攻擊的準備程度
- 將人為錯誤減至最少
- 確保員工遵循法規與既定程序
- 減少請求安全相關支援的數量

事件回應

- 確保業務持續性
- 對未填補的安全漏洞限縮損害程度
- 減輕網路攻擊造成的財務與信譽風險
- 將系統停機時間縮到最短

ACRONIS SECURITY SERVICES

多年來，Acronis 始終提供業界領先的網路資安防護技術。隨著 Acronis Security Services 的推出，服務提供商進而可透過一套佈建的服務，提供更全面的網路資安策略。

ACRONIS SECURITY ASSESSMENT SERVICE

「95% 的資料外洩是可以防止的」(OTA)

確保客戶與時俱進，同步遵循不斷推陳出新的法規要求，備戰持續攀升的數位威脅。審視客戶的安全計劃、IT 基礎架構以及預防和偵測控制措施，以利識別安全漏洞與弱點。依循 Acronis 網路資安專家的建議，剷除威脅客戶資料的所有攻擊媒介。

評估服務包含以下內容：

- 風險評估
- 社交工程
- 弱點掃描
- 修復計畫
- 滲透測試

ACRONIS SECURITY AWARENESS TRAINING

「66% 的組織表示，安全意識培訓協助他們減少了成功攻擊的次數」(CSO)

安全意識培訓由頂尖的網路資安專家依您的客戶業務需求量身打造並授課，協助客戶端員工準備情況最佳化、有效減輕各種威脅 (包括社交工程入侵)，同時減少必須先「詳閱本書」而導致的所有延遲。

培訓包含以下內容：

- 依一般員工、IT 人員和高層管理團隊各種角色進行培訓
- 合規性與認證培訓
- 多重授課選項：線上模組或實體課程

ACRONIS INCIDENT RESPONSE SERVICES

「訂定有效的事件回應計劃，資料外洩的平均總成本可減少 123 萬美元」(Ponemon Institute)

協助您的客戶整裝備戰，並對安全事件提供即時回應。對客戶環境與漏洞的肇因進行全面、整體的評估，提供客戶深入的分析。提供詳細的修復計劃，確保採取適當的行動進行復原。

服務包含以下內容：

- 受損資產識別
- 鑑定
- 威脅隔離
- 修復報告

成為客戶的安全單一窗口

「如果 MSP 能提供適切的網路資安解決方案，93% 的 SMB 即使沒有更換 MSP 的計劃，也會考慮改與新的 MSP 合作。」(Cotinum)

Acronis Security Services 以一組預先套裝服務內容的型式提供，目的在於協助我們的合作夥伴打造策略更為全面的網路資安防護服務。

- **提高獲利：**將您的安全服務組合提升為 MSSP 等級，藉以吸引新客戶。對現有客戶追加銷售，同時提高每使用者平均收入 (ARPU)。
- **減少客戶流失：**透過強化現有客戶的安全狀態以及將客戶的資安風險降至最低，維持客戶的滿意度。
- **將成本降至最低：**佈建一組預先套裝的服務內容，服務提供商不僅投入度可減至最少，也不需要額外的 IT 人員或資金支出。
- **降低複雜度：**減少因依賴多家供應商而產生的風險、管理需求與帳務煩惱。
- **更卓越的定位：**展現淵博的安全專業知識，並透過應用面更廣泛的安全產品內容，將客戶潛在的信譽毀損與法律興訟減至最少。

