Acronis

白皮書

# 服務供應商 (MSP) 如何將勒索軟體威脅轉化為收益

如何藉由網路防護服務來推動業務

據 Juniper Research 報告顯示，網路犯罪行業迅速發展，每年給企業造成的損失估計為 3 萬億美元，到 2024 年會增長到 5 億美元。[1] 網路攻擊是代價慘重的行業災難，會導致損失利潤的停機、收入損失、品牌受損、股價損害及監督機構罰款。

Acronis 網路整備性報告調查了全球範圍內的 3,400 位 IT 管理員和遠端工作者，以評估他們在 COVID-19 疫情前後的網路整備性情況，發現全球 31% 的公司每天至少遭受一次攻擊，所有受訪者中有 50% 的人報告其過去三個月內至少每週遇到一次網路攻擊。[2] 與此同時，許多研究人員的結論是停機成本可能從每小時 10,000 美元[3] 到每小時 260,000 美元不等[4]。

在眾多惡意軟體類型中，勒索軟體是目前最為普遍的網路威脅，從 2019 年第三季度到 2020 年第三季度，攻擊增長了 139%[5]。在此期間，所有產業皆受到勒索軟體影響。例如，在 2020 年第三季度，針對教育部門的成功勒索軟體攻擊增加了 388%[6]。

企業和 IT 領導者擔心下一次攻擊可能會毀掉他們的公司以及其職業生涯。

勒索軟體會有效危害其目標 (通常只是讓一位不設防的員工點擊網路釣魚電子郵件)，並導致系統突然關閉，眾目睽睽且造成嚴重干擾。同時，加密貨幣支付也妨礙了執法行動。與違反防禦措施以竊取和轉售機密資料相比，這是一種更為簡單、更有利可圖的犯罪。

## 勒索軟體：威脅和機遇並存

作為服務供應商 (MSP)，您應意識到這股特殊的網路犯罪浪潮既是威脅，也是機遇。

部分威脅源自於這樣一個事實，即在複雜的供應鏈攻擊中利用技術廠商和服務供應商來聯絡商業客戶和政府機關：最惡名昭彰的是 2020 年 12 月發現的 SolarWinds 違規事件[7]。透過闖入軟體公司並在常用的應用程式中內嵌惡意軟體，網路罪犯現在可以危害使用這些工具的服務供應商，以此進一步危害這些供應商負責管理其 IT 基礎架構的客戶[8]。

但成為勒索軟體攻擊目標只是威脅是一部分：無法阻止勒索軟體對客戶的攻擊有損 MSP 的競爭力和成長能力。對於 MSP 來說，這一挑戰日益複雜。統計資料顯示：

71%

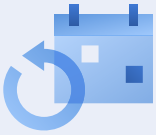
的勒索軟體攻擊目標為**中小型企業 (SMB)**[8]

3,5

的 MSP 去年**不得不應對**針對其 SMB 客戶的勒索軟體攻擊[9]

24%

的 SMB 在遭受網路攻擊後**已更換了** MSP[10]



52%

的 SMB 表示他們缺乏正確處理安全問題所需的內部技能[11]

**只有** 31%

的 MSP 對保護其客戶抵禦未來勒索軟體攻擊的能力**非常有信心**[12]

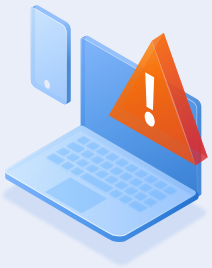
74%

使用 MSP 的 SMB 表示，如果遭受網路攻擊，他們會對其供應商**採取法律行動**[13]

每個商業挑戰都會帶來機遇。您必須保護自己免受勒索軟體攻擊，同時確保它們不會傳播。此外，透過提供可抵禦勒索軟體和其他資料遺失威脅的網路防護服務，您還有機會為客戶打造高利潤和差異化的新產品服務。考慮事項：

## 2021 年 IT 預算增長的主要驅動因素 [14]

**1.** 需要升級過時的 IT 基礎架構



**2.** IT 專案的優先順序增加


**3.** 安全性考量增加

**89%**

的 SMB **會考慮僱用新的 MSP** (若其能提供適合的網路安全解決方案)[15]

**25%**

為了從新供應商處獲得「適合的網路安全解決方案」，已經使用 MSP 的企業**願意為此支付**的年度成本有所增加[16]

**89%**

的 SMB 未使用 MSP，如果能夠 MSP 能夠提供「適合的網路安全解決方案」，他們**會考慮啟用僱用一個**[17]

因此，您可以向 SMB 客戶展示的價值主張簡單且令人注目：「讓我們把勒索軟體和其他惡意軟體攻擊帶來的威脅從您的擔憂清單中移去。我們還將保護您防範大量其他可能的資料遺失。」

挑戰在於使這項產品服務富有吸引力且可獲利，也就是說：簡單、可管理、高利潤，並且與您的現有基礎架構相容。

## MSP 對抗勒索軟體的三種常見方式及其隱患

可用於協助 MSP 應對此機遇的解決方案通常分為三類：備份、含有限勒索軟體防禦的備份，以及與第三方端點防惡意軟體相結合的備份。每種都有其局限性：

**1. 備份**本身的運作方式是將受損系統還原為攻擊之前的某個時間點。但僅依賴於備份具有幾個弱點。從備份 (尤其從諸如磁帶或雲端的較慢媒體) 還原數十個或數百個系統可能會非常耗時、中斷業務，代價極其昂貴。[18] 此外，復原點可能非常舊，以致於在備份和攻擊之間建立的大量寶貴資料可能會遺失。

**2. 含有限勒索軟體防禦的備份**可以對抗某些攻擊，從而減少單獨依賴備份進行復原的需求。但攻擊偵測通常依賴於粗劣的統計量值，將檔案變更率與基準閾值相比較。檔案變更率突然增加表示可能發生攻擊。可惜的是這種方法是反應性的，容易出現偵測失敗和誤判，每種情況都要承擔巨大成本。與單獨使用備份一樣，如果攻擊設法找到備份並進行破壞 (許多勒索軟體變體的一種功能)，從而完全阻撓復原，則這種解決方案便無濟於事。

**3. 與第三方端點防惡意軟體相結合的備份**旨在針對勒索軟體使用更為精密的端點防禦。但是，這兩種元件與及代理程式之間缺少整合，屢屢導致系統效能問題、可能中斷備份的處理序衝突，以及 MSP 的部署和管理難題。

## 適用於 MSP 的較進階且高效的選擇

第四個選項為 MSP 提供了更為簡單、有效且高效的選擇：採用 Acronis Active Protection 技術的 Acronis Cyber Protect Cloud。這種解決方案已經有 10,000 多位 MSP 在使用，所提供的網路防護服務將備份即服務與整合式 AI 增強型網路安全功能 (包括防毒、防惡意軟體及防挖礦劫持) 及自動化修復功能相結合：

- Acronis Active Protection 使用人工智慧 (AI) 和機器學習 (ML) 來偵測和解除網路攻擊。Acronis Cloud AI 基礎架構中進階行為偵測引擎的持續訓練產生了業界最低的惡意軟體偵測誤判率，包括零時差 (即先前未知的) 攻擊。
- 整合式自我防禦機制可預防勒索軟體攻擊危害 Acronis 備份程序、代理程式及封存。
- 自動化修復會使用本機快取立即還原在偵測到攻擊之前損壞的任何檔案，從而確保立即恢復業務運作，無需從備份進行完整復原。
- 弱點評估和自動化修補程式管理可彌補允許勒索軟體進入系統的安全漏洞，而 URL 篩選可封鎖傳播惡意軟體的網站。
- 相同的進階行為偵測引擎還可以識別並終止挖礦劫持攻擊，此類攻擊會秘密消耗系統資源違法挖掘加密貨幣，這對系統效能、電源及冷卻資源的消耗巨大。隨著加密貨幣價值的不斷飆升，這種普遍的惡意軟體威脅在 2020 年再次興起[19]。

總之，Acronis Cyber Protect Cloud 獨特的備份、網路安全和端點管理整合讓您能夠立即減少客戶遭受勒索軟體攻擊的風險。您只需安裝一個代理程式，即可提供完整的網路保護，同時避免處理序衝突及效能問題。

「Acronis 提供了出色的效能，易於使用且具有豐富的功能集。更為重要的是，它是測試中唯一一個針對勒索軟體攻擊提供專用保護的解決方案。這為 Acronis 贏得 AV-TEST 有史以來第一個獲認可的備份和資料安全性證書。」

**David Walkiewicz**
**測試研究主管，**
**av-test.org**

## 藉由 ACRONIS 提供網路防護服務

但對於服務供應商而言，不僅僅有進階勒索軟體防護功能。Acronis Cyber Protect Cloud 是 Acronis Cyber Cloud 的一部分，是專為服務供應商打造的多服務網路防護平台。它是**提供網路防護服務的瑞士軍刀，可同時提供：**

1. 一組整合式解決方案，包括**同類型最佳的備份、災難復原、網路安全 (包括防毒、防惡意軟體、防勒索軟體及防挖礦劫持)、檔案同步與共用、檔案公證、軟體定義儲存及端點管理。**
2. 一個用於統一服務佈建、帳戶管理、監控、整合和、白牌等的**平台**。

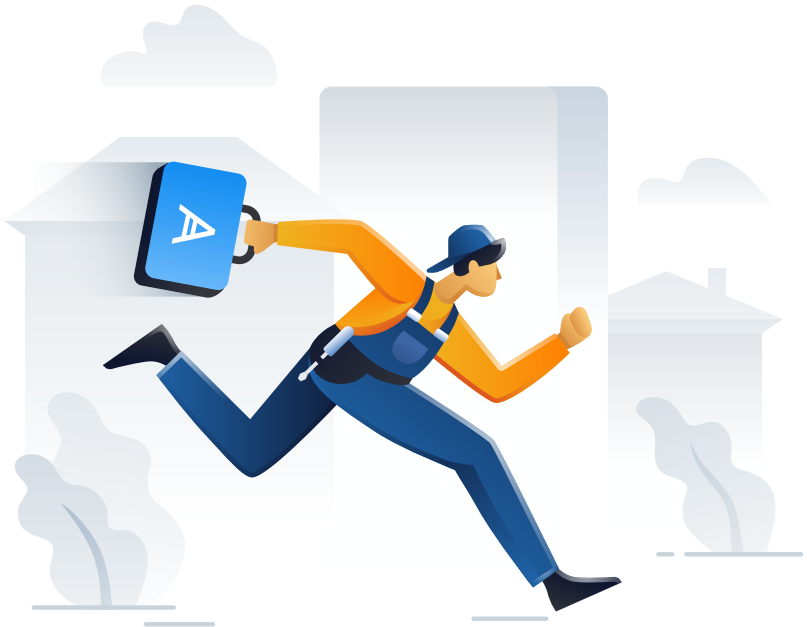
藉由 Acronis Cyber Protect Cloud，服務供應商可以提供盈利、低客戶流失率的網路防護服務，進而讓客戶在網路罪犯日益猖獗的世界中無所畏懼地開展業務。服務供應商能夠以較高效率做到這一點，從最初的系統部署到統一的服務佈建和客戶管理。Acronis Cyber Cloud 平台包含：

- 多組織用戶管理，以支援不限數量的客戶
- 多服務管理入口網站
- 白牌功能，以便於品牌推廣
- 服務使用情況配額和報告
- 與最熱門的 PSA 和 RMM 工具整合
- 透過開放式 API 自訂其他服務的整合

**瞭解 Acronis 如何讓您輕鬆、高效且安全地提供網路防護：**

請聯絡 Acronis 銷售人員，以取得調為您的使用案例的即時產品演示。 **聯絡銷售人員**

從今天開始免費試用 30 天。 **立即試用**



## 參考資料


[1] https://www.juniperresearch.com/researchstore/innovation-disruption/cybercrime-security

[2] https://www.acronis.com/en-us/resource-center/resource/532

[3] https://www.cloudradar.io/cost-of-downtime

[4] https://www.stratus.com/assets/aberdeen-maintaining-virtual-systems-uptime.pdf

[5] https://securityboulevard.com/2021/02/ransomware-trends-you-need-to-know-in-2021/

[6] https://securityboulevard.com/2020/11/successful-ransomware-attacks-on-education-sector-grew-388-in-q3-2020/

[7] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[8] https://www.acronis.com/en-us/blog/posts/defending-against-supply-chain-attacks-solarwinds-breach

[9] https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf

[10] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[11] https://www.connectwise.com/globalassets/media/assets/ebook/the-state-of-smb-cybersecurity-2020.pdf

[12] https://www.channele2e.com/influencers/msp-survey-shows-ongoing-ransomware-malware-challenges/

[13] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[14] https://swzd.com/resources/state-of-it/

[15] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[16] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[17] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[18] https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906

[19] https://www.darkreading.com/vulnerabilities---threats/cryptojacking-the-unseen-threat/a/d-id/1338903