Acronis Advanced Security + Endpoint Detection and Response (EDR)

服務供應商

簡化端點安全性

如今超過 60% 的資料外洩都涉及某種形式的駭客攻擊[1]，企業現在必須轉向進階安全性解決方案和供應商，以協助他們應對當下複雜的威脅態勢。但是，能夠應對這些威脅的大多數市場領先 EDR 解決方案會帶來：

- **高成本與複雜性，讓企業難以進入大眾市場**
- **較長的價值實現時間、較高的訓練與上線要求**
- **不完整的保護，需要額外的整合才能保證業務連續性**
- **擴展性挑戰，需要大量的安全性專業人士才能運作**

不幸的是，對於剛開始實作的服務供應商而言，執行自己的 EDR 型服務所需的技能與開支可能遙不可及。對於已經擁有安全性專業技能的供應商而言，他們可能會發現，嘗試用市場領先的解決方案來打造自己的偵測與回應服務會讓他們失去中型市場或中小型企業客戶的青睞 — 結果卻發現他們還要與其解決方案廠商的 MDR 服務競爭。

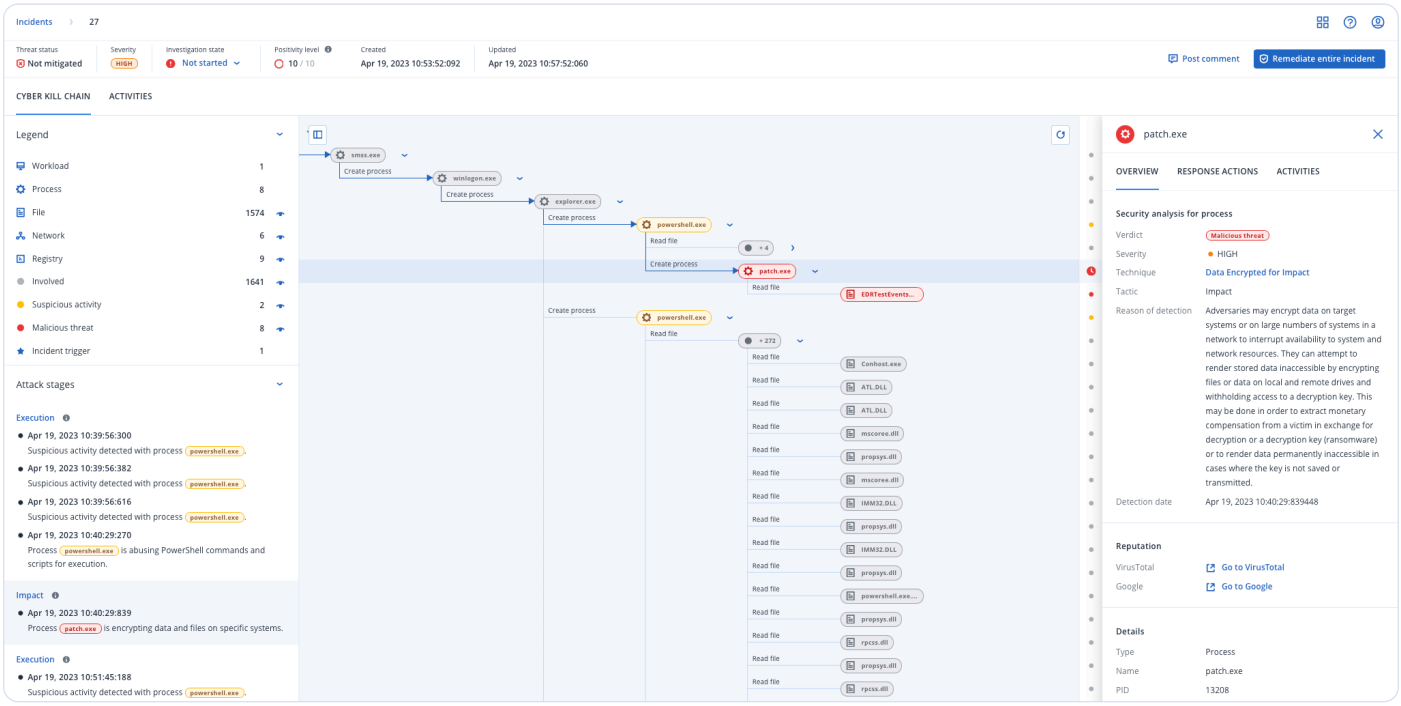
專為服務供應商設計的 Acronis Advanced Security + EDR

Acronis 瞭解服務供應商需要在提供有效服務與滿足不同客戶需求和預算之間做出平衡。

我們還知道，他們需要進階安全性解決方案來適當調整其利潤和內部技能，這種解決方案是多租用戶的、SaaS 型、可提供更好的安全性成果，並且專注於適量的自動化與易用性，以便在多個用戶端及其獨特環境中快速啟動與擴展。

Acronis Advanced Security + EDR 專為服務供應商設計，讓您可以簡化端點保護 — 快速偵測、分析與修補進階攻擊，同時確保無可比擬的業務連續性。消除多個單點產品的成本和複雜性，可為您的團隊提供一個易於管理和部署的完整網路資安防護解決方案。

藉由 Acronis 簡化偵測與回應服務



最佳化攻擊優先順序和分析以實現快速回應	整合式備份和復原功能可提供無與倫比的業務續航力	完整的網路資安防護解決方案 — 專為 MSP 設計，盡在單一代理程式中
• 透過排定潛在事件的優先順序和減少提醒疲勞，簡化調查 • 藉由自動化關聯和 AI 型引導式攻擊解譯，大規模解鎖分鐘而非小時分析 • 跨 MITRE ATT&CK® 提升可見性，以快速抓住攻擊分析與影響，包括攻擊進入的時間、造成的傷害以及它的傳播方式	• 整合式備份和復原功能，可在單點安全性解決方案失敗時提供無與倫比的業務續航力 • 簡化的一鍵修復和復原 • 跨 NIST 網路資安架構的完整、整合式防護 — 識別、保護、偵測、回應與復原，一切盡在單一解決方案之中	• 透過使用單一 Acronis 代理程式和主控台快速輕鬆地啟動新服務，以進行部署、管理和擴充 • 輕鬆跨多個用戶端進行擴充，同時保持可觀利潤並最大限度減少 OpEx，無需高技能人員組成的大型團隊來運作 • 與專注於您的成功和成就 (而非與您競爭業務) 的廠商合作。

由得到獲獎肯定的端點保護提供支援

PC EDITORS' CHOICE

↘ 編輯精選

AV-TEST The Independent IT-Security Institute

↘ AV-TEST 參與者和測試獲勝者

vb 100 VIRUS virusbtn.com

virus

↘ 獲得 VB100 認證

ICSA labs

↘ 獲得 ICSA Labs 端點防惡意軟體認證

AV comparatives

↘ 獲得 AV-Comparatives 認證

藉由 Acronis 實現無可比擬的業務靈活性

有了 Acronis，您就可以仰賴單一平台來實現全面的端點保護與業務連續性並遵循 NIST 等已有的行業標準，讓您能夠識別易受攻擊的資產與資料、主動保護這些資產與資料、偵測與阻止任何威脅、回應攻擊並從中復原。

Acronis：跨 NIST 的業務連續性

識別	保護	偵測	回應	復原
Advanced Security + EDR				
• 硬體清查 • 不受保護的端點探索	• 弱點評估 • 防止入侵 • 裝置控制 • 安全性設定	• 新興威脅動態 • 搜尋新興威脅的 IOC • 防惡意軟體與防勒索軟體 • AI 型與 ML 型行為偵測 • URL 篩選	• 快速事件分析 • 搭配隔離的工作負載修補 • 鑑定備份	• 快速復原攻擊 • 一鍵式大量復原 • 自助復原
Acronis Cyber Protect Cloud				
• 軟體清查 • 資料分類	• 修補程式管理 • DLP • 備份整合 • 網路指令碼	• 電子郵件安全性	• 透過遠端連線進行調查	• 預先整合災難復原

EDR 重要功能

事件優先順序

監控與主動關聯端點事件，並以事件警示的形式對可疑事件鏈排定優先順序

對應至 MITRE ATT&CK® 事件的自動化解譯

簡化回應並提高對威脅的回應能力，利用對應至 MITRE ATT&CK® 之攻擊的 AI 型解譯，可在幾分鐘內瞭解：

- 攻擊者如何進入系統
- 他們如何隱匿其軌跡
- 攻擊造成的損害及如何造成的
- 攻擊如何傳播

對攻擊實現一鍵回應，提供無與倫比的業務續航力

在單點解決方案失敗時佔上風 - 透過一鍵回應事件，利用網路安全、資料保護和端點安全組態管理整合的完整功能：

- **修復**：方法是隔離端點與威脅
- **進一步調查**：透過使用遠端連線和鑑定備份
- **防範日後攻擊**：透過填補開放弱點
- **確保業務連續**：依賴的是攻擊復原以及整合式備份與復原

1.來源：Verizon 的《2022 年資料外洩調查報告》