# Acronis Detection and Response

## 即時防止攻擊，透徹察覺所有網路威脅

Acronis Detection and Response 可供您抵禦規避組織防惡意軟體的威脅，是保護組織的最後一道防線。這項解決方案以零信任方法為設計軸心，可偵測並防止不符作業系統合法行為的任何異常活動，並提供即時察覺以及自動、手動修復功能。

| 威脅診斷安全性 | 即時威脅預防 | 清晰且詳盡察覺 |
|---|---|---|
| 新增威脅偵測和回應，提高端點的安全性。防止規避您的防惡意軟體防禦的攻擊，其中包括新的或未知的惡意軟體與勒索軟體、無檔案型攻擊、零時差攻擊和進階持續性威脅 (APT) | 部署可自動預防損害發生的可靠解決方案來停止針對安全漏洞的被動回應。無須手動搜尋威脅、昂貴的基礎架構或雲端連線 | 讓您的安全團隊藉由詳細察覺攻擊的時間軸、來源、策略、技術和程序 (TTP)，以及有關攻擊者試圖完成的資訊，強化您的組織安全狀態 |

## 保護您的端點和資料，避免遭受他人的失誤攻擊

| 將網路風險降至最低 / 防止任何威脅 | 確保快速回應事件 | 充分利用您的現有資源 |
|---|---|---|
| • 偵測和防止避開您的防惡意軟體防禦的進階攻擊 – 新的或未知的惡意軟體、無檔案型攻擊、零時差攻擊和 APT<br>• 增添最後一道安全層防線強化您現有的抵禦力，在漏洞造成組織資產損害之前先行阻止<br>• 採用「零信任方法」攔截不符作業系統合法行為的任何異常活動<br>• 在隔離及離線環境中工作 | • 藉由自動防護功能減少回應威脅所需的時間<br>• 透過能詳盡察覺每次攻擊，讓您的 SOC 團隊更游刃有餘<br>• 利用自動和手動修復功能<br>• 持續監控整個組織的端點和網路活動<br>• 運用由 Acronis 安全專業人員所負責的偵測與事件回應服務，進而獲得極致防護，從此高枕無憂 | • 藉清晰、詳盡察覺威脅的優勢減少額外資源的需求，擺脫不必要的議論雜音<br>• 補充您的其他防惡意軟體解決方案，無須拆換<br>• 對端點效能與頻寬耗用的影響度極小<br>• 無須額外的人員配置或昂貴的基礎架構，即可將您的 TCO 最佳化 |

## 從現代威脅防護方法中獲益

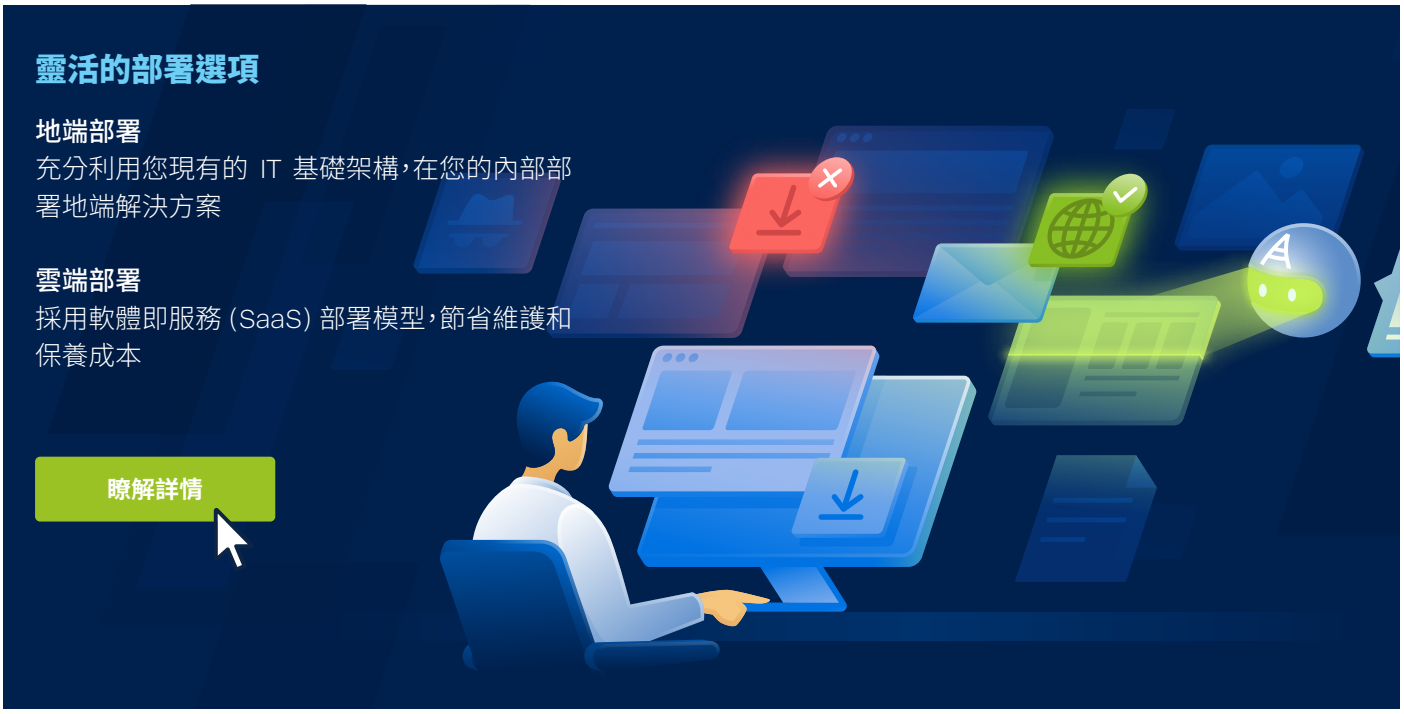
Acronis Detection and Response 為您的安全性堆疊新增了違規後威脅偵測和回應功能。識別並防止已避開其他防禦層的威脅，同時供您的網路資安團隊對為每個事件提供深入的鑑定分析。

| 自動、即時防護 | 威脅診斷防護 | 零信任方法 | 無資料氾濫 | 低 TCO |
|---|---|---|---|---|
| 一旦發現即自動防止威脅，不同於需要手動或半手動搜尋威脅和修復的解決方案。 | 偵測並防止規避新世代防毒（NGAV）解決方案的進階攻擊，例如新的或未知的惡意軟體與勒索軟體、無檔案型攻擊、零時差攻擊和 APT。 | 借助零信任方法提高威脅偵測的準確度，找出不符合法作業系統行為的任何異常活動，無須識別不斷演進的攻擊技術。 | 讓您的安全團隊能詳盡、清晰察覺威脅與事件，無須手動搜尋威脅及分析海量的資料。 | 透過自動搜尋威脅與低頻寬耗用，降低您的總持有成本 (TCO)。利用現有資源與基礎架構。 |

## ICSA LABS 認證的解決方案

ICSA Labs
Advanced Threat Defense
Certified

| 測試歷時 | 測試次數 | 惡意範本 | 偵測率 | 無害的應用程式 | 誤判率 |
|---|---|---|---|---|---|
| 33 天 | 1162 | 441 | 100% | 721 | 0.1% |




Acronis

瞭解詳情：
www.acronis.com