



IBM Security QRadar EDR

保護端點免受網路攻擊

現代化的端點威脅偵測與回應 (EDR) 解決方案可整合安全分析師體驗，並加快處理整個事件生命週期的速度。產品內建企業級 AI 和自動化功能，以提高分析師的工作效率，讓資源有限的安全團隊更能善用各種核心技術獲取更高的生產力。

IBM Security® QRadar® EDR 提供更全面的端點威脅檢測與回應方法：

解決端點威脅

智慧自動化功能幾乎可即時解決已知和未知的端點威脅。

搭載 AI 功能的威脅偵測

透過進階且持續學習的 AI 功能和簡單易用的介面，讓員工事半功倍，並有助維護持續營運。

攻擊路徑視覺化

將攻擊路徑以視覺化的故事板方式呈現，有助更明智的決策。

領先業界的告警管理

自動告警管理可緩解分析師的工作負擔，以更專注防範重要威脅

為何選擇 IBM Security QRadar EDR ?

100%

能見度

在 MITRE ATT&CK 架構的所有評估階段，都實現 100% 能見度。

100%

偵測

MITRE ATT&CK Evaluations 評估結果達到 100% 檢測率，無需變更配置。

80%

減少誤報

搭載 AI 功能的告警管理系統有助減輕分析師的工作負載。

功能及優勢

搭載 AI 功能的威脅偵測和洞察

主要功能



執行前的預防



NanoOS 和雙 AI 引擎



附加能見度



威脅獵捕



防範勒索軟體



行為偵測



API 存取



Cyber Assistant
網路安全助手



自訂教戰手冊

優勢

- 搭載 AI 功能的端點偵測
- 完整的獵捕及回應功能
- 優異的威脅解決方案
- 監控合規性
- 企業自動化
- 在任何環境中部署
- 管理偵測及回應 (MDR)

優勢特色

更深入瞭解端點運作情況

一覽無遺

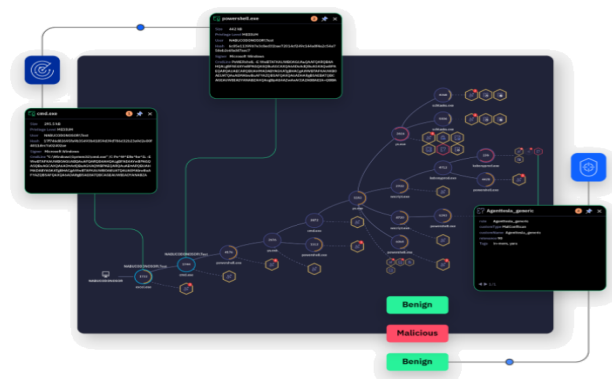
NanoOS 技術可讓您徹底瞭解端點上執行的程序和應用程式狀況。

自動化回應

AI 可近乎即時地自動偵測及回應以往未察覺的威脅。

化被動接招為主動出擊

透過易於創建的偵測及回應應用案例，在數秒內傳回結果，讓潛在的威脅無所遁形，防範攻擊於未然。



我有興趣

裝置需求

- 伺服器：硬體需求將依據端點管理數量。請參閱[系統需求](#)
- 代理程式：端點系統支援 Linux、macOS 和 Windows。請參閱支援版本的[代理程式系統需求](#)。
- 注意：如需 IBM QRadar EDR 規格及硬體/軟體支援指南，請參閱[IBM QRadar EDR 官方網站](#)