paloalto NETWORKS | CORTEX

端點安全買家必備指南

了解企業端點安全性必須提供的最重要功能

目錄

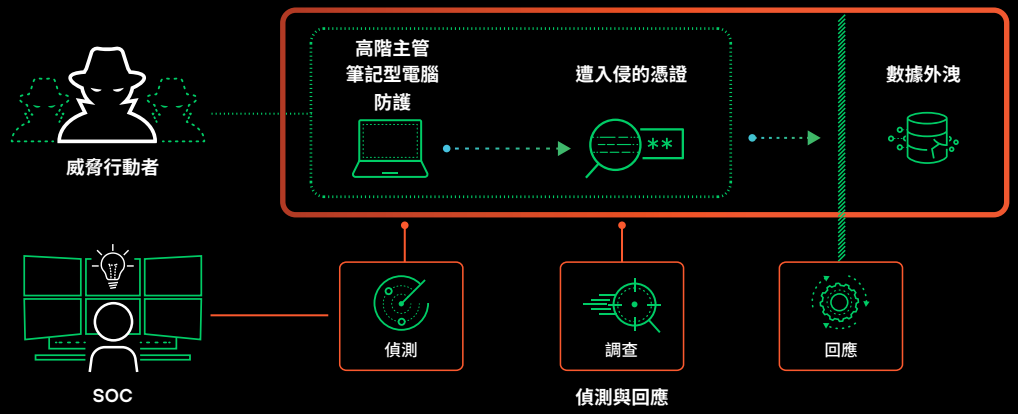
概覽

進階持續性威脅、勒索軟體即服務和 AI 支援的攻擊正在重新定義安全防護格局，不斷挑戰企業保持安全領先地位的能力。遺憾的是，當今各自為政的安全解決方案難以跟上不斷演進的威脅形勢，導致企業更容易遭受攻擊。這代表著攻擊者對於企業的入侵不再是「是否會發生」，而是「何時發生」的問題。

大量的警示、複雜的調查程序和持續無法偵測到的攻擊，早已讓安全團隊不堪負荷。隨著企業在雲端及任何其他領域擴展其數位足跡，待分析的安全遙測數據數量和多樣性呈等比級數增加，「數據淹沒」已不再是誇大其辭，而是真實的挑戰。

端點安全性是網路防禦的基礎。這是決定攻擊者遭到阻止或成功發動初步入侵的關鍵點，對於攻擊者捕捉來說也是最有用的數據來源。這對於整體安全狀況以及安全作業 (SecOps) 來說至關重要，因為他們必須在入侵發生之前先行識別並阻止網路攻擊。

因此，強大的**端點安全策略**對於維持安全領先地位至關重要。它應該能夠在傳統端點、網路、雲端工作負載、行動裝置、身分識別等領域提供全面的可視性與分析，透過統一的方法達到快速偵測與回應，以支援日益重要的安全作業。



> 到了 2028 年，30% 的企業都將採用來自相同廠商的預防性端點安全性、端點偵測與回應以及身分威脅偵測與回應，而 2024 年這一比例只有 5%。
>
> - Gartner[1]

[1] Evgeny Mirolyubov 等人，端點防護平台魔力象限，Gartner，2024 年 9 月。

了解端點安全性：
安全角色面臨的主要挑戰

安全角色面臨的主要挑戰

CISO

資訊安全長 (CISO) 努力跟董事會證明安全投資的合理性，同時展現企業安全狀況的具體改進成果。他們面臨的挑戰包括將技術指標轉化為商業價值、在不斷演進的威脅形勢中管理風險，同時確保遵循各項法規。CISO 還必須在強大安全措施與業務敏捷性和使用者生產力之間取得平衡，同時在預算限制內營運，並因應網路安全技能差距的挑戰。

SecOps 領導者

SecOps，或安全作業中心 (SOC) 領導者需確保其團隊具備適當的知識、程序和工具，以更有效地回應任何威脅。他們面臨的挑戰包括了解對手的策略和技術、在多種工具和平台之間協調如何回應，以及管理團隊面臨的警示麻痺和工作倦怠等問題。SecOps 領導者還必須不斷調整策略，以因應新型威脅、自動化資源分配，並提升平均偵測時間 (MTTD) 和平均回應時間 (MTTR)。

安全架構師

安全架構師面臨的挑戰是設計並實施一套全面的端點安全策略，既能因應不斷演進的威脅，還能無縫整合至現有的基礎結構和安全作業中。安全架構師努力識別和消除安全控制中的潛在盲點，管理氾濫的安全工具，確保各種解決方案之間的互通性。他們最主要的考量就是持續提升企業的安全狀況，同時在有效性、成本和使用者體驗之間取得平衡。

安全分析師

安全分析師位於威脅偵測與回應的最前線，負責因應不斷湧入的警示與潛在的安全事件。他們無法有效因應警示麻痺，並且經常需要處理誤判而浪費寶貴的時間。他們的主要挑戰包括更有效地排定警示優先順序、縮短調查時間，以及在日常任務與主動威脅捕捉及重大事件的深入分析之間取得平衡。

用於評估端點安全供應商能力的 10 大問題

1. 該解決方案如何處理複雜攻擊的偵測？

端點偵測與回應 (EDR) 功能

尋找一種具備最先進端點偵測與回應能力的解決方案，能夠持續監控端點是否有惡意活動跡象，因此可快速地偵測並回應複雜的威脅。

收集豐富的端點數據

有效的解決方案應能從端點收集大量遙測數據以發現潛在威脅。透過程序資訊、檔案活動、網路連線、登錄變更、使用者活動等數據的收集，該解決方案能夠進行更有效的偵測，以避免因工具過於狹隘而可能錯失的潛在威脅。

機器學習 (ML) 與行為分析技術

尋找能夠採用多種持續更新的機器學習模型來達到自動威脅防禦與偵測的解決方案。這些應該利用網路安全專家的真實見解，自動納入最新的威脅情報。這種方法可大幅降低手動分析時間、加速威脅偵測和回應，並讓分析師能夠著重於關鍵事件。

可自訂的偵測規則和預先定義的偵測

解決方案應內建豐富且立即可用的分析與偵測規則，同時具備靈活的自訂能力。此外，安全團隊應該能夠建立並微調偵測規則，以滿足其企業的特定需求和威脅形勢。這種結合預先定義以及可自訂功能的偵測方式，能確保對於各種進階攻擊提供全面的防護。

2. 該解決方案提供哪些進階威脅防禦功能？

多層方法

實施深度防禦策略，整合入侵防禦、AI 支援的惡意軟體分析、基於雲端的檔案檢查、行為威脅偵測和勒索軟體防護，確保即使攻擊者突破一層防禦，仍能由另一層攔截，進而建構一個全面的安全防護網，防範從惡意軟體到無檔案攻擊等各種複雜威脅。

行為式防護和入侵防禦

確保該解決方案能夠利用先進的行為威脅防護來分析相互關聯的程序行為，以揭露正在進行的攻擊。這種全面的監控可偵測多階段威脅，避免因單獨分析程序而遺漏任何威脅，而強大的入侵防護模組則可針對作業系統和應用程式的弱點提供關鍵防護。

AI 和機器學習式保護

實作 AI 驅動的安全引擎以全面審視所有傳入的檔案，並持續學習以對抗新興攻擊模式，進而偵測並封鎖傳統基於特徵碼的防禦措施可能忽略的複雜威脅。

3. 該解決方案的調查和回應方法是什麼？

自動建立各個事件的警示關聯性

尋找可利用機器學習自動將相關警示分組至各個統一事件的解決方案，以大幅減少警示麻痺，讓分析師能著重於優先順序較高的安全問題。

按風險排定事件優先順序並評分

部署機器學習式系統以根據風險因素分析並評分各個事件，因此能夠快速地評估攻擊範圍與影響以確保安全資源的最佳分配。

根本原因分析與攻擊鏈視覺化

尋找能夠自動找出根本原因的能力，並為每個事件提供信譽數據與視覺化攻擊鏈對應，讓分析師能夠快速了解威脅的脈絡與範圍。

自動和手動回應選項

實施靈活的回應架構，將例行性威脅的自動化動作與複雜情境下的人為介入選項相結合，讓安全團隊能夠根據威脅內容執行快速且自動化的補救與精準調整的回應。

與 SOAR 平台進行整合

選擇能與 SOAR 平台無縫整合的解決方案，以增強自動化工作流程並簡化整個安全堆疊中的事件回應程序。

4. 該解決方案如何因應警示麻痺和誤判的挑戰？

尋找可透過 AI 驅動的警示分類和優先順序排定來進行智慧警示分組並具備事件評分功能的解決方案

尋找一種 AI 支援的解決方案，以透過更具智慧的方式進行事件的分組和評分、自動建立相關事件的關聯性，並且根據影響和威脅可能性來評估風險。該系統應能利用資產關鍵性、使用者行為和威脅情報的內容式分析，並透過進階行為分析持續利用分析師的回饋進行學習，以提升優先順序排定的準確性並減少誤判率。

透過進階分析減少誤判

理想的系統應能充分利用 AI 支援的分析能力，並整合端點、網路和雲端環境的數據關聯性，以精確地區分真實威脅與無害的異常狀況，透過內容式分析將誤判的機率降到最低。

5. 該解決方案如何從傳統 EDR 擴展到 XDR 功能？

僅憑端點數據就可以獨立運作，同時具備脈絡擴展能力以增強偵測能力及工作流程整合

尋找一種能夠僅憑端點數據即可提供強大防護的解決方案，並在可用時無縫整合網路、身分和雲端數據來源，以增強威脅偵測的內容並簡化安全工作流程。

整合來自擴展來源的數據

尋找能夠無縫整合網路、雲端環境和身分系統等多種數據來源的能力，因為攻擊者會在多個環境中移動，而單一數據來源的可視性可能會留下危險的盲點。

跨數據分析和威脅關聯

該解決方案應提供先進的分析功能，能夠針對不同數據來源的威脅找出相互關聯性，從而全面呈現正在發生的安全事件。

完整的攻擊內容

理想的解決方案應能使用 MITRE ATT&CK 等共通架構，針對從初始入侵、橫向移動一直到數據外洩嘗試的整個攻擊鏈提供完整可視性。

轉型至統一的 SOC 平台

尋找一個能將多種安全工具整合至單一介面與數據來源的平台，同時確保可擴展至主要的 SOC 技術，包括 SOAR、新世代 SIEM 及攻擊範圍管理。

6. 該解決方案如何提供雲端偵測與回應？

適用於雲端特定架構 (例如容器、Kubernetes 和虛擬機器) 的執行階段安全

該解決方案應針對包括容器、Kubernetes 在內的雲端架構進行最佳化，並提供專為這些雲端原生架構進行調整的執行階段安全性，確保對於各種雲端工作負載的全面防護。

將執行階段遙測與無代理程式掃描和雲端服務供應商 (CSP) 日誌數據相結合，以全面了解雲端活動

尋找一種全面的雲端監控解決方案，將執行階段遙測、無代理程式掃描和 CSP 日誌數據與 CNAPP 安全見解相互結合，以提供對於雲端活動和工作負載行為的完整可視性。

機器學習式偵測/回應和事件管理工作流程

選擇可在機器學習驅動安全平台上執行的解決方案，該解決方案能夠跨雲端和內部部署提供統一的偵測與回應功能、支援混合雲端和多雲端架構，同時為安全團隊維護一致的工作流程。

7. 該解決方案如何整合身分式安全性？

與身分提供者進行整合

確保該解決方案能夠與 Active Directory 和 Okta 等各個主要的身分提供者進行無縫整合，以取得全面的使用者活動數據，為企業範圍的威脅偵測與回應提供必要的內容。

身分數據與其他安全遙測的關聯性

尋找一種解決方案，能夠找出身分數據與廣泛安全遙測之間的關聯性，以提供全面的使用者活動可視性，並結合風險評分和 UEBA 功能來快速識別可疑行為模式。

對於遭入侵的身分進行機器學習式、自動化偵測與回應

部署機器學習式身分威脅偵測與回應 (ITDR) 系統以自動識別異常使用者和實體行為，進而發現遭入侵的憑證和內部威脅，同時達到快速自動回應以緩減身分式攻擊。

8. 該解決方案如何簡化部署和管理？

單一代理程式安裝，部署後無需重新啟動

這最大程度地降低對於使用者的干擾，以針對大型環境進行快速部署和更新。

依預設實施最佳實務安全政策

這從第一天起就確保強大的安全狀況，同時仍允許進行自訂以滿足特定需求。

對於安全內容更新的部署進行精細且分階段的控制

如此一來就可以分階段測試及部署新的安全內容，在確保穩定性的同時最大程度地減少潛在干擾。

統一管理主控台

尋求一種解決方案，透過單一且直覺的主控台提供全面的安全管理 (從端點政策管理到威脅偵測、調查與回應)，在簡化管理程序的同時提供關於企業安全狀況的一致性觀點。

對於端點效能的影響

代理程式應透過較低的 CPU 使用率和 I/O 大幅減少對於端點效能的影響，確保在不影響使用者生產力或系統效能的情況下提供強大的安全防護。

大型企業的可擴充性

它應能輕鬆地適應不斷增長的端點數量和持續增加的數據量，而不需要大幅增加基礎結構投資。

9. 有哪些業界驗證與獨立測試結果可證明該解決方案的有效性？

在 MITRE Engenuity ATT&CK 評估中的表現

參考該解決方案在最近的 MITRE Engenuity ATT&CK 評估中的表現。尋找組合防護與偵測評分較高的解決方案，最好無需變更設定即可提供強大且立即可用的效能。關注分析涵蓋範圍以及是否存在延遲偵測情況等指標。

來自 AV-Comparatives 和其他獨立測試的結果

尋找在端點防禦與回應測試中獲得高分的解決方案，以驗證其在真實情境中的有效性。

客戶評價與分析師認可

透過業界特定評價考量同行回饋以展現在真實世界的效能，同時參考 Forrester Wave™ 和 Gartner® 魔力象限™ 等分析師報告對於該解決方案的評價，以驗證其市場地位與技術實力。

10. 該解決方案是否支援從 EDR 發展到 XDR，並最終透過 AI 和自動化實現完整的 SOC 轉型？

進步成長的基礎

尋求一種解決方案，將進階威脅防禦、偵測與回應在內等核心 EDR 功能與主機防火牆、磁碟加密支援和裝置控制等基本端點防護功能相結合，以達到端點層級的全面安全性。

XDR 功能的演進

評估該解決方案如何整合網路、雲端、身分和第三方數據來擴展至 XDR，以達到所有安全遙測的統一可視性和自動關聯能力。

達到 SOC 全面轉型的路徑

確保平台可透過 SOAR 和新世代 SIEM 功能擴充以達到完全自動化，將攻擊回應時間從幾天縮短到幾分鐘。

滿足未來需求的架構

該解決方案應提供一個統一的後端，支援貫穿所有三個階段 (從 EDR 到 XDR 再到真正的 SOC 平台)，同時保持一致的工作流程並自始至終充分利用 AI 驅動的自動化。

考慮使用 CORTEX 來制定滿足未來需求的端點安全策略

在考量端點安全策略轉型的 10 個關鍵問題後，可以明確看出在現今快速演進的威脅形勢中，採取全面且具智慧的方法至關重要。

Cortex XDR® 於是一躍成為能夠滿足這些關鍵需求的解決方案，提供超越傳統端點安全的進階威脅防禦、偵測與回應能力。

Cortex XDR 的 AI 驅動方法解決了本報告所一再強調的挑戰。它在威脅防禦方面提供業界最佳的效能，並且在 **2024 年 MITRE Engenuity ATT&CK 評估**中達到 100% 的偵測率。Cortex XDR 大幅減少警示麻痺和誤判等情況，同時整合多個來源的數據以獲得整體觀點，並提供自動和手動回應選項。這些功能與其雲端就緒架構和身分安全整合能力相結合，讓 Cortex XDR 成為現代安全團隊的強大工具。

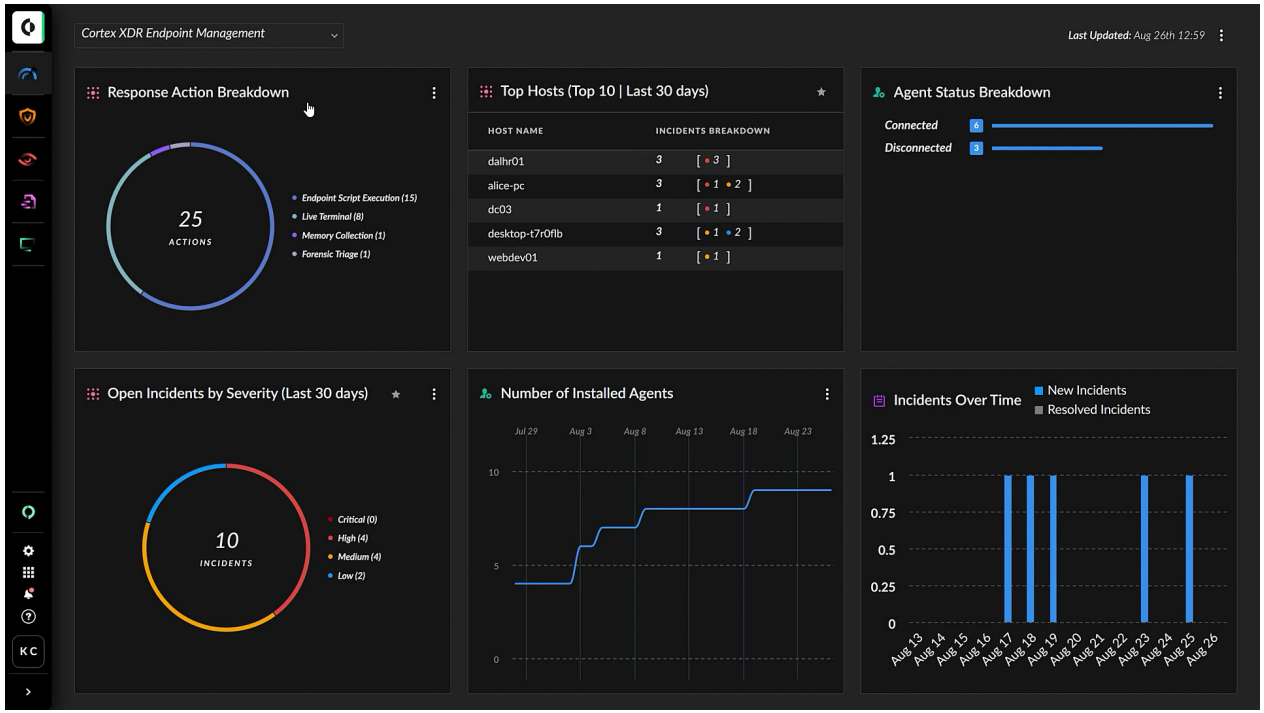


圖 1：Cortex XDR 端點管理

對於希望達到 SOC 轉型的企業來說，Cortex XDR 提供可擴充的基礎。其架構可讓安全團隊從核心 EDR 功能開始，逐步擴展到完整的 XDR 功能，以滿足企業不斷變化的需求。

作為安全之旅的下一步，**Cortex XSIAM®** 以 Cortex XDR 的功能為基礎，透過 SOAR 擴展回應自動化，並透過劃時代的 AI 驅動方法達到新世代 SIEM 擴展數據擷取能力 XSIAM 平台透過 AI 和自動化達到安全作業的轉型，並在幾分鐘內阻止威脅，而不需要花上數天或數週的時間。

在選擇 Palo Alto Networks Cortex® 解決方案後，企業投資的安全策略不僅可以滿足目前的需求，還可以因應未來的挑戰。憑藉著對於持續研發的承諾、面對新興威脅的適應能力，以及明確的未來安全發展路線圖，Cortex XDR 和 XSIAM 提供一條通往更具彈性、高效率且高效能安全狀況的路徑，以因應日益複雜的數位世界挑戰。

透過 **Cortex XDR 產品導覽**親身體驗這些功能，讓您可以探索該平台的進階功能並了解其如何達到端點安全作業的轉型。

全面的 MDR

全天候專家安全營運

我們的託管式偵測與回應 (MDR) 服務由 Cortex XDR 技術提供支援，結合專業人員的專業知識與進階威脅偵測與回應能力，提供全天候的全面安全防護。我們透過警示管理、事件回應和主動威脅捕捉來協助各種規模的企業加強安全狀況。

我們靈活且基於結果的方法，可針對企業的獨特需求量身打造自訂規則與劇本，並透過基於時間的 SLA 支援進行偵測與回應。透過與我們的合作，您可以立即提升安全作業成熟度，並由我們負責處理現代安全威脅的複雜度，讓您的團隊能著重於策略計劃。

透過適用於 Cortex XDR 的 Unit 42 MDR 確保您的未來安全無虞。

進一步了解 →

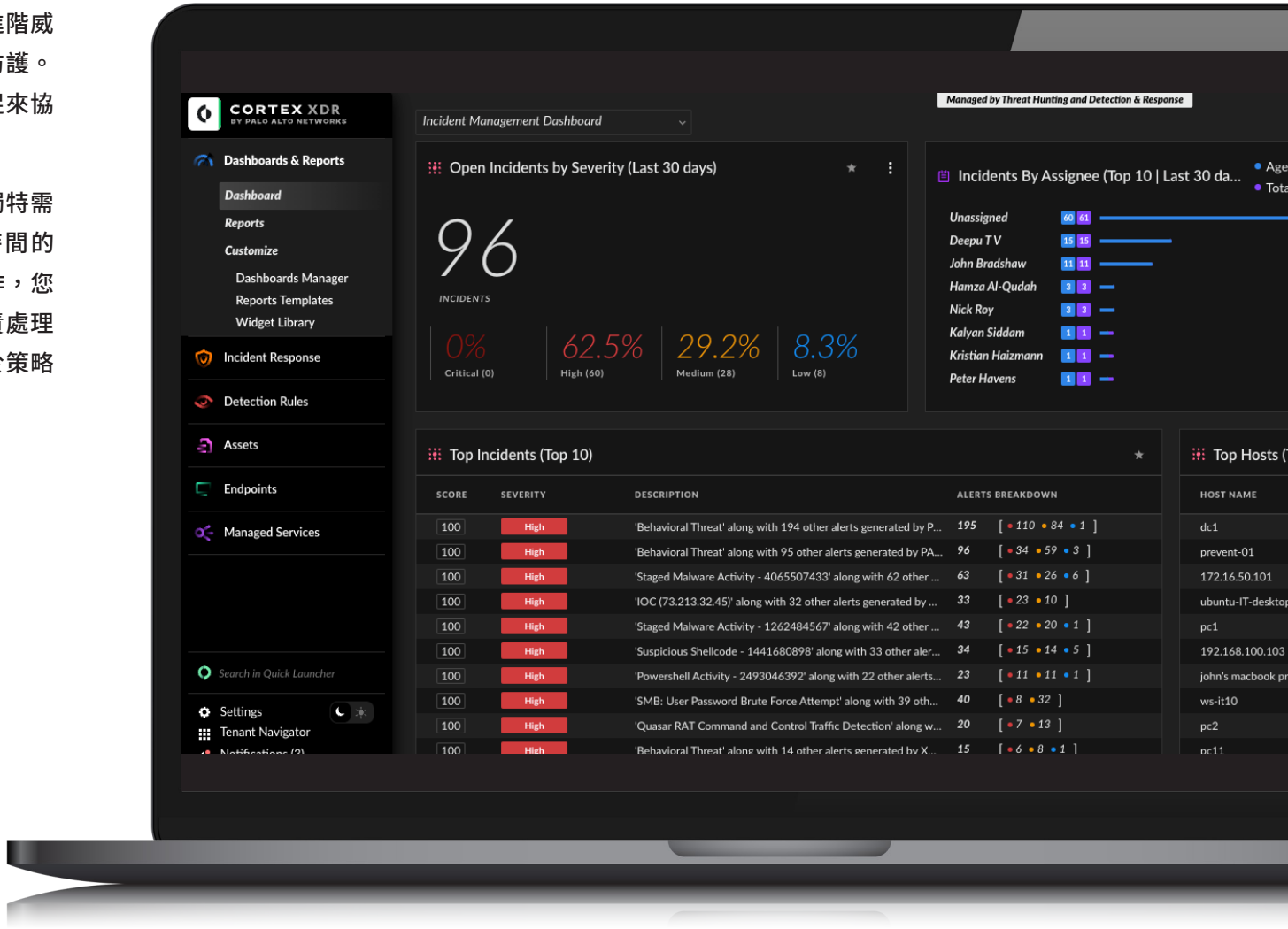


圖 2：Cortex XDR 與 Unit 42 託管式偵測與回應 (MDR) 儀表板

您必備的端點安全評估檢查清單

進階威脅防禦

多層防護能力
- ☐ 新世代防毒功能
- ☐ 勒索軟體防護
- ☐ 無檔案攻擊防禦
- ☐ 入侵防禦模組
- ☐ 行為式防護

AI/機器學習式防護引擎
- ☐ 本機沙箱功能
- ☐ 持續更新的模型

附加安全功能
- ☐ 主機防火牆功能
- ☐ 磁碟加密支援
- ☐ 裝置控制能力

偵測能力

EDR 基礎
- ☐ 即時監控
- ☐ 全面的端點遙測數據收集
- ☐ 跨來源建立事件關聯性

機器學習和分析
- ☐ 行為分析能力
- ☐ 針對不同威脅類型的多個機器學習模型
- ☐ 定期模型更新

偵測靈活性
- ☐ 預先建立的偵測規則
- ☐ 自訂偵測建立選項
- ☐ MITRE ATT&CK 架構調整

調查與回應

警示管理
- ☐ 自動警示關聯性
- ☐ 基於風險的優先順序
- ☐ 降低誤判率的能力

調查工具
- ☐ 根本原因分析功能
- ☐ 攻擊鏈視覺化
- ☐ 詳細的事件內容

回應選項
- ☐ 自動化回應能力
- ☐ 手動回應工具
- ☐ SOAR 平台整合

擴展的偵測與回應

數據整合
- ☐ 網路數據擷取
- ☐ 雲端安全整合
- ☐ 身分提供者整合

跨數據分析
- ☐ 多來源關聯性
- ☐ 統一的事件檢視
- ☐ 擴展調查的內容

雲端安全

雲端工作負載防護
- ☐ 容器安全
- ☐ Kubernetes 保護
- ☐ VM 安全性

雲端整合
- ☐ 雲端供應商日誌整合
- ☐ CNAPP 整合
- ☐ 多雲端支援

部署與管理

實作
- ☐ 單一代理程式架構
- ☐ 無需重新啟動部署
- ☐ 預設安全政策

管理
- ☐ 統一管理主控台
- ☐ 以角色為基礎的存取控制
- ☐ 政策管理工具

效能
- ☐ 系統影響低
- ☐ 面向企業的可擴充性
- ☐ 頻寬最佳化

驗證和測試

業界認可
- ☐ MITRE ATT&CK 評估結果
- ☐ 獨立測試評分 (AV-Comparatives 等)
- ☐ 分析師認可 (Gartner、Forrester)

客戶驗證
- ☐ 您所屬產業的客戶參考
- ☐ 案例研究
- ☐ 生產環境測試結果

提供未來保證

廠商評估
- ☐ 研發投資
- ☐ 功能發佈節奏
- ☐ 威脅研究能力

路線圖評估
- ☐ 計劃新增的功能
- ☐ 技術合作夥伴關係
- ☐ 整合能力

平台演進
- ☐ 可擴展至完整的 SOC 平台
- ☐ AI/機器學習開發計劃
- ☐ 自動化能力

成本和支援

定價結構
- ☐ 授權模式
- ☐ 額外的模組成本
- ☐ 大量折扣

支援服務
- ☐ 全天候技術支援
- ☐ 實作協助
- ☐ 訓練資源

合規性和報告

法規合規性
- ☐ 內建合規性報告
- ☐ 支援主要法規 (GDPR、HIPAA、PCI DSS 等)
- ☐ 自訂合規性報告建立

稽核支援
- ☐ 稽核追蹤功能
- ☐ 歷史數據保留選項
- ☐ 證據收集工具

整合能力

安全工具整合
- ☐ SIEM 整合
- ☐ 威脅情報平台整合
- ☐ 票證系統整合

API 可用性
- ☐ REST API 文件
- ☐ 自訂整合支援
- ☐ API 頻率限制和配額

數據匯出
- ☐ 自訂報告產生
- ☐ 原始數據匯出功能
- ☐ 數據格式選項

使用此檢查清單作為選擇全面端點安全解決方案的指南，該解決方案不僅可以滿足您目前的需求，而且可以為您的安全作業轉型奠定基礎。正確的決策不僅能保護您現今的企業，還能讓您更有效地因應未來的新興威脅。

廠商評估

公司穩定性
- ☐ 財務健全狀況
- ☐ 市場佔有率
- ☐ 客戶保留率

支援基礎結構
- ☐ 全球支援涵蓋範圍
- ☐ 支援回應 SLA
- ☐ 知識庫品質

社群資源
- ☐ 使用者社群規模
- ☐ 社群論壇
- ☐ 第三方整合市場

營運需求

離線能力
- ☐ 離線保護功能
- ☐ 本機偵測能力
- ☐ 數據快取機制

備份和復原
- ☐ 代理程式備份選項
- ☐ 設定備份
- ☐ 嚴重損壞復原支援

資源最佳化
- ☐ CPU 使用控制
- ☐ 記憶體最佳化
- ☐ 網路頻寬管理

立即開始

安排示範，了解 Cortex XDR 如何協助您和您的企業簡化營運、阻止大規模威脅並加速目前和未來的事件補救。

諮詢熱線：0800666326
網址：www.paloaltonetworks.tw
郵箱：contact_salesAPAC@paloaltonetworks.com

Palo Alto Networks 台灣代表處
11073 台北市信義區松仁路 100 號 6F-1