CITADEL
NETWORK GUARDIAN

CYFOUNDRY 台灣資安鑄造公司 | DATASHEET
V1.0 | Q2 2024

提升網路安全

運用最新的偵測和回應技術

在資安威脅加劇的大環境下，各企業和公司都需要一個可靠和高性價比的解決方案來保護旗下的數位資產

Citadel NDR 作為企業尋求的首選，除了具備強大的網路偵測與回應能力外，還移除了大品牌常被用戶所詬病的複雜功能設計，以減少開發成本降低用戶開銷

即時威脅情資與防護
Citadel NDR 可不斷監控和即時更新網安情資，來因應瞬息萬變的網路威脅活動，以確保企業網路的完整性

多樣整合能力
Citadel NDR 支援JSON和CEF等格式輸出，可無痛整合到既有的SIEM或SOC系統，以強化你的網路安全布局

支援各類網路架構
Citadel NDR 的叢集式架構可彈性佈署在不同的辦公場域，滿足各式複雜的網路結構，並提供快速與可靠的資安解決方案，亦提供佈署落地雲方案，滿足企業機敏需求

運用AI辨認未知威脅
Citadel NDR 藉由強大的人工智慧引擎主動辨認網路威脅，即早採取預防措施避免災害擴大

轉變您的

網路安全布局

透過 Citadel NDR 提升網路安全防禦和可視性，提供簡單而且牢不可破的網路保護。體驗即時的檢測與回應所帶來的影響、最新的威脅情報、全面支持所有網路連接技術，以及全天候的先進 AI 監控

透過 Citadel NDR 提升您的網路安全防禦，讓您的網路受到網路威脅檢測與回應技術保護

產品特點

自動阻擋與檢測
根據你的安全策略和工作需求，可以選擇Inline Mode自動阻擋惡意連線，或使用Mirror Mode進行被動檢測

強化各種設備平臺的安全
Citadel NDR 可為IT基礎設施、OT系統乃至SCADA系統，提供堅不可摧的保護，讓內部網路的每個設備免於網路威脅。Citadel還可以作為入口閘道器，縝密的監控所有網路流量，識別出任何未經授權和有害的連線，保護底下IT、IOT及OT的運作。

異常檢測
運用AI自我訓練方式，檢測異常行為，確保每一秒都在識別潛在威脅，甚至是zero-day攻擊

加強網路安全措施
Citadel NDR 整合了入侵預防系統(IPS)、入侵檢測系統(IDS)和封包捕獲(PCAP)技術，綜合多層防禦策略，運用各式的手段有效地識別和阻擋外部和內部網路威脅，確保您網路的完整性和安全

簡化安全設定
Citadel NDR 旨在通過無縫整合和自動更新威脅情報來簡化您的網路安全操作。其直觀的功能提高了可視性和合規性，保護您的組織數位足跡，保護所有網路連接設備

為什麼選擇 Citadel NDR?

我們如何從競爭中脫穎而出

成本效益

Citadel具有價格優勢，為各種規模的組織提供強而有力的檢測與回應能力

簡單好上手

Citadel NDR 導入直覺式設計，降低使用者摸索時間，不須繁瑣的步驟就可以查到你要的資訊

安全且合規

運用Citadel NDR，不但可以確保數位資料的安全，還能產生合規用的報告，以達到政府法規或是企業資安政策的要求

無痛整合既有系統

Citadel NDR具備多元安裝選項，不須繁瑣設定，就可以介接到現有的SIEM和SOC服務，無須中斷任何安全防護機制，不影響商業運作

針對當下威脅

建立的安全

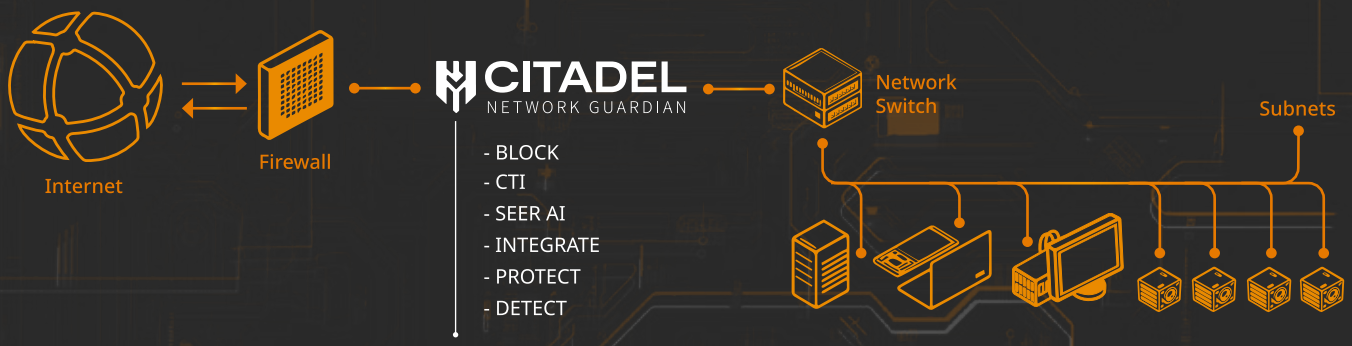
Citadel NDR 是針對瞬息萬變的網路威脅所建立的前線防禦，提升了你的安全防守範圍和能力，並可以保護易受攻擊的 IT、IoT 和 OT系統

Citadel 藉封包檢測技術，偵測駭客的外對內攻擊，以及網路內的橫向移動行為。全盤覆蓋佈署方式，確保組織的資訊免於複雜的網路威脅侵害，使 Citadel NDR 成為當前最有效的網路防護解決方案。

輕鬆安裝

Citadel NDR 無縫整合到現有網路基礎設施架構，提供快速且簡便的安裝過程
彈性的配置方式，可確保以最小的干擾保護敏感數據，強化現有網路安全布局

Inline 模式 //



Mirror 模式 //