

# 臨床網路衛生

降低裝置的風險與優化裝置的可用性

概述

沒有企業組織可以管理看不見的裝置，這正是許多醫療保健提供組織(HDO)難以管理其裝置風險的原因。缺乏對相關裝置細節的了解，加上主動裝置掃描可能會中斷患者照顧，讓 HDO 極難了解其連線裝置的攻擊面區域。若要了解和管理醫療及 IoT 裝置對 HDO 不間斷營運的風險，便需要系統性的方法。

## 主要優勢：

- 裝置風險要素的可視性與入侵的可能性
- 簡化弱點管理的計畫與執行
- 安全掃描並採取降低風險的行動，以及優化裝置的可用性

## Medigate 的臨床網路衛生

Medigate 的臨床網路衛生(CCH)模組會分析、對應與彙總未託管端點所帶來的威脅，以協助 HDO 了解與降低其裝置的風險。透過 CCH，有效弱點管理和協調策略可以讓 HDO 快速排序其連線端點內的風險，以及執行有效弱點管理和協調策略來優化其裝置的可用性並降低風險。

### 運作方式

Medigate 利用深度封包檢測(DPI)的技術深入研究每個裝置，提供重要裝置特性的可視性。接著 CCH 會將其應用到獨特的風險評估架構，以解決會影響遭入侵裝置可能性與嚴重性的個別要素。在臨床的環境中，CCH 會給每個裝置指派一個相對的風險分數。CCH 會讓 HDO 專注在最重要的事情，讓他們優先修補或分割具有已知資安弱點的裝置，並保護其整體運作的可用性與完整性。有了 CCH，HDO 可以獲得：

- **自訂的風險架構：**個別 HDO 可以打造 Medigate 裝置風險分數架構的結構，其中包括裝置屬性、網路連線、公共弱點及漏洞(CVE)等要素。
- **風險分數模擬：**計算假設裝置設定與修復活動的優勢或風險，以確保沒有干擾和意外。
- **弱點掃描協調：**身分識別感知掃描資訊支援弱點管理掃描中的適當包含/排除 IoT 及 IoMT 裝置，以確保關鍵作業與患者照顧不會中斷。
- **修復建議：**IoT/IoMT 裝置的臨床感知修正與修補建議，讓 HDO 能夠知道將其資源集中的位置。

## 結論

大部分的 HDO 難以了解與解決其連線裝置對其運作所構成的風險。Medigate 了解臨床裝置的獨特語言，不用透過 AI 或機器學習猜測其提供的資料。相對地，這些技術可以用來從裝置資料中提供先進的見解。透過 Medigate，您所有連線裝置中可用的資料都會解除鎖定且可以信任，而且 HDO 可以有信心改善照護的可用性與品質，同時安全加速其即時醫療保健計畫。

總代理



台北總公司

台北市內湖區  
瑞光路583巷32號5樓  
電話：02-2658-1818

台中辦事處

台中市北屯區文心路四段83號19樓301室

高雄辦事處

高雄市三民區民族一路80號27樓之2 A08室



電子郵件：[contact@medigate.io](mailto:contact@medigate.io)

請造訪：[medigate.io](http://medigate.io)

 **MEDIGATE**