CLAROTY

Cyberworld

購買指南

醫療保健網路安全平台

保護醫療保健環境中的 IT、IoT、IoMT、BAS
和其他網路實體系統。

CLAROTY

Cyberworld

目錄

您閱讀本指南可了解到：

網路實體系統(Cyber Physical System，CPS)被 Gartner® 定義為「協調感測、運算、控制、網路和分析以與實體世界(包括人類)互動的工程系統。在受保護的前提下，它們可以實現安全、即時、可靠、有彈性和適應性強的性能。」*

CPS常見於關鍵基礎設施和醫療保健機構，涵蓋了數量激增的連網設備，這些連網設備對醫療保健服務機構 (Healthcare Delivery Organization，HDO) 至關重要。以下是醫療保健機構CPS的主要範例：

物聯網(IoT)和醫療物聯網(Internet of Medical Things，IoMT)，例如可以追蹤健康指標的智慧手錶、遠端病患監察(如血糖監測儀或心電圖機)、醫療影像系統(如MRI機器或CT掃描儀)以及穿戴式裝置。

樓宇自動化系統(Building Automation System，BAS)，例如智慧照明和通風設備、電梯和實體通道機制、醫院病患監察、智慧樓宇、智慧電網和自動駕駛汽車。這些智慧網路系統與實體世界互動，以支援安全關鍵型應用中的即時、有保證的性能。

儘管這些設備有助於維持正常生活並提供高品質的病人護理，但它們大大增加了網路安全風險和擴大了攻擊面。保護病患安全非常重要。HDO希望加強其網路安全態勢，迫切尋找為確保這些設備的安全而設計的CPS保護平台。如今，需求的增長推動了CPS保護平台市場的迅速擴張，出現了許多新CPS安全供應商。

*Gartner於2022年9月21日發佈的《Tool: Cyber-Physical Systems Protection Platform Rating and Selection》，作者：Wam Voster、Katell Thielemann。

CLAROTY

Cyberworld

醫療保健領域的網路安全格局

CLAROTY

Cyberworld

病人護理

醫療保健機構的網路彈性和安全態勢與病患安全和照護結果直接相關。如果醫療保健機構遭受了常見的網路攻擊(例如勒索軟體、供應鏈攻擊、雲端攻擊和網路釣魚)，患者的死亡率就可能上升。為了保護病患、工作人員和訪客的人身安全，確保CPS的安全至關重要。

數位轉型

數位轉型將更多的連網設備引入醫療保健環境，改變了HDO的安全態勢。儘管更強的連接性可以節省成本和提高資源利用效率，但擴大了攻擊面擴，讓網路犯罪分子能夠進入這些本質上不安全的醫療保健環境。

舊設備

醫療保健環境中的舊設備一般是幾十年前製造的，沒有考慮到網路安全性，缺乏保護其免受網路攻擊的必要功能。隨著數位轉型的加速，這些實體隔離的設備已連接到互聯網，因此出現了新的攻擊媒介。如果更換舊設備，可能導致營運中斷，因為這可能需要停機或降低功能，會對病患安全造成嚴重影響。

50%

根據 Ponemon Institute 的調查顯示，50%的受訪醫療保健機構在遭受常見的網路攻擊后，醫療手術併發症增加；23%的受訪醫療保健機構表示，死亡率有所上升。[1]

FBI網路犯罪投訴中心(IC3)警告稱，陳舊的和/或缺乏適當安全功能的醫療設備會帶來網路風險，對病患安全、個人資料和醫院營運造成負面影響。[2]

根據《Healthcare Cybersecurity Benchmarking Study 2024》報告顯示，使用NIST網路安全框架作為主要網路安全框架的醫療保健機構，其網路保險費用增幅降低了三分之一。[3]

CLAROTY

Cyberworld

網路保險

保險公司會根據網路安全最佳實踐的標準、程序和其他措施來評估客戶的保險費用。這迫使HDO要採取更完善的網路安全措施，也給HDO帶來了額外的成本壓力。同時，HDO遭受網路攻擊的財務損失、嚴重程度和頻率在不斷上升，導致網路保險費用大幅上漲。

技能差距

針對醫院和衛生系統的網路攻擊的頻率及複雜性在不斷增加，醫療保健機構一直在努力招募、培訓和留住熟練的生物醫學技術人員。但是，醫療保健領域的人才依然短缺，預計將來會持續減少。

監管要求

由於醫療保健領域發生上述變化，監管機構要求制定網路安全最低標準，要求HDO實施具體措施以保護其關鍵業務免受網路攻擊。這些標準包括美國HHS第 405(d) 條和 HPH CPG (2024年1月發佈)、歐盟 NIS2、以及全球廣泛使用的NIST CSF。

47%

根據Claroty的《The Global Healthcare Cybersecurity Study 2023》報告顯示，47%的受訪者至少經歷過一起影響其CPS(包括醫療設備和/或樓宇管理系統設備)的網路安全事件。[4]

40%

根據 24x7 Magazine 的工作滿意度調查顯示，現任就業的生物醫學技術人員(BMET)年齡在55歲或以上的佔40%，年齡在60歲以上且接近退休的佔22%。[5]

加強網路安全措施已經成為總統的首要任務。美國白宮發佈《National Cybersecurity Strategy》，要求加強對關鍵產業的監管，並要求其採取基本的網路安全措施。[6]

CLAROTY

Cyberworld

醫療保健網路安全解決方案的選擇標準

CLAROTY

Cyberworld

具備網路安全產業專業知識

選擇CPS安全解決方案的標準之一：CPS安全供應商必須具備產業專業知識，包括透過研究團隊和公共部門的參與來推動進步。如果CPS安全供應商擁有屢獲殊榮的研究團隊，就可以讓易受攻擊設備的製造商提高其產品的安全性，還可以提高這些產品支援的關鍵營運和基礎設施的安全性。研究團隊應該揭露支撐關鍵營運的XIoT設備中的漏洞，提供所需的產業專業知識，為客戶提供更強有力的保護，抵禦最嚴峻的威脅。

對醫療保健網路安全的投入

對於醫院或醫療保健領域的其他買家來說，CPS安全供應商應該在醫療保健產業中具備豐富經驗，以及擁有優先考慮病患安全的解決方案。如果CPS安全供應商不具備醫療保健產業的專業知識、不瞭解HDO網路上的設備類型、也不能為病患提供安全有效的護理環境，則不在考慮範圍之內。CPS安全供應商還應該深入瞭解醫療保健領域的法規、醫療設備協議、營運效率、以及臨床設備所面臨的網路威脅。所以，您需要尋找多年來為HDO提供服務、並在該環境中擁有深厚專業知識的CPS安全供應商。

擁有深度可視性

沒有兩個CPS網路是完全相同的，因此不能用一種通用的方法來發現它們。CPS安全供應商應該具備多種發現方法，以便識別營運網路內的所有資產，包括那些使用獨特或專有協議、或無法僅透過被動方式存取的資產。雖然HDO一般會優先考慮被動方法，以減輕對臨床工作流程的干擾，但HDO真正需要的是深度可視性和主動掃描方法。因此，不同的設備需要獨特的發現方法。

CLAROTY

Cyberworld

單一平台提供全面保護

專注於醫療保健領域的CPS安全供應商應該提供一套統一的解決方案，為您的環境提供全面的保護。透過單一平台，可以在單獨一個地方管理、監察和控制安全解決方案，從而更輕鬆地簡化風險管理、應用補償控制與應對威脅。單一事實來源(Single Source of Truth，SSOT)可以為整個基礎設施提供安全性，無需確定範圍、部署、集成和維護多個單點解決方案，從而降低了資金成本，並最大限度地減少了資源分配和培訓要求。

實現更佳的業務成果

為了實現更佳的業務成果，HDO需要正確的數據元素來優先考慮營運效率，並提高投資報酬率(ROI)。從顯示醫療設備的使用情況和生命週期的數據，到與CMMS/CMDB的集成，CPS安全供應商都必須提供增強營運和簡化工作流程的功能。如果您與對醫療保健產業有深入瞭解的CPS安全供應商合作，就可以減輕IT團隊的負擔。因爲您能依靠其對醫療資產有深入瞭解的平台、以及如何更好地利用網路數據來改善營運，並監察設備使用情況以獲得更佳成果。此類功能會節省時間、降低成本並有效管理資源，從而為HDO帶來更高的ROI。

靈活部署

專注於醫療保健領域的CPS安全供應商應該提供雲端選項，這些選項可以在使用者提供的硬體上運作。這可以幫助HDO降低採購、維護和更新硬體的成本。它還讓您能夠根據可擴展性、成本考量或合規性標準的要求，靈活地選擇部署解決方案的位置和方式。同樣重要的是，為部署而客製化的資產發現方法。由於每個HDO都有獨特且複雜的環境，臨床與非臨床工作流程、操作因素和網路拓樸都是發現過程必須考慮的因素，CPS安全供應商應該使用多種資產發現方法。

CLAROTY

Cyberworld

實現網路和營運彈性的關鍵方法

CLAROTY

Cyberworld

發現所有CPS資產

評估CPS安全解決方案的首要標準：提供對您環境的可視性。因爲可視性為您的整個網路安全之旅奠定了基礎。新的CPS資產每天都在未經適當授權的情況下多次連接到HDO網路。如果HDO看不到或無法瞭解其資產，就不能進行全面保護。獲得對CPS的可視性，是當今安全和風險負責人面臨的最基本且最具挑戰性的任務之一。此外，傳統的安全工具往往缺乏瞭解設備工作流程所需的重要詳細信息。僅透過手動操作很難維護準確且最新的設備設定檔，使問題變得更加複雜的是連接設備設定檔的不完整性。而且，每個CPS環境都是獨一無二的，大多數環境都是複雜的，某些資產發現方法不一定有效。CPS安全供應商應該提供多種高度靈活的發現方法，這些方法可以混合和搭配使用，以最適合您獨特需求的方式提供全面的可視性。具體來說，深度封包檢測(Deep Packet Inspection，DPI)對於醫療保健環境至關重要，因為該環境擁有種類繁多的連接設備，需要多種發現方法才能實現全面的可視性。

將現有的IT工具和工作流程集成到所有CPS中

儘管傳統的安全工具缺乏瞭解設備工作流程所需的重要詳細信息，但這並不意味著它們無法保護CPS中的產品。您不應該擴展已經很廣泛的技術堆疊(例如CMMS/CMDB)，而應該評估與它們集成的CPS安全解決方案，從而彌補臨床工程團隊和安全團隊之間的技能差距。同樣重要的是，與醫療設備製造商 (Medical Device Manufacturer，MDM) 的合作，除了漏洞研究，還包括協議文件共享、MDS2、VEX和SBOM，以實現快速修復。您可以透過擴展現有的工具和工作流程，將您的技術堆疊與專門設計的CPS安全解決方案相集成，從而安全地發現風險盲點，不會危及病人的治療結果。該策略可幫助HDO控制其風險環境，並在傳統上孤立的團隊中創造進一步的可視性。此外，將臨床環境添加到現有安全計劃中，這將為屬於您臨床工作流程的設備提供綜合數據，並幫助您的團隊根據它們與醫院核心營運的關係確定優先順序。

將IT安全控制和治理擴展到XIoT環境

與IT環境不同，大多數CPS環境缺乏必要的網路安全控制和統一的治理。許多CPS環境中的IoMT設備在設計時，注重的是功能和操作的可靠性，而不是安全性，因爲這些系統最初並不打算連接到互聯網。互聯性的興起導致先前互不相連的系統與IT網路融合，但IT網路的設計初衷並不是以同樣的方式進行連接和管理。隨著數位轉型的快速發展，安全團隊對這些新互連的CPS環境的獨特挑戰缺乏認知和理解。如果HDO沒有專門的安全團隊或跨各個利害關係人推動的資產管理職責，就因缺乏統一的治理和控制措施而遭受損失。為了解決這個問題，HDO應該評估能夠提供所有設備可視性、集成現有的IT工具和工作流程的CPS安全供應商，並透過統一的安全治理和推動網路和營運彈性過程中的所有用例，幫助將IT控制擴展到CPS。

CLAROTY

Cyberworld

透過五大核心控制措施來評估CPS安全供應商

CLAROTY

Cyberworld

核心控制措施

資產發現

對於設備所有者來說，維護最新的資產庫存記錄和管理大量臨床設備是一項耗時的手動任務。如果HDO沒有準確的庫存記錄，就難以管理日常工作流程，並難以做出全面的設備生命週期管理決策。若HDO繼續依賴手動資料輸入來追蹤預防性維護與保持其環境中每台設備的合規性，就會效率低下，以及不支援他們期待實現的即時互聯的健康模式。

風險管理

僅僅發現漏洞是不夠的，您還需要評估受影響資產的情況、以及對您營運的潛在影響，確定風險的優先順序並進行補救。為了建立真正有效的風險管理計劃，應考慮採用多種資料收集方法，而不僅僅是被動收集方法，以便更動態地實現醫療設備資產可視性和風險管理。建立風險管理的第一步是安全且高效地分析設備，考慮潛在風險對營運的影響和可利用性，驗證風險，最後採取可行的補救措施，以降低風險並確保營運安全。

評估標準

- 提供有關IP位址、序號、作業系統和製造商的高級詳細信息。
- 提供動態庫存調節以追蹤設備的實體位置，從而簡化操作流程並降低風險。
- 提供可自訂的儀表板和深入的分析。
- 透過CMMS/CMDB集成，簡化設備和生命週期管理工作流程。

- 讓HDO能夠完全自訂計算風險的可能性、影響和補償控制機制。
- 採用多種發現方法來識別和分析網路上的所有CPS，映射您的通訊路徑和協議使用情況、屬性漏洞並監察威脅。
- 提供可行的建議，讓使用者能夠根據量化結果確定修復工作的優先順序。
- 提供報告和儀表板，以審查安全態勢的有效性和改進情況。

CLAROTY

Cyberworld

核心控制措施

網路防護

在醫療保健領域，想有效地分割網路可能是一個繁瑣且容易出錯的過程，需要根據您的獨特環境定義並不斷調整策略。此外，內部監察和遵守監管是一個具有挑戰性的任務，這需要細粒度、經過適當調整的策略，而許多HDO是缺乏的。如果沒有準確的設備詳細信息和行為基準，就難以管理設備網路行為。

威脅偵測

傳統的解決方案缺乏所需的網路覆蓋深度，無法正確識別、評估和優先處理醫療網路中CPS所面臨的威脅。HDO往往不完全瞭解其臨床環境，無法發現全部威脅。由於環境的複雜性、不斷擴大的CPS攻擊面、其營運的關鍵性質、以及不容忍中斷病人護理，HDO逐漸成為網路犯罪分子的攻擊目標。

評估標準

- 提供由數十位分析師多年來研究環境中數百萬台設備而製定的建議分段策略，這些策略可透過現有的基礎設施輕鬆且自動地實施。
- 實現持續監察，瞭解設備在正常情況下如何通訊，對任何違反策略的行為自動發出警報。
- 透過嚴格控制、監察和保護遠端會話，確保支援所有醫療保健用例。
- 支援與NAC、FW和EDR的深度集成，以確保執行。

- 提供多個偵測引擎，自動分析醫療保健網路中的所有設備、通訊和流程。
- 深入瞭解臨床環境中複雜的、非標準的IT工作流程及其內部多種設備，以簡化警報並幫助優化優先順序和回應。
- 提供一系列威脅偵測功能，可與您現有的技術堆疊無縫集成，從而縮小IT與醫療保健專業知識的差距。

CLAROTY

Cyberworld

核心控制措施

營運效率

臨床工程團隊依賴能夠高效操作的設備來支援病人護理。但很多時候，當需要照顧病患時，設備可能被移動或難以找到，導致耗費時間斷開連接。用於裝載設備、管理其生命週期以及在需要預防性維護時定位設備的手動例程也很耗時，導致資料不足和不準確。此外，更好地瞭解現有資產的利用率，避免在沒有所需更新或服務的情況下運行不受支援、報廢或不合規的設備。

評估標準

- 與資產管理系統集成，幫助您的臨床工程團隊和安全團隊精確地支援和保護設備。
- 透過提供自動化營運效率和風險建議，降低病人護理的風險。
- 提供有關設備位置和利用率的信息。
- 提出提高效率和優化ROI的行動建議。

CLAROTY

Cyberworld

隨著威脅情勢不斷變化和新攻擊媒介的出現，網路犯罪分子的攻擊手段也越來越高明。為了保護您的醫療保健環境，與滿足您獨特需求的CPS安全供應商合作至關重要。那麼，首先要瞭解選擇CPS安全供應商的評估標準。無論您處於網路安全之旅的任何階段，合適的供應商應該具備上述核心控制措施，還要支援所有用例。

Claroty透過提供對現代醫療保健網路各個部分的、無與倫比的可視性來實現這一點，並為整個CPS安全旅程中的所有用例提供支援。Claroty致力於透過屢獲殊榮的研究團隊和公共部門的參與來推動進步，其產品旨在為客戶提供更強大的保護，抵禦最嚴峻的威脅。Claroty還獲得頂尖的臨床設備供應商的認可，這些供應商透過Claroty的產品為自己的客戶提供支援，這表明他們不僅對Claroty產品組合的創新、成熟度與持久性充滿信心，而且對Claroty的使命、願景和深厚的領域專業知識充分信任。對於HDO，選擇合適的CPS安全供應商不是一件容易的事情。因此，Claroty撰寫了本指南，幫助HDO尋找合適的CPS安全供應商，從而有效地保護關鍵的OT、IoT、IoMT和整個XIoT生態系統。

[1] https://www.proofpoint.com/us/resources/threat-reports/ponemon-healthcare-cybersecurity-report
[2] https://www.ic3.gov/Media/News/2022/220912.pdf
[3] https://www.aha.org/news/headline/2024-02-29-study-nist-framework-associated-lower-cyber-insurance-premiums
[4] https://claroty.com/resources/reports/the-global-healthcare-cybersecurity-study-2023
[5] https://elitebiomedicalsolutions.com/resources/blog/biomed-tech-shortage-how-it-impacts-hospitals/
[6] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

關於Claroty

Claroty憑藉無與倫比的、以產業為中心的平台重新定義了網路實體系統(CPS)防護，該平台旨在保護關鍵基礎設施。Claroty平台提供市場上最深入的資產可視性和最廣泛的CPS安全解決方案，包括風險管理、網路防護、安全存取和威脅偵測，可搭配 Claroty xDome 在雲端使用，也可以搭配 Claroty CTD 在地端部署使用。Claroty平台以屢獲殊榮的威脅研究和技術聯盟為後盾，讓企業能夠有效地降低CPS風險，以最快的時間實現價值並降低整體擁有成本。在全球範圍內，已有數百家企業在數千個站台部署了Claroty。Claroty總部位於紐約，業務遍及歐洲、亞太地區和拉丁美洲。

大中華區總代理
網址 www.cyberworld.com.tw
電話 +886-2-7724-8320
電郵 info@cyberworld.com.tw