CLAROTY

從OT到CPS，工控安全再進化

Jason 詹鴻基

Claroty 大中華區技術顧問

CISSP® Certified Information Systems Security Professional

CEH™ Certified Ethical Hacker

Claroty At-A-Glance

為企業組織中提供所有網路物理系統(CPS)無與倫比的安全性

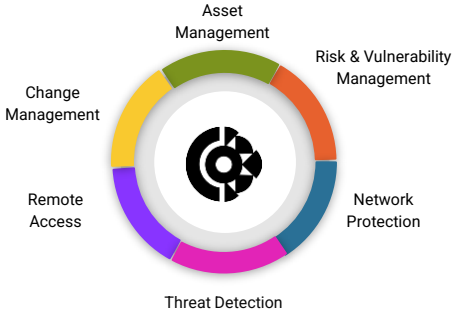
HQ: **NYC**	Founded: **2015**	Funding: **$735M (Series E)**	Customers: **600+**

深厚的領域專業知識

The Extended Internet of Things (XIoT)

Industrial **Commercial** **Healthcare**

綜合能力



全球採用

100s of Orgs, 1000s of Sites, 50+ Countries, 25+ Verticals

投資者

Rockwell Automation · GM · Bessemer Venture Partners · Schneider Electric · BMW · TEMASEK · SIEMENS · IQT IN-Q-TEL · TEAM8

來自領先行業分析公司其他受信任的第三方的驗證與堅強的情資研究團隊

DEVELOPMENTAL TESTING AND EVALUATION DESIGNATION — SAFETY ACT — SAFETY AND TECHNOLOGY

FORRESTER WAVE LEADER 2021 — Industrial Control Systems (ICS) Security Solutions

500 Technology Fast 500 2021 NORTH AMERICA Deloitte.

CLAROTY — Claroty Named a Leader in 2025 Gartner® Magic Quadrant™ for CPS Protection Platforms — Positioned Highest for Ability to Execute and Furthest for Completeness of Vision — Source: Gartner

2021 CYBERSECasia READERS' CHOICE AWARDS

SC 2021 awards EUROPE WINNER

BEST IN KLAS 2025 — HEALTHCARE IoT SECURITY

T82 THE CLAROTY RESEARCH TEAM

收集完整的Log後透過SOC平台來撰寫規則針對有問題的行為或是威脅進行阻擋

實體隔離設備都不連網，哪裡會被打?

建立所有設備的MAC地址，使用NAC確保合規設備才能接入場內

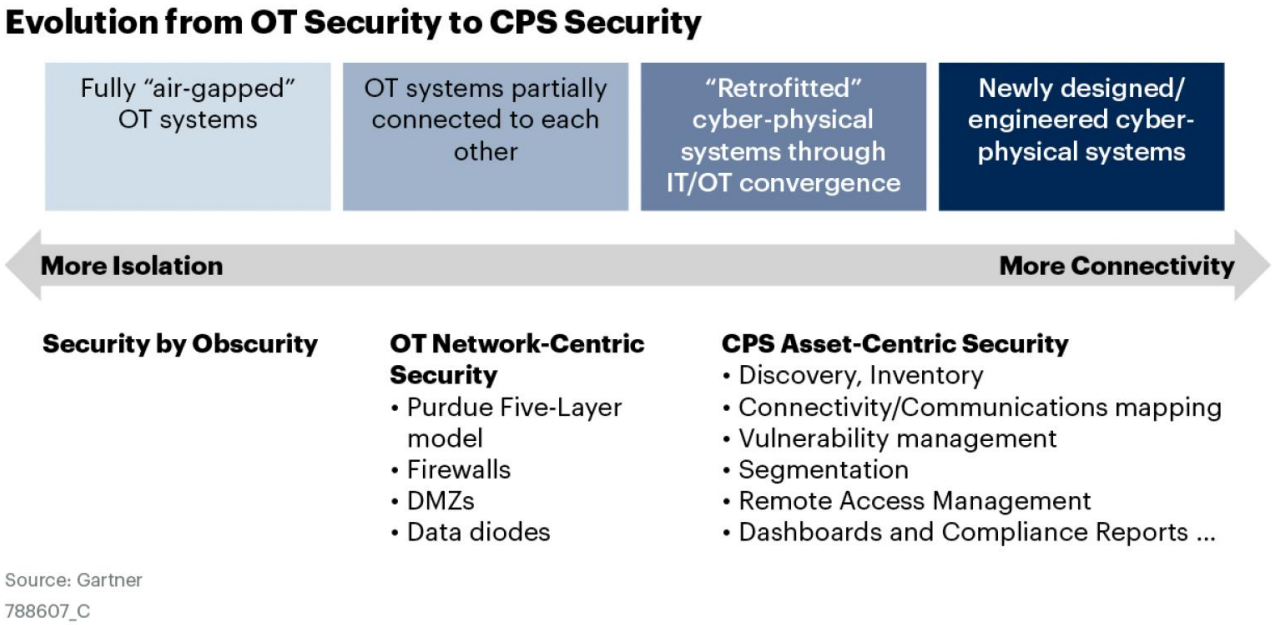
所有進場設備都要使用掃毒USB掃過一次確認沒有病毒後，透過安全機制.....

確保沒有對外連線，啟用防火牆控管保護連線....盤點工控設備通訊白名單....

.....好像都對

CLAROTY

Why CPS Security



2023 Guide for CPS Protection Platforms

CPS保護平台被認為能提升企業安全策略，提供跨平台的終端安全，並針對最新的網路攻擊進行防禦

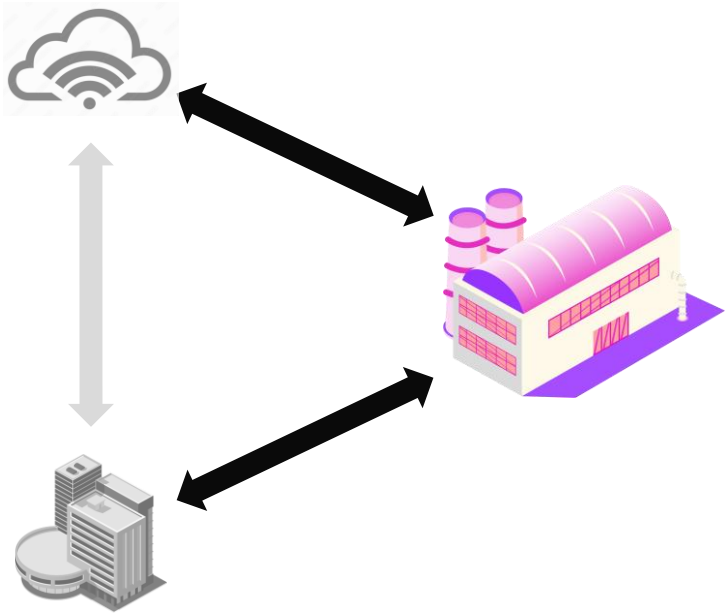
2025 Gartner® Magic Quadrant™ for CPS PP

Claroty被評為2025年Gartner®魔術象限™ CPS保護平台的領導：

- 執行能力方面表現最高
- 願景的完整性看得最遠

Additionally, based on 122 reviews from 2024 in the CPS Protection Platforms category, **Claroty has a 96% Would Recommend rating** on the Gartner Peer Insights™ website

網路攻擊造成的干擾從未停止



2023 — **Dole Foods Ransomware Attack**

Ransomware caused global fresh product producer to shutdown four NA production sites, delayed shipments up to two weeks.

2023 — **SAF Holland Ransomed by BlackCat**

Ransomware interrupted production for a large vehicle manufacturer in Germany, impacting two sites, causing a 3-month production backlog.

2021 — **Colonial Pipeline**

Largest publicly disclosed cyberattack against critical infrastructure in the U.S. involving Colonial Pipeline's IT systems.

2021 — **JBS Ransomware Attack**

A Brazil-based meat processing company, suffered a cyber attack, disabling its beef and pork slaughterhouses.

2020 — **MTA Cyberattack**

Chinese hackers exploited a zero day vulnerability to hack the company VPN resulting in a breach of MTA's computer systems.

2020 — **Lion Cyberattack**

Ransomware attack disrupts production at an Australian food and beverage company after infecting IT systems.

這張圖展現出什麼可能的問題?

誰在Modem的後方嘗試連入?

當前CPS Cybersecurity可能的疏漏現況

利用傳統IT解決方案

通常與OT系統不相容

可能會造成營運風險導致躊躇不前

單一且過時的資產發現方式

需要額外的硬體與介入

提供不完整的資產清單盤點

缺乏可行性的洞察視角

脆弱基礎的CPS安全

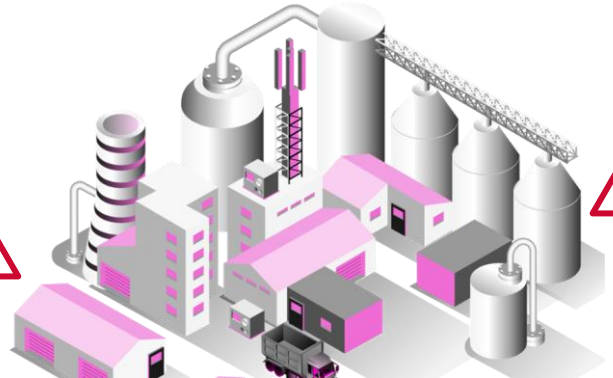
無法落實

單點方案手動組合

不同的解決方案

需要花費大量人力進行整合與維護

單點產品可能會造成安全盲點



CLAROTY

CISO CPS security pain points

- **Operational Resilience:** CISO需要確保其組織能夠有效應對CPS網路安全事件，制定應變手冊並與戰略規劃保持一致是關鍵
- **The Sprawling Tech Stack:** 管理混合的舊有本地系統和新雲端/SaaS技術對CISO來說可能充滿挑戰，更不用說xIoT、工業控制系統和CPS的複雜性，這些通常不在他們的專業領域
- **Evolving Threats and Compliance Requirements:** 跟上迅速變化的威脅和合規標準是必要的，尤需理解資訊技術與CPS之間的橫向移動
- **Talent Shortages:** 尋找具有技能的網路安全專業人士依然是一個持續的挑戰
- **Adopting New Technology:** 在維持安全的同時平衡採用創新技術是一項微妙的任務。證明工具的商業價值以實現投資回報和風險水平降低是關鍵.
- **Championing Change:** CISOs 必須在整個組織中倡導安全改進，克服對變革的抵制，並採用更強的IT/OT合作
- **CPS Secure Access:** 透過零信任存取減少風險，為內部和第三方用戶提供無摩擦、可靠且高度安全的CPS環境遠程訪問

OT/CPS環境需要不同的策略

	IT Environments	OT Environments
	IT Systems (servers, laptops, etc)	Cyber-physical systems (OT, BAS, IoT)
	**Confidentiality, Integrity, Availability**	**Safety, Reliability, Productivity**
	Standard protocols and device types	Proprietary protocols and diverse assets
	Standard security controls apply	Operational context drives security
	Compatible with most security solutions	Incompatible with most security solutions

安全措施

非一體適用

CLAROTY

建議的OT/CPS網路安全旅程

aka OT/CPS減傷

駭客/威脅

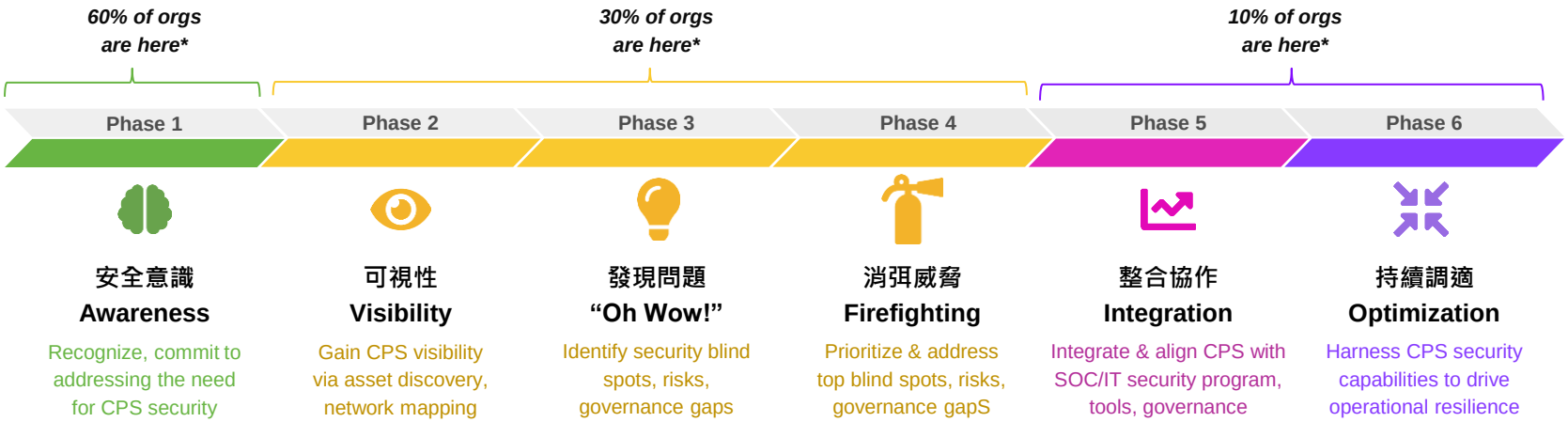
資產強度

端點防護

防火牆/邊界控管

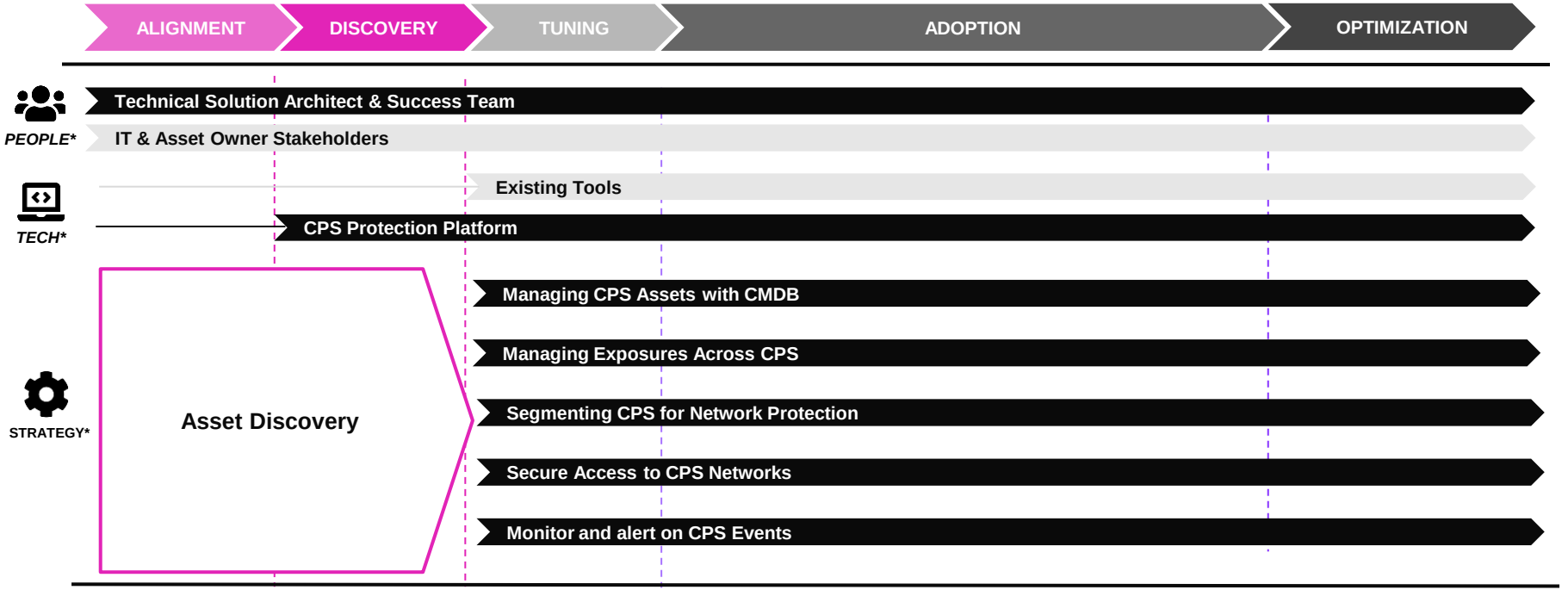
圖片出處 : @jim_toy_dream2021

CPS安全旅程從何開始?



[1]*Source: Market Guide for Operational Technology Security, Gartner, 2021*

The CPS Journey with Claroty



The Approach to CPS Cybersecurity

1. **獲取完整可視性 (盤點)**
   Gain Full Visibility into all CPS in your OT Environment

+

2. **整合現有的技術堆疊與工作流程 (分類)**
   Integrate with your Existing Tech Stack & Workflows

+

3. **延伸現有的IT安全控管至OT環境 (保護)**
   Extend your IT Security Controls to your OT Environment

CPS 曝險管理

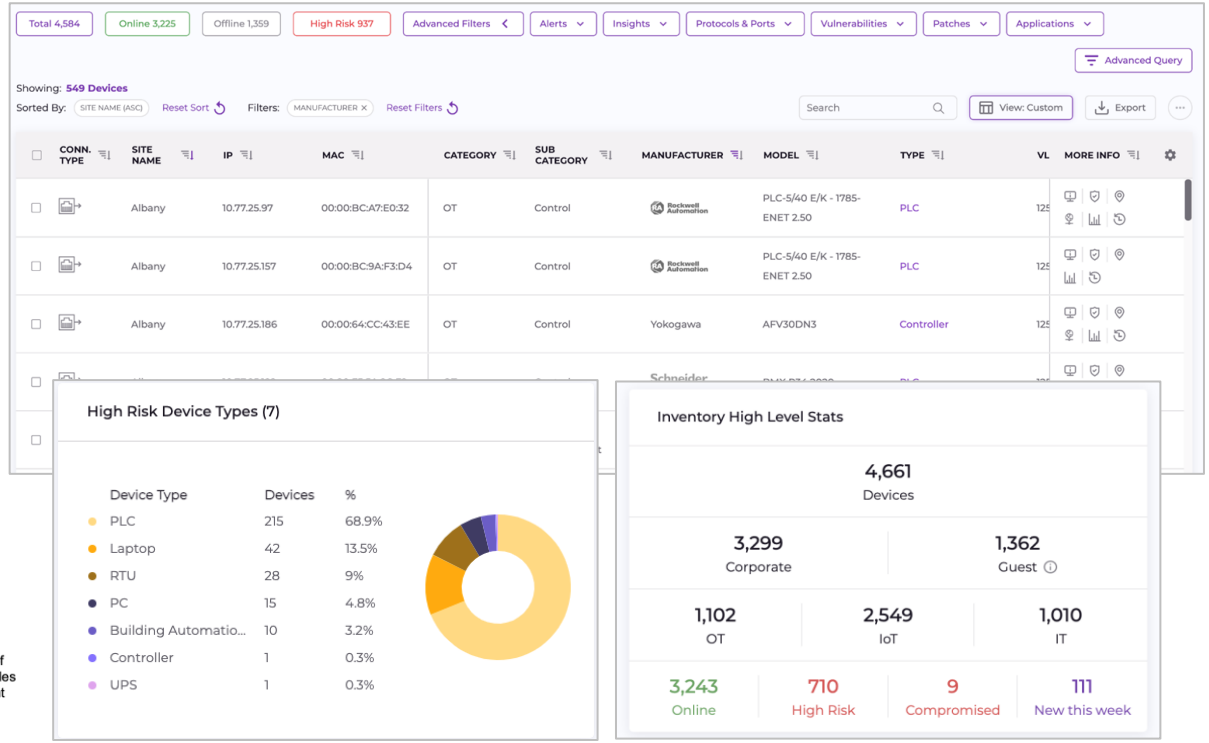
資產探索與發現

自動靈活的XIoT資產發現大幅度降低部署時間和避免傳統手動盤查的複雜度

業界最全面且具備領先的領域專業知識實現**全面可視性**，除了傳統流量識別也支援離線盤點

資產管理整合快速鑑別企業範圍內的**資產數量類型以及風險綜合評估**

支持 **450 種以上**的裝置通信協定，確保安全成熟度所需的全面深度可見性



Passive Monitoring
Continuous Monitoring of network traffic to identify asset profiles

Safe Queries
Targeted discovery of assets in their native protocol

Claroty Edge
Speedy, host-based asset profiling through localized queries

Project File Analysis
Regular ingestion of offline configuration files for asset enrichment

CLAROTY

Surprising CPS Risk Exposure facts !

Is Digital Transformation Accelerating?

83B

By 2024, there will be **83 BILLION IoT connections** — and 70% will be in critical infrastructure sectors[1].

70%

By 2026, 70% of new industrial CPS purchased will include *intelligent* design features[2].

Are traditional methods to managing Risk working?

70%

Last year, 70% of new CPS common vulnerabilities & exposures (CVEs) received *high* or *critical* CVSS scores, yet less than 8% were exploited[5].

4%

On average, traditional, CVSS-led methods for prioritizing vulnerabilities are less than **4%** efficient — meaning that 96% of resources are wasted[6].

CLAROTY

[1]*The Global Healthcare Cybersecurity Study 2023, Claroty*
[2]*Claroty Install Base Data Analysis*

傳統 OT 漏洞管理的問題

20 Million Assets

~75% Rest of assets

23% Prioritize with CVSS (Traditional VM)

具有不安全的互聯網連接且至少存在一個已知被利用漏洞 Known Exploited Vulnerability (KEV)的高風險資產 **1.3%**

在分析的 2000 萬資產中，這**“盲點”**代表數以萬計的**高度可利用、但經常被忽視**的資產

43%

其中有43%的資產是高風險但沒CVSS分數的資產[1]

漏洞管理“盲點”

57%

其中有57%的資產是具有critical CVSS分數的高風險資產[1]

CLAROTY

[1]CVSS v3.1 score of 9.0 or higher

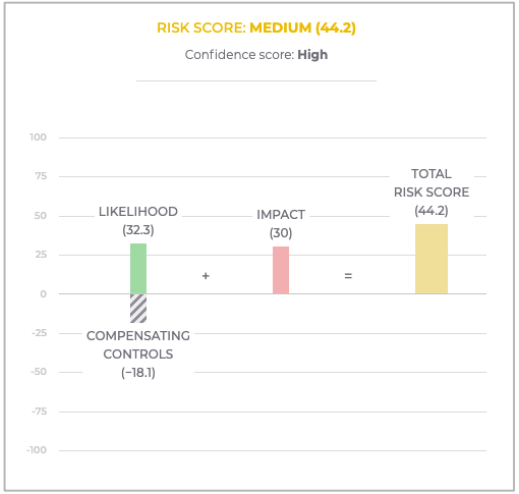
縮小漏洞暴露範圍以集中注意力

Data enrichment from CISA's Known Exploited Vulnerabilities (KEV) catalog and the Exploit Prediction Scoring System (EPSS) should **provide additional context into a vulnerability's usage or exploitability**.

理解風險與優先順序

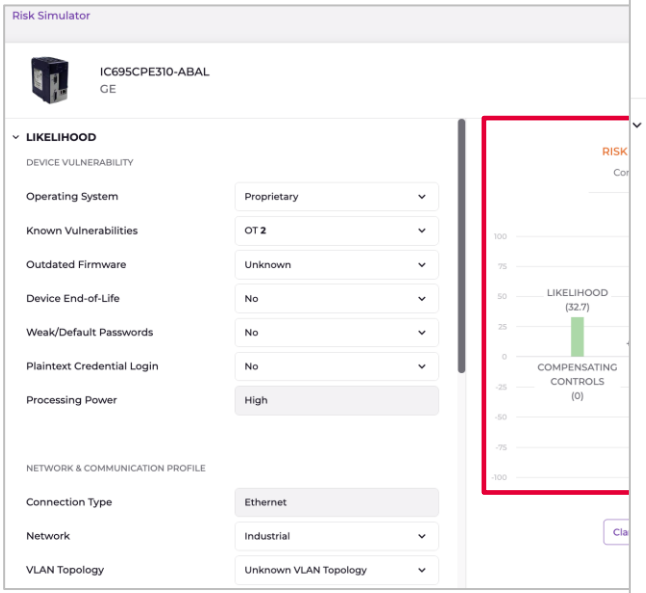
Creating a risk profile that accounts for CPS realities

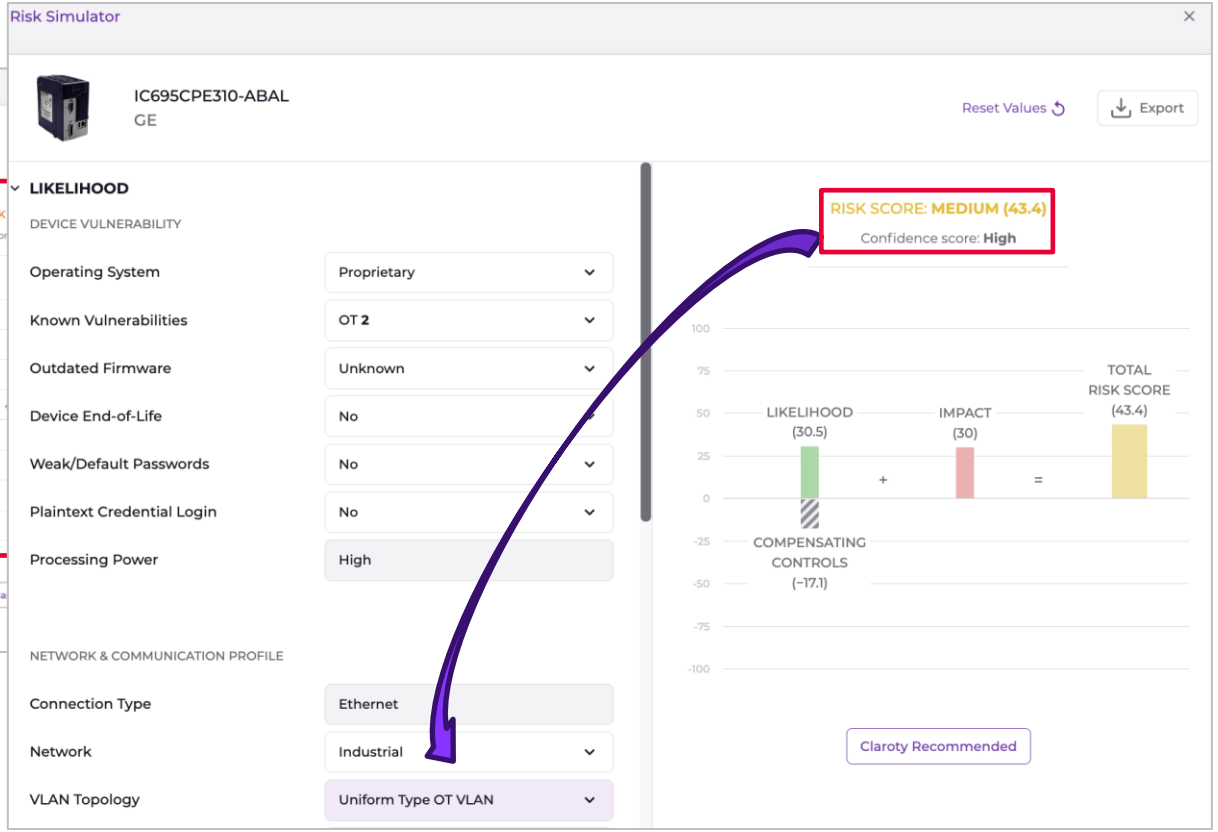
Likelihood		Compensating Controls	Impact
Network Factors	**Risk Factors**		
VLAN topology	Outdated firmware	Overall enforcement level	Equipment class
Internet comms	Operating system	Management method	Consequence of failure
Connection type	End-of-Life	Endpoint security	OT criticality
Network	Weak/default passwords	Network controls	Purpose
Unsecured protocol	Vulnerabilities	Custom controls	Business impact
Expired TLS	Plaintext credentials		



CPS 的網路風險評分應該比傳統IT 評分機制
更加具體和具有上下文關聯

風險管理

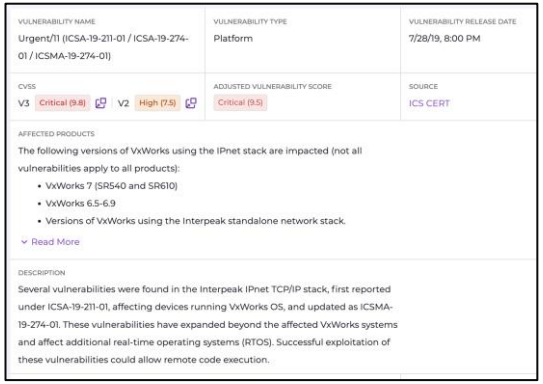




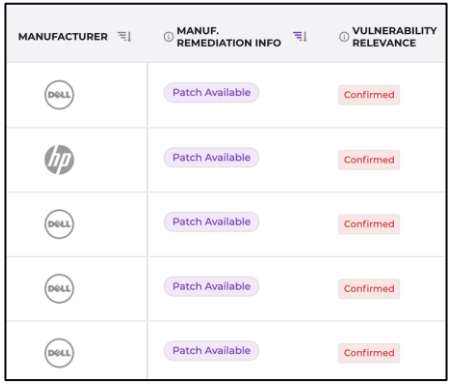
風險模擬器確認資產風險，針對資產類型提供明確方式降低風險

驗證與施作以減少曝露風險
Asset and Network-Centric Examples

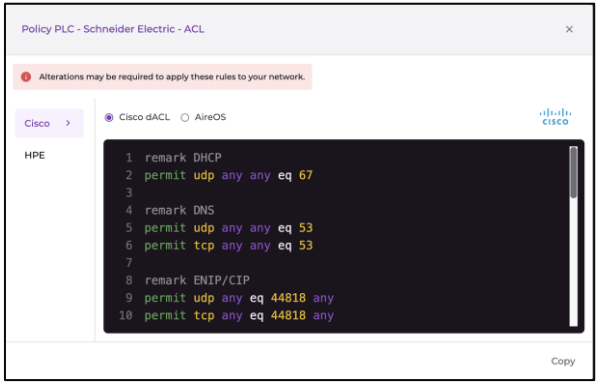
Asset-Centric Hardening



Asset Patching

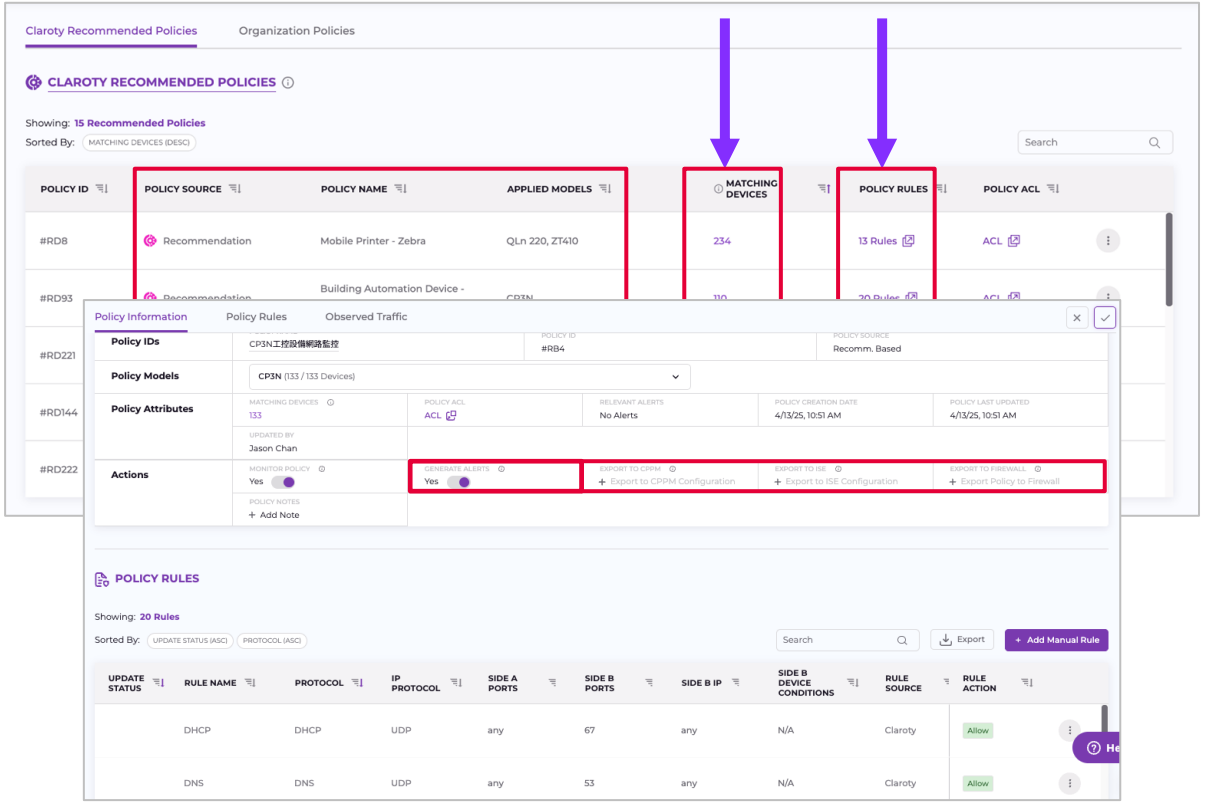


Network-Centric Hardening



虛擬網路防火牆

- Clarory內建的定義策略快速協助客戶進行網路分割
- 輕鬆自定義資產通信策略以快速檢測**未經授權**的活動
- 通過現有基礎設施進行細化策略，進行有效威脅遏止
- 監控**監管和組織**合規措施



填問卷換贈品