

從OT到CPS，工控安全再進化

Jason 詹鴻基

Claroty 大中華區技術顧問



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)

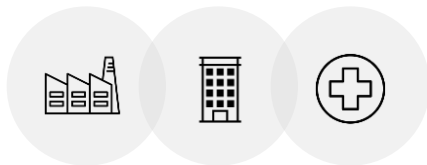
Customers: 600+

深厚的領域專業知識

綜合能力

全球採用

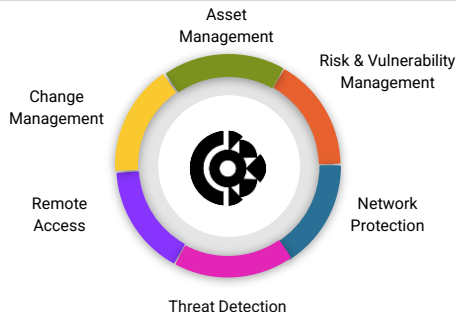
The Extended Internet of Things (XIoT)



Industrial

Commercial

Healthcare



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



投資者

Rockwell
Automation



Bessemer
Venture
Partners

Schneider
Electric



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

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.....

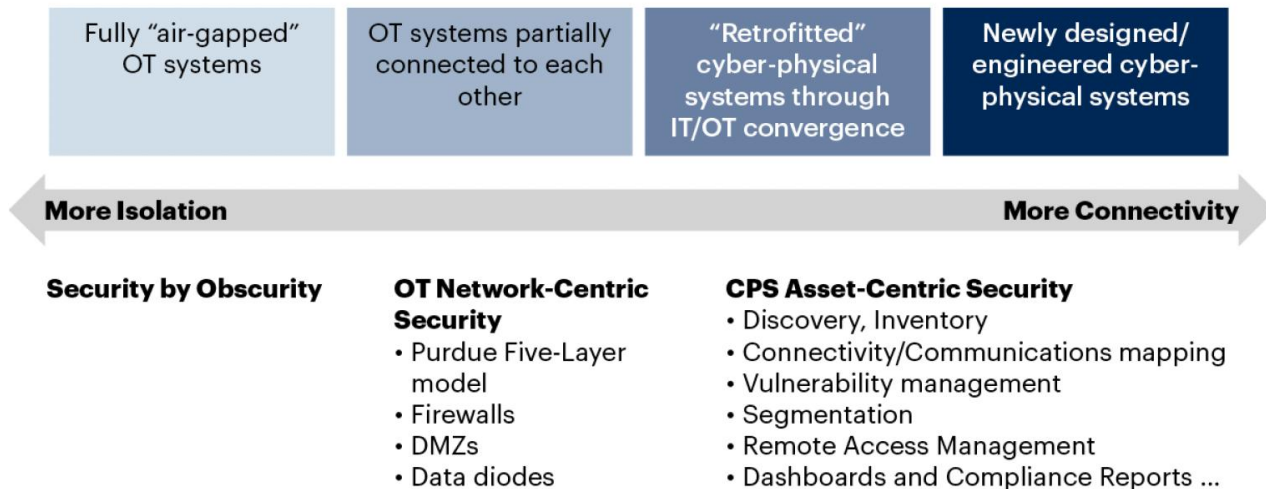
確保沒有對外連線，啟用防火牆控管保護連線....盤點工控設備通訊白名單....

.....好像都對



Why CPS Security

Evolution from OT Security to CPS Security



Source: Gartner
788607_C

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

Gartner

2025 Gartner® Magic Quadrant™ for CPS PP

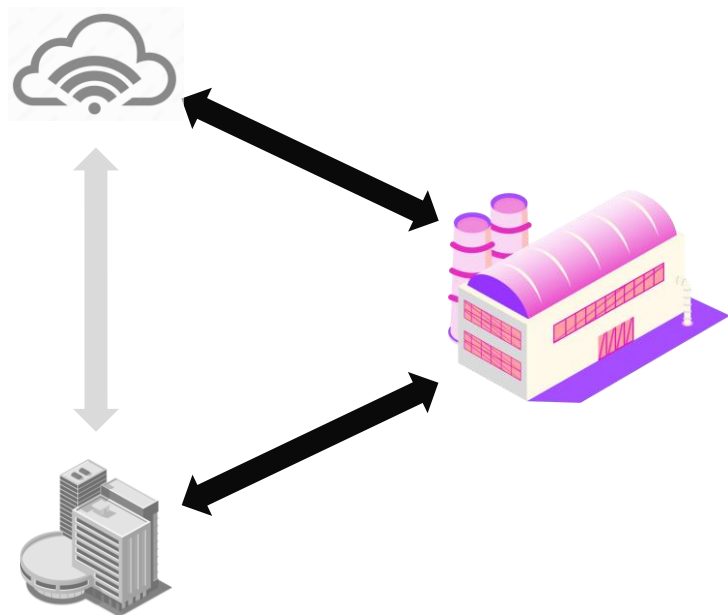
Claroty被評為2025年Gartner®魔術象限™
CPS保護平台的領導：

- 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?

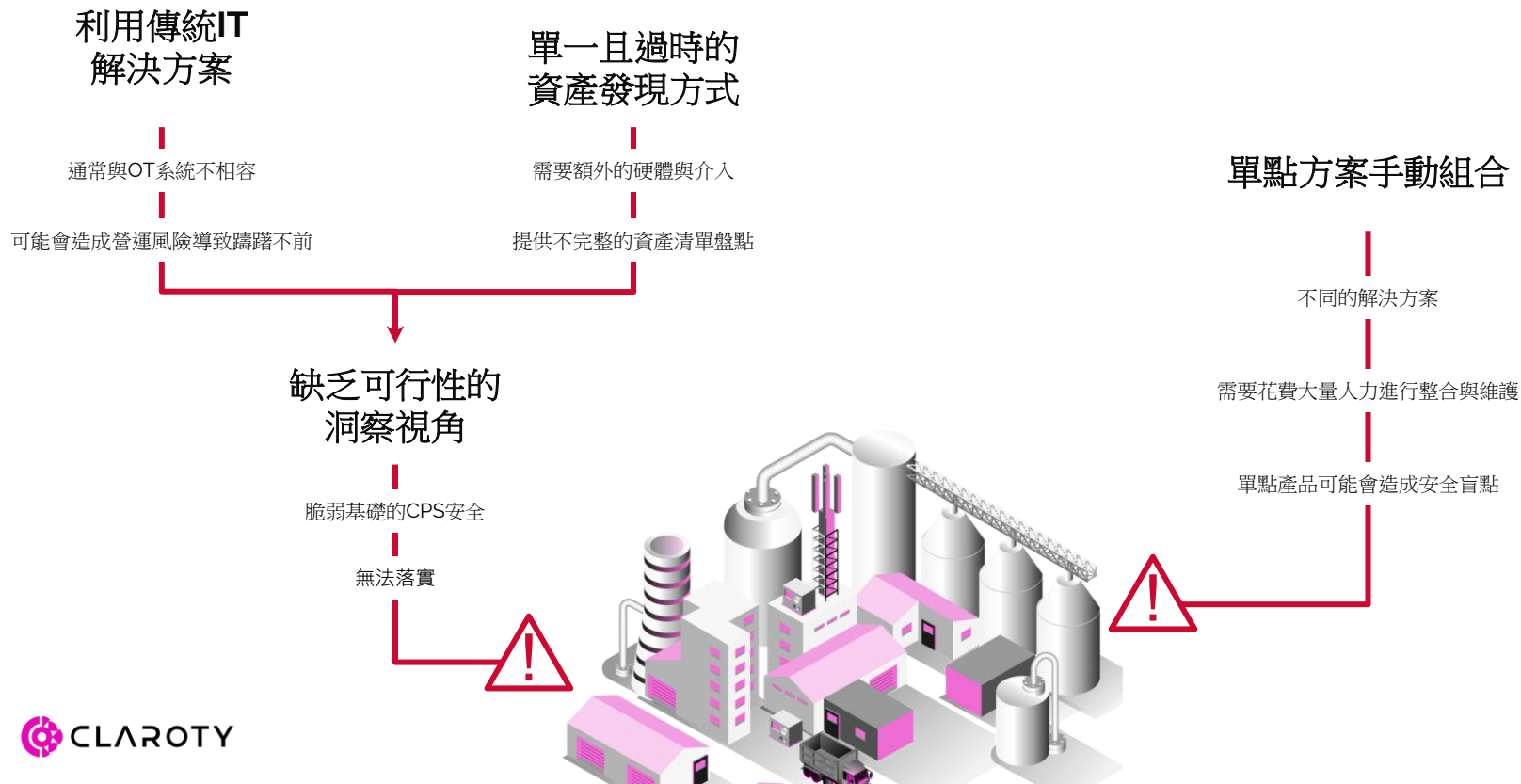
Siemens Scalance
IT-OT shopfloor
switch

Modem

誰在**Modem**
的後方嘗試
連入?



當前CPS Cybersecurity可能的疏漏現況



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



IT Systems (servers, laptops, etc)



Confidentiality, Integrity, Availability



Standard protocols and device types



Standard security controls apply



Compatible with most security solutions

OT Environments

Cyber-physical systems (OT, BAS, IoT)

Safety, Reliability, Productivity

Proprietary protocols and diverse assets

Operational context drives security

Incompatible with most security solutions

安全措施

非一體適用

IT

OT

Security

Security

IoT

Security

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

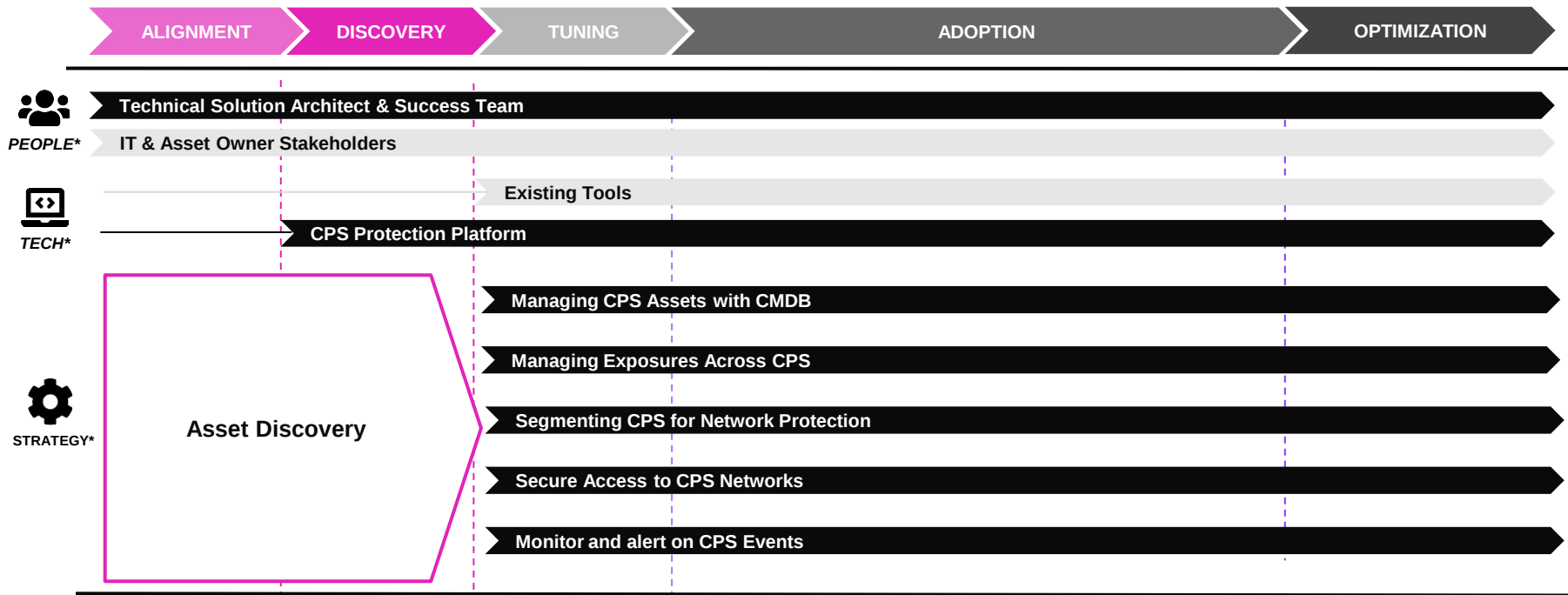
防火牆/邊界控管

CPS安全旅程從何開始？



¹Source: 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

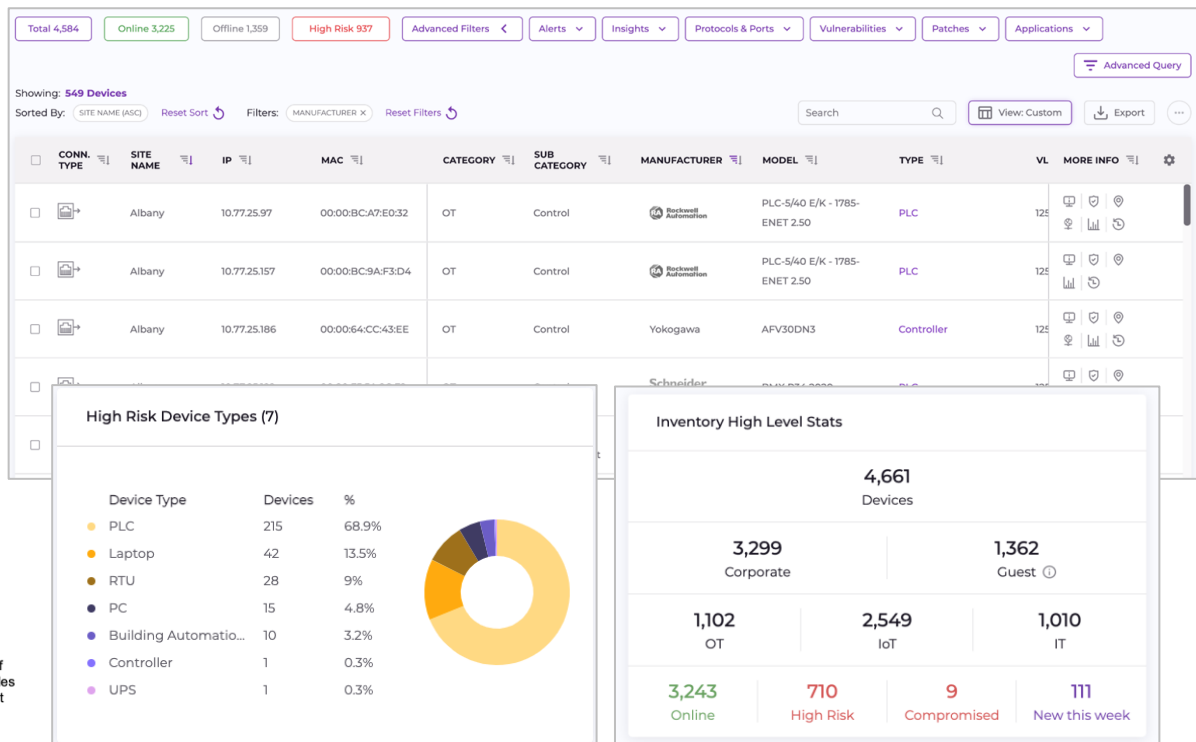
資產探索與發現

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



Clarity Edge

Speedy, host-based asset profiling through localized queries



Project File Analysis

Regular ingestion of offline configuration files for asset enrichment

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 sectors¹.

70%

By 2026, **70%** of new industrial CPS purchased will include *intelligent* design features².

Are traditional methods to managing Risk working?

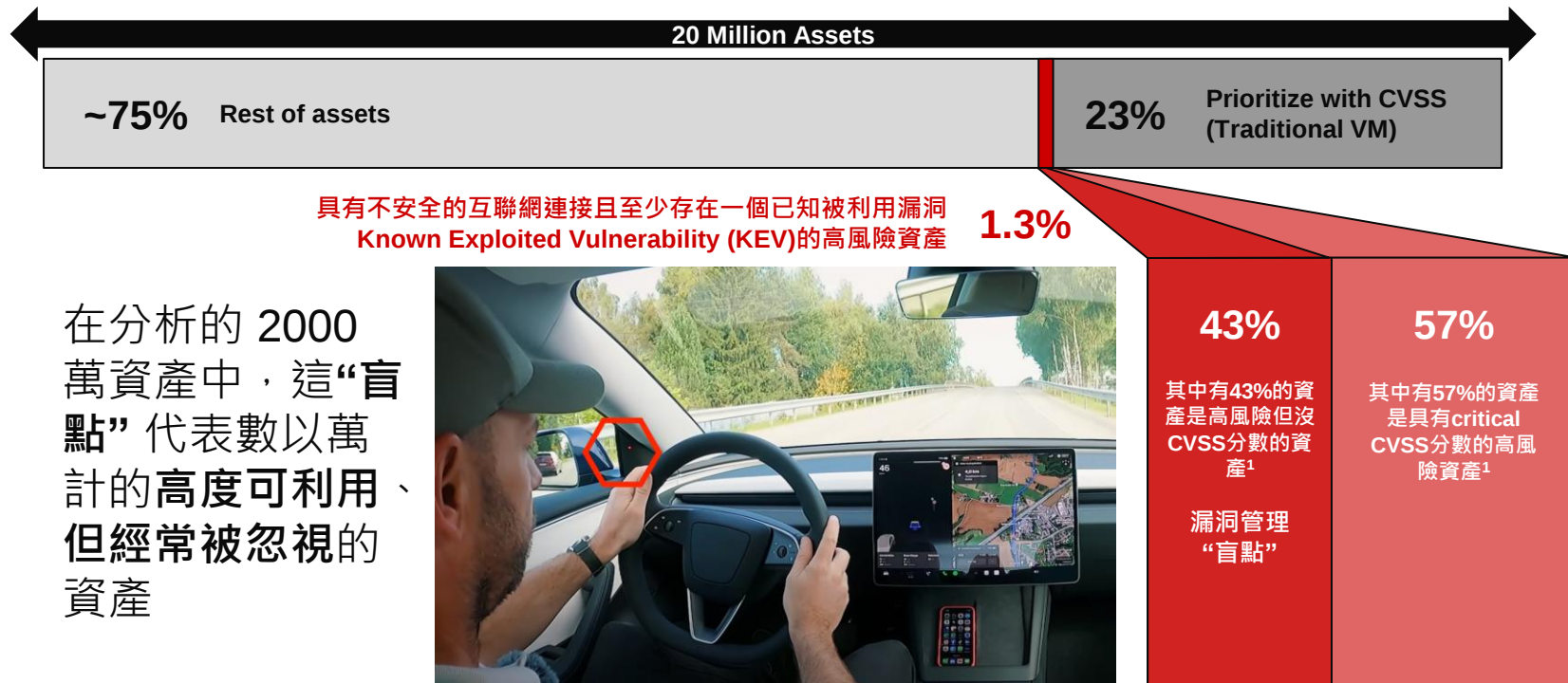
70%

Last year, **70%** of new CPS common vulnerabilities & exposures (CVEs) received *high* or *critical* CVSS scores, yet less than 8% were exploited⁵.

4%

On average, traditional, CVSS-led methods for prioritizing vulnerabilities are less than **4%** efficient — meaning that 96% of resources are wasted⁶.

傳統 OT 漏洞管理的問題



縮小漏洞暴露範圍以集中注意力

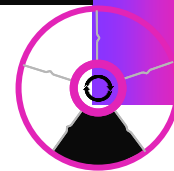
The screenshot displays a vulnerability management dashboard. At the top, a summary bar shows: Total 113,379, Relevant 378, Actively Exploited 1,074, and Remediable 195. Below this, the main view shows 40 vulnerabilities, 239 CVEs, and 3,426 device-vulnerability pairs. The interface includes sorting options (Vulnerability Priority Group (ASC)) and filters (Affected Devices, Manufacturer Remediable Devices, Actively Exploited). A detailed view of vulnerabilities is shown below, including CVE-2021-34527, CVE-2020-0787, and CVE-2021-1675. A green box highlights the 'Actively Exploited' status and the 'EPSS Score' column in the detailed view.

Vulnerability Name	Vulnerability Type	CVEs	CVSS V3 Base Score	Adjusted Vulnerability Score	Actively Exploited	EPSS Score	Vulnerability Priority Group
CVE-2021-34527	Platform	CVE-2021-34527	High (8.8)	Critical (9.1)	Actively Exploited	96.7%	Priority Group 1
2 CVEs	High (8.2)	Critical (9.1)	The Microsoft Windows Print Spooler service fails to restrict access to the RpcAddPrinterDriverEx...	Actively Exploited	96.8%	Priority Group 1	
CVE-2020-0787	High (7.8)	High (8.7)	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer...	Actively Exploited	1.1%	Priority Group 1	
CVE-2021-1675	High (8.8)	High (8.7)	CVE-2021-1675 - Windows Print Spooler Remote Code Execution	Actively Exploited	96.8%	Priority Group 1	

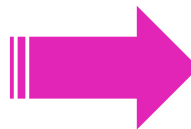
Data enrichment from CISA's Known Exploited Vulnerabilities (KEV) catalog and the Exploit Prediction Scoring System (EPSS) should **provide additional context into a vulnerability's usage or exploitability.**

理解風險與優先順序

Creating a risk profile that accounts for CPS realities

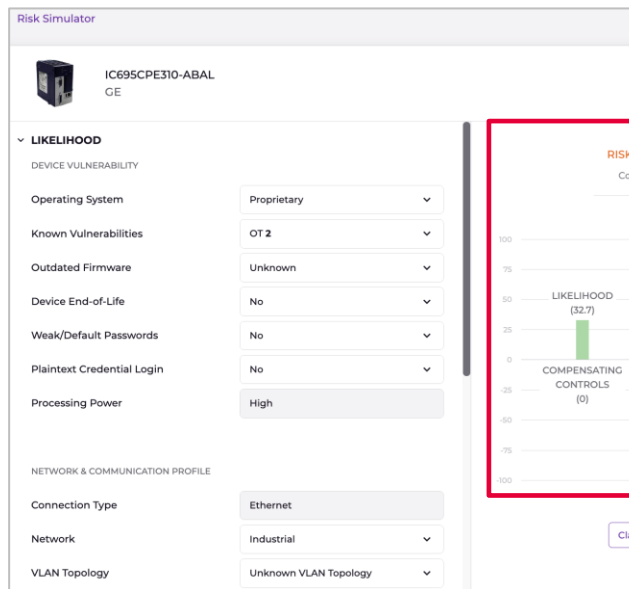


Likelihood		Compensating Controls	Impact
Network Factors	Risk Factors		
VLAN topology	Outdated firmware	Overall enforcement level	Equipment class
Internet comms	Operating system	Management method	Consequence of failure
Connection type	End-of-Life	Endpoint security	OT criticality
Network	Weak/default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

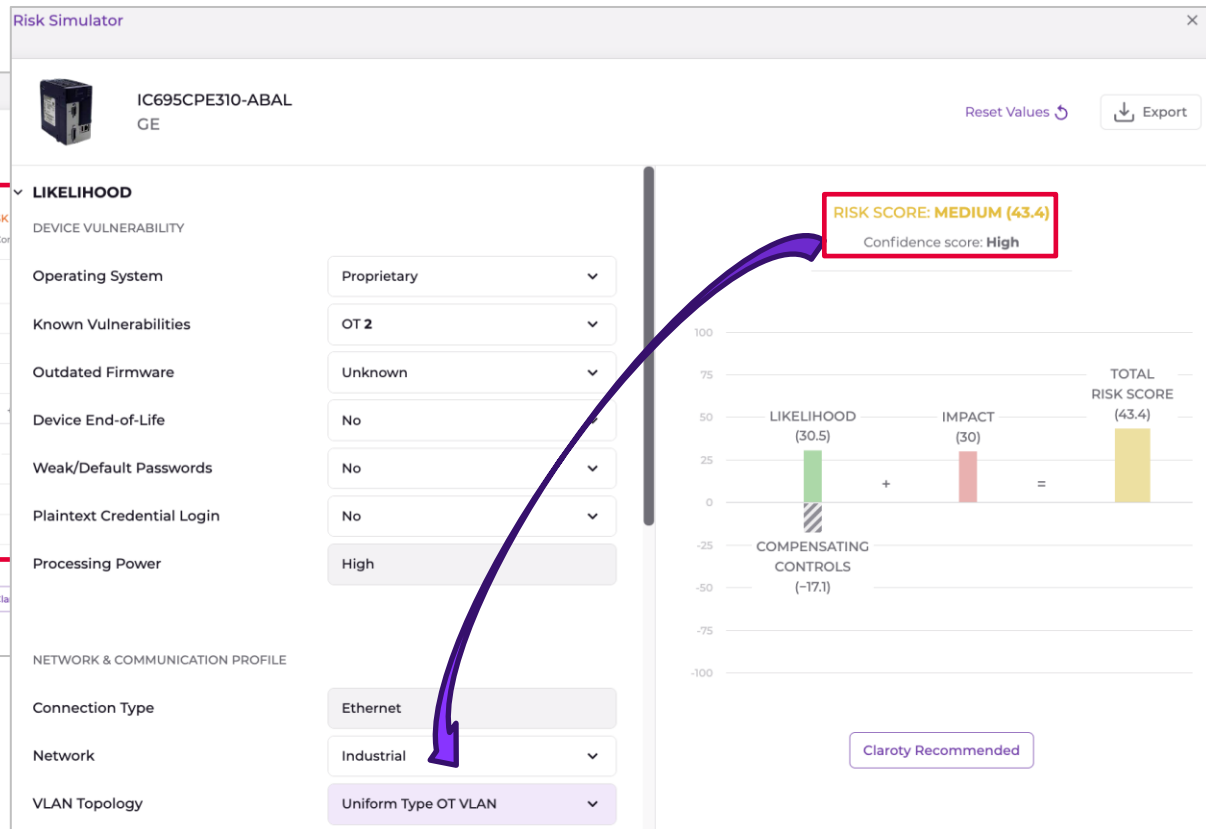


CPS 的網路風險評分應該比傳統IT 評分機制
更加具體和具有上下文關聯

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

VULNERABILITY NAME Urgent/11 (ICSA-19-271-01 / ICSA-19-274-01 / ICSCMA-19-274-01)	VULNERABILITY TYPE Platform	VULNERABILITY RELEASE DATE 7/28/19, 8:00 PM
CVSS V3 Critical (9.8) V2 High (7.5)	ADJUSTED VULNERABILITY SCORE Critical (9.5)	SOURCE ICS CERT
AFFECTED PRODUCTS The following versions of VxWorks using the IPNet stack are impacted (not all vulnerabilities apply to all products): - VxWorks 7 (SR540 and SR610) - VxWorks 6.5-6.9 - Versions of VxWorks using the Interpeak standalone network stack. Read More		
DESCRIPTION Several vulnerabilities were found in the Interpeak IPNet TCP/IP stack, first reported under ICSA-19-271-01, affecting devices running VxWorks OS, and updated as ICSCMA-19-274-01. These vulnerabilities have expanded beyond the affected VxWorks systems and affect additional real-time operating systems (RTOS). Successful exploitation of these vulnerabilities could allow remote code execution.		



Asset Patching

MANUFACTURER	MANUF. REMEDIATION INFO	VULNERABILITY RELEVANCE
D6LL	Patch Available	Confirmed
hp	Patch Available	Confirmed
D6LL	Patch Available	Confirmed
D6LL	Patch Available	Confirmed
D6LL	Patch Available	Confirmed



Network-Centric Hardening

Policy PLC - Schneider Electric - ACL	
Alterations may be required to apply these rules to your network.	
Cisco >	Cisco dACL AircOS
HPE	<pre>1 remark DHCP 2 permit udp any any eq 67 3 4 remark DNS 5 permit udp any any eq 53 6 permit tcp any any eq 53 7 8 remark ENIP/CIP 9 permit udp any eq 44818 any 10 permit tcp any eq 44818 any</pre>
Copy	

虛擬網路防火牆

Claroty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

The screenshot displays the Claroty management console interface, divided into two main sections: "Claroty Recommended Policies" and "Organization Policies".

Claroty Recommended Policies Section:

- Header: "CLAROTY RECOMMENDED POLICIES"
- Filters: "Showing: 15 Recommended Policies", "Sorted By: MATCHING DEVICES (DESC)"
- Table with columns: POLICY ID, POLICY SOURCE, POLICY NAME, APPLIED MODELS, MATCHING DEVICES, POLICY RULES, POLICY ACL.
- Highlighted rows: #RD8 (Mobile Printer - Zebra, 234 Matching Devices, 13 Rules), #RD93 (Building Automation Device - CP3N).
- Two blue arrows point to the "MATCHING DEVICES" and "POLICY RULES" columns.

Policy Information Modal (for #RD4):

- Policy ID: #RD4, Policy Source: Recomm. Based
- Policy Models: CP3N (133 / 133 Devices)
- Policy Attributes: MATCHING DEVICES (133), POLICY ACL (ACL), RELEVANT ALERTS (No Alerts), POLICY CREATION DATE (4/13/25, 10:51 AM), POLICY LAST UPDATED (4/13/25, 10:51 AM), UPDATED BY (Jason Chan).
- Actions: MONITOR POLICY (Yes), GENERATE ALERTS (Yes), EXPORT TO CP3N (+ Export to CP3N Configuration), EXPORT TO ISE (+ Export to ISE Configuration), EXPORT TO FIREWALL (+ Export Policy to Firewall).

POLICY RULES Section:

- Header: "POLICY RULES"
- Filters: "Showing: 20 Rules", "Sorted By: UPDATE STATUS (ASC), PROTOCOL (ASC)"
- Table with columns: UPDATE STATUS, RULE NAME, PROTOCOL, IP PROTOCOL, SIDE A PORTS, SIDE B PORTS, SIDE B IP, SIDE B DEVICE CONDITIONS, RULE SOURCE, RULE ACTION.
- Highlighted rows: DHCP (UDP, any, 67, any, N/A, Claroty, Allow), DNS (UDP, any, 53, any, N/A, Claroty, Allow).

填問卷換贈品



**CYBERSEC
2025**
臺灣資安大會
TEAM CYBERSECURITY
4/15-4/17 臺北南港展覽二館

歡迎蒞臨 uniXecure 智慧資安科技
AUTHENTREND CLAROTY

📍 1F 攤位編號 C234

