Check Point
SOFTWARE TECHNOLOGIES LTD

AI防護讓惡意軟體無所遁形
創新架構強化AIOT應用安全

Danny Yang l Cyber Security Evangelist
2019 Nov 27

WELCOME TO THE FUTURE OF
CYBER SECURITY
POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION

Agenda

- AI資安再進化: 精準判斷新興惡意威脅
- IoT世代的安全挑戰與完整防護
- 資料中心HyperScale創新架構

物聯網(IoT)

- 車聯網
- 智慧電網
- 智慧家庭
- 醫療連網裝置

速率與規模

- 百倍網速與千倍密集度
- 改變企業行動網路應用
- 促進萬物連網

全新架構

- 新架構與控制通訊協定
- 透過NFV實現全虛擬化
- 以MEC分散建置

5G世代將面臨的多重威脅與資安挑戰

裝置層級

- 設備將受到更大程度的危害
- 攻擊者將利用裝置漏洞進行突破
- 無法完全信任供應鏈

網路層級

- 全虛擬化後缺乏完整可視性與東-西向流量管理能力
- 5G通訊協定新的漏洞將被大量利用於惡意攻擊行動
- 退回3G/4G網路使用

5G/IoT的安全漏洞與資安事件

裝置層級

New Mirai Variant Targets Routers, Knocks 900,000 Offline

Home Hack—Is Someone Watching You?

Check Point researchers help LG fix smart home IoT vulnerability

DJI Drone Vulnerability

November 8, 2018

Research by: Oded Vanunu, Dikla Barda and Roman Zaikin

網路層級

NEWS

LTE flaws risk security and privacy of all Android smartphones on Verizon and AT&T

CERT warned of multiple vulnerabilities in LTE networks. Some affect all Android OS versions on Verizon and AT&T.

Security

Buggy devices and lazy operators make VoLTE a security nightmare

NETWORKING

Why LTE and 5G networks could be affected by these new security vulnerabilities

A group of researchers have demonstrated the ability to passively identify session details and actively hija DNS lookups, enabling phishing attacks.

sciendo Proceedings on Privacy Enhancing Technologies 2019

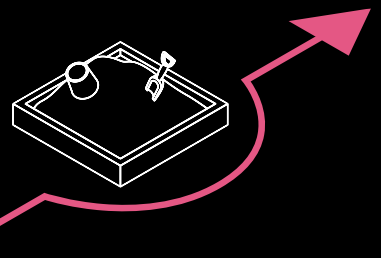
Ravishankar Borgaonkar, Lucca Hirschi*, Shinjo Park, and Altaf Shaik

New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols

過往的安全方案已未必能適用於5G/IoT世代

1 

攻擊者將運用更多未知惡意程式與多重突破口

2 

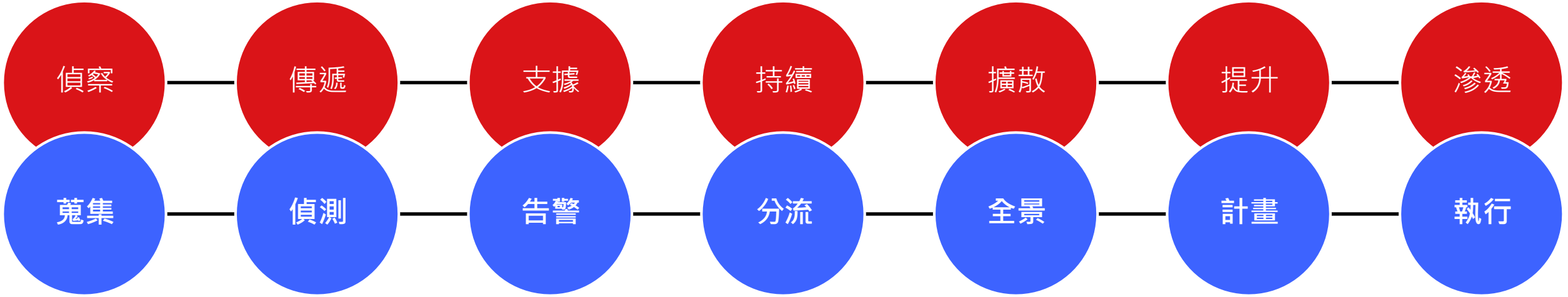
先進的規避型技術與基於AI的攻擊將更普遍

“日益複雜的攻擊型態導致了一個結論
-傳統的安全機制無法消除現今威脅”

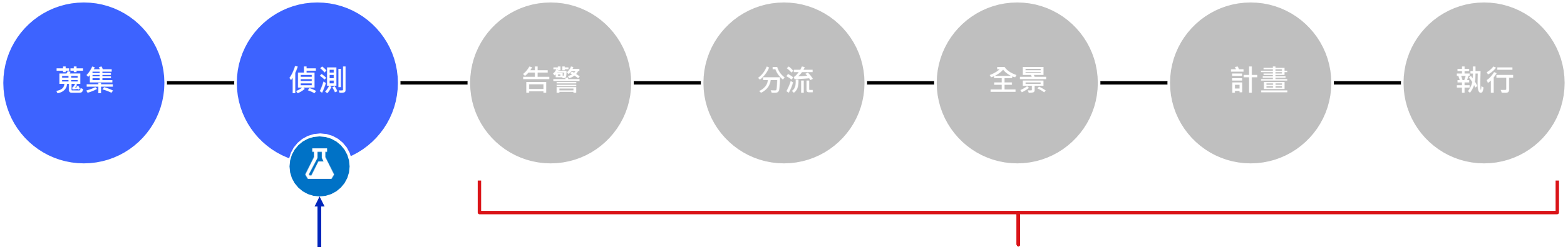
Jack Gold, Computerworld


AI技術
將推動資通訊安全革命

資安攻擊進程(Kill Chain)-攻擊方/防守方



目前安全防護聚焦面向?

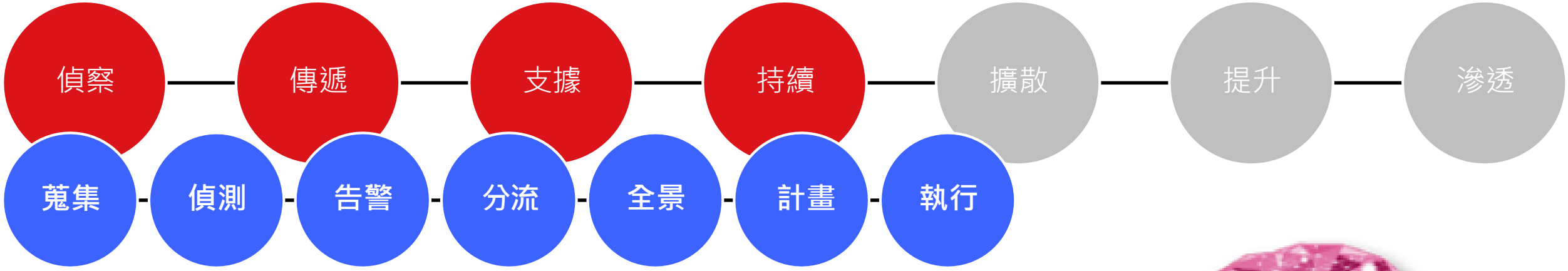


現況已運用部分ML技術
強化威脅偵測能力

多數仍仰賴人為機制
以及極少量智能進行措施

運用AI技術進行預測，提前弭平安全防護差距

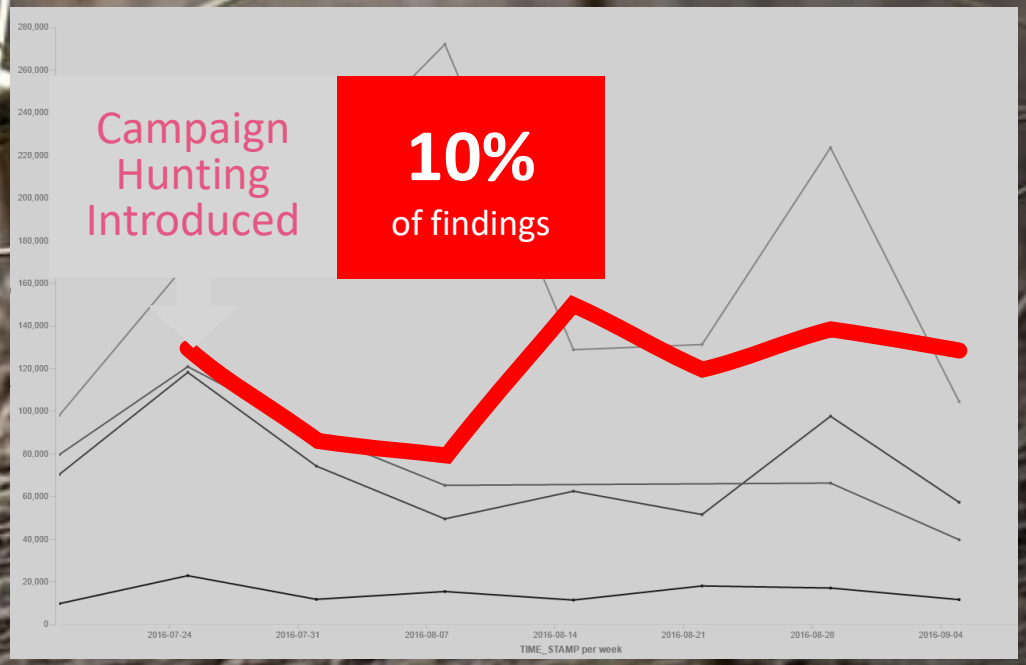
Check Point
SOFTWARE TECHNOLOGIES LTD



AI/ML技術
於Check Point安全方案應用

CAMPAIGN HUNTING

預測型威脅情資分析



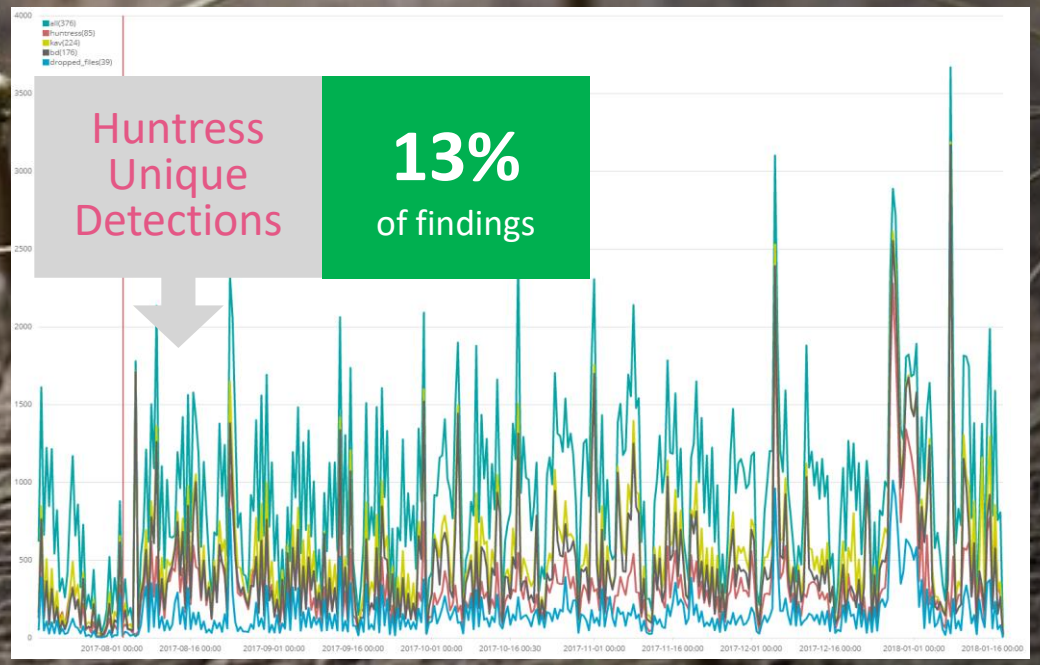
揭露尚未公開的惡意C&C與Domain

透過AI監控即時惡意活動頻率

反饋威脅指標至雲端威脅引擎

“HUNTRESS”

未知惡意程式行為分析



以APIs介接沙箱動態分析惡意執行檔

應用機器學習發現隱含威脅的惡意程式

反饋檢測參數並持續深度學習

靜態分析

“BLENDER”

混合測試執行檔主體與結構

分析檔案內文向量
與結構元素

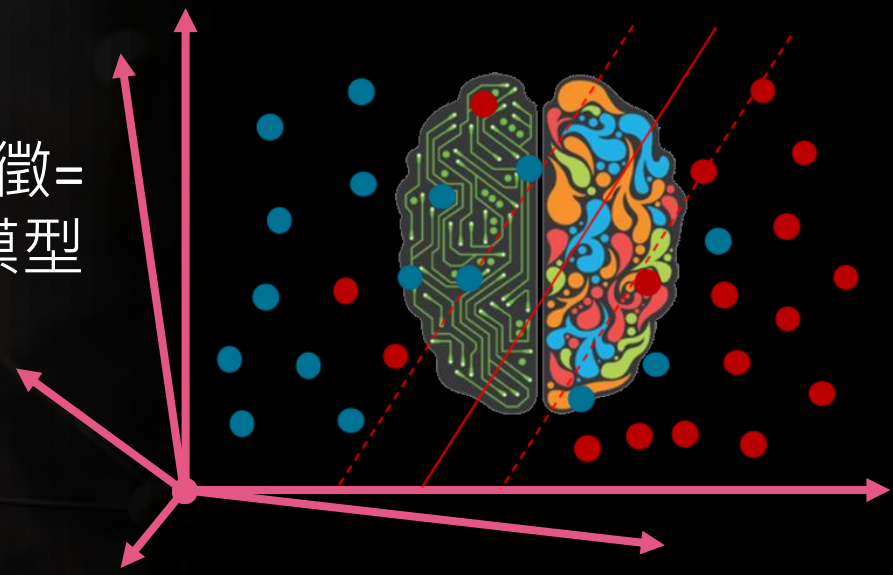
發現新型惡意程式!

動態分析

“BUFFY”

發現未知惡意執行檔

數千個特徵=
建立標準模型



動態分析ML/AI 模型範例:
特徵1 = Registry Read Ops
特徵2 = Num of Created Files

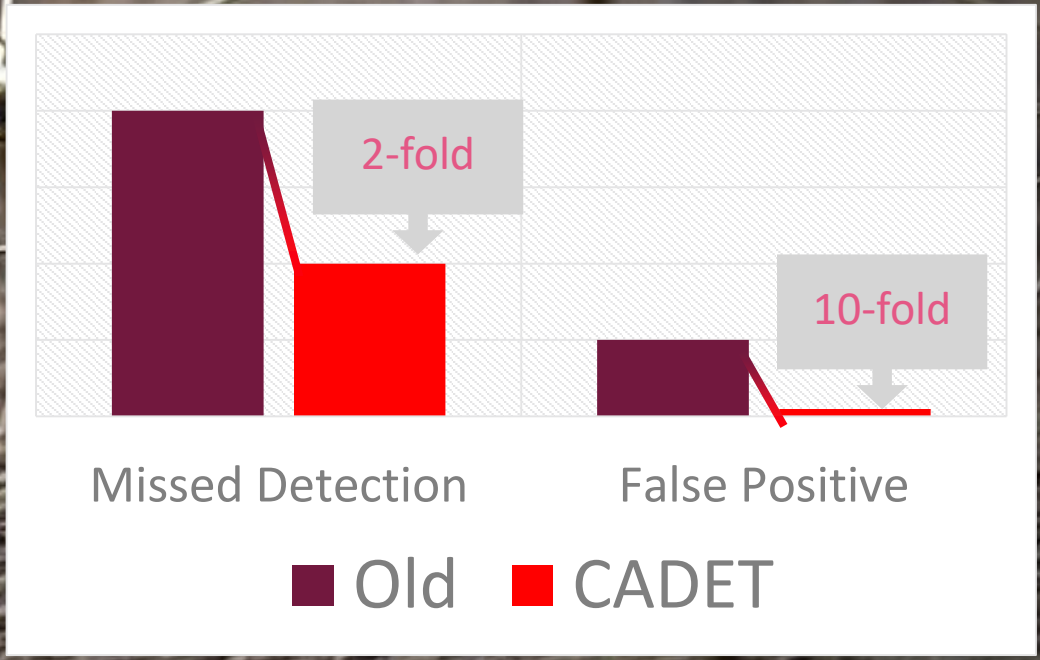
Emulation Timeline

Win10 64b,Office 2016,Adobe DC | **Win7 64b,Office 2010,Adobe 11** | Win7,Office 2013,Adobe 11 | Win8.1 64b,Office 2013,Adobe

TYPE	ACTION	SOURCE	DESTINATION
RegistryEvent	CreateKey	C:\\te_files\\emulatedFile5_1.exe	HKLM\\Software\\Wow6432Nod \\WanaCrypt0r
RegistryEvent	QueryKey	C:\\te_files\\emulatedFile5_1.exe	HKLM\\SOFTWARE\\Wow6432Node\\WanaCrypt0r
RegistryEvent	SetValueKey	C:\\te_files\\emulatedFile5_1.exe	HKLM\\SOFTWARE\\Wow6432Node\\WanaCrypt0r\\wd
RegistryEvent	CloseKey	C:\\te_files\\emulatedFile5_1.exe	HKLM\\SOFTWARE\\Wow6432Node\\WanaCrypt0r
FileSystemEvent	Read	C:\\te_files\\emulatedFile5_1.exe	C:\ Mft
FileSystemEvent	Create	C:\\te_files\\emulatedFile5_1.exe	C:\\te_files\\taskdl.exe
FileSystemEvent	Create	C:\\te_files\\emulatedFile5_1.exe	C:\\te_files\\taskse.exe
ProcessEvent	Create	C:\\te_files\\emulatedFile5_1.exe	C:\\Windows\\SysWOW64\\attrib.exe
RegistryEvent	OpenKey	C:\\te_files\\emulatedFile5_1.exe	HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows\\Safer\

“CADET”

全文感知偵查
(CONTEXT AWARE)



全文感知與威脅情資決策

擷取多樣化IT環境參數

(如郵件, 網路, 雲服務, 端點, 行動裝置)

數千 → 一個

不同屬性威脅指標 精準判斷

變種惡意程式

模糊化處理/ 重新打包

全新世代與家族

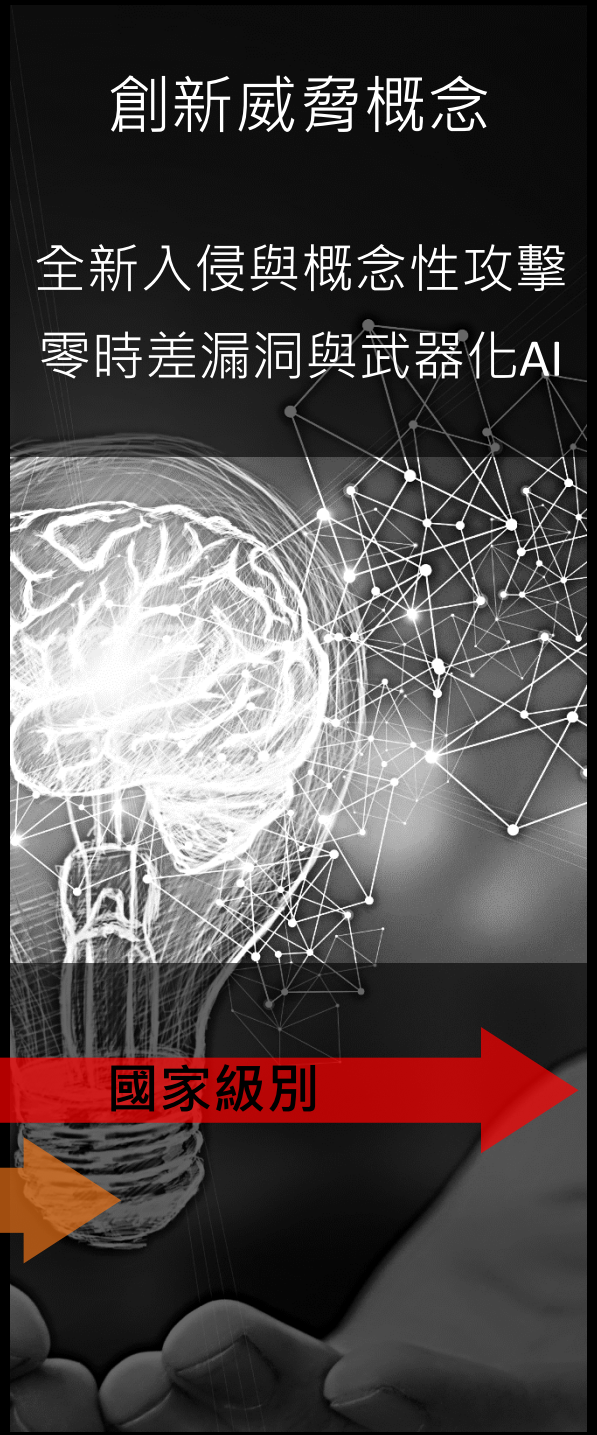
改變行為模式

植入規避程式碼

創新威脅概念

全新入侵與概念性攻擊

零時差漏洞與武器化AI



國家級別

網路罪犯

業餘駭客

AI結合敏捷的即時安全事件回應機制為必要措施!

Check Point
SOFTWARE TECHNOLOGIES LTD

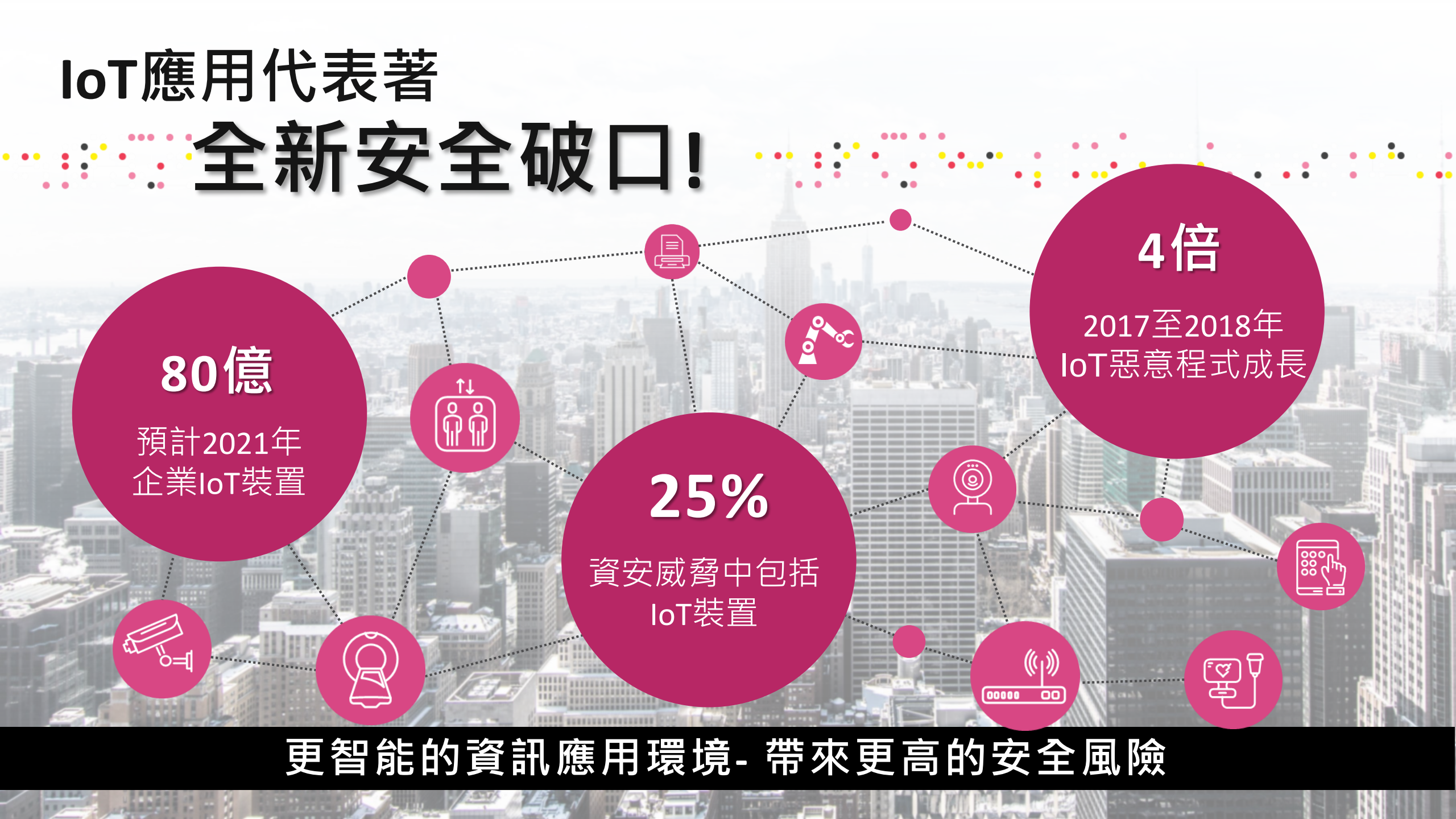
摘要

- 資料量是AI安全應用的根本元素
- 產業經驗為成功發展AI的關鍵
- 由數據驅動安全防護為未來的趨勢
- 需配合事件分析達成完整防護

AI發展目標:

更有效率並超越人類專家水平的精準預測能力

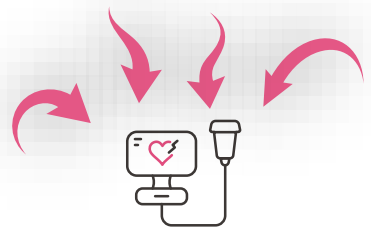
IoT應用代表著
全新安全破口!



更智能的資訊應用環境- 帶來更高的安全風險

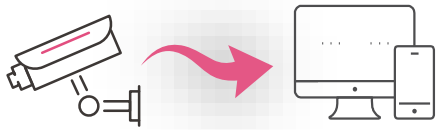
IoT 安全挑戰與風險

- 老舊軟體作業系統 / 無作業系統
- 基本的系統微控制器
- 無安全預設設計
- 無法控管的裝置
- Shadow裝置情況
- 作業面限制



裝置風險

損壞，人為操控或停機問題



網路風險

橫向擴散感染其他系統

資安優先面向: IT vs OT

Check Point
SOFTWARE TECHNOLOGIES LTD

IT 重視: 資料保護

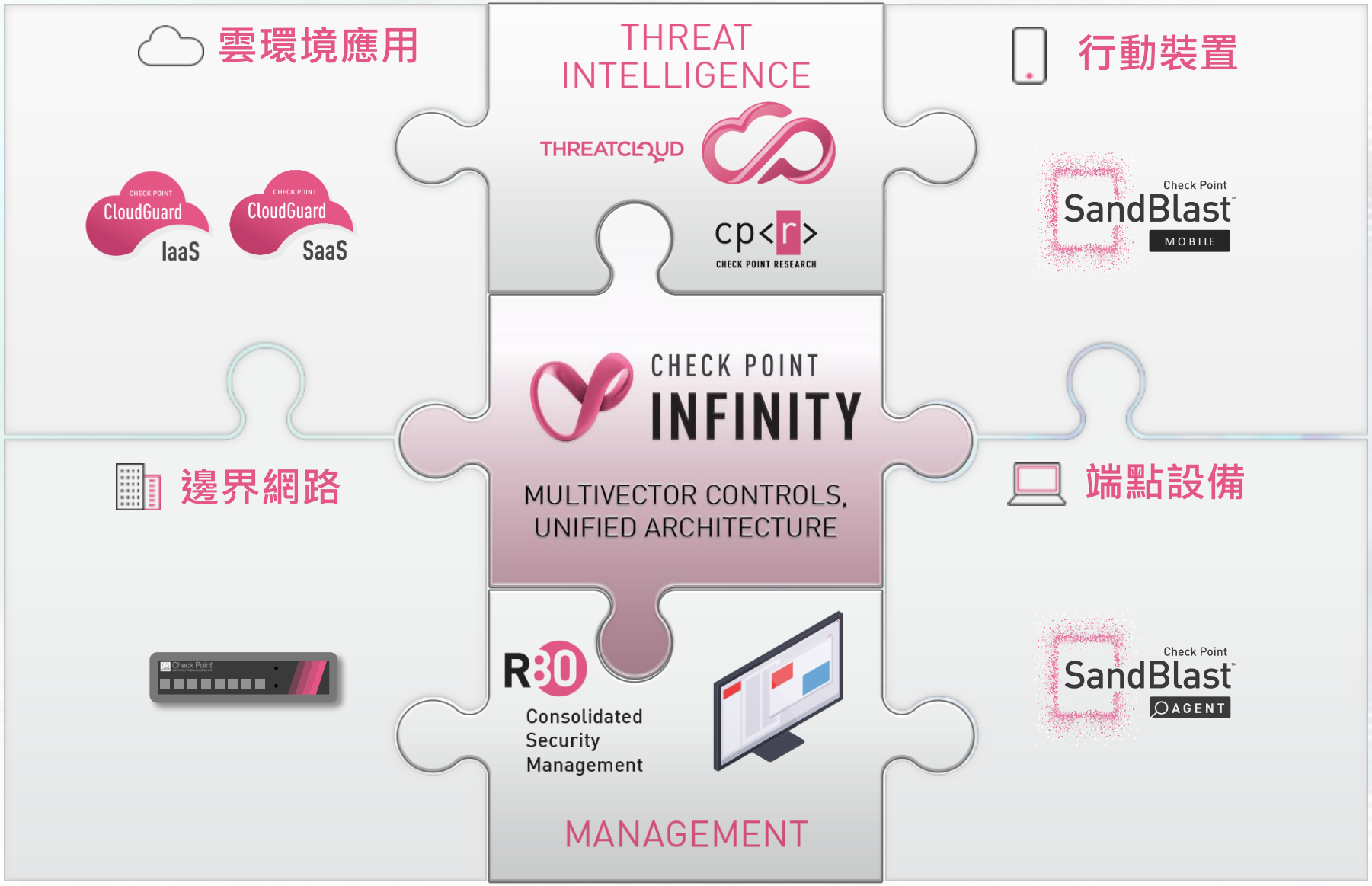
機敏性

完整性

可用性

OT 重視: 流程保障

Check Point Infinity: 完整的IT/OT零信任防護模型

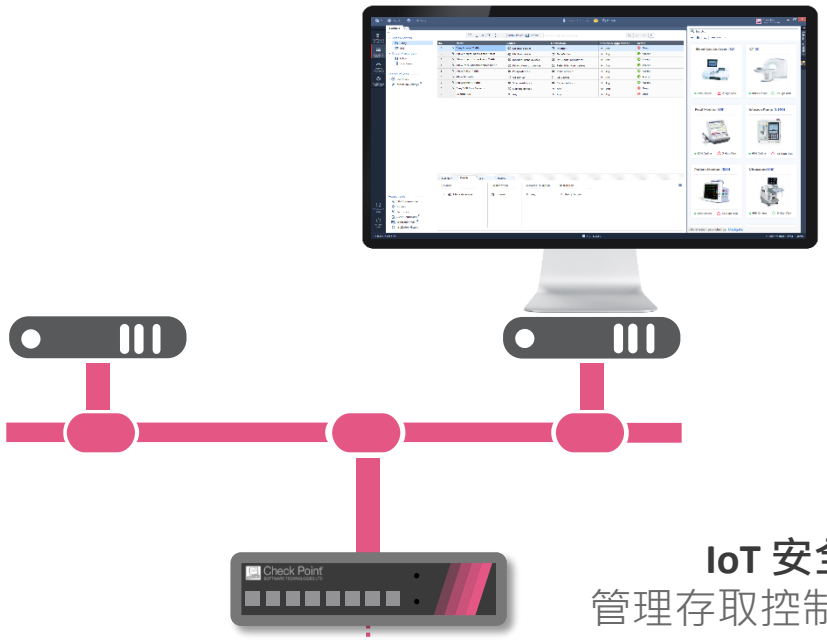


Check Point Infinity for IoT

統合智能安全方案| 簡易部署維運

IoT 啟發識別引擎
整合最多領先IoT設備供應商

ARMIS
CLAROTY Clarity for OT Networks
CYBER MDX
CYBERX
Cynerio
Indegy
MEDIGATE
ordr take control

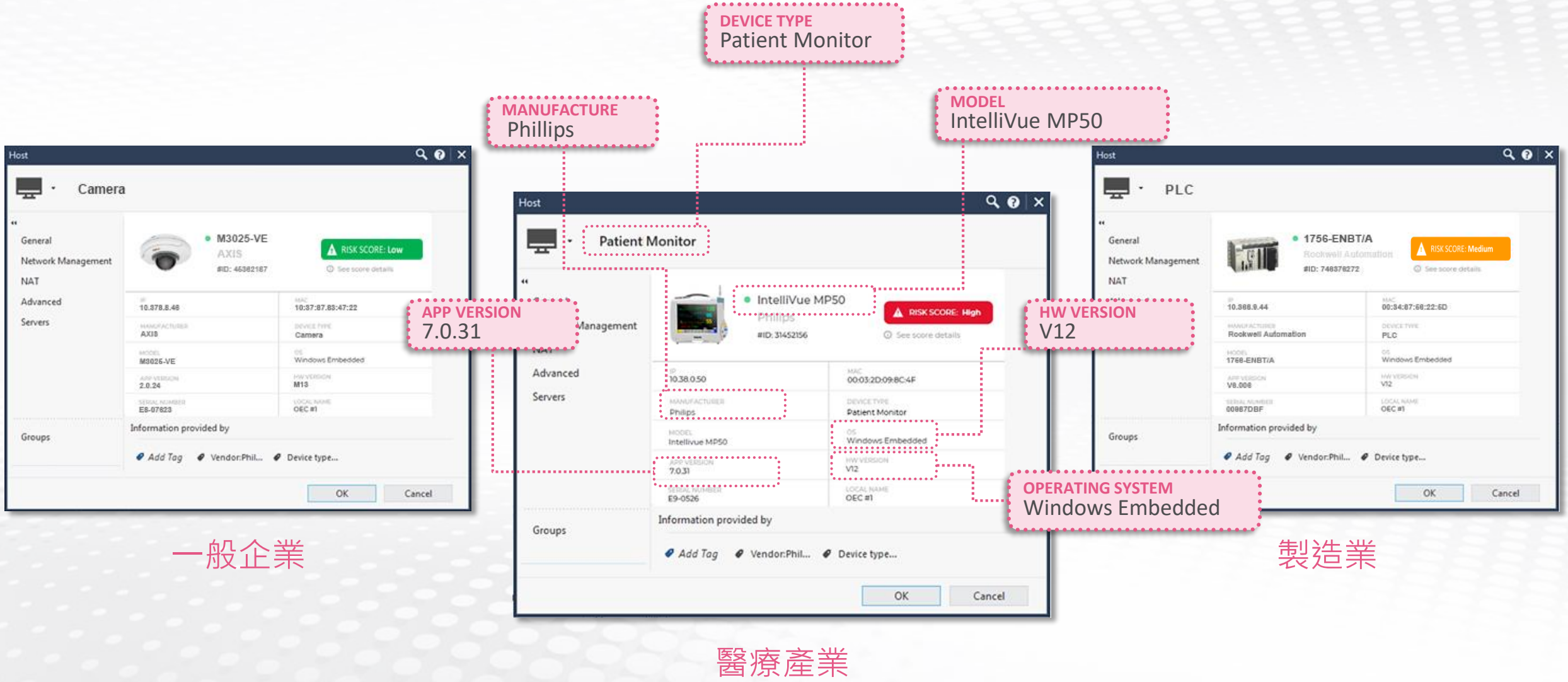


IoT 安全管控
IoT環境與設備完整管控與可視性

IoT 安全閘道
管理存取控制與威脅防護

快速發現與識別IoT裝置資訊

全面了解IoT和OT設備屬性



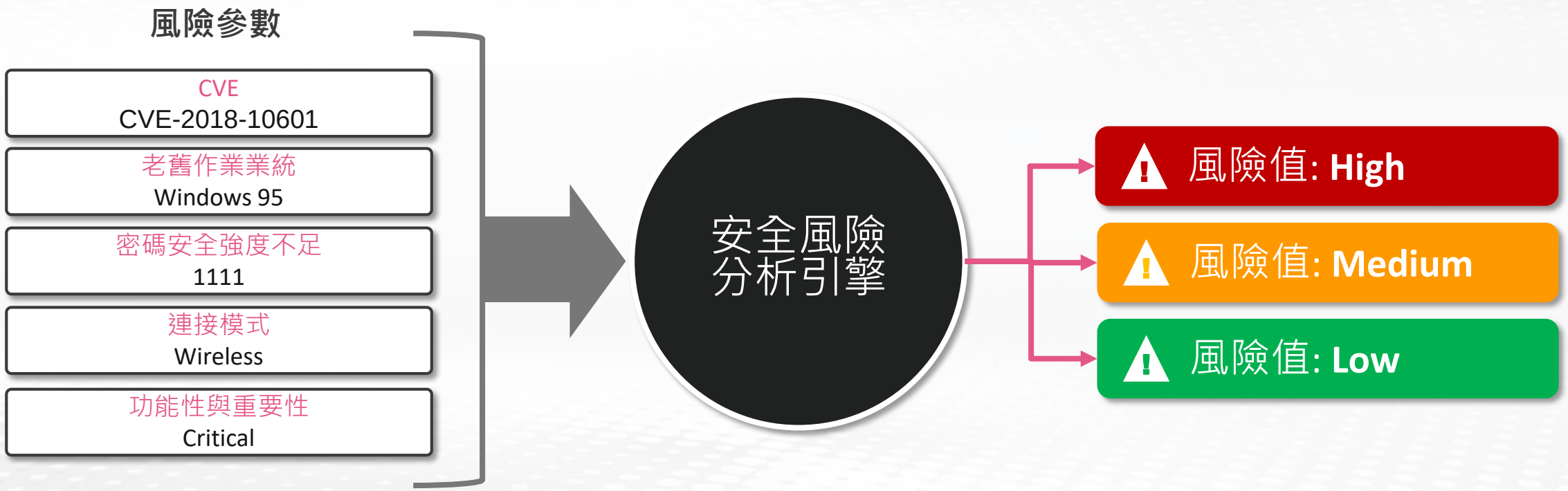
一般企業

醫療產業

製造業

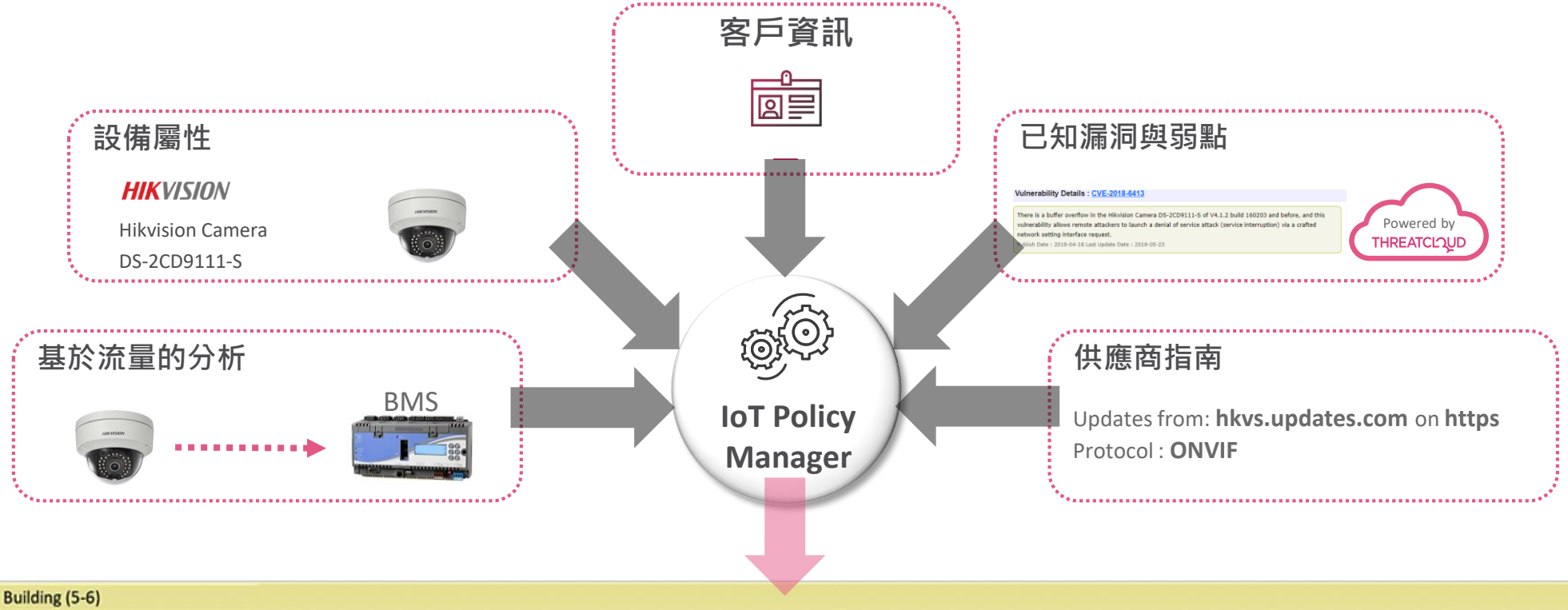
啟發性威脅分析引擎與安全可視性

獲取精準的風險評估於所有IoT與OT裝置

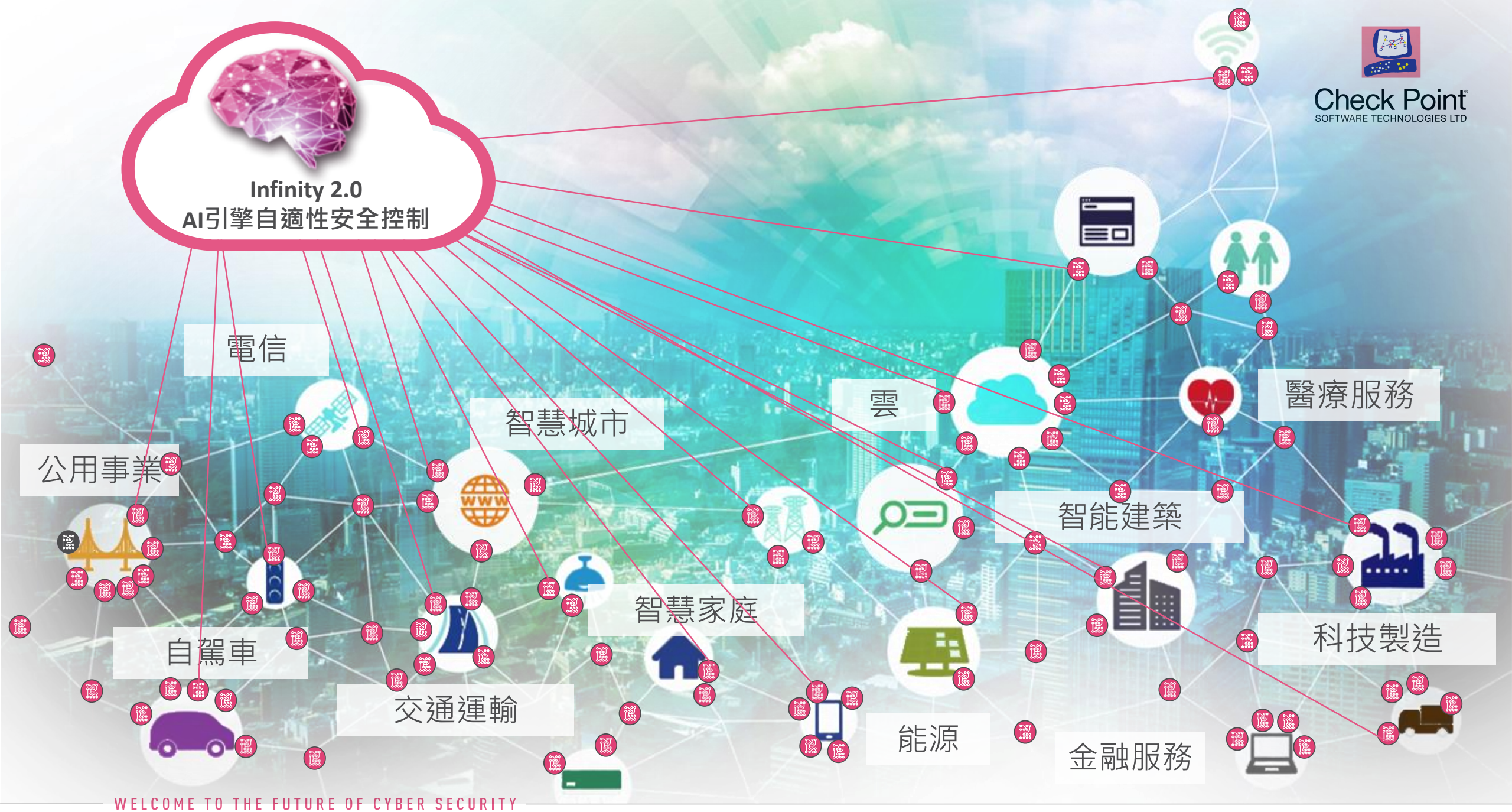


IoT感知式自動安全存取控管政策

自適應IoT環境變化，自動生成安全規則



Smart Building (5-6)							
5	IP CAM	IP CAM	Any	Any	IP CAM	NA	Policy Targets
5.1	IP CAM to BMS	IP CAM	BMS	ONVIF Protocol	Accept	Log	Policy Targets
5.2	Hikvision updates	Manufacture=Hikvision	.hkvs.updates.com	https	Accept	Log	Policy Targets




01;00;01;06
PLEASE STAND BY
創新的5G與AIoT資料中心架構設計!


5G與IoT的基礎架構難題...
網路流量
每3年翻倍爆量成長
每年資料中心數據成長率
25%
Based on Cisco GCI 2016-2021

現有規劃能否符合5G/IoT安全效能需求?

Check Point
SOFTWARE TECHNOLOGIES LTD

惡意威脅與日倍增...

企業建構安全防護平台**是否足以因應未來的成長?**

先進網路安全思維

靈活彈性的雲級可擴充安全平台

輕鬆擴展現有安全閘道效能

並按實際需求進行動態延展

– 能大幅降低停機風險
並最大限度提高安全成本效益

Check Point
SOFTWARE TECHNOLOGIES LTD

劃世代網路安全架構

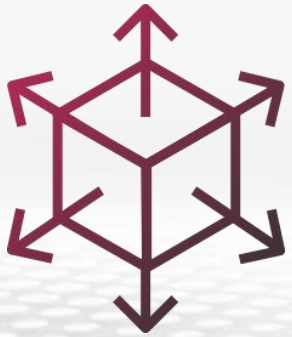
MAESTRO
HYPERSCALE ORCHESTRATOR

全球最先進安全硬體叢集技術
單一平台提供最高度效能與備援

Check Point
SOFTWARE TECHNOLOGIES LTD

MAESTRO

安全架構優勢



安全超延展性

可依不同需求搭配不同的設備
進行安全閘道叢集組合

符合業務成長與未來需求

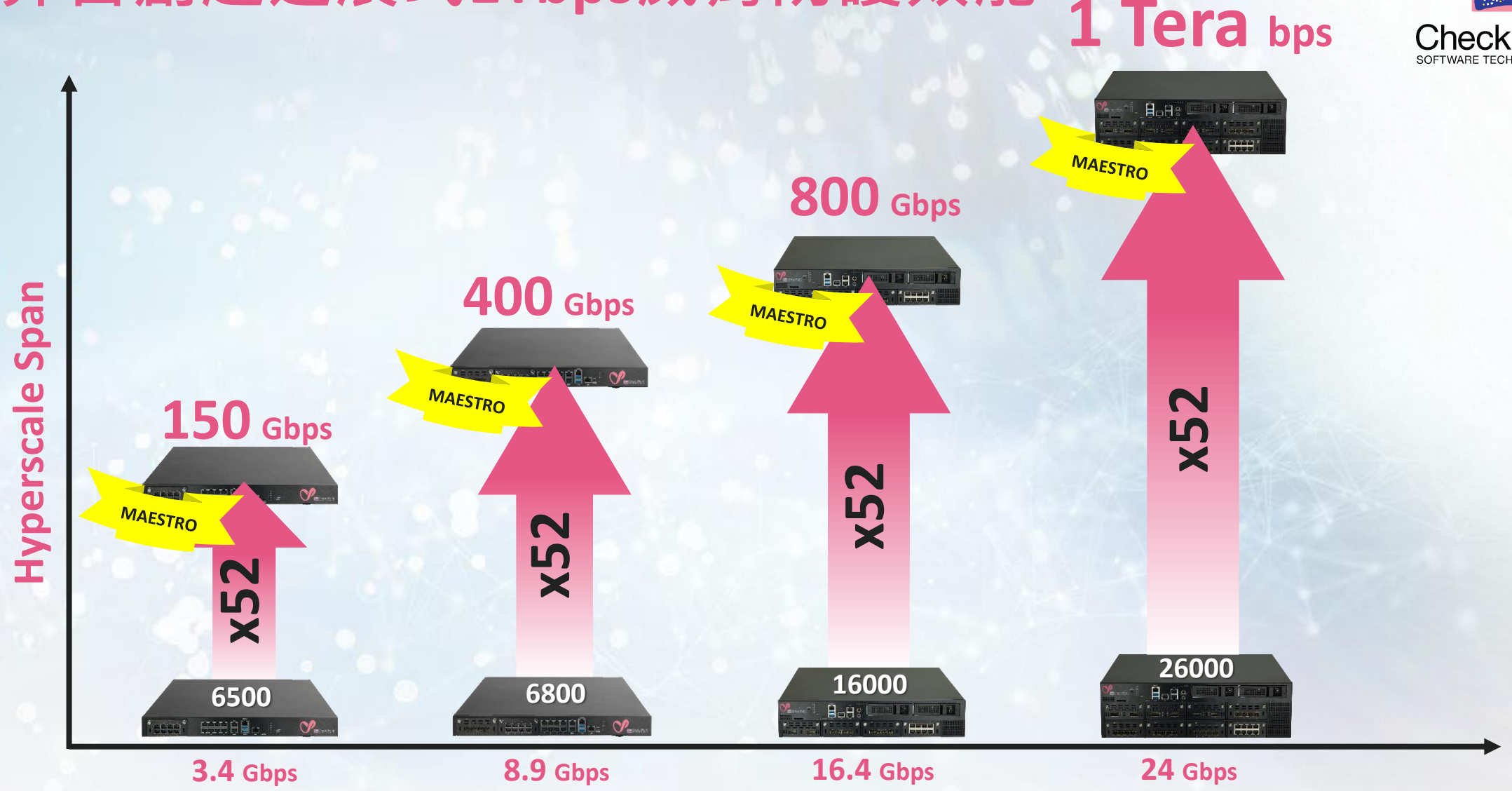
最適於成長型及新創企業的安全需求
大幅簡化管理與維運問題

雲資料中心級擴充彈性

電信/雲端中心等級的安全架構
隨心所欲的效能提升與可用性

業界首創超延展式1Tbps威脅防護效能

Check Point
SOFTWARE TECHNOLOGIES LTD



可組合成 52台閘道安全叢集 並劃分 8個安全群組

最高可承載 1,000 Gbps SandBlast啟用效能(APT威脅防護)

MAESTRO
先進硬體叢集與負載平衡技術

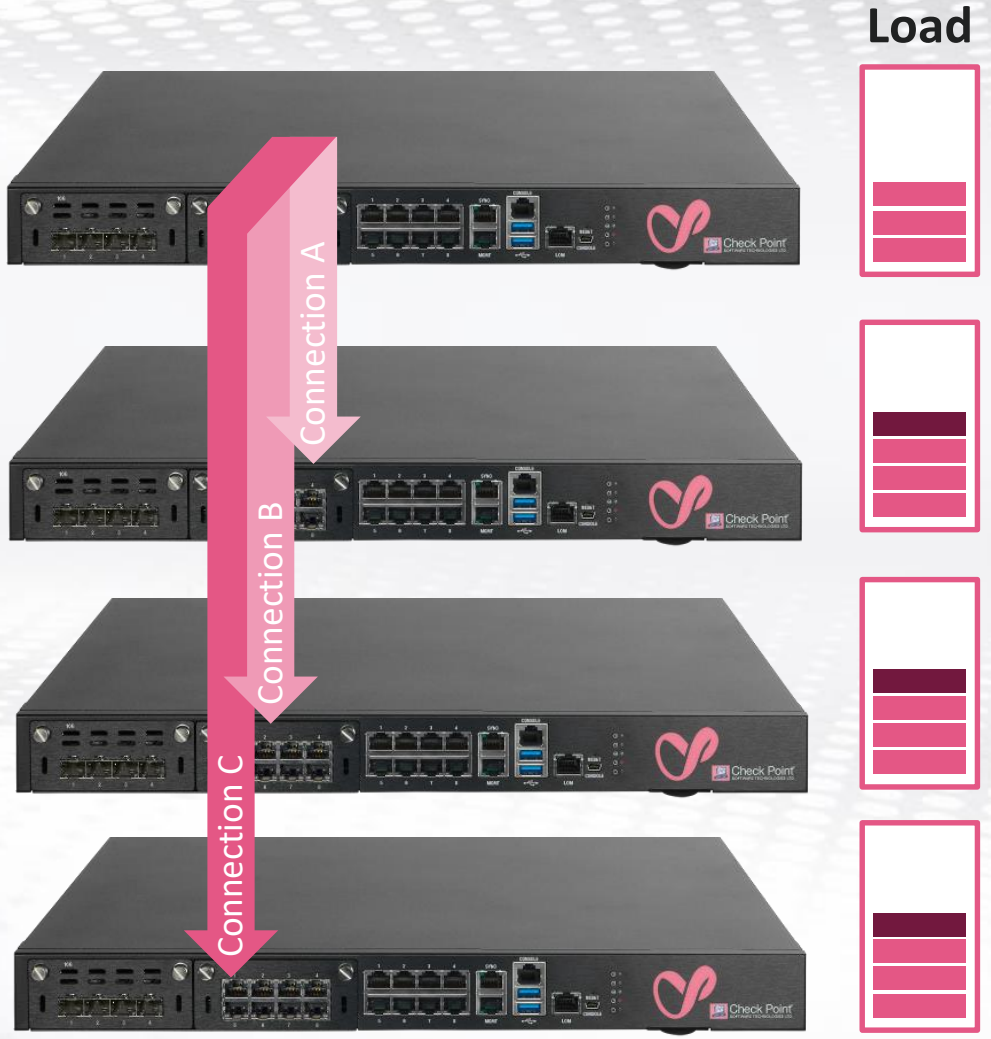
Check Point
SOFTWARE TECHNOLOGIES LTD

專利技術

HyperSync

雲資料中心專屬叢集科技
電信等級擴充能力

- 超高擴充性與完整備援機制
- N+1部署與安全效益最佳化
- 充分利用所有群組設備資源



高度可擴充性叢集與HA備援

Check Point
SOFTWARE TECHNOLOGIES LTD

傳統叢集

兩台設備

1 Gbps

MAESTRO ORCHESTRATION

三台設備

3 Gbps

1 + 1 = 1 ← 簡易對照 → **1 + 1 + 1 = 3**

實際應用範例

PilotLite™

Active/Active

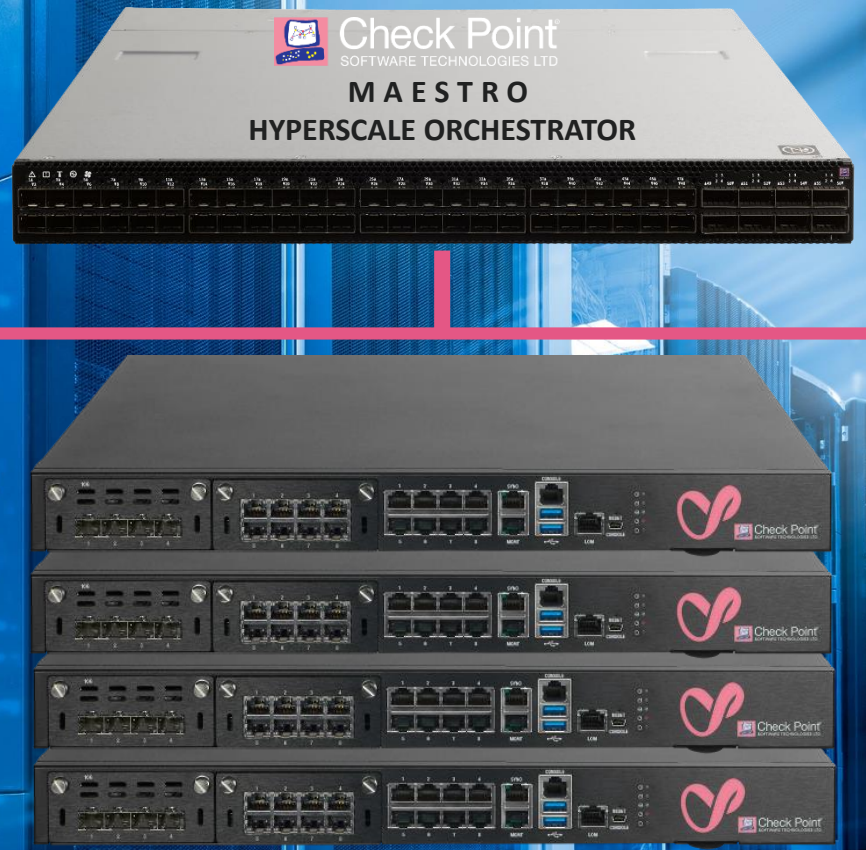
預先導入新世代安全叢集設計

PilotLite™

Active/Active

數分鐘內即可擴充叢集並符合整合管理與成長需求

PilotLite™



OFFICES

CLOUD TRAFFIC

整合閘道

單一平台管理所有虛實網路閘道

高度效益與擴充彈性

PilotLite™

Auto-Scaling

動態調度安全資源於不同的安全群組設定(Security Group)

Check Point
SOFTWARE TECHNOLOGIES LTD

Maestro

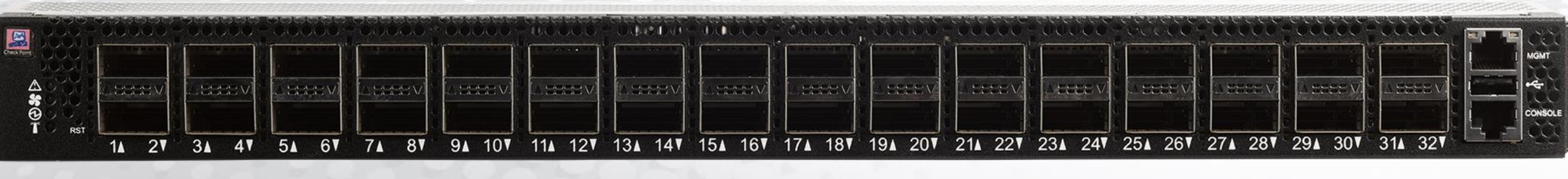
業界領先的Hyperscale網路安全解決方案與創新架構
-專為5G與AIoT高擴充性需求所打造!

快速部署

易於維運

雲端層級敏捷性

高度效益



Check Point
SOFTWARE TECHNOLOGIES LTD

THANK YOU

有任何問題，歡迎與我聯繫!

dannyy@checkpoint.com

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION