Check Point
SOFTWARE TECHNOLOGIES LTD

明日過後:
IT因應「新常態」後的資安挑戰

楊敦凱 Danny Yang l Cyber Security Evangelist

個人簡介

楊敦凱 Danny Yang

Check Point 資安傳教士
Office of the CTO

-12年IT產業經驗，曾任職於原廠、代理商

-聚焦於資安產品推廣銷售約8年時間

-曾任業務、售前顧問、產品經理等職務

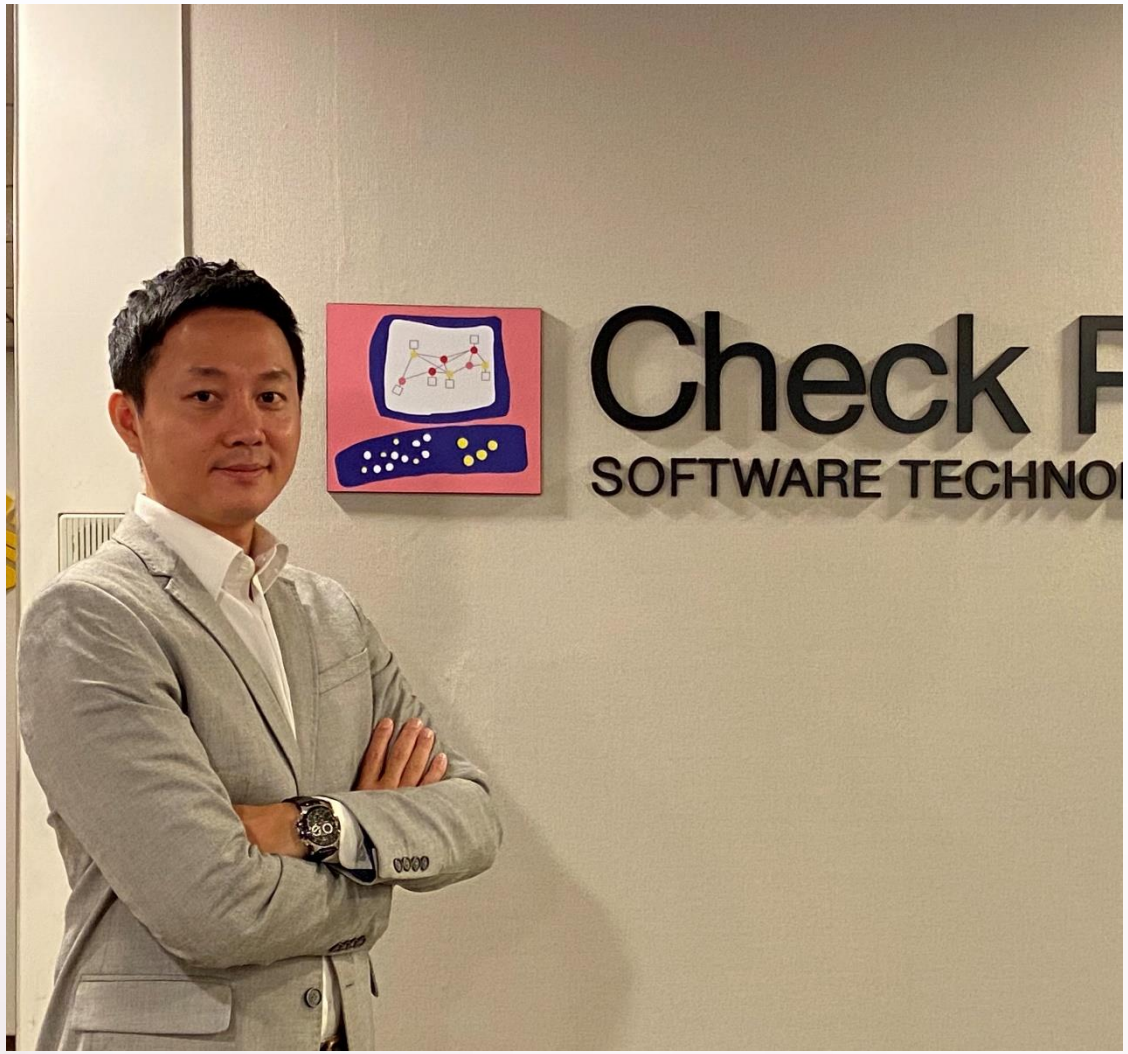
-超過50場以上的研討會講演經驗

-2016 亞太區 “Threat Talent Pitch” 冠軍

-2019 北亞區 ”SE of the Year”

-擁有包含ISO 27001 LA, PIMS BS10012 LA

CCSE, CCSA, CCSBA, CCVSA等安全證照



Agenda

- 來自上帝應許之地的資安巨擘-Check Point Software
- 2020資安威脅趨勢與「新常態」安全問題
- 跨世代安全架構藍圖: Infinity Next
- 雲端IoT與資料中心先進安全策略
- AI於資安應用與智能安全防護平台
- Let’s Kahoot!

來自上帝應許之地的資安巨擘

CHECK POINT SOFTWARE TECHNOLOGIES

全球資安傳奇- Check Point軟體科技

以色列最具價值的IT公司
市值高達 $19B

以色列創新科技的典範廠商之一
卓越的安全技術聞名全球

世界最佳安全軟體公司之一
全球科技新鮮人首選公司

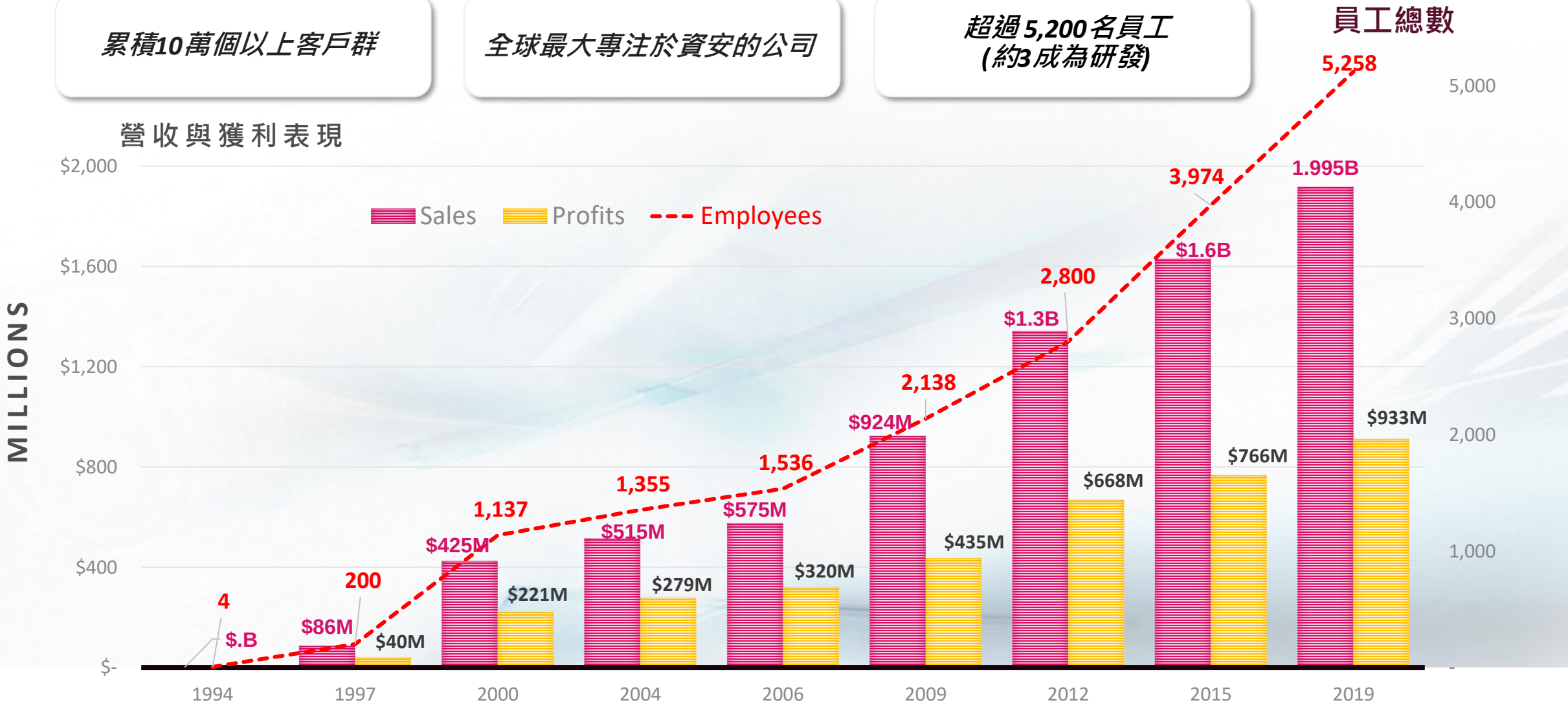
贏得2019年以色列科技大賞首獎
創辦人兼執行長 Gil Shwed

持續25年以上的穩健成長與優異獲利能力

累積10萬個以上客戶群

全球最大專注於資安的公司

超過5,200名員工
(約3成為研發)



Check Point: 最專注於Cyber Security的創新研發公司

- 世界安全領導廠牌– 擁有100,000以上客戶數, 88+全球分公司, 6,200+ 合作夥伴
- 20多年來聚焦於發展資安技術，最具遠見的創新思維
- 安全至上的尖端科技，擁有競爭廠商一倍以上的高端研發能量
- 1996即掛牌於Nasdaq科技股百強- 代號: CHKP(股價約 USD 120+)
- 超過5,200+員工，匯聚全球頂尖IT人才

財星500大企業指定安全品牌

2020資安威脅趨勢與現況分析

全球政府領袖異口同聲:
資通訊安全為最重要的議題

Donald J. Trump
美國總統

Florence Parley
法國 國防部長

需正視的存在威脅

不斷升級的網路風險
對經濟穩定和國安構成威脅

資訊戰爭已開打

我國必須準備戰鬥
網路已成為列強對抗的場所

近期影響臺灣企業/組織的資安事件

2020 Q2

高科技廠傳出辦公電腦感染勒索病毒!

政府組織人員郵件帳號遭害!

關鍵基礎設施供應商遭受網攻，多數辦公電腦被加密

2020 Q3

攻擊接二連三，高科技大廠被攻擊產線一度中斷

重要政府單位疑似被駭客攻擊; 個資檔案於暗網被兜售

2020 五大資安趨勢與現象

- 資訊犯罪更為組織化(國家級)
- 雲端安全服務風險不斷變化
- 勒索軟體方興未艾精緻化發展
- 行動裝置惡意程式快速增加
- 全新安全突破點 - 5G與IoT應用

針對式
勒索軟體攻擊

勒索軟體漏洞攻擊主要針對特定企業、地方政府和醫療組織。攻擊者花費大量時間收集受害者情報，以確保可成功進行攻擊並藉機勒索高額贖金。

精緻化的針對性攻擊

更多變種與新漏洞

惡意釣魚攻擊日益嚴重

儘管電子郵件仍然是主要攻擊手法，但網路犯罪分子也利用其他攻擊手法來誘騙目標受害者提供個人資訊、登錄憑證甚至匯款。網路釣魚也擴及手機簡訊詐騙、社群媒體以及遊戲平台上的訊息傳遞。

多面向的惡意釣魚

AI-Based釣魚攻擊

雲端服務應用
IaaS/SaaS/PaaS

某些企業已大量將工作上雲，但雲端安全意識十分匱乏，往往在雲端部署結束後才開始考慮資安問題。安全解決方案應基於雲端新架構更靈活演進，同時再次審視現有資料中心和雲端解決方案，並考慮混合(Hybrid Cloud)之可行性。

帳號與身份劫持

人為控制疏失

行動裝置威脅更為劇烈

去年銀行惡意軟體攻擊增加50%。此類Apps不僅能從受害者銀行帳戶中竊取付款資料、憑證和資金，且任何願意向該惡意軟體支付費用的人均可獲得新版本。此外，網路釣魚攻擊也越趨複雜及有效，誘使行動裝置使用者點擊惡意網站連結。

行動裝置釣魚更猖獗

應用程式權限濫用

5G&IoT改變生活
尤須重視資安

隨著5G網路加快部署，IoT裝置連接使用將大幅增速，更容易遭到大規模、多向量網路攻擊。IoT裝置及其網路和雲端連接仍為安全方面的弱點，不僅難以獲取裝置可視性，且對安全要求更加複雜。未來需要更全面的IoT安全解決方案，結合新舊控制措施，保護各產業中不斷擴增的網路。

IoT裝置漏洞為突破口

IoT架構可視性不足

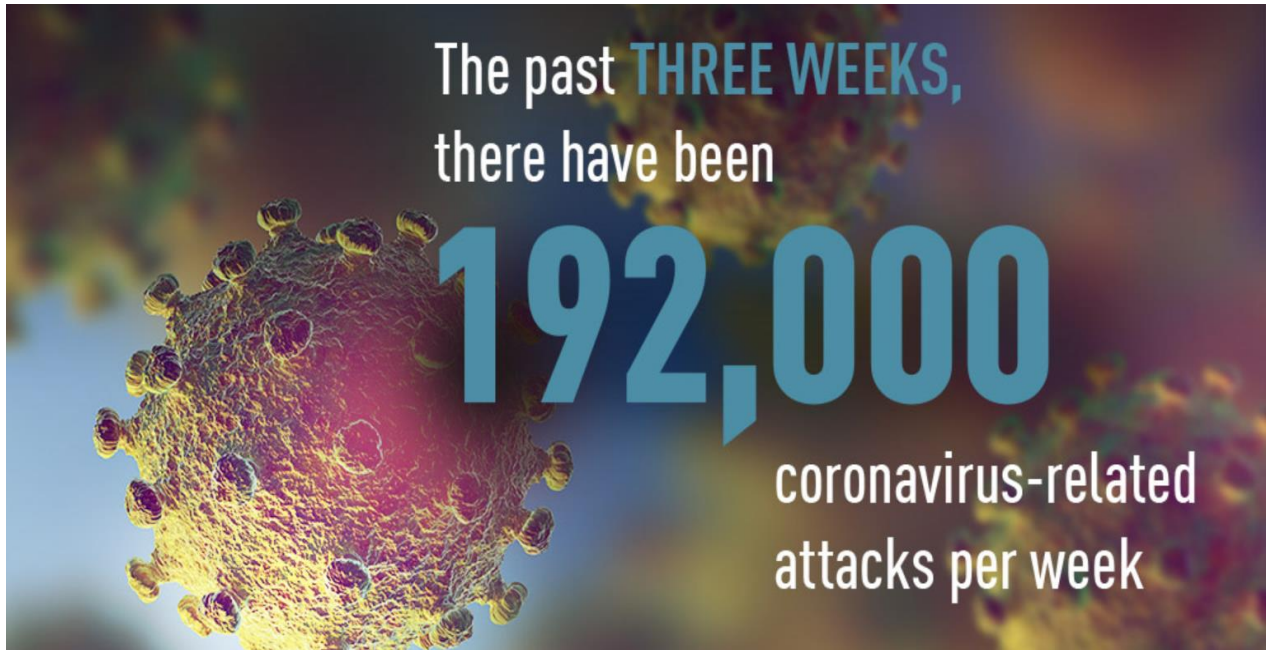
Check Point
SOFTWARE TECHNOLOGIES

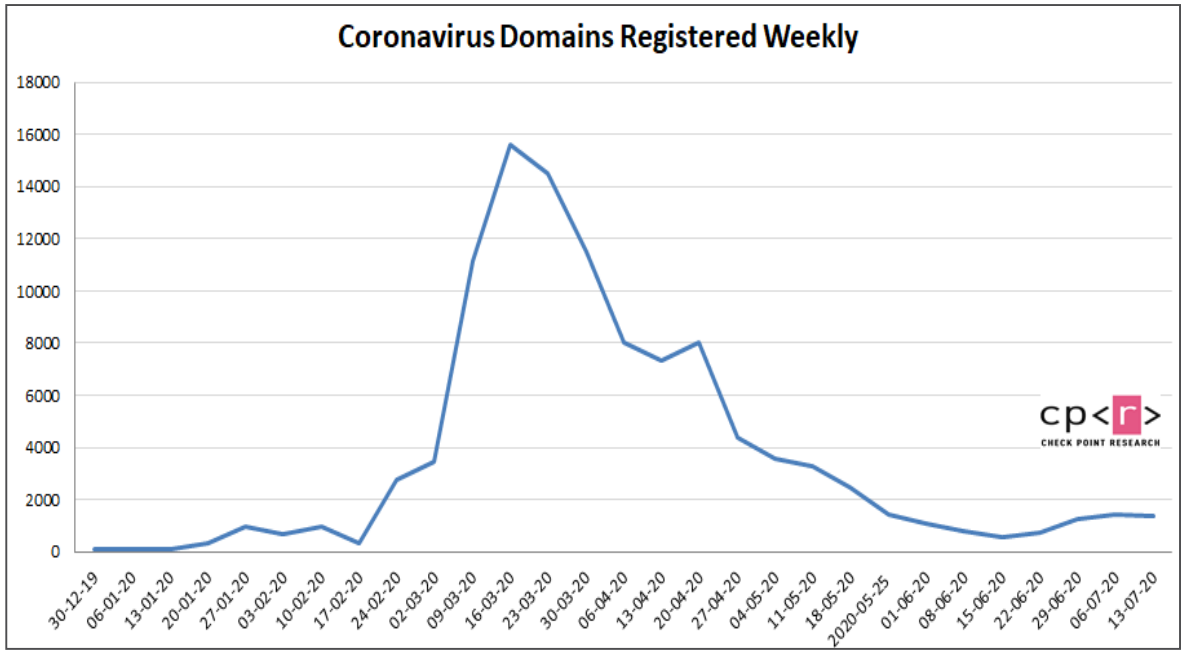
Check Point 2020年中威脅分析報告:

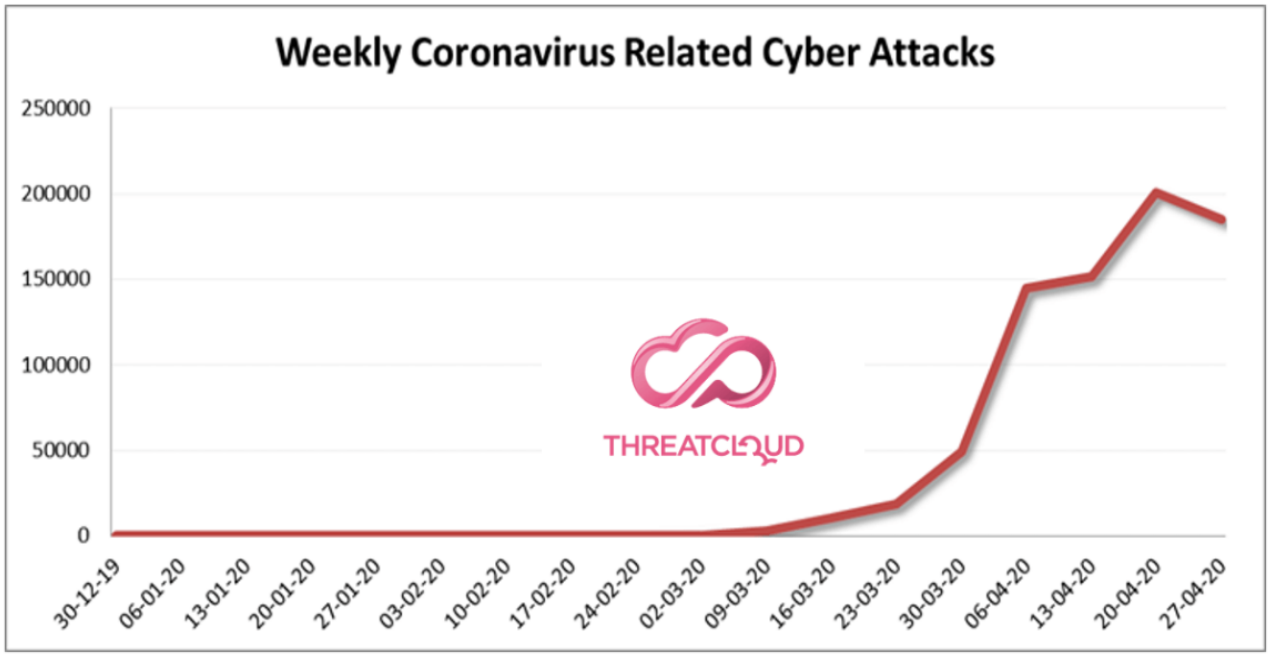
	Mobile	Banking	Cryptominer	Botnet	InfoStealer
Taiwan Avg.	9.3%	14.0%	10.3%	20.9%	10.2%
Global Avg.	4.0%	2.6%	5.5%	7.2%	2.7%

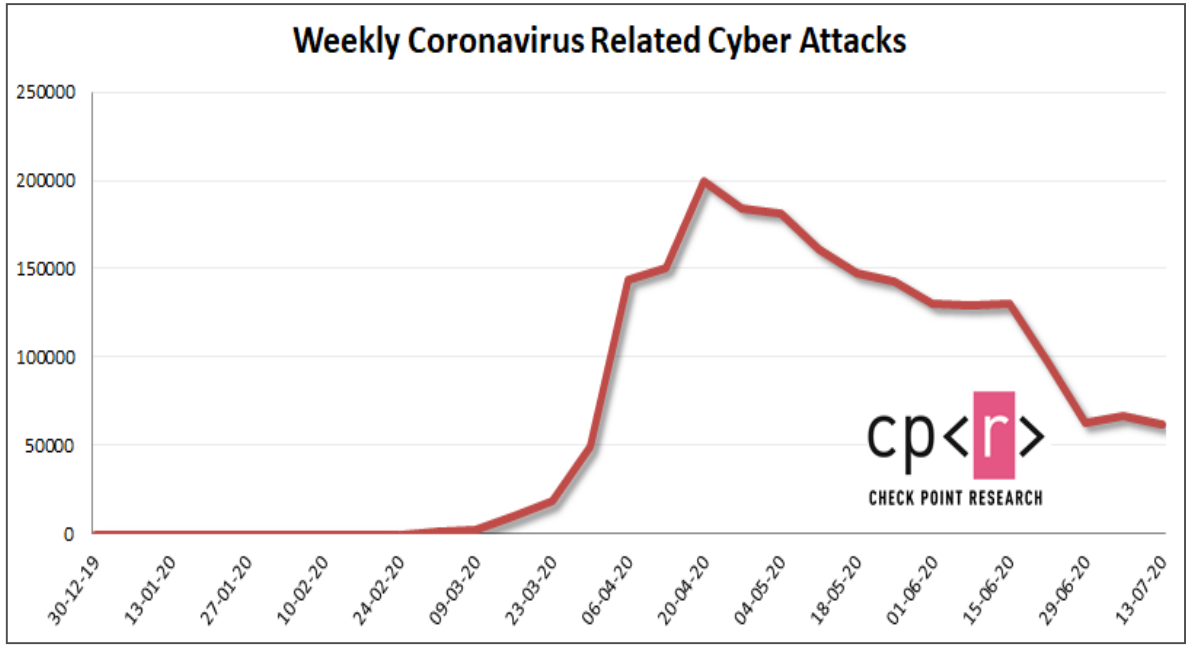
https://pages.checkpoint.com/cyber-attack-2020-trends.html Check Point Threat Report- Regional


GOD, CAN WE UNINSTALL 2020 AND REINSTALL IT,
IT HAS A VIRUS!
imgflip.com





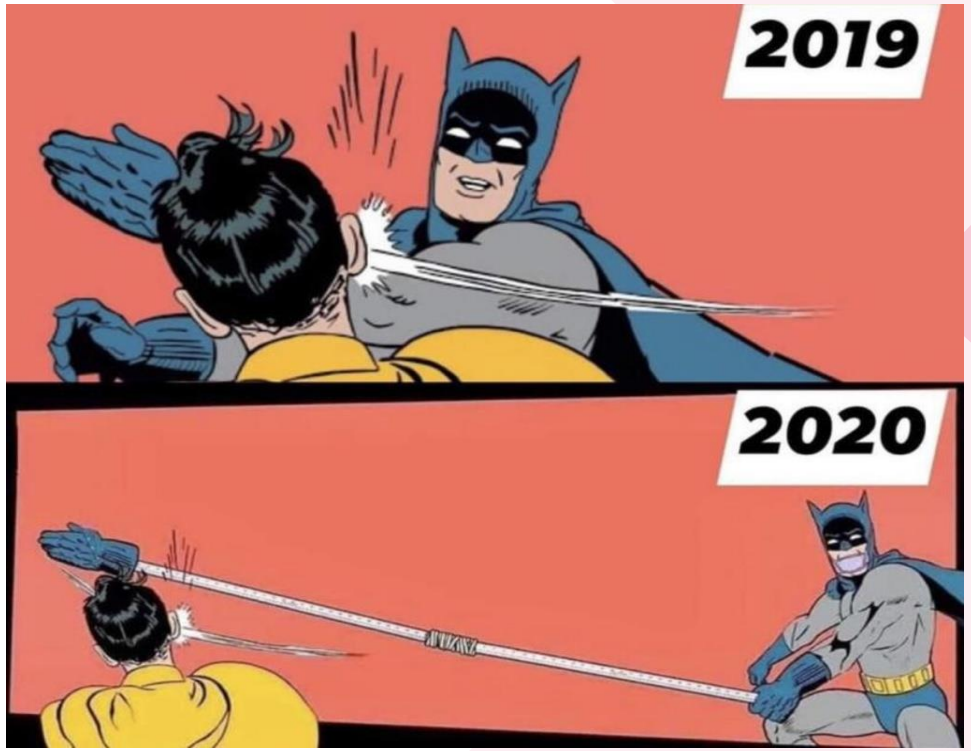




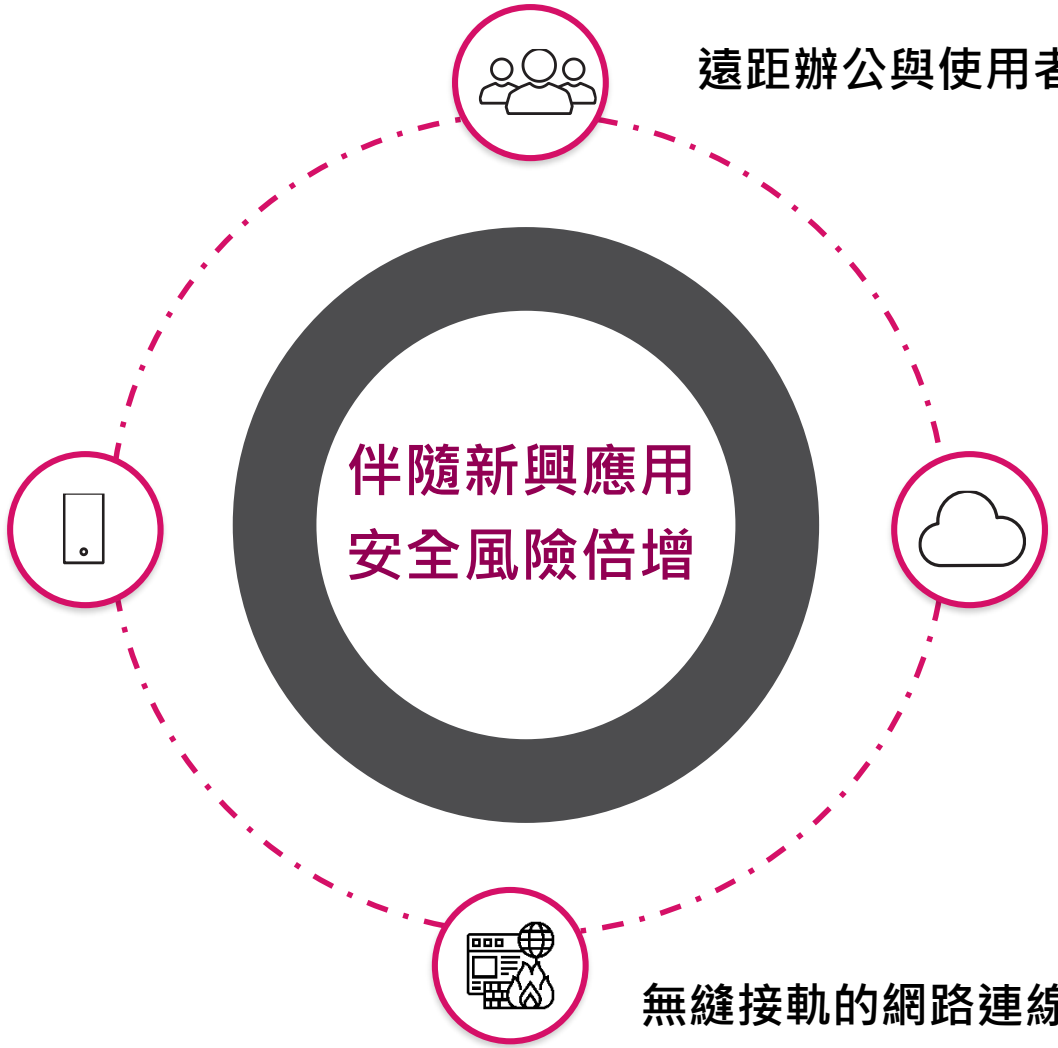
https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/

疫情過後開始重新適應新生活

- 新常態: 為接下來數年訂定新標準

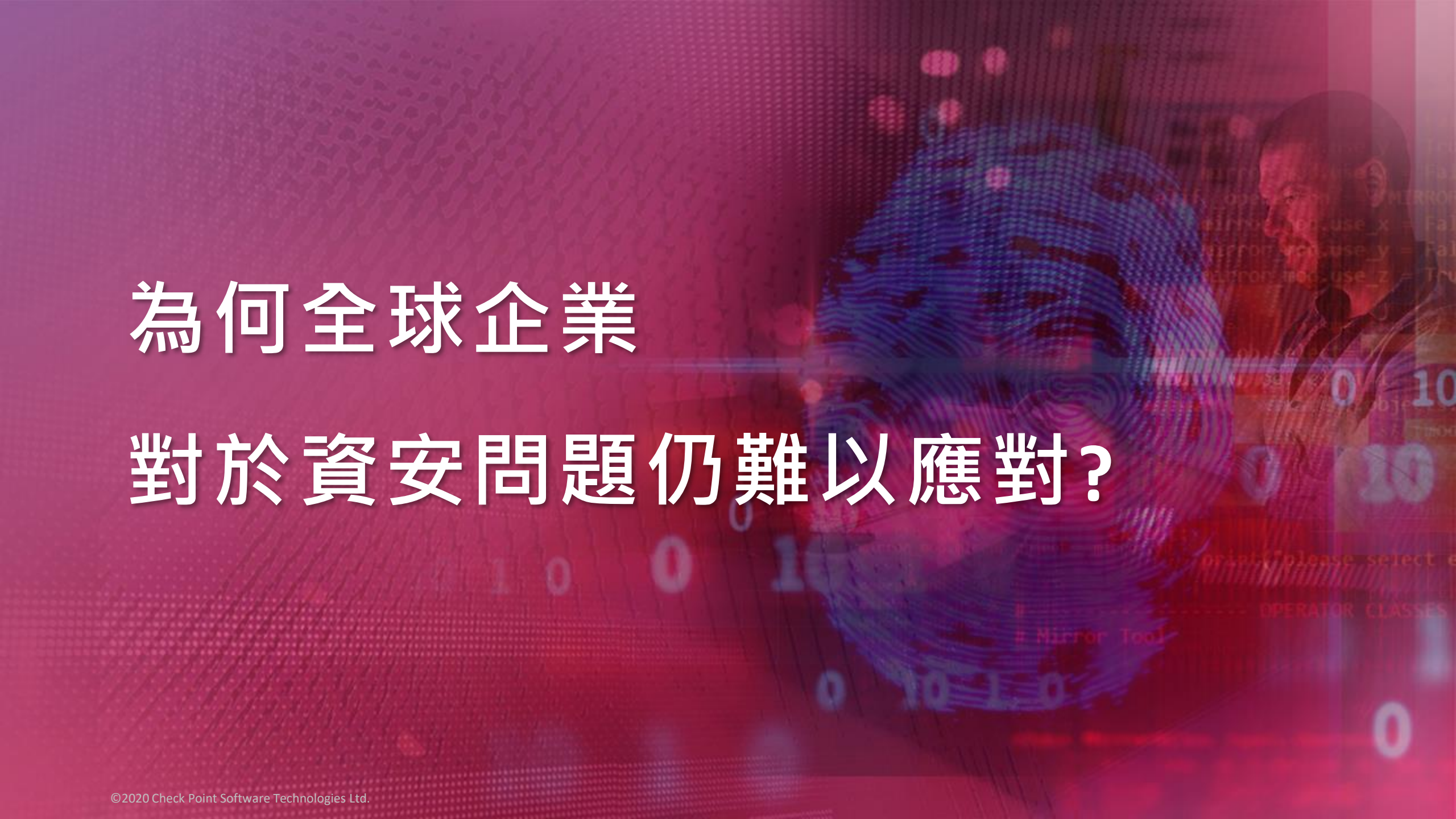


因應『新常態』後的IT型態與資安挑戰



為何全球企業

對於資安問題仍難以應對?



每個企業都有資安計畫...

直到他們被 入侵之後!

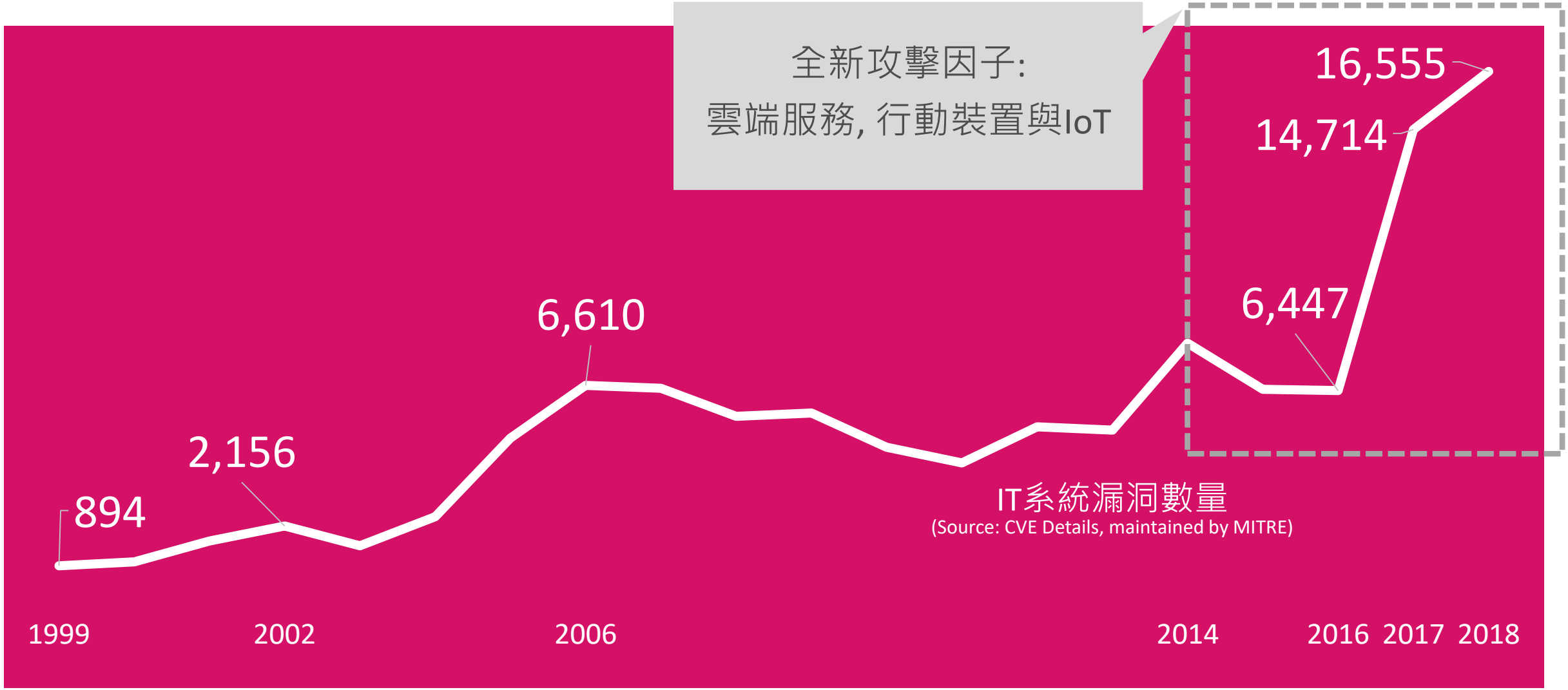
cp<r>
CHECK POINT RESEARCH

潛藏長達17年的嚴重漏洞

可自主增生(Wormable)影響其他伺服器

CVSS 10分滿分-建議即時修補

過去數年間系統漏洞問題急遽增加2.5倍!



現況IT環境已經完全改變

使用者應用完全無邊界，有效控管更為困難

傳統邊際網路
資料中心

遠距辦公與移動使用者
無邊界存取

多雲平台服務
混合雲與雲應用程式

BYOD以及行動化
IoT應用

安全攻擊面向也愈趨多元寬廣

SURFACES

VECTORS

邊界網路

移動使用者

雲端服務

行動裝置

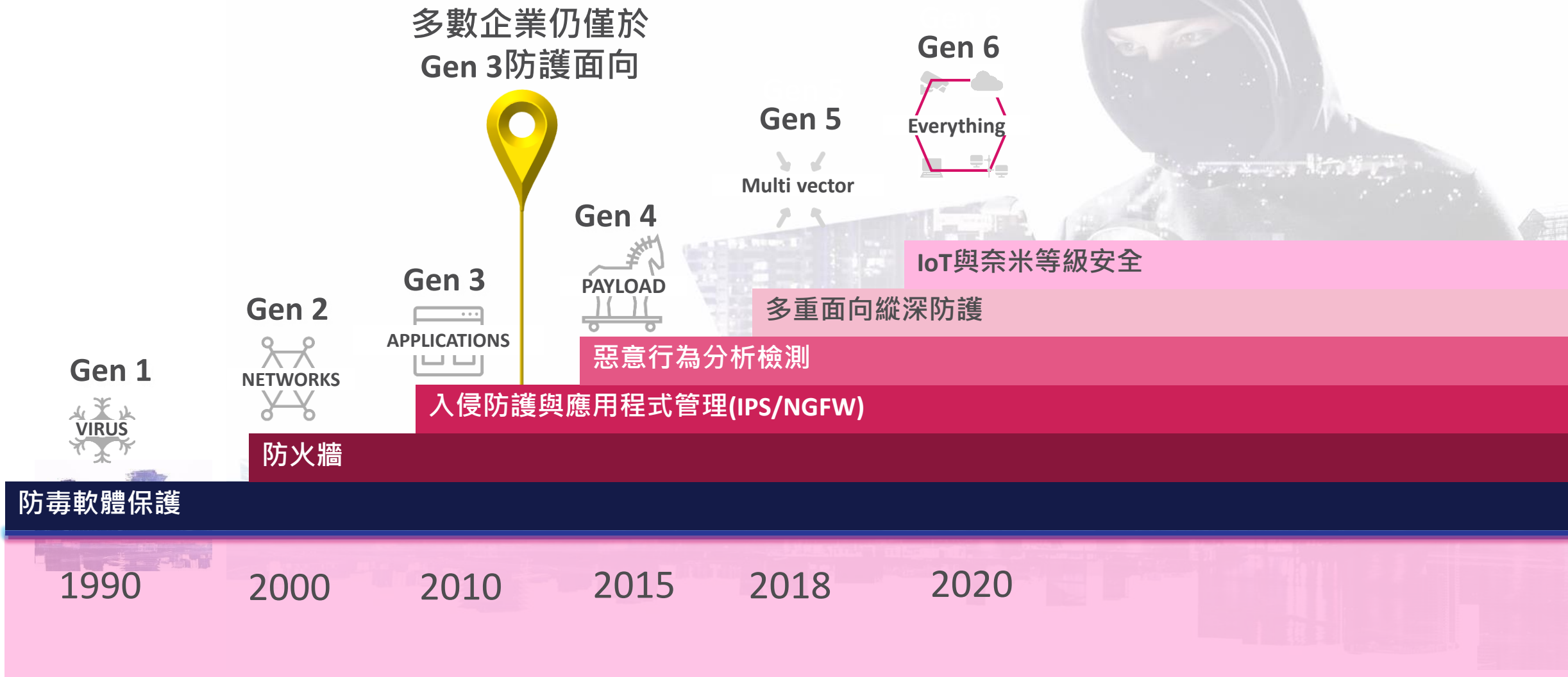
郵件		Exchange	Exchange	Exchange
網路				
檔案交換	box	box	box	box
惡意釣魚				
中間人攻擊		Malicious Networks		Malicious Networks
行動惡意程式				

#1 導入資安方案的考量面向

主要仍著重於安全偵測!

如果接受以偵測為主的安全方案
資安事件損失難以避免!

#2 – 安全方案與威脅現況的程度差異



#3 – 複雜的管理機制與人力資源匱乏

多重安全解決方案

=

疊床架屋的拼裝安全架構

Source: Former CIA director Gen (Ret) David H. Petraeus, CyberTech, Jan 2018

不同的安全方案之間無法有效協作與連動防禦
缺乏情資共享與即時自動化威脅因應措施

Source: David DeWalt/General Petraeus

未來可預見更加複雜的IT安全管理問題

Check Point®
SOFTWARE TECHNOLOGIES LTD

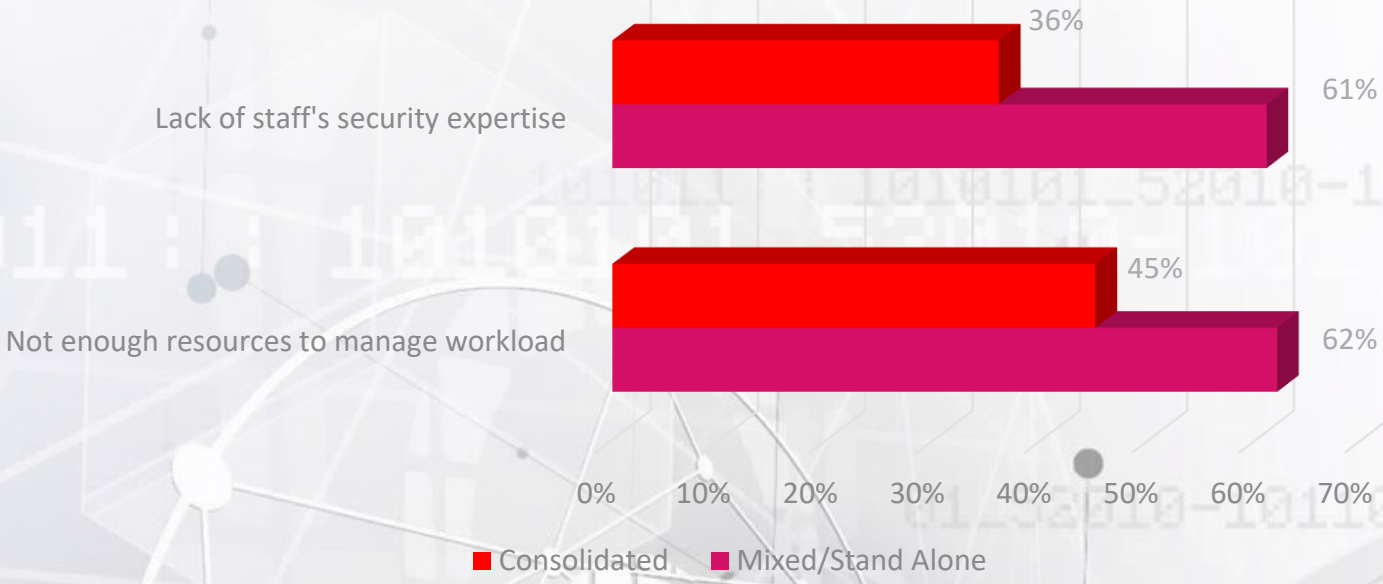
THAT'S TAKE A 10 MINS BREAK!

CHECK POINT
INFINITY NEXT

跨世代安全架構藍圖

企業部署安全方案的風險與挑戰

What challenges does your organization face in improving security efficiency



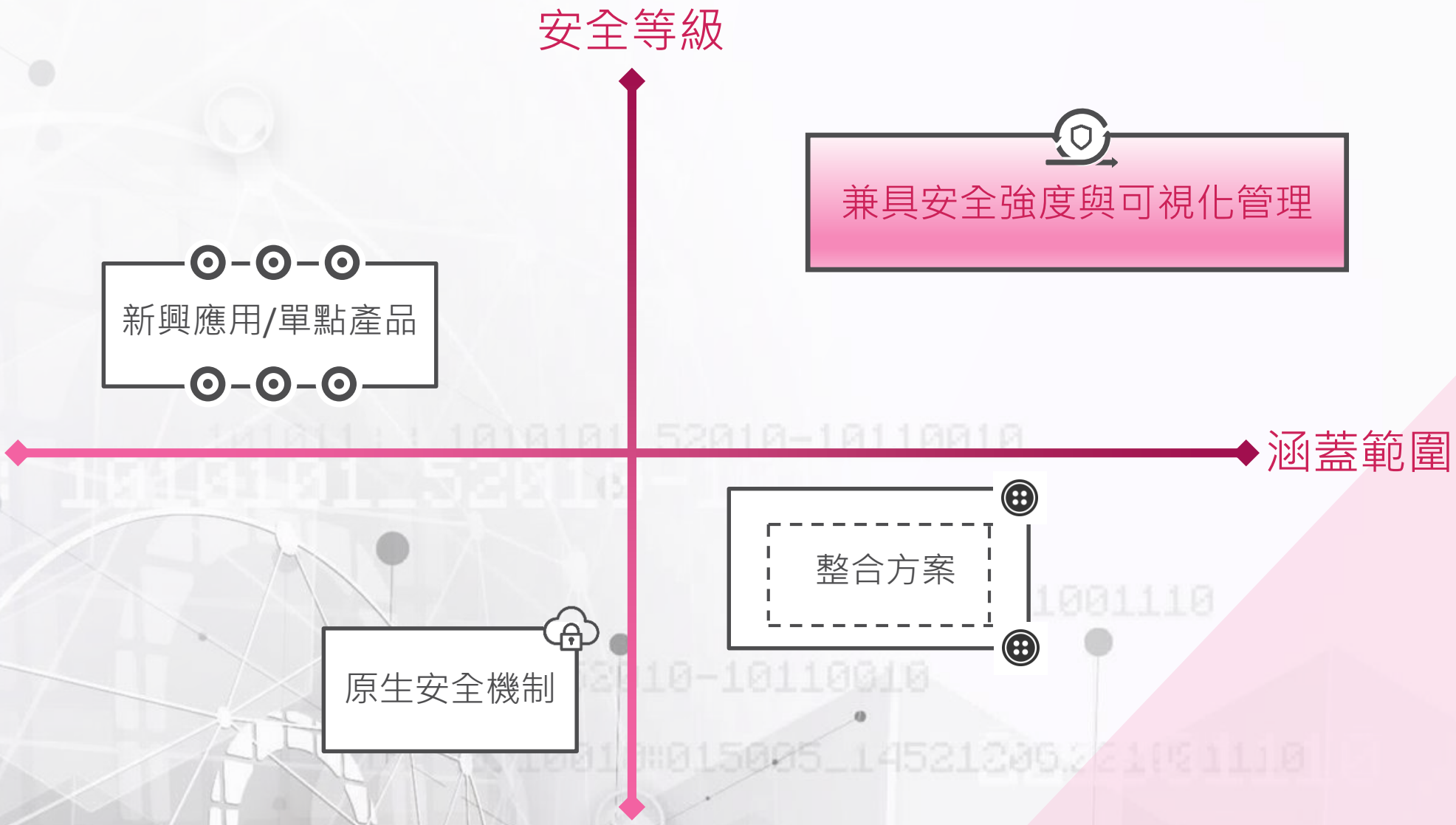
主要挑戰包括:

55% 缺乏人力資源

52% 缺乏產業與技術經驗

45% 多重供應商整合

未來安全投資與架構規劃考量



新世代企業資安原則與目標

即時防護能力

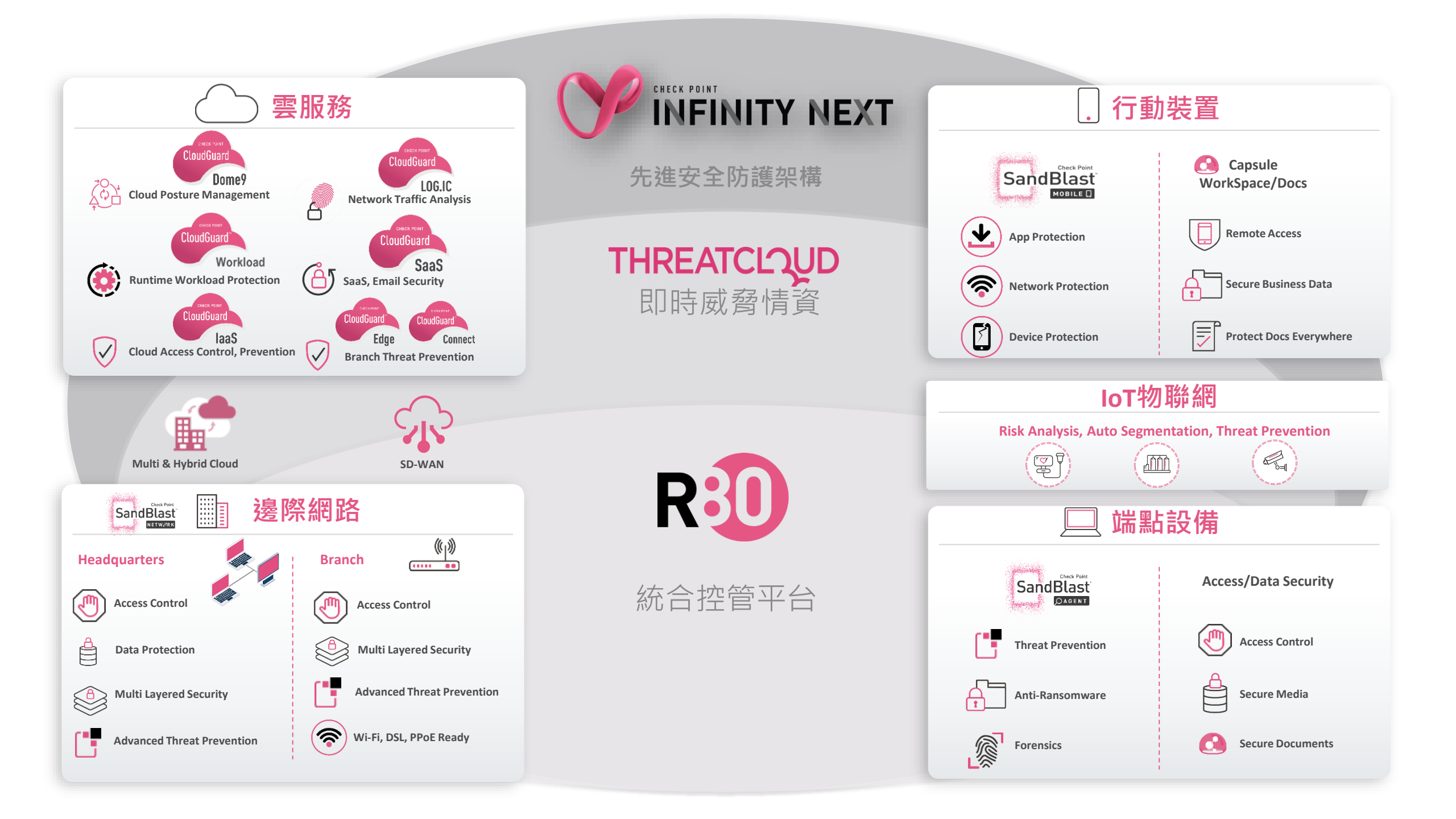
阻擋影響數位資產的威脅
監控偵測並告警

敏捷性與動態

可配合環境迅速調整
支援現況與未來的IT投資

統合控管與合規

一致化的安全政策基準
確保資安機制有效性


雲服務
CloudGuard Dome9
Cloud Posture Management
CloudGuard LOG.IC
Network Traffic Analysis
CloudGuard Workload
Runtime Workload Protection
CloudGuard SaaS
SaaS, Email Security
CloudGuard IaaS
Cloud Access Control, Prevention
CloudGuard Edge
CloudGuard Connect
Branch Threat Prevention
Multi & Hybrid Cloud
SD-WAN
CHECK POINT
INFINITY NEXT
先進安全防護架構
THREATCLOUD
即時威脅情資
R80
統合控管平台
行動裝置
SandBlast MOBILE
App Protection
Network Protection
Device Protection
Capsule WorkSpace/Docs
Remote Access
Secure Business Data
Protect Docs Everywhere
IoT物聯網
Risk Analysis, Auto Segmentation, Threat Prevention
端點設備
SandBlast AGENT
Threat Prevention
Anti-Ransomware
Forensics
Access/Data Security
Access Control
Secure Media
Secure Documents
邊際網路
SandBlast NETWORK
Headquarters
Access Control
Data Protection
Multi Layered Security
Advanced Threat Prevention
Branch
Access Control
Multi Layered Security
Advanced Threat Prevention
Wi-Fi, DSL, PPoE Ready

INFINITY NEXT:

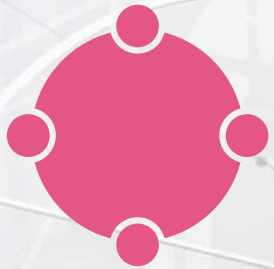
因應數位轉型而生的安全架構

多雲應用

針對所有工作負載和服務的自適應保護

IOT與行動載具

探測與保護所有物連網裝置



邊際網路

配合虛擬與實體網路環境與應用

即時防護能力

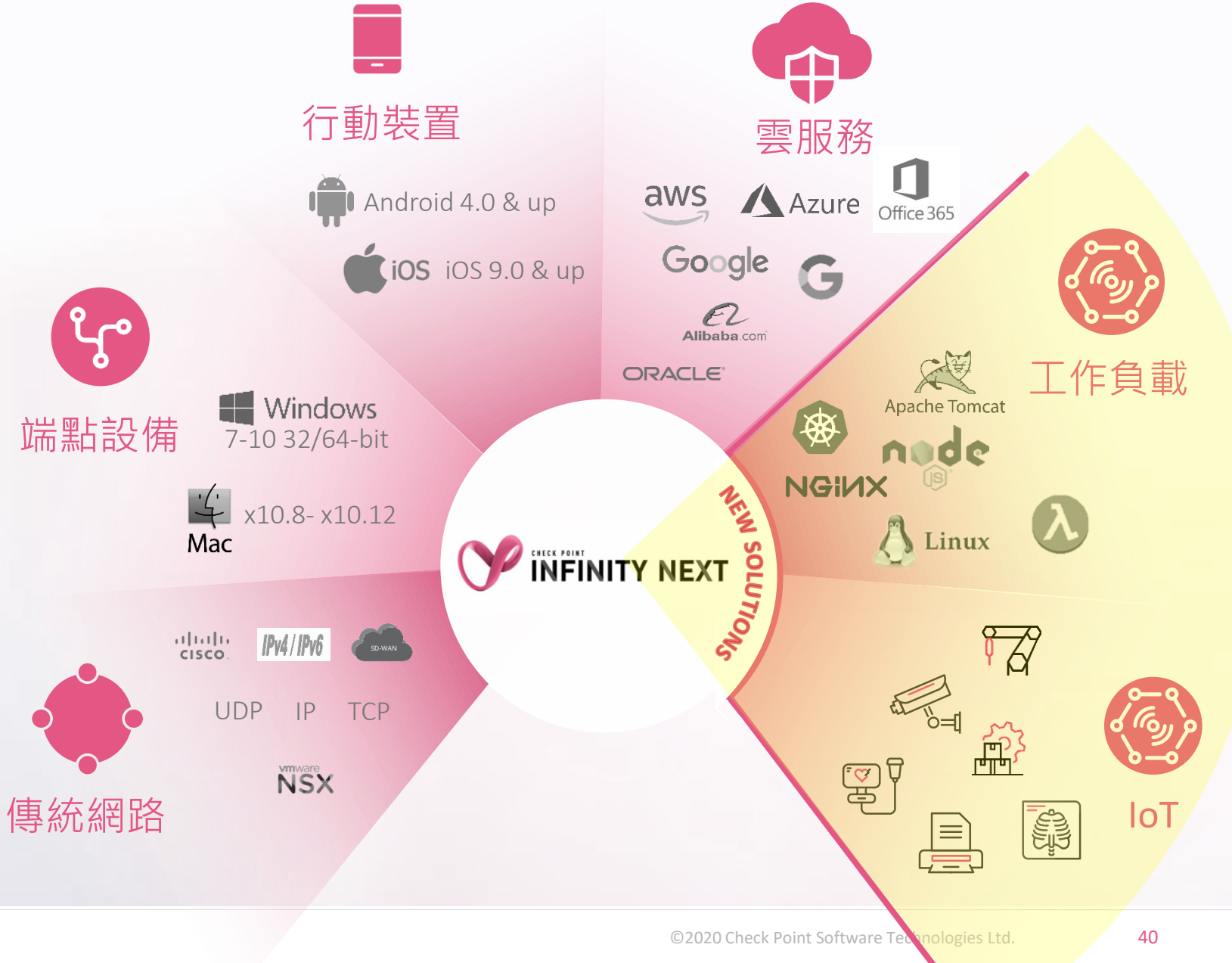
擁有60+安全檢測服務與技術

1 已知威脅防護
2 未知威脅防護
3 零信任存取
4 安全強化與合規
5 源碼與API安全

敏捷性與動態

可防護50+ IT資產類型

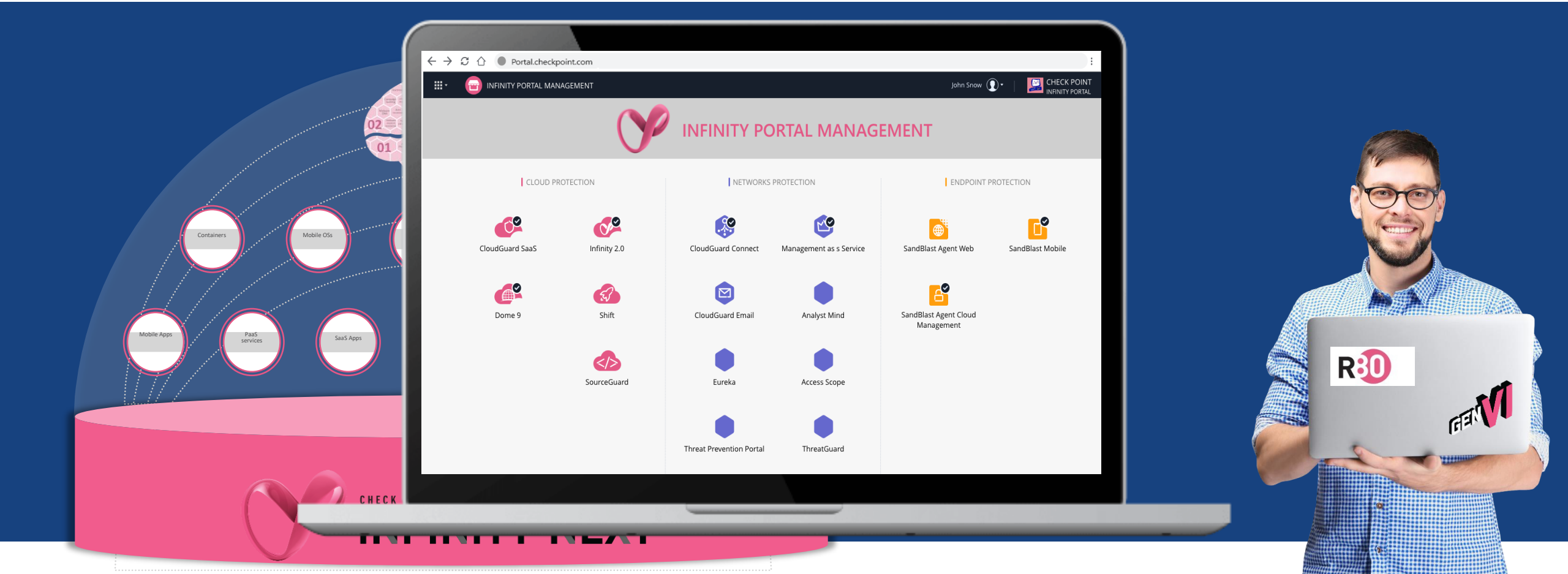
確保數位轉型安全效益



CHECK POINT
INFINITY NEXT

統合控管與合規

單一平台與高可視性報表

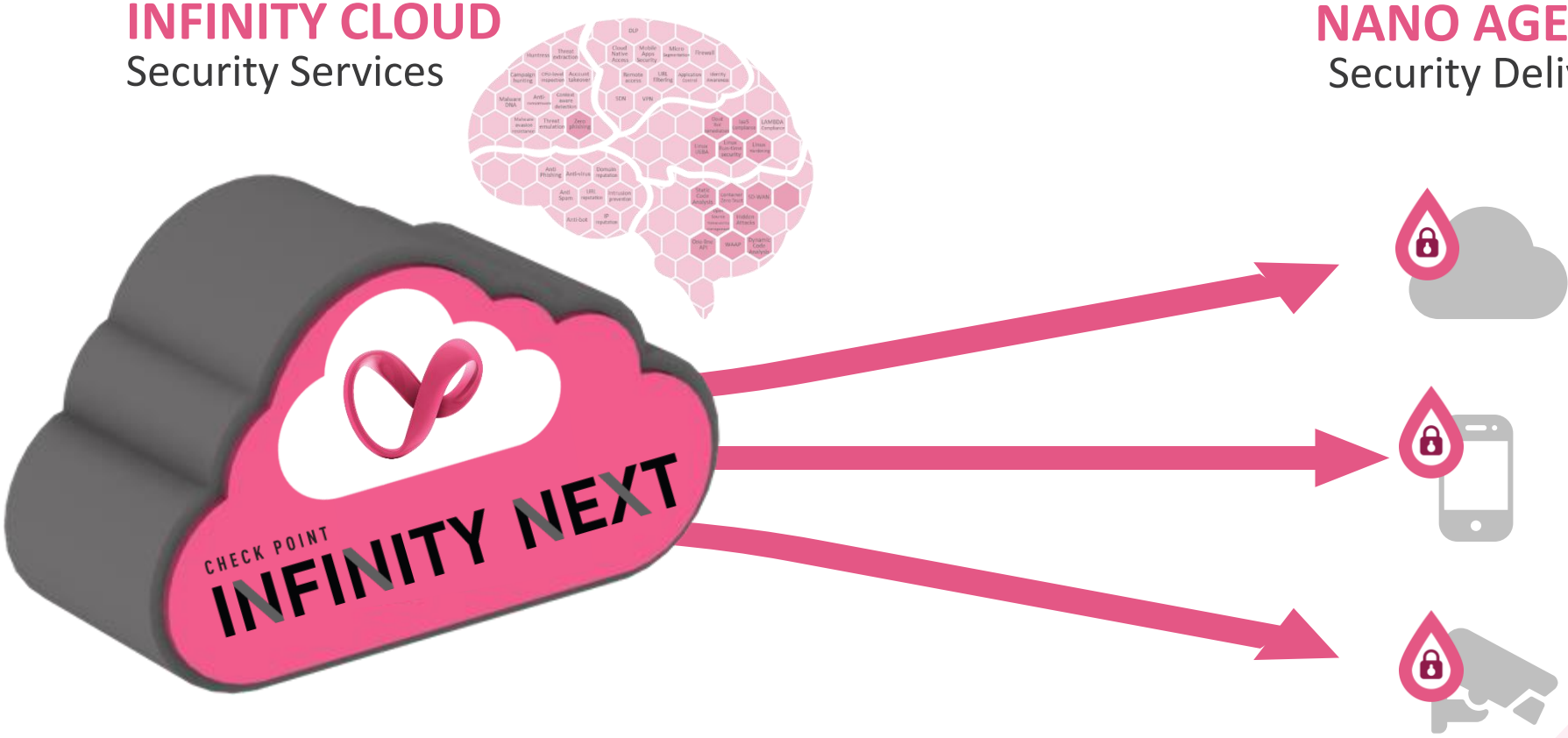


Check Point
SOFTWARE TECHNOLOGIES

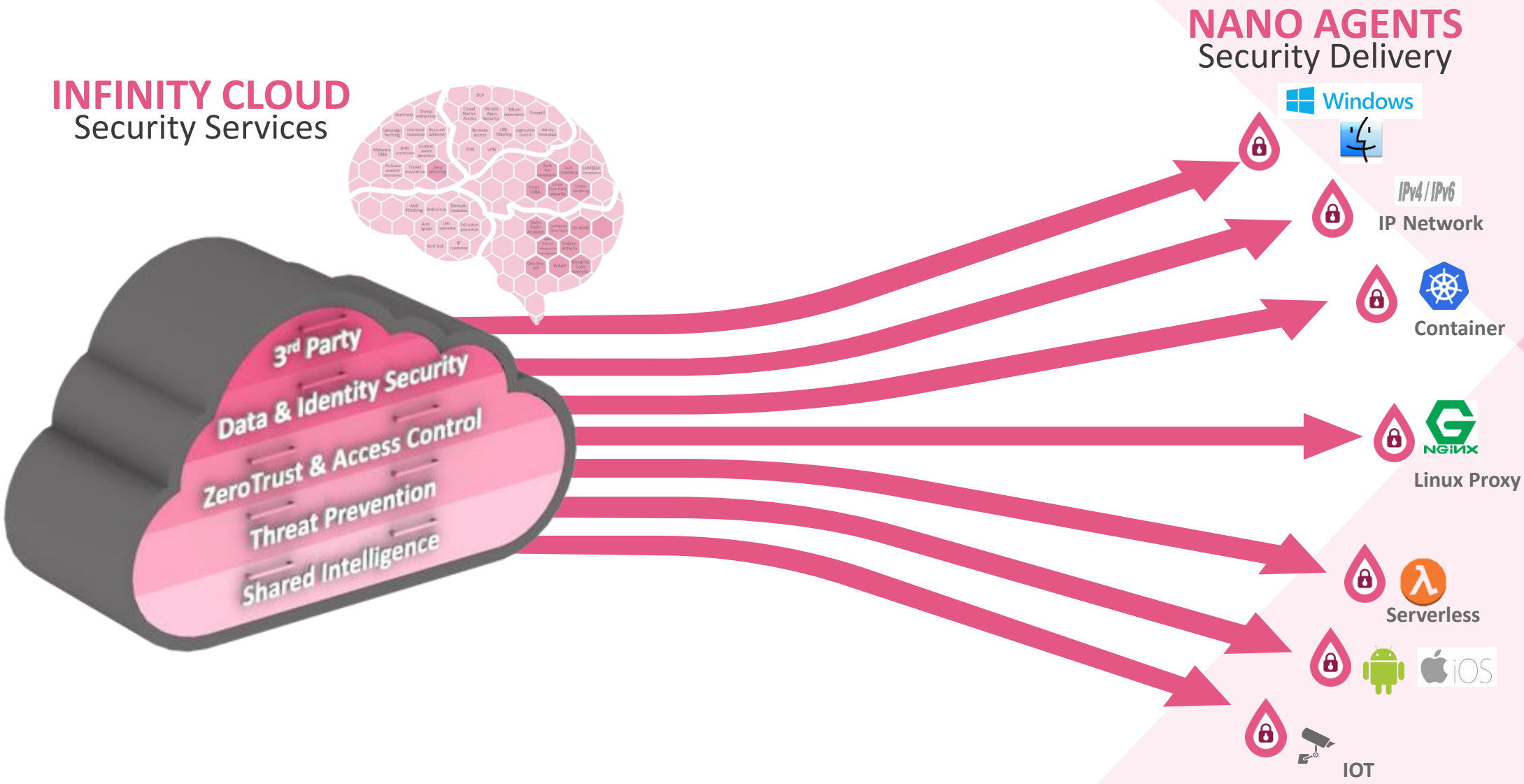
INFINITY NEXT - NANO AGENT安全架構(IoT On-device防護)

INFINITY CLOUD
Security Services

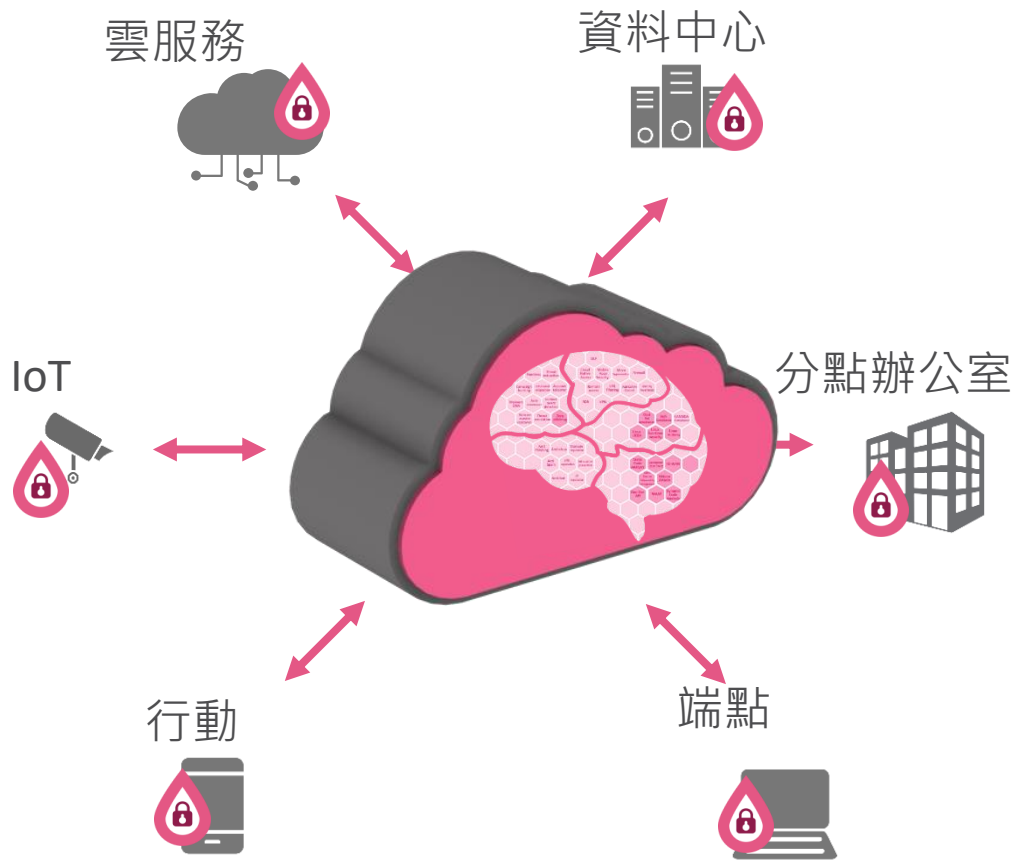
NANO AGENTS
Security Delivery



INFINITY NEXT - 最具敏捷性與安全涵蓋能力



INFINITY NEXT – 最符合未來需求的安全架構



- 最即時與完整的防護力
- 最高水平的SLA
- 低維運時間與人力
- **SECURE YOUR EVERYTHING**

CHECK POINT
INFINITY NEXT

雲端IoT與資料中心先進安全策略

應用無邊，安全無界

SECURITY EVERYWHERE

傳統資料中心

從緩速開發流程
走向應用為王
DEVSEOPS

地端自建應用

混合雲/多雲

S

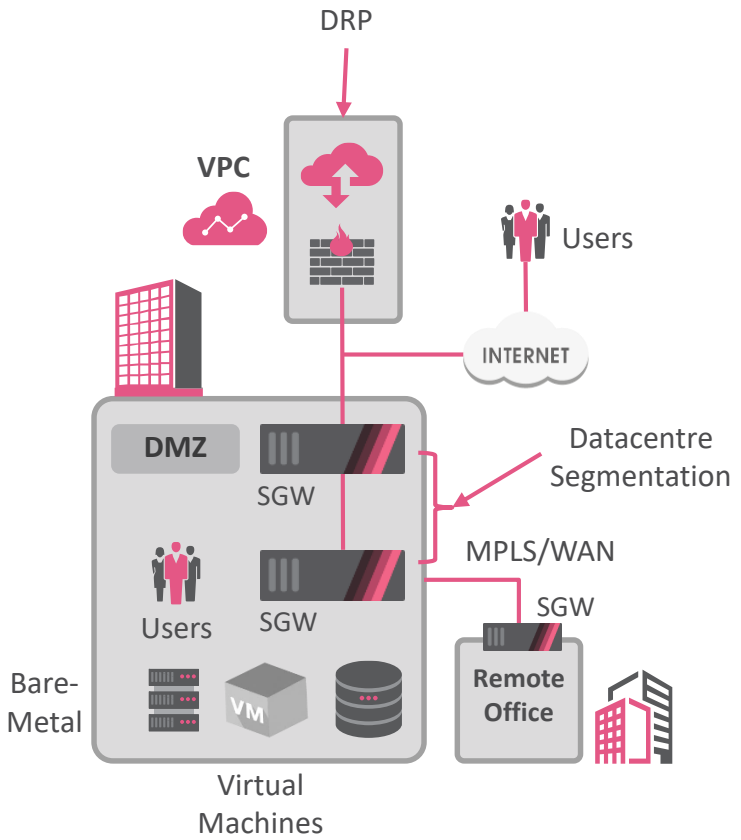
TO:

SaaS 服務

雲數位轉型與成熟度階段

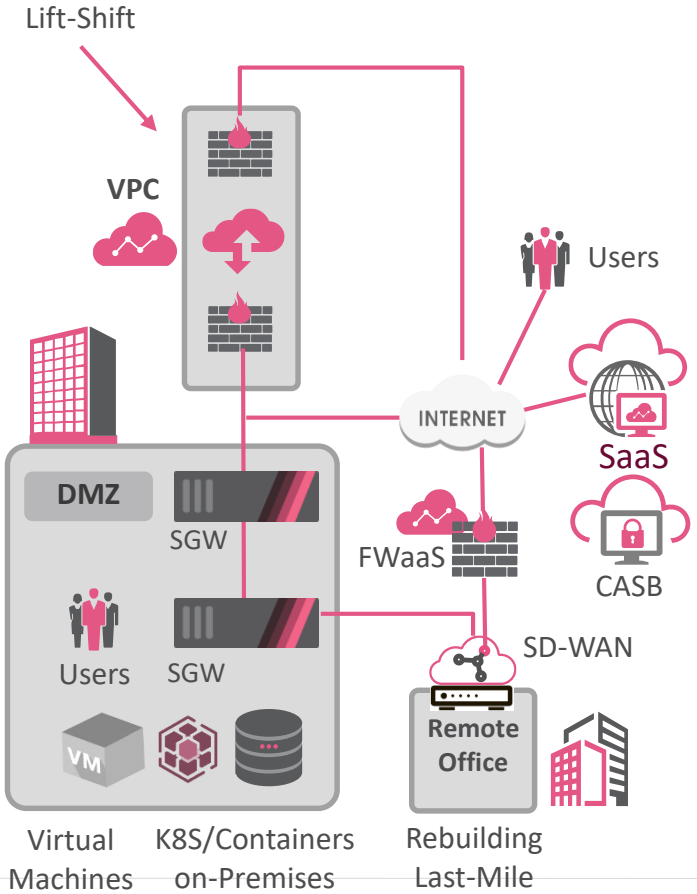
1

基礎建設為中心



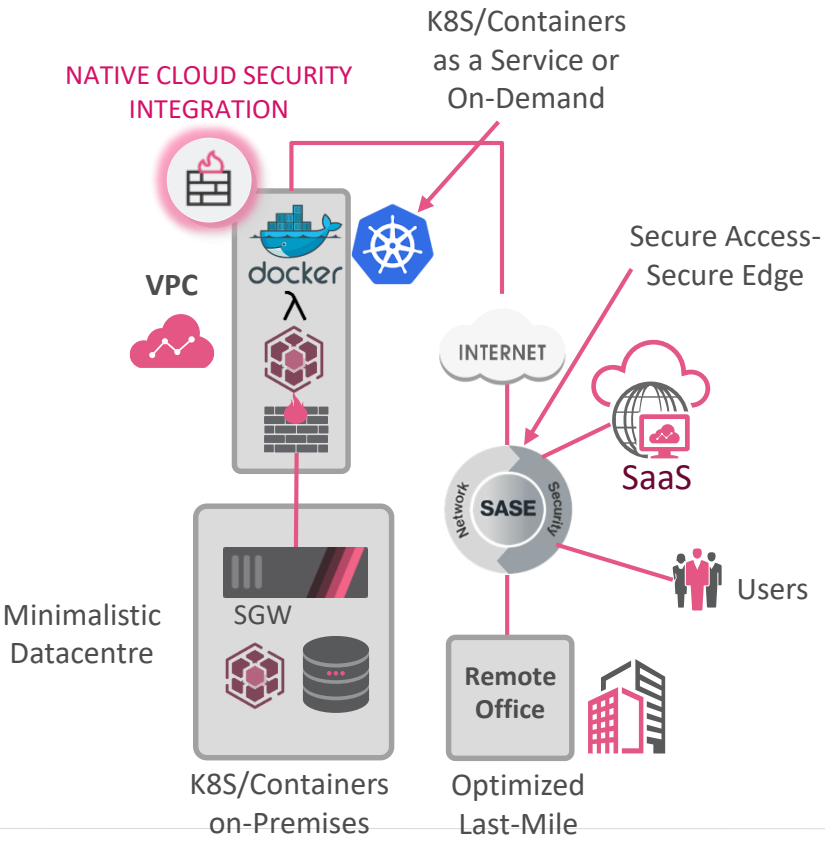
2

移轉至多雲以混合雲



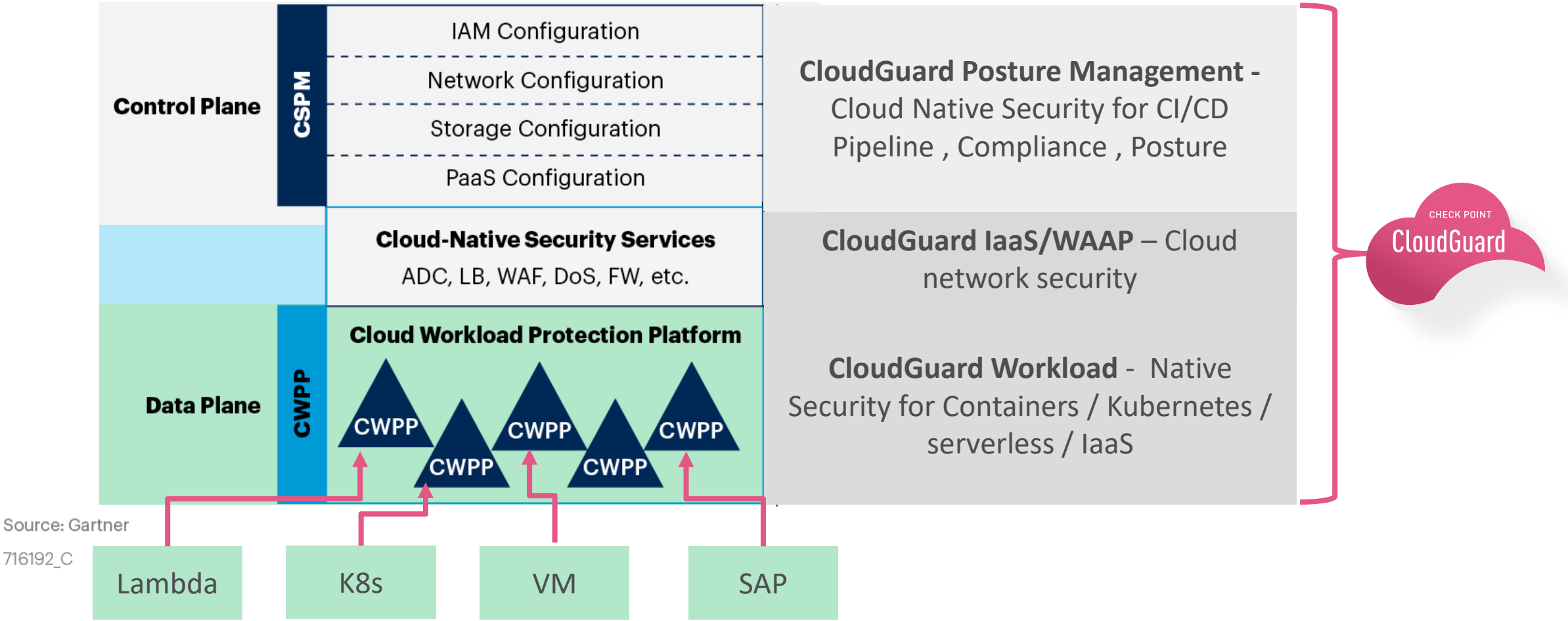
3

以雲為中心



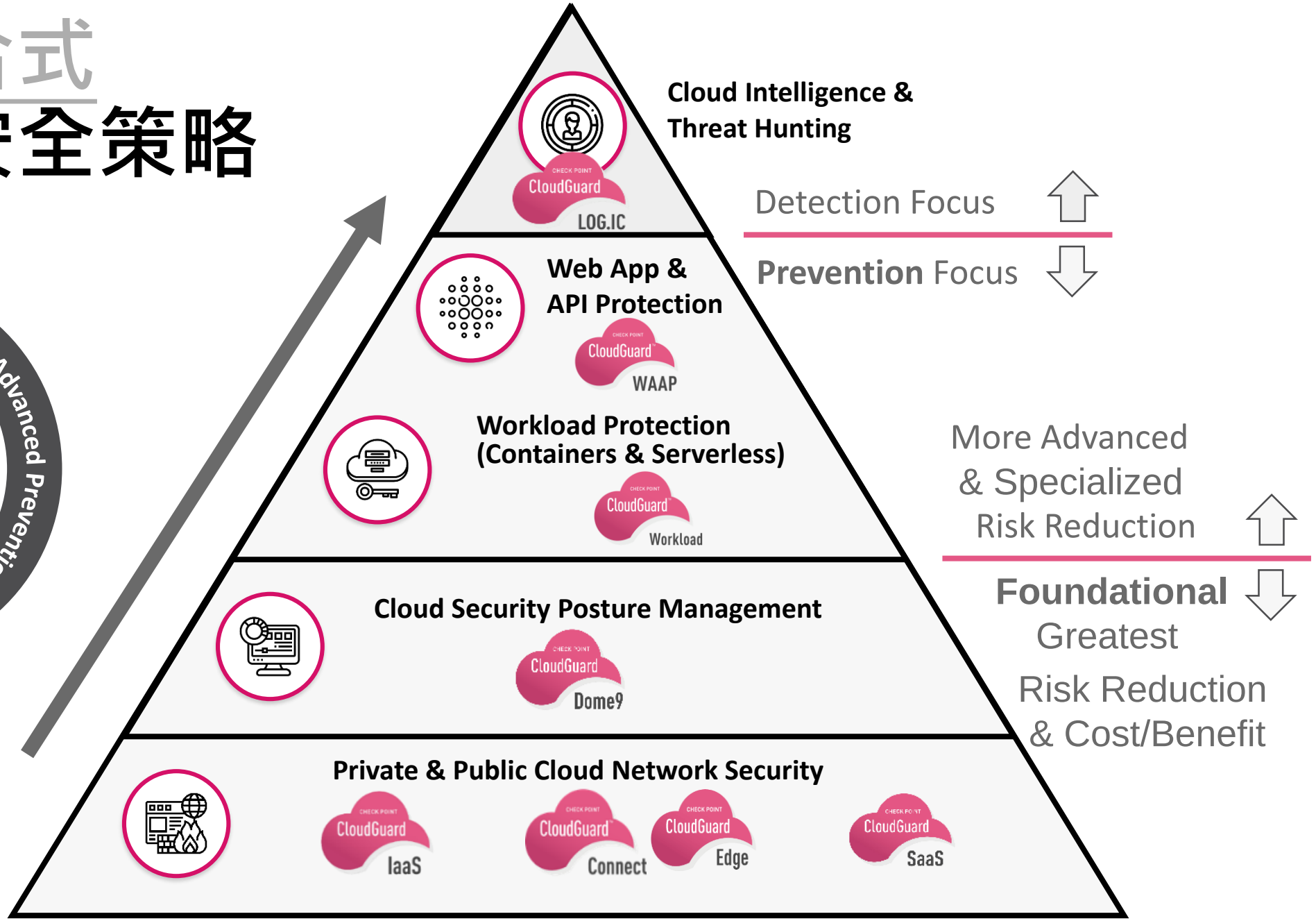
雲原生安全架構平台
Cloud-Native Application Protection Platform (CNAPP)

CWPP and CSPM Adjacency



Source: Gartner
716192_C

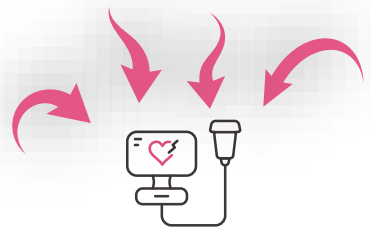
整合式
先進雲安全策略



*Source: Gartner

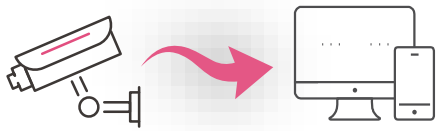
IoT 安全挑戰與風險

- 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

IT 重視: 資料保護

機敏性

完整性

可用性

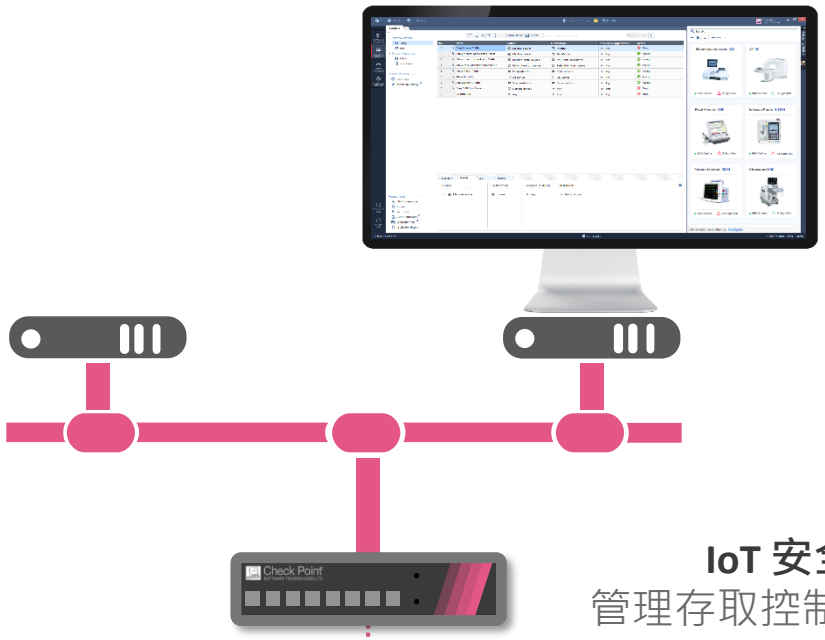
OT 重視: 流程保障

Check Point Infinity 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

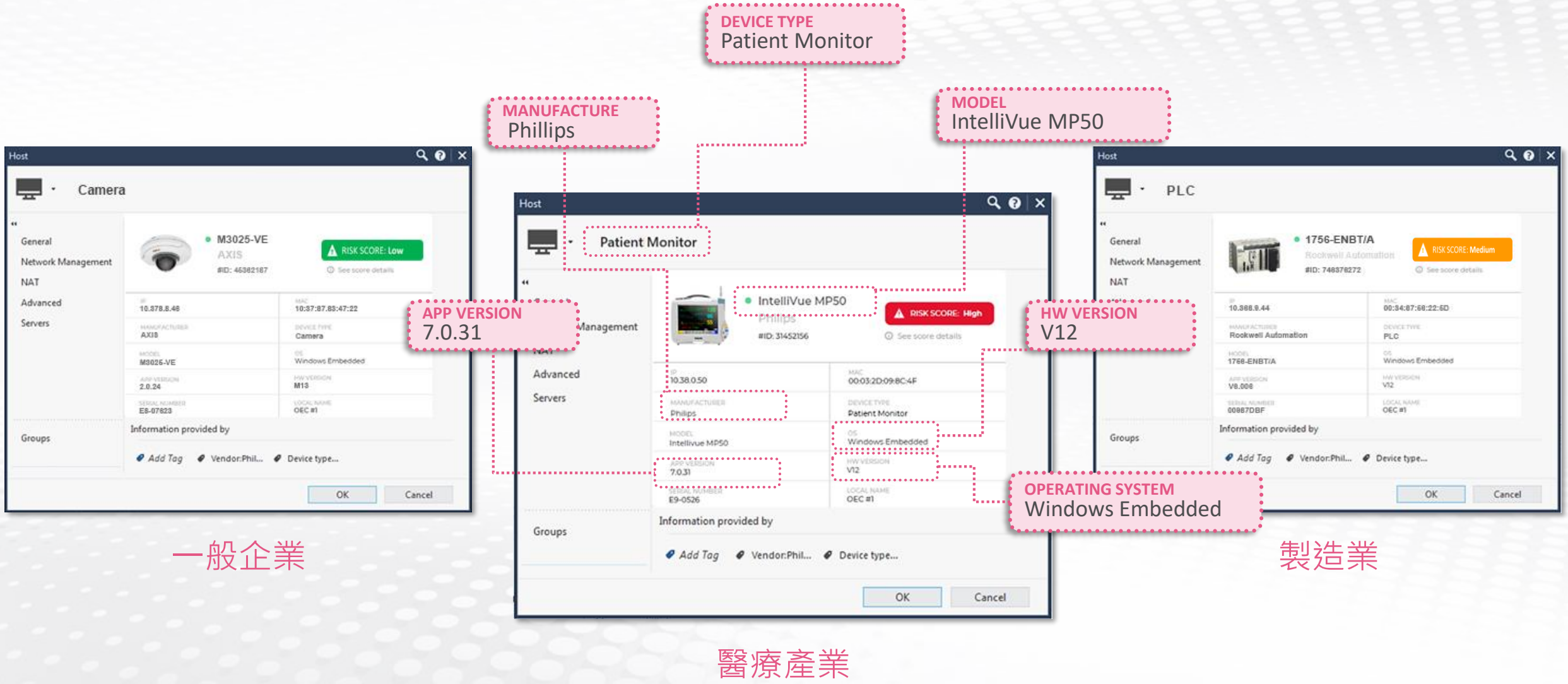


IoT 安全管控
IoT環境與設備完整管控與可視性

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



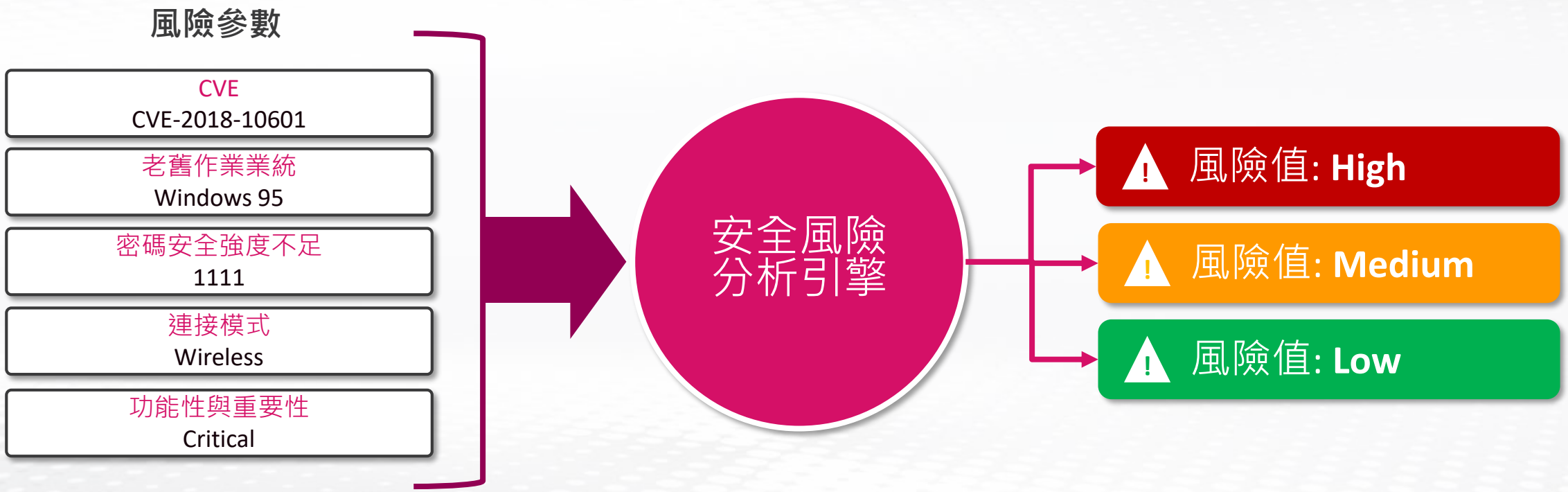
一般企業

醫療產業

製造業

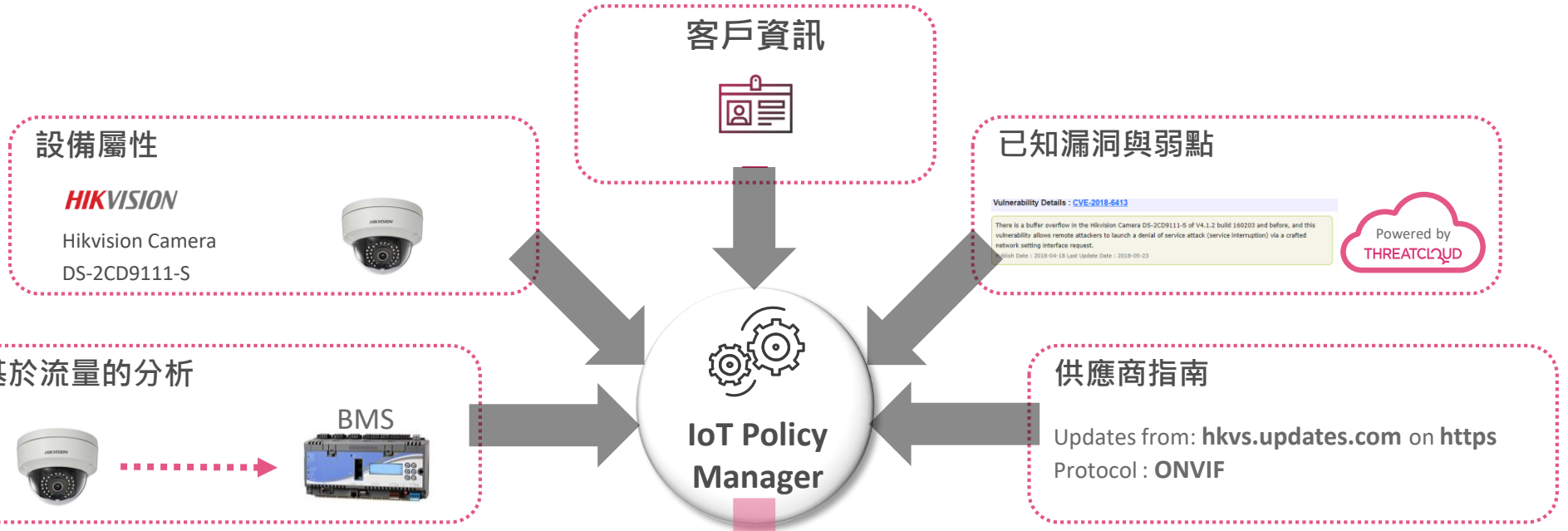
啟發性威脅分析引擎與安全可視性

獲取精準的風險評估於所有IoT與OT裝置

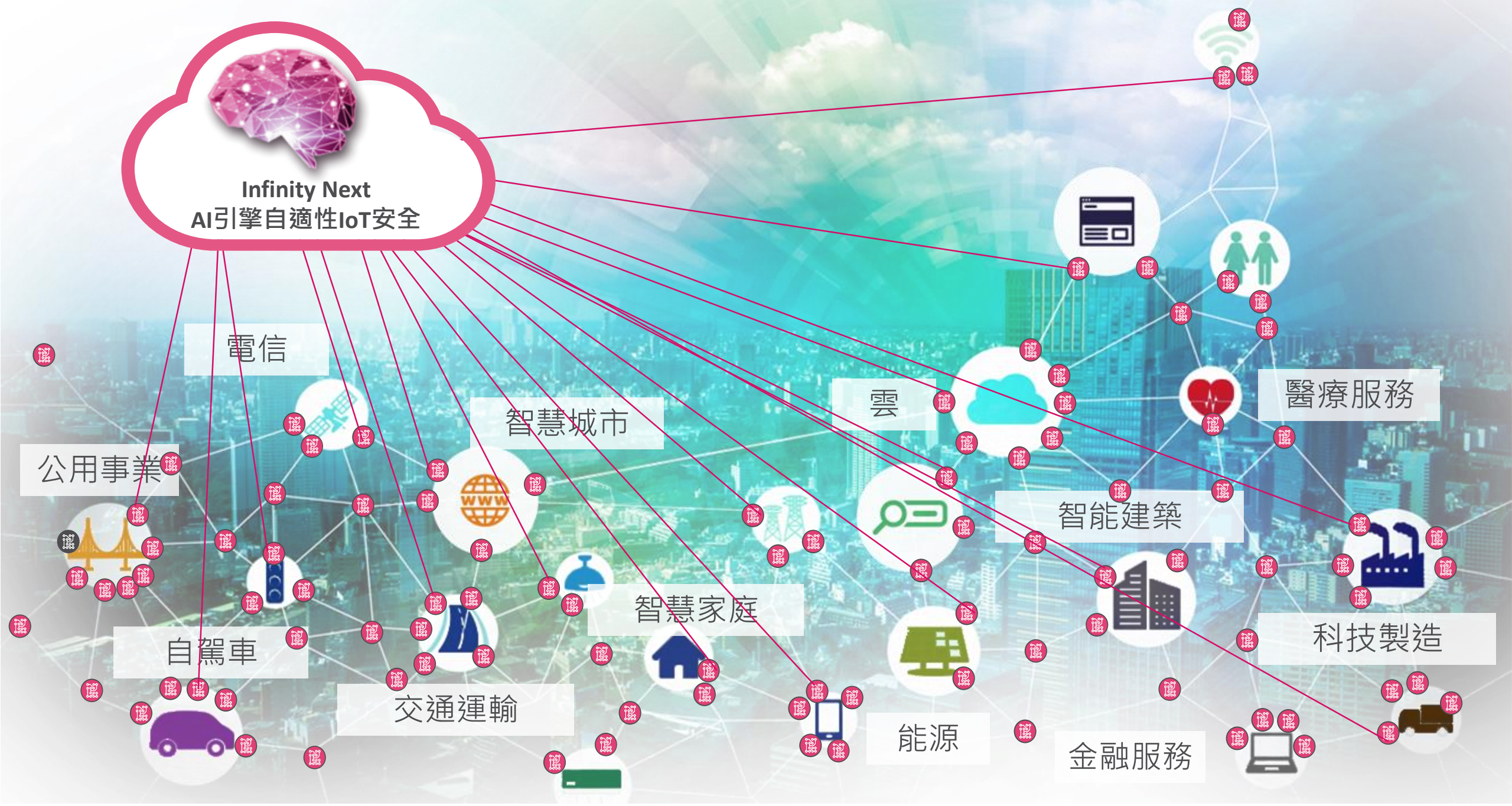


IoT感知式自動安全存取控管政策

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



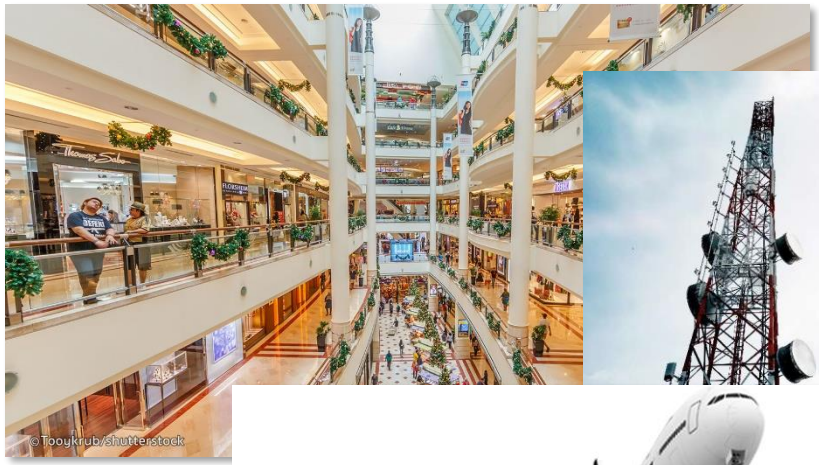
企業安全效能現況?

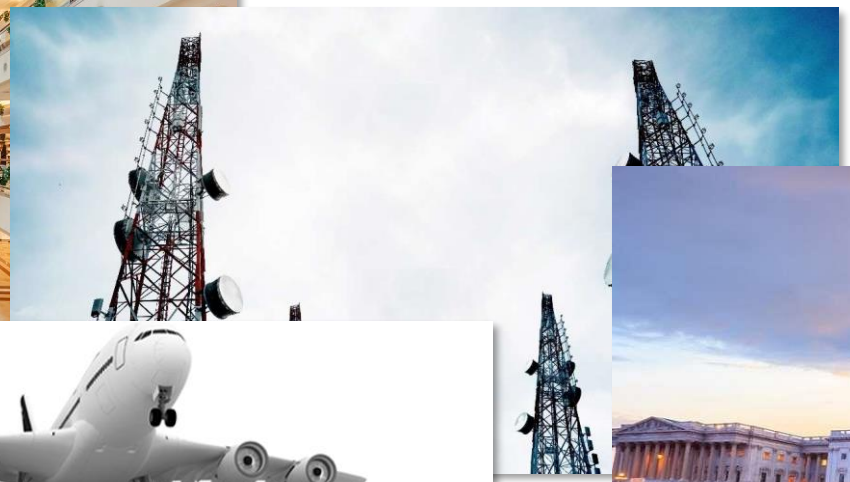
Check Point
SOFTWARE TECHNOLOGIES LTD

惡意威脅飛速成長...

企業現有的安全防護平台是否足以因應?

哪些產業將從高可擴充性架構中獲益?





政府機關與服務

交通運輸

以及所有數位化產業...

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

領先全球網路安全-Hyperscale叢集技術

Check Point Maestro

MAESTRO
先進硬體叢集與負載平衡技術

Check Point
SOFTWARE TECHNOLOGIES LTD

Check Point
SOFTWARE TECHNOLOGIES LTD

專利技術

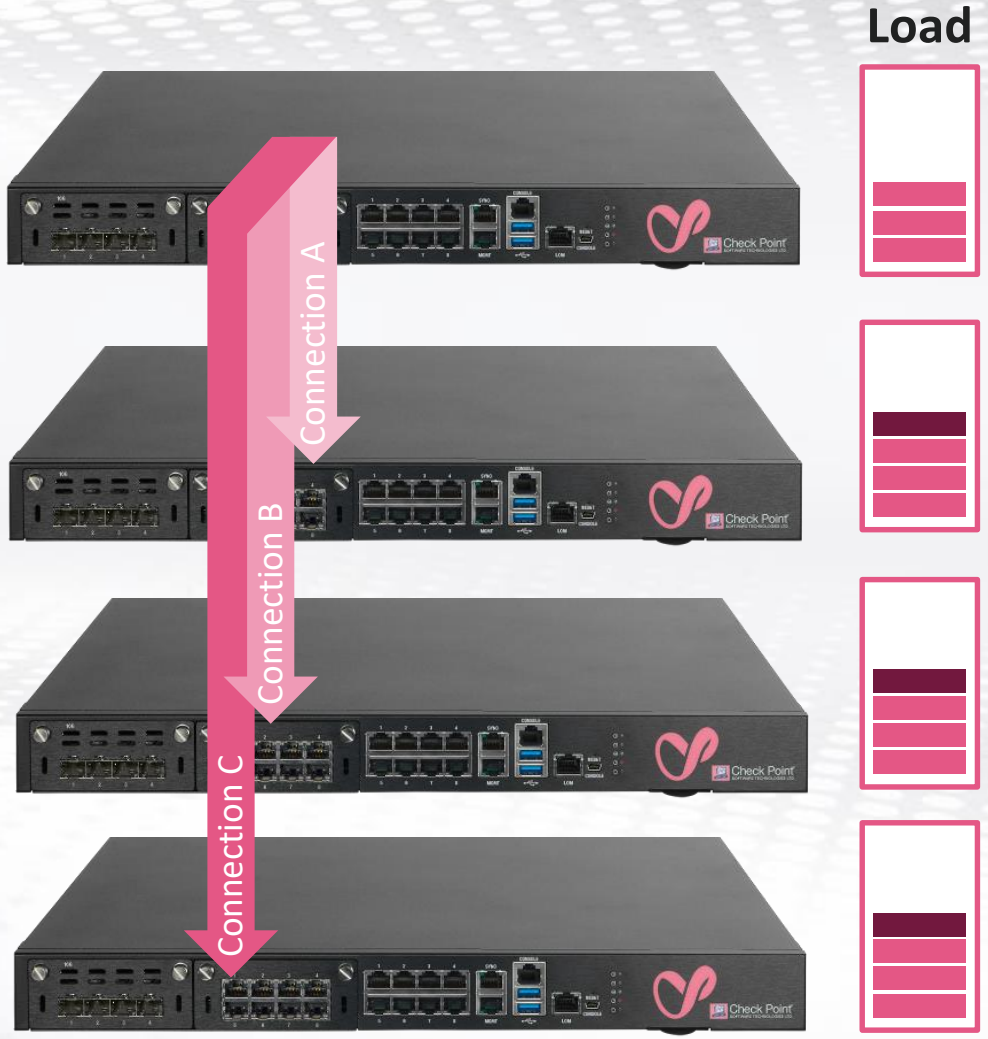
HyperSync

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



高效能叢集機制與動態備援擴充

Check Point
SOFTWARE TECHNOLOGIES LTD

傳統叢集

兩台設備

1 Gbps

MAESTRO ORCHESTRATION

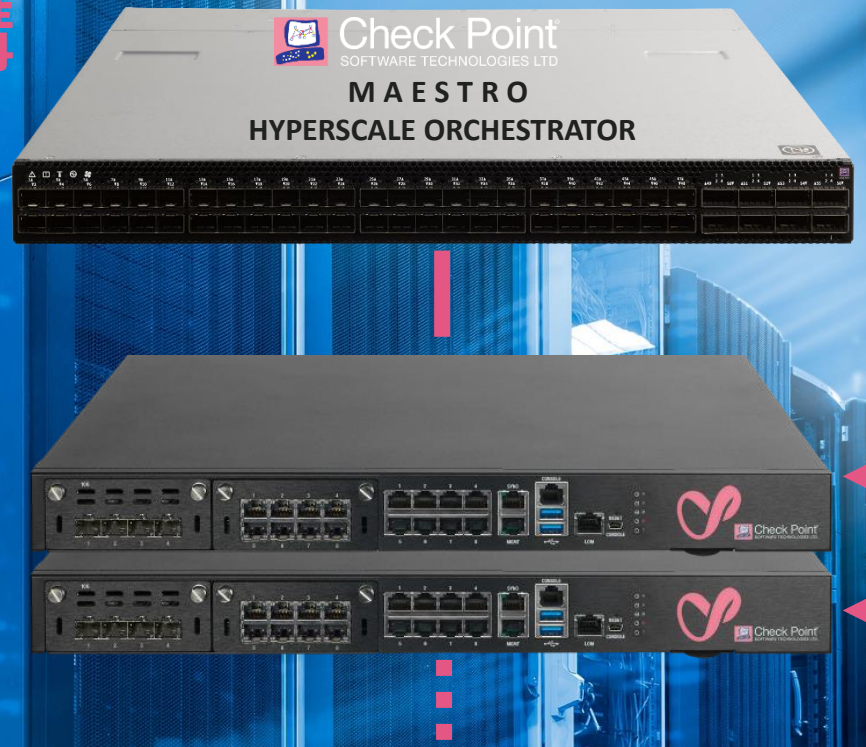
三台設備

3 Gbps

1 + 1 = 1 ⟵ 簡易對照 ⟶ **1 + 1 + 1 = 3**

應用案例說明

某客戶預先規劃
Maestro Ready架構



Active/Active

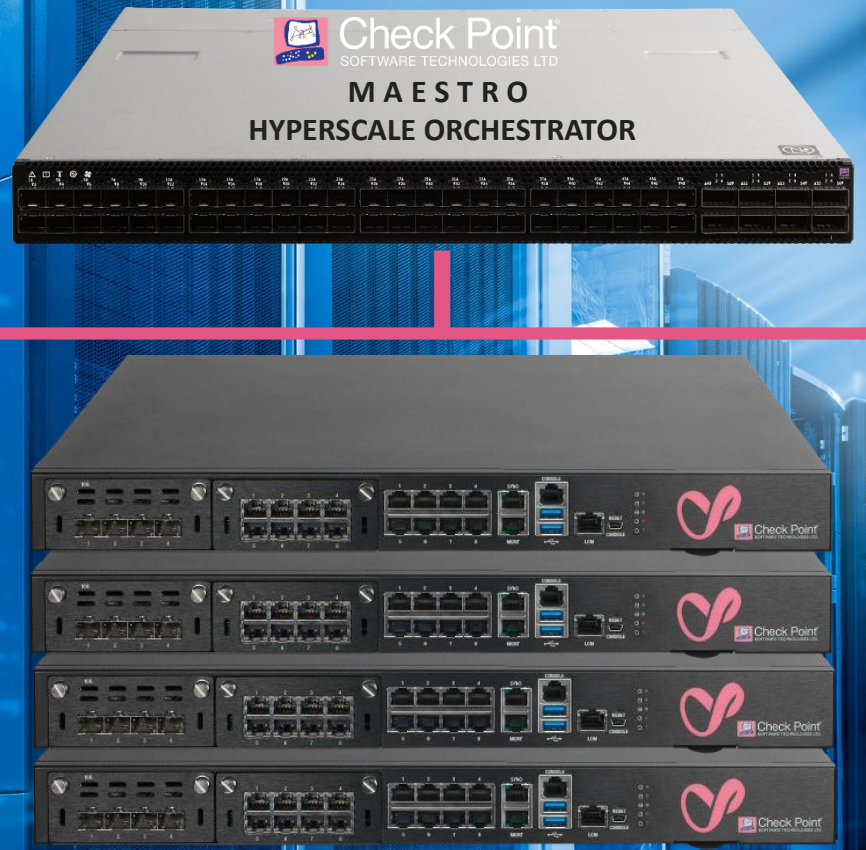
預先導入新世代安全叢集設計

某客戶預先規劃
Maestro Ready架構

Active/Active

數分鐘內即可擴充叢集並符合整合管理與成長需求

未來架構彈性高
橫向擴充能力佳



整合閘道

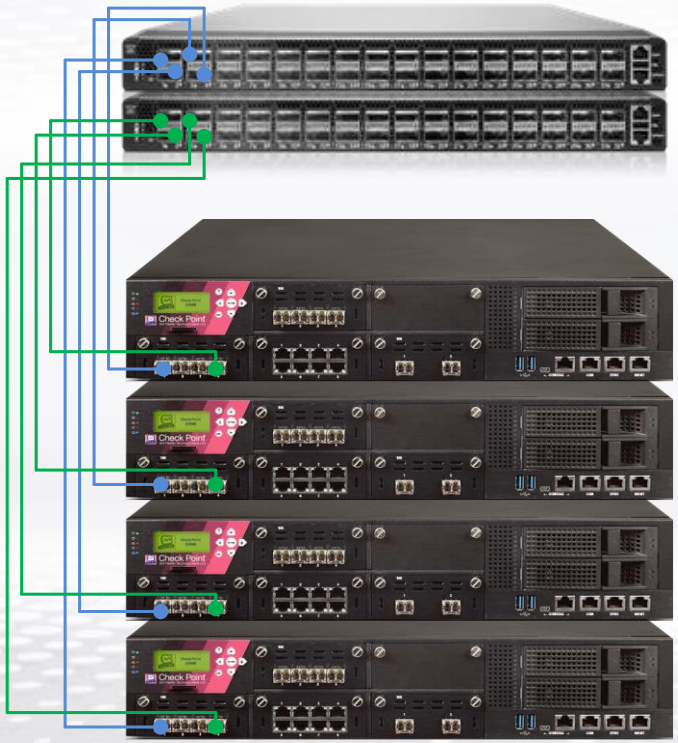
單一平台管理所有虛實網路閘道
高度效益與擴充彈性

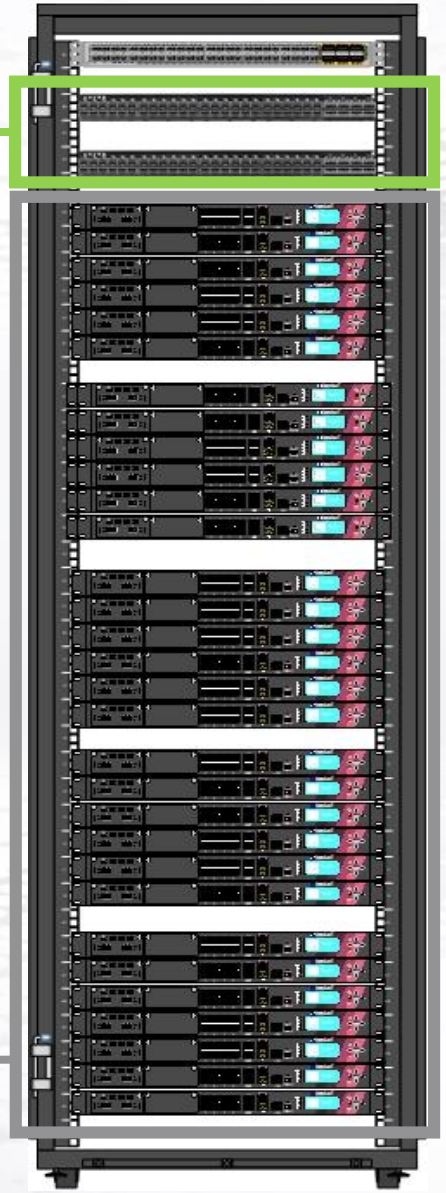
未來架構彈性高
橫向擴充能力佳

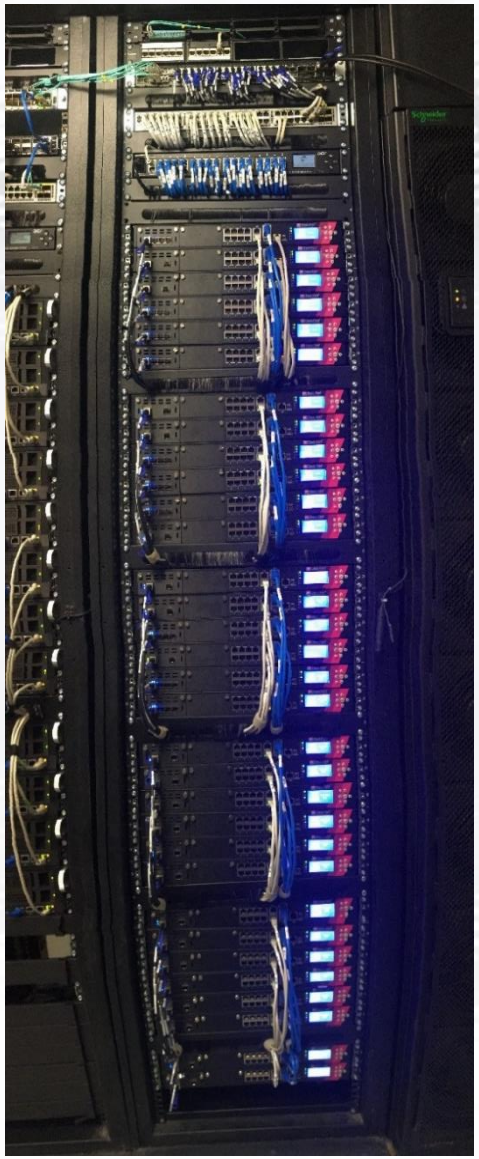
Auto-Scaling

動態調度安全資源於不同的安全群組設定(Security Group)

Orchestration Layer







Compute Resources

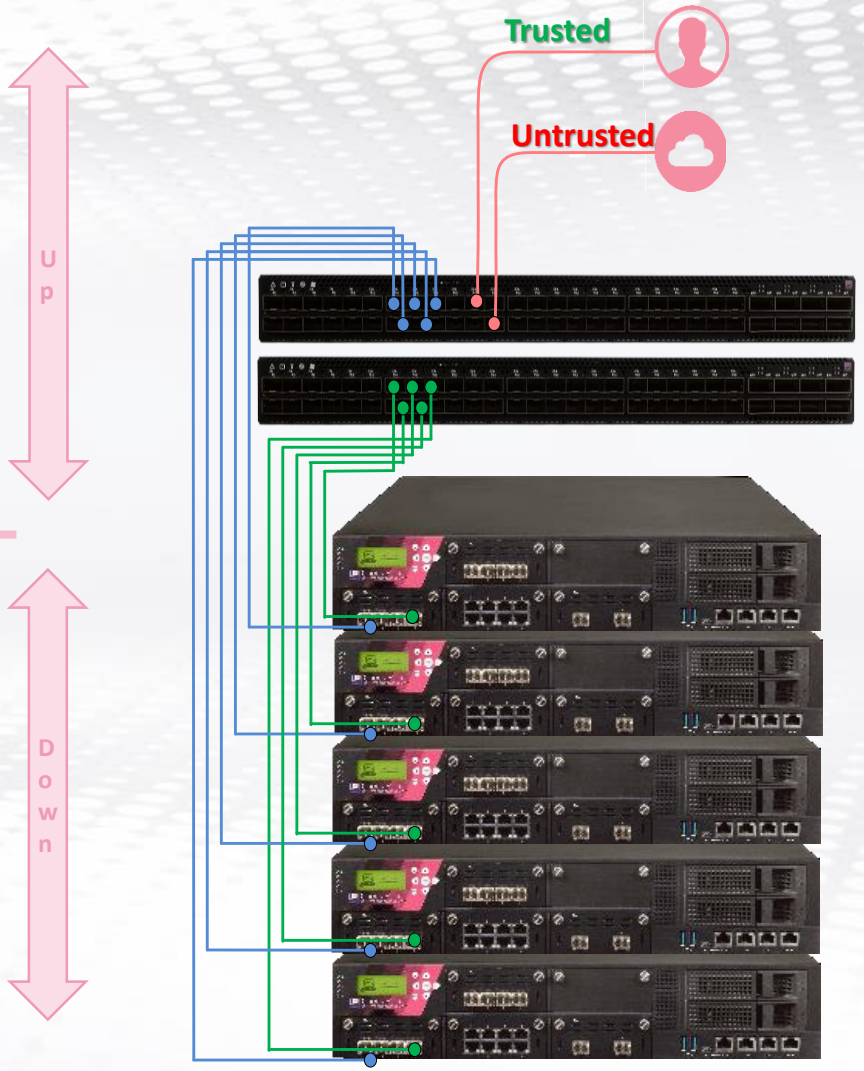
實體接線示意圖

UPLINKS

連接trusted & untrusted zones, 連接至管理介面包括SmartDashboard, WebUI, CLISH, 等。

DOWNLINKS

每台設備(10G)對接至Maestro設備(透過DAC)



https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk138233

全面APT安全防護建議架構

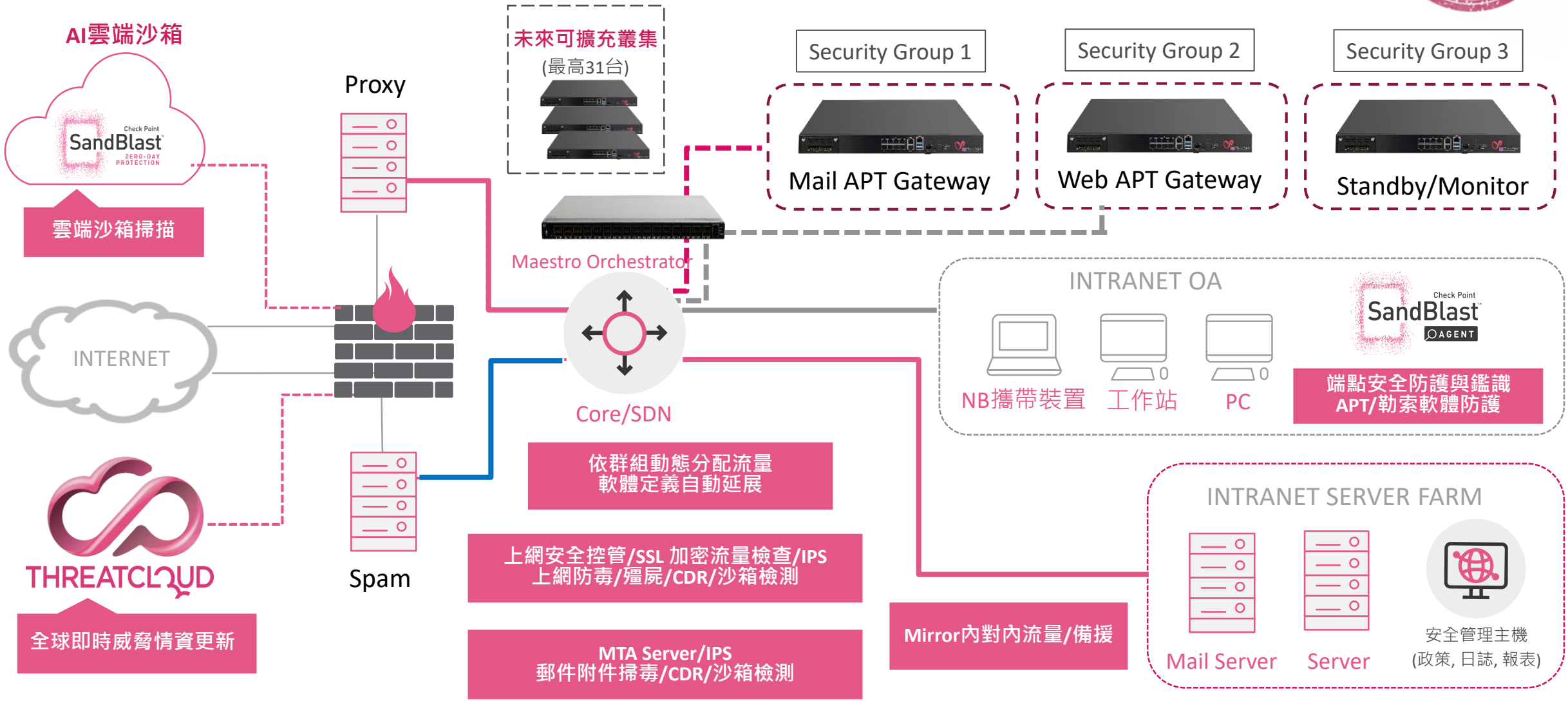
Web/Mail防護與高靈活性動態備援與擴充架構

架構彈性: Prevention/Detect

備援方式: 動態依環境需求設定

全面APT防護功能無盲點

BEST PRACTICE



2019 NSS LABS APT 防護測試 – 榮獲最高攔阻率
BREACH PREVENTION SYSTEM (BPS) TEST

NSS Labs 2017 APT防護測試-最佳防護力與性價比

Breach Prevention Systems (BPS) Test

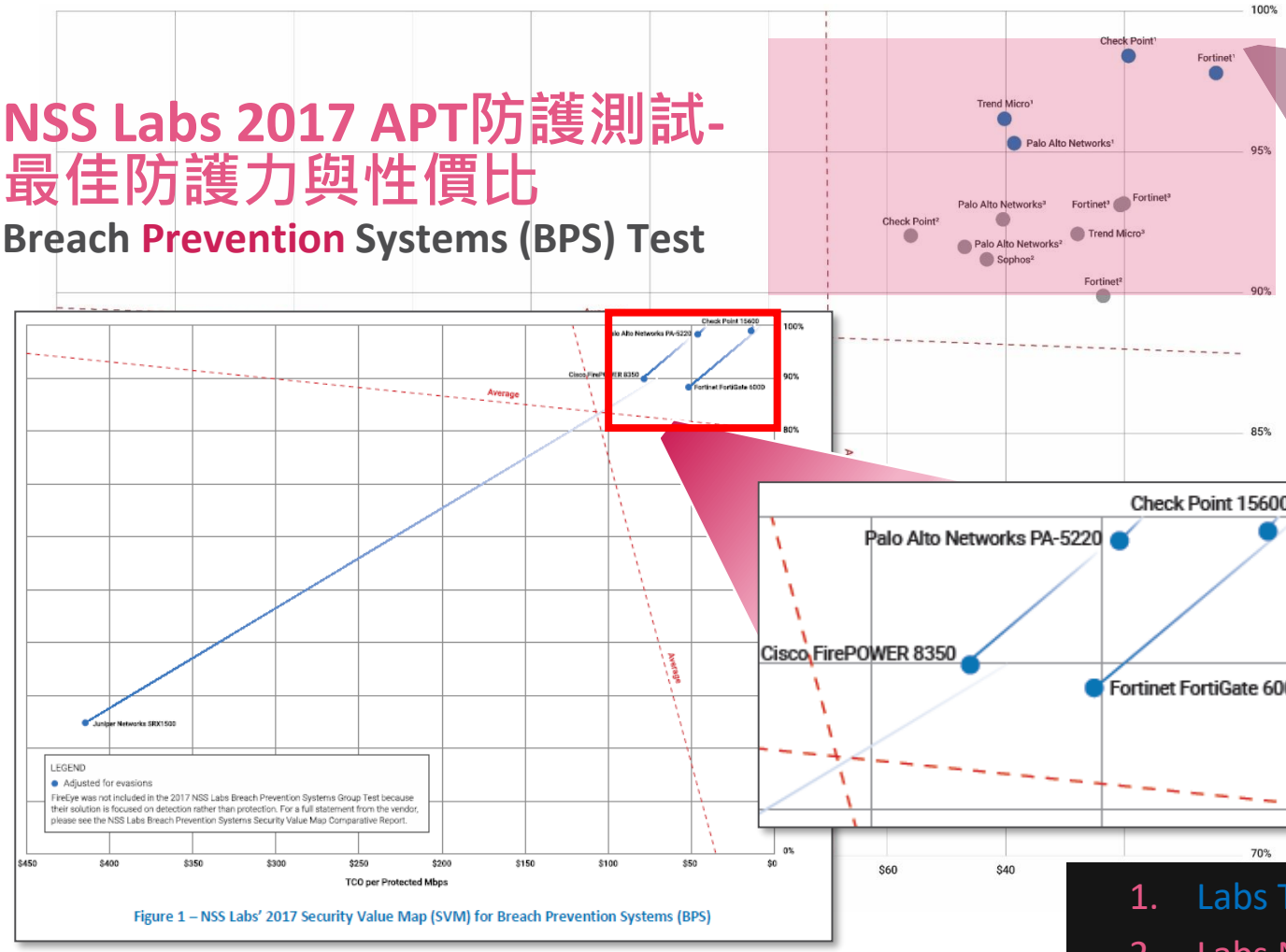
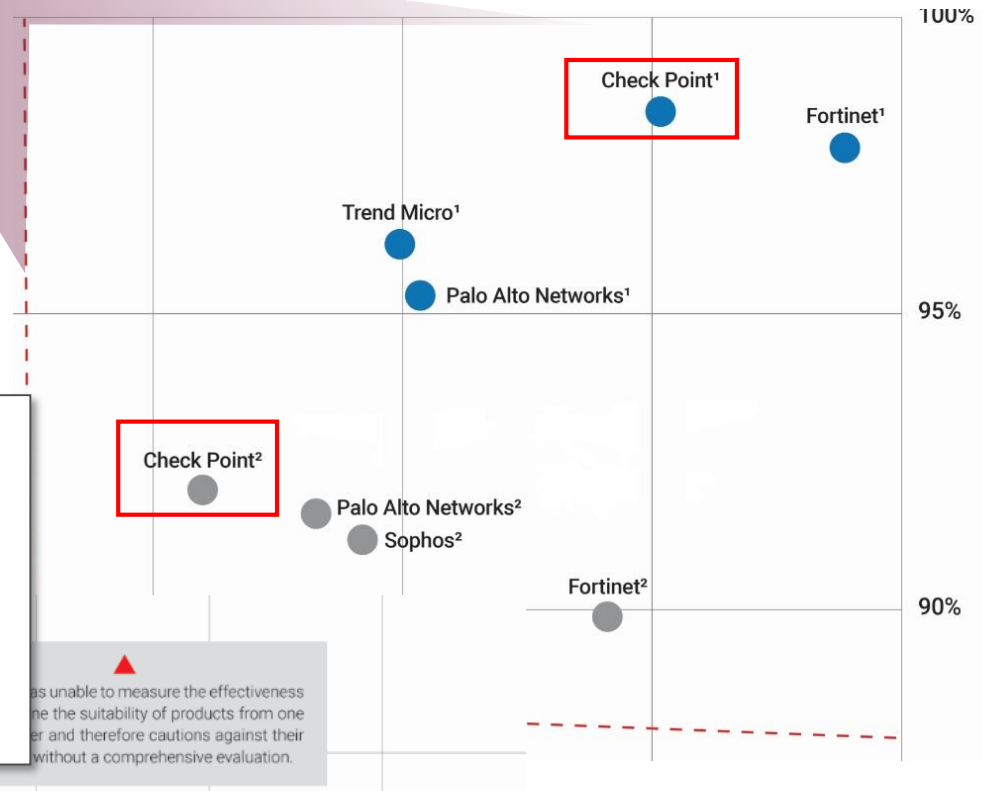
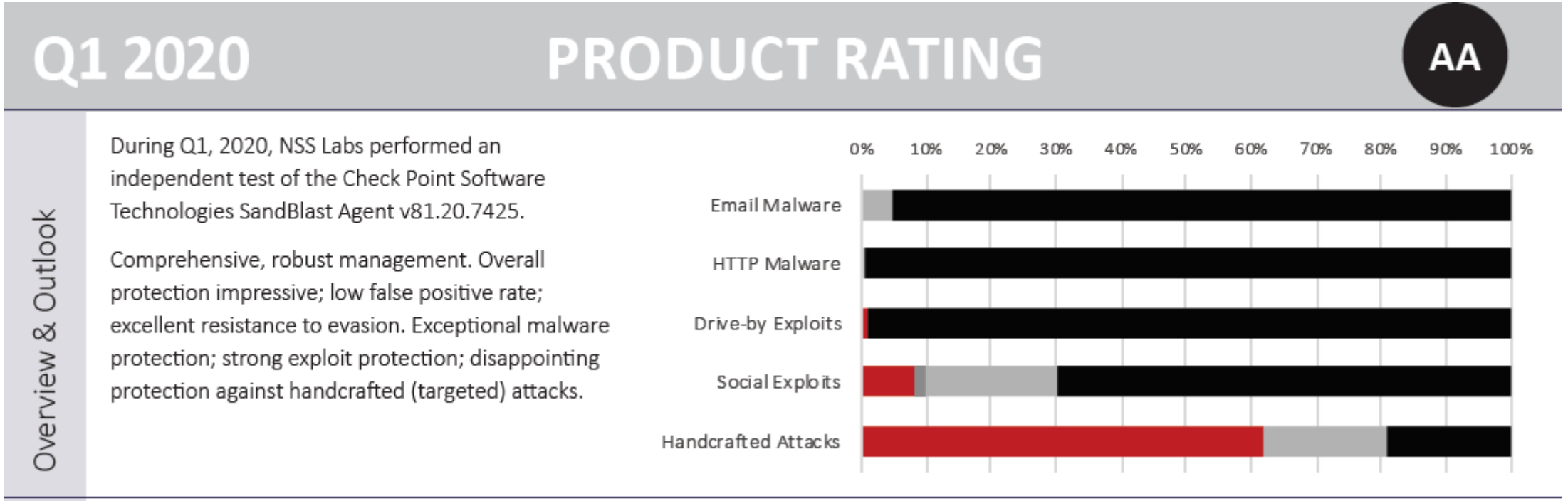


Figure 1 – NSS Labs' 2017 Security Value Map (SVM) for Breach Prevention Systems (BPS)



1. Labs Test Methodology v2.0
2. Labs NGFW Test Methodology v9.0 and AEP Test Methodology v3.0

2020 NSS LABS AEP TEST
CHECK POINT SBA -榮獲最高AA評等!



測試摘要:

-No.1 整體防禦能力(99.12%)

-評測成績優於市場主流NGAV/EDR產品

Check Point®
SOFTWARE TECHNOLOGIES LTD

THAT'S TAKE A 10 MINS BREAK!

CHECK POINT
INFINITY NEXT

AI於資安應用與智能安全防護平台

CHECK POINT THREATCLOUD:
全球最強大的威脅防禦情資引擎

200+安全威脅研究員

cp<r>
CHECK POINT RESEARCH

涵蓋範圍

100's of millions


防火牆閘道


端點裝置


雲

外部情資種子

- 安全社群
- CERTS
- 執法單位
- 資安合作伙伴
- 國際資安聯盟

豐富的人工智慧能量

- 攻擊活動監控
- 釣魚事件分析
- 惡意程式DNA
- 全景感知偵測

THREATCLOUD

Check Point
AI驅動威脅情資引擎

數據力帶來防護能力

THREATCLOUD

40億
每日情資交易量

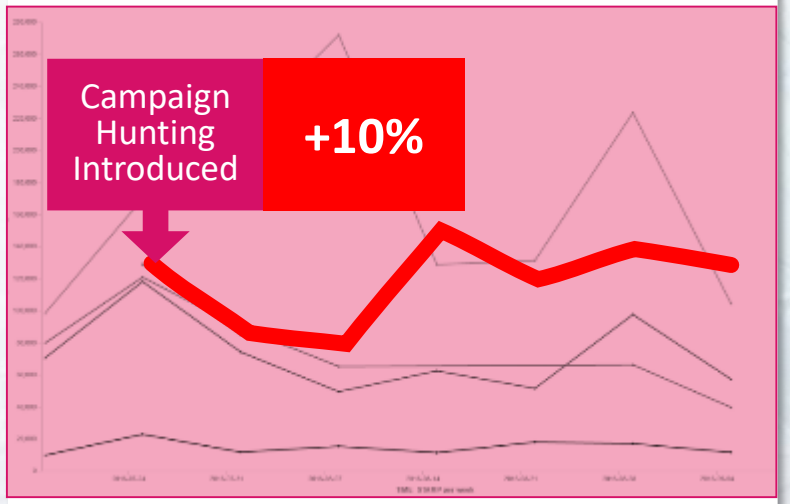
每天偵測超過7,000個
未知惡意程式

每天檢查超過
400萬個檔案

核心威脅防護引擎:
運用先進AI智能達成預測與精準判斷

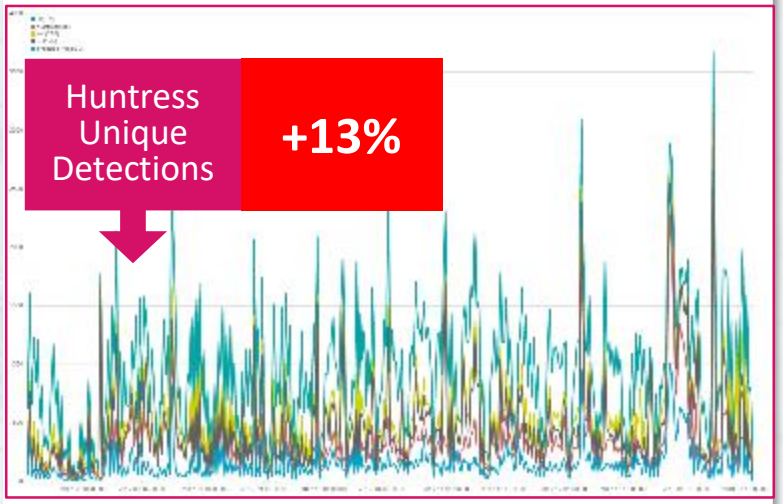
CHECK POINT UNIQUE

CAMPAIGN HUNTING



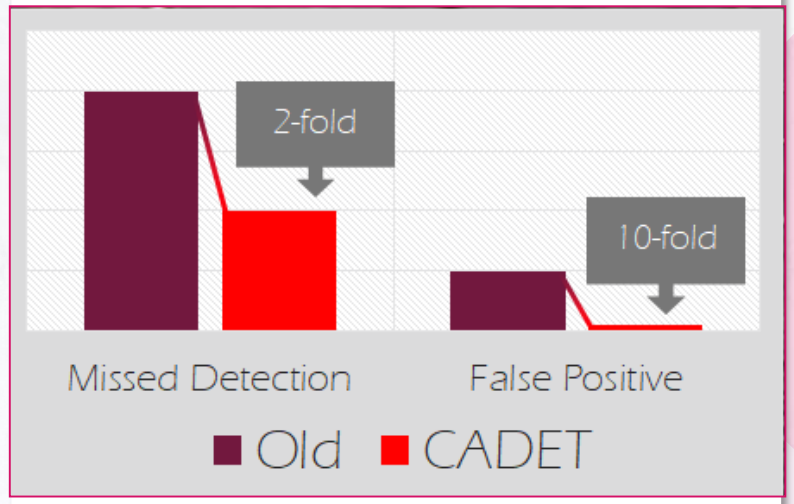
揭露未曾發現的C2惡意中繼站

HUNTRESS



動態分析惡意執行檔行為

CONTEXT AWARE DETECTION



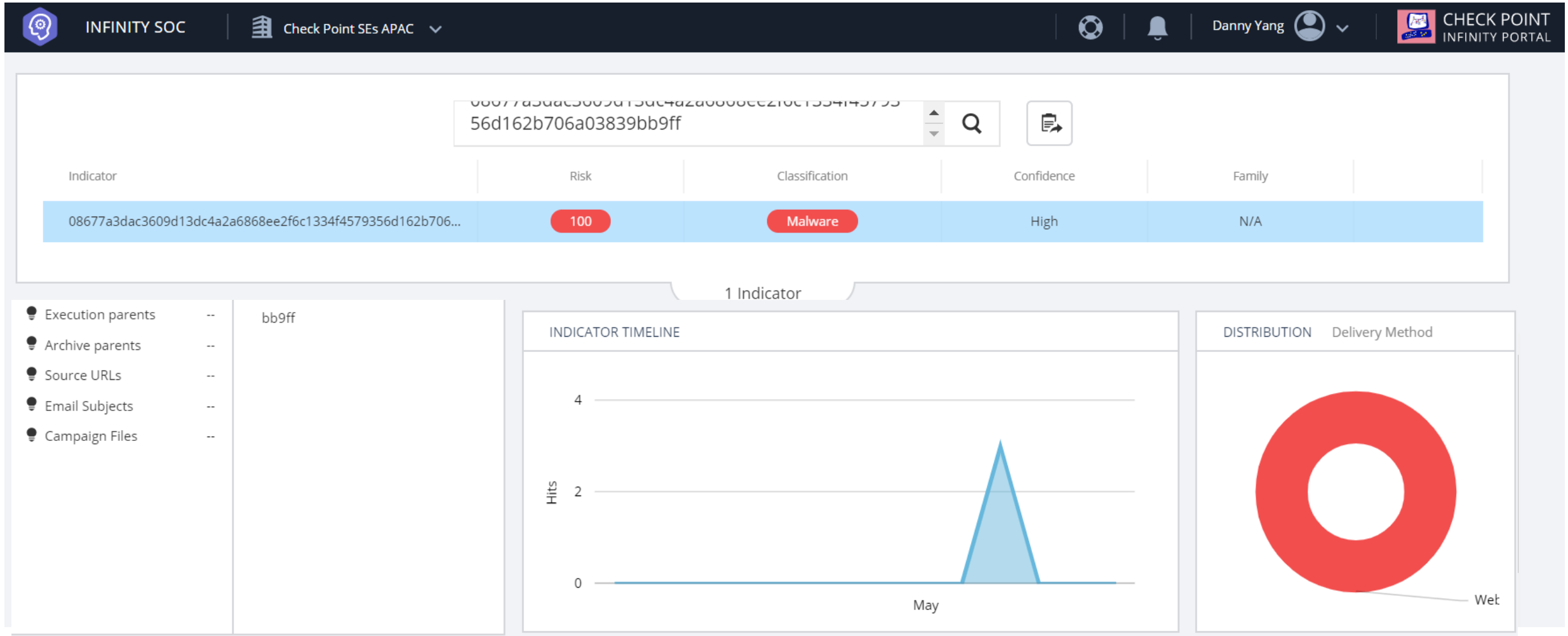
檢測完整威脅全景與多種參數
降低誤報率並強化攔截率

近期資安事件分析(勒索軟體部分)

- 時間 : 2020 5月
- 依技服中心提供之Indicator以及其他公開資訊

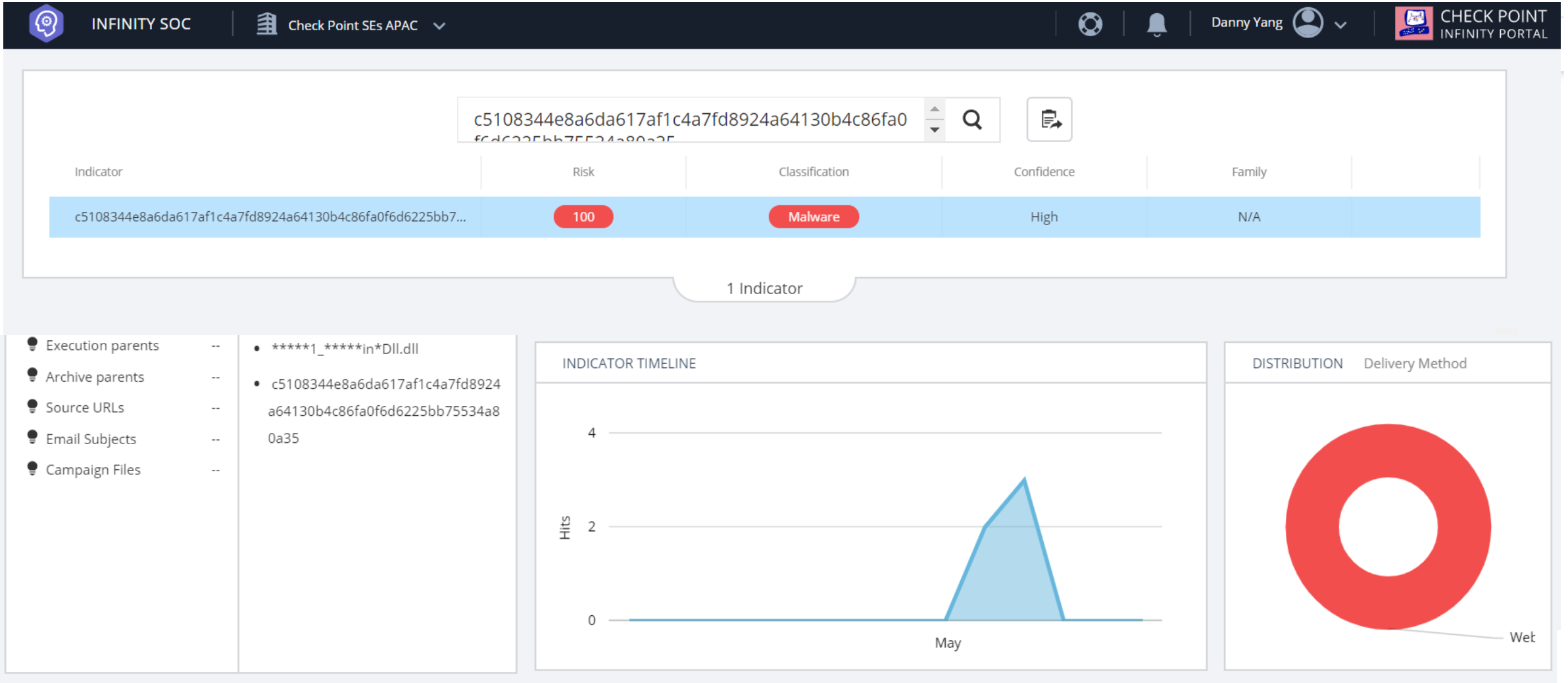
Indicator hash (SHA-256/SHA-1)	Type
08677a3dac3609d13dc4a2a6868ee2f6c1334f4579356d162b706a03839bb9ff 75e49120a0238749827196cebb7559a37a2422f8	Ransom.PS1.COLDLOCK.YPAE-A 駭客透過 GPO派送的加密軟體(Powershell 語法) (A公司)
c5108344e8a6da617af1c4a7fd8924a64130b4c86fa0f6d6225bb75534a80a35	Ransom.MSIL.COLDLOCK.YPAE-A
a2046f17ec4f5517636ea331141a4b5423d534f0	駭客透過 GPO派送的加密軟體(Powershell 語法) (B公司)
5B9B7FB59F0613C32650E8A3B91067079BCB2FC2	駭客透過 GPO派送的加密軟體(Powershell 語法) (C公司)
e7aa8f55148b4548ef1ab9744bc3d0e67588d5b7	ransom.exe -Powershell 執行後會 Drop的檔案
2051f0a253eced030539a10ebc3e6869b727b8a9	Powershell 執行後會 Drop的檔案
29cc0ff619f54068ce0ab34e8ed3919d13fa5ee9	readme.tmp -Powershell 執行後會 Drop的檔案

勒索軟體-Ransom.PS1.COLDLOCK.YPAE-A
(08677a3dac3609d13dc4a2a6868ee2f6c1334f4579356d162b706a03839bb9ff)

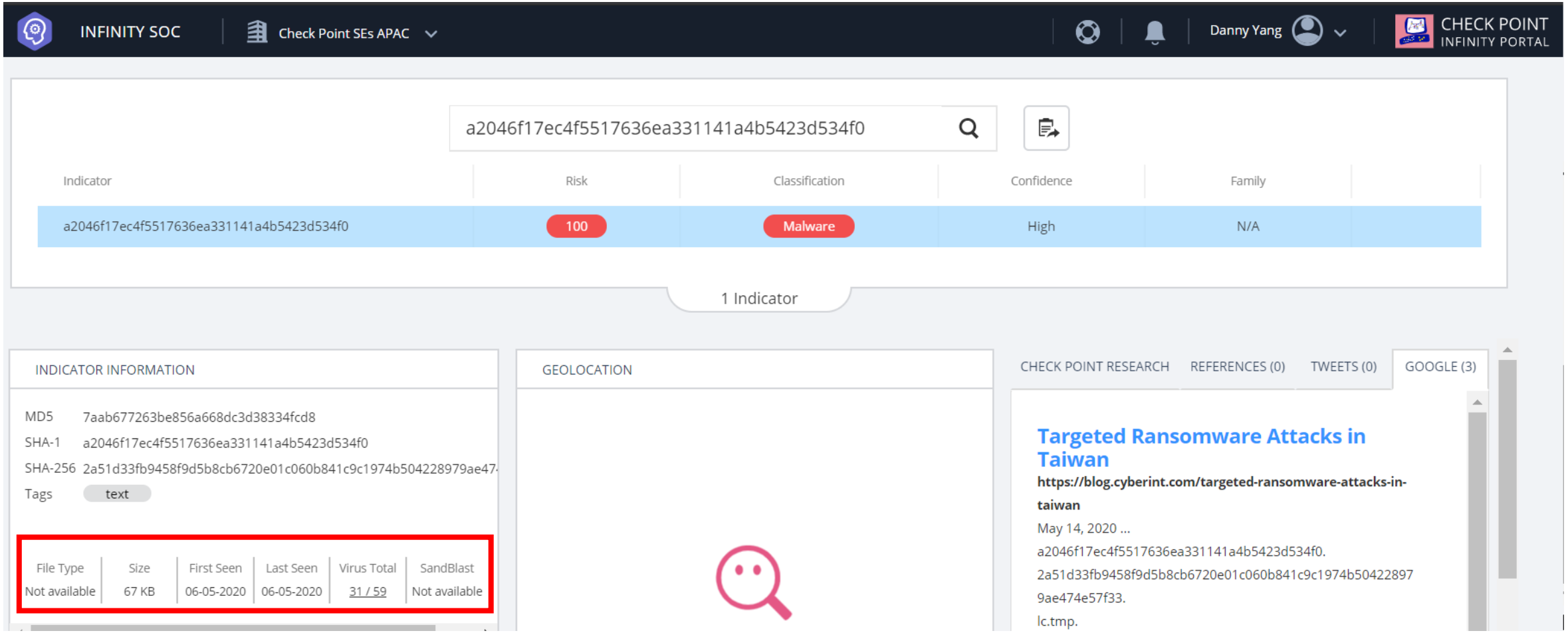


勒索軟體-Ransom.MSIL.COLDLOCK.YPAE-A

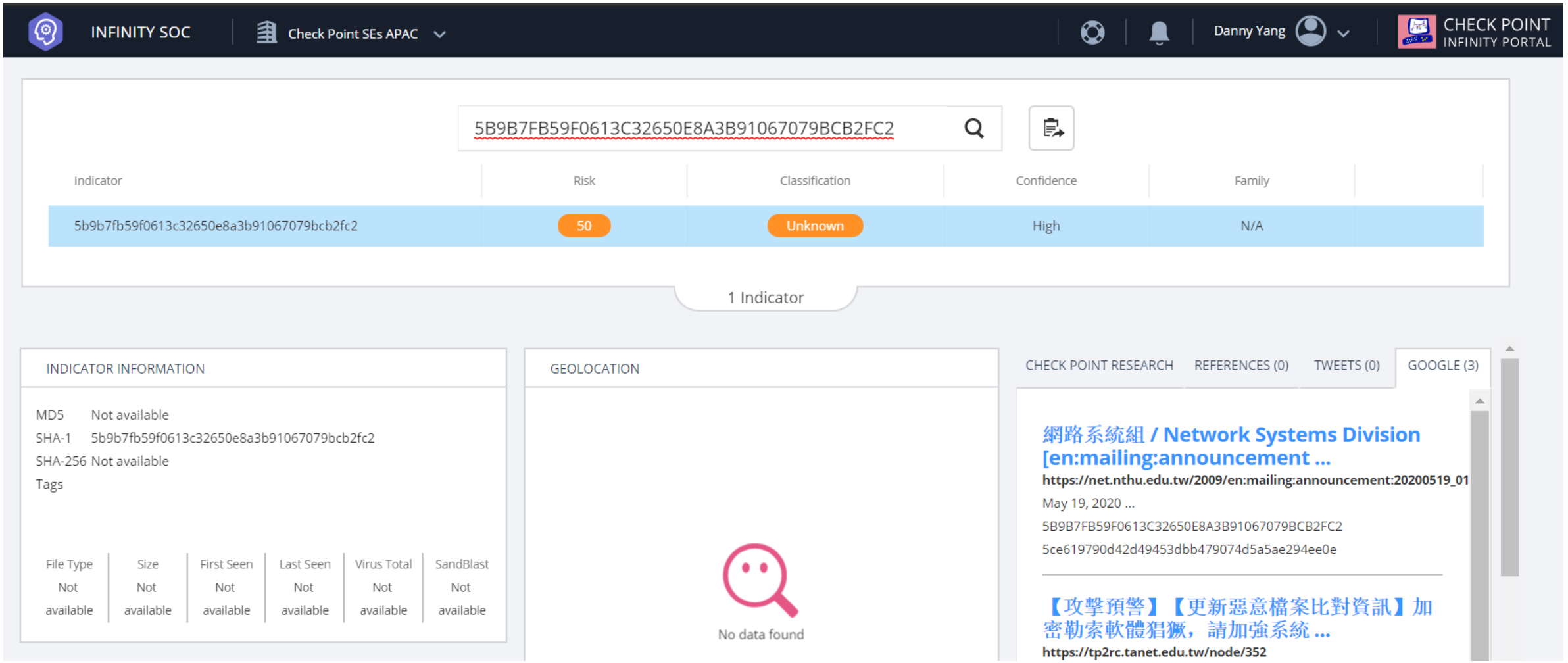
c5108344e8a6da617af1c4a7fd8924a64130b4c86fa0f6d6225bb75534a80a35



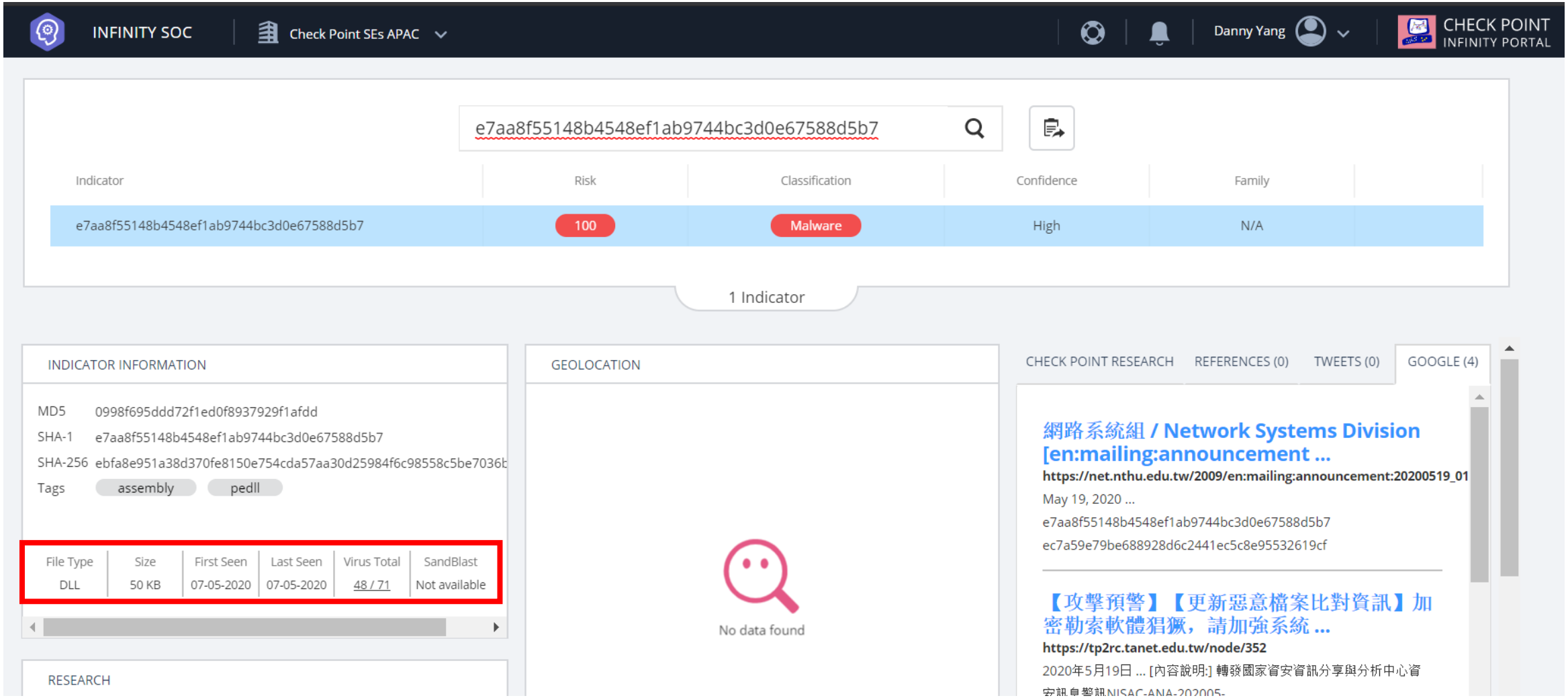
勒索軟體-lc.tmp (a2046f17ec4f5517636ea331141a4b5423d534f0)



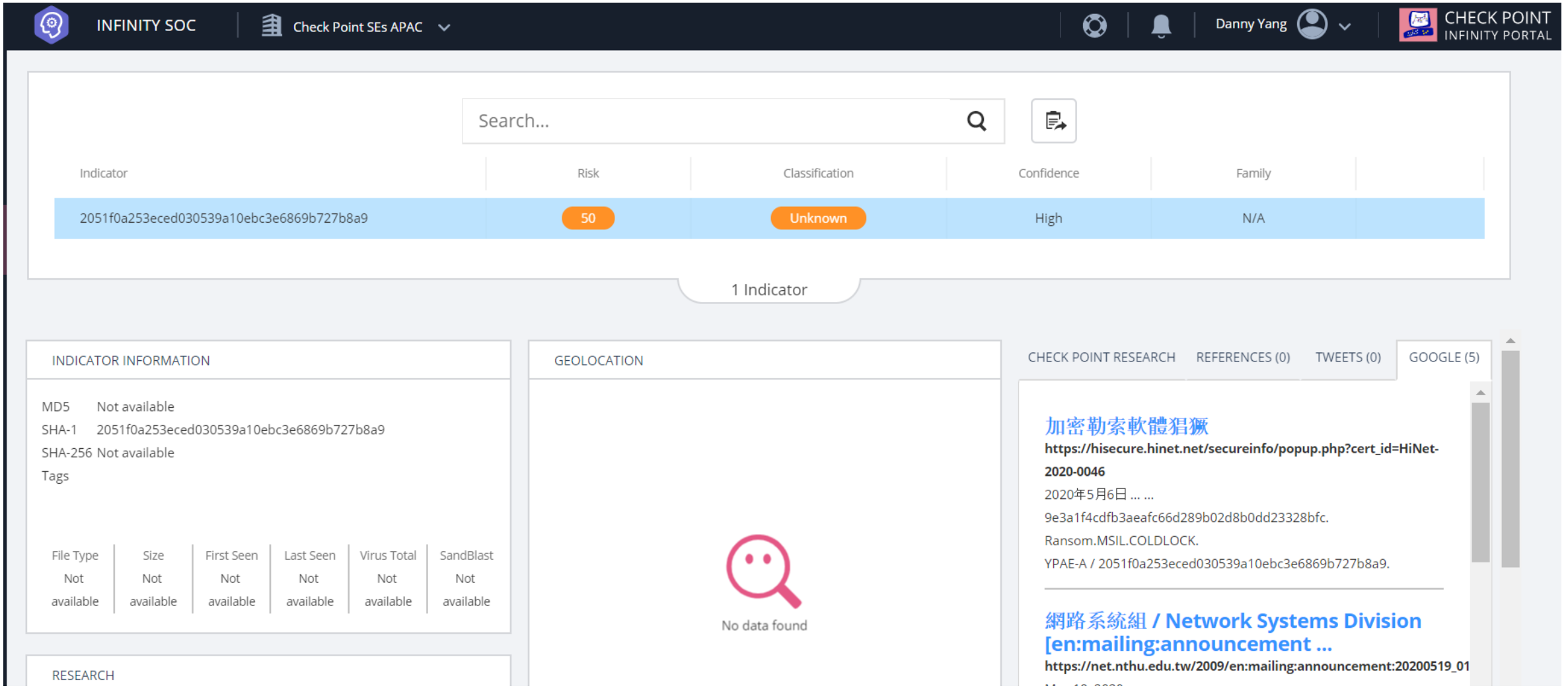
勒索軟體-lc.tmp (5B9B7FB59F0613C32650E8A3B91067079BCB2FC2)



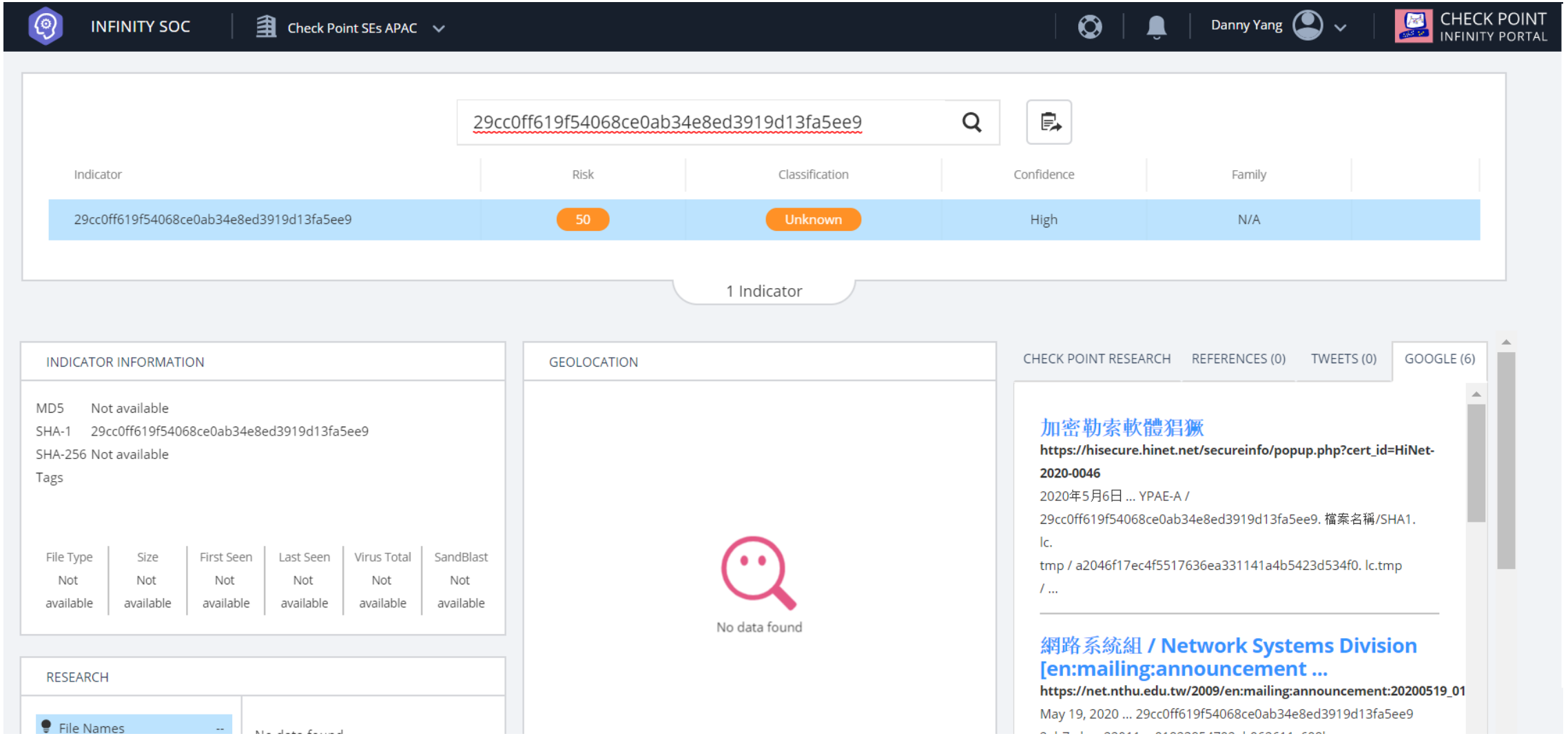
勒索軟體-ransom.exe-(e7aa8f55148b4548ef1ab9744bc3d0e67588d5b7)



勒索軟體 (2051f0a253eced030539a10ebc3e6869b727b8a9)



勒索軟體-readme.tmp (29cc0ff619f54068ce0ab34e8ed3919d13fa5ee9)



CHECK POINT
INFINITY SOC

達成SOC安全目標

99.9 % 精準度

運用AI預測組織
內部和外部的實際攻擊

迅速調查

全球最強大的
威脅情資引擎後台

非侵入式

無須安裝部署
符合隱私性要求

精準分析預測
從數百萬個事件中分析

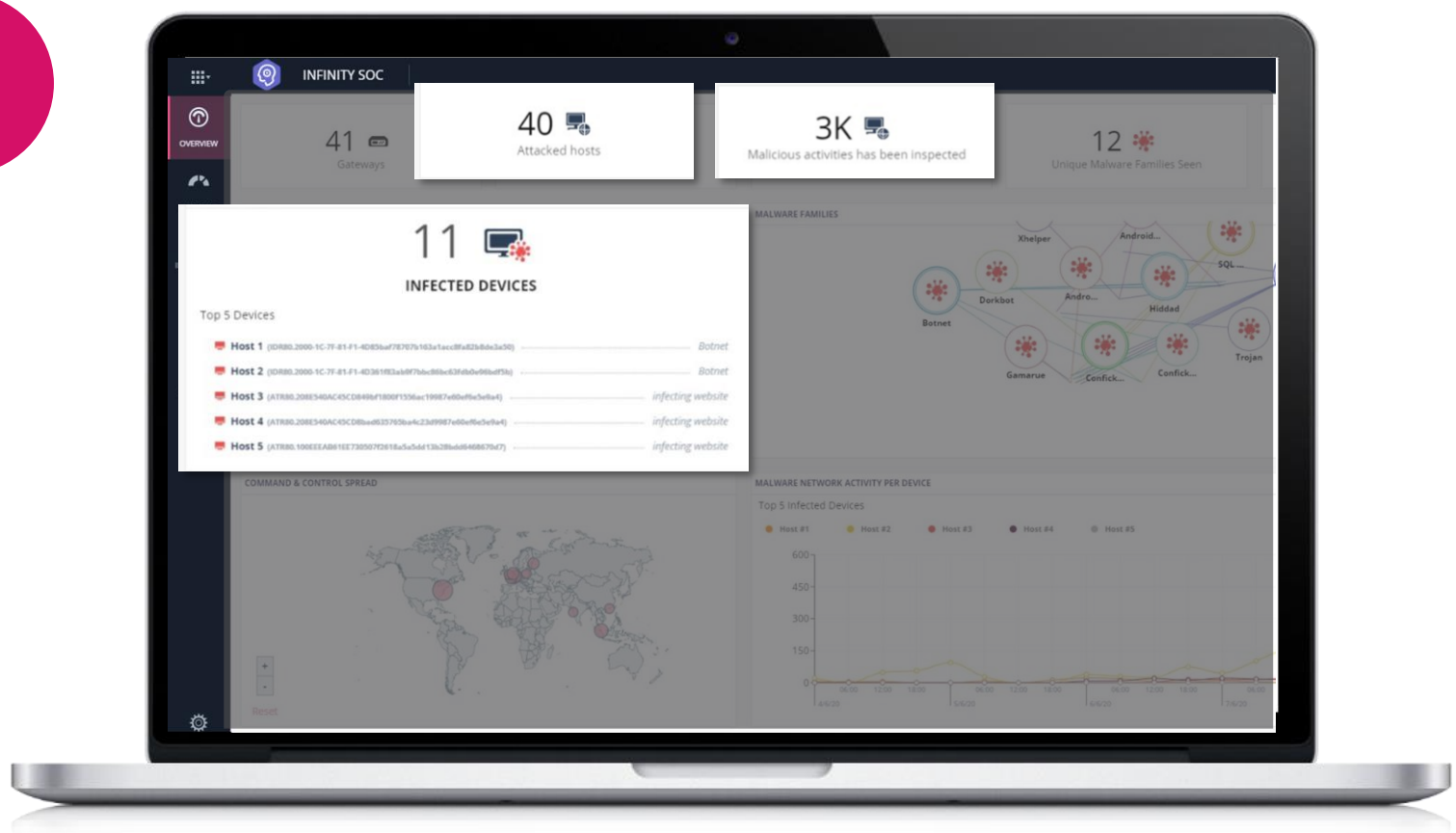
每週平均發現:

59,000,000
來自網路、雲、端點、行動、IoT、等日誌分析

3,000
惡意行為

40
目標IT數位資產

11
可能感染的數位資產



優先權掌握所有事件判斷
基於嚴重性和概率進行智能回應

99%
TRICKBOT MALWARE

99%
Host #1 6:58, 6/20/2020
Host 1 might be infected with Trickbot (High probability)

99%
ADWARE

99%
Host #2 6:58, 6/20/2020
Host 2 might be infected with Adware (High probability)

30%
EXTERNAL THREAT

30%
Lookalike URL 13:42, 6/8/2020
Lookalike URL impersonating your website (Low probability)

10%
MOBILE THREAT

10%
Mobile Device 6:57, 6/8/2020
Mobile Device might be infected with Trojan Horse (Low probability)

安全回應
一鍵修復，將攻擊影響最小化

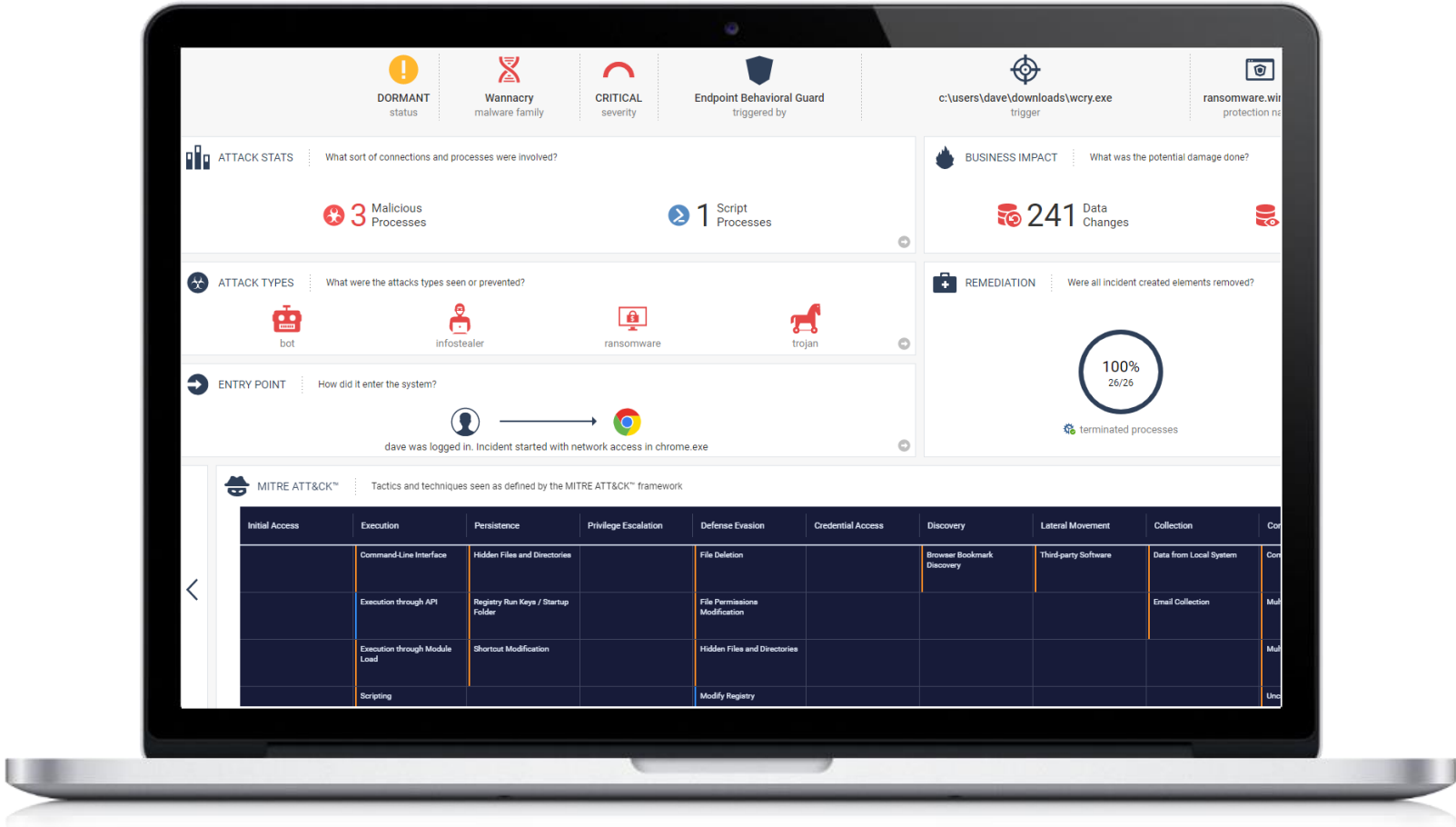
1 在受感染的主機上安裝簡易版防護代理程式

識別並封鎖所有惡意執行緒

阻斷 C&C 通訊

移除所有惡意檔案

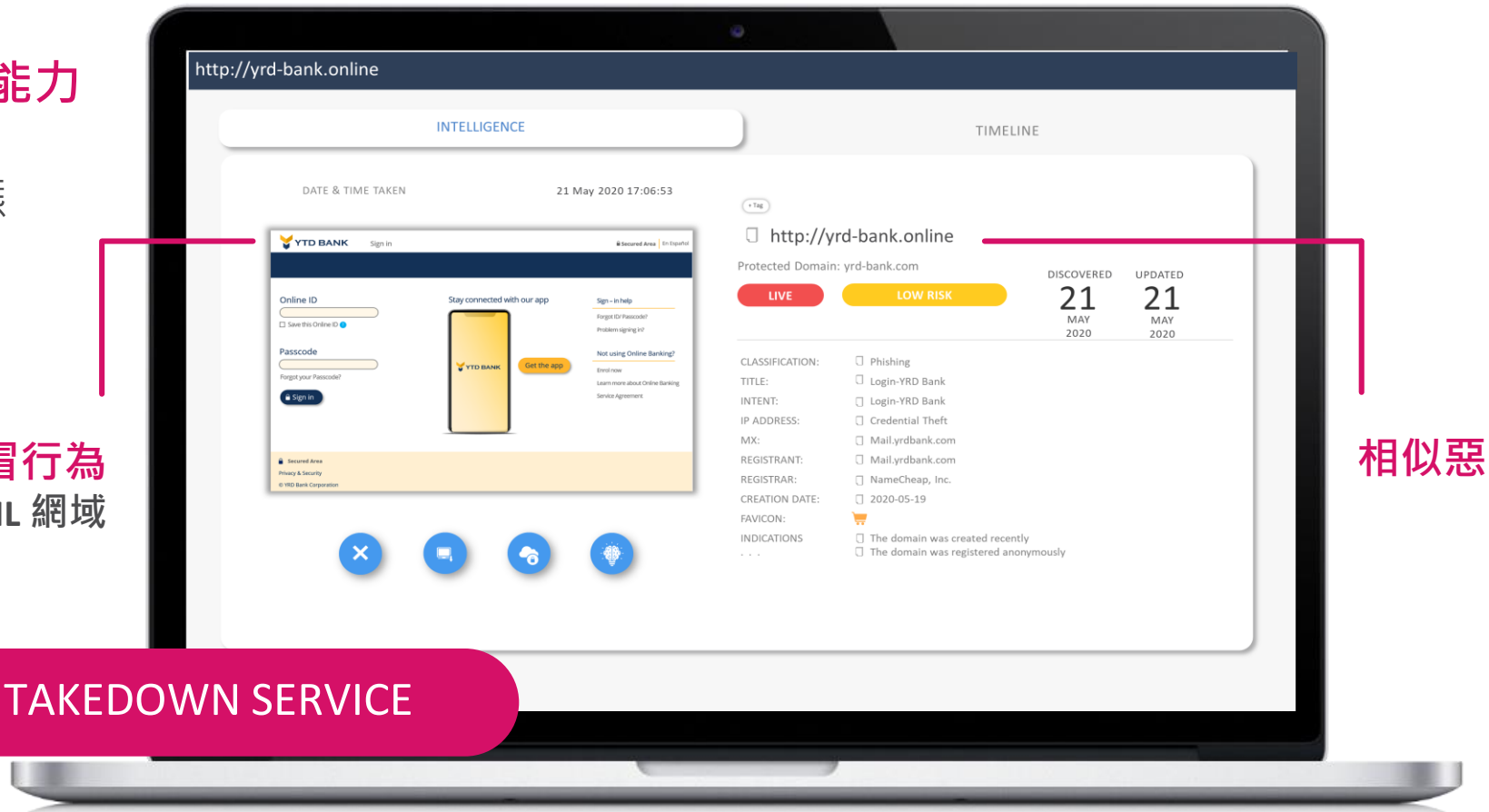
2 獲取高可視性見解的詳細鑑識分析報告



外部威脅
防止針對企業客戶和員工的網路釣魚活動

相較同業
高出3倍以上的威脅識別能力

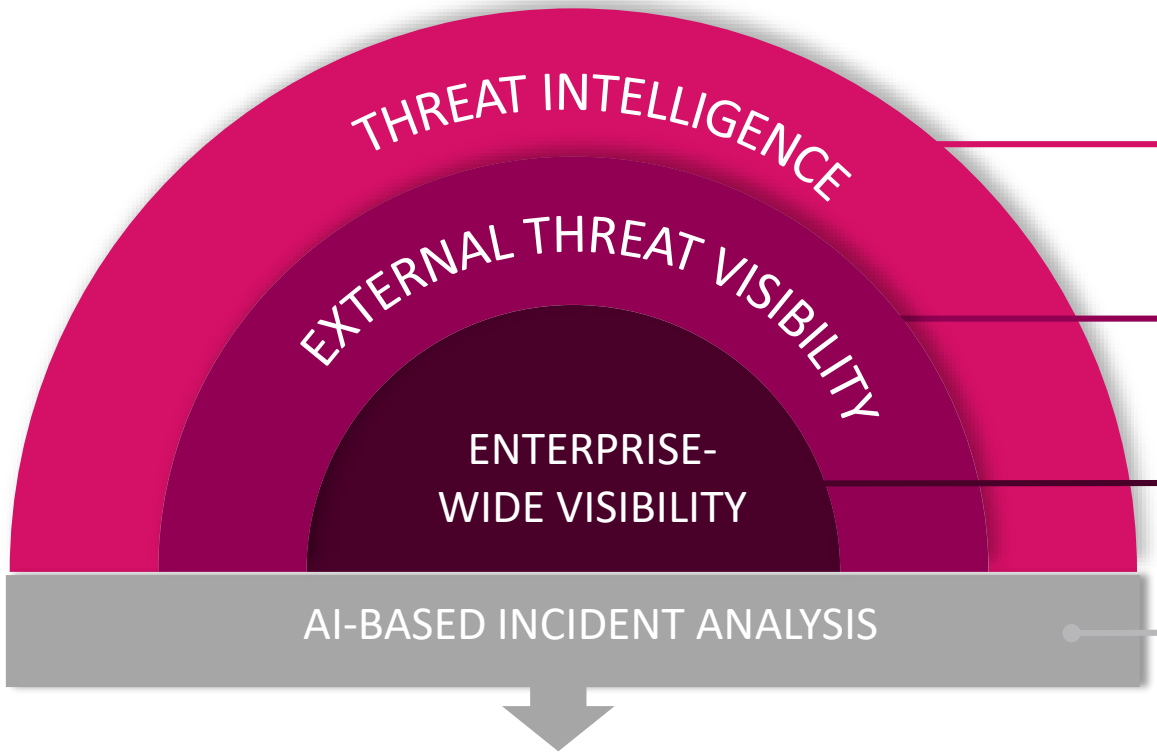
監控即時網路流量與狀態



偽冒行為
模仿網頁/EMAIL 網域

相似惡意網域

TRUE XDR:
以智慧資安完成99.9%的精準度，揭露最隱秘的攻擊



ThreatCloud大數據分析與資料查詢

即時網路流量可視性

網路、端點、行動、以及IoT裝置活動

以機器學習訓練AI而成的威脅防禦模型

‘GOOGLE SEARCH’ 任何IOC皆可方便於單一介面查詢

全球最即時先進的威脅情資資料湖

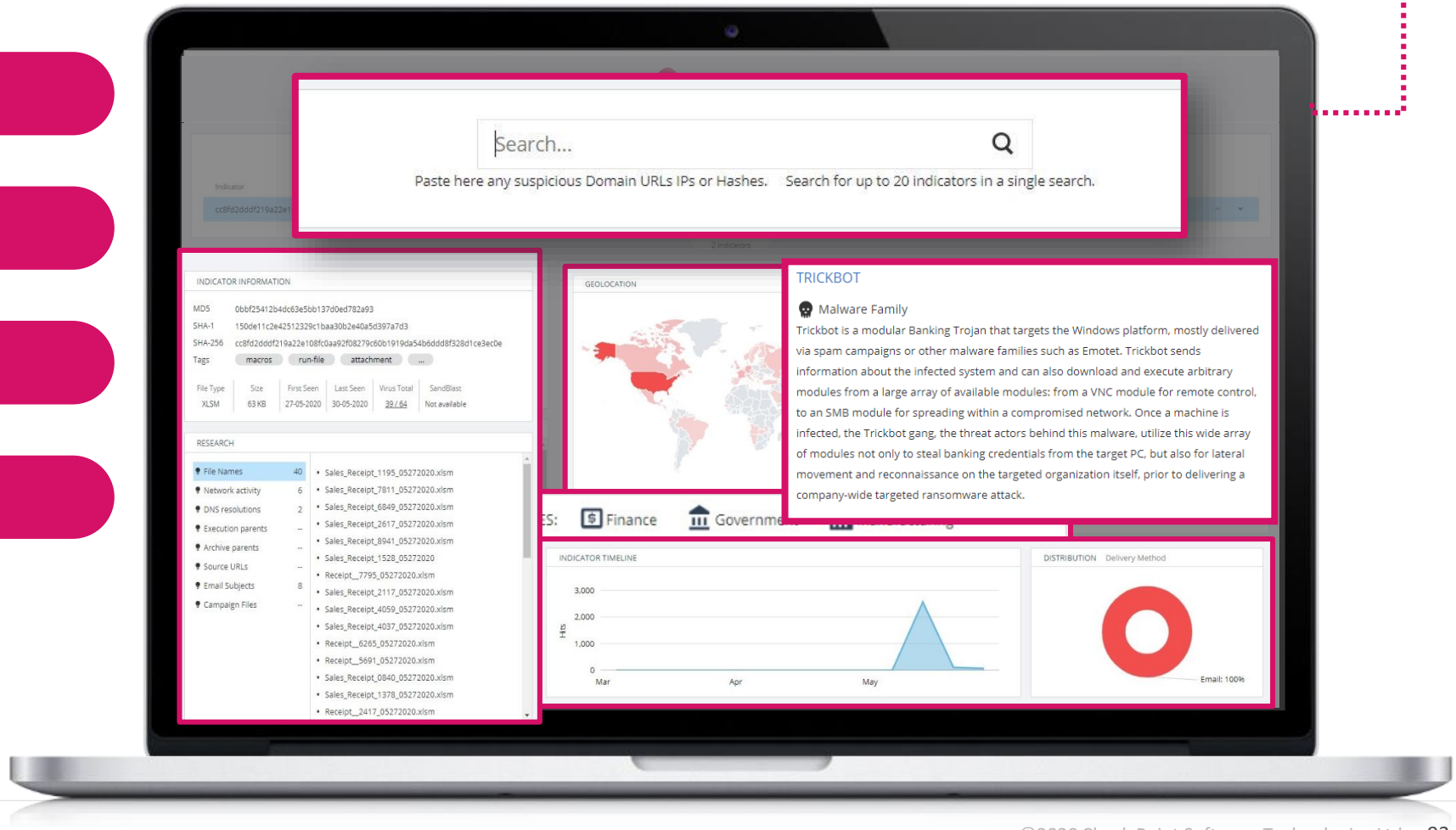
散佈區域

目標產業

攻擊時間軸與模版

獨家研究數據

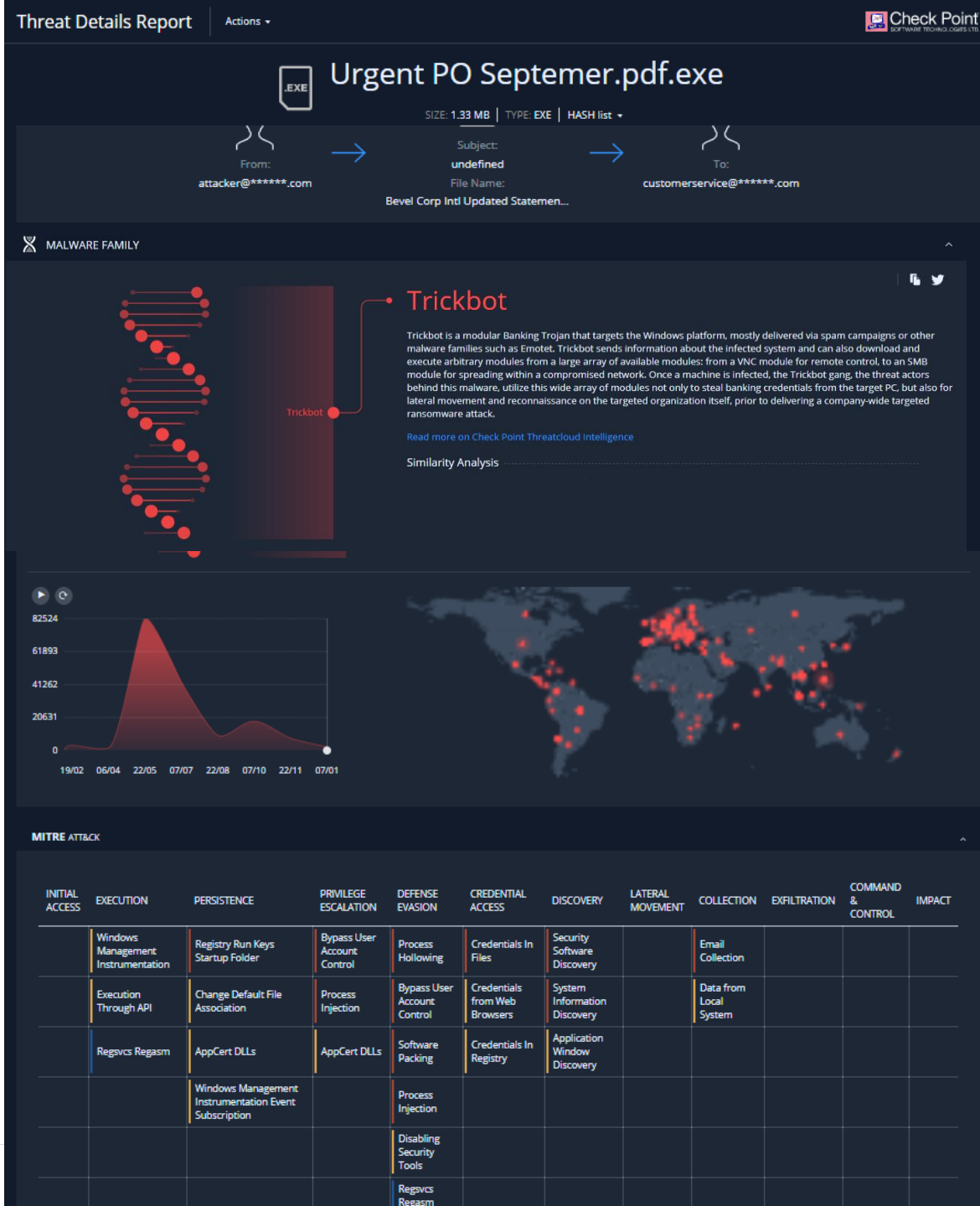
更多情報...



快速確認是否有可疑惡意檔案

SANDBLAST'S THREAT EMULATION

- 惡意程式家族
- 活躍地區
- MITRE ATT&CK techniques
- 惡意檔案模擬錄影
- 下載檔案
- C2 URLs
- 更多情報



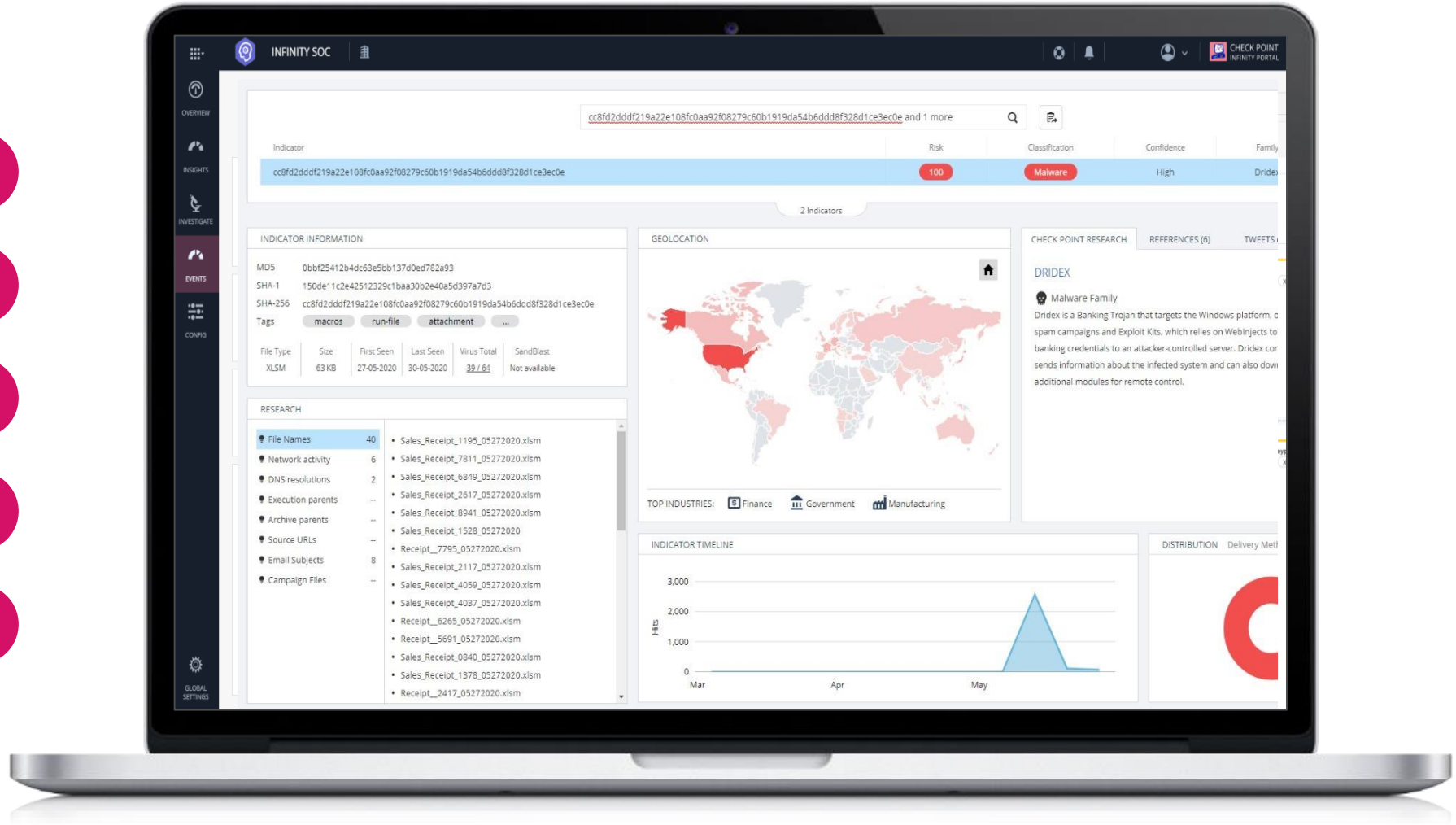
CHECK POINT
BREACH PREVENTION SYSTEMS 2.0
NSS LABS
RECOMMENDED
AUGUST 2019

INDUSTRY'S BEST CATCH RATE
2019 NSS LABS BPS

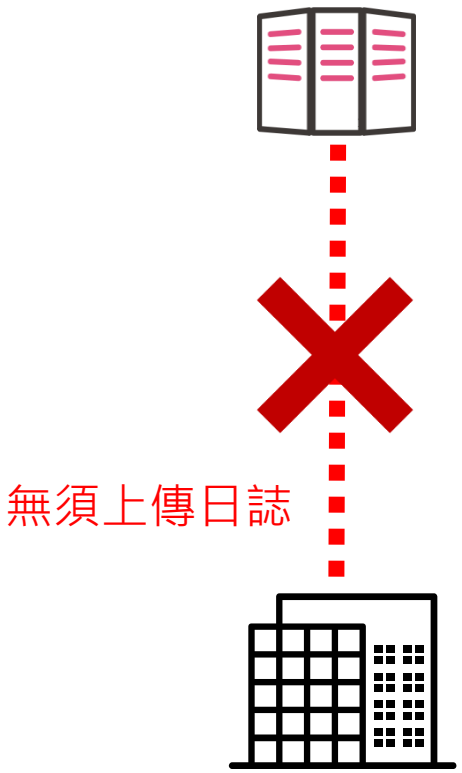
Check Point
SOFTWARE TECHNOLOGIES

降低TCO 以及避免疊床架屋的複雜管理問題
單一安全的SOC 監控平台與統合管理介面

- 內部威脅
- 外部入侵威脅
- 補救措施
- 深入調查
- 中央控管



避免隱私問題以及高昂投資
不儲存日誌或匯出客戶資訊



確保隱私並維持合規性

避免高額雲端儲存成本

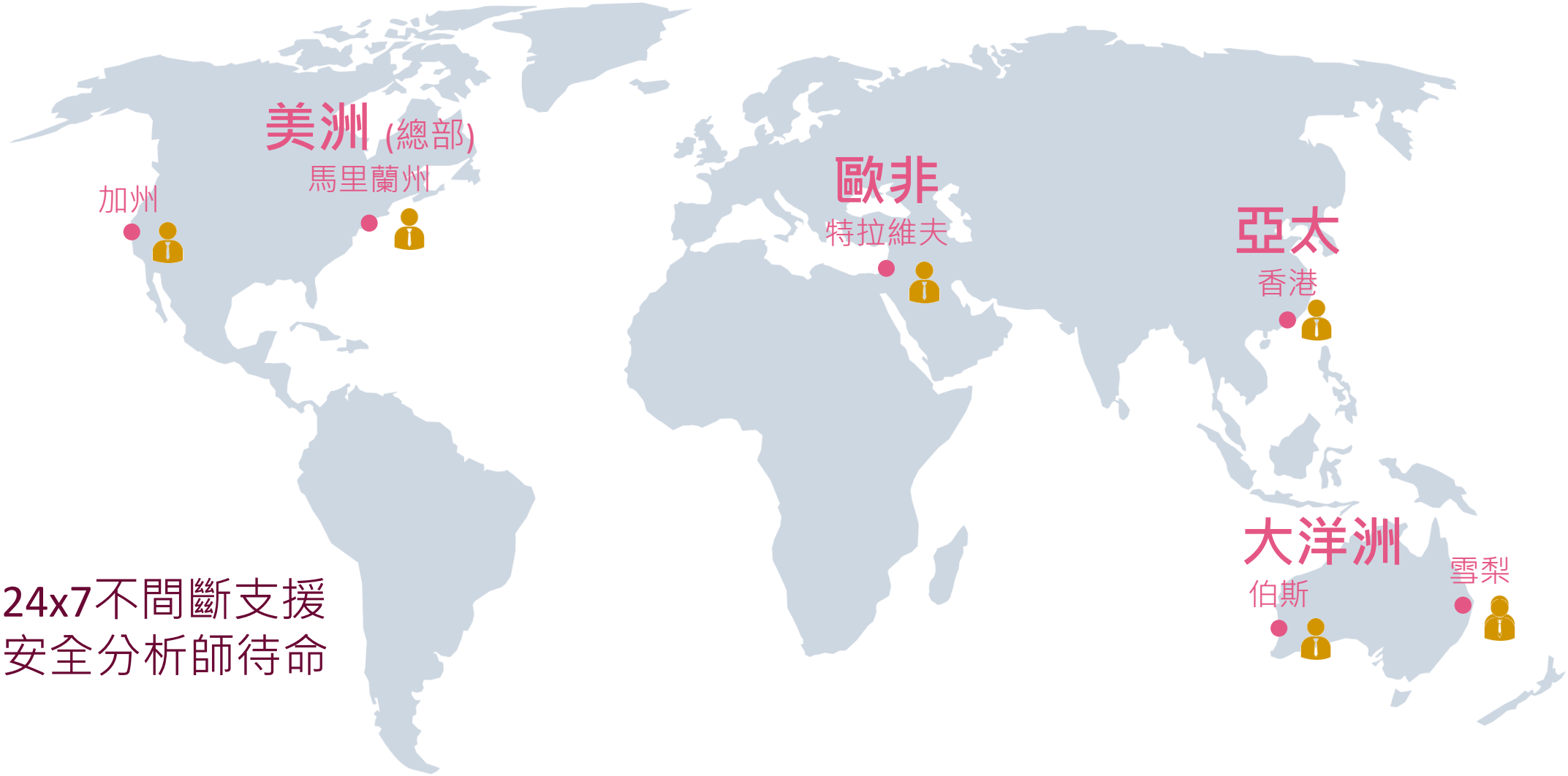
惡意威脅及資安事件發生時...您該如何處理?

NIST **SP 800-61**
Incident Response Framework

事件分析及回應服務

Info Source: NIST Computer Security Incident Handling Guide
Picture: blog.elearninsecurity.com

Check Point 安全事件分析與回應團隊(CPIRT)



全球24x7不間斷支援
資深安全分析師待命

CPIRT服務內容

事件回應服務	完整資安事件處理與因應 (依據NIST 800-61標準)
顧問服務	• 安全威脅風險評估 • 實務演練 • 訂定IR計畫與Playbooks • 安全架構檢討 • 威脅情資監控/Threat Hunting

應用範例

- Ransomware
- Malware Infection
- DDoS Attack
- Data Leakage
- Cloud Application Compromise
- Social Media Impersonation
- Web Application Attack
- Cybercrime
- Investigate Product Alerts

Check Point 事件分析與反應技術優勢

服務經驗

2018 年處理的事件量達 600件以上

可支援多國語言(華語)

擁有全球化
多位惡意程式分析師

高階研發人員支援

Check Point威脅研究團隊(CPR)
提供後台數據支援

事件分析成功率達 90%

(資料來源：2018 IRT 個案統計資料)

完整安全解決方案支援

可使用 Check Point 全系列解決方案

快速回應

具實務經驗 IRT 分析師即時回應

Check Point IR Datasheet

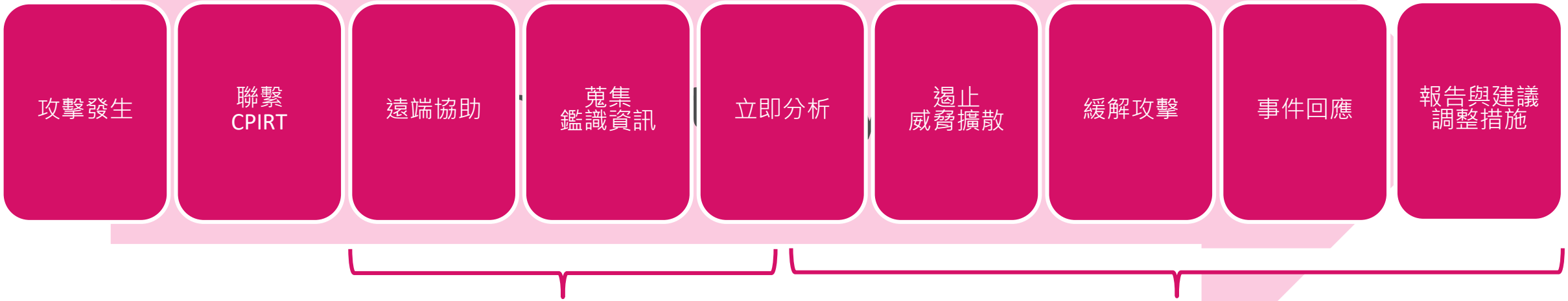
威脅事件分析與反應流程

Phone: 24x7專線(或請與臺灣Check Point團隊聯繫)

Email emergency-response@checkpoint.com

可提供全方位Check Point解決方案

- 新世代防火牆與APT功能
- 端點防護措施
- DDoS Protector
- 雲端安全與其他方式



即時提供協助!

- 識別攻擊問題
- 提供初步建議
- 確認範圍與處理時程

進行後續處理與回應

CHECK POINT

INFINITY

WITH CHECK POINT INFINITY

IT發展敏捷飛速，確保安全如影隨形

Let’s Kahoot!

CHECK POINT
INFINITY NEXT

https://kahoot.it/ or google “Kahoot!”

Pin Code:

Check Point®
SOFTWARE TECHNOLOGIES LTD

THANK YOU

Danny Yang l Cyber Security Evangelist
dannyy@checkpoint.com