CHECK POINT™

以混合網狀防火牆(HMF)框架建構全域安全連線與AI協防回應

2024 Jlead Solution Day

Kyle Feng, Security Consultant

2024 Sep 13

YOU DESERVE THE BEST SECURITY

Agenda

Infinity: 因應全網狀安全架構的防護平台

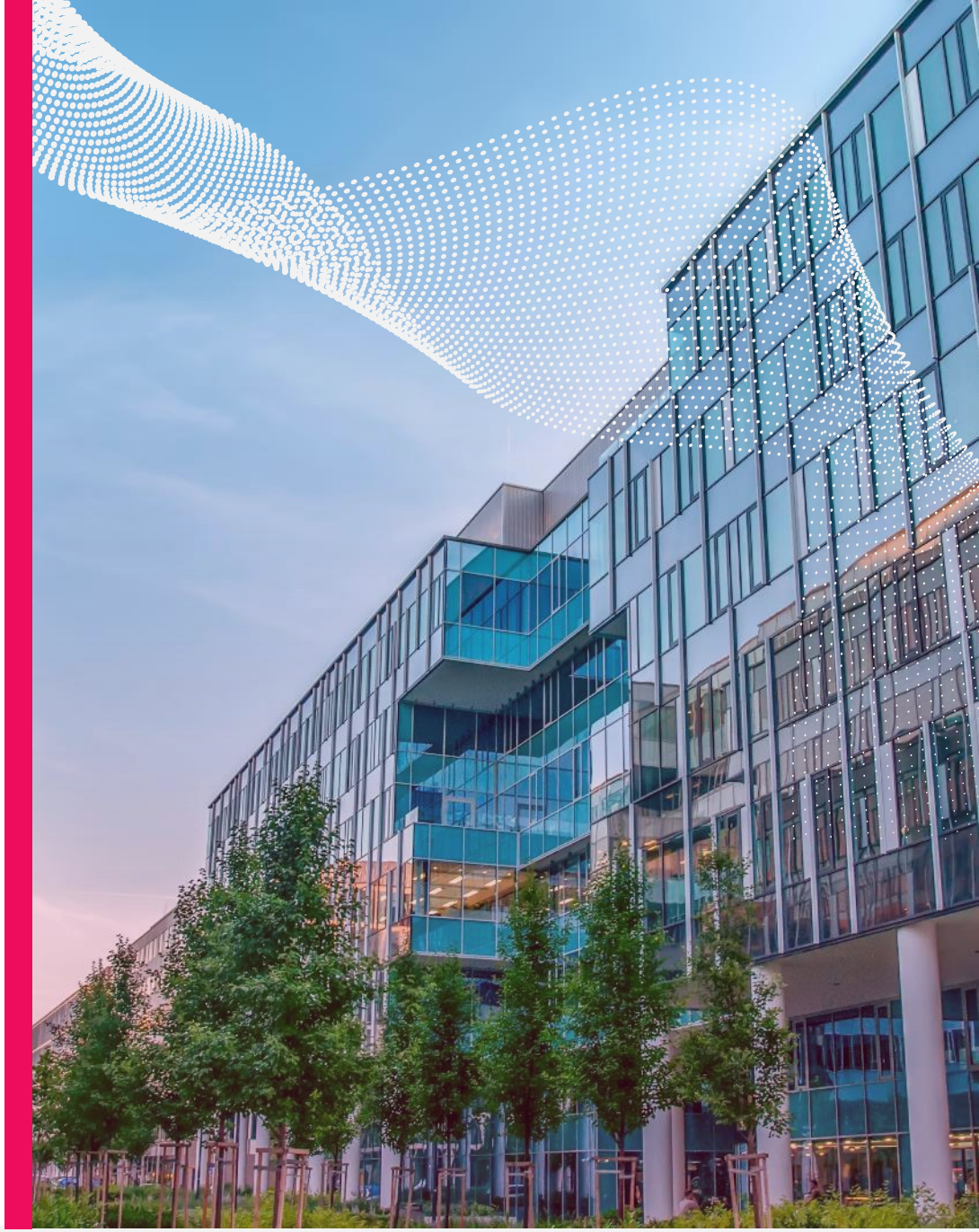
Hybrid Mesh Firewall: 未來網路安全設計基礎

三大資安銷售商機:

- AI Driven WAF, SaaS Mail Security, SASE/SSE

資安風險已經升級成商業風險

- 更複雜的法規遵循
- 資安採購預算的緊縮與排擠
- 大量且繁瑣的安全維運負擔
- 人才資源稀缺教育訓練不足



資安防護需要更迅捷的隨需延展能力

混合網路

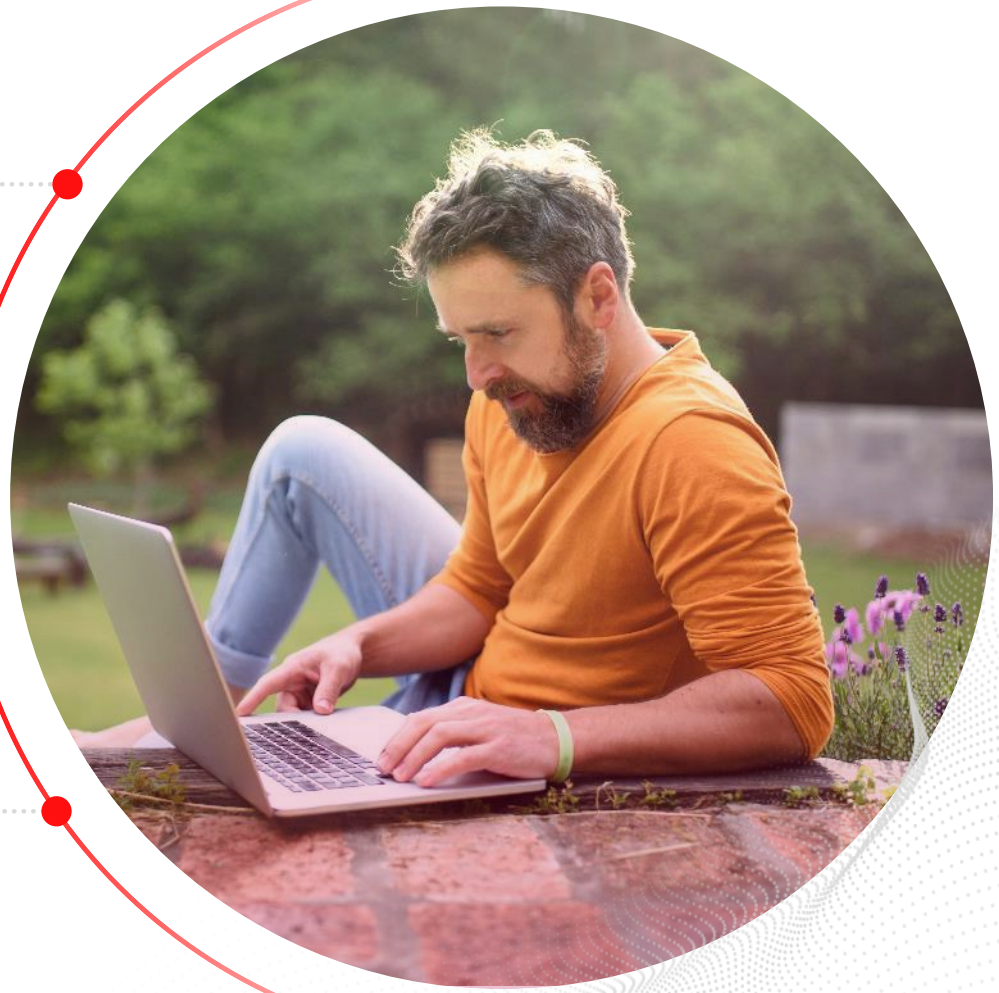
- 支援各種頻寬擴充需求
- **驅動雲環境與地端資料中心之間更具效率的安全存取**

混合工作情境

以零信任原則實踐
全網狀安全連線 (Full-Mesh)

混合雲

動態統合安全政策與態勢管理
因應各種工作負載情境應用



資安架構的遷移: 從硬體轉向混合式，以服務形塑差異

數位轉型與雲端化
工作負載與安全配置轉變

- 企業網路應用多元化
- 混合式網狀安全平台
- 統合安全管控與事件回應
- 多重型態的雲應用
- SaaS服務安全與態勢管理

以威脅防護為IT運轉核心的全面安全架構

統合 安全管理與資安服務

Infinity
Core Services

網路資安	雲端資安	端點與使用者安全
Quantum	CloudGuard	Harmony

PREVENTION-FIRST 防護優先安全營運管理平台

Infinity

AI-POWERED 先進威脅情資引擎

THREATCLOUD AI

混合式網狀防火牆平台
(Hybrid Mesh Firewall)

CHECK POINT™

Hybrid Mesh Firewall 平台主要元件

1

多元化的部署模型

- Cloud Native Firewall
- Hardware Appliance
- Virtual Firewall
- Firewall as a Service

2

豐富且一致的統合管理與進階威脅防禦

- 基於雲端的中央控管
- 自動調校與政策建議
- 雲原生與微分段的安全可視能力
- 應用程式探索與使用量識別
- 包含IoT與DNS安全的進階威脅防護

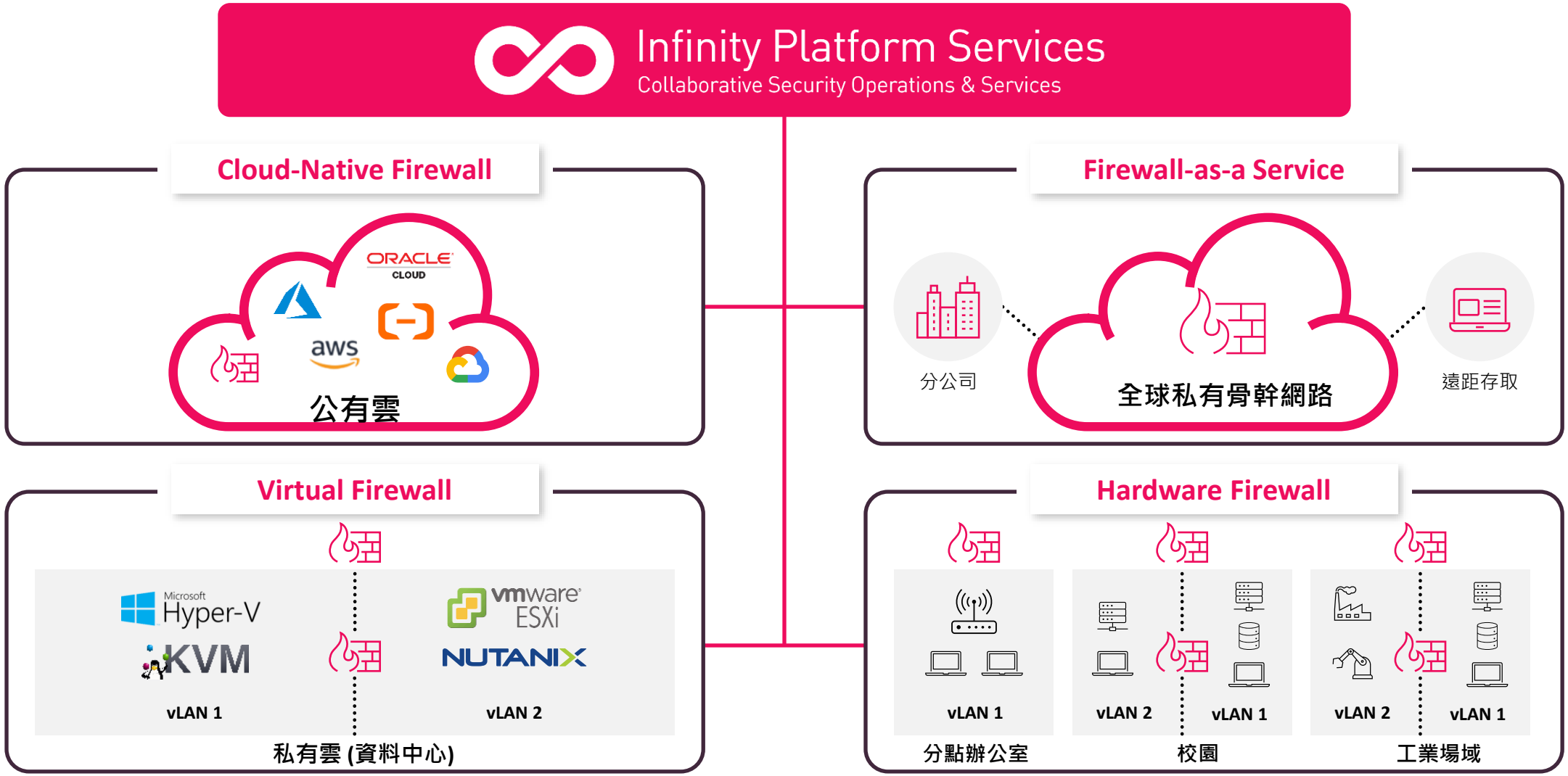
3

API與自動化實現整合

第三方整合能力:

XDR, SASE, Identity Providers, Cloud Orchestrators, CI/CD

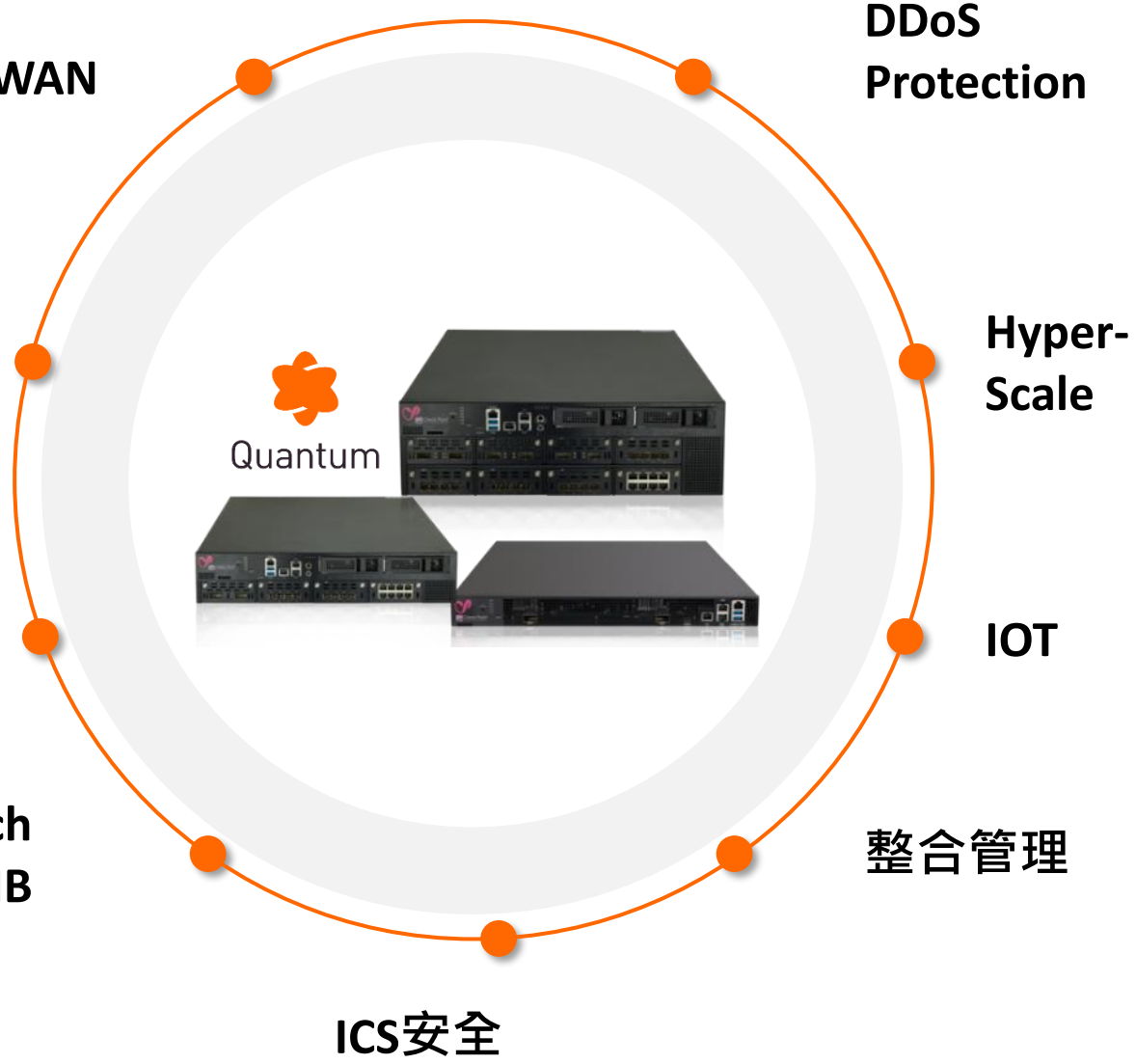
Hybrid Mesh Firewall 平台架構



Quantum
Security Gateway

保護企業網路與資料中心

- 適應任何企業規模
- 類雲化動態叢集擴充能力
- 整合IoT安全
- 整合SD-WAN
- DDoS防護



2024全新Quantum Force系列

Quantum Force

Series 9000

6款新機種
企業邊界防護級距

Series 19000

2款新機種
中大型企業網路安全

Series 29000

2款新機種
資料中心與高端應用

AI驅動與雲端傳遞的安全優化設計

10款全新網路安全閘道

類雲化動態安全網路叢集

Quantum
Maestro

Orchestrators

防火牆叢集

Maestro
Hyperscale System

智能化
負載平衡

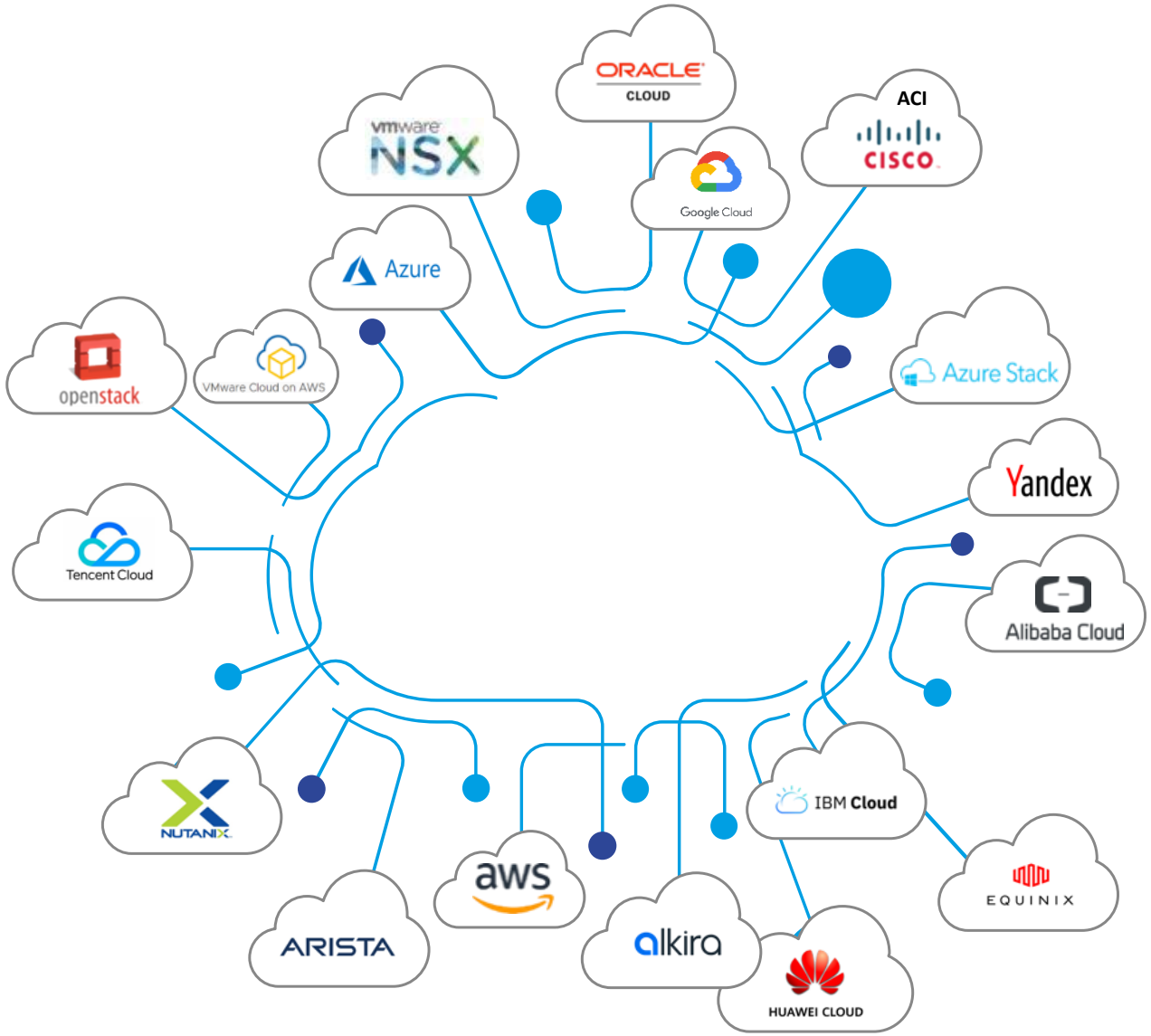
動態擴充:
1Tbps
威脅防禦效能

99.999%
營運不中斷

CloudGuard Network

保護公有雲/虛擬化與混合雲資料中心

- 雲端存取與安全防護
- 網路應用程式防火牆 (WAF)
- Cloud Native Application Protection (CNAPP)
- 雲端安全偵測回應 (CDR)

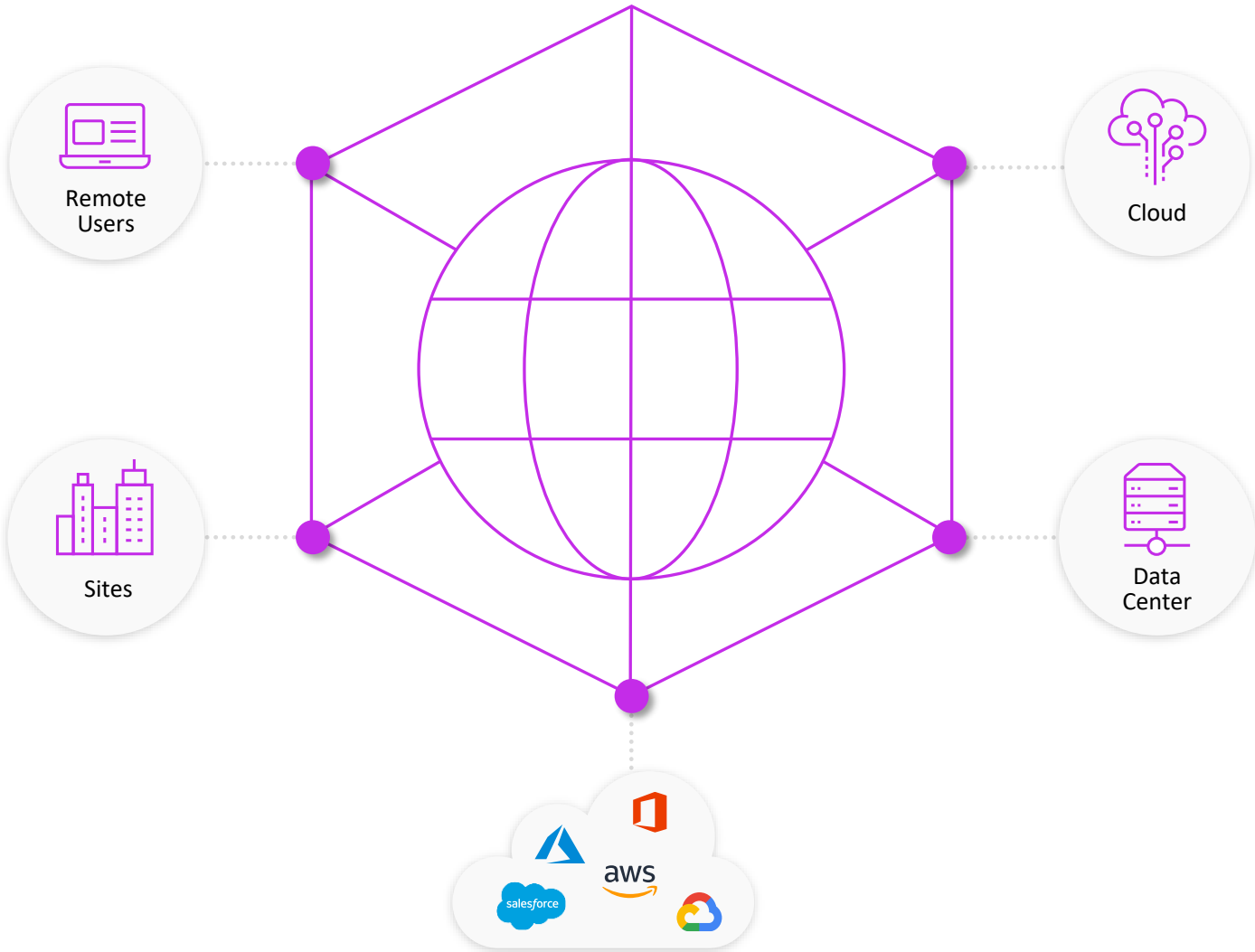


Harmony
SASE

保護遠距工作連線與負載

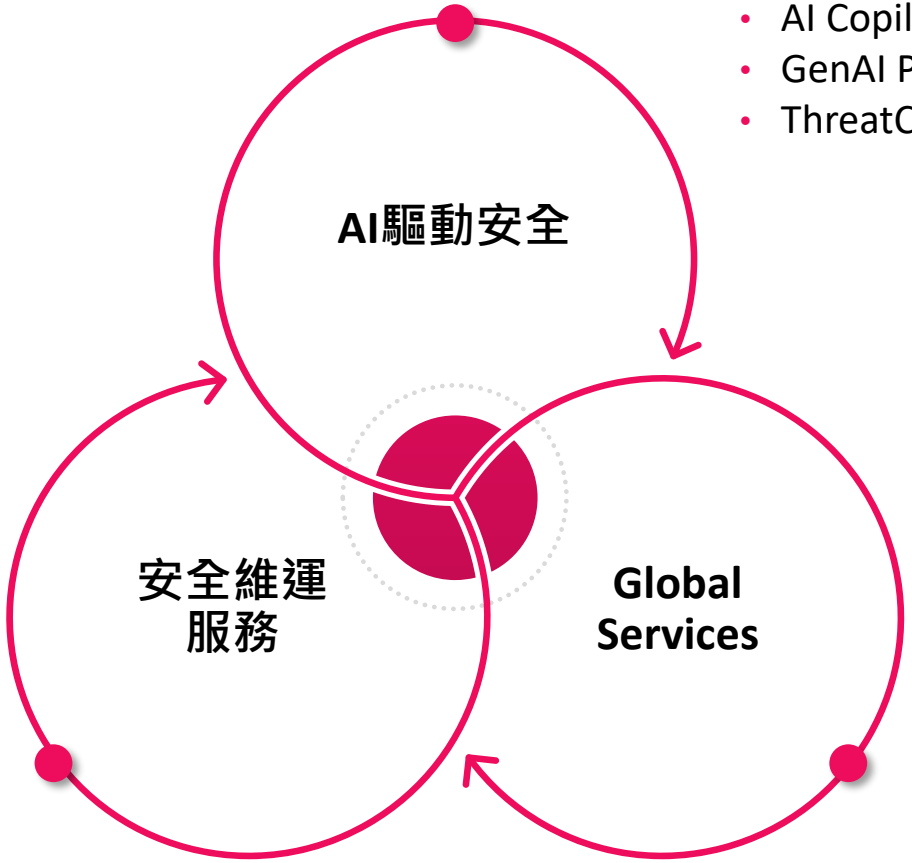
- 以雲端傳遞為主的 FWaaS
- Full Mesh連線能力
- L3-L7 防火牆
- 無代理程式存取
- Zero-Trust零信任架構

全球骨幹網路服務



Infinity
Platform

統合協作與
安全維運優化服務



- AI Copilot
- GenAI Protect
- ThreatCloud AI

XDR/XPR
- Playblocks (自動化腳本回應)
- 統合安全事件可視性

MDR/MPR
- 事件回應Incident response
- 安全顧問咨詢服務與訓練

三大資安銷售商機
WAF, SaaS Mail Security, SASE/SSE

CloudGuard WAF

CloudGuard WAF應用場域

CloudGuard WAF

Web雲化客戶

- **Web已上雲用戶**
  - 採用雲原生WAF/或未採用
  - SAP/Oracle等服務上雲
- **現行法遵要求** (合規only)
  - 資安法: 公務機關/政府
  - 上市櫃公司資安指引: 企業
  - 其他: 電商、金融、教育

On-Prem資料中心

- 地端仍有對外Web服務
  - DMZ區部署
  - 虛擬化應用
- 已採用其他WAF產品用戶
  - 預算不足 (CG WAF採Request 訂閱授權費用)
  - 非主要站台/多點部署適用
  - 無額外人力支援WAF技術

CNAPP用戶/MSSP

- 雲端服務代管與資安維運
- 容器(Container)安全應用
- API保護/API Discovery需求
- 雲端資安事件回應
- 搭配Network Security防護

基於AI驅動的WEB與API智能防護

CloudGuard WAF

CloudGuard WAF

CLOUD NATIVE WAF (可雲可地)

AI自動防護 OWASP Top 10 安全漏洞

API SECURITY & DISCOVERY

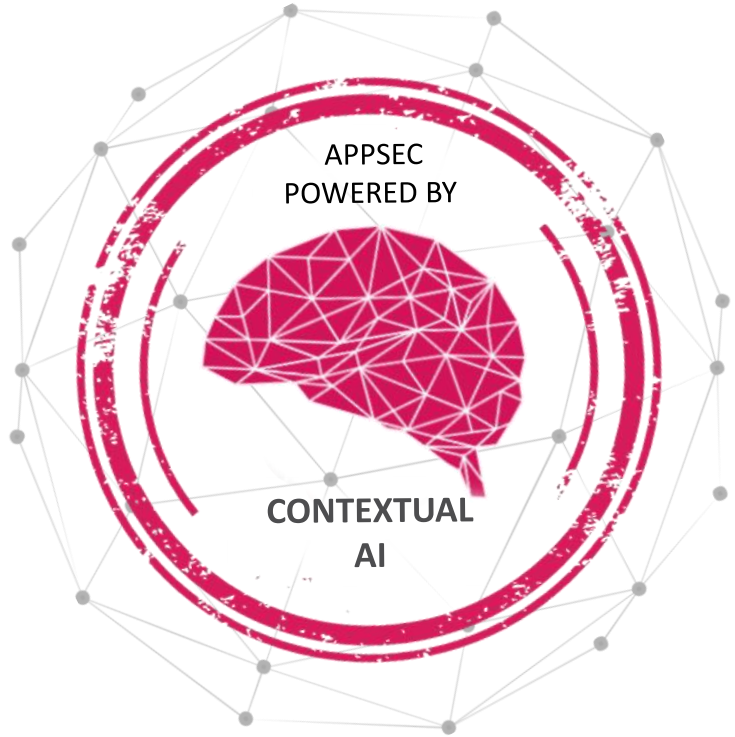
保障API呼叫安全與避免漏洞利用

BOT PREVENTION/APT防護

阻擋自動化程式攻擊

THREAT PREVENTION

整合強大的IPS防護與沙箱檔案檢測



基於AI深度學習的安全分析

CloudGuard
WAF

使用者行為分析

以使用者行為作為分析基礎
評估Web連線的可疑意圖與惡意行為

網路連線行為

從Transaction中提取攻擊指標
以預定義演算法對惡意程度分級

群體行為分析

持續透過機器學習正常使用者活動
透由數據分析來調整參數評分
自動適應並防護應用程式連線

應用程式內文檢查

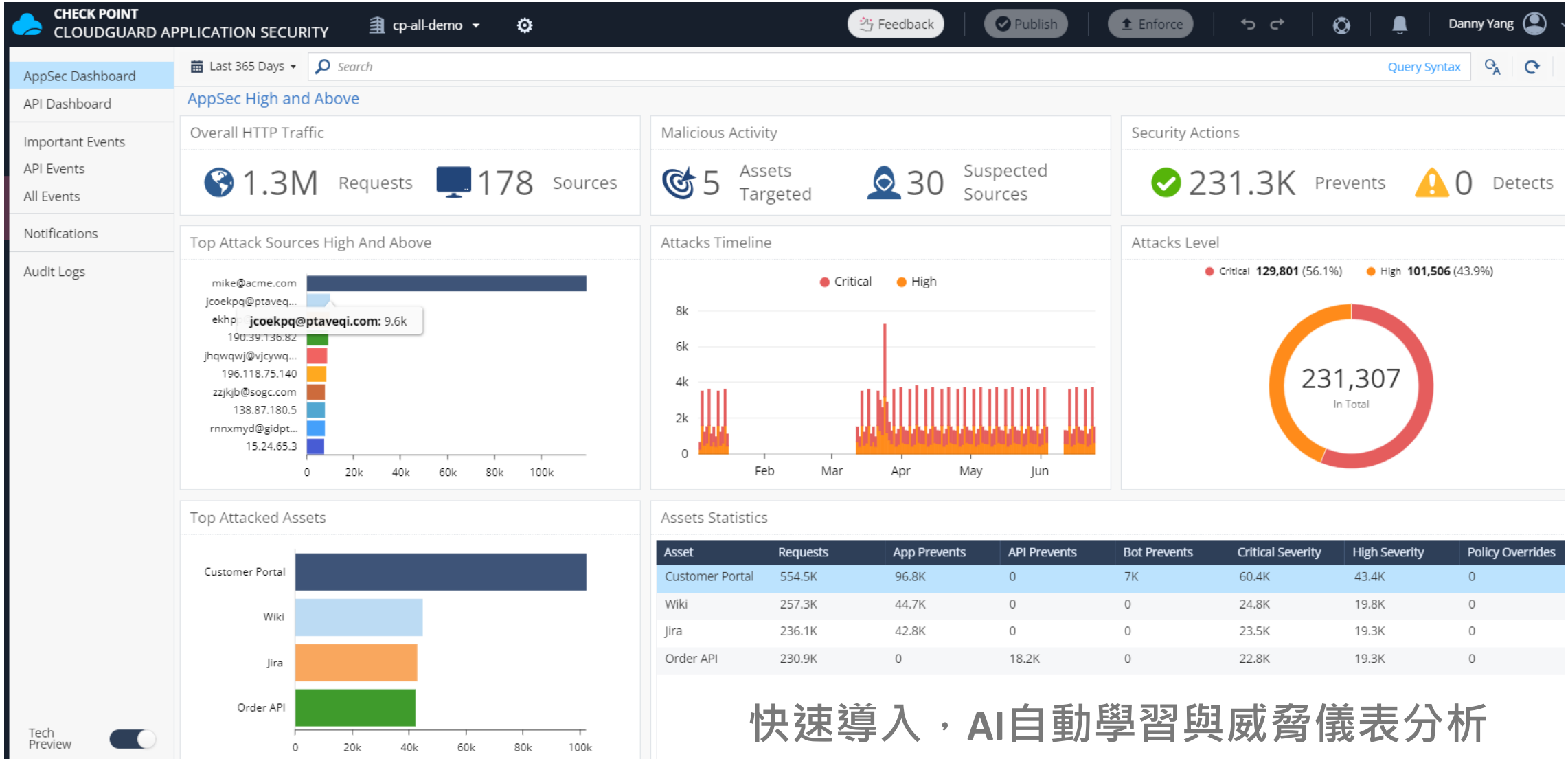
上下文字串與數值的深度學習
(Contextual)

受信任的使用者

透過建立來自受信任使用者的存取列表
加速AI學習應用程式防護

彈性部署模式: 適用於雲-地多重應用情境

CloudGuard WAF



Asset	Requests	App Prevents	API Prevents	Bot Prevents	Critical Severity	High Severity	Policy Overrides
Customer Portal	554.5K	96.8K	0	7K	60.4K	43.4K	0
Wiki	257.3K	44.7K	0	0	24.8K	19.8K	0
Jira	236.1K	42.8K	0	0	23.5K	19.3K	0
Order API	230.9K	0	18.2K	0	22.8K	19.3K	0

快速導入，AI自動學習與威脅儀表分析

Web系統安全防護

部署地點: ERP與Web站台服務　　產業型態: 傳產製造(生技醫療)

導入方案: Check Point CloudGuard WAF

CloudGuard WAF

客戶導入背景

- 興櫃公司-資安治理需求
- 未部署WAF保護對外Web服務
- 現有防火牆防護效益不彰
- 疫情後ERP服務改採Web形式

預期達成目標:

強化Web安全機制並阻擋惡意漏洞攻擊

需求與挑戰

- 資安維運與管理人力不足
- 整體IT/資安預算受限
- 需符合稽核/公司治理規範
- 簡化產品調校與自動化防護

功能驗證方式:

Nginx+Nano Agent方式部署於對外Web服務

CP勝出關鍵

- ✓ ML機制自動防護低人為介入
- ✓ 整合IPS特徵提供高防護效益
- ✓ TCO佳 (可支援多組Web服務)
- ✓ 雲端管理/提供風險分析報表
- ✓ 後續可彈性擴充 (增加授權)

後續規劃:

規劃擴充授權並涵蓋更多Web服務

Harmony SASE

Harmony SASE應用場域

Harmony SASE

欲導入零信任客戶

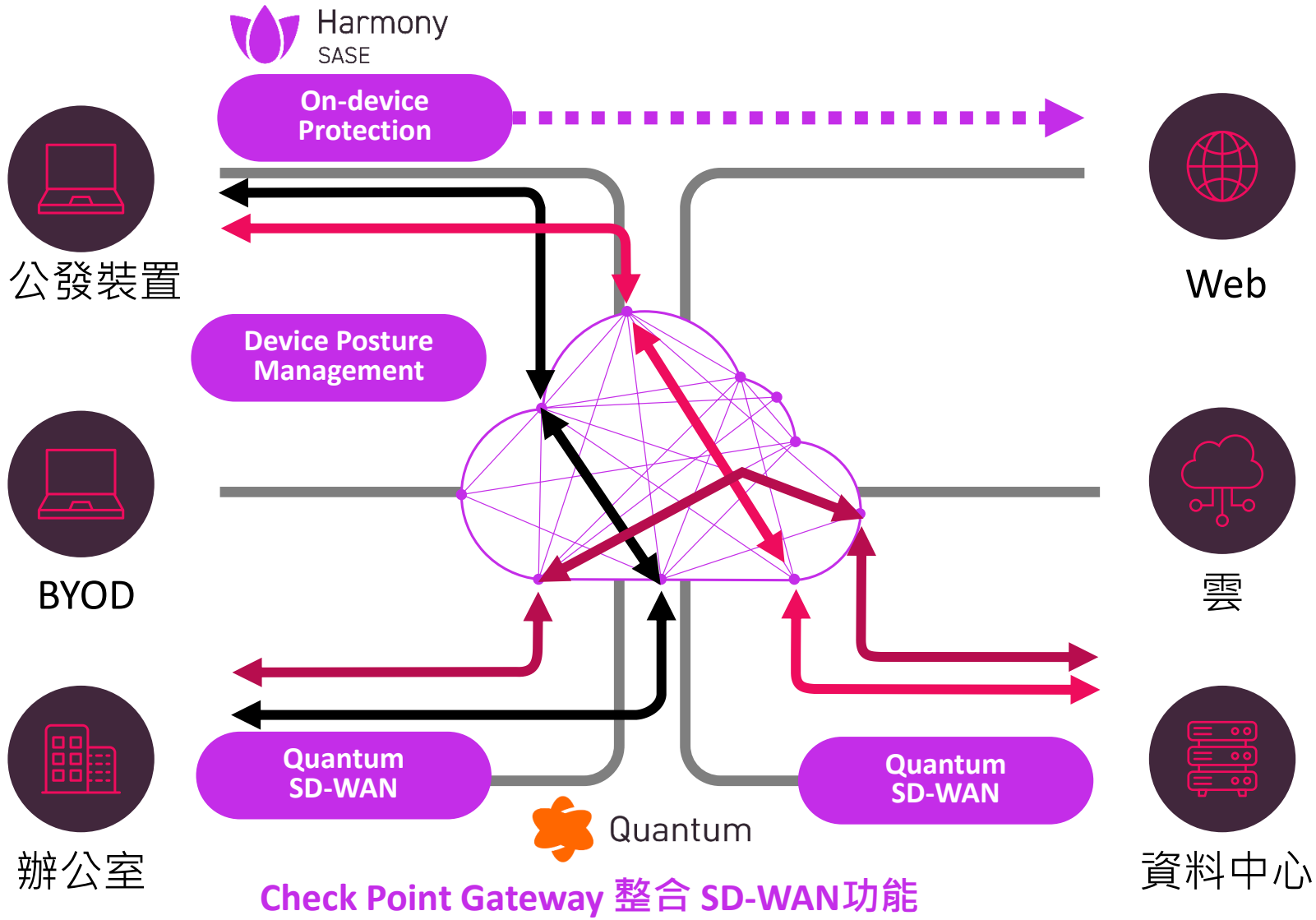
- **取代SSLVPN遠距存取**
  - 現有遠端存取安全不足
  - 評估導入ZTNA機制
  - SSL VPN服務漏洞疑慮
- **資安政策要求**
  - 公務機關/政府部門
  - 高科技製造、金融業
  - 跨國公司、多外點企業

雲化程度較高

- IT應用多為混合雲/SaaS
  - 混合資料中心(雲/地)
  - SaaS/遠距存取情境比例高
- 外點服務為傳統連線模式
  - MPLS/專線成本高昂
  - 網路/資安設備維運不易
  - 同時評估SD-WAN需求

重視資安防護需求

- 過去曾採用其他SASE方案
- 兼顧上網/內部存取安全
- 不希望架構異動過大
- 減低外部攻擊構面
- 不受設備限制/去設備化
- 目的為強化資安防護



Harmony
SASE

Hybrid SASE結合 Full Mesh & SD-WAN優化連線能力

網路效能優化 (PoPs即將落地臺灣資料中心)

Harmony SASE

服務載點遍布於70 多個全球資料中心以優化網路連線能力

Harmony SASE Use Cases摘要說明

Harmony SASE

遠端存取

情境 1 - 基於代理程式的 ZTNA

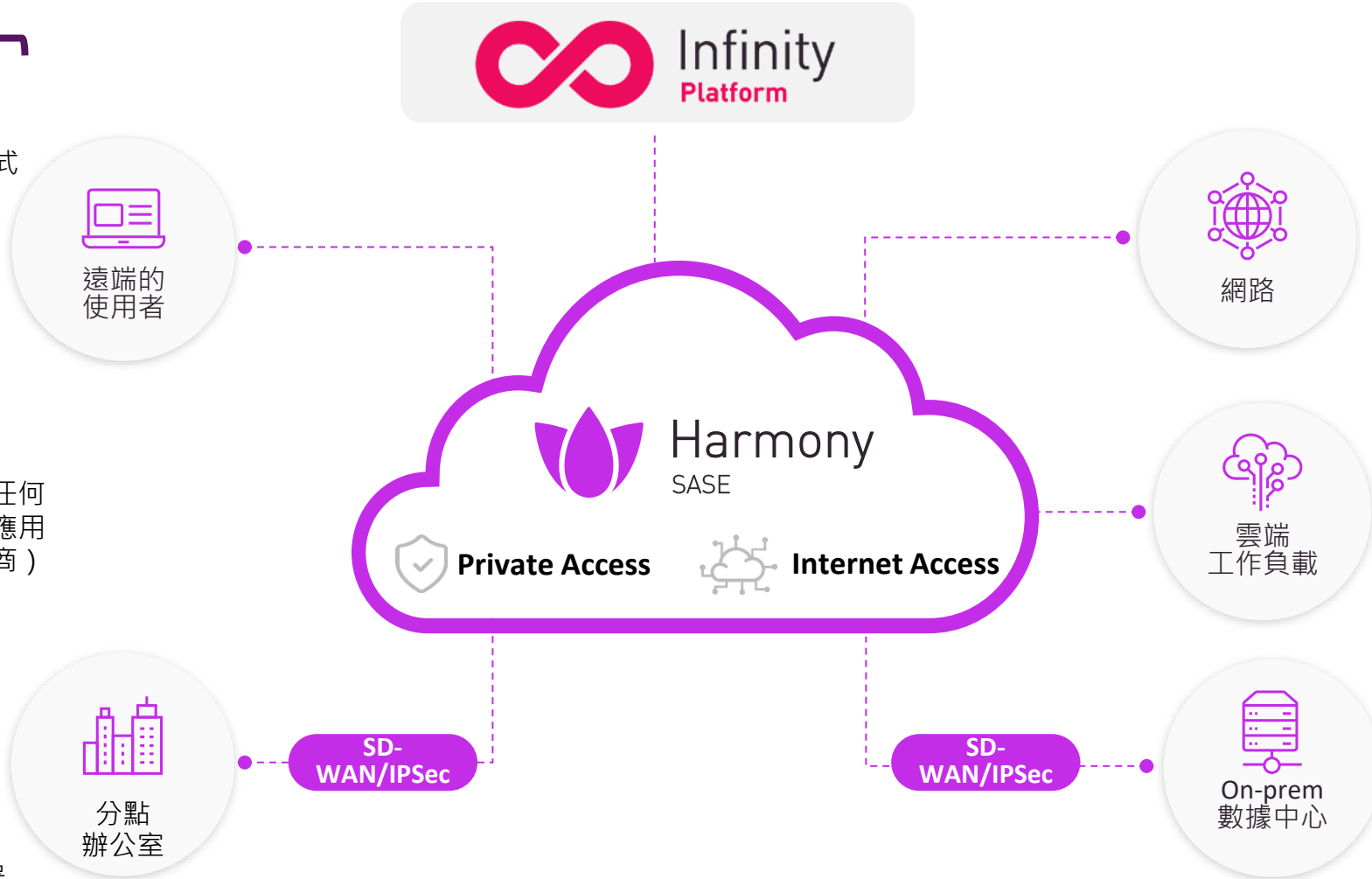
- 基於 ZTNA 原則與安全代理程式的企業應用程式存取
- 無需額外VPN 伺服器
- 支援 Windows、MAC、Linux、Chromebook、IOS 與 Android

情境 2 – 無代理程式 ZTNA 存取

- 使用入口網站從任何地方、任何裝置，採無客戶端存取企業應用程式（例如合作夥伴、承包商）

情境 3 – 分點到分點/伺服器到伺服器連線

- 使用全網狀網路拓撲，可以為專用存取建立的相同 IPSec 連線到分點、伺服器到伺服器或伺服器到用戶端流量



上網保護

情境 1 - 保護行動用戶網路的安全

- 保護遠距使用者網路瀏覽的安全存取過濾
- 適用於 Windows /Mac /Linux /Chromebook /IOS 和 Android

情境 2 - 透過上班/下班政策保護分公司流量

- 使用瀏覽器插件，使用威脅模擬/提取、零網路釣魚、DLP等功能檢查並保護所有上網流量

跨國存取安全防護

部署地點: 全球資料中心與使用者　　產業型態: 遊戲開發

導入方案: Check Point Harmony SASE (Remote/Internet Access)

Harmony SASE

客戶導入背景

- 多重雲/資料中心據點 (全球)
- 過去採用CloudFlare方案
- 開發者/廠商遠距存取頻繁
- 強化ZTNA與安全控管機制

預期達成目標:

佈建數十個服務載點，可因應多重情境

需求與挑戰

- 兼顧安全性與使用者體驗
- 需設定嚴謹的態勢管理政策
- 考量外點與使用者、BYOD
- 強化整體資安存取與防護
- 服務備援與可靠度

功能驗證方式:

於資料中心服務驗證效能與安全政策

CP勝出關鍵

- ✓ 提供獨立IP縮減外部攻擊構
- ✓ 高效電信骨幹網路與穩定性
- ✓ 授權彈性，易於擴充
- ✓ 無需硬體即可達成Full-Mesh
- ✓ 設定方式便捷部署容易

後續規劃:

視需求授權並提升資安功能 (e.g. DLP)

Harmony
Email & Collaboration

Harmony E-mail

Harmony E-mail & Collaboration應用場域

Harmony
Email & Collaboration

郵件雲化客戶

- 微軟 O365/M365用戶
  - 僅有EOP (E1/E3基本方案)
  - 加購Defender/E5包裝以上
- Google Workspace用戶
- 現行法遵要求產業
  - 資安法: 公務機關/政府
  - 上市櫃公司資安指引: 企業

已導入其他安全產品

- 上雲後仍採用LEG/SEG方案
  - Cisco, McAfee, ProofPoint
  - TrendMicro, Symantec
- 採用本地郵件安全品牌
  - 中華數位等
- 採E-Mail Hybrid Mode用戶
  - 雲地整合 (搭配Quantum)

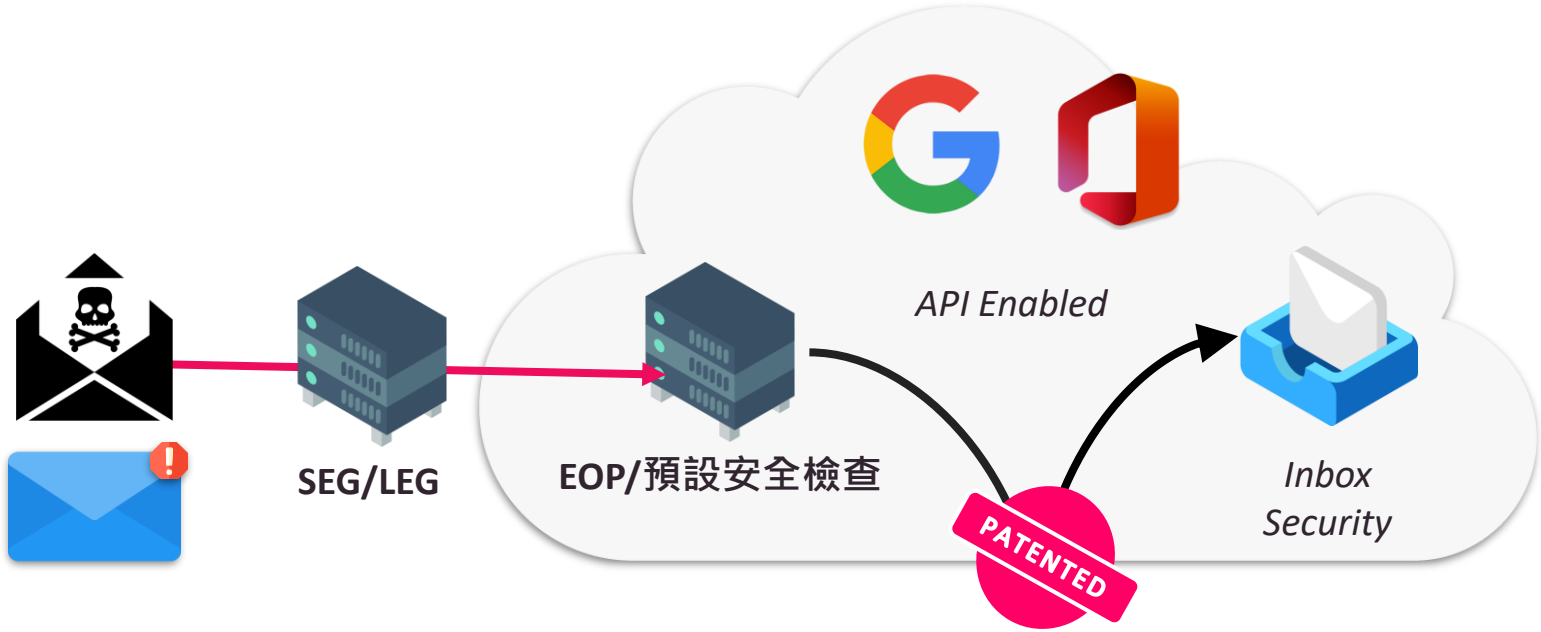
MSSP (服務供應商)

- 郵件服務代管與維運服務
- 資安事件通報與回應
- 資安事件調查分析
- 整合XDR AI分析應用
- 郵件資安加值服務

Harmony
Email & Collaboration

API介接
高效AI防禦郵件威脅

- 平階安全設計與郵件縱深防禦
- AI自動學習郵件分析模版
- API快速介接部署上線
- 直觀的統合資安事件介面
- 檢測惡意釣魚、附件與異常登入



THREATCLOUD AI

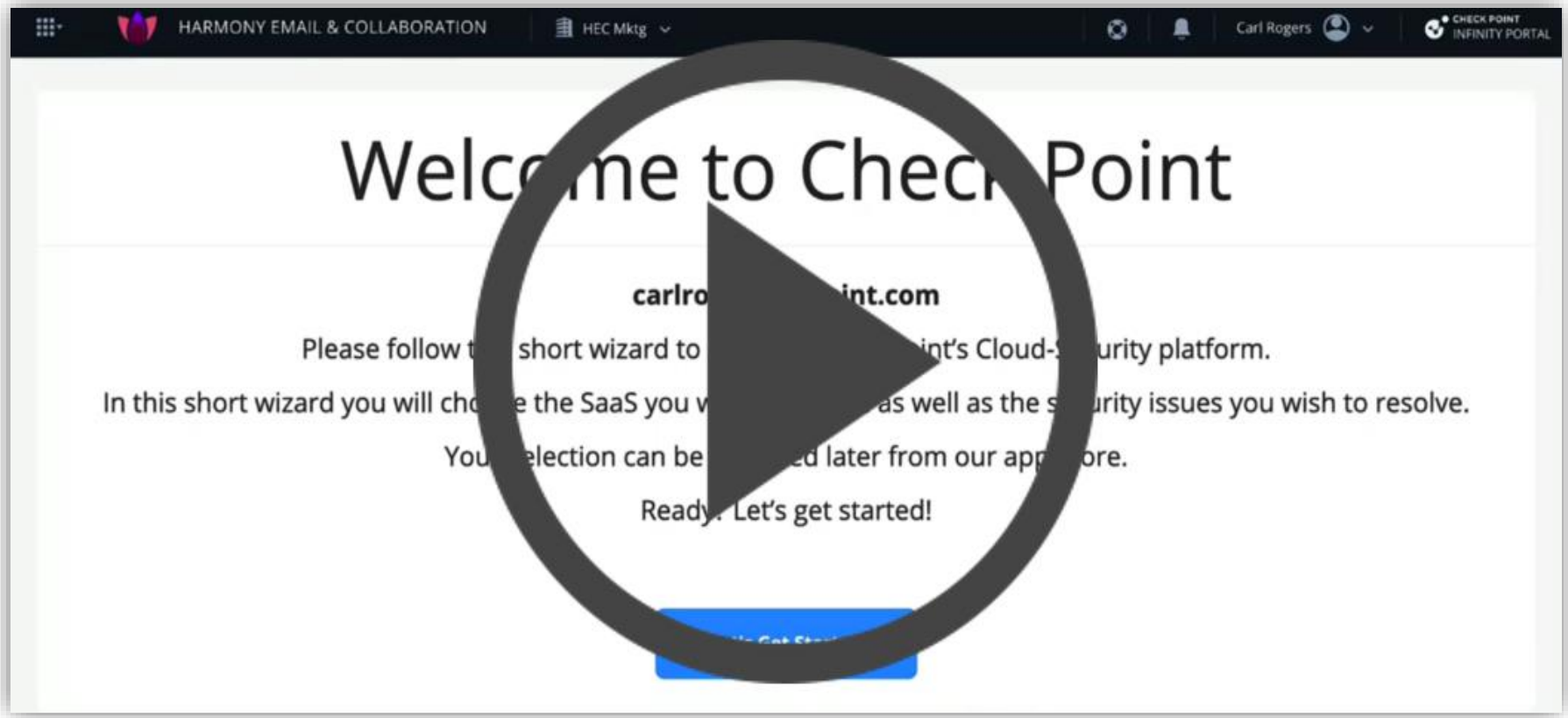
Harmony
Email & Collaboration

HEC PoC: 極速部署，無感上線

Harmony
Email & Collaboration

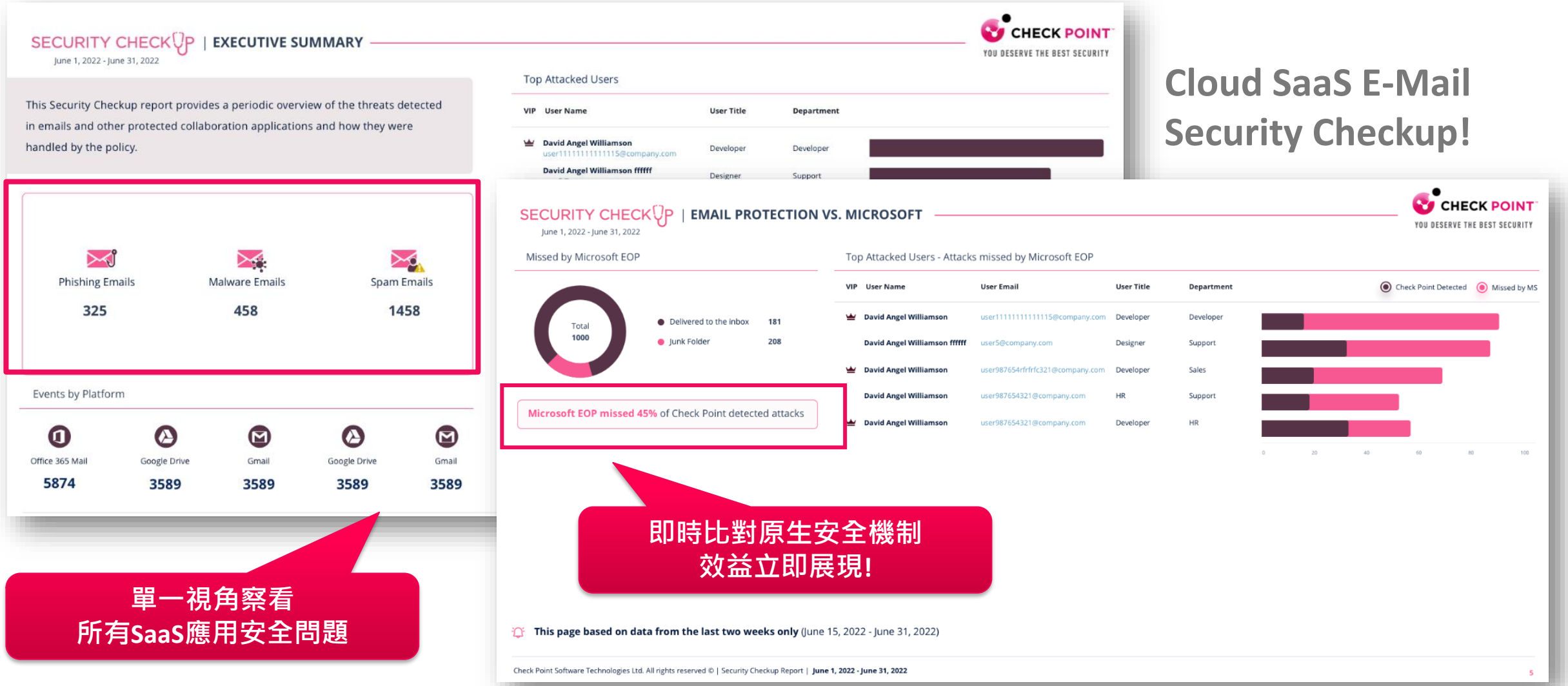
7 次點擊

30 秒



快速洞察雲端郵件風險 (5分鐘上線，7個點擊完成)

Harmony
Email & Collaboration



Cloud SaaS E-Mail Security Checkup!

單一視角察看
所有SaaS應用安全問題

即時比對原生安全機制
效益立即展現!

M365郵件安全強化

部署地點: Client OA使用者　　**產業型態: ICT解決方案代理商**

導入方案: Harmony E-Mail & Collaboration

Harmony
Email & Collaboration

客戶導入背景

- 臺灣最大ICT加值代理商
- 目標為系統上雲與敏捷開發
- 郵件全面雲端化採O365方案
- 已經訂閱M365資安(E3)

預期達成目標:
針對O365郵件以及協同工具安全強化

需求與挑戰

- 仍有少量郵件資安事件
- 建立雲端郵件縱深防禦
- 法遵需求(上市櫃資安指引)

  -郵件過濾/APT防護
- 整合安全管理降低人員負載

功能驗證方式:
API整合雲端部署，自動學習阻擋惡意郵件

CP勝出關鍵

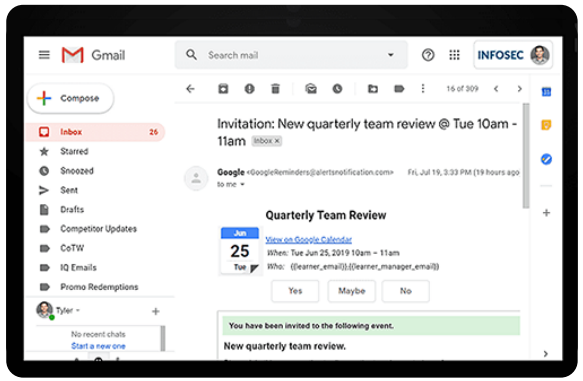
- ✓ 非侵入式快速部署介接 (API)
- ✓ 提升安全可視性(10-20%)
- ✓ 即時阻擋釣魚郵件/可疑附件
- ✓ 可支援其他協作工具應用
- ✓ 未來可納入XDR/XPR監控平台

後續規劃:
建立Teams, SharePoint等系統安全防護機制

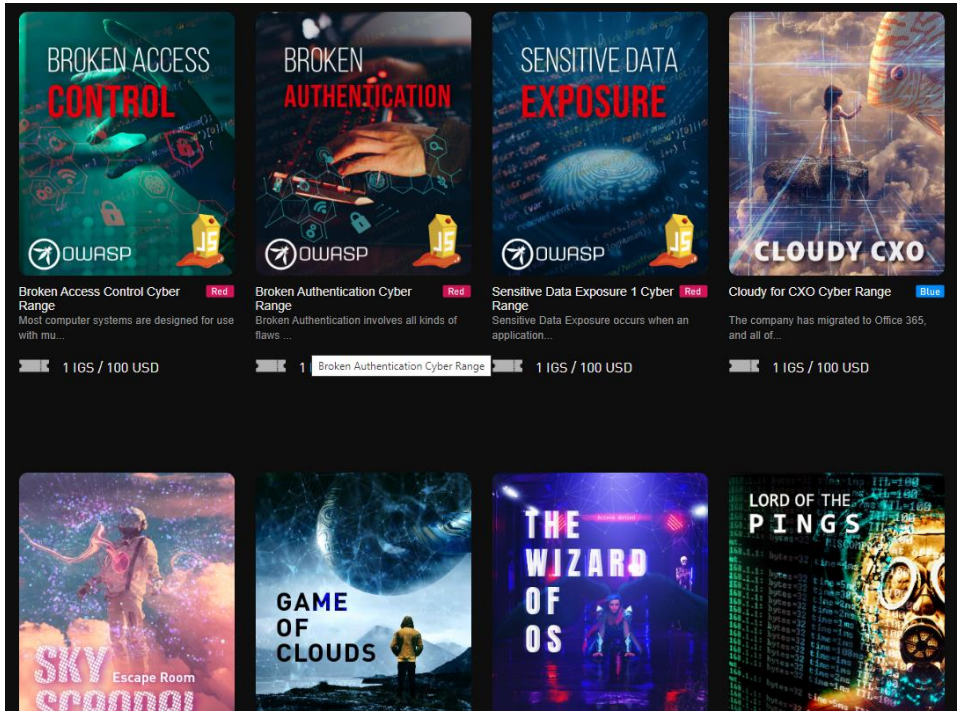
SmartAwareness & Cyber Park: 資安本質回歸至人員教育

INFOSEC IQ

社交工程釣魚演練與資安意識訓練與平台



CYBER PARK
By Check Point



Let’s Summarize

- 防火牆應用將無遠弗屆，可挖掘雲/虛擬化、微分段、遠距存取商機
- WAF需求大幅提升，把握快速銷售機會
- SASE為企業資安/網路優化首要目標之一
- 從E-Mail安全切入，社交工程/教育訓練加值
- 單一控管，全面防護的最佳選擇!
  - **鉅立資訊與Check Point團隊!**

CHECK POINT™

Thank You!

Kyle Feng, Security Consultant

kylef@checkpoint.com

YOU DESERVE THE BEST SECURITY