



AI感知，雲端交付 創新網路安全防護平台

JLead Partner Coffee Talk

Danny Yang, Cyber Security Evangelist, OCTO

2024 Mar 20

YOU DESERVE THE BEST SECURITY

Agenda

Infinity Pillars Overview

New Quantum Force & Spark

Infinity Core Service (MDR/XDR)

2024 資安攻擊態勢日趨嚴峻，臺灣企業/組織如坐針氈

威脅延續至2024，兩個月來的資安重大訊息達到9起

公告日期	公告公司	公告標題與說明
1月16日	京鼎	本公司公告部份資訊系統遭受駭客網路攻擊事件說明
1月17日	恩德	本公司公告部份資訊系統遭受駭客網路攻擊事件說明
1月19日	柏文	本公司旗下「健身工廠」會員個資遭駭客竊取事件說明
2月5日	美琪瑪	本公司公告部份資訊系統遭受駭客網路攻擊事件說明
2月5日	富野	本公司旗下分公司資訊系統遭受網路攻擊
2月15日	瑩碩生技	代子公司歐帕生技醫藥股份有限公司公告部分資料遭受駭客網路攻擊事件
2月19日	建準	本公司發生網路資安事件
2月26日	昶昕	本公司公告部份資訊系統遭受駭客網路攻擊事件說明
2月29日	中華電	說明本公司疑似資訊外流事件

資料來源：臺灣證券交易所公開股市觀測站，iThome整理，2024年3月

2023年上市櫃公司

資安事件頻仍

-資安事件即 17件

-資安相關重大訊息 6件

政府組織與

關鍵基礎設施

無法掉以輕心

<https://www.ithome.com.tw/news/161666>

零時差攻擊 (Zero-Day Attack)防護策略的質變

過去

- 具高端技術的APT組織與駭客團體
- 較為高昂的攻擊成本
- 國家級別



過時的資安防護策略

便宜行事的保守心態 (有做有交代)
只要不是產業末段班被抓交替就好

現在

- 任何有心人士
- 便宜且大量運用的攻擊手段
- AI 弭平技術差距



嶄新的資安防護策略與思維

縮短平均回應時間 (Mean-Time-To-Respond , MTTR)
限制潛在損害、評估網路資安保險

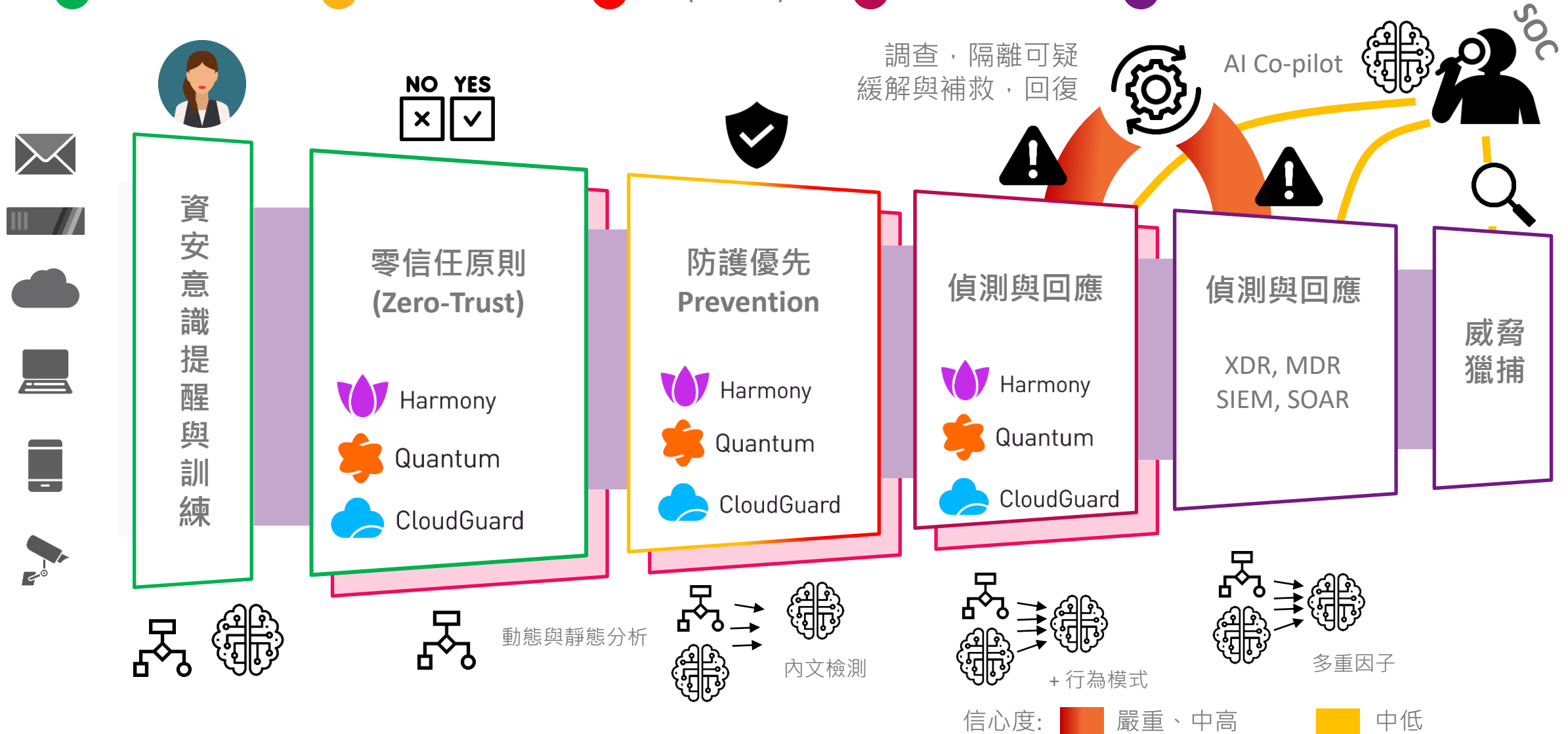


RaaS



透過AI和自動化將MTTR從數天縮減至到數分鐘

- 縮減攻擊端點構面
- 執行前預先進行防護
- 運行 (Run-Time) 保護
- 有效遏制與補救措施
- 主動分析與持續優化



Check Point: 2024 資安 x AI創新紀元

The Platform Company



雲端交付

AI感知

完整性 | 整合性 | 協作性

雲端交付: 現今資安核心與防護基礎

80%+

網路安全閘道

100%

雲端郵件
端點/行動裝置
雲端工作負載



AI智能即時威脅防護與情資引擎



90+

安全檢測引擎

50+

透由AI驅動

3B

年攻擊阻擋數量

<2 Sec

即時同步
於所有防護實施點





10+

全新AI驅動威脅檢測引擎

Quantum Titan's AI Deep Learning Engines Detect and Block Zero-Day Phishing Attacks in Real Time

New Zero-Phishing AI Engines - X4 more phishing pages detected, 42% higher detection rate

Zero Phishing

Preventing DNS Tunneling with AI Deep Learning

Deep DNS

Prevents 5X more sophisticated DNS attacks

Block C&C communications and Data theft with Deep Learning engines

Deep DGA

Brand Spoofing Prevention - Check Point Software Technologies' AI-Powered Pre-emptive Zero Phishing Prevents Local and Global Brand Impersonation Attacks

Brand Spoofing

amazon.co.jp/qzlk.cn/

Intended brand impersonation

Intended hosting site

Artificially generated

ClearSite - URLs

Massive global scale phishing campaign using malicious PDFs, identified and blocked by new ThreatCloud AI engine

Deep PDF

LinkGuard: a New Machine Learning Engine Designed to Detect Malicious LNK Files

LNK Guard

Map the macro functions and turn them to Nodes Graph

DeepVBA

The Rise of the Code Package Threat

Check Point details two recent attacks detected and blocked by

Code packages

THREATCLOUD GRAPH

Graph - URLs

AI驅動的威脅防護管理平台

10X 安全效益與整合控管

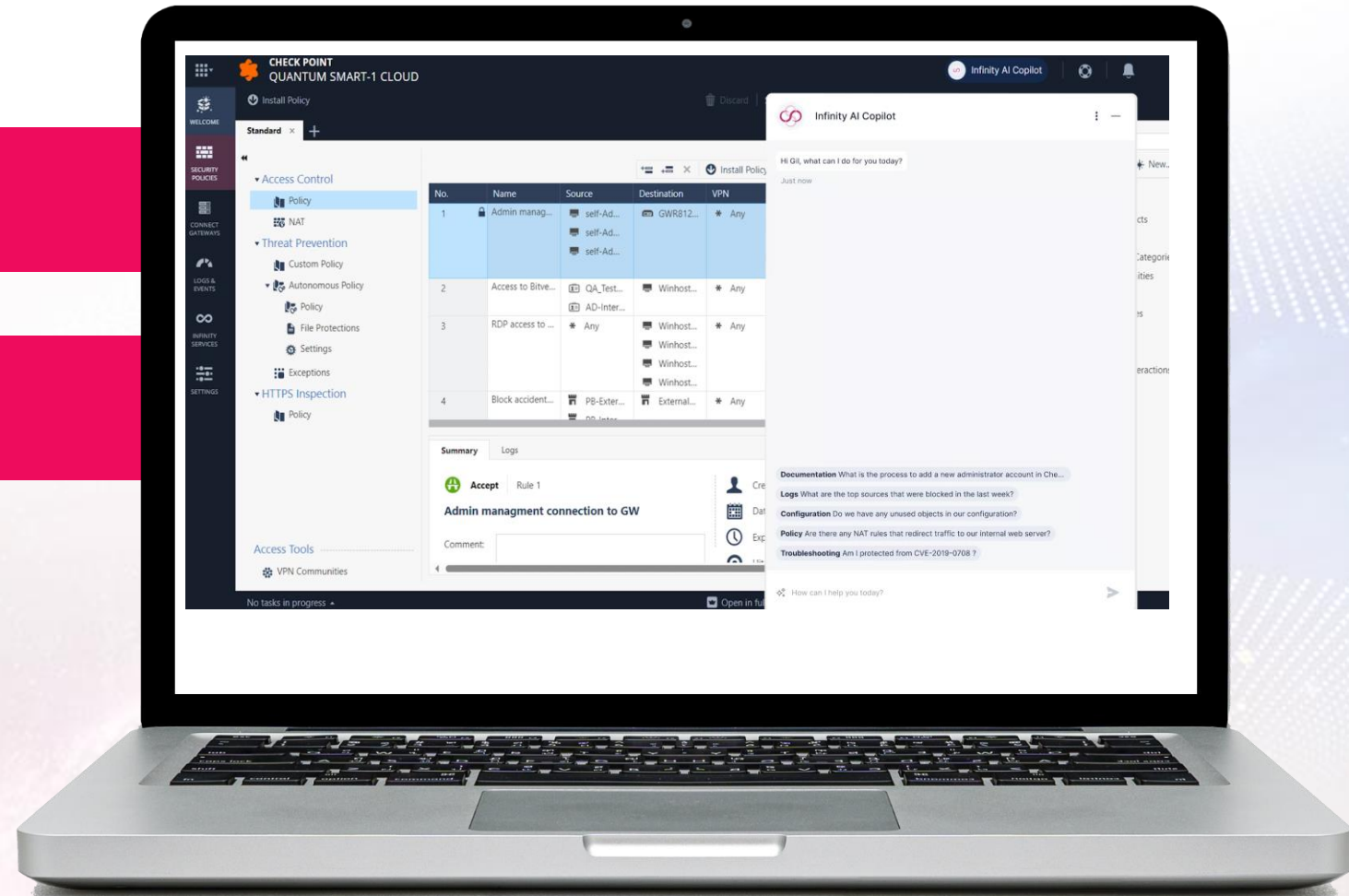


基於GPT 4.5的強大生成式AI工具

整合嵌入Infinity Platform管理系統

資安管理副駕 (Admin Copilot) NEW

資安分析師副駕 (Analyst Copilot) NEW



統合 安全管理與資安服務



網路資安



雲端資安



端點與使用者安全



PREVENTION-FIRST 防護優先安全營運管理平台



AI-POWERED 先進威脅情資引擎





Secure the Mesh Network

AI 驅動，雲端交付



Maestro HyperScale
超延展安全叢集

Quantum 安全閘道

Spark

SD-WAN

IOT

Smart-1 Cloud



Secure the Workspace

AI驅動，雲端交付

基於態勢感知與行為分析的安全存取控管



Internet Access

Private Access

Email 與SaaS協作軟體

SaaS安全態勢

端點資安(EDR/EPP)

行動資安防護



Secure the Cloud

AI 驅動，雲端交付



應用程式防火牆 (WAF)

雲端網路安全閘道

CNAPP

高效安全營運

AI 驅動，雲端交付

協作式威脅防護



全球專業服務

ThreatCloud AI

XDR/XPR

Playblocks

AI Copilot

Infinity Portal

資安代管與監測回應 (MDR)

事件回應服務 (IR)

資安顧問服務與教育訓練

2024 Zero Trust Platform 評估報告



Miercom

#1

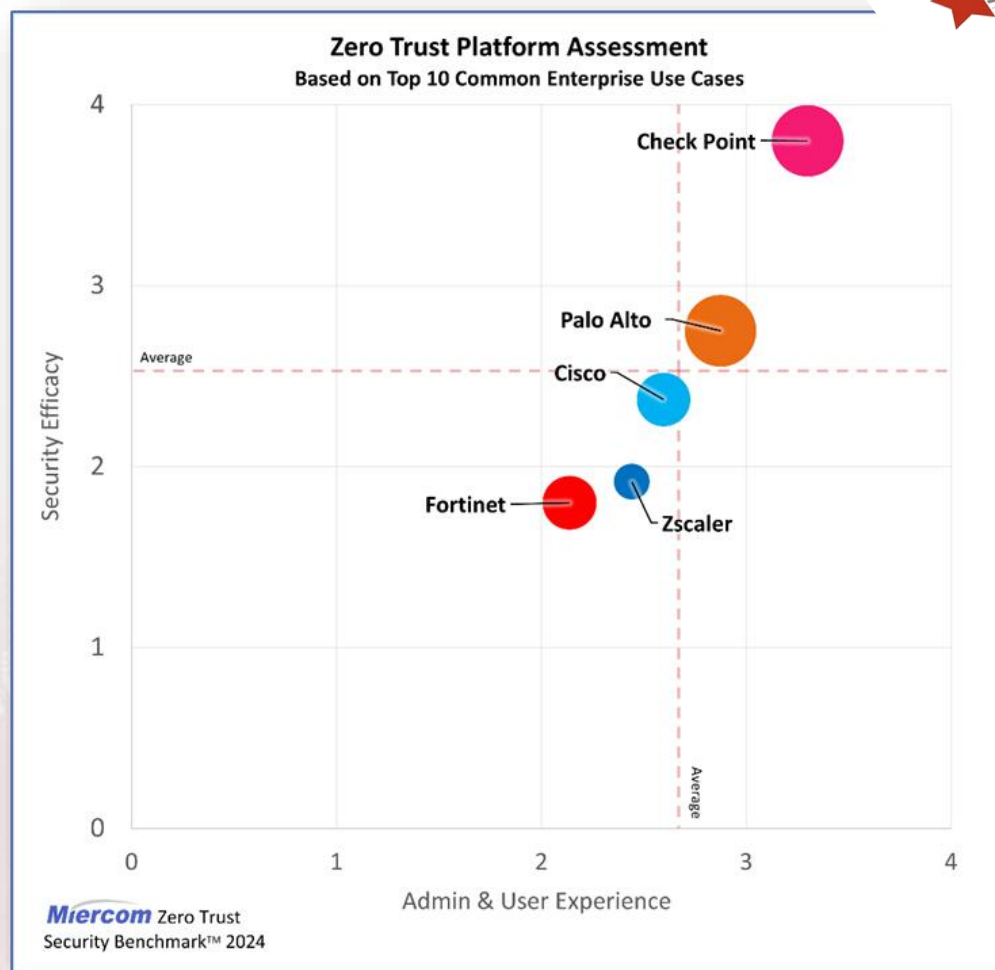
Infinity Platform

最佳

資安防護效益

最優異

管理效益 使用者體驗



2024威脅防護報告: 最佳安全防護平台與實證

2024 Security Benchmark Report

Zero+1 惡意程式威脅防護測試

最佳即時威脅防護能力!



99.8%



84%



75.4%



69.4%



47.8%



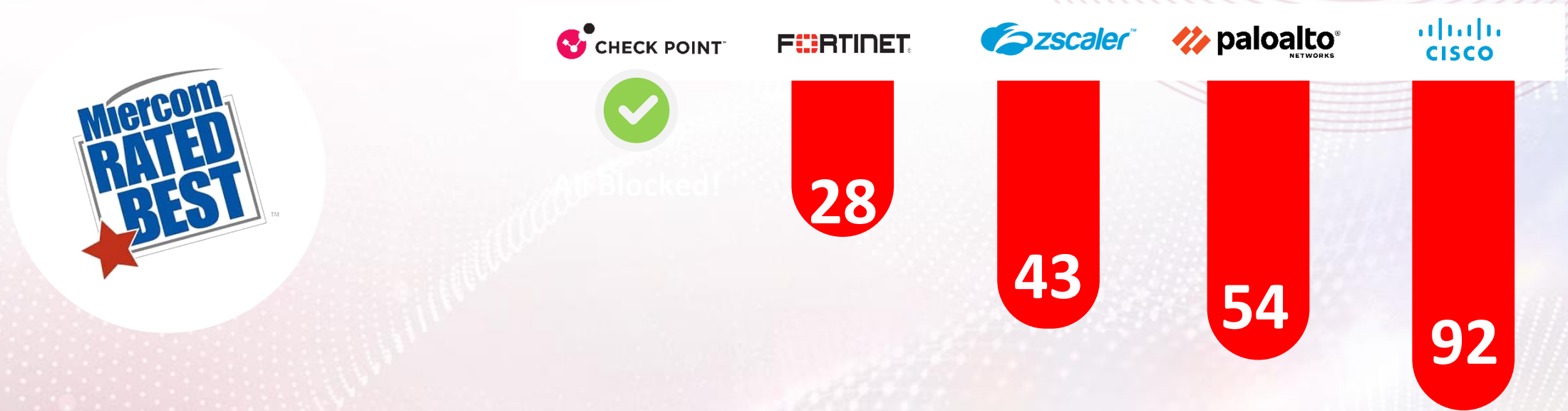
2024 最新威脅效益分析

2024威脅防護報告: 最佳安全防護平台與實證

平均每個組織每年遭受的未知攻擊數量: 177

可能會有多少惡意程式滲進您的組織?

最佳即時威脅防護能力!



Check Point幾乎阻擋所有威脅!

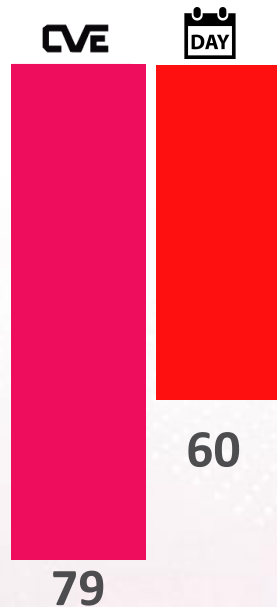
資安產品不應僅考慮性價比，隱性安全與維運成本更加重要

108X
更少的高風險漏洞數

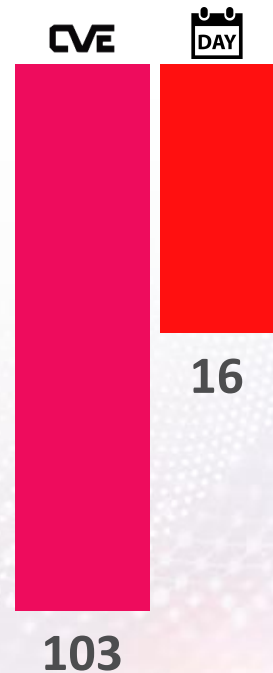
21X
漏洞回應與修復時間



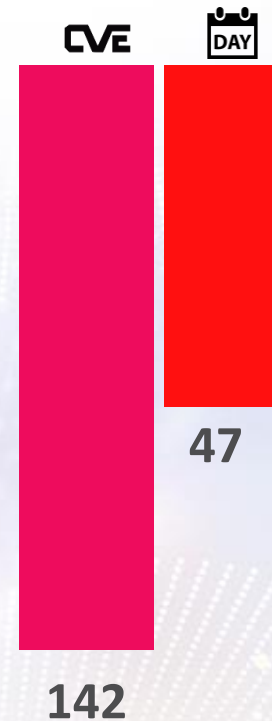
paloalto NETWORKS



FORTINET



CISCO



過去四年 (2020-2023)
重大漏洞揭露數

過去四年 (2020-2023)
修復重大漏洞(Critical & High)平均天數

Source: vendors security advisories web pages & <https://tiny.cc/urgency> Updated Jan 1st 2024

AI x 資安! 強強聯手打造全球最先進AI Cloud Protect方案



結合NVIDIA's BlueField 3 DPU 與 DOCA Framework的最佳化安全

- 針對AI特定威脅的強大防護能力
- 具擴展性的無縫整合模式
- 無需妥協的最佳化系統效能

長期合作且信任的戰略合作夥伴!

- HyperScale Orchestrator
- Smart NIC for New Quantum Force
- ThreatCloud AI (Cuda AI)





Quantum

橫跨資料中心與外點的網路防護

Check Point Infinity Platform

AI驅動，雲端交付

2024全新登場:

Quantum Force

結合AI運算與雲端傳遞技術
10款全新網路安全防護閘道!



Quantum
Force



50 AI-Based
威脅防護引擎

*Powered by ThreatCloud

業界最佳標準

99.8% 阻擋率

未知惡意程式防護能力

2X

處理效能

網路介面

綠能節電

2024 全新推出: Quantum Force系列



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機種



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

最佳威脅防禦能力
-99.8%

50 x AI分析引擎

2X 安全效能且更節能



Quantum
Force

Quantum Force Series 9100 – 9800 (6 models)

AI-Powered, Cloud-Delivered

邊界網路安全

威脅防護效能
最高可達 **20Gbps**

防火牆效能
最高可達 **400Gbps**



最高效節能1U網路閘道
• 0.88 Watt/Gbps

最高可至 **8 x 25Gb ports**
• 最高可至 **20 x 10Gb ports**
2x 擴充插槽 (9400以上)



Quantum
Force

Quantum Force 19200

AI-Powered, Cloud-Delivered

企業網路安全閘道

36.9Gbps
威脅防護效能

超高防火牆效能
處理能力最高達 800Gbps



最佳性價比
優異安全效益

多款網路介面
100G/40G/25G

中大型企業網路資安首選



Quantum
Force

Quantum Force 29200

AI-Powered, Cloud-Delivered

資料中心級網路安全閘道

63.5Gbps
威脅防護效能



最佳性價比
優異安全效益

超高防火牆效能
處理能力最高達1.4Tbps



多款網路介面
100G/40G/25G

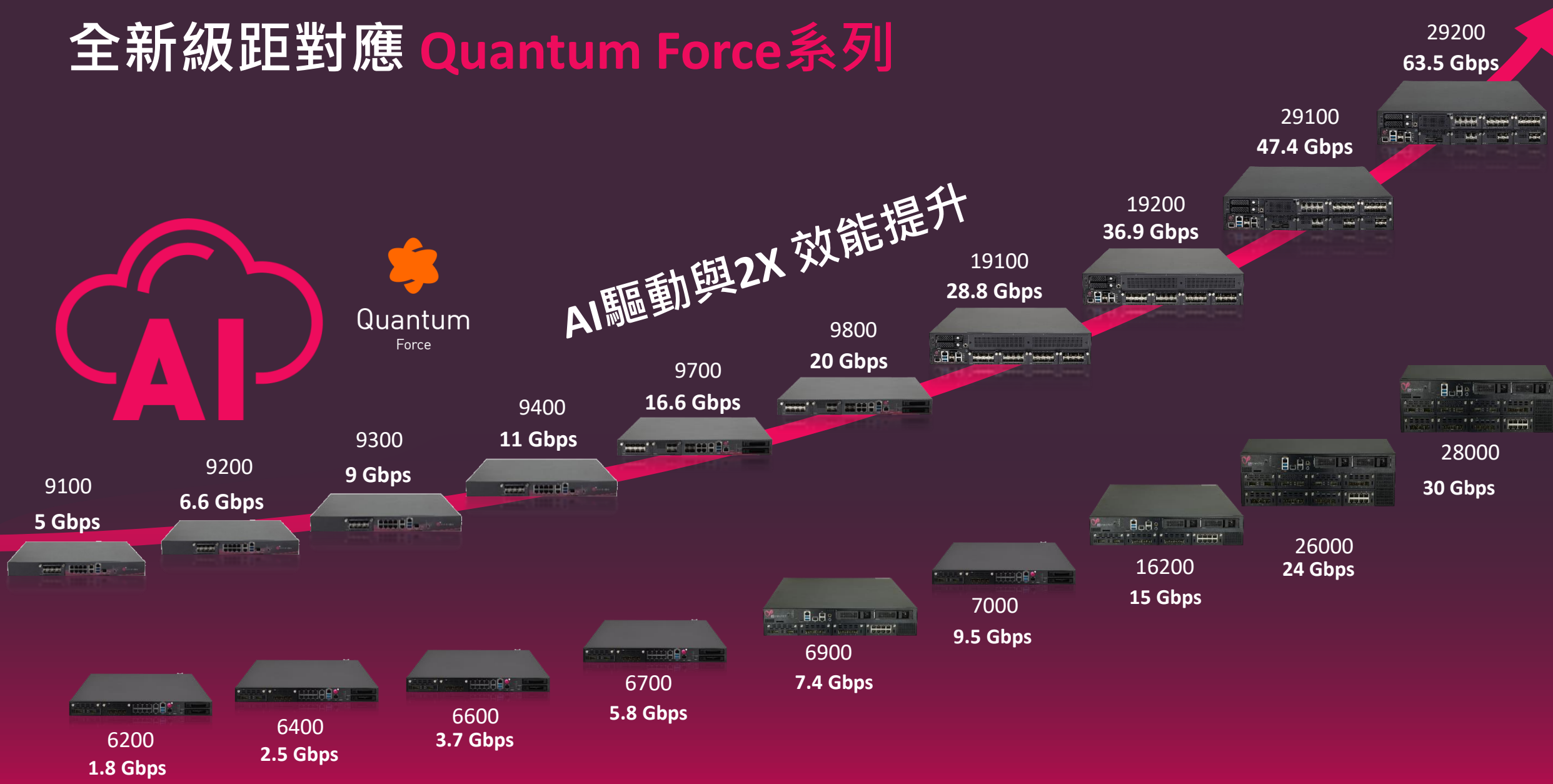
資料中心與高速網路資安首選

全新級距對應 Quantum Force系列



Quantum
Force

AI驅動與2X 效能提升





隨需擴充的超高速100G網路介面介接能力

具備靈活性和模組化，以滿足網路介接需求

- 100G核心網路與資料中心存取
- 充沛的1/10G 伺服器直連網路介接
- 可配合整體網路區段與微分段服務

最高達 7x 網路擴充槽



Up to **56** x 1/10 GbE

(or)



Up to **28** x 10/25 GbE

(or)



Up to **14** x 40/100 GbE



類Chassis叢集架構，最高可達1Tbps威脅防護效能！

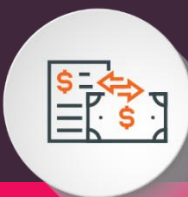
業界最先進的超延展網路安全叢集(HyperScale)



可動態擴充至：
1Tbps威脅防護處理效能



無縫遷移和添加可用資源
系統無需停機



99.999% 運行保障能力
與智能化負載分散

Maestro Hyperscale System
w/ Intelligent Load Sharing



Orchestrators

Firewalls

全新Sizing規格依據 (TLS Inspection)與優規參考

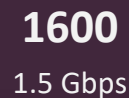
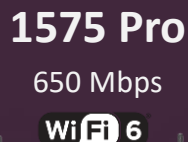
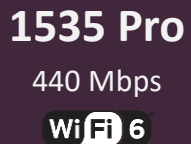


	9100	9200	9300	9400	9700	9800
Latency (Lab)	10μSec	9μSec	9μSec	1.85μSec	1.85μSec	1.85μSec
FW效能 (Ent.)	55Gbps	60Gbps	70Gbps	72.6Gbps	129Gbps	185Gbps
TP效能 (Ent.)	4.95Gbps	6.6Gbps	9Gbps	11Gbps	16.6Gbps	20Gbps
TLS+TP	2.96Gbps	3.6Gbps	5.1Gbps	5.5Gbps	9.6Gbps	10.1Gbps
TLS+TP (Web)	1.6Gbps	2Gbps	2.9Gbps	3.2Gbps	5.8Gbps	6Gbps
TLS+IPS (Web)	2.3Gbps	2.9Gbps	3.9Gbps	4Gbps	7.3Gbps	7.9Gbps

	19100	19200	29100	29200
Latency (Lab)	1.85μSec	1.85μSec	1.85μSec	1.85μSec
FW效能 (Ent.)	200Gbps	245Gbps	365Gbps	63.5Gbps
TP效能 (Ent.)	28.8Gbps	36.9Gbps	47.4.6Gbps	500Gbps
TLS+TP	14.1Gbps	18.6Gbps	24.36Gbps	24.6Gbps
TLS+TP (Web Mix)	10.2Gbps	11.2Gbps	14.6Gbps	18.6Gbps
TLS+IPS (Web Mix)	12.9Gbps	15.7Gbps	19.3Gbps	25.04Gbps

全方位安全首選: Quantum Spark-因應SMB與外點需求

超高性價比，內建資安全功能(SD-WAN+IoT)，本機+雲端控管，中文介面



小型組織/Soho (1-50 Users)

中小型企業/分點 (50-500 Users)

中型企業 (500-1000 Users)



Infinity
Core Services

新世代資安服務與智能維運 Infinity Core Service

企業組織資安風險是否有被具體識別且有效因應？

可能被攻擊的模式？

公司核心業務
安全風險？

資安長

目前資安強度是否
足夠承受外部威脅？


針對新推出的法規
是否有符合？

我們是否已正確地對
預算與資源優先分級？

CHECK POINT IS YOUR TRUSTED CYBERSECURITY PARTNER!




ASSESS
Security Evaluation and Pentesting



- Risk Assessment
- Penetration Testing
- Maturity Assessment
- Readiness Assessment

[View more](#)

TRANSFORM
Consulting and Optimization



- Remote consultation days
- Advanced Technical Account
- Infinity Security Design
- Hybrid Cloud Security

[View more](#)

MASTER
Upskilling and Training



- Training Courses
- Boot Camps
- HackingPoint
- Self-Paced Cyber Security Training

[View more](#)


RESPOND
Incident Respond and MDR



- Incident Response
- Expert Malware Analysis
- Expert Threat Briefing
- Digital Forensics

[View more](#)

MANAGED
Managed SOC and NCC



- MXDR with Managed SIEM
- Managed Firewalls
- EDR with Agent Management
- Managed CNAPP

[View more](#)



戰略式資安
顧問服務



資安平台
安全方案



資安設計/實施
系統健檢與優化



持續訓練
有效識別



事件回應/監控
安全代管代維

+30 services!

重塑資安韌性 縮短回應時間



100% ⚡

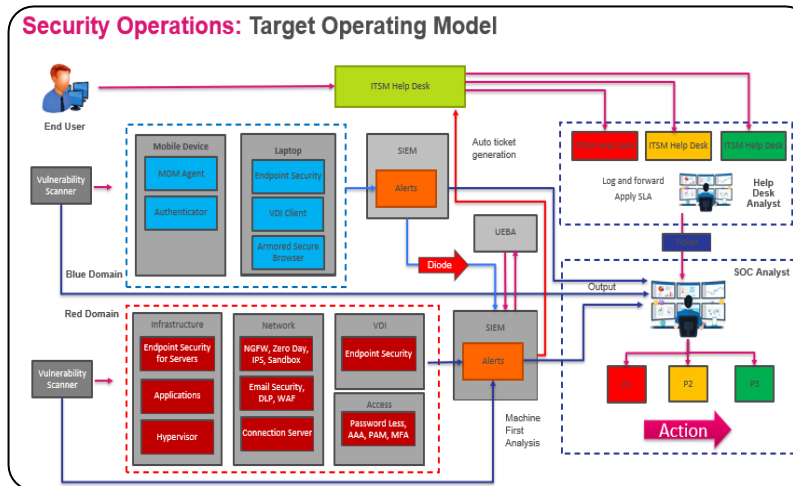
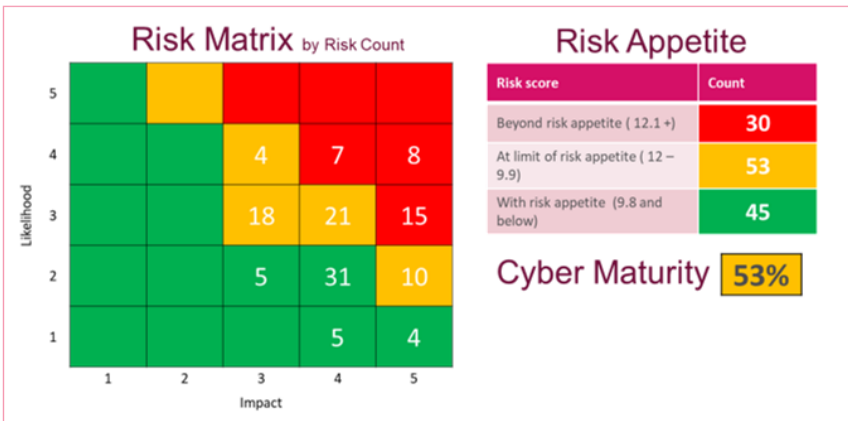


- Managed Firewalls
 - EDR with managed agents
 - MXDR with Managed SIEM
 - Managed CSPM and CNAPP
 - Cloud Migration & management
- 資安代管代維服務
- MXDR
 - MDR
 - Incident Response
 - Threat Hunting
- MDR & IR 24x7 監控與回應
- CISO Academy
 - Certifications
 - Skills Training
 - Security Awareness
 - Phishing Simulation
- 教育訓練與資安意識提升
- Staff Augmentation/ Resident engineer
 - Optimization and fine tuning
 - Complex Project implementation
 - Project Management
 - Life cycle management
- 原廠專業服務
- Cyber Risk Assessment
 - Threat Modeling
 - Cloud Maturity
 - Pen Testing
- 戰略式資安顧問服務

深具產業經驗與資安實務的全球顧問團隊

多數背景為四大事務所顧問、安全架構師、資安技術專家

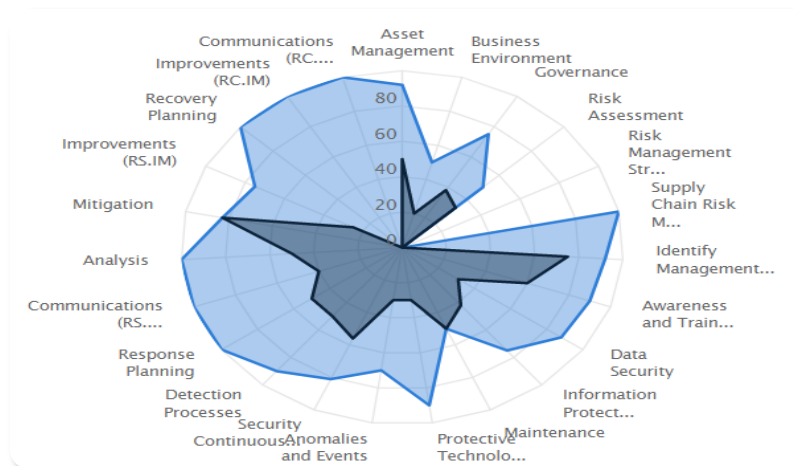
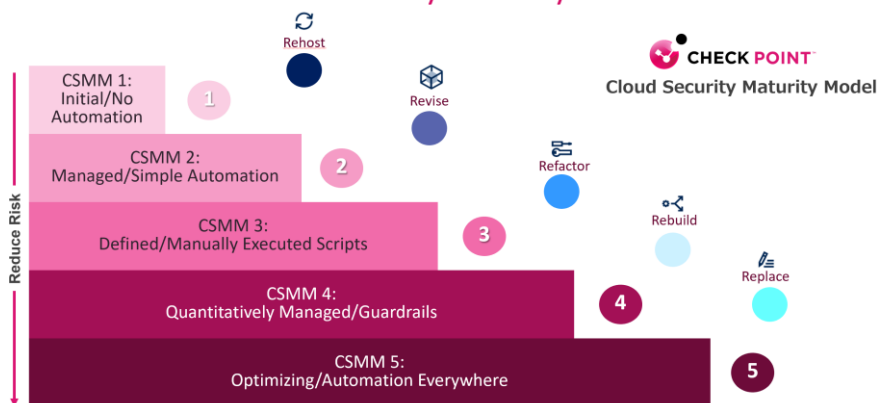
EXECUTIVE RISK DASHBOARD



戰略式資安顧問服務內容

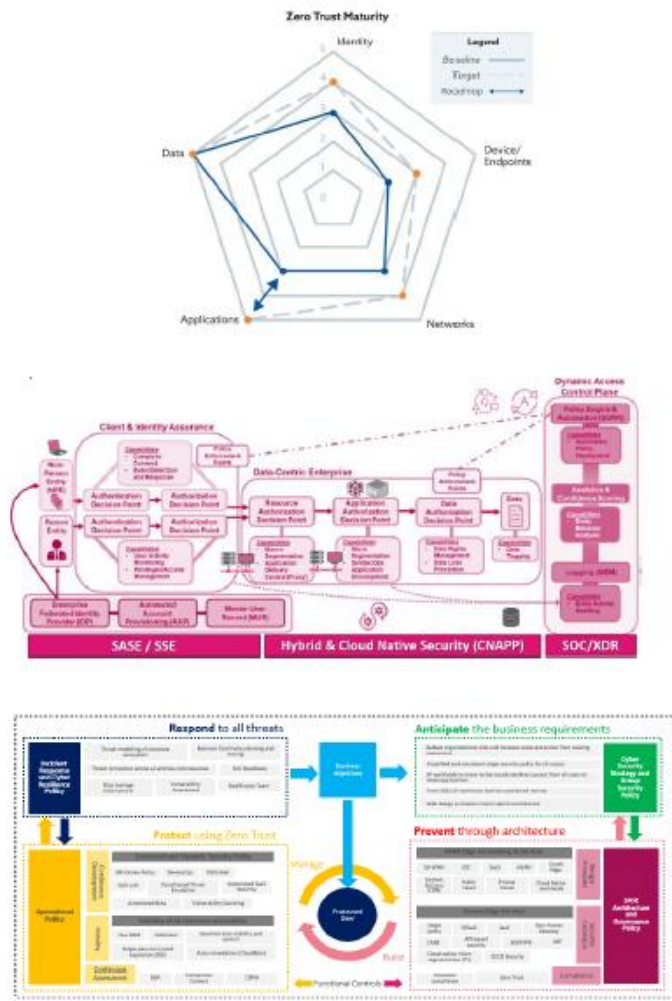
- 資安風險評估/缺口分析，滲透測試，資安架構檢視
- 零信任成熟度評估與架構檢視
- 資安框架設計 (NIST, NIS2, CIS)
- 雲端安全成熟度分析與評估
- OT/IoT 風險評估
- 勒索軟體因應措施評估
- 資安破口因應措施評估
- 資安架構檢視與建議/Cyber Mesh
- 資安情資報告與暗網探勘服務

Check Point - Cloud Security Maturity Model



應用案例: 臺灣高科技製造業內網安全與零信任架構

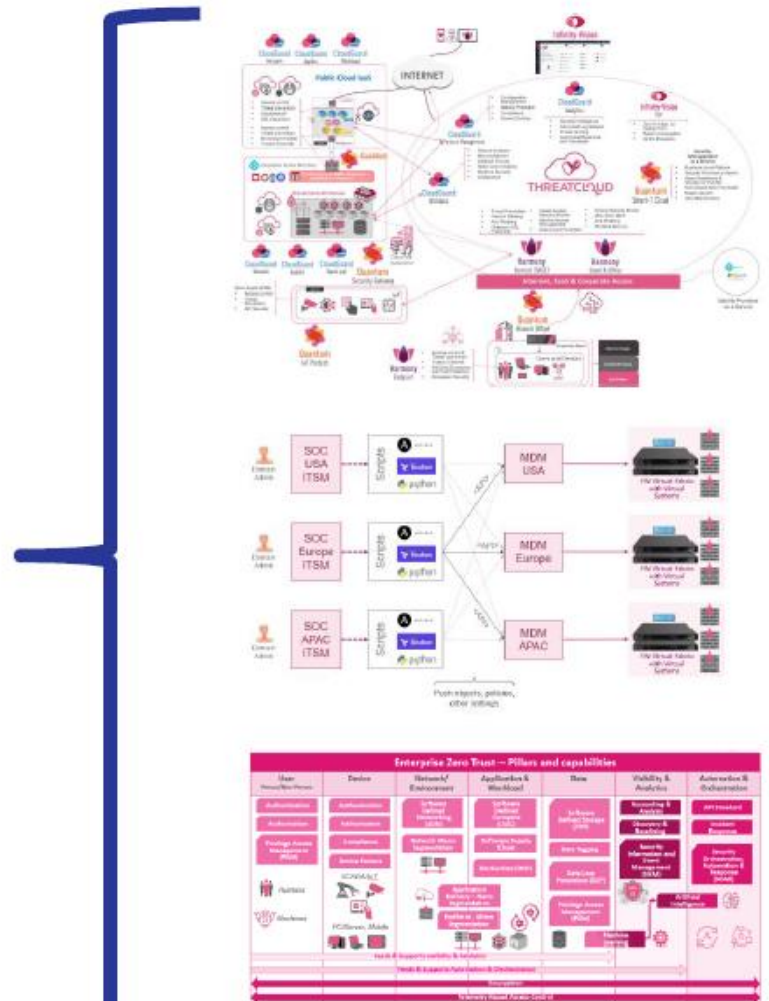
ASSESSMENT



REPORT

The report cover features the Check Point logo at the top, a central image of a hand holding a tablet displaying a padlock icon, and the title 'Zero Trust Workshop Report' at the bottom. A small text box at the bottom left of the cover reads: 'Prepared for Check Point Customer on 01 December 2022. ©2022 Check Point Software Technologies. Architecture team.'

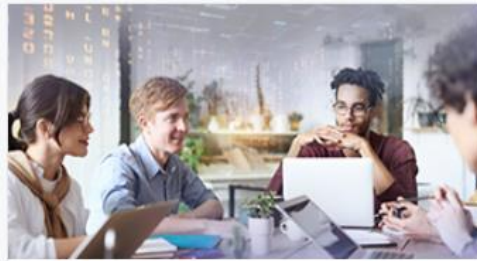
ARCHITECTURE



方案實施與系統優化，確認資安措施有效性



Advanced Technical Account Management (weekly working sessions)



Advanced Technical Account Management (biweekly working sessions)



Advanced Technical Account Management (monthly working sessions)



Maestro deployment (up to 2 Security groups or 2 VS instances)



Jumpstart for Enterprise Appliance with NGTX blades package



Jumpstart for High-End Appliance with NGTX blades package



SmartOptimize



Gateway HealthCheck

原廠專業技術服務 (PS)

- ATAM (Advanced Technical Account Management)
- JumpStart package
- Maestro Deployment
- Remote Consultation
- SmartOptimize
- HealthCheck

持續有效性安全教育訓練，提升組織整體安全意識



Distinguish Yourself With Globally-Recognized Certifications
by Globally-Recognized Organizations



CISO'S SECRETS
PODCAST

World's leading CISOs share all their SECRETS. Tune in now!

Logos: HBO MAX, NCR, SIEMENS, CardinalHealth, CATERPILLAR, GitLab



CHECK POINT

CCSA
Certified Security Administrator

CHECK POINT CERTIFIED SECURITY ADMINISTRATOR (CCSA)

- AUDIENCE**
Technical professionals who support, install, deploy or administer Check Point products.
- GOALS**
Learn basic concepts and develop skills necessary to administer IT security fundamental tasks.
- PREREQUISITES**
Working knowledge of Unix-like and Windows operating systems and TCP/IP Networking.

CHECK POINT

CCSE
Certified Security Expert

CHECK POINT CERTIFIED SECURITY EXPERT (CCSE)

- AUDIENCE**
Technical Professionals who architect, upgrade, maintain, and support Check Point products.
- GOALS**
Learn advanced concepts and develop skills necessary to design, deploy, and upgrade Check Point Security environments.
- PREREQUISITES**
CCSA Training or Certification, fundamental Unix and Windows knowledge, certificate management experience, system administration and networking knowledge.

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

INFOSEC IQ

資安意識訓練與社交工程釣魚演練平台



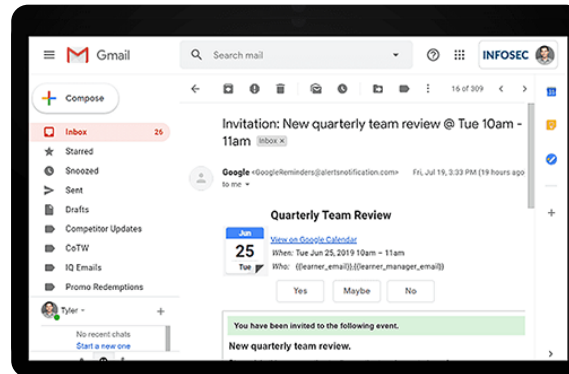
Security Awareness
LEARN MORE

Phishing Simulations
LEARN MORE

Program Automation
LEARN MORE

Reports & Assessments
LEARN MORE

Empower Your Workforce.
Secure Your Organization.



BROKEN ACCESS CONTROL
OWASP JS
Broken Access Control Cyber Range
Most computer systems are designed for use with mu...

BROKEN AUTHENTICATION
OWASP JS
Broken Authentication Cyber Range
Broken Authentication involves all kinds of flaws ...

SENSITIVE DATA EXPOSURE
OWASP JS
Sensitive Data Exposure 1 Cyber Range
Sensitive Data Exposure occurs when an application...

CLOUDY CXO
Cloudy for CXO Cyber Range
The company has migrated to Office 365, and all of...

SKY SCANDAL
Escape Room

GAME OF CLOUDS

THE WIZARD OF OS

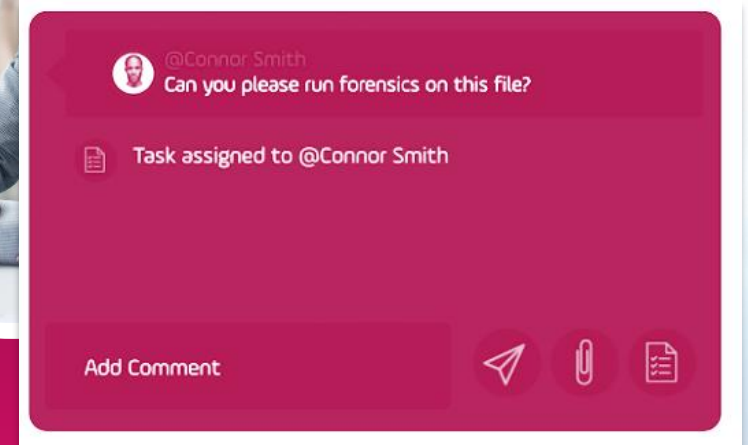
LORD OF THE PINGS

24x7 MDR+IR 專業監控回應服務



透過即時通訊、電郵、熱線(臺灣0080專線)
與專屬介面與全球安全專家在線聯繫

- 全年無休的監控回應團隊
- 全球時區專業技術支援
- 可即時分析事件並縮短回應時間
- 直覺化與易於操作的使用者介面



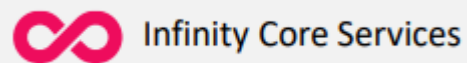
IGS Managed Services

多樣化資安解決方案代管維運



SOC-as-a-Service

- MDR \ MPR \ IR
- XDR \ XPR
- Managed SIEM \ SOAR
- ✓ Microsoft Sentinel and Defender XDR



- Harmony Endpoint
- Harmony Email & Collaboration
- Check Point SASE
- ✓ CrowdStrike / Sentinel One / Microsoft Defender for Endpoint



NOC-as-a-Service

- Check Point Quantum and Maestro
- SD-WAN
- Networks
- ✓ Cisco / Cisco Meraki / Extreme / Palo Alto / Fortinet



Cloud and IT

- CloudGuard Posture Management
- CloudGuard CNAPP
- CloudGuard Network Security
- ✓ Microsoft Defender for Cloud
- ✓ Microsoft 365



Call to Action: 歡迎申請數位資產安全韌性與健檢評估



Quantum



CloudGuard

全面網路資安可視性評估

內網流量與應用程式分析

網路APT解析與報表

Web服務與存取(WAF)



Harmony

雲端郵件與端點安全檢視

O365/SaaS郵件安全檢查(惡意程式與釣魚)

端點EDR分析與威脅獵捕



CloudGuard

雲端數位資產態勢風險感知

Cloud Posture安全管理

雲端安全事件與情資分析

風險感知與異常偵測



Infinity

XDR/XPR 資安監控與回應

全面性零時差盲點監控

情資整合與回應流程

AI智能威脅分析





Thank You!

Danny Yang Cyber Security Evangelist, OCTO

danny@checkpoint.com

YOU DESERVE THE BEST SECURITY