Check Point
SOFTWARE TECHNOLOGIES LTD

構築安全未來 防護無限延展

Check Point Infinity Total Protection

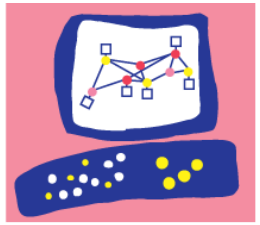
楊敦凱 Danny Yang I 技術顧問

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

CLOUD • MOBILE • THREAT PREVENTION

Agenda

- 資安趨勢與新世代管理架構
- 多面向實踐先進威脅防護
- 產品優勢分析及公司簡介



Check Point®
SOFTWARE TECHNOLOGIES LTD.

- 資訊安全趨勢與新世代管理架構

2018 世界經濟論壇:全球風險報告

WORLD ECONOMIC FORUM

Check Point SOFTWARE TECHNOLOGIES LTD

Top 5 Global Risks in Terms of Likelihood

	2016	2017	2018
1st	Large-scale involuntary migration	Extreme weather events	Extreme weather events
2nd	Extreme weather events	Large-scale involuntary migration	Natural disasters
3rd	Failure of climate-change mitigation and adaptation	Major natural disasters	Cyberattacks
4th	Interstate conflict with regional consequences	Large-scale terrorist attacks	Data fraud or theft
5th	Major natural catastrophes	Massive incident of data fraud/theft	Failure of climate-change mitigation and adaptation

回顧2017...層出不窮的惡意威脅與未知攻擊

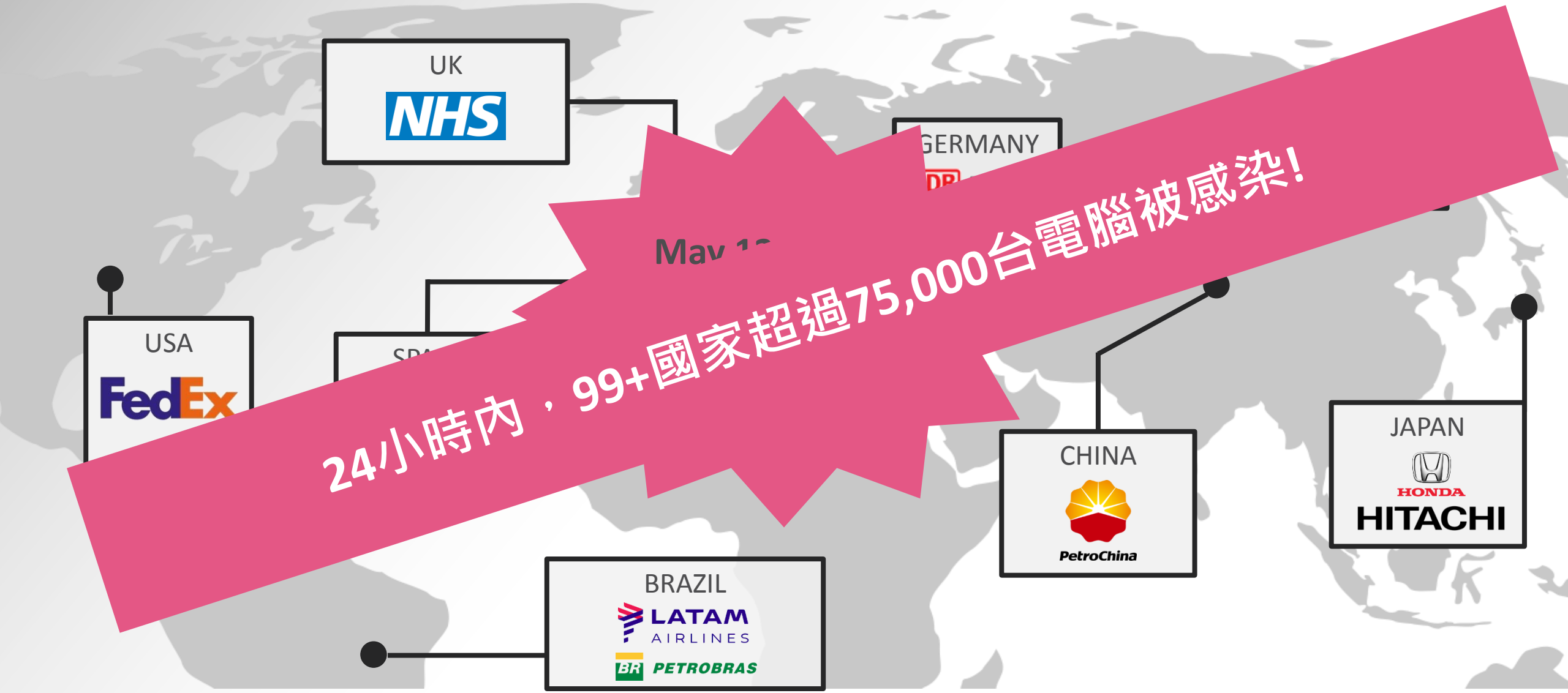
Check Point
SOFTWARE TECHNOLOGIES LTD

未知惡意攻擊

WANNACRY 勒索軟體
嚴重影響
全球逾百公司組織

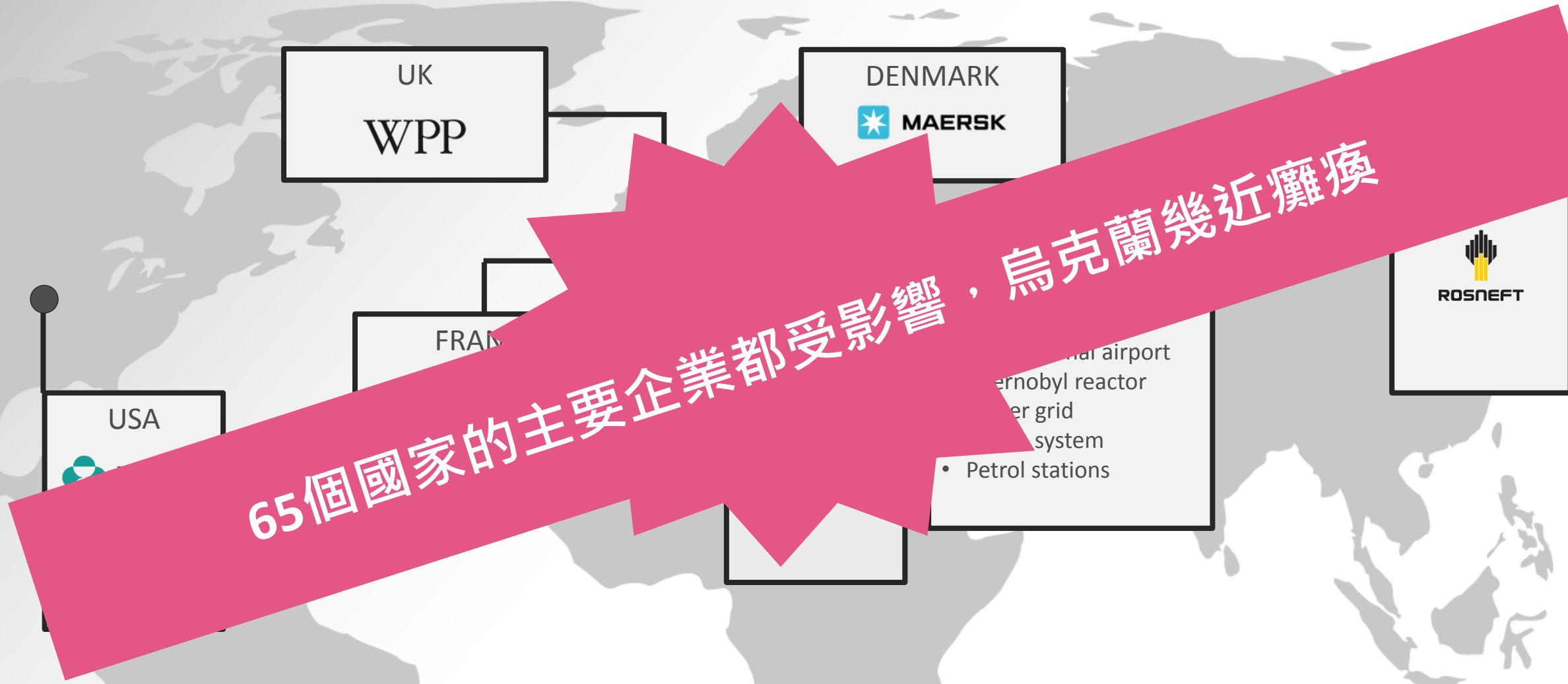
勒索軟體綁架
知名飯店電子門鎖系統
並將旅客反鎖在房間

MAY 2017: WANNACRY 全球大規模攻擊



一個半月後: NOTPETYA 再度影響全世界

Check Point
SOFTWARE TECHNOLOGIES LTD

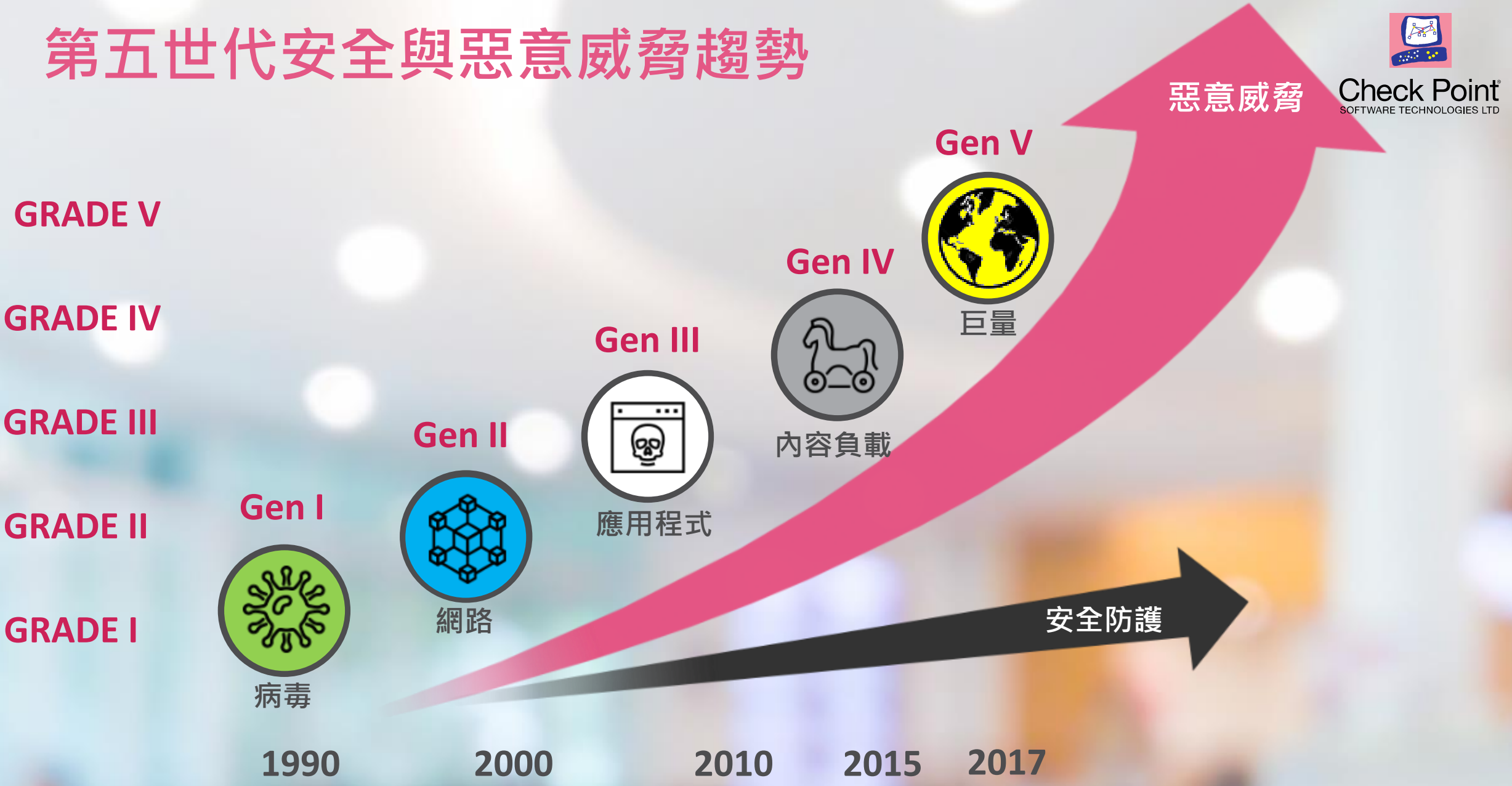


現今安全挑戰: 防堵多重突破口滲透與感染擴散

可預期的安全面向: 雲、行動、威脅防護

惡意針對性的威脅持續增長. **所有人皆是目標**

第五世代安全與惡意威脅趨勢



不同世代威脅與安全防護對照

第五代安全威脅: 巨量攻擊(Mega Attack)

多重破口

(網路, 端點, 行動)

超巨規模

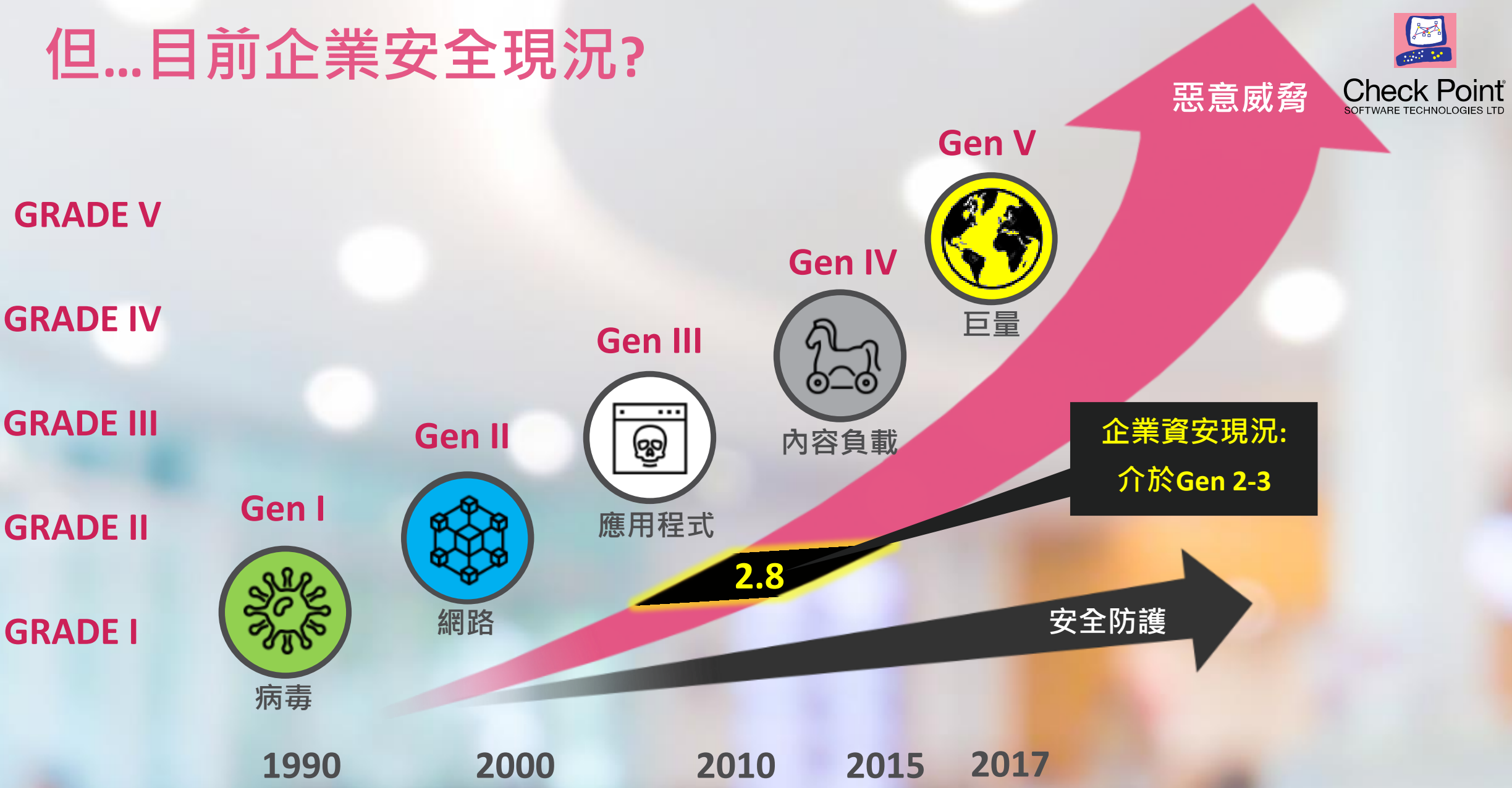
快速擴散

國家級別

橫跨產業

龐大損害

但...目前企業安全現況?

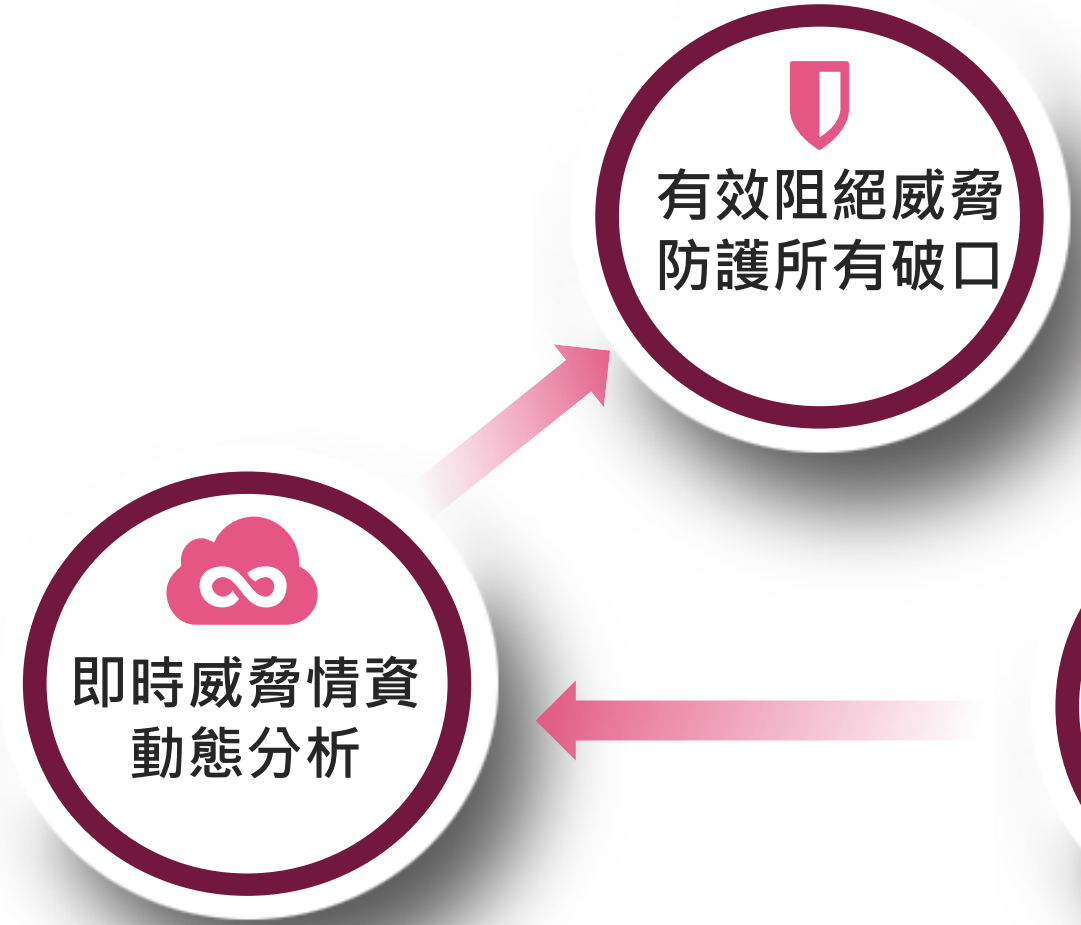

惡意威脅
Check Point
SOFTWARE TECHNOLOGIES LTD
GRADE V
GRADE IV
GRADE III
GRADE II
GRADE I
Gen I
病毒
Gen II
網路
Gen III
應用程式
Gen IV
內容負載
Gen V
巨量
企業資安現況:
介於Gen 2-3
2.8
安全防護
1990
2000
2010
2015
2017

即使已導入GEN IV 安全保護...可能還不夠!

Check Point
SOFTWARE TECHNOLOGIES LTD

如何有效導入第五代安全架構?

Check Point
SOFTWARE TECHNOLOGIES LTD



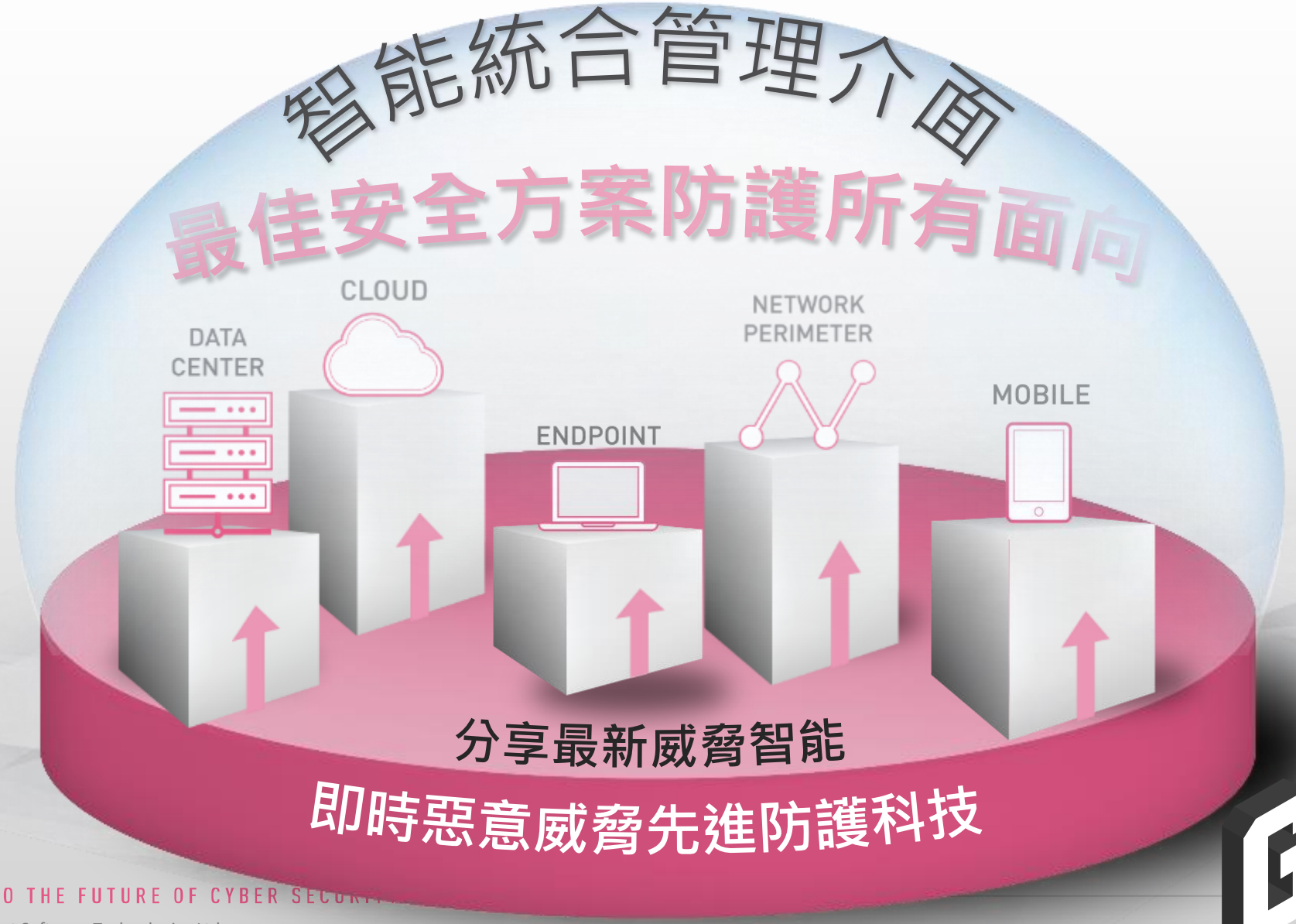
全面防堵威脅於事前/事中/事後
防護可涵蓋所有IT環境

立即隔離且清除威脅
一鍵管理安全政策

AI與大數據
全球情資共享

快速建構第五代安全模型

Check Point
SOFTWARE TECHNOLOGIES LTD



GEN V

Infinity Total Protection 第五代安全架構

Check Point
SOFTWARE TECHNOLOGIES LTD

雲端服務

CHECK POINT CloudGuard

混合雲

邊際網路與資料中心

Check Point SandBlast NETWORK

分享即時威脅情資與智能

THREATCLOUD

CHECK POINT INFINITY

R80

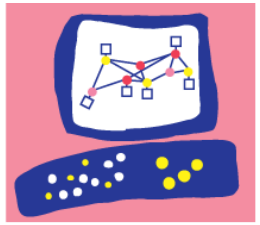
整合安全管理

行動裝置

Check Point SandBlast MOBILE

端點設備

Check Point SandBlast AGENT



Check Point®
SOFTWARE TECHNOLOGIES LTD.

- 多面向實踐先進威脅防護

專為第五代安全打造的安全閘道防護架構

新世代威脅防護科技(NGTP/NGTX)

威脅模擬
(沙箱檢測)

威脅萃取
(無害化)

IPS

防毒牆

殭屍病毒防護

電子郵件安全

新世代防火牆與進階安全技術

防火牆

應用層控制

網頁過濾

DLP

VPN

使用者識別

安全與威脅事件管理

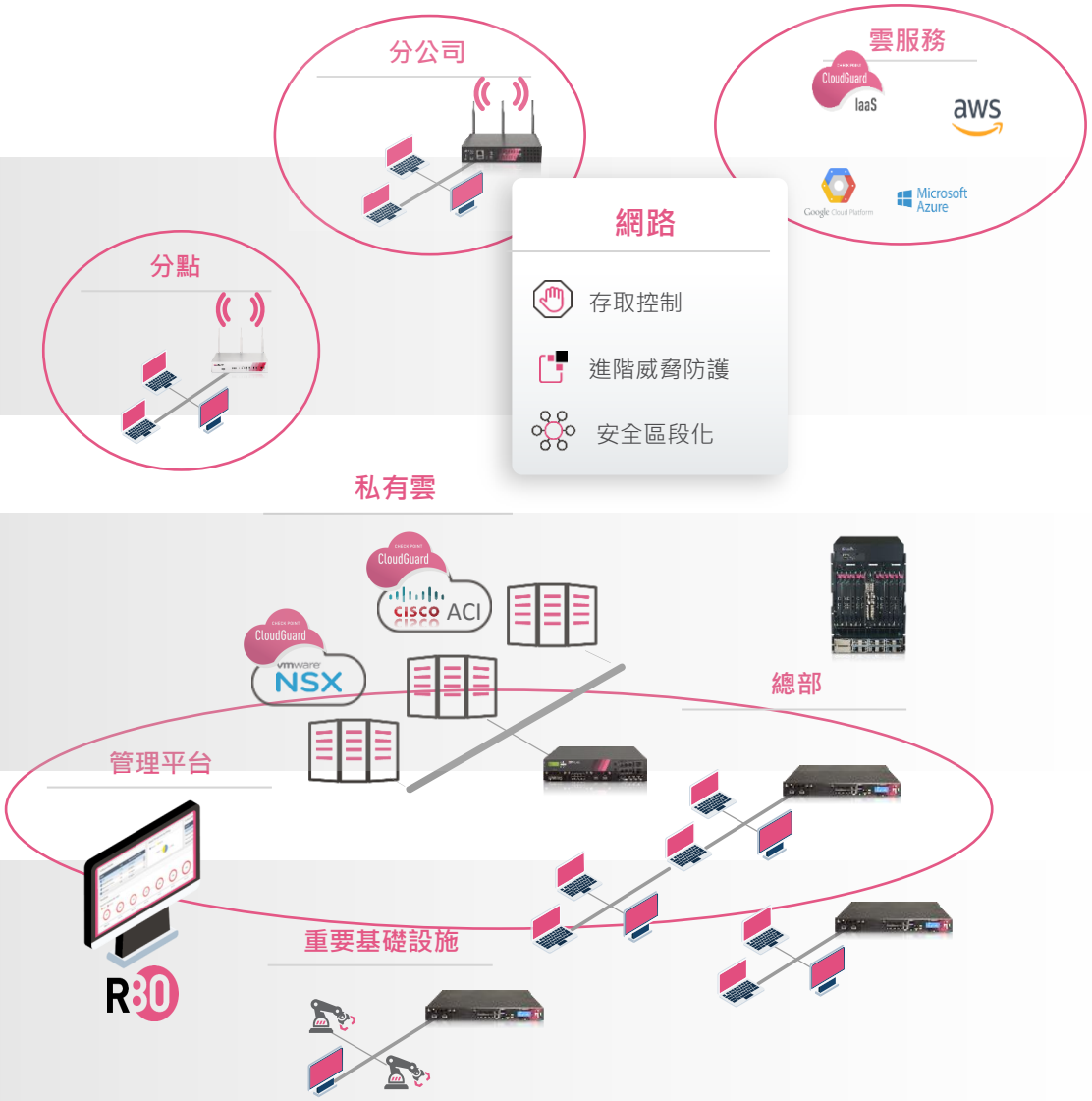
智能控管

鑑識分析

威脅可視性

報表

合規檢查



整合全球最先進防護技術
阻擋所有來自不同突破口的進階威脅

Check Point SandBlast™ ZERO-DAY PROTECTION

產品家族

NETWORK

邊界網路安全
與資料中心

GATEWAYS, CLOUD

AGENT

端點與瀏覽器
安全防護

SANDBLAST AGENT

MOBILE

行動裝置
進階威脅保護

SANDBLAST MOBILE

<API>

客製化
應用程式介接

SANDBLAST API

SANDBLAST
威脅模擬

28種綜合檢測引擎

檢測並阻擋未知惡意軟體
和零時差攻擊

SANDBLAST
威脅萃取

主動提供安全重組文件
避免檔案傳遞延遲

SandBlast 威脅模擬

業界唯一反規避沙箱技術

與數十種先進科技與機器學習

CPU-LEVEL

Human Interaction Simulator

Network Activity Monitor

FP Guard

DeepScan

UAC Monitor

SMEP Detector

Virtual Network Service

PUSH-FORWARD

Icon Similarity

Image Sanitation

Dropped File Emulation

Decoys

DGA Generator

Static Analyzer

Evasion Detection

Macro Analysis

Link Scanner

Shellcode Detector

讓惡意程式無所遁形

平均兩分鐘內完成模擬

SandBlast 威脅萃取

主動消除潛在威脅

CLEAN MODE

維持原檔案格式
移除可疑有害內容
Macros, script, embedded objects, meta data, …

CONVERT MODE

轉為**純文字**檔案
避免惡意內容
防止漏洞

支援文件檔案與圖片格式
確保所有文件檔案安全與可視性

檔案無害處理

最高安全信心等級

快速交付

最高等級安全檢查
APT防護無痛導入流程

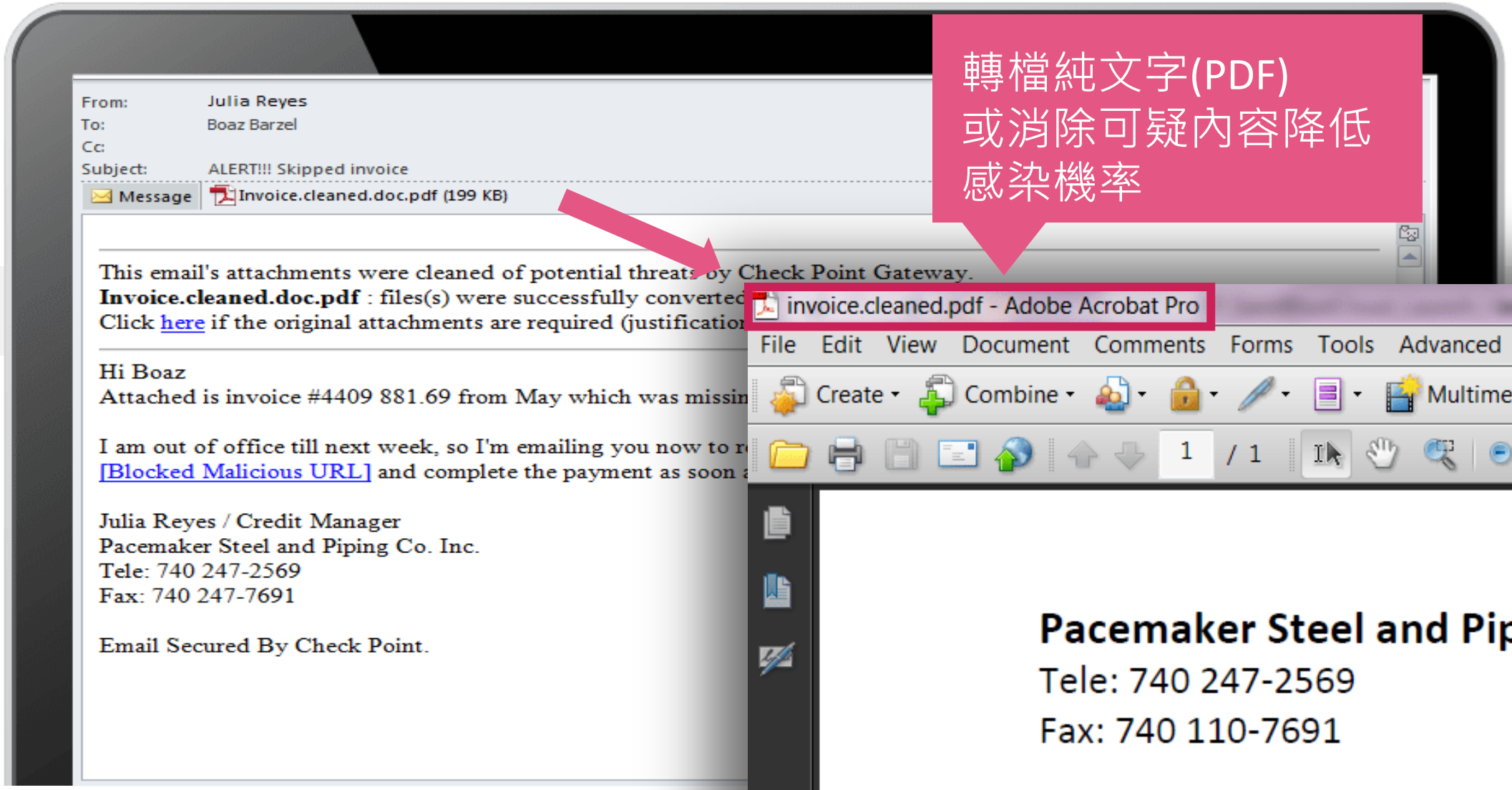
- 檔案無延遲且安全無虞
- 確保生產力兼具安全性
- 主動防護阻絕惡意威脅
- 自助式IT取回正常檔案 **(檢測良性)**

Check Point
SandBlast™
ZERO-DAY PROTECTION

威脅萃取 DEMO

即時保護不受郵件惡意附件感染

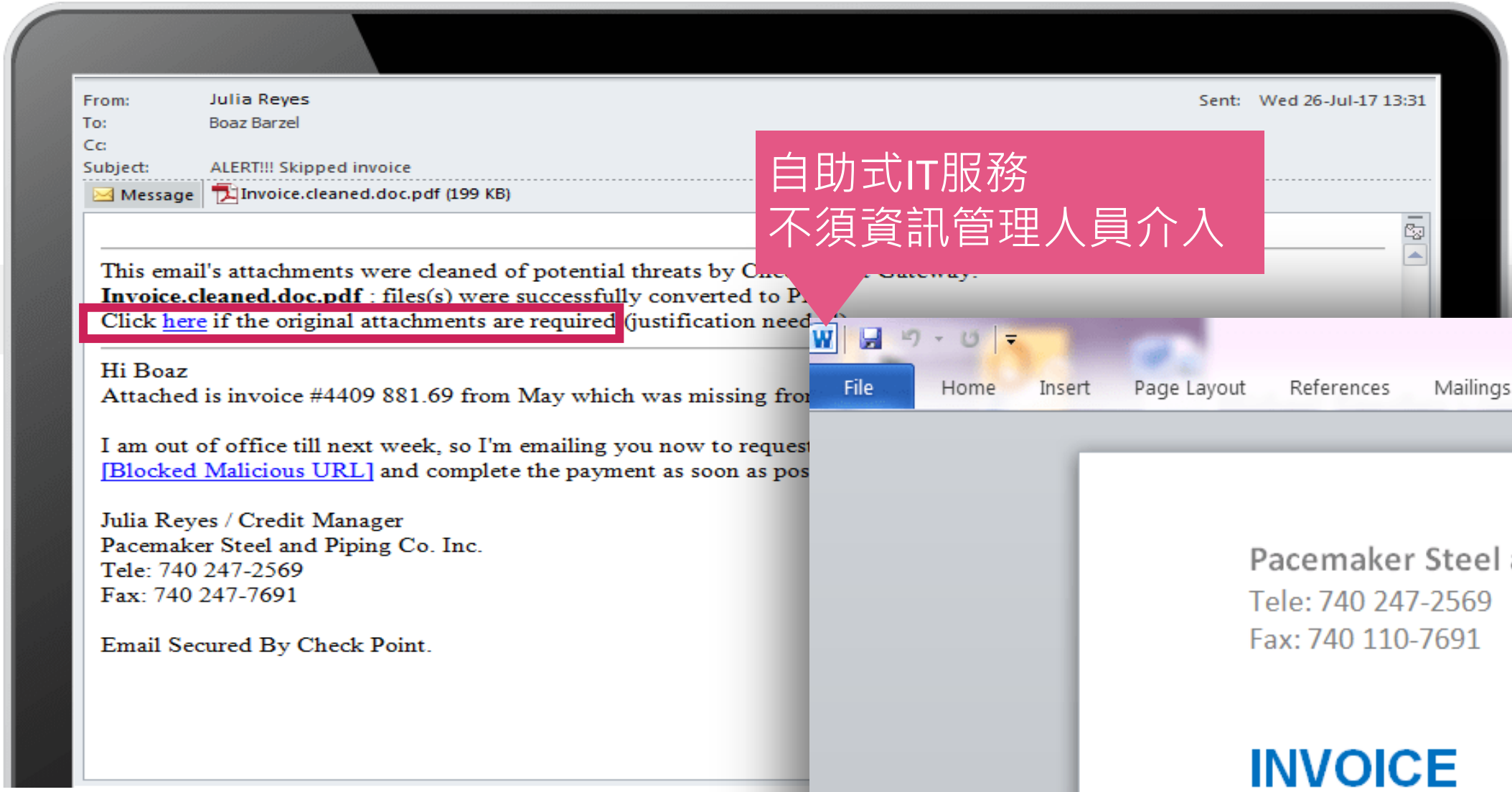
快速提供安全無害檔案



威脅萃取 DEMO

使用者自行取回原始檔案

當威脅模擬確認檔案為良性始可放行



成功防護惡意攻擊三大要素

1

立即阻擋防護

最佳檢測引擎
即時防護措施

2

隔離有害內容

強化內容隔離
降低感染風險

3

端點鑑識分析

事件快速反應
確保政策有效

Check Point
SandBlast™
AGENT

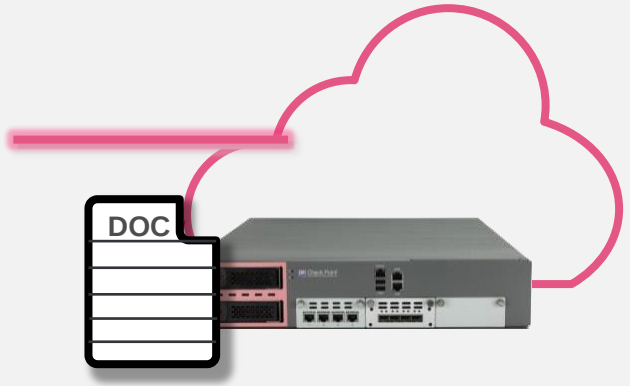
全面防堵所有突破口

保護端點與行動使用者

- 零時差防護
- 防釣魚攻擊
- 隔離可疑內容
- 自動鑑識分析
- 勒索軟體防護

零時差威脅防護(WEB)

在端點裝置消除零時差惡意威脅



SANDBLAST SERVICE
雲端沙箱或自建沙箱

1 網路下載未知檔案
送至沙箱分析

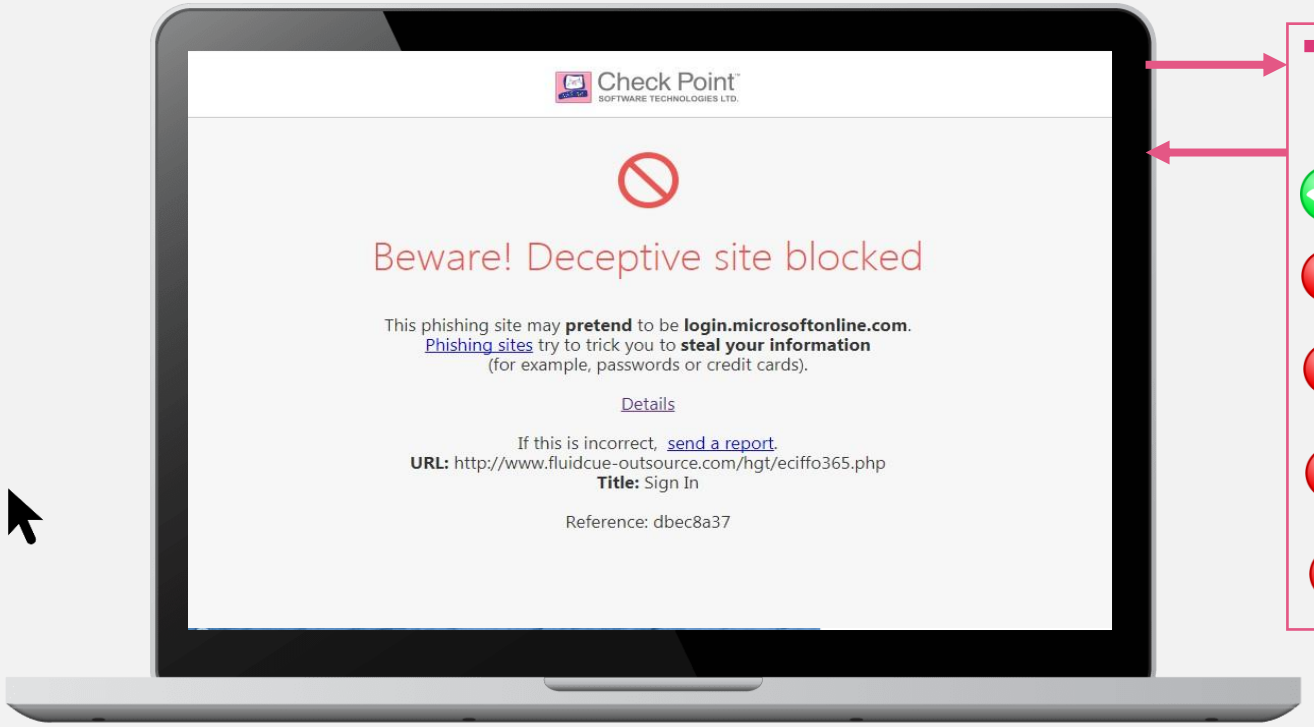
2 即時交付安全
轉檔版本(無害化)

3 原始檔案於背景
持續模擬檢測

防釣魚攻擊

阻止使用者存取惡意釣魚站台

即便此網頁未曾出現過!



THREATCLOUD

- IP Reputation
- Domain Reputation
- URL Similarity
- Lookalike Characters
- Title Similarity
- Image Only Site
- Visual Similarity
- Multiple Top-Level Domain
- Text Similarity
- Lookalike Favicon

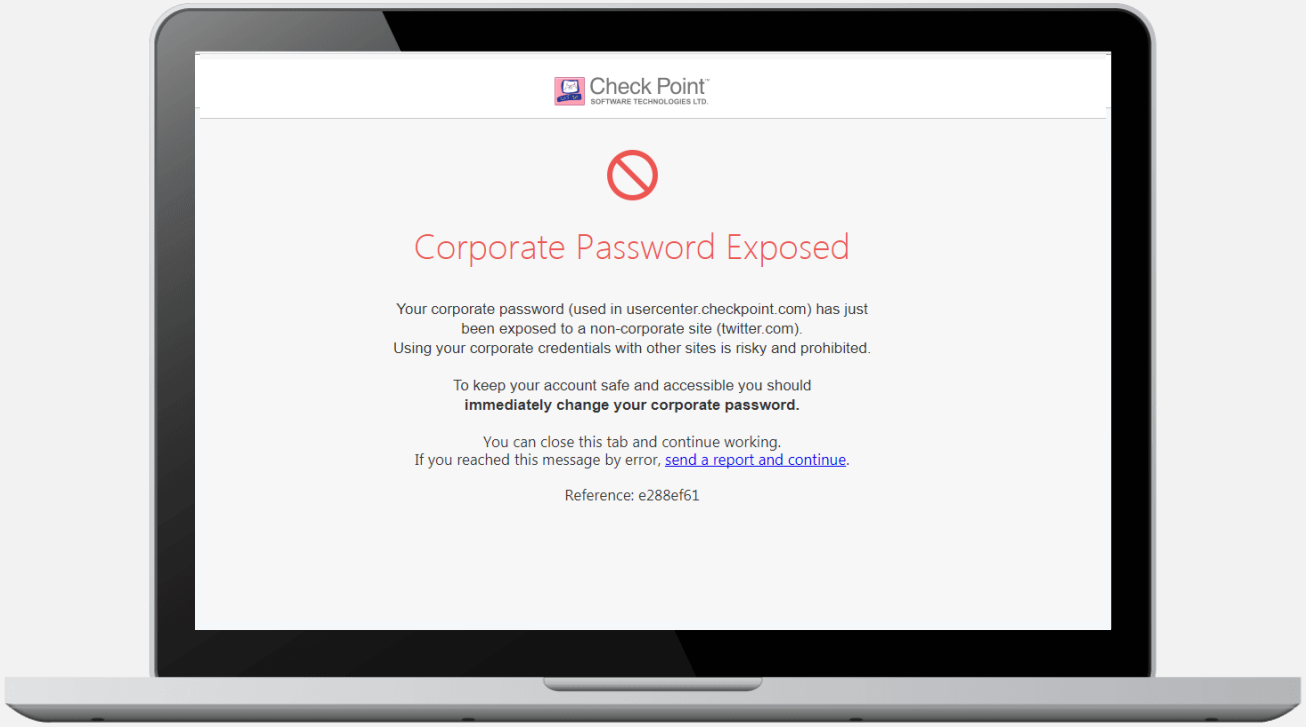
1 檢視使用者
存取未知網頁

2 先進演算法
評估風險指標

3 數秒內判定
檢測結果

防釣魚攻擊

防止公司內部帳號密碼重複使用



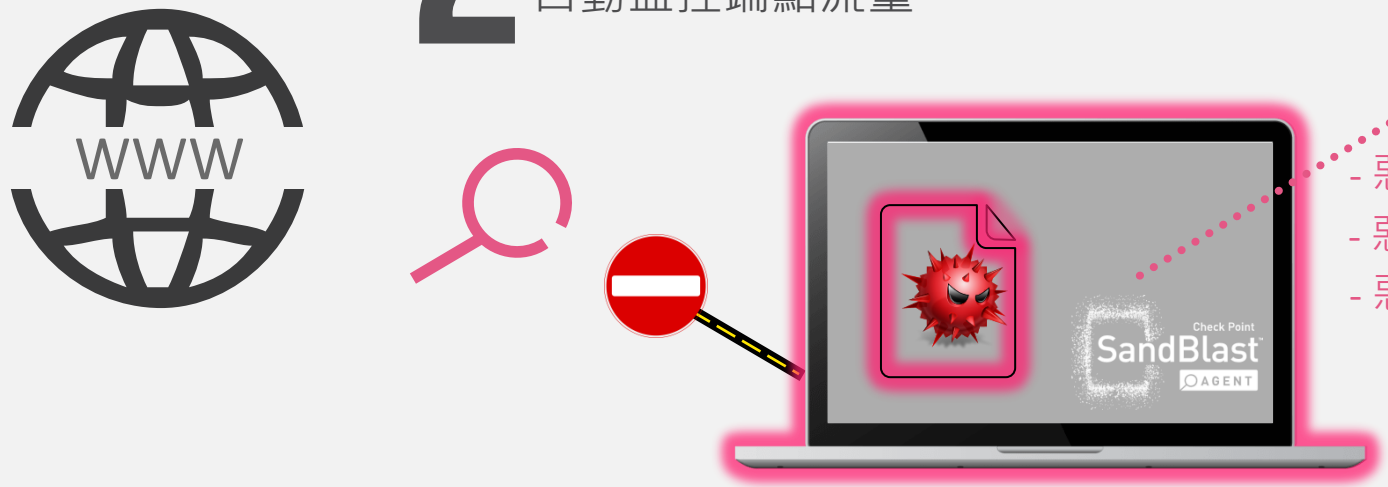
透過防止於外部網站使用企業內部密碼來保障安全性

端點殭屍病毒防護

於端點不間斷監控對外可疑流量(與C&C連線)

2 **ANTI-BOT**功能
自動監控端點流量

1 透由**THREATINTELLIGENCE**
更新最新威脅情資



THREATCLOUD
- 惡意 URLs
- 惡意 IP位址
- 惡意網路模版(Patterns)

3 **阻斷**惡意中繼站
流量與資料洩漏

4 **隔離**惡意執行程序
或鎖定系統

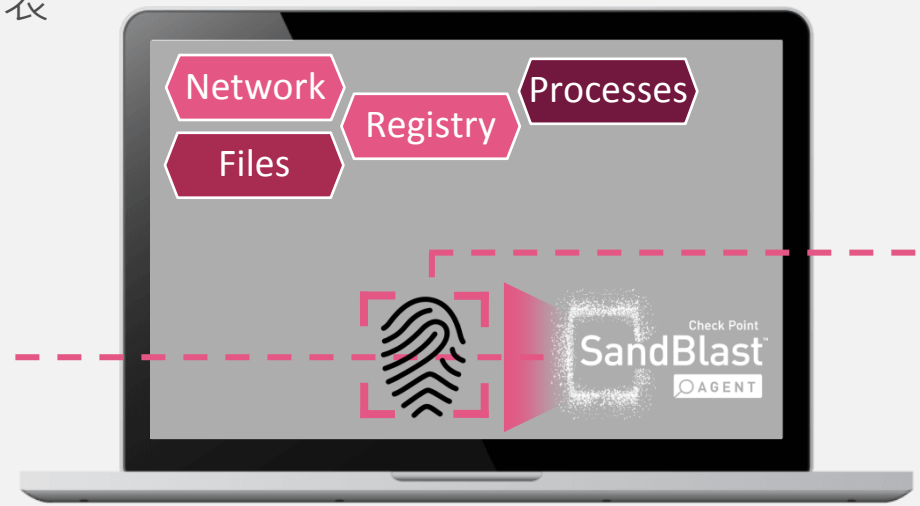
端點鑑識分析

蒐集端點鑑識資訊於事件觸發後自動產出報表

1 自作業系統與端點感知器
蒐集端點鑑識資訊

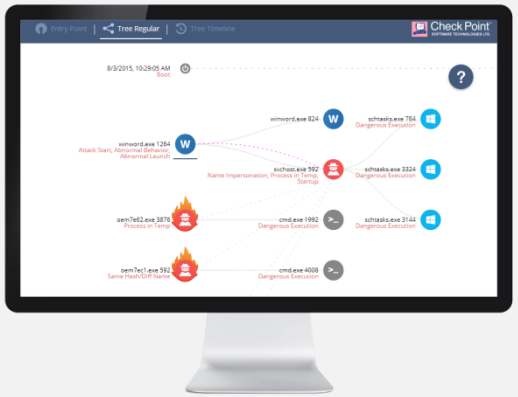
2 事件監測後自動觸發報表
或整合第三方防毒軟體

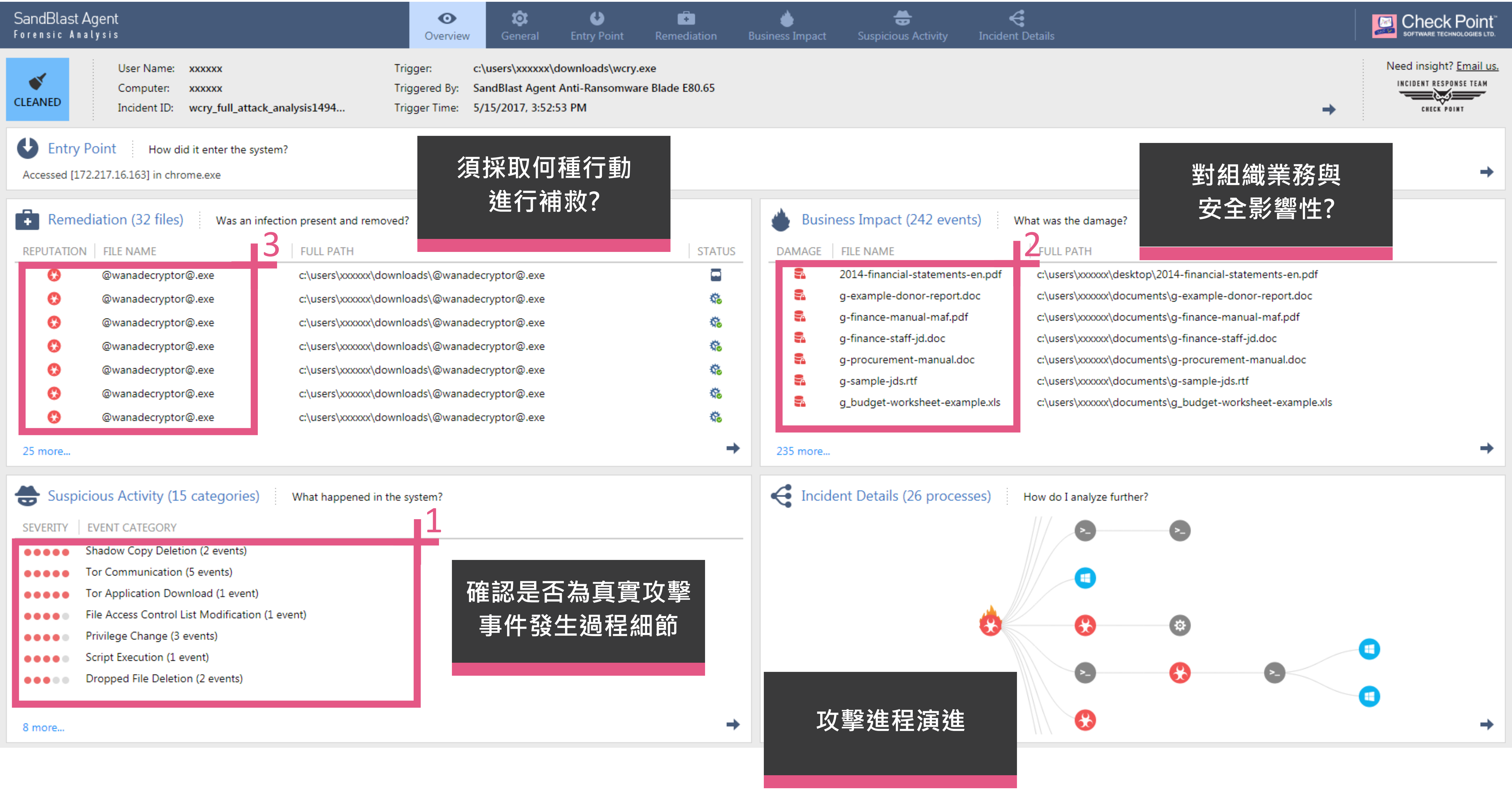
監控偵測



3 進階演算法分析鑑識
資訊評估安全風險

4 將事件整合回報予
SmartEvent主機




SandBlast Agent
Forensic Analysis
Overview
General
Entry Point
Remediation
Business Impact
Suspicious Activity
Incident Details
Check Point
SOFTWARE TECHNOLOGIES LTD.
CLEANED
User Name: xxxxxx
Computer: xxxxxx
Incident ID: wcry_full_attack_analysis1494...
Trigger: c:\users\xxxxxx\downloads\wcry.exe
Triggered By: SandBlast Agent Anti-Ransomware Blade E80.65
Trigger Time: 5/15/2017, 3:52:53 PM
Need insight? Email us.
INCIDENT RESPONSE TEAM
CHECK POINT
Entry Point
How did it enter the system?
Accessed [172.217.16.163] in chrome.exe
須採取何種行動
進行補救?
對組織業務與
安全影響性?
Remediation (32 files)
Was an infection present and removed?
3
REPUTATION
FILE NAME
FULL PATH
STATUS
@wanadecryptor@.exe
c:\users\xxxxxx\downloads\@wanadecryptor@.exe
@wanadecryptor@.exe
c:\users\xxxxxx\downloads\@wanadecryptor@.exe
@wanadecryptor@.exe
c:\users\xxxxxx\downloads\@wanadecryptor@.exe
@wanadecryptor@.exe
c:\users\xxxxxx\downloads\@wanadecryptor@.exe
@wanadecryptor@.exe
c:\users\xxxxxx\downloads\@wanadecryptor@.exe
@wanadecryptor@.exe
c:\users\xxxxxx\downloads\@wanadecryptor@.exe
@wanadecryptor@.exe
c:\users\xxxxxx\downloads\@wanadecryptor@.exe
25 more...
Business Impact (242 events)
What was the damage?
2
DAMAGE
FILE NAME
FULL PATH
2014-financial-statements-en.pdf
c:\users\xxxxxx\desktop\2014-financial-statements-en.pdf
g-example-donor-report.doc
c:\users\xxxxxx\documents\g-example-donor-report.doc
g-finance-manual-maf.pdf
c:\users\xxxxxx\documents\g-finance-manual-maf.pdf
g-finance-staff-jd.doc
c:\users\xxxxxx\documents\g-finance-staff-jd.doc
g-procurement-manual.doc
c:\users\xxxxxx\documents\g-procurement-manual.doc
g-sample-jds.rtf
c:\users\xxxxxx\documents\g-sample-jds.rtf
g_budget-worksheet-example.xls
c:\users\xxxxxx\documents\g_budget-worksheet-example.xls
235 more...
Suspicious Activity (15 categories)
What happened in the system?
1
SEVERITY
EVENT CATEGORY
Shadow Copy Deletion (2 events)
Tor Communication (5 events)
Tor Application Download (1 event)
File Access Control List Modification (1 event)
Privilege Change (3 events)
Script Execution (1 event)
Dropped File Deletion (2 events)
8 more...
確認是否為真實攻擊
事件發生過程細節
Incident Details (26 processes)
How do I analyze further?
攻擊進程演進

AGENT

勒索軟體
防護

啟發式行為監測引擎

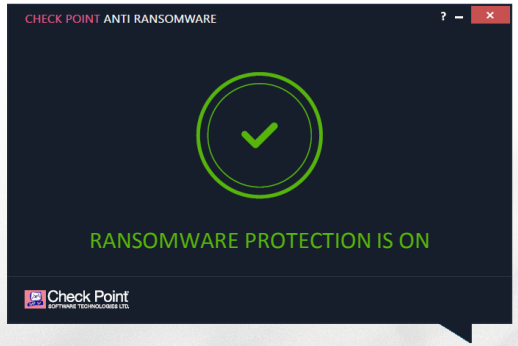
偵測勒索軟體與加密攻擊

防堵惡意勒索加密軟體及隔離
自動化快照與還原檔案

ANTI-RANSOMWARE

勒索軟體防護(ANTI-RANSOMWARE)運作原理

進行中



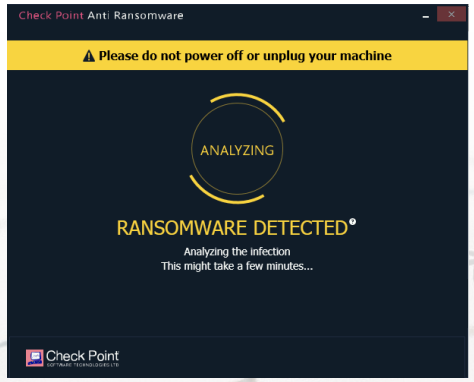
行為檢測

背景持續監控可疑勒索軟體行為與加密程序

資料快照

立即產生檔案備份
(被影響的資料)

感染後與反應

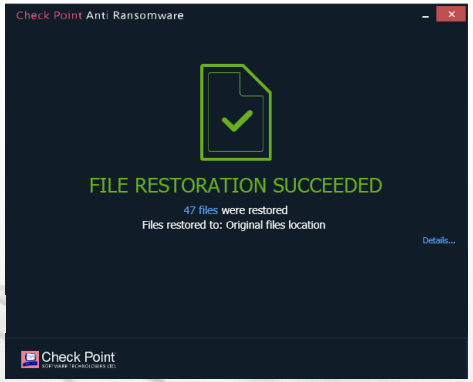


分析

啟動鑑識分析
確認攻擊細節

隔離

阻止加密軟體程序並隔離



還原

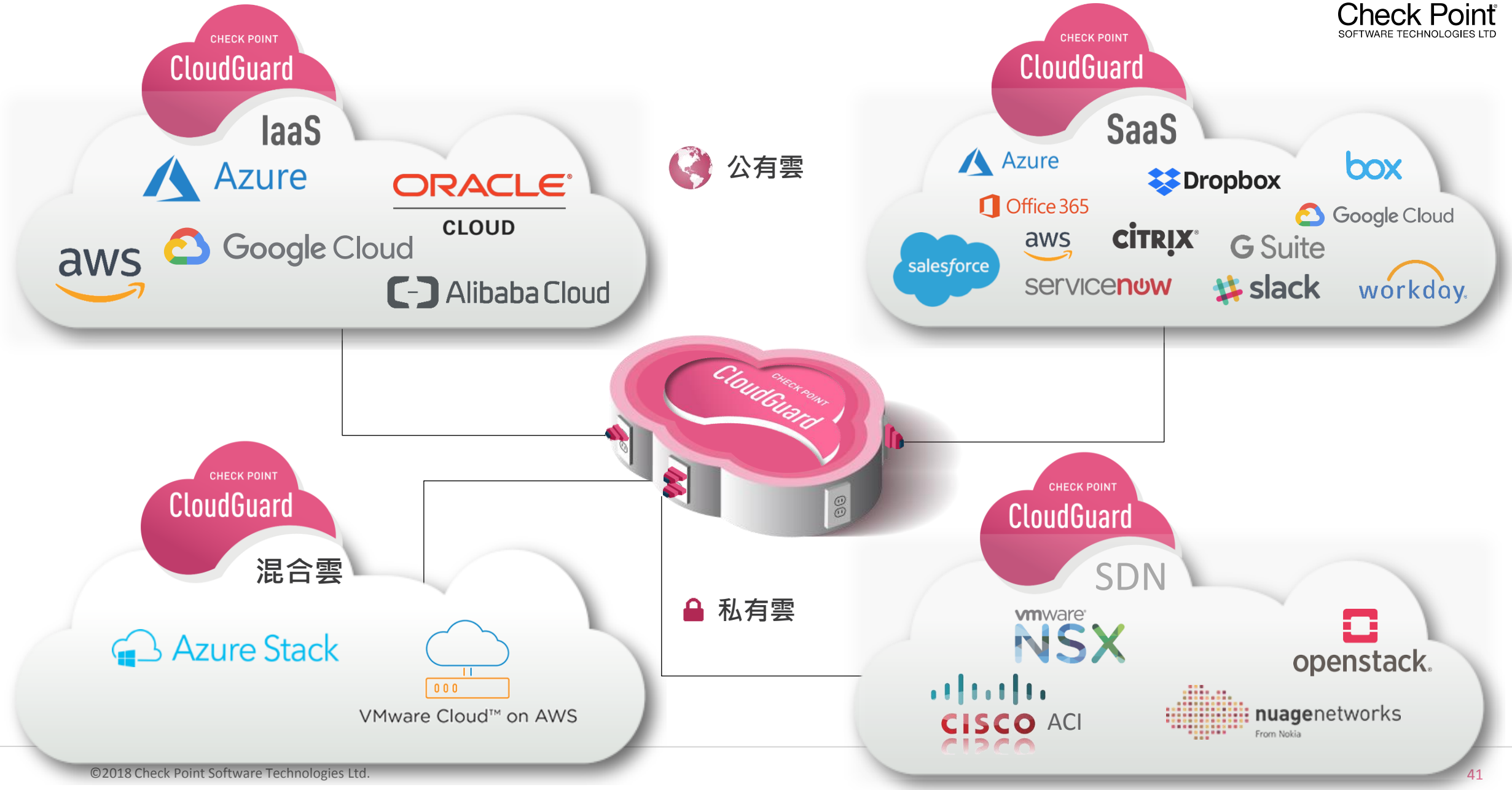
自動於快照檔案中還原原始檔

雲與行動裝置安全

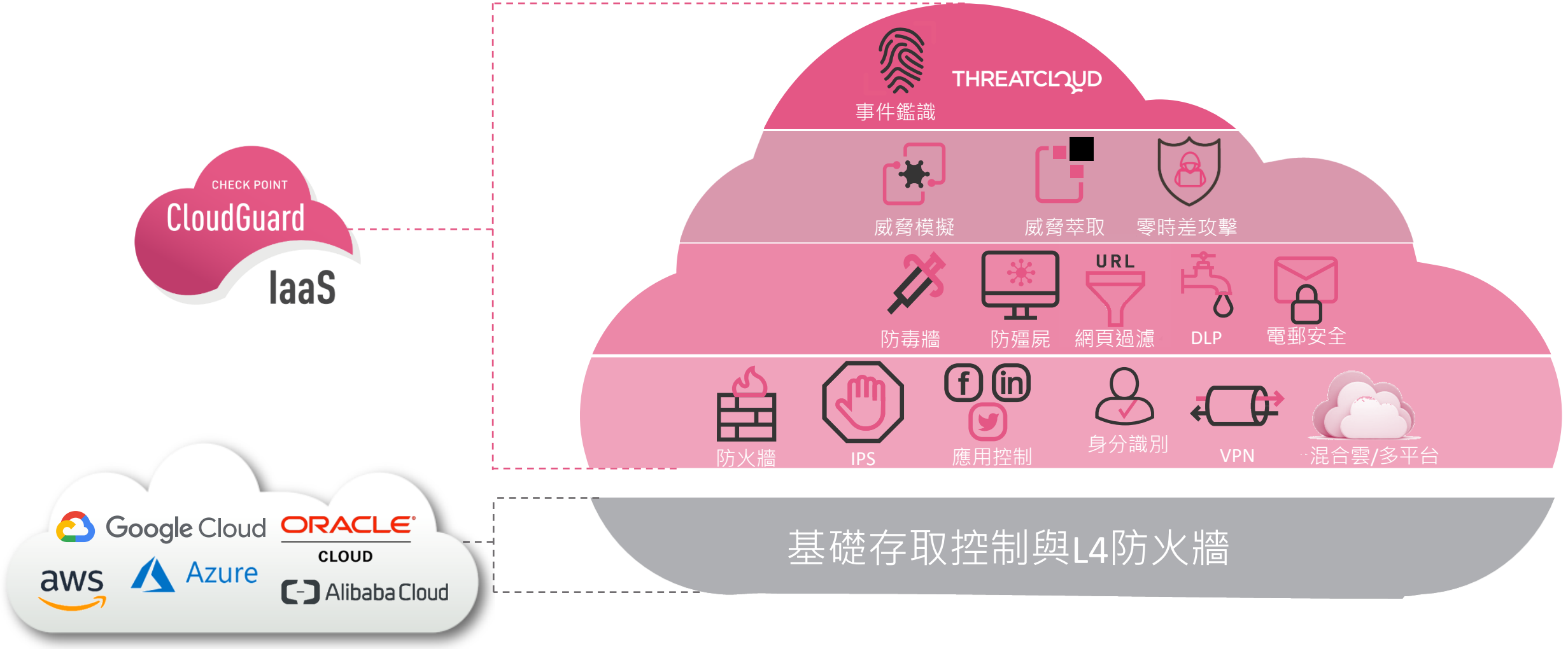
CHECK POINT CLOUDGUARD

防護所有混合雲平台，部署與地端一致性安全標準

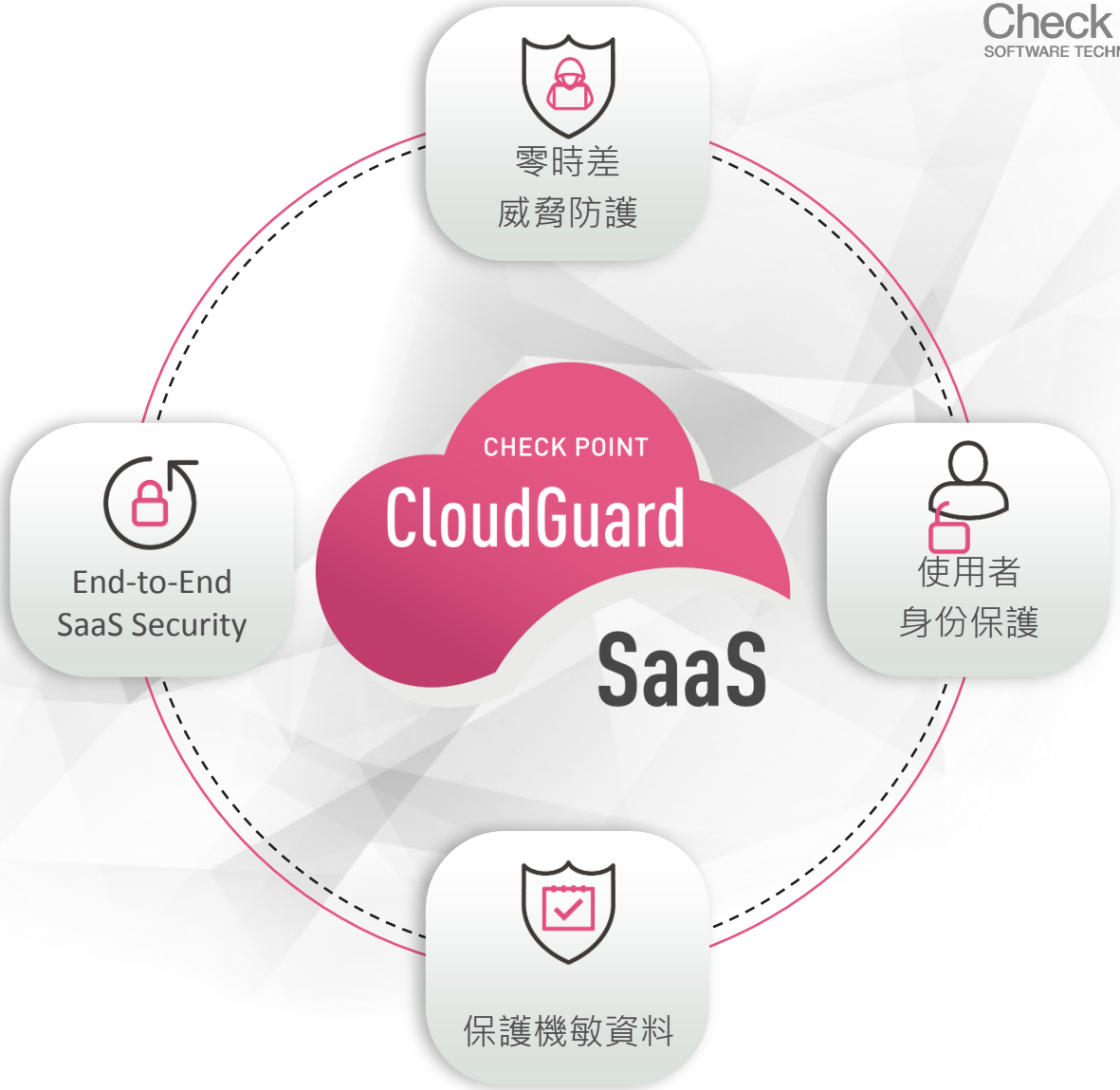
CloudGuard 產品家族



CloudGuard IaaS 雲平台進階防護方案



CLOUDGUARD SAAS
雲端服務安全方案



CloudGuard SAAS

Check Point
SOFTWARE TECHNOLOGIES LTD

SECURITY STACK

- 防止帳號盜用
- 零時差威脅防護 (SandBlast ZERO-DAY PROTECTION)
- 資料外洩防護
- 文件加密
- 減輕管理盲點

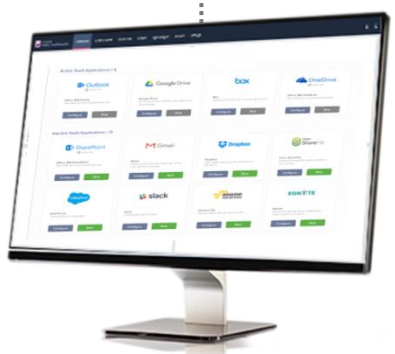
SAAS 供應商

- Office 365
- box
- Suite
- ...

API & AD

CloudGuard SaaS

GenV 安全閘道



行動威脅防護(MTD)

Android 防毒 | 網路中間人攻擊(MiTM,...)

作業系統漏洞 | 應用程式風險分析模擬

SANDBLAST MOBILE

行動資料保護

Secure Container | SSL VPN

雙重身分 | 內部資源整合

CAPSULE WORKSPACE

遠端存取

單一應用程式VPN存取 | VDI / VMI

全機VPN存取 | (安全存取郵件

CAPSULE VPN

內容管理(MCM)

檔案權限管控

檔案生命週期

CAPSULE DOCS

應用管理(MAM)

企業應用程式/商店 | 應用程式黑名單

應用程式白名單 | 應用程式管理

CAPSULE WORKSPACE

裝置管理(MDM)

設備整合管控 | 地理區域追蹤

裝置管理(設定檔) | 應用程式派送

MobileIron

MaaS360

airwatch

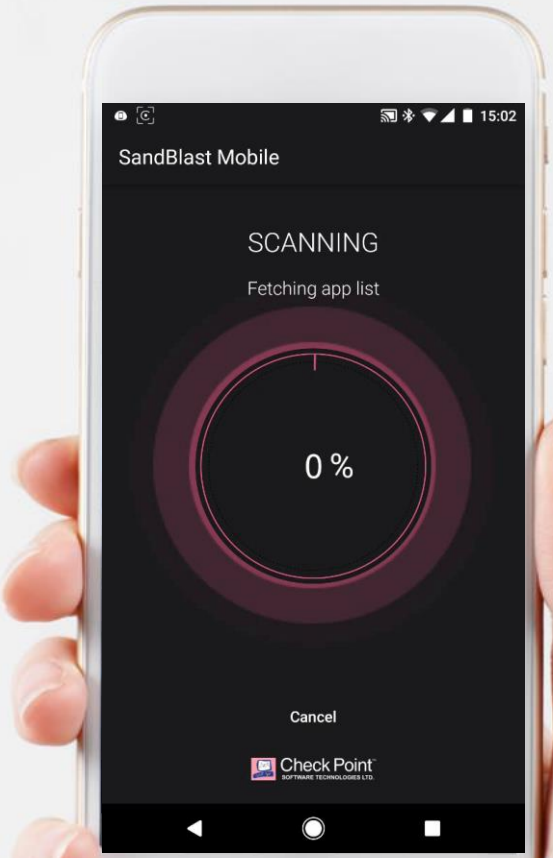
Citrix XenMobile

Microsoft Intune

BlackBerry UEM

- 已知與零時差威脅
- WIFI網路安全性
- 藍芽攻擊
- 作業系統漏洞
- 簡訊釣魚
- 改機越獄

SANDBLAST



SBM運作原理

裝置風險分析
BRE
雲端行為風險分析引擎

裝置偵測

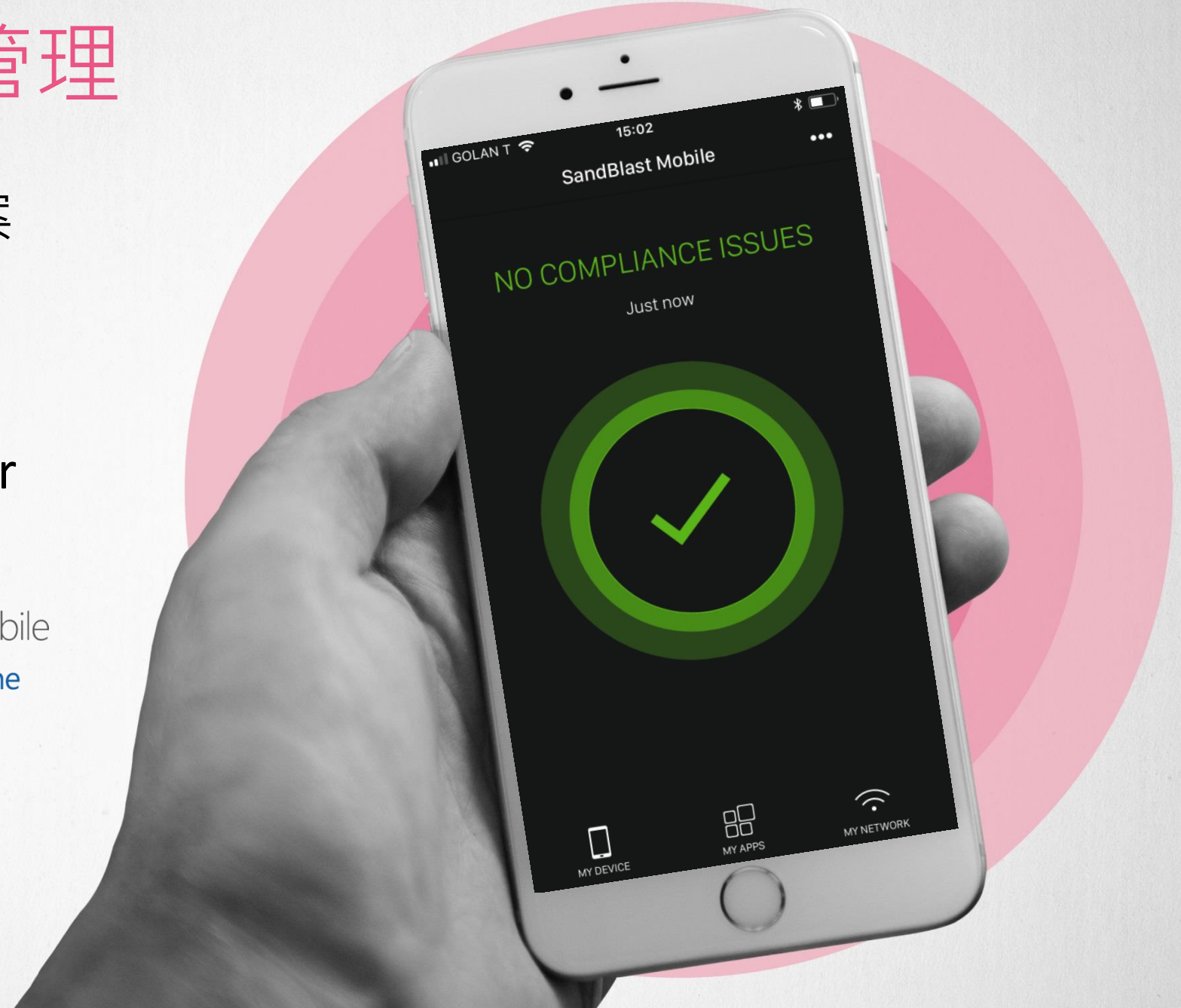
即時威脅情資監控

最簡易的部署管理

雲端式 SaaS 解決方案

能夠整合到主流的
EMM 平台和Container

MobileIron airwatch MaaS360 CITRIX XenMobile
Good BES12 Microsoft Intune



全新版本與產品線

New!

未來的安全平台

統合網路、雲端和行動裝置

R80.10

次世代安全管理原則

有效率、自動化作業

整合式威脅管理

智能統合管控

一鍵部署
所有安全措施

R80.10

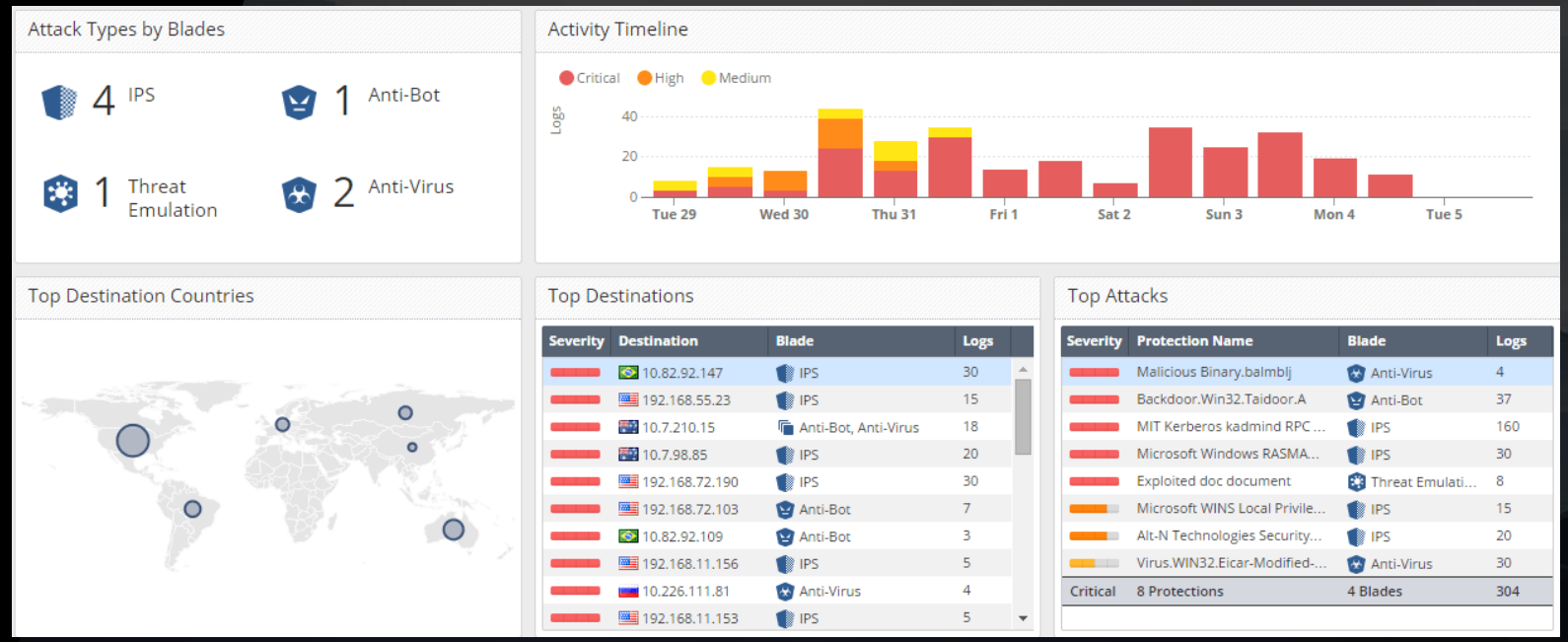
Name	Source	Destination	Services & Applications	Data	Action	Install On
Outbound access	production_net	Internet	Any	Any	AccessSubLayer	Policy Targets
Social media for marketing	marketing_role John	Internet	Twitter LinkedIn Instagram	Any	Accept	SG13800
Developers upload	developer_role	Internet	Dropbox Box	Any Direction Source Code - JAVA	Accept	SG13800 CapsuleCloud
Access Sensitive Servers	Any	Any	Any	Any	SensitiveServers	Policy Targets
Mobile Access	Mobile Devices	MailUS	MailServer	Any	Accept	Mobile
Access to Web Server	Any	WebServer	https	Any	Accept	AWS VMWare

使用者 裝置 應用程式 資料 安全閘道 私有雲 公有雲 虛擬閘道

POWERED BY: CHECK POINT INFINITY

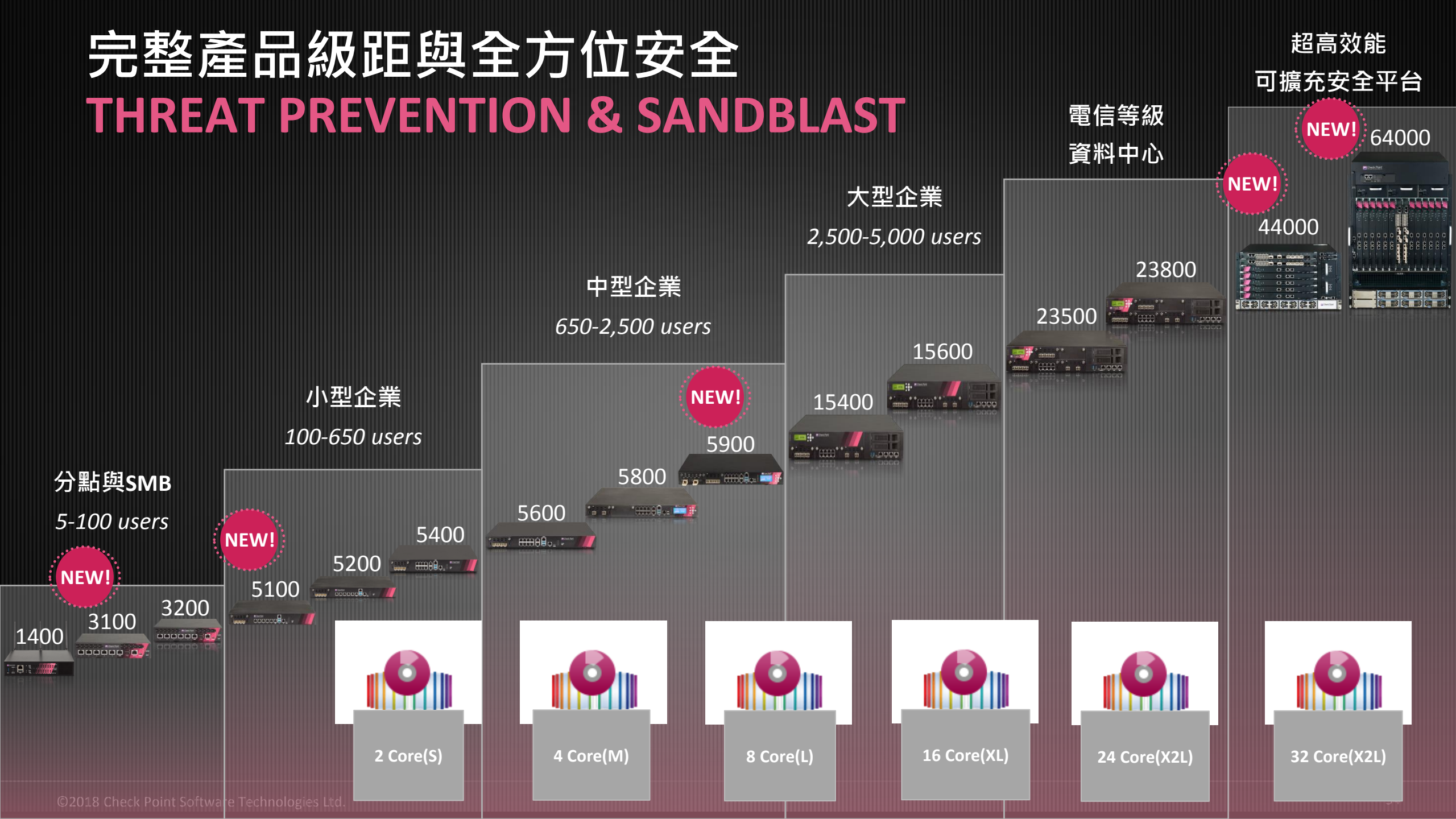
高度威脅分析可視性

R80.10



POWERED BY: CHECK POINT INFINITY

完整產品級距與全方位安全
THREAT PREVENTION & SANDBLAST



2018全新管理主機系列

Check Point
SOFTWARE TECHNOLOGIES LTD

ALL NEW SMART-1

中央控管，日誌儲存，事件管理

專為第五代安全設計的管理主機!

Check Point SMART-1

新世代管理硬體主機

優化第五代安全防護

UP TO 5 GATEWAYS

405

Up to 40,000 Logs/sec

2 cores, 16GB RAM, 1TB

UP TO 10 GATEWAYS

410

Up to 45,000 Logs/sec

2 cores, 32GB RAM, 2TB

NEW!

UP TO 25 GATEWAYS

525

Up to 60,000 Logs/sec

4 cores, 64GB RAM, 8TB

NEW!

UP TO 50 GATEWAYS

5050

Up to 80,000 Logs/sec

12 cores

128GB RAM

16TB

50 Domains

NEW!

OVER 50 GATEWAYS

5150

Up to 100,000 Logs/sec

24 cores

up to 256GB RAM

up to 48TB

200 Domains

SMB與SCADA(ICS)安全

最全面高效的威脅防護功能 2017 UTM MQ Leader

最彈性的部署與擴充能力

防火牆
身分識別
VPN

防毒
防殭屍
電子郵件安全

應用程式控制
網頁過濾

IPS
雲端沙箱
(Optional)

C/P值最高的SMB網路安全閘道

中央管理
智能介面

彈性大量部署

自動化監控
與日誌儲存

客製化報表

中央管理與日誌收容

Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT'S

關鍵基礎設施安全方案

Industrial Control Systems

CYBER DEFENSE

- SCADA流量安全可視性
- SCADA流量安全防護機制
- 可耐高溫嚴苛環境的設備

SCADA/ICS 特定通訊協定支援

超過 650 SCADA 指令
於Check Point Application Control

Check Point 1200R

專為SCADA環境設計的強固型安全閘道硬體

- **全方位安全功能(NGTP/NGTX)**
- **6x1GbE ports** 與高達2Gbps效能
- 符合相關法令規範
  IEC 61850-3 & IEEE 1613
- 無風扇/硬碟設計
- 工作溫度-40°C to 75°C
- 支援 In-line 或 Tap (Mirror) modes
- 支援多種網路路由(e.g: BGP, OSPF, IPsec, etc.)

OT安全藍圖

Check Point
SOFTWARE TECHNOLOGIES LTD

Management Facility

Main Control Center

SCADA Historian

SmartEvent

SCADA VPN

Control & monitor

Control

Monitor

PLC1

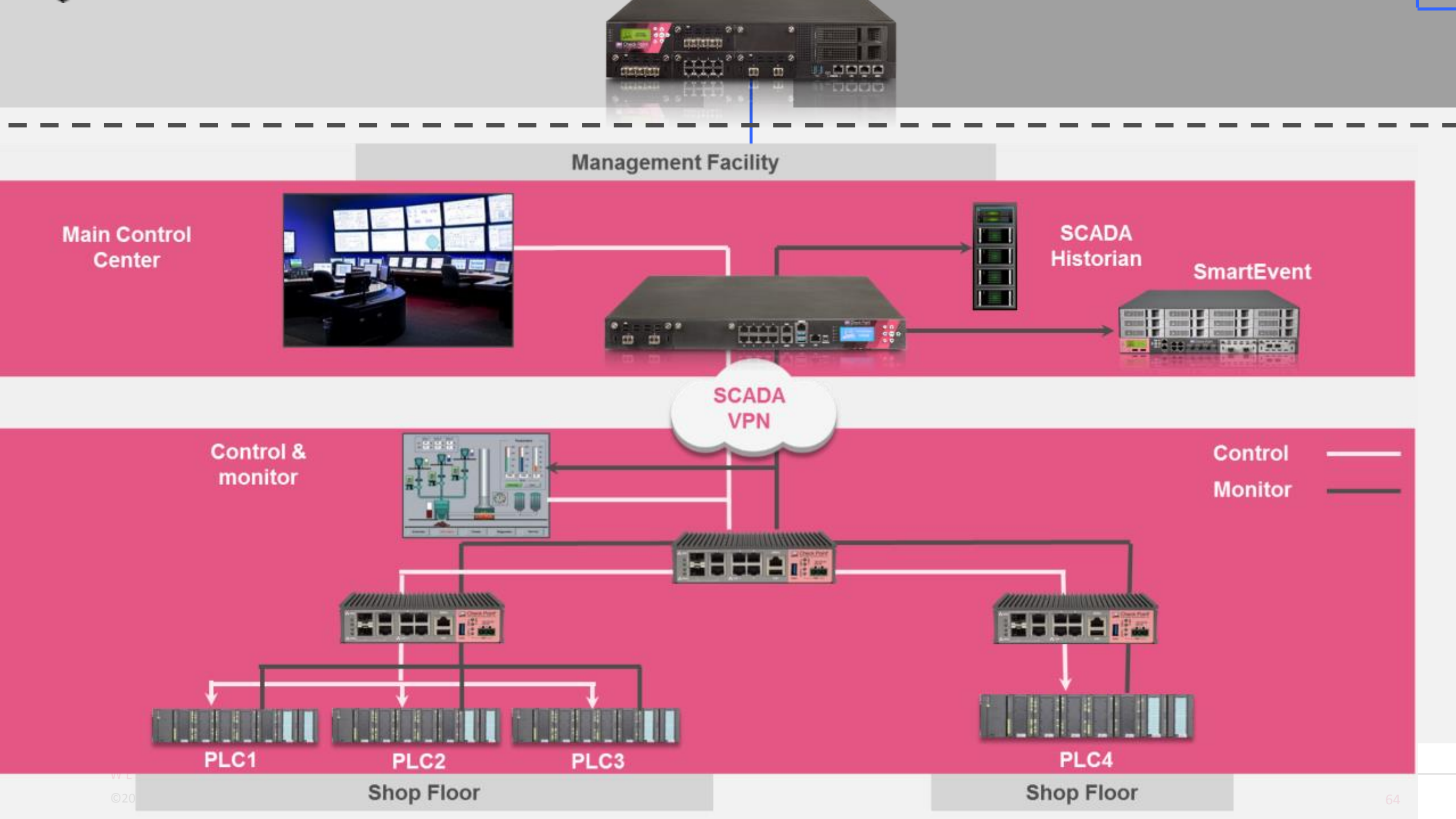
PLC2

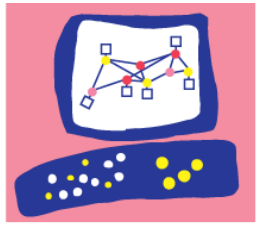
PLC3

PLC4

Shop Floor

Shop Floor

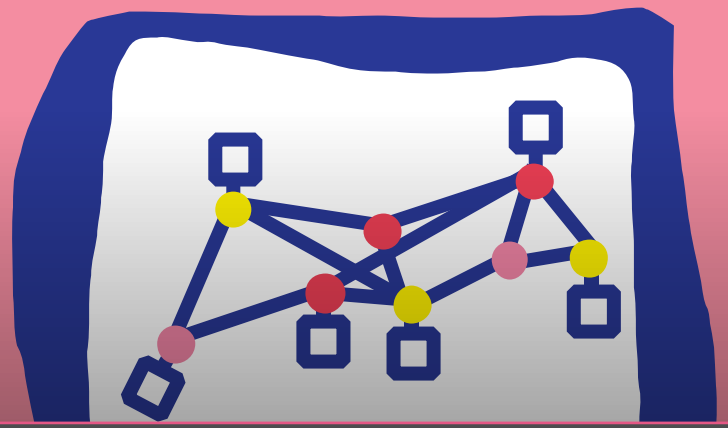

Management Facility
Main Control Center
SCADA Historian
SmartEvent
SCADA VPN
Control & monitor
Control
Monitor
PLC1
PLC2
PLC3
PLC4
Shop Floor
Shop Floor



Check Point®
SOFTWARE TECHNOLOGIES LTD.

- 產品優勢分析及公司簡介

Nasdaq科技百強，以色列安全傳奇:Check Point Software



$1.85B

2017全球營業額

1,402

研發人員
(網通安全業界最高比例)

December 2017

100,000

全球客戶群
(60+國家在地服務)

Gartner魔術象限: 企業級網路防火牆

無人能比的傳奇
連續20年領導者

Gartner

持續於
Vision完整性
領先群倫

全球最大人工智能威脅引擎

THREATCLOUD

全球高達15萬台設備事件反饋

快速編譯威脅情資分析

即時安全特徵更新

500,000,000+
惡意檔案與站台資料

700,000 +
每日惡意程式偵測量

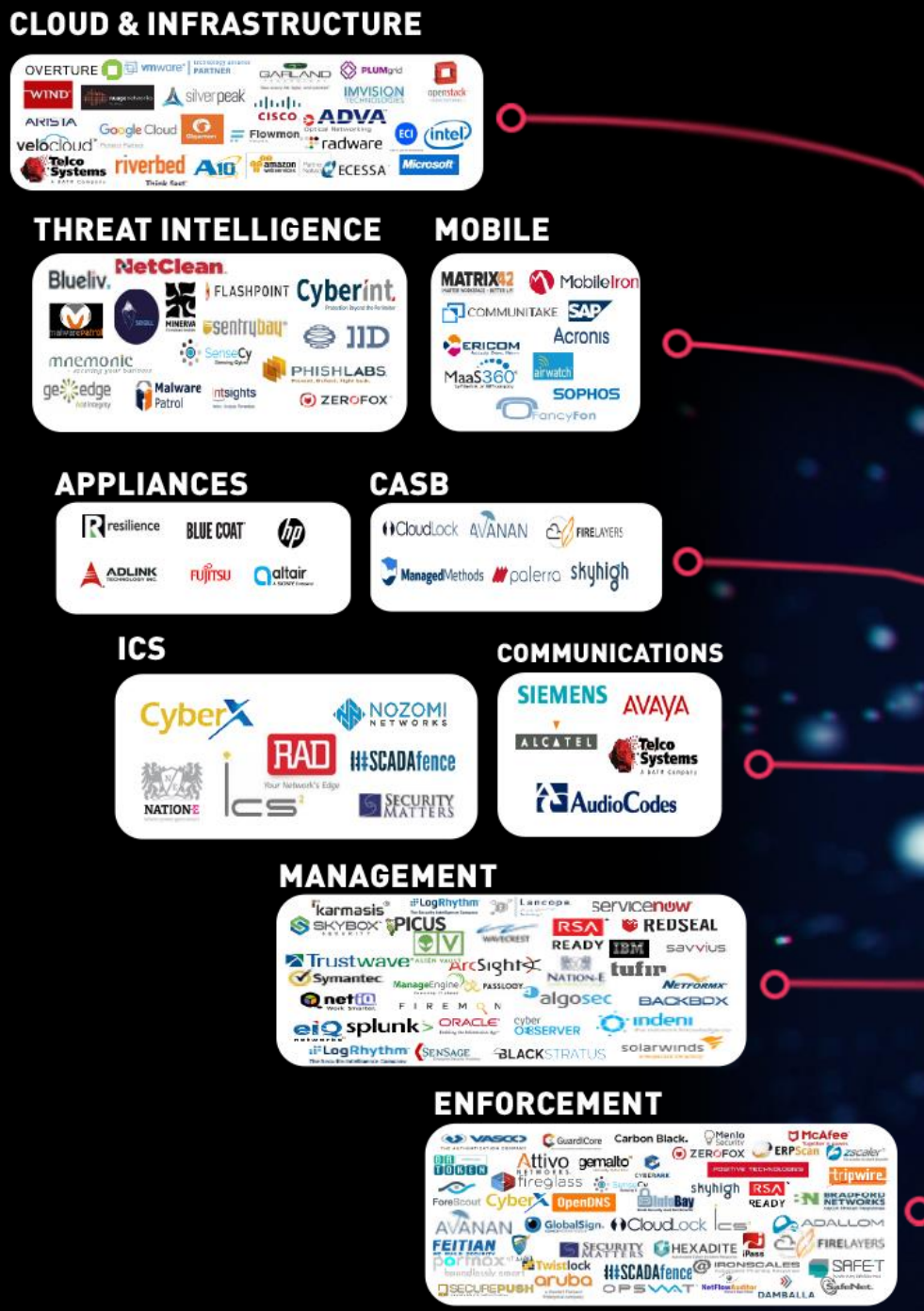
250,000,000
駭客中繼站

17,000,000
每週惡意攻擊
事件偵測量

11,000,000
惡意程式行為分析與
威脅特徵碼

最先進惡意威脅
數據資料庫

全球最大IT資安生態圈
橫跨多種產業



160+

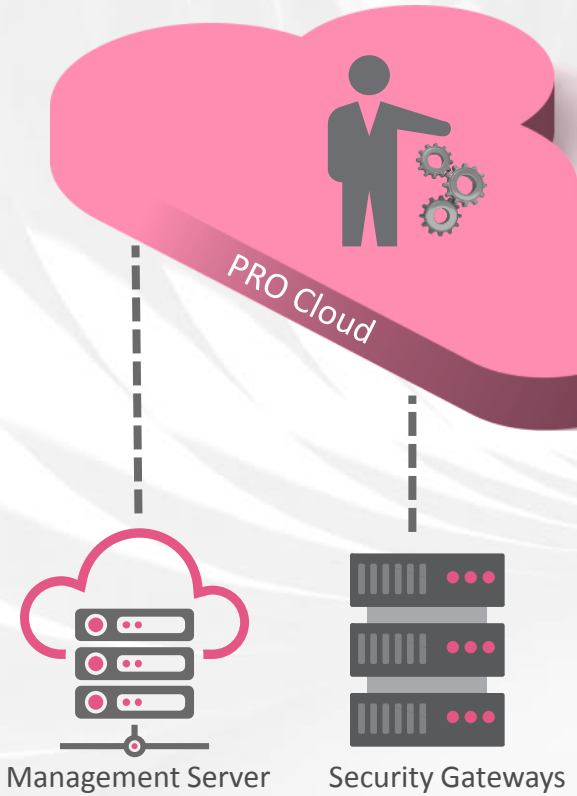
安全科技戰略夥伴

Check Point
SOFTWARE TECHNOLOGIES LTD

SOURCE: HTTPS://WWW.CHECKPOINT.COM/PARTNERS/OPSEC

主動監控與通報服務(PRO Support)

蒐集閘道/管理機資訊
至Check Point Cloud



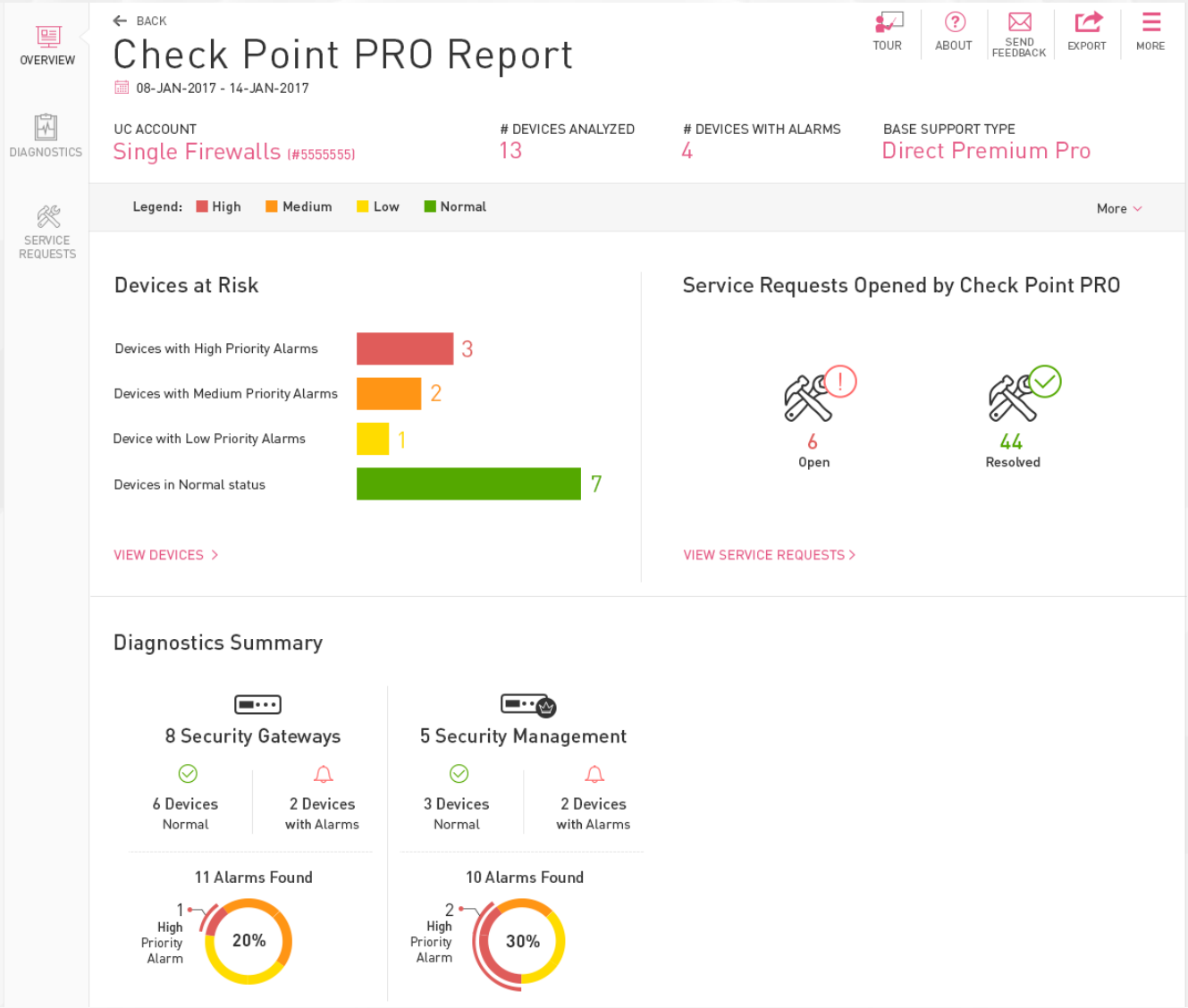
識別高重要等級的
事件與系統資訊

Check Point PRO專員
主動回報並修復狀況

在帳號內可看到完整的
歷程紀錄與可視性報表

CHECK POINT
PRO

日常維運報表管理



狀態診斷分析資訊

Check Point
SOFTWARE TECHNOLOGIES LTD

	4607 - Security Gateway Appliance SKU: CPAP-SG4607 CK:	CONFIGURATION: Cluster Security Gateway FW VERSION: R77.30	6 Alarms

Alarm Type	Alarm Description	Remediation	Priority Level
System	Logging problem detected. Gateway is writing logs locally due to high log rate	See sk40090, if the problem persists contact Check Point Support for further investigation.	
System	The following Check Point monitored processes are down: ci_cleanup	Try to start the process. If the problem persists contact Check Point support for further investigation. Additional information: 1. Check process status by running the 'cpwd_admin list' command. 2. To learn how to start various daemons, run cpwd_admin command. 3. See sk97638 to for additional information on Check Point processes and daemons	
System	RX Errors detected on machine interfaces	Presence of RX errors usually indicate a mismatch in duplex setting, mtu size, bad cabling or possibly a faulty interface card. Check the switch settings and fix the speed and duplex settings if there is a mismatch, check cabling and try a spare interface. For additional information refer to sk61922	
Patch Level	The installed Jumbo HFA version is at least two releases behind the recommended version. Installed: 198 Recommended Take: 216	Upgrade to the latest available Jumbo HFA. For more information refer to sk98028 - Jumbo Hotfix Accumulator FAQ.	
System	NTP is not configured	NTP is a vital service to synchronize the clocks on all Check Point gateways. This is very critical if you are trying to track a specific incident or troubleshoot a problem. For state synchronization between cluster members to function properly the clocks on the cluster members must be set to within 1 minute of each other. The best means of achieving this is to use NTP.	

NGFW產品安全技術比較

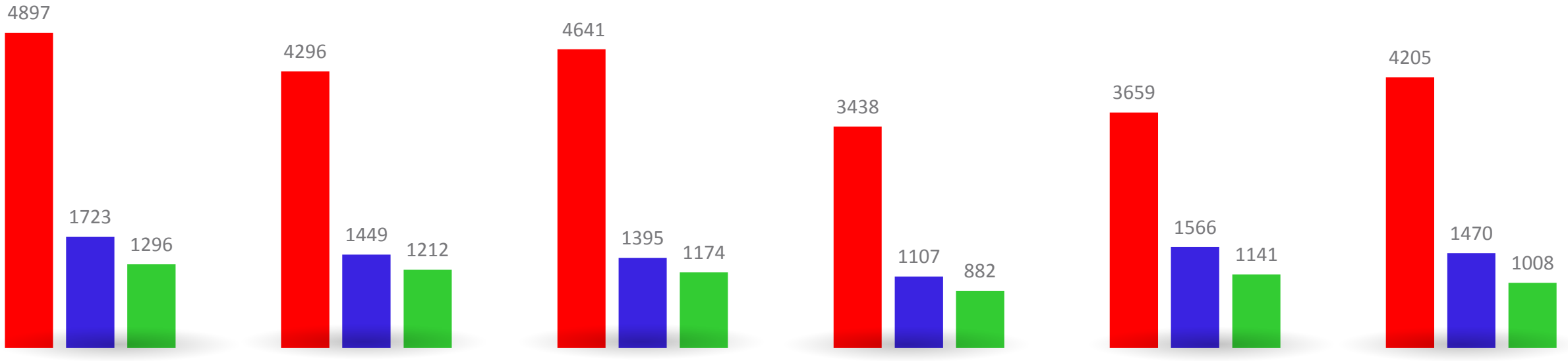
2017年重大安全漏洞平均回應時間(IPS更新)

Check Point
SOFTWARE TECHNOLOGIES LTD

	Patch Tuesday 2017	WannaCry & NotPetya CVE-2017-0144	Apache Struts 2 CVE-2017-9805 CVE-2017-9791	MELTDOWN SPECTRE CVE-2017-5753 CVE-2017-5715 CVE-2017-5754D
Check Point	40 min	1 day	1 day	12 hours
paloalto	458 min	30 days	6 days	36 hours
FORTINET	216 min	30 days	4 days	32 hours

Source: vendors security advisories web pages & http://tiny.cc/urgency

IPS特徵防護內含CVE漏洞數量 (Jan 2010-Feb 2018)



Information is current as of Jan 2010 – Feb 26, 2018 | Source: Check Point Advisories | Palo Alto ThreatVault | Fortinet FortiGuard | Mcafee Threat Intelligence | Tipping Point Digital Vaccine | SourceFire Advisories

領先業界的應用程式(L7)管理能力

Check Point
SOFTWARE TECHNOLOGIES LTD

潛在高風險應用程式	Check Point	Palo Alto Networks	Fortinet	Cisco
# 匿名穿牆/Tunnel應用程式(如 TOR, UltraSurf, HideMyAss…)	220	112	148	40
# P2P應用程式 (如 Bitorrent, WinMX…)	343	133	81	52
# 檔案雲端分享應用程式 (如 Dropbox, Google Drive, Mega…)	954	307	195	160
# 遠端控管應用程式 (如 TeamViewer, LogMeIn…)	147	96	85	67
整體可識別應用程式數量	7,794	2,554	3,738	3,511

Source: Check Point AppWiki, PAN Applipedia, Fortinet FortiGuard, Cisco FirePower , as of Feb 26, 2018

全球安全防護技術領導者

+

2017 ‘Recommended’ vendor
Breach Prevention System

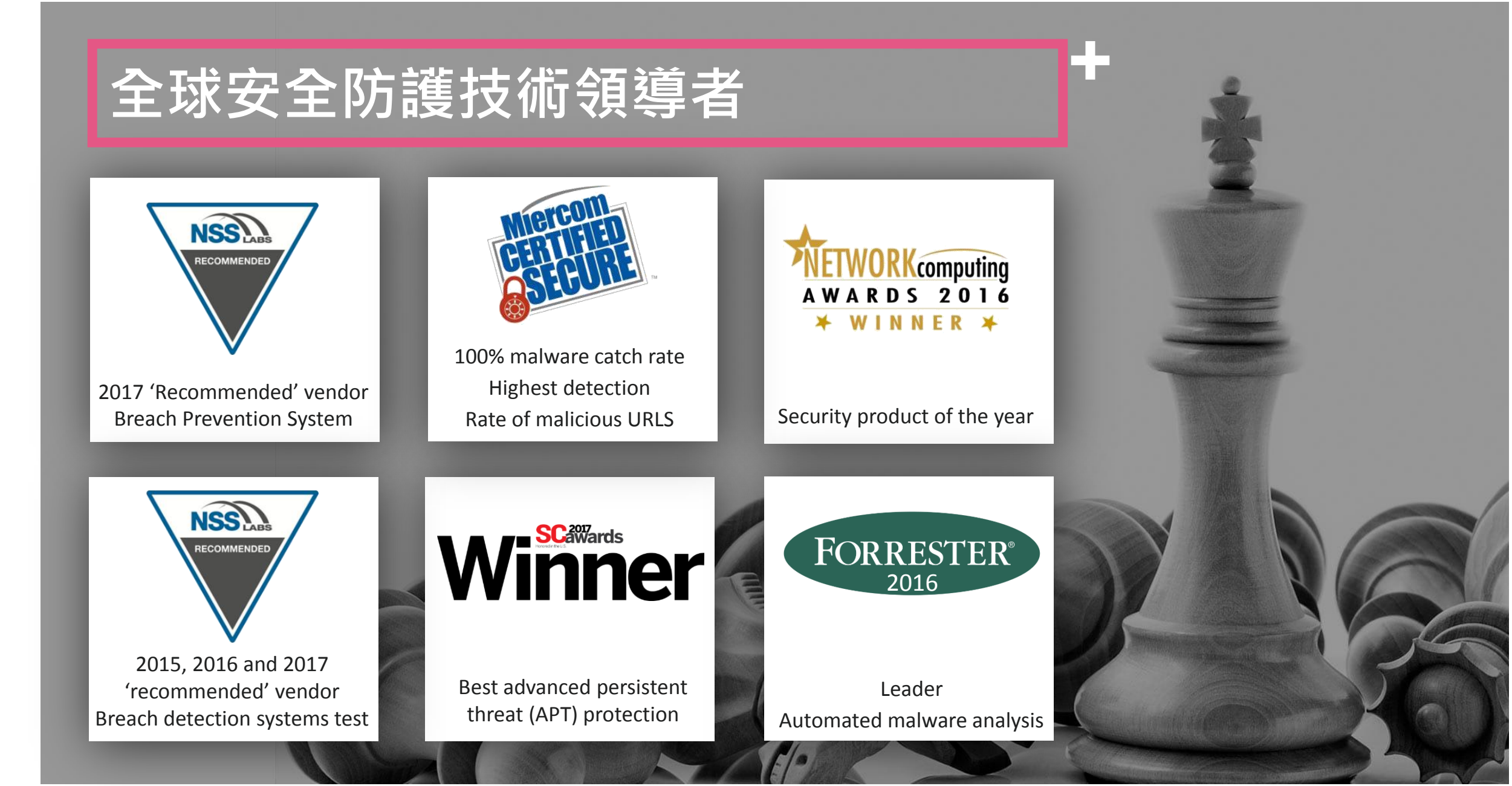
100% malware catch rate
Highest detection
Rate of malicious URLS

Security product of the year

2015, 2016 and 2017
‘recommended’ vendor
Breach detection systems test

Best advanced persistent
threat (APT) protection

Leader
Automated malware analysis



CHECK POINT SANDBLAST

最佳安全效益與性價比

2017 NSS Breach Prevention Systems Test

100% C
整體威脅
防護分數

100%
崁入下載
惡意防護

100%
社交工程
惡意防護

100%
網路下載
惡意防護

100%
電子郵件
惡意防護

100%
離線感染
測試

99.2%
惡意規避
測試

14$
最佳TCO

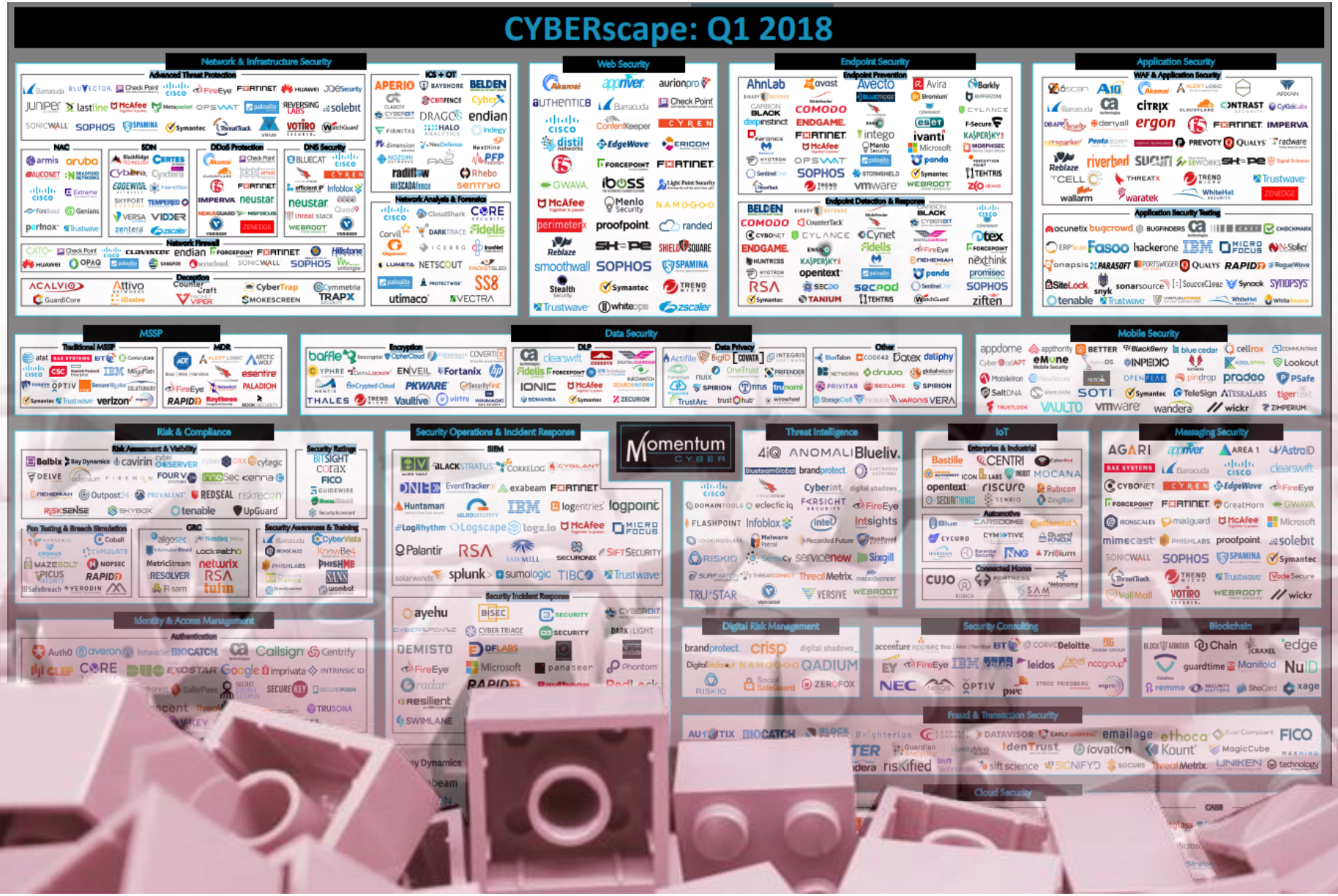
0%
誤報率

是縱深防禦? 還是疊床架屋的拼裝安全?

Check Point
SOFTWARE TECHNOLOGIES LTD

聚焦安全投資，保障企業健全TCO

Check Point
SOFTWARE TECHNOLOGIES LTD



從現在開始，重新省思安全定義

Check Point
SOFTWARE TECHNOLOGIES LTD

Check Point
SOFTWARE TECHNOLOGIES LTD

THANK YOU

Check Point Infinity Total Protection

楊敦凱 Danny Yang I 技術顧問

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

CLOUD • MOBILE • THREAT PREVENTION