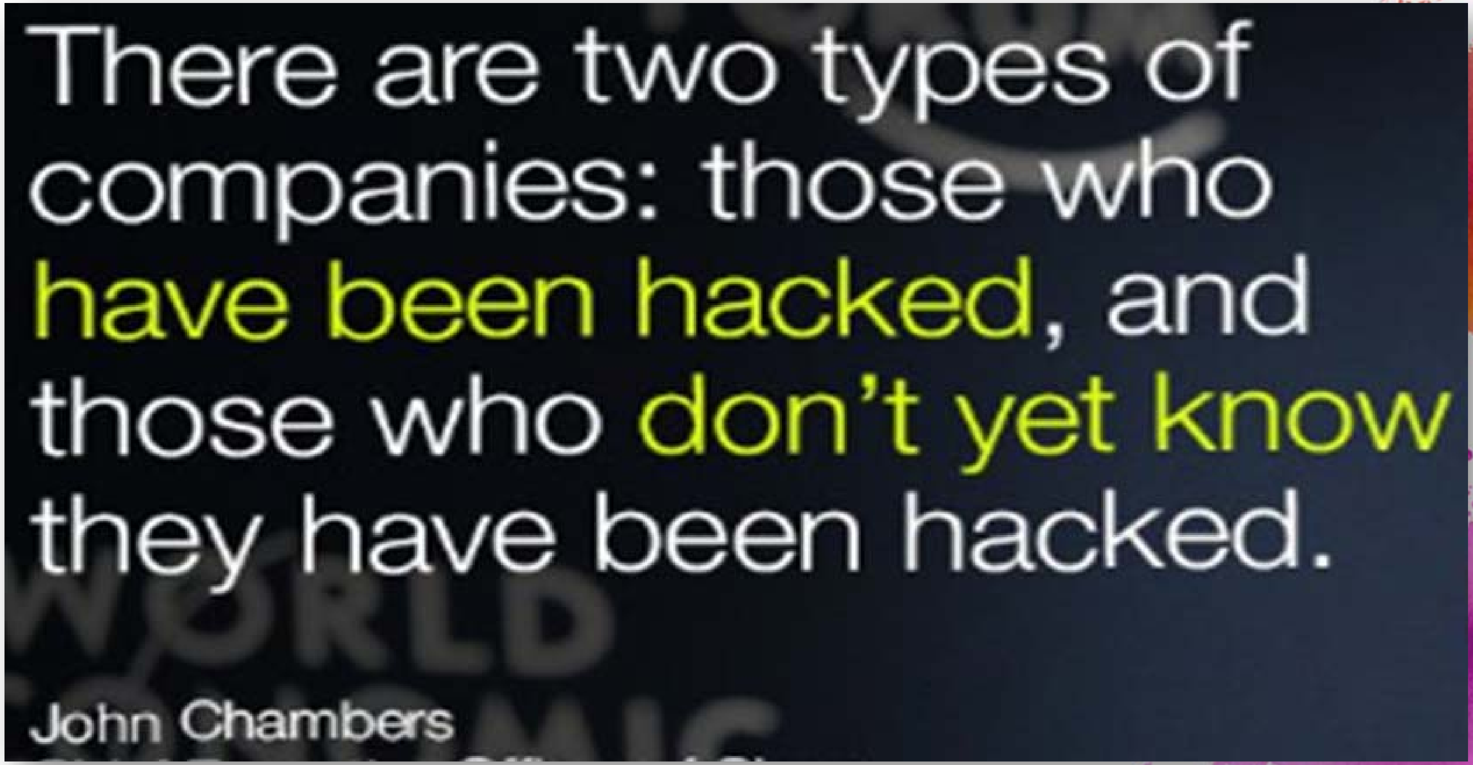
Hwacom 華電聯網

安控不可不知的資訊安全

資安產品應用部
杜偉欽 Kelvin Tu
0952-492-435
Kelvin.tu@hwacom.com

華|人|寬|頻|世|界|的|首|席|建|構|家

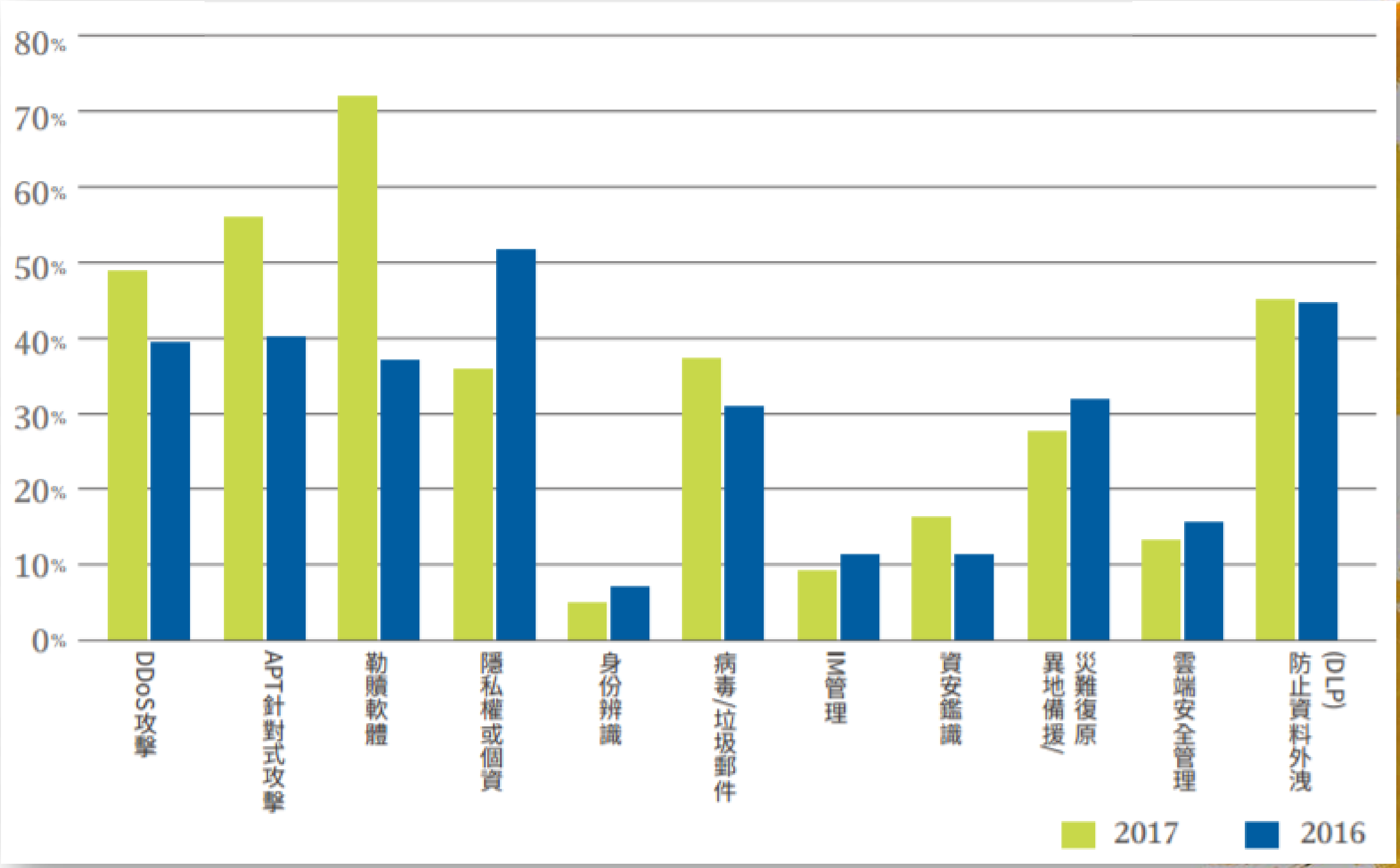
世界上有兩種類型的公司



There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked.

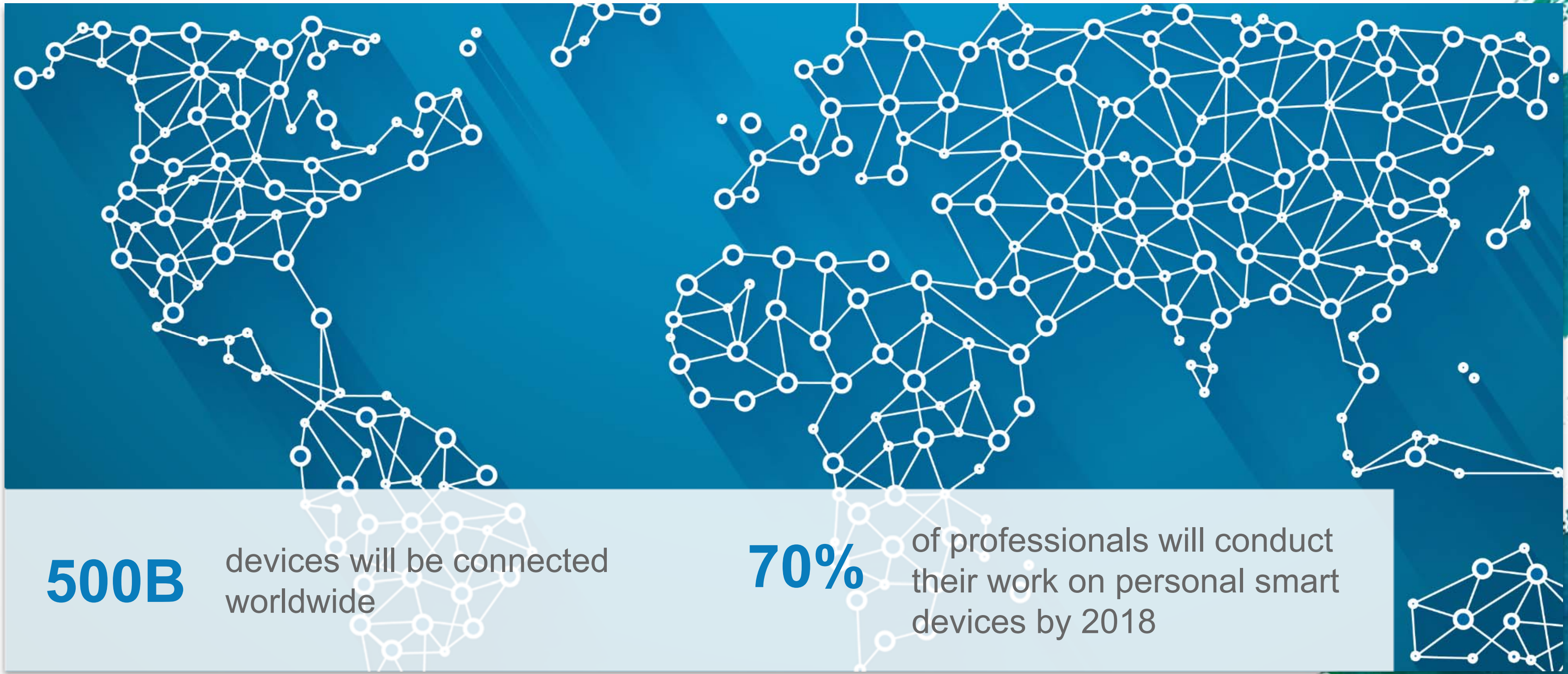
John Chambers

2017 資安事件議題



圖表參考資料：IThome

How Many Devices Will Connect to Your Network by 2030?



500B devices will be connected worldwide

70% of professionals will conduct their work on personal smart devices by 2018

DDoS 攻擊上升 6%：IoT 物聯網是主要攻擊原因！

汽車的CAN協定遭爆安全漏洞，可讓駭客關閉安全氣囊或感應器

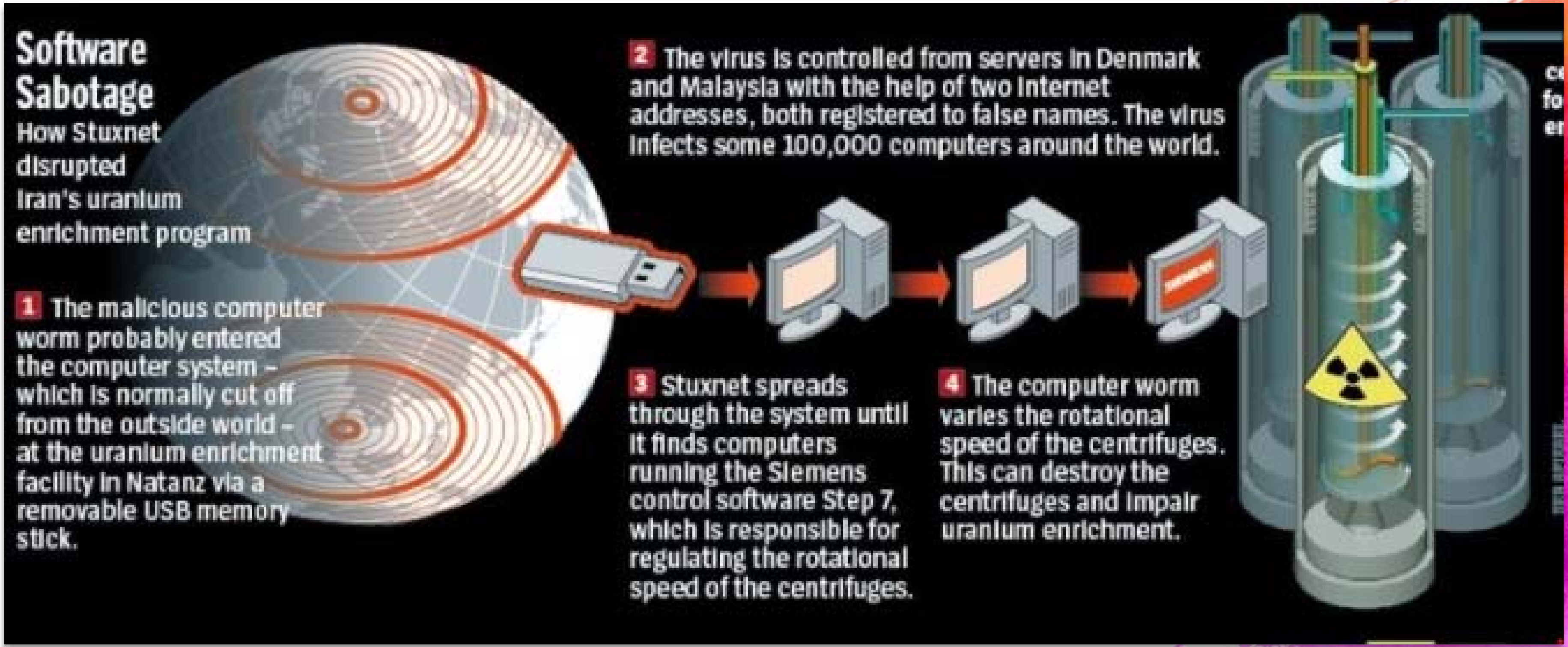
圖文參考資料：IThome

中國網路攝影機爆10多項安全漏洞，恐累及十多項品牌

圖片來源: F-Secure

文章參考資料：IThome

Zero Days – Stuxnet震網病毒



Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program

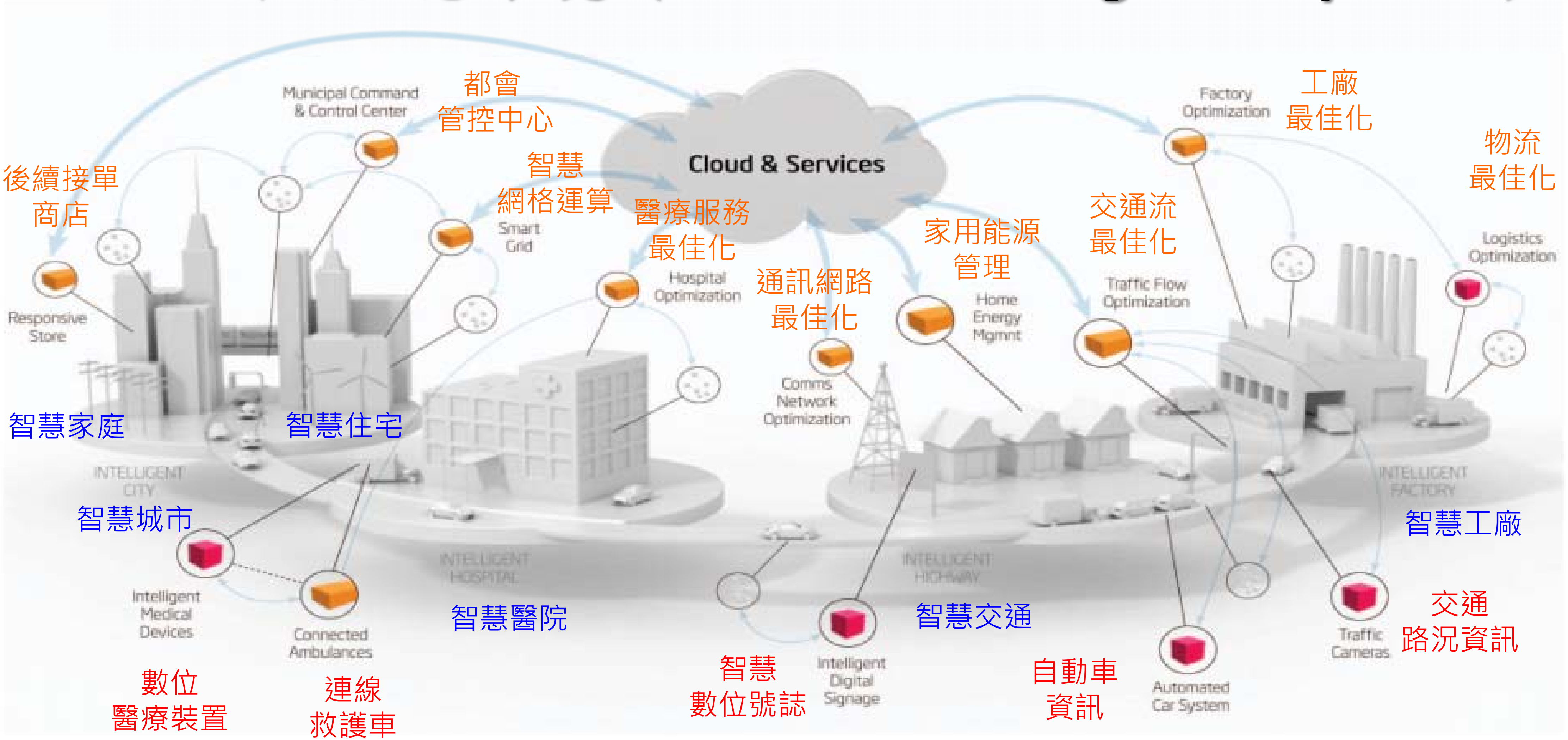
1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

物聯網生態環境（Internet of Things Eco-System ）



都會管控中心

智慧網格運算

醫療服務最佳化

後續接單商店

工廠最佳化

物流最佳化

交通流最佳化

家用能源管理

通訊網路最佳化

智慧家庭

智慧住宅

智慧城市

智慧工廠

智慧醫院

智慧交通

交通路況資訊

數位醫療裝置

連線救護車

智慧數位號誌

自動車資訊

圖片來源：http://www.satiztpm.it/internet-things/

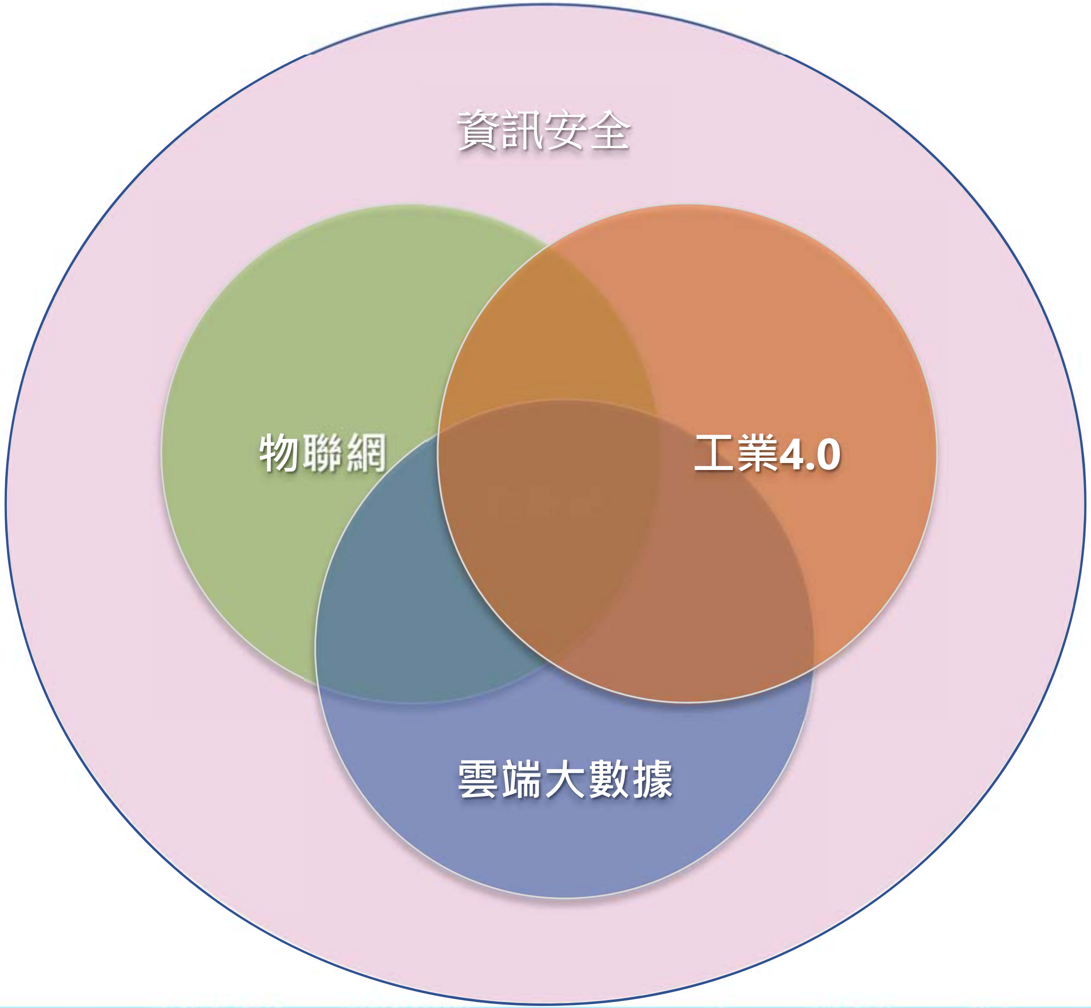
It’s harder than ever to see who is on your network and what they are doing

90% of surveyed organizations are not “fully aware” of the devices accessing their network

75% of companies say their mobile devices were targeted by malware in the last 12 months

And you can’t protect what you don’t see

We need security at all times



新的應用帶來新的威脅

Changing
Business Models

Dynamic
Threat Landscape

Complexity
and Fragmentation

行動裝置

Organizations ***lack visibility*** into the behavior of devices on their network

企業購併

Acquisitions, joint ventures, and partnerships are ***increasing in frequency***

雲端應用

Cloud usage is becoming more prevalent, but so is the ***lack of visibility into the cloud***

物聯網

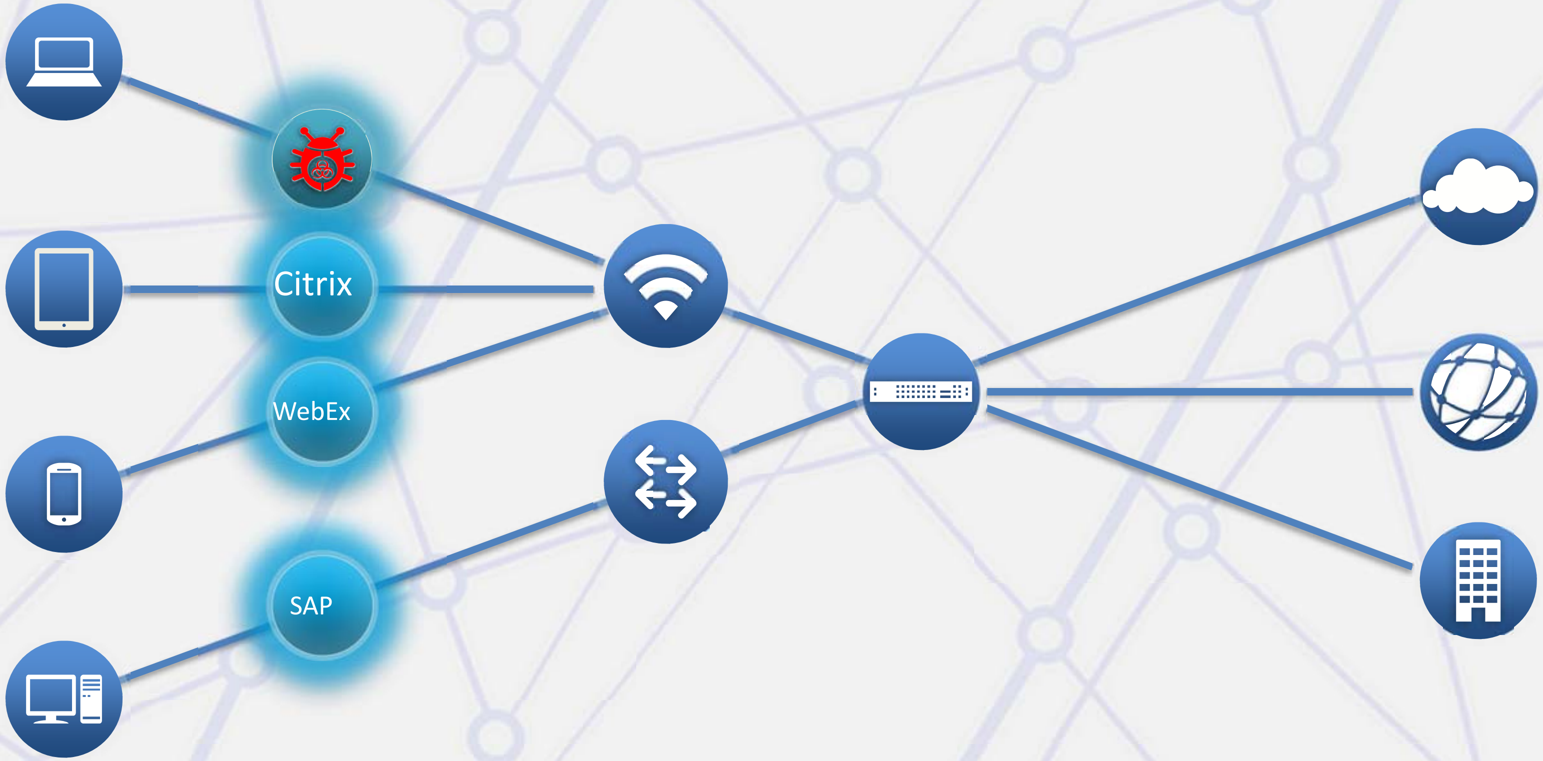
Over ***50 billion*** connected “smart objects” are projected by 2020

打擊面不斷變大….

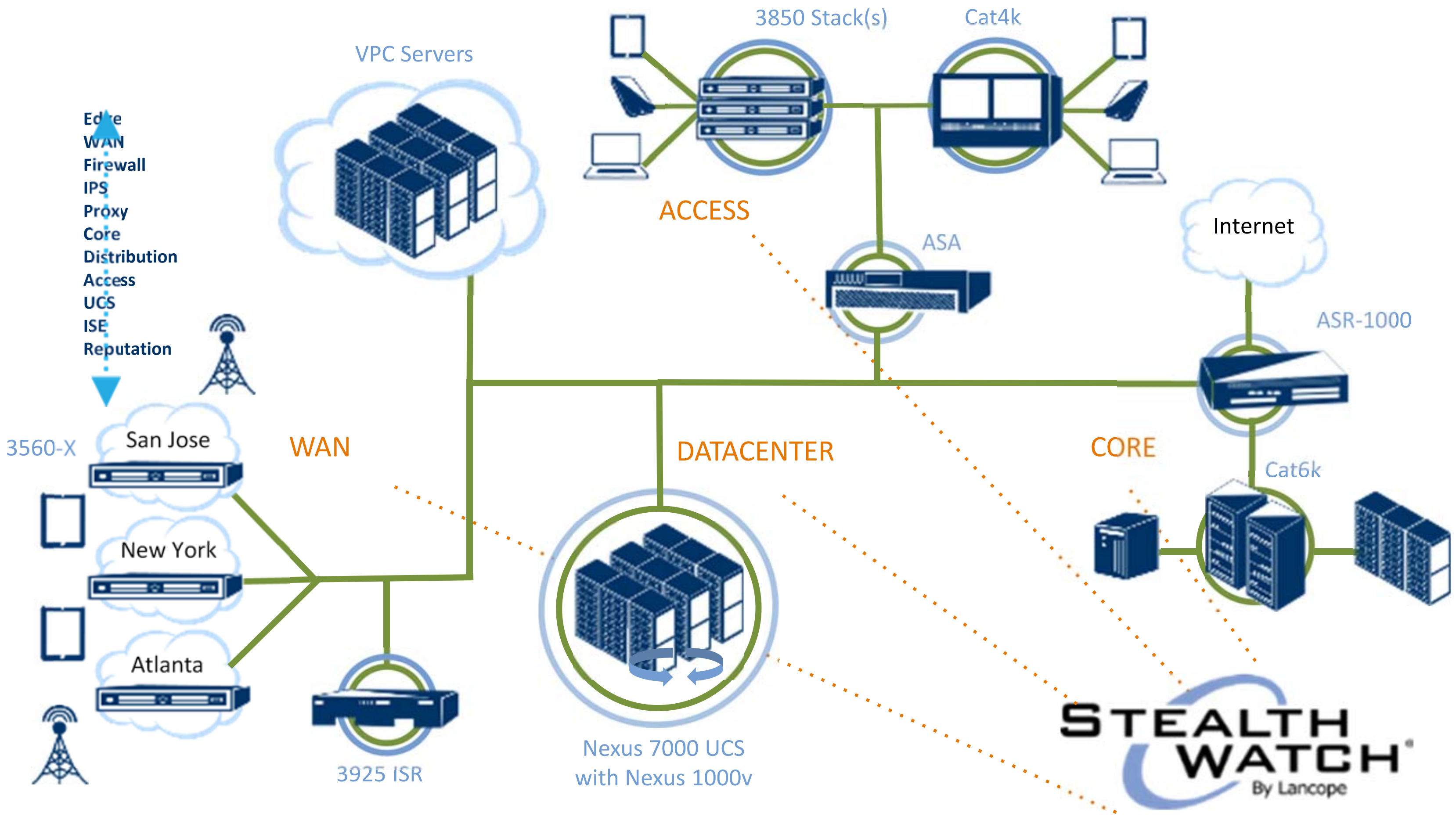
問題不在是否被入侵，而是何時

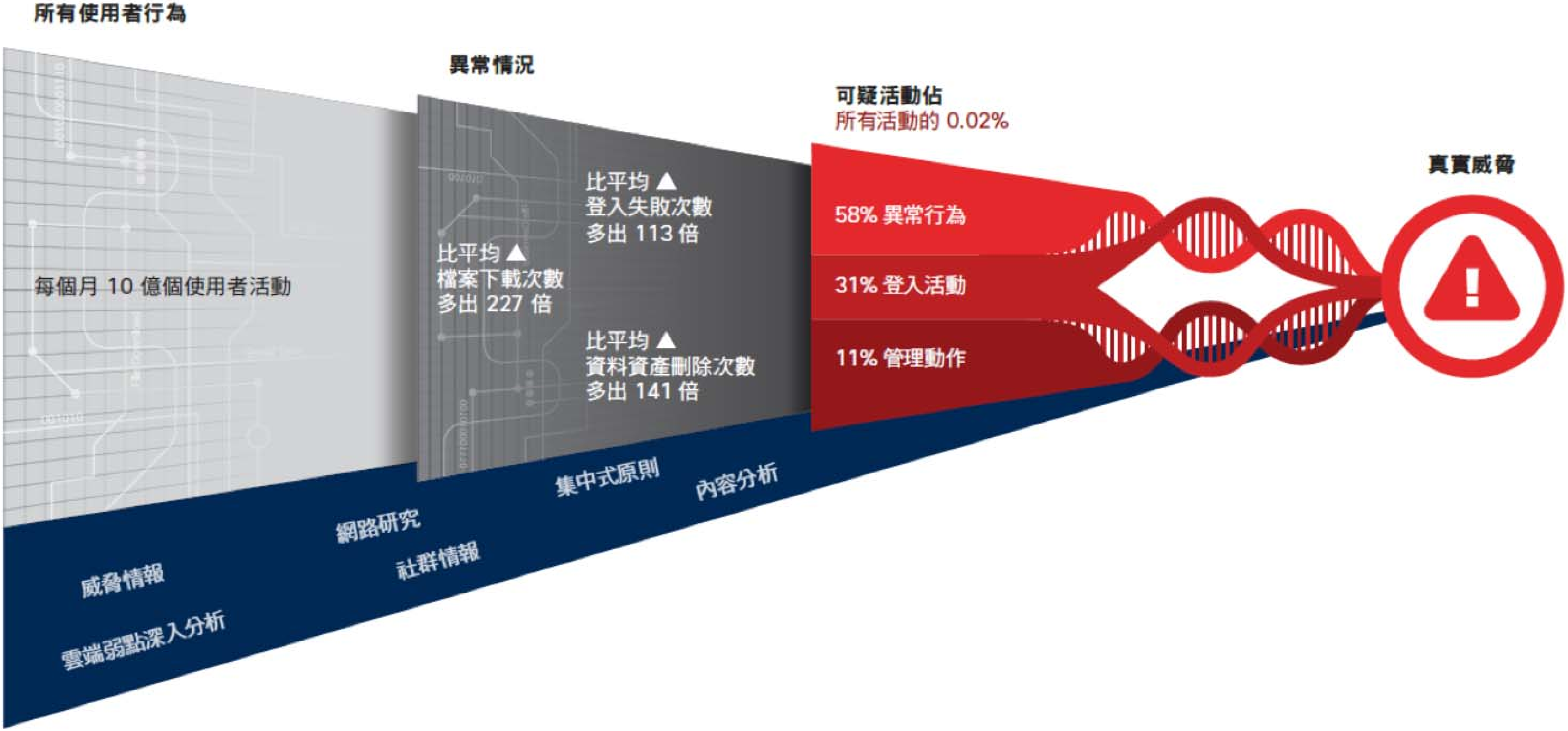
網路行為可視化分析

立即找出潛藏在網路內的駭客行為



Internal Visibility from Edge to Access, Network Is Your Sensor





所有使用者行為

每個月 10 億個使用者活動

異常情況

比平均▲
檔案下載次數
多出 227 倍

比平均▲
登入失敗次數
多出 113 倍

比平均▲
資料資產刪除次數
多出 141 倍

可疑活動佔
所有活動的 0.02%

58% 異常行為

31% 登入活動

11% 管理動作

真實威脅

威脅情報

雲端弱點深入分析

網路研究

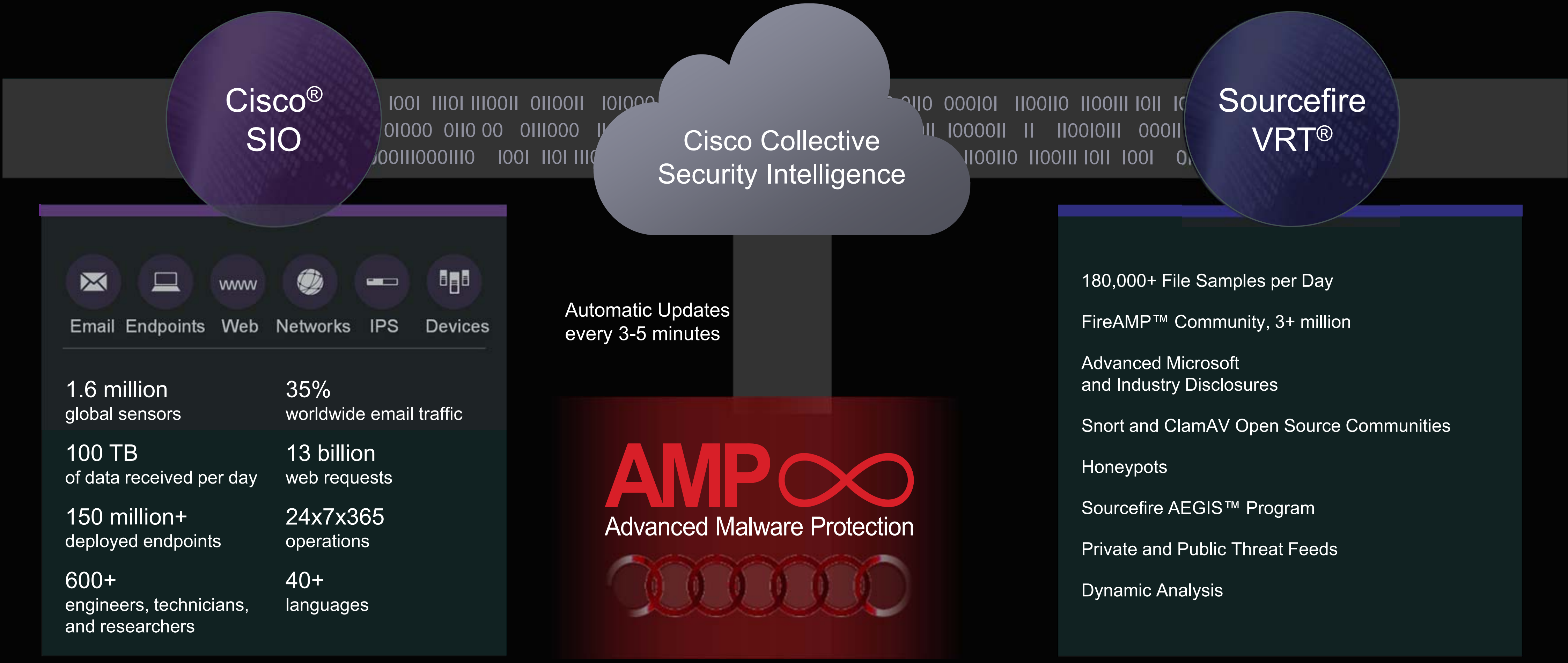
社群情報

集中式原則

內容分析

資料來源：思科 CloudLock

Cisco Advanced Malware Protection



Cisco® SIO

Email Endpoints Web Networks IPS Devices

1.6 million global sensors	35% worldwide email traffic
100 TB of data received per day	13 billion web requests
150 million+ deployed endpoints	24x7x365 operations
600+ engineers, technicians, and researchers	40+ languages

Cisco Collective Security Intelligence

Automatic Updates every 3-5 minutes

AMP

Advanced Malware Protection

Sourcefire VRT®

- 180,000+ File Samples per Day
- FireAMP™ Community, 3+ million
- Advanced Microsoft and Industry Disclosures
- Snort and ClamAV Open Source Communities
- Honeypots
- Sourcefire AEGIS™ Program
- Private and Public Threat Feeds
- Dynamic Analysis

身份管理 + 威脅可視化：Cisco ISE可解決IoT安全危機

眾多不同種類的設備

電腦、移動行動裝置、物聯網裝置的可視性及區域控管

控管每台裝置必須遵循的資安政策

可搭配威脅偵測軟體找出裝置的漏洞及威脅

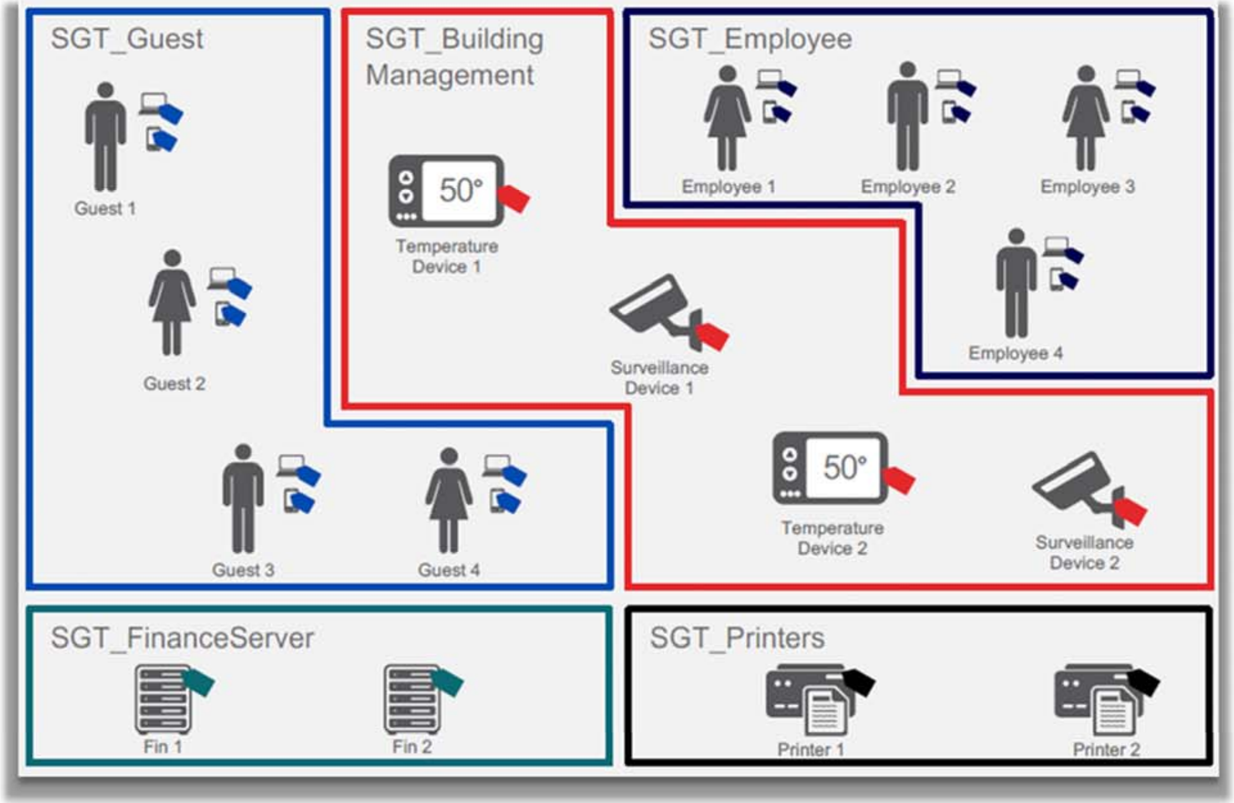
Who	Kevin
Device	Tablet, iOS, v9.1x
Location	Building 200, first floor
When	11:00 am EST on April 10
How	Wireless
Contact	555.111.3333

裝置**身份的可視性**、**可控性**和**防護**功能

以身份認證為基礎進行防禦

進一步擴展了以軟體為定義的業務政策，支援精細地劃分終端、使用者和地域的存取

藉由內部網路區域的隔離，防止惡意軟體的橫向攻擊及感染



Cisco ISE and AnyConnect

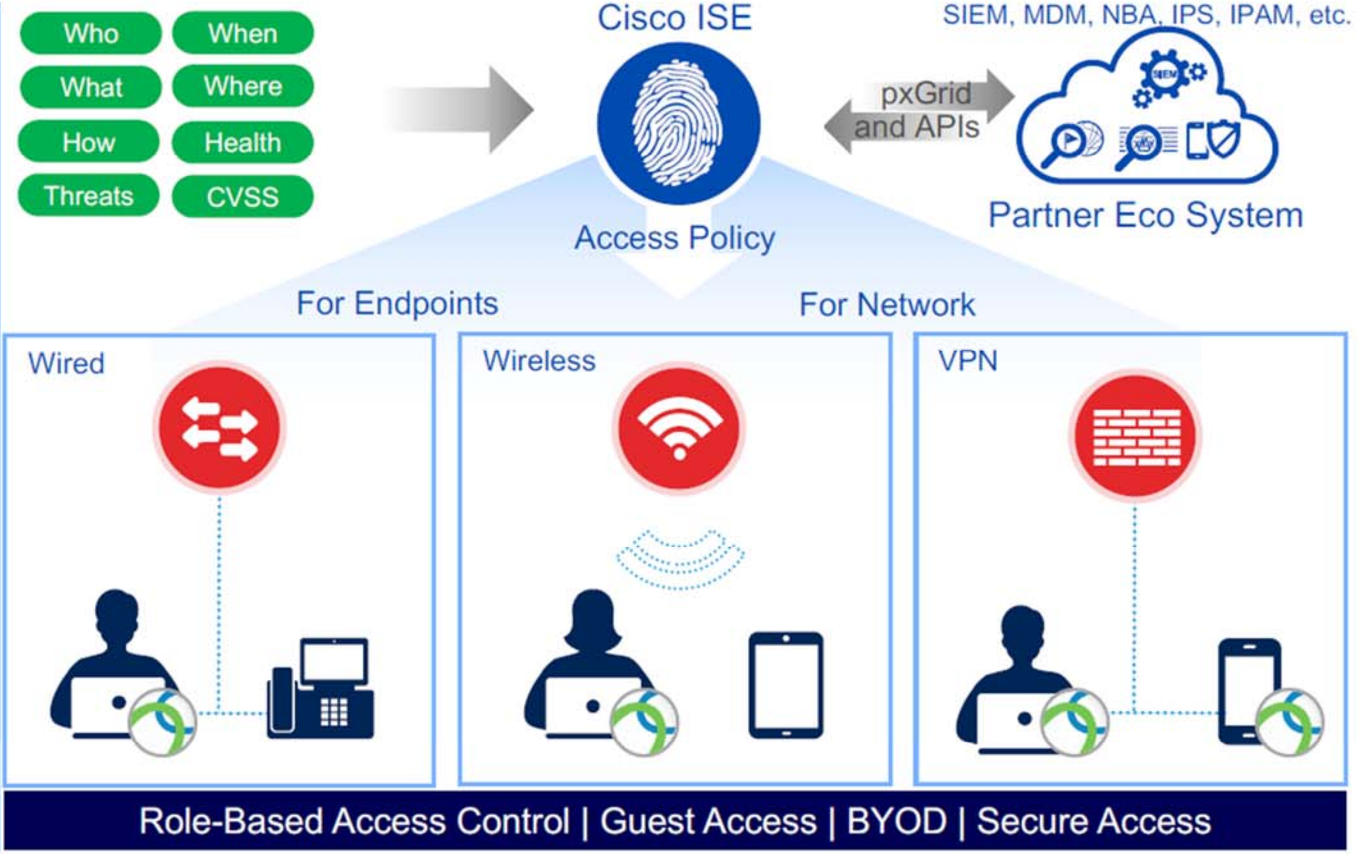
與第三方軟體分享資訊阻絕威脅

Cisco ISE

Context aware policy service, to control access and threat across wired, wireless and VPN networks.

Cisco Anyconnect

Supplicant for wired, wireless and VPN access. Services include: Posture assessment, Malware protection, Web security, MAC Security, Network visibility and more.

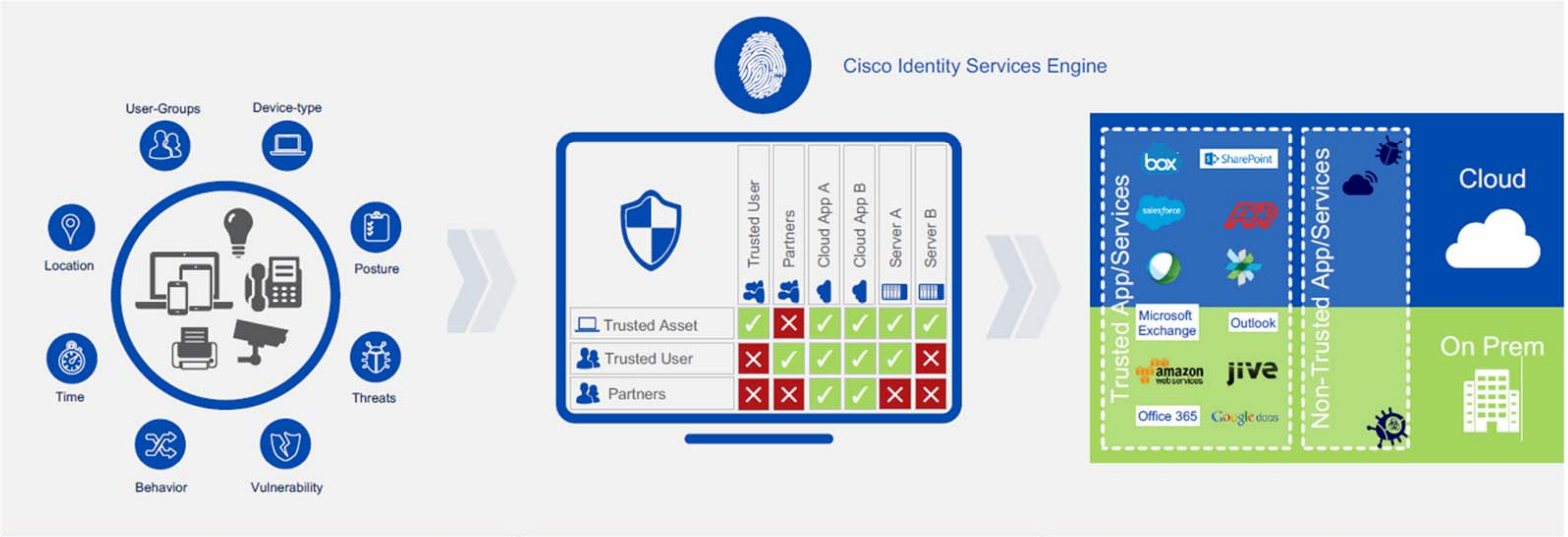


有線網路　無線網路　VPN加密網路

cisco

Managing Policy Based on ‘Trust’

Connecting Trusted Users and Devices to Trusted Services



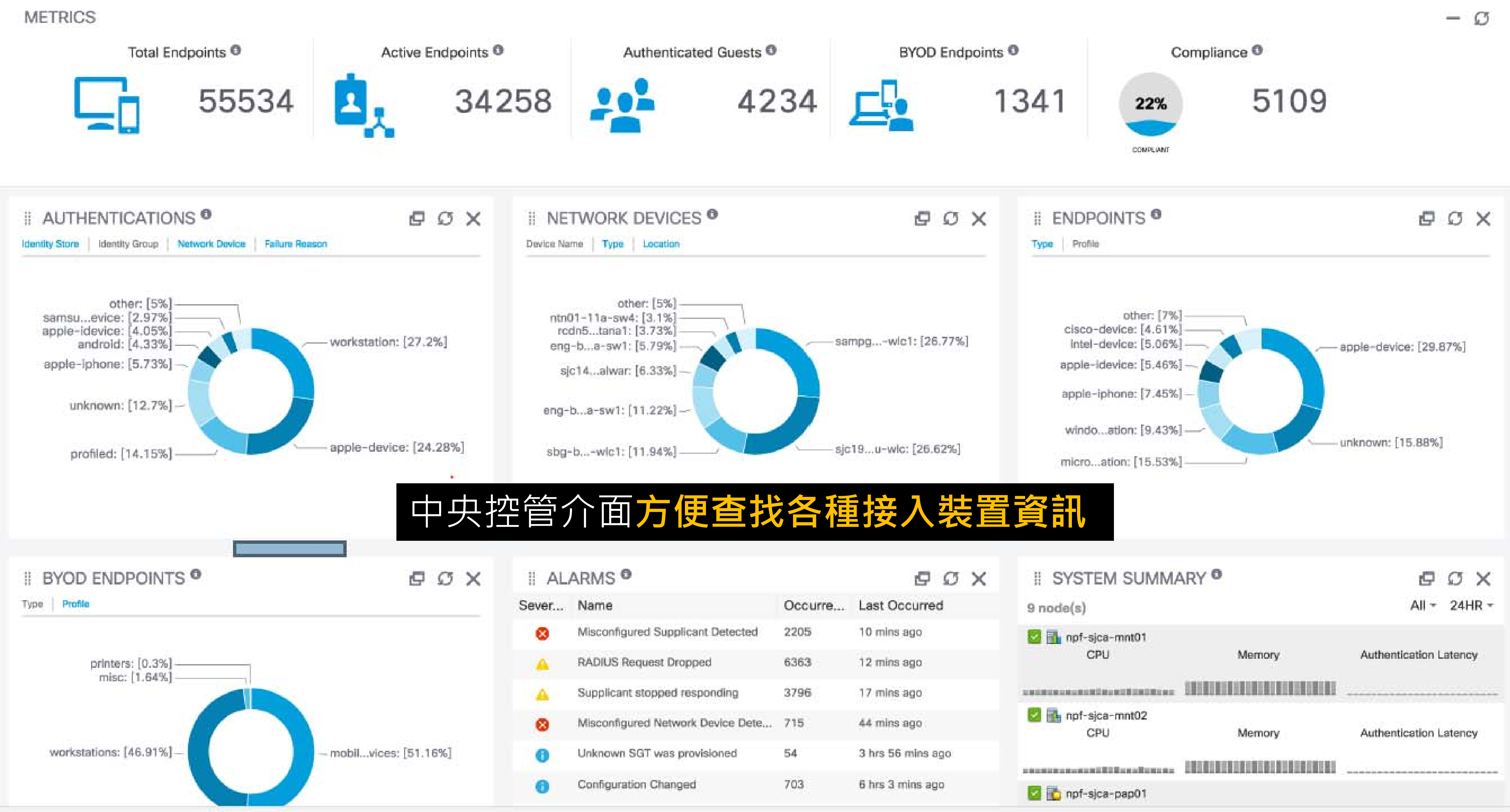
	Trusted User	Partners	Cloud App A	Cloud App B	Server A	Server B
Trusted Asset	✓	✗	✓	✓	✓	✓
Trusted User	✗	✓	✓	✓	✓	✗
Partners	✗	✗	✓	✓	✗	✗

Improved Visibility and Decision

Software-Defined Segmentation,
Service Access and Entitlement

Location-Free
App/Service Access

何種身分角色的裝置 >> 根據制定政策 >> 決定可去的區域



METRICS

Total Endpoints	Active Endpoints	Authenticated Guests	BYOD Endpoints	Compliance
55534	34258	4234	1341	5109

AUTHENTICATIONS

Identity Store | Identity Group | Network Device | Failure Reason

NETWORK DEVICES

Device Name | Type | Location

ENDPOINTS

Type | Profile

中央控管介面方便查找各種接入裝置資訊

BYOD ENDPOINTS

Type | Profile

ALARMS

Sever...	Name	Occurre...	Last Occurred
⊗	Misconfigured Supplicant Detected	2205	10 mins ago
⚠	RADIUS Request Dropped	6363	12 mins ago
⚠	Supplicant stopped responding	3796	17 mins ago
⊗	Misconfigured Network Device Dete...	715	44 mins ago
ⓘ	Unknown SGT was provisioned	54	3 hrs 56 mins ago
ⓘ	Configuration Changed	703	6 hrs 3 mins ago

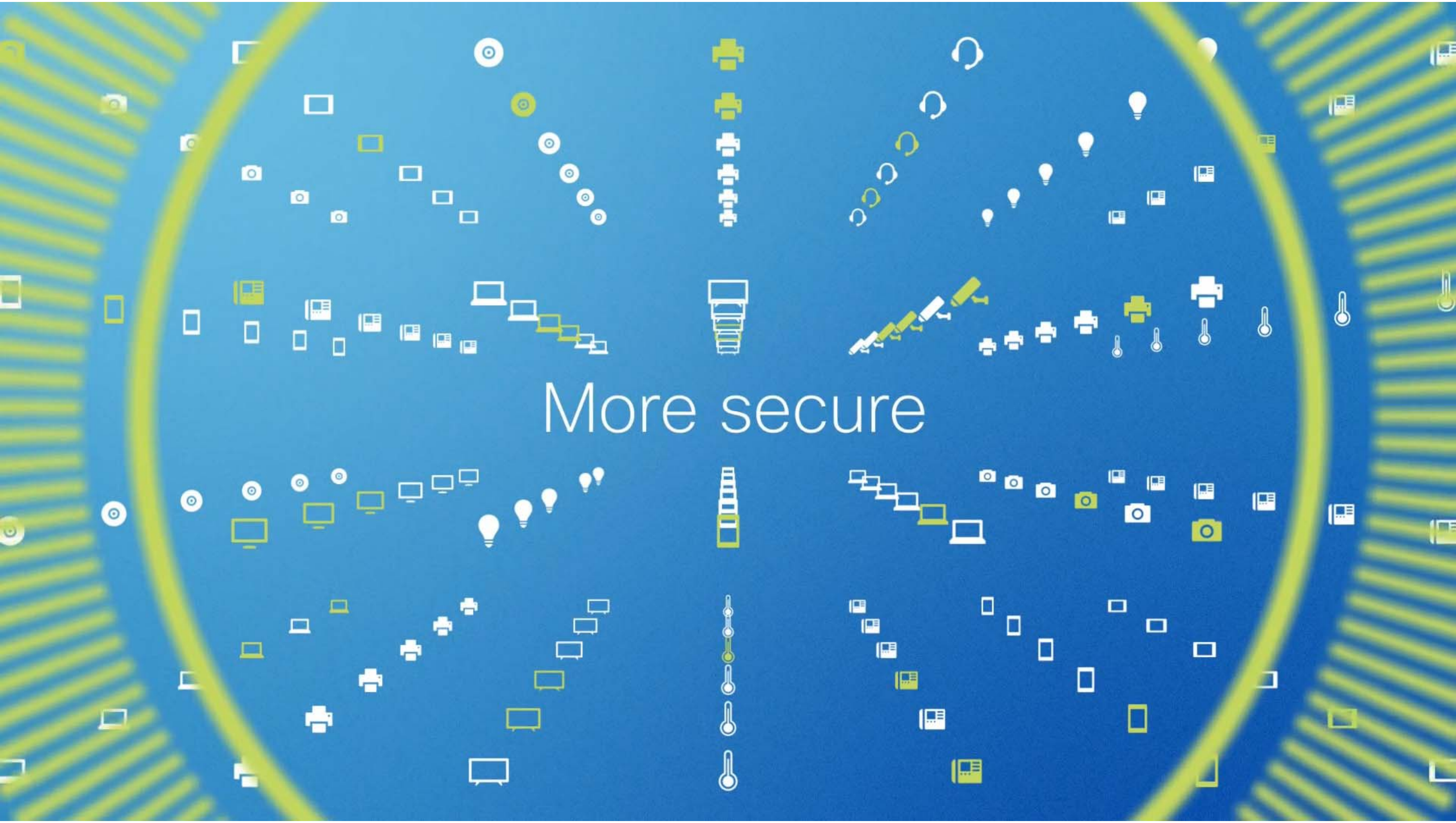
SYSTEM SUMMARY

9 node(s) All ▾ 24HR ▾

☑ npf-sjca-mnt01
CPU Memory Authentication Latency

☑ npf-sjca-mnt02
CPU Memory Authentication Latency

☑ npf-sjca-pap01

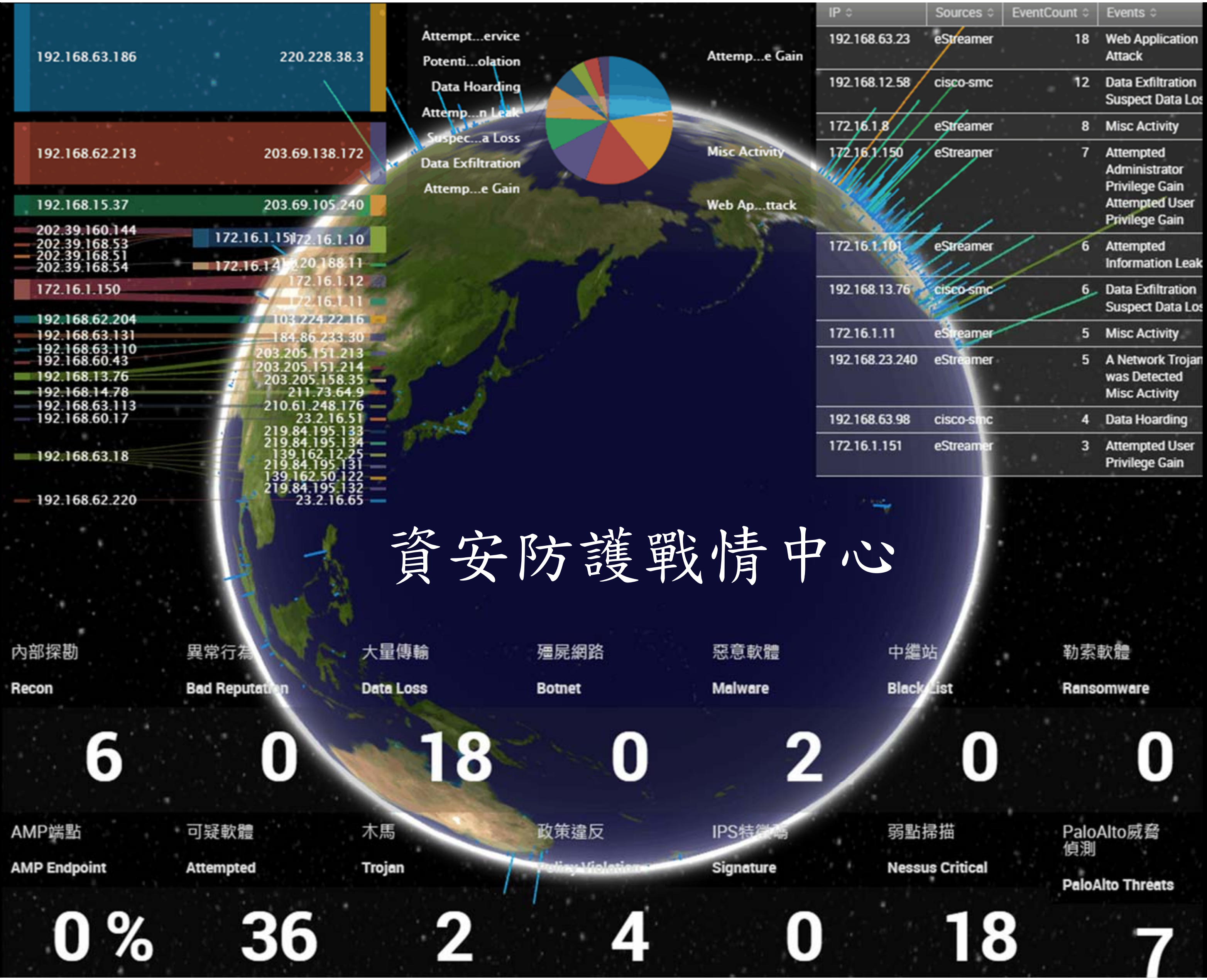

More secure

Faster Insights

快速可視發現

Better Control

更好管控措施



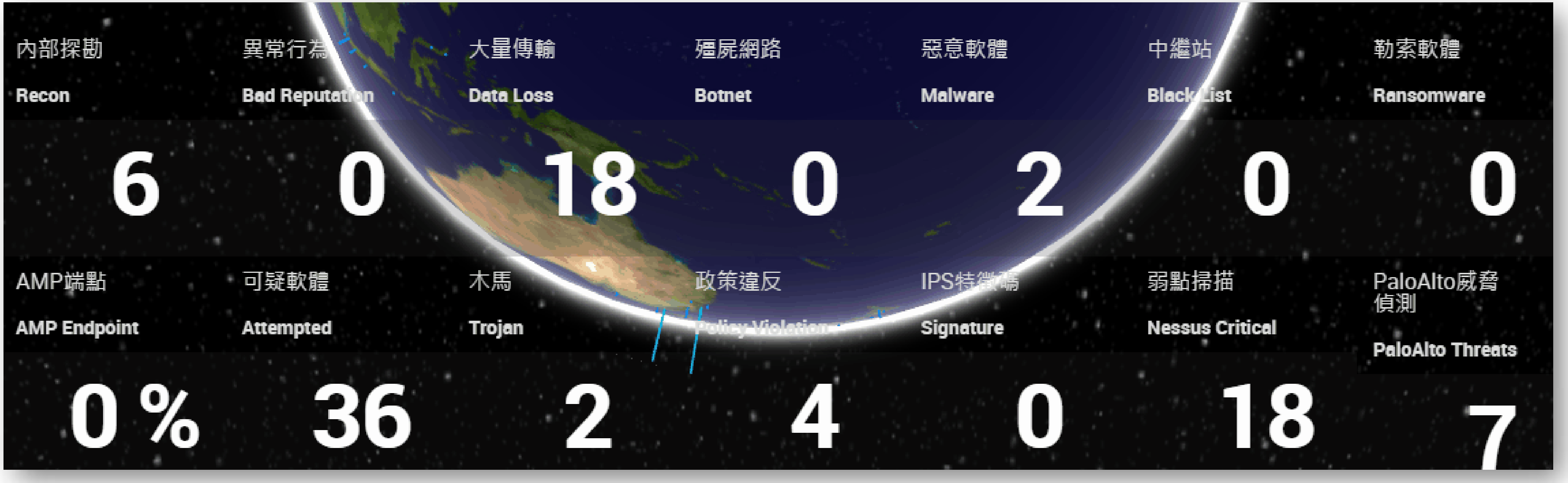
IP ⇕	Sources ⇕	EventCount ⇕	Events ⇕
192.168.63.23	eStreamer	18	Web Application Attack
192.168.12.58	cisco-smc	12	Data Exfiltration Suspect Data Los
172.16.1.8	eStreamer	8	Misc Activity
172.16.1.150	eStreamer	7	Attempted Administrator Privilege Gain Attempted User Privilege Gain
172.16.1.101	eStreamer	6	Attempted Information Leak
192.168.13.76	cisco-smc	6	Data Exfiltration Suspect Data Los
172.16.1.11	eStreamer	5	Misc Activity
192.168.23.240	eStreamer	5	A Network Trojan was Detected Misc Activity
192.168.63.98	cisco-smc	4	Data Hoarding
172.16.1.151	eStreamer	3	Attempted User Privilege Gain

資安防護戰情中心

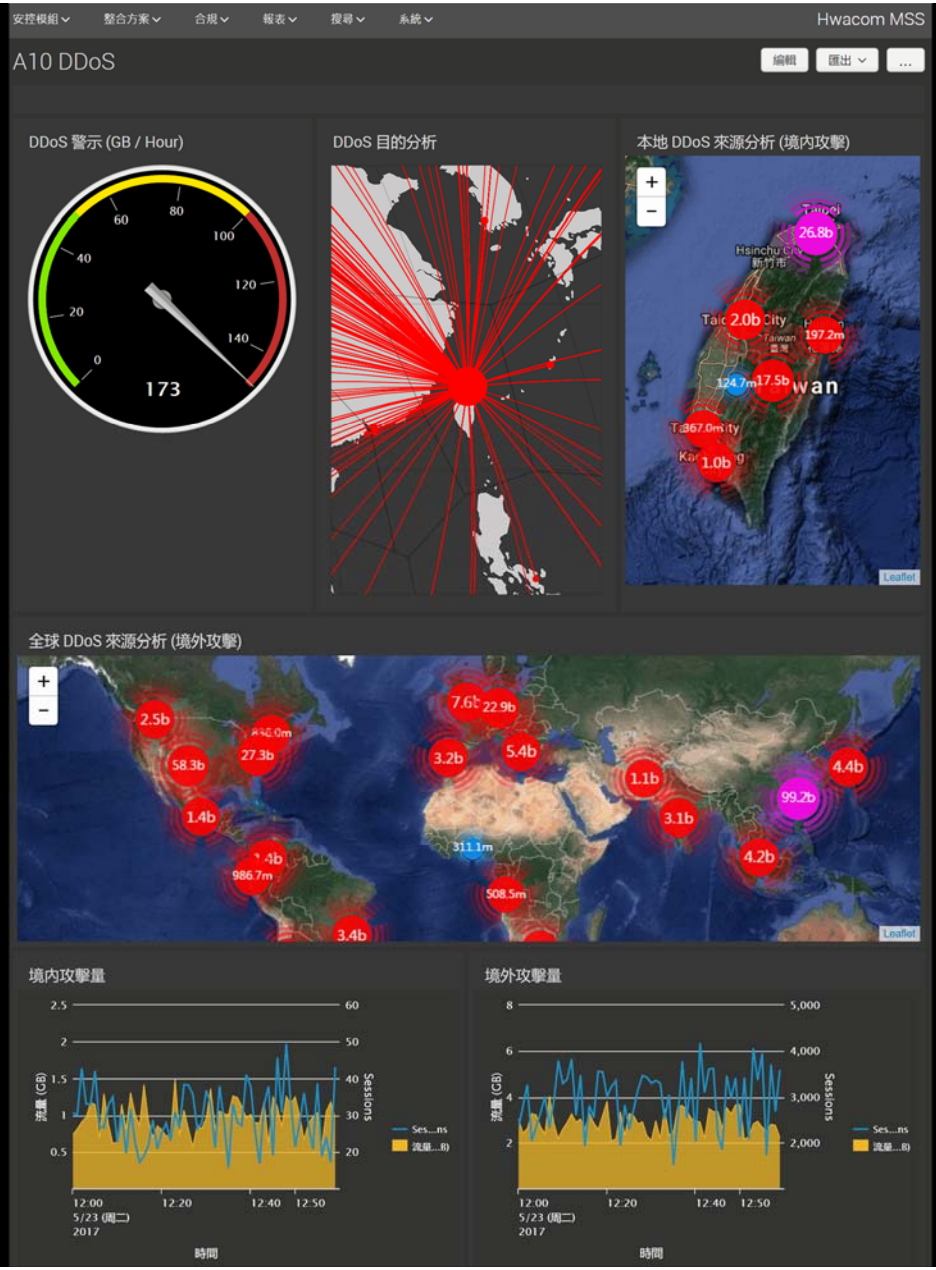
內部探勘	異常行為	大量傳輸	殭屍網路	惡意軟體	中繼站	勒索軟體
Recon	Bad Reputation	Data Loss	Botnet	Malware	Black List	Ransomware
6	0	18	0	2	0	0
AMP端點	可疑軟體	木馬	政策違反	IPS特徵碼	弱點掃描	PaloAlto威脅偵測
AMP Endpoint	Attempted	Trojan	Policy Violation	Signature	Nessus Critical	PaloAlto Threats
0 %	36	2	4	0	18	7

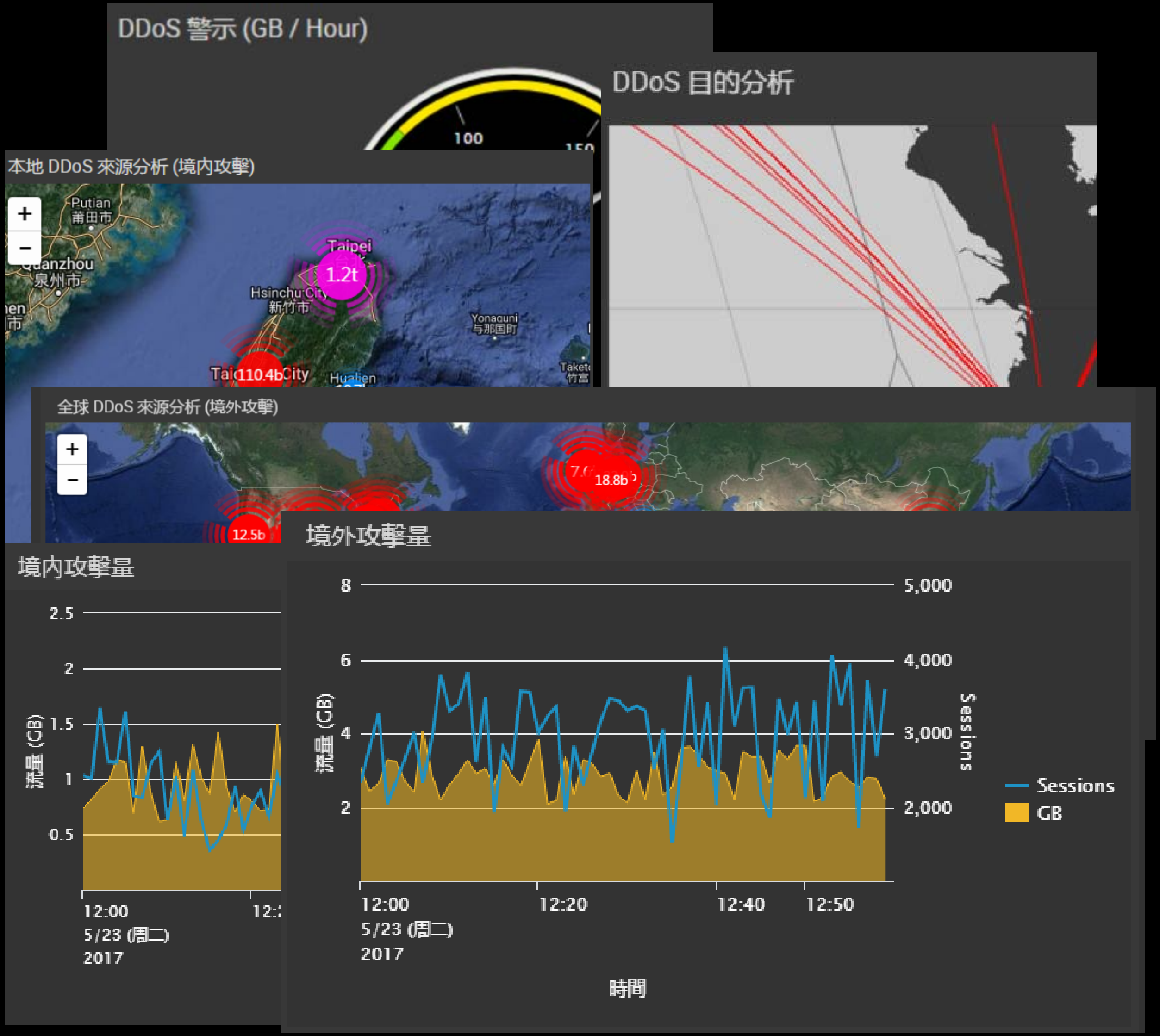
使用者行為分析模組

- 可視性行為分析模組，快速查詢安全威脅。
- 進行交叉關聯式分析，找出害群之馬。
- 自動化通知相關負責人，立即處理問題。

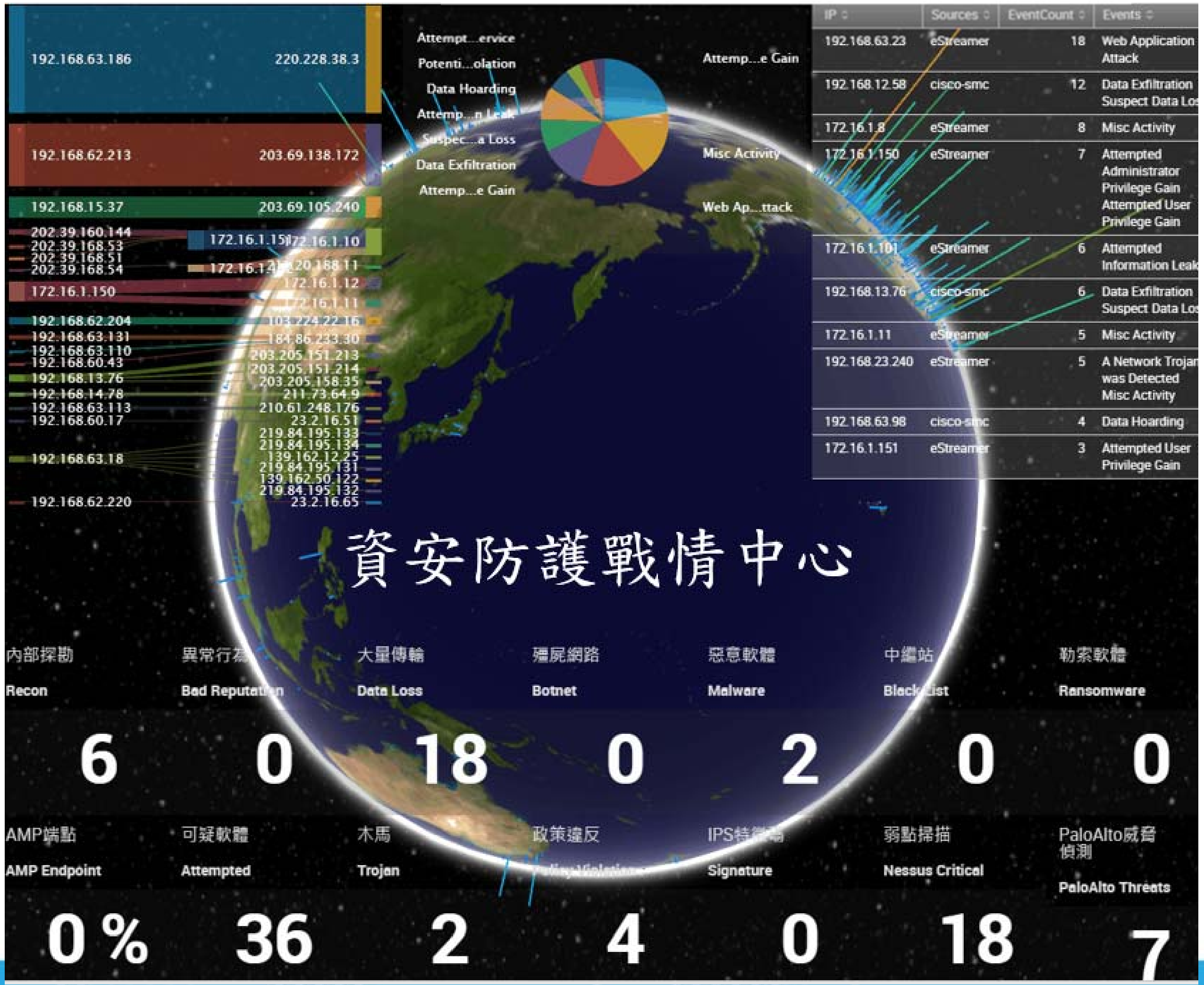


內部探勘 Recon	異常行為 Bad Reputation	大量傳輸 Data Loss	殭屍網路 Botnet	惡意軟體 Malware	中繼站 Black List	勒索軟體 Ransomware
6	0	18	0	2	0	0
AMP端點 AMP Endpoint	可疑軟體 Attempted	木馬 Trojan	政策違反 Policy Violation	IPS特徵碼 Signature	弱點掃描 Nessus Critical	PaloAlto威脅偵測 PaloAlto Threats
0 %	36	2	4	0	18	7


安控模組
整合方案
合規
報表
搜尋
系統
Hwacom MSS
A10 DDoS
編輯
匯出
...
DDoS 警示 (GB / Hour)
173
DDoS 目的分析
本地 DDoS 來源分析 (境內攻擊)
Taipei
26.8b
2.0b
197.2m
124.7m
17.5b
367.0m
1.0b
全球 DDoS 來源分析 (境外攻擊)
2.5b
58.3b
27.3b
1.4b
986.7m
7.6b
22.9b
3.2b
5.4b
1.1b
3.1b
99.2b
4.4b
4.2b
311.1m
508.5m
3.4b
Leaflet
境內攻擊量
流量 (GB)
Sessions
境外攻擊量
12:00
12:20
12:40
12:50
5/23 (周二)
2017
時間


DDoS 警示 (GB / Hour)
100
DDoS 目的分析
本地 DDoS 來源分析 (境內攻擊)
Putian
莆田市
Quanzhou
泉州市
Taipei
1.2t
Hsinchu City
新竹市
110.4b
Hualien
Yonaguni
与那国町
全球 DDoS 來源分析 (境外攻擊)
18.8b
12.5b
境內攻擊量
2.5
2
1.5
1
0.5
流量 (GB)
12:00
5/23 (周二)
2017
境外攻擊量
8
6
4
2
5,000
4,000
3,000
2,000
Sessions
12:20
12:40
12:50
時間
Sessions
GB

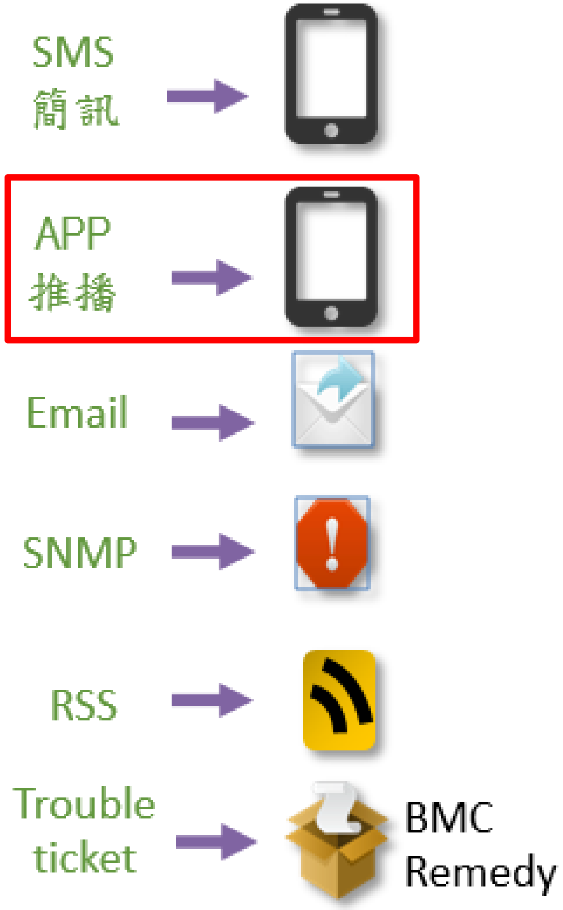
警訊即時通報



IP ⇕	Sources ⇕	EventCount ⇕	Events ⇕
192.168.63.23	eStreamer	18	Web Application Attack
192.168.12.58	cisco-smc	12	Data Exfiltration Suspect Data Los
172.16.1.8	eStreamer	8	Misc Activity
172.16.1.150	eStreamer	7	Attempted Administrator Privilege Gain Attempted User Privilege Gain
172.16.1.101	eStreamer	6	Attempted Information Leak
192.168.13.76	cisco-smc	6	Data Exfiltration Suspect Data Los
172.16.1.11	eStreamer	5	Misc Activity
192.168.23.240	eStreamer	5	A Network Trojan was Detected Misc Activity
192.168.63.98	cisco-smc	4	Data Hoarding
172.16.1.151	eStreamer	3	Attempted User Privilege Gain

資安防護戰情中心

內部探勘 Recon	異常行為 Bad Reputation	大量傳輸 Data Loss	殭屍網路 Botnet	惡意軟體 Malware	中繼站 Black List	勒索軟體 Ransomware
6	0	18	0	2	0	0
AMP端點 AMP Endpoint	**可疑軟體 Attempted**	**木馬 Trojan**	**政策違反 Policy Violation**	**IPS特徵碼 Signature**	**弱點掃描 Nessus Critical**	**PaloAlto威脅偵測 PaloAlto Threats**
0 %	36	2	4	0	18	7


SMS 簡訊 →

APP 推播 →

Email →

SNMP →

RSS →

Trouble ticket → BMC Remedy

不是唯恐天下不亂，

而是唯恐你以為天下太平。

Thank YOU