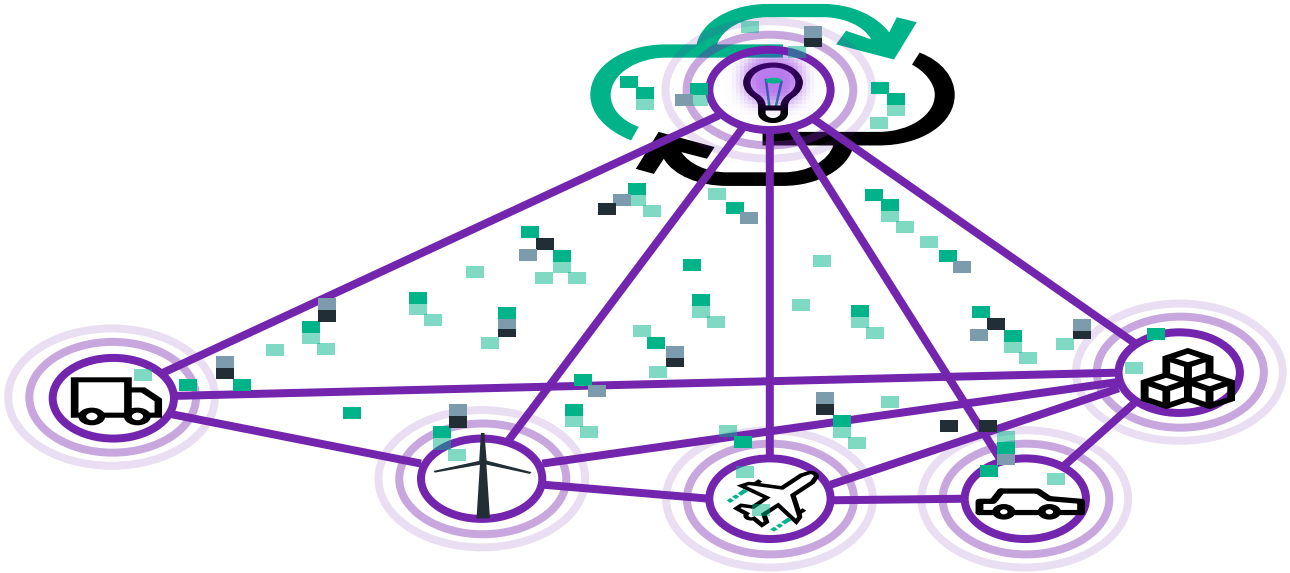
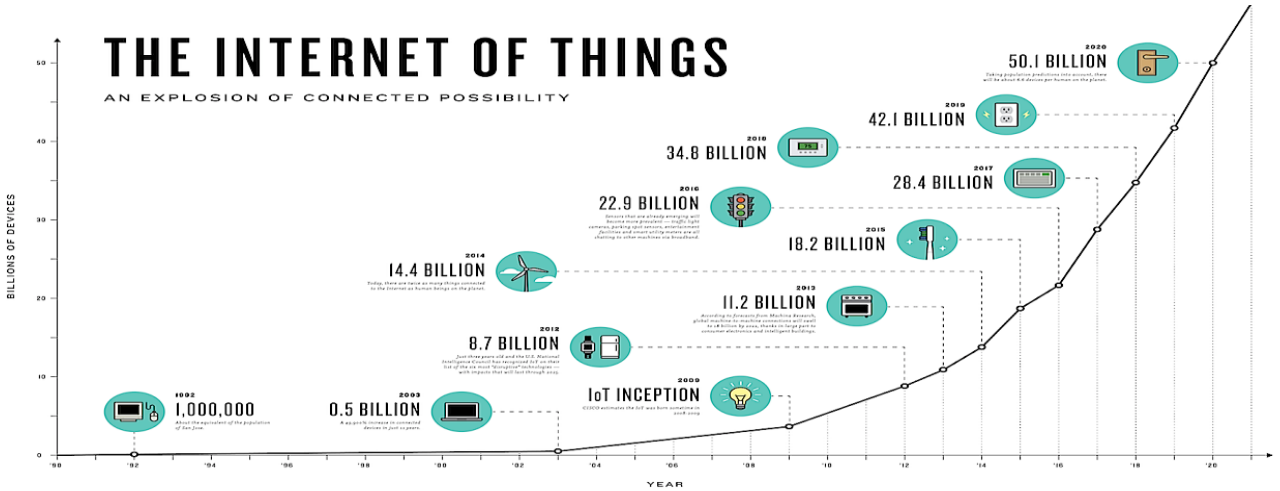
IoT補夢網

HPE 李柏厚 Bill Lee

什麼叫IoT就是Internet of Things(物聯網)





可以連上internet的設備及系統

Gartner預估在2020年有260億個設備連上物聯網

在物聯網上的資料流量

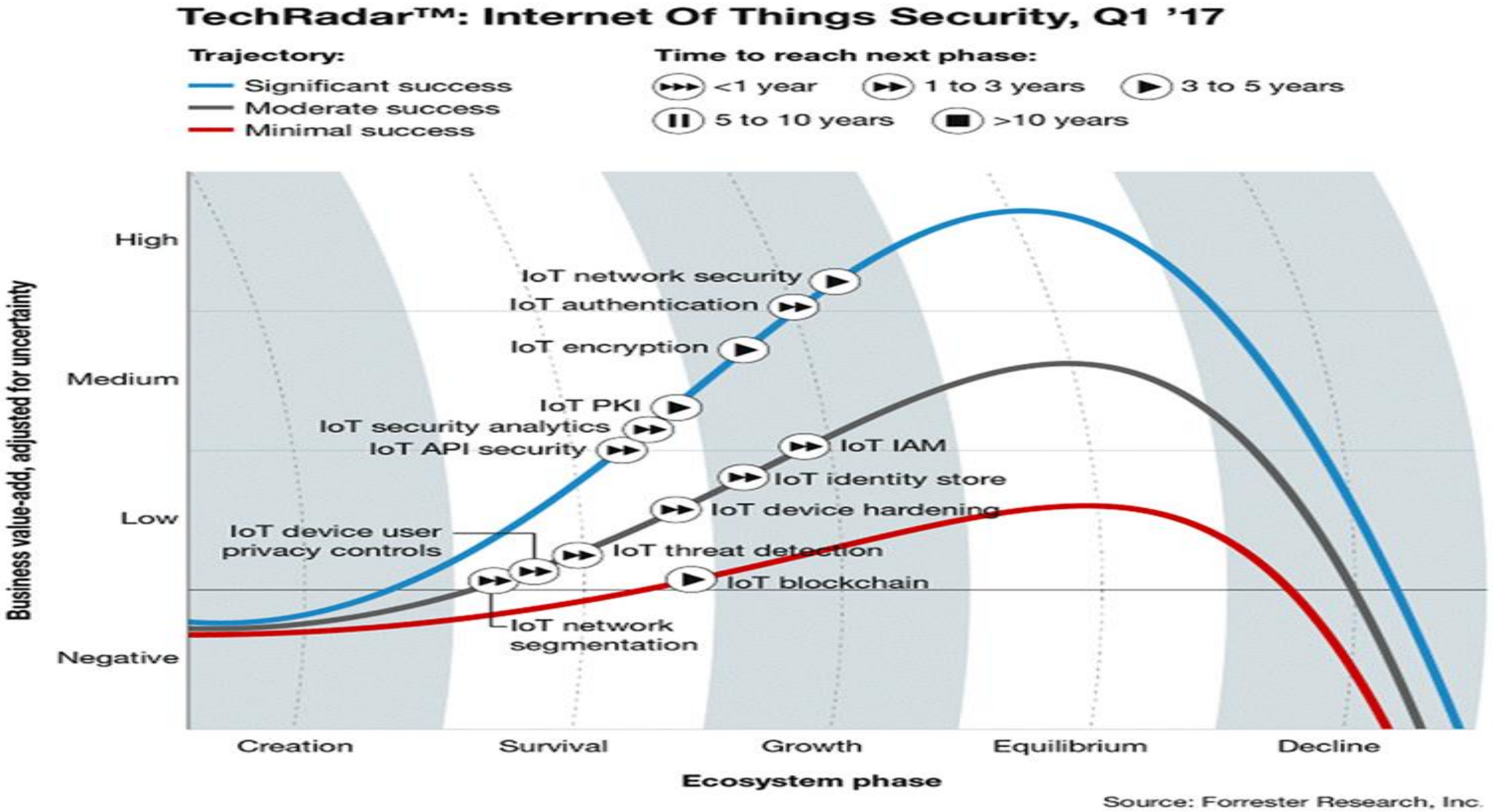
IDC預估在2020年整個IoT上的資料佔所有資料流量的10%

在物聯網的新的資料

商業、工程及科學等資訊

IoT架構特性

- IoT的硬体及軟体不一定有標準
- 端點設備可能cpu及可寫入的空間大小不一
- IoT設備可能有儲存客戶機敏資料
- 整個網路可能跨過幾個地理區域，甚至是國家
- 功能面的要求可能造成安全的忽略，例如認證


TechRadar™: Internet Of Things Security, Q1 '17
Trajectory:
Significant success
Moderate success
Minimal success
Time to reach next phase:
<1 year
1 to 3 years
3 to 5 years
5 to 10 years
>10 years
Business value-add, adjusted for uncertainty
High
Medium
Low
Negative
IoT network security
IoT authentication
IoT encryption
IoT PKI
IoT security analytics
IoT API security
IoT IAM
IoT identity store
IoT device hardening
IoT device user privacy controls
IoT threat detection
IoT blockchain
IoT network segmentation
Creation
Survival
Growth
Equilibrium
Decline
Ecosystem phase
Source: Forrester Research, Inc.

在物聯網架構及考量資安的點?

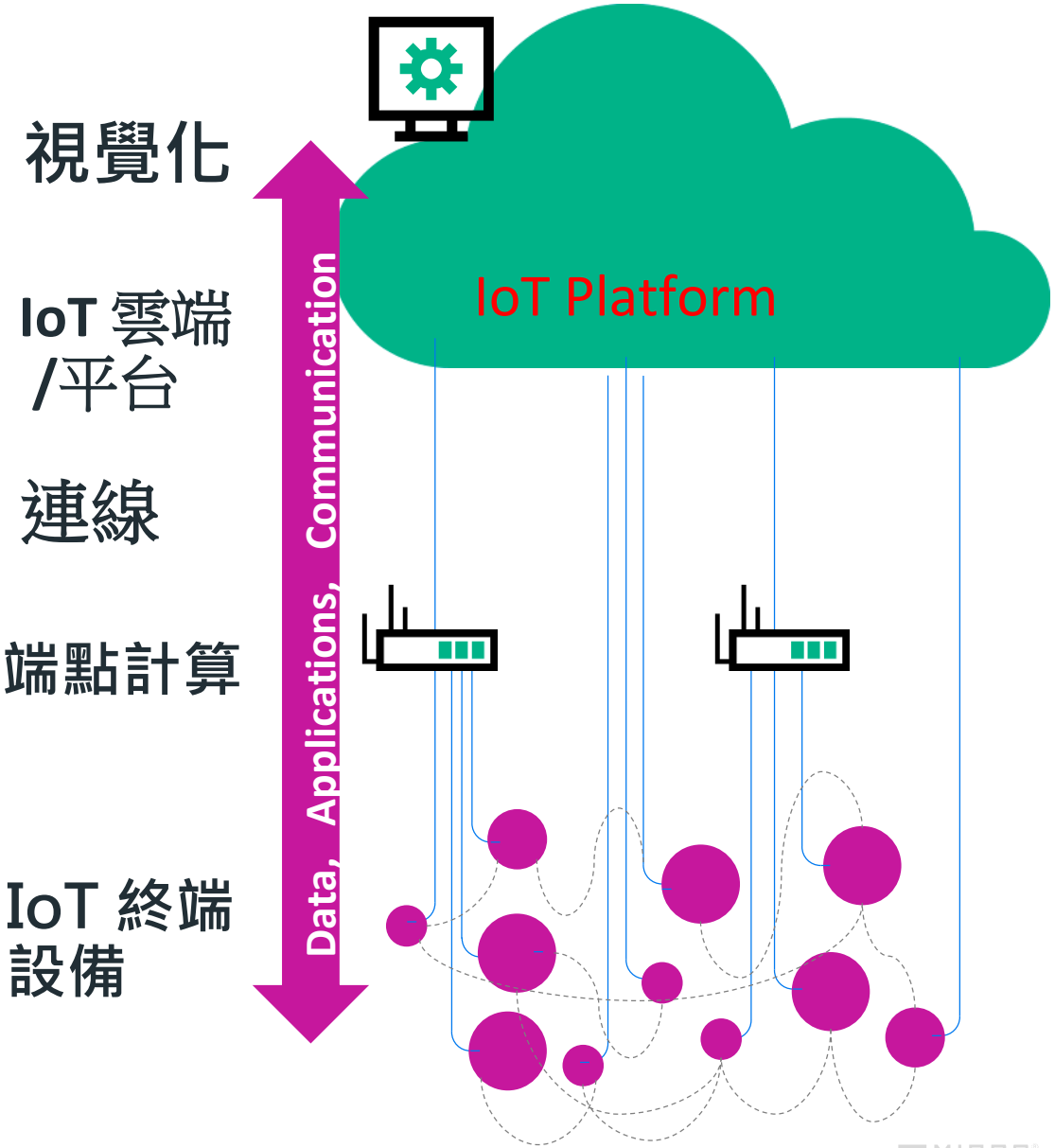
應用層-用於用視覺化的方式來讓管理者或來管理整個物聯網的運作

運作及控制IoT的架構-包含資料的儲存及大數據及機器學習做一個轉換。

連線層-用普遍，可靠及安全的連線方式來連接至端點或收集器的設備

收集器-主要是收集終端設備的資訊，例如是將運作的通訊協定(SCADA)轉成資訊的通訊協定(TCP/IP)，做資訊的擷取及轉換。

分散感應器及執行器-可能是行動或固定裝置，但常常連結於internet或private的網路，又稱M2M



在物聯網架構及考量資安的點?

破解端點及收集器

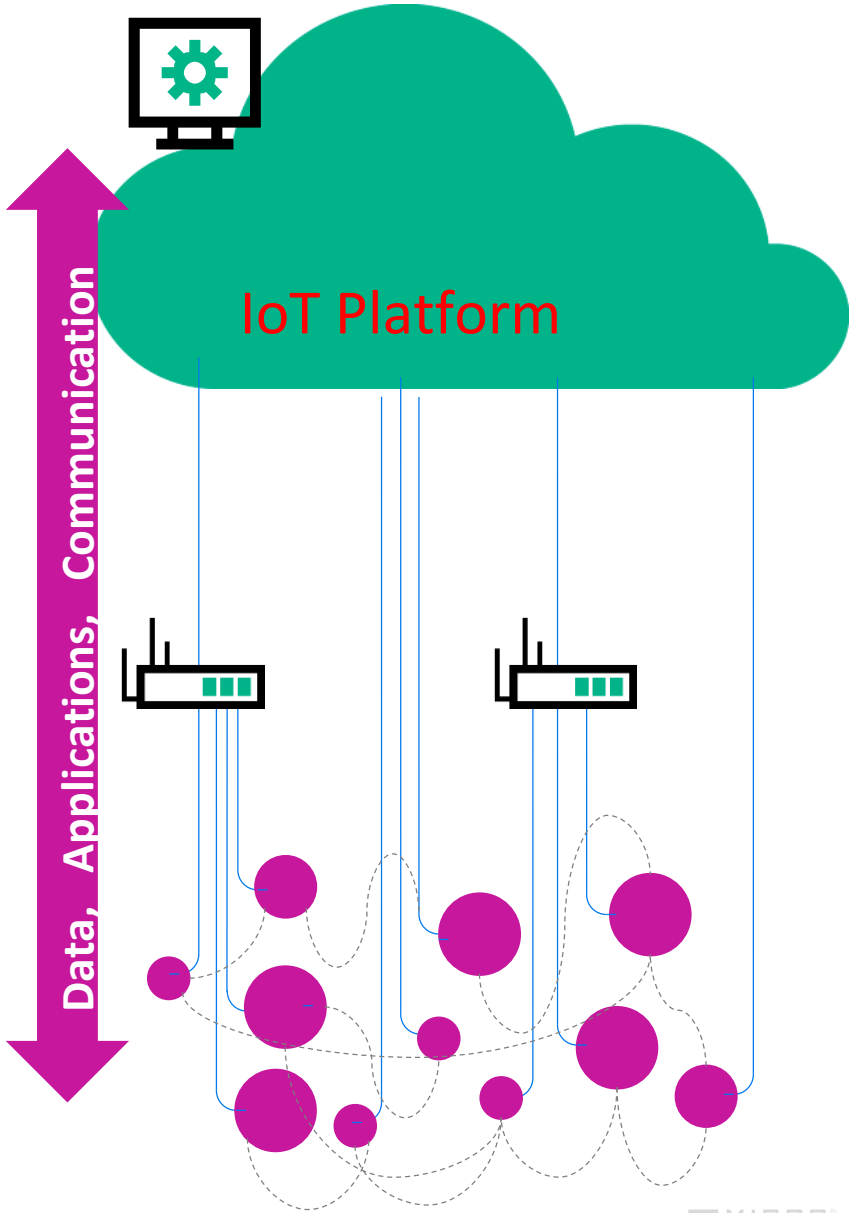
利用端點或收集器的弱點來安裝非經授權的人員，這會造成資料的外洩或是系統的運作問題。

入侵端點及收集器

利用設備上的軟体的弱點來入侵設備，尤其是那些較簡單或是沒有辦法即時修補的設備。

資料外洩

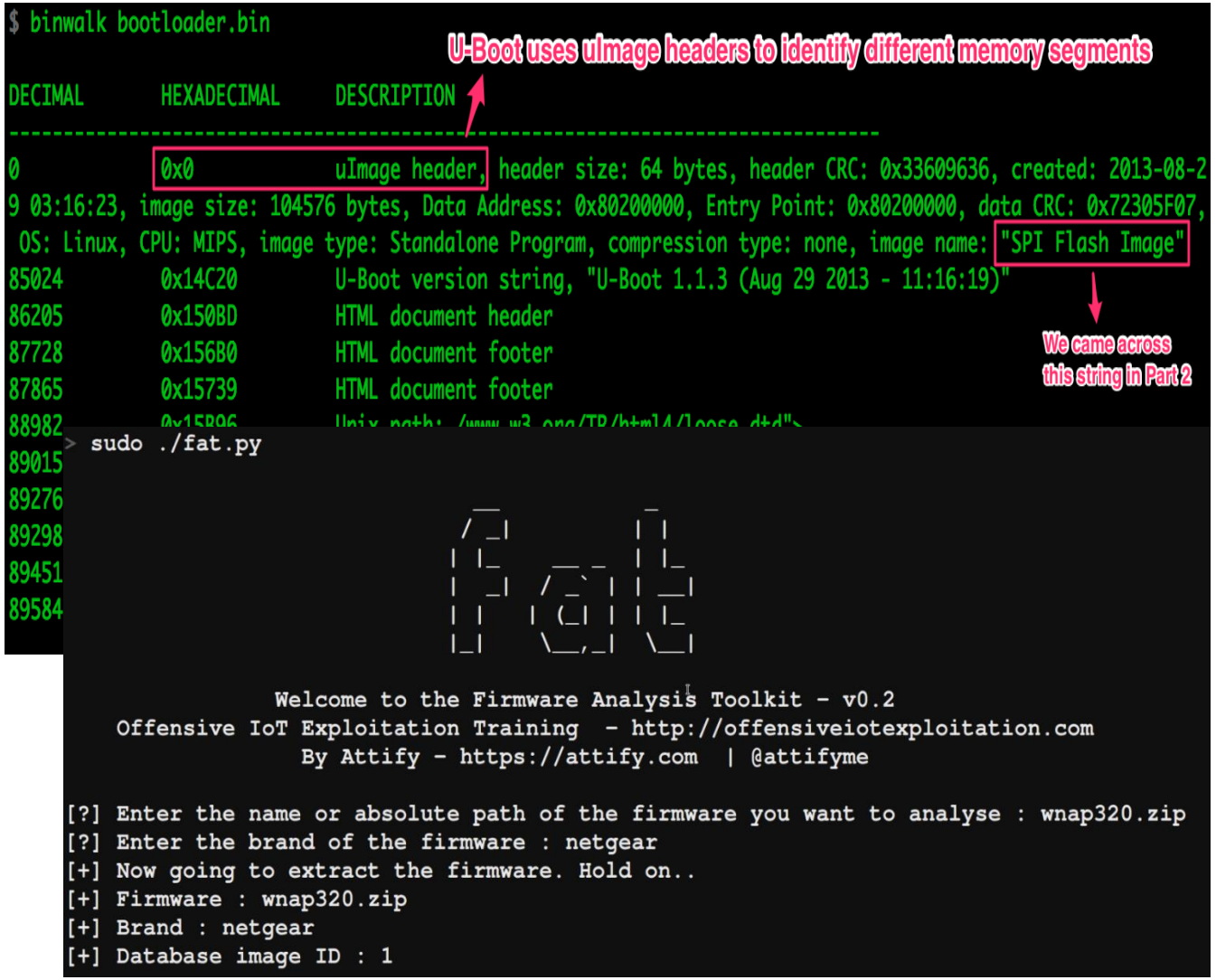
有些端點或收集器裏會有敏感性資料，例如帳號資訊。所以外洩這些資料會導致系統被入侵或個資外洩。



IoT入侵方式-Firmware(韌體)-逆向工程

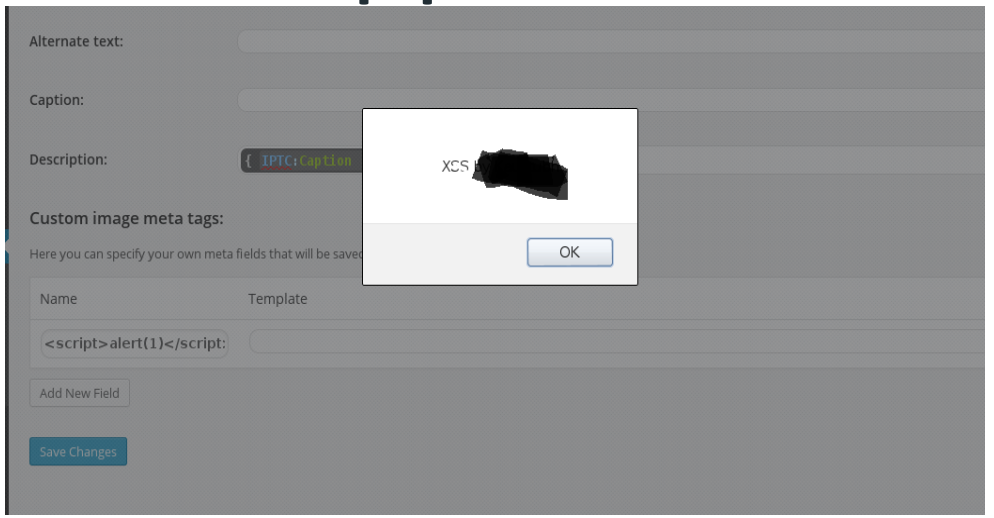
https://www.youtube.com/watch?v=A9ea9fllnME

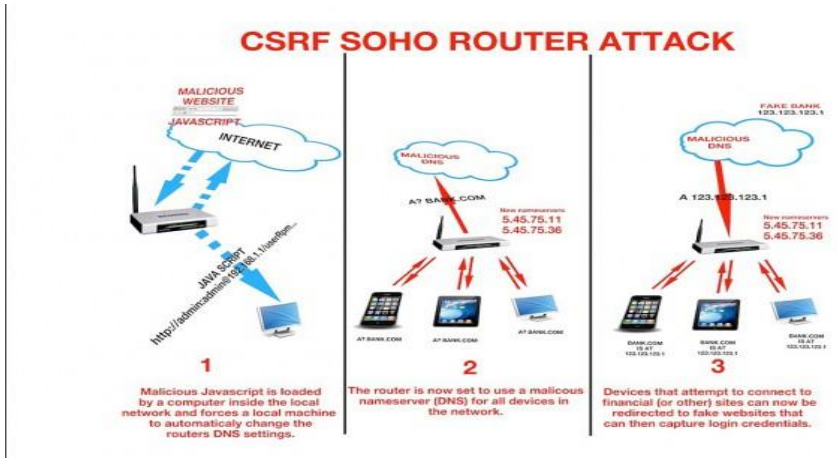
- Binwalk
- IDA Pro
- Firmware analysis toolkit



IoT入侵方式-利用Web界面做為進入點

- XSS-https://www.youtube.com/watch?v=iMSUb9wq-qo
- SQL injection
- CSRF
- Open source已知風險



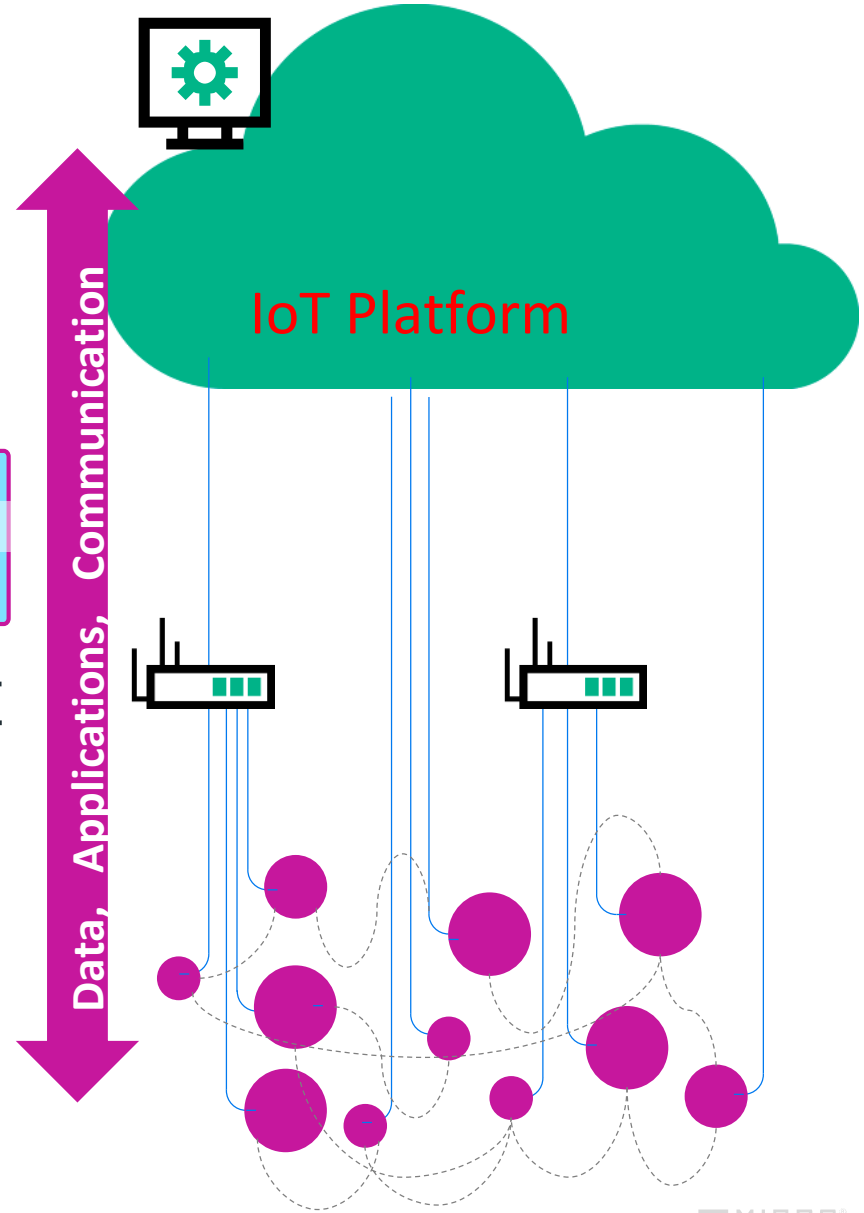


在物聯網架構及考量資安的點?

中間人攻擊(MitM)
攻擊者偵測出端點或收集器到平台之間的內容，讓整個IoT的系統造成問題。

阻斷式攻擊(DoS)
讓IoT的雲端服務如Web API或VPN不能提供服務。

未經授權存取
利用模擬授權的端點來對系統獲取資訊或取得管理權限。



網路服務商Dyn DDoS的攻擊事件

- **時間-2016/10/21**
- **事件過程**
  - 透過惡意軟体「Mirai」，利用 IPCAM、CCTV、DVR、IoT 裝置等系統對Dyn這家網路服務公司進行 DDoS 攻擊。
  - 事件是從10/21的早上7:00開始持續了兩個小時。造成上百萬的用戶無法上網。
- **問題主因**
  - 主要是他們使用的DVR已經被植入了Mirai而造成問題

思科Elastic Services Controller問題

- 事件時間-2018/2/27
- 問題原因
  - 使用開放源碼
  - 主要是可以繞過web的認證，使用空白字元來登入

資料來源:ITHOME

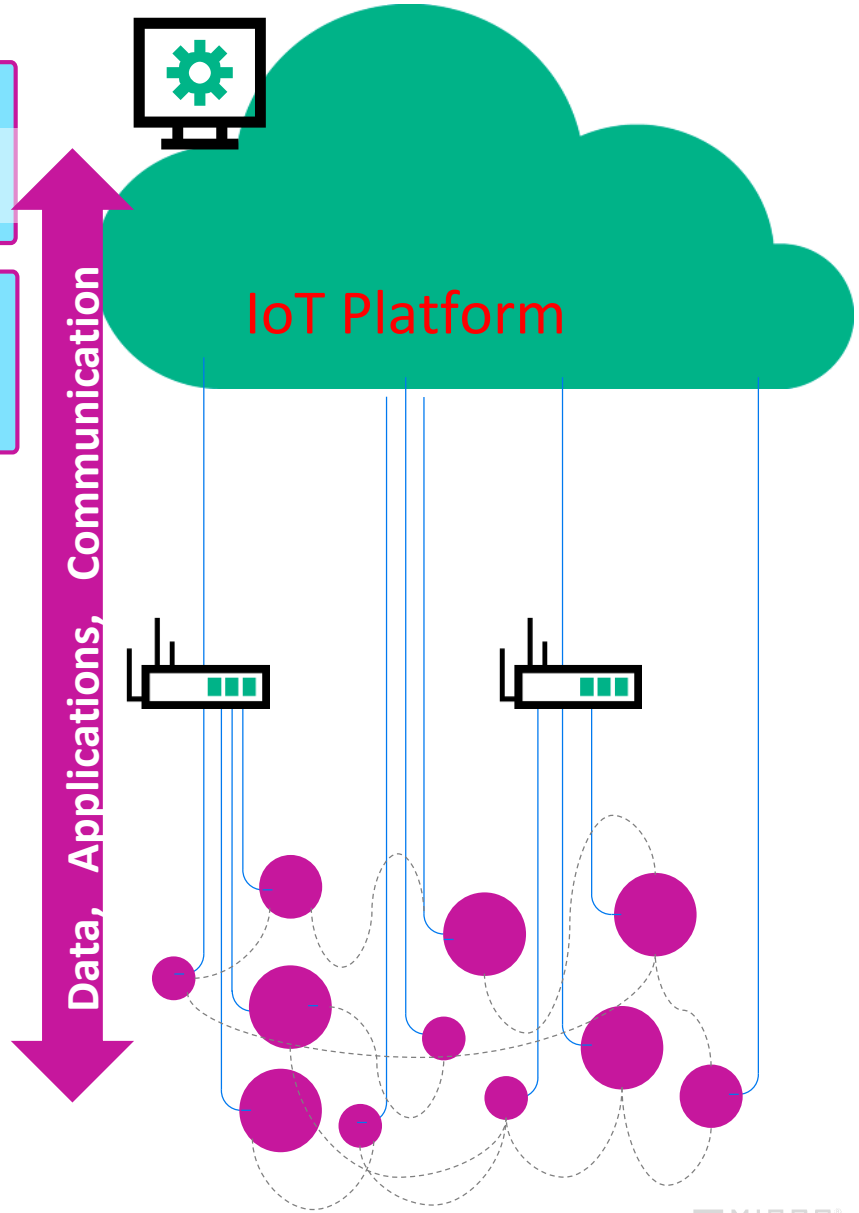
在物聯網架構及考量資安的點?

有問題的網站應用程式及API

這會造成DoS或是資料流失或是被攻擊者控管整個系統。這也是OWASP 10列出需要被保護的風險。

有目地的攻擊

攻擊者會選擇有漏洞的設備的IoT的廠商進行攻擊。就如APT的攻擊一般選擇有目的廠商做攻擊。



SCADA烏克蘭電網攻擊事件

- 時間-2015年12月
- 事件過程
  - 駭客攻擊了60座變電站，造成大規模的停電，這事件有人認為是俄羅斯主導
- 事件原因
  - 電力員工下載了惡意軟體”BlackEnergy”，然後駭客就利用軟体來切斷主控電腦及變電站連線。
  - 在電腦裏植入病毒，在同時駭客對電力公司的通話進行干擾，導致停電的居民無法和電力公司進行聯絡。

IoT問題發生主因

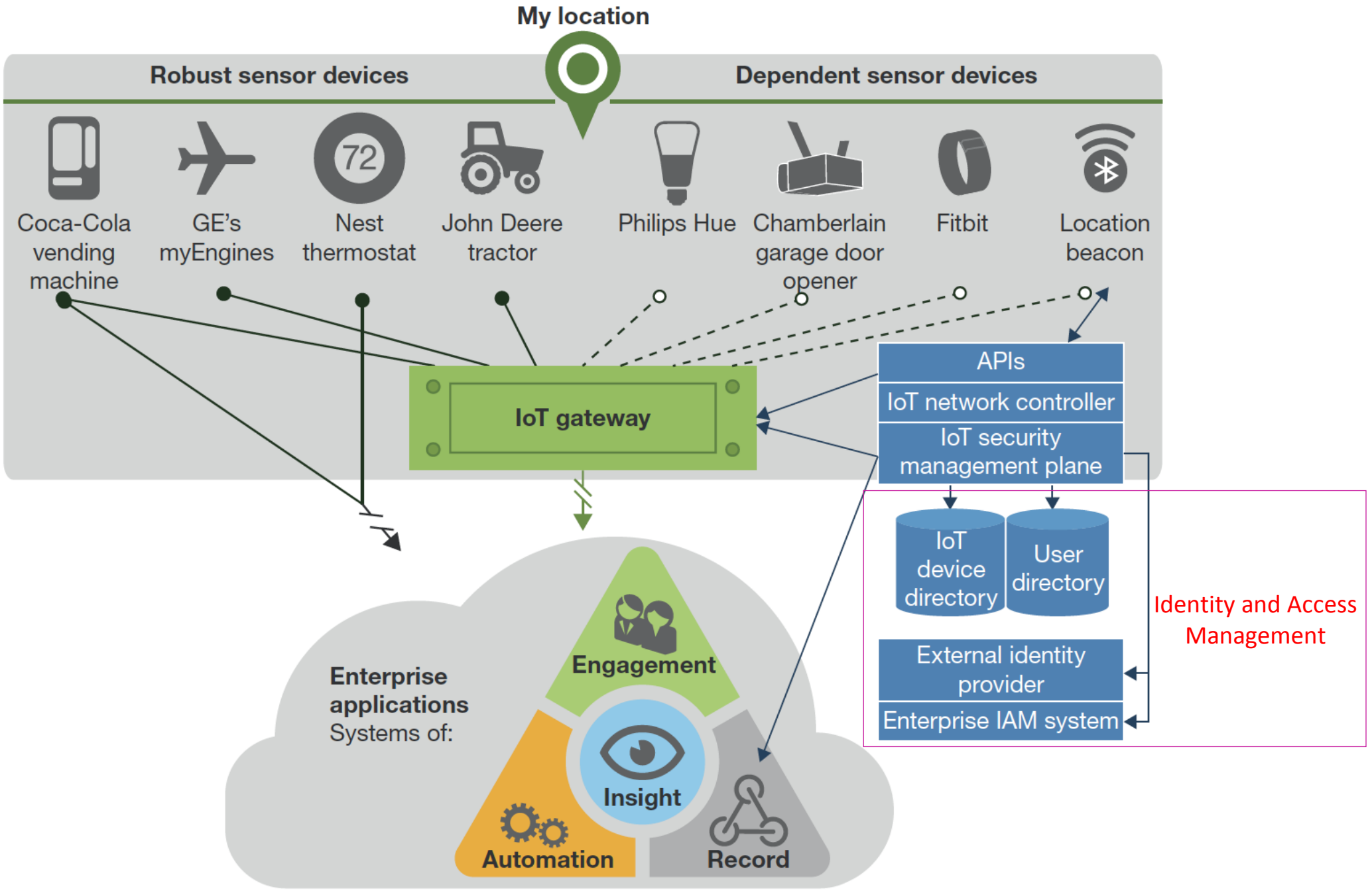
- **IoT設備安全性問題**
  - 確認連線的IoT設備是合法授權及經過嚴格認證。
  - 確保IoT設備本身沒有漏洞及安全。
  - 確保IoT的存取的控管及認證。
  - 確保IoT設備在各個連線上是否安全及加密。
- **IoT平台安全性問題**
  - 確保存取的控管及認證。
  - 確保儲存的資料安全，例如資料加密。

確保IoT安全可用到的技術

- **身份認證**
- **預防應用程式的問題**
  - 源碼掃描(白箱測試)
  - 網站滲透(黑箱測試)
- **資安事件稽核**
  - 非法攻擊
  - 合法人員的非法行為
- **加密**
  - 儲存資料加密
  - 連線加密
  - 應用程式加密

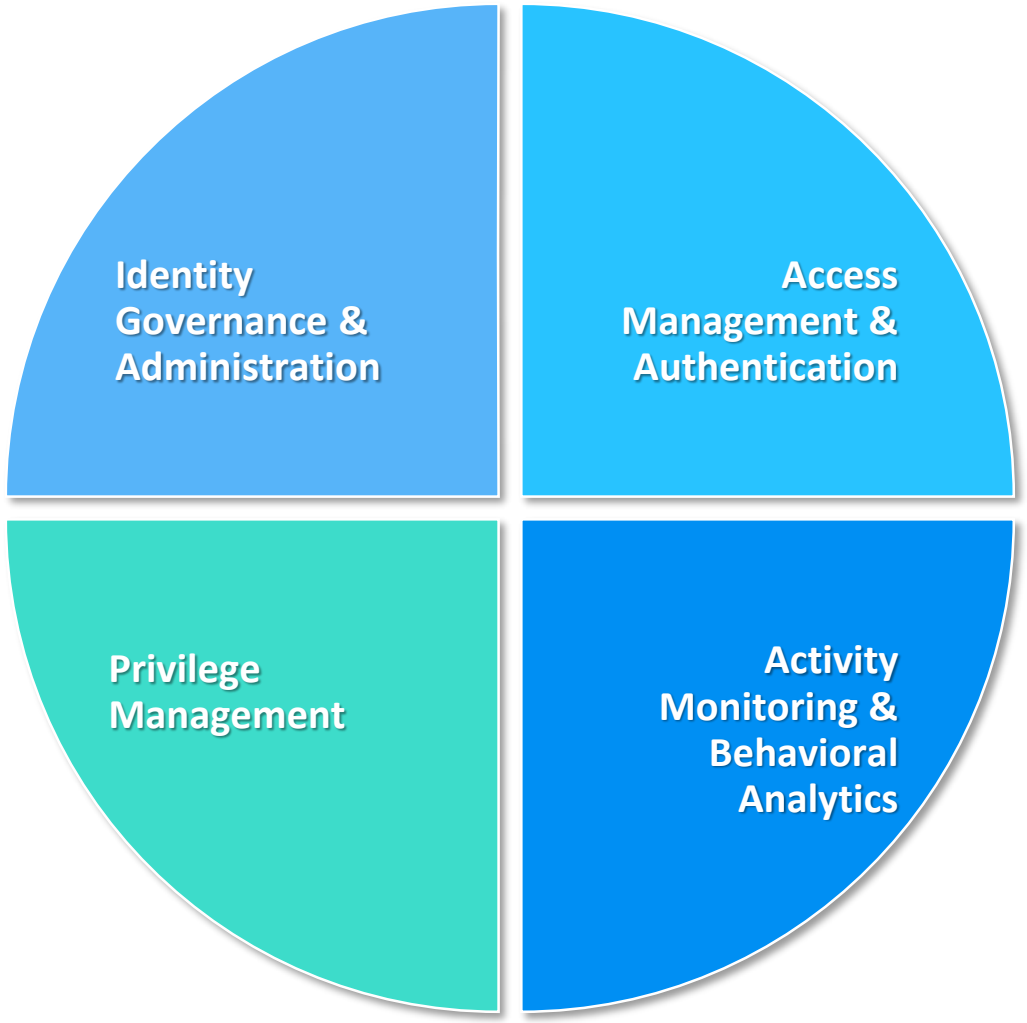
IoT身份驗證的重點

- **連線設備的確認**
- **提供對的人對的存取在對的時間**
- **認證的三因因素**
  - 使用者有什麼(Something you have)
  - 使用者知道什麼(Something you know)
  - 使用者之生物辨識(Something you are)
- **認證的技術**
  - 挑戰及回應
  - 一次性密碼
  - 憑證
  - 帳號及密碼
- **認證架構**
  - 先集中再依狀況來做適當認證設計

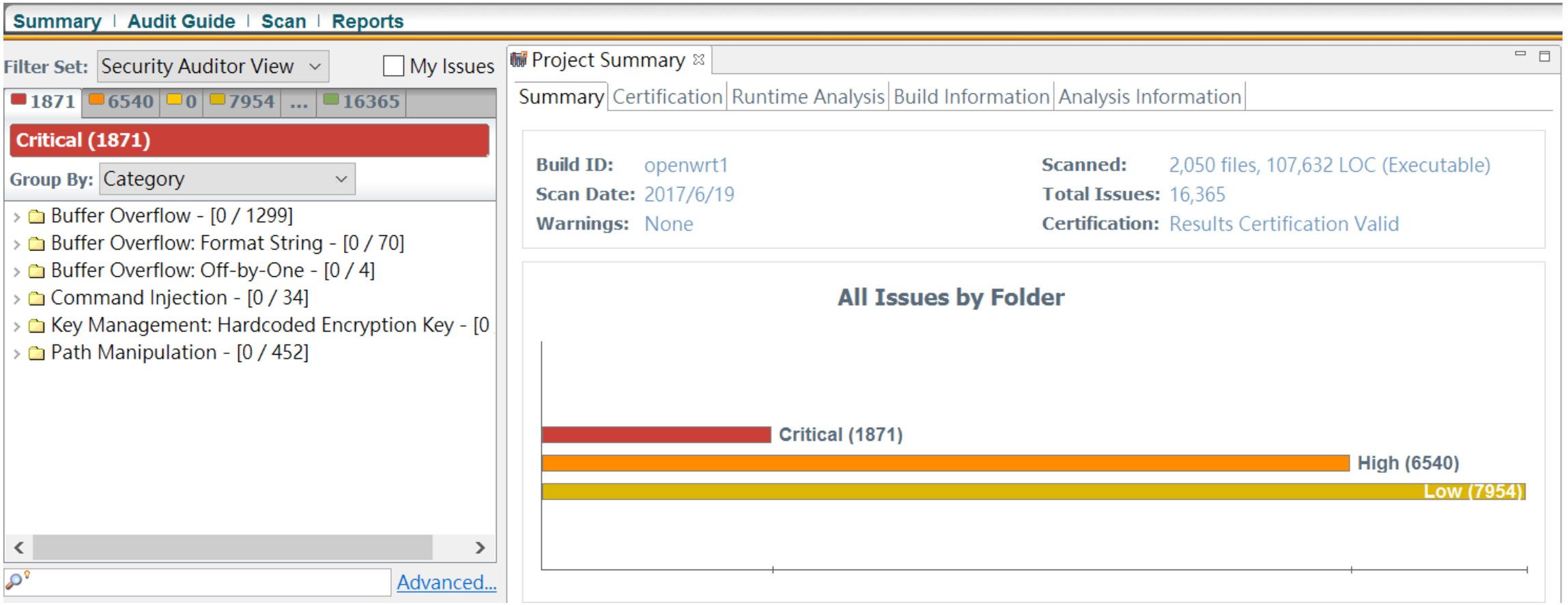


Source: "The Future Of IoT Gateways: Evolving To Enterprise Grade In 2016" Forrester report

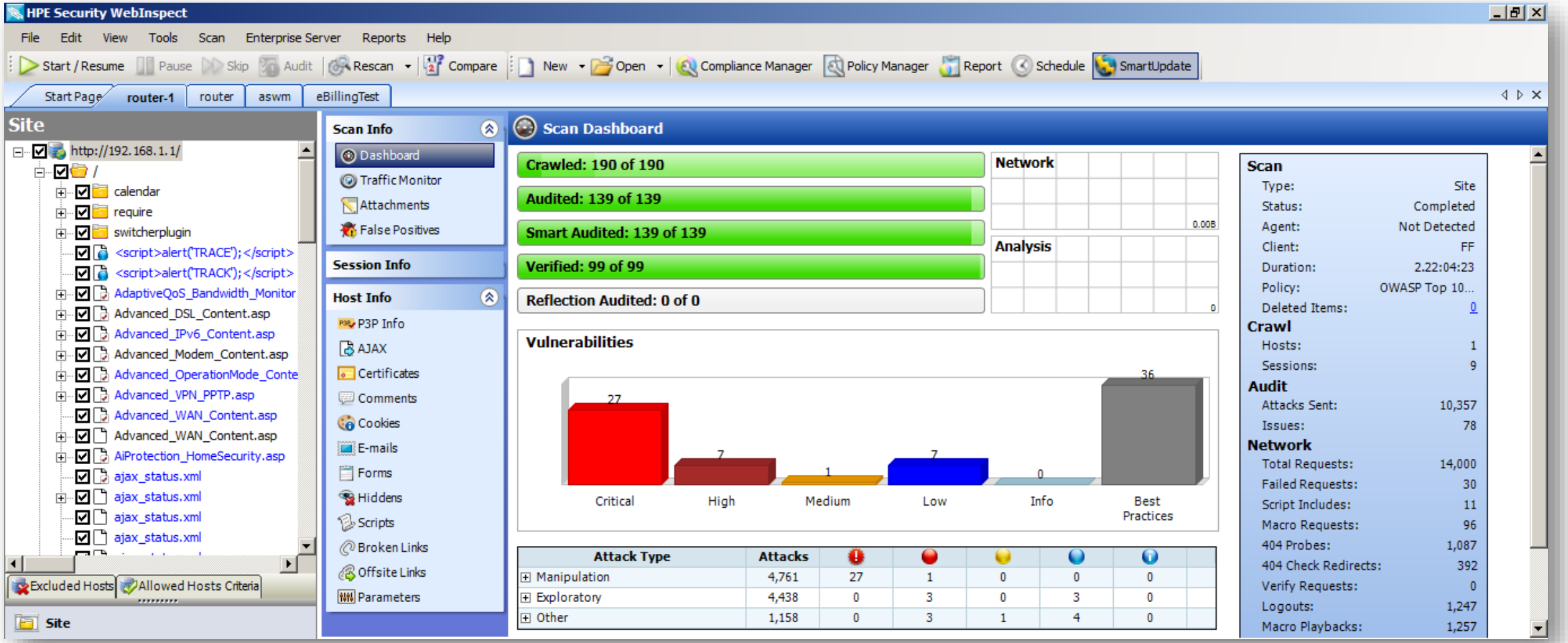
Simplicity Through Intelligence



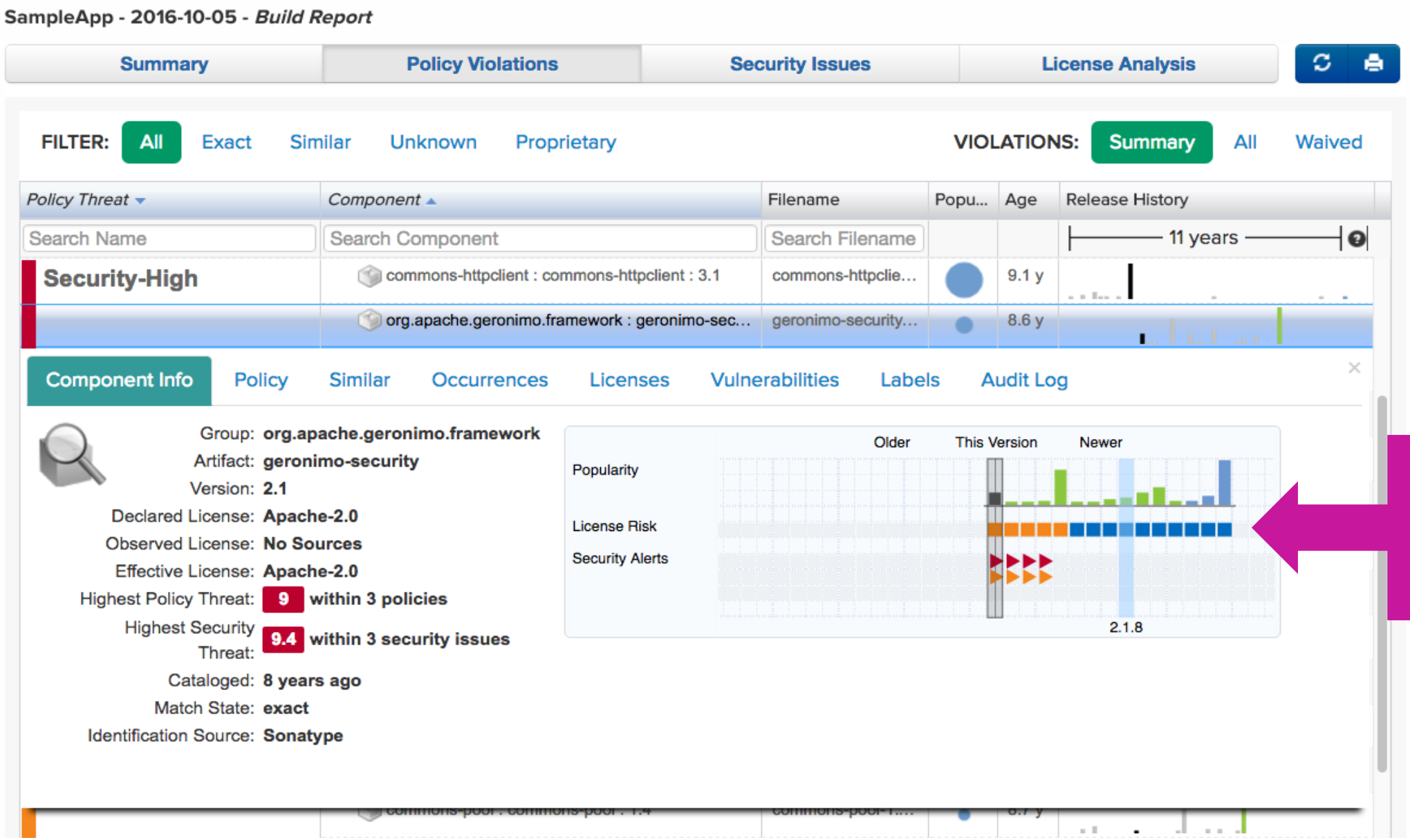
預防應用程式的問題-(白箱)-OpenWRT



預防應用程式的問題-(黑箱)-wireless router



開放源碼檢查(已知問題)

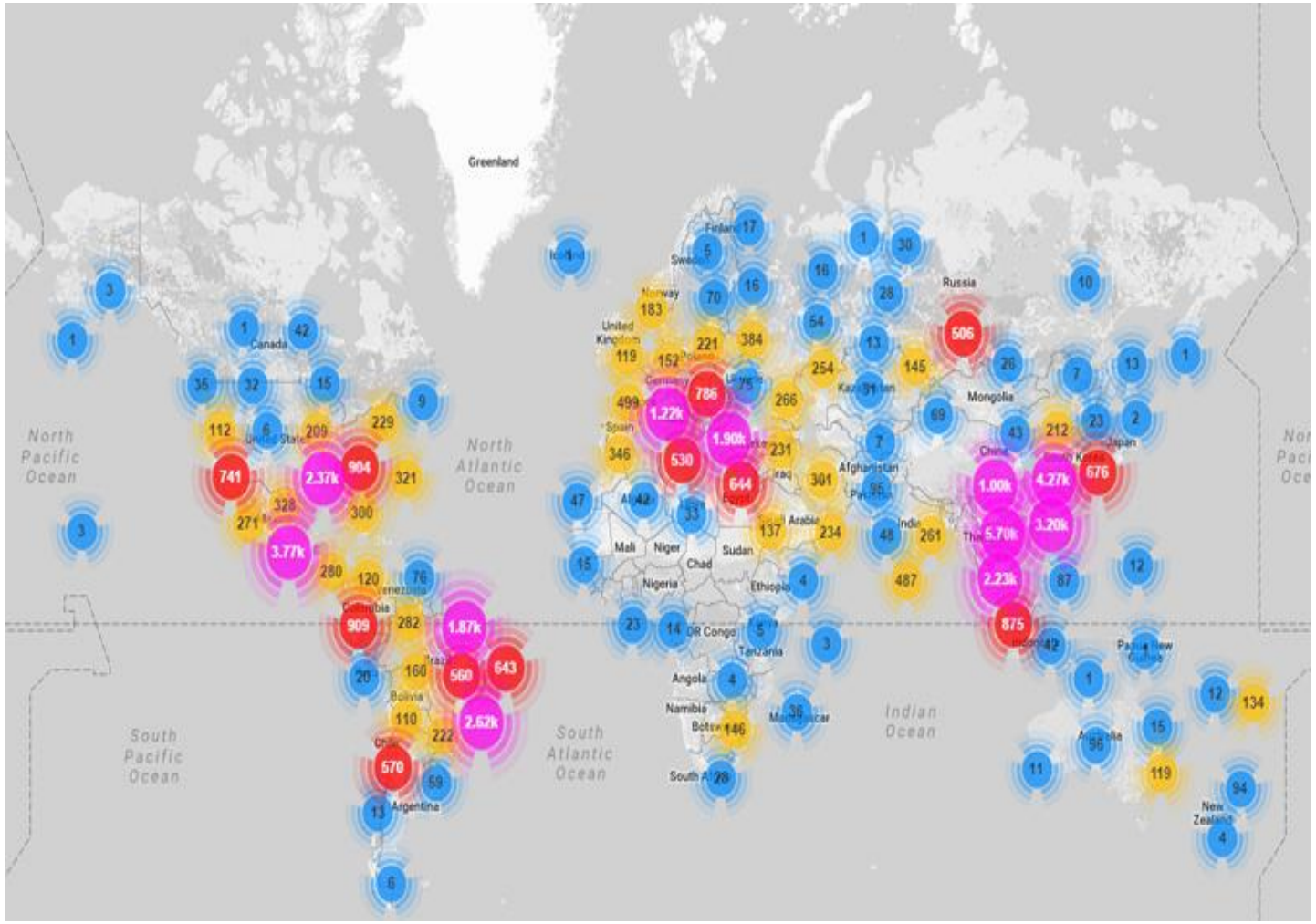


新版本上沒有風險

IoT事件稽核– Mirai Botnet

```
log /home/vac/logs/vac.log-last | egrep "pps\|.....
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ /|/g" | cut -f
1,2,3,7,8,10,11 -d '|' | sed "s/.........bps/Gbps/" | sed
"s/......pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g
rep "gone" | sed "s/gone|//"
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps
Sep|18|11:17:02|tcp_ack|19Mpps|224Gbps
Sep|18|11:44:17|tcp_ack|19Mpps|227Gbps
Sep|18|19:05:47|tcp_ack|66Mpps|735Gbps
Sep|18|20:49:27|tcp_ack|81Mpps|360Gbps
Sep|18|22:43:32|tcp_ack|11Mpps|136Gbps
Sep|18|22:44:17|tcp_ack|38Mpps|442Gbps
Sep|19|10:13:57|tcp_ack|10Mpps|117Gbps
Sep|19|11:53:57|tcp_ack|13Mpps|159Gbps
Sep|19|11:54:42|tcp_ack|52Mpps|607Gbps
Sep|19|22:51:57|tcp_ack|10Mpps|115Gbps
Sep|20|01:40:02|tcp_ack|22Mpps|191Gbps
Sep|20|01:40:47|tcp_ack|93Mpps|799Gbps
Sep|20|01:50:07|tcp_ack|14Mpps|124Gbps
Sep|20|01:50:32|tcp_ack|72Mpps|615Gbps
Sep|20|03:12:12|tcp_ack|49Mpps|419Gbps
Sep|20|11:57:07|tcp_ack|15Mpps|178Gbps
Sep|20|11:58:02|tcp_ack|60Mpps|698Gbps
Sep|20|12:31:12|tcp_ack|17Mpps|201Gbps
Sep|20|12:32:22|tcp_ack|50Mpps|587Gbps
Sep|20|12:47:02|tcp_ack|18Mpps|210Gbps
Sep|20|12:48:17|tcp_ack|49Mpps|572Gbps
Sep|21|05:09:42|tcp_ack|32Mpps|144Gbps
Sep|21|20:21:37|tcp_ack|22Mpps|122Gbps
Sep|22|00:50:57|tcp_ack|16Mpps|191Gbps
You have new mail in /var/mail/root
```

2016-09-21 DDoS vis Flooding, DNS AMP and GRE Flooding Attack

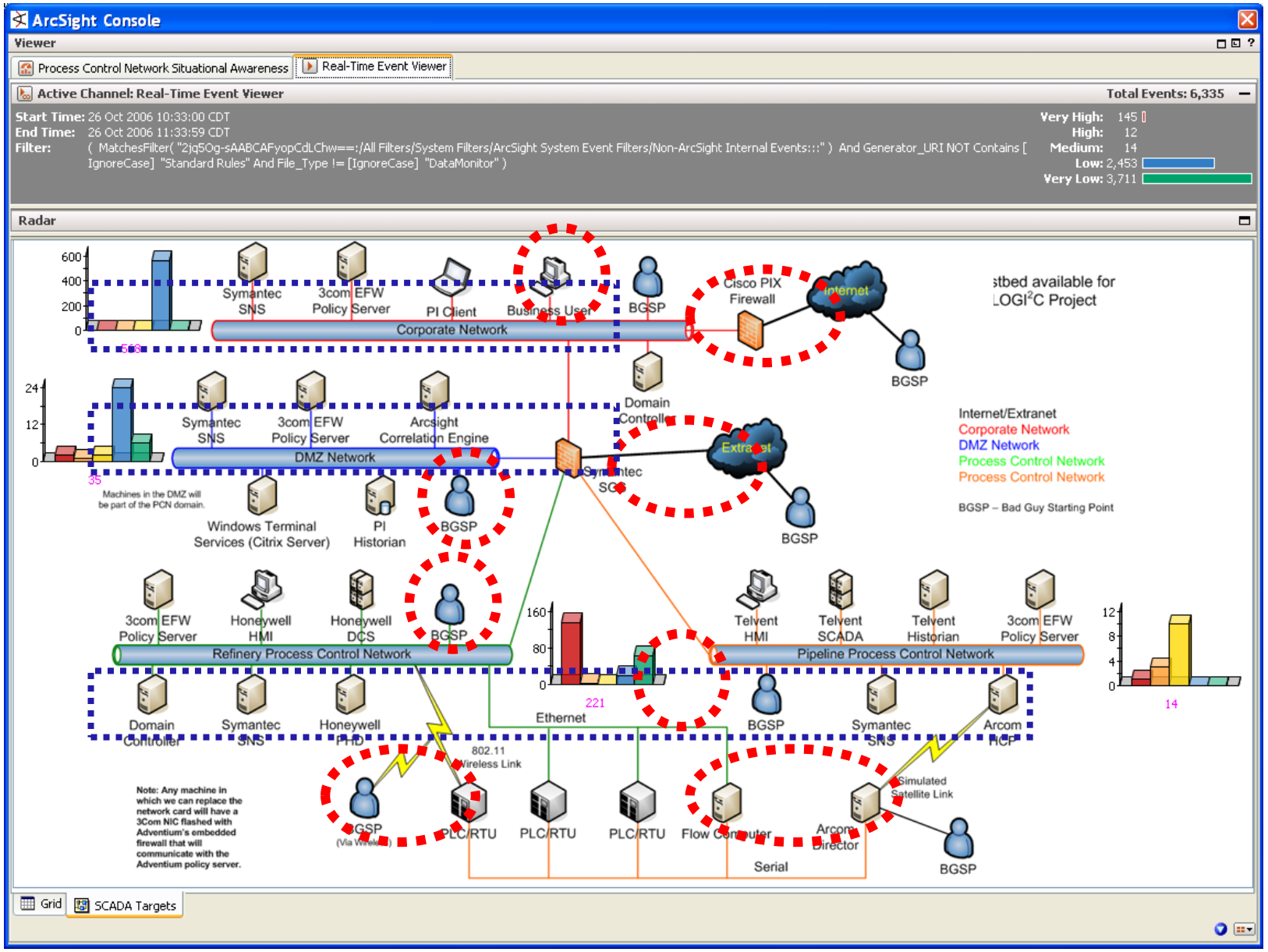


49,657 unique IPs which hosted Mirai-infected devices

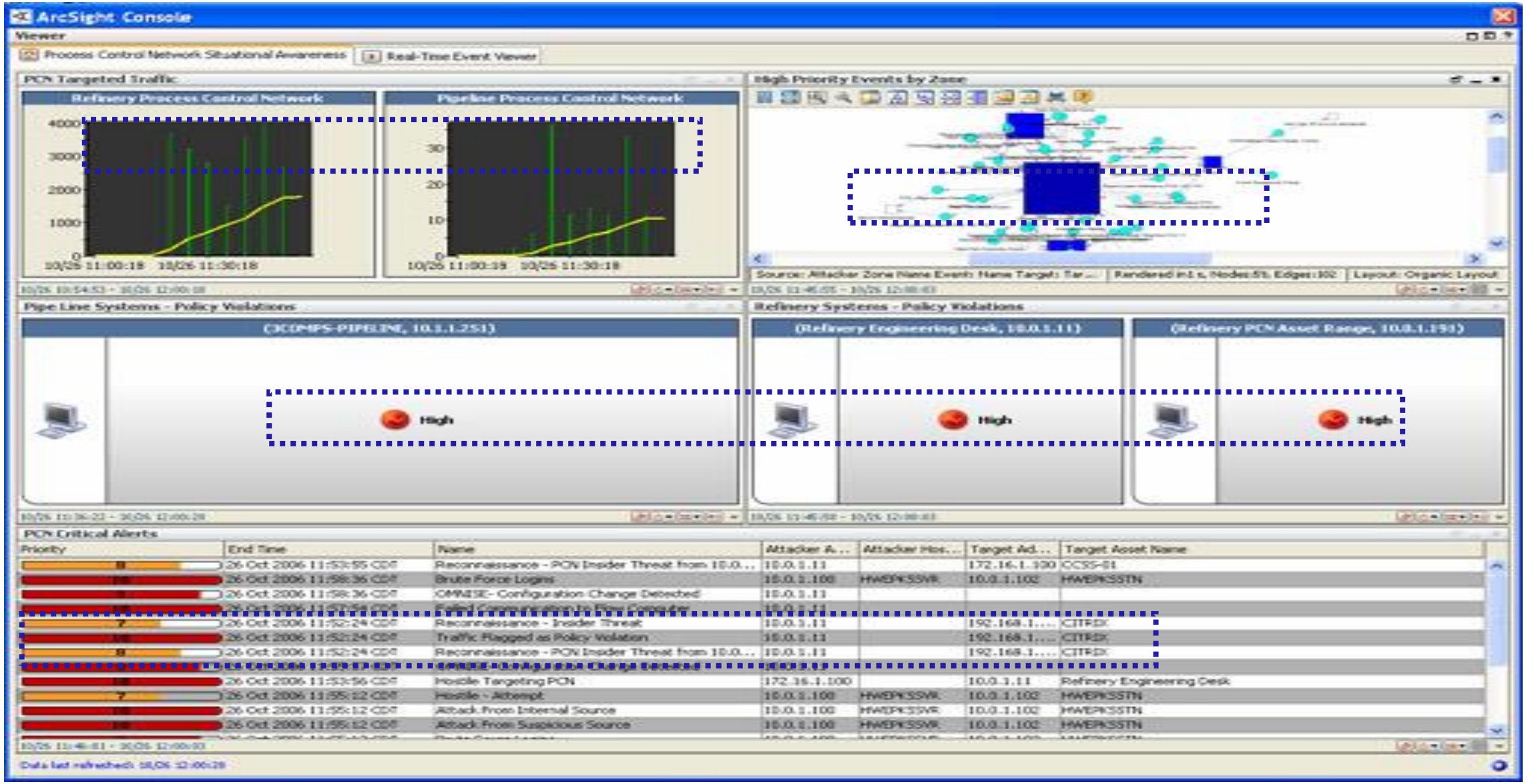
SCADA網路監控

企業及控制系統監控

- 攻擊因素
  - 內部網路
  - 外部網路
  - 無線網路
  - 衛星網路
- 企業網路狀況
- DMZ狀況



SCADA網路監控-案例



合法人員的非法行為-使用者行為分析技術

+1 頻率偏離值

+1 事件稀有度

+1 數量偏離值

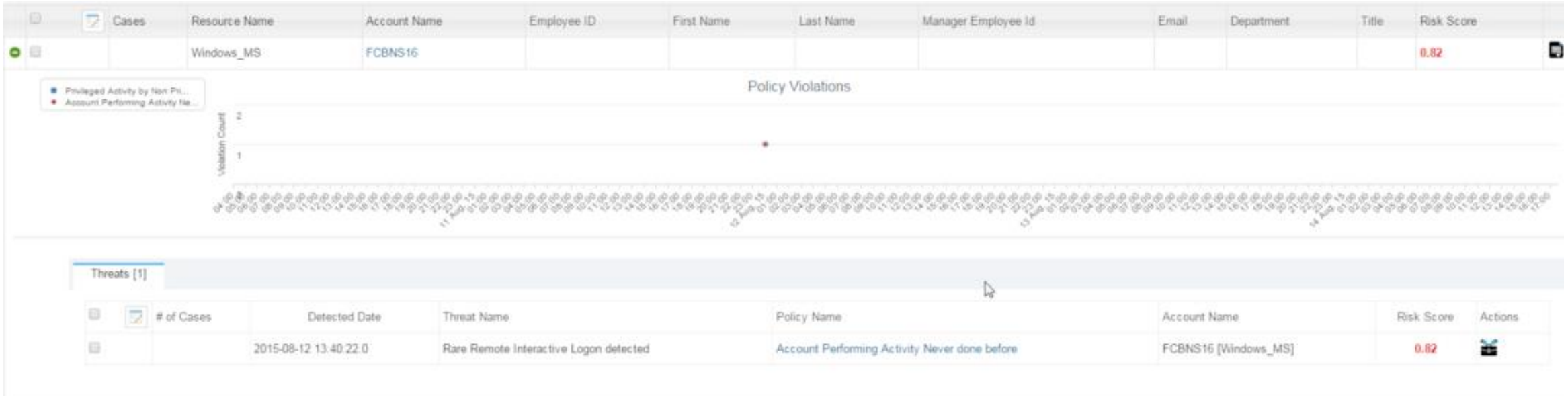
+1 同儕比較

可移活動與交易

可疑帳戶使用行為

可疑系統使用行為

合法人員非法行為案例 – 用戶進行從未見過的遠端登入行為



Cases	Resource Name	Account Name	Employee ID	First Name	Last Name	Manager Employee Id	Email	Department	Title	Risk Score
	Windows_MS	FCBNS16								0.82

Policy Violations

Threats [1]

# of Cases	Detected Date	Threat Name	Policy Name	Account Name	Risk Score	Actions
	2015-08-12 13:40:22.0	Rare Remote Interactive Logon detected	Account Performing Activity Never done before	FCBNS16 [Windows_MS]	0.82	

Case ID	Threat Indicator	Transaction	Event Date/Time	Datasource	Resource Name	Account	Employee Id	First Name	Last Name	Raw Score	Network Address
	Rare Remote Interactive Logon detected	Message: An account was successfully logged on	Fri Jul 31 18:15:34 EDT 2015	Windows_MS	Windows_MS	FCBNS16				0.82	10.52.140.33

Check Name	Frequency	Baseline	Raw Score	Generated Date		
Account performing activity never conducted before	1	0	0.82	2015-08-12 13:40:22.0	View Violations	Number of Days in the resource 10

ComputerName	EventCode	Message	TargetAccount	TargetAccountDomain	LoginType	SourcePort	Account Name	Network Address	Last Performed Date/Time	Geolocation		Frequency
										Computed	Commercial	
TORKBNS4.bns.bns	4624	An account was successfully logged on			10	1561	FCBNS16	10.52.140.33	Fri Jul 31 18:15:34 EDT 2015			1

應用程式的加密

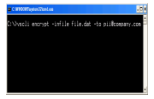
HSM

HPE SecureData
Virtual Appliance(s)

Management
Console

Authentication &
Authorization Systems

HPE SecureData
Web Services API



HPE SecureData
Command Lines

HPE SecureData
SimpleAPI
(C, Java, C#, .NET)

HPE
SecureData
Native UDFs

HPE SecureData
z/Protect, z/FPE

Partner
Integrations

SaaS & PaaS Apps
Saleforce.com

Data Protection and Masking Services

Business Applications, Data stores and Processes

Custom
Applications

Production
Databases

Payment
Devices

ETL & Data
Integration
Suites

3rd Party
Applications

Teradata
& Hadoop

HPE Nonstop
Applications &
Databases

Cloud
Broker
Gateways

Mainframe
Applications &
Databases

Web
Applications

MICRO FOCUS

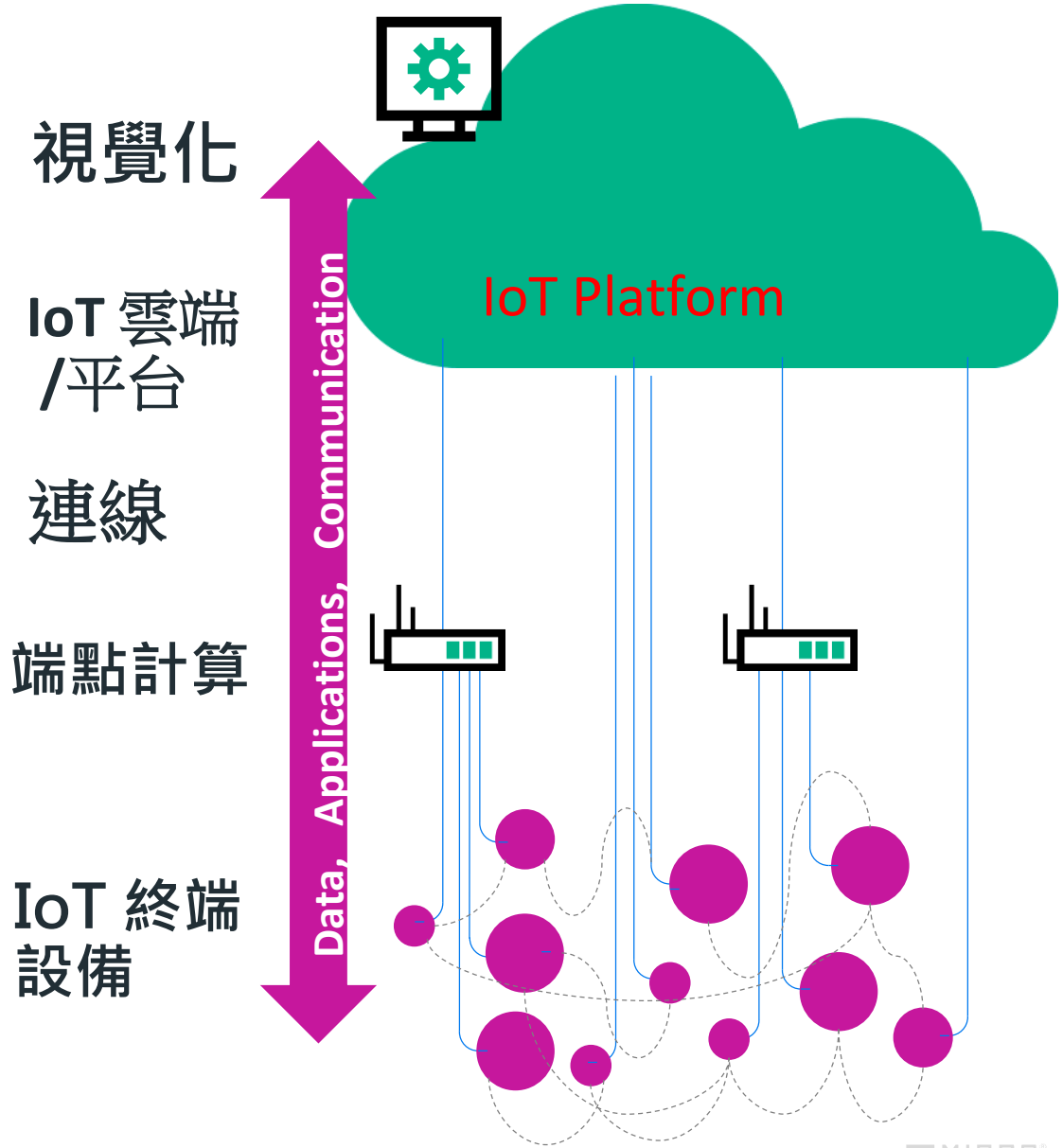
Microfocus產品對應

Arcsight(事件及非法人員監控)

Fortify(應用程式的安全檢測)

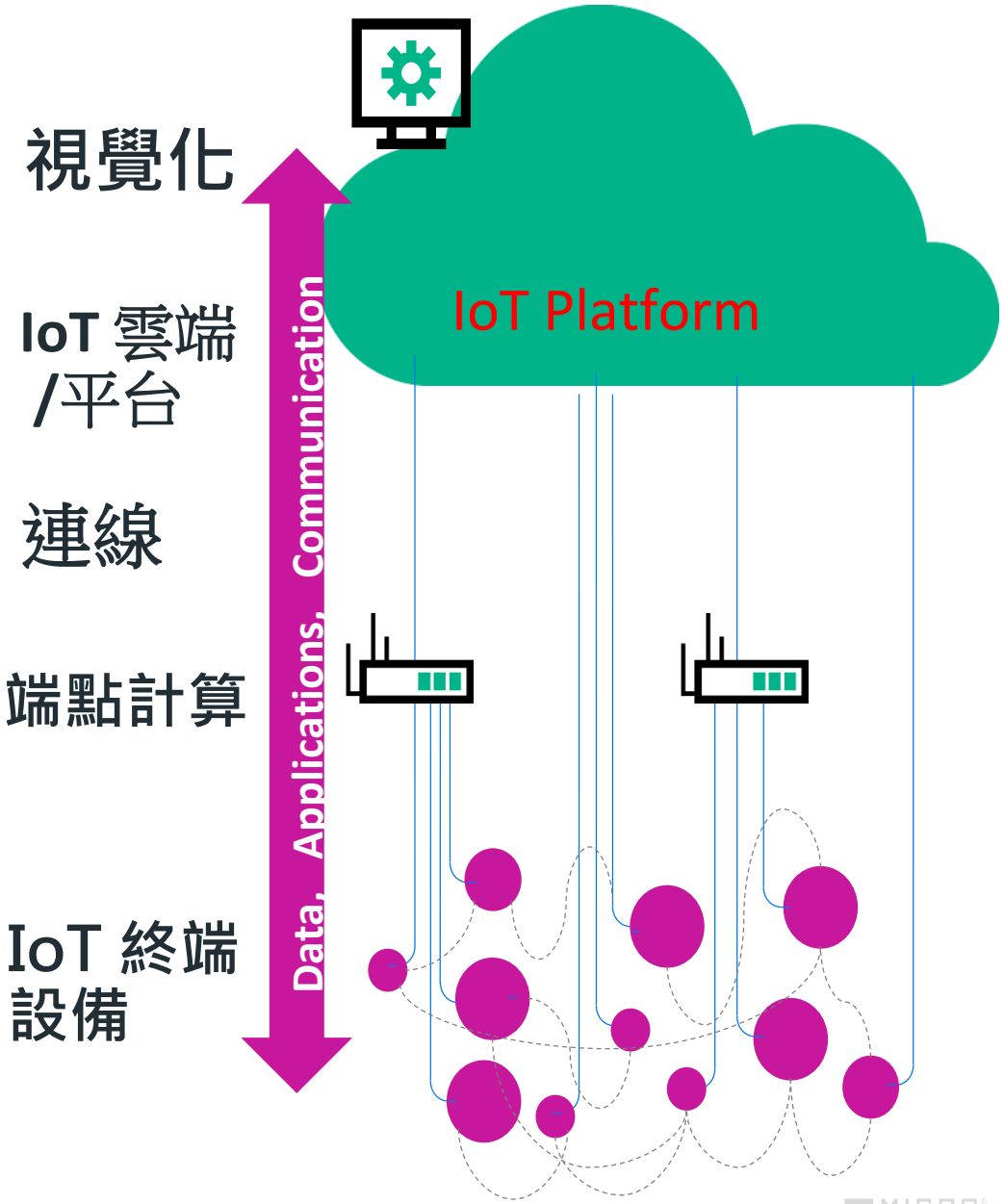
DataSecure(應用程式及資料加密)

IAM(認證管理平台)



Microfocus資安產品介紹

產品方案	應用程式	資料	連線
ArcSight	事件交叉及資安事件通知(ArcSight Data Platform, ESM – Security Information and Event Management, AppView) 資安分析 (ArcSight Interactive Discovery, DNS Malware Analytics, User Behavior Analytics)		
Fortify	源碼掃描 (Source Code Scanning) 網站掃描 (Black-Box Scanning of Web-Applications) 即時應用程式及網站保護-(RASP)		
IAM	登入認證 設備認證 認證管理		
Voltage	**端點對端點的保護敏感資料**-資料遮罩、格式保留加密技術及記號化等技術		
Atalla	Enterprise Secure **Key Management** (ESKM – Public Key Infrastructure)		



Thank you.

www.microfocus.com