AWS SUMMIT

從雲到端，打造安全的物聯網

Trend Micro IoT Security

Peter Yang, Sr. Product Manager

June 7th 2017

amazon web services

趨勢科技

TREND MICRO™

趨勢科技

- Founded in 1989 (28 years), IT security dedicated company
- 5,258 employees, cover 30 countries, 60% (3,300+) are engineers
- 500,000 enterprise customer and 155 million endpoints globally
- >$1 billion annual sales
- Founded in U.S. Headquartered in Japan
- Tokyo Exchange Nikkei Index (4704) | >$5 billion market cap
- Customers include 45 of top 50 global corporations, and 100% of the top 10:

Auto

Telecom

Banks

Oil

Gartner Magic Quadrant for Endpoint Protection Platforms

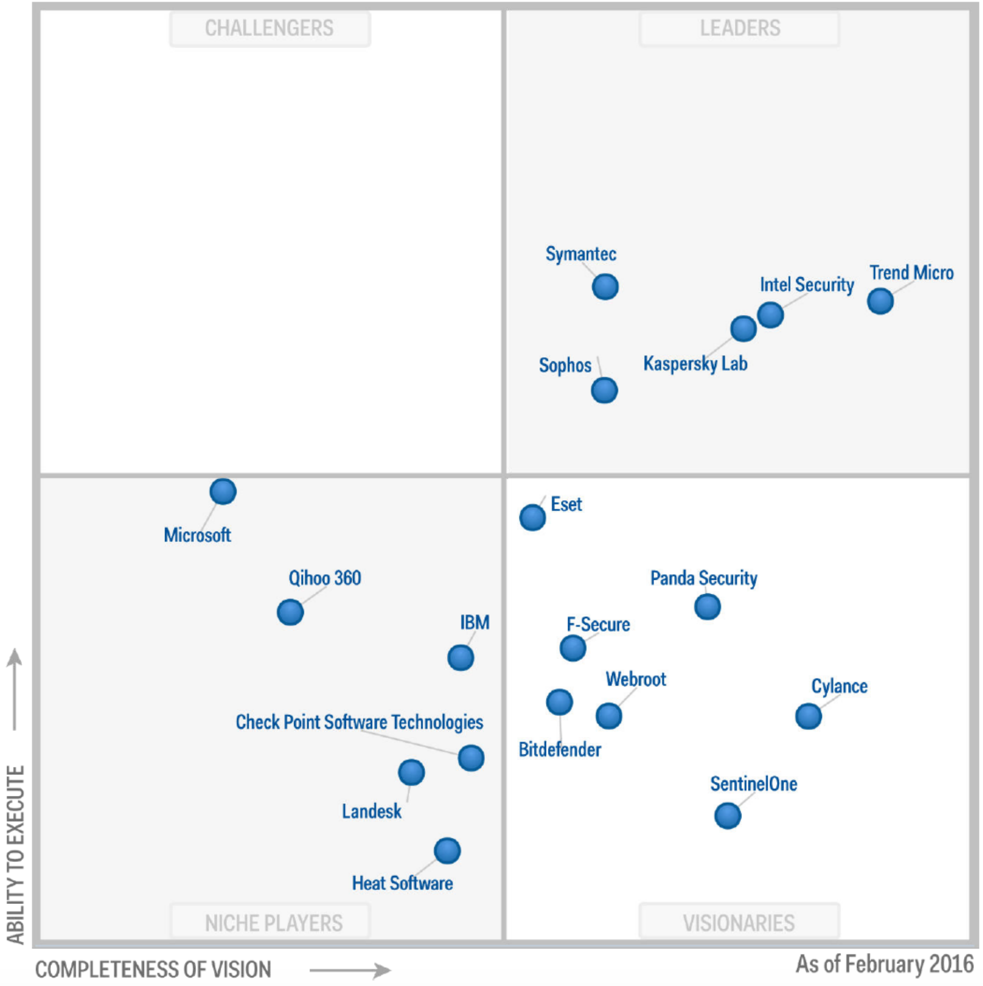
Feb 2016

Trend Micro TippingPoint® Named a Leader in 2017 Gartner Magic Quadrant for Intrusion Detection and Prevention Systems (IDPS)

Jan 2017

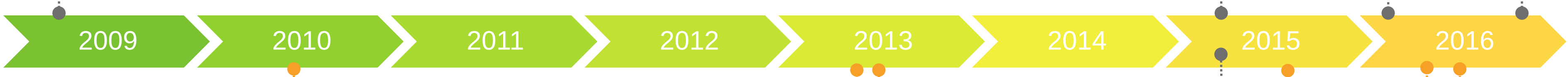
This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



重大 IoT 駭客案例回顧

Car Hacking



Hack into the OnStar telematics system of a 2009 Chevrolet Impala

- GM TOOK 5 YEARS TO FIX FULL CONTROL HACK IN MILLIONS OF VEHICLES EQUIPPED WITH ONSTAR

CarShark Software Lets You Hack Into, Control And Kill Any Car

Hackers compromise Prius, seize control of wheel, brakes and more

Researchers reveal methods behind car hack (2010 Ford Escape) at Defcon

Hackers remotely kill a Jeep on the highway

- Recall of 1.4M vehicles
- Cost of $140M+

OnStar hack remotely starts cars

- GM fix the RemoteLink App download 3M+ times

Controlling vehicle features of Nissan LEAFs across the globe

- Nissan shut down an app which controls Leaf cars

Hackers take remote control of Tesla Model S from 12 miles away

- Push Tesla to provide new firmware for bug fix

Tesla fixes bug after hackers hijack Model S

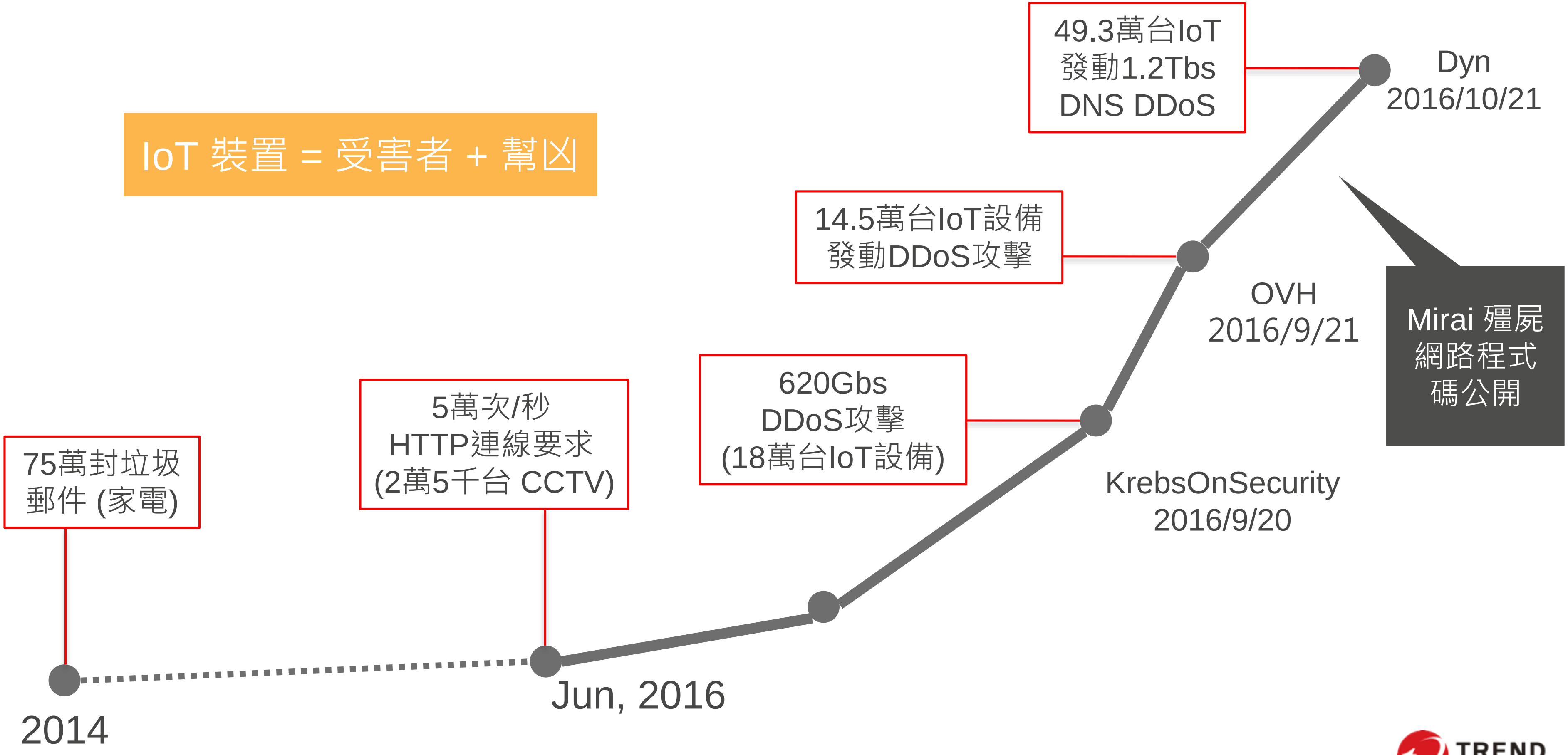
Friendly Hackers Exploit Loophole to Disable Alarm on Mitsubishi Outlander

Flaws in 2.2M BMW ConnectedDrive Infotainment System allow remote hack

OnStar

IoT DDoS 攻擊事件簿

IoT 裝置 = 受害者 + 幫凶



75萬封垃圾郵件 (家電)

2014

5萬次/秒 HTTP連線要求 (2萬5千台 CCTV)

Jun, 2016

620Gbs DDoS攻擊 (18萬台IoT設備)

KrebsOnSecurity 2016/9/20

14.5萬台IoT設備發動DDoS攻擊

OVH 2016/9/21

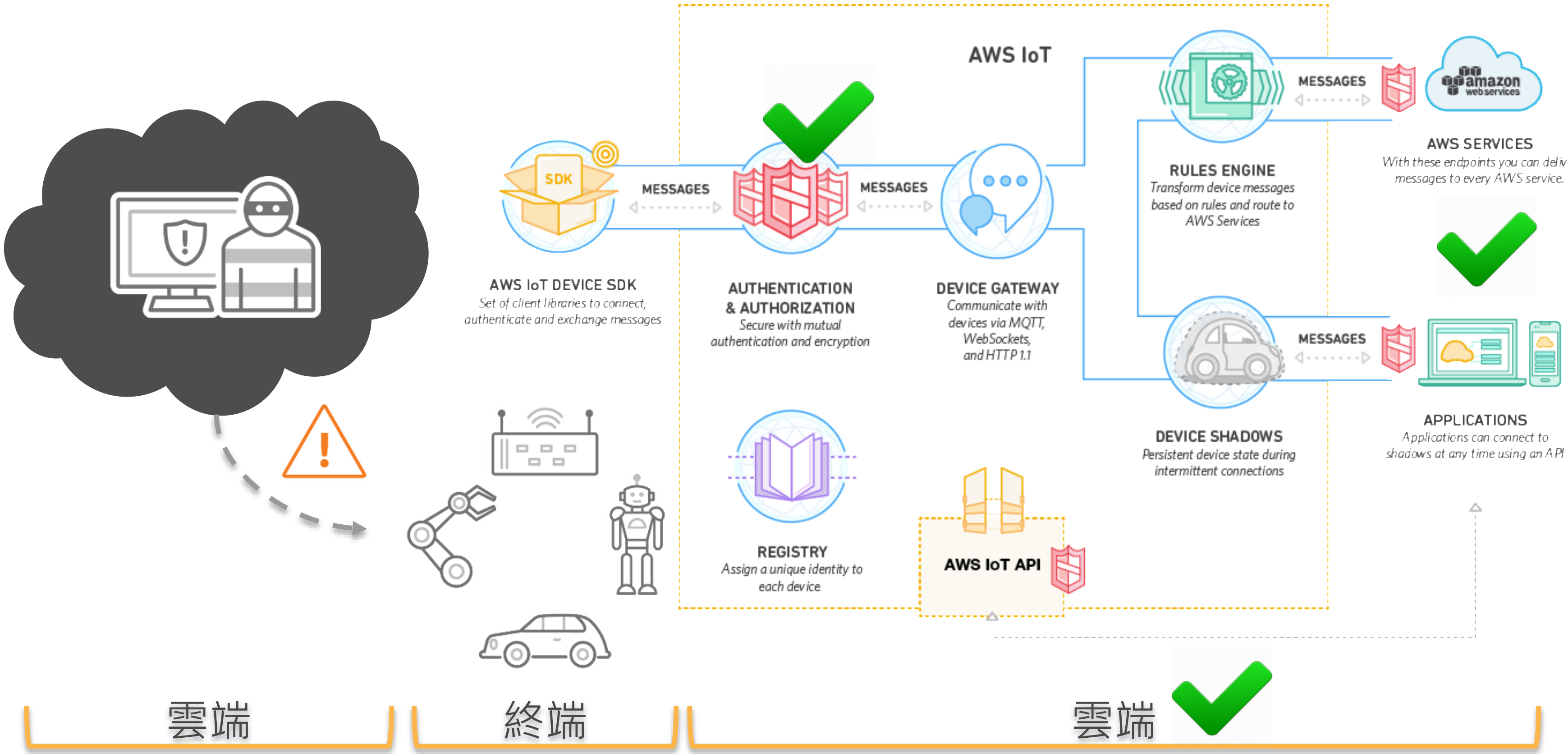
49.3萬台IoT發動1.2Tbs DNS DDoS

Dyn 2016/10/21

Mirai 殭屍網路程式碼公開

問題的根源以及解決方式

IoT 終端裝置的安全考量



AWS IoT

AWS IoT DEVICE SDK
Set of client libraries to connect, authenticate and exchange messages

AUTHENTICATION & AUTHORIZATION
Secure with mutual authentication and encryption

DEVICE GATEWAY
Communicate with devices via MQTT, WebSockets, and HTTP 1.1

RULES ENGINE
Transform device messages based on rules and route to AWS Services

AWS SERVICES
With these endpoints you can deliver messages to every AWS service.

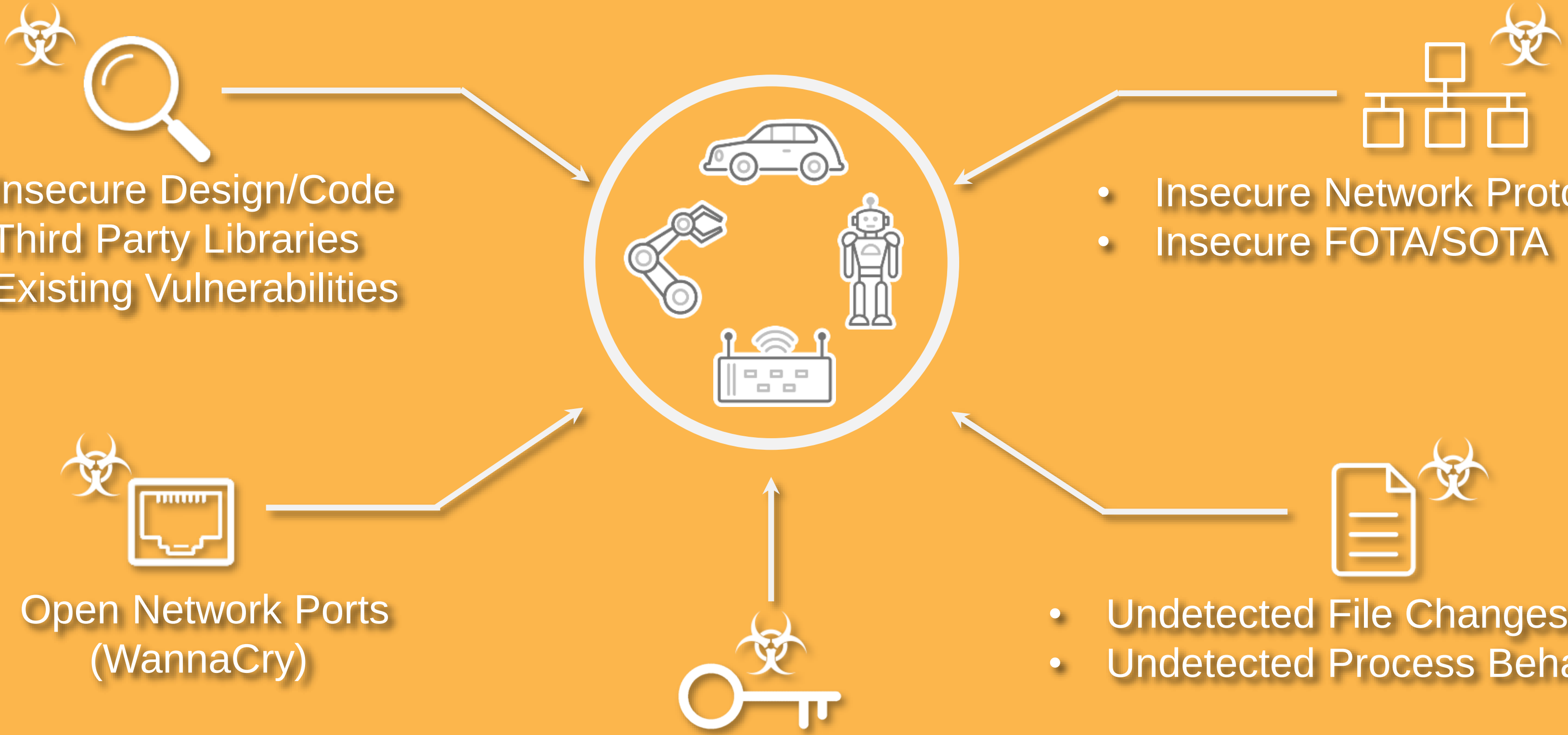
DEVICE SHADOWS
Persistent device state during intermittent connections

APPLICATIONS
Applications can connect to shadows at any time using an API

REGISTRY
Assign a unique identity to each device

AWS IoT API

IoT 終端裝置威脅來源



- Insecure Design/Code
- Third Party Libraries
- Existing Vulnerabilities

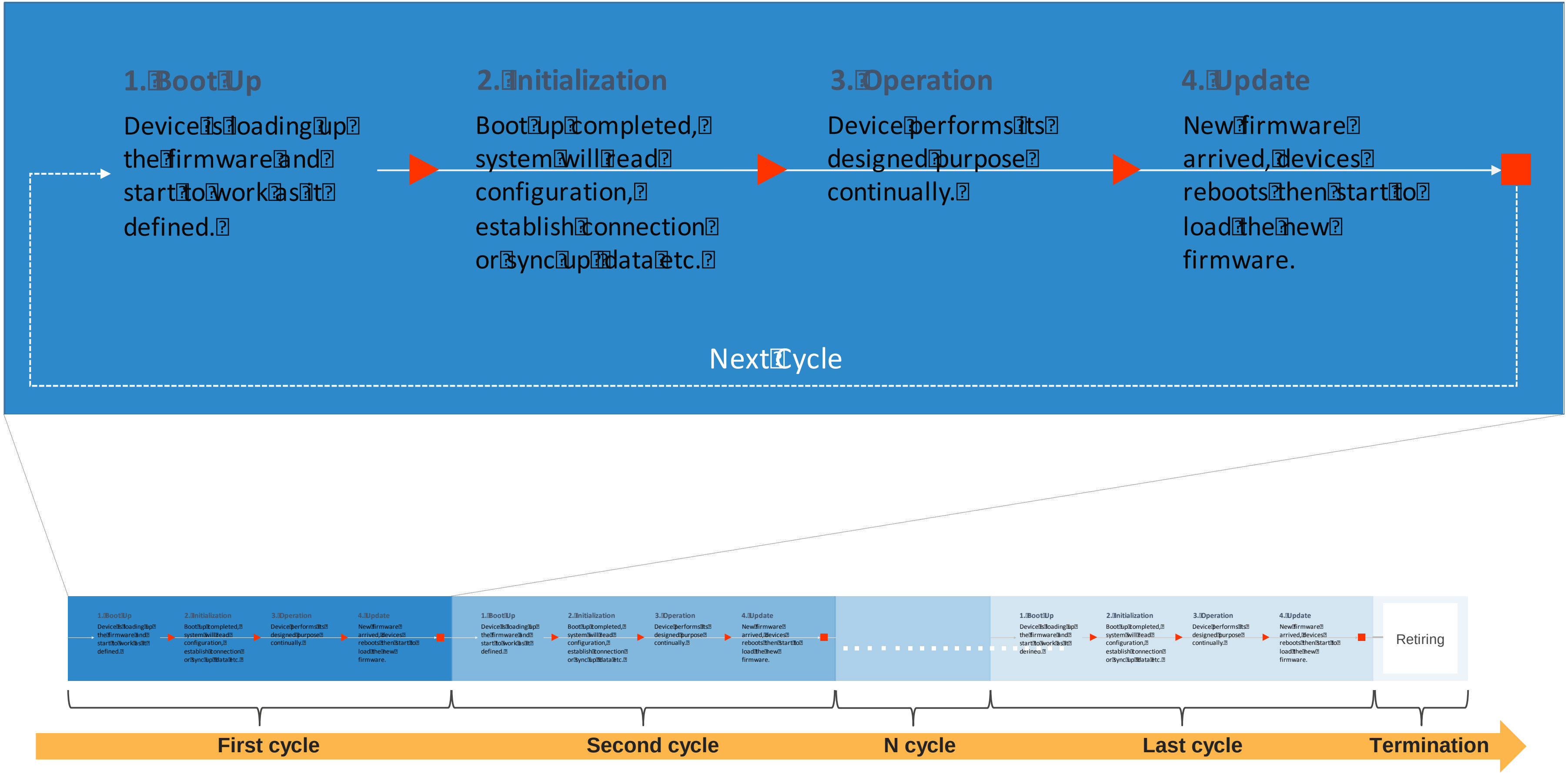
- Insecure Network Protocols
- Insecure FOTA/SOTA

Open Network Ports
(WannaCry)

Poor Authentication/Authorization
(Mirai)

- Undetected File Changes
- Undetected Process Behavior

IoT 終端設備生命週期



1. Boot Up

Device is loading up the firmware and start to work as it defined.

2. Initialization

Boot up completed, system will read configuration, establish connection or sync up data etc.

3. Operation

Device performs its designed purpose continually.

4. Update

New firmware arrived, devices reboots then start to load the new firmware.

Next Cycle

Retiring

First cycle

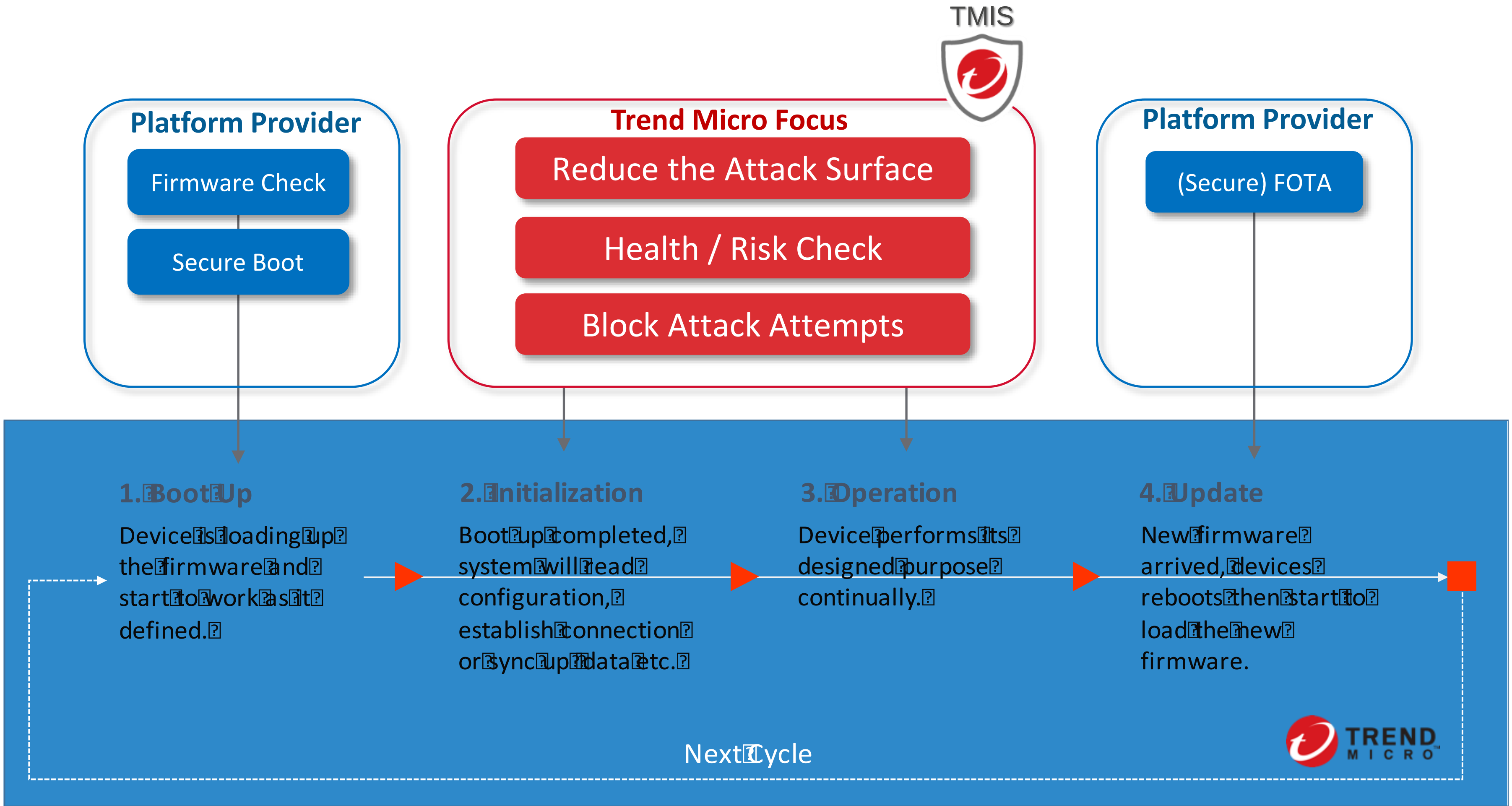
Second cycle

N cycle

Last cycle

Termination

IoT 終端設備生命週期及保護



TMIS

Platform Provider

Firmware Check

Secure Boot

Trend Micro Focus

Reduce the Attack Surface

Health / Risk Check

Block Attack Attempts

Platform Provider

(Secure) FOTA

1. Boot Up

Device is loading up the firmware and start to work as it defined.

2. Initialization

Boot up completed, system will read configuration, establish connection or sync up data etc.

3. Operation

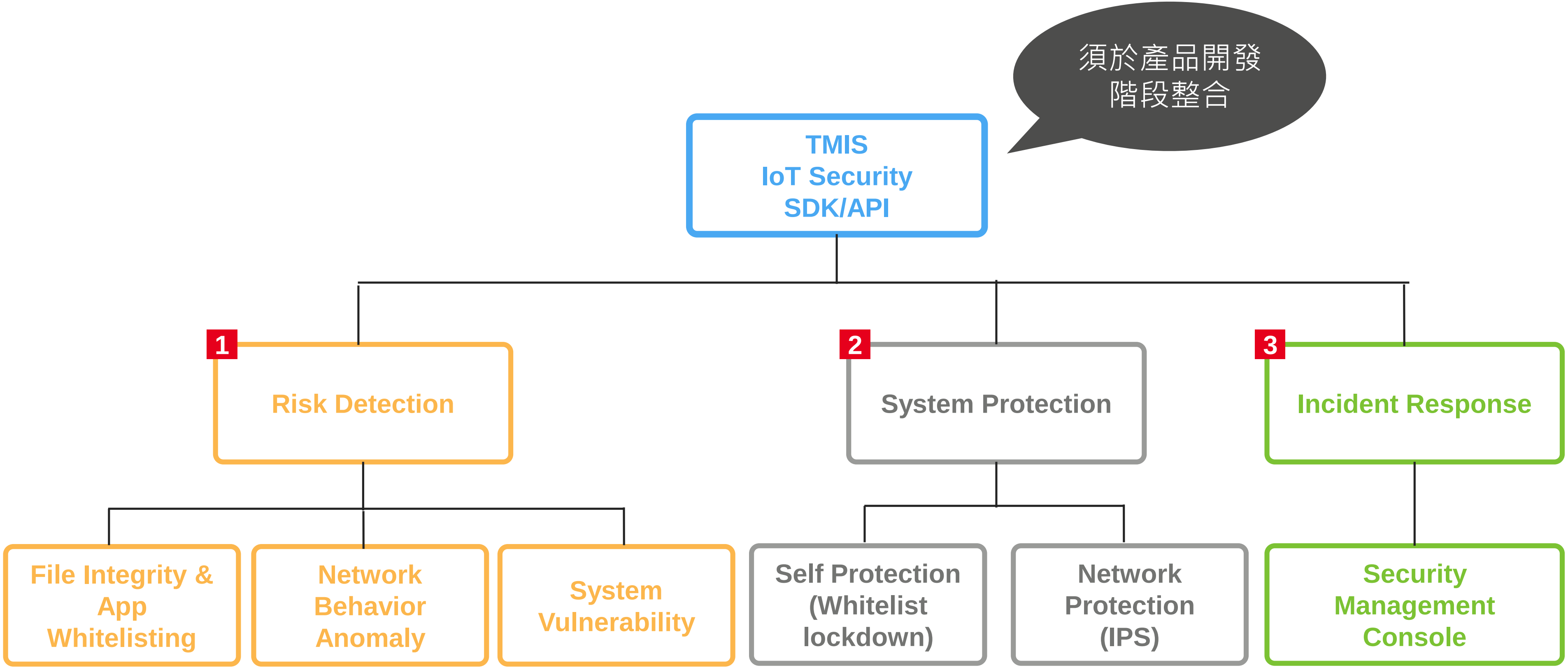
Device performs its designed purpose continually.

4. Update

New firmware arrived, devices reboots then start to load the new firmware.

Next Cycle

Trend Micro IoT Security 功能概述



須於產品開發
階段整合

TMIS
IoT Security
SDK/API

1 Risk Detection

- File Integrity & App Whitelisting
- Network Behavior Anomaly
- System Vulnerability

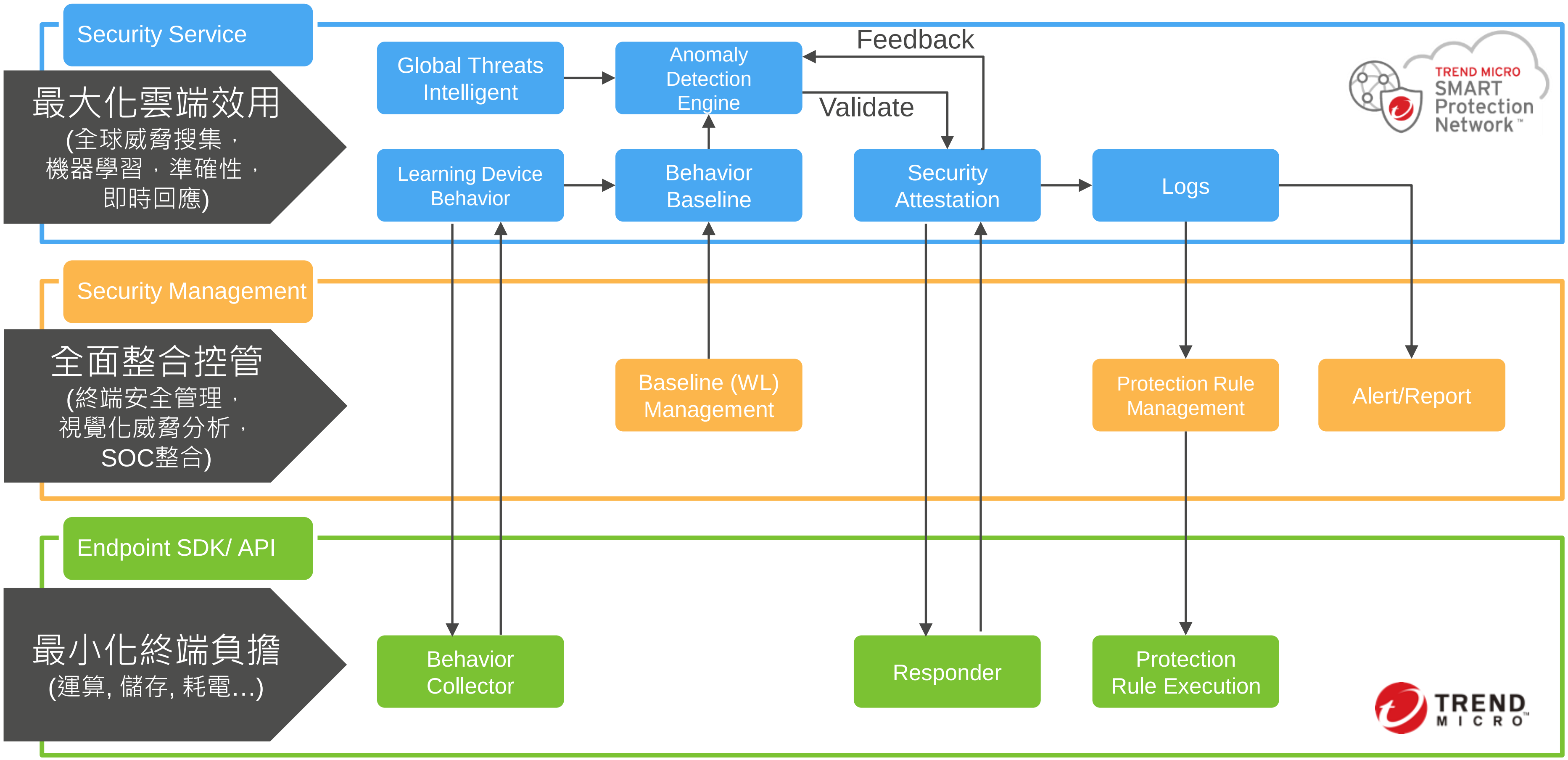
2 System Protection

- Self Protection (Whitelist lockdown)
- Network Protection (IPS)

3 Incident Response

- Security Management Console

TMIS 架構及設計理念



Security Service

最大化雲端效用
(全球威脅搜集，
機器學習，準確性，
即時回應)

Global Threats Intelligent

Anomaly Detection Engine

Feedback

Validate

Learning Device Behavior

Behavior Baseline

Security Attestation

Logs

TREND MICRO SMART Protection Network™

Security Management

全面整合控管
(終端安全管理，
視覺化威脅分析，
SOC整合)

Baseline (WL) Management

Protection Rule Management

Alert/Report

Endpoint SDK/ API

最小化終端負擔
(運算, 儲存, 耗電…)

Behavior Collector

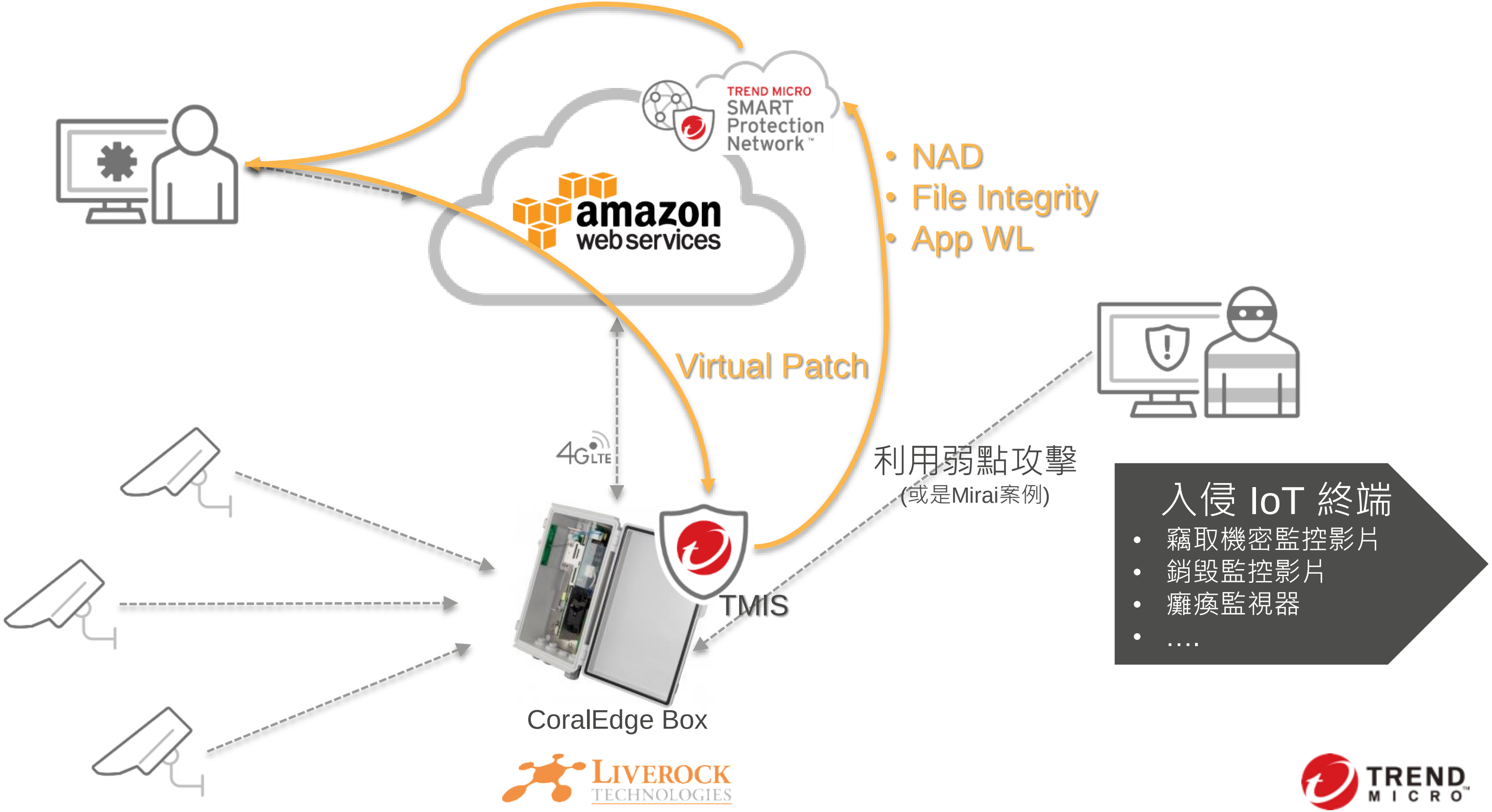
Responder

Protection Rule Execution

TREND MICRO™

客戶案例分享

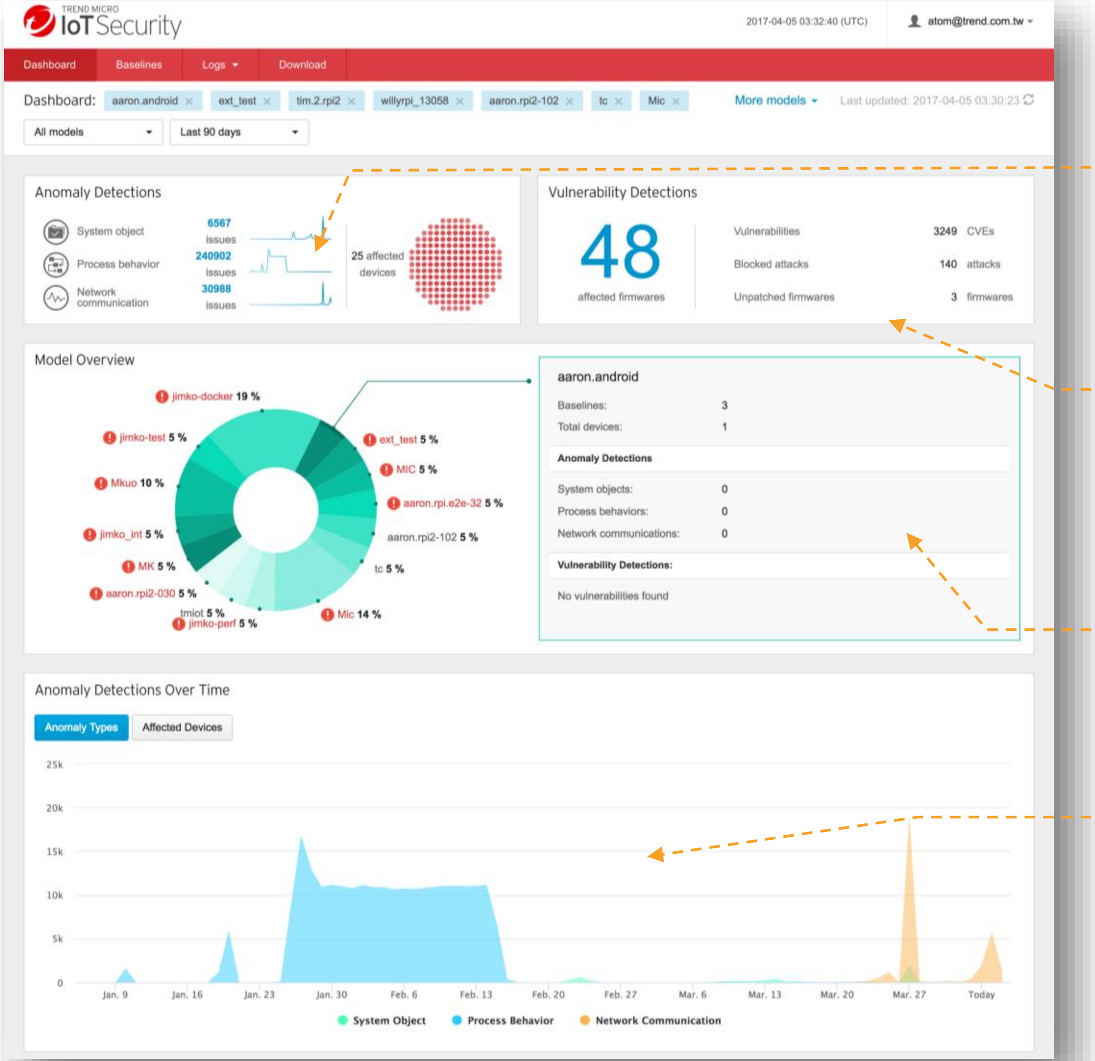
使用 TMIS 保護關鍵物聯網終端裝置



入侵 IoT 終端

- 竊取機密監控影片
- 銷毀監控影片
- 癱瘓監視器
- ….

TMIS 管理平台



2017-04-05 03:32:40 (UTC)

atom@trend.com.tw

Dashboard: aaron.android ext_test tim.2.rpi2 willyrpi_13058 aaron.rpi2-102 tc Mic

Last updated: 2017-04-05 03:30:23

All models

Last 90 days

Anomaly Detections

System object	6567 issues
Process behavior	240902 issues
Network communication	30988 issues

25 affected devices

Vulnerability Detections

48 affected firmwares

Vulnerabilities	3249	CVEs
Blocked attacks	140	attacks
Unpatched firmwares	3	firmwares

Model Overview

aaron.android

Baselines:	3
Total devices:	1

Anomaly Detections

System objects:	0
Process behaviors:	0
Network communications:	0

Vulnerability Detections:

No vulnerabilities found

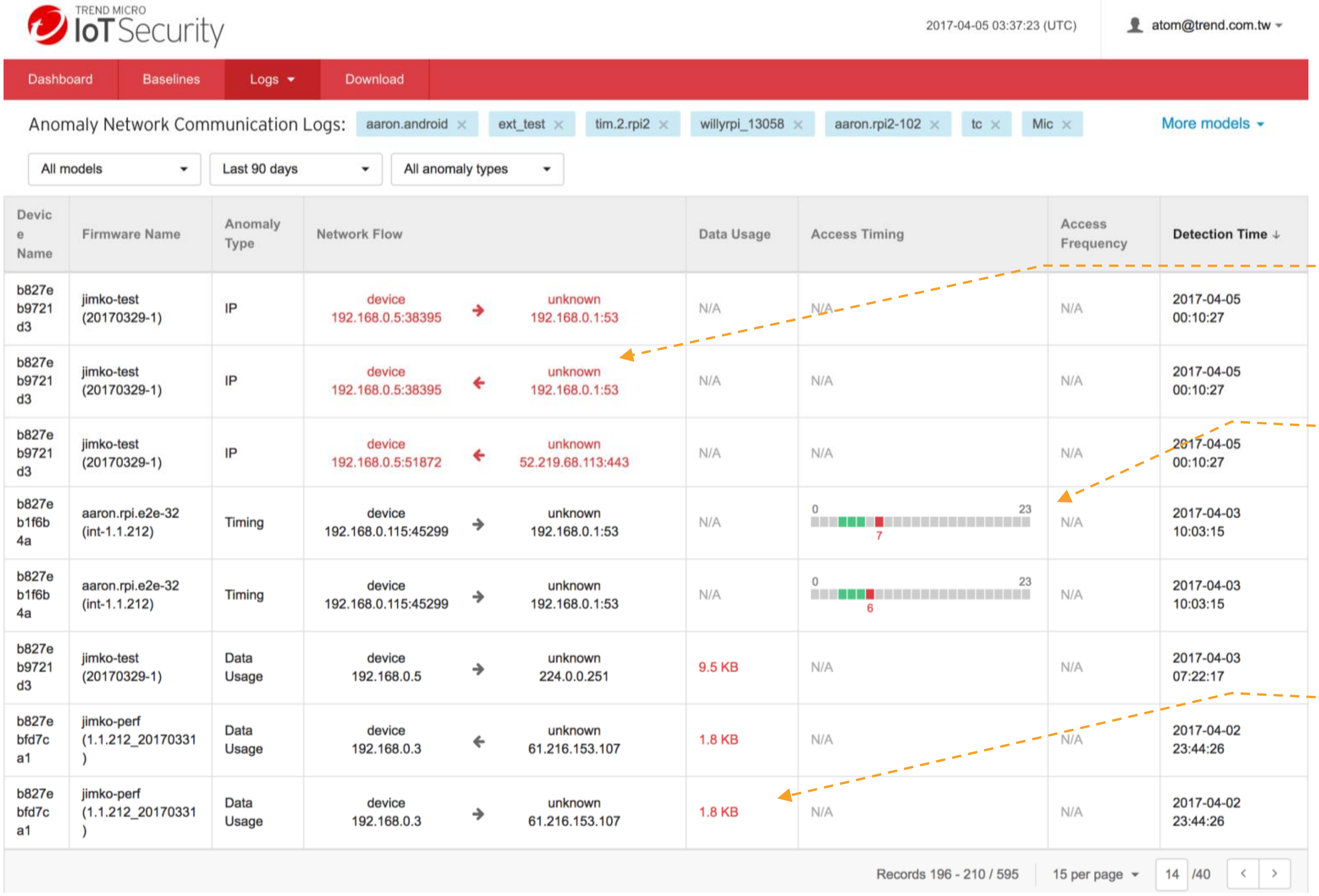
Anomaly Detections Over Time

Anomaly Detection
Make sure all IoT devices still work as originally design.

Vulnerability Detection & Virtual Patch
Understand whether IoT devices were exposed to the latest threats and take action to protect them.

Detail the cyber security status of the firmware.

Find an anomaly of IoT devices, track trends of the anomaly, and plan the next fix or take mitigate actions.



Anomaly Network Communication Logs: aaron.android × ext_test × tim.2.rpi2 × willyrpi_13058 × aaron.rpi2-102 × tc × Mic × More models

All models ▾ Last 90 days ▾ All anomaly types ▾

Device Name	Firmware Name	Anomaly Type	Network Flow			Data Usage	Access Timing	Access Frequency	Detection Time ↓
b827eb9721d3	jimko-test (20170329-1)	IP	device 192.168.0.5:38395	→	unknown 192.168.0.1:53	N/A	N/A	N/A	2017-04-05 00:10:27
b827eb9721d3	jimko-test (20170329-1)	IP	device 192.168.0.5:38395	←	unknown 192.168.0.1:53	N/A	N/A	N/A	2017-04-05 00:10:27
b827eb9721d3	jimko-test (20170329-1)	IP	device 192.168.0.5:51872	←	unknown 52.219.68.113:443	N/A	N/A	N/A	2017-04-05 00:10:27
b827eb1f6b4a	aaron.rpi.e2e-32 (int-1.1.212)	Timing	device 192.168.0.115:45299	→	unknown 192.168.0.1:53	N/A	0 23 7	N/A	2017-04-03 10:03:15
b827eb1f6b4a	aaron.rpi.e2e-32 (int-1.1.212)	Timing	device 192.168.0.115:45299	→	unknown 192.168.0.1:53	N/A	0 23 6	N/A	2017-04-03 10:03:15
b827eb9721d3	jimko-test (20170329-1)	Data Usage	device 192.168.0.5	→	unknown 224.0.0.251	9.5 KB	N/A	N/A	2017-04-03 07:22:17
b827ebfd7ca1	jimko-perf (1.1.212_20170331)	Data Usage	device 192.168.0.3	←	unknown 61.216.153.107	1.8 KB	N/A	N/A	2017-04-02 23:44:26
b827ebfd7ca1	jimko-perf (1.1.212_20170331)	Data Usage	device 192.168.0.3	→	unknown 61.216.153.107	1.8 KB	N/A	N/A	2017-04-02 23:44:26

Records 196 - 210 / 595 15 per page ▾ 14 /40

Unusual IP

Unusual Access Timing

Unusual Data Usage

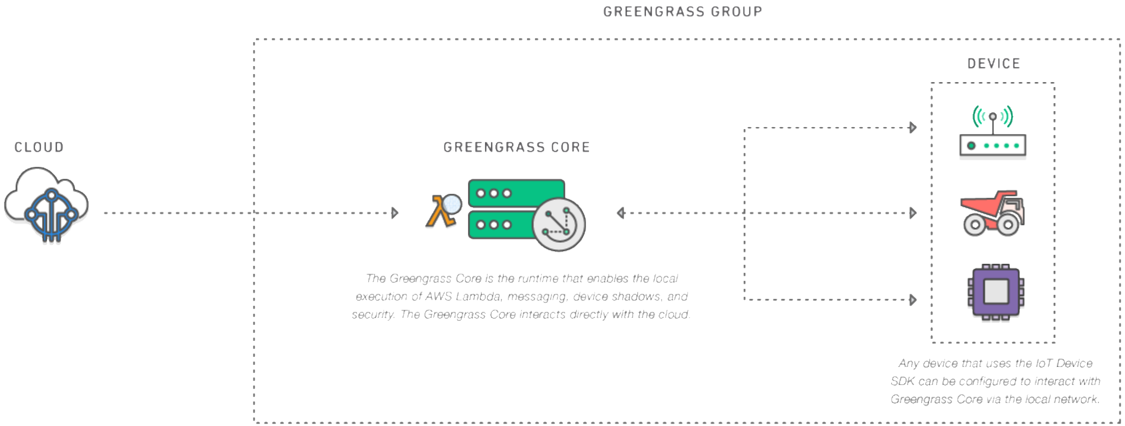
檢視你的 IoT 裝置

IoT 終端裝置分類以及安全防護對策

	Class 1	Class 2	Class 3	Class 4
Control unit	MCU (8 bit/16bit)	MCU (32bit)	MPU (32bit)	GPU, MPU, CPU (32bit/64bit)
OS	Non	Low cost RTOS	RTOS/Embedded Linux	Embedded Linux/Android/Full feature RTOS/Win 10 IoT Core
Network	ZigBee, NFC, Bluetooth	Cellar, Wi-Fi	Ethernet, Wi-Fi	Wi-Fi with other multiple network protocols
Application	Lighting, Wearables, Thermostats	Medical devices, low-end network appliances, telematics	Larger/ expensive medical or industrial automation devices; robotics; vending machines	Gateways, high-end medical devices, military devices, autonomous driving car
IoT Device Security				
Root of Trust	HW SE (Secure Element)	HW/SW PKI	HW/SW PKI	PKI/TPM
TMIS (Function)	Risk Detection (Planning)	Risk Detection (Planning)	Risk Detection/System Protection	Risk Detection/System Protection
TMIS (Method)	Restful API (Planning)	Restful API (Planning)	SDK (Agent)	SDK (Agent)
OTA/Roll back	OTA	OTA	OTA/Roll back	OTA/Roll back

Device Life Cycle

以 AWS Greengrass 為例

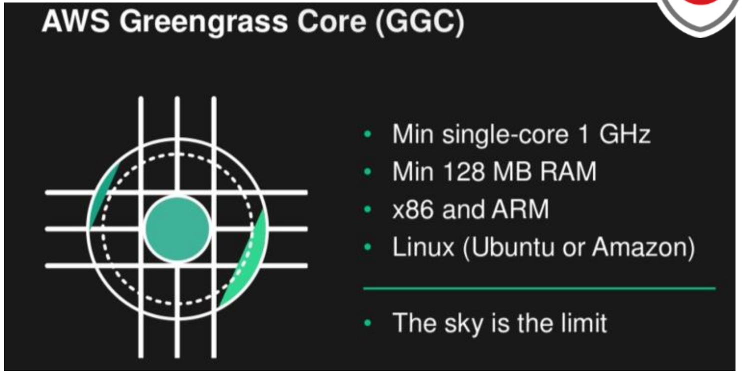


The Greengrass Core is the runtime that enables the local execution of AWS Lambda, messaging, device shadows, and security. The Greengrass Core interacts directly with the cloud.

Any device that uses the IoT Device SDK can be configured to interact with Greengrass Core via the local network.

A defined group of Greengrass Cores and other devices that are configured to communicate with one another. A Greengrass Group may represent one floor of a building, one truck, or one home.

TMIS

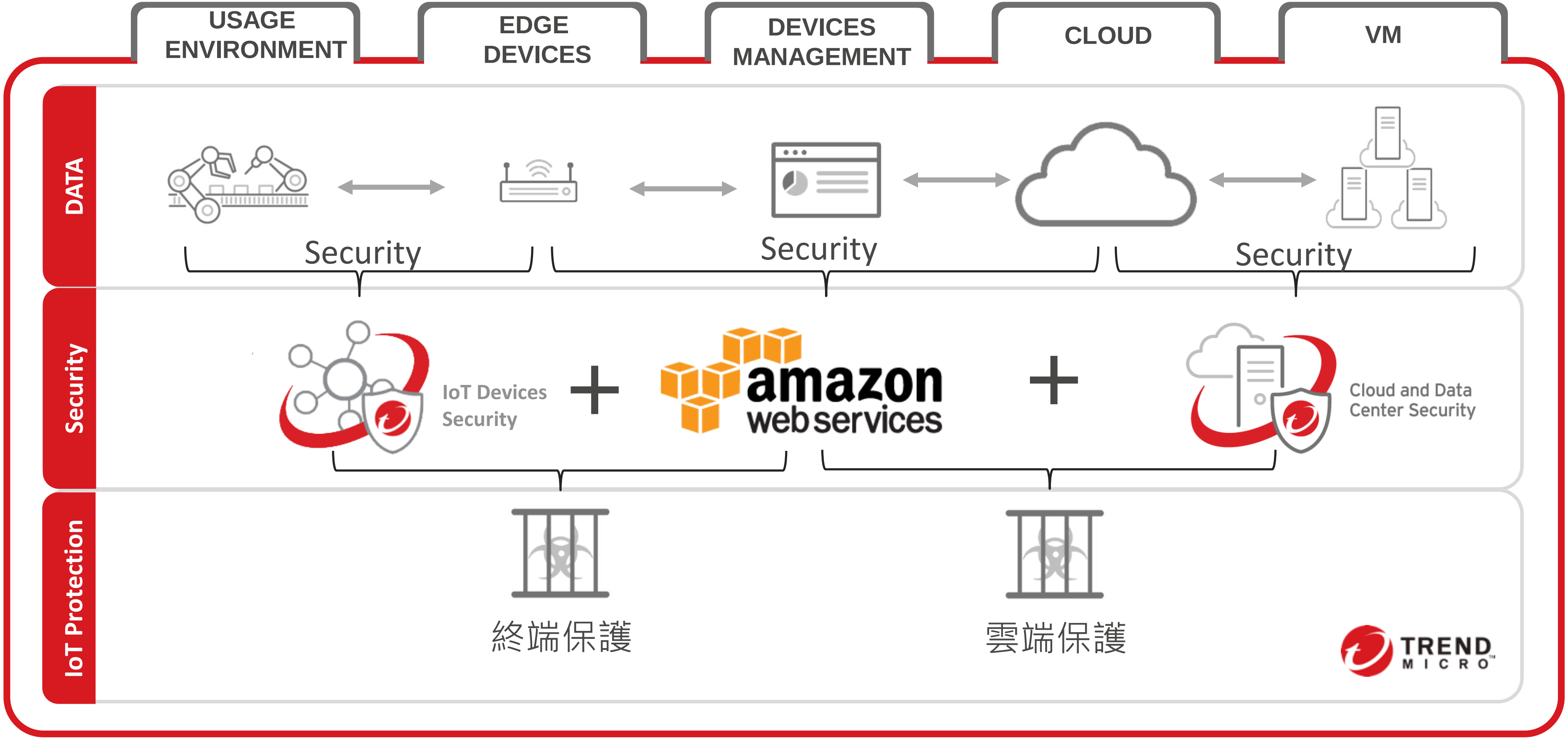


AWS Greengrass Core (GGC)

- Min single-core 1 GHz
- Min 128 MB RAM
- x86 and ARM
- Linux (Ubuntu or Amazon)

- The sky is the limit

趨勢科技與AWS打造雲到端的安全物聯網環境



AWS

SUMMIT

Thank You

Peter_yang@trend.com.tw

amazon
web services