大物聯網時代下的有線、無線資安革命

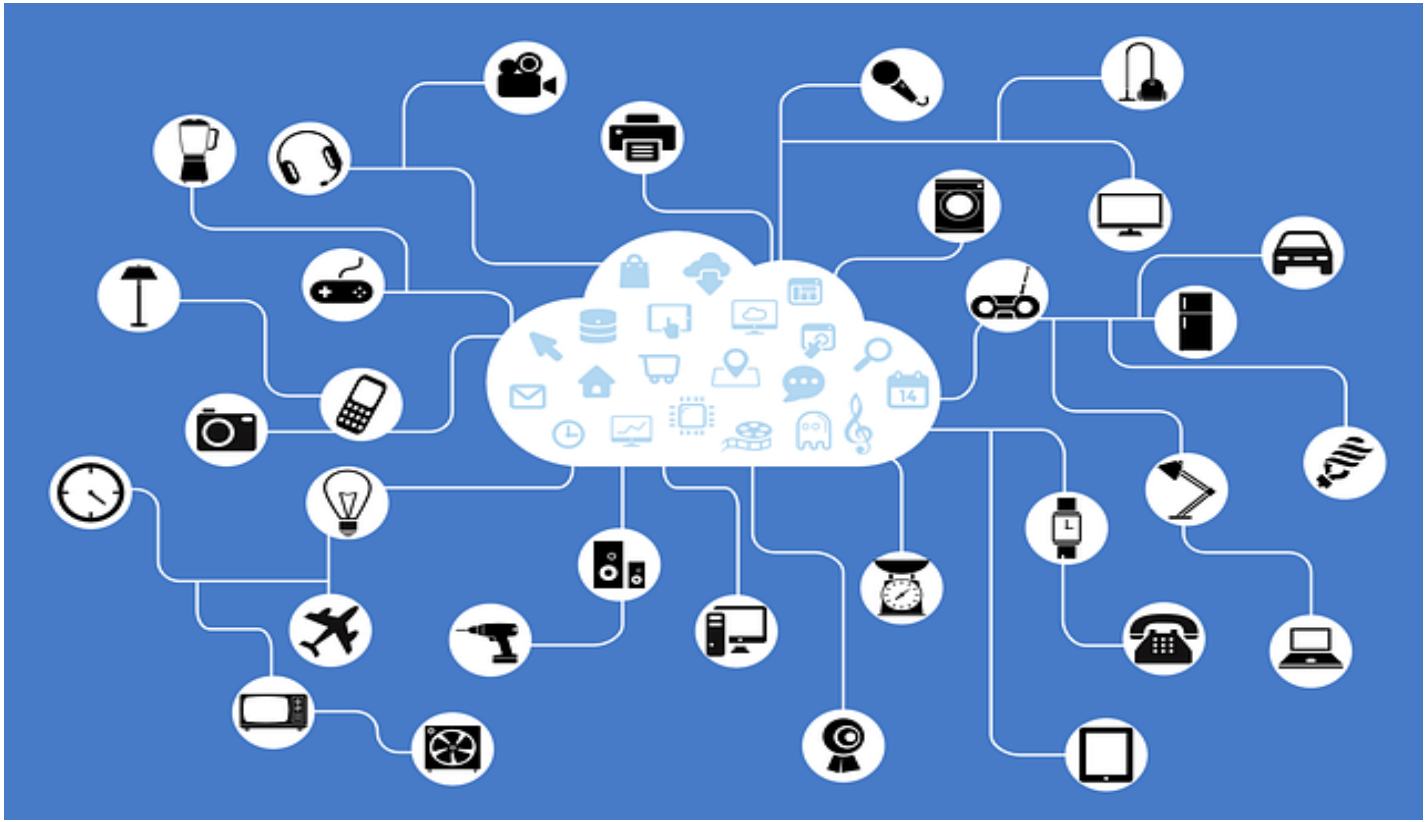
蘇 俊 銘 Kevin Su
Extreme Networks 台灣區技術顧問

Agenda

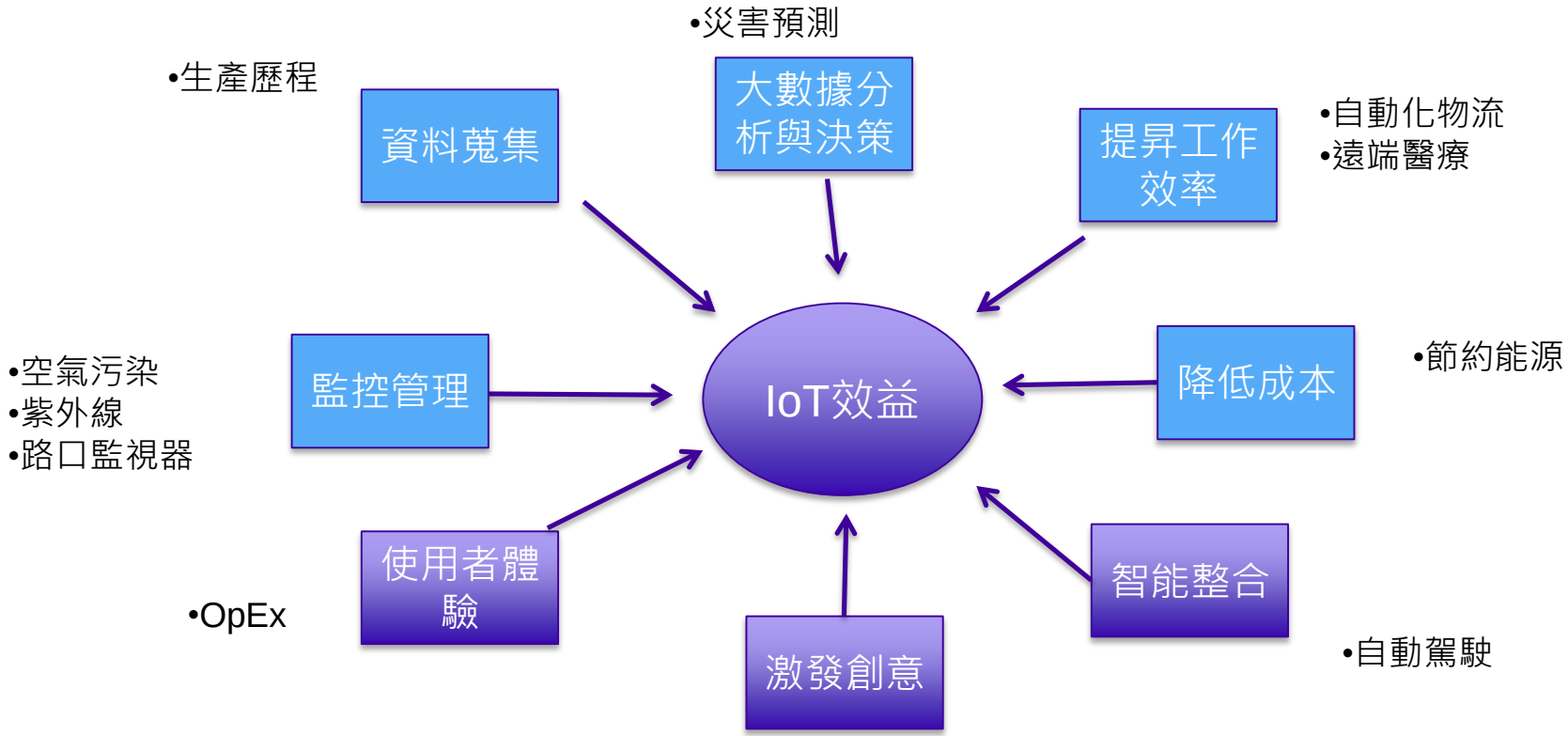
- IoT趨勢
- 校園IoT應用
- IoT面臨的安全性威脅
- 導入IoT的注意事項
- Extreme對應的解決方案
- 結論

IoT, Internet of Things（物聯網）/ IoE, Internet of Everything（萬物聯網）趨勢

- IoT應用範圍
  - 交通運輸
  - 健康醫療
  - 智慧建築
  - 公共安全
  - 智慧能源
  - 零售物流
  - 環境監控
  - 工業製造
  - 農業生產

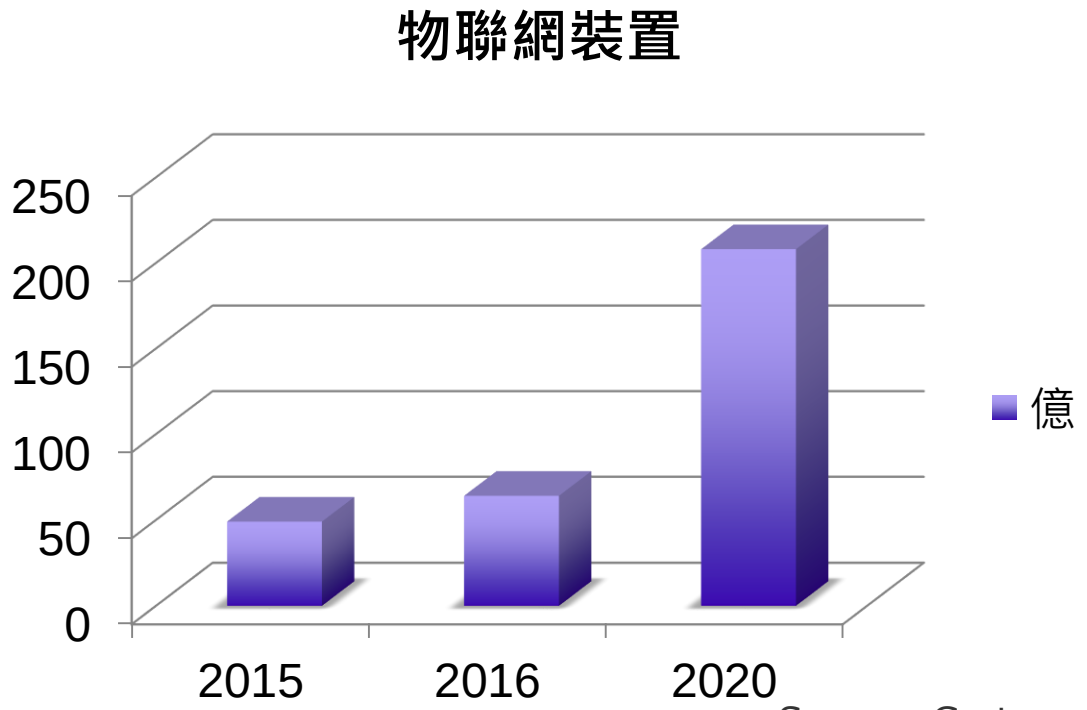


IoT為企業帶來的效益



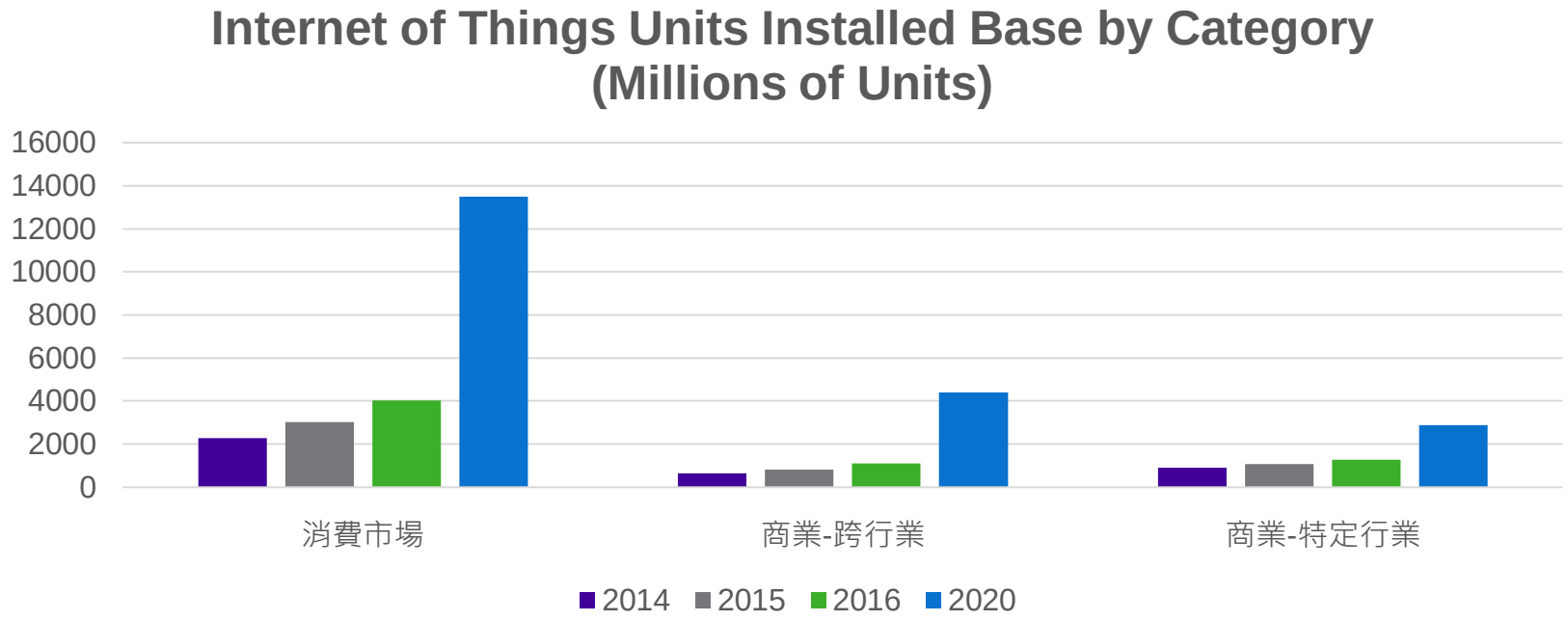
物聯網（IoT）裝置爆炸性成長

- Gardner的預測資料預估2020年時會有超過208億的物連網(IoT)裝置



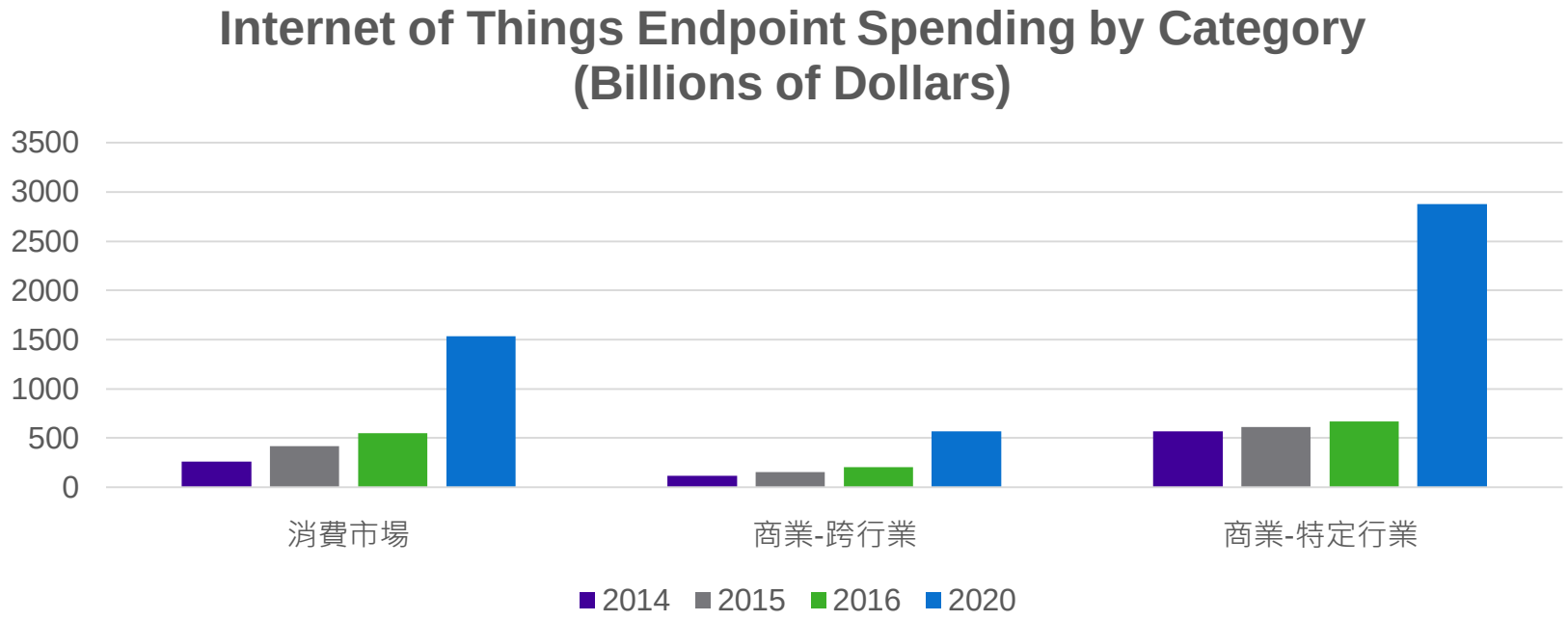
Source: Gartner (November 2015)

IoT裝置數量成長趨勢



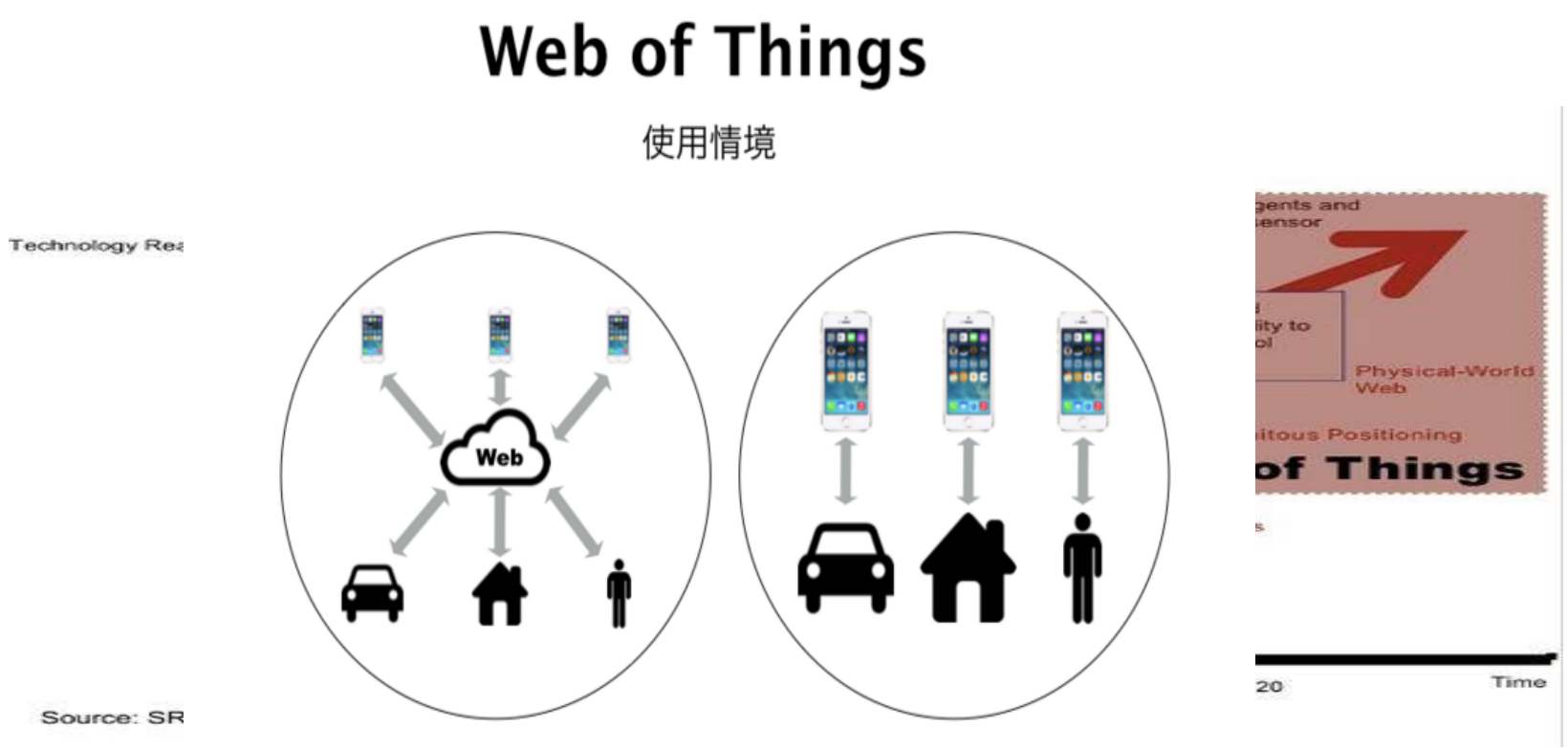
Source: Gartner (November 2015)

因應IoT裝置所衍生的應用/服務費用趨勢



Source: Gartner (November 2015)

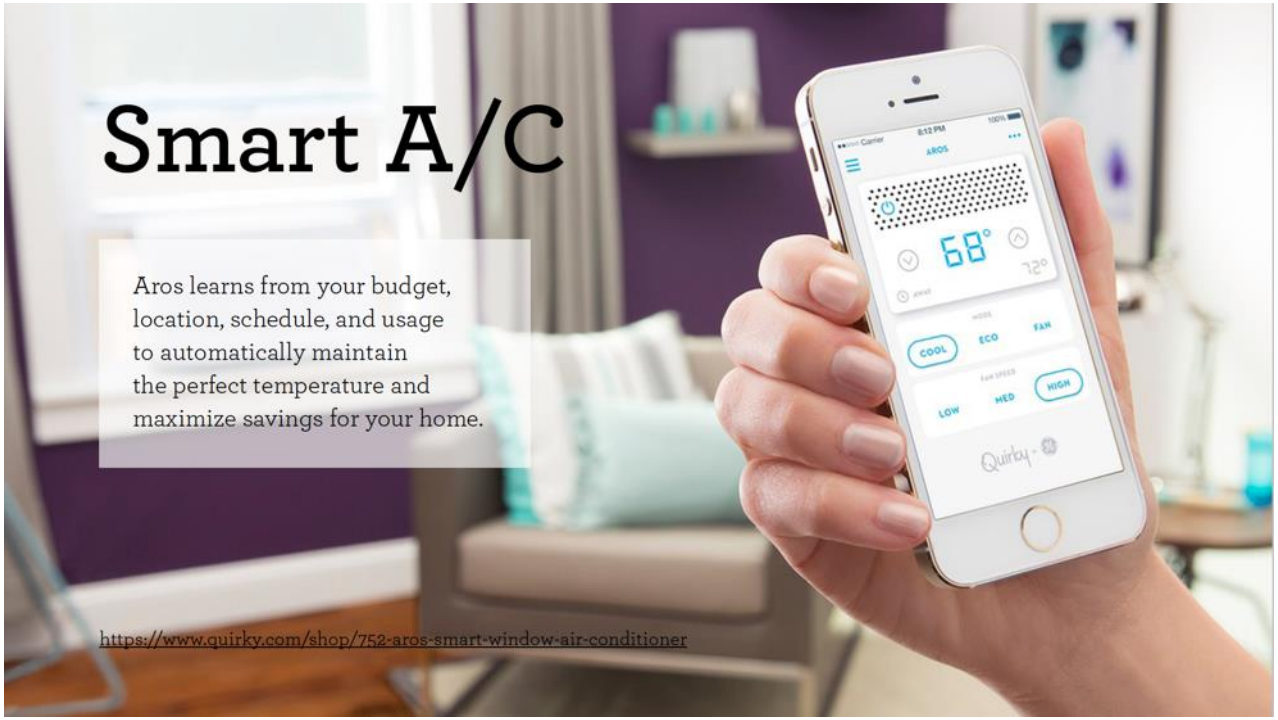
Web of Things 將是主要的 IoT 技術趨勢



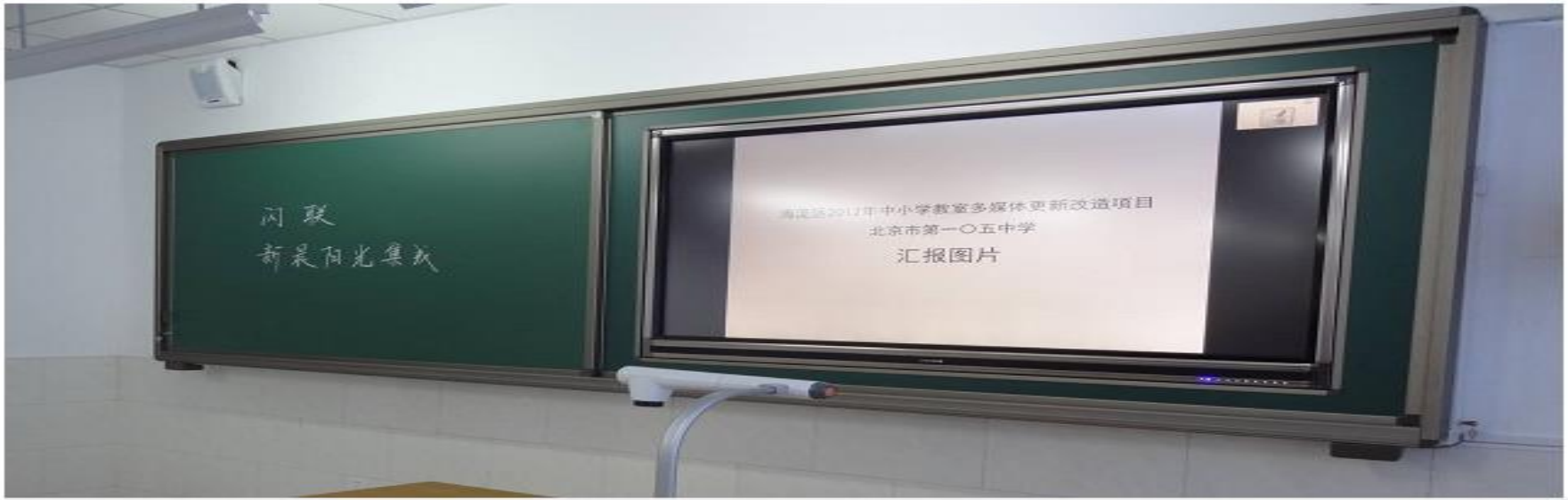
Agenda

- IoT趨勢
- 校園IoT應用
- IoT面臨的安全性威脅
- 導入IoT的注意事項
- Extreme對應的解決方案
- 結論

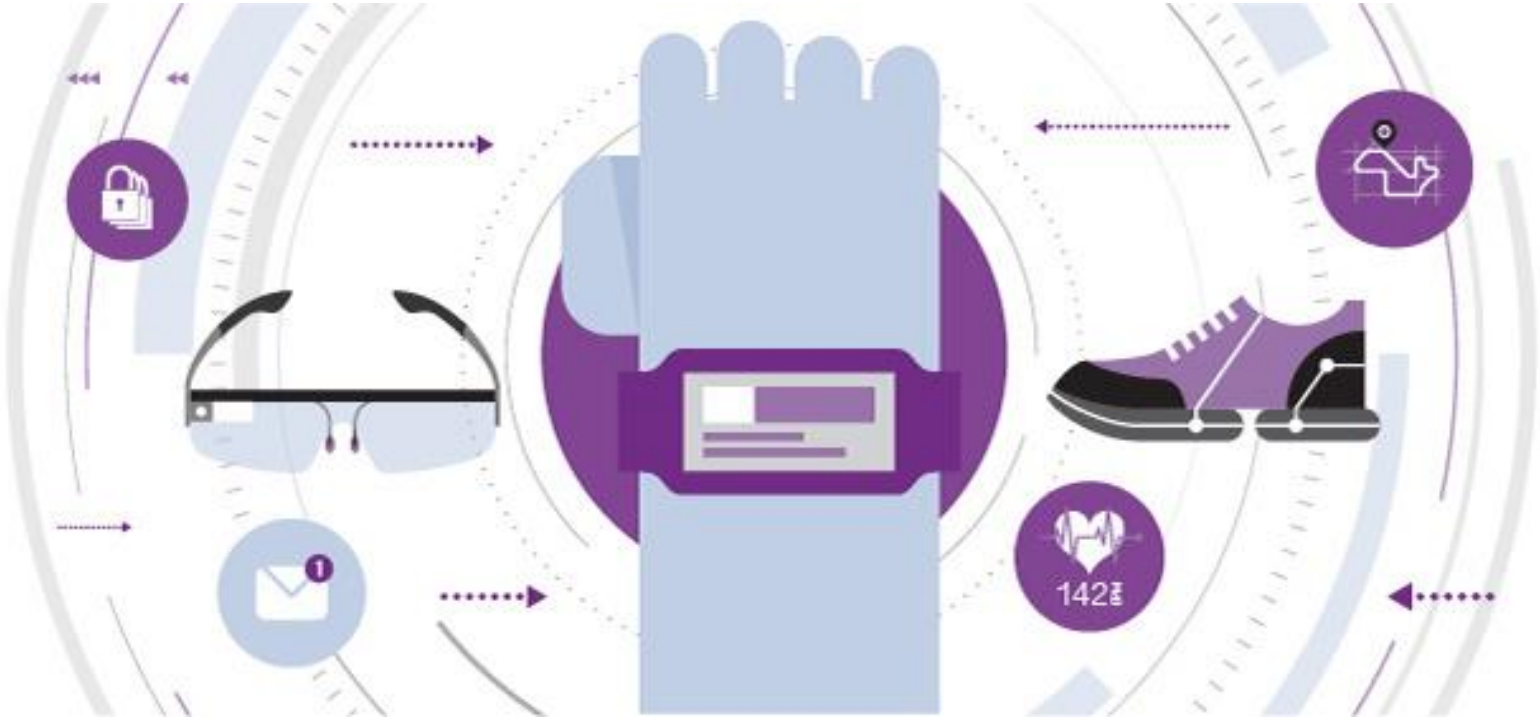
Kiosk



Creating a connected classroom with IoT



Posted November 18, 2014 by Microsoft IoT



Arduino +  Temperature sensor +  MQTT +  Bluemix & IOT Foundation =  Realtime graphing of data

Smart Mirror

A reflective mirror with programmable applications and digital display for the home, office and public environments (hotels, hospitals, retail shops).

http://www.cybertecturemirror.com/

有了IoT的協助，訊息呈現的方式不同以往

可汗學院

非盈利組織

可汗學院是由孟加拉裔美國人，麻省理工學院及哈佛大學商學院畢業生薩爾曼·可汗在2006年創立的一所非營利教育機構。 維基百科

“課堂"變得更開放和學習不再被限制於課堂

- 可汗學院利用了網路傳送的便捷與錄影重複利用成本低的特性。每段課程影片長度約十分鐘，從最基礎的內容開始，以由易到難的進階方式互相銜接。
- 教學者本人不出現在影片中，用的是一種電子黑板系統。
- 其網站目前也開發了一種練習系統，記錄了學習者對每一個問題的完整練習記錄，教學者參考該記錄，可以很容易得知學習者哪些觀念不懂，目前已有557個練習。傳統的學校課程中，為了配合全班的進度，教師只要求學生跨過一定的門檻（例如及格）就繼續往下教；但若利用類似於可汗學院的系統，則可以試圖讓學生懂得每一個未來還要用到的基礎觀念之後，再繼續往下教學，進度類似的學生可以重編在一班。在美國，某些學校已經導入「回家看可汗學院影片代替家庭作業，上課時則是做練習，再由老師或已懂的同學去教導其他同學」這樣的教學模式。

Agenda

- IoT趨勢
- 校園IoT應用
- IoT面臨的安全性威脅
- 導入IoT的注意事項
- Extreme對應的解決方案
- 結論

IoT設備潛藏的風險

- 採用開放源與新的通訊協定，相較舊協定有較多的缺點及漏洞
- 製造商設計時並未考慮安全性，設備無防毒防駭機制
- 設備的數量與多樣性造成管理的複雜度
- 爆炸性的成長數量也成為駭客偵測與覬覦的目標

作業系統漏洞的影響

Linux Flaw Affects Linux PCs, Servers, and Devices Running Android KitKat 4.4

January 21, 2016

A previously undiscovered flaw in the Linux kernel has been found, affecting “tens of millions” of Linux PCs and servers. According to researchers, the bug allows attackers to escalate local user privileges to the highest root level, and also affects devices running Android KitKat 4.4 and higher. The flaw, which dates back to 2012, affects Linux kernel versions 3.8 and later, and is found in the keyring facility where apps are allowed to store encryption keys, authentication tokens, and other sensitive security data. Once exploited, attackers could execute code on the Linux kernel and extract cached security data. As of disclosure date, security teams are investigating potentially affected devices.

http://www.trendmicro.com.my/vinfo/my/security/news/vulnerabilities-and-exploits/linux-flaw-affects-pcs-servers-and-android-kitkat

同時修補伺服器、手機和物聯網 (IoT) 裝置的必要性

- 是的，您沒看錯，您必須同時修補您的伺服器、手機和物聯網 (IoT) 裝置才能完全防堵這個漏洞。
- 這是一個由 Perception Point 研究團隊所揭露的 Linux 核心漏洞 (CVE-2016-0728)。Linux 核心是所有 Linux 作業系統的共同元件，而 Linux 系統又廣泛運用在今日的許許多多裝置。由於 Linux 不僅用於伺服器平台，就連 Android 手機、平板和各式各樣的 IoT 裝置都是使用 Linux 系統，因此 Linux 核心漏洞的影響層面非常廣泛。
- 此次出現的是一個提升本機權限的漏洞，光就它本身來看並不算是個嚴重的問題，但提升本機權限的漏洞可能搭配其他的漏洞 (尤其是應用程式漏洞) 來發動更嚴重的攻擊。
- 根據 Perception Point 研究團隊的說法，此漏洞大約影響全球 66% 的 Android 裝置。至於 IoT 裝置所受到的影響情況則不明朗。
- 此漏洞對 Android 和 IoT 裝置來說，最重要的問題還是在於如何取得系統更新。受此漏洞影響的大部分 Android 和 IoT 裝置很可能一輩子也無法獲得更新，所以此漏洞將永遠存在。
- Linux 核心目前已修正此漏洞，而 Linux 各主要發行版本也都已經有了對應的修補程式，所以，可以的話您還是應該更新您的伺服器。
- 至於受影響的 Android 手機、平板和 IoT 裝置，還是只能看看廠商是否能夠提供更新了。

POSTED ON 2016 年 01 月 27 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

Google Android作業系統的漏洞

Google » Android : Vulnerability Statistics

Vulnerabilities (187) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (7) Patches (12) Inventory Definitions (0) Compliance Definitions (0)

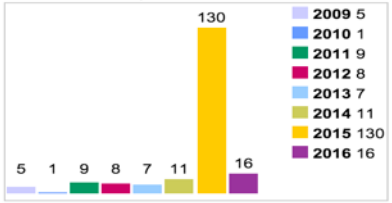
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

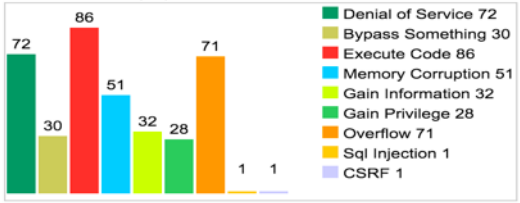
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2009	5	3								1					
2010	1	1	1												
2011	9	1	1		1					3	2	3			
2012	8	5	4	2							1				1
2013	7	1	2	2	2					1	1	3			
2014	11	1	4	1		1				1	2	1			
2015	130	56	73	65	47					22	22	16	1		
2016	16	4	1	1	1					2	4	5			
Total	187	72	86	71	51	1				30	32	28	1		1
% Of All		38.5	46.0	38.0	27.3	0.5	0.0	0.0	0.0	16.0	17.1	15.0	0.5	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year



Vulnerabilities By Type



Apple IOS作業系統的漏洞

Apple » Iphone Os : Vulnerability Statistics

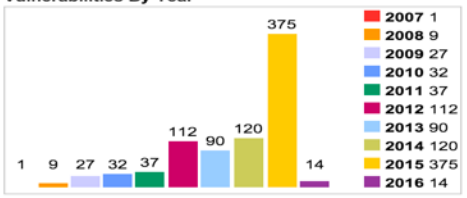
Vulnerabilities (817) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules
Related OVAL Definitions : Vulnerabilities (127) Patches (72) Inventory Definitions (0) Compliance Definitions (0)
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

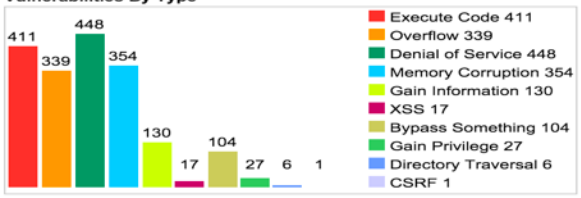
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2007	1		1	1											
2008	9	3	2		1						2				
2009	27	10	6	2	4		2			3	7				3
2010	32	14	14	9	6					5	3	2			3
2011	37	13	10	5	6		3			2	11	1			
2012	112	74	69	63	60		7			13	9	1			
2013	90	52	44	36	41		4			17	9	1			
2014	120	48	50	35	33		1	1		20	25	4			
2015	375	222	210	176	191			5		44	61	13	1		1
2016	14	12	5	12	12						3	5			
Total	817	448	411	339	354		17	6		104	130	27	1		7
% Of All		54.8	50.3	41.5	43.3	0.0	2.1	0.7	0.0	12.7	15.9	3.3	0.1	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year



Vulnerabilities By Type



IoT裝置造成隱私洩露

NETWORKWORLD

INSIDER Sign In | Register

Home > Microsoft Subnet

PRIVACY AND SECURITY FANATIC

By Ms. Smith | Follow

About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

Hacks to turn your wireless IP surveillance cameras against you

Thousands of wireless IP cameras are vulnerable to remote attacks. At Hack in the Box security conference, researchers showed how to exploit the devices in "To Watch or Be Watched: Turning Your Surveillance Camera Against You" and released a tool to automate attacks.

Network World | Apr 14, 2013 1:18 PM PT

RELATED

Widely used wireless IP cameras open to hijacking over the Internet,...

Hackers steal photos, turn Wi-Fi cameras into remote surveillance device

Kaspersky Lab launches world's first anti-malware product for UEFI

IoT 裝置發動DDoS攻擊

iThome 新聞 產品評測 CIO DevOps 技術 專題 專欄 主題頻道 研討會 社群 搜尋

新聞

Imperva：駭客以監視器攝影機組成殭屍網路，發動DDoS攻擊

資安業者Imperva發現一個由監視器攝影機組成的殭屍網路，而且駭客利用此一殭屍網路針對某一賽端服務發動了分散式阻斷服務攻擊（DDoS），突顯了物聯網時代所面臨的安全問題。

文/ 陳曉莉 | 2015-10-23 發表

按讚加入iThome粉絲團

資安業者Imperva指出，他們發現一個由監視器攝影機組成的殭屍網路，而且駭客利用此一殭屍網路針對某一賽端服務發動了分散式阻斷服務攻擊（DDoS），突顯了物聯網（IoT）時代所面臨的安全問題。

iThome 電腦報 按讚追蹤 iThome 最新報導

熱門新聞

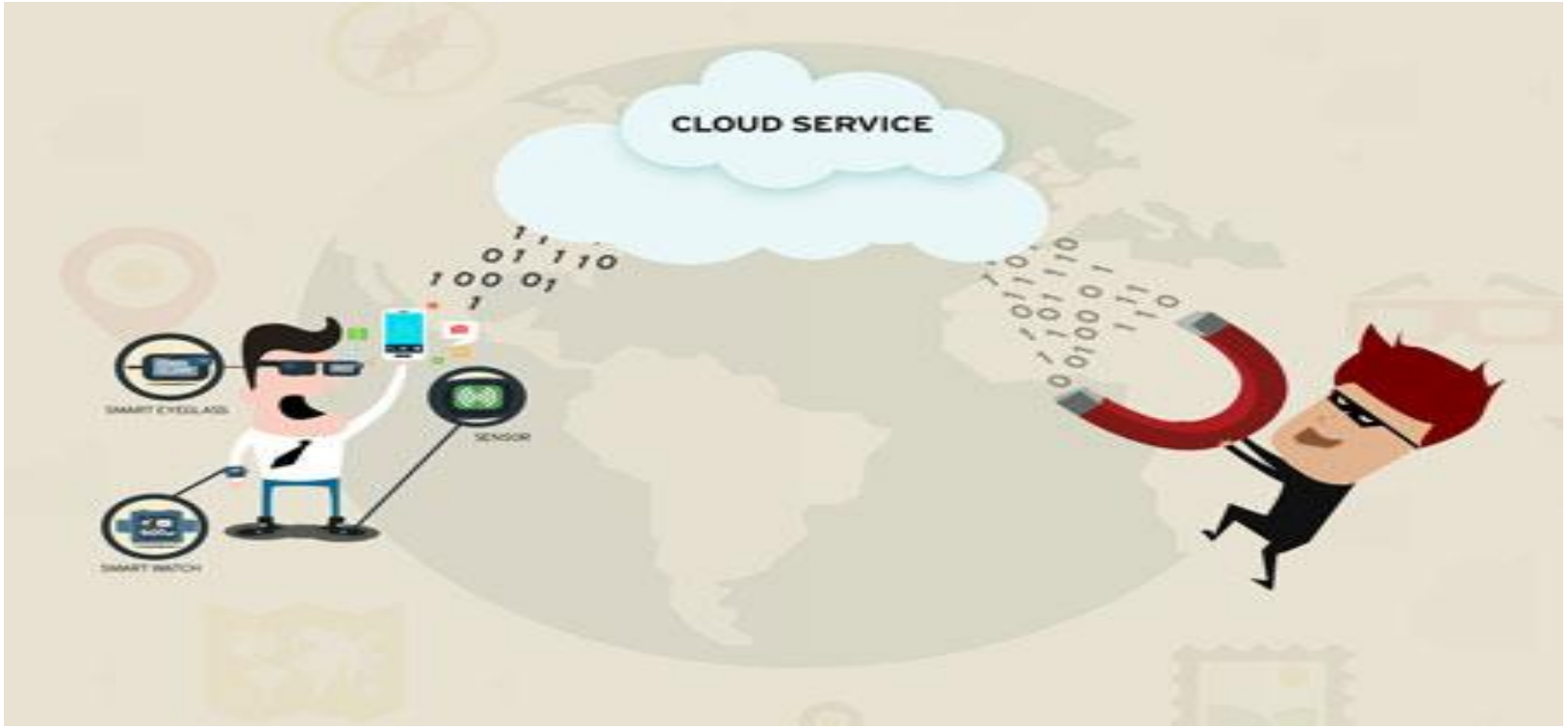
群暉DSM 6測試版新增多租戶架構Docker化NAS
2015-11-08

富士全錄新型複合機無須列印伺服器，1機可管50臺網路印表機
2015-11-08

Surface Pro 4上市前搶先曝光，台灣微軟將引進5款機型
2015-11-06

一周大事

駭客入侵雲端服務業者來竊取資料



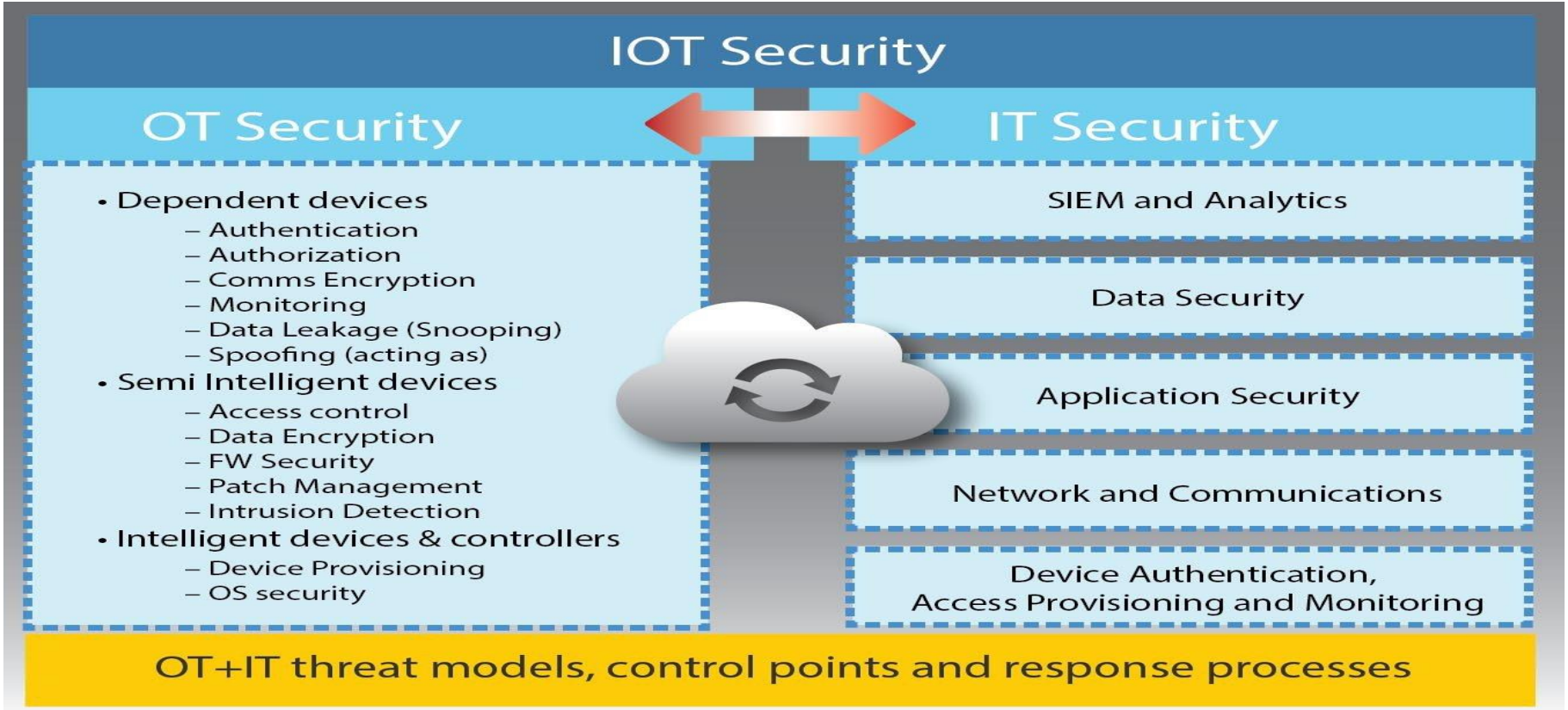
Agenda

- IoT趨勢
- 校園IoT應用
- IoT面臨的安全性威脅
- 導入IoT的注意事項
- Extreme對應的解決方案
- 結論

導入 IoT 注意事項

- 當IoT裝置以倍數成長及對於無線網路使用的依賴程度越來越高，無線網路的設計不再是以涵蓋率為考量，而是需要依使用密度，IoT應用類型頻寬來佈建無線基地台
- 慎選IoT裝置供應商除了功能面，評估該廠商對裝置漏洞處理的能力
- IoT裝置更新的複雜性與需發費的時間需列入考量
- IoT裝置本身的安全性必須納入考量，例如使用更嚴格的加密、更高強度的密碼、隨時保持裝置OS軟體更新等等。
- 網路設計透過不同網段或不同SSID來區隔服務已經不敷安全性上的需求，必須結合認證機制及動態授權能力，嚴加控管不同IoT的服務內容，避免IoT裝置上面不必要的開放連接埠，既要保護使用者、且不能犧牲裝置的功能性。
- 具備有線/無線集中控管能力的網路，可提供相同的使用經驗及安全性政策。
- 具備即時監視及控制IoT狀態與行為的能力，軌跡資訊也應使用單一資料庫，可快速追蹤使用者/IoT裝置以簡化將來Big Data 資料分析的關聯性

IoT Security = OT Security + IT Security



Agenda

- IoT趨勢
- 校園IoT應用
- IoT面臨的安全性威脅
- 導入IoT的注意事項
- Extreme對應的解決方案
- 結論

IT面對的網路架構挑戰

- 無線網路需支援高密度的使用環境
- IoT/BYOD裝置的定位與追蹤
- 無線網路的安全性強化（RF干擾及入侵偵測）
- 所有IoT設備、使用者行為的可視性
- 動態與即時的網路及存取資源配置
- 具備集中管理有線/無線能力
- 大量資料中心儲存系統及高速網路

符合物聯網需求的IT環境

- 支援高密度及高效能的無線網路
- 支援無線定位與追蹤系統
- 安全性(認證機制、入侵防禦系統、頻譜分析)
- BYOD/物聯網裝置控管
- 自動化(訪客自我註冊、網路自動管理)
- 流量可視性(大數據分析)

高密度用戶及高效能

- 早期無線網路存取的提供，大都是附加價值或加值服務，所以建置的要求以涵蓋率為主，因此建置的方式大都以不更動既有架構的前提下進行，所以tunnel及NAT的功能為市場主流。
- 隨著AP技術的演進，現在無線的存取服務在很多客戶的環境有取代有線的網路的趨勢， 使用者密度及效能面的考量變成主要的需求，傳統tunnel跟NAT的架構反而限制了整體無線網路的效能。
- Thin AP架構下的設計，尤其是802.11ac及未來的 802.11ad，WLAN controller形成瓶頸點。
- 應用場合大都以餐廳、會議室、禮堂、運動場、教室…等使用者密集的場合為主，但往後隨著IoT應用的普及和使用者使用超過兩個以上的行動設備（手機、平板、NB、穿戴式裝置），因此高密度的無線設備的連線需求，隨處可見！

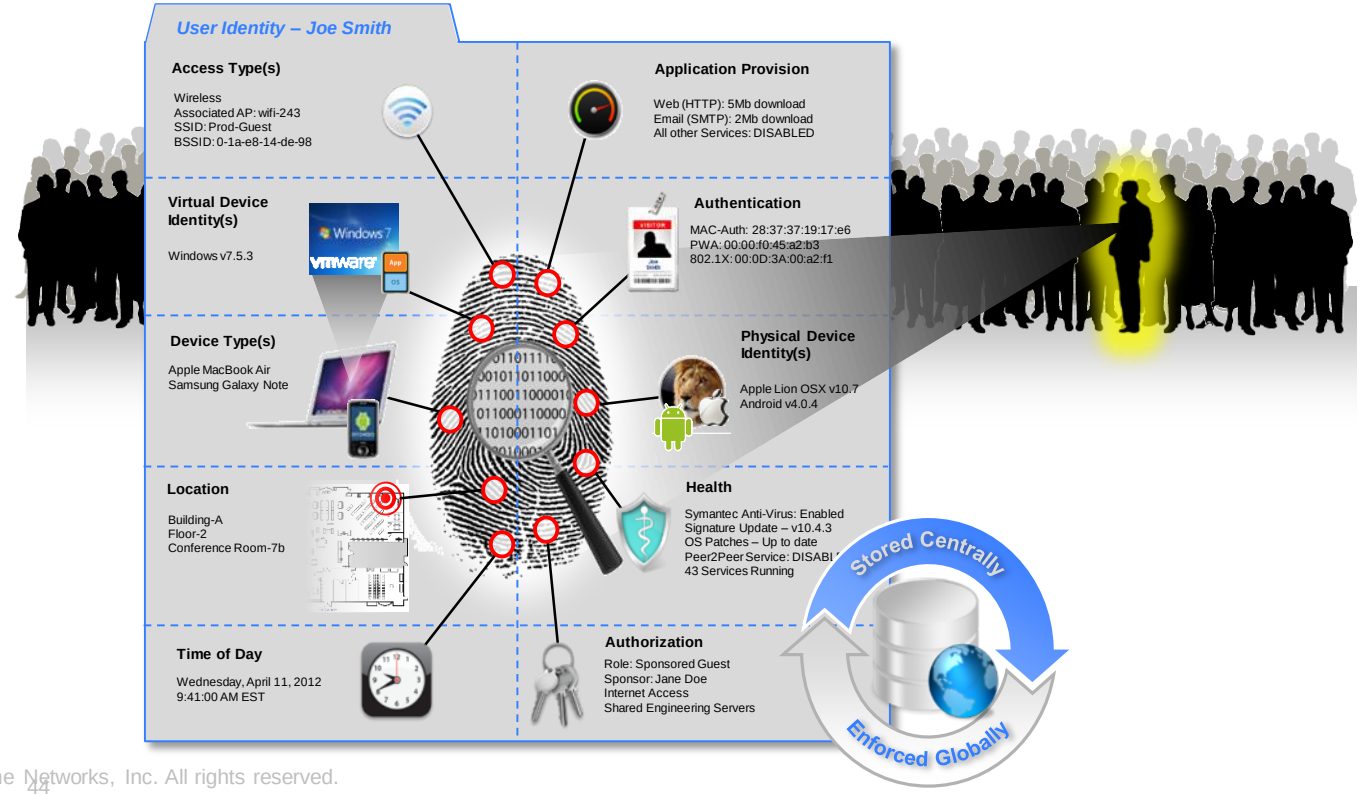
Extreme高密度用戶及高效能無線網路實績

- Number of deployed stadiums
  - 9 NFL Stadiums and 1 Collegiate Stadium with ExtremeWireless Solutions
  - 14 NFL Stadiums with Extreme Application Analytics Solution
- 6700 ExtremeWireless AP's installed at stadiums
- 1,003,382 users at football stadiums powered by ExtremeWireless
- 15,876 is the average number of unique, simultaneous wireless users per NFL game
- 544 Mbps is the average wireless bandwidth

New England Patriots
Philadelphia Eagles
Tennessee Titans
Jacksonville Jaguars
Cincinnati Bengals
Seattle Seahawks
Baltimore Ravens
Green Bay Packers
Buffalo Bills
Galaxy Macau
Diamond Light
Mount Union College
Baylor Bears
NextGen.Net

Extreme IAC - 安全性（認證、授權、稽核）

人、事、時、地、物，超過46種屬性來決定使用者/IoT裝置權限



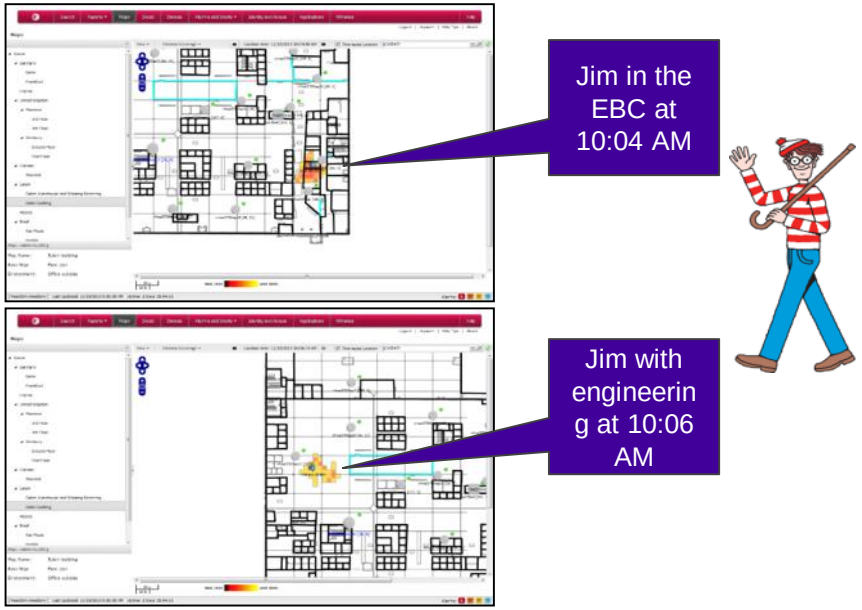
ExtemeWireless - 安全性（WIPS及RF管理）

- WIPS / WIDS 無線頻道掃描，降低網管人員 debug 困擾
- 進階頻譜掃瞄與辨別
  - 偵測辨別各種無線干擾源（如：微波/藍芽/等）
- Rogue AP 與無線攻擊行為偵測與防禦

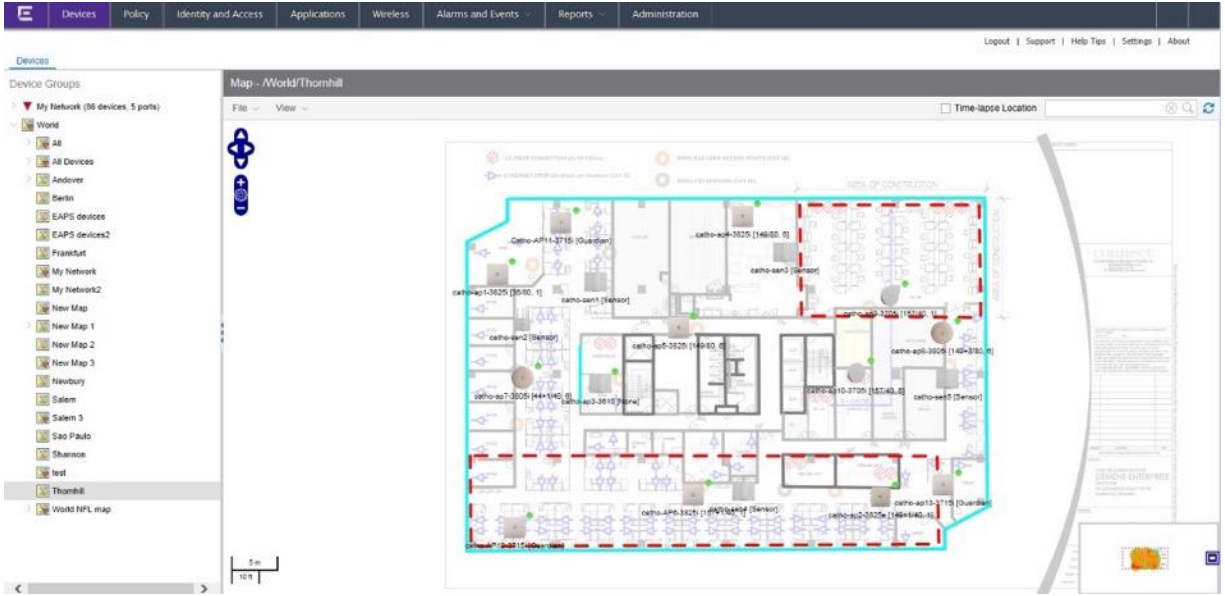
ExtremeControl - 無線訊號定位圖 使用者歷史位置

Maps – 使用者位置歷史紀錄

- Understand a wireless client's movement through the network
  - Search for clients by:
    - Username
    - Hostname
    - MAC
    - IP
- Allows better network troubleshooting



ExtremeControl - 無線訊號定位系統運用



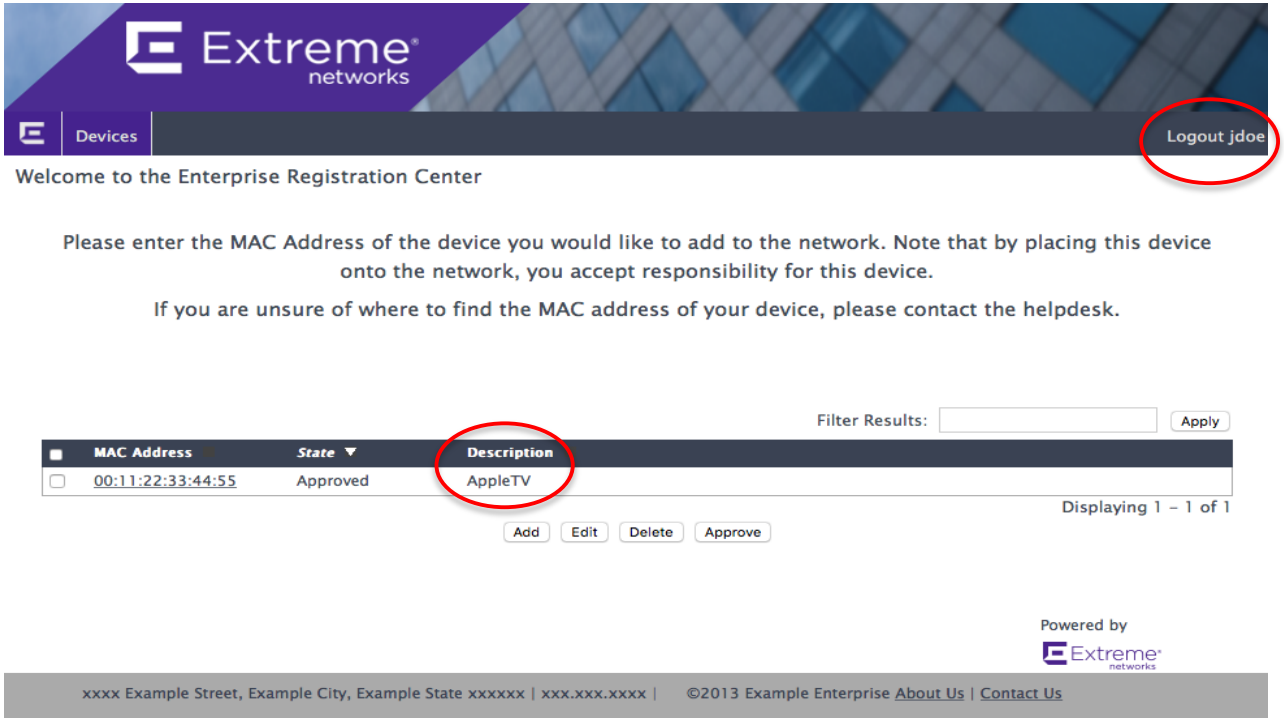
- Extreme 三點定位可提供使用者/IoT裝置定位，威脅 / Rogue AP 定位
- Extreme Area Notification可以偵測IoT裝置被移出指定位置後告警

ExtremeControl IAC - 彈性的BYOD 解決方案

- 簡單易用，適用於有線及無線的環境
- 適合多種情境
  - 使用者SSO認證-帳密 + 802.1x
  - 使用者/訪客網頁註冊
  - Facebook註冊
  - 裝置認證 – MAC + Location
  - BYOD - 帳密+Device Type + Locati
  - IoT裝置 - OS+MAC
  - 穿戴式裝置 – 自我註冊Portal

ExtremeControl IAC - 提供自我註冊

- 自我註冊IoT設備
- 可追蹤該IoT裝置的使用者
- 可限制使用者可註冊最大的設備數量
- 自用者可管理自己的IoT設備
- 無需管理者介入



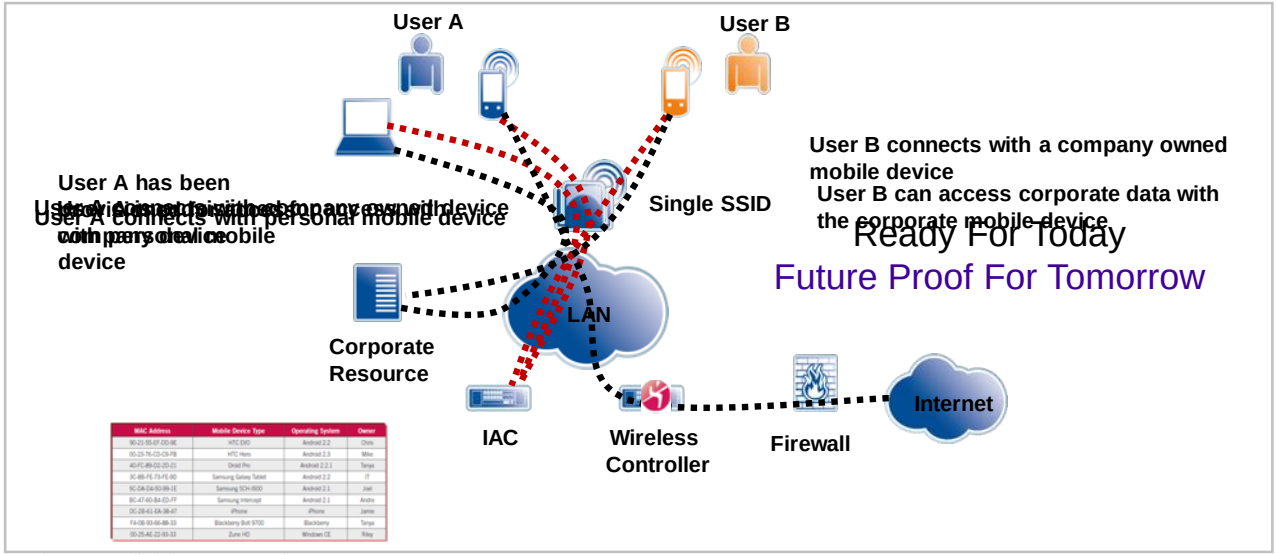
ExtremeControl IAC - BYOD/IoT裝置控管

控管所有使用網路的使用者及IoT裝置

人、事、時、地、物 - 超過46種屬性來決定使用者及IoT裝置權限

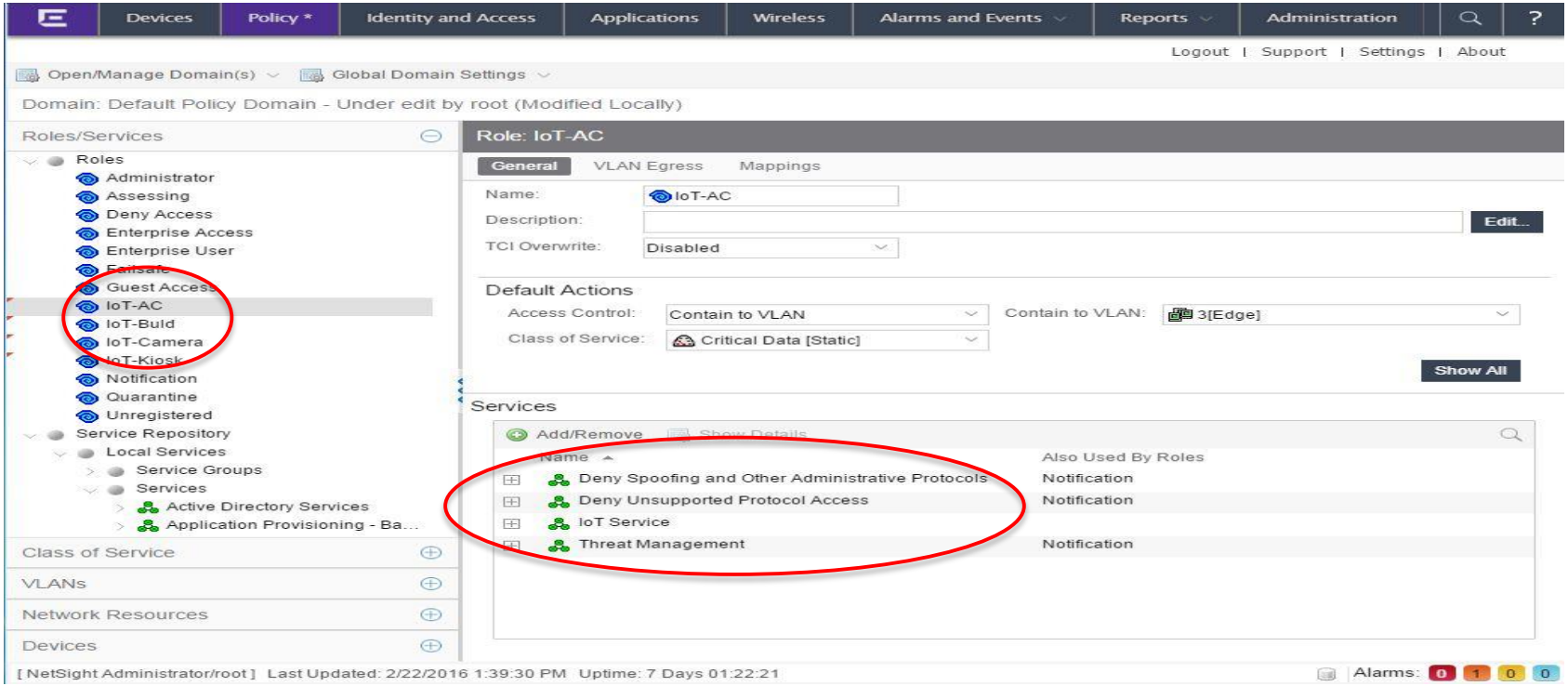
確保使用者及IoT裝置擁有獨立的拓樸架構、頻寬保障、存取權限

單一SSID配置，減少網路使用者困擾



ExtremeControl - 圖型介面設定Role及套用即生效的Policy

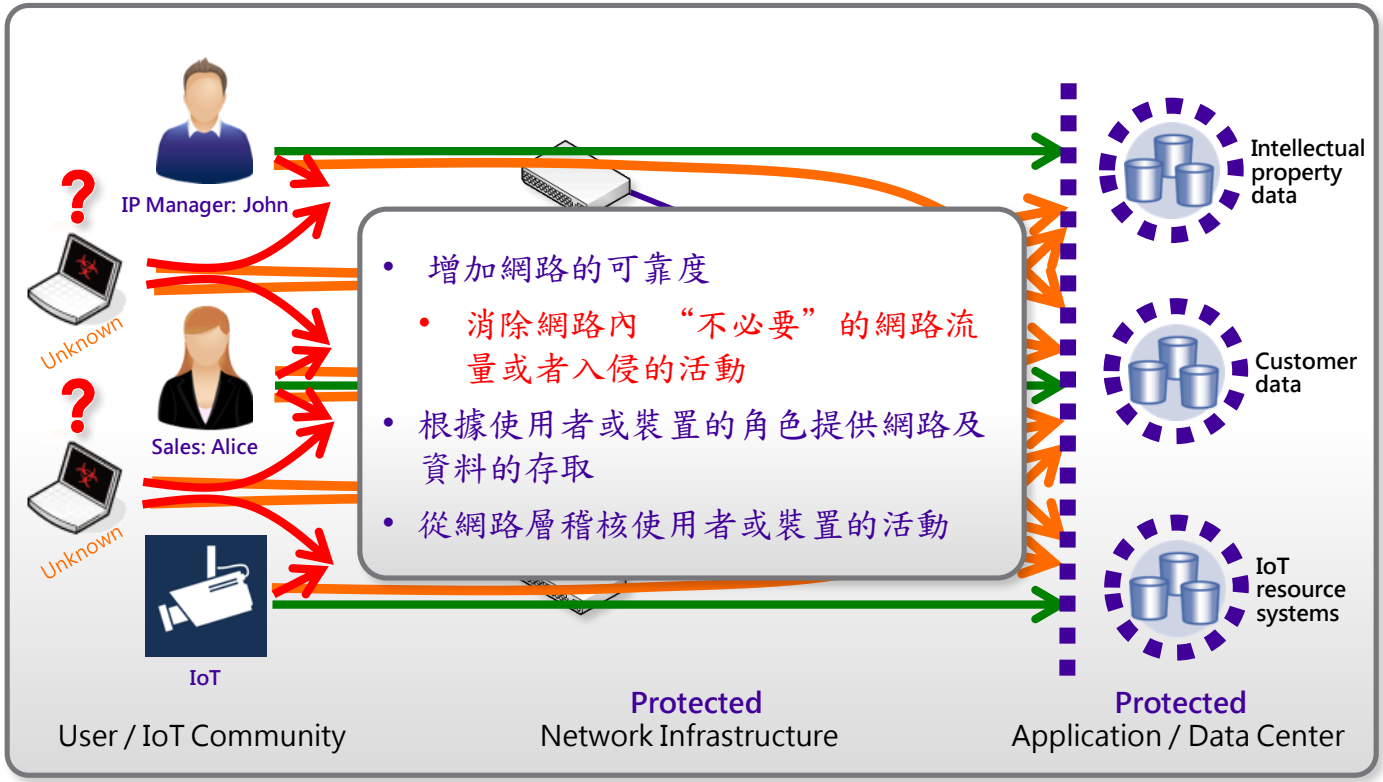
IoT裝置的數量眾多，一定要有個可以集中修改有線/無線Policy及即時套用存取權限的能力



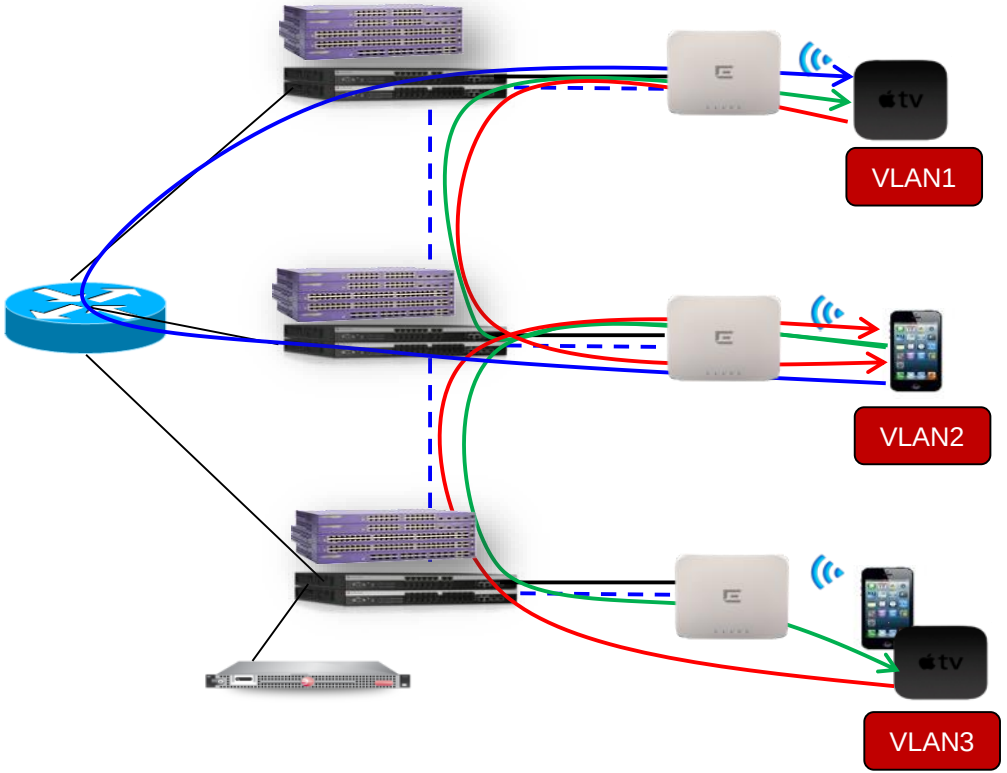
ExtremeControl – 定義Policy Role

- IoT Role：
  - 只能與其特定伺服器溝通（上下載資料）
  - 禁止IoT Role非必要的網路埠（IoT的個人防火牆）
  - 禁止IoT裝置間直接溝通（可避免被駭的IoT影響其他的IoT）
  - 限制IoT角色可使用頻寬（保持其應有的頻寬，降低有可能IoT成為攻擊來源造成其他設備的影響）
- IoT Manager：
  - 不同的IoT Manager只能管理自己負責的IoT裝置
- IoT + Location：
  - 監控IoT設備是否被移動，當設備被移出指定區域可通知管理者
- BYOD = Role：
  - 不同的Role有不同的資源存取權限，如總務的帳號不能用辦公室內以外的裝置如PC、平板登入財會系統
- BYOD + Location = Changable Role Policy：
  - 學生可以在教室內存取電子白板教學系統，在教室以外的地方如體育場或宿舍則不行

ExtremeControl - 透過存取控制可以優化網路環境



ExtremeWireless- *優異的*Multicast流量處理



- 根據流量的類型將封包送到指定的**VLAN**
- 相容於任何品牌的有線網路環境
- 可控制**multicast**的流量
- 沒有單點失效的風險
- 沒有擴充的瓶頸點

- 多媒體應用
- 數位教學、電子白板畫面的分享
- 一般教室及電腦教室
- 會議室

ExtremeAnalytics - 大數據及資料分析

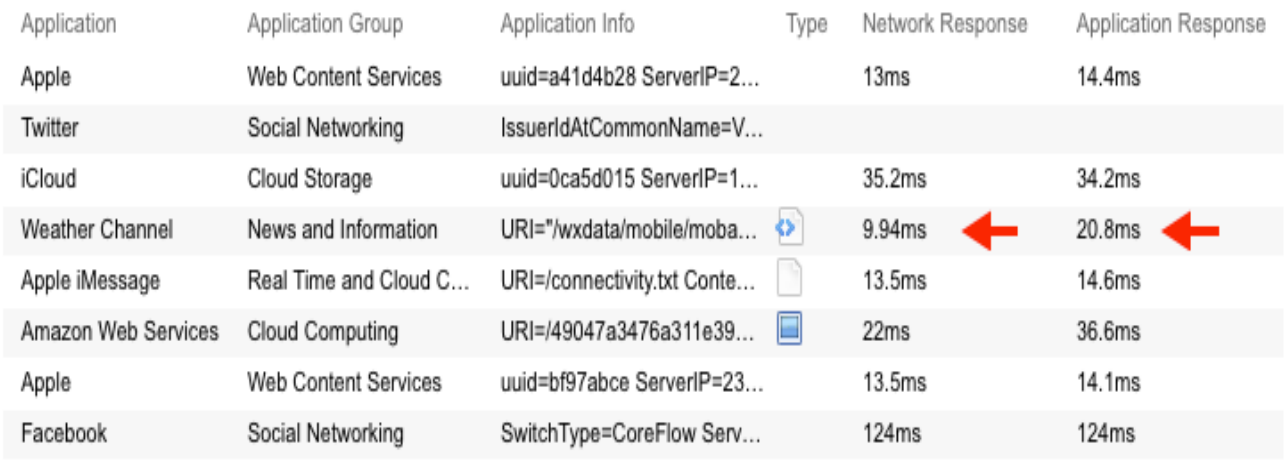
越來越多的資訊透過網路傳遞

- 如何預見網路資源的分配？
- 如何優化網路的架構？
- 如何提供更好的內部及外部使用者的使用經驗？
- 如何從中獲得更多的可用資訊提供決策判斷？

Start Troubleshooting in the Right Place

Extreme networks

Application Response Time: 透過網路回應時間與應用回應時間快速定位問題點



Top Applications by Flows and Bandwidth

Extreme networks

Dashboard | Application Flows | Fingerprints

Appliance: NOC Sensor | Applications Browser Dashboard

Start: 01/15/2014 11:00 AM

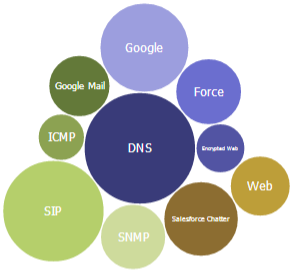
提供從不同面向（頻寬使用、Flow、使用者群組、位置）了解網路應用情形

Top Applications by Bytes

Applications -> Total: 67.42 GB

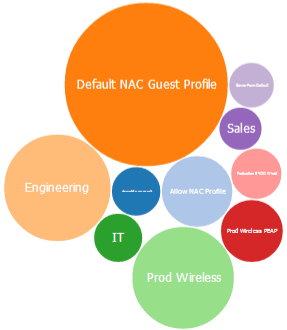
Top Applications by Flows

Applications -> Total: 1618055 flows



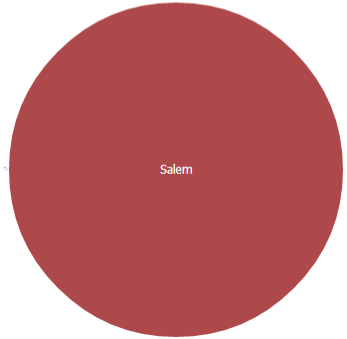
Top Profiles by Bytes

Profiles -> Total: 109.21 GB



Top Locations by Bytes

Locations -> Total: 119.36 GB

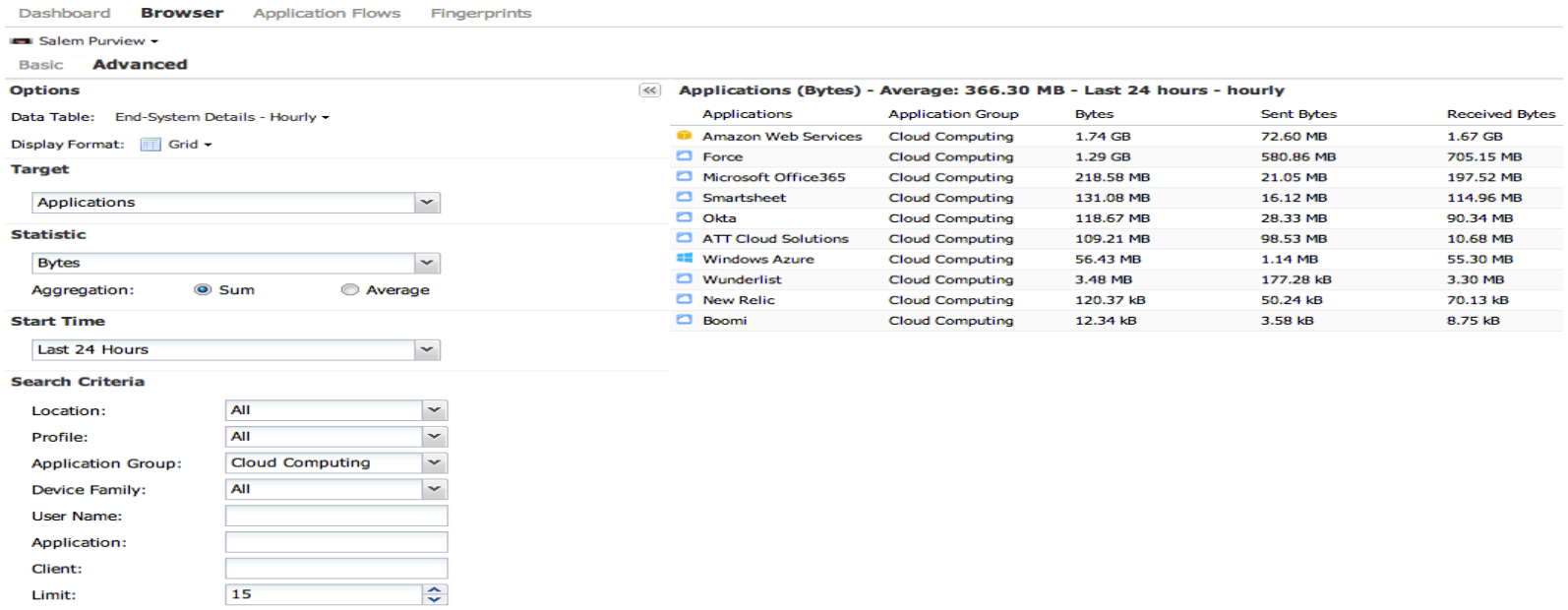


[Read-only/demo] Last Updated: 1/15/2014 11:05:41 AM Uptime: 0 Days 03:42:13

Alarms: 6 0 11 0

了解重點應用程式的使用情形

了解IoT Group和Cloud Computing應用的使用狀況



Average Bandwidth Usage for User Profiles

可觀察學生使用EOR的趨勢或是內部重要應用程式ROI的呈現與差異追蹤

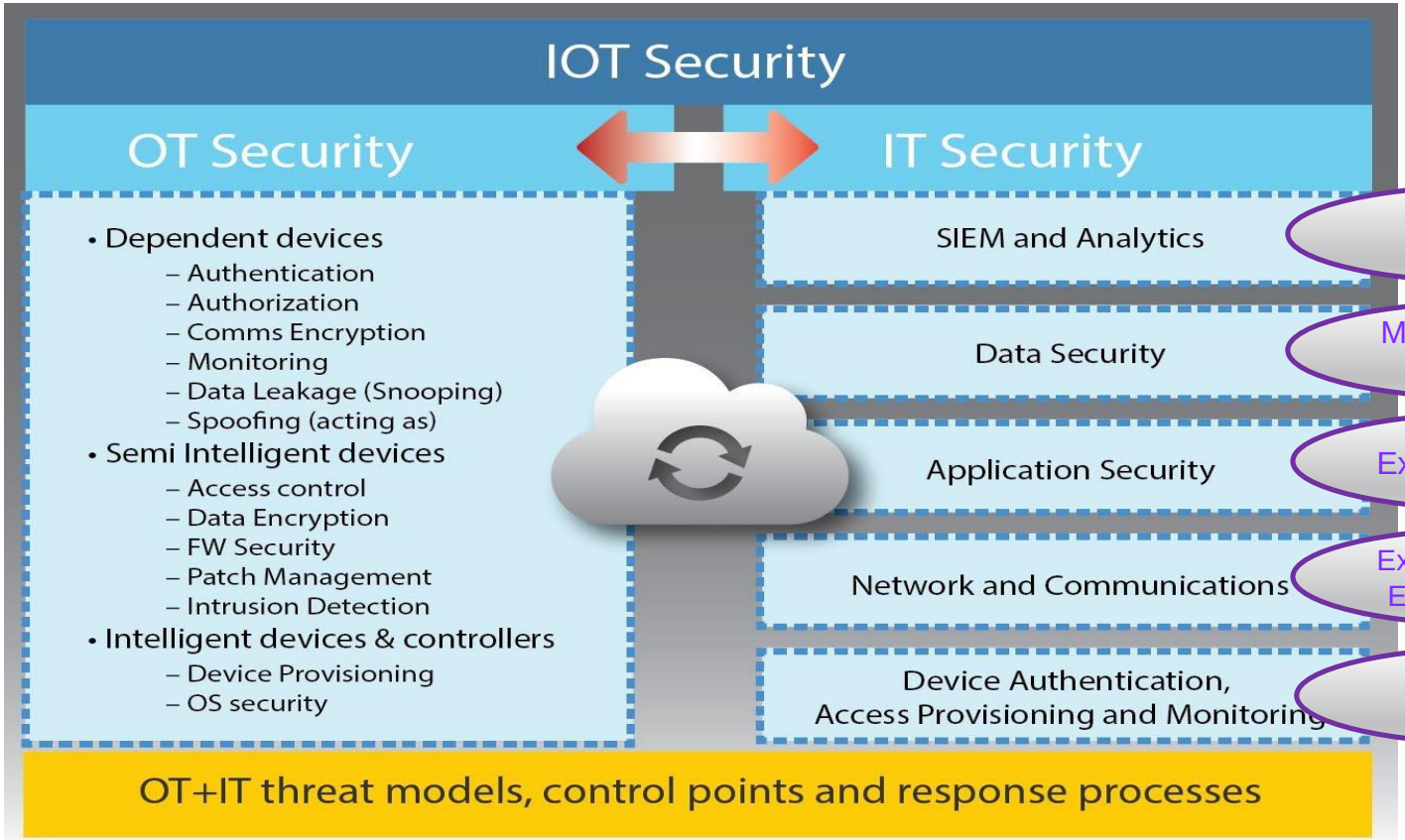
ExtremeSecurity - 資訊安全整合系統

- 資安事件預防
  - 弱點掃描（主動掃描內網設備的漏洞及提供修復方式）
  - 風險管理（主動察覺網路和系統設定上的漏洞與風險及模擬攻擊行為）
  - 威脅情資（從雲端資料庫主動更新外部威脅情資）
- 資安事件偵測
  - 資安事件警告（依優先權排序）
  - 不同平台事件記錄與分析（IoT Server、防火牆、IPS、Router、Switch、Server…）
  - 網路封包資料分析（Flow）
- 資安事件稽核
  - 資安事件查詢、追蹤、舉證
- 資安聯防
  - NetSight（NAC）、Switch、Firewall、IPS

Extreme Total Solution提供的優勢

- 降低維運負載
- 即時有效的集中政策控管
- 應用分析
- 資安事件監控管理
- 實體安全

Extreme Total Solution對應IT Security



SIEM

MACsec/802.1x/
WPA

ExtremeAnalytics

ExtremeSwitching/
ExtremeWireless

IAC/Dynamic
Policy

Agenda

- IoT趨勢
- 校園IoT應用
- IoT面臨的安全性威脅
- 導入IoT的注意事項
- Extreme對應的解決方案
- 結論

結論

- 打造智慧化、資訊化的物聯網校園是未來的趨勢，透過這樣的應用可以提供師生更好的教學環境，更便利的學習方式及更有效率的政策執行。Gartner的副總裁分析師Jim Tully博士表示，「物聯網的價值是由服務來驅動」。所以當它帶給我們更便利、更智慧的生活的同時，單位必須確保該價值不會因為不安全的產品，不適合的網路架構，不當的使用給破壞。讓我們做好準備迎接這波物聯網世代的來臨。

Better Connections. Better Experiences.
For Everyone.

Extreme networks

WWW.EXTREMENETWORKS.COM