AIoT 引動應用商機 也點燃資安烽火

■文：任芷萍

資策會產業情報研究所 (MIC) 資深產業分析師兼產品經理童啓晟預言，隨著雲端運算、萬物聯網、5G 的快速發展，未來 IT (資訊科技)、OT (營運科技)、CT (通訊科技) 結合人工智慧 (AI) 分析機制應用在各種場域，包括製造、金融、醫療、零售、交通、能源等關鍵基礎設施的資安產品及服務，乃商機所在；但網路的無所不在，也讓資安風險急速擴大。

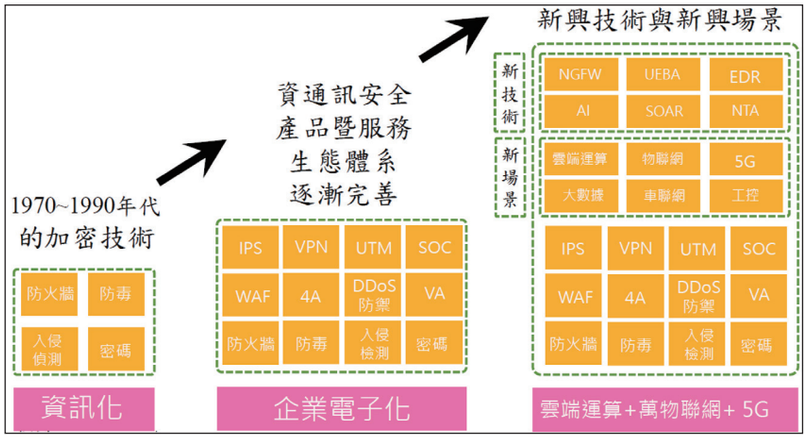
童啓晟樂見，新技術與新場景分別帶動資安產業的下一波成長。1970 ～ 1990 年代，從資訊化到後來的企業電子化、再到今天的萬物聯網和 5G，技術基本上沒有太大變化，但仍有技術隨之興起。這些新技術搭載在原有技術框架上，會產生一些應用場域 (新場景)；這對駭客來說，這就是一個絕佳的試驗裝置。攻防之間，這些新技術和新場景就是帶動資安產業成長的力量，在 AIOT 促使雲端 (Cloud) 和網路 (Cyber) 深度融合的同時，智慧科技與應用亦將加速資安技術的深度融合；繼網路、運算、儲存之後，網路安全已成第四大 IT 基礎設施。

雲端資安威脅增，「託管安全服務」需求大

從產業宏觀角度來說，併購是企業跨域、跨業結合與轉型升級的一個速效手段；通訊大廠博通 (Broadcom) 吃下賽門鐵克 (Symantec) 企業安全部門、法國航空航太公司 Thales SA 買下全球最大 SIM 卡廠商金雅拓 (Gemalto) 皆是指標案例。就 2019 年被併購方的資安次產業觀察：資安服務供應商佔 30%、身份與存取管理佔 22%、網路與端點安全佔 15%、反惡意軟體佔 11%，可反應出產業趨勢。有趣的是，這些併購案並非由傳統資安軍火商主導、而是由私募股權公司進行，且資安已成新興投資標的，國內投信業者亦針對資安發行股票型基金 (ETF)。

童啓晟總結資安有七大發展方向：雲端資安、資料外洩、深偽技術 (Deepfake)、5G 資安、工控資安、勒索軟體 (Ransomware) 和宅辦公資安 (WFH Security)。首先，將工作負載移轉到雲端，正在轉變企業組織對於「託管安全服務」(MSS) 的消費模式，AWS、Google、Microsoft、Oracle 和 Rackspace 等雲端服務大廠相繼開始增強其 MSS 產品。以軟體即服務 (SaaS) 形式提供的 MSS 產品將有越來越多的市場需求，包括：身份與存取管理 (IAM)、安全郵件

圖 1：新技術與新場景將帶動資安產業下一波成長



資料來源：資策會 MIC (2020/05)

表 1：2019 十大資安併購案

	併購方	被併購方	觀測重點
1	Broadcom	Symantec企業安全部門	以107億美元收購，為2019年最大的資安併購案。2020年1月Broadcom再將其將網路安全服務部門拆售給Accenture，在這項交易後，Symantec企業安全部門將整併到Accenture資安服務部門下
2	Thales	Gemalto	Thales 2017年12月宣布以56億美元收購Gemalto，歷時15個月後在2019年4月完成併購
3	Francisco Partners, Evergreen	LogMeIn	私募股權投資公司以 43 億美元收購
4	Thoma Bravo	Sophos	私募股權投資公司以 39 億美元收購
5	VMware	Carbon Black	21 億美元交易案
6	OpenText	Carbonite	14.2億美元交易案。2020年2月Carbonite以 6.18 億美元收購 Webroot
7	F5	Shape Security	10億美元交易案，2020年2月完成收購
8	Jacobs Engineering Group	KeyW	8.15億美元交易案。Jacobs Engineering Group計劃將 KeyW 整合到其航空、技術與核能業務中，擴大其在情報、網路及反恐領域的服務
9	Insight Venture Partners	Recorded Future	7.8億美元交易案。Insight Venture Partners擁有眾多的資安公司投資組合，包括對Tenable、OneTrust、Thycotic、Darktrace及SentinalOne的所有權或投資
10	Orange	SecureLink	5.77億美元交易案。繼2018年AT&T以6億美元收購AlienVault之後，又有一家電信公司進入了資訊安全領域，2020年2月又收購了英國的SecureData

資料來源：資策會 MIC (2020/05)

表 2：歷年十大資料外洩事件

企業/機構	外洩的資料筆數	資料外洩日期
Yahoo	30億	2013 年 8 月
Mega	27億	2019 年 1 月
Weibo	5.38億	2019 年 1 月
Starwood Hotels & Resorts Worldwide	3億	2018 年 11 月
Equifax	1.455億	2017 年 7 月
eBay	1.45億	2014 年 5 月
Heartland Payment Systems	1.34億	2008 年 3 月
Target	1.1億	2013 年 12 月
TJX Companies	9,400萬	2006 年 12 月
JP Morgan & Chase	8,300萬（7,600 萬家庭與 700 萬小型企業）	2014 年 7 月
Uber	5,700萬	2017 年 11 月

資料來源：資策會 MIC (2020/05)

管理、分散式阻斷服務 (DDoS)、事件檢測和回應，以及資安資訊與事件管理 (SIEM)。

童啓晟分析，雲端資安主要問題是：資料的遺失與洩漏，包括不適當的權限控管所造成的未授權存取、不安全的應用程式介面 (API) 及雲端錯誤配置等，連帶使需求端的雲端威脅持續增加，促使雲端資安產品在五年內可能成長三倍！身為供給端的軍火商當然不會錯過這個大好形勢，伺機尋求外援、截長補短：2019 年 10 月，趨勢科技 (Trend Micro) 以 7,000 萬美元收購雲端安全新創 Cloud Confomity；今年 2 月，惠普 (HPE) 買下雲端安全新創公司 Scytale。其次，資料外洩也成為歸納重點，且由單點外擴至整個打擊面。

「資安合規」成爲未來 5G 市場決戰關鍵

網路犯罪集團竊取資料的目的不外乎：製作偽卡、進行詐騙、冒用身份、恐嚇取財等。前不久視訊軟體 Zoom 爆出 53 萬筆帳密流入暗網 (黑市)，受害者遍及摩根大通、花旗銀行及學校等機構；萬豪酒店 (Marriott) 員工帳密遭駭，有 520 萬筆客戶資訊可能因此外洩……，皆曾引發資安恐慌。另一個幾可亂真、防不勝防的是深偽技術，收集目標人物的公開影片或音訊，利用 AI 學習、模仿聲音，或假冒信件格式欺騙企業進行轉帳皆屬此類。童啓晟揭密，Deepfake 影片可經由臉部模糊度、不規則眨眼頻率來辨識 (Deepfake 影中人幾乎不眨眼)。

童啓晟指出，AI 對於資安就像一把雙面刃，雖有人以之作惡，但也有資安公司用 AI 進行詐騙分析、優化防禦策略。另一方面，為支撐多元化業務，5G 網路大

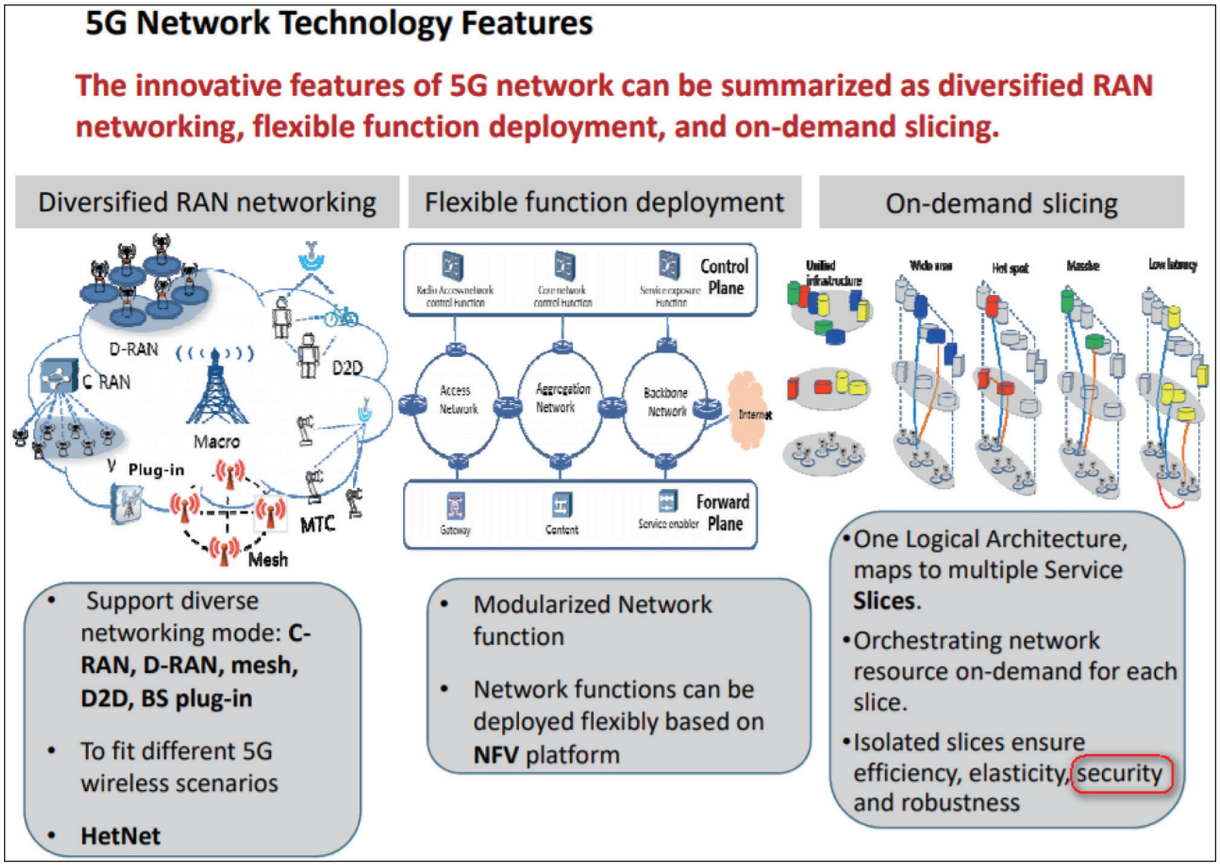
量使用軟體定義網路 (SDN)、網路功能虛擬化 (NFV)、網路切片 (Networking Slicing)、多接取邊緣運算 (MEC) 等新技術，使網通設備漏洞成為5G服務的不穩定變數；業者尤其關心「資料在地化」議題，因為各區域法規不盡相同且罰則相當重，「資安合規」已然成為未來 5G 市場決戰關鍵。面對 5G 多元技術發展，廠商應針對不同市場需求調整策略、進行佈局。

例如，歐盟《一般資料保護法規》(GDPR)、《網路與資訊系統安全指令》(NIS Directive)、《歐盟網路安全法案》(EU Cybersecurity Act) 等資安監管措施；美國加州的《萬物聯網裝置的資訊隱私法案》、《加州消費者隱私法案》以及今年 3 月白宮新頒佈的《美國保護 5G 安全國家戰略》和《保護 5G 安全國家戰略》。與此同時，工業 4.0 讓封閉式工控環境逐漸開放，與網路的連接頻率也提高，頓成駭客覬覦目標。近年全球工控資安事件頻傳，手法也更為刁鑽，德國煉鋼廠、伊朗核能設施、烏克蘭電網、越南航空站、美國水廠和捷運系統都曾慘遭毒手。

資安轉型＝防禦復原力，開發系統之初就得擬定架構

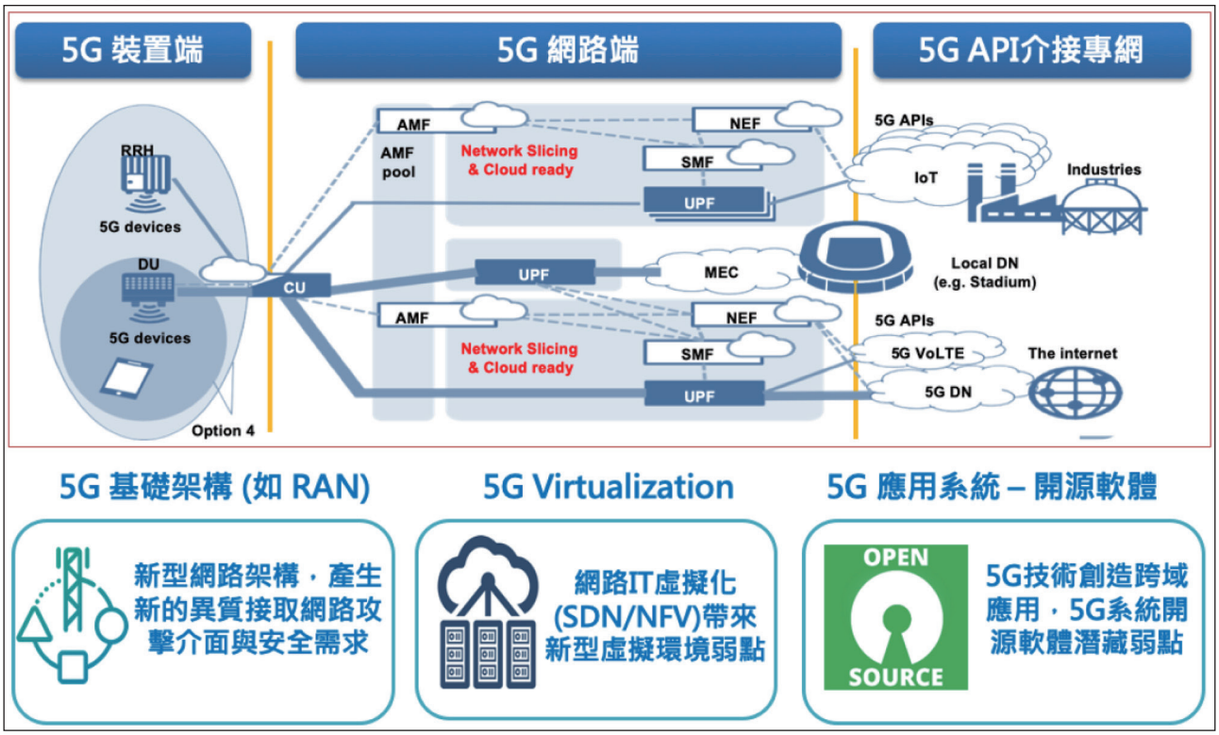
童啓晟建議，OT 資安有三大策略：隔離管制 (Segmentation)、可視監控 (Visibility) 和關鍵保護 (Secure Mission-Critical Assets)；勒索軟體的威脅亦不可輕忽，它們不再只是將電腦資料加密以獲取贖金，也開始向家庭物聯網下手。在肺炎疫情爆發後，因為生活方式的改變，資安防護商機更加湧現，防疫與防駭將並駕齊驅、同等重要，應從維運管理、應用服務、裝置設

圖 2：5G 網路技術特性——分散式無線存取網路 (RAN)、彈性功能部署、隨需切片



資料來源：https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2019/ITUPITA2018/ITU-ASP-CoE-Training-on-/5G%20networks%20and%203GPP%20Release%2015_vf.pdf (2019/10)

圖 3：5G 資安挑戰



資料來源：資策會 MIC (2020/05)

備和基礎架構多管齊下。最後談到企業資安轉型策略的佈局思維，童啓晟主張聰明的企業資安準則是「零信任」(Zero Trust)——預期被駭客攻擊並制訂因應計畫、而非事後才被動亡羊補牢。

資安轉型的地位等同「防禦的復原力」，必須量身訂做、風險校準程式與投資，讓技術面和管理面相輔相成，制定企業持續營運計畫 (BCP)，即所謂的「資安左移」(Security Shift)——開發系統之初，就要把整個架構擬好。未來整個資安產業會強調「無邊界安全性」。從這次疫情就能體會：數位邊境越來越模糊，建立對資安的基本認識和意識，將是日後企業數位邊境防禦的關鍵；因為人往往是資安最脆弱的一環，而對未來的不確定性，將是資安最大威脅。資策會資安所創新通訊安全中心主任林志信補充，5G 深入垂直領域後，資安的重要性更有增無減。

首當其衝的是，若外銷產品有安全性漏洞會被開罰，網通設備在外銷前必須經過安全檢測、甚至要出具報告才能避免受罰；其次，智慧工廠、自駕車等關鍵場域，更是容不得停機風險；再者，5G 不再是純硬體解決方案，開源軟體的廣泛應用，也可能成為資安弱點。在 5G 實踐萬物相連後，資安威脅恐從謀財進階為「駭命」。林志信表示，就行動網路架構演進來看，4G 為降低成本，已開始嘗試將部署在外的基地台輕量化、將重裝運算資源集中在雲端中心的分離作法；5G 進一步導入虛擬化網路，盡量用軟體解決、便於更新，開放式伺服器繼之而起。

5G 資安三面向：裝置端、網路端、API 介接專網

林志信摘要，5G 資安涵蓋三個面向：裝置端、網路端和 API 介接專網。裝置端須符合 3GPP 及個別產業的資安規範；網路端可能有系統面的安全疑慮，包括核心網設置及 API 規範；開放式無線接取網路 (RAN) 的品質保證。5G 導入 SDN/NFV，與異質接取網路之新型網路技術架構，IoT 設備間亦有多種接入方式，若遭到惡意程式感染更加難以追蹤、且易產生資安

破口。早在4G時代，就曾出現在合法的手機與基地台之間偽設一個假基地台，誘使手機連到假基地台後，利用上傳真實資訊、以假手機去跟真的基地台連線，形成「中間人攻擊」(MITM)。

此類攻擊多半是衝著特定對象而來，以明文傳送的SIM卡id資訊將被一覽無遺；所幸，最重要的國際移動用戶辨識碼(IMSI)因加密而不至於讓人全盤掌握，惟仍存在以下風險：發送網址的譯文遭到竄改，誤導用戶至其他惡意網站、植入木馬。有鑑於此，5G補強措施包括：

1. 在SIM卡多加入一把營運商的公鑰，即使有假基地台存在，也無法獲知IMSI資訊；
2. 金鑰架構強化，5G核心網與終端之間多一個邊緣設備(Edge)，會有許多開放介面，故5G多設一個AKA(認證和金鑰協定)作為保護層；
3. 資料傳輸加密簽章，4G只有做加密、沒有簽章，而5G兩者兼具。

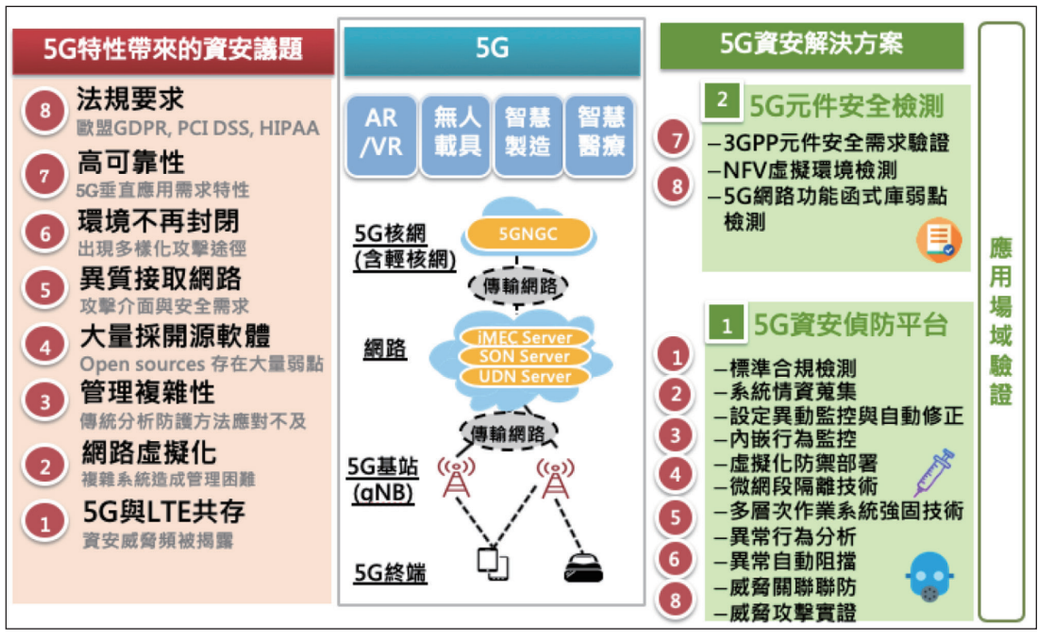
林志信說明，行業法規對網路系統有多方規範，例如，工控傳輸訊令的封包必須能分析到網路第七層(應用層)，統整5G資安解決方案有兩大主軸：1. 事前元件安全檢測，包括3GPP元件安全需求驗證、NFV虛擬環境檢測、5G網路功能函式庫弱點檢測；2. 專網維運中的資安偵防平台，必須了解網路狀態、即時監控、查核是否照原定藍圖在運作，有兩大議題：一是怎麼確保元件是安全的？二是如何持續監控網路系統？不只核心網、還包括終端裝置。因為終端聯網裝置多採用同系統，一旦出現漏洞、被植入惡意程式，擴散速度更為驚人。

金融機構：每天都在應戰資安威脅

林志信特別提到，核心網因為有MEC能力，可上架一些APP，資料有被不法管理者收集的風險，管理不可不慎。不同應用有不同要求，常見的威脅類型有：偽冒身份、資料竄改、抵賴、訊息洩漏、服務阻斷、權限提升、橫向擴散。在評估風險等級後，據以制定管理方法、預測剩餘風險並判斷是否需要額外管理機制。金融體系向來是駭客的頭號目標之一，台新金控資訊長暨資安長孫一仕透露，其間甚至不乏「國家級駭客」蹤跡，他們的攻擊手法非常多樣、且可用資源非常多，為金融業帶來莫大壓力；今年，忽悠人的「詐騙型」的勒索病毒又有增加之勢。

駭客入侵手法相當多，郵件、網頁、虛擬私人網路(VPN)皆是途徑，尤其是企業控制員工帳密的網路伺服器一旦被駭，很容易被取得高權限、在企業內部散播病毒或發動假交易且通常潛伏很久。雲端運算也是金融業所關注的技術焦點，以達到兩個目的：減降及營運彈性，在短時間

圖4：5G資安議題



資料來源：資策會MIC (2020/05)

內擴大營運效能，但資安是不容妥協的先決條件。企業物聯網也成為金融機構挑戰：預估今年 IoT 設備將達 200 億個，卻無特定安全框架或法規來規範資安事項及資料的安全性；而這些設備多是簡單設計且廣佈各地，供應商本身又缺乏定期補丁、解決漏洞的資源和能力。

孫一仕描述，業界目前的作法是：定期檢視相關的設備資安漏洞，同時以隔離網段的方式將物聯網設備跟正規營運網路切分——先前就發生過金融機構的錄音設備，因為網段關係形成資安破口。為因應潛藏的資安風險，金融機構會採取以下幾項措施以防範：首先是進行「紅藍軍演練」——紅軍是指金融業安排的外部專業資安機構，藍軍乃銀行本身，由紅軍對藍軍發起生產環境上的「有限度攻擊」(在不影響正常營運下)，以便及早找出潛在的資安漏洞並加以填補；其次是針對國內外曾發生的 ATM 威脅，進行實地演練，確認是否已有防護措施。

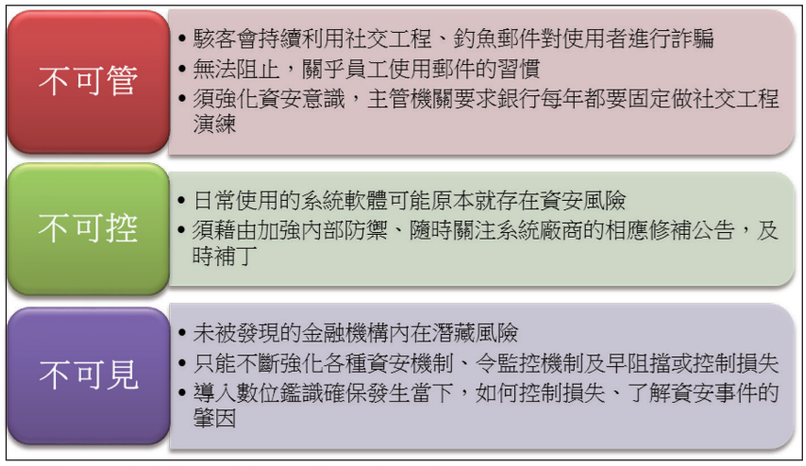
完整資安防護體系&完備處理流程作業

緊接是「滲透測試」(Penetration Test, PT)，以駭客思維模擬可能的攻擊環境，嘗試找出潛藏的資安漏洞，有別於「紅藍軍演練」由外而內攻堅，滲透測試著重模擬已成功進入內部的駭客，意欲何為？下一個攻防要點是「進階式持續威脅」(APT)。現在的 ATM 攻擊已非用單一手法、在特定時間點進行，有些攻擊會長達 3 ～ 6 個月、耐心尋找破口。曾有成功取得最高權限的駭客一面製造勒索病毒的「假象」，讓銀行徒耗心力在排除勒索病毒的工作，一面又聲東擊西、大肆進行假交易將存款轉出；金融機構服務通路廣、客戶群龐大，對抗 APT 是重要一環。

最後一項是 DDoS 攻擊——最簡單的即是以「殭屍電腦」對特定對象的網站發出異常大量存取要求而癱瘓服務。過去幾年有不少國內機構曾身受其害，需借助流量清洗 (Clean Pipe) 解決，但有時間和頻寬限制；所以，金融機構本身也要進行 DDoS 演練，以便攻擊發生時能及時因應。孫一仕呼籲，面對這麼多可能風險，要有完整資安防護體系。以辨識、防護、偵測、回應、復原等不同階段為橫軸，「防範資安風險的環節」為縱軸——包括：使用者、資料、網路、應用程式及設備，資安技術 vs. 人員投入和處理能力的權重佔比，會有階段性的差異。

然而，不管在哪個階段，都要有完備的處理流程。資安威脅對金融機構而言，每天都在發生，事到臨頭能否快速回應就非常重要。孫一仕建議：1. 成立資安應變小組，成員應涵蓋不同部門的專業，甚至連對外關係都需進來；2. 成員從一開始就要了解自己的任務、各司其職，方可有條不紊地迎戰；3. 訂定資安應變的標準作業流程 (SOP)，成員才不會無所適從，且要安排資安災害的定期演練，檢視原有 SOP 是否需修正；4. 建立資安監控中心，從多面向監控資安威脅，及早示警、降低損失。一言以蔽之，了解、面對、因應，是與身處風險環境的生存之道。 CTA

圖 5：金融資安風險



資料來源：台新金控資訊長暨資安長孫一仕；筆者整理

5G 智能邊緣肩負重任 嵌入式系統的資安怎解？

■文：任芸萍

5G 時代正式來臨！但眾所期盼的高頻寬、低延遲，恐將對物聯網 (IoT) 連接更具破壞力，網路即時檢測迫在眉睫。5G 資料中心需支援自動化和雲端技術，讓內容服務供應商 (CSP) 可透過加值服務做配置和管理，為用戶 IoT 設備提供在線安全保護，或由用戶自行控管帳戶中的 IoT 設備訪問權限。然而，5G 從集中式網路過渡到軟體定義網路 (SDN) 的過程，由於少了居中的網路監控檢查點，將使網路漏洞更加複雜；所幸，虛擬網路的「安全即服務」(SaaS) 平台可讓用戶遠端獲取安裝或更新，營運商亦可用機器學習識別、消除各種應用程式威脅。

ResearchAndMarkets 預估到 2025 年，全球 5G 安全市場總額將達 65 億美元，「基礎設施安全」是營收貢獻最高的分眾市場，達 25.6 億美元，而「通訊安全」是增長最快者，年複合成長率 (CAGR) 為 49.2%。5G 的另一個重要標記是邊緣運算 (Edge Computing)，結合物聯網、雲端和邊緣運算，保護在容器 (Container) 中運行的設備、應用程式和微服務的安全需求變得更加重要，而公鑰基礎結構 (PKI) 是有效且具有成本效益的方式，例如，以某種方式將身份綁定到密鑰、對某些內容進行身份驗證。這幾年，「私有路由 PKI」的需求正在激增。

Arm「PSA」：爲物聯網奠定平台安全架構

多數組織希望藉此明確限定誰能獲得憑證並控制設備，造成導入更多依「產品線」為單位的信任根 (RoT) 碎片。因為物聯網製造商並不想讓旗下設備與用戶其他 IoT 設備在相同的信任根上驗證身份；反之，多數用戶也傾向將不同設備予以適度區隔。著眼於物聯網碎片化特性，在邊緣設備市佔甚高的安謀 (Arm) 於 2017 年發表首個通用框架——平台安全架構 (PSA)，意在為萬物聯網奠定信賴基礎，讓 Arm-based 產品能在共同的安全基礎上互通，由分析、規劃 (設計)、執行和認證四階段組成，可提供具代表性的物聯網威脅模式及安全性分析。

圖 1：Arm PSA 四大階段

資料來源：https://developer.arm.com/architectures/security-architectures/platform-security-architecture；筆者整理

PSA 讓硬體與韌體規格皆可建構在關鍵安全原則的基礎上。特別一提的是：PSA 不受作業系統種類限制，可支援 Arm 旗下所有即時作業系統 (RTOS) 和 Arm Mbed OS 物聯網作業系統，以及軟體廠商夥伴的作業系統。其中，執行階段的三組 PSA API，可確保跨設備硬體信任根實現跨應用程式 (互操作性)，包括 RTOS 和軟體開發人員的 PSA 功能 API、安全專家的 PSA 韌體框架 API，以及晶片製造商的 TBSA API。Arm 還為其安全 IP 系列產品新增兩項元件：

- Arm TrustZone CryptoIsland：在晶片內部運行的智慧卡層級安全機制，CryptoIsland-300 為第一代解決方案，鎖定需要高層級分析與安全性的應用，包括低功耗廣域網路 (LPWA)、儲存及車用等；
- Arm CoreSight SDC-600 安全除錯管道：SDC-600 整合一個專屬的驗證機制用來除錯存取，支援完整除錯功能且不損及系統安全，在物聯網裝置的各個生命週期階段皆適用。

Arm 隨後在 2018 年推出首套 PSA 威脅模型與安全分析 (TMSA) 文件——考量哪些資產該受到保護？推測可能遭遇到的威脅？面向一些熱門物聯網裝置 (如：智慧水錶、網路攝影機、資產追蹤裝置) 發表新 TMSA 範本以及開源參考實作韌體「Trusted Firmware-M」(支援 Cortex-A 應用處理器)，從基礎架構到部署建置皆包羅在內；Arm 並設立專案軟體開發團隊，專門負責適合連結 MCU 的安全處理環境 (Secure Processing Environment, SPE)。解決了基本的資安結構問題，「合規性」是另一挑戰，尤其是面臨區域性法規的歧異。

GlobalPlatform SESIP：助力「合規性」認證

由安全數位服務和設備標準行業協會 GlobalPlatform 發佈的「物聯網平台安全評估計畫」(SESIP) 定義了可信賴評估 IoT 平台安全性和終端設備安全性的獨

圖 2：SESIP 五個保證級別、標記和定義

資料來源：https://trustcb.com/iot/sesip/；筆者整理

立認證標準，在提供合規性框架方面處於領先地位，涵蓋許多最佳實踐準則和法規要求，包括：美國 NISTIR 8259 建議、歐盟 EN303645 標準、英國針對消費者物聯網的法規建議安全性，以及俄勒岡和加利福尼亞 (SL-327) 物聯網安全和數據收集法律，讓最終用戶可循設備的獨立審核安全聲明作為選購依據，設備開發人員亦可借助預先認證的組件，經濟高效地滿足安全要求並加速上市。

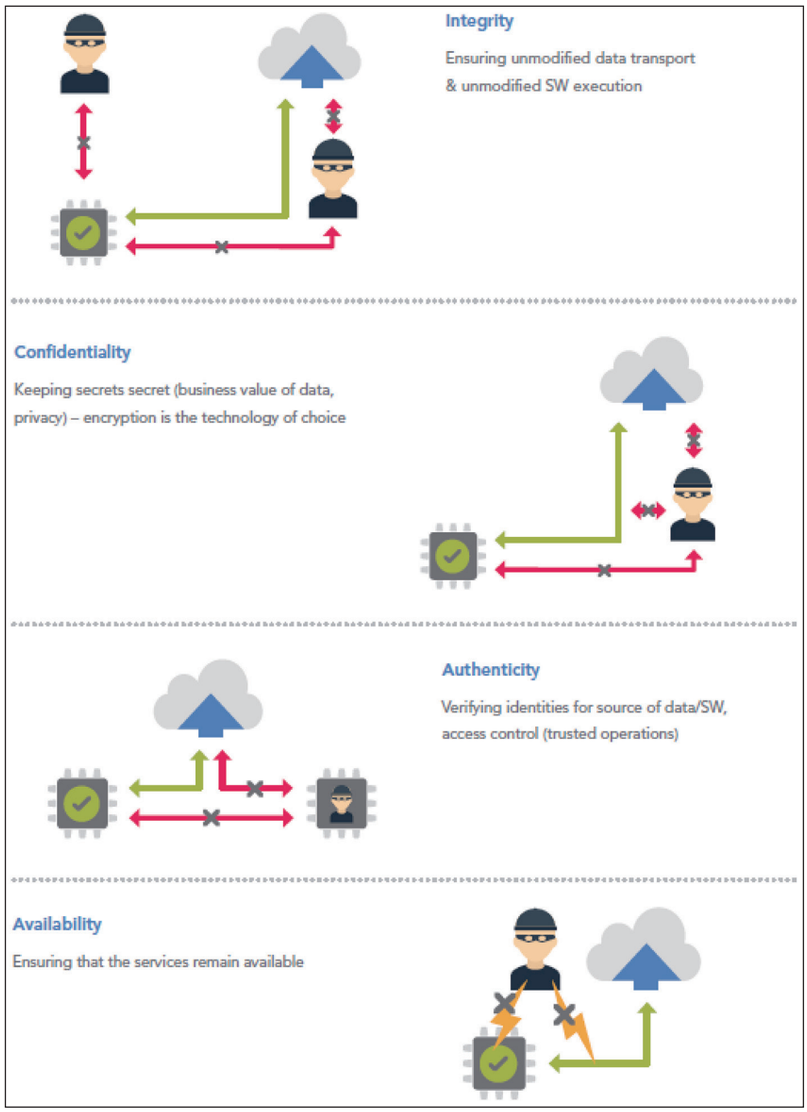
這將有助營運商採購、保險並提高對供應商安全聲明的可見性以管理網路風險。SESIP 旨在對單個物聯網平台組件進行認證，提供安全功能及其抵禦實體、邏輯和軟體攻擊能力的認證。SESIP 平台歸 TrustCB 所有，它也是 Arm PSA 的主要合作夥伴，差別在於：Arm 在硬體級別具有很高的規範性，而 SESIP 更偏重於動態認證。RISC-V International 亦與 GlobalPlatform 攜手為物聯網設備 IC 和 SoC 的開發制訂開放標準，包括在受信任的執行環境 (TEE) 中執行程式的處理器。2019 年，與 GlobalPlatform 相容的 TEE 發貨數量較前一年增加 50%。

經由統一規範、已知硬體漏洞訊息交換以及克服這些漏洞所需的功能，使上述合作雙方可更新每個組織的各自技術文檔和框架，以滿足不斷發展的安全要求。預計短期到中期的示例將集中於 TEE 的應用程式介面、微控制器 (MCU) 的保護配置文件和相應的安全性增強，更有利於協作式開源硬體開發。恩智浦 (NXP) 去年同時獲得 SESIP 與 Arm PSA 認證，產品線涵蓋 MCU、應用處理器 (AP) 和交叉處理器 (兼具 AP 性能、MCU 低功耗與即時操作特性)。NXP 表示，如此可將敏感的數據資產與用戶的應用程式予以隔離。

NXP：坐擁 PSA 和 SESIP 認證，亦不缺席國際資安標準制訂

基於 ROM 的安全啓動過程、利用安全儲存設備的密鑰創建硬體信任根的好處是：從硬體引導程式、建立信任鏈、加載程式、操作系統到應用程式軟體的整個軟體堆

圖 3：設計上的安全性取決於——完整性、機密性、真實性與可用性，須將它們組合到系統中以提供端到端的安全性，應對潛在攻擊並兼顧成本及安全效益



資料來源：https://www.nxp.com.cn/docs/en/white-paper/NXP-FROM-IOT-TO-IOTRUST-WP.pdf

疊，每步皆經過嚴謹身份驗證；有數款交叉處理器和 MCU 還集成了 SRAM 的物理不可複製功能 (PUF)。使用 SRAM 固有自然變化生成「按需密鑰」及「可信賴運算群組」(TCG) 定義的設備身份組合引擎 (DICE) 安全標準，可增強 PKI 或非對稱加密的安全性。憑藉這些安全設計，NXP 嵌入式處理器可達到或超過 PSA 和 SESIP 一級標準，部分系列甚至可達二級。

不只坐擁 PSA 和 SESIP 認證，NXP 還與世界各國政府和國際機構建立聯繫，對於協調安全預期、認證、要求和法規助益匪淺——例如，NXP 已與《信任憲章》中的歐洲網路安全組織 (ECSO) 等物聯網主要參與者以及歐盟網路與資訊安全局 (ENISA) 密切合作；同時，積極參與 ISO、FIDO、GlobalPlatform 和 NFC 論壇等標準化組織，以促進安全互操作性。針對關鍵應用，NXP 亦通過 ISO/IEC 15408-1 ...3 等全球安全通用標準和 CC (Common Criteria) EAL 6+ 認證 (註：CC EAL 是目前最全面的評價準則，共分為七級)。

順帶一提，NXP 日前發佈升級版 MIFARE DESFire EV3 IC 產品 (掃描範圍更大、交易速度更快)，其軟、硬體支援開放式加密演算法，也已通過 CC EAL 5+ 認證；它還具有交易計時器可減輕中間人攻擊 (MITM)，並利用唯一「安全獨特 NFC」(Secure Unique NFC, SUN) 訊息傳遞功能，為每次點擊生成唯一的身份驗證訊息，然後將該訊息發送到伺服器進行驗證以防止非法複製。DESFire EV3 將集成到 NXP 的 MIFARE 2GO 雲端服務中，基於 MIFARE 產品的數位化憑證及 NXP 生態系統簡化行動／穿戴設備的集成工作，協助推展非接觸式交易。

WISeKey：邊緣設備智能提高，攻擊面隨之增加

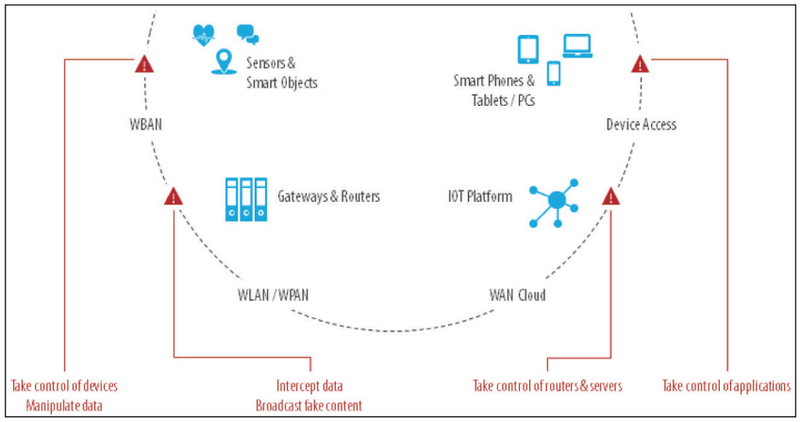
瑞士網路安全公司 WISeKey 相信協同物聯網、人工智慧 (AI)、數據分析、連通性和數位認證工作，可實現早期預警系統 (EWS)。例如，城市、政府和企業可創建一個全球感測器網路，將個人行為與匿名數位身份結合，檢測病毒傳播；但這將需要在全球範圍內進行標準化、安全性、信任、規劃和實施，並強調隱私，擬藉由以下步驟達陣：1. 發行包括真實性數位憑證的儲存設備；2. 加密反映至少一個與物理對象唯一相關的特徵訊息；3. 使用網路電腦，必要時檢查數位真實性憑證的有效性；4. 與驗證或認證機構合作，即時驗證數位真實性憑證狀態。

WISeKey 生態系的數位身份正在讓半導體安裝呈現指數級增長：安全晶片增長到 16 億個、RoT 增長到 50 億套。WISeKey OISTE RoT 是 TCG 的一組功能，RoT 充當單獨的運算引擎、控制嵌入它的 PC 或移動設備的 TCG 平台密碼處理器。RoT 與區塊鏈 (Blockchain) 的結合產生了一個新的 Trust 協定，允許區塊鏈擴展具有嵌入式安全性的可信交易，確保使用 RoT 信任的密鑰對提交到區塊鏈的每個交易做數位簽名，並結合垂直信任流程由信譽良好的第三受信任方透過區塊鏈提供的固有分散式信任進行驗證。

物聯網增加了網路攻擊風險，隨著邊緣設備智能提高，攻擊面也會增加。這種雙重信任模型解決了互聯網最大挑戰之一：彌合當前零散的信任域，包括許多政府使用的現有、不兼容的國家 RoT。一個具體應用是 WISeID，它使用身份的可信分佈式賬本技術儲存對象和人員身份，並為連接的對象提供數位憑證識別、身份驗證和驗證的能力，上述微服務費將藉由 WISeID 令牌收取。在美國，WISeKey 的晶片使用獨特的安全憑證 ID 和 SSH 加密密鑰來保護和認證超過 5,000 萬個路由器。這項技術還用於閉路電視 (CCTV)、數位視訊錄影機 (DVR) 和衛星天線。

IoT 設備晶片設計必須一開始就嵌入安全性，RoT 也必須嵌入連接的設備中；WISeKey 生態系統已擴展到智能卡、智能城市、無人機、防偽、智能照明、伺服器、行動電話等。WISeKey 在 IoT 邊緣擁有獨特優勢：VaultIC Secure Elements 可保護大數據，使用 AI 分析，可幫助工業應用檢測網路安全攻擊或在設備發生故障前預知。WISeKey 一系列通過經 Common Criteria 認證的防篡改微處理器，

圖 4：IoT 擴展方便且可執行許多破壞性的應用程式，卻也為駭客遠程控制設備、攔截／操縱數據、篡改路由器／伺服器，甚至控制應用程式大開方便之門



資料來源：https://www.wisekey.com/solutions/iot-connected-devices/iot-security/

可實現對敏感資產的安全儲存和使用，並在現場唯一標識、認證和保護設備；其數位身份可透過本地 Webtrust 認證的 PKI 或作為雲端服務進行有效管理。

Microchip：無論規模大小，皆應建置嵌入式安全防護

根據《Fortinet 威脅態勢報告》顯示，去年全球 12 件大漏洞、有半數是瞄準 IoT 設備而來；而物聯網網路安全的未來，在於強大的「嵌入式保護」。微芯科技 (Microchip) 亦認為，攻擊數量將持續增長，且越來越多的事物被連接將導致漏洞持續增加，所以需要在設計之初，就為嵌入式系統的所有層級考慮安全措施，包括：設備儲存、通訊硬體和協定、節點 (Node)、閘道器 (Gatewaay)、設備管理系統和雲端運算等。值得留意的是，他們強調：所有類型的系統都需要安全性，但不一定需要相同類型的安全性；定義產品的安全類別，將可更好地評估。

這將確定重大威脅及可採取的保護設計安全措施。Microchip 說明，RoT 在受信任的嵌入式系統中可得到保護，作為保護應用程式的基礎——以密鑰驗證身份。如果密鑰被欺騙，則未經授權或惡意用戶可順勢控制系統交易，後患無窮，故應從最初就正確實現對嵌入式系統的信任。為避免創建偷窺／竊取密鑰的後門，需將加密原始功能和身份驗證密鑰都儲存在設計的安全容器中，Microchip 可配置的安全元件能發揮關鍵作用，且可與任何微控制器或微處理器 (MPU) 搭配使用：基於硬體的密碼加速器，還可顯著減少執行時間和功耗。

這些設備中還嵌入了高品質的亂數產生器和 EEPROM 的安全密鑰儲存。此外，還有防篡改和旁路 (bypass) 信道攻擊保護，阻止對嵌入式系統憑證的訪問。篡改通常有一個目標：以任何可能的方式提取密鑰，最直接的方式是探查晶片以查找儲存密鑰的憑證；而旁路攻擊是非侵入式、不會直接探查電路，乃依賴電路運行時從電路洩漏的訊息，涉及電源／電磁輻射 (EMI) 分析、定時匯流排監控、暫寄器、快取記憶體 (cache) 或隨機存取記憶體 (RAM) 攻擊。除了供身份驗證的密鑰和憑證之安全容器，Microchip 還為不同規模大小的設備提供安全配置。

其 CryptoAuthentication 系列的信任平台是一項三層服務，允許預先配置或完全自定義的安全元素，以及硬體安全儲存，有效防止密鑰被未經授權的用戶隱藏，應對各種規模項目的安全認證。惟有安全地在設備中配置密鑰，才能確保製造商在整個設備現場部署期間或整個生命週期內，都不會曝露密鑰。結合 Trust Platform，可在物聯網節點提供安全的身份驗證、耗材系統的防偽、附件身份驗證和智財權 (IP) 保護，以驗證任何系統的韌體。當然還有最決絕的作法是：將解密密鑰刻錄到 OTP (一次性編程) 自製晶片、安裝韌體並驗證後再使用。

如此一來，這些密鑰將永遠無法重新編程；據此創建的受信任平台模組，會將最終用戶的設備應用程式與網路以物理形式切分，或是以安全啓動模式，先在安全操作系統的啓動映像中驗證簽名後，再在網路接口執行作業系統，將其與晶片組和解密密鑰隔離。要不然，就是將設備與主網從根本上拆開；可能的話，將它們與外網完全隔離或另設獨立區域網以縮小攻擊面。

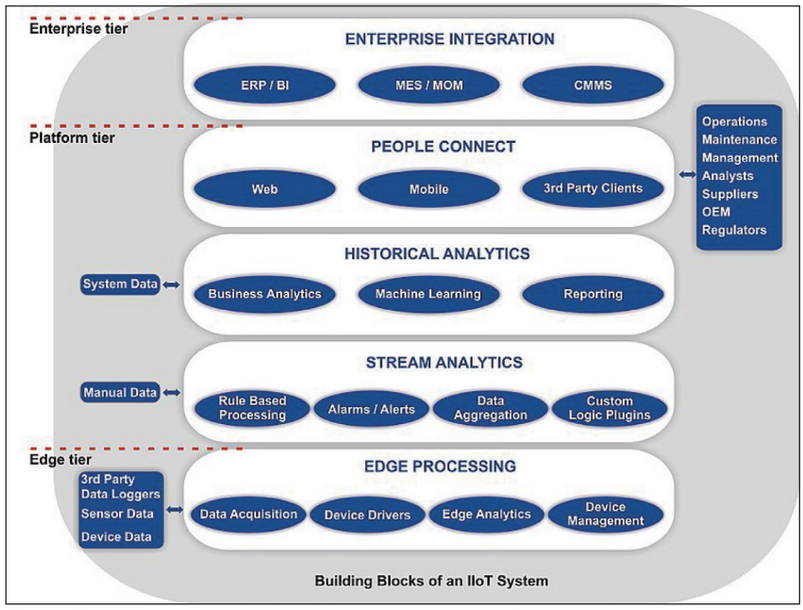
CTA

IIoT 數位轉型：OT 網路威脅急升，IT 如何應援？

■文：任芷萍

《思科 (Cisco) 2020 年全球網路趨勢報告》預測，2022 年全球網路將連接 146 億個物聯網 (IoT) 設備，而機器通訊 (M2M) 將佔所有聯網設備的 51%，多數將以無線方式連接到網路。時至今日，不少企業更是冀望借助 IoT 和人工智慧 (AI) 維繫營運或保護員工健康；例如，用 AIoT 自動執行公務、進行無接觸交通／支付、改善物流和供應鏈管理，或透過 AI 驅動的穿戴式 IoT 設備測量員工體溫或做相關健康指標監控。在全球企業擁抱數位轉型之際，面對勒索軟體、「分散式阻斷服務」(DDoS) 等資安威脅，許多企業都選擇使用專網部署物聯網。

圖 1：工業物聯網 (IIoT) 組成可概略分為三層——邊緣、平台和企業，實際應用上的區隔可能不是如此絕對



資料來源：https://commons.wikimedia.org/wiki/File:IIoT_System_Building_Blocks.jpg

因為數位轉型，營運技術 (OT) 也從傳統獨立系統走向網路連接。儘管多數組織已實施資訊技術 (IT) 安全措施，但 OT 至今仍是新領域。在工業物聯網 (IIoT) 促使 IT、OT 融合的同時，IT 風險也被完整擴及 OT 層面，OT 無法再延續原有封閉優勢、憑藉與世隔絕的天然護城河而獨善其身。IBM X-Force 發現 2019 年針對工業控制系統 (ICS) 和 OT 的數位攻擊，較前一年同期增加 2000%(亦即 20 倍) 以上！其中多涉及利用資料採集和監控 (SCADA) 和 ICS 硬體組件中的已知漏洞，或以暴力登錄技術進行的密碼噴霧攻擊。

ICS 和 SCADA 受衝擊，「統一威脅管理」出線

ICS 涵蓋大部分 OT 分層體系結構，包括管理工業過程多種不同類型的設備、系統、控件和網路，其中最常見的是 SCADA 系統和分佈式控制系統 (DCS)，新一代安全團隊必須了解工業協定的相關知識，對於通訊工具和流程相當重要。Stuxnet (震網，又稱作「超級工廠」) 是首個針對 ICS 的 Windows 蠕蟲病毒，利用西門子 (Siemens) SIMATIC WinCC/Step7 漏洞感染 SCADA 系統，向可編程邏輯控制器 (PLC) 寫入代碼並將代碼隱藏，在尋找其他軟體前多次複製，且類似攻擊有增多趨勢。新威脅和攻擊機制的興起，已從根本上

改變 ICS 和 SCADA。

2017 年現蹤的 TRITON 惡意軟體，更是首開專攻保護人類生命的工業安全系統之先河；透過安全儀表系統 (SIS) 修改記憶體中的韌體、添加惡意功能，使攻擊者可讀取或修改內容並實現自定義代碼，達到干擾工安程式目的。Global Market Insights 預測，2026 年 ICS 安全市場的增長將達 20%、達 120 億美元；施耐德電氣 (Schneider Electric)、漢威聯合 (Honeywell)、洛克威爾自動化 (Rockwell Automation)、卡巴斯基實驗室 (Kaspersky Lab) 和趨勢科技 (Trend Micro) 是 ICS 安全市場的主要參與者。

他們特別提到，「統一威脅管理」(UTM) 因結合多種安全服務和功能、且可使用單個管理控制台管理各種安全功能，屆時亦將呈 20% 以上的穩定增長。另根據資安公司 Fortinet 和市調機構 Forrester 的聯合調查顯示，OT 託管的 ICS/SCADA 系統正遭受新威脅、容易受到網路攻擊——在融合 IT/OT 追求營運效率的同時，亦導致廣泛的連接並帶來更多傳統 IT 風險，來源之一是：基礎架構增加將曝露業務合作夥伴。因此，向適當的人員授予適當訪問權限至關重要，必須讓合作夥伴及組織與之建立的關係類型都是有意義的。

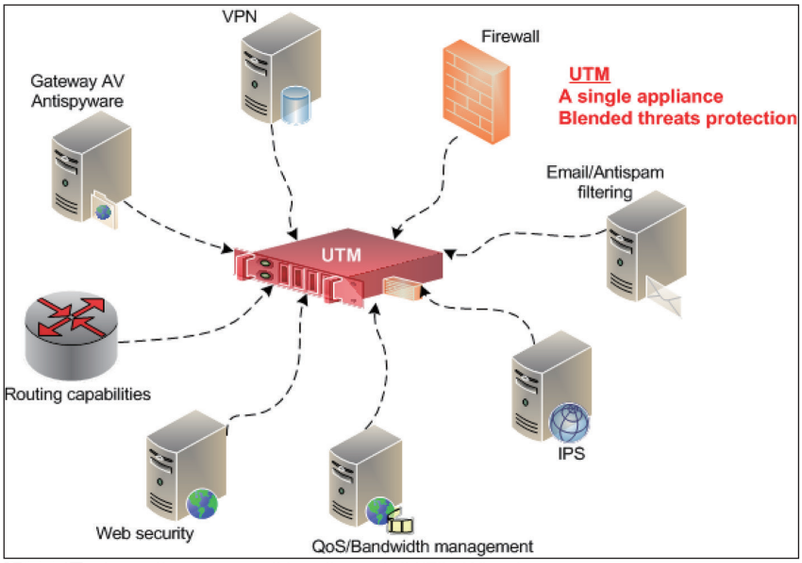
防禦 OT 網路攻擊的短板

「合規性」亦已成為管理 OT 系統所關注的議題，其中影響最大的法規是：一般資料保護規範 (GDPR)、國際協會 (ISA) 標準與聯邦資訊安全管理法 (FISMA)。Fortinet 獨力發佈的《營運技術和網路安全狀況報告》更指出，有高達 74% 的 OT 組織在過去 12 個月中曾經歷惡意軟體入侵而損害生產力、收入、品牌信任度、知識產權和人身安全。為此，西班牙電信集團全球網路安全部門 ElevenPaths 宣佈與 Fortinet 擴大合作，利用集成逾 360 種技術的 Fortinet Security Fabric ICS，為 IIoT 用戶提供即時漏洞保護和安全遠程訪問。

常規的資安工作專注於資訊保全、網路彈性、事件響應、數據恢復和業務連續性，但這遠遠不足；經統計，防禦 OT 網路攻擊的短板在於：缺少 OT 設備清單、缺乏遠程網路可訪問性、過時的軟／硬體、OT 傾向在既有信任環境工作而有礙融合，以及混亂的訪問控制和權限管理。所幸，包括美國工業控制系統網路緊急回應小組 (ICS-CERT) 和英國國家基礎設施保護中心 (CPNI) 等政府組織已發佈相關建議和指導，國際自動化協會 (ISA) 也已開發帶有「區域和管道」框架的標準，以解決 ICS 網路安全最緊迫的缺陷並提供改進管理的指南。

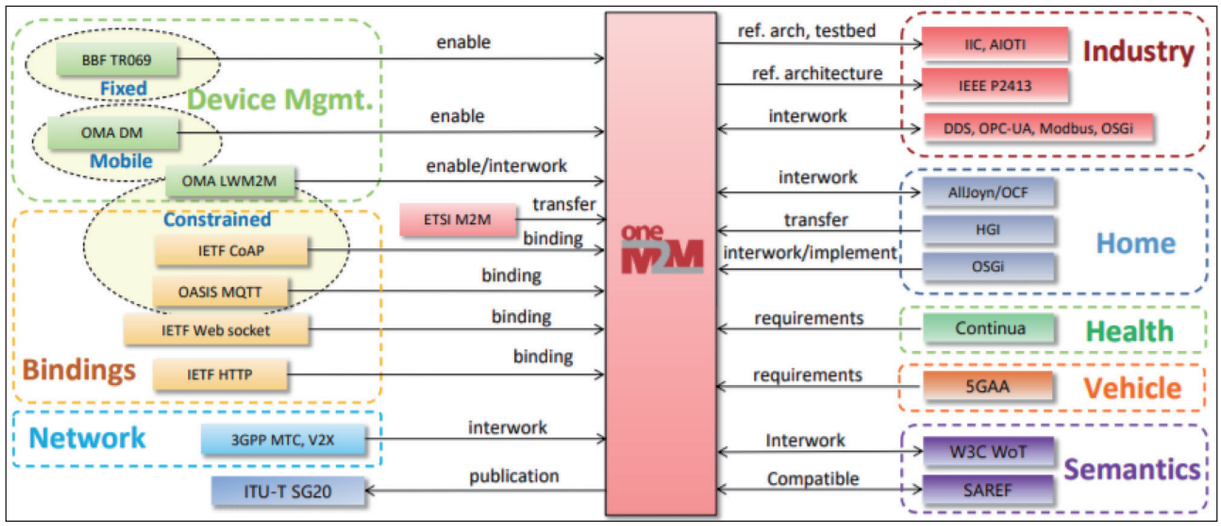
非營利性 ICS-ISAC 組織正聚焦於共享相關知識，國際標準倡議組織 oneM2M 亦分別與 IoT 連接聯盟 (ICA)、工業互聯網聯盟 (IIC) 合作。另有鑑於仍有許多 ICS 都位於非 IP 的專網，須經由特定閘道器 (Gateway) 和控制軟體才能連接互聯網；開放連接基金會 (OCF) 提供一個通用框架，能搭 IP 之便承載來自現有自動化專網的數據。OCF 利用「表現層狀態轉換」(REST) 模型簡化底層軟體堆疊的應用程式，使 Web 服務得以大規模採用。另為使堆疊更適合小型設備，以二進制變體 CoAP 取代 HTTP，並在 CBOR 中壓縮 JSON

圖 2：「統一威脅管理」(UTM) 以單一應用迎戰多方威脅



資料來源：https://commons.wikimedia.org/wiki/File:What-is-utm.png

圖 3：oneM2M 組織志在作為跨行業／行業特定協議的互操作性樞紐



資料來源：https://www.onem2m.org/images/files/IIC_oneM2M_Whitepaper_final_2019_12_12.pdf

數據以傳輸小量數據。

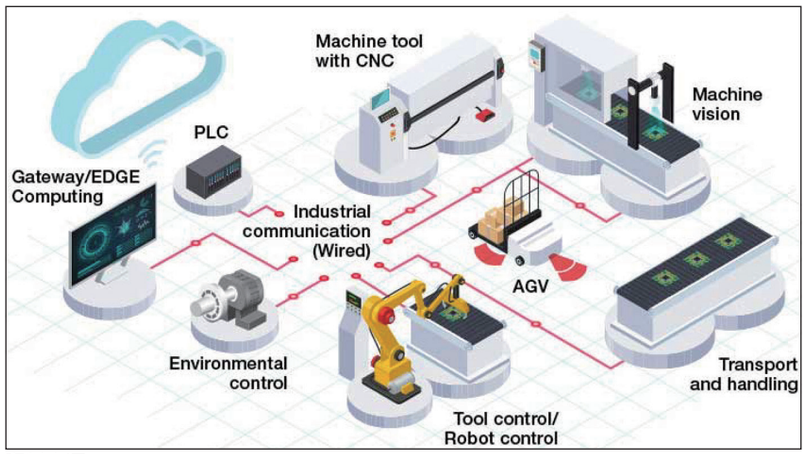
當中所有數據傳輸均受「資料包傳輸層安全」(DTLS) 標準保護。OCF 還資助 IoTivity，使其與 OCF 標準同步實現開源堆疊，OCF 已在核心框架的 IoTivity 定義創建安全 IoT IP 設備所需的多數內容，開發者只需將所選的 IP 網路接口綁定到底層，然後在頂層執行所選的應用程式協定即可，讓 ICS 可繼續以原有方式通訊，亦可走 Thread 等新一代無線傳輸。最重要的是，此方式具有端口層，可移植到各種平台和操作系統，IP-based 通訊可透過本地或雲端來控制設備；為確保互操作性，OCF 訂有認證程序和一致性測試規範。

IIoT 安全計畫始於網路風險評估，應具權重概念

物聯網的網路堆疊加大資安挑戰，尤其是難以升級或補丁的老舊工業系統設備。專家認為，保護 OT 與 IT 截然不同：首先，OT 技術疊代週期比 IT 長且往往歷史悠久。其次，OT 網路注重系統正常運作甚於保護數據，難仿效 IT 暫停系統以補丁、更新或維護；反之，OT 網路的 PLC 與端點偵測及回應 (EDR) 技術亦不相容。IT、OT 網路擁有一致的可見性和控制點是關鍵，兩者差距過大會有盲點、予攻擊者可乘之機。組織應擴展 OT 管理並集成到現有 IT 流程，包括從 IT 網路提供安全度量和遙測的資安監控中心 (Security Operations Center, SOC)。

此前，必須完全掌握任何使用中的過時操作系統及可能帶來的所有潛在威脅，並予以量化這些風險以便組織可就嚴重的網路攻擊之維護停機成本做出明智判斷，同時需牢記這些漏洞，並註記每一個

圖 4：製造工廠中的所有組件都在 OT 網域內進行連接和控制，為保護此域免受通訊外部環境 IT 侵害，通常需要安全的閘道器把關，且數據格式和通訊協定可在邊緣調整



資料來源：https://www.ti.com/applications/industrial/industry-4-0.html

OT 資產及其與 IT 網路的脈絡，增加捕獲和阻止攻擊的機會。安全服務廠商主張，IIoT 安全計畫始於網路風險評估，應具權重概念。若無法折衷，則需為邊緣設備提供強力保護，例如，採用單向閘道器設備。邊緣運算 (Edge Computing) 是 IIoT 的基礎組成，對工業 4.0 至關重要，可減少機器／設備感測數據直接發送到遠程雲端的時間延遲和頻寬成本。

邊緣運算通常發生在資源受限的設備，而功能越來越強大的智慧手機也躋身邊緣設備之列，可運行邊緣軟體堆疊。另一方面，邊緣正成為在離線模式下的機器學習／深度學習裝置，多是將已訓練完成的模型用於分類和預測。邊緣設備常身兼閘道器和中樞 (Hub) 角色，必須提供安全訪問並跟蹤、監視、檢測、管理設備群。甚至，還負責軟體和韌體的更新。從物料資源規劃軟體 (MRP) 到公司目錄服務、再到消息代理、數據湖 (Data Lake)，邊緣運算平台必須與各種服務和應用程式整合，包括：輕型目錄存取協定 (LDAP) 和特權身份管理 (IAM) 系統。

如此，可提供基於角色的訪問控制 (RBAC)，每個 IT/OT 角色都應該與定義明確的角色相關聯，以指定其執行特定操作。例如，應用程式開發人員不應擁有執行韌體升級的權限。Forescout 公司主張以四個技巧來驗證企業的 OT 安全：1. 主動識別、分類和監控 OT 網路資產；2. 協調 IT 和 OT 團隊以執行整合網路安全計畫；3. 使用價值證明 (PoV) 準確評估供應商的適用性；4. 重新評估 OT 安全供應商環境來適應新興市場動態。值得留意的是，Gartner 預言到 2023 年底，有高達 60% 的單點式 OT 安全服務商將被更名、重新定位、併購或徹底消失！

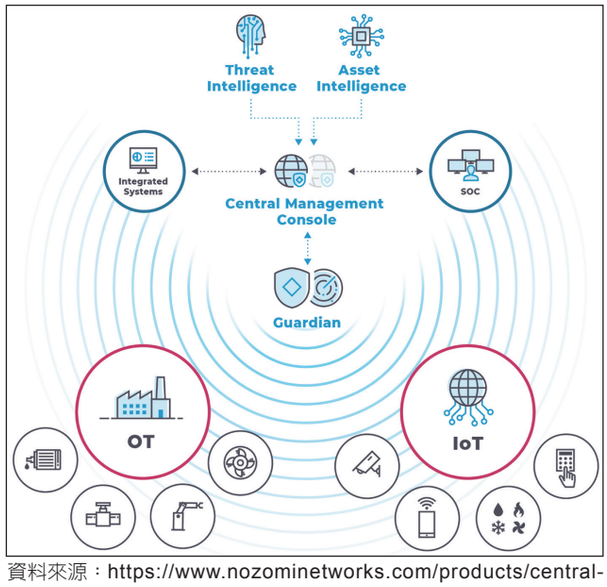
駭客攻擊趨向智能化，「嚴格的網路分段」是防禦第一步

IoT 安全方案業者 Nozomi Networks 表示，駭客正在發動更高竿的攻擊，例如，利用漏洞或盜竊憑證獲得網路的特權訪問，直接將勒索軟體部署到關鍵營運資產先前的研究和學習環境。Nozomi Networks 甫被市調公司 Forrester 評比為目前最成熟的 OT 安全解決方案供應商，提供一體機與虛擬機方案，支援多元工業網路協定、採用非侵入式監測、可彈性根據場域網路環境連接設備節點架構與數量快速部署，且可與眾多資安產品整合聯防。一旦發現異常，可在第一時間示警並啓動應變程序。他們呼籲，隨著遠程訪問越見普及，企業必須更加提高警覺：

1. 使用被動流量監控、識別關鍵資產和運行狀態並為其設定底線，以提高 OT 環境的可見性；
2. 在 IT 和 OT 環境使用異常檢測技術增強檢測能力；
3. 檢查網路基礎結構的運行狀況，並確保網路隔離和防火牆策略妥善到位；
4. 確保修補了所有設備和服務，並設法縮短補丁程式週期；
5. 部署支持快速訪問受影響文件的彈性備份策略；
6. 執行資產強化以禁止勒索軟體用於傳播服務，遠程訪問精靈已無法使用，且短期內將不復返。

惟有功能強大的安全性和可見性工具包，包括資產和威脅情報訂閱及可快速部署的附件 (如智能輪詢和遠程收集器)，方可應對 OT 和 IoT 系統帶來的營運挑戰。物聯網安全的第一道防線應是「嚴格的網路分段」，添加受保護的虛擬區

圖 5：在各種混合環境中部署 Nozomi Networks 解決方案，可實現快速資產發現、網路可視化並加速安全性



資料來源：https://www.nozominetworks.com/products/central-management-console/

域網 (VLAN)、實體防火牆或其他邏輯切分將 IoT 網路與其他網路元素隔離；有些敏感設備甚至可阻止它們連接外網，或僅在特定時間範圍內允許維護和補丁。思科正在透過一系列軟體更新，為客戶提供更高級的網路分段、自動化和對物聯網終端的深入可視性 (visibility)。

Container & DevSecOps：執行安全隔離

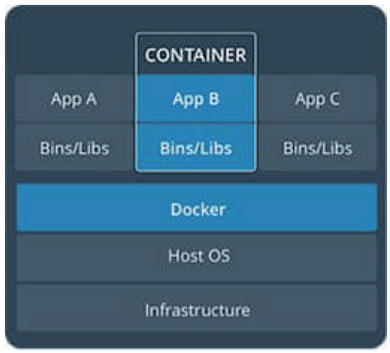
在過去的兩年中，「容器」越來越受歡迎，使開發人員能在由名稱空間和控制群組 (Cgroup) 組成的隔離封包中執行軟體；在建構、啓動容器時，必須從一開始就內置端到端安全性，以便每個利用該技術的人都能從中受益。當需要更多資源時，容器使「橫向擴展」分佈式應用程式變得更加容易；但當開發人員使用容器支援其應用程式時，必須意識到這些部署將需要的新安全模型。容器之間的相互通訊端口是裸露的，會讓防火牆或基於主機的入侵檢測系統 (Host-IDS) 忘了它的存在；偏偏容器沒有標準的安全模型或規定，慎選元件供應商就顯得格外重要。

一般而言，容器風險來自於三方面：容器映像本身、如何更新以及如何隨時間運行。每個容器都是一個基本映像，包括應特定作業所需；它可在內部開發並儲存在私有註冊表中，或從公共註冊表中獲取。無論「於公於私」，都應在部署前檢查 Docker 映像，以免每次從容器註冊表中提取圖像時，都將現有漏洞引入應用程式。專家呼籲，檢查放入公司註冊表的圖像是不可少的步驟，且應保持最新狀態；若在創建後才發現漏洞，則應將易受攻擊的容器繼續存在於註冊表，直到被調用出去。只要需要工作量，活動容器將繼續運行。

這意味著對於具有大量流量的應用程式，容器映像可能將持續較長時間而發生問題。除了在註冊表中掃描圖像外，每個運行中的圖像也應隨時間進行掃描；這種連續方式也有助於捕獲可能隨時間累積的潛在容器問題。為免在創建容器圖像且運行後，因另行調用或導入而增加漏洞，掃描容器的即時圖像也不可少。惡意軟體仍是駭客進入物聯網設備的常用方法，若是未經更動的帳密預設值，更容易被駭客摸清底細；一旦惡意軟體創建足夠大的殭屍網路，就能發動 DDoS 攻擊，進而癱瘓線上服務。

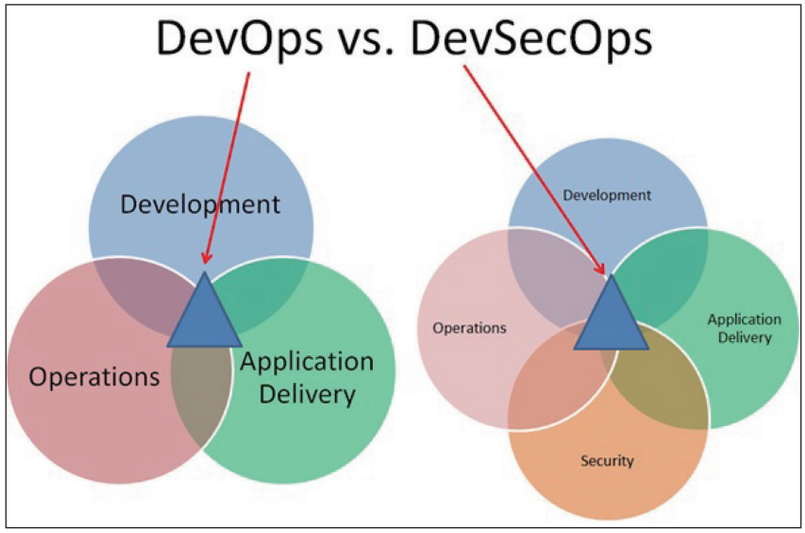
一個名為「CallStranger」的嚴重漏洞，被發現會影響數十億個 IoT 設備的「UPnP」(通用即插即用) 核心協定，就是 DDoS 的最佳跳板。雖說勤於更新和雙因素 (2FA) 認證能多加一層保護，但只要具備聯網通訊能力，攝影機亦可能遭遇中間人攻擊 (MITM)，解決之道是：採用更高防護等級的加密

圖 6：容器提供一種資源友好的方式，可將託管於閘道器、PLC 或工業電腦等設備的邊緣運算程序隔離



資料來源：https://www.digikey.tw/zh/articles/taking-the-iiots-head-out-of-the-cloud

圖 7：DevOps vs. DevSecOps 的區別——強調一開始就要考慮應用和基礎架構的安全性，還要讓某些安全閘道實現自動化，防止 DevOps 工作流程變慢



資料來源：https://www.redhat.com/zh/topics/devops/what-is-devsecops；https://commons.wikimedia.org/wiki/File:DevOps_vs_DevSecOps_Mginise.jpg

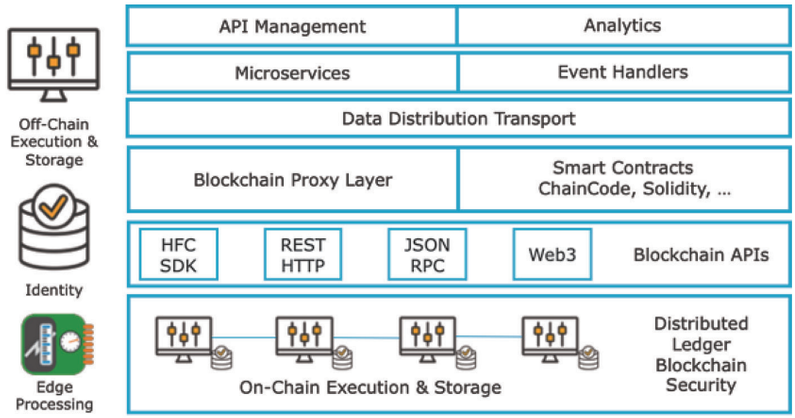
工具或將硬體安全模組 (HSM) 集成到所有攝影機中。除了路由器和無線攝影機外，攻擊現在還涉及智能燈泡和虛擬語音助理。這些物聯網設備通常很小、缺乏硬體物理空間來容納額外安全功能所需資源；或許有些智能邊緣設備很大，但是大部分空間仍被佔用。

此時，集成安全功能和定期修補設備可從 DevSecOps 方法中受益，由組織中的開發人員和營運人員共同負責應用程式或服務，將安全功能以代碼集成，減少安全功能佔用空間、或根本毋需專用的安全硬體。設備供應商正在面臨越來越嚴格的政府法規、網路安全標準和採購要求。除了功能測試外，安全軟體開發生命週期 (SSDLC) 也須列入考慮。DevSecOps 在開發過程中，有助於縮短上市時間並實現高品質的數據保護，但這需要集成產品安全評估、安全軟體開發和漏洞檢測三方面專業。為逐項確認合規性，「漏洞掃描」和「模糊測試」缺一不可。

IIoT 生態安全：數位雙胞胎 vs. 區塊鏈

前者是與常見漏洞和披露 (CVE) 數據庫資訊比對、發現已知問題，後者旨在發現未知弱點，而 AI 端點分析對此助益匪淺——大規模識別以前未知端點，後從各種上下文資源和 AI 中提取、分類並制訂策略。Market Insights Reports 預估，全球網路安全 AI 市場將從 2019 年的 88 億美元成長至 2026 年的 382 億美元，期間年複合成長率 (CAGR) 達 23.3%。「數位雙胞胎」(Digital Twins，數位分身) 是另一個 IIoT 資安議題；IDC 預測到 2023 年，全球有 65% 的製造商將因此節省 10% 製程營運支出，但有 79% 企業未審查其合作生態系的安全風險，更有 32% 根本沒有採取任何措施。

圖 8：區塊鏈的分佈式特性、捆綁的安全措施及智能合約之類的相關功能可幫助製造商快速追蹤貨物、透明管理，且使供應鏈流程和付款自動化



資料來源：https://blog.semi.org/technology-trends/blockchain-opportunities-in-the-semiconductor-and-electronics-manufacturing-supply-chain

由於多種安全漏洞，英國企業和家庭中超過十萬個無線主動式攝影機可能容易受到駭客攻擊；除了訪問網路，還可透過其他方式擅自啓用網路攝影機，包括用肩膀衝浪 (Shoulder Surfing) 獲取個人識別碼 (PIN)、密碼和憑證，或偷窺受害者並運用訊息發動釣魚攻擊、將攝影機添加到殭屍網路等。企業和工業物聯網協作風險管理廠商 Jitsuin 正在透過協作和分佈式改變遊戲規則，協助揭示、減少和報告整個 IoT 價值鏈中的風險；Jitsuin 已宣佈加入數位分身聯盟 (Digital Twin Consortium, DTC)，旨在建立對互聯事物及其數位雙胞胎的現實信任。

此外，在物聯網供應鏈中，區塊鏈 (Blockchain) 可驗證產品出處並追蹤資產，在買方和賣方之間建立可信賴的關係。沃爾瑪 (Walmart) 正在使用區塊鏈技術收集農產品運輸環境中的數據，以追蹤新鮮度。市調公司 Research Dive 預估至 2026 年底，全球區塊鏈 IoT 市場將達 58 億美元，CAGR 達 91.5% ！報告指出，區塊鏈和物聯網共同消除中間人功能，極大程度提高了供應鏈效率，惟增強設備之間的安全通訊和隱私協定是這個組合的關鍵驅動力；按應用劃分，可分為智能合約、數據安全、資料共享、資產追蹤與管理等幾大分衆市場。

自宅辦公！家庭就是我的工作場所

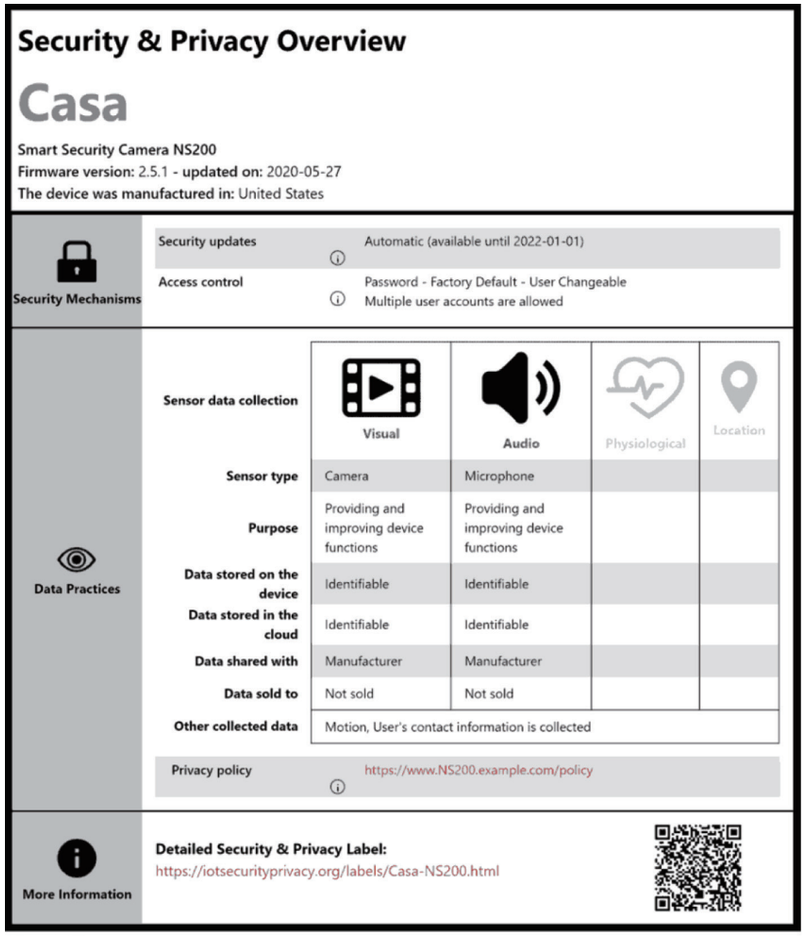
IoT 設備可為攻擊者提供進入

家庭網路的便捷途徑；隨著在家工作風氣漸盛，攻擊者有機會借道員工個人網路長驅直入企業網路。後疫情時代，網路安全或成業務連續性的關鍵，這也意味著企業需培訓員工如何使用虛擬私人網路 (VPN) 連接，以確保企業可以控制數據流是否安全，而不會使 BYOD(自攜電子設備) 的工作模式帶來進一步風險。可擴展的虛擬化安全工具有助於保護遠程工作人員的 IoT 設備，VPN 和虛擬防火牆啓用加密，監視進出本地網路的數據，並防止惡意軟體進入家中的 IoT 設備。

相較於軟體方案，有人仍主張保護智能家居設備的「通訊通道」才是治本方法，例如，使用硬體加密閘道器作為物聯網系統之資訊流中樞。理想中，網路服務供應商 (ISP) 應通過具有安全功能的閘道器來保護用戶。食品行業協會 (FMI) 認為肺炎疫情對遠程網路技術的壓力將為 IoT 安全市場促生新機會，預估 2027 年市值將達 480 億美元。然有趣的是：消費者可願為隱私和安全付費？設備供應商可有望獲得溢價報酬？或許，透過拉高採購門檻、讓劣質品自然在市場中敗下陣是一種方法。

日前，卡內基美隆大學提出一個創新概念：仿效食物的營養標示推出的「安全和隱私標籤」，旨在為消費者提供軟、硬體安全更新、技術支援、數據收集、第三方共享等訊息，協助人們理解潛在風險。標籤標示於設備盒外部，傳達設備收集的數據類型、目的、與誰共享等重要訊息。掃描 QRCord 可線上訪問第二層標籤，獲得設備保留數據時效、共享數據頻率等進一步訊息。《網路盾牌法案》已明示將為物聯網設備創建一套標準，然後為合格產品貼上標籤；上述兩層共顯示 47 條不同慣例的相關訊息，算是向前邁出一大步。 CTA

圖 9：「安全和隱私標籤」第一層是貼在設備包裝上或顯示在線上購物網站，而第二層可經由 URL 或 QR Cord 訪問



資料來源：https://www.iotsecurityprivacy.org/

下期預告：

AI 與嵌入式系統