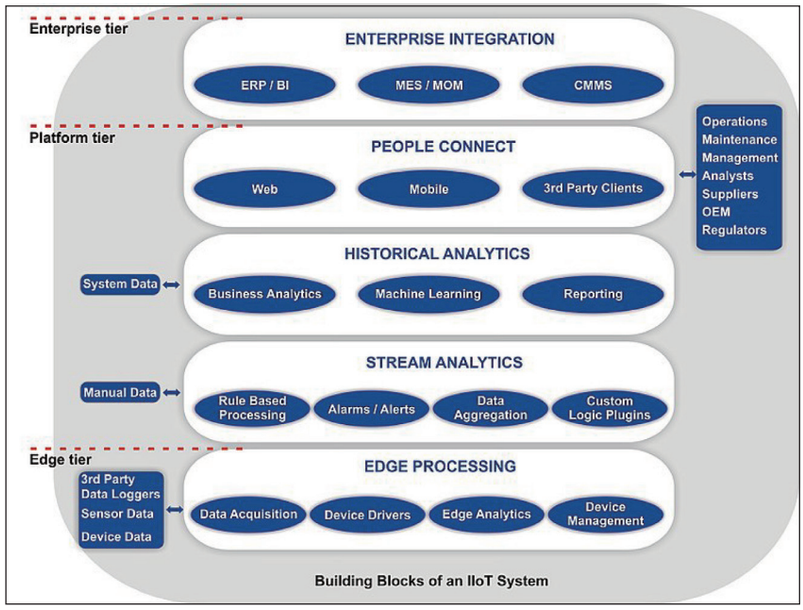
IIoT 數位轉型：OT 網路威脅急升，IT 如何應援？

■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。

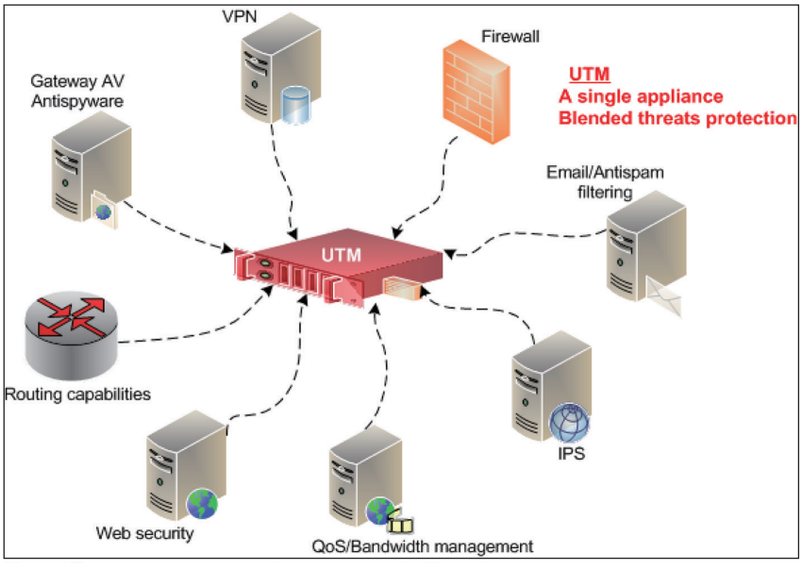
防禦 OT 網路攻擊的短板

「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。

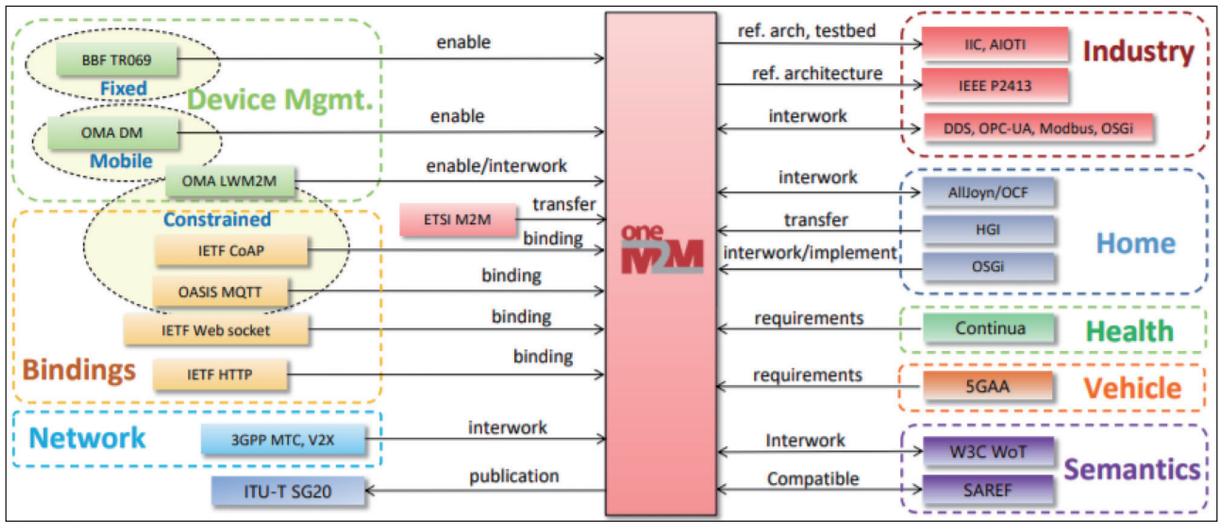
非營利性 ICS-ISAC 組織正聚焦於共享相關知識，國際標準倡議組織 oneM2M 亦分別與 IoT 連接聯盟 (ICA)、工業互聯網聯盟 (IIC) 合作。另有鑑於仍有許多 ICS 都位於非 IP 的專網，須經由特定閘道器 (Gateway) 和控制軟體才能連接互聯網；開放連接基金會 (OCF) 提供一個通用框架，能搭 IP 之便承載來自現有自動化專網的數據。OCF 利用「表現層狀態轉換」(REST) 模型簡化底層軟體堆疊的應用程式，使 Web 服務得以大規模採用。另為使堆疊更適合小型設備，以二進制變體 CoAP 取代 HTTP，並在 CBOR 中壓縮 JSON

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。

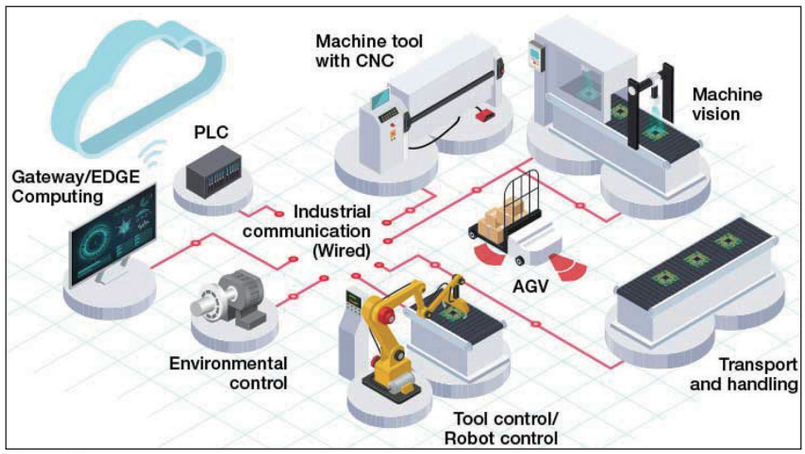
當中所有數據傳輸均受「資料包傳輸層安全」(DTLS) 標準保護。OCF 還資助 IoTivity，使其與 OCF 標準同步實現開源堆疊，OCF 已在核心框架的 IoTivity 定義創建安全 IoT IP 設備所需的多數內容，開發者只需將所選的 IP 網路接口綁定到底層，然後在頂層執行所選的應用程式協定即可，讓 ICS 可繼續以原有方式通訊，亦可走 Thread 等新一代無線傳輸。最重要的是，此方式具有端口層，可移植到各種平台和操作系統，IP-based 通訊可透過本地或雲端來控制設備；為確保互操作性，OCF 訂有認證程序和一致性測試規範。

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！

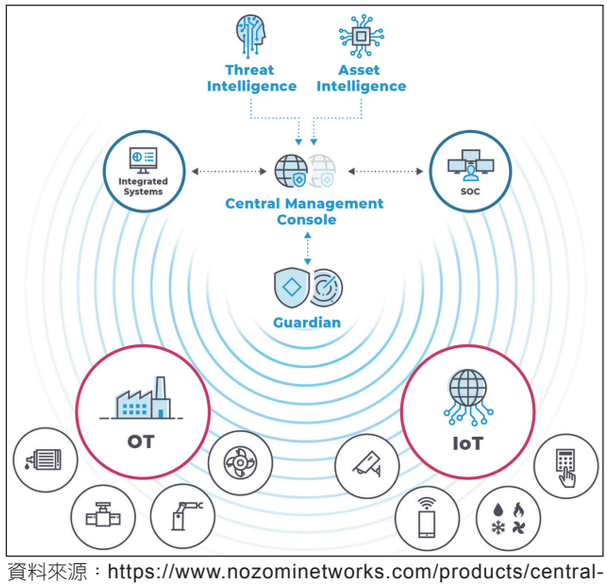
駭客攻擊趨向智能化，「嚴格的網路分段」是防禦第一步

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

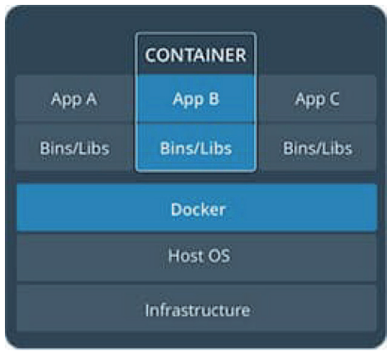
在過去的兩年中，「容器」越來越受歡迎，使開發人員能在由名稱空間和控制群組 (Cgroup) 組成的隔離封包中執行軟體；在建構、啓動容器時，必須從一開始就內置端到端安全性，以便每個利用該技術的人都能從中受益。當需要更多資源時，容器使「橫向擴展」分佈式應用程式變得更加容易；但當開發人員使用容器支援其應用程式時，必須意識到這些部署將需要的新安全模型。容器之間的相互通訊端口是裸露的，會讓防火牆或基於主機的入侵檢測系統 (Host-IDS) 忘了它的存在；偏偏容器沒有標準的安全模型或規定，慎選元件供應商就顯得格外重要。

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。

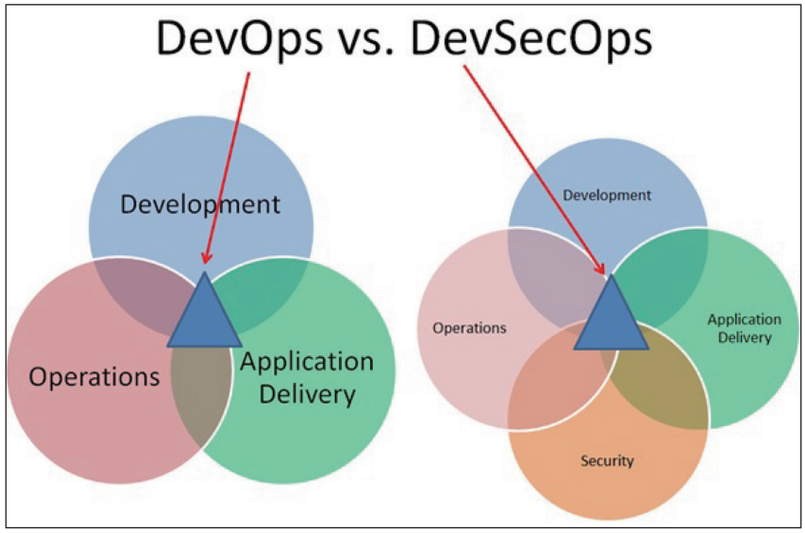
一個名為「CallStranger」的嚴重漏洞，被發現會影響數十億個 IoT 設備的「UPnP」(通用即插即用) 核心協定，就是 DDoS 的最佳跳板。雖說勤於更新和雙因素 (2FA) 認證能多加一層保護，但只要具備聯網通訊能力，攝影機亦可能遭遇中間人攻擊 (MITM)，解決之道是：採用更高防護等級的加密

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

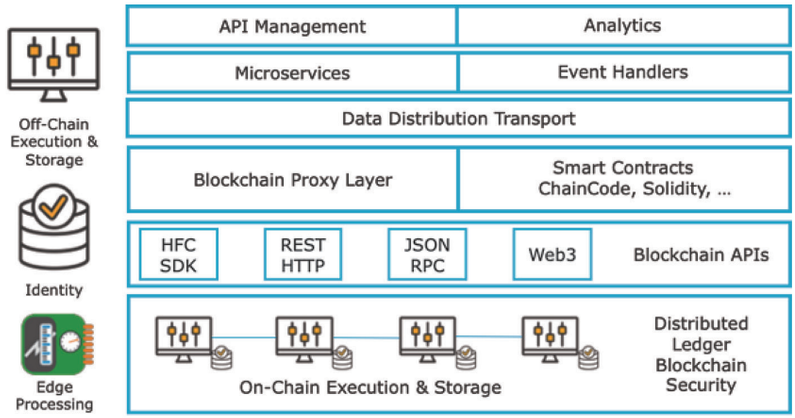
工具或將硬體安全模組 (HSM) 集成到所有攝影機中。除了路由器和無線攝影機外，攻擊現在還涉及智能燈泡和虛擬語音助理。這些物聯網設備通常很小、缺乏硬體物理空間來容納額外安全功能所需資源；或許有些智能邊緣設備很大，但是大部分空間仍被佔用。

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

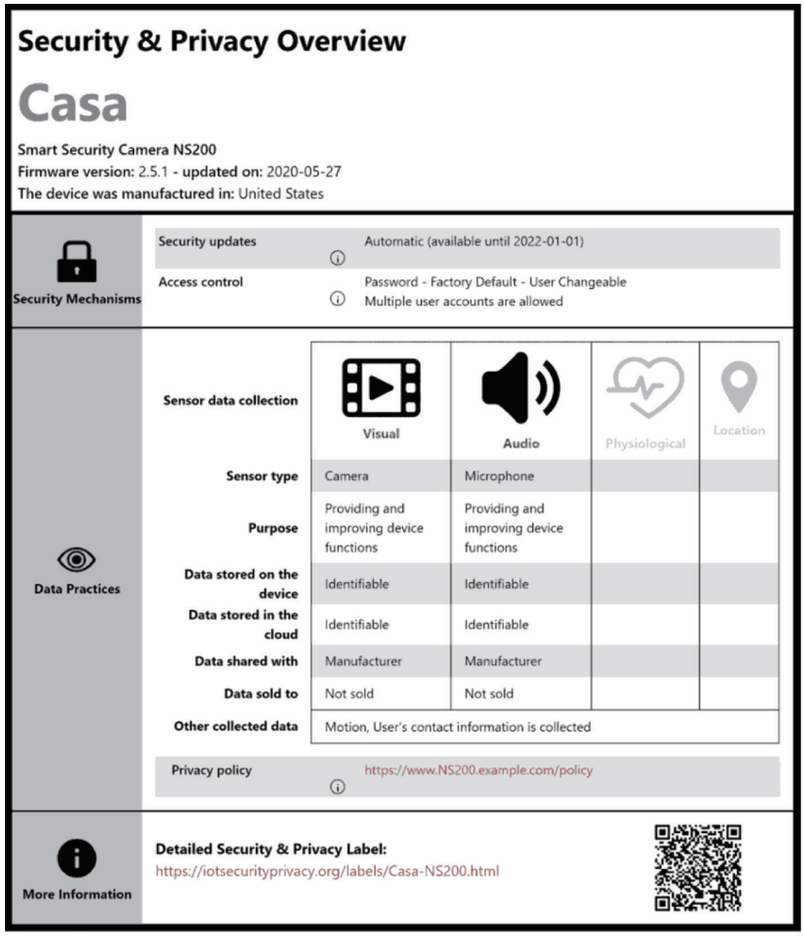
IoT 設備可為攻擊者提供進入

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