CYBERSEC 2022 臺灣資安大會

供應鏈資安論壇

工控資安新戰略
打造多層次防禦網

蕭睿廷 Ryan Hsiao

華碩雲端　架構規劃部　經理

2022/09/22

asusCLOUD

講師簡介

蕭睿廷 Ryan Hsiao

華碩雲端 架構規劃部 經理

經歷簡介

- 華碩雲端 資深架構師
- 迎棧科技 資深架構師
- 趨勢科技 技術專案經理
- 群環科技 技術顧問
- 星展銀行 資訊部經理
- 精誠資訊 技術經理

專業證照

- **PMP** 專案管理師
- **VCP** (VMware Certified Professional)
- **CNCF CKA** (Certified Kubernetes Administrator)
- **CCNA** (Cisco Certified Network Associate)
- **MCSE** (Microsoft Certified System Engineer)

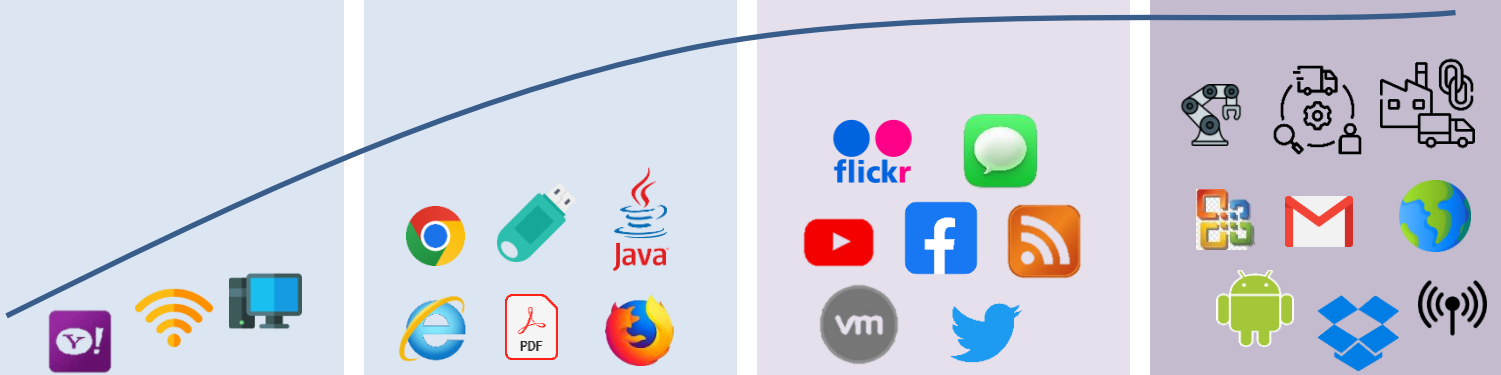
1. 全球資安趨勢洞察
2. 供應鏈資安挑戰解析
3. OT 關鍵 5 大應用情境
4. 實戰案例分享

全球資安趨勢洞察

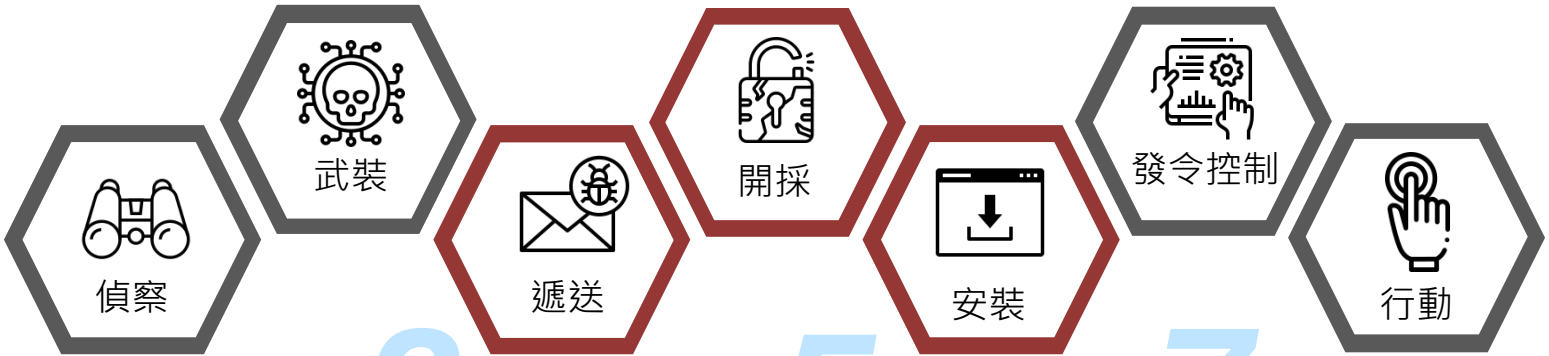
全球資通安全發展趨勢

asusCLOUD

時代	PC	網際網路	行動網路	IoT / AI / 5G
	2000	2005	2010	2018~Now
資安威脅	蠕蟲病毒	間諜軟體 惡意軟體	進階持續性威脅 網路軟體	複合型網路攻擊 供應鏈威脅
資安因應	端點防護	網路防禦	雲端安全	智慧安全



資安攻擊 7 大步驟



1 RECONNAISSANCE
Harvesting email addresses, conference information, etc.

2 WEAPONIZATION
Coupling exploit with backdoor into deliverable payload

3 DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION
Exploiting a vulnerability to execute code on victim's system

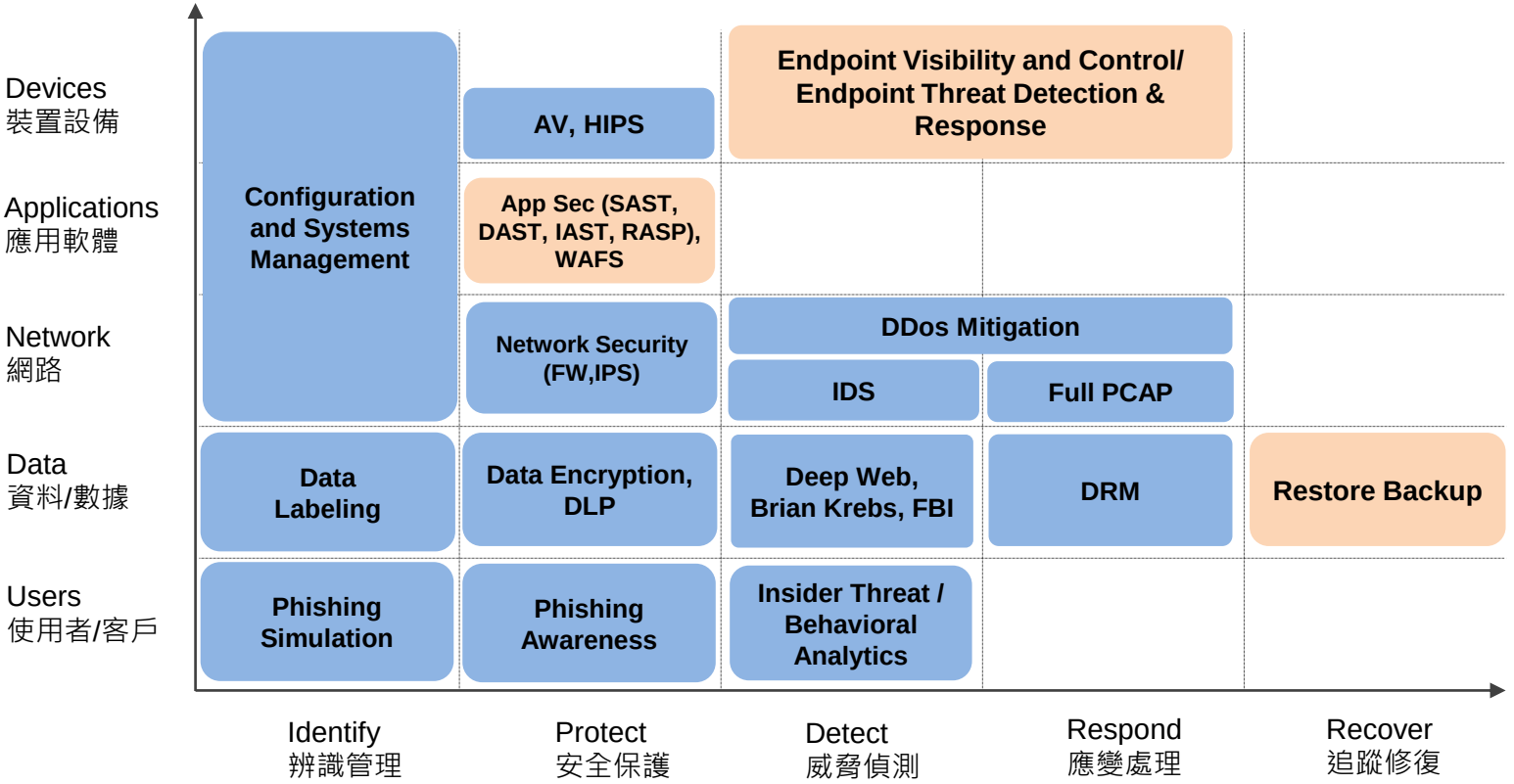
5 INSTALLATION
Installing malware on the asset

6 COMMAND & CONTROL
Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

資料來源：Lockheed Martine

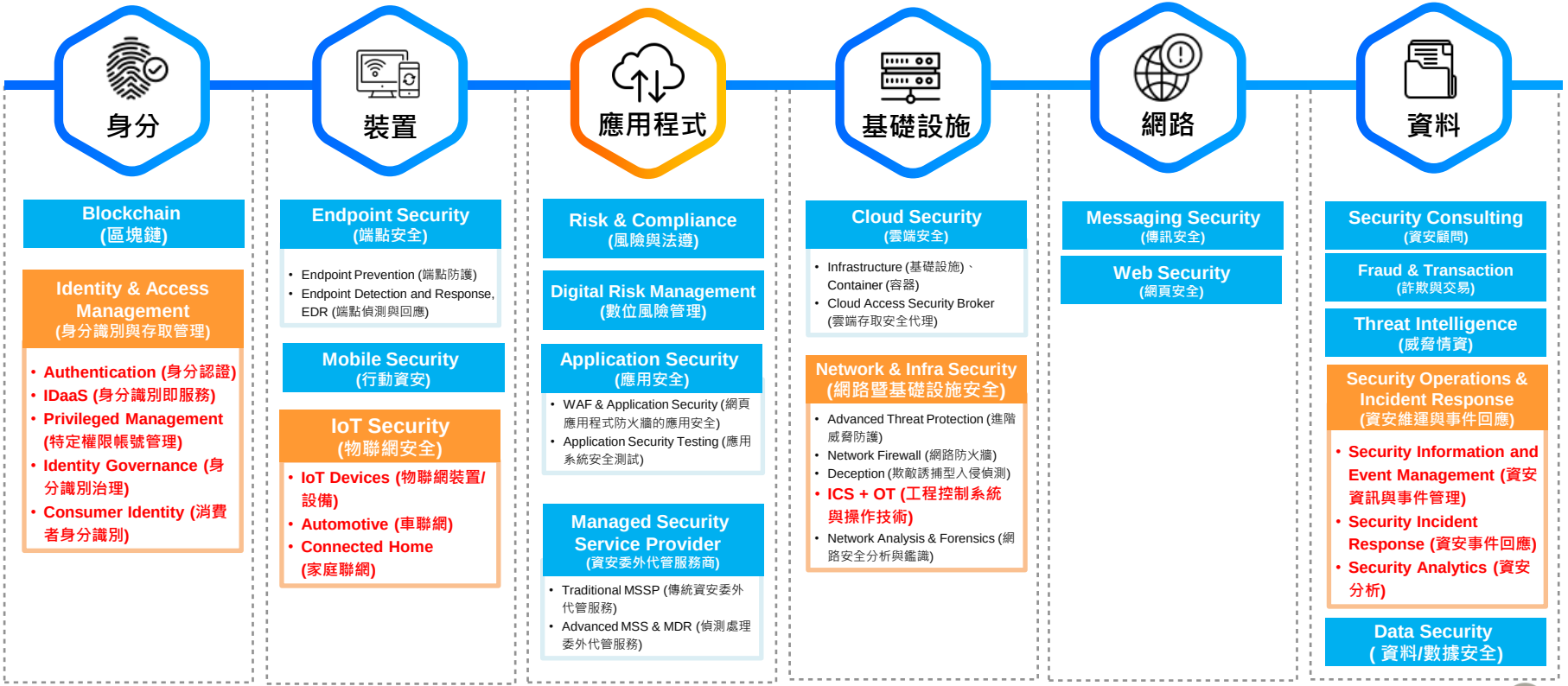
打造全方位資安防護網


Devices
裝置設備
Applications
應用軟體
Network
網路
Data
資料/數據
Users
使用者/客戶
Configuration and Systems Management
AV, HIPS
Endpoint Visibility and Control/ Endpoint Threat Detection & Response
App Sec (SAST, DAST, IAST, RASP), WAFS
Network Security (FW,IPS)
DDos Mitigation
IDS
Full PCAP
Data Labeling
Data Encryption, DLP
Deep Web, Brian Krebs, FBI
DRM
Restore Backup
Phishing Simulation
Phishing Awareness
Insider Threat / Behavioral Analytics
Identify
辨識管理
Protect
安全保護
Detect
威脅偵測
Respond
應變處理
Recover
追蹤修復

供應鏈資安挑戰解析

全球 AIoT 資安佈局重點

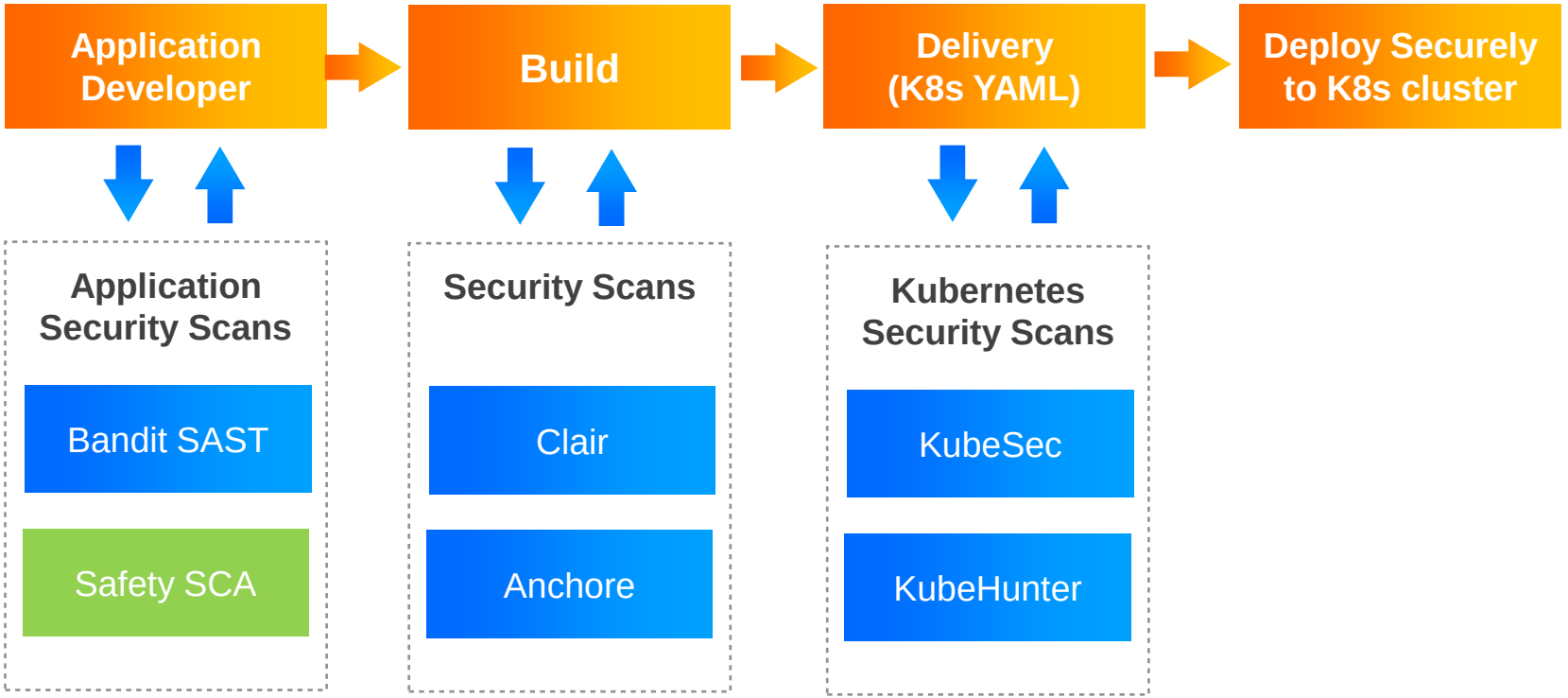
asusCLOUD



資料來源：MIC

應用程式開發安全性 DevSecOps CI/CD

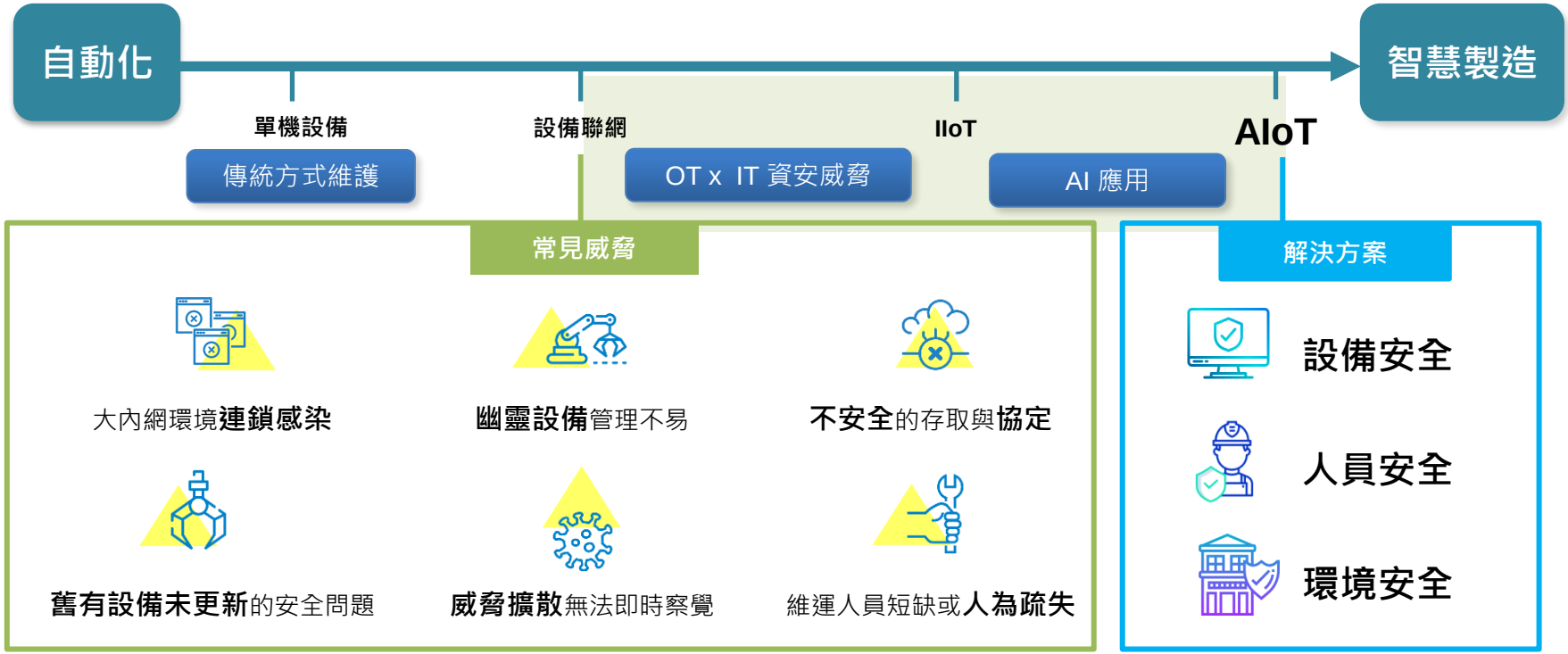
asusCLOUD



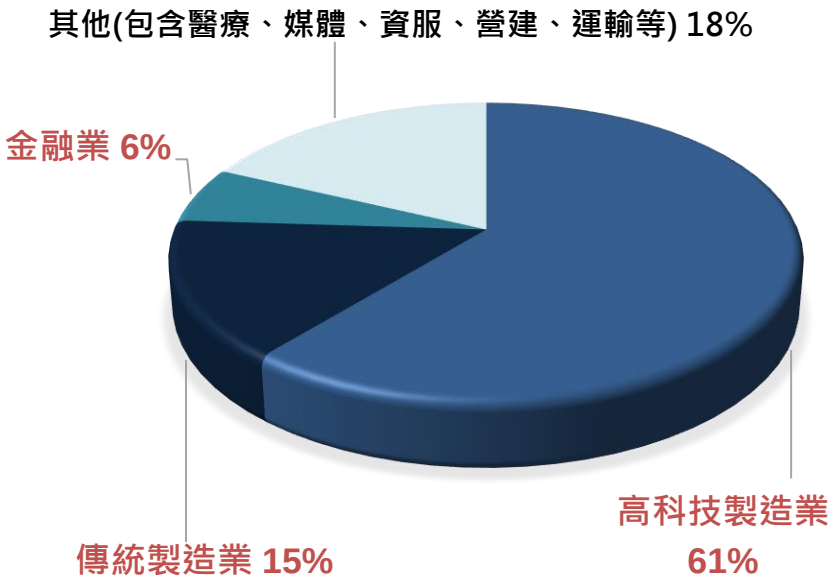
IT 與 OT 資安需求的差異

	IT	OT
性能要求	非實時性	實時性
可用性要求	一般可用性	高可用性要求
風險管理要求	機密性和完整性	人身安全及生產過程
資訊安全焦點	保護 IT 資產	保護現場系統
非預期後果	資訊安全解決方案	資訊安全工具不足
資源限制	足夠的資源	資源有限

OT 環境挑戰與解方


自動化
智慧製造
單機設備
傳統方式維護
設備聯網
OT x IT 資安威脅
IIoT
AI 應用
AIoT
常見威脅
大內網環境連鎖感染
幽靈設備管理不易
不安全的存取與協定
舊有設備未更新的安全問題
威脅擴散無法即時察覺
維運人員短缺或人為疏失
解決方案
設備安全
人員安全
環境安全

台灣製造業資安挑戰：資安事件產業歷年趨勢



76% 高科技及傳統製造業
為 2021 上半年**目標式勒索攻擊**對象

目標式勒索製造業前兩大受害者類別

48% **零組件供應商**

24% **代工廠**

Source：TXOne Networks《趨勢台灣資安應變服務團隊(CSIRT)資料》

智慧製造業資安三大需求

	跨廠區管理	設備連網 遠端連線需求	IT / OT 混合環境下 OT 資安解決方案需求
痛點	• 智慧工廠跨廠商因新舊設備產線混用，多以人力監管，未導入自動化，管理不易。	• 數位轉型加速進程，設備連網需求增加。	• 現有 IT 資安解決方案未能完全適用於 OT 環境
關鍵解方	• 高度資產可視化、網路資訊行為可視化等可協助快速發現、掌控、應變、排除事件設備連網遠端連線需求 (如數據中台，戰情中心)。	• 傳統網路實體隔離已不再是解方，需由內而外全面檢視網路系統架構與部署零信任資安防護。	• 導入 OT 資安解決方案，可即時偵測、防護與應變於工控環境中的資安問題，且兼具生產線營運與品質

資料來源：供應鏈資訊安全強化_教戰手則 (acw.org.tw)

製造業工控資安常見痛點

勒索攻擊肆虐
加密工控電腦

駭客攻擊大量加密廠區電腦資料
造成生產中斷、產能銳減

機台無預警故障
造成資料毀損

廠區機台無預警停機或故障
導致數據資料毀損或遺失

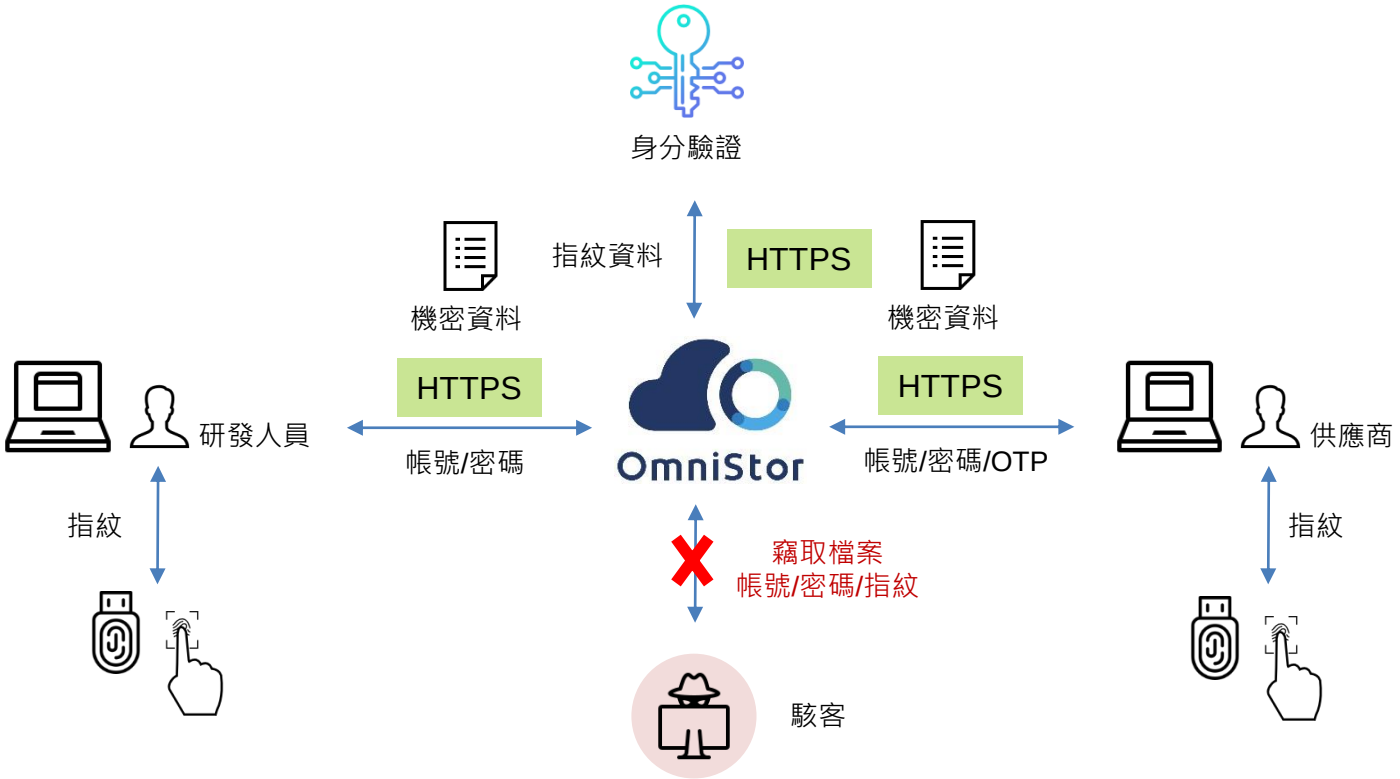
供應鏈資料交換
恐有資安漏洞

傳統交換機制有安全疑慮
郵件傳輸受大檔限制

OT 關鍵 5 大應用情境

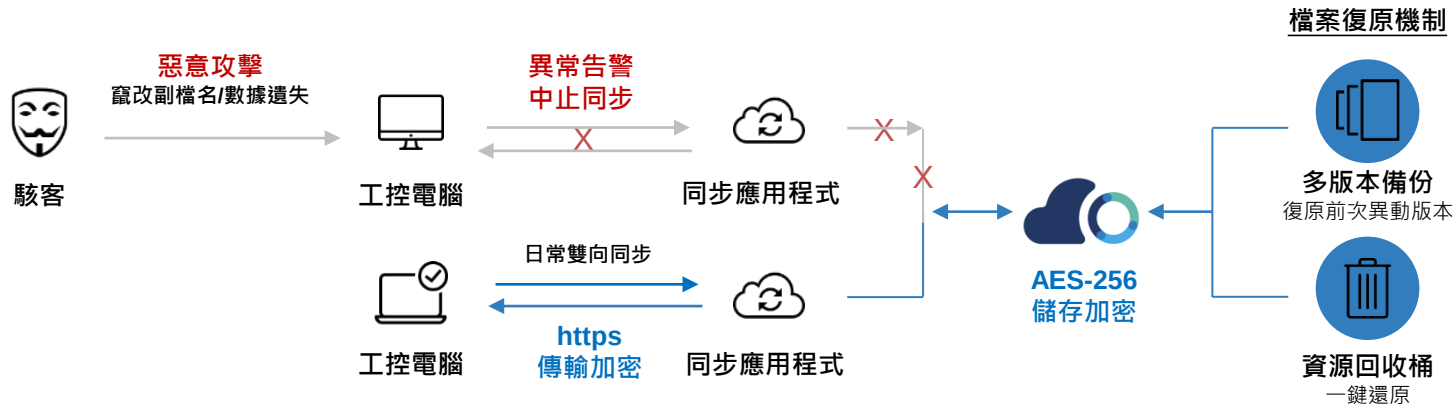
-由內而外打造檔案安全防護網-

應用情境 1：供應鏈零信任檔案交換架構



應用情境 2：工控資料安全防護

勒索病毒被視為企業資安事件的頭號公敵，常見因攻擊事件導致工控資料遺失或者遭惡意竄改，OmniStor 的異常偵測及阻斷機制，可確保資料的隔離，安全的傳輸與儲存加密，避免工業電腦連鎖感染，保障工控資料應用的安全性

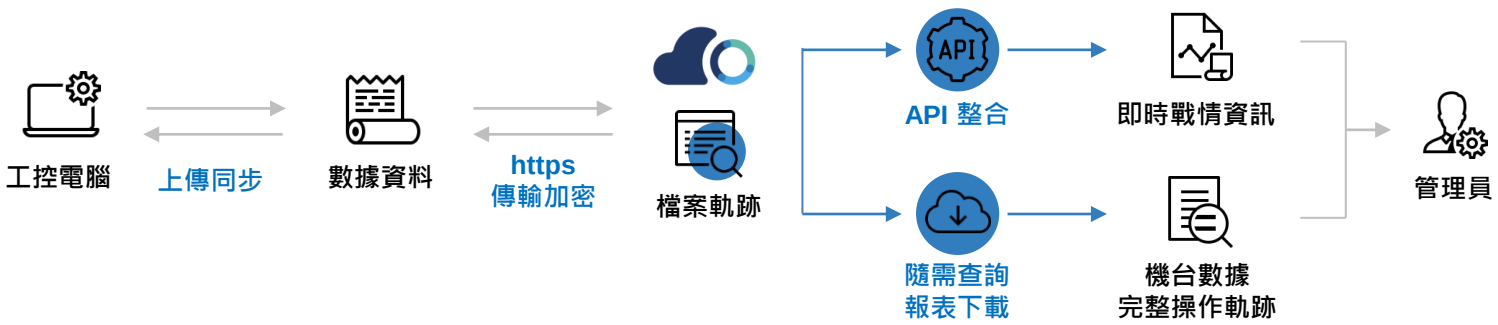


應用情境 3：威脅停損與營運持續

工控環境若遇系統及設備故障，經常影響產線的正常運作及業務營運，OmniStor 協助及時停損威脅，快速復原關鍵的 OT 數據及資料。有多個分據點的企業，在頻寬有限的情況下，亦可透過近端存取及同步的機制恢復營運

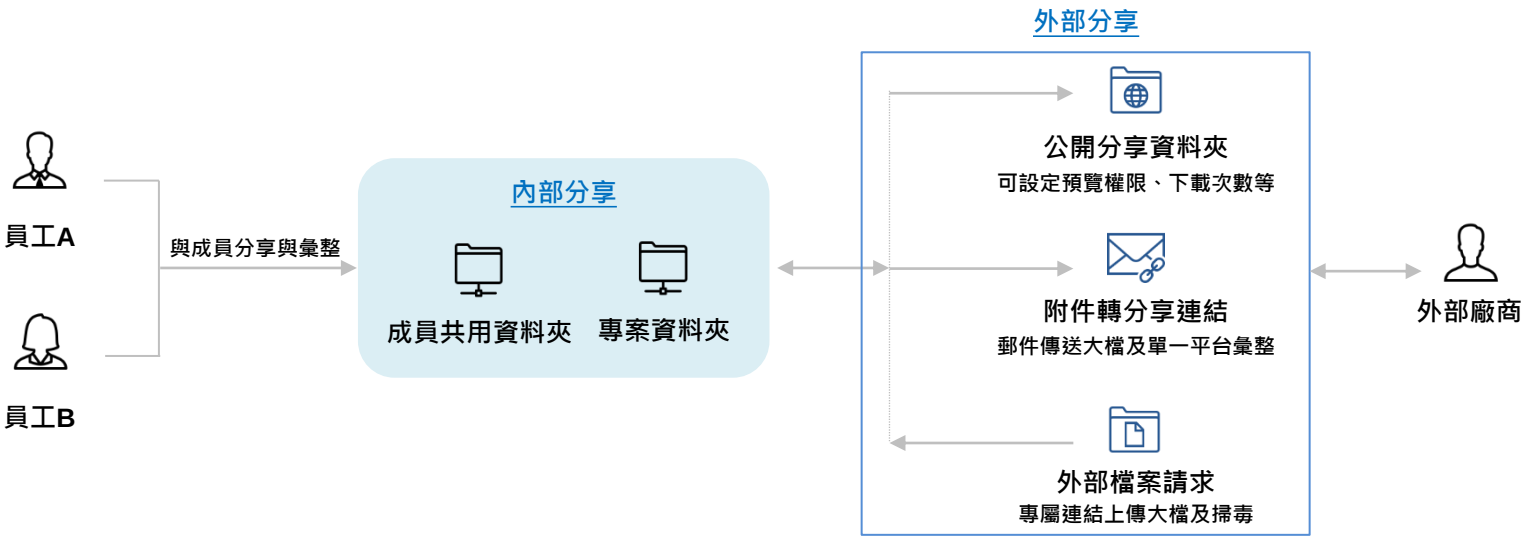
應用情境 4 ：資料軌跡實時監控

傳統儲存機制， OT 管理者不容易掌握關鍵數據傳輸及使用軌跡，若遇資安事件，對於蒐證以及監控亦是一大挑戰，OmniStor 提供完整的報表日誌，輔助管理者查閱歷史資料軌跡，更可透過 API 整合戰情分析加速產能輔助決策



應用情境 5：檔案安全分享

傳統檔案分享與交換機制，不論是未受保護的機密資料的交換機制，或是大檔傳輸工具如 USB、電子郵件、FTP 等的資安疑慮，都潛藏著各種內外部資安風險威脅，OmniStor 透過單一平台針對各類資料分享設定安全機制，兼顧資產保護與協作效率，驅動產業創新



實戰案例分享

IPC 工控系統資安保護方案

華碩雲端與夥伴協助半導體龍頭客戶為 IPC 工控系統打造全方位的資料保護方案，從威脅防禦、攻擊停損、營運持續性三大層次，提供了以下應用：

威脅防禦

- **磁碟系統狀態監測**
  實時監控系統健康狀態，發生異常及時告警
- **應用程式白名單**
  控管產線應用程式存取權，防中毒或勒索威脅
- **檔案異常行為自動偵測**
  遇竄改副檔名或大量刪除異常狀況，立即告警阻斷威脅

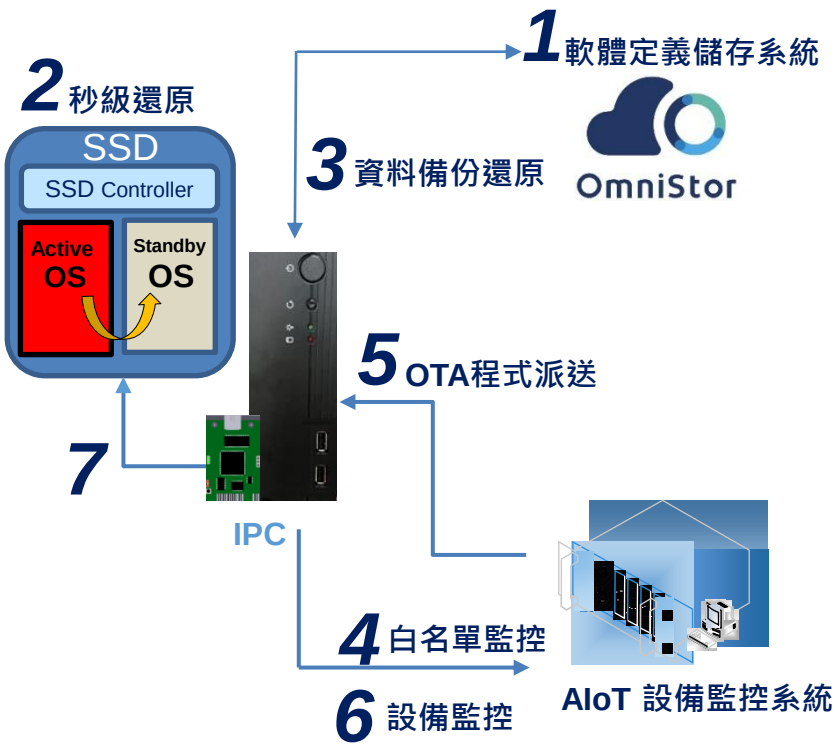
攻擊停損

- **磁碟系統快照備份**：
  遇系統災難可透過容錯機制即時還原，快速恢復營運
- **無接觸式備份還原**：
  透過遠端下指令即可重啟工業電腦，節省人力與時間成本

營運持續

- **產線資料自動備份及還原**
  自動備份重要生產數據，遇災難快速復原

應用案例：IPC 工控系統資安保護方案架構



應用案例功能

1. 軟體定義資料儲存系統
2. SSD 秒級備份/還原系統
3. 資料備份還原
4. 應用程式白名單防護
5. OTA 程式派送
6. 設備監控系統
7. 遠端電源控制系統

縮短計畫性停機時間與 IPC 異常導致產能下降

- 停機時間縮短 **51** 倍，**3** 小時縮短至 **3.5** 分鐘
- 產能加大
- 更快反應產線，彈性調整


asusCLOUD
THANK YOU