

建構雲端時代的 網路安全防護

Axis台灣地區專案業務經理
羅翊峰



議程

- 網路安全 – 目標與威脅
- Axis 採取的方式
- Axis 如何協助您達成網路安全目標



IoT 世界

網路安全和實體安全緊密相連。

一個領域的漏洞通常會影響另一個領域，例如：

- ▲ 未經授權的存取
- ▲ 設備篡改
- ▲ 資料外洩
- ▲ 營運中斷

網路安全的 3 大支柱 – C.I.A.

Confidentiality
機密性

資訊只能由授權方
存取

Integrity
完整性

資訊不應被外部單位
篡改

Availability
可用性

授權方取得資訊的權
限不應受到干擾

但現實是...

Confidentiality
機密性

使用者資料和憑
證遺失

Integrity
完整性

不信任

Availability
可用性

停機時間

常見的風險與威脅

未經授權的
存取

內部威脅

惡意軟體感染

DDoS 攻擊

社會工程攻擊

供應鏈攻擊



終端用戶面對的挑戰

- ▲ 外部攻擊，例如未經授權的存取、勒索軟體
- ▲ 不斷變化的威脅情勢
- ▲ 合規和監管挑戰
- ▲ 資源限制
- ▲ 技術複雜性



挑戰

我們希望在網路安全領域成為**值得信任**
的合作夥伴。
透明非常重要。

Johan Paulsson
Axis Communications 全球技術長



Axis 公司簡介

#1

影像監控產業的領導者

1984

成立於瑞典 Lund

Network solutions

影像監控、門禁管制、
對講機與音訊系統

2023 整年
銷售額達

1.6B 美元

16億美元，15 億歐元

Trusted
ECO
SYSTEM
of partners



從 2015 年開始

Canon

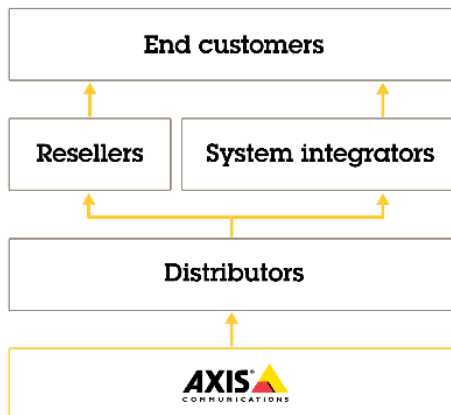
集團的一部分

從 2016 年開始

2N

Axis 集團旗下公司

2-tier BUSINESS MODEL



從 2007 年開始

Committed to

UN Global Compact

ISO/IEC 27001

認證

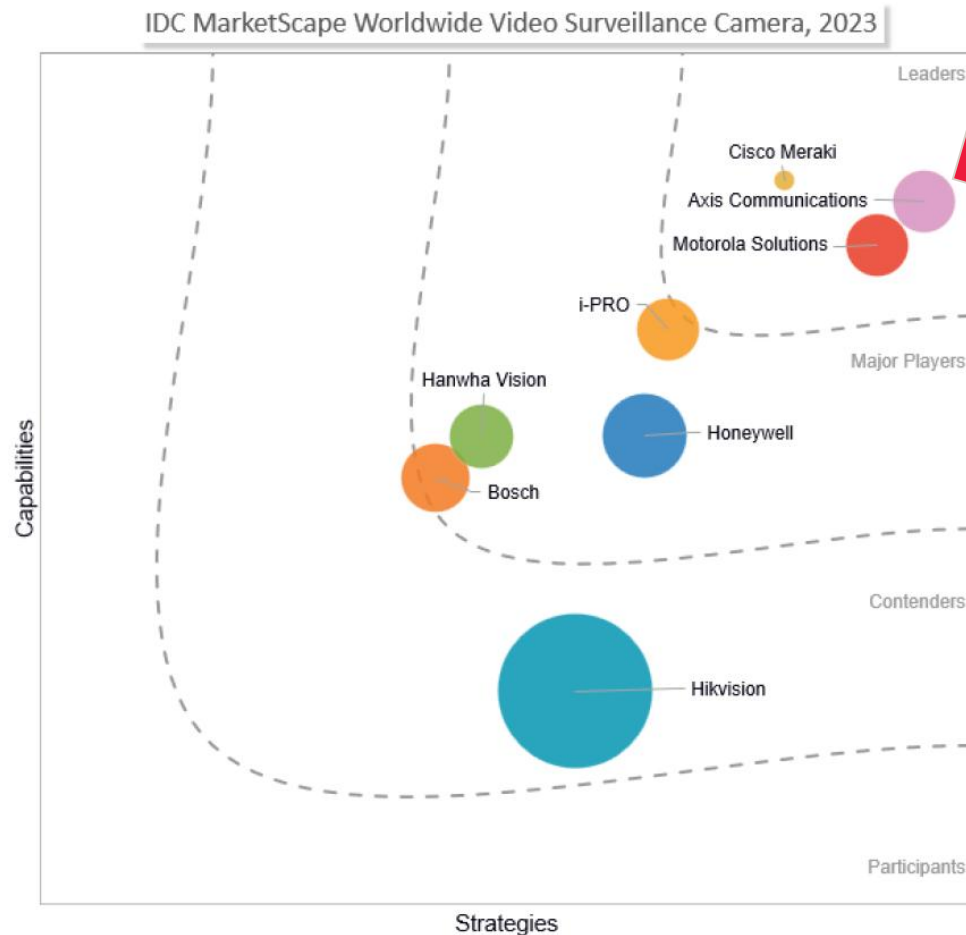
造就我們的時刻



IDC MarketScape: 2023 年全球影像監控攝影機供應商評核

AXIS Communications
在 2023 年 IDC
MarketScape 全球影像
監控攝影機供應商評核中
被評為**領導者**

根據每一家公司目前的
能力和未來的策略進行
評估



Source: IDC, 2023



Axis能滿足當前客戶需求同時策略性的針對未來產業需求做好準備的能力深獲認可

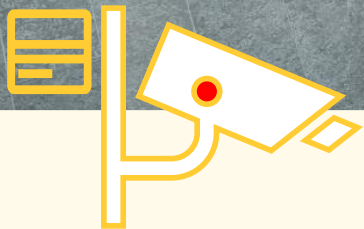
Axis針對創新與可靠性採取平衡的方式，使該公司成為應對當前與新興影像監控技術趨勢的關鍵角色

圖像來源IDC, 2023



3 層級防護

Axis透過其安全平台，提供跨邊緣、伺服器 and 雲端環境的系統防護



邊緣

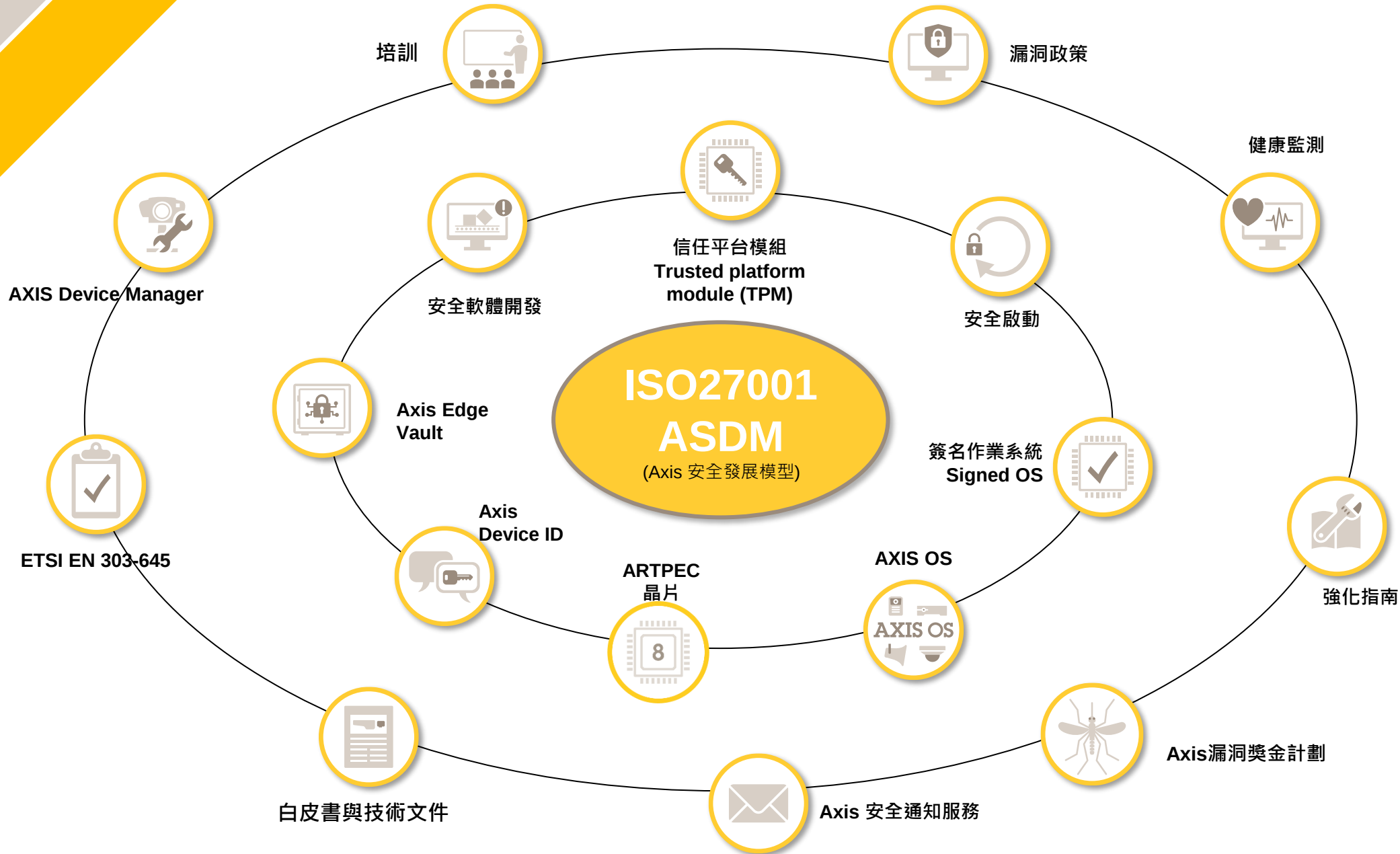


伺服器



雲端

安全基礎: 透明, Axis 安全開發模型, AXIS OS, Axis Edge Vault



監管合規性

ISO 27001

ETSI EN 303 645

NDAA

FIPS 140-3

FIPS 140-2



Axis如何支持您的網路安全目標

Confidentiality 機密性

- Axis Device ID
- 信任平台模組
Trusted platform
module (TPM)
- IEEE 802.1x, 1AR,
1AE

Integrity 完整性

- 簽署作業系統
Signed OS
- 簽署韌體 Signed
Firmware
- 簽署輸出影像
Signed Video

Availability 可用性

- AXIS Device
Manager
- 混合雲 Hybrid
Cloud

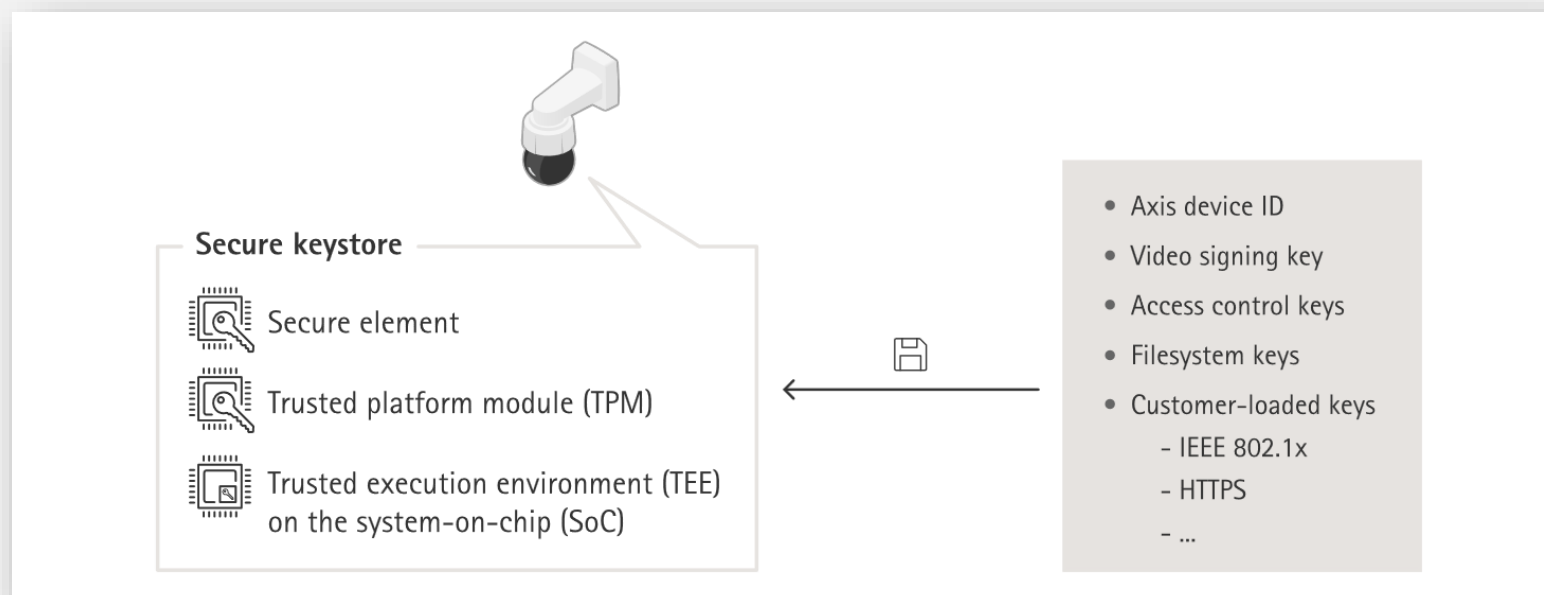
裝置認證



Axis Device ID

- ▲ 工廠提供的符合 IEEE 802.1AR 標準的認證
- ▲ 提供安全的裝置識別
- ▲ 防止供應錯誤的產品
- ▲ 允許自動化且安全的網路接入
- ▲ 確保用戶僅在網路上安裝正版Axis產品
- ▲ 減少部署時間

Axis 裝置中的金鑰庫



- ▶ Axis裝置中的安全金鑰庫可以採用安全元件/TPM/TEE
- ▶ 符合通用標準和/或最新 FIPS 140-3 3 級或 FIPS 140-2 2 級標準的要求

資料加密

▲ HTTPS

- ▲ AXIS Camera Station 伺服器與用戶端之間的 AES-256 加密影像串流
- ▲ 用於自動資料通訊加密的 IEEE 802.1AE MACsec
- ▲ 透過 SRTP/RTSPS 保護影像串流
- ▲ 邊緣儲存加密
- ▲ 匯出錄影加密

影像認證

▲ 簽名影像

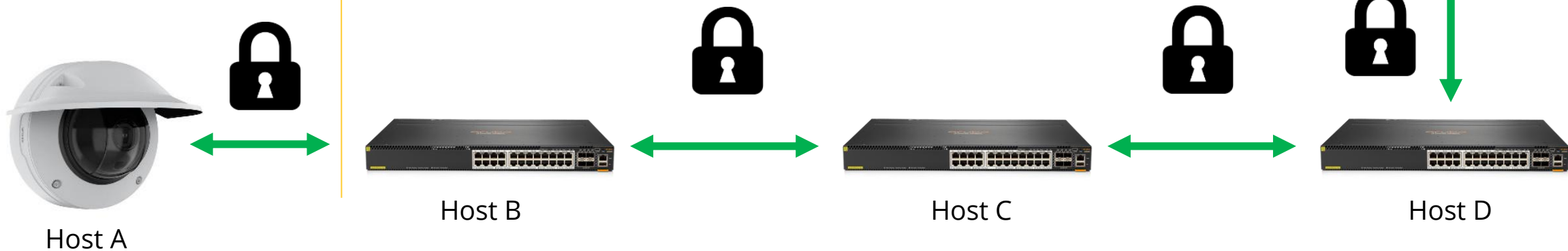
- ▲ 提供影像即時簽名
- ▲ 透過追溯到生成影像的攝影機來驗證影像的來源



企業 網路 安全

利用零信任網路安全控制，例如 IEEE 802.1X、IEEE 802.1AR

透過 IEEE 802.1AE MACsec 在基礎層面引入資料加密，以提高整體網路安全性



網路安全的生命週期方法

Axis致力於確保我們產品的網路安全，**透過透明的生命週期網路安全方式**支援先進的安全技術。



安全基礎：透明, Axis 安全開發模式, AXIS OS, Axis Edge Vault

安裝安全解決方案 – 一步一步

識別並驗證

修補

透明度

CVE編號機構

抓錯賞金計劃

AXIS Device Manager Extend

Axis安全通知服務

掌握Axis最新消息，隨時取得領先

參觀 Axis 體驗中心
實體 線上



Visit Axis Experience Center



Visit Axis Virtual AEC



羅翊峰 Jarvis Luo
Axis Communications
台灣地區專案業務經理
Email: jarvis.luo@axis.com

追蹤
安迅士臉書專頁



Follow Axis Facebook Page

訂閱安迅士
YouTube 頻道



THANK YOU

