SecuTex

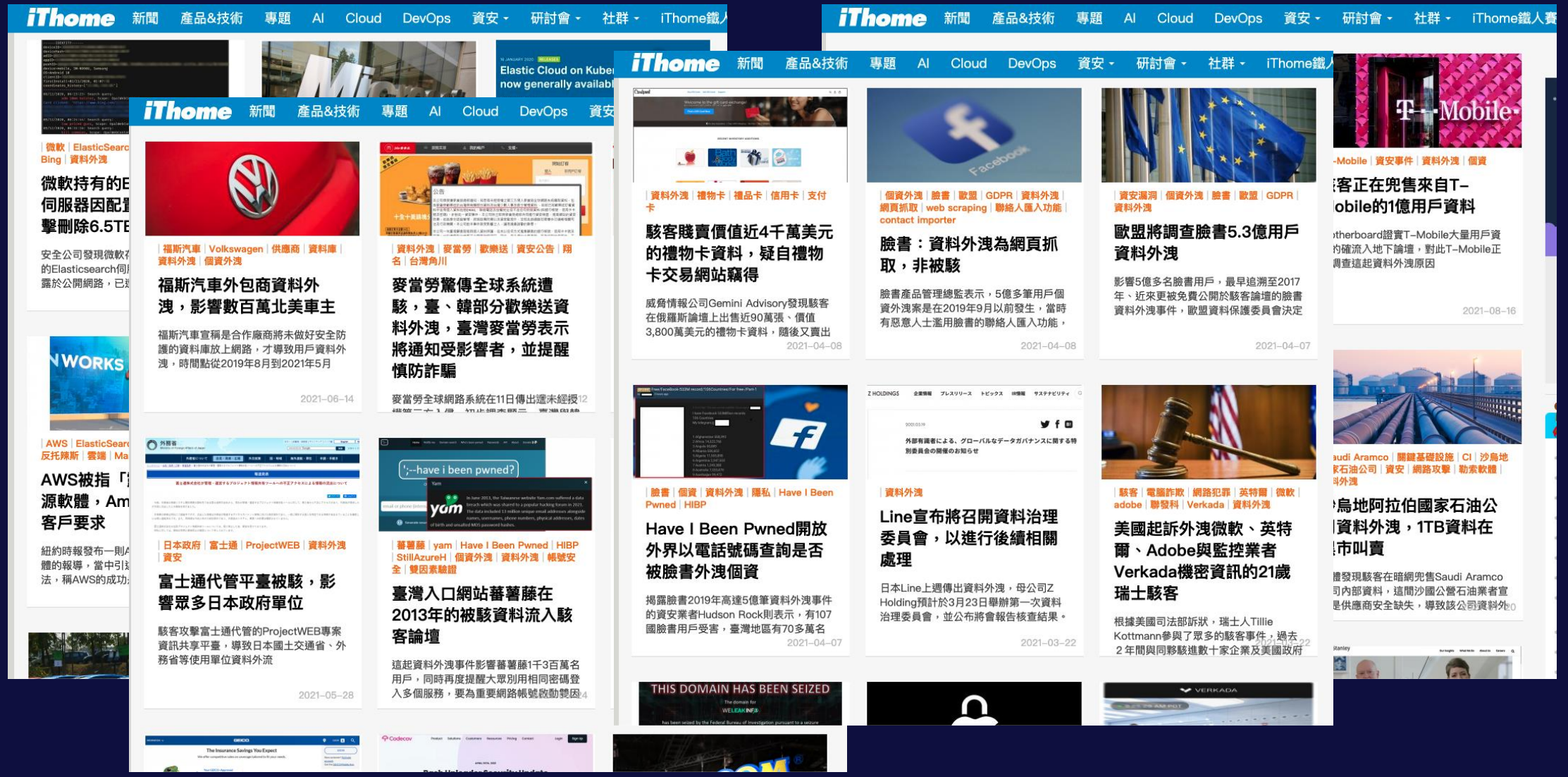
中華資安國際
CHT Security

SecuTex Network Protection
先進資安威脅防禦系統

SecuTex

資安環境說明

中華資安國際
CHT Security


iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 iThome鐵人賽
福斯汽車外包商資料外洩，影響數百萬北美車主
麥當勞驚傳全球系統遭駭，臺、韓部分歡樂送資料外洩，臺灣麥當勞表示將通知受影響者，並提醒慎防詐騙
富士通代管平臺被駭，影響眾多日本政府單位
臺灣入口網站蕃薯藤在2013年的被駭資料流入駭客論壇
駭客賤賣價值近4千萬美元的禮物卡資料，疑自禮物卡交易網站竊得
臉書：資料外洩為網頁抓取，非被駭
歐盟將調查臉書5.3億用戶資料外洩
Have I Been Pwned開放外界以電話號碼查詢是否被臉書外洩個資
Line宣布將召開資料治理委員會，以進行後續相關處理
美國起訴外洩微軟、英特爾、Adobe與監控業者Verkada機密資訊的21歲瑞士駭客
客正在兜售來自T-Mobile的1億用戶資料
烏地阿拉伯國家石油公司資料外洩，1TB資料在市叫賣
AWS被指「源軟體，Am客戶要求
微軟持有的E伺服器因配置擊刪除6.5TE
THIS DOMAIN HAS BEEN SEIZED
VERKADA

資料外洩事件頻傳

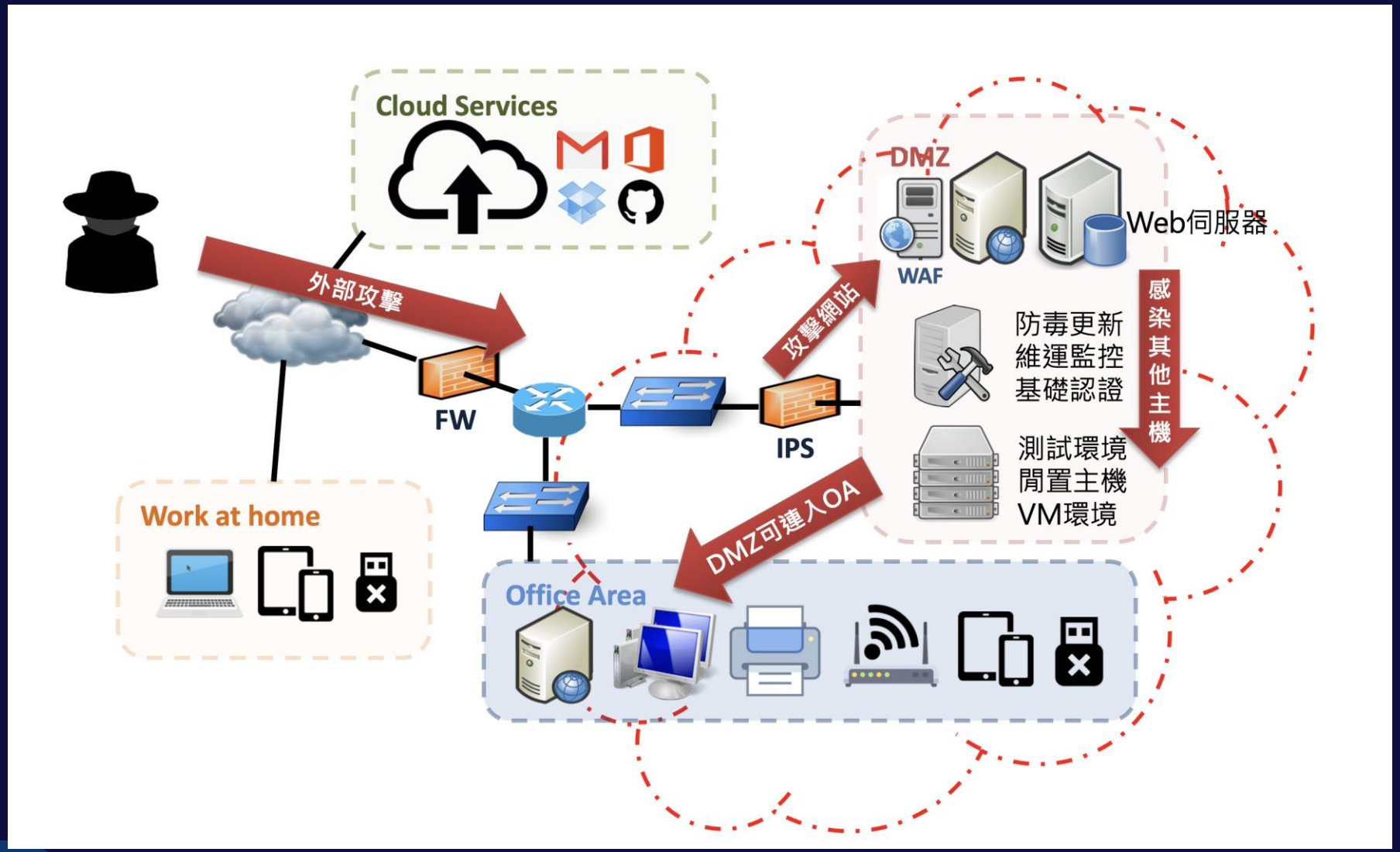
勒索軟體盛行，產業哀鴻遍野

資安威脅日增

- COVID-19疫情造成工作方式改變，企業開放網路邊界讓員工WFH，開放意味著更多的風險
  - 當發生資安事件時，企業想在短時間之內了解的事：

MIS要花多少時間才能回答上面的這些問題？

企業被駭客入侵時...


Cloud Services
DMZ
Web伺服器
WAF
外部攻擊
攻擊網站
感染其他主機
防毒更新
維運監控
基礎認證
FW
IPS
測試環境
閒置主機
VM環境
Work at home
DMZ可連入OA
Office Area

事件調查取證區域

當進行資安事件調查時，我們通常仰賴以下的資料來源：

防護死角/盲點

Firewall Log	大型企業可能會匯出Netflow或是Traffic log到SOC或是內部資料倉儲供調閱，但數量龐大，可能只包含Layer 3-4資訊，較不利於快速檢索
IDS/IPS Log	僅包含特徵名稱、風險等級與標的等，無法呈現具體觸發的內容，原因以及伺服器回應
Web 伺服器/OA主機 Log	保留了存取的相關軌跡，但資料量多時檢索不易，且在實務上很常日誌會因為設定、攻擊者竄改而失真或是資料遺失
Web Application Firewall Log	針對Web應用程式提供更深層的檢測與保護，但若設定不當可能無法完整保護網站

僅有資安偵測設備，無完整保留流量紀錄，難以重現攻擊內容及影響範圍

安全閘道

警衛

24小時監控錄影

- 偵測到攻擊時才開始保留證據
  - 沒有事前的證據
- 保留的證據不是Raw Data
  - Syslog 文字證據力有限
- 不同系統的證據需要時間彙整
  - 跨不同平台,無法即時同步調閱
- 端點跡證難以保留
  - 加密型或APT攻擊最後會消除攻擊足跡

SecuTex

SecuTex先進資安威脅防禦系統介紹

中華資安國際
CHT Security

產品功能說明

全時側錄

- 封包全速抓取
- 完整封包保存

即時檢索

- 支援連結層到應用層的封包解析
- 高達300種以上的檢索條件

即時偵測

- 即時偵測異常網路行為
- 即時惡意黑名單偵測

資安聯防

- 支援CEF日誌即時匯出
- 支援在地資安威脅情資訂閱

產品優勢

SecuTex

1 全時側錄，保存所有payload而不只metadata

2 具備攻擊偵測能力，可偵測異常網路行為及惡意黑名單

3 可擔任即時鑑識分析平台，即時採證封包匯出

4 最完整情資，掌握即時國內網路威脅與第一手網軍攻擊樣本

5 SOC整合，完整之服務流程

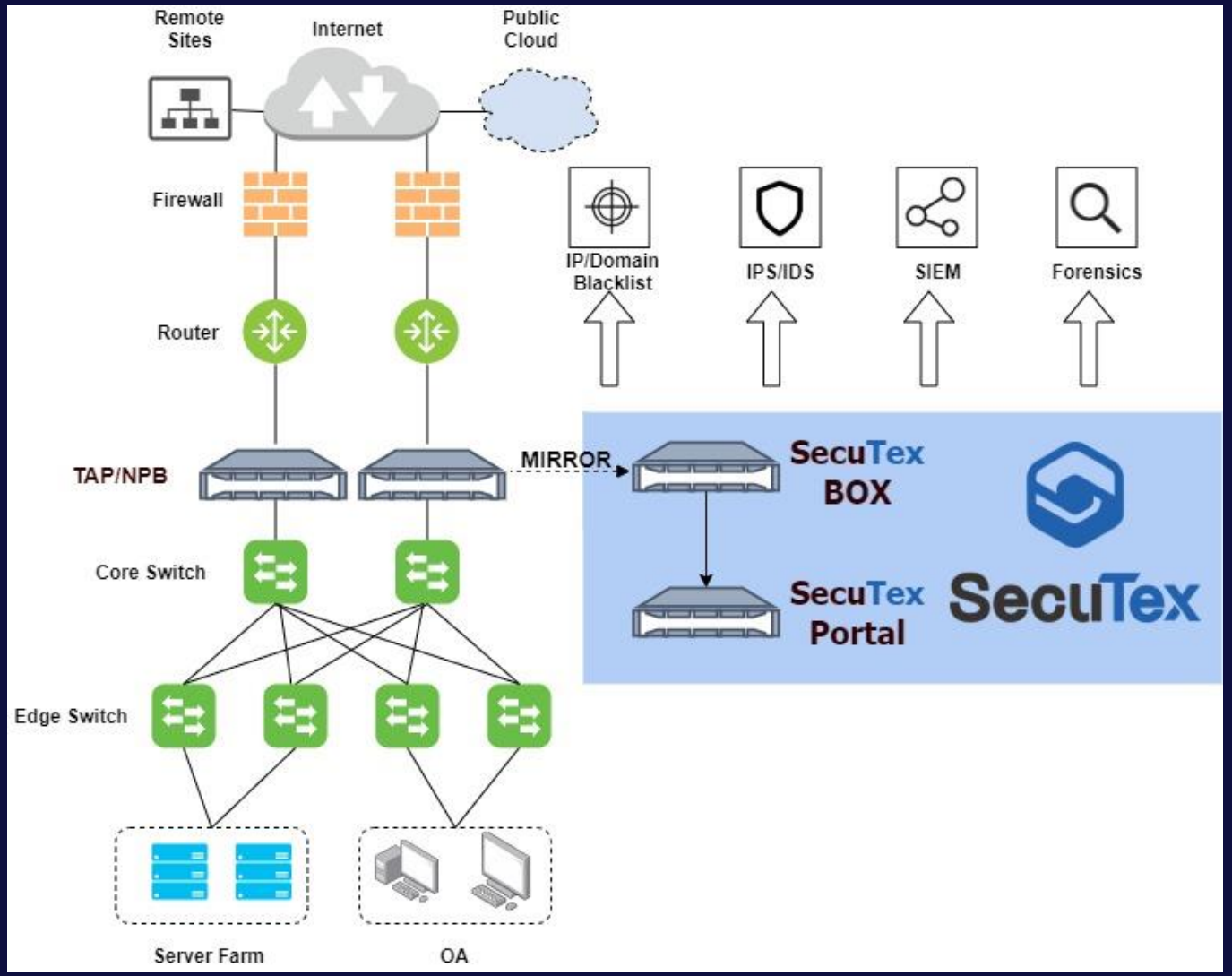
6 國內自主研發團隊，快速回應國內客戶需求

SecuTex

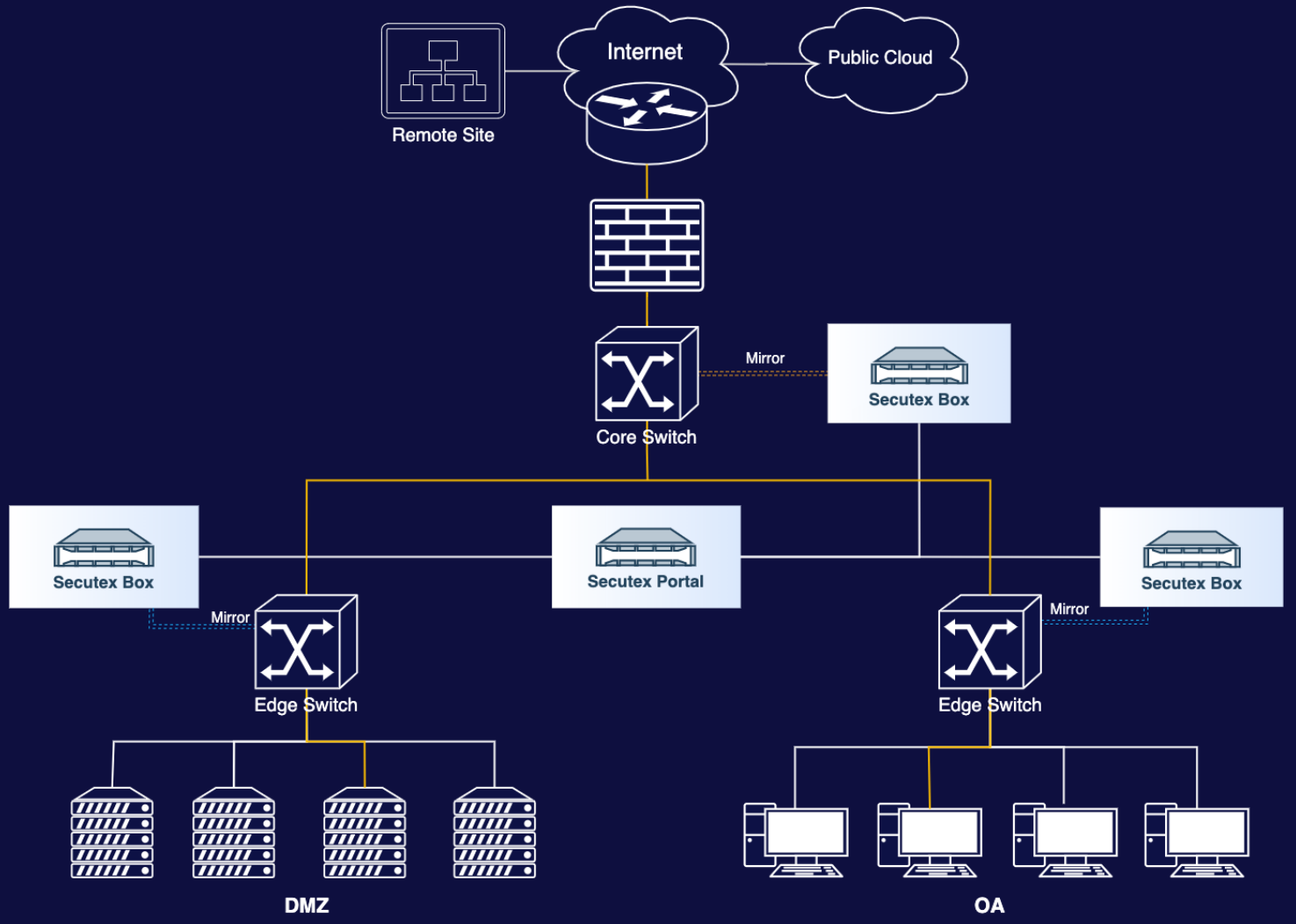
產品佈署架構

中華資安國際
CHT Security

SecuTex NP –產品架構



SecuTex NP – 部署架構示意圖 – 南北向側錄



SecuTex

產品介面展示

中華資安國際
CHT Security

風險儀表板

- 儀表板提供視覺化的風險係數、資安地圖、告警資訊、流量資訊，使用者可以輕鬆了解一日的網路風險概況，並可通過選擇不同的日期，回朔查詢過往的風險概況資訊。

謝謝您的聆聽