opengear
A DIGI COMPANY

當遇上未曾見過的環境狀況

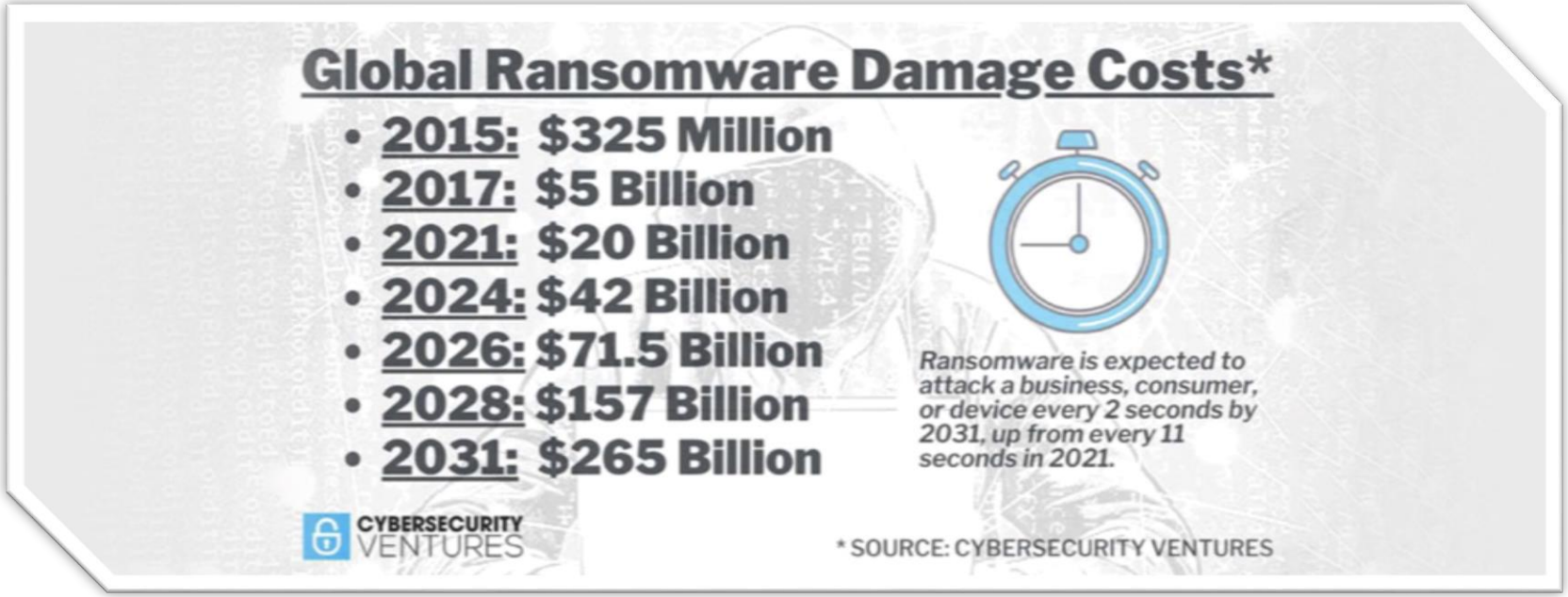
帶外管理(Out of Band Management)與網路安全保持一致

文加荣 (Vincent Boon)
亞太區銷售工程師

CIO/CTO預測與優先事項

人工智能	自動化	網路安全

網路攻擊的數量和複雜性將會增加



2024 年十大網路安全威脅

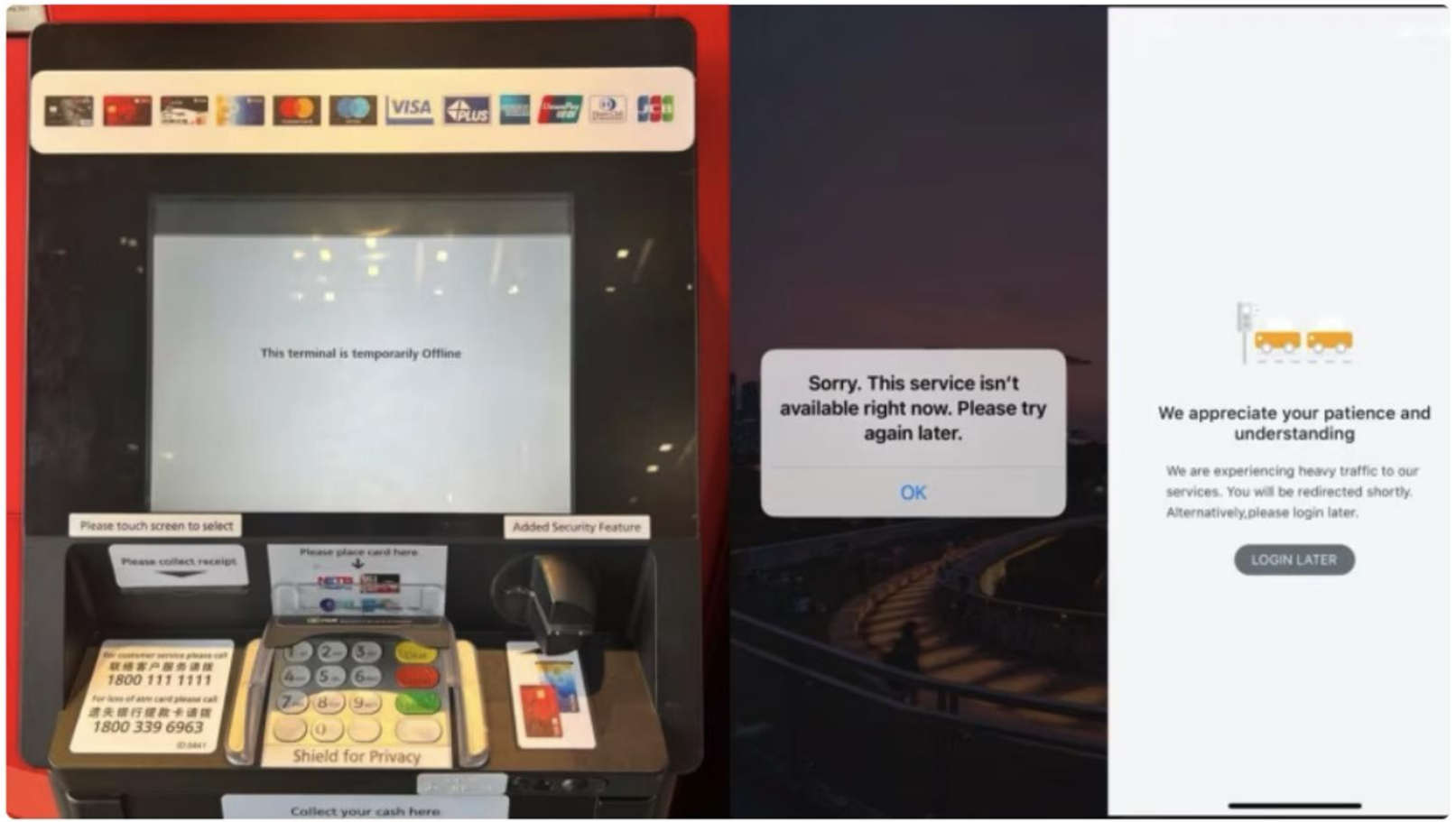
摘自 https://www.embroker.com/blog/top-cybersecurity-threats/

- 隨著科技和智能的進步，我們將會看到安全威脅變得更加複雜，因此付出的代價也會更高。
- 專家預測，到 2025 年，全球網路犯罪造成的損失將達到 10.5 兆美元，比 2015 年的 3 兆美元來的更多。

摘自 https://

X Post

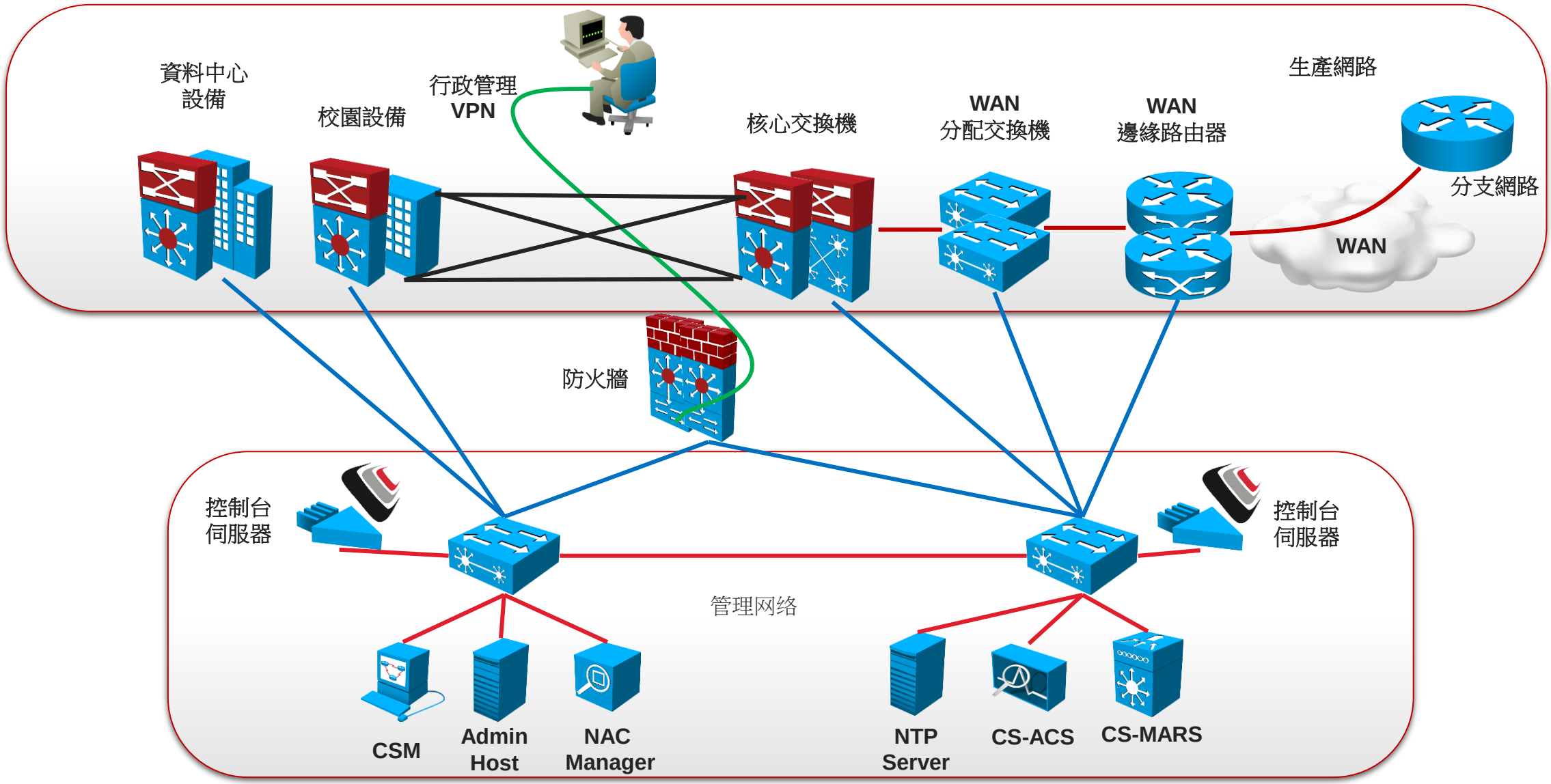
Virgin Australia
@VirginAustralia · **Follow**



An error message on a DBS ATM at Central Mall and screenshots of the DBS iBanking service page and PayLah! service during the Oct 14, 2023 banking outage that affected DBS and Citibank.

Read 6 replies

傳統的網路架構，舊有的管理方式來應對



我們面臨的問題

限制

面對傳統網路架構上，管理IT基礎設施的主要痛點是它無法很好地擴展到外部分支機構。

無法正確「引導」管理人員對於外部分支機構基礎設施的連接。

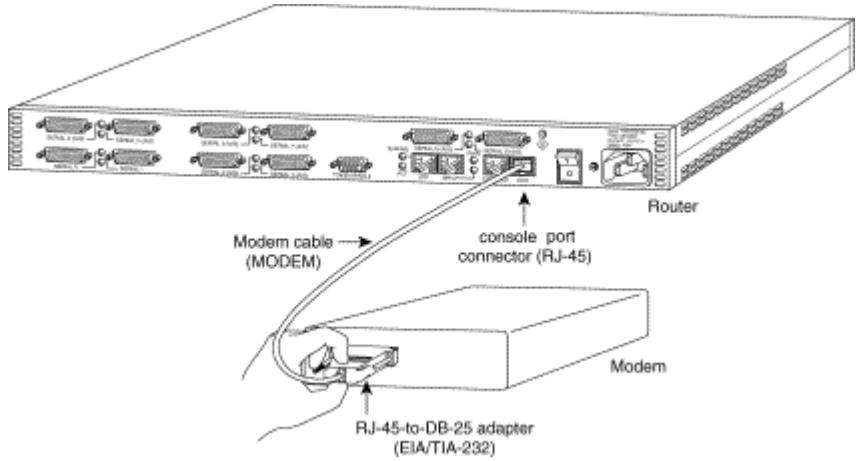
當發生這種情況時，通常只能透過其它管道來處理遠端基礎設施的安全管理問題。

預算考量

企業高層施加壓力以求降低基礎設施的管理成本。公司IT部門被要求用更少的資源做更多的事情。

「既然你們已經在那裡了，我還能用你們做什麼呢？ 老闆想做更多事，但不想花錢...」

遠端存取管理(Remote Access)的由來



- 首先使用一台數據機和一條console cable。

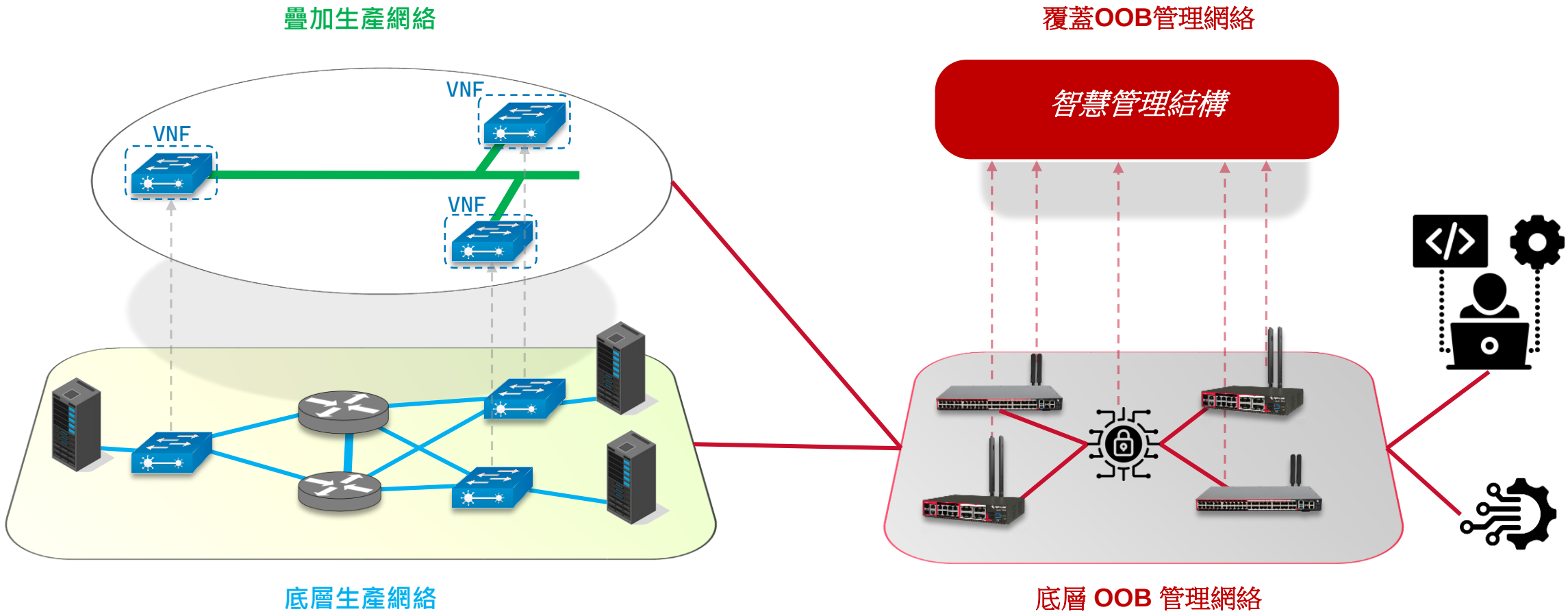
- Console server / Terminal server 是一種透過

  網路技術提供對遠程設備的系統控制台存取的設備或服務。

- 帶內管理(in-band management)涉及透過Telnet/SSH、RDP/VNC等協定管理設備。當網路發生故障且不通時，需要使用備援路徑才能到達網路節點(尤其是關鍵網路)。在這裡，我們需要一個安全的遠端緊急網路存取路徑，以便在網路流量中斷時對設備進行管理和故障排除。因此，帶外管理(out of band management)作為帶內管理工具是不夠的。
- 大多數用戶使用帶內管理來存取其端點設備。
- 現在網路已經蓬勃發展，安全性已經成為一個主要問題？

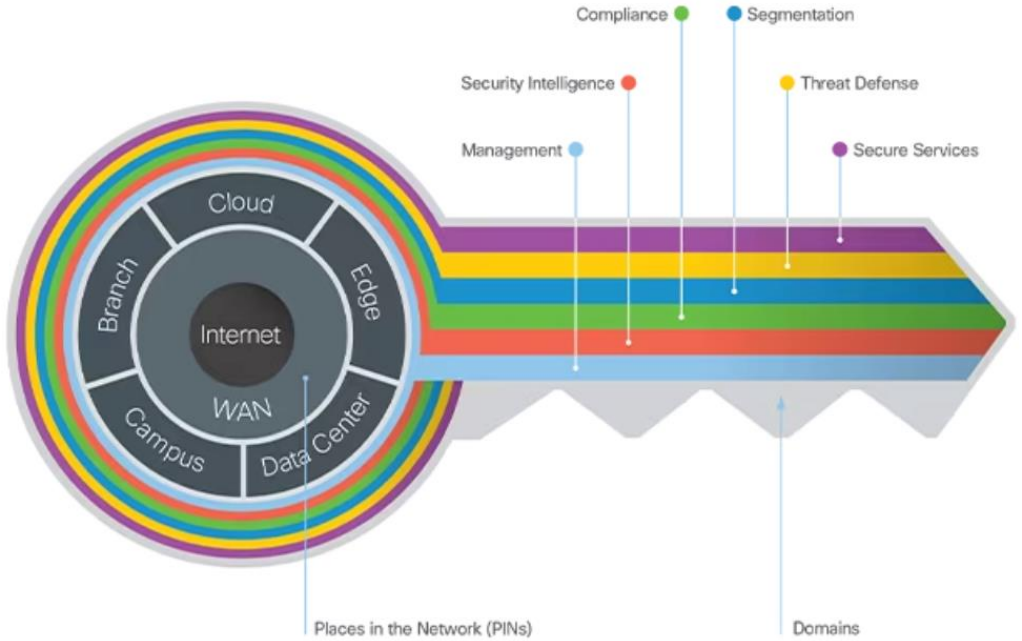
現代網路

現代帶外(out of band)管理網路 – 智慧管理結構



網路不斷發展和扁平化，安全框架也必須不斷發展

適合所有人的 SAFE KEY 安全架構



What is Blue Line?

Smart Out-of-Band

安全能力描述
記錄/報告： 集中收集事件資訊
策略/配置： 統一基礎架構管理和合規性驗證
時間同步： 設備時鐘校準。
漏洞管理： 基礎設施的持續掃描和報告
分析/關聯： 即時資訊的安全事件管理。
異常偵測： 識別受感染主機掃描其他易受攻擊的主機
監控： 網路流量巡檢

網路隔離與緊急存取:OOB專用通道

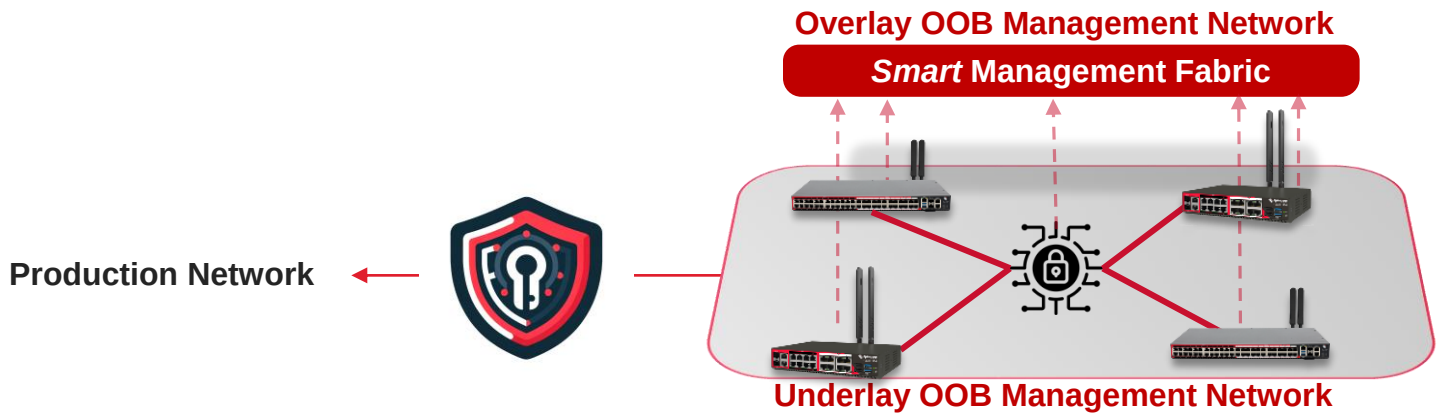
問題陳述：網路不僅面臨外部威脅，還面臨內部威脅； 依賴單一網路進行管理可能是一個重大漏洞。

目前實踐：企業經常使用複雜的多層安全措施，但某些部署情況是日常流量和管理流量同時共存在相同的基礎架構。

OOB 解決方案：

每日：**OOB** 提供獨立、安全的網絡，透過隔離管理流量來增強防禦。

當網路中斷時：提供可靠的替代訪問路線，並具有針對緊急情況的獨特憑證，從而降低風險。



透過 OOB 集中管理並實現安全部署和復原

問題陳述：網路安全威脅需要一個安全、有彈性的網路架構，能夠快速恢復並安全重新部署。

現行狀態：定期修補和安全部署實踐至關重要，但通常不足以從複雜的網路安全攻擊中快速恢復。

OOB 優勢：

每日：透過 **OOB** 確保持續、安全的修補過程，不受主要網路漏洞的影響。
隔離環境以根據需要限制存取。

當網路中斷時 : 即使在網路受損期間，也可以透過 **OOB** 安全地重建和重新部署生產環境。

OOB 用於增強監控、合規性和隱性安全性

問題陳述：持續監控和合規性至關重要，但可見的安全活動可能會提示未經授權的用戶，包括潛在的攻擊者。

現行狀態：安全團隊實施連接埠日誌記錄並維護事件回應手冊，但通常在主網路內，有暴露和乾擾的風險。

OOB 解決方案：

每日：**OOB** 網路提供安全、隱藏的監控和記錄通道，遠離窺探。

當網路中斷時：自動化劇本可以對主網路之外的事件做出反應，確保謹慎回應且有效回應。

OOB 作為可信營運的基礎

問題陳述：在不斷變化的安全威脅中，維護網路配置和資料完整性的可靠事實來源具有挑戰性。

現行狀態：組織依賴可信任平台模組(TPM)、安全複製協定(SCP)和資料收集解決方案，但通常與其操作環境位於同一網路中。 加密靜態資料可以保護文件和文檔，確保只有擁有權限的人，才能存取它們。

OOB 整合：

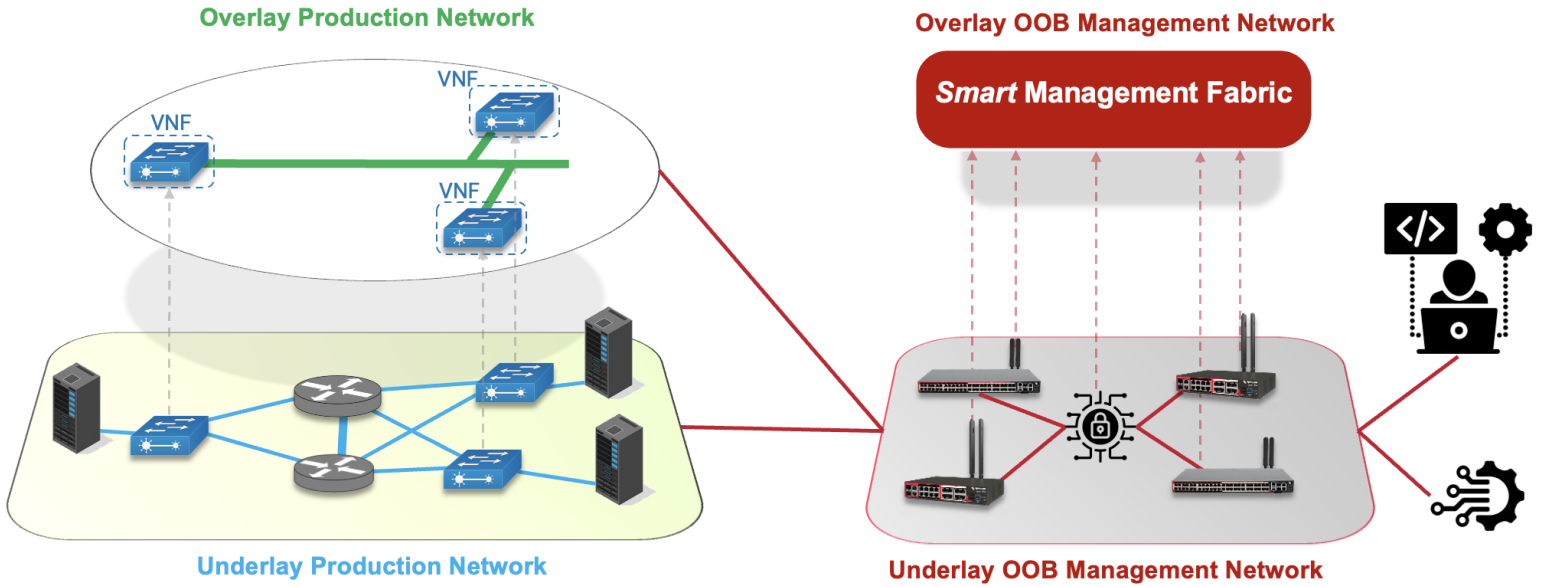
第一天：建立 **OOB** 作為配置和資料「真實來源」的安全路徑，獨立於主網路。

每日：透過隔離、受保護的路徑增強資料收集和安全配置儲存。

：擴大安全工具的範圍，同時確保其營運免受網路威脅。

總結

- 網路安全是一項持續的日常活動。
- 您的網路必須有具有不同憑證的替代存取路線，以應對緊急情況，從而降低風險。
- 不要使用您的日常網路來管理您的網路基礎設施。



opengear
A DIGI COMPANY

Thank You

www.opengear.com