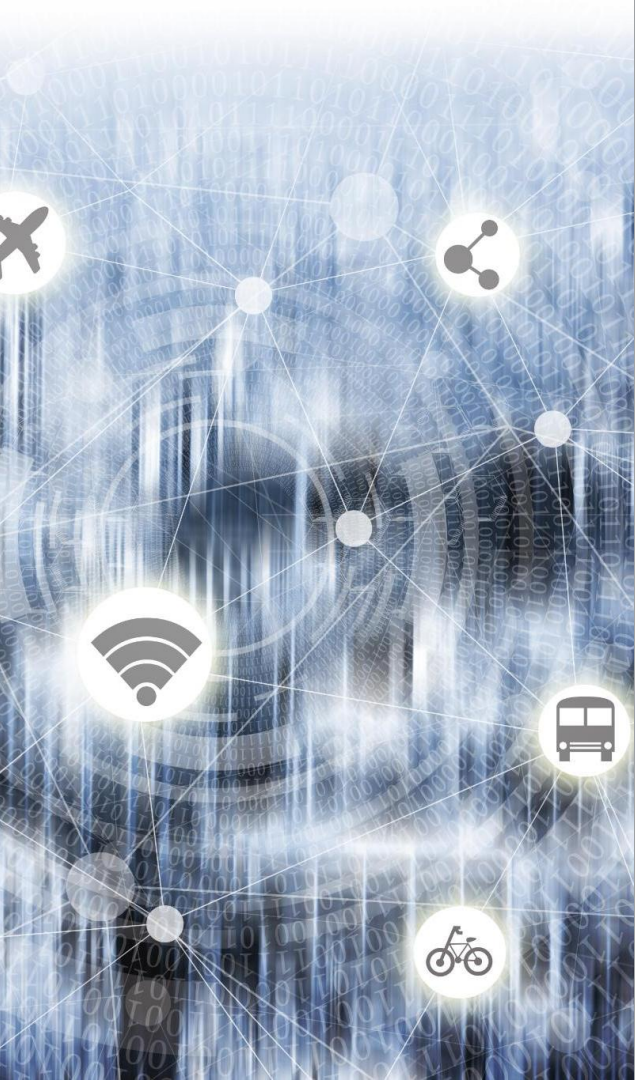
AI 驅動-新世代可視性網路

Public Sector & Service Provider
林文棋

- Network Visibility
- Simple Network Management-Cisco DNAC
- Application Visibility-Cisco Thousaneye
- Simple Security Management-Cisco Security Cloud Control
- Unify Data platform-Cisco Splunk
- AI NOC-Cisco AI Canvas
- AI SOC-Cisco Foundation AI
- Q&A



What is Network Visibility

全面性的網路監控
網路可視性可實現對企業網路中所有裝置、活動及流量的即時監控。

強化安全性與效
可視性能幫助及早偵測網路安全威脅，並有效提升網路效能管理。

支援複雜的網路環
網路可視性對於管理包含雲端服務、物聯網與遠端工作者在內的複雜架構至關重要。

促進疑難排解與管控
它能協助 IT 團隊快速識別並解決網路瓶頸，確保業務運作順暢。

Why is Network Visibility Important?

網路安全風險偵測
網路可視性能即時偵測惡意軟體與未經授權的存取等威脅，強化企業安全性。

效能管理
可視性能協助識別包括延遲與壅塞在內的網路瓶頸，從而提升使用者體驗與營運效率。

法規遵循
網路可視性能協助企業遵循 GDPR 與 ISO 27001 等法規，降低法律風險與聲譽損害。

跨平台監控
它可實現對地端雲端與遠端環境的監控，確保現代企業的網路安全與穩定性。

Management tools

Campus and Branch

Catalyst Center
Topology, client details, location, etc.

webex
Voice and video experience

Cisco Meraki
Topology, client details, location, etc.

ThousandEyes
WAN, Internet, App Insights

SD-WAN
WAN Details

Identity Intelligence
User trust level, identity checks & reasons

Data Center

Nexus Dashboard
Data center network management.

Hyperfabric
Data center network management.

Intersight
Unified management, automation, security.

Security and Observability

splunk>
Cisco and third-party insights

Firewall
Security & connection events

ISE
Authentication Insights

Duo
Authentication & compliance

Secure Access
Private & SAAS Resource Access

XDR
Related Threat Incidents

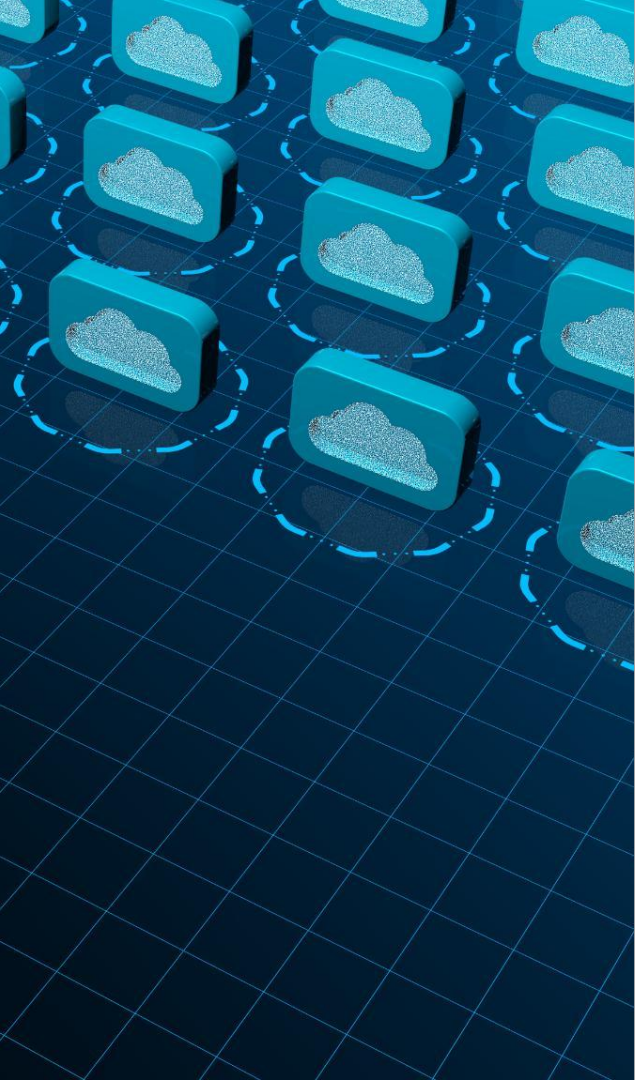
有線無線同一控管-Cisco DNAC

DNA Center 控制器
DNA Center 控制器是核心管理單元，可部署於本地或雲端，用於管理整個平台。

整合式網路設備
與 DNA Center 整合的 Catalyst 交換器、路由器及無線控制器，可實現自動化與即時監控。

安全性整合
與 Cisco ISE 及其他安全工具的整合，能加強存取控制並提供威脅防護。

即時資料收集
串流遙測能即時收集操作數據，支援自動化及 AI 驅動的網路洞察。



應用層的點對點監控-Thousaneye

網路效能監控
ThousandEyes 從使用者、應用程式與基礎架構等角度監控網路效能，以確保營運可視性。

即時問題偵測
該平台可提供即時偵測與疑難排解洞察，以快速解決網路問題。

雲端與 SaaS 可視性
ThousandEyes 提供對雲端環境、SaaS 服務及網際網路依賴性的深度可視性，以便更好地管控。

強化使用者體驗
全面性的監控可提升營運效率、使用者體驗與數位環境中的服務穩定性。

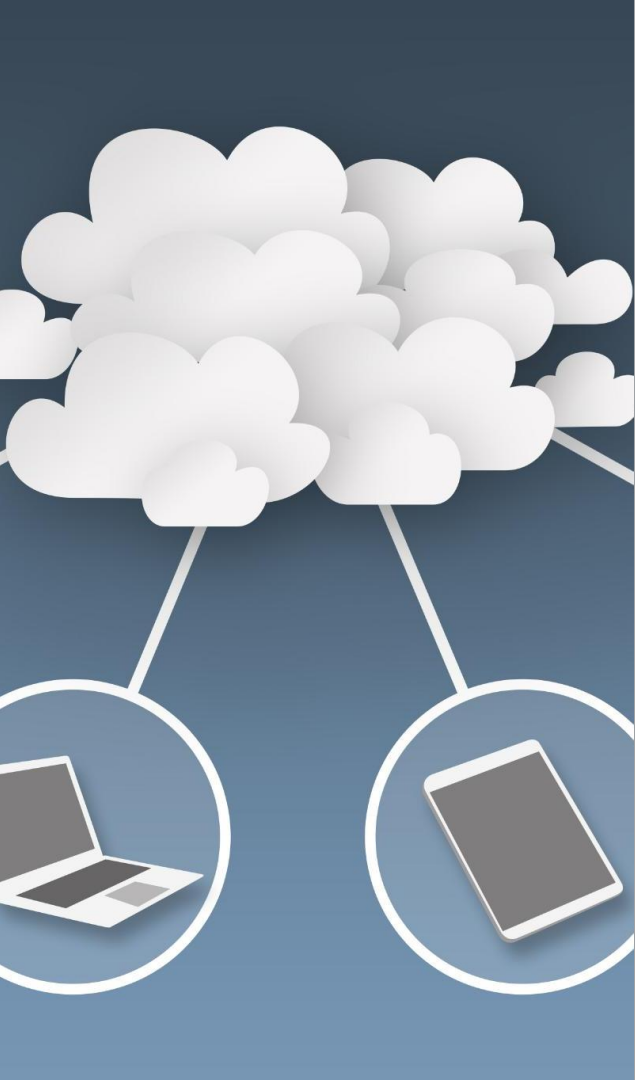
單一安全控管平台-Cisco Security Cloud Control

集中式安全管理
此平台提供統一介面，簡化混合式與多雲環境中的安全性政策管理。

AI 驅動的自動化
其雲原生設計支援 AI 自動化，以提升裝置布建、政策更新與營運效率。

整合式安全功能
可管理多項安全功能，如混合網格防火牆與零信任網路存取，以強化整體安全態勢。

簡化的管理體驗
該平台旨在降低複雜性並加速價值實現，透過將 Cisco 安全與網路產品整合至單一平台。



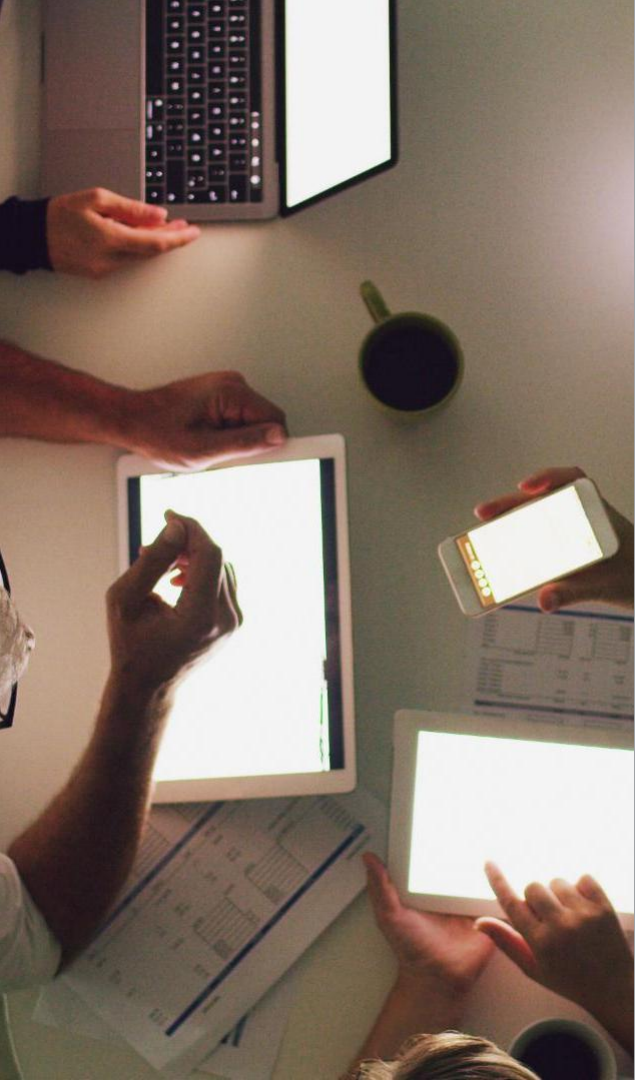
統一資料平台-Splunk

統一數據平台
Splunk 提供一個統一平台，支援安全性、可觀測性、IT 管理與商業分析。

多元化數據整合
支援來自 TCP、UDP、HTTP、檔案系統及遠端資料湖的數據，實現全面整合。

高度擴充性與彈性
該平台可從單一筆電擴展至 PB 級的企業部署，涵蓋雲端、本地端或混合環境。

可延伸的功能性
透過數千種第三方整合與自訂視覺化工具，可大幅延伸平台的功能。



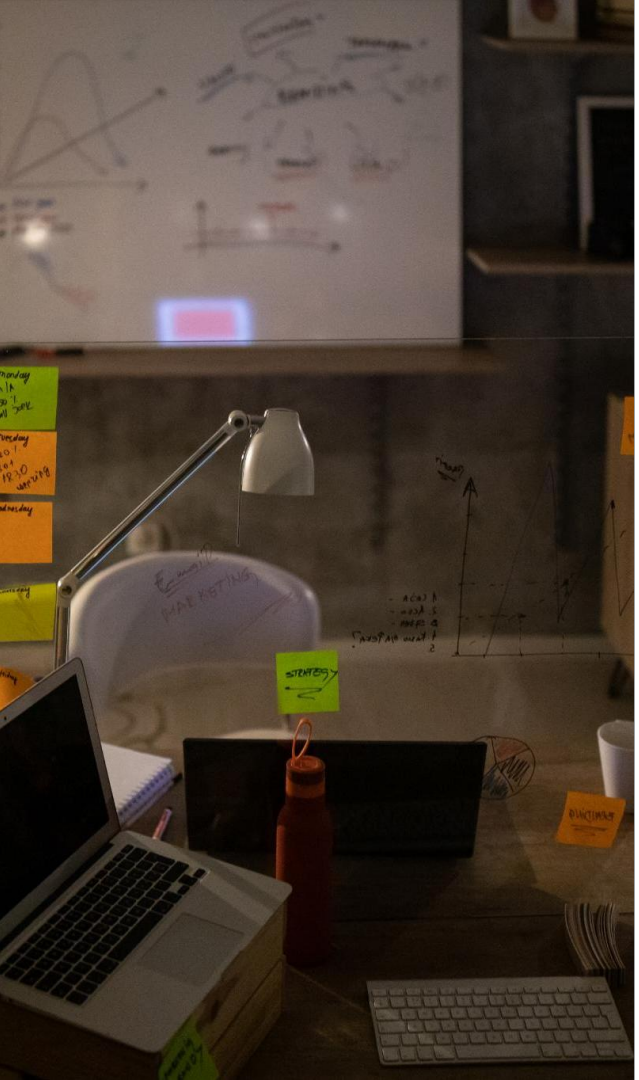
AI維運平台-Cisco AI Canvas

生成式使用者介面與推理
AI Canvas 配備生成式使用者介面與內建推理功能，可有效支援跨領域疑難排解。

統一智慧工作空間
此平台將即時遙測、AI 洞察與團隊協作整合至單一智慧工作空間，以進行全面性分析。

與 Cisco 裝置整合
AI Canvas 透過 Agentic 系統與分布於 Cisco 各業務單位的連接器，與 Cisco 裝置連結，以強化數據整合。

可延伸的 API 與未來工作流程整合
此平台提供 API、SDK 與 UI 元件，以便與其他產品整合，並規劃與 ServiceNow 的無縫工作流程整合。



開放架構

協作式調查工作空間
AI Canvas 可搭配 Splunk ITSI 等工具，實現高效的事件分析與協作式調查。

可延展的多領域架構
該平台採用 MCP 架構，以支援廣泛的 AI Agentic Ops 整合，並強化跨平台協作。

工作流程應用程式整合
AI Canvas 可與 Webex Contact Center 等工作流程應用程式整合，確保使用者操作與溝通的無縫體驗。

可自訂的 API 與框架
內部團隊與合作夥伴可透過提供的 API 來自訂與擴充平台，以符合特定需求。

Lists | SRTK0023940 | SRTK0023941 | SRTK0023942

Details

Application performance degradation at San Jose branch office

Assign Resolve Open in AI Canvas Save

Priority	State	Category	Updated by	Impact
P1	New	Inquiry/Help	Jackie Miller	High

Ticket

Ticket *
SRTK0023941

Incident type *
Network performance

Priority *
P1

Affected service *
Enterprise Financial Platform (EFP)

URL *
https://finance.example.com/transactions

Description *
Received a ThousandEyes alert and reached out to Maria Chen to confirm. She said users at San Jose branch experiencing frequent transaction failures and timeouts in EFP. Started approximately 30 minutes ago. Affects all 24 users at the branch. No recent changes reported.

Reported by *
System Administrator

Timestamp *
03/28/2025 09:45 AM PST

Rule *
ServiceNow Stg1

ID *
234945

Reported by *
System Administrator

Automated diagnostics *
- Cisco Meraki Alert: "Packet Loss Detected - SJ-MX105-01" - WARNING
- ThousandEyes Alert: "HTTP Transaction Test - San Jose to EFP" - CRITICAL
- Test Results: Test ID 895623 (URL: https://finance.example.com/transactions): 16.4% packet loss detected

One more thing…

Open Source Security LLM-Foundation-SEC-8B

專為網路安全打造的模型

Foundation-sec-8b 是一個擁有 80 億參數的大型語言模型（LLM），專門針對網路安全挑戰與操作而設計。

開源且透明

其開放權重設計讓組織在導入 AI 強化安全防護時，具備更高的透明度與彈性。

最佳化的架構與訓練

此模型針對安全任務進行架構與訓練上的最佳化，樹立業界全新效能標竿。.

應用場景

安全營運中心（Security Operations Centers）
自動化警示分類與事件摘要，提升安全營運中心的回應速度與效率。

主動式威脅防禦（Proactive Threat Defense）
支援攻擊模擬與漏洞優先排序，預先預測並減緩潛在威脅。

工程合規支援（Engineering Compliance Support）
協助程式碼審查與合規性評估，確保開發過程符合安全標準。

客製化安全整合（Customized Security Integrations）
提供符合組織需求與風險概況的量身打造安全解決方案。

Thank you