

Simply Operations with AgenticOps 用AI代理來簡化營運

Michael Wang

思科大中華區網路事業部總經理

Jackie Chen

零壹科技 資深經理

Akira Chen

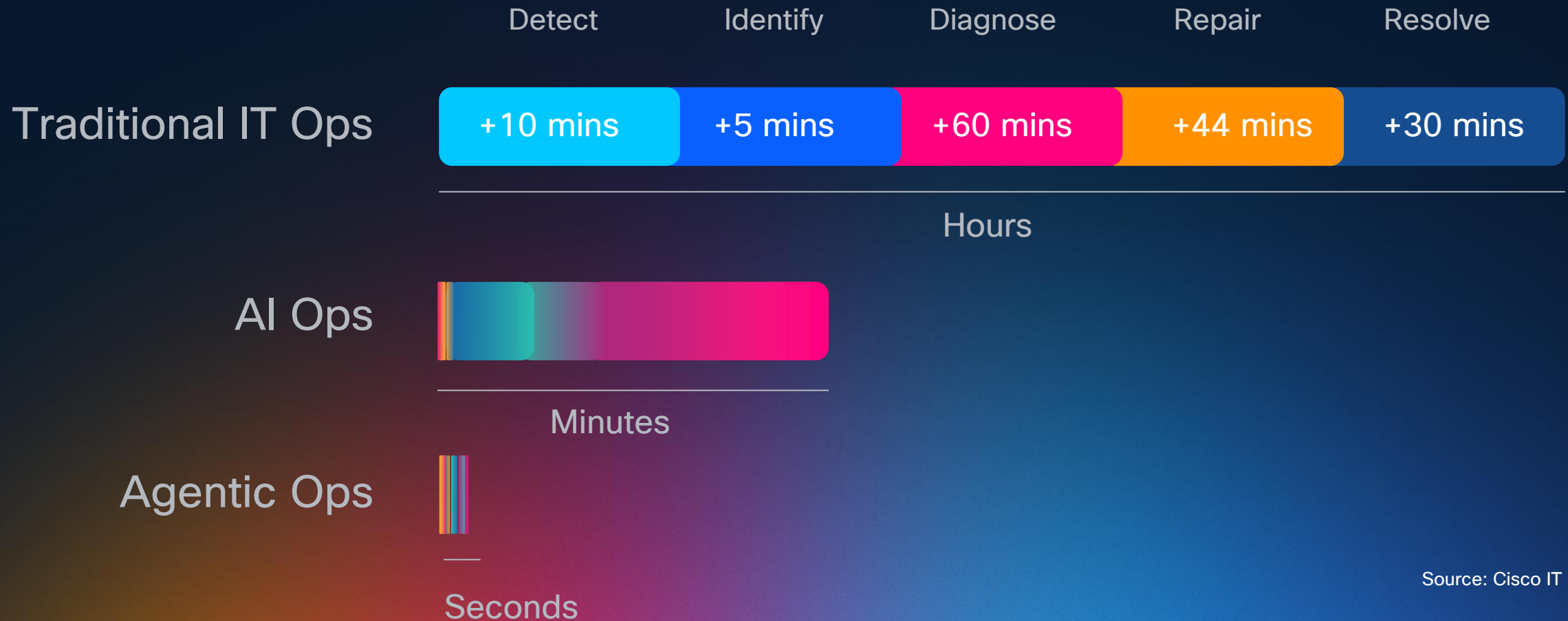
零壹科技 資深經理



AI 進化，引領無限可能

Innovate with AI. Connect with Resilience.

AI對IT維運的影響

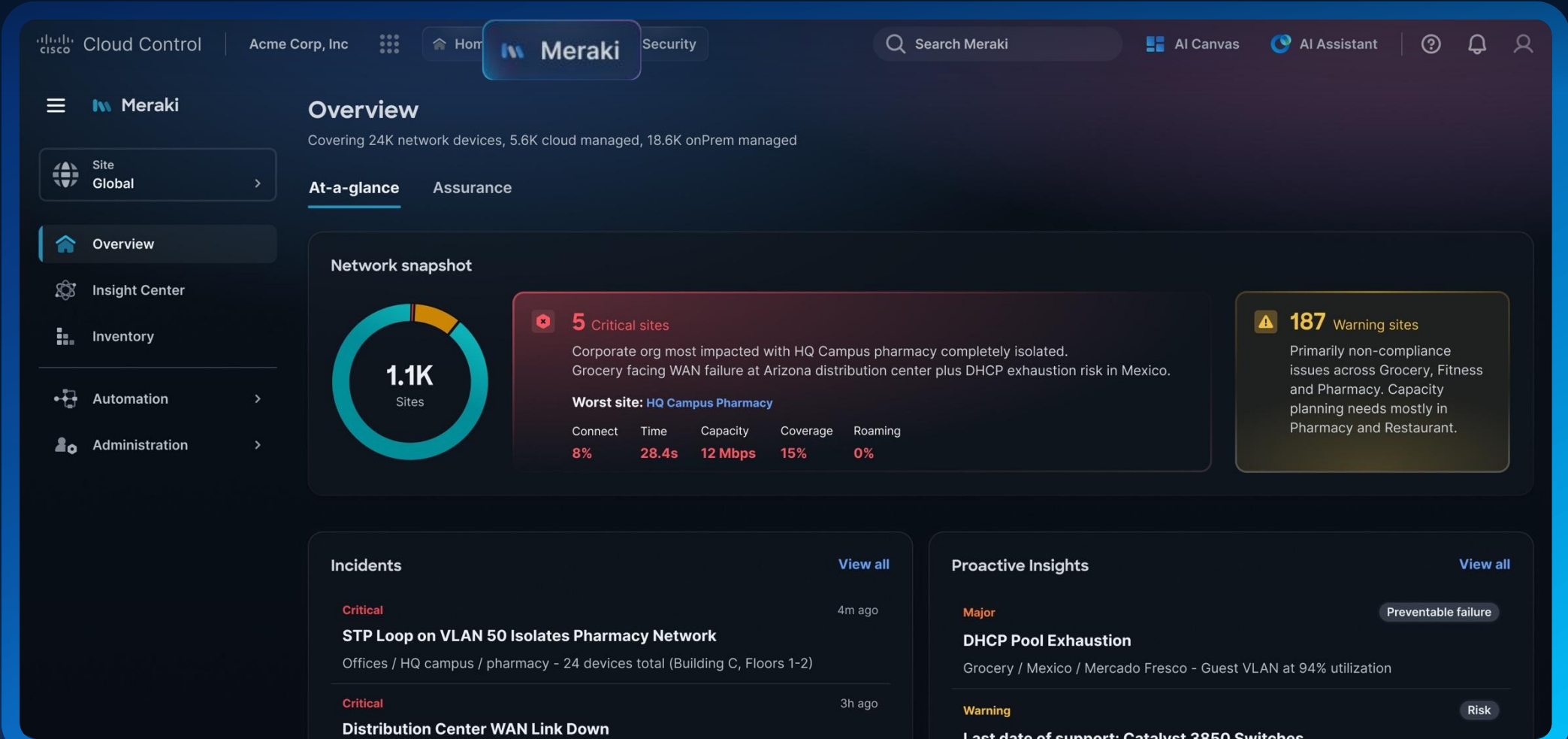


Source: Cisco IT

Controlled Availability - June 2026

Meet Cisco Cloud Control

Our cross-domain, unified platform for AgenticOps



AgenticOps

Powered by Cisco Cloud Control

AI Assistant | AI Canvas | Agent Studio | Cisco dashboards | Third party & APIs



**Cross-domain
telemetry**



**Purpose-built
models**



**Trusted
agents**

AgenticOps 簡化網路的能力

全天候24小時，提供CCIE級專業指導

自主故障排除

提供可信的根本原因與
修復方案。
幾分鐘內

持續優化

讓網路保持最佳狀態。
自動的

信任度驗證

讓每一次改變都更安全。
可預測的

Powered by deep reasoning and deterministic execution

主動式合成測試

及早發現異常

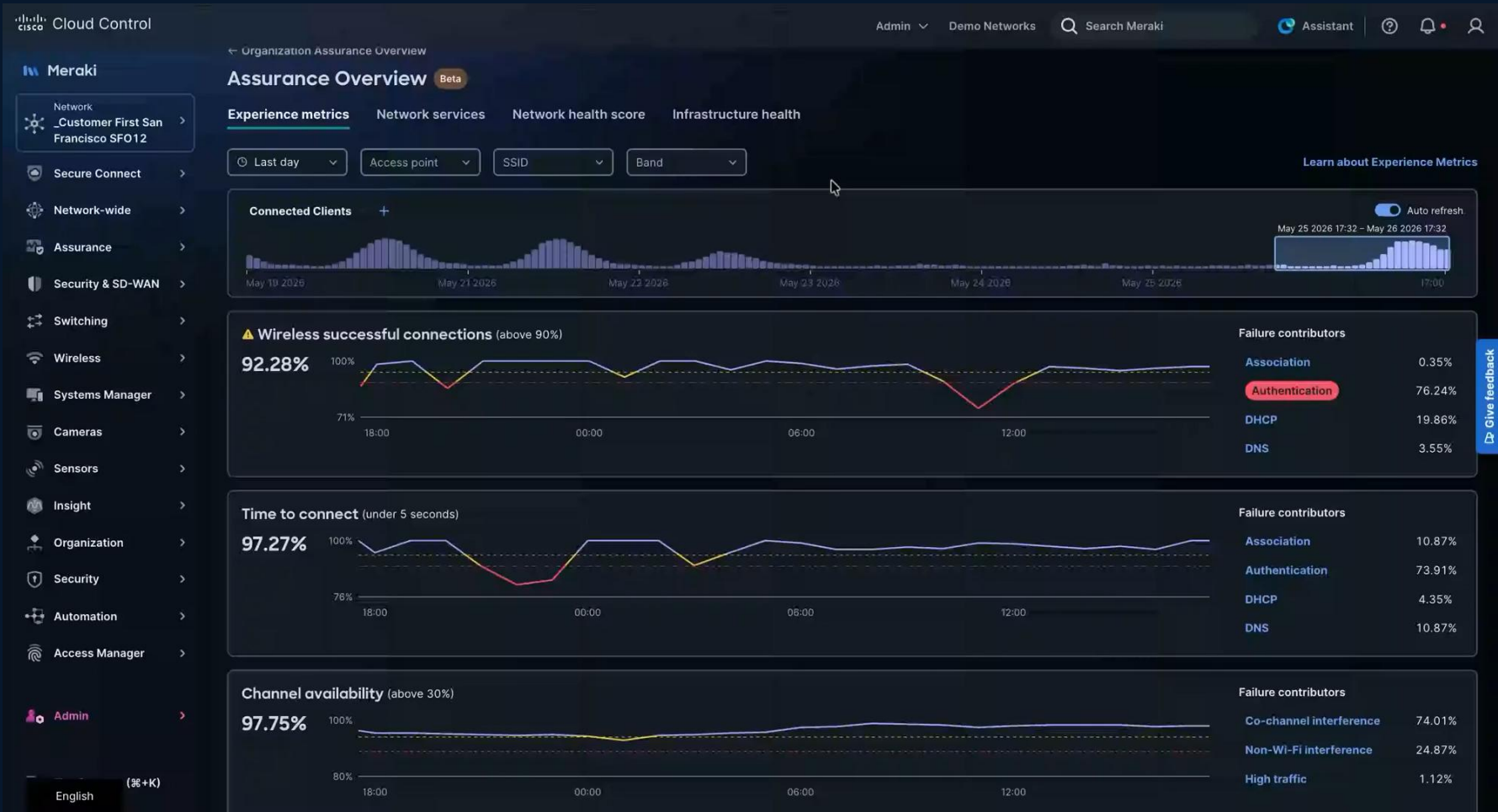
透過模擬使用者行為與網路狀況，在真實使用者受影響前識別問題。

驗證被動洞察

將被動監測的發現與主動測試相互證實，以確認潛在問題的範圍與性質。

確認爆發範圍

量化問題在不同用戶群或服務中的影響程度。



AI PCAP Analyzer

自主故障排除

Network

Acme Corp - Branch 3

Secure Connect

Network-wide

Assurance

Cellular Gateway

Security & SD-WAN

Switching

Wireless

Systems Manager

Cameras

Sensors

Insight

Organization

Security

Automation

Find in Menu (⌘+K)

English

Temporary permissions mode

Write

End temporary permissions

← All captures

Summary

AI-generated

Complete PCAP analysis

The client successfully completed association and the 4-way handshake, and a DHCP Discover was sent and received a DHCP Offer from the server. However, the client did follow up with a DHCP Request, leaving the IP address assignment incomplete.

✔ **Association and 4-way handshake** — The client successfully authenticated, associated, and completed the WPA2-PSK 4-way handshake with the AP.

📄 **DHCP Discover sent and Offer received** — The client issued a DHCP Discover, which was forwarded by the AP. A DHCP Offer was returned from the server (10.10.10.1) indicating the DHCP server was reachable and responsive.

⚠ **Block Ack negotiation difficulties** — Multiple retransmissions of Block Ack requests were observed, and the client repeatedly responded with unspecified failure status code suggesting some instability in the data path after association.

✖ **No DHCP Request following the Offer** — After receiving the DHCP Offer, the client did not send a DHCP Request to accept the offered address, leaving the IP assignment incomplete. More logs may need to be examined to determine why the client did not proceed.

Packet Flow

Reasoning

Does the analysis look good?

70:bb:5b:b3:84:50_3hlcjs_dhcp_no_dhcp_request

AI Highlighter

Bad

EAP

Management

Control

Data

Apply

No.	Time	Source	Destination	Transmitter	Receiver	Protocol	PHY type	Length
1	0.000000000	CiscoMeraki_4f:2f:40	CiscoMeraki_4f:2f:40	8e:88:91:4f:2f:40	CiscoMeraki_4f:2f:40	LLC	802.11a (OFDM)	150
2	7.680182000	CiscoMeraki_4f:2f:40	CiscoMeraki_4f:2f:40	8e:88:91:4f:2f:40	CiscoMeraki_4f:2f:40	LLC	802.11a (OFDM)	150
3	9.113179000	CiscoMeraki_4f:2f:40	CiscoMeraki_4f:2f:40	8e:88:91:4f:2f:40	CiscoMeraki_4f:2f:40	LLC	802.11a (OFDM)	150
4	16.179475000	CiscoMeraki_4f:2f:40	CiscoMeraki_4f:2f:40	8e:88:91:4f:2f:40	CiscoMeraki_4f:2f:40	LLC	802.11a (OFDM)	150
5	23.041138000	CiscoMeraki_4f:2f:40	CiscoMeraki_4f:2f:40	8e:88:91:4f:2f:40	CiscoMeraki_4f:2f:40	LLC	802.11a (OFDM)	150
6	25.292384000	CiscoMeraki_4f:2f:40	CiscoMeraki_4f:2f:40	8e:88:91:4f:2f:40	CiscoMeraki_4f:2f:40	LLC	802.11a (OFDM)	150
7	32.066879000	Apple_b3:84:50	CiscoMeraki_4f:2f:40	Apple_b3:84:50	CiscoMeraki_4f:2f:40	802.11	802.11b (HR/DSSS)	157
8	32.069451000	CiscoMeraki_4f:2f:40	Apple_b3:84:50	CiscoMeraki_4f:2f:40	Apple_b3:84:50	802.11	802.11b (HR/DSSS)	407
9	32.071672000	Apple_b3:84:50	CiscoMeraki_4f:2f:40	Apple_b3:84:50	CiscoMeraki_4f:2f:40	802.11	802.11b (HR/DSSS)	78
10	32.078149000	CiscoMeraki_4f:2f:40	Apple_b3:84:50	CiscoMeraki_4f:2f:40	Apple_b3:84:50	802.11	802.11b (HR/DSSS)	76
11	32.081354000	Apple_b3:84:50	CiscoMeraki_4f:2f:40	Apple_b3:84:50	CiscoMeraki_4f:2f:40	802.11	802.11b (HR/DSSS)	213

Packet Flow

AI-generated

Complete PCAP analysis

Packet capture timeline

⚠ DHCP no dhcp request

Apple Watch Ultra 2

Closet WIFI 7 AP

Probe Request

2

Start

Authentication

Authentication

Association Request

Association Response

2

EAPOL M1

EAPOL M2

EAPOL M3

Done

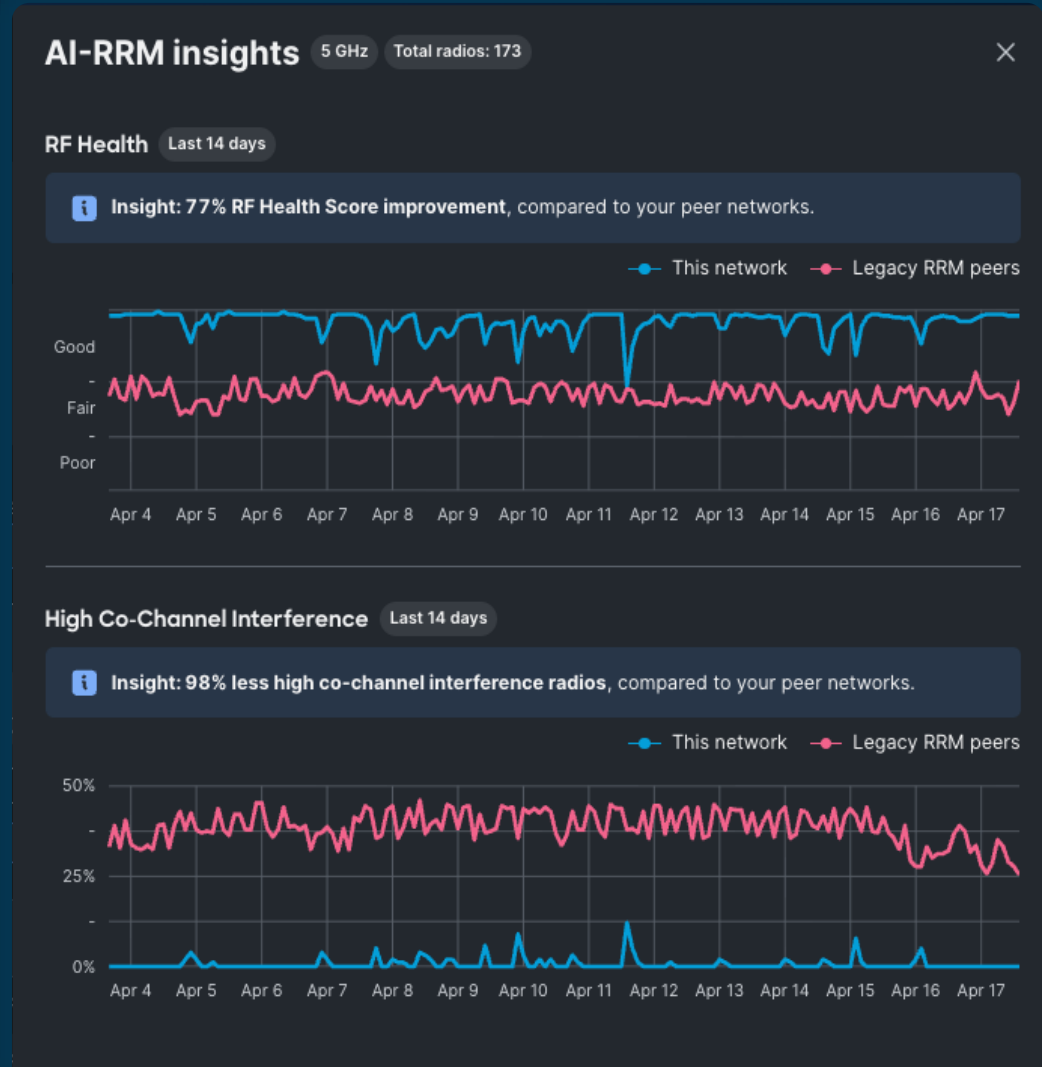
AI-RRM

RF Health – 始終連線 Wi-Fi 稽核

利用 AI 模型與遙測微調射頻

- +44% Faster Wi-Fi
- AI Busy Hour
- 射頻健康儀表板與同儕比較

*“Cisco has enabled us to be more efficient, leveraging tools like Cisco AI-RRM so we **don't have to spend much time tweaking our wireless environments.**” – Nutrien*



AI 配置建議



AI 網路優化

- 評估準備度——網路與客戶
- 預測前後效能提升
- 建議更好的效能與安全性提升設定建議



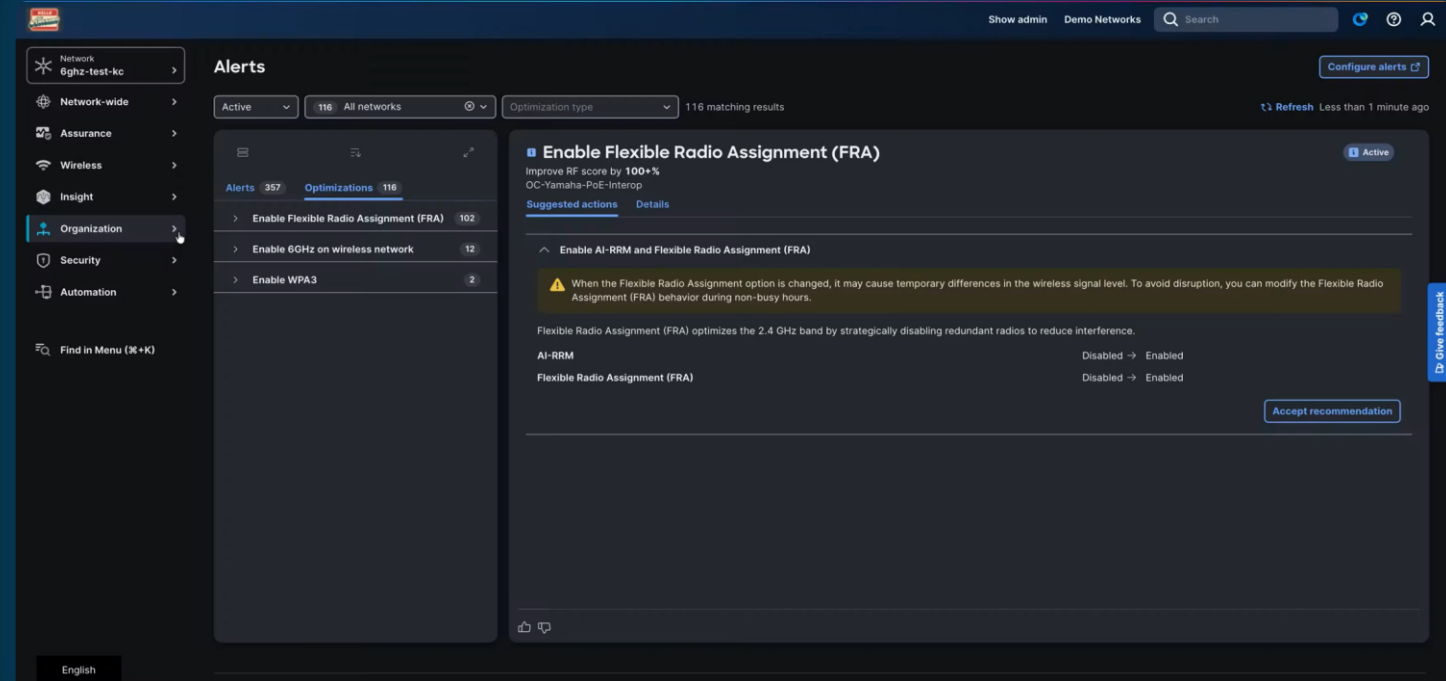
推薦類型

Available

- WPA3
- 6GHz upgrade
- 802.11r enablement
- Flexible Radio Assignment

Impact

- 安全性提升
- 更快的資料傳輸速率
- 更快的漫遊
- 減少同頻干擾



ALPHA JULY 2026

數位孿生

在套用變更前先驗證

模擬裝置、連接性與配置，呈現真正的數位孿生

The screenshot displays the Cisco Meraki Cloud Control interface. The top navigation bar includes 'Cisco Meraki', 'Home', 'Meraki', and 'Security'. The main content area is titled 'Networking actions' and 'Updated 1m ago'. A 'Monitor' button is visible. The interface shows a 'Digital Twin' section with a 'Dashboard' and 'Projects' view. The main content area displays a 'Nook-HQ-SF — IOS-XE 17.12.4 Upgrade' project. It includes a 'Validation Summary' section with a table of target images and a 'Tests to be Run' section. The 'Validation Results' section shows 15 of 15 tests passed, with a progress bar indicating 3/3 devices. The 'NEXT STEP' is to 'Deploy the twin-validated image to production via the Meraki controller for Nook-HQ-SF'. The bottom of the interface shows a 'Reasoning Log' with an entry 'Action plan defined' dated Jun 1, 9:54am EDT.

Cloud Control Cisco Meraki Home Meraki Security

Networking actions Updated 1m ago Monitor

Rogue RADIUS server Active

Digital Twin Dashboard Projects

Nook-HQ-SF — IOS-XE 17.12.4 Upgrade

Reasoned about the request

Here are all 11 devices in the twin. The 5 Catalyst switches (2x C9300, 3x C9200) are eligible for an IOS-XE upgrade — I've pre-selected them. The 6 MS120 access switches are on a different firmware track.

You can pick manually, or I can choose a minimal representative set (3 of 5) that still covers every hardware model, stack configuration, and starting version — saving validation time without losing coverage.

Search devices... All Core Distribution Access

DEVICE	MODEL	VERSION	ROLE	STACK	STATUS	
☒	C9300-1	C9300-48P	17.09.5	Core	StackWise	Eligible
☒	C9300-2	C9300-48P	17.09.5	Core	StackWise	Eligible
☒	C9200-1	C9200-48P	17.09.5	Distribution	—	Eligible
☒	C9200-2	C9200-48P	17.09.5	Distribution	—	Eligible
☒	C9200-3	C9200-24P	17.09.4a	Distribution	—	Eligible
☐	MS120-1	MS120-8FP	15.2(7)	Access	—	Ineligible
☐	MS120-2	MS120-8FP	15.2(7)	Access	—	Ineligible

Validation Summary

Target image IOS-XE 17.12.4

Device	Core	17.09.5	17.12.4
C9300-1	Core	17.09.5	17.12.4
C9200-1	Distribution	17.09.5	17.12.4
C9200-3	Distribution	17.09.4a	17.12.4

Tests to be Run

12 tests planned

- Image compatibility
- MD5/SHA integrity
- Boot mode
- DRAM
- Boot verification
- StackWise reconvergence
- Flash space
- Inactive package cleanup
- License state
- Image install
- Feature regression
- Config comparison

Validation Results

15 of 15 tests passed 3/3 devices

- ✓ C9300-1 5/5 checks
- ✓ C9200-1 5/5 checks
- ✓ C9200-3 5/5 checks

Total duration: ~12 min total

NEXT STEP Deploy the twin-validated image to production via the Meraki controller for Nook-HQ-SF.

Validation complete — use chat to export or download

Exit to production

Type your response...

Insight Organization

REASONING LOG

- ✓ Action plan defined Jun 1, 9:54am EDT

Quarantined rogue server 173.26.46.146 and re-authenticated prospective cl...

思科AgenticOps開放生態 MCP Servers

Most of AI Capability has been ready in Dashboard

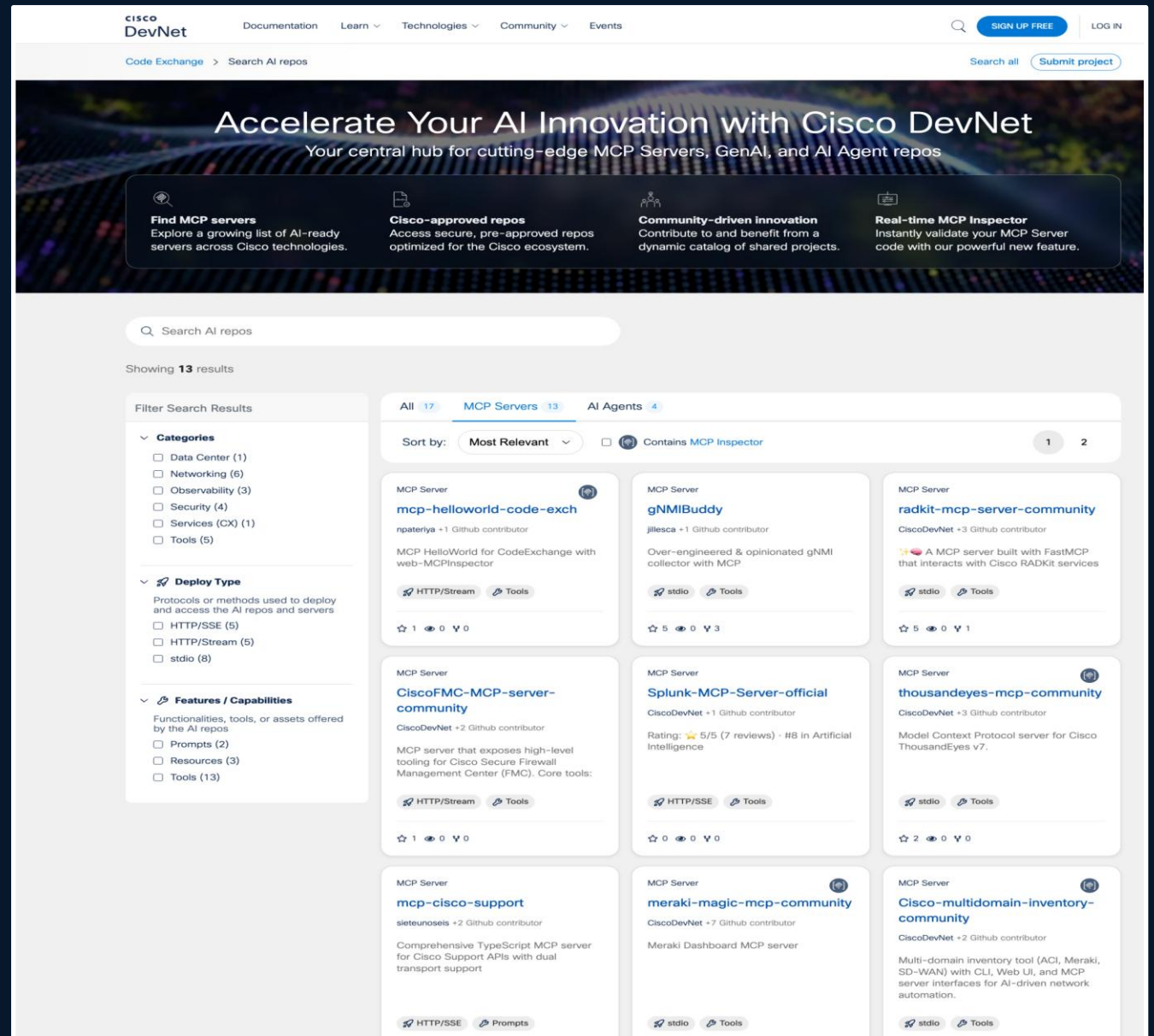
- AI Assistant, AI PCAP Analyzer, AI-RRM, AI troubleshooting, etc.
- Cisco Cloud Control and AI Canvas on the way for GA

Cisco Official MSP Servers

- Webex, Splunk, ThousandEyes, Cisco Support

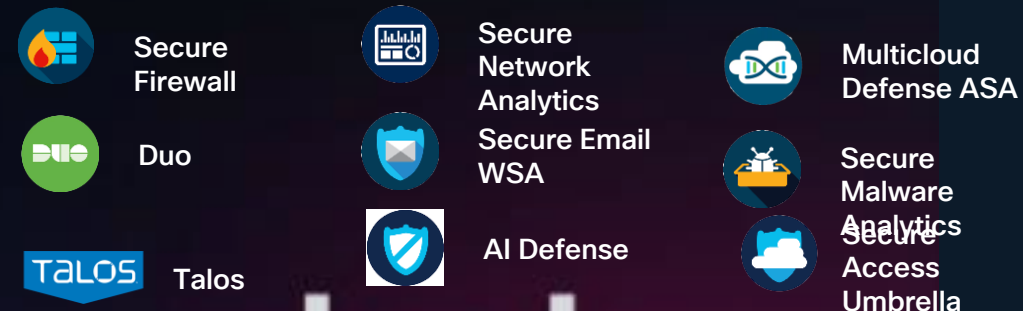
Community MSP Servers

- Meraki, Catalyst Center, FMC



Cisco x 零壹科技

Cisco | 網路與資安基礎設施



Splunk | 統一數據分析平台

Cisco 旗下數據平台



SIEM / SOAR
威脅偵測與應變



Observability
全棧可觀測性



Data Platform
AI 數據分析



零壹科技 Zerone | 台灣資深整合服務夥伴

原廠授權 / 技術支援 / 導入建置 (Solution Delivery)

Splunk 台灣資深代理商 · 企業 IT 現代化最佳夥伴



架構規劃與導入建置



7x24 維運支援 / MSSP



教育訓練與原廠認證



企業客戶

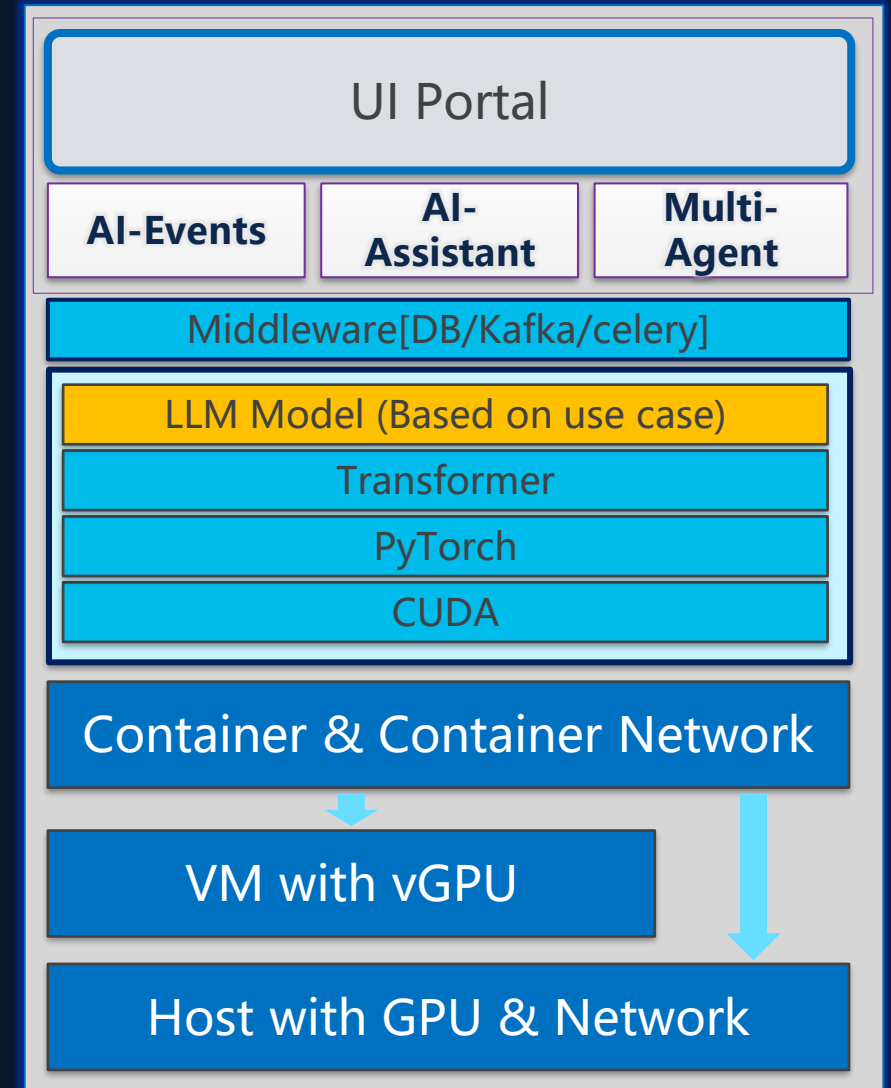
全面提升資安防護力、營運可視性與 AI 驅動決策效率

AgenticAIOps自主推理與行動力

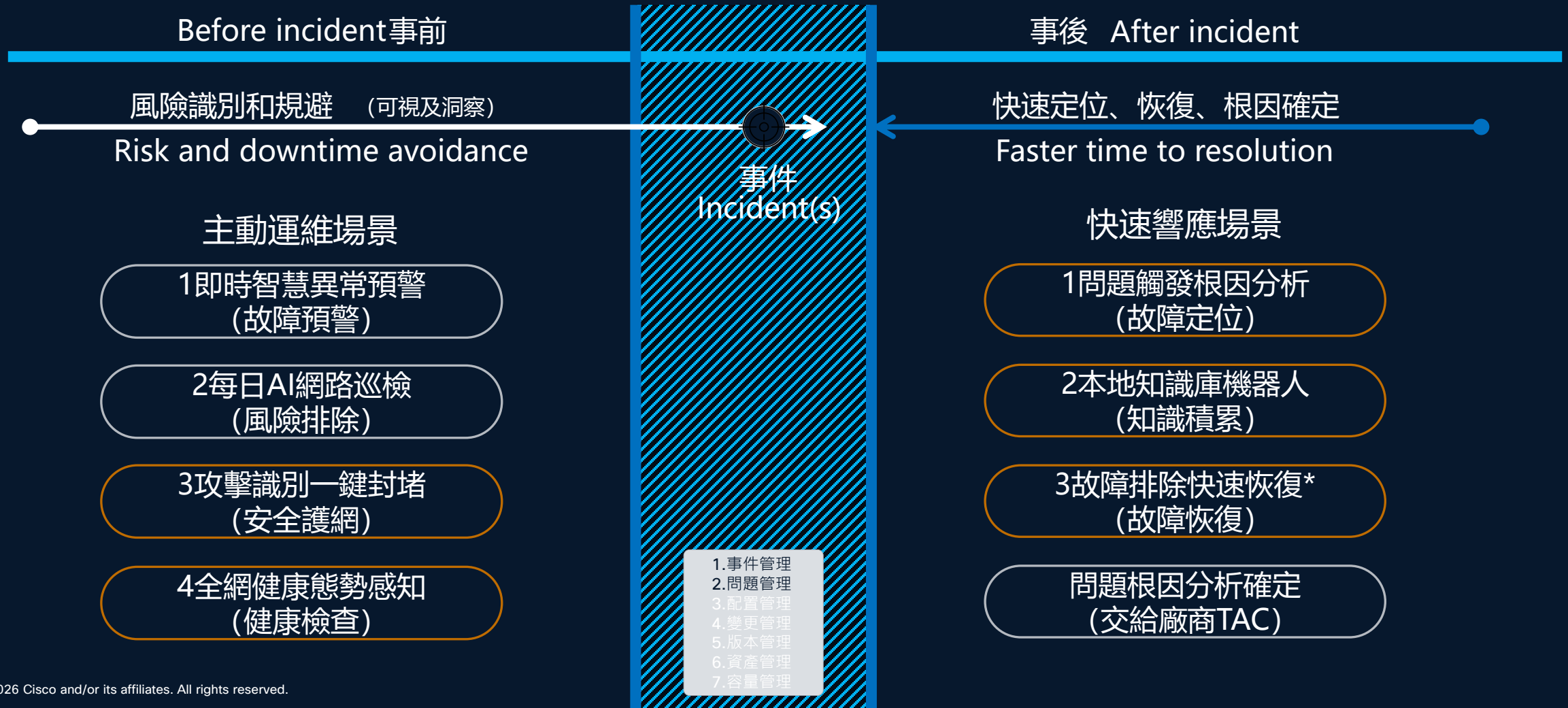
基於On-Prem開源大語言模型（LLM）+思科知識庫+客戶實際運維數據訓練所得的運維智慧體
客戶本地部署（On-Prem模式）（無需外傳數據，保護客戶數據安全及隱私）

三個元件：

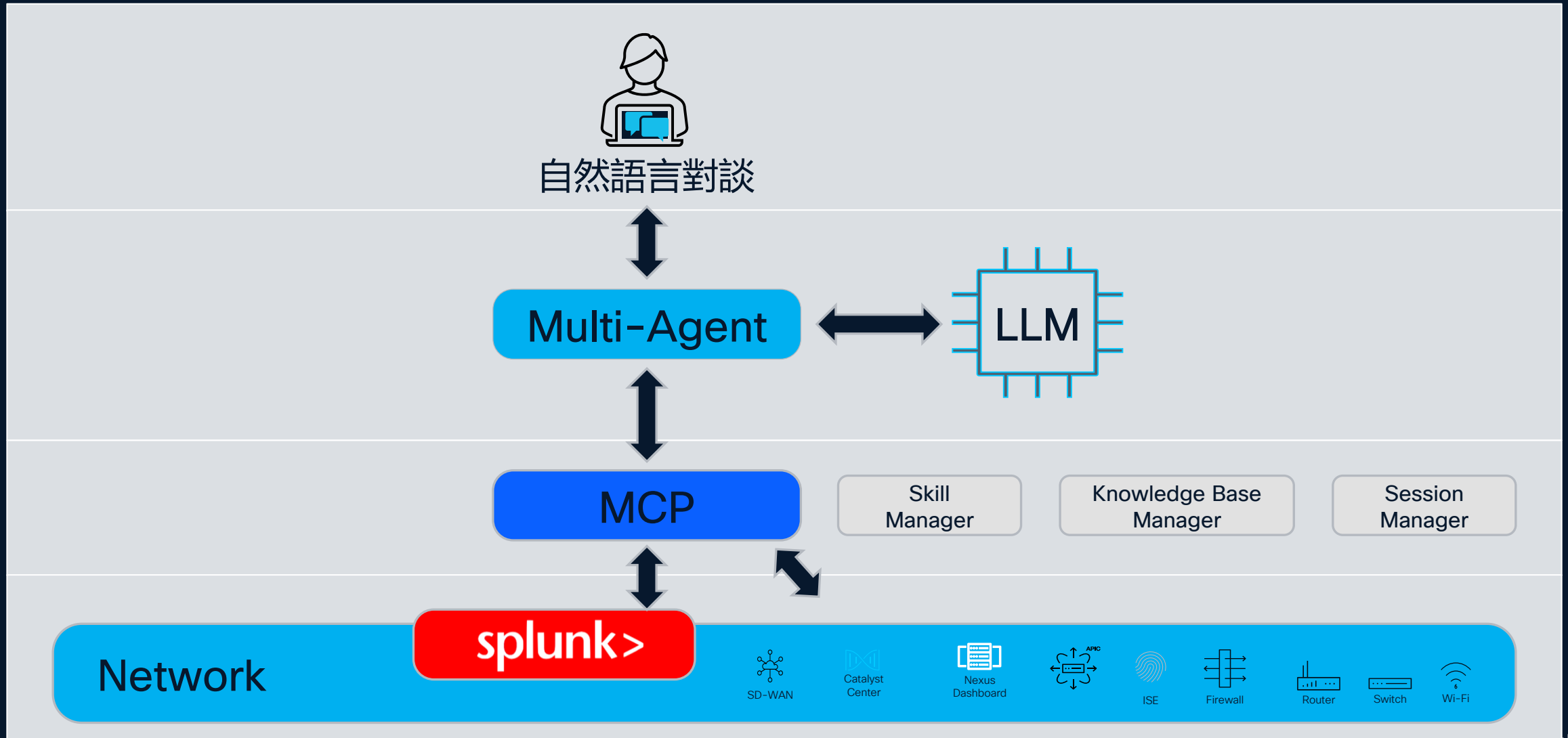
1. **AI-Events**：基於LLM的日誌及事件分析平臺（跨廠商全棧即時異常判斷和操作建議）
2. **AI-Assistant**：基於LLM的自然語言AI助手（凝練專家經驗並通過MCP實現輔助操作）
3. **Multi-Agent**：基於LLM的多AI輔助運維智慧體（多智慧體實現自動化閉環操作）



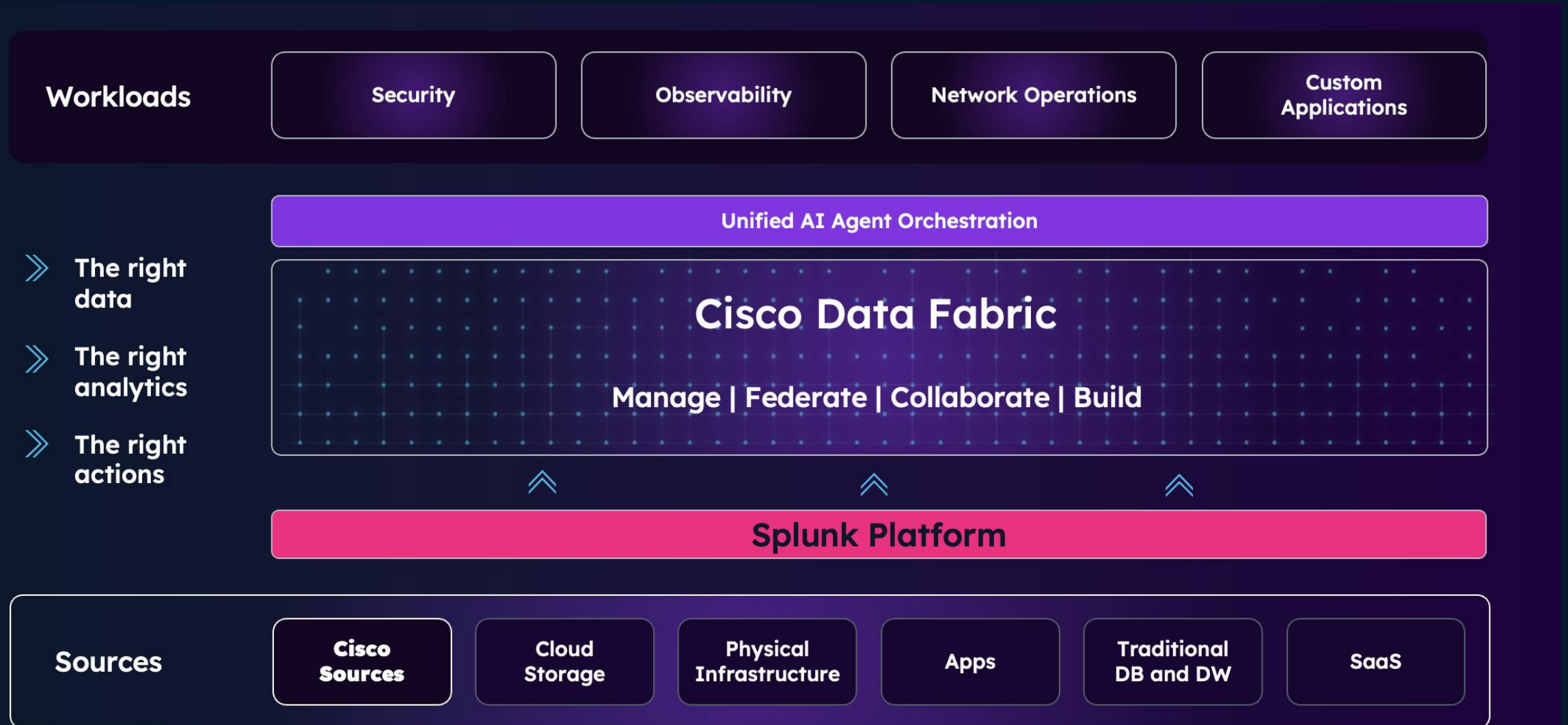
AgenticAIOps使用的場景



Multi-Agent Collaboration



Cisco Data Fabric



Three Security Pillars of Cisco Agentic AI

Pillar 1

Protect your business and avoid the risks of outsourced execution.

Identity for Agents

- Agent identity management (Duo IAM)
- Agent visibility (Identity Intelligence)
- MCP Gate access control
- Dynamic privilege management

Pillar 2

Protect your agent from external attacks.

AI Defense + DefenseClaw

- DefenseClaw governance framework
- AI Defense red team testing
- Agent Runtime SDK
- LLM Security Leaderboard

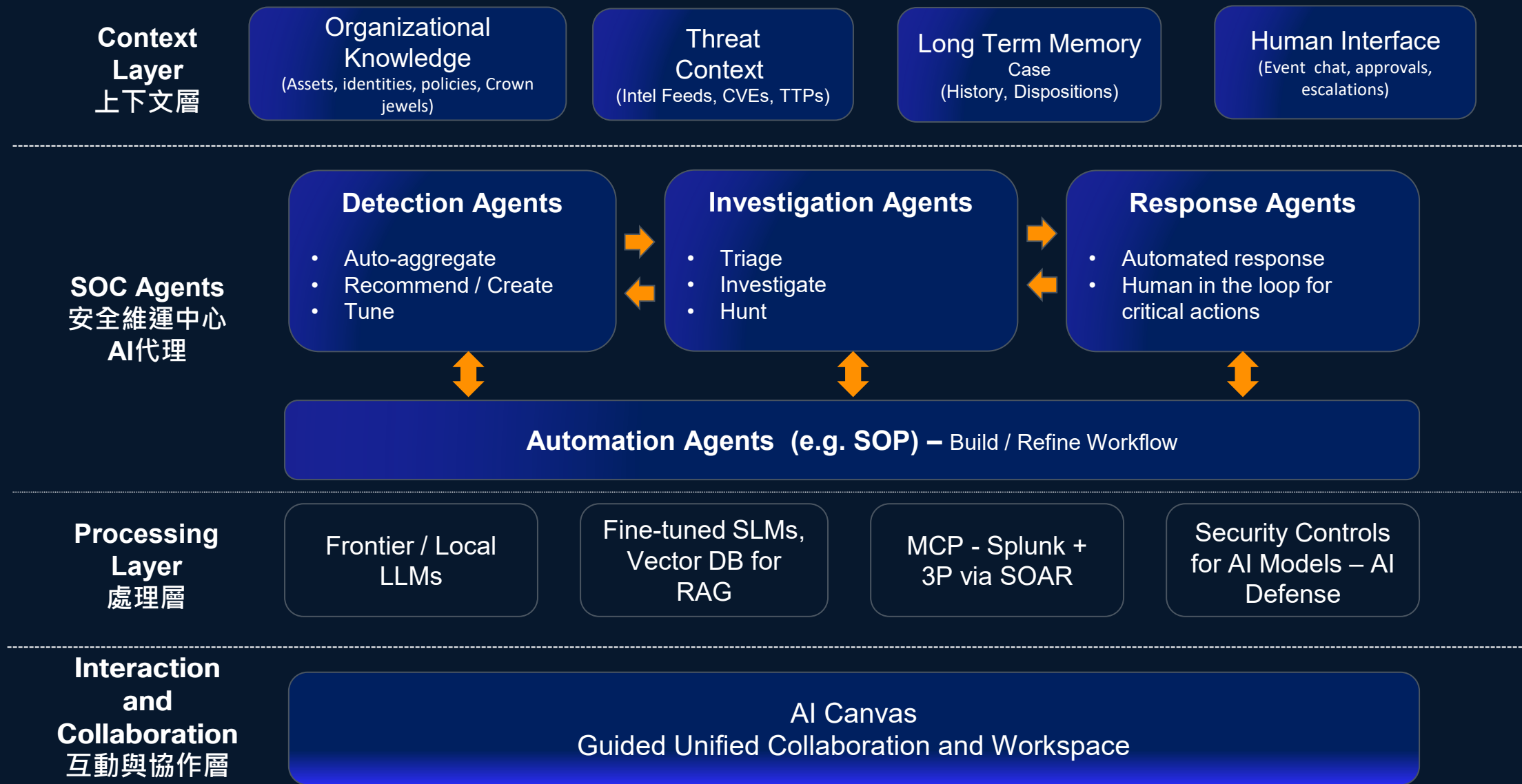
Pillar 3

Visibility and detection response for proxy applications.
代理應用的可見性與偵測反應

Agentic SOC (Splunk)

- Exposure Analytics
- Detection Studio
- Federated Search
- 6 Major Specialized SOC Agents

Agentic SOC Architecture 代理式AI安全維運中心架構



Agentic SOC Agents 安全維運中心AI代理

AI analysis

Summary MITRE TTPs IOCs and Recommendations

Malicious

Technical Analysis

Relevant code

Description

Purpose

Example matching Regex

SurfL

Disposition

True positive

ID

Type

Time

Last updated

Reference ID

Investigation type

Description

Notes

Files

Malware Reversing Agent

Extracts IOCs, flags evasion, and groups recurring behaviors.

Streamline alert prioritization with AI-driven triage.



splunk-cloud

Mission Control Security analytics Security content Configure Search

Triage Agent

Default views

Analyst queue

AI suggested disposition

AI disposition: True positive

True positive

Benign positive

False positive

Other

Undetermined

Malicious PowerShell execution

24 hour risk threshold exceeded for user-administrator

Possible Phishing Attack

Unusual network activities detected from 52.218.245.82 to 52.216.133.181

3 failed login attempts within 24 hrs on device 10.34.56.354

Threat Activity Detected from 56.143.202.14 to 8.108.191.107

Email files written outside of the Outlook directory

splunk> SOAR Example playbook

Start

Build a playbook to isolate a host with EDR

To do this, we will first need to get additional context of the suspicious host with a custom code block, and then isolate the host by the action block.

CODE Custom code

ACTION Isolate host

Add all

Guided Response Agent

Translate natural language intent into functional, tested SOAR playbooks

Multimodal AI translates the document into a response plan

splunk-cloud

Mission Control Analytics

Import JSON ipsum

Build a playbook to isolate a host with EDR

To do this, we will first need to get additional context of the suspicious host with a custom code block, and then isolate the host by the action block.

CODE Custom code

Response plans

Basic Investigation

Insider threat

Phishing Response

Self Replicating Malware

Suspicious email

Basic Investigation

SOP Agent



Cisco × Zero One | Full-Stack AIOps

核心：以 **Splunk** 作為 **Data Fabric** — 相容思科產品，打破數據孤島，滿足 AI 時代的全面需求



全思科生態系

Fully Cisco Stack

Cisco Cloud Control

採用思科產品為核心的雲端維運平台，享受原廠無縫整合、高效且即時的服務體驗。

適合：全 **Cisco** 環境、追求最速落地



客製化自由整合

Custom Integration

Splunk Data Fabric

打造企業專屬平台，透過 **Splunk** 匯流思科與非思科設備數據，構建 **Three Security Pillars** 三大安全支柱。

適合：混合廠牌環境、想自建平台



專家地端客製化

On-Prem by Cisco CX

Cisco CX 專家團隊

面對高度合規或機敏限制，**Cisco CX** 專家團隊進駐，從規劃、設計到落地，全程量身打造。

適合：資料機敏產業、資料不外流

AI 轉型的終點，不是導入工具 — 是為企業創造實質商業效益。

透過思科與代理式運維架構，守護安全、簡化 IT、提高產值、放大競爭力。

CISCO Connect

Thank you



