

Cisco Agentic Ops

AI-native IT infrastructure management

Alan Dumdei
Solutions Architect, USPS



Cisco AgenticOps

Today

AI-RRM

AI powered wireless optimization

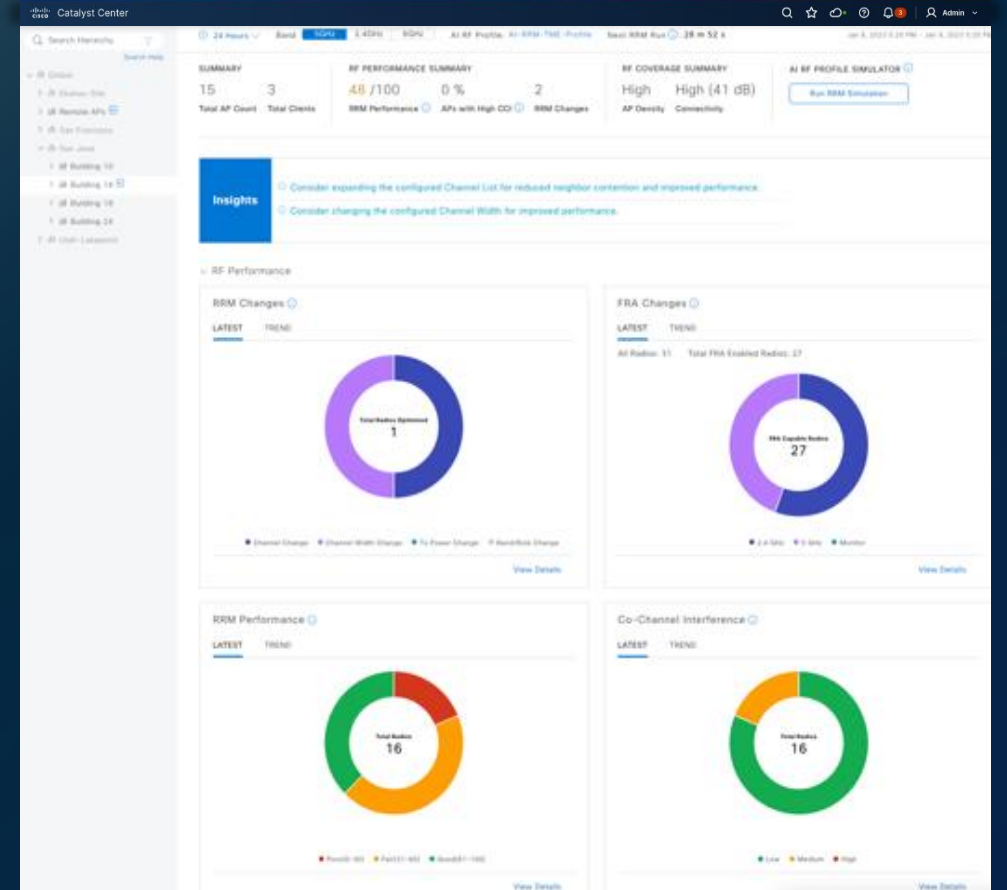
AI-RRM now in use by more than **5K customers** and **over 650K access points**.

“Two years of escalations ended **within six hours of enabling AI-RRM!**”

-Network Admin

“AI RRM’s intelligent radio tuning has reduced **more than 95% of our configuration updates** in our multiple sites.”

- Chief Network Admin



Intelligent Capture and AI Packet Analyzer

AI powered insights and troubleshooting

Accelerating issue resolution with AI

500 Million+ Proactive PCAPs Performed

Reduces manual effort to reproduce and diagnose

Embedded PCAP viewer to streamline troubleshooting

AI powered analysis delivers clear actionable insights

The screenshot displays the Meraki Intelligent Capture and AI Packet Analyzer interface. The main view is titled "network_traffic.pcap (Analysis)" and shows a "Packet Capture Analysis Summary" section. This summary includes a "Tests summary" with the following results:

- Analysors: 2/4 analyzers failed, 2/4 analyzers did not have packets present.
- DHCP: 1/2 tests failed, 1/2 tests passed.
- ARP: 1/1 tests failed.
- ICMP: No ICMP packets present.
- DNS: No DNS packets present.
- MAC address summary: These MAC addresses appeared in at least one of the failed tests: 0f:8e:d9:a2:8b:98, 45:b2:d6:22:d6:f6, df:b4:8f:ae:35:4d, 5c:w9:5e:aa:41:d0, 49:87:30:b3:39:25.

The "Packet Capture Analysis Summary" section also includes a "DHCP" section with the following results:

- DHCP transactions completed: Passed.
- Multiple DHCP servers seen: Failed (3).
- ARP requests have no responses: Failed (2).

The interface also features a "Multiple DHCP servers seen" issue card on the right side, which provides details for the issue, including the frame numbers (13, 23, 31, 46) and the IP addresses (192.168.128.1, 192.168.128.2).

AI Assistant as entry point to AgenticOps across Cisco Portfolio



Cisco Meraki

Topology, client details, location, etc.



Duo

Authentication & compliance



Secure Access

Private & SAAS Resource Access



Catalyst Center *

Topology, client details, location, etc.



SD-WAN

WAN Details



WAN, Internet, App Insights



Cisco and third-party insights



Voice and video experience

The screenshot shows the Cisco ThousandEyes Alerts interface. The main content area displays a table of active alerts:

Alert Rule	Start (GMT+5:30)	Scope	Impacted Tests
Default Network Alert Rule 2.0	Dec 2, 2025 21:50:00	2 agents	outlook.office.com:443 - Network

An AI Assistant chat window is open on the right side of the screen, showing a conversation:

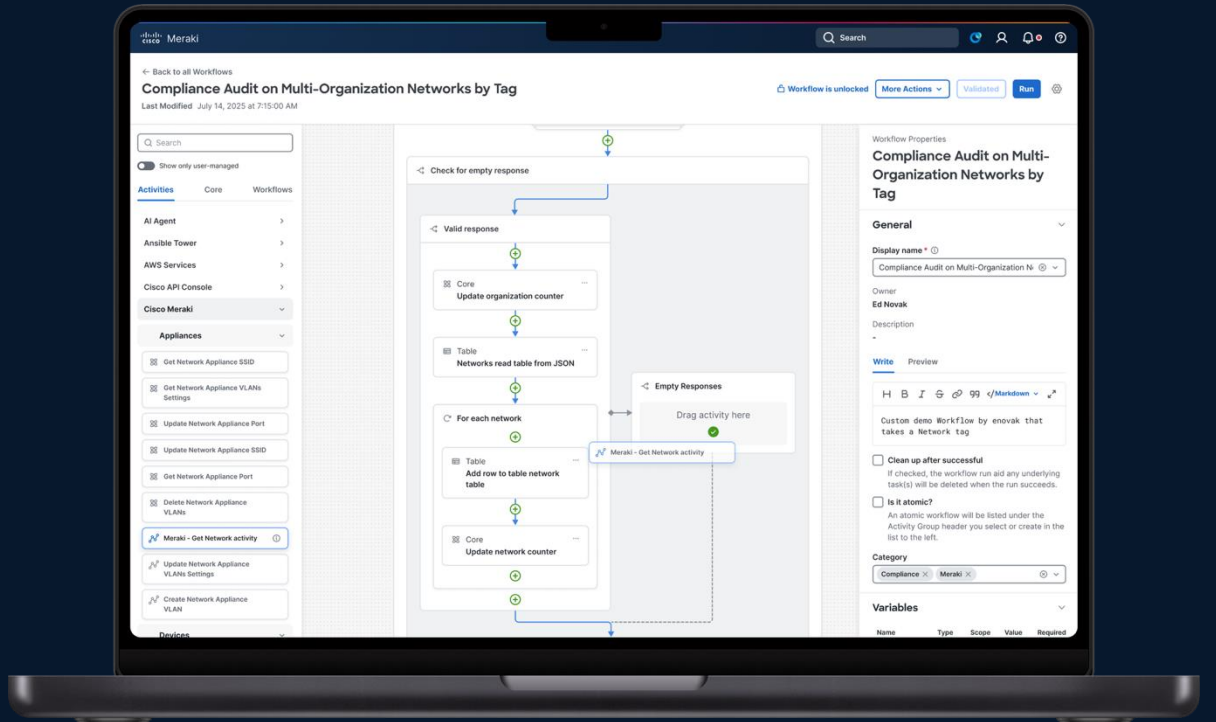
- User: show me alerts from this past week
- AI Assistant: Fetching alerts from past 7 days.
- AI Assistant: Alerts
- AI Assistant: We detected 1 alert in the last 7 days, 1 of which is minor. The latest minor alert was 'Default Network Alert Rule 2.0' applied on the target 'cea_server'. The alert started at December 02, 2025 11:20:00 and is ongoing, impacting 1 test across 2 locations: C9K-STANDALONE-1.cisco.com and C9K-STANDALONE-2.cirrus.cloud. The alert triggered because the packet loss was 100%, which is above the threshold of 10%.

(*) EFT

Agentic workflows

Leverage built-in AI Assistant integration for agentic operations using natural language

- AI powered automation natively in the Meraki dashboard
- Leverages built-in AI Assistant integration for agentic operations
- Automates workflows across Meraki, Catalyst Center, Catalyst SD-WAN Manager, ISE, Nexus, and more



Cloud-Hosted
Automation

Drag and Drop
Creation / Editing

Custom and
Pre-Built

For Cisco & Third-Party
Domains

AI Assistant Cisco
Workflows

Demo

Global Overview

Organization
BXB DMZ MikePod 1

Network
Campus Fabric

Cloud

Network-wide

Assurance

Switching

Wireless

Insight

Organization

Automation

Access Manager New

Find in Menu

Configuration overview

SSIDs Showing 15 of 15 SSIDs. [Hide disabled SSIDs.](#)

	Campus Fabric - wireless WiFi	Unconfigured SSID 1	Unconfigured SSID 2	Unconfigured SSID 4	Unconfigured SSID 5	Unconfigured SSID 6	Unconfigured SSID 7	Unconfi							
Enabled	<input type="button" value="enabled"/>	<input type="button" value="disabled"/>	<input type="button" value="disabled"/>	<input type="button" value="enabled"/>	<input type="button" value="enabled"/>	<input type="button" value="enabled"/>	<input type="button" value="enabled"/>	<input type="button" value="enabled"/>							
Name	rename	rename	rename	rename	rename	rename	rename	rename							
SSID Admins	<input type="button" value="access disabled"/>	<input type="button" value="access disabled"/>	<input type="button" value="access disabled"/>	<input type="button" value="access disabled"/>	<input type="button" value="access disabled"/>	<input type="button" value="access disabled"/>	<input type="button" value="access disabled"/>	<input #"="" type="button" value="access dis</td> </tr> <tr> <td>Access control</td> <td> edit settings	edit settings	edit settings	edit settings	edit settings	edit settings	edit settings	edit settin
Encryption	PSK (WPA2)	PSK (WPA3-SAE)	PSK (WPA3-SAE)	PSK (WPA3-SAE)	PSK (WPA3-SAE)	PSK (WPA3-SAE)	PSK (WPA3-SAE)	PSK (WPA							
Sign-on method	None	None	None	Click-through splash page	Click-through splash page	Click-through splash page	Click-through splash page	Click-thro							
Bandwidth limit	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited							
Client IP assignment	Meraki DHCP	Local LAN	Local LAN	Local LAN	Local LAN	Local LAN	Local LAN	Local LAN							
Clients blocked from using LAN	yes	no	no	no	no	no	no	no							
Wired clients are part of Wi-Fi network	no	no	no	no	no	no	no	no							
VLAN tag	n/a	100	100	104	31	31	30	30							
Tunnel	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled							
Splash page															
Splash page enabled	no	no	no	yes	yes	yes	yes	yes							
Splash theme	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a							

or [cancel](#)

(Please allow 1-2 minutes for changes to take effect.)

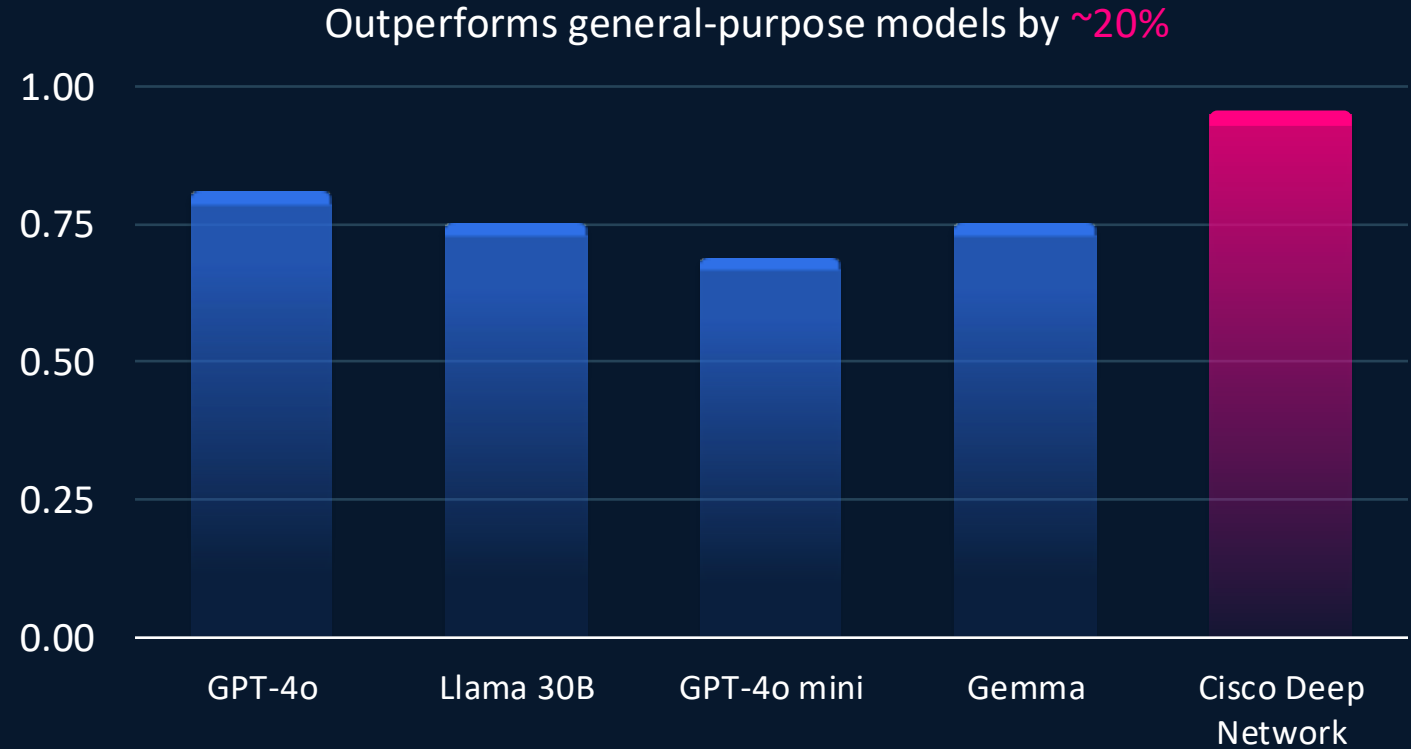
Cisco AgenticOps

Tomorrow

The Cisco Deep Network Model

Purpose-built for networking,
expert accuracy

- More precise reasoning for troubleshooting, configuration, and automation
- Fine-tuned on 40+ years of expertise and expert-vetted for accuracy
- Evolves with live telemetry and real-world Cisco TAC and CX insights



Accuracy on CCIE-style multiple choice questions (590-question benchmark), May 2025

Putting it all together



Large System prompt

- 1600 line prompt
- Focus on making Foundational Model network centric

Framework Flexibility

- Orchestration is flexible
- No Vendor lock in

Memory-Powered Intelligence

- 3 Tiers
 - Personalization
 - Contextual
 - Conversational
- Learn from every single session
- Recognize patterns across networks
- Smarter over time

User Extensibility

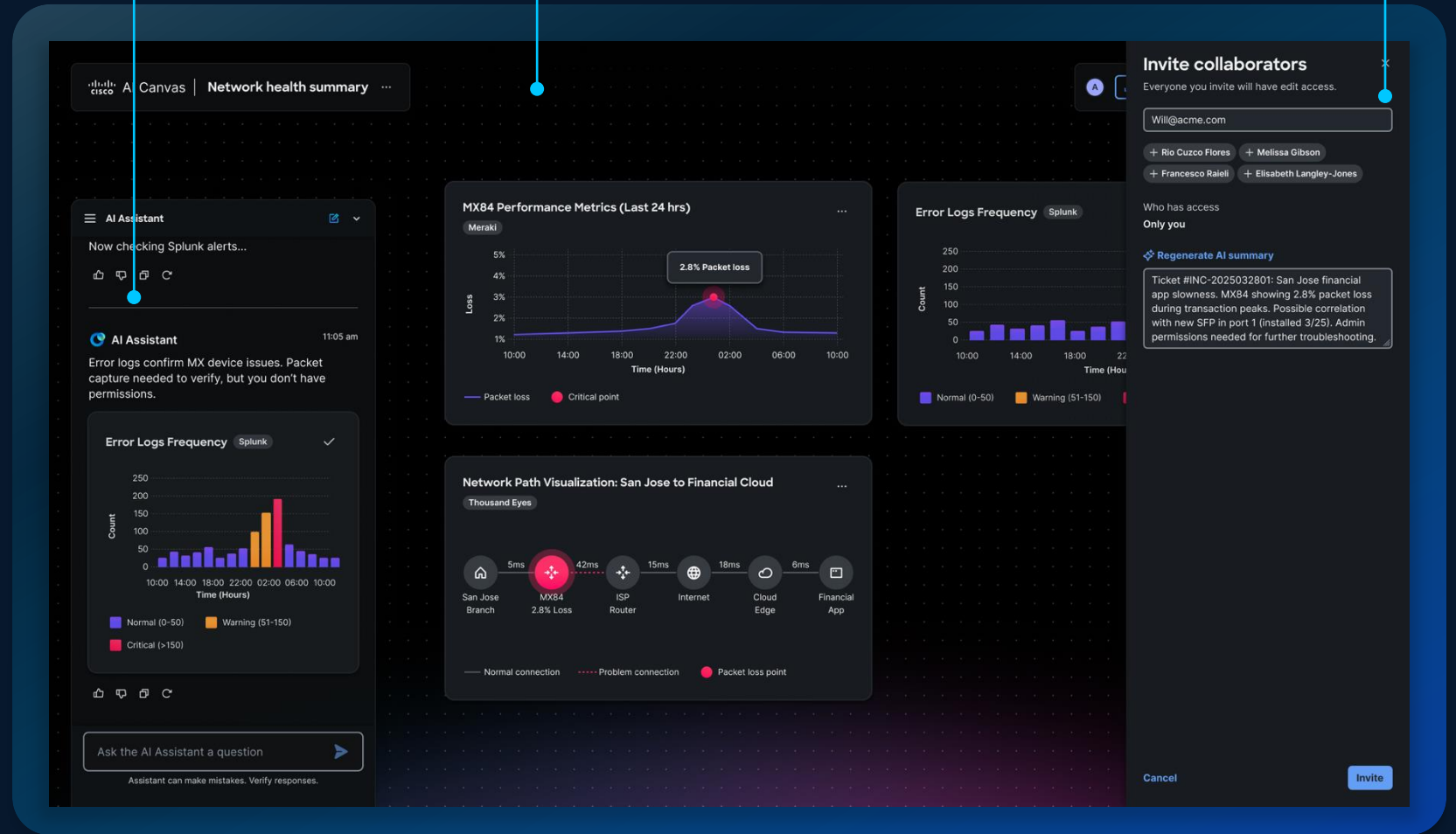
- Custom MCP servers
- Runbooks (Gen AI)

AI Assistant

Shared Workspace

Users

- Single canvas for cross domain troubleshooting
- Generative UI with reasoning built-in
- Multi-Player environment
- Keeps NetOps, SecOps, IT and execs on the same page



Cisco AI Canvas

Demo



Generate report

View activity


Share

Ask the AI Assistant a question



Assistant can make mistakes. Verify responses.





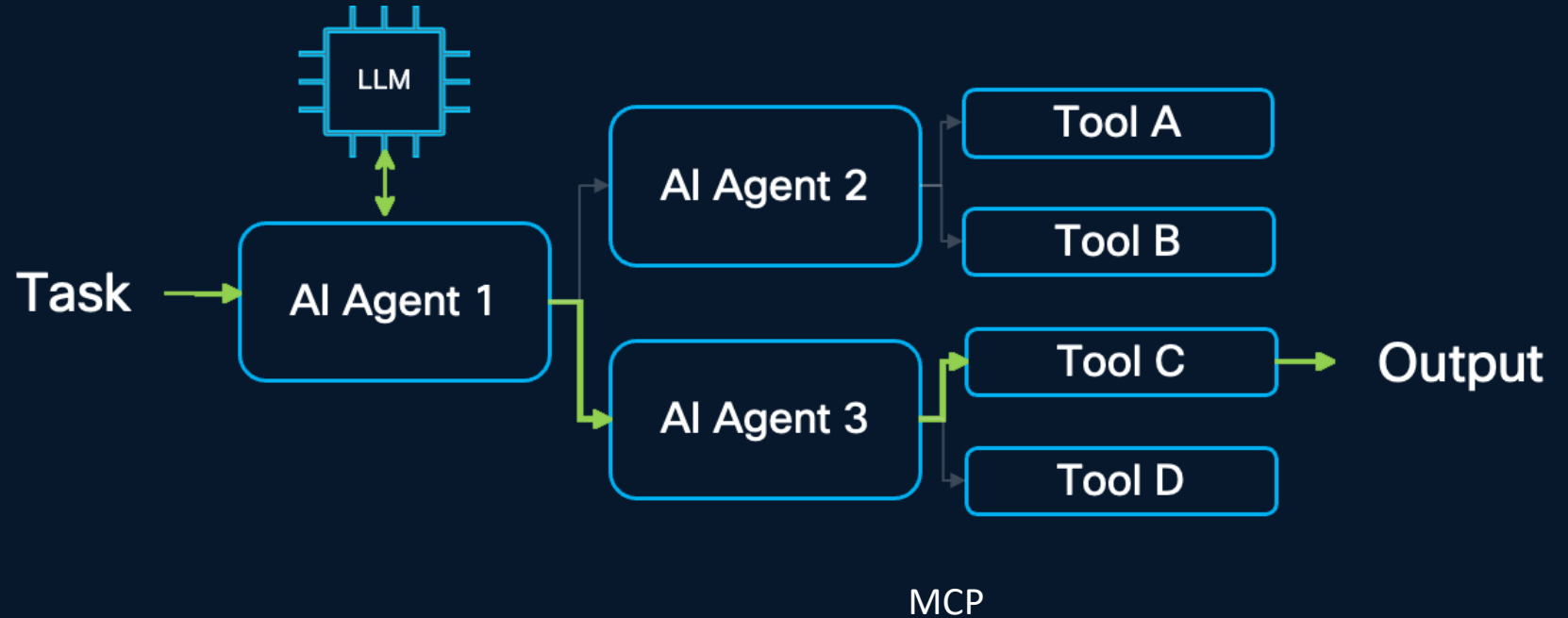
Agentic AI gives models the ability to interact with systems and take actions

Agents Empower LLMs to Solve Real-World Problems

AI Agents reason on problems and use tools to solve them

AI Agent Experience

Agents LLMs, and Tools



Capabilities

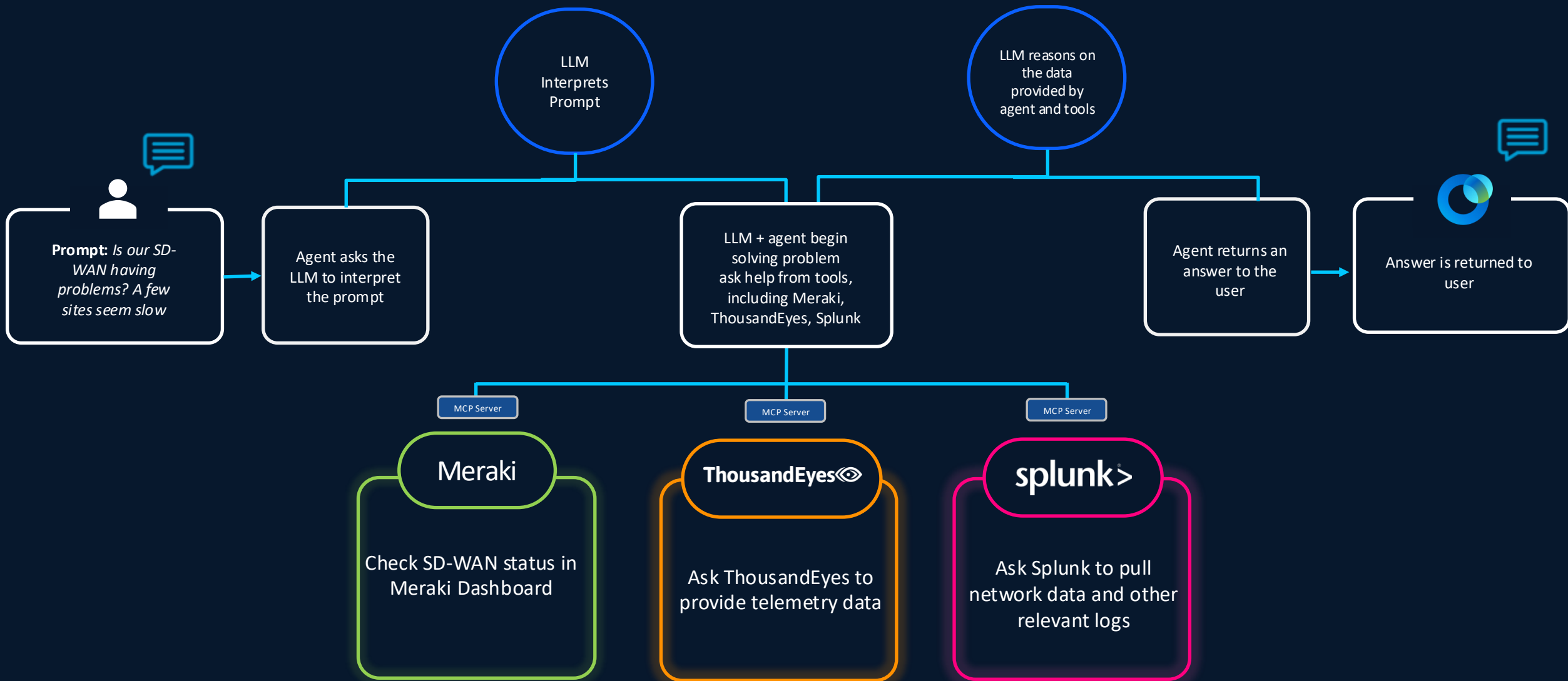
Reason & plan

Chooses
Agents & Tools

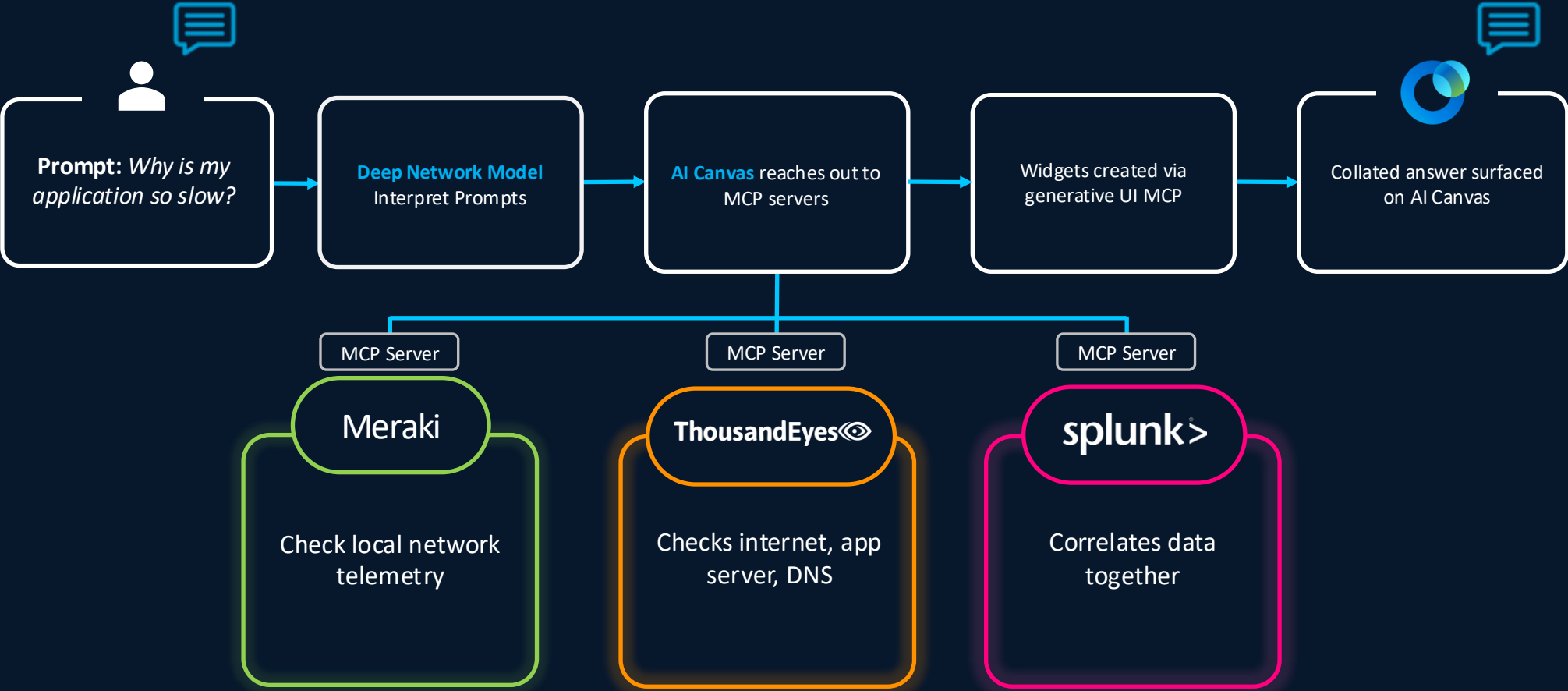
Adapt &
Recover

Execute
Autonomously

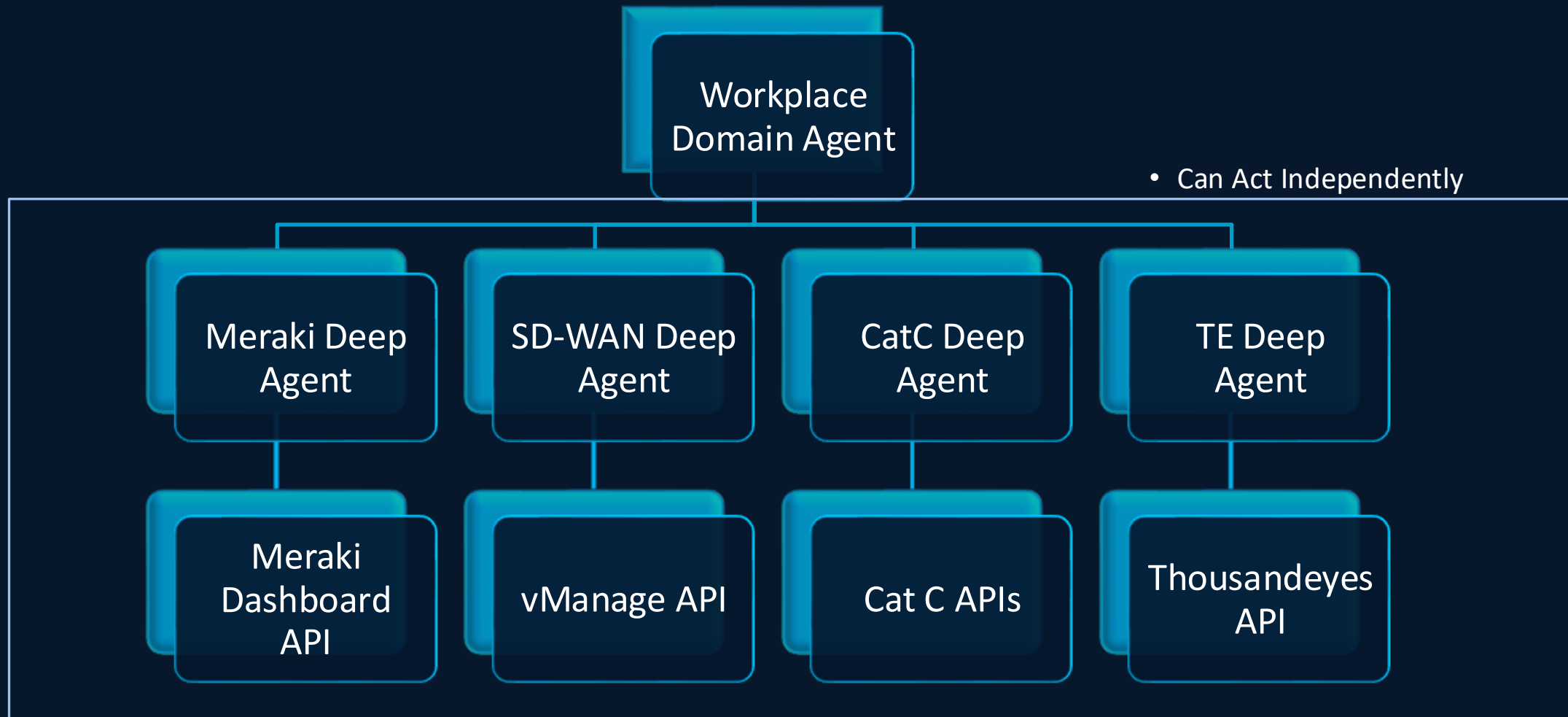
An Agentic Ops Example



Putting Together AI Canvas's Components



Cisco Deep Agent Core

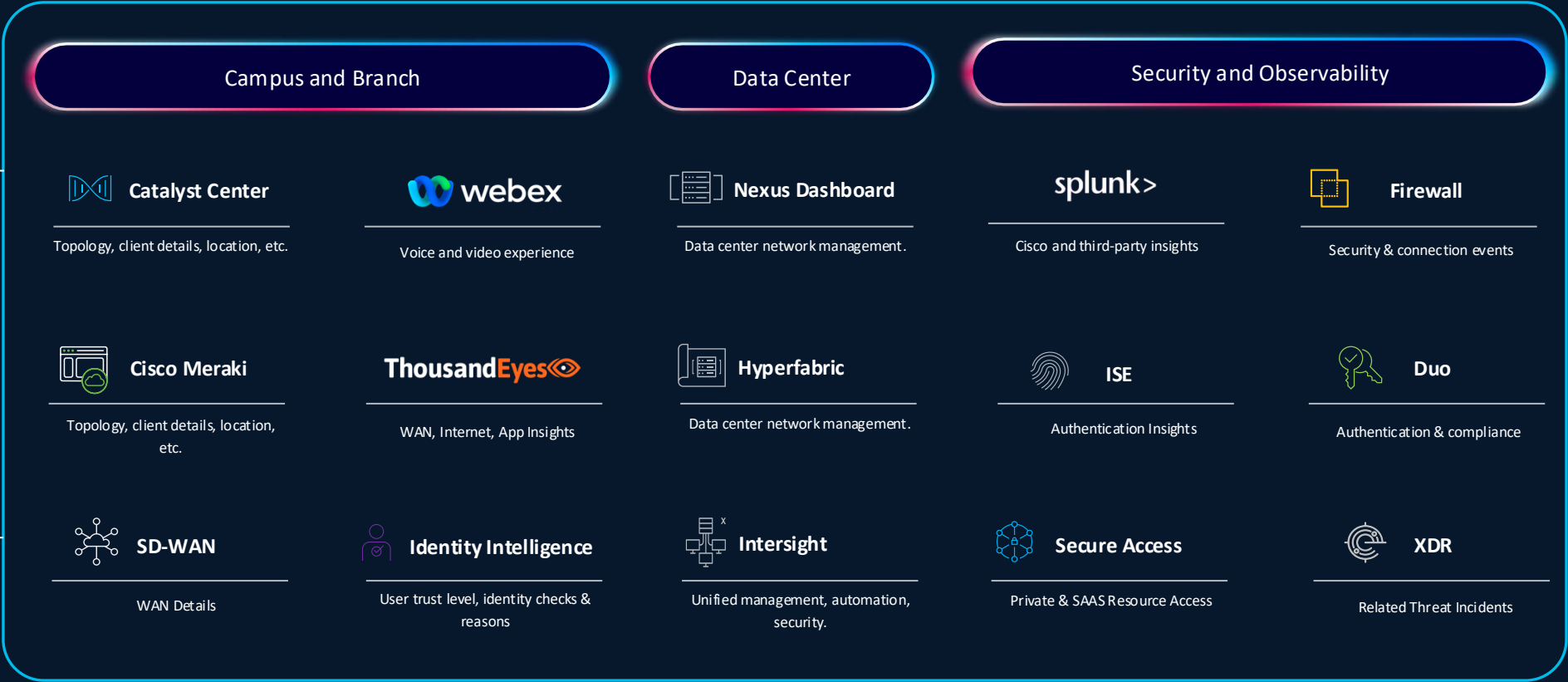
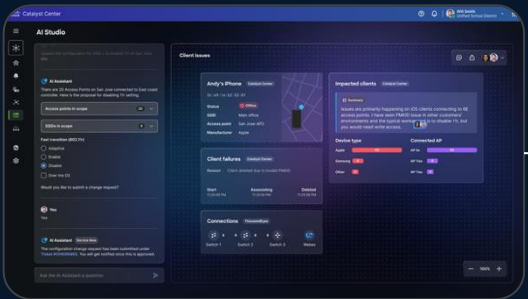


AgenticOps with cross-product skills and unified data

AI Assistant



AI Canvas



Cisco Cloud Control

An AI-native management platform that reimagines how organizations **manage, operate, and optimize** their IT infrastructure

The screenshot displays the Cisco Cloud Control dashboard with a dark theme. On the left is a navigation sidebar with sections: Home, AI Canvas (with pinned items like Application Performance Monitor, Network Fabric Management, and Micro and Perimeter Segmentation), Networking (highlighted with a red box), Security, Collaboration, and Observability. Below these are Admin Console options like Users and Role, Products and Services, Inventory, Licensing, Integration, and Support.

The main dashboard area features a central flow diagram showing 'Users' (101k) leading to 'Endpoints' (298k, with 27 failed) and then to 'Connected events' (123k, with 30k blocked). From 'Connected events', the flow splits into 'Internet' (1.2k), 'Cloud' (581), and 'Private' (109). A '92% Threats contained' gauge is also shown. Below this are several summary cards: 'Campus and branch' (Wireless: 10k, Switches: 4k, Routers: 207), 'WAN circuits' (392, 3 failed), 'Firewall' (253, 5 failed), 'Data center' (287, 5 failed), and 'Applications' (29, 4 degraded).

At the bottom, there are four panels: 'Security health score' (59/100, +15) for Alex Moreno, showing 7 vulnerabilities and a 34.2% auth success rate; 'Endpoints' (Networking) showing a bar chart with 47% for laptop (24), 35% for smartphone (18), and 18% for other; 'Packet loss' (Networking) showing a line graph increasing from 5% at 8:00 to 15% at 10:00; and 'Recent changes' (3) listing updates like 'Switch configuration updated' and 'Application patch deployed'.

The screenshot displays the Cisco Cloud Control interface for Acme Co. North America. The top navigation bar includes the Cisco logo, the company name, a search bar, and utility icons for help, notifications, AI Assistant, and user profile. A left sidebar lists navigation options: Home, AI Canvas (highlighted with a red box), Inventory, Topology, Favorites, Meraki Dashboard, ThousandEyes, Security Dashboard, Splunk Cloud Platform, Webex Control Hub, and Admin Console. The main content area features a 'All networks online' status card, two notification cards, and a 'COMPLETED' 'Access Point Deployment' card. The deployment card shows a progress bar at 32 of 32 deployed and four status indicators: 32 of 32 APs online, Assurance enabled, Network updated, and Internet accessible.

Cloud Control | Acme Co. North America

Search | AI Assistant

- Home
- AI Canvas
- Inventory
- Topology
- Favorites
- Meraki Dashboard
- ThousandEyes
- Security Dashboard
- Splunk Cloud Platform
- Webex Control Hub
- Admin Console

All networks online

Updated 32 seconds ago

New objective: October Digital Improvements
Nikitha added you as a contributor to a new network objective.
[Review](#) [Assign Tasks](#)

Report created: Wireless Performance Audit SJC-STE3
Your autonomous agent completed the wireless site audit.
[View Report](#) [Share Report](#)

COMPLETED

Access Point Deployment

Jaxon and Silvia deployed 32 new Access Points at SJC-STE1.

32 of 32 deployed

- 32 of 32 APs online
- Assurance enabled
- Network updated
- Internet accessible

[Send Kudos](#) [View Site Deployment](#)

Home

AI Canvas

Inventory

Topology

Favorites

Meraki Dashboard

ThousandEyes

Security Dashboard

Splunk Cloud Platform

Webex Control Hub

Admin Console

AI Canvas | Webex call quality issues on laptop de...

A T

Generate report

View activity

Share

AI Assistant

AI Assistant

Changes implemented. Monitoring the impact.

Revert changes

Data rate improvement

CatalystCenter



ServiceNow HDSK0045372

ServiceNow Priority 2

Reported by Mario Alegria (Alegria@company.com) on March 27, 2025 14:23 PST

Description User reports frequent audio drops and poor call quality when on Webex meetings, primarily in Building 4 of San Jose campus.

ServiceNow Ticket HDSK0045372

Authentication events Catalyst Center

Total events	Successful	Failed	Avg connection time	Avg time range
14	11	11	1.2 s	12 s

Event Type	Connection Time	Data Rate	Access Point	Status
Initial Authentication	0.9s	26 Mbps	B4-FL2-AP07	Success
Re-Authentication	—	6 Mbps	B4-FL2-AP12	Failed
Re-Authentication	0.8s	26 Mbps	B4-FL2-AP12	Success
Re-Authentication	—	9 Mbps	B4-FL2-AP12	Failed

Client health Catalyst Center

Health score



Client details

Device Laptop
 MAC address 8C:95:38:E2:7B:43
 Connection Alegria@company.com
 OS OS 15.2.1

Connection details

IP address 10.67.89.143
 Radio band 5 GHz
 Connected AP Catalyst 9166 (WIFI 6E) B4-FL2-AP12

Endpoint metrics ThousandEyes

Connection details

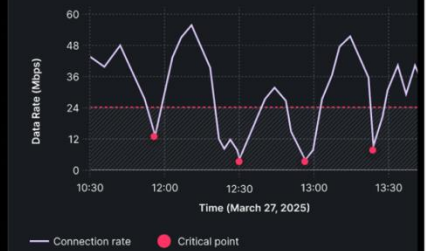
Device Laptop / OS 15.2.1
 Call route Mario's device -> meetings.webex.com

Service metrics

Packet loss **1.8%** ↑ 0.8%

Network jitter **18 ms** ↑ 8ms

Client connection rate Catalyst Center



Ask the AI Assistant a question

Assistant can make mistakes. Verifv responses.

Cisco Cloud Control: Your entire Cisco infrastructure. One login. One view.

Inventory

Last day

List view

AI insights

104 Assets



13 Critical PSIRT



17 LDOS ≤ 90d



24 Stale (> 60m)



82/22 Mngd / Unmngd



Critical PSIRT vulnerabilities detected Critical

13 Critical PSIRTs on 11 devices, highest in Tokyo Office.

Impact: Security risk - immediate patching required

11 devices 95% confidence

Filter Open in AI canvas More action

High-Risk Device Concentration Critical

3 devices (3%) have risk scores ≥80.

Impact: Concentrated risk exposure across infrastructure

3 devices 88% confidence

Filter Open in AI canvas More action

License Compliance Issues Warning

22 licenses expired (22%), 7 expiring soon.

Impact: Support coverage gaps and compliance risk

19 devices 97% confidence

Filter Open in AI canvas More action

Search

Filter 1

Filter 2

Filters 104 results

Generate report

<input type="checkbox"/>	Host name	Product family	Product	PID	S/W version	LDOS	EoVSS	PSIRT	Risk score	Site	Owner	License
<input type="checkbox"/>	wireless-058	Wireless	AIR-CAP...	OCAKLX	17.4.23	11/17/2026	4/13/2026	C:2 H:1	91	TYO Office	Wireless Team	Not reqi
<input type="checkbox"/>	ntw-061	Networking	ISR4000	T8RQG4	17.6.56	4/27/2026	11/13/2028	C:2 H:2	91	SFO HQ	NET Team	Activ
<input type="checkbox"/>	ntw-091	Networking	2960X	UB5DV0	21.8.70	7/8/2025	7/12/2025	C:2	86	SFO HQ	NET Team	Expir
<input type="checkbox"/>	iotedge-059	IoT/Edge	LoRaWAN...	V6TLWO	19.8.75	4/8/2025	5/5/2026	C:1 H:1	69	AUS DC	COL Team	Activ
<input type="checkbox"/>	iotedge-011	IoT/Edge	IR1101	PS3SAD	13.6.64	7/7/2025	2/3/2027	H:2	58	AUS DC	COL Team	Activ
<input type="checkbox"/>	dtc-003	Data center	UCS-C220	L47G30	23.0.83	4/18/2025	8/23/2025	H:3	57	LDN Office	DC Team	Expir
<input type="checkbox"/>	dtc-021	Data center	UCS-C220	7QAE6L	14.3.47	9/19/2026	5/18/2027	H:3	57	LDN Office	DC Team	Activ

Home

AI Canvas

Inventory

Topology

Favorites

Meraki Dashboard

ThousandEyes

Security Dashboard

Splunk Cloud Platform

Webex Control Hub

Admin Console

Inventory

Last day

List view AI insights

104 Assets

13 Critical PSIRT

17 LDOS ≤ 90d

24 Stale (> 60m)

82/22 Mngd / Unmngd

AI search

Filter

Saved views

Saved searches

Filters 104 results

Actions

Show devices with critical PSIRTS

Show devices with high security risks

Show devices with license compliance issues

<input type="checkbox"/>	Host name	Product family	Product	PID	S/W version	LDOS	EoVSS	PSIRT	Risk score	Site	Owner	License
<input type="checkbox"/>	wireless-058	Wireless	AIR-CAP...	OCAKLX	17.4.23	11/17/2026	4/13/2026	C:2 H:1	91	TYO Office	Wireless Team	Not req
<input type="checkbox"/>	ntw-061	Networking	ISR4000	T8RQG4	17.6.56	4/27/2026	11/13/2028	C:2 H:2	91	SFO HQ	NET Team	Activ
<input type="checkbox"/>	ntw-091	Networking	2960X	UB5DV0	21.8.70	7/8/2025	7/12/2025	C:2	86	SFO HQ	NET Team	Expir
<input type="checkbox"/>	iotedge-059	IoT/Edge	LoRaWAN...	V6TLW0	19.8.75	4/8/2025	5/5/2026	C:1 H:1	69	AUS DC	COL Team	Activ
<input type="checkbox"/>	iotedge-011	IoT/Edge	IR1101	PS3SAD	13.6.64	7/7/2025	2/3/2027	H:2	58	AUS DC	COL Team	Activ
<input type="checkbox"/>	dtc-003	Data center	UCS-C220	L47G30	23.0.83	4/18/2025	8/23/2025	H:3	57	LDN Office	DC Team	Expir

Cisco Cloud Control embedded experience

Cloud Control | Ford Motor Co. North America

Search | AI Assistant

Meraki

- Network New York HQ
- AI Canvas
- Secure Connect
- Network-wide
- Assurance
- Security & SD-WAN
- Switching
- Wireless
- Systems Manager
- Sensors
- Insight
- Organization**

Find in Menu (⌘+K)

Organization Summary

Last day | Network tags

Organization insights

All | Clients | Network devices | Connectivity | Applications

Network health breakdown

168 Total networks

- Good: 132
- Fair: 33
- Poor: 3

Top alerting networks

View all alerts

45

0

London, SFO-Corp, Chicago-Data Center, San Francisco, Tokyo

Device status

4 offline

- Uplinks: Online
- Cellular gateways: 1
- WAN appliances: 1 offline, 2
- Switches: 2 offline, 1
- Controllers: Online
- Access points: 1 offline
- Cameras: Online
- Sensors: Online

Search | Health status | 48 results

Network	Health score	Score trend	Network tags	Clients	Network devices	Connectivity	Applications
Nook-HQ-SF	80/100	-10	Branch	82/100	76/100	100/100	96/100
Network name	82/100	-20	Office	48/100	84/100	100/100	100/100
Network name	84/100	-20	Office	48/100	84/100	100/100	100/100
Network name	86/100	-9	Office	80/100	76/100	100/100	100/100 ₂₈
Network name	88/100	+5	Branch	100/100	100/100	100/100	20/100

Cisco Cloud Control embedded experience

The screenshot displays the Cisco Cloud Control interface for Ford Motor Co. in North America. The main dashboard is titled "Overview" and is last updated 2 minutes ago. A sidebar on the left contains a menu with "AI Defense" highlighted in a red box. The central dashboard features a large circular gauge showing "89k Events detected" with a +5% increase over the previous 14 days. The gauge is divided into "53k blocked" (red) and "36k monitored" (blue). Surrounding the gauge are five data cards: "Applications" (32 total, 2 disconnected), "Agents" (64 total), "Models" (128 total, including custom and foundation models), "Knowledge bases" (42 total), and "User-accessed apps" (a list of apps like Copilot Github, AI assistant, DeepAI, Enterprise AI, and SuperMemory).

AI Defense Overview

Applications → 32
2 connections disconnected [See details](#)
Protection: 4 Unprotected, 16 Protected

Agents → 64

Models → 128
Custom models (86) | Foundation models (48)
Latest validation reports [View all](#)
robert.echo.d2 —
AdaptLLM —
Meta-llama2 55% (1543/2207)
OpenAI/GPT-4o 100% (2207/2207)

Knowledge bases → 42

User-accessed apps →
Last detected apps sorted by risk and date

App Name	Date
Copilot Github	Sep 29, 2024
AI assistant	Sep 28, 2024
DeepAI	Sep 29, 2024
Enterprise AI	Sep 28, 2024
SuperMemory	Sep 29, 2024

Events detected
89k
+5% previous 14 days
53k blocked 36k monitored
[Events overview](#)

Security fused into the network

Securing users, things,
and agents



Securing network access



Securing network
connectivity



Securing the device



New threats attack networks directly



Attacks on Infrastructure

Exploits like Salt Typhoon that target unpatched software on key infrastructure



Attacks on Encryption

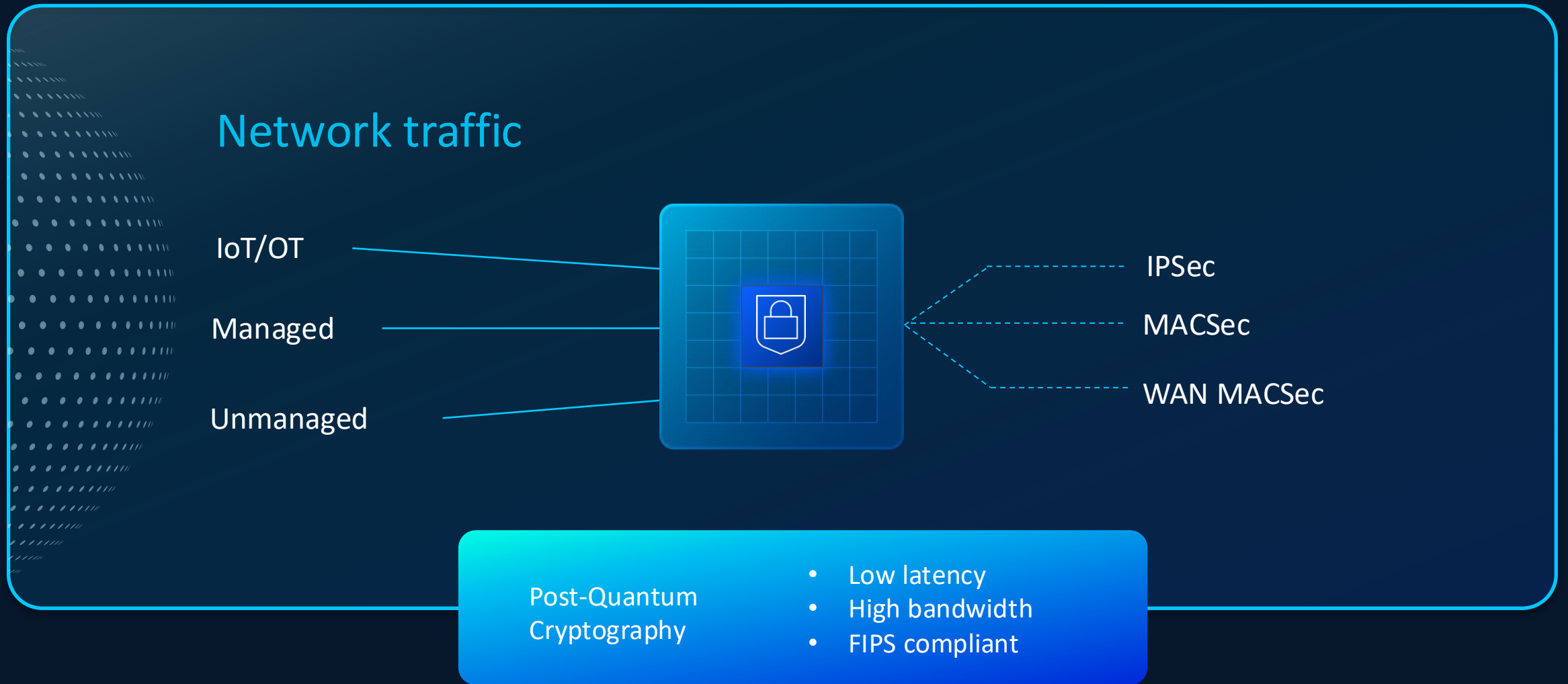
“Harvest now, decrypt later” attacks where encrypted data is extracted and stored, anticipating quantum computing.

Securing the device

Secure from hardware to software, from boot time to runtime



Securing network connectivity



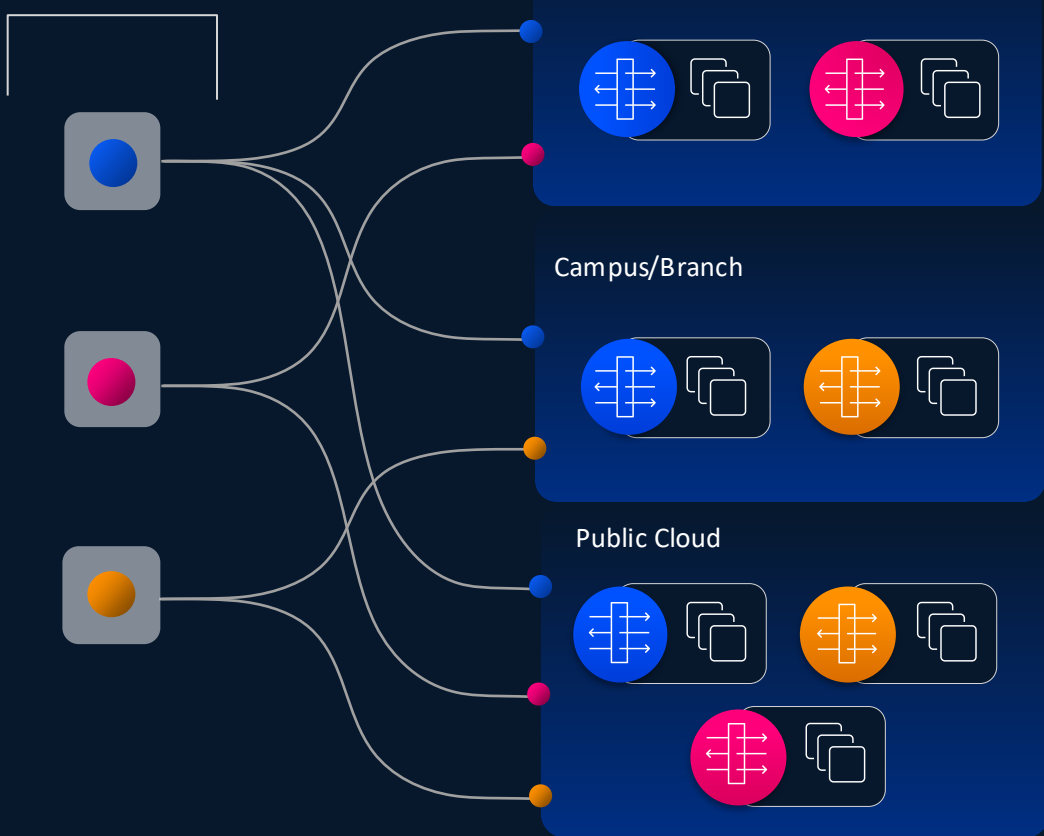
Today, Firewall Policy Management is Fragmented

Traditional Policy Management

- Policy configuration is device-by-device
- Translating one intent to multiple policies across vendors takes time and is error-prone
- Adding firewall devices over time makes the problem exponentially worse

Solving these challenges requires a different approach

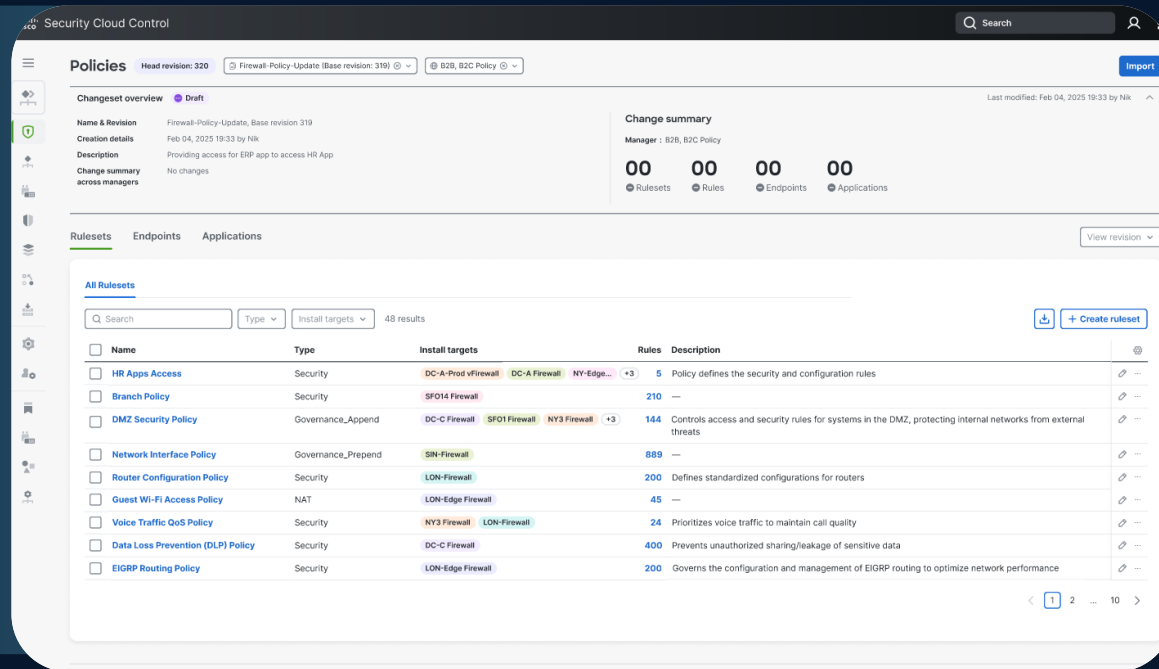
Multiple vendor user interfaces



Introducing Mesh Policy Engine

Cisco is the Only Enterprise Firewall Vendor that Extends Policy to non-Cisco Enterprise Firewalls

- A policy manager (not a device manager or policy converter)
- Retain the “what” and “where” of the policy and the “why”
- Change enforcement points, not policy
- Cisco plus the other enterprise firewall vendors



Cisco Security Cloud Control

Data Center



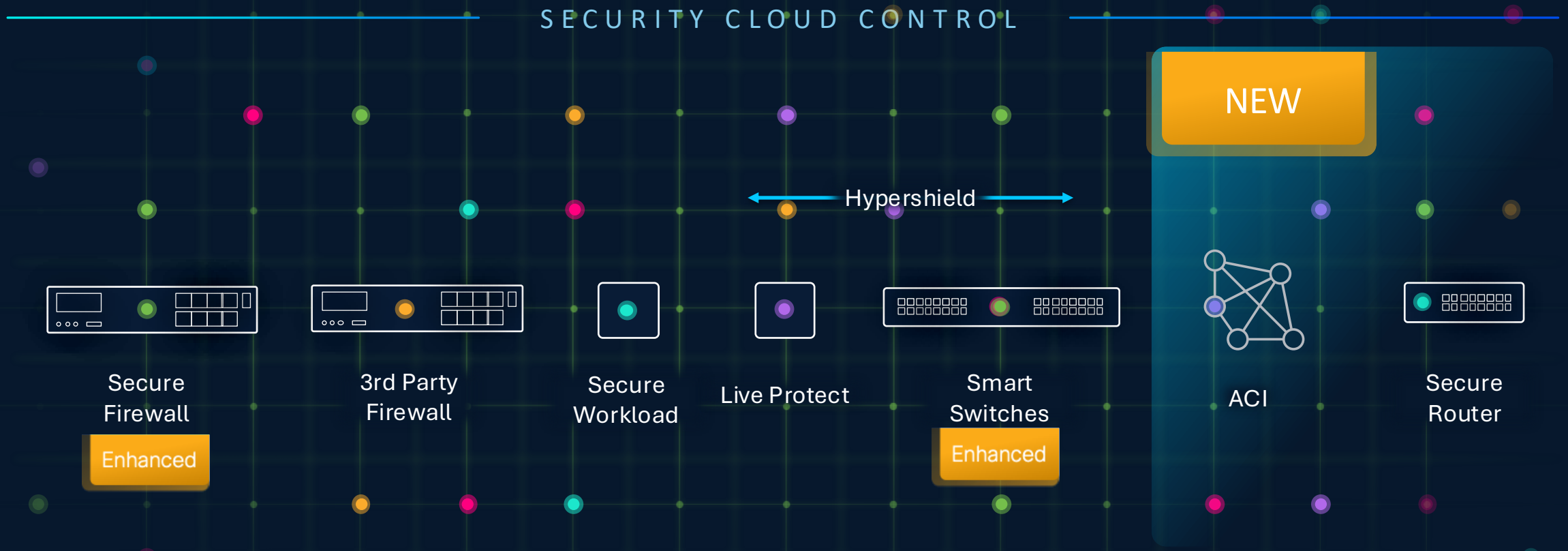
Campus/Branch



Public Cloud



Cisco Hybrid Mesh Firewall



Write Policy Once, Enforce Across the Mesh

Cisco Universal ZTNA



Seamless experiences
AI-powered Identity and Device Intelligence



Effective, distributed
enforcement



Traditional apps



Private apps



Internet apps



SaaS apps

