

CISCO Live !

Cisco Live AMER 26

Jiri Rott

June 2026

Venues

Mandalay Bay

- Registration and Cisco Store
- Breakouts and Tech Seminars
- World of Solutions
- Keynotes
- Keynote Deep Dives
- Certification Testing Center
- Meeting Village
- Learn with Cisco
- Walk-in Labs / TAC / DevNet
- IT Leadership Program
- Press and Analyst Conference

Four Seasons *Executive Symposium*

MGM Grand *Auxiliary Events*

Luxor Hotel *Instructor-Led Labs*

Allegiant Stadium *Celebration*



Week-at-a-Glance

Sun, May 31		Mon, June 1	Tues, June 2	Wed, June 3	Thurs, June 4
Morning	Technical Seminars & Instructor-Led Labs	Content	Cisco Keynote Content	Cisco Keynote Content	Content
		World of Solutions 10 am-6 pm	World of Solutions 10 am-6 pm	World of Solutions 10 am-6 pm	World of Solutions 10 am-2 pm Brunch 10 am- 1 pm
Afternoon	Technical Seminars & Instructor-Led Labs	1:1 Meeting Village			
		Content	Content	Content	Content
		Executive and Add-On Programs			
			Press and Analyst		
Evening		Reception 4 pm- 6 pm		Celebration	

cisco Live ! Celebration

MARCOON 5
THE CHAINSMOKERS

Wednesday, June 3
7:30 – 11 p.m.

© 2026 Cisco and/or its affiliates. All rights reserved.



Keynotes

• Tuesday, June 2 | 8:30 – 10:15 AM PST | Lead in the agentic era

Cisco Vision and Strategy



Chuck Robbins
Chair and Chief Executive Officer

Conversation with Brian Niccol, Starbucks Coffee Company



Brian Niccol
Chair and CEO, Starbucks

Product Strategy
Tier 1 Launches and Demos



Jeetu Patel
President and Chief Product Officer

Conversation with DJ Sampath + Hasmukh Ranjan
Cisco Cloud Control



DJ Sampath
SVP and General Manager, AI Software and Platform



Hasmukh Ranjan
SVP and Chief Information Officer, AMD

Close



Jeetu Patel
President and Chief Product Officer

• Wednesday, June 3 | 8:30 – 10:00 AM PST | From agentic vision to enterprise reality

Welcome



Liz Centoni
EVP and Chief Customer Officer

CX



Liz Centoni
EVP and Chief Customer Officer



Scott Malone
VP of IT, GEODIS



John Hoenemier
Director of Data Network Security, GlobalFoundries

Product Deep Dive and Demos



Jeetu Patel
President and Chief Product Officer



Tom Gillis
SVP and General Manager, Infrastructure and Security



Anurag Dhingra
SVP and General Manager, Enterprise Connectivity and Collaboration



Kamal Hathi
SVP and General Manager, Splunk



Demo Presenters

Close



Jeetu Patel
President and Chief Product Officer

Key launch highlights



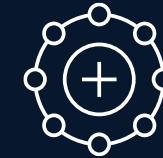
Simplified operations powered by AgenticOps

New autonomous operations
capabilities and
new Multicloud Fabric



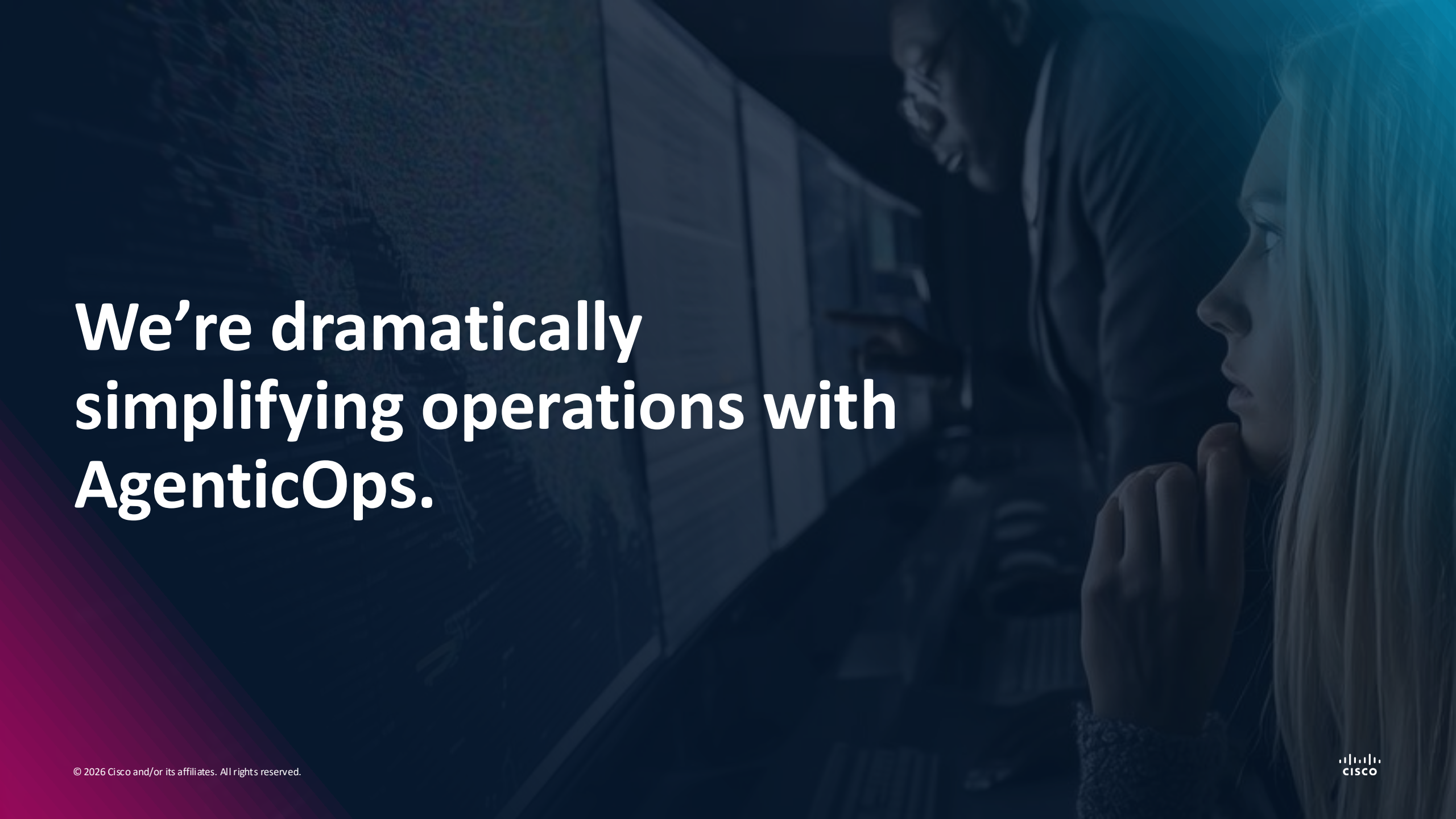
Security fused into the network

Live Protect
on campus and branch
Smart Switches



Scalable AI-ready devices

Expansion of next generation
line up



**We're dramatically
simplifying operations with
AgenticOps.**

Cisco Cloud Control

The power of one

One login

Sign in once. See everything.

One inventory and topology

Every asset. See how it all connects, in real time.

One view for alerts

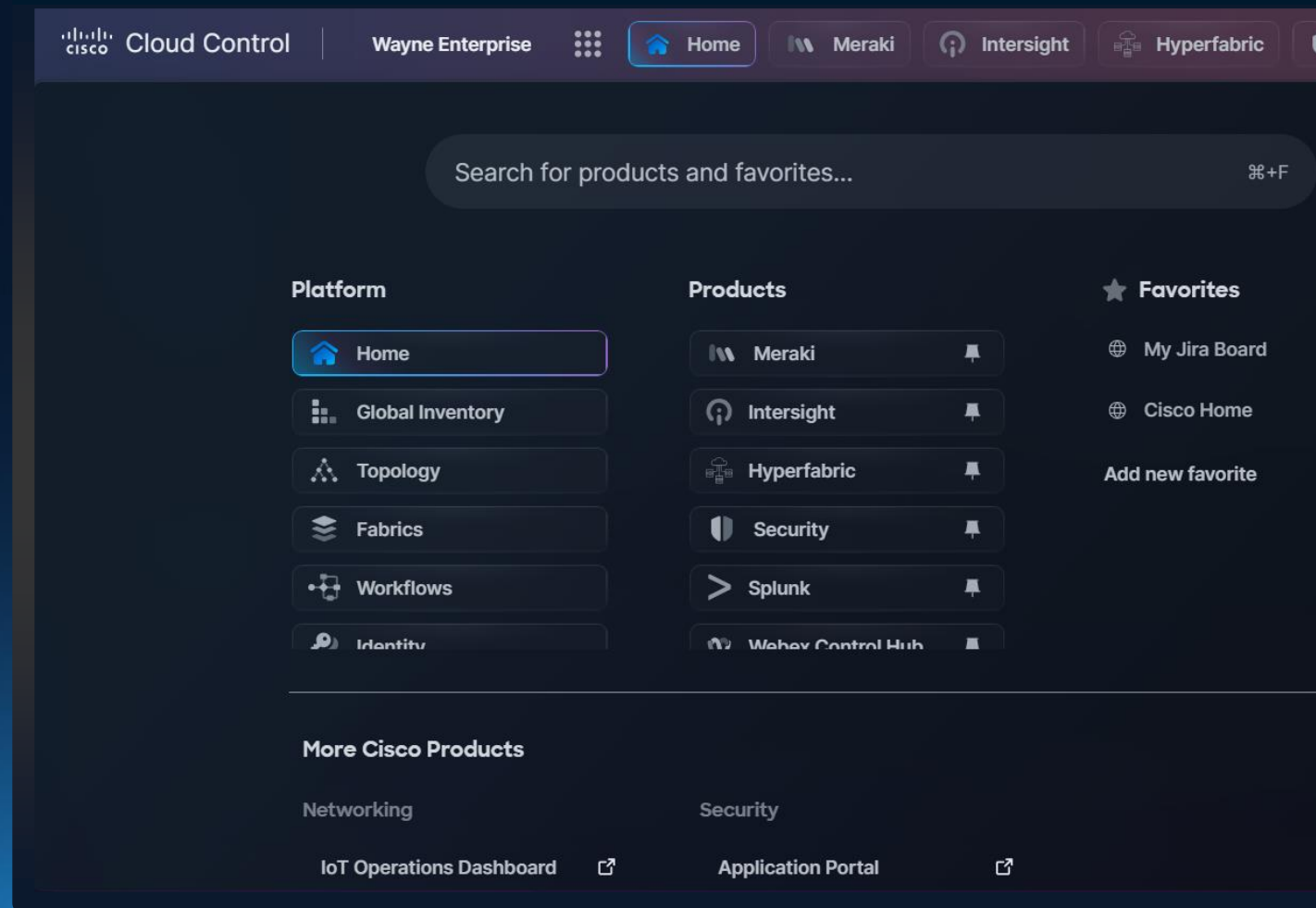
Actions correlates alerts across every product.

One assistant

Quick answers and tasks with AI Assistant.

One agentic workspace

Investigate, execute and resolve with AI Canvas.



The platform

Cisco's unified operational platform

Cisco Cloud Control

Integrated products

Meraki

Catalyst Center

Intersight

Nexus Dashboard

Nexus Hyperfabric

Secure Access

ThousandEyes

Splunk

Collaboration Control
Hub

IQ

AI workspace

AI Canvas

Collaborative agentic workspace

AI Assistant

Conversational entry point

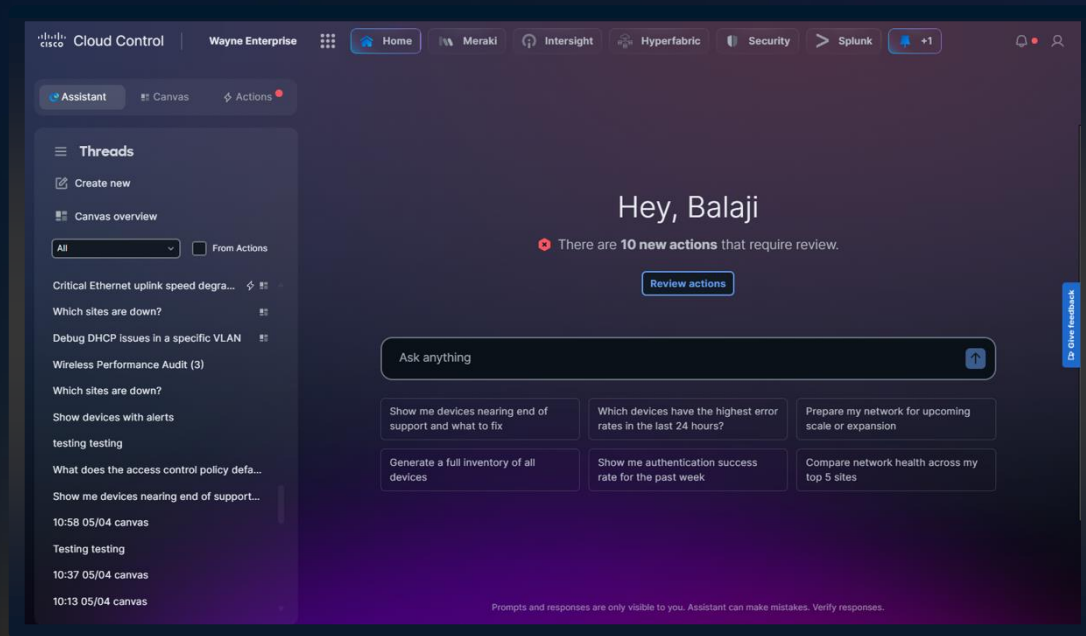
Platform services

- Cisco Identity
- Unified Inventory
- Cisco Topology
- Cisco Alerts
- Cisco Licensing

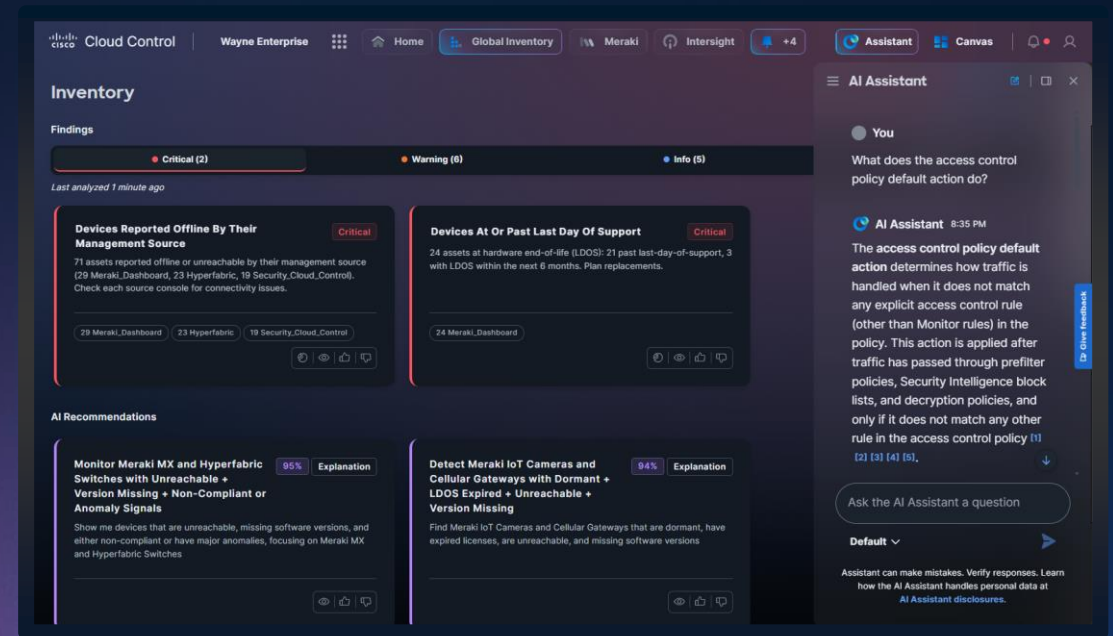
AI Assistant

Ask about your infrastructure, anywhere

Homepage view

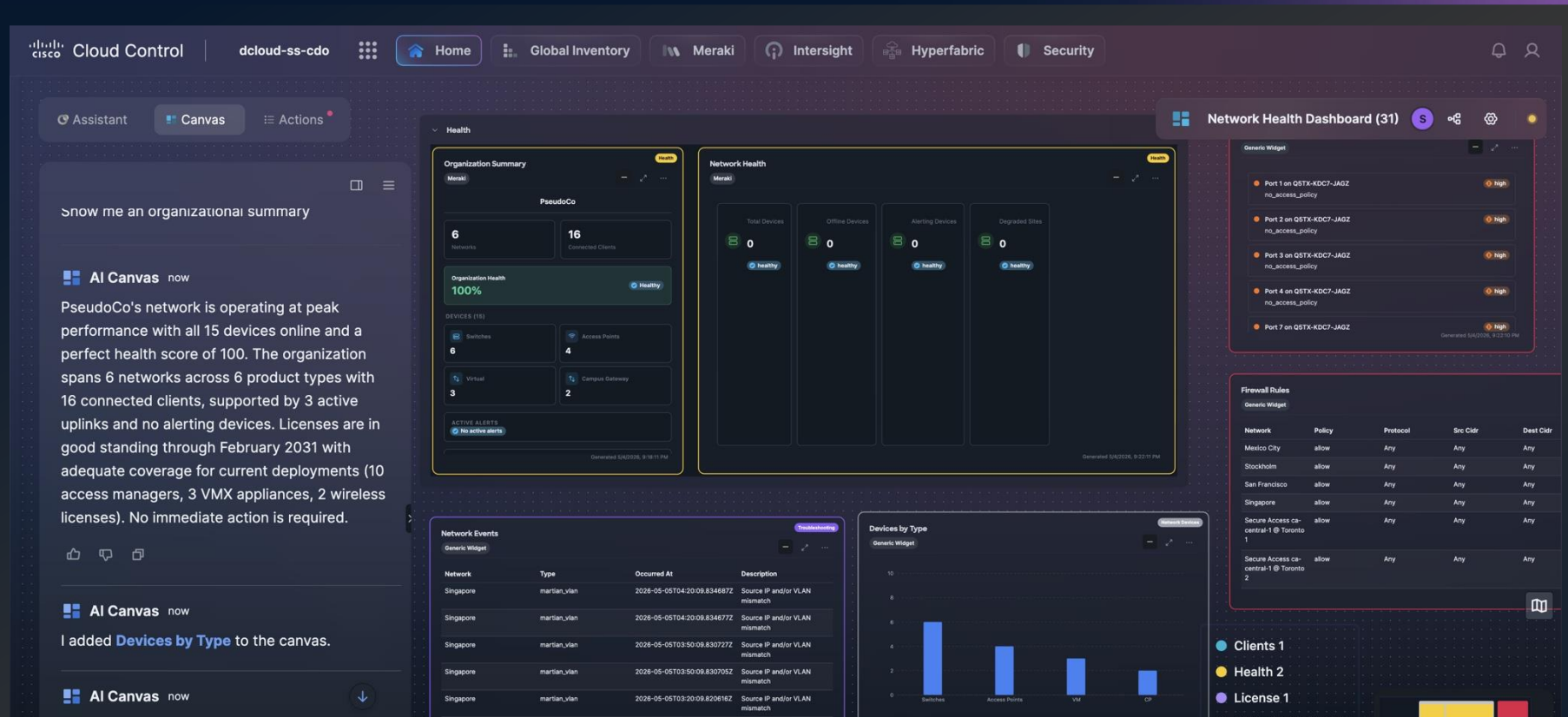


Sidebar view



Cisco AI Canvas

The industry's first multiplayer workspace for cross-domain agentic operations



Two surfaces. One intelligence.

Feature	Cisco AI Assistant	Cisco AI Canvas
What's it for	Quick answers and tasks	Investigate and explore
How you use it	Conversational chat	Visual workspace
Collaboration	Single player, private	Multiplayer, shareable
Typical session	Seconds to minutes	Minutes to hours
Output	Text answers: summaries, recommendations, answers	Interactive widgets: Visualized data, topologies, timelines, reports
Where it shines	Speed. Move through your day faster.	Context. Explore the “why” behind the data

AgenticOps

Powered by Cisco Cloud Control

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



Cross-domain
telemetry

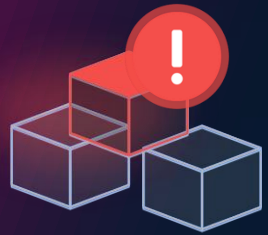


Purpose-built
models

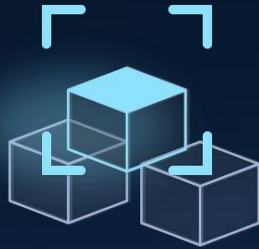


Trusted
agents

The Agentic Loop



Sense



Diagnose



Remediate



Validate



Deploy

BETA JUNE 2026

Introducing Agentic Actions for networking

Root cause analysis and closed-loop remediation with trust and transparency

The screenshot displays the Cisco Meraki Cloud Control interface. The top navigation bar includes 'Cisco Meraki', 'Home', 'Meraki', and 'Security'. A search bar and links for 'AI Canvas' and 'AI Assistant' are also present. The left sidebar shows a menu with 'Cisco Meraki', 'Network-wide', 'Assurance', 'Security & SD-WAN', 'Switching', 'Wireless', 'Systems Manager', 'Cameras', 'Sensors', and 'Insight'. The main content area is titled 'Networking actions' and includes a 'Monitor' button. Below this, there are tabs for 'Incidents' (3), 'Alerts' (98), and 'Optimizations' (12). The 'Incidents' tab is active, showing a list of incidents. The first incident is 'Rogue RADIUS server', which is 5m ago and has 286 clients, 2,002 devices, and is associated with SFO12. The second incident is 'Wireless capacity degraded due to sticky clients', 20m ago, with 50 clients and 50 devices, associated with SJC16. The third incident is 'Unreachable network devices due to unreachable switch', 1h ago, with 50 clients and 50 devices, also associated with SJC16. The 'Rogue RADIUS server' incident is expanded, showing a 'BRIEFING' section with 'AI Monitoring' and 'High confidence'. The briefing text states: '428 clients failed to authenticate due to invalid certificates'. The 'Issue' section notes: '20% of connection attempts made by 428 prospective clients in Cisco Meraki organization failed.' The 'Root cause' section states: 'Rogue server 173.36.46.146 is contributing to 96% of authentication failures.' Below the briefing, a 'RECOMMENDED ACTION' section is shown, indicating a duration of 2-3 minutes and potential network disruptions. The actions are: 1. 'Quarantine rogue server' (Medium risk), which includes a table with 'Target location' (RADIUS server 173.36.46.146) and 'MAC Address' (0a:35:23:38:aw:38). 2. 'Re-authenticate clients', which includes a table with 'Target endpoints' (428 clients connected to rogue server). Both actions have a 'View reasoning' link. At the bottom, there is a 'REASONING LOG' section.

Cloud Control | Cisco Meraki | Home | Meraki | Security

Search Meraki | AI Canvas | AI Assistant

Networking actions | Updated 1m ago | Monitor

Incidents 3 | Alerts 98 | Optimizations 12

Rogue RADIUS server 5m ago

286 clients | 2,002 devices | SFO12

Wireless capacity degraded due to sticky clients 20m ago

50 clients | 50 devices | SJC16

Unreachable network devices due to unreachable switch 1h ago

50 clients | 50 devices | SJC16

Rogue RADIUS server Active

173.36.46.146 | 4 networks | June 1, 2026 at 9:23am EDT | Assurance | ID: 280382...

BRIEFING AI Monitoring | High confidence

428 clients failed to authenticate due to invalid certificates

Issue

- 20% of connection attempts made by 428 prospective clients in Cisco Meraki organization failed.

Root cause

- Rogue server 173.36.46.146 is contributing to 96% of authentication failures.

RECOMMENDED ACTION 2-3 minutes | Potential network disruptions | Apply all changes

Quarantine rogue server Medium risk

- Quarantine rogue server

Target location	MAC Address	View reasoning
RADIUS server 173.36.46.146	0a:35:23:38:aw:38	View reasoning

- Re-authenticate clients

Target endpoints	View reasoning
428 clients connected to rogue server	View reasoning

REASONING LOG

BETA JUNE 2026

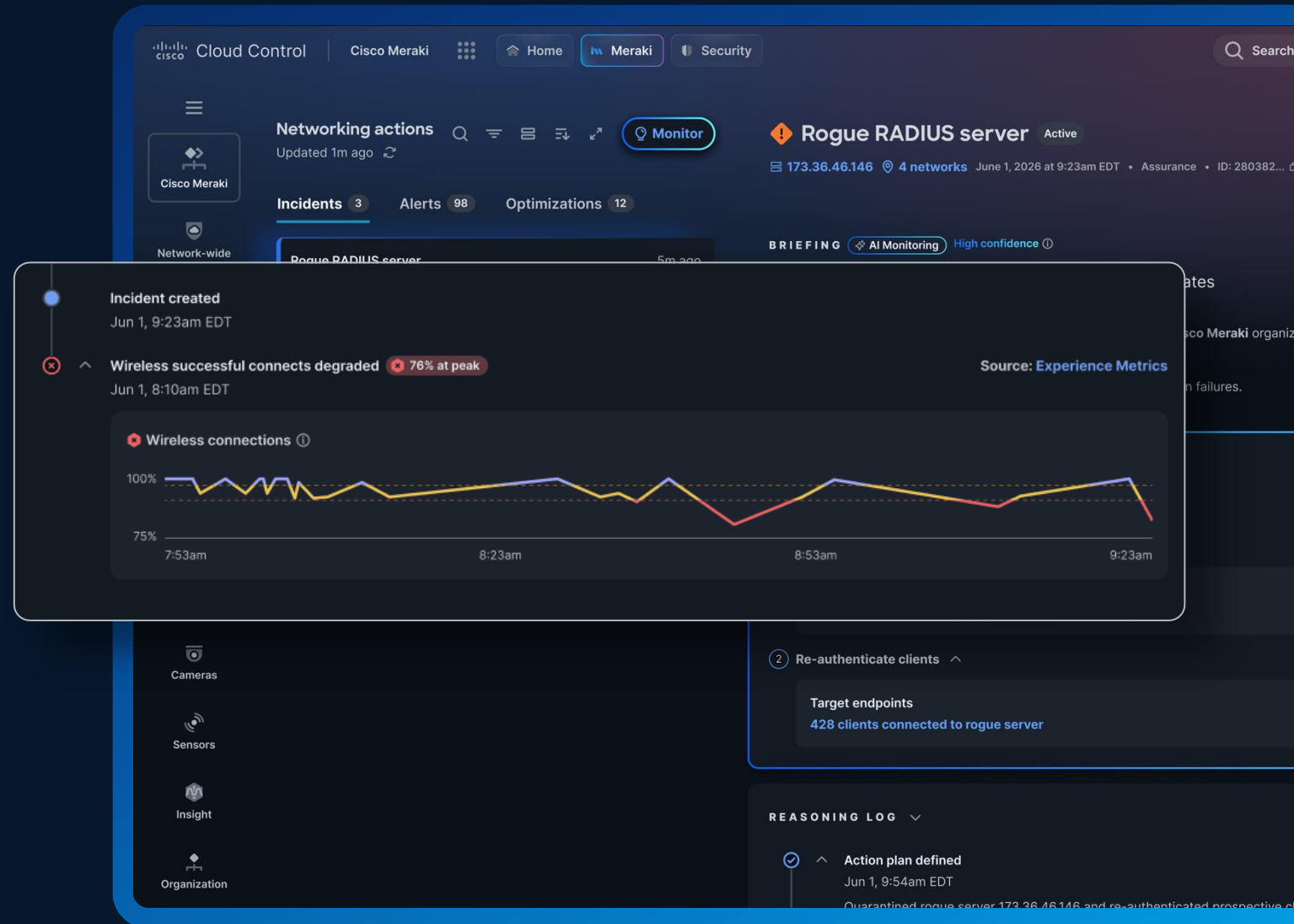
Enhanced Experience Metrics

Continuous real-time experience assessment

Monitors user outcomes and creates incidents

Shift from observing systems to understanding experiences

Collapses thousands of signals into a single view

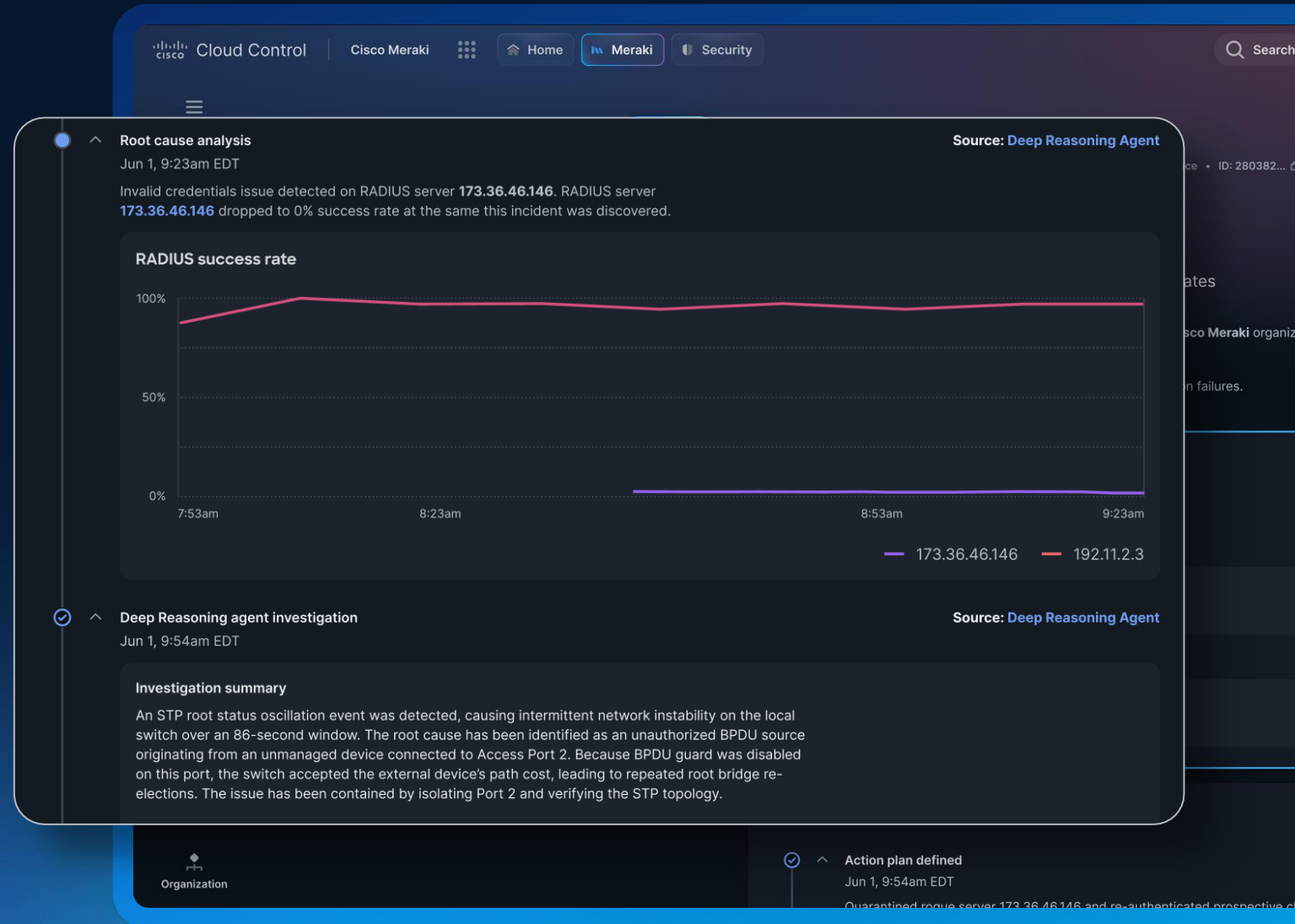


Deep Reasoning

Deeply investigates
to identify root cause

Correlates symptoms, assesses
impact,
and refines conclusions for greater
accuracy

Available to agents and humans via
the AI Assistant



ALPHA JULY 2026

Digital Twin

Validates before
applying changes

Emulates devices, connectivity, and
configuration in a true Digital Twin

The screenshot displays the Cisco Cloud Control interface, specifically the 'Networking actions' section. A 'Monitor' button is visible. The main content area shows a 'Nook-HQ-SF — IOS-XE 17.12.4 Upgrade' task. Below the task title, there is a summary of the request and a list of devices to be upgraded. The devices are categorized by role (Core, Distribution, Access) and status (Eligible, Ineligible).

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

Below the table, there is a 'Validation Summary' section showing the results of the validation process. It includes a 'Validation Results' bar indicating that 15 of 15 tests passed, and a 'NEXT STEP' button to deploy the twin-validated image to production.

Validation Summary

Target image: **IOS-XE 17.12.4**

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

Reasoning Log

- ✓ Action plan defined
Jun 1, 9:54am EDT
Quarantined rogue server 173.36.46.146 and re-authenticated prospective c...

Cisco IQ™ - It is just few clicks away!

Where human expertise meets agentic intelligence

<https://iq.cisco.com/>



Built for different jobs. Designed to work together

IQ

AI-powered services

- Lifecycle visibility & planning
- Assessments & compliance gaps
- Expert-informed guidance
- Benchmarking & risk prioritization
- Support & Professional Services

For planners & decision makers

Same asset truth across
both experience



Cloud Control

AI-powered operations

- Live telemetry across your IT estate
- Cross-domain visibility
- Real-time action & remediation
- AI Canvas collaborative workspace
- Automated resolution workflows

For operators & daily drivers

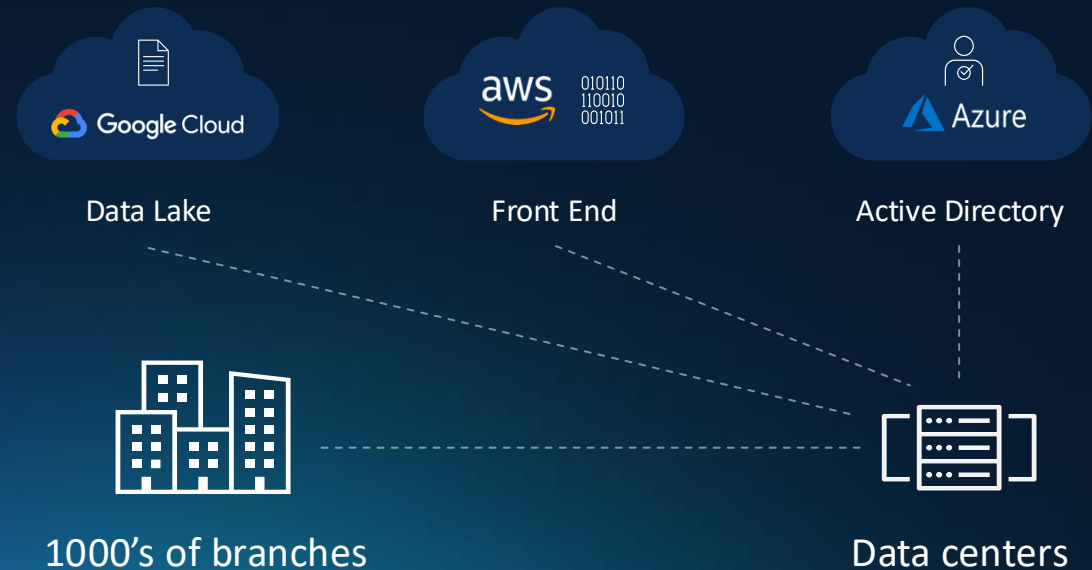
Multivendor clouds create bottlenecks and complexity

Enterprise workloads ->
AI multicloud workloads

Hub connectivity -> Distributed
connectivity

Multiple clouds ->
Multicloud network

Typical multicloud architecture



BETA JUNE 2026

Introducing Cisco Multicloud Fabric

Single multicloud networking service – available via Cloud Control

Instantly available global fabric across clouds

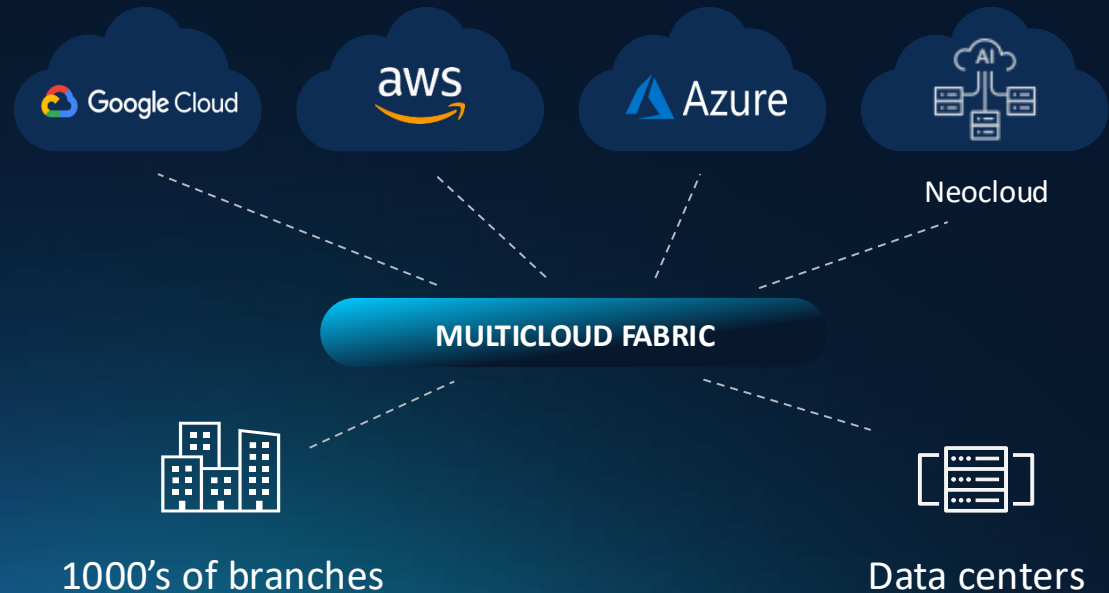
Built-in security and end-to-end visibility

Use Cases

Site-to-Cloud

Cloud-to-Cloud

Multicloud Fabric



Alpha July

CLI profiles

Cloud management at scale

- Deploy configuration updates to thousands of switches in minutes
- Use dynamic templates to automatically adapt configurations
- Maintain familiar CLI workflows while gaining cloud-managed control

The top screenshot shows the 'Configuration Profiles' section in the Meraki dashboard. It displays a table with one profile named 'IGMP Fast leave' applied to 179 switches. The bottom screenshot shows the 'Switches' section, listing 10 switches across all networks. The switches are categorized by status (Alerting, Online, Offline) and network (Campus A Network, Remote Branch Network).

Name	Model	Serial number	IP address	Status	Network	Uptime	CLI Profile
SFO12-2-CA29X	MS390-24UX	Q3ED-XQ37-XD6C	10.10.1.1	Alerting (2 alerts)	Campus A Network	9h 52m	IGMP Fast leave
SFO12-2-CB81Z	C9300-48P	FCW212419CF	10.10.1.2	Online	Campus A Network	28d 20h 44m	IGMP Fast leave
SFO12-2-CO06Y	MS390-48UX	Q3ED-XQ37-AB3K	10.10.1.3	Online	Campus A Network	14d 6h 12m	IGMP Fast leave
SFO12-2-CW52A	MS125-48	Q2SW-SCX8-9AKL	10.10.1.4	Alerting (1 alert)	Campus A Network	3d 14h 22m	IGMP Fast leave
SFO12-2-CD11B	MS250-48FP	Q2SW-SCX8-9AMH	10.10.1.5	Online	Campus A Network	45d 2h 08m	IGMP Fast leave
SFO12-2-CE33C	MS390-24UX	Q3ED-XQ37-CD8P	10.10.1.6	Online	Campus A Network	7d 18h 55m	IGMP Fast leave
RB01-2-AA10X	MS125-24P	Q2SW-SCX8-9ANN	192.168.10.1	Online	Remote Branch Network	62d 4h 30m	IGMP Fast leave
RB01-2-AB22Y	MS250-24P	Q2SW-SCX8-9APP	192.168.10.2	Alerting (3 alerts)	Remote Branch Network	1d 8h 10m	IGMP Fast leave
RB02-2-AC45Z	MS390-48UX	Q3ED-XQ37-EF9Q	192.168.20.1	Online	Remote Branch Network	33d 11h 42m	IGMP Fast leave
RB02-2-AD88W	C9300-24P	FCW213311DE	192.168.20.2	Offline (1 alert)	Remote Branch Network	—	IGMP Fast leave

June 2026

Cloud Management for IOS XE Secure Routers

Operational simplicity for full-stack locations

- Enterprise-grade power and resilience with Meraki simplicity
- Full-stack branch management, now more powerful than ever
- Future-proof branches in minutes

The screenshot displays the Cisco Meraki cloud management interface. The top navigation bar includes the Cisco logo, the word "Meraki", and a search bar. The left sidebar contains a menu with options: Global Overview, Organization (Secure WAN TME Demo - IOS XE), Network (Small-Med Branch BR102 - Seattle SEA), Network-wide, Assurance, Security & SD-WAN, Cameras (with a "Learn more" link), Organization, Automation, and Find in Menu.

The main content area is titled "Inventory" and includes a subtitle: "View deployed and available devices in your organization, or claim new devices. After selecting devices, you can add to a new or existing network." Below this is a search bar and a "Deployment status" dropdown menu. A table lists three devices with columns for MAC address, Cloud ID, Serial number, Network, Model, Claimed on (UTC), Order number, and Country.

MAC address	Cloud ID	Serial number	Network	Model	Claimed on (UTC)	Order number	Country
cc:6a:33:45:36:00	Q4LD-UW44-4UNJ	FDO2912M0F0	Datacenter DC10 - Atlanta ATL	C8455-G2	Sep 26 2025 23:18		
d0:85:43:1b:70:e0	Q4LH-9JCP-U28Y	FDO2924M07R	Large Branch BR101 - New York LGA	C8355-G2	Nov 13 2025 17:41		
e4:a4:1c:83:0d:a0	Q4LL-24KU-5KJJ	FGL2902L2VN	Small-Med Branch BR102 - Seattle SEA	C8235-G2	Nov 18 2025 14:02		

Below the inventory table, a detailed view of a network device is shown. The device is identified as "Network SJC_BRANCH" with MAC address "e4:a4:1c:83:62:60" and model "C8235-G2". A "Configuration source: Cloud" label is present. A "Set a location for this appliance" dialog box prompts the user to add an address and check the move marker to update its location. The "ADDRESS" field is populated with "104.251.70.68" and marked as "Active". The "HOSTNAME" field is empty.

On the right side of the detailed view, a "CLI terminal" window is open, displaying the output of the command "Router>show crypto autovpn session". The output shows local information, device number, ID, and VPN registry details for WAN-1 and WAN-2.

```
Router>show crypto autovpn session
Local Information:
Device Number: 306267, ID: 114893eed6

Local-WAN info learnt from VPN Registry
Local-WAN Interface
-----
WAN-1      TenGigabitEthernet0/0
WAN-2      TenGigabitEthernet0/0

VPN Registry-1 158.115.133.140:9353
Local-WAN      Status P
WAN-1          Connected 104
WAN-2          Disconnected

VPN Registry-2 158.115.141.233:9353
Local-WAN      Status P
```

A man with a beard and glasses, wearing a large headset, is seated at a desk in an office environment. He is looking towards the left side of the frame, presumably at a computer monitor. The background is slightly blurred, showing office shelves and equipment. The overall image has a blue and purple color overlay.

**The network is the enforcement
layer that is always present.**

SECURE NETWORKING ARCHITECTURE

Security fused into the network

Advanced security at every layer

AgenticOps

Hybrid mesh firewalling

Zero Trust access

Scalable network segmentation

Secure infrastructure

UNITED BY COMMON POLICY

AI + Quantum = Attacks at machine speed



AI
accelerates discovery



Quantum
undermines
encryption



Small cracks
expose full
attack paths

Zero-minute attacks break your Zero-Trust architecture

SECURE NETWORKING ARCHITECTURE

Security fused into **the network**

Live Protect
on Smart Switches

GA AUG 2026

Post-Quantum
Cryptography
now for SD-WAN

GA AUG 2026

Cisco Firewall
on Secure Routers

GA AUG 2026

GA Sept 2026



Cisco Live Protect

Closes the 'patch gap' –
defending products in
production against frontier AI
threats.

Block vulnerabilities instantly; update
on your schedule.

The screenshot displays the Cisco Cloud Control interface for managing Security Advisories. The left sidebar shows the navigation menu with 'Security' selected. The main content area is titled 'Security Advisories' and includes tabs for 'Advisories', 'Devices', and 'Live Protect Shields'. The 'Live Protect Shields' tab is active, showing a summary of 6 results and a table of shields. The right sidebar provides configuration options for a selected shield, including deployment mode (Monitoring, Enforcing, Deactivate) and deployment details.

Security Advisories

Advisories | Devices | **Live Protect Shields**

Live Protect Shields

6 results

1 Available

Search shields Impact Shield Status Version 6 results

Advisory ID	CVEs
cisco-sa-ios-xe-cmd-inject-rPJM8BGL	CVE-2025-20334
cisco-sa-story4-medium-27-1779407786	CVE-2025-10000
cisco-sa-story4-critical-27-1779407786	CVE-2025-20000
cisco-sa-story4-low-27-1779407786	CVE-2025-30000
cisco-sa-story4-medium-27-1779407786	CVE-2025-30000
cisco-sa-story4-critical-27-1779407786	CVE-2025-40000

Deploy Live Protect Shields

Deploy Live Protect Shields to mitigate advisories.

About this Shield

Advisory ID
[cisco-sa-ios-xe-cmd-inject-rPJM8BGL](#)

Shield description
Detects and blocks malicious command injection

Choose deployment mode

☒ **Monitoring**
Vulnerability-related events are logged, but exploit attempts are not blocked.

☐ **Enforcing**
Exploit attempts are automatically blocked and vulnerability-related events are logged.

☐ **Deactivate**
Stop monitoring or protecting exploit attempts on the selected devices.

Deployment details

[cisco-sa-ios-xe-cmd-inject-rPJM8BGL](#) **Monitoring** to **0 devices**

Command Injection Detection Shield

Impact **High** CVEs CVE-2025-20334

Devices (1)

You are deploying Live Protect Shield in monitoring mode for the devices below.

Deployment (0 items)



Quantum Resilience

Future-ready communication and products

Now is the time to make your network post-quantum secure

Harvest now



Decrypt later

Sectors affected now



Financial services



Government & Defense



Energy & Utilities



Healthcare



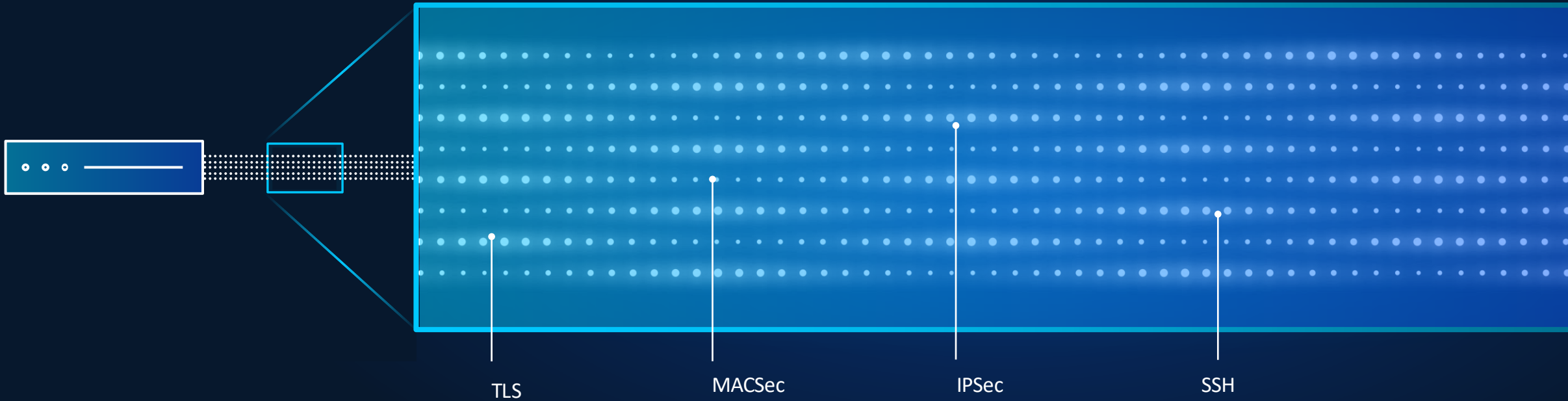
Manufacturing

Cisco Live America 2026



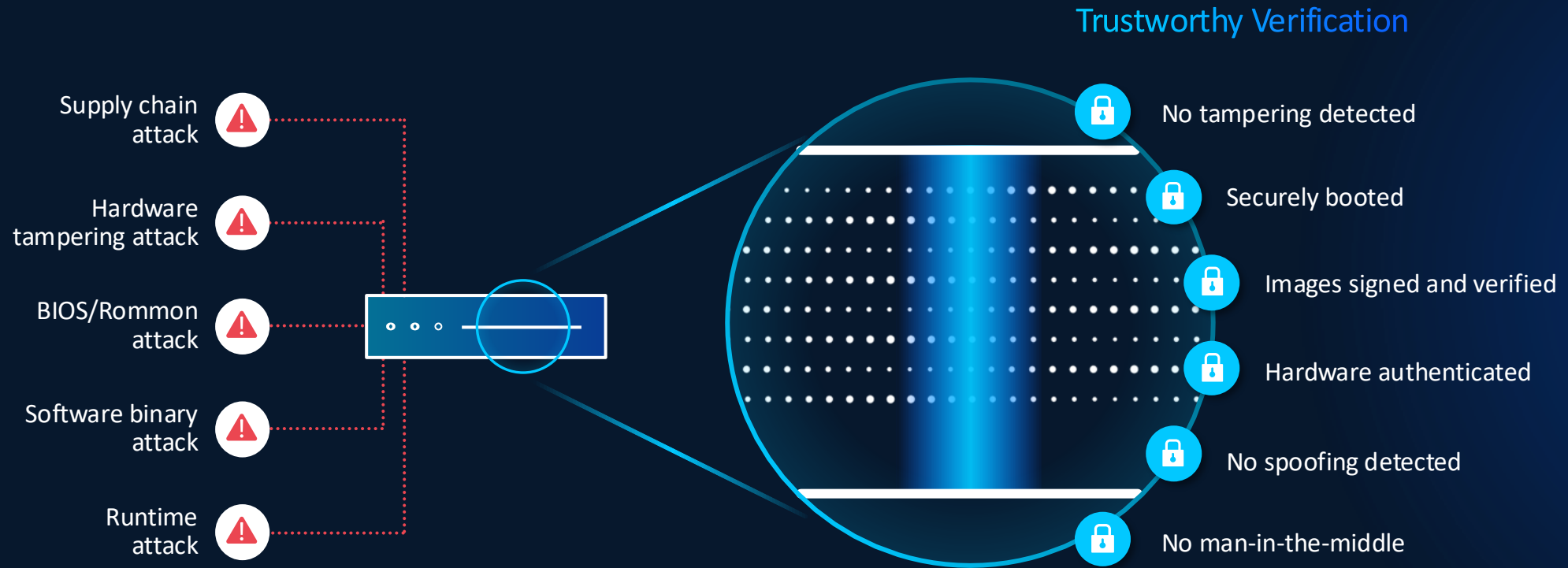
Protect sensitive data from 'Harvest Now, Decrypt Later'

Quantum-safe communication



Build resilient networks based on trustworthy devices

Quantum-safe products



GA August 2026

Cisco Firewalls on Secure Routers

Define intent once. Enforce consistently.

- Firewall intelligence on every router
- One console for enterprise-wide policies
- Identity-driven control limits lateral movement
- Faster changes, fewer handoffs, flexible licensing

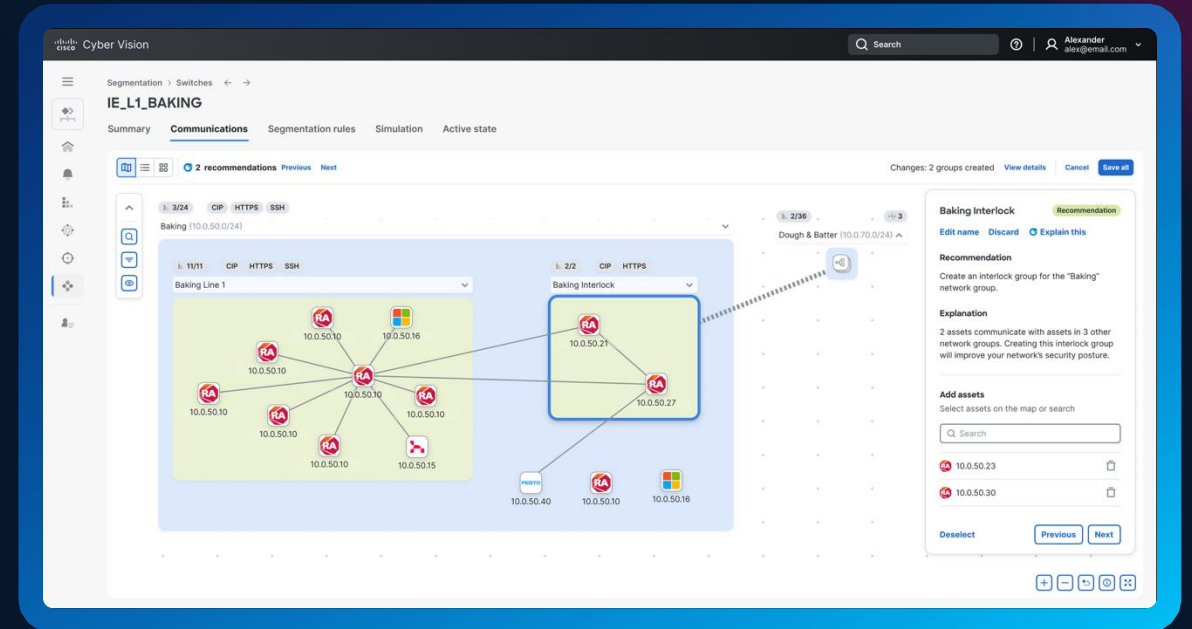


GA September 2026

Cisco Cyber Vision

Segment industrial networks in weeks, not years

- Move from flat, unsegmented networks to effective, policy-based protection
- AI-assisted policy recommendations to guide OT users when implementing segmentation
- Risk-free policy simulation to ensure segmentation will not disrupt production
- Network native policy enforcement at 10Gbps line-rate by industrial switches



**Scalable devices
are the foundation for
the AI era.**

Scalable devices, ready for AI



Smart
Switches



Secure
Routers



Secure
Firewalls



Scalable
Wi-Fi 7



Industrial
IoT

← Unified hardware | Unified software | Unified management →

Orderable June 2026

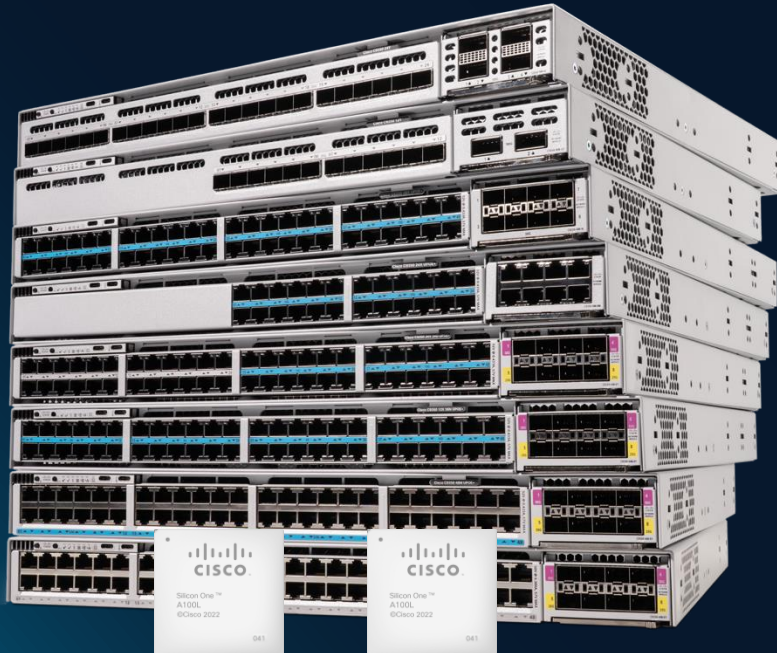
Cisco C9350 Series Smart Switches mGig and Fiber Fixed Access for the AI-ready Campus

Up to 1.6Tbps for
High AI performance

PQC & integrated
security

Intelligent energy
efficiency

In-network application
hosting



Cisco C9350-24Y - 24x 25G/10G/1G SFP28*

Cisco C9350-12Y - 12x 25G/10G/1G SFP28*

Cisco C9350-48S - 48x 1G SFP*

Cisco C9350-24S - 24x 1G SFP*

Cisco C9350-48HXG - 24x 10G-mGig & 24x 1G w/ 90W UPoE+*

Cisco C9350-48HXN - 12x 10G-mGig & 36x 5G-mGig w/ 90W UPoE+

Cisco C9350-24HX - 24x 10G-mGig w/ 90W UPoE+

Cisco C9350-48HM - 48x 2.5G w/ 90W UPoE+*

* Available in next phases.

Orderable May 2026, September 2026

Cisco C9550 Series Smart Switches

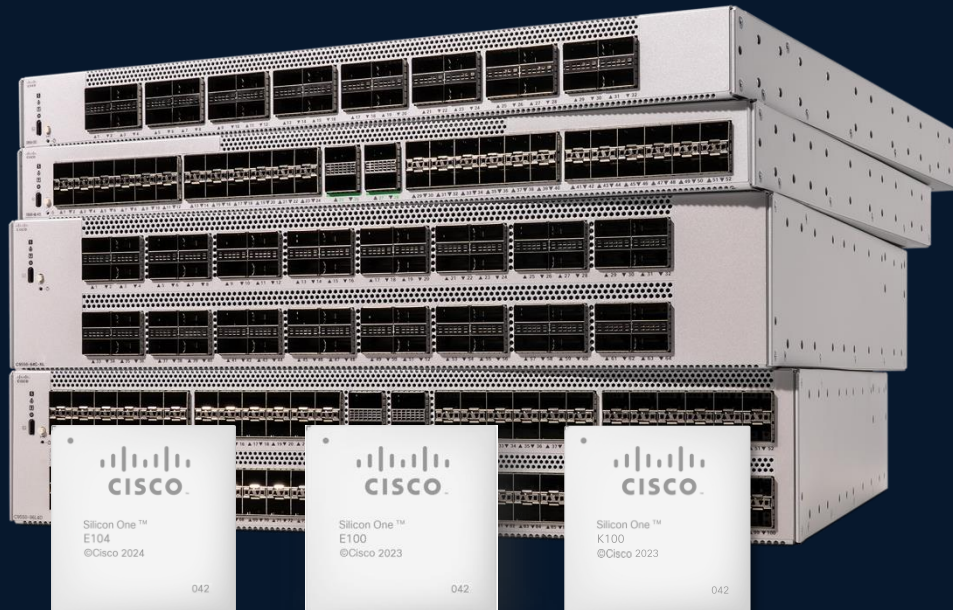
Fixed Core and Aggregation Built for the AI Era

Up to 6.4Tbps for
High AI performance

PQC & integrated
security

Intelligent energy
efficiency

In-network application
hosting



C9550-24L4CD - 24x 1/10/25/50G - 4x 40/100G/ 2x 400G

C9550-48L4CD - 48x 1/10/25/50G - 4x 40/100G/ 2x 400G

C9550-96L4D - 96x 10/25/50G - 4x 40/100/400G

C9550-32C - 32x 40/100G (QSFP)*

C9550-64C-XL - 64x 40/100G (QSFP)*

Orderable June 2026

Premium outdoor Wi-Fi 7 Cisco Wireless 9177 Series

Designed for demanding outdoor environments

URWB for low latency connections in demanding environments

Multiple antenna formats for custom outdoor coverage



CW9177I/E/D

CW9177 Specs

IOS-XE 26.2.1 and 26.1.x



CW9177I

Omni directional antenna
For Horizontal mounting



CW9177D

Directional antenna
(72x72 – 7 dBi)



CW9177E

External antenna
8x N-type connector

Key specs

12spatial streams
4x4 on 2GHz, 4x4 on 5 GHz, 4x4 on 6 GHz
-or-
4x4 on 2GHz, and dual 4x4 on 5 GHz
Accelerometer (I,D,E*)
CleanAir Pro

BLE/IoT and dedicated scan radio

10 Gbps copper and SFP+ port

DC Power input

Global Use AP

IP67

Operating Temp: -40°C to 65°C w/o solar

Secure networking, simplified for the AI era

8100 Series



Flexible
connectivity for the
smallest sites

Available Sept 2026

8200 Series



Cost-effective
branch
connectivity

8221/8225: Available Aug 2026

8211/8221L: Available Sept 2026

8300 Series



Scale secure
routing and SD-WAN for
large branch

Available Sept 2026

8600 Series



High-throughput aggregation
for modern data centers

Available Sept 2026

Cisco Unified Edge: Future-Ready Performance

Integrates compute, networking, storage, and security

AI-ready edge

Compute node

Compute

Storage

Software

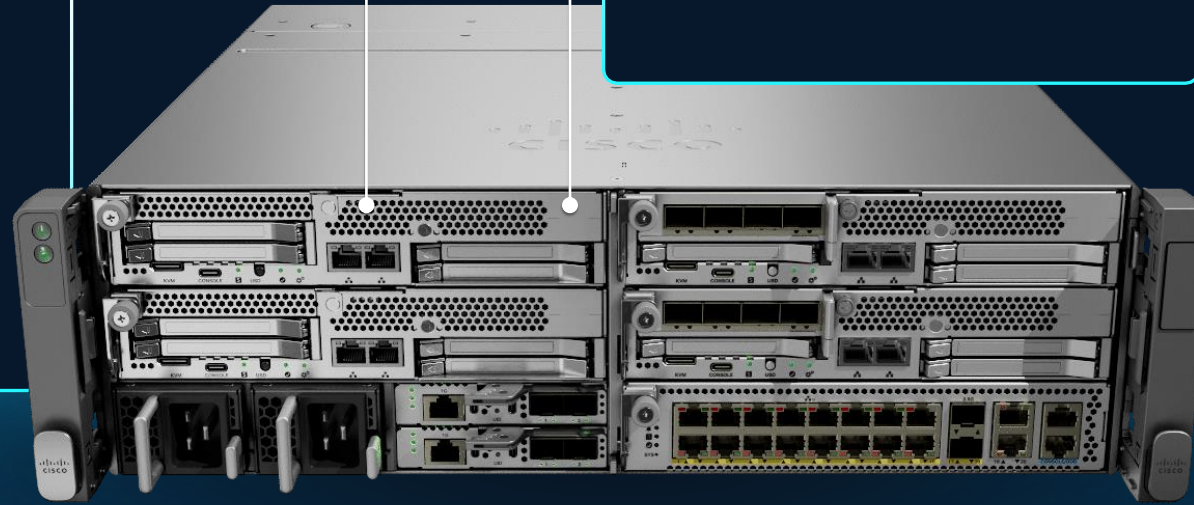


GPU

Half-height/half-length GPU

NVIDIA L4 first

Additional GPUs on roadmap



Intel Xeon 6 SoC

CPU native AI inferencing (AMX)

Confidential compute (TDX & SGX)

Integrated Ethernet

Scalable multithreaded
cores (12, 20, 32)

NUTANIX



vmware
by Broadcom



Microsoft

intel



SUSE

Introducing Secure Router Node for Unified Edge

Enabling Integrated networking and security alongside compute and storage



Secure Router Node



High-Speed 10GE and 2.5mG uplinks

Higher LAN port density

Up to **360W** PoE Capacity

Post Quantum ready

Orderable June 2026

Cisco IR1000 Rugged Series Secure Routers



- Designed for space and power constrained environments (in <1.5" depth enclosure)

- Runs on sub-5W solar or battery power

- Quantum-safe and trusted in any environment



Introducing Cisco Secure IR1000 Series

IR1001-G2



Essential security at the edge for simplified traffic flows at scale

- OT aware application firewall
- Policy based OT traffic isolation
- Secure communication w/ post quantum encryption

IR1005-G2



Greater visibility and control of security for complex traffic flows at the edge

- ⊕ OT aware intrusion detection & prevention w/ NGFW
- ⊕ Proactive network assurance with ThousandEyes
- ⊕ Secure device w/ post quantum authentication

Key launch highlights



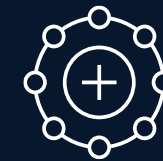
Simplified operations powered by AgenticOps

New autonomous operations
capabilities and
new Multicloud Fabric



Security fused into the network

Live Protect
on campus and branch
Smart Switches



Scalable AI-ready devices

Expansion of next generation
line up



Cisco named a Leader by Gartner for Enterprise Wired and Wireless LAN Infrastructure

Source: Gartner, Magic Quadrant™ for Enterprise Wired and Wireless LAN Infrastructure, Mike Leibovitz, Christian Canales, Tim Zimmerman, May 18, 2026

Gartner and Magic Quadrant are trademarks of Gartner, Inc. and/or its affiliates.

Gartner does not endorse any company, vendor, product or service depicted in its publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner publications consist of the opinions of Gartner's business and technology insights organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this publication, including any warranties of merchantability or fitness for a particular purpose.

Figure 1: Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure



Gartner

Děkujeme za pozornost !!!

... A těšíme se v září na shledanou.

