CISCO Connect

Modernize the Network with Cisco Secure Campus



Lila Rousseaux
Principal Solutions Designer

Ian Procyk
Solutions Designer

Oct 21st 2026

Who are Lila and Ian?

- Campus and Operations Lady
- Joined Cisco 1999
- Based in Toronto Canada
- Off the clock: Mom of 2 teens

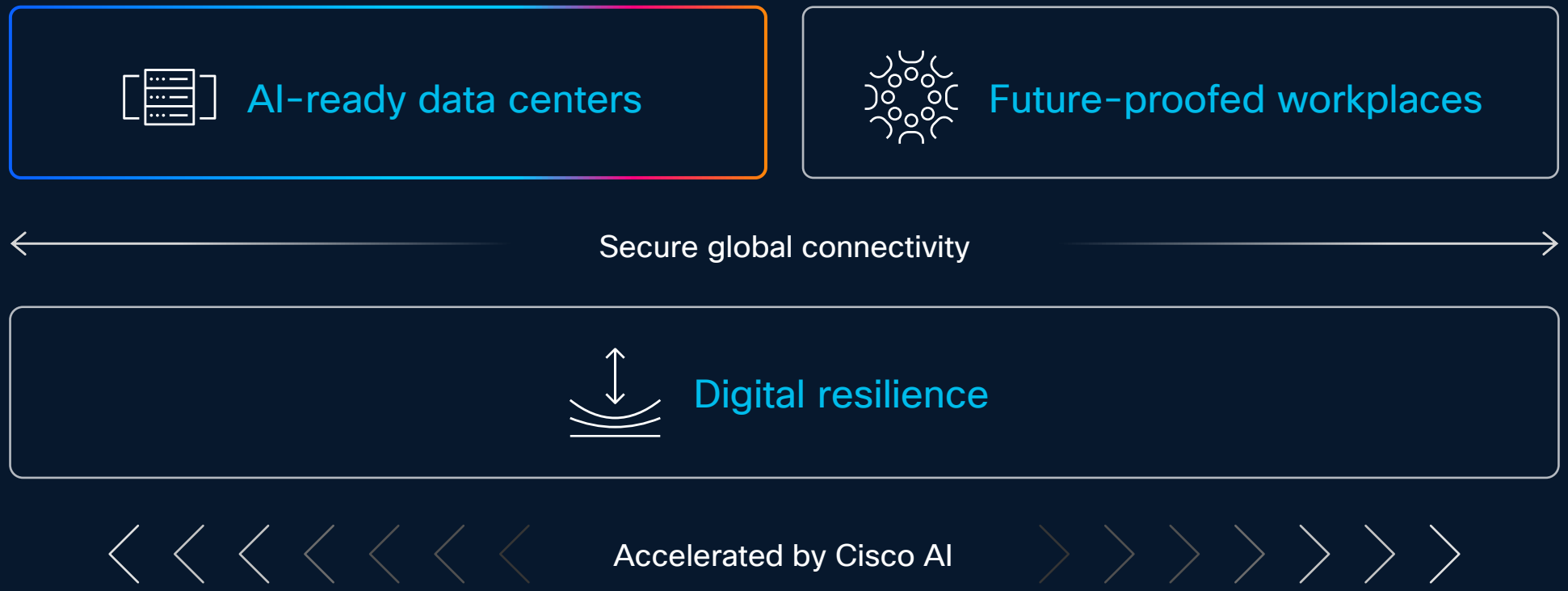


- Wireless Guy
- Joined Cisco 2011
- Based in Vancouver, BC
- Off the clock: Volunteer: Ham Radio Nerd
  Licensed 1997: VE7HHS



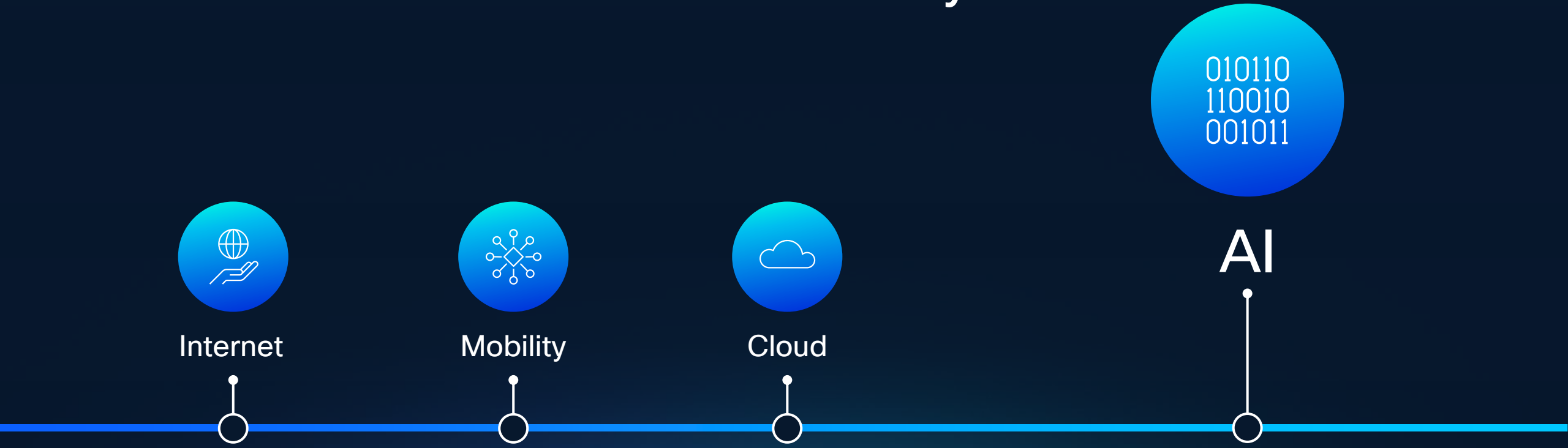
© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco powers how people and technology work together across the physical and digital worlds



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

AI is the biggest disruption we have seen yet



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

AI adoption is accelerating



Chatbots

Productivity tools



Agents

Digital coworkers

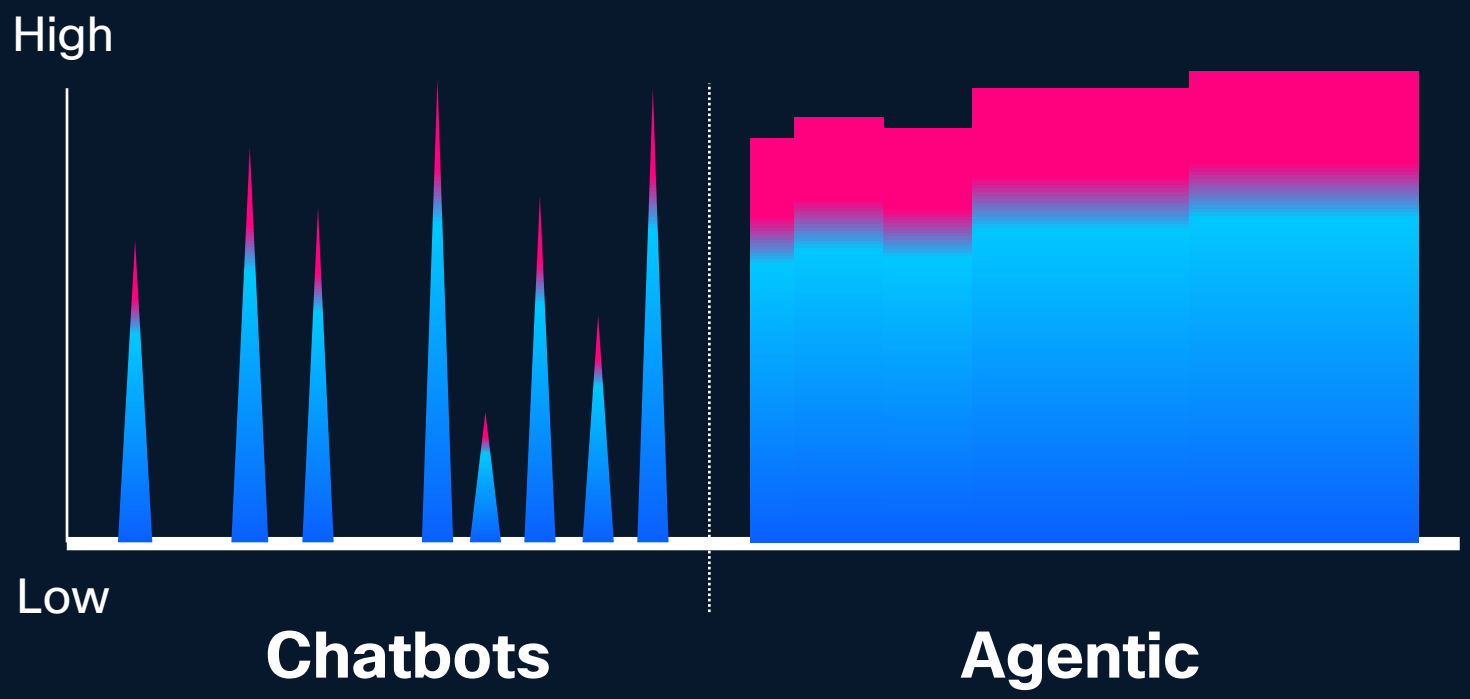
Creating new network demands

Changing traffic patterns
Increased sustained east-west traffic

Agentic execution
Beyond DC, across environments

Need for AgenticOps
Keeping Agents running, moving beyond human-paced operations

AI-driven threats
Rapidly evolving security needs



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

Frontier AI models are creating an entirely new level of risk

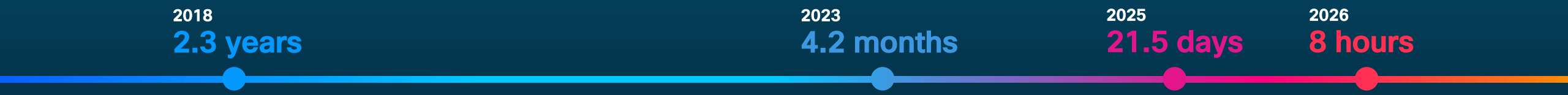
Vulnerabilities weaponized at scale

- More vulnerabilities
- Weaponized even faster
- Even specialized environments exposed

Not a one-time patch event

Each new model release will improve vulnerability discovery

THE AVERAGE TIME TO EXPLOIT VULNERABILITIES



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

Sources: Cisco Blog, "Strengthening the Foundation: A Predictable, Customer focused Response to AI-Accelerated Vulnerability Discovery," April 7, 2026; zerodayclock.com, June 23,2026

Our approach to addressing these new demands:

Architecture for the AI-ready secure network



Simplified operations powered by AgenticOps



Security fused into the network

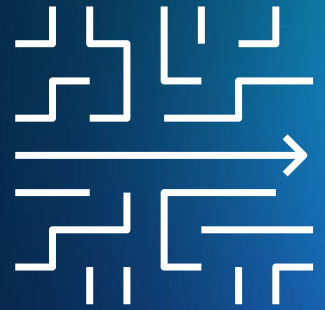


Scalable devices ready for AI

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

cisco

Simplified operations powered by AgenticOps



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

A day in the NOC

Imagine: Same incident, different operating model

- Users report poor call quality
- Login, collaboration experience management
- Login, check observability tool
- Login, check networking tool
- Manually correlate timestamps
- Escalate, war room, coordination
- Resolved, hours later

- Related alerts are surfaced as one correlated incident
- From the alert, Seamlessly launch an investigation across domains
- Get a suggestion for a fix. Operator approved. Agents executes and confirms.
- Operator resolves in minutes

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

AgenticOps Adoption Journey

Foundation: Controller Intelligence

Controller-Native AI & MCP

- Catalyst Center
- Meraki
- Nexus Dashboard
- SD-WAN

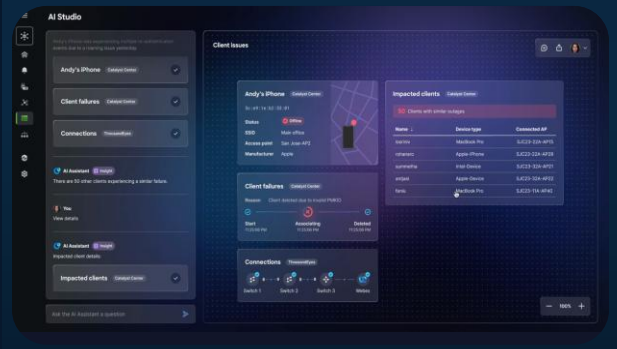
AI-driven network automation

Agentic Workflows



Unified Operations for Agentic IT

Cisco Cloud Control with AI Canvas

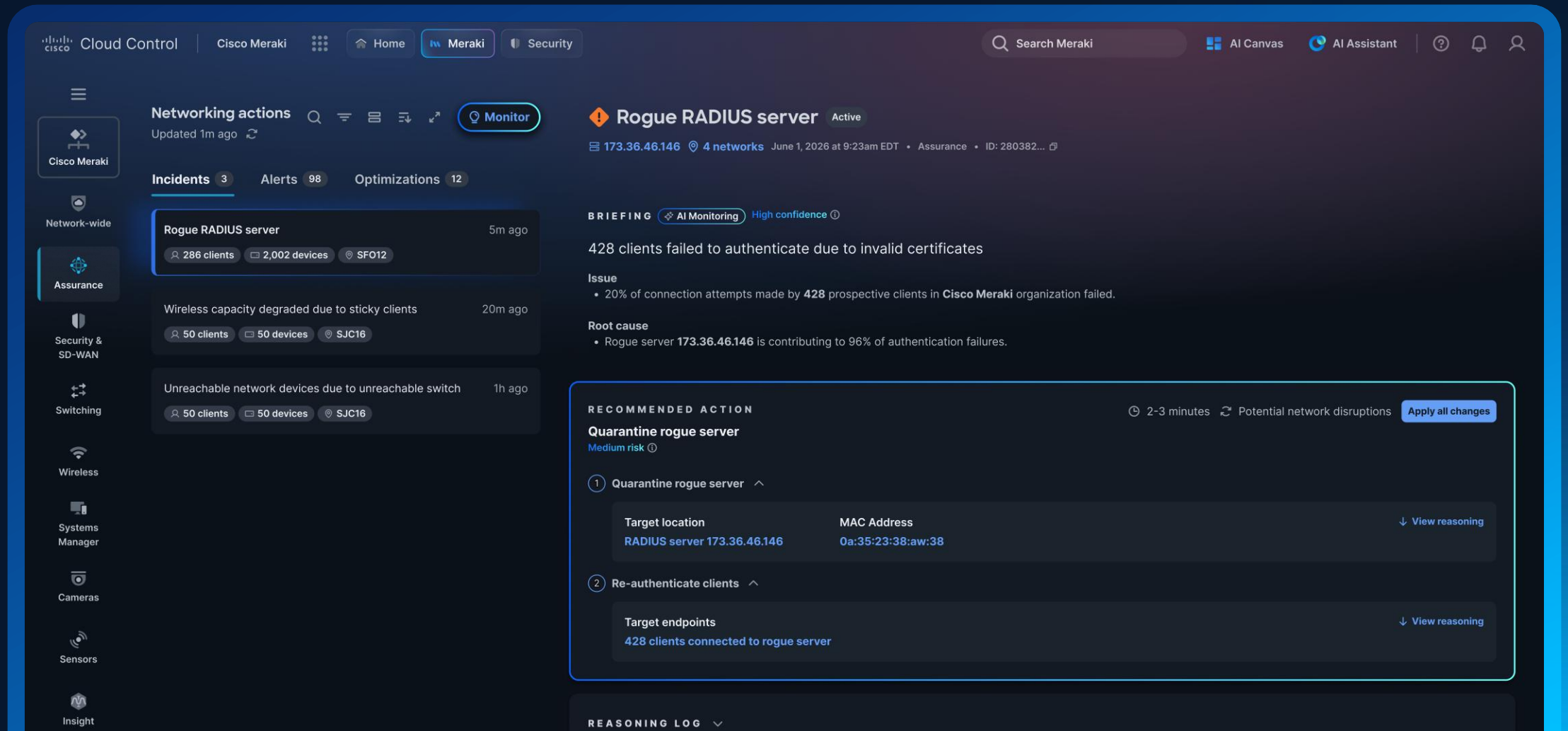


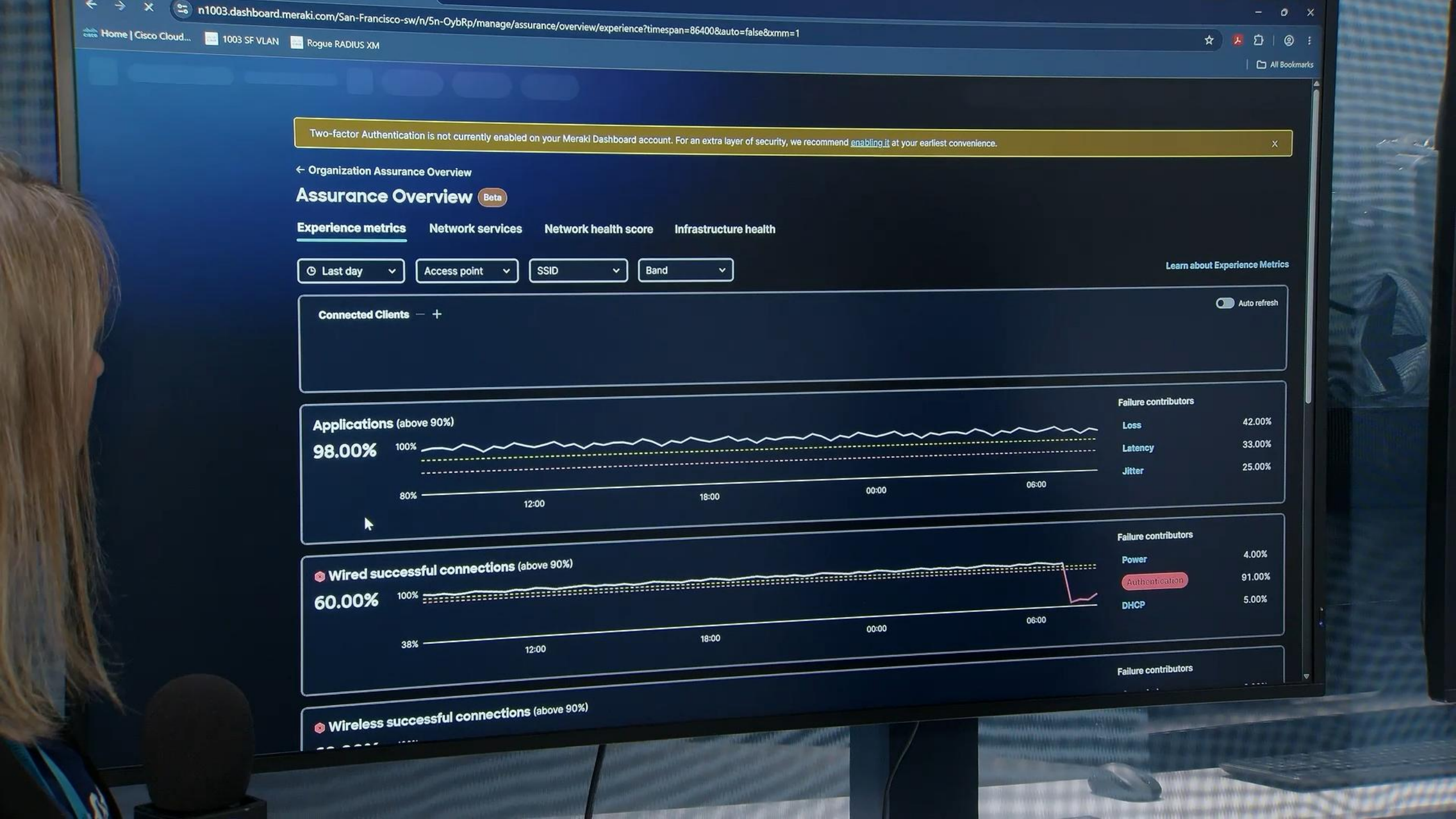
© 2026 Cisco and/or its affiliates. All rights reserved.

Beta Jun 2026

Introducing Agentic Actions for networking

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




n1003.dashboard.meraki.com/San-Francisco-sw/n/5n-OybRp/manage/assurance/overview/experience?timespan=86400&auto=false&xmm=1
Home | Cisco Cloud...
1003 SF VLAN
Rogue RADIUS XM
All Bookmarks
Two-factor Authentication is not currently enabled on your Meraki Dashboard account. For an extra layer of security, we recommend enabling it at your earliest convenience.
← Organization Assurance Overview
Assurance Overview
Beta
Experience metrics
Network services
Network health score
Infrastructure health
Last day
Access point
SSID
Band
Learn about Experience Metrics
Connected Clients
Auto refresh
Applications (above 90%)
98.00%
100%
80%
12:00
18:00
00:00
06:00
Failure contributors
Loss 42.00%
Latency 33.00%
Jitter 25.00%
Wired successful connections (above 90%)
60.00%
100%
38%
12:00
18:00
00:00
06:00
Failure contributors
Power 4.00%
Authentication 91.00%
DHCP 5.00%
Failure contributors
Wireless successful connections (above 90%)

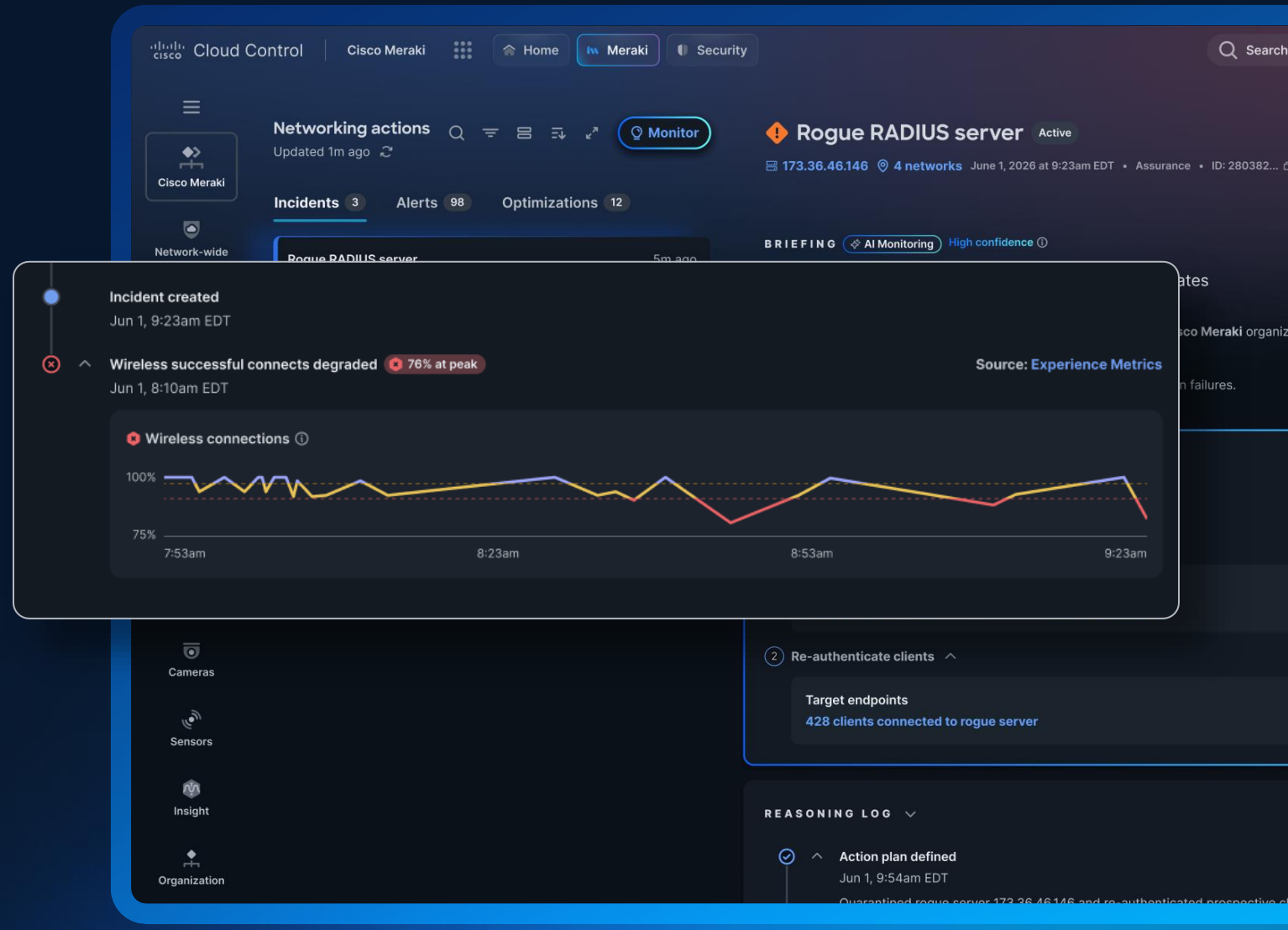
Enhanced experience metrics

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



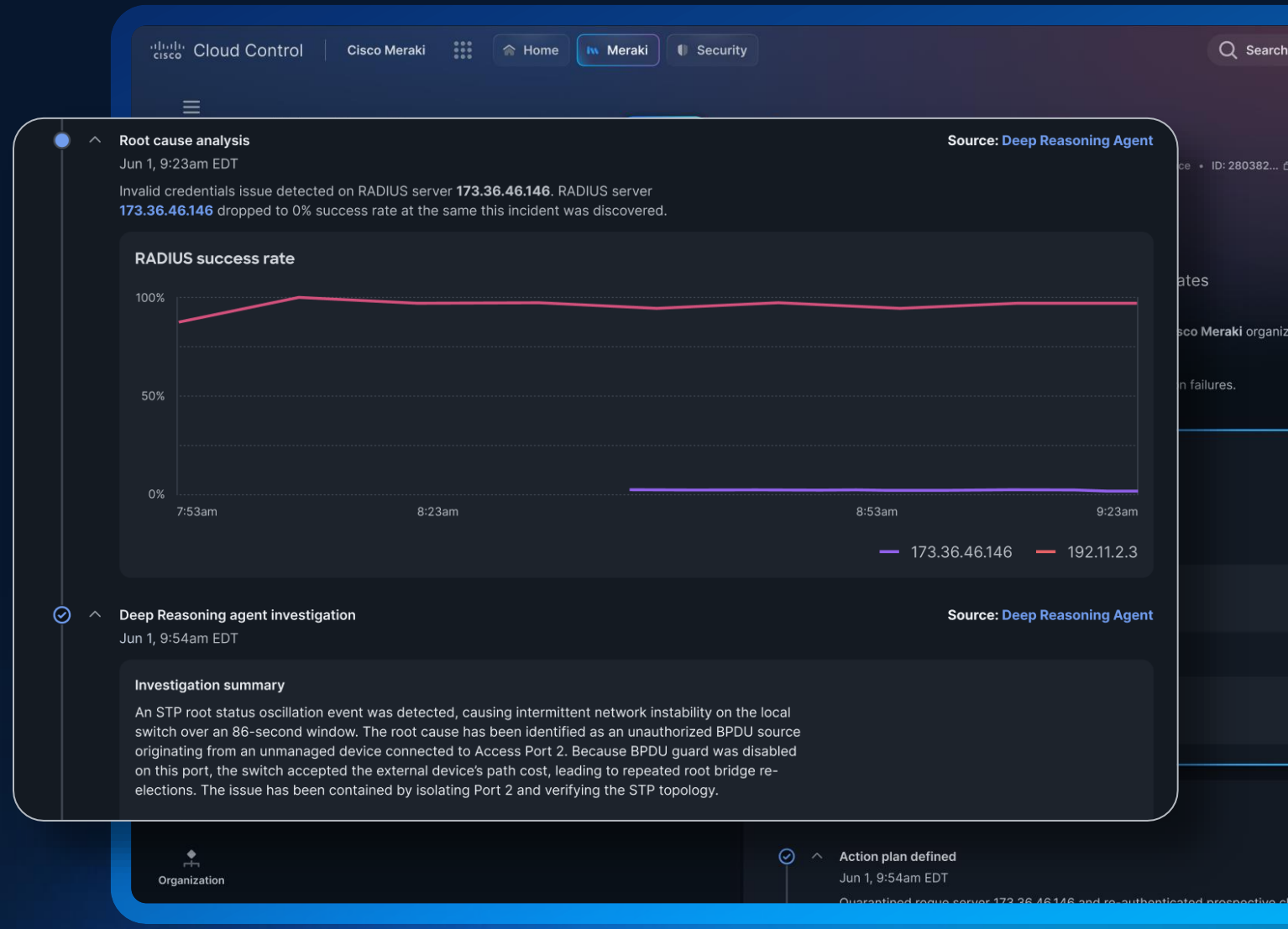
© 2026 Cisco and/or its affiliates. All rights reserved.

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



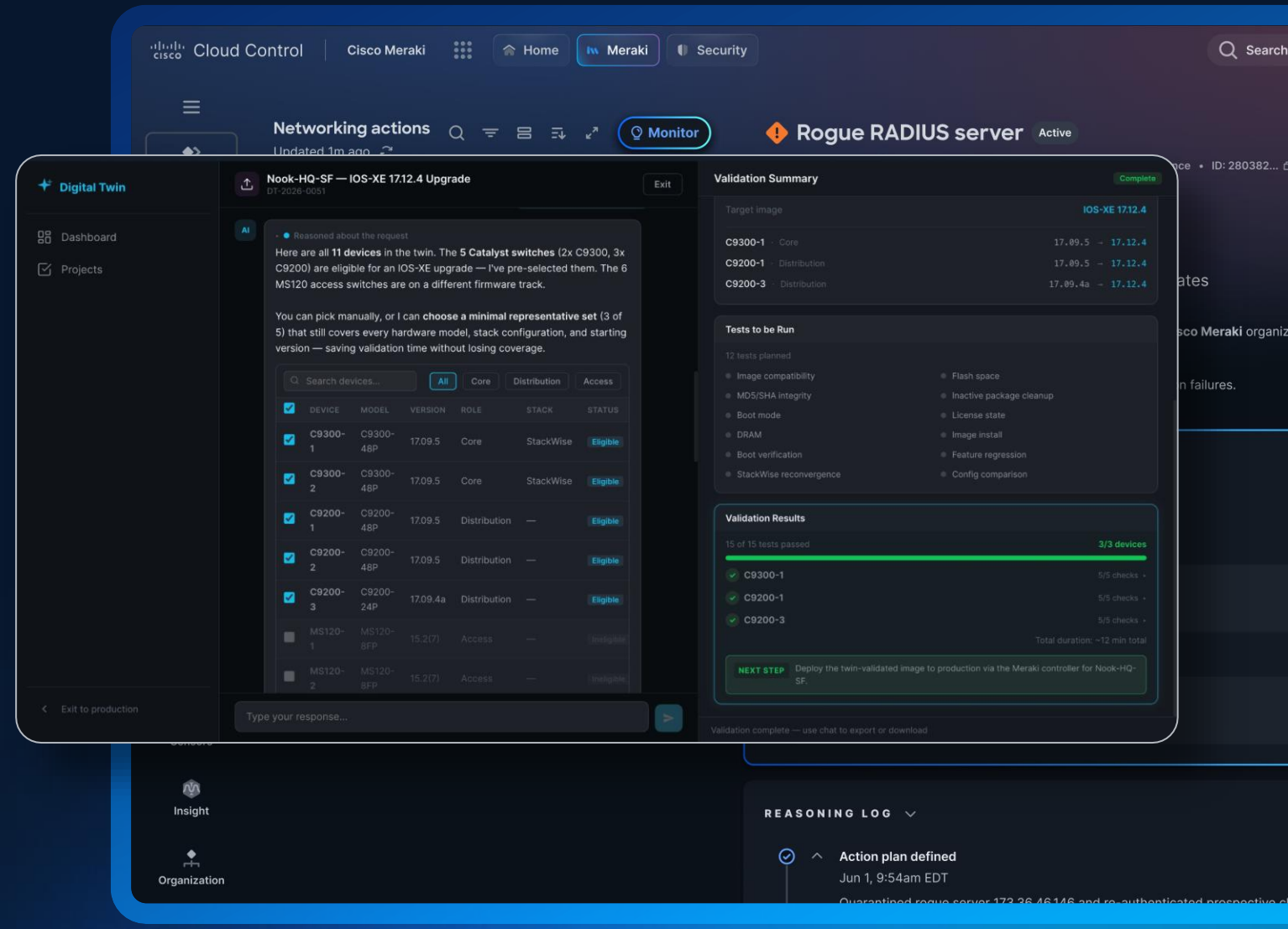
© 2026 Cisco and/or its affiliates. All rights reserved.

Alpha Jul 2026

Digital twin

Validates before applying changes

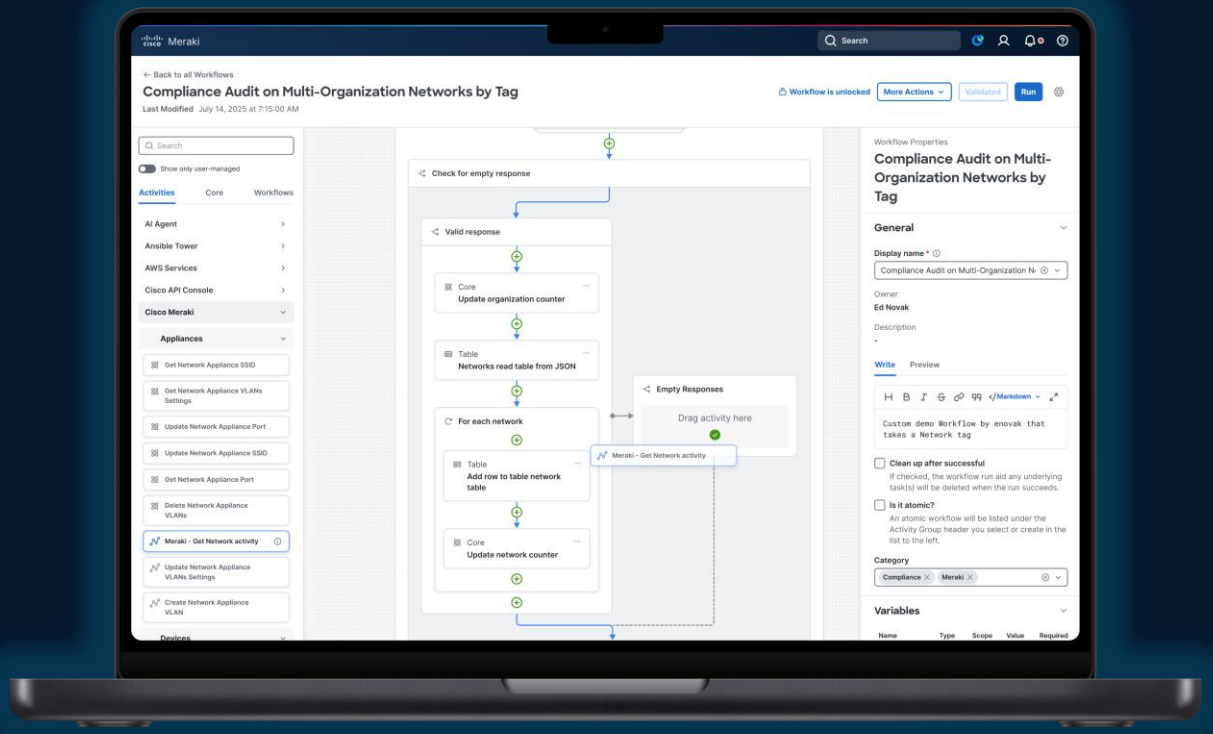
Emulates devices, connectivity, and configuration in a true Digital Twin



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

AI-driven network automation with Agentic Workflows

Low code/no code automation tool integrated with
Meraki Dashboard and Cisco Cloud Control

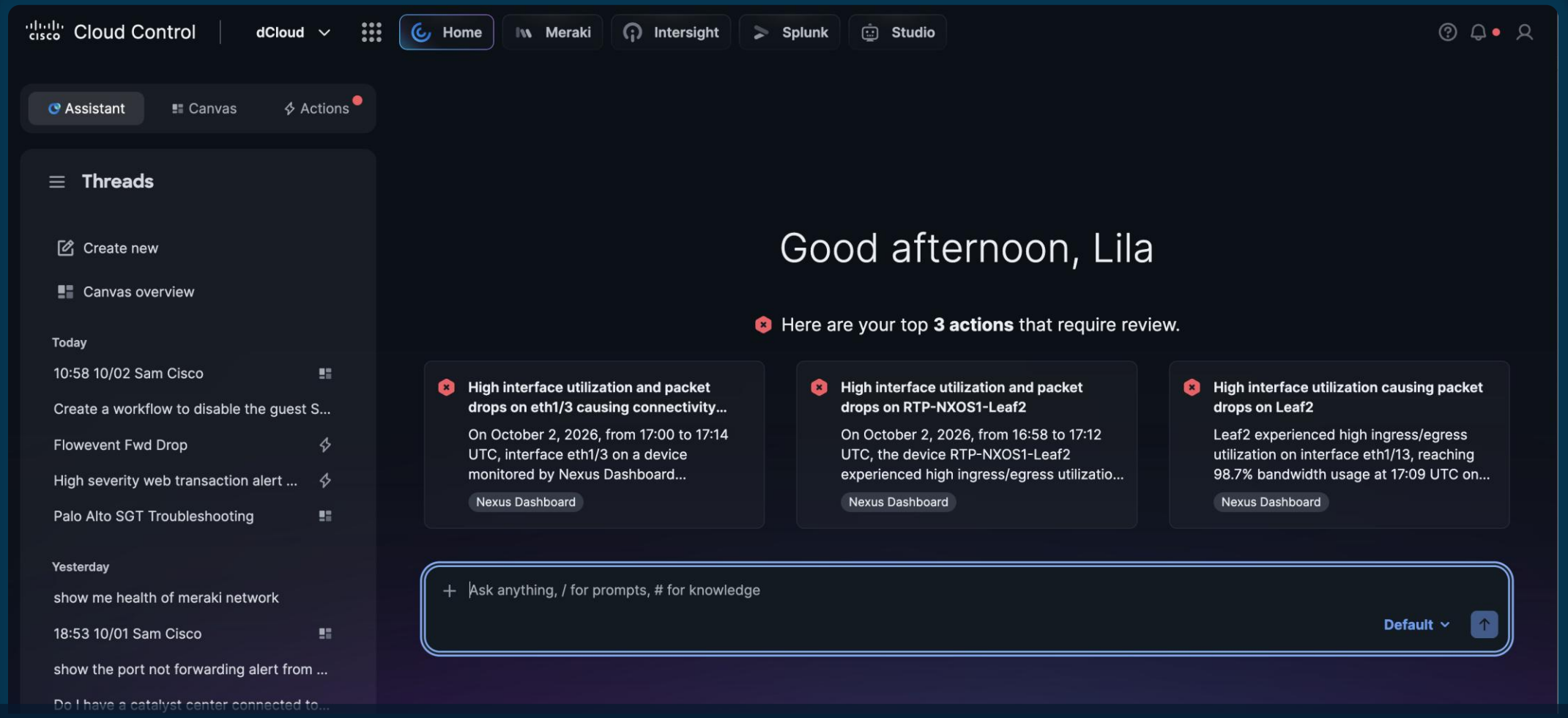


Cloud-Hosted Automation | Cloud-Hosted Automation | Integrated with AI Assistant | Custom and Pre-Built | For Cisco & Third-Party Domains

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

Cisco Cloud Control with AI Canvas

The unified operations platform for agentic IT



Meraki • ThousandEyes • Security Cloud Control • Splunk • Nexus Dashboard • Catalyst SD-WAN • Intersight • Webex • Cisco IQ • Catalyst Center

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

Cisco Cloud Control

Demo

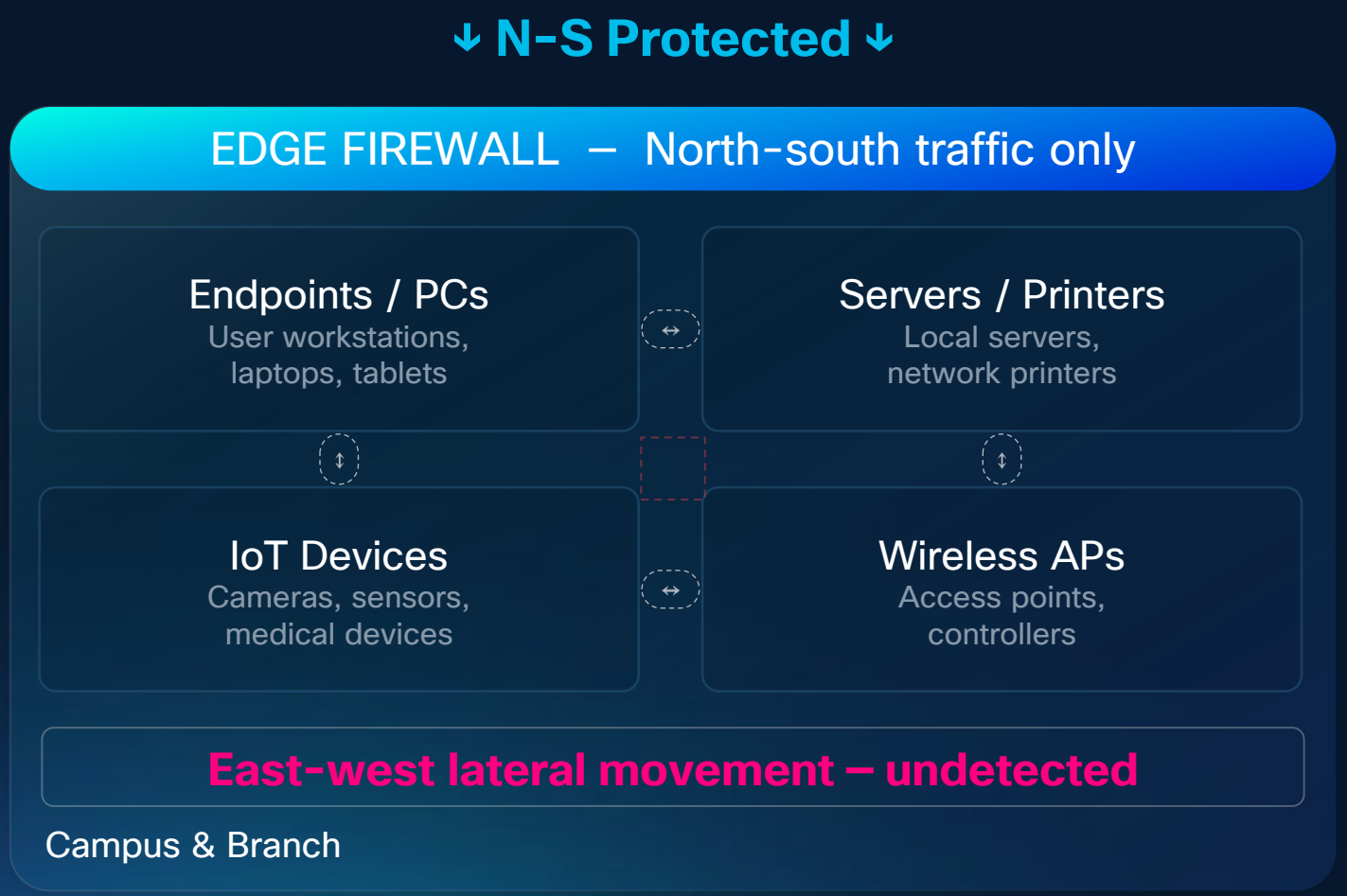
© 2026 Cisco and/or its affiliates. All rights reserved.

Security fused into the network



How security is deployed today

Edge firewall appliances only inspect traffic crossing the perimeter — not traffic moving laterally within your network



The problem: Edge firewalls are blind to internal traffic

Ransomware spreads endpoint-to-endpoint on campus — no micro-segmentation, no inline encryption, no identity-based access control

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

Why the network is the answer

Only the network has the position, visibility, and scale to deliver security everywhere

Sees all

Universal visibility

Every packet traverses the network — no agent or appliance matches this reach.

Line rate

Zero performance penalty

Security in silicon at wire speed. No hairpinning, no overhead.

One policy

Enforced consistently everywhere

One policy model, coordinated enforcement at every point.

The network is the only universal control point.
Fuse security into it, and every device is protected by default.

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

cisco

What security should be

Security must be fused into the network – not bolted on at the edge

Protect the infrastructure

Hardware-rooted trust with secure boot and runtime integrity verification

Addresses:
Salt Typhoon, BlackTech

Protect data in motion

Line-rate encryption campus to cloud with post-quantum readiness

Addresses:
Harvest Now Decrypt Later

Prevent lateral movement

Identity-based segmentation and inline firewall at the switch stop ransomware and AI-driven lateral movement

Addresses: AI-Driven Lateral Movement, E-W blind spot

Continuous verification

Every user and device continuously verified by identity and posture

Addresses:
Implicit trust exploitation

Distributed & Coordinated

Policy enforced at every network point – not a single edge appliance

Addresses:
Centralized bottleneck

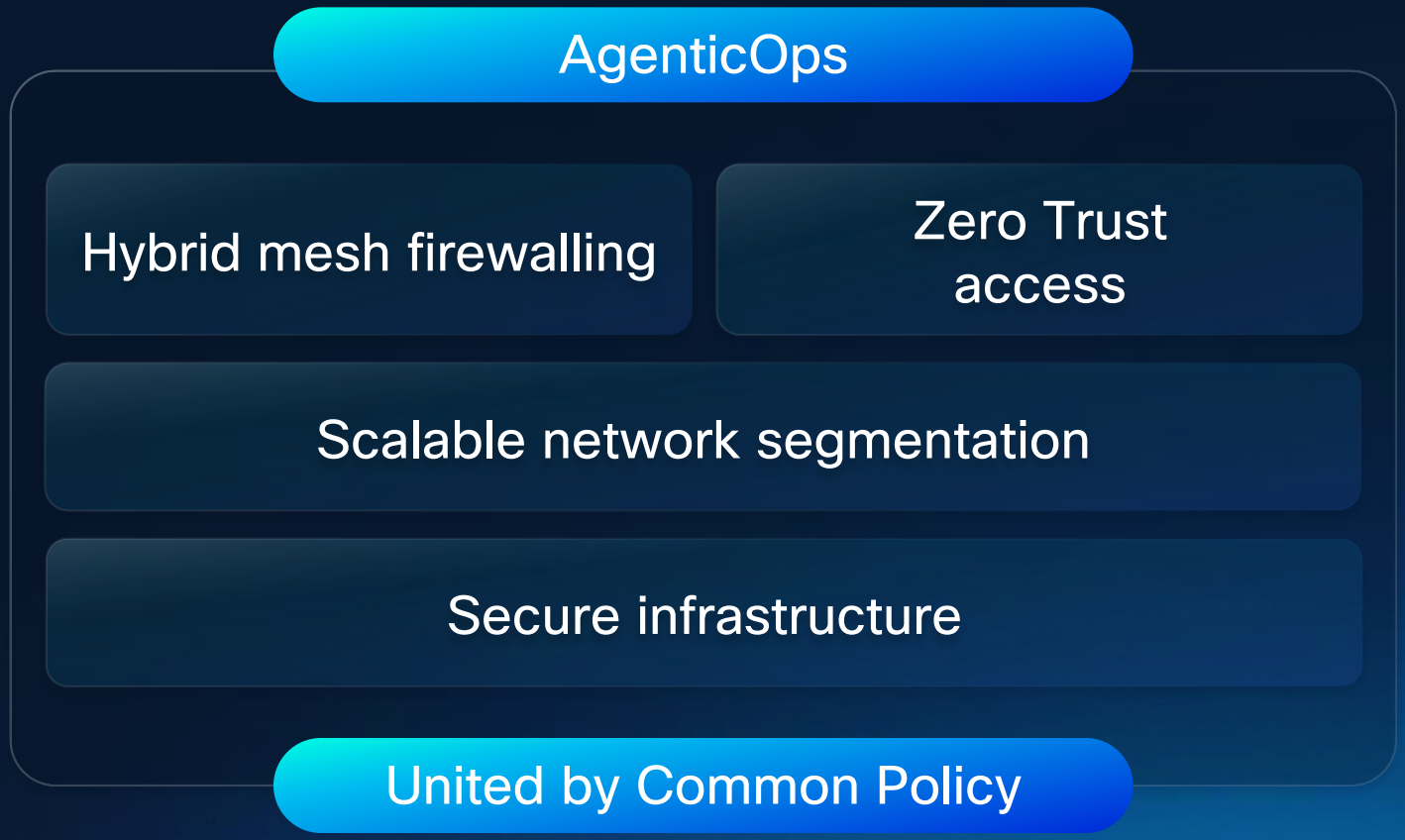
Centralized Management enhanced with AI to speed up detection, diagnosis and resolution

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

cisco

Reference design for fusing security into the network





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

Secure Infrastructure: Protecting data and connectivity

Encrypted Communications

Prevent snooping



The Switch
Secured

AES-256 - MACsec
IPSec
WAN MACsec

Data plane Security — Protects against ‘harvest now decrypt later’ attack

PQC signed IOS XE — Protects against forging & unauthenticated OS

PQC Compliant Secure Boot — Protects against boot-level tampering

Quantum Resistant and PQC Compliant Ready

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

Full Stack PQC

From Secure Boot to Secure Transport on Cisco 9000 Smart Switches



MACsec | IPsec | TLS | SSH

NIST-approved algorithms for Secure Transport

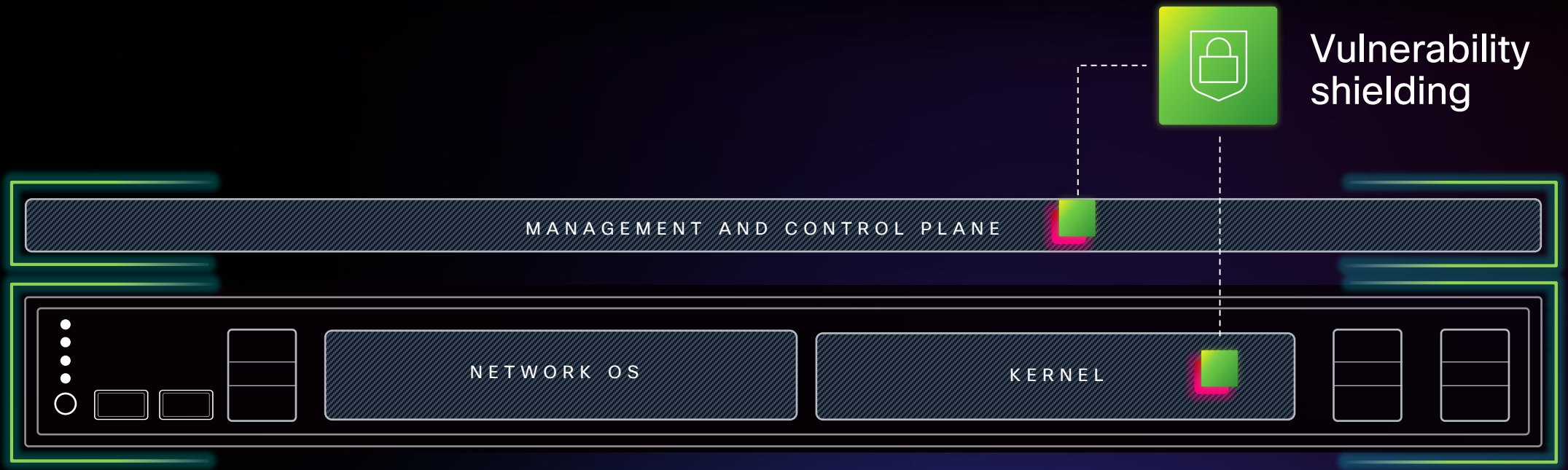
AES-GCM-256 LMS ML-DSA ML-KEM SHA-512

NIST-approved algorithms for Secure Boot

ROMMON | OS | Datapath between CPU and TAm

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

Live Protect: Threat protection without patch or reboot



EXTENDING ACROSS CISCO NETWORKING AND SECURITY

Apply policy to live system

Protect now, patch in planned window

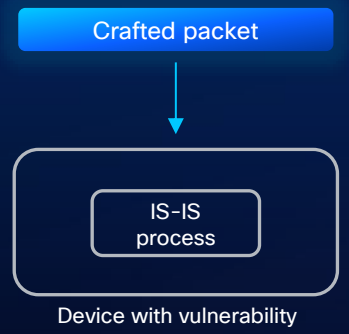
No downtime or switch reboot

Continuous re-validation

Blocking an IS-IS denial-of-service attack with a Live Protect Shield

Example: CVE-2025-20241

The attack



- Crafted packets reach vulnerable IS-IS parser
- IS-IS process may restart
- Device reload creates DoS condition

Live Protect



- Shield at vulnerable IS-IS function path
- Exploit condition blocked
- Normal IS-IS routing preserved

Operator benefit



- Avoid unplanned reloads / upgrades
- Preserve routing stability
- Patch through planned change control

Resilient Infrastructure with Cisco

Baseline security posture out-of-the-box



Increased default protections



Removed legacy insecure features



Advanced capabilities for better detection & response

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

cisco

Security by default



Out-of-the-box secure settings and proactive risk alerts

1] Deprecates insecure protocols with Insecure Feature Warnings

2\ Restrict the use of insecure protocols with Insecure Feature Restrictions ("Insecure Mode" available but discouraged)

Insecure Feature Warnings & Restrictions

Use buttons on right to toggle selections.

Search Feature / Protocol...

Insecure Feature Warnings | Insecure Feature Restrictions

Hide platform columns where every value is N/A

Viewing: Insecure Feature Warnings 20 / 20 rows Platform columns shown: 23 / 23

FEATURE / PROTOCOL	CATALYST CENTER	FW - ASA	IOS-XE	IOS-XR	ISE	MERAKI - CLOUD	MERAKI - CORE	MERAKI - MR	MERAKI - MS	MERAKI - MV	MERAKI - MX	NX-OS
BootP Server	N/A	N/A	17.18.2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
FTP	N/A	10.5/9.25	17.18.2	25.4.1	3.6	N/A	N/A	N/A	N/A	N/A	N/A	10.7.1
HTTP	N/A	N/A	17.18.2	25.4.1	3.6	N/A	N/A	N/A	N/A	N/A	N/A	10.7.1
IP Finger	N/A	N/A	17.18.2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
IP Source Routing	N/A	N/A	17.18.2	25.4.1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	10.7.1
MD5 for authentication and 3DES for encryption of SNMPv3 traffic	3.1.6	10.5/9.25	17.18.2	26.3.1	3.6	Q4 FY26	N/A	N/A	N/A	N/A	N/A	10.7.1
NTP Control Messages	N/A	N/A	26.1.1	N/A	N/A	TBD	N/A	N/A	TBD	N/A	N/A	N/A
On-Demand Routing	N/A	N/A	17.18.2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Plain-text and weak credentials	3.1.6, N/A	N/A	17.18.2, N/A	26.3.1, N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	10.7.1,
RADUIS using pre-shared keys and MD5	3.1.6	11.0	17.18.2	25.4.1	3.6p1	Q2 FY27	N/A	N/A	Q1 CY27	N/A	27.1	10.7.1
SNMPv1 / SMNPv2c	3.1.6	10.5/9.25	17.18.2	26.3.1	3.6	Q4 FY26	N/A	N/A	N/A	N/A	N/A	10.7.1
SNMPv3 without authentication	3.1.6	10.5/9.25	17.18.2	25.4.1	3.6	Q4 FY26	N/A	N/A	N/A	N/A	N/A	10.7.1

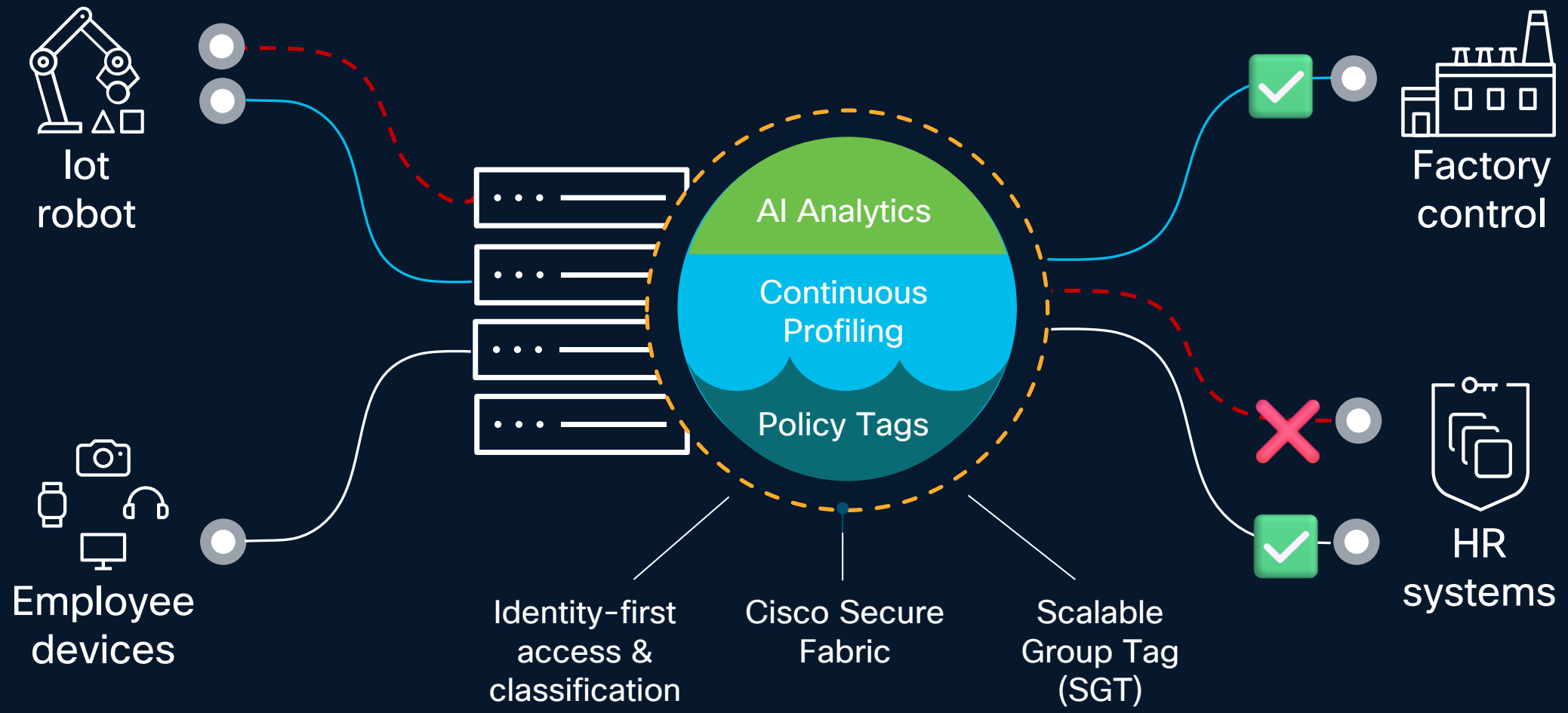
https://www.cisco.com/c/en/us/about/trust-center/resilient-infrastructure/feature-deprecation-and-removal-details.html#~insecure-feature-warnings

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

cisco

Scalable network segmentation

Continuously verified identity and group policy applied across the network



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

Scalable devices ready for AI



Introducing

Scalable devices ready for AI



Smart Switches



Secure Routers



Campus Gateway



Secure Firewall



Large Venue Wi-Fi 7

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

cisco

Cisco C9350 Smart Switches

- High-performance, low latency
- Post-quantum secure
- Cisco Silicon One + co-processor for security and AI
- Intelligent energy efficiency

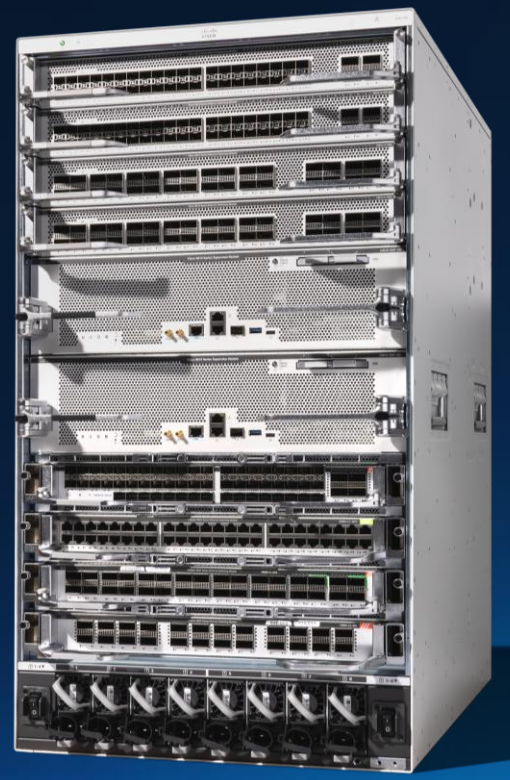


Smart Switches for the AI-powered campus

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

Cisco C9610 Modular Core Smart Switches

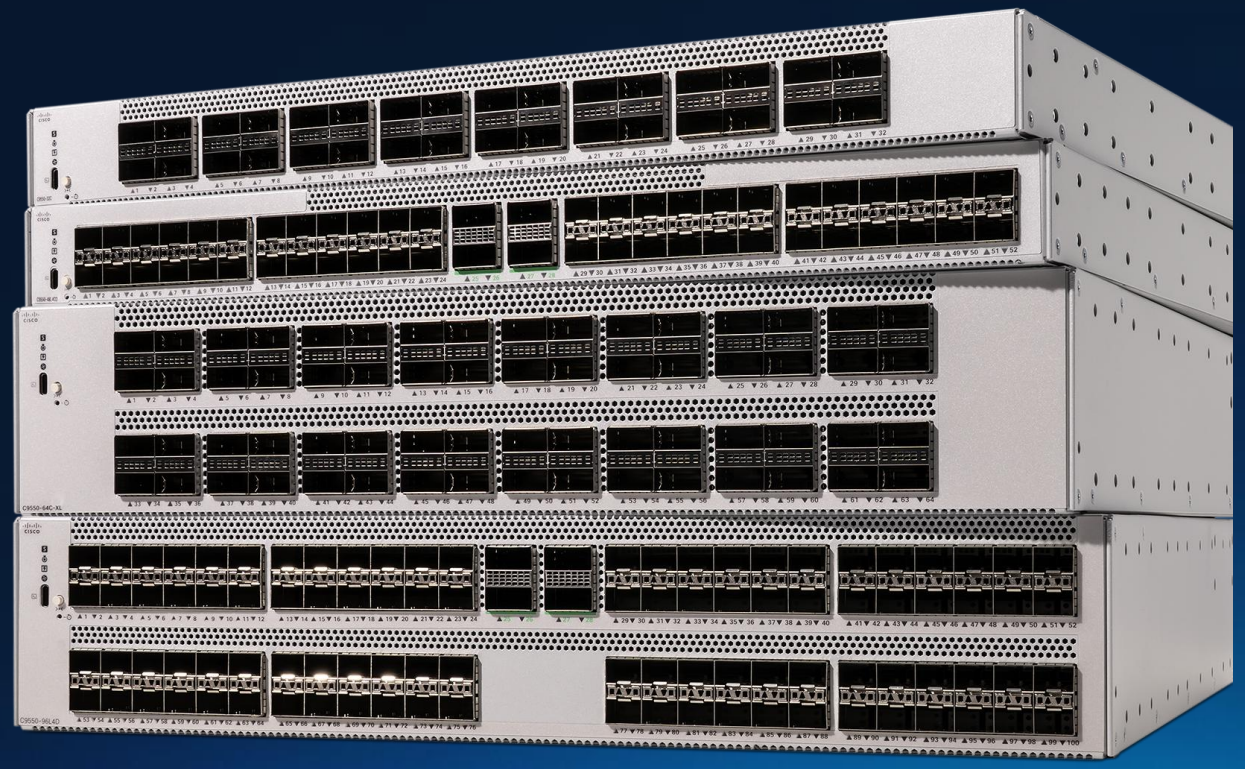
- Unparalleled density, speed, and security
- High density chassis with state-of-the-art hardware
- Backward compatible chassis with front to back airflow
- Entirely modular and upgradable system
- Powered by Cisco Silicon One



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

Cisco C9550 Fixed Core Smart Switches. Built for AI Scale.

- 400G Campus Core
- Up to 6.4 Tbps switching capacity
- 3.9B packets/second
- Quantum safe



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

Cisco 8000 Series Secure Routers + Firewall for Campus and Data Center

Campus



8400 Secure Router



Firewall 3100 Series

Data Center



8500 Secure Router



Firewall 4200 Series



Firewall 6100 Series

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

cisco

Powered by

Silicon One A100L & Silicon One K100L

- Boosts hardware encryption post quantum security
- High-scale and low latency for time-sensitive applications
- Flexible and programmable for future AI and ML workloads
- Efficient power performance
- Intelligently adaptable to mitigate link failures, congestion, and bandwidth challenges



Cisco Silicon One for Scale, Security, and Efficiency

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

cisco



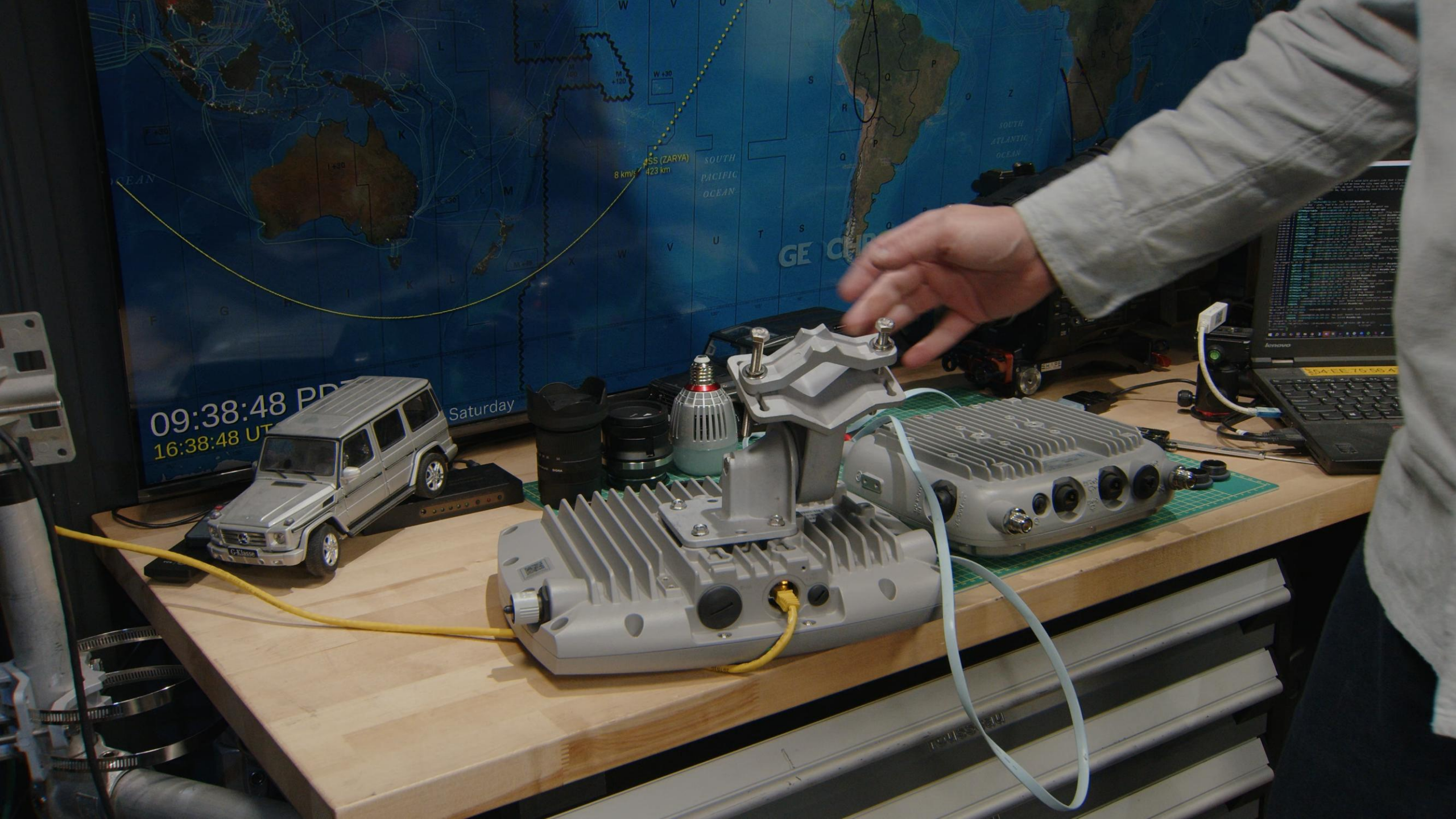
- Lila - wireless guy - what's the deal with w

Wi-Fi 7 for the Modern Campus

Coffee shops	Residence halls	Classrooms	Lecture **halls, libraries**	Outdoor	Auditoriums	Stadiums, large **venues**
						
CW9171I	**CW9172I/H**	**CW9174I/E**	**CW9176I/D1**	**CW9177I/D/E**	**CW9178**	**CW9179F**
Lower density deployments, compact form factor	Moderate-density deployments, wall plate	Moderate to high-density deployments	High-performance, omni & directional antenna options, URWB	High-end outdoor, 3 variants for optimal coverage, URWB	Ultra-high performance, high-density deployments, URWB	High-density, large venues, configurable beam patterns
Available	Available	Available	Available	Coming soon	Available	Available

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

cisco


SOUTH
PACIFIC
OCEAN
SOUTH
ATLANTIC
OCEAN
Saturday

Cisco Campus Gateway

follows IOS-XE based CW9800L/M/H variants

Scales up to 5,000 APs and 50,000 clients

Easy migration for existing LAN controller architectures

No need to re-cable, change VLANs, or disrupt operations



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

Stay tuned for the next session...

Cisco brings its IT expertise to rugged environments.

Unified management



IOS XE Operating System

Enterprise Grade
Best of IT innovations

+

Industrial Strength
Purpose built for harsh environments

Standardized equipment | Centralized management | Enterprise-wide security
High-performance networking | One licensing model

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

cisco

Thank you




CISCO