

AI-Powered Wireless Connectivity

HK Cisco Connect

Avinash Salian- Wireless Sales Lead (APJC)



Investment momentum in wireless is accelerating



8 in 10 organizations have
increased wireless investments
in the past 4-5 years

1 in 3

Expect wireless budget
increases of 50%+
over the next five years

But four barriers converge to block return on investment in 2026

Only 19% of organizations are operating Wi-Fi 6E or 7



Say operational complexity is increasing
Report visibility gaps when troubleshooting
Believe AI-driven automation will simplify operations

Operational complexity beyond human scale

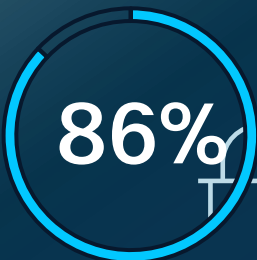
Claude Mythos to identify thousands of zero-day vulnerabilities

- Mythos Preview found a 27-year-old vulnerability in OpenBSD
- It also discovered a 16-year-old vulnerability in Ffmpeg



The Quantum Threat: "Harvest Now, Decrypt Later"

Intensifying wireless security threats



The growing talent gap is more than an HR issue

86% of organizations struggle to fill wireless roles

Growing talent gaps

AI is the #1 driver for each operational barrier

#1

Driver of operational complexity:
AI workloads

#2 Security risks

#3 Bandwidth demand
and unpredictability

#1

Security threat:
AI generated attacks

#2 Unmanaged devices

#3 Increased usage of IoT

#1

Recruitment challenge:
AI skills

#2 Internal budget constraints

#3 Geographic limitations
and remote work demand

Inversely, AI is empowering IT teams with



Significant time
savings



Fewer
wireless tickets



Faster wireless
ticket resolution

This is the wireless AI paradox:

AI is both the **primary source of escalating challenges** and, the **leading driver for wireless ROI and simplicity.**

Overcoming these barriers **simultaneously** resolves the paradox and unlocks ROI

Refresh legacy infrastructure



Simplify Operations



Mitigate wireless security threats



Address talent gaps

Architecture for the AI-Ready secure network

Simplified operations
powered by AgenticOps



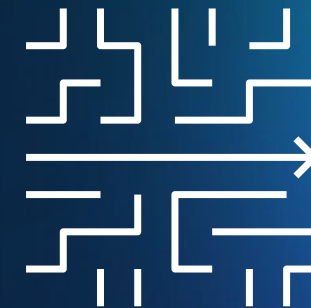
Security
fused into the network



Scalable devices
ready for AI



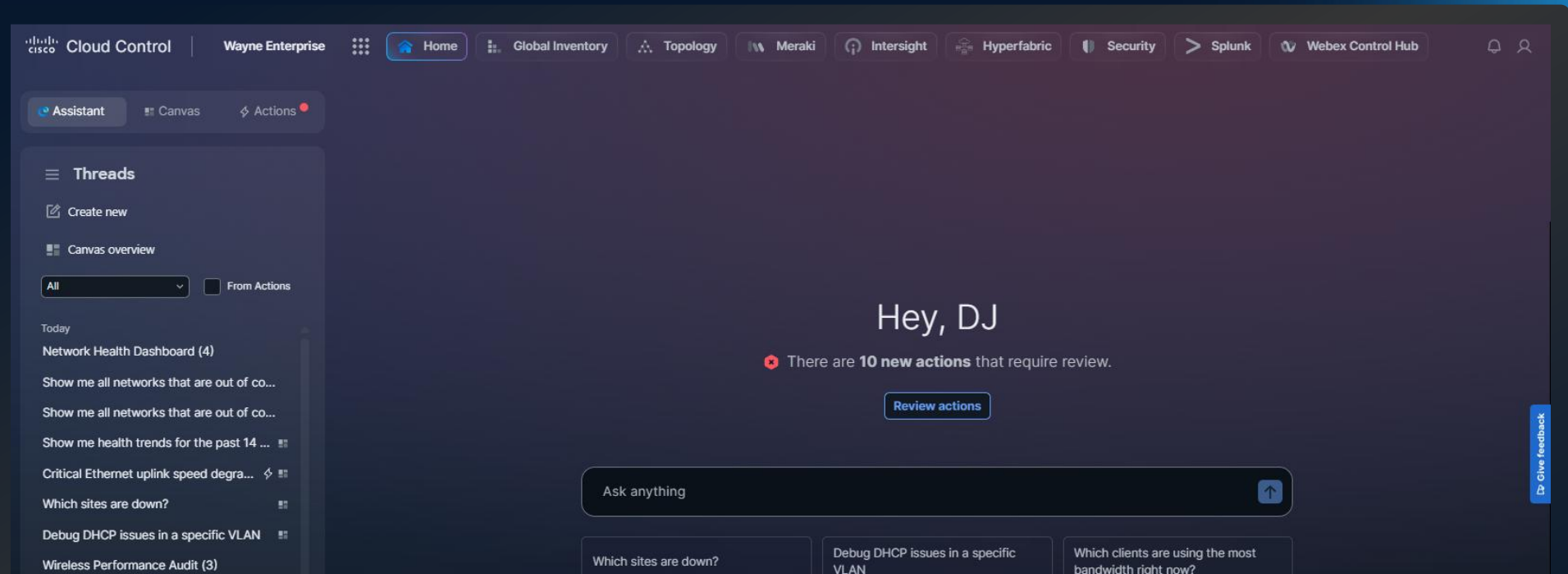
Simplified operations powered by AgenticOps



Cisco Cloud Control

One platform. Every domain. The foundation everything else is built on.

Meraki · ThousandEyes · Security Cloud Control · Splunk · Nexus Dashboard · Catalyst SD-WAN · Intersight · Webex · IQ · & more



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

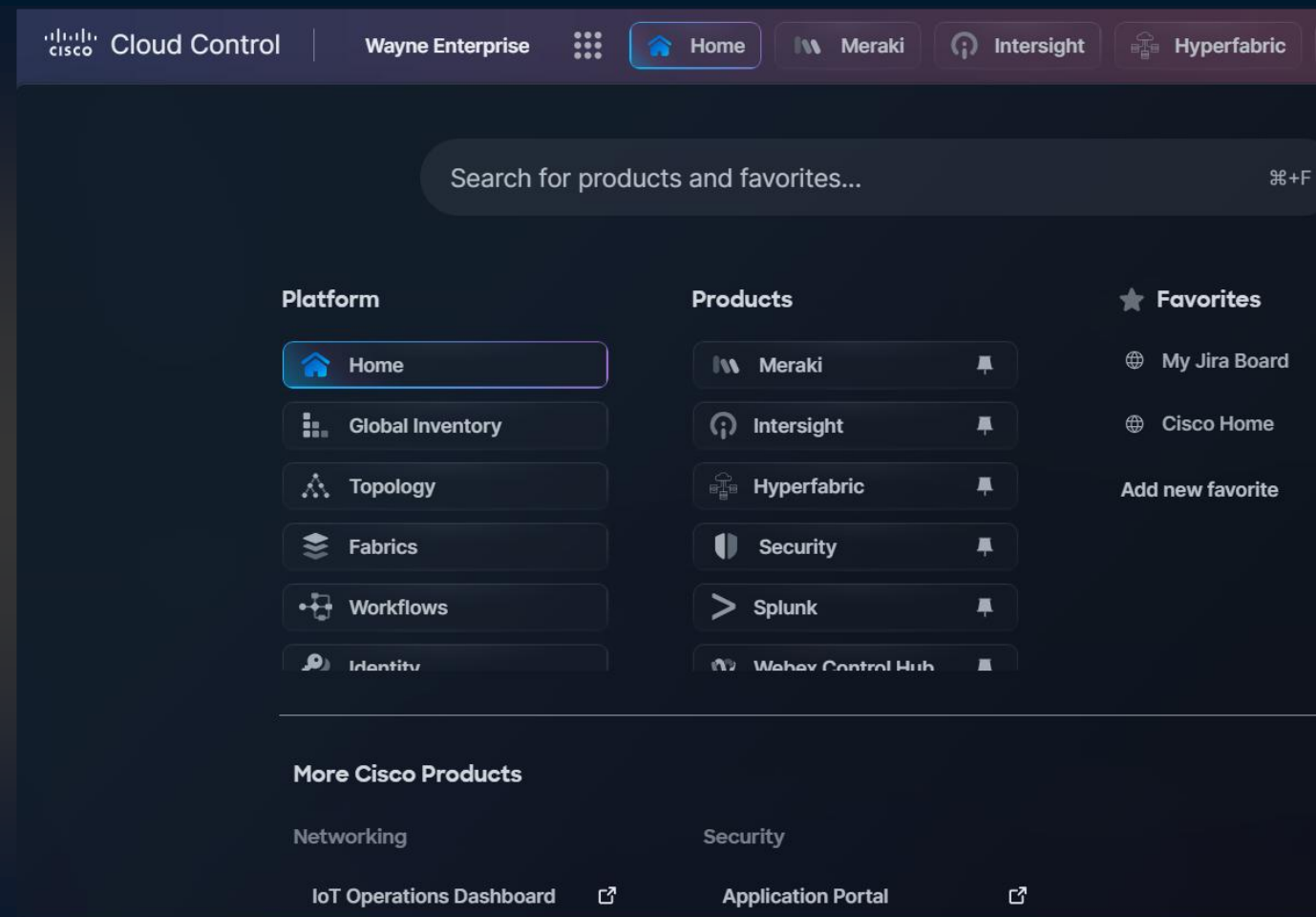
Actions correlates alerts across every product.

One assistant

Quick answers and tasks with AI Assistant.

One agentic workspace

Investigate, execute and resolve with AI Canvas.



Simple, Unified Management Platform

Platform

Management

Assurance

API

AgenticOps

Hardware



Smart
Switches



Secure
Routers

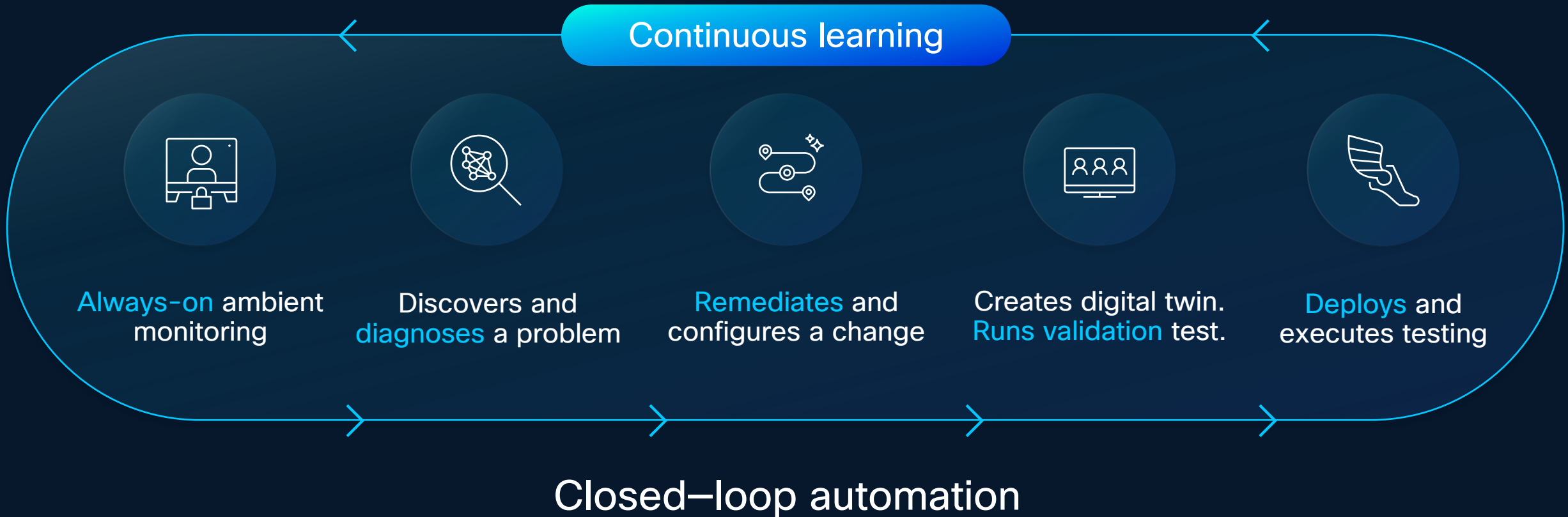


Scalable
Wireless



Industrial
IoT

AgenticOps



AgenticOps capabilities for to simplify networking

CCIE-level expertise across your network 24/7

Autonomous Troubleshooting

Delivers credible root
cause and remediation.
In minutes.

Continuous Optimization

Keeps the network
in its best state.
Automatically.

Trusted Validation

Makes every
change safer.
Predictably.

Powered by deep reasoning and deterministic execution

AgenticOps capabilities for to simplify networking

CCIE-level expertise across your network 24/7

Autonomous Troubleshooting

Delivers credible root cause and remediation.
In minutes.

Experience Metrics (XM)

Embedded ThousandEyes Agents

Site Analytics

Assurance Health

Wi-Fi Readiness Dashboard

AI PCAP Analyzer

Continuous Optimization

Keeps the network in its best state.
Automatically.

AI-RRM

AI Config Recommendation

AI Based Baseline Dashboard

Trusted Validation

Makes every change safer.
Predictably.

Synthetic ActiveTesting

Experience Metrics

Don't let users suffer in silence

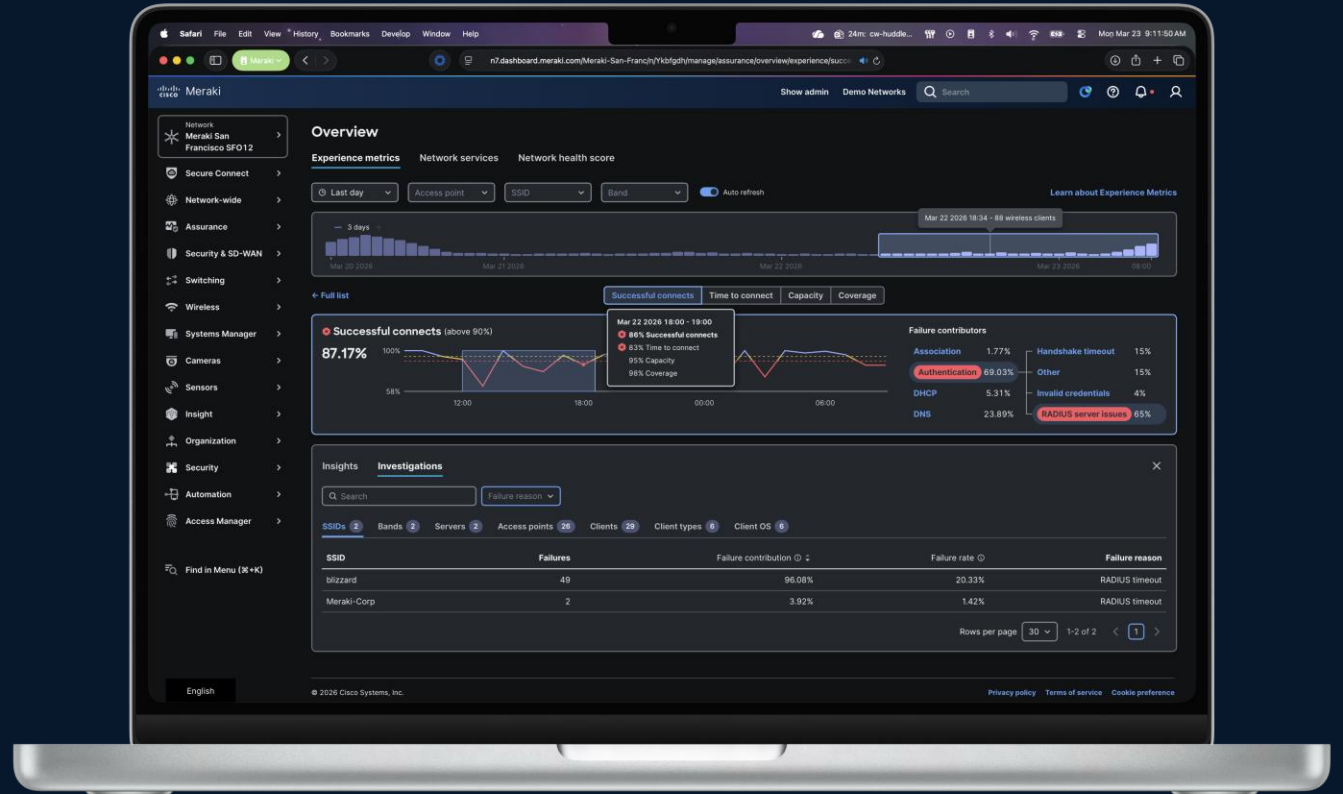
Continuously track and analyze user experience in real-time.

Symptom to RCA in a single workflow

Link experience degradation to service health, infrastructure status, and client-specific anomalies.

Key Experience Metrics

Monitor essential metrics such as Time to Connect, Successful Connects, Channel Availability, and Coverage.



Synthetic Testing

Proactively assure readiness

Validate infrastructure performance with scheduled synthetic tests, catching issues

Accelerate issue resolution

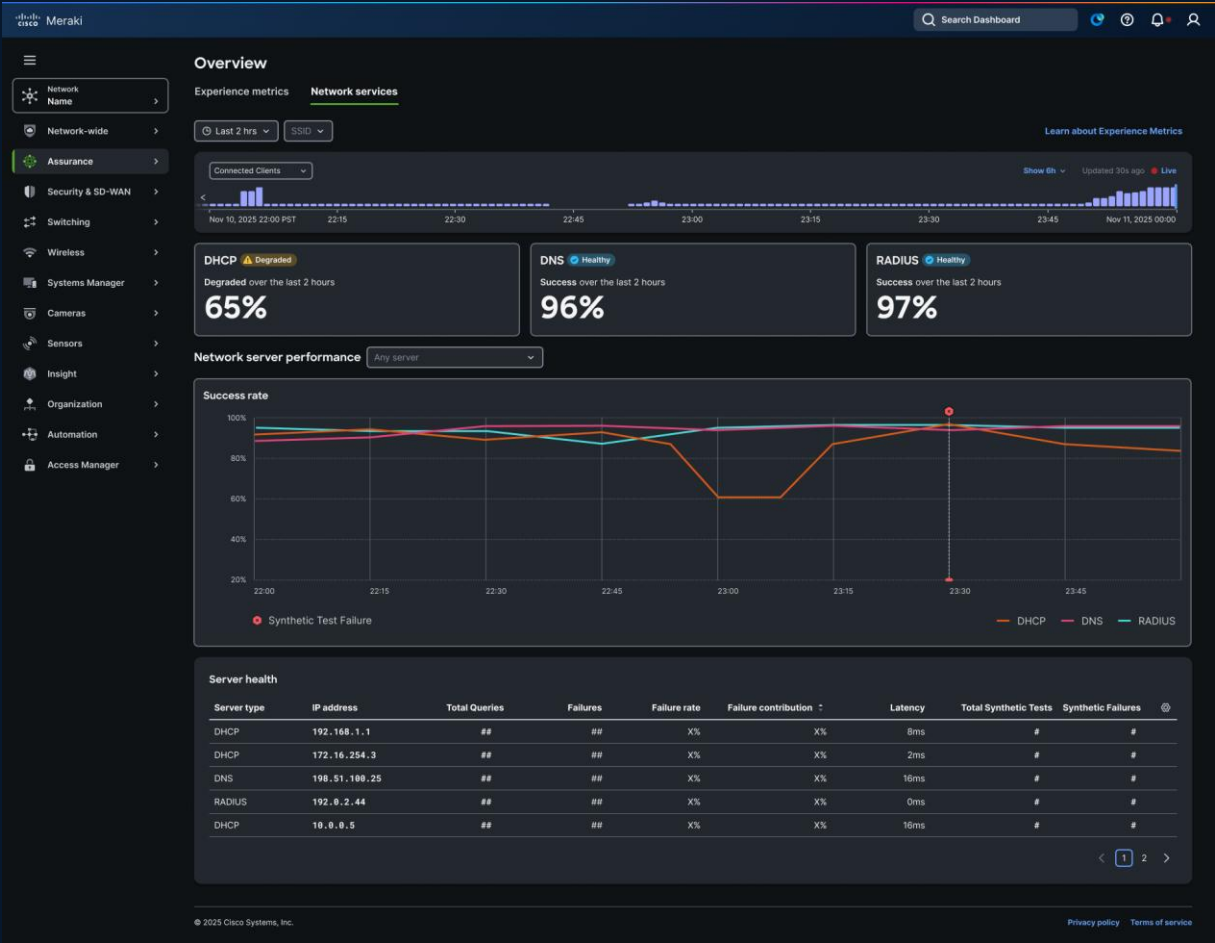
Reduce MTTR by quickly identifying issues, understanding root causes, and resolving them faster

End-to-end visibility

Track application performance from AP to cloud, monitor unmanaged devices, and run natively



Synthetic Testing



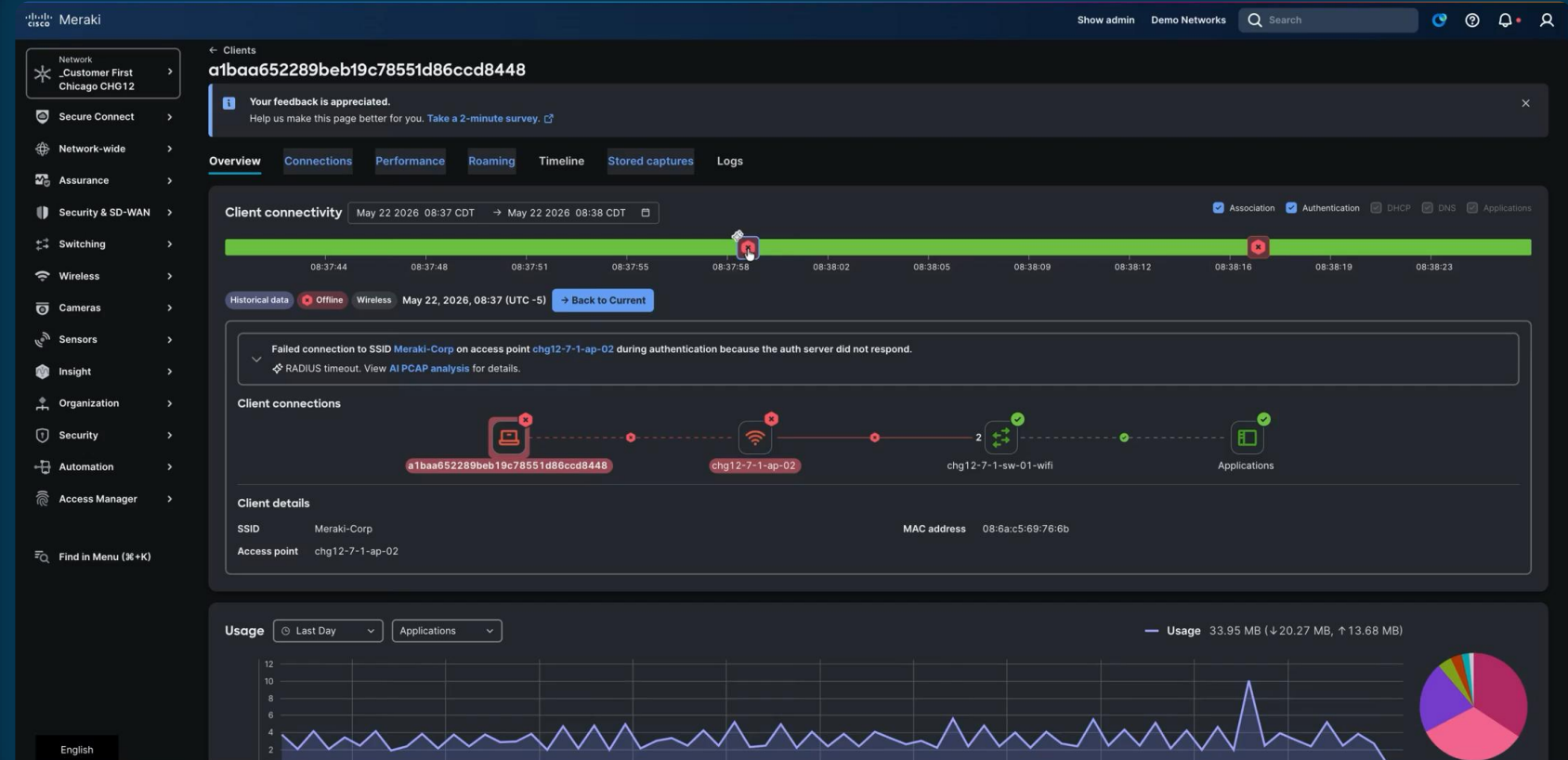
AI PCAP Analyzer

Autonomous Troubleshooting

Reducing troubleshooting
times from weeks to seconds

AI Summary

Reasoning



Packet Capture

AI Highlighter

Remediation suggestion

AI Configuration Recommendations



AI network optimization

- Assesses readiness – network and client
- Predicts before-and-after performance improvements
- Suggests better configuration recommendations for performance and security improvements



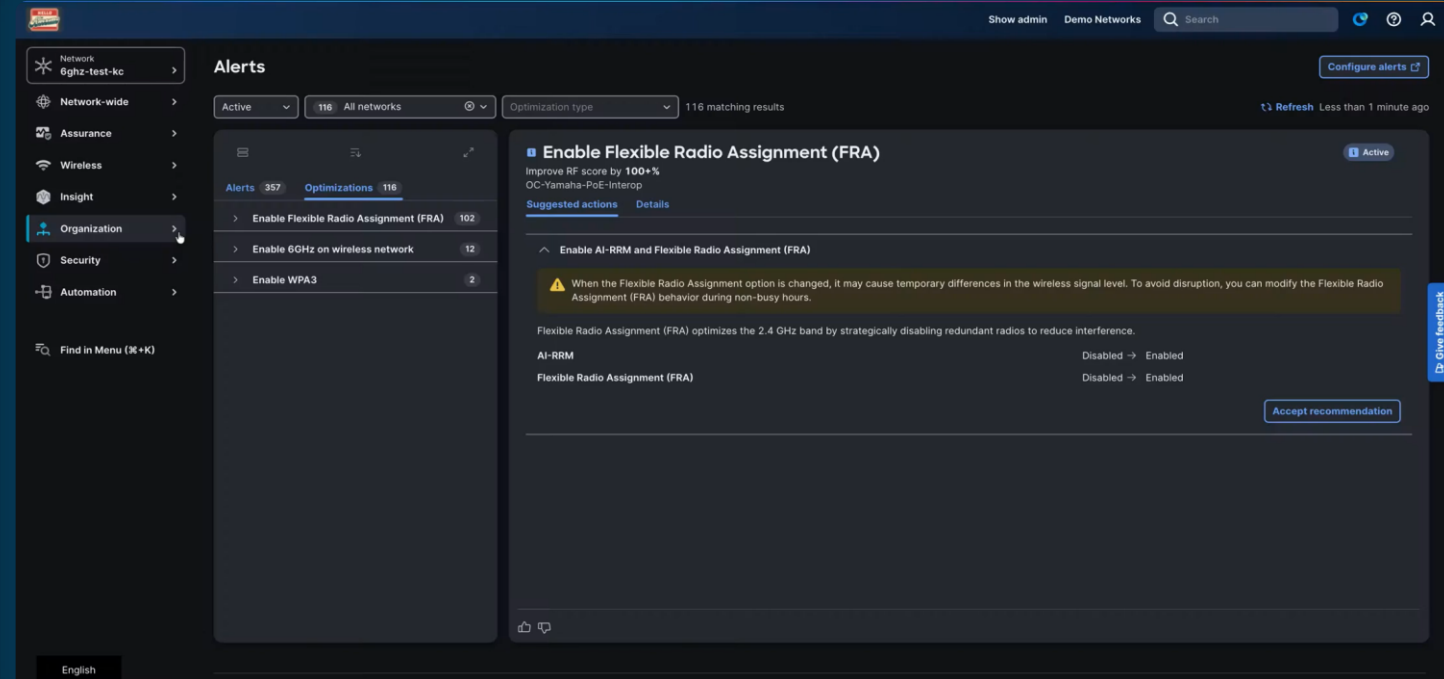
Types of recommendations

Available

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

Impact

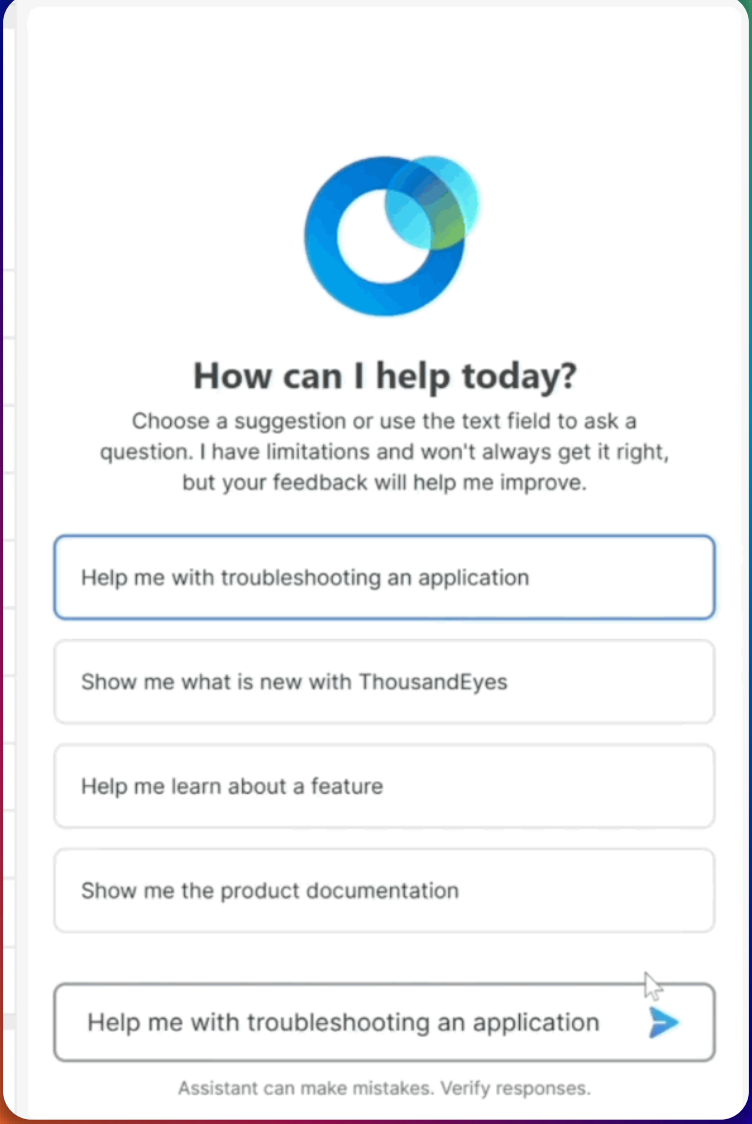
- Improved security
- Faster data rates
- Faster roaming
- Reduce co-channel interference



Expedite troubleshooting and remediation with AI Assistant

Native, GenAI-based Agentic Network Interface

- Understand Wireless, Wired, WAN and Internet networking experience
- Understand unique network contexts such as Network Telemetry, Configuration, Firmware
- Answers dynamic network inquiries and answers
- Dynamic query parameter derivations and composite



The image shows a mockup of the AI Assistant interface. At the top is a logo consisting of two overlapping circles, one blue and one green. Below the logo is the heading "How can I help today?" followed by a paragraph: "Choose a suggestion or use the text field to ask a question. I have limitations and won't always get it right, but your feedback will help me improve." There are five buttons with the following text: "Help me with troubleshooting an application", "Show me what is new with ThousandEyes", "Help me learn about a feature", "Show me the product documentation", and "Help me with troubleshooting an application". A mouse cursor is pointing at the bottom button. At the bottom of the interface, there is a small disclaimer: "Assistant can make mistakes. Verify responses."

How can I help today?
Choose a suggestion or use the text field to ask a question. I have limitations and won't always get it right, but your feedback will help me improve.

Help me with troubleshooting an application

Show me what is new with ThousandEyes

Help me learn about a feature

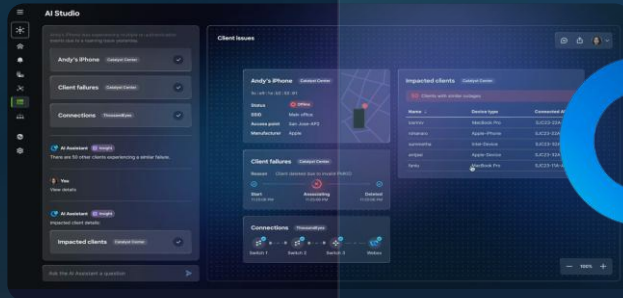
Show me the product documentation

Help me with troubleshooting an application

Assistant can make mistakes. Verify responses.

In Future

Cisco AgenticOps



cisco
AI Assistant

AI Canvas

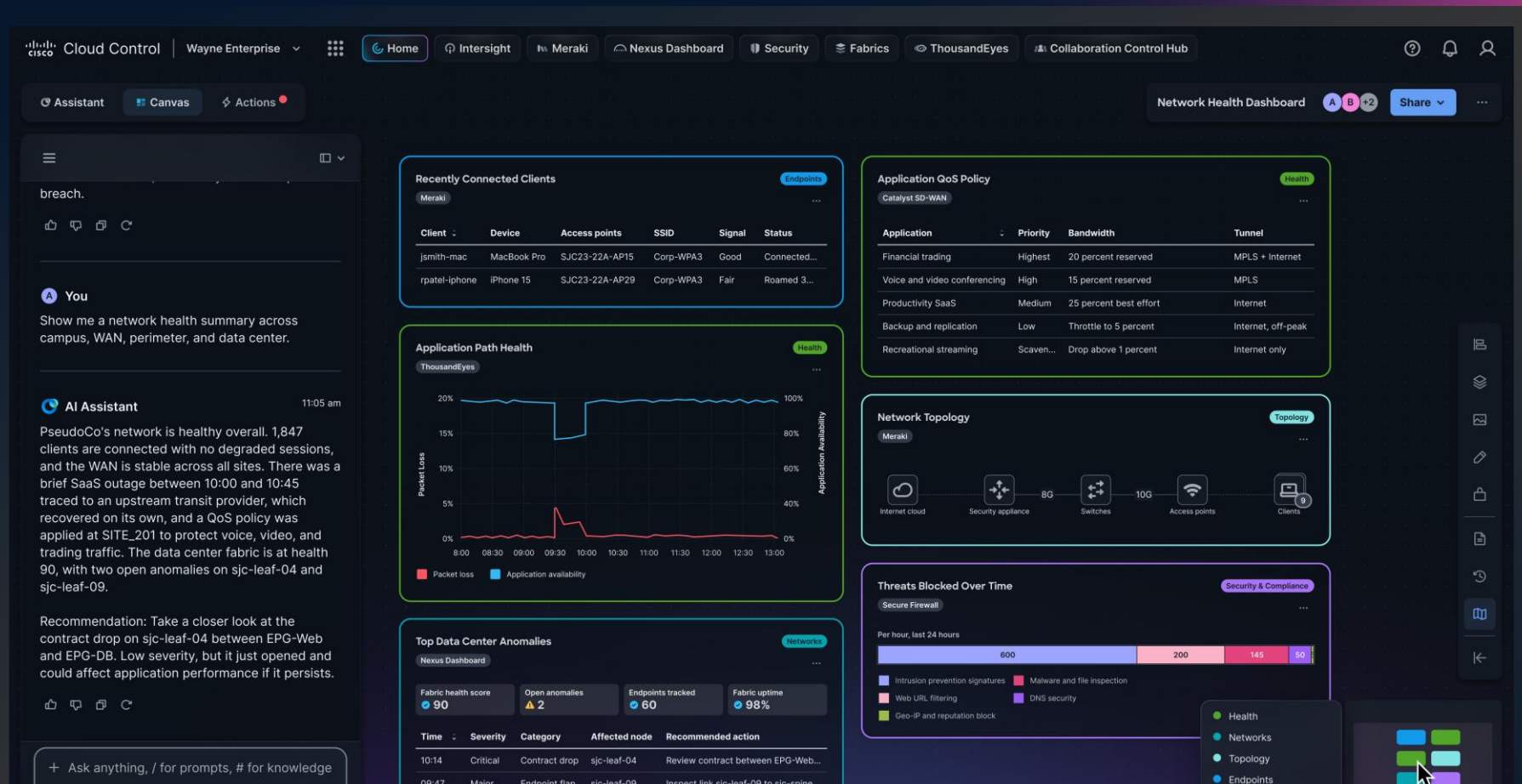
AI Assistant

Cross-domain collaborative troubleshooting Accelerate network operations

POWERED BY DEEP NETWORK MODEL

Cisco AI Canvas

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



Security fused into the network



Secure Networking Architecture

Advanced security at every layer

- Identity-first
- Continuously verified
- Enterprise-wide policies
- Comprehensive threat intel
- Distributed enforcement



Make networks more secure with less OPEX

Delivering scalable segmentation, secure infrastructure, and common policy

Network focus steps



Secure AP onboarding

Automating MACsec



Secure AP infrastructure

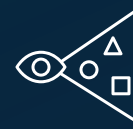
Resilient infrastructure & PQC

Endpoint focus steps



Secure Endpoint onboarding

Access Manager & ISE



Endpoint profiling and telemetry

Consistent, highly accurate profiling across the platform



Policy identification and enforcement

Scalable Segmentation with TrustSec Security Group Tags

MACsec Support

Challenge:

Unencrypted wired link between the access point and switch is prone to eavesdropping, intrusion, and man-in-the-middle attacks

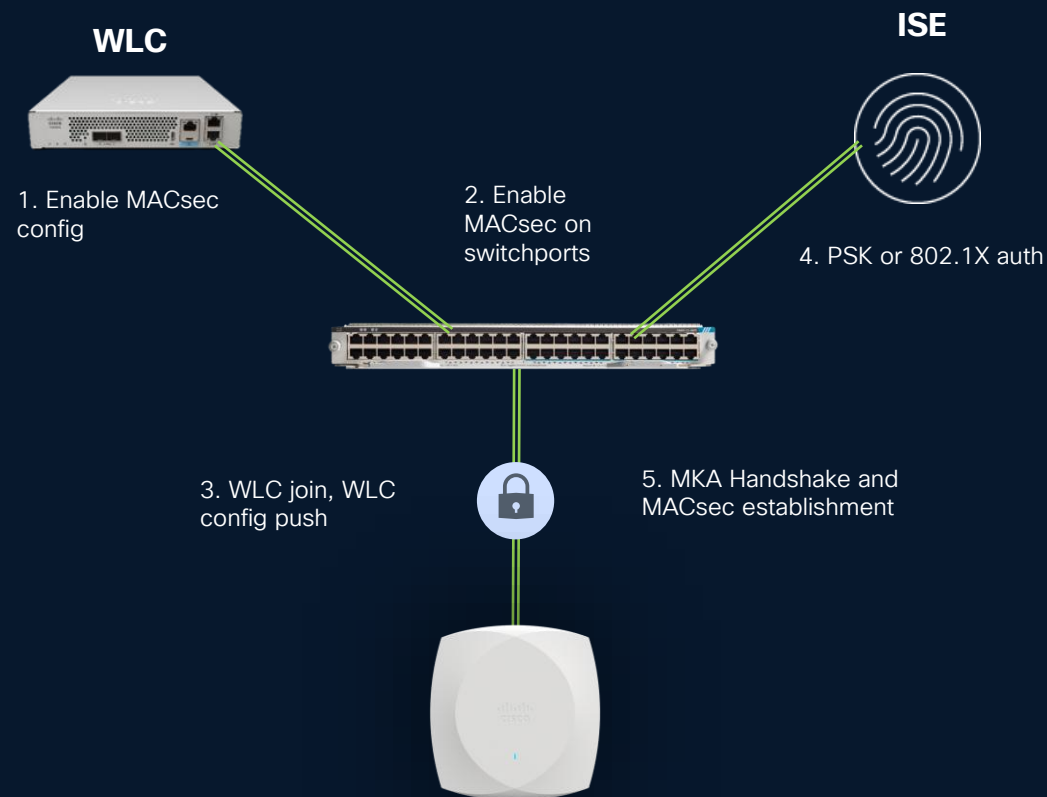
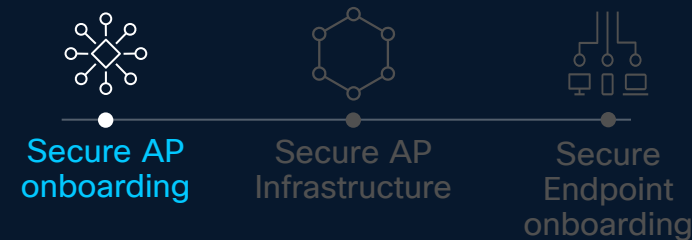
Product Capability:

- MACsec config push from WLC upon AP join
- 802.1X or PSK for AP authentication
- L2 encryption on the wire (AP <-> SWITCH)

Customer Benefit:

Zero-trust networking, passwordless authentication, and hardware-rooted identity for APs.

Encrypting the AP uplink helps provide added protection against threats while addressing confidentiality and integrity

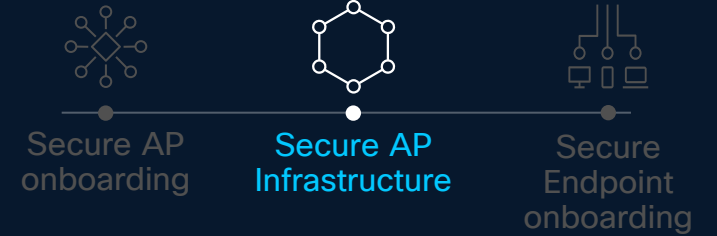


IOS-XE 26.1.1
IBN SDA / non-SDA
3.2.x

Supported On-Prem APs:
W7: CW9174I/E | CW9176I/D1 | CW9178I | CW9179F
W6E: CW9164 | CW9166I/D1 | C9136
W6: C9130AXI/AXE | C9124AXE/AXD (Copper Port)

Cisco Resilient Infrastructure

Bolster security of network configurations effortlessly



**Protect by
warnings**

AVAILABLE NOW

**Protect by
default**

AVAILABLE SOON

**Protect by
deprecation**

NEXT PHASE

Cisco.com/go/ri

Building Quantum resistant wireless networks

CNSA 2.0 (US Public Sector)
Regional Mandates



Public-key

Symmetric-key

Software and
Firmware Updates

010110
110010
001011

Encryption

Generate the encryption key for
secure communication



Authentication

Verify the authenticity of the
communicating devices / users



Secure Boot

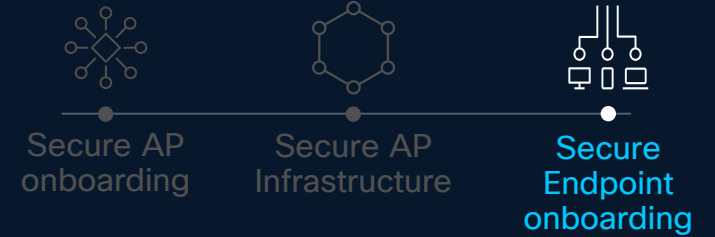
Ensure authenticity and integrity
of software and hardware

Secure
Communication

Secure Product

Cisco Access Manager

Instantly **enforce existing authorization methods** without extra hardware or consoles



The screenshot shows the 'Wireless > Access Control' page in the Meraki Dashboard. It features four radio button options for authentication methods. The first option is 'MAC-based access control (no encryption)', with a dropdown menu set to 'Access Manager' and a note 'RADIUS server is queried at association time'. The second option is 'Enterprise with', also with a dropdown set to 'Access Manager' and a note 'User credentials are validated with 802.1X at association time'. The third option is 'Identity PSK with RADIUS', with a dropdown set to 'Access Manager' and a note 'RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address'. The fourth option is 'Identity PSK without RADIUS', with a note 'Devices are assigned a group policy based on its passphrase'. The 'Access Manager' dropdowns are highlighted with red boxes.

Wireless > Access Control

page on Meraki Dashboard



Certificate-based

EAP-TLS with
Entra ID user lookup



Username and password

EAP-TTLS/PAP with
Entra ID user lookup



MAC authentication bypass

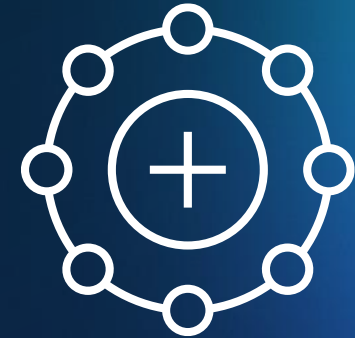
Apply authorization based
on user group or
attribute membership



Identity pre-shared key

Apply pre-defined policies
based on unique pre-shared
keys to endpoints

Scalable devices ready for AI



Industry-leading wireless portfolio

Outcomes enabled by wireless

Indoor location and wayfinding

Multi-sensor connect

Ultra-reliable wireless backhaul

Occupancy

API and ecosystem

Coffee shops	Residence halls, retail	Classrooms, carpeted spaces	Lecture halls, libraries	Outdoor	Campus with Location	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	NEW	AVAILABLE	AVAILABLE

Introducing the CW9177 Series

Tri-band 4x4, 12ss
2/5/6 or 2/5/5

Compatible with both Catalyst
and Meraki mounts where
possible

AFC support for 6 GHz
outdoor in US, CA at Launch



Cisco URWB and Mesh
Support – now on Wi-Fi 7
HW

SFP+ port for fiber to the AP

Unified Licensing & Global
Use AP – both WLC and
Meraki

Wi-Fi 6E and 7 - Outdoor/Ruggedized Portfolio

Extension of enterprise



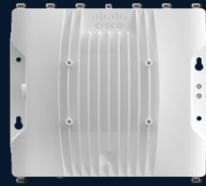
CW9163E - Wi-Fi 6E
"E" SKU

Shipping

Industrially rugged
& HazLoc



IW9165E



IW9167E
IW9167E-HZ

IW916x - Wi-Fi 6E

Shipping

Performance/
complex deployments



High-end outdoor 7
I,D,E SKUs

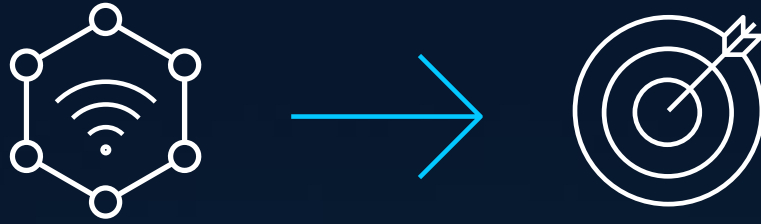
New

Stadium/
Convention centers



CW9179F
Specialized outdoor 7

Shipping



**From wireless infrastructure to business
outcomes, delivered together**

It's more than just an Access Point



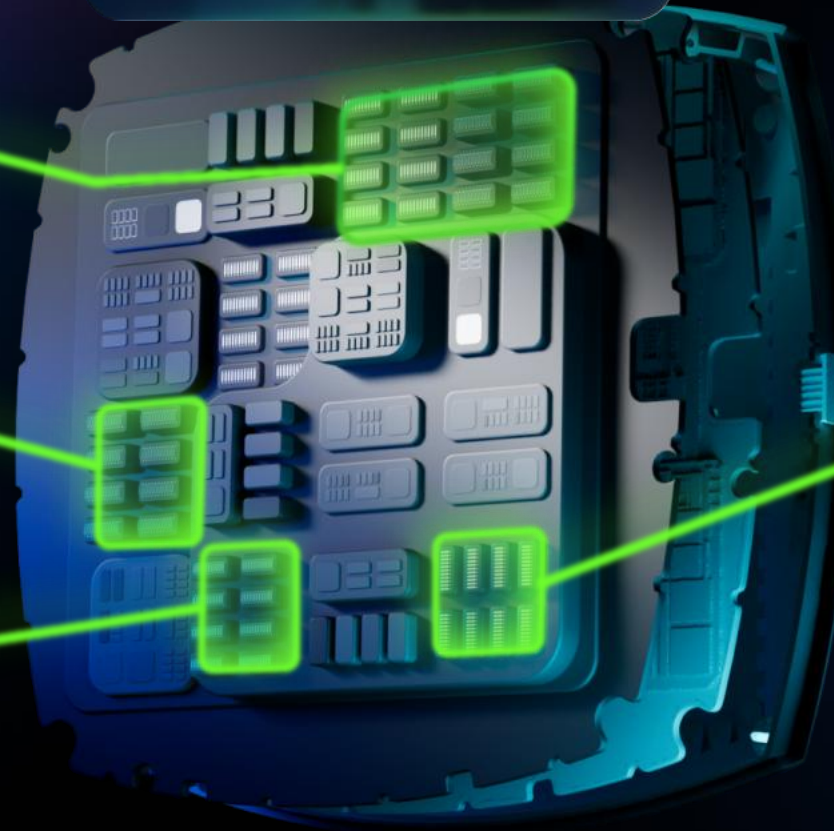
WiFi - 7

ACCESS POINTS

Quad-Radio WiFi
for unfettered connectivity

BLE 6.0 Radios
connect and manage a high
density of sensors

UWB & GPS Radios
for next-level location accuracy



Spaces Multivendor Gateway
Supports multiple participating 3rd party IoT
devices simultaneously

Bi-directional streaming data
Manage devices from Spaces Cloud and receive
sensor telemetry at scale

24/7 monitoring for use cases
Proactive monitoring for APs, WLCs, and other on-
prem infrastructure.

Spaces-led use case testing
Ensuring APs meet technical requirements for
mission critical use cases



Can also be the network for Smart Spaces

CAMPUS | BUILDINGS | FLOORS | ROOMS | DESKS



Cisco Wireless



Cisco Switches



Room Bars & Room Kits



Meeting Boards &
Integrated Room Systems



Desk & Phone Series



Seamless
Connectivity



Indoor
Navigation



Asset
Tracking



Occupancy
Analytics



Sustainability



Staff
Duress



Omni-channel
Experiences

Recap

01

Wireless is becoming a strategic platform for the AI era

Investment is accelerating, but ROI is constrained by legacy infrastructure, operational complexity, security threats, and talent gaps.

02

Organizations that address these barriers together unlock stronger ROI

- Accelerate Wi-Fi modernization
- Adopt AI-driven operations
- Modernize security holistically
- Invest in wireless talent

03

Cisco helps organizations implement this with an AI-ready secure network

- Simplified operations powered by AgenticOps
- Security fused into the network
- Scalable infrastructure ready for AI

