

Agents of Change: Optimizing Every Workplace with Agentic Ops



March 24, 2026



Colin Raymond

Cisco Networking Platform
Public Sector Product Leader

Global Operations Are Hard to Scale

86%

of IT organizations
struggle with a skills
shortage

\$1M+

cost in hourly
downtime

13%

of IT organizations
are AI-ready

Another Massive Technology Disruption

Internet

Mobility

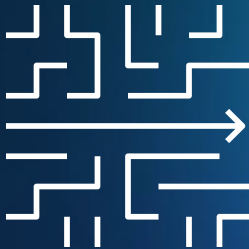
Cloud

AI

The background is a dark, futuristic cityscape at night, with numerous skyscrapers and buildings illuminated with various colors. Overlaid on this are many vertical, glowing lines in shades of blue, purple, and pink, extending from the bottom of the frame towards the top. A large, rounded rectangular shape with a blue-to-cyan gradient is centered in the upper half of the image, containing white text.

**A network
purpose built for AI
is required**

Simplified Operations Powered by AgenticOps



Industry's Most Trusted Platform

Unmatched real-world intelligence for smarter AI insights, proven reliability, and faster problem solving

40M

Managed devices

+8M devices YoY

8M+

Switches

1B+

Connected clients

27M+

Access points

7B+

Tests per day (ThousandEyes)

2M+

Routers

5T+

Datapoints per day

Unified Management to Simplify Operations

PLATFORM

Management

API / Integrations

Assurance

Intelligence - AgenticOps

HARDWARE



Smart
Switches



Secure
Routers



Wireless



Industrial
IoT

Journey to Network Platform Convergence

Cloud Platform

Hardware
and license
convergence

Common User
Experience

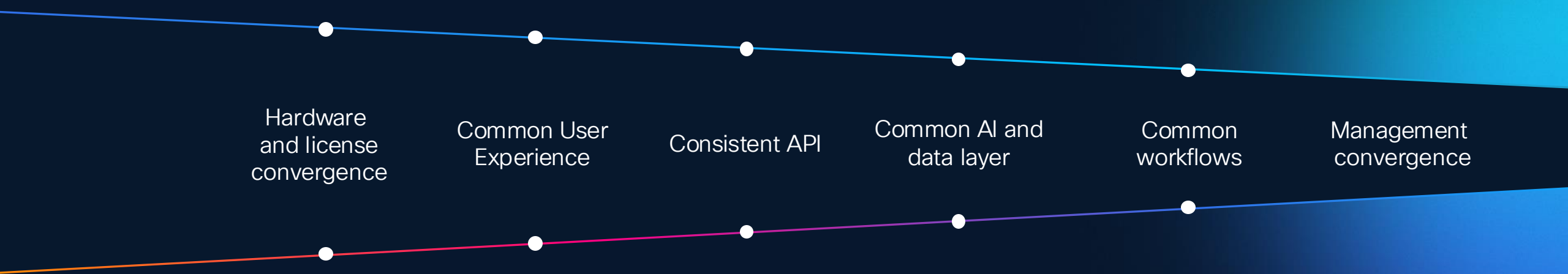
Consistent API

Common AI and
data layer

Common
workflows

Management
convergence

On-Prem Platform



Cloud Management Across the Networking Portfolio



Wireless

Full wireless support
Scale large campus wireless
with Campus Gateway

AVAILABLE



Switching

New | Expanded management
for access and core switching

New | IE3500 Rugged Series
Switching support

C9200, C9500, C9610 – AVAILABLE

C9600, C9400 – GA SEPTEMBER

IE3500 – GA APRIL



Routing

New | Expanded management
for Secure Routers

C8200, C8300, C8400 – GA JUNE

Bringing together the power of Catalyst and simplicity of Meraki

The Meraki dashboard displays an 'Organization Summary' for 'The Green Company'. It features a central 'Organization insights' section with a donut chart showing 9 impacted networks out of 900. Key metrics include 3 critical alerts (40% increase), 14 warnings (7% increase), and 352 informational alerts (7% increase). A table titled 'Impact across networks' shows the following data:

Issue type	Total impacted	Change
Clients	543	+511
Network devices	13	+1
Infrastructure	9	+6
Applications	4	+2

Below this is a 'Networks by health score' table with 100 results. The table columns are Network, Health score, Score change, Network tags, Clients, Network devices, Infrastructure, and Applications. The first few rows show:

Network	Health score	Score change	Network tags	Clients	Network devices	Infrastructure	Applications
Network name	70 pts	-24pts	Office	48 pts	84 pts	100 pts	100 pts
Network name	82 pts	-12pts	Office	54 pts	84 pts	99 pts	100 pts
Network name	84 pts	+1 pts	Office	68 pts	84 pts	99 pts	100 pts

The Catalyst Center dashboard provides a comprehensive overview of network health. It starts with a 'Welcome, Alexander' message and a 'Network status changes' summary for 24k total devices, 105k endpoints, and 900 applications across 25 sites. Key alerts include 3 critical alerts (40% increase), 14 major alerts (7% increase), 15 poor sites (7% increase), and 11 expired certificates (10% increase).

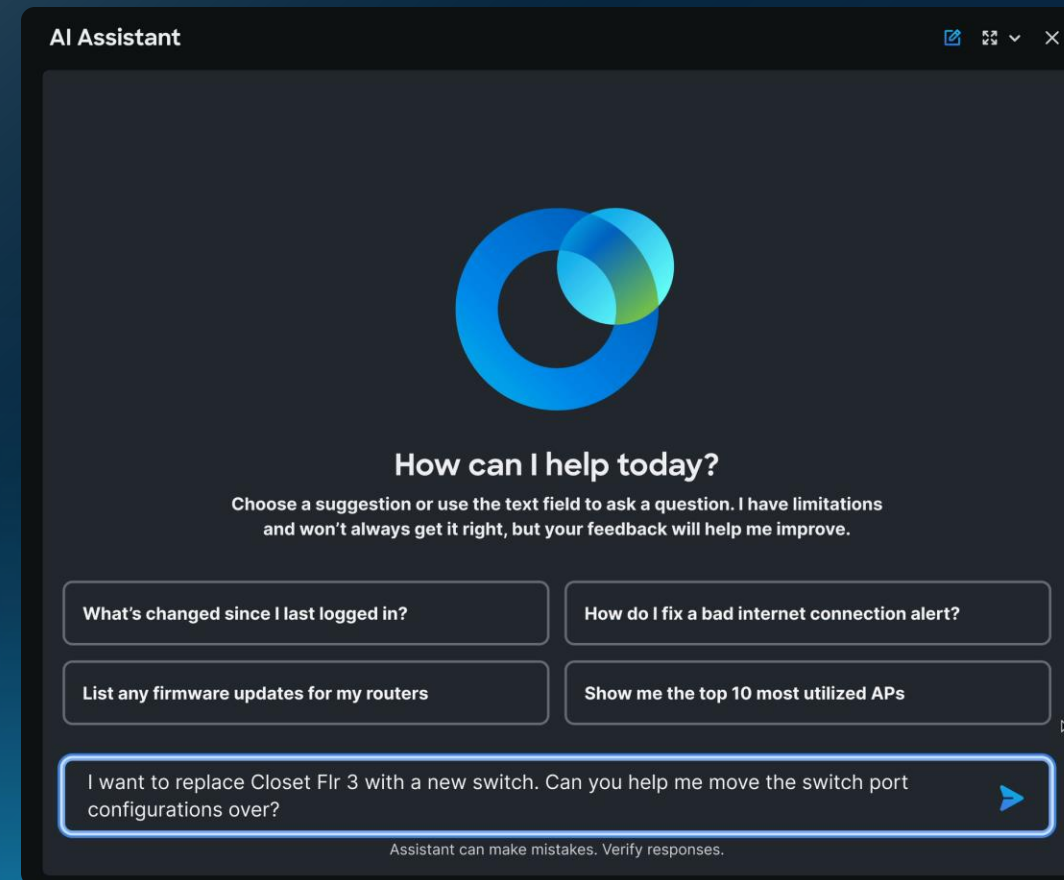
The 'Monitor' section includes several widgets:

- Routing:** 1.6k total in inventory, 99% healthy. Major alerts: 3. Alerting sites: 29. Routers: 11/1,607.
- Switching:** 2.3k total in inventory, 97% healthy. Critical alerts: 2. Alerting sites: 13. Core: 131. Distribution: 6/450. Access: 91/1,608.
- Endpoint:** 1.6k total concurrent endpoints, 96% healthy. Endpoints of low trust score (1-3): 576 (20%). Total unique endpoints seen in the last 24 hours: 2420. Major alerts: 2. Alerting sites: 33. Wired Endpoints: 5/4,554. Wireless Endpoints: 136/15k.
- Application:** 906 total, 98% healthy. Top 5 unhealthy applications. Data usage: 318.6 GB. Avg Throughput: 30.3 Mbps. Major alerts: 23. Alerting sites: 35. Business relevant apps: 75. Default apps: 10/527.

New Networking Skills for AI Assistant

Seamless monitoring, troubleshooting, and management across Cisco architectures

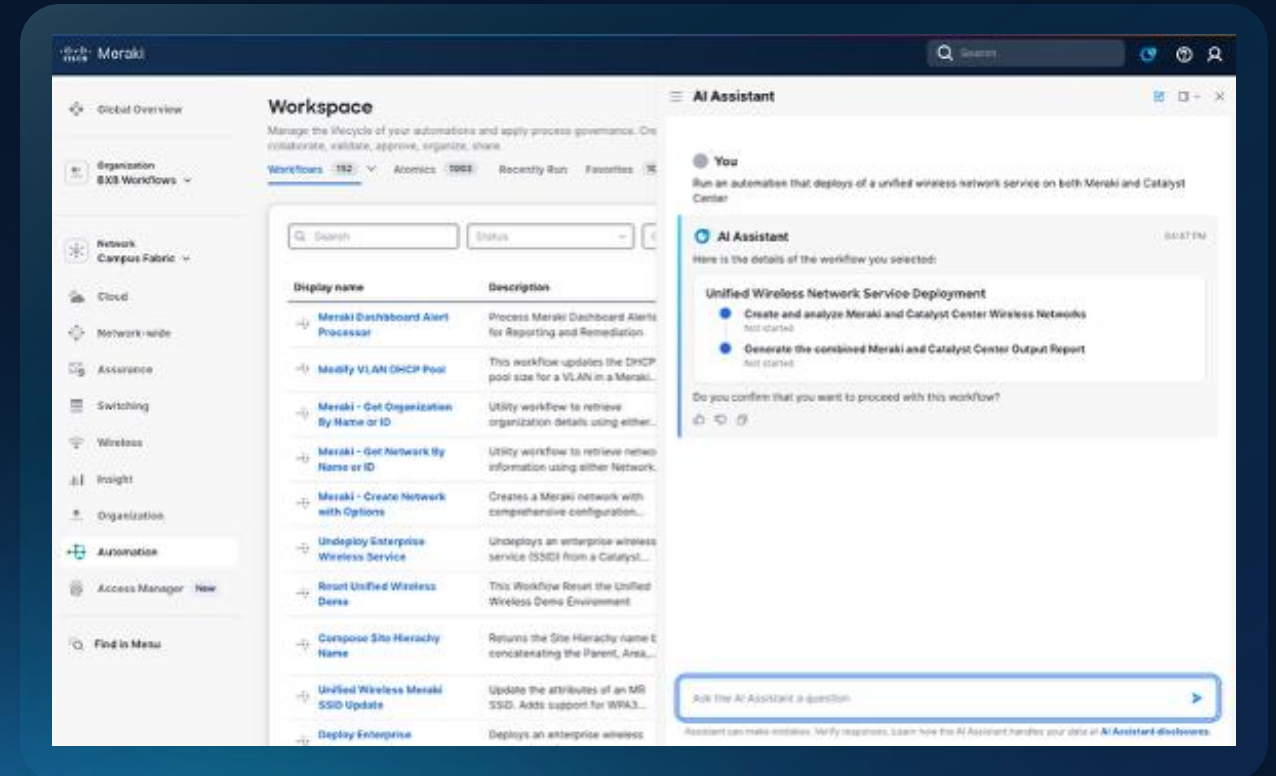
- Ask, explore, and act in natural language
- New automated workflows for config changes and switch migrations
- New integrated assurance capabilities



Agentic Workflows

Agentic automation across cloud and on-prem deployments

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



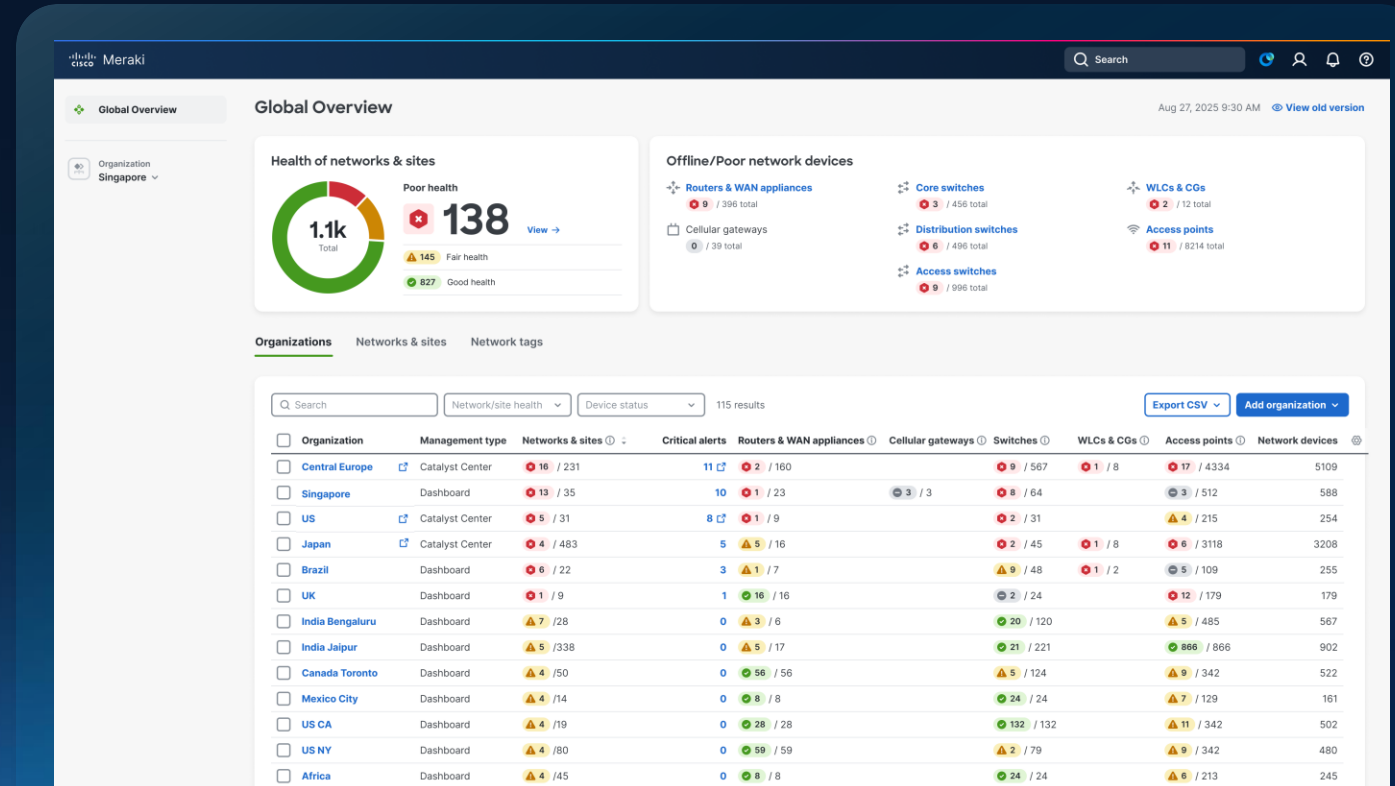
Global Overview

A single cloud experience integrating Meraki and Catalyst Center in the Meraki dashboard

Simplify hybrid operations – global view across Meraki and Catalyst Center

Troubleshoot faster – network, sites, and device alerts in one view

Streamline operations – secure SSO, no re-authentication



Global Overview

View old version

+ Add client

Clients

Organization
Prabhjit-Home-Org

Uplinks 1 total

WAN appliances 1 total

Switches 1 total

Access points 2 total

All
Online

All
Online

All
Online

1
Online

Network
Blossom Hill Home

Network-wide

Assurance

Security & SD-WAN

Switching

Wireless

Cameras

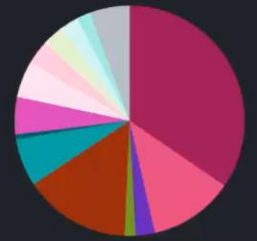
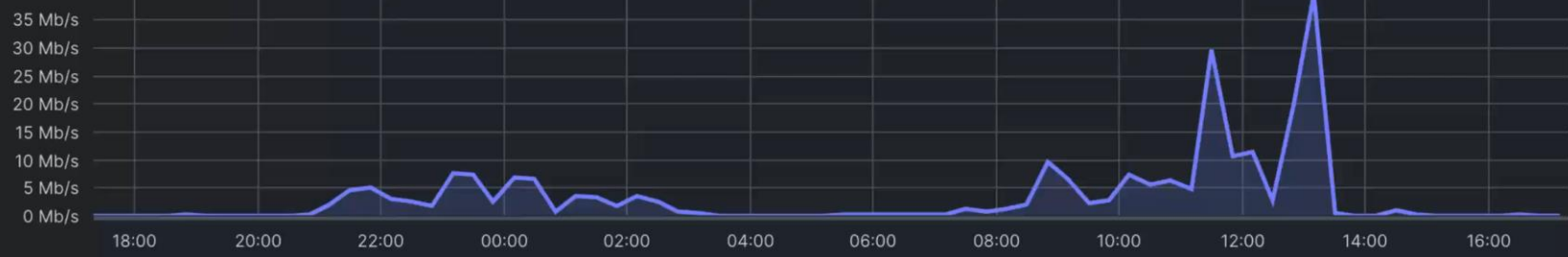
Organization

Automation

Find in Menu

Usage and clients

Usage 33.21 GB (↓ 18.42 GB, ↑ 14.79 GB)



Applications details

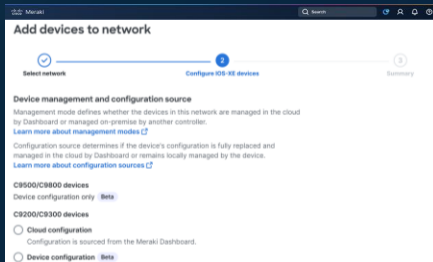
Search for clients Filters 13 results

Download

Status	Description	Connected to	IPv4 address	MAC address	Usage
Wired	eero	LivingRoom-MX	192.168.128.45	64:da:ed:95:2e:c1	31.2 GB
Wired	Eufy Home Base	MS130-24	192.168.40.7	04:17:b6:b3:5e:8b	4.6 MB
Wired	livingroom-ap-e0cbbc88cd71	LivingRoom-MX	192.168.20.3	e0:cb:bc:88:cd:71	3.61 MB
Wired	ms130-24-149f43ee5be1	LivingRoom-MX	192.168.128.2	14:9f:43:ee:5b:e1	37.53 MB
Wireless	PBAGGA-M-W723	LivingRoom-AP	192.168.4.18	e2:4d:92:3a:14:3d	13.36 MB
Wireless	PBAGGA-M-W723	LivingRoom-AP	192.168.40.5	8a:2b:c0:29:ee:ae	1.1 MB

Large Campus Cloud Capabilities

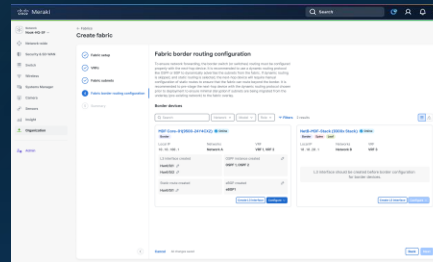
Powerful Switching Capabilities



Support campus deployments with BGP, VRF, ISSU, and IOS XE stacking

BETA NOW

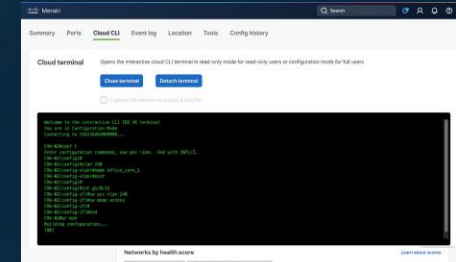
Fabric for Secure Networking



Simplify NetOps with a secure fabric and micro/macro-segmentation

BETA | NOV

Cloud CLI for Flexibility

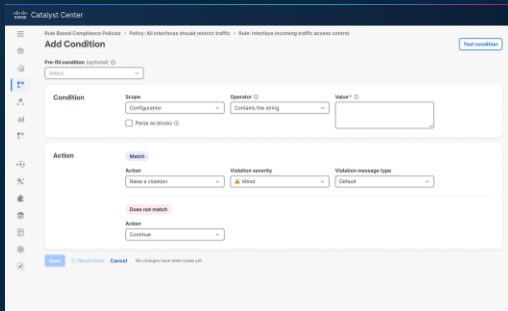


Simplify onboarding and flexibility with operating mode options and Cloud CLI

AVAILABLE

Catalyst Center – Scaling with Flexibility and Automation

Rule-Based Compliance



Custom compliance rules and to detect issues network-wide

AVAILABLE

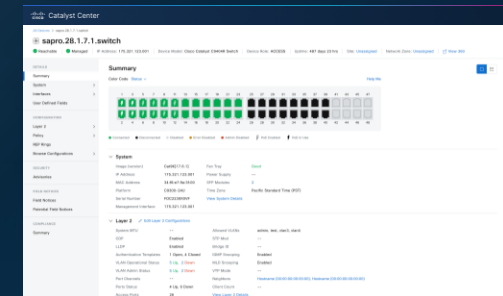
Virtual Appliance Support for Azure



Deploy a virtual appliance on Azure for operational flexibility

AVAILABLE

Campus Automation



Enable device-by-device feature learning and configuration

AVAILABLE

APIs and Apps to Automate Operations

PLATFORM

Management

API / Integrations

Assurance

Intelligence - AgenticOps

HARDWARE



Smart
Switches



Secure
Routers



Wireless



Industrial
IoT

APIs and Agent Integrations



API & Automation

2000+

API Endpoints

19M

API Calls/Month
+30% YoY

Infrastructure as Code

1000+

Customers



MCP and Agents

New | ThousandEyes MCP

Cisco Networking Marketplace

Largest exclusive catalog of turnkey apps to unlock new business outcomes

370+ apps offer custom-built automation, insight and security

servicenow

PagerDuty

Boundless

ekahau

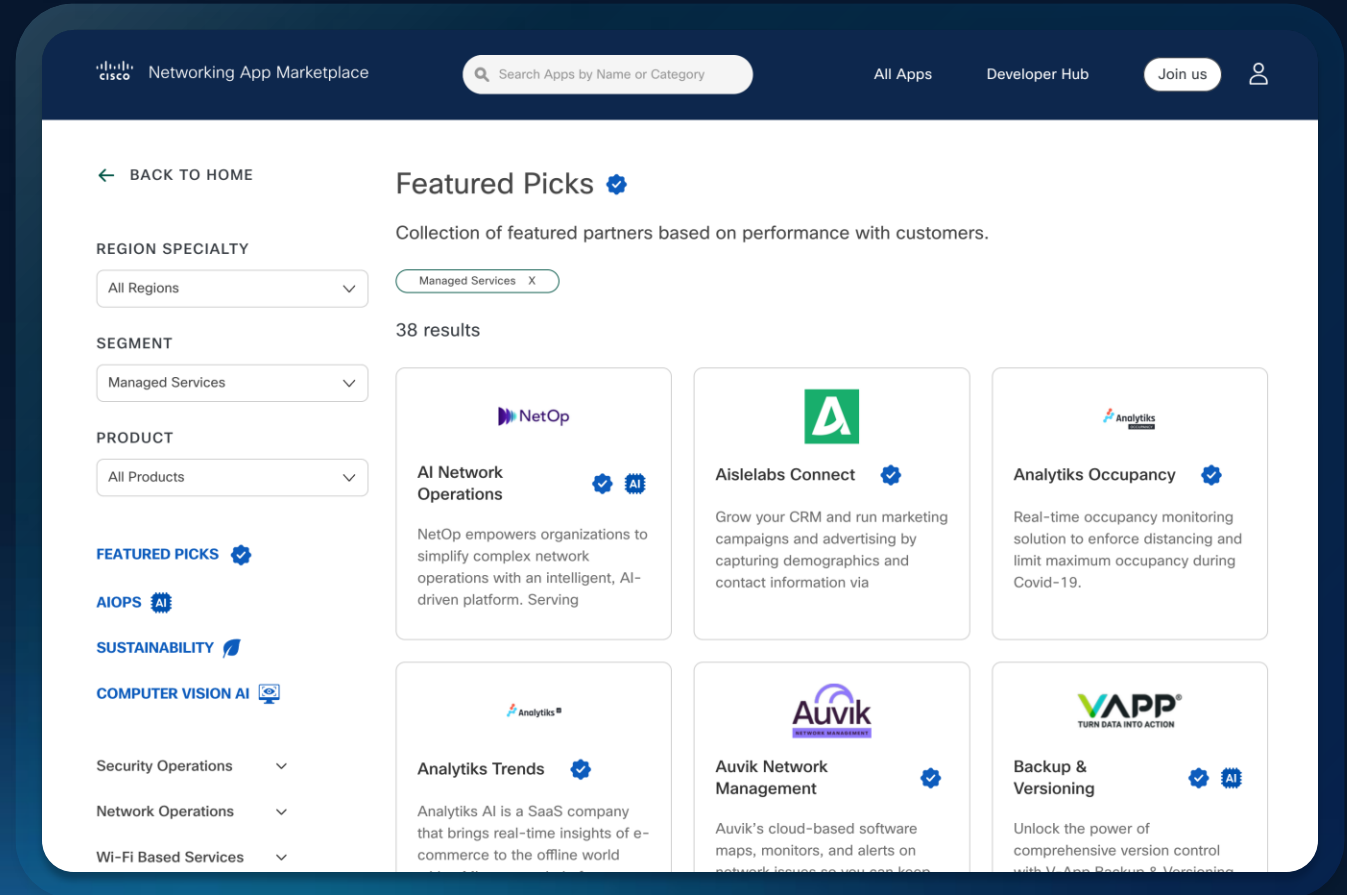
Red Hat

splash access.

netbox

infoblox

Megaport



Multilayered Assurance to Simplify Operations

PLATFORM

Management

API / Integrations

Assurance

Intelligence - AgenticOps

HARDWARE



Smart
Switches



Secure
Routers



Wireless



Industrial
IoT

Today's Operations Can't Keep Up

Traditional Approaches

- Alerts & dashboards
- Manual correlation
- Slow decisions
- Risky changes

Assurance + AgenticOps

- Experience objectives
- Shared context & change awareness
- Agents prioritize & act
- Closed-loop validation

Reactive

Proactive

Cisco Assurance

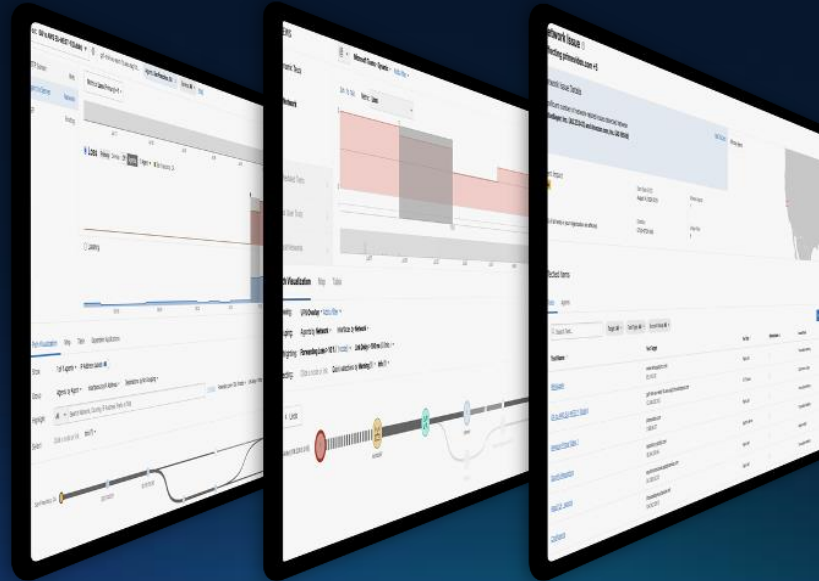
More visibility

Traffic Insights Extends
Visibility for Real-User Traffic
Now Available

Cisco Industrial Networking for
Visibility from OT Networks
Now Available

Mobile Agent Give Insight Into
Android Devices
Now Available

More intelligence



Experience Metrics Give Deeper
Insight Into Wireless Experience
Currently in Alpha

Cloud Insights Correlates
Changes in the Cloud
Now Available

Stronger platform

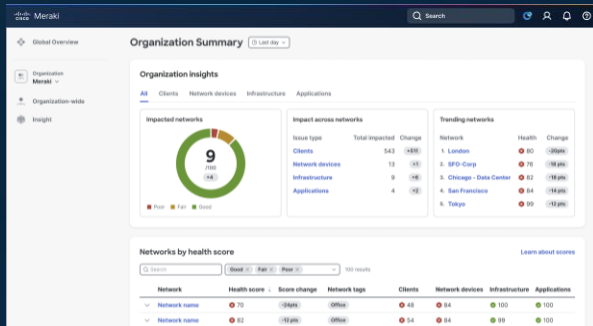
Cisco AI Assistant Helps Customers
Operationalize the Platform
Now Available

MCP Server Integrating
ThousandEyes Data with Agentic AI
Now Available

Splunk Integration End-to-End
Observability
Now Available

Real-Time Clarity From the Client to Enterprise-Wide

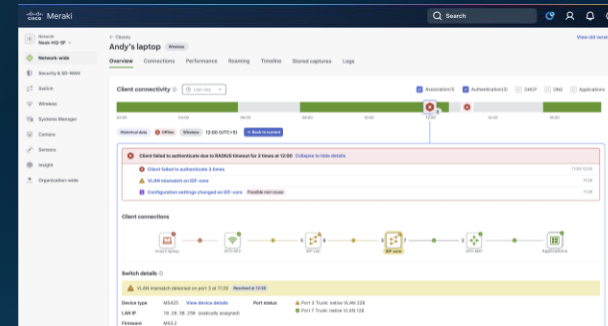
Organization-wide assurance visibility



Visibility across every site—spot trends, surface issues, drill into site-level detail

AVAILABLE

Client-side assurance insights



End-to-end visibility for every individual client

AVAILABLE

Our Unified Platform

PLATFORM

Management

API / Integrations

Assurance

Intelligence - AgenticOps

HARDWARE



Smart
Switches



Secure
Routers

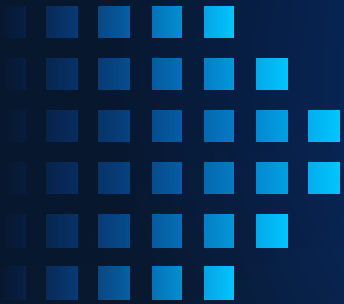


Wireless

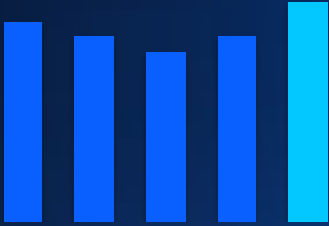


Industrial
IoT

Cisco's AgenticOps



Cross-domain telemetry



Ensemble of models and domain expertise



Agentic capabilities

- Cisco/Splunk dashboards GA
- AI Assistant GA
- AI Canvas Early Access
- Cisco Cloud Control Early Access
- Other Applications Coming Soon

Purposeful interactions

New AgenticOps Capabilities 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

Autonomous Troubleshooting

Delivers credible root cause and remediation. In minutes.

Beta CYQ2 26

- Parallel troubleshooting with advanced root cause analysis
- Triage campus, branch, internet, and industrial connectivity and experience issues
- Deterministic workflows for auto-remediation, configuration, and containment

The CTO Laptop (MAC: 2c:cf:67:95:03:a3) is currently offline and has experienced repeated DHCP failures in the last 2 hours while connecting to SSID "t-GARR" via the access point "FL5 HQ VPN SSID". No application-level issues were detected for this client, and no other clients are reported as impacted in the application assurance data. The most recent and relevant event is a DHCP failure at 2026-01-22T05:10:45Z, which is likely the root cause of the connectivity problem. No correlated events were found for this event.

Recent DHCP failure events for CTO Laptop

Events include time, SSID, and access point for the last 2 hours.

Time	SSID	Access point
Jan 21, 2026, 09:10 PM PST	t-GARR	FL5 HQ VPN SSID
Jan 21, 2026, 09:00 PM PST	t-GARR	FL5 HQ VPN SSID
Jan 21, 2026, 08:51 PM PST	t-GARR	FL5 HQ VPN SSID
Jan 21, 2026, 08:44 PM PST	t-GARR	FL5 HQ VPN SSID

Troubleshooting Steps:

1. Check for an exhausted DHCP pool, which is a common cause of DHCP issues.
2. Create a test SSID in NAT mode and attempt to connect the CTO Laptop.
3. Consider reducing the DHCP lease duration to free up more addresses for new clients.
4. Run a packet capture on the AP's wired interface while attempting to connect the affected client. Use Wireshark with the "dhcp" filter to check for DHCP Offers and Acknowledgments. If these are missing, the issue may be upstream or with the DHCP server.

Continuous Optimization

Keeps the network in its best state. Automatically.

Beta CYQ2 26

- Builds and maintains a live operational model of user experience
- Executes expert tuning actions across RF, QoS, path control planes, and more
- Continuously tailors towards Experience Metrics

AP Offline Detected & Auto-Recovered

I detected Conference Room 3A (MR46) went unreachable in network `L_28304` and automatically restored connectivity.

Impact Detected:

- AP offline for 2m 34s
- 12 clients disconnected
- Active video call disrupted

Workflow Executed:

`ap_recovery`

1. Verified AP status via dashboard
2. Checked uplink switch port
3. Initiated PoE power cycle
4. Monitored AP reconnection
5. Verified client reassociation

Actions Taken:

- PoE cycle on switch port Gi1/0/14
- AP rebooted successfully
- Clients auto-rejoined

Result:

- AP back online in 47s
- All 12 clients reconnected
- No manual intervention needed

Meraki AI Assistant • Detected 2:47 PM • Resolved 2:48 PM • No human intervention required



Bandwidth Abuse Detected & Mitigated

I detected a single client consuming 78% of available bandwidth on `Guest-WiFi` and automatically applied traffic shaping to restore fair access.

Impact Detected:

- Client `DC:A6:32:xx:xx:91` using 847 Mbps
- 34 other guests experiencing <2 Mbps
- 8 complaints in last 15 min

Workflow Executed:

`bandwidth_policy`

1. Identified top bandwidth consumer
2. Analyzed traffic pattern (torrent)
3. Applied per-client limit policy
4. Verified bandwidth redistribution
5. Logged incident for review

Trusted Validation

Makes every change safer. Predictably.

Beta CYQ2 26

- Models impact/blast radius before change
- Validates changes against live telemetry, topology
- Guides agents to the next safe action
- Deep reasoning for audit-ready compliance reports and more

The screenshot displays the Meraki AI Assistant interface. On the left, a sidebar shows a list of recent threads, including 'Requesting a security audit for...' and 'Assessing network security ma...'. The main content area shows a chat conversation where the user asks 'Do a security audit for London'. The AI Assistant responds with a detailed 'Security Audit Report: London Network'.

Security Audit Report: London Network

Summary
Security architecture audit for London network (L_546829496481087792) covering firewall protection, threat prevention, wireless security, switching security, network segmentation, VPN configuration, logging/monitoring, and incident response readiness.
Overall Security Score: 6.6/10 (Good)

Top 3 Immediate Actions:

1. Replace any-to-any allow firewall rule with specific rules and add explicit default deny
2. Implement inter-VLAN firewall rules to isolate Finance, IoT, and Guest segments from corporate network
3. Apply 802.1X authentication to user-facing switch ports and restrict trunk port VLANs

Key Finding
The London network demonstrates **strong threat prevention and monitoring capabilities** (IDS/IPS enabled, AMP active, comprehensive logging), but suffers from **critical weaknesses in access control and segmentation**. The network has 9 VLANs including sensitive segments (Finance, IoT, Guest) but lacks inter-VLAN firewall controls, allowing unrestricted lateral movement. Additionally, 27 of 28 switch access ports lack 802.1X authentication, and an open corporate SSID (CL26) exposes wireless traffic to eavesdropping.

Details
Critical & High Severity Findings

Area	Finding	Severity	Evidence	Recommendation
Firewall (L3)	Any-to-any allow rule as default policy	Critical	L3 firewall contains single rule: 'Any -> Any allow'	Replace with specific allow rules following least-privilege principle; add explicit default deny rule at end
Firewall (L3)	No explicit default deny rule	High	Firewall policy ends with allow-all instead of deny-all	Add explicit 'deny any any' rule as final rule in firewall policy

Ask the AI Assistant a question Default

Assistant can make mistakes. Verify responses. Learn how the AI Assistant handles your data at [AI Assistant disclosures](#).

Global Overview

Organization NexaCorp

Network California

Network-wide

Assurance

Security & SD-WAN

Switching

Wireless

Systems Manager

Insight

Organization

Automation

Find in Menu

View old version

+ Add client

Clients

Uplinks 1 total

All Online ✓

WAN appliances 1 total

All Online ✓

Switches 1 total

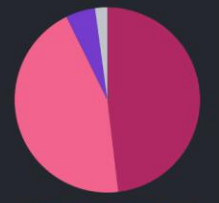
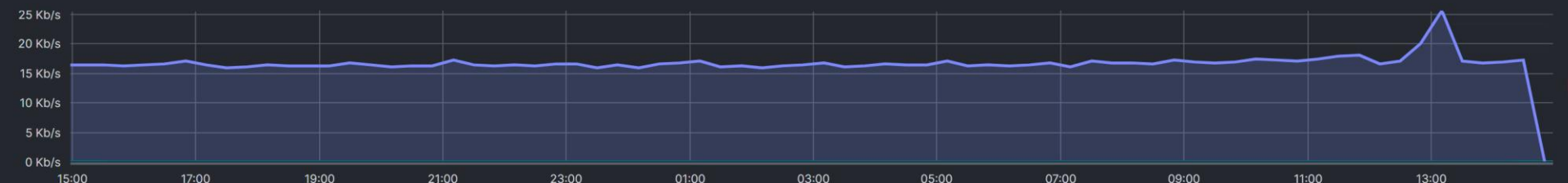
All Online ✓

Access points 2 total

1 Online ✓

Usage and clients

All clients | Last day | Applications



Applications details

CTO Laptop | Status, type, OS | Connected to | VLAN | Policy | Tunneled through | 1 result | Reset all | Download

Status	Description	Connected to	IPv4 address	MAC address	Usage	Device type, OS	Last seen (UTC-7)	Onboarding
<input checked="" type="checkbox"/> Wireless	CTO Laptop	FL5 SF Desk	10.10.11.4	2c:cf:67:95:03:a3	—	Chrome OS	Mar 9 2026 14:57	—

Rows per page 30 | 1

- Network TRADA-TR010
- Network-wide
- Assurance
- Switching
- Wireless
- Sensors
- Organization
- Automation
- Admin

Alerts

Configure alerts

Alerts 7 Optimizations 45

Active Resolved

30 All networks

Optimization type

45 matching results

Refresh As of 1 minute ago

Active optimizations

Optimization type	Network count	Impact ⓘ	Category
Enable WPA3	26	90 APs 588 clients	Security
Enable 802.11r	11	703 APs 999+ clients	Performance
Enable 6GHz on wireless network	8	95 APs 237 clients	Performance

Give feedback

Give your feedback

- Global Overview
- Organization NexaCorp
- Network California
- Network-wide
- Assurance
- Security & SD-WAN
- Switching
- Wireless
- Systems Manager
- Insight
- Organization
- Automation
- Find in Menu

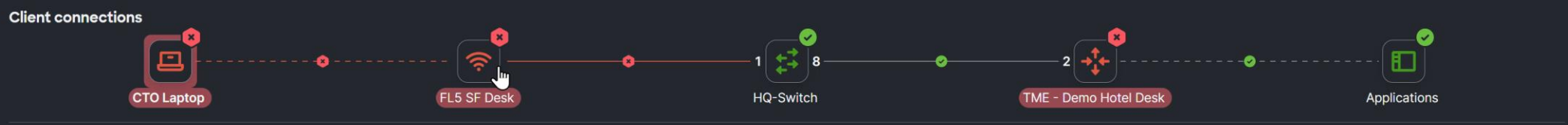
← Clients
CTO Laptop ✎

- Overview**
- Connections
- Performance
- Roaming
- Timeline
- Stored captures
- Logs



Historical data ✖ Offline Wireless Mar 09, 2026, 12:40 (UTC -7) → Back to Current

Failed connection to SSID `_Miles_Meraki` on access point `FL5 SF Desk` because the DHCP server rejected the client's request. 42 correlated events



Client details

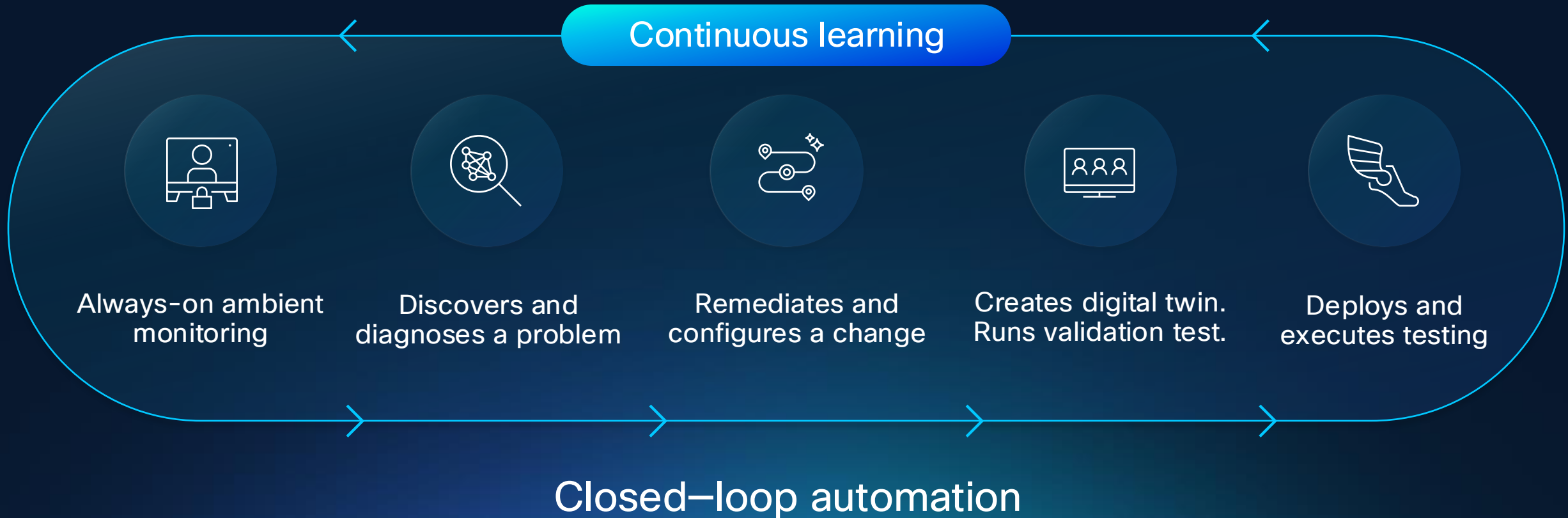
SSID `_Miles_Meraki` MAC address `2c:cf:67:95:03:a3`
 Access point `FL5 SF Desk`

Usage 🕒 Last Day 📄 Applications

No data available

No data

AgenticOps in Practice



BETA

AI Canvas

Troubleshooting and execution across multiple domains

Collaboration across multiple users (NetOps, SecOps and execs)

Built on the foundation of the Deep Network Model

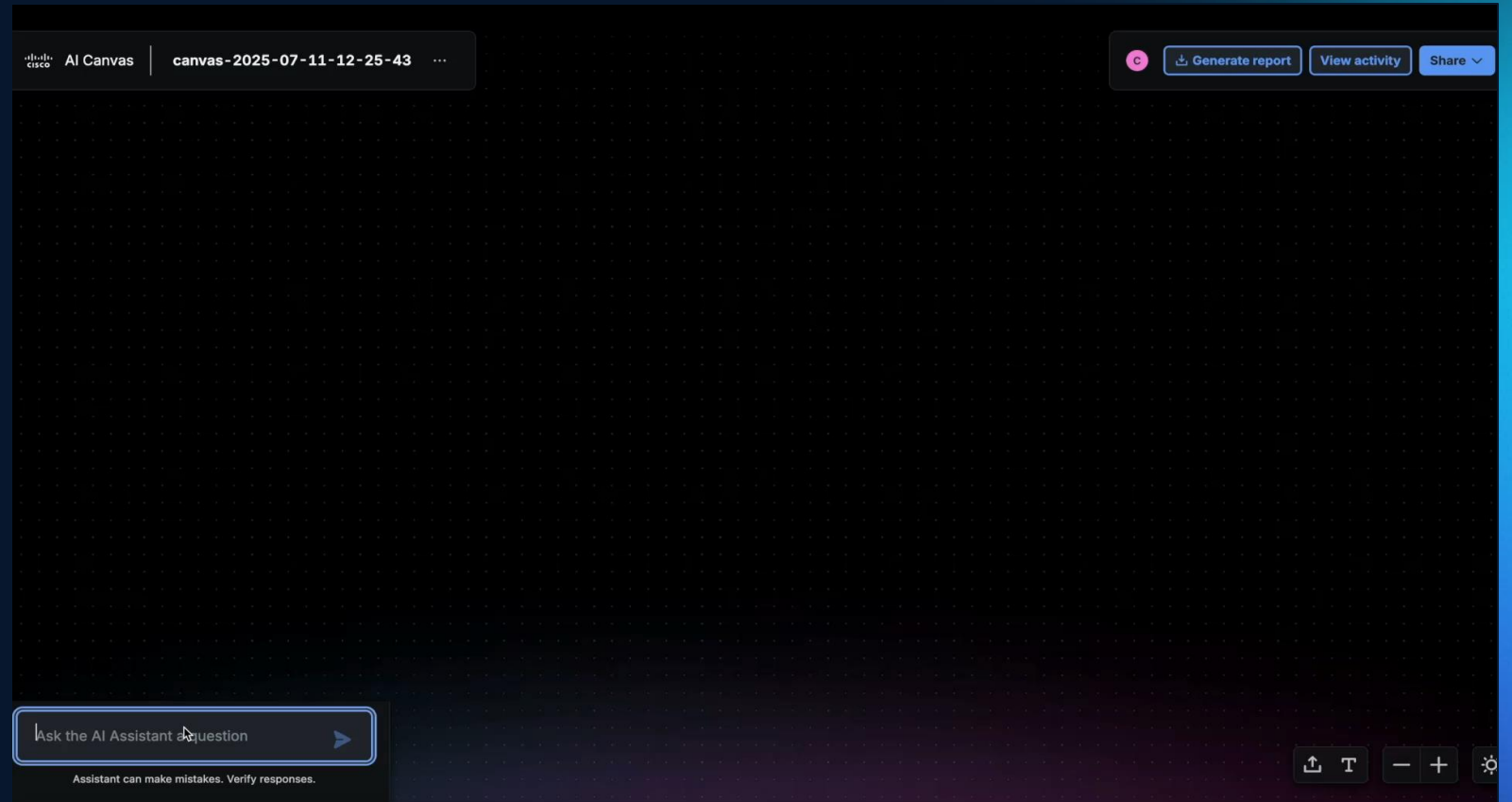
The screenshot displays the AI Canvas interface for "Application performance degradation". The interface includes several key components:

- AI Assistant Panel:** A chat window on the left with a menu icon and a close icon. It contains the text: "This graph shows a clear link between congestion and application failures. When the interface gets congested, financial app failures spike almost instantly. Right now, critical transactions are competing with non-essential traffic during busy periods. The concurrent scheduling of mandatory security-related software updates could be a significant contributor to these congestion events." Below the text is a graph titled "SJ-MX105-01 network congestion statistics vs. EFP application performance" from Splunk, showing Packet Loss (blue line) and Transaction failure rate (red line) over time from 8:00 to 08:30. At the bottom of the panel is a text input field "Ask the AI Assistant a question" and a disclaimer "Assistant can make mistakes. Verify responses."
- ServiceNow Ticket Card:** A card titled "ServiceNow SRTK0023941" with a "Reported by" field (System Administrator on 03/28/2025 at 09:45 AM PST) and a "Description" field (Received a ThousandEyes alert and reached out to Maria Chen to confirm. She said users at San Jose branch experiencing 3-5 second delays when processing financial transactions in EFP. Started approximately 30 minutes ago. Affects all 24 users at the branch. No recent changes reported.).
- Meraki Performance Card:** A card titled "SJ-MX105-01 WAN interface performance" showing a "Loss rate" of 16.4% (up from a baseline of 2.3%). It also lists "WAN interface latency" (87ms baseline $\pm 50\text{ms}$) and "Jitter" (15ms baseline $\pm 5\text{ms}$).
- Network Segment Performance Analysis Card:** A card titled "Network segment performance analysis" showing a flow diagram with four stages: Enterprise network (16.4% loss), Gateway, Internet, and Application (financeapp.com). A legend indicates "Connection" (blue line) and "Packet loss point" (red dot).
- Meraki Performance Graph:** A line graph titled "SJ-MX105-01 performance (last 24 hrs)" showing Packet Loss (0% to 20%) over Time (Hours) from 20:00 to 20:00. A red dot marks a "Critical point" at approximately 10:00.
- Email Thread Card:** An email thread card from Maria Chen to Support, cc'ing Jackie Torres and Jorres. The subject is "URGENT: Status Update needed on Financial Application Performance Issues". The body text reads: "Hello Team, I'm following up regarding the ongoing performance issues with the Enterprise Financial Platform (EFP) affecting our San Jose branch. This performance degradation is severely impacting our ability to serve customers. We have end-of-month financial processing scheduled for tomorrow, and we need reassurance that this issue will be resolved by then. Could you please provide an immediate status update on troubleshooting efforts and expected resolution timeframe? If there's a workaround we can implement in the meantime, that would be extremely helpful. Thank you for your urgent attention to this matter. Best regards, Maria Chen, Senior Director, Financial Operations".

At the top right of the interface are buttons for "Generate report", "View activity", and "Share". At the bottom right are icons for "Print", "Zoom in", and "Zoom out".

Demo

AI Canvas with Meraki & ThousandEyes



Click on the video in presenter mode to enlarge

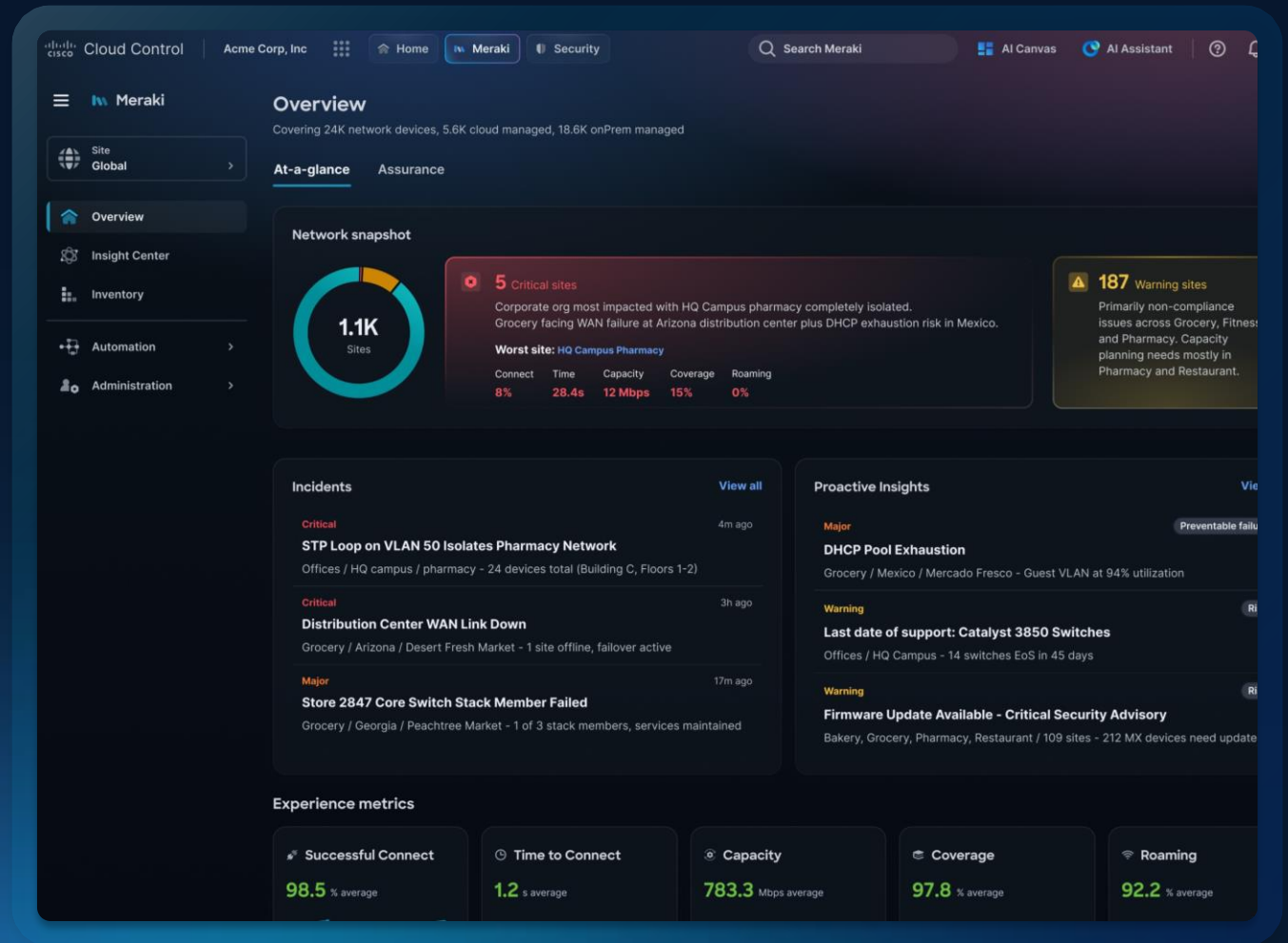
Unified Management for Operational Simplicity

Flexible deployments for cloud, on-prem, and hybrid

Unified management experience

Enterprise capabilities and scale

AI-powered automation and assurance



Proven Business Outcomes With Our Platform

80%

Fewer
support tickets

80%

Faster
resolution times

90%

Less time spent on
configuration changes

Let's Talk Next Steps



Start an AI-readiness assessment

Work with our experts to plan your new architecture



Try AI Assistant

Get instant insights and automate manual tasks



Start a free product trial

Speak with your Cisco account team to get started

Thank you



