CISCO Connect

Modernize the Network with Cisco Secure Campus



Russ Widener
System Engineer

Dave Cappelli
Enterprise Networking Specialist

Agenda

01 Why Modernize Now?

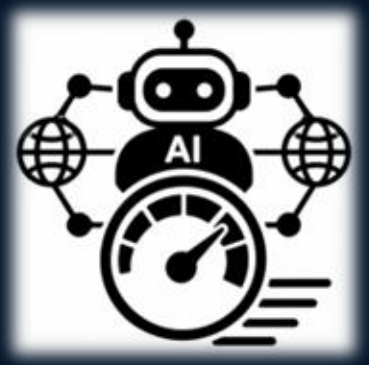
02 Security in the Network

03 The Next Gen Campus Portfolio

04 Simplified operations, powered by AgenticOps

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

The Modern Campus Needs



Performance to Meet Agent Demands



Agent Identity and Distributed Security



Defend Against AI-Accelerated Exploits



PQC-Ready

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

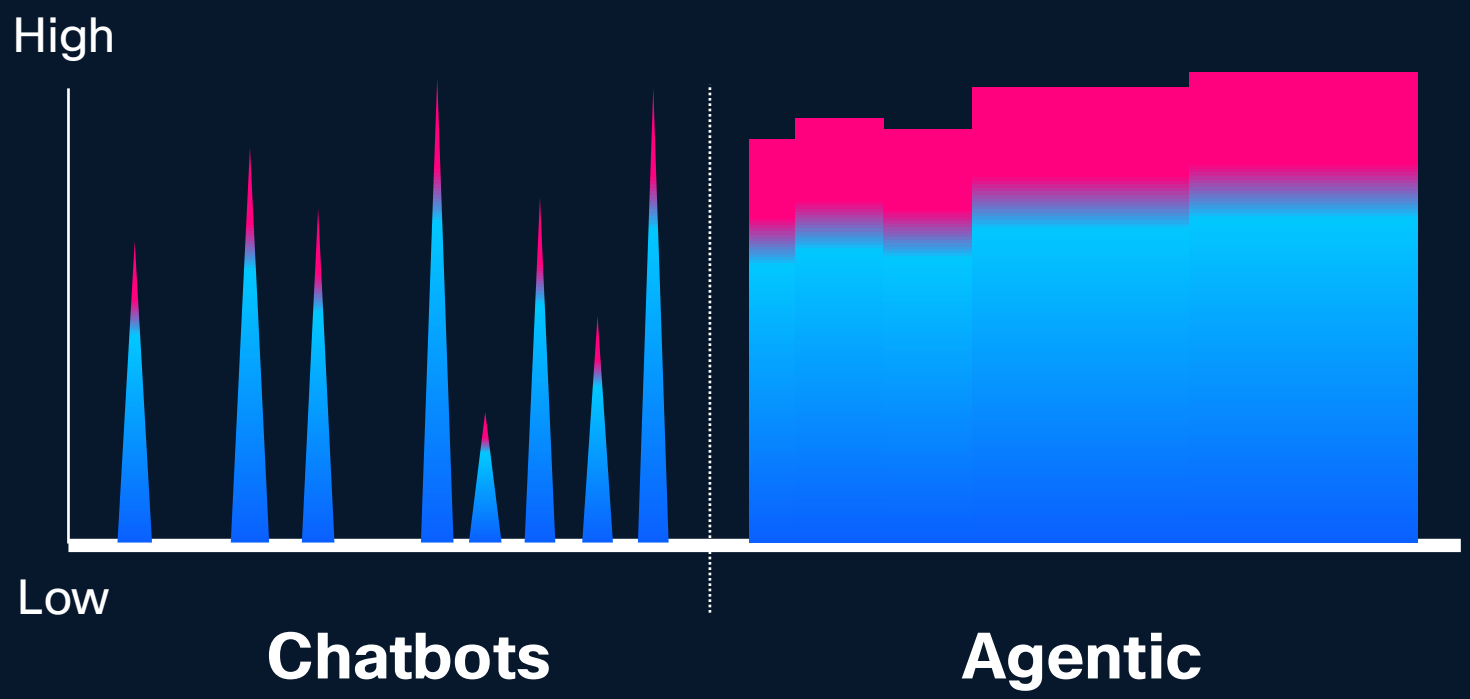
Creating new network demands

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.

Agentic AI in the Campus

Agentic AI is moving into the campus. Why?

- **Cost Reduction**: Local hardware solutions reduce persistent agent deployment costs by up to 80%
- **Token Multipliers**: Agentic workloads consume 4x to 15x more tokens than basic chat applications because multi-step autonomous reasoning triggers continuous loops.
- **Growth in Reasoning**: Global reasoning workloads have surged 320 times year-over-year, driving projections for token consumption to grow 3,400% by 2030.

As Agentic AI moves closer to the data, networks need to adapt



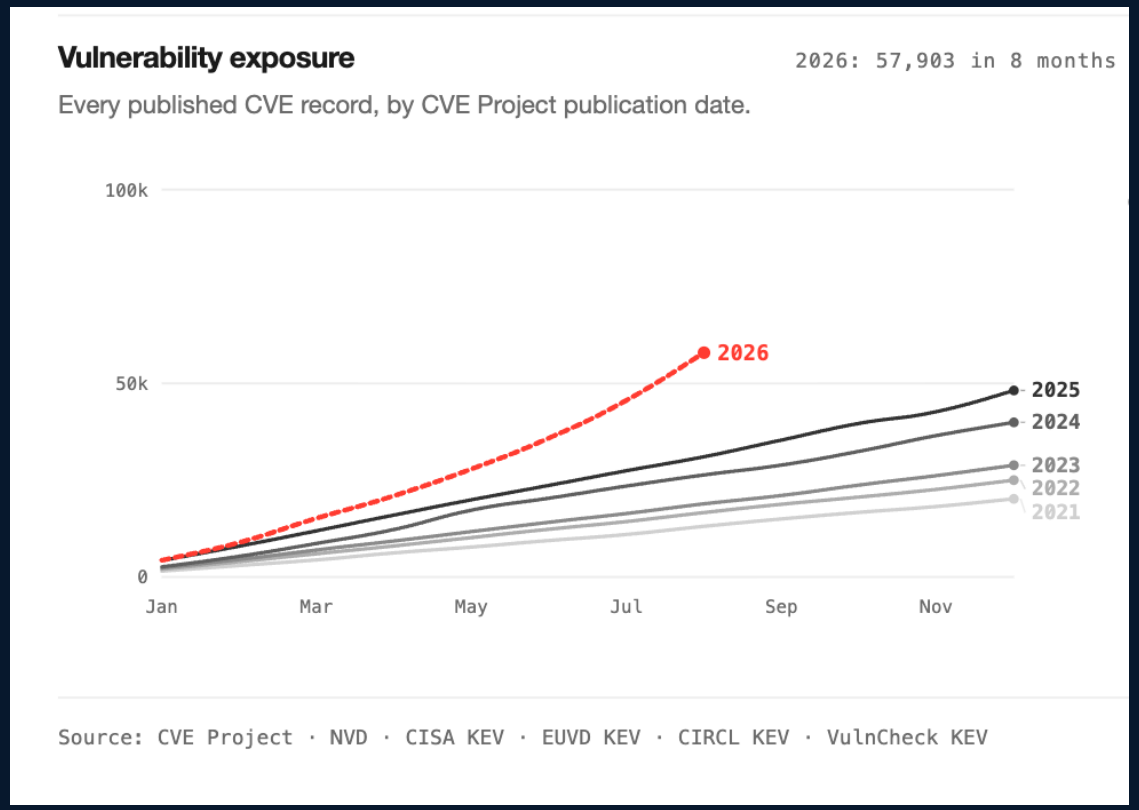


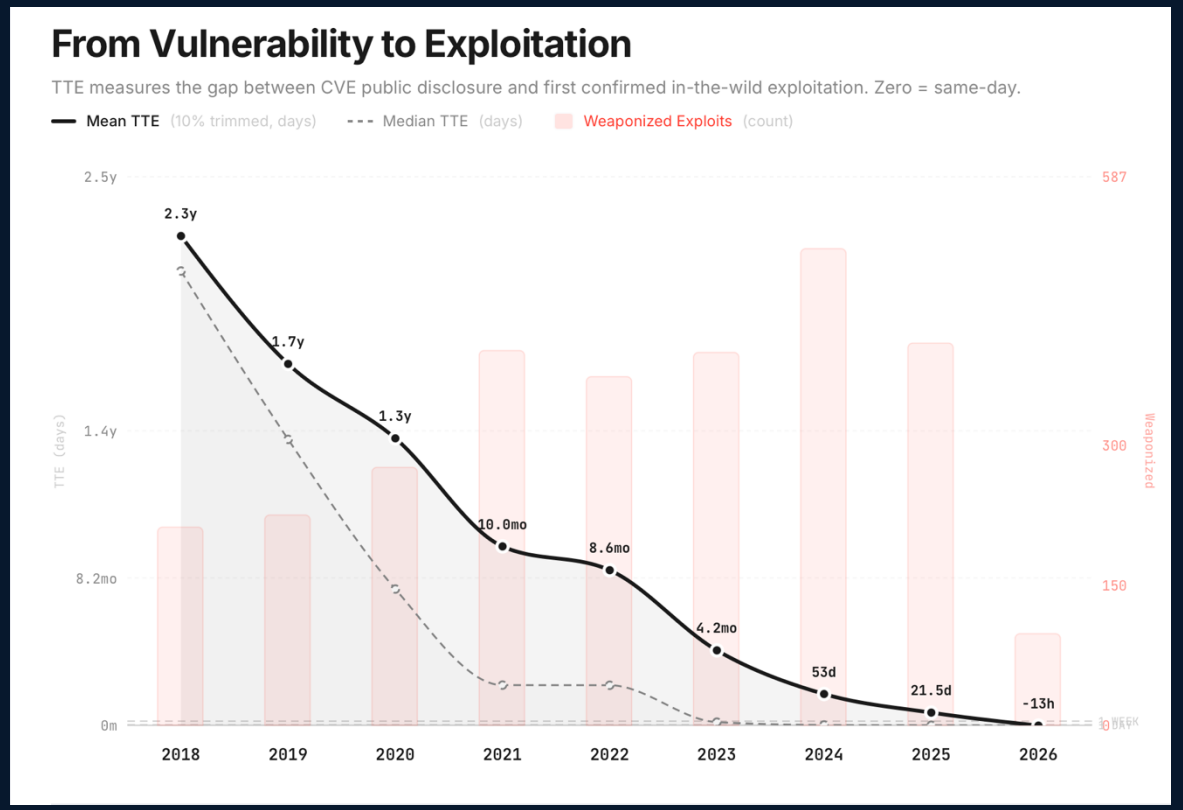


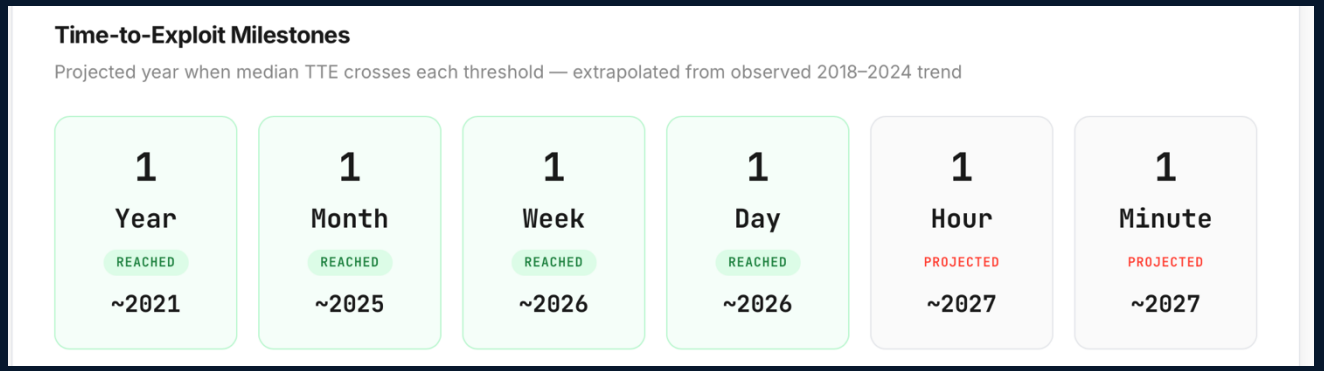
© 2026 Cisco and/or its affiliates. All rights reserved.

Threats are increasing in volume and speed

https://ZeroDayClock.com

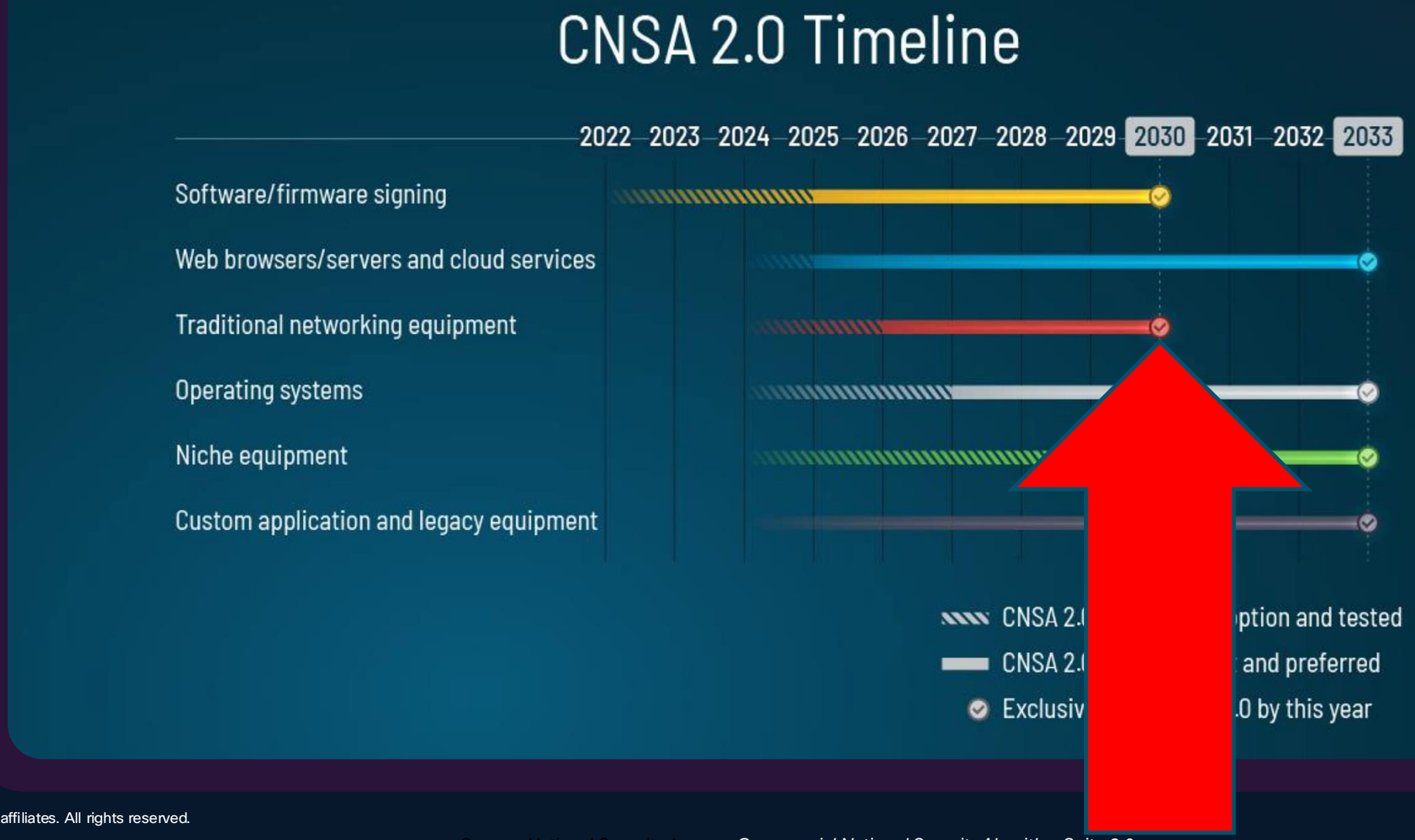






© 2026 Cisco and/or its affiliates. All rights reserved.

Post Quantum is Approaching



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

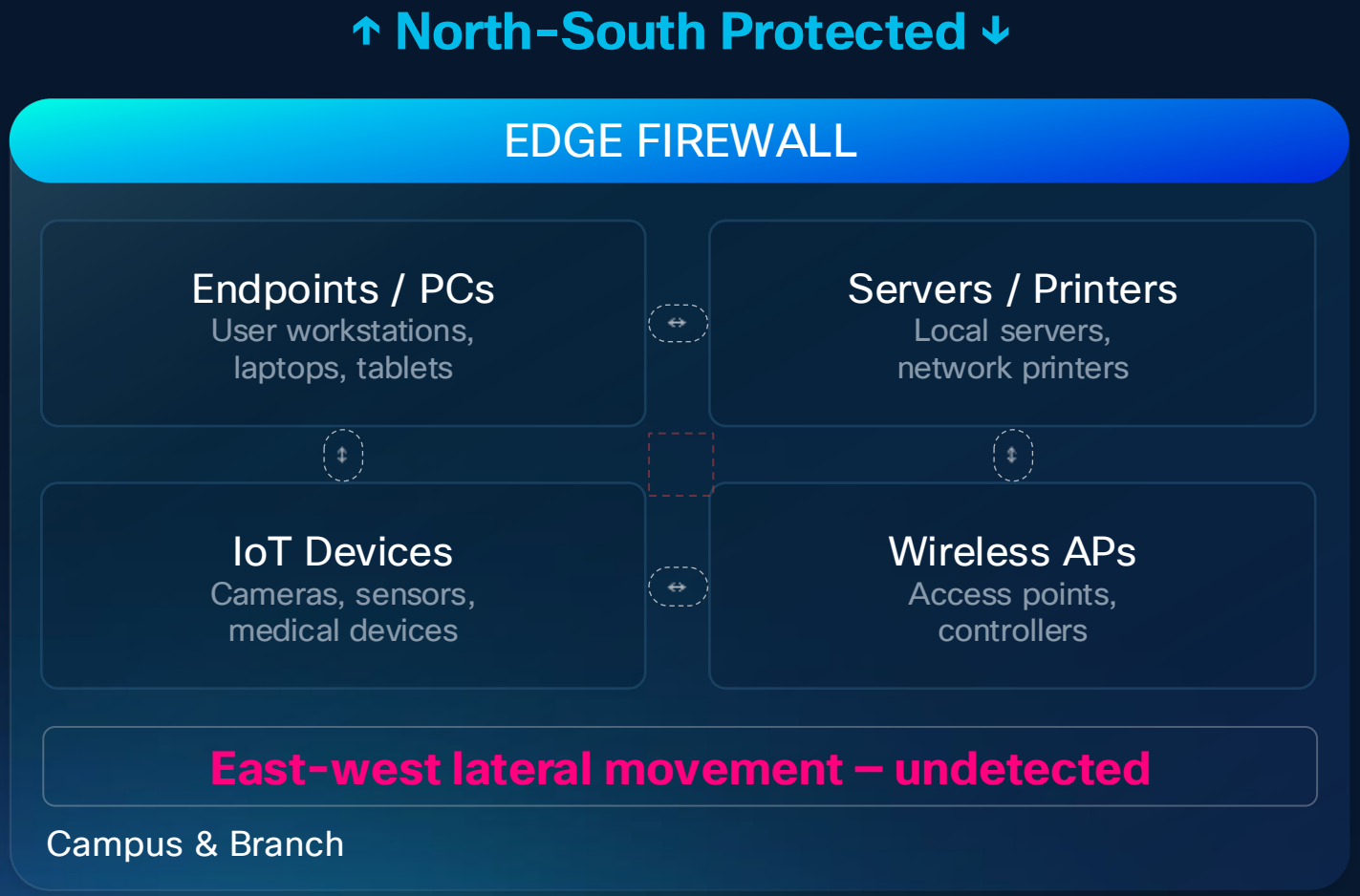
Source: National Security Agency, *Commercial National Security Algorithm Suite 2.0*

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

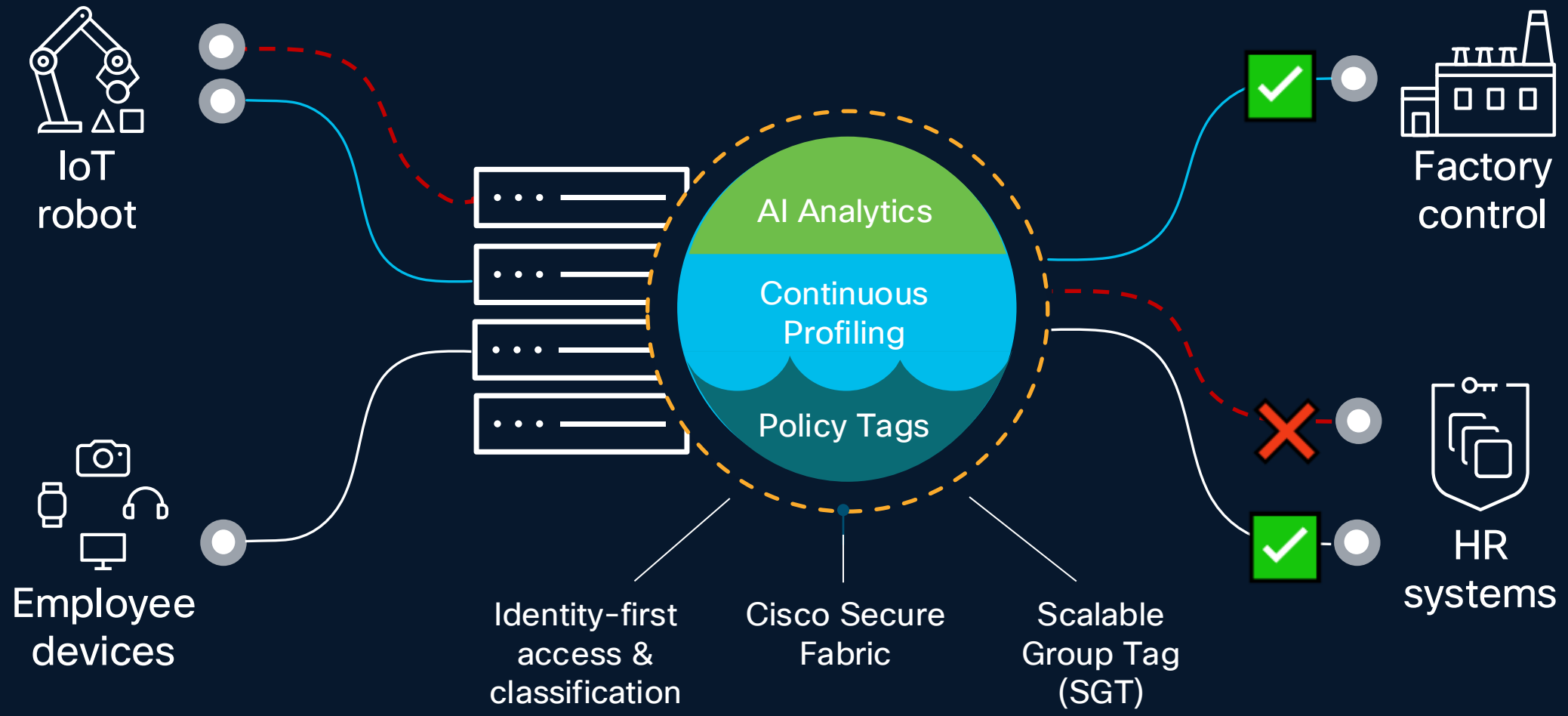
One policy model, coordinated enforcement at every point.

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.

Scalable network segmentation

Continuously verified identity and group policy applied across the network

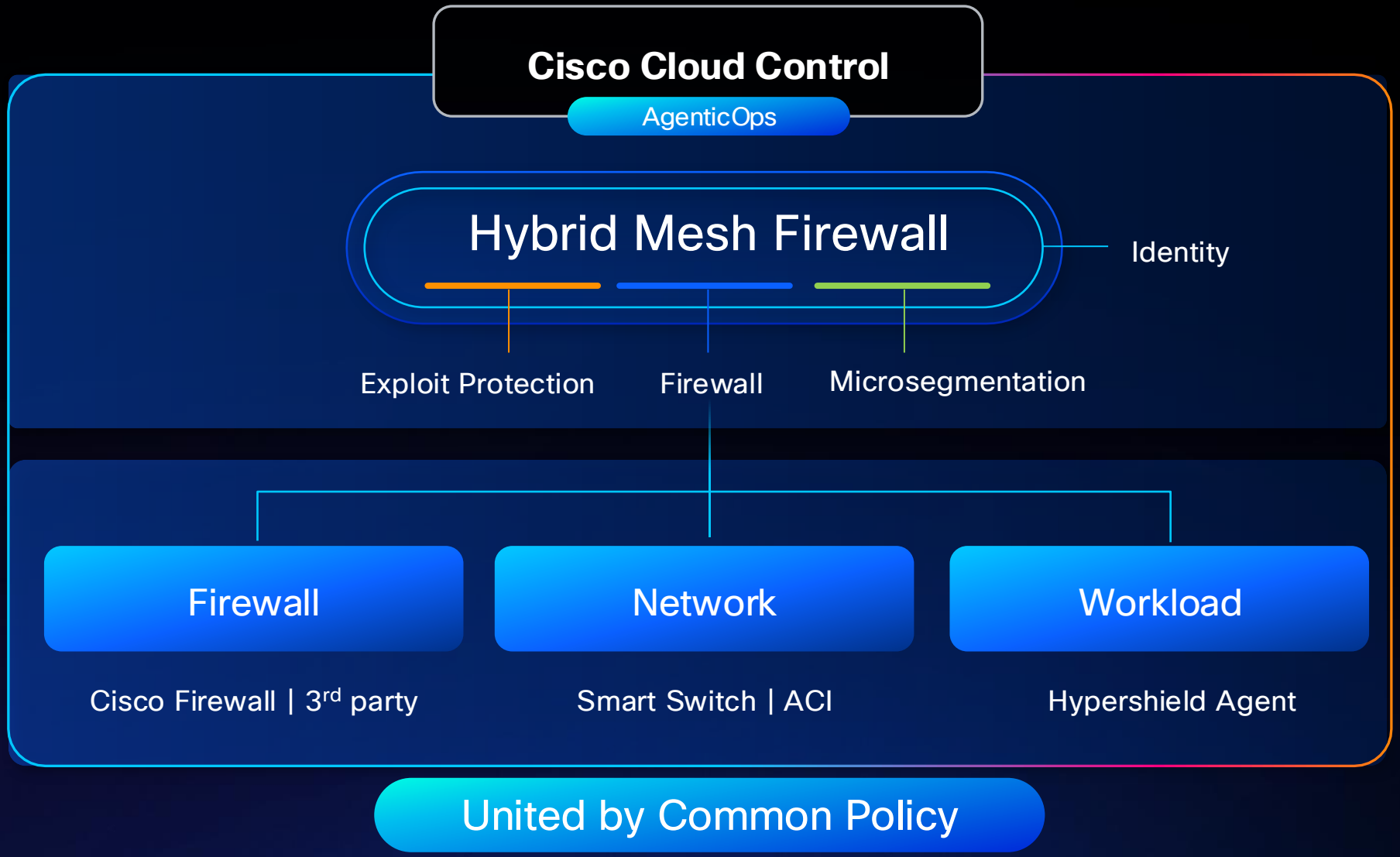


© 2026 Cisco and/or its affiliates. All rights reserved.

Centralized Policy, Distributed Enforcement

Reference Secure Networking Architecture

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



Secure Infrastructure

Patching takes time

Software Maintenance Upgrade (SMU)

5-6 weeks turnaround

May require reload

Limited coverage

Needs an available fix for CVE

Release-specific

VS

Compensating Controls

Turnaround in days for high priority

Never requires reload

Can cover ~25% non-SMUable

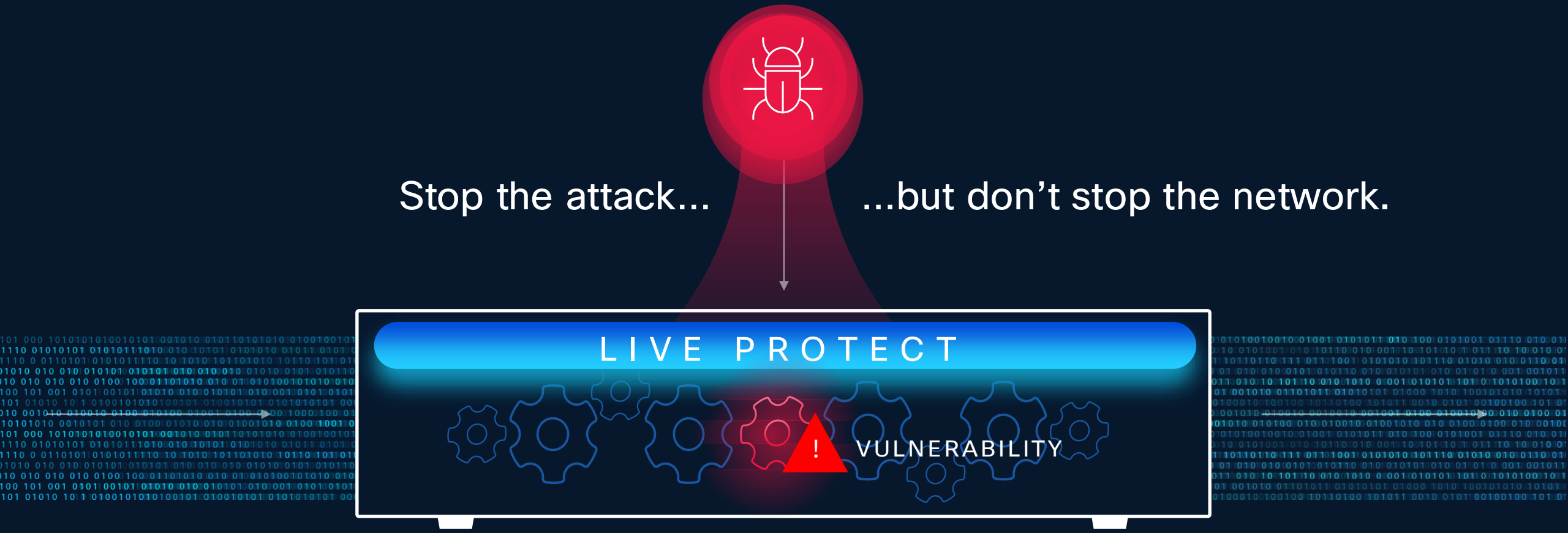
Blocks CVE even when fix unavailable

Works across releases

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

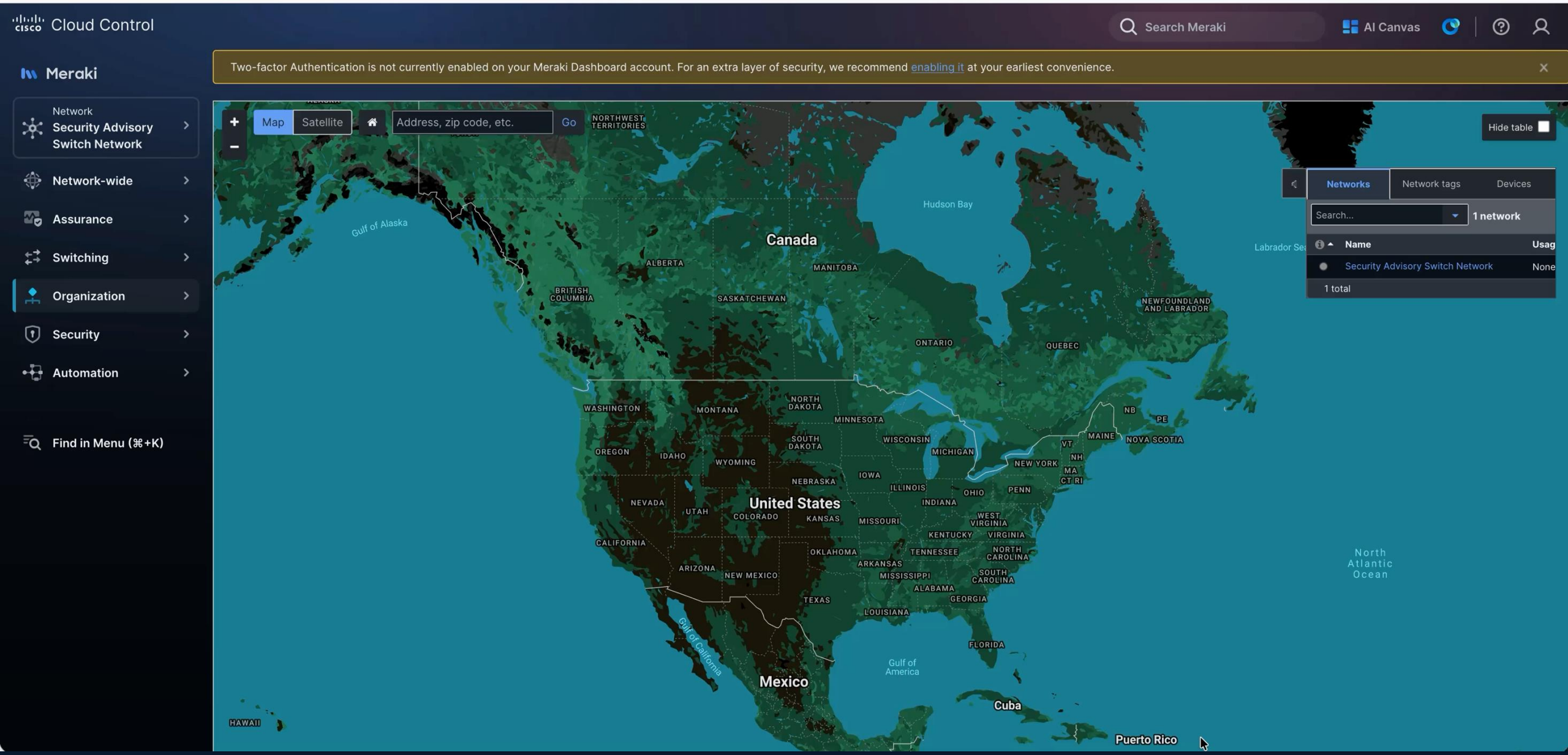
Secure infrastructure - Cisco Live Protect

Vulnerability shielding for Cisco networking devices



In Early Field Trials Now
Switches, Wireless, Routers

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



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

Day-0 threat is shielded, but patching is still needed

The New Scheduled Disclosure Model

NEW

Twice-monthly, fixed days

Security-hardened software publishes on the 1st and 3rd Wednesdays of each month at 1600 GMT.

Seven-day advance notice

The list of covered technologies and platforms is published 7 days ahead. No release planned = no notice.

Two extended maintenance releases per year

IOS XE, IOS XR, NX-OS, Firepower/ASA and SD-WAN; Cisco will not release two core operating system updates on the same day.

Why the change

Frontier AI models and agentic analysis are surfacing bugs across large codebases faster than ad-hoc disclosure was built to absorb – while the gap between disclosure and exploitation has effectively closed.

A fixed cadence with advance notice turns patching into a planned activity that aligns to change control.

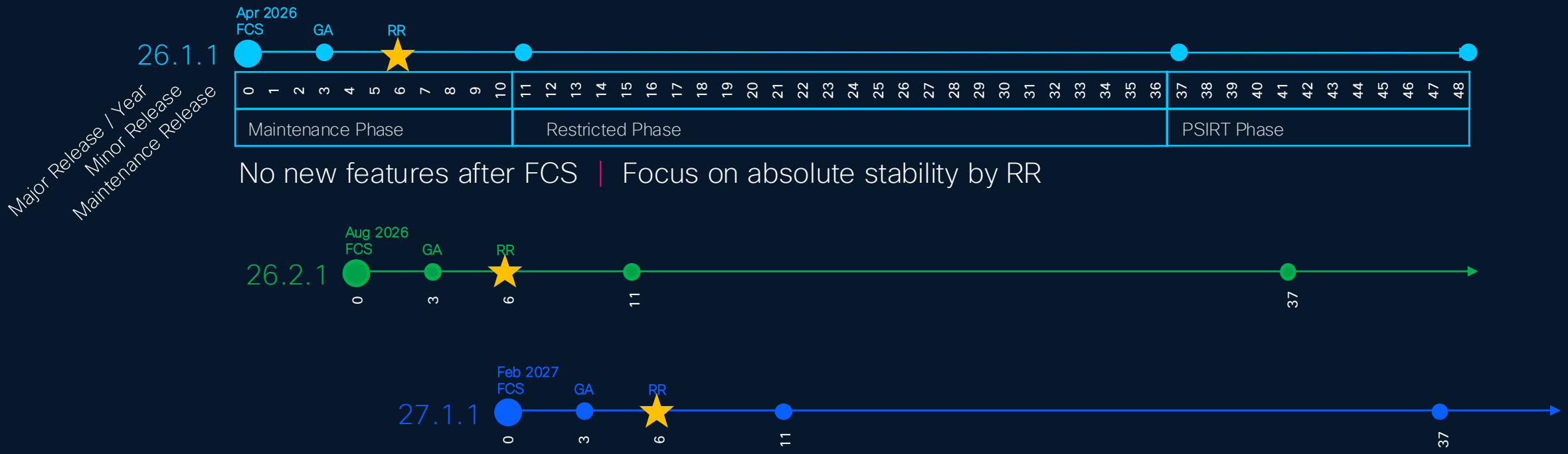
© 2026 Cisco and/or its affiliates. All rights reserved.

New IOS-XE Release Strategy

Longer time between OS upgrades with fewer operational distractions

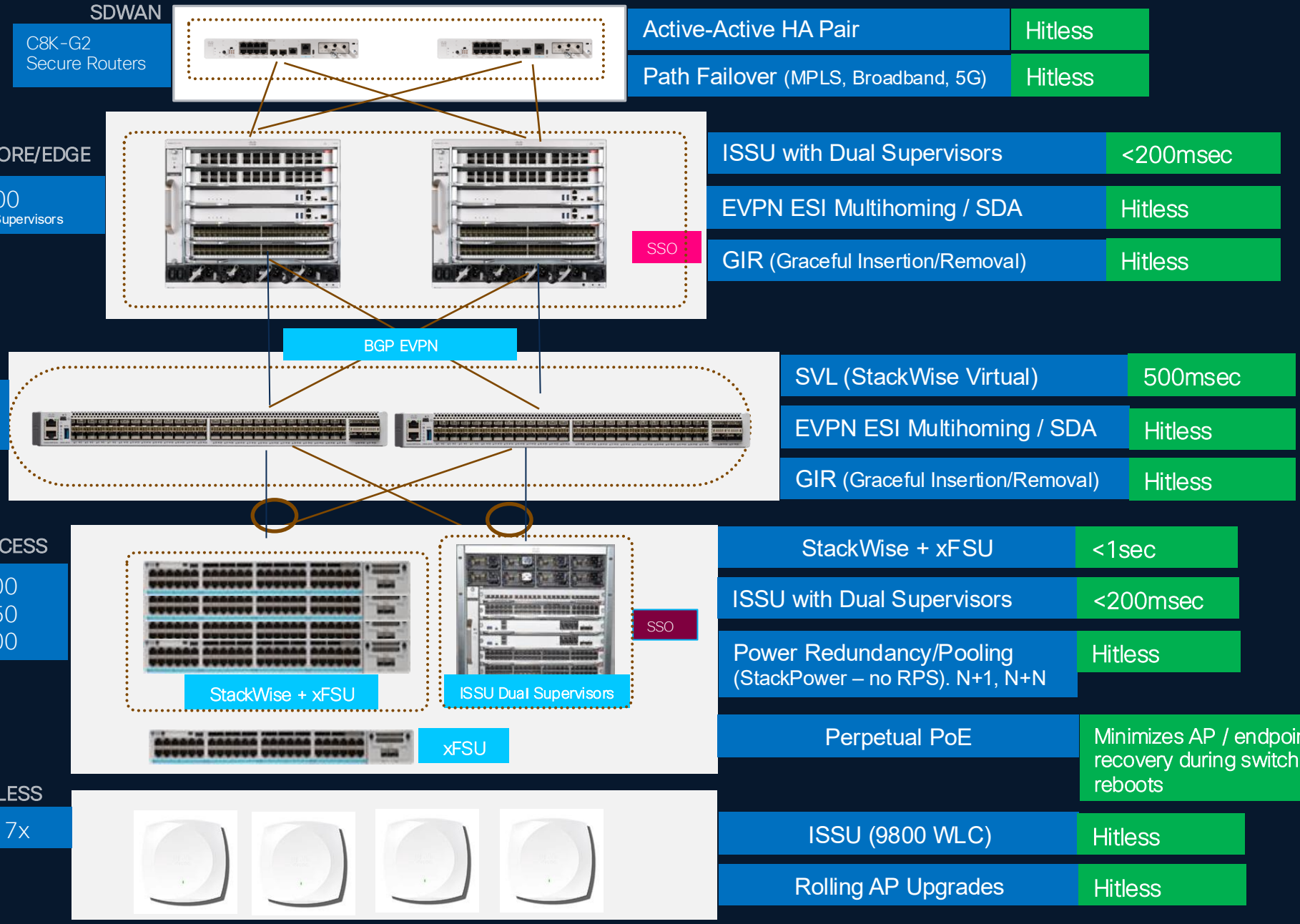
2
Extended Maintenance Release / Year (48mo Support)

6m
Gap between Recommend Releases



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

High-Availability Campus



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

The Next Gen xFSU on C9350 Smart Switches

Achieving **Sub-sec downtime** for upgrades and reloads

Upcoming Support
Standalone IOS XE 26.1.1
Stack CY26Q3

What's New in C9350 xFSU

Control Plane Reload Now 3x Faster

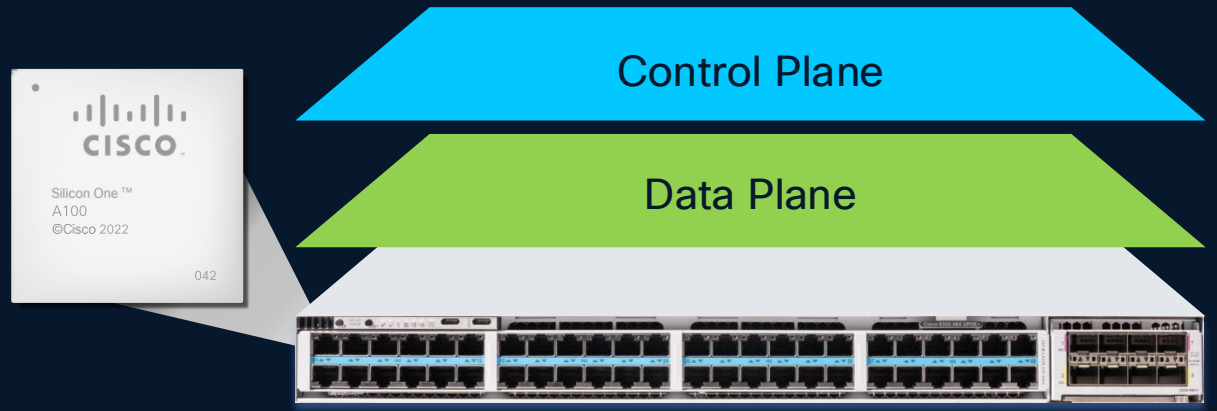
C9350 uses ***kexec-based reload*** instead of ROMMON.
This reduces bring-up time from **3 min to just *1 min*.**

S1 ASIC Preservation Minimized Downtime

Unlike UADP, S1 ASIC isn't fully reset.
Downtime limited to traffic ***impacting registers***.

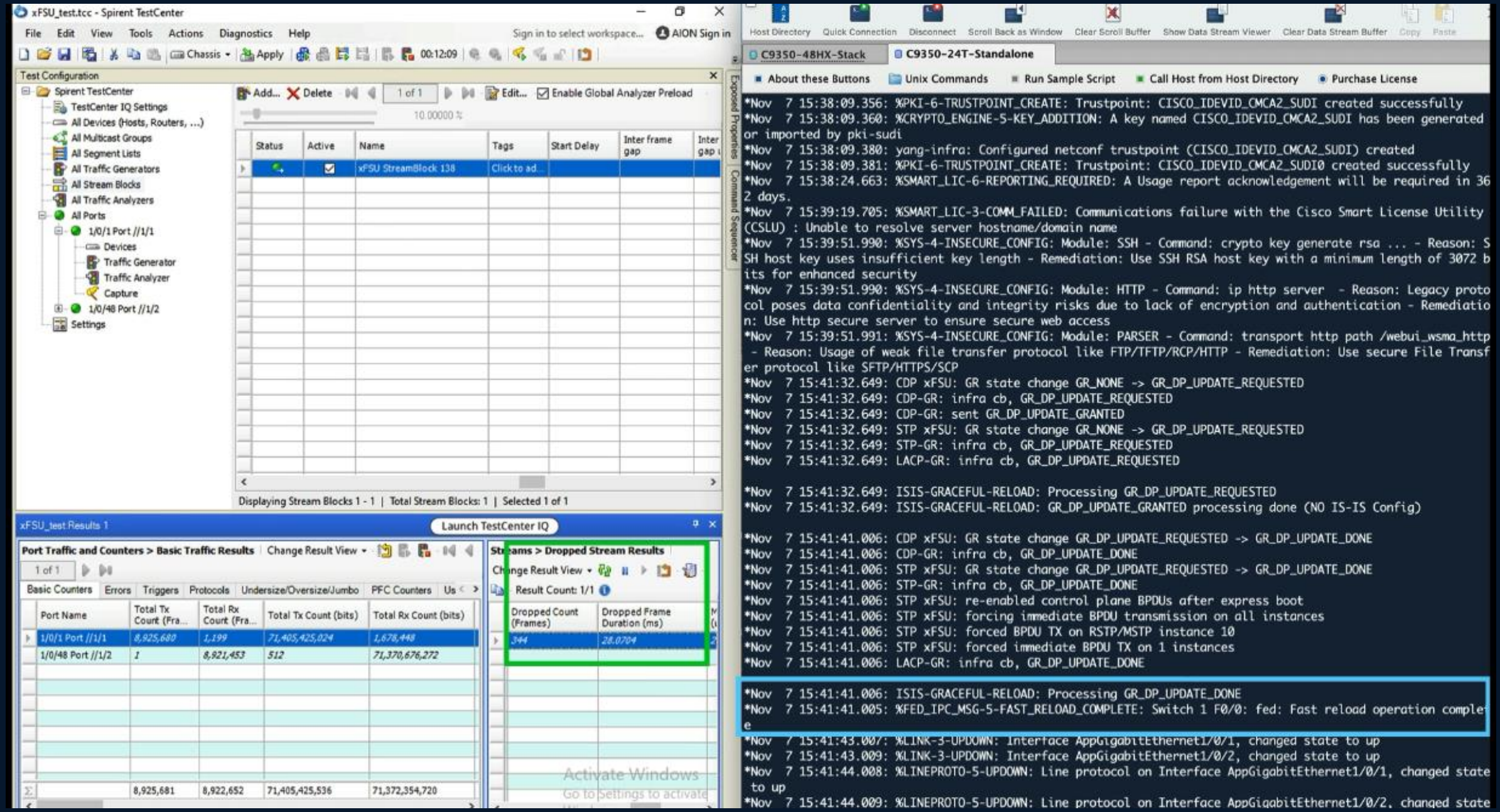
Layer 2 Resiliency with STP Offload

STP offload to NPU Host ensures ***uninterrupted BPDU*** transmission.
This allows xFSU support on Layer 2 roots.



Performance Breakthrough
<1 sec Downtime

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



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

PQC Ready

Cisco Post Quantum Cryptography

26.2.1 / 26.2.2

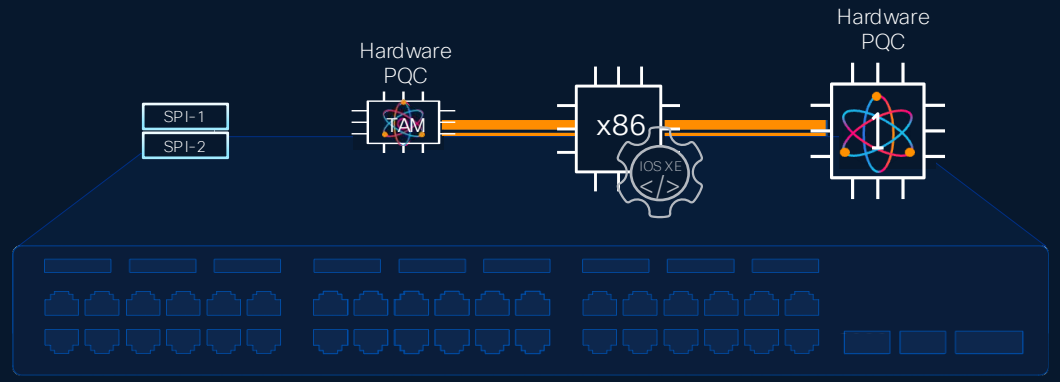
Cisco Modern Campus is Quantum-Resistant

Securing the Device

Step 1: Image Signing & Secure Boot

Cisco Trust Anchor Module on FPGA chipset:

1. Verifies PQC-signed Rommon
2. Verifies unmodified IOS XE
3. Protects the datapath between TAM and CPU



Securing the Data

Step 2: Quantum-Resistant Key Exchange & Data Encryption

Cisco Trust Anchor Module on FPGA chipset:

1. Quantum-resistant key exchange

HW data encryption on Silicon1 chipset

2. Quantum-resistant data encryption

C9350 | C9550 | C9610 | WiFi 7 | G2 Routers

1. Rommon verification using LMS
2. OS image signing and verification using ML-DSA
3. Bus encryption between CPU and TAM using ML-KEM
4. SSH key exchange with ML-KEM
5. IKEv2 with ML-KEM
6. EAP-TLS 1.3 with ML-KEM
7. TLS 1.3 with ML-KEM

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

The Modern Campus Portfolio



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 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.

C9350 Portfolio Expansion

Providing fiber-to-the-desktop, collapsed core, and more ways to power Wi-Fi-7

Available Q3CY26
1G Fiber Downlinks



Cisco C9350-48S
48x 100Mbps / 1G SFP



Cisco C9350-24S
24x 100Mbps / 1G SFP

Q4CY26
mGig Fiber Downlinks



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



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

Available now
mGig Copper Downlinks



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



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

Q4CY26
mGig Copper Downlinks



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

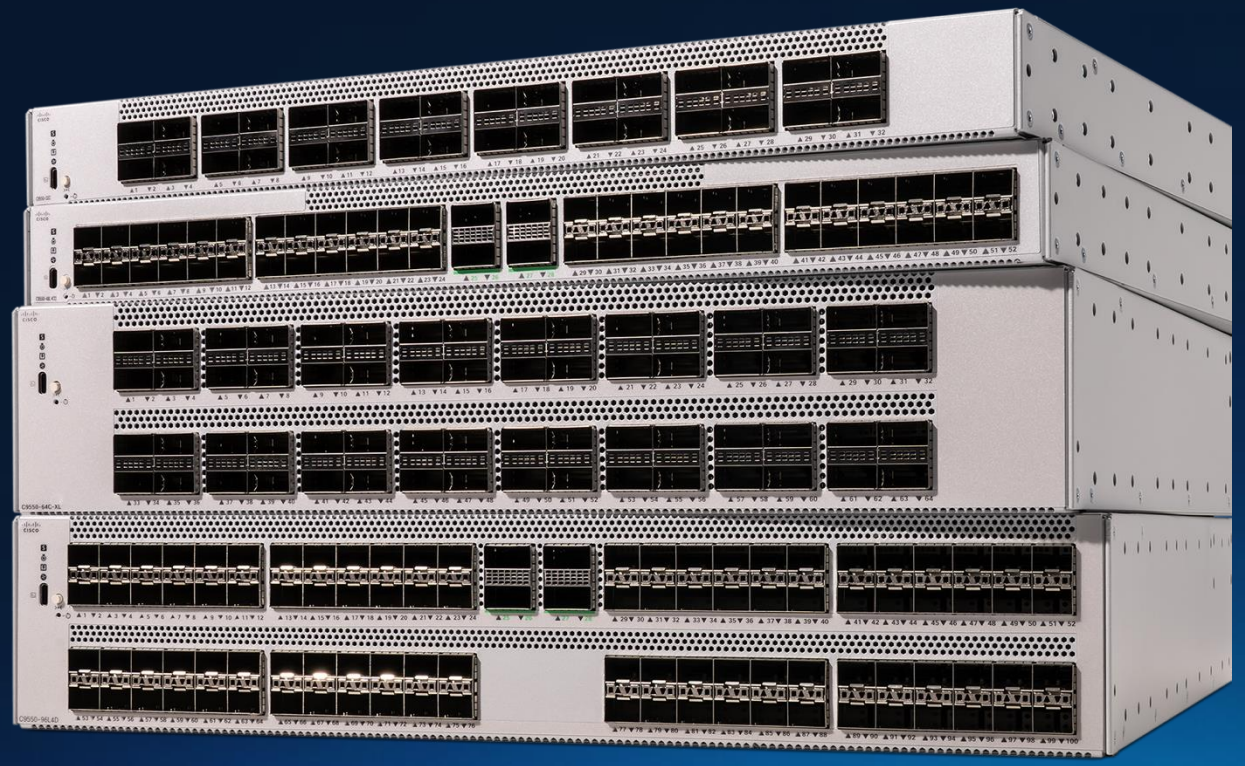


Cisco C9350-48HM
48x 2.5G w/ 90W UPoE+

© 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.

INTRODUCING

Cisco C9550 Series Smart Switches

Powerful, secure, easy to manage



Cisco Silicon One NPU2.0: industry's most powerful, programmable ASICs

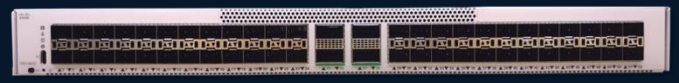
High-performance, Next-gen Multi-core x86 CPU & DRAM

High-throughput, Secure On-device Application Hosting

Cisco IOS XE w/ Cisco Smart Stacking (NGSVL)

Post-Quantum Secure Boot & Trust Anchor

Orderable



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



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



C9550-96L4D
96x 1/10/25/50G + 4x 400G (2RU)



Coming Soon



C9550-32C
32x 40/100G

C9550-64C-XL
64x 40/100G (2RU)
+8GB HBM with on-chip buffers



Wi-Fi 7 for the Modern Campus

Coffee shops	Residence halls	Classrooms	High Density	Outdoor	Highest Density	Stadiums, large **venues**
				New		
						
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	Available	Available	Available

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

cisco

Cisco Campus Gateway



CW9800H1-MCG

Scales up to 12,000 APs and 64,000 clients

Throughput up to 100 Gbps

New



CW9800L-MCG

Scales up to 1,000 APs and 10,000 clients

Throughput up to 10 Gbps

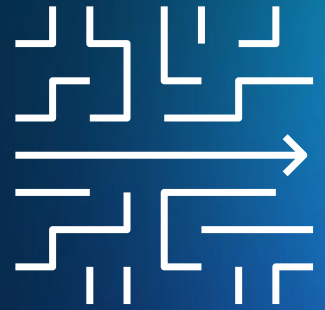
Cloud management simplicity with L3 roaming scale

Easy migration for existing WLC architectures

Supports clustering and disaster recovery failover

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

Cloud Management Updates



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

Cloud management across the networking portfolio



Wireless

Full WiFi6E & WiFi7 support

Campus Gateway for L3 roaming



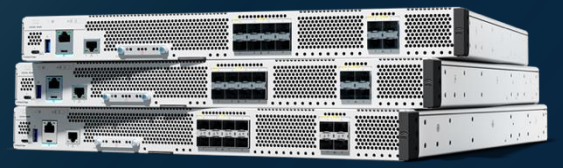
Switching

C9200, C9300, C9500 switches

New | C9350 & C9550

New | C9400 & C9600 Modular switches

New | IE3500 OT Series



Routing

New | Secure Routers

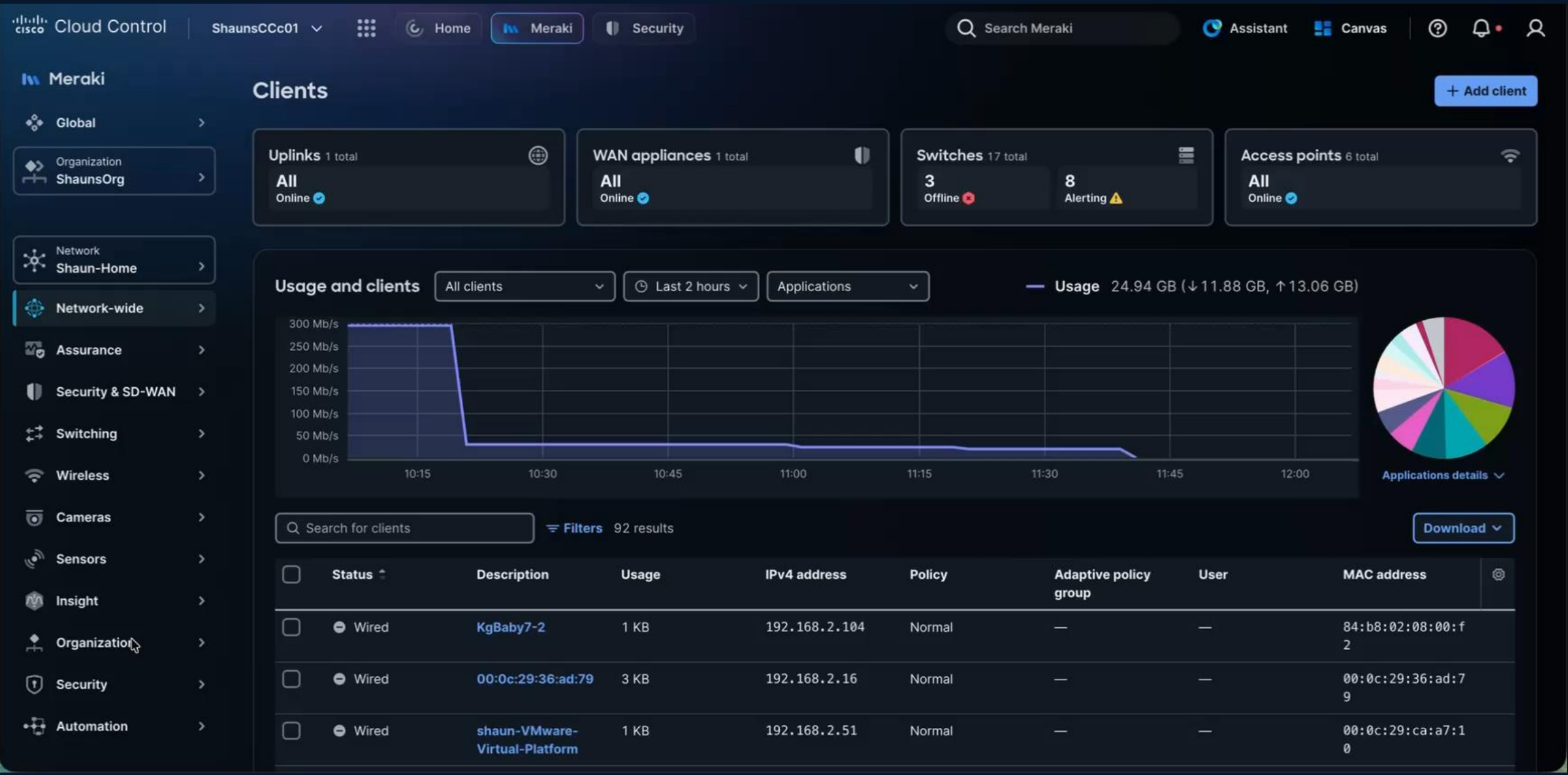
Cellular Gateways for 5G connectivity

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

C9000 Switches are now cloud-managed, but what about every IOS-XE feature?

Introducing CLI Profiles

Beta Coming Soon



Introducing

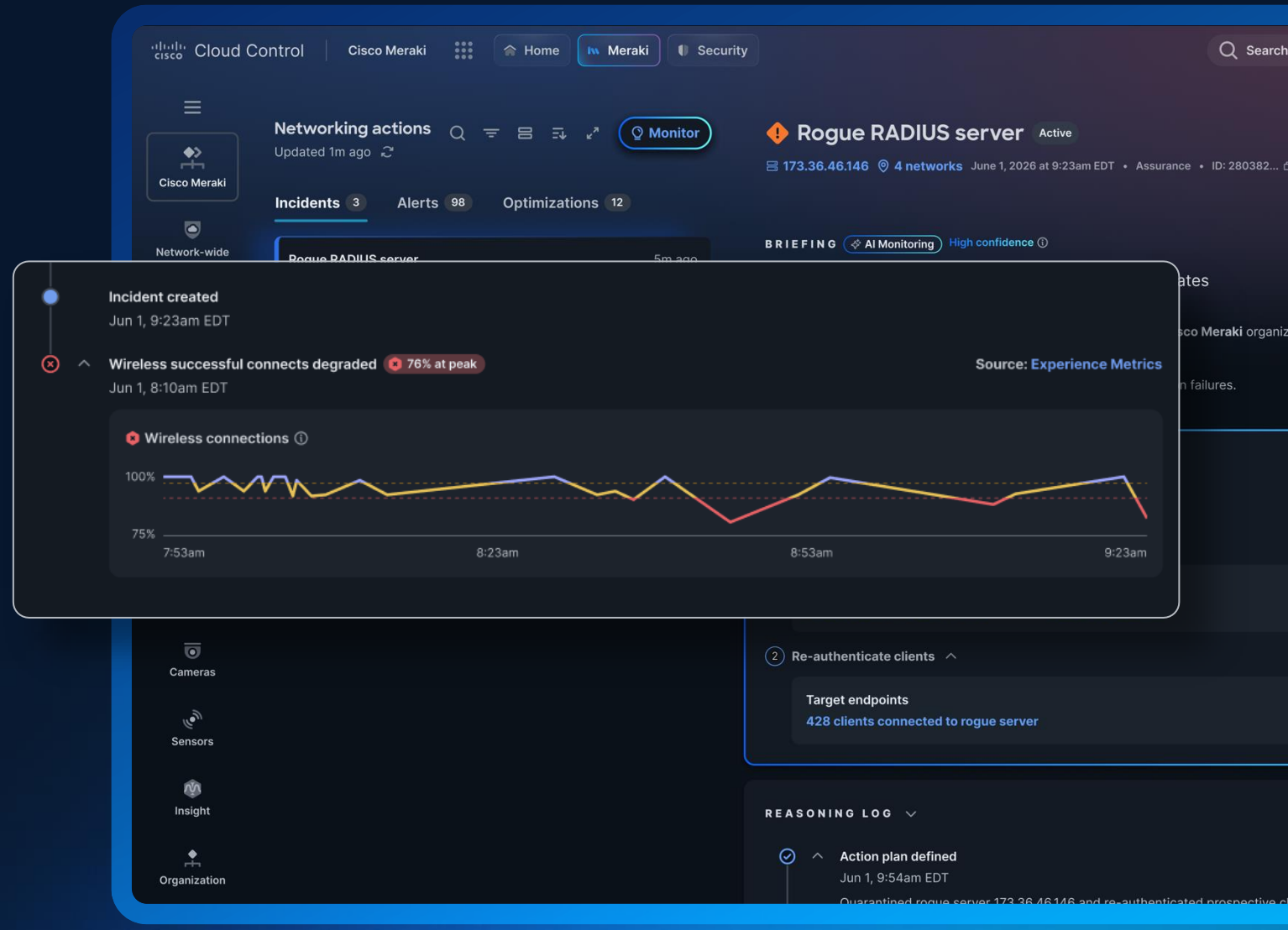
Enhanced experience metrics

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

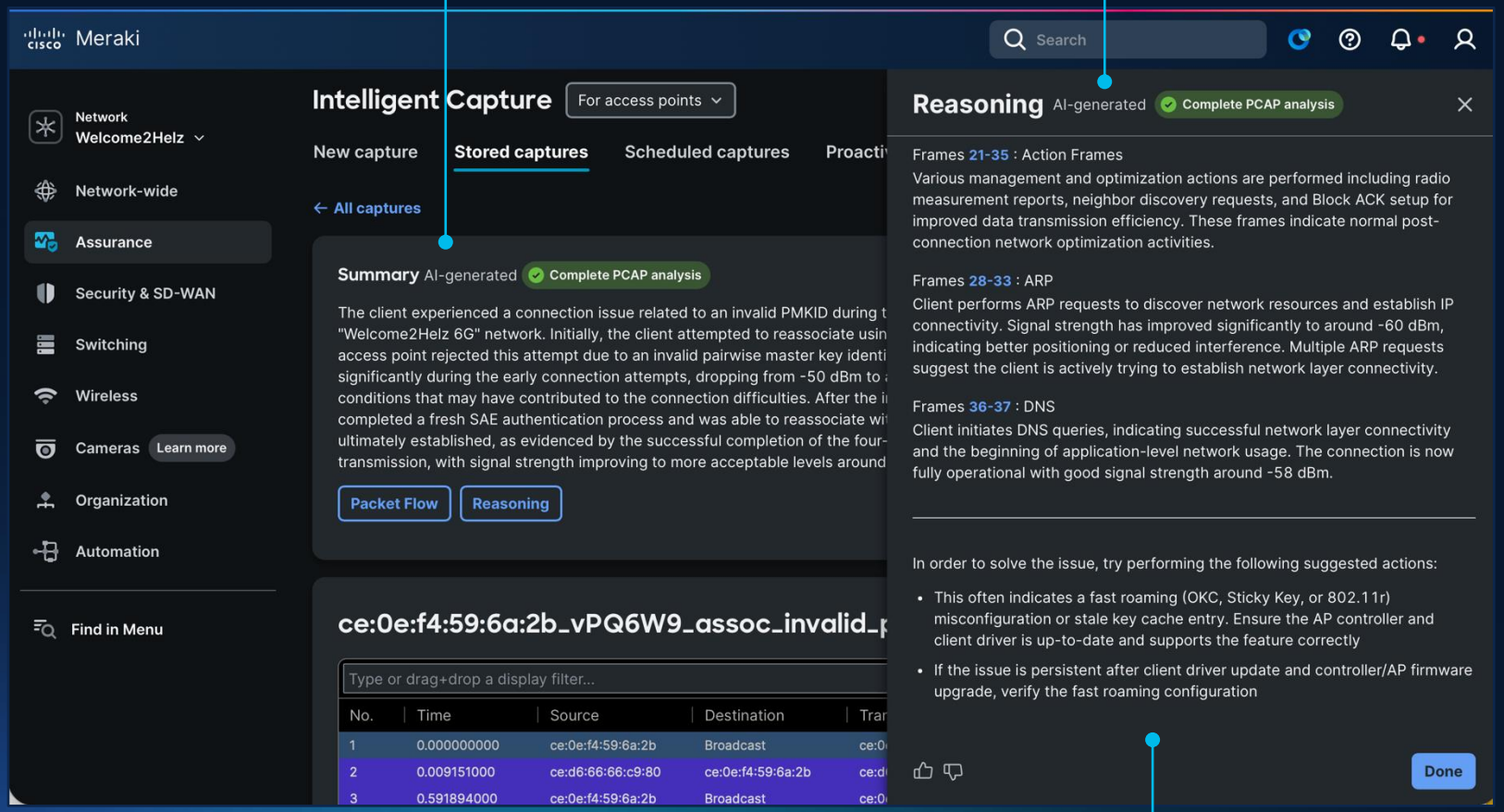


© 2026 Cisco and/or its affiliates. All rights reserved.

Introducing

AI Packet Analyzer

- Automatically seizes the moments of client failure and uploads PCAP files to the AI cloud
- Quickly analyzes PCAPs with AI summary
- Isolates fault with reasoning view or visually with packet flow view
- Actionable recommendation provided to resolve issue



Network
Meraki San Francisco SFO12
Secure Connect
Network-wide
Assurance
Security & SD-WAN
Switching
Wireless
Systems Manager
Cameras
Sensors
Insight
Organization
Security
Automation
Access Manager
Find in Menu (⌘+K)
English

Overview

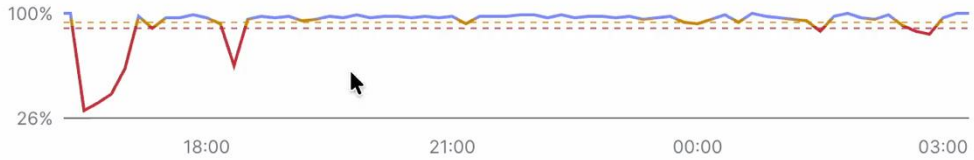
Experience metrics | Network services | Network health score

Custom | 26/02/2026, 16:15 → 27/02/2026, 03:19 | Access point | SSID



Successful connects (above 90%)

91.33%

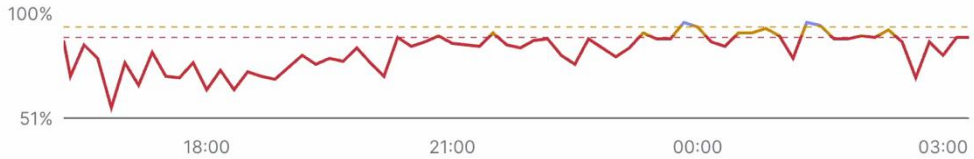


Failure contributors

Association	56.67%
Authentication	35.00%
DHCP	6.92%
DNS	1.41%

Time to connect (under 5 seconds)

81.47%

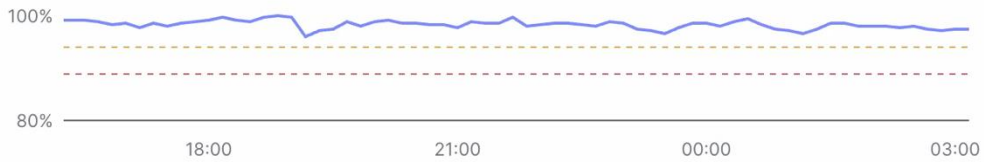


Delay contributors

Association	8.97%
Authentication	15.53%
DHCP	55.29%
DNS	20.21%

Capacity (above 90%)

98.27%



Failure contributors

Co-channel interference	69.03%
Non-Wi-Fi interference	16.34%
High traffic	14.63%

Coverage (above 95%)



Failure contributors

Give feedback

Introducing 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

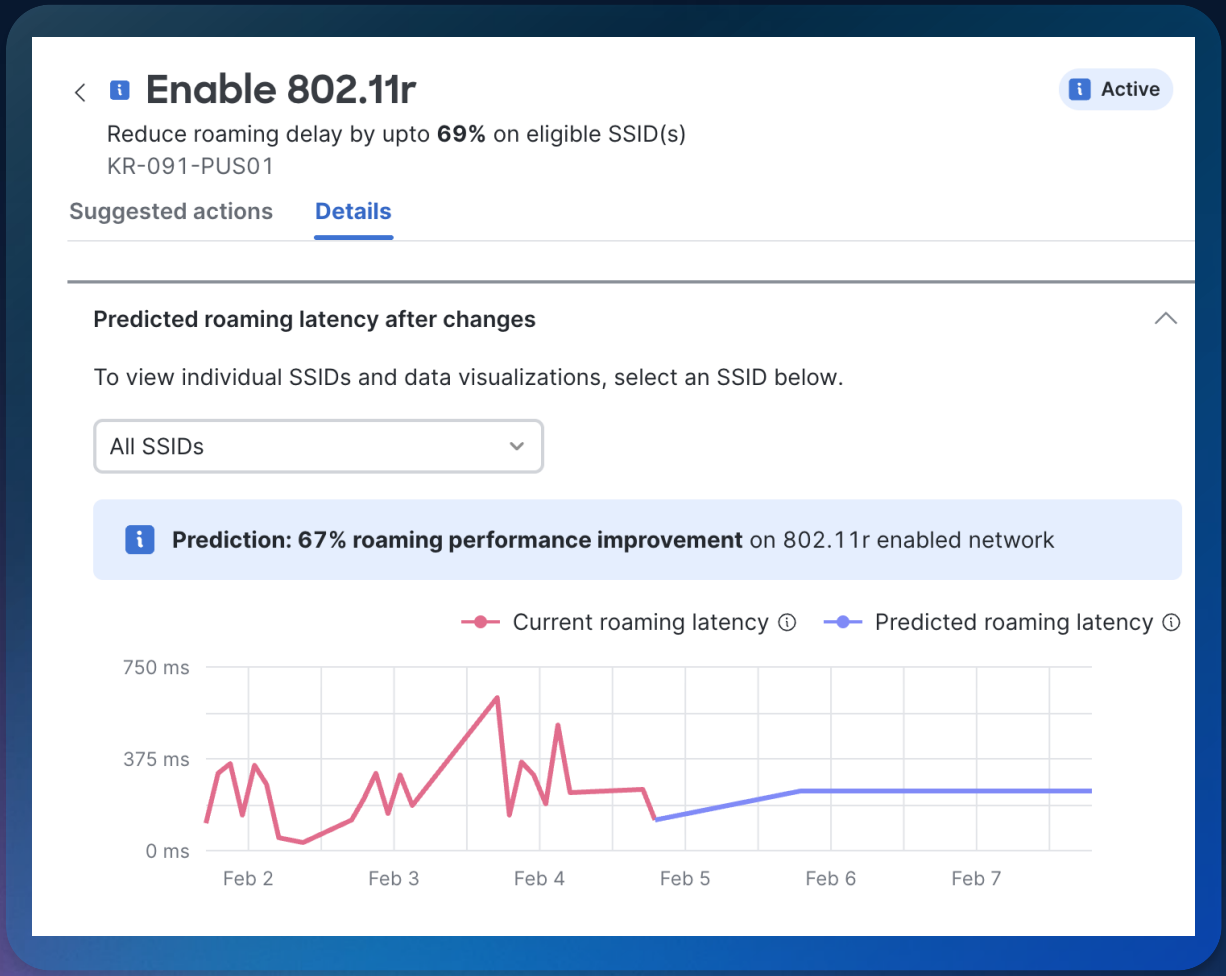
Types of recommendations

Available

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

Coming Soon

- Coverage hole mitigation
- Transmit power range optimization
- 5-GHz band and channel list optimization



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

Network
HQ-Uranus-Mesh-VLAN-Testbed
Network-wide
Assurance
Security & SD-WAN
Switching
Wireless
Insight
Organization
Automation
Access Manager
Admin
Find in Menu (⌘+K)

Alerts

Started last week

Configure alerts

Alerts 219 | Optimizations 12

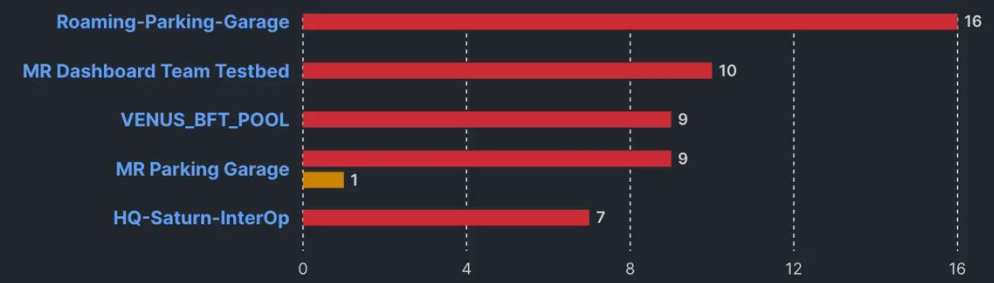
Alerts triggered over time

Active | Dismissed | Resolved | 219 All networks | Alert Type | Device Type | Device Tags | 219 matching results | Refresh Less than 1 minute ago

154 Critical | 65 Warning | 0 Informational

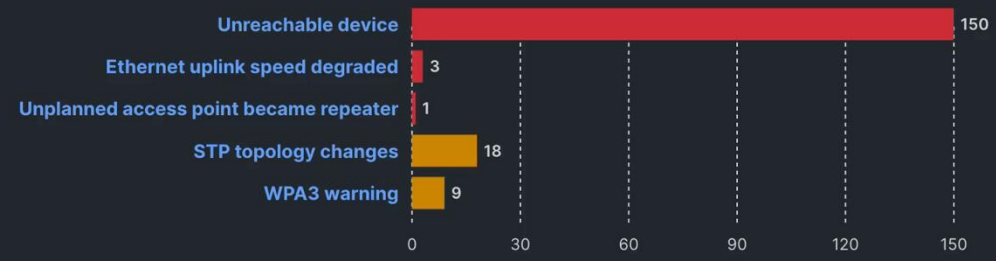
Top alert counts

By network



View details

By alert type



View details

Active alerts

Severity	Alert type	Alert count	Device types	Network count	Last alerted	Category
	Unreachable device	150	MS MR +3	73	Jan 29 01:29 UTC	Connectivity
	Ethernet uplink speed degraded	3	MR Cat...	3	Jan 28 22:23 UTC	Device Health
	Unplanned access point became repeater	1	Cat...	1	Jan 27 15:38 UTC	Device Health

Give feedback

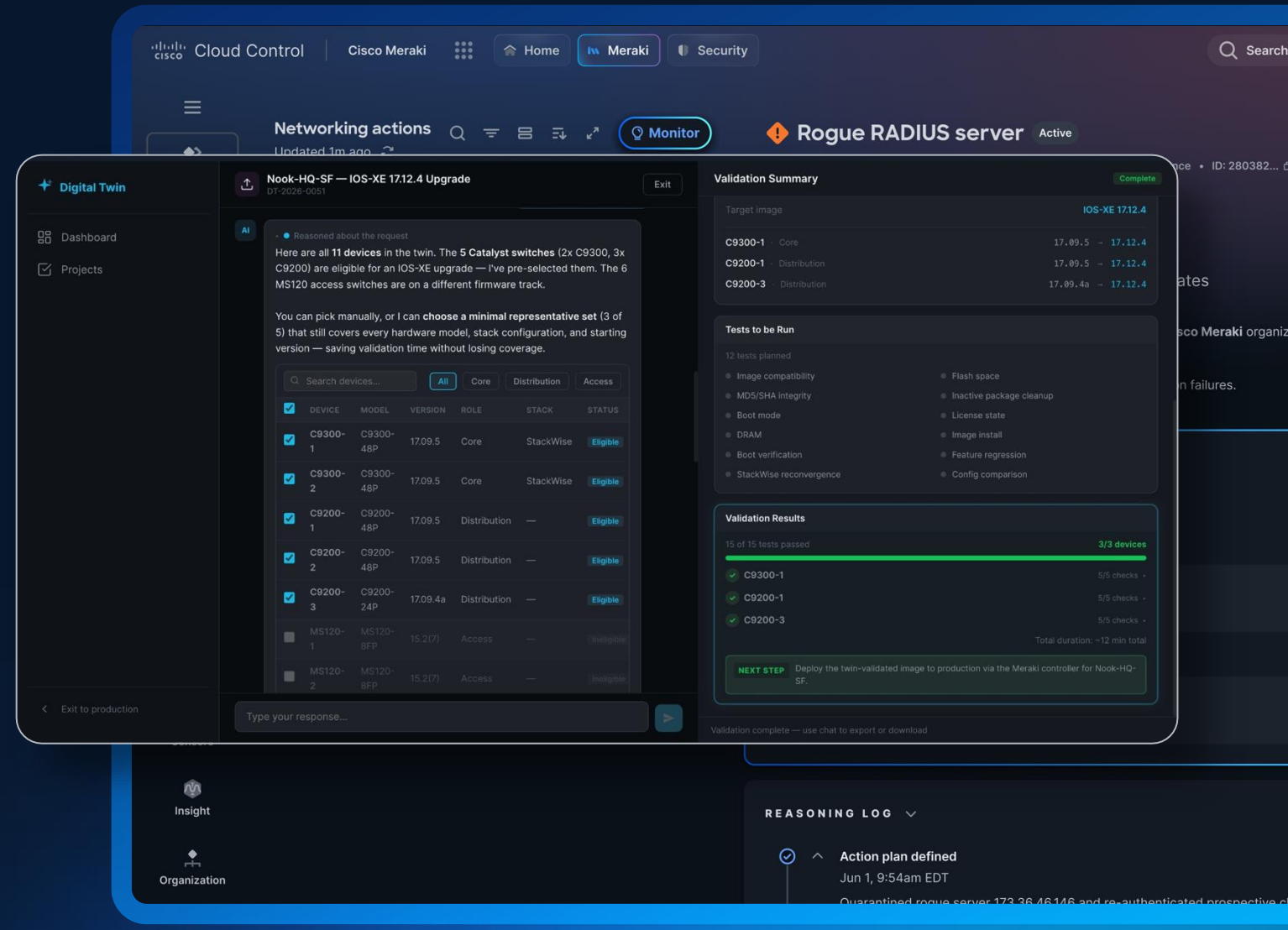
English

Alpha Coming Soon

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.

Modernize the Network

Scale for the AI Era

- Network performance, agility, and security must evolve to keep up
- Cisco has a full suite of campus products ready for these modern challenges

Proactive Cyber Defense

- Blocking Day-0 exploits is critical
- Structured, seamless patching to minimize disruption
- Plan for PQC today



Security Fused into the Network

- Perimeter FWs are not sufficient for lateral movement
- The network has visibility, is pervasive, and provides east-west segmentation

Operational Transformation

- Complete cloud-managed portfolio
- No feature compromise - Full IOS-XE feature set
- Intelligent assurance and proactive prediction for greater network stability

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

CISCO Connect

Thank you

