Cisco Tech Day

Denver

March 3, 2026

Cisco Tech Day
Denver

Unlocking the future of Secure Networking

Olivia Wolf

Solutions Engineer

Another massive technology disruption

AI is bringing changes and challenges

1,000s

AI Agents per enterprise expected

#1 risk

AI-enhanced malicious attacks

64%

of orgs face IT skills shortage by 2026

Is your Campus Network AI ready?

For explosive traffic, for increased security risks, for more complexity

Architecture for the AI-Ready secure network

AgenticOps
for operational simplicity

Security
fused into the network

Scalable devices
ready for AI

AgenticOps for operational simplicity

Unifying Catalyst & Meraki

Catalyst		Meraki
Catalyst Center	MANAGEMENT	**Meraki Dashboard**
Catalyst License	LICENSE	**Meraki License**
Catalyst Hardware	CISCO HARDWARE	**Meraki Hardware**

Our unified platform

PLATFORM

Management

Assurance

API / Integrations

Intelligence

HARDWARE

Smart Switches

Secure Routers

Wireless

Industrial IoT

cisco

A unified OS for cloud and on-prem management

The foundation of operational simplicity

Fast, consistent out-of-box provisioning

- Simple day 0 operations
- Simple, streamlined onboarding
- Automated port config
- Secure, fast onboarding of devices

Expanding IOS XE capabilities available in the cloud

CLOUD MANAGEMENT AVAILABLE NOW

1H'26


C9300L


C9300


C9300X


C9200L


C9500


C9200/CX


C9300LM

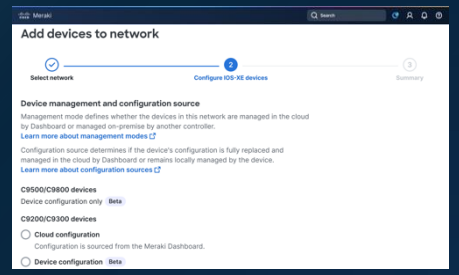

C9350


Modular

cisco

Large campus cloud capabilities

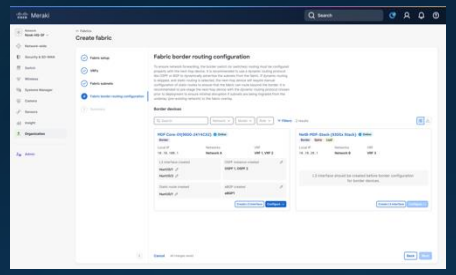
Powerful Switching Capabilities



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

BETA

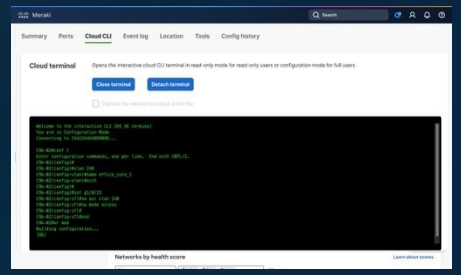
Fabric for Secure Networking



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

BETA

Cloud CLI for Flexibility



Simplify onboarding and flexibility with operating mode options and Cloud CLI

AVAILABLE NOW

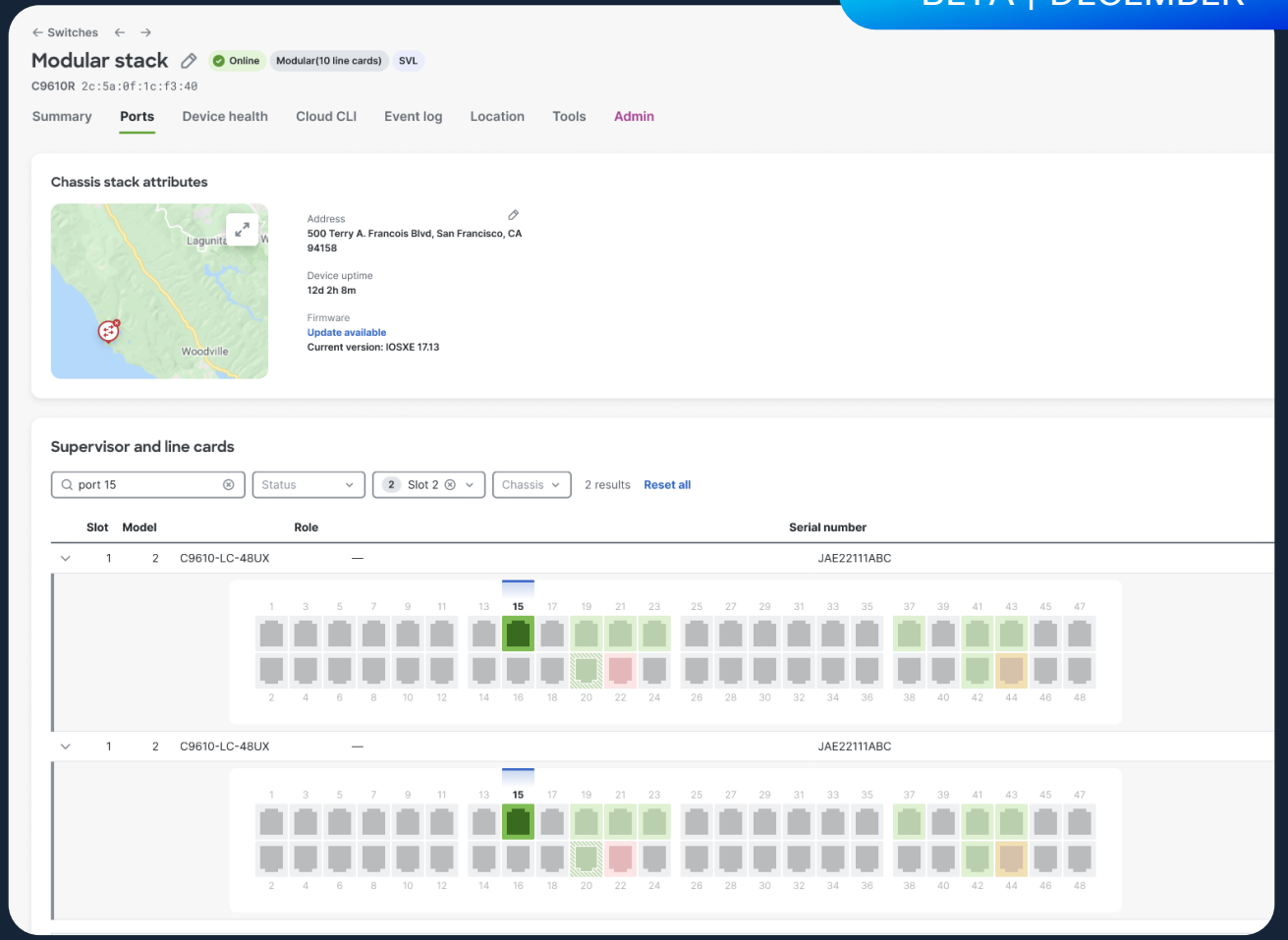
Cloud-managed switching

Cloud management for modular switches

Sophistication, simplicity, and scale, in a single view

Expanding cloud management support into modular core switches

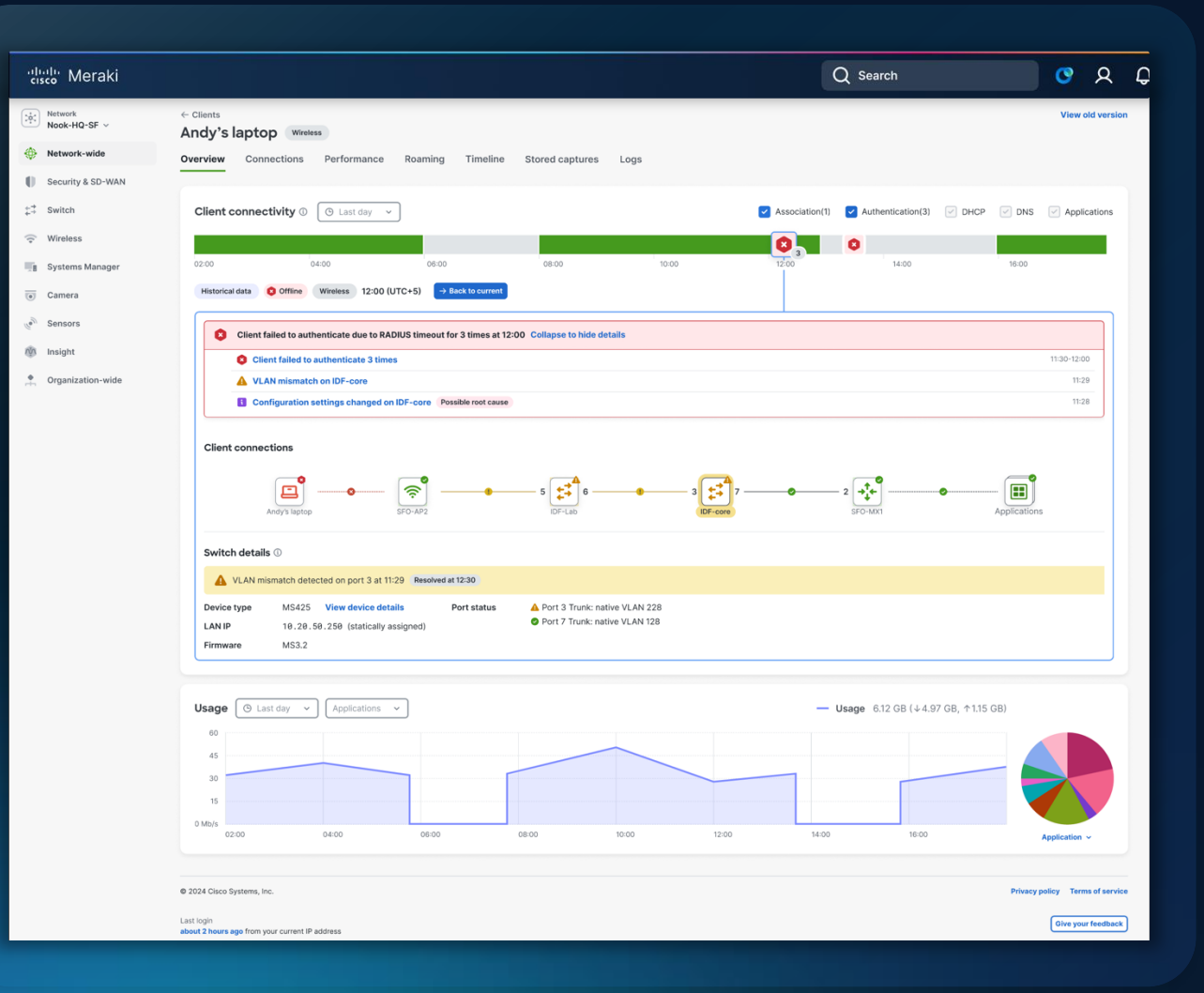
BETA | DECEMBER



C9610 Smart Switches

Assurance across every digital experience

- Deep visibility across both owned and unowned networks
- AI-powered insights surface experience-impacting issues instantly
- Closed-loop workflows trigger automated remediation
- AI Assistant accelerates root cause analysis end-to-end

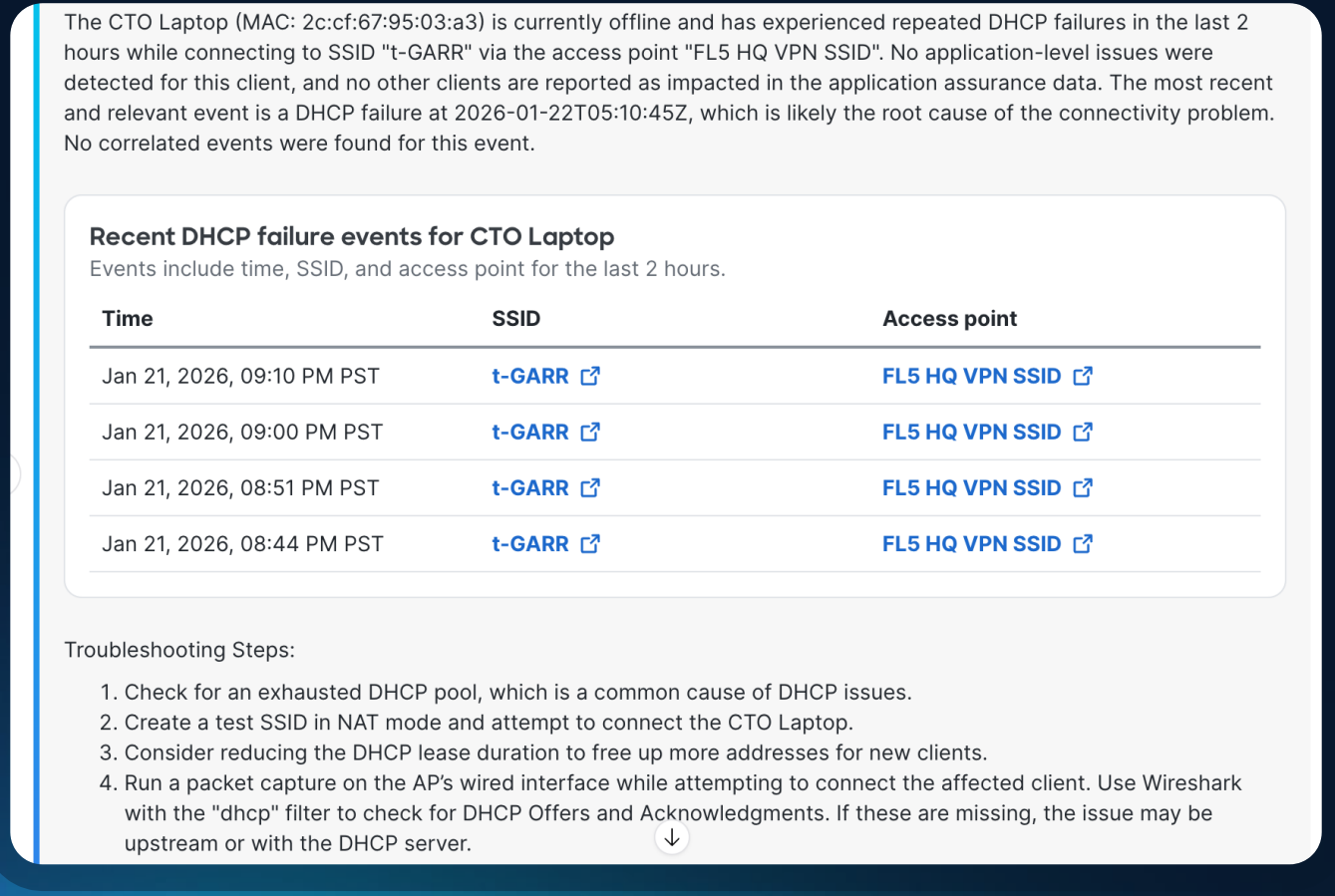


Autonomous Troubleshooting

Delivers credible root cause and remediation. In minutes.

Beta CYQ2 26

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

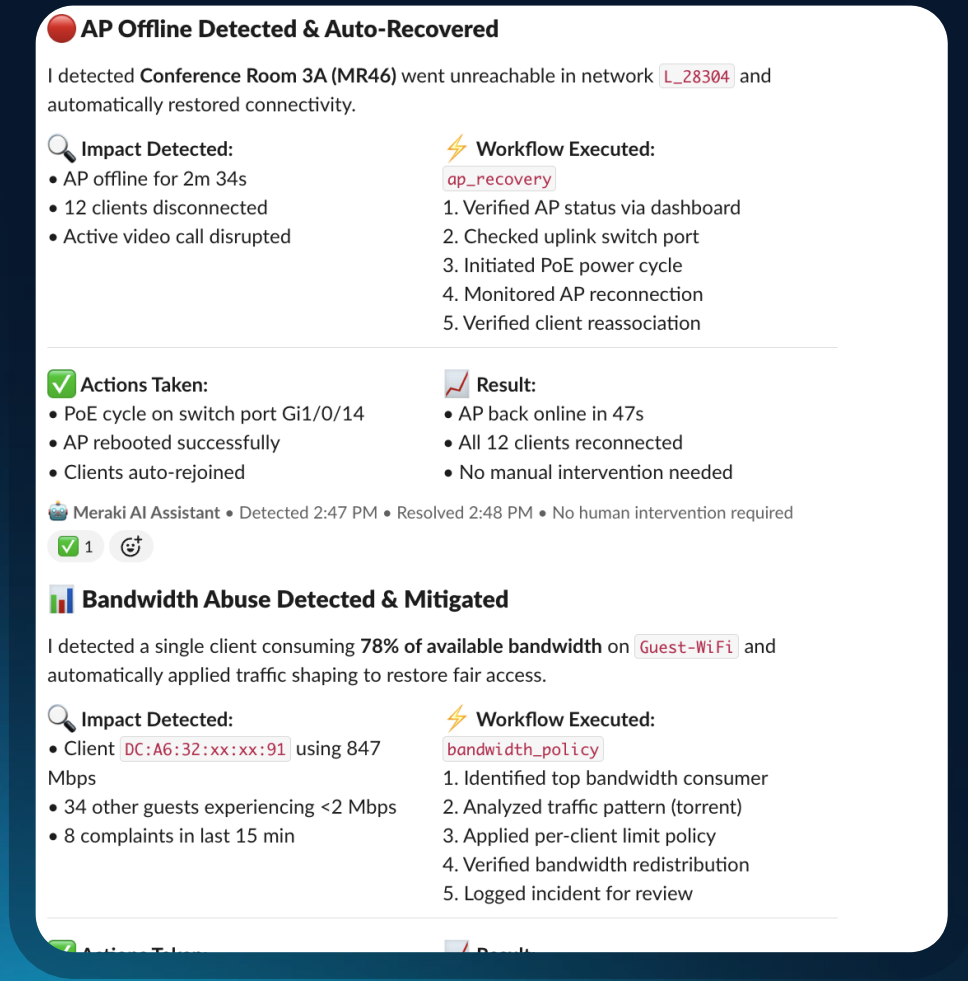


Continuous Optimization

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

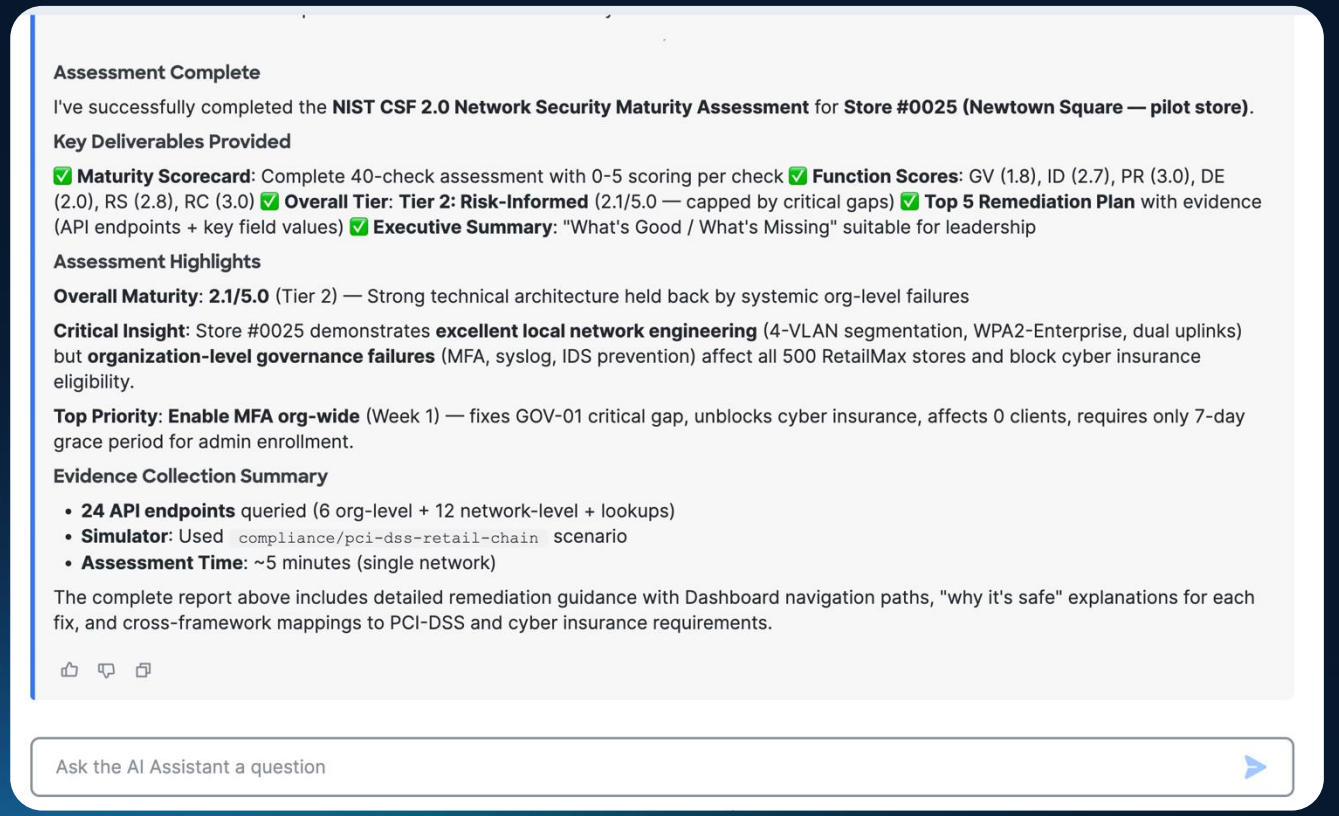


Trusted Validation

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



Security fused into the Network

New threats attack networks directly

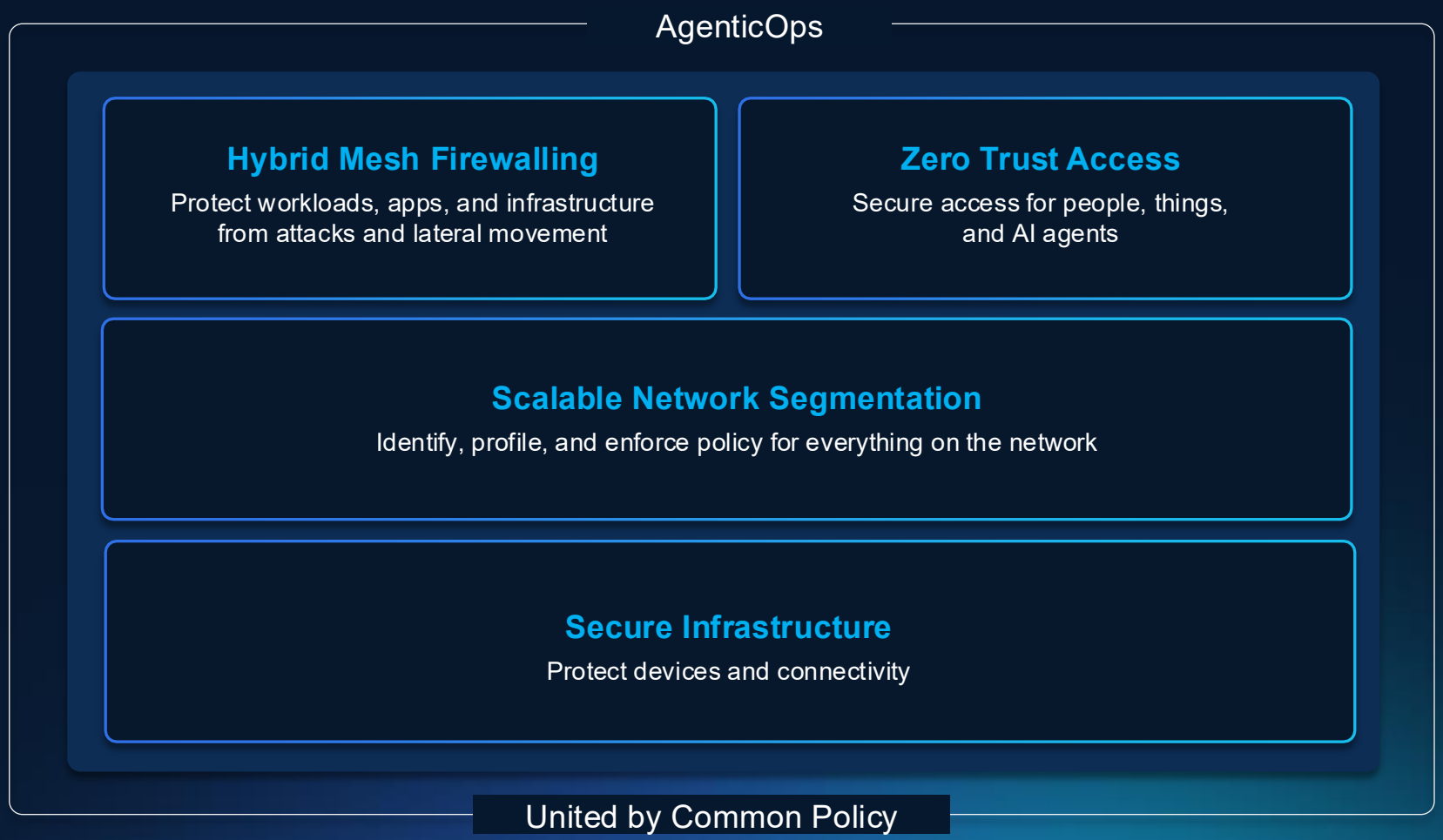
Attacks on Infrastructure

Exploits like Salt Typhoon that target unpatched software on key infrastructure

Attacks on Encryption

“Harvest now, decrypt later” attacks where encrypted data is extracted and stored, anticipating quantum computing.

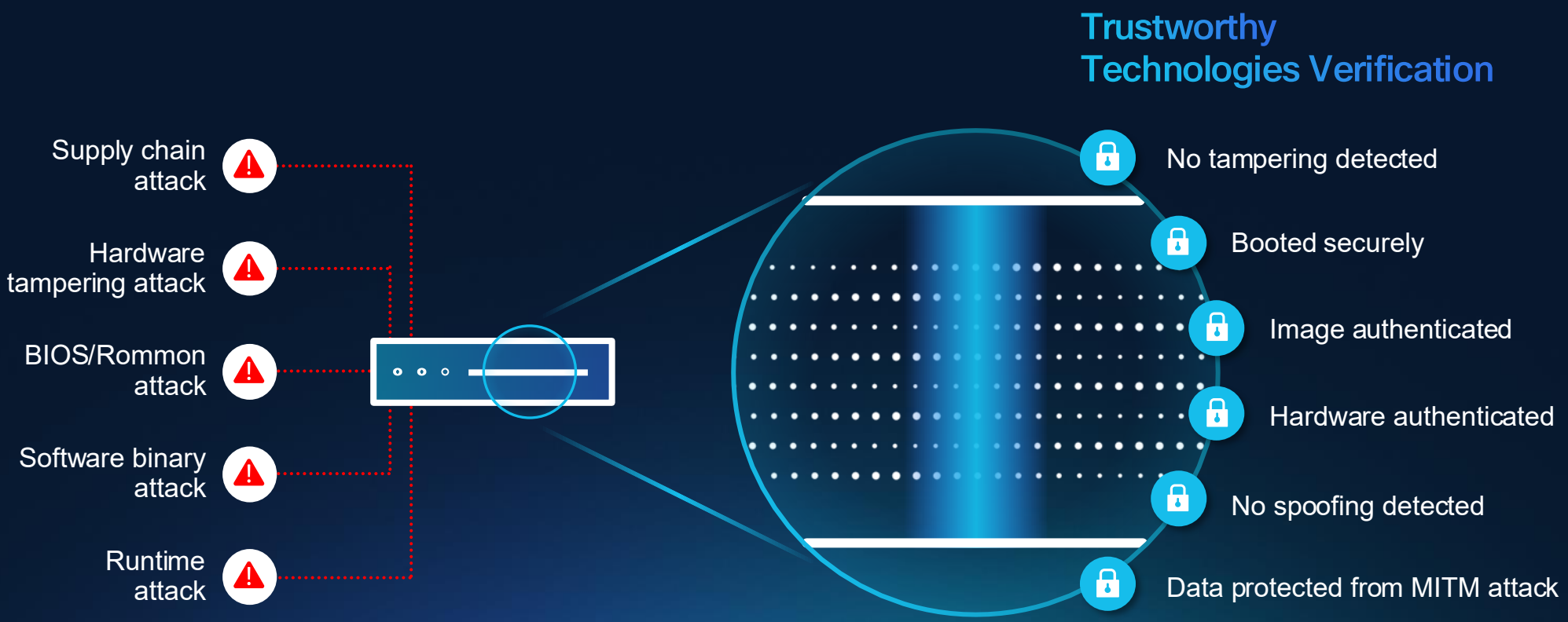
Reference design for fusing security into the network



- Identity-first
- Continuously verified
- Enterprise-wide policies
- Comprehensive Threat Intel
- Distributed Enforcement

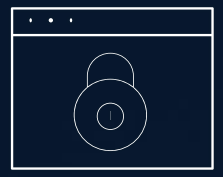
Secure Infrastructure: Securing the device

Secure from hardware to software, from boot time to runtime



Secure Infrastructure > Resilient Infrastructure

Enhancing baseline security posture out-of-the-box



Security by default

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

Deprecates then removes insecure protocols in IOS-XE

Real-time threat response

Immediate shielding from vulnerabilities without disrupting operations

LiveProtect “shields” to zero-day vulnerabilities

Future-ready resilience

Transparent risk visibility and post-quantum cryptography readiness

Prompts secure data collection with most secure protocols and methods

Secure Infrastructure - Cisco Live Protect

Vulnerability shielding for Cisco networking devices

Network Device Security

Overview | Device vulnerabilities

73 All vulnerabilities

12 Live Protect available for deployment

37 Live Protect deployed

Search | CVSS score | Device family | Live Protect status | Filters | 73 results | Apr 22 2025 09:41 | Rescan

Vulnerability	Details	CVSS	Affected devices	Live Protect	Hits
CVE-2023-20198 New	Web UI Unauthorized Access Vulnerability	10.0	1	Available	—
CVE-2024-20169	Command Injection Vulnerability	9.8	1	Available	—
CVE-2023-20154	SNMP Remote Code Execution	9.8	2	Pending	—
CVE-2023-20049 New	Authentication Bypass Management Interface	9.6	1	Protection	6
CVE-2024-20467	Privilege Escalation via CLI	9.1	1	Observation	5
CVE-2024-20480	SSH Key Management Vulnerability	9.1	2	Available	—
CVE-2023-20177 New	IPv6 RA Guard Bypass	8.6	1	Protection	1
CVE-2024-20508	Privilege Escalation through Configuration API	8.6	2	Protection	3
CVE-2023-20200	CLI Privilege Escalation	8.6	2	Pending	—
CVE-2024-20437	Buffer Overflow in HTTP Server	8.4	1	Observation	8

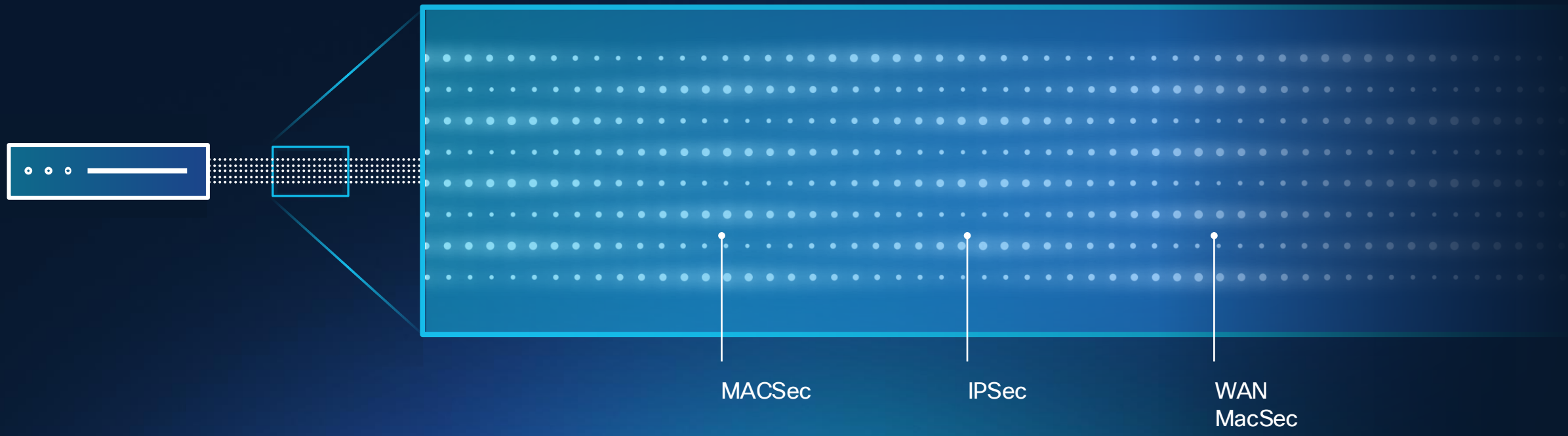
Rows per page 20 | 1-20 of 73 | 1 | 2 | ... | 10

Securing network connectivity

Secure and protect your data over unowned infrastructure

Post-Quantum Cryptography

Future proof investments | Protect against quantum | Secure sensitive data



Classical methods vs PQC high-level

Classical

- Private Key-Public Key exchange
- Quantum computers could generate the private key
- Quantum vulnerable

Hybrid-PPK

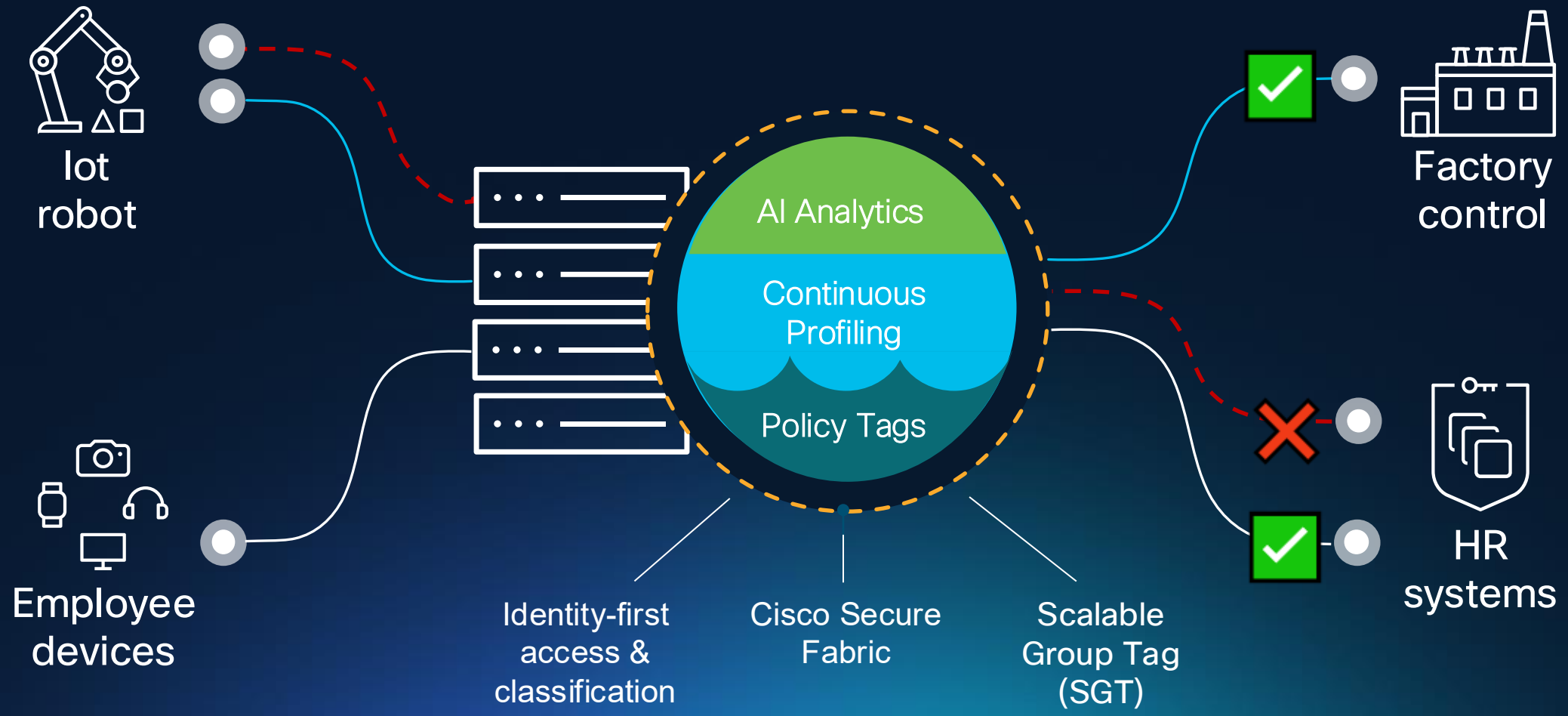
- Private Key-Public Key exchange
- New Key (PPK) not exchanged
- Quantum resistant

ML-KEM

- The initiator generates:
  Encapsulation key (Public)
  Decapsulation key (Private)
- Only the encapsulation key is securely exchanged with the responder.
- The decapsulation key remains confidential and is never transmitted.
- Quantum secure

Scalable network segmentation

Continuously verified identity and group policy applied across the network



Segmentation and deep inspection of traffic between zones

Cisco hybrid-mesh firewall

SECURITY CLOUD CONTROL

Cisco Firewalls

Physical | Virtual | Cloud | FWaaS

3rd Party Firewalls

Smart Switches

eBPF

Workload Agents

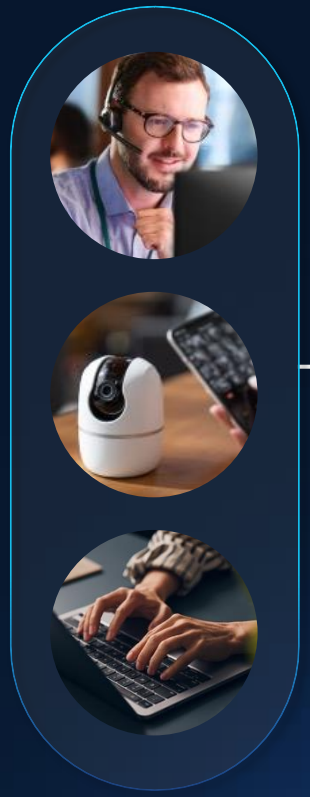
Define once, enforce everywhere

cisco

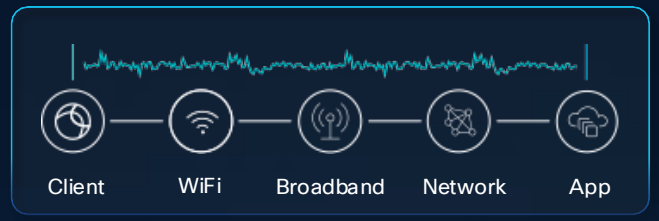
Zero Trust Access: Cisco SASE

Secure access for people, things and AI Agents

Every device, person, thing, everywhere



Zero downtime:
Experience and Policy Assurance

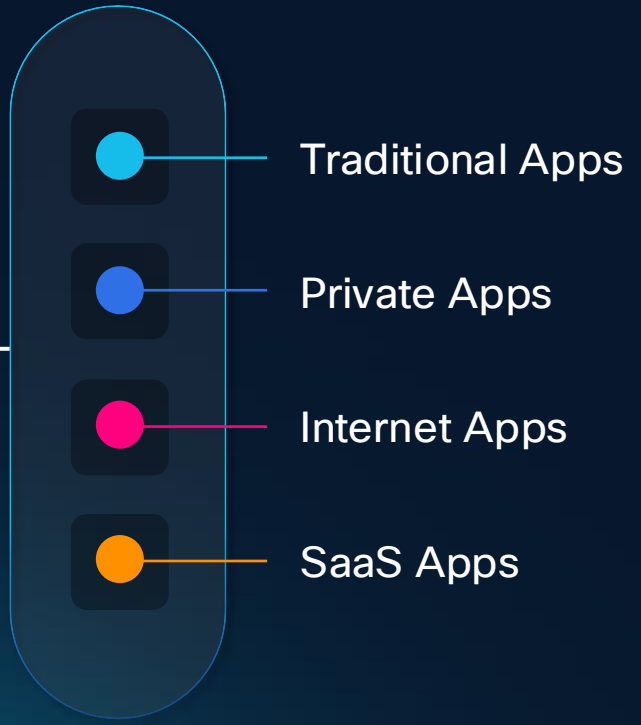


Zero impostors:
Identity Trust

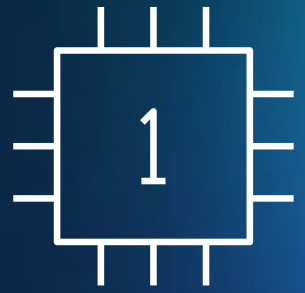
Data Loss Prevention	Remote Browser Isolation	AI Access
Firewall as a Service	Secure Web Gateway	Zero Trust Network Access
Cloud Access Security Broker	DNS Security	VPNaaS

Consistent Security:
Security Service Edge

Zero friction:
We do the plumbing



Scalable devices ready for AI



What technologies make up the Secure Network?

Catalyst Center | Meraki Dashboard

Wi-Fi

Wi-Fi 7
Wireless Controllers
Campus Gateway

Switching

Cisco Catalyst
Cisco Meraki
Cisco Smart Switches

Routing

Cisco Secure Routers
Cisco Catalyst 8000

Assurance

Wireless, Wired and
Wide-Area Networks
Cisco ThousandEyes

Authorization and scalable segmentation

Identity services engine (ISE), Software defined access (SDA) and Scalable group tags (SGT), NGFW

INTRODUCING

Scalable devices ready for AI

Smart Switches

Secure Routers

Campus Gateway

Secure Firefwall

Large Venue Wi-Fi 7

INTRODUCING

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

INTRODUCING

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

Gigabit performance, powerful security and more connectivity all in one compact device

New 8100 Series Secure Routers

Flexibility for hybrid management with IOS XE

European DSL to Fiber Conversion

Up to 3x more throughput with Secure Networking Processor

Orderable Feb 2026

Upgrade path for Meraki customers with MX OS

Cloud managed branch operations with integrated Wi-Fi and 5G Cellular

Up to 2x more throughput

Orderable April 2026

LAUNCHED JUNE 2025

Cisco 8000 Series Secure Routers for every size location

NEW SKUs

Small Branch: 8100

4 Variants

IPsec:
Up to 1.5 Gbps

Threat Protection:
Up to 1 Gbps

Ports:
1 GE

NEW SKUs

Medium Branch: 8200

4 Variants

IPsec:
Up to 5 Gbps

Threat Protection:
Up to 2.5 Gbps

Ports:
2.5 GE, 2 x 10 GE

Large Branch: 8300

2 Variants

IPsec:
Up to 20 Gbps

Threat Protection:
Up to 7 Gbps

Ports:
5 GE, 4 x 10 GE

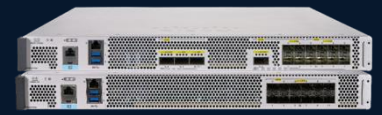
Campus: 8400

2 Variants

IPsec:
Up to 45 Gbps

Threat Protection:
Up to 11 Gbps

Ports:
25 GE



Data Center: 8500

2 Variants

IPSec:
Up to 60 Gbps

Route Scale up to 8M

Ports:
40/100 GE

The Power of Cisco 8000 Series Secure Router
Security

Consistent Security Policy Construct

Built-in Secure Firewall

NIST Compliant PQC

Ready for IPsec/MACsec

Throughput Improvement

10x IPsec, 2x Threat Protection

Line rate MACsec

LAN/WAN MACsec on all FPGE[1]

Security AI/ML

Ready to offload (C8300/C8400)

Tamper Detection

Physical (open chassis) Intrusion Detection

[1] Supported on C8200, C8300, C8400, C8500

Wi-Fi 7 for every operational scale

CW9172H

6 Spatial Streams

Hospitality

CW9174E

8/10 Spatial Streams

External antennas

CW9176D1

12 Spatial Streams

Integrated Directional

CW9179F

16 Spatial Streams

LPV/Stadium

CW9171I

4 Spatial Streams

Omnidirectional

CW9172I

6 Spatial Streams

Omnidirectional

CW9174I

8/10 Spatial Streams

Omnidirectional

CW9176I

12 Spatial Streams

Omnidirectional

CW9178I

16 Spatial Streams

Omnidirectional

Wi-Fi 7 | Global Use AP | Unified License | AI Optimized

Cisco extends the campus network architecture to outdoor and rugged spaces









Consistent Network Architecture

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

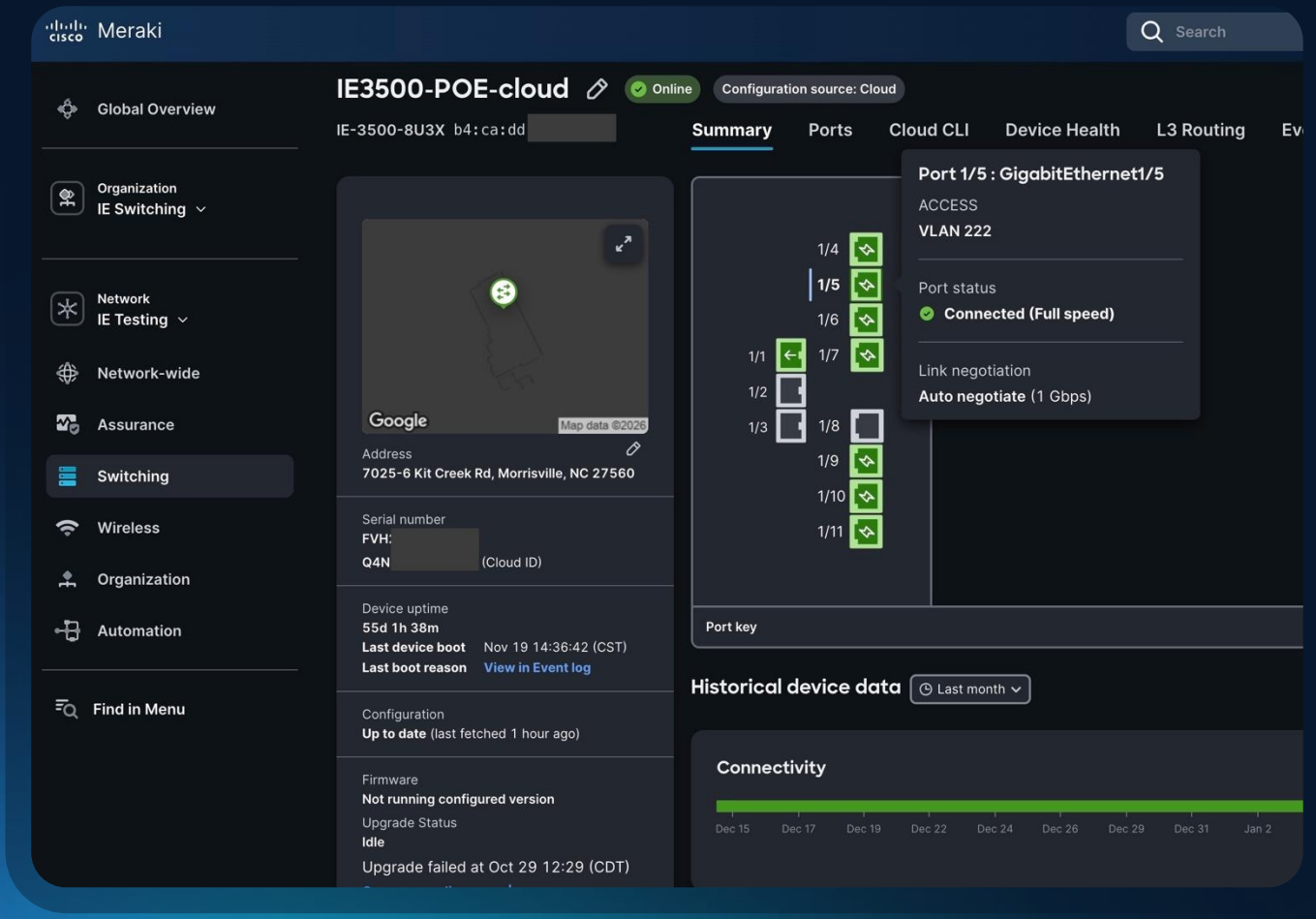
Standardized equipment | Centralized management | Enterprise-wide security
High-performance networking | One licensing model

Cloud Management of IE3500 Switches

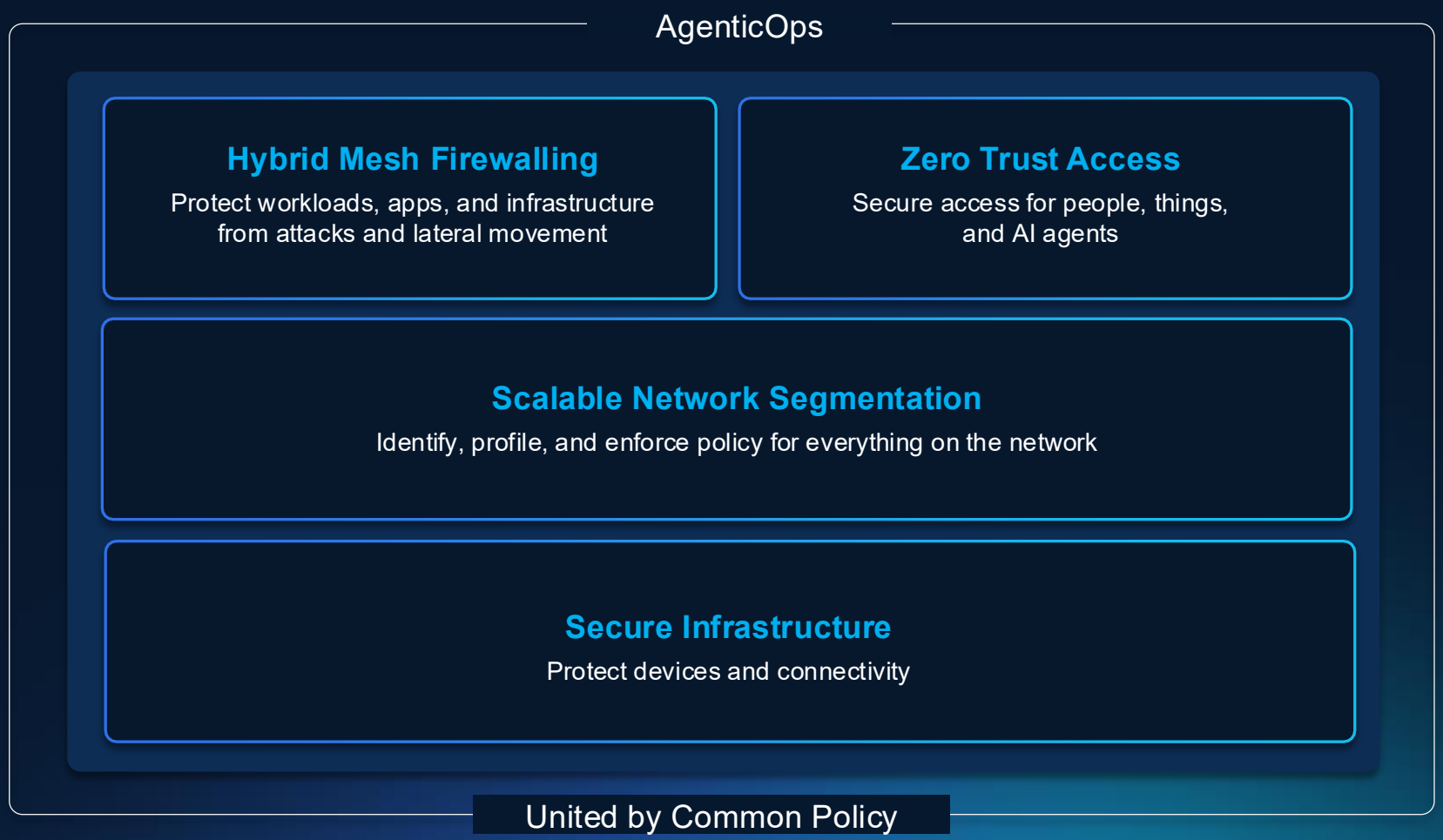
Rugged networking, cloud-simple

Beta Feb 26

- A single dashboard to manage enterprise and rugged switches
- Easily extend enterprise networks to outdoors and uncarpeted spaces
- Allow IT teams to enforce consistent security policies across the entire enterprise network footprint



Reference design for fusing security into the network



- Identity-first
- Continuously verified
- Enterprise-wide policies
- Comprehensive Threat Intel
- Distributed Enforcement

Thank you to our sponsors!

World Wide Technology, Inc.

PRESIDIO®

Where Technology Means More®

Thank you


CISCO