



# 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

Internet

Mobility

Cloud

AI

# 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

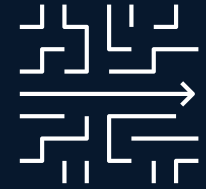
# Is your Campus Network AI ready?

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



# Architecture for the AI-Ready secure network

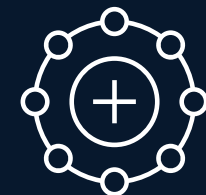
AgenticOps  
for operational simplicity



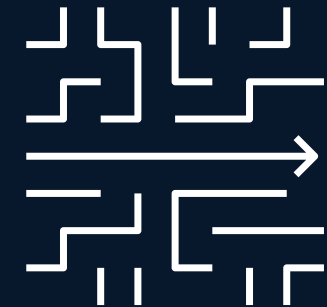
Security  
fused into the network



Scalable devices  
ready for AI



# AgenticOps for operational simplicity



# Unifying Catalyst & Meraki

## Catalyst

Catalyst Center

Catalyst License

Catalyst Hardware

MANAGEMENT

LICENSE

CISCO HARDWARE

## Meraki

Meraki Dashboard

Meraki License

Meraki Hardware

# Our unified platform

PLATFORM

Management

Assurance

API / Integrations

Intelligence

HARDWARE



Smart  
Switches



Secure  
Routers



Wireless



Industrial  
IoT

# 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



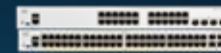
C9200L



C9500



C9200/CX



C9300LM



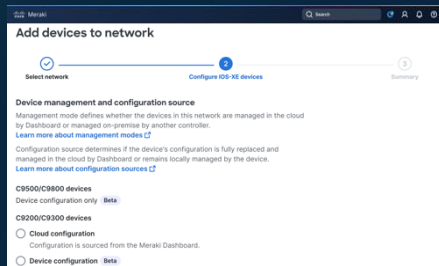
C9350



Modular

# Large campus cloud capabilities

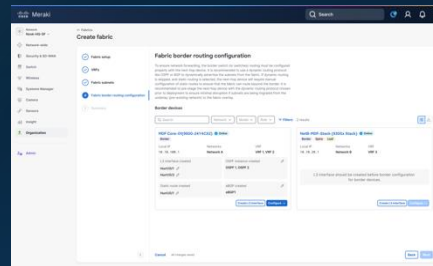
## Powerful Switching Capabilities



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

BETA

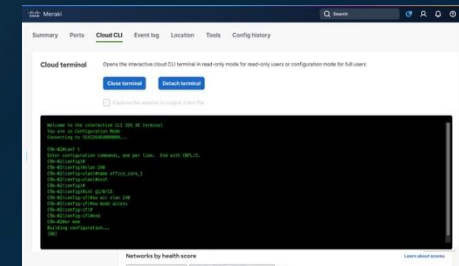
## Fabric for Secure Networking



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

The screenshot shows the Cisco Cloud Management Center interface for a 'Modular stack' of C9610R switches. The interface includes a navigation menu with options like Summary, Ports, Device health, Cloud CLI, Event log, Location, Tools, and Admin. The main content area is divided into two sections: 'Chassis stack attributes' and 'Supervisor and line cards'. The 'Chassis stack attributes' section displays a map of the device location (500 Terry A. Francois Blvd, San Francisco, CA 94158), device uptime (12d 2h 8m), and firmware information (Current version: IOSXE 17.13). The 'Supervisor and line cards' section shows a table of line cards with columns for Slot, Model, Role, and Serial number. Below the table, there are two visual representations of the line card slots, each showing a grid of 48 ports (2 rows by 24 columns). The ports are color-coded: green for online, red for offline, and orange for a warning. The first grid shows port 15 as green and port 20 as red. The second grid shows port 15 as green and port 20 as red.

C9610 Smart Switches

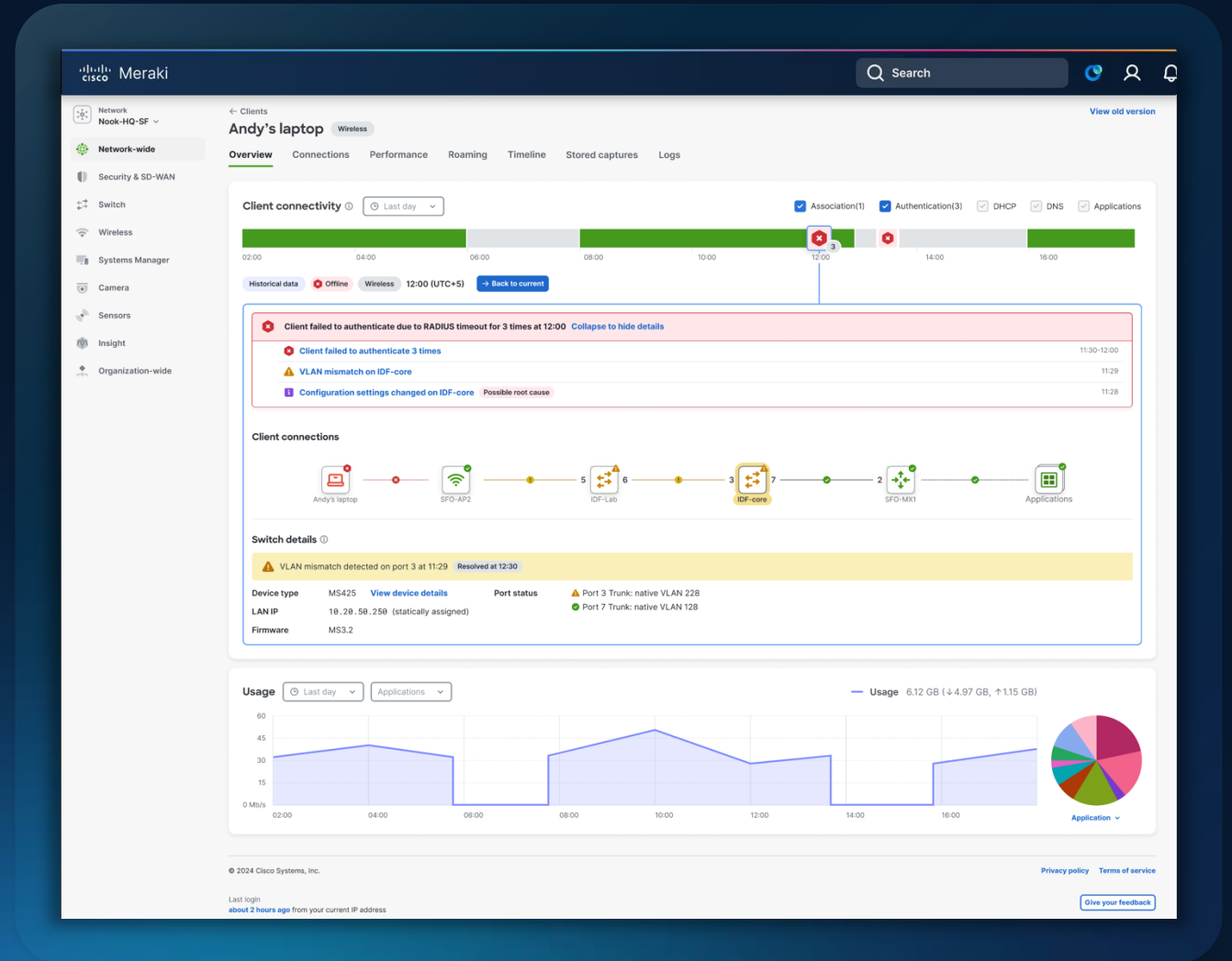
# Assurance across every digital experience

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
- 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 | <a href="#">t-GARR</a> | <a href="#">FL5 HQ VPN SSID</a> |
| Jan 21, 2026, 09:00 PM PST | <a href="#">t-GARR</a> | <a href="#">FL5 HQ VPN SSID</a> |
| Jan 21, 2026, 08:51 PM PST | <a href="#">t-GARR</a> | <a href="#">FL5 HQ VPN SSID</a> |
| Jan 21, 2026, 08:44 PM PST | <a href="#">t-GARR</a> | <a href="#">FL5 HQ VPN SSID</a> |

### 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

### Assessment Complete

I've successfully completed the **NIST CSF 2.0 Network Security Maturity Assessment** for **Store #0025 (Newtown Square — pilot store)**.

### Key Deliverables Provided

✅ **Maturity Scorecard:** Complete 40-check assessment with 0-5 scoring per check ✅ **Function Scores:** GV (1.8), ID (2.7), PR (3.0), DE (2.0), RS (2.8), RC (3.0) ✅ **Overall Tier: Tier 2: Risk-Informed** (2.1/5.0 — capped by critical gaps) ✅ **Top 5 Remediation Plan** with evidence (API endpoints + key field values) ✅ **Executive Summary:** "What's Good / What's Missing" suitable for leadership

### Assessment Highlights

**Overall Maturity: 2.1/5.0** (Tier 2) — Strong technical architecture held back by systemic org-level failures

**Critical Insight:** Store #0025 demonstrates **excellent local network engineering** (4-VLAN segmentation, WPA2-Enterprise, dual uplinks) but **organization-level governance failures** (MFA, syslog, IDS prevention) affect all 500 RetailMax stores and block cyber insurance eligibility.

**Top Priority: Enable MFA org-wide** (Week 1) — fixes GOV-01 critical gap, unblocks cyber insurance, affects 0 clients, requires only 7-day grace period for admin enrollment.

### Evidence Collection Summary

- **24 API endpoints** queried (6 org-level + 12 network-level + lookups)
- **Simulator:** Used `compliance/pci-dss-retail-chain` scenario
- **Assessment Time:** ~5 minutes (single network)

The complete report above includes detailed remediation guidance with Dashboard navigation paths, "why it's safe" explanations for each fix, and cross-framework mappings to PCI-DSS and cyber insurance requirements.



Ask the AI Assistant a question



**Security fused into the Network**



# New threats attack networks directly



## Attacks on Infrastructure

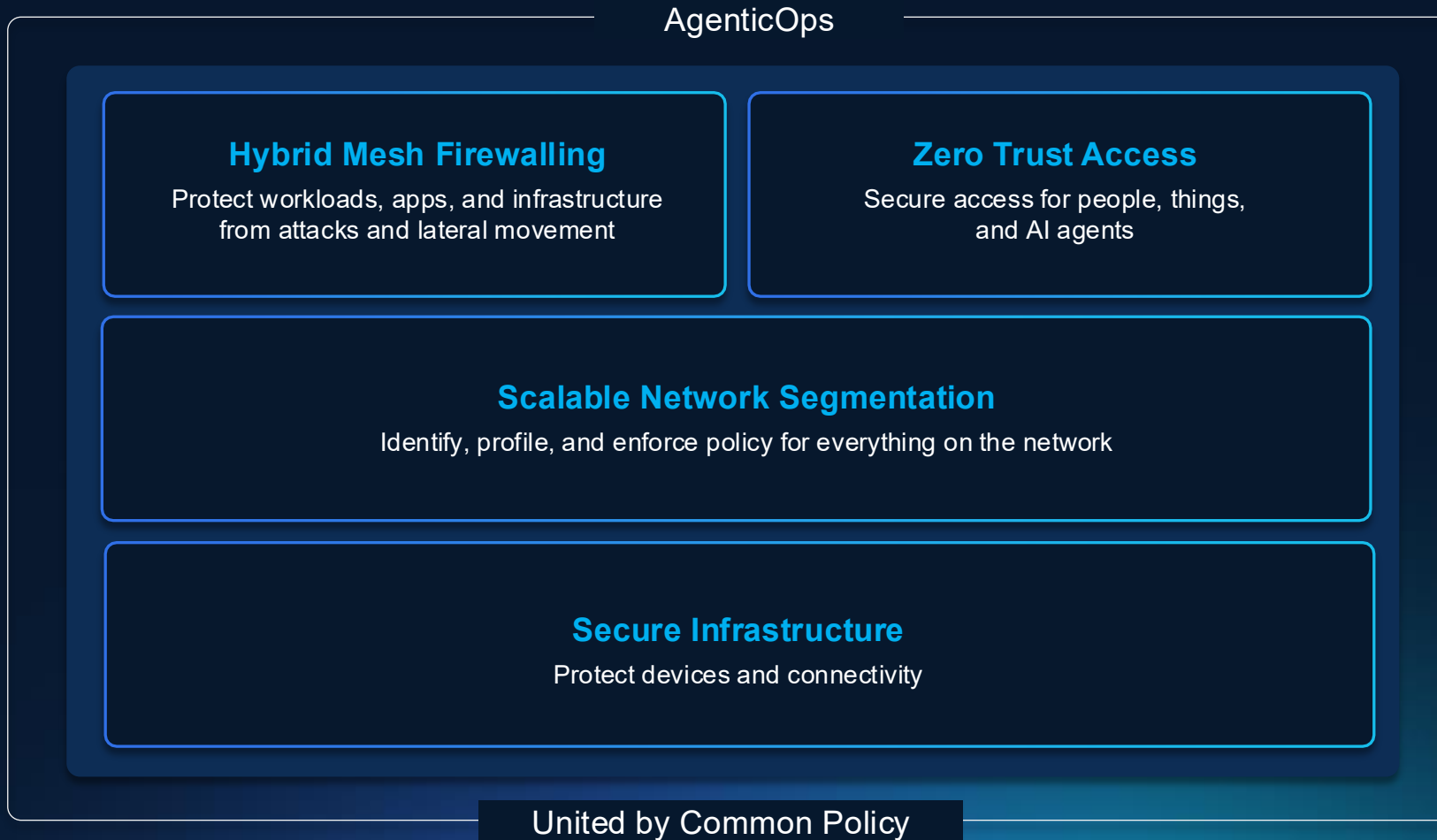
Exploits like Salt Typhoon that target unpatched software on key infrastructure



## Attacks on Encryption

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

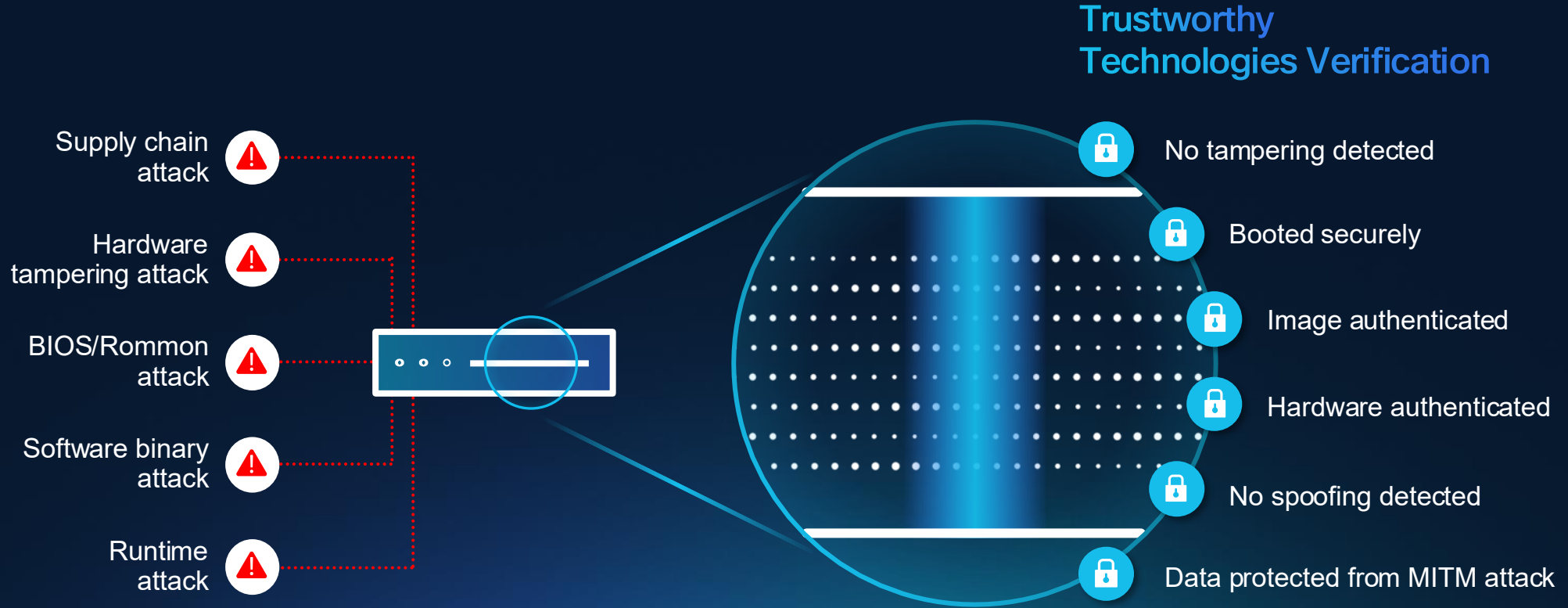
# Reference design for fusing security into the network



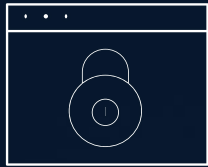
- Identity-first
- Continuously verified
- Enterprise-wide policies
- Comprehensive Threat Intel
- Distributed Enforcement

# Secure Infrastructure: Securing the device

Secure from hardware to software, from boot time to runtime



# 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



Stop the attack...

...but don't stop the network.

LIVE PROTECT

VULNERABILITY

CISCO SWITCHES

# 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 <sup>i</sup> <input type="text"/>                                | Affected devices | Live Protect <sup>i</sup>                       | Hits <sup>i</sup> |
|---|--|---|------------------|---|-------------------|
| <a href="#">CVE-2023-20198</a> <span>New</span> | Web UI Unauthorized Access Vulnerability       | <div style="width: 100%;"><div style="width: 100%;"></div></div> 10.0 | 1                | <span style="color: green;">✔ Available</span>  | — ...             |
| <a href="#">CVE-2024-20169</a>                  | Command Injection Vulnerability                | <div style="width: 100%;"><div style="width: 100%;"></div></div> 9.8  | 1                | <span style="color: green;">✔ Available</span>  | — ...             |
| <a href="#">CVE-2023-20154</a>                  | SNMP Remote Code Execution                     | <div style="width: 100%;"><div style="width: 100%;"></div></div> 9.8  | 2                | <span style="color: green;">✔ Pending</span>    | — ...             |
| <a href="#">CVE-2023-20049</a> <span>New</span> | Authentication Bypass Management Interface     | <div style="width: 100%;"><div style="width: 100%;"></div></div> 9.6  | 1                | <span style="color: blue;">✔ Protection</span>  | 6 ...             |
| <a href="#">CVE-2024-20467</a>                  | Privilege Escalation via CLI                   | <div style="width: 100%;"><div style="width: 100%;"></div></div> 9.1  | 1                | <span style="color: blue;">✔ Observation</span> | 5 ...             |
| <a href="#">CVE-2024-20480</a>                  | SSH Key Management Vulnerability               | <div style="width: 100%;"><div style="width: 100%;"></div></div> 9.1  | 2                | <span style="color: green;">✔ Available</span>  | — ...             |
| <a href="#">CVE-2023-20177</a> <span>New</span> | IPv6 RA Guard Bypass                           | <div style="width: 100%;"><div style="width: 100%;"></div></div> 8.6  | 1                | <span style="color: blue;">✔ Protection</span>  | 1 ...             |
| <a href="#">CVE-2024-20508</a>                  | Privilege Escalation through Configuration API | <div style="width: 100%;"><div style="width: 100%;"></div></div> 8.6  | 2                | <span style="color: blue;">✔ Protection</span>  | 3 ...             |
| <a href="#">CVE-2023-20200</a>                  | CLI Privilege Escalation                       | <div style="width: 100%;"><div style="width: 100%;"></div></div> 8.6  | 2                | <span style="color: green;">✔ Pending</span>    | — ...             |
| <a href="#">CVE-2024-20437</a>                  | Buffer Overflow in HTTP Server                 | <div style="width: 100%;"><div style="width: 100%;"></div></div> 8.4  | 1                | <span style="color: blue;">✔ Observation</span> | 8 ...             |

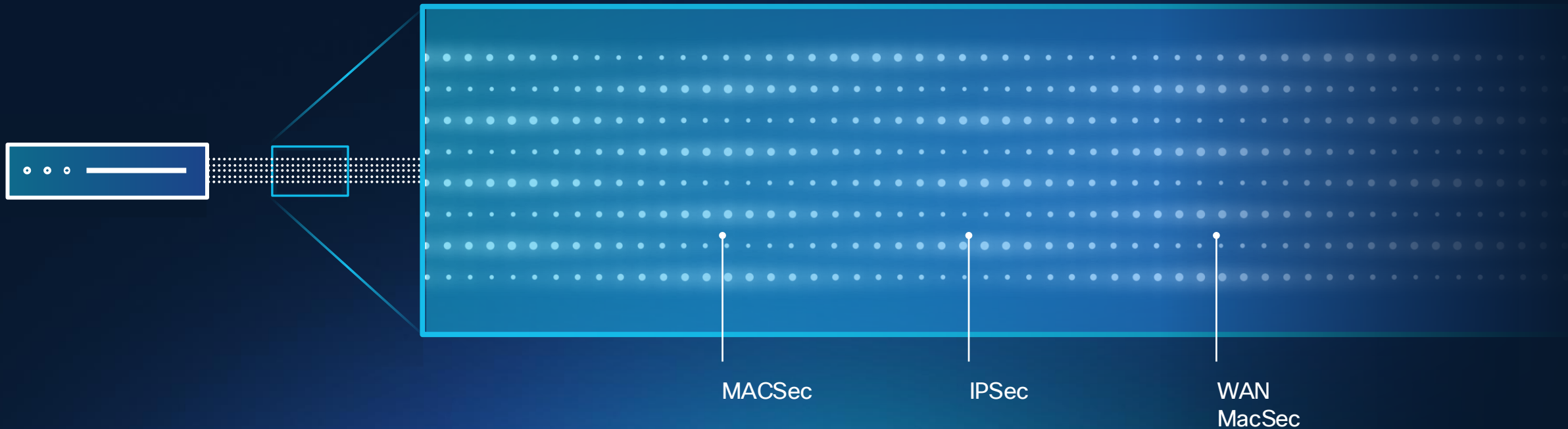
Rows per page  1-20 of 73 <  2 ... 10 >

# 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

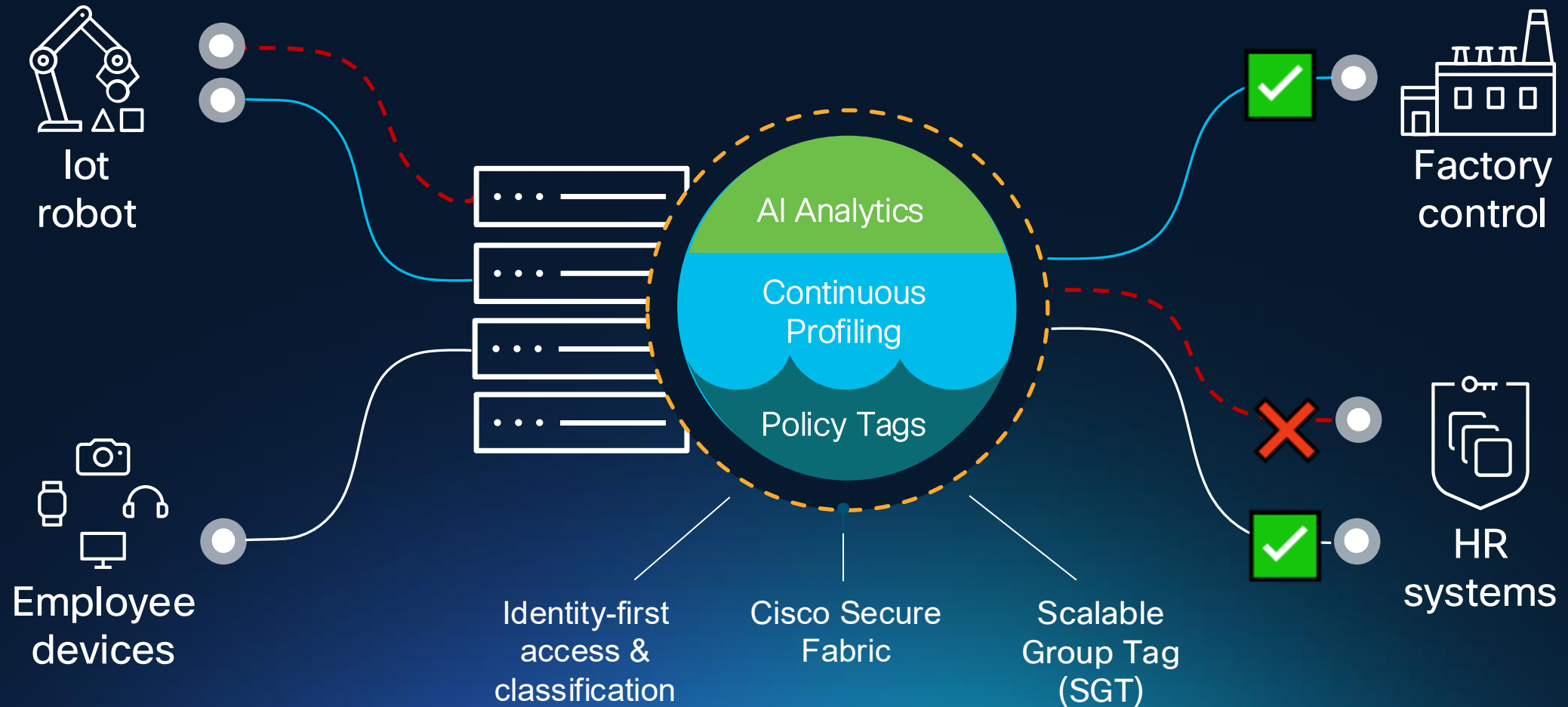


## ML-KEM

- 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



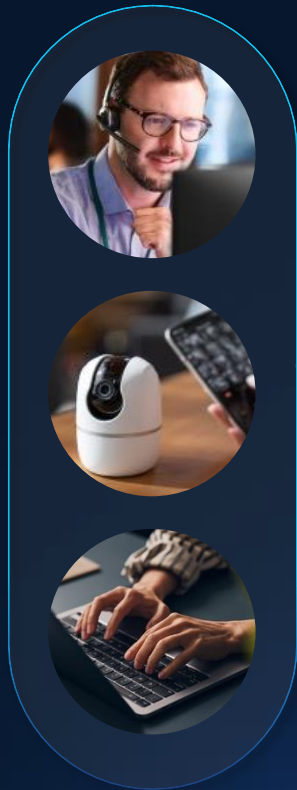
# Zero Trust Access: Cisco SASE

## Secure access for people, things and AI Agents

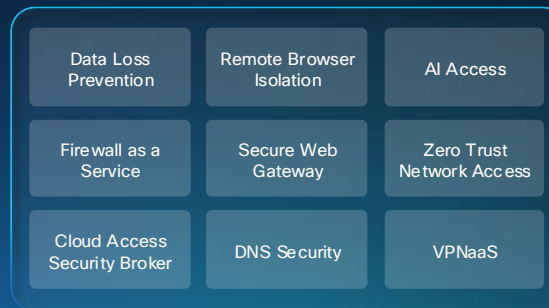
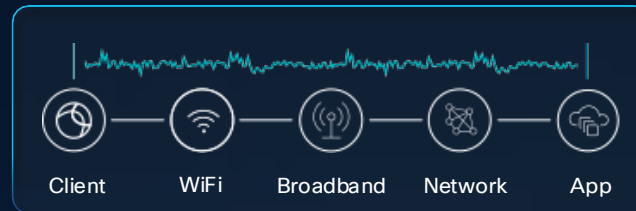
Every device, person, thing, everywhere

**Zero downtime:**  
Experience and Policy Assurance

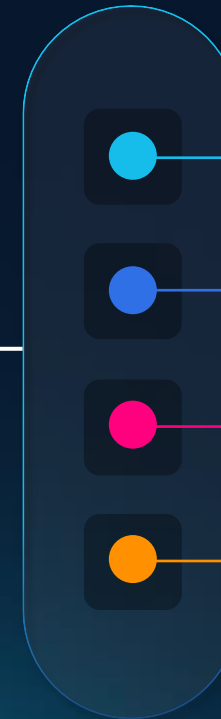
**Zero friction:**  
We do the plumbing



**Zero impostors:**  
Identity Trust



**Consistent Security:**  
Security Service Edge



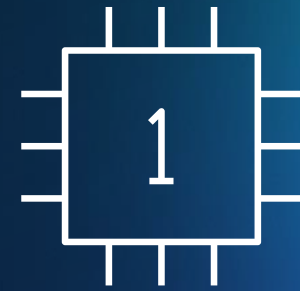
Traditional Apps

Private Apps

Internet Apps

SaaS Apps

**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 Firewall



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

Backward compatible  
chassis with front to  
back airflow

Powered by Cisco  
Silicon One

High density  
chassis with state-  
of-the-art hardware

Entirely modular and  
upgradable system



# 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



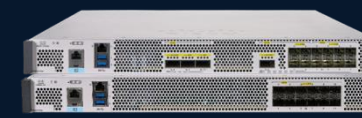
## Campus: 8400

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<sup>[1]</sup>

## 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



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

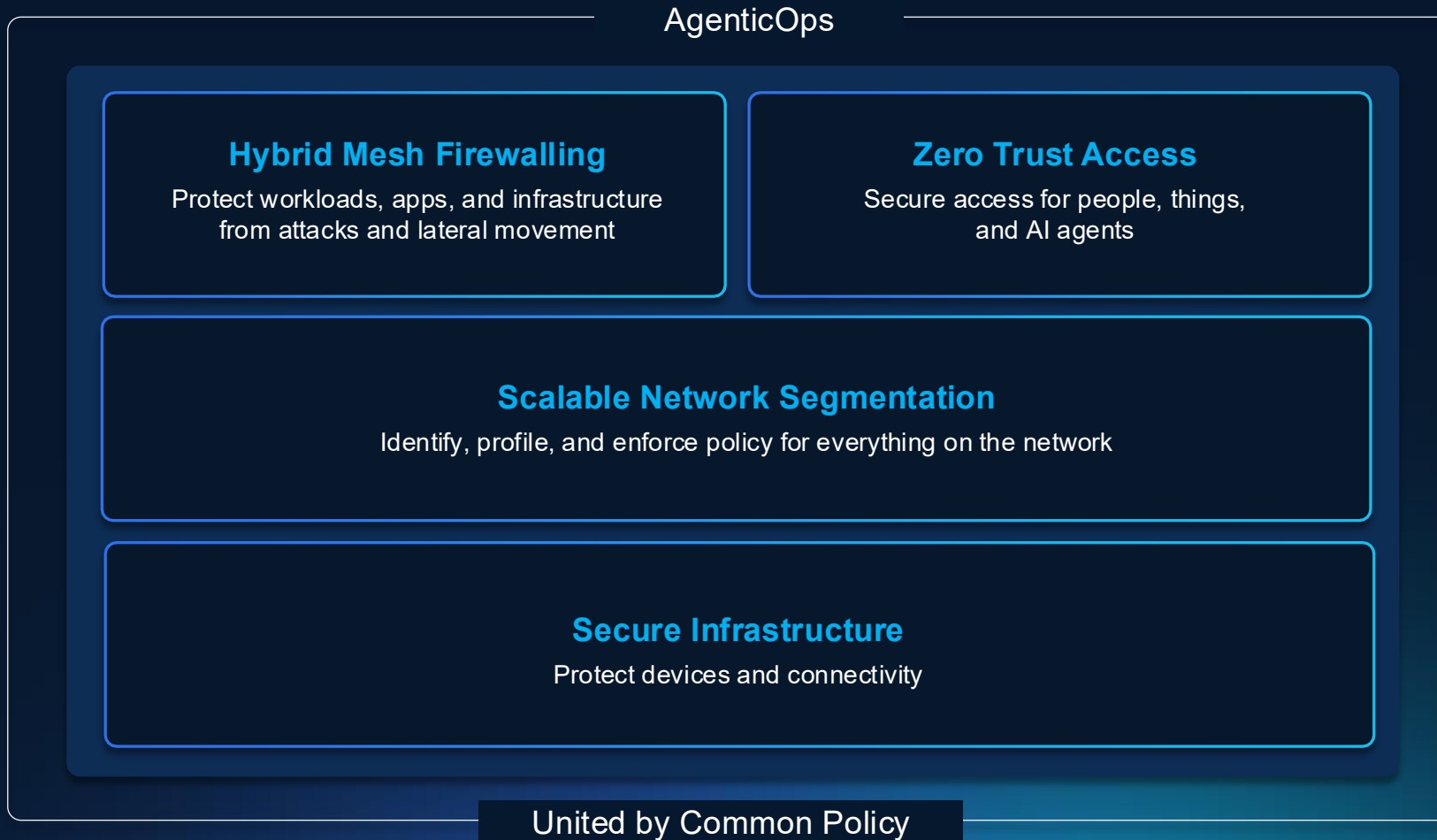
- A single dashboard to manage enterprise and rugged switches
- Easily extend enterprise networks to outdoors and uncarpeted spaces
- Allow IT teams to enforce consistent security policies across the entire enterprise network footprint

The screenshot shows the Meraki cloud management interface for a switch named 'IE3500-POE-cloud'. The interface is dark-themed and includes a search bar at the top right. The main content area is divided into several sections:

- Global Overview:** Shows the switch is 'Online' and configuration source is 'Cloud'. The switch ID is 'IE-3500-8U3X b4: ca: dd'.
- Summary:** Displays a map of the switch's location in Morrisville, NC, with a Google map view. It also shows the address: '7025-6 Kit Creek Rd, Morrisville, NC 27560'.
- Serial number:** Shows 'Q4N' and 'Q4N' (Cloud ID).
- Device uptime:** Shows '55d 1h 38m'.
- Last device boot:** Shows 'Nov 19 14:36:42 (CST)'. A link for 'View in Event log' is provided.
- Last boot reason:** Shows 'View in Event log'.
- Configuration:** Shows 'Up to date (last fetched 1 hour ago)'.
- Firmware:** Shows 'Not running configured version'. Upgrade status is 'Idle'. A note indicates 'Upgrade failed at Oct 29 12:29 (CDT)'.

On the right side, there is a 'Ports' section showing a list of ports (1/1 to 1/11) with their status. A tooltip for 'Port 1/5: GigabitEthernet1/5' is open, showing it is 'ACCESS VLAN 222' and 'Connected (Full speed)'. The link negotiation is set to 'Auto negotiate (1 Gbps)'. Below the ports is a 'Historical device data' section with a 'Last month' filter and a 'Connectivity' graph showing a green bar from Dec 15 to Jan 2.

# 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®



Thank you



