

The AI-Ready Campus & Branch: Powering Smart Workplaces and Secure, Scalable Networks

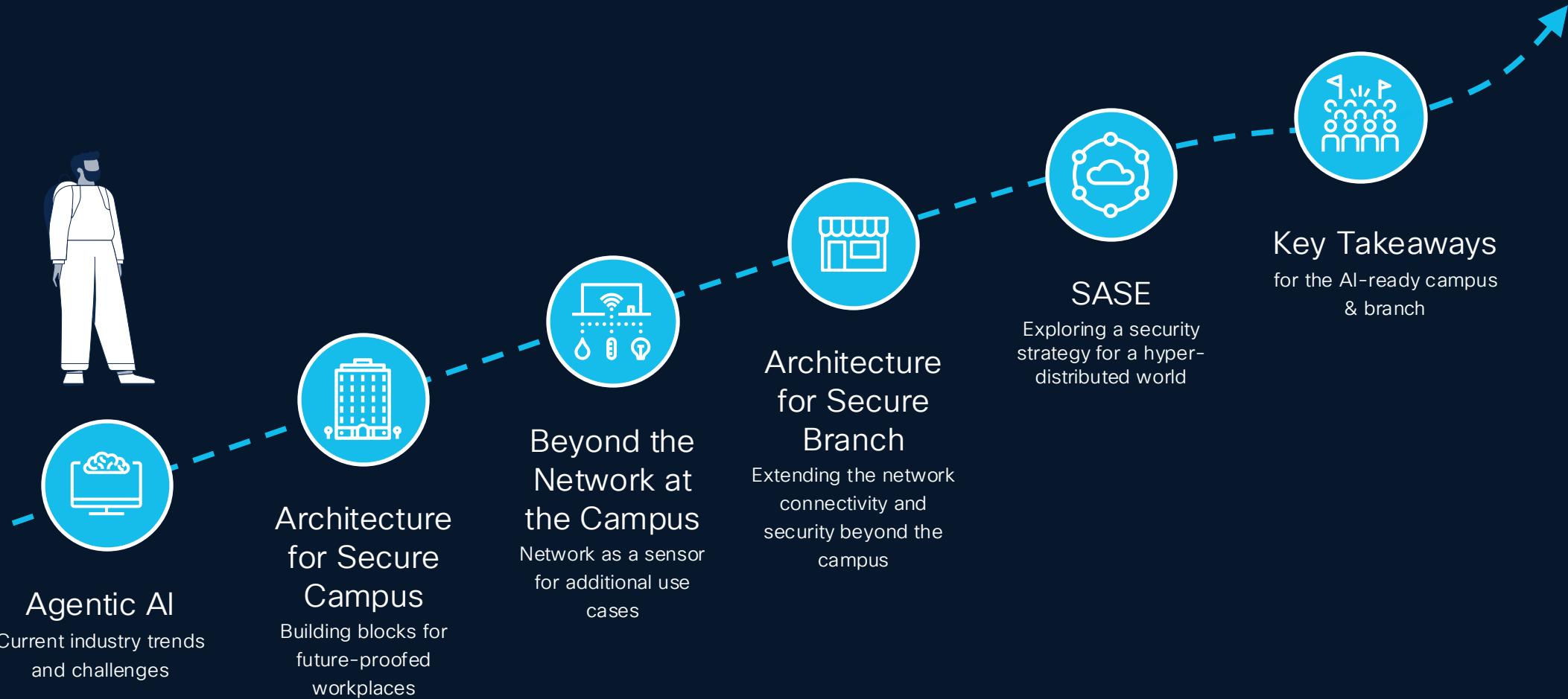


Curtis Lyon (culyon@cisco.com)
Solutions Engineer

Allan Hernandez Yela (allanher@cisco.com)
Solutions Engineer

December 11, 2025

Today's journey for this session



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

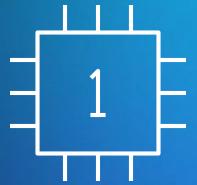


Architecture for Secure Campus

Operational simplicity
powered by AI



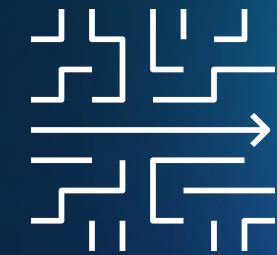
Scalable devices
ready for AI



Security
fused into the network



Operational simplicity
powered by AI



Unifying Catalyst & Meraki

Catalyst

Catalyst Center

Catalyst License

Catalyst Hardware

MANAGEMENT

LICENSE

CISCO HARDWARE

Meraki

Meraki Dashboard

Meraki License

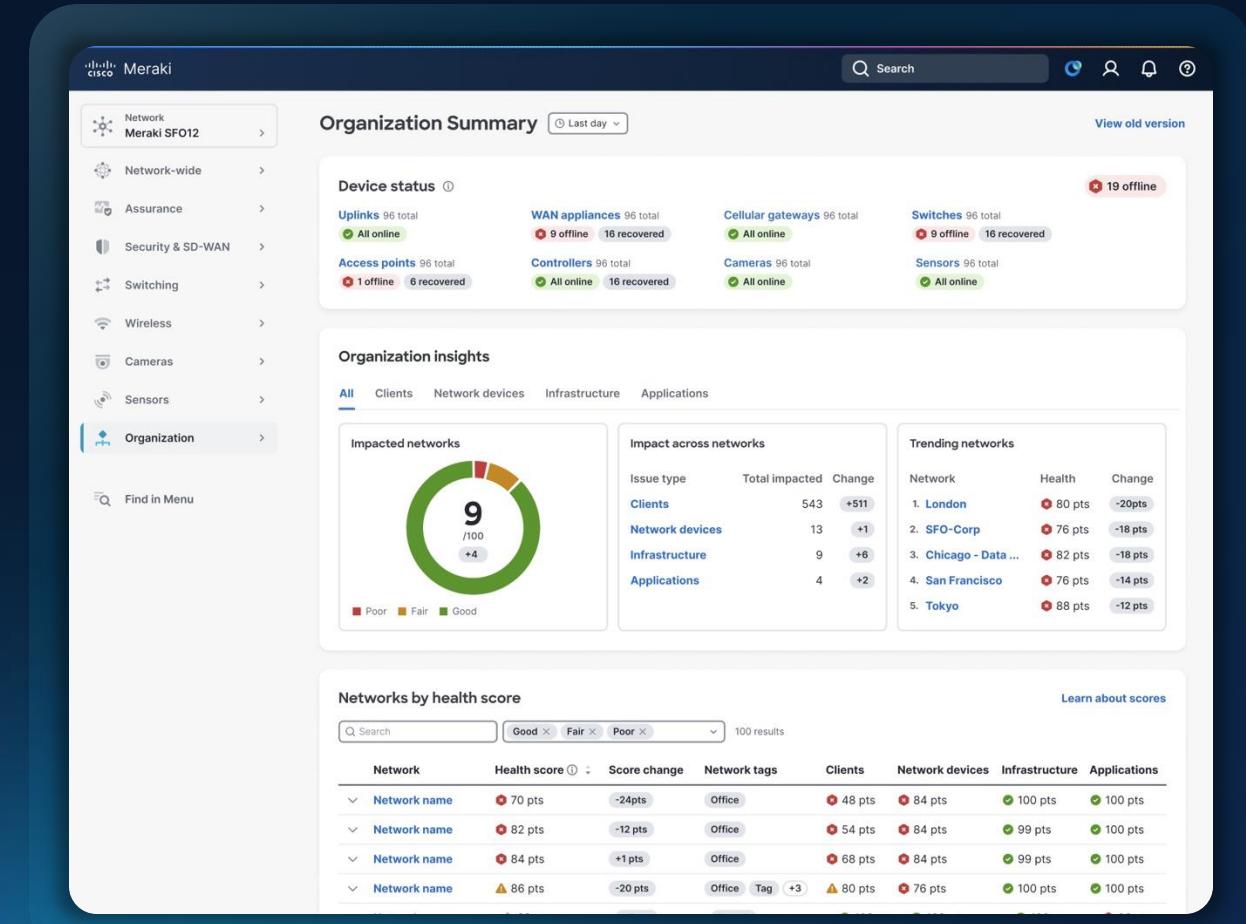
Meraki Hardware

Unified Management – Catalyst and Meraki, any environment

Seamless control across cloud, on-prem, or hybrid

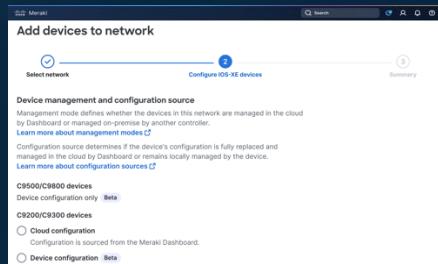
New enterprise campus capabilities

AI-powered automation and assurance



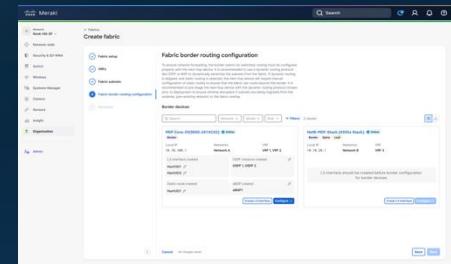
Large campus cloud capabilities

Powerful Switching Capabilities



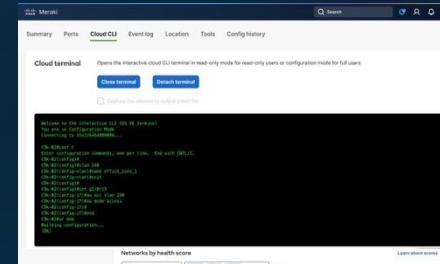
Support campus deployments with BGP, VRF, ISSU, and IOS XE stacking

Fabric for Secure Networking



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

Cloud CLI for Flexibility



Simplify onboarding and flexibility with operating mode options and Cloud CLI

AgenticOps

The New Standard for IT Operations

ALPHA I OCTOBER



AI Canvas

Cross-domain collaborative troubleshooting

CONTROLLED RELEASE I OCTOBER



CISCO
AI Assistant

AI Assistant

Accelerate network operations

POWERED BY DEEP NETWORK MODEL

Cut MTTR to near seconds with AI-driven root cause and resolution.

Catch critical issues **early with AI that sees across the stack.**

Operate at scale with lean teams and built-in AI expertise.

Troubleshoot faster together with shared context across teams.

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, a comprehensive platform for network monitoring and troubleshooting. The top navigation bar includes the Cisco logo, 'AI Canvas', and a search bar for 'Application performance degradation'. On the right, there are user status indicators (J, W), a 'Generate report' button, 'View activity', and 'Share' options.

The main content area is organized into several cards:

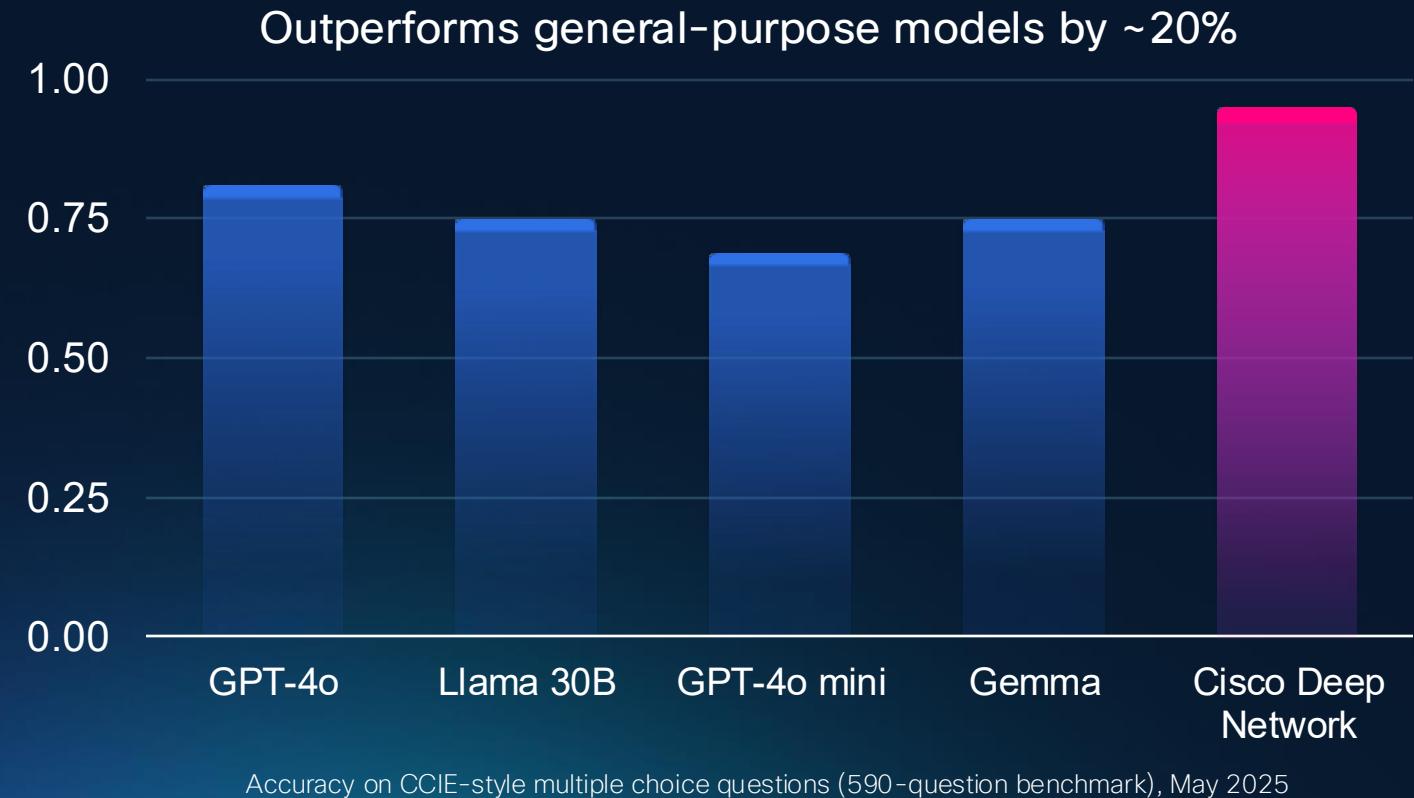
- AI Assistant:** A text box explaining the relationship between network congestion and application failures, mentioning financial app failures and mandatory security-related software updates.
- SJ-MX105-01 network congestion statistics vs. EFP application performance:** A Splunk-generated chart showing Packet Loss (blue line) and Transaction failure rate (red line) over time. The chart shows a significant spike in both metrics around 10:00 AM.
- ServiceNow SRTK0023941:** A ServiceNow ticket alert for a financial application at the San Jose branch, reporting 3-5 second delays during processing. It includes a ticket link: ServiceNow Ticket SRTK0023941.
- SJ-MX105-01 WAN interface performance:** A card showing a 16.4% loss rate, with WAN interface latency at 87ms (baseline <50ms) and Jitter at 15ms (baseline <5ms).
- SJ-MX105-01 performance (last 24 hrs):** A line graph showing packet loss over the last 24 hours, with a red dot marking a critical point at approximately 11:00 AM.
- Network segment performance analysis:** A diagram showing the network topology from the Enterprise network (16.4% loss) through the Gateway and Internet to the Application (financeapp.com). A red dot indicates a packet loss point on the connection line.
- Message from Maria Chen:** An email message from Maria Chen to the IT Support team regarding financial application performance issues. It asks for an immediate status update and a workaround. Maria Chen is a Senior Director, Financial Operations.

At the bottom, there are controls for zooming in and out (T, -, +) and a 'Ask the AI Assistant a question' input field with a 'Verify responses' link.

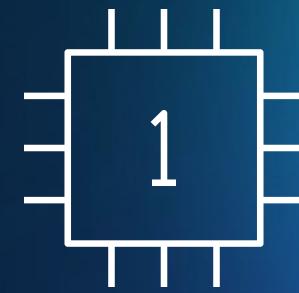
Deep Network Model

Purpose-built for networking,
expert accuracy

- More precise reasoning for troubleshooting, configuration, and automation
- Fine-tuned on 40+ years of expertise and expert-vetted for accuracy
- Evolves with live telemetry and real-world Cisco TAC and CX insights



Scalable devices ready for AI



What technologies make up the Secure Campus?

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



ThousandEyes

Medium
Large



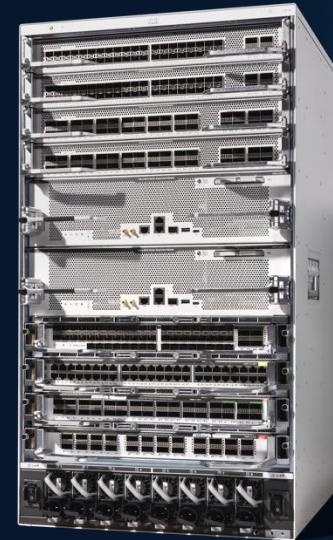
High-performance,
low latency

Cisco Silicon One +
co-processor for
security and AI

Post-quantum
secure

Intelligent energy
efficiency

Introducing Smart Switches for the AI-powered campus



Cisco C9350 & 9610 Smart Switches

AVAILABLE TODAY

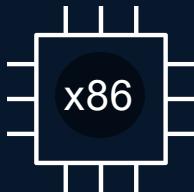
Introducing the Next Generation of Campus Switching

Silicon One ASICs, AI-Ready Infrastructure, Updated IOS-XE



Silicon One ASICs Adaptability

- Programmable at all layers
- Permits multiple use cases in a converged solution
- Virtual slicing for parallel processing



X86 Processor AI Readiness

- Control-Plane scale for agentic-AI and AI agents at scale.
- Enhances Software-assisted Services (AVC/XDR)
- Advanced App-Hosting with AI-Hosting (Edge Compute)



Updated IOS XE Security

- Supports post-quantum cryptography
- Trustworthy Linux kernel that securely hosts applications
- Leverage advanced Linux features for Cisco Live Protect

Smart Power, PoE Assurance and Energy dashboard

More throughput to support increased traffic to data center

Advanced embedded NGFW for secure branch connectivity

Post-quantum secure

DevOps style Branch-as-code for rapid deployment

Introducing Secure Routers for the AI-powered unified branch



Cisco 8000 Secure Routers

Cisco 8000 Series Secure Routers for every size location



Small Branch:
8100

4 Variants

IPsec:
Up to 1.5 Gbps

SD-WAN:
Up to 1 Gbps

Threat Protection:
Up to 1 Gbps



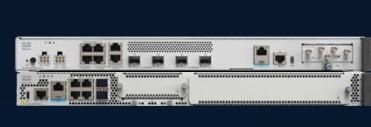
Medium Branch:
8200

2 Variants

IPsec:
Up to 5 Gbps

SD-WAN:
Up to 4 Gbps

Threat Protection:
Up to 2.5 Gbps



Large Branch:
8300

2 Variants

IPsec:
Up to 20 Gbps

SD-WAN:
Up to 15 Gbps

Threat Protection:
Up to 7 Gbps



Campus:
8400

3 Variants

IPsec:
Up to 45 Gbps

SD-WAN:
Up to 23 Gbps

Threat Protection:
Up to 11 Gbps



Data Center:
8500

2 Variants

IPSec:
Up to 45 Gbps

SD-WAN:
Up to 23 Gbps

Route Scale up to 8M

Wi-Fi 7 for every operational scale

NEW



CW9171I

4 spatial streams

Omnidirectional

Ceiling mount and
wall plate form factor



**CW9172 &
CW9172H**

6 spatial streams

Omnidirectional

Ceiling mount and
wall plate form factor

NEW



**CW9174I &
CW9174E**

8 spatial streams

Omnidirectional

External antennas

5Gbps



**CW9176D &
CW9176I**

12 spatial streams

Integrated directional

10 Gbps, GPS, UWB



CW9178

16 spatial streams

Omnidirectional

2x 10 Gbps, GPS, UWB

NEW



CW9179F

16 spatial streams

Software-defined radios

2x 10 Gbps, GPS

Wi-Fi 7 | Global use AP | Unified license | AI optimized

Scales up to
5,000 APs
and 50,000 clients

Easy migration for
existing LAN
controller
architectures

No need to
re-cable, change
VLANs, or disrupt
operations

Introducing The New Campus Gateway



AVAILABLE TODAY

Cisco Campus Gateway

Role Play

AVAILABLE | NOW

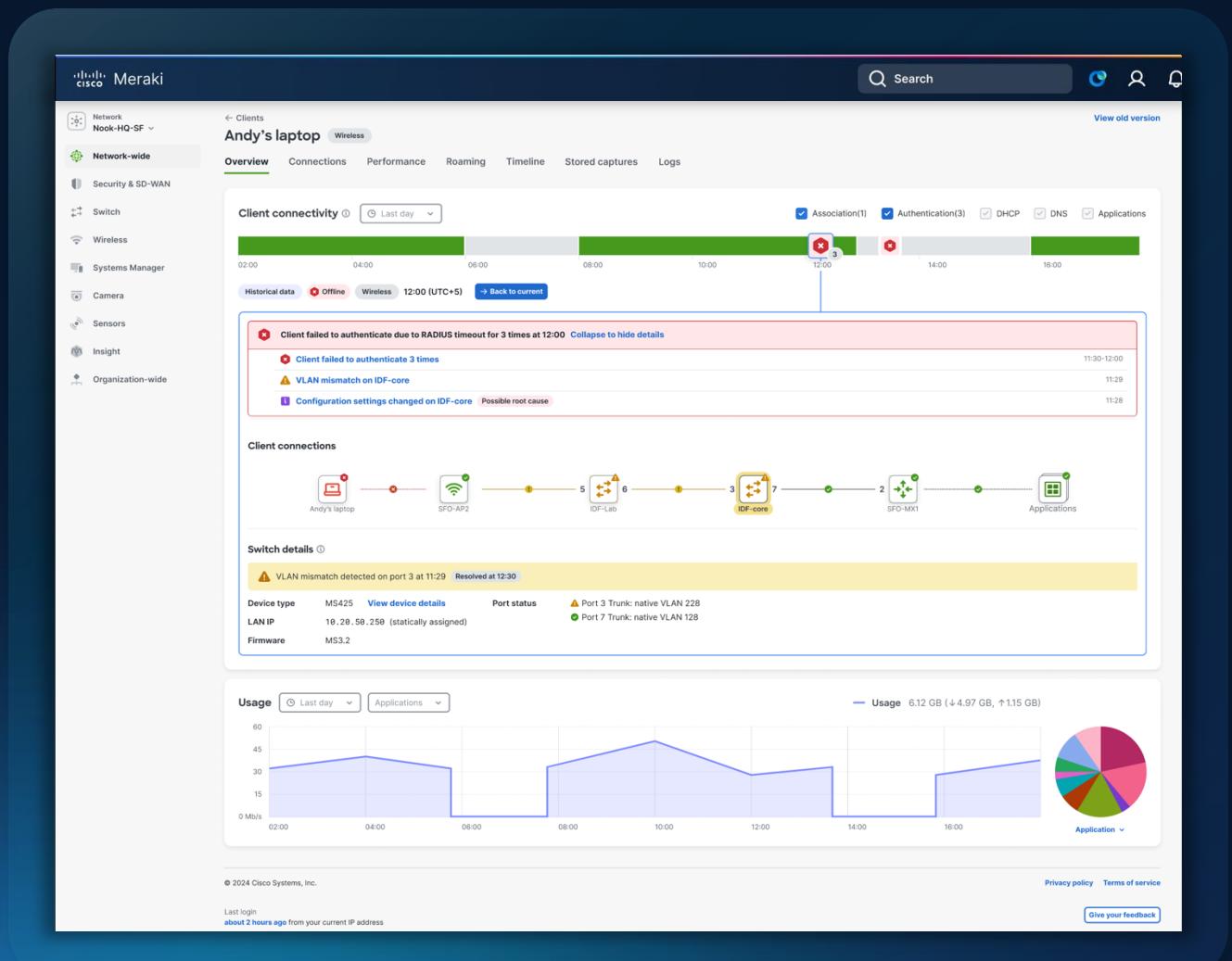
Assurance across every digital experience

Deep visibility across both owned and unowned networks

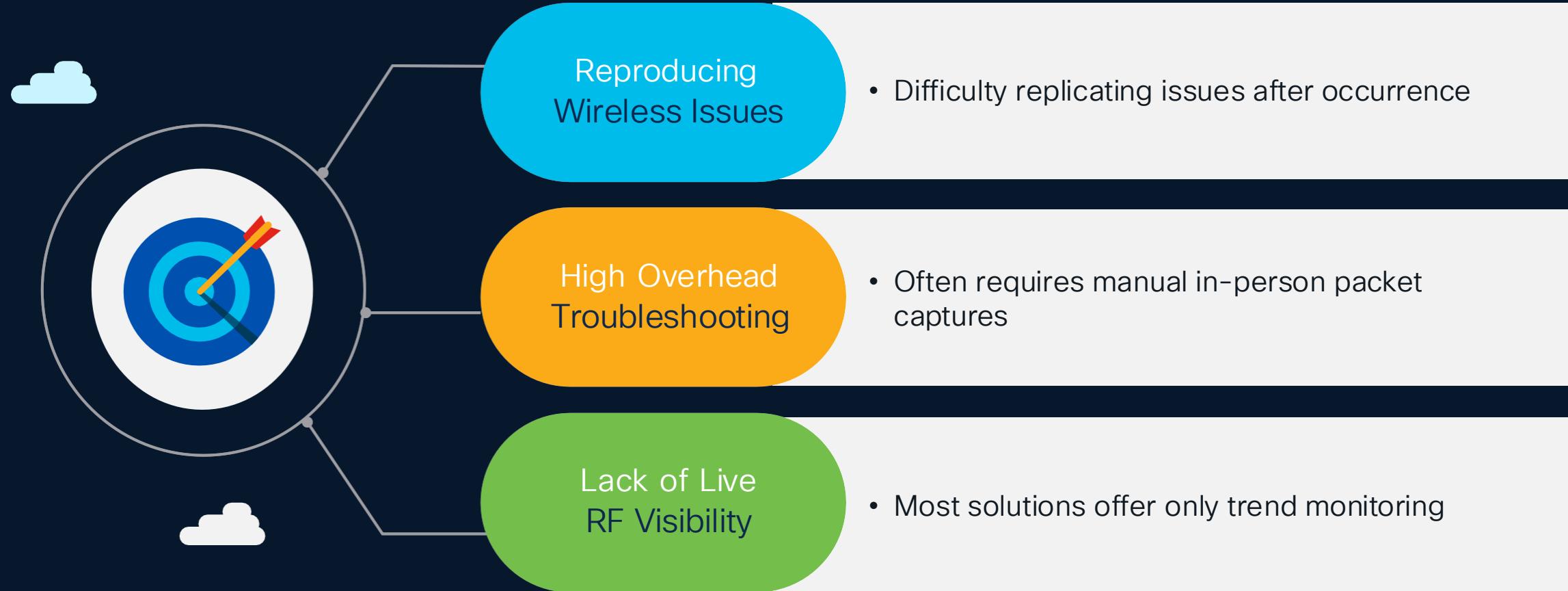
AI-powered insights surface experience-impacting issues instantly

Closed-loop workflows trigger automated remediation

AI Assistant accelerates root cause analysis end-to-end



Intelligent Packet Capture



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.

Security fused into the network

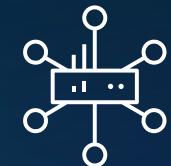
Securing network
connectivity



Securing network
access



Securing the device



Securing network connectivity

Network traffic

IoT/OT

Managed

Unmanaged



IPSec

MACSec

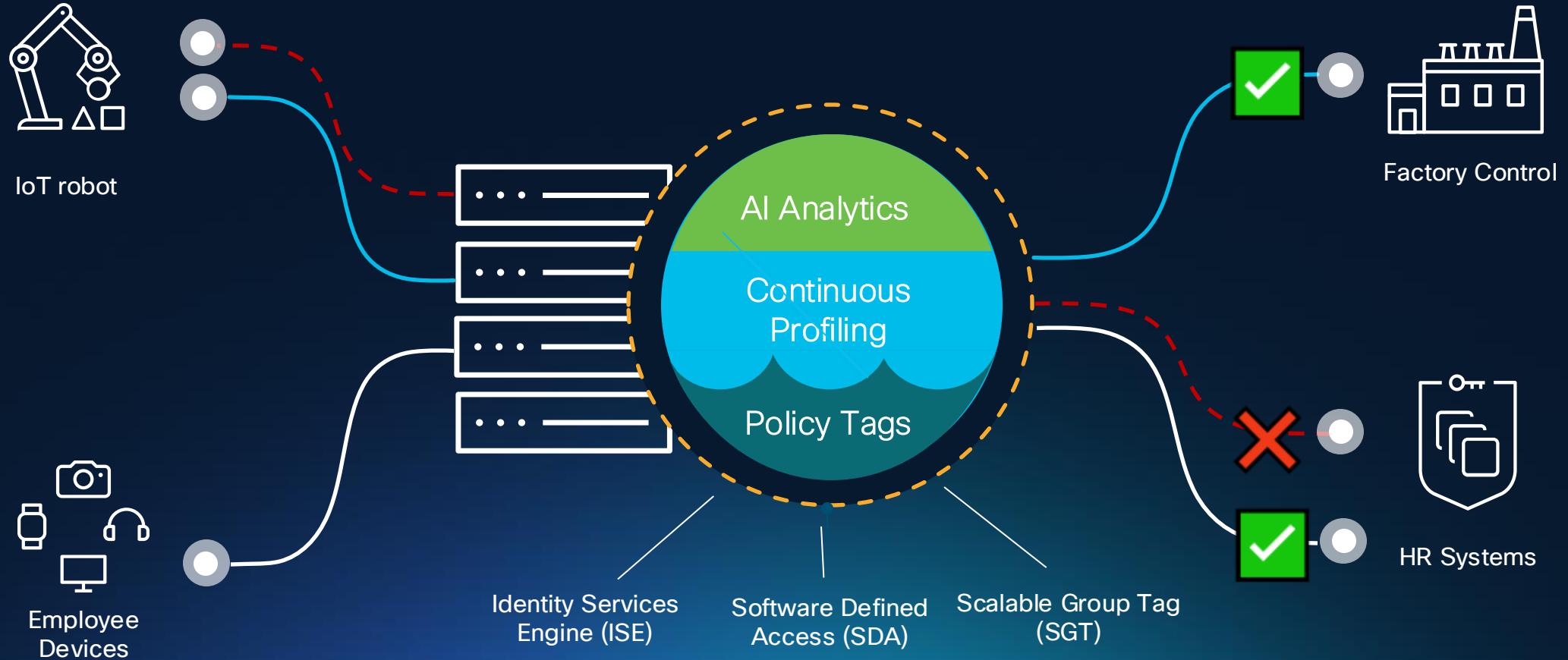
WAN MACSec

Post-Quantum
Cryptography

- Low latency
- High bandwidth
- FIPS compliant

Securing network access

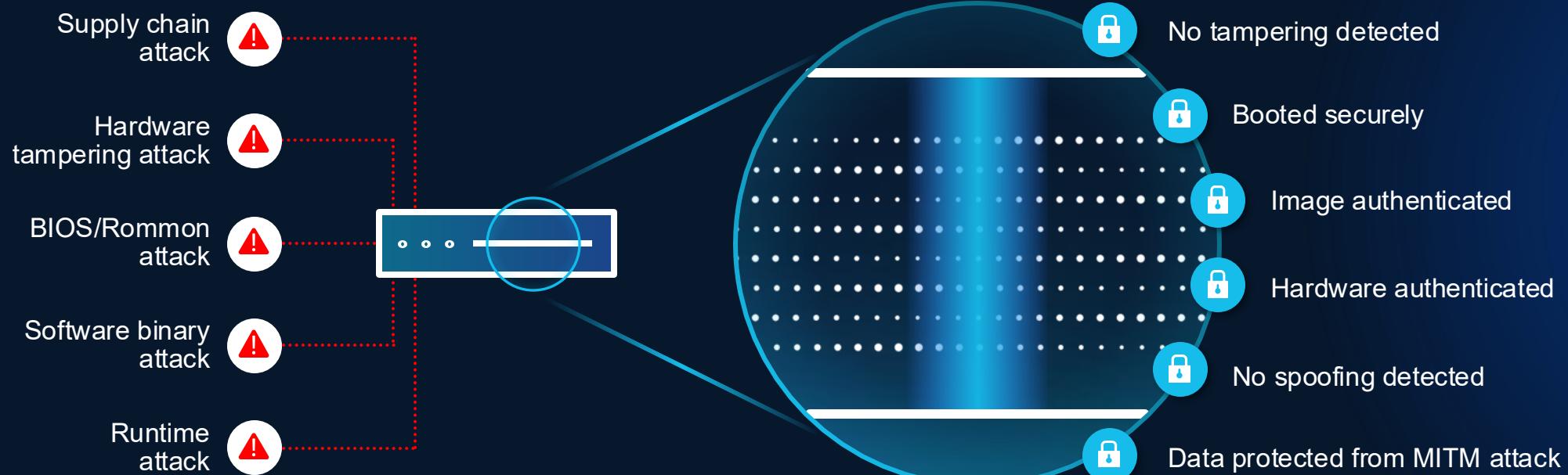
Scalable microsegmentation to protect every connection



Securing the device

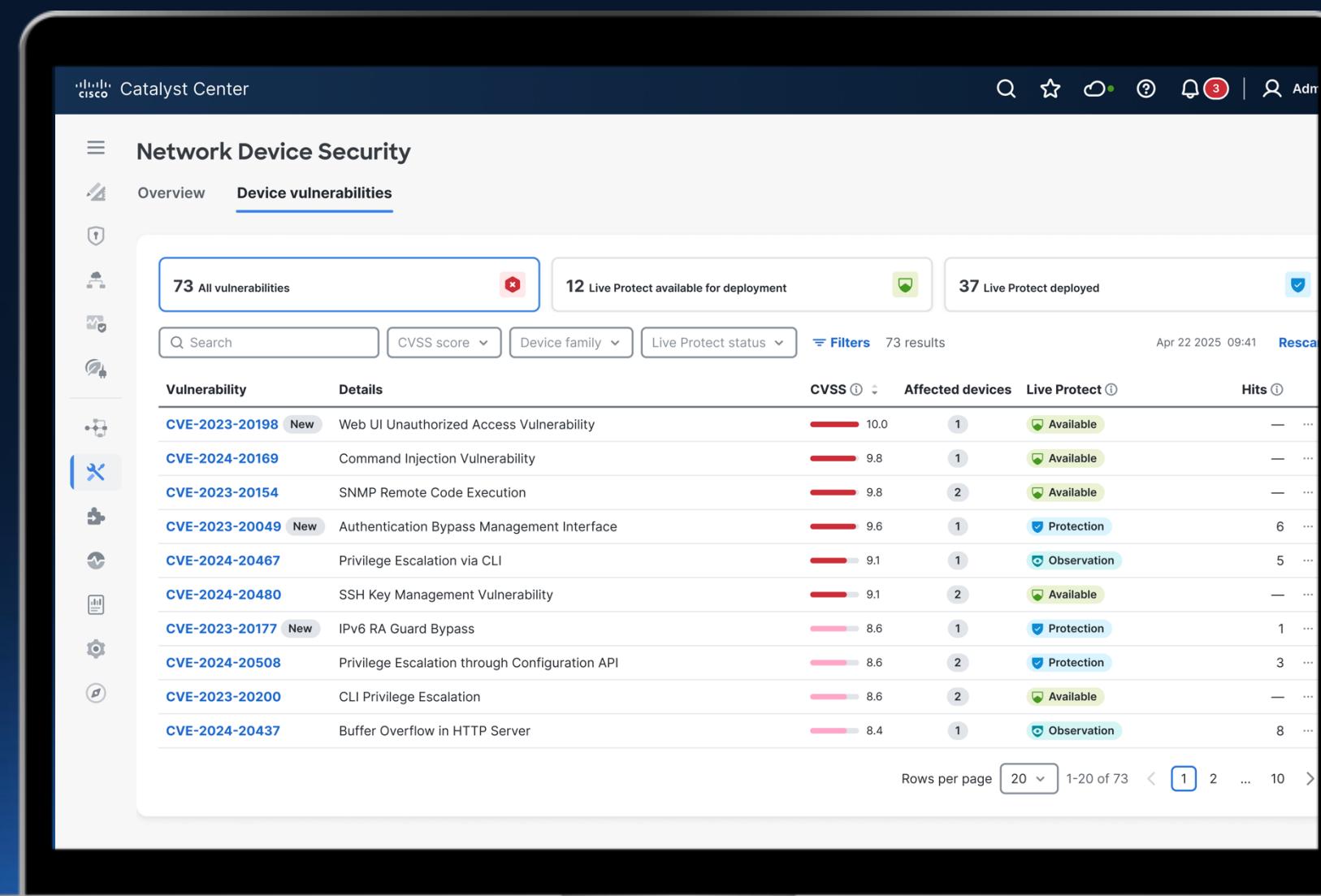
Secure from hardware to software, from boot time to runtime

Trustworthy Technologies Verification



Live Protect

Mitigate new threats in near-real time—without upgrading image or rebooting device



The screenshot shows the Cisco Catalyst Center Network Device Security interface. The top navigation bar includes a search icon, a star icon, a cloud icon, a refresh icon, a bell icon with a '3' notification, and a user profile icon. The main title is 'Network Device Security' with tabs for 'Overview' and 'Device vulnerabilities' (which is selected). On the left, there is a vertical sidebar with icons for device management, security, and monitoring. The main content area displays a table of vulnerabilities:

Vulnerability	Details	CVSS	Affected devices	Live Protect	Hits
CVE-2023-20198 <small>New</small>	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	Available	—
CVE-2023-20049 <small>New</small>	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 <small>New</small>	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	Available	—
CVE-2024-20437	Buffer Overflow in HTTP Server	8.4	1	Observation	8

At the bottom, there are buttons for 'Rows per page' (20), '1-20 of 73', and navigation arrows. The date 'Apr 22 2025 09:41' and a 'Rescan' button are also visible.

Challenges in the branch

**Growing
operational
complexity**



**Rising security
vulnerabilities**



**Lean IT teams &
talent shortages**



**Demanding apps
and new AI
workloads**



This requires a new
branch architecture

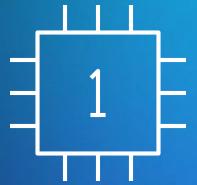


Architecture for Unified Branch

Operational simplicity
powered by AI



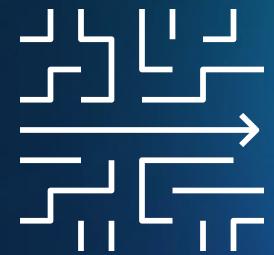
Scalable devices
ready for AI



Security
fused into the network



Operational Simplicity powered by AI



What products make up the Unified Branch?

Meraki Dashboard



Wi-Fi

Cisco Wi-Fi 7



Switching

Cloud-Managed Catalyst
Meraki Switching
Cisco Smart Switches



Routing+ Firewall+SASE

Meraki MX
Cisco Secure Routers
Secure Access + SASE

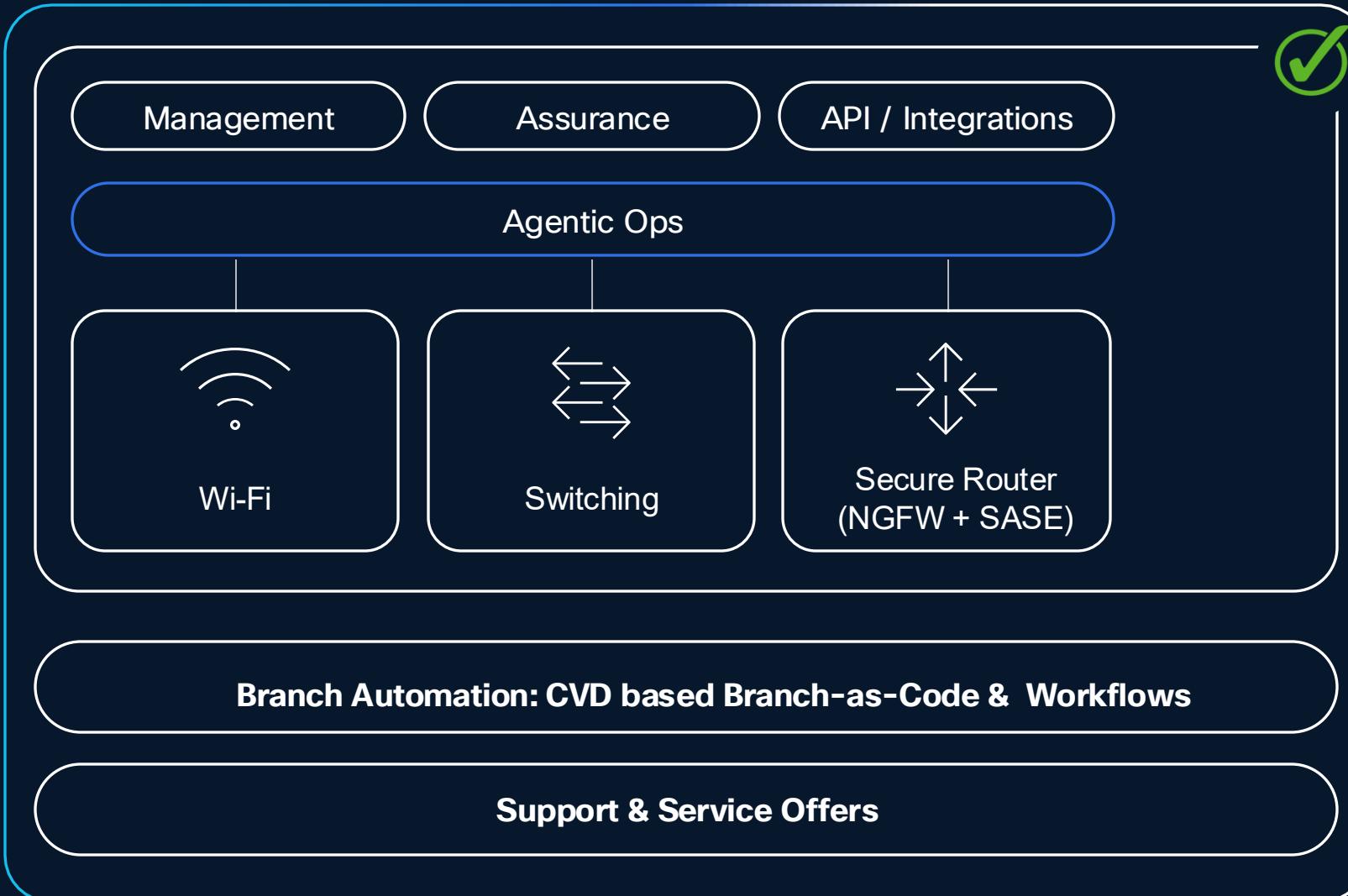


ThousandEyes

Small
Medium
Large



Introducing Unified Branch: Platform led Secure Networking Architecture



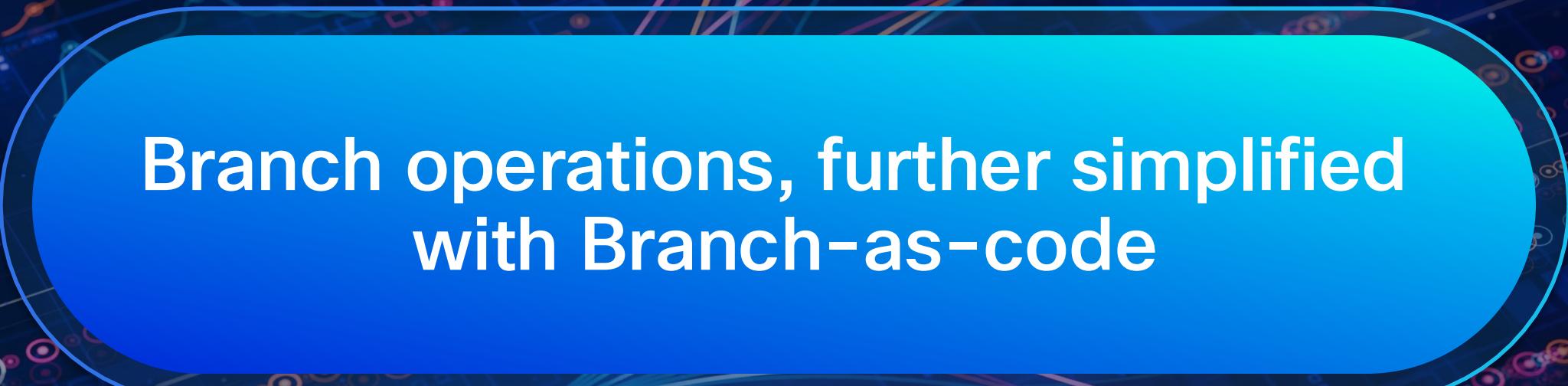
Full stack + platform led architecture:
Secure WAN services, Switching
and Wi-Fi

ThousandEyes – proactive, end-to-end
visibility, performance insights, and
assurance.

New automation toolkit – Branch as
Code and workflows –prebuilt data
model and automation to deploy Branch
at scale.

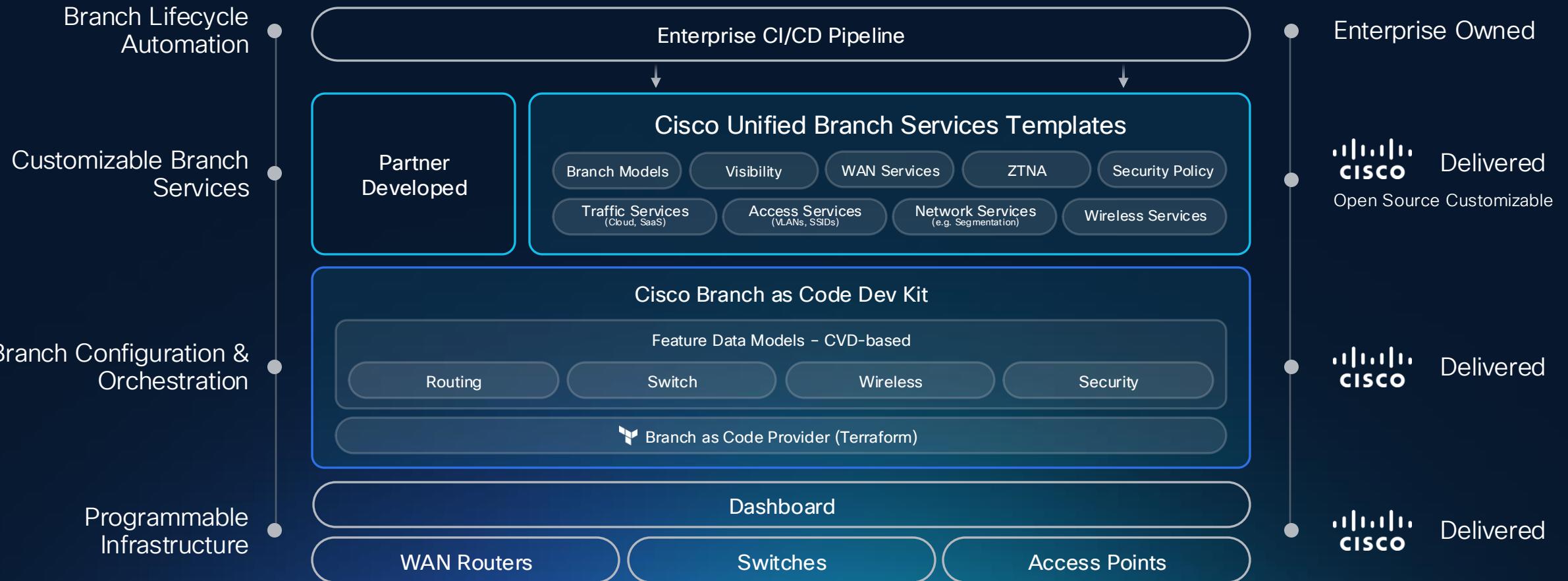
Cisco Validated Design – recommend
and tested branch designs for reliable &
resilient operation.

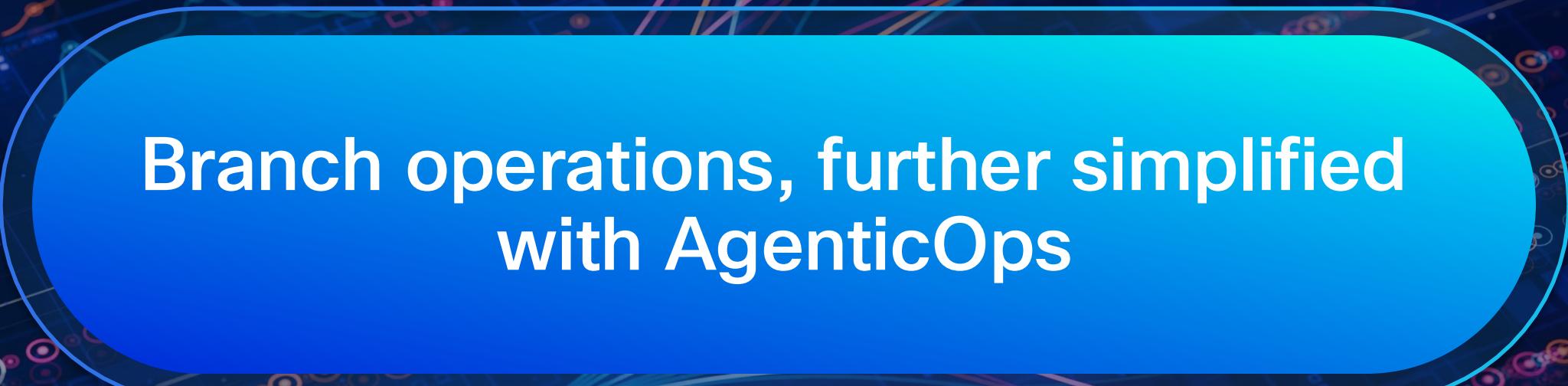
Aligned Support & Service offers
Enhanced support for Unified Branch
streamlines & enhances customer care



Branch operations, further simplified
with Branch-as-code

Large scale deployments with Branch as Code stack





Branch operations, further simplified
with AgenticOps

Scalable branch devices ready
for AI

Introducing the industry's most advanced secure router

Secure Networking Processor

Post Quantum Security capable
with 3x higher throughput

Advanced Security

NGFW and SASE with
3x Threat protection

Assurance

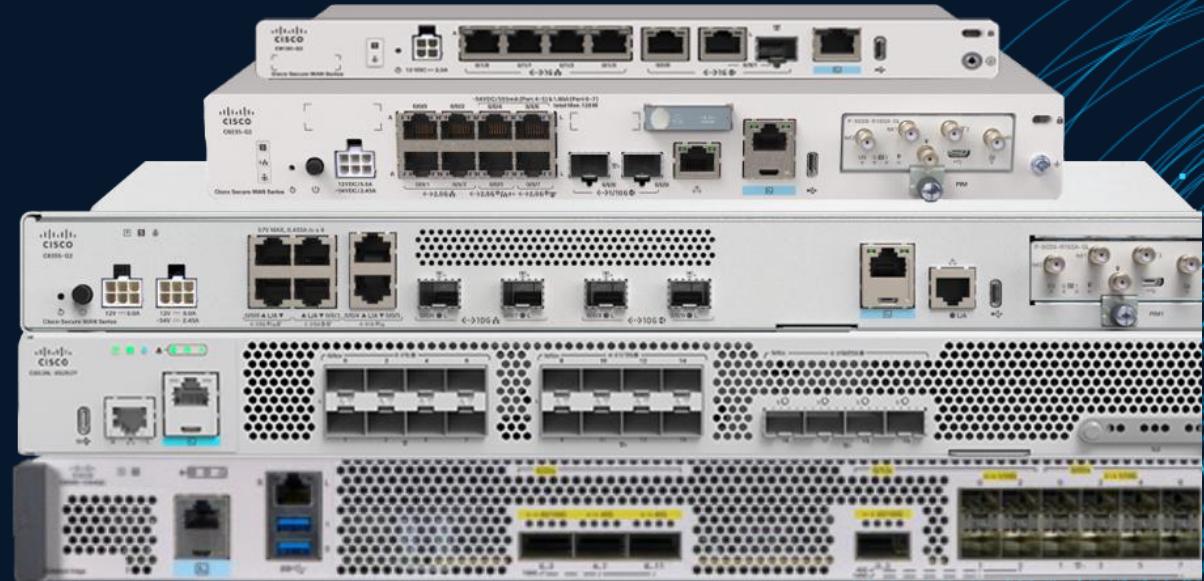
ThousandEyes with Traffic Insights
AI Troubleshooting

Cloud Management

IOS-XE managed by dashboard

Simplified Licensing

Cisco Networking & Routing Subscriptions



Cisco 8000 Series
Secure Routers

Secure Networking Processor

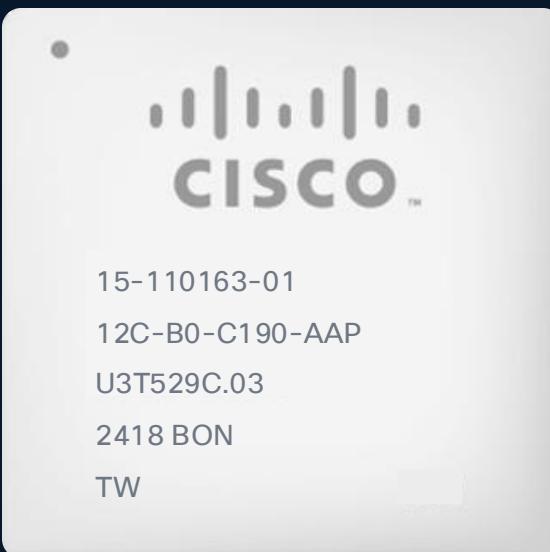
Purpose built for the Future AI Workloads

C8400, C8300, C8200, C8100 Series Secure Routers are powered by 'secure networking processor'



Security

- Inline Crypto
- PQC capable crypto engine
- Cisco Secure Firewall acceleration
- Built-in AI/ML inferencing engine



Networking

- Integrated hardware accelerators
- Various Ethernet standards- 2.5mGig, 5mGig, 10GE, 25GE
- Performance defined Power - 30%+ power saving
- Programmable uCode - feature parity

1.5 Gbps encrypted
threat protection

Up to 3x price-
performance

Integrated SD-WAN

Introducing Advanced on-box threat inspection for the branch



AVAILABLE DEC 2025

Cisco Secure Firewall 200 Series

Security fused into the network

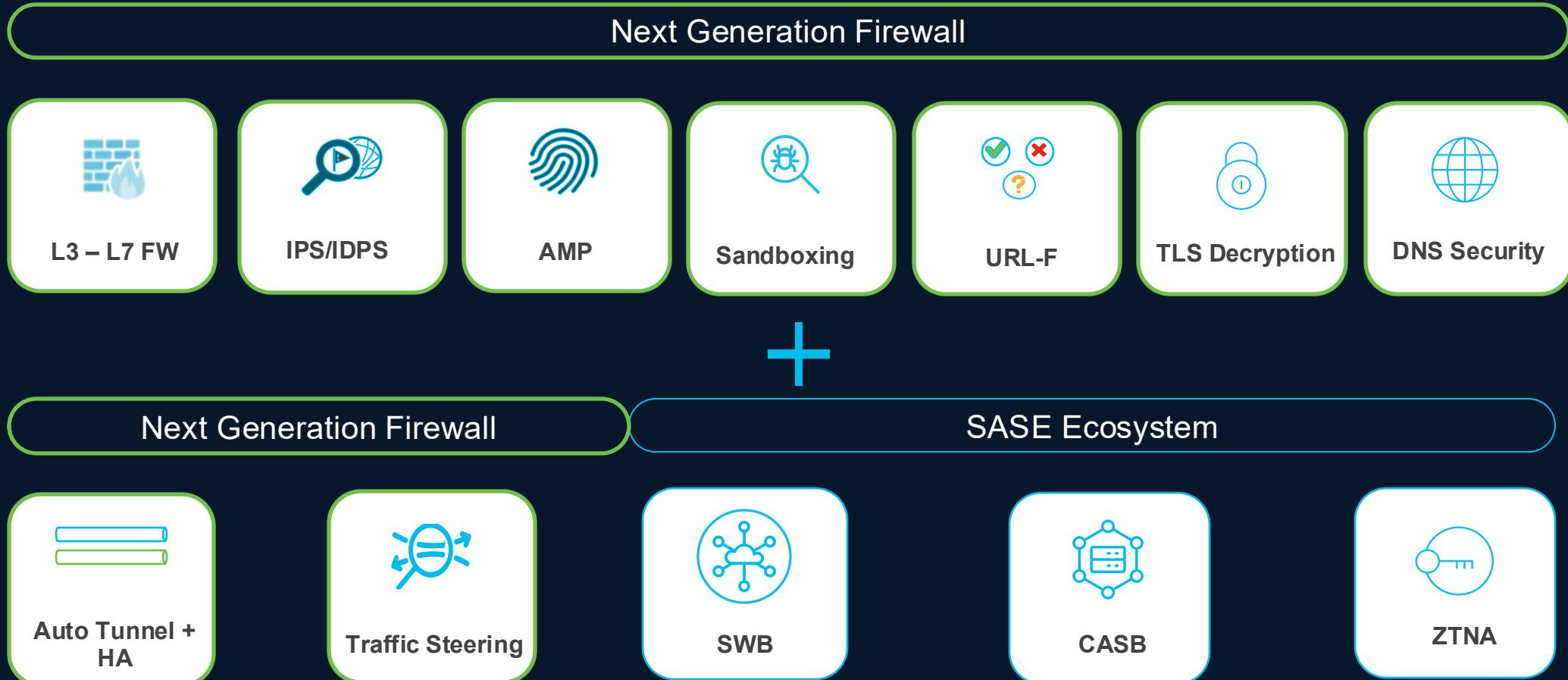


Cisco eases your journey to a future proof secure branch



*when combined this is known as SASE architecture

Secure Firewall embedded in the Secure Router



SASE: Secure Access integrated with Cisco SD-WAN

Your security strategy for a hyper-distributed world

SASE

Secure
SD-WAN

Converged set of **cloud networking**

+

Security
Service Edge

Converged set of **cloud security**

End-to-end Assurance with ThousandEyes

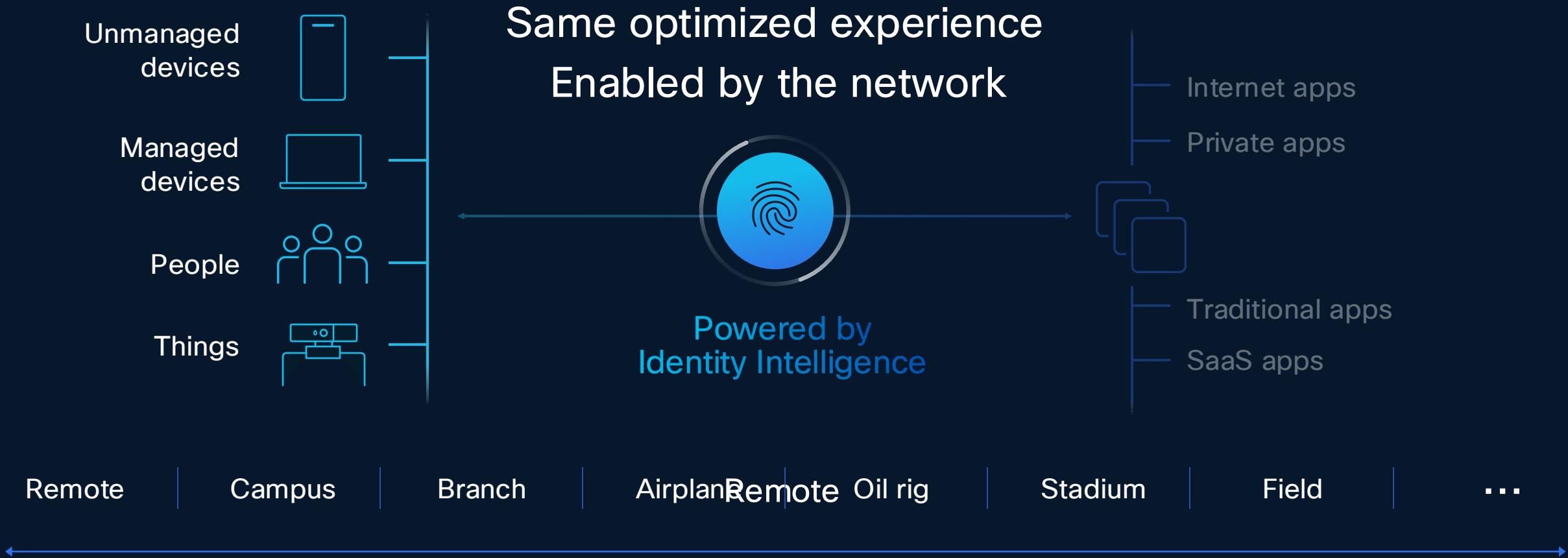
Extend consistent identity context across SD-WAN and cloud security enforcement

ISE security group tags (SGTs) for granular access policy



* Capabilities are planned but not yet available or guaranteed.

Securing Users, Device access to Apps with Universal ZTNA from Cisco



Thank you



