

Delivering on the Promise of the AI-Ready Campus & Branch: Smart, Secure and Scalable Networks

Corey Turner, Solutions Engineering Director

Brett Moore, Solutions Engineer

Michael Kutka, 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?

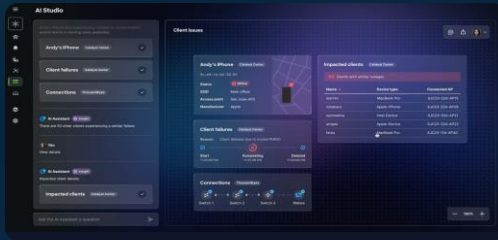
For explosive traffic, for increased security risks, for more complexity



AgenticOps

The New Standard for IT Operations

ALPHA | OCTOBER



AI Canvas

Cross-domain collaborative troubleshooting

CONTROLLED RELEASE | OCTOBER



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.

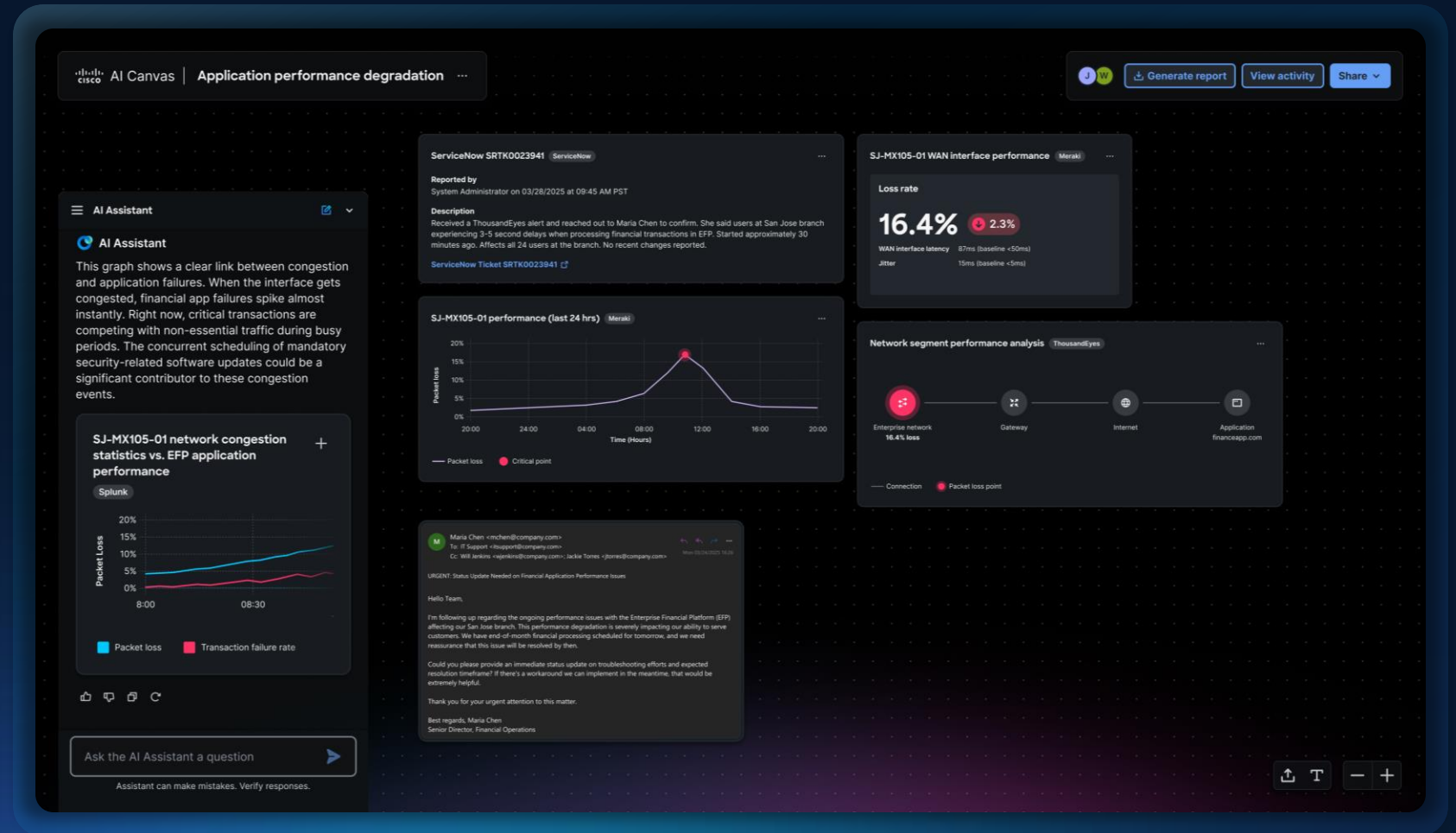
ALPHA | OCTOBER

AI Canvas

Troubleshooting and execution across multiple domains

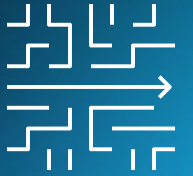
Collaboration across multiple users (NetOps, SecOps and execs)

Built on the foundation of the Deep Network Model

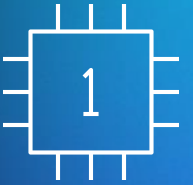


Architecture for Secure Campus

Operational simplicity
powered by AI



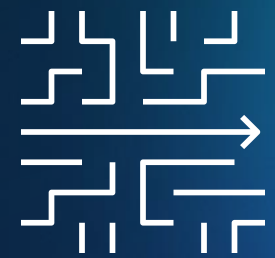
Scalable devices
ready for AI



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

Our unified platform

PLATFORM

Management

Assurance

API / Integrations

Intelligence

HARDWARE



Smart
Switches



Secure
Routers



Wireless



Industrial
IoT

Expanded cloud-managed networking portfolio



Wireless

Full wireless support
Scale large campus wireless
with Campus Gateway

GA | MAY



Switching

Expanding cloud management
support from fixed access to
modular (C9610)

GA | DEC



Routing

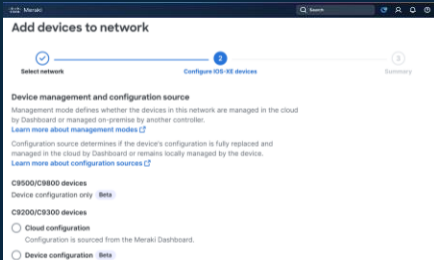
Next-gen routing
support coming

ALPHA | JUNE

Powered by cloud management with IOS XE

Large campus cloud capabilities

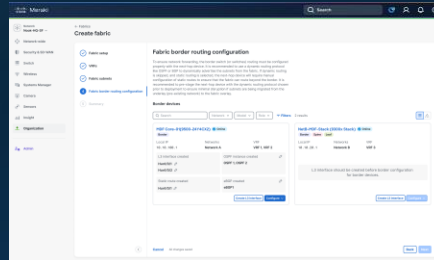
Powerful Switching Capabilities



Support campus deployments with BGP, VRF, ISSU, and StackWise

BETA| NOW

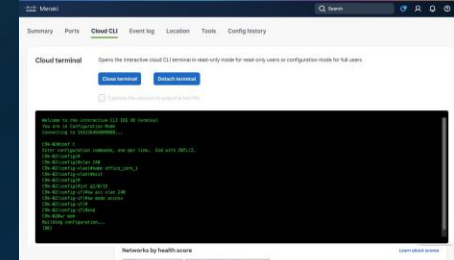
Fabric for Secure Networking



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

BETA | DEC

Cloud CLI for Flexibility



Simplify onboarding and flexibility with operating mode options and Cloud CLI

GA | NOW

AVAILABLE | NOW

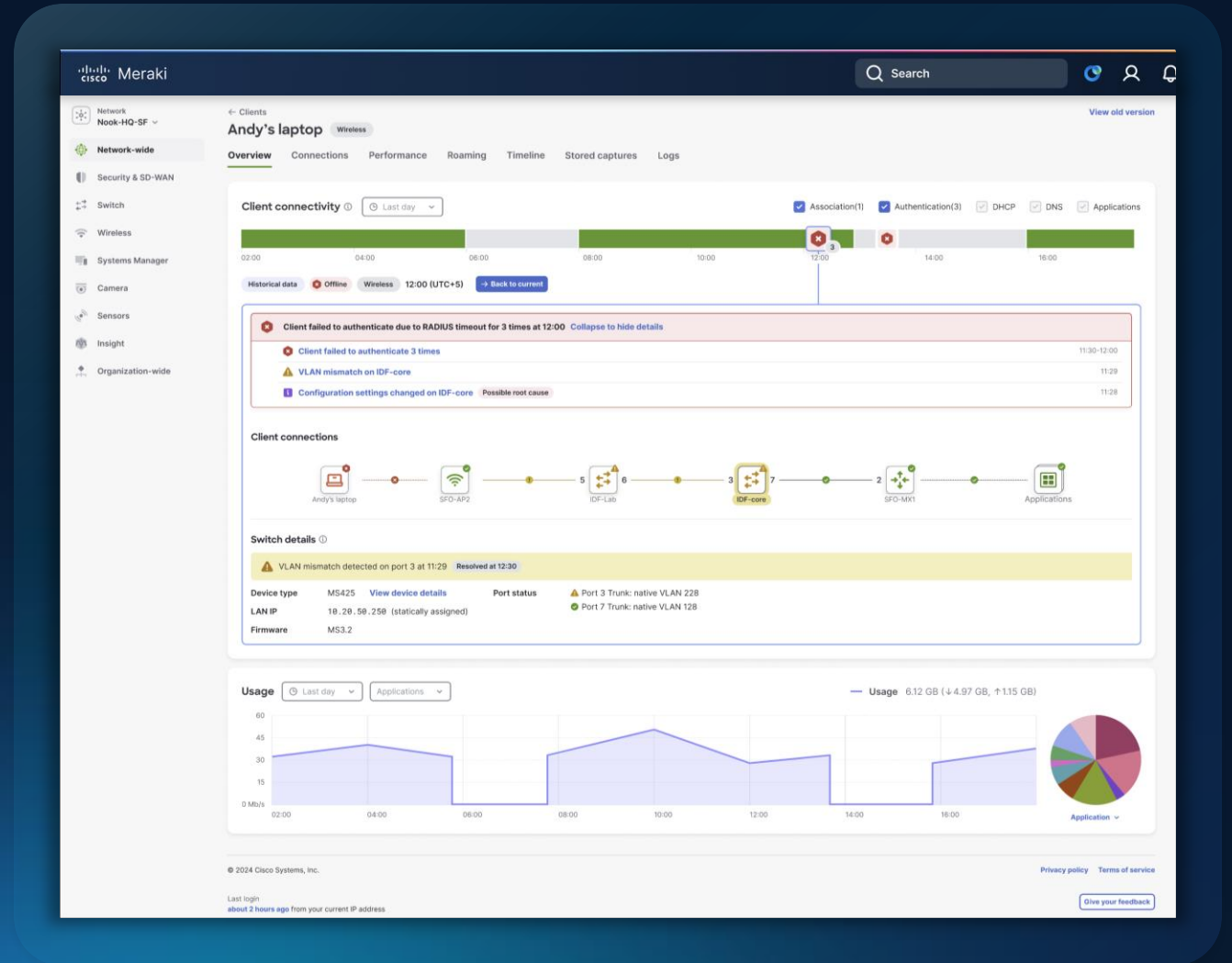
Assurance across every digital experience

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



[Show Filters](#)

< > >|



00:30

00:45

01:00

01:15

01:

01:45

02:00

Map

Table

2 Of 2 Agents ▼

IP Address Labels ☒

Agents by Agent ▼

Interfaces by IP Address ▾

Destinations by No Grouping ▾

All ▾

Search Network, Country, IP Ac

0 matches

Forwarding Loss > 10% (0 Nodes) ▼

Link Delay > 100ms (0 Links) ▼

Click a node or link

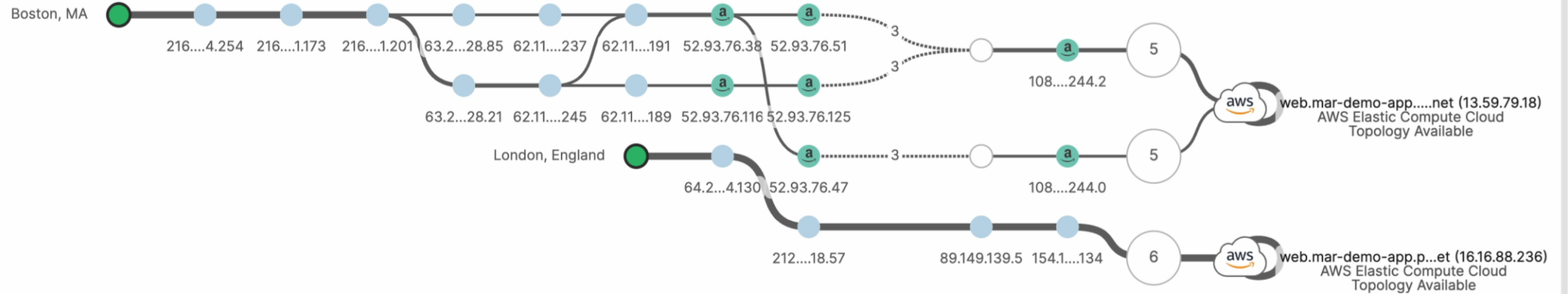
Info (1) ▼

8 hops

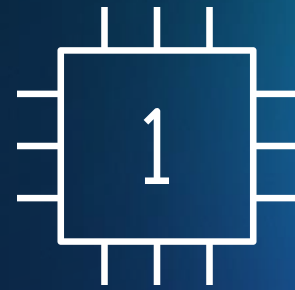
3 hops

↶ Undo (1)

Reset To Default



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

INTRODUCING

Scalable devices ready for AI

Smart Switches



Secure Routers



Campus Gateway



Secure Firewall



Large Venue Wi-Fi 7



ALL ORDERABLE JUNE 2025

Introducing Smart Switches for the AI-powered campus

High-performance,
low latency

Cisco Silicon One +
co-processor for
security and AI

Post-quantum
secure

Intelligent energy
efficiency



Cisco C9350 Smart Switches

AVAILABLE JUNE 2025

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

Introducing

Smart Switches for the AI-powered campus



AVAILABLE JUNE 2025

Cisco C9610 Modular Core Smart Switches

Boosts hardware
encryption post
quantum security

Intelligently adaptable to
mitigate link failures,
congestion, and
bandwidth challenges

Flexible and
programmable for
future AI and ML
workloads

High-scale and
low latency for time-
sensitive applications

Efficient power
performance

Powered by Cisco Silicon One for Scale, Security, and Efficiency



**Silicon One A100L and
Silicon One K100L**

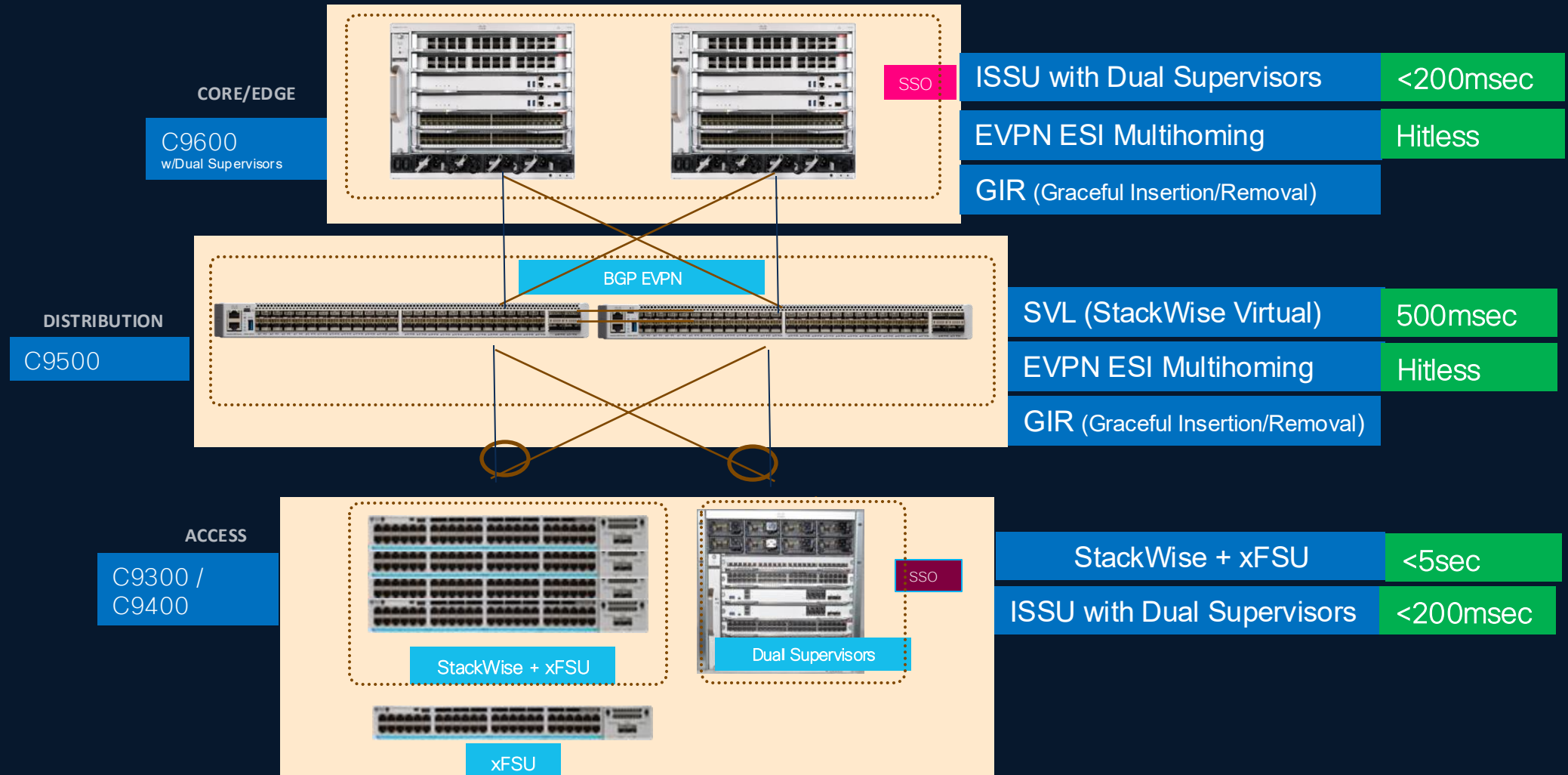
Highly Resilient Architectures

Catalyst 9000: Redundancy at Every Layer



Minimize traffic impact across all layers of redundancy

Campus Resiliency at Every Layer



Catalyst 9K – EVPN Multihoming

17.18.1: Beta for Non-Fabric | Fabric available now

17.18.2 + 26.1.1: GA code expected in Q1 2026

Meraki Fabric

Create fabric

Network-wide

Security & SD-WAN

Switch

Wireless

Systems Manager

Camera

Sensors

Insight

Organization

Admin

1 Fabric setup

2 VRFs

3 Fabric subnets

4 Fabric border routing configuration

5 Summary

The Meraki fabric can be composed of one or many networks and devices in those networks to provide a BGP-EVPN fabric overlay.

To create a fabric, you will need to provide a name, select one or many networks where the fabric will be built, and select and assign the roles to the applicable switches in the list below.

Fabric name

San Jose campus

Select networks/network group

Network A

Network B

BGP autonomous system number

65500

BGP auth key

Underlay loopback IP pool

192.0.0.0/23

Select roles for devices

The list will populate all fabric supported switches that are in the networks selected. The default roles are defined as Borders, Spines, and Leaves, but can be modified to assign multiple roles to a single switch based on the network design and use case.

Search

Network

Model

Role

Filters 6 results

2 items selected Select all

Remove role

Edit role

Devices	Status	Local IP	Networks	Serial column	Tag	Roles	Action
☒ MDF Core-01(9500-24Y4CX2)	Online	10.10.100.1	Network A	Serial number	Tag		
☒ MDF Dist-01 (9500-48Y4Cx2)	Online	10.10.192.1	Network A	Serial number	Tag 1 Tag 2		
☐ MDF Dist-02 (9500-48Y4Cx2)	Online	10.10.176.1	Network A	Serial number	Tag 2	Leaf	
☐ NetB-MDF-Stack (9300x Stack)	Online	10.10.20.1	Network B	Serial number	Tag 3	Border Spine Leaf	
☐ NetC-MDF-Stack (9300x Stack)	Online	10.10.40.1	Network C	Serial number	Tag	Border	
☐ NetD-MDF-Stack (9300x Stack)	Online	10.10.30.1	Network D	Serial number	Tag	Border	

Rows per page

30

1-30 of 300

1

2

...

10

>

Cancel All changes saved

Next

Wi-Fi 7 for every operational scale



CW9172

6 spatial streams

Omnidirectional

Ceiling mount and
wall plate form factor



CW9176I

12 spatial streams

Omnidirectional

10 Gbps, GPS, UWB



CW9176D1

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

Security fused into the Network



Security Fused into the Network



Securing application access over the WAN

Protecting user access and application interactions

SASE/UZTNA

- Continuous identity, posture and risk assessment across every session



Securing network connectivity

Safeguarding and optimizing network connections

Quantum-resistant:

- MACsec
- IPsec
- WAN MACsec



Securing network access

Securing connectivity to the network

Authorization and scalable segmentation

- Identity services engine (ISE)
- Software defined access (SDA) and Security Group Tags (SGT)
- NGFW



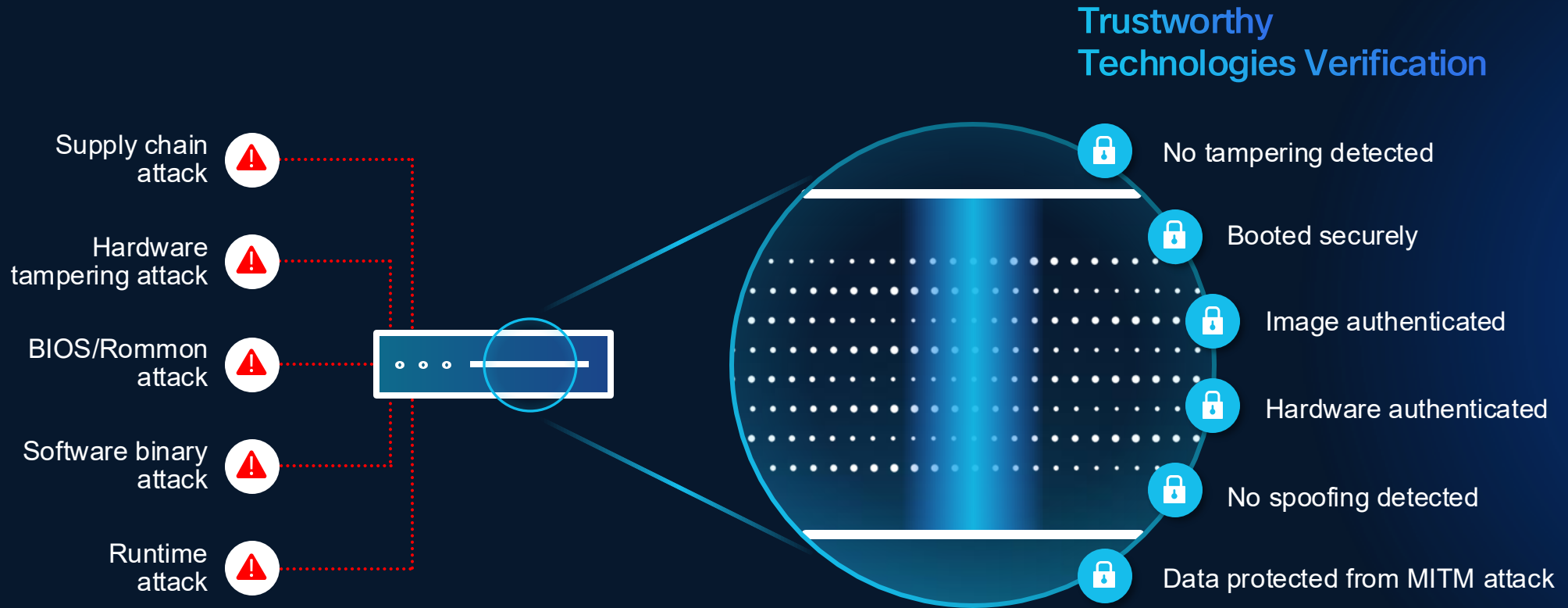
Securing the device

Protecting and ensuring compliance of devices

Quantum-resistant secure boot
Compensating controls

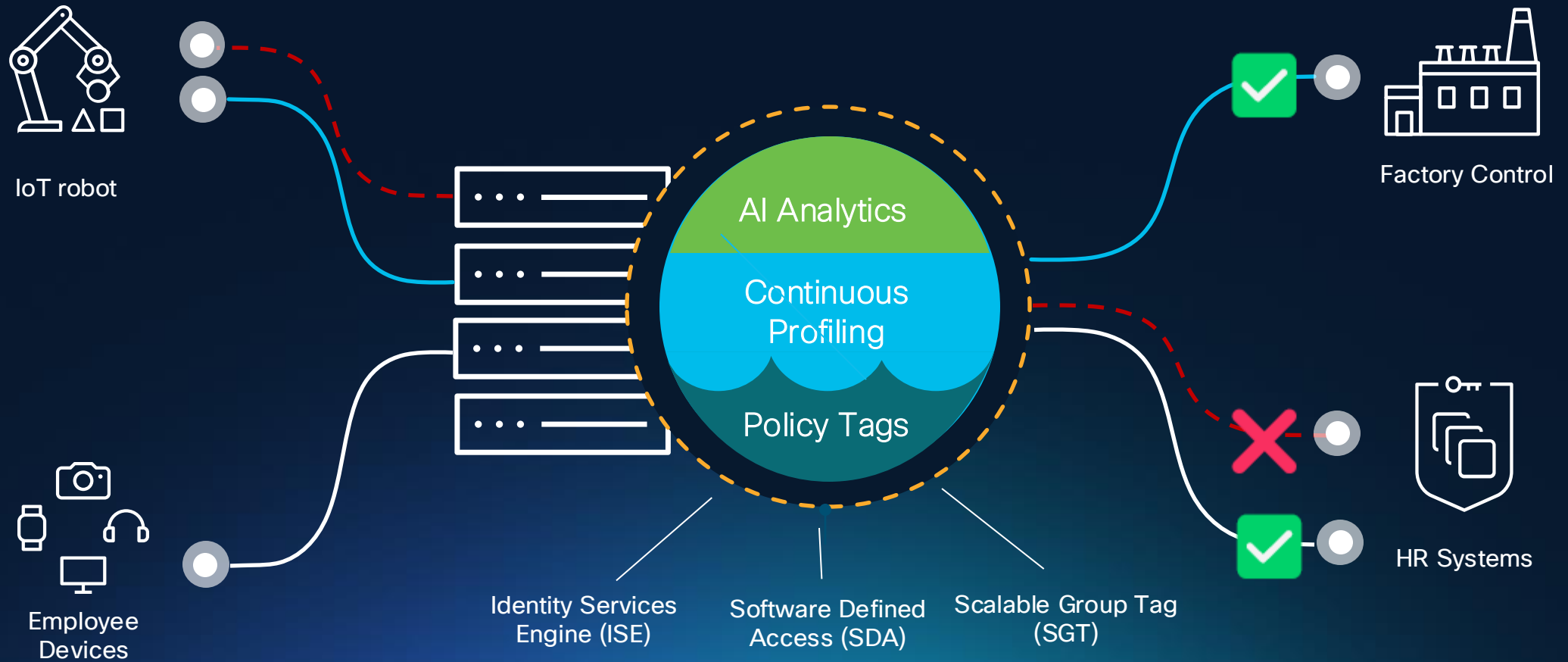
Securing the device

Secure from hardware to software, from boot time to runtime



Securing network access

Scalable microsegmentation to protect every connection



FUTURE

Live Protect

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

The screenshot displays the Cisco Catalyst Center interface for Network Device Security. The main section is titled "Device vulnerabilities" and shows a summary of 73 all vulnerabilities, 12 Live Protect available for deployment, and 37 Live Protect deployed. Below this is a table of vulnerabilities with columns for Vulnerability, Details, CVSS score, Affected devices, Live Protect status, and Hits. The table lists several vulnerabilities, including CVE-2023-20198, CVE-2024-20169, CVE-2023-20154, CVE-2023-20049, CVE-2024-20467, CVE-2024-20480, CVE-2023-20177, CVE-2024-20508, CVE-2023-20200, and CVE-2024-20437. The Live Protect status for each vulnerability is indicated by a green shield icon and a label (Available, Protection, or Observation). The interface also includes a search bar, filters, and a pagination control at the bottom right.

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	Available	—
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	Available	—
CVE-2024-20437	Buffer Overflow in HTTP Server	8.4	1	Observation	8

Network Device Security

Overview Device vulnerabilities

73 All vulnerabilities



12 Live Protect available for deployment



37 Live Protect deployed



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 >

Challenges in the branch

**Growing
operational
complexity**



**Rising security
vulnerabilities**



**Lean IT teams &
talent shortages**



**Demanding apps
and new AI
workloads**



Accelerate Innovation with Network Automation

Up to

90%

reduction in time to
launch new services.

Up to

70%

reduction in OpEx for
service delivery.

50%

fewer provisioning
steps with automation

Source: [ACG Research](#)

**This requires a new
branch architecture**

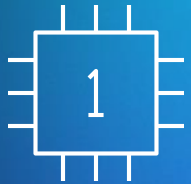


Architecture for Unified Branch

Operational simplicity
powered by AI



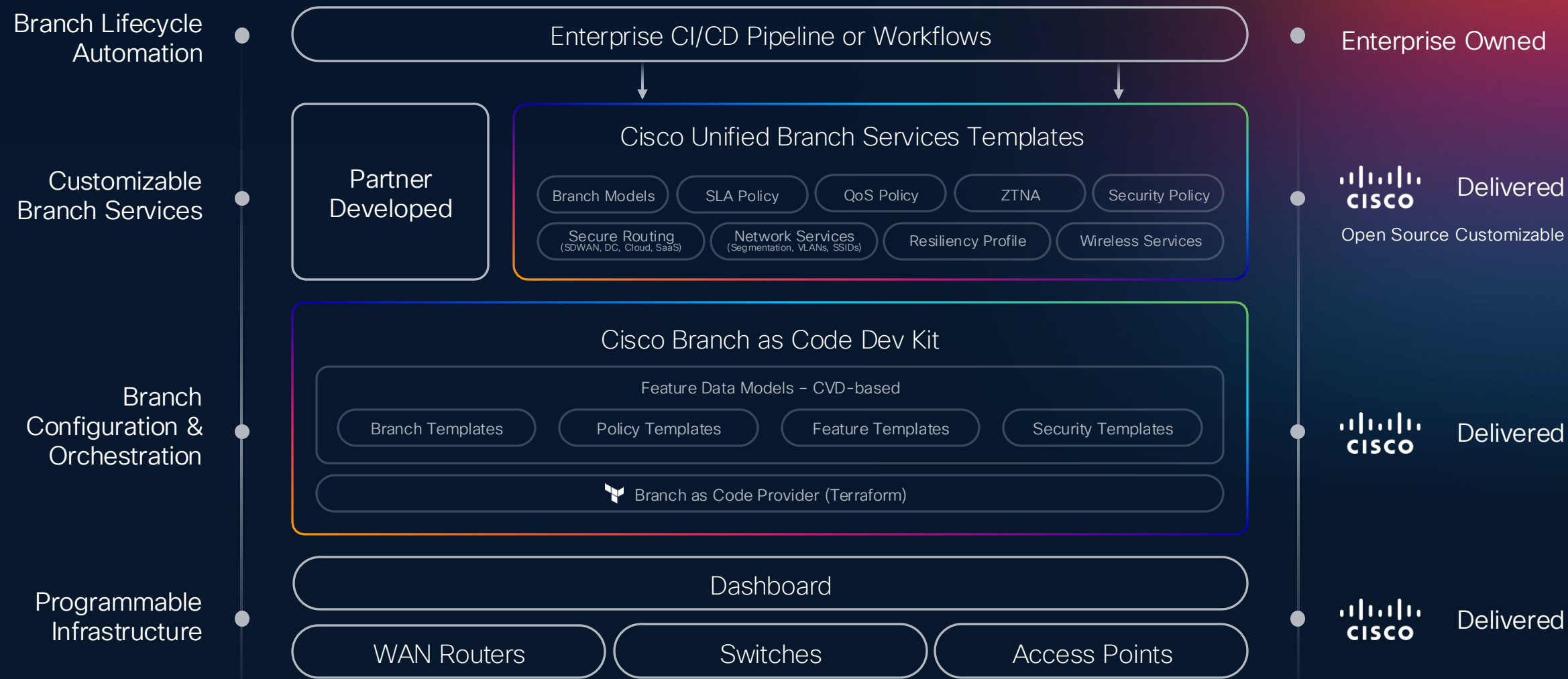
Scalable devices
ready for AI



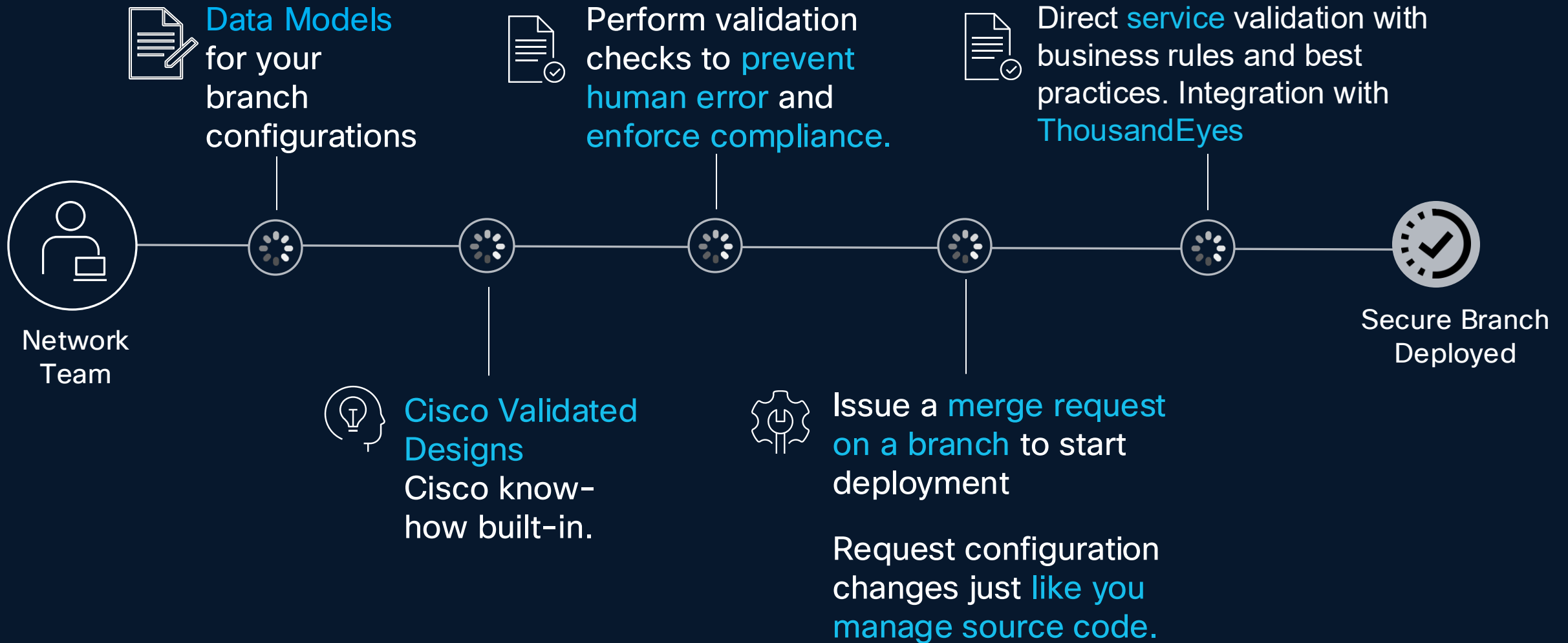
Security
fused into the network



Introducing Unified Branch: Platform led Secure Networking Architecture



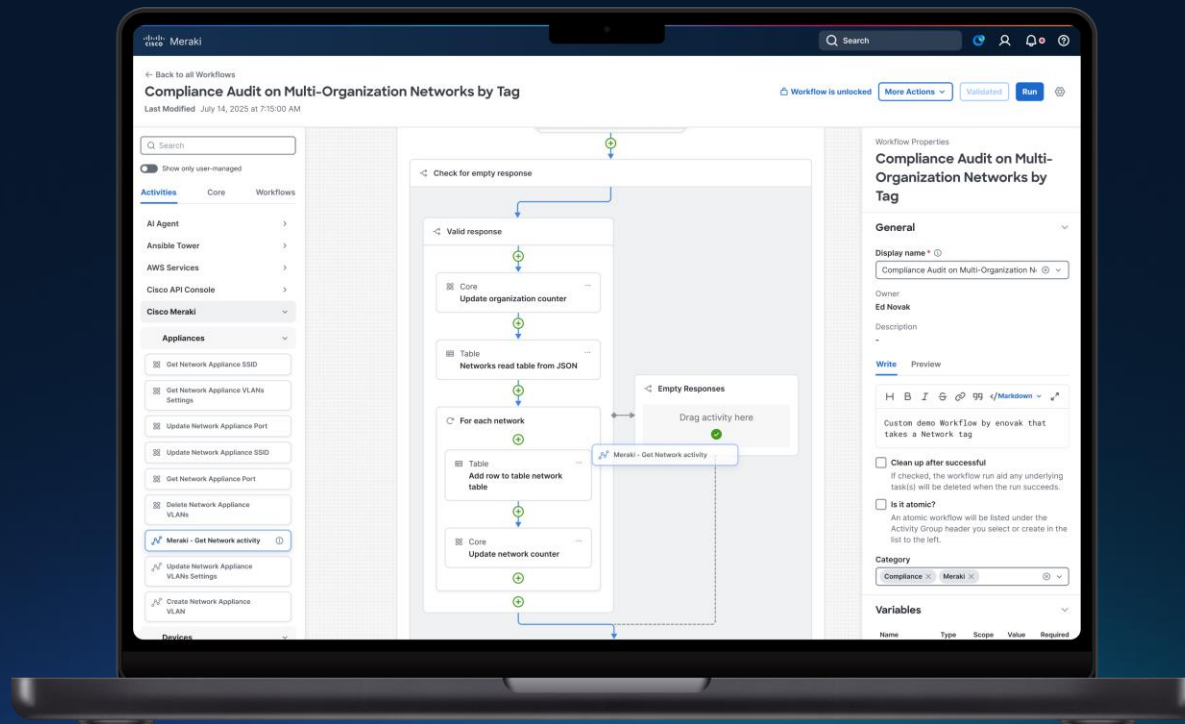
Unified Branch-as-Code Workflow



Introducing Workflows for Cisco Networking

AI-ready network automation

Low code/no code free automation tool integrated within the Meraki Dashboard



Cloud-Hosted
Automation

Drag and Drop
Creation / Editing

Custom and
Pre-Built

For Cisco & Third-
Party Domains

Network automation for Cisco and third-party applications



Automate tasks across Catalyst Center and SD-WAN, Meraki, ISE, ACI, Nexus, and more.

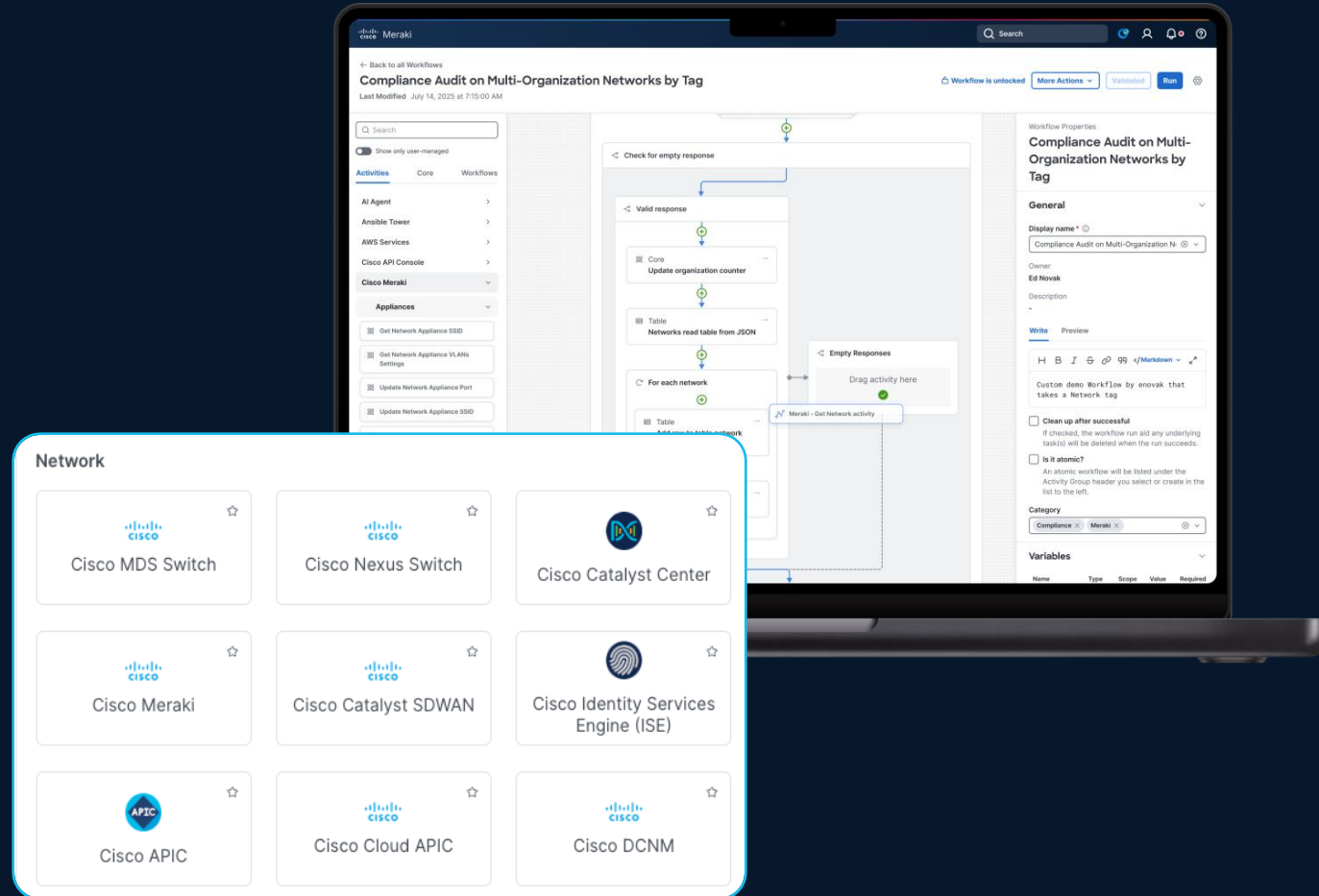


Integrate third-party applications such as ServiceNow and Jira with Cisco domains.



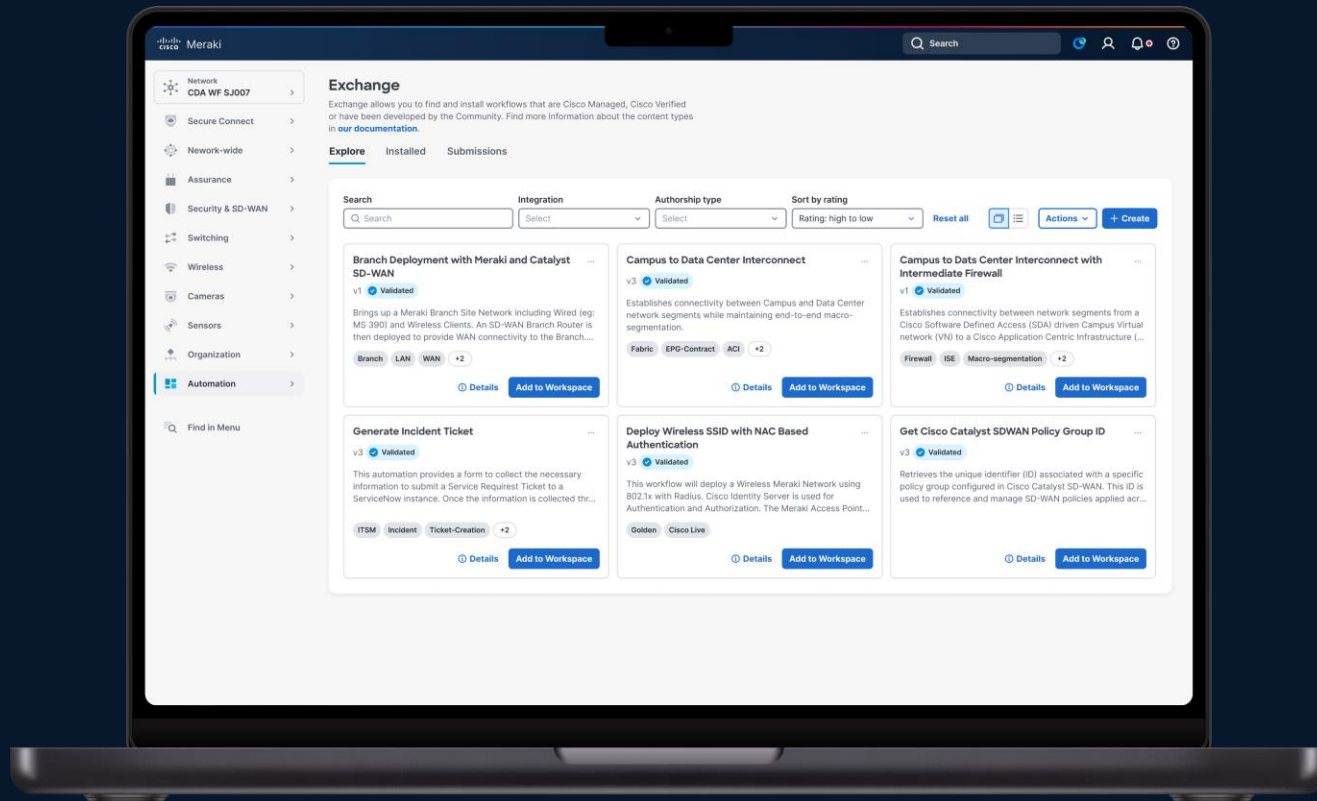
Connect cloud and on-premise controllers to extend automation across the Cisco portfolio and beyond.

Drag and drop your automation



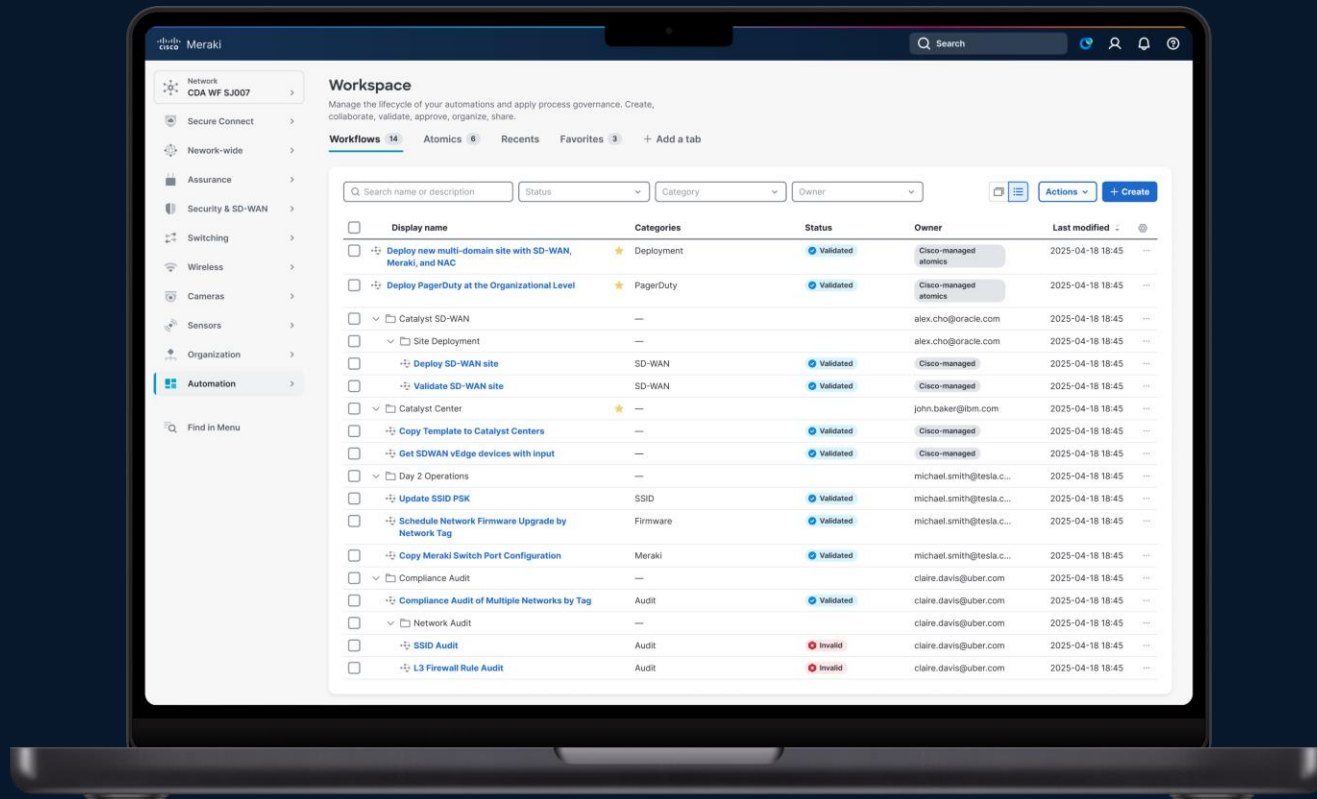
Bring your automation design to life with an intuitive drag-and-drop interface. Adapters provide automation capabilities across the Cisco portfolio. Each adapter contains a range of validated actions that can be automated across respective controllers.

Browse the Exchange



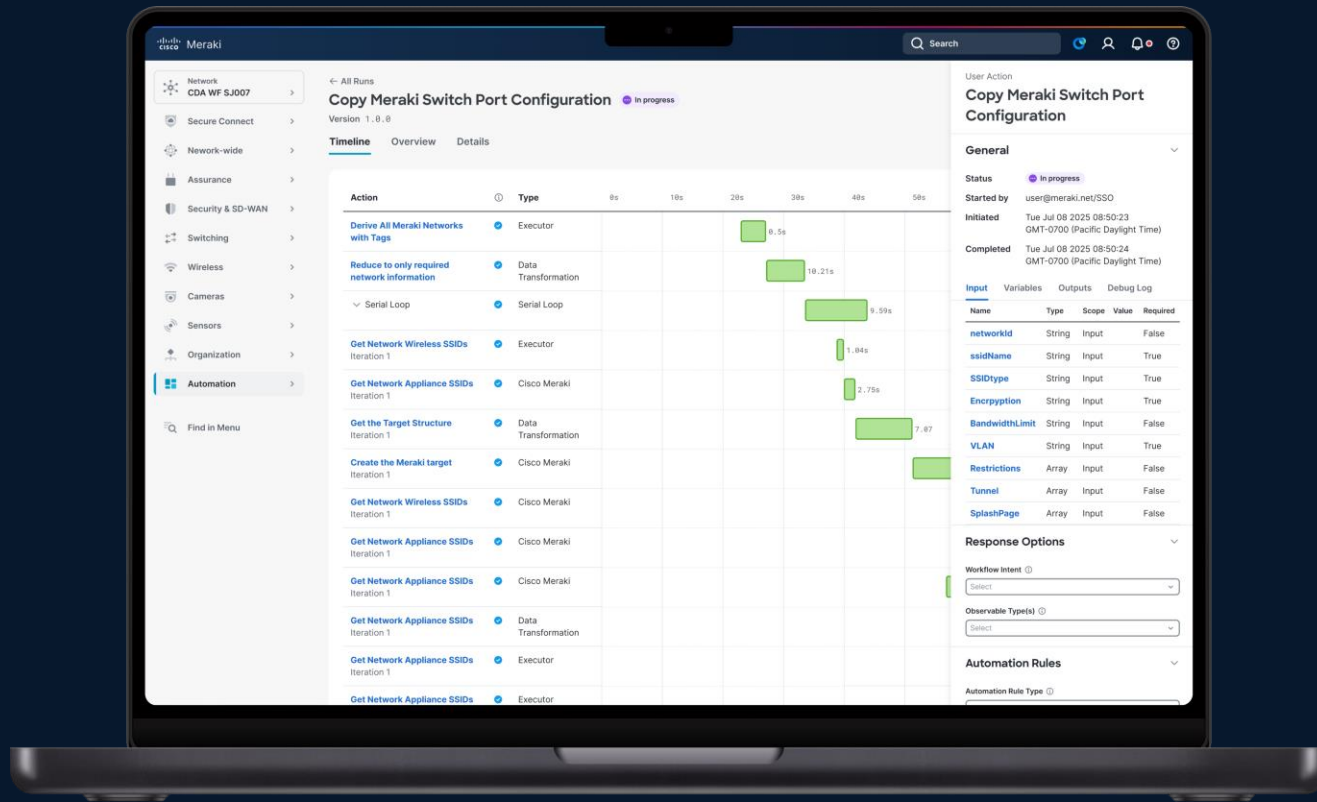
Workflows features an exchange of pre-made automations that solve common use cases. These automations can be run as is or easily customized in the drag-and-drop workflow editor. We frequently update our library with new, free automations.

View workflows in one place



Manage the lifecycle and status of your automations in the Cisco Meraki dashboard. Oversee processes and approve, collaborate, and validate parameters all in one place.

Monitor progress for active runs



Get insight into active automations from Workflows in the Automation tab in the Cisco Meraki dashboard. Monitor runs, see statuses, identify targets, troubleshoot errors, and keep logs for compliance and visibility.

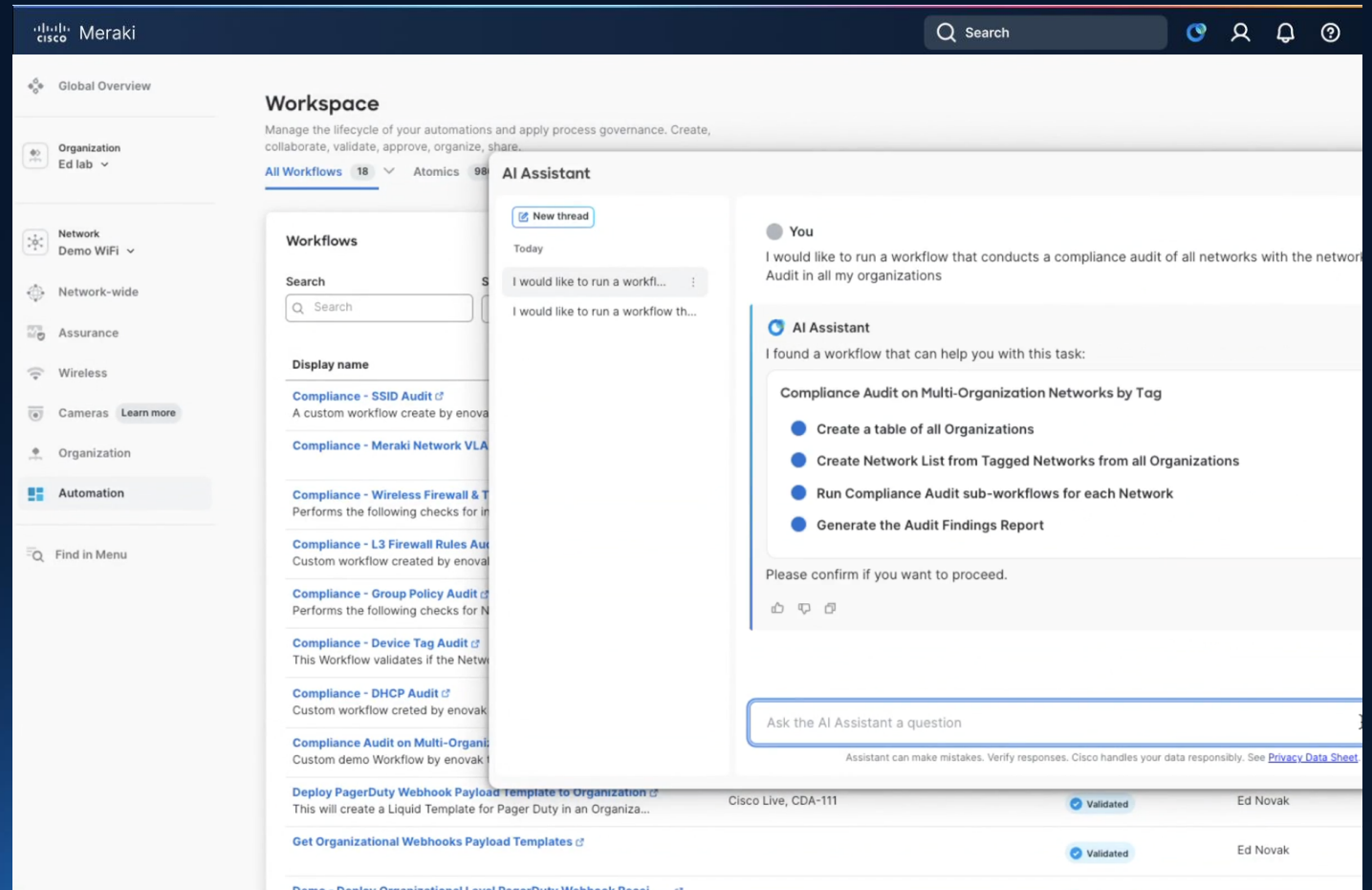
Workflows is fully integrated with Cisco AI Assistant

Leverage built-in AI Assistant integration for agentic operations using natural language

Faster workflow creation

Streamlined operations

Accelerated outcomes



AI Assistant powered RCA and resolution for issues in branch

Finds root cause—not just the alert

Provides full stack visibility

Pinpoints the issue and guides the fix

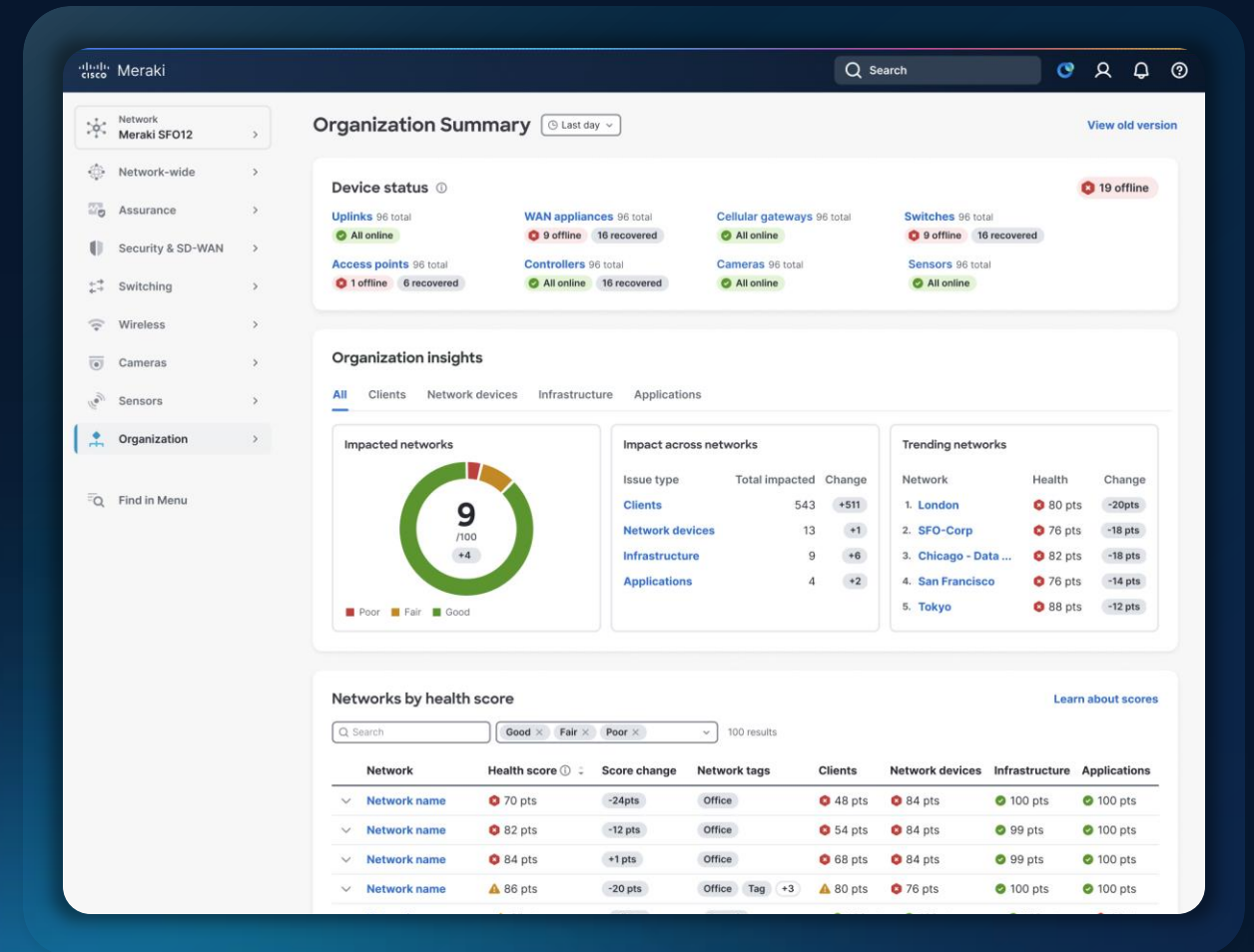


Unified Management – Catalyst and Meraki, any environment

Seamless control across cloud, on-prem, or hybrid

AI-powered automation and assurance

Granular access policy by user, device or application



**Scalable branch devices ready
for AI**

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

Deliver exceptional branch experiences

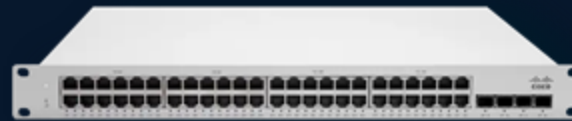
Smart Wi-Fi 7 access points and cloud-managed switches

Sustainable and energy efficient designs

Make every space smarter



Cisco Wireless
Wi-Fi 7



Cloud-managed
Switching



Security fused into the network



Security fused into the branch network

Securing users, things,
and agents UZTNA/SASE



Securing network access



Securing network connectivity



Securing the device



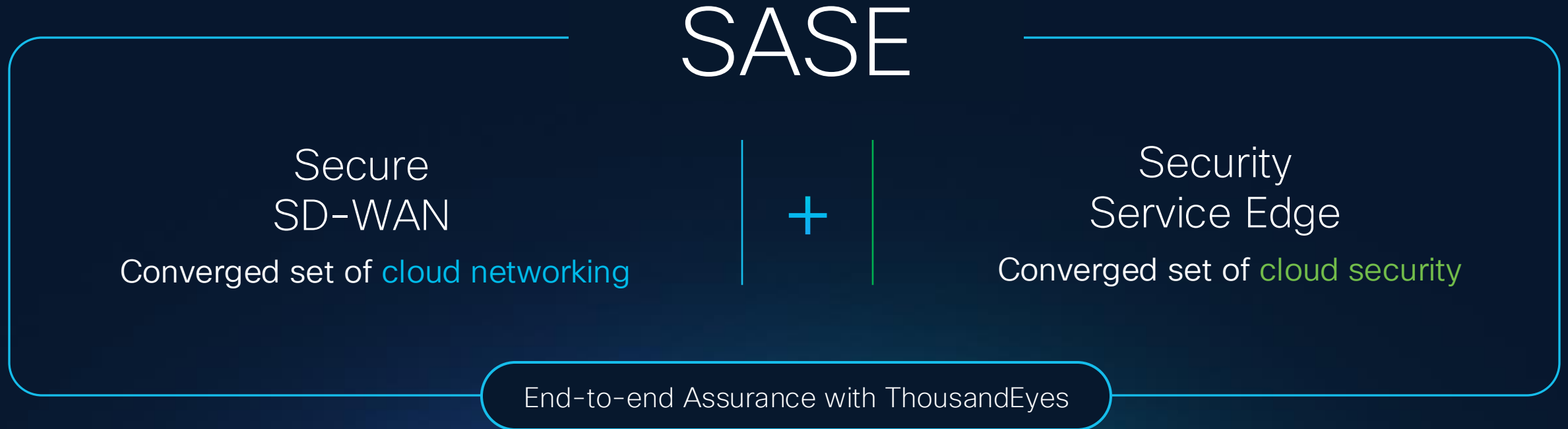
Cisco eases your journey to a future proof secure branch



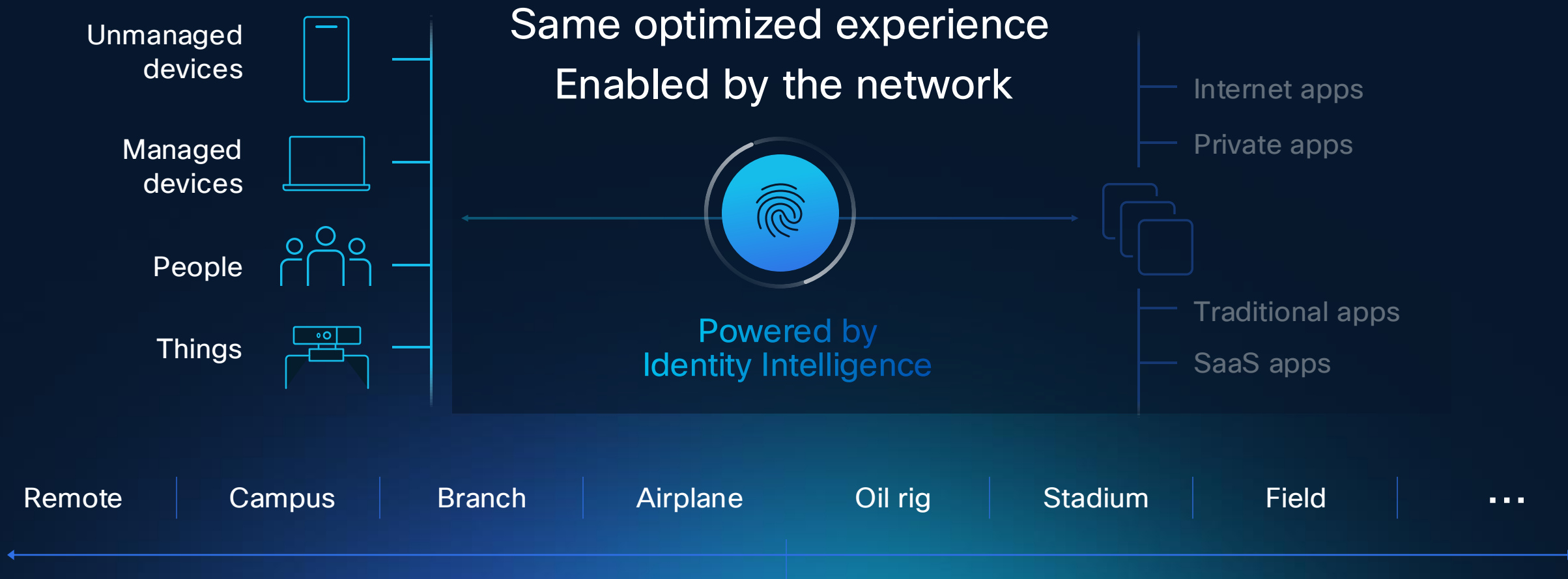
*when combined this is known as SASE architecture

SASE: Secure Access integrated with Cisco SD-WAN

Your security strategy for a hyper-distributed world



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



Thank you



