

Delivering on the promise of the Secure Campus & Unified Branch for the AI Era



Christopher Ronderos
Solutions Engineer

John Cervantes
Account Executive

Chris Shannon
Solutions Engineer

October 8, 2025

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

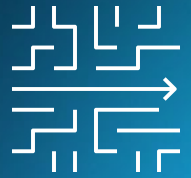
Is your Campus Network AI ready?

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

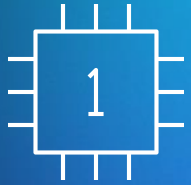


Architecture for Secure Campus

Operational simplicity
powered by AI



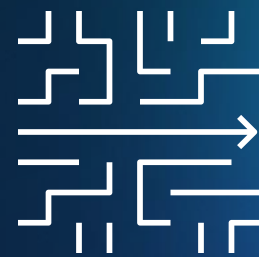
Scalable devices
ready for AI



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

Our unified platform

PLATFORM

Management

Assurance

API / Integrations

Intelligence

HARDWARE



Smart
Switches



Secure
Routers



Wireless

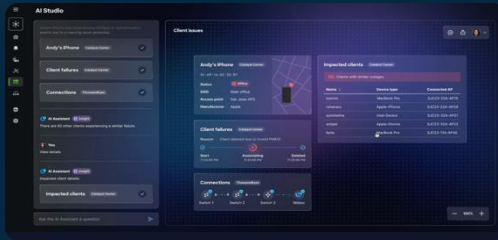


Industrial
IoT

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.

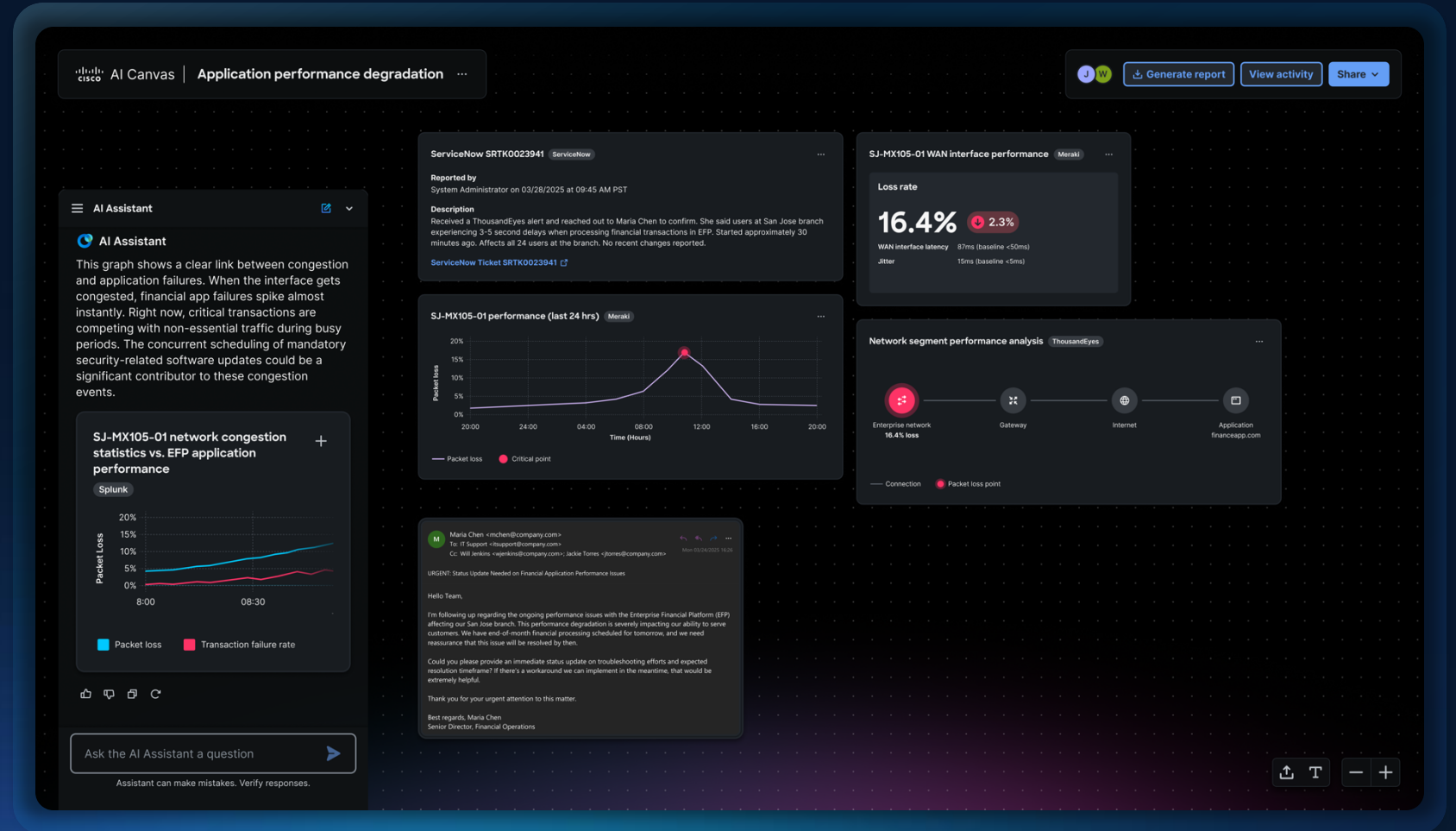
ALPHA | OCTOBER

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



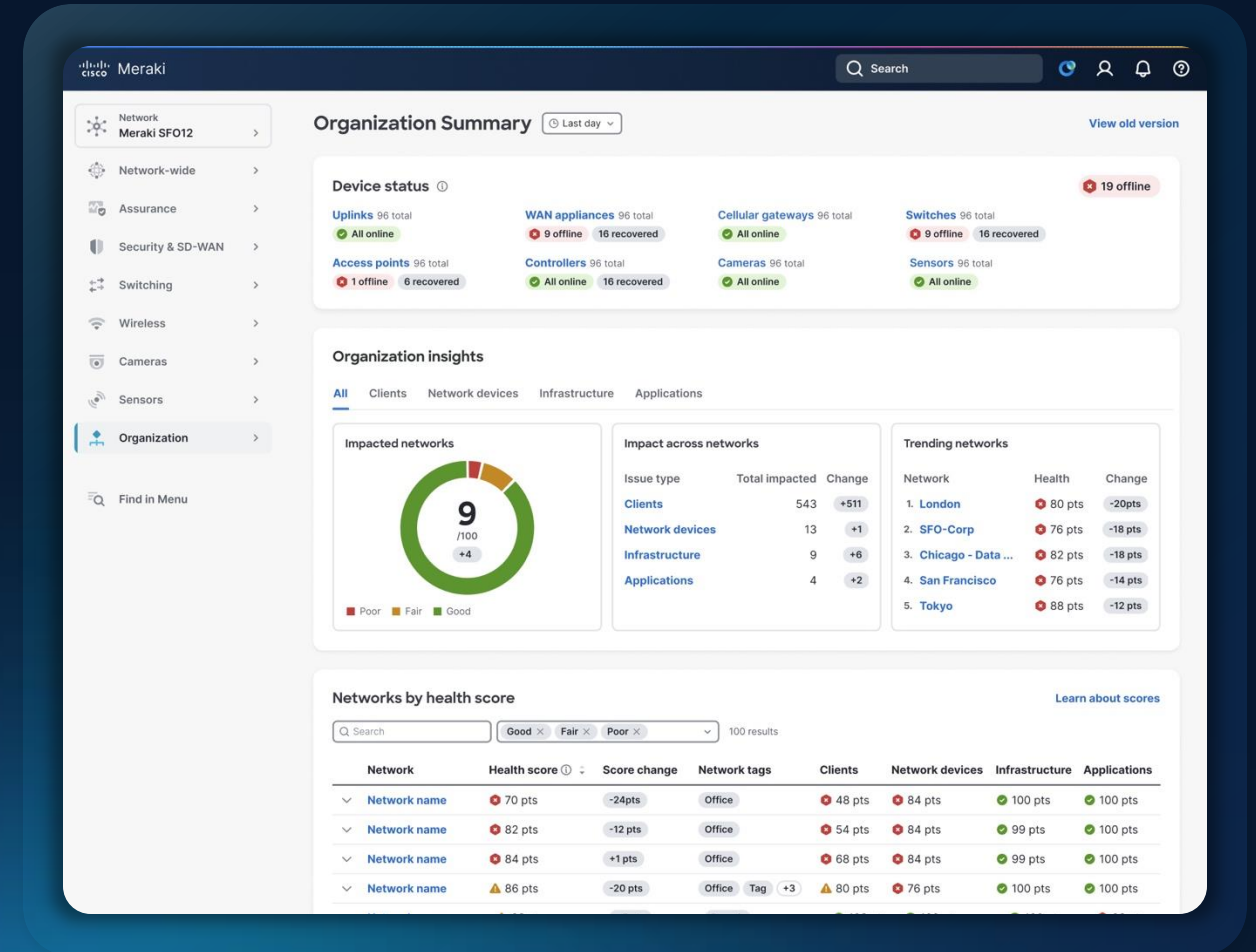
GA | JUNE

Unified Management – Catalyst and Meraki, any environment

Seamless control across cloud, on-prem, or hybrid

New enterprise campus capabilities

AI-powered automation and assurance



Expanded cloud management for Catalyst portfolio



Wireless

Full wireless support
Scale large campus wireless
with Campus Gateway

GA | MAY



Switching

Expanded management for
access and core switching,
including C9200 and C9500

GA | JULY



Routing

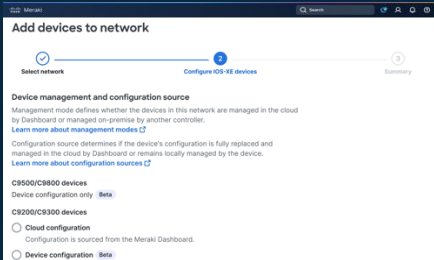
Next-gen routing
support coming

ALPHA | JUNE

Cloud management powered by cloud-native IOS XE

Large campus cloud capabilities

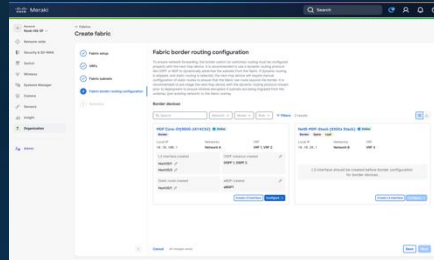
Powerful Switching Capabilities



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

GA | MAY

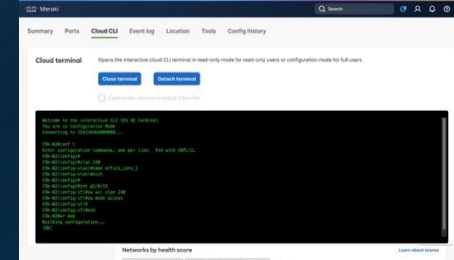
Fabric for Secure Networking



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

GA | JULY

Cloud CLI for Flexibility



Simplify onboarding and flexibility with operating mode options and Cloud CLI

ALPHA | JUNE

Inventory

[View old version](#)

View deployed and available devices in your organization. You can claim new devices to add to the list below. After selecting devices below, you can add them to a new or existing network.

[Global Overview](#)[Organization](#)
Eh ▾[Network](#)
Eh2 ▾[Network-wide](#)[Assurance](#)[Switching](#)[Wireless](#)[Insight](#)[Organization](#)[Access Manager](#)[Find in Menu](#)☐ MAC address☐ 14:9f:43:ee☐ 6c:7f:0c:fb☐ 6c:7f:0c:fb☐ 6c:7f:0c:fb☐ ac:d3:1d:ff☐ cc:9c:3e:e8☐ 14:9f:43:ee☐ b8:ab:61:fa☐ b4:df:91:15☐ 6c:de:a9:00☐ bc:db:09:e2☐ bc:db:09:e2☐ bc:db:09:e2:d3:e6☐ 2c:3f:0b:05:4d:80☐ 2c:3f:0b:04:5b:80☐ 00:84:1e:3e:6e:8a☐ 14:9f:43:e9:0d:2a

Claim individual devices



Scan with Meraki mobile app

Download the Meraki Mobile app for iOS or Android and use Claim Device

Enter manually

Claim individual devices and license keys, or just hardware. To name device at the same time, enter using the format: "device cloud ID, name" for each line

Device Cloud ID (Meraki serial number) or license key - one per line

Where can I find these numbers?

[Cancel](#)[Back](#)[Claim devices](#)[Download ▾](#)[+ Claim devices](#)

MS130R-8P

MS150-48MP-4X

MS150-24MP-4X

MS150-24P-4X

Z4

CW9164I

MS130R-8P

MS130R-8P

MV13

MV13

MS130-12X

MS130-12X

MG51

MS390-24UX

MS390-24U

MT40

MT40

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

AVAILABLE | NOW

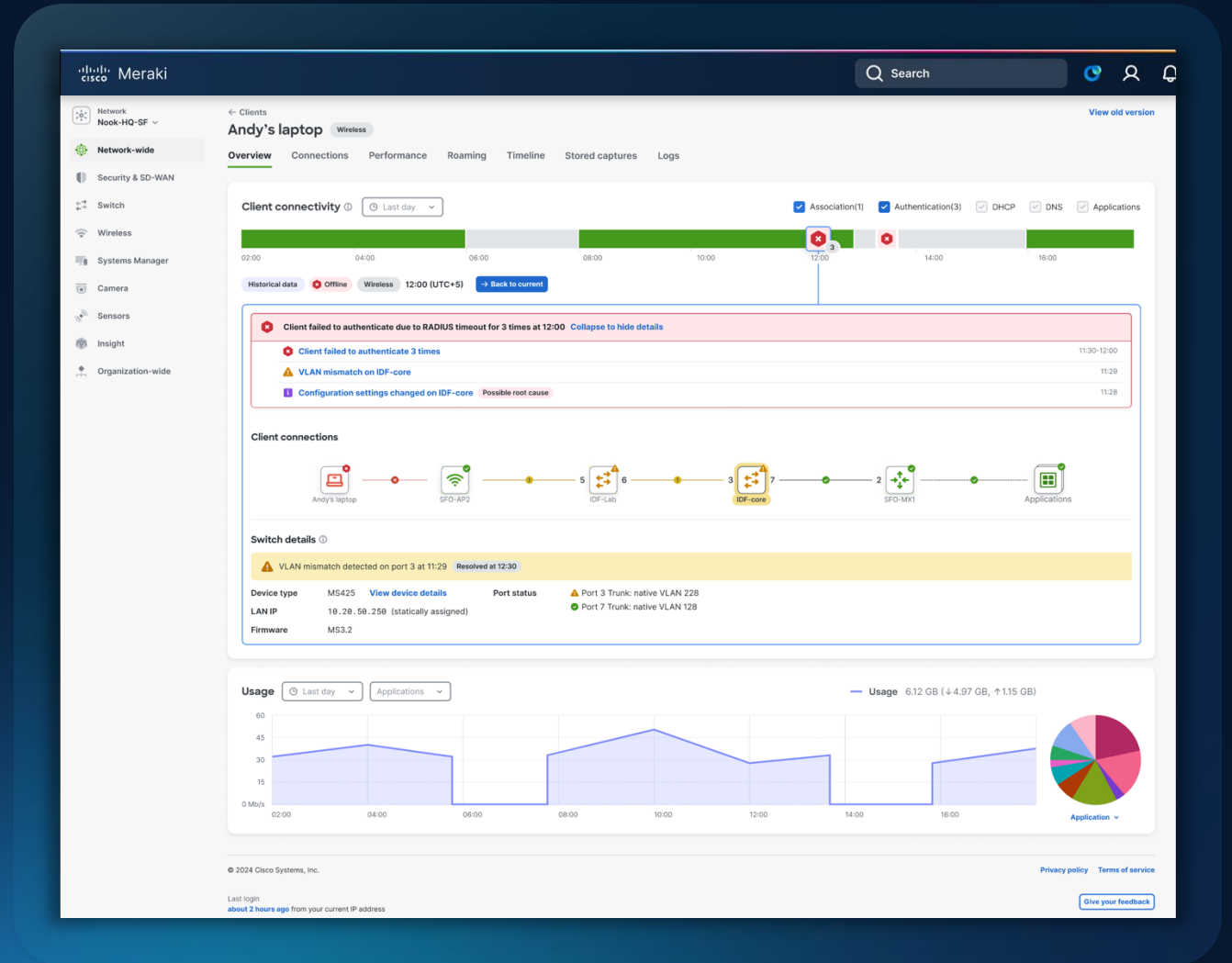
Assurance across every digital experience

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



Mon, Jun 2 00:52 – 00:54 PDT (13 hours ago)

[Show Filters](#)

< > >|

00:30

00:45

01:00

01:15

0'

45

02:00

Path Visualization

Map

Table

Show

2 Of 2 Agents ▼

IP Address Labels ☒

8 hops

3 hops

Group

Agents by Agent ▼

Interfaces by IP Address ▼

Destinations by No Grouping ▼

Highlight

All ▾

Search Network, Country, IP Ac

0 matches

Forwarding Loss > 10% (0 Nodes) ▾

Link Delay > 100ms (0 Links) ▼

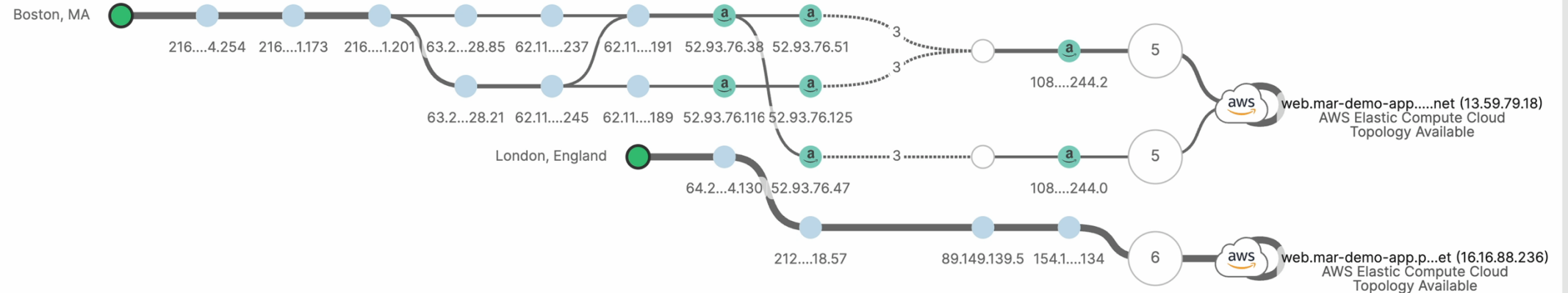
Select

Click a node or link

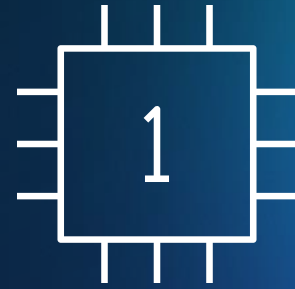
Info (1) ▼

↶ 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

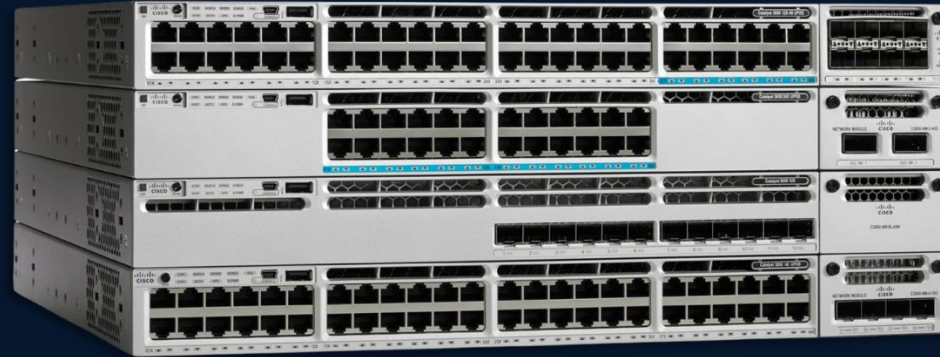
High-performance,
low latency

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 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**

Cisco 8000 Series Secure Routers + Firewall for Campus and Data Center

Campus



8400 Secure Router



Firewall 3100 Series

Data Center



8500 Secure Router



Firewall 4200 Series



Firewall 6100 Series

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



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 access to apps
anywhere



Securing network
connectivity



Securing network
access

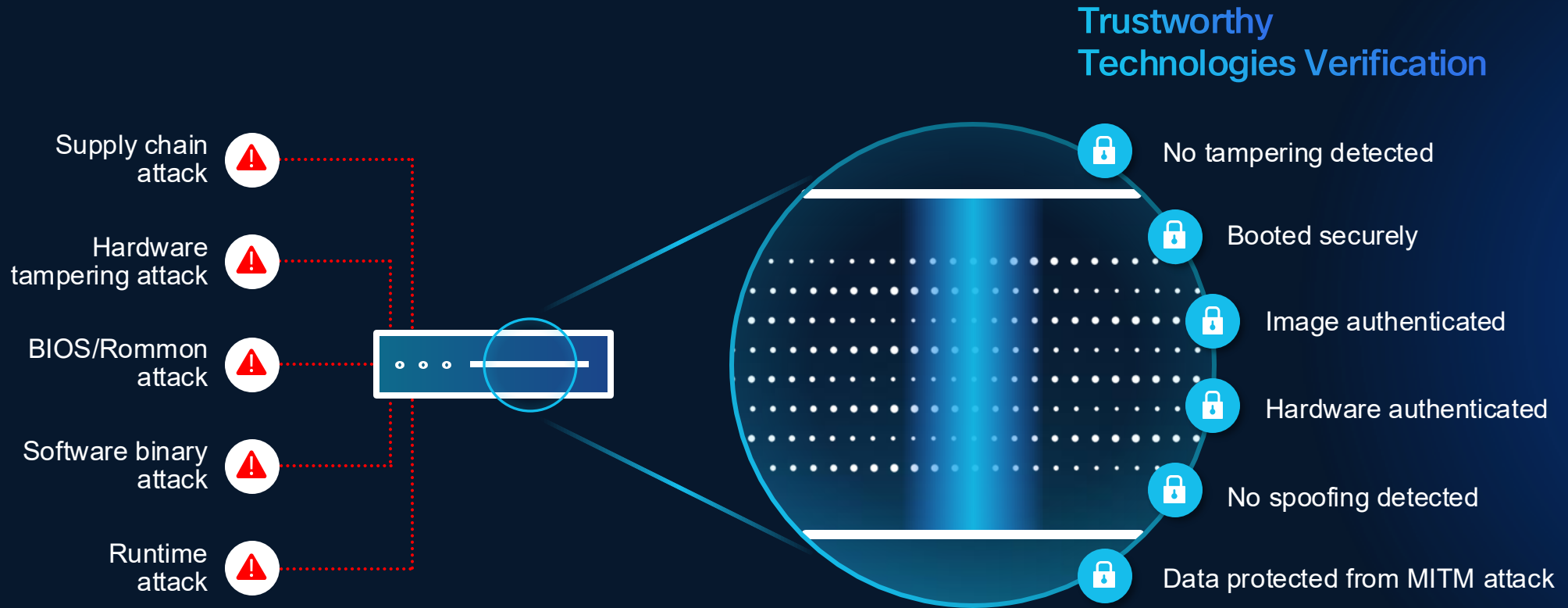


Securing the device



Securing the device

Secure from hardware to software, from boot time to runtime



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 'Device vulnerabilities' tab is active, showing a summary of 73 vulnerabilities, 12 available for deployment, and 37 deployed. A table lists specific vulnerabilities with their CVSS scores, affected devices, and Live Protect status.

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 ...

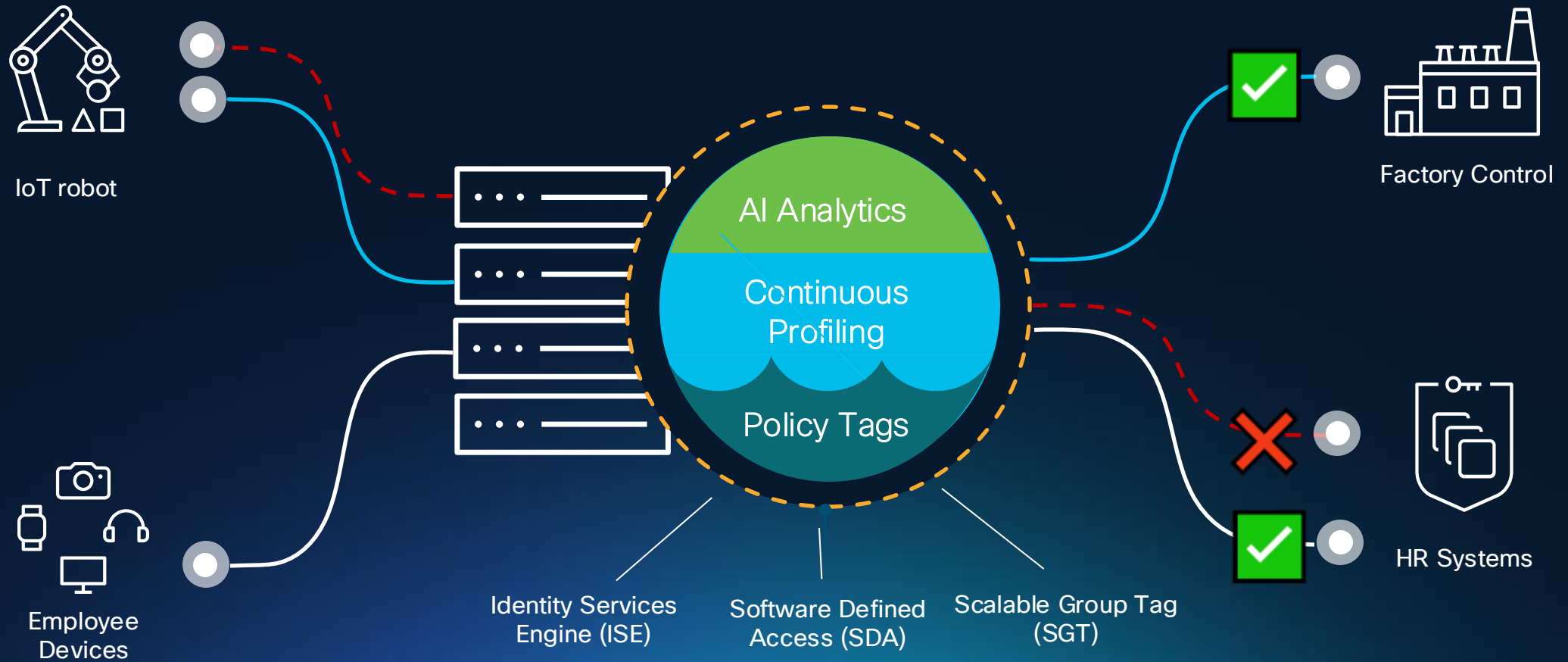
Rows per page 20 ▾ 1-20 of 73 < 1 2 ... 10 >

Securing network connectivity

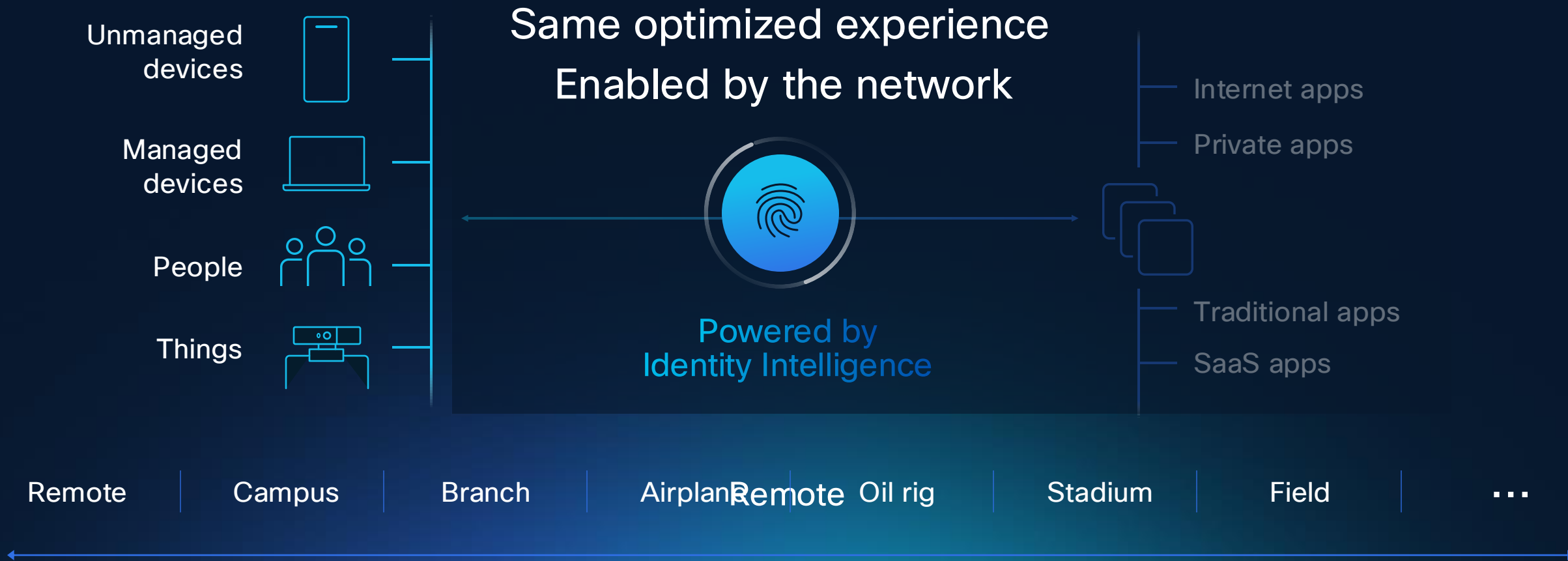


Securing network access

Scalable microsegmentation to protect every connection



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



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**

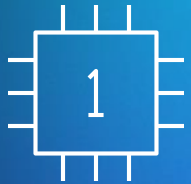


Architecture for Unified Branch

Operational simplicity
powered by AI



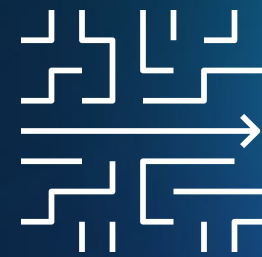
Scalable devices
ready for AI



Security
fused into the network

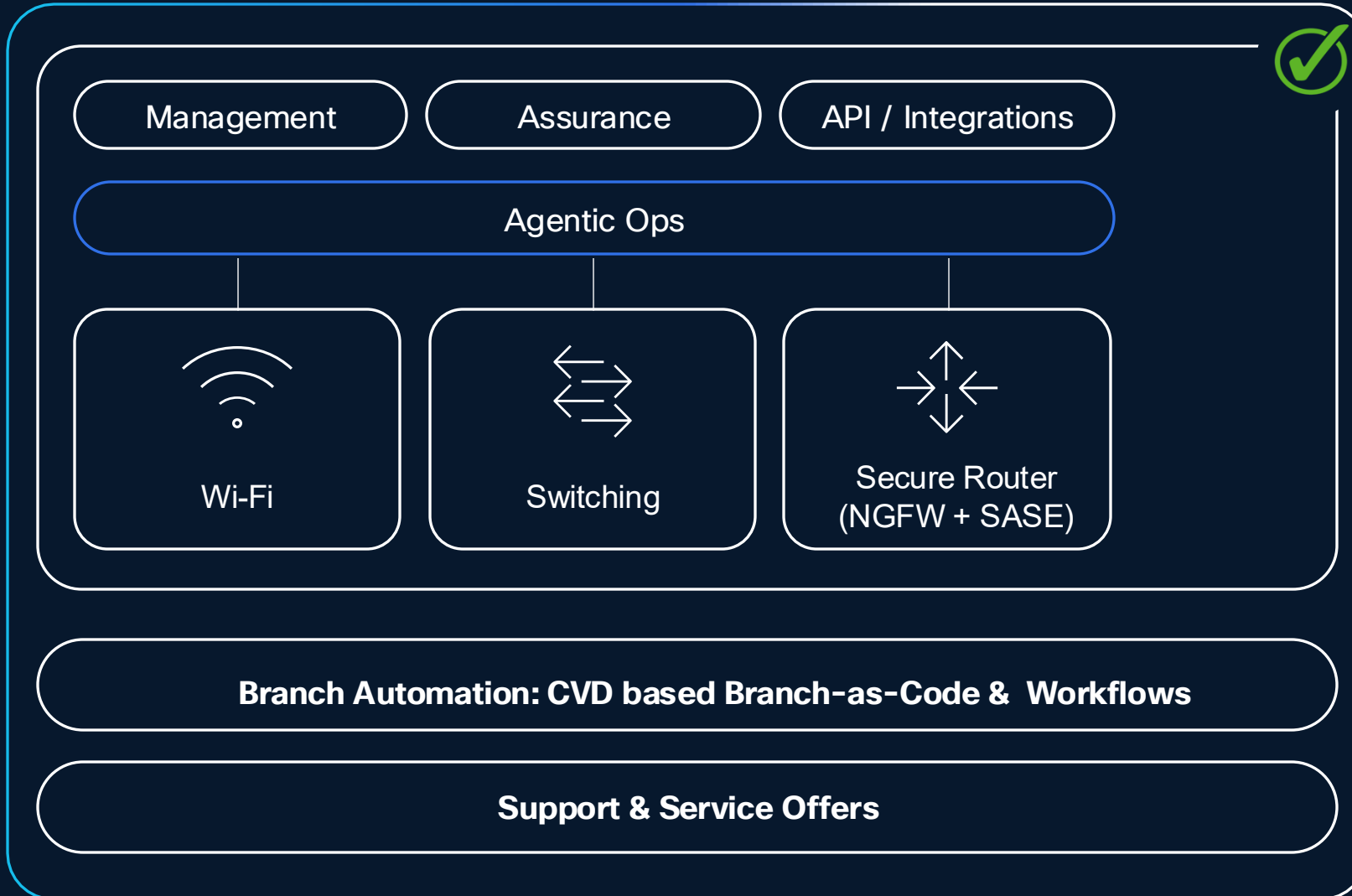


Operational Simplicity powered by AI





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

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

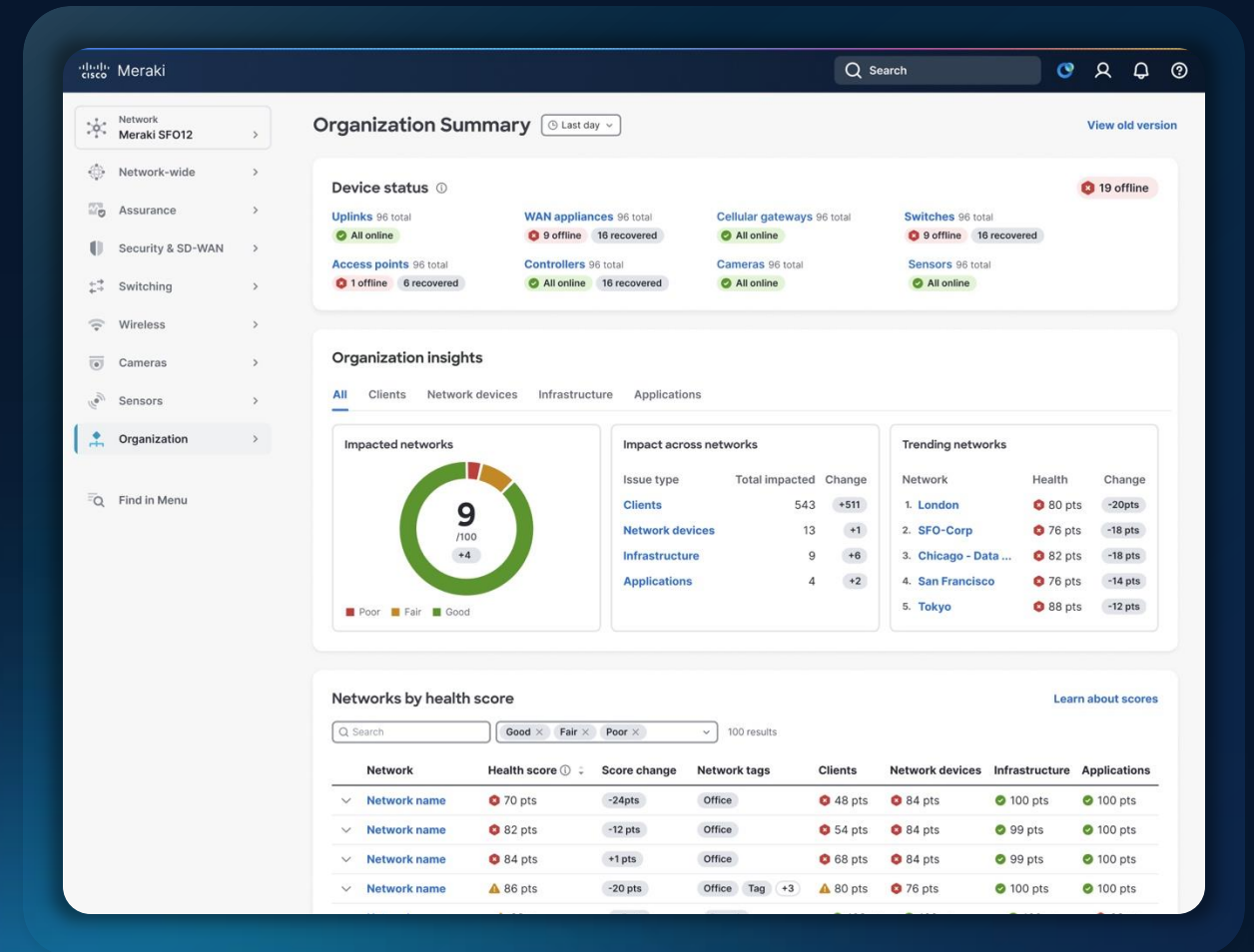
Small
Medium
Large

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



Flexible management options

Meeting customers where they are

Self Managed



BYO Management

Leverage CLI or 3rd party tools

On-premises or Cloud

Use cases require on-prem delivery, or advanced configuration



SD-WAN Manager & Catalyst Center

Cloud

Prefer cloud-enabled delivery for simplicity



Meraki Dashboard

Delivering optimized, simplified experiences for all customers

AVAILABLE | NOW

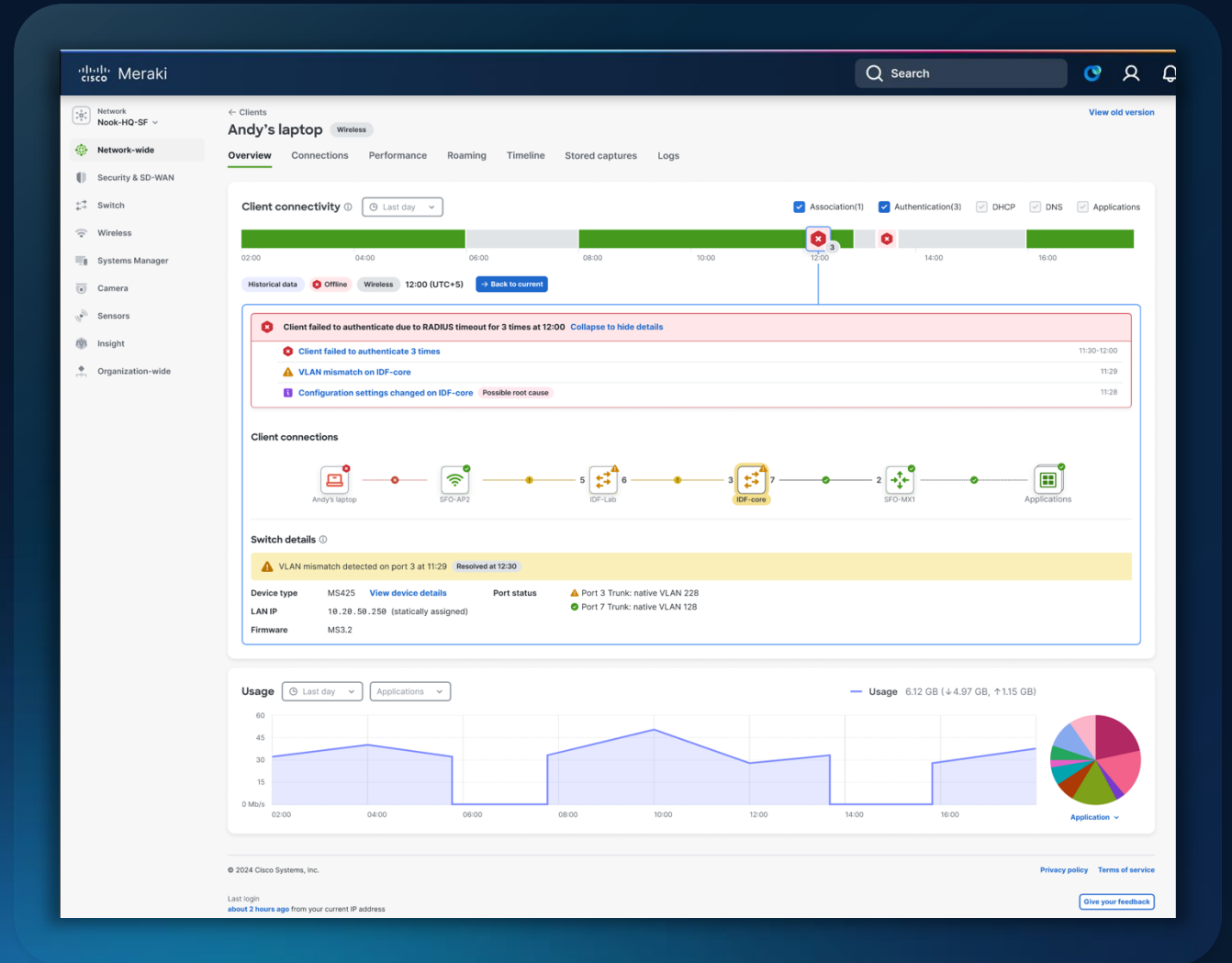
Assurance across every digital experience

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



Predictive path recommendations

Proactive guidance
for maintaining
network stability

Optimize WAN
performance

Generate long-term
recommendations for
network optimization

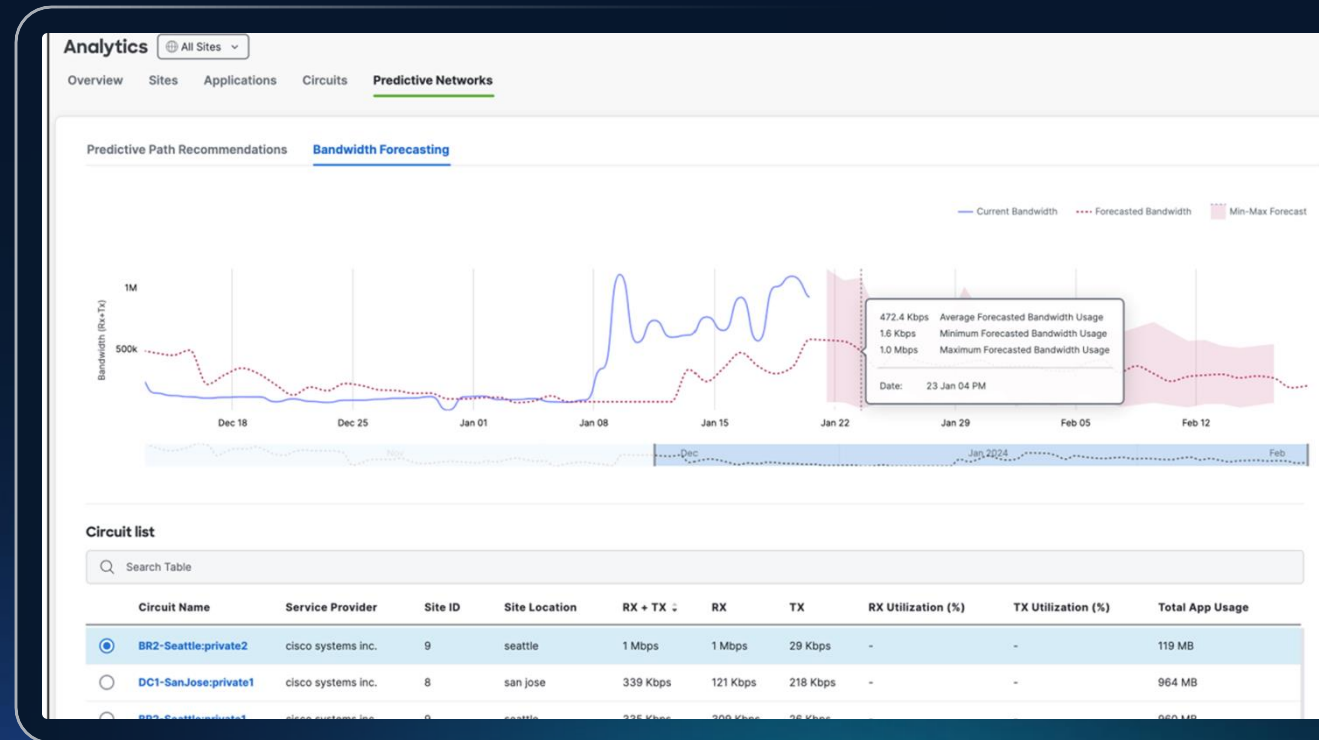


AVAILABLE NOW

Bandwidth forecasting

Monitor usage trends for capacity planning

Get a better understanding of growth trends, seasonality, surge, min/max band, and performance



AVAILABLE NOW

Global Overview

Overview - Meraki Dashboard x Cloud And Enterprise Agents V x +
n28.meraki.com/BachtelNet-HQ/n/eeDUXaC/manage/assurance/overview?from=assurance+overview

vidcast

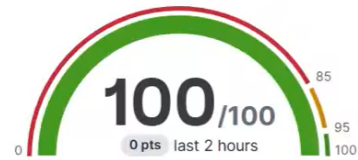
Organization
Bachtel Bank

Global Overview

Overview

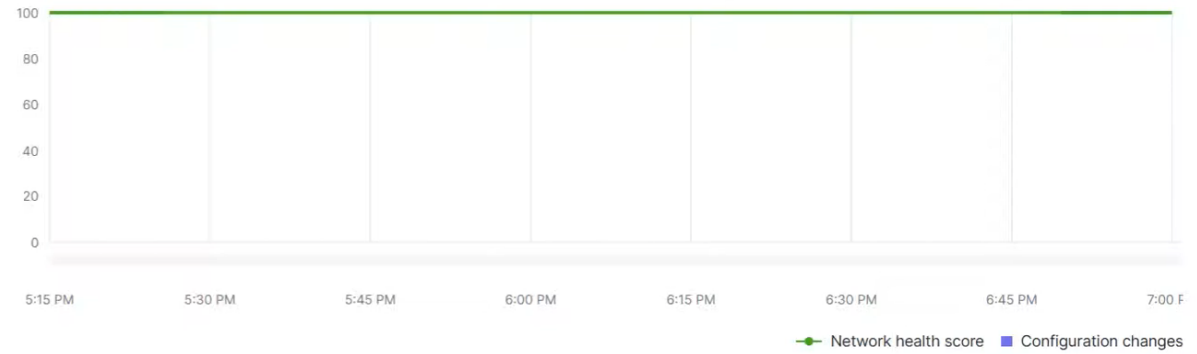
Last 2 hours

Network health score  Good



Does the score feel right?  

[Learn about scores](#)



Clients 53 total  Good

100/100 0 pts last 2 hours

 Wireless 0 issues

100/100 +0 pts

 Wired 0 issues

100/100 +0 pts

 Remote 0 issues

—/100 — pts

Network
Bachtel Bank -

Organization
Bachtel Bank

Network-wide

Network
Bachtel Bank - TU

Assurance

Network-wide

Cellular Gateway

Assurance

Security & SD-

Cellular Gateway

Switching

Security & SD-WAN

Wireless

Switching

Systems Mana

Wireless

Systems Manager

Cameras

Cameras

Sensors

Sensors

Insight

Insight

Organization

Organization

Give feedback

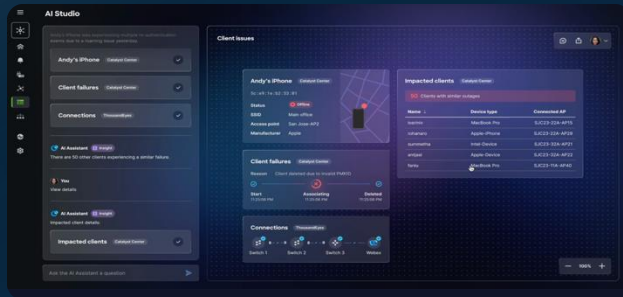
Give feedback

The background is a dark blue field filled with a complex network of glowing, multi-colored lines (pink, orange, blue) that connect various nodes and shapes. These nodes include circles, squares, and rectangles, some of which are highlighted with a bright glow. The overall effect is a sense of dynamic, interconnected digital data or a neural network.

**Branch operations, further simplified
with AgenticOps**

AgenticOps Lineup

ALPHA | OCTOBER



AI Canvas

Cross-domain collaborative troubleshooting

BETA | JUNE



AI Assistant

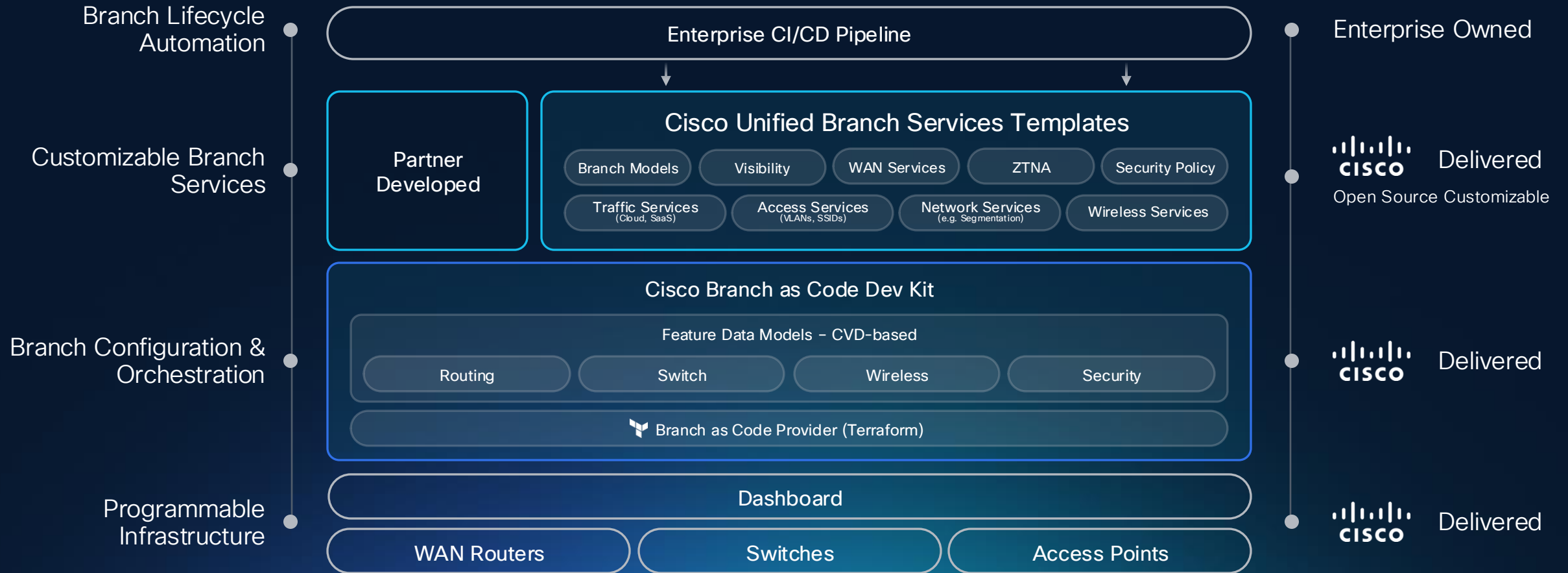
Accelerate network operations

POWERED BY DEEP NETWORK MODEL

The background is a dark blue field filled with a complex network of glowing lines and nodes. The lines are primarily purple, pink, and orange, with some white and light blue accents. They form a web-like structure, with some lines curving and others straight. Nodes are represented by small circles, squares, and other geometric shapes, some of which are highlighted with a bright glow. The overall effect is one of high-tech connectivity and data flow.

**Branch operations, further simplified
with Branch-as-code**

Large scale deployments with Branch as Code stack





1



1

Search or go to...

Project

M Meraki As Code Demo

Pinned

Repository

Pipelines

Issues 0

Merge requests 0

Commits

Terraform states

Manage

Plan

Code

Build

Secure

Deploy

Help

Admin

Filter pipelines



Show Pipeline ID



**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

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

Deliver exceptional branch experiences

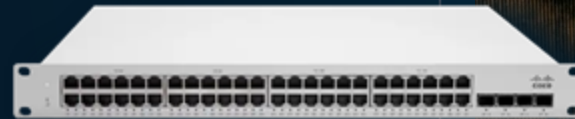
Smart Wi-Fi 7 access points and cloud-managed switches

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



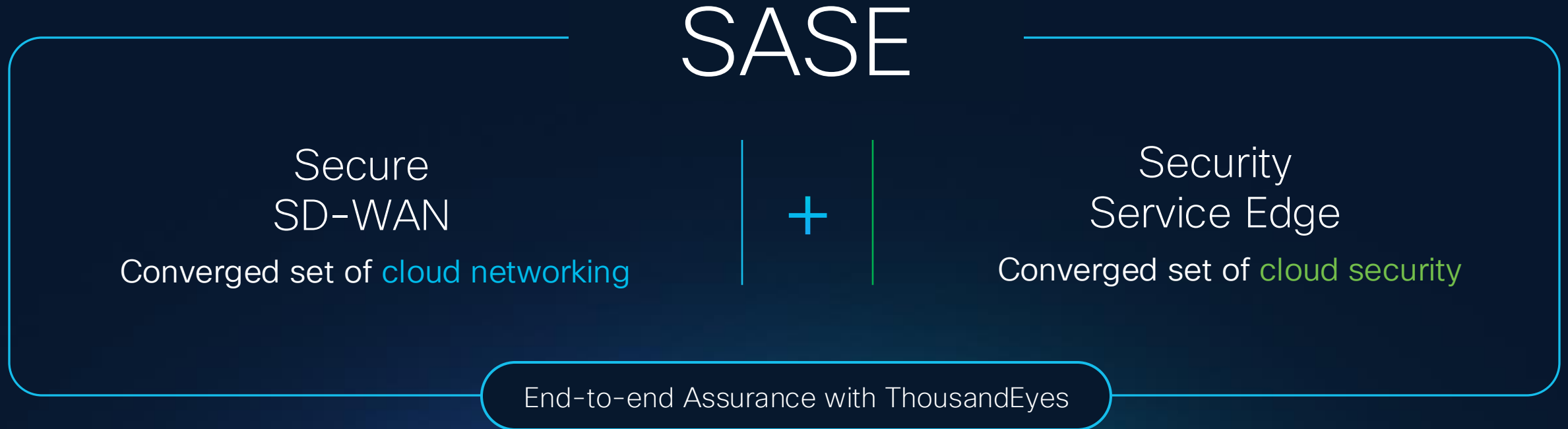
Cisco eases your journey to a future proof secure branch



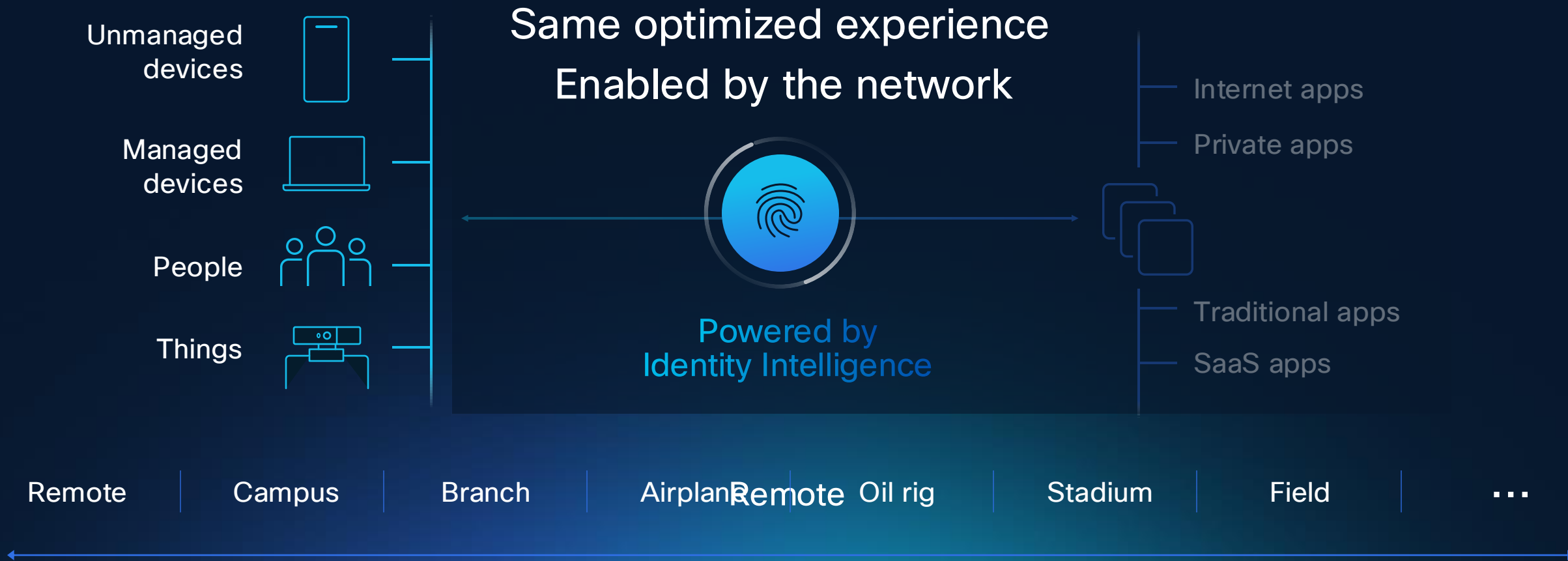
*when combined this is known as SASE architecture

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

