

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



Peter Jerhamre
Solutions Engineer

Today's IT environments are more complex, noisy, and fragmented than ever



70%

of IT pros say alert fatigue is a top challenge



85%

of IT outages caused by **human error** are procedure or process related



112

SaaS apps are used by the **average enterprise**, operating across the 2.2 public clouds



15+

hours of average mean time to resolution for critical incidents. MTTR is still too high

AI is bringing changes and challenges

1,000s

AI Agents per
enterprise expected

#1 risk

AI-enhanced
malicious attacks

64%

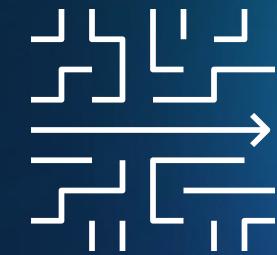
of orgs face IT skills
shortage by 2026

Is your Campus Network AI ready?

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



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

Coming in 2026



AI Canvas

Cross-domain collaborative troubleshooting

Available Now



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.

Coming in 2026

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 monitoring and collaboration platform. At the top, a header bar includes the Cisco logo, the title 'AI Canvas | Application performance degradation', and user profile icons for 'J' and 'W'. Action buttons for 'Generate report', 'View activity', and 'Share' are also present.

The main content area is organized into several cards:

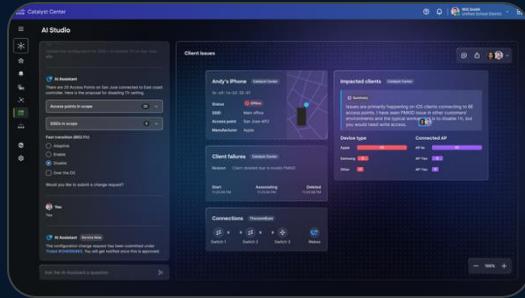
- AI Assistant:** A text box explaining the relationship between network congestion and application failures, mentioning financial app failures and mandatory security-related software updates.
- SJ-MX105-01 network congestion statistics vs. EFP application performance:** A Splunk-generated chart showing Packet Loss (blue line) and Transaction failure rate (red line) over time. The x-axis shows hours from 8:00 to 20:00, and the y-axis shows Packet Loss from 0% to 20%. The chart shows a significant spike in packet loss around 12:00.
- ServiceNow SRTK0023941:** A ServiceNow alert card for a financial application at the San Jose branch. It details a 3-5 second delay in processing transactions, reported by a System Administrator on 03/28/2025 at 09:45 AM PST. The ticket number is SRTK0023941.
- SJ-MX105-01 WAN interface performance:** A card showing a 16.4% loss rate over a 24-hour period, with a baseline of 2.3%. It includes metrics for WAN interface latency (87ms) and Jitter (15ms).
- 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 12:00.
- Network segment performance analysis:** A diagram showing the network topology from the Enterprise network through a Gateway and Internet to an Application (financeapp.com). It highlights a 16.4% loss point on the connection to the gateway.
- Ask the AI Assistant a question:** A text input field for interacting with the AI Assistant, with a note: 'Assistant can make mistakes. Verify responses.'
- 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 if available.

Agentic Ops Across IT and SecOps

AI Assistant



AI Canvas



Campus and Branch

Catalyst Center

Topology, client details, location, etc.

webex

Voice and video experience

Cisco Meraki

Topology, client details, location, etc.

ThousandEyes

WAN, Internet, App Insights

SD-WAN

WAN Details

Data Center

Nexus Dashboard

Data center network management.

Hyperfabric

Data center network management.

Identity Intelligence

User trust level, identity checks & reasons

Intersight

Unified management, automation, security.

Security and Observability

splunk

Cisco and third-party insights

Firewall

Security & connection events

Duo

Authentication & compliance

Secure Access

Private & SaaS Resource Access

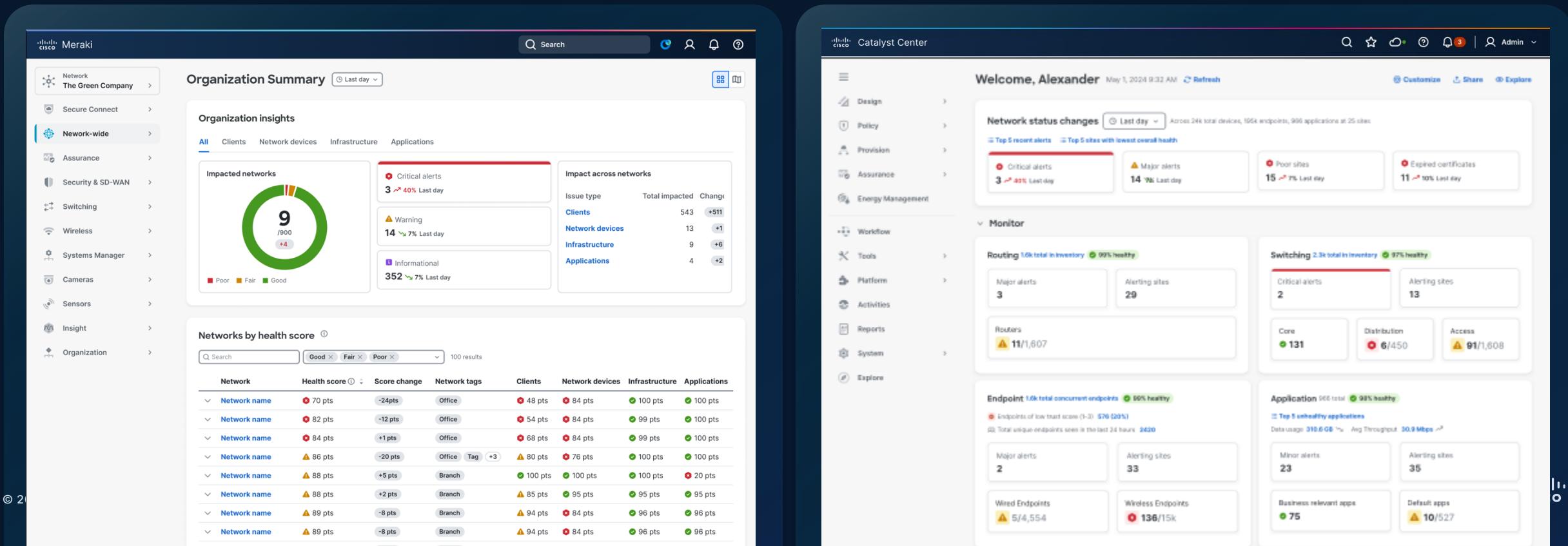
XDR

Related Threat Incidents

AVAILABLE NOW

Common experience

Bringing together the power of **Catalyst** and simplicity of **Meraki**



The image displays two side-by-side screenshots of network management interfaces, illustrating the integration of Cisco Catalyst and Meraki.

Left Screenshot: Meraki Organization Summary

This screenshot shows the Meraki interface for 'The Green Company'. The top navigation bar includes 'Secure Connect', 'Nework-wide', 'Assurance', 'Security & SD-WAN', 'Switching', 'Wireless', 'Systems Manager', 'Cameras', 'Sensors', 'Insight', and 'Organization'. The main content area features an 'Organization insights' section with a '9/900' score and a 'Impact across networks' table:

Issue type	Total impacted	Change
Clients	543	+511
Network devices	13	+1
Infrastructure	9	+6
Applications	4	+2

Below this is a 'Networks by health score' table:

Network	Health score	Score change	Network tags	Clients	Network devices	Infrastructure	Applications
Network name	70 pts	-24pts	Office	48 pts	84 pts	100 pts	100 pts
Network name	82 pts	-12 pts	Office	54 pts	84 pts	99 pts	100 pts
Network name	84 pts	+1 pts	Office	68 pts	84 pts	99 pts	100 pts
Network name	86 pts	-20 pts	Office, Tag	80 pts	76 pts	100 pts	100 pts
Network name	88 pts	+5 pts	Branch	100 pts	100 pts	100 pts	20 pts
Network name	88 pts	+2 pts	Branch	85 pts	95 pts	95 pts	95 pts
Network name	89 pts	-8 pts	Branch	94 pts	84 pts	96 pts	96 pts
Network name	89 pts	-8 pts	Branch	94 pts	84 pts	96 pts	96 pts

Right Screenshot: Catalyst Center

This screenshot shows the Catalyst Center interface for 'Alexander'. The top navigation bar includes 'Customize', 'Share', and 'Explore'. The main content area features a 'Welcome, Alexander' message and a 'Network status changes' section:

Critical alerts	Major alerts	Poor sites	Expired certificates
3 ↗ 42% last day	14 ↗ 1% last day	15 ↗ 7% last day	11 ↗ 10% last day

Below this are sections for 'Monitor' (Routing, Switching, Tools, Platform, Activities, Reports, System, Explore), 'Endpoint' (total concurrent endpoints, endpoints of low health score, total unique endpoints), and 'Application' (total applications, top 5 unhealthy applications, data usage, minor alerts, alerting sites, wired and wireless endpoints, business-relevant apps, default apps).

AVAILABLE | NOW

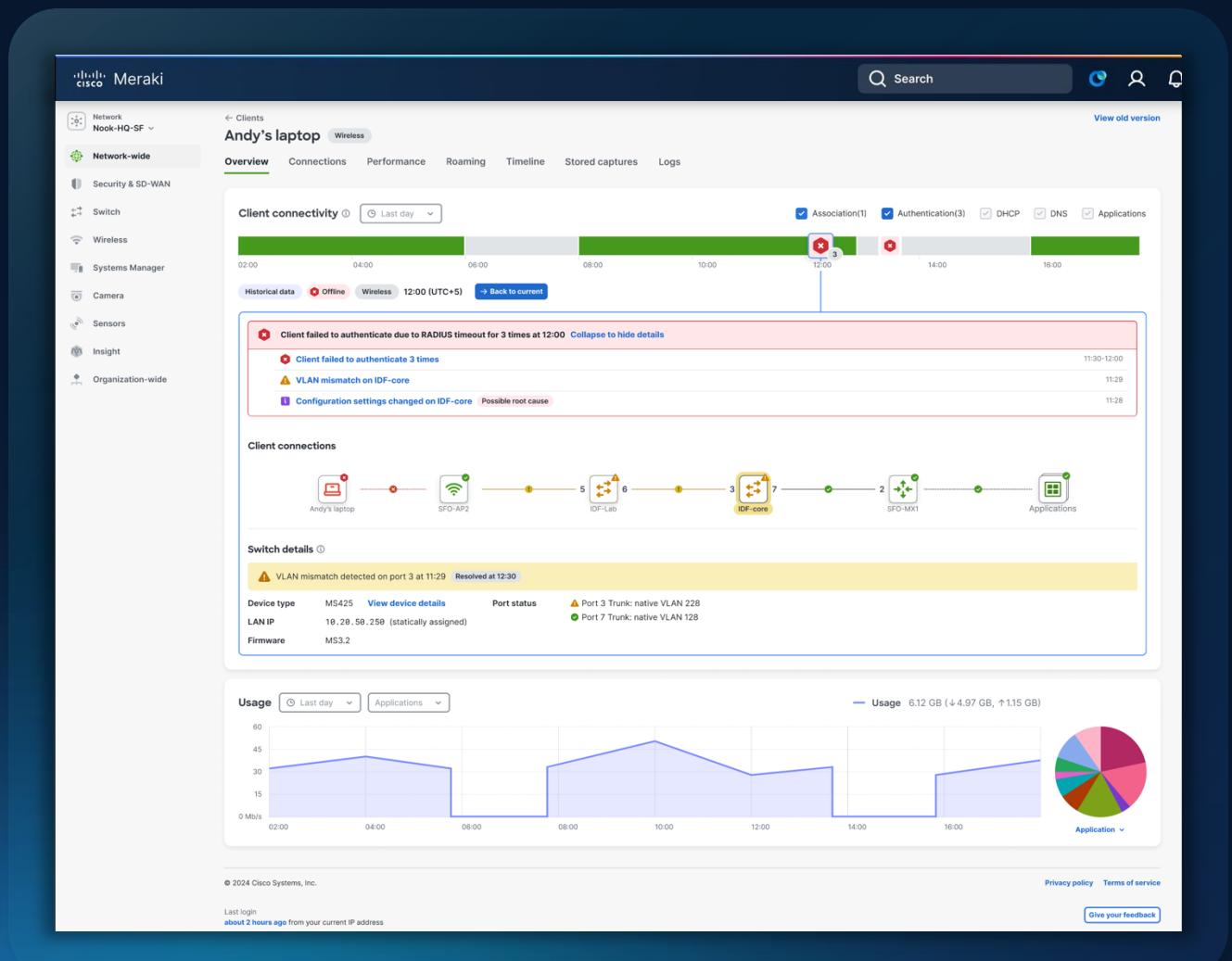
Assurance across every digital experience

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



Mar Demo App

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

[Show Filters](#)

< > >

May 5 May 8 May 11 May 14 May 17 May 20 May 23 May 26 May 29 June

00:30

00:45

01:00

01:15

01:30

01:45

02:00

[Path Visualization](#)[Map](#)[Table](#)

Show

2 Of 2 Agents

IP Address Labels

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)

8 hops

3 hops

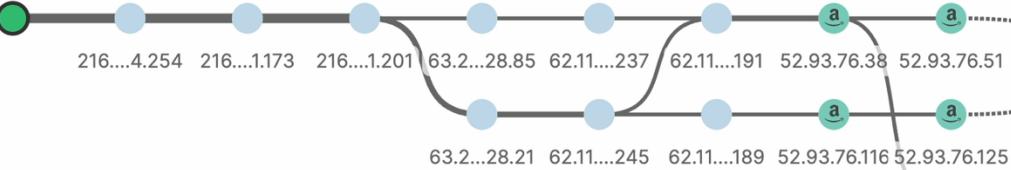
[Undo \(1\)](#)[Reset To Default](#)

Select

Click a node or link

Info (1)

Boston, MA



London, England

 web.mar-demo-app....het (13.59.79.18)
AWS Elastic Compute Cloud
Topology Available

212....18.57

89.149.139.5 154.1....134

6

 web.mar-demo-app.p....et (16.16.88.236)
AWS Elastic Compute Cloud
Topology Available

Unified network management

Cisco networking platform

Coming Soon

Unified network management with flexible deployments for cloud, on-prem, and hybrid in a single cloud dashboard experience integrating Meraki and Catalyst Center

Unified management experience

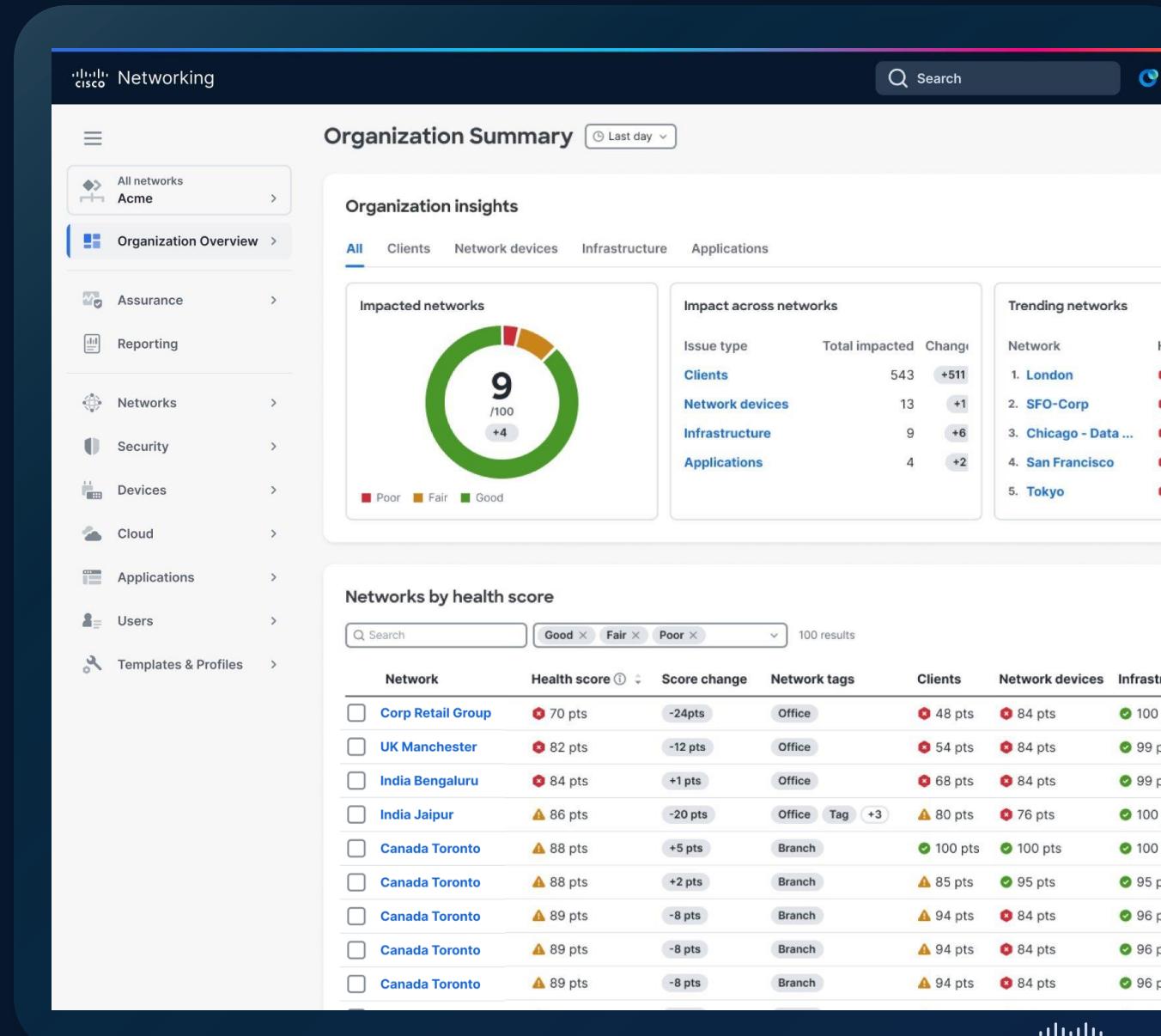
Global health visibility and actionable alerts

Secure SSO for seamless workflows

Simplified AI-powered network operations across cloud and on-prem environments

Enterprise campus capabilities and scale

AI-powered automation and assurance



The screenshot shows the Cisco Networking Platform dashboard. The top navigation bar includes the Cisco Networking logo, a search bar, and a 'Coming Soon' button. The left sidebar lists various management categories: All networks (Acme), Organization Overview, Assurance, Reporting, Networks, Security, Devices, Cloud, Applications, Users, and Templates & Profiles. The main content area is titled 'Organization Summary' with a 'Last day' dropdown. It features a 'Organization insights' section with tabs for All, Clients, Network devices, Infrastructure, and Applications. A large circular gauge chart in the 'Impacted networks' section shows a score of 9/100, with a legend for Poor (red), Fair (orange), and Good (green). Below this are sections for 'Impact across networks' (listing Clients, Network devices, Infrastructure, and Applications) and 'Trending networks' (listing London, SFO-Corp, Chicago - Data ..., San Francisco, and Tokyo). The bottom section, 'Networks by health score', is a table with columns: Network, Health score (with a dropdown for Good, Fair, Poor), Score change, Network tags, Clients, Network devices, and Infrastructure. The table lists various network locations with their respective scores, changes, and tags like Office, Branch, and Tag +3.

Cisco Cloud Control

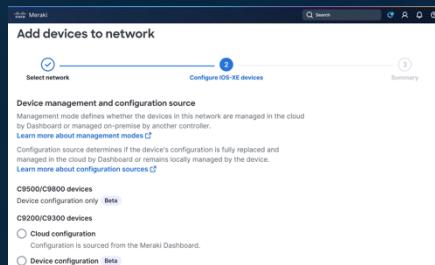
An AI-native management platform that reimagines how organizations **manage, operate, and optimize** their IT infrastructure

Coming in 2026

The screenshot shows the Cisco Cloud Control interface. The top navigation bar includes the Cisco logo, a search bar, and user information for 'Admin Acme Corp.'. The left sidebar has a 'Home' button and sections for 'AI Canvas' (Pinned: Application Performance Monitor..., Network Fabric Management, Micro and Perimeter Segmentation, See all), 'Networking', 'Security', 'Collaboration', 'Observability', and 'Admin Console' (Users and Role, Products and Services, Inventory, Licensing, Integration, Support). The main dashboard features a large circular 'Connected events' section with a total of 123k (30k blocked) and 27 failed events. It also shows 'Users' (101k, 82 Strong posture, 67 Moderate posture), 'Endpoints' (298k, 27 failed), and network segments: 'Internet' (1.2k), 'Cloud' (581), and 'Private' (109, 92% Threats contained). Below this are 'Campus and branch' metrics: Wireless (10k), Switches (4k), Routers (207), WAN circuits (392), Firewall (253), Data center (287), and Applications (29, 4 degraded). The 'Security health score' for 'Alex Moreno' is 59/100. The 'Endpoints' section shows a bar chart with 47%, 35%, and 18% segments. The 'Packet loss' section shows a line graph from 8:00 to 10:00. The 'Recent changes' section lists 'Switch configuration updated' (Catalyst 9500, Florida branch on June 1, 2025 at 10:50am PST), 'Firewall policy modified' (ASA firewall, HQ data center on June 1, 2025 at 10:40am PST), and 'Application patch deployed' (Healthcare app (v4.2.3) on June 1, 2025 at 10:15am PST). The bottom of the screen includes an 'AI Assistant' section and a 'View change log' button.

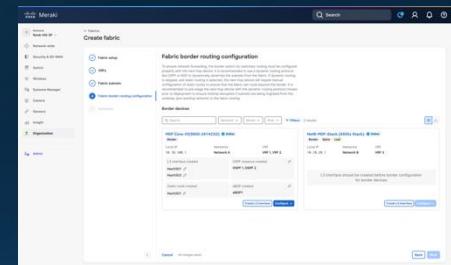
Large campus cloud capabilities

Powerful Switching Capabilities



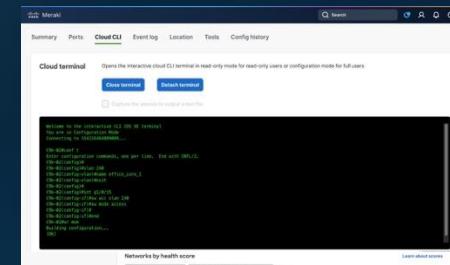
Support campus deployments with BGP, VRF, ISSU, and IOS XE stacking

Fabric for Secure Networking



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

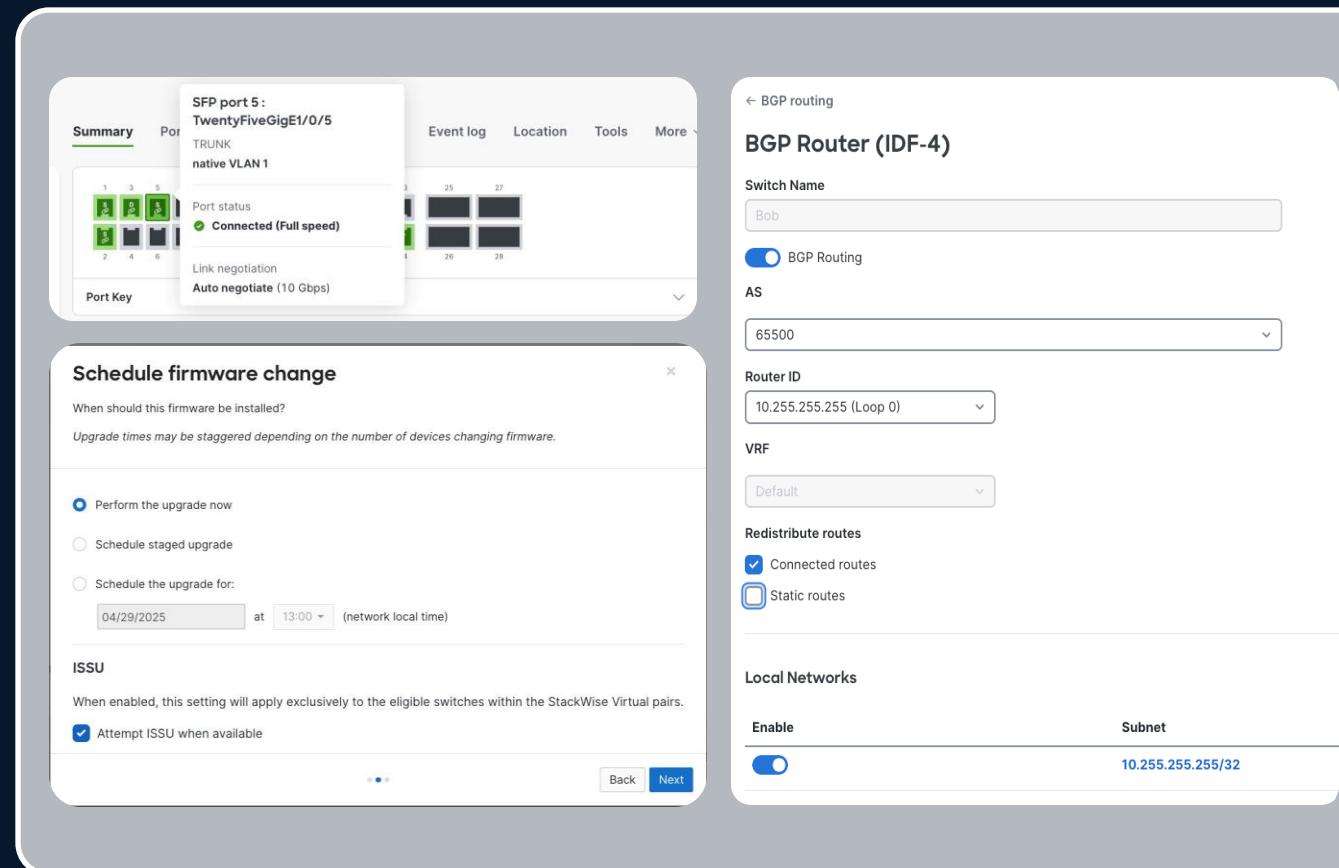
Cloud CLI for Flexibility



Simplify onboarding and flexibility with operating mode options and Cloud CLI

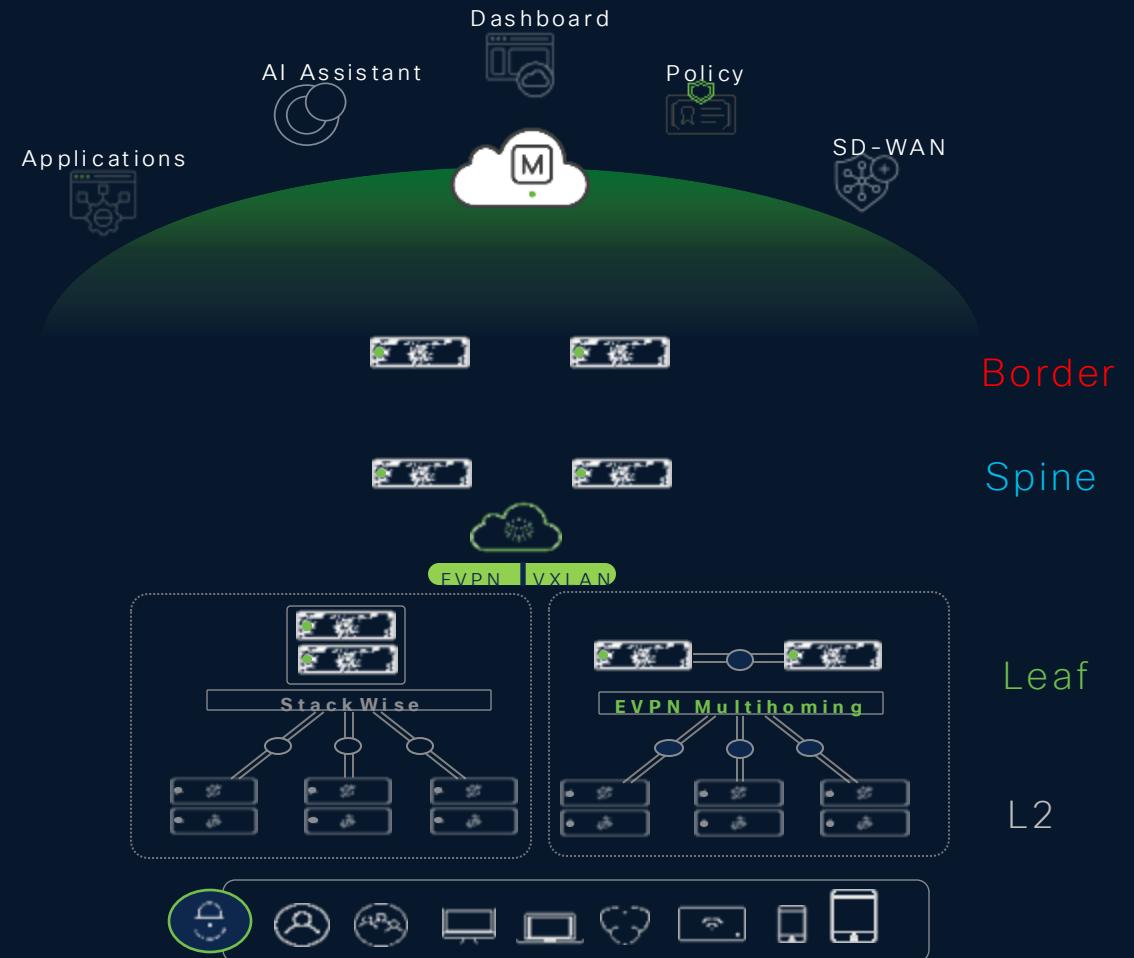
Simplicity, with new Enterprise capabilities and scale

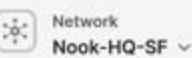
- Advanced routing configurations with BGP, VRF support, and Routed Ports
- High availability with In-Service Software Upgrade (ISSU), StackWise Virtual, and Rapid Per-VLAN STP+
- Cloud intelligence: SmartPorts (Profiles), Intelligent Capture (scheduling), Device Uptime, Device Health, and Digital Optical Monitoring
- Expand new platforms support: MS390, C9200/CX/L, C9300/LM/L/X, C9500*



Cloud-Managed Fabric Solution

-  **Simplified management as a single logical entity**
-  **Focused on brownfield migration**
-  **Flexible deployment and staging**
-  **Securing the network with Adaptive Policy**
-  **Optimized L2 extension**
-  **Day-2 Operational Assurance**





Network
Nook-HQ-SF

← Fabrics

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 X Network B X

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.

Q 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
<input checked="" type="checkbox"/> MDF Core-01(9500-24Y4CX2)	Online	10.10.100.1	Network A	Serial number	Tag		0
<input checked="" type="checkbox"/> MDF Dist-01 (9500-48Y4Cx2)	Online	10.10.192.1	Network A	Serial number	Tag 1 Tag 2		0
<input type="checkbox"/> MDF Dist-02 (9500-48Y4Cx2)	Online	10.10.176.1	Network A	Serial number	Tag 2	Leaf	0
<input type="checkbox"/> NetB-MDF-Stack (9300x Stack)	Online	10.10.20.1	Network B	Serial number	Tag 3	Border Spine Leaf	0
<input type="checkbox"/> NetC-MDF-Stack (9300x Stack)	Online	10.10.40.1	Network C	Serial number	Tag	Border	0
<input type="checkbox"/> NetD-MDF-Stack (9300x Stack)	Online	10.10.30.1	Network D	Serial number	Tag	Border	0

Rows per page

30

1-30 of 300

<

1

2

...

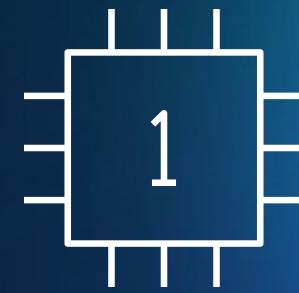
10

>

Cancel All changes saved

Next

Scalable devices ready for AI



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 NOW

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 NOW

**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

Announcing 19 new switches joining Cisco's leading portfolio

DIN-rail Portfolio



IP67 Portfolio



Rackmount Portfolio



Wi-Fi 7 for every operational scale



CW9172H

6 Spatial Streams

Dorm Rooms, Hospitality



CW9174E

8/10 Spatial Streams

External antennas

Dec 2025



CW9176D1

12 Spatial Streams

Integrated Directional

UWB



CW9179F

16 Spatial Streams

LPV/Stadium



CW9171I

4 Spatial Streams

Omnidirectional

Dec 2025



CW9172I

6 Spatial Streams

Omnidirectional



CW9174I

8/10 Spatial Streams

Omnidirectional

Dec 2025



CW9176I

12 Spatial Streams

Omnidirectional

UWB



CW9178I

16 Spatial Streams

Omnidirectional

UWB

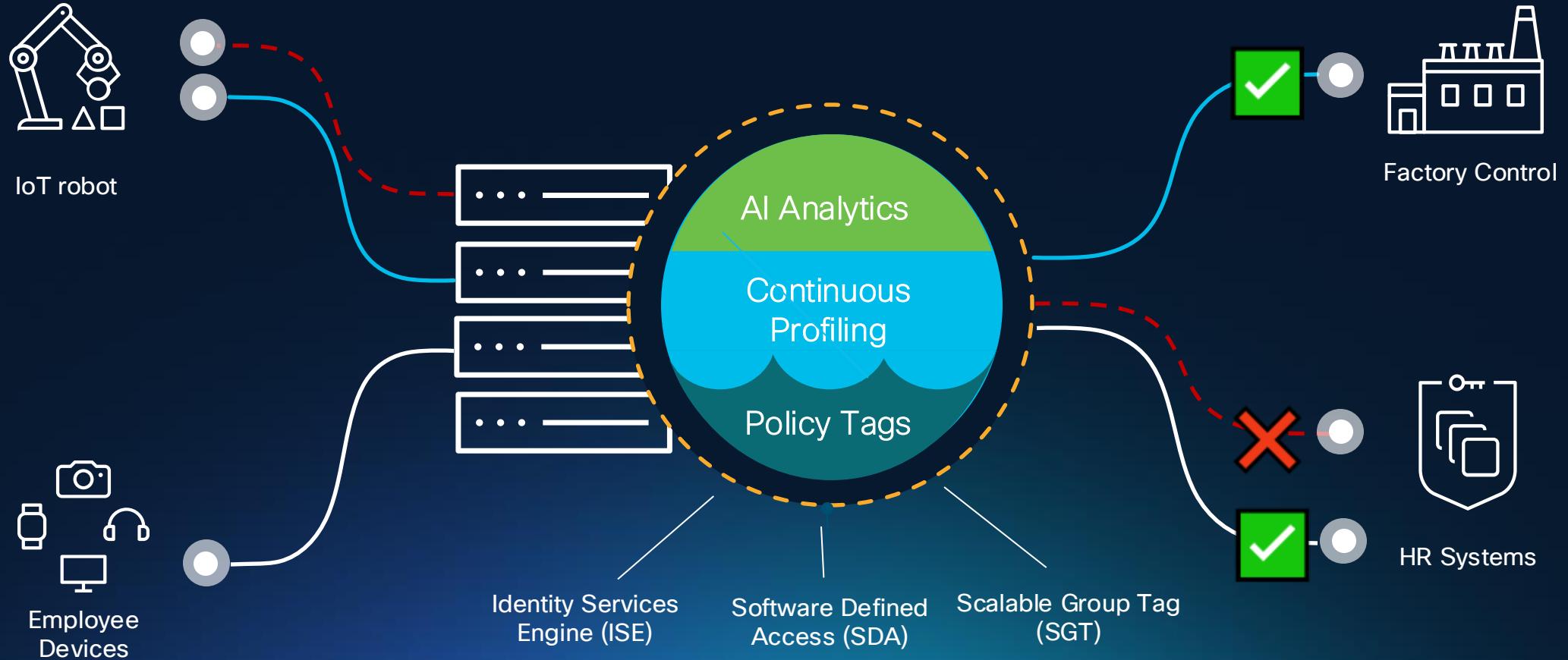
Wi-Fi 7 | Global Use AP | Unified License | AI Optimized

Security fused into the Network



Securing network access

Scalable microsegmentation to protect every connection



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.

Securing network connectivity

Network traffic

IoT/OT

Managed

Unmanaged



IPSec

MACSec

WAN MACSec

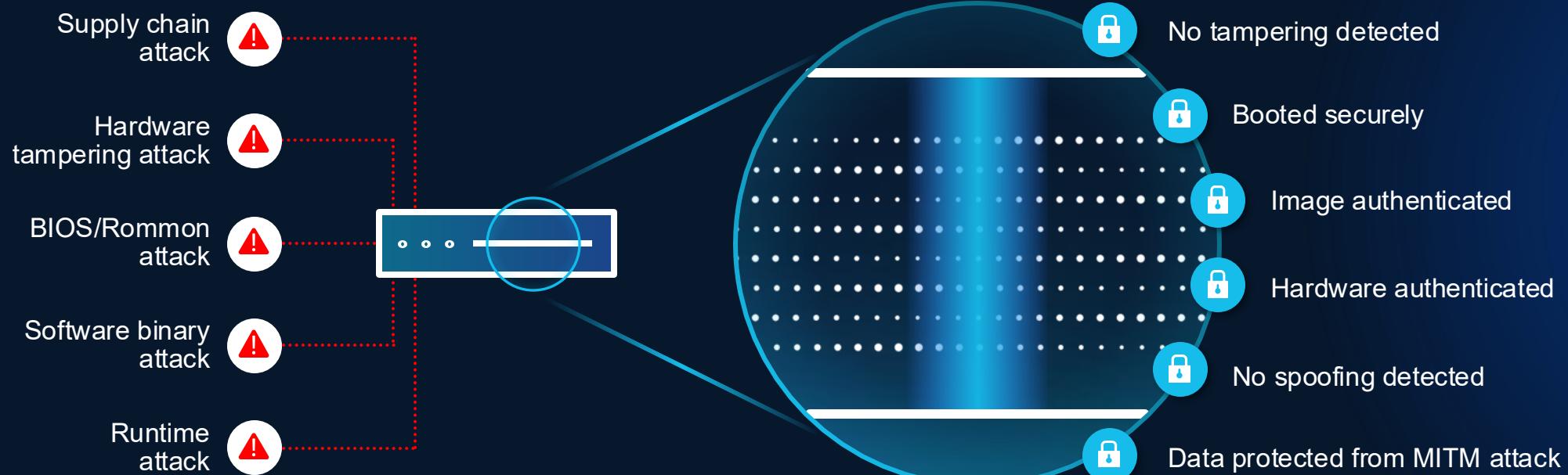
Post-Quantum
Cryptography

- Low latency
- High bandwidth
- FIPS compliant

Securing the device

Secure from hardware to software, from boot time to runtime

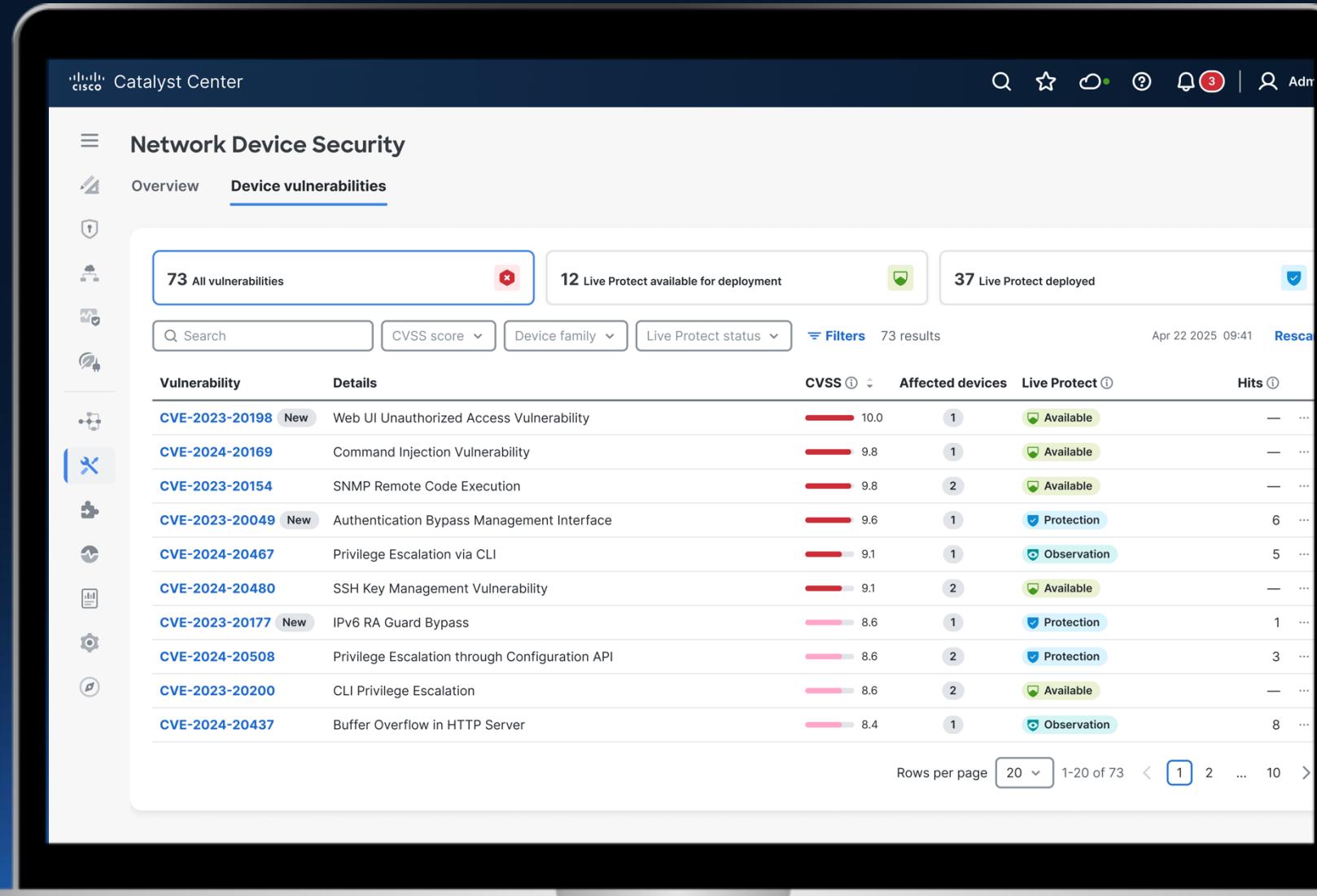
Trustworthy Technologies Verification



Coming

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 main title is "Network Device Security" with tabs for "Overview" and "Device vulnerabilities". The "Device vulnerabilities" tab is selected. At the top, there are three status boxes: "73 All vulnerabilities" (red), "12 Live Protect available for deployment" (green), and "37 Live Protect deployed" (green). Below these are search and filter options: "Search", "CVSS score", "Device family", "Live Protect status", and "Filters". The main table lists 73 vulnerabilities with the following data:

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 pagination controls: "Rows per page" (20), "1-20 of 73", and page numbers 1, 2, ..., 10.

Key Takeaways

1 A future proof campus network

- High performance, hyper-resilient campus network serves users with lightening fast reliable connectivity (including Wifi7)
- Up to 90W Power for IOT & Collaboration devices, ability to add as many 4K Cameras / Video / AI agents one day), and low latency to support advanced workloads such as AR or robotics.
- Ability to run more complex services right on the switch (e.g. Hypershield in the future)

2 The most secure campus infrastructure on the market

- Cisco is a trusted security partner, offering a compelling vision, components needed for Security, with a a roadmap for the future
- Cisco Delivered Secure Architecture offers Layered Security, Protecting Devices, Data Traffic, and Endpoints.
- Automation to manage micro & macro segmentation at scale. Works with existing NGFW, and delivers consistent Policy across my entire network.

3 Simpler NetOps

- Cisco is delivering greater simplicity from Cisco with a plan for consistency between on Prem and Cloud, allowing migration to cloud over time (remote offices first and/or leverage hybrid mode etc.)
- Leverage benefits of SDA from the cloud, with a simpler more streamlined experience.
- AI Assistant and End2End Assurance help get application visibility and troubleshoot faster.

Thank you

