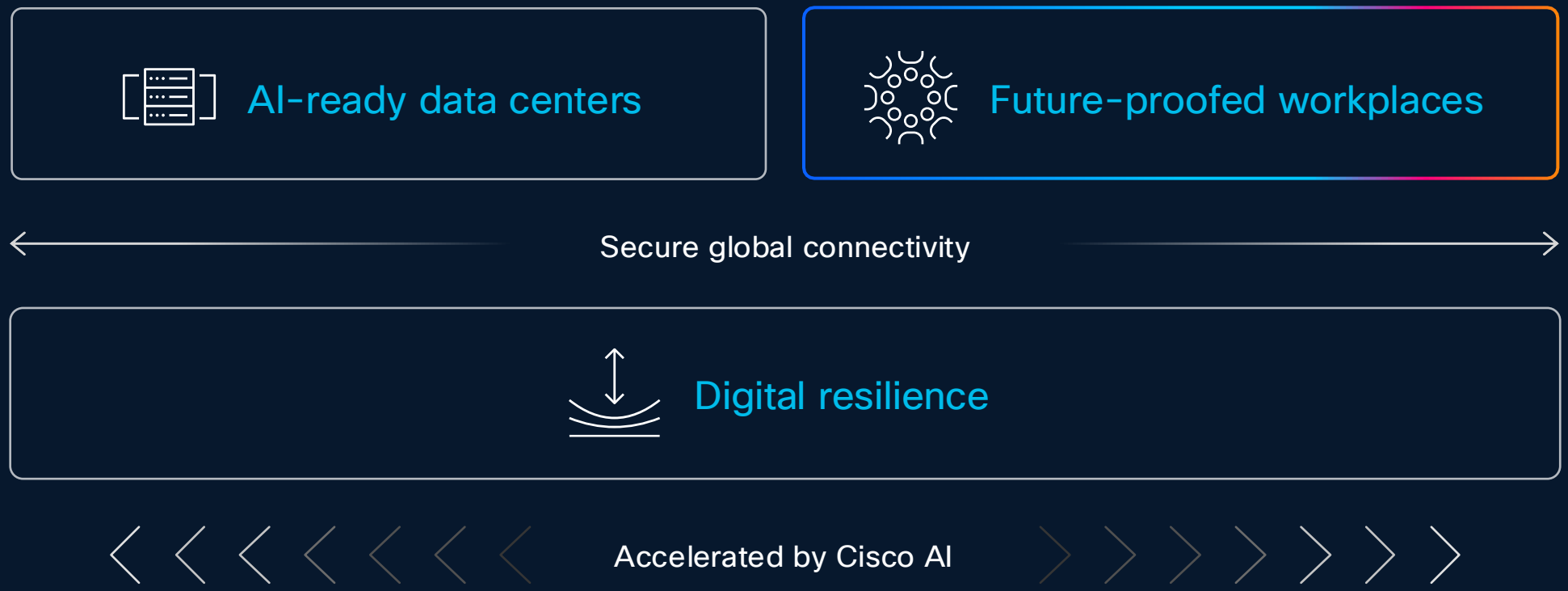
CISCO Connect

Modernize the Network with Cisco Secure Campus



Brandon Dodd - Solutions Engineer
David Friday- Solutions Engineer

Cisco powers how people and technology work together across the physical and digital worlds



© 2026 Cisco and/or its affiliates. All rights reserved.

Future-proofed workplaces

Empower and secure every worker, anywhere work happens



Modernize and secure the network

With scalable devices, AgenticOps, and security fused into the network



Secure the human and agentic workforce

With identity, zero trust, SASE, and agent protection



Create intelligent workplace experiences

With collaboration and networking feeding data and intelligence

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

AI is accelerating networking and security challenges across the Campus



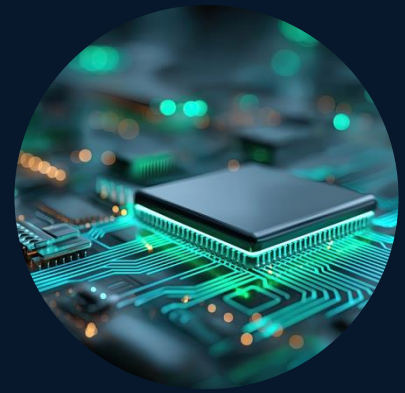
144:1

Non-human identities outnumber humans



84%

of high severity attacks come from inside



68%

of cyber incidents involve machine identities

Machine-speed interactions require AI-ready networking with machine-speed security

*Jul 2024-Jun 2025 Sources: Gartner, Bitdefender 2025, Cybersecurity Assessment Report, The NHI & Secrets Risk report H1 2025

© 2026 Cisco and/or its affiliates. All rights reserved.

As the network becomes more complicated, so does the security challenge



© 2026 Cisco and/or its affiliates. All rights reserved.

Our approach: Architecture for the AI-ready secure network

Simplified operations
powered by AgenticOps



Security
fused into the network



Scalable devices
ready for AI



What happens when everything connected to the network is moving at machine speed?

© 2026 Cisco and/or its affiliates. All rights reserved.

Operations must evolve before automation can scale

Critical Campus Operations Capabilities



Visibility across everything



Proactive issue resolution



Continuous optimization

© 2026 Cisco and/or its affiliates. All rights reserved.

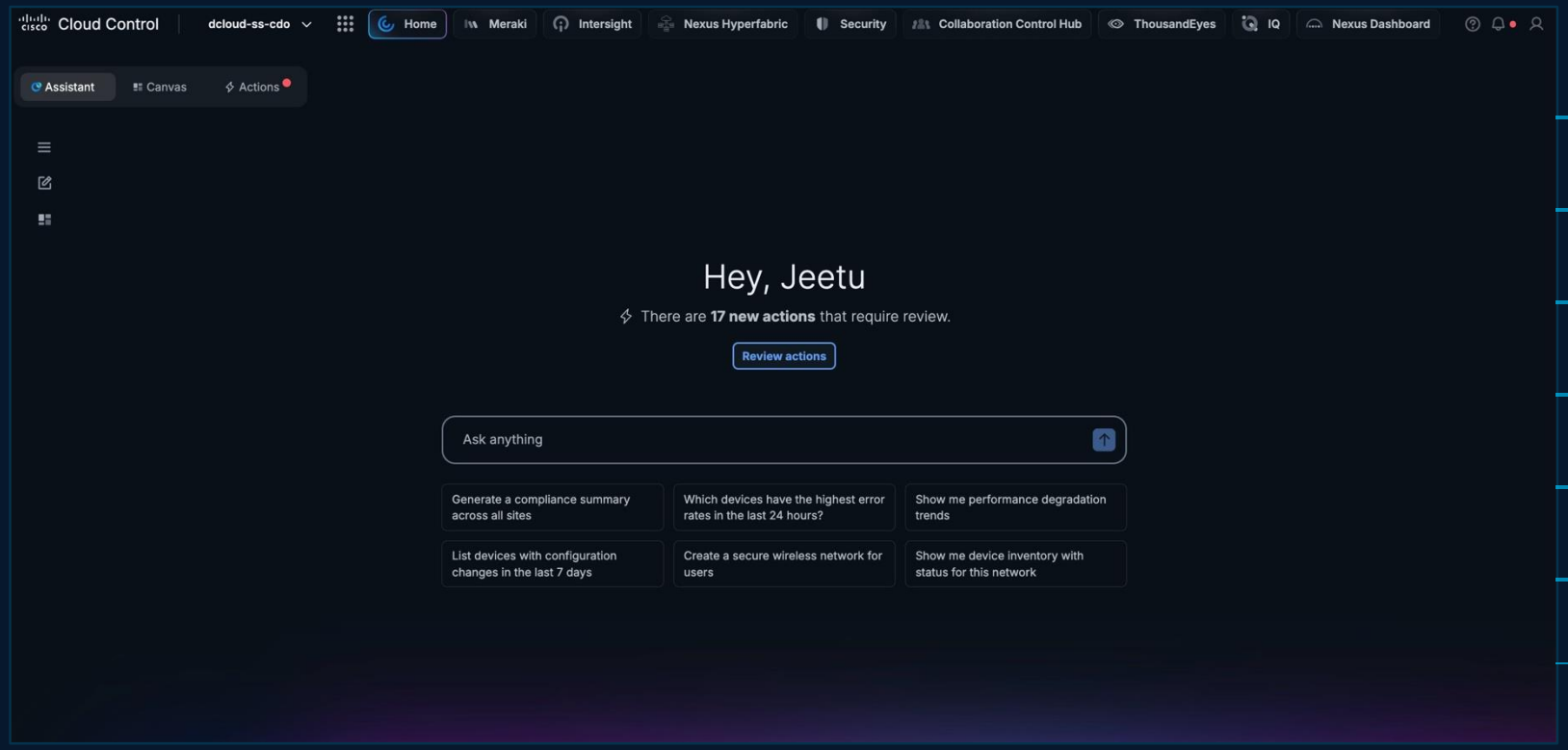


CISCO Cloud Control

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Visibility across everything with Cisco Cloud Control



- Data center networking
- Workplace networking
- Compute
- Security
- Observability
- Collaboration
- Service providers

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Cloud Control

The power of one

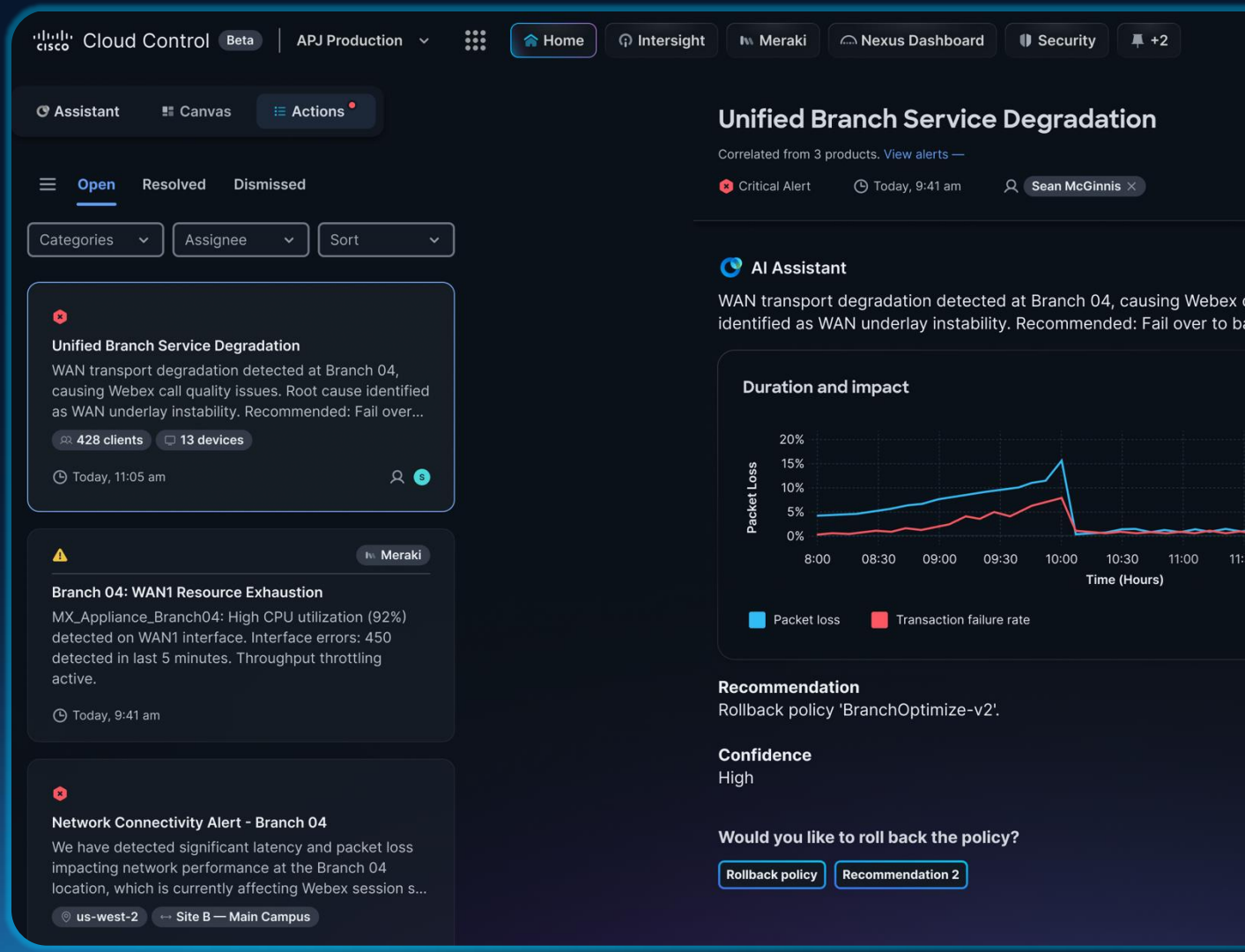
One login
Sign in once. See everything.

One inventory and topology
Every asset. See how it all connects, in real time.

One view for alerts
Actions correlates alerts across every product.

One assistant
Quick answers and tasks with AI Assistant.

One agentic workspace
Investigate, execute and resolve with AI Canvas.



© 2026 Cisco and/or its affiliates. All rights reserved.

Proactive issue resolution with AgenticOps

Cisco Cloud Control

AI Assistant | AI Canvas | Studio | Cisco dashboards | Third party & APIs



Cross-domain telemetry



Purpose-built models



Trusted agents

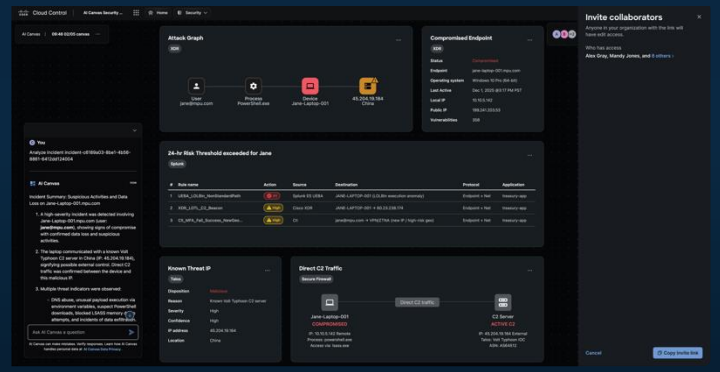
© 2026 Cisco and/or its affiliates. All rights reserved.

Automation and Assurance are essential elements

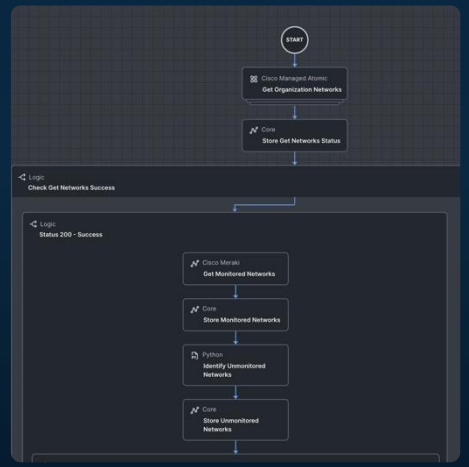
From Alerts to Answers in Minutes
AI Assistant

cisco AI Assistant

Cross-domain collaborative troubleshooting
AI Canvas



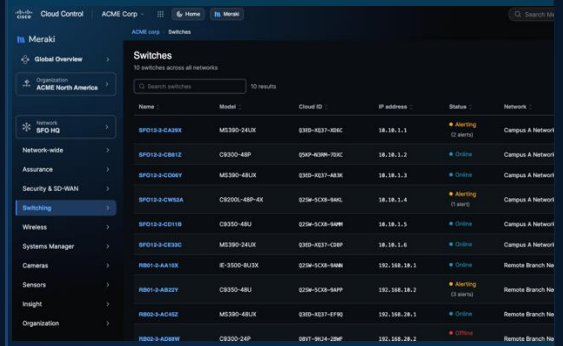
AI-driven network automation
Agentic Workflows



© 2026 Cisco and/or its affiliates. All rights reserved.

Continuous optimization enables operational clarity

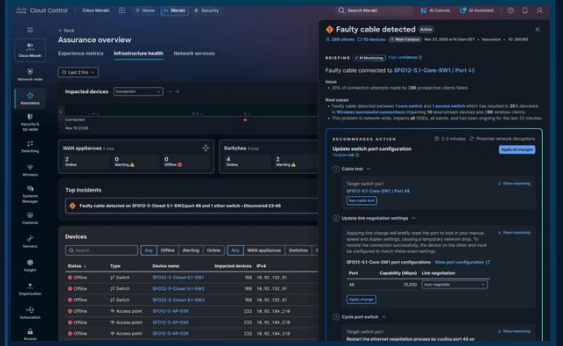
CLI Profiles



Cloud management at scale

BETA

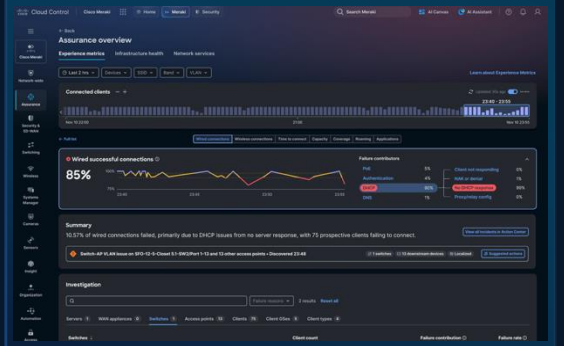
Infrastructure health



Resolve infrastructure issues before users feel them

ALPHA

Experience Metrics



Understand user impact

BETA

Fabric troubleshooting with AI Assistant



Accelerate RCA and remediation

BETA

© 2026 Cisco and/or its affiliates. All rights reserved.

How AgenticOps works: data, model, people, action

Cisco Cloud Control is one control plane where operators and agents work from the same data



1 Collect

Telemetry from networking, security, observability and compute, plus ServiceNow, Okta, Entra ID and others via Marketplace



2 Correlate

Cisco Data Fabric: a Splunk-based store of cross-domain log data, so agents see correlated events, not one product's view



3 Reason

Deep Network Model: a networking LLM trained on CCIE-level content and Cisco U courseware. Cisco cites 20%+ higher precision than general models



4 Investigate

AI Assistant answers in plain language and escalates. In AI Canvas, operators and agents test likely causes in parallel



5 Act

Identity, permissions, policy and operator oversight govern every agent. Important actions stay under human control

- **GA in the U.S.:** Cloud Control, AI Canvas, AI Assistant
- **No extra charge:** included in Essentials and Advantage subscriptions
- **Late 2026:** Cloud Control Studio (Agent Builder, App Builder)

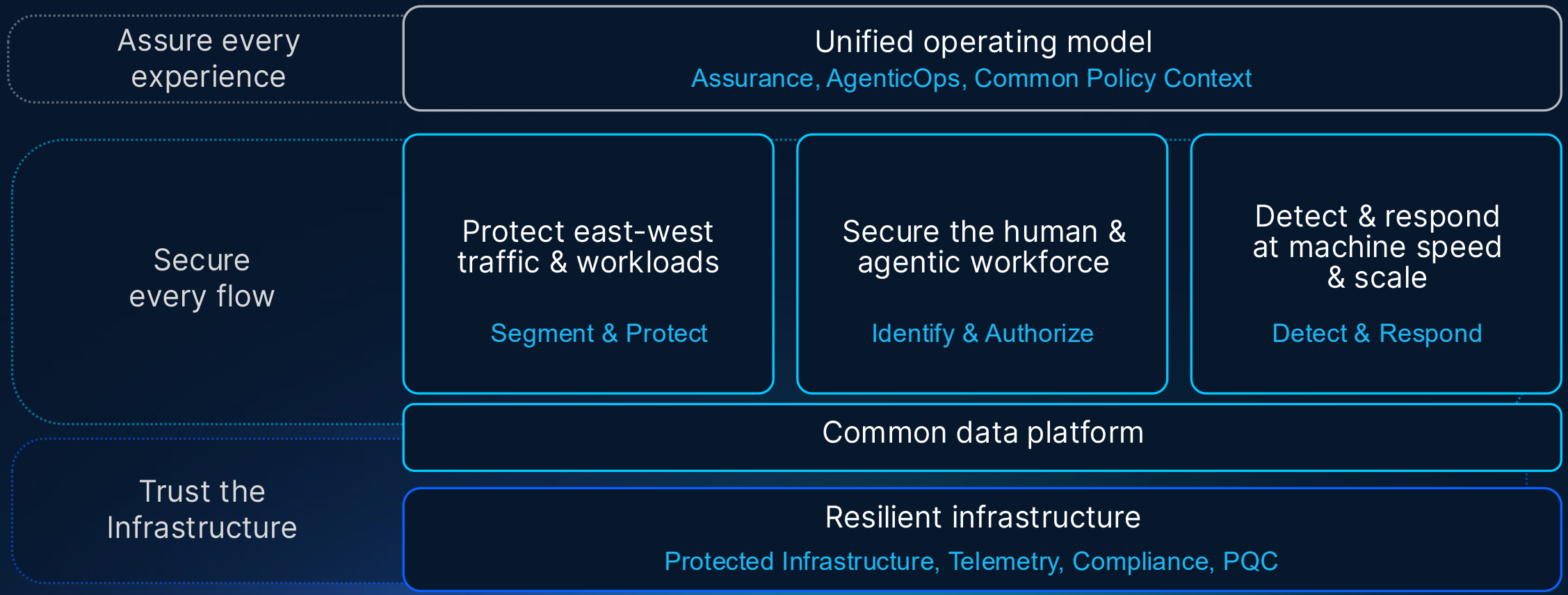
Sources: Cisco Cloud Control At a Glance (Aug 2026); Cisco blog, Meet the Cisco Deep Network Model (2025); Cisco blog, A New Era for Networking (2025); TechTarget, Cisco Cloud Control unites AgenticOps (Jun 2026)

© 2026 Cisco and/or its affiliates. All rights reserved.

Demo! AgenticOps

The network is the only enforcement layer that is always present

The solution: a platform approach to security



© 2026 Cisco and/or its affiliates. All rights reserved.

Each security pillar maps to a mechanism on the switch

What actually enforces "Segment & Protect," "Identify & Authorize" and "Detect & Respond"

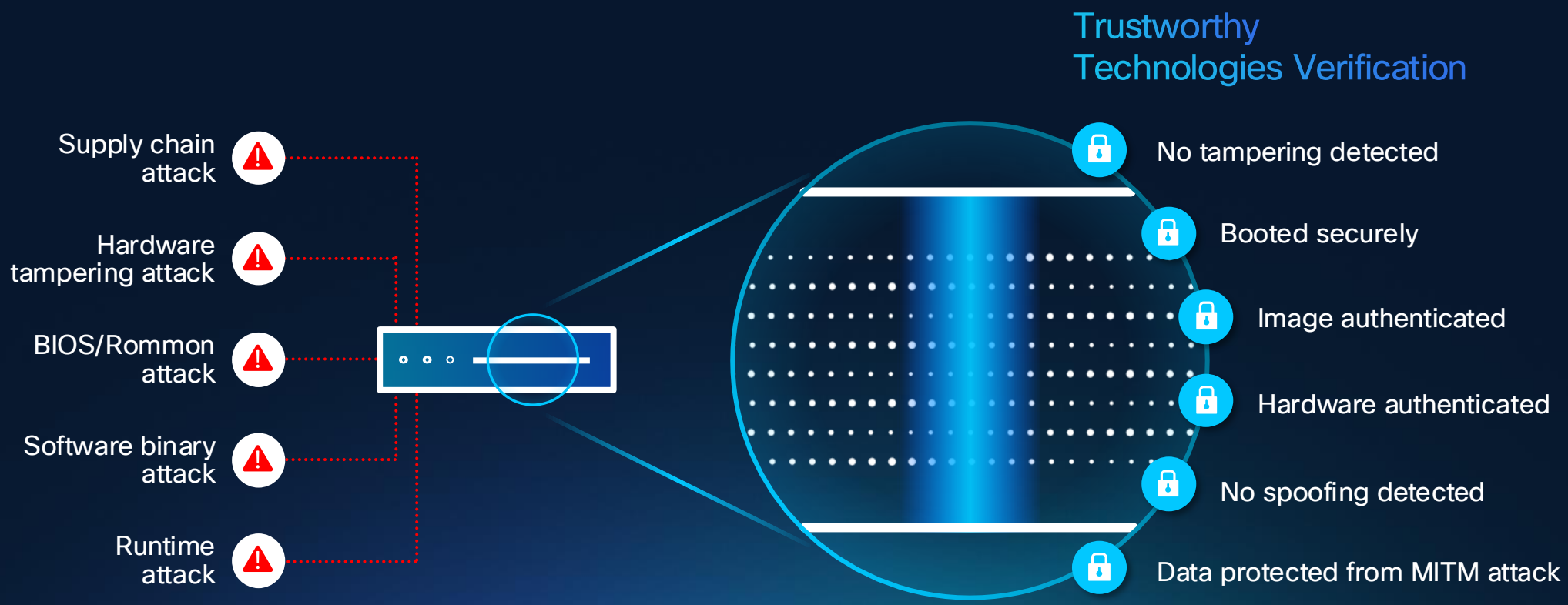
	Segment & Protect	Identify & Authorize	Detect & Respond
Threat it answers	*Lateral movement with valid credentials and approved tools*	*Machine identities (144:1) with no owner, profile or policy*	*Living-off-the-land activity that looks like normal admin work*
Mechanism	TrustSec SGTs classify traffic at ingress; SGACLs enforce group policy in switch hardware; VXLAN and VRFs separate macro segments	802.1X and MAB with Cisco ISE; profiling gives every device, service and agent an identity and an SGT; IP Device Tracking keeps bindings current	Flexible NetFlow at line rate on Silicon One; flows feed Cisco Data Fabric for cross-domain correlation in AI Canvas and Splunk
Where it runs	C9350 and C9550 (VXLAN and TrustSec segmentation); smart switches join Hybrid Mesh Firewall policy	Access edge on C9350; ISE policy follows the user or device across wired and wireless	C9350: 128K HCAM entries shared by ACLs and NetFlow. C9550: up to 64K NetFlow entries per direction

Sources: Cisco C9350 and C9550 Smart Switches data sheets (2026); Cisco blog, A New Era for Networking (2025); Bitdefender Labs (2025); Entro Labs H1 2025

© 2026 Cisco and/or its affiliates. All rights reserved.

Trust the infrastructure: Securing the device

Secure from hardware to software, from boot time to runtime



© 2025 Cisco and/or its affiliates. All rights reserved.

Chain of trust: from silicon to runtime

Anchored in hardware at boot, provable on demand, defended while running



Trust Anchor (TAm)

Tamper-resistant chip: secure storage, RNG, key store, crypto engine

Secure boot

Hardware-anchored microloader checks the boot chain; halts boot on compromise

Signed images

SHA-512 hash signed with a Cisco private key, verified before load

SUDI identity

IEEE 802.1AR X.509v3 cert; private key bound to the TAm, never exported

Runtime defenses

ASLR, BOSC and X-space block code-injection attacks

Live Protect

eBPF compensating controls for new CVEs, without a reboot

Prove it live

Signed outputs include your nonce, so a compromised device can't replay old results.

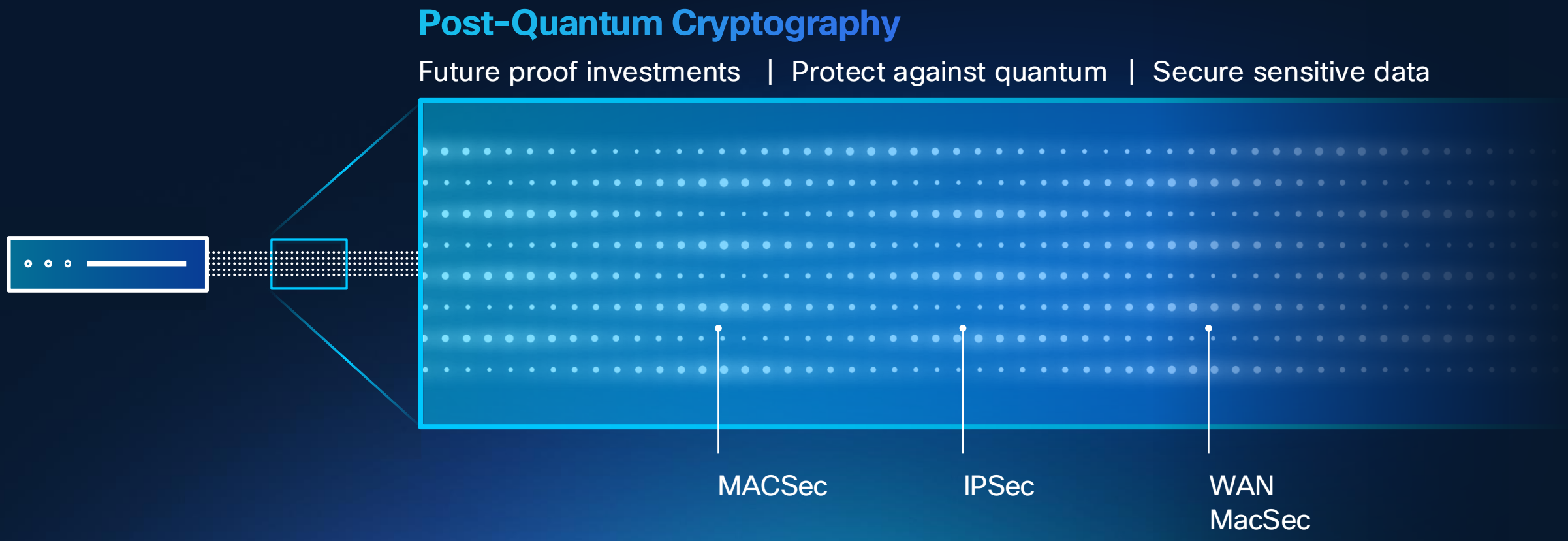
`show platform integrity sign nonce 12345`	Boot-chain measurements, signed by the device
`show software authenticity running`	Signer and certificate of the running image
`show platform sudi certificate sign nonce 12345`	SUDI certificate chain plus a signature over your nonce

Sources: Cisco Trustworthy Technologies data sheet; Cisco IOS XE Forensic Data Collection Procedures; Meraki Live Protect Configuration Guide (2026)

© 2026 Cisco and/or its affiliates. All rights reserved.

Trust the infrastructure: securing network connectivity

Secure and protect your data over unowned infrastructure



© 2025 Cisco and/or its affiliates. All rights reserved.

Building a quantum resistant network



Encryption

Generate the encryption key for secure communication



Authentication

Verify the authenticity of the communicating devices / users



Secure Boot

Ensure authenticity and integrity of software and hardware

Building Post Quantum Resistance

© 2026 Cisco and/or its affiliates. All rights reserved.

Quantum-safe IPsec on IOS XE is two lines of config

Hybrid ML-KEM-768 key exchange, verified in the show output

IOS XE 26.1: ML-KEM-768 hybrid key exchange for IKEv2 and IPsec (NIST FIPS 203)

IOS XE 26.2: ML-DSA-44/65/87 signatures for IKEv2 authentication, so the tunnel is quantum-safe end to end

Hybrid by design: classical ECDH (group 20) and ML-KEM together, never weaker than today

Why now: traffic recorded today can be decrypted once quantum attacks mature (harvest now, decrypt later)

Configuration (hub and spokes)

```
crypto ikev2 fragmentation mtu 1400
!
crypto ikev2 proposal PQC-PROPOSAL
 pqc mlkem768 optional
 encryption aes-cbc-256
 integrity sha512
 group 20
```

Verification

```
R1# show crypto ikev2 sa detailed
 Encr: AES-CBC, keysize: 256, PRF: SHA512,
   DH Grp:20, Auth sign: PSK, Auth verify: PSK
 PQC Key Exchange: ML-KEM-768
 Quantum-safe Encryption using PQC: ML-KEM-768
```

Cisco lab: three Cisco 8000 Secure Routers (C8235-G2), IOS XE 26.2, Advantage license

Source: Cisco DevNet blog, Post-Quantum Key Exchange on Cisco Routers, IPsec Series Part 9 (Sep 2026)

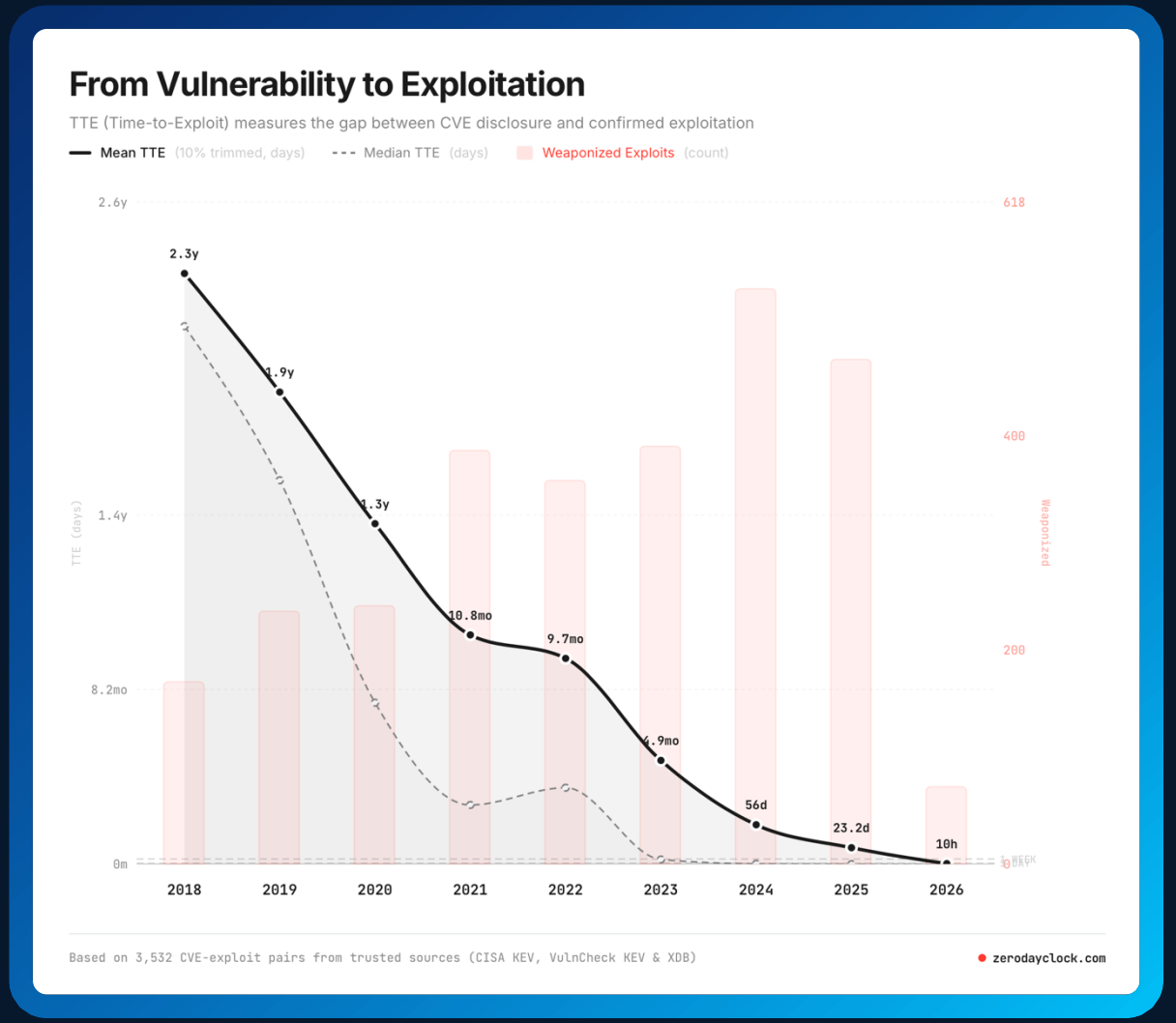
© 2026 Cisco and/or its affiliates. All rights reserved.

What happens when a vulnerability emerges after deployment?

© 2026 Cisco and/or its affiliates. All rights reserved.

Vulnerability reports are spiking; the weaponization window has collapsed.

Industry-wide Impacting All Vendors

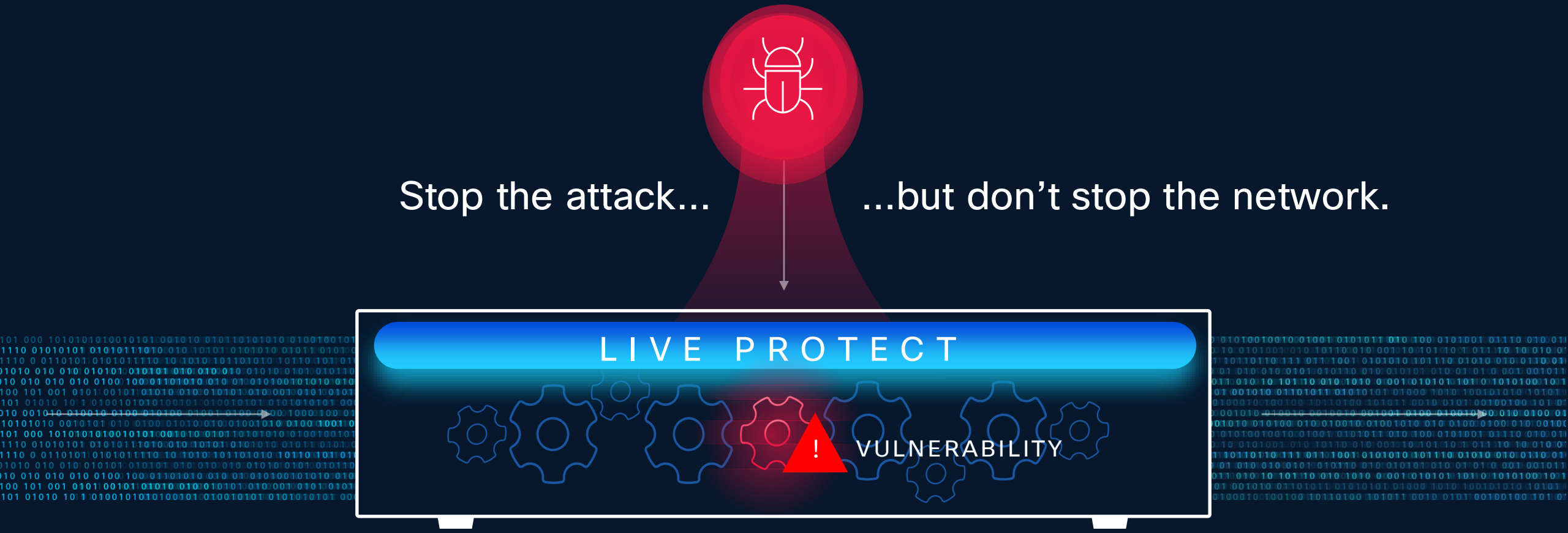


Source: https://vulntools.net/cnas/GitHub_M

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Live Protect

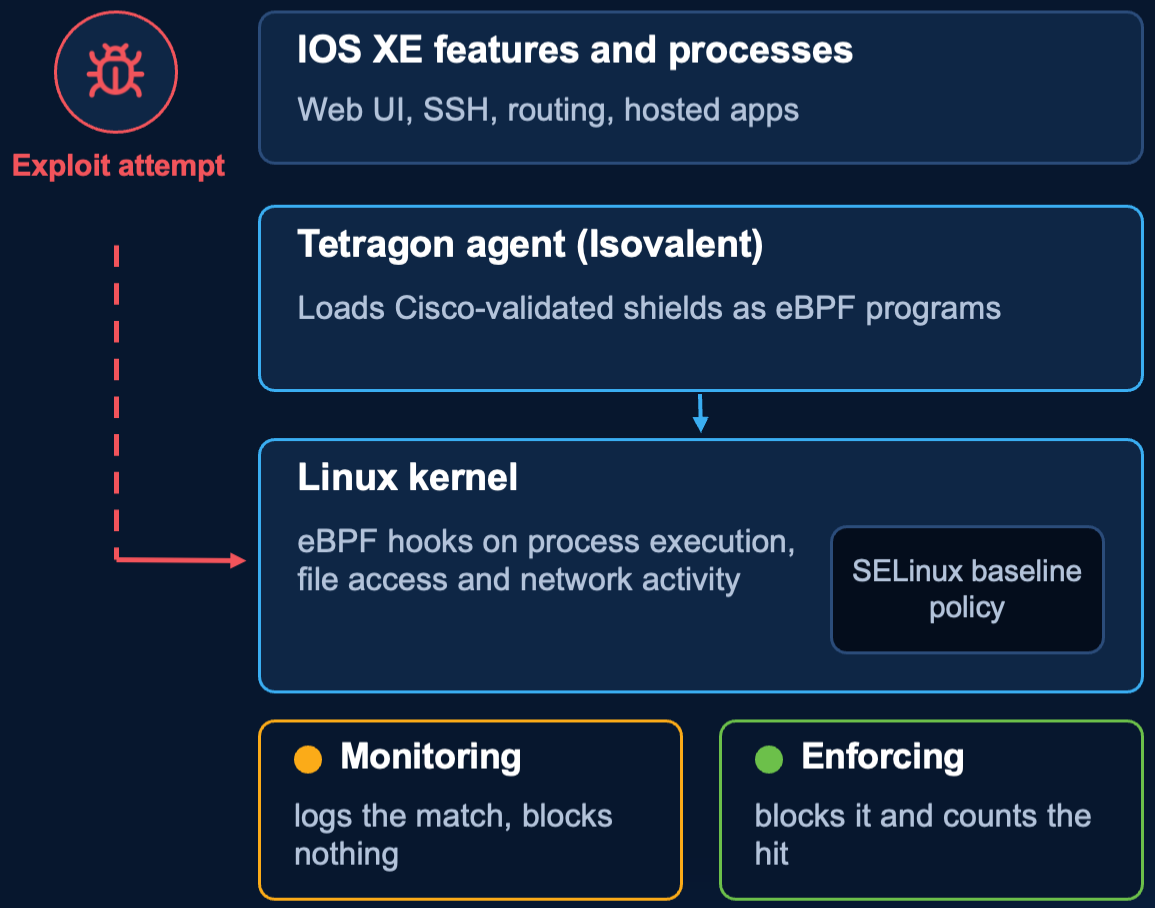
Vulnerability shielding for Cisco networking devices



© 2026 Cisco and/or its affiliates. All rights reserved.

Live Protect: a kernel-level shield, not a patch

eBPF enforcement inside IOS XE, deployed without an upgrade or a reboot



One shield per advisory

A Cisco-validated, CVE-specific control, packaged as a signed .lps.SPA.bin file and installed beside the IOS XE image

No upgrade, no reboot

eBPF programs attach to the running kernel. The kernel source is never modified and the switch keeps forwarding

Buys time; doesn't replace the fix

The shield blocks the exploit path while the permanent fix moves through your normal upgrade cycle

Sources: Meraki docs, Cisco Live Protect Configuration Guide (Sep 2026); Network World, Cisco details Live Protect (2026); Isovalent, Cisco Live 2025 recap

© 2026 Cisco and/or its affiliates. All rights reserved.

Why it matters: the 2023 IOS XE Web UI exploit

34 days from first activity to first fix, and the only interim fix was turning the feature off

Sep 18
First related activity observed

Sep 28
Cisco TAC case flags unusual device behavior

Oct 12
Second wave; implant deployed

Oct 16
Advisory and Talos blog: CVE-2023-20198 (CVSS 10.0)

Oct 20
CVE-2023-20273 (CVSS 7.2) found: root escalation, implant written to disk

Oct 22
Fixes begin rolling out, 17.9 train first

41,000+ devices

estimated implanted within days of disclosure (Censys, LeakIX)

Interim fix: turn it off

`no ip http server` and `no ip http secure-server` on every exposed device

The third option

A compensating control blocks the exploit path, keeps the service up, and buys time to patch on schedule

Sources: Cisco Talos, Active exploitation of Cisco IOS XE Software Web UI (Oct 2023); Cisco PSIRT advisory (Oct 16, 2023); The Hacker News, citing Censys and LeakIX (Oct 2023)

© 2026 Cisco and/or its affiliates. All rights reserved.

Demo! LiveProtect!

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	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

© 2025 Cisco Systems, Inc.

RTP-ND-AI
Home
Manage
Analyze
Admin

Device Security

Related content Refresh

Security advisories | Topology

Advisories | Devices

Filter by attributes

Enable Live Protect

	Name	Fabric	Security advisories	Live protect	Live Protect Shield: Protected	Live Protect Shield: Monitored	Live Protect Shield: Available	Model	Software version	Serial number	Total hit count
☐	RTP-AI1-FE-Leaf3	rtp-ai1-fe	2	Not enabled	-	-	1 1	N9K-C9332D-GX2B	10.6(2)	FLM292804PZ	-
☐	RTP-AI1-FE-Leaf4	rtp-ai1-fe	2	Not enabled	-	-	1 1	N9K-C9332D-GX2B	10.6(2)	FLM29360DPS	-
☐	RTP-AI1-FE-Spine1	rtp-ai1-fe	2	Enabled	-	1	1	N9K-C9332D-GX2B	10.6(2)	FDO28240HEB	-
☐	RTP-AI1-FE-Spine2	rtp-ai1-fe	2	Enabled	-	1	1	N9K-C9332D-GX2B	10.6(2)	FDO28290CGQ	-
☐	RTP-AI1-FE-sLeaf1	rtp-ai1-fe	-	Enabled	-	-	-	N9324C-SE1U	10.6(2s)	FDO29400BW2	-
☐	RTP-AI1-FE-sLeaf2	rtp-ai1-fe	-	Enabled	-	-	-	N9324C-SE1U	10.6(2s)	FDO29360W9X	-
☐	RTP-AI1-Leaf1	rtp-ai1	2	Enabled	1	-	1	N9K-C9332D-GX2B	10.6(2)	FDO28290CGX	-
☐	RTP-AI1-Leaf2	rtp-ai1	2	Enabled	1	-	1	N9K-C9332D-GX2B	10.6(2)	FDO28290CJB	-
☐	RTP-AI1-Leaf3	rtp-ai1	2	Not enabled	-	-	1 1	N9K-C9332D-GX2B	10.6(2)	FDO28290CQT	-
☐	RTP-AI1-Leaf4	rtp-ai1	2	Not enabled	-	-	1 1	N9K-C9332D-GX2B	10.6(2)	FDO28290CET	-

Customer case study:

Nutrien®
Feeding the Future®

"Many of our workers move from site to site and location to location. Having it be simple for them—having it be consistent across all sites, all locations, and just work wherever they are—is really important to the business of Nutrien."

Mark Murray, VP, IT Infrastructure and Cybersecurity, Nutrien

Zero Trust
Unified security posture at scale

4 hours
Secure fabric deployed

1 km
Connectivity delivered underground



© 2026 Cisco and/or its affiliates. All rights reserved.

An AI-ready network starts with infrastructure designed for AI.

© 2026 Cisco and/or its affiliates. All rights reserved.

Scalable devices, ready for AI

- Unified hardware
- Unified software
- Unified management
- Post-quantum ready



Smart Switches



Secure Routers



Industrial devices



Secure Firewall



Scalable Wi-Fi 7

CISCO SILICON ONE
K-SERIES & A-SERIES

© 2026 Cisco and/or its affiliates. All rights reserved.

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

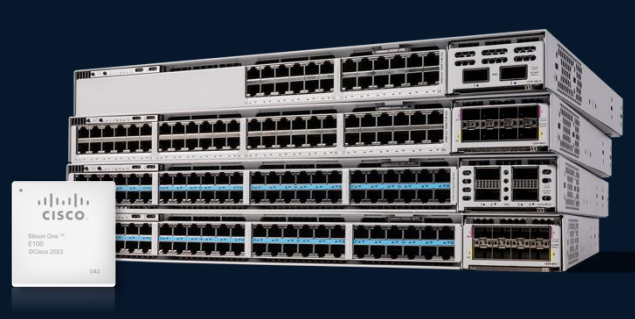

C9350


Modular

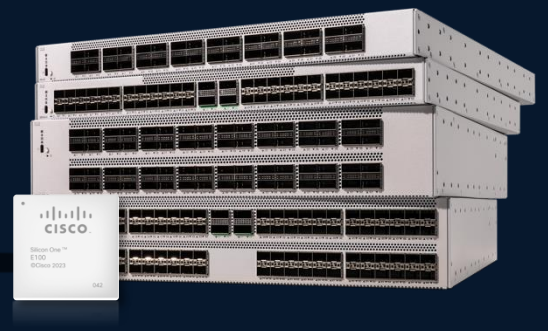
© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Smart Switches Built for AI Scale and Security.

- High-performance, low latency for AI scale
- Cisco Silicon One + co-processor for security and AI
- Quantum Safe
- Intelligent energy efficiency
- Sub-second upgrades



C9350 Access
New variants



C9550 Fixed Core & Agg.
New model

© 2026 Cisco and/or its affiliates. All rights reserved.

Powered by Silicon One

- Boosts hardware encryption post quantum security
- High-scale, low latency for time-sensitive apps
- Flexible and programmable for AI and ML
- Efficient power performance
- Intelligently adaptable to mitigate link failures, congestion, and bandwidth challenges



Cisco Silicon One for Scale, Security, and Efficiency

© 2026 Cisco and/or its affiliates. All rights reserved.

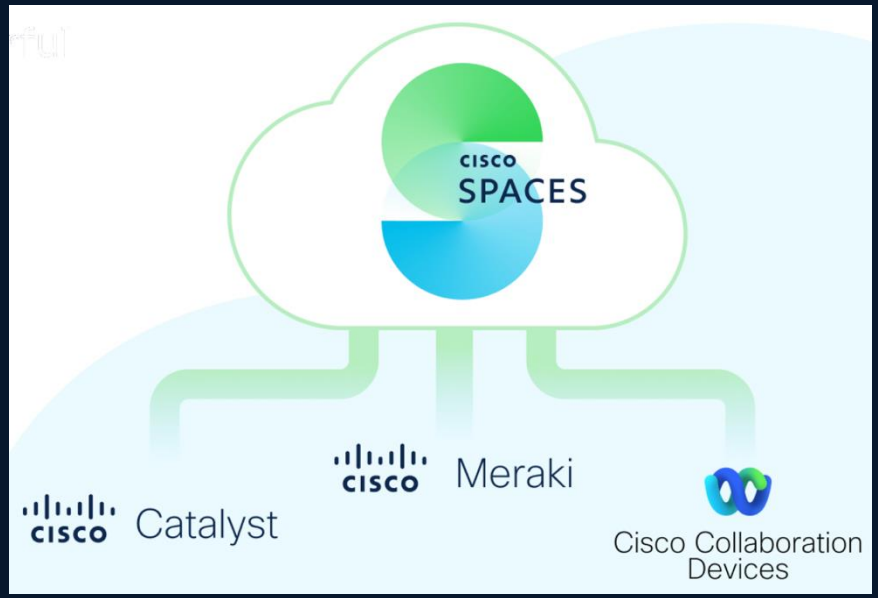
Beyond basic wireless connectivity

Unlock new experiences, insights, and business outcomes
from the same wireless infrastructure

Seamless Wi-Fi onboarding

Occupancy analytics

Ecosystem partner outcomes



Indoor navigation

Asset tracking

Workspace finder & booking

Energy efficiency

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Smart Cameras bring physical security onto the network

Cisco Smart Cameras (along with Axis devices) connect and can be managed through the Meraki Dashboard

NETWORK FOUNDATION

Connectivity behind every camera

SWITCHING

Switching provides wired camera connections and power where supported.

WIRELESS

Cisco wireless connects Wi-Fi devices and camera across the facility.

CAMERA CHOICE

Cisco + Axis camera portfolio

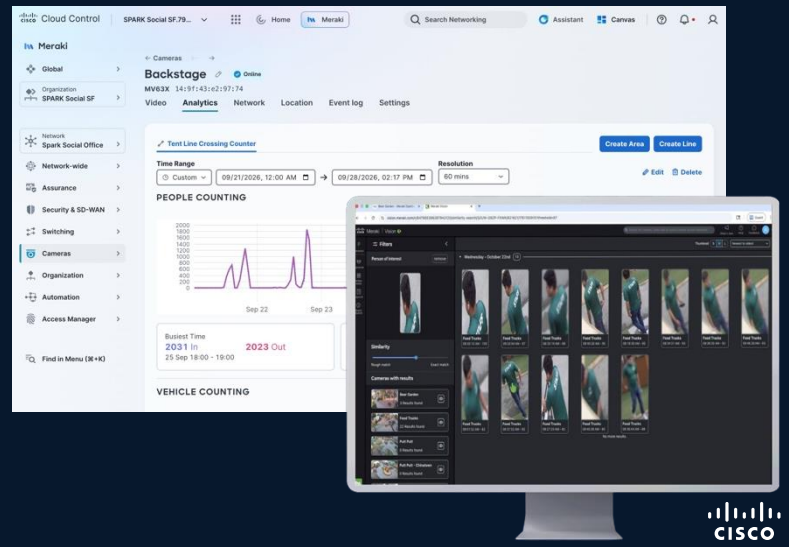
Cisco Smart Cameras and supported Axis devices expand cloud-managed camera choice.



CLOUD OPERATIONS

Manage and act from the cloud

Manage supported Axis devices alongside Cisco Smart Cameras through Meraki Dashboard. Camera analytics and AI-powered features help teams locate key footage and data.



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco extends the campus network architecture to outdoor and rugged spaces











Consistent Network Architecture

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco brings its IT expertise to rugged environments

Unified management



IOS XE Operating System

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

© 2026 Cisco and/or its affiliates. All rights reserved.