AI driven Automation and Assurance

Roque Gagliano
Principal solutions Engineer

Session ID: BRKATO-2065

Cisco Webex App

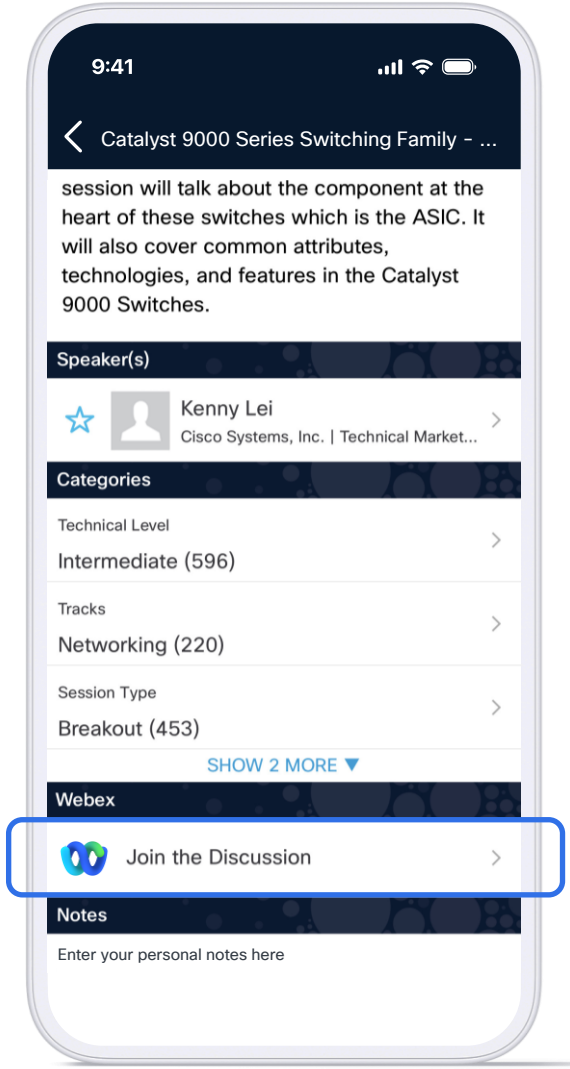
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKATO-2065

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

Agenda

01 AI and Agentic systems for Autonomous Networking

02 AI Enabled operations

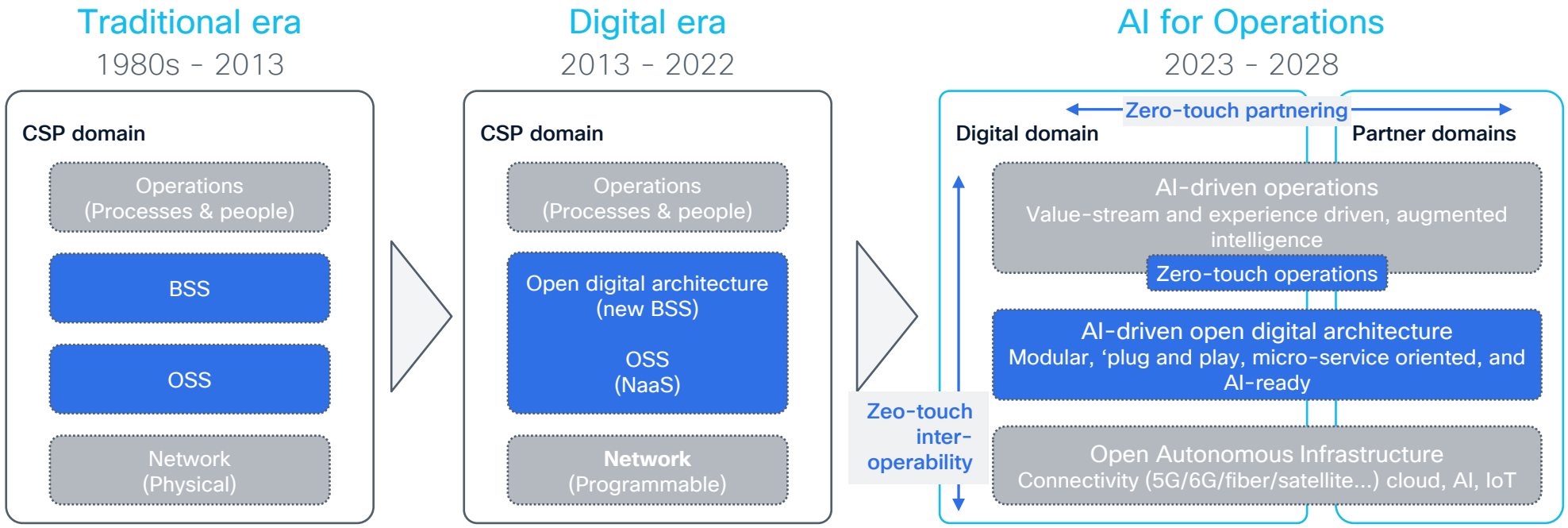
03 Summary

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

AI and Agentic systems for Autonomous Networking

Networks towards “AI-for-Operations”

Culture, Integrations and regulations are main barriers



[Source: - TMF Open Digital Architecture LINK]

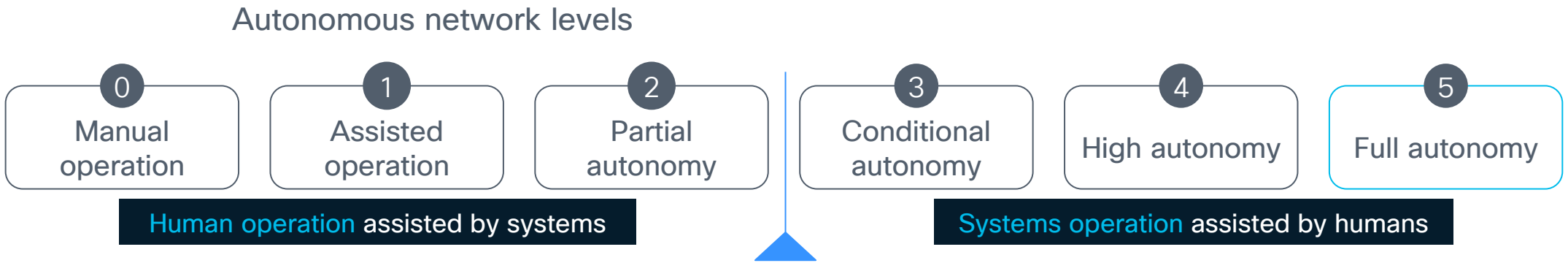
51% found Culture as the main barrier for adoption

48% found Integrations as the main barrier for adoption

[Source: CapGemini Research Jan 2024, 123 Telco surveyed - Transport Domain - LINK]

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

Journey and drivers for autonomous networking



84%

of companies are currently at initial levels of autonomy

The big disruption

61%

aiming to achieve Level 3 or above by 2028

$ Network Monetization

Operational efficiency

Resource efficiency and energy savings

Experience excellence

Source: Cap Gemini "Capgemini Research Institute, Autonomous Telco Networks Survey, December 2023-January 2024

Source: https://inform.tmforum.org/research-and-analysis/reports/autonomous-networks-exploring-the-evolution-from-level-0-to-level-5

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

cisco

Evolving from reactive to preventative to prescriptive

To succeed we need more intelligent systems

Reactive

Minimize the impact of network incidents

- Time series anomaly detection
- Root cause analysis

Improve operational KPIs and reduce churn

Preventive

Reduce the occurrence of network incidents

- Toxic factor identification
- Automated maintenance

Improve customer experience and optimize operations

Prescriptive

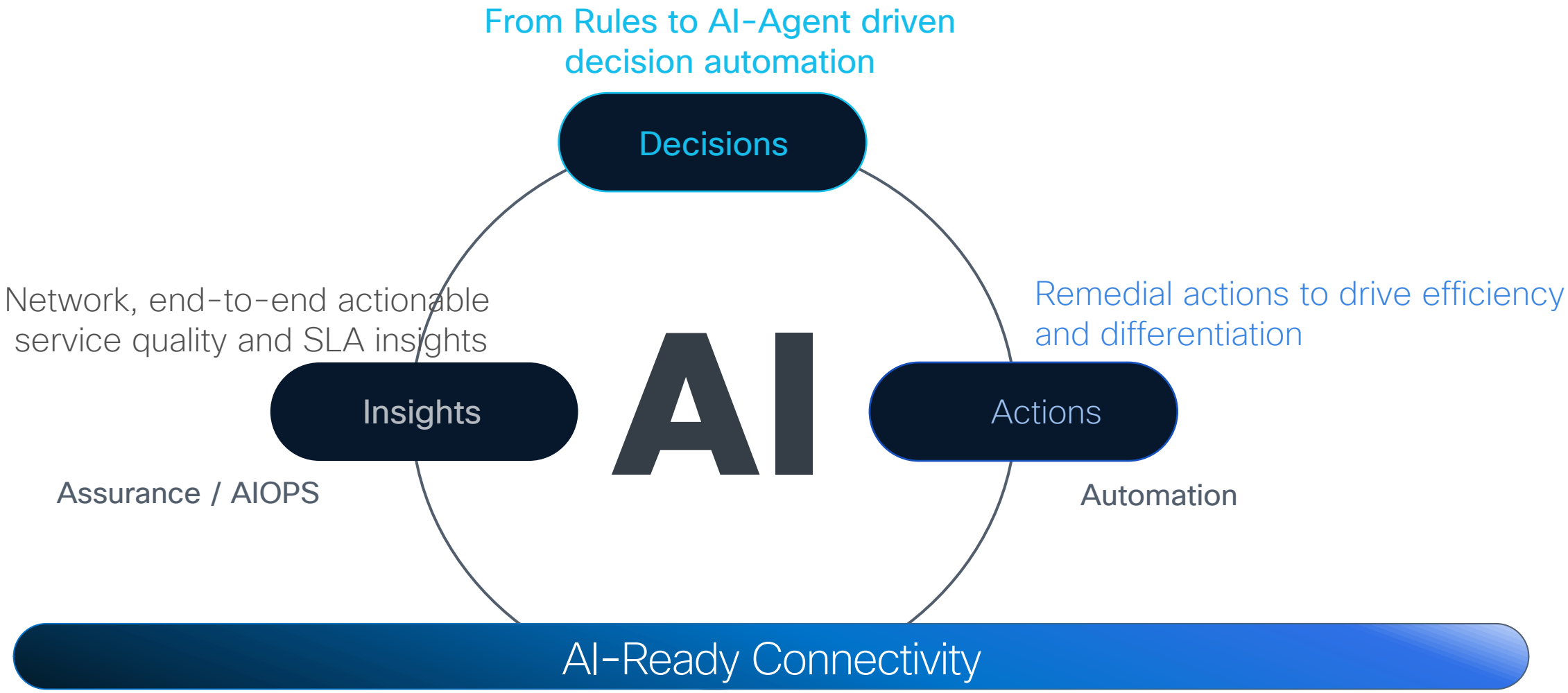
Automatically align network operations to policy/intent goals

- Operational recommendations
- Co-pilot code and config generation

Simplify operation lifecycle and reduce time-to-value

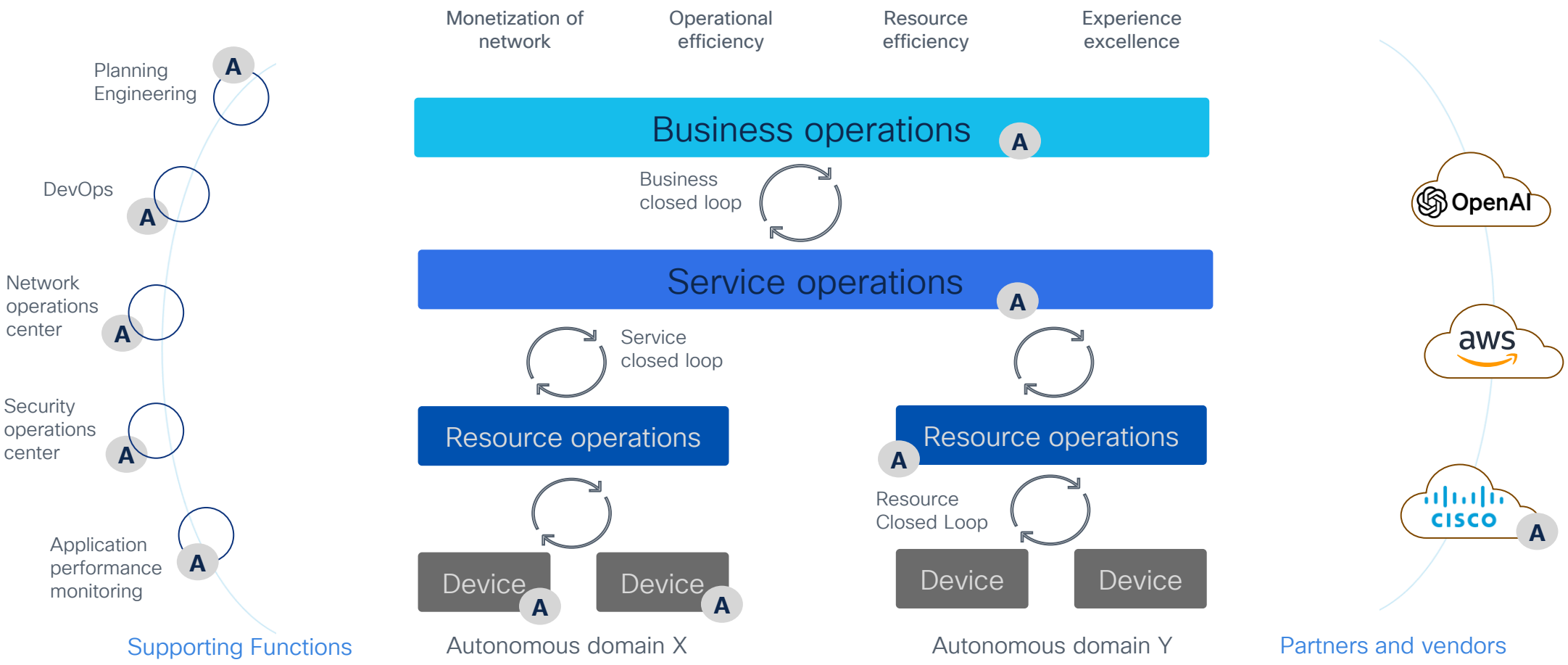
© 2025 Cisco and/or its affiliates. All rights reserved.

Our Vision for Operational Excellence



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

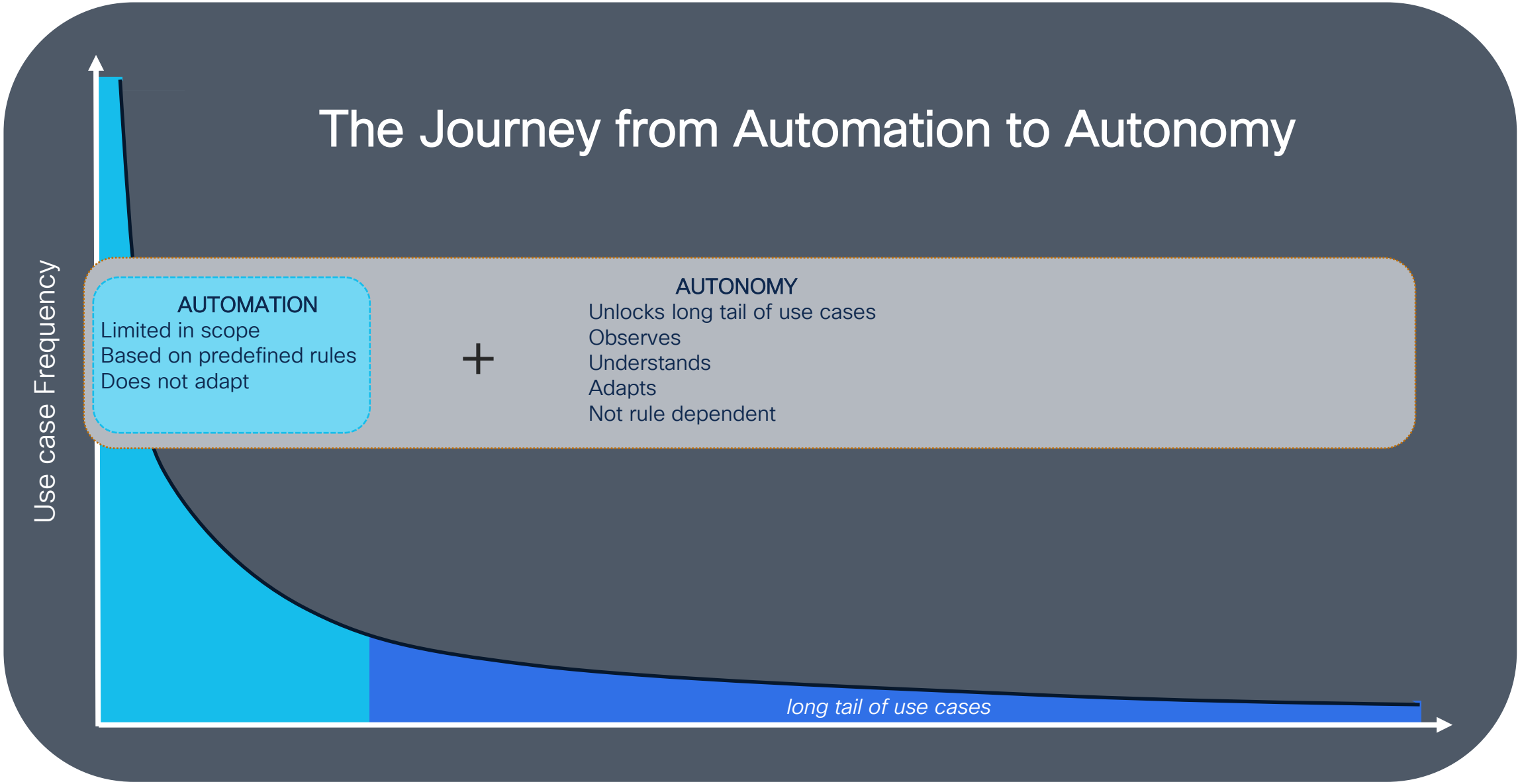
Autonomous networks requires a system view



Source: "Autonomous Networks Business Requirements & Architecture", TM Forum

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

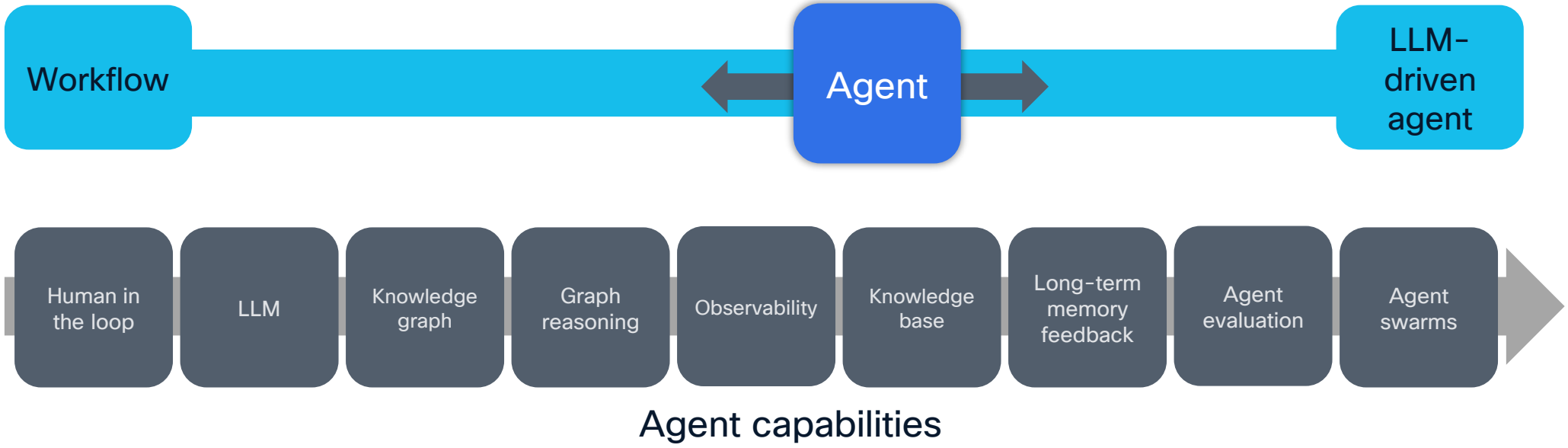
The Journey from Automation to Autonomy



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

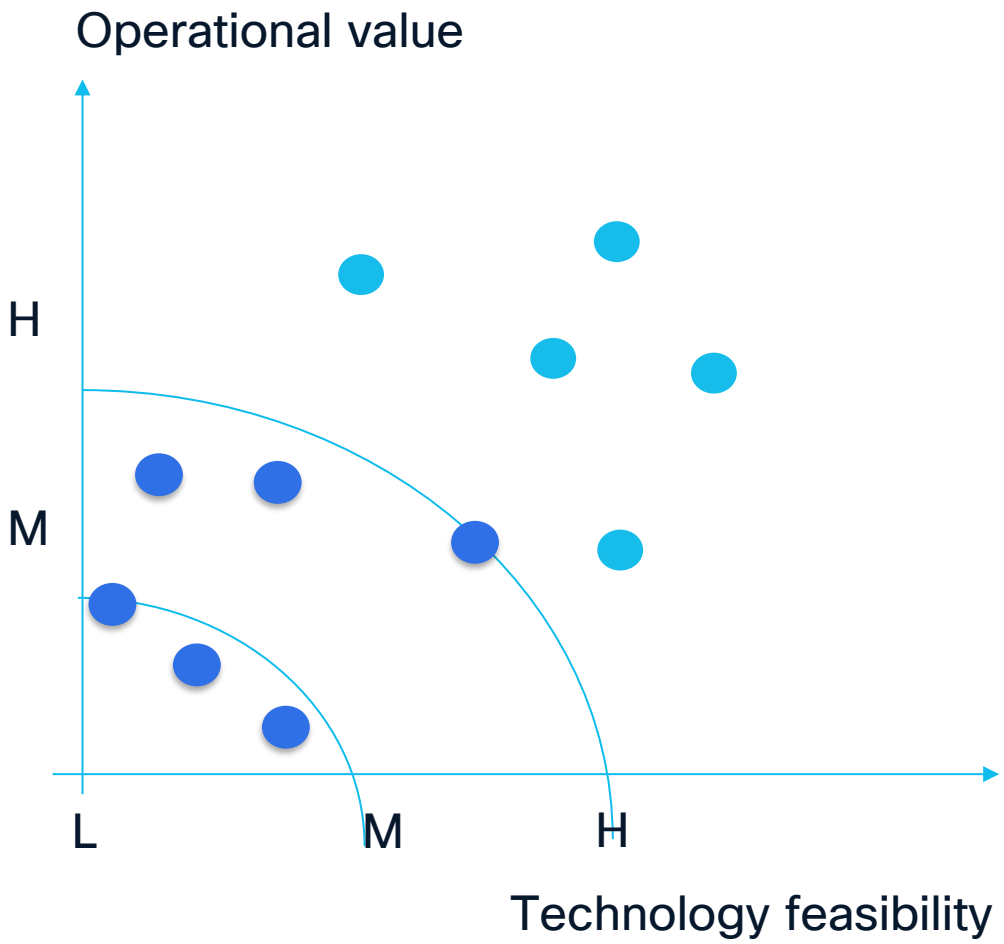
AI Agents are ...

“It is a partially or totally LLM-orchestrated workflow.”



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

What are the high value scenarios?



TMF-defined High Value scenarios

Services	Service provisioning
	Service assurance
	Complaints handling
IP networks	Fault management
	Network change
	Energy efficiency

Who builds the Agents and UseCases?

Services	Custom use case
	Root cause analysis
	NOC assistant
IP networks	Toxic factor identification
	Configuration drift
	Metric forecasting

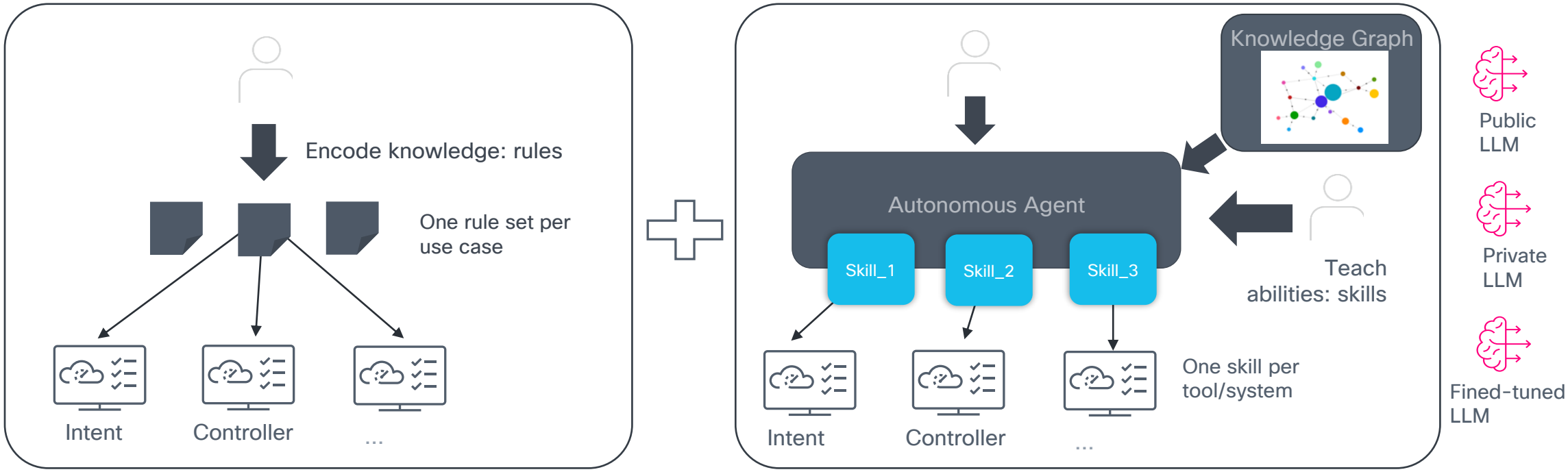
Your customer's roadmap to autonomous networking level 4/5

Vendor | Integrator | Customer

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

The future of Automation at Scale

"Give a man a fish, and you feed him for a day, teach a man to fish, and you feed him for a lifetime."



- Low scale: 1s/10s of closed loop use cases
- Knowledge encoded in rules -> invest in rules

- Each rule-set associated with one use case
- Static, limited
- L2/L3 – Autonomous Network Levels

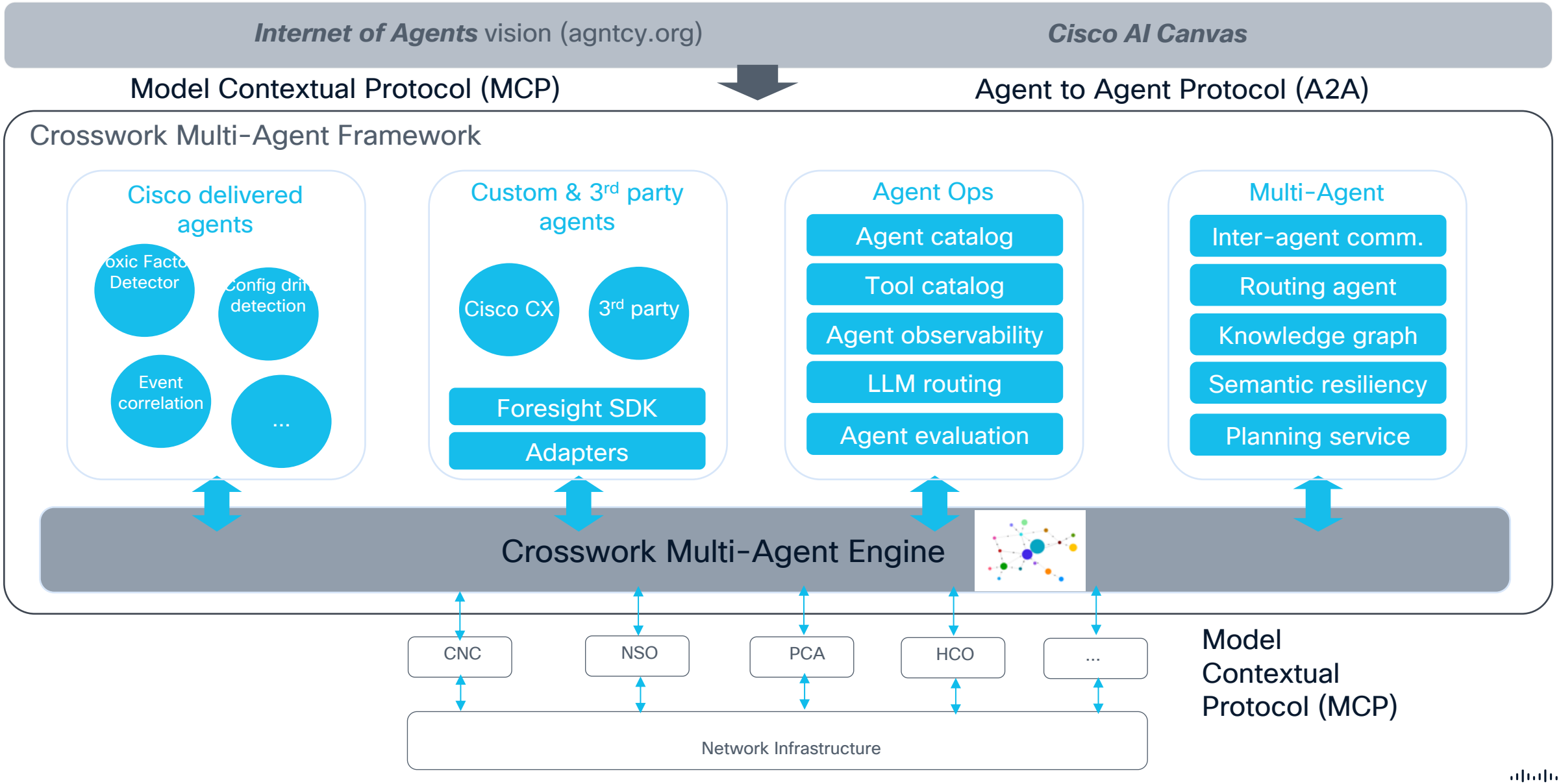
- Large scale: 100s/1000s of closed-loop use cases
- Knowledge compiled in LLM.
- Context tailors LLM responses.

- Skills enable Agent to interact -> invest in skills
- Dynamic, autonomous, extensible
- L4/L5 – Autonomous Network Levels

tmforum | L4 Autonomy blueprint | Phase 1 (2025-2027) Autonomous Agent driven closed loop | Phase 2 (2028-2030) Multi-agent collaboration for complex and multi-domain closed loop

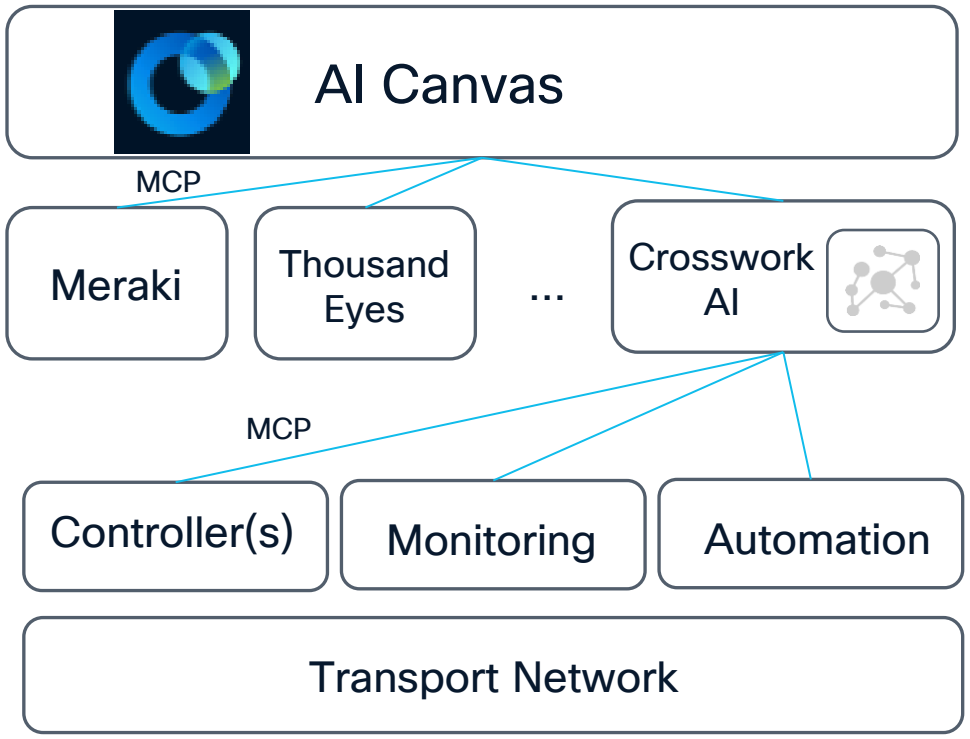
© 2025 Cisco and/or its affiliates. All rights reserved.

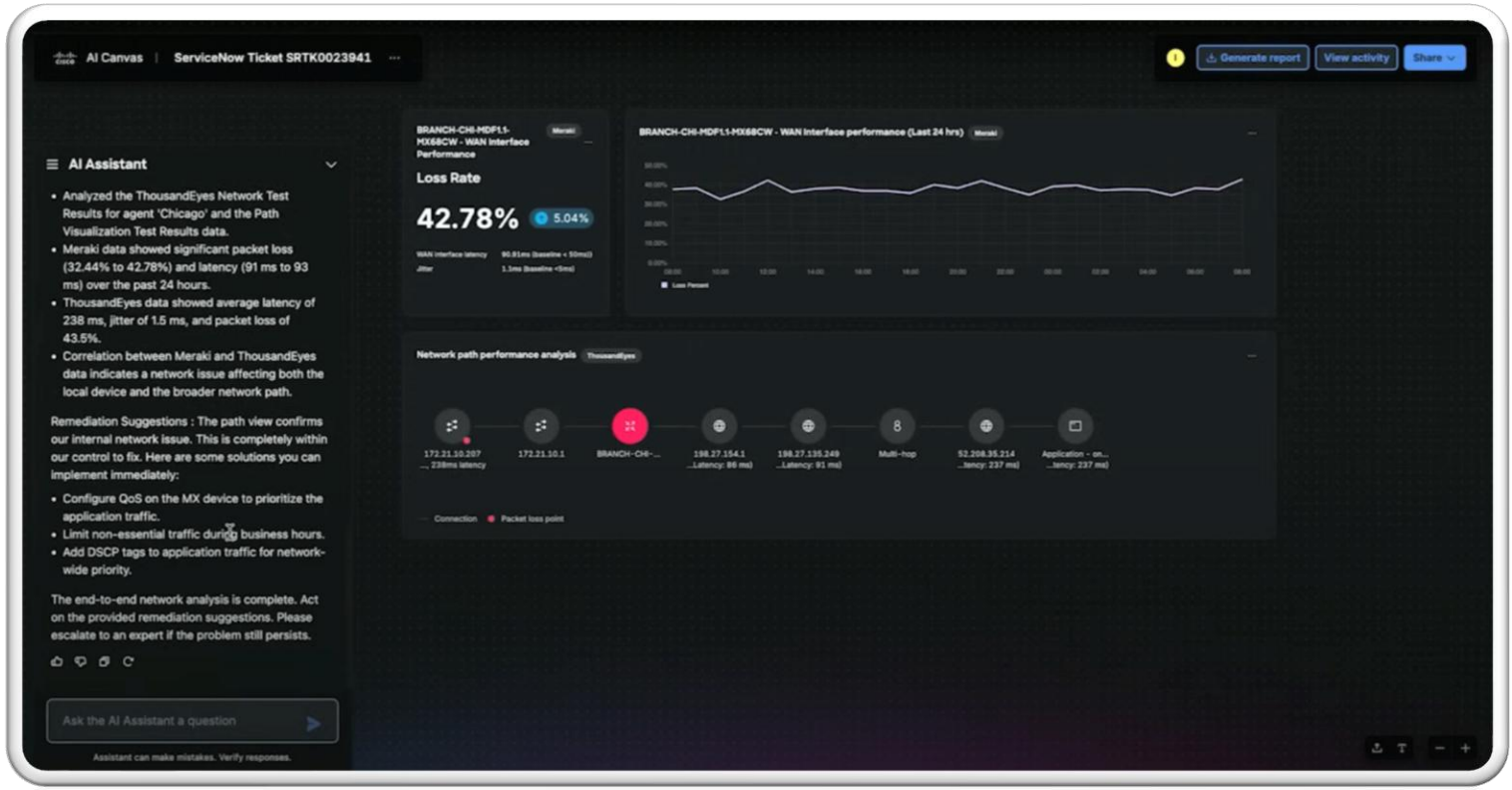
Making Agents Production Ready for Network Automation



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

Cisco AI Canvas





PEOPLE + AI AGENTS + DATA

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

AI Agent Use Cases

Use case	Description	Expected outcome
Toxic Factor Detection	The goal of this use case is to analyze past network events in order to surface patterns that may be influencing negatively the network performance. It uses ML pattern detection algorithms.	Prevent future failures. Increase Mean Time Between Failures (MTBF)
Configuration Drift Detection	Enable a vendor agnostic and template free detection of configuration anomalies by using ML techniques (Configuration Language Models) that learn automatically how a configuration is supposed to be in the customer network	Prevent failures triggered by configuration changes.
Zero-Day Event Correlation	Enable high-quality network event correlation and noise reduction using new techniques such that there is no requirement to implement correlation rules (hence, enabling zero-day correlation even for unseen events)	Operational noise reduction. Improve Mean Time to Detect (MTTD) and Mean Time to Repair/Resolve (MTTR).
AI Automation Developer Agent	Lower the entry barrier for automation artifacts development (yang models, scripts, templates, workflows) by using Agents that can automate the process and automatically generate the required artifacts without requiring the user to have the skills to do this manually	Ease automation adoption (NSO, WFE, CNC). Improve time to value
Network Queries & Reports	AI-Agent focused on replying to complex network queries and reports	Improve MTTD and MTTR
Network Troubleshooting & Root Cause Analysis	Accelerate troubleshooting processes by implementing AI Agents that evaluate different troubleshooting trajectories and autonomously identify the root cause.	Improve MTTR.

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

cisco

AI Agent Use Cases (cont)

Use case		
Brownfield Discovery	Simplify the integration of brownfield infrastructure (devices, configuration, services) by automating the discovery of key entities using AI Agents in a vendor agnostic approach.	Accelerate automation and integration over brownfield.
Compliance & Reporting	Use AI Agents to automate the evaluation of network state against compliance rules. Leverage the flexible nature of Agent based reasoning to accommodate a wide range of compliance and state verification use cases	Improve MTBF and accelerate change management.
Coordinated Maintenance	Use AI to automate and improve the process of large scale maintenance processes such as software upgrades by including verification of impact (what-if) and optimization of scheduling (operational research algorithms for constrained programming)	Prevent maintenance related failures. Increase MTBF
Sustainability Optimization	Use AI mechanisms to identify power consumption hot-spots and provide recommendations on how to improve it by: network design, configuration change, etc.	OPEX optimization
Failure Prediction	Use AI mechanisms to help predict certain type of failures. First candidates are optical transceivers, fiber optics.	Prevent failure impact. Increase MTBF.
Design / Operational / Configuration Recommendations	Using data collected across customers and our Cisco internal knowledge base, automatically generate recommendations that will help customers in design / operational and configuration decisions.	Accelerate decisions and improve decision quality. Prevent network failures by aligning with best practices learned from data.

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

use case

Toxic Factor Identification

description

Detection risk factors that may be influencing negatively the performance of the network

from automation

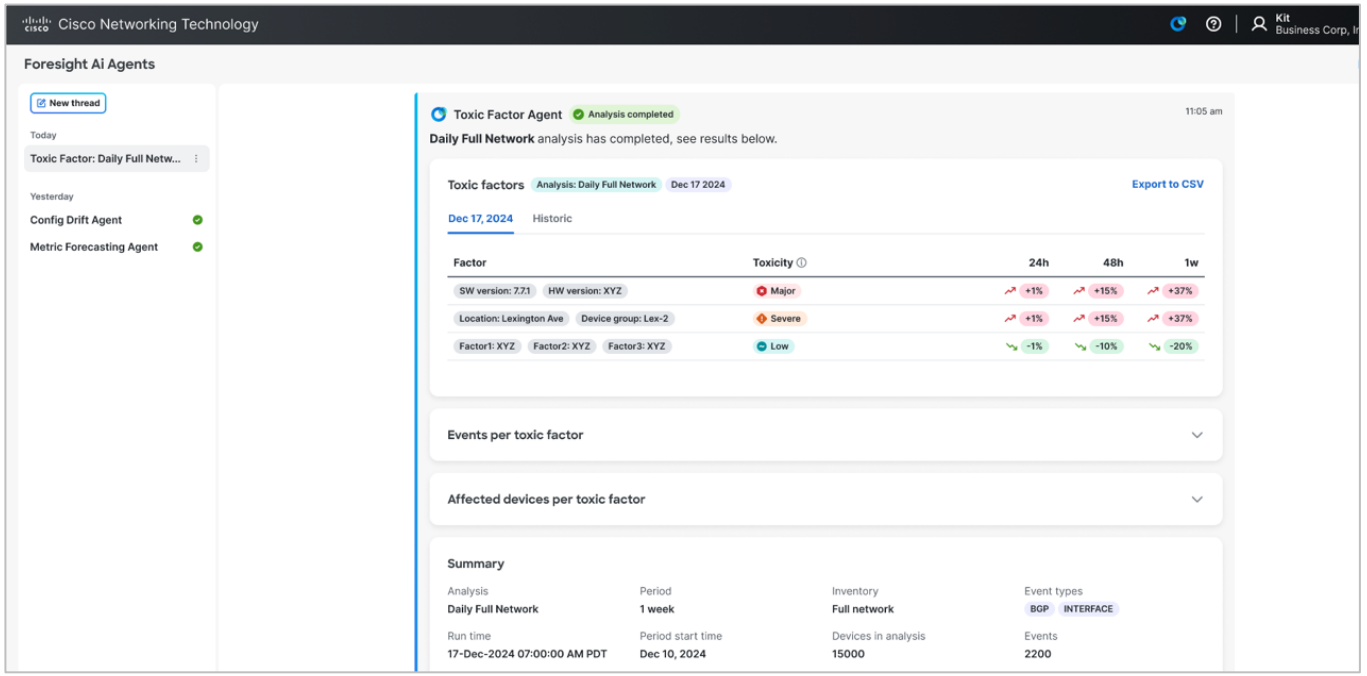
Manually analyze the impact of specific factors such as a certain software release or hardware in network event

to autonomy

AI Frequent Pattern detection algorithms are used to autonomously identify any combination of factors that have a negative impact in the occurrence of network failures

outcomes & benefits

- No need for manual analysis for each factor.
- Multivendor by architecture.
- Prevention of network failures due to identification of risk factors associated.
- Identification of unknown unknowns.
- Improved MTBF.



availability

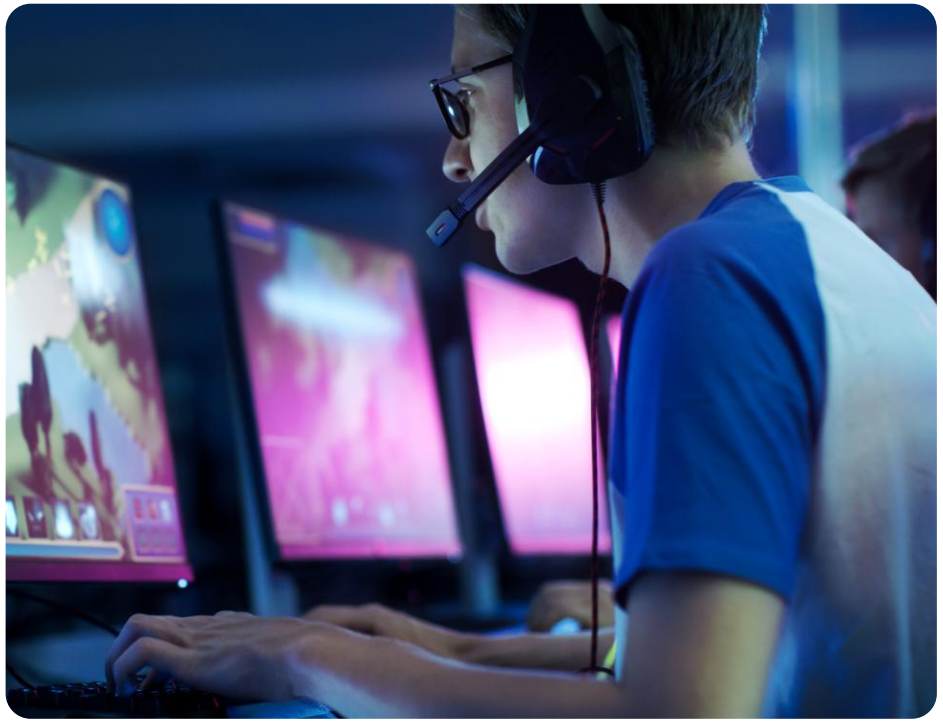
Q4 CY25

compatibility

- Crosswork Multi-Agent Platform
- Crosswork Network Controller 7.2

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

Two tmforum Catalyst use cases



Game X: Elevating Customer Experience via Self-Governed Converged Networks

Champions

colt

Türk Telekom

Telefónica

stc

verizon

Participants

aws

cognizant

cisco

Ni2

ETIYA

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

cisco

1

Industry blueprint and application

4

Network domains

5

Open APIs

11

High value use cases

15

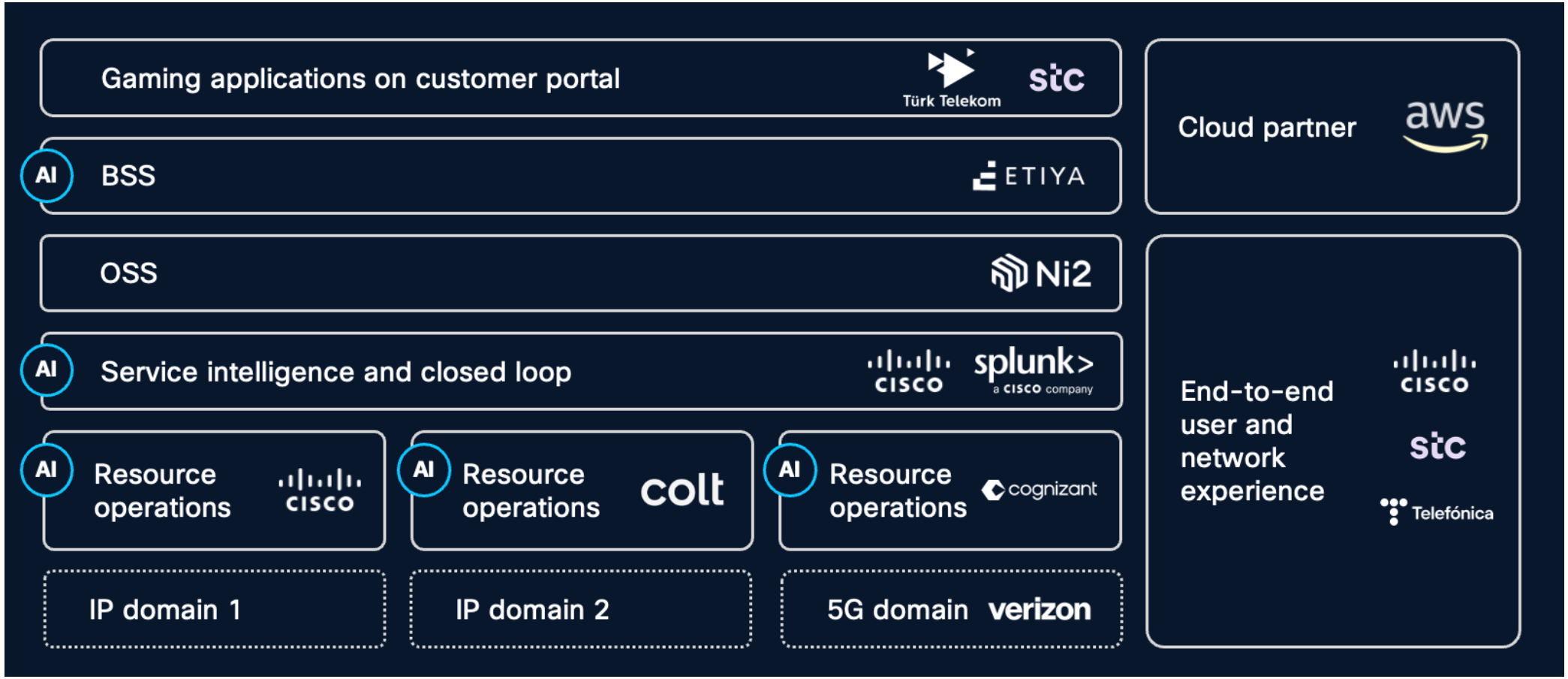
AI agents

32

People collaborating

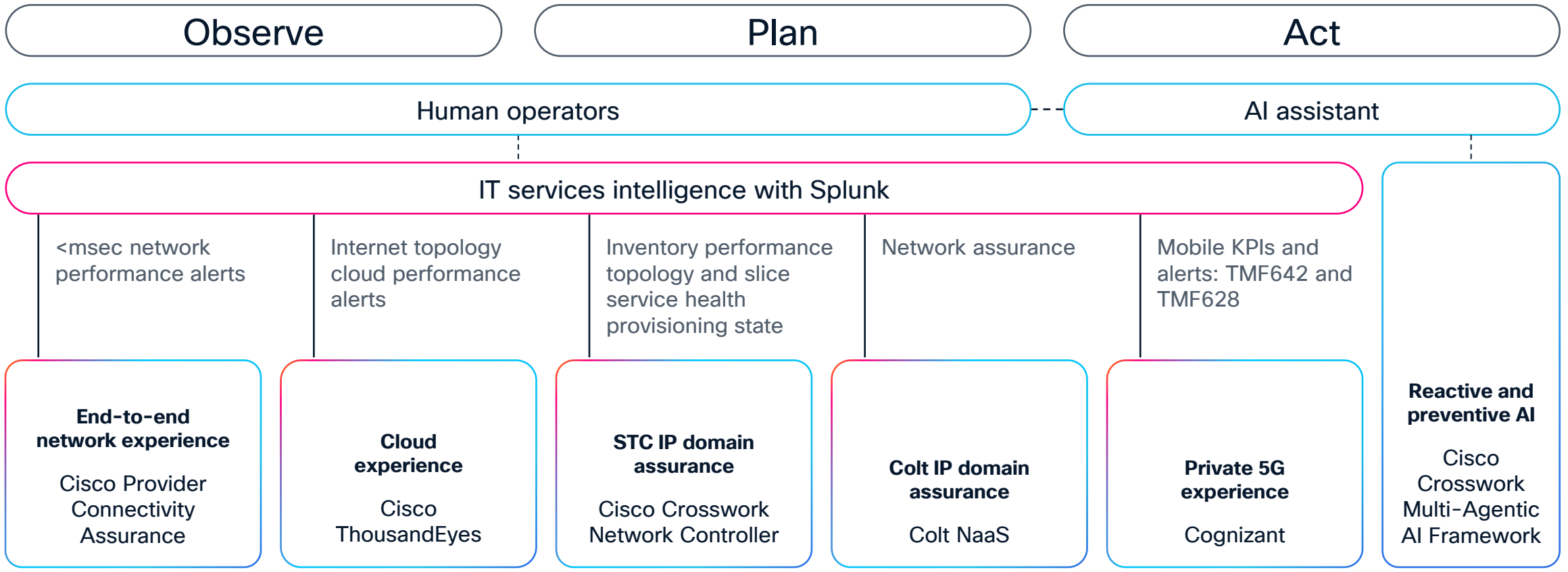
© 2025 Cisco and/or its affiliates. All rights reserved.

TM Forum Catalyst ecosystem and collaboration to enable autonomous networking Level 4



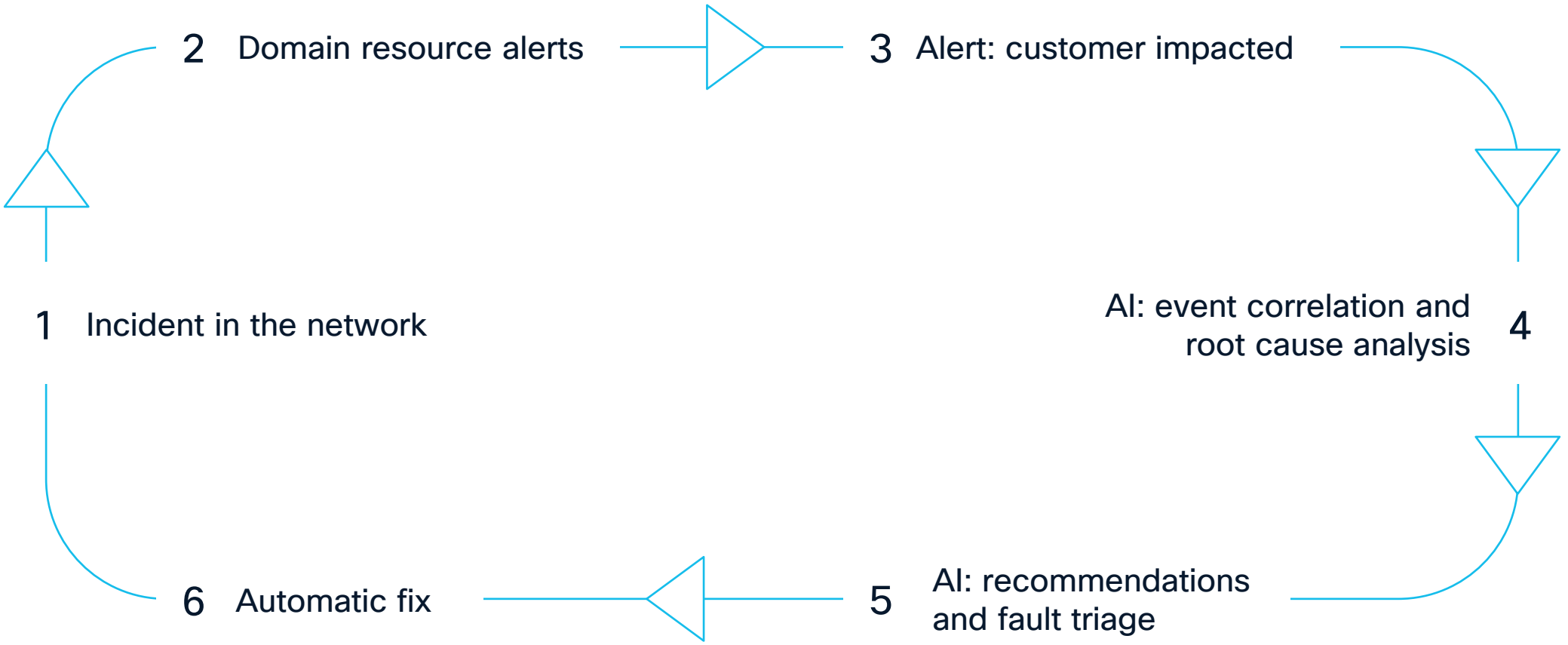
© 2025 Cisco and/or its affiliates. All rights reserved.

One Cisco story in action



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

Demo in a real network

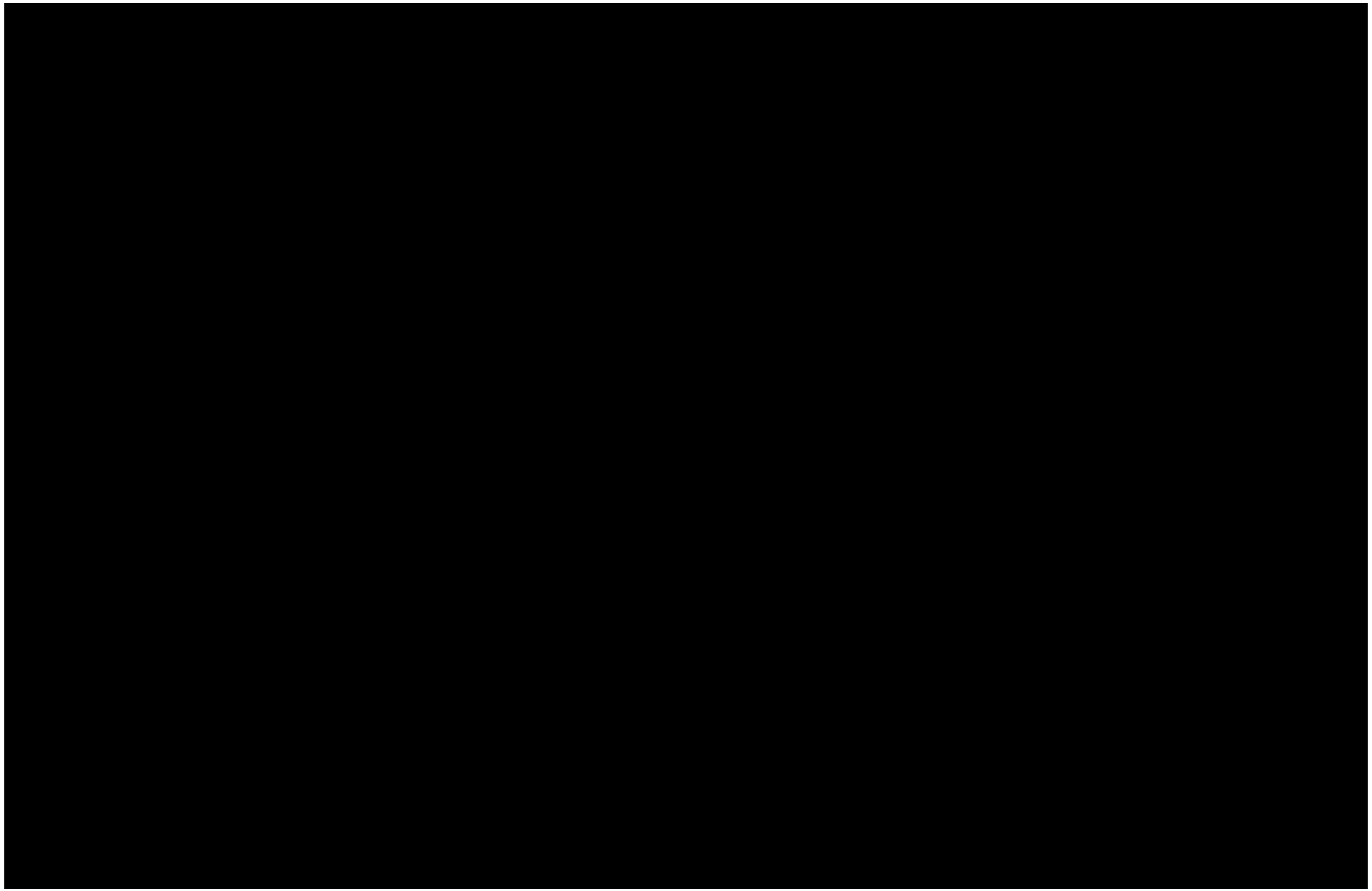


© 2025 Cisco and/or its affiliates. All rights reserved.

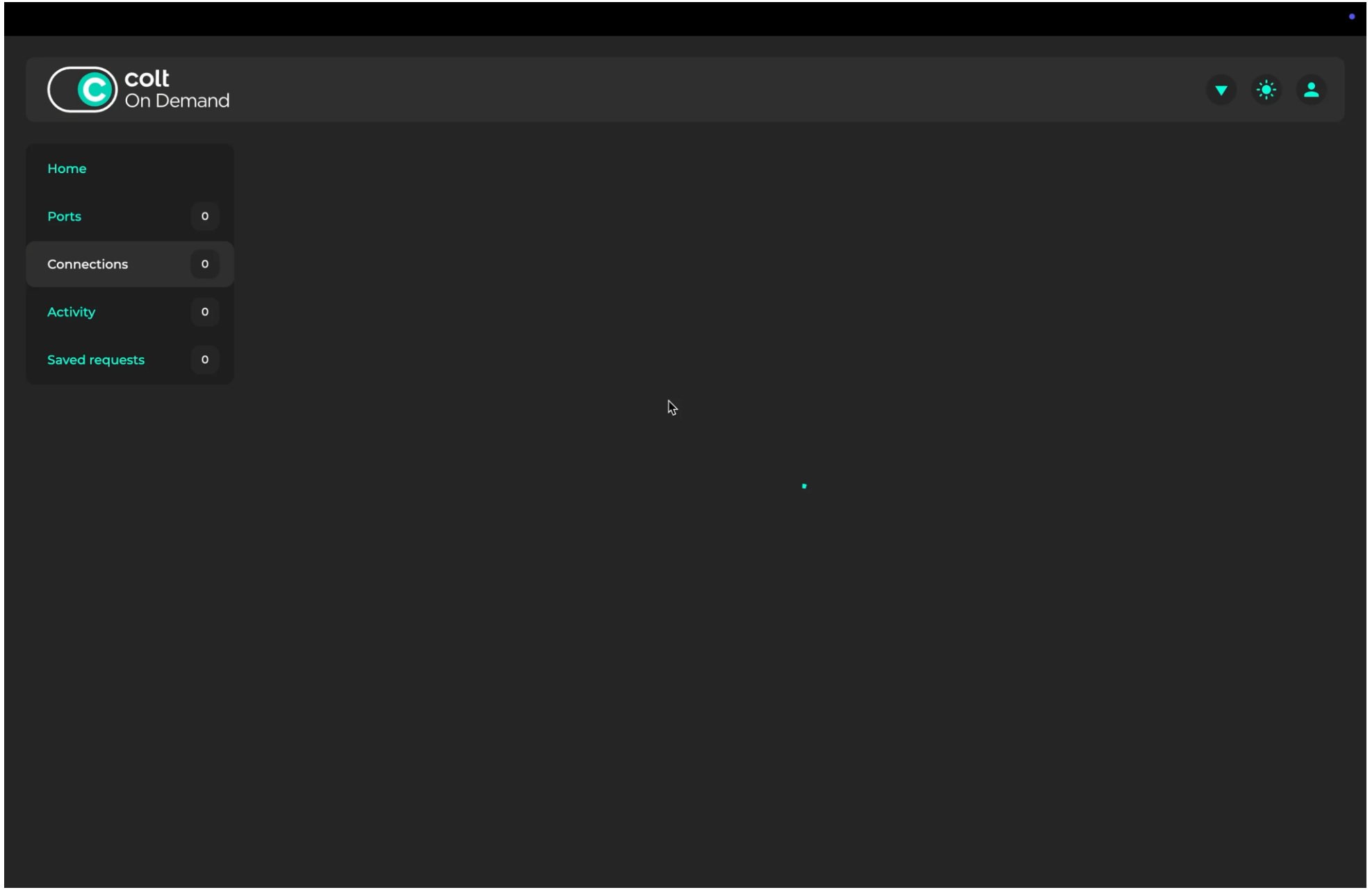
AI Enabled operations

Cisco Automation and Assurance Update

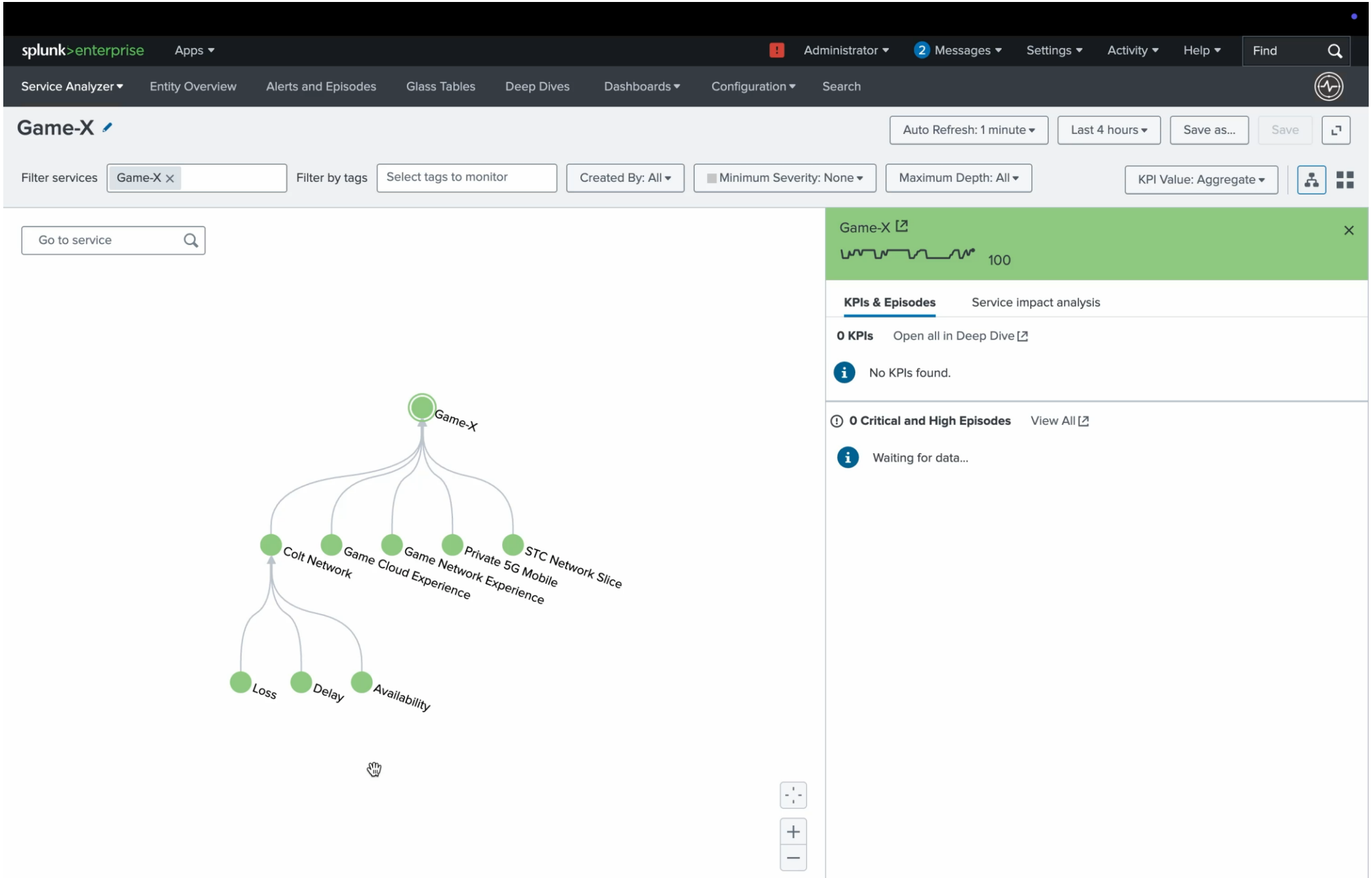
CISCO Live !



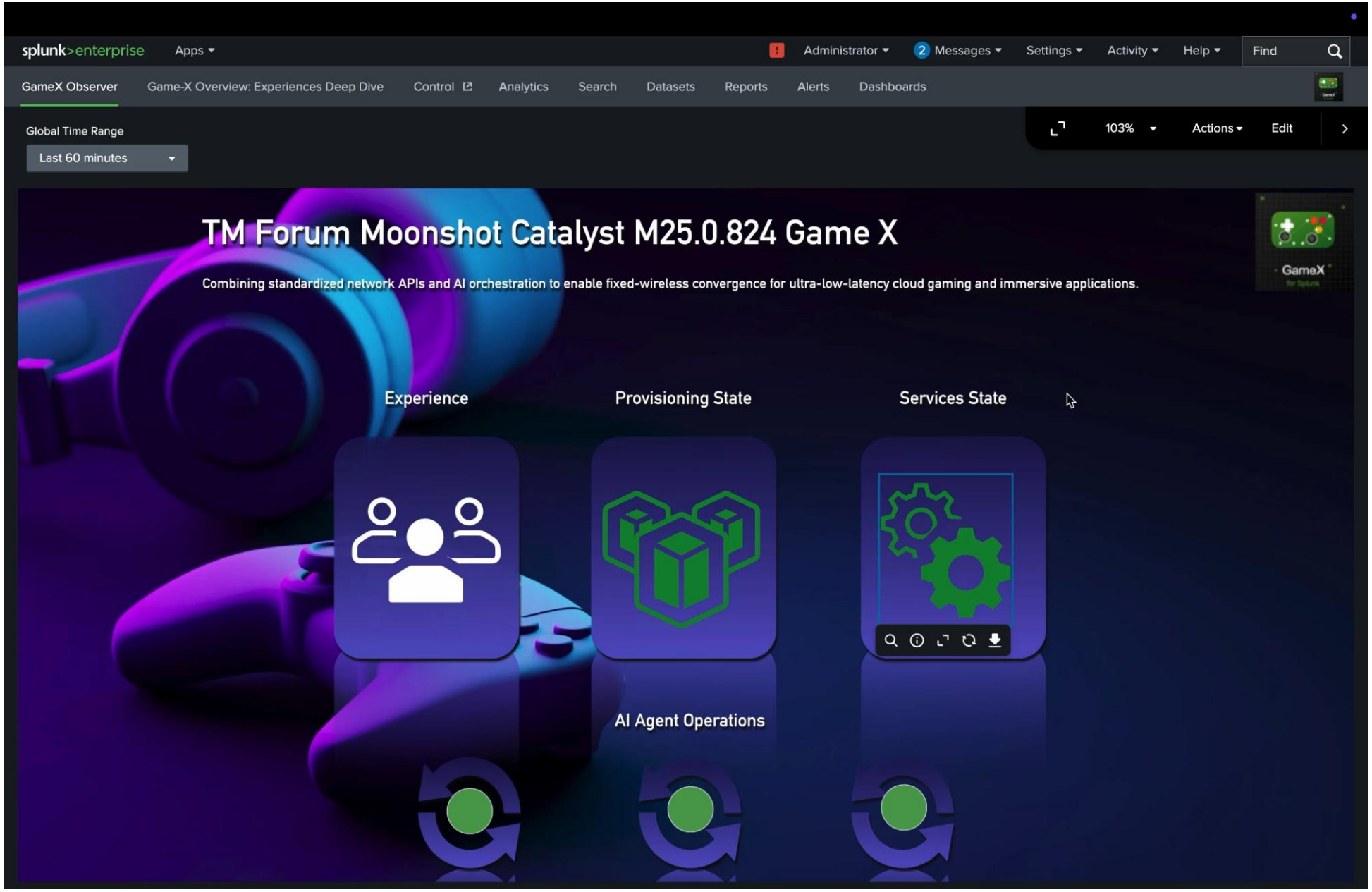
© 2025 Cisco and/or its affiliates. All rights reserved.



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



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



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

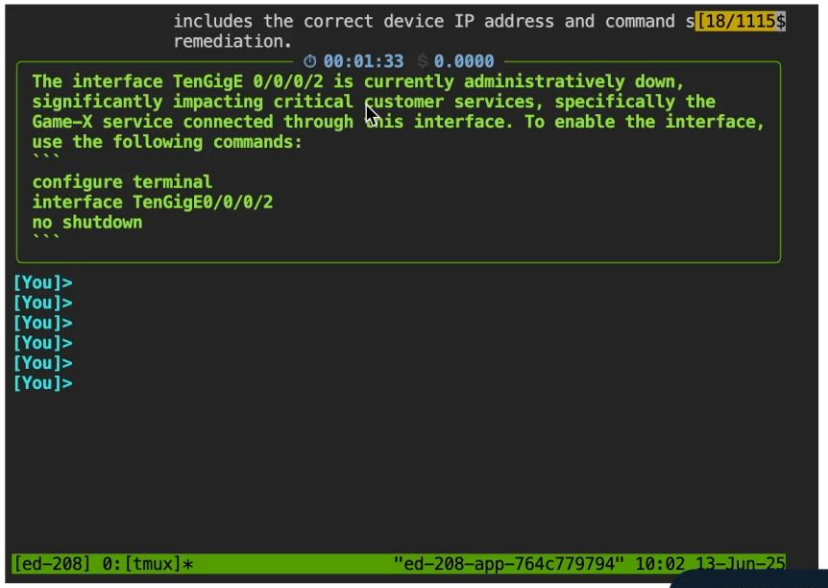
Fault	Frequency	Days	Total	Impacted Systems
AAA BADSERVERTYPEERROR	5	30	90	81%
IP DUPADDR	2	2	4	25%
OSPF FLOOD WAR	90	180	3000	41%
INVALIDKEY OSPF	20	40	300	62%
NACM_INIT	4	7	40	36%

Name	Employee ID
Lester William 24 minutes ago	#34899
Gabriella Fletcher 3 hours ago	#34859
Marcia Banks 9 hours ago	#348499
Irina Garcia 17 hours ago	#348149
Javier Griffin 1 day ago	#348125

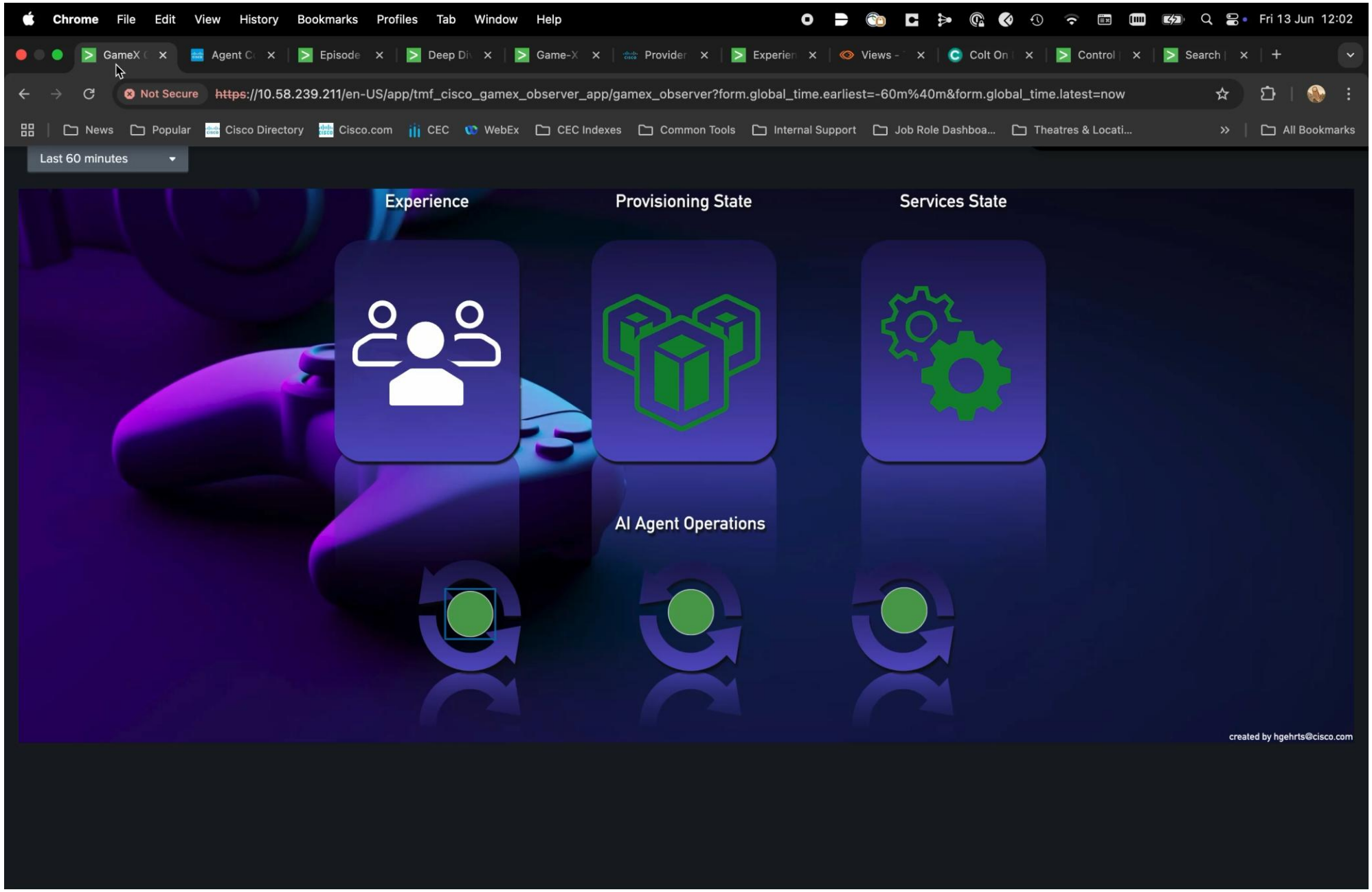
TACACS COMMUNICATION

```
Tacacs Communication:
Connected to the server.
```

ENGAGE MODEL



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



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

Cisco Details ‘Salt Typhoon’ Network Hopping Credential Theft Tactics

Cisco Talos observed Chinese hackers pivoting from a compromised device operated by one telecom to target a device in another telecom.

...

The research team also noted the extensive use of LOTL techniques, piggybacking on built-in networking features rather than deploying traditional malware. The attackers modified router configurations, altered authentication settings, and used guest shell environments on Cisco Nexus devices to execute commands stealthily.

...

Source; https://www.securityweek.com/cisco-details-salt-typhoon-network-hopping-credential-theft-tactics/

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

Before the attack...

router configuration

```
81   feature tacacs+ vrf management
82   tacacs-server login host 10.15.1.10 vrf management seq-num 1 key 7 0x960c890aa72610d6aca0 port 1623
83   tacacs-server login host 10.15.1.15 vrf management seq-num 2 key 7 0x960c890a272610d6aca0 port 1623
84   aaa local authentication unlock-timeout 1
85   aaa authentication login default vrf management group tacacs+ local
86   snmp-server enable snmp vrf management
87   snmp-server view all .1 included vrf management
88   snmp-server community test group network-operator vrf management
89   snmp-server host 10.15.1.12 traps version 2c test udp-port 162 vrf management
90   snmp-server host 10.15.1.13 traps version 2c test udp-port 162 vrf management
91   feature ntp vrf management
92   ntp enable vrf management
93   ntp server 10.15.1.14 vrf management
94   username admin role network-admin password encrypted $1hde642ysfh5eyw3
95   no username ios
96   feature rsyslog vrf management
97   logging server 10.15.1.15 5 facility local0 vrf management
98   !
```

All authentication configuration settings are defined as expected

After the attack...

router configuration

```
77   no errdisable cause stp-bpdu-guard
78   errdisable link-flap-setting max-flaps 5 time 60
79   no feature telnet vrf management
80   feature ssh vrf management
81   feature tacacs+ vrf management
82   tacacs-server login host 10.15.1.10 vrf management seq-num 1 key 7 0x960c890aa72610d6aca0 port 1623
83   tacacs-server login host 10.15.1.11 vrf management seq-num 2 key 7 0x960c890a272610d6aca0 port 1623
84   aaa local authentication unlock-timeout 1
85   aaa authentication login default vrf management group tacacs+ local
86   snmp-server enable snmp vrf management
87   snmp-server view all .1 included vrf management
88   snmp-server community test group network-operator vrf management
89   snmp-server host 10.15.1.12 traps version 2c test udp-port 162 vrf management
90   snmp-server host 10.15.1.13 traps version 2c test udp-port 162 vrf management
91   feature ntp vrf management
92   ntp enable vrf management
93   ntp server 10.15.1.14 vrf management
94   username admin role network-admin password encrypted $1hde642ysfh5eyw3
95   username admin2 role network-admin password encrypted $1hdsgsdfhfdghw4
96   no username ios
97   feature rsyslog vrf management
98   logging server 10.15.1.15 5 facility local0 vrf management
99   !
```

Authentication configuration was ’silently’ changed. A new user is configured.

Access compromised, attackers can potentially jump across devices.

If the change goes ‘unnoticed’ it may stay for days, weeks or months.

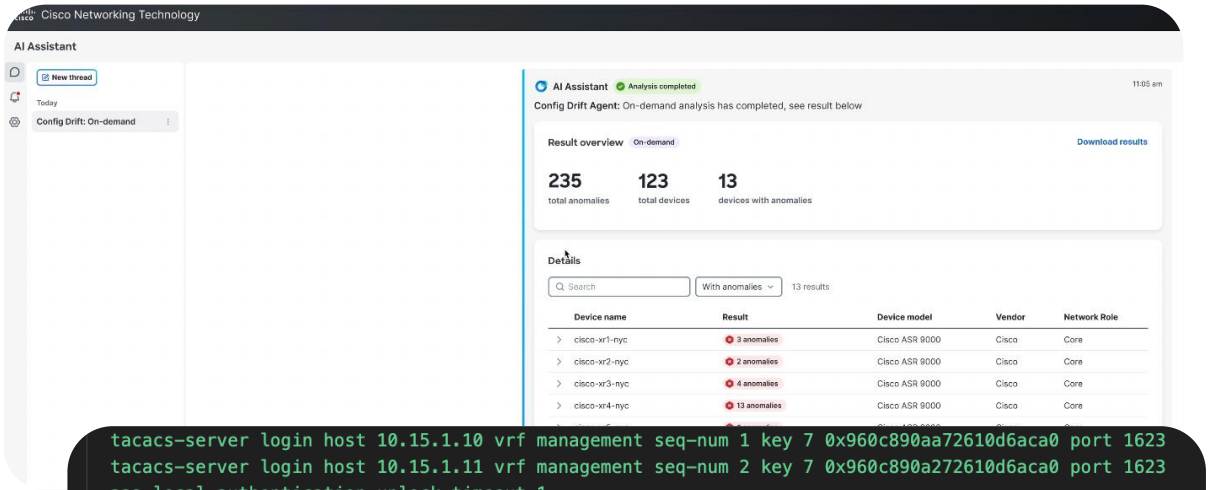
© 2025 Cisco and/or its affiliates. All rights reserved.

With configuration drift detection AI Agent, integrated with Cisco AI Assistant

router configuration

```
77  no errdisable cause stp-bpdu-guard
78  errdisable link-flap-setting max-flaps 5 time 60
79  no feature telnet vrf management
80  feature ssh vrf management
81  feature tacacs+ vrf management
82  tacacs-server login host 10.15.1.10 vrf management seq-num 1 key 7 0x960c890aa72610d6aca0 port 1623
83  tacacs-server login host 10.15.1.11 vrf management seq-num 2 key 7 0x960c890a272610d6aca0 port 1623
84  aaa local authentication unlock-timeout 1
85  aaa authentication login default vrf management group tacacs+ local
86  snmp-server enable snmp vrf management
87  snmp-server view all .1 included vrf management
88  snmp-server community test group network-operator vrf management
89  snmp-server host 10.15.1.12 traps version 2c test udp-port 162 vrf management
90  snmp-server host 10.15.1.13 traps version 2c test udp-port 162 vrf management
91  feature ntp vrf management
92  ntp enable vrf management
93  ntp server 10.15.1.14 vrf management
94  username admin role network-admin password encrypted $1hde642ysfh5eyw3
95  username admin2 role network-admin password encrypted $1hdsgsdfhfdghw4
96  no username ios
97  feature rsyslog vrf management
98  logging server 10.15.1.15 5 facility local0 vrf management
99  !
```

Config drift AI Agent




```
tacacs-server login host 10.15.1.10 vrf management seq-num 1 key 7 0x960c890aa72610d6aca0 port 1623
tacacs-server login host 10.15.1.11 vrf management seq-num 2 key 7 0x960c890a272610d6aca0 port 1623
aaa local authentication unlock-timeout 1
aaa authentication login default vrf management group tacacs+ local
snmp-server enable snmp vrf management
snmp-server view all .1 included vrf management
snmp-server community test group network-operator vrf management
snmp-server host 10.15.1.12 traps version 2c test udp-port 162 vrf management
snmp-server host 10.15.1.13 traps version 2c test udp-port 162 vrf management
feature ntp vrf management
ntp enable vrf management
ntp server 10.15.1.14 vrf management
username admin role network-admin password encrypted $1hde642ysfh5eyw3
username admin2 role network-admin password encrypted $1hdsgsdfhfdghw4
(remove)
no username ios
feature rsyslog vrf management
logging server 10.15.1.15 5 facility local0 vrf management
!
```

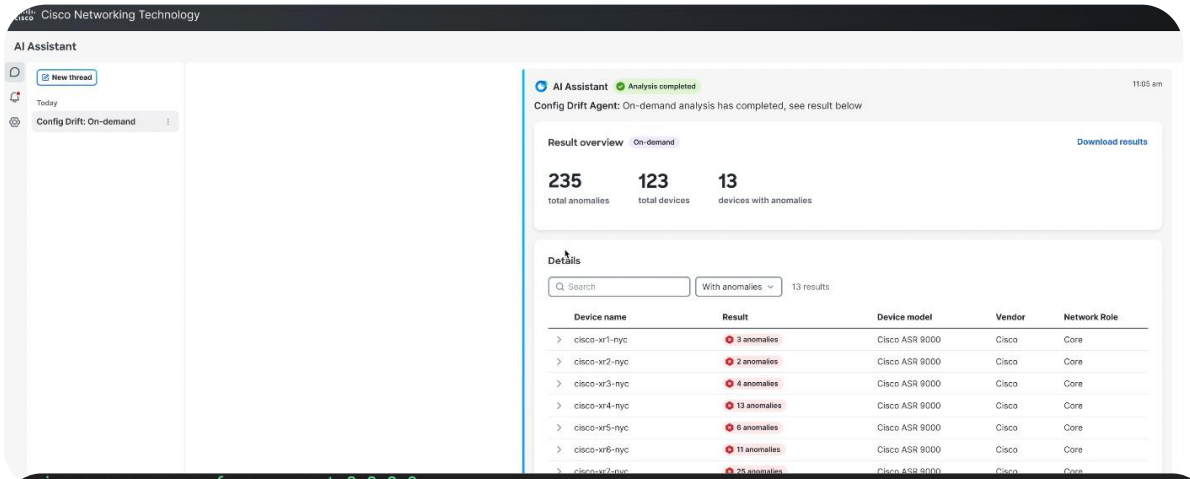
© 2025 Cisco and/or its affiliates. All rights reserved.

With configuration drift detection AI Agent, integrated with Cisco AI Assistant

router configuration

```
no feature telnet vrf management
feature ssh vrf management
feature tacacs+ vrf management
tacacs-server login host 10.15.1.10 vrf management seq-num 1 key 7 0x960c890aa72610d6aca0 port 1623
tacacs-server login host 10.15.1.12 vrf management seq-num 2 key 7 0x960c890a272610d6aca0 port 1623
aaa local authentication unlock-timeout 1
aaa authentication login default vrf management group tacacs+ local
snmp-server enable snmp vrf management
snmp-server view all .1 included vrf management
snmp-server community test group network-operator vrf management
snmp-server host 10.15.1.12 traps version 2c test udp-port 162 vrf management
snmp-server host 10.15.1.13 traps version 2c test udp-port 162 vrf management
feature ntp vrf management
ntp enable vrf management
ntp server 10.15.1.14 vrf management
username admin role network-admin password encrypted $1hde642ysfh5eyw3
no username ios
feature rsyslog vrf management
logging server 10.15.1.15 5 facility local0 vrf management
!
```

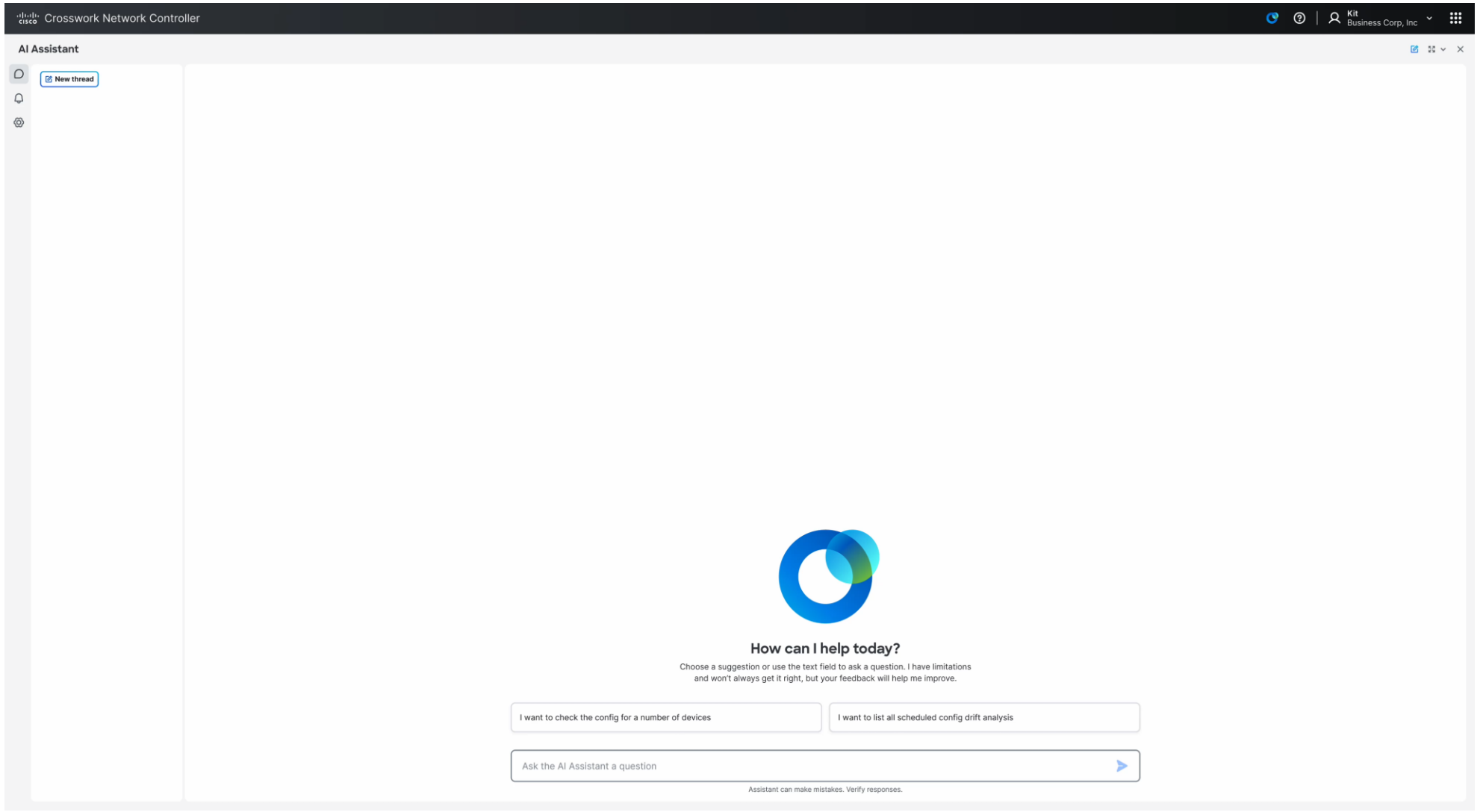
Config drift AI Agent




```
ip name-server vrf management 8.8.8.9
errdisable cause link-flap
no errdisable cause stp-bpdu-guard
errdisable link-flap-setting max-flaps 5 time 60
no feature telnet vrf management
feature ssh vrf management
feature tacacs+ vrf management
tacacs-server login host 10.15.1.10 vrf management seq-num 1 key 7 0x960c890aa72610d6aca0 port 1623
tacacs-server login host 10.15.1.12 vrf management seq-num 2 key 7 0x960c890a272610d6aca0 port 1623
(replace with tacacs-server login host 10.15.1.11 vrf management seq-num 2 key 7 0x960c890a272610d6aca0 port 1623)
aaa local authentication unlock-timeout 1
aaa authentication login default vrf management group tacacs+ local
snmp-server enable snmp vrf management
snmp-server view all .1 included vrf management
snmp-server community test group network-operator vrf management
snmp-server host 10.15.1.12 traps version 2c test udp-port 162 vrf management
snmp-server host 10.15.1.13 traps version 2c test udp-port 162 vrf management
```

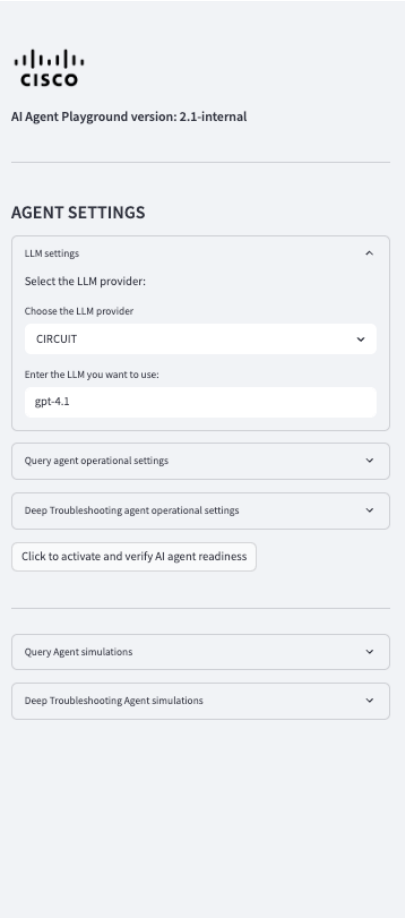
© 2025 Cisco and/or its affiliates. All rights reserved.

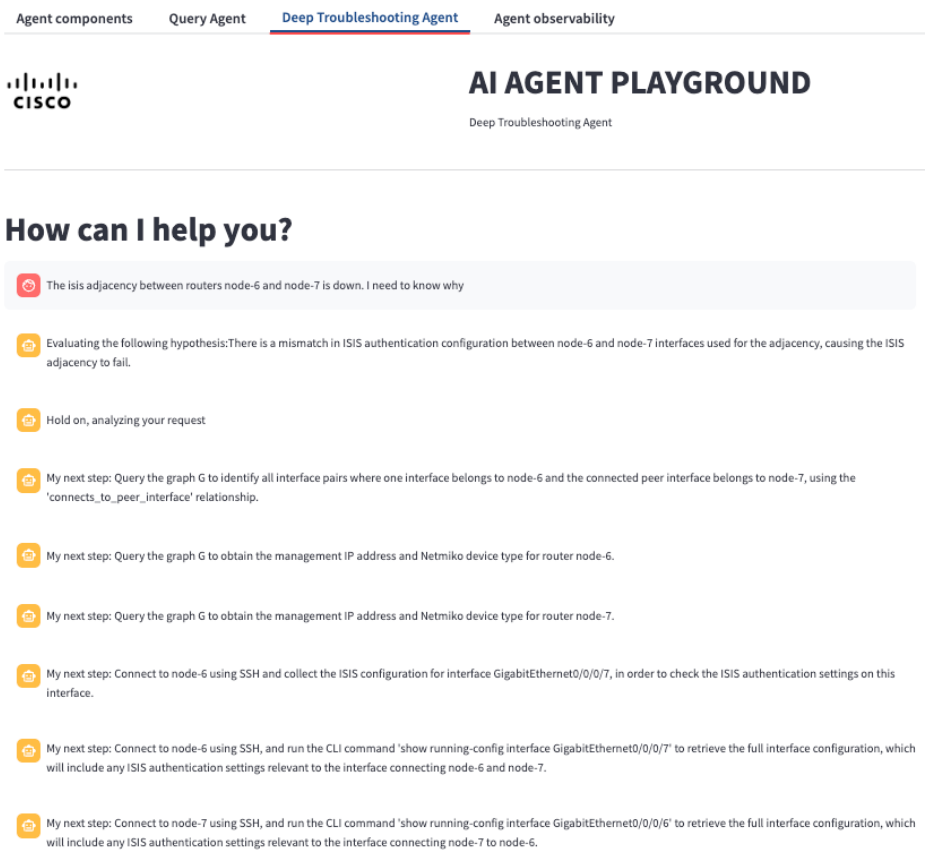
Demo Configuration Drift



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

Agentic Playground Workshop/Lab





- Available at:
  - Automation Developer Days
  - Cisco Live
  - Autoconf
- Planned to be release with Agentic Framework
- Regular workshops with customers using Cisco dcloud virtual labs

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

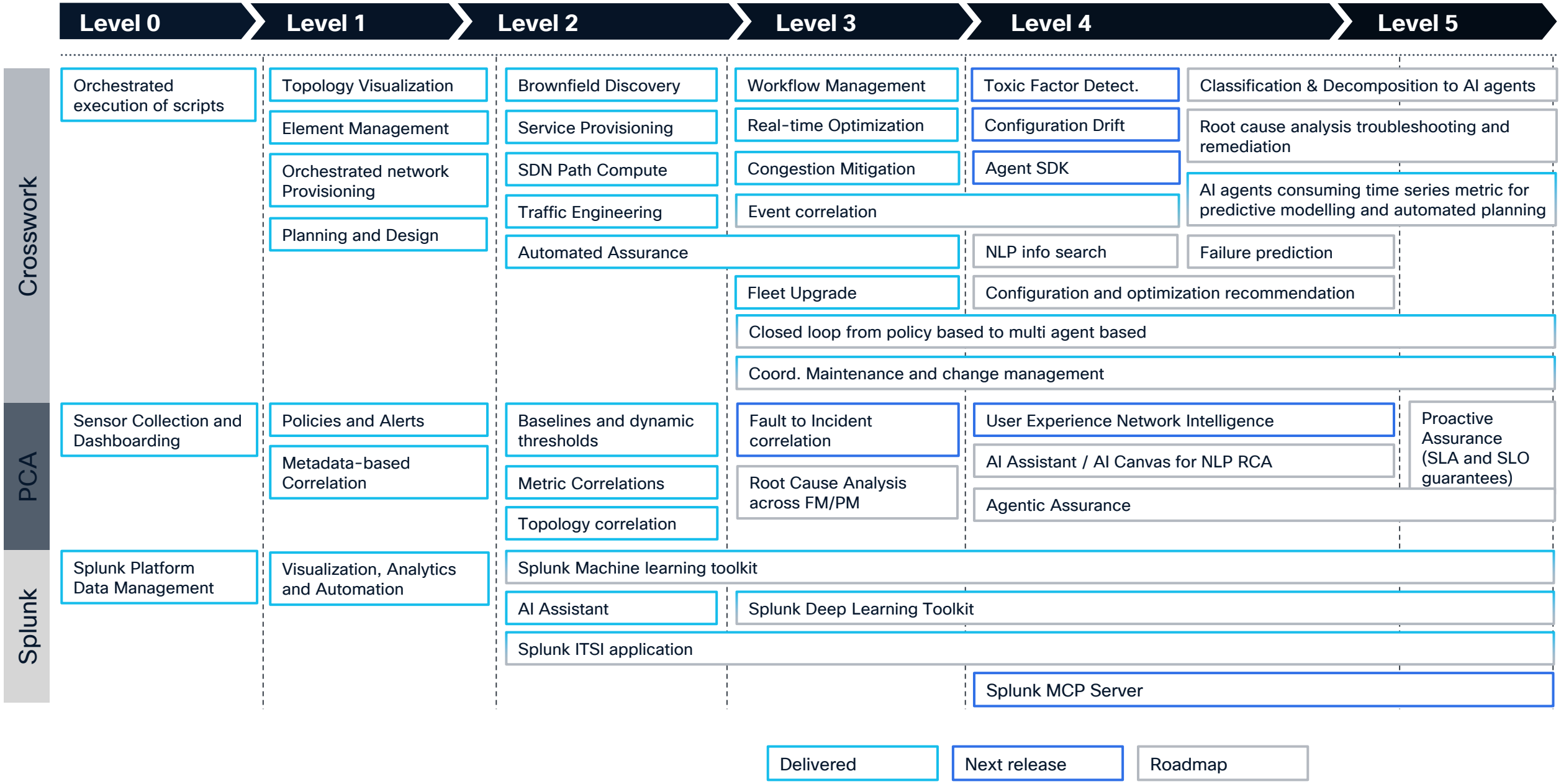
AI Agent Roadmap

	2HCY25	1HCY26	2HCY26	2027
Reactive		• Incident co-pilot.	• Network troubleshooting and root cause analysis • Brownfield discovery.	
Preventive	• Toxic Factor Detector • Configuration Drift Detection	• Noise reduction (Zero-Day Event Correlation)	• Compliance & reporting (Agent based) • Coordinated maintenance • Sustainability optimization • Brownfield discovery	• Failure prediction
Prescriptive		• Automation adoption (AI Automation developer agent)	• Device migration	• Network Design recommendations • Configuration recommendations • Operational recommendations. • Multi-layer optimization
Framework	• Baseline for first two agents		SDK	

Committed Planning Radar NSO CNC

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

cisco



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

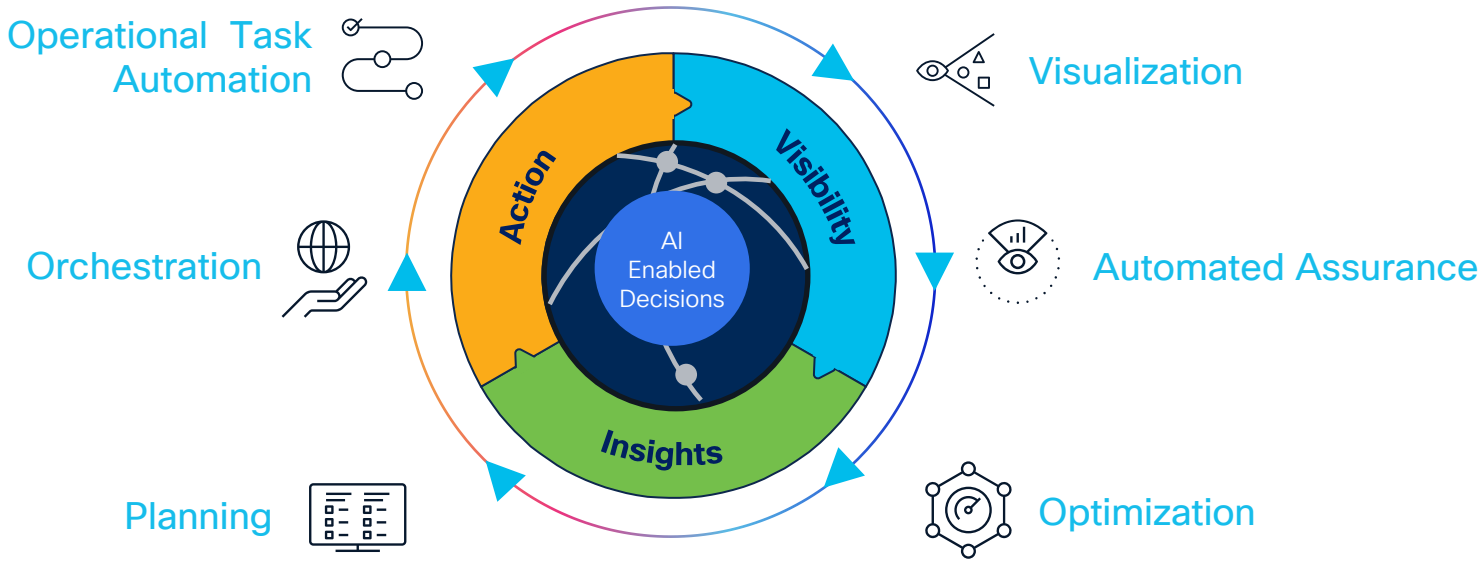
AI Enabled operations

Cisco Automation and Assurance Update

cisco Live !

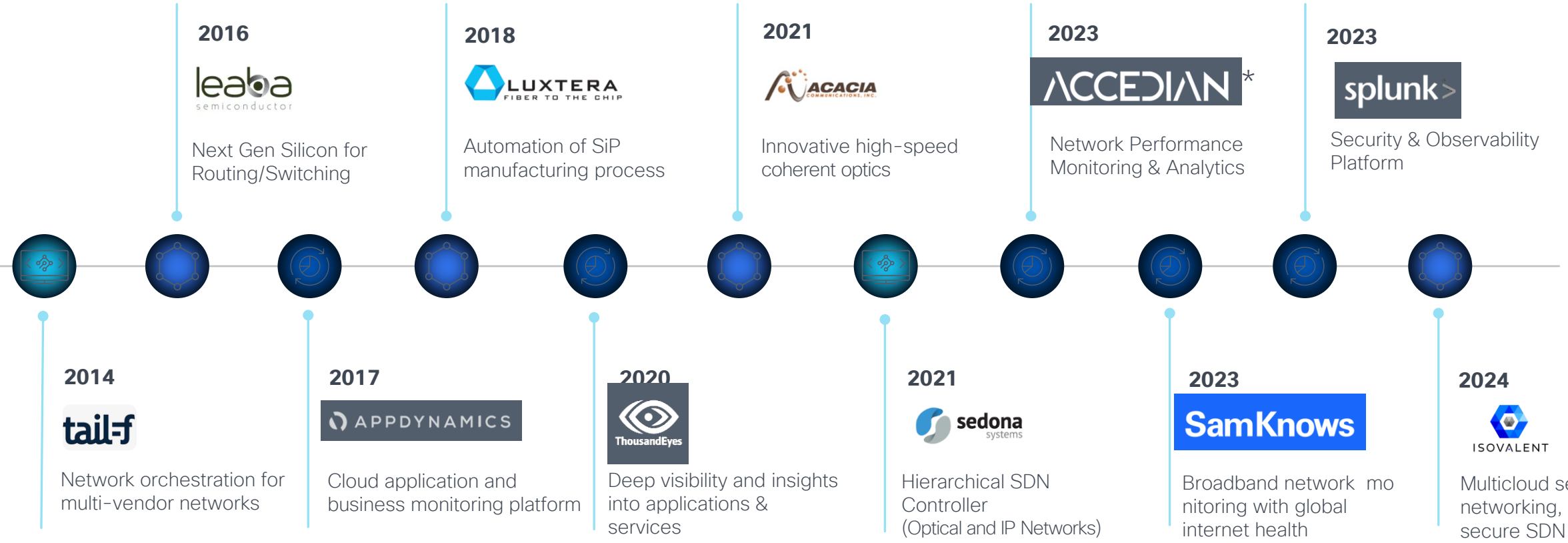
Cisco Automation And Assurance

- Most Comprehensive Functions
- Intent-driven Automation
- Modular, Multi-vendor & Extensible
- Multi-agentic AI
- Low-code/ No-code Experience
- Scalable, Resilient & Secure
- Deep Visibility & Analytics



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

Consistent investment speeding innovation



High-performance sustainable networks

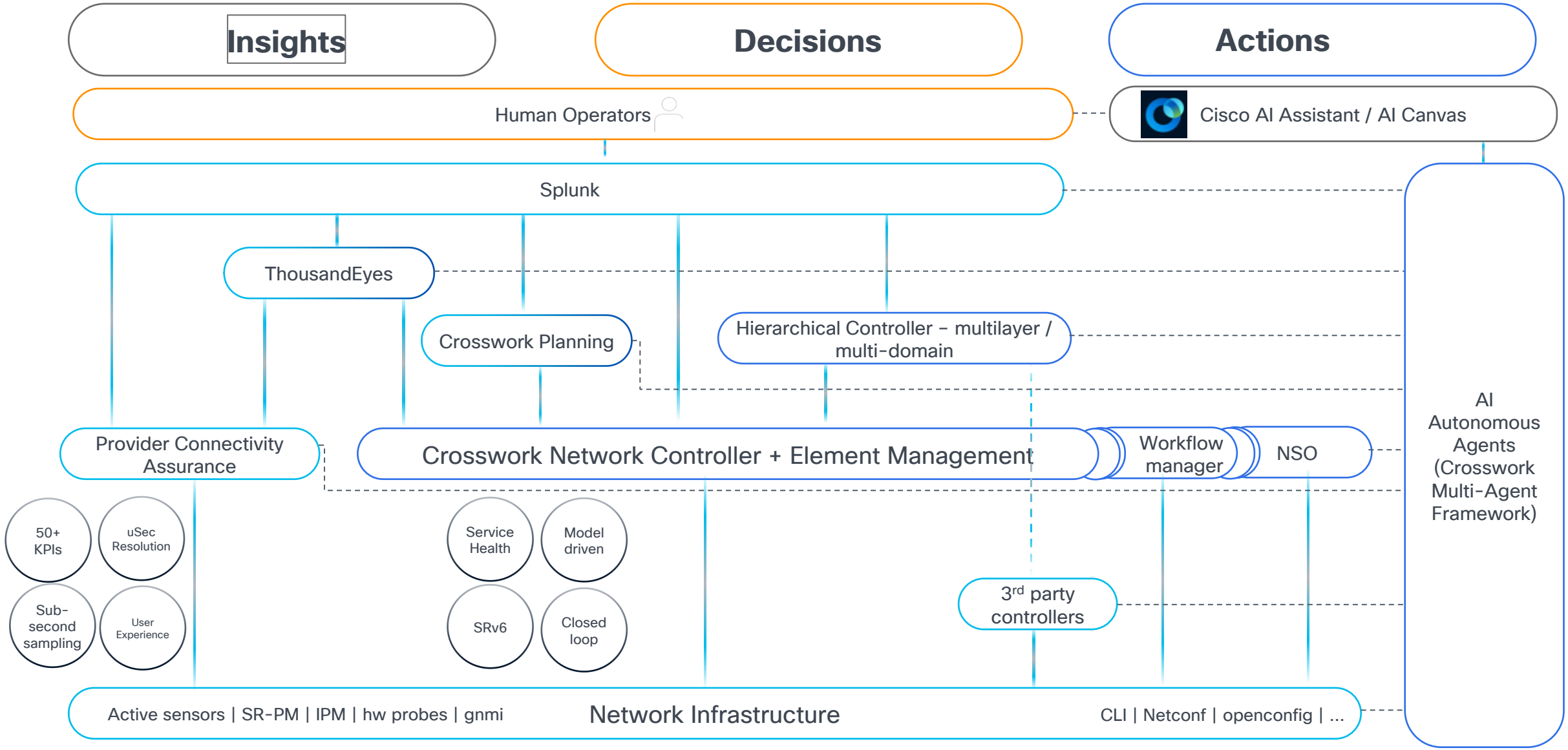
Observability

Orchestration and automation

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

cisco

Towards AI for Operations



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

Introducing Crosswork Planning

Predictive AI

Predict the impact of network changes, traffic growth, new services, and potential failures

Capacity Planning

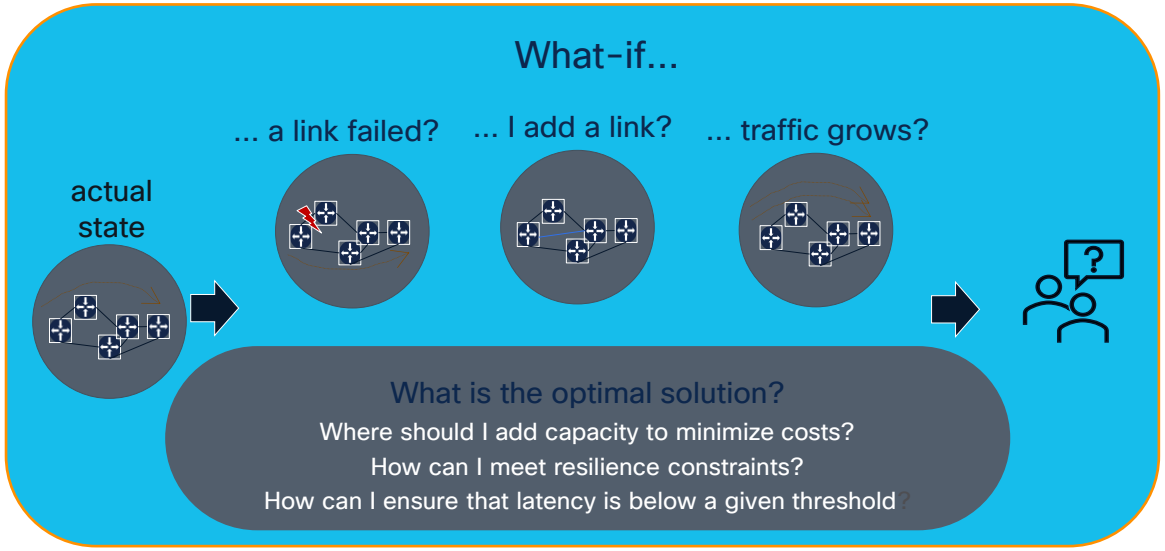
Leverage measured or simulated traffic data for accurate predictions

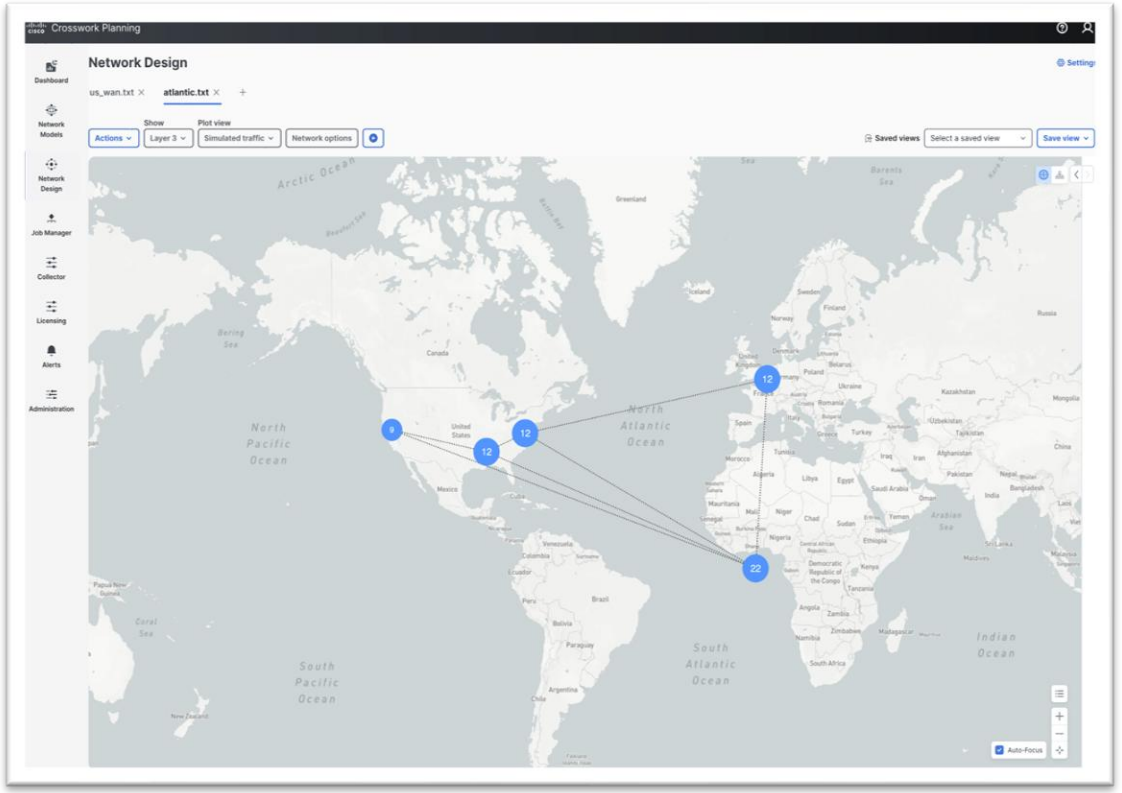
Services Optimization

Optimize network design for efficiency and reliability

Benefits

Reduced operational costs
Improved network performance
Enhanced agility
Proactive planning
Simplified Capacity planning





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

We're Still Pushing Boundaries

Optimistic transactions

9X Performance

Scalable database

3X Scale

Multi-vendor support across protocols

Operational performance

10X Less downtimes

Out-of-band service protection

More use cases, less ups!

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

cisco

Where are customers using Cisco NSO – TOP uses

Wide Area Networks	AI Datacenters/Cloud	Security
• MPLS / SR / SRv6 Networks • All your B2B automation • Could include CPE • Mobile Backhaul • Expand to LAN Area Networks and Datacenter interconnects. • Expand to SD-WAN • Expand to Microwaves • Expand to Optical Services	• DC Fabric automation • Direct device access or via controller • NaaS solutions with security and load-balancing • NFV Orchestration (NFVO and CNFO)*	• Compliance reports • Firewall Management • ACL, IPS, WebFiltering rules • Standalone, as part of DC or Mobile GiLAN

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

AI-Enabled Functionality (Planned / Roadmap)

- NSO will integrate the Agentic AI-ops backend Crosswork AI that we have developed to enable AI-enabled capabilities that align with NSO's areas of focus
- Details of our initial agents follow
- AI Assisted service creation
- MCP server
- Cisco AI Assistant
  - Leverage Crosswork AI use cases
  - Documentation search, sample code search

AI Package wizard: https://www.youtube.com/watch?v=OY8oWcN122E

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

CNC: Service and Device Lifecycle Automation

OSS/BSS and/or Hierarchical Controller

REST/RESTCONF Model-based

Crosswork Network Controller

Operation Automation via Workflow Manager

Multi-vendor Fleet upgrade | Golden Config | Device Onboarding | Programmable closed-loop | Migrations

Service and transport provisioning

- YANG service models
- 170+ multivendor devices supported in addition to Netconf
- L2VPN, L3VPN, SR-TE, SRv6, RSVP-TE, Tree-SID and more
- Programmable to support new services and devices

NSO

Visualization

- Service, network, and device views
- End-to-end dynamic path and policy view
- Traffic engineering dashboard
- Flexible algorithm
- Transport slices and slice catalog
- Inventory, fault, performance

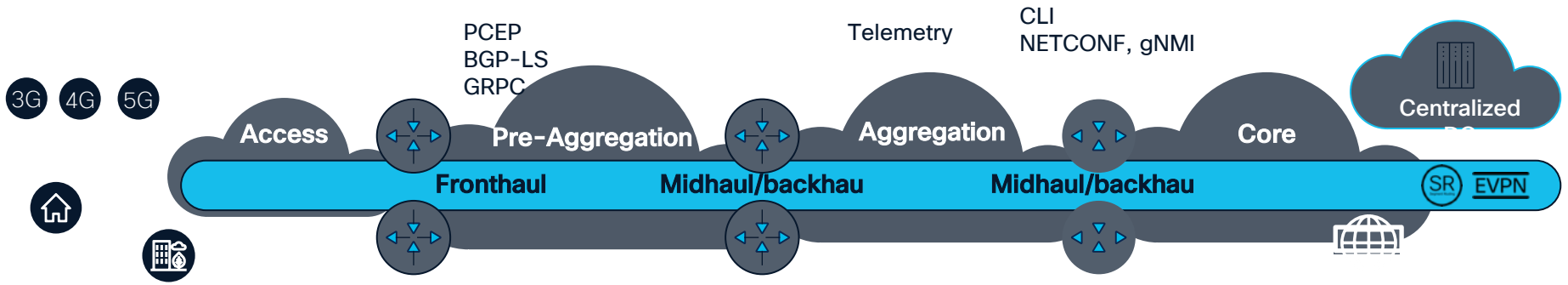
Element management (FCAPS)

Dynamic traffic engineering & path optimization

Service assurance

Embedded probes | External probes

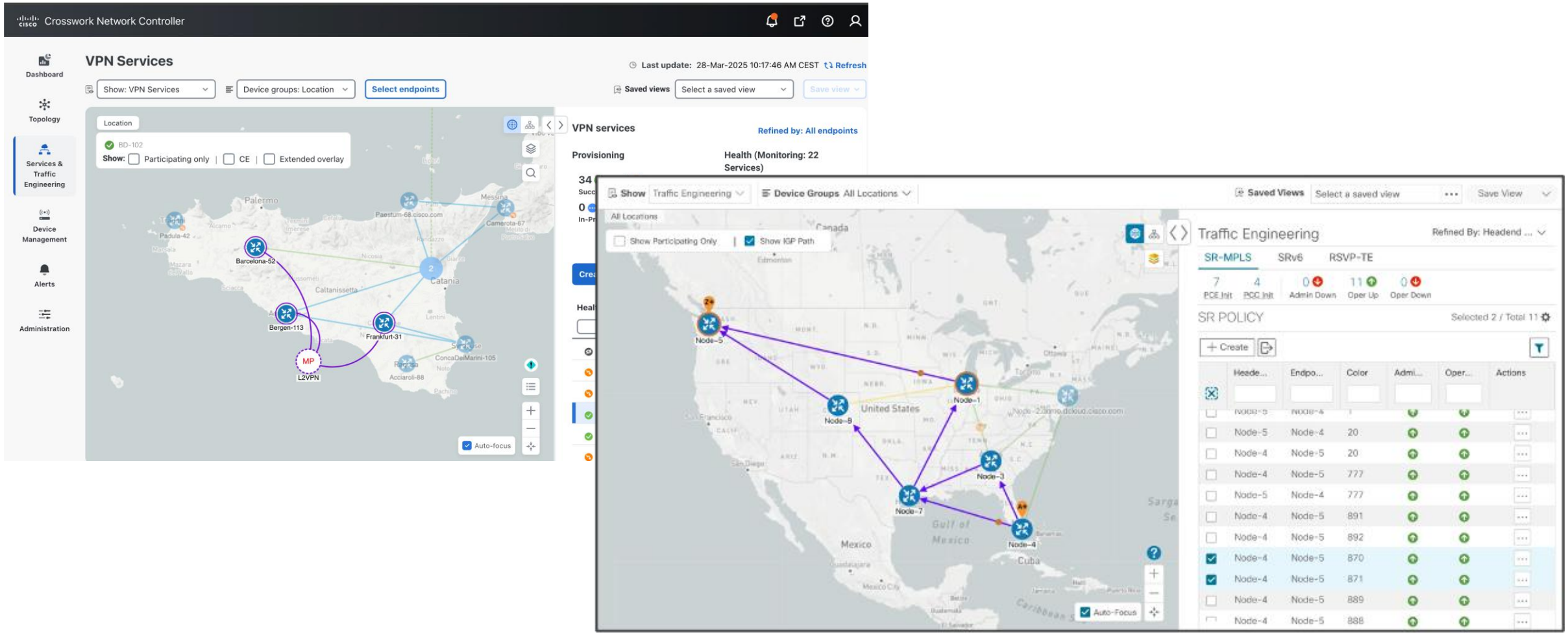
Closed-loop automation



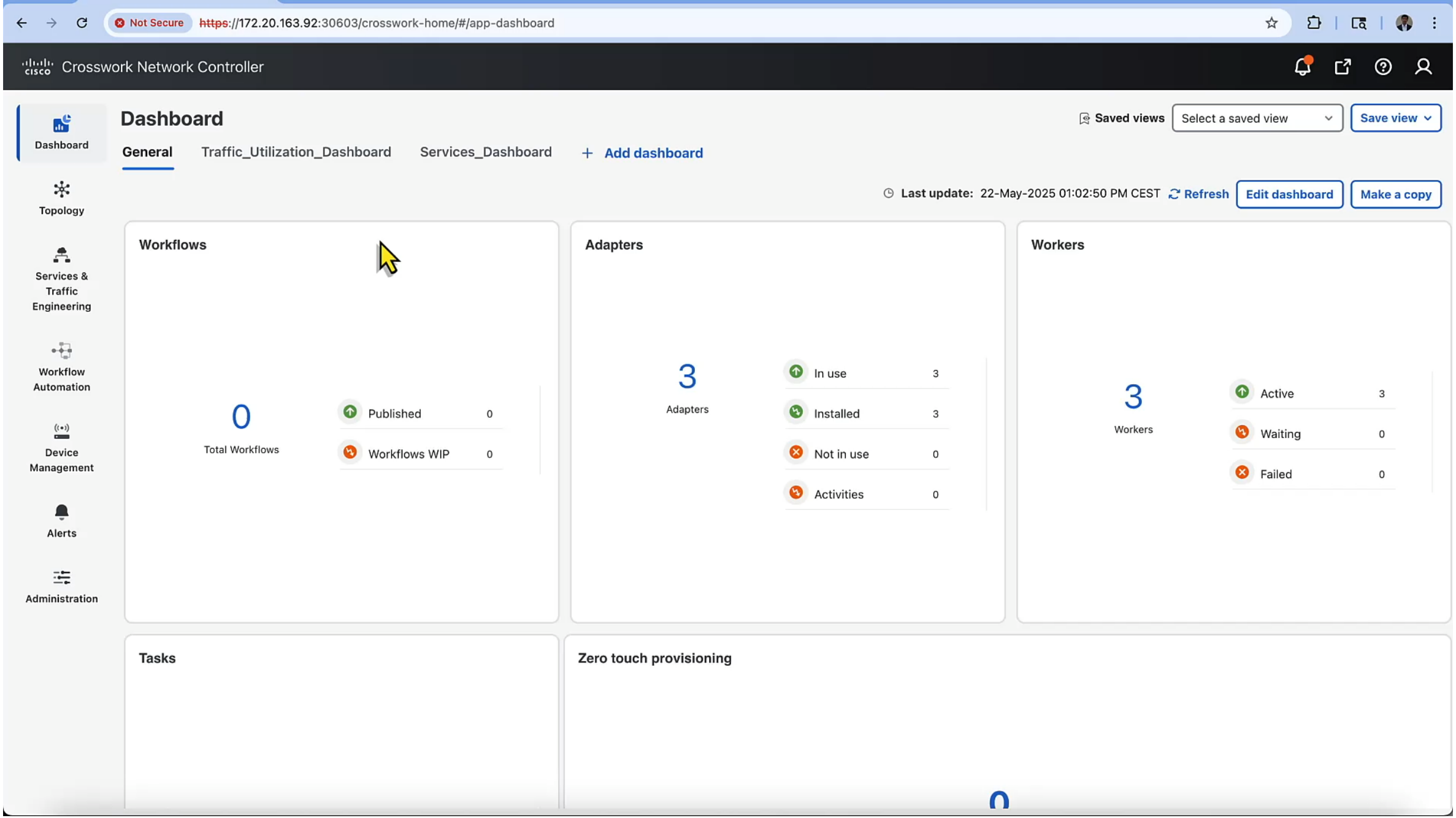
© 2025 Cisco and/or its affiliates. All rights reserved.

CNC: Service Lifecycle Automation

Provisioning, Visualize, Control and Assurance

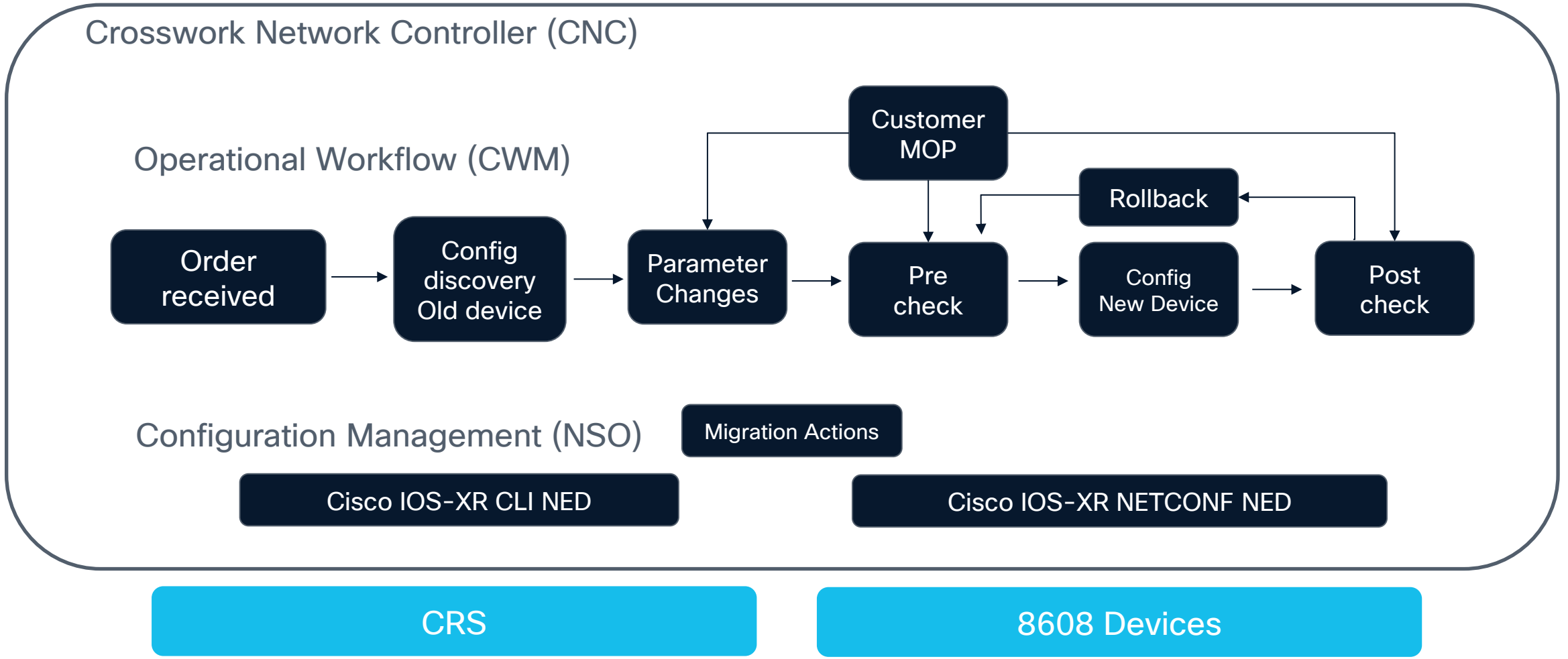


© 2025 Cisco and/or its affiliates. All rights reserved.



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

Migration Process Automation Workflow



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

Provider Connectivity Assurance solution overview

High-level view

Open automation & APIs

Open data & alerts

Cloud-Native Platform: Time series and Events

Management, automation, data collection and data analytics

User Personas & Use Cases

- End customers
- Service managers
- Engineering
- Operations
- Capacity planning
- IT and network

Software Sensor Layer

Containerized & horizontally scalable

Hardware Sensor Layer

With embedded PM

Metrics from other sources

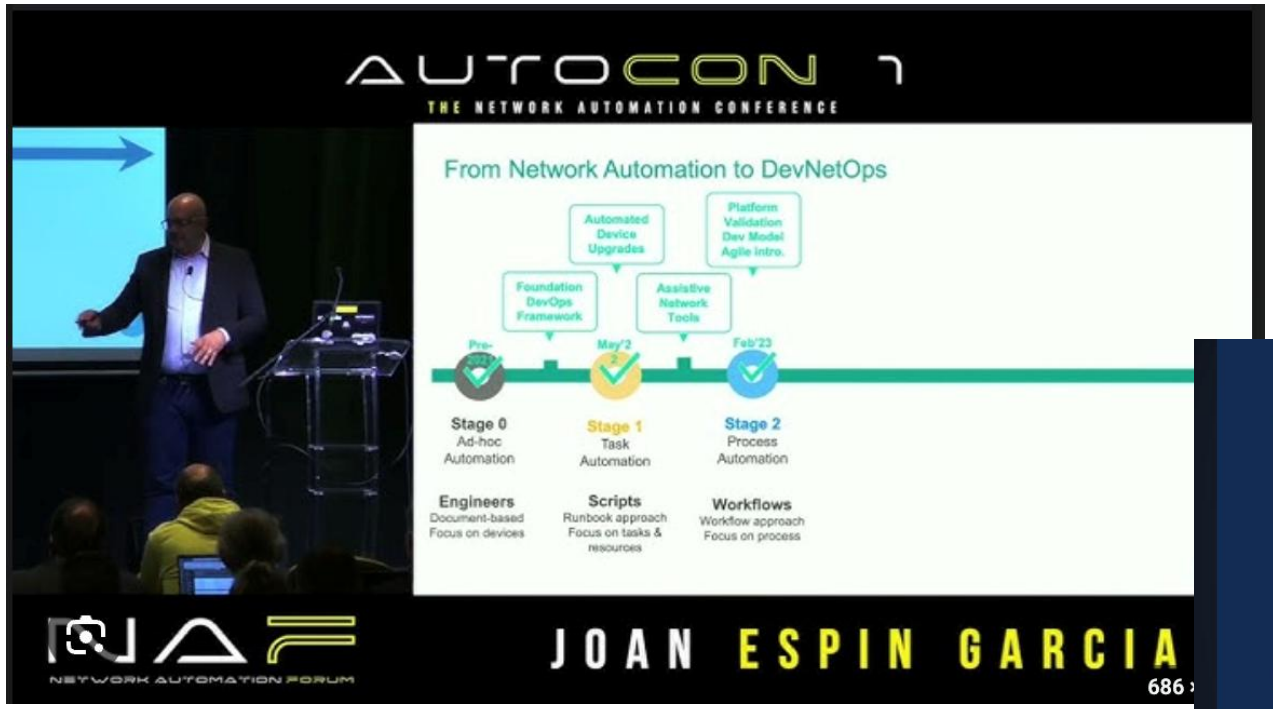
gNMI, SNMP, REST

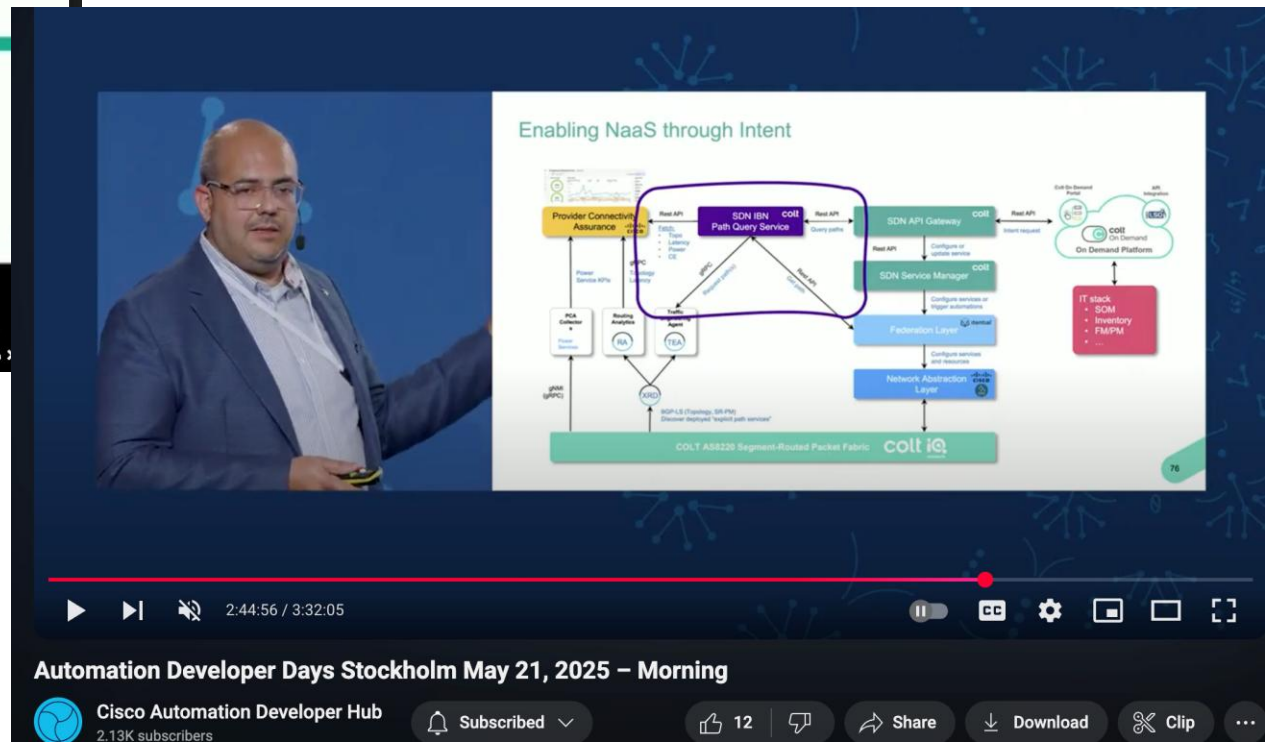
Routing and Path Analytics

Topology-aware assurance

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

Customers References - Colt

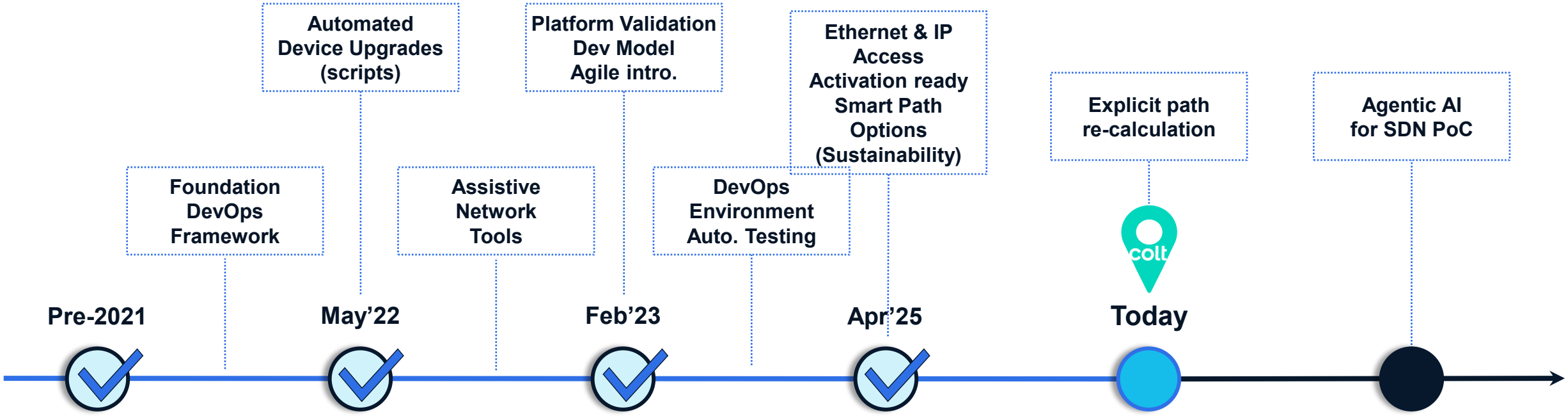




Watch the story from the source;
https://www.youtube.com/watch?v=Jv5xnPG0g5I

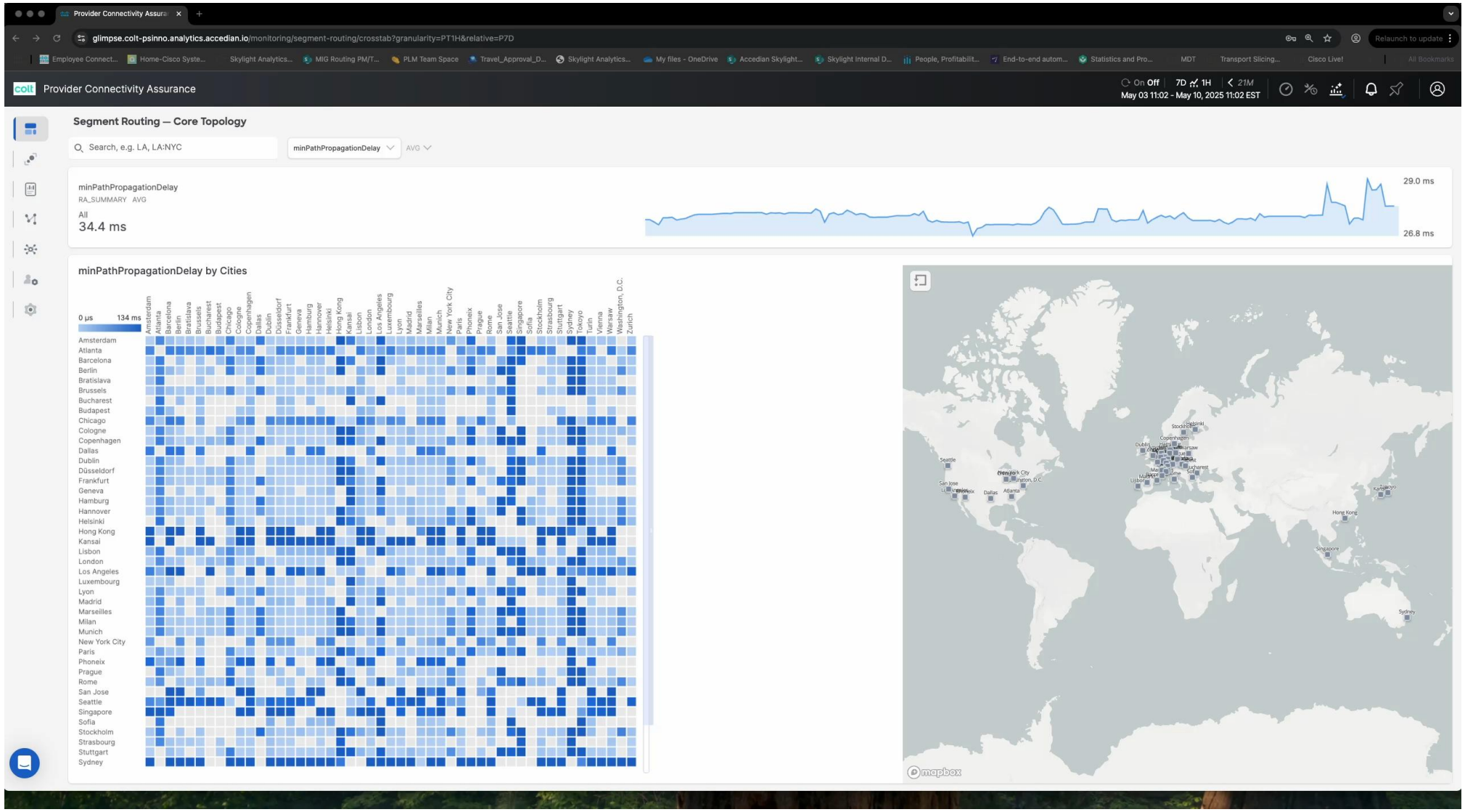
© 2025 Cisco and/or its affiliates. All rights reserved.

Colt's automation journey so far



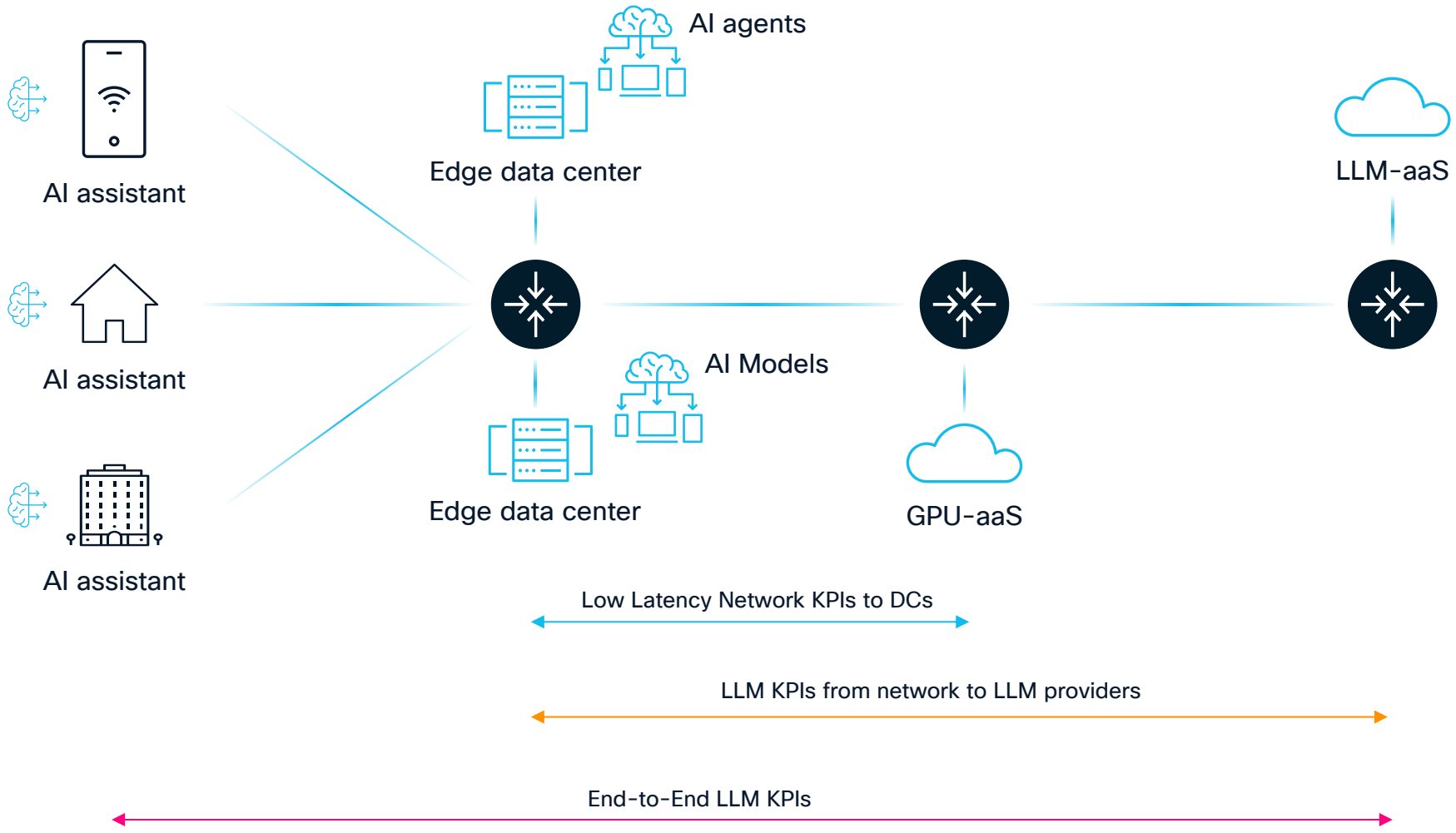
© 2025 Cisco and/or its affiliates. All rights reserved.

Colt Example: Path Details and ECMP Compare



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

Infrastructure for AI: Measure and optimize AI performance



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

LLM + Network Performance Correlation

Key LLM Performance Metrics

Request Latency

This is the amount of time each request takes to process by the LLM from start to finish.

Time To First Token

The amount of time the LLM takes to return the first token in a response to a request.

Time Per Output Token

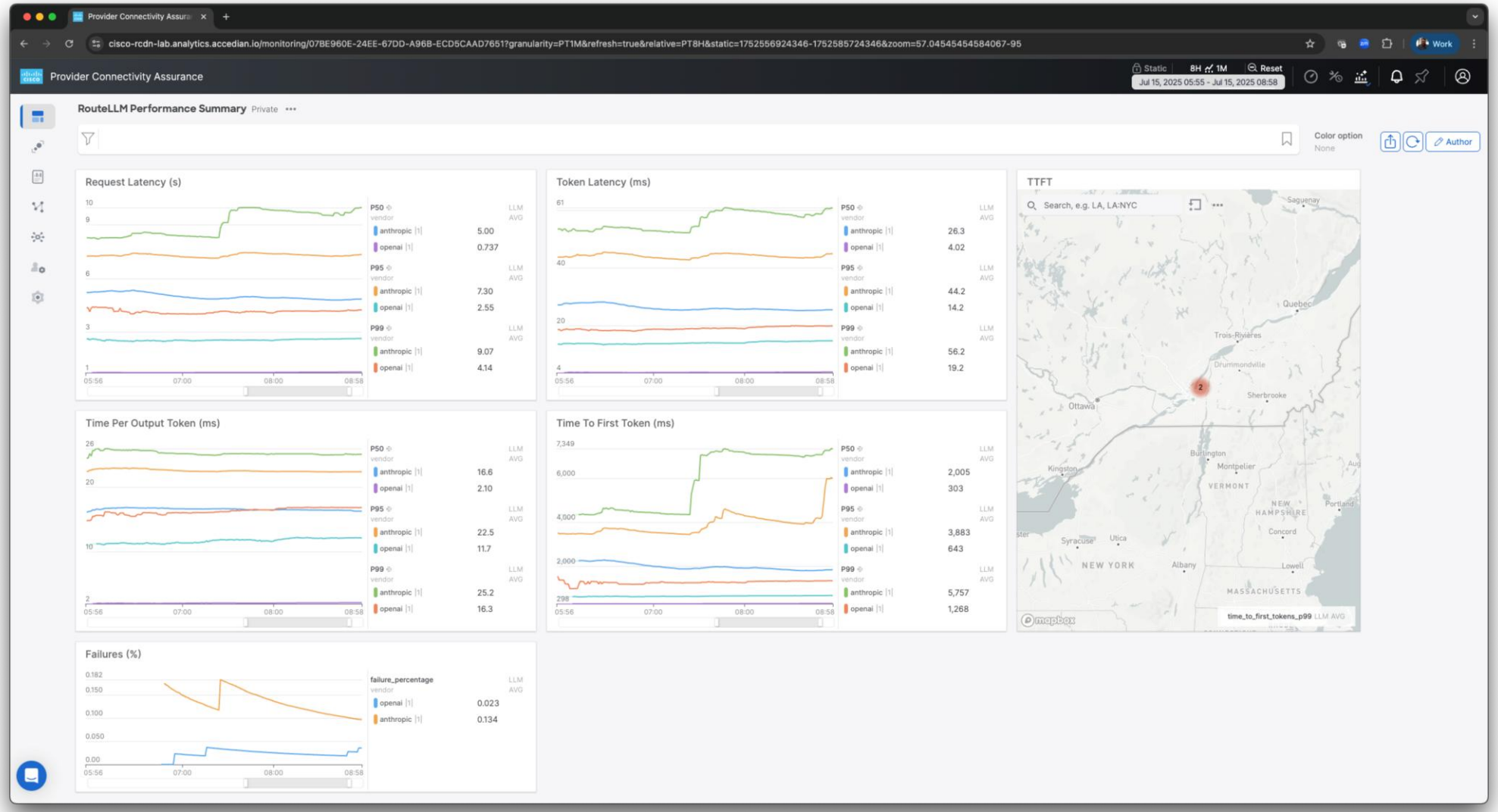
The amount of taken to generate each token after the first token (a.k.a. inter-token latency) in a response.

Token Latency

The amount of time taken to generate each token in the response (request latency / total number of tokens).

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

Using Provider Connectivity Assurance for network and LLM Experience



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

Summary

- Operators face a Perfect Storm of handling Complexity, Increasing consumer expectations, Knowledge contention & OpEx constraints
- Cisco is investing heavily on multi-vendor network automation and assurance platforms, including additional AI capabilities to address any customer requirement
- We are actively working with our SP customers to explore, define and develop the Automation Use Cases that will accelerate their journey to a Systems-led operating model

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

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

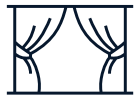
Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

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

Continue your education



Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

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

Thank you

CISCO