CISCO Connect

# Delivering a Secure Network for the AI-ready Campus and Branch

Future-Proofed Workplaces

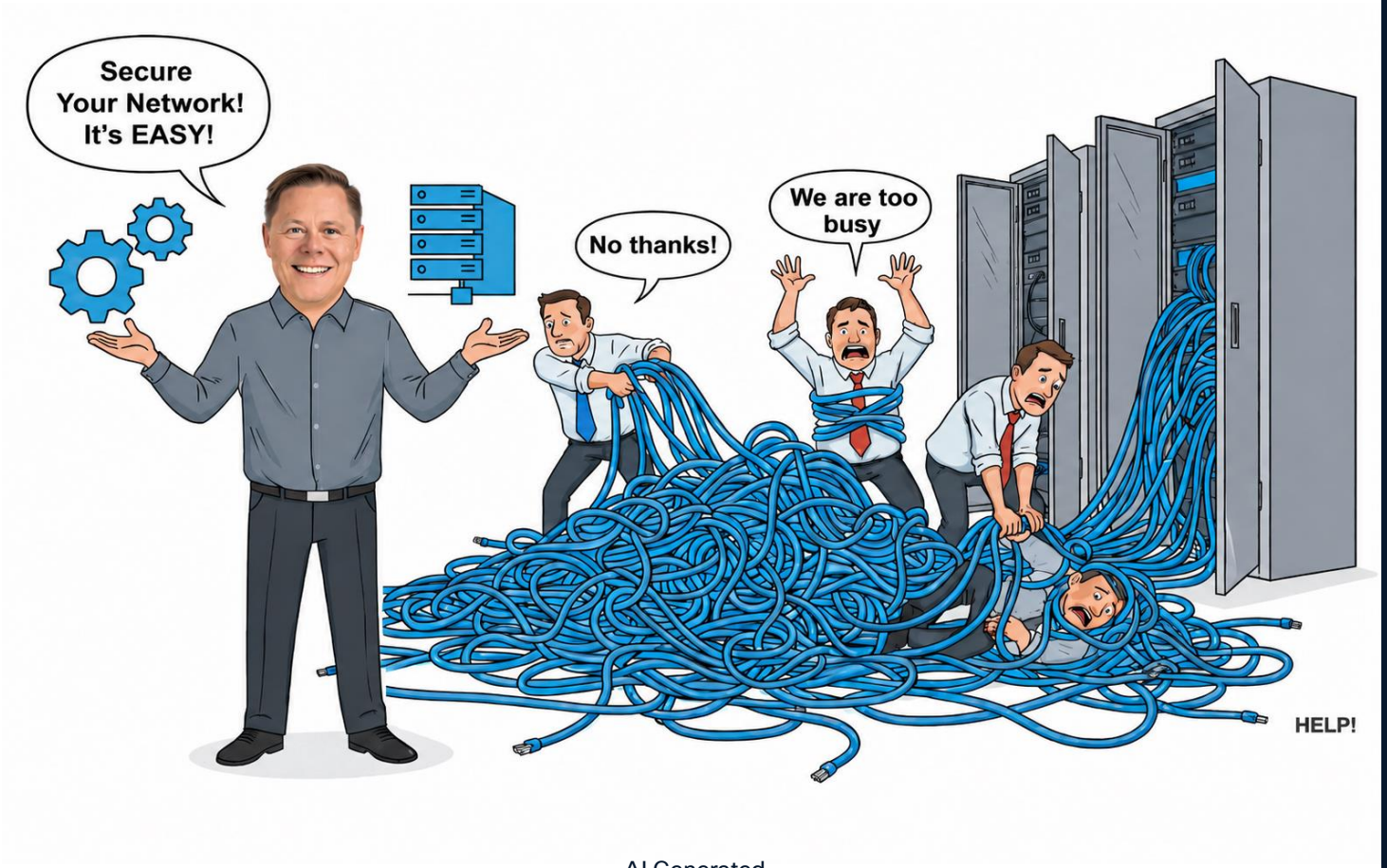
Patrick Mosimann
Solutions Engineer

Ricardo Kaufmann
Solutions Engineer

June 17th, 2026

# About Patrick...

19+ years in Networking
  3 years as customer
  3 years as a partner
  3 years as a competitor
10+ years at Cisco




AI Generated

# About Ricardo...

CISCO CERTIFIED CCDE DESIGN # 2023::66

CISCO CERTIFIED CCIE ENTERPRISE # 65507

- Sports & Traveling
- Solutions Engineer Routing & SD-WAN

**14+ years in Networking**

7 years as customer
2 years as partner
1 year as a competitor
2.5 years at Cisco

# Agenda

1. Introduction
2. Why Secure Networking?
3. What is Secure Networking?
4. The Challenge of building an End-to-End ‘Reference Architecture’
5. Closing / Next Steps

# Why Secure Networking?

# Is your Campus Network AI ready?

- For explosive traffic
- For more complexity
- For increased security risks

# Network complexity is increasing security risk

## Identities are changing

Explosion of IoT, OT, and unmanaged devices raises risk of lateral movement

## Workloads are everywhere

Remote work, SaaS, and cloud adoption erode the traditional security perimeter

## Threats from AI are here

Rise of AI-powered attacks overwhelm network and security teams

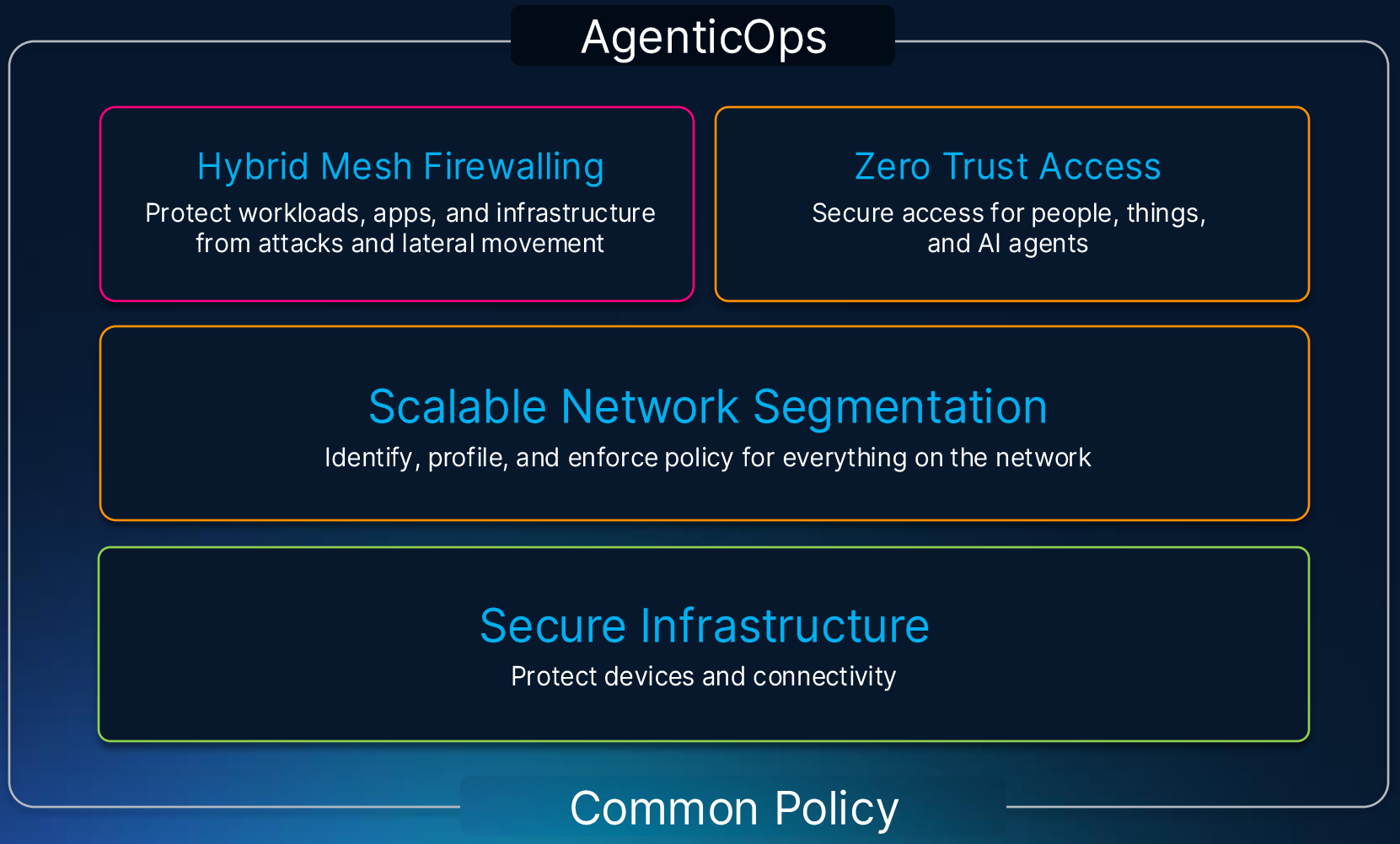
MORE USERS. MORE DEVICES. SMARTER THREATS.

# What is Secure Networking?

# Introducing Cisco's Secure Networking

## Security infused into the network

- Identity-first
- Continuously verified
- Enterprise-wide policies
- Comprehensive threat intel
- Distributed enforcement
- Streamlined Operations




*Source: Zeus Kerravala, ZK Research, 2025

# A unified framework for managing security policies across diverse IT environments

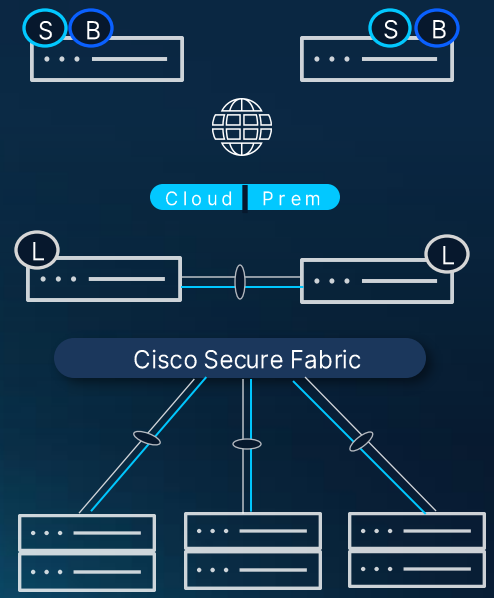

**Scalable Network Segmentation**

# Securing network access and eliminating lateral movement

## Native segmentation
VLAN, SGT, VRF/VPN


## Strengthened with NAC
ISE and Access Manager


## Automated secure fabric
Cloud and On-Premise




## Scalable Network Segmentation

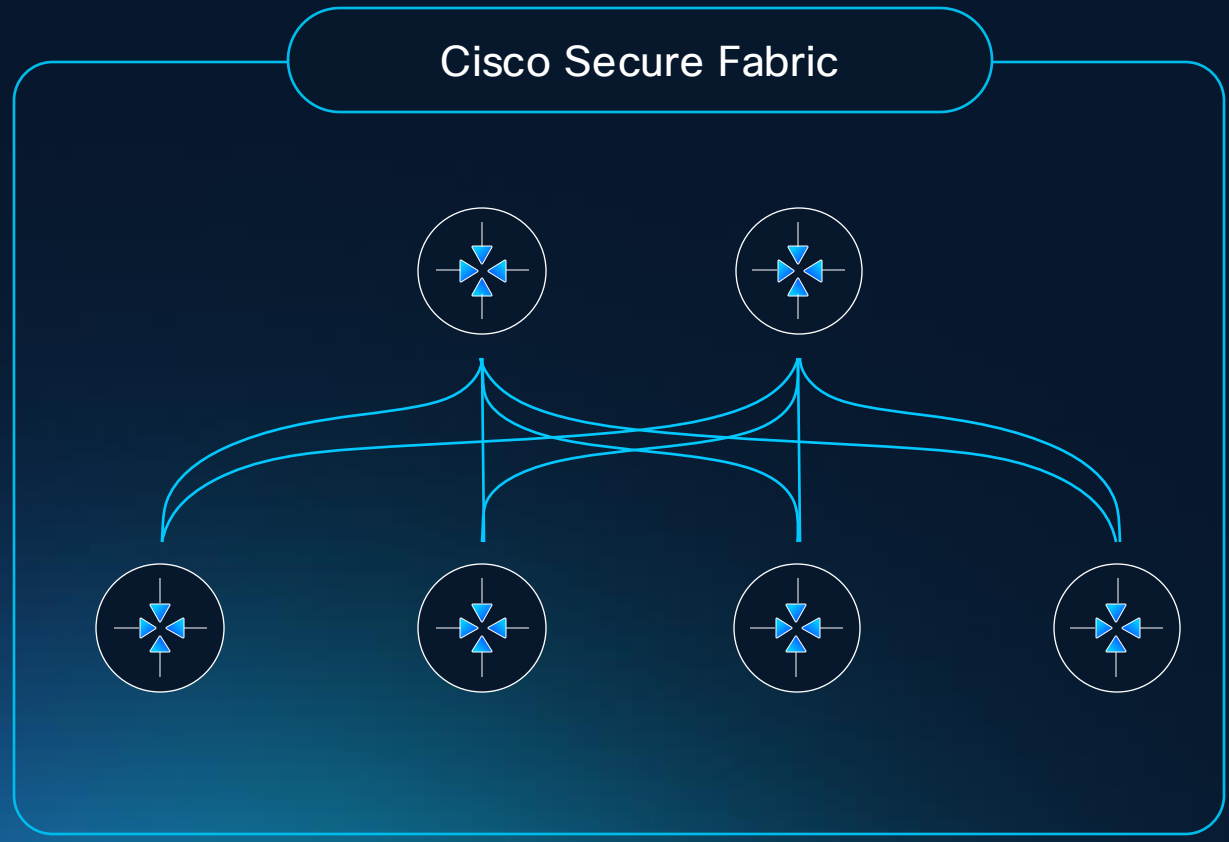
# Simplifying network segmentation through automation with campus fabric

IOS XE Switches,
Access Points, Routers

Cloud Fabric

On-Premise Fabric (SDA)

Programmable Fabric



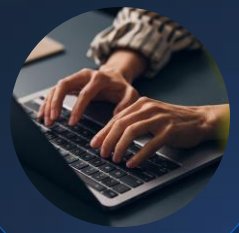

Scalable Network Segmentation

# A unified framework for managing security policies across diverse IT environments


**Scalable Network Segmentation**

# Connecting and securing every corner of the network

Users, Devices, and Things



Data Loss Prevention (DLP)

WAN Optimization and Routing

Secure Web Gateway (SWG)

Firewall as a Service (FWaaS)

Cloud Access Security Broker

Remote Browser isolation (RBI)

Campus LAN

Consistent WAN Security

Security Service Edge + SD-WAN

Secure Application Access

Traditional Apps

Private Apps

Internet Apps

SaaS Apps

## Zero-Trust Network Access

# Hybrid Mesh Firewall: Distributed Firewall Policy

Advanced protection, simplified operations and real-time intelligence for a more secure, scalable future

## Security Cloud Control

Secure Firewall (physical) | Secure Firewall (virtual) | Secure Firewall (cloud) | Secure Router


SSE | Secure Workload | Isovalent runtime protection | 3rd Party Firewall | ACI

← Native enforcement points go deeper → Integrate with existing

Write policy once - enforce across the mesh

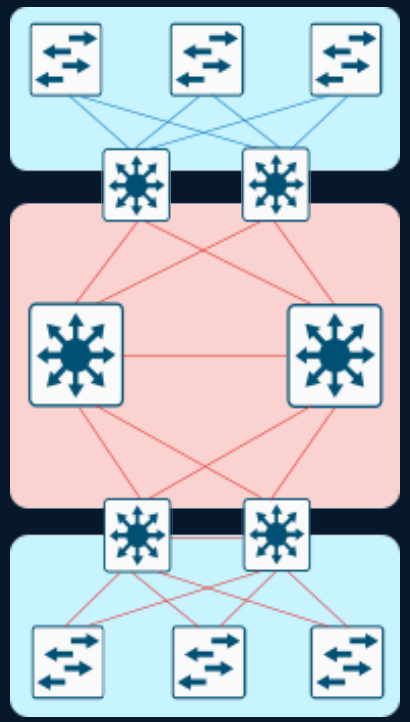
# The Challenge of building an End-to-End ‘Reference Architecture’

# Why do we divide into Layers & Domains?

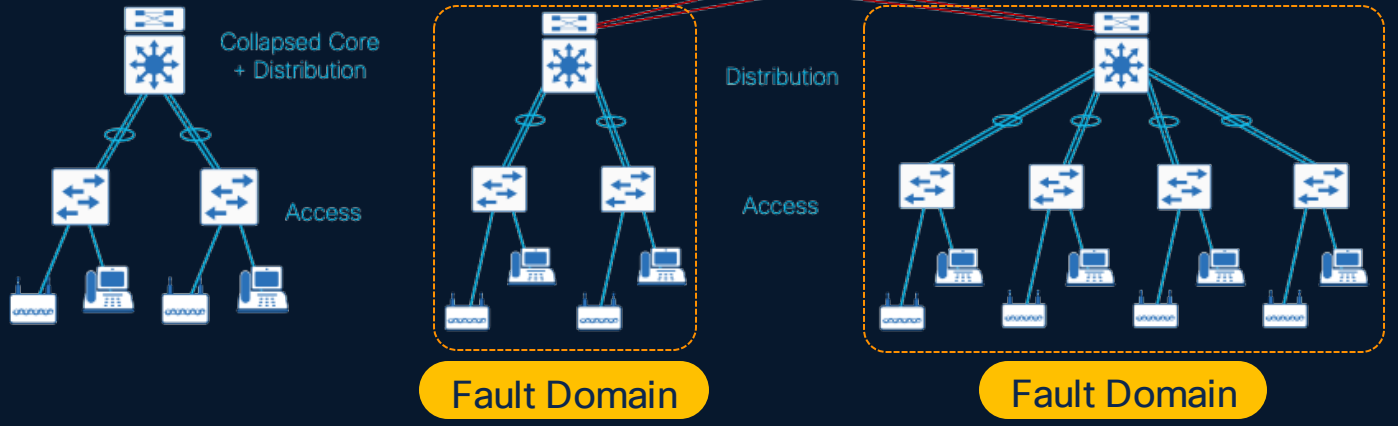
## Why can't we just collapse Layers & Domains?

The eternal battle between: "reducing complexity & costs" and "maximizing stability & reliability"

*Separate Roles*

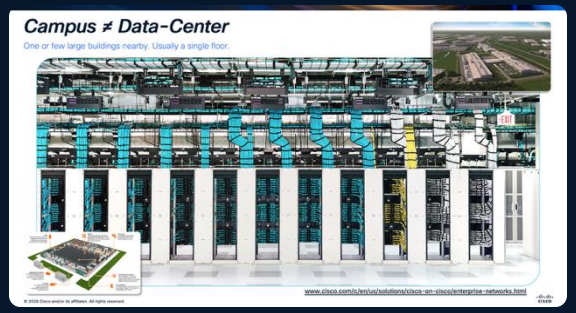


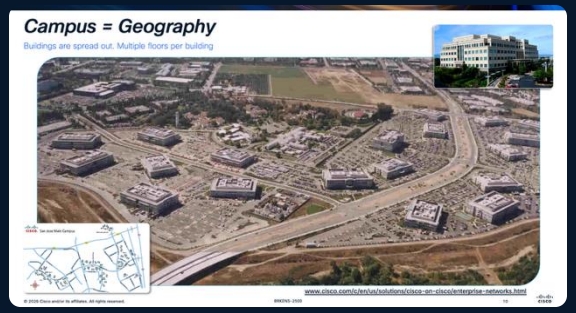
SCALE




*Different Features*


*Different Ops Teams*

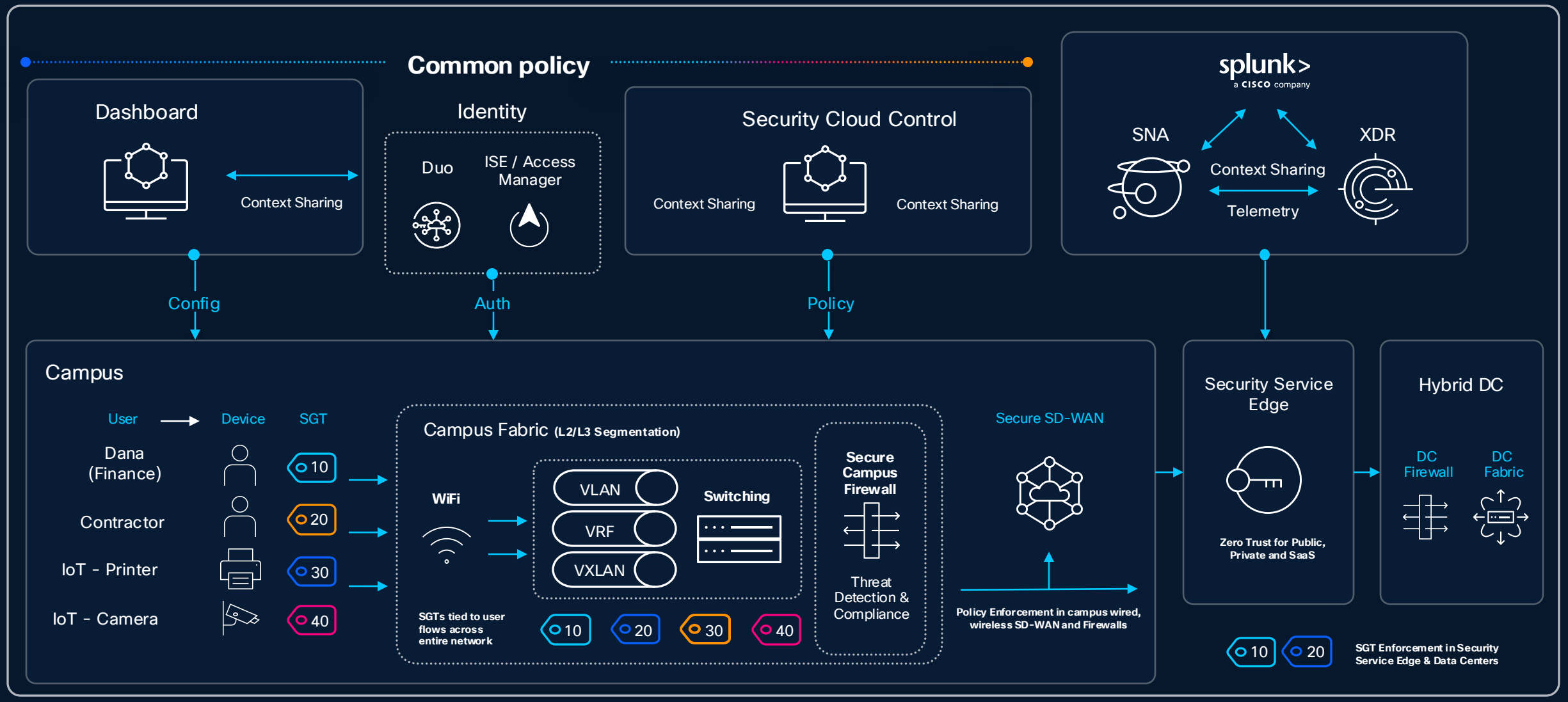



*Different Environments*

# Secure campus and branch

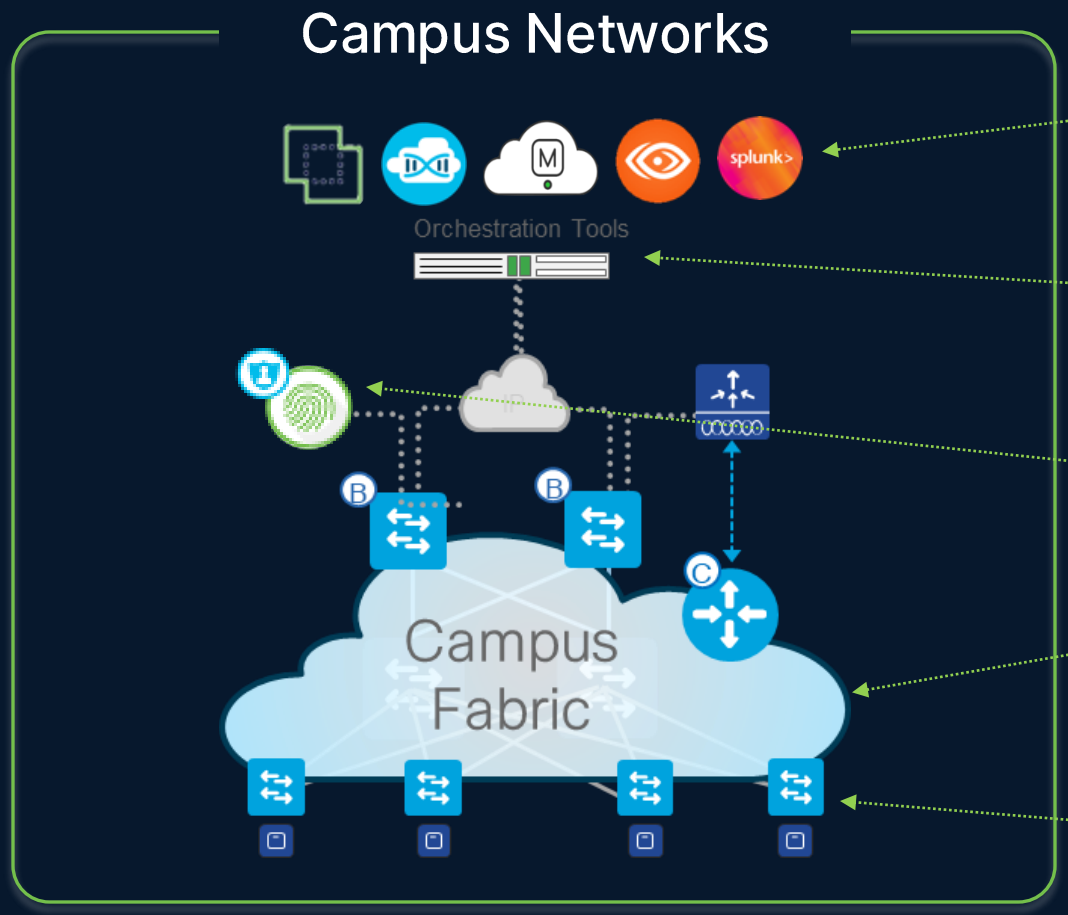
## Reference Design



# Introducing the **Secure Networking** Reference Architecture (**SNRA**) Multi-Layer ‘Reference Model’

# Secure Networks – Solution Layers

Full-Stack Multi-Layer Reference Model (like the OSI Model)




5 **Extended Ecosystem** (Splunk, ThousandEyes, etc.)
Sharing device & flow analytics with external management tools

4 **Unified Management & Agentic Ops**
On-Premise & Cloud Automation & Analytics, including AIOps
ENTRY 1

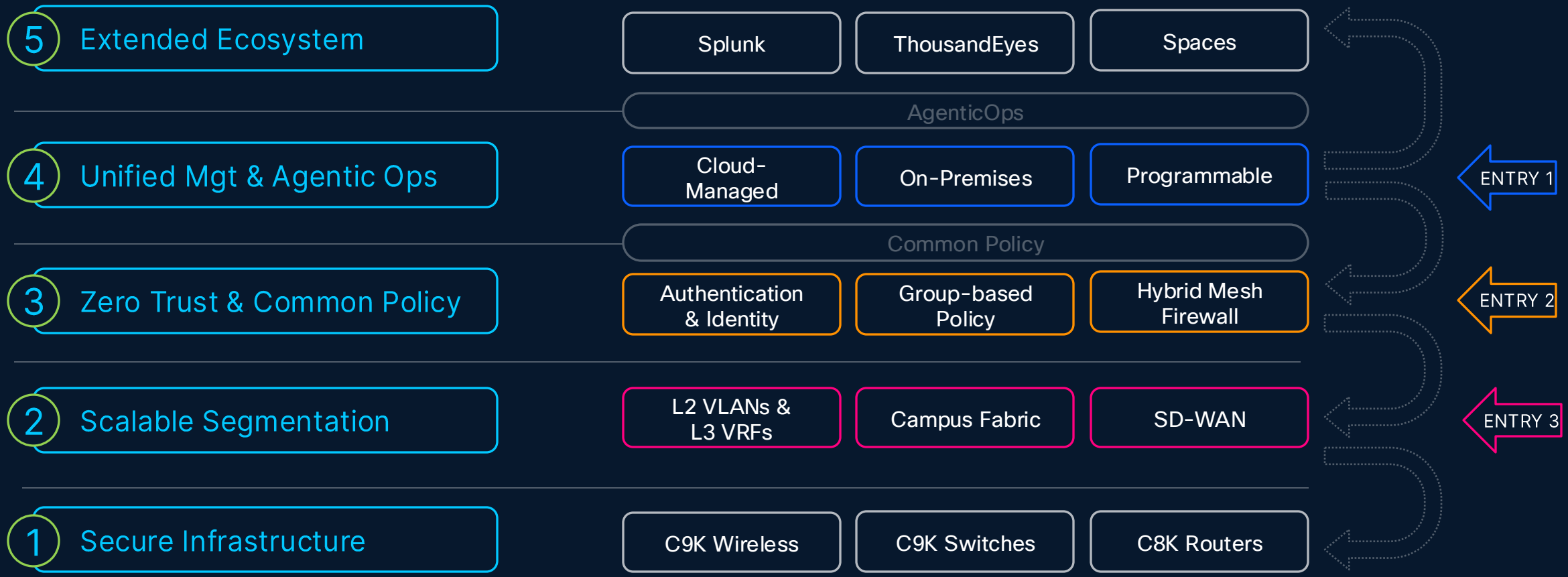
3 **Zero Trust Access & Common Policy**
Identity, Policy, Hybrid Mesh Firewall, Threat Detection & Response
ENTRY 2

2 **Scalable Network Segmentation**
Network for L2/L3 & Multicast, with SGT & VRF segmentation
ENTRY 3

1 **Secure Infrastructure**
Wired & Wireless devices, Unified Hardware, Software & Licensing

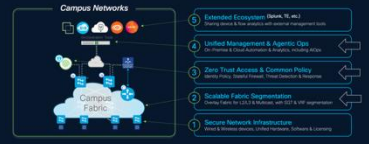
# Secure Networks – Solution Layers

Each Layer can be designed independently (connects to other layers)

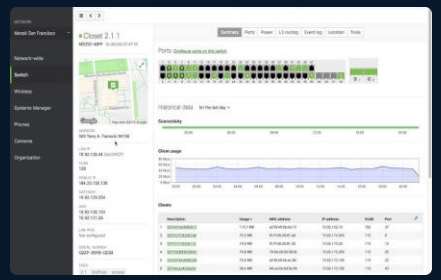


# Management Type – Journey Map

Start from your Management or Operational model




## Cloud Managed



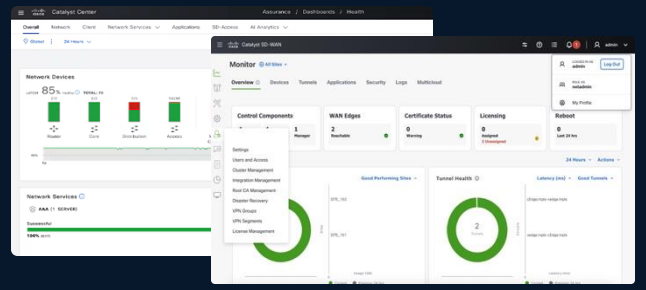
4 **Meraki Dashboard**
Cloud-Managed LAN, WLAN & WAN

3 **Access-Manager + SCC**
Cloud-managed NAC + Group Policy

2 **Cloud Fabric & SD-WAN**
Cloud-automated Underlay & Overlay

1 **Meraki for C9K & C8K**
Cloud Switching, Wireless & Routing

## On-Premises



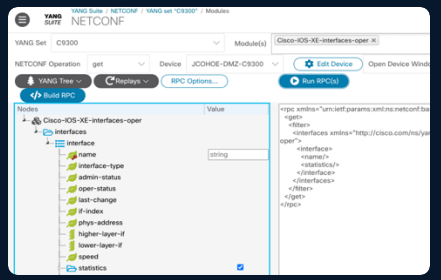
4 **Cat Center & SDWAN Mgr**
On-Premises LAN, WLAN & WAN

3 **Cisco ISE + FMC**
On-Premises NAC + Group Policy

2 **SD-Access & SD-WAN**
Premises-automated Underlay & Overlay

1 **CC for C9K & SDW for C8K**
Premises Switching, Wireless & Routing

## Programmable (DIY)



4 **Programmable (DIY)**
Customer-managed APIs or CLIs

3 **RADIUS + CTS + SCC API**
Customer-managed NAC + Group Policy

2 **Custom Fabric & WAN**
Customer-managed Underlay & Overlay

1 **Programmable C9K & C8K**
Custom Switching, Wireless & Routing



NOTE: Slide is animated

# Introducing the SNRA Modular ‘T-shirt Sizing’

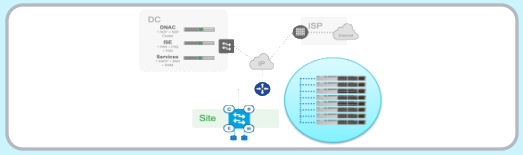
# Secure Networks – Modular T-shirt Sizing

XS

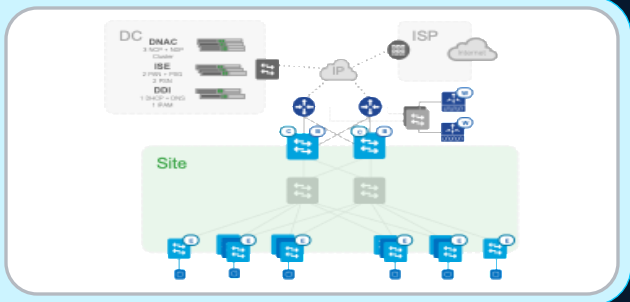
XL

## 1 Baseline Modules

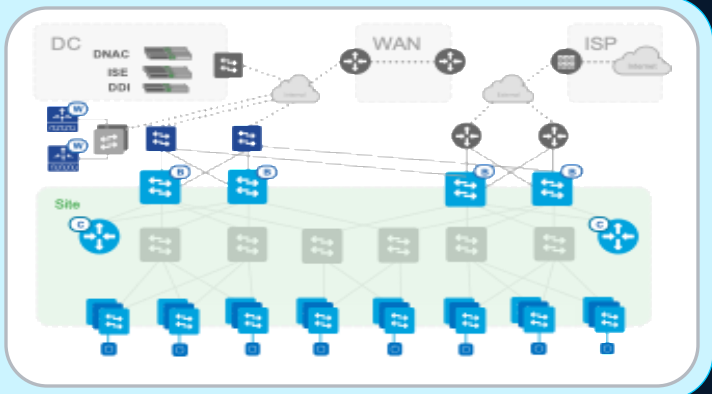
**Small**
*1-2 Tier LAN*
*≤ 5K endpoints*



**Medium**
*2-3 Tier LAN*
*≤ 25K endpoints*




**Large**
*3-4 Tier LAN*
≥ 50K endpoints




## 2 Specialized Modules

**Ultra HA Networks**
Networks with ultra high-availability requirements with minimal to zero down time in critical networks
(Hospitals, Financial Institutions, etc.)

**Critical Security Networks**
Networks with critical security requirements requiring high confidentiality and integrity requirements
(Defense Sector, etc.)

**Multicast Heavy Networks**
Networks with high number of camera feeds for security and monitoring resulting into a specialized multicast design
(Stadiums, Casinos, etc.)

**Digital Audio Video Networks**
Networks with digital audio and video end points like mic and speakers with various QoS/PTP/etc requirements.
(Schools, Media, etc.)

**Smart Powered Buildings**
Networks powering smart buildings and modern workspaces using PoE infrastructure
(Hospitality, Manufacturing, etc.)

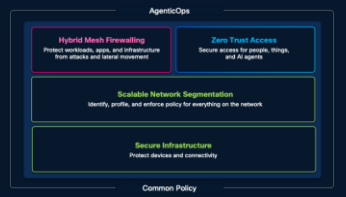
Secure Networking

# Secure Network Infrastructure

1 **Network Infrastructure**
Wired & Wireless devices, Unified Hardware, Software & Licensing

Secure Networking

# Reference design for Secure Network Infra




**Scalable Network Segmentation**

Identify, profile, and enforce policy for everything on the network

**Secure Infrastructure**

Protect devices and connectivity

**Secure Wireless:** Cisco C9K APs & WLC/MCG

- Access Point
- Wireless Control

**Secure Switching:** Cisco C9K Series Switches

- Access & IOT
- Core & Distribution

**Secure Routing:** Cisco Secure Routers

- Branch and Campus
- Data Center

**Secure Firewall:** Cisco NG Firewalls

- Distributed Virtual
- Central Appliance

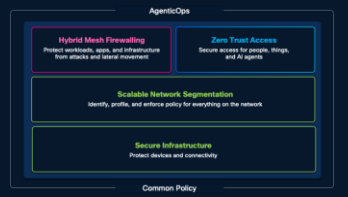
Secure Networking

# Scalable Fabric Segmentation

2 **Scalable Fabric Segmentation**
Overlay Fabric for L2/L3 & Multicast, with SGT & VRF segmentation

Secure Networking

# Reference design for Scalable Network Segmentation



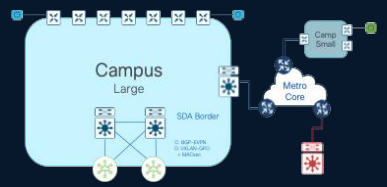

2

## Scalable Network Segmentation

Identify, profile, and enforce policy for everything on the network

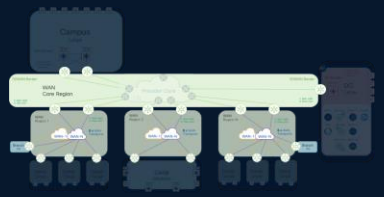
**Secure Fabric:**
Campus Overlay for Wired & Wireless LAN

- Wired Overlay
- Wireless Overlay




**Secure SDWAN:**
SDWAN Overlay for Core & Branch WAN

- Core Overlay
- Branch Overlay



**Secure Data Center:**
DC Overlay for Data Center LAN

- DC Overlay
- Storage Overlay


**Secure Firewall:**
Overlay integration for Hybrid Mesh Firewall

- Distributed Virtual
- Central Appliance


1

## Secure Infrastructure

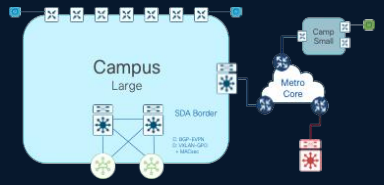
Protect devices and connectivity



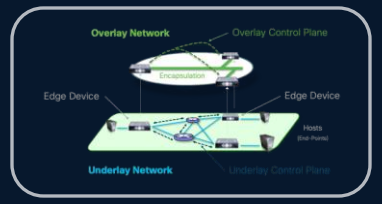
cisco

# Cisco Campus Fabric

Key Concepts & Considerations (Why it matters)

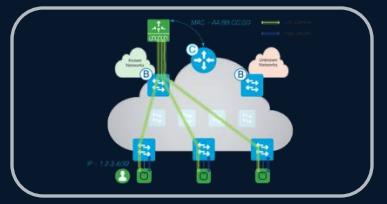



## 1 L2 & L3 Overlay



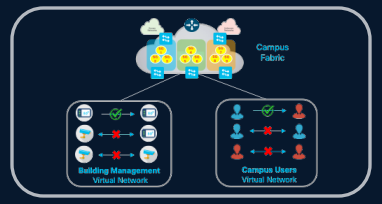

- Support L2 Broadcast & Multicast bridging behavior
  - without reliance on L2 protocols (eg. STP)
- Support IPv4 & IPv6 L3 routing protocols
  - abstracts IGP & EGP into single 'overlay'
- Enable L2 VLANs & L3 Anycast GW across Campus
  - without enabling L2 across the Core

## 2 Wireless Integration



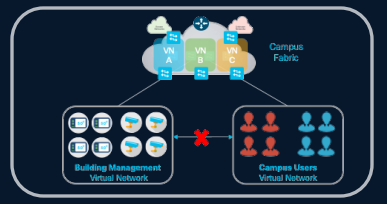
- Simplifies L2 & L3 wireless roaming in the 'overlay'
  - maximizes load-balance & redundancy
- Offload Wireless Data traffic to the Access switches
  - without tunneling back to WLC
- Enables a common policy for wired and wireless
  - single point of policy enforcement

## 3 Micro-Segmentation



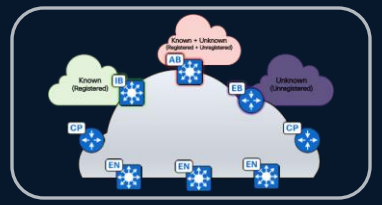

- Segments endpoints based on an Identity (SGT)
  - rather than based on VLAN or IP/subnet
- Enables Group (SGT) based ACL & QoS and more
  - address-independent services
- Fabric natively carries SGT inside of VXLAN-GPO

## 4 Macro-Segmentation



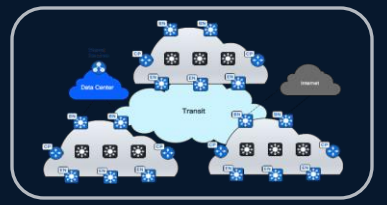

- Segments Groups (IP) into Virtual Networks (VN)
  - isolates VNs from other VNs
- Enables L2 & L3 VPN services and security
  - without MPLS or other VPNs
- Fabric natively carries VNID inside of VXLAN-GPO

## 5 Fabric Handoff




- Support for L2 or L3 hand-off at Fabric Border
- Native VXLAN hand-off to carry SGT & VRF
  - Includes Cisco NG Firewalls + VXLAN
- Simple IP/MPLS + CTS/SXP hand-offs
  - Includes legacy & third-party Firewalls

## 6 Multi-Site & Mult-Domain Fabrics

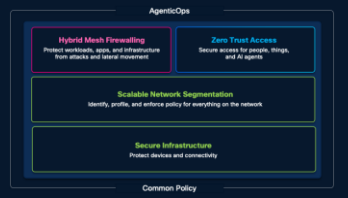



- Connects multiple Fabric Sites & Domains
- Native VXLAN + LISP Transit between Campuses
  - integration with EVPN multi-site
- Native VXLAN + EVPN Transit with Data Centers
  - hierarchical EVPN multi-site



cisco

# Reference design for Scalable Network Segmentation




2

**Scalable Network Segmentation**

Identify, profile, and enforce policy for everything on the network

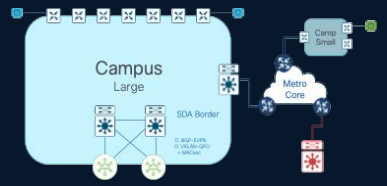
**Secure Fabric:**
Campus Overlay for Wired & Wireless LAN

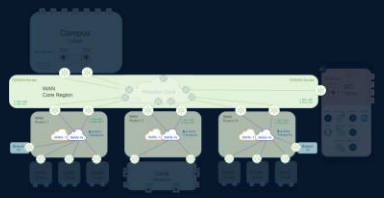
**Secure SDWAN:**
SDWAN Overlay for Core & Branch WAN

**Secure Data Center:**
DC Overlay for Data Center LAN

**Secure Firewall:**
Overlay integration for Hybrid Mesh Firewall

Wired Overlay | Wireless Overlay | Core Overlay | Branch Overlay | DC Overlay | Storage Overlay | Distributed Virtual | Central Appliance





1

**Secure Infrastructure**

Protect devices and connectivity

# Cisco SASE

**Secure SD-WAN**
Catalyst and Meraki

+

**Secure Services Edge**
Cisco Secure Access

+

**Identity First**
ISE + Identity Intelligence

## Key Highlights

**Experienced through Common Platform**
Single dashboard (SCC) for Secure Access, Catalyst SD-WAN

**Extended Network to the Cloud**
End-to-End Segmentation with SGT and VPN information

**Single Global Security Policy**
ZTNA, CASB, DLP, AI Access...

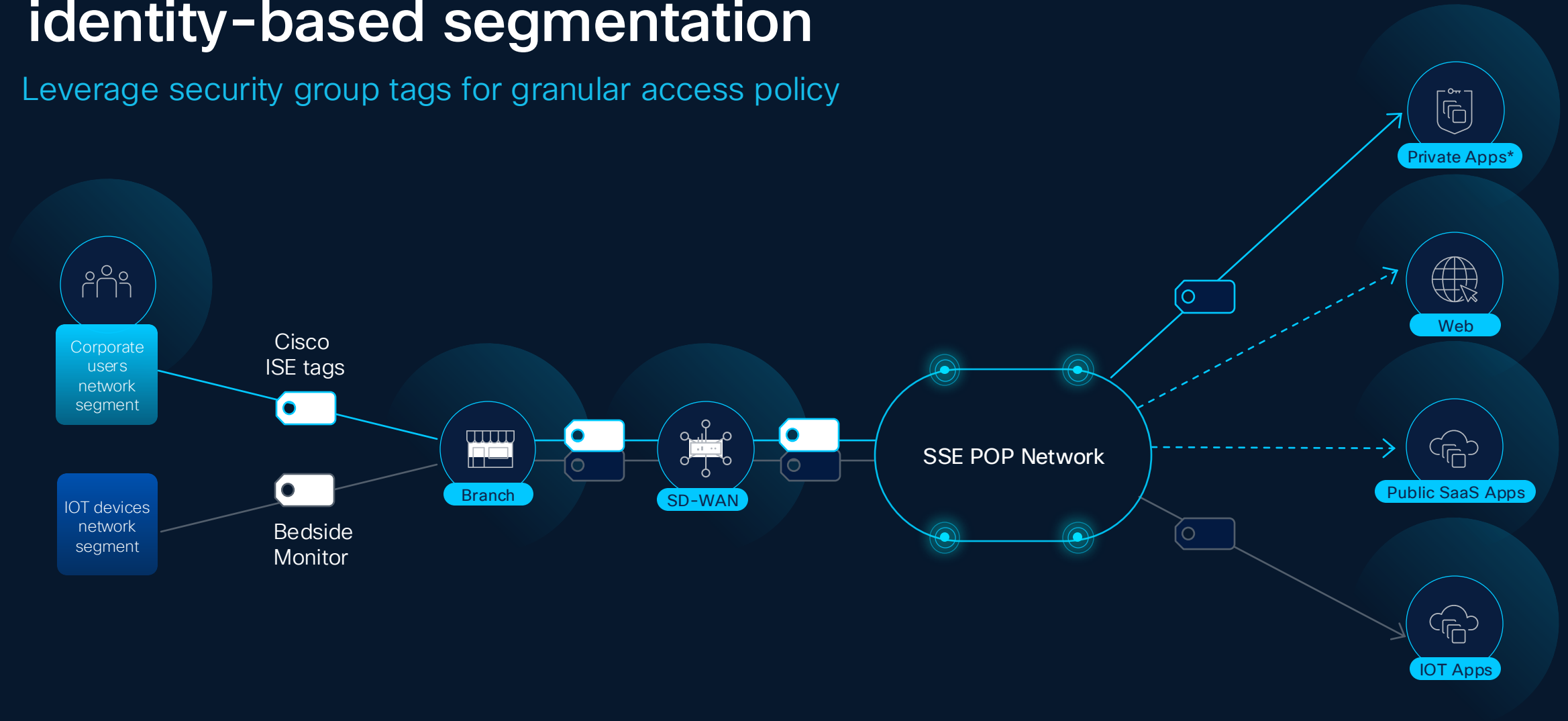
**Seamless Integration**
Consolidate network and security into a single architecture

**Ease of Operation**
Define once, use objects everywhere across SASE experiences

**End-to-End Observability and Troubleshooting**
powered by ThousandEyes

# Securing network access with identity-based segmentation

## Leverage security group tags for granular access policy






* Capabilities are in-development but not yet available or guaranteed.

# Core Capabilities

SD-WAN Manager

Security Cloud Control

Splunk

## SD-WAN

- Transport Abstraction
- Policy-based path selection
- QoS & App SLA
- 0-Touch Provisioning
- Segmentation

+

## Next Generation Firewall

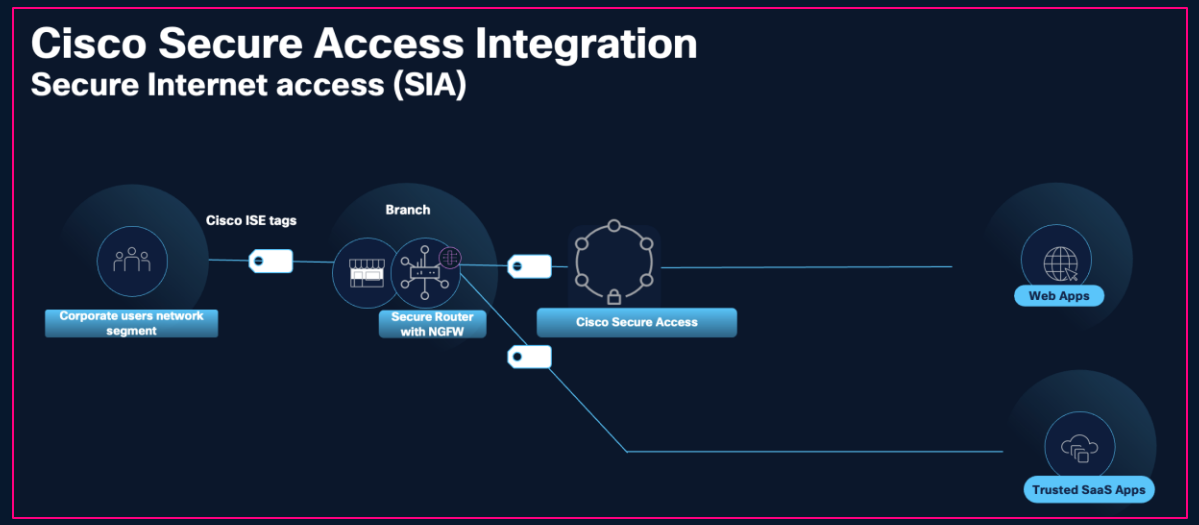
- L3 – L7 FW
- IPS/IDPS
- AMP
- Sandboxing
- URL-F
- TLS Decryption
- EVE, SnortML

+

## SSE Ecosystem

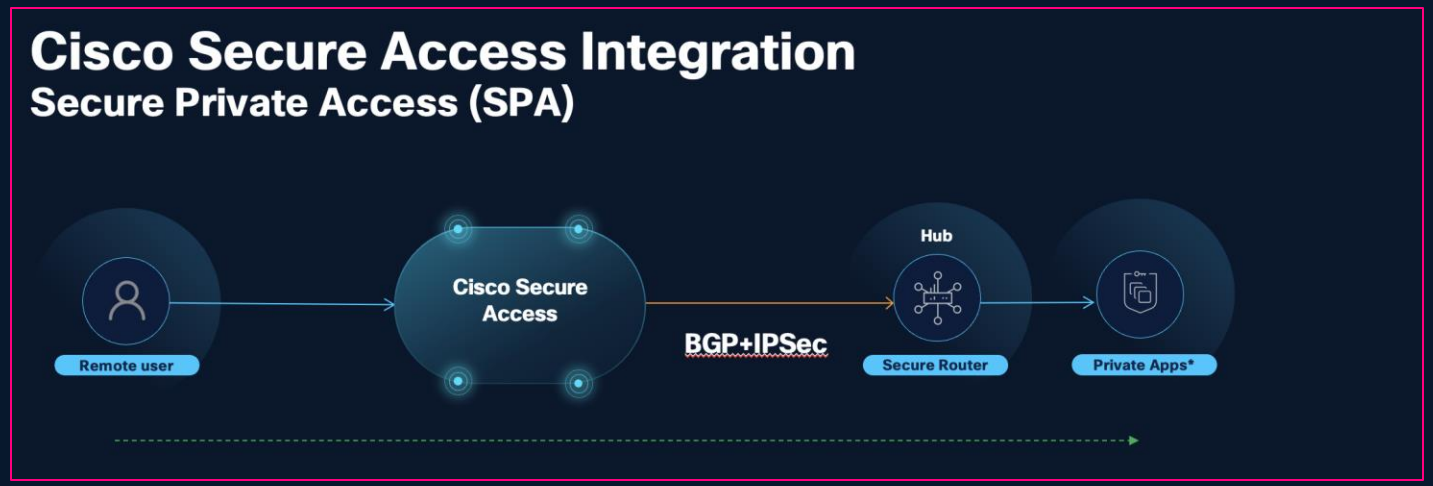
- Auto Tunnel + HA
- ZTNA
- CASB
- FWaaS
- DLP
- SWG

# SD-WAN to SSE – Use Cases




***Protect Branch → Internet traffic***

- **Automated tunnels** to closest SSE POPs
- **Flexible load-sharing** via weighted ECMP, with HA
- Route or **policy-based traffic redirection** to SSE
- **Context Sharing** (SD-WAN VPN/VRF, ISE SGT) with Cisco Secure Access




***Protect Remote User → on-premises & private apps traffic***

- **Automated tunnels** closest SSE POPs
- **Flexible load-sharing** via weighted ECMP, with HA
- **BGP-based connectivity** between remote users and private resources
- Segment/service VPN based tunnels

# Cisco Secure Access - Architecture

Managed Endpoint

Clientless

SD-WAN Branch

## Core SSE – Full Stack Security

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB) and DLP

Zero Trust Network Access (ZTA)

Firewall as a Service (FWaaS) and IPS

## Cisco delivers the core and more in a single subscription...

DNS Security

Multimode DLP

Advanced Malware protection

Sandbox

Talos Threat Intelligence

VPN as a Service

Digital Experience Monitoring*

Remote Browser Isolation*

## Add-on solutions

XDR

DUO MFA/ SSO

CSPM

Web

Private Apps

SaaS Apps

Secure Networking |

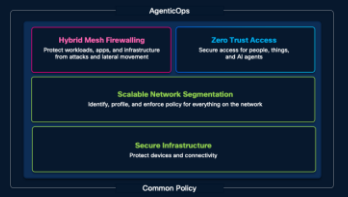
# Zero Trust Access & Common Policy

3 Zero Trust Access & Common Policy

Identity Policy, Stateful Firewall, Threat Detection & Response

# Cisco Zero Trust Segmentation

End to End identity-based segmentation from User to App




## Unified security

## Unified policy

Dashboard

Identity Services

Duo

ISE / Access Manager

Security Cloud Control

SNA

splunk>

XDR

Context Sharing

Context Sharing

Context Sharing

Context Sharing

Config

Auth

Policy

Telemetry

### Campus & Branch

| User | Device | SGT |
|---|---|---|
| Dana (Finance) | | 10 |
| Contractor | | 20 |
| IoT - Printer | | 30 |
| IoT - Camera | | 40 |

### Campus Fabric (L2/L3 Segmentation)

WiFi

VLAN

VRF

VXLAN

Switching

SGT enforcement in Campus wire & wireless 10 20 30 40

**Campus Firewall**

Threat Detection & Compliance

### Secure SDWAN

SGT enforcement in SDWAN & Firewalls

### Security Service Edge

Zero Trust for Public, Private and SaaS

### Hybrid DC

DC Firewall

DC Fabric

ACI

10 20 SGT enforcement in Security Service Edge & Data Centers



cisco

# Zero Trust Access & Common Policy

*Design Workflow*

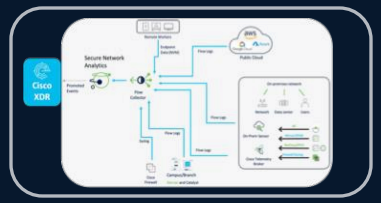

## 1 Identity & Group Policy


- Identity and Micro Segmentation Group Policy for Secure Fabric – powered by Cisco ISE

## 2 Stateful Firewall Policy

- Stateful Firewall and Macro Segmentation – powered by Cisco Security Cloud Control

## 3 Threat Detection & Response




- Threat Detection and Response – powered by Cisco SNA and Cisco Splunk

Secure Networking

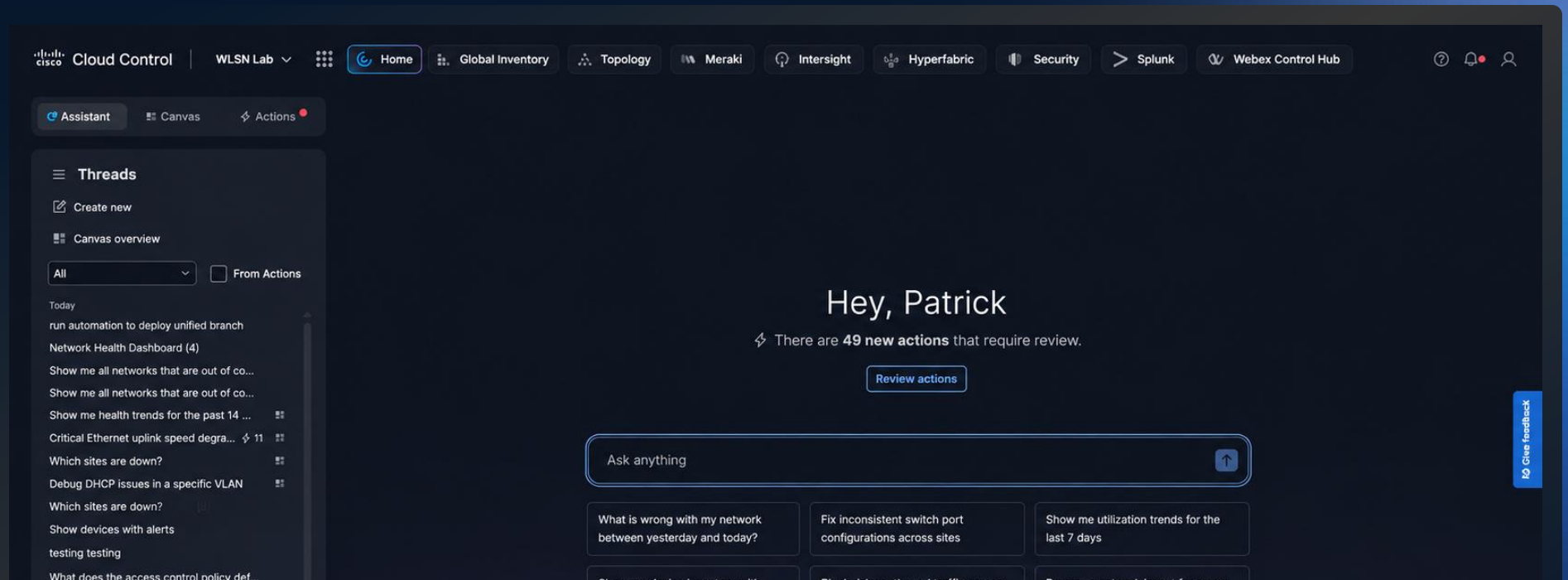
# Unified Management & Agentic Ops

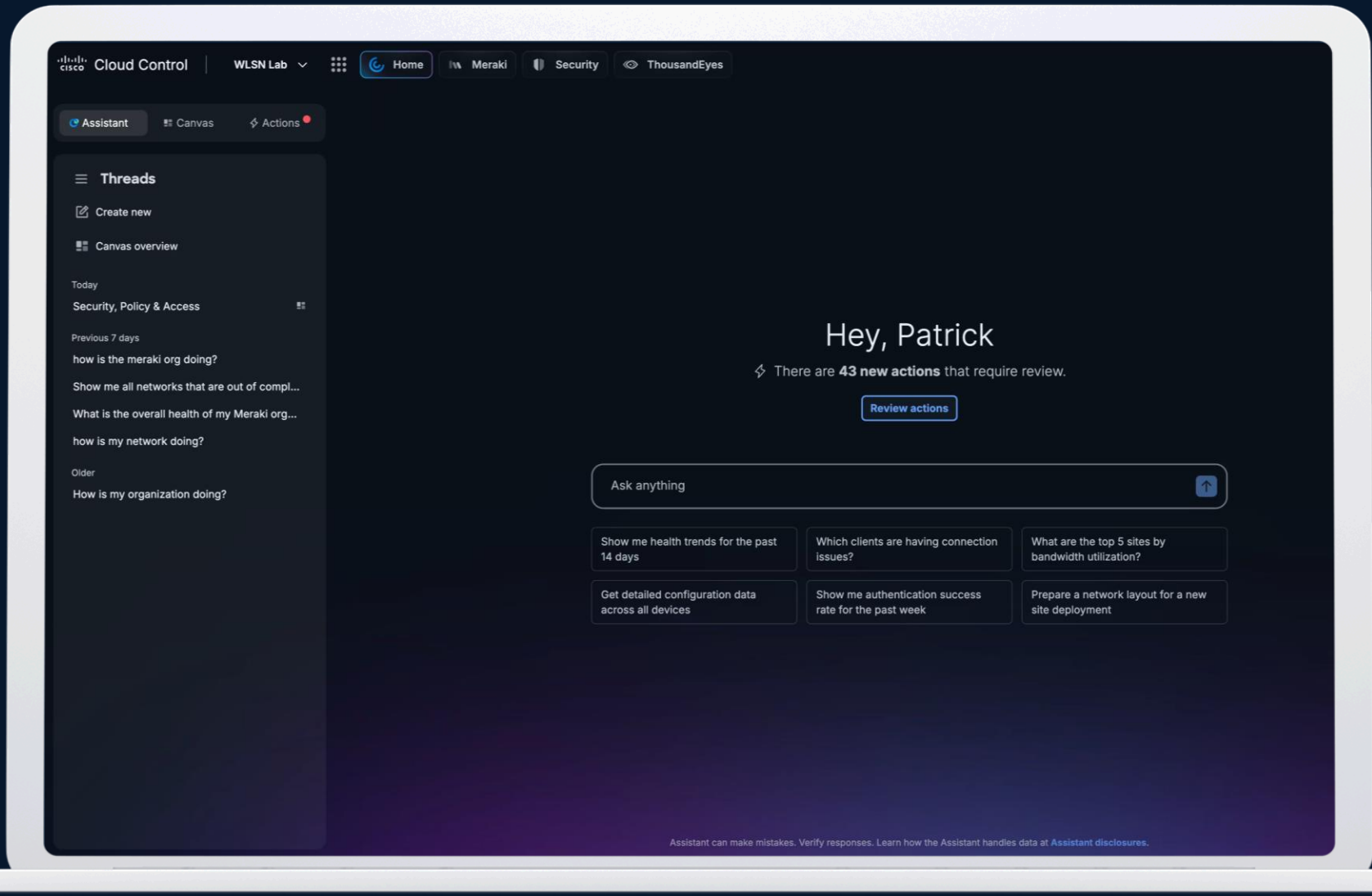
4 **Unified Management & Agentic Ops**
On-Premise & Cloud Automation & Analytics, including AIOps

# Cisco Cloud Control

One platform. Every domain. The foundation everything else is built on.

Meraki · Catalyst Center · Catalyst SD-WAN · Security Cloud Control · ThousandEyes · Splunk · Nexus Dashboard · Intersight · IQ · & more





Assistant | Canvas | Actions

## Threads

Create new

Canvas overview

Today

Security, Policy & Access

Previous 7 days

how is the meraki org doing?

Show me all networks that are out of compl...

What is the overall health of my Meraki org...

how is my network doing?

Older

How is my organization doing?

# Hey, Patrick

There are **43 new actions** that require review.

Review actions

Ask anything

Show me health trends for the past 14 days

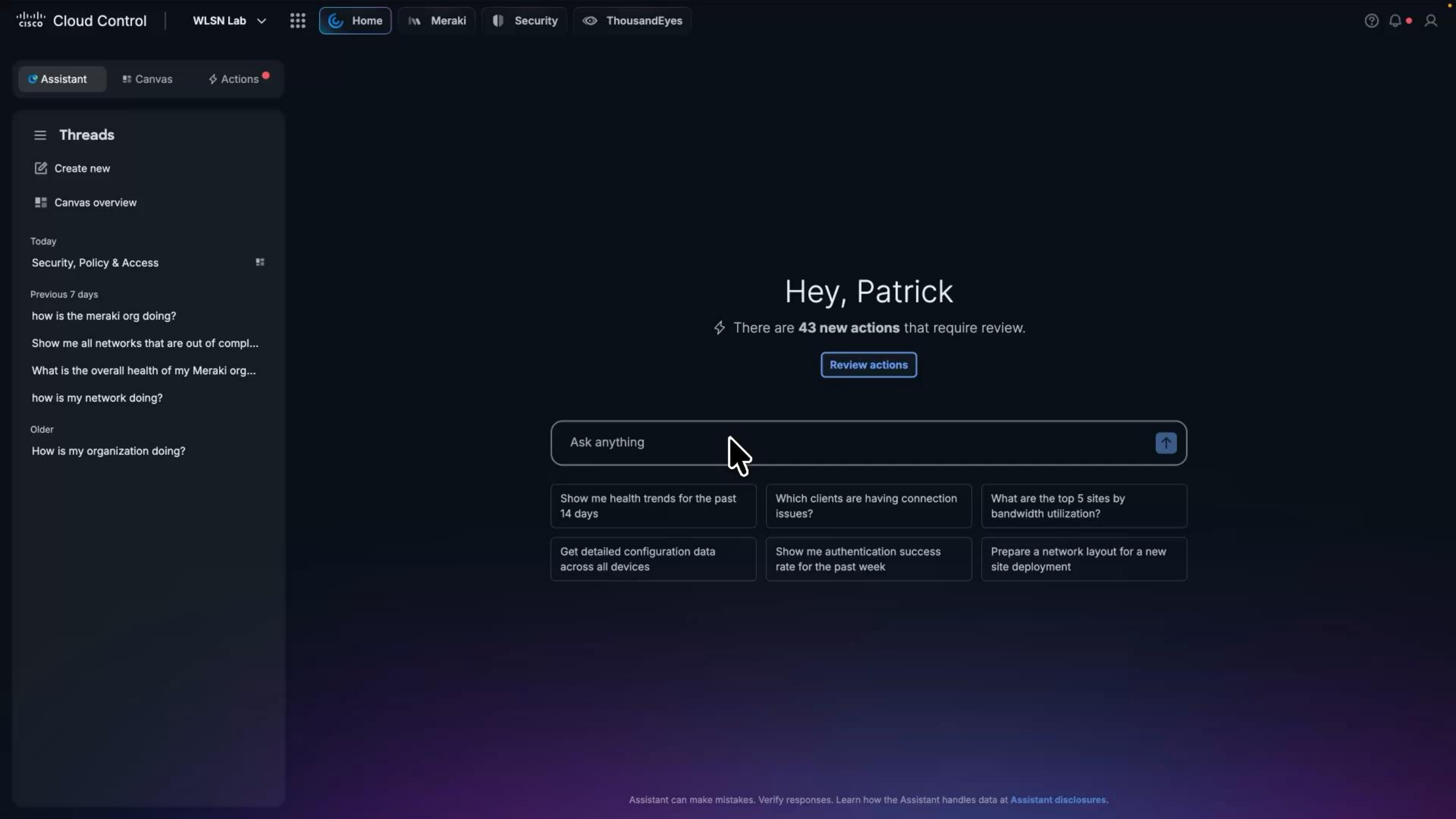
Which clients are having connection issues?

What are the top 5 sites by bandwidth utilization?

Get detailed configuration data across all devices

Show me authentication success rate for the past week

Prepare a network layout for a new site deployment


Cloud Control
WLSN Lab
Home
Meraki
Security
ThousandEyes
Assistant
Canvas
Actions
Threads
Create new
Canvas overview
Today
Security, Policy & Access
Previous 7 days
how is the meraki org doing?
Show me all networks that are out of compl...
What is the overall health of my Meraki org...
how is my network doing?
Older
How is my organization doing?
Hey, Patrick
There are 43 new actions that require review.
Review actions
Ask anything
Show me health trends for the past 14 days
Which clients are having connection issues?
What are the top 5 sites by bandwidth utilization?
Get detailed configuration data across all devices
Show me authentication success rate for the past week
Prepare a network layout for a new site deployment
Assistant can make mistakes. Verify responses. Learn how the Assistant handles data at Assistant disclosures.

Global Overview
Organization
WLSN Meraki
Network
WLNS01-Fabric
Network-wide
Assurance
Switching
Wireless
Insight
Organization
Security
Automation
Access Manager
Find in Menu (⌘+K)

← Fabrics

# Fabric-WLSN (ASN: 65213)

Deployed | Last deploy: Success

Preview changes | Deploy

Summary | Device roles | VRFs | Border configuration | Fabric subnets

## Fabric devices

### Single role deployment

2 Deployed / 4 Total devices

| Border(s) | Leaf(s) | Spine(s) |
|---|---|---|
| 0 /4 | 2 /4 | 0 /4 |

### Multi role deployment

2 Deployed / 4 Total devices

| Border(s)/Leaf(s) | Border(s)/Spine(s) | Spine(s)/Leaf(s) | Border(s)/Spine(s)/Leaf(s) |
|---|---|---|---|
| 0 /4 | 2 /4 | 0 /4 | 0 /4 |

## Deployment summary

**Border configuration** 2 total
2 Deployed / 2 total configurations

**VRFs** 1 total
1 Deployed / 1 total VRFs

**Fabric subnets** 2 total
2 Deployed / 2 created subnets

**Underlay subnets** 0 total
0 Deployed / 0 total subnets

## Statistics

**BGP Peers**
0% healthy
Online: -
Offline: -

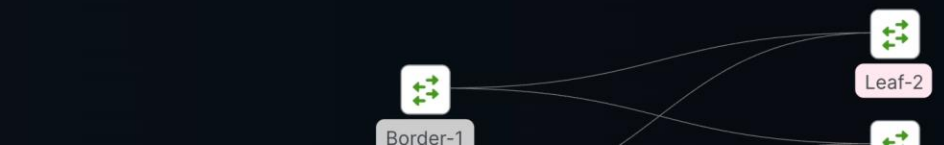
**Ext border peers**
0% healthy
Online: -
Offline: -

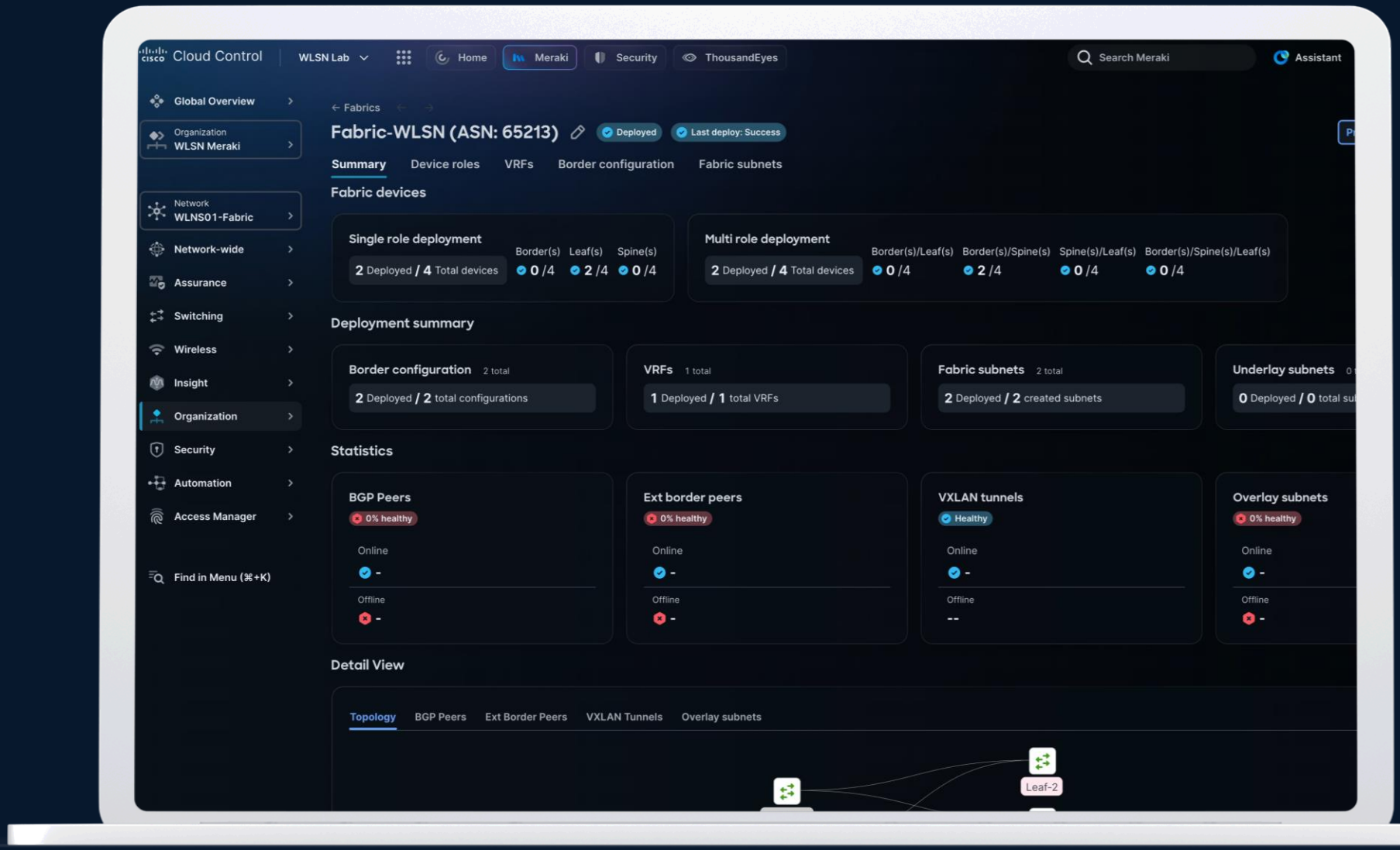
**VXLAN tunnels**
Healthy
Online: -
Offline: --

**Overlay subnets**
0% healthy
Online: -
Offline: -

## Detail View

Topology | BGP Peers | Ext Border Peers | VXLAN Tunnels | Overlay subnets





BETA JUNE 2026

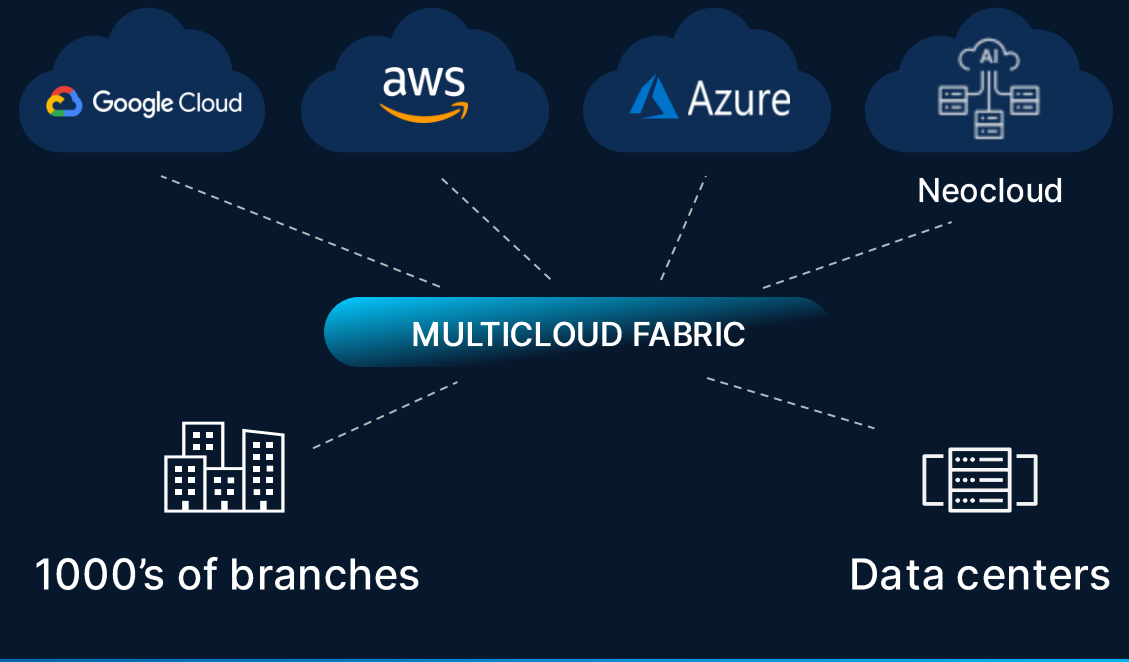
# Introducing Cisco Multicloud Fabric

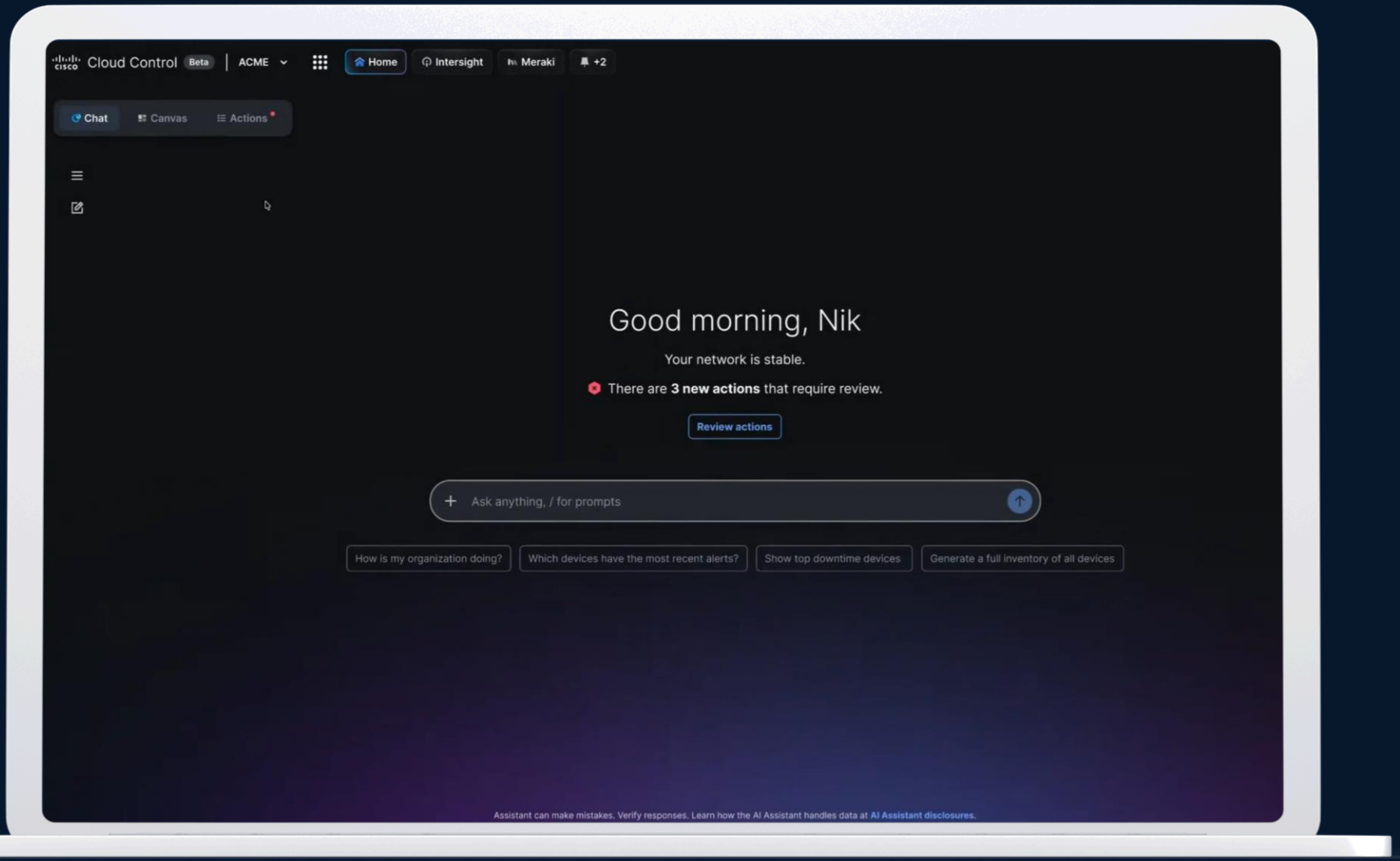
Single multicloud networking service – available via Cloud Control

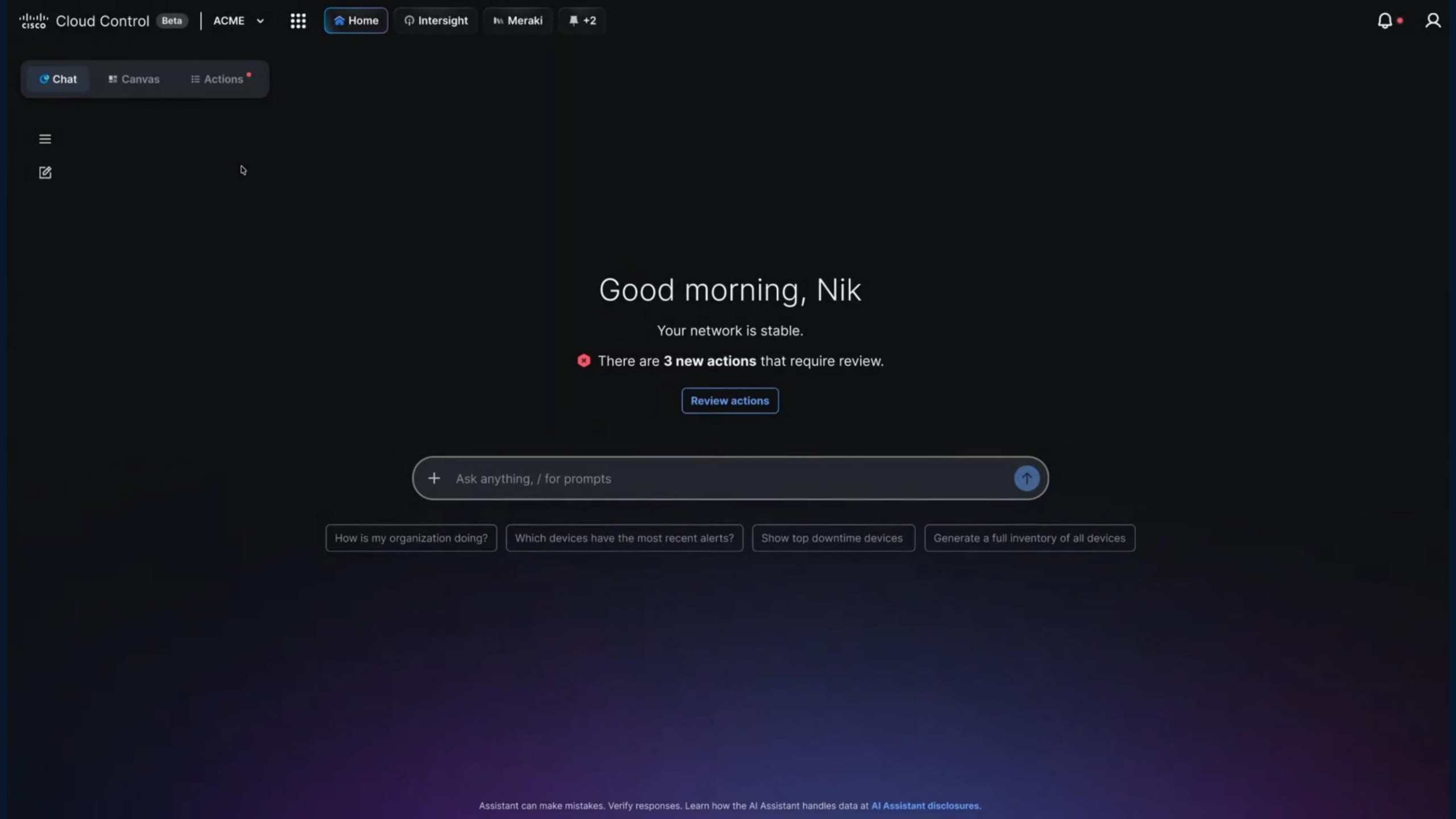
Instantly available global fabric across clouds

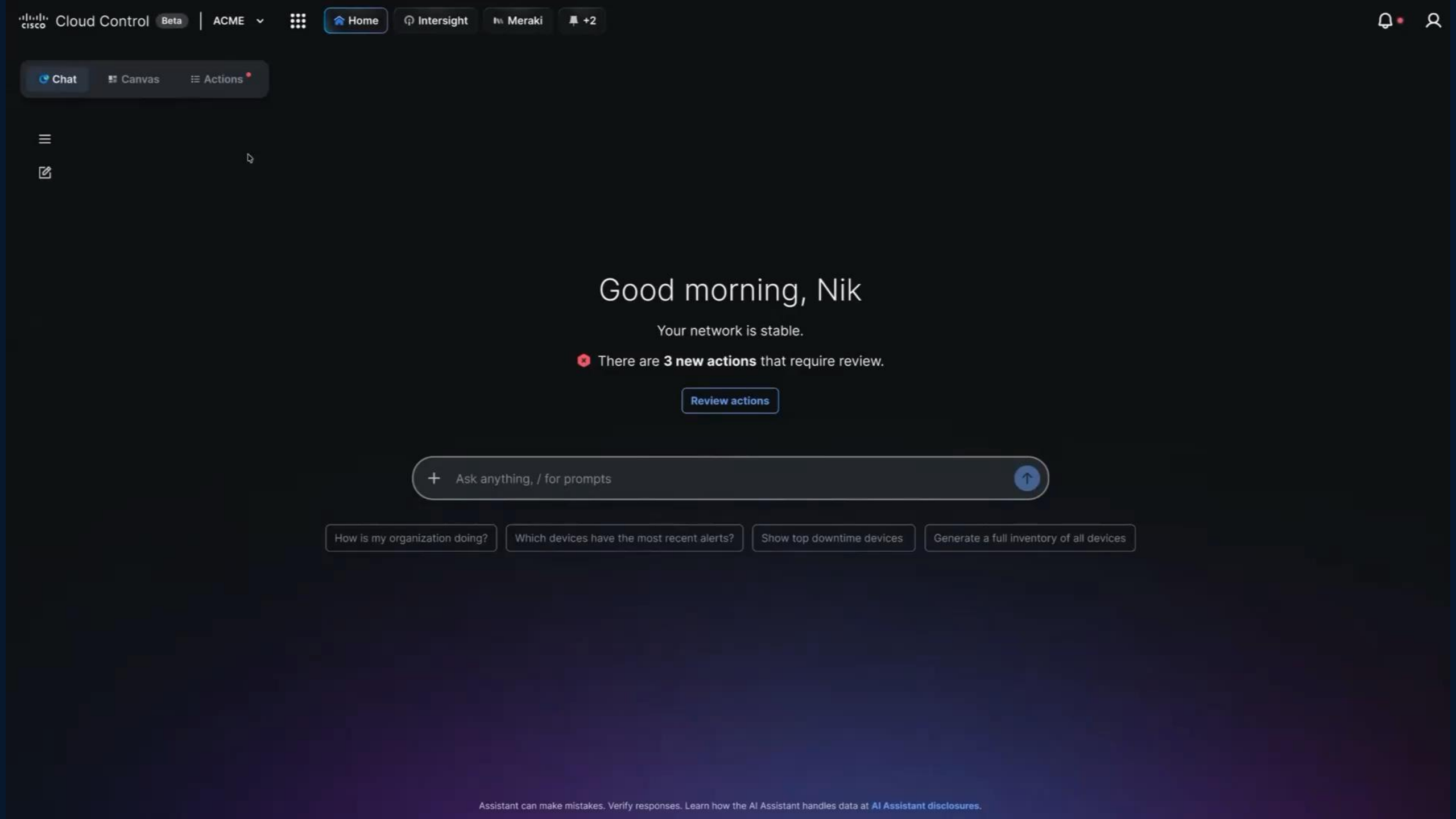
Built-in security and end-to-end visibility

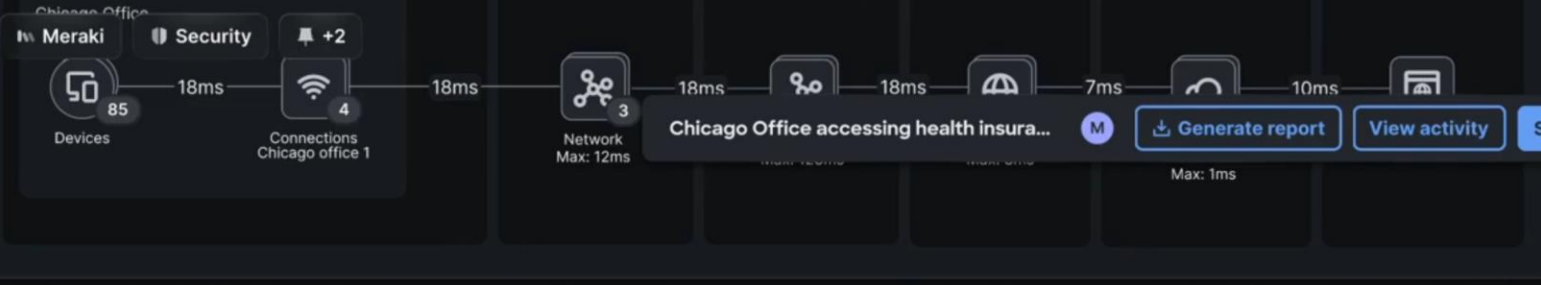
**Use Cases** Site-to-Cloud Cloud-to-Cloud






Cloud Control
Beta
ACME
Home
Intersight
Meraki
+2
Chat
Canvas
Actions
Good morning, Nik
Your network is stable.
There are 3 new actions that require review.
Review actions
Ask anything, / for prompts
How is my organization doing?
Which devices have the most recent alerts?
Show top downtime devices
Generate a full inventory of all devices
Assistant can make mistakes. Verify responses. Learn how the AI Assistant handles data at AI Assistant disclosures.


Cloud Control
Beta
ACME
Home
Intersight
Meraki
+2
Chat
Canvas
Actions
Good morning, Nik
Your network is stable.
There are 3 new actions that require review.
Review actions
Ask anything, / for prompts
How is my organization doing?
Which devices have the most recent alerts?
Show top downtime devices
Generate a full inventory of all devices
Assistant can make mistakes. Verify responses. Learn how the AI Assistant handles data at AI Assistant disclosures.




Chicago Office accessing health insura... | Generate report | View activity | Share

Chat | Canvas | Actions

Close Canvas

**AI Assistant** 11:05 am

I found several dependencies for **Health_quote_k8s.** Issue detected between the app and database **healthclaims-aurora-us-east-1** in AWS region **us-east-1** because of **security group** rule.

**Issue analysis**
When App Server attempting to query the Amazon Relational Database Service (RDS), the RDS Inbound Rule not allowing traffic from App Server. A recent security hardening update removed the App Server's access rule.

**Recommendation**
Navigate to the RDS Instance in your AWS cloud console.
**https://us-west-2.console.aws.amazon.com/rds/home?region=us-east-1#databases:**

Edit RDS Inbound Rule to allow traffic from the App Server's **Security Group ID sg-0a1b2c3d4e5f6g7h8**

Connectivity should be immediate once updated.

App dependency check
Multicloud Network | ThousandEyes Clo...

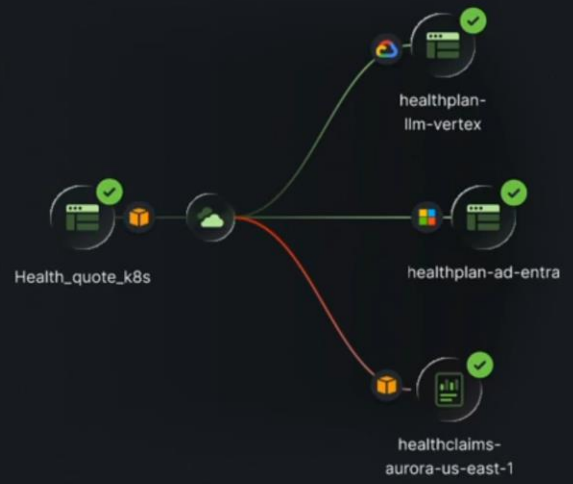
Ask anything, / for prompts

Auto

Assistant can make mistakes. Verify responses. Learn how the AI Assistant handles data at **AI Assistant disclosures.**

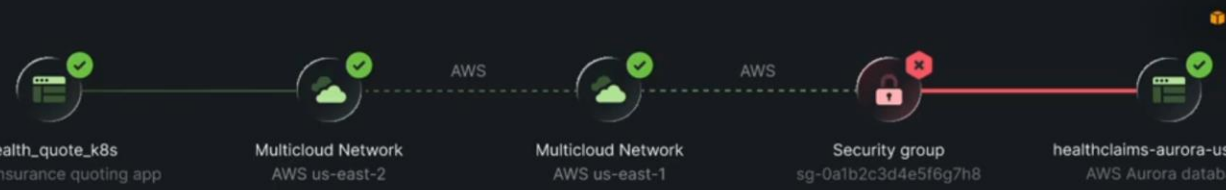
## App dependency check

Multicloud Network | ThousandEyes Cloud Insights

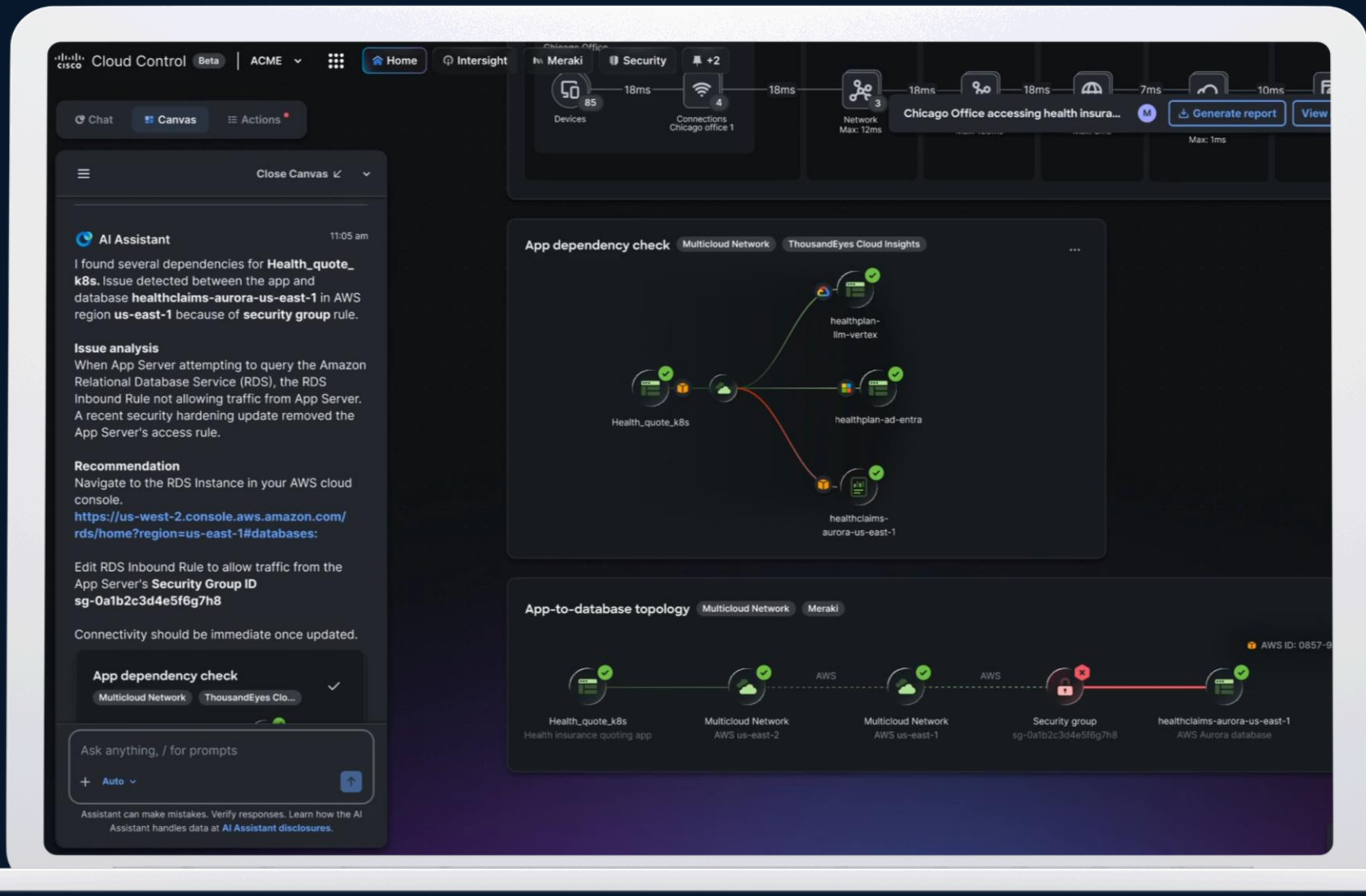



## App-to-database topology

Multicloud Network | Meraki




70%



Secure Networking

# Extended Ecosystem

5

## Extended Ecosystem

Sharing device & flow analytics with external management tools

Marketplace

# One platform. Every tool you need

## Fast time to value

Pre-built, ready-to-deploy solutions. Go live in minutes, not months.

## Work with your existing tools

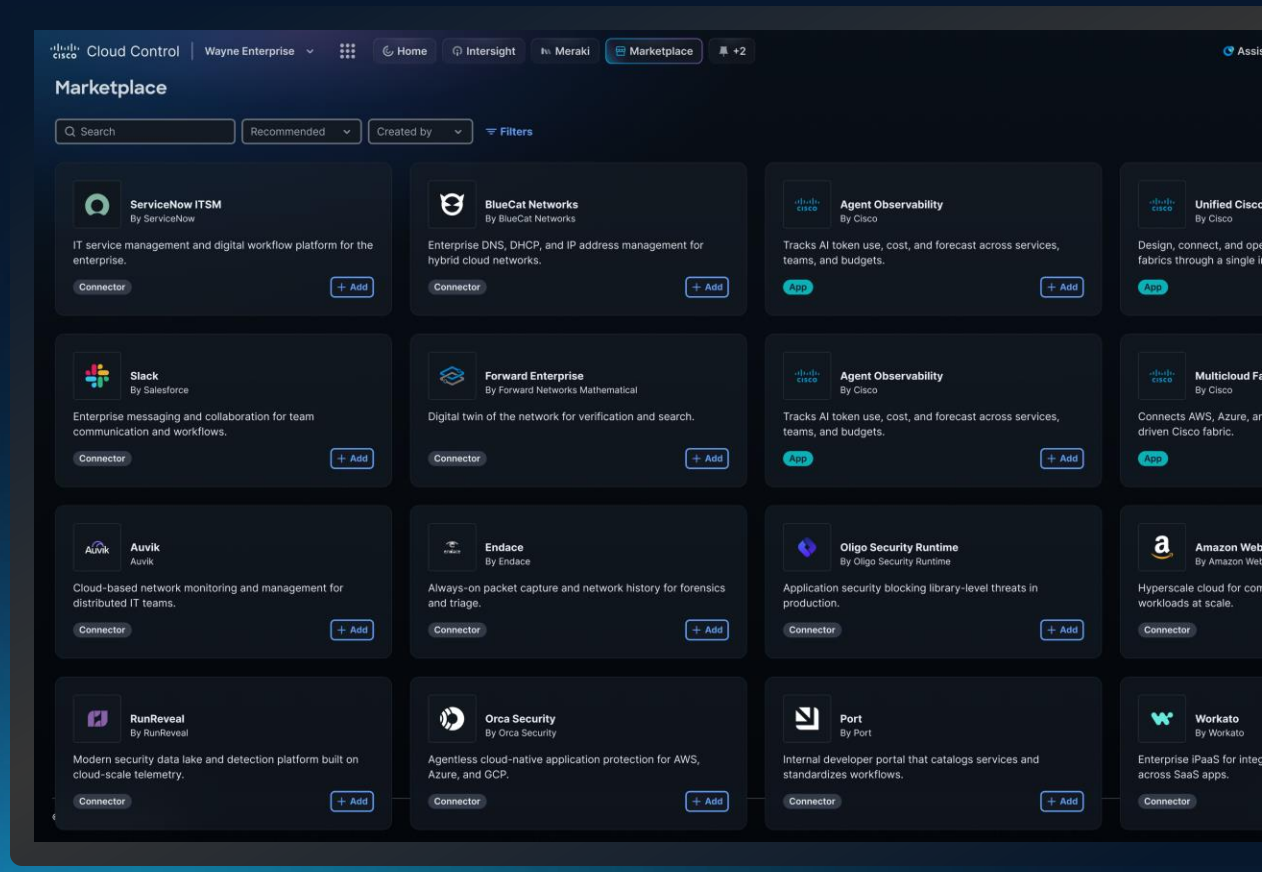
ServiceNow, Azure, Slack, Webex, and many more.

## Built for your team

Solutions tailored for Network Admins, IT Ops, MSPs, and System Integrators

## Trusted & secure

Admin-controlled installs, pre-deployment validation, and centralized alerts



# Closing / Next Steps

# Secure Networking v1.0

FYI


This is our first cross-domain and end-to-end Cisco reference architecture in the modern era!

- Version 1.0 delivers 'Secure Networking' outcomes
  - Many Domains, PINs, Products & Protocols
  - Based on the currently available Products
  - There are some challenges, limits and gaps
- We will continue to evolve in the future* (v2.0+)

SNRA v1.0 Versions:

- IOSXE 26.1.(latest)
- Meraki Q2CY26 (latest)
- Catalyst Center 3.2.1.(latest)
- SDWAN Manager 20.18.2.(latest)
- ISE 3.5.(latest)
- TE Q2CY26 (latest)
- SNA 7.6.(latest)
- FMC 10.0.(latest)
- SCC Q2CY26 (latest)

CISCO VALIDATED DESIGN

* Feature Roadmap aligned to SNRA

# Call to Action

Implementing SNRA – Layer by Layer

5 Extended Ecosystem

4 Unified Mgt & Agentic Ops

3 Zero Trust & Common Policy

2 Scalable Segmentation

1 Secure Infrastructure

## CHECKLIST

### Increase overall Visibility & Observability

- leverage the robust ecosystem of Cisco and third-party tools and data-sources to increase observability and integrate multiple support systems.

### Simplify Ops with Unified Tools & AI

- consistently deploy fabrics globally, leveraging a unified management experience, with model-driven programmability and Agentic Ops.

### Embrace secure ZTNA & Common Policy

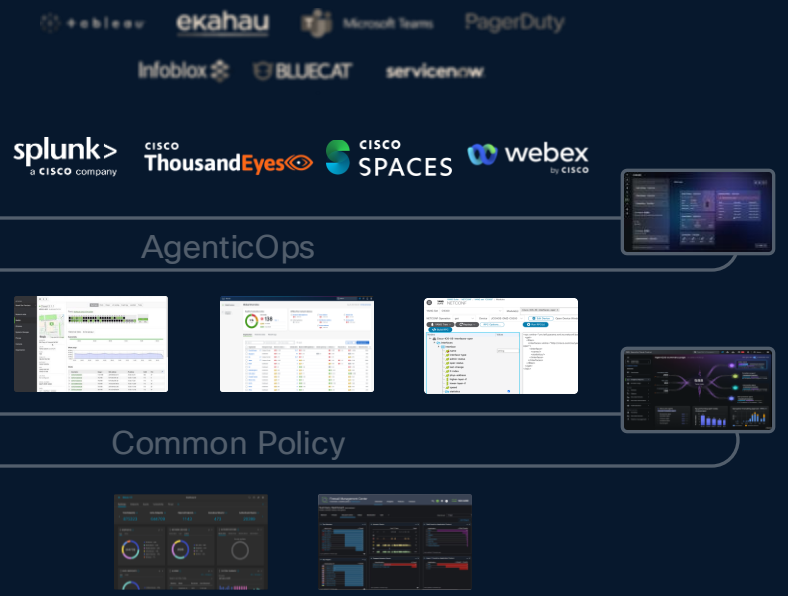
- employ easy endpoint identification & authentication, integration of hybrid mesh firewall, with end-to-end identity-based common policy.

### Migrate Traditional to Fabric Overlay

- leverage network automation to simplify migration, implementing consistent design, and using an incremental site-by-site approach.

### Refresh to latest Cisco Secure products

- install scalable devices, with security fused in, using Unified Hardware, Unified Software, Unified Licensing & Unified Support.



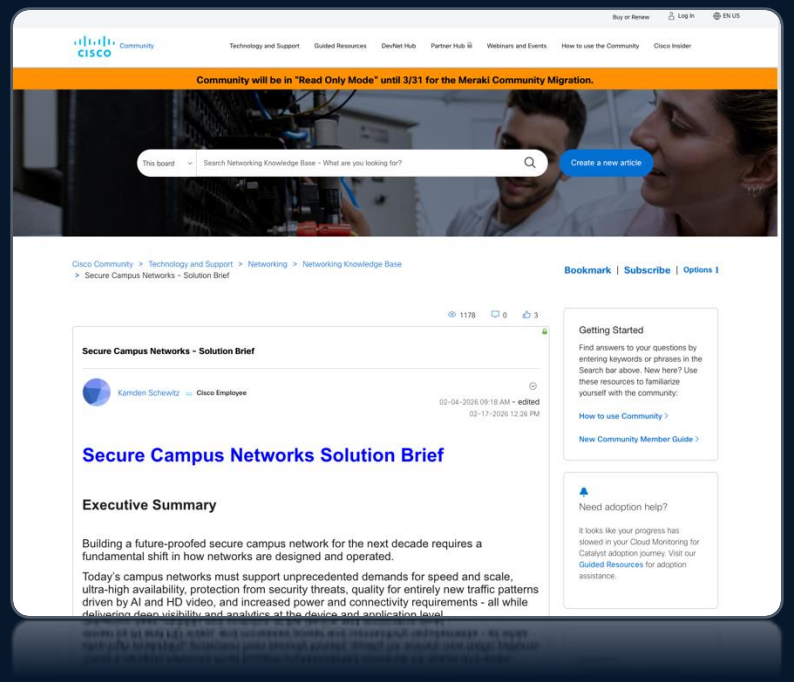


Scalable Wi-Fi 7 | Smart Switches | Secure Routers | Secure Firewall

FYI

# Secure Networking Resources

Start your Secure Network Reference Architecture




## Public SNRA References

- Secure Networking Overview
- Secure Campus & Branch Networking
- Secure Campus Networks – Solution Brief

Published

## New SNRA Cisco Validated Designs

- Secure Network Reference Architecture – End-to-End Architecture Guide
- Secure Network Reference Architecture – Cloud-managed Design Guide
- Secure Network Reference Architecture – On-Premises Design Guide
- Secure Network Reference Architecture – Programmable Design Guide

Published

June 2026

## Related References

- BRKENS-2614 - Campus Design with Secure Network Reference Architecture

June 2026

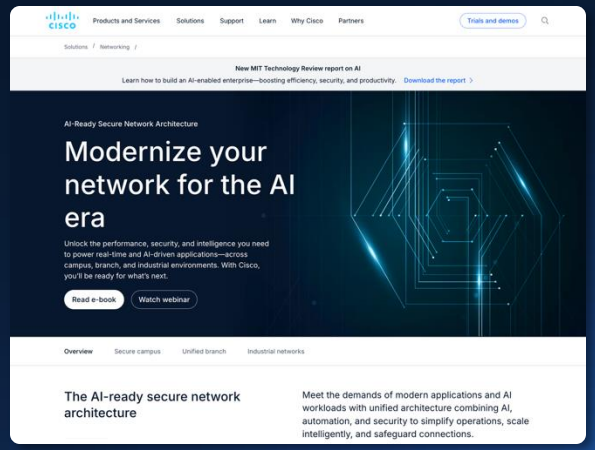
## Existing Cisco Validated Designs

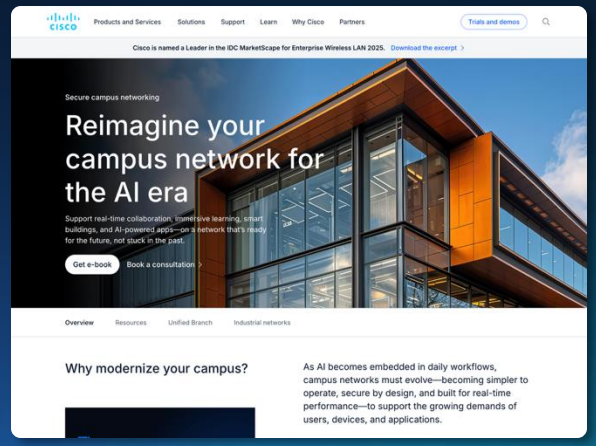
- Cisco Cloud Fabric Validated Case Study — New
- Cisco SD-Access Design Guide — New
- Cisco Unified Branch Design Guide — Updated
- Cisco Common Policy Integration Guide — Updated

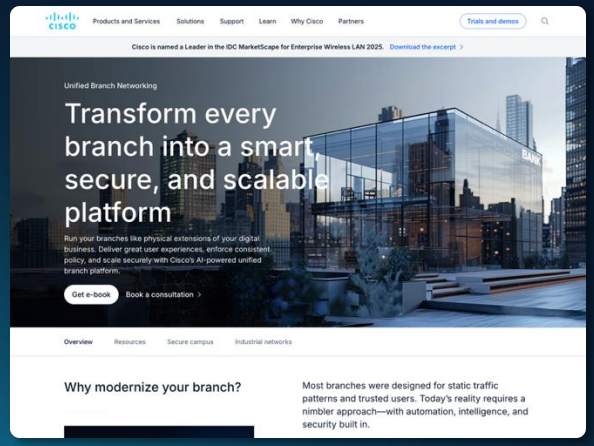
FYI

# *Secure Networking* on Cisco.com


www.cisco.com/site/us/en/solutions/transform-infrastructure/secure-networking-overview.html




www.cisco.com/site/us/en/solutions/networking/campus-branch-networking/index.html

# Thank you


CISCO