

# Managed AI SASE for the AI era: HKBN's AI security fabric

**Jackal Chau**

General Manager of Technology Business,  
HKBN Enterprise Solutions

**Ranganath Balasubramanyam**

APJC SASE Technical Leader  
Cisco



# Who Are We?



Jackal Chau

General Manager - Technology Business  
HKBN Enterprise Solutions

- **Professional Experience:** Over 20 years of experience in the IT industry, including 4 years with HKBN
- **Leadership Role:** Leads a team of more than 1200+ technology professionals, overseeing service delivery and operations across Hong Kong and Mainland China.
- **Areas of Expertise:** Specializes in AI, cybersecurity, multi-cloud solutions, managed services, and enterprise infrastructure transformation.
- **Leadership Philosophy:** Passionate about driving customer success through innovation, operational excellence, and secure digital transformation.



Ranganath Balasubramanyam

APJC SASE Technical Leader  
Cisco

- **Core Experience:** 20 years of hands-on and management experience in tech (IT, networking, telecom), including 13 years at Cisco.
- **Global Exposure:** Extensively traveled and worked with major global companies across the USA, UK, Malaysia, Australia, New Zealand, China, Hong Kong and Japan.
- **Key Skills:** Strong leadership in engineering, client relations, marketing support, and vendor/alliance management.
- **Core Philosophy:** Focuses on technology driving, relationship building, teamwork, and customer success.

# AI Revolution and the Hybrid Workplace: From Productivity Shift to Security Challenge

## AI Revolution Challenge

- Generative AI shifted from experimental technology to a boardroom priority overnight.
- This forced an immediate re-evaluation of human-centric workflow.
- It also redefined what productivity means for the modern enterprise.
- The transition happened faster than most organizations could plan for, leaving leaders to adapt at the same pace as the technology.

## AI Reshapes Hybrid Workflow and Productivity

- The hybrid workspace is where this challenge becomes real.
- People work everywhere, across office, home, and mobile environments.
- They access everything, from enterprise applications to cloud and AI services.
- At the same time, they expect both seamless experience and consistent protection.
- Security can no longer depend on a fixed network edge or a single location.

The question is no longer if you will adopt AI – It's how securely you will get there.

# AI Is Transforming the Business – Bring Us the new Security Risk

## ***Generative AI Explosion***

Employees across every department are adopting GenAI tools at unprecedented speed — often without IT visibility or governance policies in place.

## ***Data Privacy at Risk***

Sensitive corporate data, customer records and regulated information are being submitted to AI models — creating serious compliance and breach exposure

## ***Shadow AI***

Unsanctioned AI application bypass security controls entirely, making it nearly impossible for IT teams to enforce data protection policies

## ***Expanding Threat Landscape***

AI-powered cyberattacks are becoming more sophisticated, faster, and harder to detect — and traditional defenses simply cannot keep pace.

# Cisco + HKBN Will Be Your Solutions

## Intelligent Steering of AI Traffic (SD-WAN + NBAR)

- Automatically identifies and classifies AI traffic
- Routes traffic to the fastest path for low latency

## Understands AI Intent (Secure Access + AI Defense)

- Inspect AI interactions in real time
- Visibility into LLM and MCP communications
- Protects with supply chain, read teaming and runtime guardrails

## HKBNES Delivers

- High-Speed, Low-Latency Fiber Backbone
- 7x24 Active SOC Monitoring (Human + AI)
- One-Stop-Shop with Local Expertise

## HKBN AI SASE-Powered Managed Service

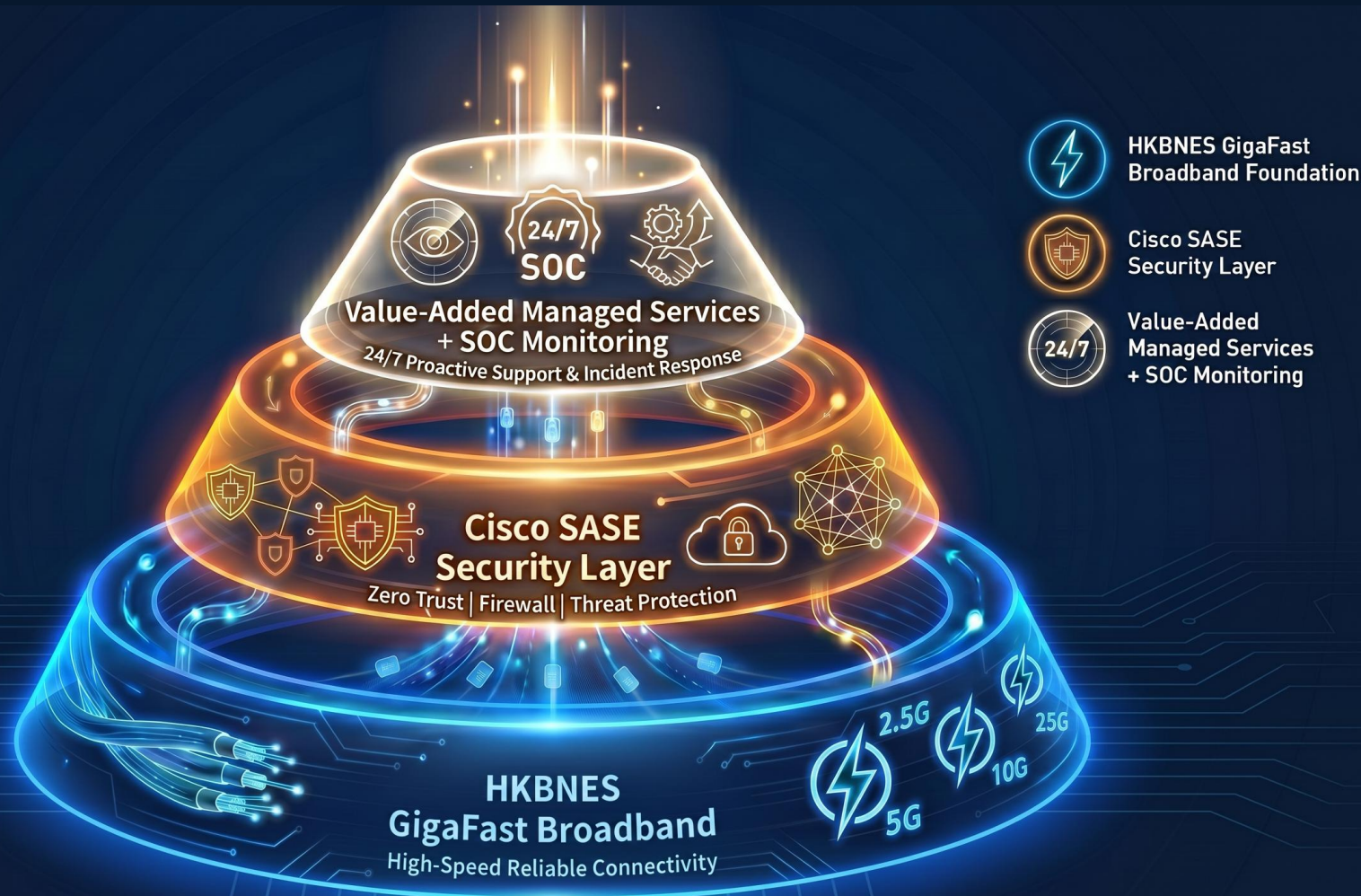
# HKBN AI SASE-Powered Managed Service

## Agenda:

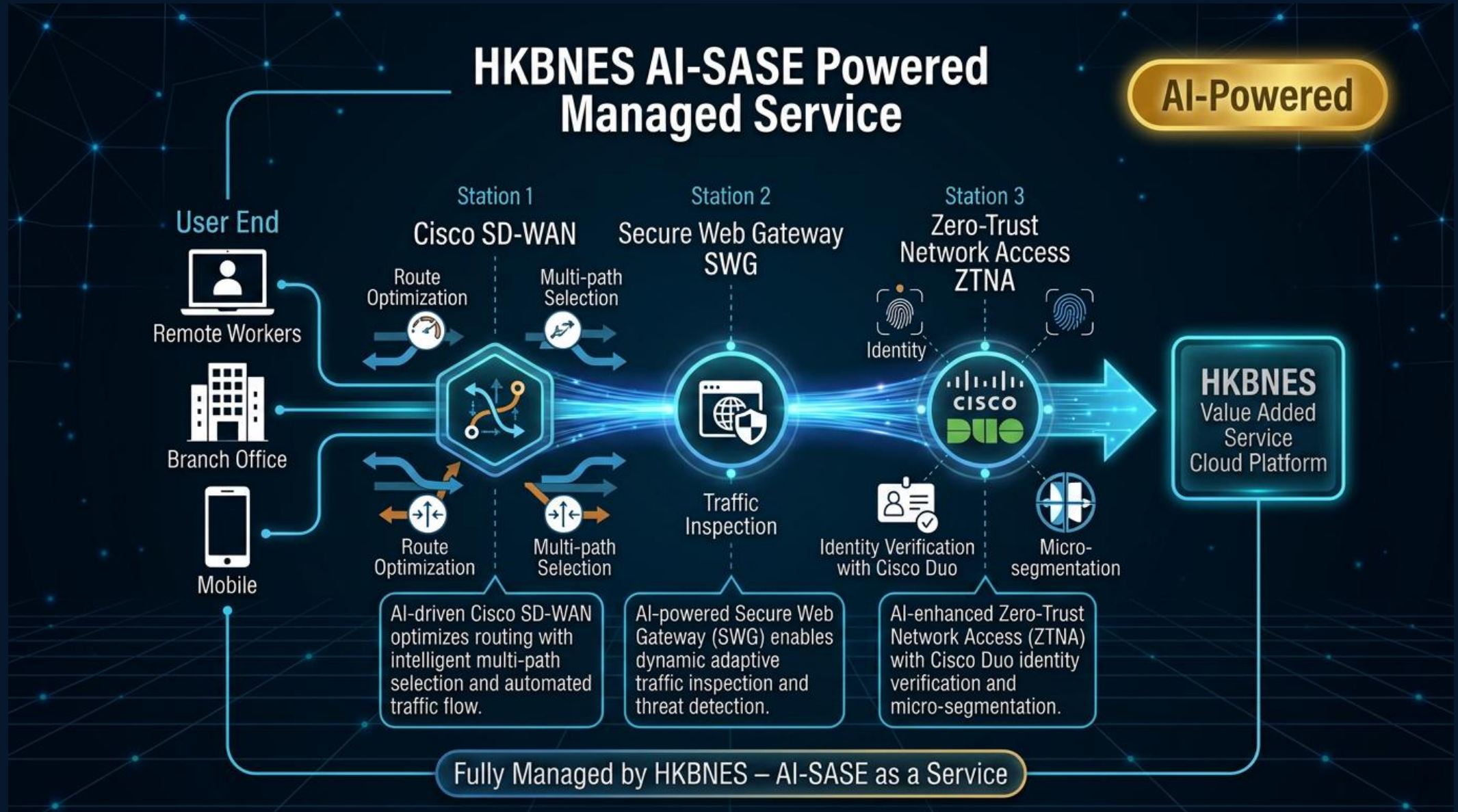
- The Power of Cisco SASE Integration
- From the Foundation – Connectivity for AI Era
- Our Managed Services Edge – Enterprise Design, 24x7 SOC, Local Support

# HKBNES AI SASE-Powered Managed Service Stack

Converges network and security capabilities into a single cloud-delivered framework – eliminating complexity, reducing costs and dramatically improving visibility.



# The Power of Cisco SASE Integration with HKBN



# From the Foundation – Connectivity for AI Era

HKBN's GIGAFAST Broadband and high-speed backbone provide the stable, low-latency path that Cisco SASE needs for optimal performance

## GIGAFAST Broadband —Built for the AI Era

**Secure Access Service Edge (SASE)** relies heavily on internet quality. If the underlying network pipe is congested, security tools will feel slow to your employees.

**HKBN's High-Speed Backbone:** We provide the low-latency, high-performance fiber underlay that guarantees your AI traffic and user data travel fast and reliably.

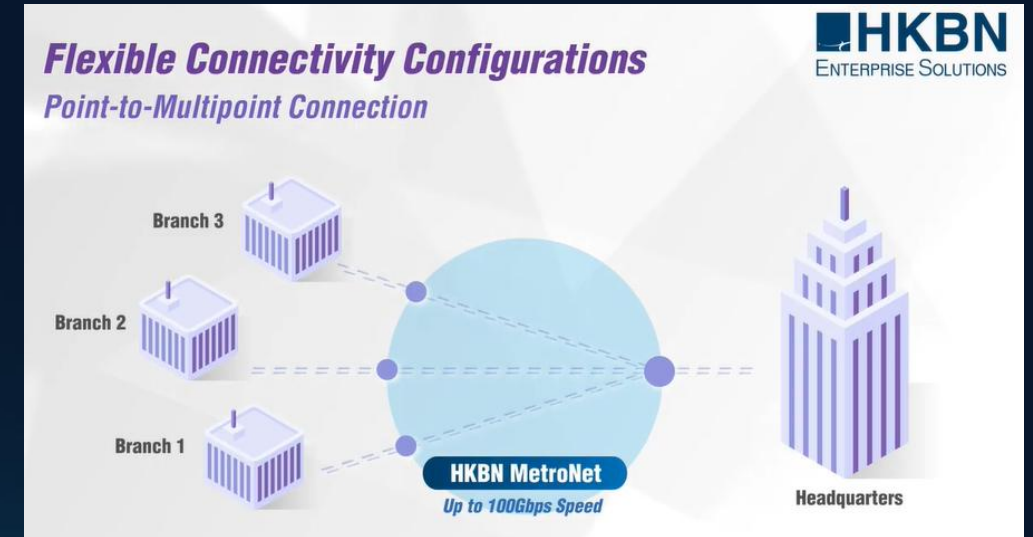
Think of it as the **express highway** for both your digital workforce and your AI engines. No congestion, no delays.



# 100Gbps MetroNet – The Ideal Underlay for Your Cisco SASE Solution

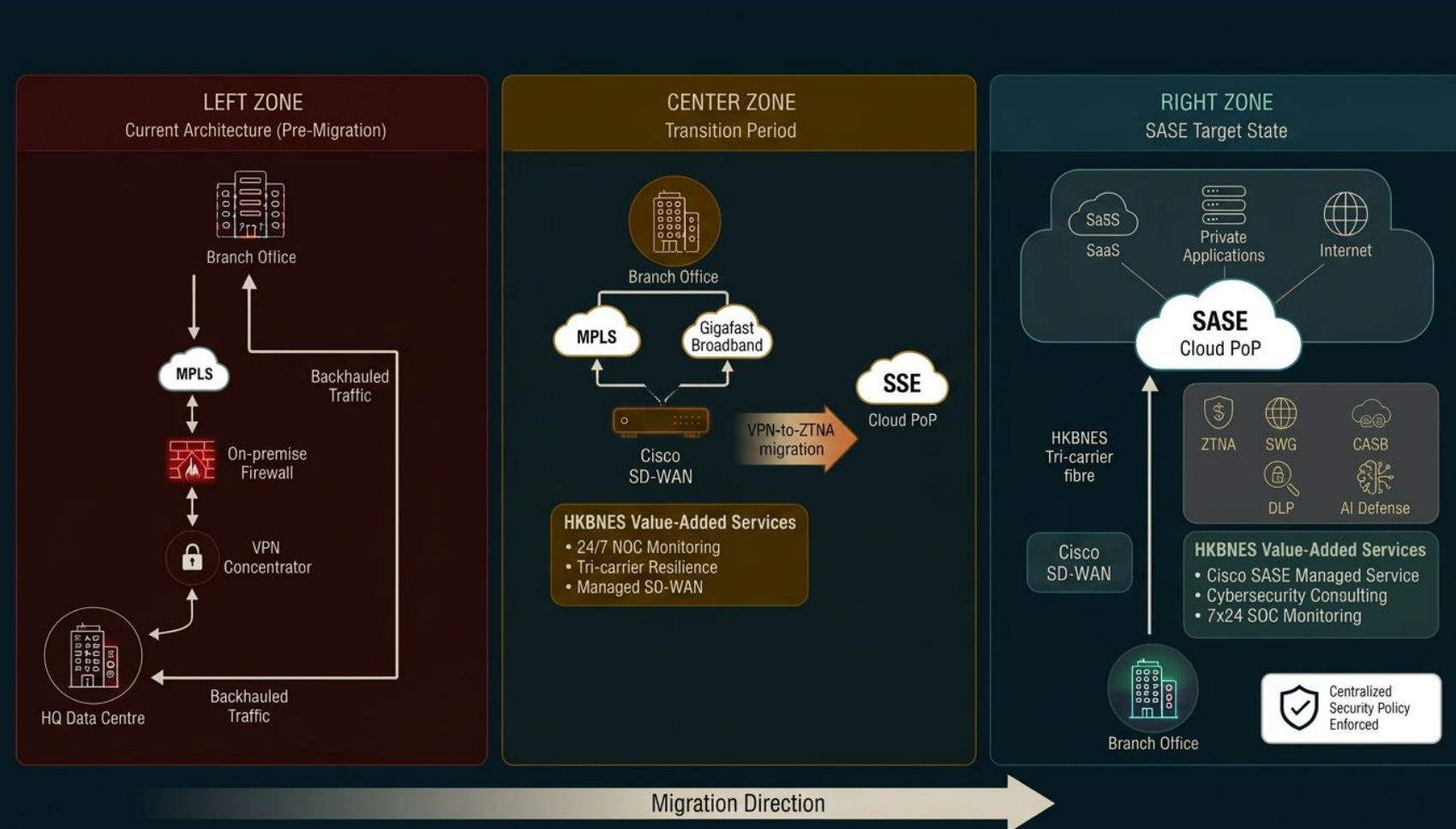
## Why HKBN MetroNet Is the Perfect Foundation for Your Cisco SASE Investment

- Gartner reports that **45% of enterprises face SASE performance challenges due to inadequate network infrastructure.**
- SASE success depends heavily on **low-latency, highly available underlay connectivity.**
- SD-WAN can optimize traffic paths, but it **cannot create performance out of an unreliable line.**
- HKBN MetroNet provides exactly this reliable, high-performance "expressway" for your SASE deployment.



# Migrating a Branch to SASE – The HKBNES Way

- Legacy environments come with real constraints: aging MPLS circuits, on-premise security appliances, varied branch configurations, and teams that can't afford downtime. HKBN's deployment methodology is designed to accommodate that complexity while moving enterprises decisively toward a cloud-native, zero-trust architecture.
- Each phase is managed end-to-end by HKBN's certified Cisco engineers, with clear milestones, risk mitigation checkpoints, and communication protocols that keep IT and business stakeholders aligned throughout the transition



# 7x24 SOC Monitoring

Tools alone don't stop threats. Eyes on glass – around the clock. HKBNES's Security Operations Center provides the human and automated intelligence layer that turns Cisco SASE telemetry into decisive action.



## Continuous Threat Monitoring

HKBNES SOC analysts monitor SASE environment 24 hours a day, 7 days a week, 365 days a year – detecting anomalies, correlating events, and triaging alerts before the incidents have been escalated.



## Real-Time Alert Response

When Cisco SASE surfaces a threat signal – whether a policy violation, a ZTNA anomaly, or a suspicious SWG event – HKBN's SOC doesn't just log it. Analysts investigate, validate and initiate the appropriate response workflow immediately.



## Managed Tools & Intelligence

HKBNES provides and operates the full Cisco SASE toolchain – SIEM integration, threat intelligence feeds and automated playbooks – so enterprise gain enterprise-grade security operations without building an internal SOC from scratch.

# One-Stop Managed Service – Simplifying Your Cisco SASE Journey

## The HKBNES Difference – Why Choose Our Managed Service

### What You Get

### Why it Matters

One partner for everything

Connectivity (MetroNet backbone), security (Cisco SASE), hardware, and managed support – all from one provider

Local expertise

1,200+ engineers. 1,300+ certifications

24/7 SOC

We see issues before you do – proactive alerts and rapid resolution

Coordinated support

One team manages everything – no vendor handoffs, no delays, one resolution path for all issues

# The Unified Branch & AI

Ranganath Balasubramanyam  
APJC SASE Technical Leader

July 2026





Need to do more with  
less



Workers and workloads  
live everywhere



Opportunities and threats  
of AI

# A resilient, secure branch is critical for delivering exceptional consumer experiences



Need for fast, reliable  
Wi-Fi and internet  
connection



Workloads shifting to  
SaaS, public cloud,  
and data center



No local IT support –  
increase the need for  
operational simplicity



Post-quantum  
cryptography

# Our approach: Architecture for the AI-ready Unified Branch



**Simplified operations,  
powered by AgenticOps**



**Security fused into  
the network**



**Scalable devices  
ready for AI**

Unified Branch

# Deploy branches in minutes, manage at scale

Unified Branch automation toolkits



## Cisco validated design

Blueprints for full stack  
branch architecture

Available

## Agentic workflows

Automated script to  
deploy a validated design

Available

## Branch-as-code

Programmable infrastructure  
deployed using code

Available

Begin your AI powered automation journey with Agentic Ops:  
AI Assistant & Agentic Workflows

# Approach to Universal ZTNA

## SASE Evolution

Secure  
SD-WAN

+

Security  
Service Edge

+

Trusted Identity  
Edge

SINGLE-VENDOR SASE

End-to-end visibility and assurance

# The network's new role



Of network engineers  
have security as part of  
their remit\*



**98%** of IT leaders say secure networking is important to operations and growth



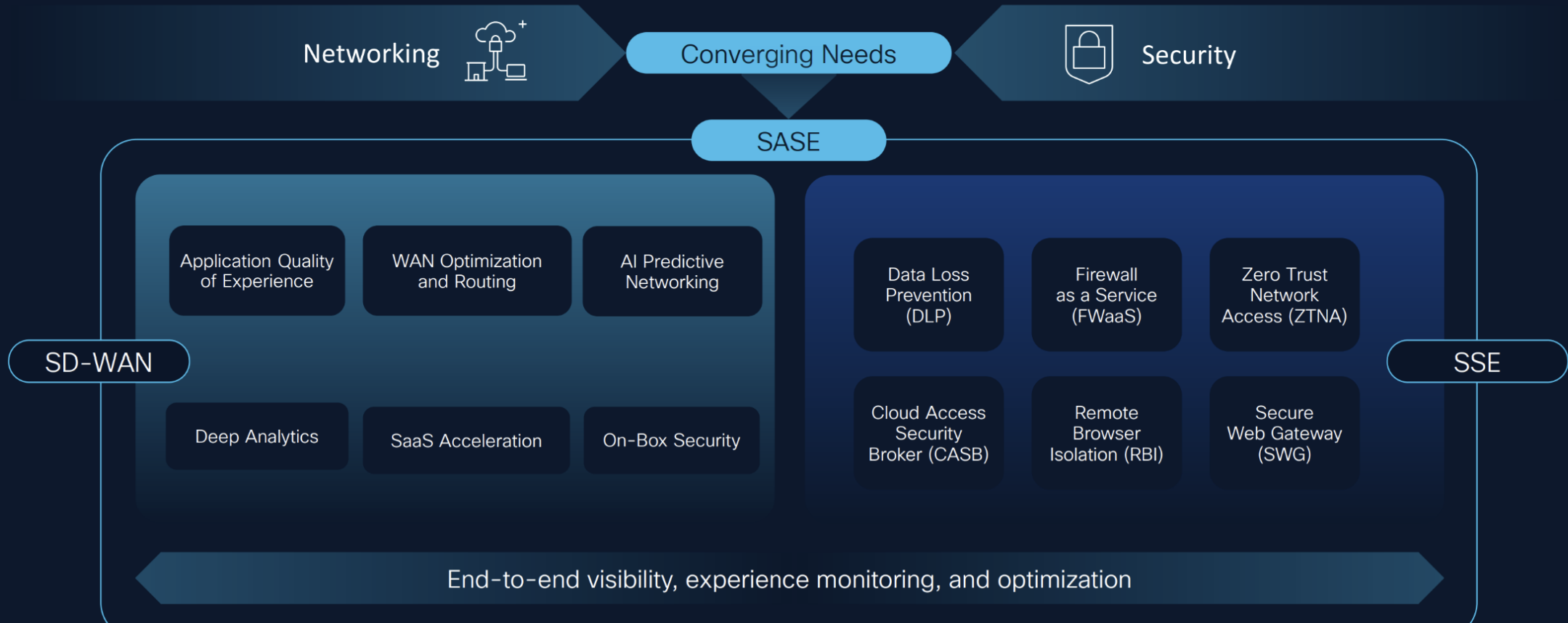
**94%** believe a modernized network will enhance cybersecurity



**42%** recognize integrating network and security as a key area requiring significant improvement

# Secure Access Service Edge (SASE)

*The architecture for a securely connected experience in today's hyper-distributed environment*



# Cisco Secure Access: Built Around What Matters Most

Five Areas of Protection and Simplicity



Secure the Internet & Web: Block threats before they reach your users



Secure Private Access: Connect users to apps safely, from anywhere



Protect Your Data & Cloud Apps: Control what leaves and where it goes



Identity & Trust: Know who your users are at every moment



Simplify Operations: One console. One client. One policy.

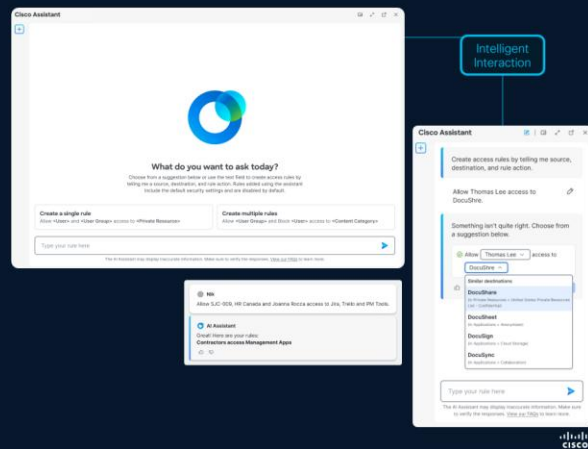
# AI driven SASE Innovation

## Policy Assistant

Let AI do the heavy lifting

### Simplified Experience

- Infer Required access based on language input at prompt
- Reduce rule creation time by up to 70%
- Default disable to ensure administrator has ability to review generated content



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

## Visibility: AI Cloud Visibility Security for AI

- Automatically uncover AI assets, in the cloud, and SaaS
- Understand usage and relative risk status
- Dive into details and compensate with controls

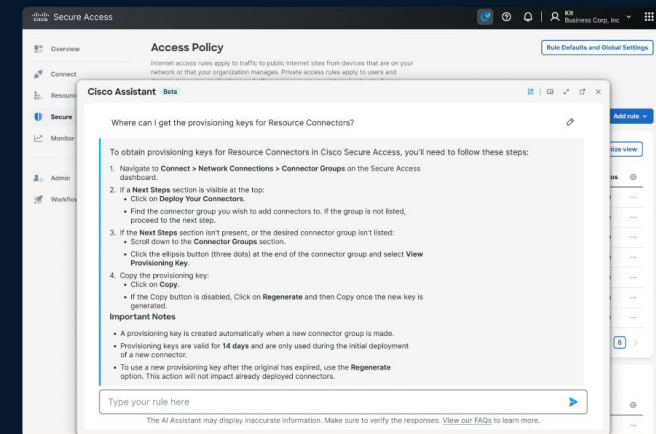
| App Discovery <span>Secure Access</span>                                                                                                                                         |                                          |                                           |                                   |            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-------------------------------------------|-----------------------------------|------------|
| Use Secure Access to identify third-party generative AI applications, their usage, risk score, and protection status. <a href="#">Learn more about AI application discovery.</a> |                                          |                                           |                                   |            |
| <input type="text" value="Search"/>                                                                                                                                              | <input type="text" value="Subcategory"/> | <input type="text" value="Content type"/> | <input type="text" value="Risk"/> |            |
| Application name                                                                                                                                                                 | Sub-category                             | Content type                              | Risk status                       | Identities |
| <a href="#">Microsoft Copilot</a>                                                                                                                                                | Search                                   | Conversational Chat                       | Low                               | 2          |
| <a href="#">OpenAI ChatGPT</a>                                                                                                                                                   | Search                                   | Conversational Chat                       | High                              | 3          |
| <a href="#">You.com</a>                                                                                                                                                          | New Office Productivity                  | Multimodal Content Generator              | Medium                            | 2          |
| <a href="#">Backyard AI</a>                                                                                                                                                      | New Content Management                   | Conversational Chat                       | Medium                            | 2          |
| <a href="#">GitHub Copilot</a>                                                                                                                                                   | New Application Development and Testing  | Code Assistant & Generator                | Low                               | 1          |
| <a href="#">Google Bard</a>                                                                                                                                                      | New Search                               | Conversational Chat                       | Low                               | 1          |

## Documentation Assistant

Personalized answers at your fingertips

### Ease of Use

- Personalized answers based on conversation
- Complete knowledge of Secure Access and its features
- Guide you with process or explain features
- Provide caveats and disclaimers when necessary
- We are used to keyword matches – it's a skill, but now we don't need to worry about that



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

# Introducing

## Cisco 8000 Series Secure Routers for the AI-powered unified branch

- Cisco designed secure networking processor supports increased traffic
- Post-quantum security ready
- Advanced routing and next-generation firewall
- Built for secure SD-WAN and SASE



# The Power of Cisco 8000 Series Secure Router

## Hardware Innovation & Network Connectivity

### Secure networking processor



HW accelerated  
Security & Networking

### Fanless model



Small, medium, large  
branch

### 25GE WAN



Campus Router

### Tamper Detection



Physical (open chassis)  
Intrusion Detection

### Secure Boot



Post-Quantum  
Safe (Future)

### Dying Gasp



Small, medium, large  
branch

### mGig/10GE



Migration from 1GE

### NIST Compliant PQC



Ready for  
IPsec/MACsec

# Secure your network at every size and location

| AVAILABLE                                                                        | AVAILABLE                                                                         | AVAILABLE                                                                          | AVAILABLE                                                                           | AVAILABLE                                                                           | AVAILABLE                                                                           |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|  |  |  |  |  |  |
| Cisco 8100 Series Secure Routers                                                 | Cisco 8200 Series Secure Routers                                                  | Cisco 8300 Series Secure Routers                                                   | Cisco 8400 Series Secure Routers                                                    | Cisco 8500 Series Secure Routers                                                    | Cisco 8600 Series Secure Routers                                                    |
| Small Branch                                                                     | Medium Branch                                                                     | Large Branch                                                                       | Campus                                                                              | Data Center                                                                         | Data Center                                                                         |
| IOS XE                                                                           |                                                                                   |                                                                                    |                                                                                     |                                                                                     |                                                                                     |
| AVAILABLE                                                                        | AVAILABLE                                                                         | AVAILABLE                                                                          | AVAILABLE                                                                           | AVAILABLE                                                                           | AVAILABLE                                                                           |
| MX                                                                               |                                                                                   |                                                                                    |                                                                                     |                                                                                     |                                                                                     |
| AVAILABLE                                                                        | AVAILABLE                                                                         | AVAILABLE                                                                          | AVAILABLE                                                                           | -                                                                                   | -                                                                                   |

# Major Global Sports Brand in Greater China

Cisco SD-WAN and SSE win across 300 stores in China

## Customer Challenges



- 1. Rapid, flexible network deployment for a global store network.
- 2. Dispersed security systems causing inefficient management.
- 3. Large device scale complicating lifecycle management.
- 4. Complex cross-regional compliance, especially in China.

## Cisco solution

Meraki SD-WAN, Cisco Secure Firewall, and Secure Access in a [single platform](#).

- ✓ Integrated Application Acceleration
- ✓ Visibility Included
- ✓ Simplified Single-Dashboard with AI Ops

## Remote Access Unification and Smooth Migration

Cisco AnyConnect users can migrate smoothly to CSA without redeploying Cisco Secure Client, reducing risks and ensuring business continuity.

## Boundary Business Isolation (Secure Firewall):

Cisco Secure Firewall creates fine-grained internal network segmentation and centralized policy management across Greater China for enhanced security.



### Performance

Integrated WAN optimization ensures speed for critical apps.

WAAS Integrated



### Security

Built-in Cisco Secure Access

SASE integrated



### Visibility

ThousandEyes provides end-to-end network insight.

ThousandEyes



### Simplicity

Single platform reduces hardware footprint & ops cost.

Single Platform

# Large Electronics Service in Korea | Integrated Architecture & Business Value

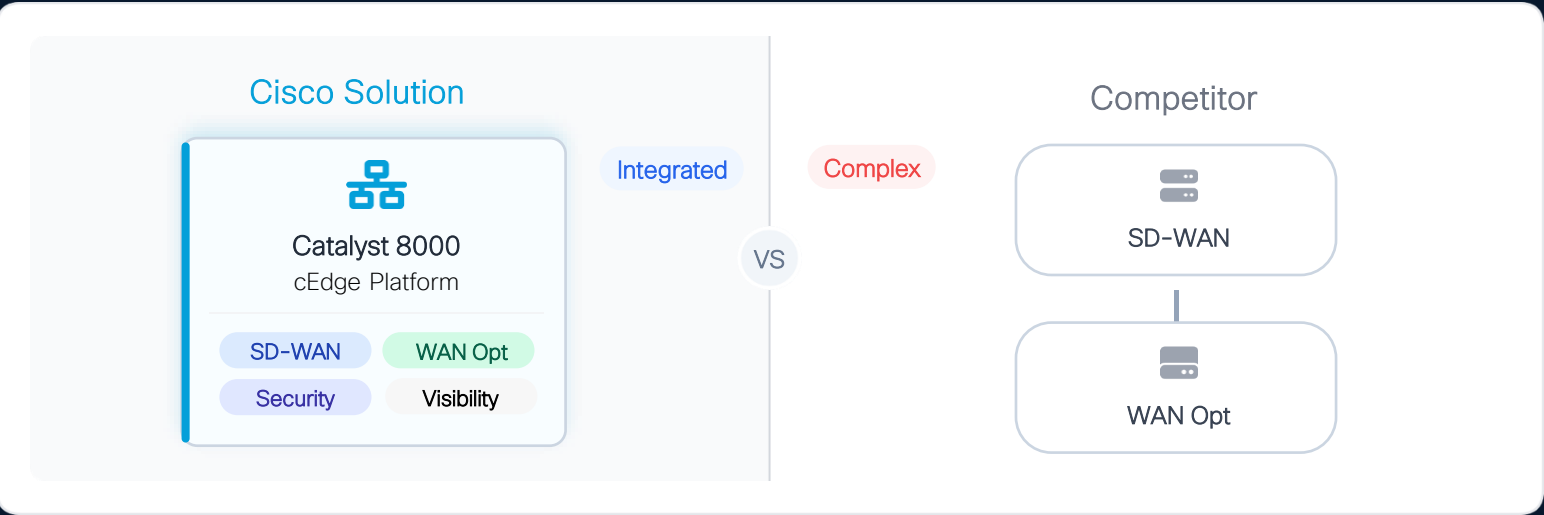
## Cisco solution

Catalyst 8000 cEdge delivered SD-WAN, Security, and WAN Optimization in a **single platform**.

- ✓ Integrated Application Acceleration
- ✓ ThousandEyes Visibility Included
- ✓ Simplified Single-Dashboard Ops

## Why Competitors Failed

Competitor required a **separate appliance** to meet WAN optimization needs. This "two-box" solution increased complexity, point of failure, and management overhead.



## Performance

Integrated WAN optimization ensures speed for critical apps.

**WAAS Integrated**



## Security

Built-in Cisco Secure Access (Umbrella) protection.

**SASE Ready**



## Visibility

ThousandEyes provides end-to-end network insight.

**ThousandEyes**



## Simplicity

Single platform reduces hardware footprint & ops cost.

**Single Platform**

## Commercial Model

72-Month MSEA  
Optimized TCO Structure

## Future Opportunities

Contact Center  
SD-WAN Expansion

Nationwide Full SASE  
Security Expansion

# The Talent Gap is Real

Specialized cybersecurity talent in Hong Kong is incredibly difficult to find — and even harder to retain. This is the challenge every customer faces today.

What happens when roles stay empty?

- Security gaps go unmonitored
- Compliance risks increase
- Internal IT teams are overstretched
- Incident response slows down

Your internal IT team was never meant to carry this burden alone.

## Severe Shortage

Global cybersecurity talent gap  
Continues to widen – Hong Kong is no exception

## High Cost

Specialized roles command premium salaries, straining IT budgets significantly

## Retention Risk

Even when hired, top talent is quickly poached by competitors

# HKBN's One-Stop-Shop Managed Service

One integration partner – Reduce vendor complexity  
Connectivity + Security + Managed Service in a single commercial model

# What this means for you

You don't need more vendors.

You need **one integration partner** to own the outcome from the network to applications & operations with high security level.

We will meet you where you are, and work around your tech ecosystem.

## Market Leader:

Trusted by 1 in 2 HK enterprises

## Proven Track Record:

Decades of ICT experience  
managing our city-wide network

## Elite Team:

**1,200+ Engineers**  
**1,300+ certifications**

1



### One accountable partner across your tech stack

Most enterprises juggle 6 to 10 vendors across cloud, network, security & infrastructure.

**HKBNES helps you unify the entire stack with a single SLA.** One clear escalation path & absolute accountability. No finger-pointing.

2



### Connectivity backbone + SI engine

Most system integrators lack a native network. Most telcos lack integration expertise. **We do both.**

Our carrier-grade network seamlessly powers your infrastructure & applications.

3



### Proven outcomes & AI acceleration

**Enterprise scale:** Powering a 100G financial exchange backbone, a 160-site SD-WAN, & zero-downtime cloud migration for top property developers.

**AI-ready:** Seamlessly deploying agentic AI & automation platforms, fully backed by managed GPU infrastructure.

# One Partner. One Network. One Security Framework

We handle the network, security, and operations

## Connectivity

Fast networks across regional markets

High-speed fiber with very low delay and latency

99.99% guaranteed uptime

## Cisco SASE Security

Combined network and cloud security

Zero Trust access control for all users

One simple online dashboard

## Managed Operations

1,200+ engineers. 1,300+ certifications

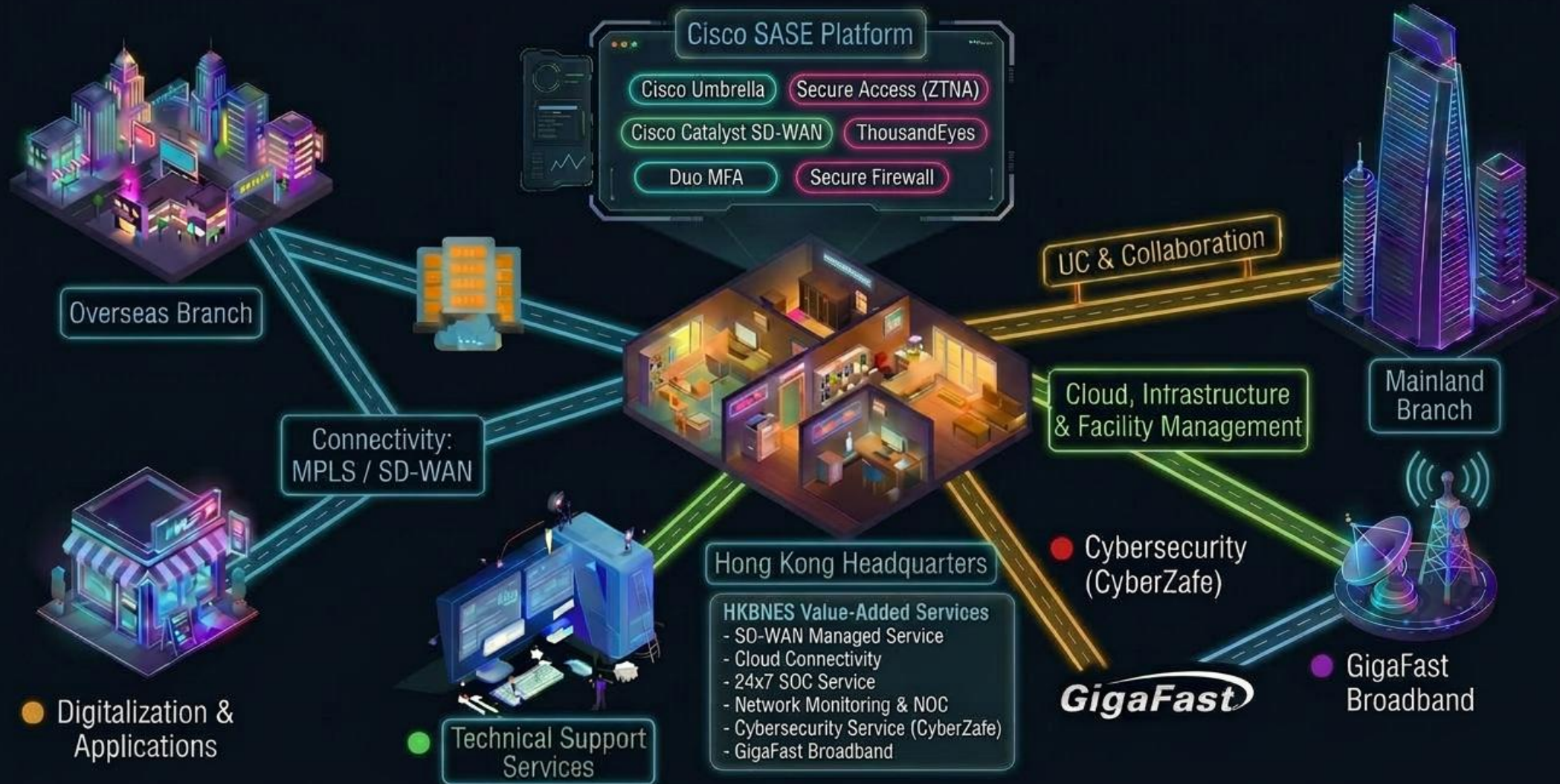
24/7 SOC monitoring and support

Smart AI tools for fast troubleshooting

# Go Global with HKBNES Managed SASE Service

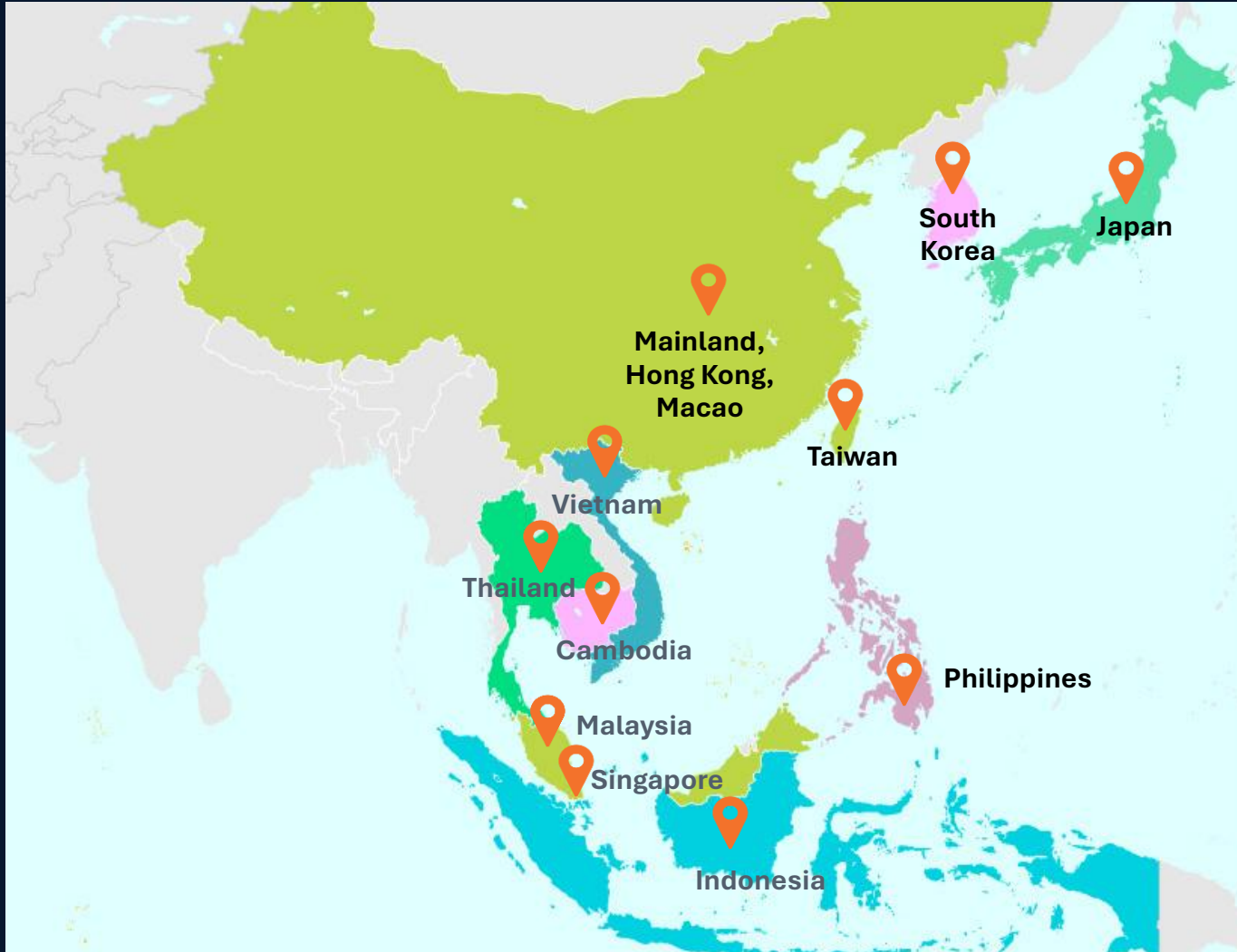
Extend your operations to the Mainland, Macao, ASEAN & beyond.

● Connectivity & Endpoint   ● Cloud Infrastructure & Facility Management   ● UC & Collaboration   ● Unified Communications & Collaboration



# Beyond Hong Kong, Across ASEAN

One partner wherever you operate.

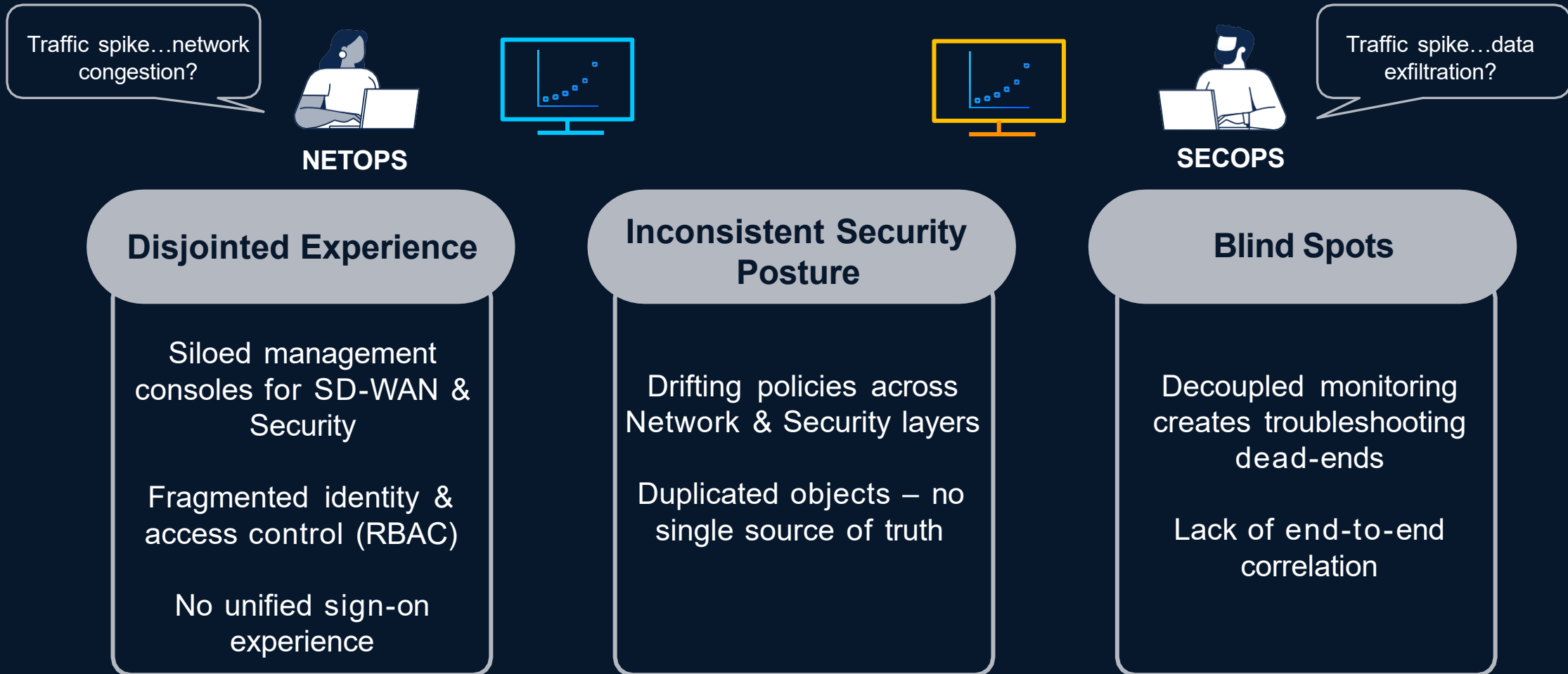


## HKBN's Partners in ASEAN

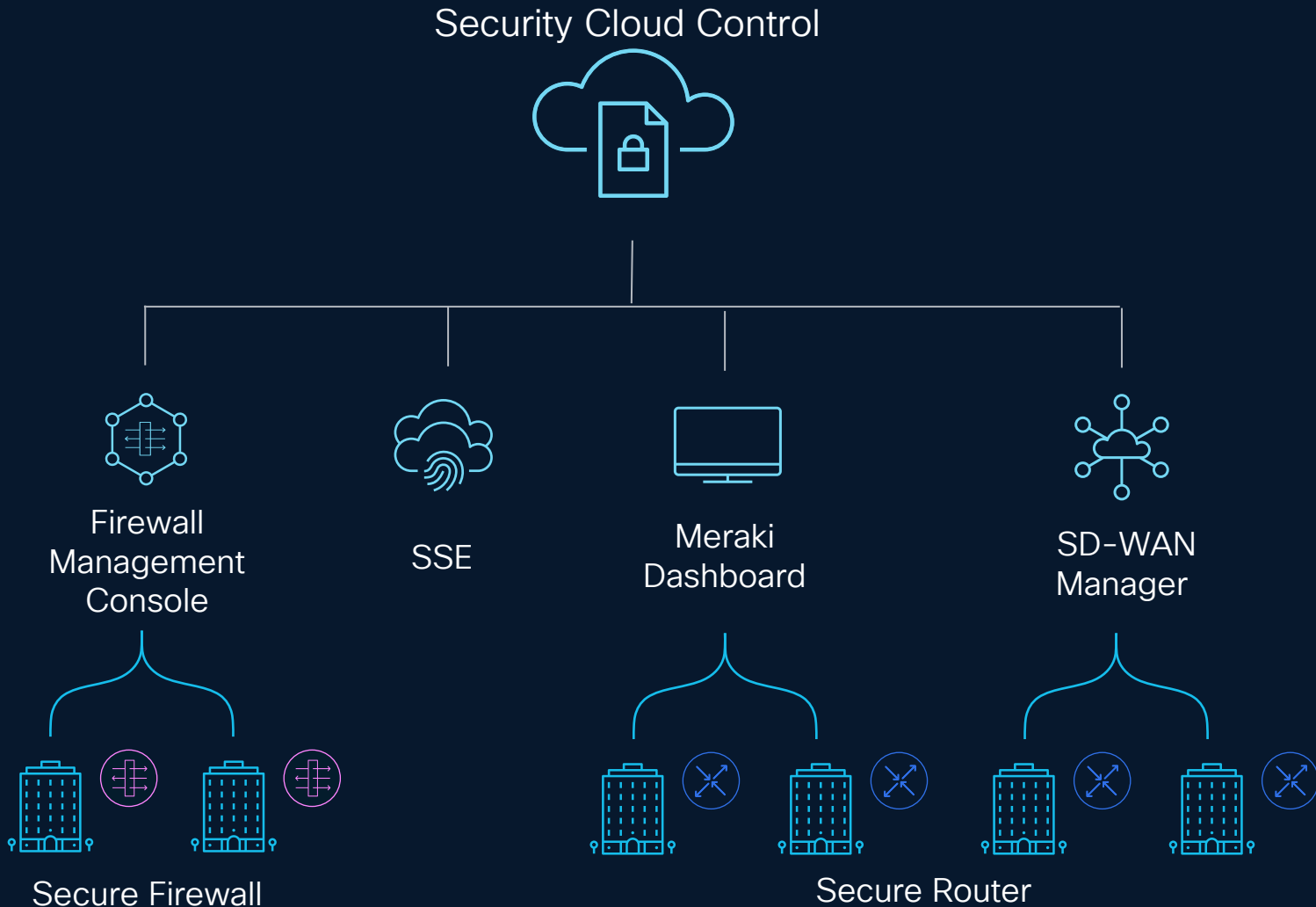
Aznet (South Korea)  
SystemsGo, Computec (Japan)  
HKBN JOS (Mainland, Hong Kong, Macao)  
Welttend (Taiwan)  
Thakral One (Vietnam)  
Clarity (Thailand)  
Positron Multiverse (Cambodia)  
Nexus (Philippines)  
Starhub (Malaysia, Singapore)  
CDW (Singapore)  
Berca (Indonesia)  
and more...

# The high cost of fragmented operations

## Challenges of managing SASE



# Security Cloud Control



## Security Object/Policy Configuration

- Create security objects for Secure Router NGFW stack
- Push security policies to different security solutions using single orchestrator

## Monitoring

- Common logging repository via SAL (Security Analytics and Logging)

## Troubleshooting

- Leverage SCC tools for security troubleshooting

# Cisco ThousandEyes Platform

## Experience & Service Assurance



### Digital experience

End user | Mobile  
IIoT | VoIP



### Proactive monitoring

Web | Network  
BGP | DNS



### Global visibility

On-Prem | Cisco  
3rd party



### Domain insights

Traffic | WAN  
Internet | Cloud

## AI-powered platform

Automation | Integrations | APIs



Path  
visualization



Cross-layer  
correlation



Anomaly detection &  
alerting



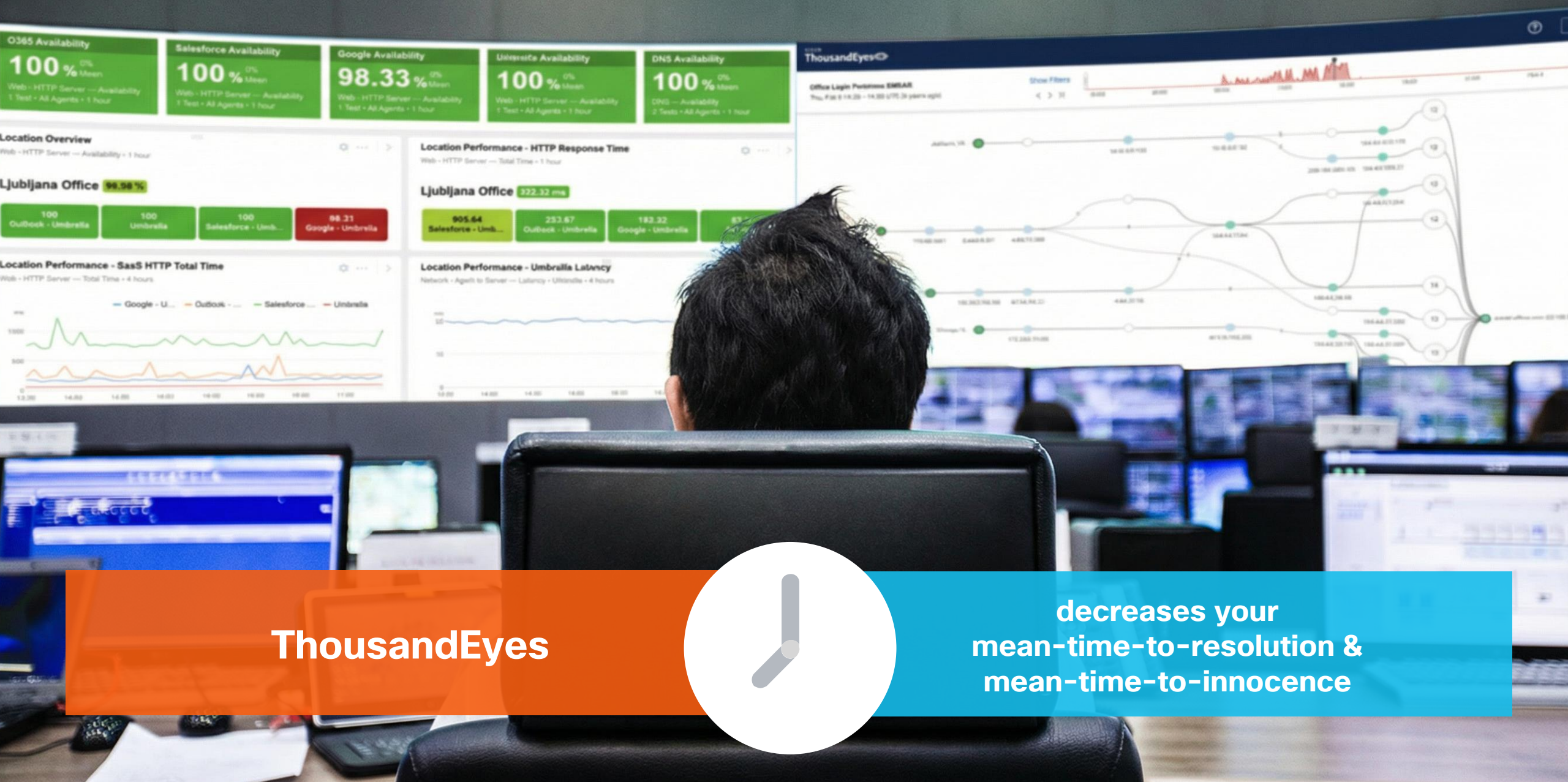
Event summarization



Predictive  
recommendations



Natural language  
query



ThousandEyes



decreases your  
mean-time-to-resolution &  
mean-time-to-innocence

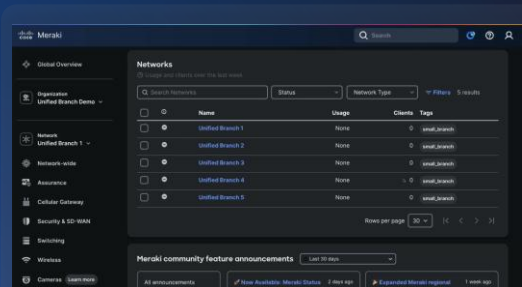
# Latest Innovations

All new!

# CY2026 A Year of Innovation



## AgenticOps for operational simplicity



### Unified Branch



## Security fused into the network



### Firewall, SASE, and quantum readiness



## Scalable devices ready for AI



### Secure Routers

# Unified Approach to Security



## Benefits

- Common NGFW libraries, objects and threat feeds
- Support of advanced NGFW services across Cisco platforms (ex EVE \*, SnortML \*\*)

## Management

- Centralized management across various enforcement points using SCC
- Common Policies with advanced services using Mesh Policy Engine

\*EVE = Encrypted Visibility Engine - [More](#)

\*\*SNORT ML = machine learning-based neural network exploit detection for Snort - [More](#)

# AgenticOps

The New Standard for IT Operations

Available now



**cisco**  
**AI Assistant**

**AI Assistant**

Accelerate network operations

Alpha



**AI Canvas**

Cross-domain collaborative troubleshooting

Powered by deep network model

Cut MTTR to near seconds  
with AI-driven root cause  
and resolution.

Catch critical issues  
**early with AI that sees  
across the stack.**

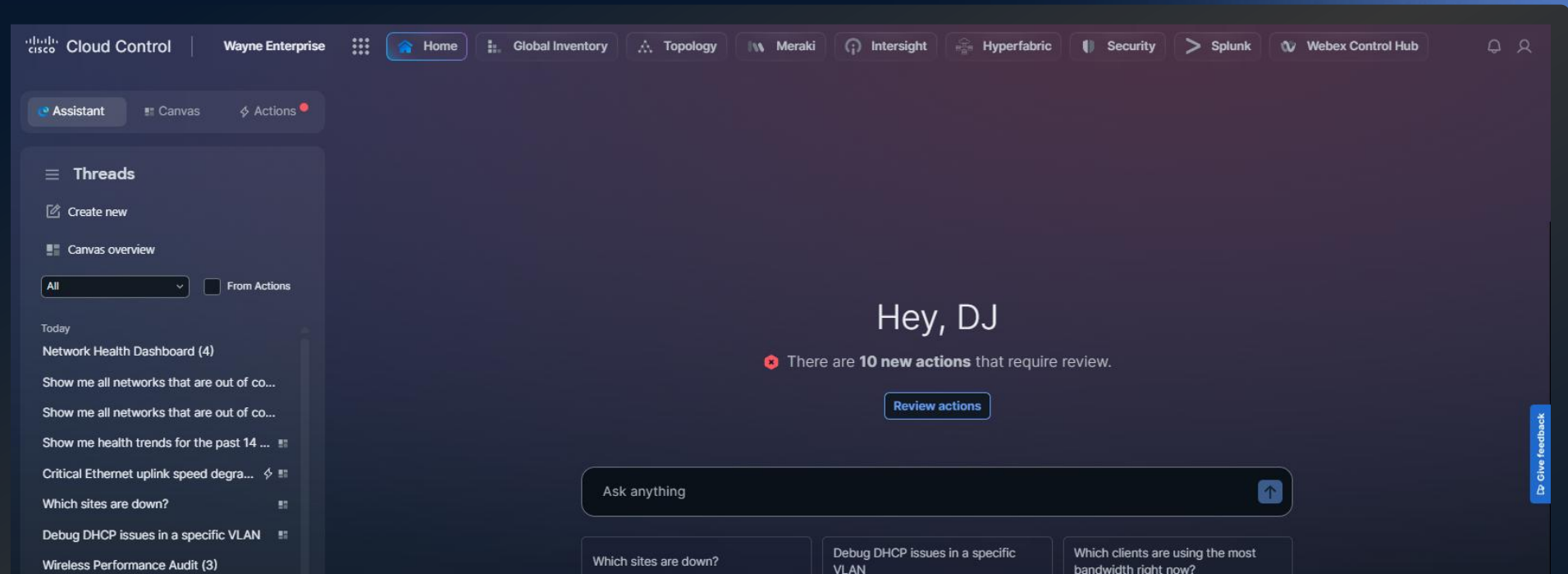
Operate at scale with  
lean teams and built-in  
AI expertise.

Troubleshoot faster  
together with shared  
context across teams.

# Cisco Cloud Control

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

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



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

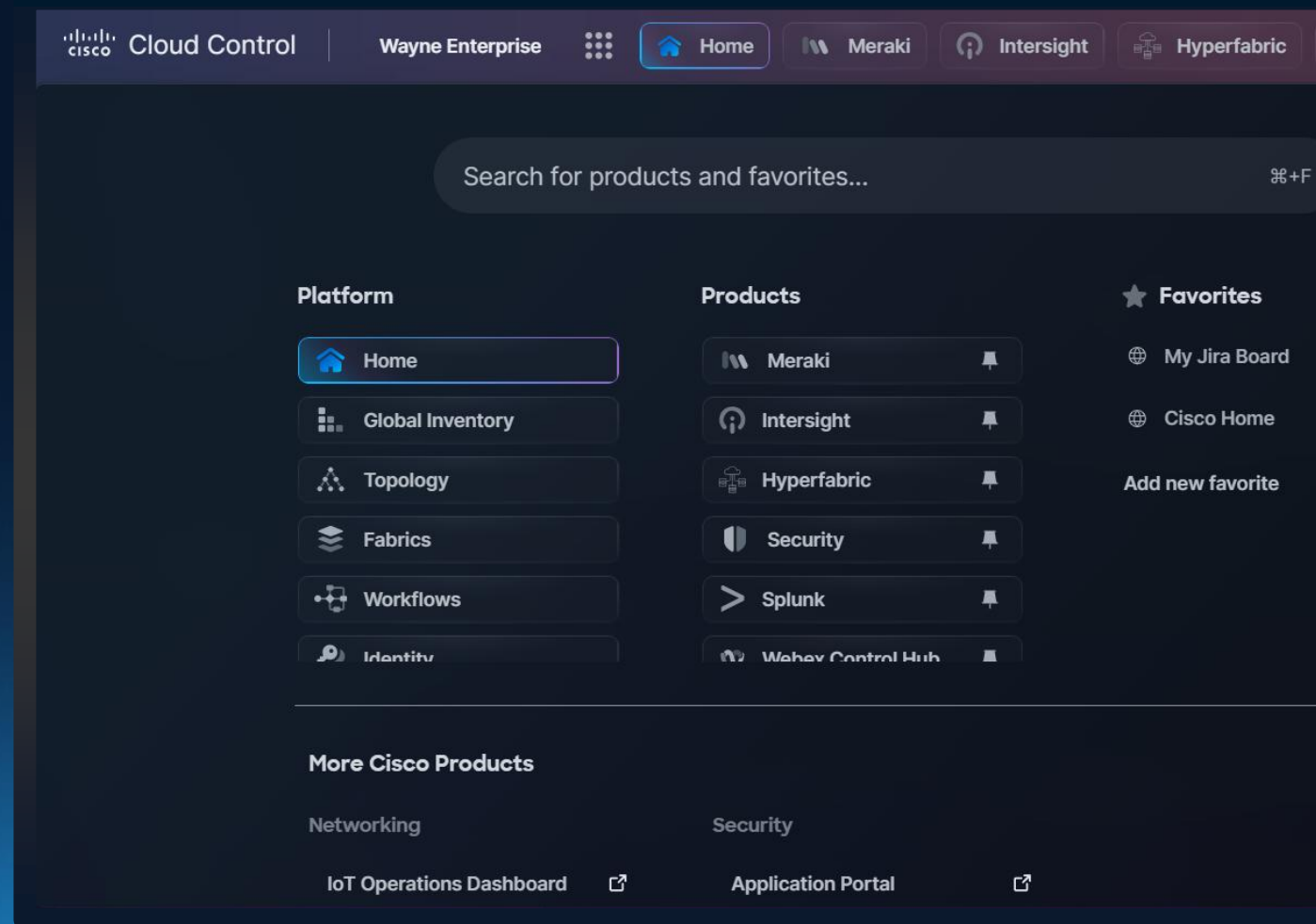
Actions correlates alerts across every product.

## One assistant

Quick answers and tasks with AI Assistant.

## One agentic workspace

Investigate, execute and resolve with AI Canvas.



One login

# Log in once, **access every** Cisco product

 Cloud Control



## Sign in

Based on your email we were able to identify multiple products associated with your account.

Sign in to one to get started.



Security



Meraki



Thousand...



Intersight



Hyperfabric



Developer...



Splunk



Webex Co...

# Unified inventory

# See every Cisco asset in one list

The screenshot displays the Cisco Cloud Control Unified Inventory dashboard. The top navigation bar includes the Cisco logo, 'Cloud Control', and a user profile 'Wayne Enterprise'. The main navigation menu features 'Home', 'Global Inventory' (selected), 'Topology', 'Meraki', 'Intersight', 'Hyperfabric', 'Security', '+2', 'Assistant', and 'Canvas'. The 'Inventory' section has tabs for 'Insights' and 'Assets'. Under 'Findings', there are filters for 'Critical (2)', 'Warning (6)', 'Info (5)', and 'All (13)'. A note indicates 'Last analyzed 24 minutes ago'. Two critical findings are highlighted: 'Devices Reported Offline By Their Management Source' (69 assets) and 'Devices At Or Past Last Day Of Support' (24 assets). Below these are 'AI Recommendations' for monitoring Meraki MX and Hyperfabric switches (95% confidence) and detecting Meraki IoT cameras and cellular gateways (94% confidence). The bottom section shows 'Security Exposure', 'Lifecycle Horizon', and 'Compliance Posture' metrics.

**Inventory** Insights Assets

**Findings**

Critical (2) Warning (6) Info (5) All (13)

Last analyzed 24 minutes ago

**Devices Reported Offline By Their Management Source** Critical

69 assets reported offline or unreachable by their management source (27 Meraki\_Dashboard, 23 Hyperfabric, 19 Security\_Cloud\_Control). Check each source console for connectivity issues.

27 Meraki\_Dashboard 23 Hyperfabric 19 Security\_Cloud\_Control

**Devices At Or Past Last Day Of Support** Critical

24 assets at hardware end-of-life (LDOS): 21 past last-day-of-support, 3 with LDOS within the next 6 months. Plan replacements.

24 Meraki\_Dashboard

**AI Recommendations**

**Monitor Meraki MX and Hyperfabric Switches with Unreachable + Version Missing + Non-Compliant or Anomaly Signals** 95% Explanation

Show me devices that are unreachable, missing software versions, and either non-compliant or have major anomalies, focusing on Meraki MX and Hyperfabric Switches

**Detect Meraki IoT Cameras and Cellular Gateways with Dormant + LDOS Expired + Unreachable + Version Missing** 94% Explanation

Find Meraki IoT Cameras and Cellular Gateways that are dormant, have expired licenses, are unreachable, and missing software versions

**Security Exposure**

Advisory severity rolled up across assets (PSIRT and security bulletins). Hover legend rows in product for exact counts.

**Lifecycle Horizon**

Hardware and software support runway. LDOS >90d matches the Overview tile for consistency.

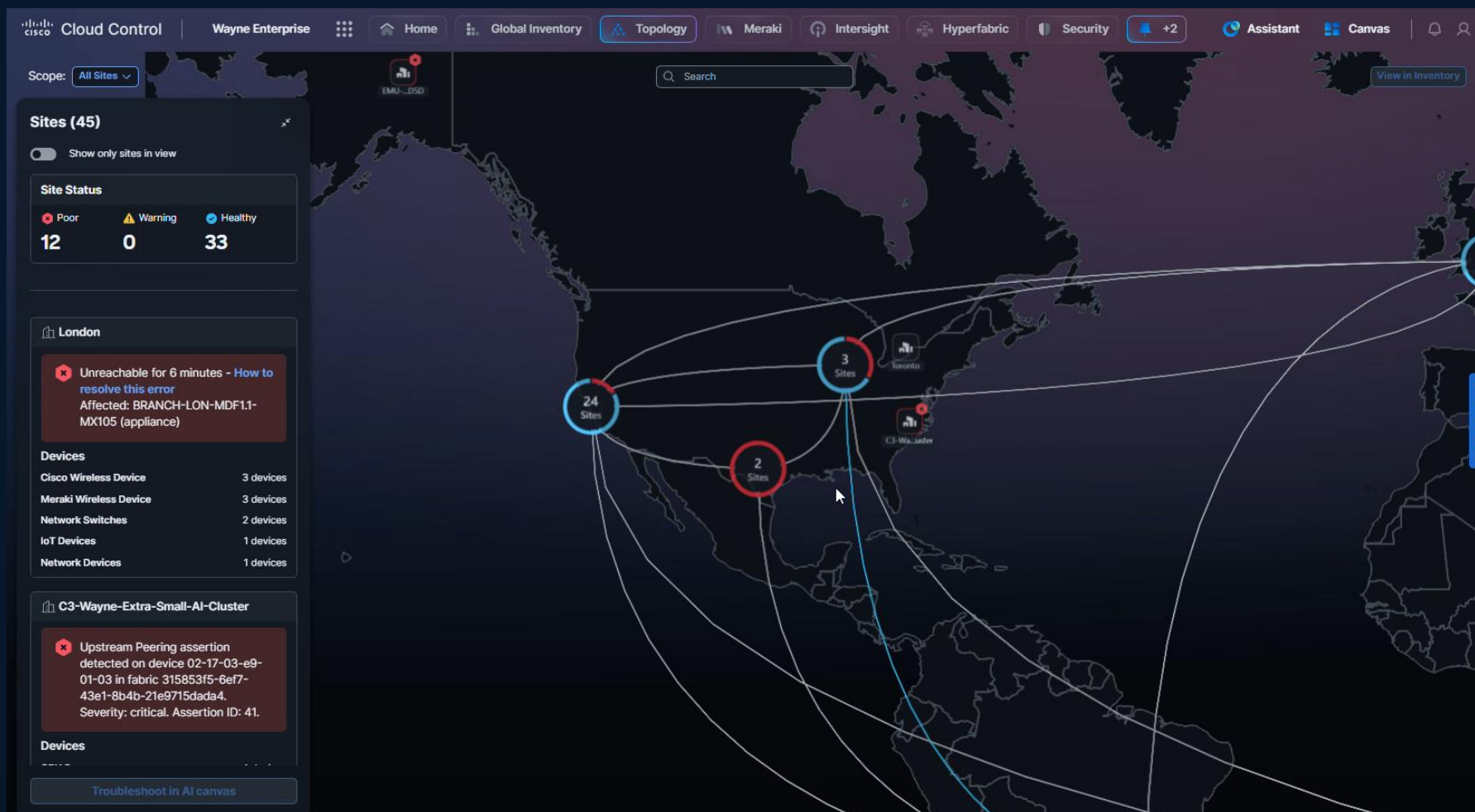
**Compliance Posture**

Policy and control coverage across inventory (org baselines, mandatory checks, and exceptions).

Give feedback

Unified topology

# See every site, branch and device in one view



## Actions

# Every alert, correlated and actionable

## Alerts with answers

Alerts correlated across domains, paired with recommended next steps.

## Personalized to how you operate

AI surfaces what matters most to you, today.

## Investigate or escalate with AI

Dig deeper with the AI Assistant, or open AI Canvas with full context preserved.

The screenshot displays the Cisco Cloud Control interface for Wayne Enterprise. The top navigation bar includes links to Home, Meraki, Intersight, Hyperfabric, Security, Splunk, and Webex Control Hub. Below the navigation bar, there are tabs for Assistant, Canvas, and Actions. The main content area shows a list of alerts under the 'Open' tab. The alerts are sorted by severity, assignee, and sort by. The first alert is 'Sustained high WAN usage on Meraki Assurance M...' with a severity of 'Warning' and a timestamp of 'Today, 3:57 PM'. The second alert is 'Critical Ethernet uplink speed degradation on multi...' with a severity of 'Critical' and a timestamp of 'Today, 2:04 PM'. The third alert is 'High WAN Usage Detected on Meraki Assurance M...' with a severity of 'Warning' and a timestamp of 'Today, 1:56 PM'. The fourth alert is 'Ethernet uplink speed degradation on MR46 wirele...' with a severity of 'Critical' and a timestamp of 'Today, 1:01 PM'. The fifth alert is 'Access Point Communication Loss with Wireless L...' with a severity of 'Critical' and a timestamp of 'Today, 1:01 PM'. The sixth alert is 'Sustained High WAN Usage on Meraki Assurance ...' with a severity of 'Warning' and a timestamp of 'Today, 1:01 PM'. On the right side, there is a detailed view of the 'Critical Ethernet uplink speed degradation on multiple Meraki devices' alert. It includes a 'Summary' section with the text: 'Multiple Meraki devices including wireless access points and switches experienced critical Ethernet uplink speed degradation due to negotiation failures. Affected devices include BRANCH-LON-114-MR44, Assurance AP, and Assurance Switch, impacting network performance and device health.' Below the summary is a 'Linked Notifications' section with two entries: 'Ethernet uplink speed degraded' (Affected: BRANCH-LON-114-MR44 (wireless) and Unknown device) and 'Ethernet uplink speed degraded' (Affected: Assurance AP (wireless) and Assurance Switch (switch)). At the bottom right, there is a chat window with the AI Assistant. The chat window shows a message from 'You' asking for help with a critical severity incident from Meraki. The AI Assistant responds with a detailed explanation of the incident and provides a link to the linked notifications. The chat window also includes a text input field and a 'Send' button.

Cloud Control | Wayne Enterprise | Home | Meraki | Intersight | Hyperfabric | Security | Splunk | Webex Control Hub

Assistant | Canvas | Actions

Open | Resolved | Dismissed

Severity | Assignee | Sort by

**Sustained high WAN usage on Meraki Assurance M...**  
The Meraki Assurance MX appliance (device Q2KY-APYN-FD42) experienced sustained high WAN usage over a period...  
Today, 3:57 PM

**Critical Ethernet uplink speed degradation on multi...**  
Multiple Meraki devices including wireless access points and switches experienced critical Ethernet uplink speed...  
Today, 2:04 PM

**High WAN Usage Detected on Meraki Assurance M...**  
Two notifications reported high WAN usage on the Meraki Assurance MX appliance (device Q2KY-APYN-FD42) within a...  
Today, 1:56 PM

**Ethernet uplink speed degradation on MR46 wirele...**  
The MR46 wireless device at BRANCH-LON-115 experienced a critical ethernet negotiation failure resulting in degraded upli...  
Today, 1:01 PM

**Access Point Communication Loss with Wireless L...**  
An access point (DCSA-11-CW91620) stopped communicating with the Wireless LAN Controller LP-DCSA-C9800-L-C on...  
Today, 1:01 PM

**Sustained High WAN Usage on Meraki Assurance ...**  
The Meraki Assurance MX appliance (device Q2KY-APYN-FD42) experienced sustained high WAN usage over a 20...

**Critical Ethernet uplink speed degradation on multiple Meraki devices**  
Critical | Today, 2:04 PM | Assign to me

**Summary**  
Multiple Meraki devices including wireless access points and switches experienced critical Ethernet uplink speed degradation due to negotiation failures. Affected devices include BRANCH-LON-114-MR44, Assurance AP, and Assurance Switch, impacting network performance and device health.

**Linked Notifications**

**Ethernet uplink speed degraded**  
Affected: BRANCH-LON-114-MR44 (wireless) and Unknown device  
2h

**Ethernet uplink speed degraded**  
Affected: Assurance AP (wireless) and Assurance Switch (switch)  
2h

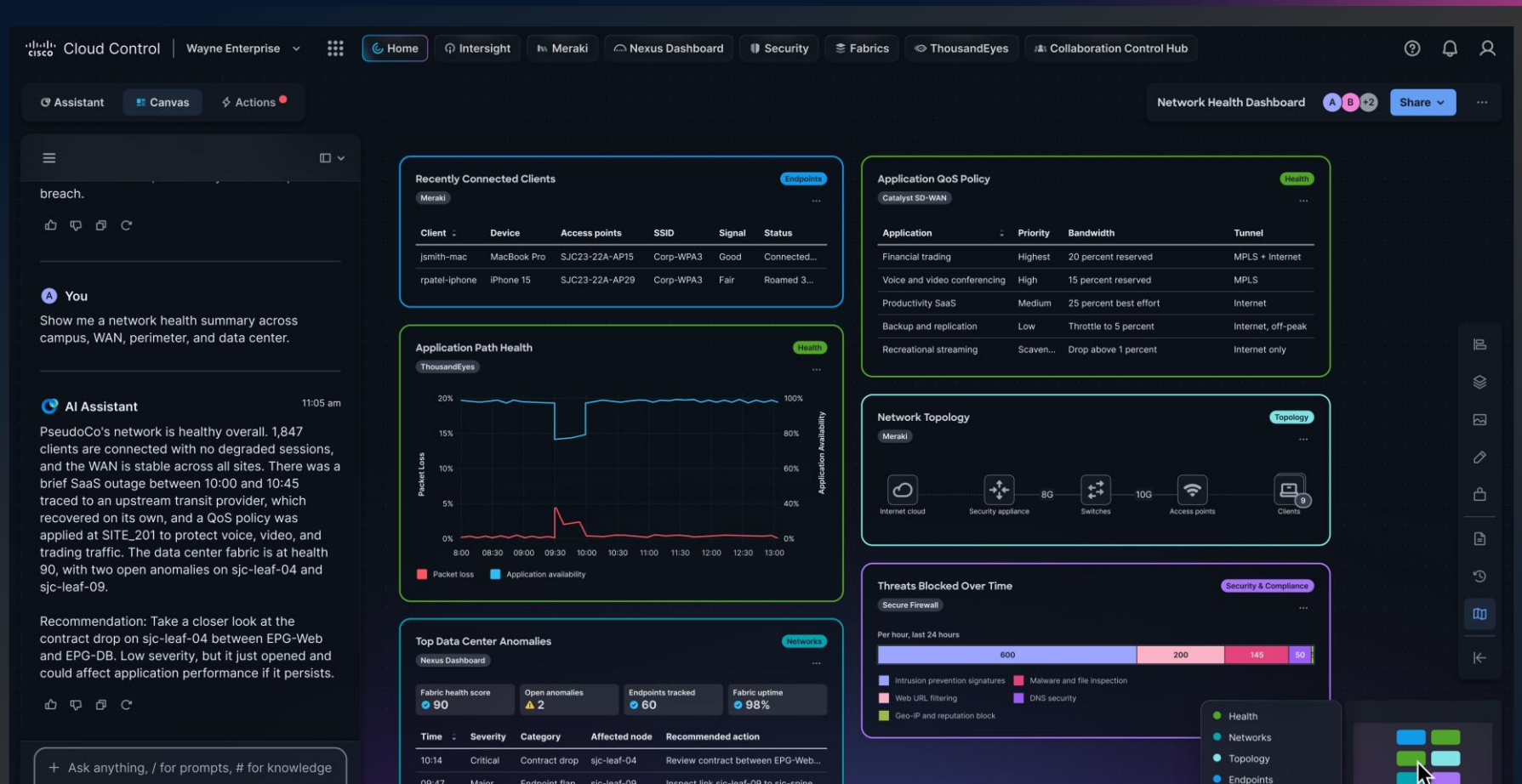
**You**  
I received a critical severity incident from meraki:  
Critical Ethernet uplink speed degradation on multiple Meraki devices Multiple Meraki devices including wireless access points and switches experienced critical Ethernet uplink speed degradation due to negotiation failures. Affected devices include BRANCH-LON-114-MR44, Assurance AP, and Assurance Switch, impacting network performance and device health.  
Linked notifications:  
[critical] Ethernet uplink speed degraded Affected: BRANCH-LON-114-MR44 (wireless) and Unknown device Product: meraki Devices: Q3AL-38LC-AGVH Category: device\_health  
[critical] Ethernet uplink speed degraded Affected: Assurance AP (wireless) and

Ask anything

Prompts and responses are only visible to you. Assistant can make mistakes. Verify responses.

# Cisco AI Canvas

The industry's first multiplayer workspace for cross-domain agentic operations



Thank you

[rangbala@cisco.com](mailto:rangbala@cisco.com)



**Closing**

# Your SASE Journey Starts Now

Some providers offer you bandwidth. Others offer you security.

**HKBNES delivers both – integrated, managed, and supported locally.**

Cisco SASE → World-class security

HKBN MetroNet → High-performance connectivity

Our Managed Services → We handle everything

Local Expertise → We're here, always

**We succeed when you succeed.**

# Build Your Secure Future Today

## *Evaluation Your Attack Surface*

Identity the hidden gaps in your distributed network.  
Understand where your current architecture falls short —  
before adversaries find those weaknesses first

## *Partner with HKBNES Experts*

Take the next step in your AI transformation journey. Secure  
your network, manage your risk, and scale with confidence —  
backed by Cisco SASE and HKBNES expertise.

**Ready to begin?** Speak with an HKBNES solutions specialist today  
and discover how we can architect your path in resilience

