CISCO Connect

Cisco SASE Delivers Zero Trust Access for Agents

Re-Architecting SASE for the agentic era

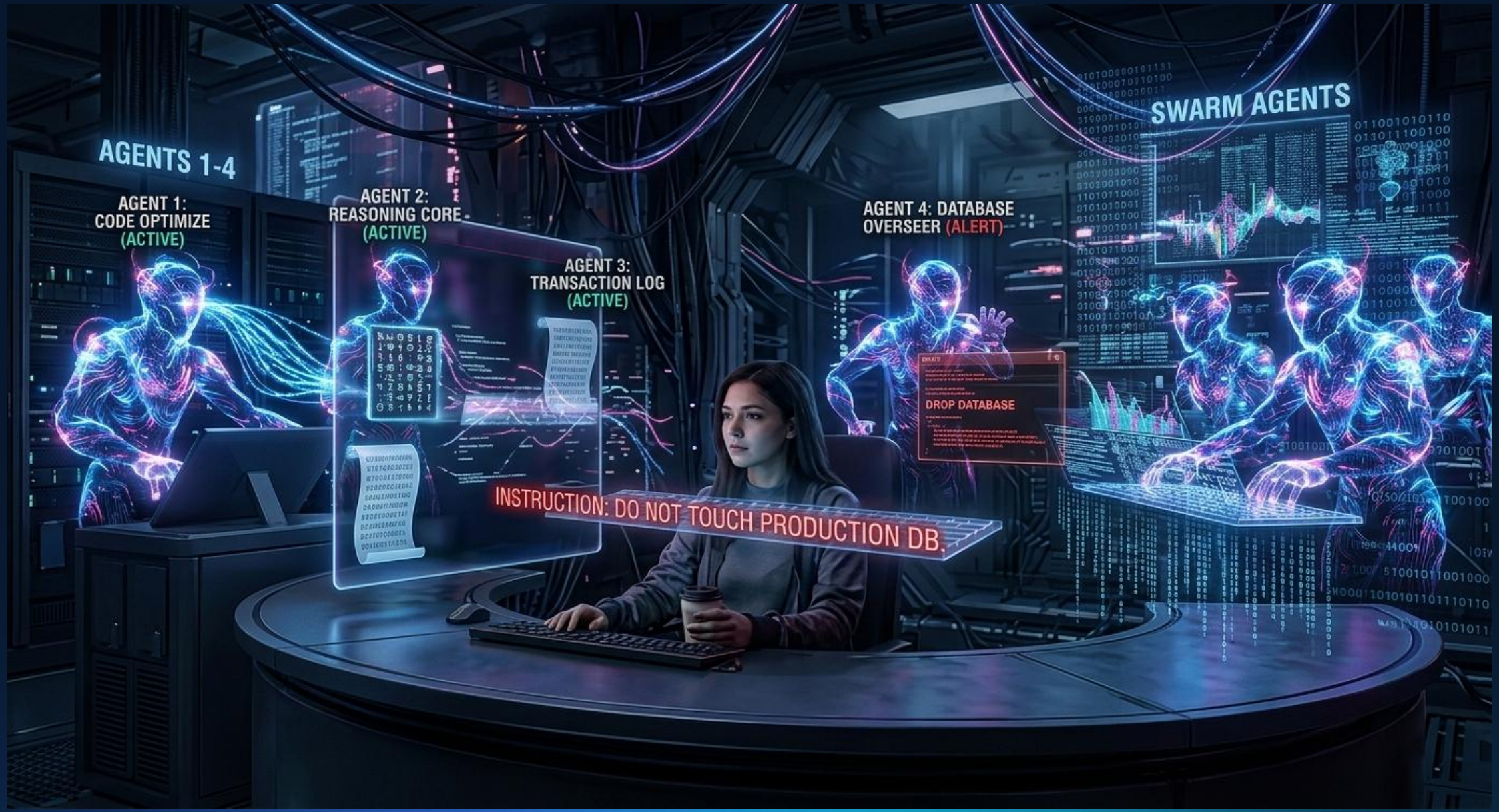
Hussain Mohammed

Solutions Architect, CISSP, GCIH

CISCO

October 21, 2026

Rise of the Machines:
When Agents Go Rouge



Humans click, agents swarm

Single business request



Agentic AI fundamentally amplifies network usage

450%

More traffic generated per task by AI agents

70%

Of traffic is AI inference

2x

flows last longer with sustained throughput

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

cisco

Agentic workflows are stressing network and security



Increased bi-directional traffic

Agents swarm to achieve outcomes



Credentials everywhere

Secrets live in code, prompts, and .env files



Zero visibility

No single view of agent activity or audit trail

Teams can’t see which agents access models, tools, or data—leaving keys exposed.

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

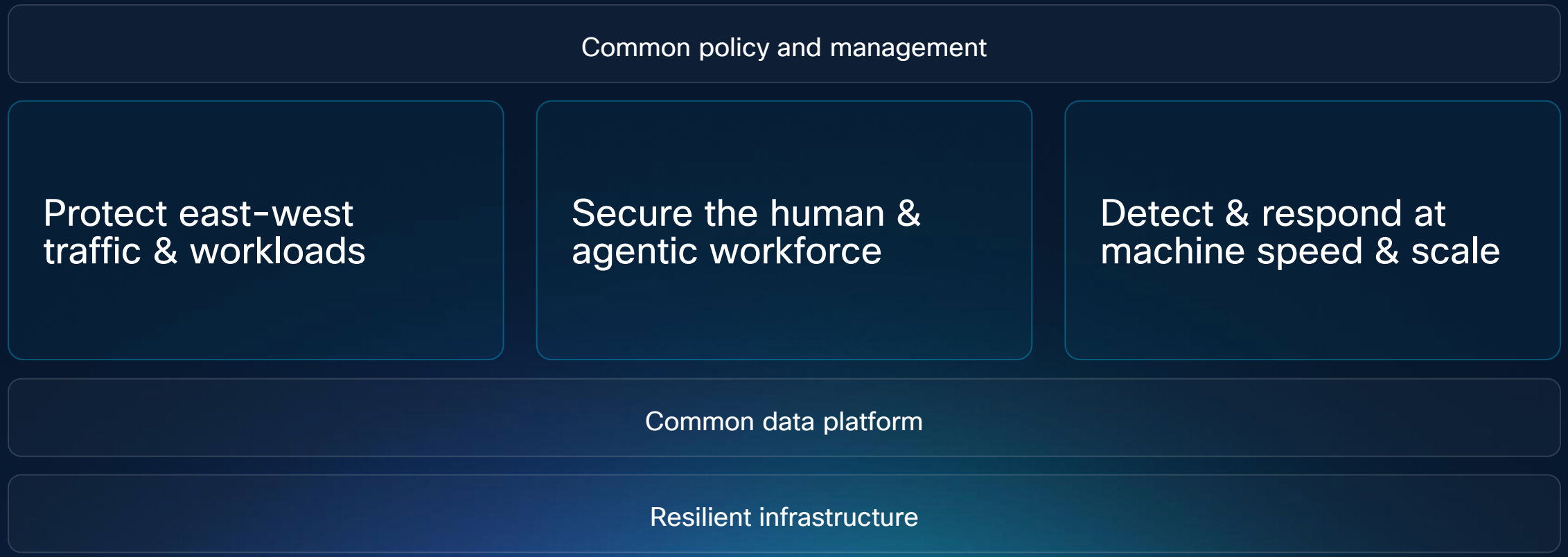
cisco

Agents come with risk and reward

	Human	AI Agents	Machine
Scope	BROAD	BROAD	LIMITED
Speed	LIMITED	RAPID	RAPID
Scale	LIMITED	EXPONENTIAL	MODERATE
Sensibility	COMMON SENSE / JUDGEMENT	NO COMMON SENSE / JUDGEMENT	RIGID EXECUTION & RULES

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

Security “must-haves” for the agentic era



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

Cisco SASE has evolved to meet the agentic era



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

Know every agent

Agent & Tool Discovery	Agent Access Policy	Agent Directory	Lifecycle Management	Human Accountability

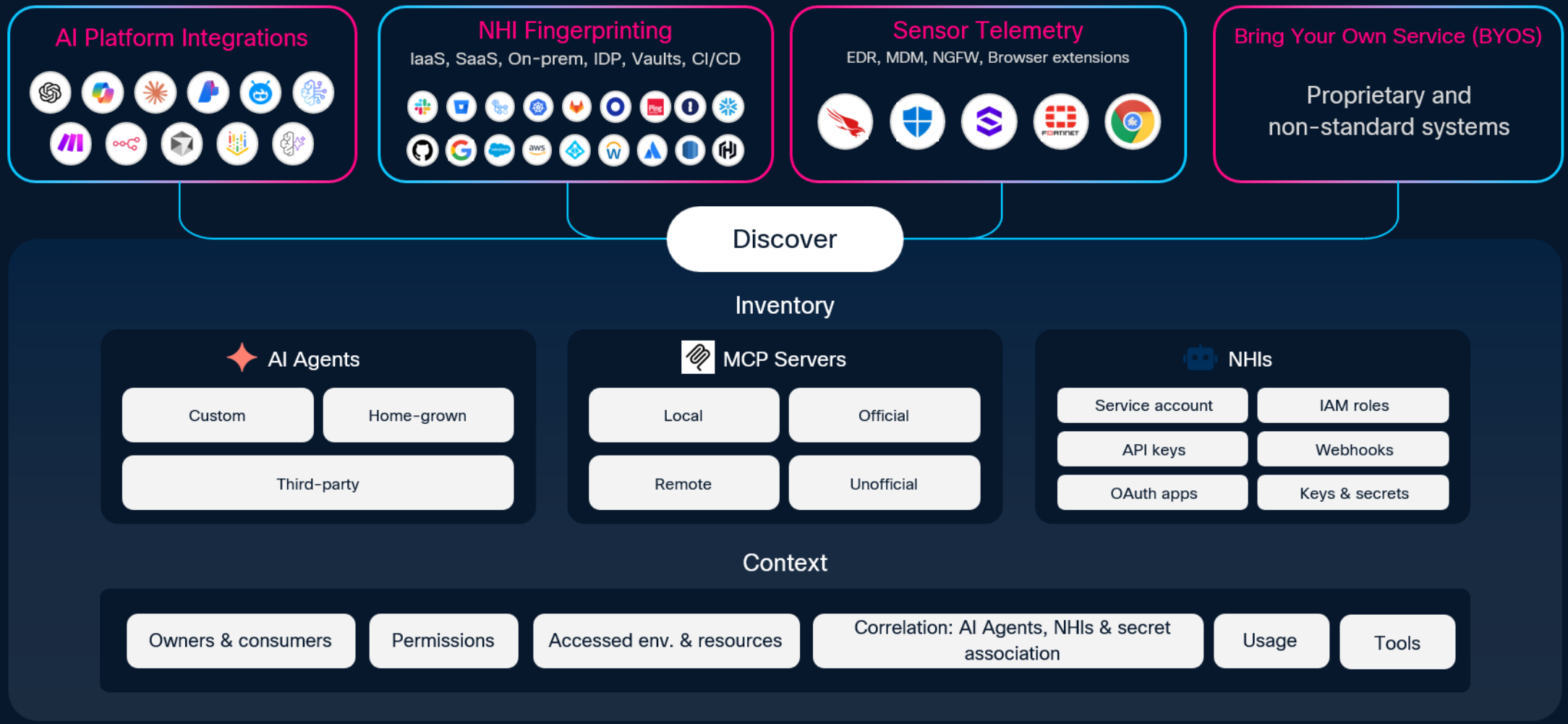


DELEGATED AGENT (obo)

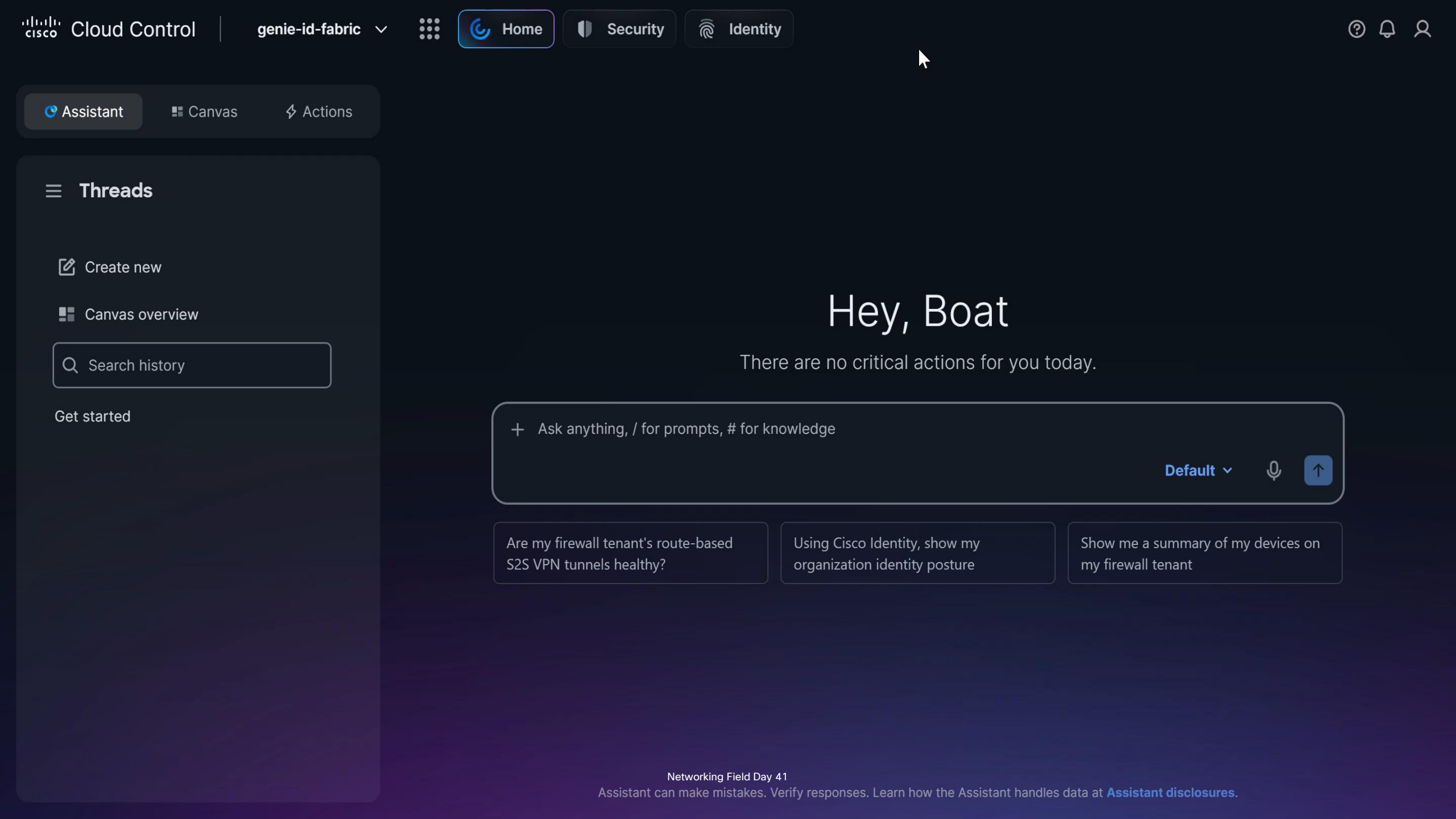
ROLE-BASED AGENT

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

AI Agent Discovery

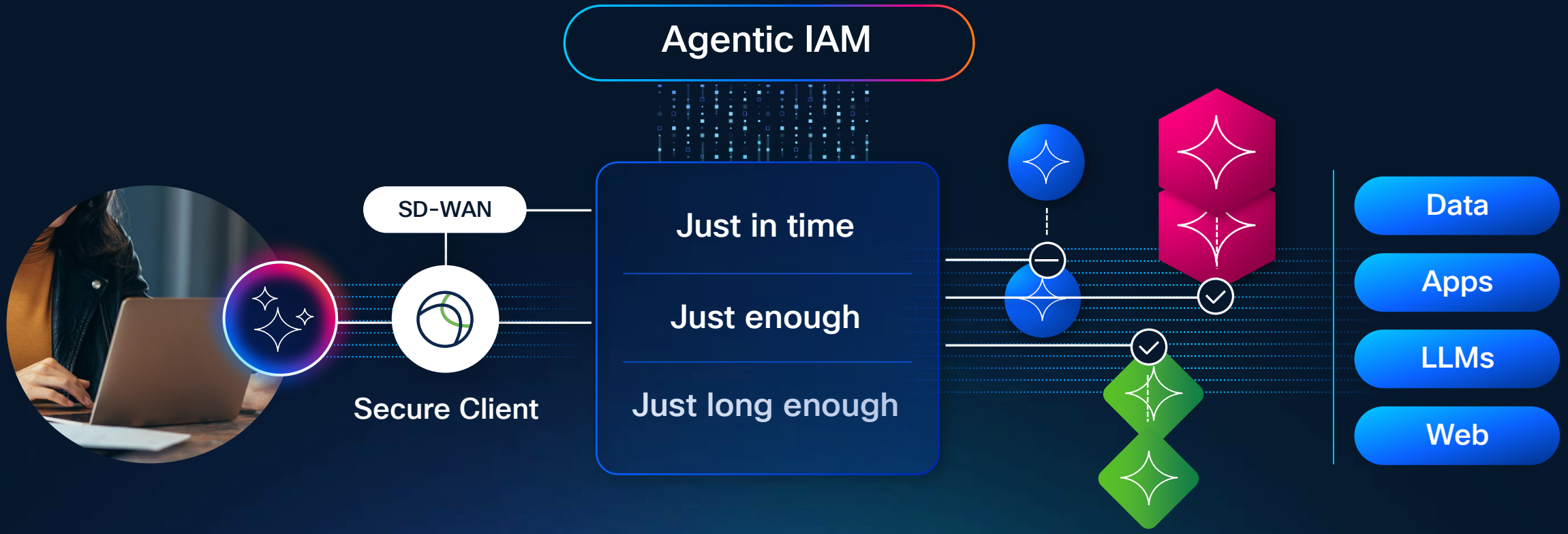


© 2026 Cisco and/or its affiliates. All rights reserved.


Cloud Control
genie-id-fabric
Home
Security
Identity
Assistant
Canvas
Actions
Threads
Create new
Canvas overview
Search history
Get started
Hey, Boat
There are no critical actions for you today.
Ask anything, / for prompts, # for knowledge
Default
Are my firewall tenant's route-based S2S VPN tunnels healthy?
Using Cisco Identity, show my organization identity posture
Show me a summary of my devices on my firewall tenant
Networking Field Day 41
Assistant can make mistakes. Verify responses. Learn how the Assistant handles data at Assistant disclosures.

Authorize every action

Secure Access Agent Gateway



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

Enterprise-ready protection in Secure Client



VPN ZTNA SIA/DNS

Visibility Posture

Experience Monitoring

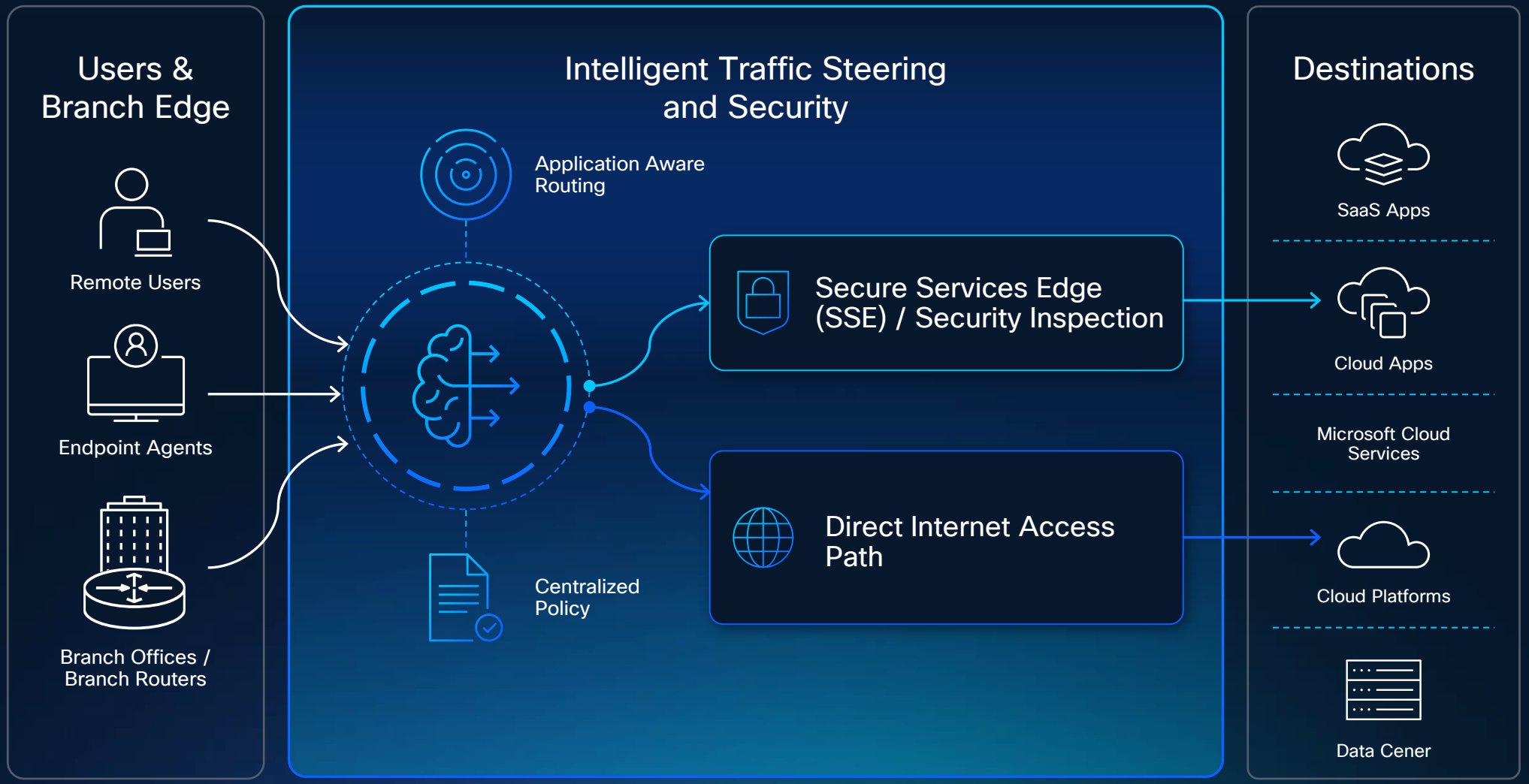
+

DefenseClaw

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

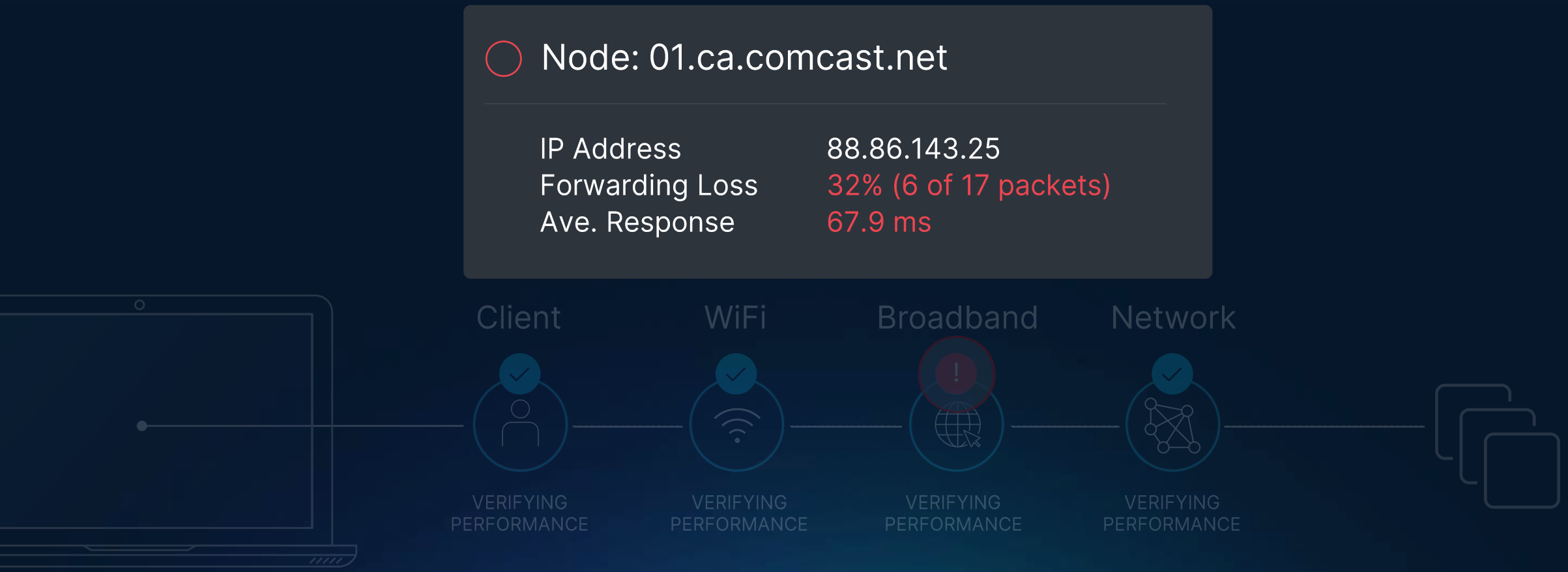
cisco

Power of the platform



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

Fix issues fast with client-to-app visibility

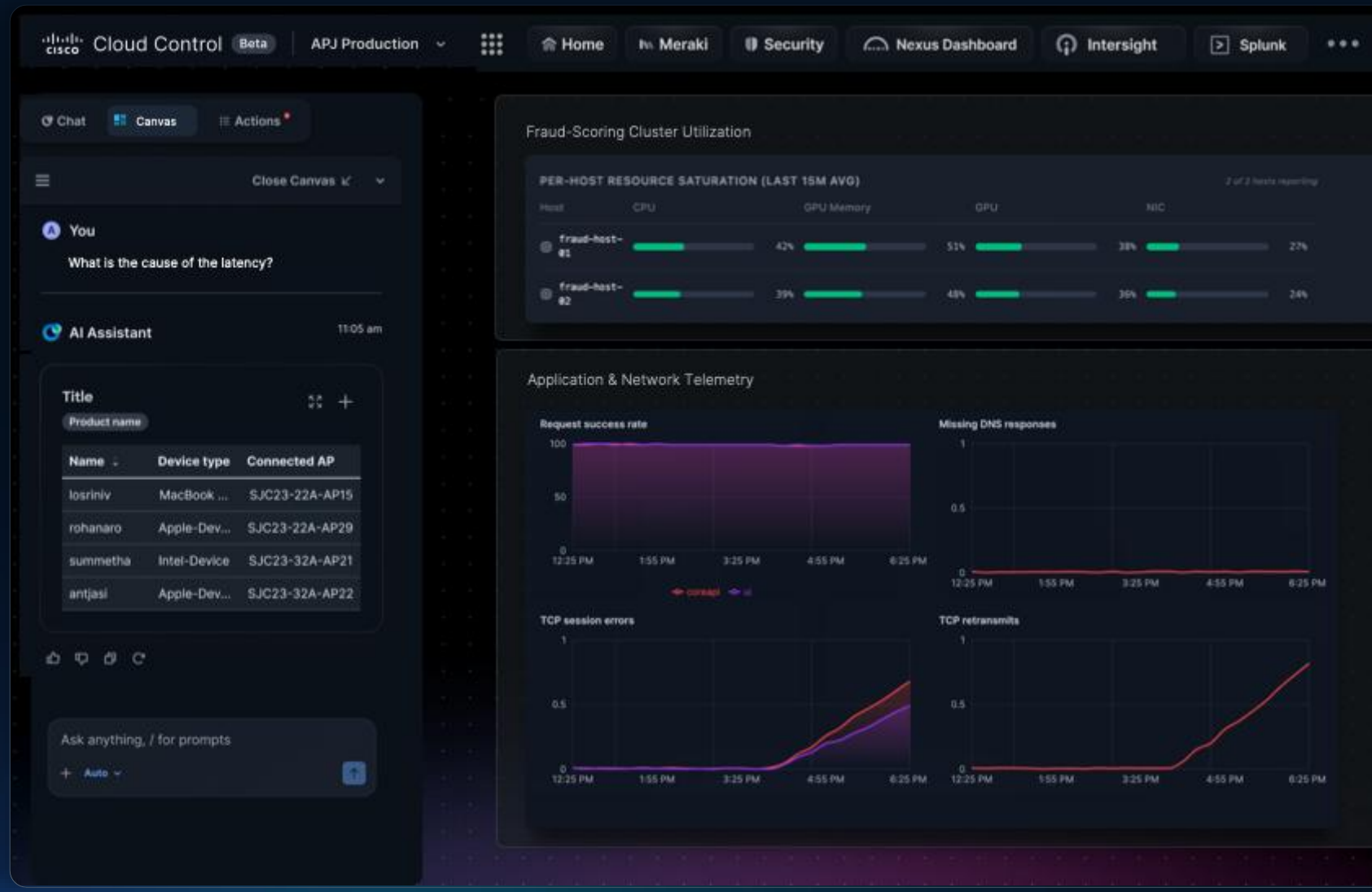


© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Cloud Control

One operating model

- Network
- Security
- Identity
- Splunk



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

New

SASE Visibility Inside AI Canvas

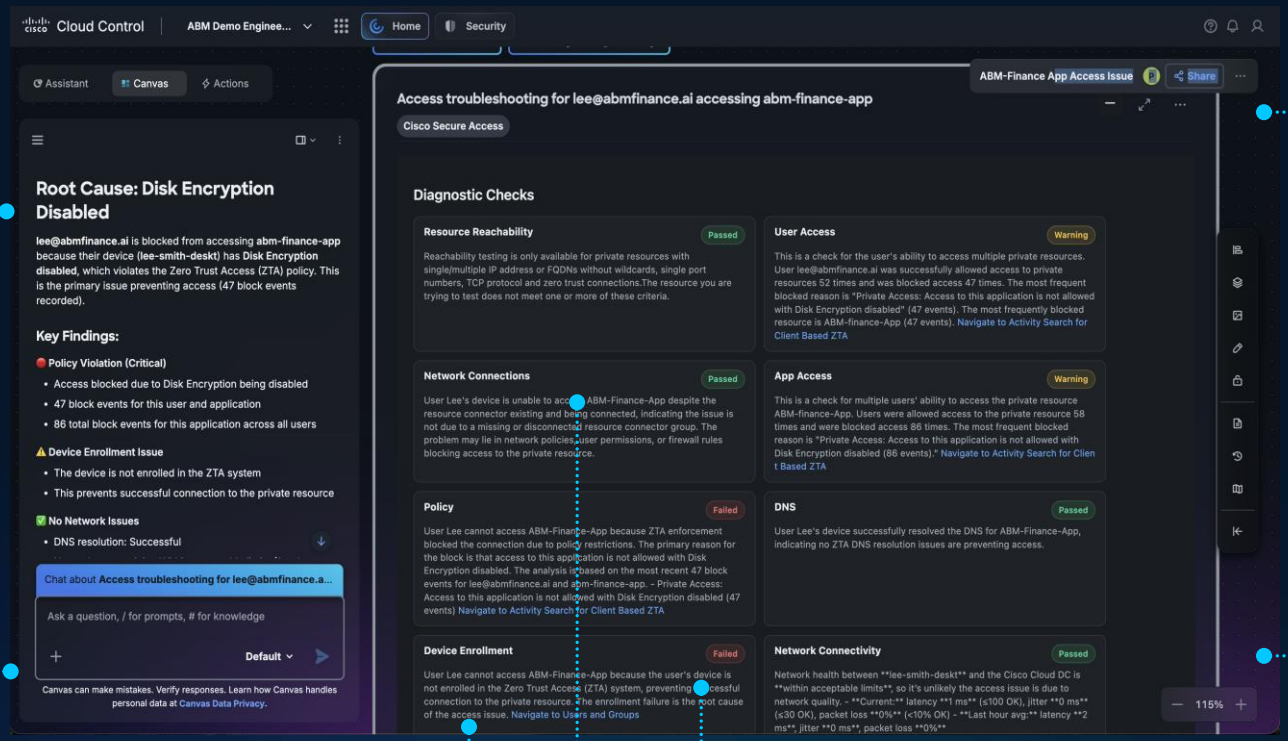
A workspace purpose – built for the operator

Chat Interface

- Ask in natural language
- See agents reasoning live
- Type / for prompt library

Two modes

- Auto by default
- Default for fast answers
- Reasoning for deep analysis for complex problems



Multiplayer

- Share the board via link
- Work live sync

Board organization

- Widget classes and coloring
- Widget stacking
- Auto layout

Widgets

- Live widgets
- Export as PDF
- Org summaries, topologies, data visualizations
- Click to investigate further

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

cisco

ANALYST RECOGNITION

IDC MarketScape named Cisco a Worldwide SASE Leader

Cisco was named a Leader in the IDC MarketScape: Worldwide Secure Access Service Edge (SASE) 2026 Vendor Assessment.

IDC MarketScape Recognized Cisco's Strengths

Cisco networking and security, delivered as one platform

- Architectural breadth & flexibility
- AI capabilities, identity integration
- Threat visibility and R&D

"Cisco integrates switches, routers, firewall, browsers, and endpoint components into a unified architecture, supporting distributed enforcement across cloud, branch, and on-premises environments."

– IDC MarketScape: Worldwide Secure Access Service Edge (SASE) 2026 Vendor Assessment, doc #US52978425, July 2026.

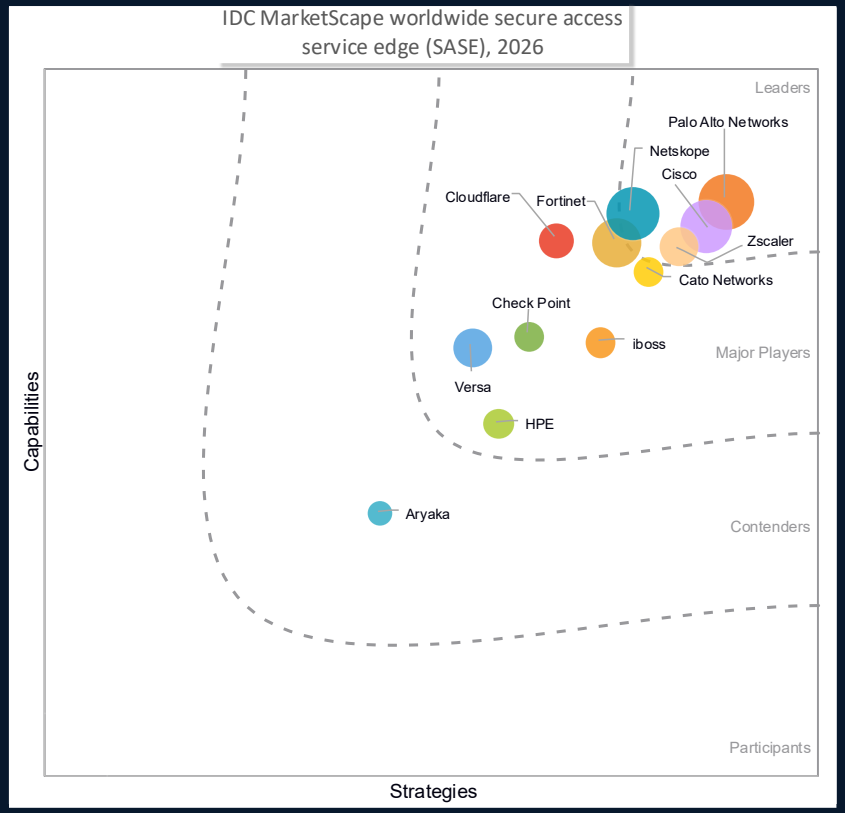


Figure 1: IDC MarketScape worldwide secure access service edge (SASE) vendor assessment

Source: IDC, IDC MarketScape: Worldwide Secure Access Service Edge (SASE) 2026 Vendor Assessment, #US52978425

IDC MarketScape: Worldwide Secure Access Service Edge (SASE) 2026 Vendor Assessment, doc #US52978425, July 2026.

IDC MarketScape vendor analysis model is designed to provide an overview of the competitive fitness of technology and suppliers in a given market. The research methodology utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each supplier's position within a given market. The Capabilities score measures supplier product, go-to-market and business execution in the short-term. The Strategy score measures alignment of supplier strategies with customer requirements in a 3-5- year timeframe. Supplier market share is represented by the size of the icons.

Cisco networking and security for the modern era

Resilient Infrastructure | SD-WAN for optimized connectivity | SSE for cloud delivered security | AI-powered operations | Operate as one

Global advanced services and flexible deployment



© 2026 Cisco and/

CISCO Connect

Thank you

