CISCO Connect

Humans Click, Agents Swarm

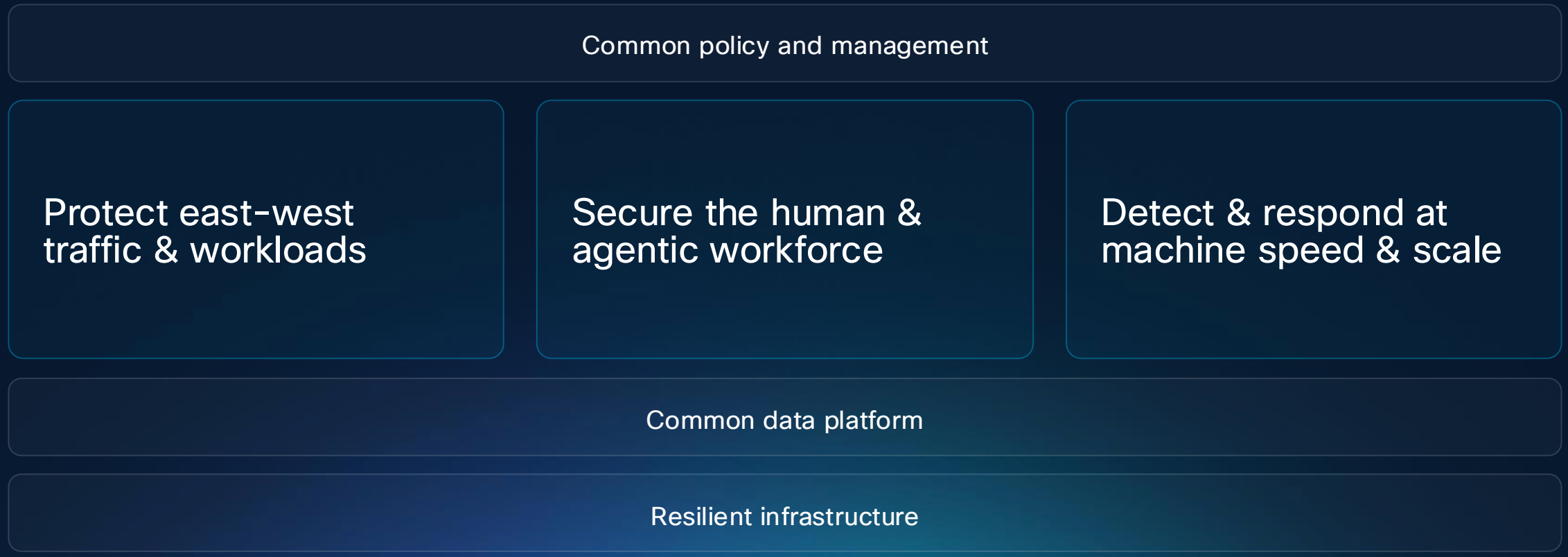
Re-Architecting SASE for the agentic era

Ben Craig
Solutions Engineer - SASE



October 13, 2026

Security “must-haves” for the agentic era



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

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

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.

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.

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

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

Astrix Discover makes non-human identity activity visible

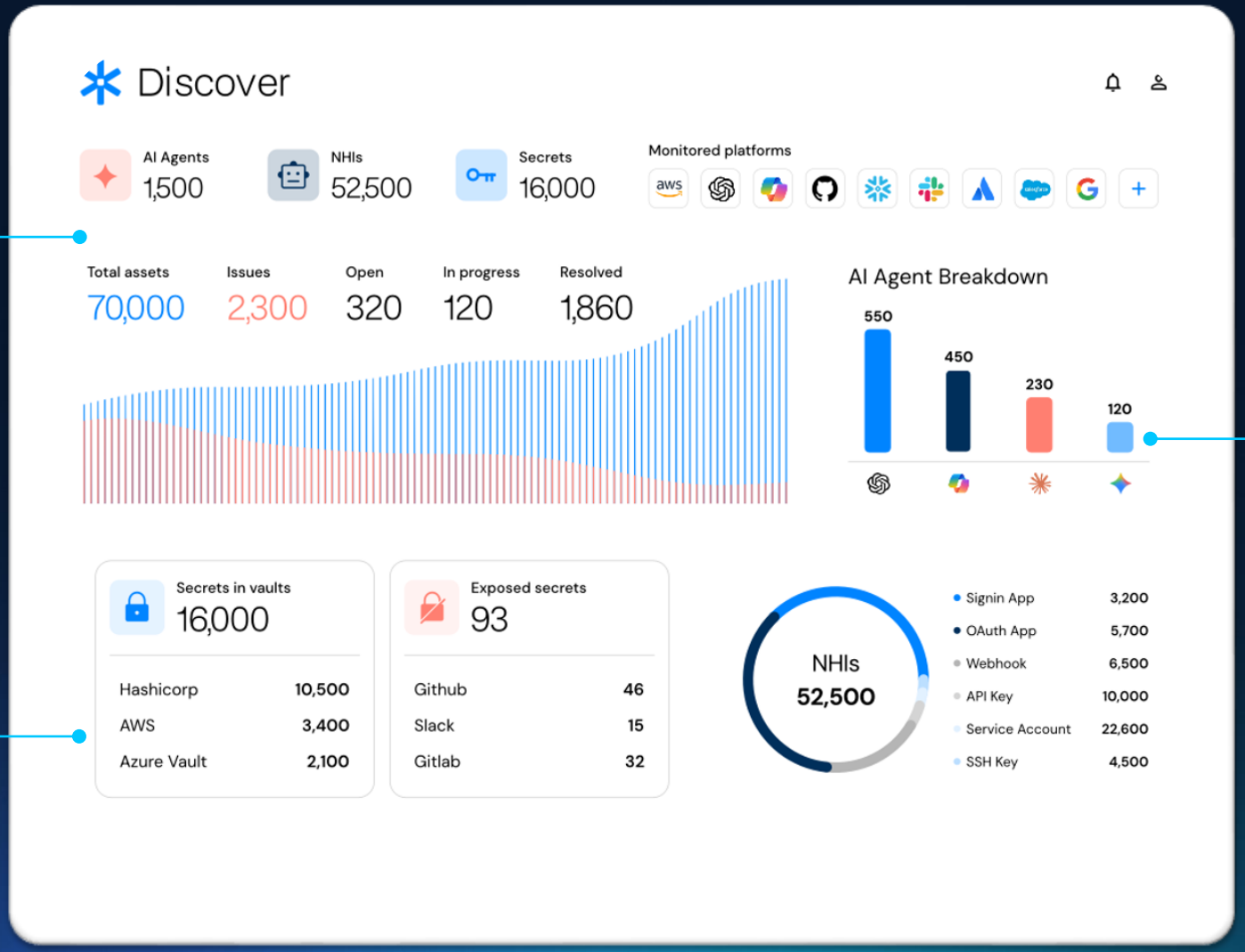
One view for AI agents, NHIs, secrets, connected platforms, open issues, and identity composition.

Real time Inventory

AI agents, NHIs, secrets, and connected platforms in a single visibility layer.

Risk and remediation

Issues, status, progress, and resolved findings stay visible together.



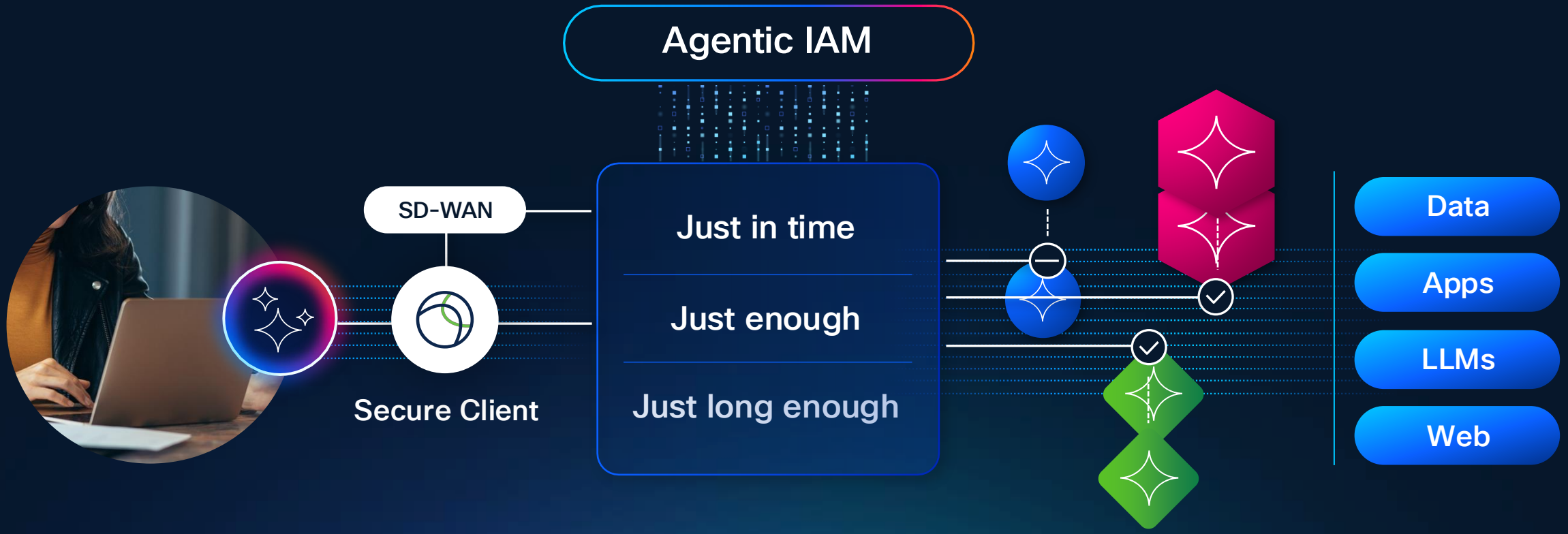
Identity context

Service accounts, OAuth apps, API keys, webhooks, SSH keys, and sign-in apps are mapped.

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

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

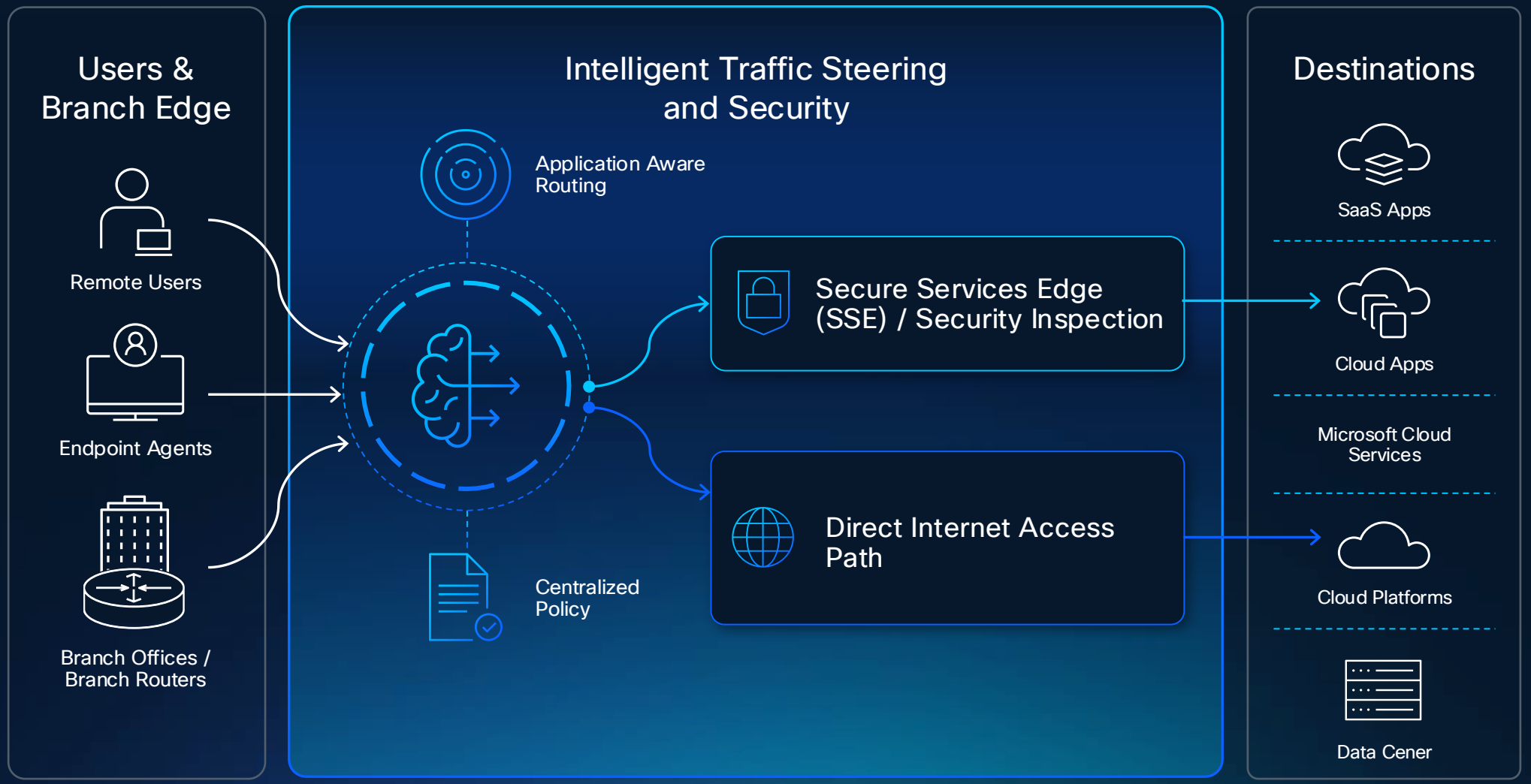
Experience Monitoring

+

DefenseClaw

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

Power of the platform

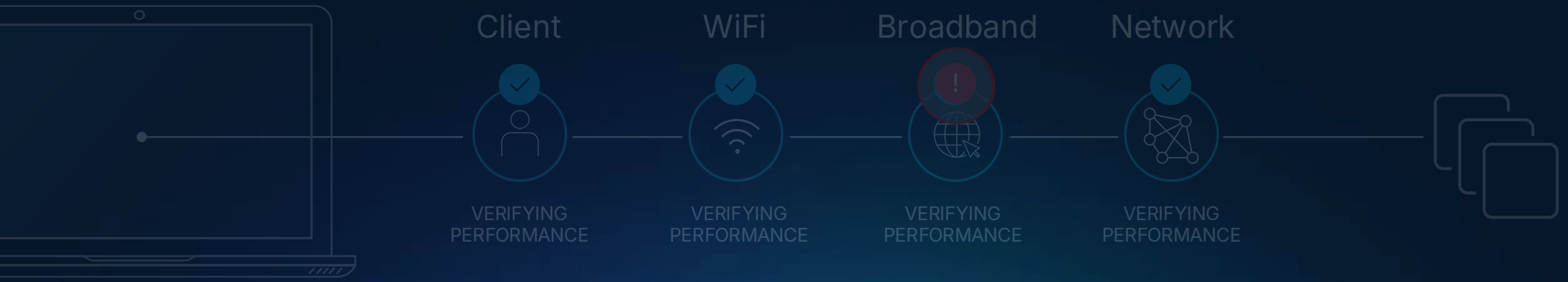


© 2026 Cisco and/or its affiliates. All rights reserved.

Fix issues fast with client-to-app visibility

Node: 01.ca.comcast.net

IP Address	88.86.143.25
Forwarding Loss	32% (6 of 17 packets)
Ave. Response	67.9 ms

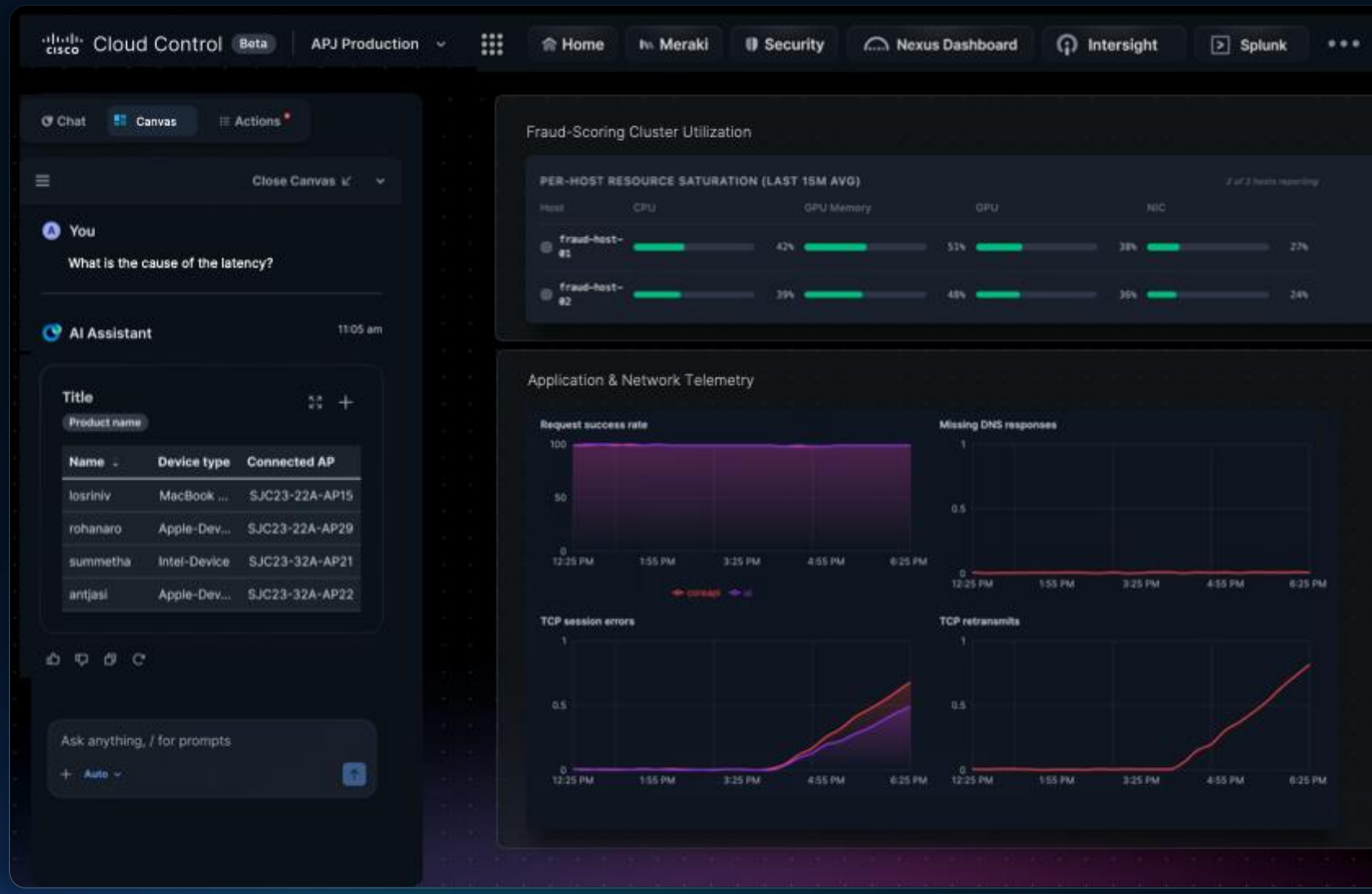


© 2026 Cisco and/or its affiliates. All rights reserved.

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

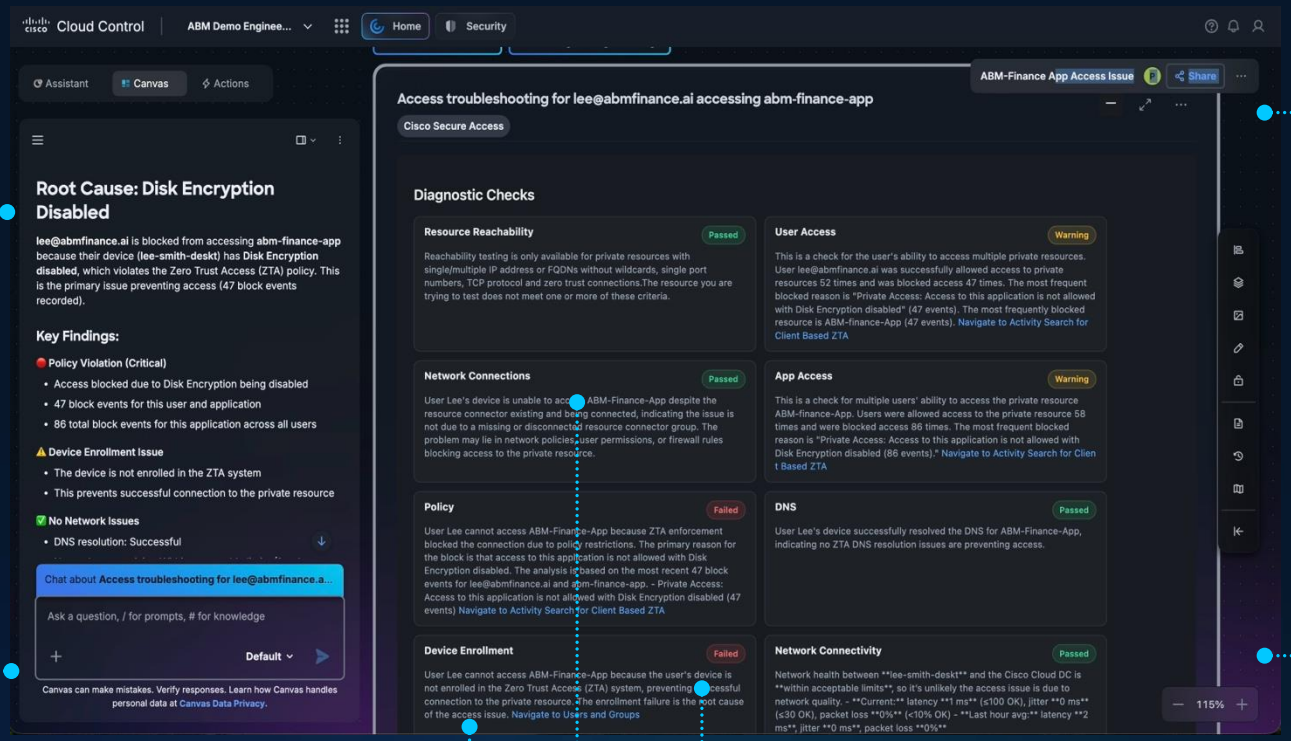
A workspace purpose – built for the operator

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.

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.

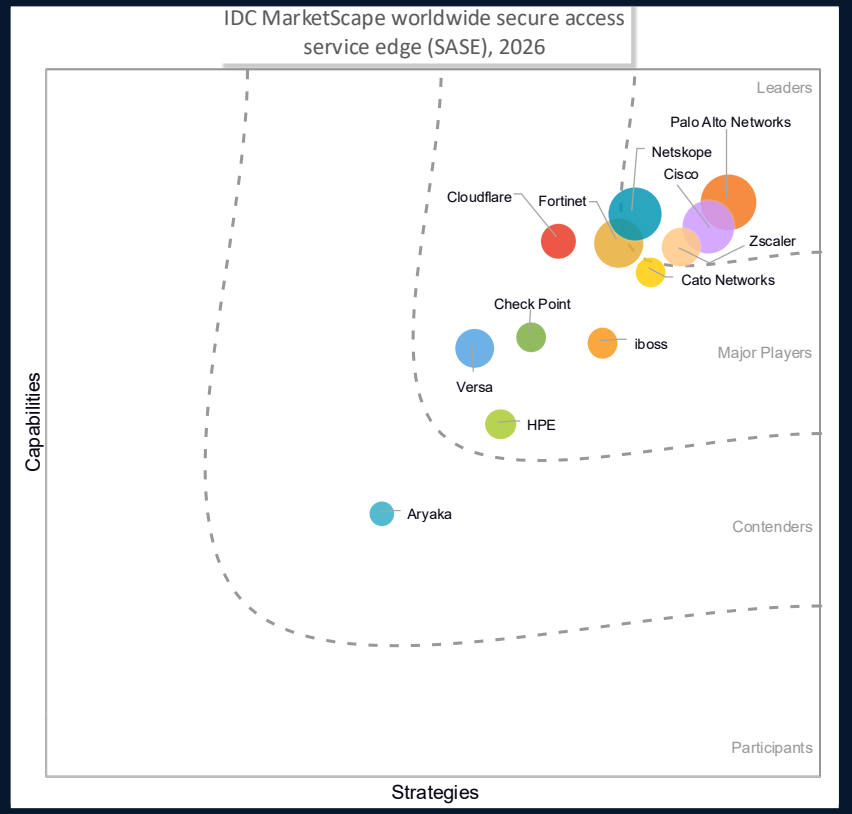


Figure 1: IDC MarketScape worldwide secure access service edge (SASE) vendor assessment

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/