CISCO Engage | Tech Day Miami

# Secure Connectivity for the AI-Ready Enterprise

## The Complete Story

Joe Rubino, Secure Routing, SASE SE

Antonio Hurtado, CISSP – Security SE – Southeast US


February 19, 2026

# Reimagine networking with innovative SD-WAN

## Simpler

Simplified networking that is scalable and efficient

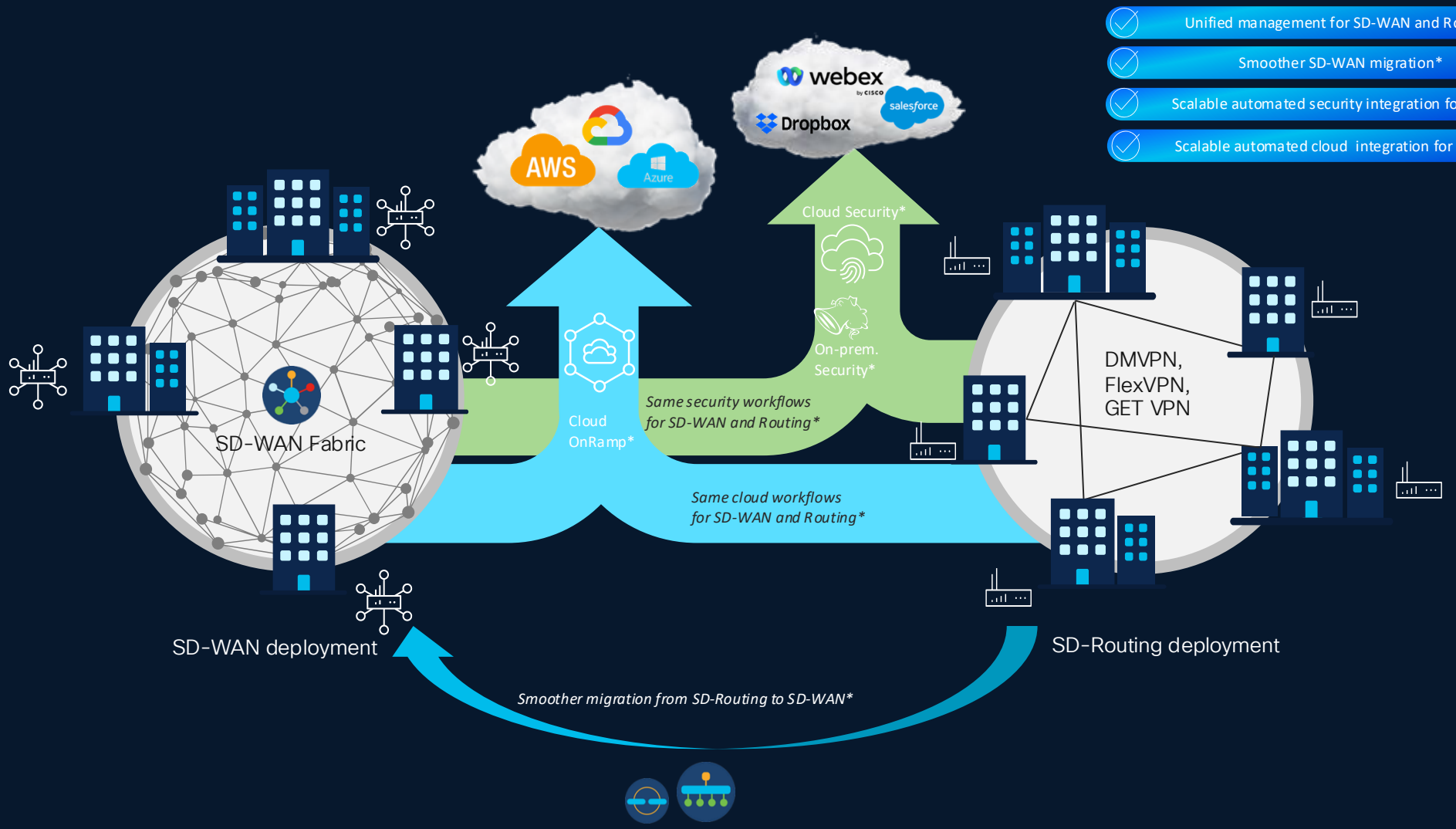
## Smarter

AI powered capabilities that power end-to-end visibility

## Safer

Security integrations designed to be SASE-ready and always-on

# Unified Management: SD-WAN and SD-Routing

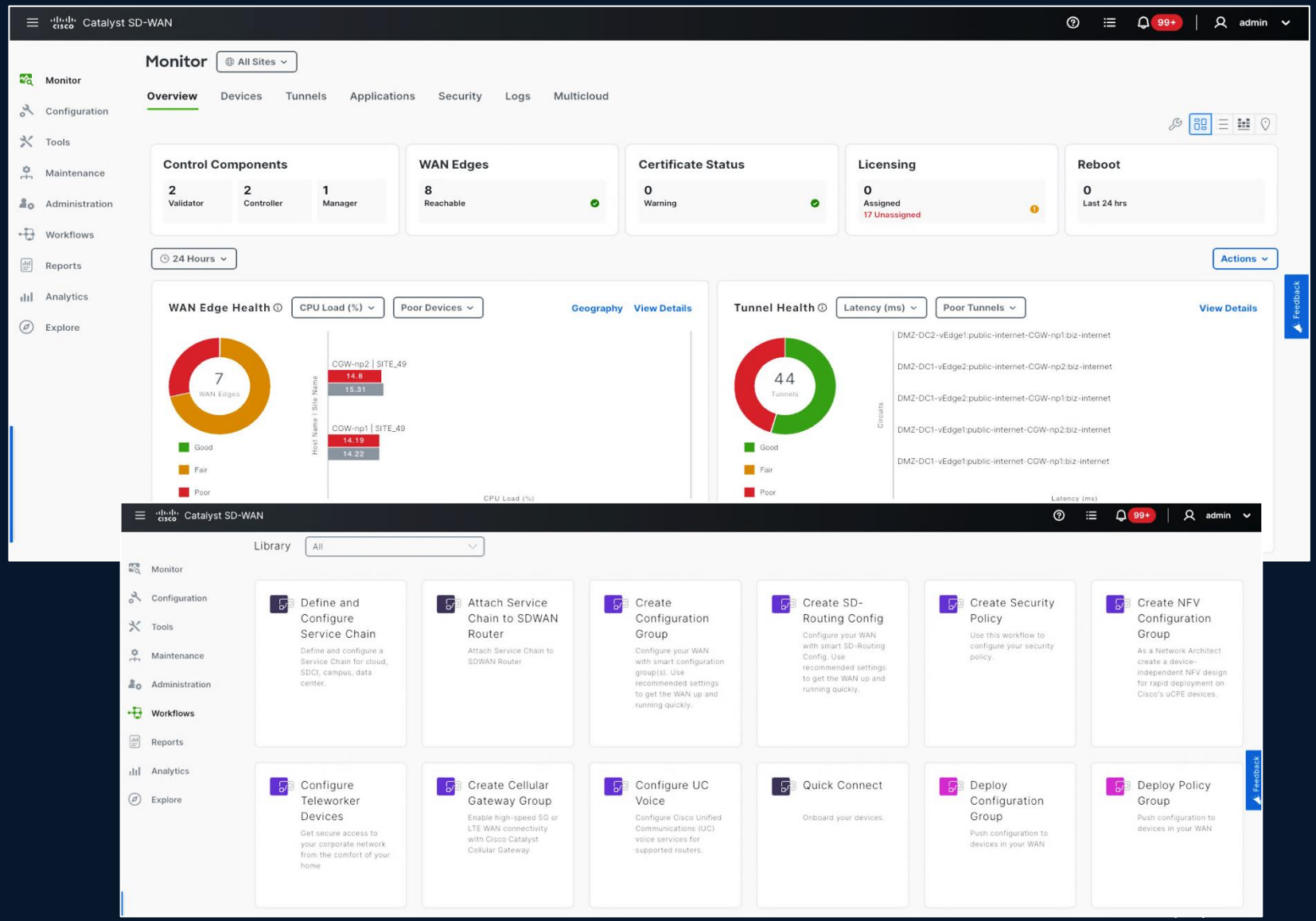





* On Roadmap for future releases

# SD-WAN Manager (UI)

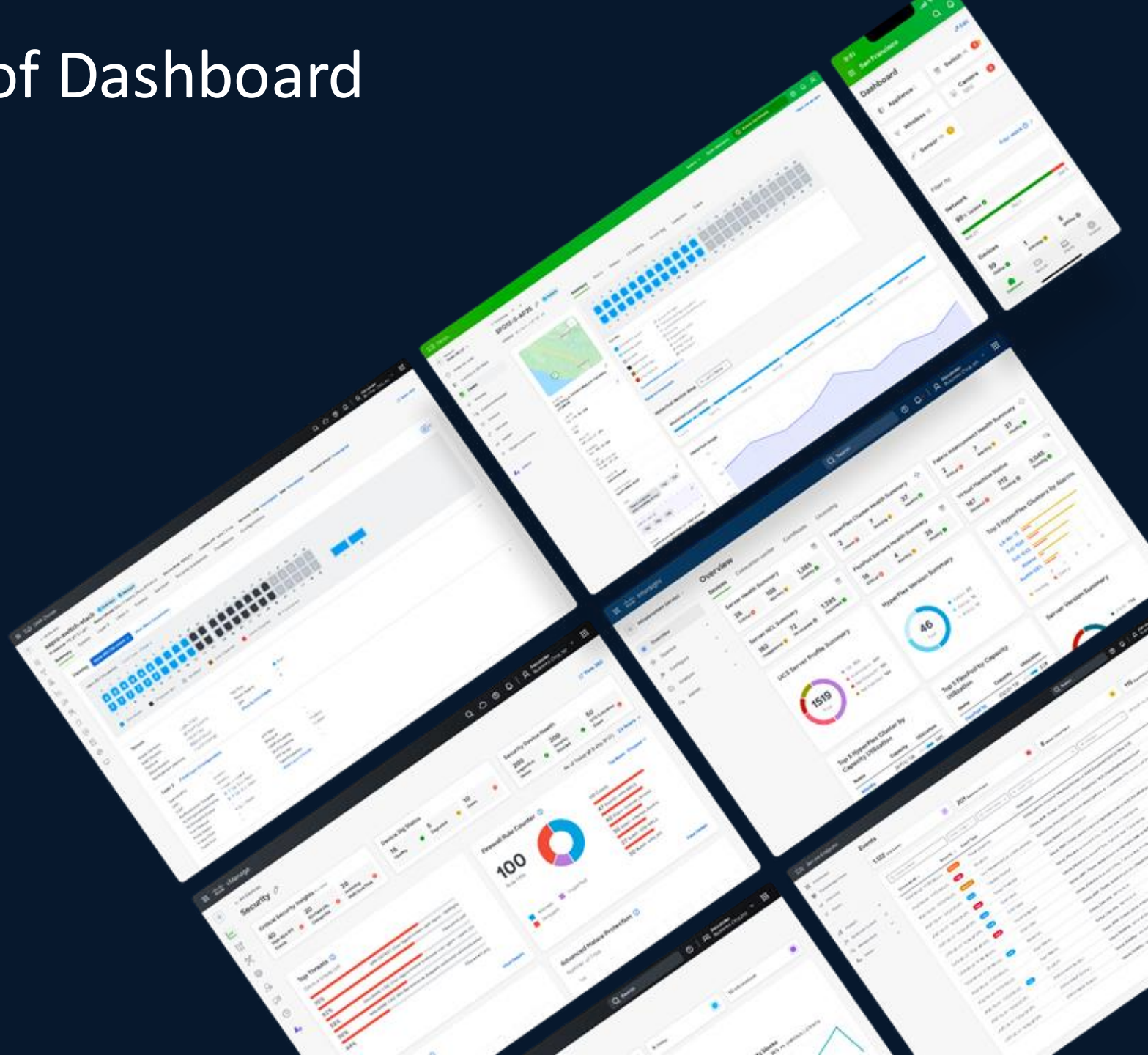
- Enhanced UI
- Guided Workflow
- Simplified Configuration
- Granular Management
- Smart Troubleshooting



# Common Look and Feel of Dashboard

**Unified experience** across Networking and Security dashboard

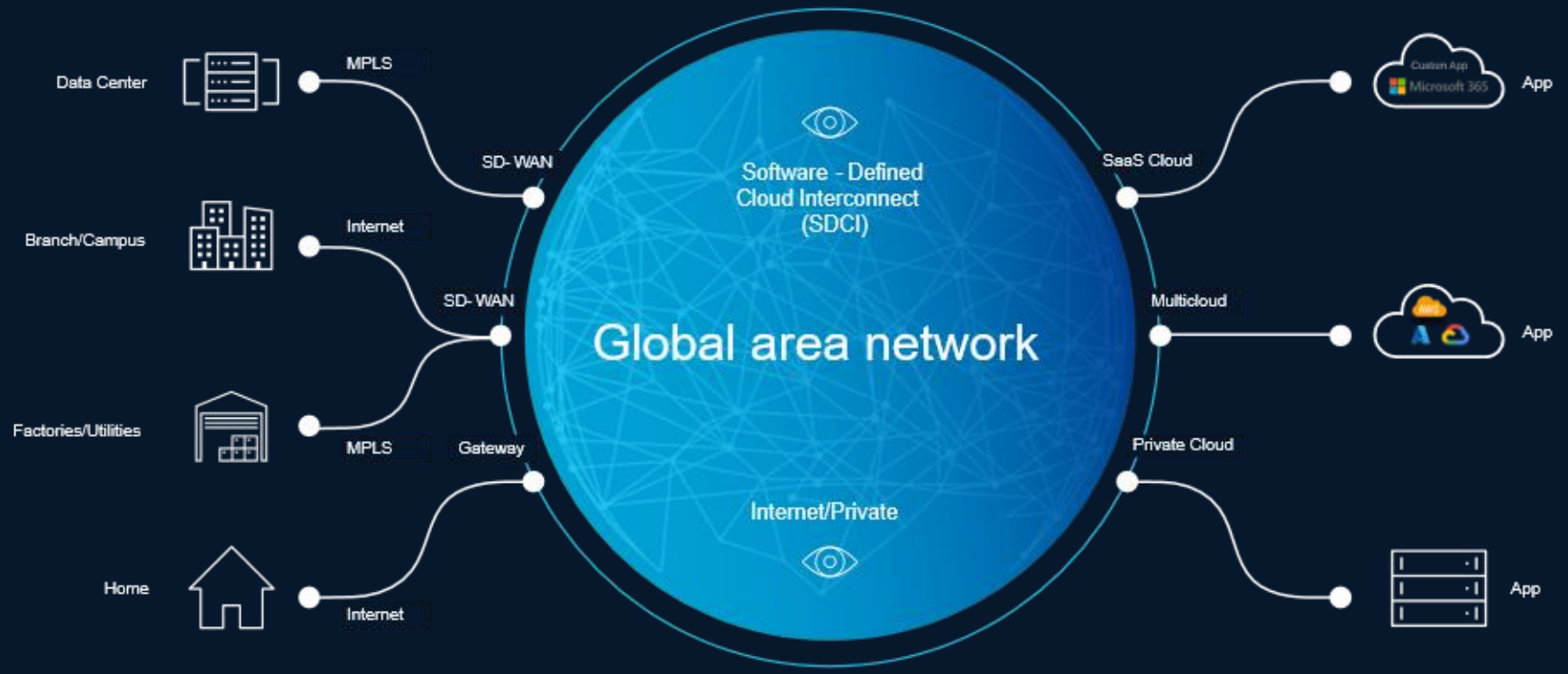
- Catalyst Center
- Catalyst SD WAN
- Cisco Security Cloud
- Meraki
- Spaces
- ISE
- Intersight



# Simplifying WAN management for the complex, distributed enterprise

| | Multi-Region Fabric (MRF) | Multi-tenant Edge | Cloud On-ramp |
|---|---|---|---|
| **What does it do?** | Simplify and segment large-scale, geographically distributed networks with a central core | Securely and efficiently manage multiple tenants on a shared SD-WAN infrastructure | Simplifies and automates secure, optimized connectivity between on-premises and cloud environments |
| **What is the value?** | Operational simplification, enhanced security, scalability, and improved performance across multiple regions | Reduces costs, improves operational efficiency, and provides tenant-specific control and visibility for multi-customer environments | Accelerates multicloud connectivity made easy for better user experiences, simplified operations, and strengthened security across hybrid environments |

# Cloud OnRamp: Making cloud easy for the hybrid world




- Optimized SaaS experience
- Simple, automated SD-WAN extension to the cloud
- Integrated middle-mile backbones
- Built-in, cloud-based security

Automated connectivity, discovery, and optimization for any cloud

# Reimagine networking with innovative SD-WAN

## Simpler

Simplified networking that is scalable and efficient

## Smarter

AI powered capabilities that power end-to-end visibility

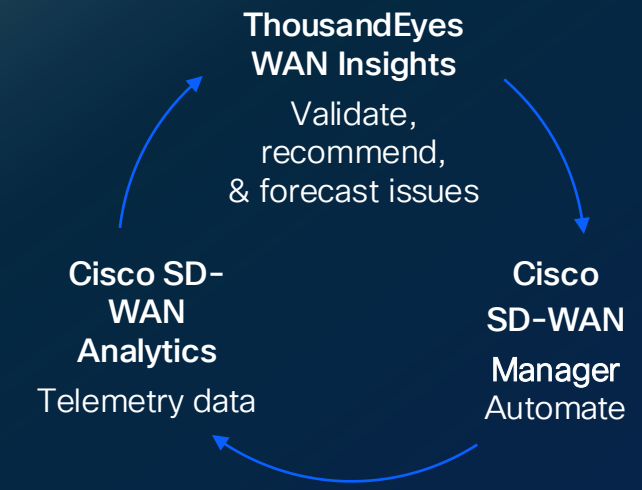
## Safer

Security integrations designed to be SASE-ready and always-on

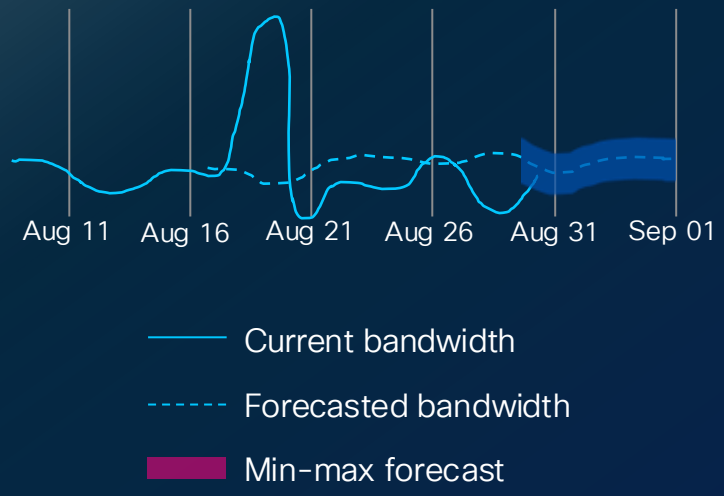
AI-native

# Network operations

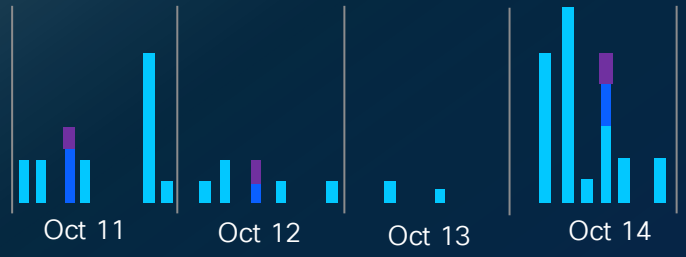
## Predictive Path Recommendations




## Bandwidth Forecasting

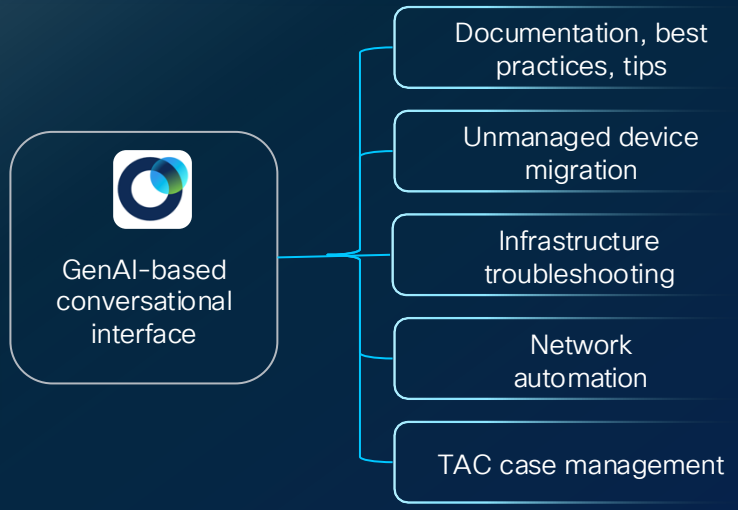



## Anomaly detection



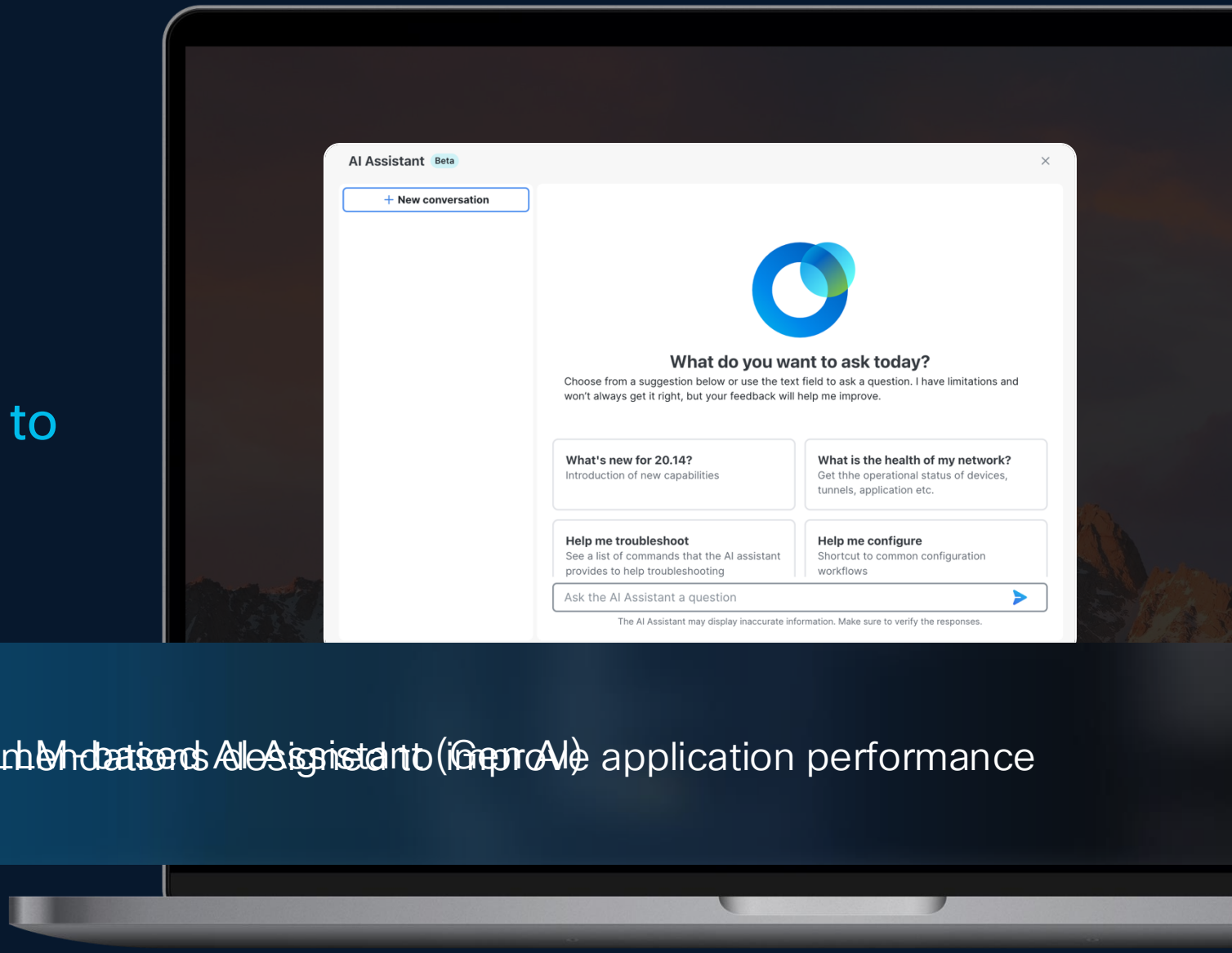

| KPI | Detected | Rate | # sites |
|---|---|---|---|
| Loss | 28 | 2.34 | 7 |
| Latency | 0 | 0 | 0 |
| Jitter | 0 | 0 | 0 |

## Cisco AI Assistant



# Using AIOps to streamline day-2 operations

## Proactively optimize network and application performance to achieve higher operational efficiency




**Predictive Path Recommendations**

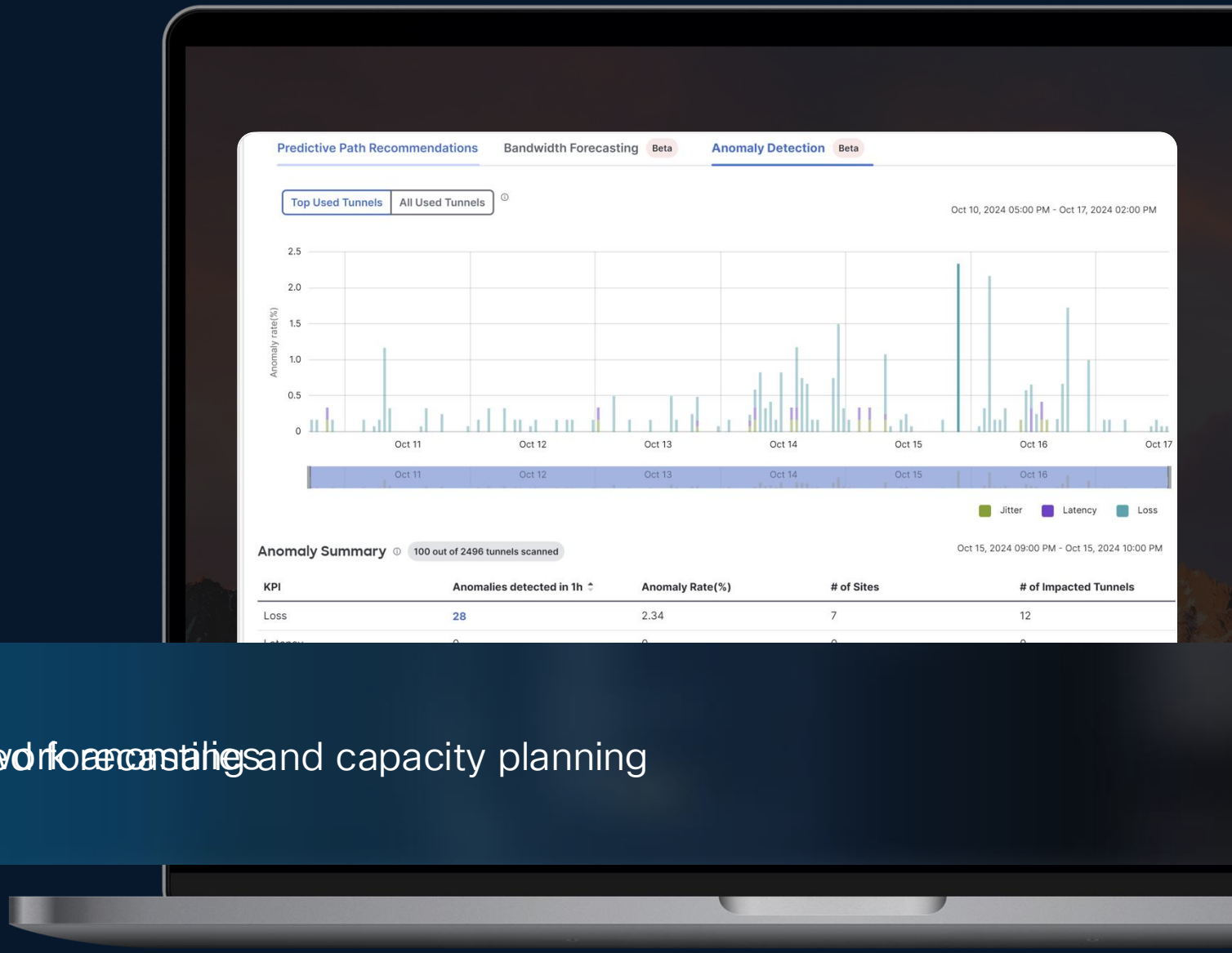
**AI Assistant**

Interactive LLM-based Assistant (GenAI)

Path recommendations designed to improve application performance

# Using AIOps to streamline day-2 operations

Mitigate issues **before** they impact performance along with root cause analysis to reduce MTTR



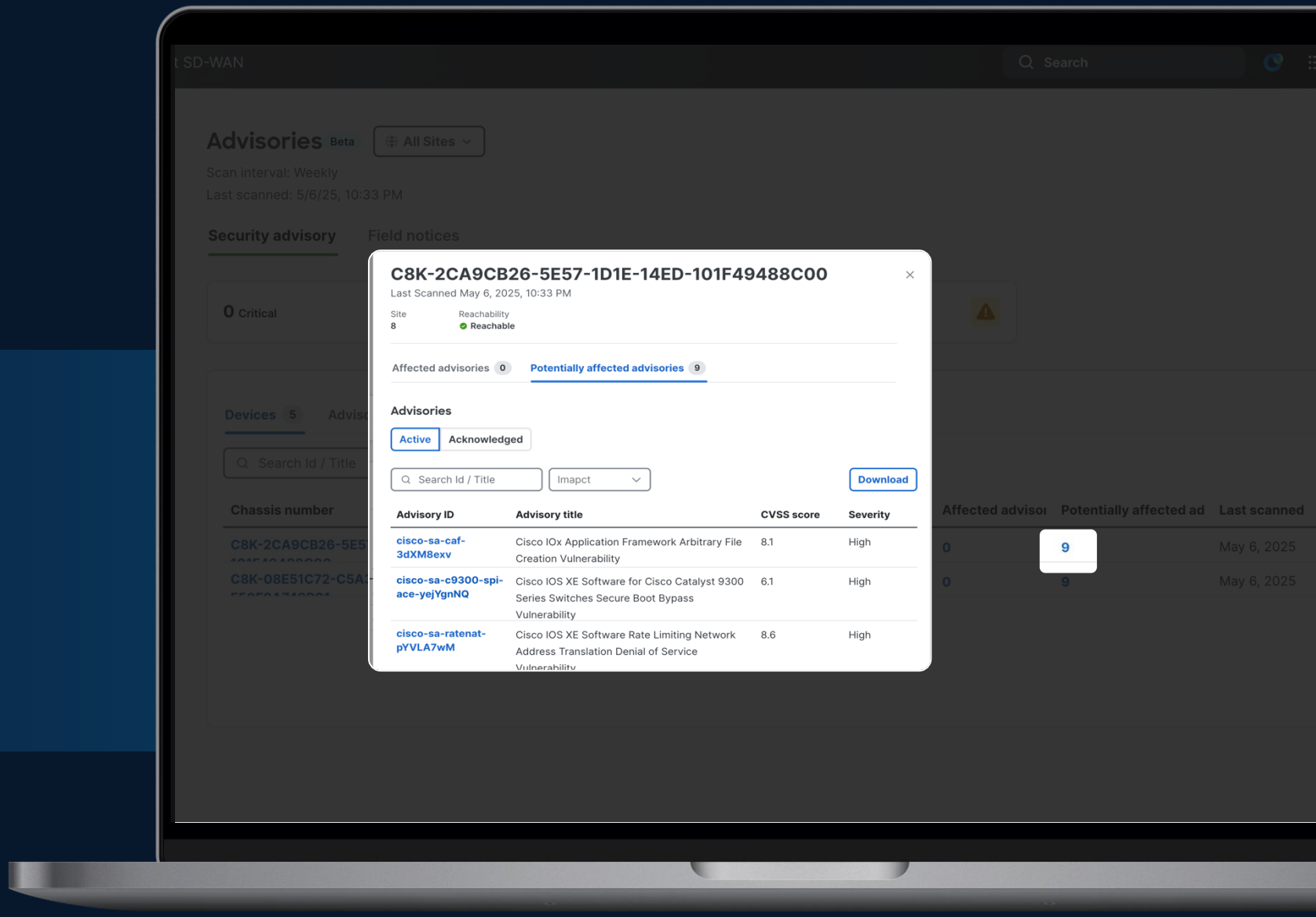

Anomaly Detection

Bandwidth Forecasting

AI/ML-based forecasting and capacity planning

# Proactively stay ahead of threats

Actionable insights on Security Advisories and Field Notices applicable to your SD-WAN fabric



# Reimagine networking with innovative SD-WAN

## Simpler

Simplified networking that is scalable and efficient

## Smarter

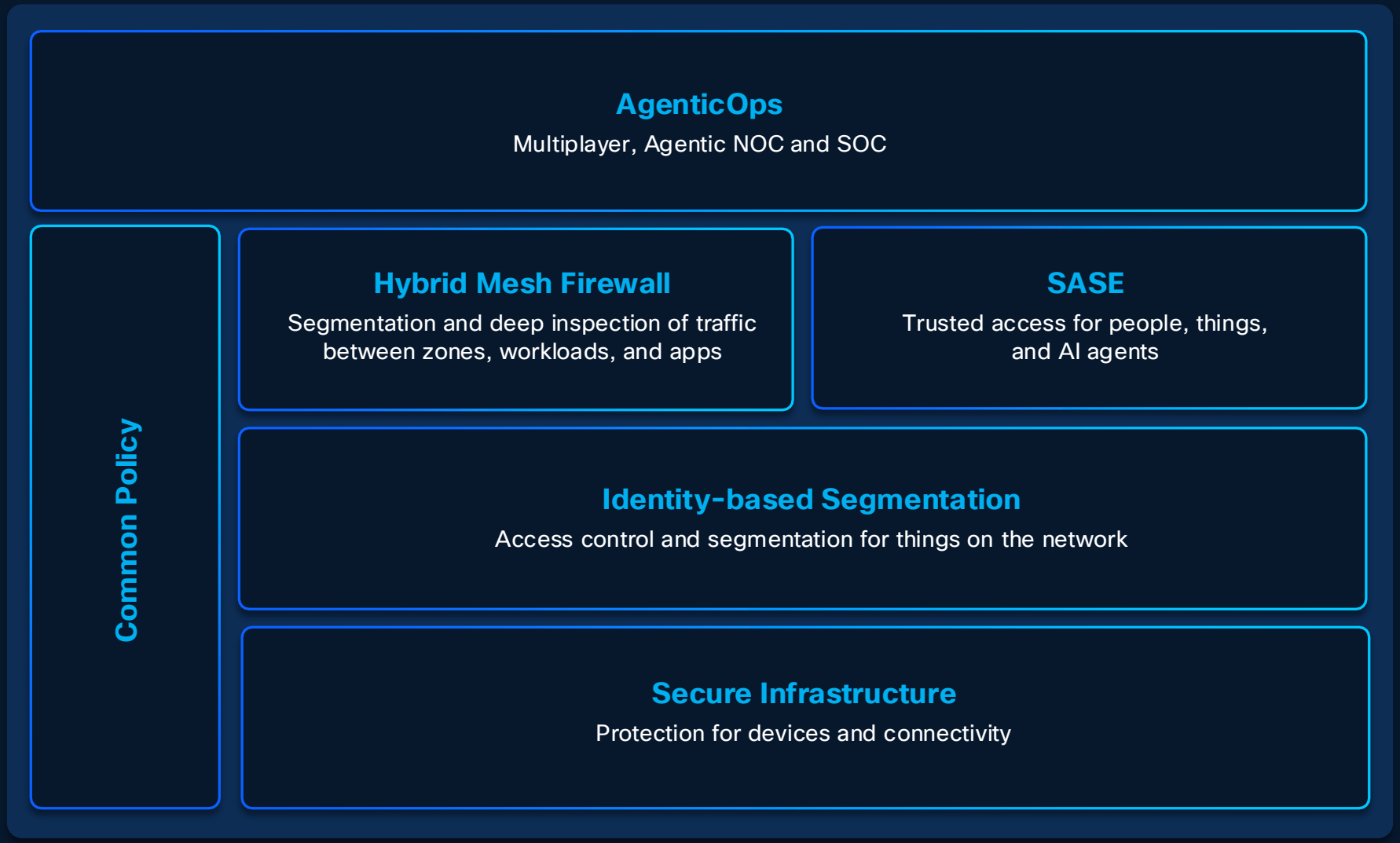
AI powered capabilities that power end-to-end visibility

## Safer

Security integrations designed to be SASE-ready and always-on

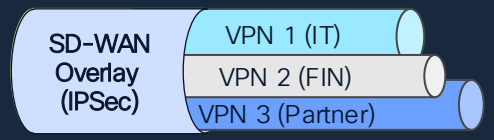
Secure Networking

# Reference design for fusing security into the network



# Granular Network and/or Security Segmentation (802.1x / ISE)

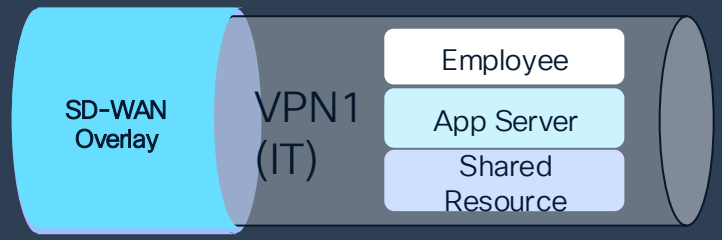
## Macro Segmentation




VPN (VRF) Level Segmentation

- IT VPN
- Finance VPN
- Partner VPN

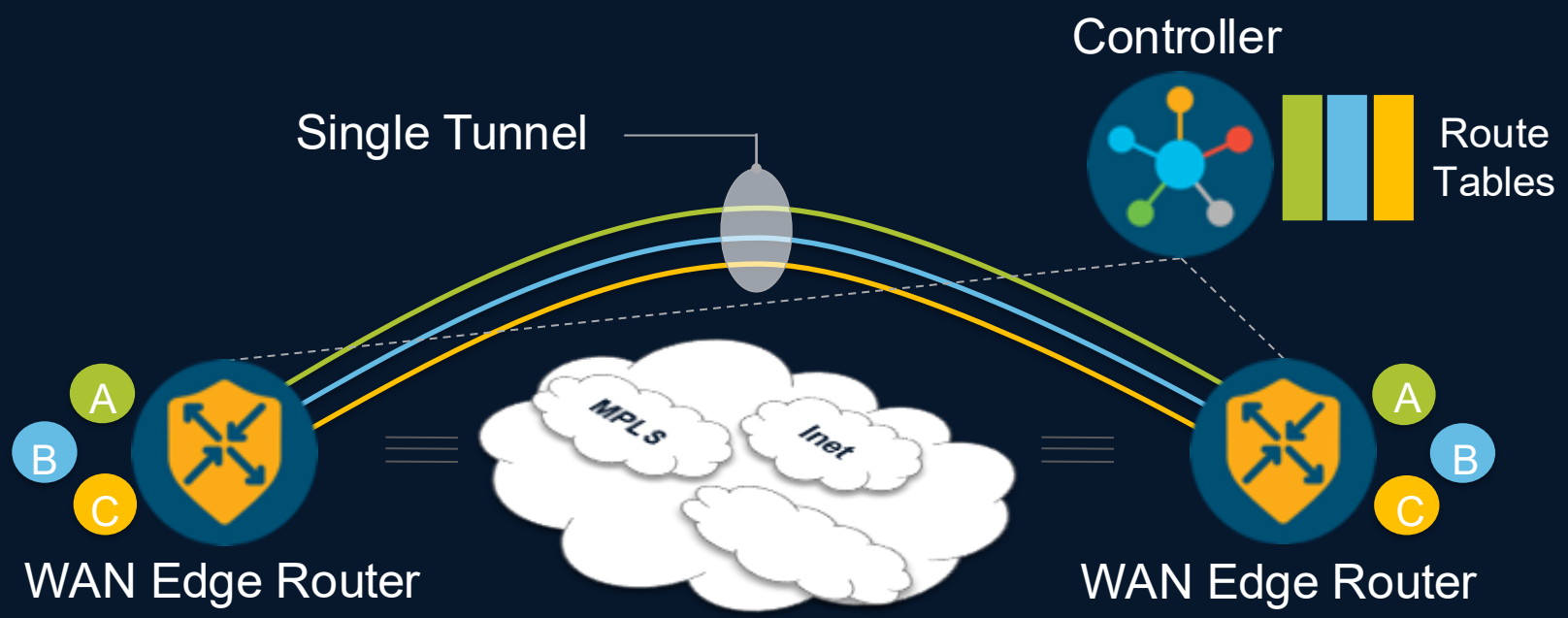
## Micro Segmentation

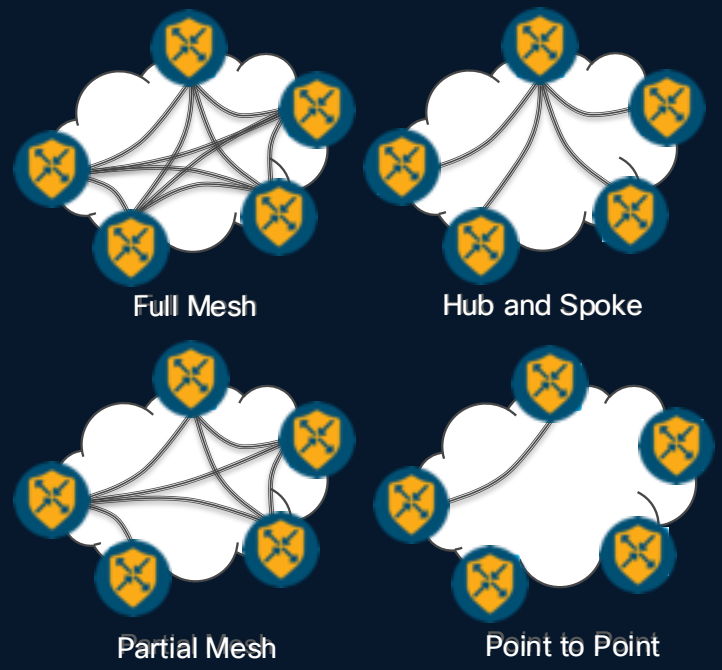



Group Level Segmentation (SGT)
Example: IT VPN

- Employee
- App Servers
- Printers

# End-to-End Segmentation with Multi-VRF Topology




Segment connectivity across the SD-WAN fabric without reliance on underlay transport

WAN Edge routers maintain per-VPN routing table for complete control plane separation

# Core Security Capabilities

SD-WAN Manager

SCC

Splunk

## Cisco Secure Router's Built-in NGFW

**L3 – L7 FW**
Manage traffic traversing the branch

**IPS/IDPS**
Protect assets from bad actors

**AMP**
Protect against malware

**Sandboxing**
File Analysis using Threat Grid

**URL-F**
Filter Internet traffic

**TLS Decryption**
Inspect encrypted traffic

**EVE***
Protect against Encrypted threats without full decryption

**Snort ML***
Protects from Zero day threats

+

## Cisco SSE Ecosystem

**Auto Tunnel + HA**
Automatic IPsec tunnels to SSE – 8/ 8 Standby

**Traffic Steering**
App based traffic inspection and redirection to SSE

**CASB**
Govern access to cloud applications

**FWaaS**
Manage traffic to the internet

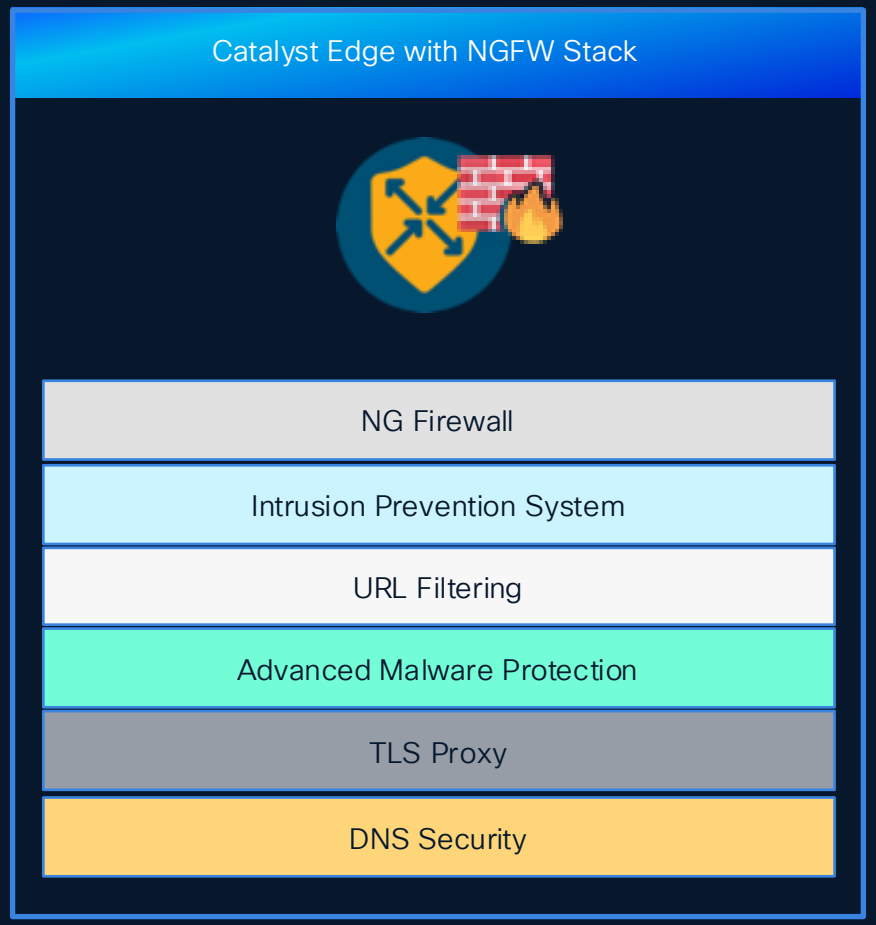
**DLP**
Protect sensitive data from unauthorized access

**DNS/SWG**
Protect web servers / applications



** Future capabilities*

# Catalyst SDWAN with L7 NGFW





ISE/AD Integration for Identity based FW rules

LAUNCHED JUNE 2025

# Cisco 8000 Series Secure Routers for every size location

## Small Branch: 8100

4 Variants

IPsec:
Up to 1.5 Gbps

Threat Protection:
Up to 1 Gbps

Ports:
1 GE

2 NEW SKUs

## Medium Branch: 8200

4 Variants

IPsec:
Up to 5 Gbps

Threat Protection:
Up to 2.5 Gbps

Ports:
2.5 GE, 2 x 10 GE

## Large Branch: 8300

2 Variants

IPsec:
Up to 20 Gbps

Threat Protection:
Up to 7 Gbps

Ports:
5 GE, 4 x 10 GE

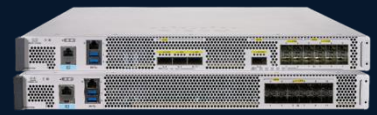
## Campus: 8400

2 Variants

IPsec:
Up to 45 Gbps

Threat Protection:
Up to 11 Gbps

Ports:
25 GE



## Data Center: 8500

2 Variants

IPSec:
Up to 60 Gbps

Route Scale up to 8M

Ports:
40/100 GE

# Secure Networking Processor

## Purpose built for the Future AI Workloads

C8400, C8300, C8200, C8100 Series Secure Routers are powered by ‘secure networking processor’

### Security

- Inline Crypto
- PQC capable crypto engine
- Cisco Secure Firewall acceleration
- Built-in AI/ML inferencing engine


### Networking

- Integrated hardware accelerators
- Various Ethernet standards– 2.5mGig, 5mGig, 10GE, 25GE
- Performance defined Power – 30%+ power saving
- Programmable uCode – feature parity

# Key Takeaways

## Secure networking processor

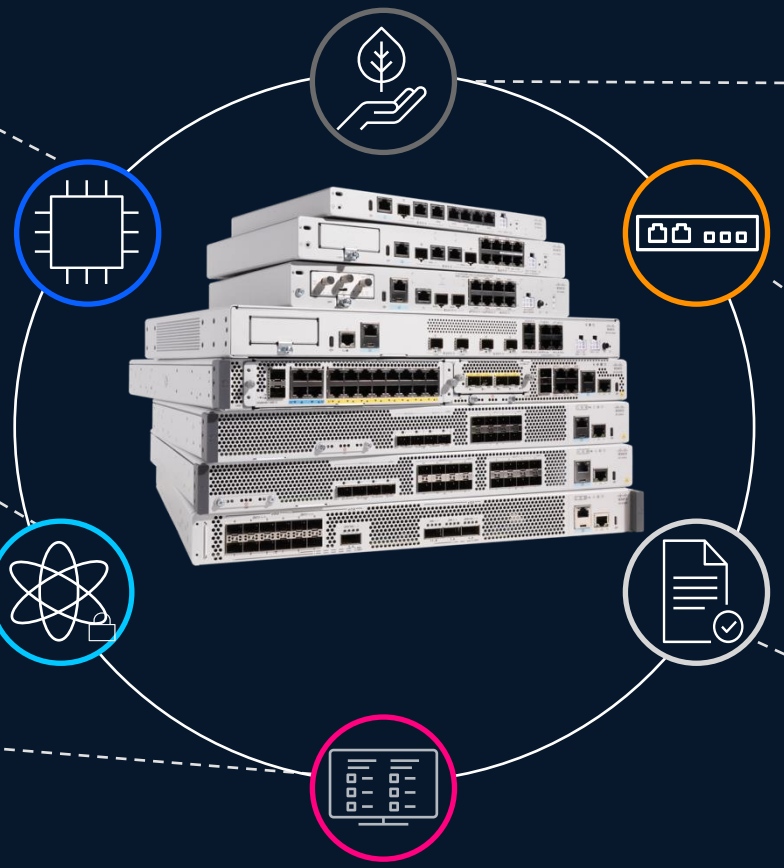
- Integrated hardware accelerators
- Inine crypto processing
- Increased performance, uncompromised security

## Post-Quantum Crypto Capable

- Prepare the network for quantum attacks
- NIST compliance for IPsec & MACsec
- Post Quantum Safe secure boot (future)

## Management

- Catalyst SD-WAN Manager
- Catalyst Center
- Meraki Dashboard (future – mid 2026)



## Sustainability

- Fan-less medium branch 8200-G2
- Fan-less large branch 8355-G2
- Energy star certified: C8400,8500-G2

## Port Density

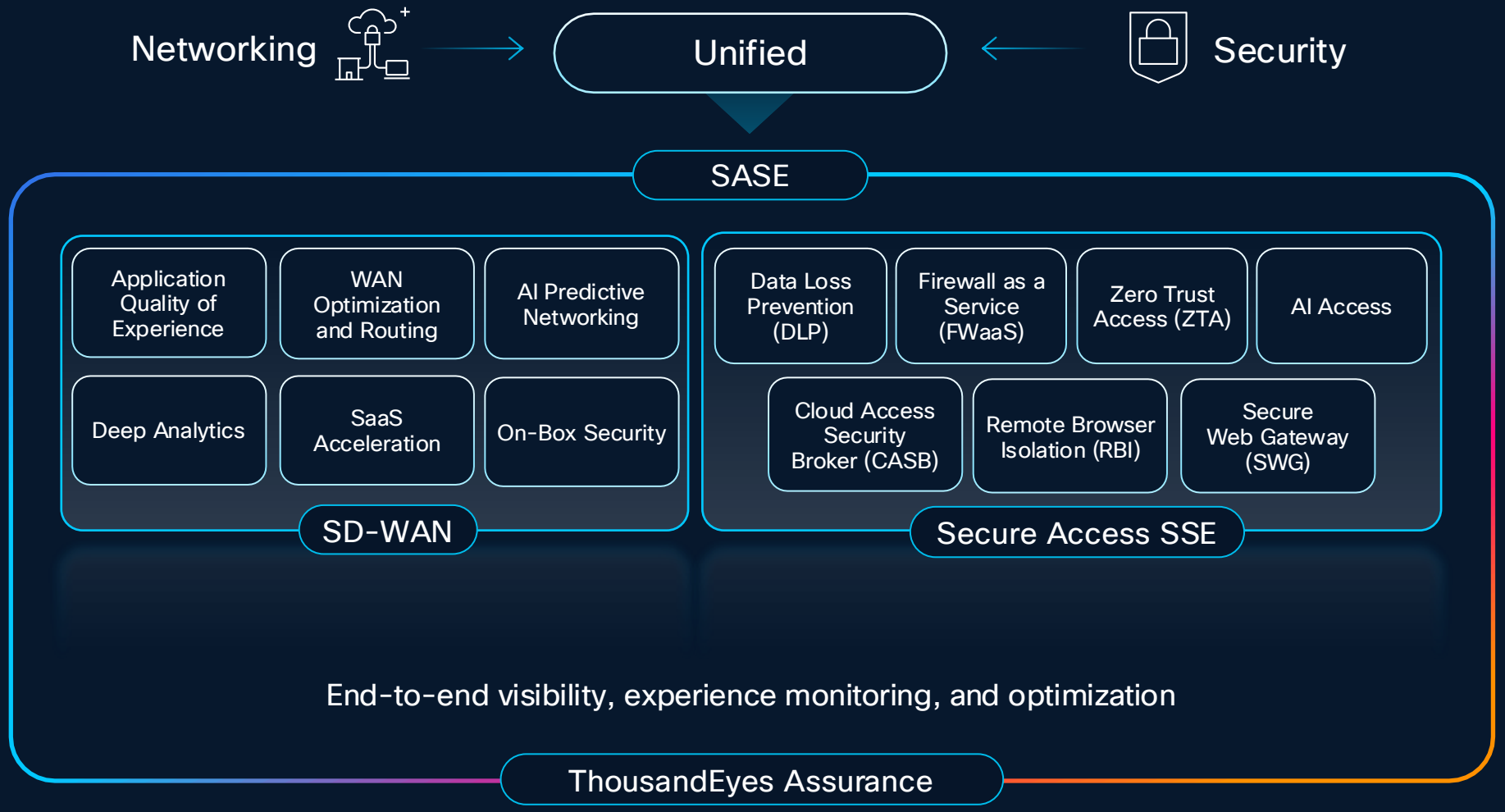
- Flexible L2/L3 ports
- 2x 10G port medium branch
- 4x 25G port campus router

## Documentation & More

- Individual TDMs, mechanical drawings, cheat sheets, sustainability
- Datasheets, HIG, SCG, FAQs, RFP Boilerplate
- CCAPP, Router Selector, Power Calc.

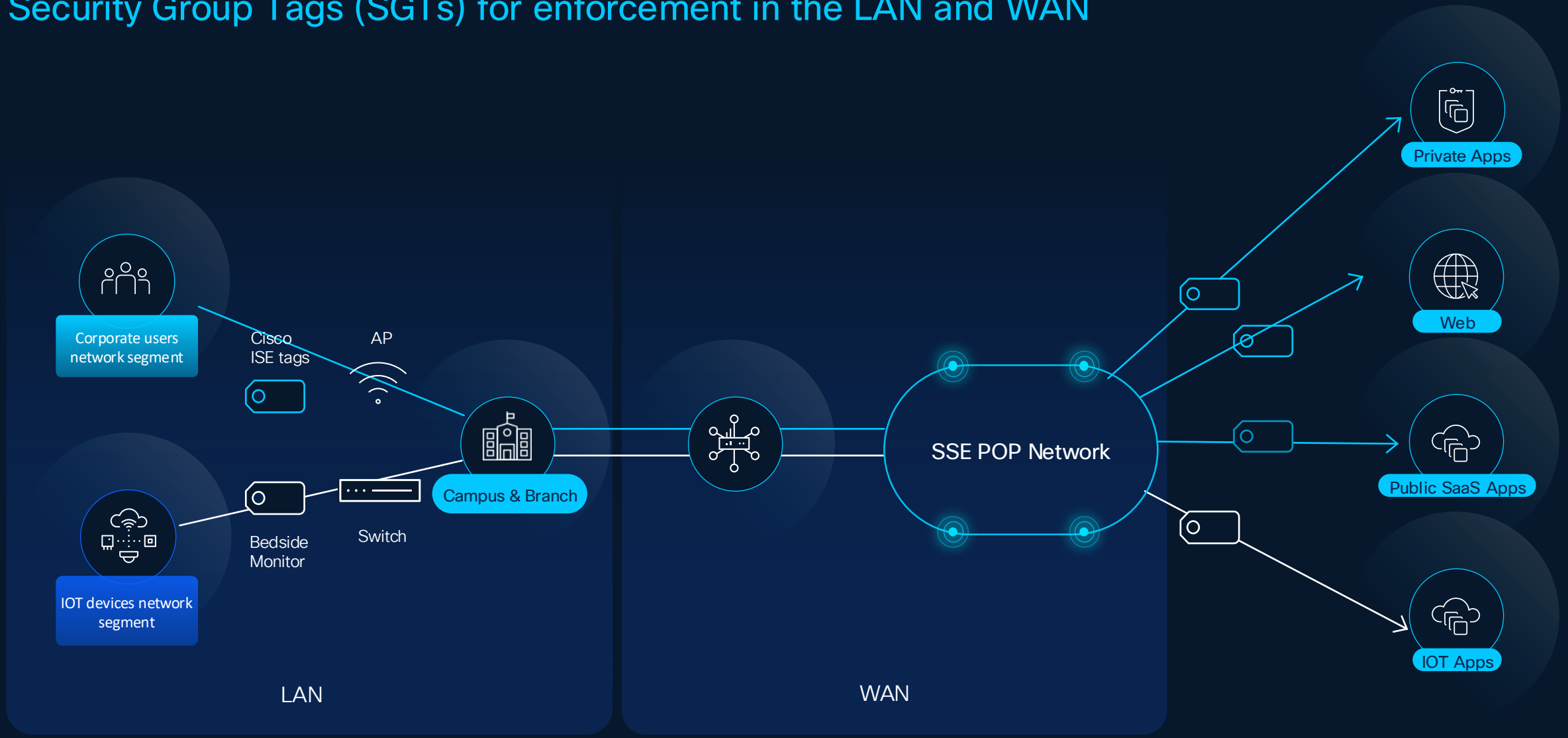
# Cisco Secure Access Service Edge (SASE)

Performance, reliability, and security. Unified.



# Policy-based segmentation for secure IT, IoT and OT

## Security Group Tags (SGTs) for enforcement in the LAN and WAN



# SASE: Secure Access integrated with Cisco SD-WAN

## Your security strategy for a hyper-distributed world

## SASE

Secure
SD-WAN

Converged set of cloud networking

+

Secure
Services Edge / CSA

Converged set of cloud security

End-to-end Assurance with ThousandEyes



cisco

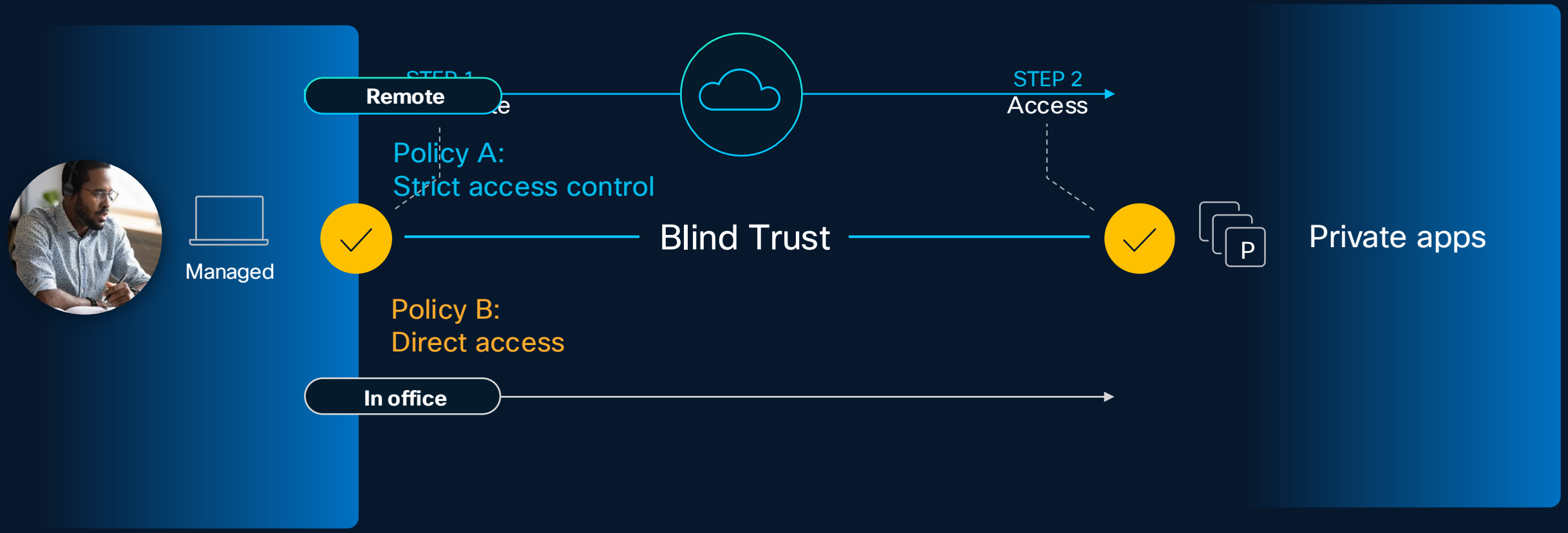
# Cisco Zero Trust Access

Secure SD-WAN + Secure Services Edge + Trusted Identity Edge

SINGLE VENDOR SASE

End-to-end Assurance with ThousandEyes

# Traditional ZTA: Work from home solution




Managed devices, private apps

Different policies for home versus office

Blind trust between authentication and access

# Cisco Zero Trust Access

Unmanaged

Managed

Remote

In office

## Native experience

Popular mobile devices and Google Chrome

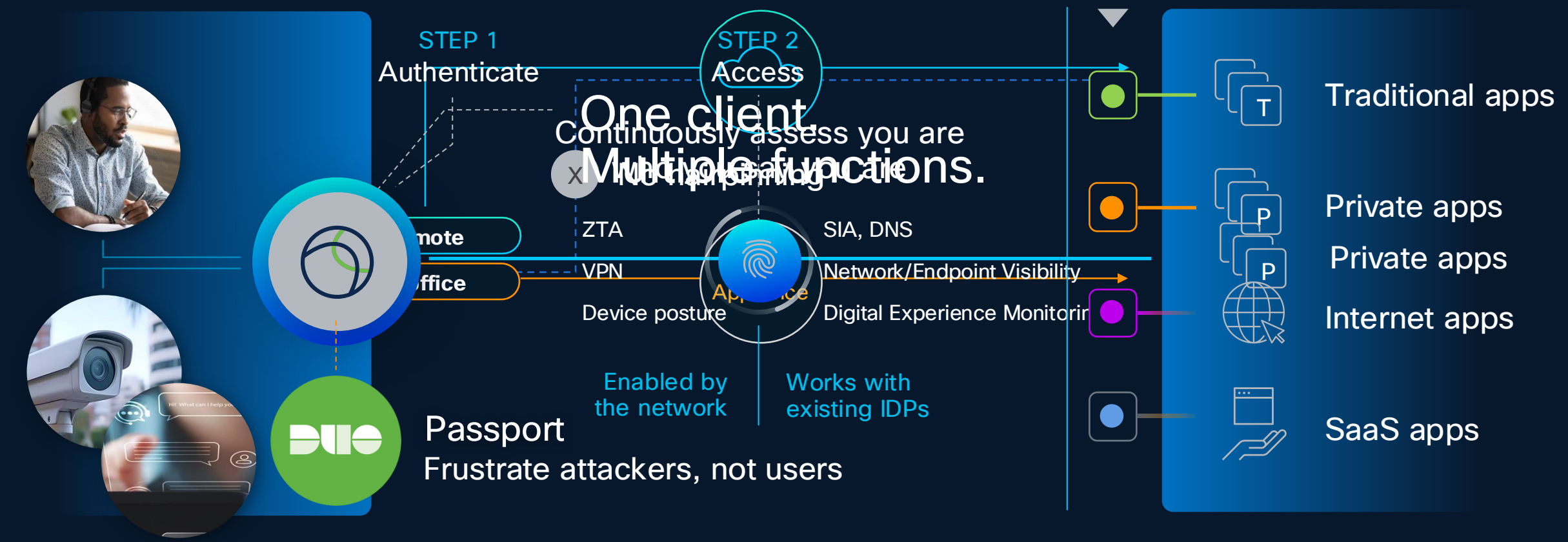
## Things and agents are people too

P

Private apps

Every device, people, things, agents everywhere

# Cisco Zero Trust Access




Every device, people, things, agents everywhere

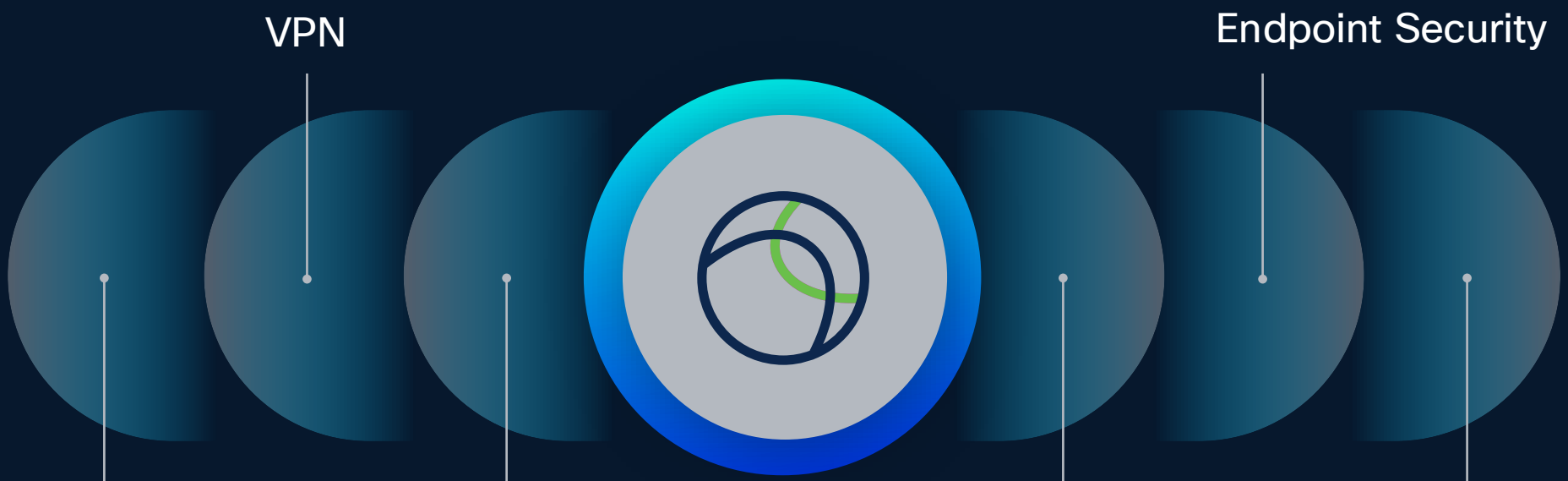
One policy, all apps, no hairpinning

Seamless user to app experience

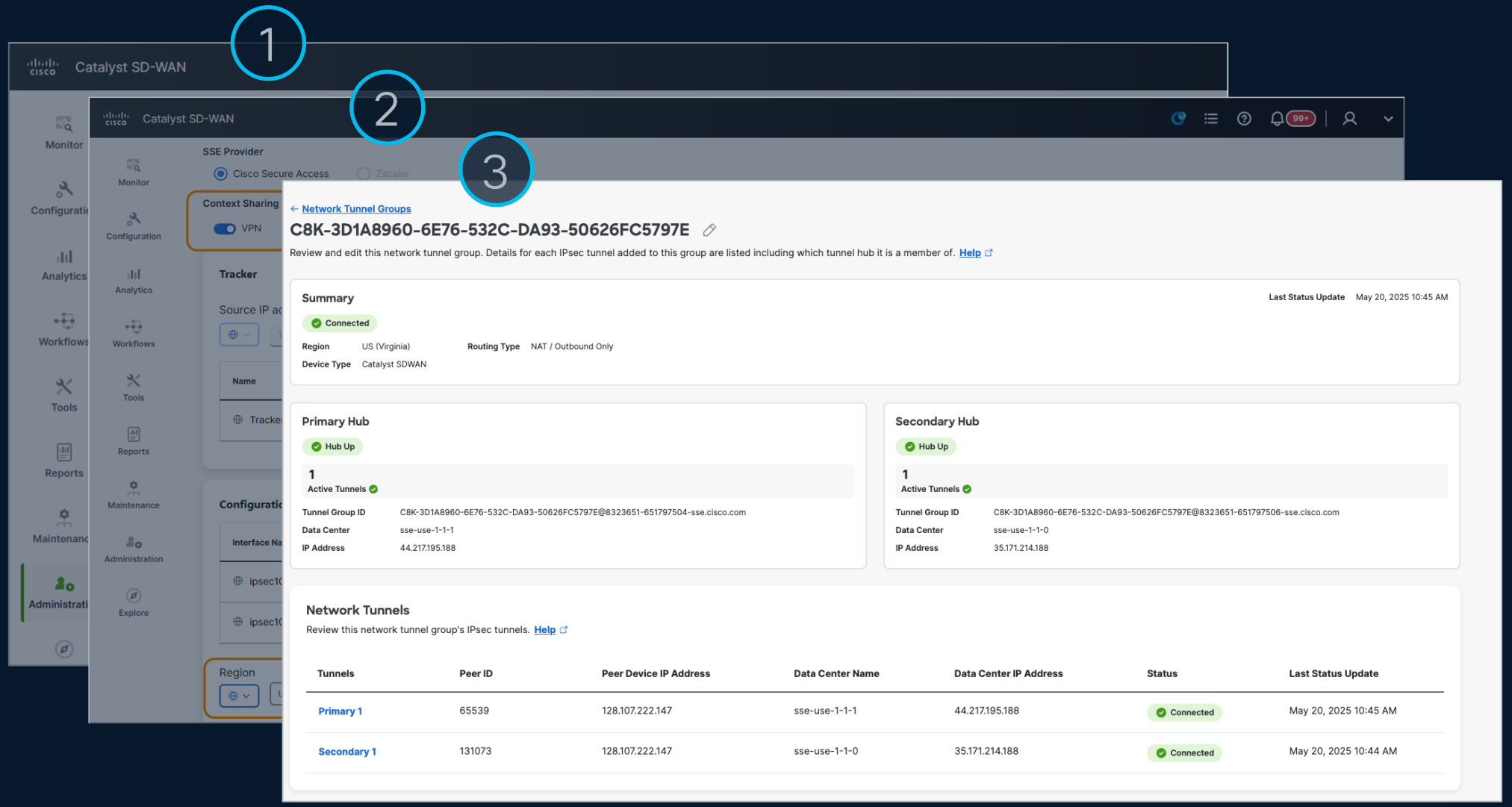
No blind trust with Identity Intelligence

# Zero Friction

# One client, multiple functions



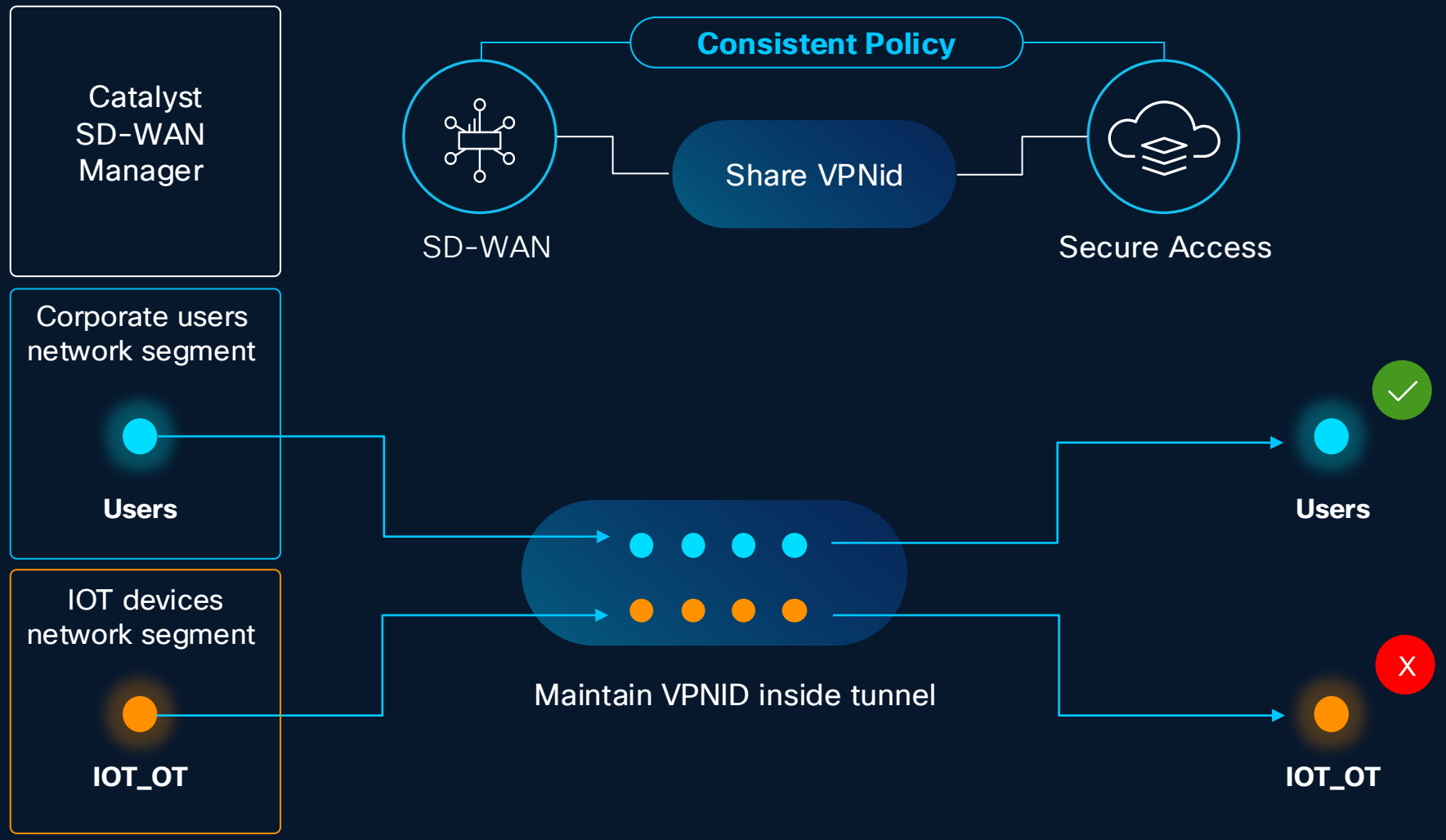
# Extending SDWAN Identity Context to Secure Access



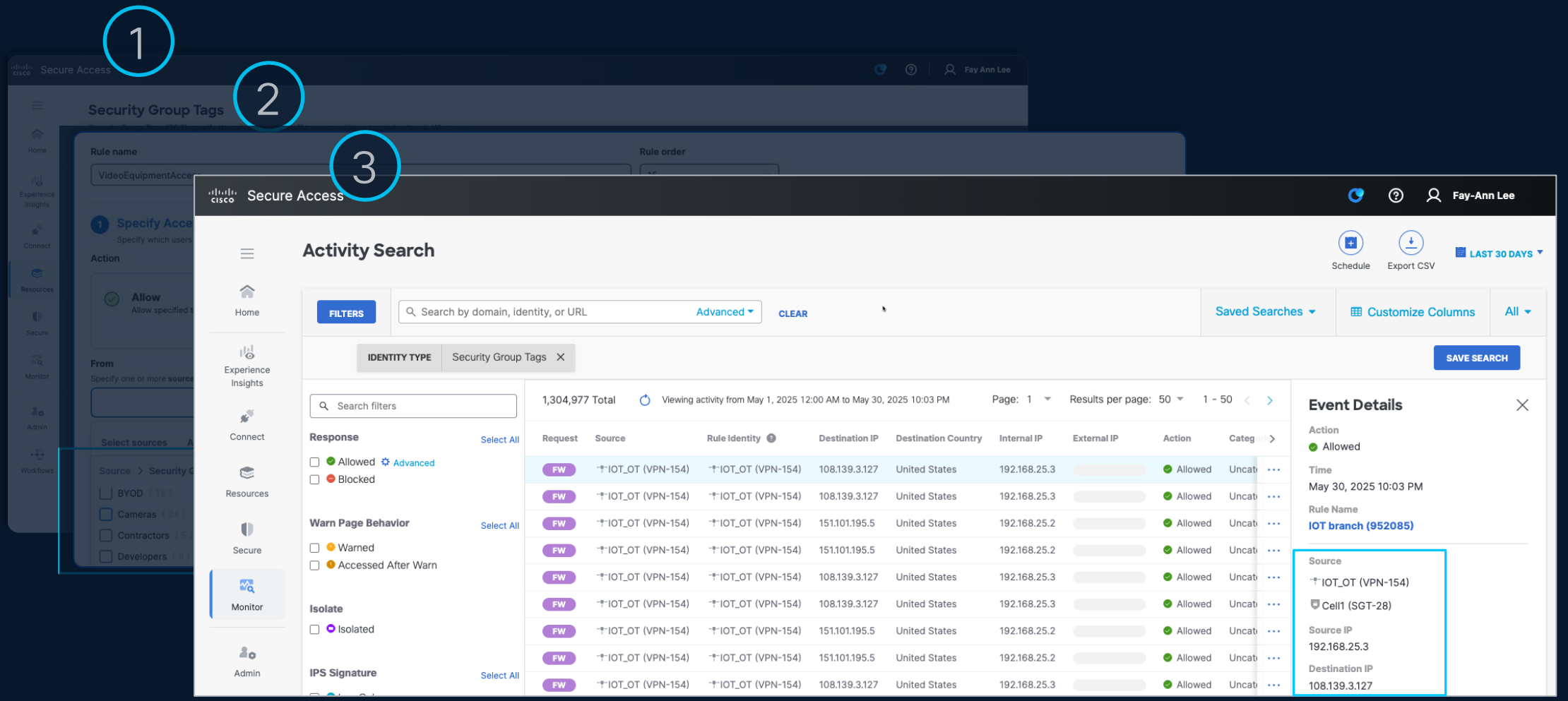
# Catalyst SD-WAN

## VPNid support for consistent segmentation

- VPNiD Based policy across both SDWAN & Secure Access
- Maintain segmentation in branch & in the cloud



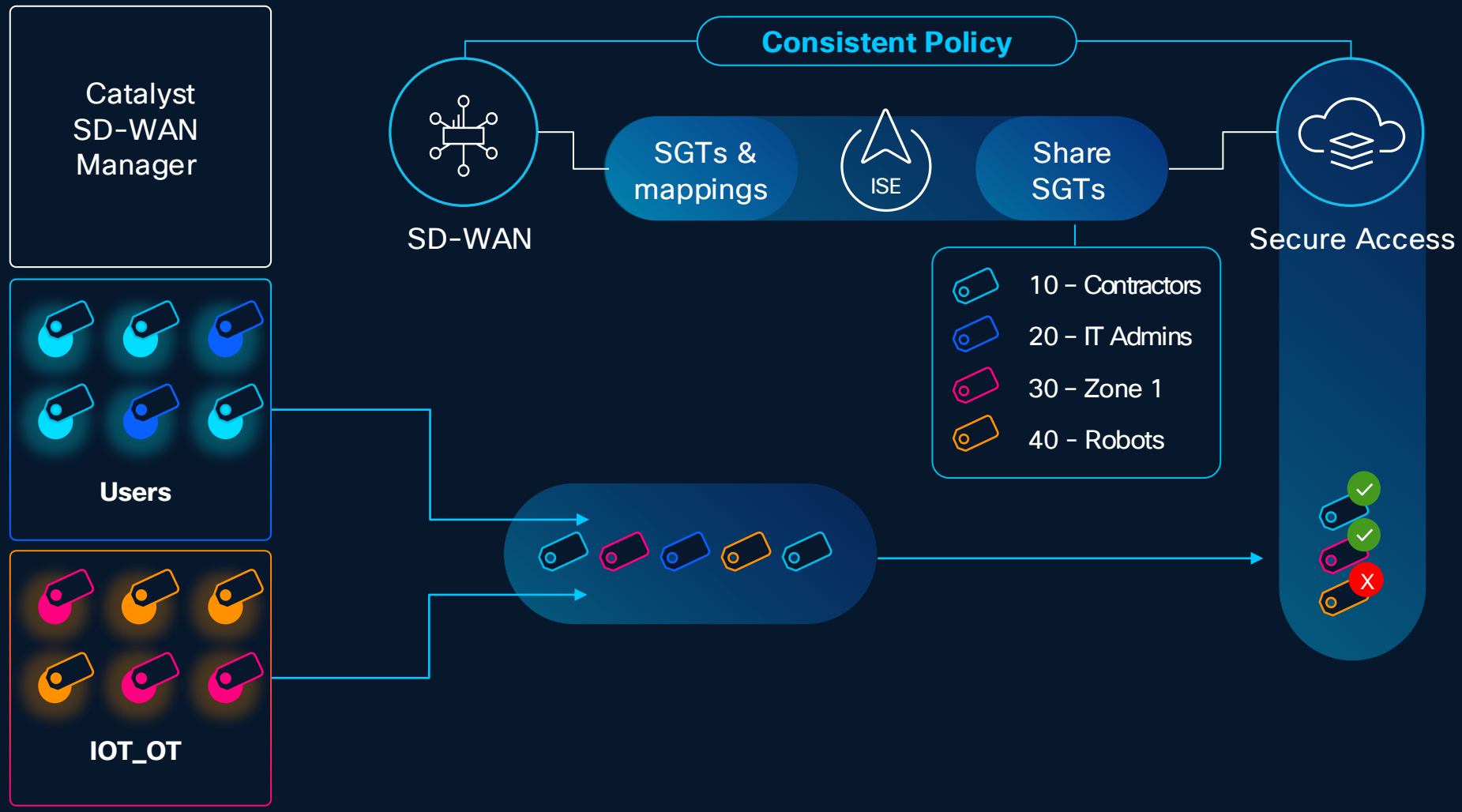
# Leveraging SGTs in Cloud based policy enforcement



# Identity Services Engine (ISE)

## Leverage SGTs for granular access control

- SGT Based Policy across network & Cloud
- Maintain micro segmentation through Secure Access
- Uniquely identify devices and traffic based on context from ISE
- Apply policy to SGT Based identity

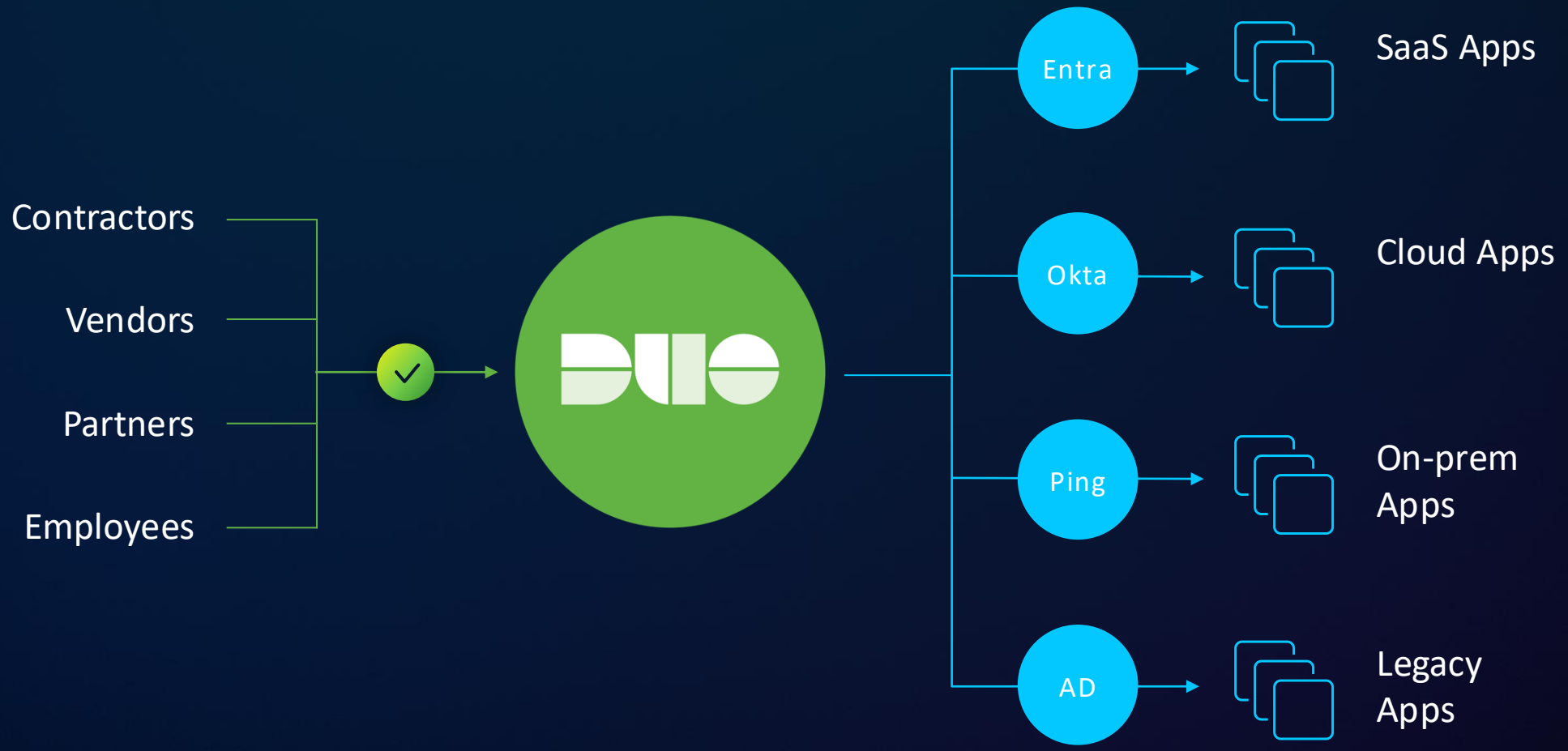


# Duo Identity & Access Management (IAM)

Standalone IAM when required

Identity broker for existing IAM

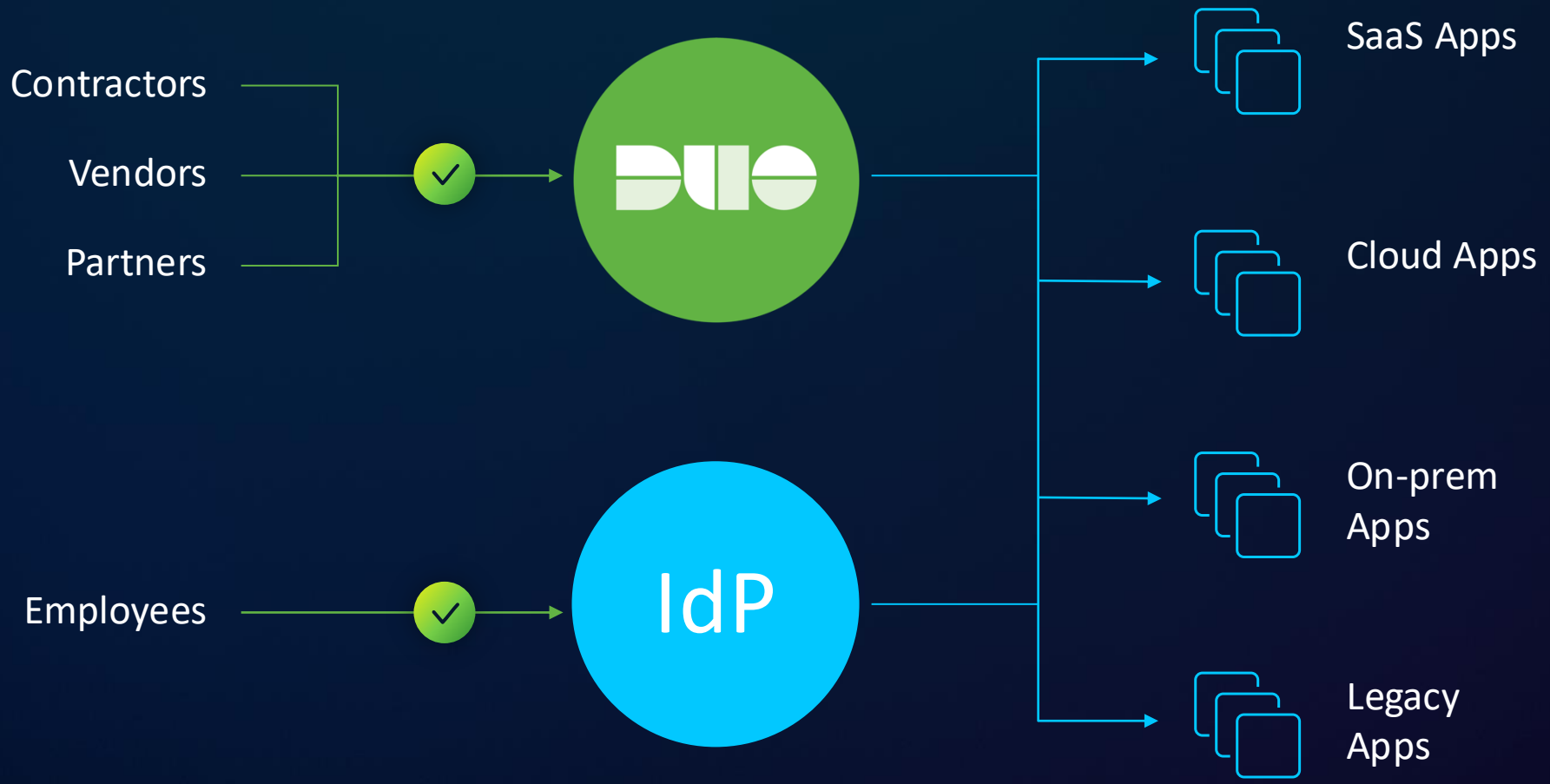
Alternate directory for third-party users



Standalone IAM when required

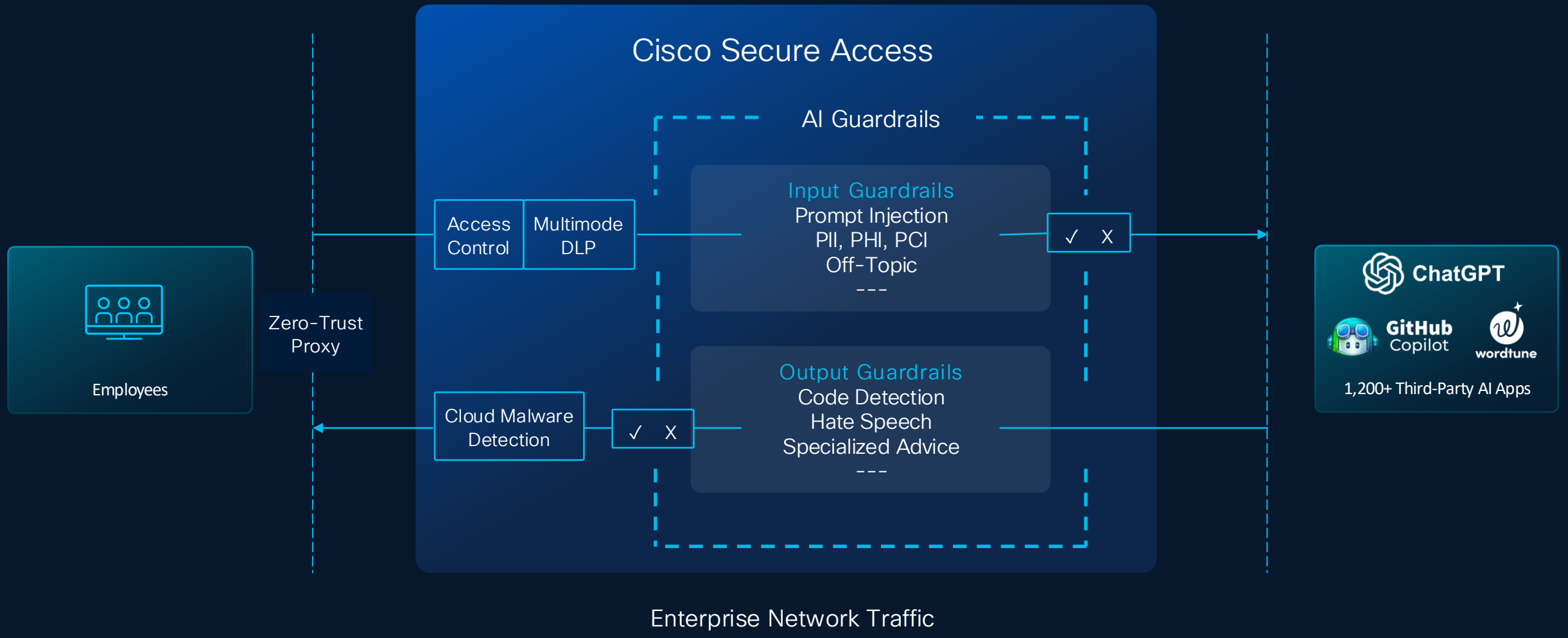
Identity broker for existing IAM

Alternate directory for third-party users



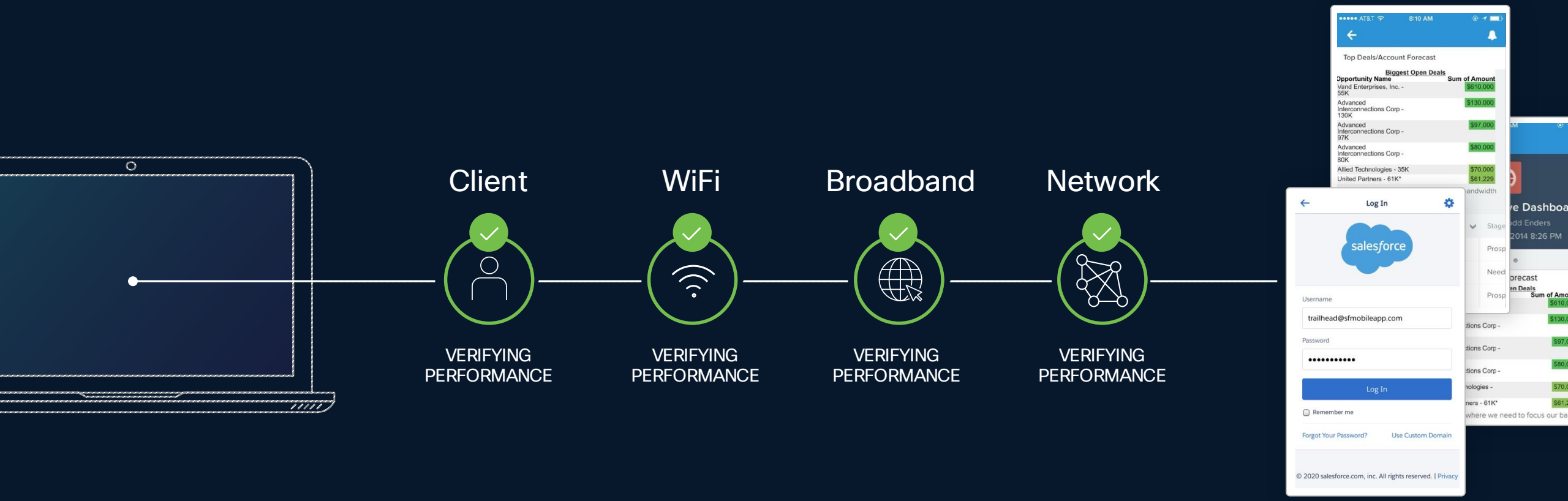
# AI Access

# Protecting usage of third-party AI apps



# Shadow AI Security with Cisco Secure Access Demo

# Fix issues fast with Digital Experience Monitoring




## Historical performance and recommendations

# Flexible Management

# Security Cloud Control

## Define policy once and enforce anywhere

Secure Firewall
(FTD, ASA)

Hypershield

Multicloud
Defense

Secure
Workload

Secure Access

AI Defense

NEW

Secure Router

NEW

3rd party
firewalls



cisco

# Security Cloud Control

Define policy once and enforce anywhere

Cisco Firewalling | AI Defense | 3rd Party Firewalls

Secure Firewall | Secure Workload | Hypershield

Secure Access (FW as a service) | Secure Router NGFW

Unified AI Assistant:
Simplify policy administration **by up to 70%**



cisco

NEW

# Security Cloud Control

## Industry's first multi-vendor intent-based policy


Absorb and optimize existing rules

Change enforcement points, not policy

No rip and replace

# Cisco clears the path to zero trust

**Control access** across all users and things for tighter security

Protect identities with identity intelligence

**Build resilience** with optimized infrastructure and simplified IT

# Thank you