Universal ZTNA from Cisco, powered by single vendor SASE

Ensures zero trust for all users, apps, and locations

Andreas Häggander, Solutions Engineer

Dec 2025

How do the industry define Universal ZTNA

"Universal Zero Trust Network Access applies zero-trust principles uniformly to all users, devices, and things for consistent, risk based least-privilege access everywhere."

Zero Trust principles

1. Never assume trust
2. Always verify
3. Enforce least privilege

Zero Trust success factors

1. Respect user privacy and user experience
2. Adjust policy to risk
3. Consistent experience across environments

Zero Trust must be defined holistically

Principles

Strategy

Architecture

Capabilities

Technologies

Features

Key focus areas

Principles

Single vendor SASE

Strategy

Secure Access Service Edge (SASE)

Architecture

Segmentation

ZTNA

Phishing-resistant MFA

Capabilities

SD-WAN

SWG, CASB, FWaaS, DLP, DEM

Security Service Edge (SSE)

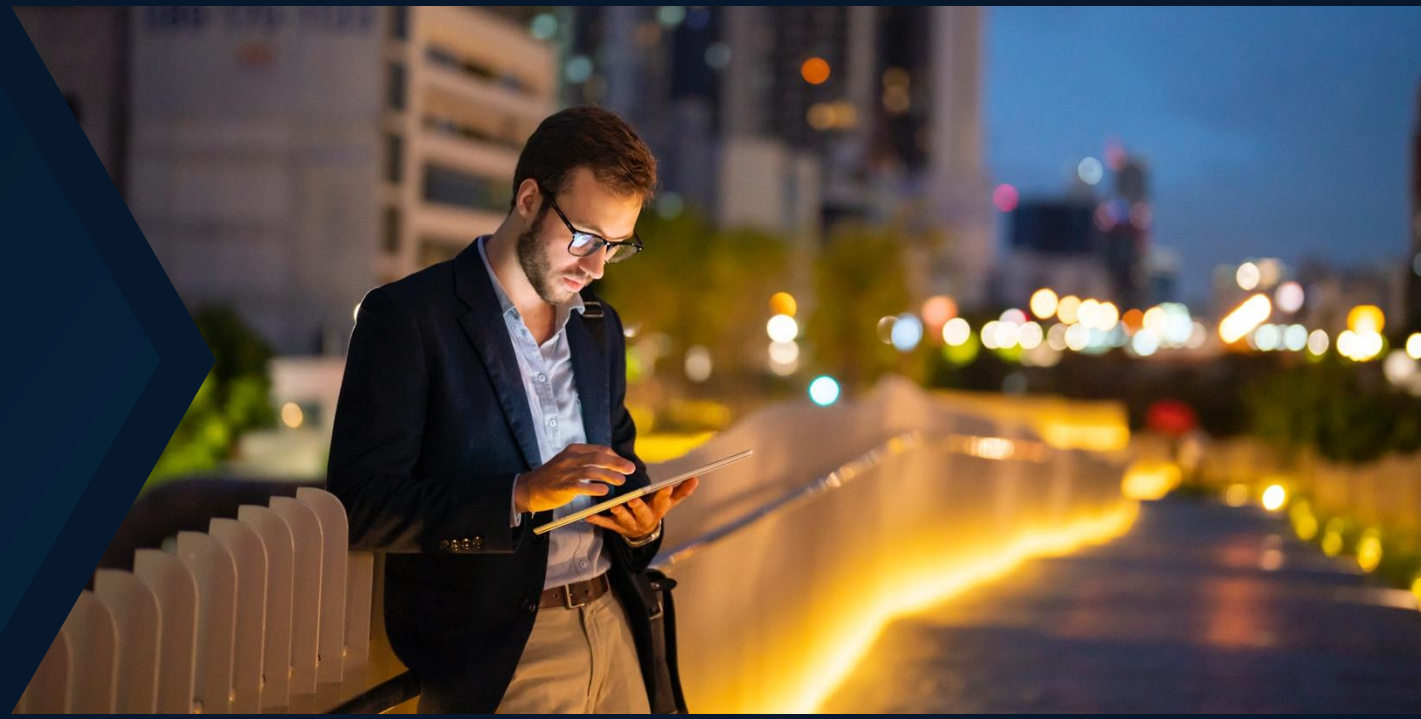
Technologies

Single client, single management (SCC)

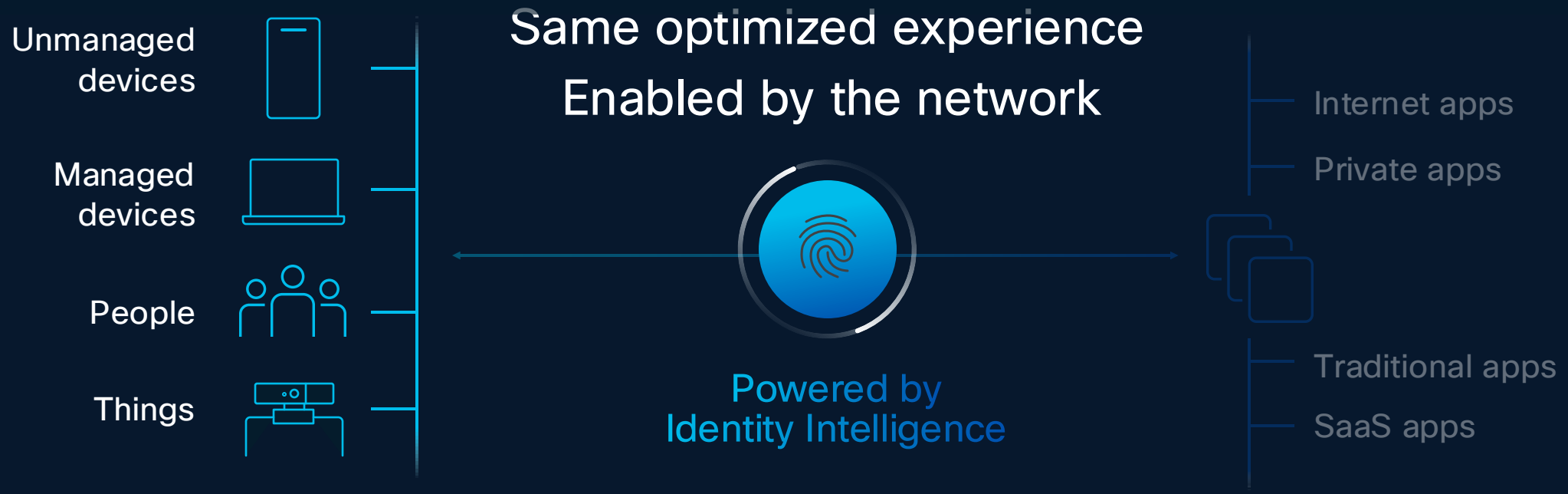
Identity Intelligence

Features

Traditional ZTNA was designed for a different time and different needs



Universal ZTNA from Cisco



Remote | Campus | Branch | Airplane | Remote | Oil rig | Stadium | Field | ...

Cisco’s Universal ZTNA

Secure SD-WAN + Security Service Edge + Trusted Identity Edge

SINGLE VENDOR SASE

End-to-end Assurance with ThousandEyes

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

+

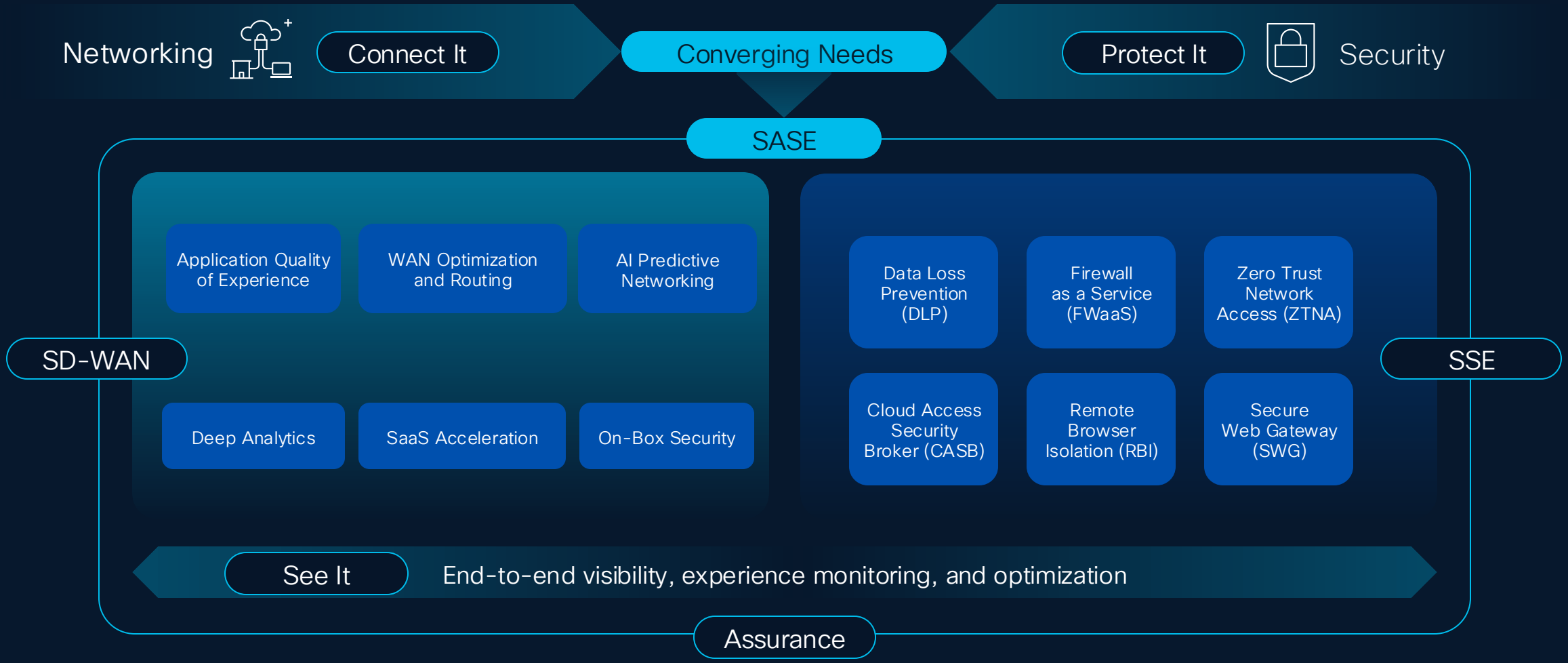
Security
Service Edge

Converged set of cloud security

End-to-end Assurance with ThousandEyes

Secure Access Service Edge (SASE)

Single vendor SASE from Cisco helps you see it all, protect it all, and perform everywhere.

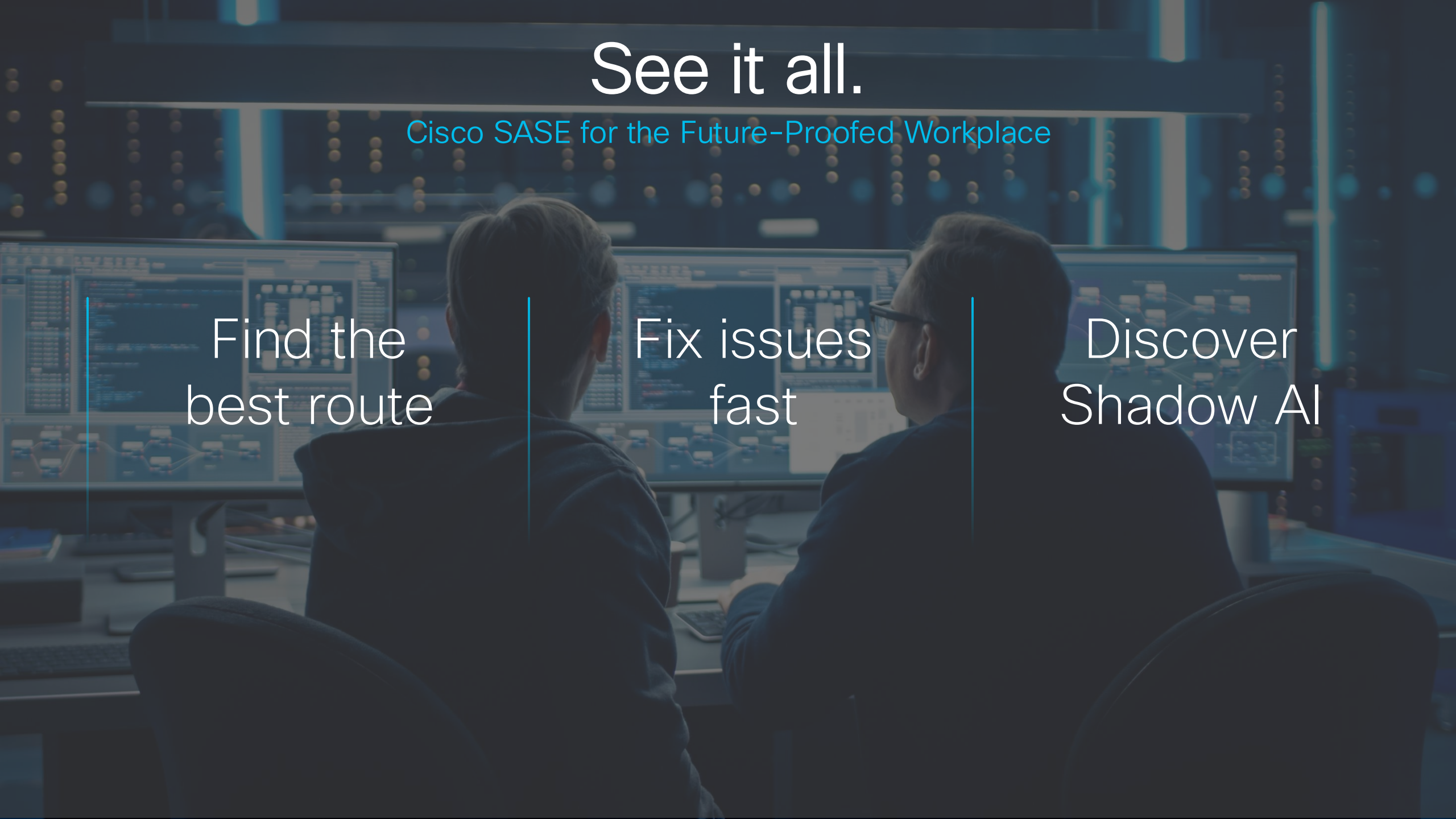


See it all

Protect it all

Perform everywhere

Simplified management and connectivity across everything in one platform



See it all.

Cisco SASE for the Future-Proofed Workplace

Find the best route

Fix issues fast

Discover Shadow AI

See it all.

Find the best route

End-to-end visibility for optimal network performance and security

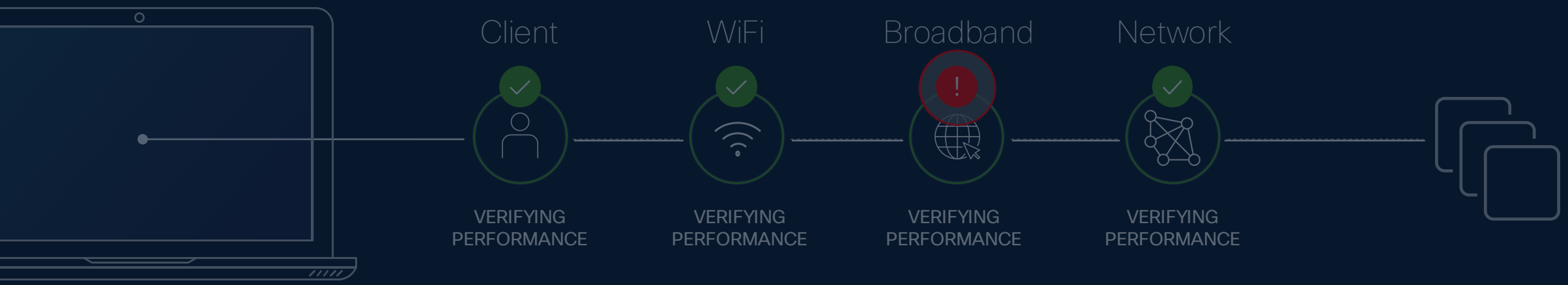
*Some PoPs are available on demand or by request.

See it all.

Fix issues fast with Experience Insights

Node: 01.ca.comcast.net

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



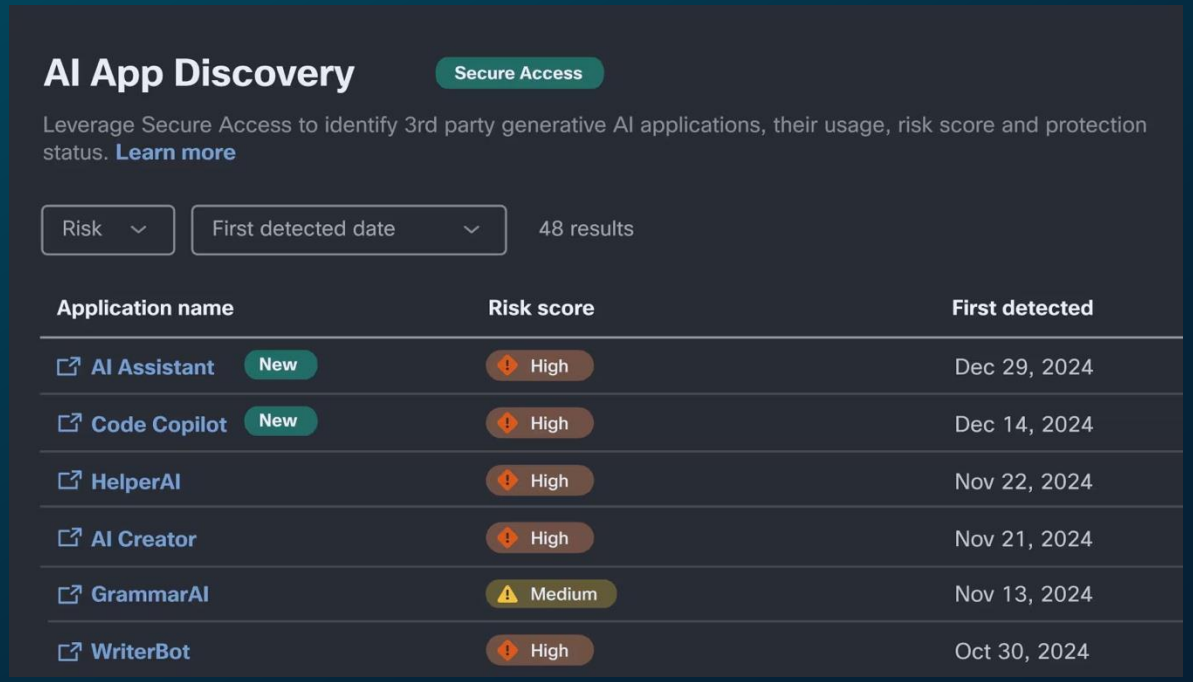
Depictions are examples only.

See it all.

Discover GenAI app usage with AI Access

Superior visibility & control

- Discover Shadow AI
- Define acceptable use
- Machine learning finds unstructured data
  - Patent applications
  - M&A
  - Financial statements and more



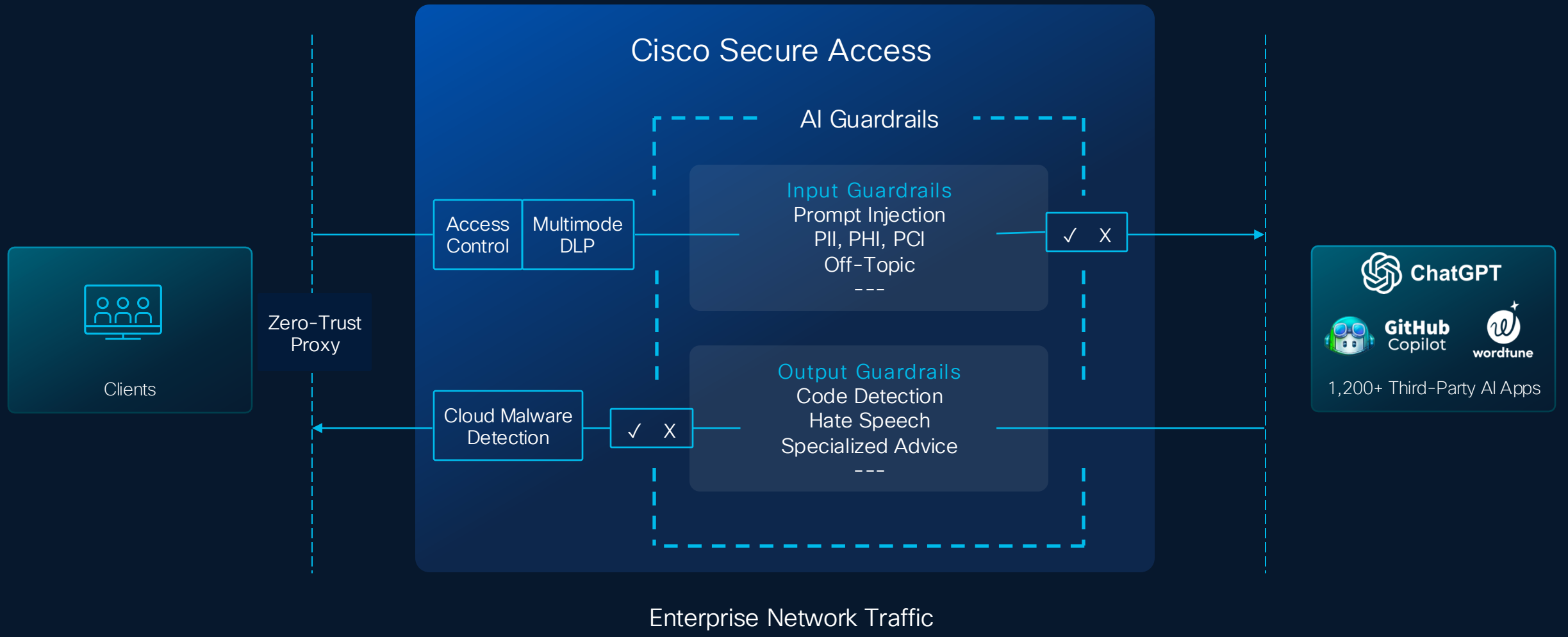
1200+
AI Apps Protected

100%
Guardrails for top AI Apps

1
Unified Security Framework

See it all.

Protecting usage of third-party AI apps



Protect it all.

Networking designed for security everywhere.

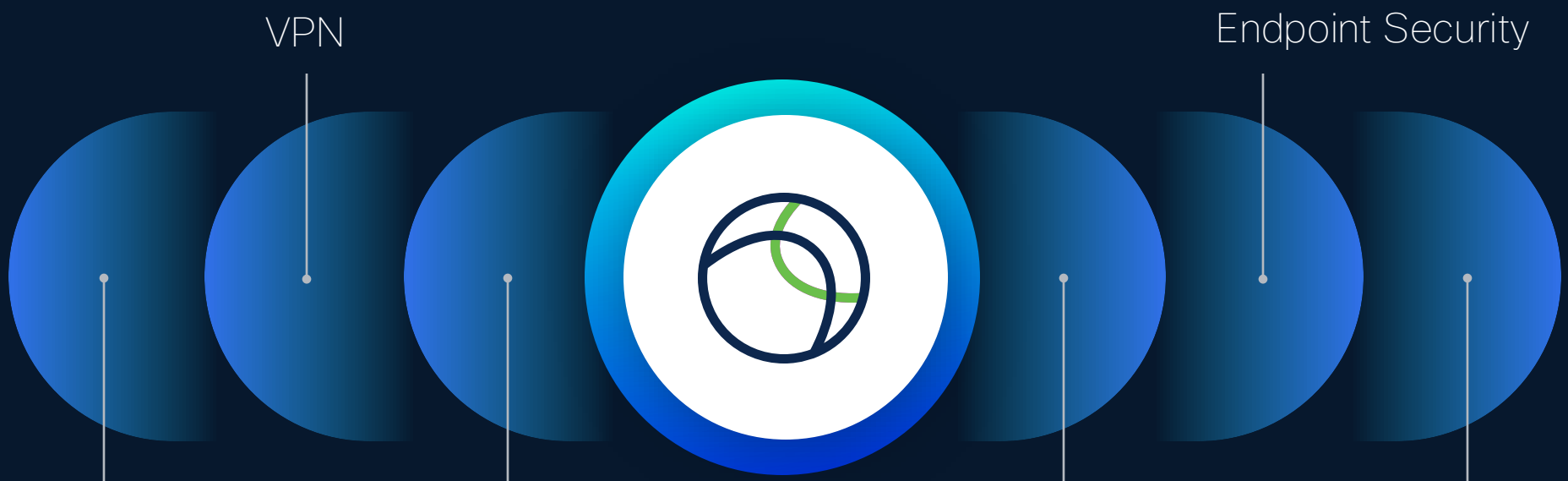
Single client, single policy

Seamless transition to ZTNA

Secure access for all users, and things*

*Including protecting GenAI app usage

One client, **multiple functions**



Protect it all.

Seamless Access

The evolution of our AnyConnect client makes access easy.

We handle the plumbing

Go to work

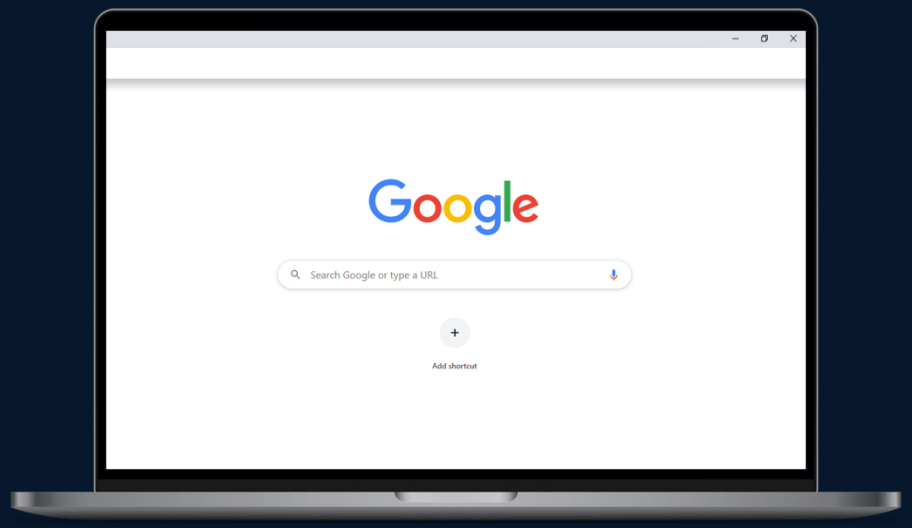
- Modern Private Apps
- Legacy Private Apps
- SaaS Apps
- Internet

Protect it all.

Mobile OS and Browser Integration

Secure access for contractors using unmanaged devices

BYOD via enterprise managed Google Chrome
Advanced protocol support for Apple, Samsung



Chrome Enterprise Browser

Native OS Integration

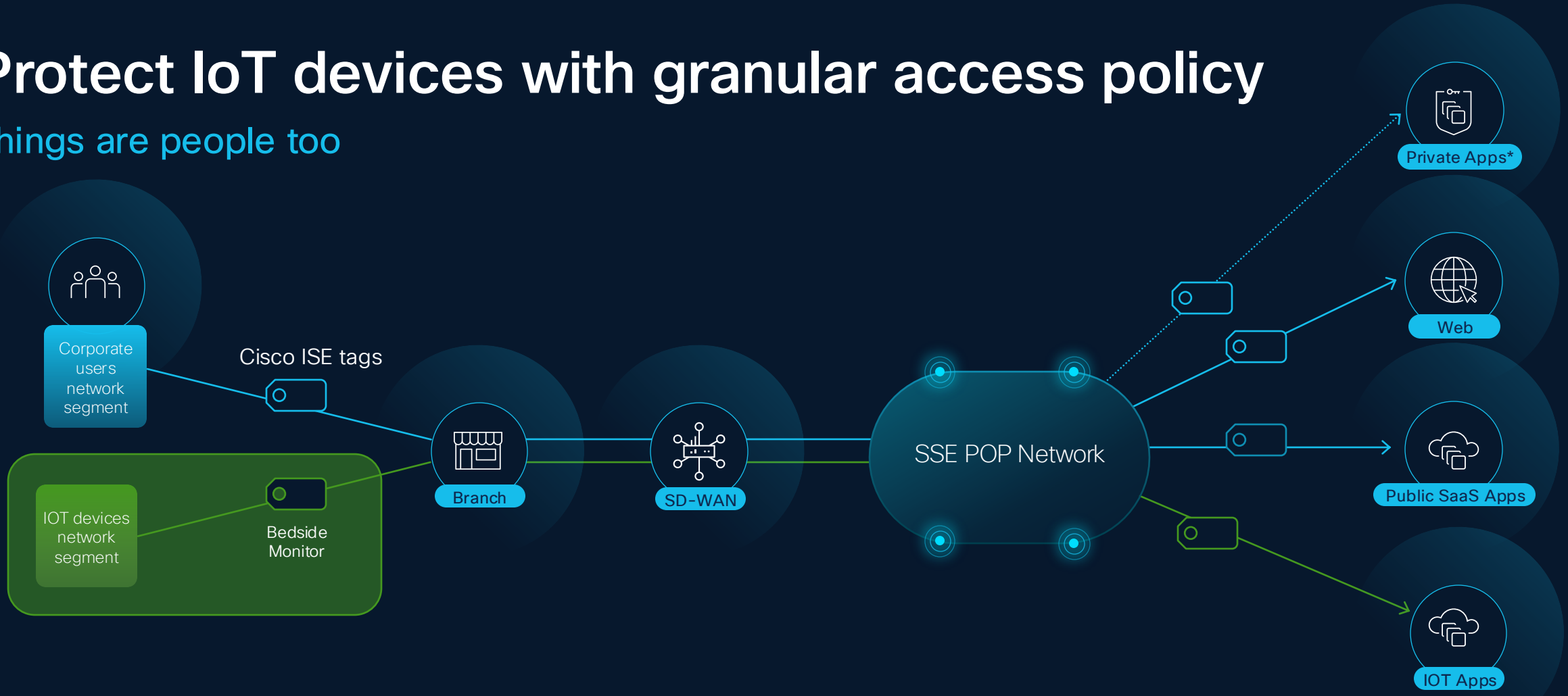
Extend consistent identity context across SD-WAN and cloud security enforcement

ISE security group tags (SGTs) for granular access policy

* Capabilities are planned but not yet available or guaranteed.

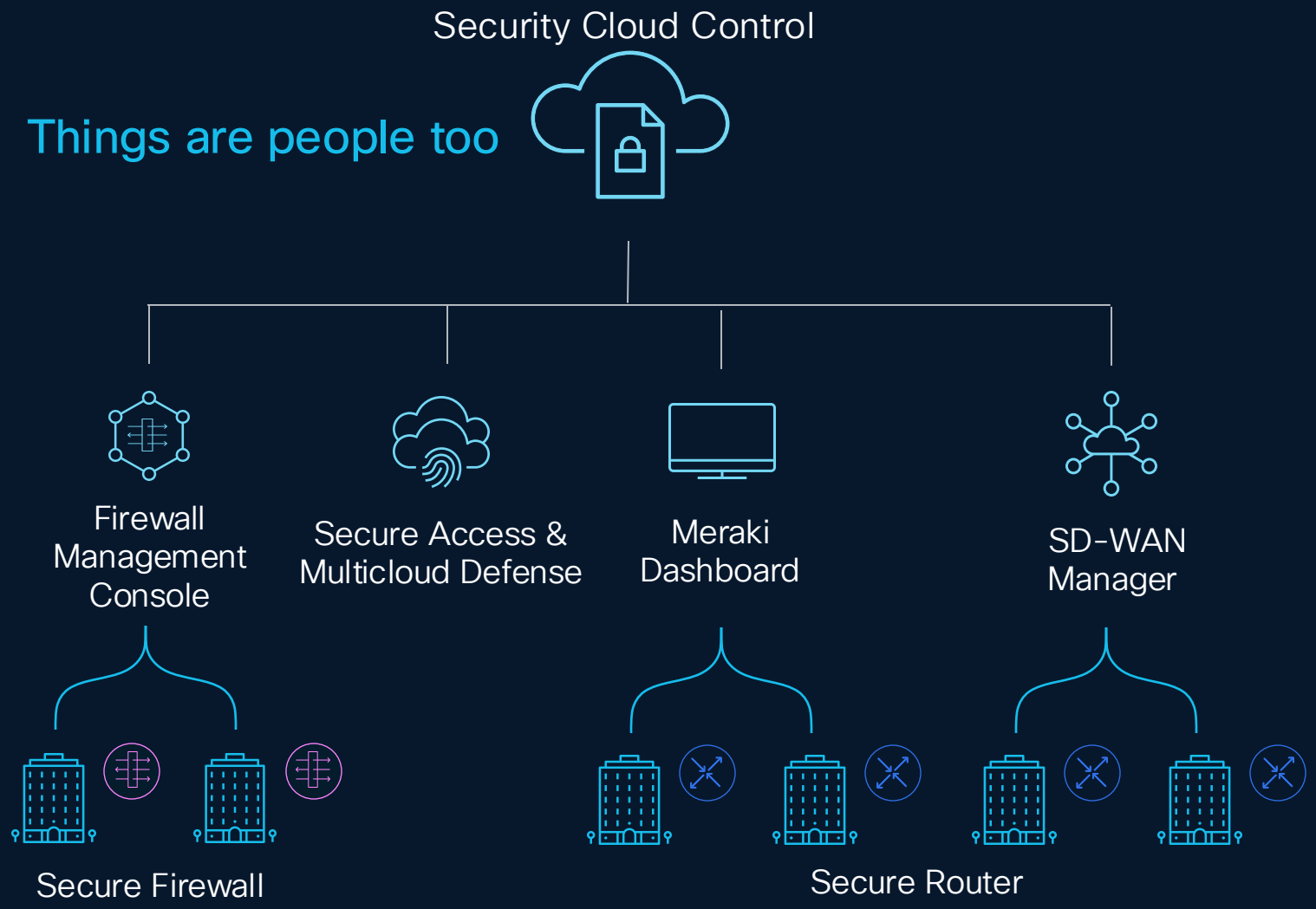
Protect IoT devices with granular access policy

Things are people too



* Capabilities are planned but not yet available or guaranteed.

Cisco Security Cloud Control – One place for Policies



Security Object/Policy Configuration

- Push security policies to different security solutions using single orchestrator

Monitoring

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

Troubleshooting (Future)

- Leverage SCC tools for security troubleshooting

Perform everywhere.

Simplified networking for zero downtime, always-on resilience.

Cloud-agnostic, high-performance connectivity

Consistent user experience - everywhere

Integrated policy and traffic management

Predictive path recommendations for zero downtime

AI-powered insights for smarter and faster networking

AI-Powered Insights

Predicts network issues before they happen

Proactive Optimization

Dynamically selects the best path for each application

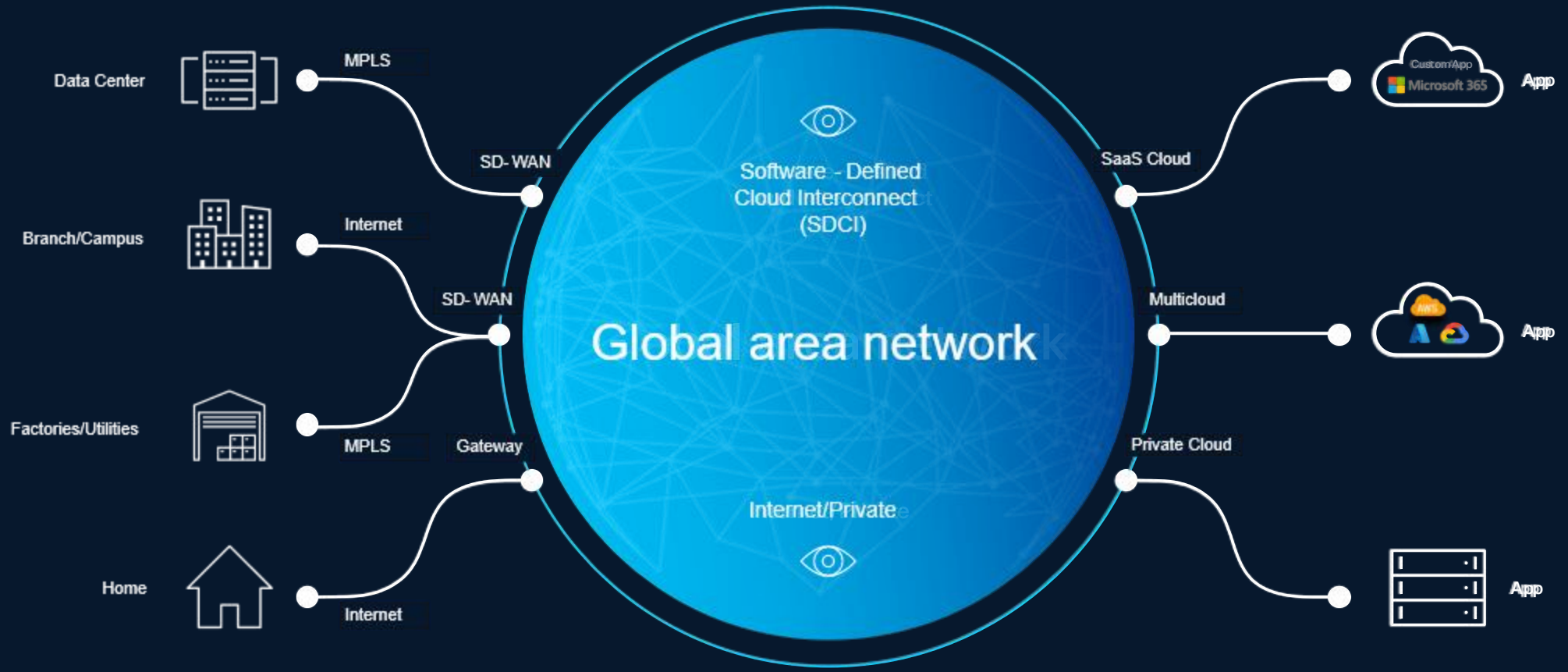
Reduced Disruptions

Minimizes downtime and improves efficiency

Seamless Performance

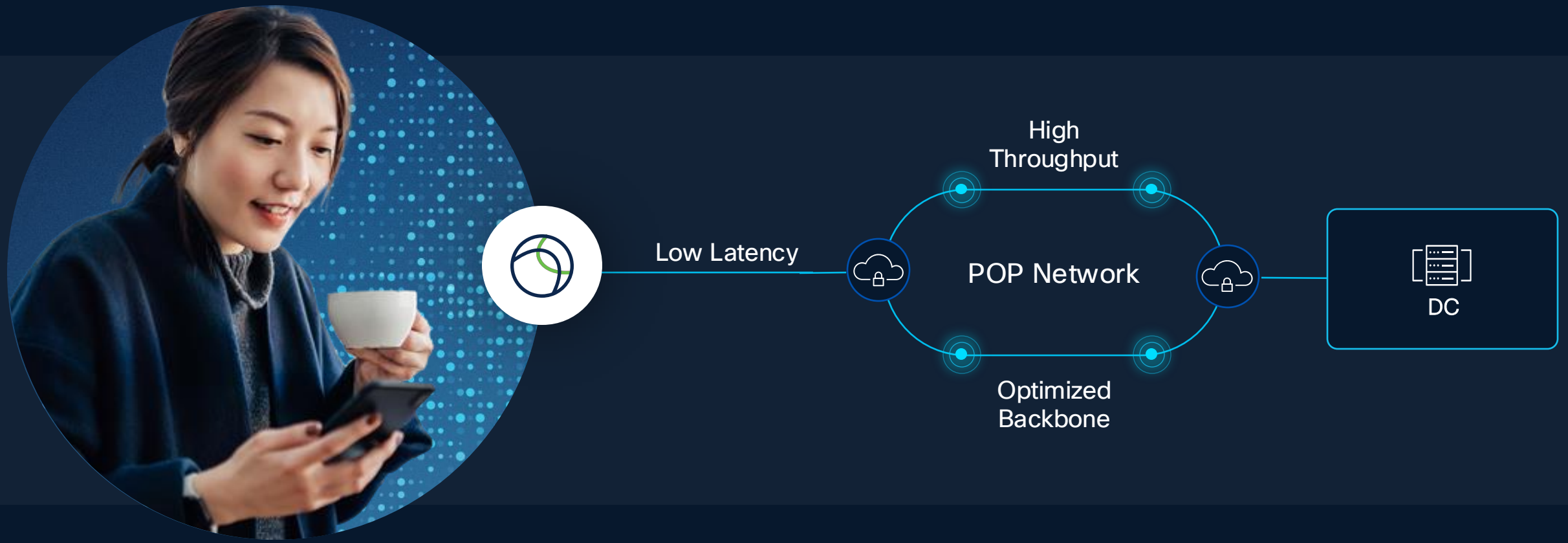
Ensures consistent and reliable user experience

Cloud OnRamp: Making cloud easy for the hybrid world



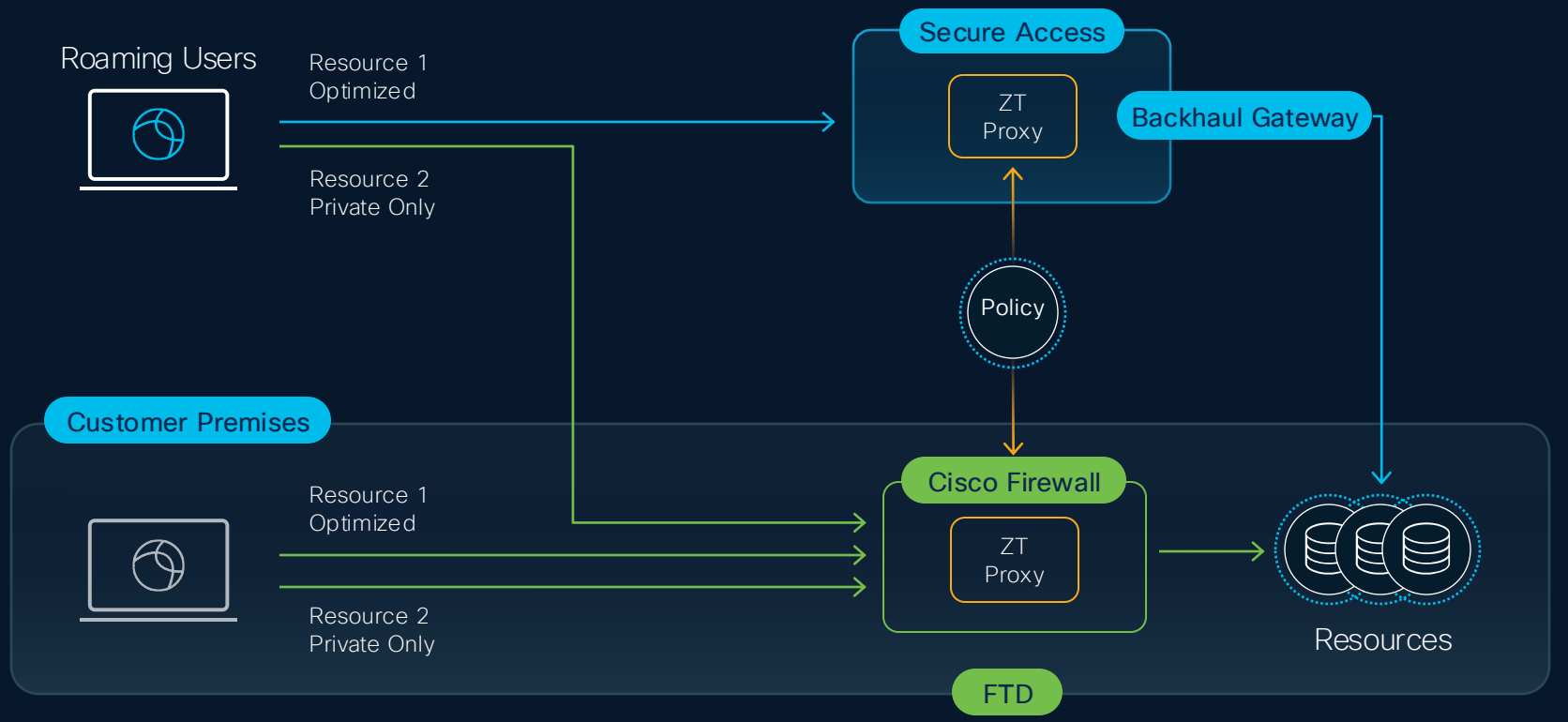
Cisco’s modern PoP architecture optimizes user experience

Leverages MASQUE/QUIC, Vector Packet Processing (VPP), and a global peering



Hybrid Private Access for flexible enforcement

Single set of ZTNA policies used in cloud and on-premise



Cisco’s Universal ZTNA

Secure SD-WAN + Security Service Edge + Trusted Identity Edge

SINGLE VENDOR SASE

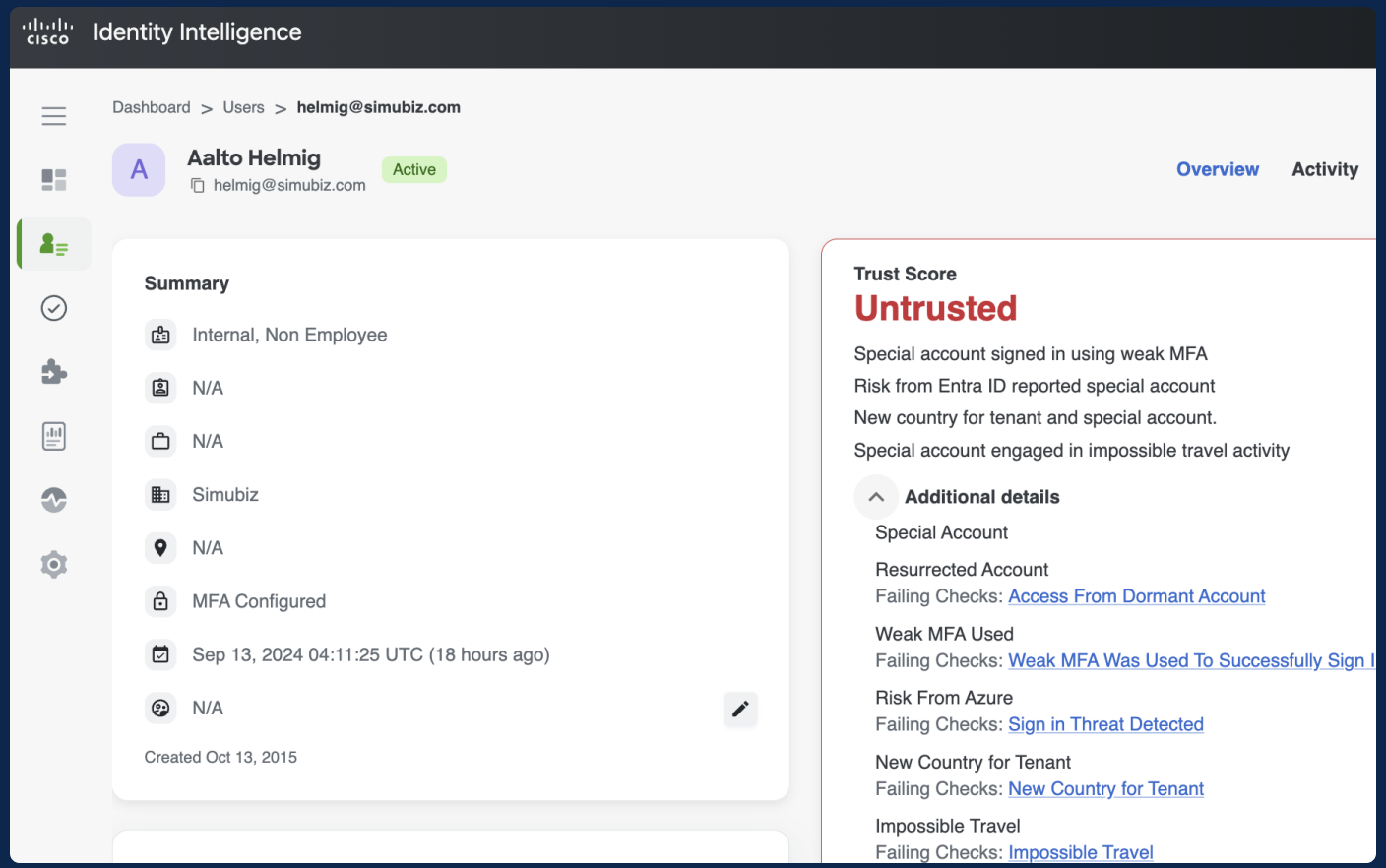
End-to-end Assurance with ThousandEyes

Cisco Identity Intelligence

SailPoint
Dragos
Crowdstrike
Salesforce
Cisco ISE
Okta
PingIdentity
Auth0
Microsoft
Google
Cyberark
Amazon


Cisco Identity Intelligence
USERS
MACHINES
SERVICES
HRIS
DATA
APPS
PLATFORMS
RELATIONSHIPS
LOGS
SESSIONS
LOCATION
FACTORS
EMAILS
UID
ROLE
CONNECTED
IDENTITIES
IOT
UNMANAGED
USER DEVICES
MDM
INFRASTRUCTURE
PASSKEYS
BROWSERS
GROUPS
SUBSET
ACCESSED THROUGH
LOCATION
PERMISSIONS
workday
okta
ON PREM
SaaS
aws
WORKLOADS

Identity Intelligence continually assesses user trust



User Trust Score

Identity Intelligence provides a dynamic user trust score based on user behaviors, actions, and posture to Secure Access for continuous zero trust enforcement.

Easy Workflows

After assessment, take response action from the console.

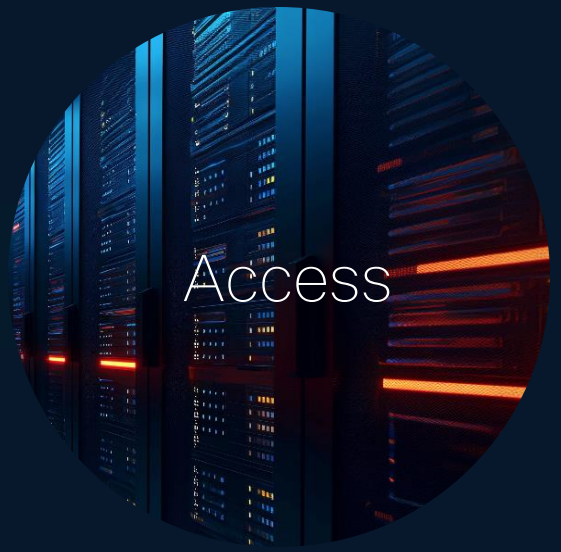
Key Scores

- Trusted
- Favorable
- Neutral
- Questionable
- Untrusted
- Unknown

Identity Intelligence

Continuously assess you are
who you say you are

BLINK RUST

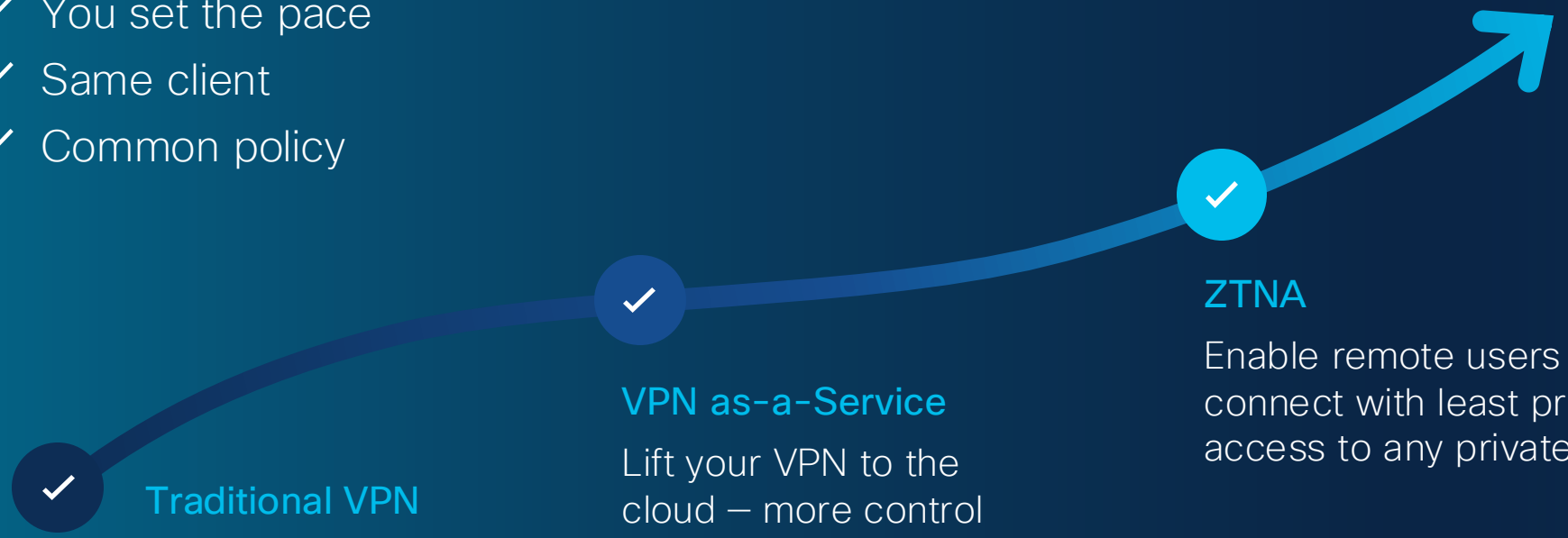


Works with existing IDPs

How do we start ?

Flexible journey to Universal ZTNA

- ✓ You set the pace
- ✓ Same client
- ✓ Common policy



Traditional VPN

Network level access – difficult to control at app level

VPN as-a-Service

Lift your VPN to the cloud – more control and easier to manage

ZTNA

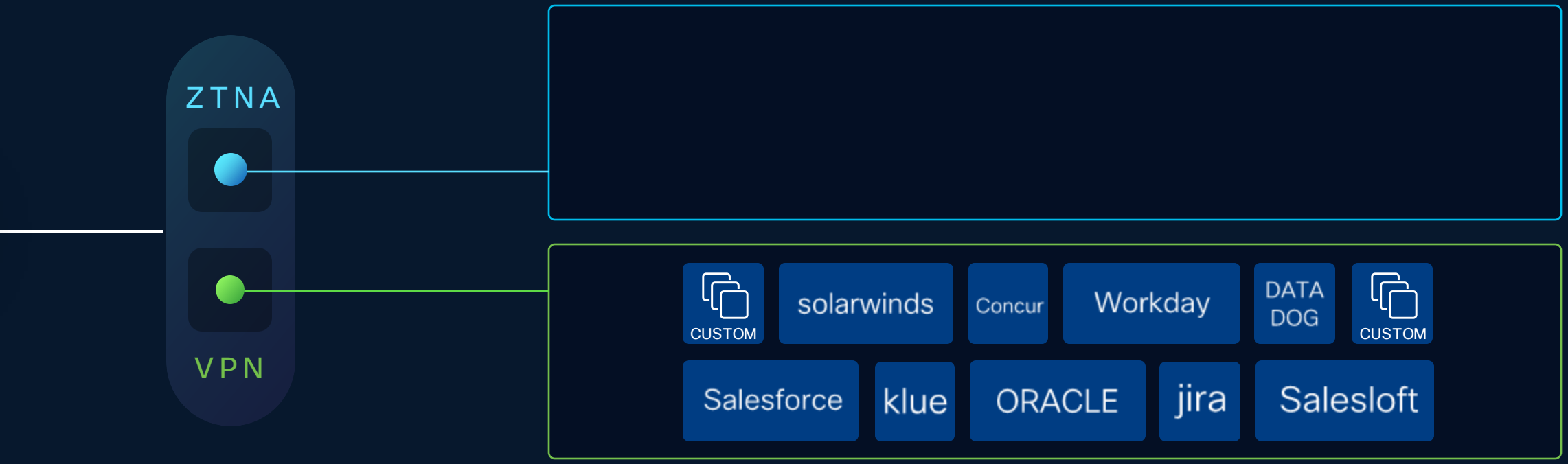
Enable remote users to securely connect with least privilege access to any private app.

Universal ZTNA

Any user/device/thing securely connect with least privilege access to any app – anywhere.

Seamless Experience

One client simplifies ZTNA roll-out



Summary

Cisco SASE for the Future-Proofed Workplace

See it all.

Find the best route, fix issues fast, and discover Shadow AI

Protect it all.

Secure access to all apps for all kinds of users and things

Perform Everywhere.

Zero trust with latency of ~40ms or less for 99% of business users

Simplified management and connectivity across everything in one platform

cisco

Thank You !