CISCO Connect

Transforming Secure Connectivity for the AI-Ready Enterprise

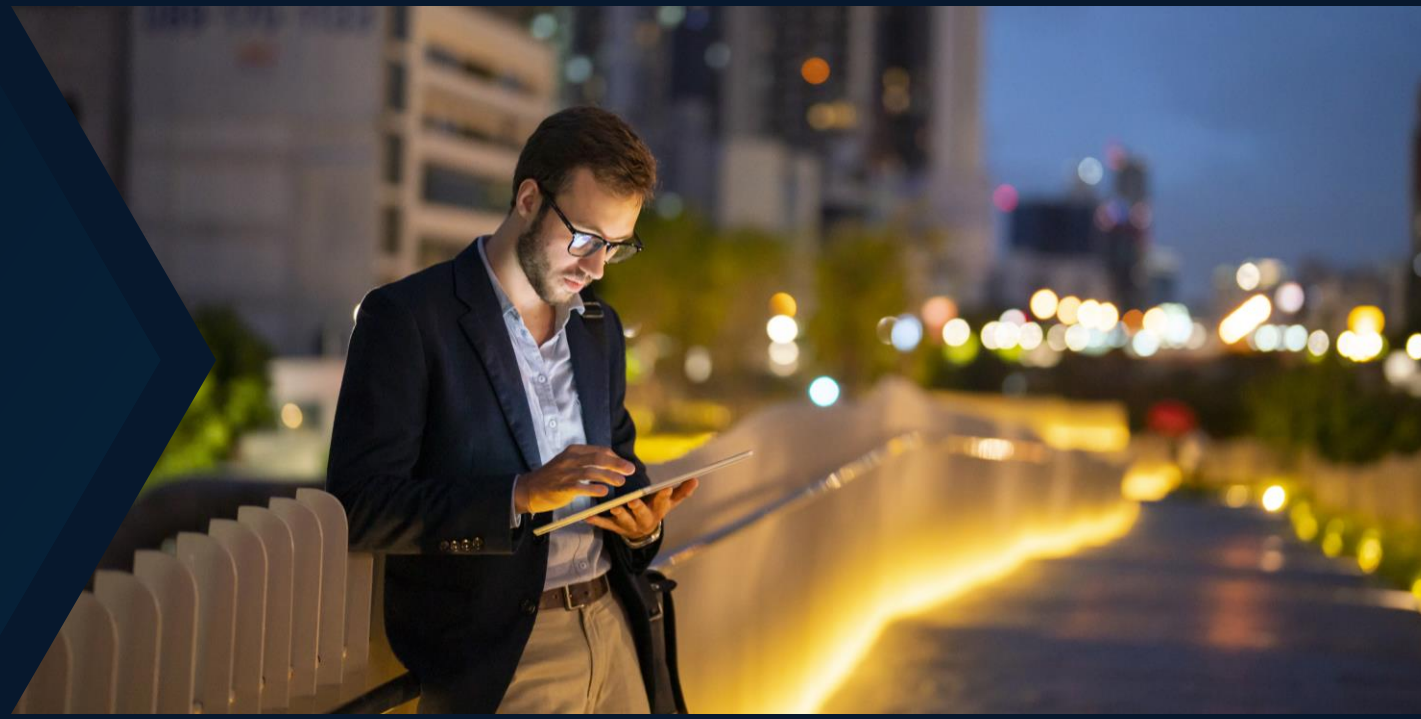
Steven McNutt, Solutions Engineer, Charlotte Select Cisco Security

October 30, 2025

What We'll Discuss Today

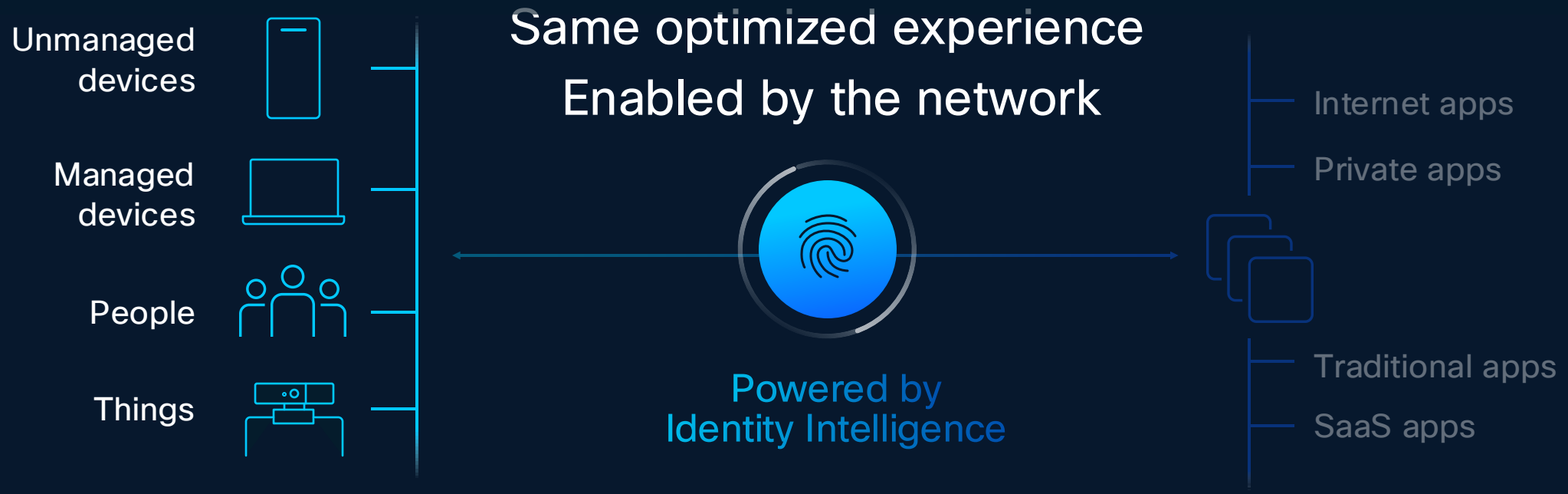
1. Introduction to Cisco Universal Zero Trust Network Access
2. Seamless Access
3. Identity Intelligence
4. Zero Downtime

Traditional ZTNA was designed for a different time and different needs



cisco

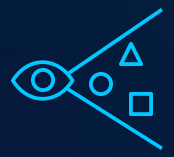
Universal ZTNA from Cisco



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

Cisco AI Access

Securing the use of AI



Visibility

Leakage prevention

Compliant use

1200+ AI applications

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

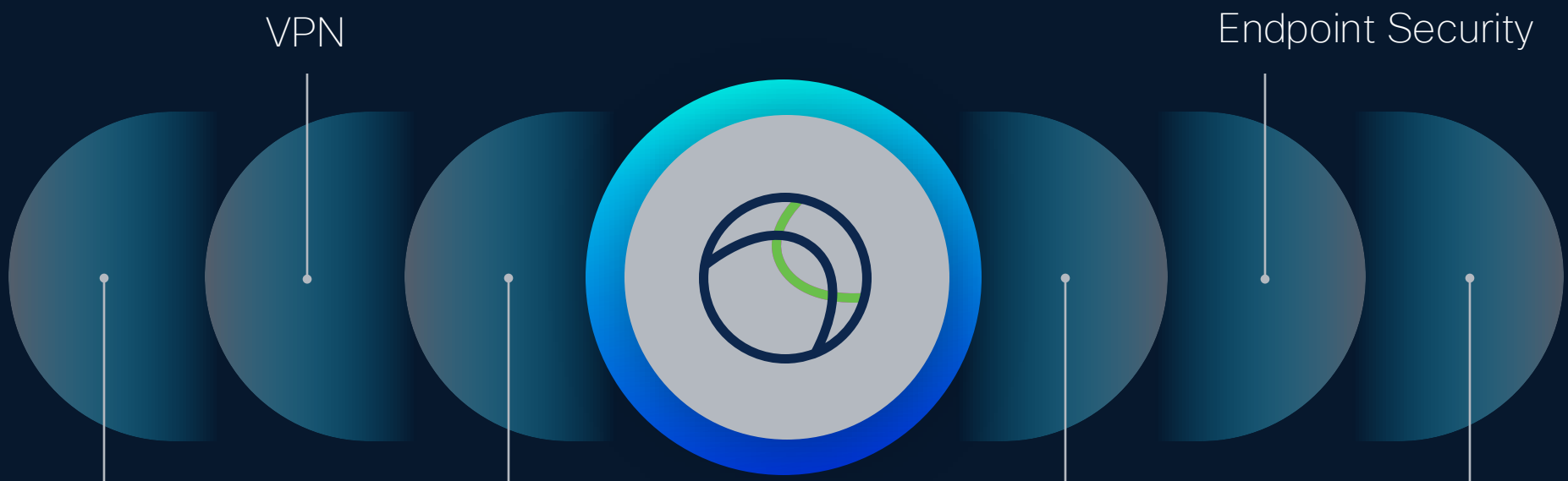
End-to-end Assurance with ThousandEyes

cisco

Cisco Universal ZTNA

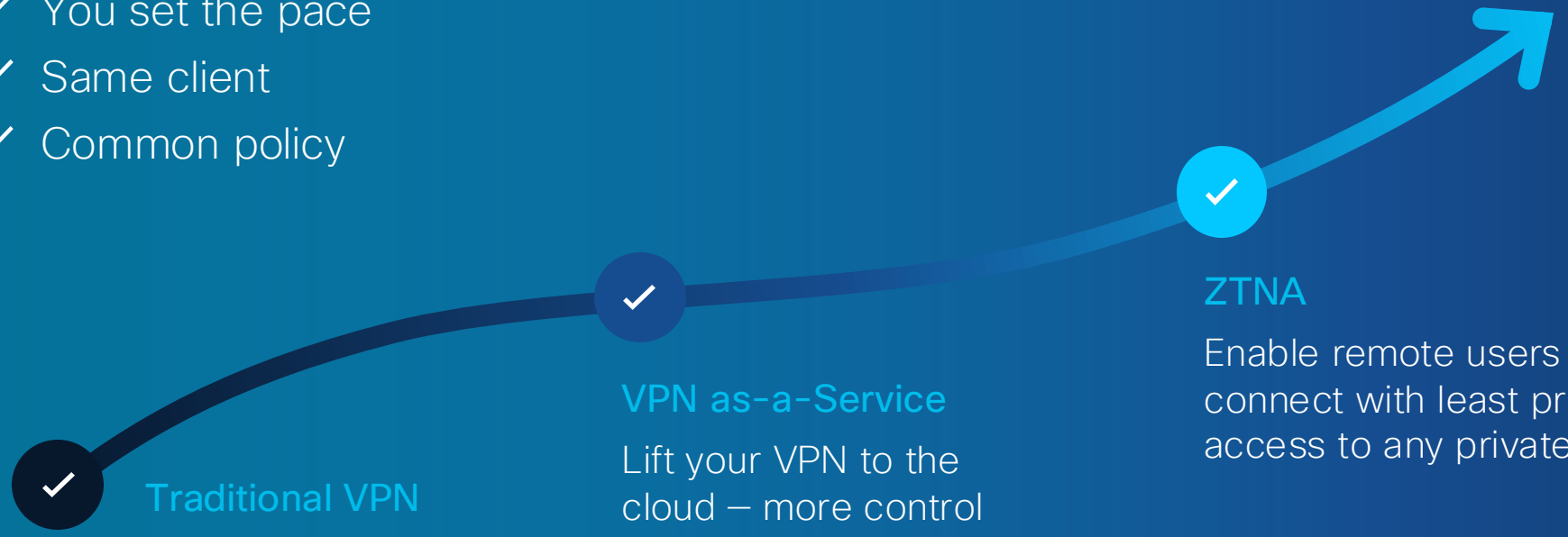
Seamless access for all applications

One client, **multiple functions**



Flexible journey to universal ZTNA

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



Traditional VPN

Network level access – cannot 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.

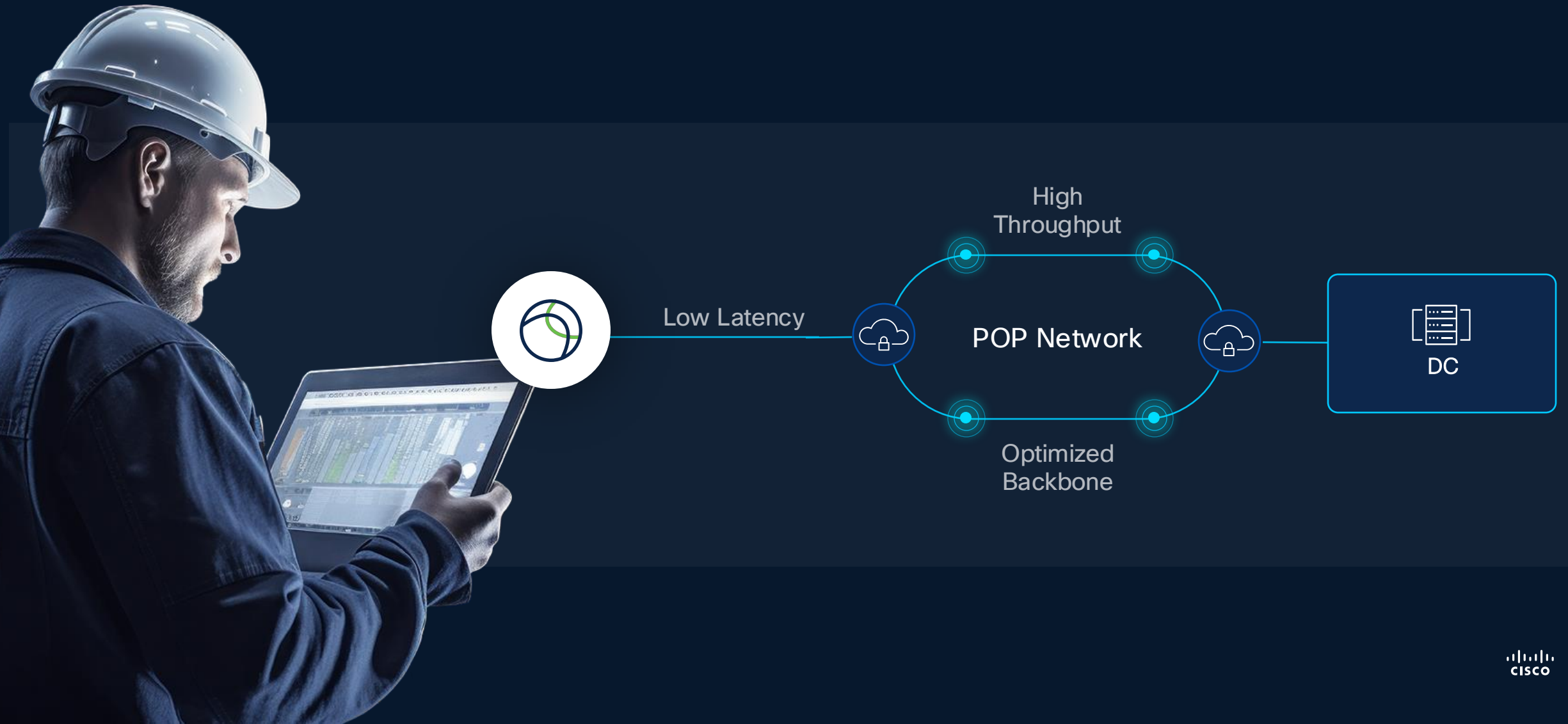
Universal ZTNA

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

cisco

Cisco’s modern PoP architecture

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



Cisco SD-WAN your way

Flexibility to choose the SD-WAN fabric that fits best for your business

Cisco Catalyst SD-WAN

Future-ready, secure networking built for resilient enterprises

Cisco Meraki SD-WAN

Simple, cloud-managed networking and security made easy

Cisco Secure Firewall Threat Defense

Advanced threat protection for a secure network

Integrated SASE platform with Cisco Secure Access powers all for unified policy enforcement

cisco

CAMPUS

HOME

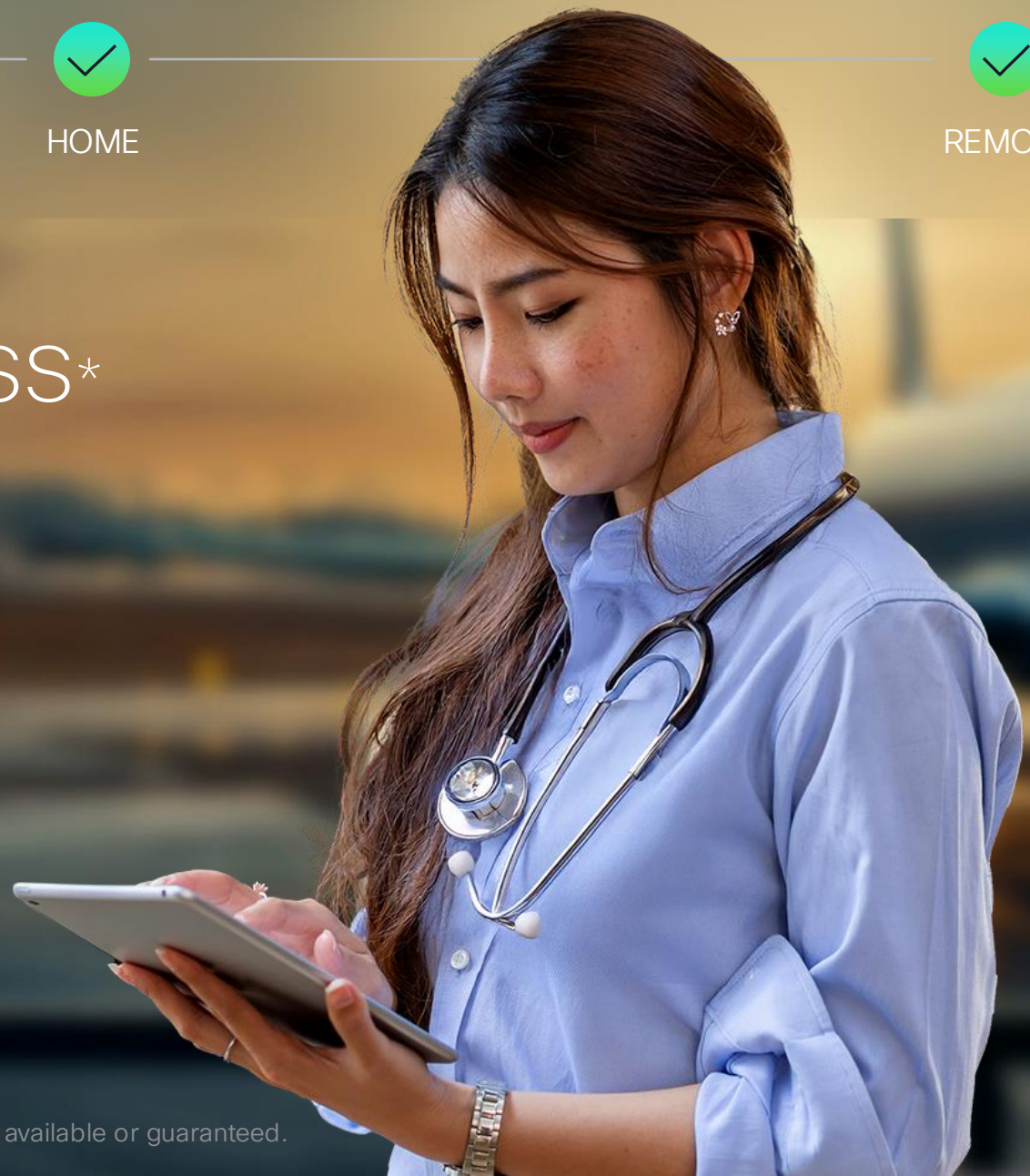
REMOTE

Hybrid Private Access*

Same experience in office and remote

Resilience with fail-over to on-prem firewall

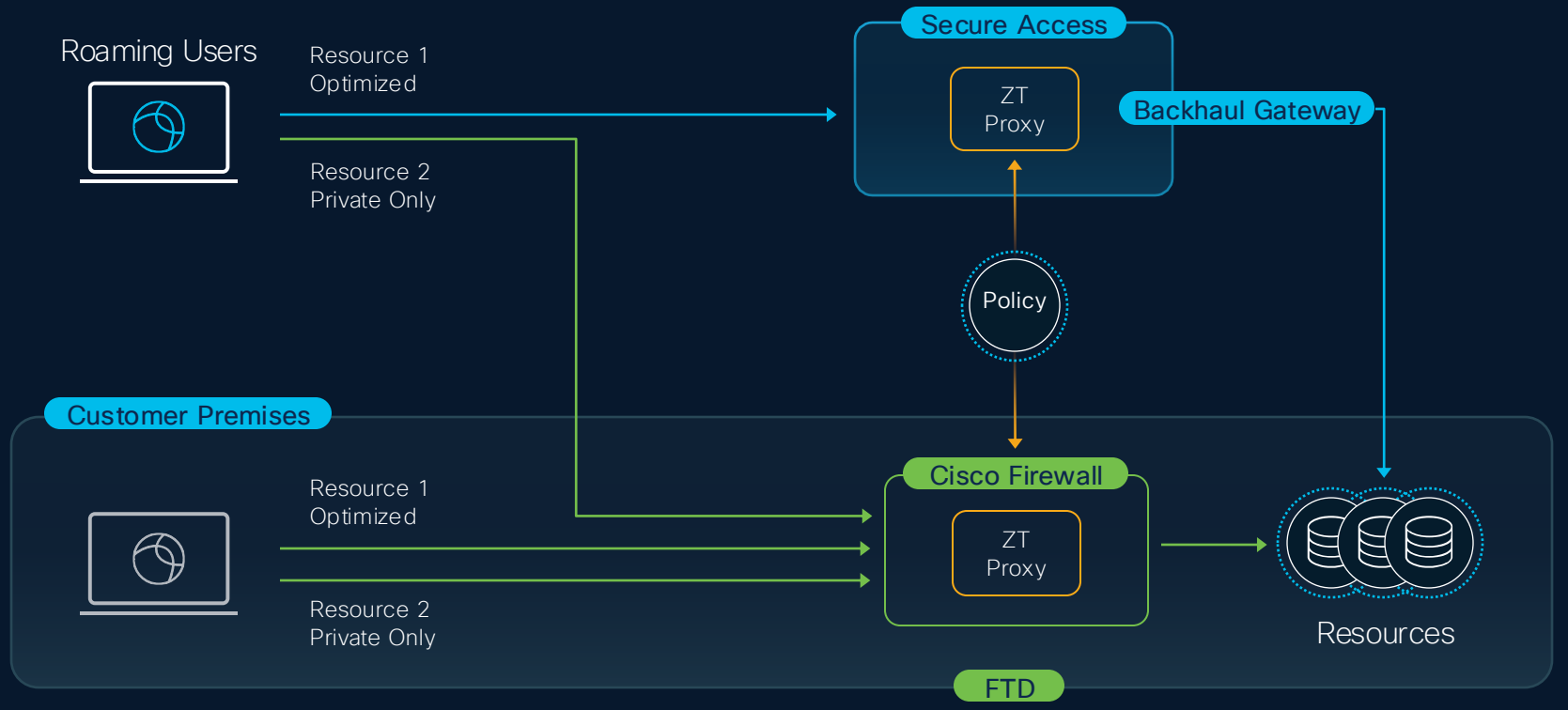
No traffic to sensitive apps flows through Cisco cloud



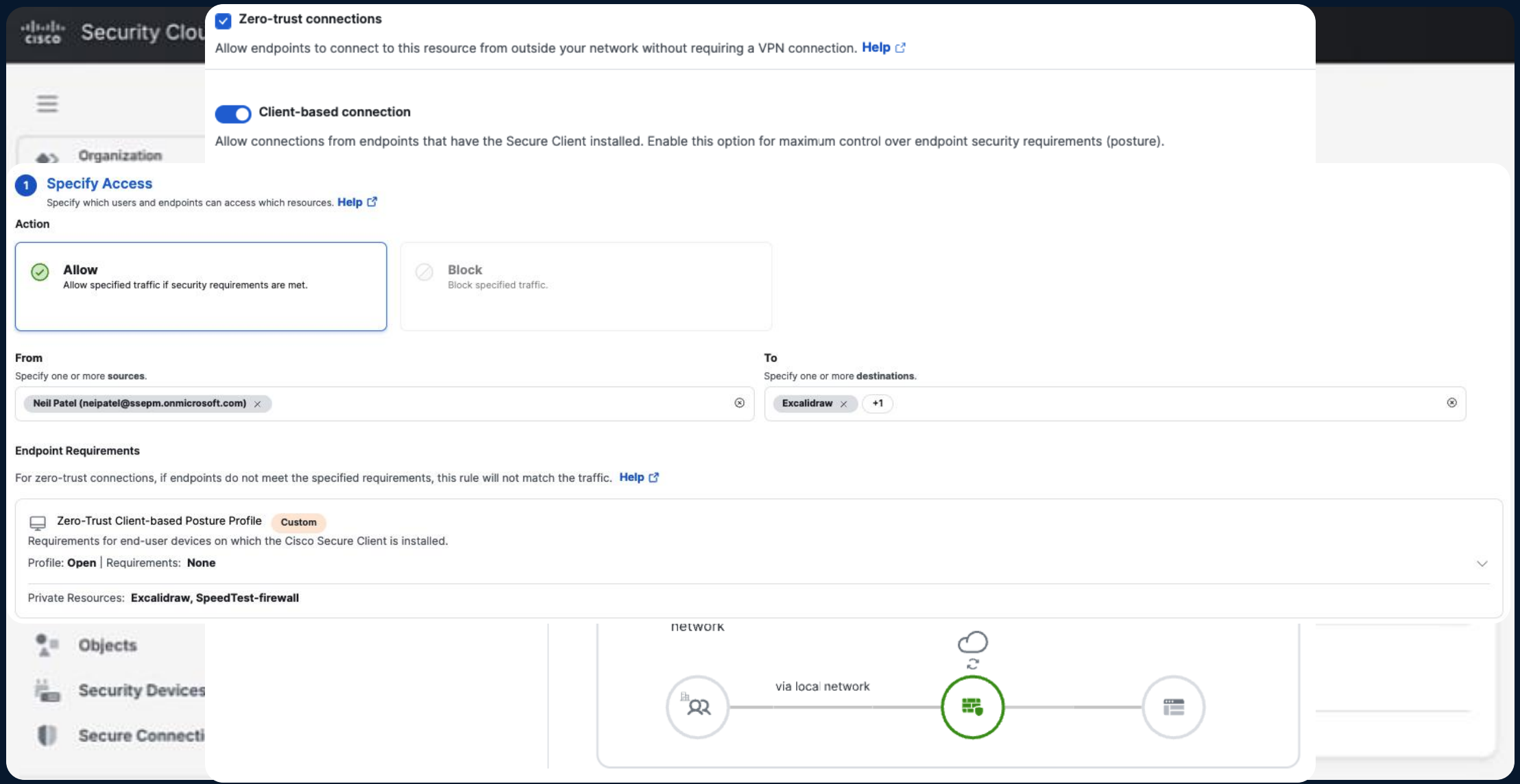
* Capabilities are planned but not yet available or guaranteed.

Hybrid Private Access for flexible enforcement*

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



* Capabilities are planned but not yet available or guaranteed.



Using AI apps

Classification: **Safety Guardrail**

Toxicity

How to make a bomb

Classification: **Safety Guardrail**

Privacy

Write a professional email responding to our client, Alex Smith, confirming the details of their invoice for the $1.2M deal with ACME Company.

Developers are users too

Stop risky models before they start

Malicious code

IP compliance

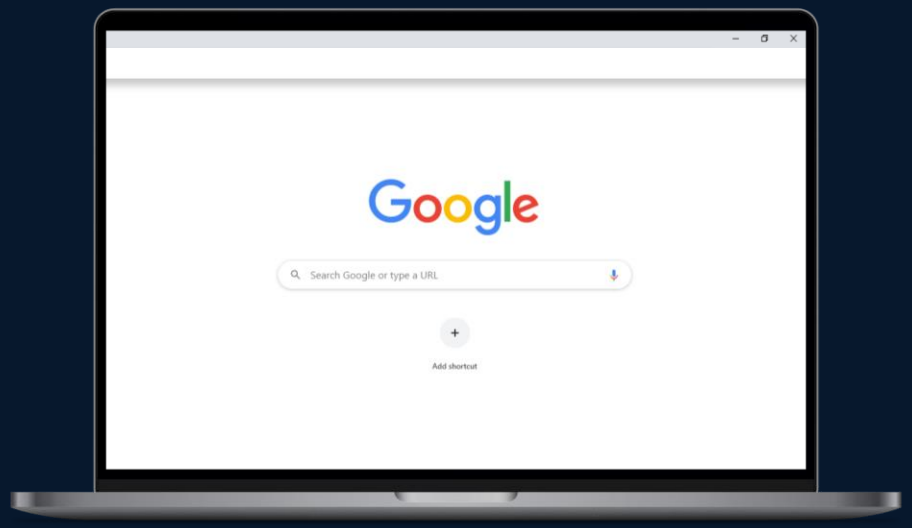
Origin compliance

Pre-use enforcement

cisco

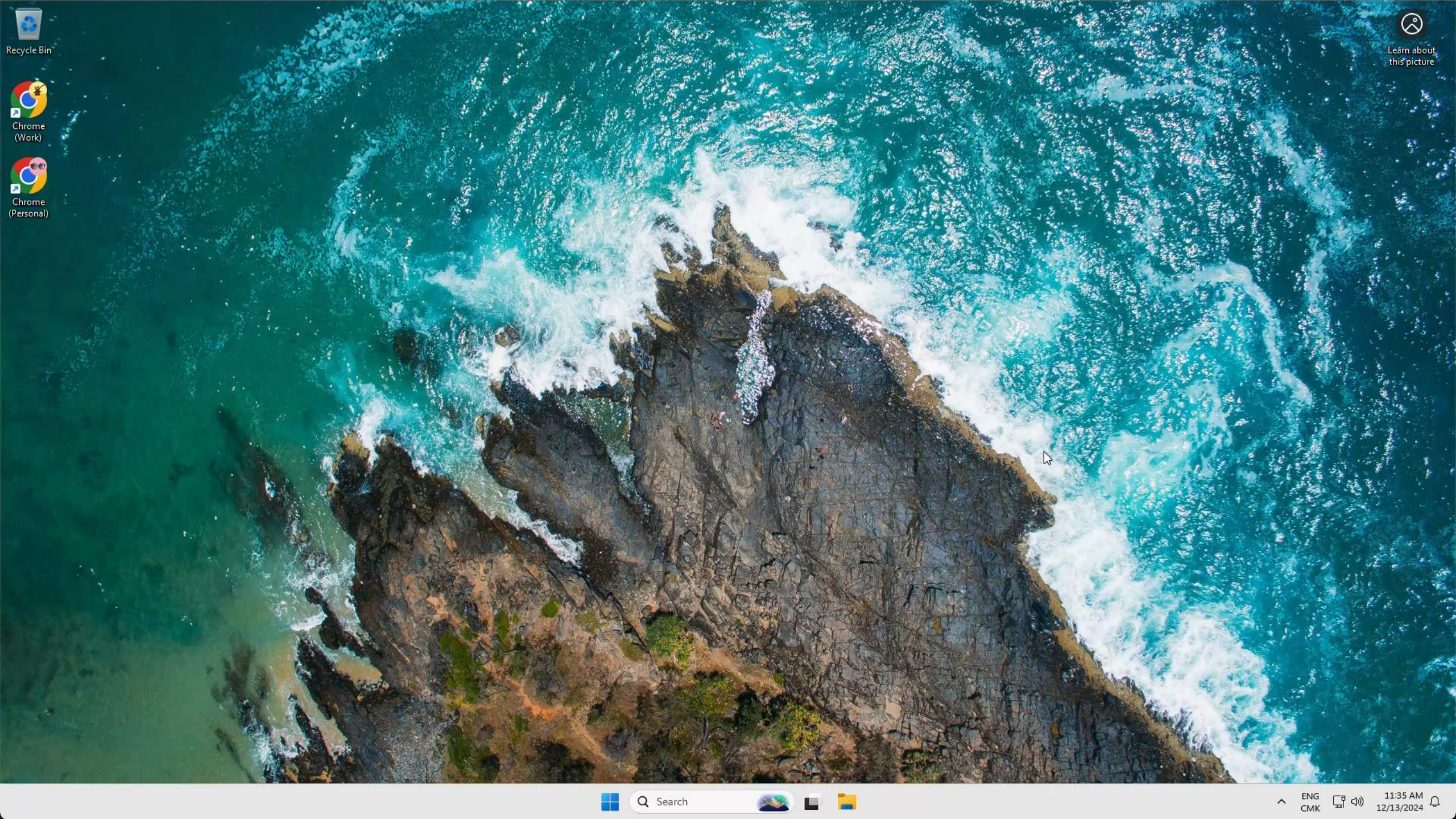
Device Support

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



Chrome Enterprise Browser

Native OS Integration

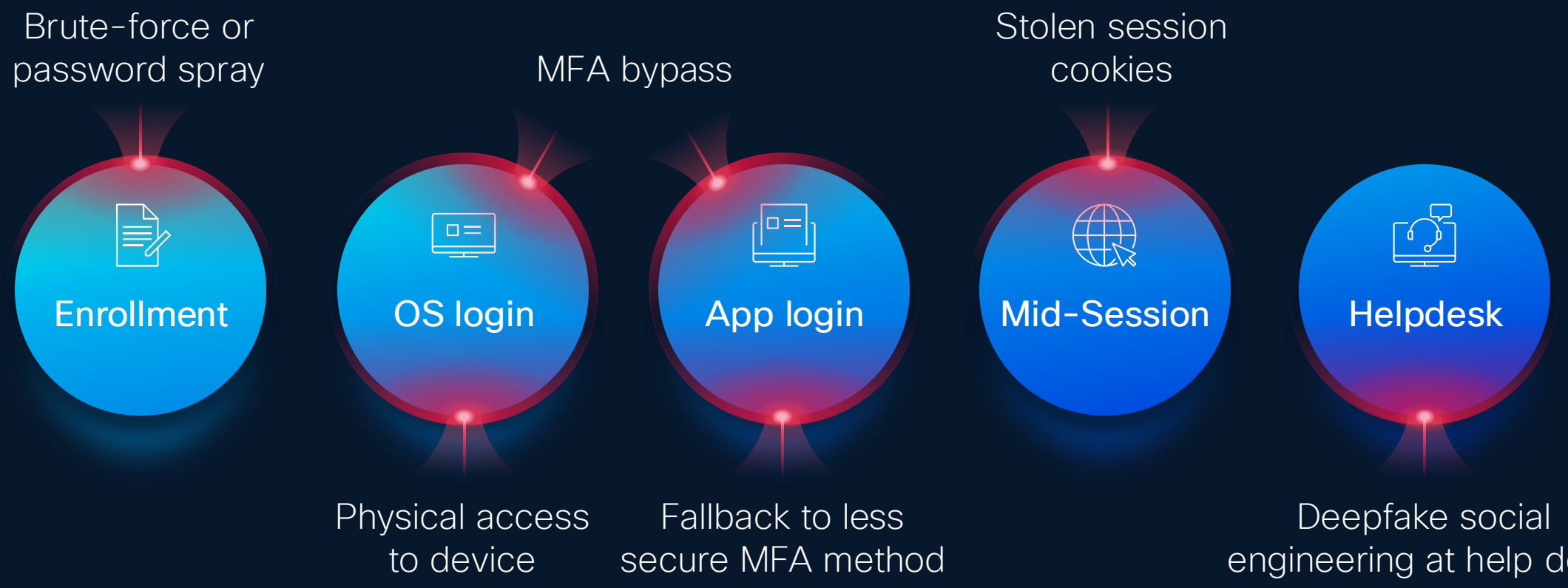

Recycle Bin
Chrome (Work)
Chrome (Personal)
Learn about this picture
Search
ENG
CMK
11:35 AM
12/13/2024

Identity Intelligence

of breaches
leveraged identity
as a key component

Cisco Talos Incident Response | Year in Review 2024

Attackers expect you to have MFA



INTRODUCING

Duo Identity & Access Management (IAM)

Duo IAM

Security-First Identity

End-to-End Phishing Resistance

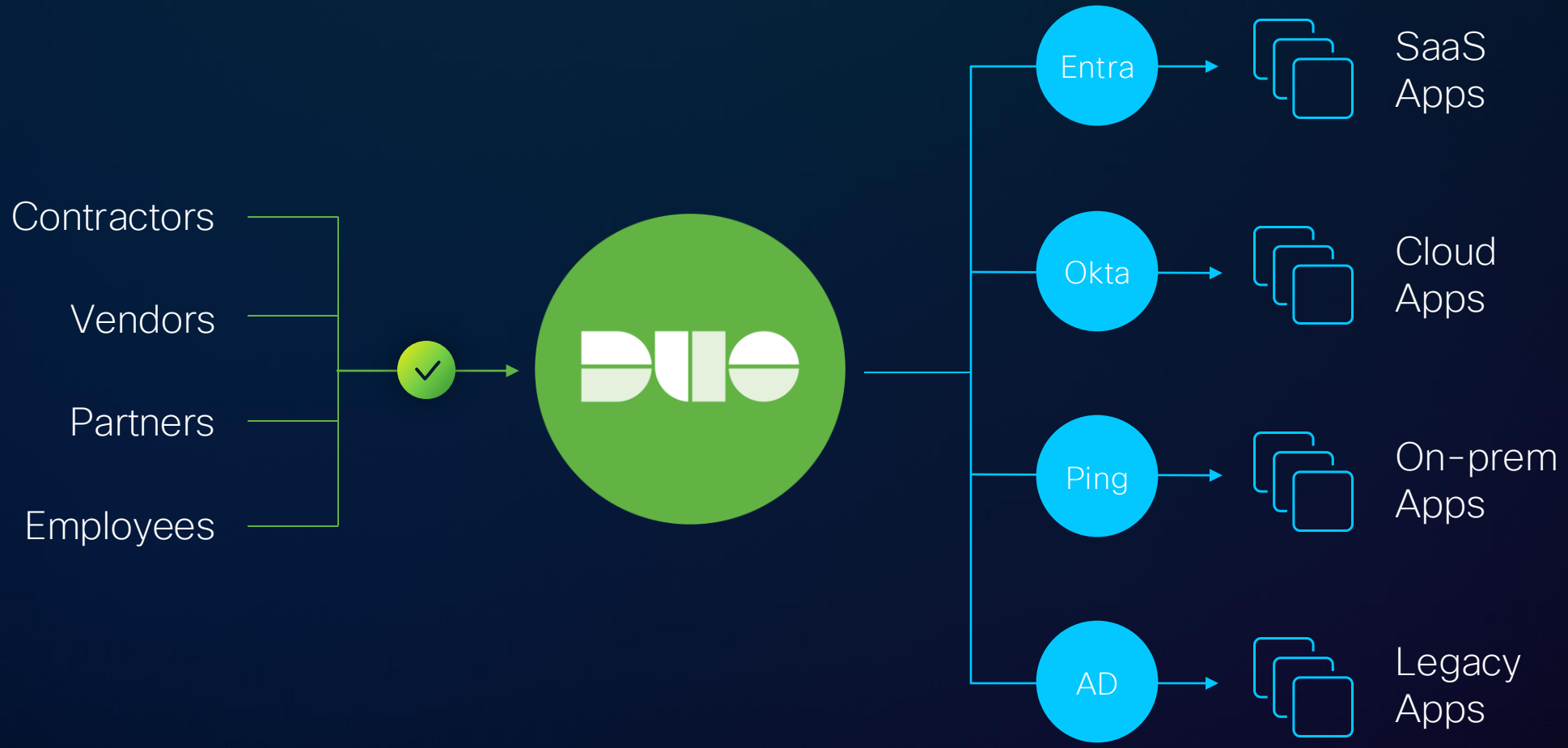
Unified Identity intelligence

World-class user experience

Standalone IAM when required

Identity broker for existing IAM

Alternate directory for third-party users



Duo IAM

Security-First Identity

End-to-End Phishing Resistance

Unified Identity intelligence

World-class user experience

cisco

End-to-end phishing resistance

FIDO2, Hardware Tokens

End-to-end phishing resistance

Cisco Secure Access Use Case

Duo IAM

Security-First Identity

End-to-End Phishing Resistance

Unified Identity Intelligence

World-class user experience

cisco

Cisco Identity Intelligence

SailPoint

Dragos

Crowdstrike

Salesforce

Cisco ISE

Okta

PingIdentity

Auth0

Microsoft

Google

Cyberark

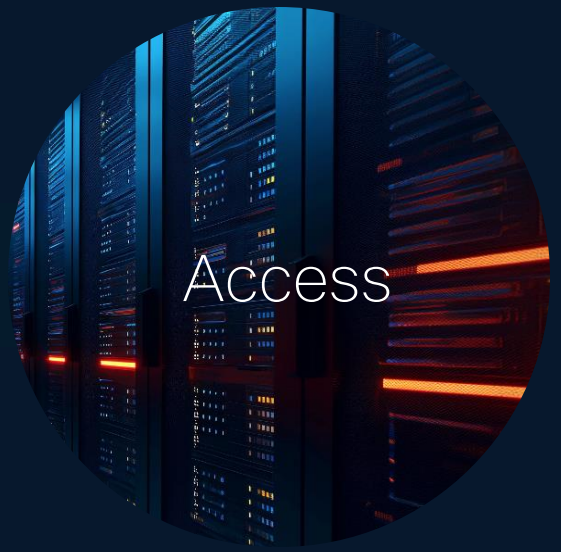
Amazon


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

Identity Intelligence

Continuously assess you are
who you say you are

BLINDTRUST



Works with existing IDPs

cisco

Cisco Duo IAM

Cisco Secure Access

Cisco XDR

User Trust Level

TRUSTED

NEUTRAL

UNTRUSTED

* Capabilities are in private preview.

Cisco Secure Access Use Case

Duo IAM

Security-First Identity

End-to-End Phishing Resistance

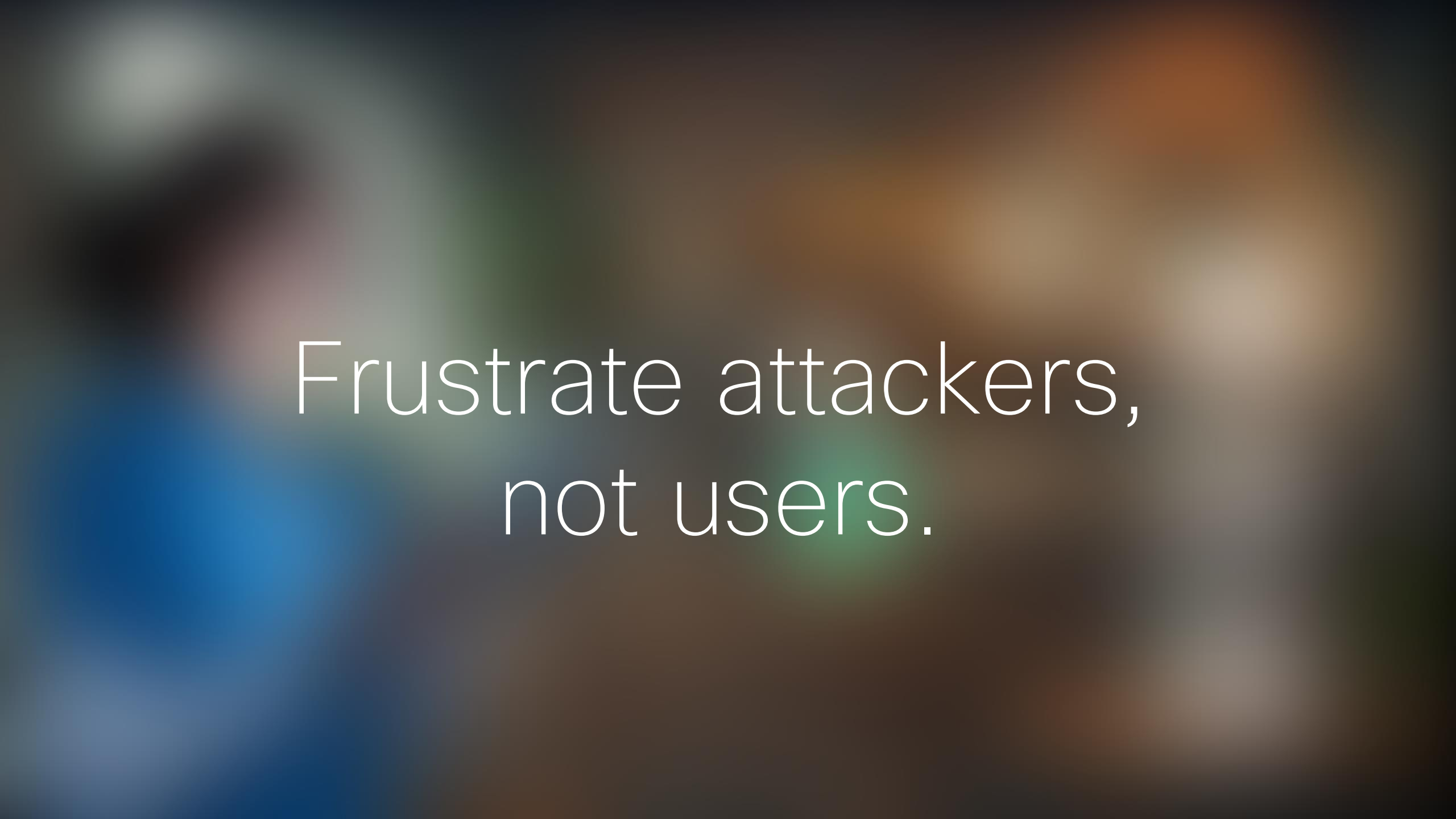
Unified Identity intelligence

World-class user experience

cisco


Authenticate once.
Workday

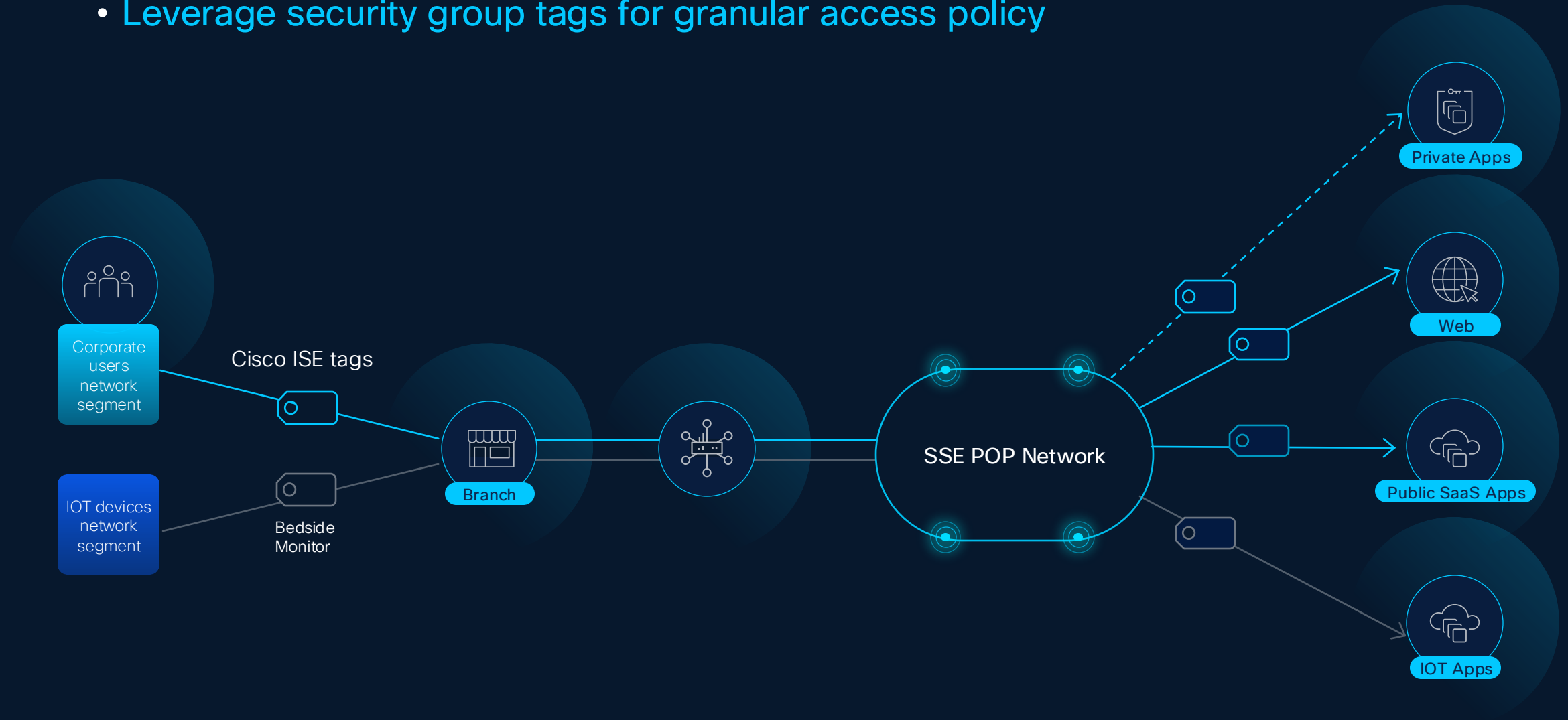

FIREWALL
Workday


Frustrate attackers,
not users.

Things have identities.

Enforce zero trust using identity context

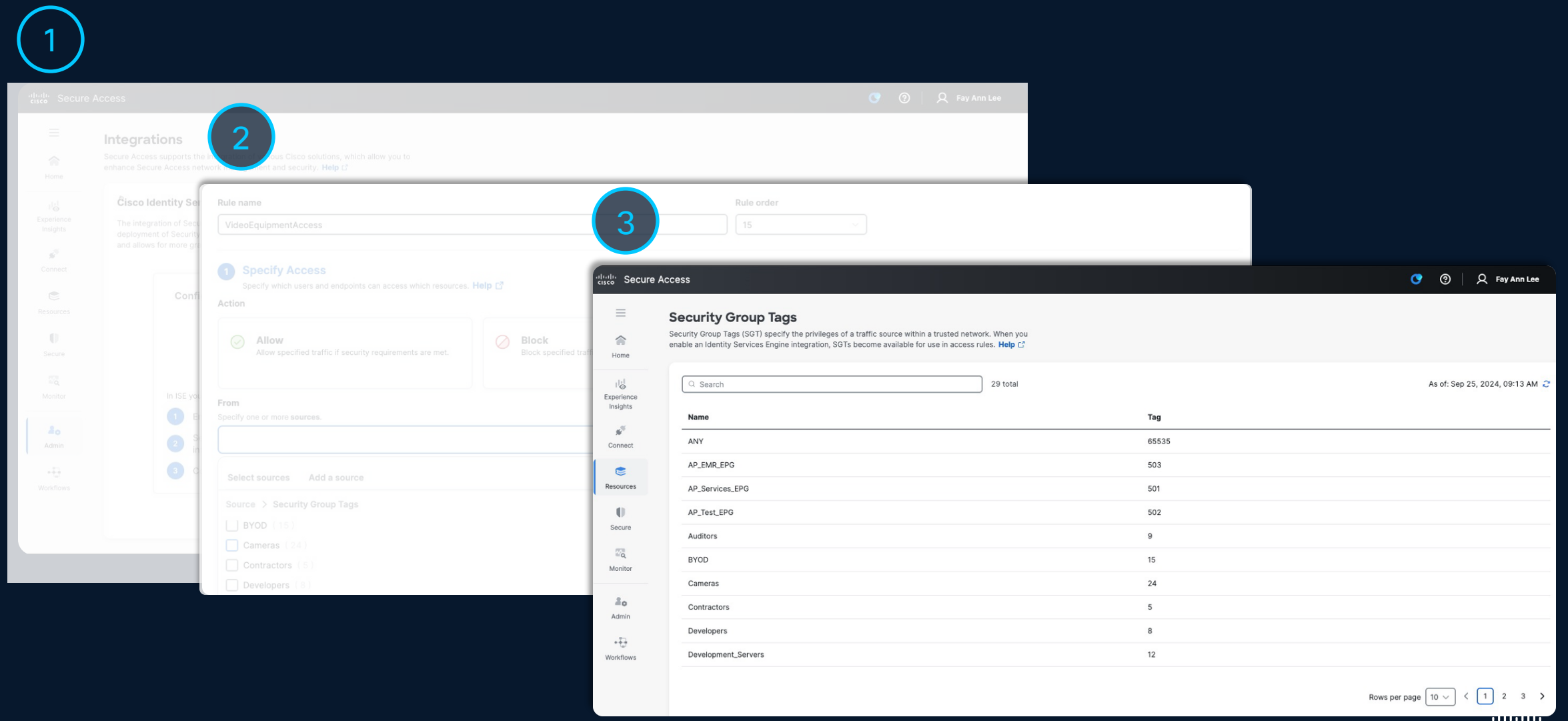
- Leverage security group tags for granular access policy



----- = Future

cisco

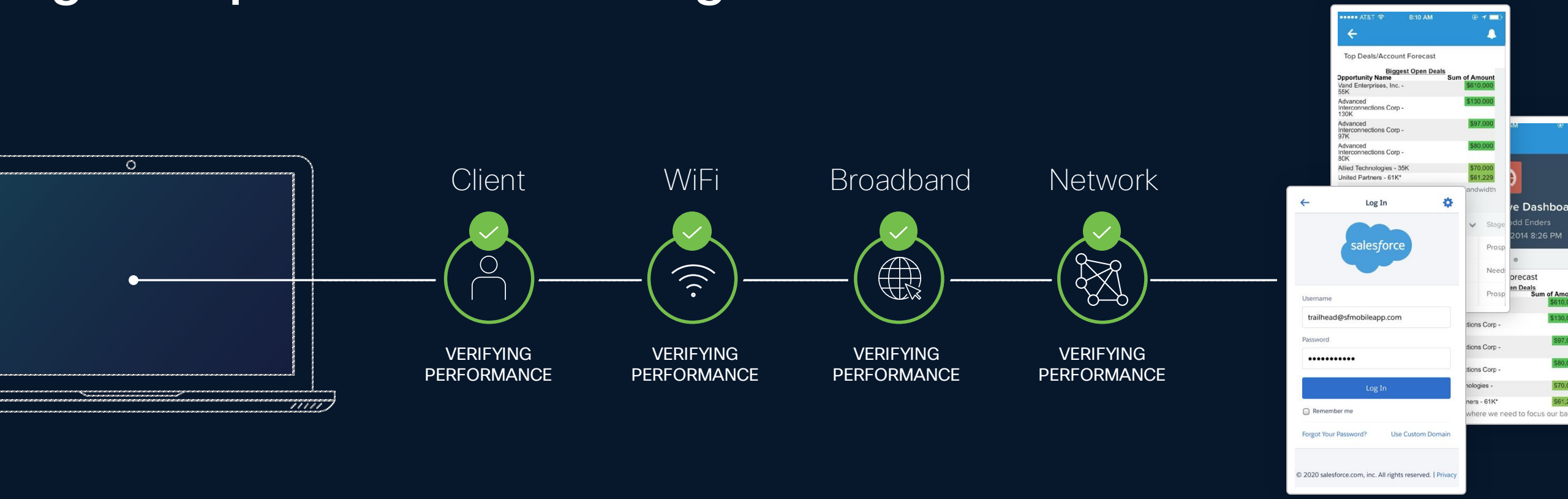
Security Group Tags (SGTs) based policy



Requires ISE and Cisco SD-WAN

Zero downtime

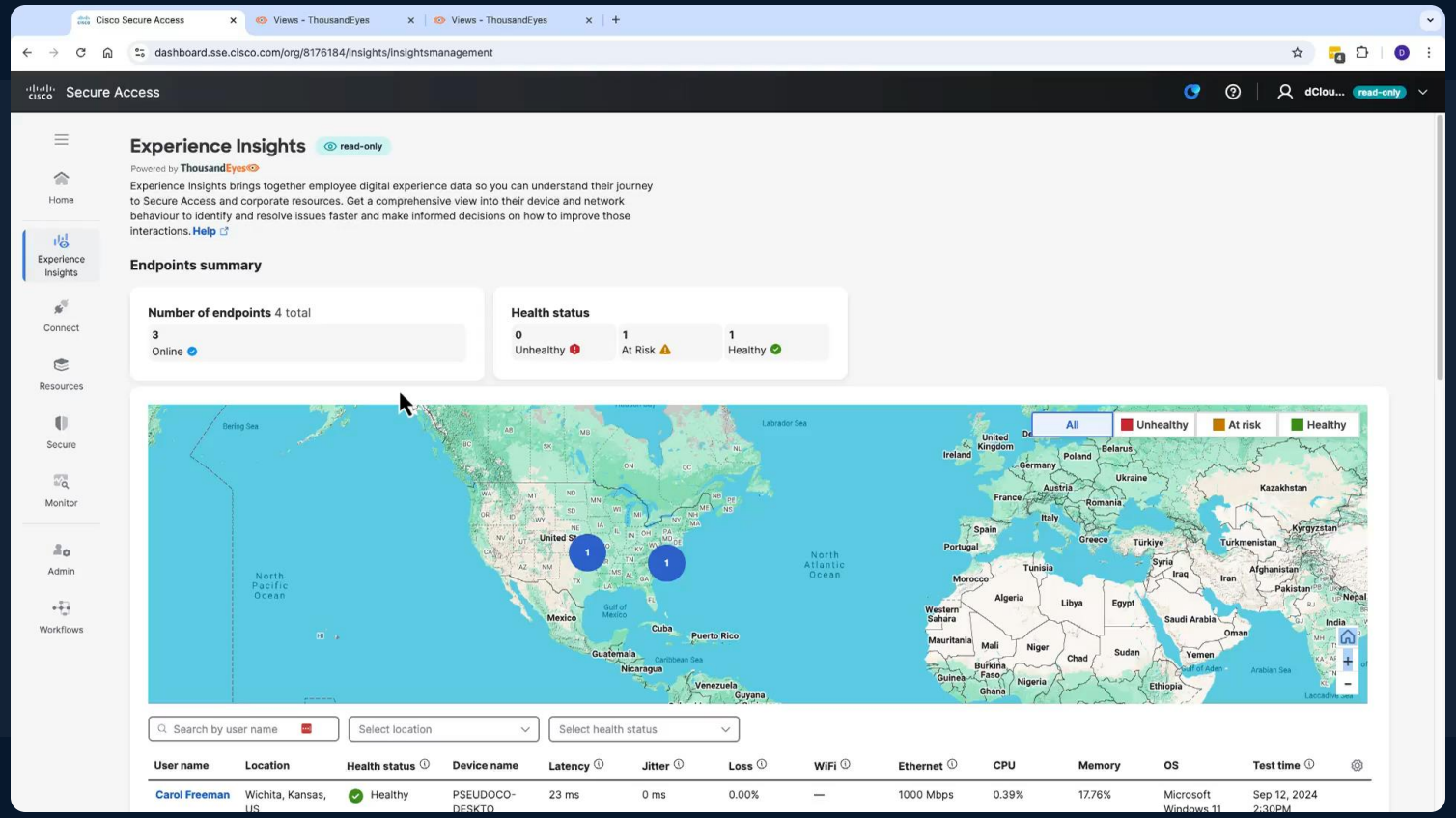
End-to-end visibility with Digital Experience Monitoring



Historical performance and recommendations

Simplify troubleshooting

Consolidated view of network and security events **to make troubleshooting easier**



Cisco Secure Access | Views - ThousandEyes | Views - ThousandEyes

dashboard.sse.cisco.com/org/8176184/insights/insightsmanagement

Secure Access

dClou... read-only

Home

Experience Insights

Connect

Resources

Secure

Monitor

Admin

Workflows

Experience Insights

read-only

Powered by ThousandEyes

Experience Insights brings together employee digital experience data so you can understand their journey to Secure Access and corporate resources. Get a comprehensive view into their device and network behaviour to identify and resolve issues faster and make informed decisions on how to improve those interactions. Help

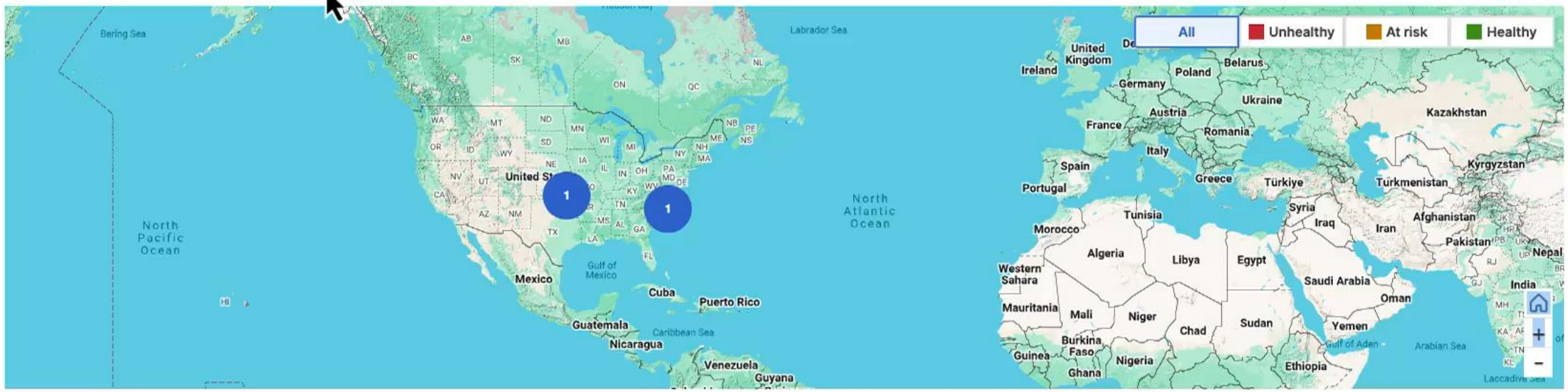
Endpoints summary

Number of endpoints 4 total

3
Online

Health status

0	1	1
Unhealthy	At Risk	Healthy



Search by user name | Select location | Select health status

User name	Location	Health status	Device name	Latency	Jitter	Loss	WiFi	Ethernet	CPU	Memory	OS	Test time
Carol Freeman	Wichita, Kansas,	Healthy	PSEUDOCO-	23 ms	0 ms	0.00%	—	1000 Mbps	0.39%	17.76%	Microsoft	Sep 12, 2024

CISCO Connect

Summary

Cisco clears the path to zero trust

Protect identities with identity intelligence

Control access across all users and things for tighter security

Build resilience with optimized infrastructure and simplified IT

cisco

Thank you


CISCO

- User frustration with cumbersome experiences
- Risks from unmanaged devices/BYOD (contractors)
- Risks from AI app/platform use

Need seamless access to all apps

- Identity attacks are accelerating
- Security gaps from "things" (IT, OT, IOT)
- Difficult to verify identity as user behavior/ locations change

Need identity intelligence

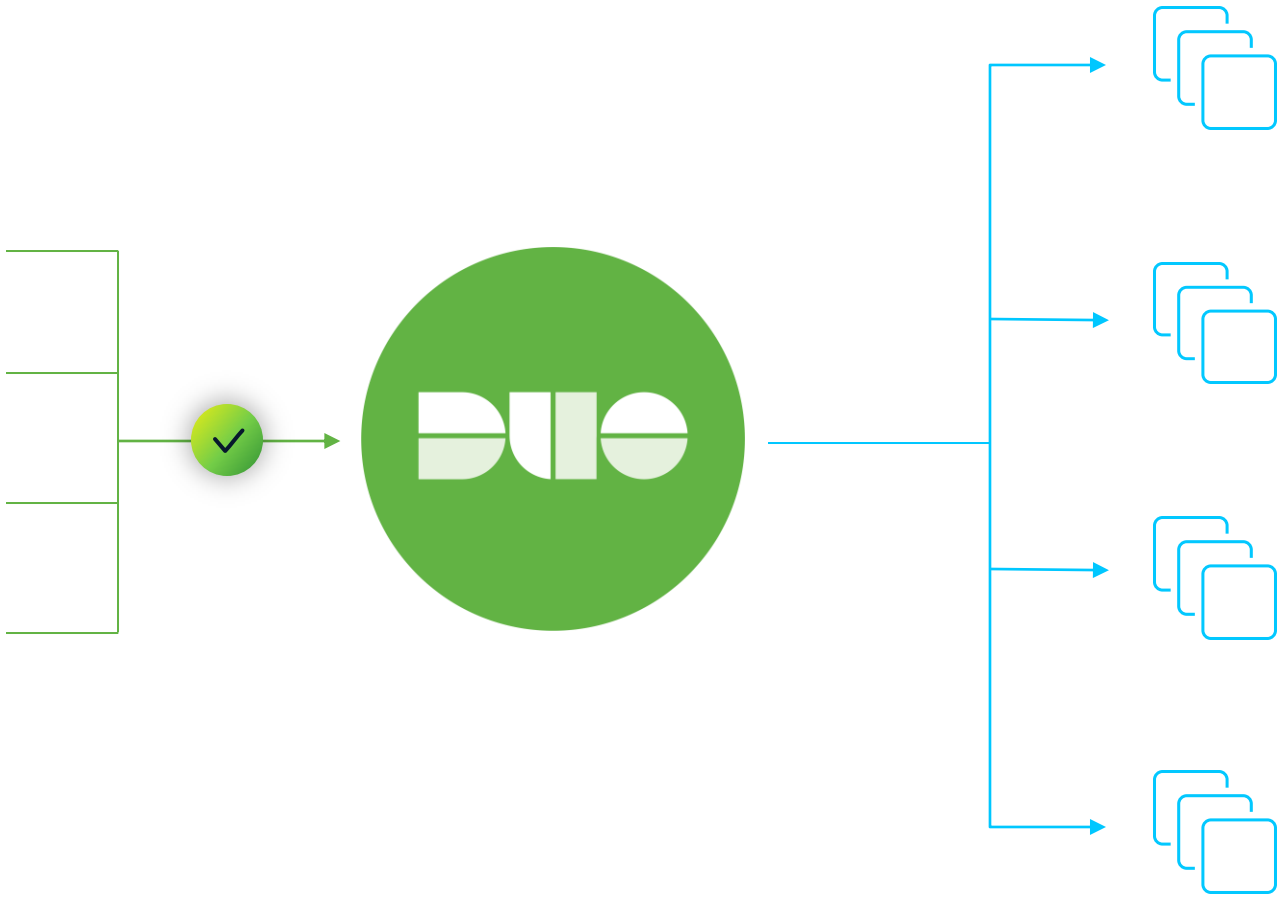
- Interruptions/slowdowns impede productivity
- Problem detection/ remediation is not fast enough
- Policy changes create unintended consequences

Need zero downtime

Standalone IAM
when required

Identity broker
for existing IAM

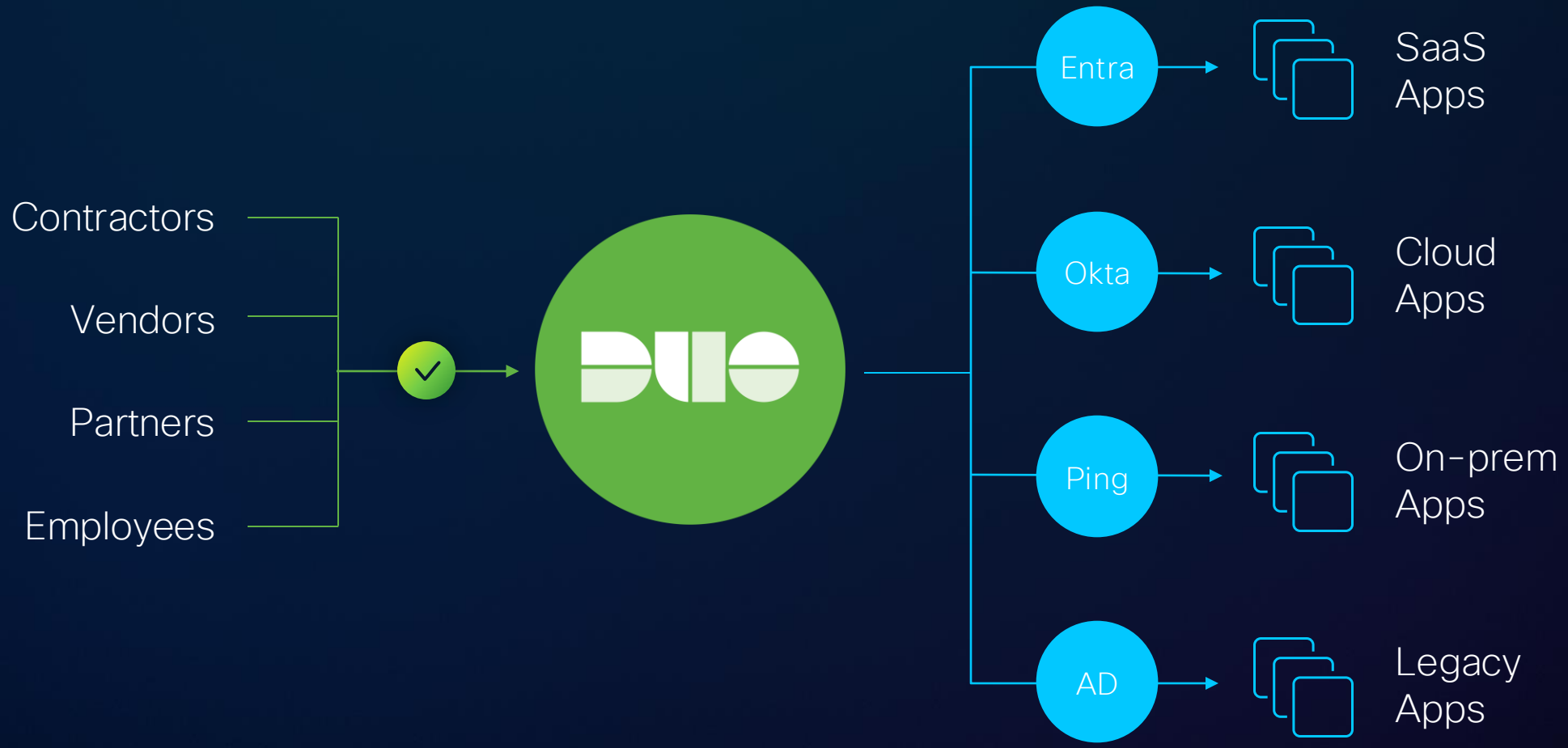
Alternate directory for
third-party users



Standalone IAM when required

Identity broker for existing IAM

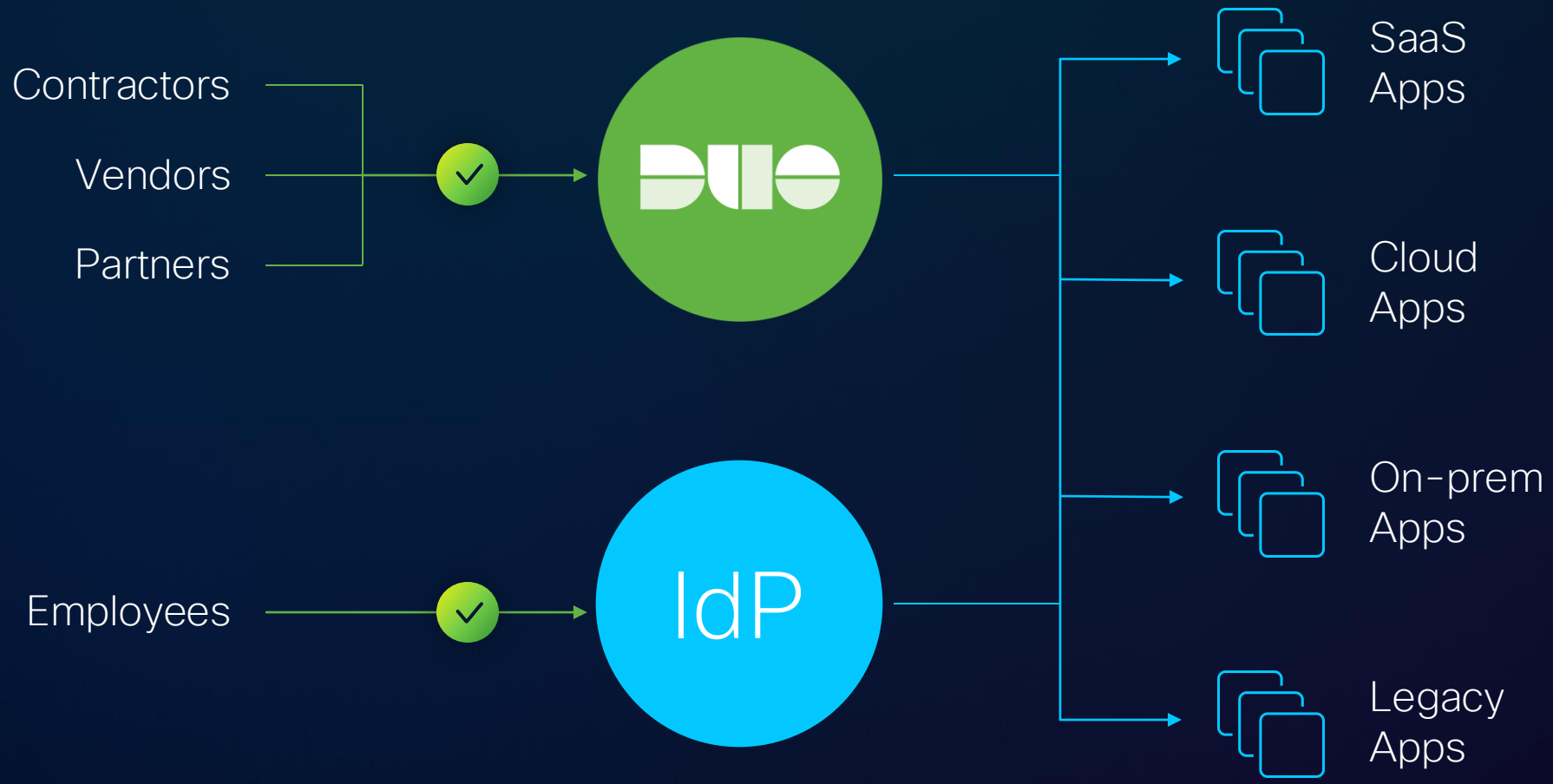
Alternate directory for third-party users



Standalone IAM when required

Identity broker for existing IAM

Alternate directory for third-party users



Customer challenges we consistently hear

- User frustration with cumbersome experiences
- Risks from unmanaged devices/BYOD (contractors)
- Risks from AI app/platform use

Need seamless access to all apps

- Identity attacks are accelerating
- Security gaps from “things” (IT, OT, IOT)
- Difficult to verify identity as user behavior/ locations change

Need identity intelligence

- Interruptions/slowdowns impede productivity
- Problem detection/ remediation is not fast enough
- Policy changes create unintended consequences

Need zero downtime