CISCO Connect

Transforming Secure Connectivity for the AI-Ready Enterprise

Brandon Gordon, Security Solutions Engineer

March 24, 2026

What We'll Discuss Today

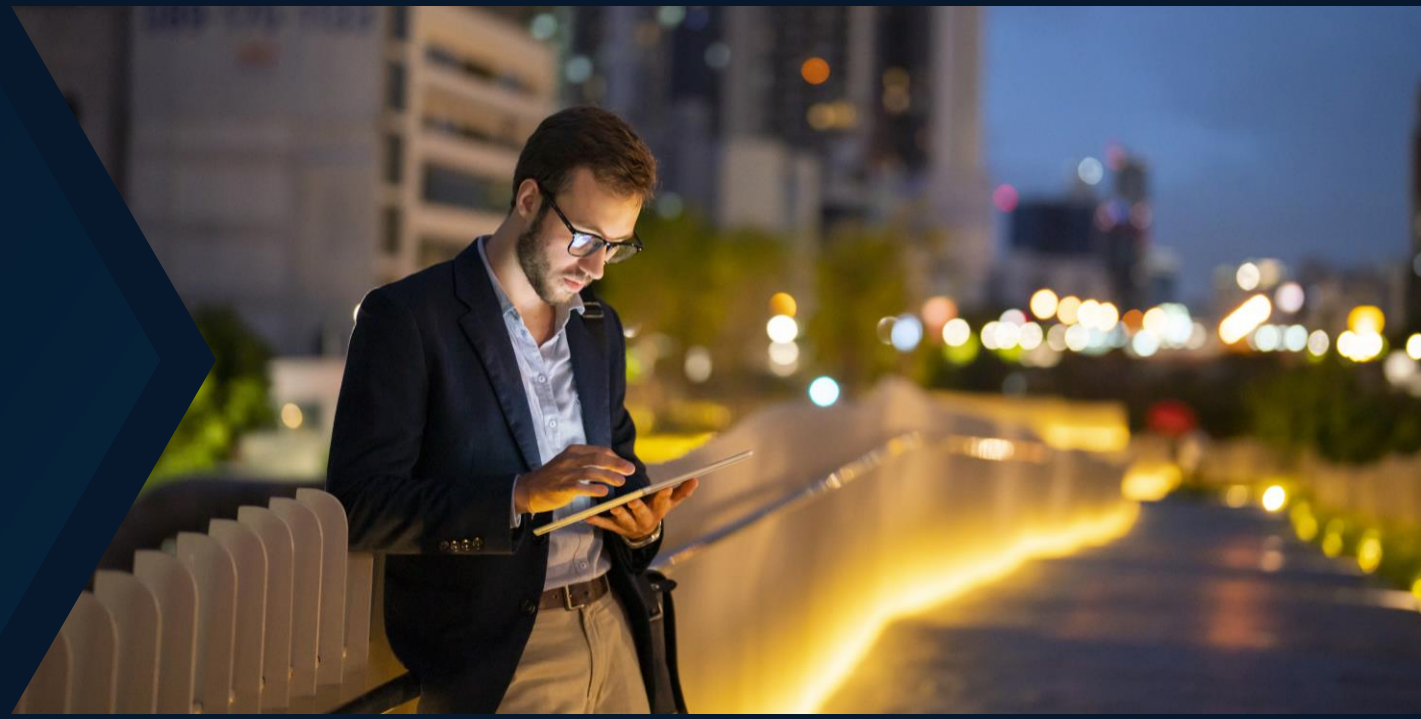
1. Introduction to Cisco Universal Zero Trust Network Access
2. Seamless Access
3. Duo – Security-first IAM
4. Cisco Identity Intelligence
5. Zero Trust for Agentic AI

slido

https://cs.co/connect-uztna

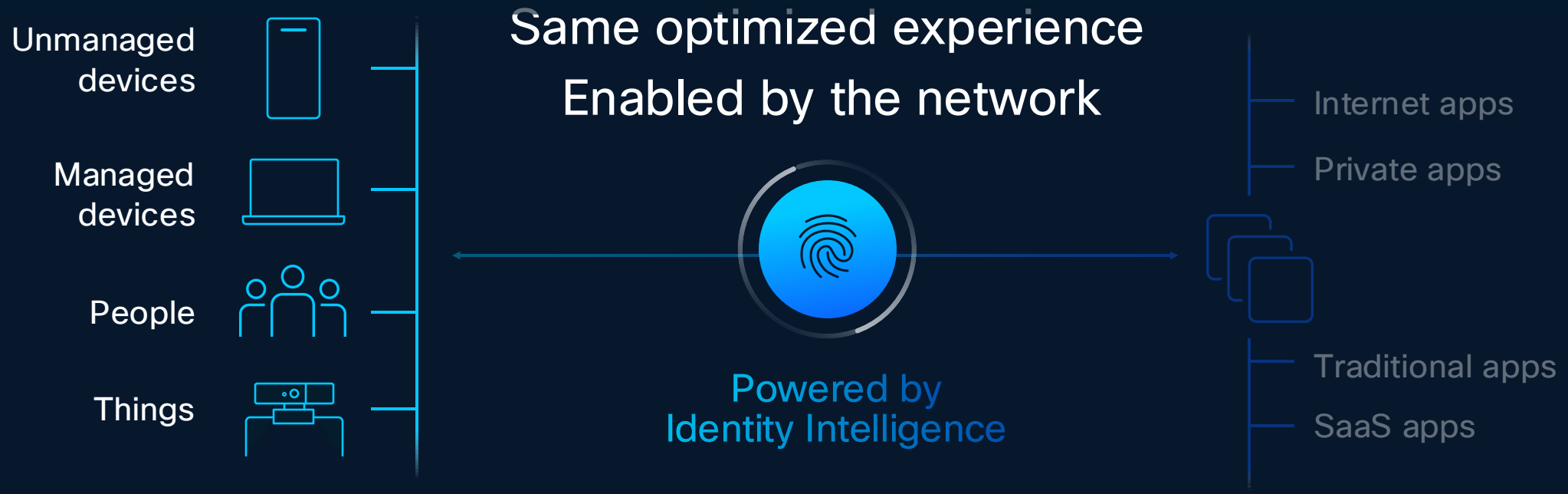
cisco

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 Universal ZTNA

Takes ZTNA to users and **devices**

slido

https://cs.co/connect-uztna

cisco

Seamless Access for All Applications

Zero Friction: Transparent UZTNA

STEP 1
Authenticate,

STEP 2
Access private app

We do the plumbing, 1Gbps!

Continuously assess identity and posture transparently

CII
Secure SSO
Passport

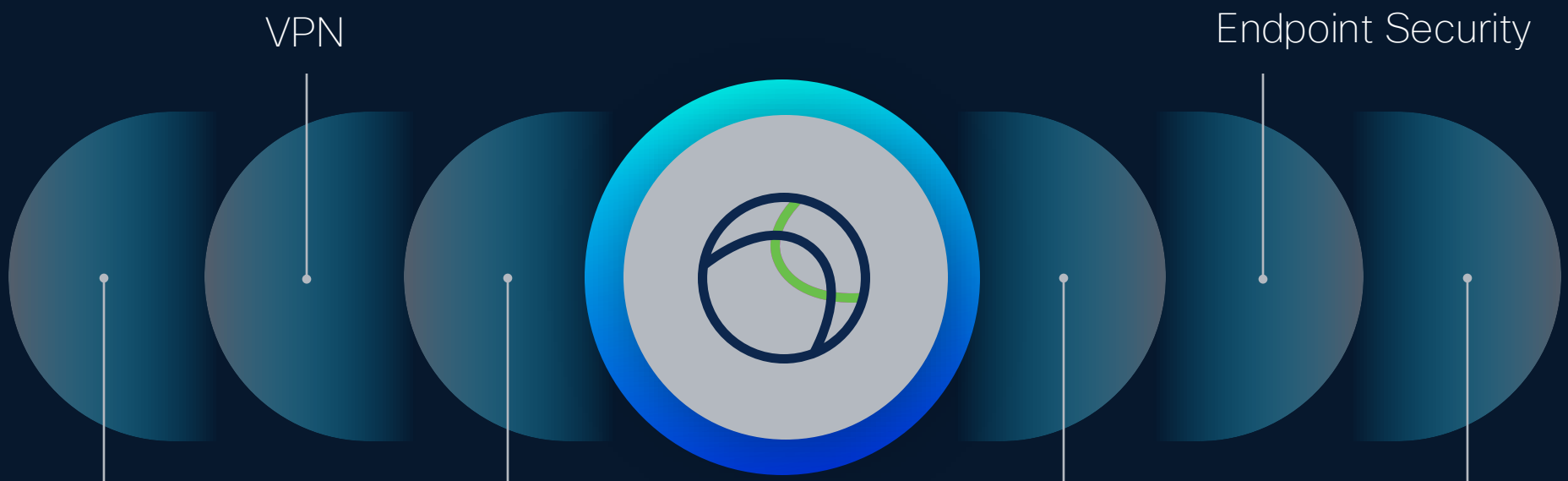
Traditional apps

Private apps

Internet apps

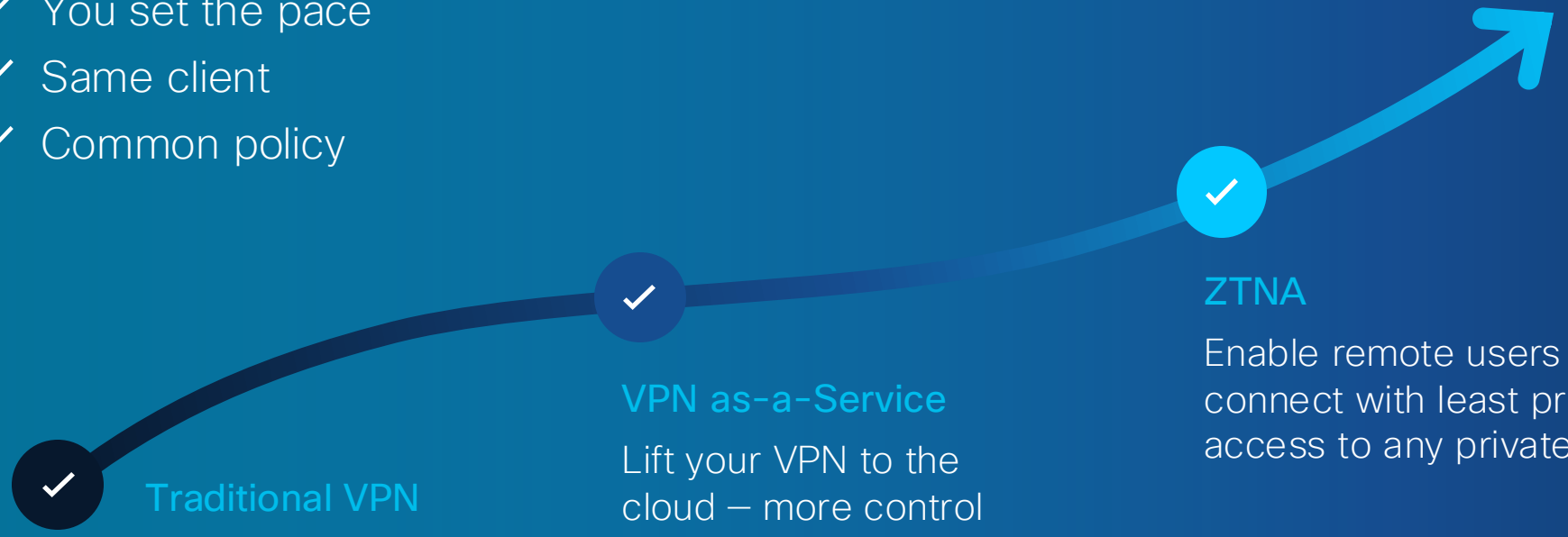
SaaS apps

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.

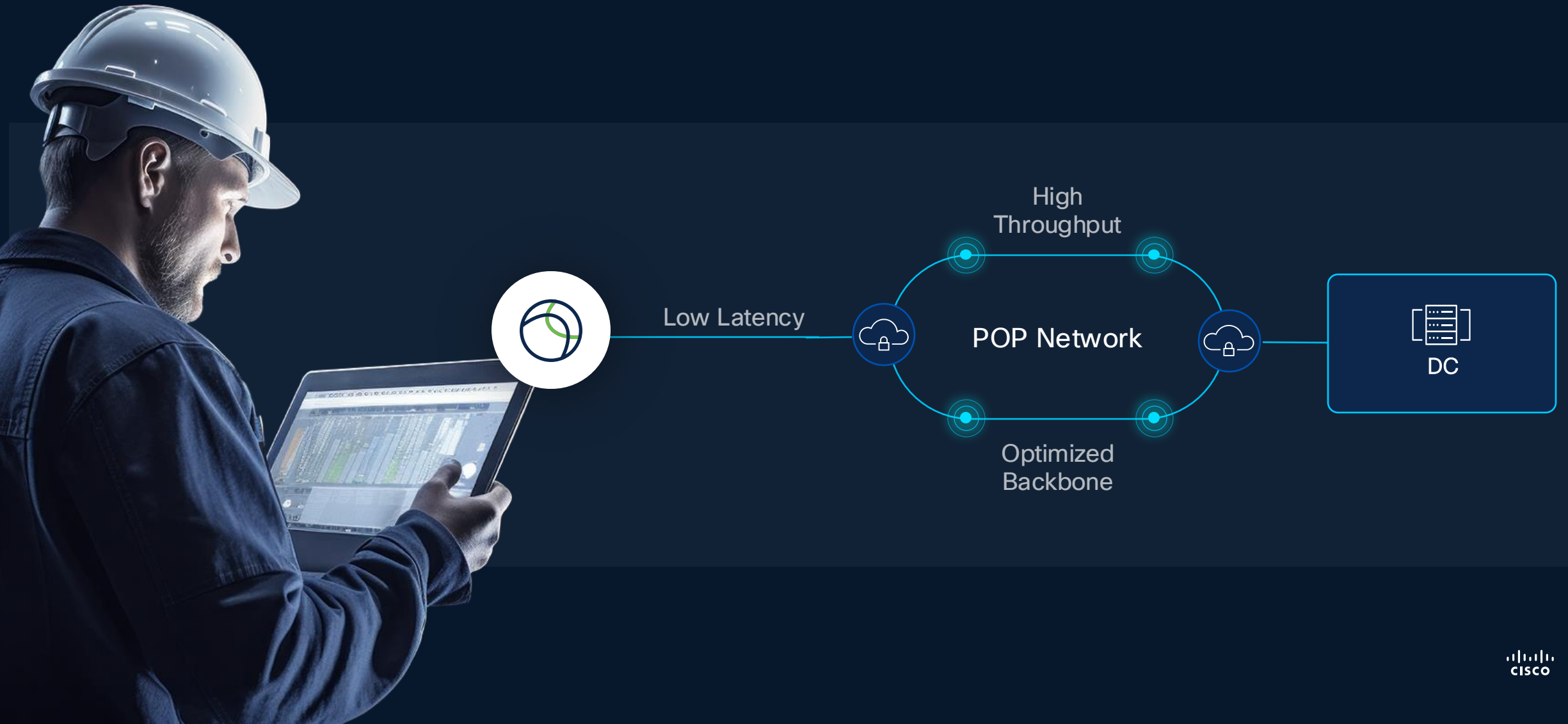
Universal ZTNA

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 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

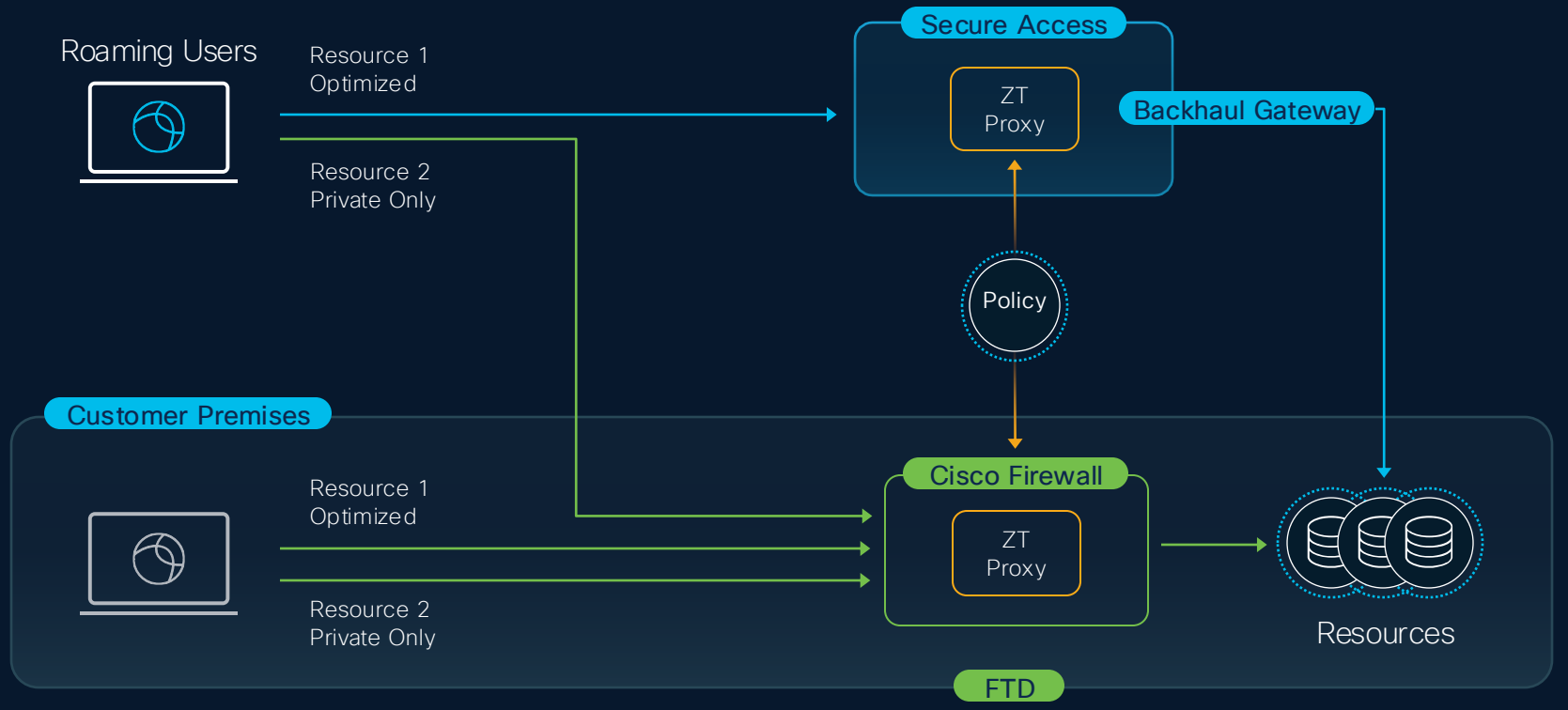
Advanced threat protection for a secure network

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

cisco

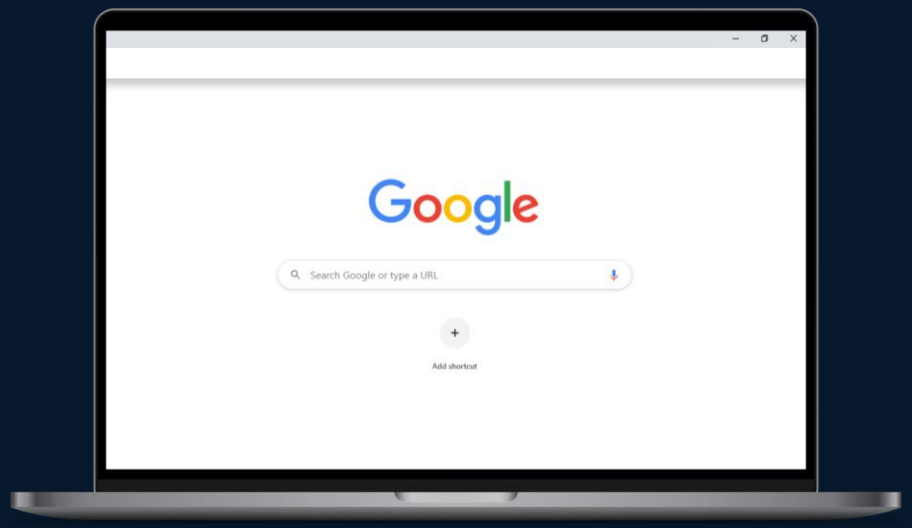
Hybrid Private Access for Flexible Enforcement

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



Device Support

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

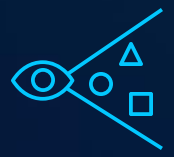


Chrome Enterprise Browser

Native OS Integration

Cisco AI Access

Securing the use of AI



Visibility

Leakage prevention

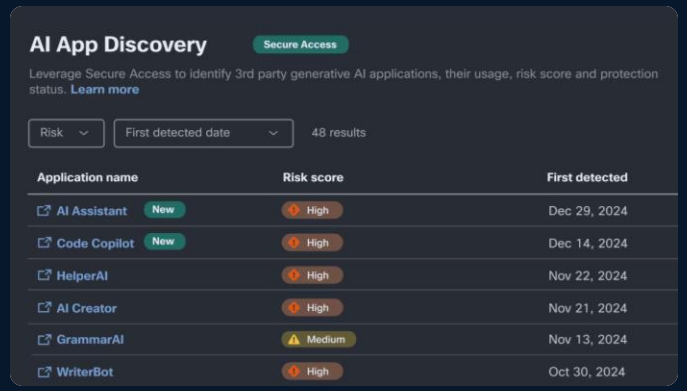
Compliant use

1200+ AI applications

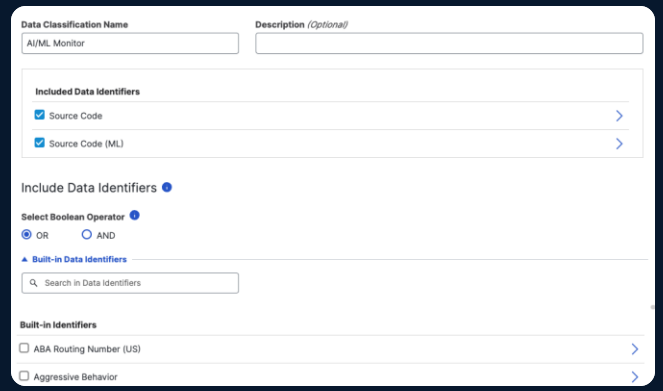
Zero Blind Spots: Secure Access for AI Users

AI Access protection that goes beyond discovery

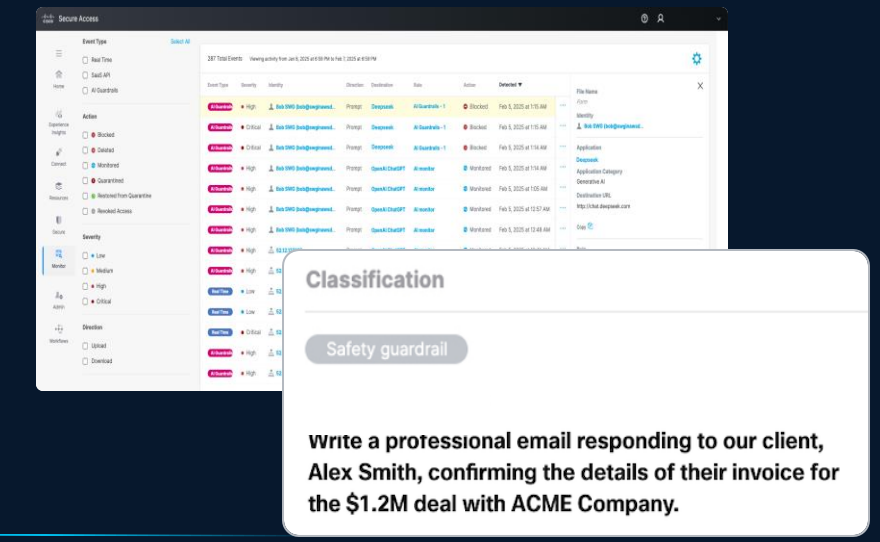
Discover shadow AI & block specific apps



Advanced AI/ML DLP controls



Enforce guardrails for AI queries: Security, Privacy, Safety



1200+
AI Apps Protected

100%
Guardrails for top AI Apps

1
Unified Security Platform

cisco

Zero Blind Spots: Secure Access for AI Developers

AI supply chain and risk management

Allow visibility & responsible usage of Hugging Face Models

Origin Risk

IP Risk

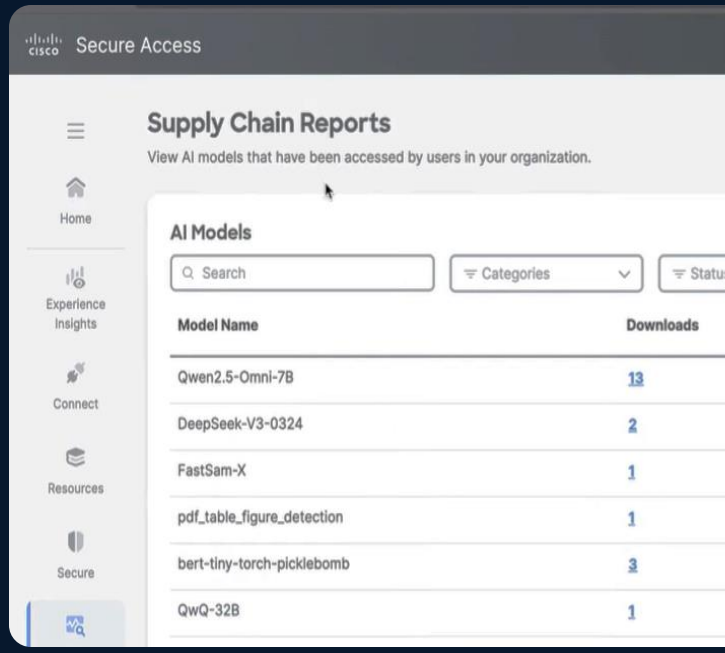
Malicious Code

Hugging Face

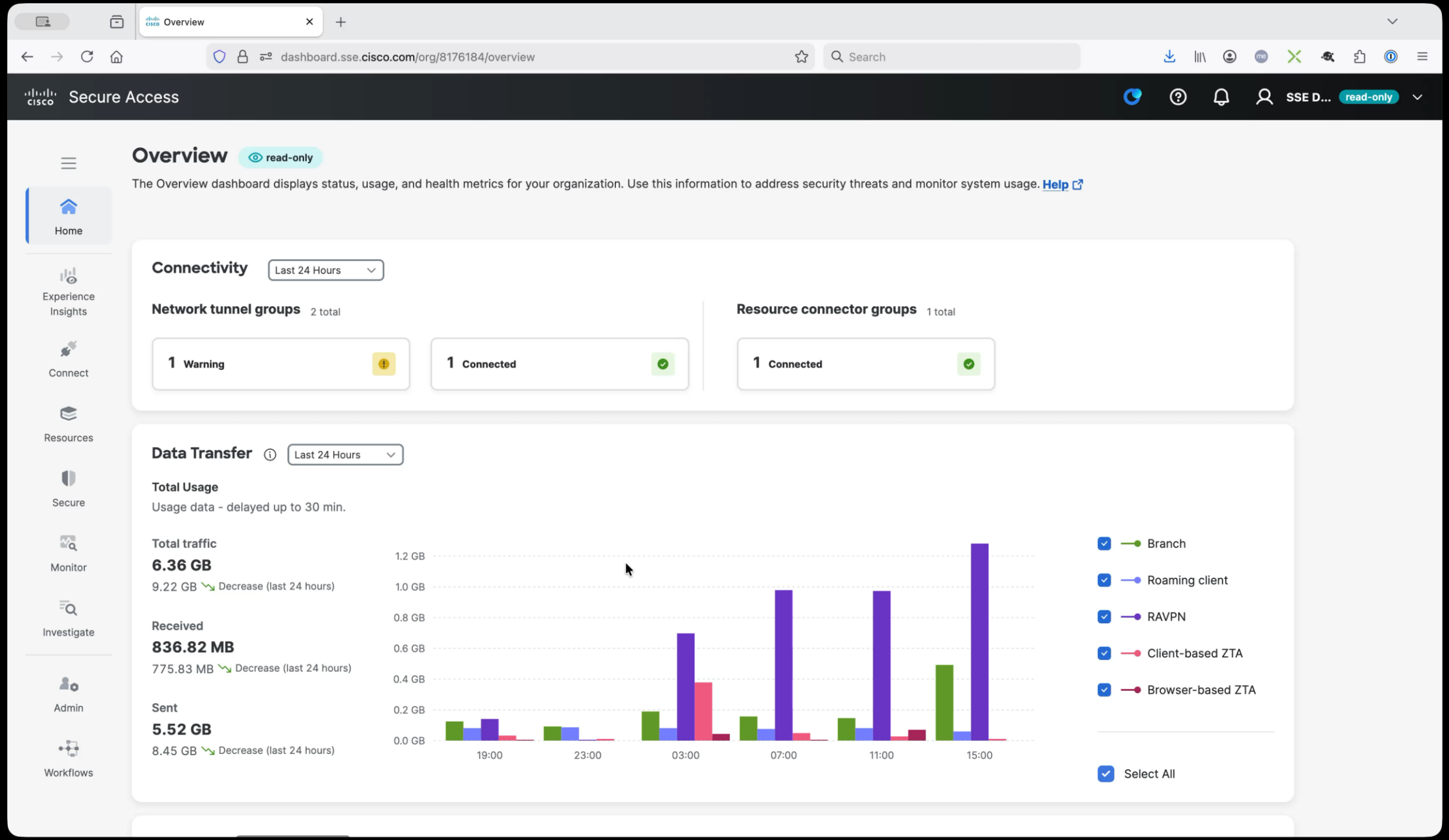
Name-XXX-YYY-vvlknsek-test

Train | Deploy | Use in XYZ

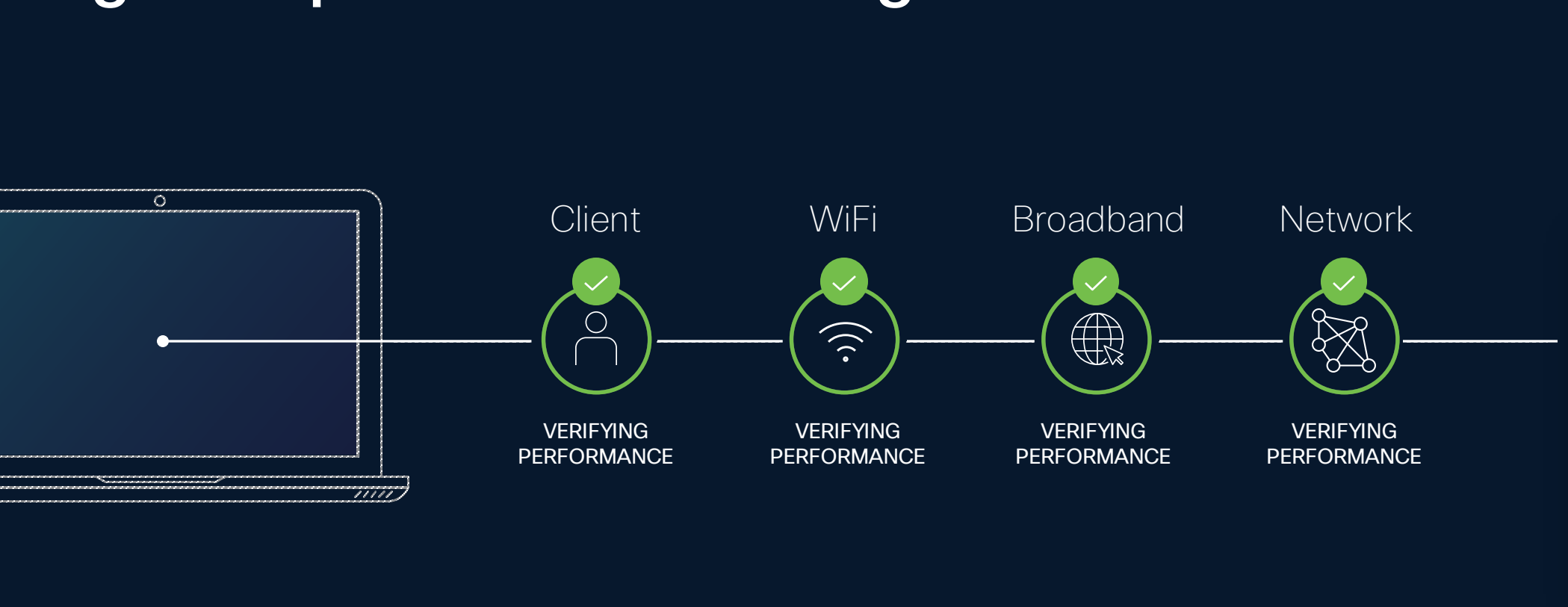
This model exfiltrates user data.



Demo – AI Access and AI Supply Chain Risk


Overview
dashboard.sse.cisco.com/org/8176184/overview
Search
Secure Access
SSE D...
read-only
Overview
read-only
The Overview dashboard displays status, usage, and health metrics for your organization. Use this information to address security threats and monitor system usage. Help
Home
Experience Insights
Connect
Resources
Secure
Monitor
Investigate
Admin
Workflows
Connectivity
Last 24 Hours
Network tunnel groups 2 total
1 Warning
1 Connected
Resource connector groups 1 total
1 Connected
Data Transfer
Last 24 Hours
Total Usage
Usage data - delayed up to 30 min.
Total traffic
6.36 GB
9.22 GB Decrease (last 24 hours)
Received
836.82 MB
775.83 MB Decrease (last 24 hours)
Sent
5.52 GB
8.45 GB Decrease (last 24 hours)
1.2 GB
1.0 GB
0.8 GB
0.6 GB
0.4 GB
0.2 GB
0.0 GB
19:00
23:00
03:00
07:00
11:00
15:00
Branch
Roaming client
RAVPN
Client-based ZTA
Browser-based ZTA
Select All

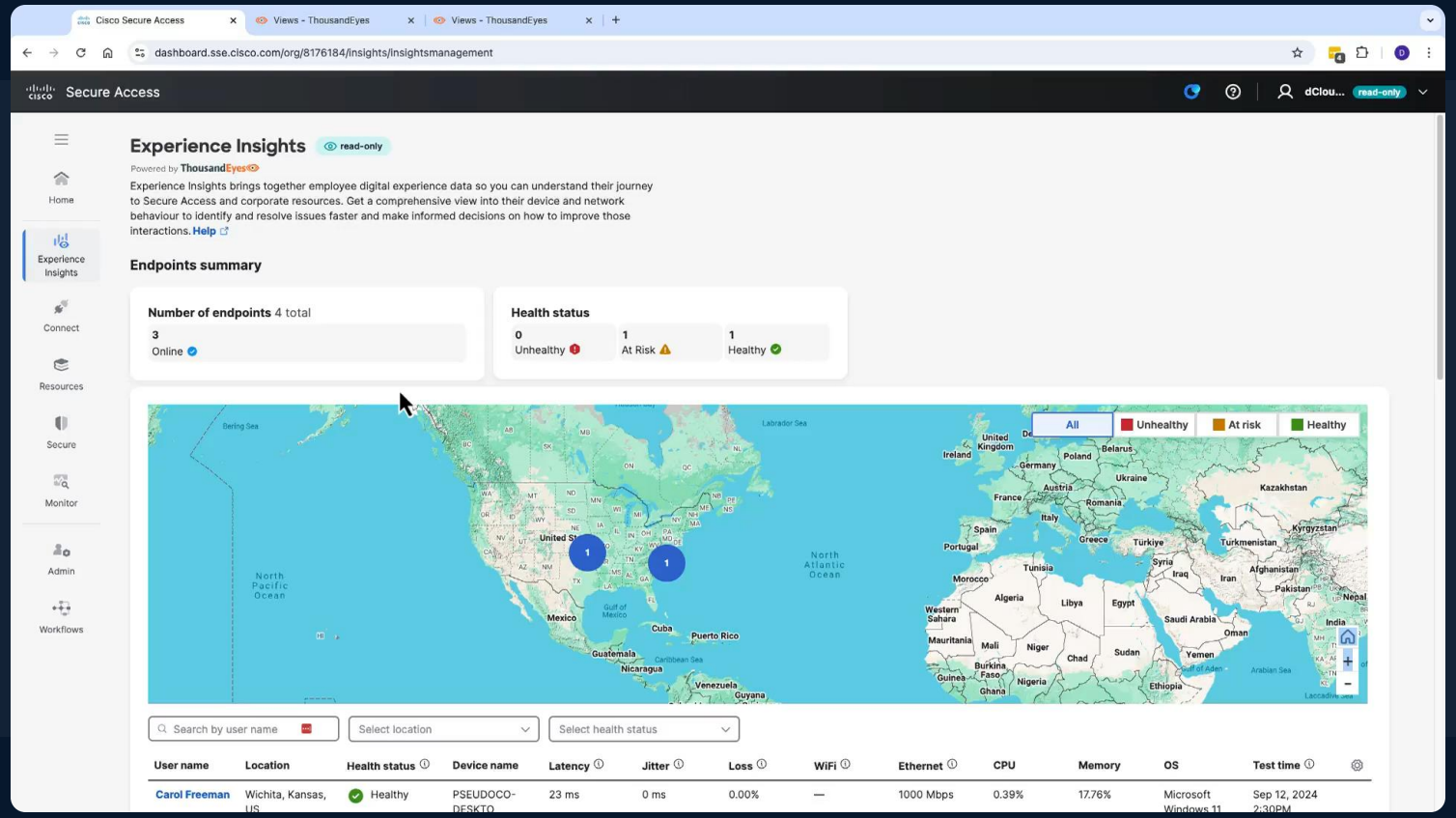
End-to-End Visibility with Digital Experience Monitoring



Historical performance and recommendations

Simplify Troubleshooting

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



Identity Intelligence

slido

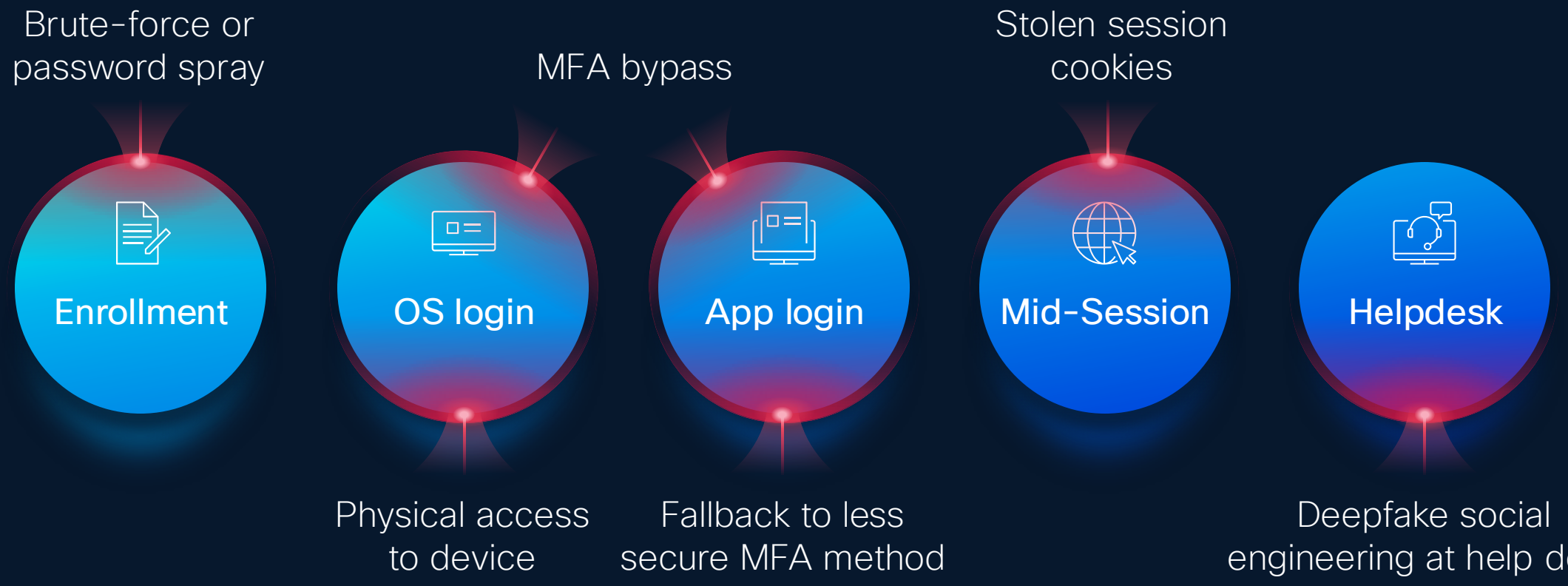
https://cs.co/connect-uztna

cisco

of breaches
leveraged identity
as a key component

Cisco Talos Incident Response | Year in Review 2025

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

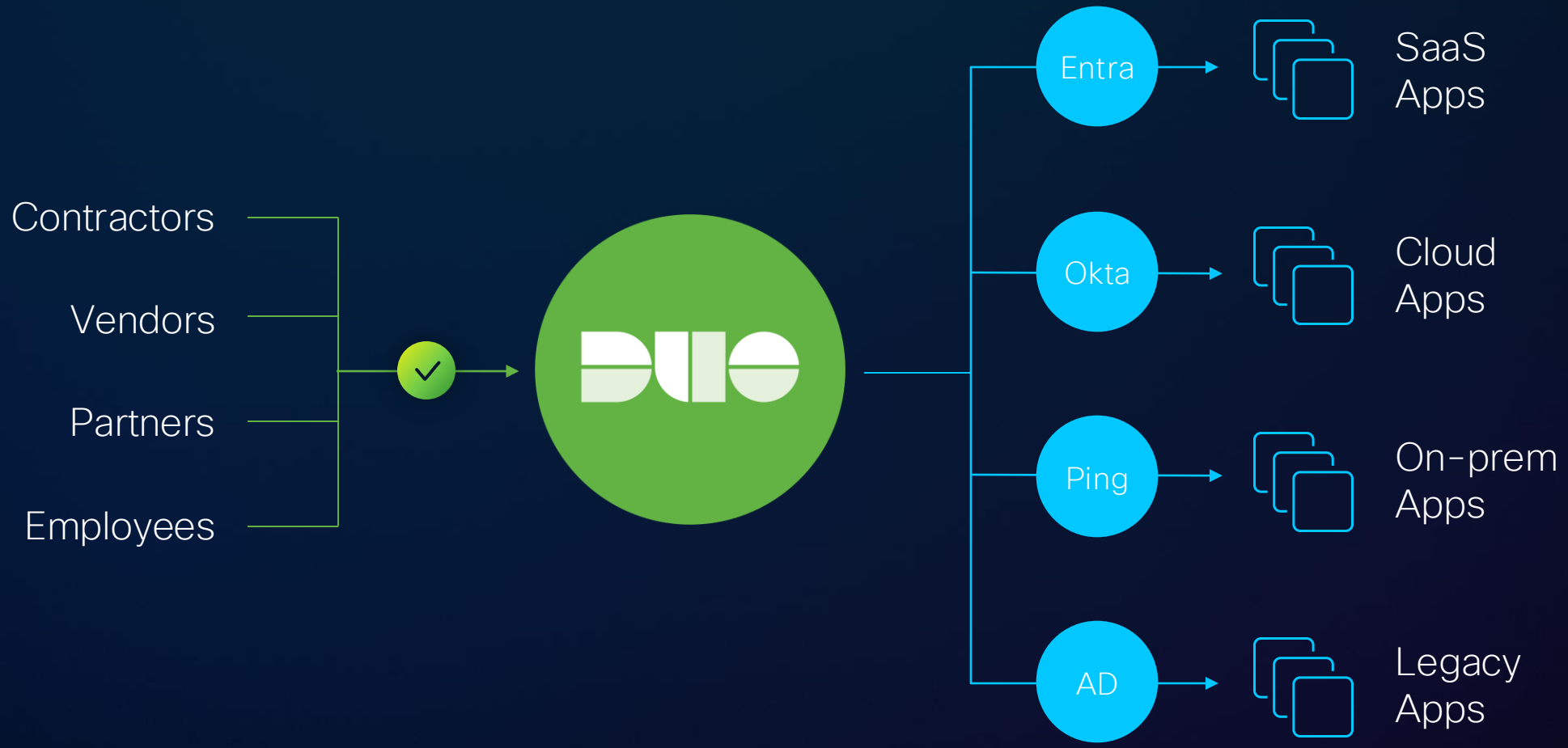
World-class user experience

cisco

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

End-to-End Phishing Resistance

FIDO2, Hardware Tokens

End-to-End Phishing Resistance

Duo IAM

Security-First Identity

End-to-End Phishing Resistance

Unified Identity Intelligence

World-Class User Experience

Cisco Identity Intelligence

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

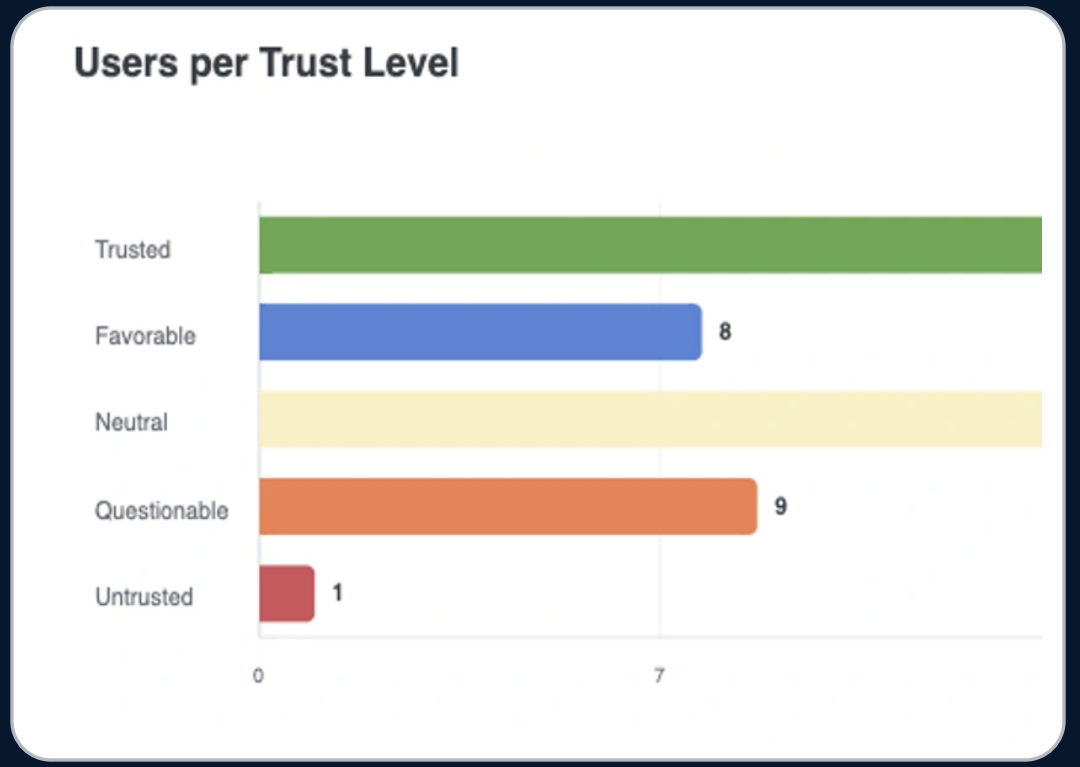
Zero Imposters: Identity-Based User Trust Level

- In Duo, Secure Access, and Firewall
- A user's trust level is determined via risk inputs
- Score dynamically changes

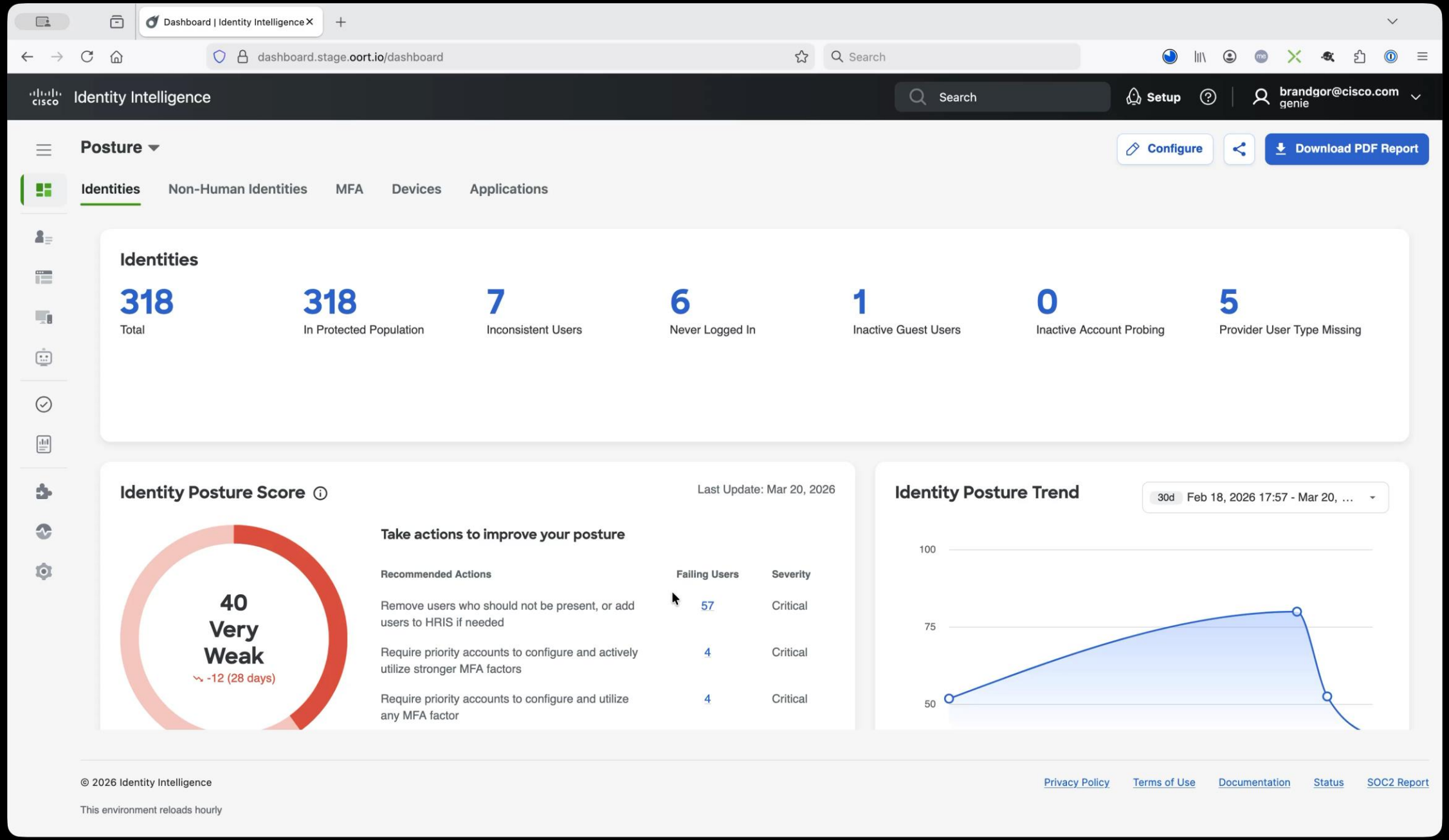
User risk inputs

- Inherent Risk (exec/admin roles)
- Posture Risk (MFA, password strength, device posture)
- Behavior Risk (recent activity, anomalies)
- Action Risk (real-time signals: IP, location, app)

Trust level output



Demo – Cisco Identity Intelligence


Dashboard | Identity Intelligence
dashboard.stage.oort.io/dashboard
Search
Identity Intelligence
Search
Setup
brandgor@cisco.com
genie
Posture
Configure
Download PDF Report
Identities
Non-Human Identities
MFA
Devices
Applications
Identities
318
Total
318
In Protected Population
7
Inconsistent Users
6
Never Logged In
1
Inactive Guest Users
0
Inactive Account Probing
5
Provider User Type Missing
Identity Posture Score
Last Update: Mar 20, 2026
40
Very
Weak
-12 (28 days)
Take actions to improve your posture
Recommended Actions
Failing Users
Severity
Remove users who should not be present, or add users to HRIS if needed
57
Critical
Require priority accounts to configure and actively utilize stronger MFA factors
4
Critical
Require priority accounts to configure and utilize any MFA factor
4
Critical
Identity Posture Trend
30d
Feb 18, 2026 17:57 - Mar 20, ...
100
75
50
© 2026 Identity Intelligence
Privacy Policy
Terms of Use
Documentation
Status
SOC2 Report
This environment reloads hourly

Cisco Secure Access Use Case

Duo IAM

Security-First Identity

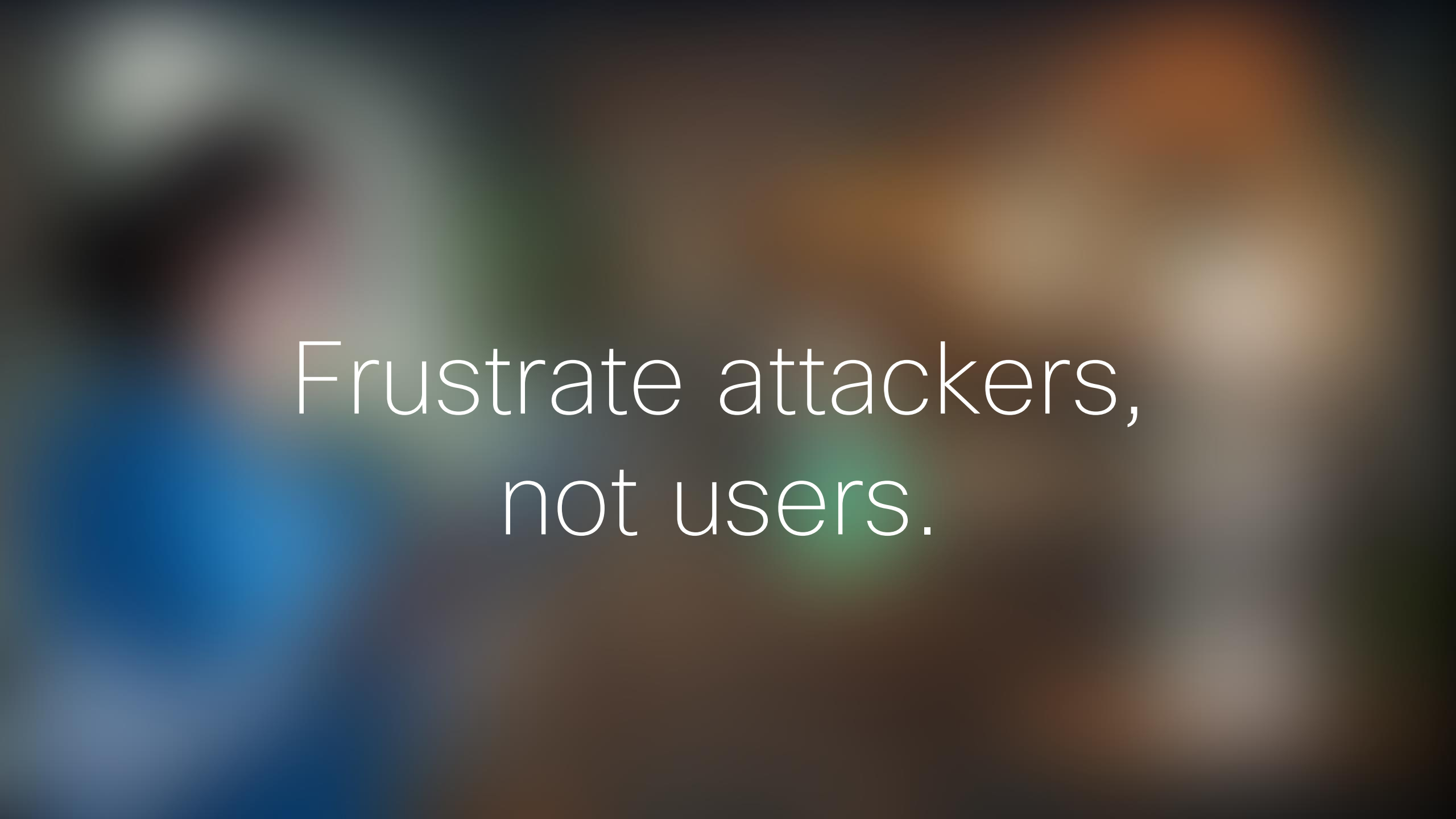
End-to-End Phishing Resistance

Unified Identity intelligence

World-Class User Experience

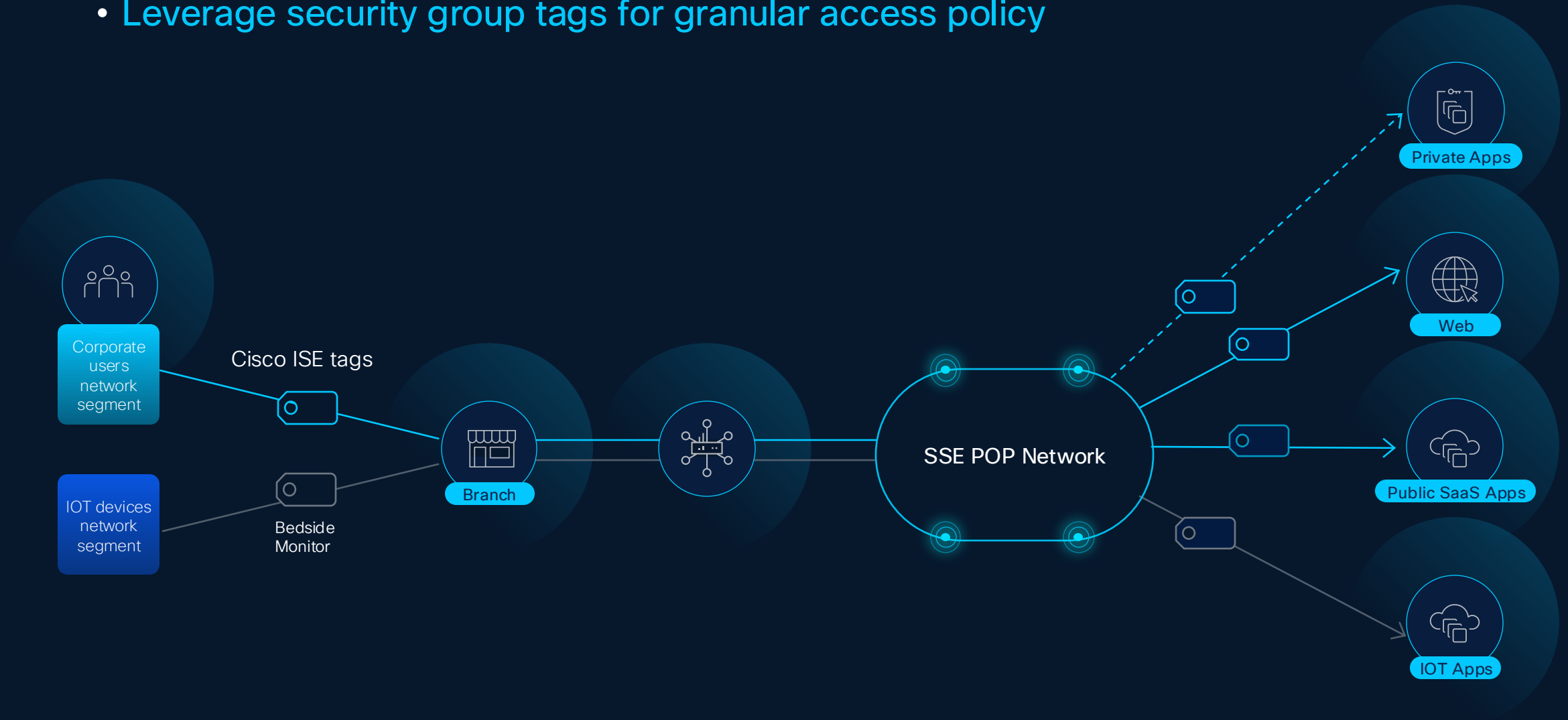
cisco


Authenticate once.
Workday


Frustrate attackers,
not users.

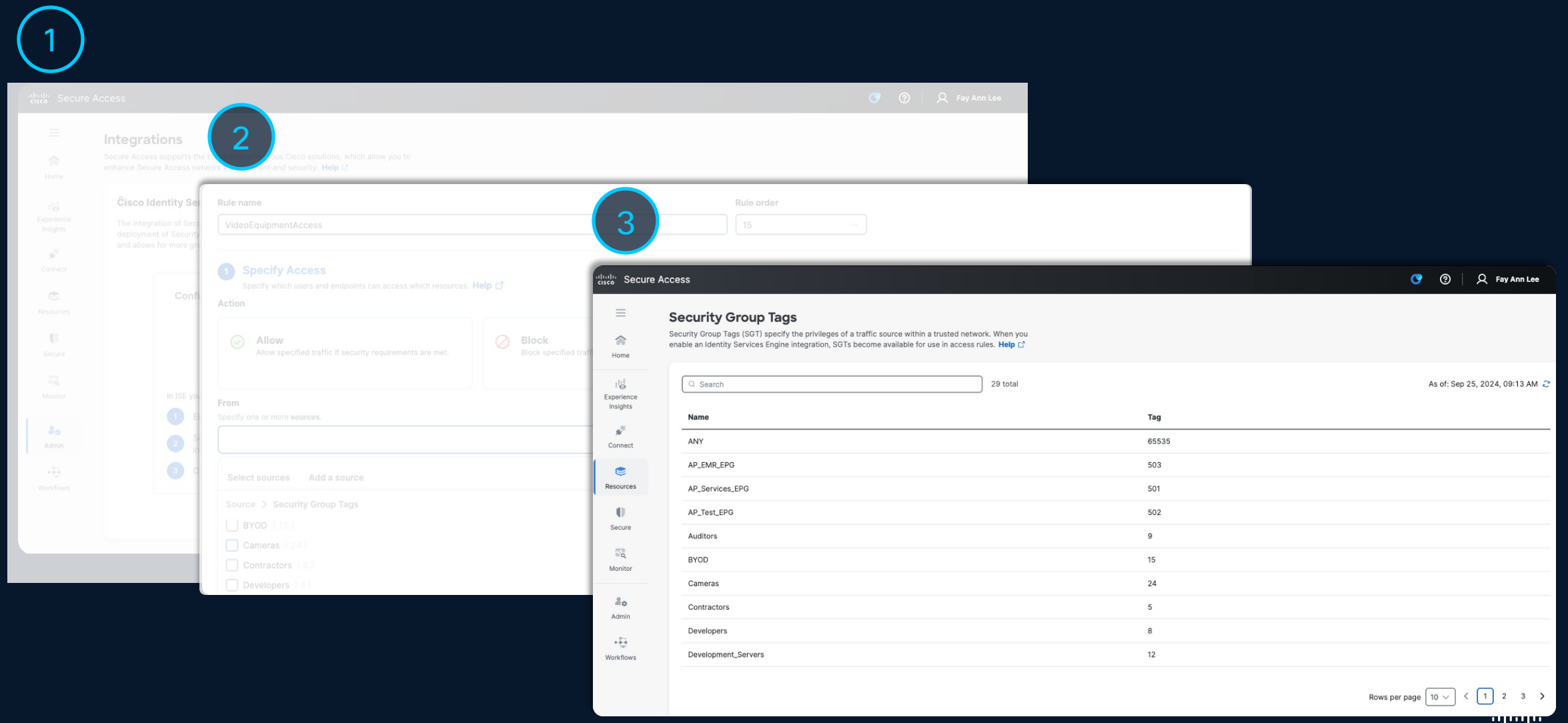
Enforce Zero Trust Using Identity Context

- Leverage security group tags for granular access policy



----- = Future

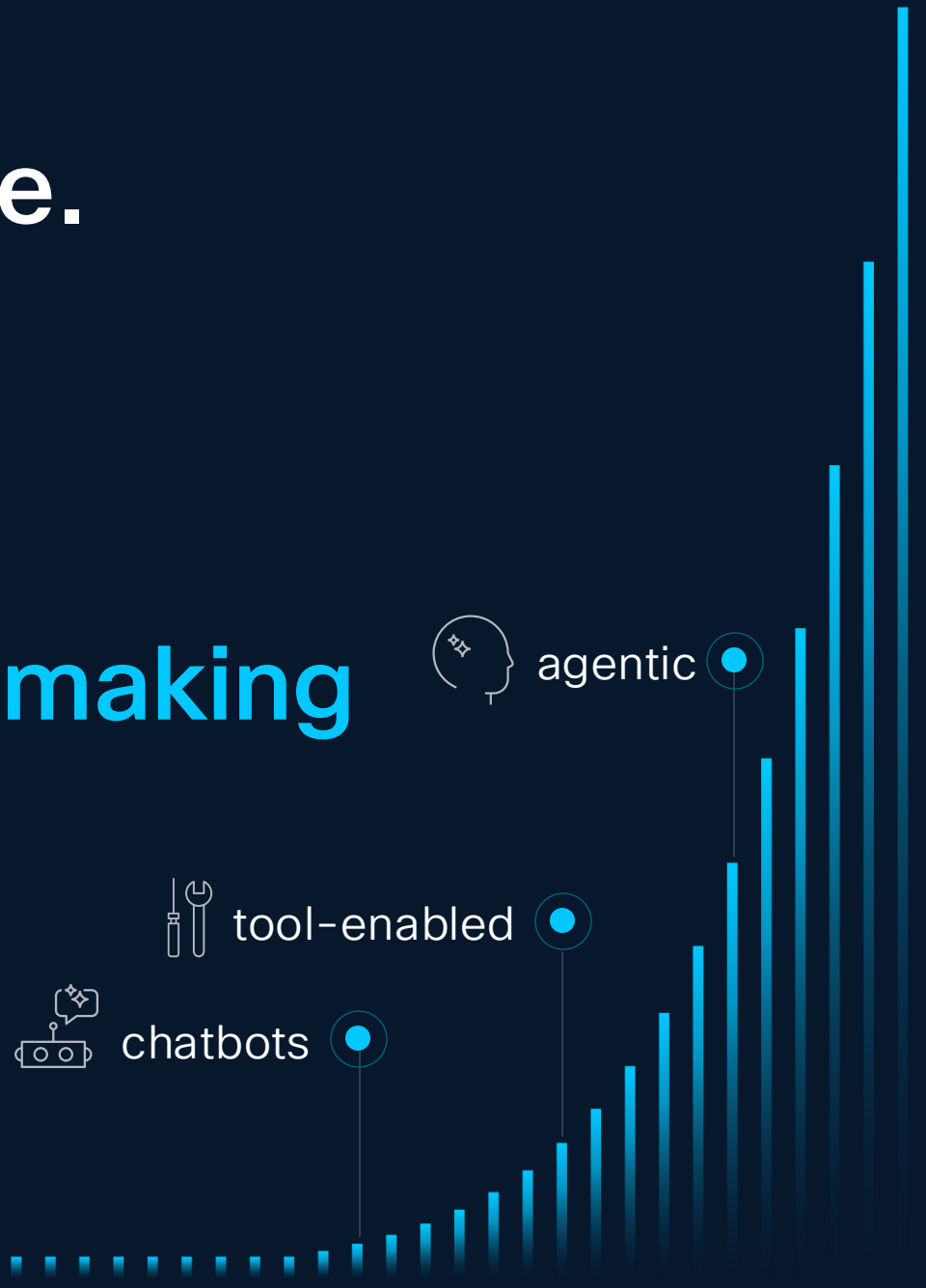
Security Group Tags (SGTs) Based Policy



Requires ISE and Cisco SD-WAN

AI is evolving at a rapid pace.

from static knowledge
to real-time knowledge
to autonomous decision-making



The Agentic Era Has Begun

Agentic AI Use Case

Source: Cisco Survey of Security and IT executives, January 2026, n = 224

The Agent Trust Gap

85%
Experimentation and adoption

Top concerns

- Access control
- Data exfiltration
- Unpredictable autonomy

5%
Production deployment

Source: Cisco survey of security and IT execs, Jan 2026, n=224
* Pilot, Limited Production, or Broad Production

cisco

Agents Are the ‘Worst Of Both Worlds’

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

Know Every Agent

Agent Discovery

Discover agents from various sources, monitor their lifecycle for posture or configuration issues, as well as possible risky behavior

Agent Directory

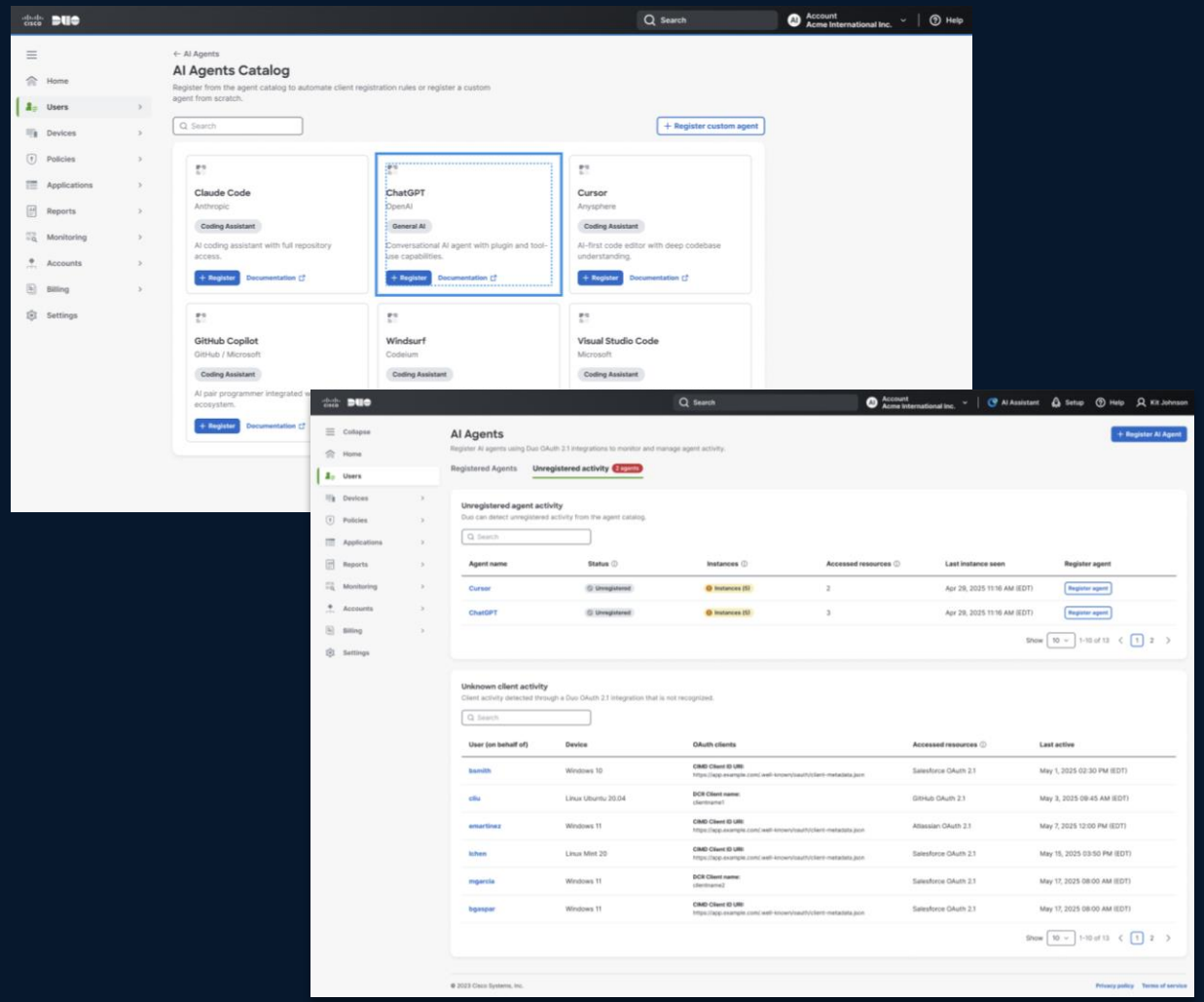
Create a directory with a list of agents, human owners, registration rules, tool access and agent activity logs

Agent Identity Lifecycle Management

End to end visibility and management into the agent lifecycle to reduce unwanted sprawl

Agent-Human Accountability

Have visibility and traceability into agent owners to manage accountability for agent actions



Agent Is Provided Just Long Enough Access Based

Access Token: 30 mins

Agent Access: Allowed

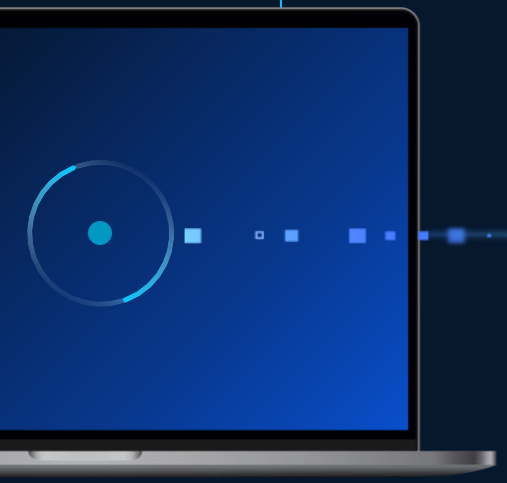
Prompt:

OpenClaw Run my build in Github

OpenClaw Agent | has build-only access | to development code in | Github

OpenClaw runs the build and returns no errors;

Build successful



Agent

Secure Access Gateway

Github MCP Server

Tools & Resources (DevOps Pipeline)

Depictions are examples only.

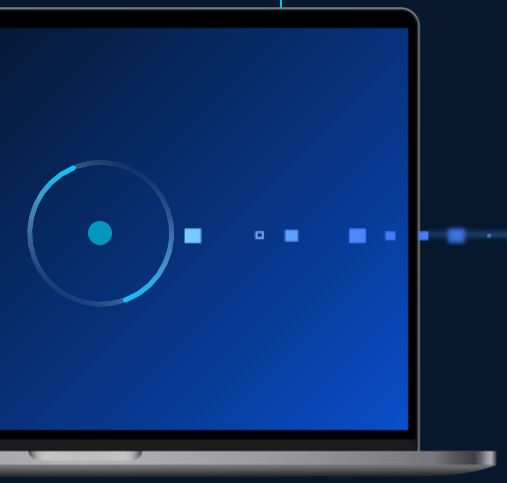
Agent Is Denied Access Token

Agent Access: Denied

OpenClaw tries to merge code in production

OpenClaw Agent | has build-only access | to production code in | Github

Agent is not allowed to merge code in production



Agent

Secure Access Gateway

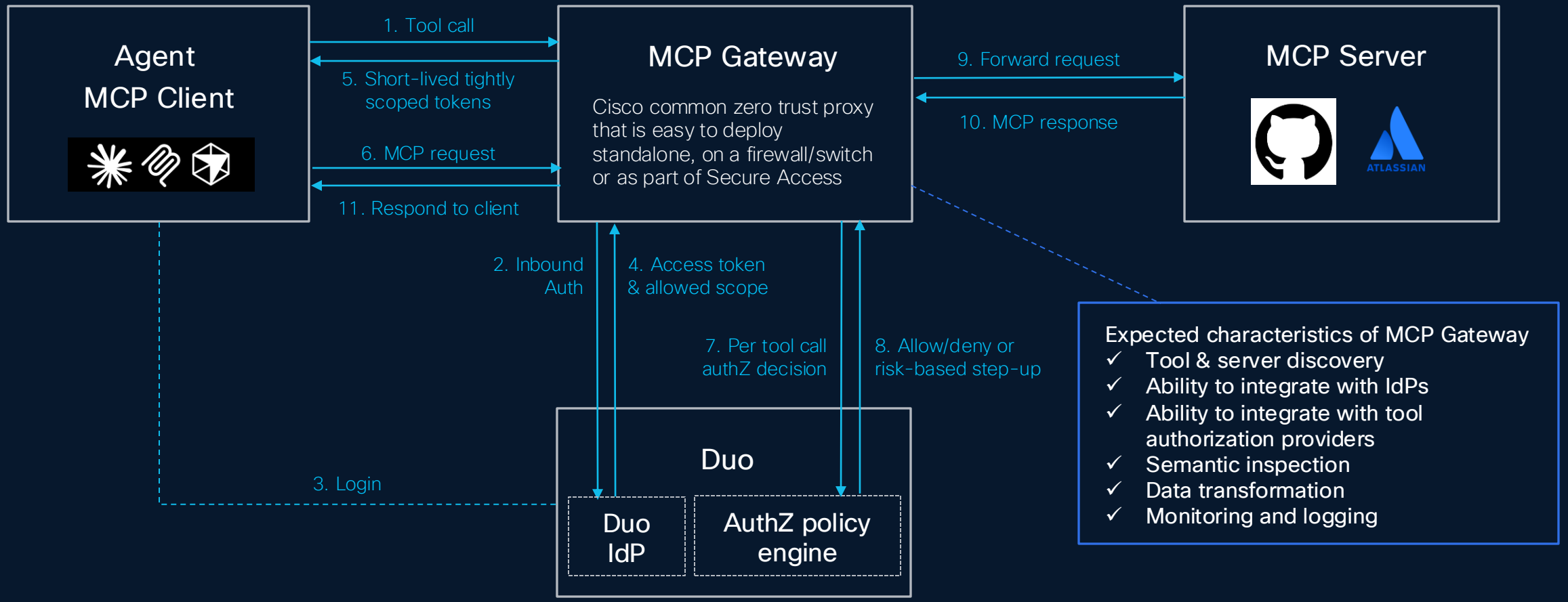
Github MCP Server

Tools & Resources (DevOps Pipeline)

Depictions are examples only.

Vision: Cisco's Unique Strength in Identity + Networking

Duo IAM + MCP Gateway



Example:
A user running Claude Desktop locally that connects to GitHub's MCP server for repository access

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

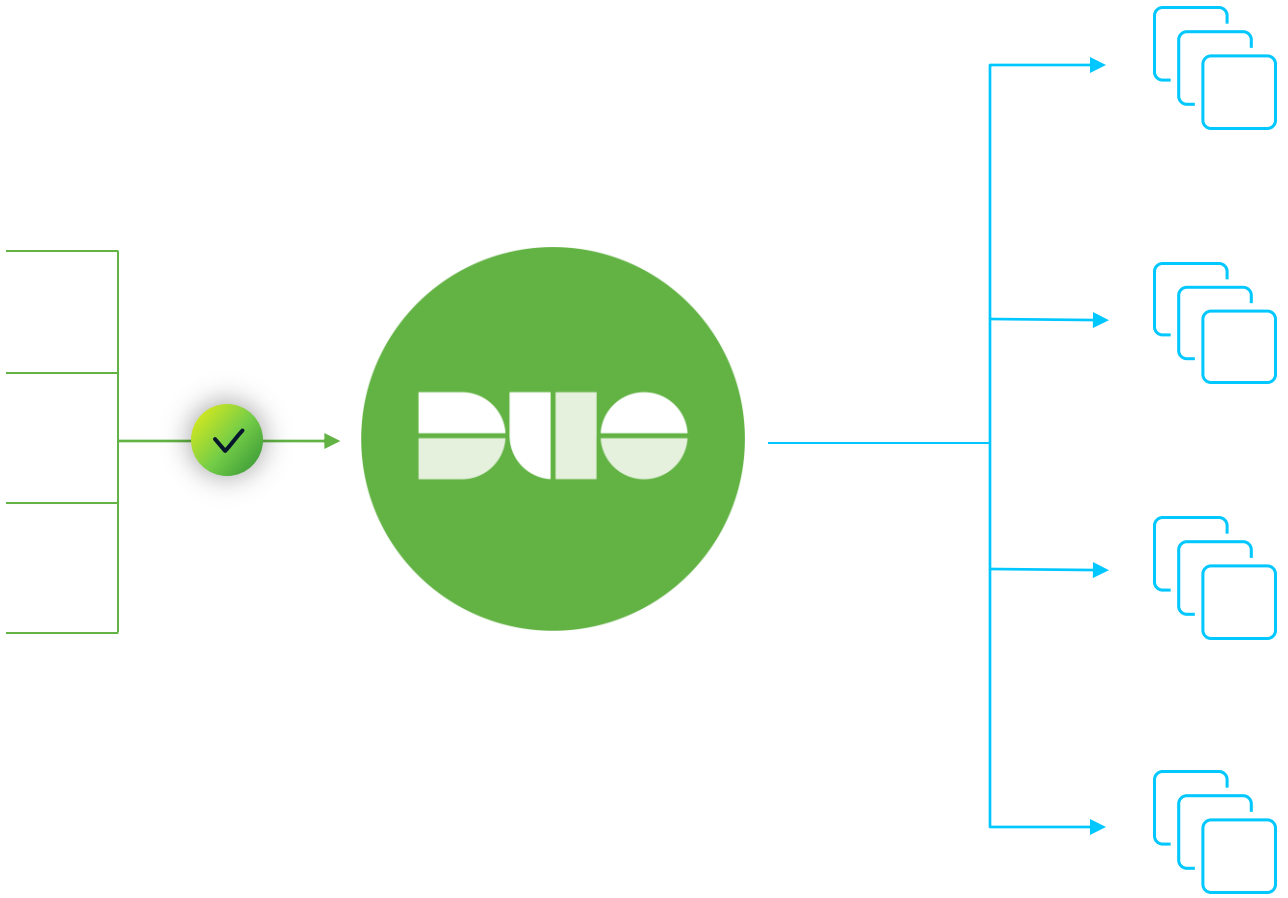
- Interruptions/slowdowns impede productivity
- Problem detection/ remediation is not fast enough
- Policy changes create unintended consequences

Need zero downtime

Standalone IAM
when required

Identity broker
for existing IAM

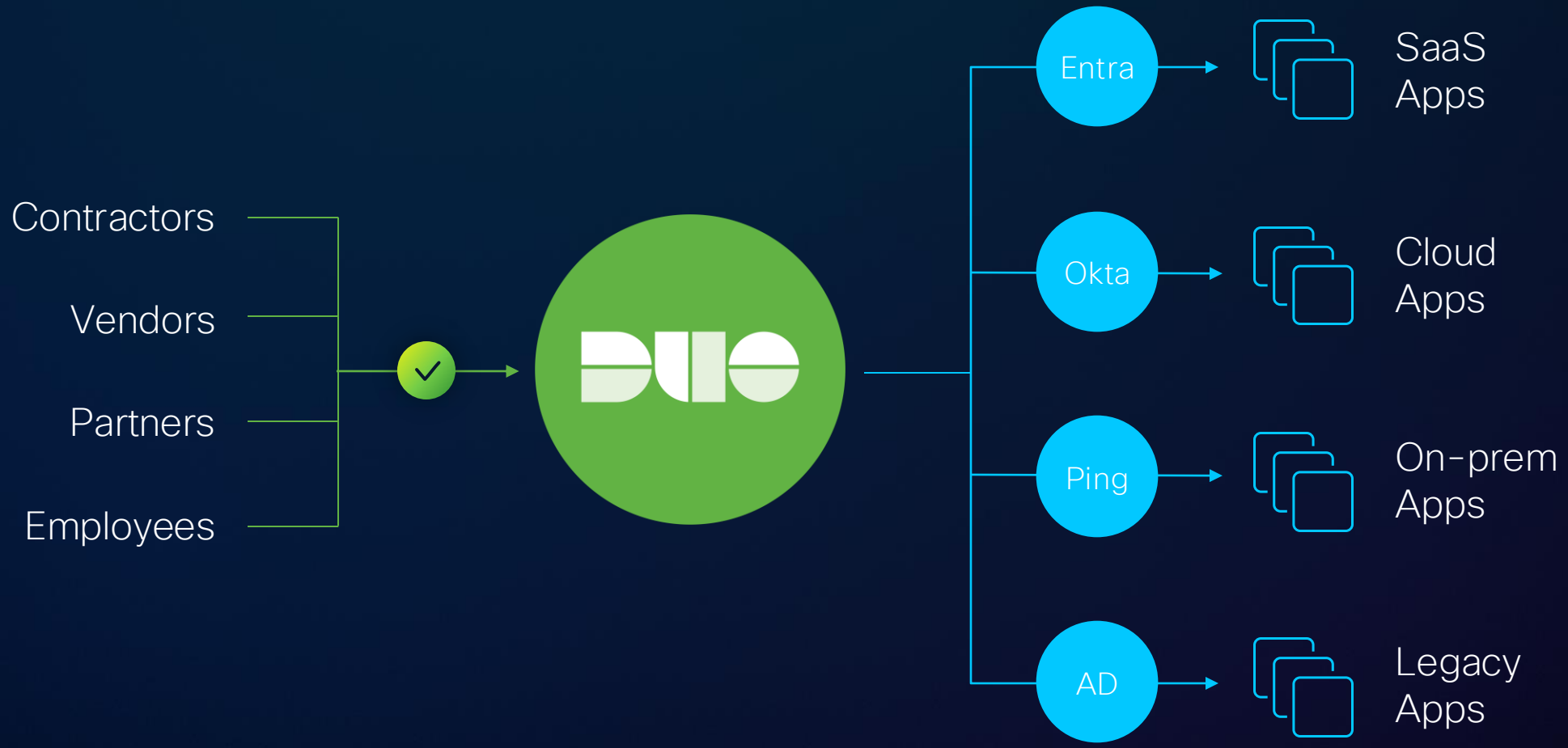
Alternate directory for
third-party users



Standalone IAM when required

Identity broker for existing IAM

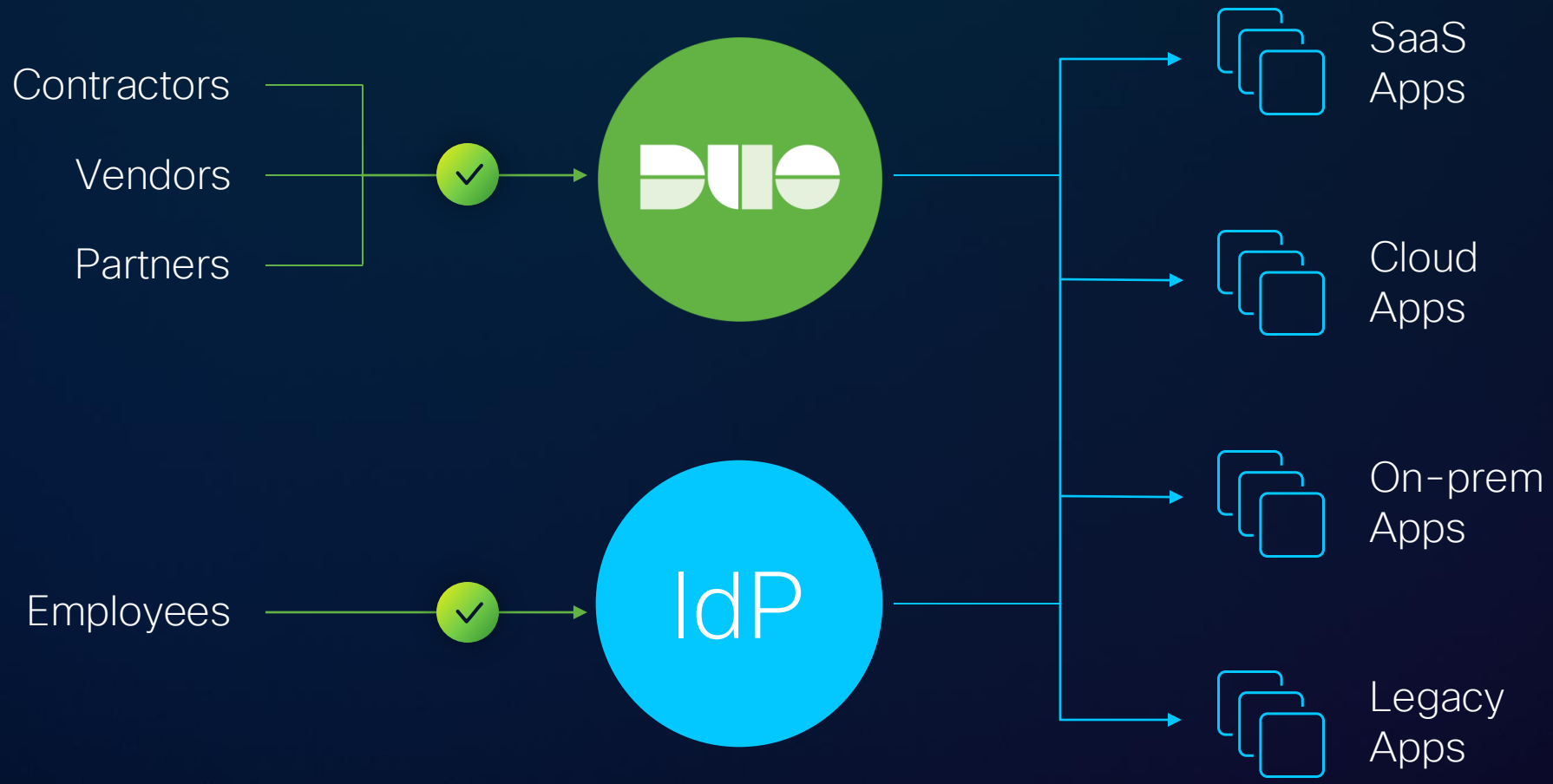
Alternate directory for third-party users



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