

Transforming Secure Connectivity for the AI-Ready Enterprise

Brandon Gordon, Security Solutions Engineer



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

<https://cs.co/connect-uztna>

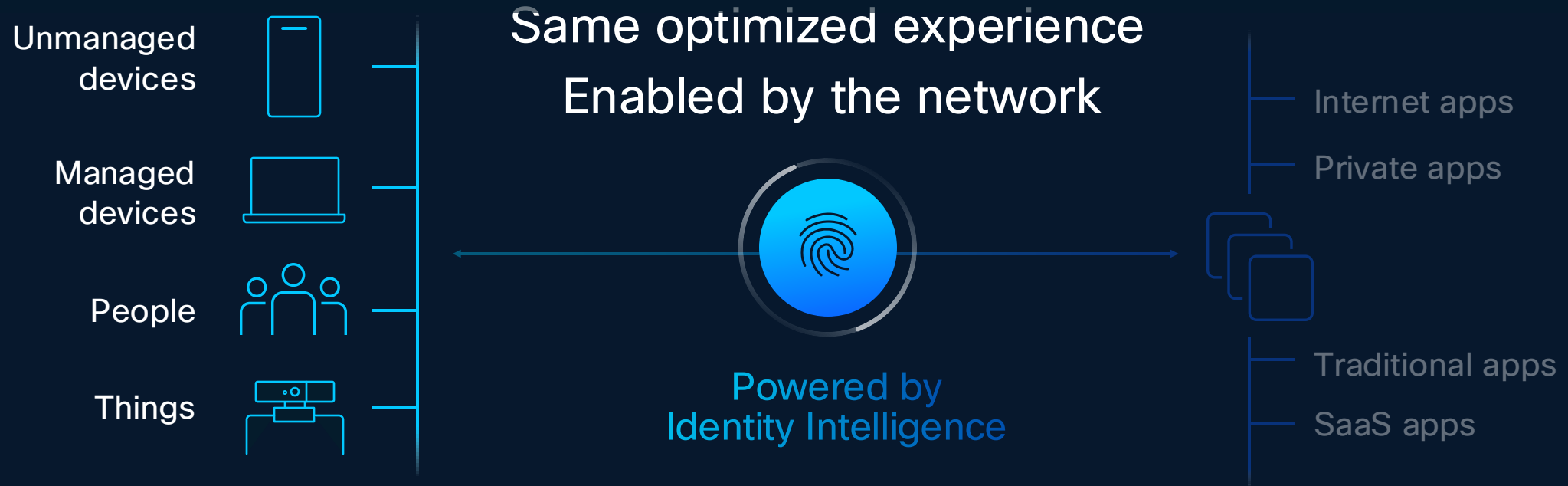
slido



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 Universal ZTNA

Takes ZTNA to users and **devices**

SD-WAN

+

Security
Service Edge

+

Identity
Trust

Cisco SASE

End-to-end Assurance with ThousandEyes
Talos Threat Intelligence

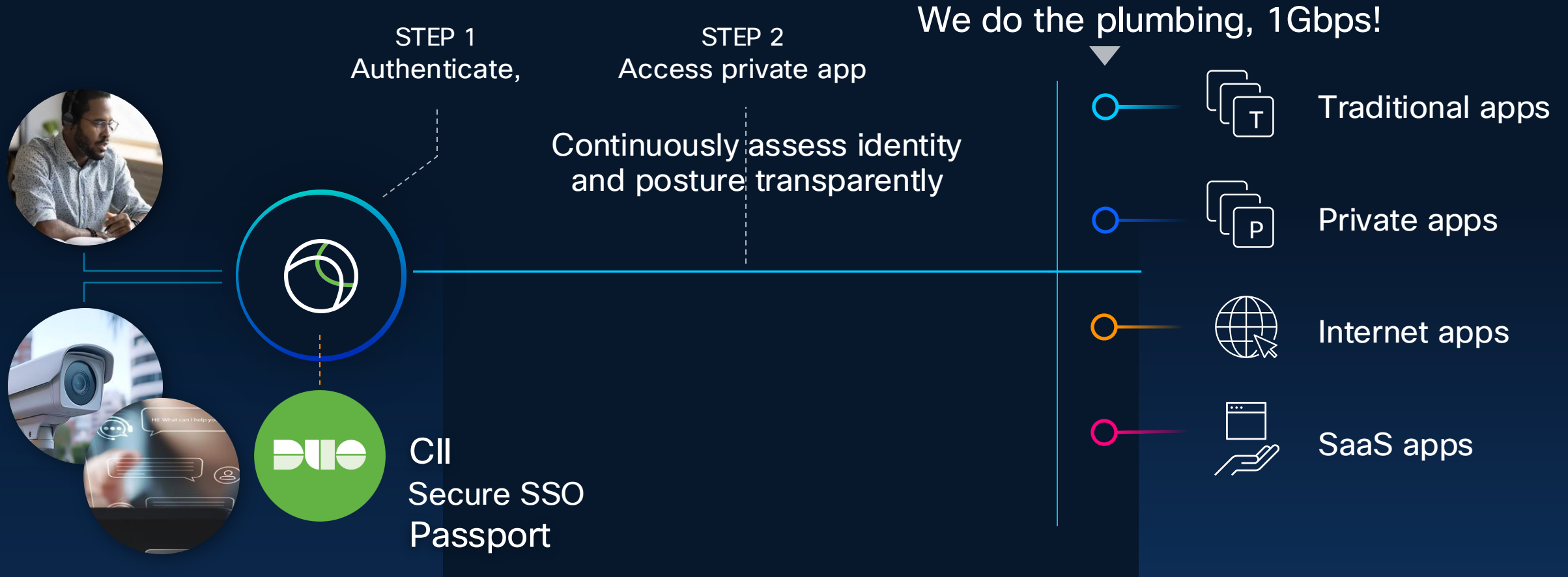
<https://cs.co/connect-uztna>

slido

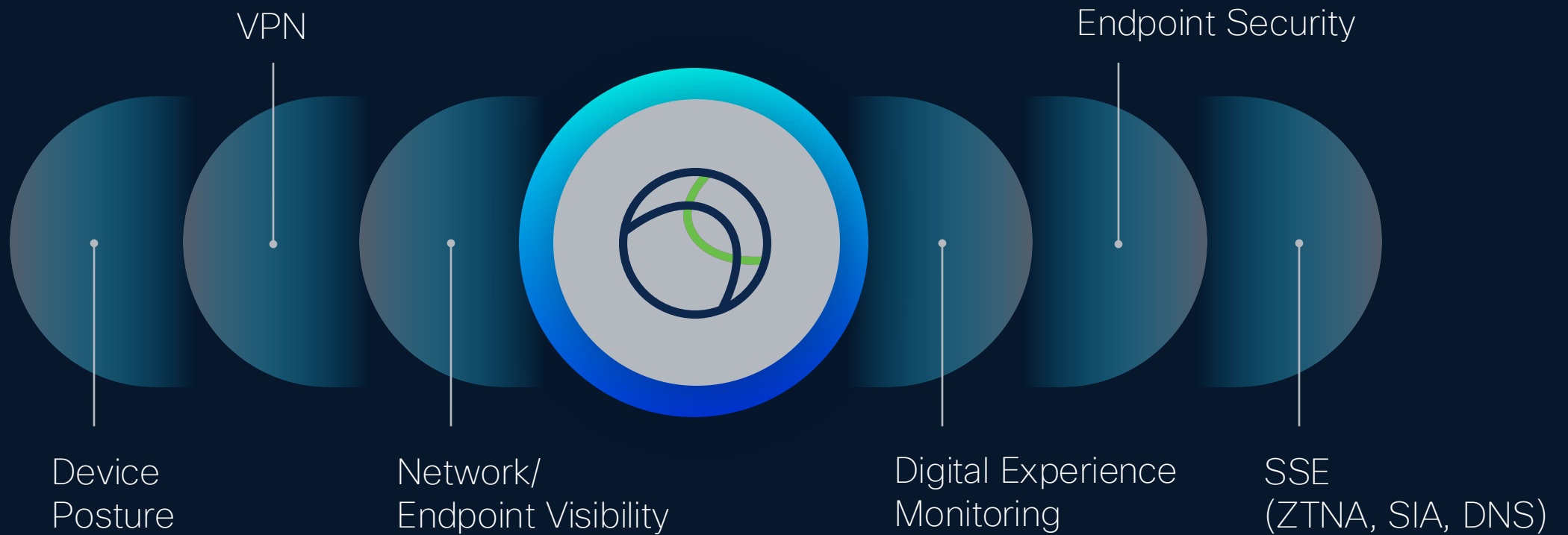


Seamless Access for All Applications

Zero Friction: Transparent UZTNA



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.

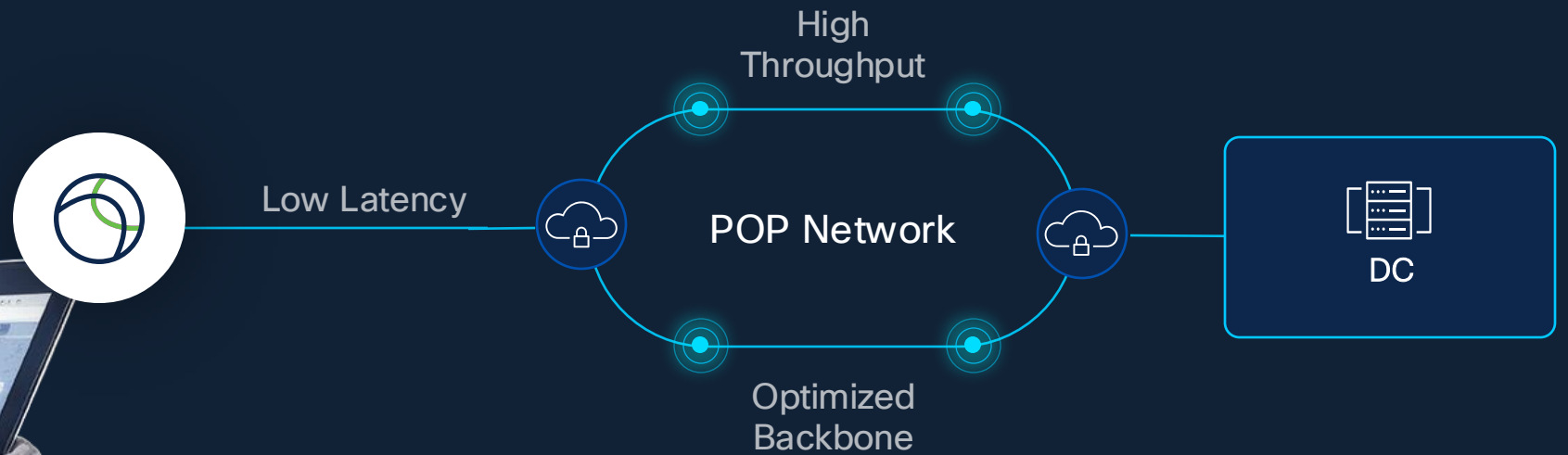


Universal ZTNA

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

Cisco'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



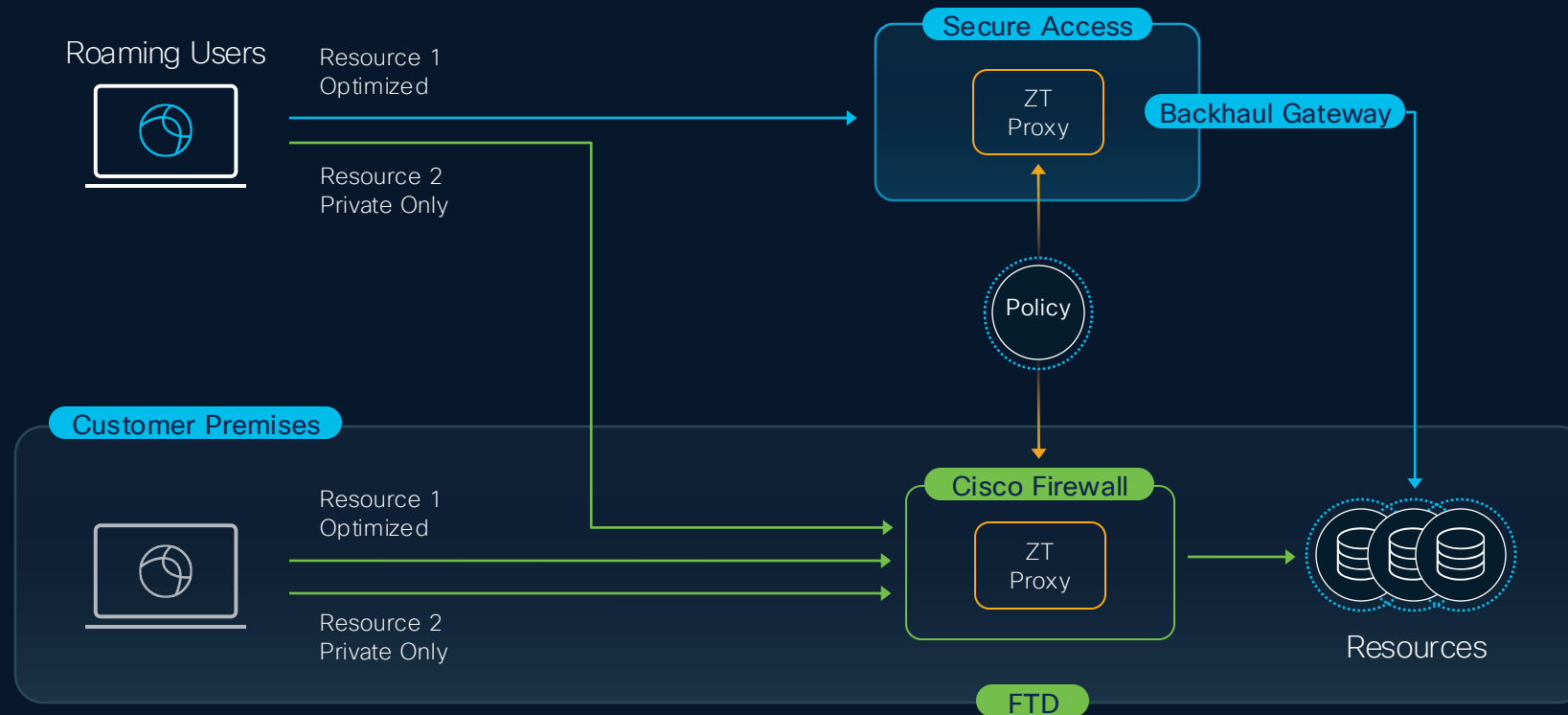
Cisco Secure Firewall Threat Defense

Advanced threat protection for a secure network

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

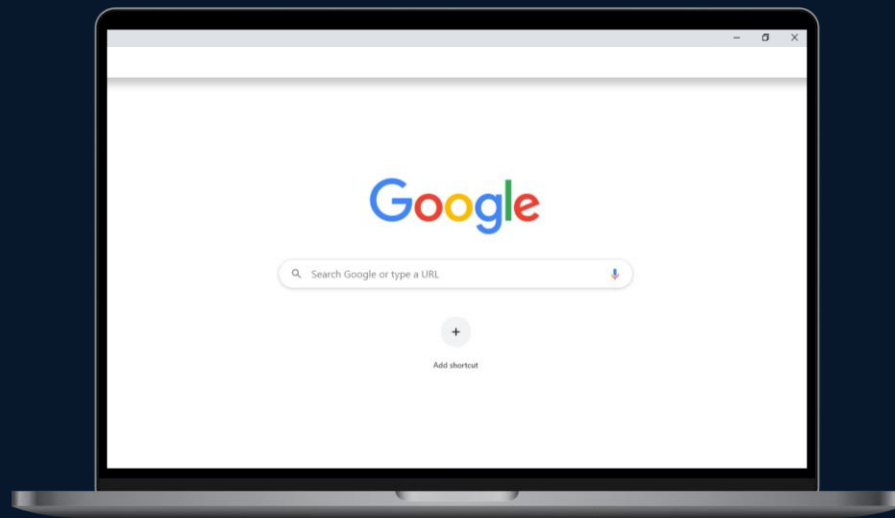
Hybrid Private Access for Flexible Enforcement

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



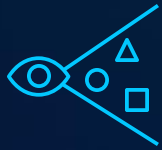
Chrome Enterprise Browser



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

Application name	Risk score	First detected
AI Assistant New	High	Dec 29, 2024
Code Copilot New	High	Dec 14, 2024
HelperAI	High	Nov 22, 2024
AI Creator	High	Nov 21, 2024
GrammarAI	Medium	Nov 13, 2024
WriterBot	High	Oct 30, 2024

Advanced AI/ML
DLP controls

Data Classification Name: AI/ML Monitor

Description (Optional):

Included Data Identifiers:

- Source Code
- Source Code (ML)

Include Data Identifiers:

Select Boolean Operator:

OR AND

Built-in Data Identifiers:

ABA Routing Number (US)

Aggressive Behavior

Enforce guardrails for AI queries:
Security, Privacy, Safety

Secure Access

287 Top Events: Showing events from Jan 1, 2025 at 00:00:00 to Feb 1, 2025 at 00:00:00

Event Type	Severity	Priority	Destination	File Name
Blocked	High	Critical	Blocked	File Name
Blocked	High	Critical	Blocked	File Name
Blocked	High	Critical	Blocked	File Name
Blocked	High	Critical	Blocked	File Name
Blocked	High	Critical	Blocked	File Name
Blocked	High	Critical	Blocked	File Name
Blocked	High	Critical	Blocked	File Name
Blocked	High	Critical	Blocked	File Name
Blocked	High	Critical	Blocked	File Name
Blocked	High	Critical	Blocked	File Name

Classification

Safety guardrail

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

1200+
AI Apps
Protected

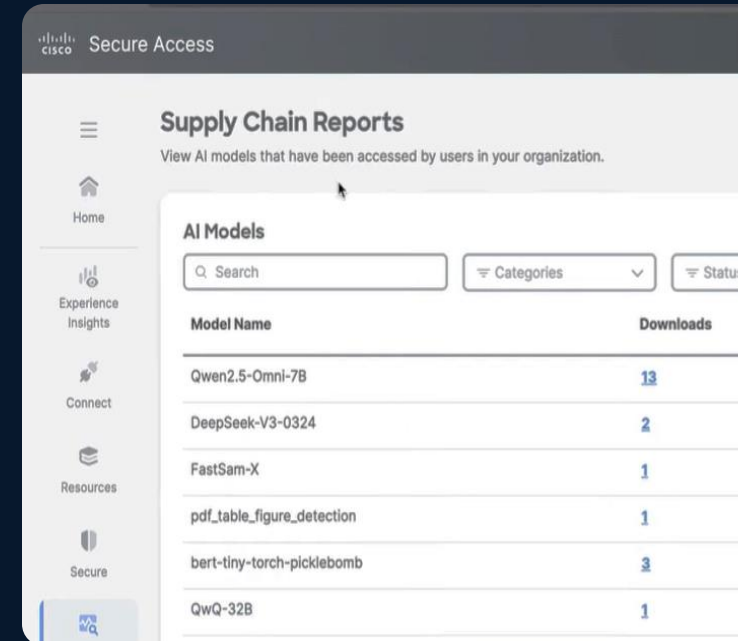
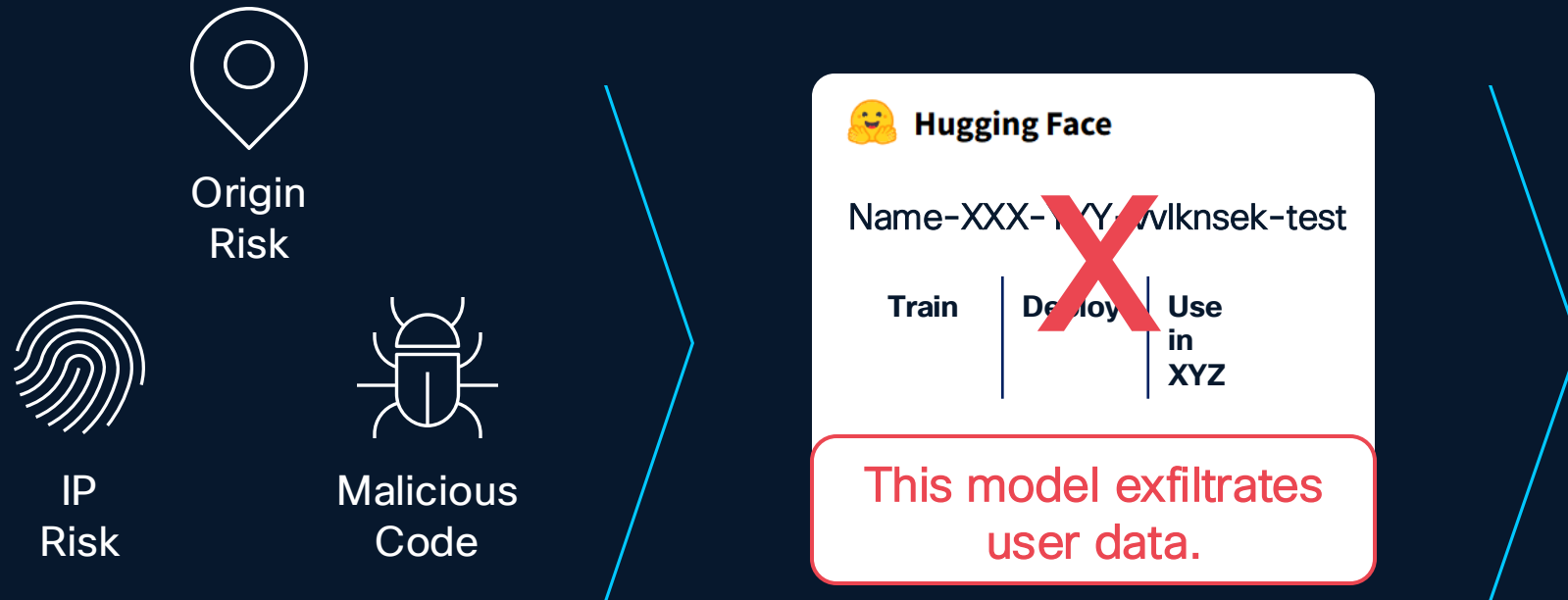
100%
Guardrails for
top AI Apps

1
Unified Security
Platform

Zero Blind Spots: Secure Access for AI Developers

AI supply chain and risk management

Allow visibility & responsible usage of Hugging Face Models



Demo – AI Access and AI Supply Chain Risk

- Home
- Experience Insights
- Connect
- Resources
- Secure
- Monitor
- Investigate
- Admin
- Workflows

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](#)

Connectivity

Last 24 Hours

Network tunnel groups 2 total

1 Warning 

1 Connected 

Resource connector groups 1 total

1 Connected 


Data Transfer

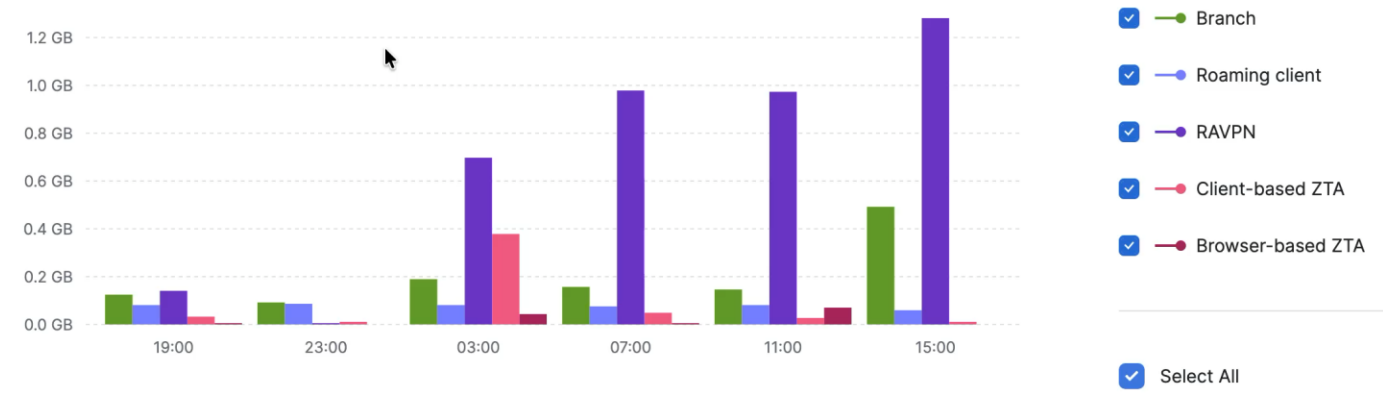
Last 24 Hours

Total Usage
Usage data - delayed up to 30 min.

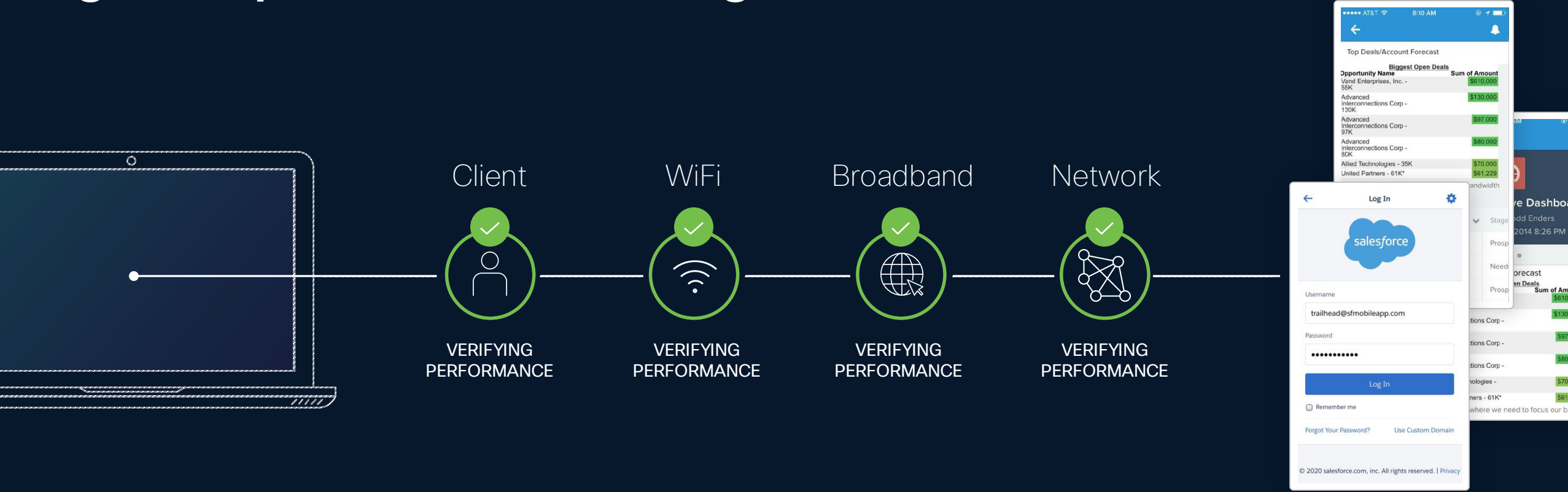
Total traffic
6.36 GB
9.22 GB  Decrease (last 24 hours)

Received
836.82 MB
775.83 MB  Decrease (last 24 hours)

Sent
5.52 GB
8.45 GB  Decrease (last 24 hours)



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

The screenshot displays the Cisco Secure Access Experience Insights dashboard. The page title is "Experience Insights" with a "read-only" indicator. Below the title, there is a brief description: "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".

The main content area features an "Endpoints summary" section with two cards:

- Number of endpoints 4 total**: 3 Online (blue dot icon)
- Health status**: 0 Unhealthy (red dot icon), 1 At Risk (yellow triangle icon), 1 Healthy (green checkmark icon)

Below the summary is a world map showing the locations of endpoints. Two blue circles with the number "1" are placed over the United States and Mexico. A legend above the map indicates: All (blue), Unhealthy (red), At risk (yellow), Healthy (green).

At the bottom of the map area, there are search filters: "Search by user name", "Select location", and "Select health status".

Below the map is a table with the following columns: User name, Location, Health status, Device name, Latency, Jitter, Loss, WiFi, Ethernet, CPU, Memory, OS, and Test time. The table contains one row of data:

User name	Location	Health status	Device name	Latency	Jitter	Loss	WiFi	Ethernet	CPU	Memory	OS	Test time
Carol Freeman	Wichita, Kansas, US	Healthy	PSEUDOCO-DESKTO	23 ms	0 ms	0.00%	—	1000 Mbps	0.39%	17.76%	Microsoft Windows 11	Sep 12, 2024 2:30PM

Identity Intelligence

<https://cs.co/connect-uztna>

slido





60
percent

of breaches
leveraged identity
as a key component

Cisco Talos Incident Response | Year in Review 2025

Attackers Expect You to Have MFA

Brute-force or password spray



Enrollment

MFA bypass



OS login



App login

Stolen session cookies



Mid-Session



Helpdesk

Physical access to device

Fallback to less secure MFA method

Deepfake social engineering at help desk

INTRODUCING

Duo Identity & Access Management (IAM)



Duo IAM

Security-First
Identity

End-to-End
Phishing Resistance

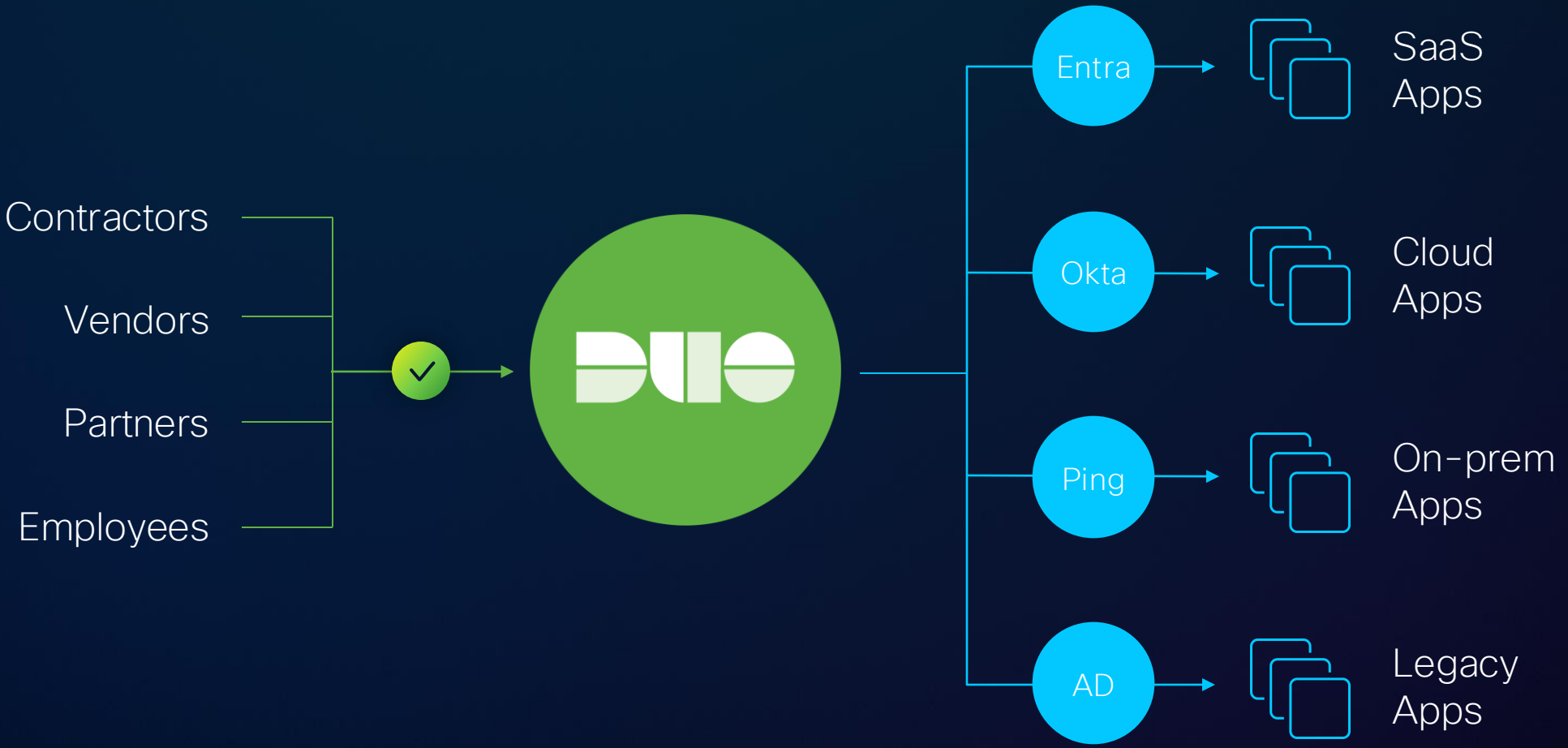
Unified Identity
intelligence

World-class user experience

Standalone IAM
when required

Identity broker
for existing IAM

Alternate directory for
third-party users



Duo IAM

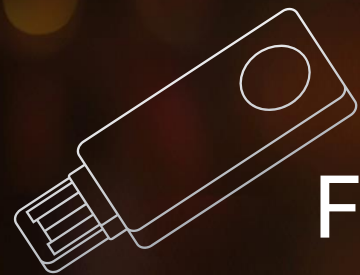
Security-First
Identity

End-to-End
Phishing Resistance

Unified Identity
intelligence

World-Class User Experience

End-to-End Phishing Resistance



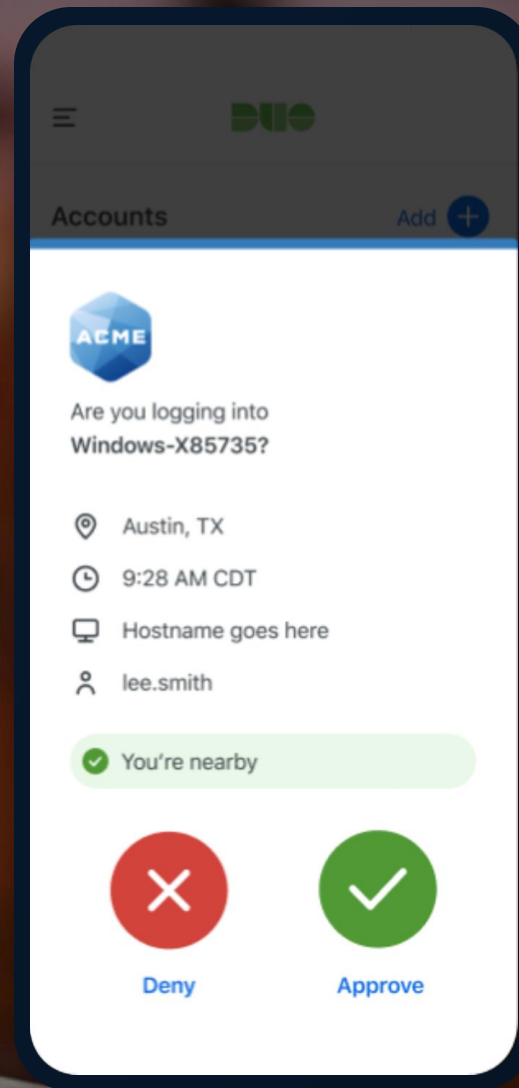
FIDO2, Hardware
Tokens

End-to-End Phishing Resistance

Proximity Verification



Bluetooth Low Energy (BLE)



Duo IAM

Security-First
Identity

End-to-End
Phishing Resistance

Unified Identity
Intelligence

World-Class User Experience

SailPoint

Dragos

Crowdstrike

Salesforce

Okta

PingIdentity

Cisco ISE

Auth0

Cyberark

Microsoft

Google

Amazon

Cisco Identity Intelligence



USERS



MACHINES



SERVICES



HRIS



DATA



APPS



PLATFORMS



SailPoint

Dragos

Crowdstrike

Salesforce

Cisco ISE

Okta

PingIdentity

Auth0

Microsoft

Google

Cyberark

Amazon

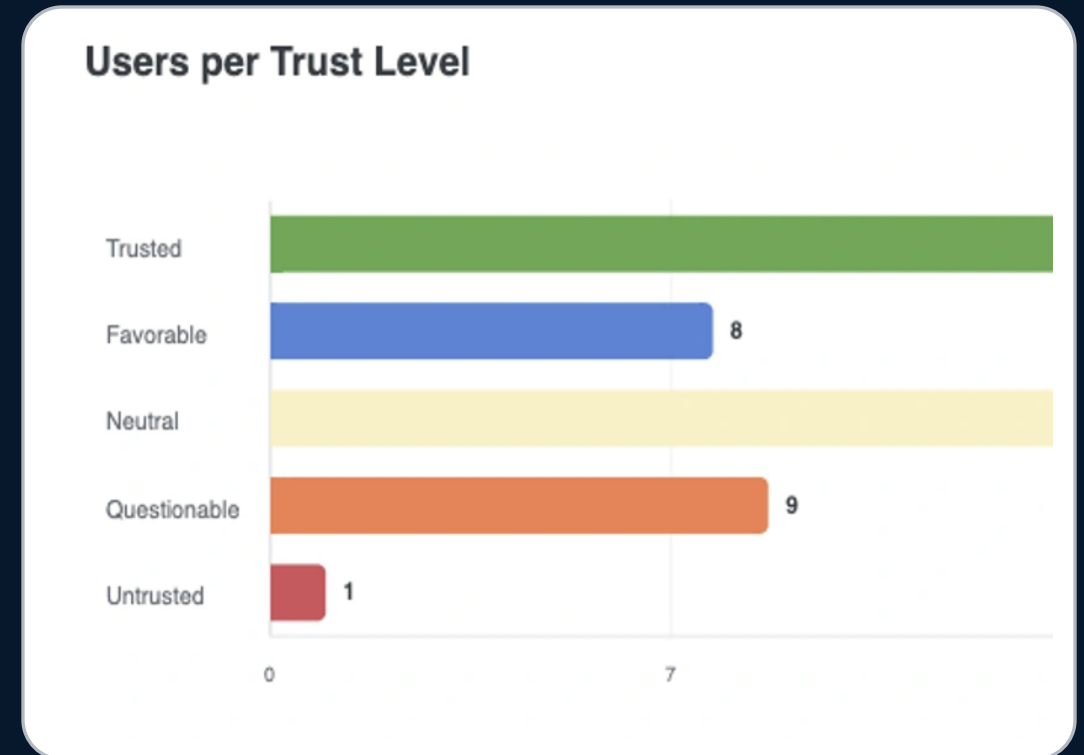
Zero Imposters: Identity-Based User Trust Level

- 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

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



Take actions to improve your posture

Recommended Actions

- Remove users who should not be present, or add users to HRIS if needed
- Require priority accounts to configure and actively utilize stronger MFA factors
- Require priority accounts to configure and utilize any MFA factor

Failing Users

Failing Users	Severity
57	Critical
4	Critical
4	Critical

Identity Posture Trend

30d Feb 18, 2026 17:57 - Mar 20, ...



Cisco Secure Access Use Case

Duo IAM

Security-First
Identity

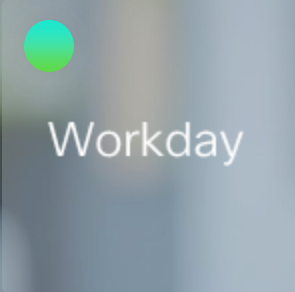
End-to-End
Phishing Resistance

Unified Identity
intelligence

World-Class User Experience



Authenticate once.



Frustrate attackers,
not users.

Enforce Zero Trust Using Identity Context

- Leverage security group tags for granular access policy



Security Group Tags (SGTs) Based Policy

1

The screenshot shows the Cisco Secure Access 'Integrations' page. A red circle highlights the 'Integrations' header. Below it, there is a description of the integration and a list of resources. A vertical navigation menu on the left includes Home, Experience Insights, Connect, Resources, Secure, Monitor, Admin, and Workflows.

2

This screenshot shows the 'Specify Access' configuration step. A red circle highlights the 'Rule name' field, which contains the text 'VideoEquipmentAccess'. To the right, the 'Rule order' is set to 15. Below the rule name, there are two action buttons: 'Allow' (with a green checkmark) and 'Block' (with a red X). The 'From' section is currently empty, with a 'Select sources' button and a list of available sources including BYOD (15), Cameras (24), Contractors (5), and Developers (8).

3

This screenshot shows the 'Security Group Tags' list page. A red circle highlights the 'Resources' menu item in the left navigation pane. The main content area displays a table of Security Group Tags with 29 total items. The table has columns for 'Name' and 'Tag'. The current page shows 10 rows.

Name	Tag
ANY	65535
AP_EMR_EPG	503
AP_Services_EPG	501
AP_Test_EPG	502
Auditors	9
BYOD	15
Cameras	24
Contractors	5
Developers	8
Development_Servers	12

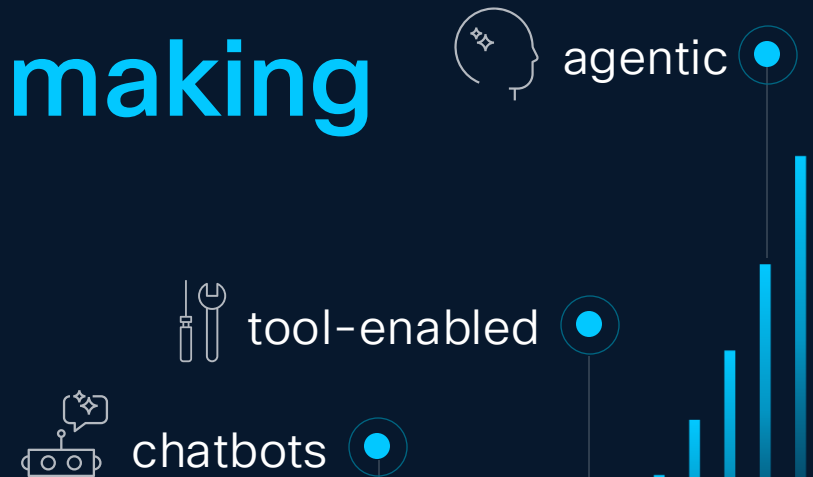


AI is evolving at a rapid pace.

from **static knowledge**

to **real-time knowledge**

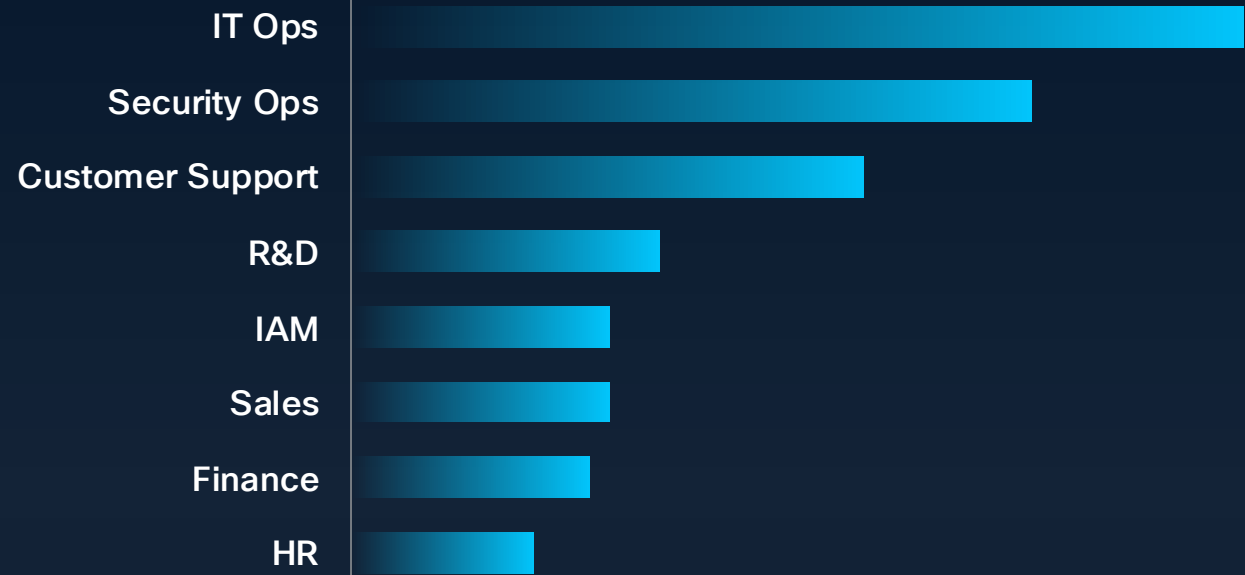
to **autonomous decision-making**



The Agentic Era Has Begun



Agentic AI Use Case

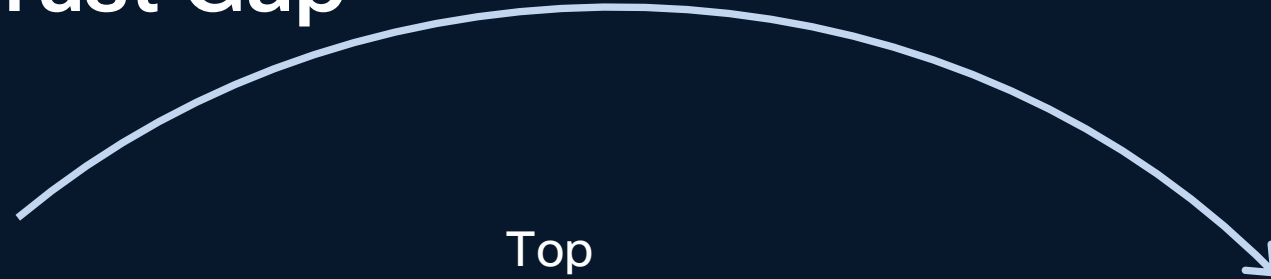


Source: Cisco Survey of Security and IT executives, January 2026, n = 224

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

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

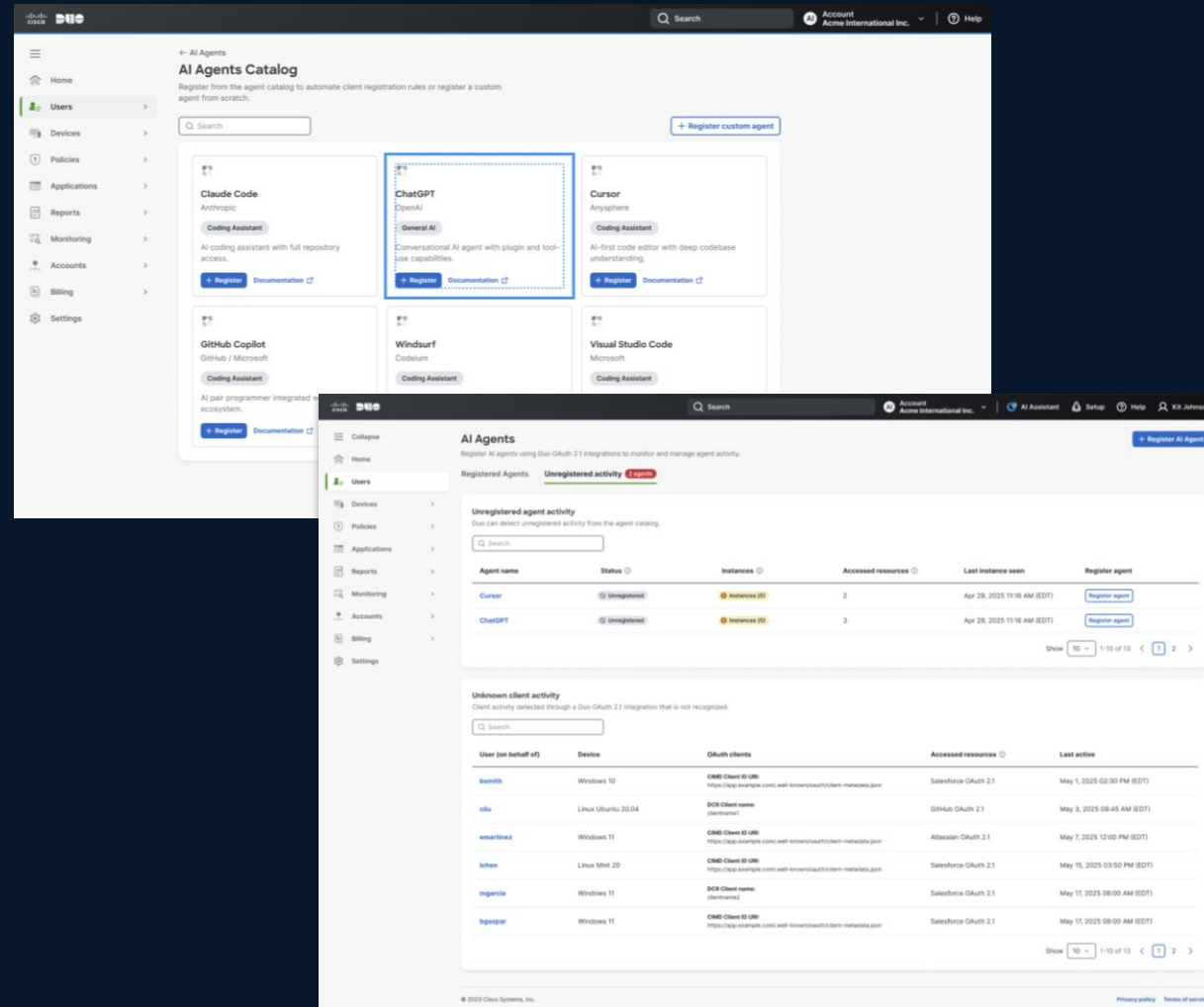
Create a directory with a list of agents, human owners, registration rules, tool access and agent activity logs

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

Tools &
Resources
(DevOps
Pipeline)

Agent

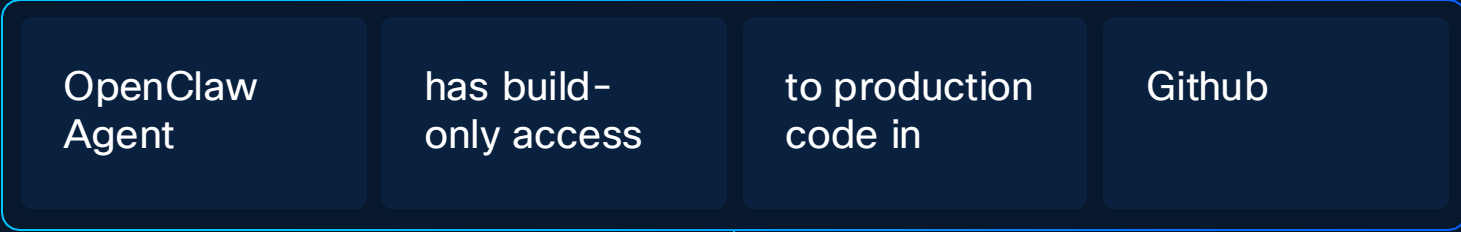
Secure Access
Gateway

Github MCP Server

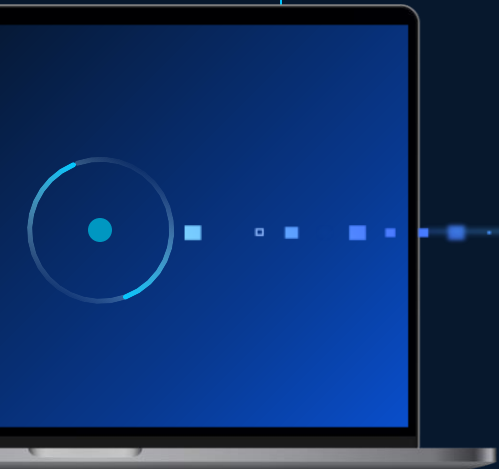
Agent Is Denied Access Token

Agent Access: **Denied**

OpenClaw tries to merge code in production



Agent is not allowed to merge code in production

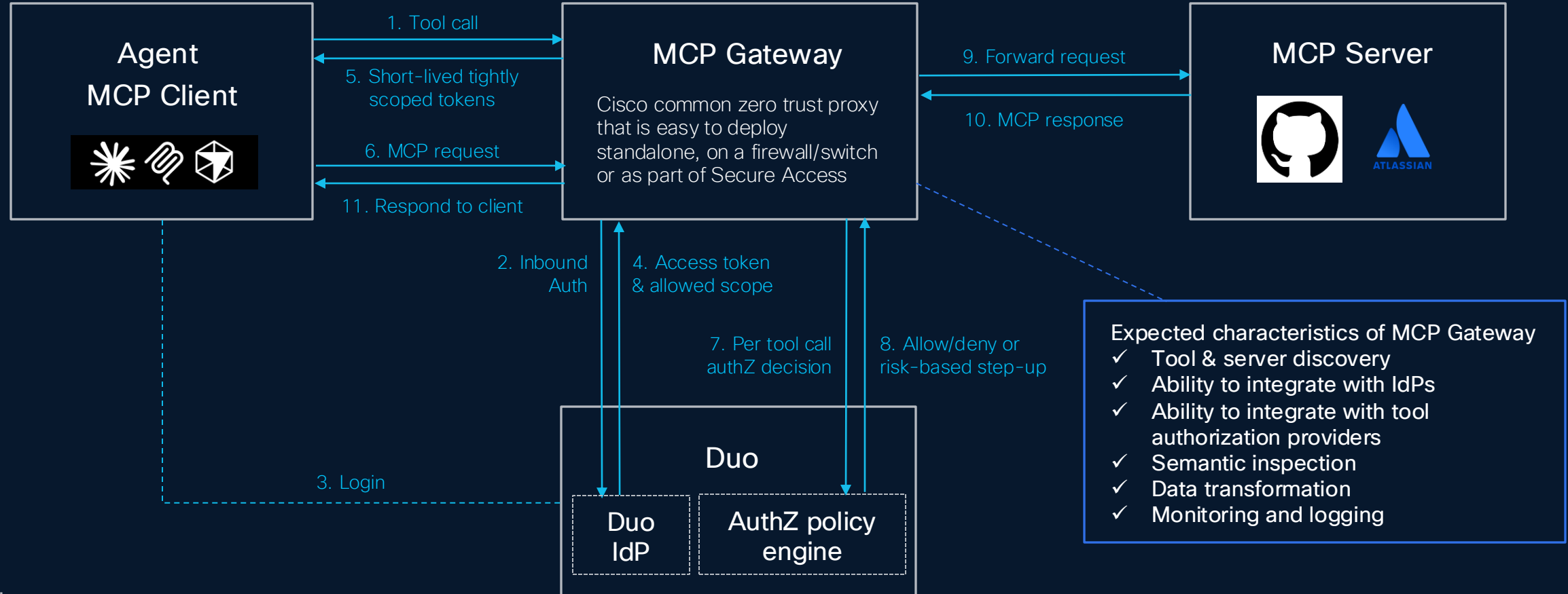


Tools & Resources (DevOps Pipeline)

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

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 Connect

Thank you





- 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

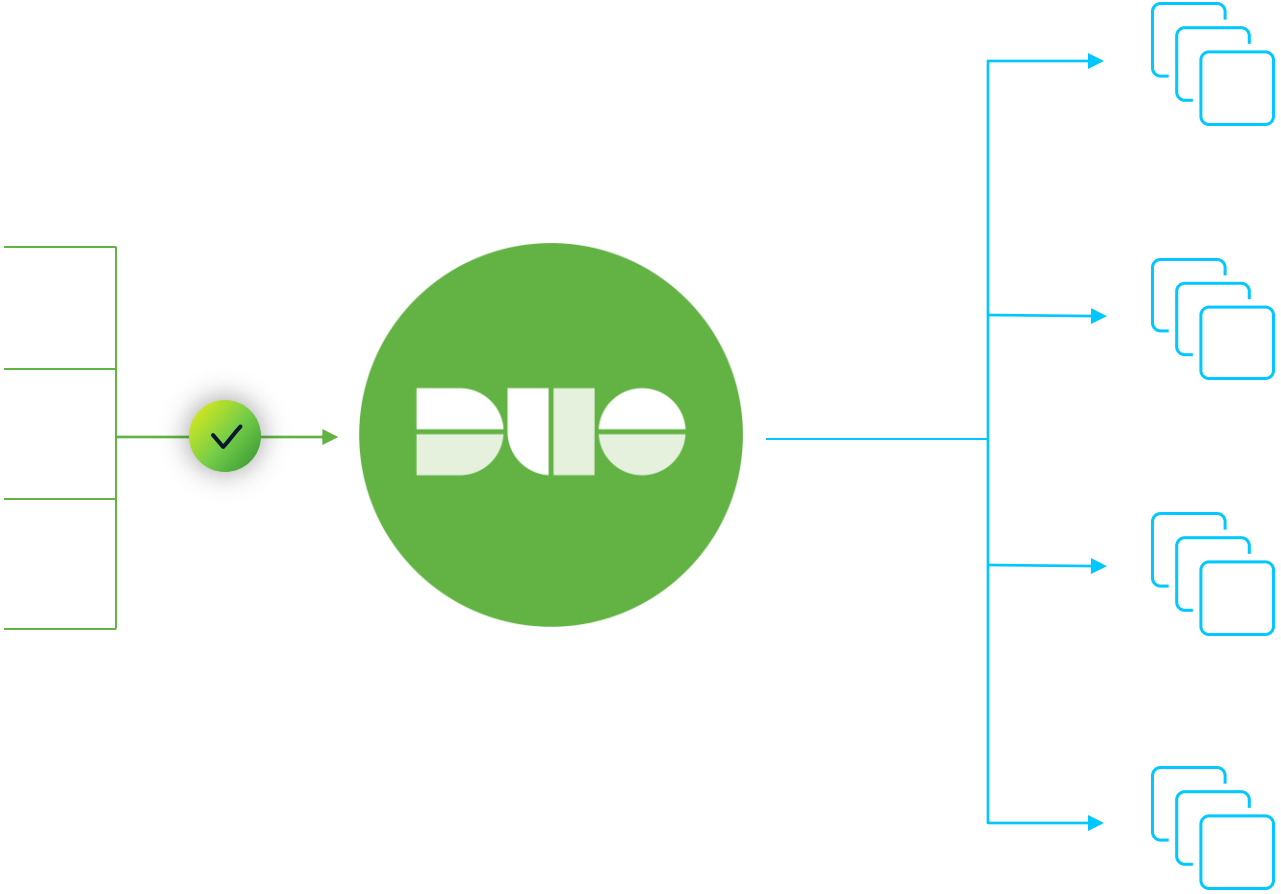
- Interruptions/slowdowns impede productivity
- Problem detection/remediation is not fast enough
- Policy changes create unintended consequences

Need zero downtime

Standalone IAM
when required

Identity broker
for existing IAM

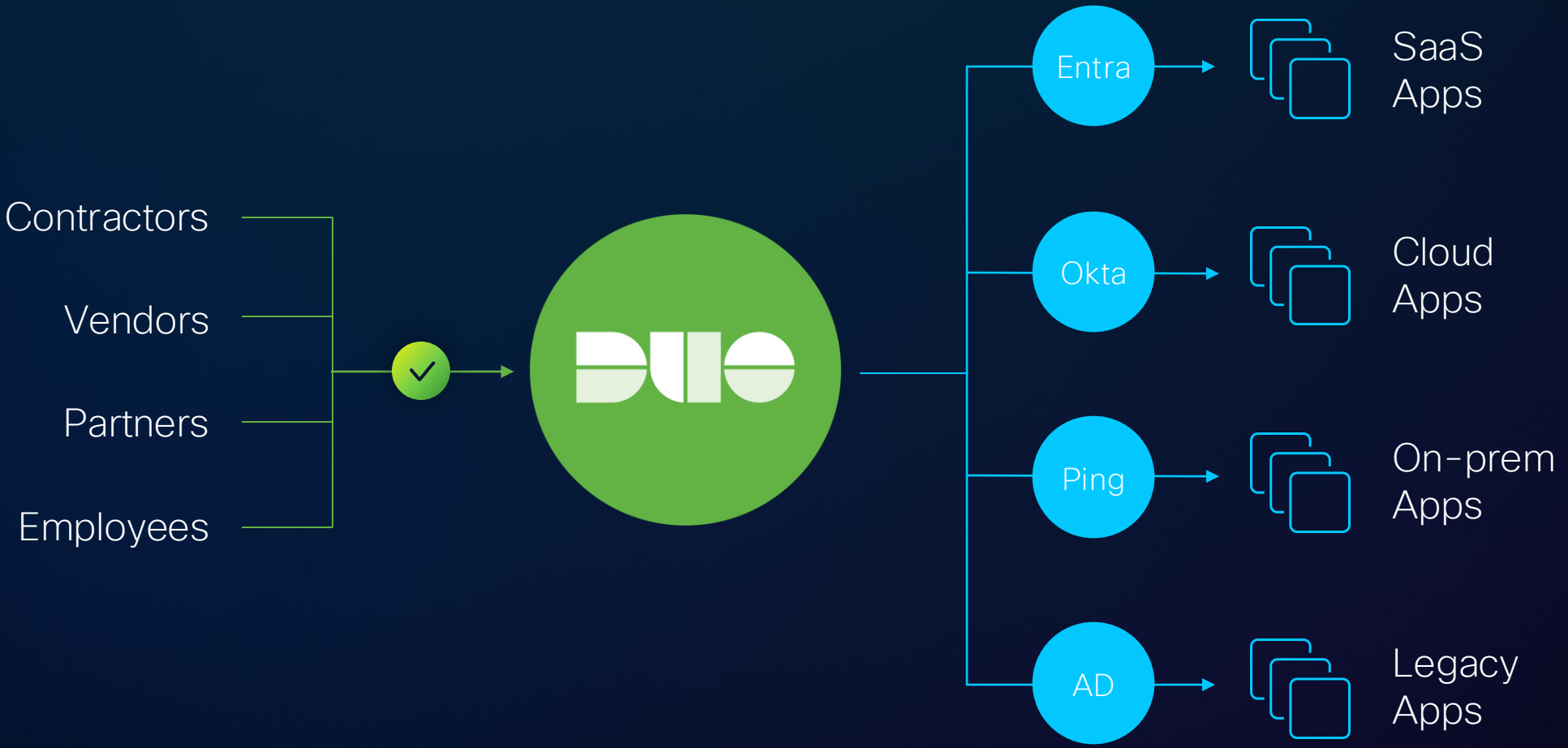
Alternate directory for
third-party users



Standalone IAM
when required

Identity broker
for existing IAM

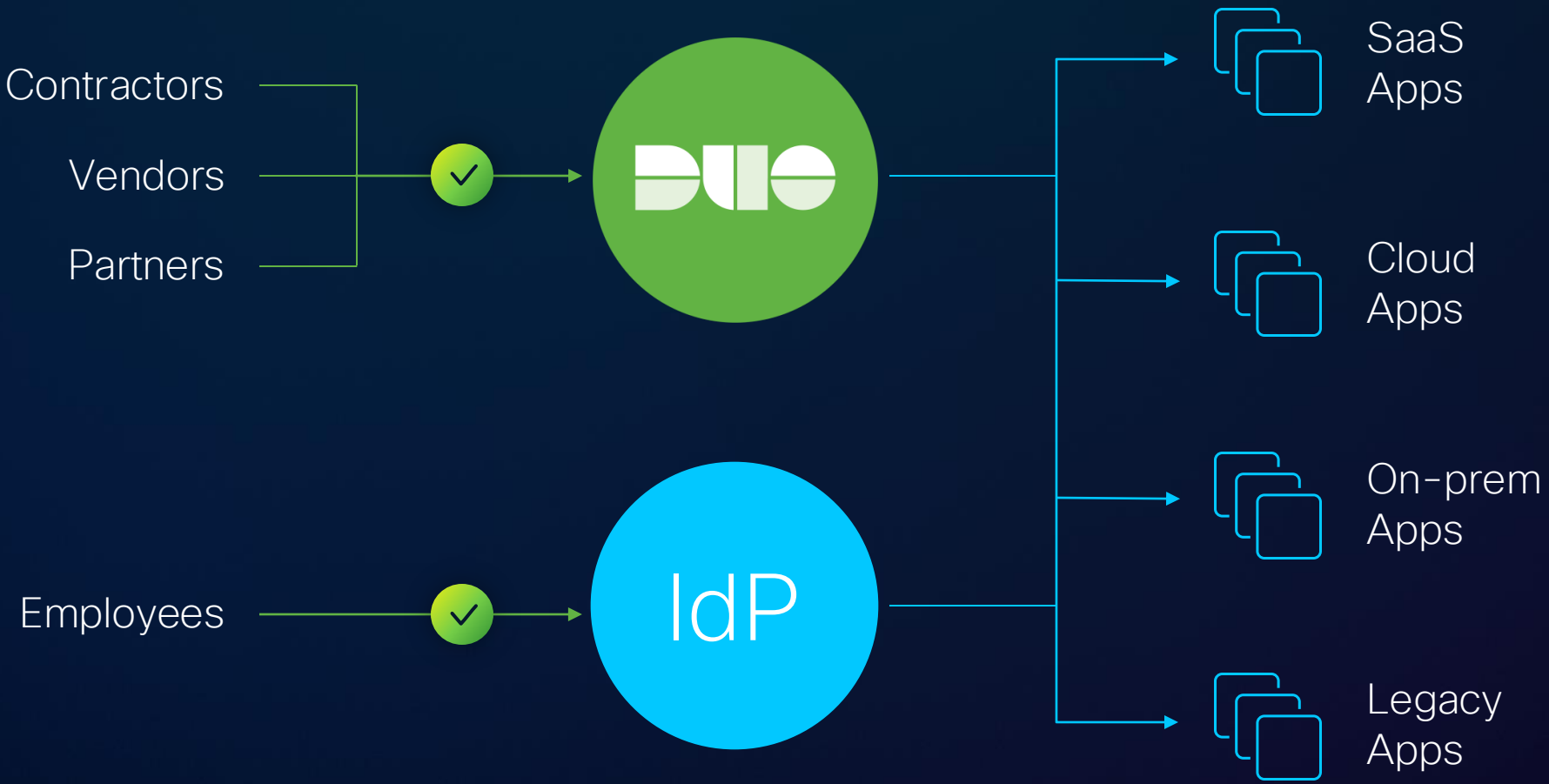
Alternate directory for
third-party users



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