

Modernizing Security With Cisco's SSE

Cloud-First SASE with Cisco's SSE Platform

JP Sanchez
Cybersecurity Solutions Engineer
U.S. Public Sector

Bill Allsup
Cybersecurity Solutions Engineer
Global Enterprise West

December 17, 2025



Before we get Started...

Do ya remember Cisco's Security Cloud Control Mission

Reduce complexity for customers



Security Cloud Control

North Star: Define policy once and enforce anywhere

Hybrid Mesh Firewall

AI Defense

3rd Party Firewalls

Secure Firewall

Secure Workload

Hypershield

Secure Access

Secure Router NGFW



Unified AI Assistant: Across all Products
Simplify policy administration

Meaningful Product Integrations

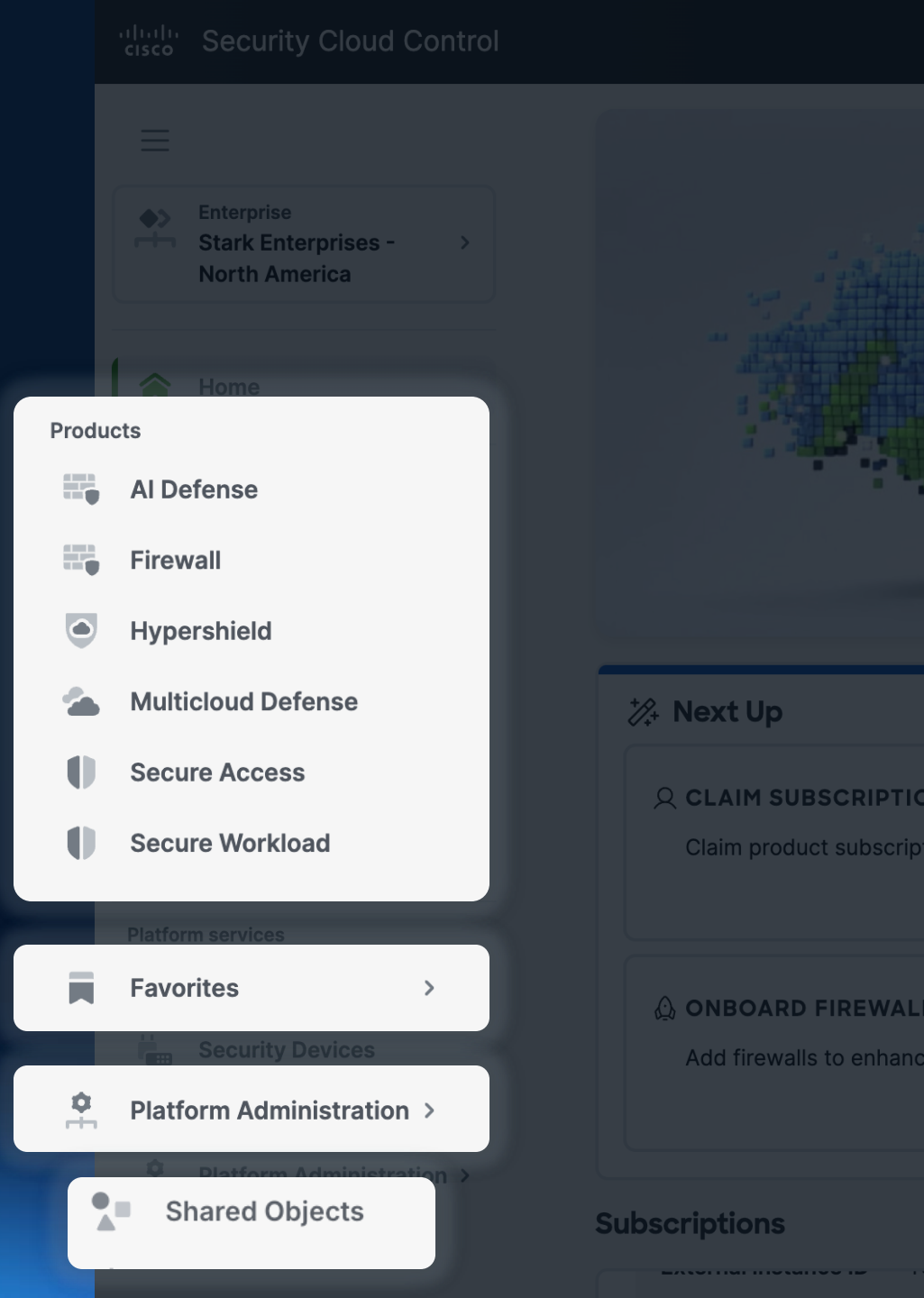
→ Policy & Object Sharing Across Products

→ Access product capabilities from single interface

→ Personalize your admin experience

→ Manage roles and groups across products

→ Centralized audit log for compliance





The Agenda:

- The challenges we are solving for
- What is SASE?
- SASE With Cisco
- Why Cisco Secure Access (SSE)
- AI Access
- *Migrating from Umbrella to Secure Access

**Current Workplace
Challenge – What are we
solving for?**

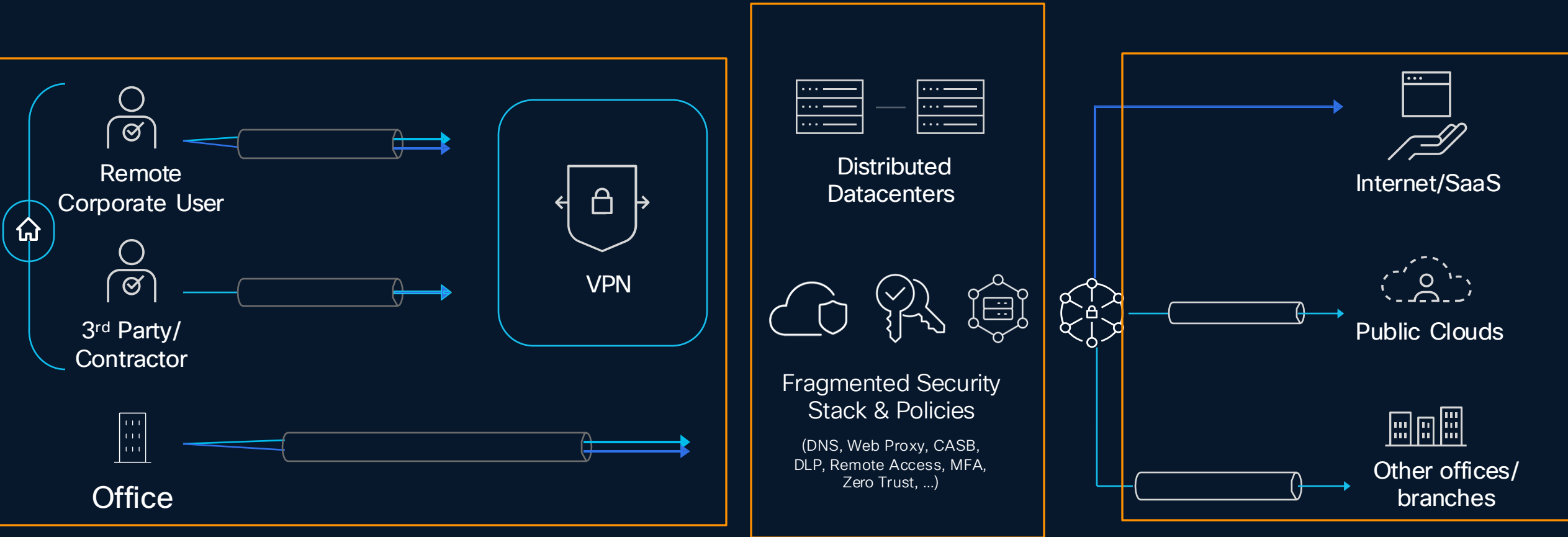
Applications and users are **everywhere** **Security is Hard**



Policy Challenges

An architecture never designed for hybrid work

↔ Internet Traffic
↔ Private Traffic
Secure Tunnel

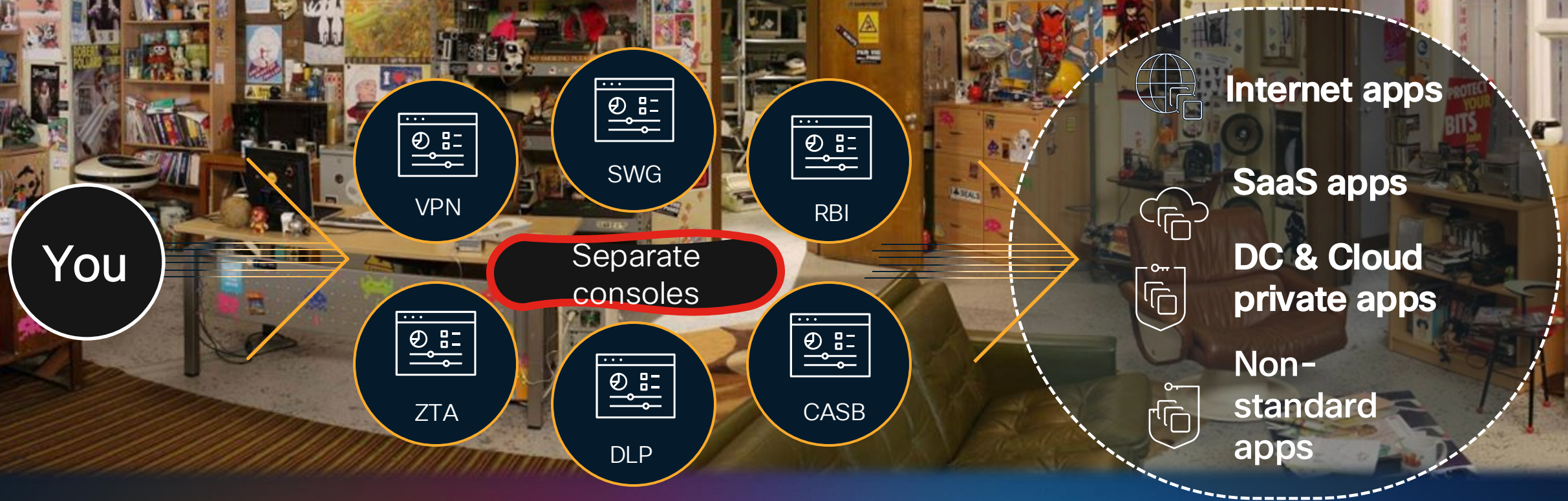


Poor user experience
Lower productivity

Large sets of individual solutions and vendors
Complexity of operations and costs

Gaps in security posture born out of complexity and fragmentation

• Security Challenges



Multiple products increase cost and inefficiencies

- Licenses/hardware
- Policy management
- Client management
- Alert Generation & Reporting
- Operational Cost
- Experience Monitoring?



How can Cisco deliver Networking and Security Services..

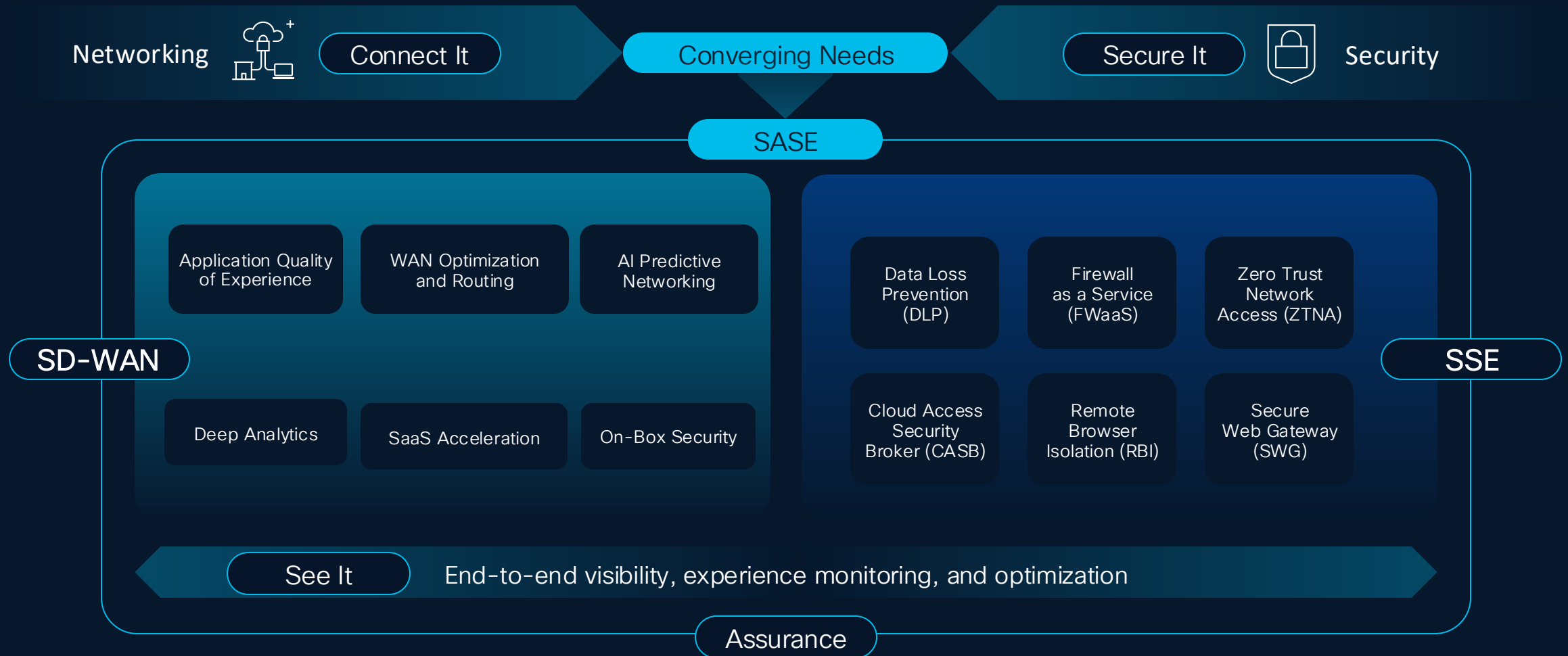
Secure Access Service Edge (SASE)

By 2025, 65% of enterprises will consolidate SASE components to one or two vendors, with 30% of large organizations moving to a single SASE platform by 2028.

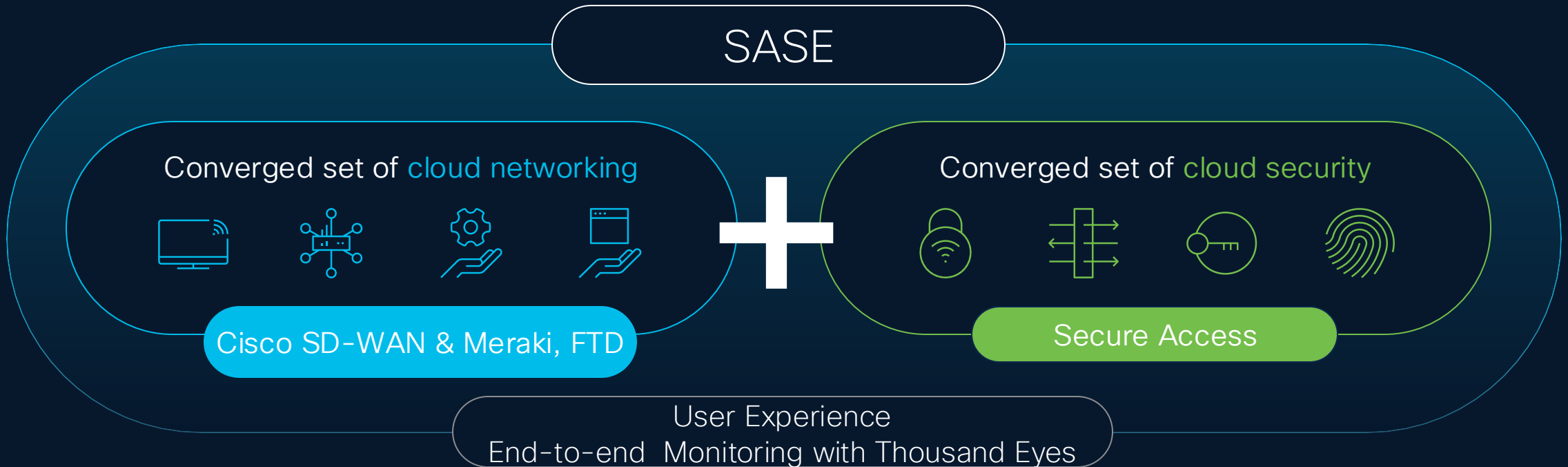
Gartner®

Secure Access Service Edge

The architecture for a securely connected experience in today's hyper-distributed environment



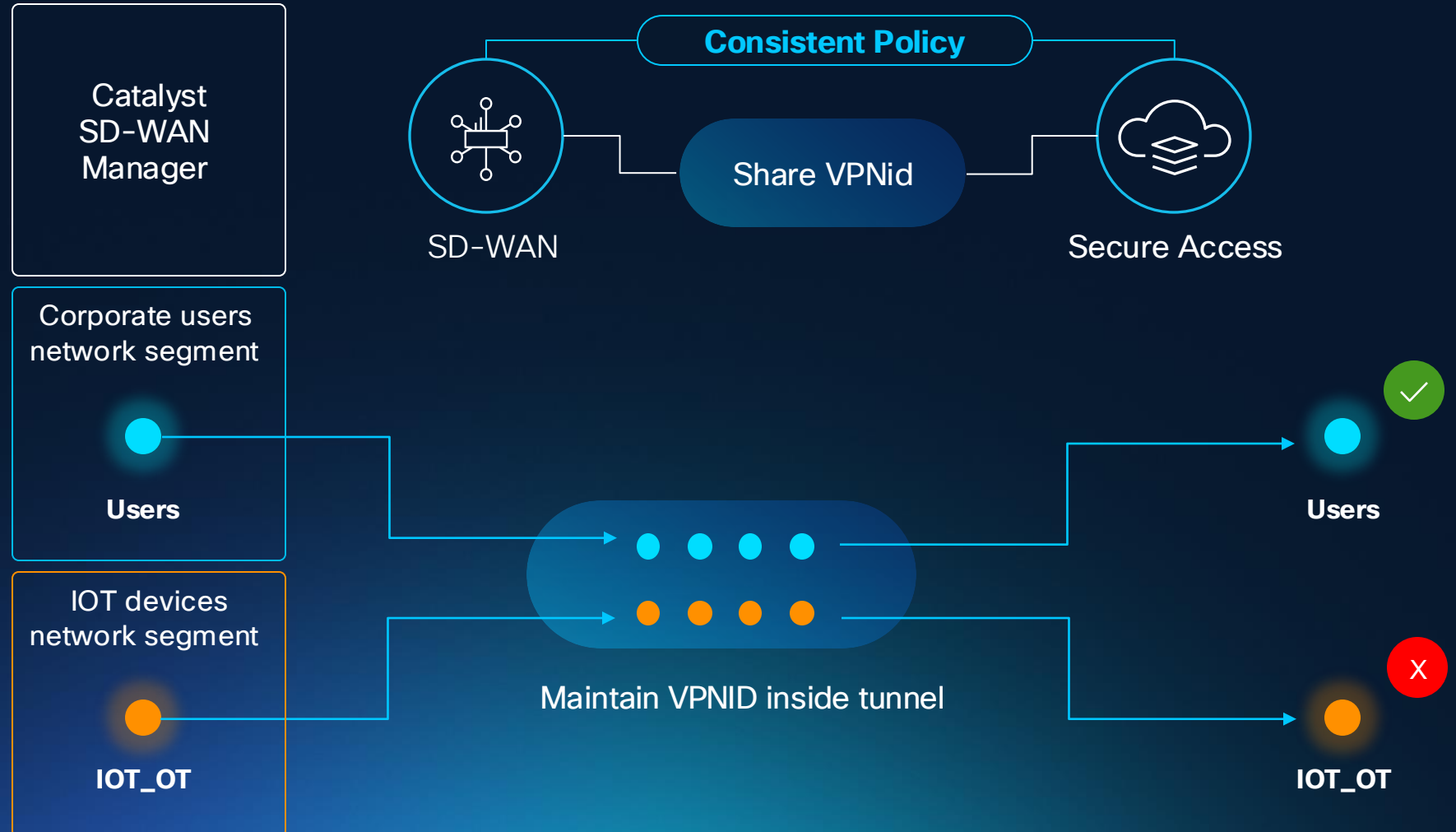
SASE with Cisco



Catalyst SD-WAN

VPNid support for consistent segmentation

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



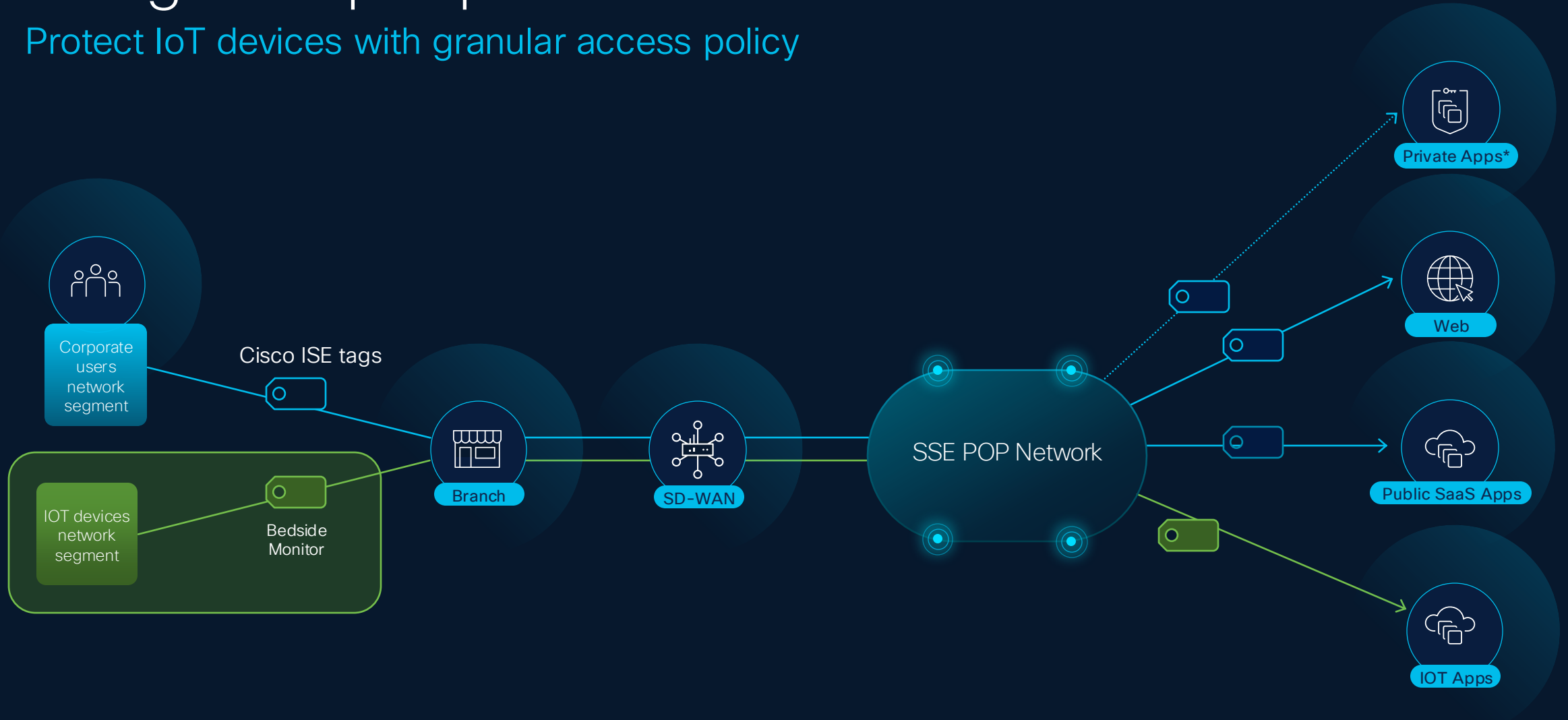
SD-WAN+ISE+Secure Access = Secure the Branch

ISE security group tags (SGTs) for granular application access



Things are people too

Protect IoT devices with granular access policy



Cisco SD-WAN + Secure Access accelerates IT outcomes



- End-to-end visibility – even on un-owned networks
- Identity Intelligence
- AI Access guardrails

- Global policies enforced locally
- Smart auth for users & things
- Secure BYOD with mobile/OS integrations

- Zero friction, zero downtime
- Predictive path recommendations
- Policy assurance

See more, solve more across your network

End-to-end visibility for optimal network performance (SDWAN) and security (Secure Access)

Find the best route

AI-powered analytics drive Predictive Path
Recommendations for optimal performance

Fix issues fast

Visibility from the edge to the
application across all types of networks

Future-proofed protection

Detect and enforce safe and
secure usage of GenAI apps

Cisco Secure Access

Security Services Edge

What's driving interest in security service edge (SSE)?

- Ongoing changes in the mix of cloud and on-premise applications/data
- Frequent changes in the mix of users/locations/device types
- Continually changing threats and attack tactics
- Lean Teams - aka Multiple Hats
- Zero Trust Architecture

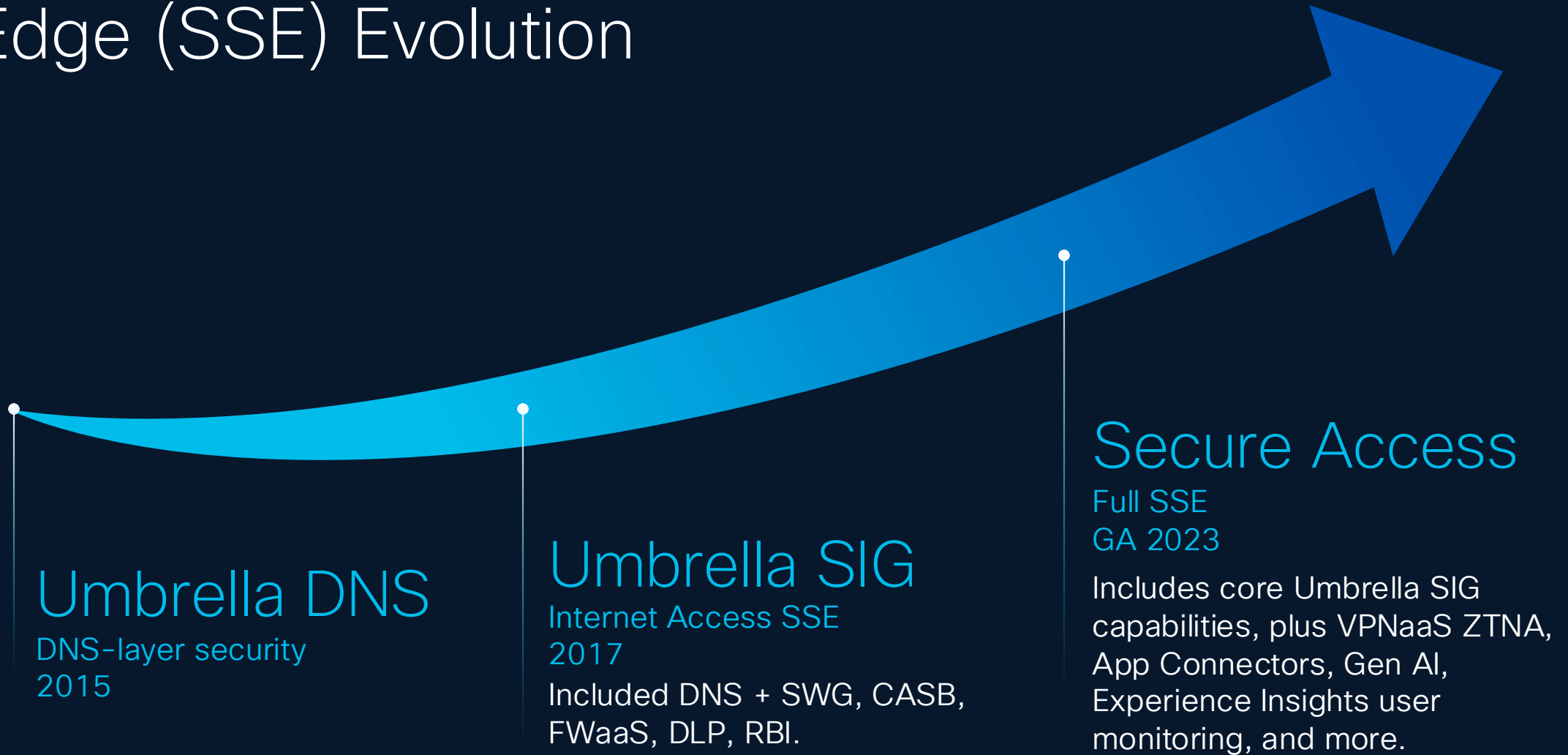
Tool sprawl and complexity are increasing risk and decreasing productivity

Cisco Secure Access

Modernize your defense with converged cloud security grounded in Zero Trust



Cisco Security Service Edge (SSE) Evolution



Cisco Secure Access: Extended SSE protection



SSE core capabilities

- Secure Web Gateway
- Zero Trust Network Access
- Firewall as-a-Service
- Cloud Access Security Broker
- Data Loss Prevention
- Advanced Malware Protection
- Sandbox



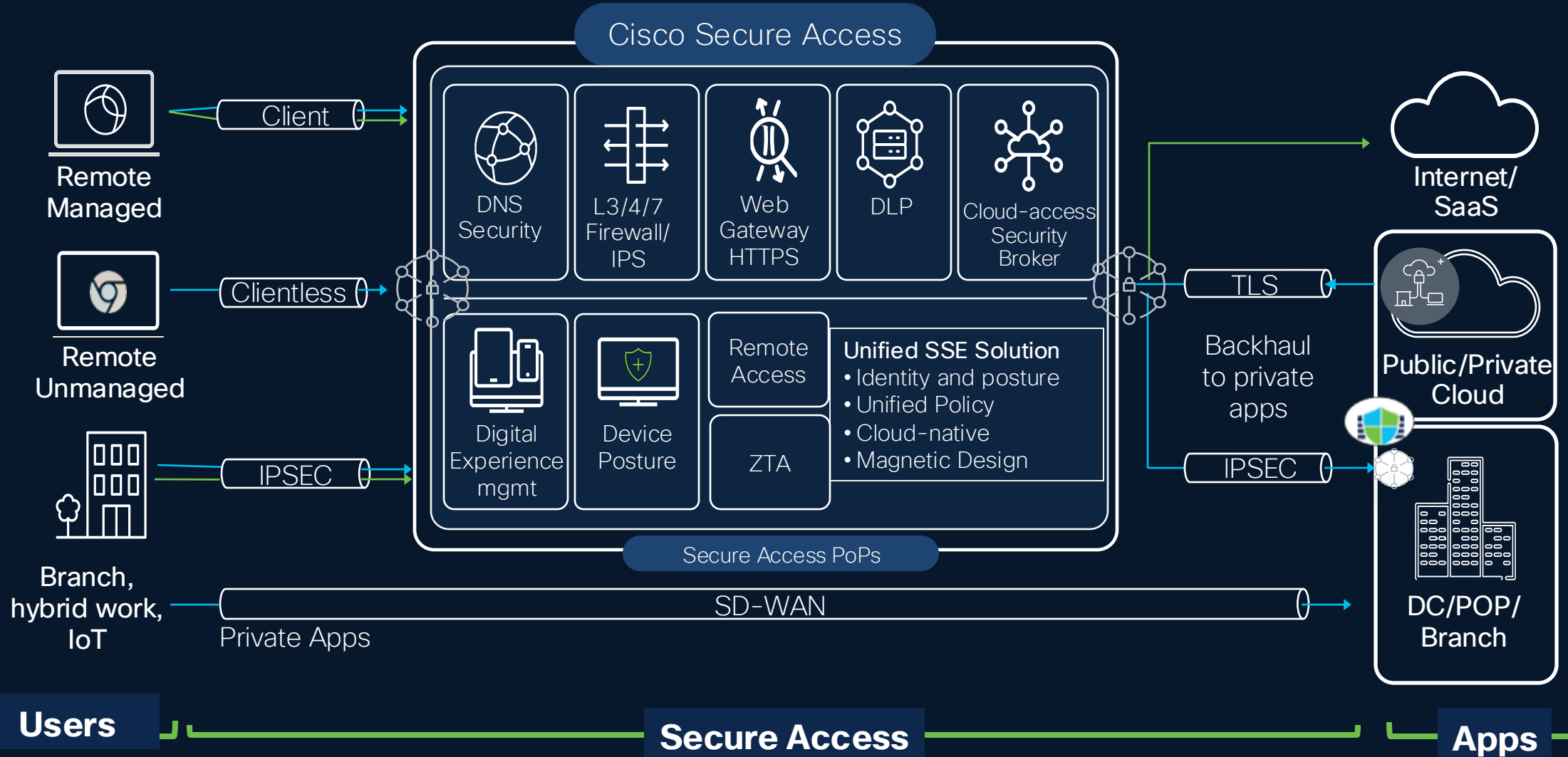
So much more

- VPN as-a-Service
- AI Access and Usage Controls
- Digital Experience Monitoring
- DNS Security
- Remote Browser Isolation
- Talos Threat Intelligence
- Cloud Malware Protection

Cisco delivers the core and more in a single subscription...

Cisco Secure Access

Unified Architecture



The User Experience

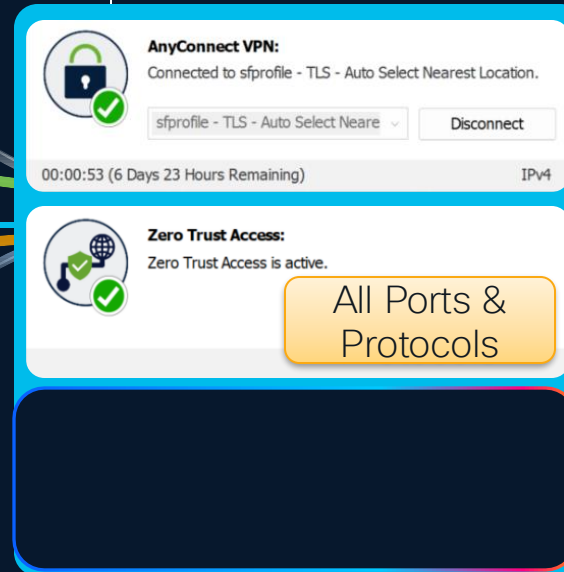
Users

STEP 1
Log In

STEP 2
Securely start work

Applications

Secure Client



Secure
Access

Per Application Access
DC1 & DC2 , Cloud

VPN Tunnel
Server Initiated traffic

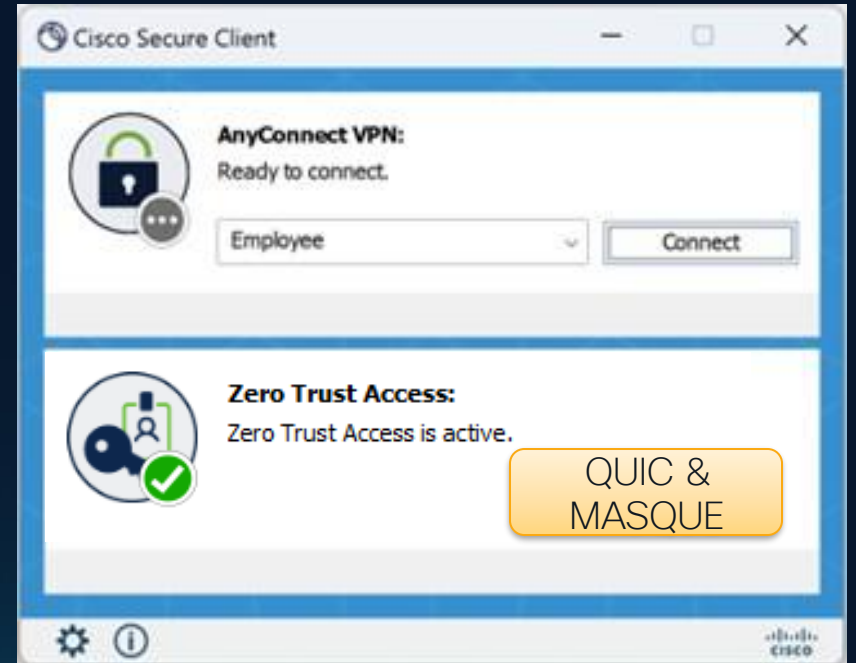
SaaS apps

Internet apps
The Wild West!

One client, multiple functions

Zero Trust Access Module

- Transparent user experience
- Proxied resource access with fine-grained access control
- Service managed client certificates with TPM/hardware enclave key storage
- Support for both TCP and UDP applications (for private and Internet access)





Recycle Bin



Google Chrome




Microsoft Edge






Webex


Cisco Secure Client

**Zero Trust Access:**
Registration is required to access secure resources.

Enroll

**Umbrella:**
Umbrella is active.

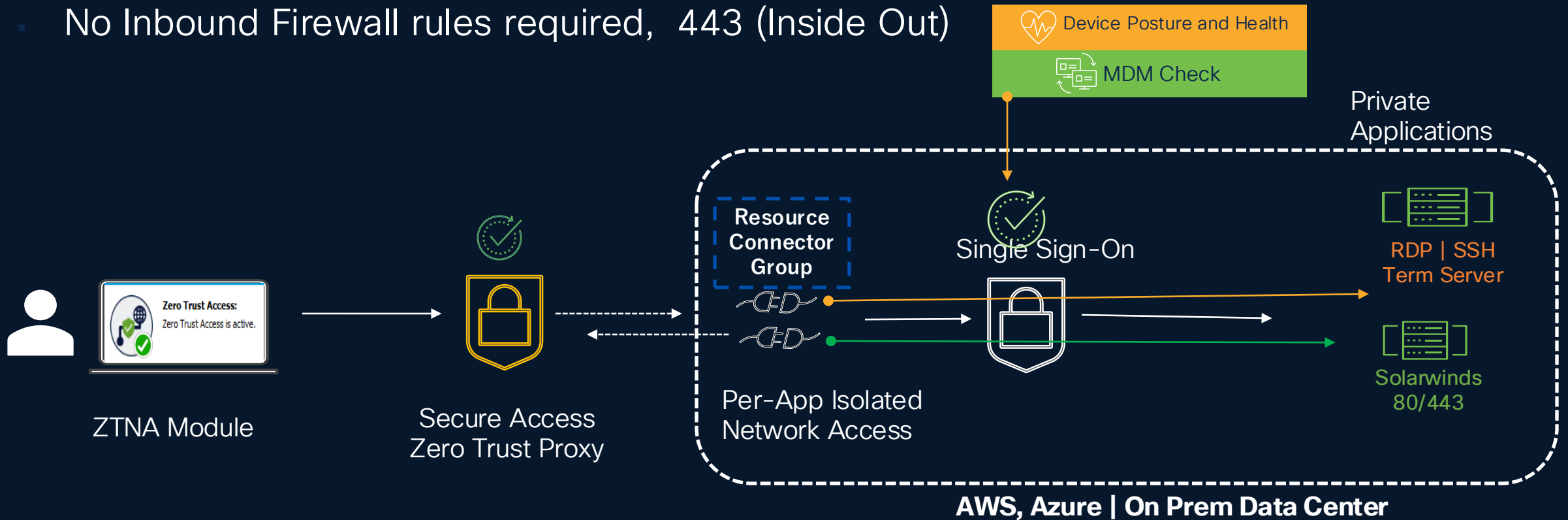




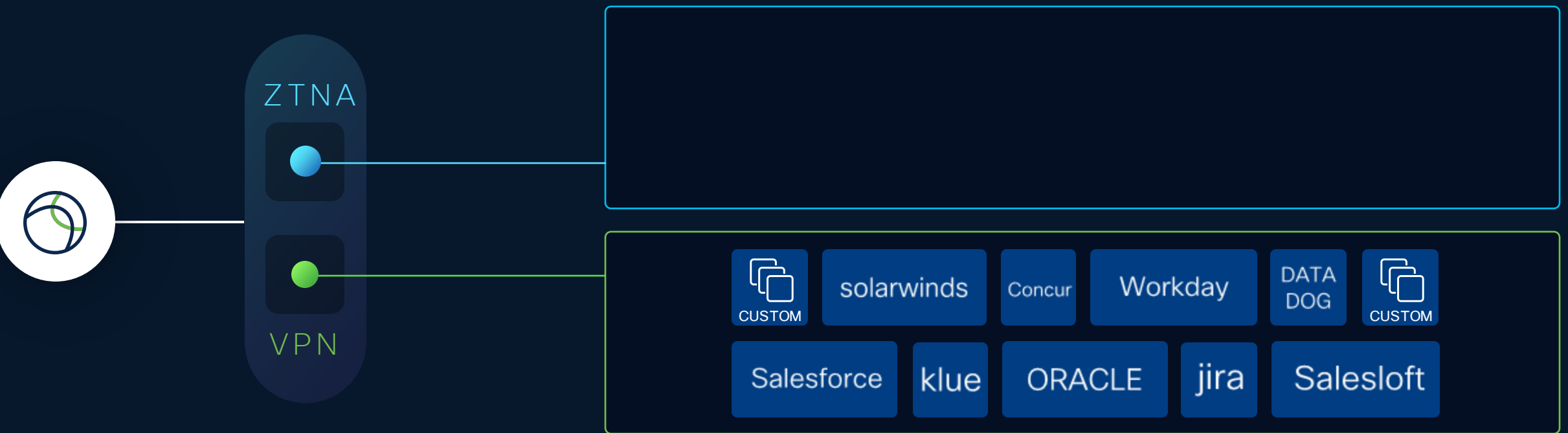
Cisco ZTNA – Modern Approach > VPN DTLS

Benefits:

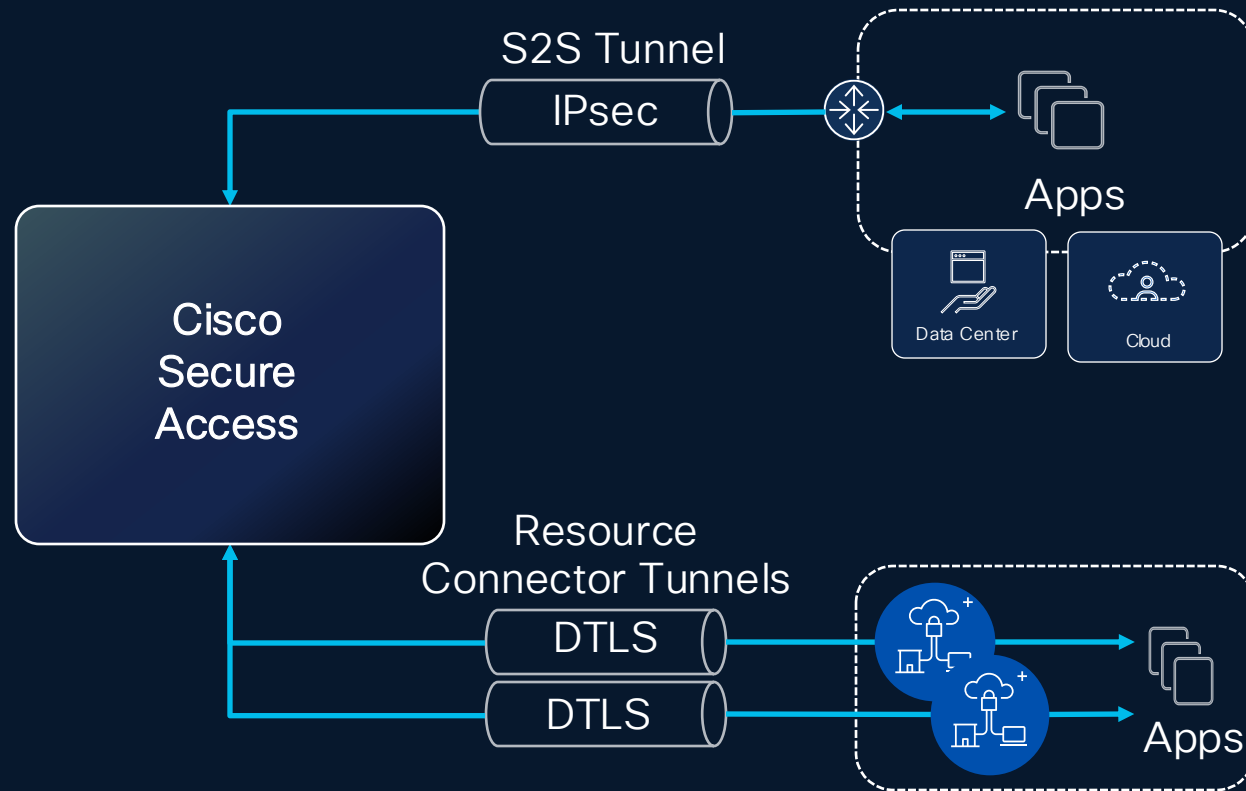
- Identity to Application Access (Zero Trust Principles)
- No direct resource access (forward proxy architecture)
- No Inbound Firewall rules required, 443 (Inside Out)



Secure Access simplifies ZTNA roll-out



Connecting to Private Applications



Site-to-site Tunnels with IPsec

- Standards-based IPsec connection
- Single tunnel for Internet and private application access
- Static or BGP routing support
- Auto failover for redundancy + ECMP for scale
- Fallback for resource connectors

Resource Connectors

- Lightweight VM for AWS, Azure, ESXI, Docker
- All traffic egresses from Resource Connector IP
- Access applications with overlapping IPs
- Outbound connection / no firewall holes required
- No routing configuration required
- Auto failover / load balancing

Secure Access Regions – AWS coverage



Legend

- Available
- Coming Soon
- Subject to Demand

Secure Access Regions – DCv2 (Physical Edge DC)



In Development & Coming Soon

Amsterdam
Frankfurt
Chicago
Dallas

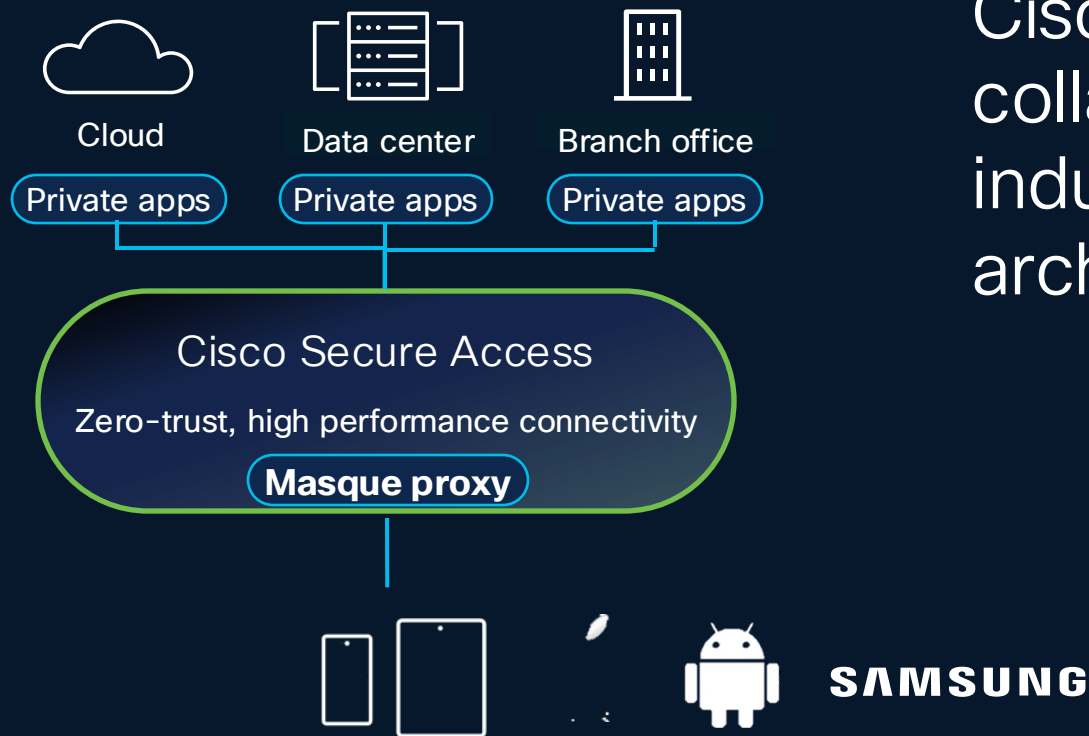
Tokyo
Osaka
Mumbai
Chennai
Aukland

Legend

- Available
- In Development

Zero Trust secure access from mobile devices

Apple iOS and Android on Samsung



Cisco and major mobile providers collaborated to develop the industry's first zero-trust architecture for mobile devices

- Apple iOS 17+
- Generic Android 14+
- Android on Samsung Knox 3.10+

Technology innovation and flexibility: Either TCP/TLS or new QUIC/UDP protocols

Simplified Admin & User Experience

“Build products that people love, that they use repeatedly and talk to their friends and family about enthusiastically.” – Jeetu Patel

Security Cloud Control

Define policy once and enforce anywhere

Secure Firewall
(FTD, ASA)

Hypershield

Multicloud
Defense

Secure
Workload

Secure Access

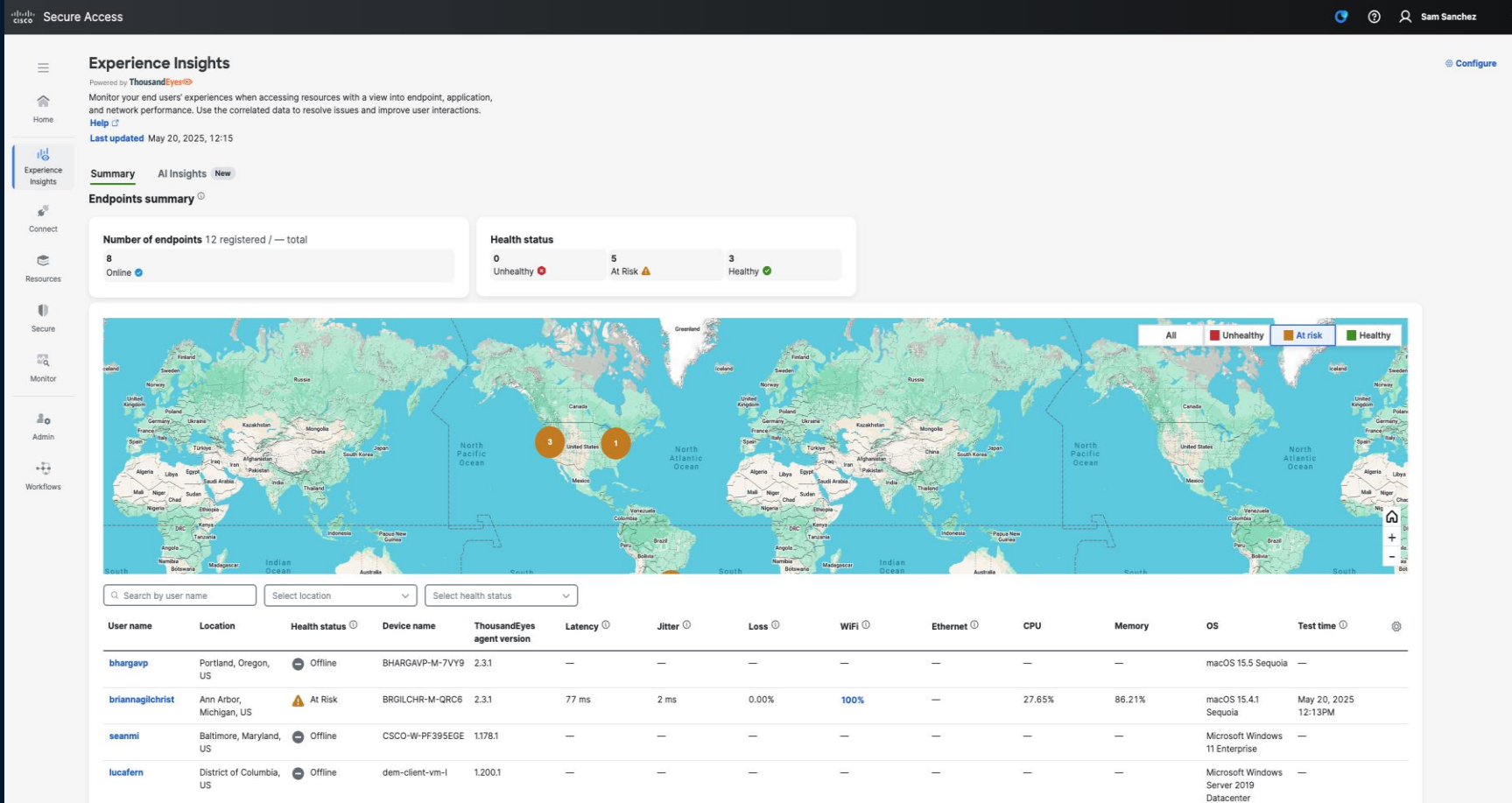
AI Defense

Secure Router

3rd party
firewalls

Global Workforce Visibility

Gain a complete view of user experience, for both remote and hybrid workers

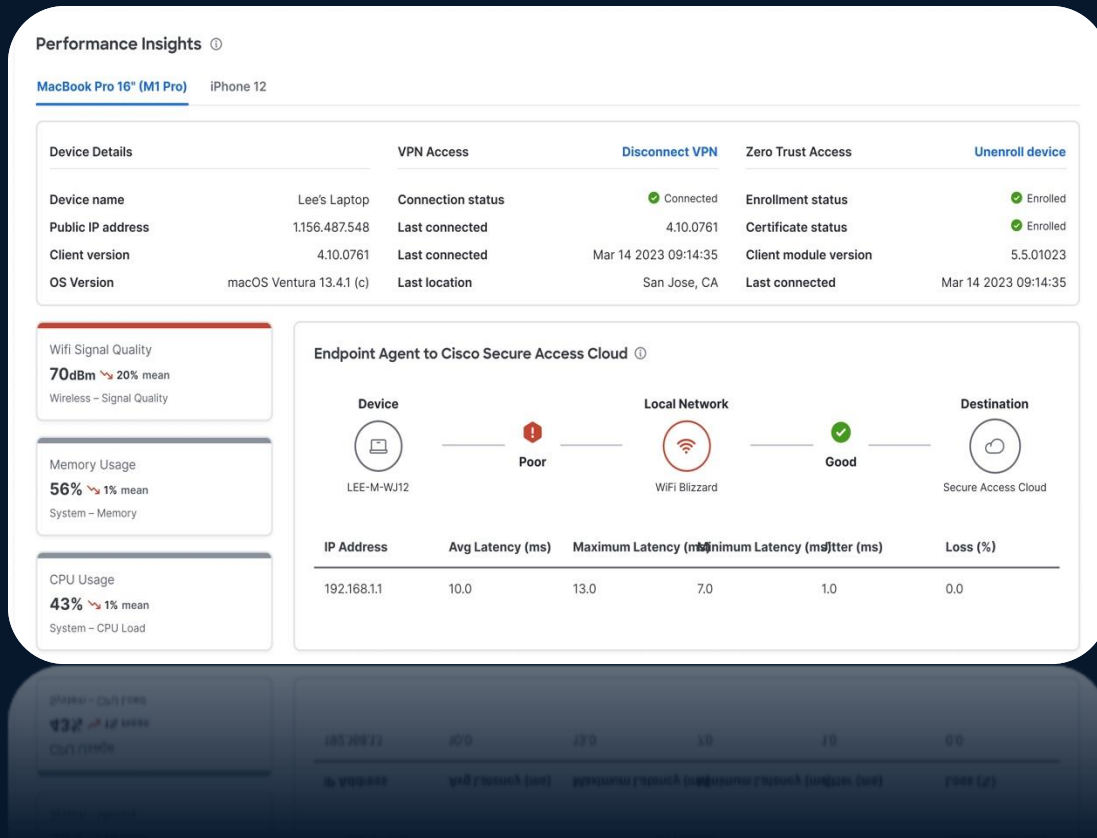


Simplified Experience

- Monitor all endpoints within a **single SSE dashboard**
- Lightweight ThousandEyes Endpoint Agent included with CSC at **no extra cost**
- **Continuous monitoring for efficient troubleshooting**

Monitor The User Experience

Monitor health and performance as users access applications and resources



Optimize user productivity by automatically, providing details on the user's experience, enabling faster issue detection and resolution

Monitoring examples:

- Endpoint performance – CPU/memory (and the processes causing high utilization), Wi-Fi
- Network performance – endpoint to Secure Access
- Top SaaS applications performance
- Collaboration performance monitoring (Webex, MS Teams)
- User specific events

Secure Access Intent Based Policy



Unified Policy Evaluation

941 Rules

Change view

<input type="checkbox"/>	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status	
<input type="checkbox"/>	1	Any employee access to any...	Private	Allow	Any User...	+3 Any Applic...	+1	4.1K		...
<input type="checkbox"/>	2	US-Canada Employees	Private	Block	North Ame...	+4 Company...	+4	1.2K		...
<input type="checkbox"/>	3	Product Management Resour...	Internet	Warn	PM User Gr...	+1 Product M...	+2	924		...
<input type="checkbox"/>	4	Europe Content Block List	Internet	Isolate	Europe Em...	+7 EU Catego...	+7	-		...
<input type="checkbox"/>	5	Contractors access to Lab App	Private	Allow	Contractor...	+6 Lab Applic...	+9	1.2M		...
<input type="checkbox"/>	6	Workday resources	Internet	Block	Any User G...	+7 Cisco Wo...	+12	73K		...
<input type="checkbox"/>	7	Workday resources	Internet	Block	Any User G...	+7 Cisco Wo...	+12	73K		...
<input type="checkbox"/>	8	Workday resources	Internet	Block	Any User G...	+7 Cisco Wo...	+12	73K		...
<input type="checkbox"/>	9	Workday resources	Internet	Block	Any User G...	+7 Cisco Wo...	+12	73K		...
<input type="checkbox"/>	10	Workday resources	Internet	Block	Any User G...	+7 Cisco Wo...	+12	73K		...

Rows per page 100 < 1 2 ... 5 >

Default Access Rules ⓘ

Rule name	Action	Sources	Destinations	Security	Posture	
For all private destinations	Block	Any	Any private destination	-	-	...
For all internet destinations	Allow	Any	Any internet destination		-	...

Consistent Security Enforcement

- Transit agnostic
- Private & Internet enforcement
- Per application / destination

Full IPS

- Built on Snort 3.0
- Complete Signature Set
- TALOS updated

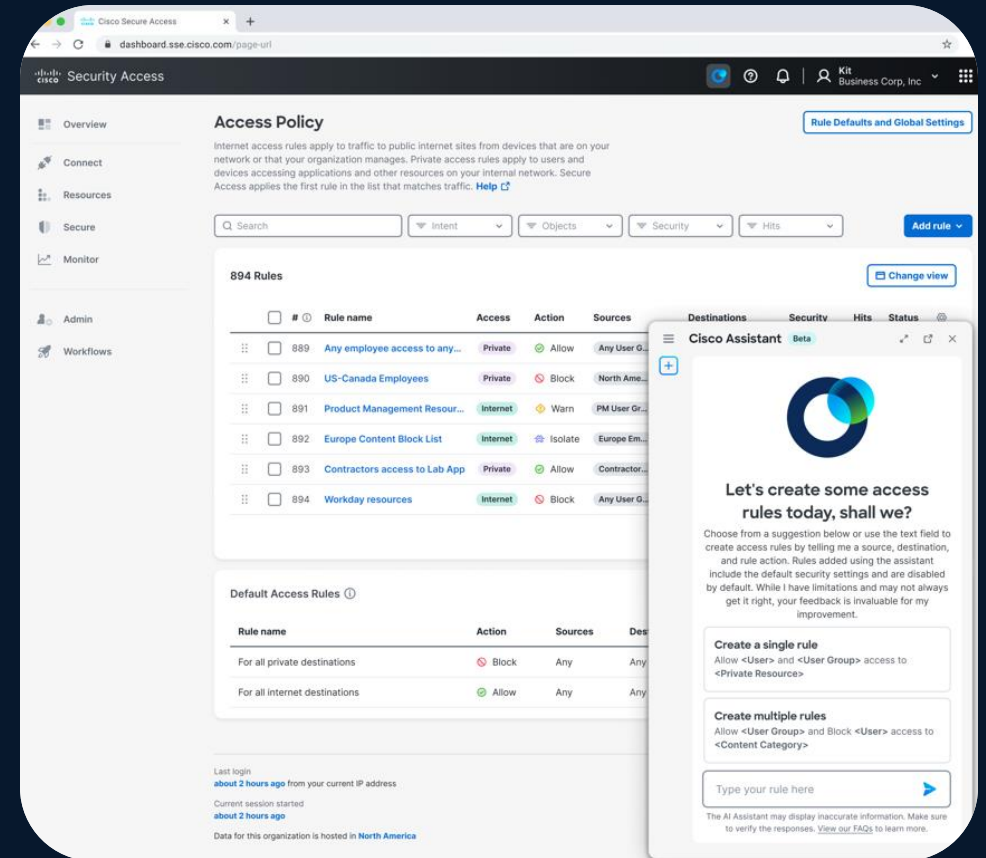
Unified Internet + Private Policy

- Single view of all access
- Filter and sort view
- No need to pivot

Cisco AI Assistant for Secure Access

AI for Security

- Built with Generative AI natural language to:
 - Simplify and speed policy administration by up to 70%
 - Reduce human error
 - Improve operational efficiency



Better Efficacy. Better Experience. Better Economics.

Troubleshooting Assistant

Automate troubleshooting Secure Access

Prompts:

“Why can't Lee Parker access Jira”

- Private App Access Issue
- Multi Agent **Orchestration**
- Faster **Time** to Resolution

You
Why can't Lee Meadows access Jira2?

AI Assistant 11:05 am

I have identified the user **Lee Meadows** with email address **lmeadows@abc.com** and **Jira 2** (Office Productivity App) in our system. Verify settings in the event details section and then click Analyze events.

Event details

Sources: Lee Meadows (lmeadows@abc.com) ▾

Destinations: Jira 2 (Office productivity app) ▾

Connection Type: ZTNA ▾

Device type: macOS × ▾

Devices: Lee-mac-C4605 (ZTNA) ▾

Analyze event

AI Assistant 11:08 am

Event analysis:

Based on the information provided, here are the possible reasons why **Lee Meadows** cannot access **Jira2**:

- A ZTA block event occurred for **Lee Meadows**
- A **Resource Connector 2** connection was issue for **Lee Meadows**

Note that these are possible reasons only, and further investigation may be required to determine the exact cause.

ZTA Access failure analysis 1 Block 7/7 checks

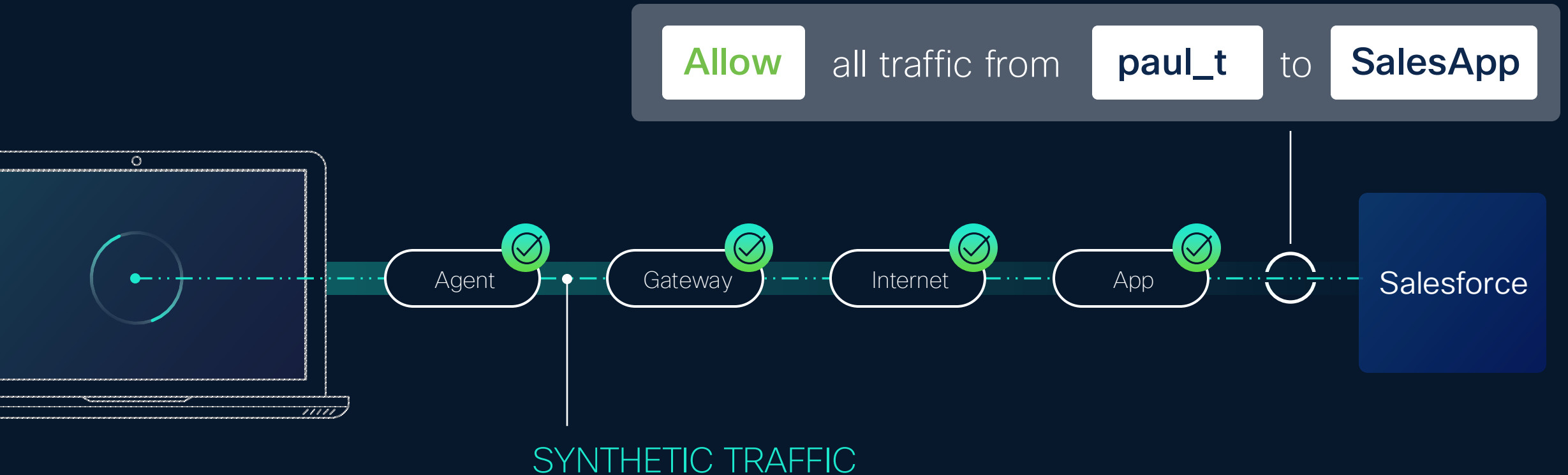
- ✓ Device Enrollment
- ✓ Access Policy
- ✓ Endpoint Posture
- ✓ User Authentication
- ✓ DNS
- ✓ IPS Profile
- ✗ Resource Connector 1 Block



of outages are from
misconfigurations

Policy Assurance

Positive Policy: **Verified**



Secure Access

Securing the use of generative AI

AI risk is already impacting businesses



86% have experienced an AI-related security incident in the past 12 months



Only 45% have resources and expertise for comprehensive AI security assessments

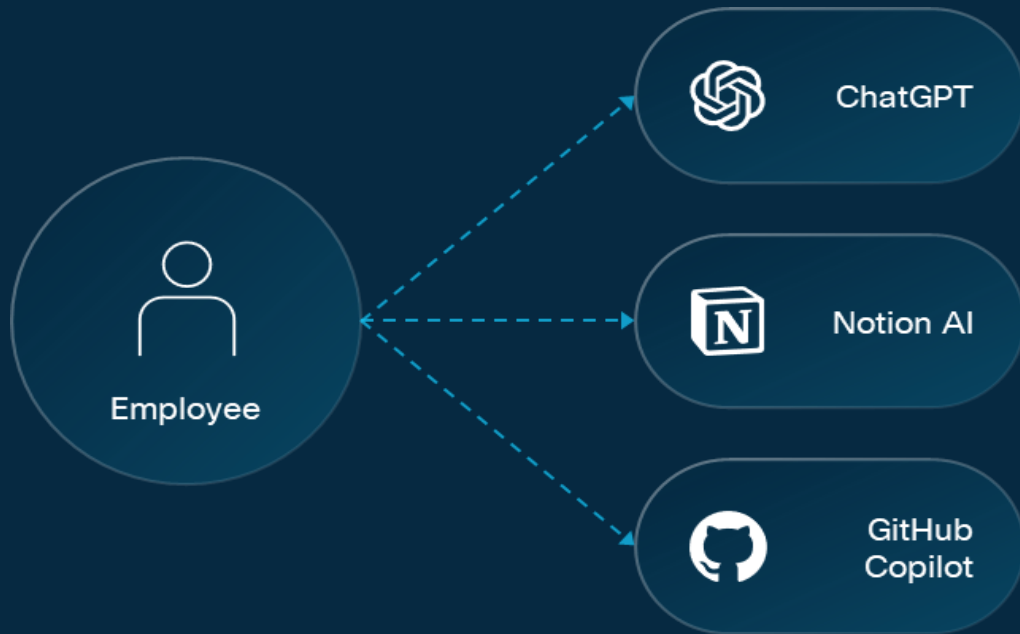


41% do not have mature controls on data used to train AI models

Two distinct areas of AI risk

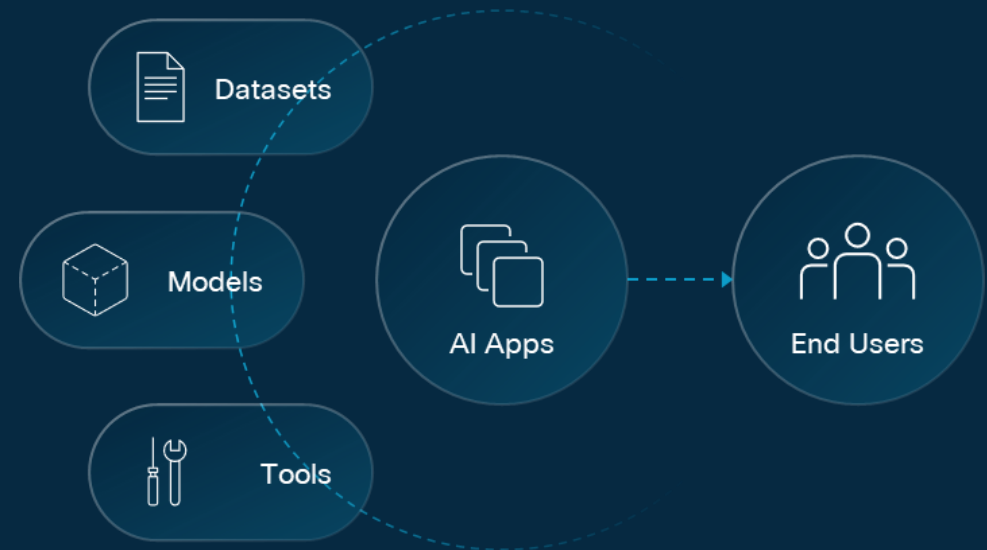
Third-Party AI Tools – AI Access with Secure Access

Manage employee use of **third-party AI tools**, preventing data leakage and other business risks, with Cisco Secure Access.



First-Party AI Applications – AI Defense* (Available as a separate product)

Enable end-to-end secure development of **first-party AI applications** across your business with Cisco AI Defense.



Security for AI with Secure Access

Discover and control the usage of 1,200 Gen-AI apps



**ROBUST
INTELLIGENCE**

now part of **CISCO**

2024

Threat Visibility



Discover and
Assess Activities

Leakage Prevention



DLP Inspection of
Prompts/Uploads

Threat Prevention



Block Apps and
Control Downloads

Realtime DLP **content** now supports the **inbound** use-case

AI Guardrail Categories – Security for AI

- Intent Based Detection

Security

- Prompt Injection
- Response Detection

Both direction analysis is important

Privacy

- American Bankers Association (ABA) Routing Number (US)
- Bank Account Number (US)
- Credit Card Number
- Driver's License Number (US)
- Plus other common PII

Safety

- Harassment
- Hate Speech
- Profanity
- Sexual Content & Exploitation
- Social Division & Polarization
- Violence & Public Safety Threats

Map guardrails to standards and frameworks like:



Secure Access sees and controls AI use

Superior visibility & control

- Discover Shadow AI; define acceptable use
- Granular control
 - Sensitive documents
 - Source code
- Machine learning finds unstructured data
 - Patent applications
 - M&A
 - Financial statements and more

AI App Discovery Secure Access

Leverage Secure Access to identify 3rd party generative AI applications, their usage, risk score and protection status. [Learn more](#)

Risk ▼ First detected date ▼ 48 results

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

1200+
AI Apps Protected

100%
Guardrails for top AI Apps

1
Unified Security Framework

AI protection that goes beyond discovery

Cisco AI Access, powered by AI Defense

Discover Shadow AI + Define Acceptable Use

AI App Discovery

Secure Access

Leverage Secure Access to identify 3rd party generative AI applications, their usage, risk score and protection status. [Learn more](#)

Risk

First detected date

48 results

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 DLP Controls

Data Classification Name

Description (Optional)

AI/ML Monitor

Included Data Identifiers

☒ Source Code

☒ Source Code (ML)

Include Data Identifiers

Select Boolean Operator

OR

AND

Built-in Data Identifiers

Search in Data Identifiers

Built-in Identifiers

☐ ABA Routing Number (US)

☐ Aggressive Behavior

☐ AWS - Access Key

☐ AWS - API Key

☐ AWS - Secret Key

☐ AWS - Session Token

☐ Azure - Access Key

Machine learning guardrails for AI use

Secure Access

287 Total Events

Showing events from Jan 6, 2024 at 00:00:00 to Jan 1, 2025 at 00:00:00

Event Type	Severity	Source	Destination	Risk	Action	Interval	App Name
AI Assistant	High	192.168.1.1	192.168.1.1	High	Blocked	7 days	AI Assistant
Code Copilot	High	192.168.1.1	192.168.1.1	High	Blocked	7 days	Code Copilot
HelperAI	High	192.168.1.1	192.168.1.1	High	Blocked	7 days	HelperAI
AI Creator	High	192.168.1.1	192.168.1.1	High	Blocked	7 days	AI Creator
GrammarAI	Medium	192.168.1.1	192.168.1.1	Medium	Blocked	7 days	GrammarAI
WriterBot	High	192.168.1.1	192.168.1.1	High	Blocked	7 days	WriterBot

AI Access: Deeper Protection for Gen-AI Apps

AI guardrails in Secure Access DLP policy

- Adds to the traditional DLP capabilities.
- Uses predictive classifier model to detect “intent” in prompts vs regex type patterns
- Example: “please generate a table with all emails from the attached database”

Data Loss Prevention Policy

When enabled through its rules, the Data Loss Prevention policy can monitor or block the data being uploaded to the web. As well, it can discover and protect the sensitive data stored and shared in your cloud sanctioned applications. [Help](#)

DISCOVERY SCAN

ADD RULE

12 DLP Rules							
Rule Type	Name	Severity	Action	Identities or File Owners	Destinations	Data Classifications File Labels	Last Modified
AI Defense	AI Defense traffic direction	Medium	Monitor	Inclusion 1 Identity	Inclusion 2 Applications	Data Classifications Privacy guardrail	Dec 17, 2024

Data Classifications

Select data classifications to add them to this rule.

Search Classifications

☒

Privacy guardrail

PREVIEW

☒

Copy of Privacy guardrail

PREVIEW

☒

Custom Privacy guardrail

PREVIEW

☒

Example AI Classification

PREVIEW

☒

Safety guardrail

PREVIEW

☒

Security guardrail

PREVIEW

Security guardrail

Protect your generative AI applications from threats and unauthorized access and prevent these applications from being used to carry out such activities.

Included Data Identifiers (OR Boolean)

☒ Code detection

☒ Prompt injection

DATA CLASSIFICATION

AI protection that goes beyond discovery

Cisco AI Access, powered by AI Defense

Discover AI Guardrails for AI
Discover AI Guardrails for AI
Discover AI Guardrails for AI

Data Classification Name

AI/ML Monitor

Description (Optional)

Included Data Identifiers

☒ Source Code

Secure Access

Event Type

☐ Real Time

☐ SaaS API

☐ AI Guardrails

Action

☐ Blocked

☐ Deleted

☐ Monitored

☐ Quarantined

☐ Restored from Quarantine

☐ Revoked Access

Severity

☐ Low

☐ Medium

☐ High

☐ Critical

Direction

☐ Upload

☐ Download

287 Total Events

Viewing activity from Jan 8, 2025 at 6:59 PM to Feb 7, 2025 at 6:59 PM

Event Type	Severity	Identity	Direction	Destination	Rule	Action	Detected
AI Guardrail	High	Bob SWG (bob@swginsw...	Prompt	Deepseek	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:15 AM
AI Guardrail	Critical	Bob SWG (bob@swginsw...	Prompt	Deepseek	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:15 AM
AI Guardrail	Critical	Bob SWG (bob@swginsw...	Prompt	Deepseek	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:14 AM
AI Guardrail	High	Bob SWG (bob@swginsw...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:14 AM
AI Guardrail	High	Bob SWG (bob@swginsw...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:05 AM
AI Guardrail	High	Bob SWG (bob@swginsw...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:57 AM
AI Guardrail	High	Bob SWG (bob@swginsw...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:48 AM
AI Guardrail	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:41 AM
AI Guardrail	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:37 AM
Real Time	Low	52.12.127.197	Upload	Datadog	New Rule	Monitored	Feb 5, 2025 at 12:35 AM
Real Time	Low	52.12.127.197	Upload	Datadog	New Rule	Monitored	Feb 5, 2025 at 12:35 AM
Real Time	Critical	52.12.127.197	Upload	Mozilla Firefox	Raja_test_rule	Blocked	Feb 5, 2025 at 12:28 AM
AI Guardrail	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:56 PM
AI Guardrail	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:54 PM

File Name

Form

Identity

Bob SWG (bob@swginsw...)

Application

Deepseek

Application Category

Generative AI

Destination URL

http://chat.deepseek.com

Copy

Rule

AI monitor

Severity

High

Direction

Prompt

Classification

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

☐ AWS - Access Key

☐ AWS - API Key

☐ AWS - Secret Key

☐ AWS - Session Token

☐ Azure - Access Key

Why Cisco Secure Access?



Safer for everyone

Most comprehensive SSE solution with 3x the security capabilities in one cloud service



AI-first Security Service Edge



Better for users

Seamless, secure access connecting your workforce to anything from anywhere



High performance zero trust



Easier for IT

Converged security in one console, one client, one cloud for simplified operations



Cost-effective efficiencies

Migration Offers

Cisco Secure Access Elevate Offer: Cost-Effective Evolution

Take your Umbrella investment
to the next level with Cisco Secure Access

Get up to full investment credit

Up to Full Umbrella subscription
balance credit, applied to
Cisco Secure Access

Flexibly upgrade on your schedule

Free one-year Umbrella
subscription, as you upgrade
to Cisco Secure Access

Why Upgrade To Secure Access?

Customers receive stronger security, at no additional cost:

DNS Defense

- Cloud DLP (SaaS API DLP)
- Cloud malware scanning
- Enhanced management with a streamlined policy model
- A simplified path to full SSE

Secure Internet Access

All of the above AND:

- Digital Experience Monitoring (DEM) powered by ThousandEyes
- Remote Browser Isolation

Also Need UZTNA?

DNS Defense and SIA include a 100-seat trial of our ZTNA+VPNaaS (SPA package)

Upgrading is simple

Upgrade on your timeline

- Secure Access and Umbrella instances run simultaneously
- The free Upgrade Manager is a part of the Umbrella UI
- Upgrade Manager policy replication is extremely simple

Technical Migration

Streamlined experience with the Secure Access Upgrade Manager

Complete policy migration in less than an hour

- **Umbrella DNS and SIG Migrations available now**

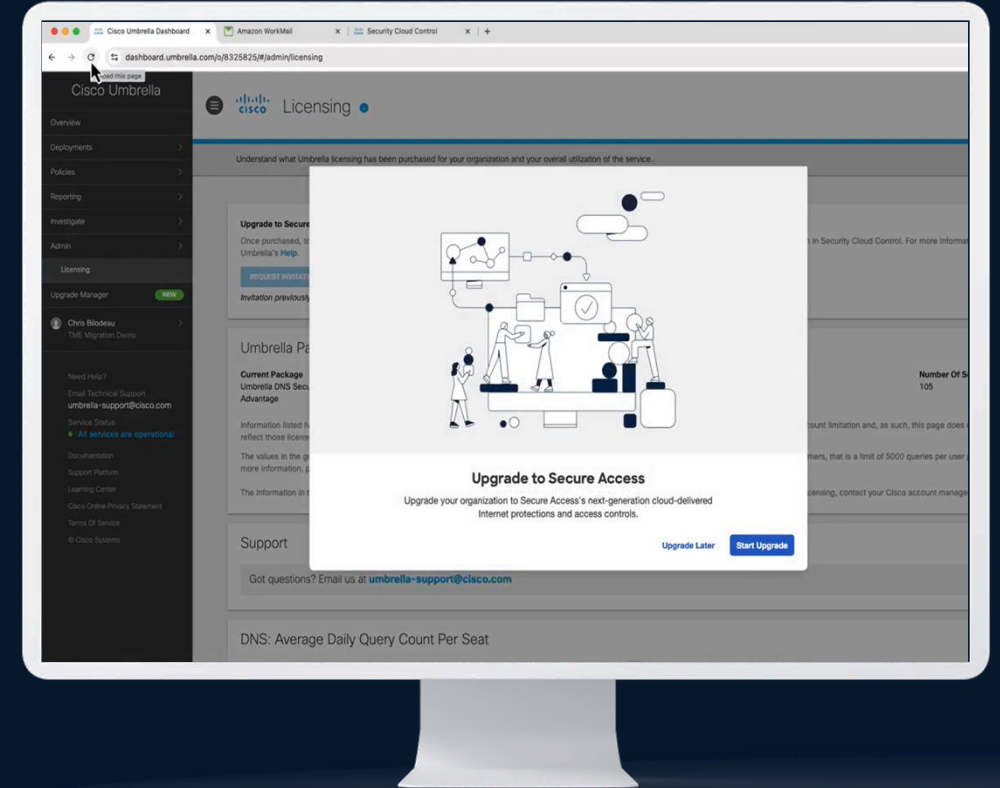
- [Onboarding guide](#)
- [Vidcast \(DNS\)](#)

Available Now

- Umbrella DNS to Secure Access DNS Defense
- Umbrella SIG to Secure Access SIA Phase 1 (DNS and SWG)

Future

- Umbrella SIG to Secure Access SIA Phase 2 (Firewall, Network Tunnels)



- ✓ Migration wizard: translates Policies to Secure Access Rules
- ✓ Gives customer control of migration
- ✓ Provides a “dual view” where customers can access both Umbrella and Secure Access from a single interface

Call to action

1

Get with your Account Team

Leverage our current **migration** from Umbrella to Secure Access offers, **SASE workshops, PoVs, AI/Security Assessments** and more.

[Elevate Offer](#)

2

Plan to Adopt Zero Trust Policy

Granular context aware for any user anywhere, enforce granular, context-aware policies with advanced AI-assisted security controls.

[Future-Proof Workplace](#)

3

Leverage SASE

Take advantage of Cisco's current migration offers and expert services to simplify your journey to a converged, cloud-native Security Service Edge (SSE) architecture.

[SASE Offers](#)

Call to action

1

Get with your Account Team

Go deeper into the architecture, Workshop, POV to align your use cases to our solution.

2

Migrate from Umbrella to Secure Access

Leverage our current **migration** from Umbrella to Secure Access offers, **SASE workshops, PoVs, AI/Security Assessments** and more.

3

Leverage SASE

Take advantage of Cisco's current migration offers and expert services to simplify your journey to a converged, cloud-native Security Service Edge (SSE) architecture.

Thank you

