

# 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



Before we get Started...

# Do ya remember Cisco's Security Cloud Control Mission?

Reduce complexity for customers

## Cisco Strategy



Meet unified solution demand



Reduce complexity for customers



Optimize cross product integrations

## Customer Benefits



Improved security outcomes



Improved operational efficiency



Easier setup and configuration



Platform advantage for MSPs

# 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

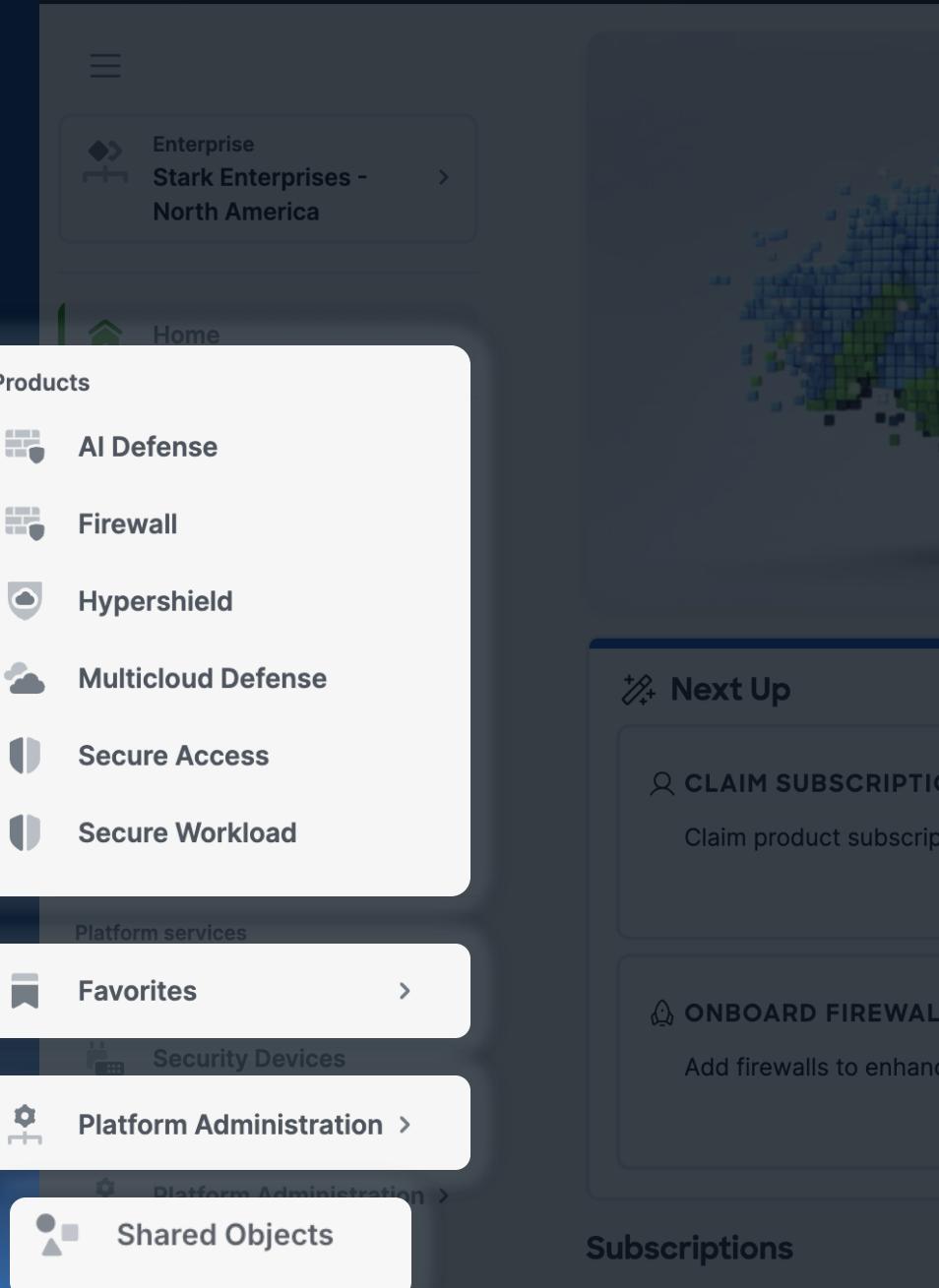
→ Policy & Object Sharing Across Products

→ 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?

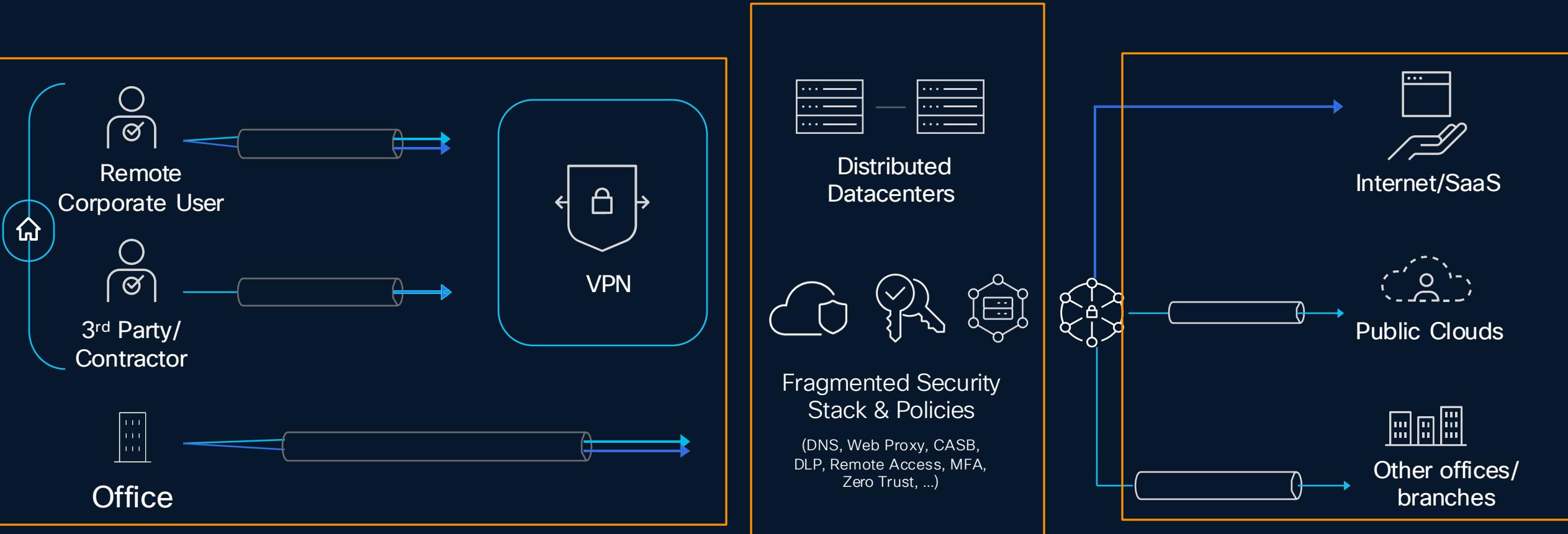
# Applications and users are **everywhere** Security is Hard



# Policy Challenges

An architecture never designed for hybrid work

↔ Internet Traffic  
↔ Private Traffic  
— Secure Tunnel

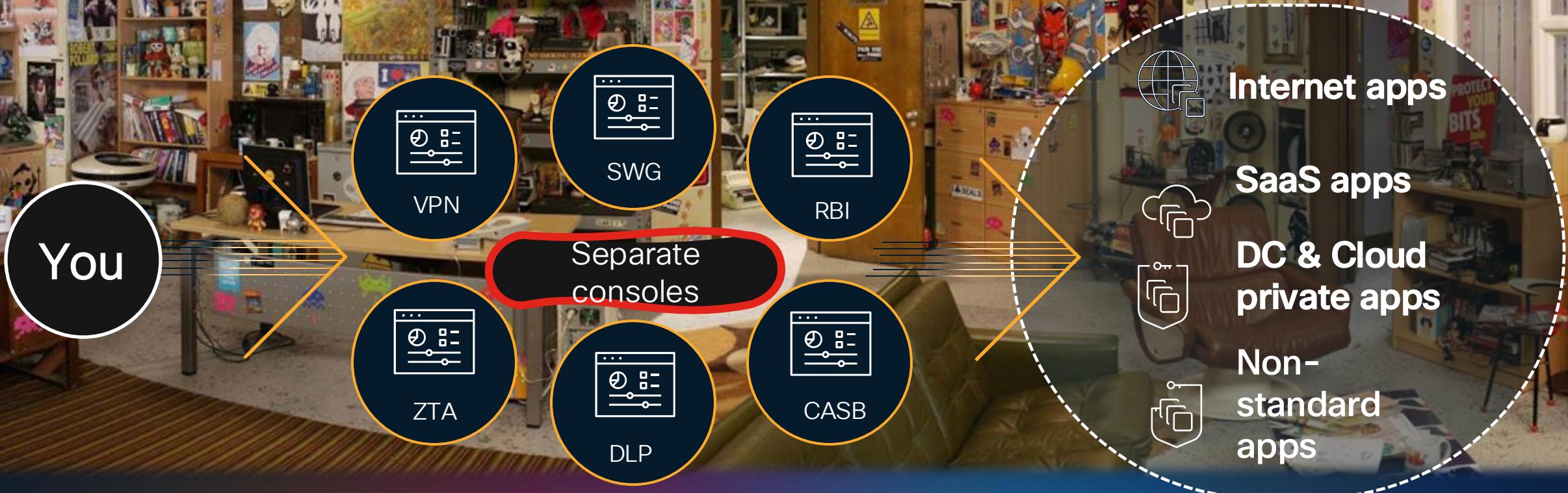


Poor user experience  
Lower productivity

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..

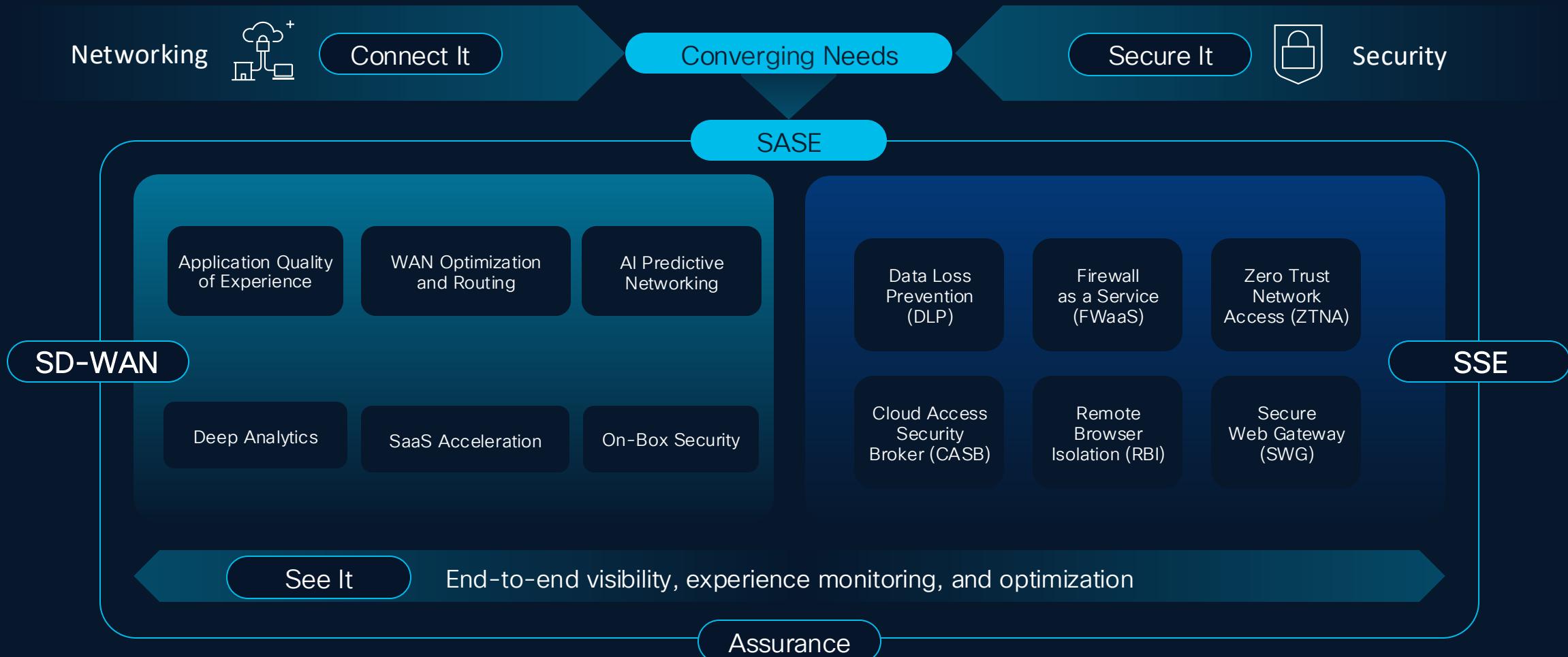
# Secure Access Service Edge (SASE)

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



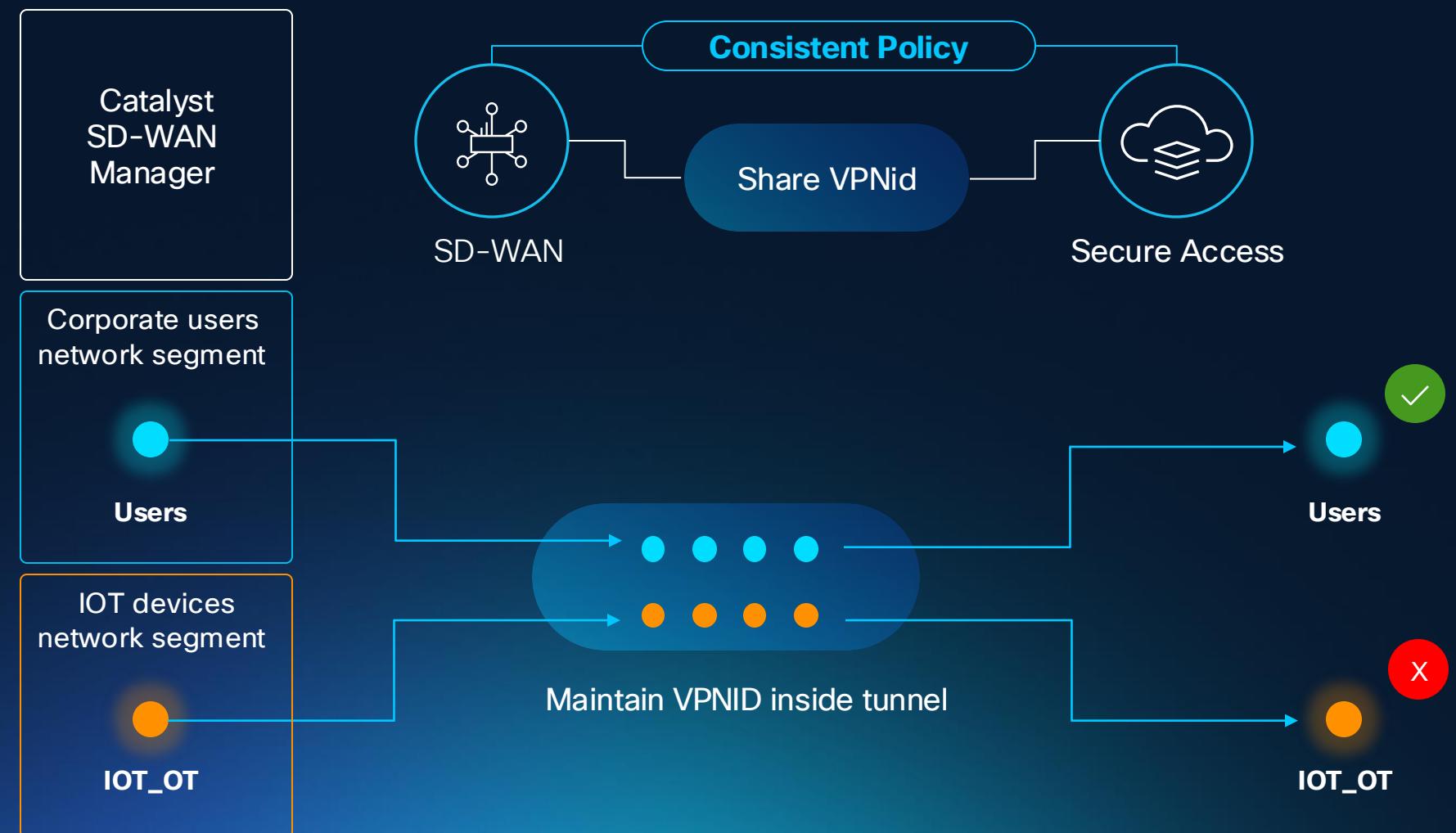
# SASE with Cisco



# Catalyst SD-WAN

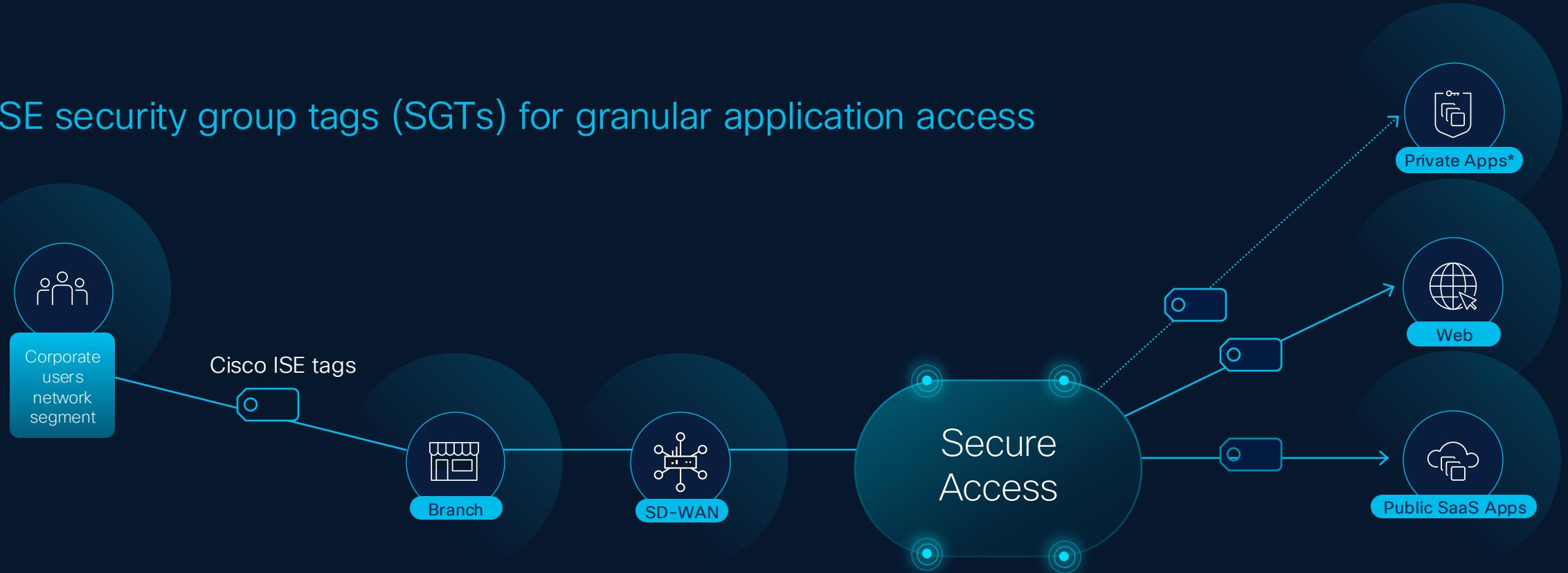
## VPNid support for consistent segmentation

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



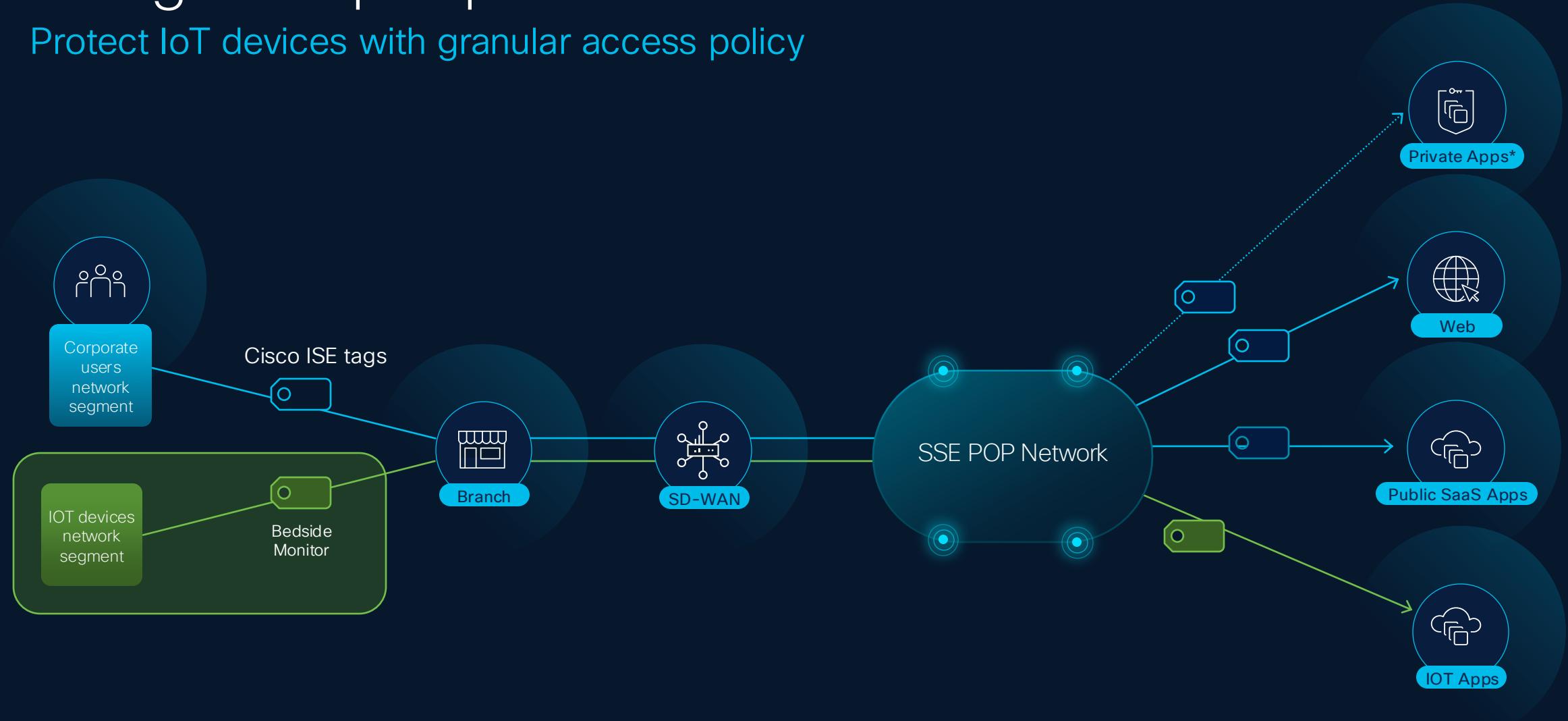
# SD-WAN+ISE+Secure Access = Secure the Branch

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

INTELLIGENT



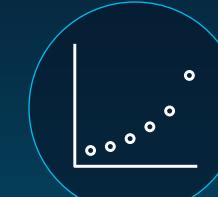
See

SECURE



Protect

ASSURED



Perform

- 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

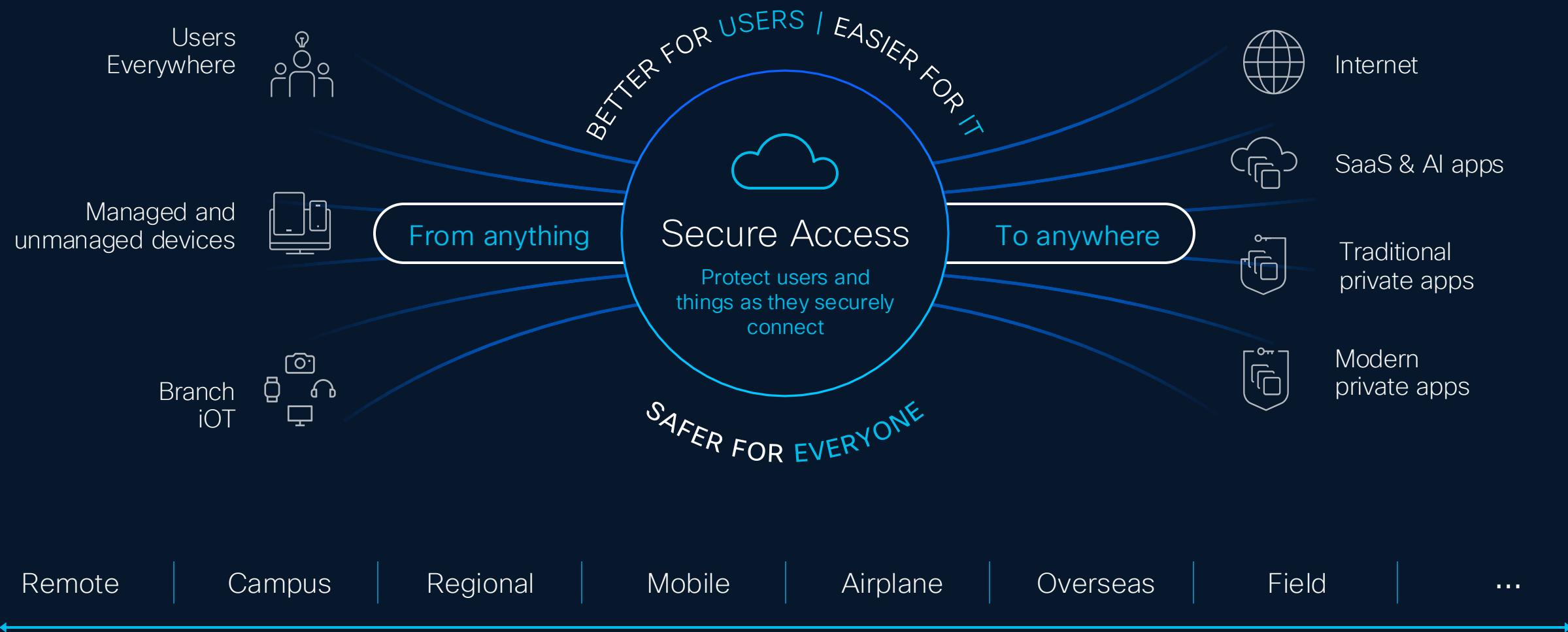
# What's driving interest in security service edge (SSE)?

- 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

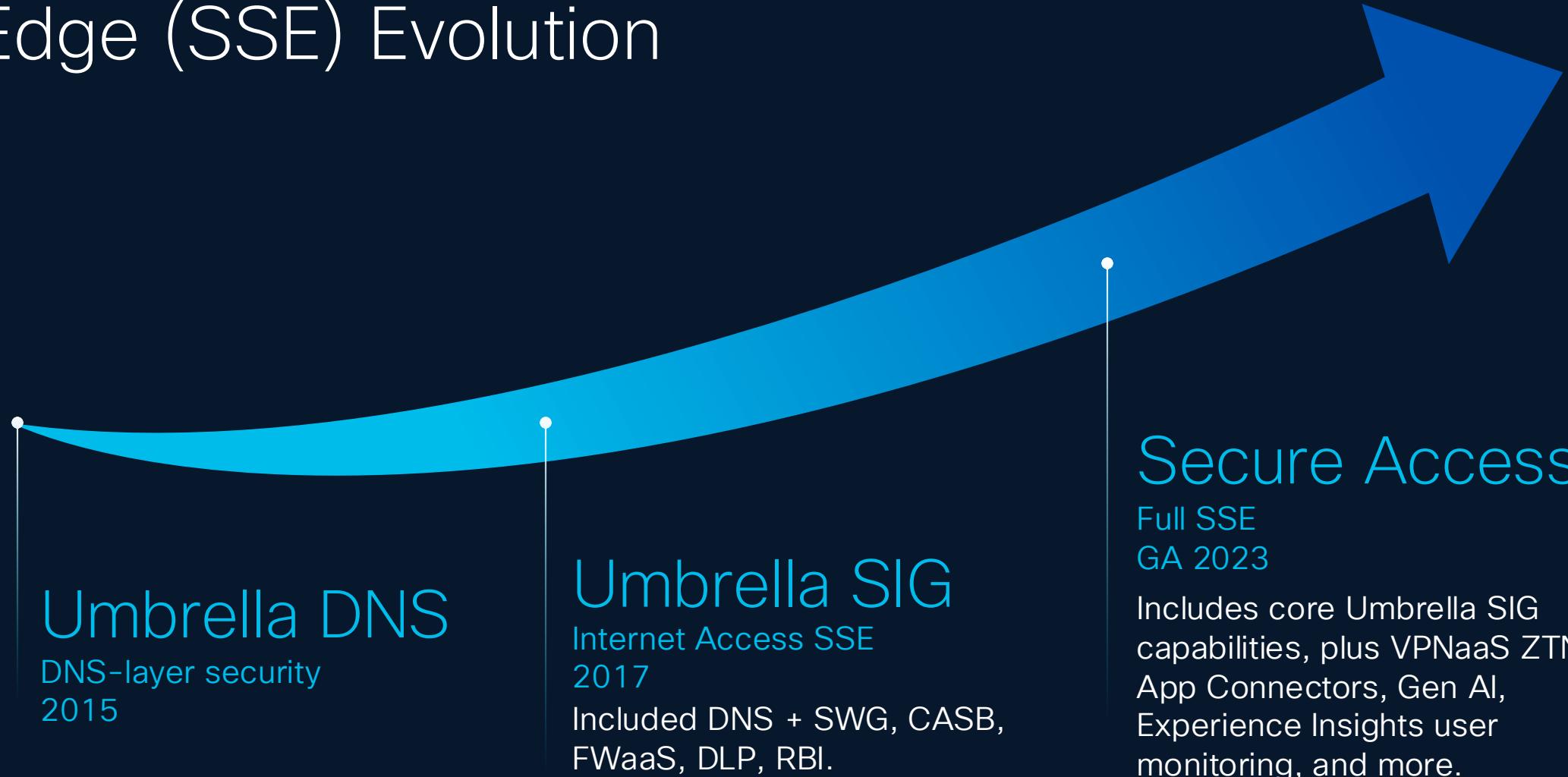
Tool sprawl and complexity are increasing risk and decreasing productivity

# 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



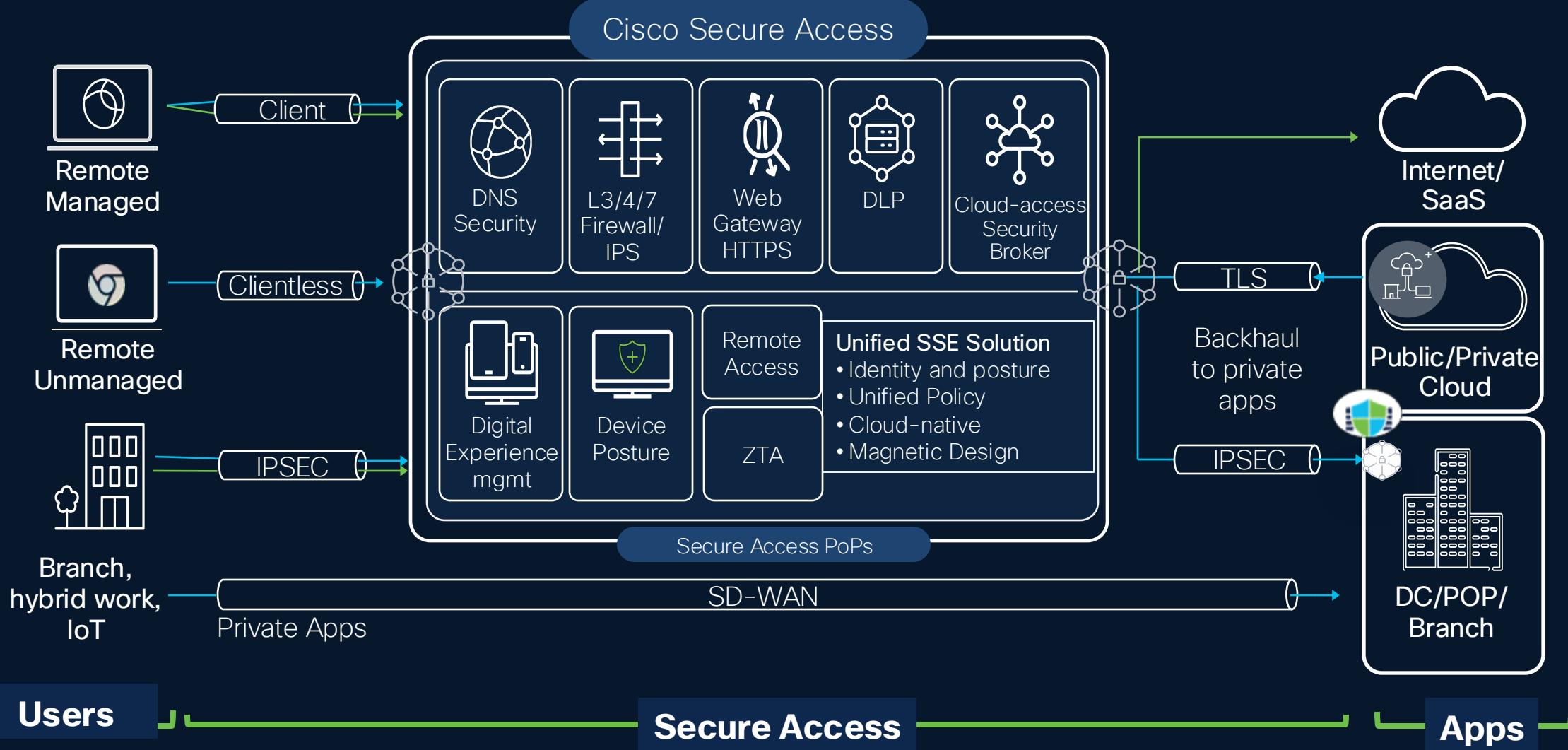
## So much more

- 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

Per Application Access  
DC1 & DC2 , Cloud

VPN Tunnel  
Server Initiated traffic

Secure Access

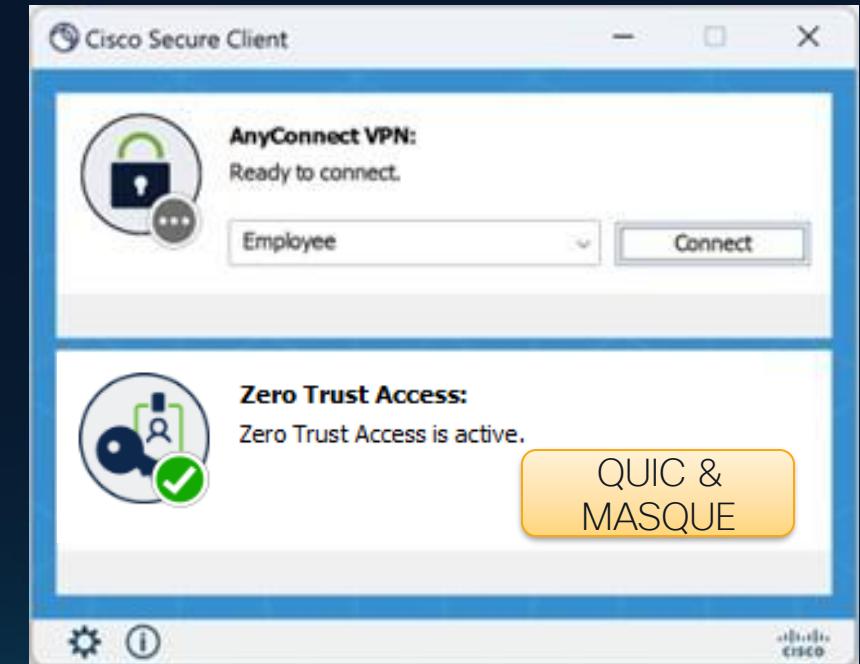
SaaS apps

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



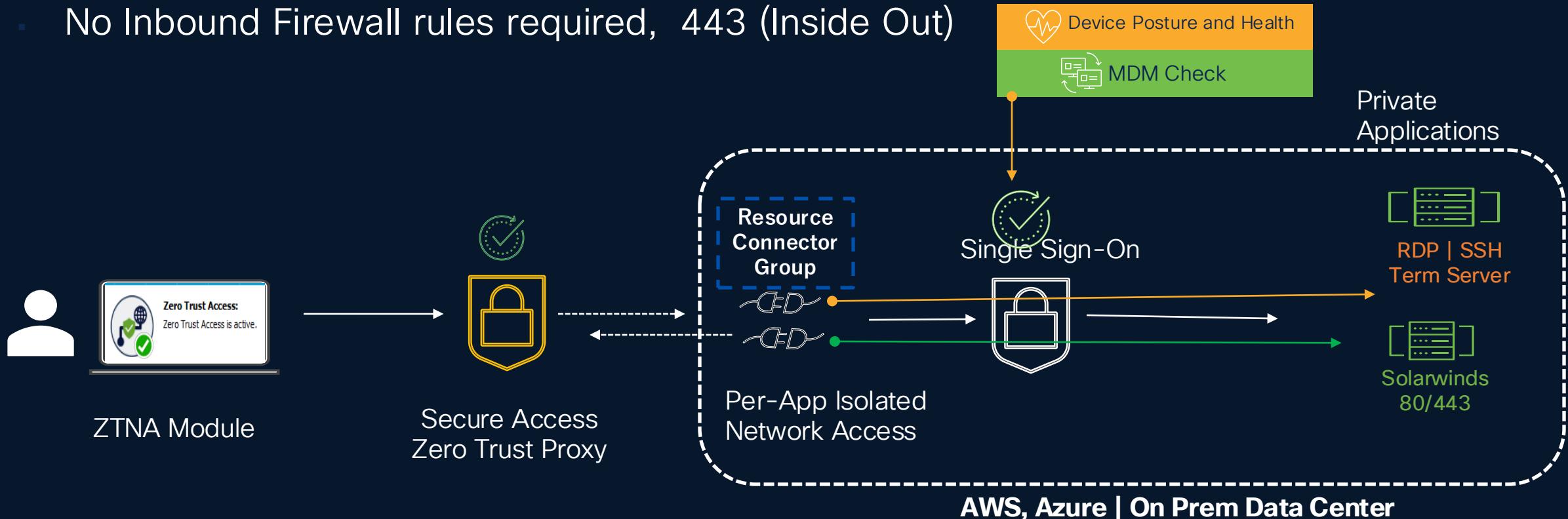
Webex



# Cisco ZTNA – Modern Approach > VPN DTLS

## Benefits:

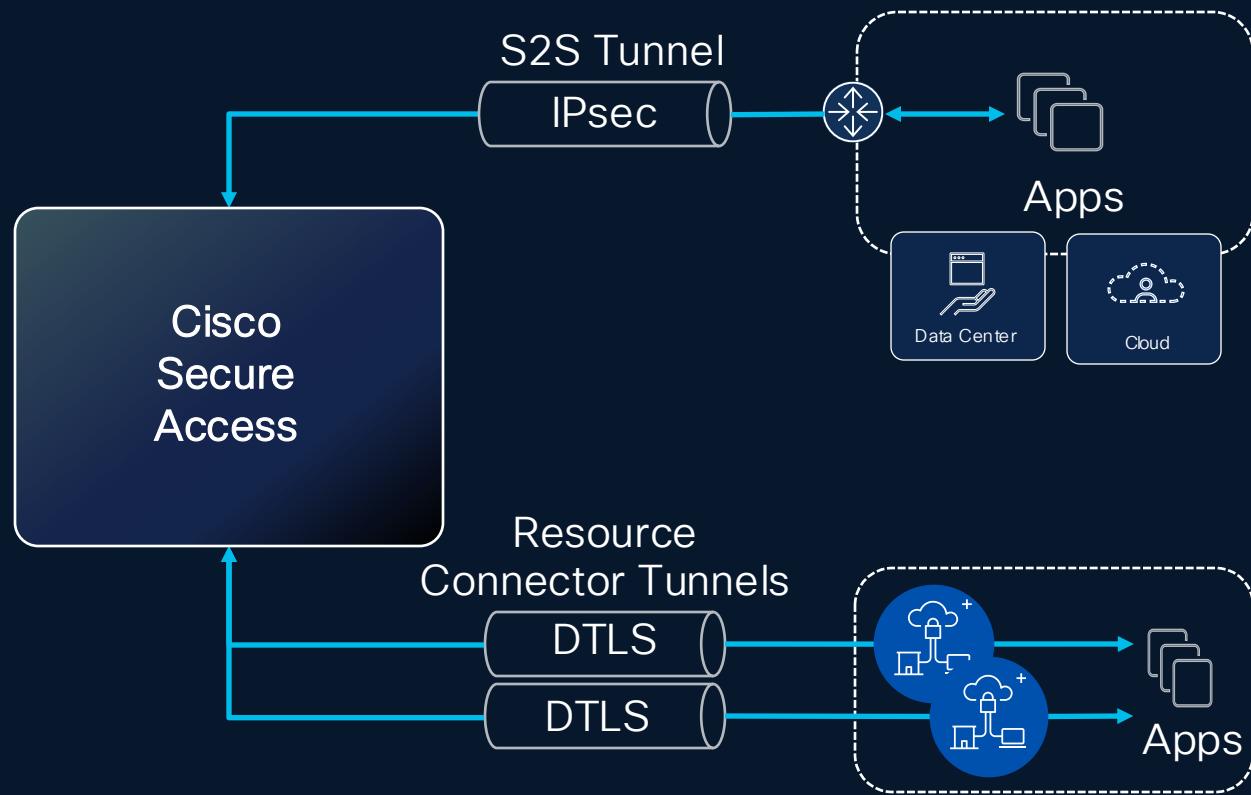
- Identity to Application Access (Zero Trust Principles)
- No direct resource access (forward proxy architecture)
- No Inbound Firewall rules required, 443 (Inside Out)



# 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

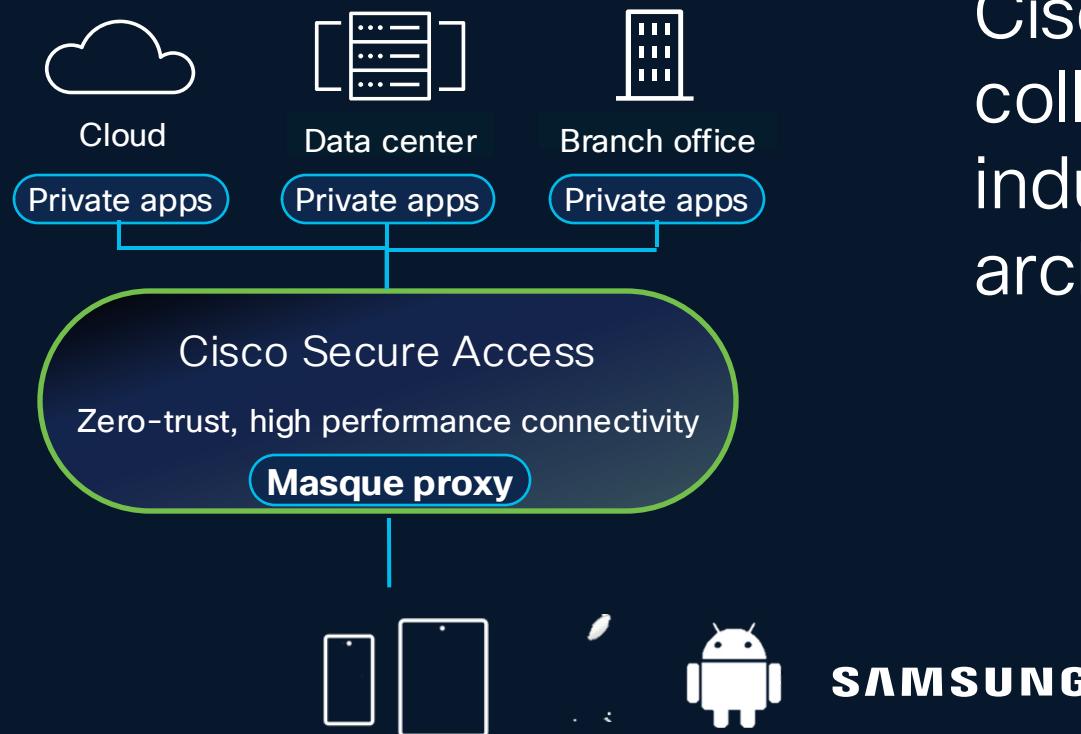
- Available
- Coming Soon
- Subject to Demand

# Secure Access Regions – DCv2 (Physical Edge DC)



# 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

Secure Access

Sam Sanchez

Experience Insights

Powered by ThousandEyes®

Monitor your end users' experiences when accessing resources with a view into endpoint, application, and network performance. Use the correlated data to resolve issues and improve user interactions.

Last updated May 20, 2025, 12:15

Summary AI Insights New

Endpoints summary

Number of endpoints 12 registered / — total

8 Online 0 Unhealthy 5 At Risk 3 Healthy

Health status

All Unhealthy At Risk Healthy

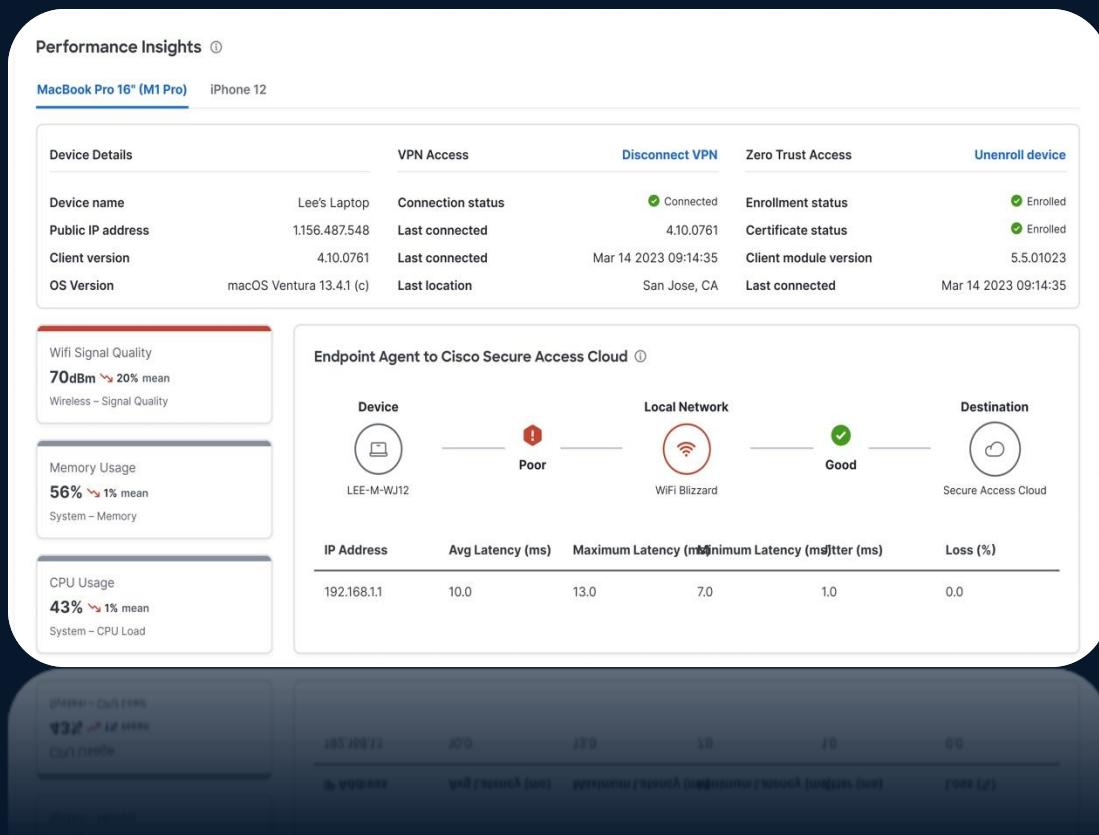
User name	Location	Health status	Device name	ThousandEyes agent version	Latency	Jitter	Loss	WiFi	Ethernet	CPU	Memory	OS	Test time
bhargavp	Portland, Oregon, US	Offline	BHARGAVP-M-7VY9	2.3.1	—	—	—	—	—	—	—	macOS 15.5 Sequoia	—
briannagilchrist	Ann Arbor, Michigan, US	At Risk	BRGILCHR-M-QRC6	2.3.1	77 ms	2 ms	0.00%	100%	—	27.65%	86.21%	macOS 15.4.1 Sequoia	May 20, 2025 12:13PM
seanmi	Baltimore, Maryland, US	Offline	CSCO-W-PF395EGE	1.178.1	—	—	—	—	—	—	—	Microsoft Windows 11 Enterprise	—
lucafern	District of Columbia, US	Offline	dem-client-vm-1	1.200.1	—	—	—	—	—	—	—	Microsoft Windows Server 2019 Datacenter	—

## 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



The screenshot shows the 'Performance Insights' section of the Cisco Secure Access Cloud interface. It includes a table of device details, a 'Wifi Signal Quality' card (70 dBm, 20% mean), a 'Memory Usage' card (56%, 1% mean), a 'CPU Usage' card (43%, 1% mean), and a 'Endpoint Agent to Cisco Secure Access Cloud' diagram. The diagram shows a 'Device' (LEE-M-WJ12) with a 'Poor' connection to a 'Local Network' (WiFi Blizzard) which is 'Good', and a connection to a 'Destination' (Secure Access Cloud) which is 'Good'. Below the diagram is a table of network performance metrics: IP Address (192.168.1.1), Avg Latency (ms) (10.0), Maximum Latency (ms) (13.0), Minimum Latency (ms) (7.0), Jitter (ms) (1.0), and Loss (%) (0.0).

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

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

## Consistent Security Enforcement

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

Balanced Security and Connectivity Default IPS Profile		
Prevention	Block (9353)	Log Only (488)
Blocked IPS signatures are always blocked and logged as a threat.	Ignore (40380)	
Signatures		
• MALWARE-BACKDOOR serveme runtime detection		
• MALWARE-BACKDOOR remote hack 1.5 runtime detection - logon		
• MALWARE-BACKDOOR remote hack 1.5 runtime detection - execute file		
• MALWARE-BACKDOOR remote hack 1.5 runtime detection - get password		
• MALWARE-BACKDOOR remote hack 1.5 runtime detection - start keylogger		

## 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

The screenshot shows the Cisco Secure Access dashboard. The main area displays the 'Access Policy' section, which includes a search bar and filters for Intent, Objects, Security, and Hits. Below this is a table titled '894 Rules' showing various access rules with columns for Rule name, Access, Action, Sources, and Destinations. A sidebar on the right is titled 'Cisco Assistant Beta' and contains a 'Let's create some access rules today, shall we?' section with a text input field and suggestions for creating rules. The sidebar also includes sections for 'Create a single rule' and 'Create multiple rules'.

Better Efficacy.

Better Experience.

Better Economics.

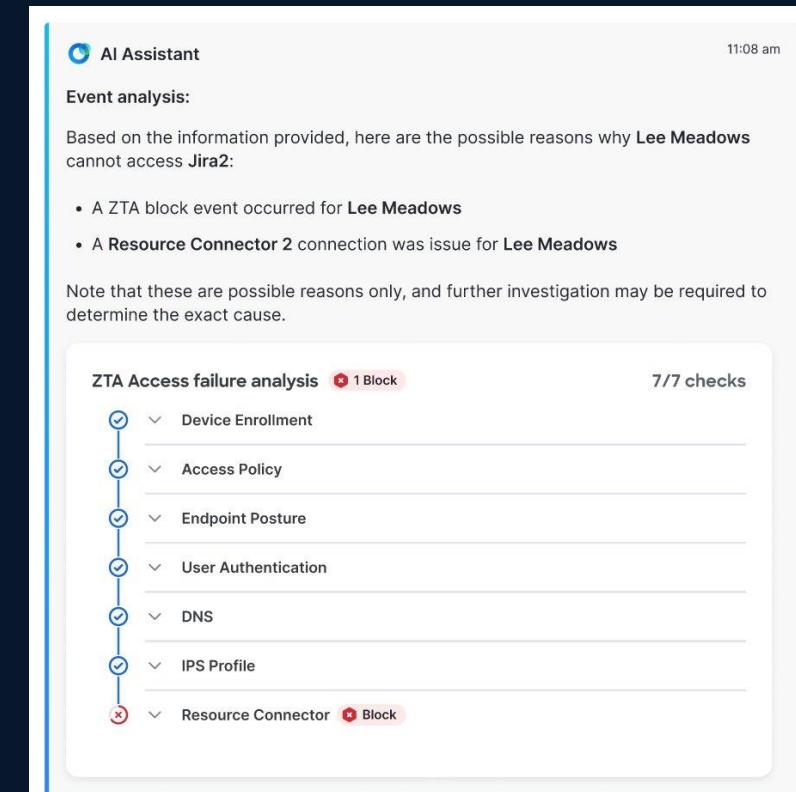
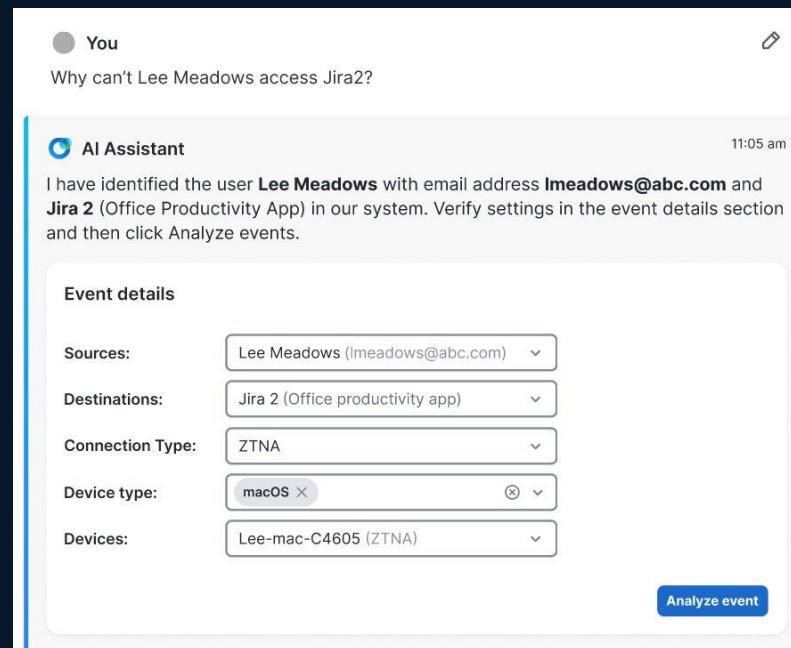
# Troubleshooting Assistant

Automate troubleshooting Secure Access

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

Prompts:

“Why can't Lee Parker access Jira”

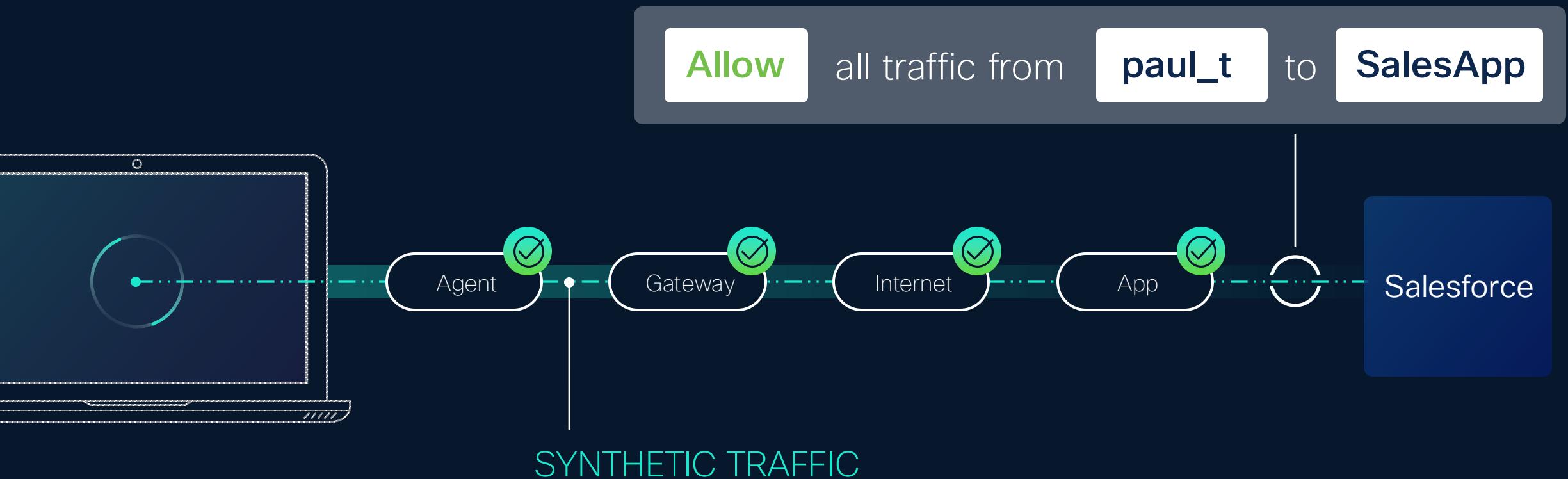




of outages are from  
misconfigurations

# 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

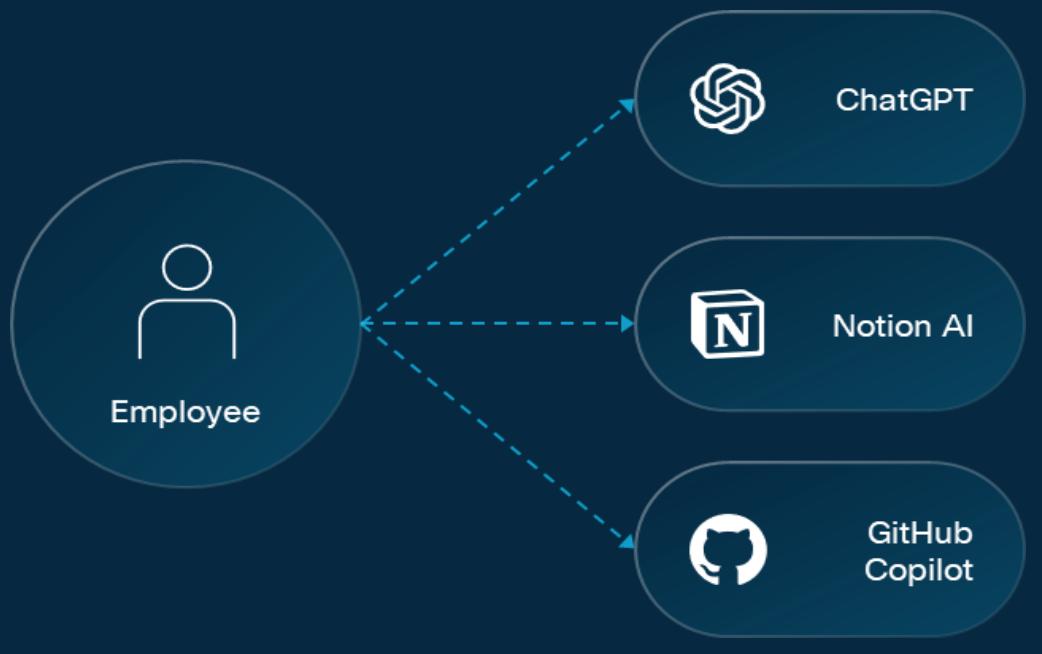


**41%** do not have mature controls on data used to train AI models

# Two distinct areas of AI risk

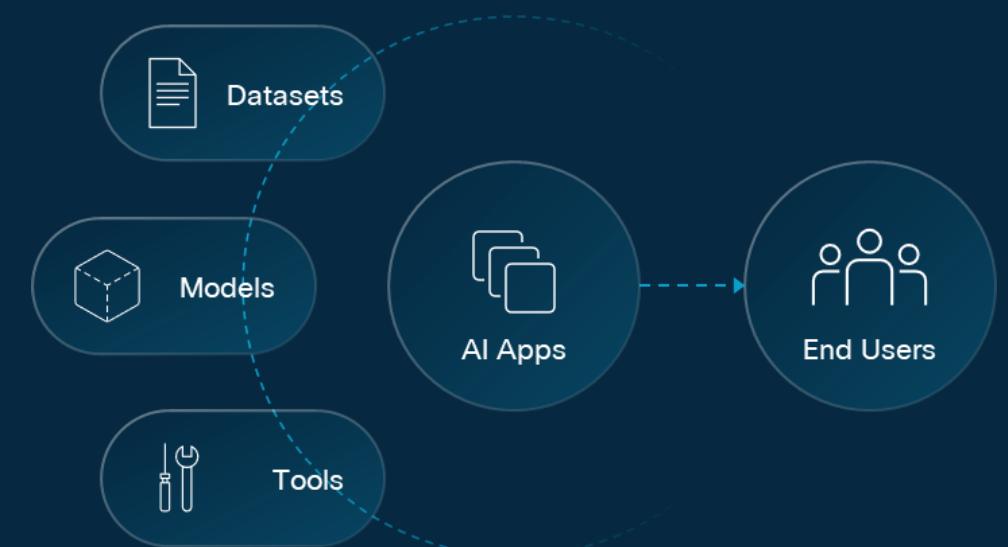
## Third-Party AI Tools – AI Access with Secure Access

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



## 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 <span>New</span>	High	Dec 29, 2024
Code Copilot <span>New</span>	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](#)

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** 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**

Search in Data 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**

**Select All**

**Event Type** **Priority** **Details** **Actions** **Alerts** **Deleted**

Event Type	Priority	Details	Actions	Alerts	Deleted
File	High	File 1, 2024-12-01 10:00:00	Block	File 1, 2024-12-01 10:00:00	
File	High	File 2, 2024-12-01 10:00:00	Block	File 2, 2024-12-01 10:00:00	
File	High	File 3, 2024-12-01 10:00:00	Block	File 3, 2024-12-01 10:00:00	
File	High	File 4, 2024-12-01 10:00:00	Block	File 4, 2024-12-01 10:00:00	
File	High	File 5, 2024-12-01 10:00:00	Block	File 5, 2024-12-01 10:00:00	
File	High	File 6, 2024-12-01 10:00:00	Block	File 6, 2024-12-01 10:00:00	
File	High	File 7, 2024-12-01 10:00:00	Block	File 7, 2024-12-01 10:00:00	
File	High	File 8, 2024-12-01 10:00:00	Block	File 8, 2024-12-01 10:00:00	
File	High	File 9, 2024-12-01 10:00:00	Block	File 9, 2024-12-01 10:00:00	
File	High	File 10, 2024-12-01 10:00:00	Block	File 10, 2024-12-01 10:00:00	
File	High	File 11, 2024-12-01 10:00:00	Block	File 11, 2024-12-01 10:00:00	
File	High	File 12, 2024-12-01 10:00:00	Block	File 12, 2024-12-01 10:00:00	
File	High	File 13, 2024-12-01 10:00:00	Block	File 13, 2024-12-01 10:00:00	
File	High	File 14, 2024-12-01 10:00:00	Block	File 14, 2024-12-01 10:00:00	
File	High	File 15, 2024-12-01 10:00:00	Block	File 15, 2024-12-01 10:00:00	
File	High	File 16, 2024-12-01 10:00:00	Block	File 16, 2024-12-01 10:00:00	
File	High	File 17, 2024-12-01 10:00:00	Block	File 17, 2024-12-01 10:00:00	
File	High	File 18, 2024-12-01 10:00:00	Block	File 18, 2024-12-01 10:00:00	
File	High	File 19, 2024-12-01 10:00:00	Block	File 19, 2024-12-01 10:00:00	
File	High	File 20, 2024-12-01 10:00:00	Block	File 20, 2024-12-01 10:00:00	
File	High	File 21, 2024-12-01 10:00:00	Block	File 21, 2024-12-01 10:00:00	
File	High	File 22, 2024-12-01 10:00:00	Block	File 22, 2024-12-01 10:00:00	
File	High	File 23, 2024-12-01 10:00:00	Block	File 23, 2024-12-01 10:00:00	
File	High	File 24, 2024-12-01 10:00:00	Block	File 24, 2024-12-01 10:00:00	
File	High	File 25, 2024-12-01 10:00:00	Block	File 25, 2024-12-01 10:00:00	
File	High	File 26, 2024-12-01 10:00:00	Block	File 26, 2024-12-01 10:00:00	
File	High	File 27, 2024-12-01 10:00:00	Block	File 27, 2024-12-01 10:00:00	
File	High	File 28, 2024-12-01 10:00:00	Block	File 28, 2024-12-01 10:00:00	
File	High	File 29, 2024-12-01 10:00:00	Block	File 29, 2024-12-01 10:00:00	
File	High	File 30, 2024-12-01 10:00:00	Block	File 30, 2024-12-01 10:00:00	
File	High	File 31, 2024-12-01 10:00:00	Block	File 31, 2024-12-01 10:00:00	
File	High	File 32, 2024-12-01 10:00:00	Block	File 32, 2024-12-01 10:00:00	
File	High	File 33, 2024-12-01 10:00:00	Block	File 33, 2024-12-01 10:00:00	
File	High	File 34, 2024-12-01 10:00:00	Block	File 34, 2024-12-01 10:00:00	
File	High	File 35, 2024-12-01 10:00:00	Block	File 35, 2024-12-01 10:00:00	
File	High	File 36, 2024-12-01 10:00:00	Block	File 36, 2024-12-01 10:00:00	
File	High	File 37, 2024-12-01 10:00:00	Block	File 37, 2024-12-01 10:00:00	
File	High	File 38, 2024-12-01 10:00:00	Block	File 38, 2024-12-01 10:00:00	
File	High	File 39, 2024-12-01 10:00:00	Block	File 39, 2024-12-01 10:00:00	
File	High	File 40, 2024-12-01 10:00:00	Block	File 40, 2024-12-01 10:00:00	
File	High	File 41, 2024-12-01 10:00:00	Block	File 41, 2024-12-01 10:00:00	
File	High	File 42, 2024-12-01 10:00:00	Block	File 42, 2024-12-01 10:00:00	
File	High	File 43, 2024-12-01 10:00:00	Block	File 43, 2024-12-01 10:00:00	
File	High	File 44, 2024-12-01 10:00:00	Block	File 44, 2024-12-01 10:00:00	
File	High	File 45, 2024-12-01 10:00:00	Block	File 45, 2024-12-01 10:00:00	
File	High	File 46, 2024-12-01 10:00:00	Block	File 46, 2024-12-01 10:00:00	
File	High	File 47, 2024-12-01 10:00:00	Block	File 47, 2024-12-01 10:00:00	
File	High	File 48, 2024-12-01 10:00:00	Block	File 48, 2024-12-01 10:00:00	
File	High	File 49, 2024-12-01 10:00:00	Block	File 49, 2024-12-01 10:00:00	
File	High	File 50, 2024-12-01 10:00:00	Block	File 50, 2024-12-01 10:00:00	
File	High	File 51, 2024-12-01 10:00:00	Block	File 51, 2024-12-01 10:00:00	
File	High	File 52, 2024-12-01 10:00:00	Block	File 52, 2024-12-01 10:00:00	
File	High	File 53, 2024-12-01 10:00:00	Block	File 53, 2024-12-01 10:00:00	
File	High	File 54, 2024-12-01 10:00:00	Block	File 54, 2024-12-01 10:00:00	
File	High	File 55, 2024-12-01 10:00:00	Block	File 55, 2024-12-01 10:00:00	
File	High	File 56, 2024-12-01 10:00:00	Block	File 56, 2024-12-01 10:00:00	
File	High	File 57, 2024-12-01 10:00:00	Block	File 57, 2024-12-01 10:00:00	
File	High	File 58, 2024-12-01 10:00:00	Block	File 58, 2024-12-01 10:00:00	
File	High	File 59, 2024-12-01 10:00:00	Block	File 59, 2024-12-01 10:00:00	
File	High	File 60, 2024-12-01 10:00:00	Block	File 60, 2024-12-01 10:00:00	
File	High	File 61, 2024-12-01 10:00:00	Block	File 61, 2024-12-01 10:00:00	
File	High	File 62, 2024-12-01 10:00:00	Block	File 62, 2024-12-01 10:00:00	
File	High	File 63, 2024-12-01 10:00:00	Block	File 63, 2024-12-01 10:00:00	
File	High	File 64, 2024-12-01 10:00:00	Block	File 64, 2024-12-01 10:00:00	
File	High	File 65, 2024-12-01 10:00:00	Block	File 65, 2024-12-01 10:00:00	
File	High	File 66, 2024-12-01 10:00:00	Block	File 66, 2024-12-01 10:00:00	
File	High	File 67, 2024-12-01 10:00:00	Block	File 67, 2024-12-01 10:00:00	
File	High	File 68, 2024-12-01 10:00:00	Block	File 68, 2024-12-01 10:00:00	
File	High	File 69, 2024-12-01 10:00:00	Block	File 69, 2024-12-01 10:00:00	
File	High	File 70, 2024-12-01 10:00:00	Block	File 70, 2024-12-01 10:00:00	
File	High	File 71, 2024-12-01 10:00:00	Block	File 71, 2024-12-01 10:00:00	
File	High	File 72, 2024-12-01 10:00:00	Block	File 72, 2024-12-01 10:00:00	
File	High	File 73, 2024-12-01 10:00:00	Block	File 73, 2024-12-01 10:00:00	
File	High	File 74, 2024-12-01 10:00:00	Block	File 74, 2024-12-01 10:00:00	
File	High	File 75, 2024-12-01 10:00:00	Block	File 75, 2024-12-01 10:00:00	
File	High	File 76, 2024-12-01 10:00:00	Block	File 76, 2024-12-01 10:00:00	
File	High	File 77, 2024-12-01 10:00:00	Block	File 77, 2024-12-01 10:00:00	
File	High	File 78, 2024-12-01 10:00:00	Block	File 78, 2024-12-01 10:00:00	
File	High	File 79, 2024-12-01 10:00:00	Block	File 79, 2024-12-01 10:00:00	
File	High	File 80, 2024-12-01 10:00:00	Block	File 80, 2024-12-01 10:00:00	
File	High	File 81, 2024-12-01 10:00:00	Block	File 81, 2024-12-01 10:00:00	
File	High	File 82, 2024-12-01 10:00:00	Block	File 82, 2024-12-01 10:00:00	
File	High	File 83, 2024-12-01 10:00:00	Block	File 83, 2024-12-01 10:00:00	
File	High	File 84, 2024-12-01 10:00:00	Block	File 84, 2024-12-01 10:00:00	
File	High	File 85, 2024-12-01 10:00:00	Block	File 85, 2024-12-01 10:00:00	
File	High	File 86, 2024-12-01 10:00:00	Block	File 86, 2024-12-01 10:00:00	
File	High	File 87, 2024-12-01 10:00:00	Block	File 87, 2024-12-01 10:00:00	
File	High	File 88, 2024-12-01 10:00:00	Block	File 88, 2024-12-01 10:00:00	
File	High	File 89, 2024-12-01 10:00:00	Block	File 89, 2024-12-01 10:00:00	
File	High	File 90, 2024-12-01 10:00:00	Block	File 90, 2024-12-01 10:00:00	
File	High	File 91, 2024-12-01 10:00:00	Block	File 91, 2024-12-01 10:00:00	
File	High	File 92, 2024-12-01 10:00:00	Block	File 92, 2024-12-01 10:00:00	
File	High	File 93, 2024-12-01 10:00:00	Block	File 93, 2024-12-01 10:00:00	
File	High	File 94, 2024-12-01 10:00:00	Block	File 94, 2024-12-01 10:00:00	
File	High	File 95, 2024-12-01 10:00:00	Block	File 95, 2024-12-01 10:00:00	
File	High	File 96, 2024-12-01 10:00:00	Block	File 96, 2024-12-01 10:00:00	
File	High	File 97, 2024-12-01 10:00:00	Block	File 97, 2024-12-01 10:00:00	
File	High	File 98, 2024-12-01 10:00:00	Block	File 98, 2024-12-01 10:00:00	
File	High	File 99, 2024-12-01 10:00:00	Block	File 99, 2024-12-01 10:00:00	
File	High	File 100, 2024-12-01 10:00:00	Block	File 100, 2024-12-01 10:00:00	

# 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	1 Identity	Inclusion 2 Applications	Data Classifications Privacy guardrail	Privacy guardrail	Dec 17, 2024

**Data Classifications**  
Select data classifications to add them to this rule.

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

Discard Mac Binary and AI  
Guardrails, AI Protection

**Data Classification Name**  
AI/ML Monitor

**Description (Optional)**

**Included Data Identifiers**

Source Code

**Secure Access**

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 Overtrials	High	Bob SWG (bob@swginaawsd...	Prompt	Deepseek	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:15 AM
AI Overtrials	Critical	Bob SWG (bob@swginaawsd...	Prompt	Deepseek	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:15 AM
AI Overtrials	Critical	Bob SWG (bob@swginaawsd...	Prompt	Deepseek	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:14 AM
AI Overtrials	High	Bob SWG (bob@swginaawsd...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:14 AM
AI Overtrials	High	Bob SWG (bob@swginaawsd...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:05 AM
AI Overtrials	High	Bob SWG (bob@swginaawsd...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:57 AM
AI Overtrials	High	Bob SWG (bob@swginaawsd...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:48 AM
AI Overtrials	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:41 AM
AI Overtrials	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 Overtrials	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:56 PM
AI Overtrials	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:54 PM

AWS - Access Key

AWS - API Key

AWS - Secret Key

AWS - Session Token

Azure - Access Key

File Name: Form  
Identity: Bob SWG (bob@swginaawsd...  
Application: Deepseek  
Application Category: Generative AI  
Destination URL: http://chat.deepseek.com  
Copy  
Rule: AI monitor  
Severity: High  
Direction: Prompt  
Prompt: Classification  
Classification: Safety guideline  
1 March 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.

# 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

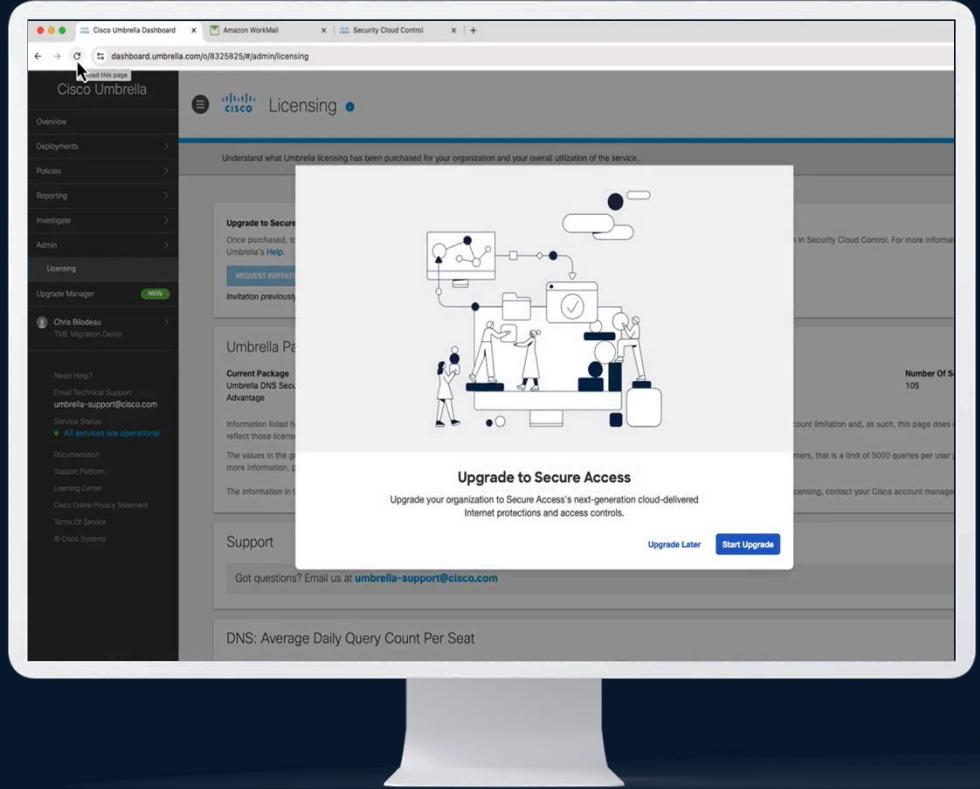
- **Umbrella DNS and SIG Migrations available now**
  - Onboarding guide
  - Vidcast (DNS)

## 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

