CISCO SECURE

The bridge to possible

UTCAL Webinar

Cisco Secure Access

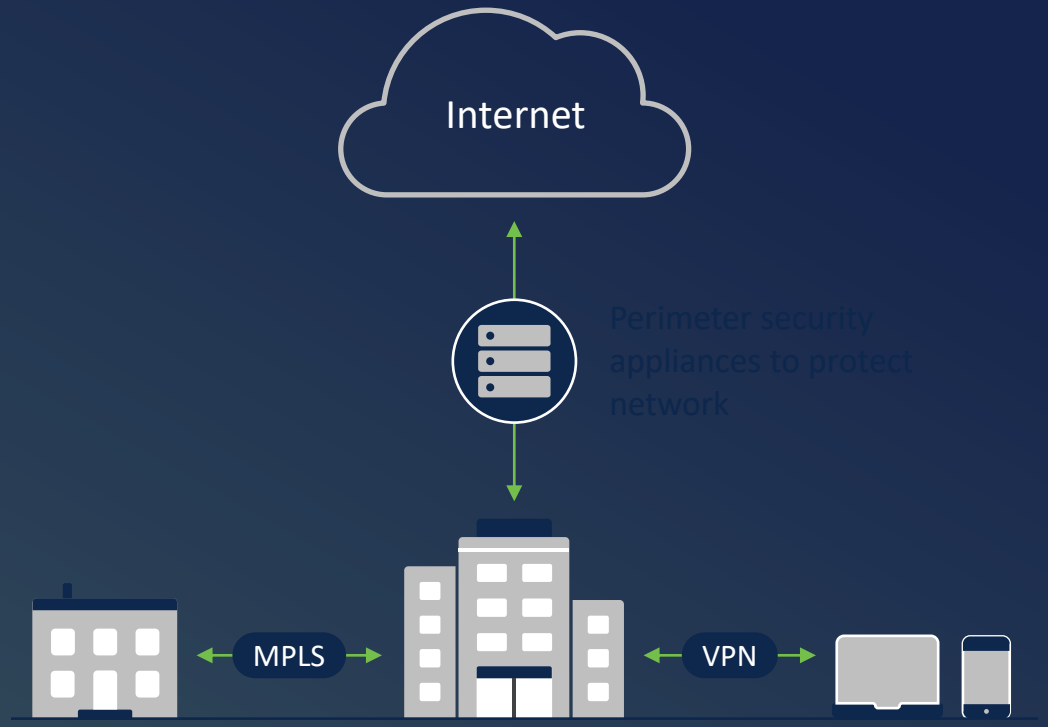
Modernizando a proteção em Infraestrutura crítica de Utilities com Security Services Edge (SSE)

George Almeida
Solutions Engineer – Security Sales – CCIE/CISSP/CISM

10/Jun/2026

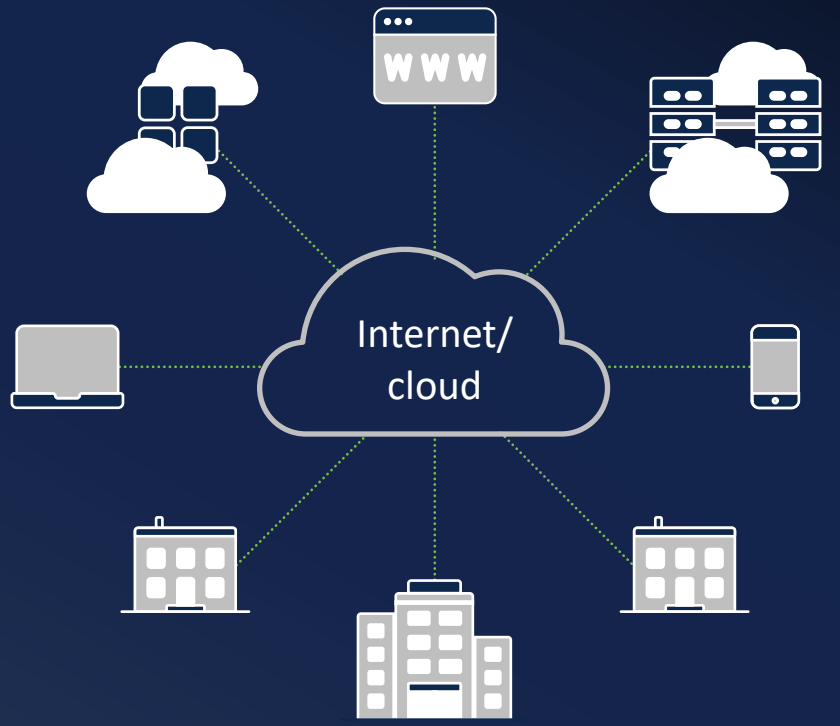
Network Transformation

From



DC-centric

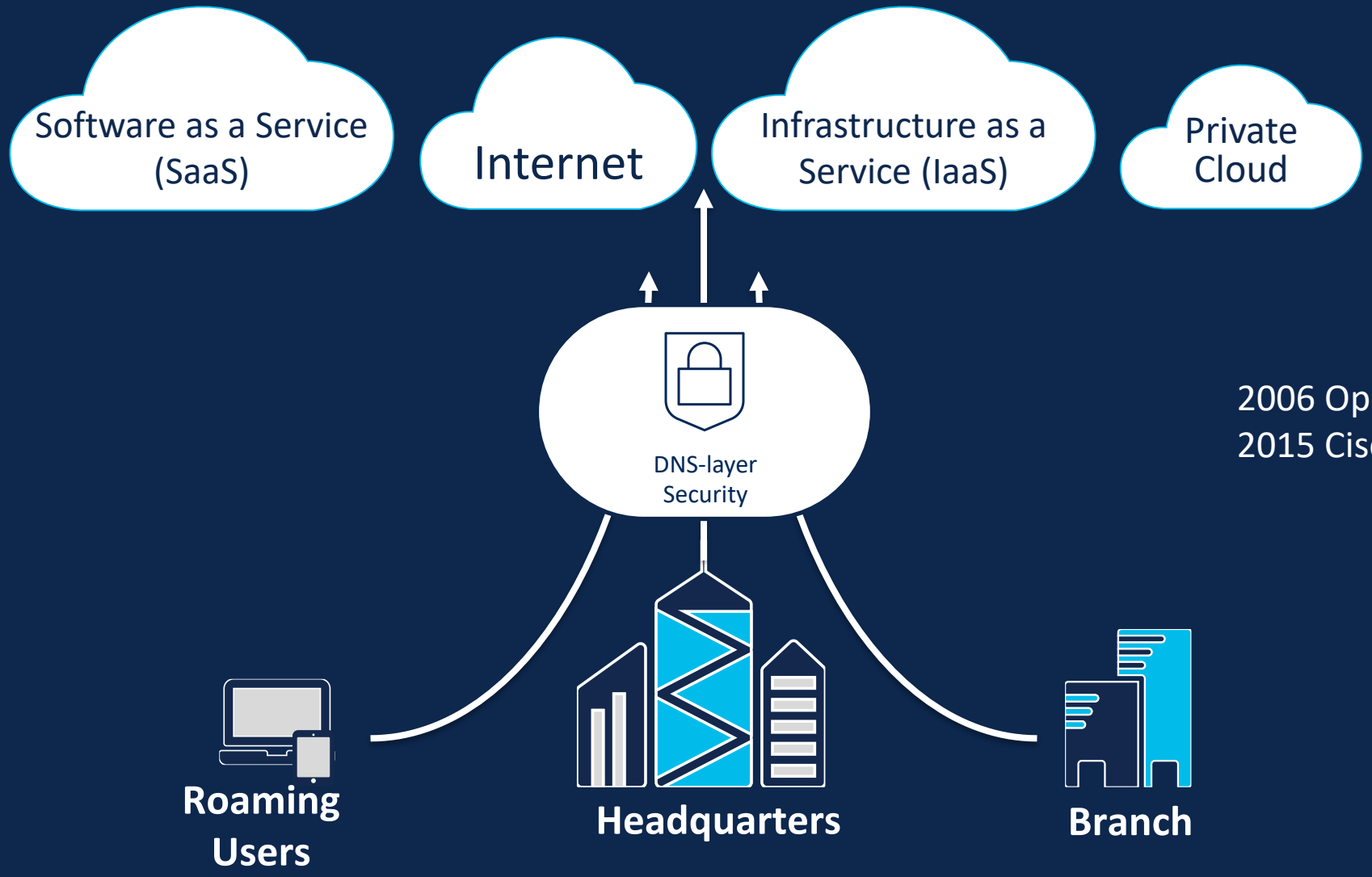
To



Internet/cloud-centric

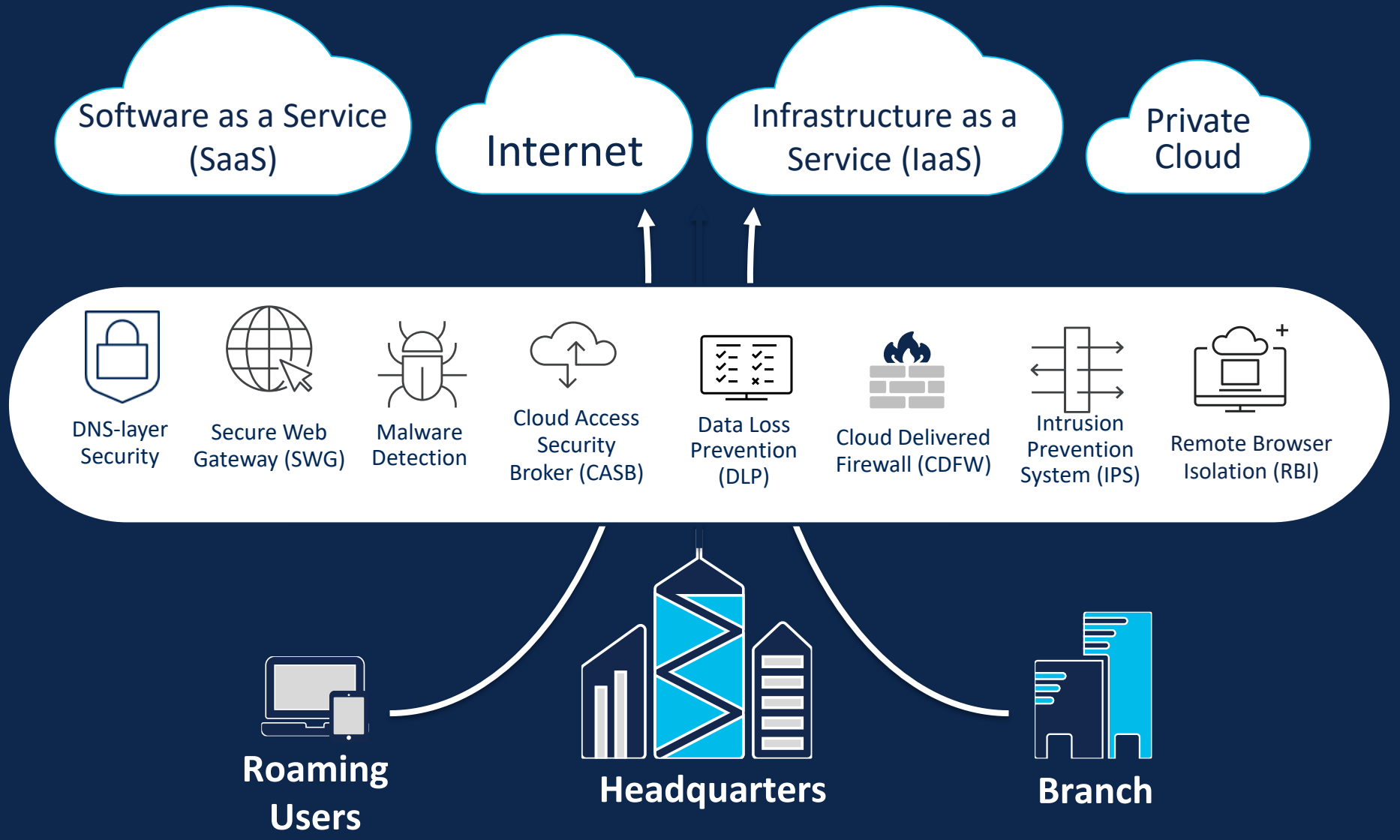
Long history of Cloud Protection

Cisco Umbrella DNS Protection



2006 OpenDNS Launch
2015 Cisco acquisition

Cisco Umbrella Secure Internet Gateway (2017)



Cisco Secure Access (2023)

Full SSE solution

Cisco Security Cloud Control

Unified Security Management

Secure Firewall ASA

Secure Firewall Threat Defense

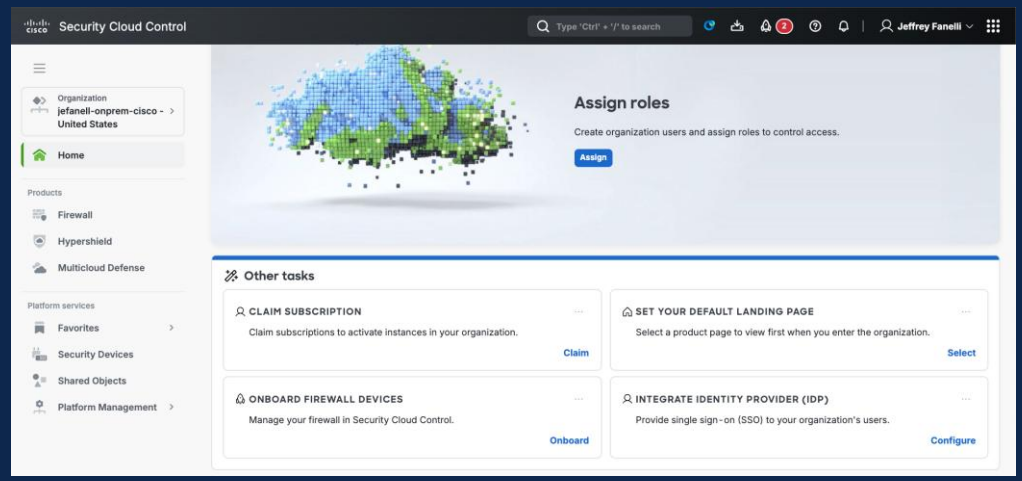
Multicloud Defense

Hypershield

Secure Access

Secure Workload

AI Defense



Integrations

Dynamic Objects

Licensing

Provisioning

Tenancy

User Management

RBAC

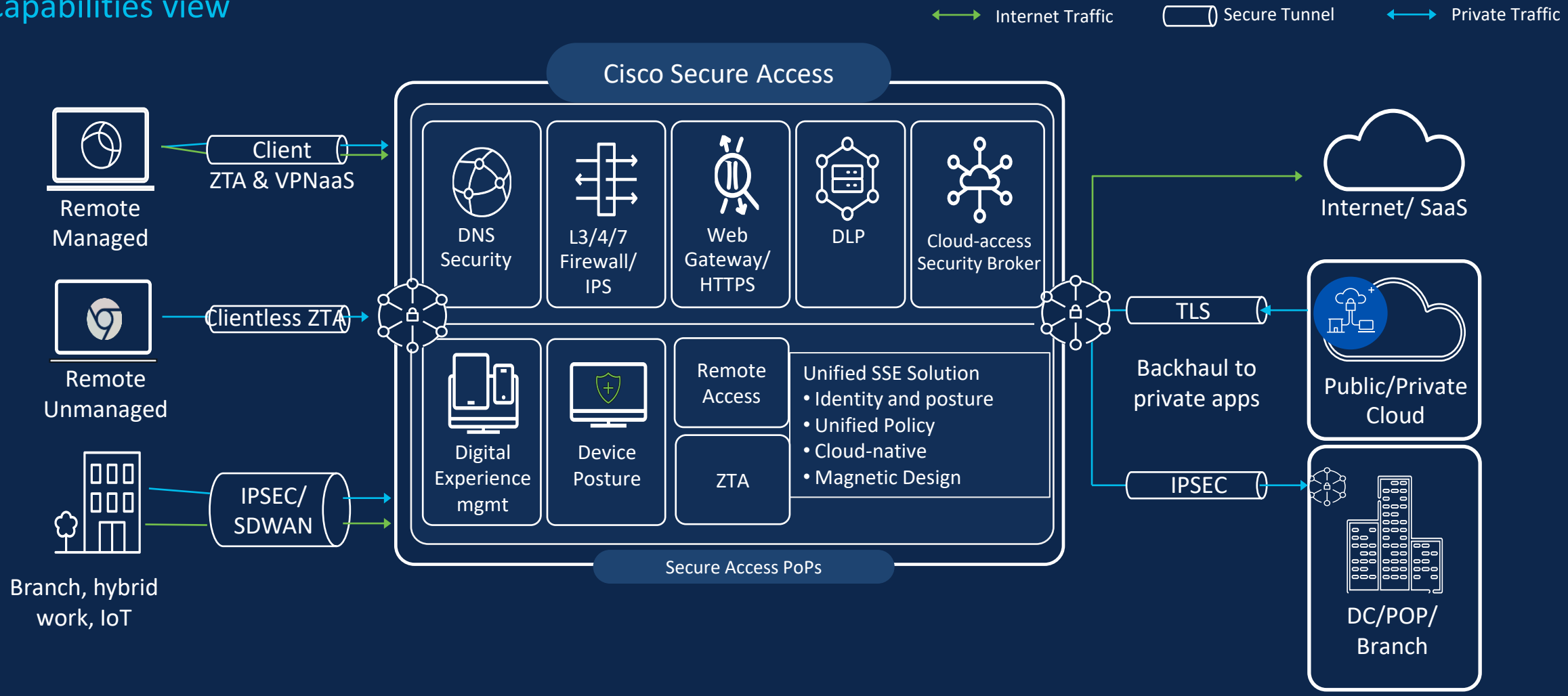
API Gateway

Unified AI Assistant

Common UI Experience

Cisco Secure Access

Capabilities view



Cisco Secure Access- User Anywhere

STEP 1
Log In

STEP 2
Securely start work

ZTA
VPN
SaaS
Direct

Secure Access

Private apps
Traditional apps
SaaS apps
Internet apps

We handle the connectivity, access control and security

Easy, frictionless user experience

Remote User Connectivity Methods

Internet Traffic
Private Traffic
Secure Tunnel

Client-based ZTA

- Authentication and Posture per session
- QUIC tunnel (MASQUE proxy) or TCP/HTTP2
- Private and Internet Traffic (All ports & protocols)
- SAML Auth + Auto re-new or Certificate

Client-based VPNaaS

- Authentication & Posture at Connect time
- TLS, DTLS, or IPsec Tunnel
- Carry **Internet & Private Traffic** (All ports & protocols)
- SAML, (+) Cert, & (+) Multi-Cert Authentication

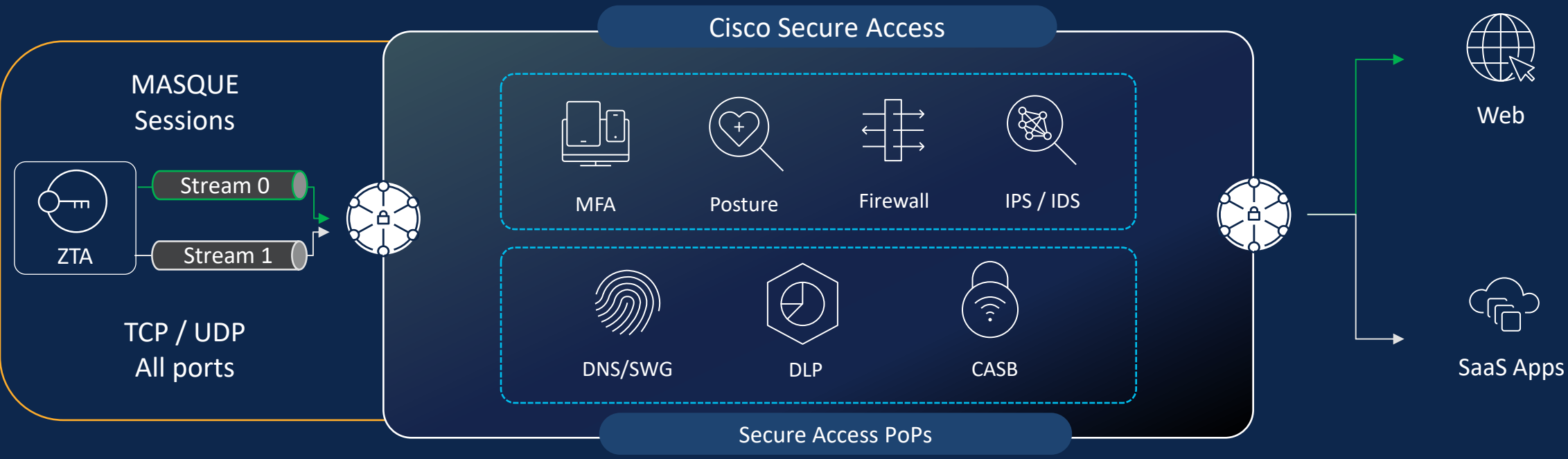
Unmanaged Device

Clientless ZTA

- Accessible from any browser that supports SAML/Cookies
- Request based posture (browser version, OS, geo-location)
- Web applications, `RDP or SSH

Client-based Zero Trust Access

Internet Connectivity

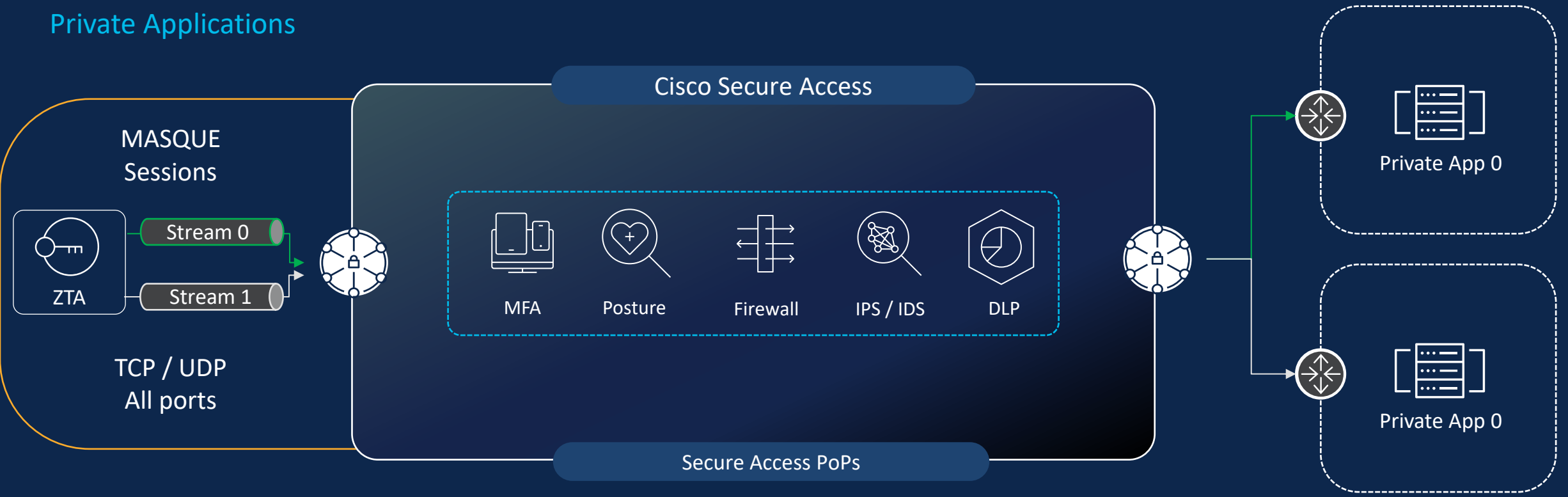


- Transparent user experience
- Trusted Network Detection
- Service managed client certificates with TPM-protected key storage

- Session-based security
- No VPN tunnels
- User and group-packet steering
- User and group-based policy

Client-based Zero Trust Access

Private Applications

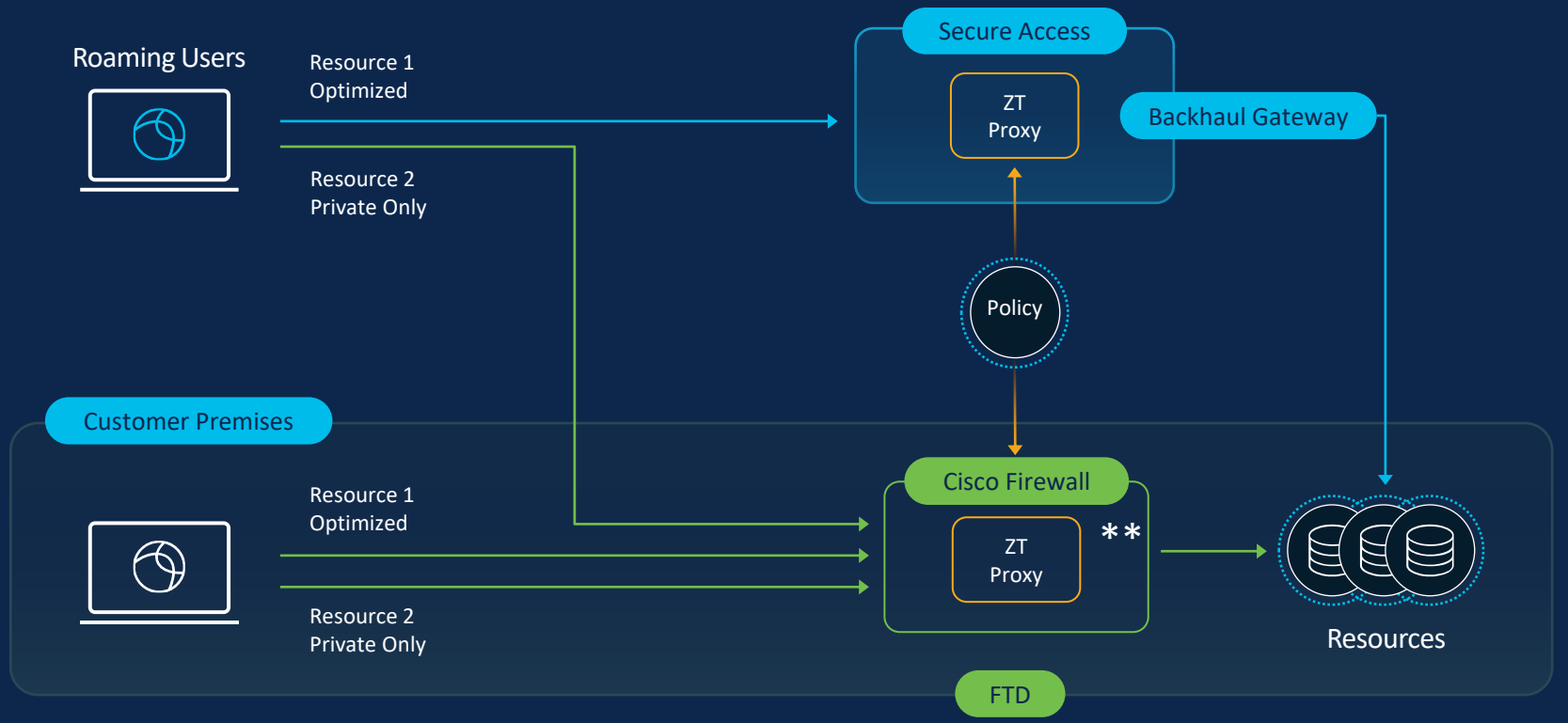


- Transparent user experience
- Forward proxied resource access with coarse or fine-grained access control
- Service managed client certificates with TPM-protected key storage

- Inside to out L4-7 tunnels from RCs
- No routing complexities
- Apps are hidden, supports overlapping subnets
- Easy to scale with high availability

Hybrid Private Access for flexible enforcement

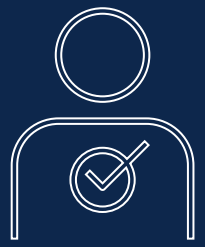
Single set of ZTNA policies used in cloud and on-premise



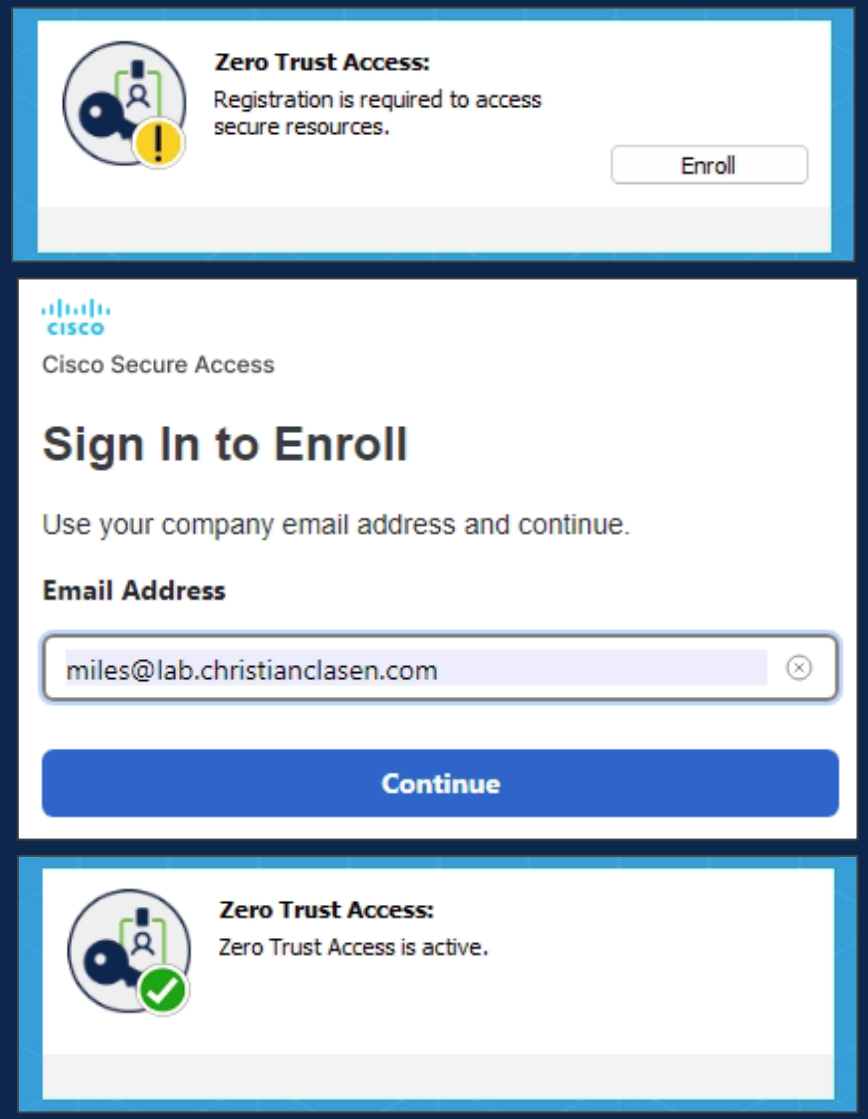
** Roadmap: policy enforcement on 8k routers

Client-based ZTA: Enrollment

Certificate
- No user interaction
- Deploy with MDM
- Bring-your-own Certificate Authority



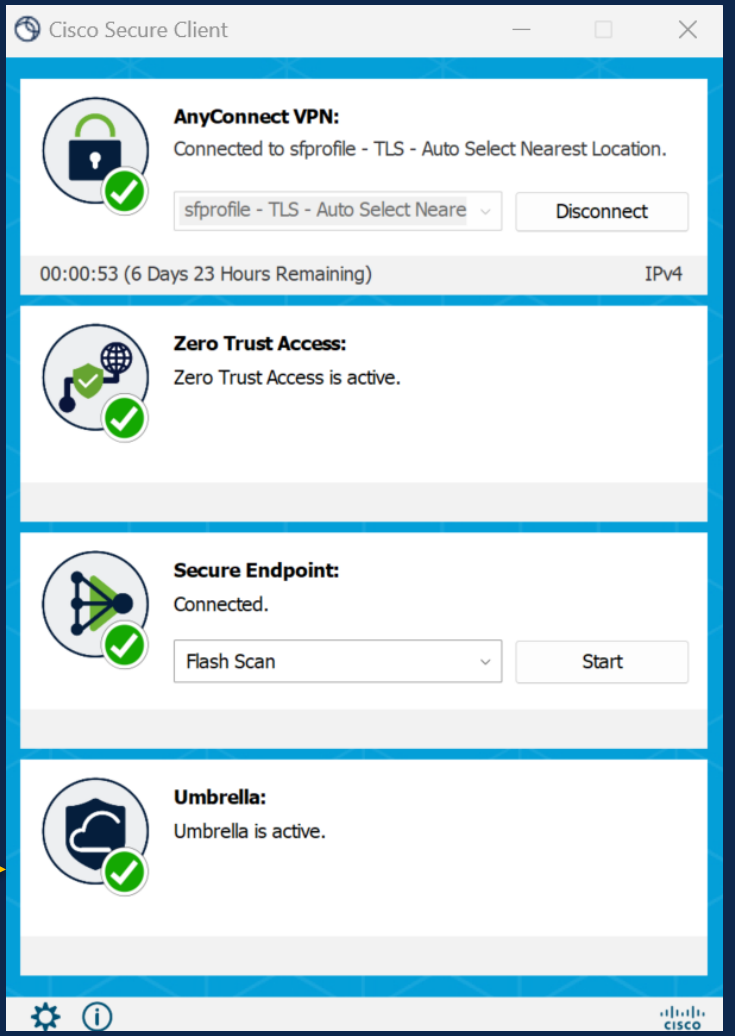
SAML
- User prompted to enroll
- Enforce Multi-Factor Auth
- Multiple Identity Provider support



Cisco Secure Client

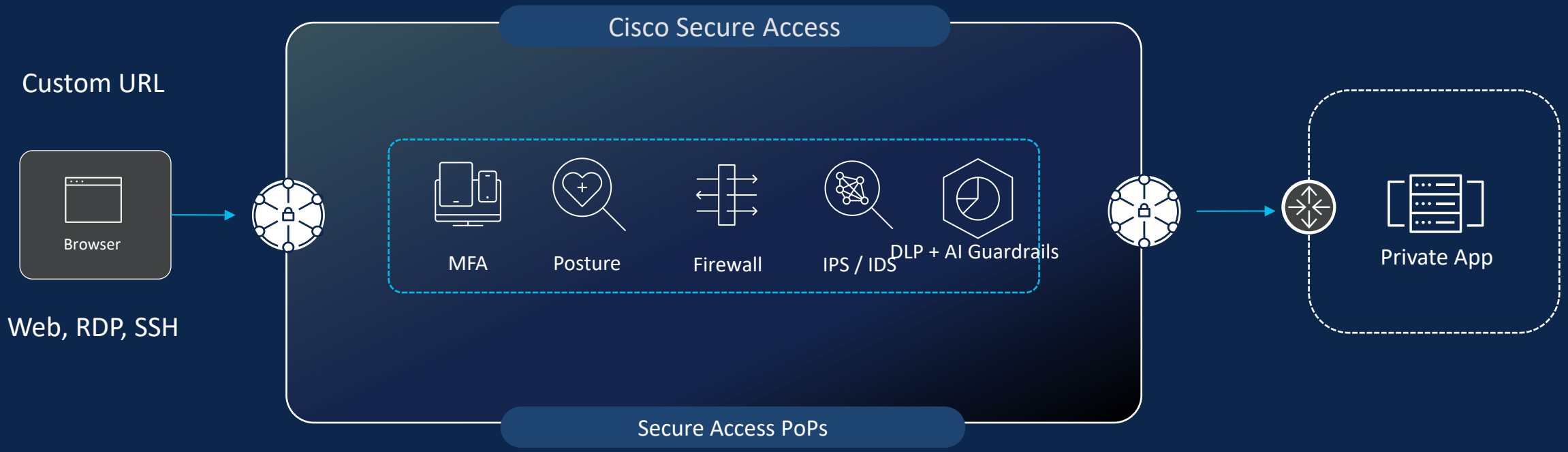
Suite of security service enablement modules

- AnyConnect VPN
- Full SSE ZTA Module
- Secure Endpoint
- DNS/SWG (Umbrella)
- Thousand Eyes (No UI)
- Cloud Management Module (No UI)
- Diagnostic and Reporting (DART)



Clientless Zero Trust Access

Secure Private Access

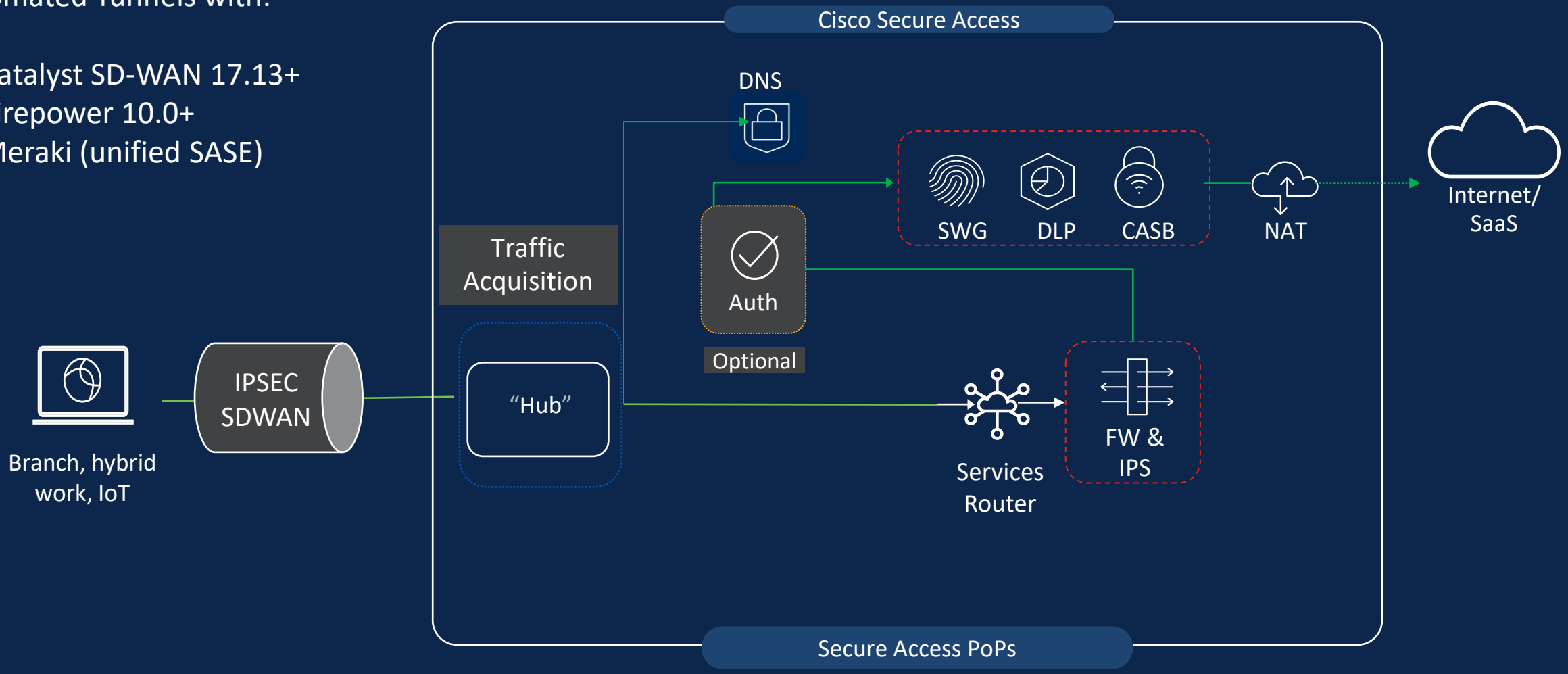


- Ideal for unmanaged devices and BYOD use-cases
- Automatically generated publicly resolvable FQDN for per app access
- HTTP/S, Remote Desktop Protocol, Secure Shell supported
- SAML authentication

Branch - SDWAN/SASE

Automated Tunnels with:

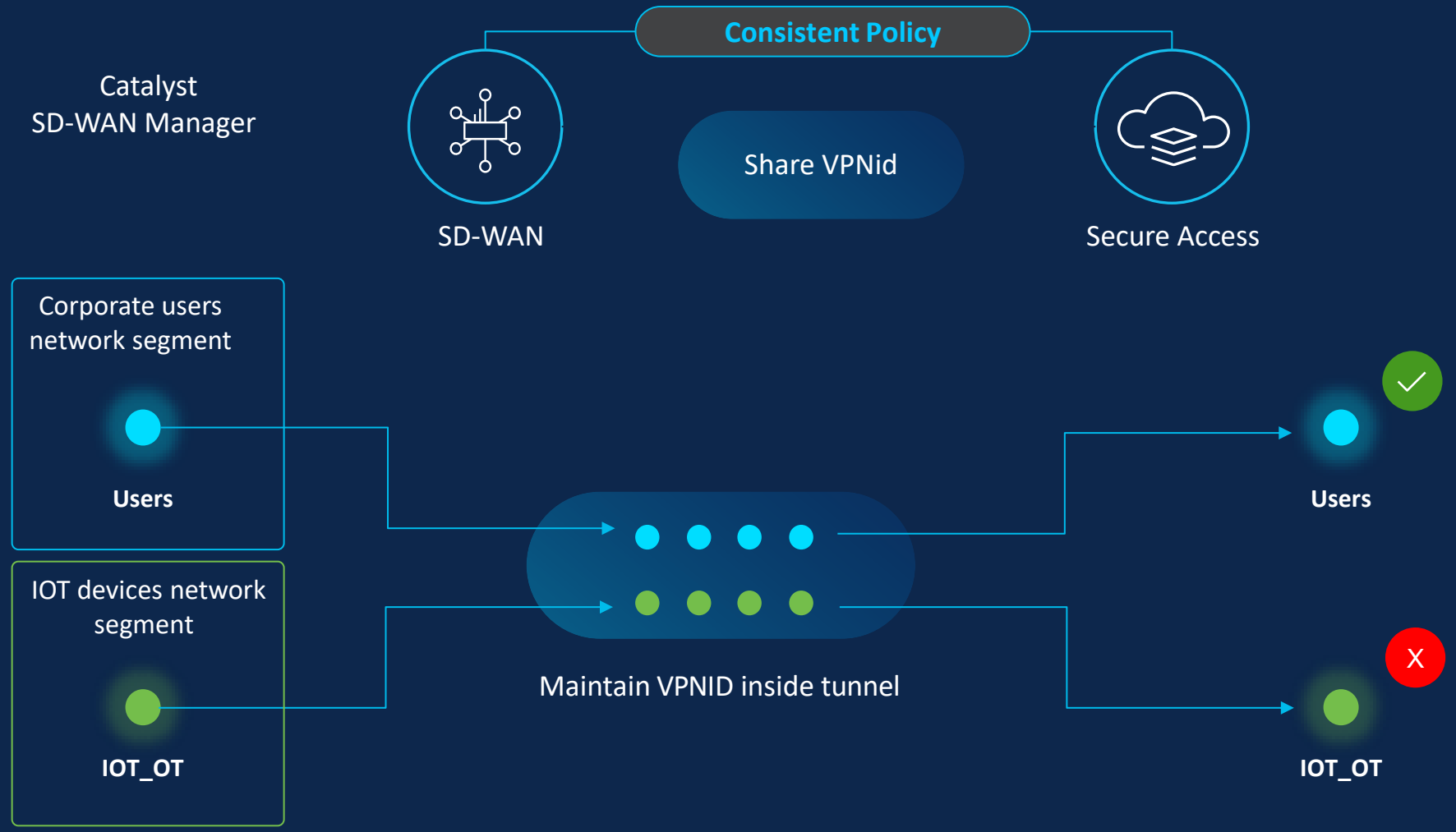
- Catalyst SD-WAN 17.13+
- Firepower 10.0+
- Meraki (unified SASE)



Integration with Catalyst SD-WAN

VPNid support for consistent segmentation

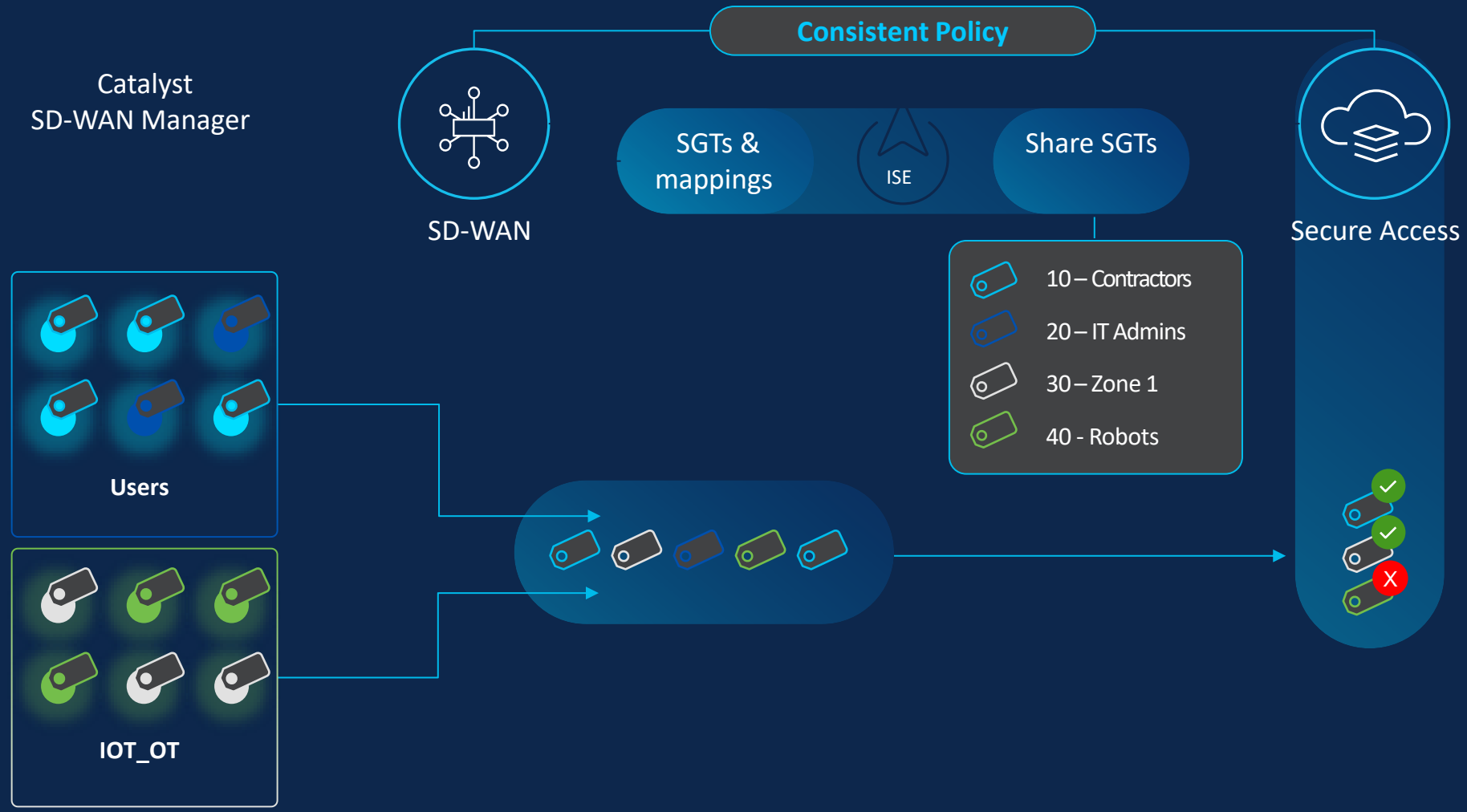
- VPNiD Based policy across both SDWAN & Secure Access
- Maintain segmentation in branch & in the cloud



Integration with Identity Services Engine (ISE)

Leverage SGTs for granular access control

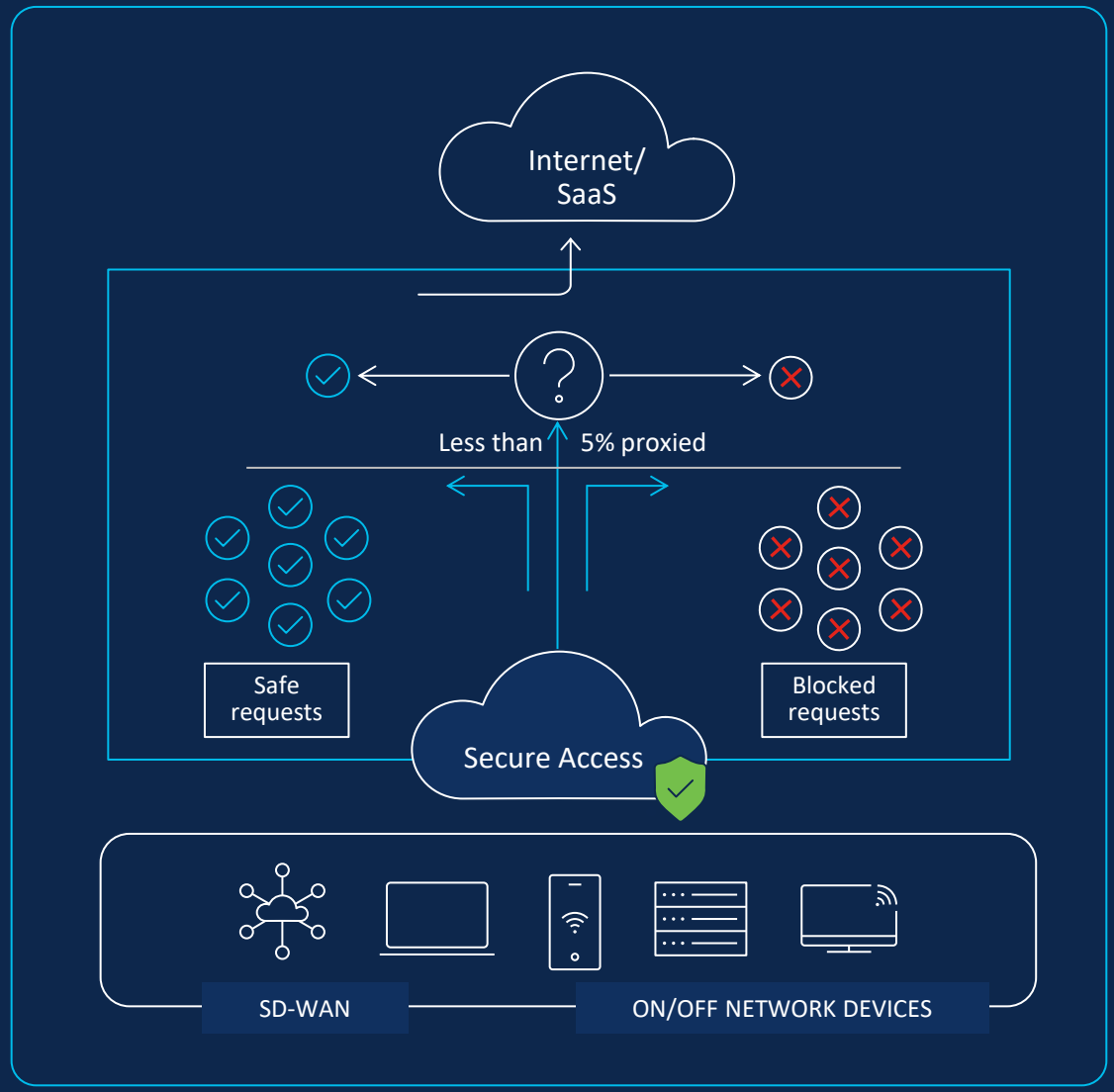
- SGT Based Policy across network & Cloud
- Maintain micro segmentation through Secure Access
- Uniquely identify devices and traffic based on context from ISE
- Apply policy to SGT Based identity



Security Layers

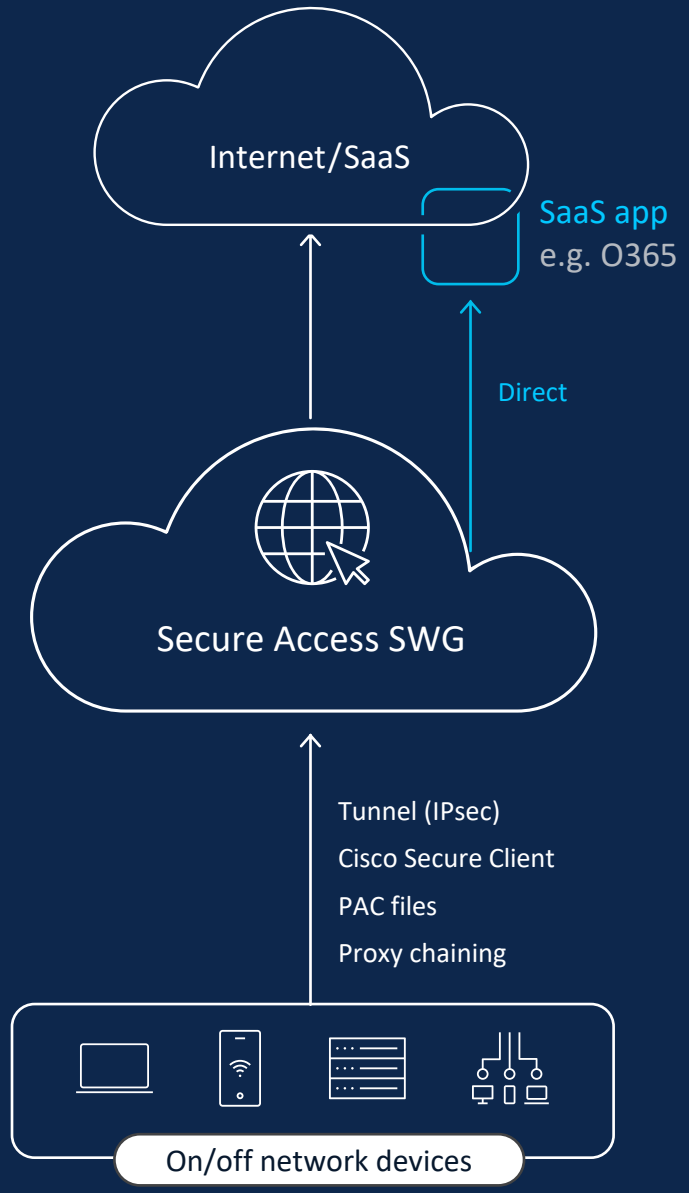
Cisco DNS-layer security

- Deploy enterprise-wide in minutes
- Protect users on & off the corporate network
- Block malware, phishing, CNC callbacks
- Prevent visits to risky web sites
- Stop threats early and reduce alert triage
- Accelerate internet access



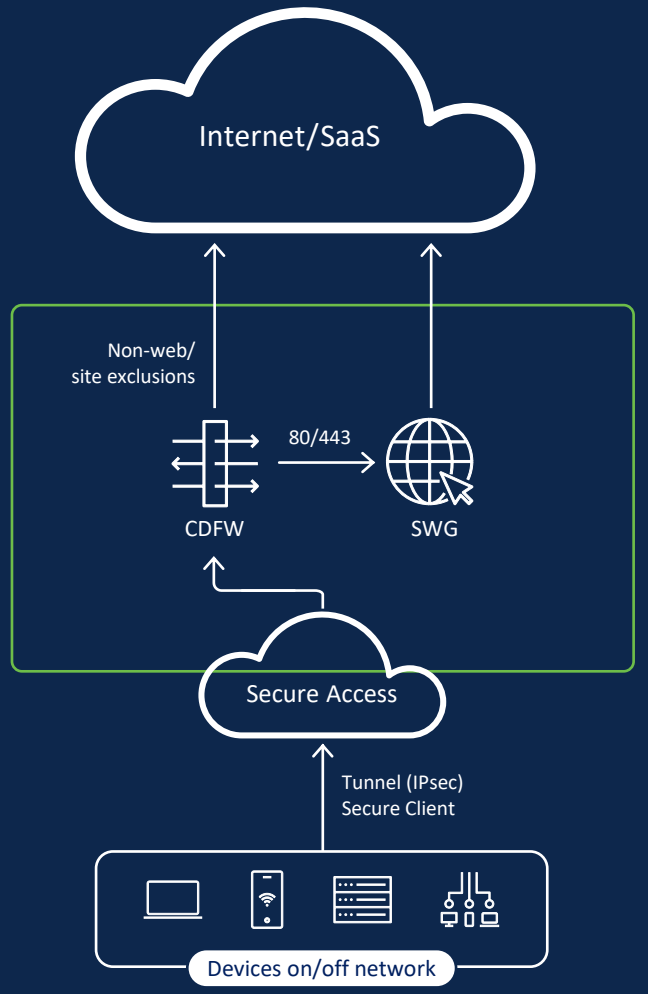
Secure Access SWG

- Full or selective TLS decryption
- TLS 1.3 native support
- Category or URL filtering for content control
- App visibility and granular controls
- Full URL level reporting
- Malware scanning includes two anti-virus engines and Secure Endpoint (AMP) lookup
- Secure Malware Analytics file sandboxing
- File type controls
- Remote Browser Isolation (RBI)

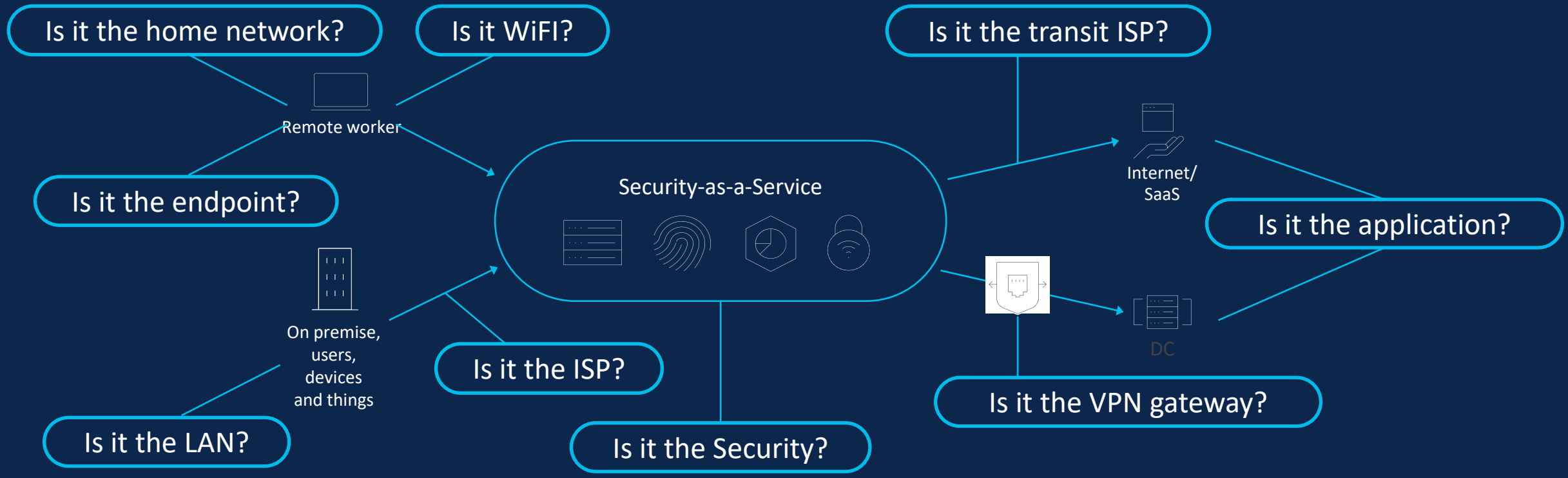


Layer 7 Firewall with IPS/IDS

- Send traffic to Secure Access (all ports and protocols)
- Block high risk applications and protocols (layer 7 application visibility and control)
- Centrally manage IP, port, protocol and application rules (layer 3, 4 and 7 with IPS)
- Forward web traffic (ports 80/443) to secure web gateway
- IPsec tunnel termination or client-based ZTA/VPN



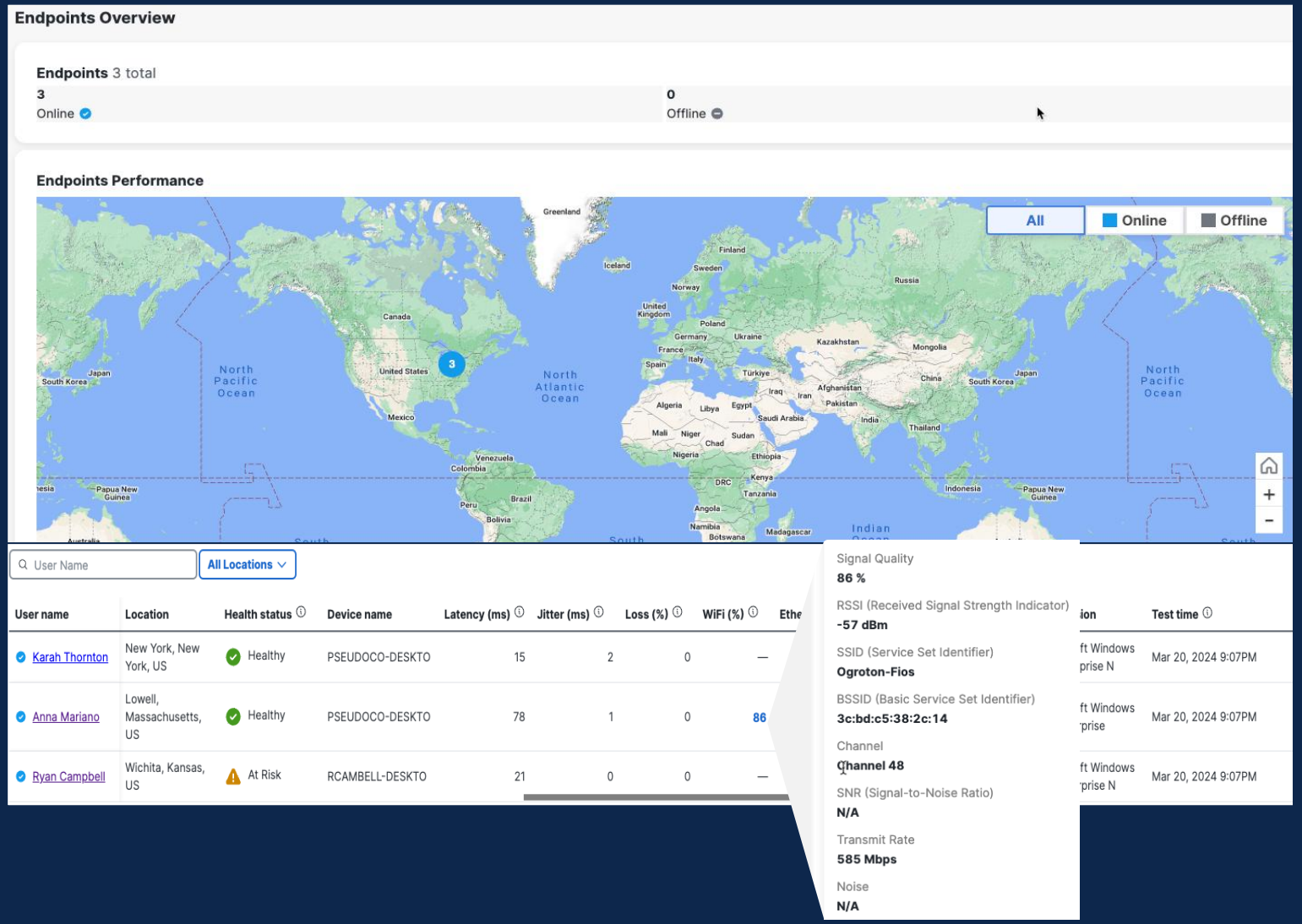
Troubleshooting the hybrid work experience



Secure Access Experience Insights

POWERED BY ThousandEyes

Monitor user digital experience without separate agents or management portals



- Global visibility of registered endpoint status
- Is part of the Cisco Secure Access dashboard
- Includes ThousandEyes Embedded Endpoint Agent(EPA) as a module in Cisco Secure Client

Cisco AI Assistant in Secure Access

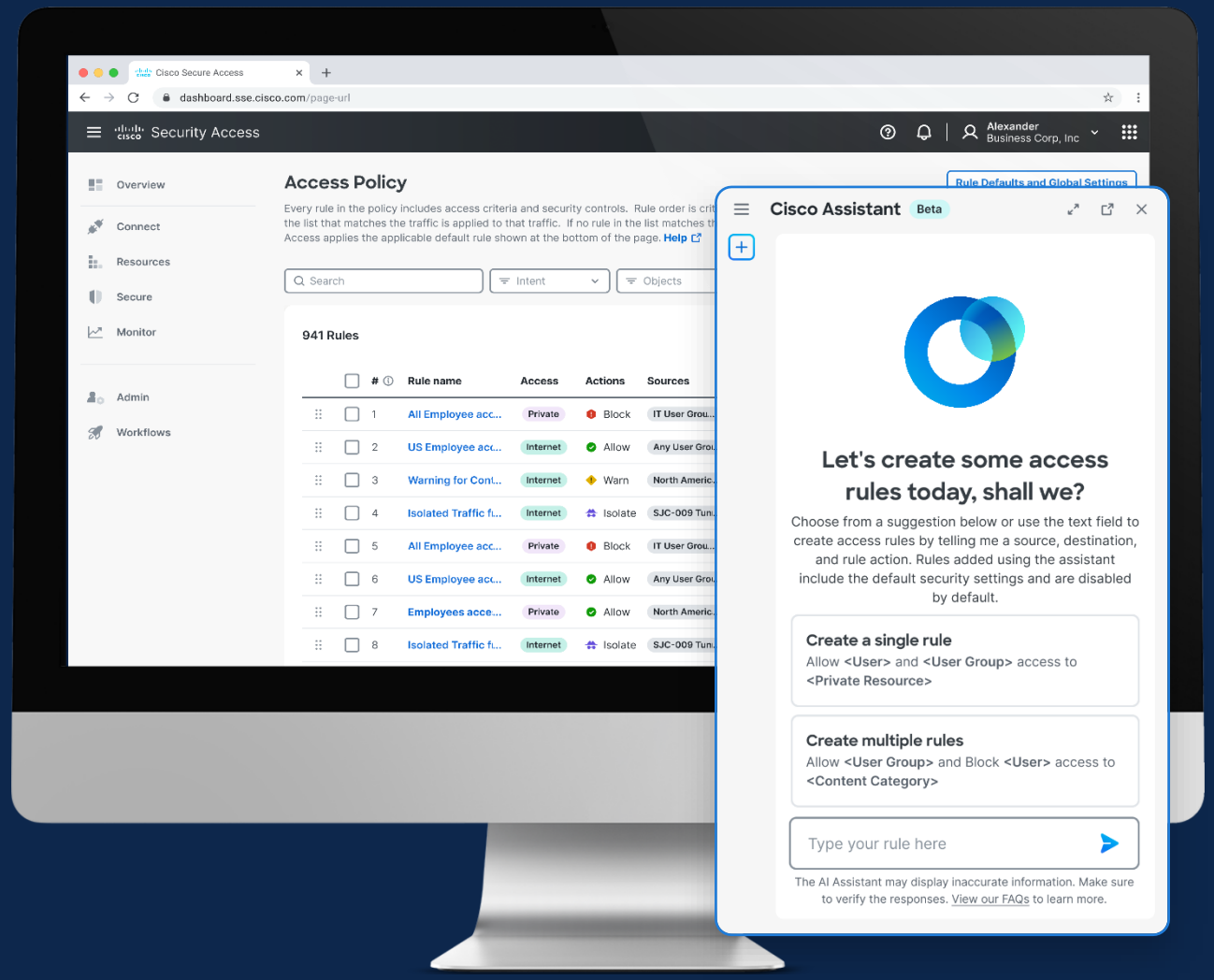
Built with Generative AI natural language to:

Simplify and speed policy administration by up to 70%

Reduce human error

Improve operational efficiency

Better efficacy.
Better experience.
Better economics.



Dashboard visual is for illustrative purposes only

Secure Access | Identity Intelligence

User Trust Level

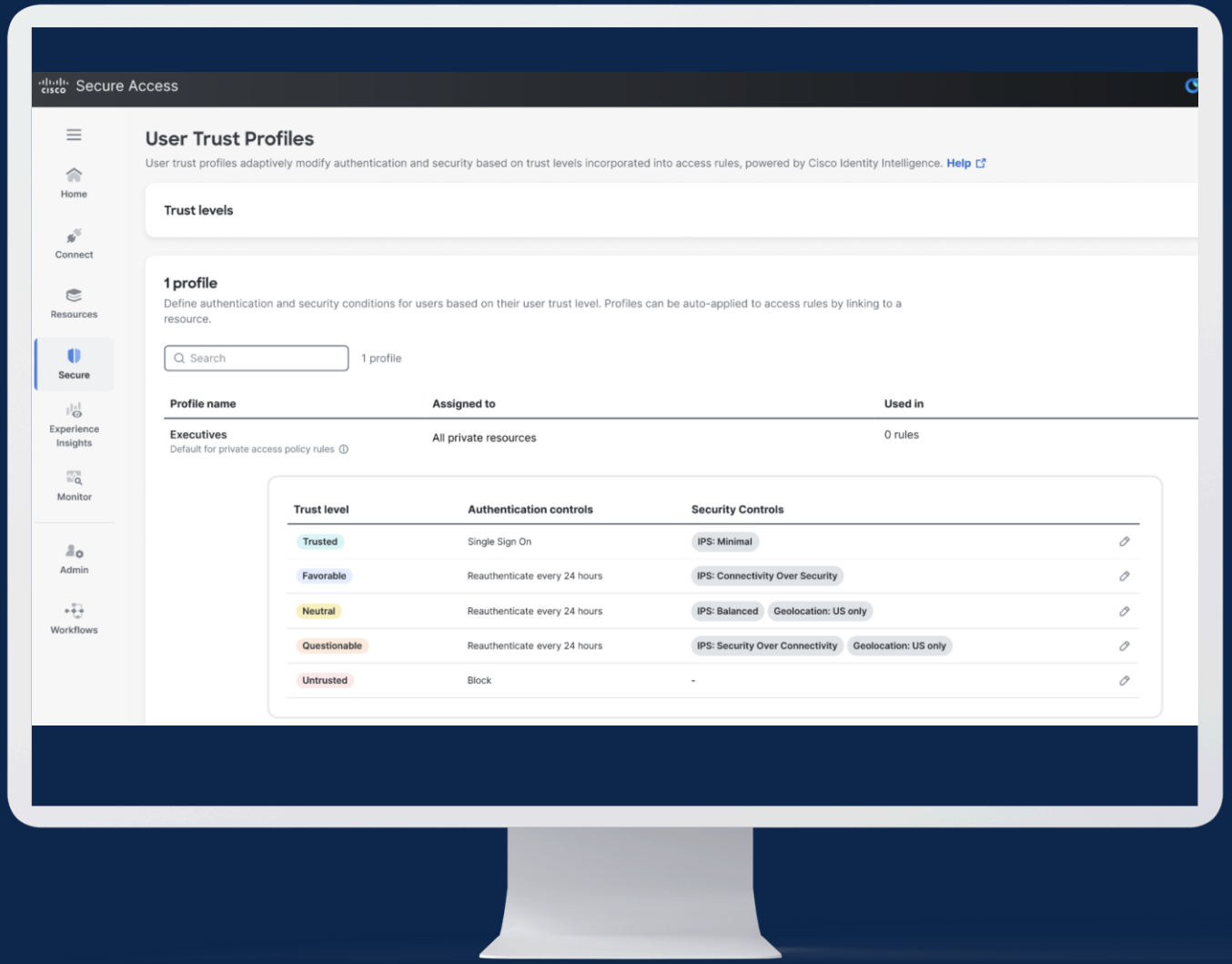
Identity Intelligence will be providing a user trust level for integrating solutions to leverage. Will be a single level, determined by a user's behaviors, actions and posture.

Easy Workflows

After assessment, seamlessly take response action from the console.

Key Levels

- Trusted
- Favorable
- Neutral
- Questionable
- Untrusted
- Unknown



Cloud Access Security Broker (CASB)

- Shadow IT visibility (Categories, Risk levels, Usage)
- Granular control of SaaS app usage
- Tenant Controls (eg.: M365, Google, Slack, Webex, Youtube)
- Detect and remove malware from cloud file storage apps
- Multimode DLP (Inline, API SaaS, Endpoint, Email/ETD integration)

Secure Access: protecting the usage of AI

Protect intellectual property as it flows in and out of AI systems

Threat Visibility	Leakage Prevention	Threat Prevention
Discover and Assess Activities	DLP Inspection of Prompts/Uploads	Block Apps and Control Downloads

Discovers and controls over **185** Gen AI apps (including APIs)

Secure Access: SSE that truly understands AI

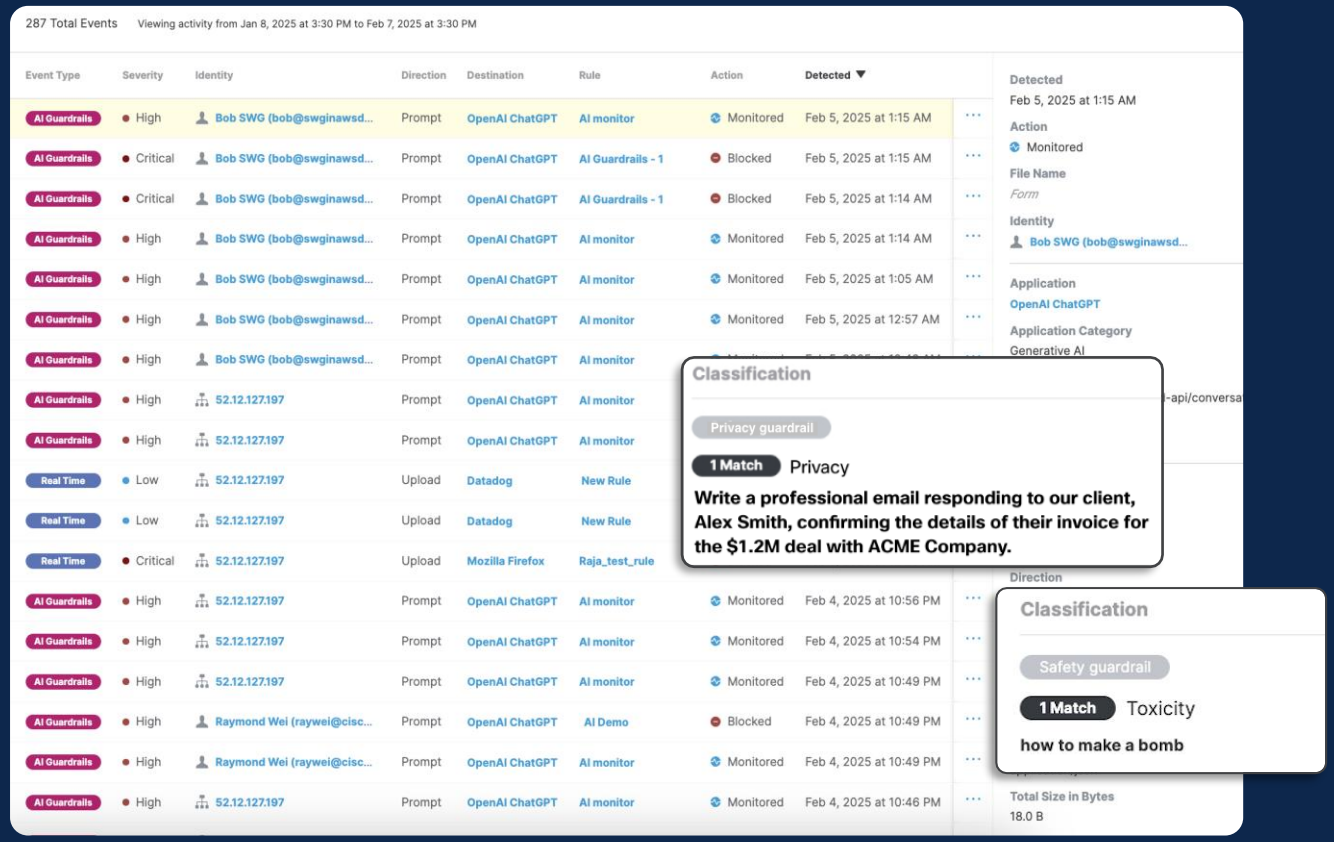
Powered by AI Defense models to *understand intent*

Intelligent Protection

- Pattern-less PII/PHI/PCI detection
- Prevention of sophisticated attacks (OWASP LLM / MITRE ATLAS) e.g., prompt injection
- Intent-based toxicity detection

Zero-Friction Security

- Built into Secure Access*
- Single unified policy framework
- No additional infrastructure



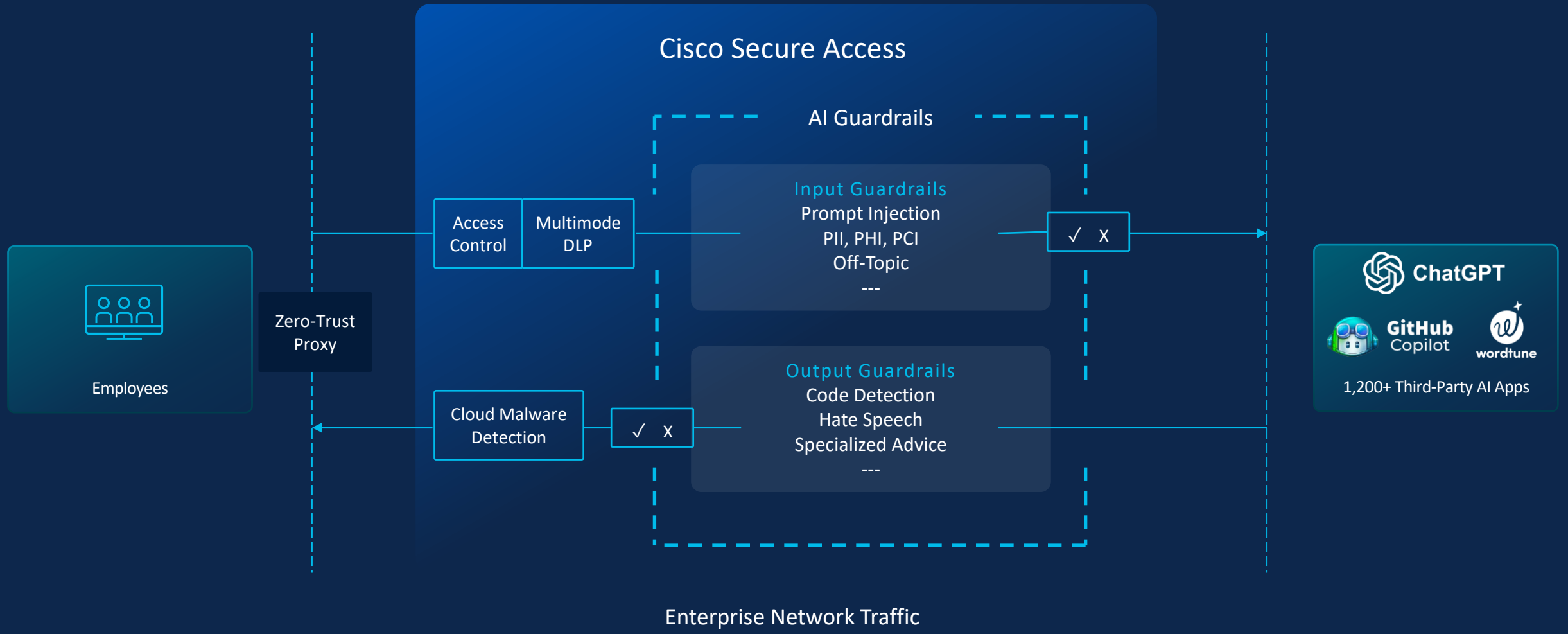
1200+
AI Applications Coverage

100%
Top 16 AI Apps Coverage

1
Unified Security Framework

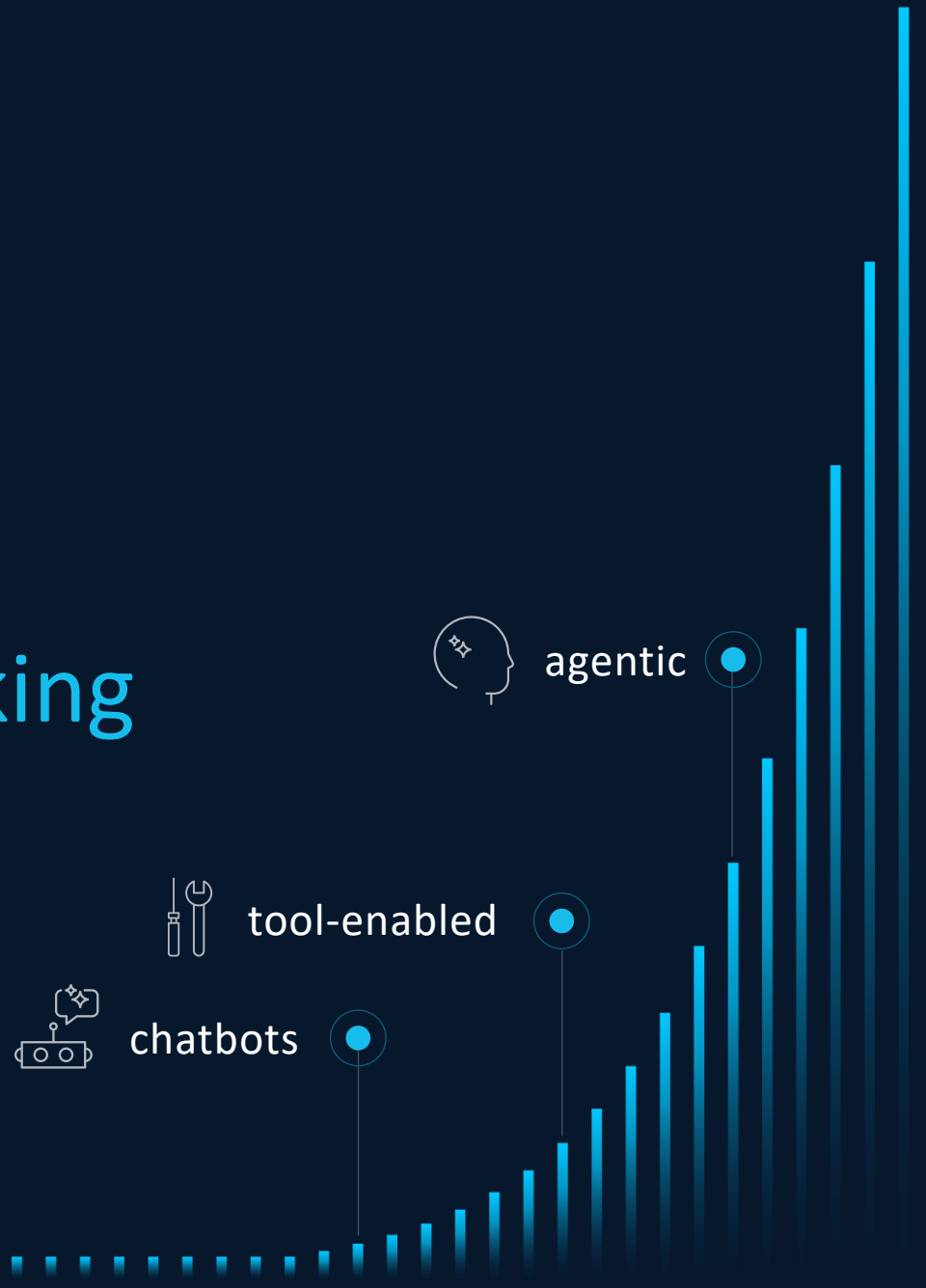
(*) included in Secure Access Advantage

Protecting usage of third-party AI apps



AI is evolving at a rapid pace.

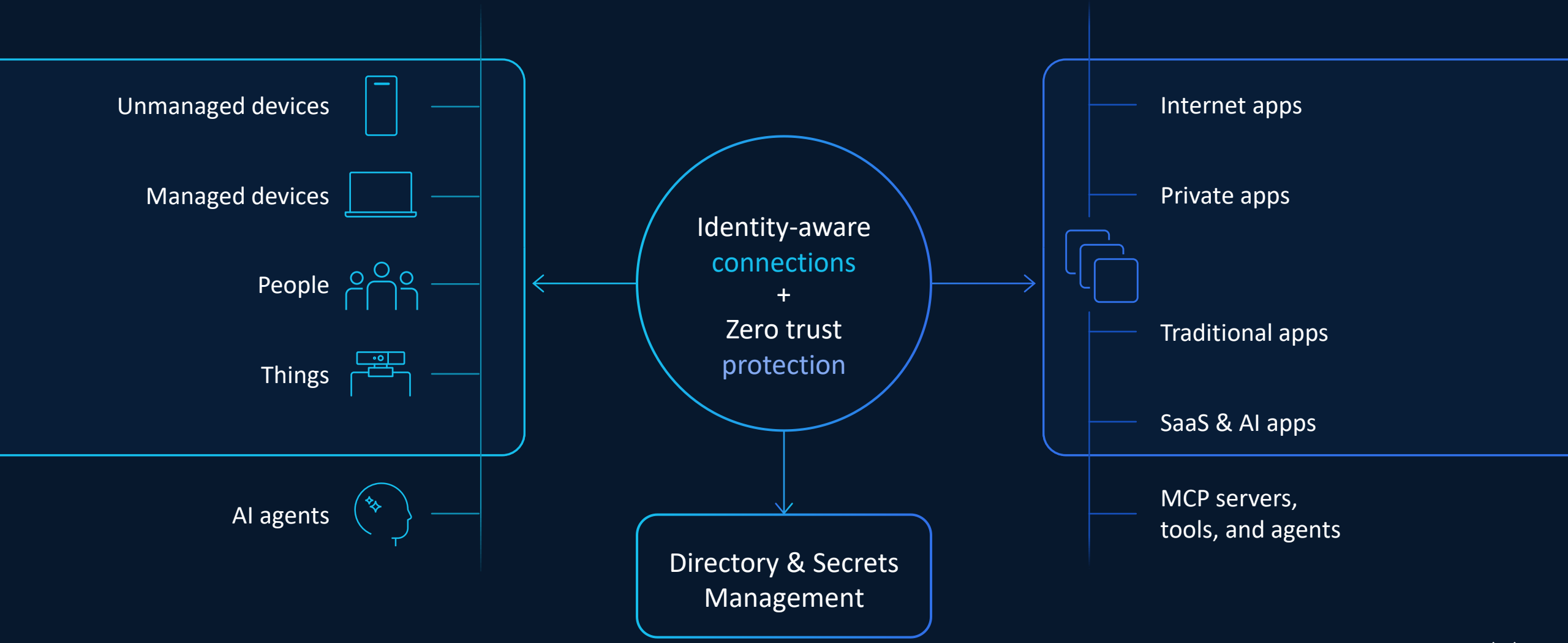
from static knowledge
to real-time knowledge
to autonomous decision-making



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

Extending Cisco's Zero Trust Access to secure Agentic AI (Coming soon)



KNOW EVERY AGENT | AUTHORIZE EVERY ACTION | ADAPT TO RISK IN REAL TIME

Visibility, identity, and ownership for every AI agent interacting with your environment

Agentic IAM by Duo

- Agent & Tool Discovery
- Agent Directory
- Agent Access Policy
- Human Accountability
- Lifecycle Management

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

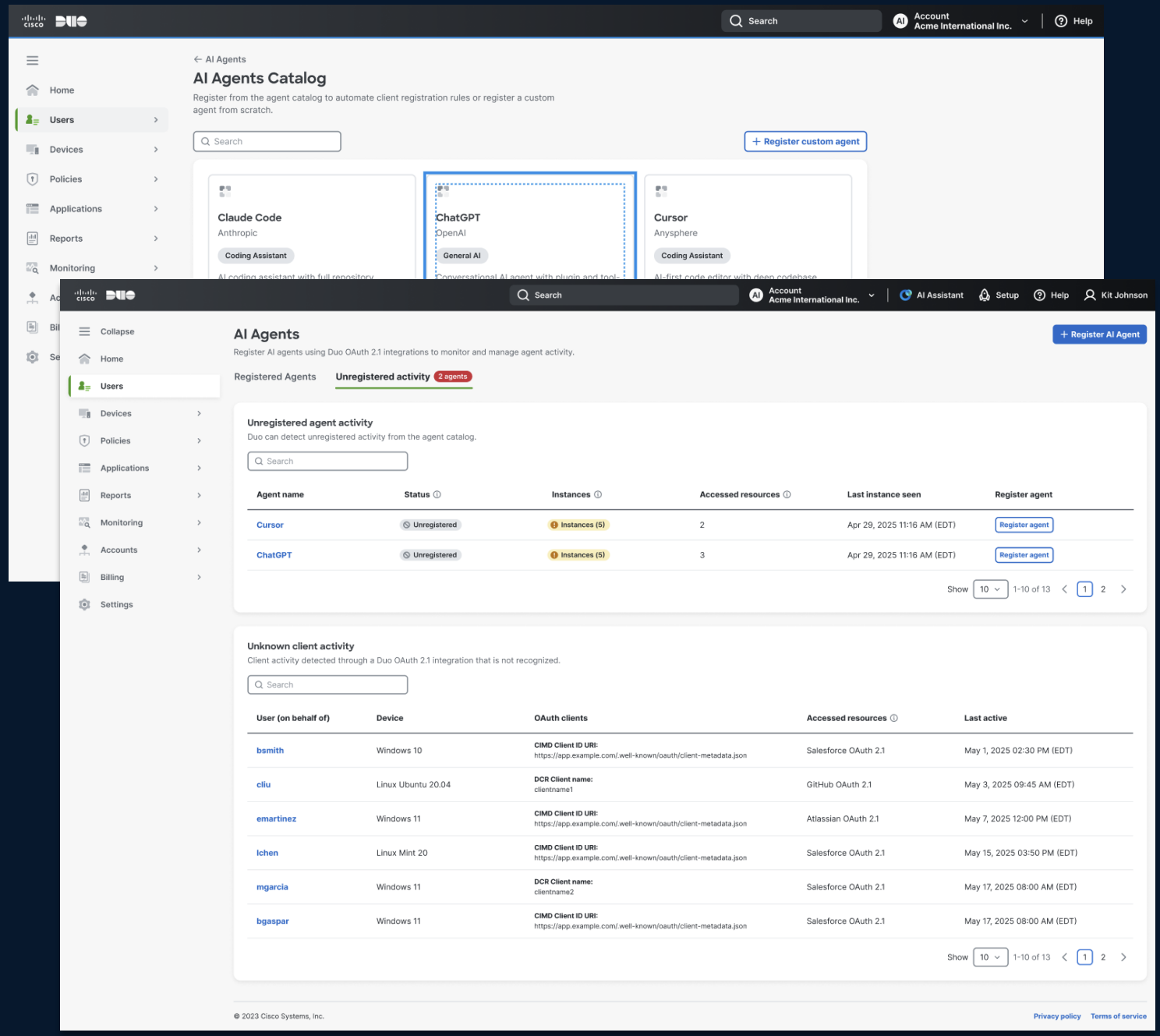
Create a directory with a list of agents, human owners, registration rules, tool access and agent activity logs

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



May 4, 2026 Leave a Comment

Executive Platform

Securing the Agentic Workforce: Cisco Announces Intent to Acquire Astrix Security

4 min read

Peter Bailey

Today, I'm thrilled to announce our intent to acquire Astrix Security Ltd., a pioneer in Non-Human Identity (NHI) Security.

We're seeing an explosion of AI agents that are already reshaping the digital enterprise. Soon, every person in an organization will be supported by a network of AI agents working continuously at machine speed, accessing data, making decisions, and taking action on their behalf.

These agents represent an entirely new class of coworker: capable of incredible productivity, but also capable of unintended harm or malicious behavior if left unsecured. This is the new attack surface, and it is growing faster than most organizations realize.

As organizations race to adopt agentic technologies, security teams are under real pressure to enable their teams while securing the use of agents. But agent capabilities are advancing faster than most security models, creating a widening gap in visibility, governance, and response. According to Cisco's AI Readiness Index, only 24% of organizations can control agent actions with proper guardrails and live monitoring, and just 31% feel fully capable of securing their agent AI systems.

That gap between agentic capability and organizational readiness continues to widen. With the emergence of AI models, like Mythos, we're seeing threat actors reshape the risk landscape in ways that are impossible to ignore. Security teams are now confronting a new class of high-impact, AI-accelerated risks.

At Cisco, we are deeply focused on helping customers address this gap. This is the work that drives us every day.

Meeting the Moment: Our Commitment to AI Security

Cisco has been moving quickly to enable the safe and secure use of AI.

Share

AI Defense helps organizations safely build AI applications by protecting the models and agents built internally. We've also extended our Zero Trust Access architecture

https://blogs.cisco.com/news/cisco-announces-intent-to-acquire-astrix-security

KNOW EVERY AGENT | AUTHORIZE EVERY ACTION | ADAPT TO RISK IN REAL TIME

Consistently enforced where agents access enterprise data & tools.

Agentic Workforce

Tools, resources and data

Authorize every action

Just in time access

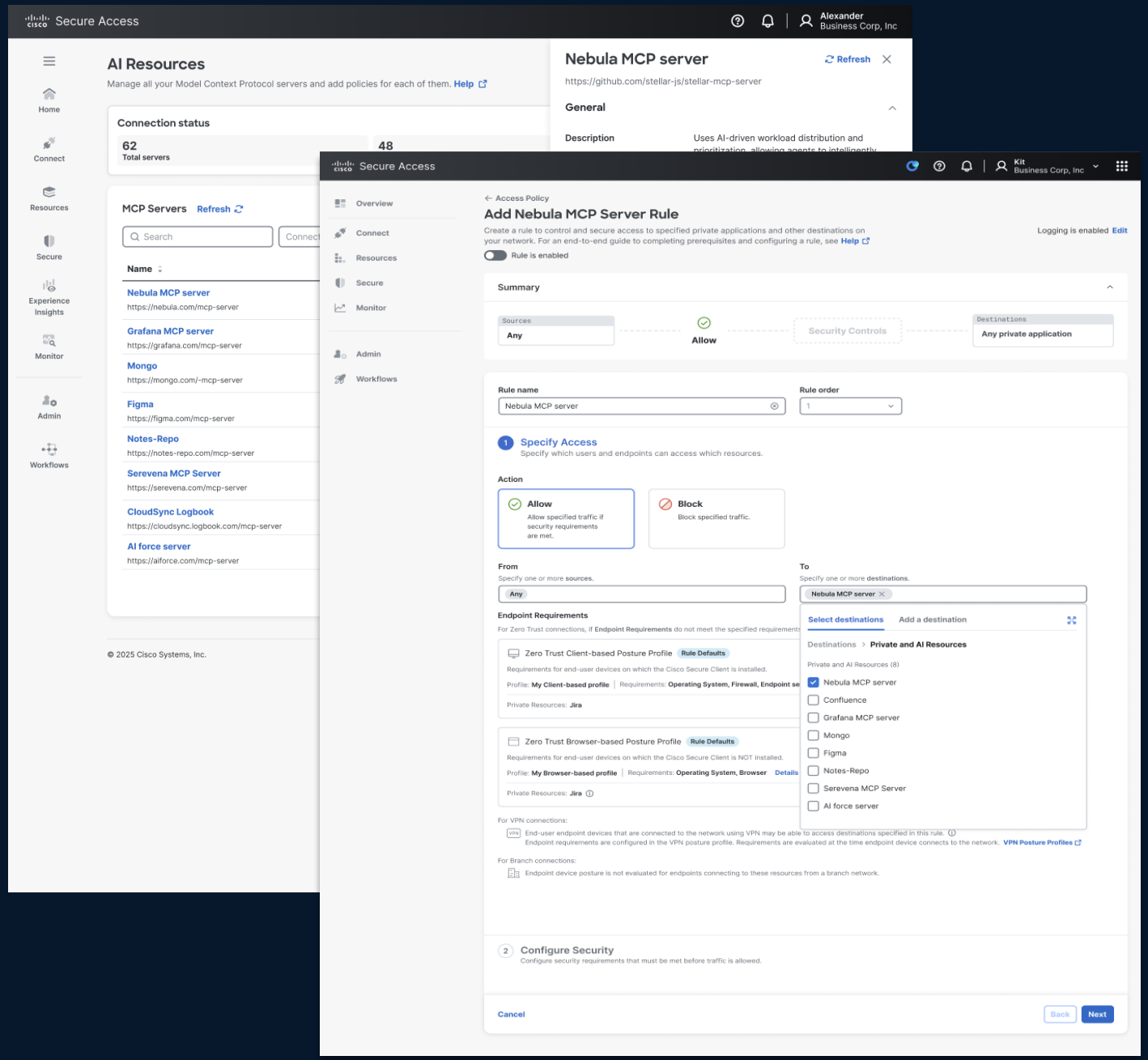
Provide access to the agents only when they require access to the tools and resources, not before and not after

Just enough access

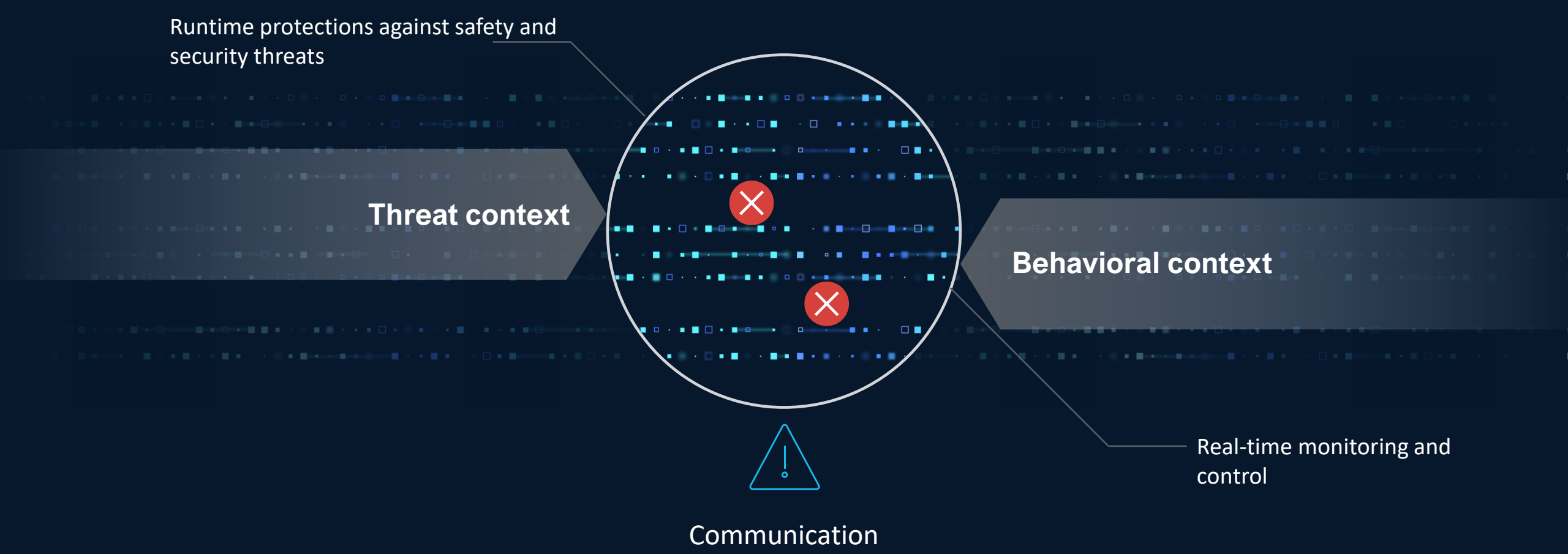
Integrated with identity context, provide access to agents only to the tools and resources that they need access to perform their tasks

Just long enough access

Provide time-bound short-lived OAuth tokens (between 5 mins to 1 hour) to agents to perform their tasks



Use intent, threat, and behavioral context to adjust protection decisions.



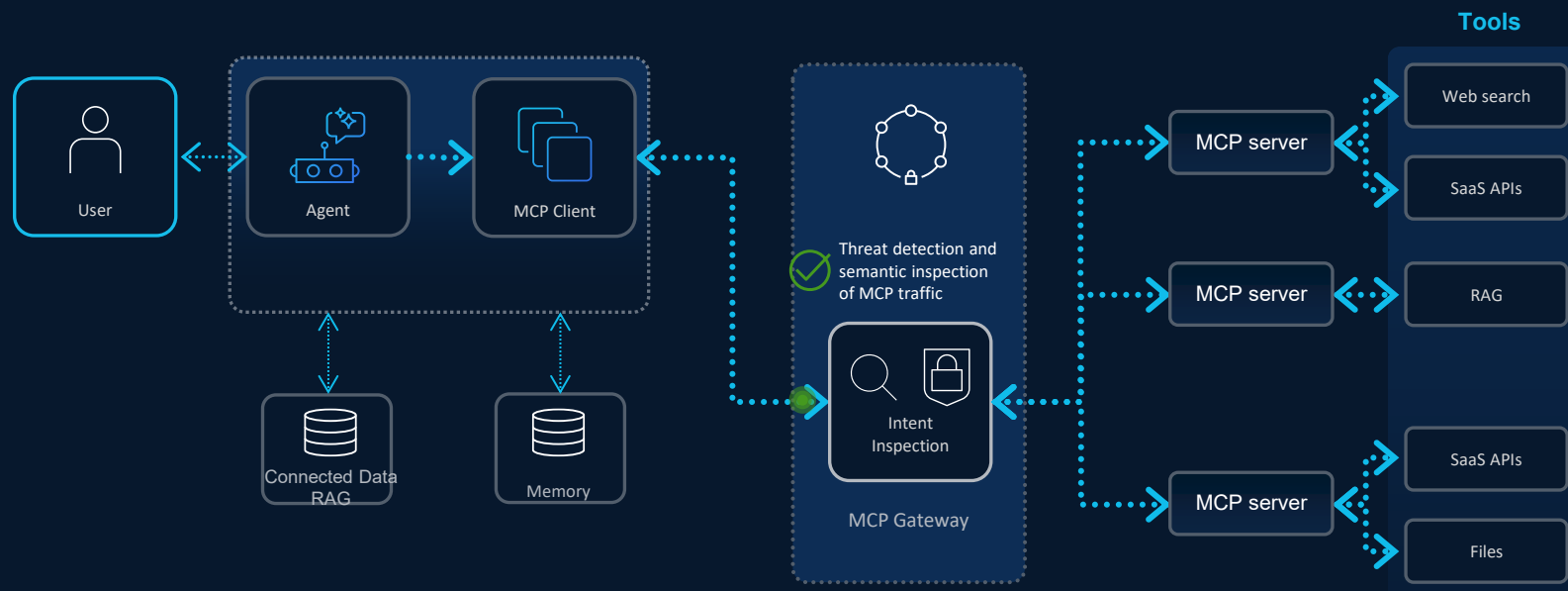
Adapt to risk in real time

Intent based activity monitoring

Continuously monitor the agent network traffic to identify any malicious prompts, rogue agents or agent activity drift in real-time

Safety & security guardrails

Define safety and security guardrails around agent activity and prevent rogue agents or agent activity drift from impacting the enterprise infrastructure



Cisco Agentic AI Security

Observability with Splunk

Manage Agent identity

with

Duo Agentic IAM

Enforce Agent Access

with

Secure Access

Protect Agents

with

AI Defense

AI- Ready Infrastructure with AI Pods

More information…

- Zero Trust for the Agentic AI
  - https://www.cisco.com/site/us/en/solutions/artificial-intelligence/security/securing-agentic-ai/index.html
  - https://blogs.cisco.com/security/security-agentic-ai-how-cisco-brings-zero-trust-to-your-new-digital-workforce

- Agentic AI Infographic
  - https://www.cisco.com/c/dam/m/digital/usc/Security-Advisory-Board/Agentic_AI_Infographic.pdf

- Cisco Secure Access
  - https://www.cisco.com/site/us/en/products/security/secure-access/index.html


cisco SECURE