CISCO Engage | Tech Day

Cisco Universal ZTNA

The Evolution of Zero Trust Network Access

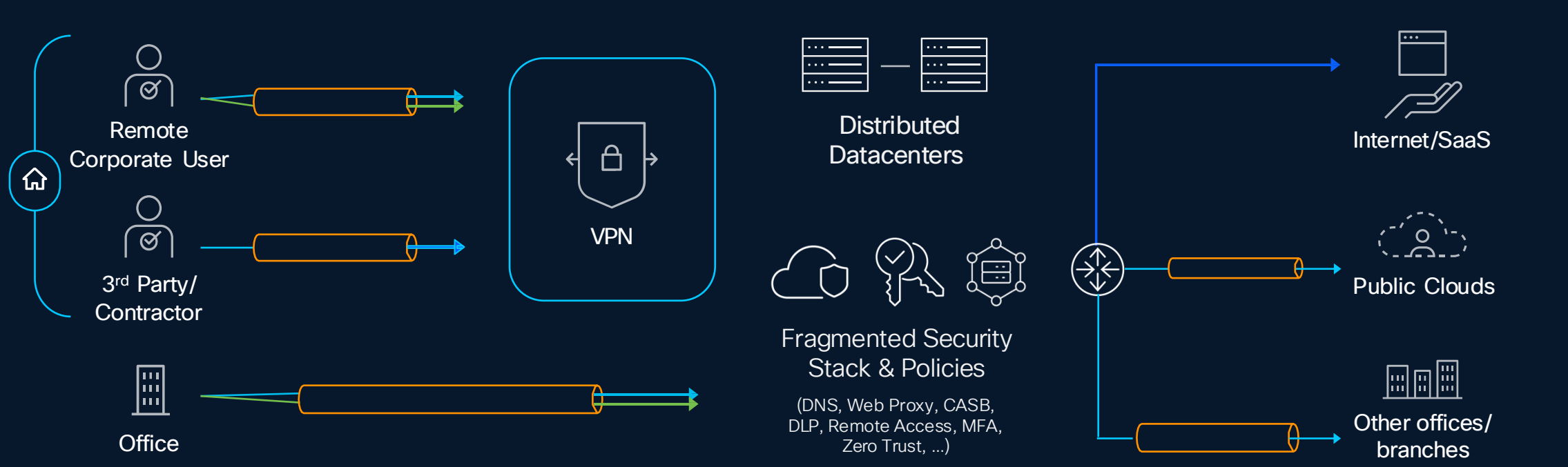
Lou Norman CCIE CISSP
Cyber Security Architect,
linkedin.com/in/lounorman

Nicholas Whitaker CCNP
Solution Engineer

March 18th, 2026

Challenge

An architecture never designed for hybrid work



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

Cisco Secure Access

Modernize your defense with converged cloud security grounded in Zero Trust

Remote | Campus | Regional | Mobile | Airplane | Overseas | Field | ...

Step 1
Authenticate

Step 2
Go to Work

ZTNA

VPN

SaaS

Direct

Private apps

Traditional VPN

SaaS apps

Internet apps

Unified Architecture

Endpoint

Browser

Branch

Cisco® Secure Access

Unified Administration

- Unified Administration
- Single Dashboard
- Single Policy Ruleset
- Single SLA
- ZTNA and VPNaaS
- Secure Internet Access

Unified Security

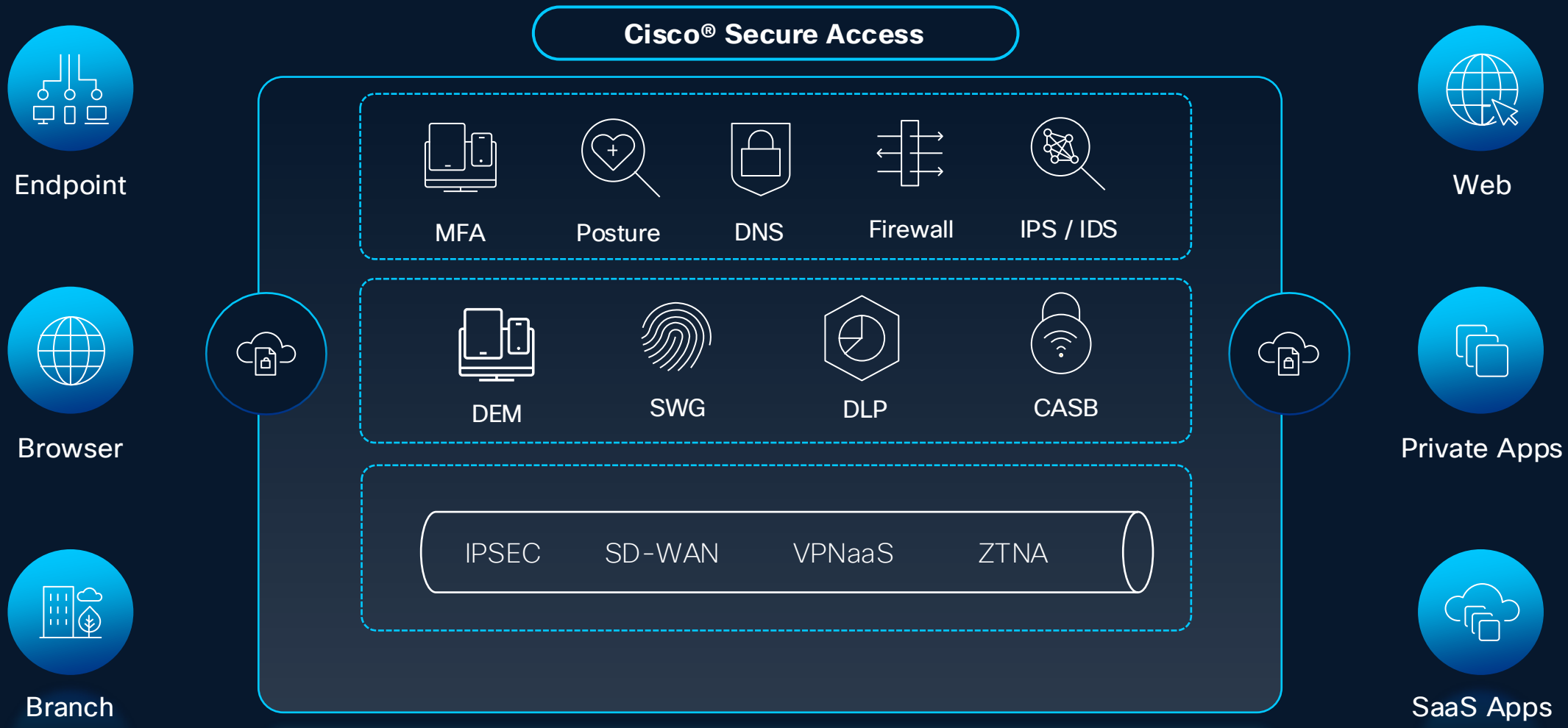
- Flexible connectivity
- Consistent Inspection
- Layers 3–7 Protection
- Firewall, Proxy, DLP
- Malware Protection

Web

Private Apps

SaaS Apps

Unified Architecture



Cisco Secure Client

Suite of security service enablement modules

AnyConnect VPN (Core)

ZTA Module

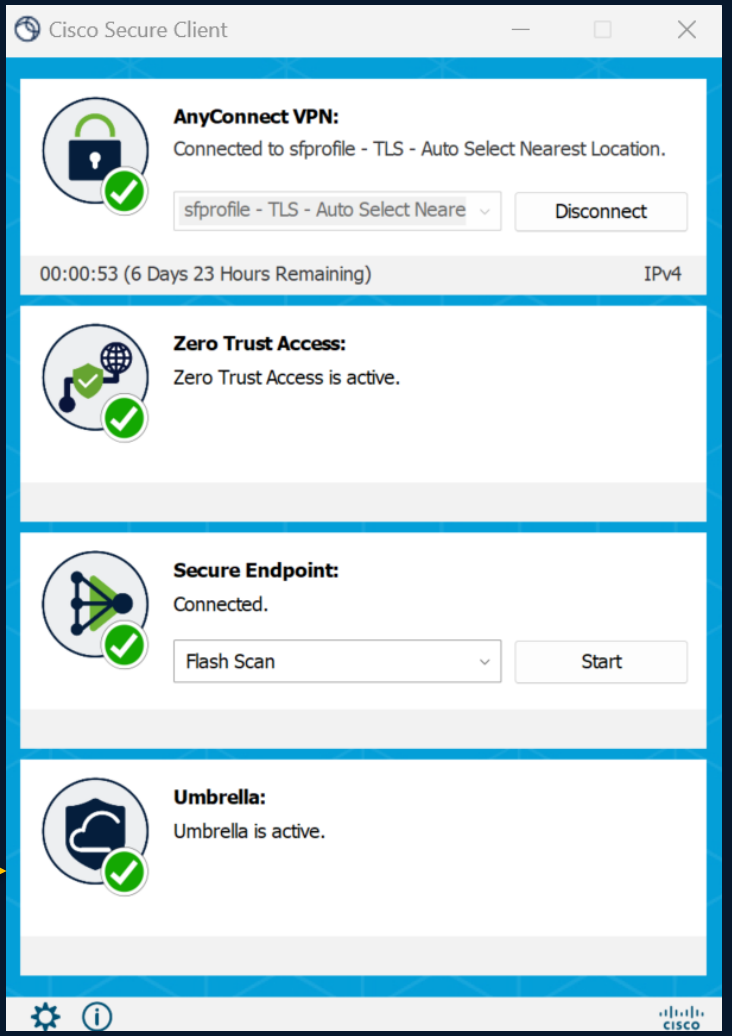
Secure Endpoint (AMP)

Roaming Module

Thousand Eyes (No UI)

Cloud Management Module (No UI)

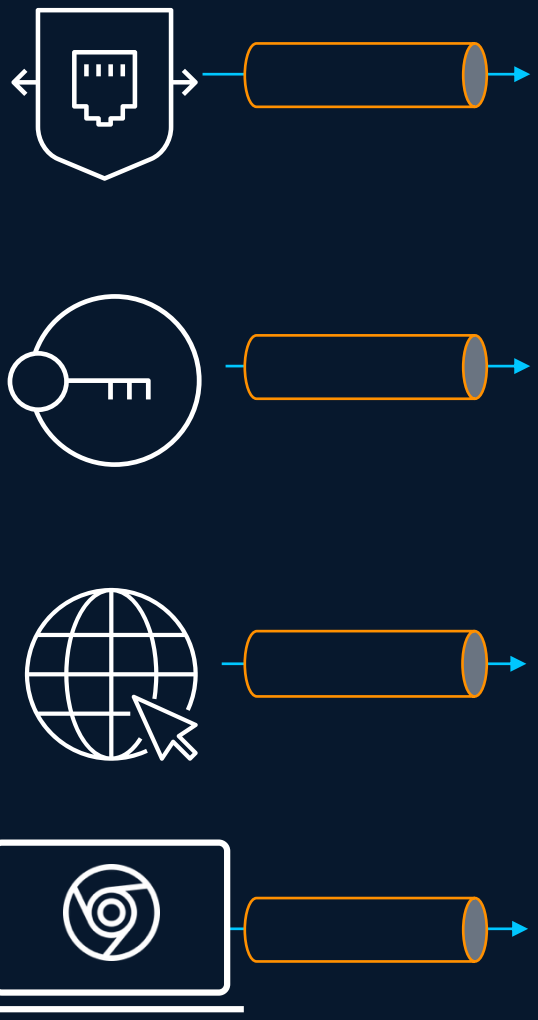
Diagnostic and Reporting (DART)



Traffic Acquisition Methods

Cisco Secure Client

Unmanaged Endpoint



AnyConnect VPN Module

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

ZTNA Module

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

Roaming Security Module

- Device Enrollment (profile)
- Carry **Internet DNS & Web Traffic** (80/443)

Clientless ZTA

- Accessible from any browser that supports SAML/Cookies
- Request based posture (browser version, OS)
- Private Web, RDP, and SSH Apps
- Integration with Google Enterprise Browser

cisco

Secure Private Access

Posture

Authorization check prior to application access

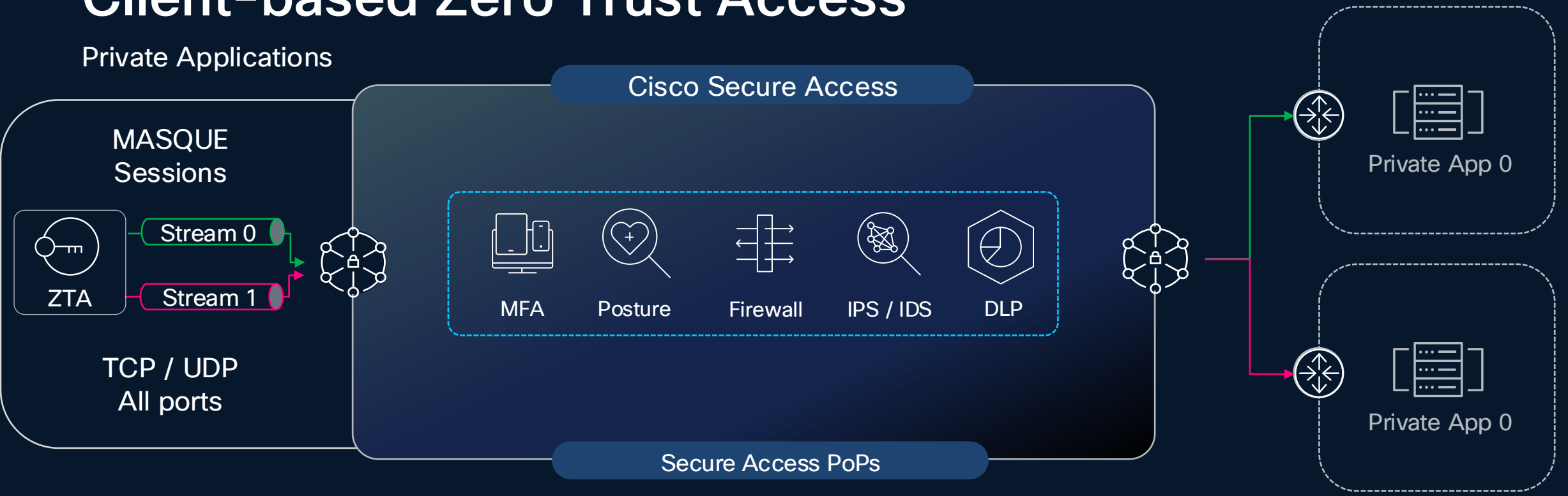
Authorization and access check per session

Supported AV vendors:

[Client-based ZTA](#)
[VPN-as-a-service](#)

	VPNaaS	ZTA Client-based	ZTA Browser
Operating System	✓	✓	✓
Anti-Malware	✓	✓	
Firewall	✓	✓	
Disk Encryption	✓	✓	
Certificate Check	✓		
Browser Check	✓		✓
System Password		✓	
File Check	✓		
Registry Check (windows only)	✓		
Process Check	✓		

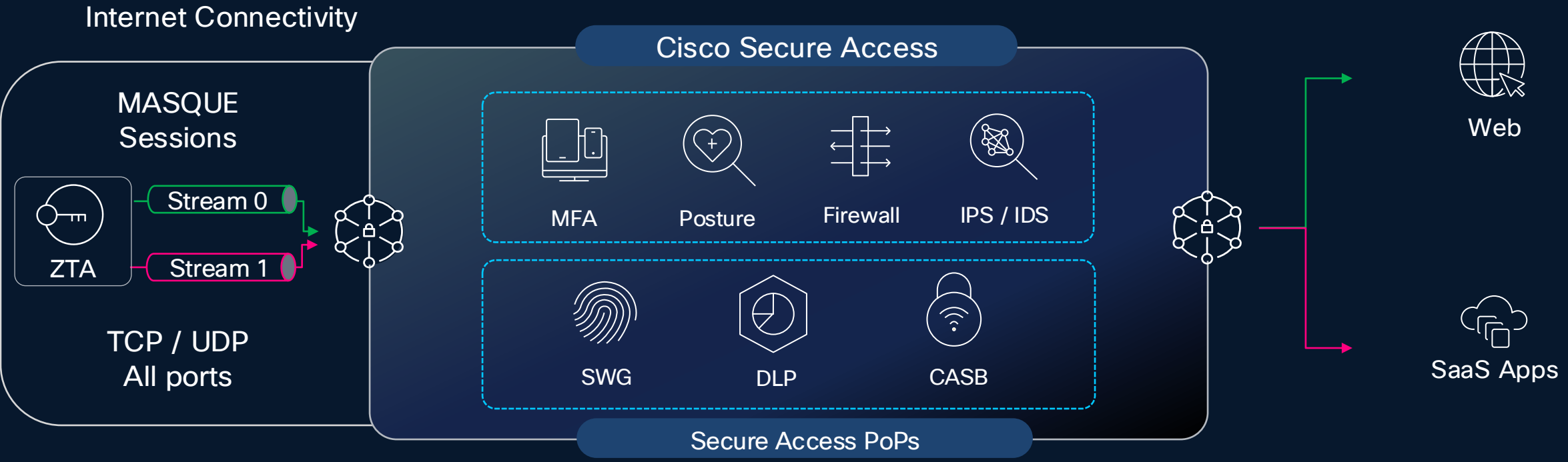
Client-based Zero Trust Access



- 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

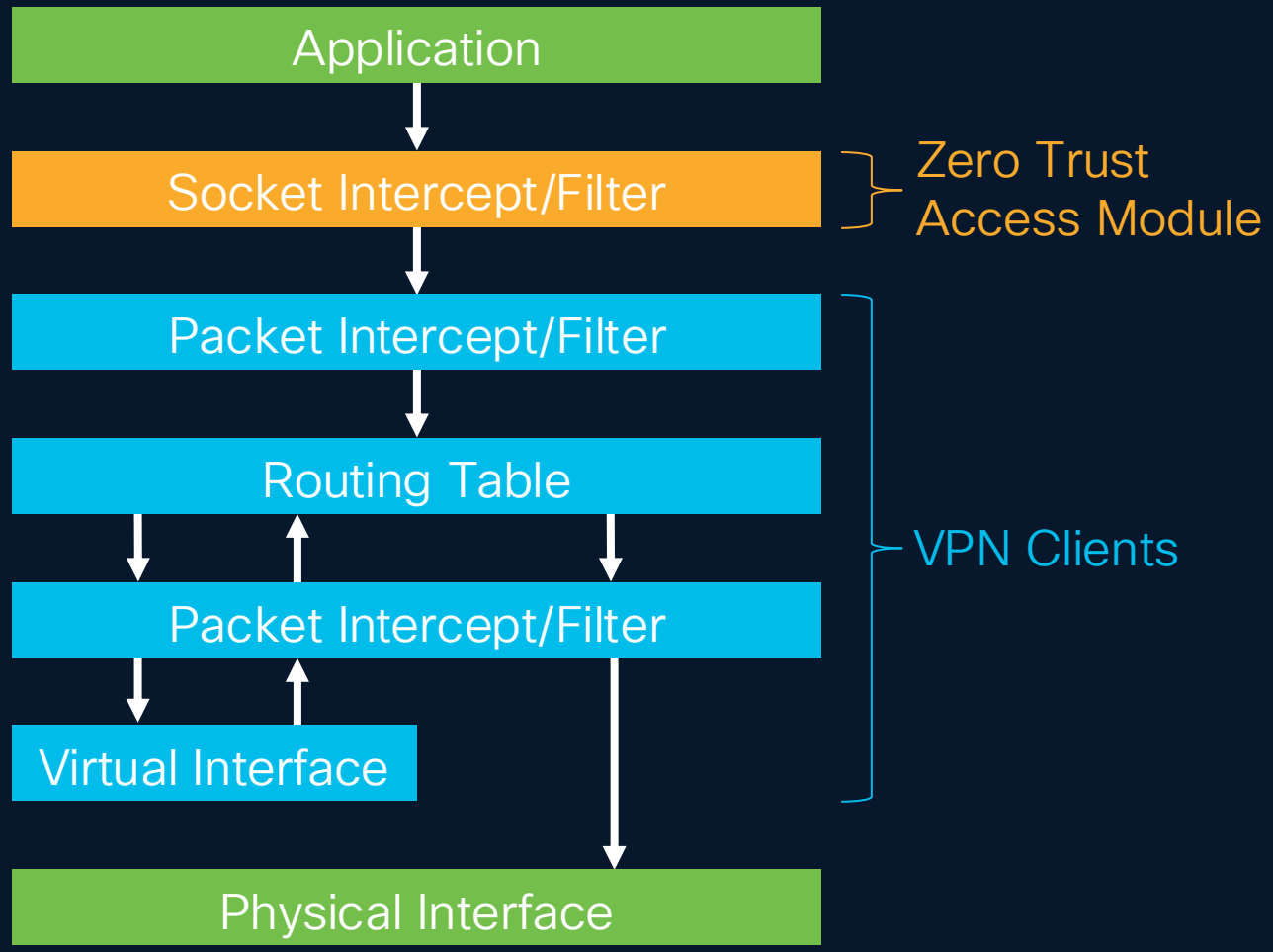
Client-based Zero Trust Access



- 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

Secure Client ZTA Module: Socket Intercept

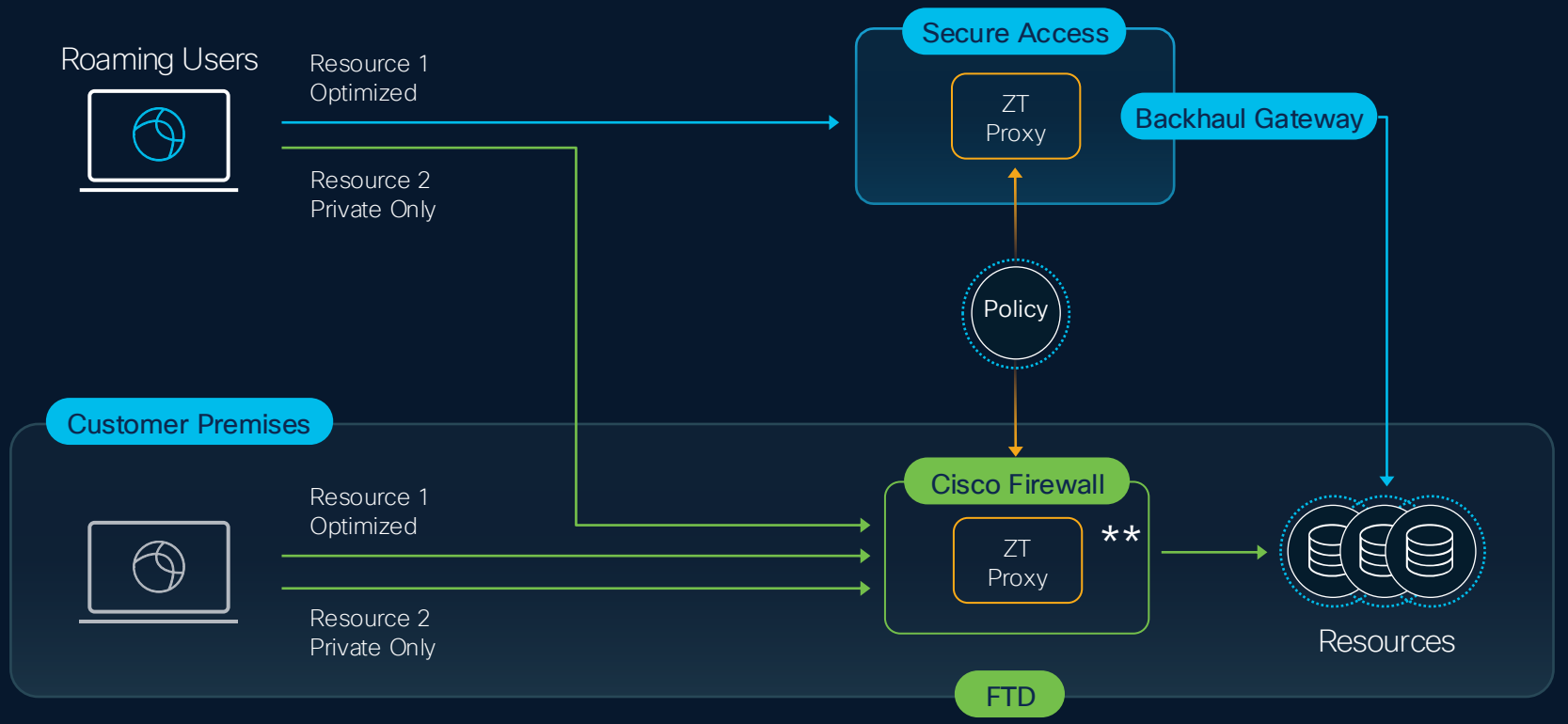


Why Socket Intercept?

- Control of DNS and application traffic *before* VPN clients
- No route table manipulation
- Ability to capture traffic by IP, IP subnet, FQDN and FQDN wildcard
- Interoperability with Cisco and non-Cisco VPNs

Hybrid Private Access for flexible enforcement

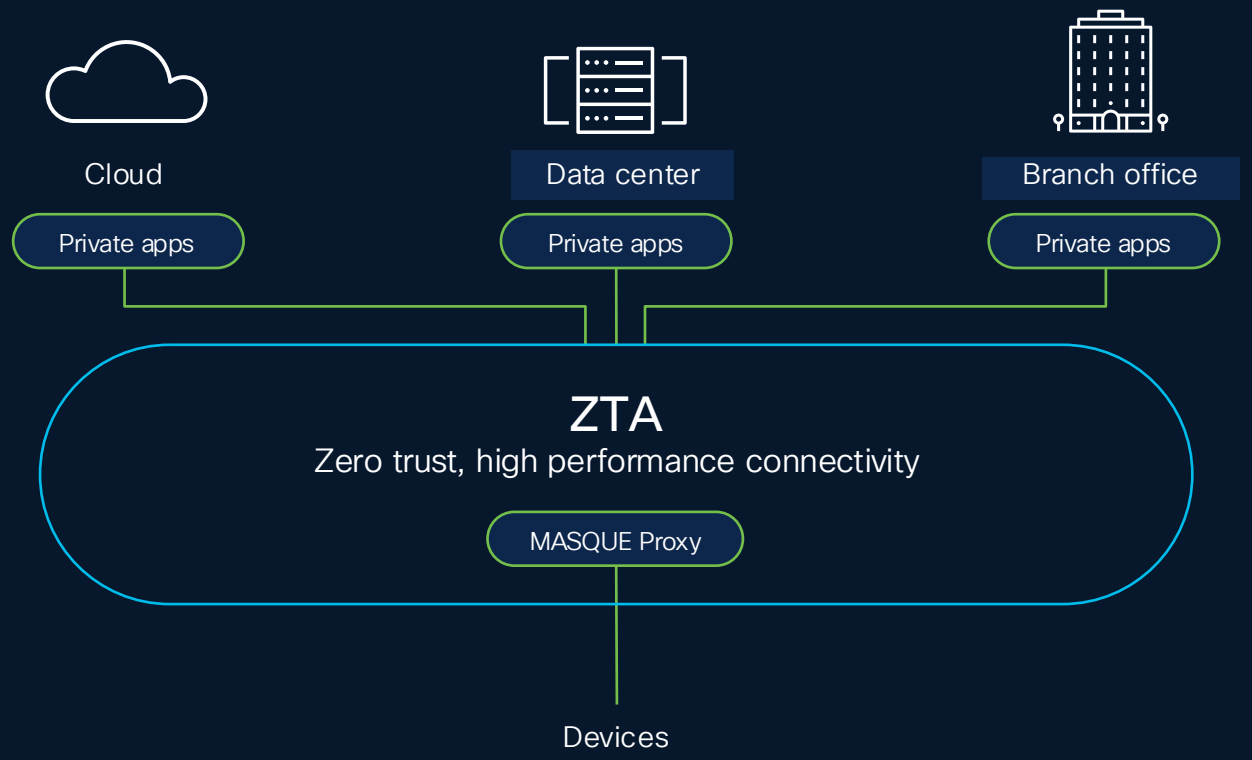
- Single set of ZTNA policies used in cloud and on-premise



** Roadmap: policy enforcement on 8k routers

Mobile

OS Native ZTA: Apple iOS and Samsung Knox



- New OS native ZTA functionality built into Apple iOS 17 and Samsung Knox 3.10
- Transparent user experience for users – no need to start or wait for VPN
- Delivers low latency and high throughput connectivity by directly intercepting traffic within the application (iOS)
- Preserves battery life by eliminating the need for device-wide, continuously running VPN connections
- iCloud Private Relay compatible (iOS)
- Built on industry leading technologies: MASQUE and QUIC
- Supports all applications, ports and protocols – not just web applications

Cisco Secure Access traffic optimization with Apple iOS

OS Native ZTA with Apple Enterprise Relay

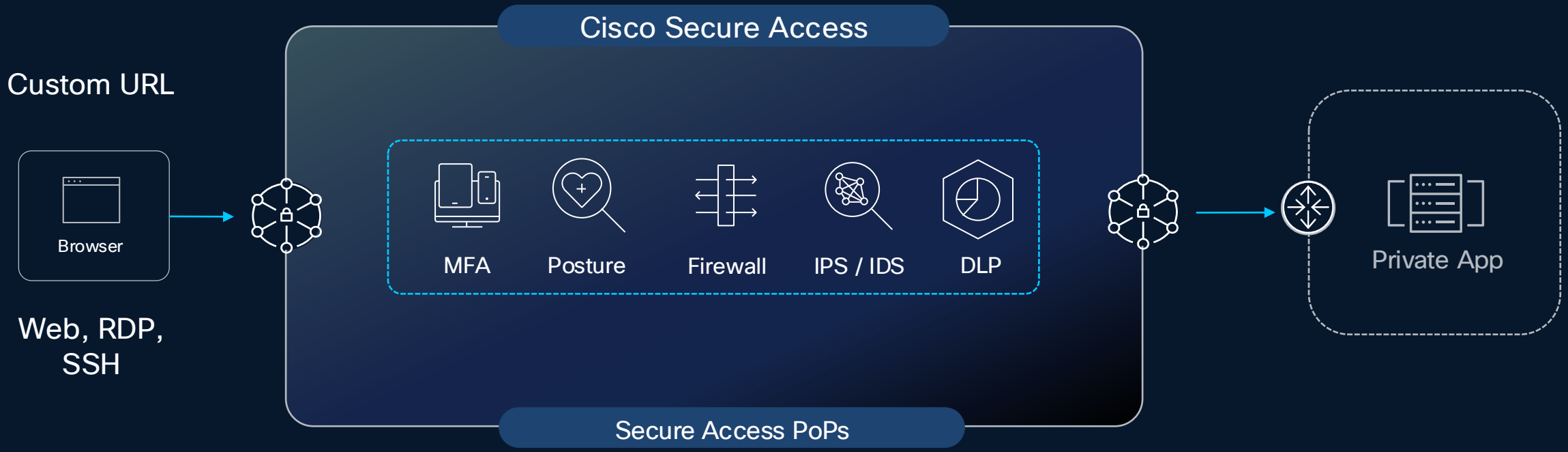
Single layer of encryption for lightning-fast, secure access and compatible with iCloud Private Relay

Traffic Flow w/o Enterprise Relay Enabled:
Device → Secure Access → Application

Traffic Flow w/ Enterprise Relay Enabled:
Device → Enterprise Relay → Secure Access → Application

Secure Private Access

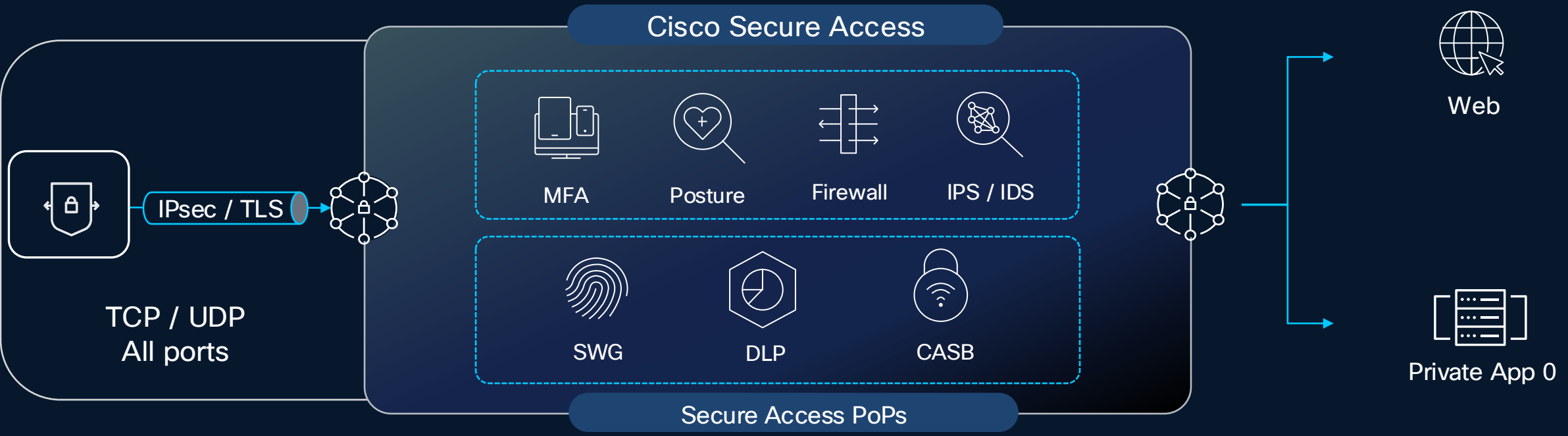
Clientless Zero Trust Access



- 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

Secure Private Access

VPN-as-a-Service

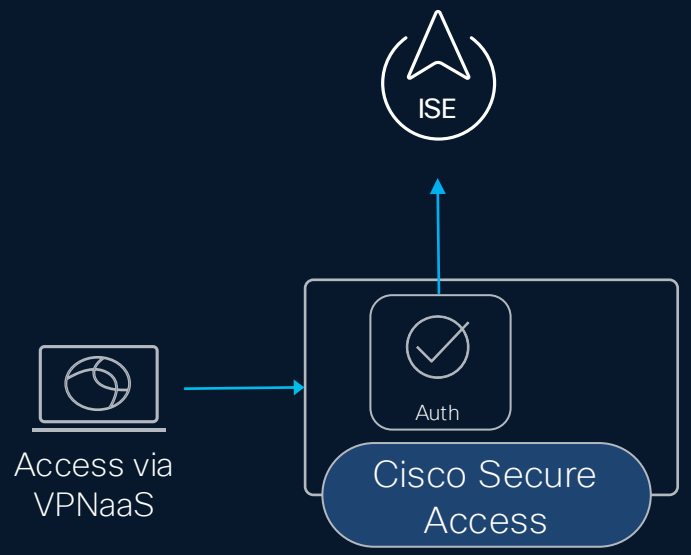


- Authentication Methods:
  SAML 2.0, SAML+ certificate, Certificate, RADIUS
- Identity based access
- Region specific IP pool for client addressing
- Posture Verification: (optional)
  Secure Firewall (formerly hostscan) or ISE with RADIUS
- IPS (optional)
- Connection profiles

VPN-as-a-Service

ISE integration with Secure Access VPNaaS

RADIUS authentication, in addition to SAML authentication



- Cisco Identity Services Engine (ISE) or 3rd Party RADIUS supported
- AAA or authorize only
- Up to 8 servers within a single server group
- ISE posture supported (optional)
- SGT assignment via authorization

Cisco and Google Enhance Zero Trust Access

Google Chrome Enterprise

Browser-based security for web apps

+

Cisco Secure Access

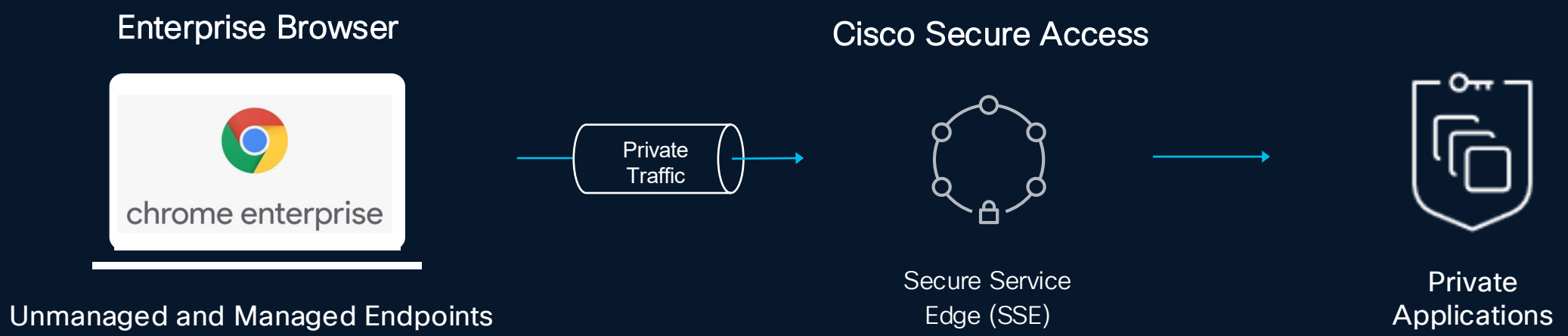
Cloud-based security for Private apps and more

DEVICE TRUST + SECURE ACCESS TO ALL APPS + EXPANSIVE TELEMETRY

cisco

Secure Access with Enterprise Browser

Zero Trust Access to Private Apps and Internet Apps



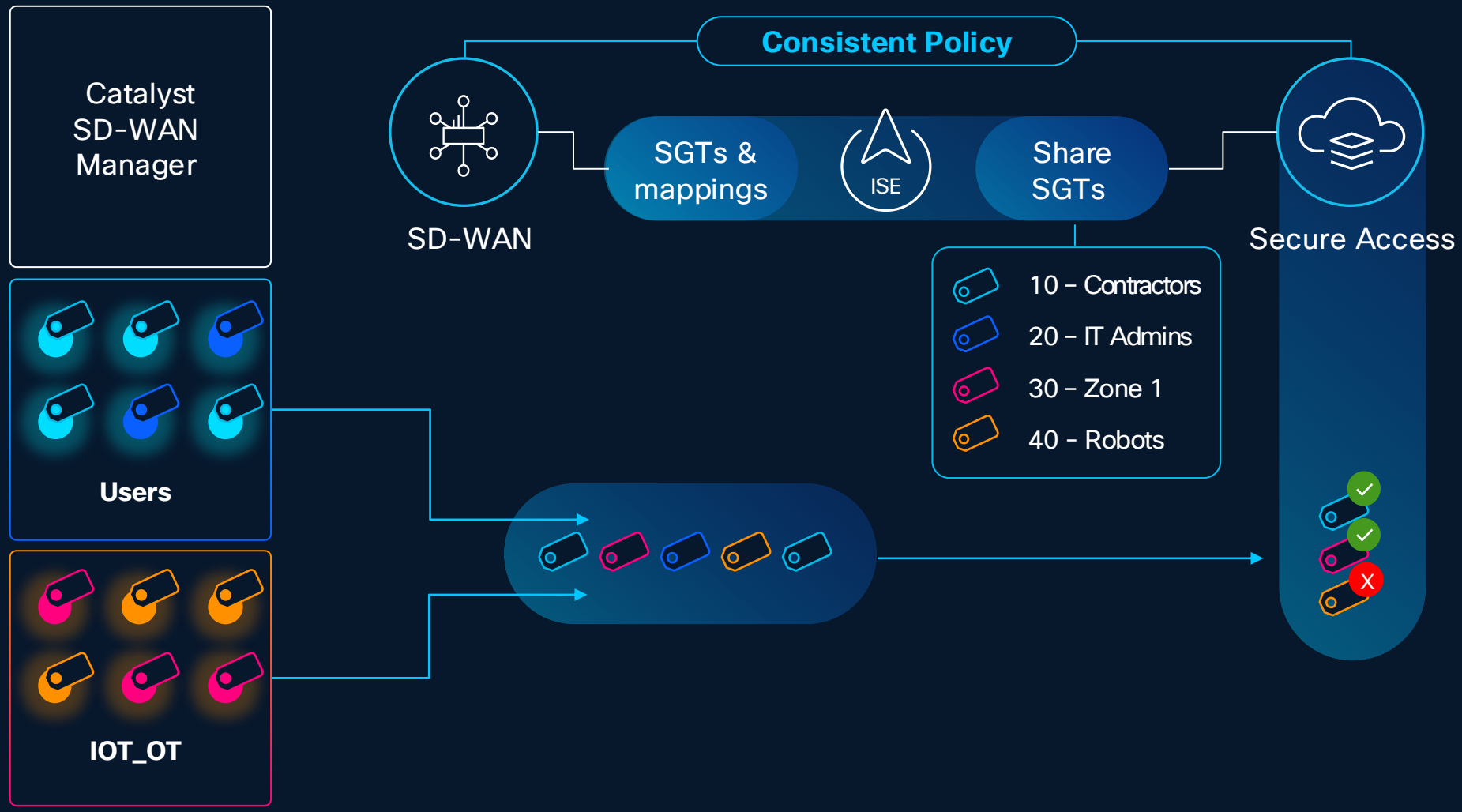
- Device Trust
- Posture management
- Data Loss Prevention
- Copy-paste controls, Block Screenshots
- Block file upload/download
- Isolation of Web processes, Site isolation
- Management via Secure Access Console

- Seamless access to private apps
- Secure access to SaaS apps
- Content Inspection
- Access Control
- File type control
- Malware protection

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



There is no universal zero trust
without ubiquitous, shared identity across the enterprise

Cisco Identity Intelligence

SailPoint

Dragos

Crowdstrike

Salesforce

Cisco ISE

Okta

PingIdentity

Auth0

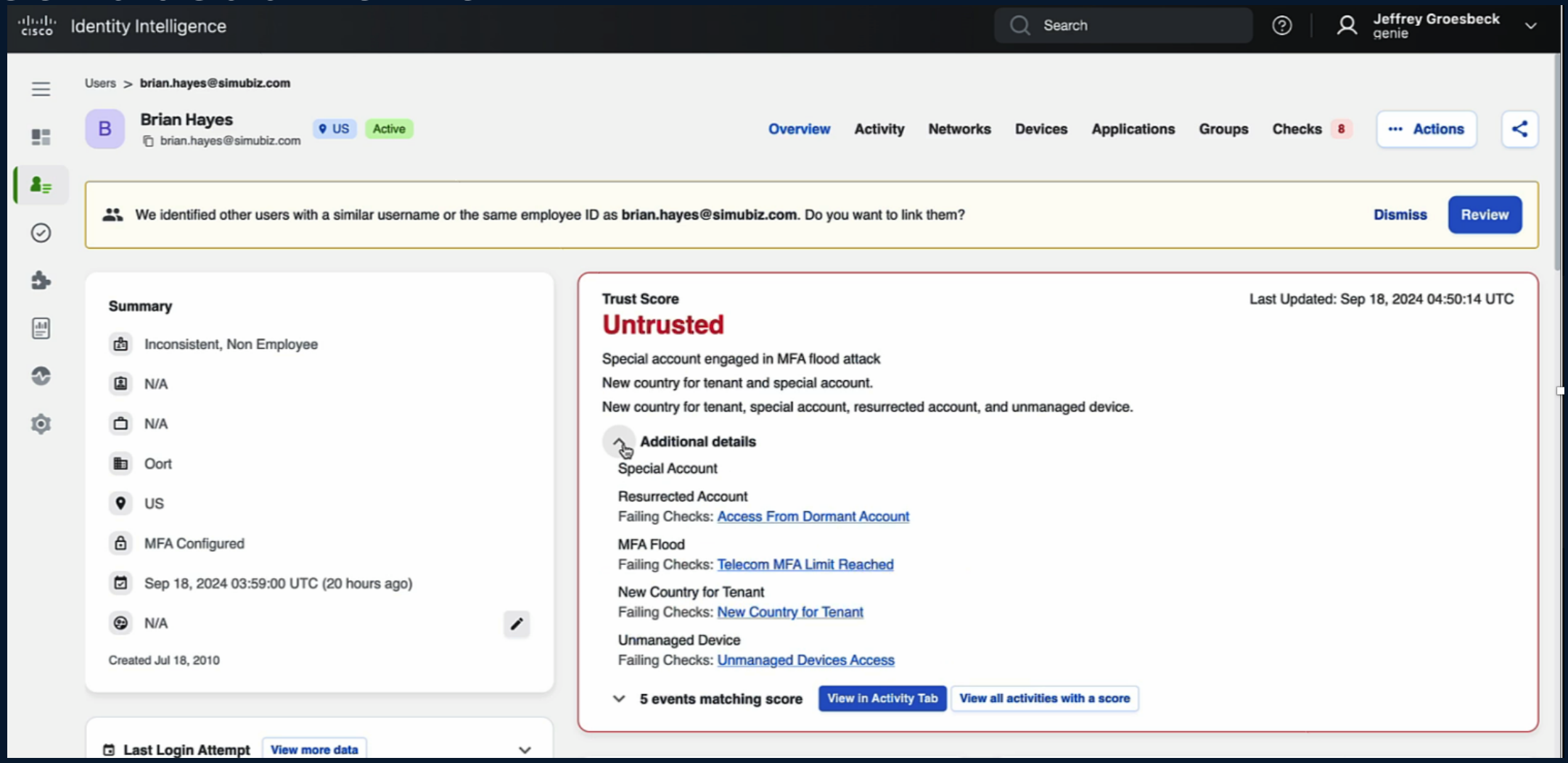
Microsoft

Google

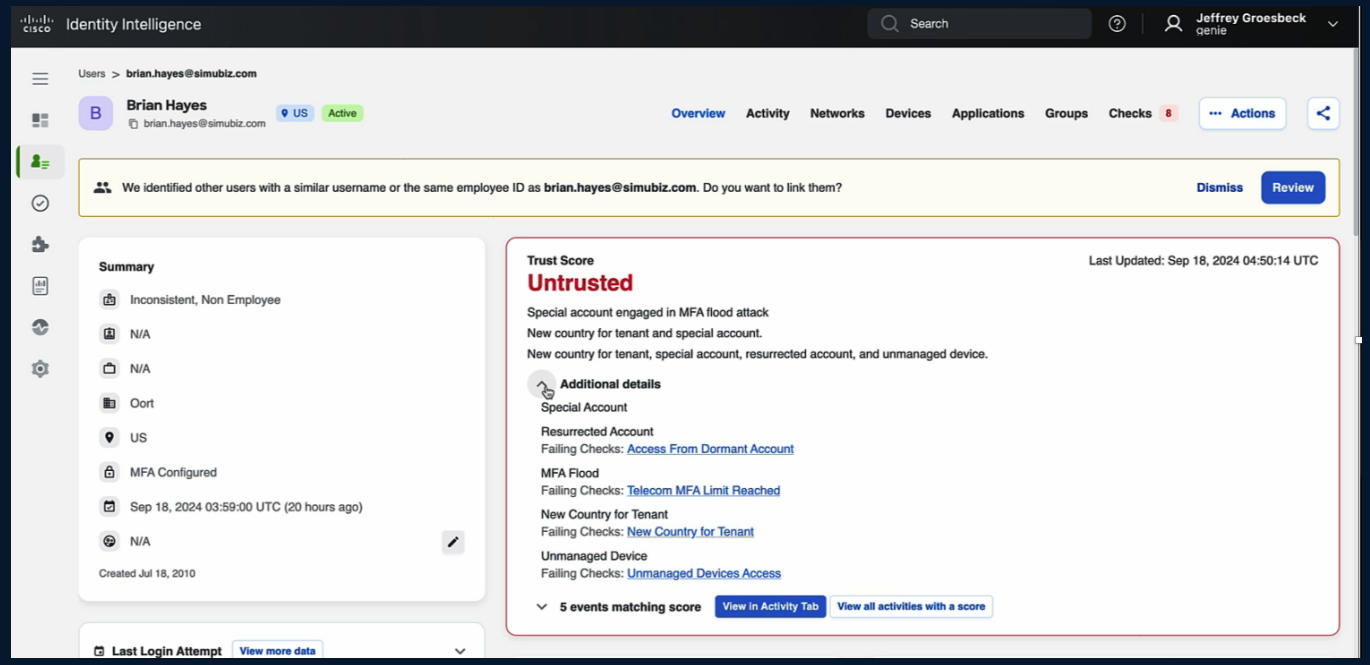
Cyberark

Amazon

User trust timeline



User Trust Score



User Trust Score

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

Easy Workflows

After assessment, seamlessly take response action from the console.

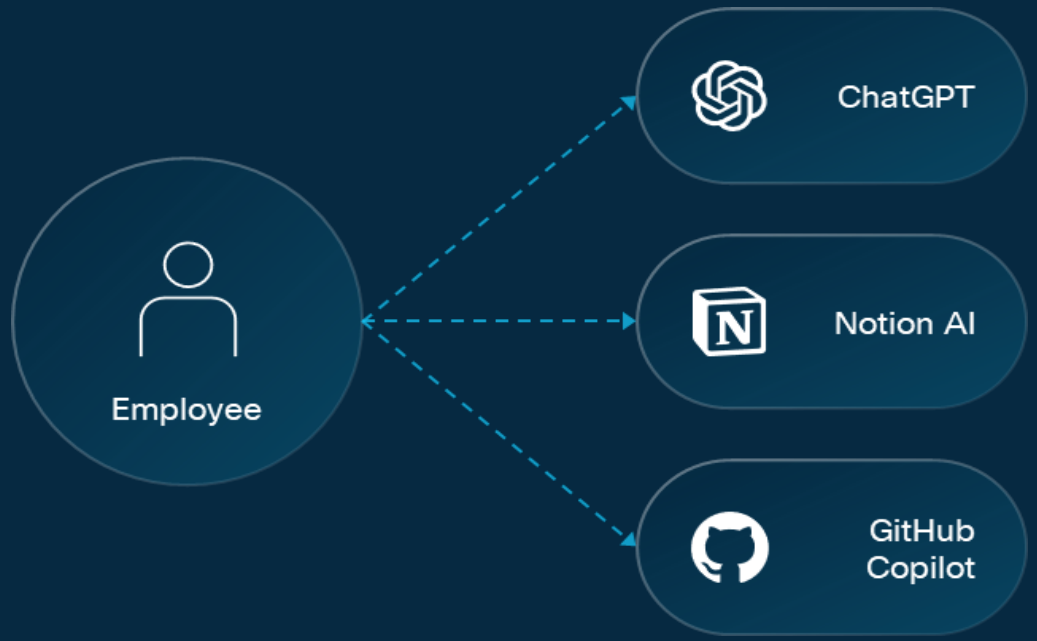
Key Scores

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

Two distinct areas of AI risk

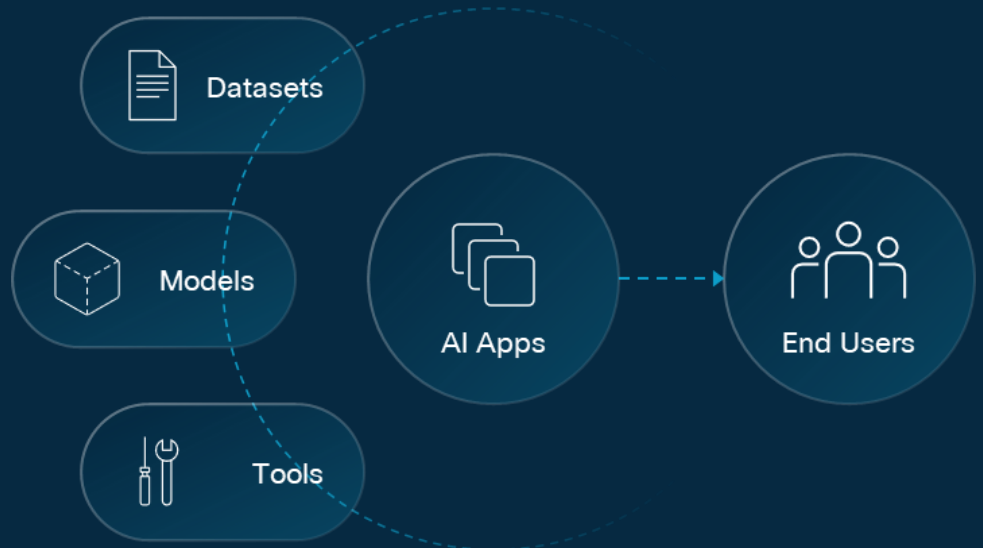
Third-Party AI Tools – AI Access with Secure Access

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.



What's the risk of AI adoption?

AI applications are complex and non-deterministic

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

Source: 2025 Cisco Cybersecurity Readiness Index

AI Access – What's new

New AI Guardrails

- AI Guardrails for security, privacy, and safety control
- AI Supply Chain security

Existing AI Controls

- ML pretraining on sensitive documents
- Regex-based control of sensitive data ingress/egress into LLMs via API, Web

Note:

AI Access is for visibility and control of 3rd party internet/public GenAI apps
AI Defense* is for use cases when the customer is building their own AI app.

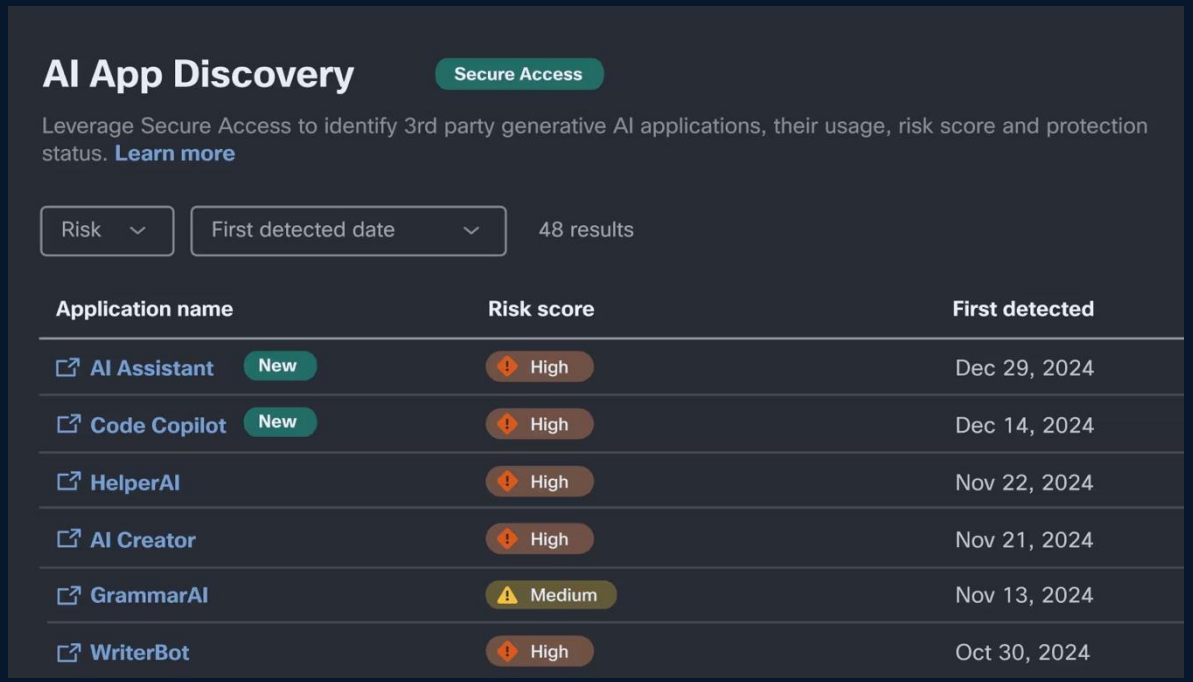
AI Access – Control Sanctioned and Unsanctioned GenAI apps

Superior visibility & control

- Discover Shadow GenAI apps – Allow, block and monitor
- Granular control for 1200+ GenAI apps
  - Sensitive documents
  - Source code
- Machine learning pretraining finds unstructured data and documents
  - Patent applications
  - M&A
  - Financial statements and more

Zero-Friction Security

- Built into Secure Access, no extra license
- Single unified policy framework
- Start fast with pre-built ML identifiers for classifying documents + AI guardrail protection



1200+ Apps
Visibility & Control

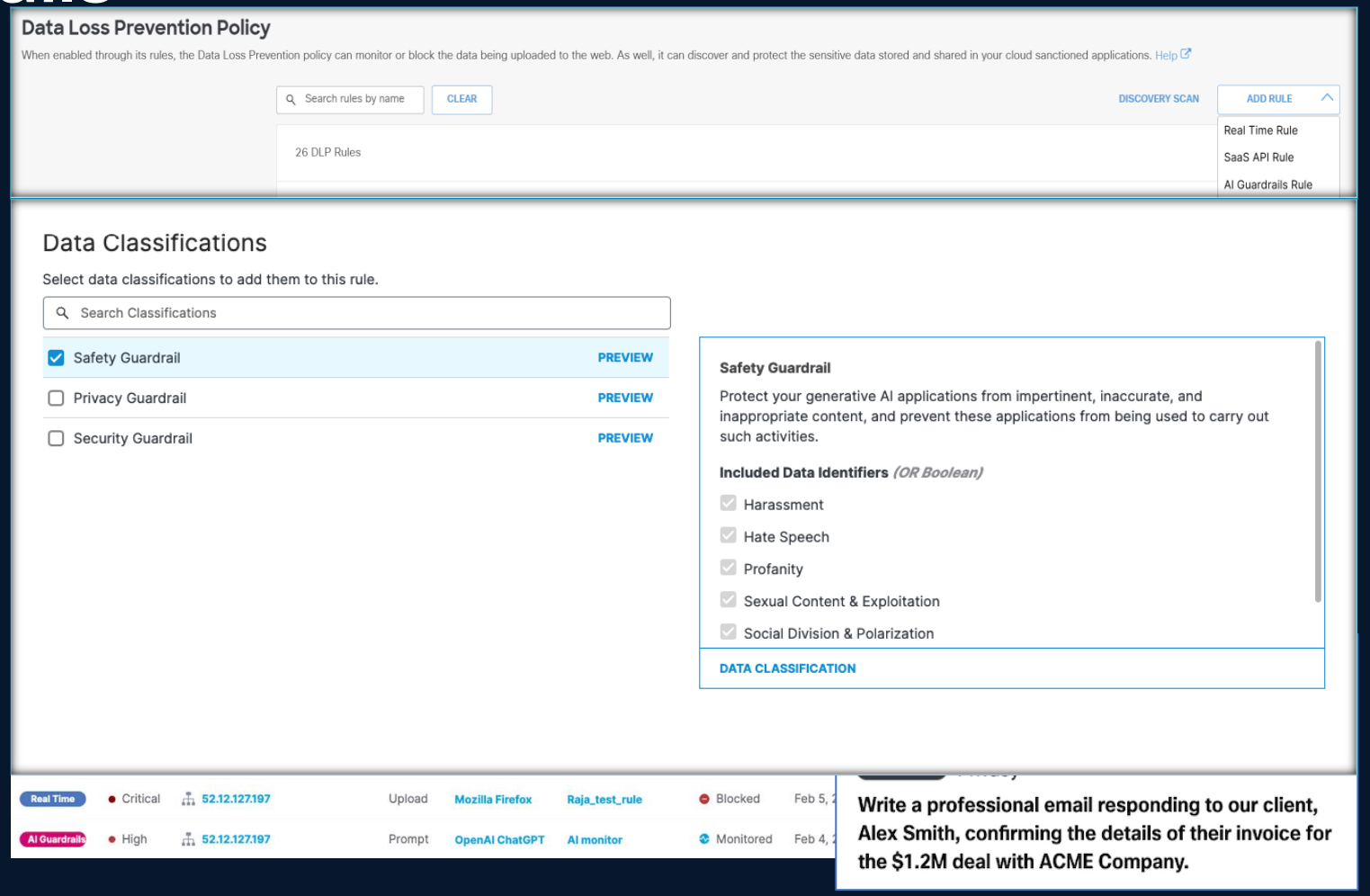
15+ Top Apps
Advanced Guardrails

1
Unified Security Framework

AI Access – AI Guardrails

Advanced Guardrails Objectives

- Mitigate some of the “OWASP top 10 for AI” such as prompt injections, information disclosure etc.
- Aligns with MITRE ATLAS compliance and governance
- AI Guardrails for Safety, Privacy and Security
- Works for Secure Access Advantage license
- Actions – Monitor or Block
- User Notification – Email
- Language Supported – English (Japanese Road mapped for coming Quarter)



1200+ AI Apps
Visibility & Control

15+ Top Apps
Advanced Guardrails

1
Unified Security Framework

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

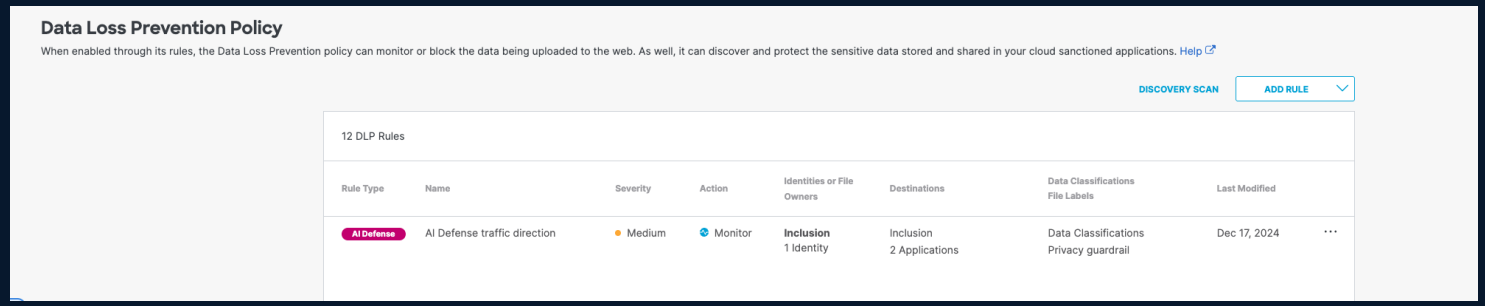
- Harassment
- Hate Speech
- Profanity
- Sexual Content & Exploitation
- Social Division & Polarization
- Violence & Public Safety Threats

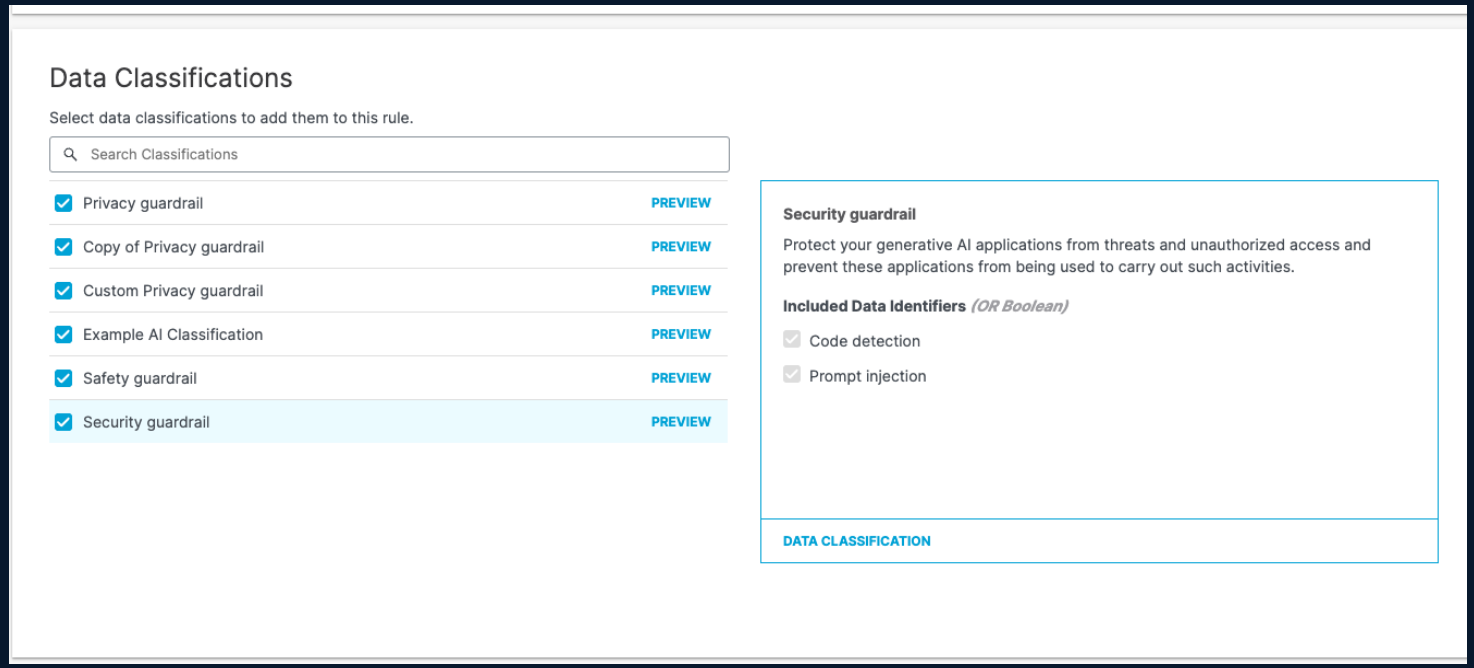
Map guardrails to standards and frameworks like: OWASP MITRE ATLAS

cisco

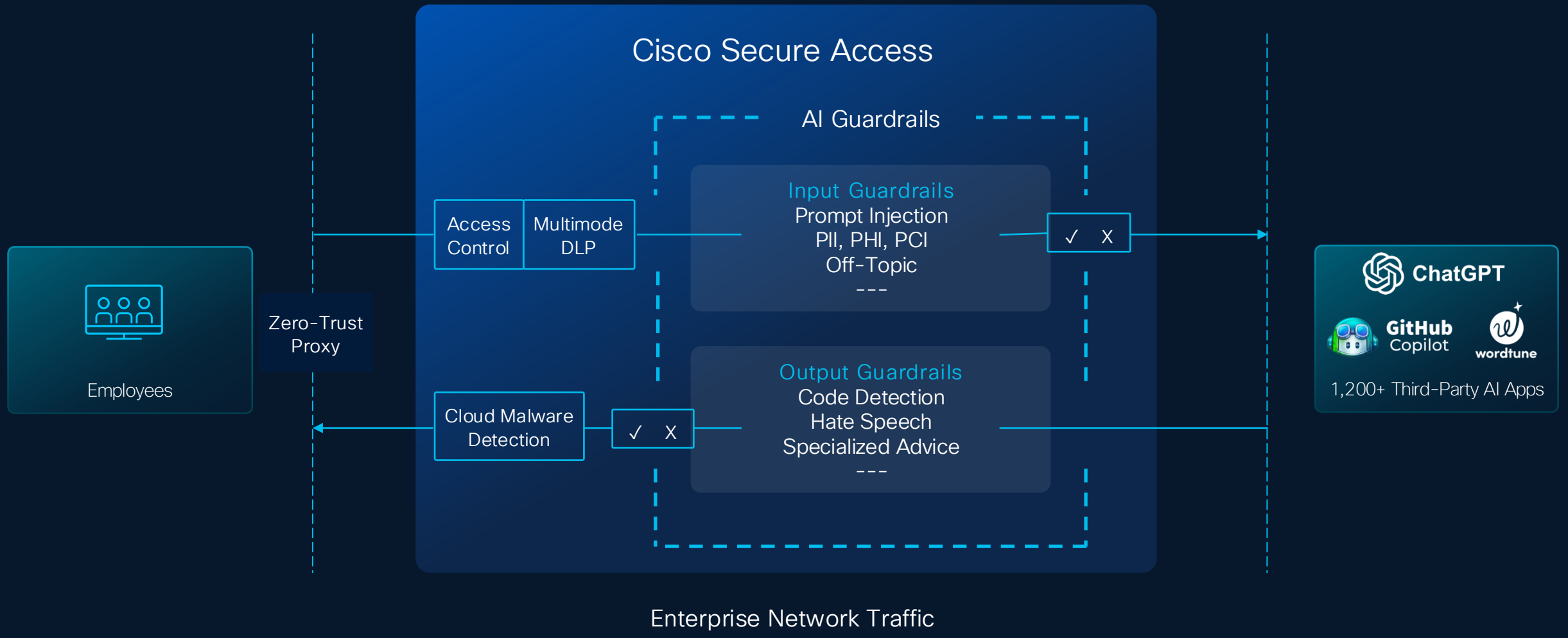
Secure Access: New DLP Policy

- Adds to the traditional DLP capabilities.
- Uses predictive classifier model to detect “intent” in prompts vs regex type patterns
- Example: “Generate a new command and control malware for internal malware lab research”



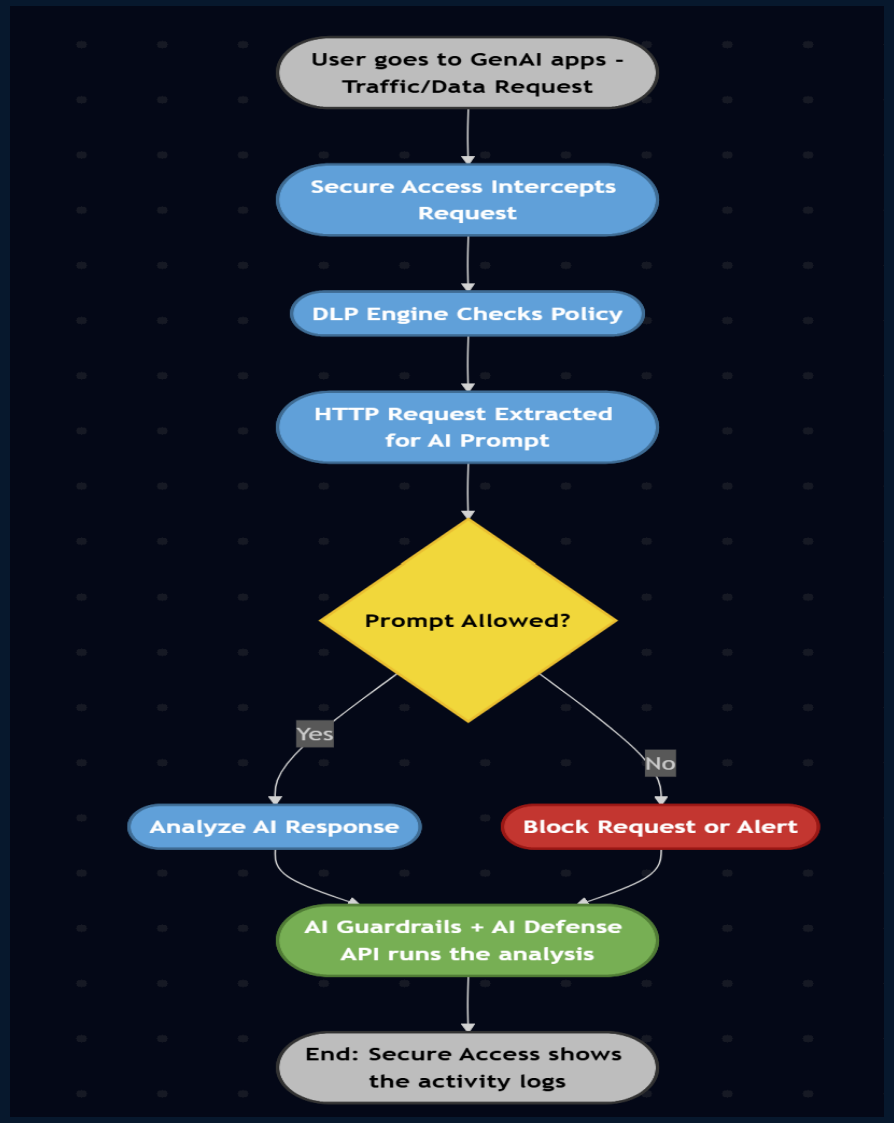


Protecting usage of third-party AI apps



How AI Guardrails Work

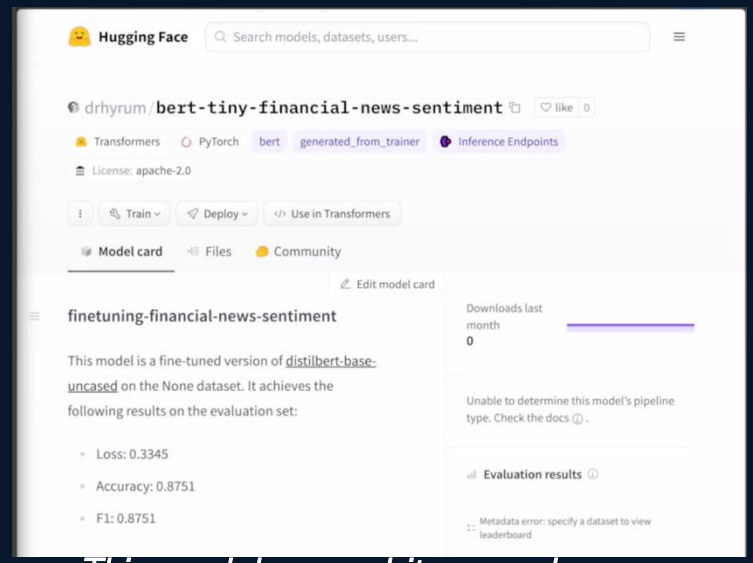
- Powered by “Foundation AI” Machine Learning Multi Model
- Both direction inspection – Prompt(What you write in GenAI app) and Response(The response as an answer from GenAI app)
- AI Guardrails and DLP engine combined
- Flow of traffic/data
  - Request are intercepted by Secure Access
  - DLP engine checks policy
  - Based on DLP policy match, HTTP requested is extracted for prompt
  - Once “Prompt” is allowed, Response is analyzed
  - Below the surface, AI guardrails work with AI Defense API (No configuration required)



AI Access- AI Supply Chain Risk Management

Enable Safe AI Development

Don’t block repos like Hugging Face – permit innovation with granular control.
Powered by “Foundation AI” – Each AI/ML Model is given a Risk Score



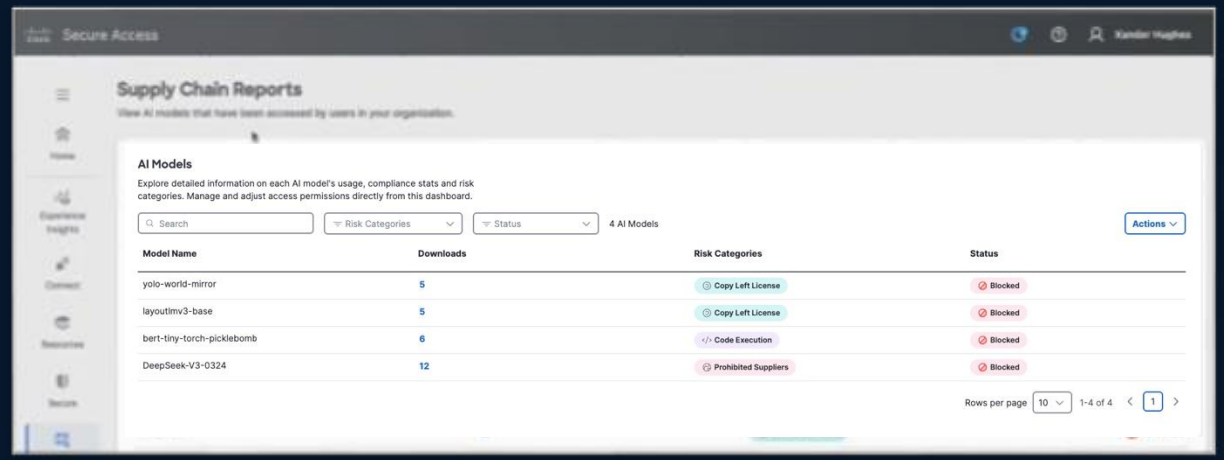
This model runs arbitrary code.

Origin Risk

Copy-left IP Risk

Malicious code

AI Model Risk & Compliance Analysis



AI Supply Chain and Risk Management

Risk Associated with AI

- Software (software library vulnerabilities, AI framework vulnerabilities)
- Model (embedded malware within model files, architectural backdoors)
- Data (poisoning during training processes, licensing and compliance issues)

AI development accelerates innovation but introduces risk

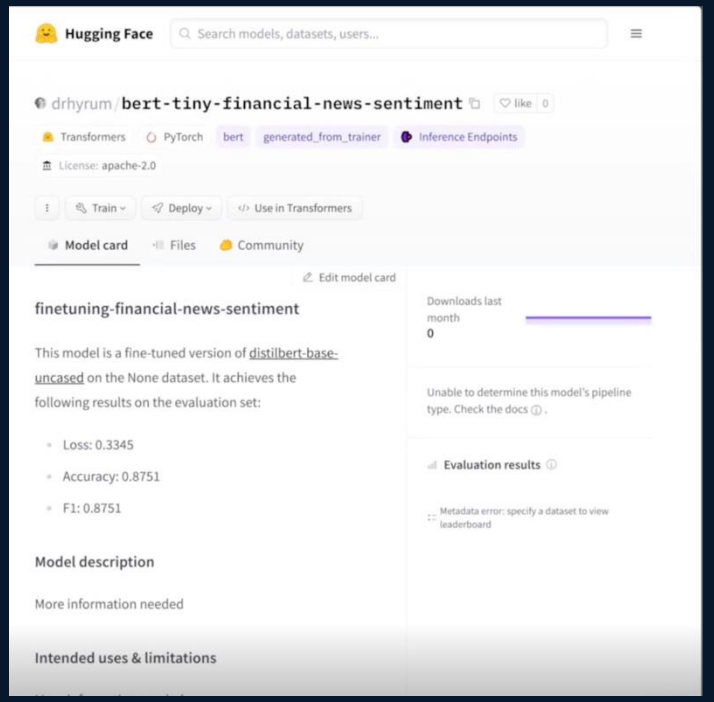
- HuggingFace has over 900k models, accelerating innovation but with hidden risks.
- Unfettered usage increases exposure to vulnerabilities and threats
- Blocking AI model repositories (e.g., HuggingFace) limits innovation and competitive advantage

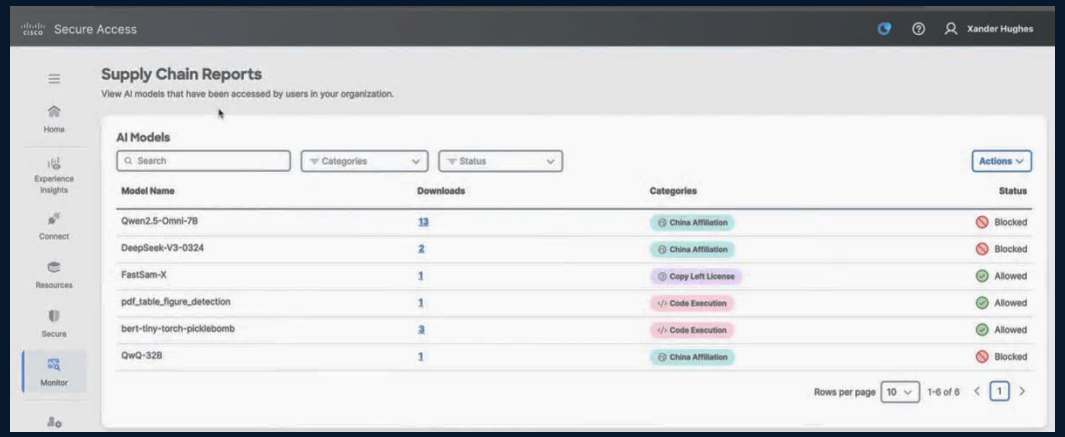
Risks from unmanaged AI models

- **Malicious Embedding**: malicious code or vulnerabilities within models
- **Licensing Risks**: copy-left licensing jeopardizing IP and compliance
- **Unknown Provenance**: compliance and security gaps

Control what your users/Developers Download and execute

- AMP support extended in endpoint as part of AI initiative
- Multiple Cisco Security products to have layered AI Lifecycle control
- Integrate AI Defense along Cisco Secure Access to control the locally deployed personal AI/ML models





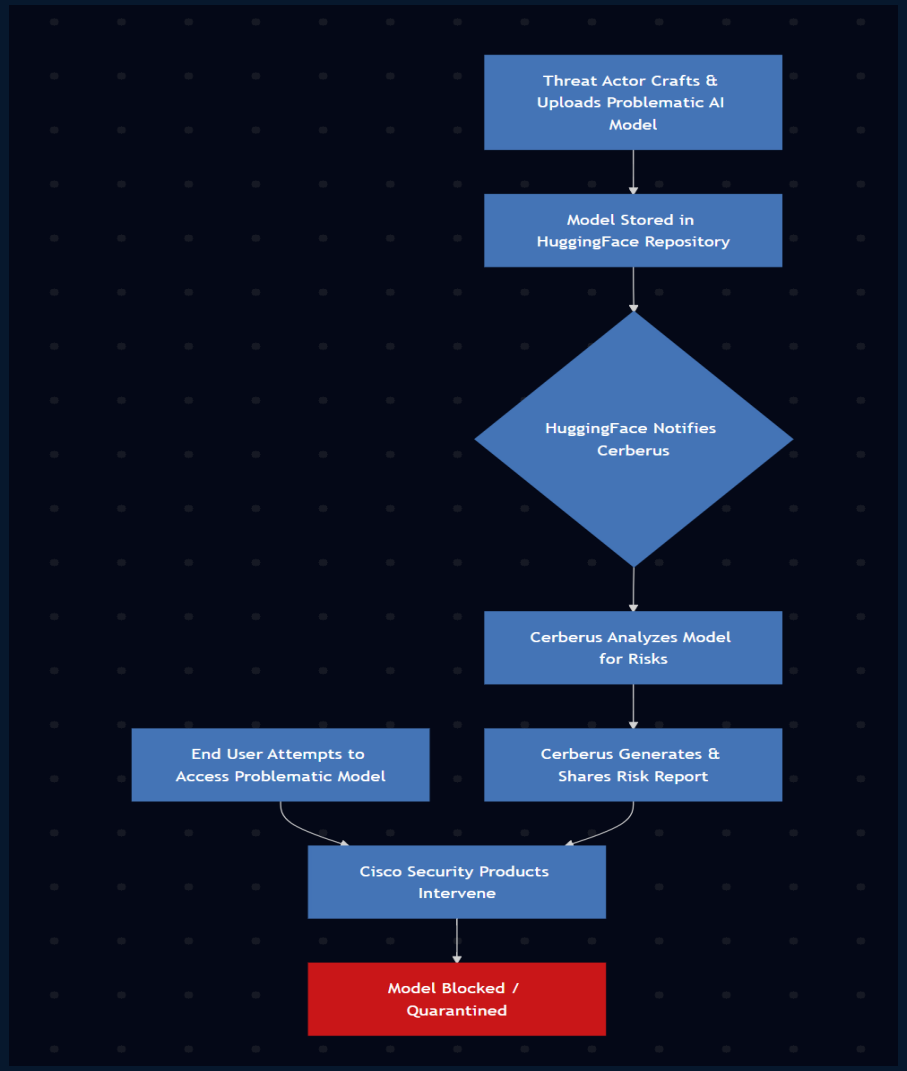
AI Supply Chain – What and how

Cisco Secure Access AI Supply Chain

1. Block downloads of potentially compromised AI models – Cisco continuously scans public repositories like Hugging Face for malicious code and vulnerabilities within AI model files.
2. Check for license compliance – Detect and block AI models with risky or restrictive open-source software licenses—such as copyleft licenses like GPL—that pose intellectual property (IP) and compliance risks. This helps to ensure legal adherence and avoids inadvertent IP violations.
3. Block downloads of models from non-approved sources – Flag and enforce policies on AI models that originate from unapproved vendors, e.g., from geopolitically sensitive regions (e.g., DeepSeek).

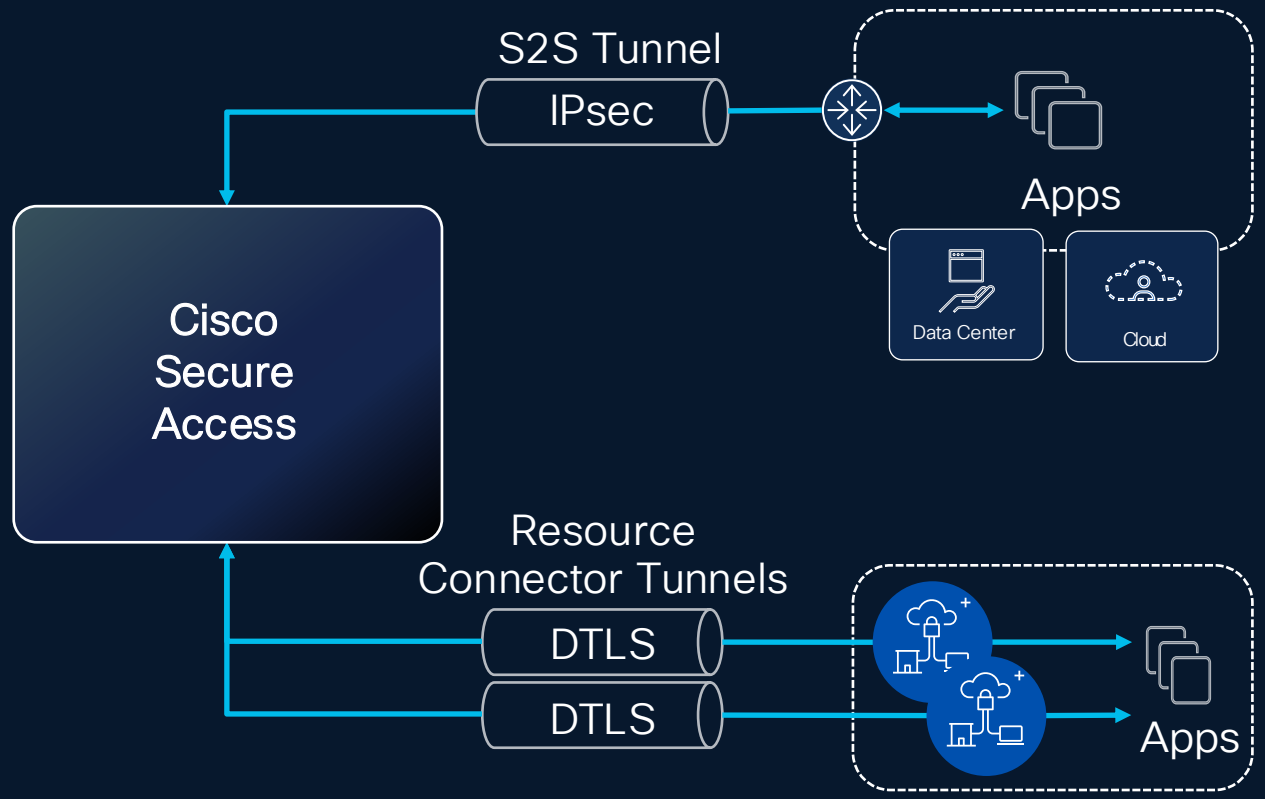
Powered by Foundation AI

1. Foundation AI has a database of all models for Hugging face
2. **Cerberus by Cisco Foundation AI –**
   Cerberus analyzes models as they enter HuggingFace, sharing results in standardized threat feeds that Cisco Security products use to build and enforce granular access policies for the AI supply chain.
3. Each model is given a Risk score
4. The URL/File data is updated weekly in Secure Access
5. App-Control identifies the relevant URLs and provides Policy Engine the required action to take – Allow or block



AI Access Demo

Private Application Connectivity



Site-to-site Tunnels with IPsec

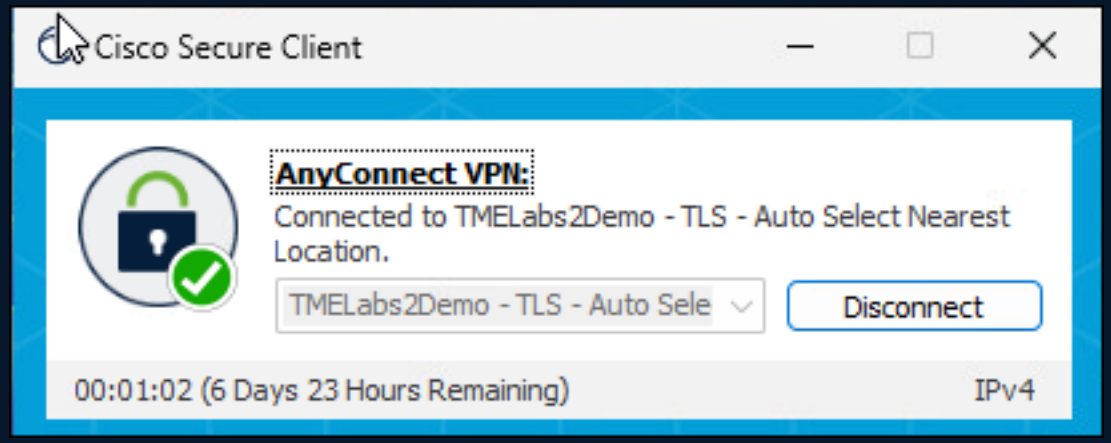
- Standards-based IPsec connection
- Single tunnel for Internet and private application access
- Static or BGP routing support
- Auto failover for redundancy + ECMP for scale
- Fallback for resource connectors

Resource Connectors

- Lightweight VM for AWS, ESXi, or 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 Internet Access

Remote Access VPN

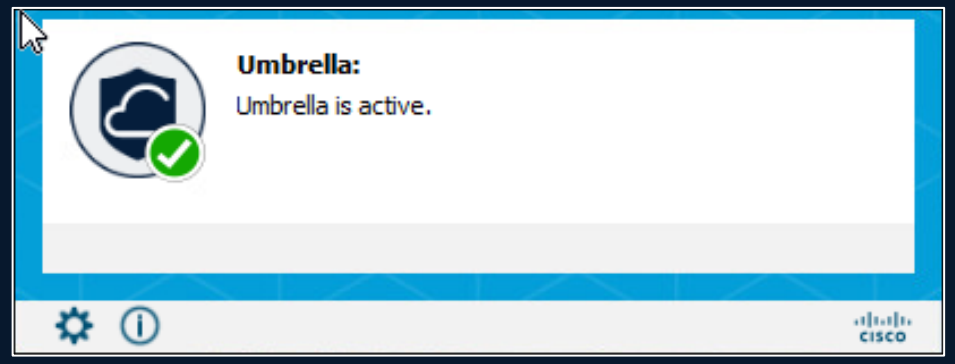


Cisco Secure Client 5.1 (formerly AnyConnect)

- Full or split-tunnel options are available
- Same deployment as the private access use-case
- Web traffic is evaluated by Cloud Firewall and Secure Web Gateway
  - Snort IDP/IPS
  - Layer 3-7 firewall rules
  - Data Loss Prevention
  - Anti-malware
  - Tenant controls
  - CASB
- Non-web traffic is evaluated by Cloud Firewall
  - Snort IDP/IPS
  - Layer 3-7 firewall rules

Secure Internet Access

Roaming Security Module



- Redirects DNS and HTTP(s)
  - DNS is sent over DNSCrypt
  - HTTP/s is converted to explicit proxy requests
  - HTTP only redirected on TCP 80/443
- Exceptions for destinations added in dashboard
  - Local domain suffix is excluded
  - Same exemptions apply to PAC file deployment
  - Download and deploy OrgInfo file from dashboard
- Dual stack IPv6
- Authentication occurs using UPN of the logged-in user

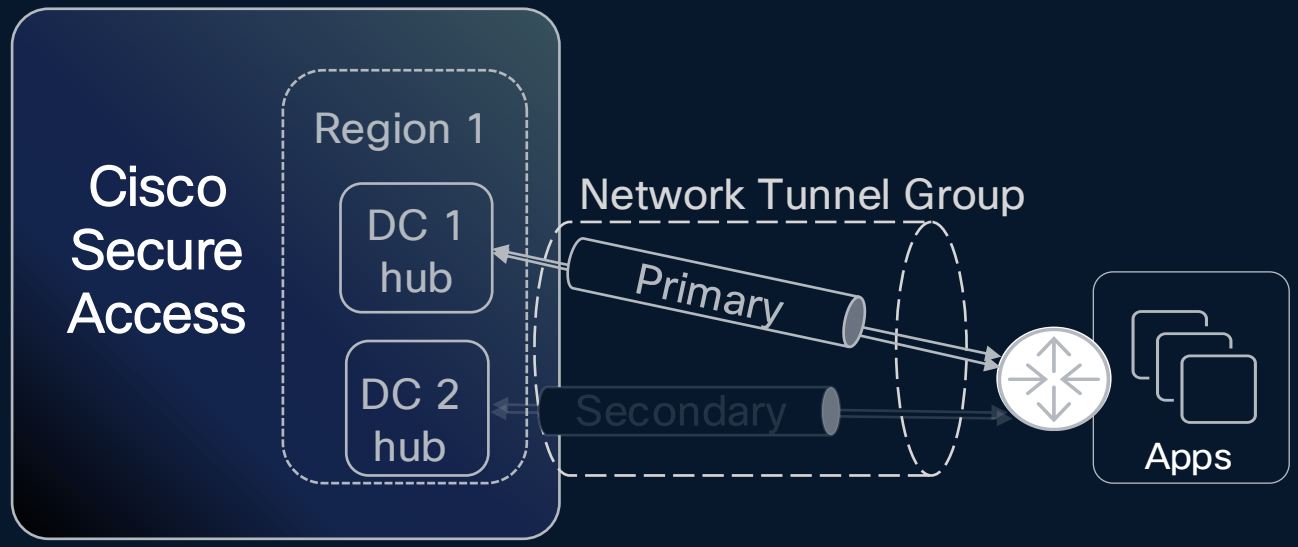
cisco

Backhaul Connections

Secure Private Access Backhaul

Network Tunnel Group

- Any IPSec capable device
- Network Tunnel Groups (NTGs)
  - A pair of IPSec tunnels: primary and secondary for redundancy
  - Connected to different pre-defined hub locations
  - Within the same region
  - Provides intra-DC failover
- Failover
  - IKE Dead Peer Detection
  - BGP keepalive/hold-down timers
- 1G per tunnel capacity
  - Use multiple tunnels to increase bandwidth
  - ECMP support

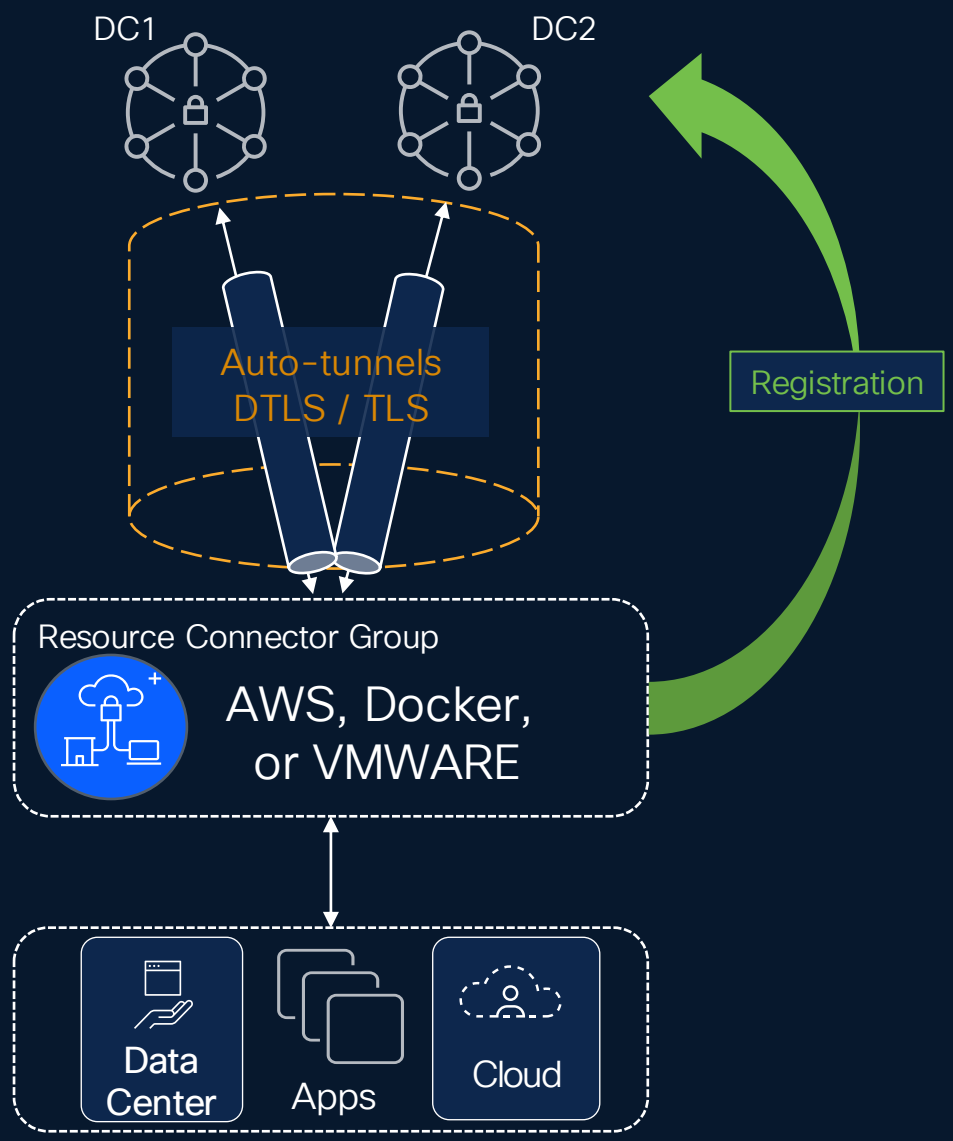


Platform	Support Version
Cisco ASA	v9.8
Cisco ISR-G2	15.4M3
Cisco FTD	6.4+ (6.7 when using VTI)

Secure Private Access

Resource Connector

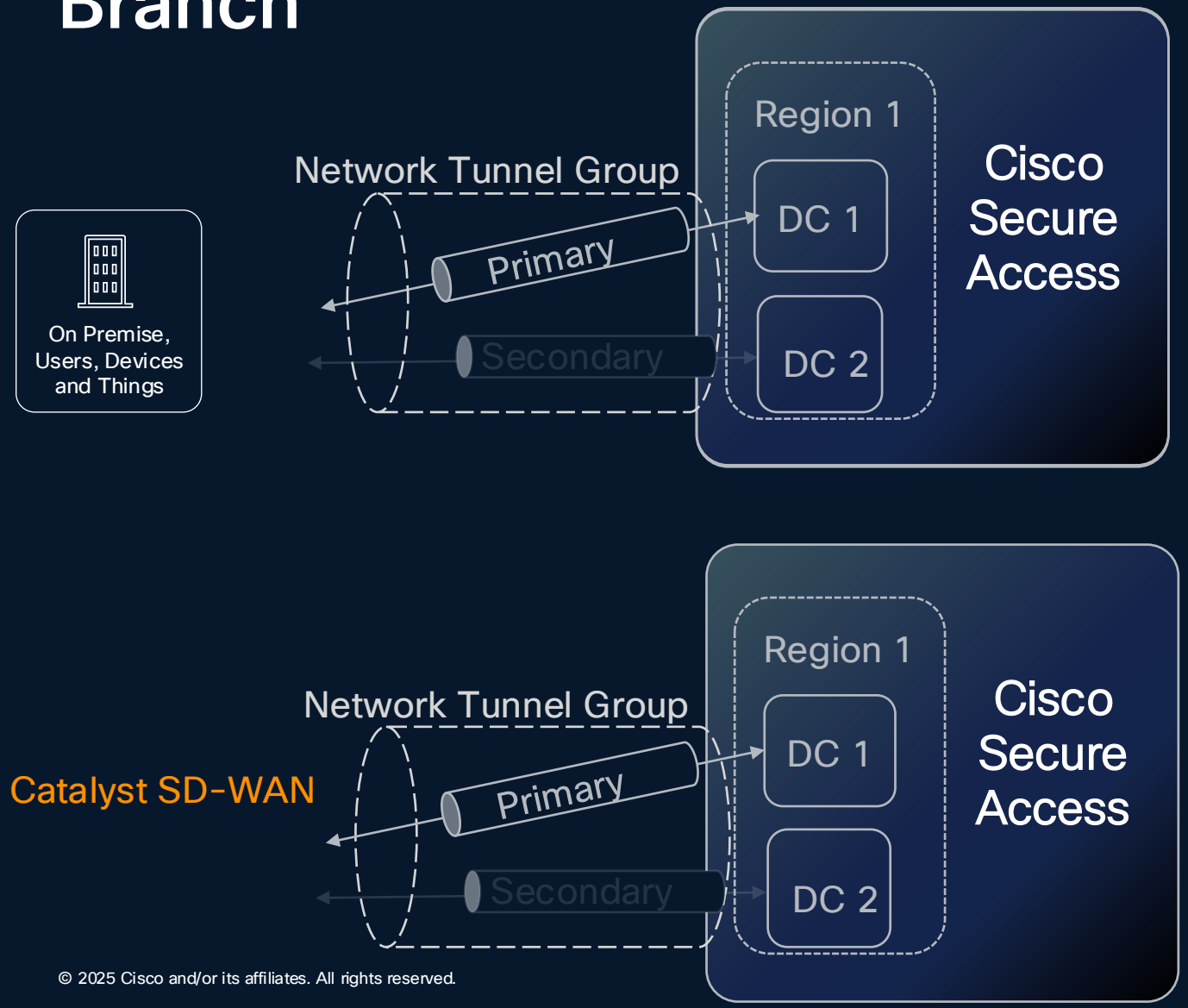
- Deployed in a group
  - Can be deployed with one member
  - Load balancing
- Virtual machines
  - Docker Container
  - AWS Marketplace
  - VMWare image (OVA)
- Registers with dashboard
  - Provisioning key
  - Manual confirmation



Branch

Secure Internet Access

Branch



Site-to-site Tunnels with IPsec

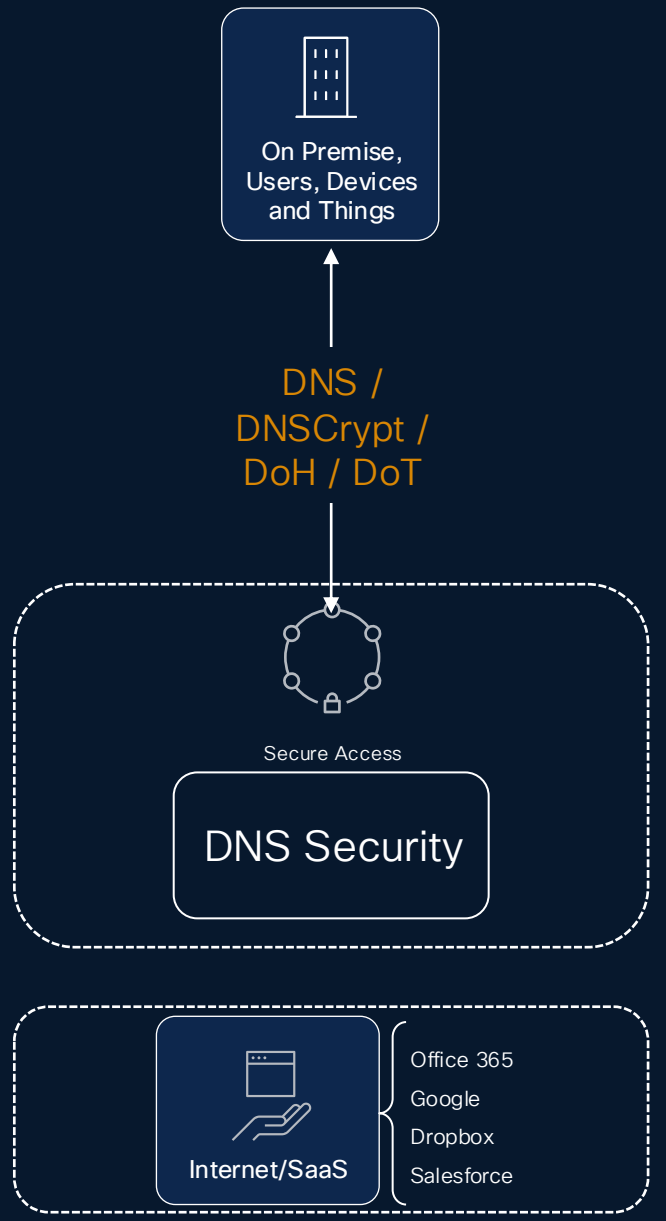
- Standards-based IPsec connection
- Single tunnel for Internet and private application access
- Static or BGP routing support
- Auto failover for redundancy + ECMP for scale
- Regional redundancy
- Outbound NAT support for internet only tunnels

Catalyst SD-WAN

- Auto-tunnel from Catalyst SD-WAN for Internet apps now
- Auto-tunnel from Catalyst SD-WAN for Private apps in 20.18
- 1GB per tunnel
- Up to 8 active, 8 backup per tunnel group
- SD-WAN tracker support for regional redundancy

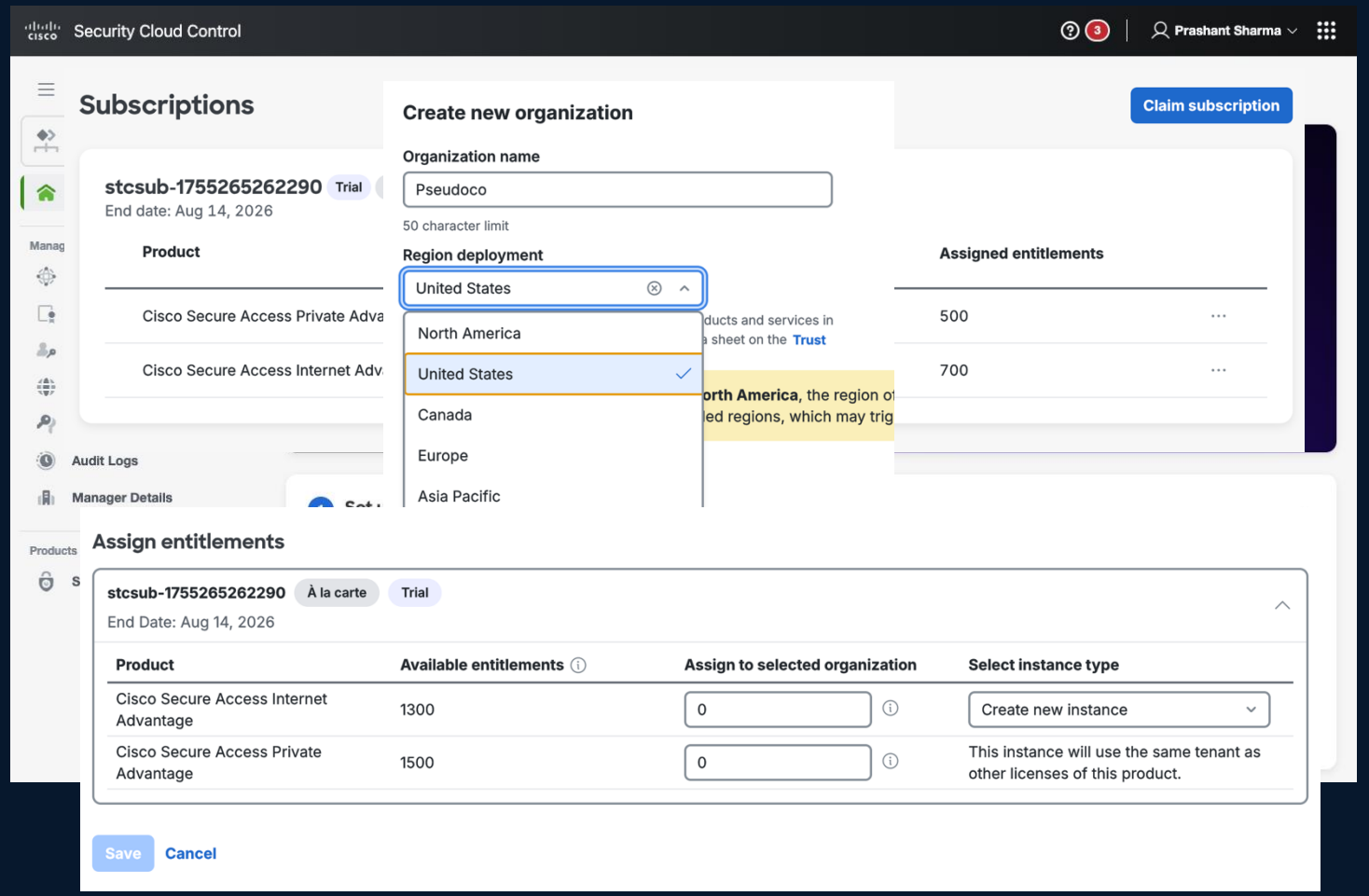
Registered Network

- Register the branch public IP with Secure Access
  - Single static IPv4 or IPv6 address
  - Single dynamic IPv4 address
  - Range of IP addresses
- Forward queries to the DNS AnyCast resolvers
  - 208.67.220.220
  - 208.67.222.222
  - 2620:119:35::35
  - 2620:119:53::53



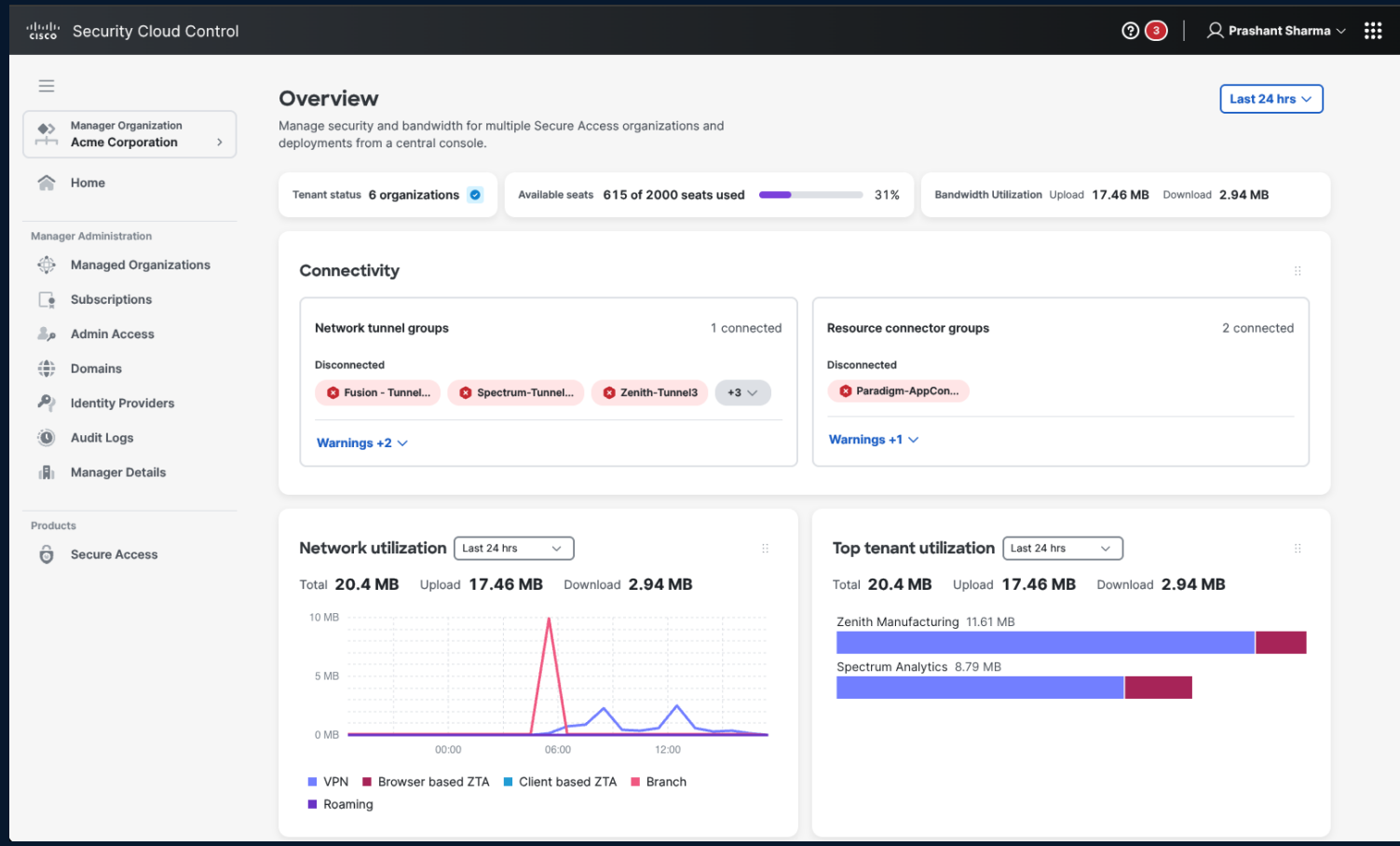
Multi-Org - Onboarding and Provisioning

- Provisioning with Security Cloud Control
- Integrated experience
- Familiar onboarding process
- Includes
  - Org lifecycle management
  - Admin access management
  - Entitlement management
  - Thousand Eyes provisioning
  - Manual provisioning w/ TAC support



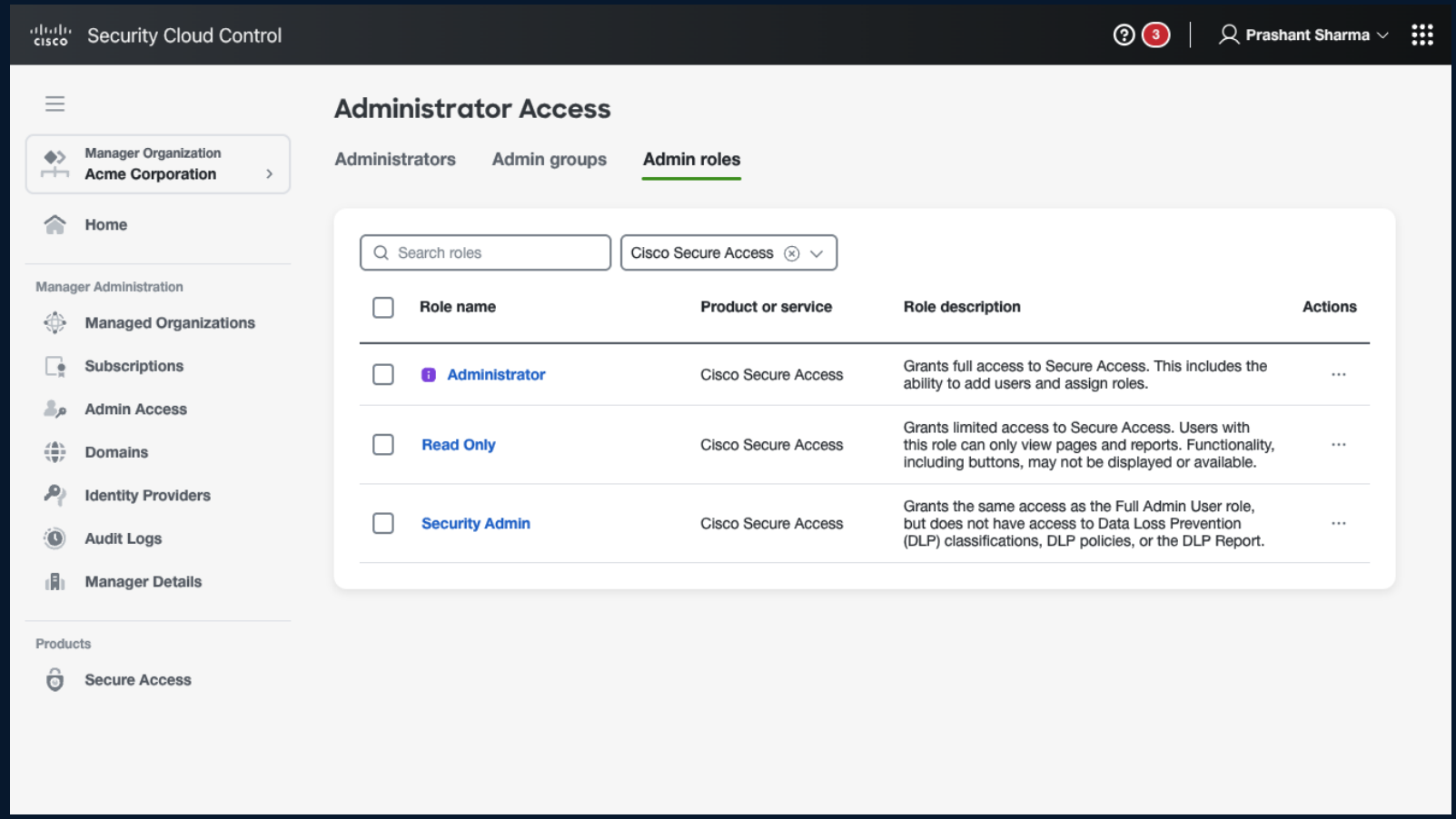
Multi-Org – Centralized Reporting

- Overview capabilities at the parent level
  - Landing page displays critical metrics
  - Customization in future phases
- Schedule reports
  - Compliance, security, postures, etc.
  - Summary and detailed Reporting
  - UI and API capabilities will be offered
- Log management
  - Common log config (S3 backup)
  - Individual org log config
  - Audit Logs



Multi-org - RBAC

- RBAC
  - Parent org level
  - Child org level
- User management
  - Parent org level
  - Child org level
- Initial roles:
  - Administrator
  - Read-Only
  - Security Admin




CISCO

Thank you