CISCO Connect

Universal Zero Trust Access

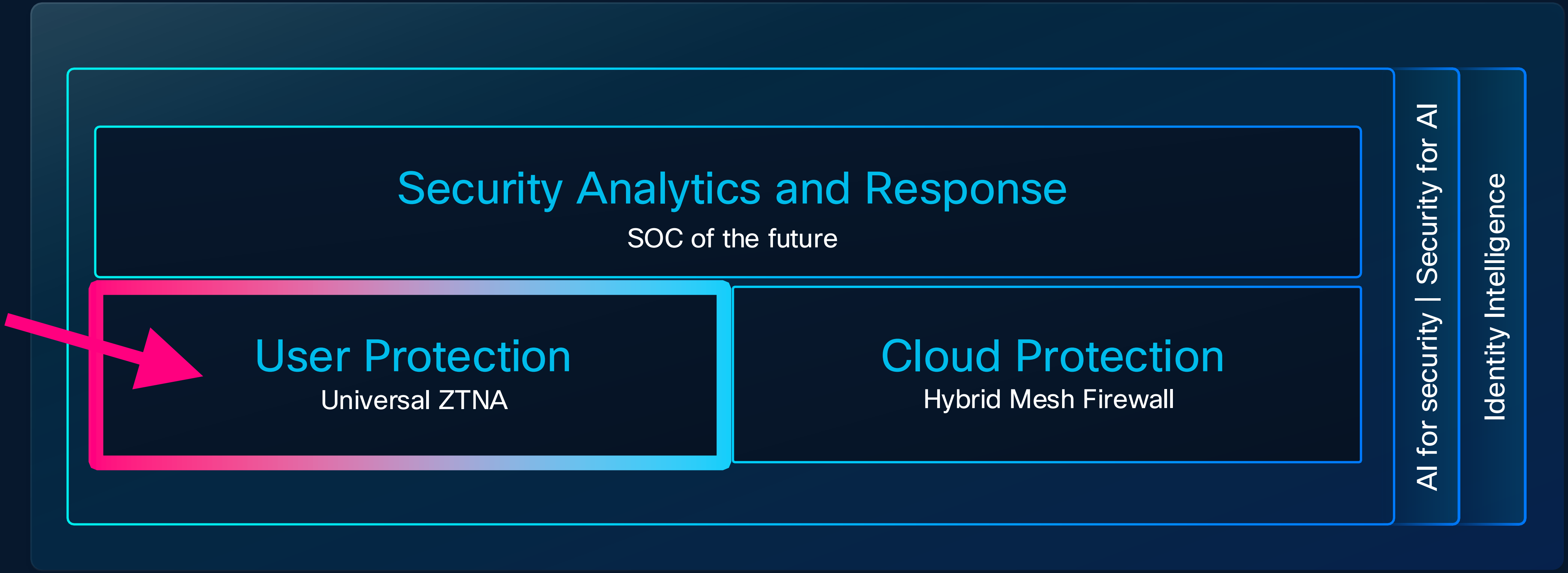
Håkan Nohre

Cisco EMEA Cyber Security

28 years, 1 month, 24 days, 5 hours

Dec 2, 2025 A.D

Cisco Security Cloud Architecture



Security Analytics and Response

SOC of the future

User Protection

Universal ZTNA

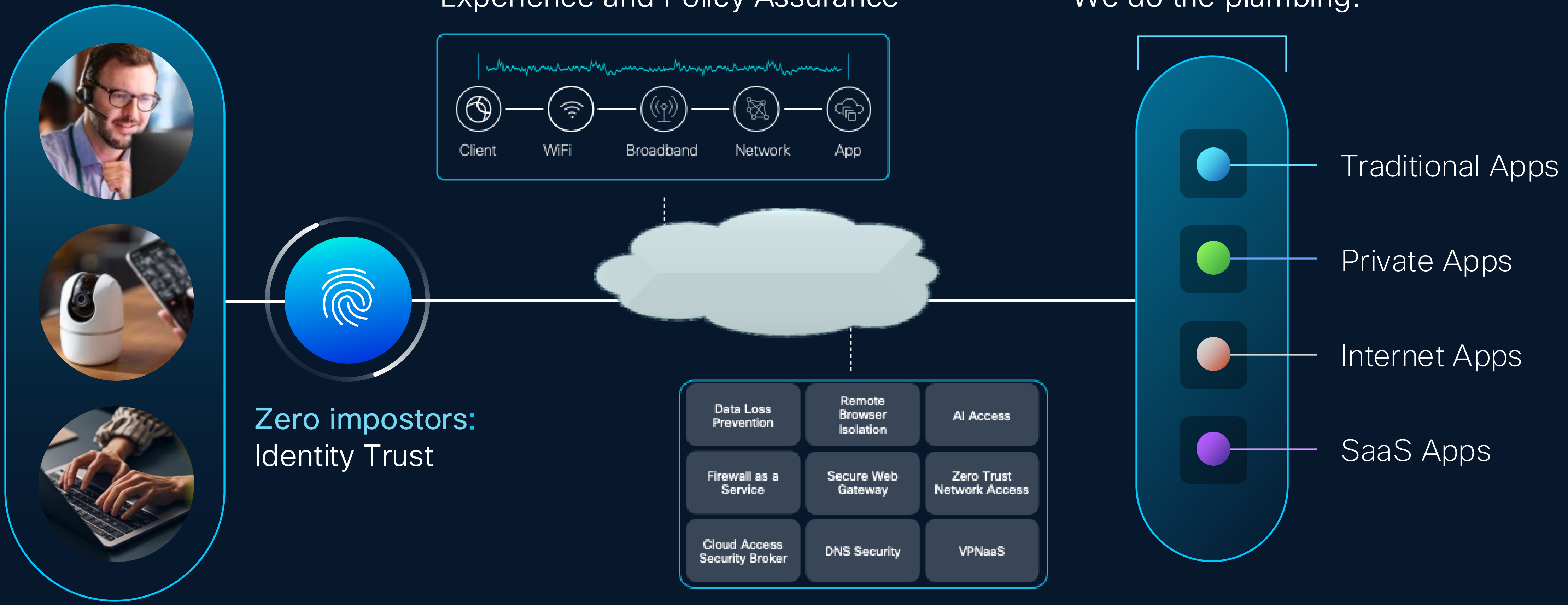
Cloud Protection

Hybrid Mesh Firewall

AI for security | Security for AI

Identity Intelligence

Cisco Universal ZTNA



Every device, person, thing, everywhere

Zero impostors:
Identity Trust

Zero downtime:
Experience and Policy Assurance

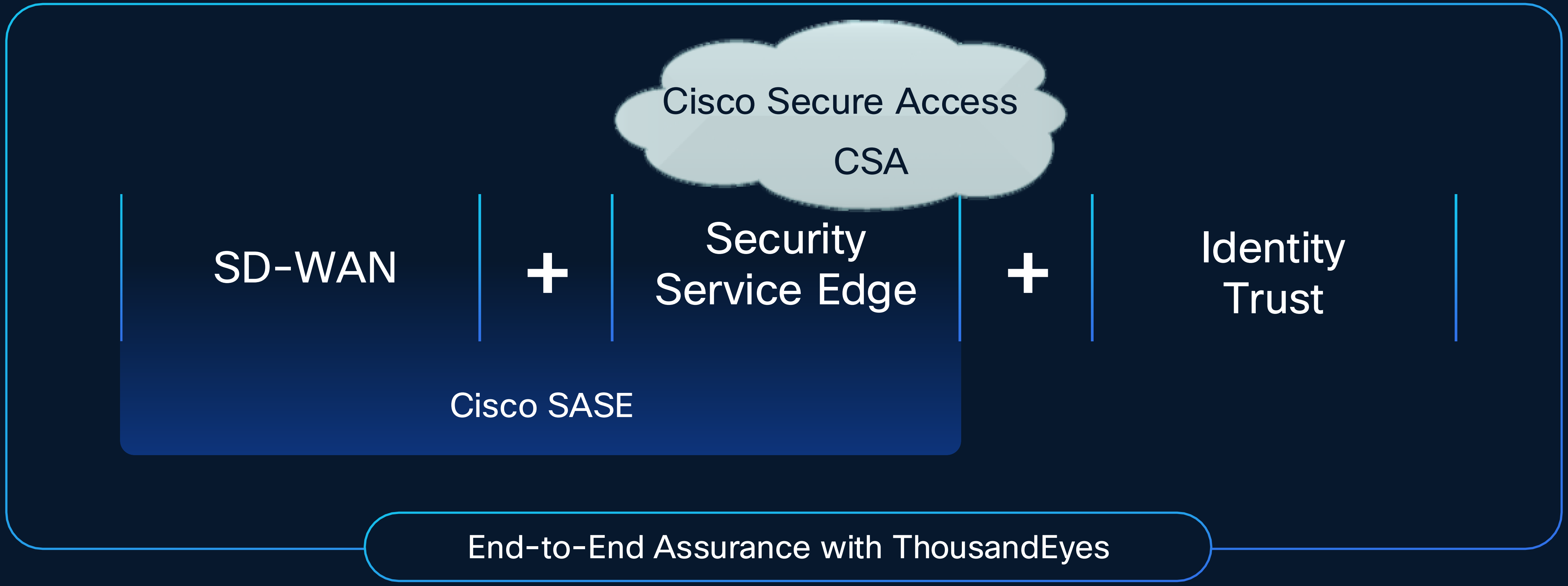
Data Loss Prevention	Remote Browser Isolation	AI Access
Firewall as a Service	Secure Web Gateway	Zero Trust Network Access
Cloud Access Security Broker	DNS Security	VPNaaS

Consistent Security:
Security Service Edge

Zero friction:
We do the plumbing.

- Traditional Apps
- Private Apps
- Internet Apps
- SaaS Apps

Cisco Universal ZTNA (Mathematics)



Cisco Secure Access

CSA

SD-WAN + Security Service Edge + Identity Trust

Cisco SASE

End-to-End Assurance with ThousandEyes

Simplified Security

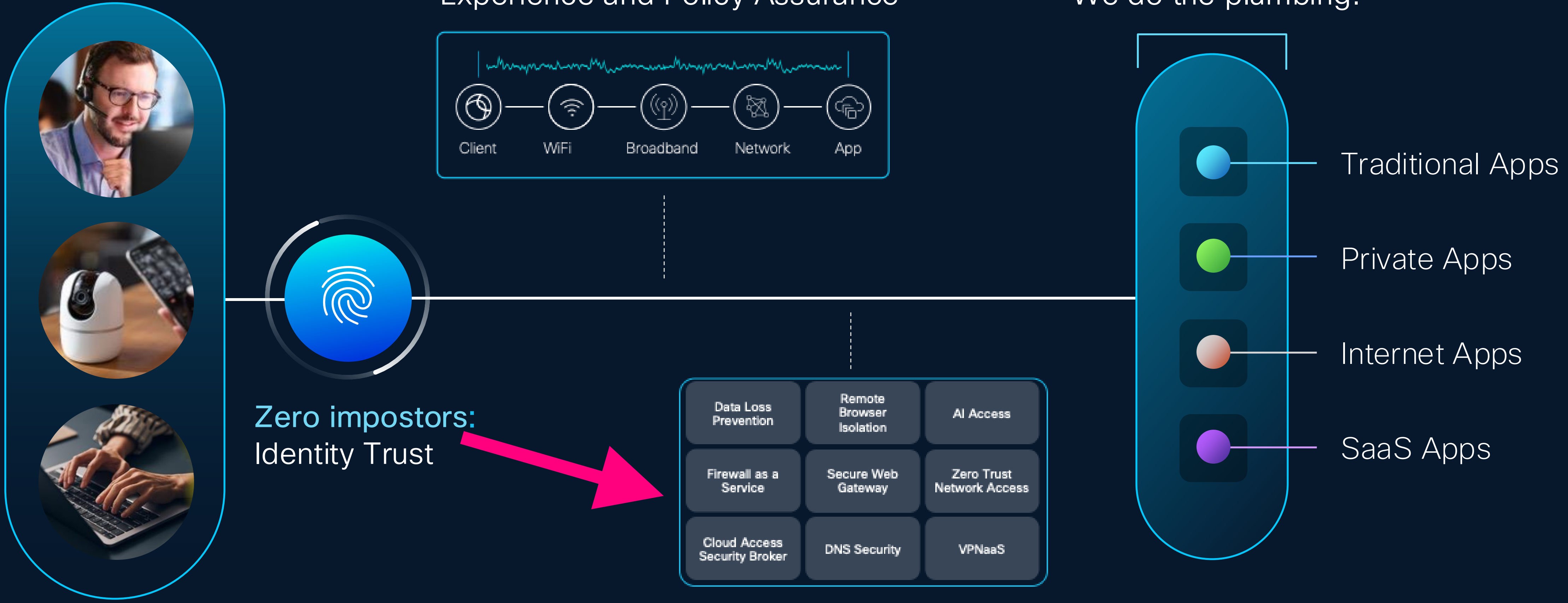
- Simple for Users
  - One client or no client
  - Transparent experience
- Simple for IT admins
  - SaaS
  - Security Cloud Control
  - Integrated with the Network

Cisco Universal ZTNA

Every device, person, thing, everywhere

Zero downtime:
Experience and Policy Assurance

Zero friction:
We do the plumbing.

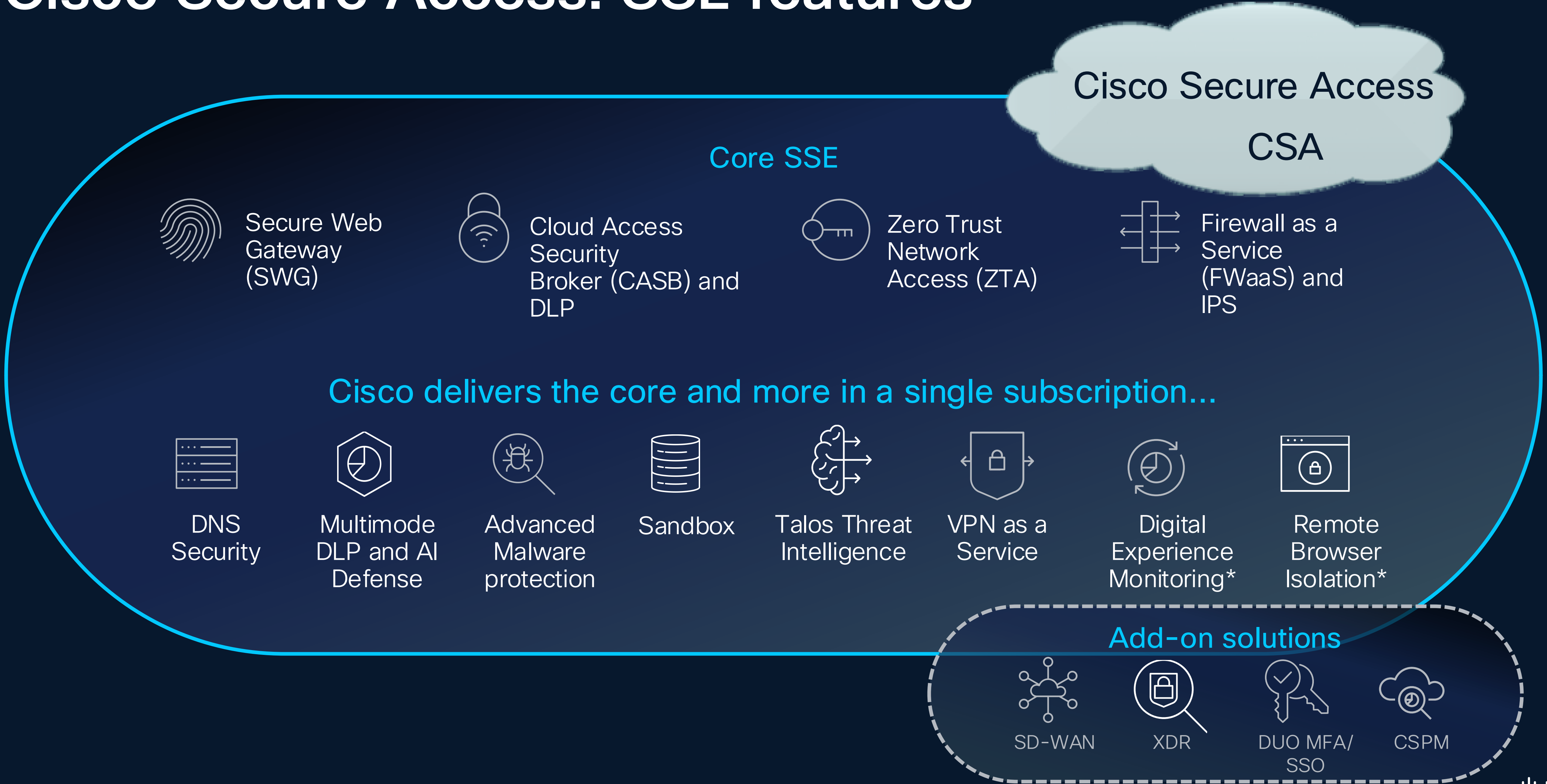


Zero impostors:
Identity Trust

Data Loss Prevention	Remote Browser Isolation	AI Access
Firewall as a Service	Secure Web Gateway	Zero Trust Network Access
Cloud Access Security Broker	DNS Security	VPNaaS

Consistent Security:
Security Service Edge

Cisco Secure Access: SSE features



Cisco Secure Access

CSA

Core SSE

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB) and DLP
- Zero Trust Network Access (ZTA)
- Firewall as a Service (FWaaS) and IPS

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

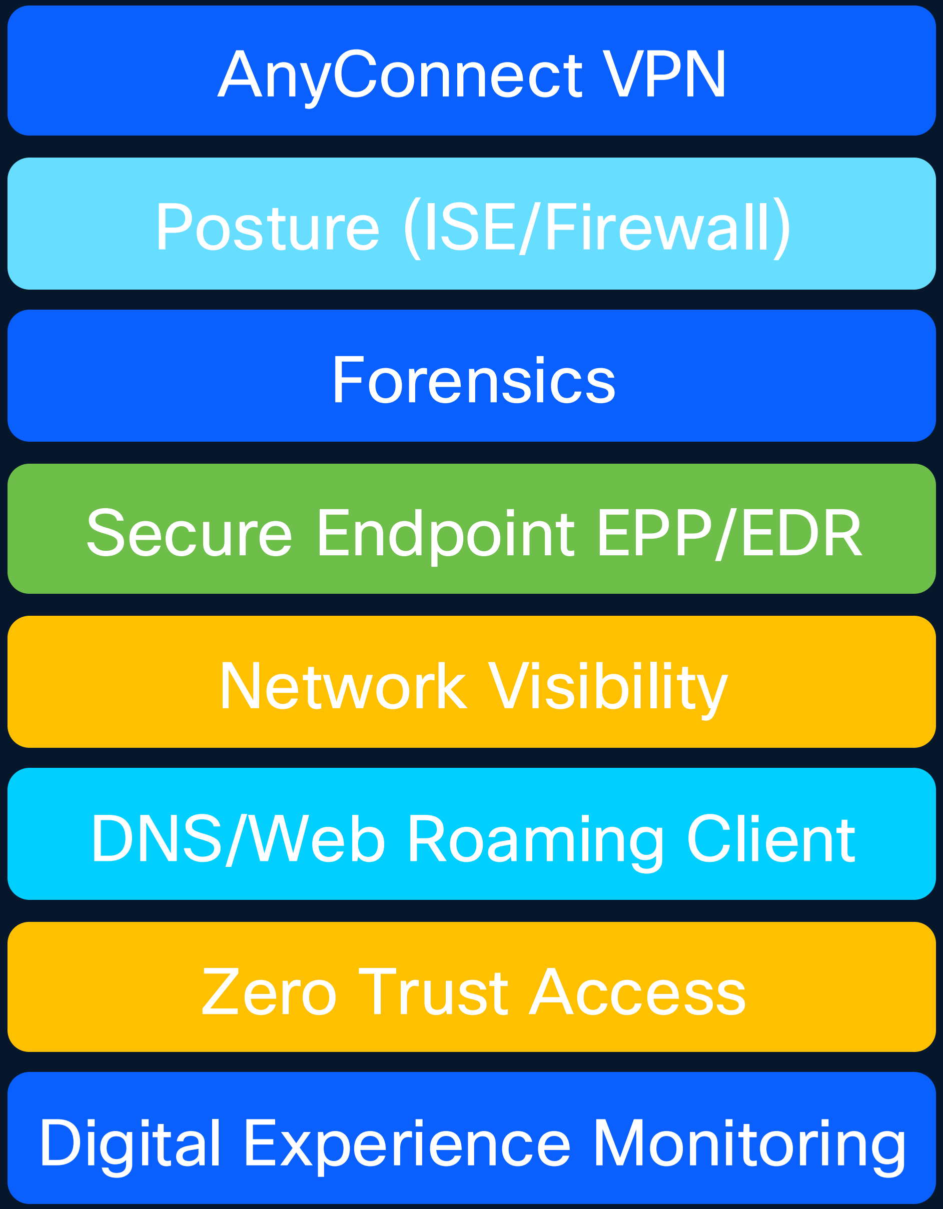
- DNS Security
- Multimode DLP and AI Defense
- Advanced Malware protection
- Sandbox
- Talos Threat Intelligence
- VPN as a Service
- Digital Experience Monitoring*
- Remote Browser Isolation*

Add-on solutions

- SD-WAN
- XDR
- DUO MFA/ SSO
- CSPM

Cisco Secure Client

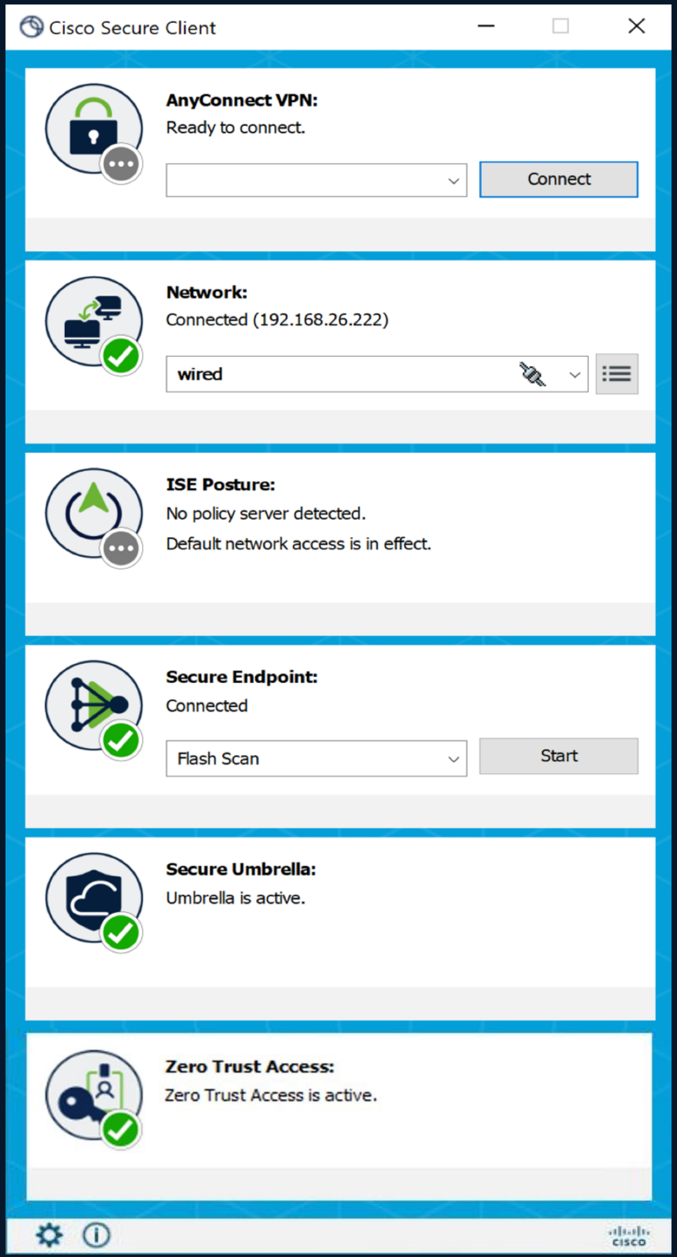
- Modular design



- AnyConnect VPN
- Posture (ISE/Firewall)
- Forensics
- Secure Endpoint EPP/EDR
- Network Visibility
- DNS/Web Roaming Client
- Zero Trust Access
- Digital Experience Monitoring

Cisco Secure Client

- Modular design
- **One GUI for the user**



AnyConnect VPN:
Ready to connect.

Network:
Connected (192.168.26.222)

wired

ISE Posture:
No policy server detected.
Default network access is in effect.

Secure Endpoint:
Connected

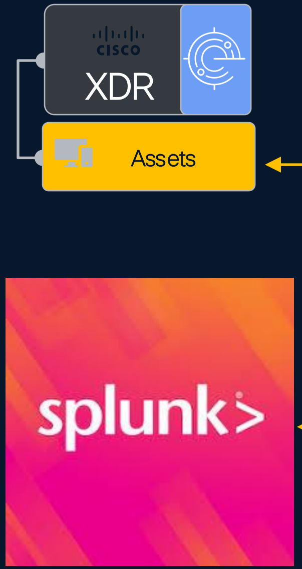
Flash Scan

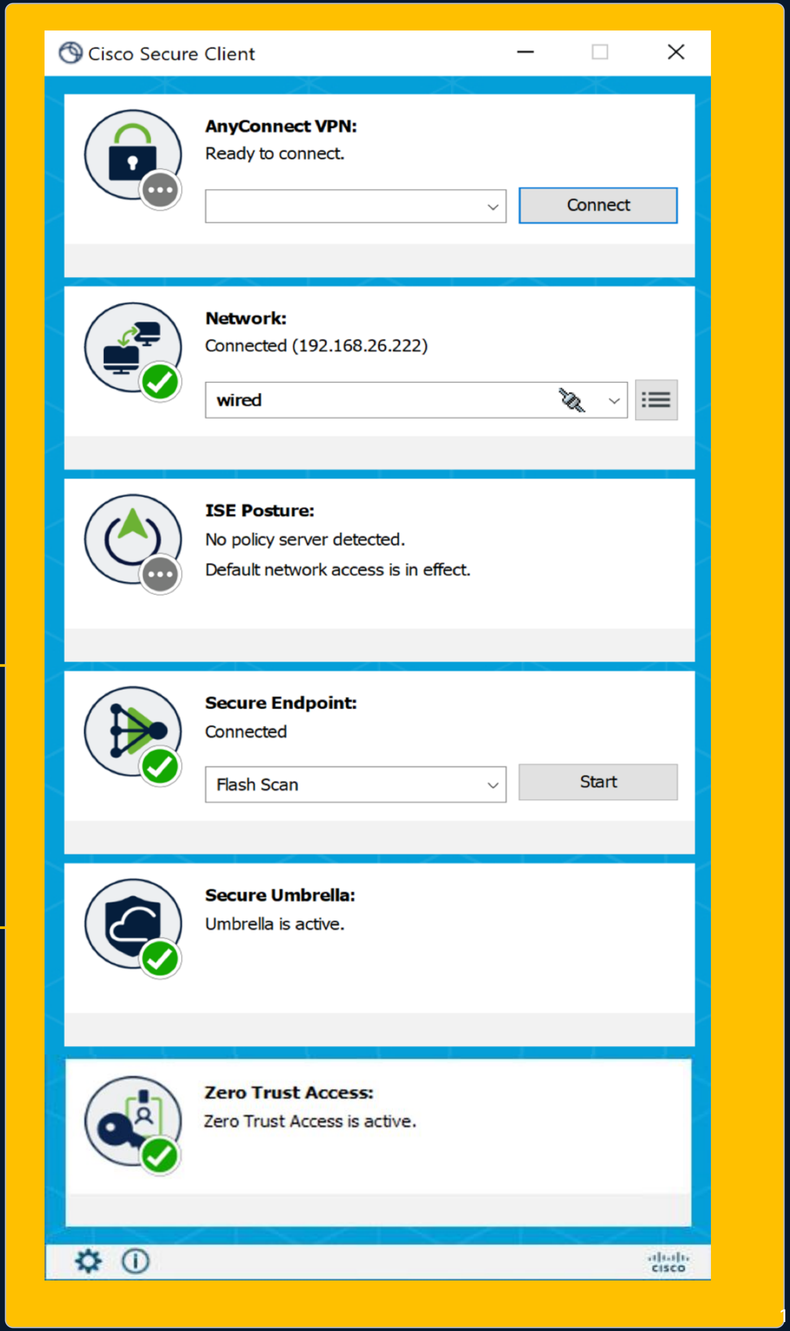
Secure Umbrella:
Umbrella is active.

Zero Trust Access:
Zero Trust Access is active.

Cisco Secure Client

- Modular design
- One GUI for the user
- **One Identity for the SOC**




Cisco Secure Client

AnyConnect VPN:
Ready to connect.

Connect

Network:
Connected (192.168.26.222)

wired

ISE Posture:
No policy server detected.
Default network access is in effect.

Secure Endpoint:
Connected

Flash Scan

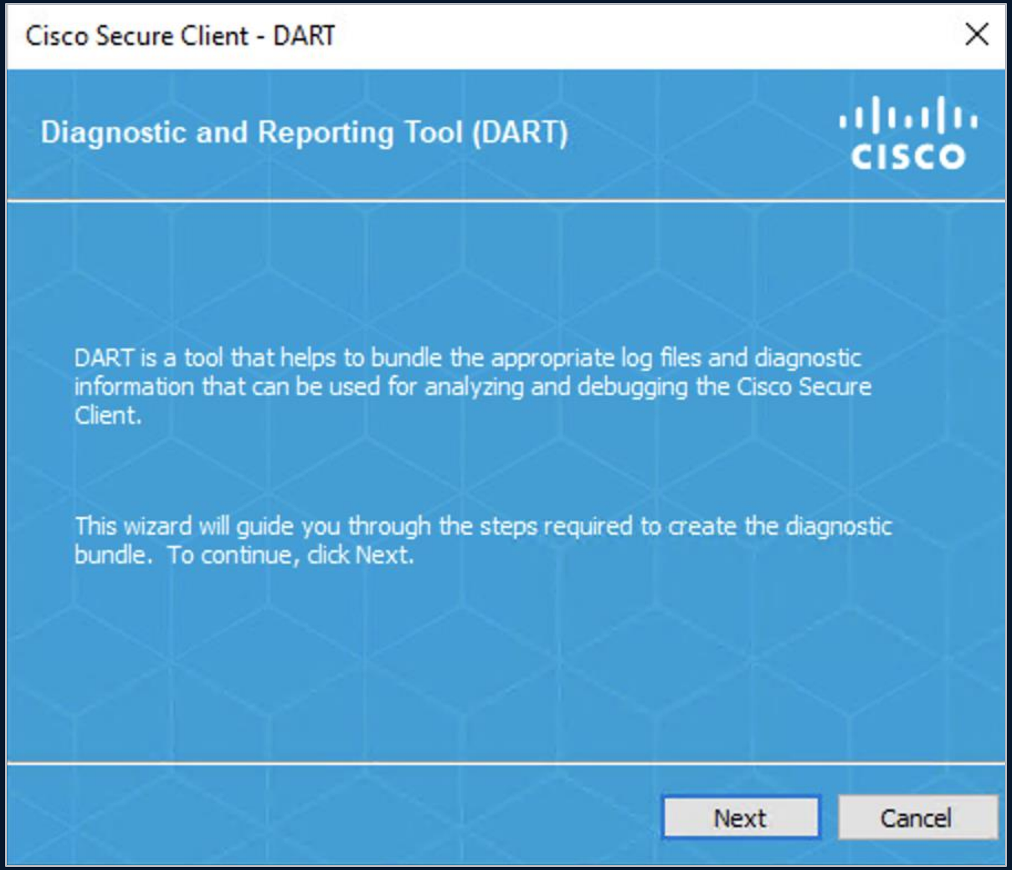
Start

Secure Umbrella:
Umbrella is active.

Zero Trust Access:
Zero Trust Access is active.

Cisco Secure Client

- Modular design
- One GUI for the user
- One Identity for the SOC
- **One troubleshoot tool for admins**



Cisco Secure Client - DART
Diagnostic and Reporting Tool (DART)
Next
Cancel

DART is a tool that helps to bundle the appropriate log files and diagnostic information that can be used for analyzing and debugging the Cisco Secure Client.

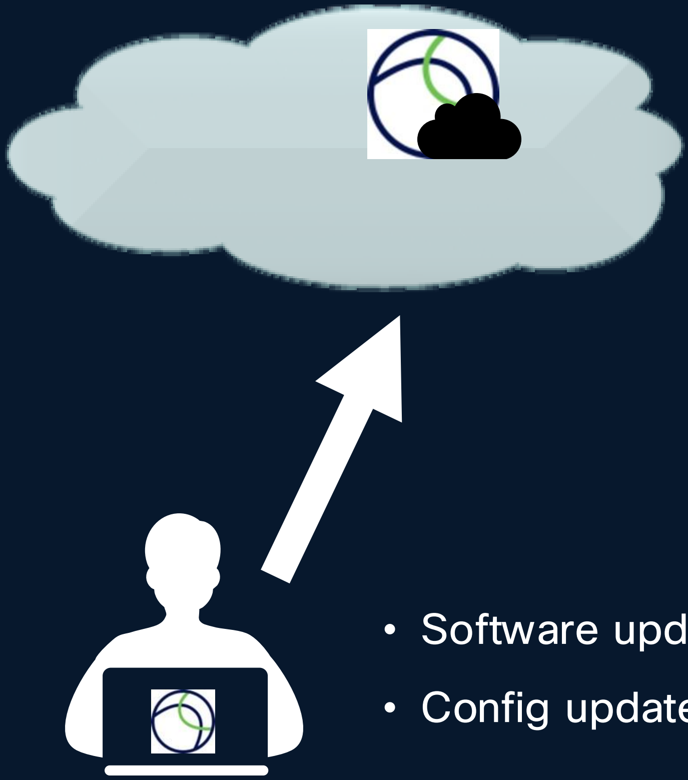
This wizard will guide you through the steps required to create the diagnostic bundle. To continue, click Next.

Cisco Secure Client

- Modular design
- One GUI for the user
- One Identity for the SOC
- One troubleshoot for admins
- **One install file for admins**

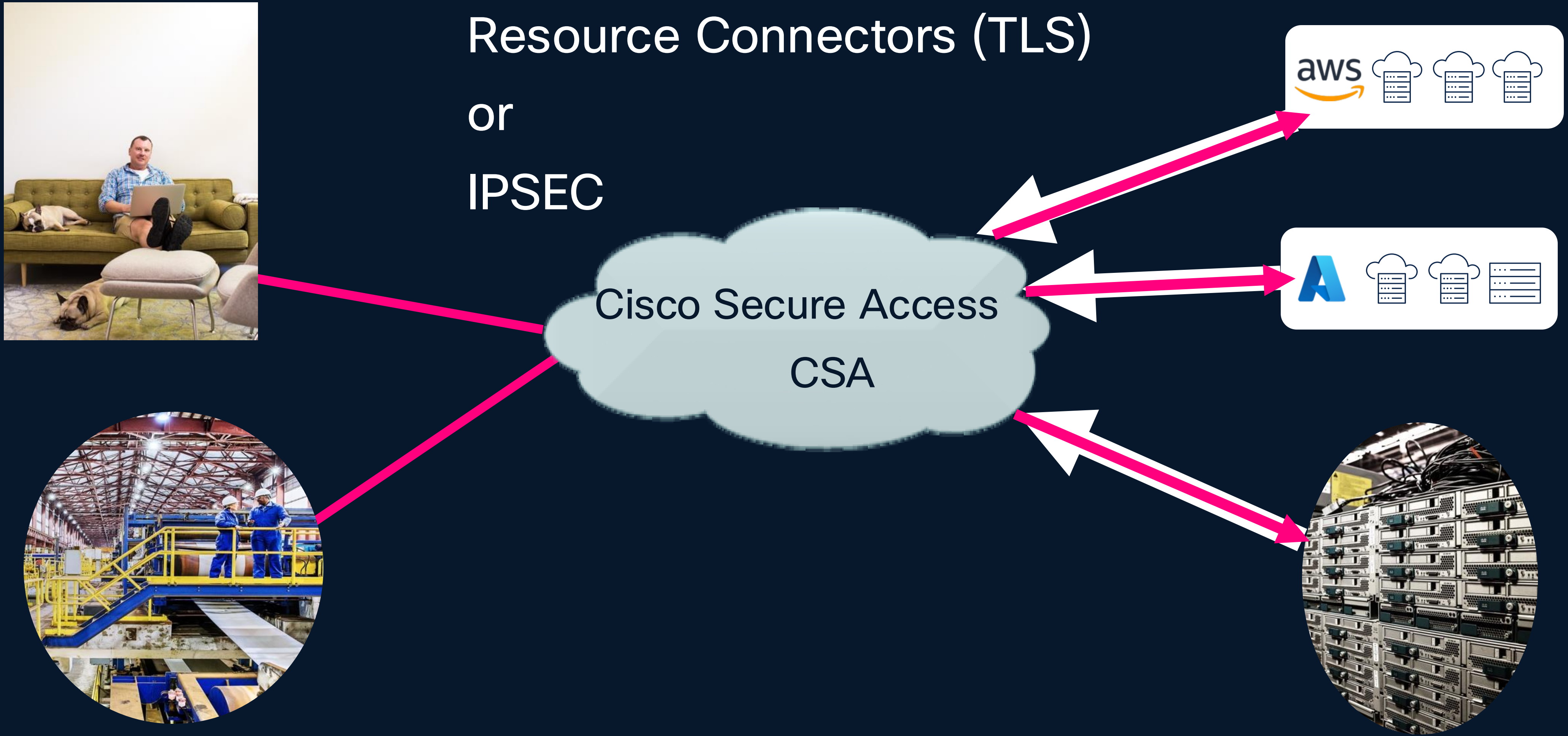
Cisco Secure Client

- Modular design
- One GUI for the user
- One Identity for the SOC
- One troubleshoot for admins
- One install file for admins
- **Optionally Cloud-Managed (SaaS)**



- Software updates
- Config updates

Secure Private Access: Connecting our Apps



Resource Connectors (TLS)

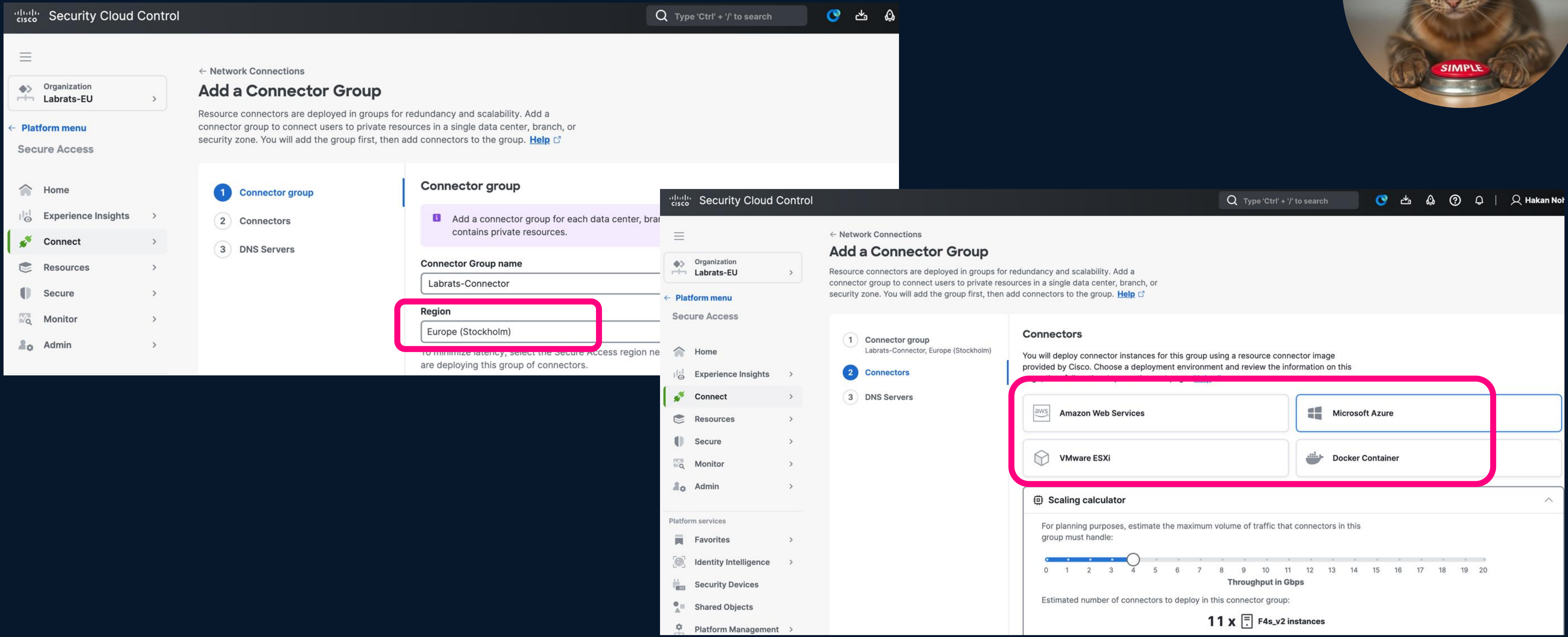
or

IPSEC

Cisco Secure Access

CSA

Resource Connectors



Security Cloud Control

Type 'Ctrl' + '/' to search

Organization
Labrats-EU

← Platform menu

Secure Access

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

← Network Connections

Add a Connector Group

Resource connectors are deployed in groups for redundancy and scalability. Add a connector group to connect users to private resources in a single data center, branch, or security zone. You will add the group first, then add connectors to the group. Help

1. Connector group
2. Connectors
3. DNS Servers

Connector group

Add a connector group for each data center, bra contains private resources.

Connector Group name: Labrats-Connector

Region: Europe (Stockholm)

To minimize latency, select the Secure Access region ne are deploying this group of connectors.

Security Cloud Control

Type 'Ctrl' + '/' to search

Hakan Nol

Organization
Labrats-EU

← Platform menu

Secure Access

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

Platform services

- Favorites
- Identity Intelligence
- Security Devices
- Shared Objects
- Platform Management

← Network Connections

Add a Connector Group

Resource connectors are deployed in groups for redundancy and scalability. Add a connector group to connect users to private resources in a single data center, branch, or security zone. You will add the group first, then add connectors to the group. Help

1. Connector group
   Labrats-Connector, Europe (Stockholm)
2. Connectors
3. DNS Servers

Connectors

You will deploy connector instances for this group using a resource connector image provided by Cisco. Choose a deployment environment and review the information on this

- Amazon Web Services
- Microsoft Azure
- VMware ESXi
- Docker Container

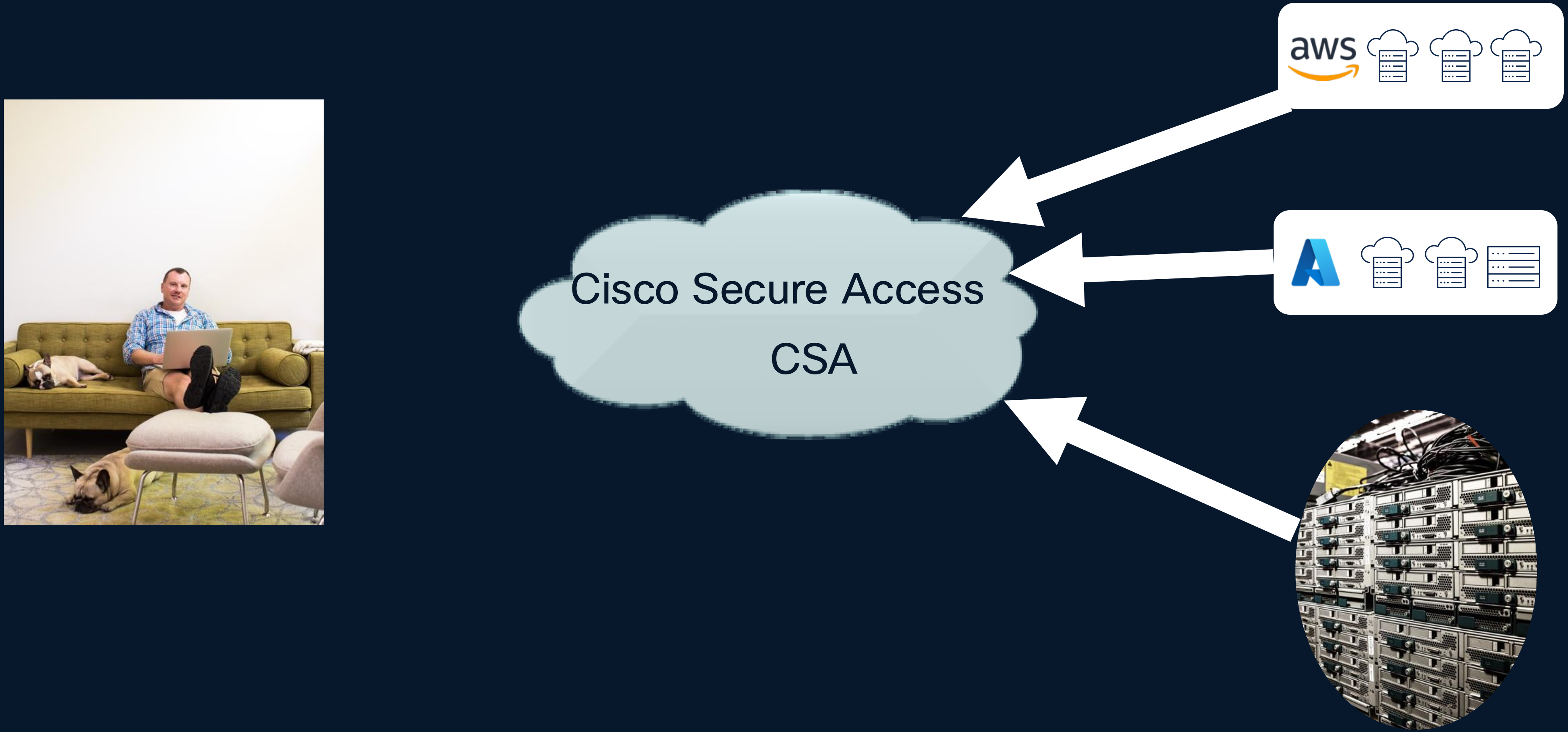
Scaling calculator

For planning purposes, estimate the maximum volume of traffic that connectors in this group must handle:

Estimated number of connectors to deploy in this connector group:

11 x F4s_v2 instances

Connecting our Users: Zero Trust Access

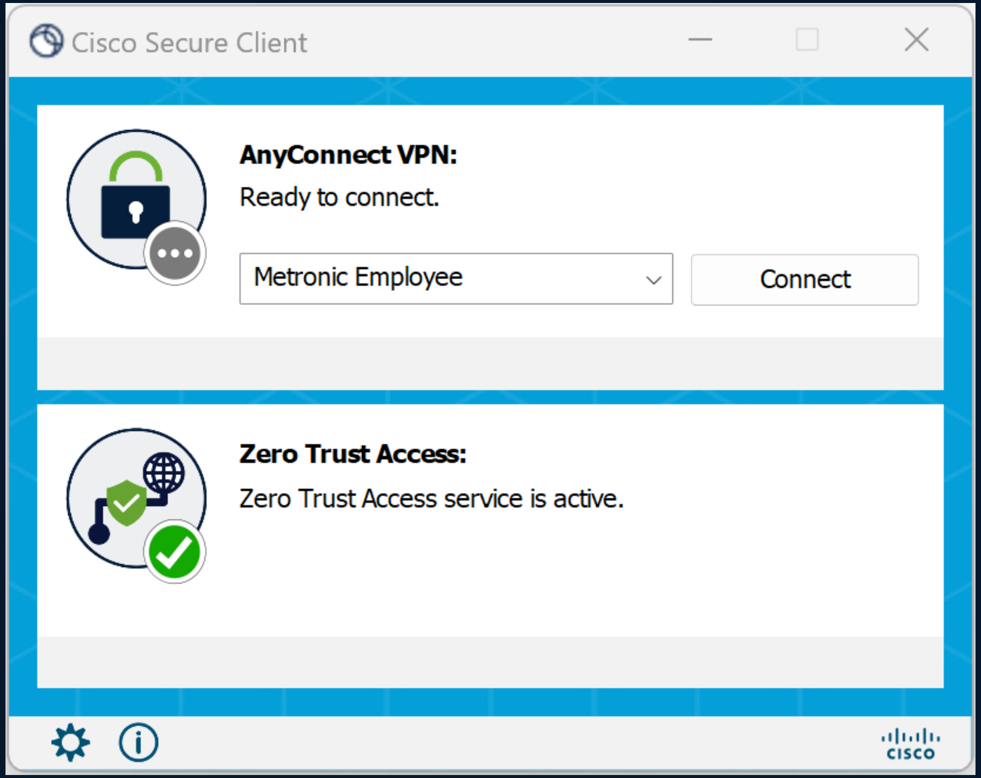


Cisco Secure Access

CSA

Secure Private Access : Zero Trust Access

- Transparent user experience
- Next-generation protocols (QUIC/MASQUE)
- Support for most TCP/UDP apps

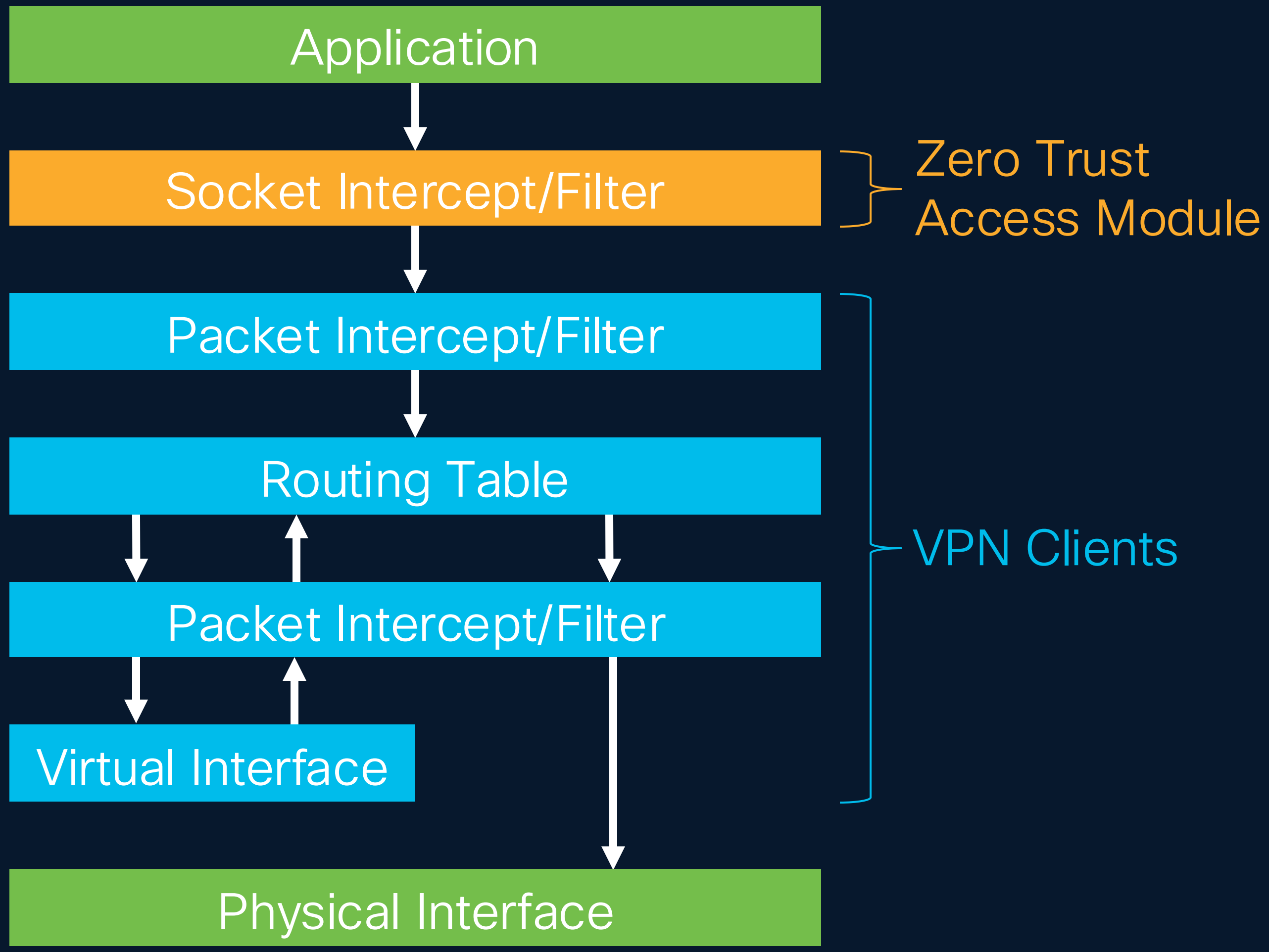


AnyConnect VPN:
Ready to connect.

Metronic Employee

Zero Trust Access:
Zero Trust Access service is active.

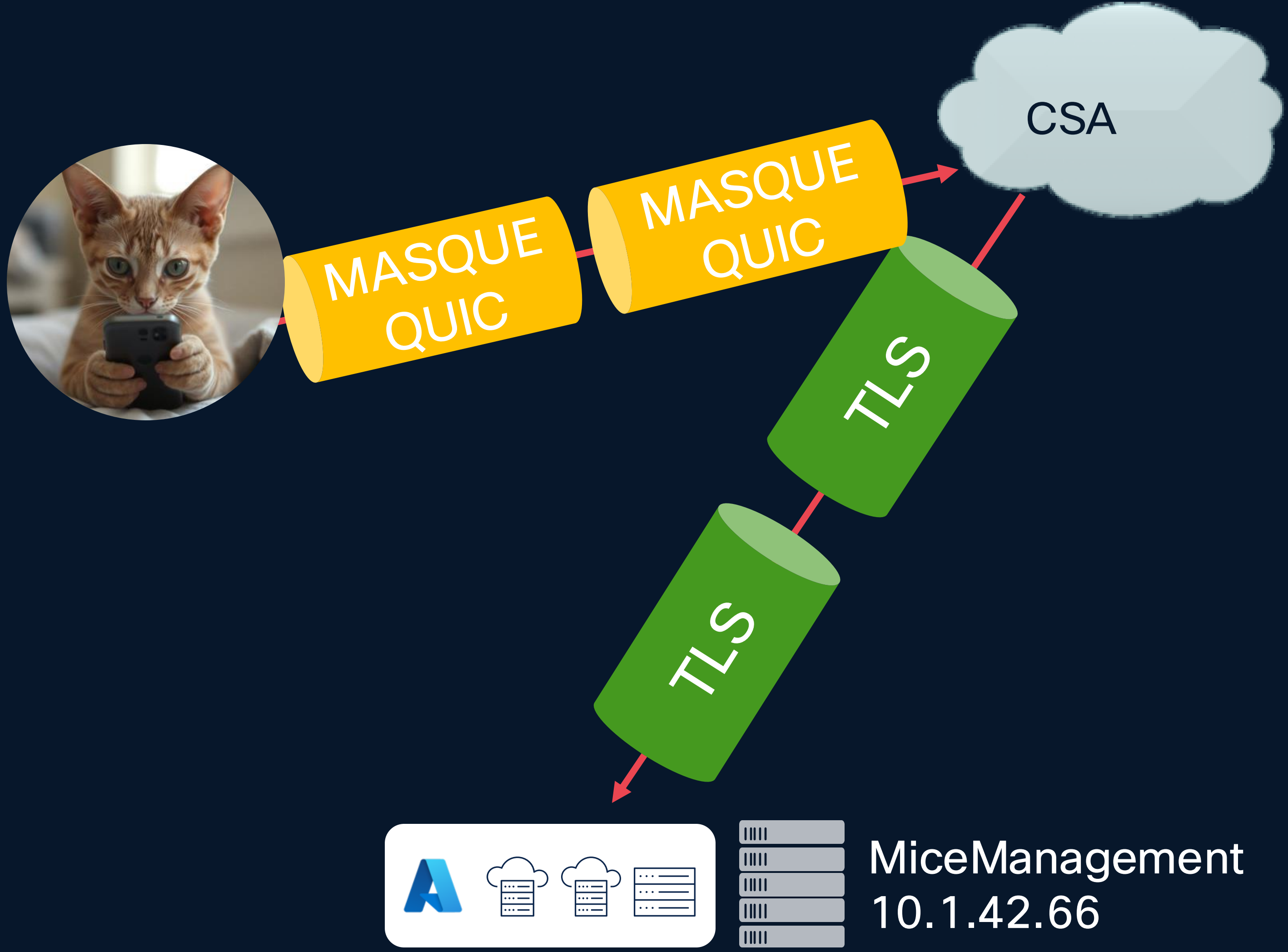
Secure Client ZTA Module: Socket Intercept

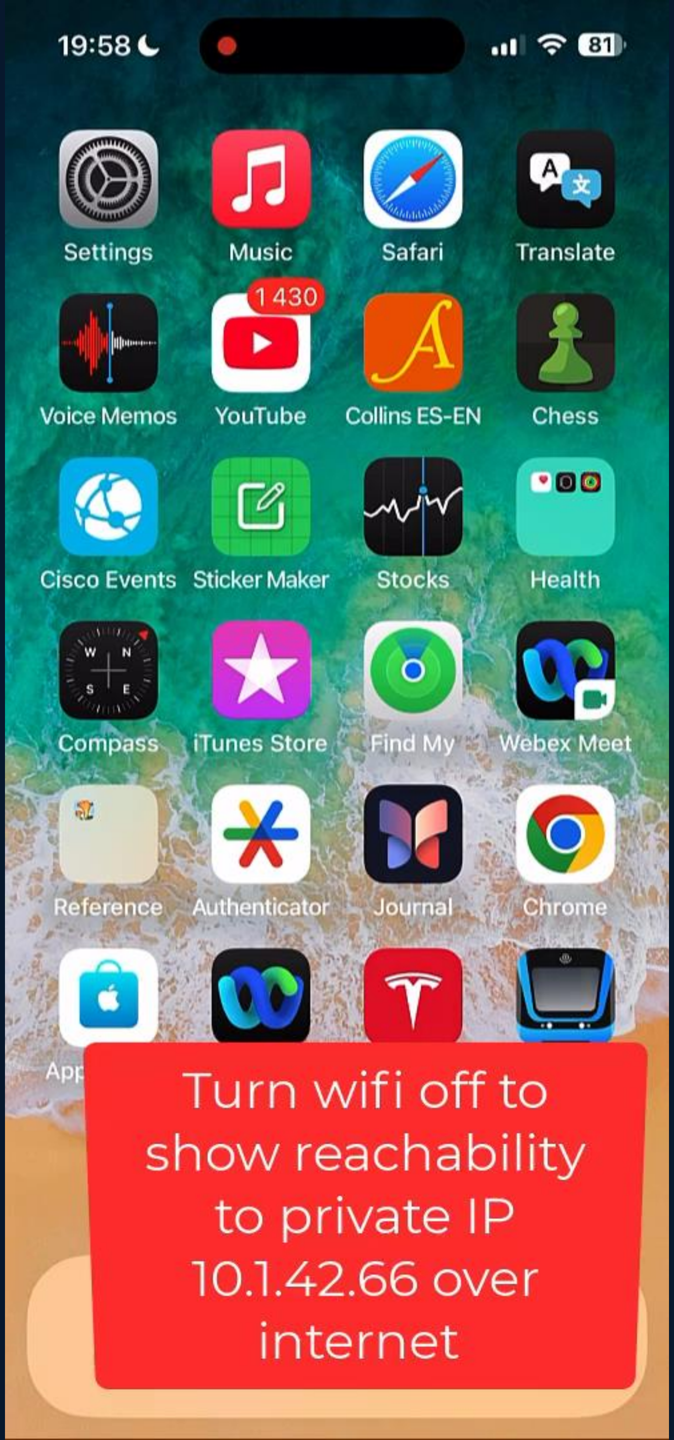


Why Socket Intercept?

- 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

Warning! Maybe the Lamest Demo Ever!





Turn wifi off to show reachability to private IP 10.1.42.66 over internet

Zero Trust Access with QUIC!

- Quick UDP Internet Connections
- RFC 8999...9002
- Default protocol for all major browsers
- 0 RTT connections, multiplexing
- Native support in Apple IOS, Android

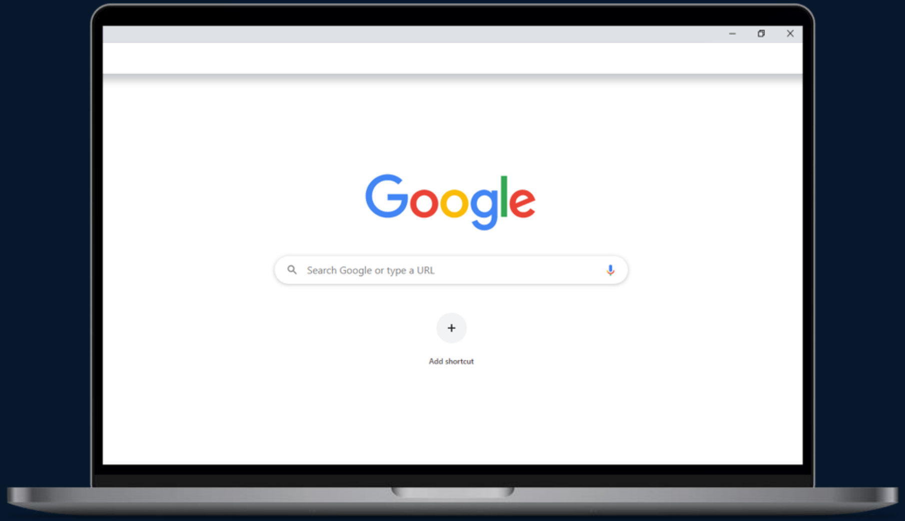
Some old apps do not work with Zero Trust Access

- Client-to-client traffic (e.g. peer-to-peer VoIP)
- Server-to-client traffic (e.g. remote desktop, remote assistance)
- Applications that require a unique client IP (e.g. SMBv1)
- Applications that require SRV DNS records (e.g. Active Directory, Kerberos, SCCM)
- Applications that require the server to send a data payload (after the TCP 3-way handshake) before the client will send a data payload (e.g. MySQL Studio)
- Applications that perform an ICMP connectivity check prior to connecting via TCP or UDP

We can use AnyConnect VPN!

Private Access for Unmanaged Devices

BYOD via enterprise managed Google Chrome
Advanced protocol support for Apple, Samsung

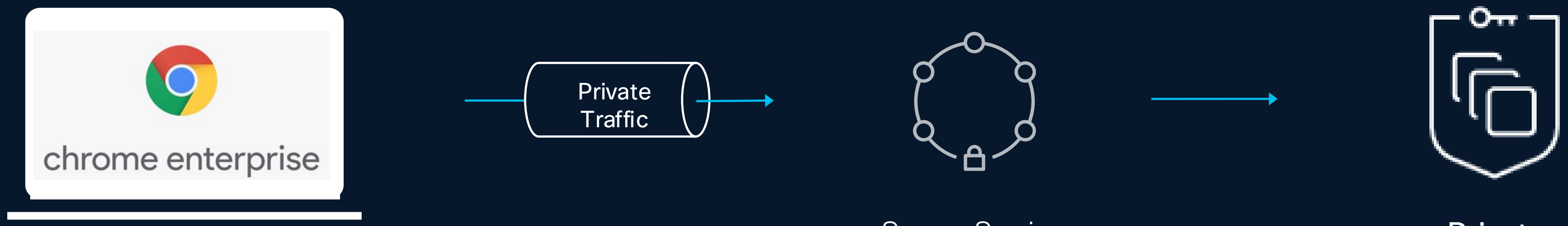


Chrome Enterprise Browser

Native OS Integration

Secure Access with Enterprise Browser

Zero Trust Access to Private Apps and Internet Apps



Enterprise Browser

Unmanaged and Managed Endpoints

Cisco Secure Access

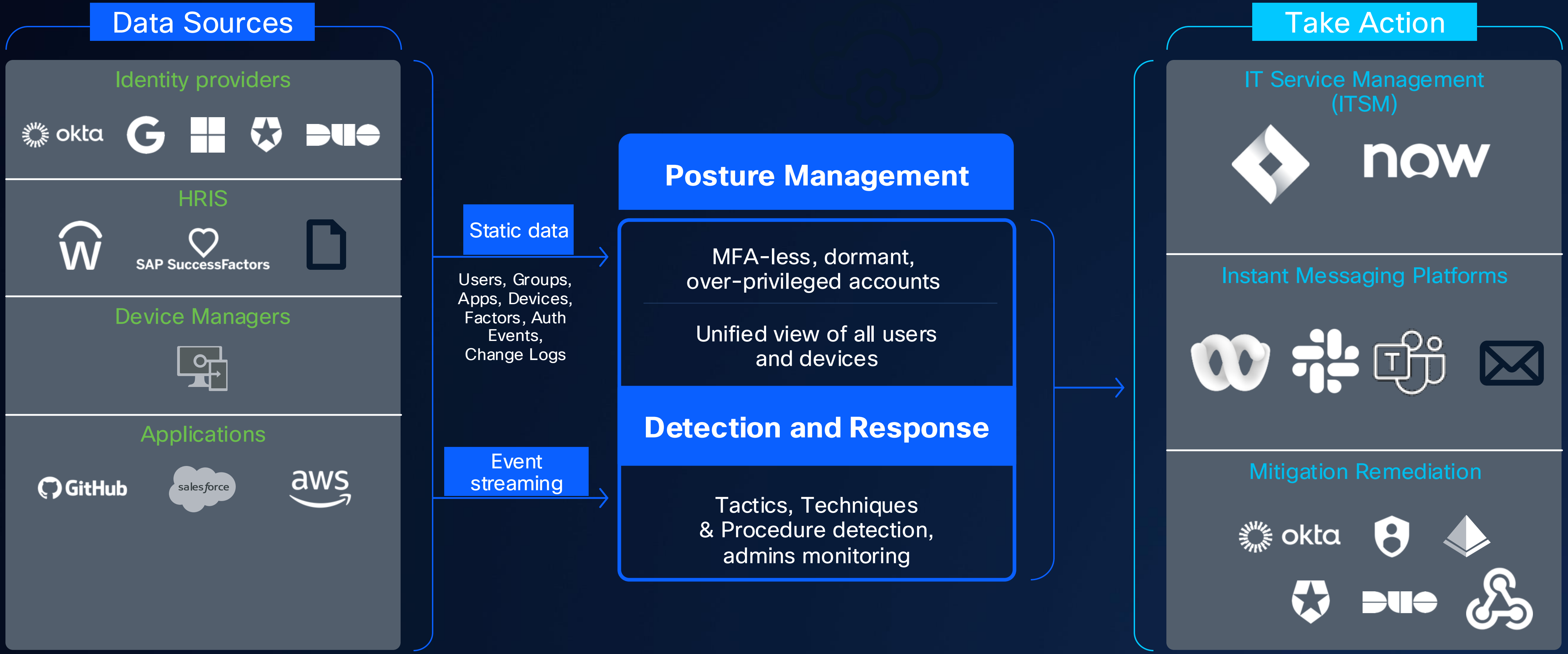
Secure Service Edge (SSE)

Private Applications

- 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

Cisco Identity Intelligence



Data Sources

Identity providers

HRIS

SAP SuccessFactors

Device Managers

Applications

GitHub

salesforce

aws

Static data

Users, Groups, Apps, Devices, Factors, Auth Events, Change Logs

Event streaming

Posture Management

MFA-less, dormant, over-privileged accounts

Unified view of all users and devices

Detection and Response

Tactics, Techniques & Procedure detection, admins monitoring

Take Action

IT Service Management (ITSM)

now

Instant Messaging Platforms

Mitigation Remediation

User Risk Level: Can be used in Policies and Investigations!

Proactive

Dormant Accounts

Never Logged In Accounts

Accounts without MFA

Users using weak MFA

Contractor account access

Too many administrators

Reactive

Service accounts with interactive logins

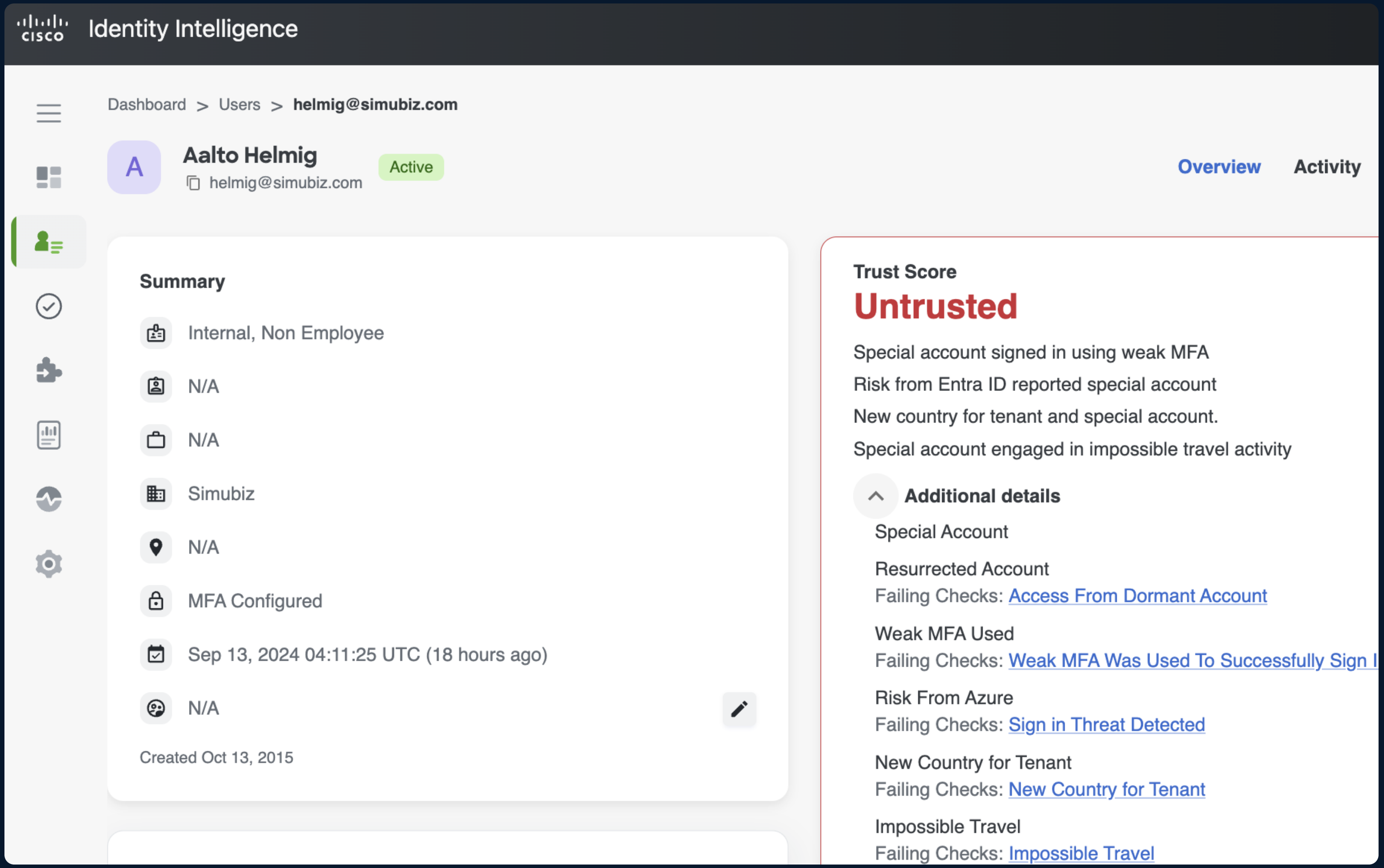
MFA manually activated and utilized

Access from denied countries

Account under heavy attack

Activity log of a user

User Risk Level: Can be used in Policies and Investigations!



Aalto Helmig Active
helmig@simubiz.com

Summary

Internal, Non Employee
N/A
N/A
Simubiz
N/A
MFA Configured
Sep 13, 2024 04:11:25 UTC (18 hours ago)
N/A

Created Oct 13, 2015

Trust Score
Untrusted

Special account signed in using weak MFA
Risk from Entra ID reported special account
New country for tenant and special account.
Special account engaged in impossible travel activity

Additional details

Special Account

Resurrected Account
Failing Checks: Access From Dormant Account

Weak MFA Used
Failing Checks: Weak MFA Was Used To Successfully Sign I

Risk From Azure
Failing Checks: Sign in Threat Detected

New Country for Tenant
Failing Checks: New Country for Tenant

Impossible Travel
Failing Checks: Impossible Travel

User Trust Score

Identity Intelligence provides a dynamic user trust score based on user behaviors, actions, and posture to Secure Access for continuous zero trust enforcement.

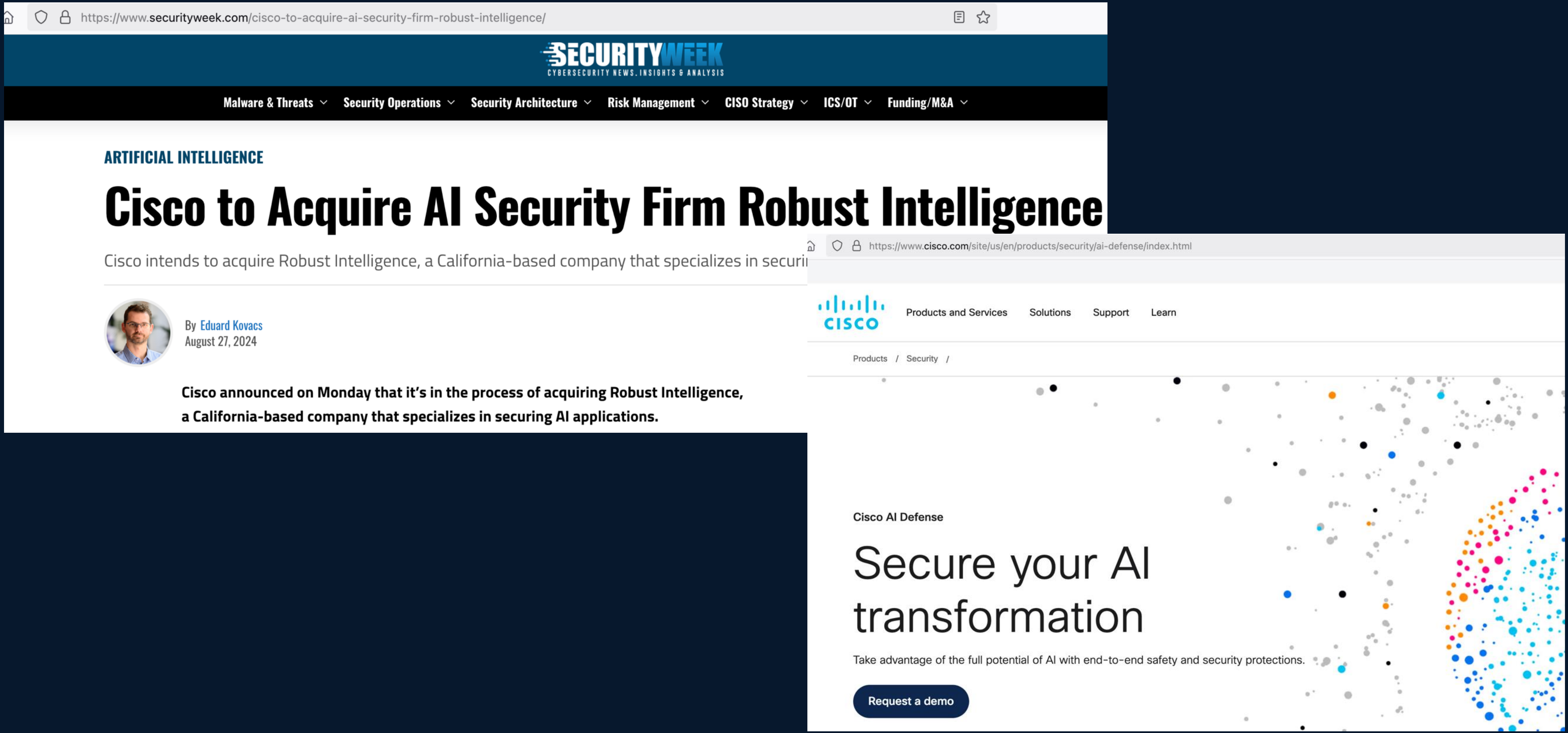
Easy Workflows

After assessment, take response action from the console.

Key Scores

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

Cisco Acquires Robust Intelligence



https://www.securityweek.com/cisco-to-acquire-ai-security-firm-robust-intelligence/

ARTIFICIAL INTELLIGENCE

Cisco to Acquire AI Security Firm Robust Intelligence

Cisco intends to acquire Robust Intelligence, a California-based company that specializes in securi

By Eduard Kovacs
August 27, 2024

Cisco announced on Monday that it's in the process of acquiring Robust Intelligence, a California-based company that specializes in securing AI applications.

https://www.cisco.com/site/us/en/products/security/ai-defense/index.html

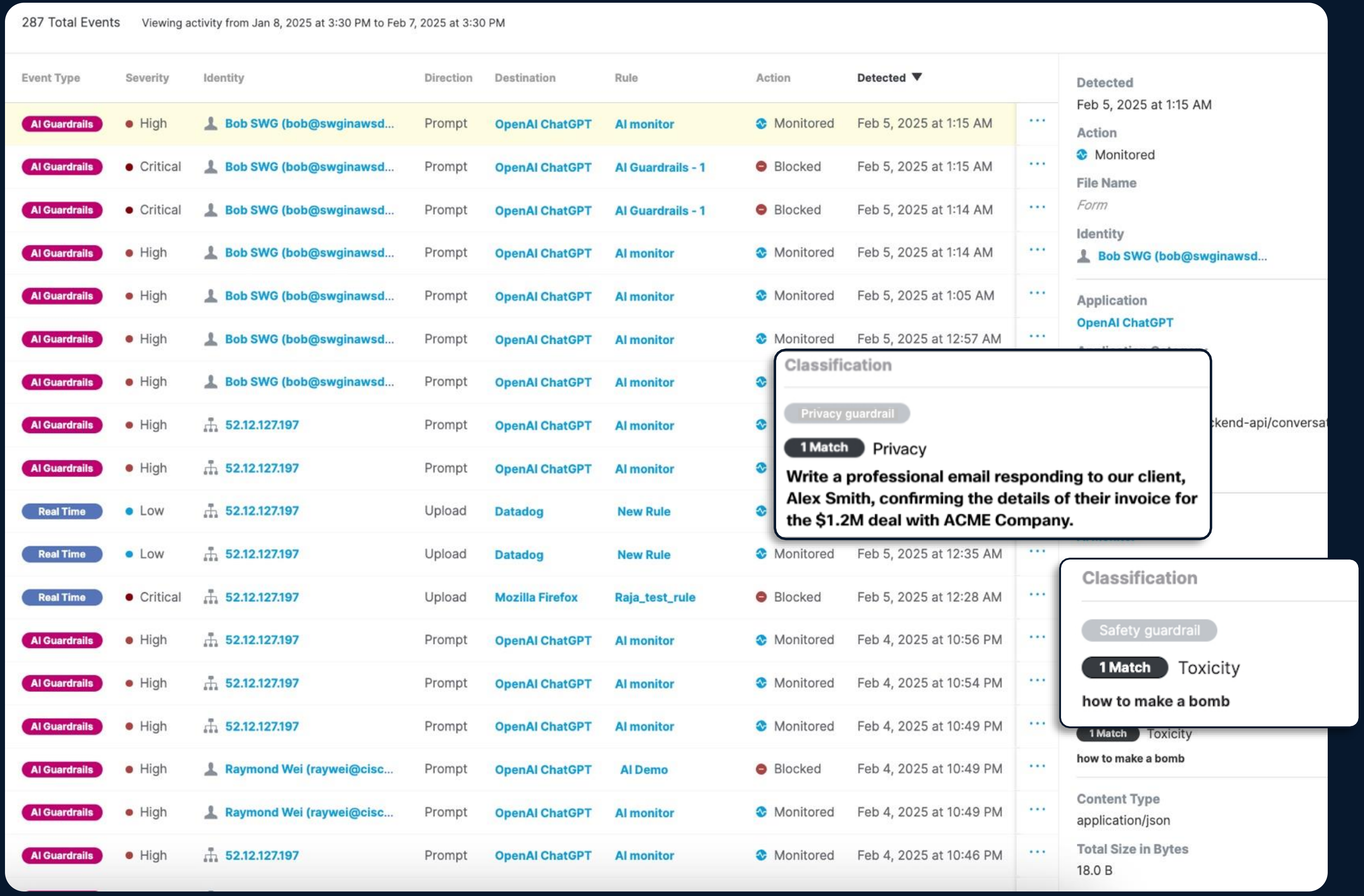
Cisco AI Defense

Secure your AI transformation

Take advantage of the full potential of AI with end-to-end safety and security protections.

Protect Our Users

- Done by the Network!
- Transparent insertion with Cisco SSE (Secure Access)
- Uses AI, not hard coded signatures



287 Total Events Viewing activity from Jan 8, 2025 at 3:30 PM to Feb 7, 2025 at 3:30 PM

Event Type	Severity	Identity	Direction	Destination	Rule	Action	Detected ▼
AI Guardrails	● High	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:15 AM
AI Guardrails	● Critical	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:15 AM
AI Guardrails	● Critical	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:14 AM
AI Guardrails	● High	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:14 AM
AI Guardrails	● High	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:05 AM
AI Guardrails	● High	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:57 AM
AI Guardrails	● High	Bob SWG (bob@swginawsd...	Prompt	OpenAI ChatGPT	AI monitor		
AI Guardrails	● High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor		
AI Guardrails	● High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor		
Real Time	● Low	52.12.127.197	Upload	Datadog	New Rule		
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 Guardrails	● High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:56 PM
AI Guardrails	● High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:54 PM
AI Guardrails	● High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:49 PM
AI Guardrails	● High	Raymond Wei (raywei@cisc...	Prompt	OpenAI ChatGPT	AI Demo	Blocked	Feb 4, 2025 at 10:49 PM
AI Guardrails	● High	Raymond Wei (raywei@cisc...	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:49 PM
AI Guardrails	● High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 10:46 PM

Detected
Feb 5, 2025 at 1:15 AM

Action
Monitored

File Name
Form

Identity
Bob SWG (bob@swginawsd...

Application
OpenAI ChatGPT

ckend-api/conversat

1 Match Toxicity
how to make a bomb

Content Type
application/json

Total Size in Bytes
18.0 B

Classification

Privacy guardrail

1 Match 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.

Classification

Safety guardrail

1 Match Toxicity

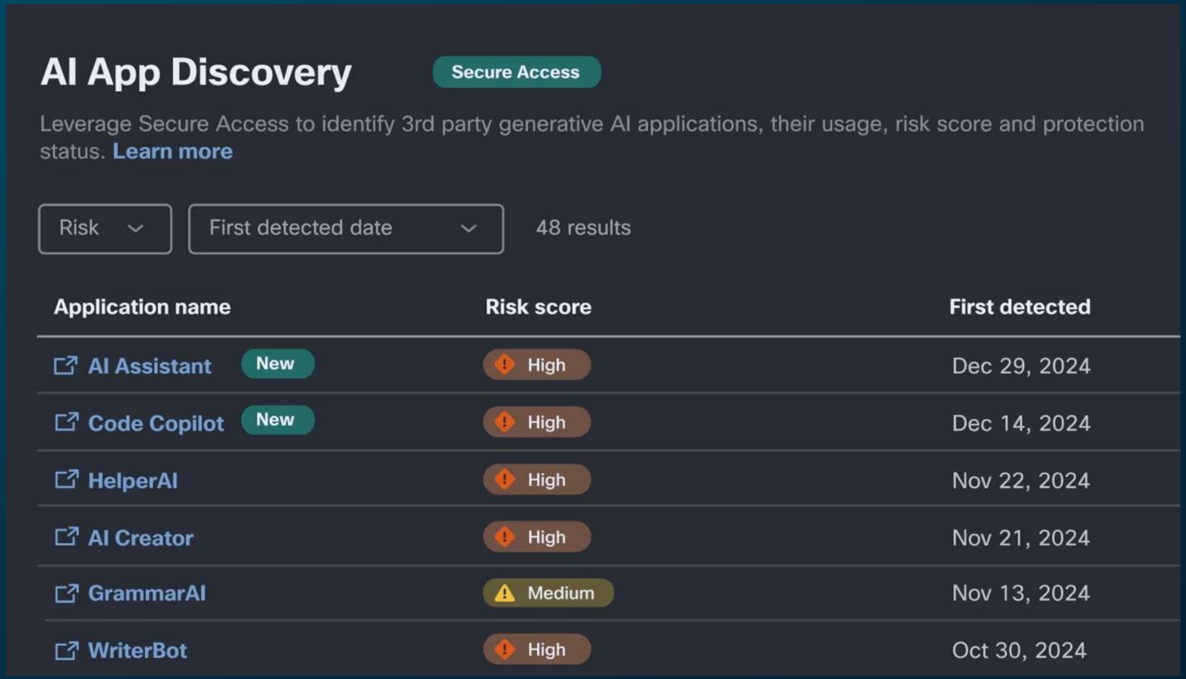
how to make a bomb

See it all.

Discover GenAI app usage with AI Access

Superior visibility & control

- Discover Shadow AI
- Define acceptable use
- 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

48 results

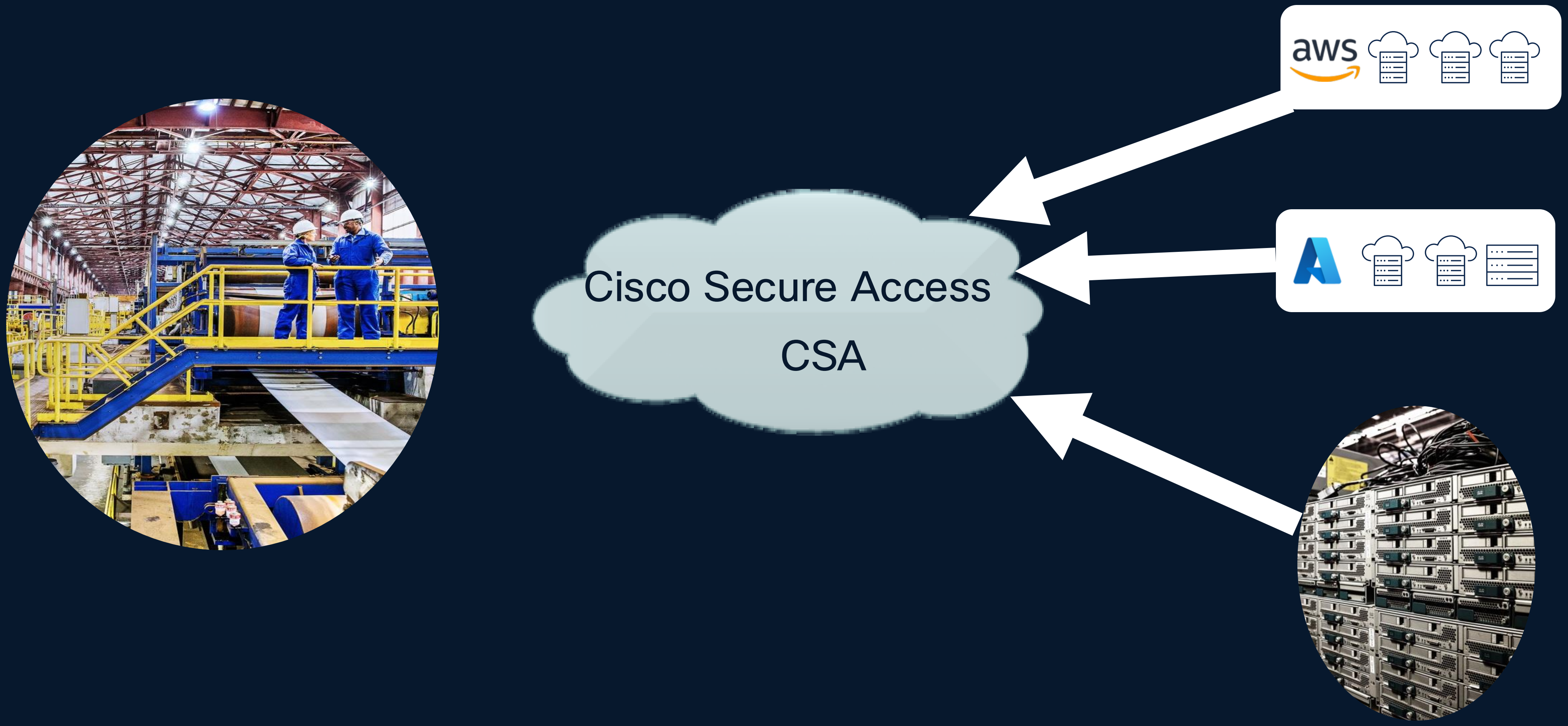
Application name	Risk score	First detected
AI Assistant New	High	Dec 29, 2024
Code Copilot New	High	Dec 14, 2024
HelperAI	High	Nov 22, 2024
AI Creator	High	Nov 21, 2024
GrammarAI	⚠ Medium	Nov 13, 2024
WriterBot	High	Oct 30, 2024

1200+
AI Apps Protected

100%
Guardrails for top AI Apps

1
Unified Security Framework

Connecting our Networks: Zero Trust Access



Cisco Secure Access

CSA

Identity Services Engine (ISE)

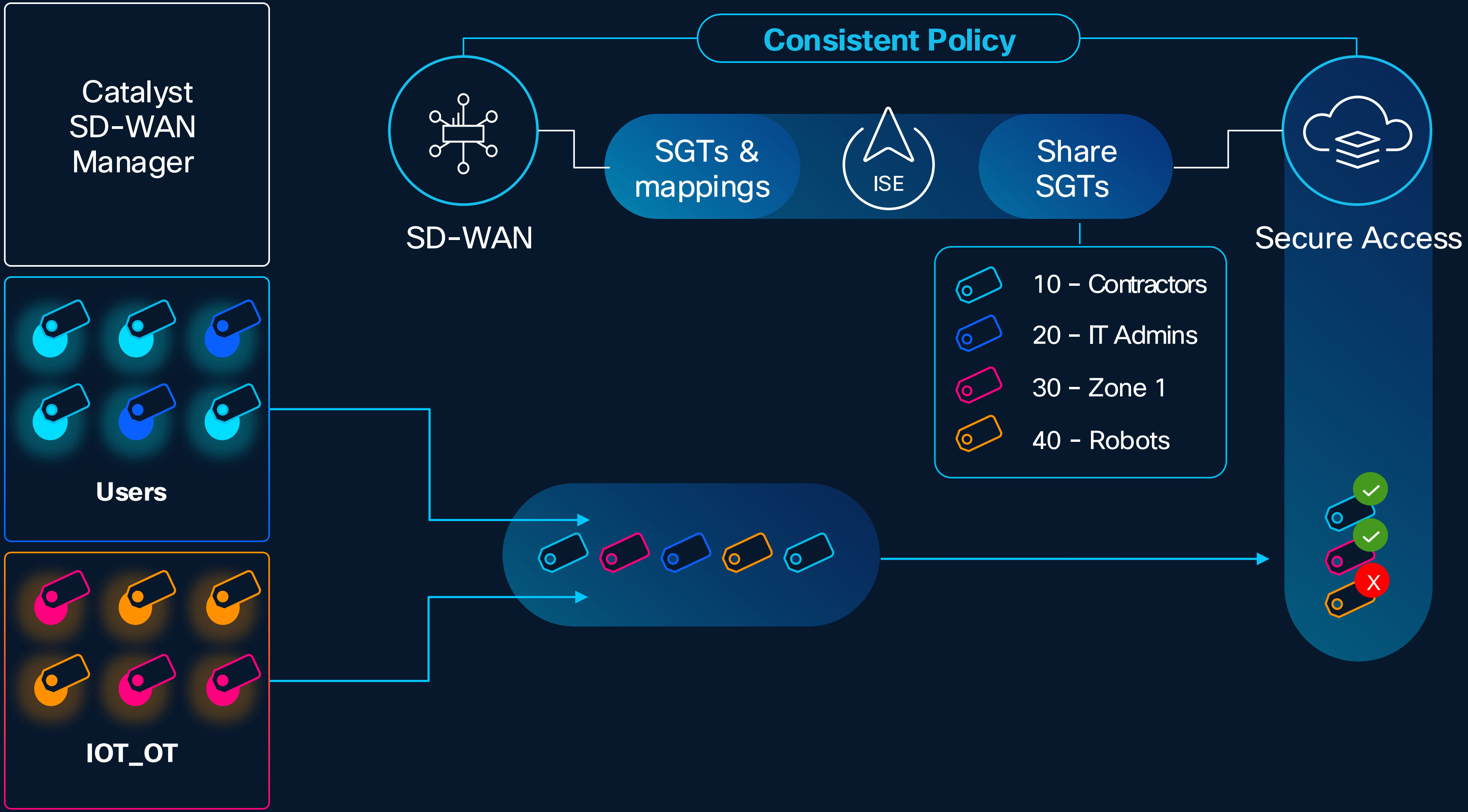
Leverage SGTs for granular access control

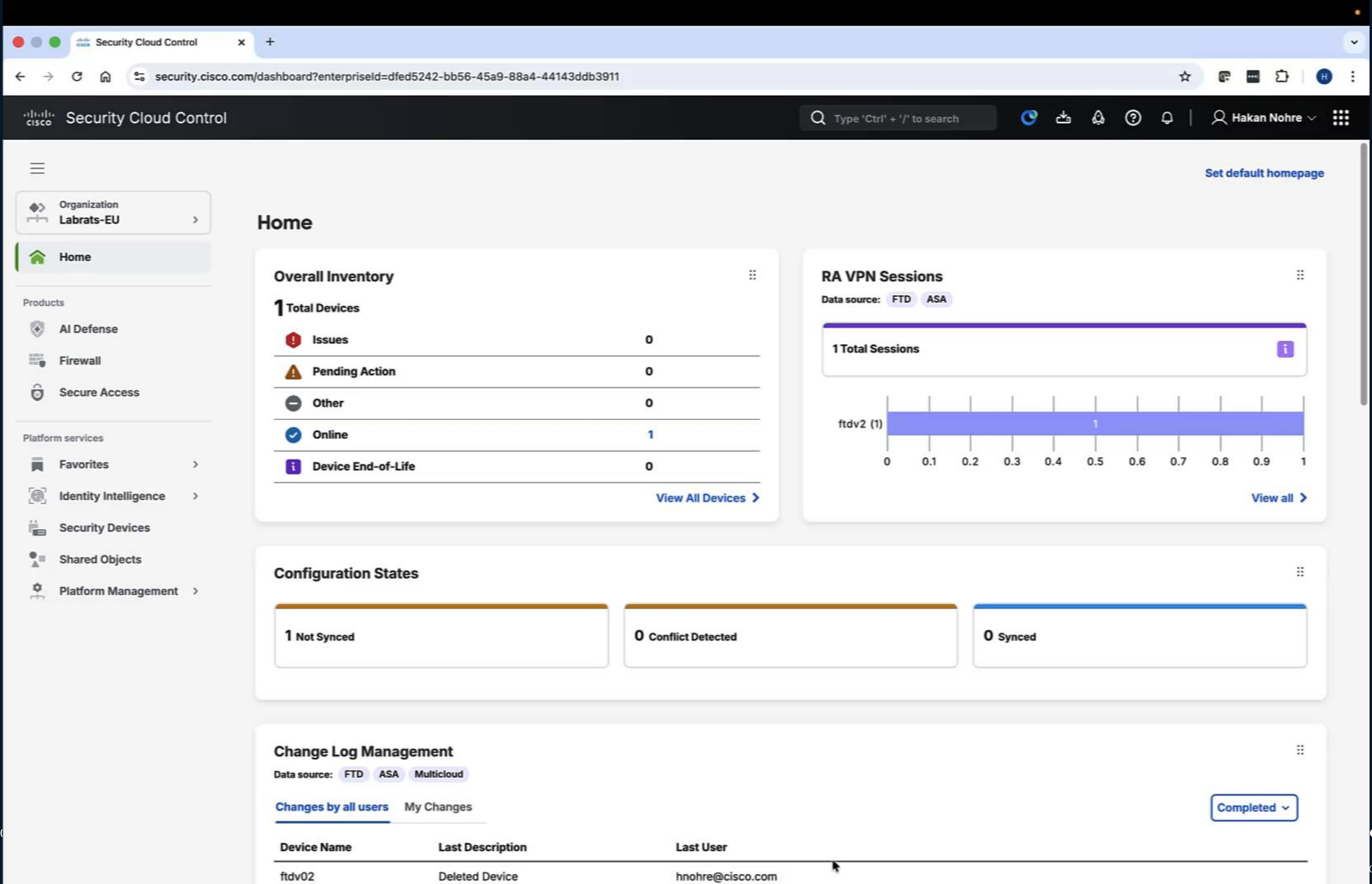
SGT Based Policy across network & Cloud

Maintain micro segmentation through Secure Access

Uniquely identify devices and traffic based on context from ISE

Apply policy to SGT Based identity





Home

Overall Inventory

1 Total Devices

Issues	0
Pending Action	0
Other	0
Online	1
Device End-of-Life	0

View All Devices

RA VPN Sessions

Data source: FTD ASA

1 Total Sessions

Configuration States

1 Not Synced

0 Conflict Detected

0 Synced

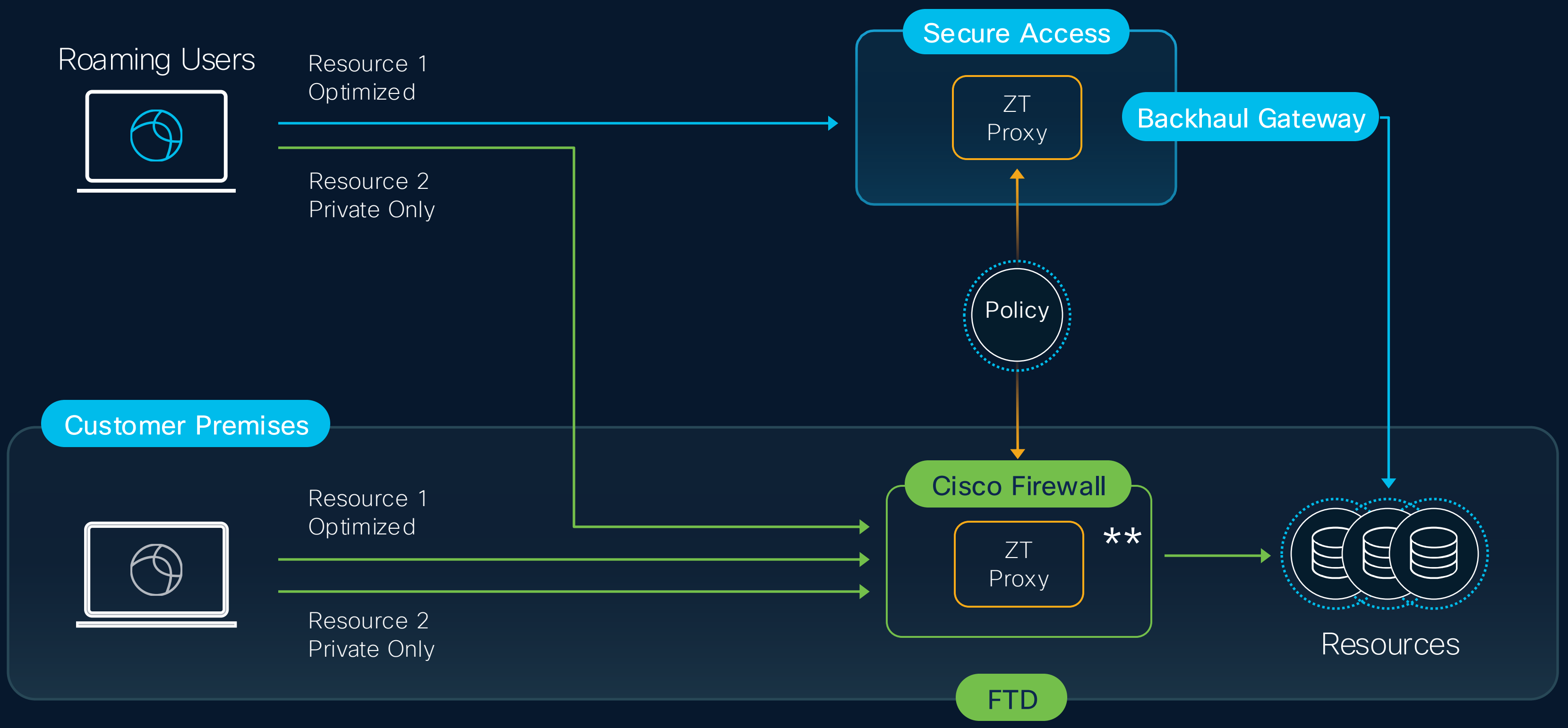
Change Log Management

Data source: FTD ASA Multicloud

Device Name	Last Description	Last User
ftdv02	Deleted Device	hnohre@cisco.com

Hybrid Private Access for Flexible Enforcement

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

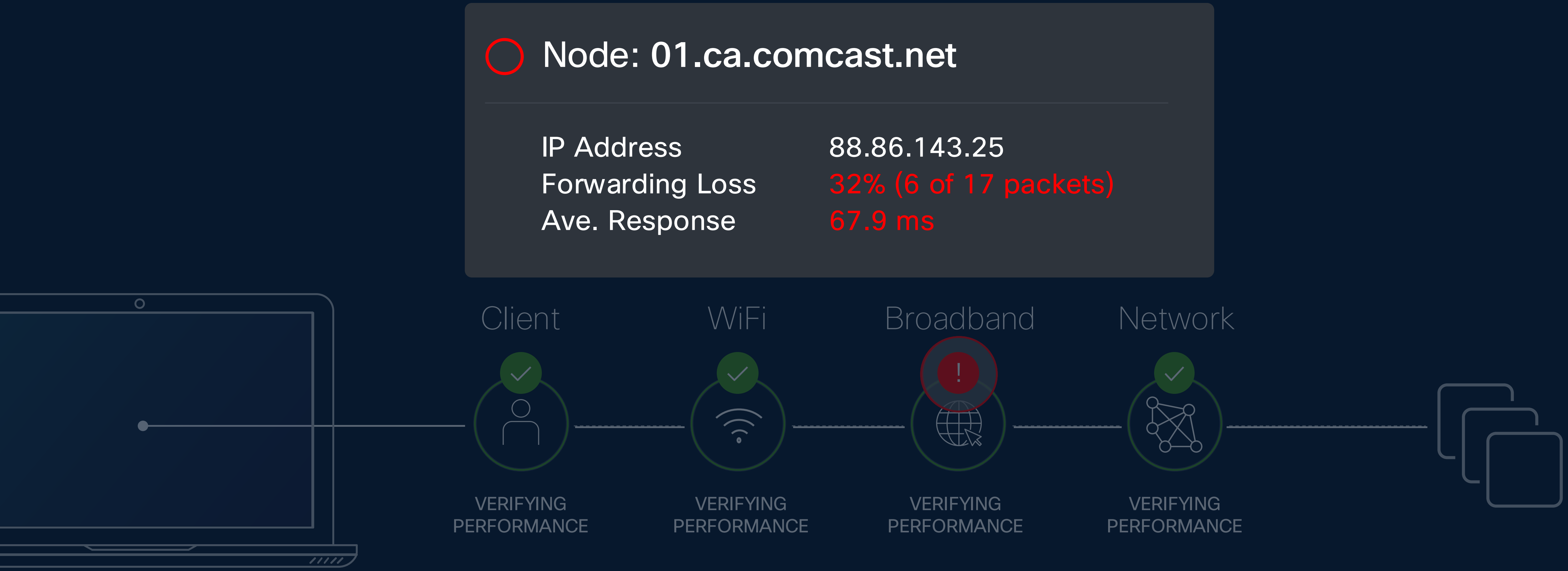


** Roadmap: policy enforcement on 8k routers

* Capabilities are in private preview.

See it all.

Fix issues fast with Experience Insights



○ Node: 01.ca.comcast.net

IP Address	88.86.143.25
Forwarding Loss	32% (6 of 17 packets)
Ave. Response	67.9 ms

Depictions are examples only.

Call to Action: Make it...

- Simple for Users
- Simple for Admins
- Integrated with the Network

cisco