Cisco Secure Access

Stepping Behind the Curtain

Jonny Noble - Cloud Security Technical Marketing
@JonnyNoble3

BRKSEC-2438

Webex App

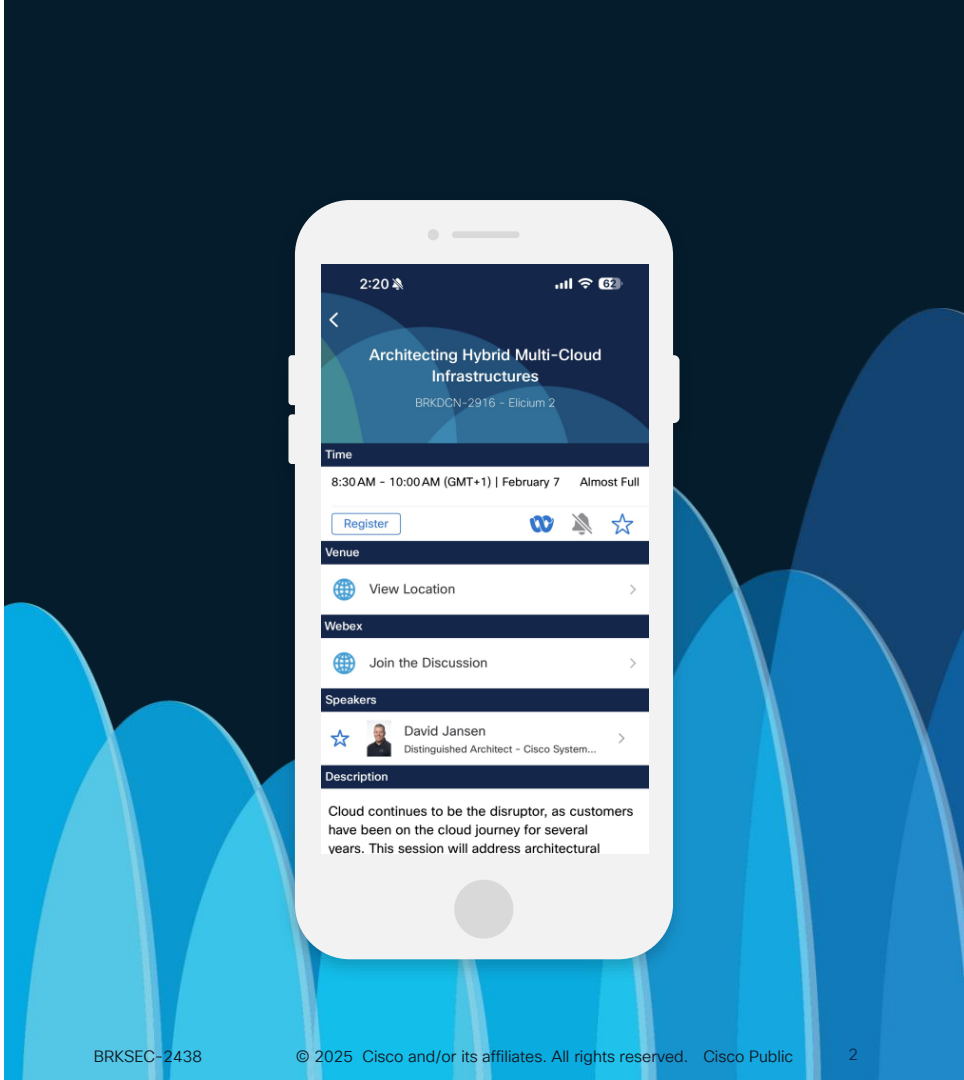
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.



Session abstract

- When end users connect to and consume cloud services, they don't know (and usually don't need to care) what's going on behind that curtain that drives the functionality they need and maintains a great experience. This should apply also in the case of cloud security solutions.
- Cisco Secure Access commits to provide the best experience for end users and admins alike. This session will take you on that journey, starting from the end user's perspective and drilling down into the cloud-native services that power the solution and guaranty an availability of five nines that Cisco can stand behind. We will cover how the cloud datacenter architecture provides speed, scalability, resilience, and consistency within each datacenter, across regions, and expanding to the complete global network. End to end performance monitoring is powered by Cisco's ThousandEyes technology providing visibility and transparency into the first, middle, and last mile.
- Thanks to additional Cisco technologies that are fully integrated into the solution through a single dashboard (and simple licensing), admins can easily set access policies and monitor performance, so that end users don't get distracted with decisions on how to access the resources they need to get through their work day.
- And before the curtain drops, we will conclude with demos that show how all of this comes together, providing you too with a great experience!

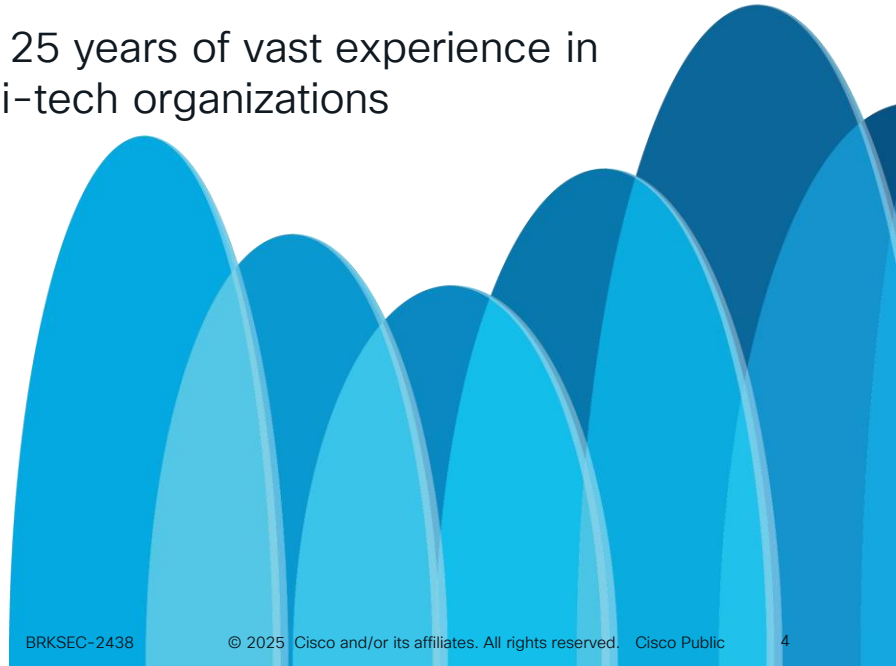
Jonny Noble - About me...

I am Director of Technical Marketing for Cloud Security at Cisco, with expertise in Secure Service Edge and surrounding SASE-related technologies.

I am focused on cyber-security and have over 25 years of vast experience in customer-facing disciplines in leading global hi-tech organizations

I am a seasoned speaker at Cisco Live events and regularly represent Cisco at numerous other customer and partner events, trade shows, and exhibitions.

I hold degrees in Electronics, Sociology, a Business MBA, and am CISSP certified



cisco Live!

When I’m not speaking at Cisco Live…

slido

Where have you joined us from today?

ⓘ Start presenting to display the poll results on this slide.

Agenda

- Session Introduction
- Setting the scene for Cisco Secure Access
- What have we built?
- Cloud architecture deep dive
- Experience Insights (+ demos)
- AI for Security; Security for AI (+ demos)
- Summary and Q&A

slido

Are you an existing customer?

ⓘ Start presenting to display the poll results on this slide.

Cisco Secure Access: A transformation journey

- This SSE offering has been many years in the making…
- Not just the last 18 months as we built this solution

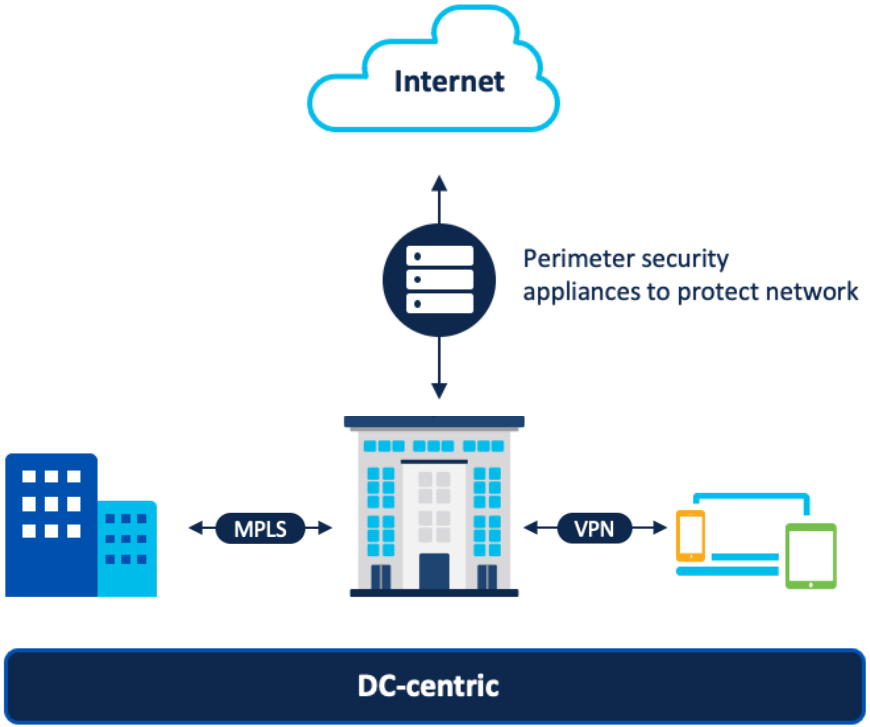
- Many insights learned over the last 8 years with Cisco Umbrella, which was originally designed for resolving DNS queries
- Highly optimal infrastructure today, totally redesigned from scratch
- Not only the infrastructure, but also the services running on it

- In this session we'll drill down on the infrastructure and services…

  …and see a few other cool innovations too!

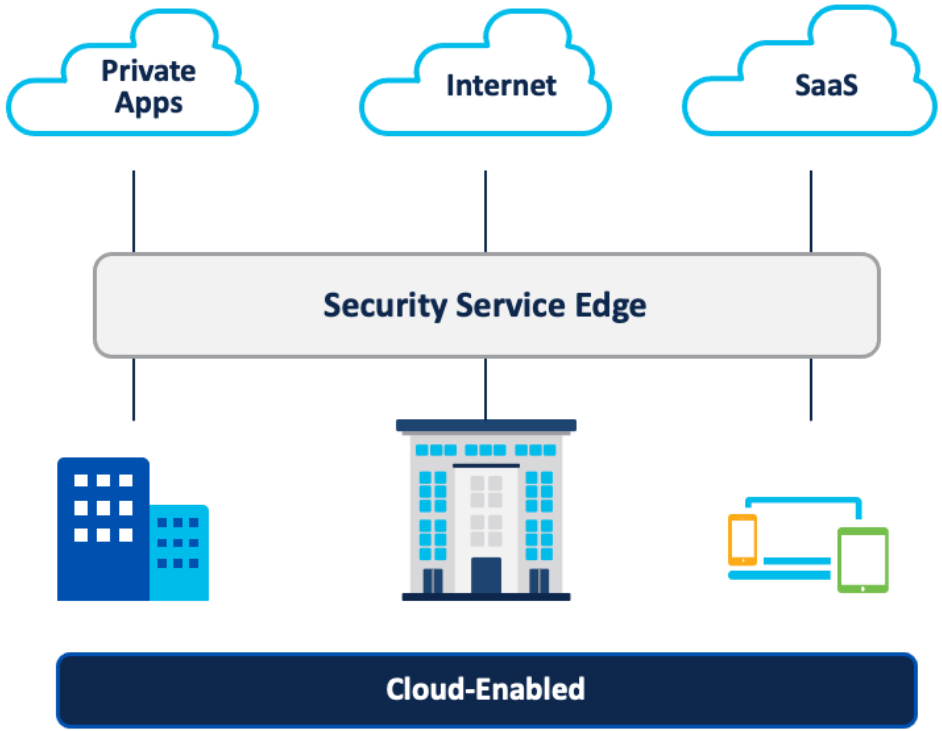
Transformation

...of our infrastructure and platform



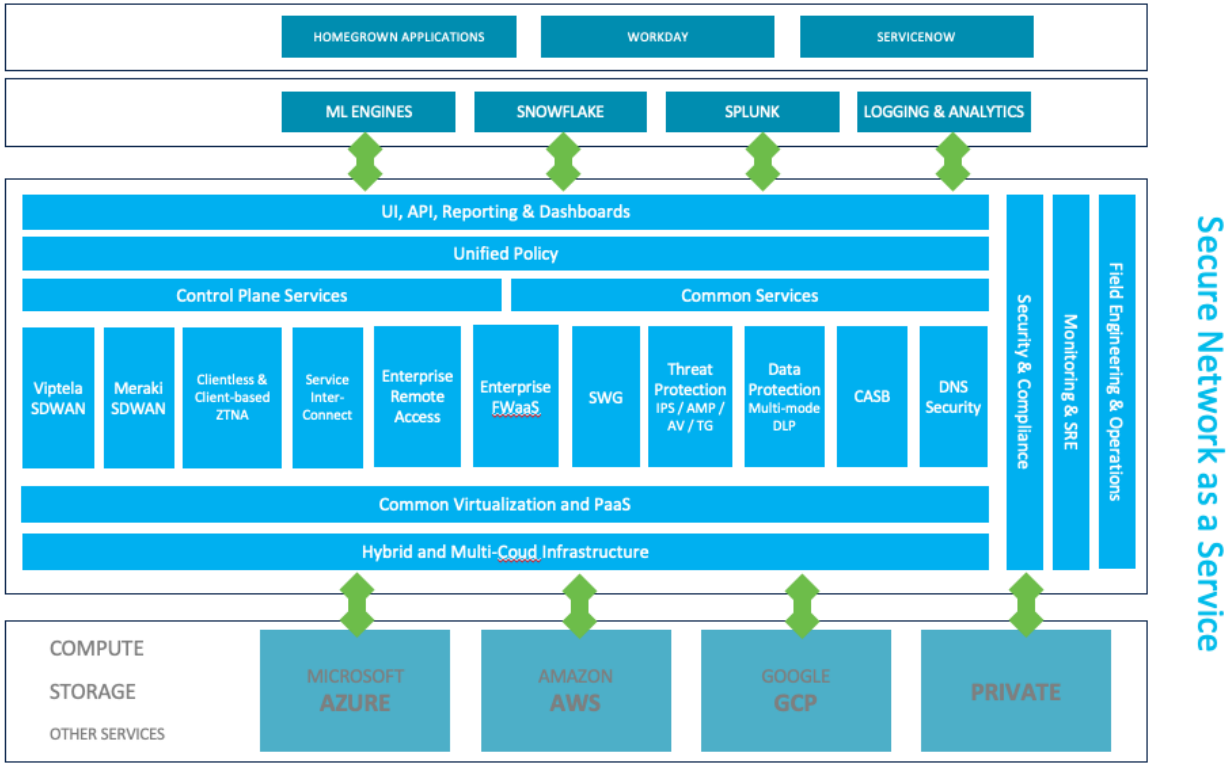
Transformation

...of our infrastructure and platform



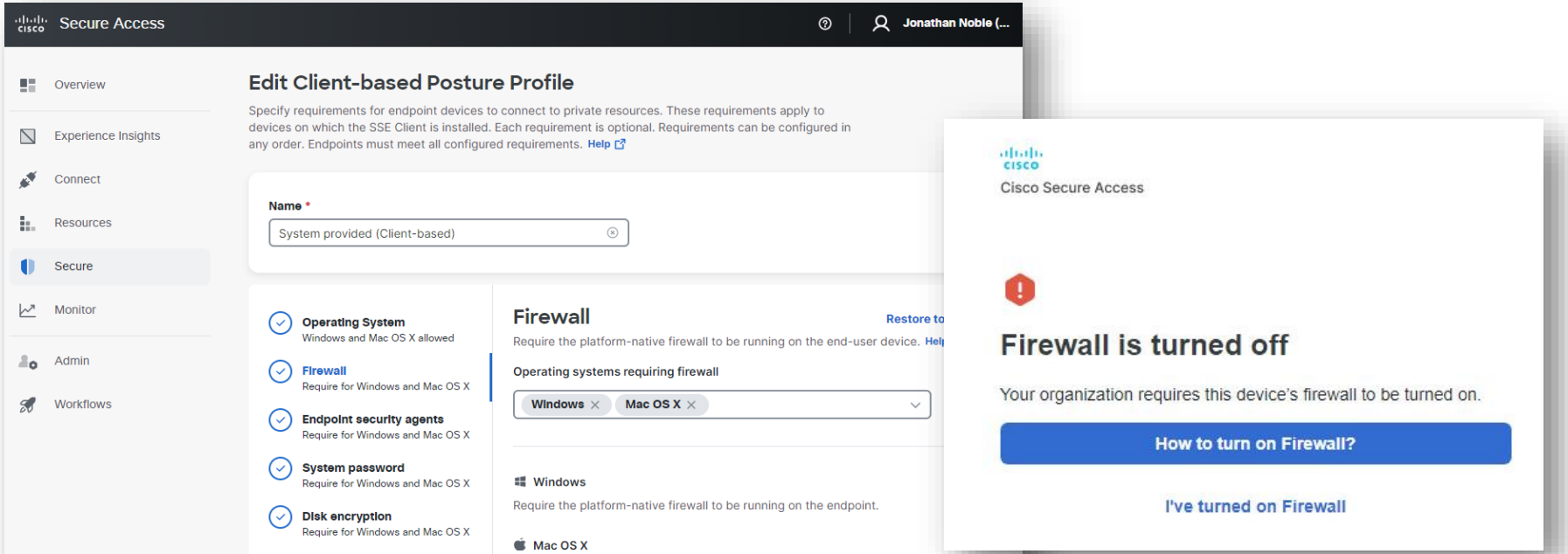
Transformation

...of our product architecture



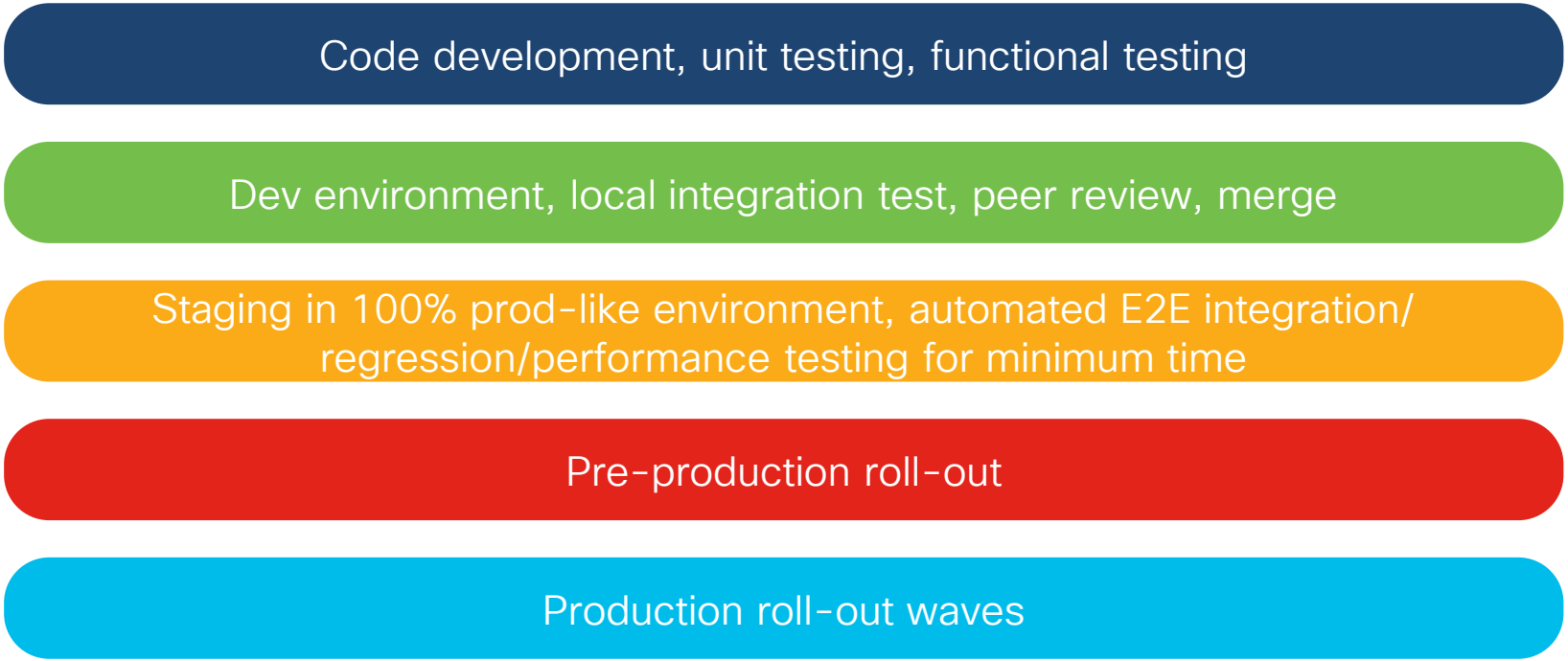
Transformation

…of our customers' admin and end-user experience



Transformation

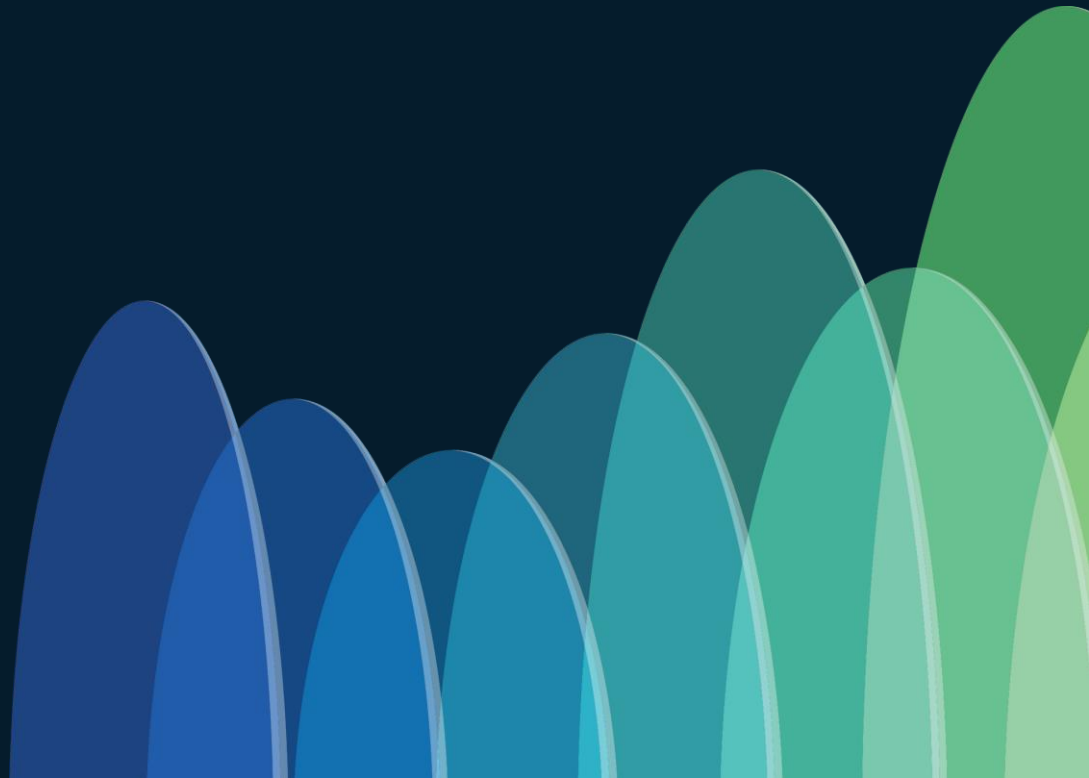
...of our software delivery systems



Result:

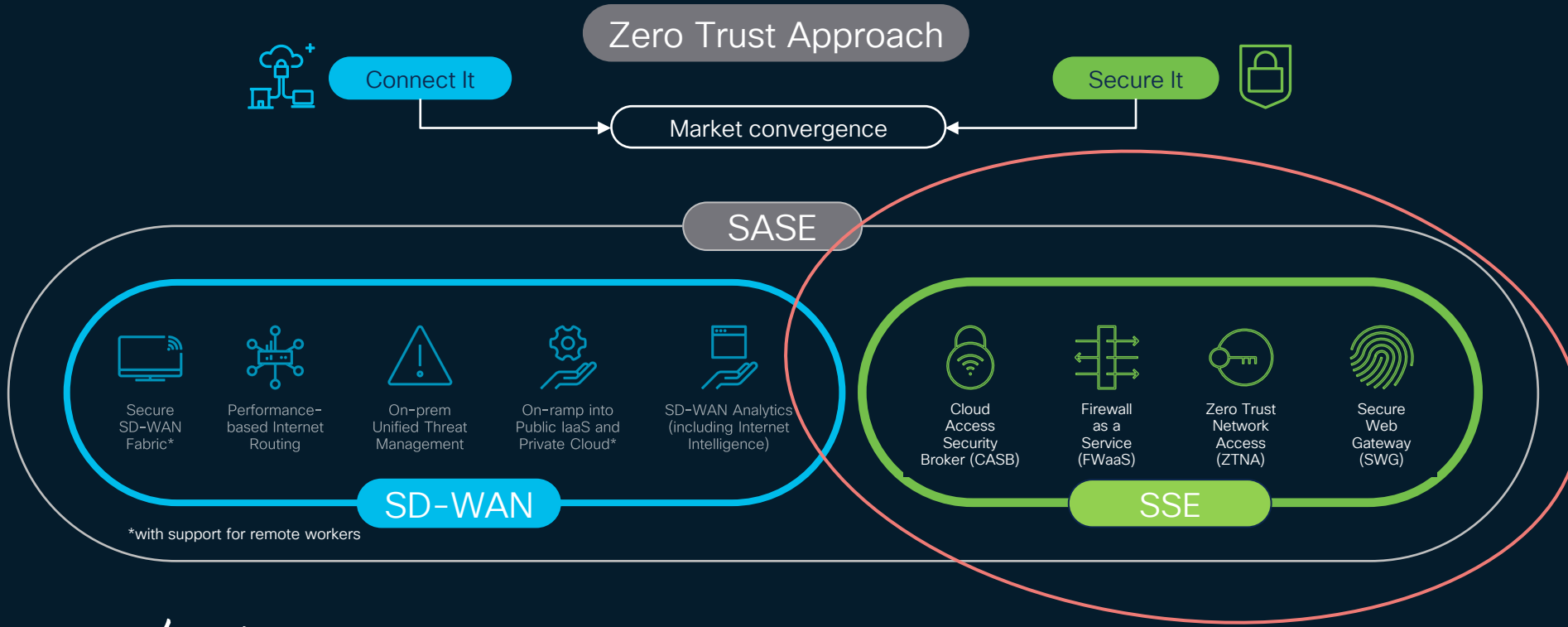
Cisco Secure Access

Hint: Slido quiz coming... 😎



SASE/SSE approach is the technology foundation

Fundamental to your security strategy for a hyper-distributed world



Cisco Secure Access

A comprehensive Security Service Edge (SSE) solution to accelerate your SASE journey

Core SSE Capabilities

Firewall as a Service (FWaaS)

+

Secure Web Gateway (SWG)

+

Cloud Access Security Broker (CASB)

+

Zero Trust Network Access (ZTNA)

and so much more in one subscription...

- Integration with Cisco SD-WAN and ISE
- 3rd party integrations (IdP, MDM (posture), and other security tools)
- Global scale with Cisco data centers and public cloud locations

Going beyond core Security Service Edge

Cisco Secure Access

- VPNaaS
- Digital Experience Monitoring
- DNS Security
- Remote Browser Isolation
- Data Loss Prevention
- Advanced Malware Protection
- Sandbox
- Talos Threat Intelligence
- AI-powered Platform

Consolidate security into one cloud solution with a single subscription

slido

Which ONE of the following statements is TRUE?

ⓘ Start presenting to display the poll results on this slide.

Cisco Secure Access

Modernize your defense with converged cloud security in a single subscription

Better for Users

Facilitate a frictionless workforce experience

Easier for IT

Lower cost and increase efficiencies

Safer for Everyone

Reduce risk and improve business resilience

Imagine cybersecurity that's

safer and easier for everyone

Unique secure access that is easier and safer for everyone...

From anywhere

Remote users

Managed and unmanaged devices

Cisco Secure Access

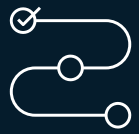
Better for Users

Exceptional User Experience

Users Login and get to work

Easier for IT

Simplified IT Operations



IT has one dashboard to see traffic, set policies, and analyze risk

Safer for Everyone

Tighter Security

Converged, cloud-native security defends against the unknown

Converged cloud-native security on a single platform

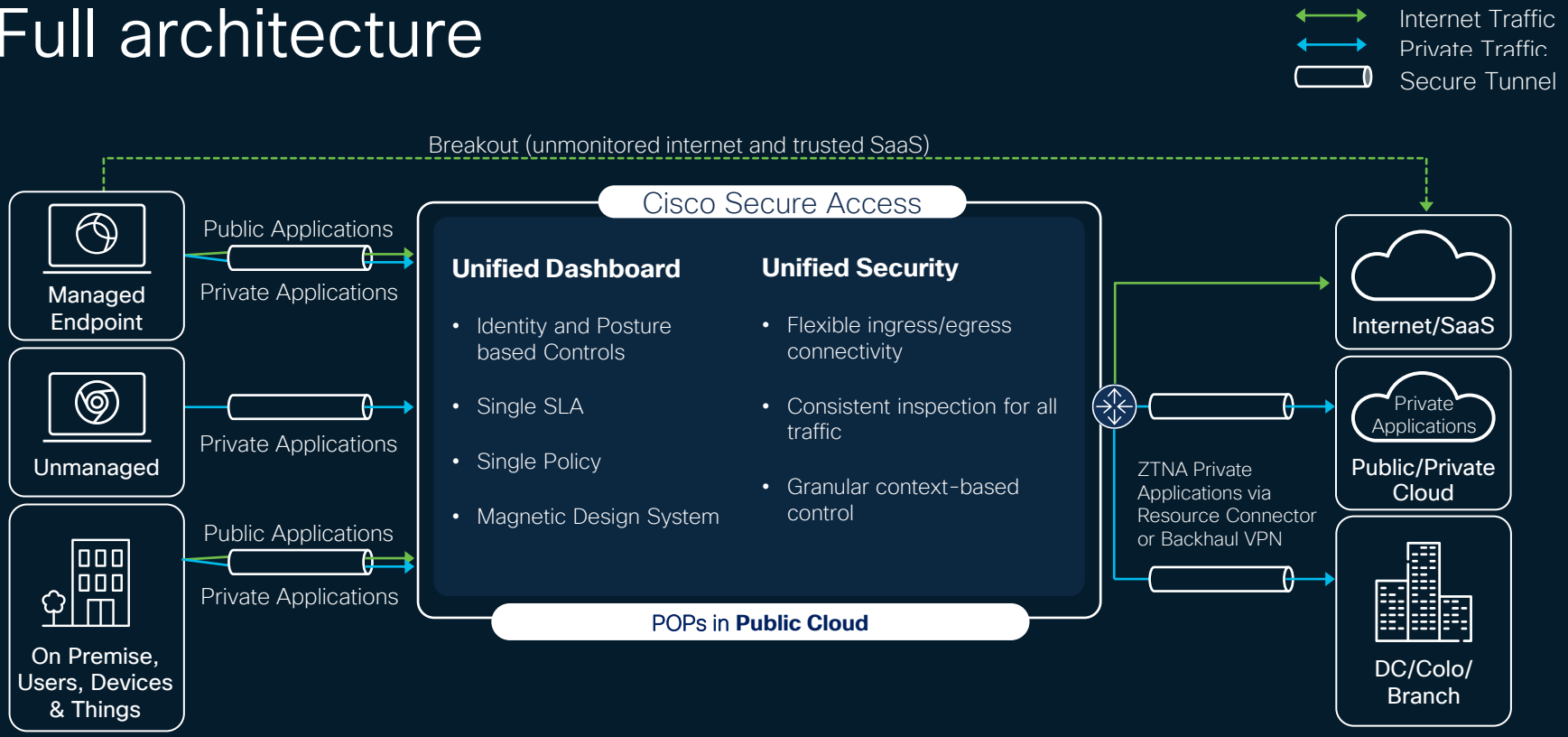
To anything

Web

Public SaaS apps

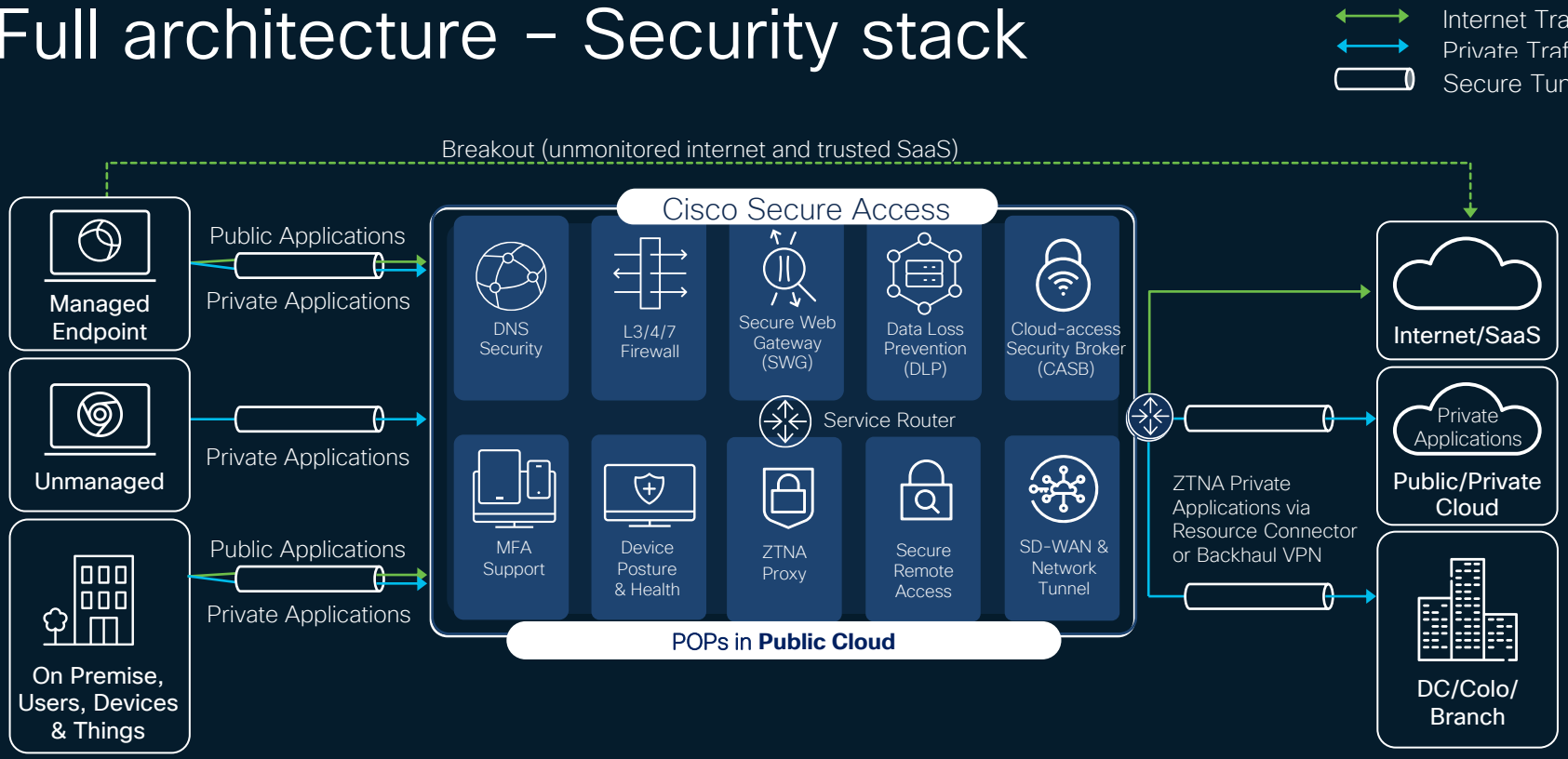
Private apps

Full architecture



Users & Devices — **How** — **Apps**

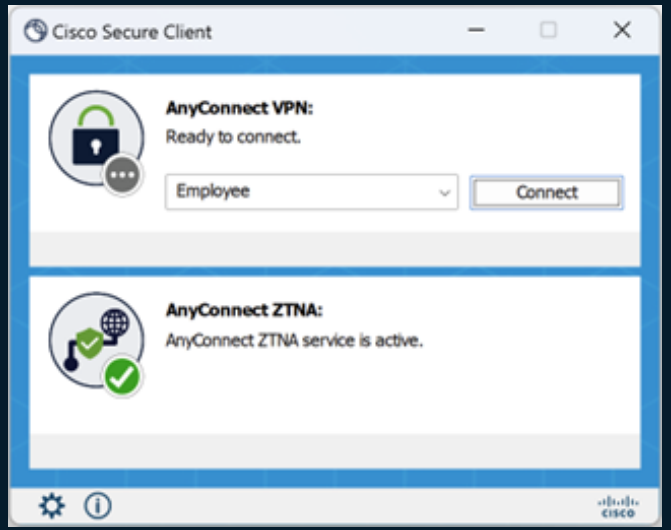
Full architecture – Security stack



Cisco Secure Client - Zero Trust Access module

- Transparent user experience
- Proxied resource access with coarse-grained or fine-grained access control
- Service managed client certificates with TPM/hardware enclave key storage

- Support for both TCP and UDP applications
- Cisco and third-party VPN client interop
- Next-generation protocol (QUIC & MASQUE)



What are QUIC and MASQUE?

QUIC (not an acronym)

- UDP-based, stream-multiplexing, encrypted transport protocol
- First used in Google Chrome in 2012
- Used for HTTP/3, Apple iCloud Private Relay, SMB over QUIC, DNS over QUIC, etc.
- Optimized for the next generation of internet traffic with low latency and high capacity, compared to TLS over TCP
- Supports micro-tunnels

MASQUE (Multiplexed Application Substrate over QUIC Encryption)

- IETF working group focused on next generation proxying technologies on top of the QUIC protocol
- Provides the mechanisms for multiple proxied stream and datagram-based flows inside HTTP/2 and HTTP/3
- Used by iCloud Private Relay since 2021
- HTTP/2 and HTTP/3 extensions allow for the signaling and encapsulation of UDP and IP traffic

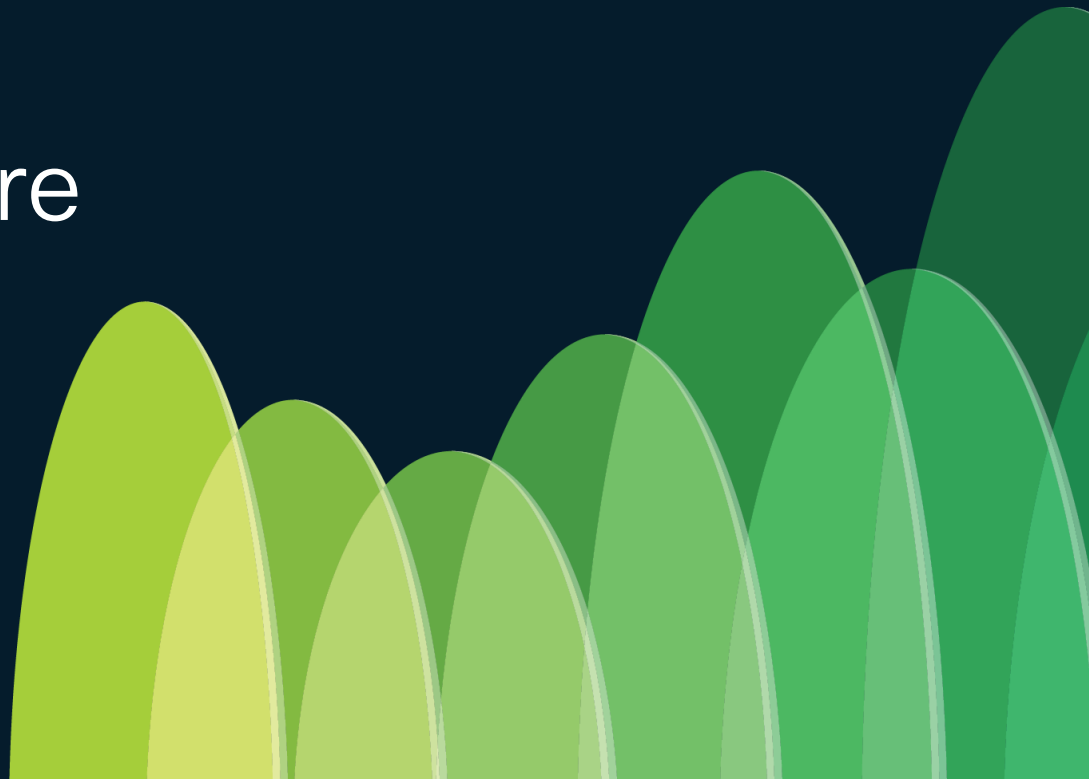
When combined, MASQUE + QUIC provides an efficient and secure transport mechanism for TCP, UDP and IP traffic for both web and non-web protocols

slido

What are the advantages of using QUIC and MASQUE for ZTA? (multiple)

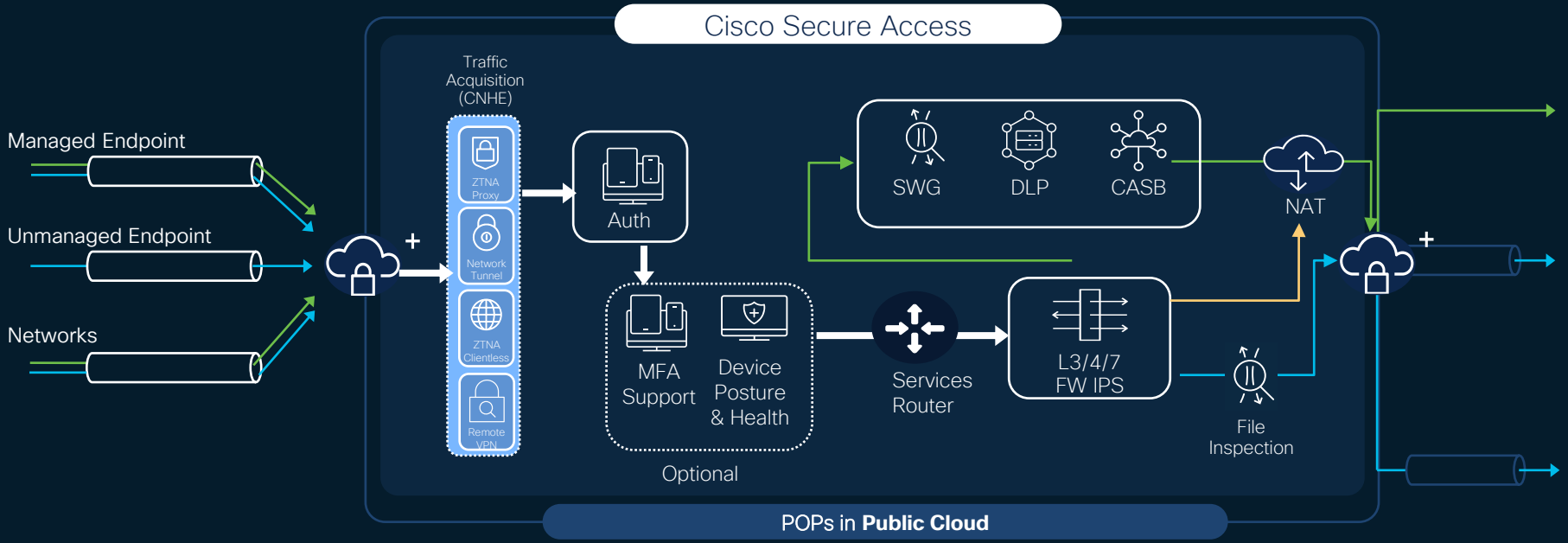
ⓘ Start presenting to display the poll results on this slide.

Cloud Architecture Deep Dive

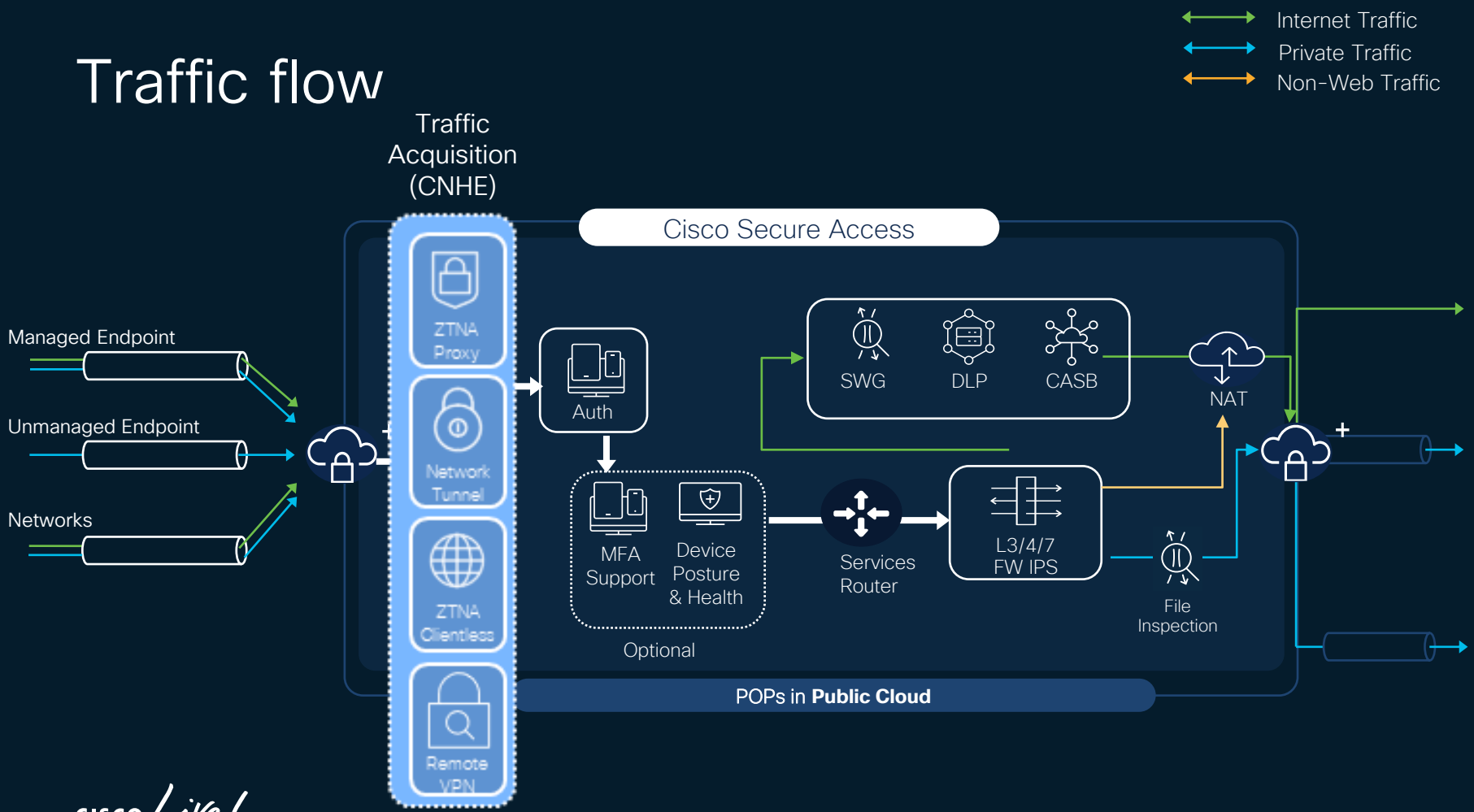


cisco Live!

Traffic flow



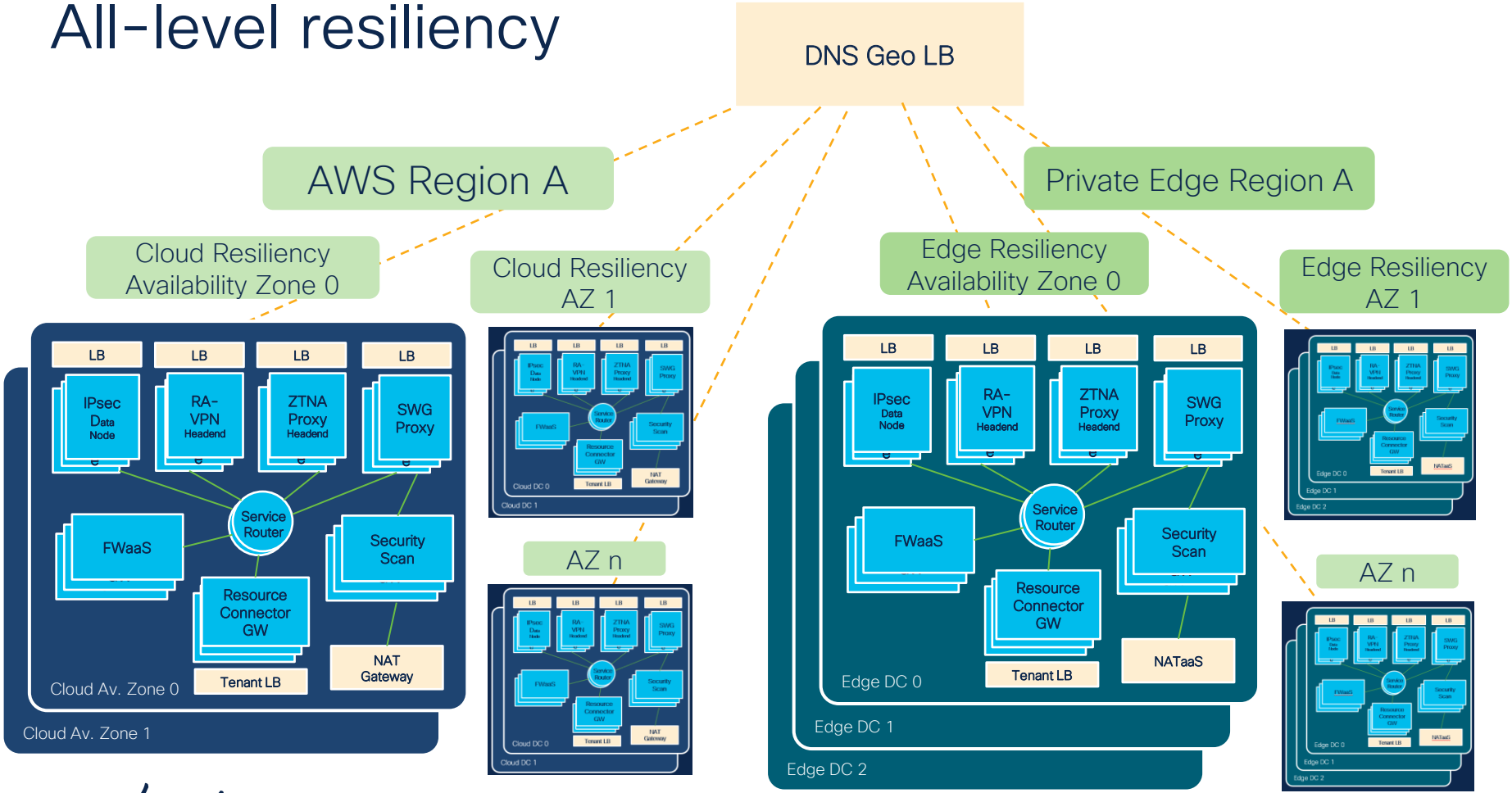
Traffic flow



Supported use-cases

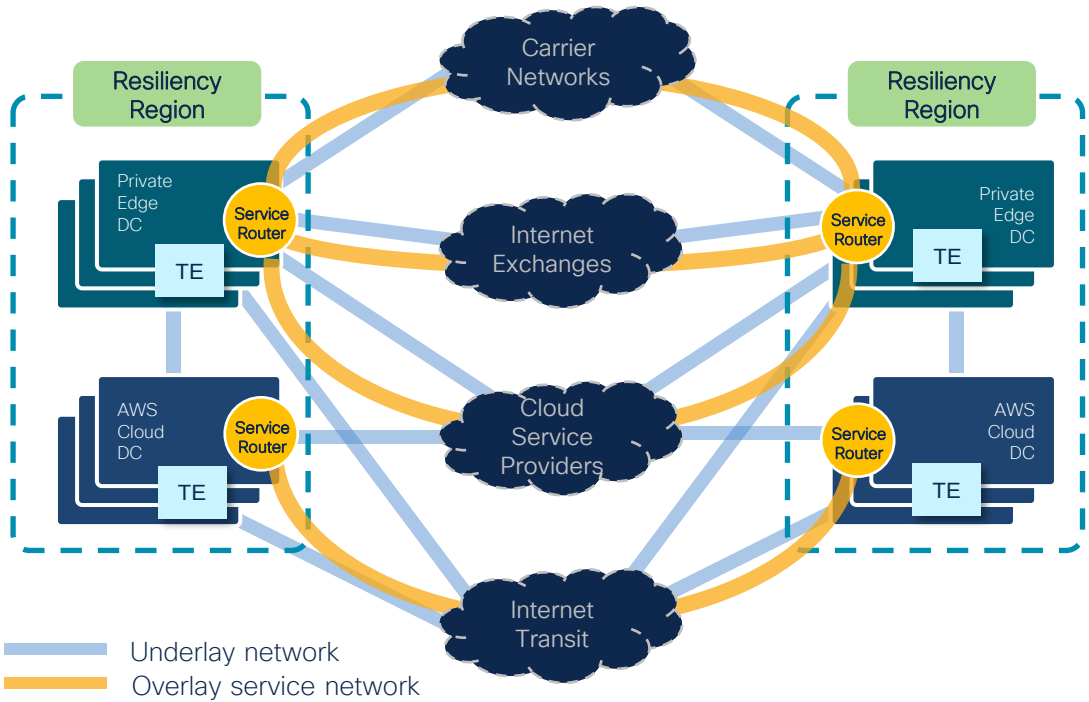
1. DNS security
2. Branch to internet
3. Branch to branch
4. RAVPN user to internet
5. RAVPN user to branch/private app
6. Client-based ZTNA to private app via S2S VPN
7. Clientless ZTNA to private app via S2S VPN
8. SWG roaming user to internet
9. RAVPN user to RAVPN user
10. Branch user to RAVPN user
11. Client-based ZTNA to private app via Resource Connector
12. Client-less ZTNA to Private App via Resource Connector
13. Cisco SD-WAN to Internet, DIA use case

All-level resiliency



Global scale architecture

Connecting users and apps from anywhere to anywhere, with low latency and high availability



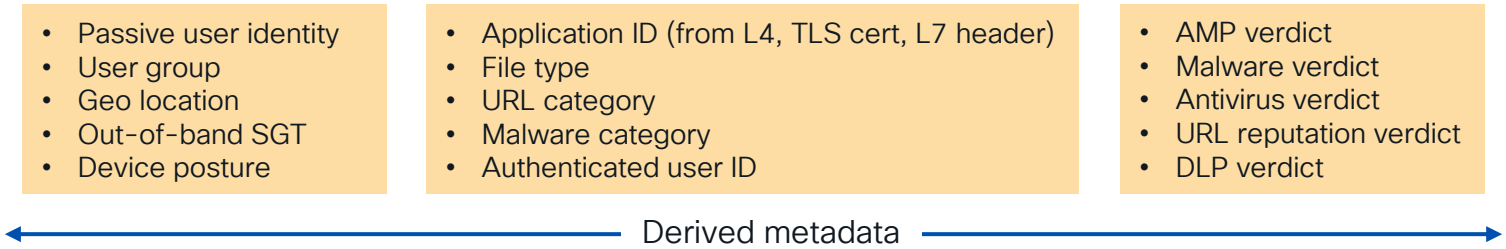
- Overlay service network independent of underlying network architecture (CSP, private network or hybrid)
- Overlay Service Router interconnects services within and across POPs, and globally
- Private peering to major carriers, Internet exchanges and CSPs for low latency and redundancy
- ThousandEyes (TE) integration and private tooling for continuous mentoring for availability, latency and optimal paths

“Flex-Single-Pass” architecture

- Our Flex-Single-Pass processing ensures that we achieve and maintain the optimal balance for performance, flexibility, and security
- Not just deployment of appliances in a virtual form factor in the cloud (would provide performance but not scale or reliability)
- Packets traverse the services without any redundant processing
  - We decrypt in one service and the decrypted data is transported with high bandwidth into our other services
  - After user identity is derived, that user’s identity is shared everywhere so that the policy enforcement is consistent
- All services can be scaled independently, for parsing policy logic and deep packet inspection, then all merged for final verdict and logging

“Flex-Single-Pass” architecture

- Each service responsible for its own layer → parallel scans with no redundant processing
- Consistent multi-stage policy evaluation as data becomes available (L3/4→L7→content)
- Metadata shared across services for flexible services and end-to-end policy
- Optimized for flexibility/scalability and single-service performance
- Expanded to global connections with Service Router – consistent security even traversing across geo-regions



Proven security capabilities converged in one cloud service

Secure access regions – AWS coverage

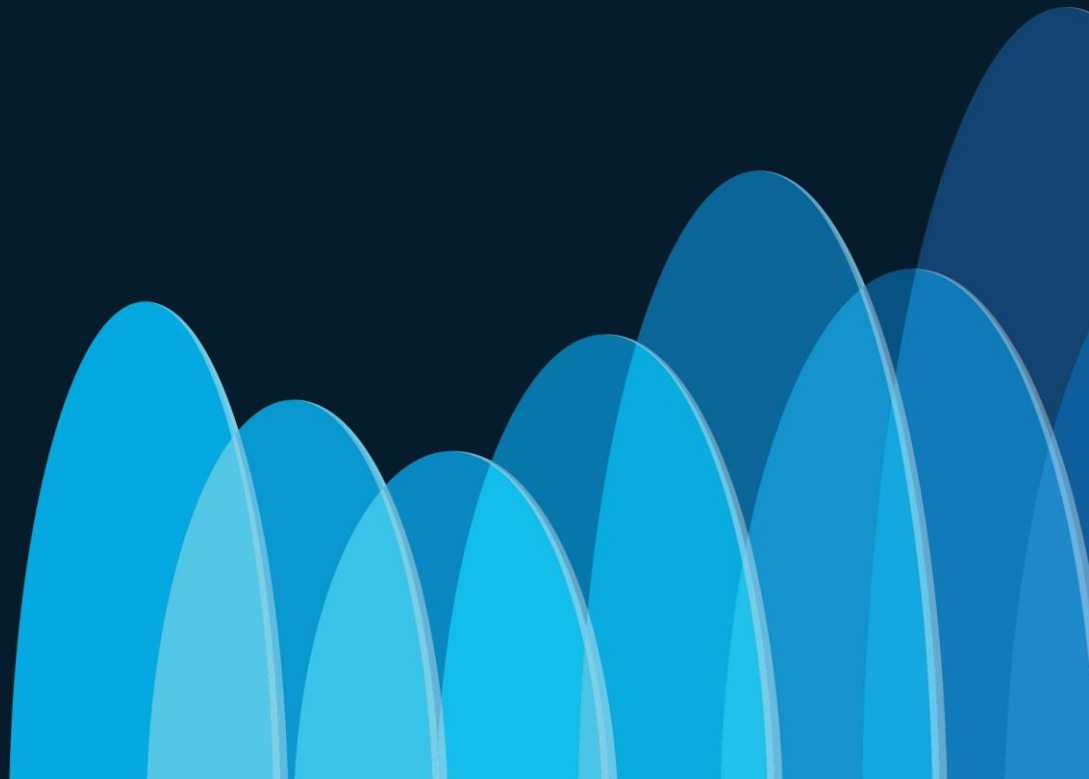
Secure access regions – Physical DC coverage

In Development & Coming Soon	
Amsterdam	Tokyo
Frankfurt	Osaka
Chicago	Mumbai
Dallas	Chennai

Legend

- Available
- Available (PP)
- In Development

Experience Insights



cisco Live!

What is Digital Experience Monitoring?

"Digital experience monitoring (DEM) technologies monitor the availability, performance and quality of an end user or digital agent experiences when using a device or application." – Gartner

Enhance troubleshooting capabilities and proactively monitor our customer's connectivity experience to Cisco Secure Access and their favorite applications

Metrics → Information → Actionable Intelligence

Digital Experience Monitoring > Experience Insights

DEM

Q: Is it "Monitoring" or "Management" for the acronym "DEM"?

A: Digital Experience Monitoring (DEM) is often adjusted to read Digital Experience Management (DEM)

- This is to convey our intention to not just monitor and identify, but also find ways to offer actionable remediation and optimization capabilities in this space
- The DEM feature set within Secure Access is collectively named:

Experience Insights

Experience Insights functionality

- ThousandEyes provides the foundational functionality for the first iteration of this feature space
- ThousandEyes EndPoint Agents (EPA) is installed as a module under Cisco Secure Client, to obtain end-user metrics
  - Provides automated collection of key metrics, vital in identifying device's health and performance, including CPU; memory; WiFi strength; network quality (latency, jitter, packet loss); connectivity to Cisco Secure Access
- ThousandEyes Enterprise Cloud Agents (ECA) are deployed within Secure Access to monitor connectivity from Secure Access Cloud to common SaaS apps and private resources

Experience Insights architecture

- Provisioning/Enrollment of Agents
- Configuration Pushes
- Metrics Data Collection
- APIs for posting/retrieval

Customer Endpoint to Cisco DC Performance

1 Remote User to DC Performance

End User

Managed Endpoint

Cisco Secure Client

VPN (DNS LB Region)

ThousandEyes Endpoint Agent

Roaming Client (DNS LB Global)

ZTNA (DNS LB Global)

ThousandEyes Cloud

ENTERPRISE AGENTS

DC

Cisco Secure Access

DNS Security

L3/4/7 Firewall

Secure Web Gateway (SWG)

Data Loss Prevention (DLP)

Cloud-access Security Broker (CASB)

MFA Support

Device Posture & Health

Secure Access (ZTNA/VPNaaS)

Unified SSE Dashboard
- Identity and Continuous Posture-based Controls
- Unified Policy
- Single SLA
- Magnetic Design System

POPs in Public Cloud and Cisco Edge Data Centers

cisco

Admin

DEM Dashboards

2 DC to SaaS App Performance Monitoring

DC to Apps Performance

box

salesforce

Office 365

aws

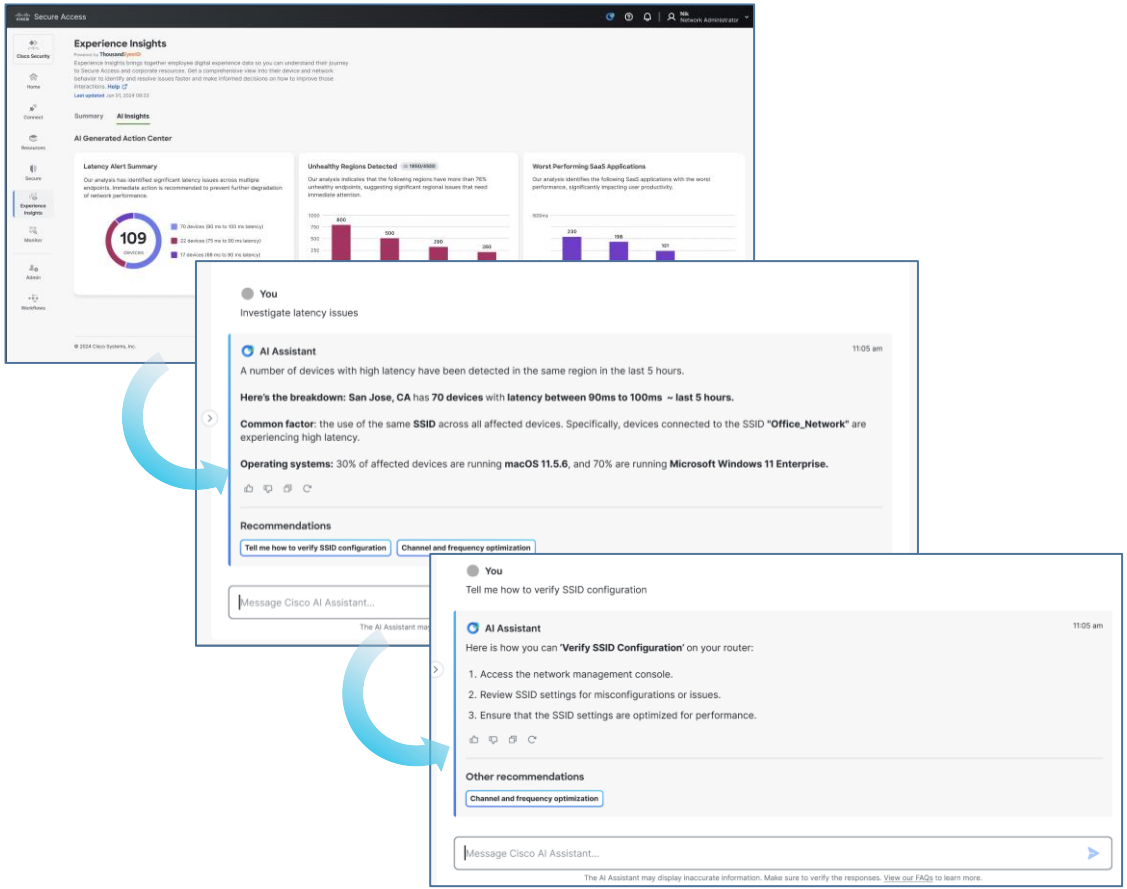
SaaS apps

DEM: End-to-End Network and HTTP Tests

- Create network or http tests to public or private resources to monitor data path
- Segment visualization with per hop view to the performance
- Requires ThousandEyes Essentials or Advantage license
- Available in Secure Access dashboard without cross-launch

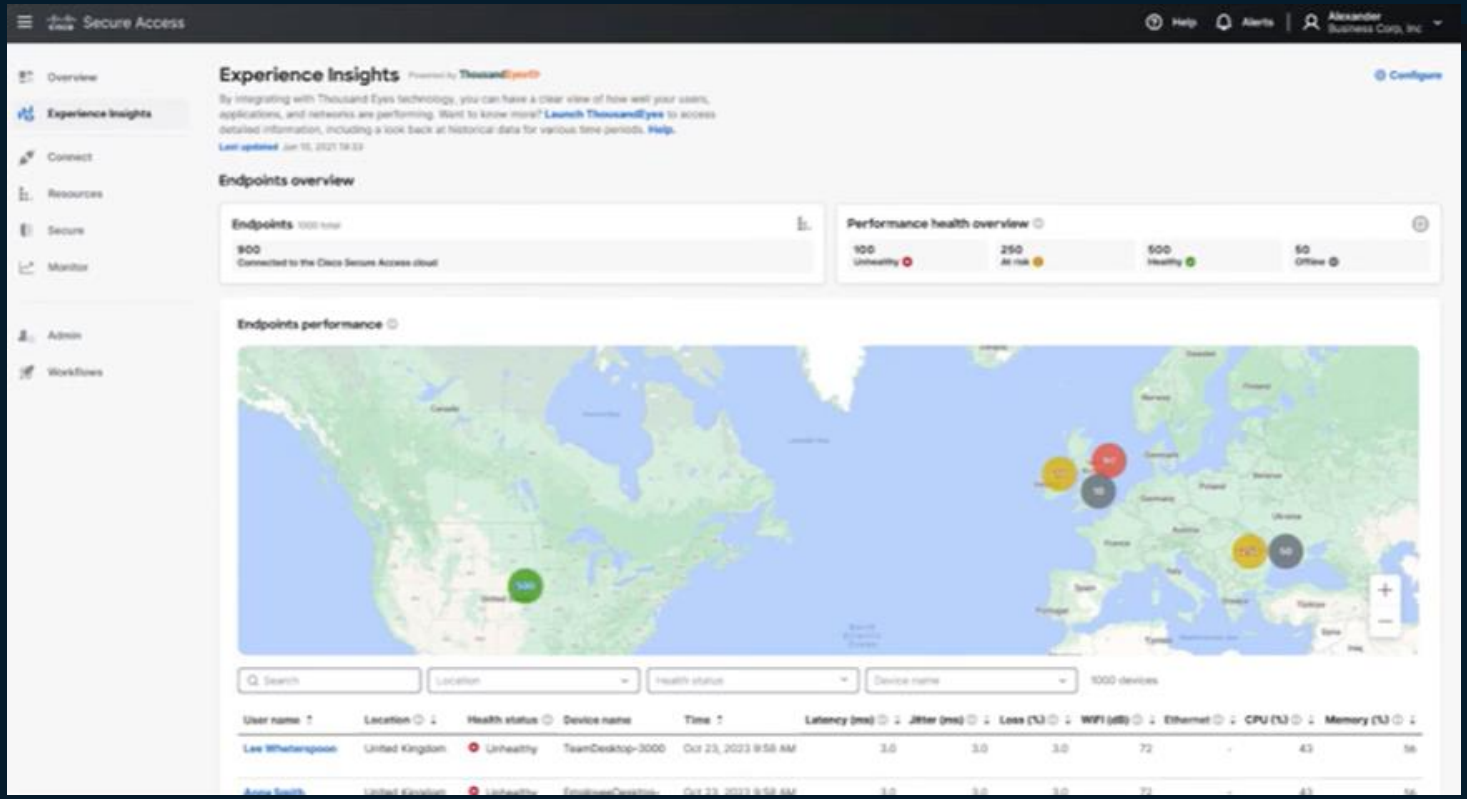
AI Insights for Experience Insights

- Powered by Gen-AI, and helps admins find information on network performance metrics, status of the devices, SaaS apps, and inventory information
- Troubleshoot connectivity issues quickly instead of having to go through multiple pages and tools to resolve the issues

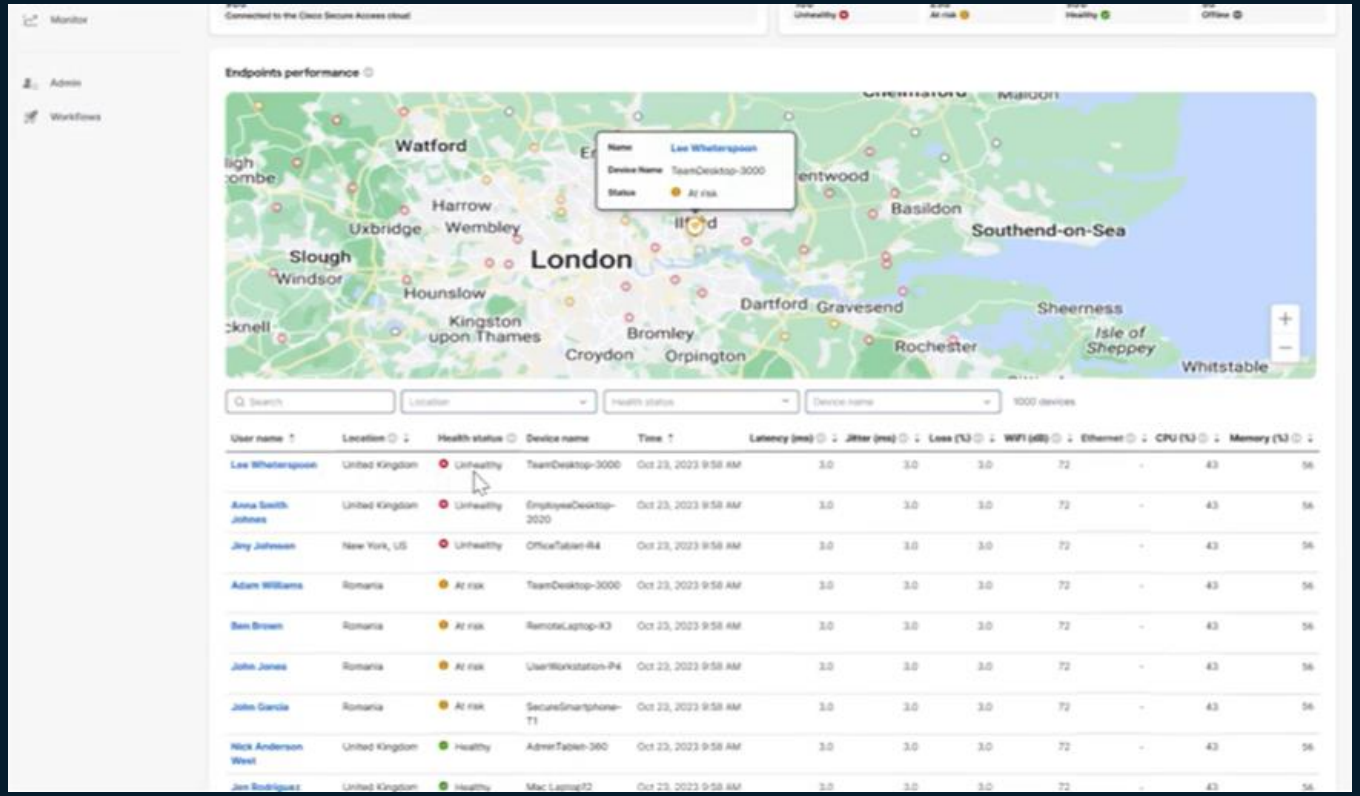


Demo:
Experience Insights

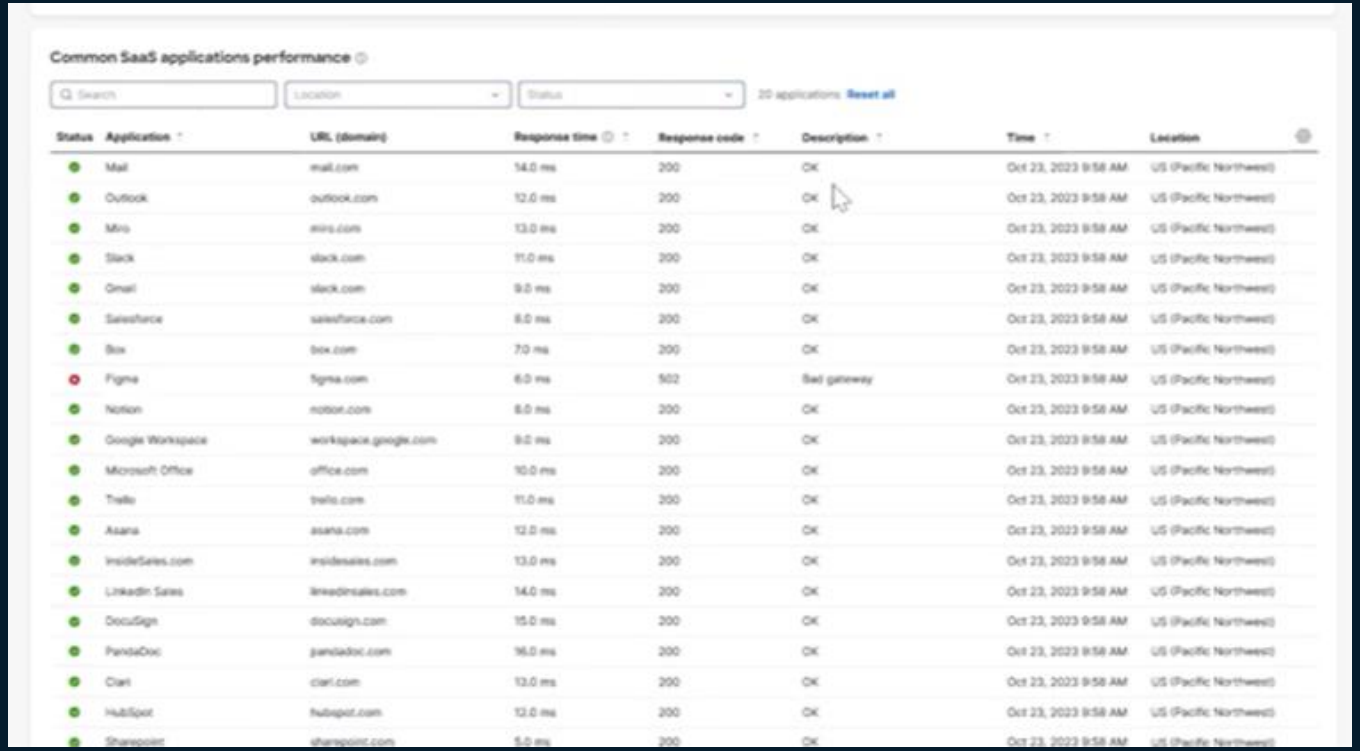
Demo reminder: Experience Insights



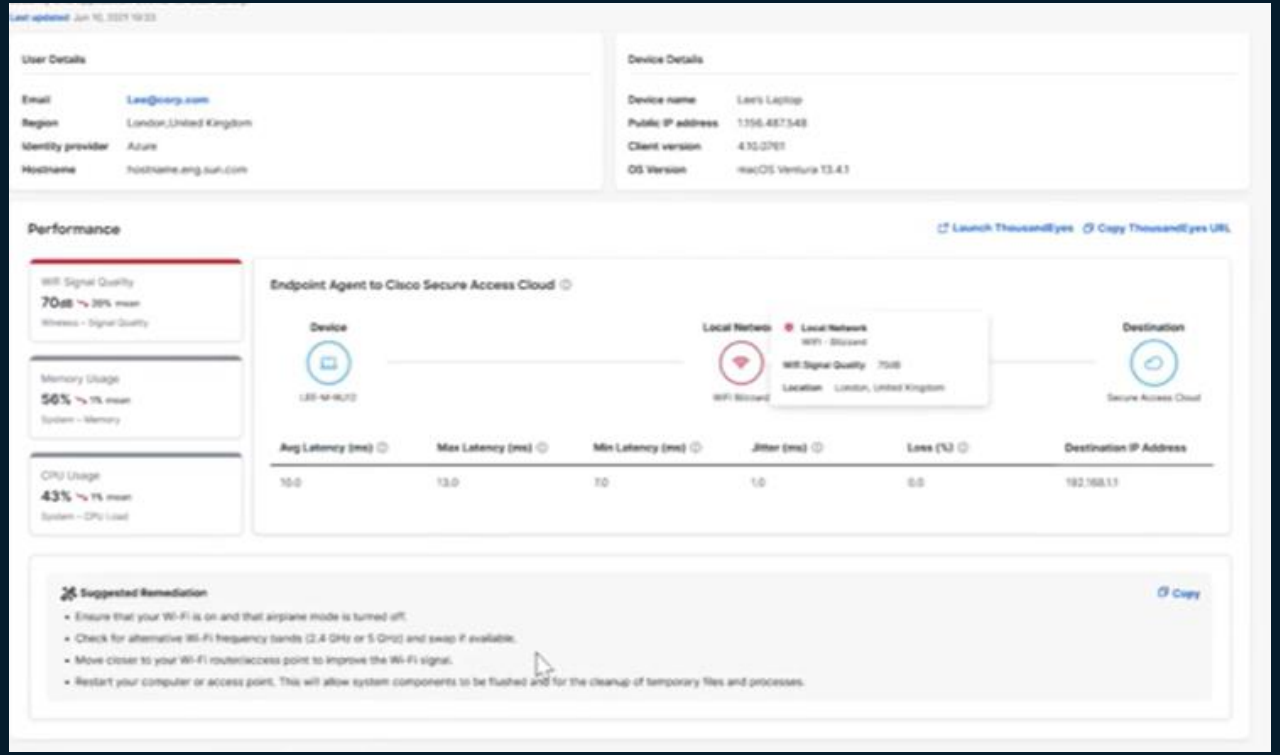
Demo reminder: Experience Insights



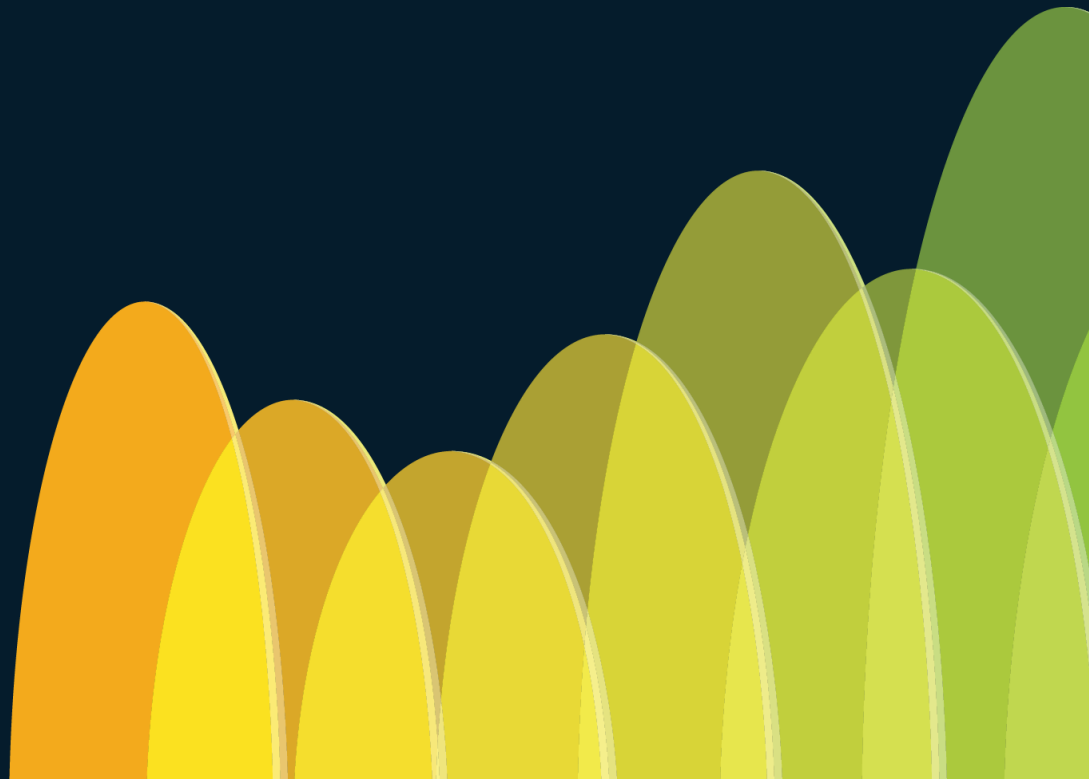
Demo reminder: Experience Insights



Demo reminder: Experience Insights



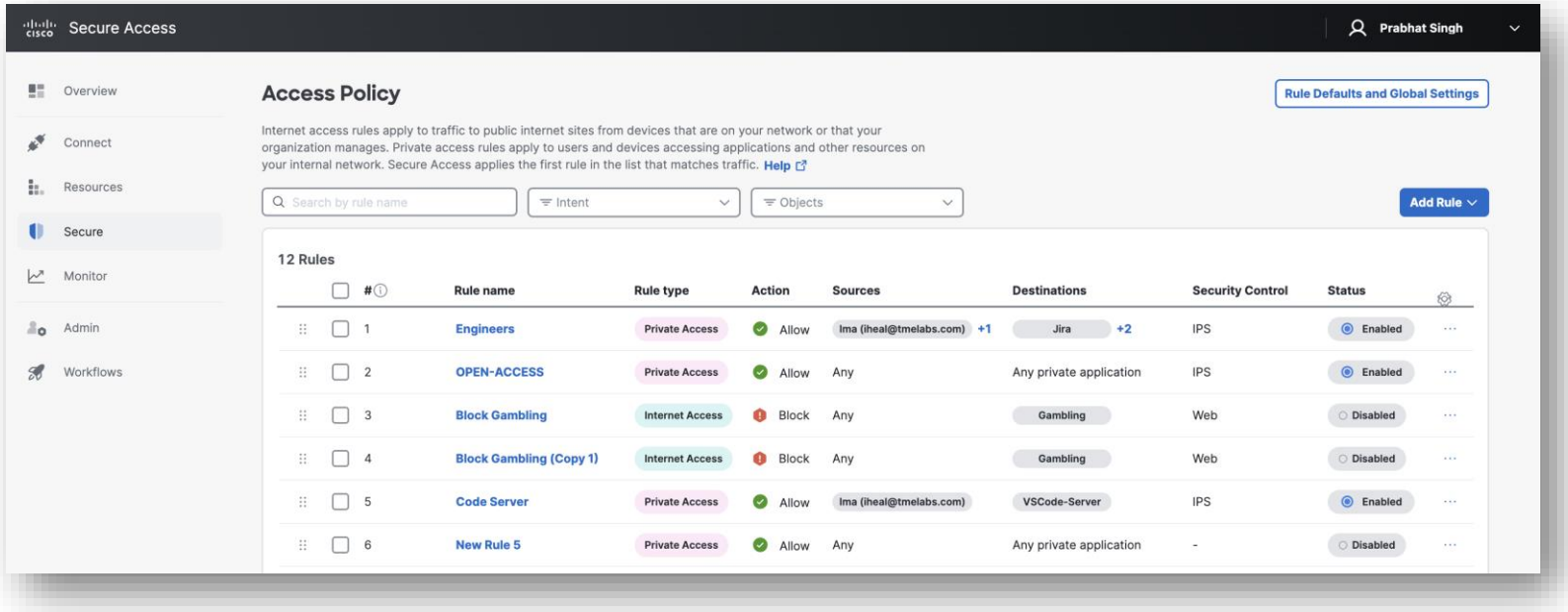
AI for Security; Security for AI



cisco Live!

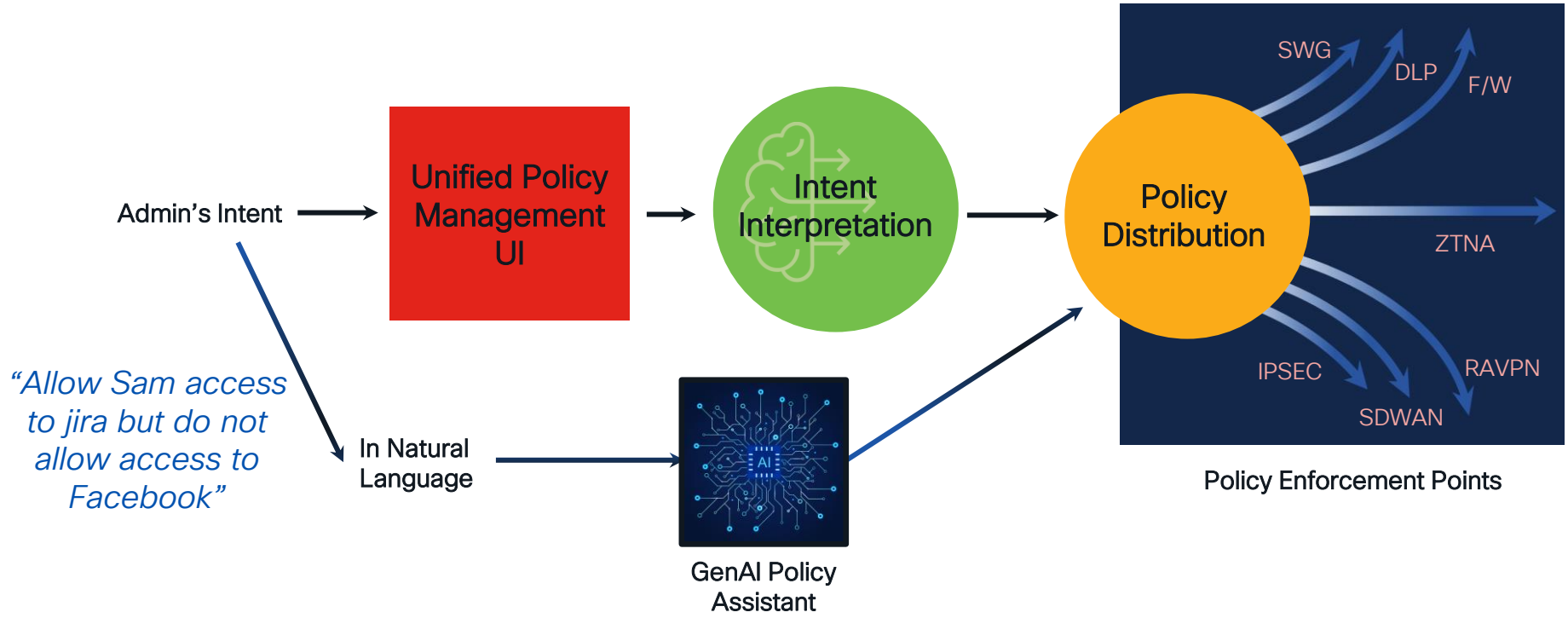
Unified, single, intent-based policy

- Based on the “what”, not the “how”
  - Allow Sam access to Jira, but not to Facebook
  - No mention of Firewall or SWG, only what to allow and deny



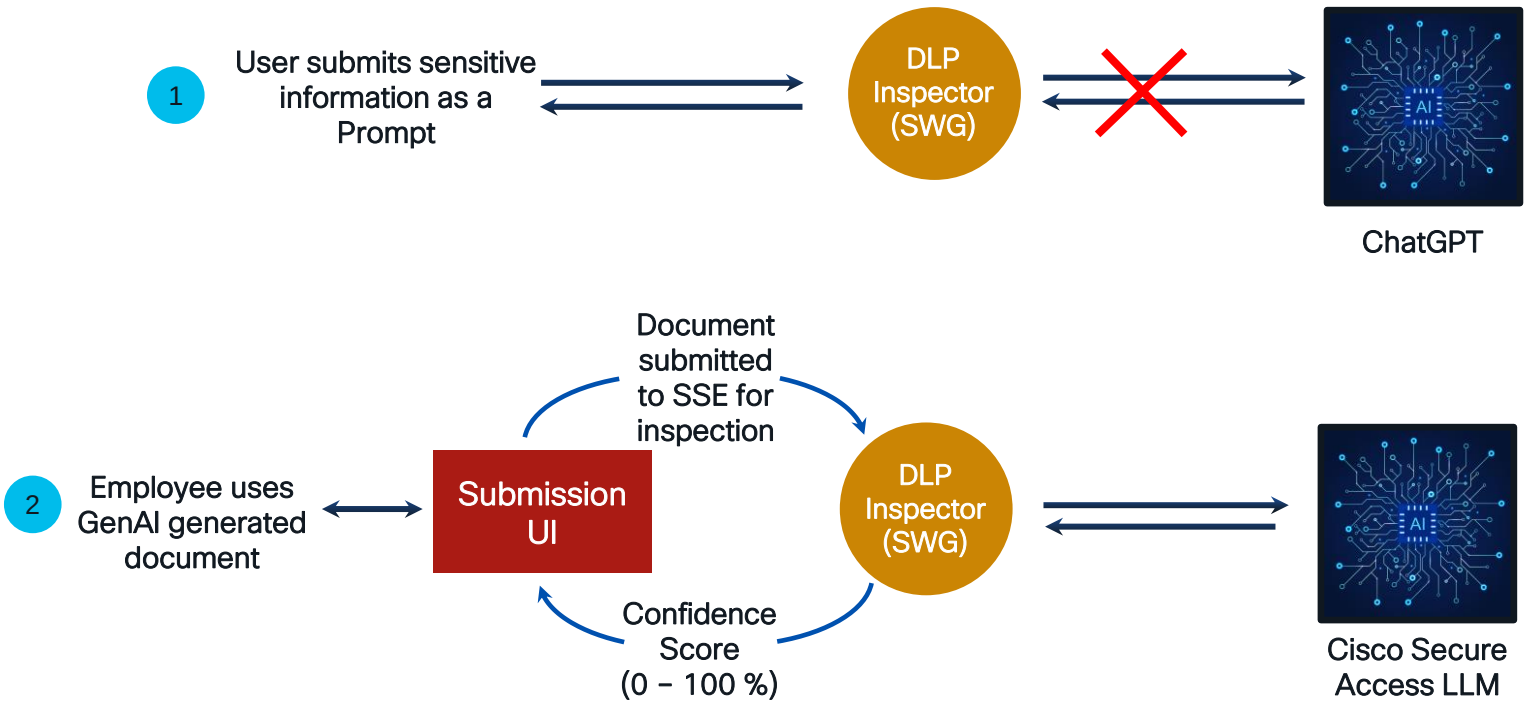
Intelligent unified, intent-based policy

(first-to-market innovation)



Generative AI-Driven capabilities for data protection

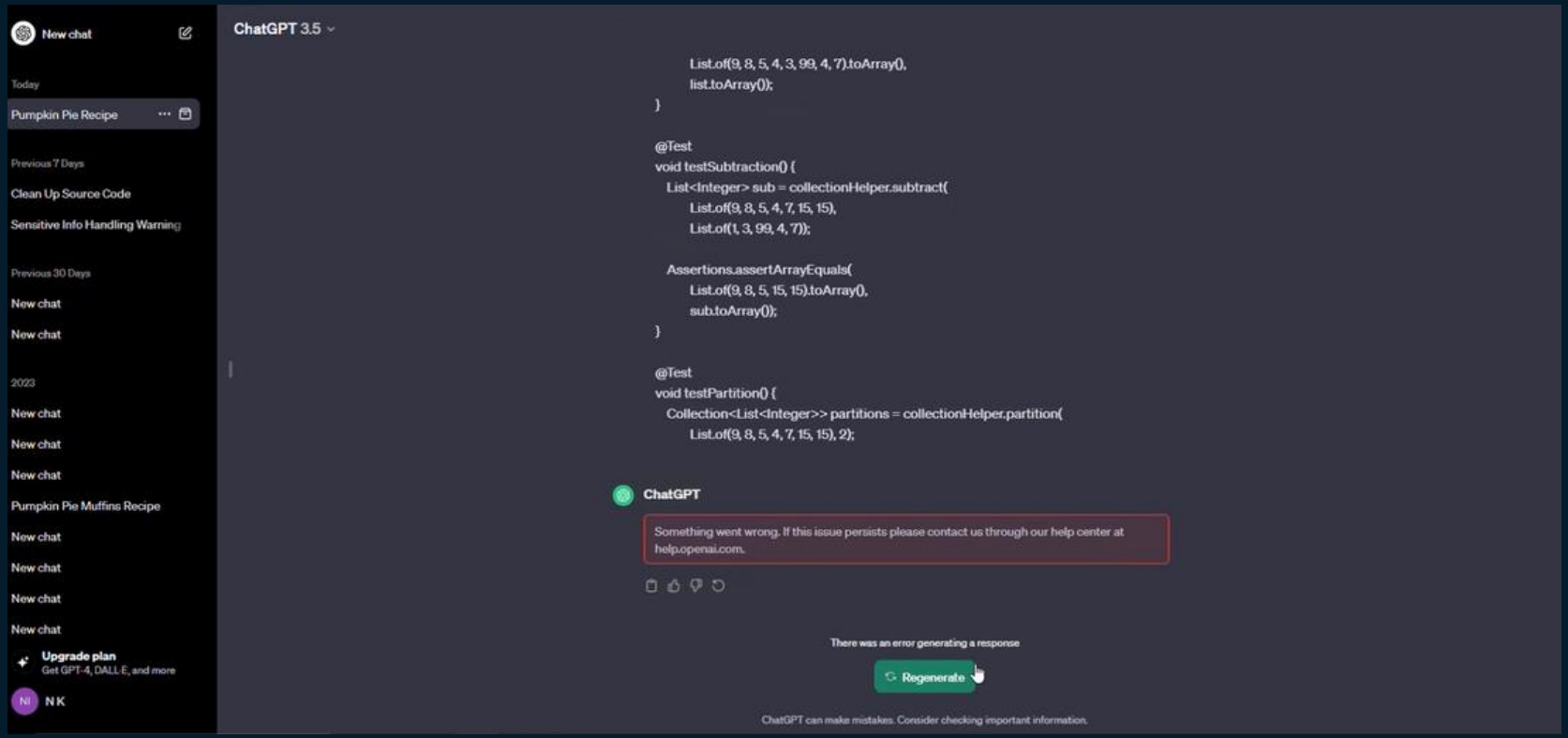
(first-to-market innovation)



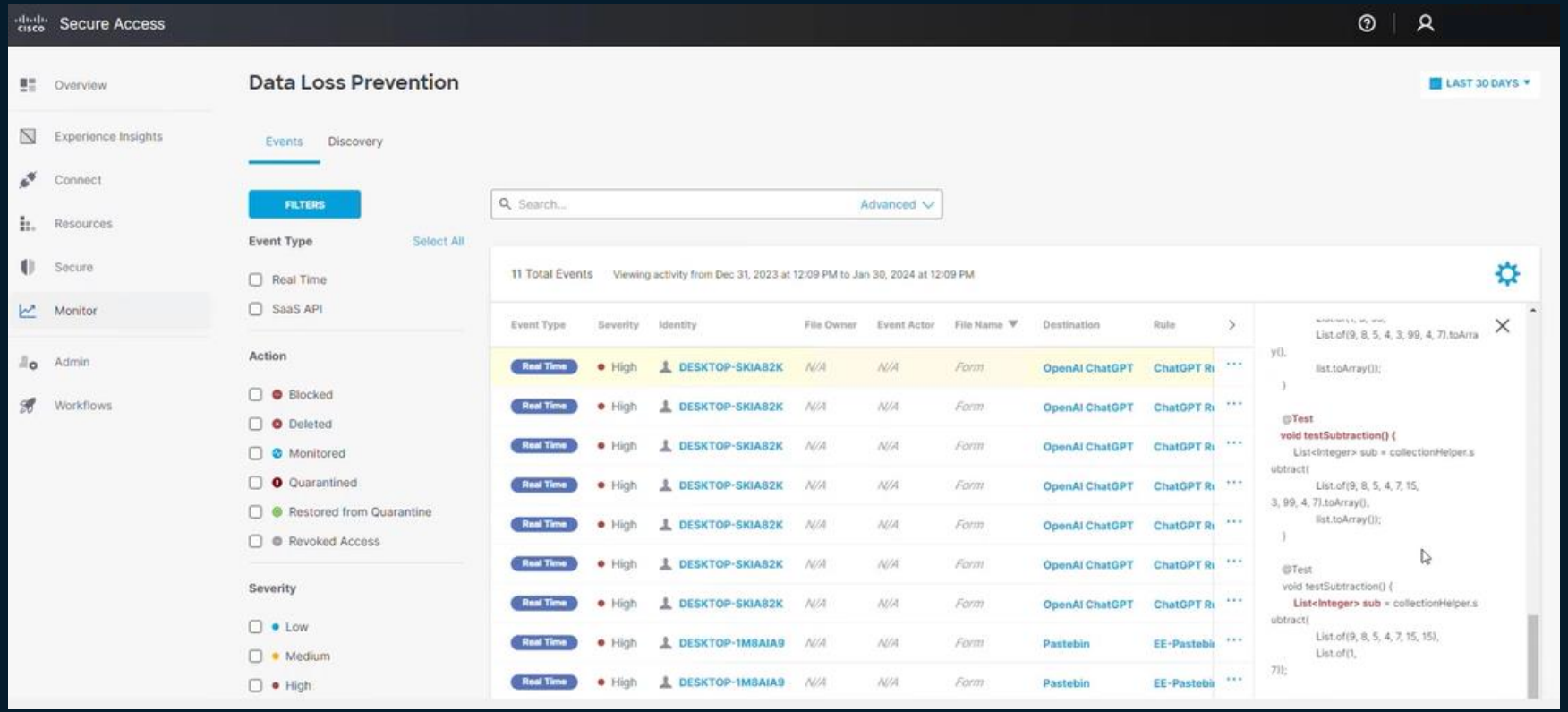
Demo:

Blocking data leakage into ChatGPT (Security for AI)

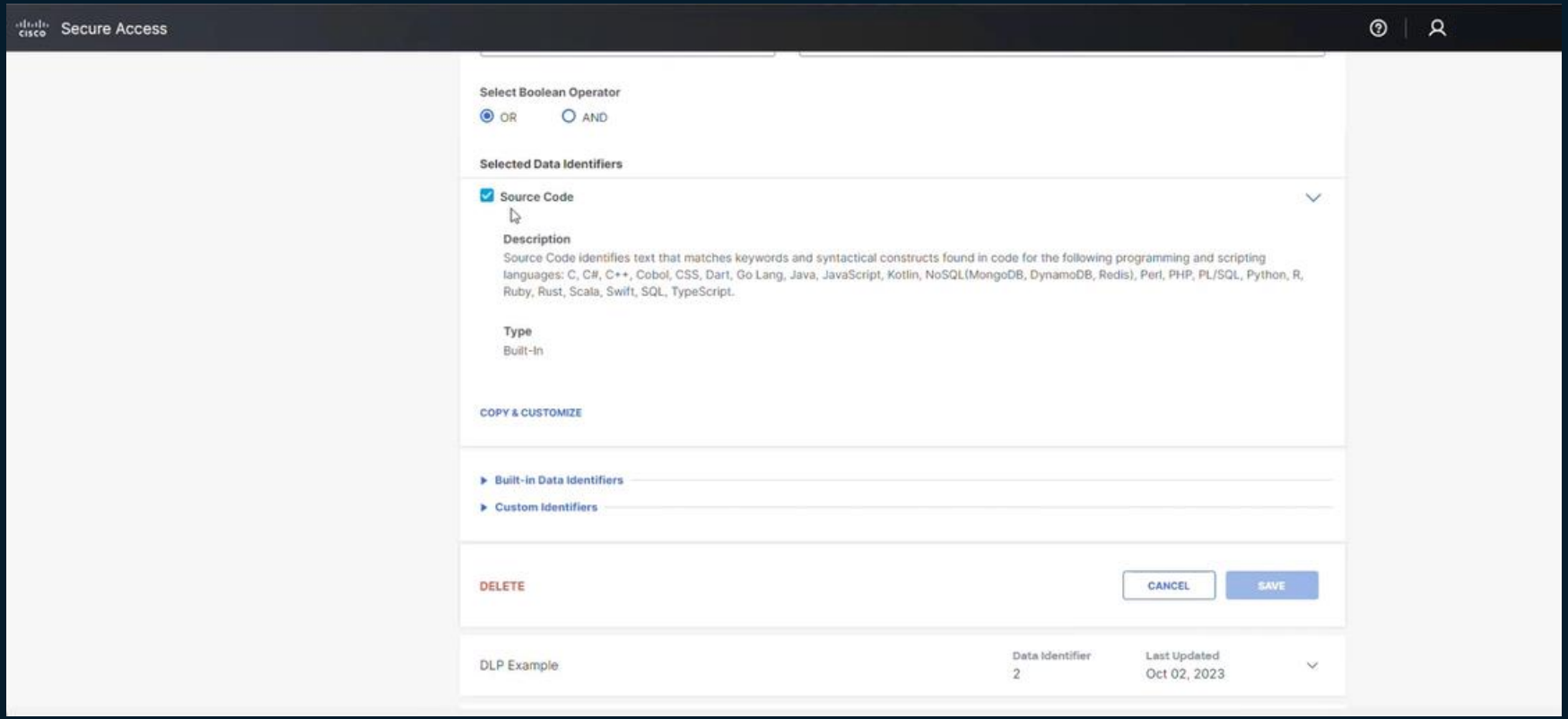
Demo reminder: Security for AI



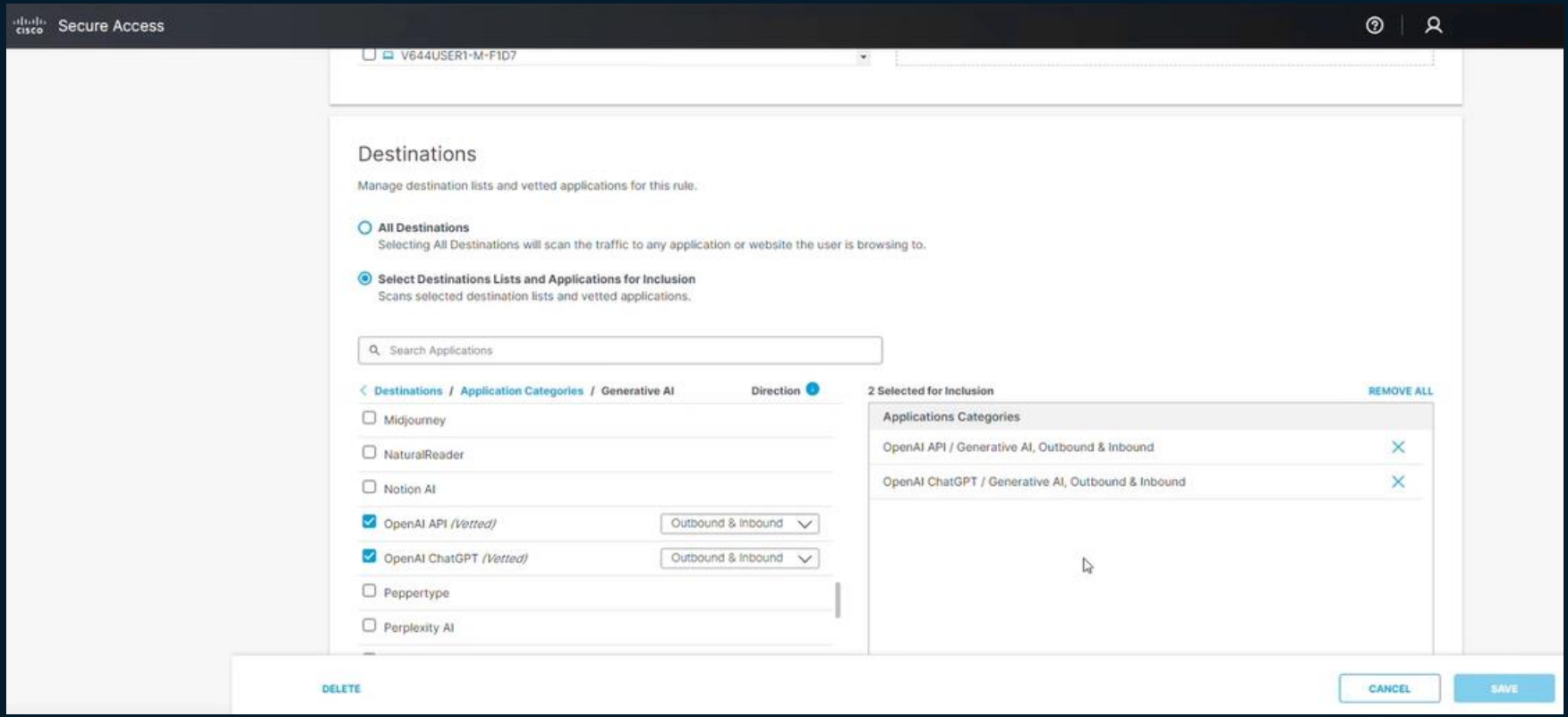
Demo reminder: Security for AI



Demo reminder: Security for AI



Demo reminder: Security for AI



slido

Which of the following statements are TRUE? (multiple)

ⓘ Start presenting to display the poll results on this slide.

Summary and Call to Action

- Cisco Secure Access: Modern innovations for SSE to solve our customers' current and future use-cases
- Emphasis on simplicity, future-proof cloud architecture to ensure scale, performance, reliability
- Integration of technologies under single dashboard, management through single policy, and simple transparent licensing
- Not the first to market, but researched 2+ years to address pain points customers have with other SSE solutions

- Remember, the early bird gets the worm, but...
  the second mouse gets the cheese!

Join our Security Research Community

Participating in design research gives you a place to share your thoughts and experiences to influence the future of Cisco Security Products.

cisco Live!

Webex App

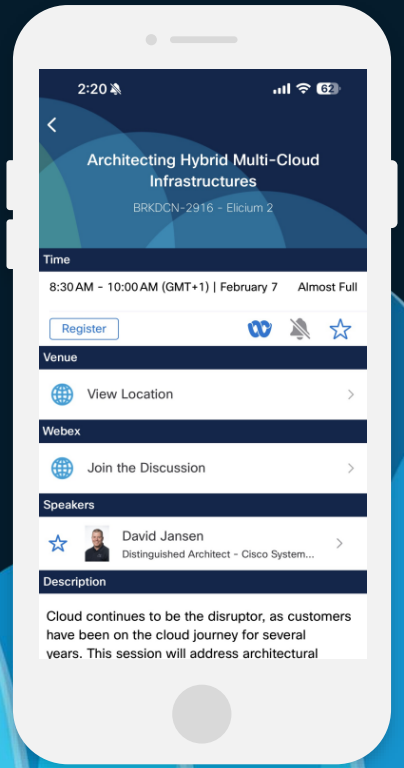
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.



Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

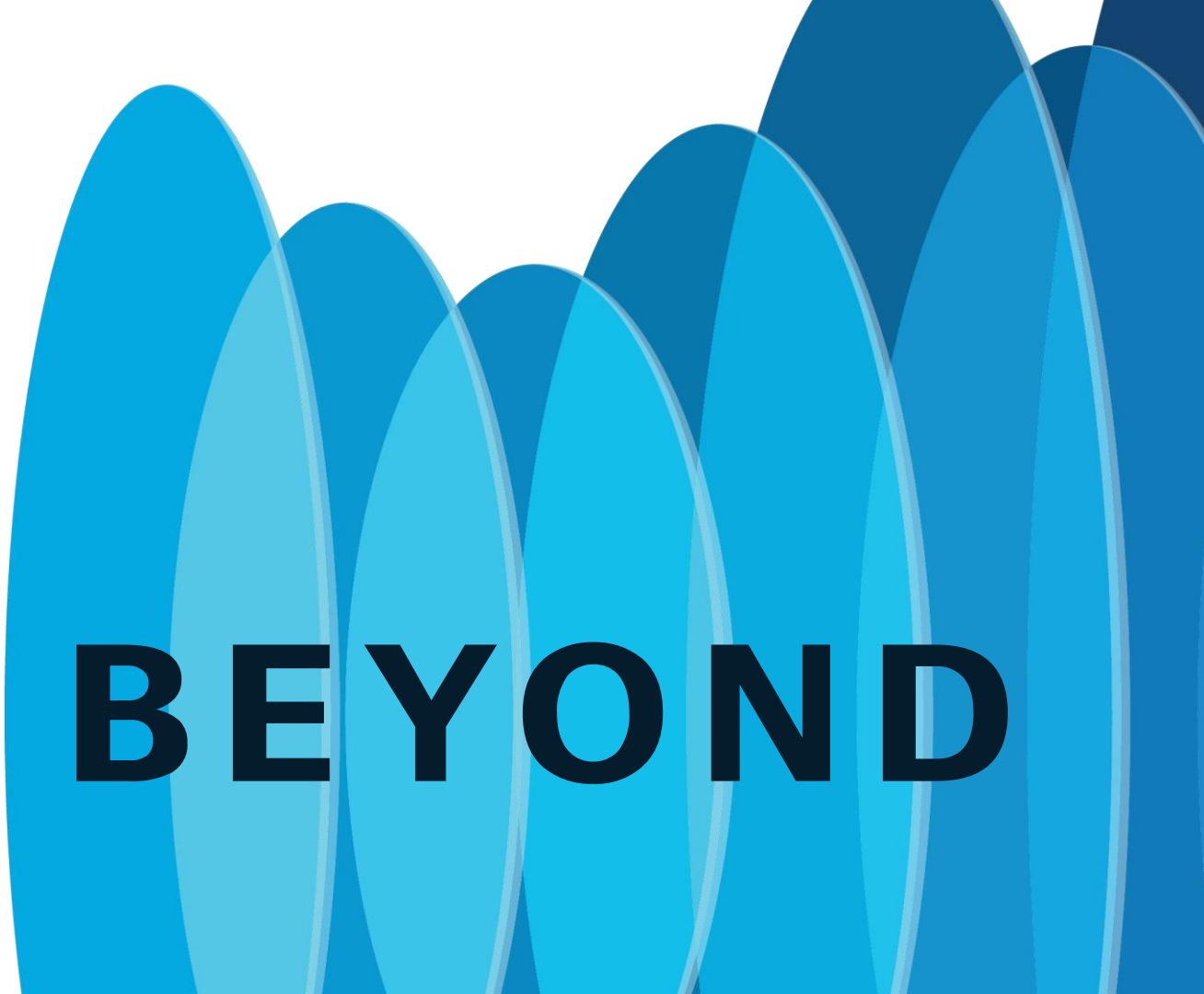
Content Catalog

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND