



# Cisco Secure Access

Stepping Behind the Curtain

Jonny Noble - Cloud Security Technical Marketing

@JonnyNoble3

BRKSEC-2438

CISCO *Live!*



# Webex App

## Questions?

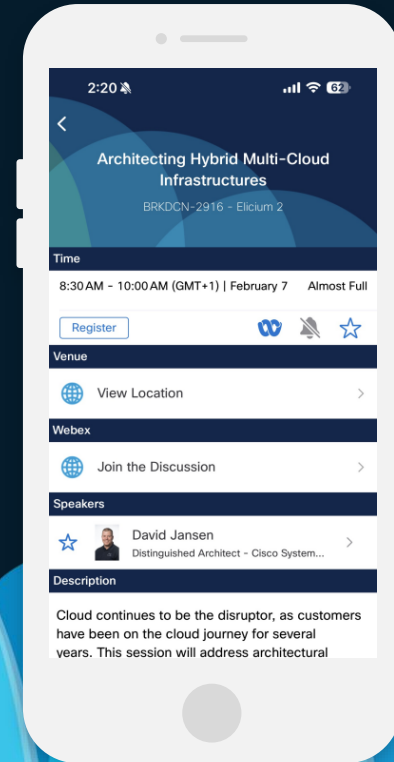
Use the Webex app to chat with the speaker after the session

## 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.

**CISCO** *Live!*



# 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



# When I'm not speaking at Cisco Live...



cisco *Live!*



# 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



# 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

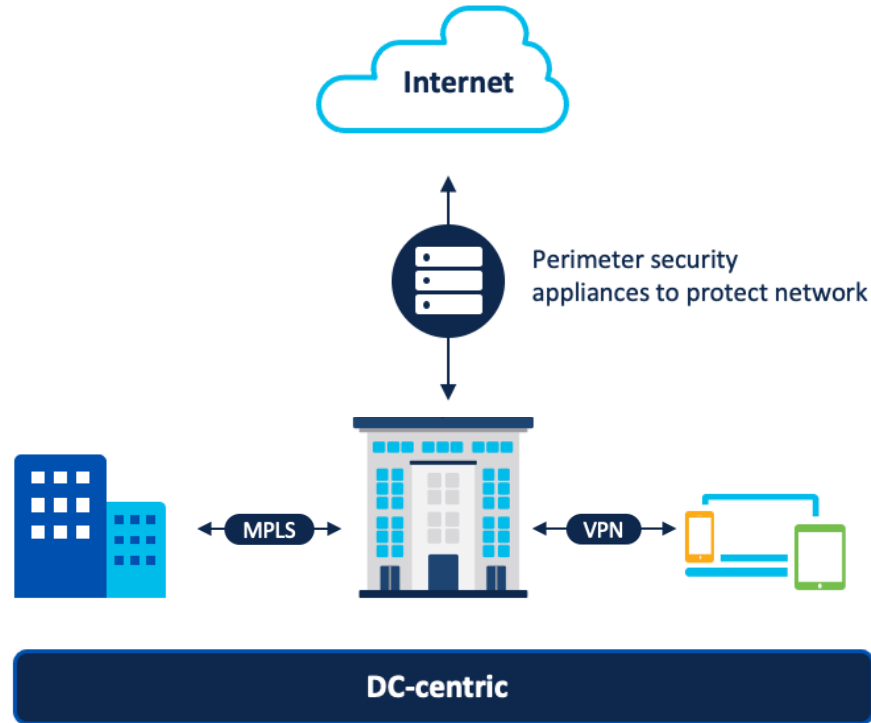
- Many insights learned over the last 8 years with Cisco Umbrella, which was originally designed for resolving DNS queries
- Highly optimal infrastructure today, totally redesigned from scratch
- Not only the infrastructure, but also the services running on it

- In this session we'll drill down on the infrastructure and services...  
  
...and see a few other cool innovations too!



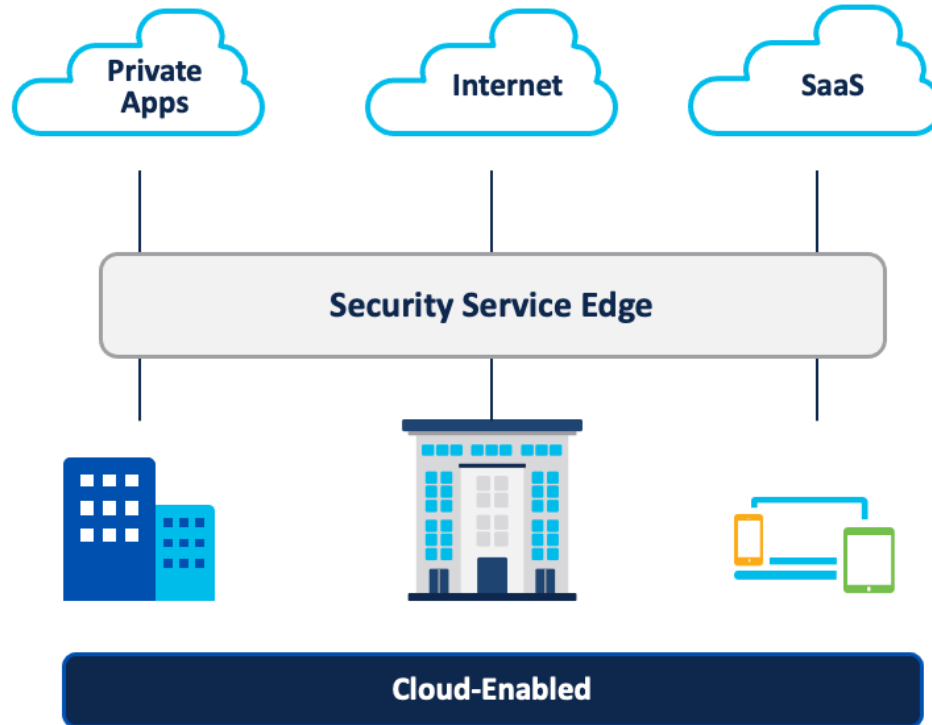
# Transformation

...of our infrastructure and platform



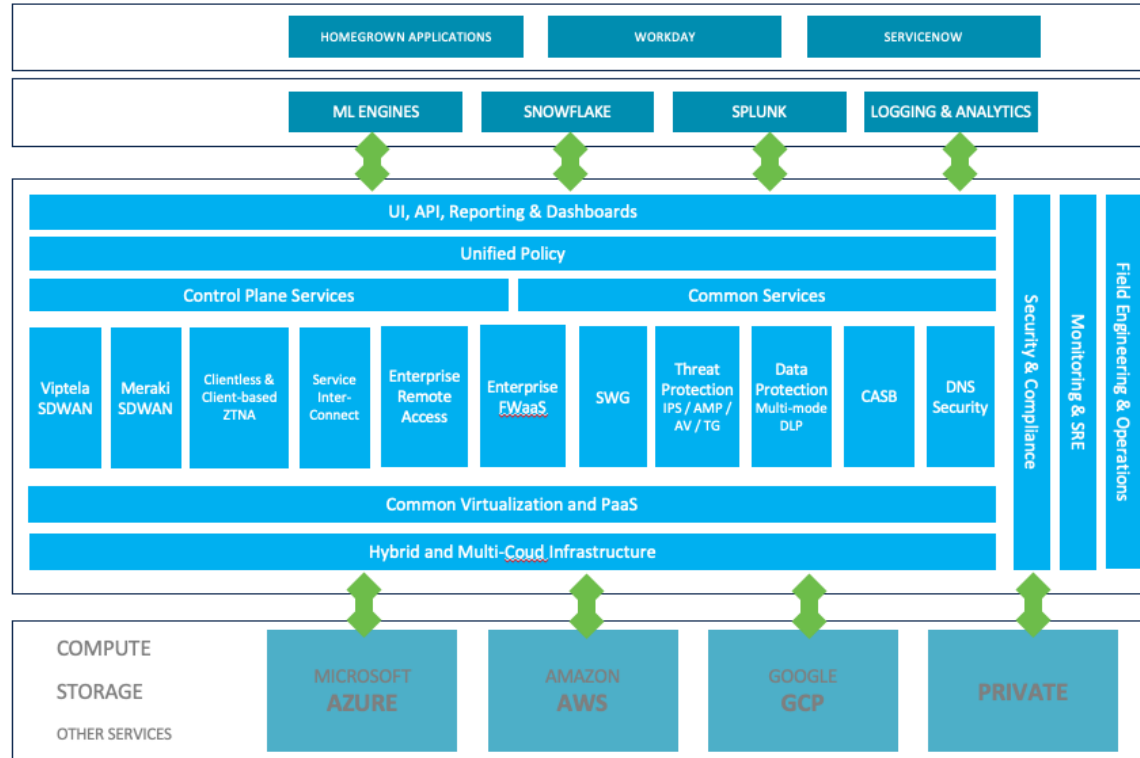
# Transformation

...of our infrastructure and platform



# Transformation

...of our product architecture



Secure Network as a Service

# Transformation

...of our customers' admin and end-user experience

The screenshot shows the Cisco Secure Access admin console. The left sidebar contains navigation options: Overview, Experience Insights, Connect, Resources, Secure (highlighted), Monitor, Admin, and Workflows. The main content area is titled 'Edit Client-based Posture Profile' and includes a description: 'Specify requirements for endpoint devices to connect to private resources. These requirements apply to devices on which the SSE Client is installed. Each requirement is optional. Requirements can be configured in any order. Endpoints must meet all configured requirements. Help'. Below this is a 'Name' field with the value 'System provided (Client-based)'. A list of requirements is shown on the left, each with a checkmark: Operating System (Windows and Mac OS X allowed), Firewall (Require for Windows and Mac OS X), Endpoint security agents (Require for Windows and Mac OS X), System password (Require for Windows and Mac OS X), and Disk encryption (Require for Windows and Mac OS X). The 'Firewall' section is expanded, showing 'Operating systems requiring firewall' with 'Windows' and 'Mac OS X' selected. Below this, there are instructions for Windows and Mac OS X: 'Require the platform-native firewall to be running on the endpoint.' At the bottom of the configuration page are 'Cancel', 'Save and Exit', and 'Next' buttons.

The notification dialog box has the Cisco logo and 'Cisco Secure Access' at the top. It features a red hexagonal icon with a white exclamation mark. The main heading is 'Firewall is turned off'. Below the heading, the text reads: 'Your organization requires this device's firewall to be turned on.' A prominent blue button with white text says 'How to turn on Firewall?'. At the bottom, there is a blue link that says 'I've turned on Firewall'.

# Transformation

...of our software delivery systems

Code development, unit testing, functional testing

Dev environment, local integration test, peer review, merge

Staging in 100% prod-like environment, automated E2E integration/  
regression/performance testing for minimum time

Pre-production roll-out

Production roll-out waves

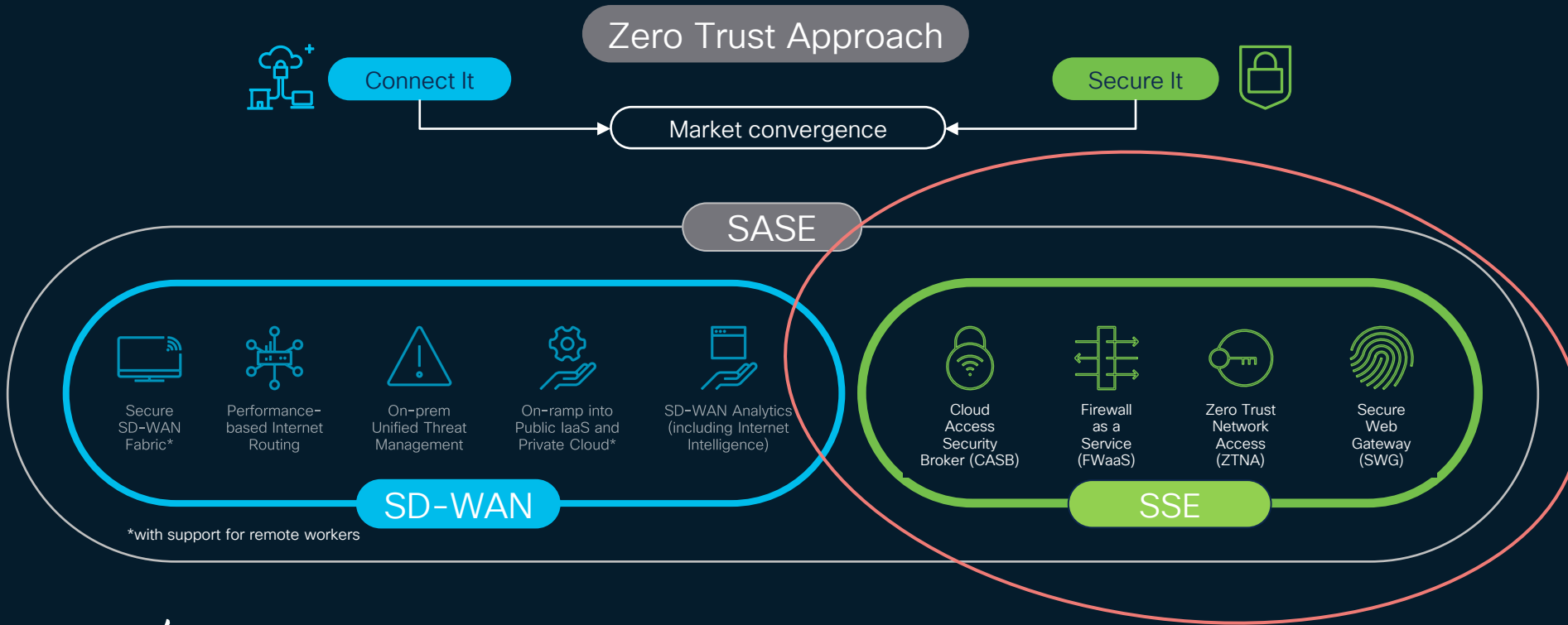
Result:

# 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
- 3<sup>rd</sup> 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



Which ONE of the following statements is TRUE?

① 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

Cisco Secure Access

To anything



Remote users



Managed and unmanaged devices

Better for Users

Exceptional User Experience

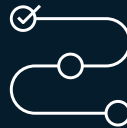


Users Login and get to work



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



Web



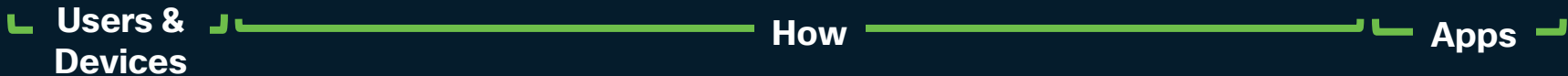
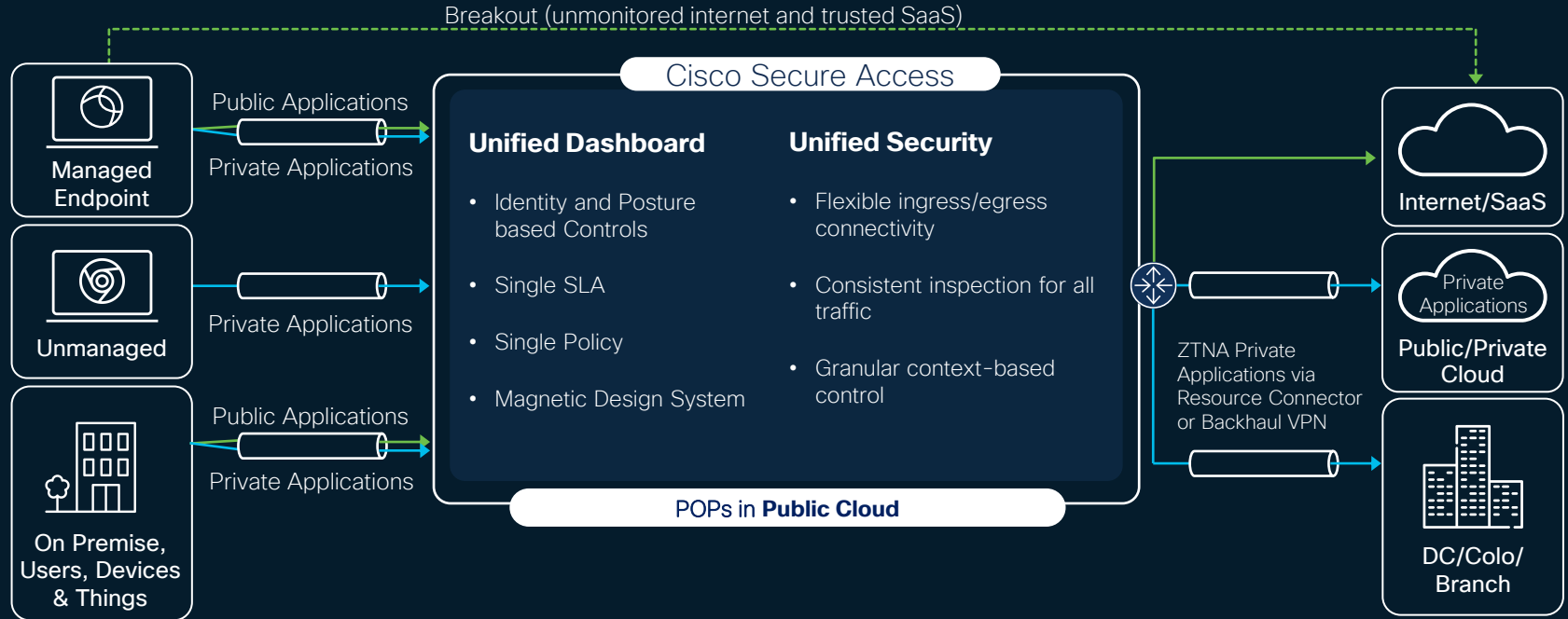
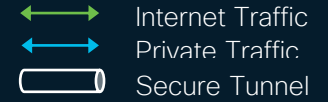
Public SaaS apps



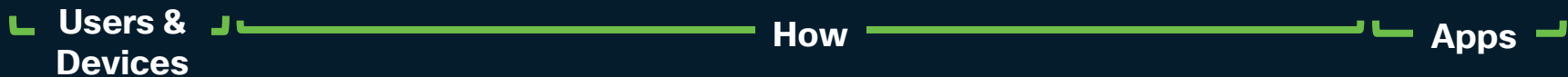
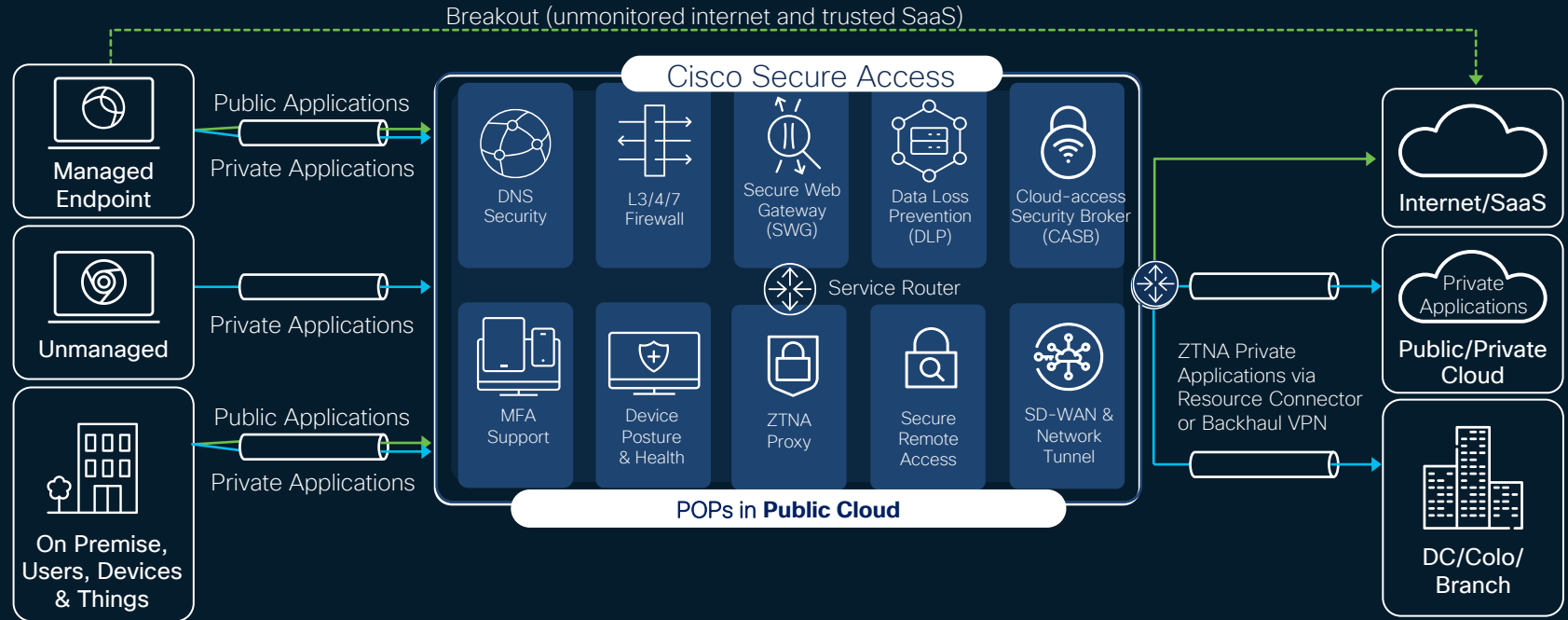
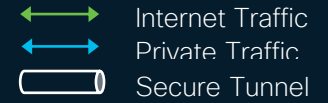
Private apps

Converged cloud-native security on a single platform

# Full architecture

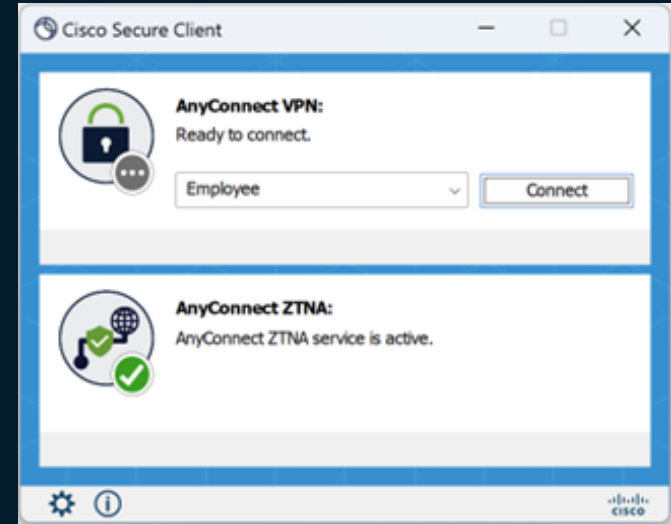


# Full architecture – Security stack



# 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



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

① Start presenting to display the poll results on this slide.

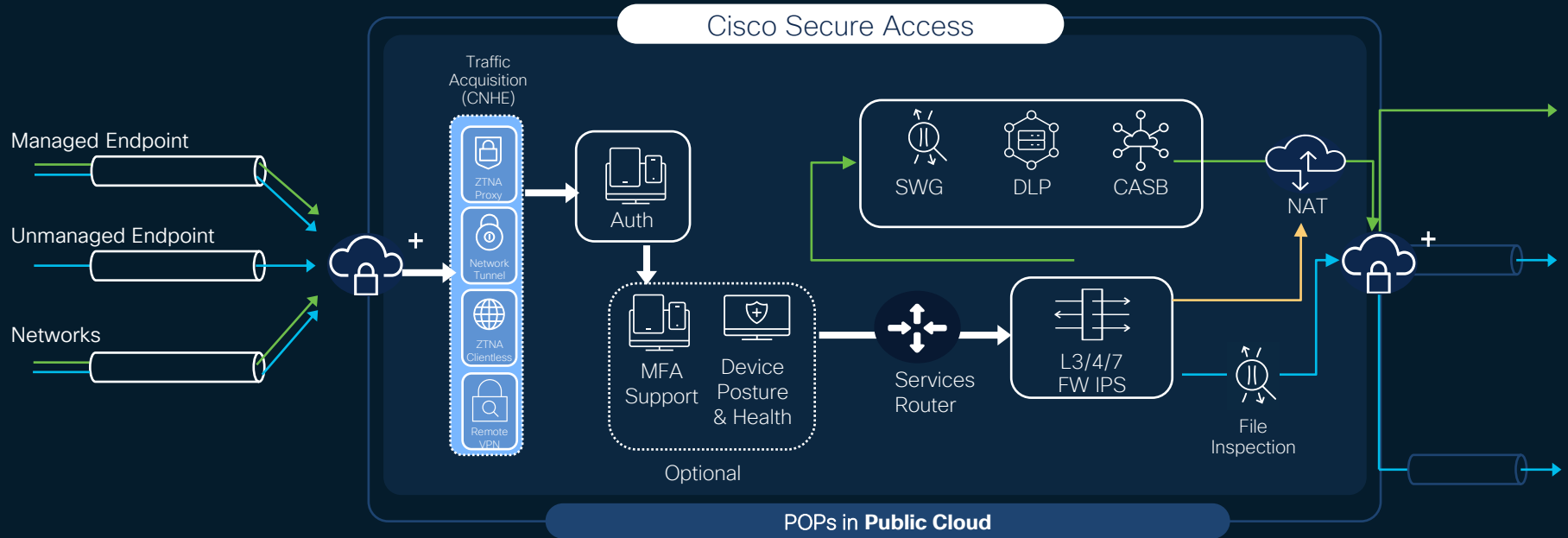
# Cloud Architecture Deep Dive

CISCO *Live!*



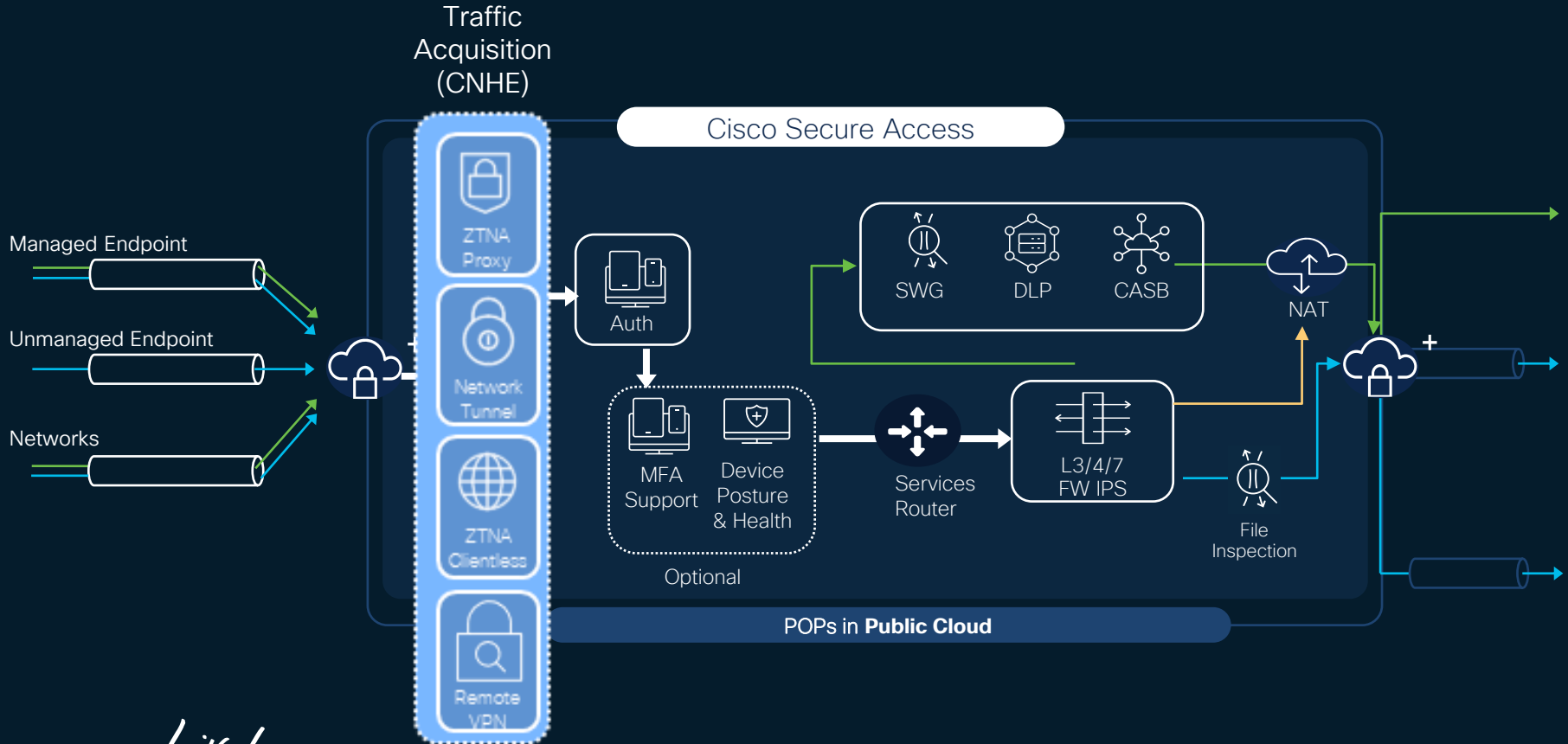
# Traffic flow

- ↔ Internet Traffic
- ↔ Private Traffic
- ↔ Non-Web Traffic



# Traffic flow

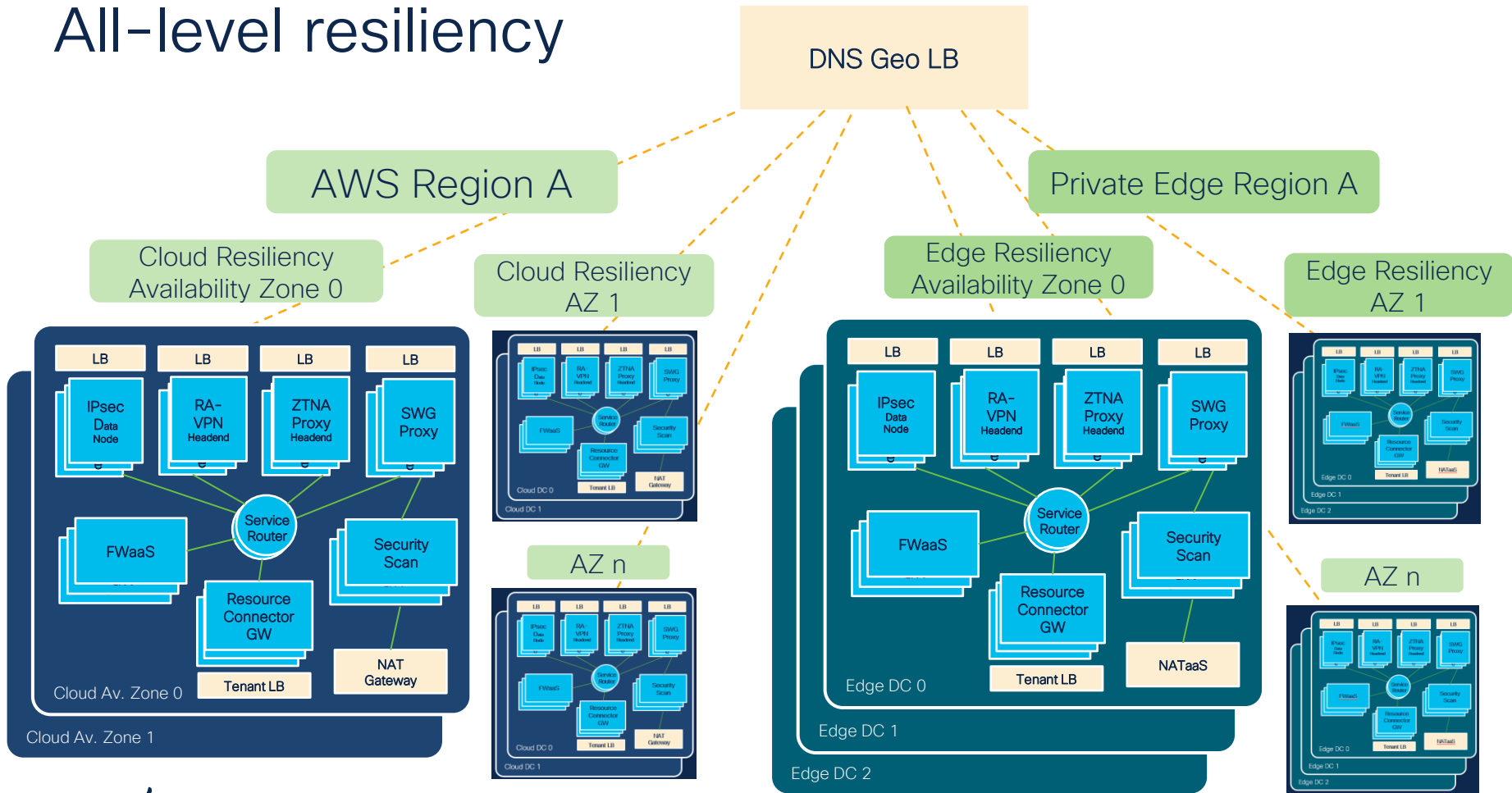
- ↔ Internet Traffic
- ↔ Private Traffic
- ↔ Non-Web Traffic



# Supported use-cases

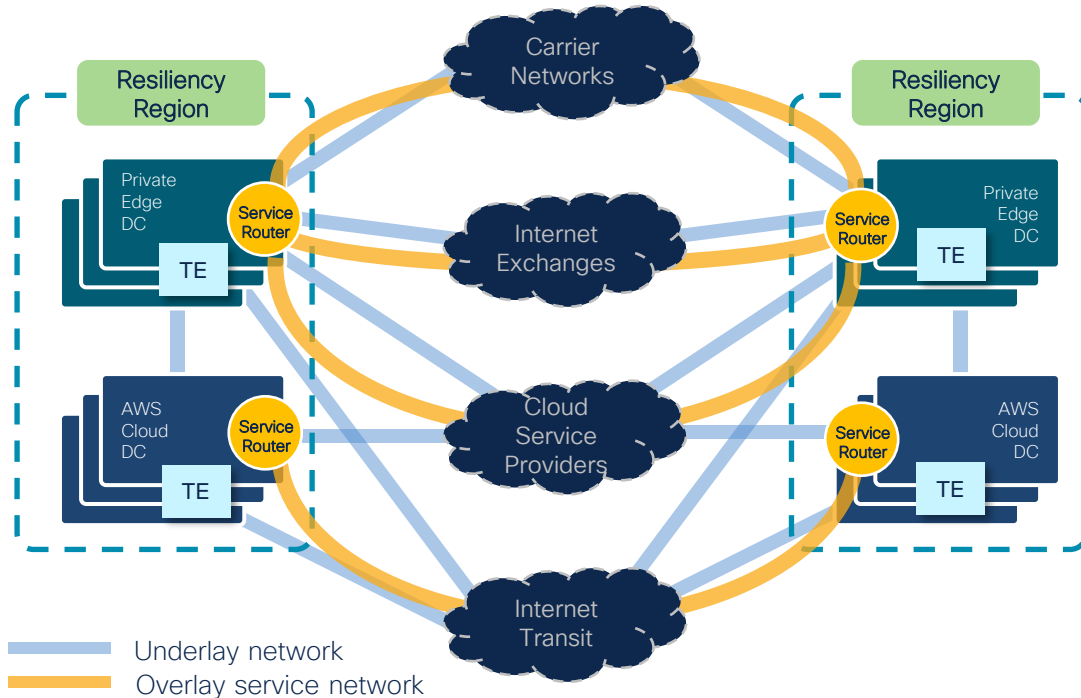
1. DNS security
2. Branch to internet
3. Branch to branch
4. RAVPN user to internet
5. RAVPN user to branch/private app
6. Client-based ZTNA to private app via S2S VPN
7. Clientless ZTNA to private app via S2S VPN
8. SWG roaming user to internet
9. RAVPN user to RAVPN user
10. Branch user to RAVPN user
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

- Passive user identity
- User group
- Geo location
- Out-of-band SGT
- Device posture

- Application ID (from L4, TLS cert, L7 header)
- File type
- URL category
- Malware category
- Authenticated user ID

- AMP verdict
- Malware verdict
- Antivirus verdict
- URL reputation verdict
- DLP verdict

← Derived metadata →

# Proven security capabilities converged in one cloud service



# Secure access regions – AWS coverage



## Legend

- Available
- By Request

# 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!*

A series of overlapping, rounded, teardrop-shaped abstract elements in various shades of blue, ranging from light to dark, positioned in the bottom right corner of the slide.

# 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

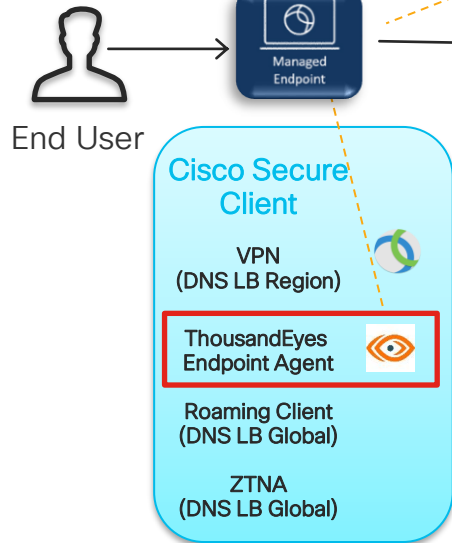


- **ThousandEyes** provides the foundational functionality for the first iteration of this feature space
- ThousandEyes EndPoint Agents (EPA) is installed as a module under Cisco Secure Client, to obtain end-user metrics
  - Provides automated collection of key metrics, vital in identifying device's 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

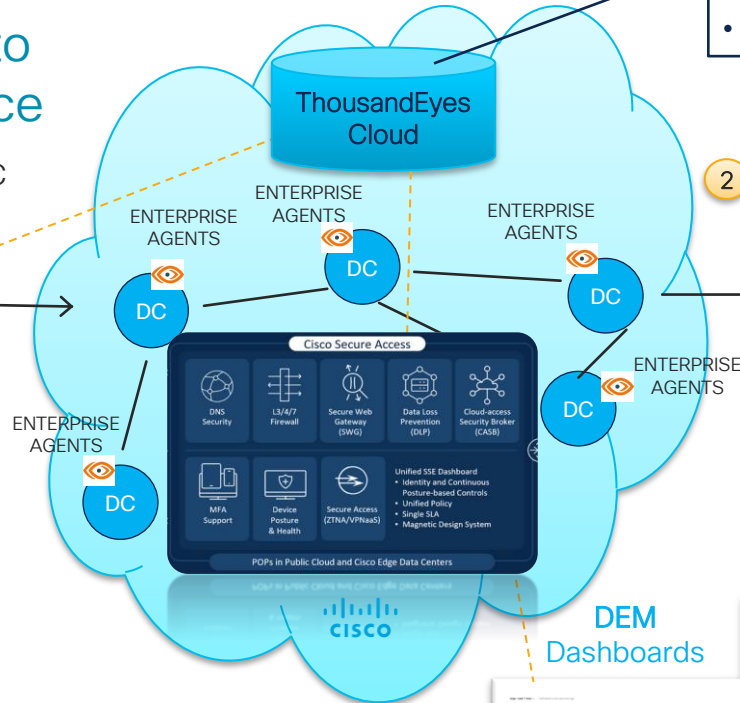
# Experience Insights architecture

## Customer Endpoint to Cisco DC Performance

1 Remote User to DC Performance



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



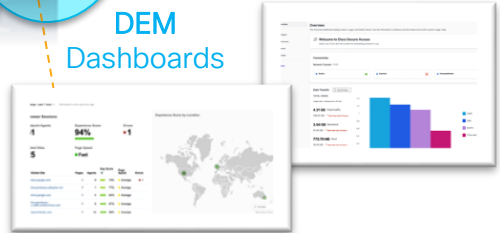
2 DC to SaaS App Performance Monitoring

## DC to Apps Performance



SaaS apps

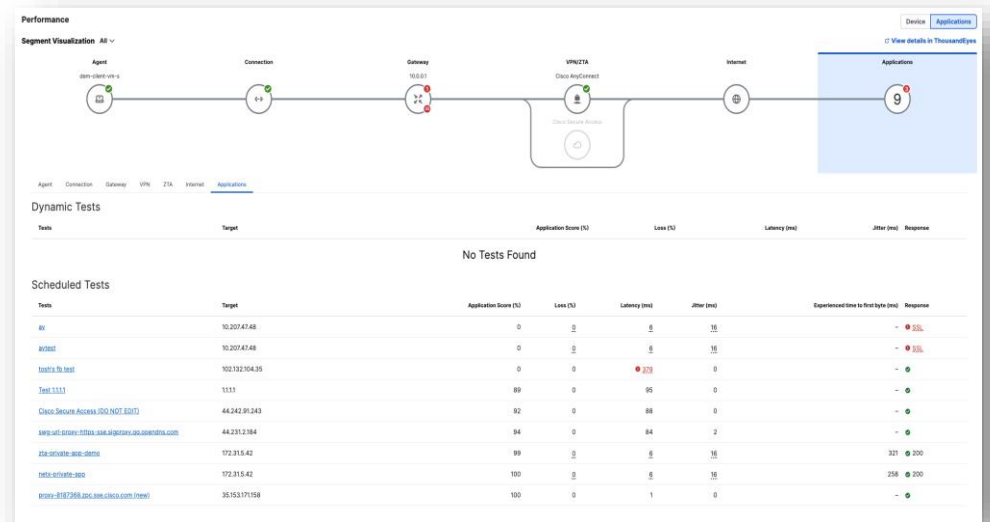
Source	Application	URL	Client	Response Time (s)	Status
✓	sales	www.sales.com	124 ms	200	
✓	bing	www.bing.com	82 ms	200	
✓	sales	www.sales.com	82 ms	200	
✓	salesforce	login.salesforce.com	55 ms	200	
✓	cloudgate	www.cloudgate.com	114 ms	200	
✓	amazon	www.amazon.com	107 ms	200	



*cisco Live!*

# DEM: End-to-End Network and HTTP Tests

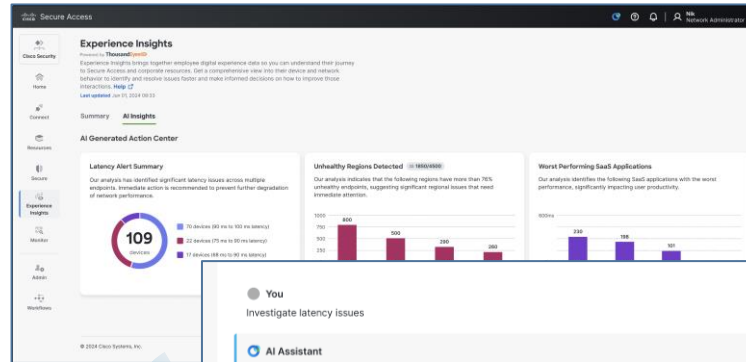
- Create network or http tests to public or private resources to monitor data path
- Segment visualization with per hop view to the performance
- Requires ThousandEyes Essentials or Advantage license
- Available in Secure Access dashboard without cross-launch



# 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



**You**  
Investigate latency issues

**AI Assistant** 11:05 am  
A number of devices with high latency have been detected in the same region in the last 5 hours.

**Here's the breakdown: San Jose, CA has 70 devices with latency between 90ms to 100ms - last 5 hours.**

**Common factor:** the use of the same SSID across all affected devices. Specifically, devices connected to the SSID "Office\_Network" are experiencing high latency.

**Operating systems:** 30% of affected devices are running macOS 11.5.6, and 70% are running Microsoft Windows 11 Enterprise.

**Recommendations**  
[Tell me how to verify SSID configuration](#) [Channel and frequency optimization](#)

**You**  
Tell me how to verify SSID configuration

**AI Assistant** 11:05 am  
Here is how you can 'Verify SSID Configuration' on your router:

1. Access the network management console.
2. Review SSID settings for misconfigurations or issues.
3. Ensure that the SSID settings are optimized for performance.

**Other recommendations**  
[Channel and frequency optimization](#)

Message Cisco AI Assistant... [The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more.](#)

# Demo: Experience Insights

CISCO *Live!*



# Demo reminder: Experience Insights

**Experience Insights** Powered by ThousandEyes

By integrating with ThousandEyes technology, you can have a clear view of how well your users, applications, and networks are performing. Want to know more? [Launch ThousandEyes](#) to access detailed information, including a look back at historical data for various time periods. [Help](#)

[Learn updated](#) Jun 10, 2023 10:33

### Endpoints overview

**Endpoints** 1000 total

800  
Connected to the Cisco Secure Access cloud

### Performance health overview

100 Unhealthy ● 250 At risk ● 500 Healthy ● 50 Offline ●

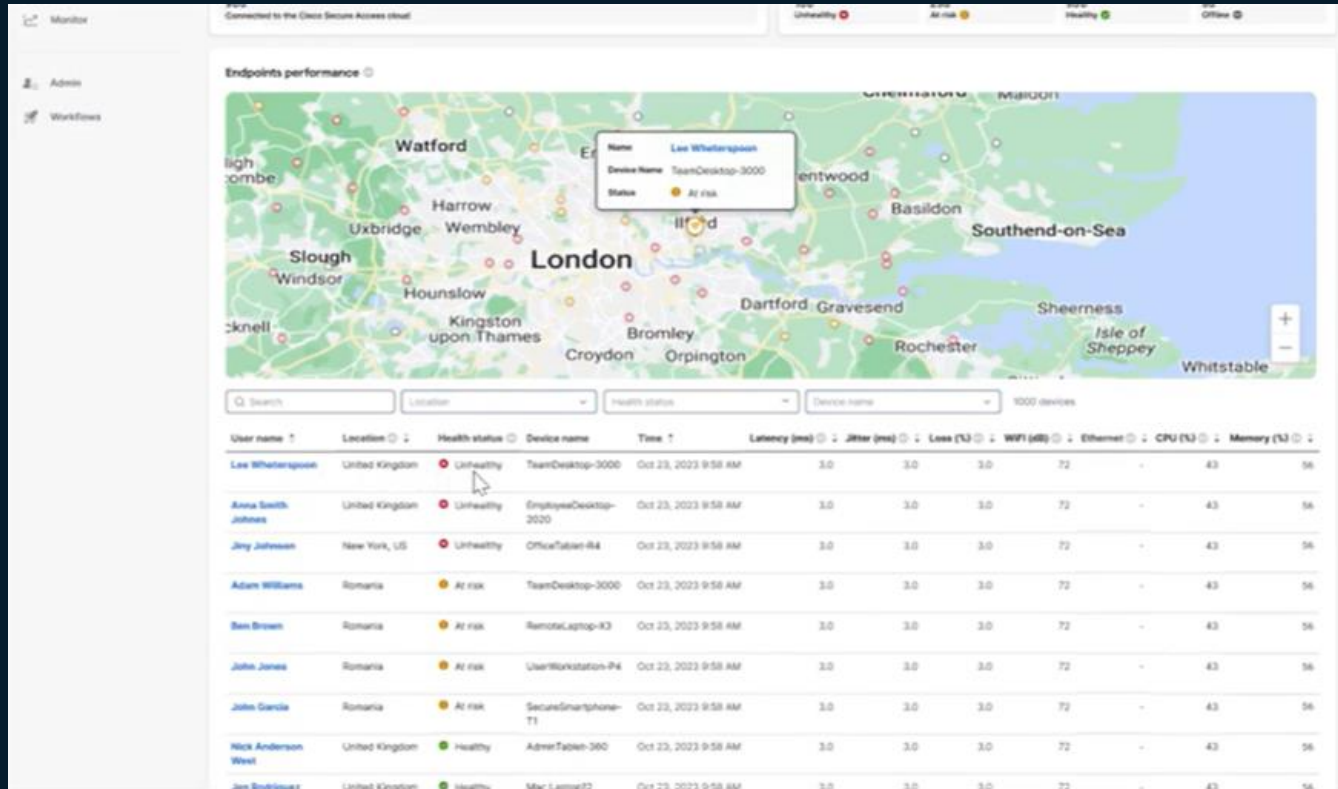
### Endpoints performance

Map showing device locations across North America and Europe.

Search: [ ] Location: [ ] Health status: [ ] Device name: [ ] 1000 devices

User name	Location	Health status	Device name	Time	Latency (ms)	Jitter (ms)	Loss (%)	WiFi (dB)	Ethernet	CPU (%)	Memory (%)
Lee Whelan@psop	United Kingdom	Unhealthy	TeamDesktop-2000	Oct 23, 2023 9:58 AM	3.0	3.0	3.0	72	-	43	56
Anna Smith	United Kingdom	Unhealthy	TeamDesktop-2000	Oct 23, 2023 9:58 AM	3.0	3.0	3.0	72	-	43	56

# Demo reminder: Experience Insights



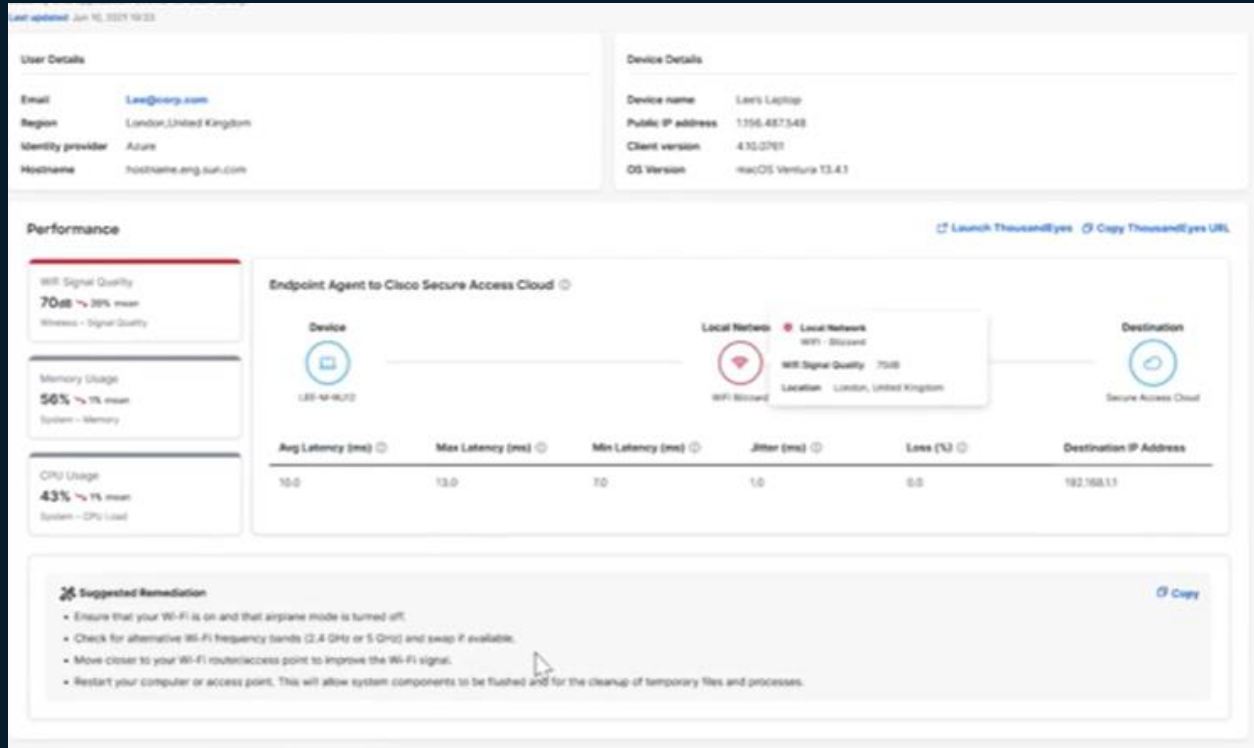
# Demo reminder: Experience Insights

Common SaaS applications performance

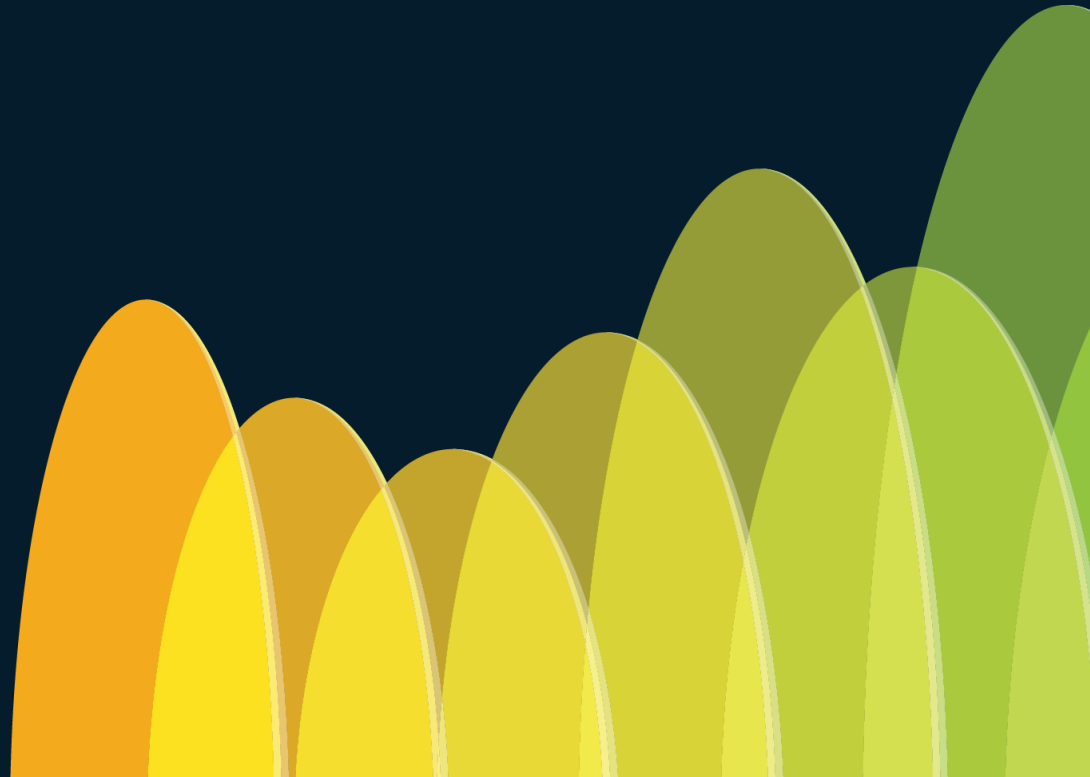
Search Location Status 20 applications [Reset all](#)

Status	Application	URL (domain)	Response time	Response code	Description	Time	Location
●	Mail	mail.com	14.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Outlook	outlook.com	12.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Miss	miss.com	13.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Slack	slack.com	11.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Gmail	gmail.com	9.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Salesforce	salesforce.com	8.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Box	box.com	7.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Figma	figma.com	6.0 ms	502	Bad gateway	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Notion	notion.com	8.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Google Workspace	workspace.google.com	8.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Microsoft Office	office.com	10.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Trello	trello.com	11.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Asana	asana.com	12.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	InsideSales.com	insidesales.com	13.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	LinkedIn Sales	linkedin.com	14.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	DocuSign	docuSign.com	15.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	PandaDoc	pandadoc.com	16.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Clari	clari.com	13.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	HubSpot	hubspot.com	12.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)
●	Sharepoint	sharepoint.com	5.0 ms	200	OK	Oct 23, 2023 9:58 AM	US (Pacific Northwest)

# Demo reminder: Experience Insights



# AI for Security; Security for AI



# Unified, single, intent-based policy

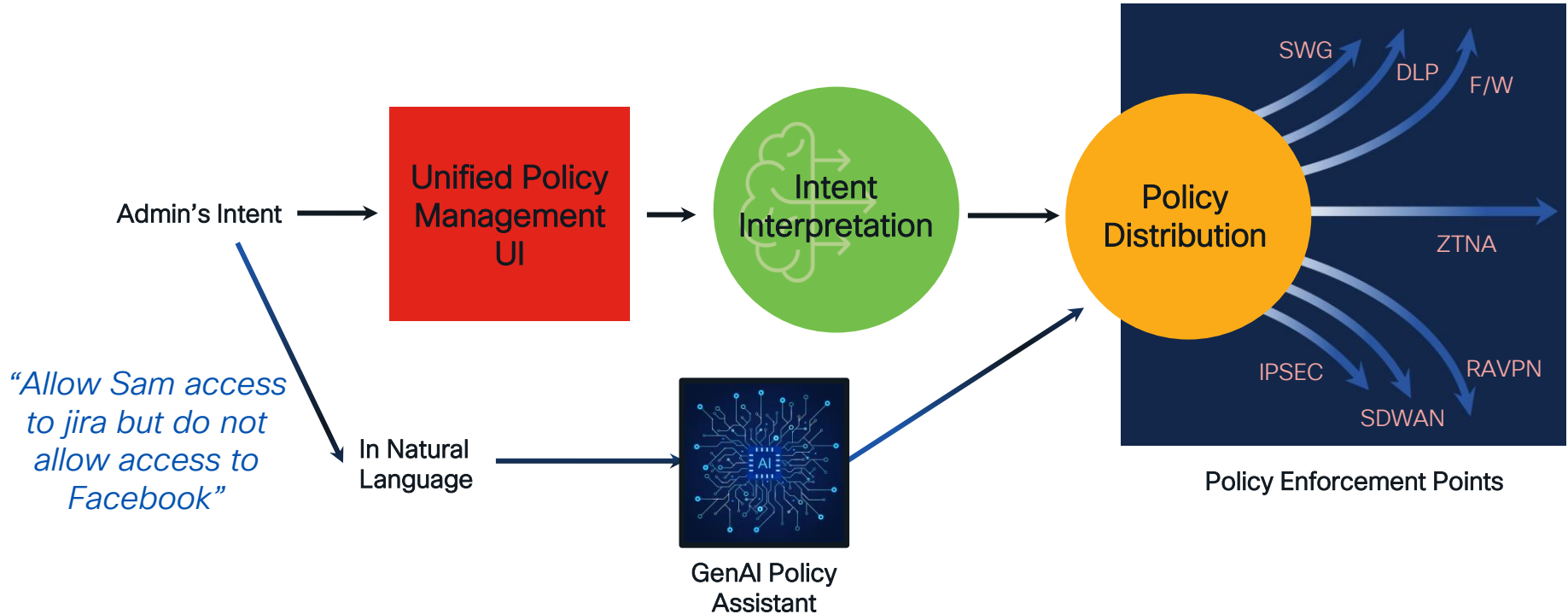
- Based on the “what”, not the “how”
  - Allow Sam access to Jira, but not to Facebook
  - No mention of Firewall or SWG, only what to allow and deny

The screenshot displays the Cisco Secure Access interface for configuring Access Policies. The page title is 'Access Policy' and it includes a search bar and filters for 'Intent' and 'Objects'. Below the search bar, there is a table listing 12 rules. The table columns are: #, Rule name, Rule type, Action, Sources, Destinations, Security Control, and Status. The rules are as follows:

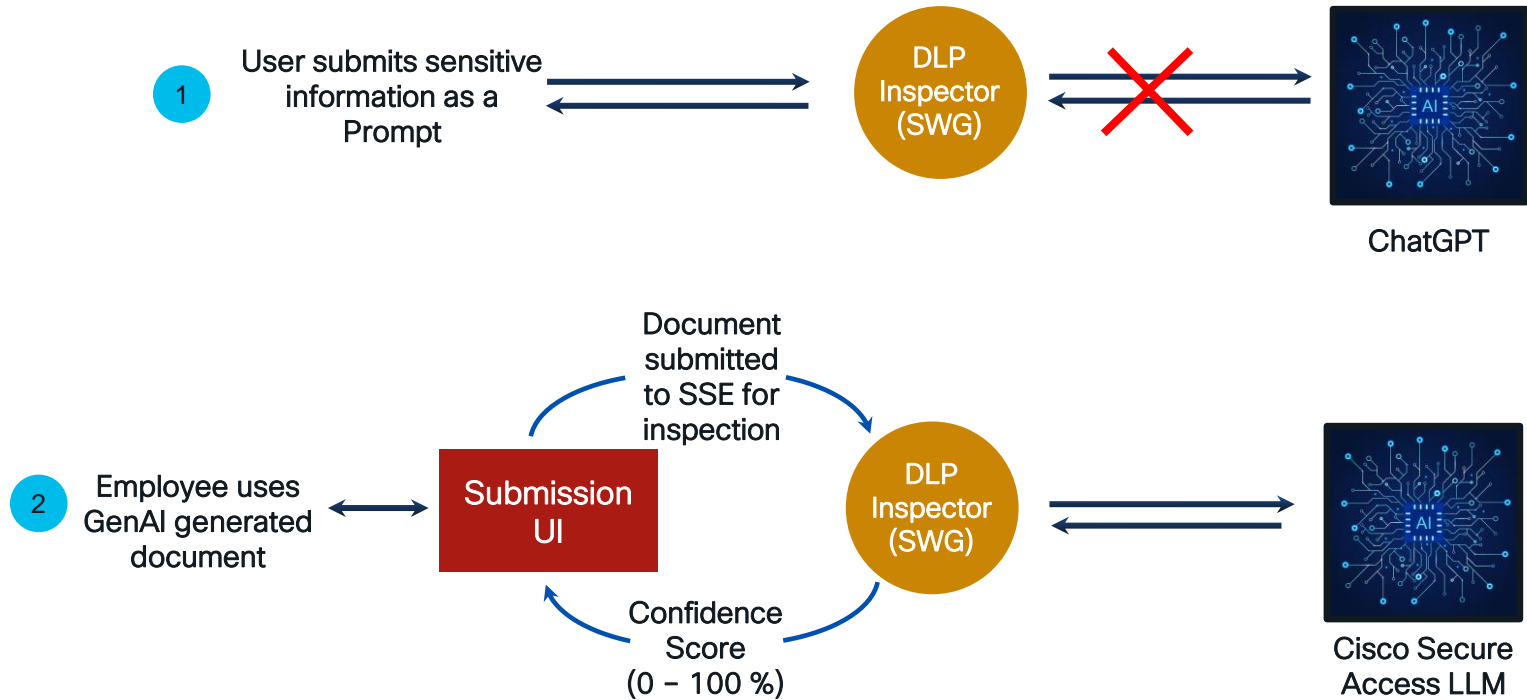
#	Rule name	Rule type	Action	Sources	Destinations	Security Control	Status
1	Engineers	Private Access	Allow	lma (lma@tmelabs.com) +1	Jira +2	IPS	Enabled
2	OPEN-ACCESS	Private Access	Allow	Any	Any private application	IPS	Enabled
3	Block Gambling	Internet Access	Block	Any	Gambling	Web	Disabled
4	Block Gambling (Copy 1)	Internet Access	Block	Any	Gambling	Web	Disabled
5	Code Server	Private Access	Allow	lma (lma@tmelabs.com)	VSCoDe-Server	IPS	Enabled
6	New Rule 5	Private Access	Allow	Any	Any private application	-	Disabled

# 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)

CISCO *Live!*



# Demo reminder: Security for AI

The screenshot shows a ChatGPT chat window with a dark theme. On the left is a sidebar with a 'New chat' button and a list of previous chats. The main chat area shows a code snippet in Java. Below the code, the ChatGPT response is an error message: 'Something went wrong. If this issue persists please contact us through our help center at help.openai.com.' Below the error message are icons for copy, thumbs up, thumbs down, and refresh. At the bottom, there is a message 'There was an error generating a response' and a 'Regenerate' button. A footer note states 'ChatGPT can make mistakes. Consider checking important information.'

```
ListOf(9, 8, 5, 4, 3, 99, 4, 7).toArray(),
list.toArray());
}

@Test
void testSubtraction() {
    List<Integer> sub = collectionHelper.subtract(
        ListOf(9, 8, 5, 4, 7, 15, 15),
        ListOf(1, 3, 99, 4, 7));

    Assertions.assertArrayEquals(
        ListOf(9, 8, 5, 15, 15).toArray(),
        sub.toArray());
}

@Test
void testPartition() {
    Collection<List<Integer>> partitions = collectionHelper.partition(
        ListOf(9, 8, 5, 4, 7, 15, 15), 2);
```

ChatGPT

Something went wrong. If this issue persists please contact us through our help center at [help.openai.com](https://help.openai.com).

There was an error generating a response

Regenerate

ChatGPT can make mistakes. Consider checking important information.

# Demo reminder: Security for AI

The screenshot displays the Cisco Secure Access Data Loss Prevention (DLP) interface. The left sidebar contains navigation options: Overview, Experience Insights, Connect, Resources, Secure, Monitor, Admin, and Workflows. The main area is titled "Data Loss Prevention" and includes tabs for "Events" and "Discovery". A search bar and "Advanced" filter options are present. The "Event Type" section has checkboxes for "Real Time" and "SaaS API". The "Action" section includes checkboxes for "Blocked", "Deleted", "Monitored", "Quarantined", "Restored from Quarantine", and "Revoked Access". The "Severity" section has checkboxes for "Low", "Medium", and "High".

The central table displays 11 total events, showing activity from Dec 31, 2023, to Jan 30, 2024. The table columns are: Event Type, Severity, Identity, File Owner, Event Actor, File Name, Destination, and Rule. The events listed are:

Event Type	Severity	Identity	File Owner	Event Actor	File Name	Destination	Rule
Real Time	High	DESKTOP-SKIA82K	N/A	N/A	Form	OpenAI ChatGPT	ChatGPT Ri
Real Time	High	DESKTOP-SKIA82K	N/A	N/A	Form	OpenAI ChatGPT	ChatGPT Ri
Real Time	High	DESKTOP-SKIA82K	N/A	N/A	Form	OpenAI ChatGPT	ChatGPT Ri
Real Time	High	DESKTOP-SKIA82K	N/A	N/A	Form	OpenAI ChatGPT	ChatGPT Ri
Real Time	High	DESKTOP-SKIA82K	N/A	N/A	Form	OpenAI ChatGPT	ChatGPT Ri
Real Time	High	DESKTOP-SKIA82K	N/A	N/A	Form	OpenAI ChatGPT	ChatGPT Ri
Real Time	High	DESKTOP-SKIA82K	N/A	N/A	Form	OpenAI ChatGPT	ChatGPT Ri
Real Time	High	DESKTOP-SKIA82K	N/A	N/A	Form	OpenAI ChatGPT	ChatGPT Ri
Real Time	High	DESKTOP-1M8AIA9	N/A	N/A	Form	Pastebin	EE-Pastebin
Real Time	High	DESKTOP-1M8AIA9	N/A	N/A	Form	Pastebin	EE-Pastebin

On the right side, a code editor displays the following code snippet:

```
y().  
  List.of(9, 8, 5, 4, 3, 99, 4, 7).toArray  
)  
  listToArray();  
}  
  
@Test  
void testSubtraction() {  
  List<Integer> sub = collectionHelpers  
  subtract(  
    List.of(9, 8, 5, 4, 7, 15,  
3, 99, 4, 7).toArray(),  
    listToArray());  
}  
  
@Test  
void testSubtraction() {  
  List<Integer> sub = collectionHelpers  
  subtract(  
    List.of(9, 8, 5, 4, 7, 15, 15),  
    List.of(1,  
7));  
}
```

# Demo reminder: Security for AI

The screenshot shows the Cisco Secure Access configuration page for a Data Identifier. The interface includes a top navigation bar with the Cisco logo and 'Secure Access' text. The main content area is titled 'Select Boolean Operator' and shows 'OR' selected. Below this is the 'Selected Data Identifiers' section, which contains a single entry: 'Source Code'. The entry is expanded to show its description: 'Source Code identifies text that matches keywords and syntactical constructs found in code for the following programming and scripting languages: C, C#, C++, Cobol, CSS, Dart, Go Lang, Java, JavaScript, Kotlin, NoSQL(MongoDB, DynamoDB, Redis), Perl, PHP, PL/SQL, Python, R, Ruby, Rust, Scala, Swift, SQL, TypeScript.' The entry's type is listed as 'Built-In'. At the bottom of the configuration area, there are 'DELETE', 'CANCEL', and 'SAVE' buttons. Below the configuration area is a table with the following data:

DLP Example	Data Identifier	Last Updated
	2	Oct 02, 2023

# Demo reminder: Security for AI

The screenshot shows the Cisco Secure Access configuration page for rule V644USER1-M-F1D7. The 'Destinations' section is active, with the option 'Select Destinations Lists and Applications for Inclusion' chosen. Below this, a search bar is present. A list of applications is shown, with 'OpenAI API (Vetted)' and 'OpenAI ChatGPT (Vetted)' selected. To the right, a modal window titled '2 Selected for Inclusion' displays the selected categories: 'OpenAI API / Generative AI, Outbound & Inbound' and 'OpenAI ChatGPT / Generative AI, Outbound & Inbound'. At the bottom of the interface, there are 'DELETE', 'CANCEL', and 'SAVE' buttons.

**Destinations**  
Manage destination lists and vetted applications for this rule.

All Destinations  
Selecting All Destinations will scan the traffic to any application or website the user is browsing to.

Select Destinations Lists and Applications for Inclusion  
Scans selected destination lists and vetted applications.

Search Applications

[Destinations](#) / [Application Categories](#) / [Generative AI](#) Direction

<input type="checkbox"/> Midjourney	
<input type="checkbox"/> NaturalReader	
<input type="checkbox"/> Notion AI	
<input checked="" type="checkbox"/> OpenAI API (Vetted)	Outbound & Inbound
<input checked="" type="checkbox"/> OpenAI ChatGPT (Vetted)	Outbound & Inbound
<input type="checkbox"/> Peppertype	
<input type="checkbox"/> Perplexity AI	

2 Selected for Inclusion REMOVE ALL

Applications Categories	
OpenAI API / Generative AI, Outbound & Inbound	X
OpenAI ChatGPT / Generative AI, Outbound & Inbound	X

DELETE CANCEL SAVE



Which of the following statements are TRUE?  
(multiple)

① 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.



# Webex App

## Questions?

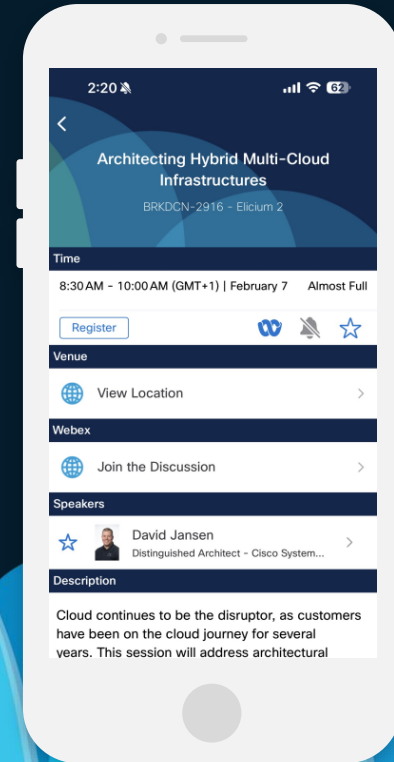
Use the Webex app to chat with the speaker after the session

## 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.

**CISCO** *Live!*



# 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](https://ciscolive.com/on-demand). Sessions from this event will be available from March 3.



Thank you

CISCO *Live!*

CISCO *Live!*

GO BEYOND

A series of overlapping, vertically-oriented ovals in various shades of blue, ranging from light to dark, positioned on the right side of the image.