

# Securing the New Era of AI-Powered Collaboration

Future-Proofed Workplaces – Session 4



Matt Klawiter et al.

March 2026

# Safe Harbor Statement

This presentation contains “forward-looking” statements that involve risks, uncertainties and assumptions. If the risks or uncertainties ever materialize or the assumptions prove incorrect, our results may differ materially from those expressed or implied by such forward-looking statements. All statements other than statements of historical fact could be deemed forward-looking, including, but not limited to, any projections of financial information; any statements about historical results that may suggest trends for our business; any statements of the plans, strategies, and objectives of management for future operations; any statements of expectation or belief regarding future events, technology developments, or enforceability of our intellectual property rights; and any statements of assumptions underlying any of the foregoing.

These statements are based on estimates and information available to us at the time of this presentation and are not guarantees of future performance. Actual results could differ materially from our current expectations as a result of many factors, including but not limited to: the unpredictable nature of our rapidly evolving market and quarterly fluctuations in our business; the effects of competition; and any adverse changes in our indirect channel relationships. These and other risks and uncertainties associated with our business are described in the company’s annual report on Form 10-K. The forward-looking statements in this presentation are made as of the date of the initial publication of this presentation, and we disclaim any obligation to update these statements at any time in the future.

# Agenda

1. **Intro**
2. **Access Control and Compliance**
3. **Deepfake and Spam Detection**
4. **AI for On-Prem**
5. **Digital Resilience for Collaboration**

# Connected Intelligence

Building the Workplace of Today, for the Workforce of Tomorrow

# Security and Trust

Most major cloud collaboration platforms provide a solid security baseline by default;

- Strong encryption for calls, meetings, messages, file sharing
- Administrative controls, MFA, SSO
- Meeting participant and lobby controls
- Security assessments and certifications – SOC 2/3 (global), IRAP (Australia) etc



For many organizations, the  
“default” is enough.

But.....

# When Collaboration is Mission-Critical....

Collaboration can be mission-critical – e.g. emergency services, hospitals, operational areas

WAN communications may not always be reliable –e.g. deployed/remote locations

High SLA's won't help if your ISP has issues, or somebody forgets to “dial before they dig” outside your building

Customers can choose to keep services on-premises, but these deployments may not provide the feature set or integration with the wider enterprise that users have come to rely on



# If You Need a Higher Level of Trust...

Trust in companies, governments and institutions is dropping – many organizations want to take security in their own hands

External and Internal threats, leaks, deepfakes and identity fraud are on the rise

How do we verify not only our own users, but external people we are meeting with?

Conflicting priorities between security and empowering your workforce with modern capabilities



# Equip the Platform to Meet Your Needs



**Identity**



**Security**



**Digital Resilience**

# Security Innovations in Webex Suite

Digital Resilience

---

Proactive Resiliency

RBAC and Compliance

---

Control Hub

Deepfake Detection

---

 Pindrop®

AI for On-Prem

---

Cisco AI Pods

# Access Control and Compliance

# Webex Role Based Access

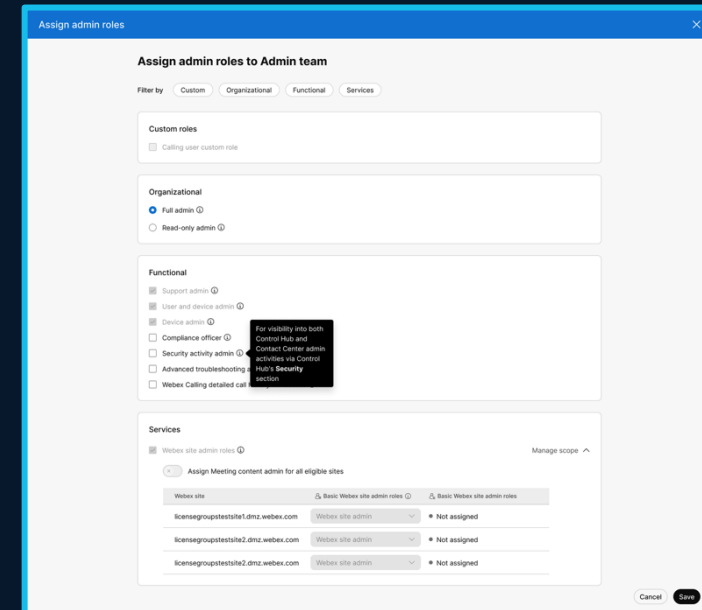
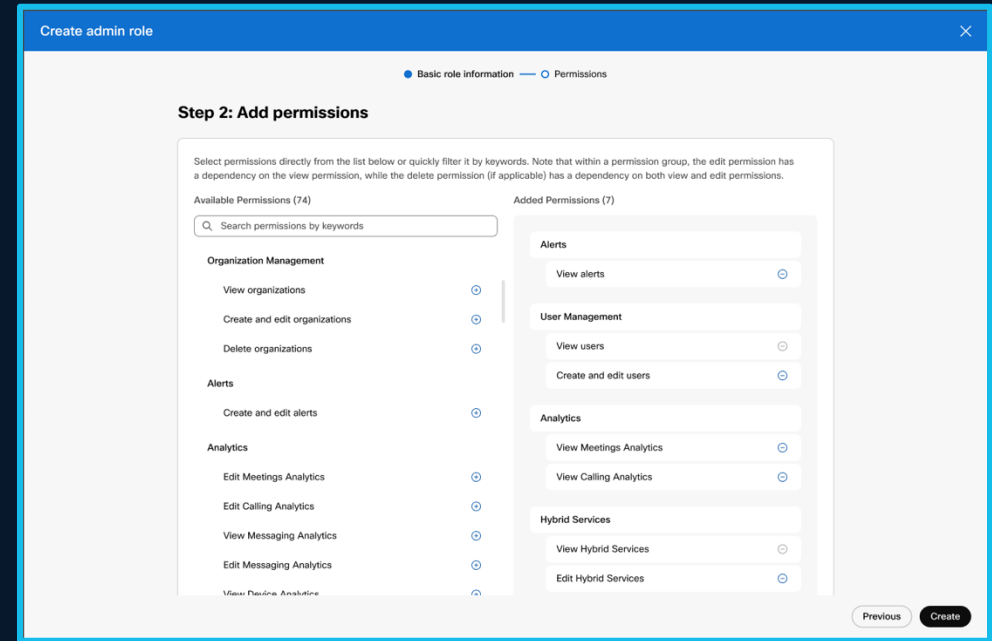
- Cisco is currently delivering a flexible, customer-defined RBAC solution to address current and future customer and partner administrative access requirements.
- Cisco's RBAC solution offers a custom role builder based on assigned permissions and a delegated administration solution to segment access to an organization's assets.



# Custom Role-Based Access

## Objectives:

- Maintain the **existing set of Webex Static Roles**
- **Respect principle of least privilege** allowing fine-grained control permissions
- Provide avenues to **assign roles to groups of users**
- **Conditional** rendering of control hub limited to the controls the admin has permission to use
- Customers have the ability to **create and define their own custom roles**



# Custom RBAC – Current Status

## Location Admin – Available NOW

- Restrict admin activities to one or more locations

## Permission Groups – In Beta NOW

- User Management
- Device Management – Workspace Insights
- Calling
- PSTN
- Analytics
- Troubleshooting
- Reporting
- License Management
- Messaging

## Permission Groups Coming Soon to Beta

- Meetings
- Audit Services
- Devices
- Contact Service
- Hybrid Calendar

<https://gobeta.webex.com>

# Post Quantum Resistant Cryptography

Webex uses PQ resistant ciphers today for media and signaling  
AES-256-GCM – preferred cipher for signaling and media  
PQ resistant ciphers needed for key negotiation

## Three phases of PQ support

- 1) Webex adoption of CiscoSSL version with PQ support
  - Provides support for TLS with PQ resistant key negotiation
- 2) Webex adoption of PQ resistant key negotiation for signaling to Webex KMS
  - Provides PQ resistant signaling encryption for user generated content (chat, files etc)
- 3) Webex adds support for PQ resistant deterministic key generation fo MLS
  - Provides PQ resistant key negotiation for media and content shared in E2EE'd Meetings

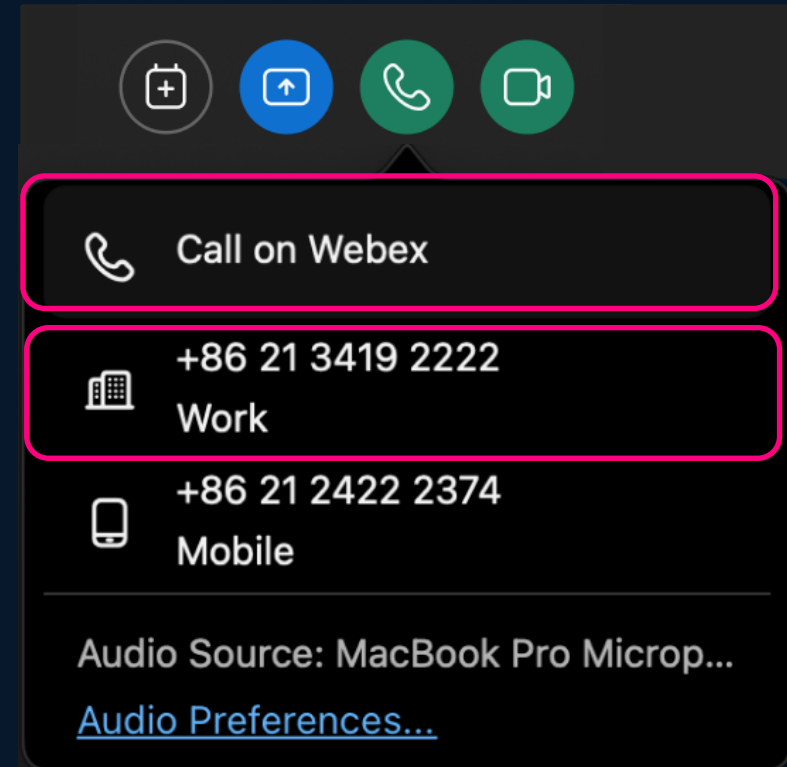
# New Feature - E2E Encrypted Calls with Webex Calling

## Webex App E2E Encrypted 1:1 Calls

- Call on Webex
- Webex Calling

*Today: Webex App (Desktop, Mobile)*

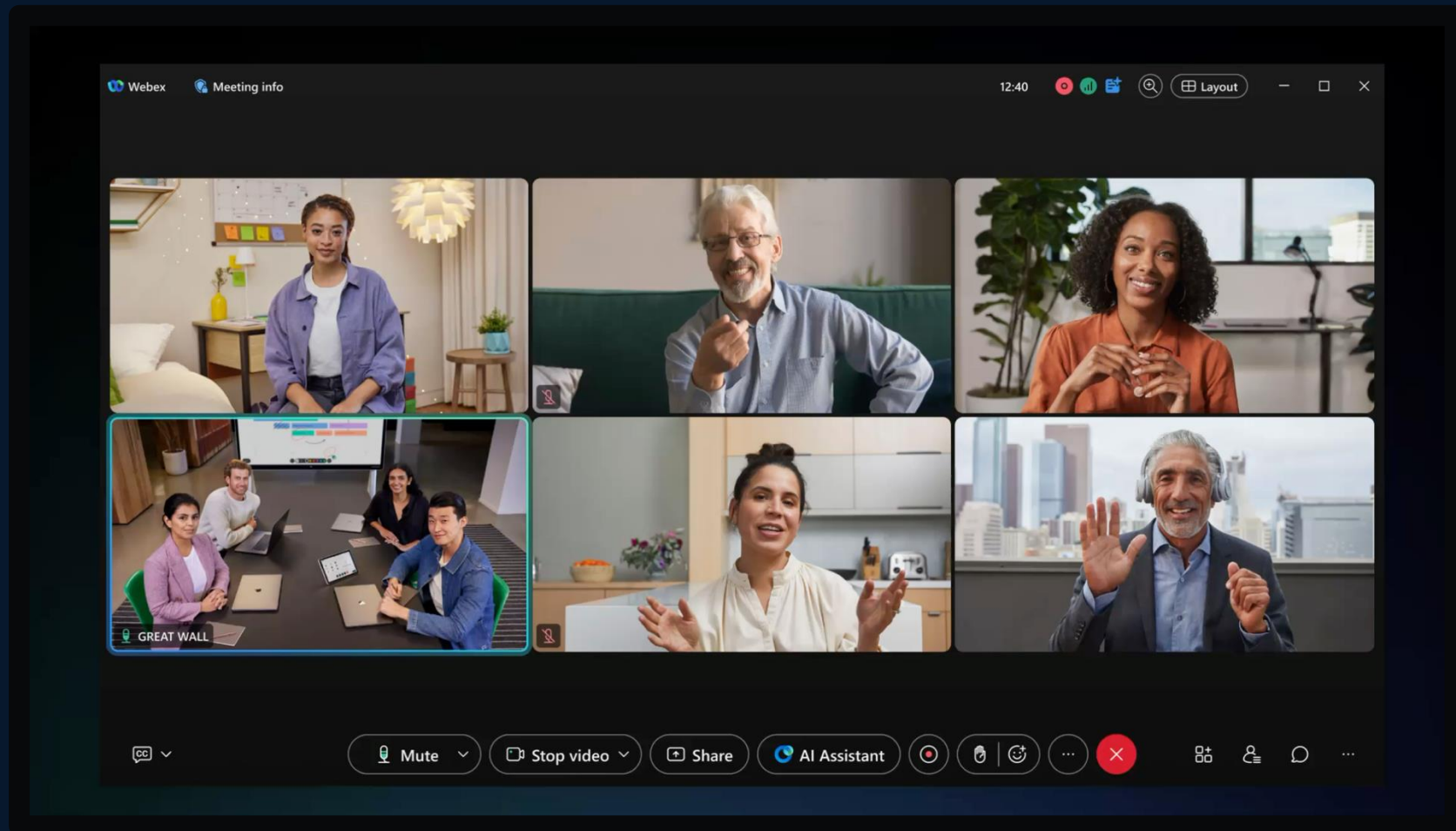
*Planned: Devices*



ENHANCED

# End-to-End Encryption

Secure, feature-rich end-to-end encrypted meeting experiences



# Zero Trust Security for Webex Meetings : E2E Identity

The screenshot displays a Webex meeting interface. On the left, a sidebar shows meeting details for a 'Feature Planning Meeting' hosted by Clarissa Smith. The 'Security' tab is active, displaying connection details: 'Server connection: TLS with ECDH and AES-256-GCM' and 'Media connection: AES-256-GCM'. It also lists encryption status: 'Zero Trust end-to-end encryption', 'Audio: Yes', 'Video: Yes', 'Screen and application sharing: Yes', 'Chat, files, whiteboards, and annotation: Yes', and 'Others (such as embedded Webex apps, embedded third-party apps, etc.): No'. A link to 'Learn more about end-to-end encrypted connections' is provided. The main area shows a 3x2 grid of video thumbnails for participants: Clarissa Smith, Henry Riggs, Isabelle Brennan, Kevin Woo, Marise Torres, and Great Wall. On the right, a 'Participants (6)' list shows names, roles (e.g., host, presenter), and email domains, with some marked as 'Unverified'. Meeting controls at the bottom include 'Mute', 'Stop video', 'Share', 'Record', and 'Apps'.

**Feature Planning Meeting**  
Host: Clarissa Smith

Copy meeting information

General Security

Server connection  
TLS with ECDH and AES-256-GCM

Media connection  
AES-256-GCM

Zero Trust end-to-end encryption

Audio: **Yes**  
Video: **Yes**  
Screen and application sharing: **Yes**  
Chat, files, whiteboards, and annotation: **Yes**  
Others (such as embedded Webex apps, embedded third-party apps, etc.): **No**  
[Learn more about end-to-end encrypted connections](#)

Participants (6)

- Clarissa Smith (Me, host • company.com)
- Kevin Woo (Presenter • example.com)
- Henry Riggs (Unverified)
- Isabella Brennan (company.com)
- Marise Torres (Unverified)
- Great Wall (company.com)

Mute all Unmute all

Mute Stop video Share Record Apps

# Webex Meetings : Lobby Controls and User Verification

**Participants (12)** ✕

🔔 **Kristine Stone** is waiting in the lobby. <sup>^</sup>  
Internal • cisco.com

Let in Remove

🔍 Search ↓↑

In the meeting 👤

- Clarissa Smith  
Host, me
- Umar Patel  
Presenter
- Henry Riggs ... 🔇
- Isabella Brennan ... 🔇
- Kristin Stone ... 🔇
- M Marise Torres  
@example.com ... 🔇
- GREAT WALL ... 🔇

Mute all Unmute all ...

**Participants (12)** ✕

🔔 **5 participants** are waiting in the lobby. <sup>^</sup>

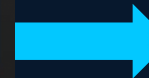
View

🔍 Search ↓↑

In the meeting 👤

- Clarissa Smith  
Host, me
- Umar Patel  
Presenter
- Henry Riggs ... 🔇
- Isabella Brennan ... 🔇
- Kristin Stone ... 🔇
- M Marise Torres  
@example.com ... 🔇
- GREAT WALL ... 🔇

Mute all Unmute all ...



**4 participants** are waiting in the lobby. ✕

- Internal ⓘ
- Kristine Stone  
cisco.com
- External ⓘ
- Murad Higgins  
ibm.com
- Molly  
ibm.com
- Unverified ⓘ
- Emily

Select all Admit Remove

These users are signed in but are not part of your organization.

These participants aren't authenticated or signed in so Webex can't verify their identities.

**Internal Users  
(Authenticated)**

**External Users  
(Authenticated)**

**Unverified Users  
(Not Authenticated)  
(Not Signed In)**

# Deepfake and Spam Detection

# Pindrop + Cisco Webex

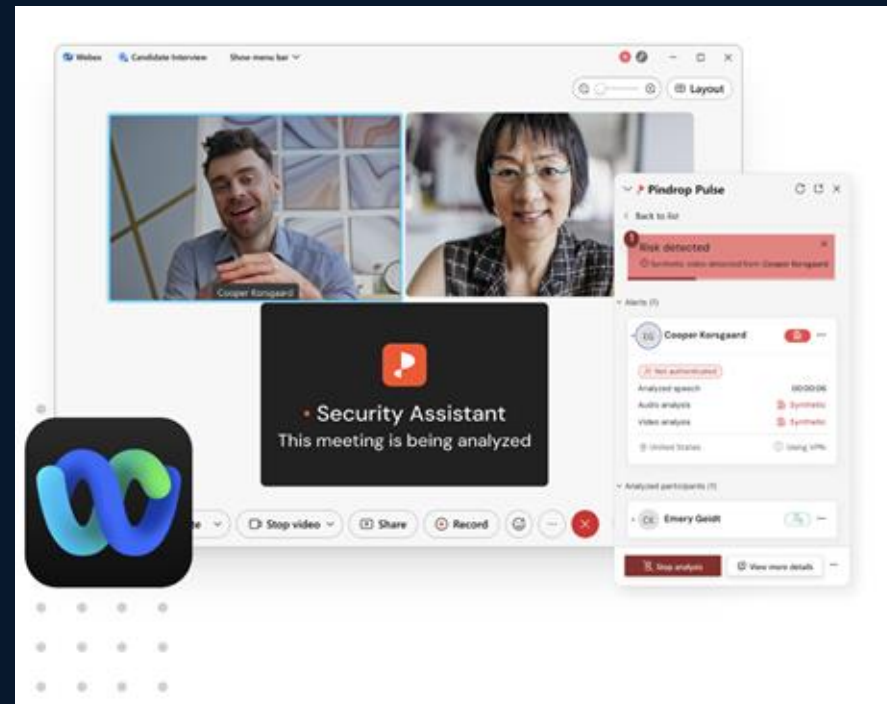
Together we're  
defending your  
business  
channels



Calling



Meetings



Contact Center

# What Makes Pindrop® Pulse for Meetings Different



Real Human

Deepfake /  
Content  
Forensics

Tech depth: 14 year  
head start; 75  
deepfake patents;  
650+ AI engines in  
training set

+



Right Human

Identity &  
Voice Auth

Industry-first and  
real-time, multi-  
factor analysis

+



Right Place

Location / IP  
Risk

Geolocation:  
industry-first location  
capabilities to detect  
location mismatch

# Multi-factor behavioral analysis



Is it a real human?

## Liveness

### Deepfake Detection

Analyze audio to identify AI-generated voices and block fraud attempts before they escalate—with 99% accuracy.



Something You Are

## Voice

### Deep Voice® Engine

Authenticate callers quickly and detect fraud early by analyzing over 250 vocal characteristics



Something You Have

## Device

### Phoneprinting® Technology

Create a unique device profile by analyzing 1,300+ audio features. Catch anomalies and verify callers without interrupting their experience



Something You Do

## Behavior

### Behavior Analysis

Spot suspicious behavior patterns in near real-time. Detect robotic activity to streamline authentication and reduce ATO



Something You Use

## Metadata

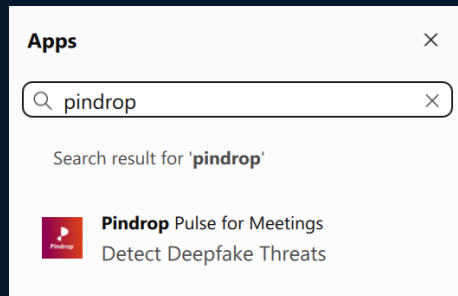
### Caller ID Validation + Spoof Detection

Validate phone numbers and assess the risk of caller ID spoofing even before the call connects

# Webex Meetings Deepfake Detection

Webex is partnering with Pindrop to deliver Deepfake detection in Webex Meetings

Add Pindrop Pulse to Webex (Pindrop license required)



The screenshot shows a Webex Meeting interface with two video feeds. The left feed shows Chelsey Krull, and the right feed shows Sarosh Shahbuddin. A large black overlay with the Pindrop logo and the text 'Security Assistant is recording this call' is centered over the video feeds. On the right side, the 'Pulse for Meetings' panel is open, displaying analysis results for Chelsey Krull. The panel shows 'Analyzed speech' with a duration of 00:00:06, 'Audio analysis' as 'Synthetic', and 'Video analysis' as 'Synthetic'. Below this, 'Analyzed participants (1)' lists Sarosh Shahbuddin. At the bottom of the panel, there are buttons for 'Stop analysis' and 'View more details'.



# Deepfake Detection – Native Integration

Roadmap to more natively integrate deepfake detection capabilities into Webex



# Webex CC Agent Screen Pop Available

The screenshot displays the Webex Contact Center Desktop interface. At the top, the status is 'Engaged' with a 'PU' (Present User) indicator. The main workspace shows a call from +18056306527. A 'Screen Pop' is active, displaying the Pindrop logo and the number 8058070607. Below this, there are two status boxes: a red 'AUTH STATUS' box indicating 'Not Authenticated' with the message 'Caller doesnt match the account profile', and a green 'RISK STATUS' box indicating 'Low Risk'. A feedback bar at the bottom shows 'Send Feedback' and 'Did Not Authenticate'. The left sidebar contains a list of recent calls.

Contact Center Desktop

+18056306527 01:53

+18056306527 01:52

Hold Consult Transfer Pause Recording End

Contact History Screen Pop

Screen Pop

Pindrop

Pindrop

8058070607

00:03:22

**AUTH STATUS**  
Not Authenticated  
Caller doesnt match the account profile

**RISK STATUS**  
Low Risk

Instruction boxes are used to streamline your agents workflows by providing customizable text to inform the agent on the next steps. As an example, you can prompt the agent to ask KBA questions as part of the process

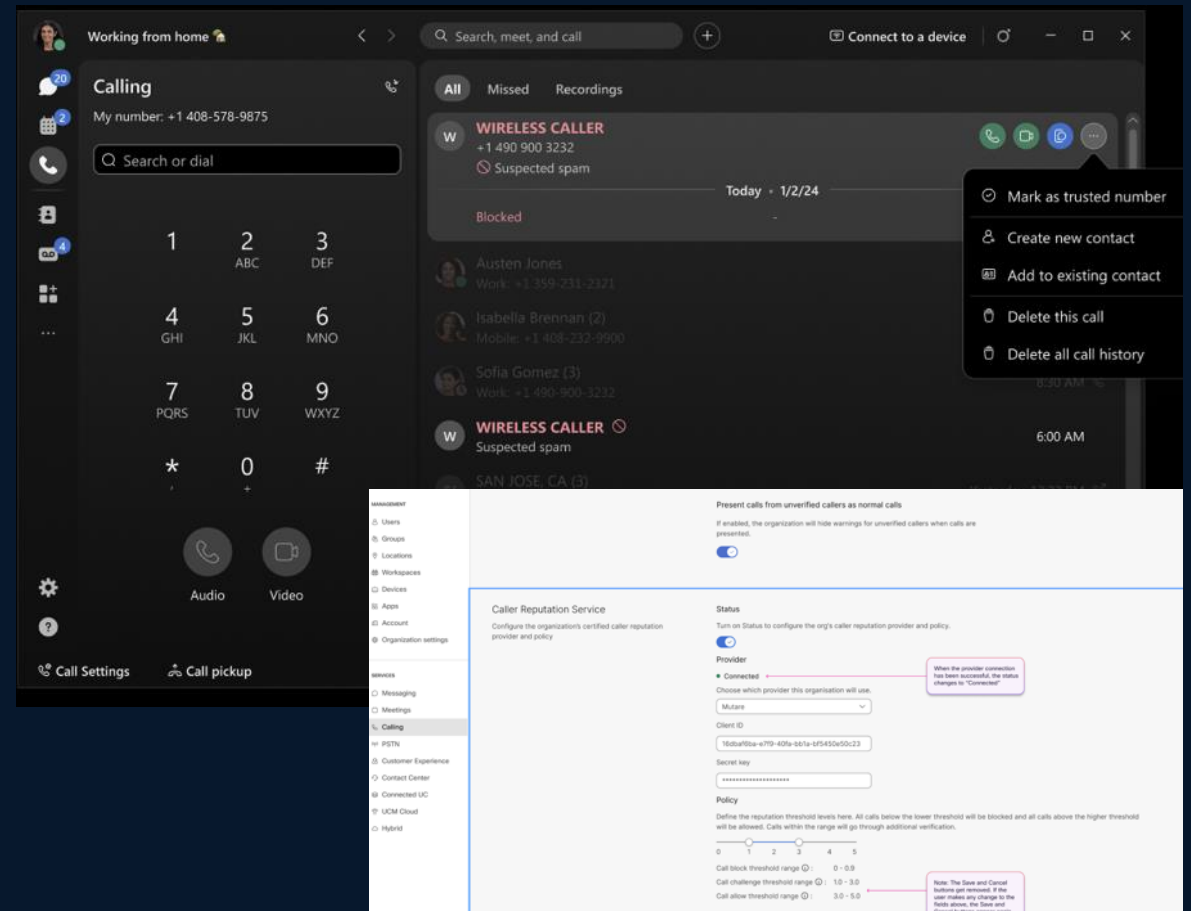
Send Feedback Did Not Authenticate

Phone Number	Profile	Time
+18056306527	N/A	04:52 PM
+18056306527	Default	04:50 PM
+18058070607	Default	04:33 PM
+18058070607	Default	04:28 PM
+18058070607		

# Spam and DDoS protection on Webex Calling

Eliminate distractions and boost security by minimizing unwanted and fraudulent calls

- Proactively blocks SPAM calls to protect Webex Calling users from fraud, minimize distractions, and provide secure, reliable calls—powered by integration with Mutare, a certified Caller Reputation Provider partner (CCRP)
- Configured in Control Hub, the integration lets administrators set a reputation threshold for calling numbers—automatically blocking calls below the threshold to ensure only trusted calls reach users
- Supported in branch offices in all regions with organization hosted in North America



# AI for On-Prem

General Availability  
Q2 CY26

NEW

# AI PODs for Webex

On-prem AI simplified –  
deploy, scale and innovate  
with confidence



# Collaboration AI Pods

Leverage Cisco AI pods to deliver AI-driven collaboration capabilities internally, for cloud and on-premises meetings

## On-Prem/Air-Gapped

Deliver AI capabilities to on-prem Cisco Meeting Server – no cloud connection required.

Proposed capabilities:

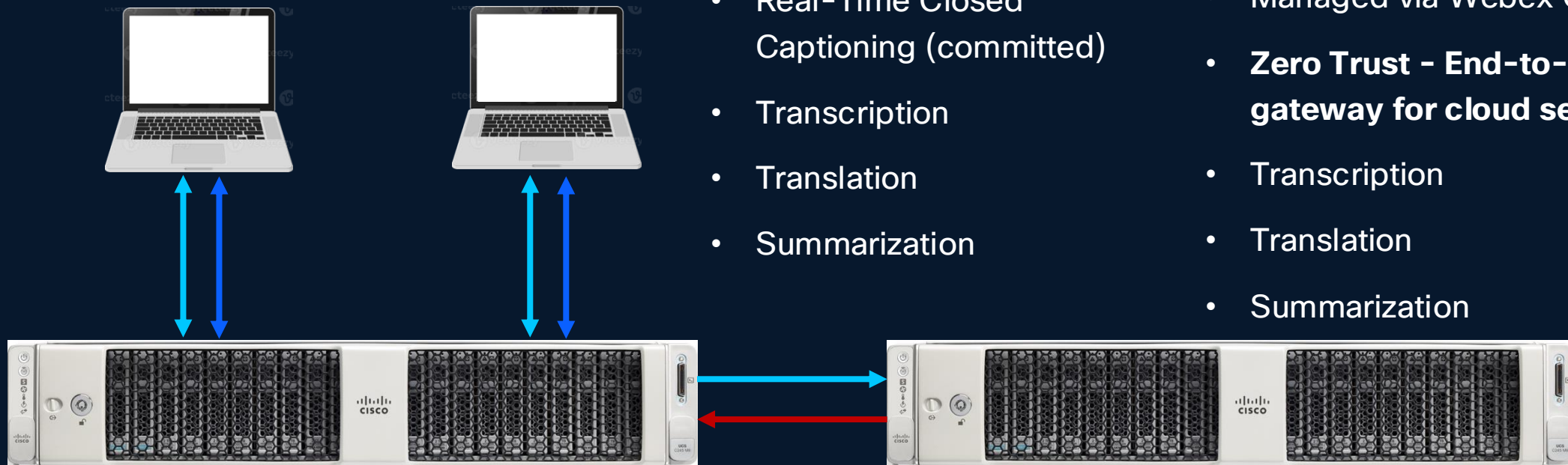
- Real-Time Closed Captioning (committed)
- Transcription
- Translation
- Summarization

## Webex w/Video Mesh

Deliver AI capabilities to Webex Meetings from on-prem infrastructure, for hyper-secure meetings.

Proposed Capabilities:

- Managed via Webex Control Hub
- **Zero Trust - End-to-End Encrypted gateway for cloud services**
- Transcription
- Translation
- Summarization



Cisco Meeting Server (CMS) or Video Mesh

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco AI Pod  
UCS C245 M8 Rack Server w/ NVIDIA H100 GPU

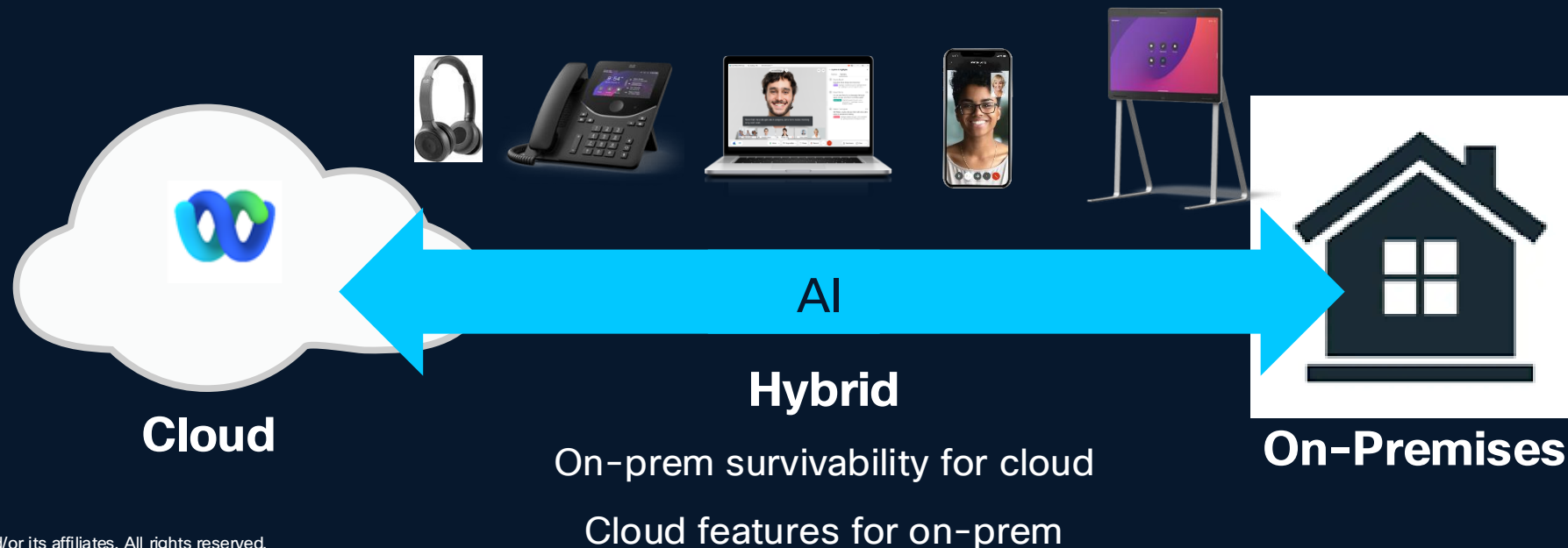
# Digital Resilience for Collaboration

# Digital Resilience

**Digital Resilience** is the ability of an organization to keep its business securely up and running despite any disruption.

For **collaboration technologies**, this can mean:

- keeping critical services running in spite of network, cloud or service disruptions
- providing additional assurance or higher security posture to your communications and data
- Extending cloud and AI capabilities to resilient on-premises deployments

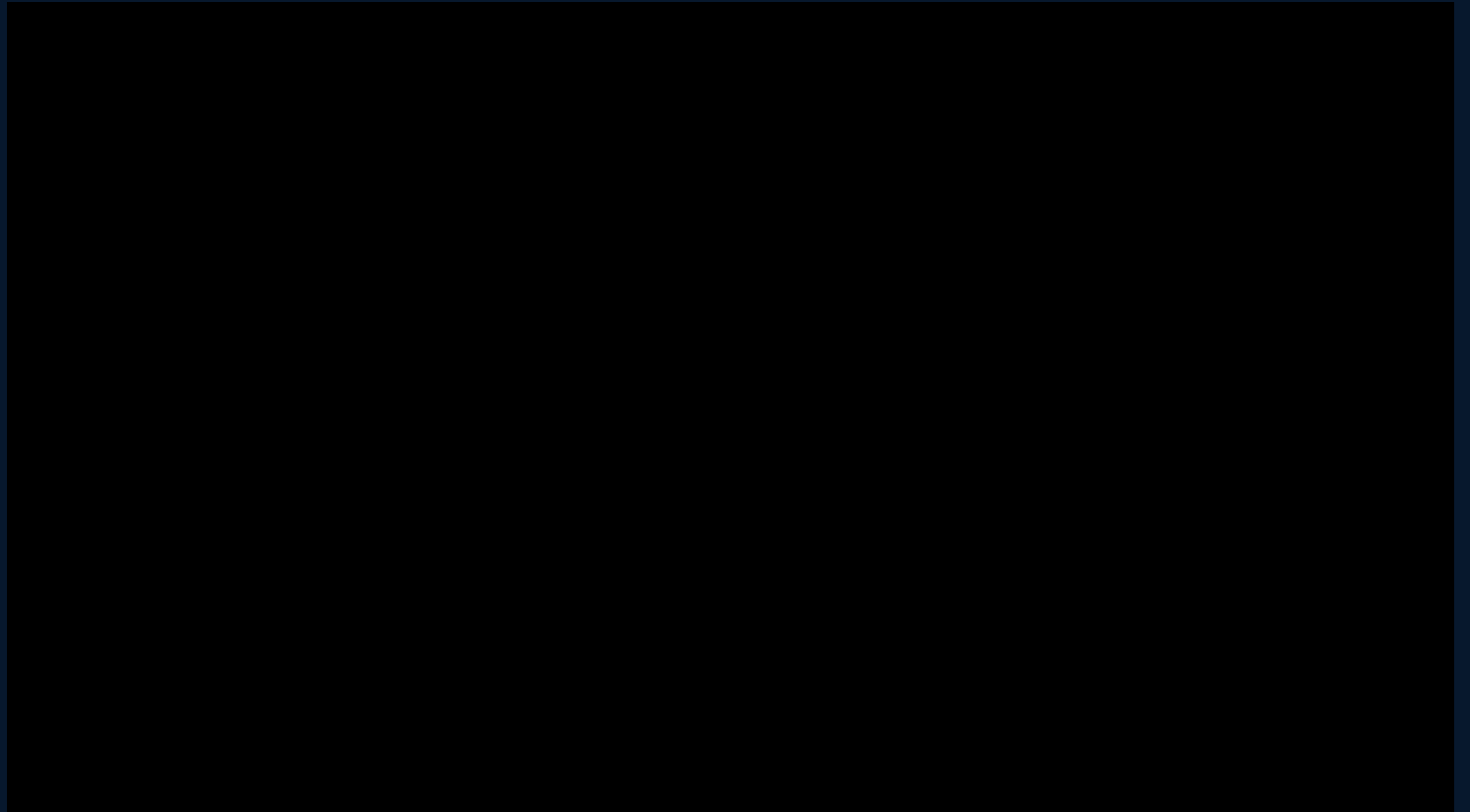


# Packet Loss - Audio Disruption in Calls and Meetings

It's very common for users to experience packet loss or poor network conditions, even during day to day use

The likelihood of these incidents can increase during emergencies - network interruptions, congestion

These are often when it's most critical to be able to communicate clearly



# Audio Resilience with Webex AI Codec

Webex AI codec uses advanced encoding, decoding and AI to reduce bandwidth usage and provide high audibility at up to 80% packet loss

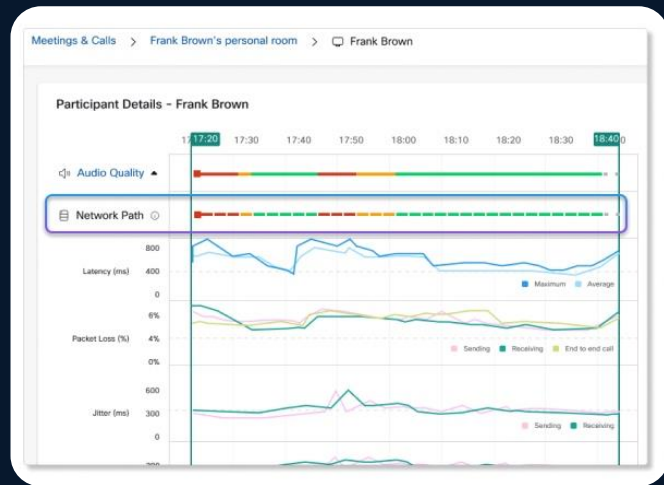
Supports Webex Calling 1:1 and Webex Meetings between compatible devices (Webex App – desktop and mobile)

Calls and Meetings automatically switch to AI codec when packet loss detected

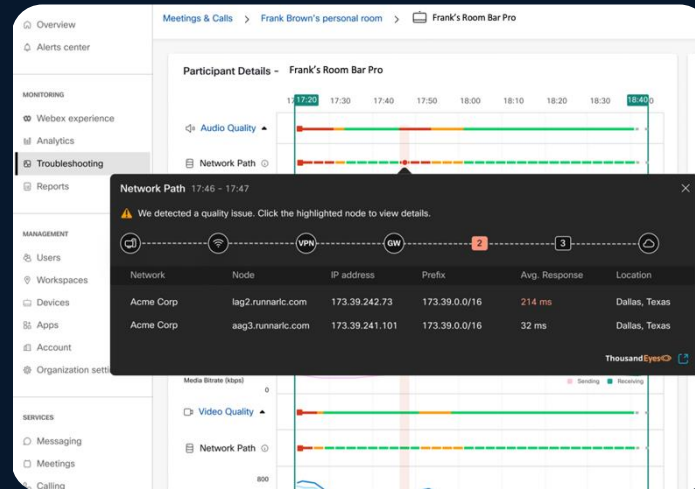
## ***Roadmap:***

***Transcode for non-compatible devices, CUCM support***

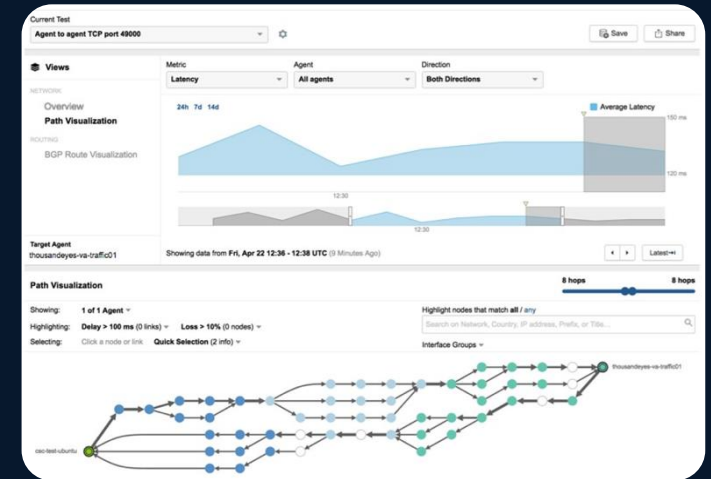
# ThousandEyes now integrated into the Webex Suite



Webex Meetings



Webex Devices



Webex Calling

Troubleshoot Calling in Control Hub with the Thousand Eyes Endpoint Agent

# Survivability in a cloud service

Each element of the service needs to be examined



Telephony connection

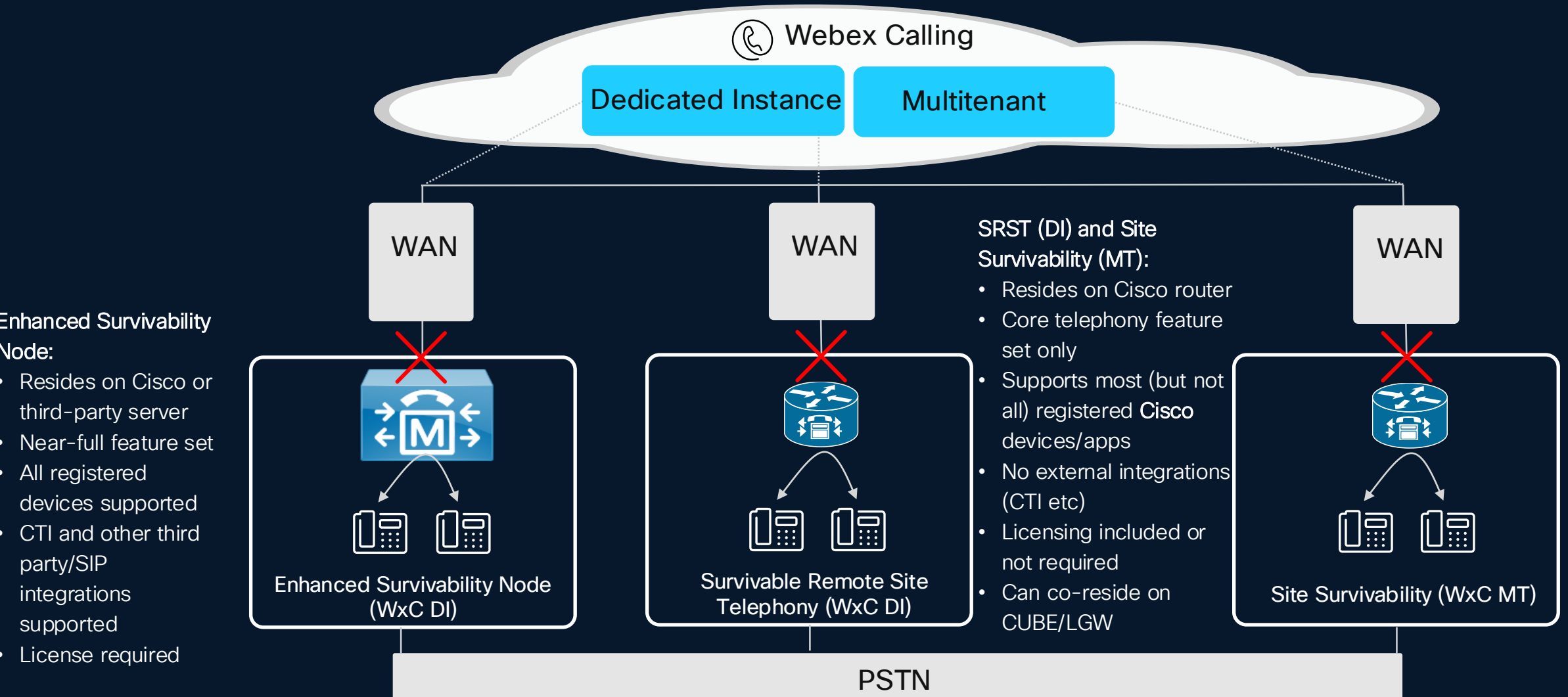


Platform



End user devices

# Webex Calling On-Prem Survivability Options



# Leader in Collaboration Security



TechVision  
RESEARCH

“Rated most secure” by  
TechxVision

Webex has the most security and privacy controls and is the only major UC&CaaS vendor that provides Ultra Secure Communications



Recognized by NSA as  
“best in breed”

No Jitter Dec. 2021: [Evaluating Cisco, Microsoft, Zoom on UCaaS Security | No Jitter](#)

SOURCE: [National Security Agency Cybersecurity Information – Selecting and Safely Using Collaboration Services for Telework](#)

