
IAUG
CONVERGE
NOVEMBER 2-4, 2026 | SAVANNAH, GA

IAUG CONVERGE 2026 • SAVANNAH, GA

Voice Security

Trusted voice communications for the AI fraud era

David Lew
Sr. Solutions Architect

Joel Haist
Client Executive

© Private and confidential

Agenda

Three topics frame the discussion.

CALLING IDENTITY

Outbound trust, branded calling, and the vendor landscape.

LAYERED VOICE SECURITY

Identity threats, risk-based controls, and orchestration.

USE CASES & NEXT STEPS

KBA replacement, readiness assessment, and ownership.



STATE OF BRANDED CALLING

Branded calling is becoming verified identity

Verified identity helps customers recognize legitimate calls, but coverage and presentation still vary.

AUTHENTICATE **Confirm the calling number**

STIR/SHAKEN helps verify that the caller is authorized to use the number.

ADD CONTEXT **Show who is calling**

Rich Call Data can add a verified business name, logo, and call reason.

MONITOR **Protect reputation**

Analytics and remediation still matter because verified identity does not prove intent.

Sources: FCC 25-76 (Oct 2025); IETF RFC 9795 and RFC 9796 (Jul 2025); ATIS RCD standard 1000094.v002

CUSTOMER USE CASE

Outbound calls lose trust before customers answer.

Spam labeling and missing caller identity reduce contact rates and make legitimate calls look suspicious.

01

Spam labels suppress reach

Legitimate calls display as Spam or Scam Likely, causing customers to avoid the call.

02

No verified brand context

Unknown numbers show no trusted business name, logo, or reason for the call.

03

Business impact

Lower answer rates reduce campaign effectiveness and increase repeat attempts.

C1 RESPONSE **Register and monitor numbers, remediate spam labels, and add verified branded calling.**

BRANDED CALLING VENDORS

The display layer is similar, while adjacent security services differ

Current enterprise portfolios from First Orion, Hiya and TransUnion



DECISION POINT	FIRST ORION	HIYA	TRANSUNION
PRIMARY FOCUS	Enterprise branding and reputation	Global voice intelligence	Telecom identity and authentication
CORE SERVICES	Branding, reputation monitoring, spoof blocking	Branding, registration, spam analytics, AI detection	Branding, caller authentication, spoof protection
BEST FIT	Brand protection and U.S. carrier reach	International reach and analytics	Identity breadth and carrier integration

Selection criteria: carrier and device coverage, verification method, reputation remediation, analytics, and international needs.

Sources: official vendor product pages reviewed September 2026

IAUG CONVERGE

BRANDED CALLING USE CASE

Branded calling restores identity to legitimate outbound calls.

Verified business information helps customers recognize the caller and understand the reason for the call.

01

Recognize the business

Display the verified business name and logo on supported devices.

02

Explain the call

Show a call reason such as appointment, service, or collections

03

Improve engagement

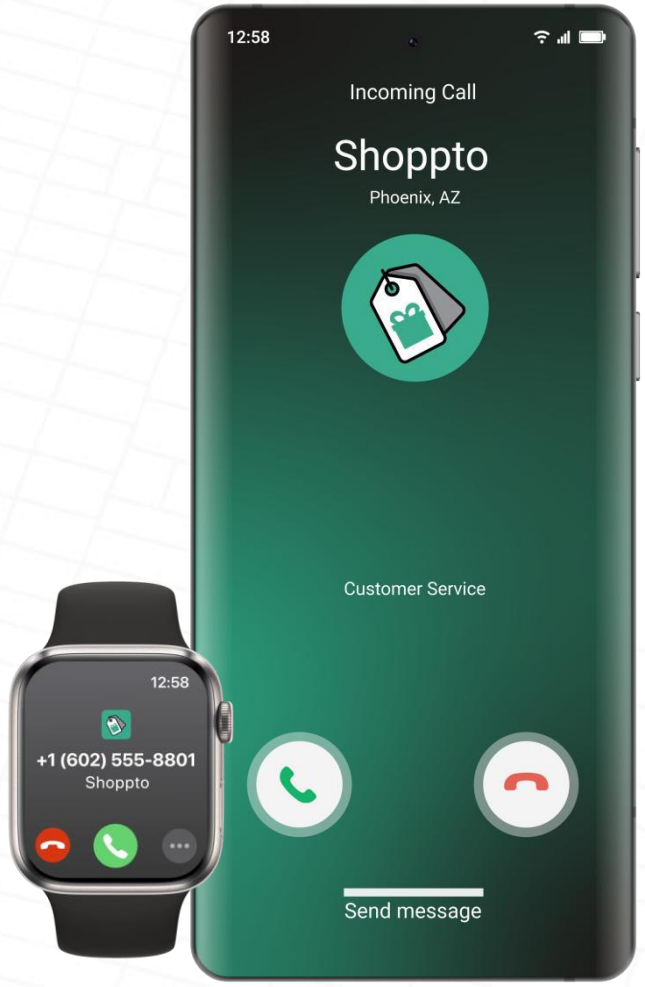
Reduce confusion from unknown numbers and support better answer rates.

ALSO REQUIRED Number registration, reputation monitoring, spam-label remediation, and campaign governance.

Branded Calling with Logo

Build trust by displaying your logo and reason for calling.

- Boost brand recognition with your logo and reason for the call.
- Protect outbound numbers and branding from spoofing.
- Reassure customers that your branded calls are authenticated.
- Give enterprises end-to-end control through Call Authentication.



Recognizable. Authenticated. Trusted.

Available on all major U.S. carriers*

*Device reach varies. Call Authentication is required for branded calling with logo. Source: First Orion, supplied presentation, page 8.

Voice Security

Latest voice attacks

Recent Reported attacks and emerging tactics



01 **AI voice impersonation**

Cloned voices seek payments or access to customer accounts.

02 **IT help-desk vishing**

Fake security updates lure employees to sites that steal logins and MFA tokens.

03 **AI-automated scam calls**

Conversational bots can personalize fraud attempts at scale. Emerging risk.

04 **Caller-ID spoofing**

Trusted numbers disguise payment scams and extortion calls.

Business risks: account takeover, payment fraud and data theft

A composable security fabric for trusted inbound, outbound, and contact-center voice.



- Passive Voice Authentication
- Deepfake Detection
- Call Trust & Reputation
- Branded Calling
- Real-Time Risk Scoring
- Dashboard Visibility
- Open API Integration

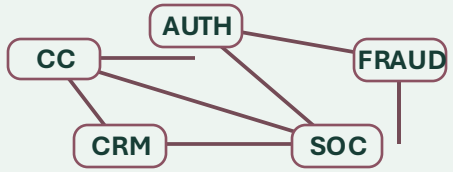
Inbound, outbound, and contact-center trust signals — orchestrated through open integration.

Orchestration turns fragmented voice security into one coordinated control plane.

No single vendor solves every voice-security challenge—so the platform needs one layer to coordinate response, policy, and analytics.

WITHOUT ORCHESTRATION

Complexity multiplies.



- Point-to-point integrations
- Separate APIs & decision logic
- Inconsistent policy enforcement
- Cross-vendor automation gaps
- Changes ripple across integrations

ORCHESTRATION

policy • workflow • telemetry

WITH ORCHESTRATION

One control plane. Three outcomes.

01 Automated Response

Block fraud and redirect risk
Step-up authentication
Notify SOC and update CRM/logs

02 Vendor Flexibility

Add vendors without contact center changes
Preserve workflows
Introduce capabilities incrementally

03 Centralized Analytics

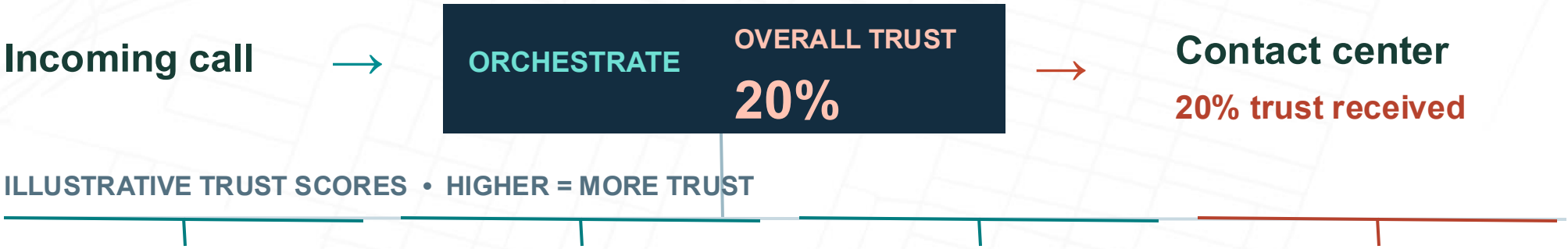
Fraud and deepfake trends
Authentication and routing outcomes
Automation and security performance

RESULT → faster response • consistent policy • lower integration friction

© Private and confidential.

One call, multiple assessments

Module trust scores → Overall score → Contact center



Identity Assurance Fraud Risk Synthetic Media Defense

Identity, fraud signals and synthetic voice

100%

No concern in this assessment

Call Defense

Call authenticity and voice-network threats

100%

No concern in this assessment

Voice Traffic Filtering

Robocalls, spam and unwanted traffic

100%

No concern in this assessment

Inbound Call Risk Intelligence

Additional inbound spam and scam signals

20%

Elevated spam / scam risk

Added call-path delay **0 ms**

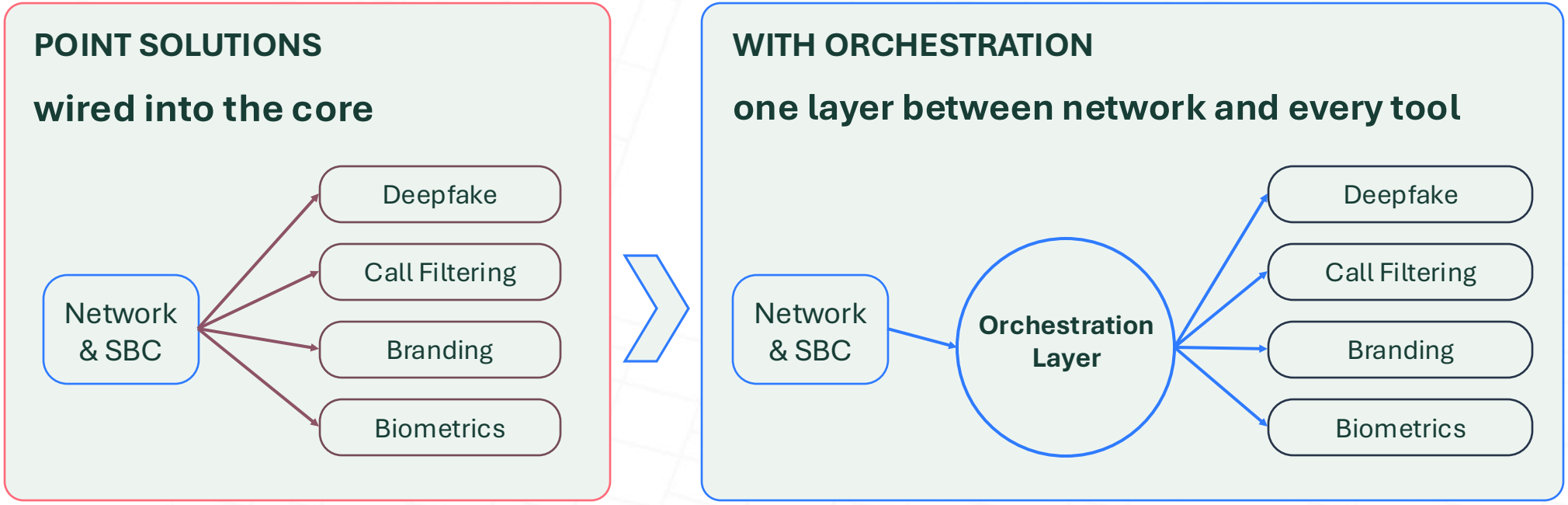
Subject to integration and latency validation

DESIGN TARGET

Example policy: lowest module score sets overall trust

One orchestration layer harnesses the AI tool explosion.

Plug each tool into the control plane once; add, swap, or retire apps without rebuilding the core network.



Signals do not share. Reintegration repeats.

Apps share signals in real time. Core network untouched.

© Private and confidential.

EXAMPLE → Deepfake detection flags synthetic audio; orchestration updates shared treatment data so the next call is blocked at the door.

Voice Security Use Case

Replacing Knowledge Base Authorization (KBA) with risk-adaptive voice trust decisions.

CURRENT-STATE RISK

Why KBA should be retired.

Static questions are exposed, slow, and increasingly inadequate against AI-enabled social engineering.

Data is exposed

Answers are discoverable from breaches, public records, and social media.

Friction is costly

Manual Q&A extends handle time and creates peak-volume bottlenecks.

AI changes the threat

Synthetic voices and social engineering make static questions insufficient.

CORE RECOMMENDATION → Replace KBA with a risk-adaptive voice trust decision, not another static shared secret.

RECOMMENDED ARCHITECTURE

Target model: layered voice trust.

A caller is continuously evaluated across independent layers before sensitive actions are authorized.

1

Call origin & reputation

STIR/SHAKEN, caller reputation, spoofing signals

2

Passive voice biometrics

Vocal characteristics compared with enrolled profiles

3

Deepfake & liveness

Synthetic audio, replay, anomaly checks

4

Contextual risk

History, transaction sensitivity, behavior, IVR journey

5

Policy decision

Allow, step up, restrict, route, block, or review

DESIGN PRINCIPLE → No single factor decides identity or authorization by itself.

Voice Security Assessment

From evidence to an executable voice-security roadmap.

VOICE SECURITY READINESS ASSESSMENT

Can your security team see what is happening on the phone?

A structured evaluation scored against real attack paths and translated into a prioritized, costed remediation roadmap.

74 controls

9 domains

9 attack paths

1 exec page

WHY IT MATTERS

- The channel few monitor
- Ownership falls between voice engineering and security
- Synthetic and cloned voice lowers the attack barrier

WHAT YOU RECEIVE

- Executive dashboard
- Threat readiness radar
- Prioritized findings
- Costed remediation roadmap

ASSESSMENT COVERAGE

Executive deepfake • Account takeover • Vishing • Caller ID spoofing • Voice AI manipulation • TDoS • Toll fraud • SIP attack • Biometric spoofing

HOW IT RUNS → 2–3 weeks: scope & prepare • workshops & evidence • scoring & QA • executive readout • costed roadmap

Q&A

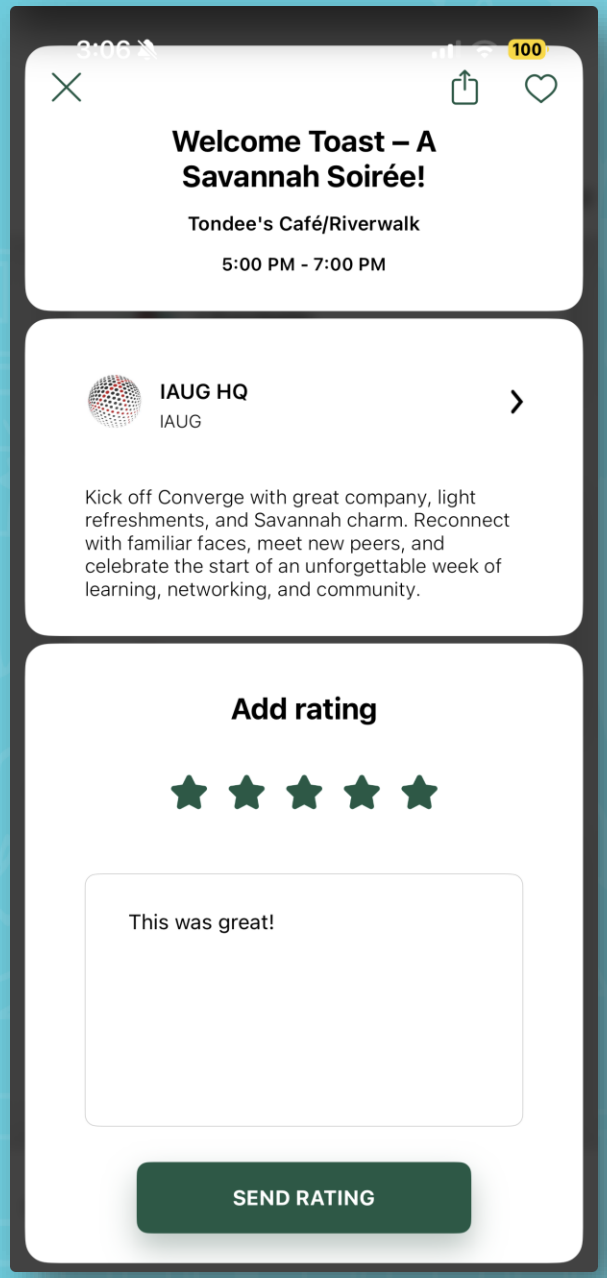
Questions & discussion

Join the IAUG Community + download the app!

International Avaya Users Group

International Avaya User Group (IAUG)

SCAN HERE



Thank you!

Please take a moment to provide a rating and feedback in the IAUG Converge App.

All feedback is hidden and anonymous.

1. Click on this session.
2. Scroll to the bottom and find "Add rating."
3. Select between one (low) to five (high) stars.
4. Leave an optional comment explaining your rating.
5. Click, "Send Rating."