AURAYA

UNMATCHED VOICE INTELLIGENCE

EVA FOR CONTACT CENTERS



Secure every customer interaction without adding unnecessary friction.

EVA for Contact Centres brings together device and number intelligence, voice biometrics, liveness, fraud intelligence and continuous verification to help organisations establish trust in real time.

Five core signals are assessed concurrently and scored together, giving your organisation the intelligence to apply its own risk rules while legitimate customers experience faster, more natural authentication.

The Authentication Dilemma

Traditional authentication was built for a different threat landscape. Credentials can be stolen, phone numbers can be spoofed, devices can change hands and voices can now be cloned.

No single signal provides enough confidence on its own.
EVA for Contact Centres uses multi-modal risk analysis to assess the device, the speaker, the authenticity of the audio, known fraud indicators and the continued presence of the authorised person.

The result is a more complete view of risk that can be passed into your existing customer journey, allowing your organisation to decide whether to allow, route, step up or decline an interaction based on its own rules.

EVA
FOR CONTACT CENTERS

How EVA Establishes Trust Across Every Interaction

On every interaction, EVA asks five questions concurrently to build a more complete picture of identity and risk.

1. Is this a device we trust?

Device Trust & Initial Identity Claim
Before the customer speaks, device and number signals provide an initial identity claim and independent indication of risk. EVA can assess signals associated with the originating device and network to help flag risks such as caller ID spoofing, recent SIM or number swaps, unrecognised devices and devices associated with previous fraud.

2. Is this the person's voice?

Voice Verification
EVA compares the speaker's voice against their enrolled voiceprint and returns a biometric match score, adding another layer of confidence to the interaction.

3. Is this a live person?

Liveness & Synthetic Voice Defence
EVA assesses whether speech is coming from a live person in the moment, screening for synthetic and cloned voices, recorded playback and injected audio. Where additional assurance is required, EVA can use a randomised spoken challenge that a previously captured recording cannot anticipate.

4. Is this someone we already know is a threat?

Fraudster Screening
EVA screens interactions against watchlists of known and suspected fraudsters, surfacing probable matches so fraud and security teams can apply the appropriate response.

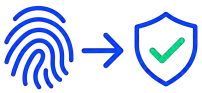
5. Is the authorised person still speaking?

Continuous Presence Assurance
EVA continues assessing the speaker throughout the interaction, at minute two and minute twenty, not just at the initial authentication event.
Together, these five signals provide a continuous, risk-based layer of identity assurance without adding unnecessary friction for legitimate customers.

Key Enterprise Benefits



Enrol Customers Where It Makes Sense
EVA supports flexible enrolment across the customer journey. Customers can enrol during a natural conversation with an agent or voice bot, actively through the IVR, within an already authenticated app or browser session, during new-customer onboarding, or in bulk using existing recordings. EVA checks enrolment quality throughout the process to help ensure voiceprints meet the required standard before they are accepted.



Move Off Legacy Biometrics Without Starting Again
Organisations that have invested years building an enrolled population shouldn't have to ask every customer to start again. EVA can regenerate new voiceprints from existing enrolment and verification recordings, allowing established customer populations to transition from legacy voice biometric platforms without requiring mass re-enrolment. The newly enrolled population is optimised, and a report can be generated automatically showing how much better it will perform once turned on, allowing the customer to see the improvement in their own data before committing.



Active or Passive But Always Frictionless.
EVA supports both active and passive verification. Customers can verify actively by responding to a short prompt or passively through natural conversation with an agent or voice bot, with no additional authentication process required. Verified customers can move directly into self-service or reach an agent already verified, helping reduce repetitive security questions and the need to read sensitive personal information aloud.



Maintain Trust Throughout the Interaction
Authentication shouldn't end after the initial identity check. EVA continuously assesses whether the person speaking remains consistent with the verified speaker throughout the interaction. When a customer is transferred to another agent, specialist or supervisor, the verification signal travels with the interaction, helping the receiving agent maintain confidence without forcing the customer through another round of security questions.



One Voiceprint Across Every Channel.
A centrally managed voiceprint can support identity verification across contact centre calls, voice bots, mobile apps, browsers and other digital interactions. A customer enrolled on a call can verify digitally, while a customer enrolled through an authenticated digital interaction can be recognised when they next call the contact centre. This creates a more consistent identity experience across channels without requiring separate biometric enrolment programmes.

Enterprise Visibility & Reporting

EVA provides visibility from individual verification outcomes through to specialist biometric performance analysis.



Native Interaction Data
EVA runs natively inside your selected contact centre platform (CCaaS) for faster, easier deployment with no new systems to manage. Leveraged and managed directly by your CCaaS team, per-call enrolment and verification outcomes write directly to the platform's interaction records, making biometric status and reporting seamlessly available across customer journeys, agents, and connected systems.



Your Analytics Environment
Full biometric telemetry can be streamed to an analytics destination selected by your organisation, supporting enrolment trends, verification performance and fraud reporting within your existing BI environment.



ArmorVox Console
Specialist biometric reporting is included with every deployment. The ArmorVox console provides visibility into:

- Enrolment health and voiceprint quality
- Security threshold and performance tuning
- Independent biometric performance auditing
- Voiceprint inspection and management
- Audit history

EVA provides visibility from individual verification outcomes through to specialist biometric performance analysis.

Virtual Native on Leading Contact Centre Platforms

EVA is virtual native on Amazon Connect, Genesys Cloud, Five9 and NICE CXone. Customer journeys are configured using each CCaaS platform's own tools, with verification status surfaced within the existing agent experience.

This means your team can use the skills and tools it already knows; enabling faster deployment, simpler ongoing support and new use cases without unnecessary vendor involvement.

Supported environments include:

- Amazon Connect
- Genesys Cloud
- Five9
- NICE CXone

Auraya's open API architecture also provides the flexibility to integrate EVA into other cloud-based and on-premise contact centre environments.

Built to Scale

EVA is designed for high-volume enterprise environments, with auto-scaling capabilities supporting variable demand as interaction volumes change. Deployment options include secure SaaS, private cloud and on-premise environments, giving organisations the flexibility to meet security, operational and data sovereignty requirements.

Compliance and Assurance

EVA is built for enterprise and regulated environments where security, privacy and control are critical.

- SOC 2 Type II — Report Issued
- ISO/IEC 27001:2022 Certified
- GDPR compliant: Biometric data handled as special category personal data, with Auraya acting as processor or sub-processor under customer data processing agreements.
- Independent Penetration Testing: Conducted at least annually and after every major release.

Synergy:
The Unified EVA Ecosystem

EVA for Contact Centres forms part of Auraya's broader voice intelligence ecosystem, designed to help organisations strengthen identity assurance and fraud protection across different interaction environments.

Auraya's broader capabilities include:

EVA Digital: Voice biometric authentication for digital interactions, including web and mobile environments.

EVA Forensic: Advanced fraud intelligence and forensic capabilities, including fraudster watchlist screening and analysis of suspicious voice interactions.

Together, EVA for Contact Centres, EVA Digital and EVA Forensics operate across shared voiceprint infrastructure, allowing organisations to extend authentication and fraud protection across channels without creating separate biometric enrolment programmes.

Ready to Strengthen Identity Assurance?

Email info@aurayasystems.com to book a demo and see how EVA for Contact Centers can strengthen identity assurance, reduce authentication friction and protect your organisation against evolving fraud threats.

AURAYA

UNMATCHED VOICE INTELLIGENCE

About Auraya

Auraya is a specialist voice intelligence company helping enterprise and government organisations establish trust with every interaction. Combining deep expertise in voice biometrics with device intelligence, fraud prevention and synthetic voice defence, Auraya delivers secure and frictionless identity assurance which is specifically designed for complex, regulated environments.

Through flexible deployment and a global ecosystem of technology and delivery partners, Auraya supports organisations in strengthening security while creating simpler, more trusted experiences for legitimate customers across all interaction channels.

aurayasystems.com
info@aurayasystems.com

Australia & New Zealand | Asia Pacific | United Kingdom & Europe | Americas