BLUEWAVE COMMUNICATION SECURITY · VOICEGUARD

VoiceGuard & CallCenter Guard

Detect cloned voices. Analyse phone deception.

IN ONE PARAGRAPH

VoiceGuard is BlueWave AI's protection against deception on phone calls. It gives separate signals on three questions: could the voice be synthetic or cloned, does the conversation show a deceptive pattern, and can the call's origin be verified. The three capabilities are at different stages and complement each other. CallCenter Guard applies VoiceGuard in the contact centre; partners can also build it into their own services or offer it to end users.

THE PROBLEM: FAKE VOICES AND REAL-VOICE DECEPTION

- Voice cloning is cheap, and a cloned voice can ask for money, data or an approval in the voice of a relative, a manager or a member of staff.
- But the attack is a chain of deception that also works with a real human voice: urgency, posing as someone else, demands for secrecy, pressure to skip the usual security step. That is why VoiceGuard does not stop at asking whether the voice is real.

THREE QUESTIONS, THREE CAPABILITIES

Voice: could it be synthetic or cloned? VoiceGuard Engine	AVAILABLE
Conversation: does it show a deceptive pattern? Vishing and social engineering pattern analysis	DEMONSTRABLE PROTOTYPE, PERFORMANCE VALIDATION UNDERWAY
Origin: can the caller be verified? BlueWave Witness	PLANNED PARTNER CAPABILITY

- **Voice:** works on live audio streams and recorded files, including narrowband telephone audio. Several consecutive segments are assessed together to reduce false alerts from brief noise. Each alert can be traced to the model version and the segments behind it. It does not identify the speaker and is not legal evidence.
- **Conversation:** flags deception even when the voice is real; in our demo it also flags calls made with a real human voice. It does not read minds and is not a lie detector.
- The signals are not merged into a single 'fraud / not fraud' verdict. The customer's or partner's rules decide the next step: proceed, verify further, suspicious, block or inconclusive.

BLUEWAVE WITNESS: VERIFYING WHERE A CALL COMES FROM

- The calling organisation, for example a bank or a service provider, signs its own calls. The person receiving the call sees one of three states:
- **VERIFIED:** the call really comes from the organisation. This verifies its origin, not that everything said is true or that every request is safe.
- **NOT VERIFIED:** no signature. On its own, a missing verification is not a sign of fraud; confirm any money movement on another channel.
- **FLAGGED:** no signature, and detection also fires. Hang up and call back on a known number. This is not a legal finding of fraud.
- Witness complements detection: detection asks what may be fake, Witness asks what can be verified. Status: planned partner capability, with a proof of concept on a simulated telephone channel; not a finished mobile app.

Gergely Vass, CEO · gergely.vass@bluewaveai.co · +36 20 441 5497
Gyula Németh, CTO · gyula.nemeth@bluewaveai.co · +36 30 560 9260

CALLCENTER GUARD: VOICEGUARD IN THE CONTACT CENTRE

- **Where it helps:** decisions taken by phone where a fake voice could get through: account recovery and password resets, new device or phone-number registration, phone approvals and callbacks, customer data changes, internal IT helpdesk requests, and reviewing suspected fraud calls afterwards.
- **For:** banks, insurers, outsourced contact centres (BPOs), helpdesks and any team that handles requests by phone.
- **The audio available:** the organisation's own call recordings today; live inbound calls once connected.
- **What we can test on existing recordings:** whether the signal is useful in one selected process, at what false-alert rate, processing time, share of unusable audio and review workload. These are measures, not promised results.
- **What needs live integration later:** the live call connection (SBC/SIPREC) is in development; bringing alerts into the agent or fraud-management workflow is planned and built together with the customer.
- CallCenter Guard does not identify the speaker, prove fraud or end a call; your agents stay in charge.

PARTNER, API AND END-USER APPLICATIONS

- **Partner integrations:** We work with partners to integrate VoiceGuard capabilities into their existing platforms and services. Technically this uses a REST/WebSocket API and events; the production security layer is part of the rollout.
- **Through a partner to end users (B2B2C):** banks, operators or app providers can offer protection to their own customers under their own brand. A planned mobile service, CallGuard Mobile, is part of this route.
- A mobile app does not automatically get access to the audio of a phone call; the route to the audio is designed with each partner, platform by platform.

WHAT SETS THE TECHNOLOGY APART

- **Control over data:** processing can run in your own environment; an on-premise installation package is in development. Customer data is not used for model training by default.
- **Adaptable to your data:** the trainable layer is small, so it can be fine-tuned on approved customer data. The engine is built on Kolmogorov–Arnold Network (KAN) layers.
- **Built for telephone audio:** it works on narrowband audio. Capacity and accuracy are measured on your hardware and data rather than quoted in general.

WHERE THINGS STAND

Synthetic and cloned voice detection, on recordings and via API	AVAILABLE
Vishing and social engineering pattern analysis	DEMONSTRABLE PROTOTYPE, PERFORMANCE VALIDATION UNDERWAY
Listen-only analyser added to a call (demo environment); VideoGuard	DEMONSTRABLE PROTOTYPE
Live contact-centre connection (SBC/SIPREC), production API security, SIEM connector	IN DEVELOPMENT
BlueWave Witness · CallGuard Mobile · MessageGuard and LinkGuard	PLANNED

THE FIRST JOINT ASSESSMENT

- A short call about one process or user scenario, and the audio that is lawfully available for it.
- An assessment on existing recordings or approved samples, with a written report and a joint decision on whether and how to continue.
- We agree the scope, terms and any fees of an assessment before it starts. We have presented our voice detection to teams at three Hungarian banks.

NEXT STEP

A short conversation about where phone-channel deception matters to you or your colleagues: a contact centre, a customer-facing service, or a platform you run. If fraud prevention or customer service sits with a colleague, please feel free to forward this document.

Gergely Vass, CEO · gergely.vass@bluewaveai.co · +36 20 441 5497
Gyula Németh, CTO · gyula.nemeth@bluewaveai.co · +36 30 560 9260