aurigin.ai

# Enabling trust in content and real-time communication in the age of AI

The team

# Combines AI, data science and audio expertise

aurigin.ai

Luzi Sennhauser
Co-Founder & CEO
ETH Data Scientist
McKinsey

Simon Thomé
Co-Founder & CPO
ESME Computer Scientist
PwC

Nicolas Wagner

Kudret Esmer

Mirjam Kaeser

Violeta Petrovic

Georgios Xypolitos

Daniel Banyay

Andreas Sennheiser
Co-Founder & Investor
Co-CEO of Sennheiser
Global leader in premium audio expertise

Extensive strategic partnership with Sennheiser (globally leading pro audio equipment manufacturer) providing great synergies in terms of distribution and audio capability sharing. This partnership is facilitated through Andreas Sennheiser's dual role as aurigin.ai chairman and Sennheiser CEO

The Problem

aurigin.ai

# Generative AI has made voice impersonation scalable and real-time

**01**

## AI changed the game

Voice clones need seconds of audio. Attacks are real-time, scalable, and undetectable.

**02**

## Legacy tools are failing

Social Engineering attacks bypass MFAs. Humans can no longer detect AI generated voices, making awareness training insufficient.

**03**

## The cost of inaction

One spoofed call can trigger system compromise, data leaks, and operational failure.

The Problem

aurigin.ai

# Voice remains the most trusted, unprotected channel in enterprises

Network – firewalls, SASE

Endpoints – EDR, XDR

Identity – IAM, MFA

---

**Voice** - One call bypasses every infrastructure layer, the human becomes the vulnerability

- **Builds on trust** - people comply with a familiar voice without questioning it
- **No time to verify** - real-time interactions are immediate
- **Direct impact** - delivers actionable instructions & authorizations

Example: Impersonation of Jamie Dimon

aurigin.ai

# 20 seconds of audio are enough to impersonate anyone on a phone call

**20 seconds reference audio**
from the web


**Undetectable impersonation**
(e.g., on a phone call)

*Click to watch the video*

**$10M–$100M**
Annual damage potential for a medium-sized bank

**69%**
Likelihood of getting attacked with vishing in a given year

**90%**
Success rate of CEO fraud

Real world impact

# Organizations are already losing millions to voice fraud

## $25M

### Deepfake CFO impersonation - Arup

A finance worker joined a video call with the CFO and senior executives. Every person on the call was AI-generated.

## $100M

### IT helpdesk vishing - MGM Resorts

An impersonated employee requested a credential reset, leading to ransomware installed that paralyzed operations for a week.

## $17B

### Call center account takeovers

61% of account takeover losses happen through call centers. Projected global ATO losses reached $17B in 2025.

Our solution

aurigin.ai

# Unmask real-time caller impersonation with AI deepfake detection and voice watermarking

## Synthetic Voice Detection

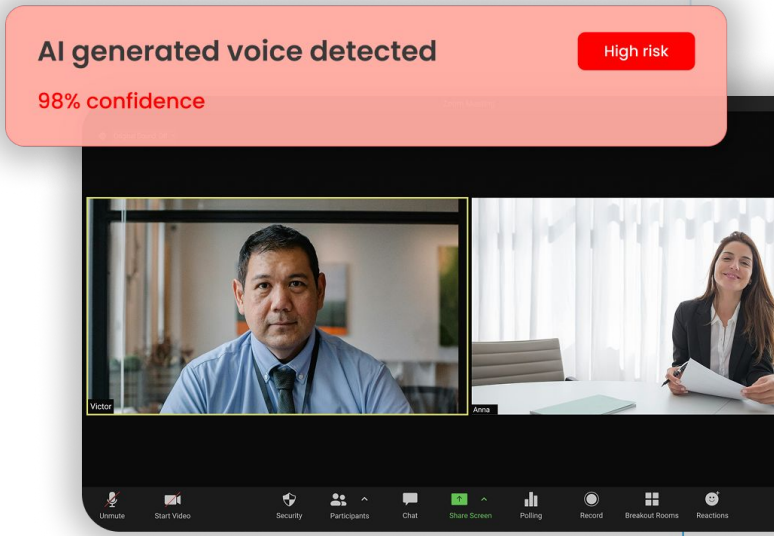
Continuously monitors call audio to identify and flag deepfake and replayed voices

## Voice Identity Verification & Watermarks

Matches the caller's voiceprint and cryptographic watermark to confirm they are who they claim to be

## Behavioral Style Matching

Compares speaking rhythm, word choice, and conversation patterns against the caller's known profile



Products & Integrations

aurigin.ai

# Protection for every voice channel in the organization

Add-ons for contact center solutions

GENESYS NICE

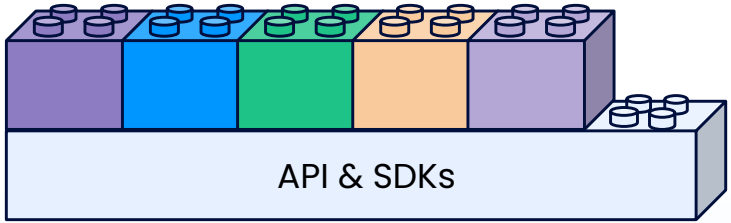
Desktop app

Browser plugin

Foundation for custom solutions

Add-ons for conferencing tools

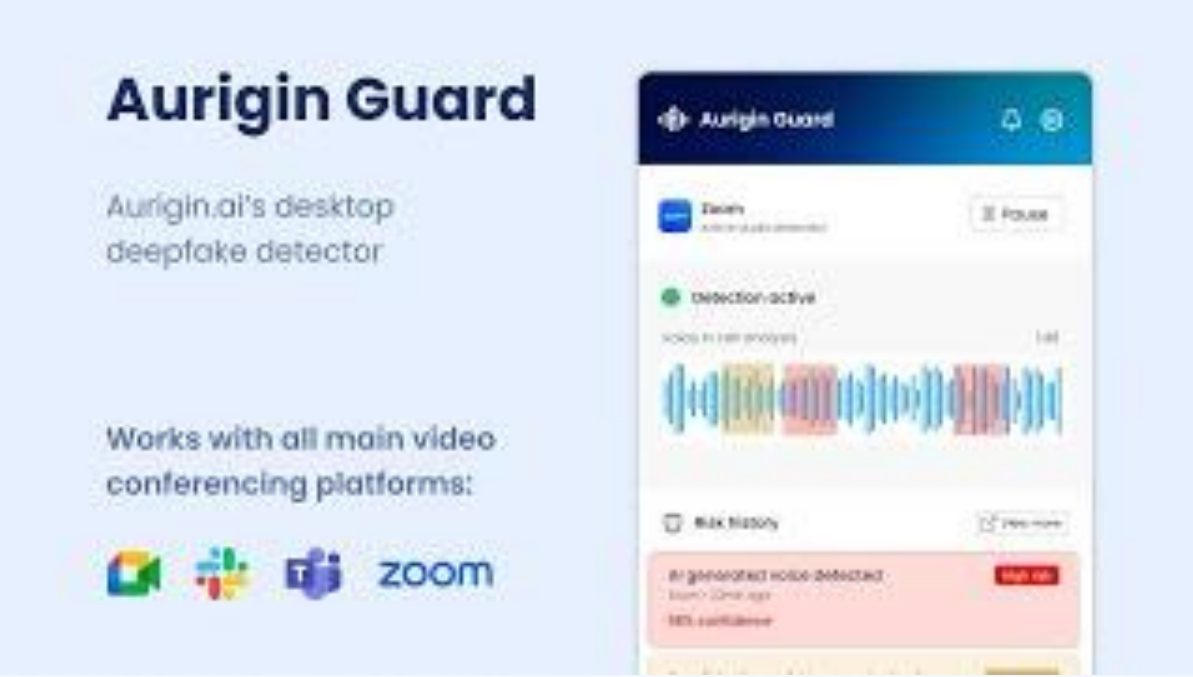
zoom



Demo

aurigin.ai

# AuriginGuard - Real-time voice security for enterprise communication




*Click to watch the demo*

Market leading technology

aurigin.ai

# Built to perform in enterprise context, when trust and timing matter most

**98%+**
Accuracy

**<50ms**
Latency

**On prem**
Deployment

**80+**
Supported languages

---

PHONEXIA

*"You have half the error rate than the next-best player we have evaluated you against."*
Chief Product Officer

ANTI AI

*"Testing showed Aurigin had best accuracy vs competitors"*
CTO

Telos Alliance

*"I ran the first files thru the web-based analyzer. The clone detection was impressive.*
DSP Software Engineer

ingenID
Biometric Innovations

*"You've achieved 96+% accuracy overall. So, quite good."*
CEO

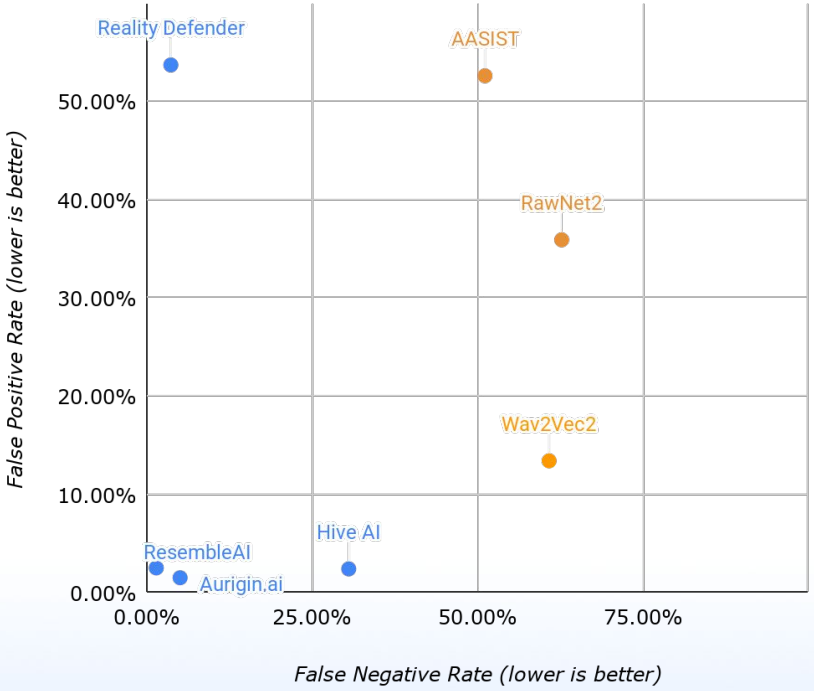
TRUSTED INFORMATION ALLIANCE

*"Having tested your tool and comparing it with the AI audio detection tools we regularly use, we are confident we can use it in our verification process."*
Deepfakes Analysis Unit

Podonos benchmark on audio deepfake detection technologies

aurigin.ai

# Independent benchmarks confirm our industry-leading accuracy




Source: https://www.podonos.com/blog/deepfake-audio-benchmark

**Top tier — Aurigin and Resemble lead the field:**

Two commercial APIs separate themselves clearly from the rest. Both are production-ready, both over 96 % accuracy, and both deliver F1 above 0.96. The choice between them depends on which error you can least afford in your deployment.

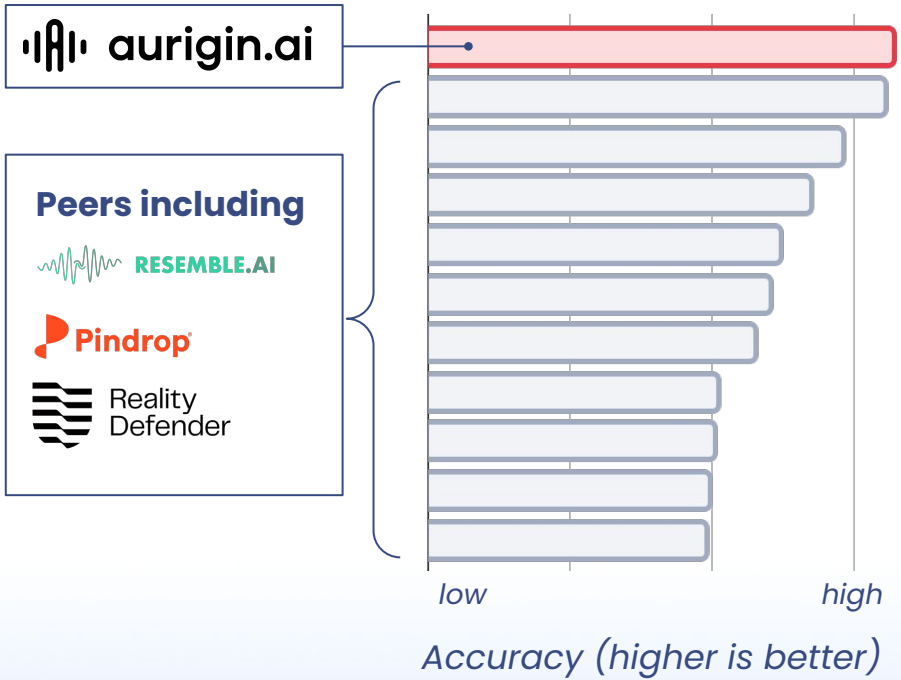
...

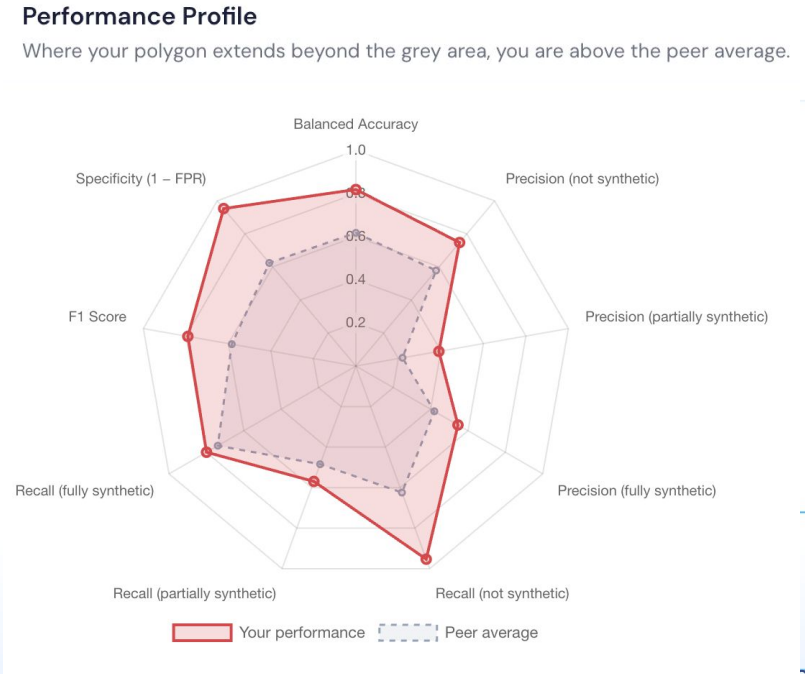
- **Aurigin AI — 96.75 % accuracy**, F1 **0.967**, **FPR 1.5 %.** Best at *protecting real audio*: only ~1 in 65 genuine clips is wrongly flagged. FNR is 5.0 %. Choose Aurigin when **false alarms on real audio are worse than missed fakes** — e.g. content moderation at scale, automated takedowns, journalist verification, anywhere a wrongful "fake" label is reputationally costly.

In short: **both are excellent**. They sit at opposite corners of the precision/recall trade-off, and the right pick is the one whose error profile matches the cost of mistakes in your application.

aurigin.ai

# Our models are top ranked in an independent benchmark by the UK government




Source: https://www.deepfakebenchmark.com

Partnerships

# Large tech players, telcos, and cybersecurity companies rely on our technology

aurigin.ai

## swisscom Reseller & MSP

Swisscom operates enterprise cloud, contact center, and collaboration environments (e.g. Microsoft Teams, Genesys) for enterprises in Switzerland. Aurigin can be deployed within Swisscom-managed infrastructure and integrated into end-customer communication and onboarding tools. Depending on the customer setup, Swisscom's role ranges from commercial ownership only (billing and contracting, with Aurigin operating the technology) to a fully managed service (Swisscom owning customer operations and support, Aurigin licensing the technology and providing model updates).

## EY Integration Partner

EY leverages its trusted enterprise relationships to identify exposure to voice fraud through vishing simulations, penetration testing, and employee awareness programs. Aurigin provides the technology (desktop app or integrations) and ensures technical deployment within the customer environment. EY then embeds the technology into business processes, controls, and operating models to ensure adoption and risk reduction at scale.

## PHONEXIA Technology Partner

Phonexia operates a voice biometrics platform used by contact centres and enterprises globally. Aurigin is integrated as a complementary layer to Phonexia's speaker verification engine, adding real-time deepfake detection to an existing identity stack. When a caller is verified, Aurigin simultaneously determines whether the voice is human or synthetic.

aurigin.ai

# Create your account today on Aurigin.ai - and test for free

Or get in touch

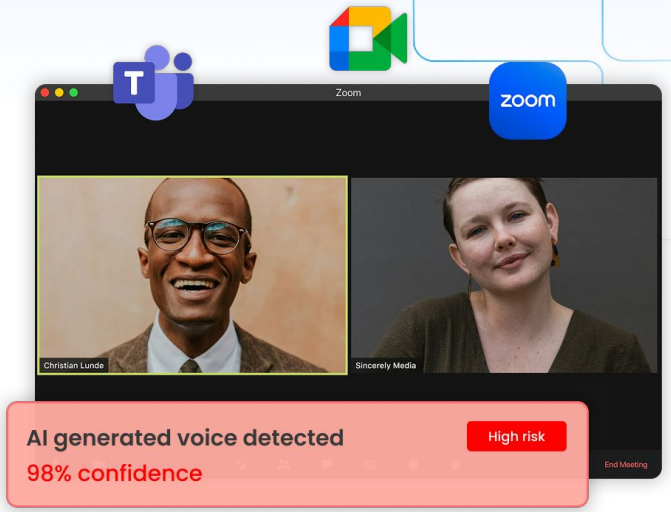
simon@aurigin.ai

AuriginGuard

aurigin.ai

# Real-time vishing protection for enterprise communication

Every call analyzed in real-time, silently without disrupting the conversation. When a threat is detected, the employee gets a clear alert.




### VIP/CFO impersonation

A cloned executive on a Teams call pressuring finance into a fraudulent transfer

### Fake interview candidates

An impostor using AI voice and video to fake their way through an interview

### Behavioral style matching

A fake client or supplier on Teams rerouting payments or changing mandates

- → Native desktop app or Teams, Zoom, Webex, Google Meet add-ons
- → On-premise, on-device and cloud options
- → SIEM/SOC logging out of the box
- → Minutes to deploy with a standard MDM push

*"In 2024, a deepfake video call convinced a finance employee to transfer $25M."* - Arup

AuriginShield

aurigin.ai

# The voice fraud prevention layer for contact centers and helpdesks

From IVR to human agents to post-call analytics. It integrates with your existing CCaaS, biometrics, and fraud tools.

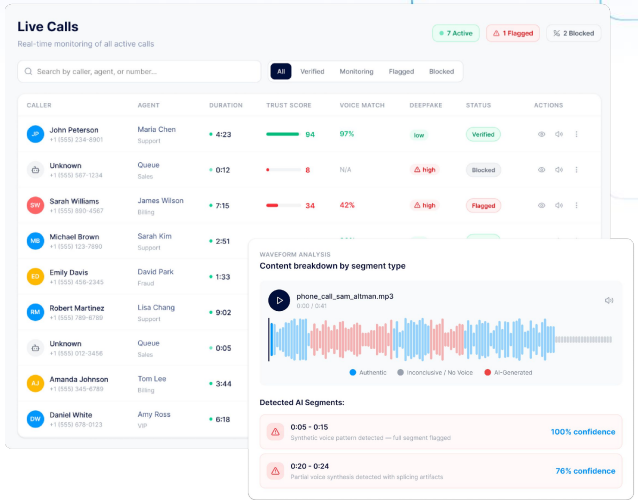
**Deepfake detection**
Real-time detection of AI-generated and cloned voices.

**Verified caller identity**
Confirms caller identity through voice biometrics and cryptographic audio signing.

**Bot filtering**
Identifies automated and synthetic callers before they reach an agent.

**Real-time trust scoring**
Every call gets a live risk score helping agents to question authenticity

**Compliance audit trails**
Meet the requirements from FINMA, DORA, EU AI act regarding deepfakes




→ Deployable in minutes on-premise or in the cloud

→ GRPc, REST API and add-ons for GENESYS and NiCE

**Stop fraud** **Cut handle time** **Pass audits** **Stay ahead**

*"There are still some financial institutions that will accept a voice print as authentication… That is a crazy thing to still be doing. AI has fully defeated that. I am very nervous that we have a significant, impending fraud crisis." – Sam Altman*

AuriginPhoneGuard

aurigin.ai

# The live AI scam detection for every phone call

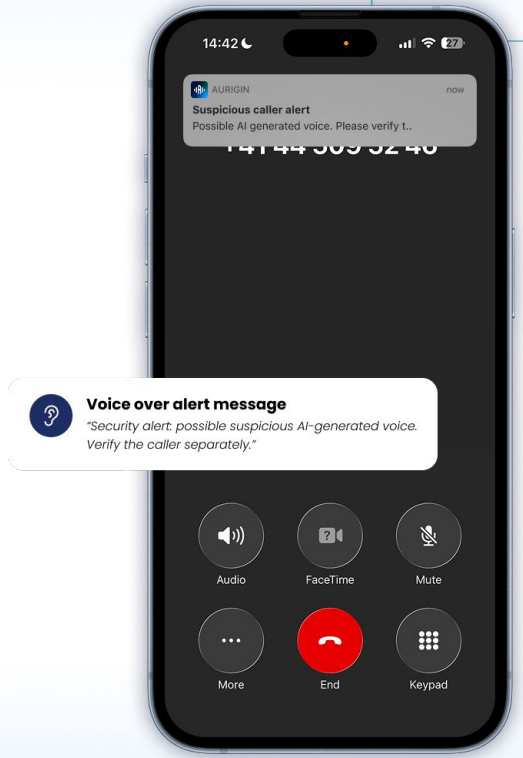
Detection runs transparently in the background. The moment a synthetic voice enters the line, the user hears a voiceover alert without breaking the conversation.

**Deepfake detection**
Real-time detection of AI-generated and cloned voices.

**Live voice alerts**
Spoken warning the moment a cloned voice is detected on the call.

**In-app or SMS notification**
Instant visual alert with details on suspicious caller

**History and logs**
Every alert is logged either to the app or to a SIEM system for analysis by the security team




→ Deployable in minutes as a docker container or as an iOS, Android app

→ Privacy is preserved as voice is analyzed live, with no conversation ever stored

*"The US FTC reported imposter scams cost consumers $2.7 billion in 2023, with AI voice cloning identified as a rapidly growing vector."*

AuriginInspect

aurigin.ai

# The forensic-grade audio deepfake detection platform for court proceedings and medias

From audio uploads to court-ready expert report with layered, explainable analysis backed by Aurigin's 98% detection accuracy.

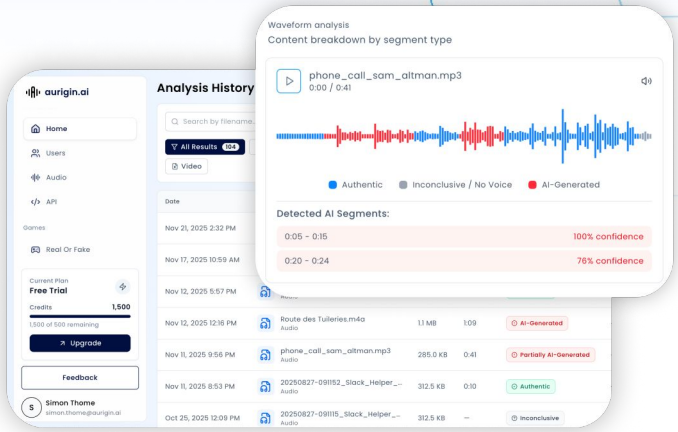
**Calibrated detection**
Likelihood ratio scoring for genuine vs synthetic with characterised uncertainty.

**Segment localization**
Time-stamped, region-by-region classification.

**Acoustic Attribution**
Ranked breakdown of cues driving each decision.

**Model transparency**
Model version, benchmark dataset, EER and Cllr metrics displayed.

**Forensic PDF report**
Structured report ready for expert witness submission.




→ Full chain of custody. Files signed and C2PA provenance chain.

→ On premise and cloud options

**Defend findings**

**Accelerate casework**

**Meet ISO 27042**

**Stay sovereign**

*"In a UK child custody dispute, a mother submitted a doctored audio recording to portray the father as violent and threatening attempting to deny him access to his children. The court could not initially verify whether the audio was genuine or fabricated." - The National (2020) · Berkeley Tech. L.J. (2025) · ISO/IEC 27042*

Business model

aurigin.ai

# Deployment and licensing models aligned with enterprise needs

## SaaS

per seat, per month

- ✓ Tiered pricing based on number of users
- ✓ Predictable costs as teams scale
- ✓ Unlimited usage during critical interactions

## Usage Based

per minute

- ✓ Pay-as-you-go or prepaid credit model
- ✓ Credits consumed per processing unit
- ✓ Supports system-level integrations at scale