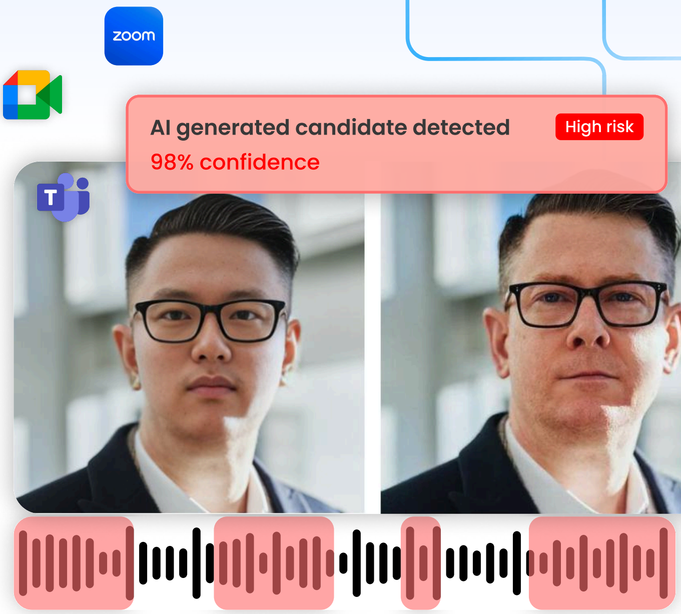
aurigin.ai

Hiring Fraud Prevention

Real-time detection of fake candidates in online interviews



Understanding the threat

Fraudsters use AI-generated LinkedIn profiles, resumes, and deepfakes to **create fake identities in online interviews**. They pose as legitimate professionals exploiting recruiters' trust, **wasting valuable time, draining hiring budgets, and gaining unauthorized access to internal systems or sensitive data.**

> *In 2024, cybersecurity firm KnowBe4 unknowingly hired a North Korean posing as a U.S. software engineer, who used deepfakes to install malware on a laptop during remote onboarding.*
>
> *Source: Cyberscoop*

Key challenges

- → Traditional background checks and video interviews **fail to spot AI-generated faces, cloned voices, and fake identities**
- → **Hiring pressure and talent shortages** let deepfake applicants slip through weak screening
- → **Recruiting and security teams often work in silos**, leaving identity verification gaps during onboarding.

1 in 4 candidate profiles will be fake by 2028

$250-600 million lost yearly to North Korean IT workers

15% of recruiters have seen deepfake activity

Sources: Gartner, Fortune, Study finds

Solution

Aurigin.ai enables organizations to **instantly verify candidate authenticity and stop deepfake hiring fraud** before it **wastes time, money, or damages trust.**

- → **Instant detection:** Identifies AI-generated voices in real-time
- → **Seamless Integration:** Works across Teams, Meet, Zoom, and enterprise hiring systems
- → **Continuous protection:** Monitors, alerts, and logs incidents for compliance and audit readiness
- → **Flexible deployment:** Cloud, on-prem, or isolated environments for full data privacy

98% accuracy | **40+ languages** | **<50ms latency**

EY swisscom 1291 GROUP venturelab VERIFYLABS.AI TRUSTED INFORMATION ALLIANCE

Aurigin.ai AG info@aurigin.ai www.aurigin.ai