imper.ai

SOLUTIONS BRIEF

Catch the candidate who isn't who they say they are.

Detect proxy interviewers and North Korean IT workers across every hiring touchpoint, before access is granted.

The hiring pipeline is now an attack surface

Remote hiring has created a new identity blind spot. Hiring teams are increasingly encountering candidates who are not who they claim to be; from North Korean IT workers (DPRK) to synthetic applicants and proxy interviewers to deepfake-assisted impersonation and coordinated laptop farm operations. As generative AI enables realistic voice cloning, deepfake video, and fabricated digital personas, traditional screening methods and interviews can no longer reliably assess whether the person engaging with your team is genuine.

imper.ai's Impersonation Detection Engine runs across every hiring touchpoint, application, screening, interview, offer, onboarding, and correlates infrastructure-layer signals across the full process. A candidate clean at screening but showing Astrill VPN and AnyDesk at the technical interview is flagged on the pattern. No documents. No biometrics. No new steps for recruiters.

Security Benefits

No documents, no biometrics
Infrastructure-layer signals only. Nothing to forge, nothing to deepfake, no PII exposure.

Cross-touchpoint correlation
Signals from application, screening, and interview are correlated,

Reduced insider risk exposure
Detects high-risk candidates before trust, access, or credentials are extended.

Operational Benefits

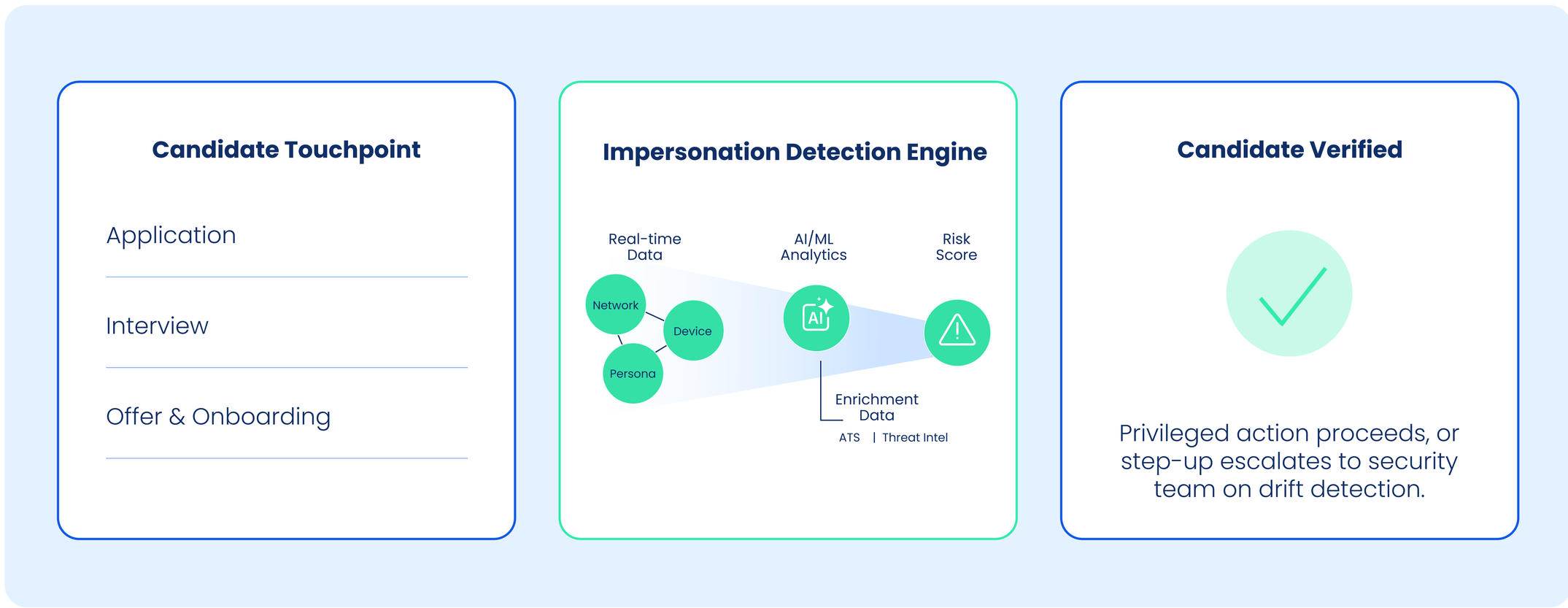
No new steps for recruiters
Embeds into existing ATS. Recruiter workflows remain unchanged.

Pre-credential prevention
Catches impersonation before access, credentials, or trust are extended.

Faster hiring decisions
Allows legitimate candidates to move forward without added steps or friction.

How imper.ai surfaces hiring fraud, without disrupting candidates

imper.ai analyzes infrastructure-layer signals (network, device, behavior) across every candidate interaction and correlates them with hiring context from your ATS. Risk surfaces in the recruiter's existing workflow. The candidate experience is unchanged. The Impersonation Detection Engine runs in the lobby of interviews on every platform.



1

Infrastructure signal capture

During every candidate touchpoint interviews, offer, even onboarding, imper.ai seamlessly captures network, device, and behavior telemetry No new step for the recruiter, no friction for the candidate.

2

Correlate across touchpoints

Signals from earlier interactions are correlated with later ones, plus ATS context. A candidate clean at screening but showing Astrill VPN and AnyDesk at the technical interview is flagged.

3

Generate a risk score

The Impersonation Detection Engine produces a real-time risk score from the correlated signals. The score reflects the likelihood that the candidate is operating from attacker infrastructure or is not the person they claim to be.

4

Hire or escalate

Low risk: the candidate moves through the funnel without added friction. High risk: the security teams are alerted before any offer or credentials are extended.

Candidate verified Hiring proceeds. No friction for the candidate. No manual review queue for the recruiter.

Impersonation risk detected Security reviews the signal evidence before credentials are extended.

Sample Detection Signals

- Anomalous & Unmatching Location
- Latency mismatches
- Virtual Audio Devices
- Virtual Machine
- Remote-Controlled Device
- Clean Device / Burner Environment

imper.ai was founded by cyberintelligence experts to stop workforce impersonation and social engineering attacks that route around authentication. Built specifically for workforce identity risk, the platform verifies the operator behind the account, not just the credential in front of it.

imper.ai

Get a demo →