Pindrop

Deepfake Readiness Checklist

Deepfakes and AI impersonations are making it harder to trust what you see and hear across everyday business interactions. Point-in-time authentication is no longer enough—identity needs to be verified continuously, in real time, not just at login. This checklist provides practical steps for making that shift across your enterprise.

1 Verify where your enterprise currently attempts identity verification with a one-time check

Audit which real-time business channels rely on static authentication (e.g., MFA, background check, login). Identify potential weaknesses in these channels, such as moments when identity is assumed, instead of verified.

WHY?

Identity is increasingly assumed in live interactions, creating exploitable gaps for impersonation and deepfakes.

2 Secure high-risk workflows beyond traditional IAM boundaries

For most enterprises, these interactions are potential vulnerabilities:

- Remote hiring and onboarding
- Vendor and third-party interactions
- IT helpdesk and password reset workflows
- Financial approvals

WHY?

Insider threats and fraudulent hires are rising due to weak identity verification in these flows.

3 Surface real-time risk signals to users and security teams

Deploy visible, in-session security indicators (e.g., alerts, risk scores, and participant analysis) that inform decision-making during interactions.

WHY?

Delayed detection is ineffective against fast-moving, AI-driven attacks occurring in live conversations.

4 Validate location and session integrity in real time

Continuously monitoring IP, geolocation, timezone mismatches, and VPN usage during sessions can flag anomalies dynamically rather than relying on pre-session checks.

WHY?

Attackers increasingly use location obfuscation to bypass controls and impersonate trusted users.

5 Strengthen participant authentication

Adopt voice biometric authentication, behavioral analysis, and device profiling solutions to verify that participants are not only human, but the correct individuals that show up for every interaction.

WHY?

Ruling out deepfakes is just one part of the equation. Enterprises must validate “right human” continuously, as well.

6 Align policies and trainings with AI-driven threat models

Update security policies to reflect:

- Deepfake-enabled impersonation
- AI-generated insider threats

Match enforcement mechanisms to these realities. Update security awareness training to include deepfake threats.

WHY?

With social engineering and internal threats, it’s imperative to inform employees of common signs of AI threats and train them on the tools they can use to catch them.

7 Deploy real-time deepfake detection across communication channels

Integrate tools, like Pindrop Pulse® for Meetings, that analyze audio and video streams live to detect synthetic media, voice cloning, and AI-generated personas. Focus on environments with high business impact from step 1: executive meetings, financial approvals, hiring interviews.

WHY?

AI-enabled fraud has surged by 1390% and is specifically targeting live interactions.[1]

Is your business ready to withstand AI attacks?
Speak to a deepfake defense expert today.

[1] Based on Pindrop customer data analysis from Q1 2026 in comparison to the previous five quarters.

pindrop.com | info@pindrop.com