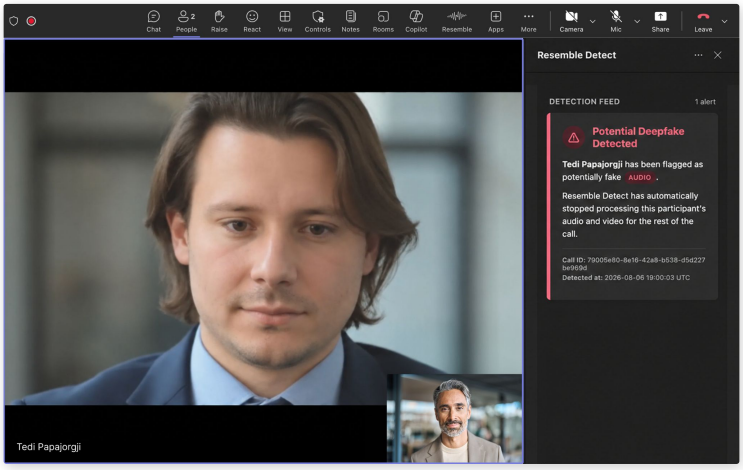
Resemble AI for Microsoft Teams

RESEMBLE.AI

Native, real-time deepfake detection for enterprise meetings.

Seeing and hearing someone on a video call is no longer enough. Attackers can now use AI-generated voice and video to impersonate executives, candidates, vendors, customers, and partners in real time.

Resemble Detect brings real-time audio and video deepfake detection into your Teams meetings, flagging suspicious participants while the call is happening, without adding an extra attendee.



RESEMBLE.AI | Microsoft Teams

Resemble helps security, fraud, compliance, and IT teams add a real-time trust layer where important decisions happen.

WHY IT MATTERS

Deepfake risk is moving from isolated scams into everyday business workflows:

- ✓ Executive impersonation and payment fraud
- ✓ Fake candidates and interview fraud
- ✓ Vendor, partner, and customer impersonation
- ✓ Sensitive meetings with external participants
- ✓ Identity swaps between interview rounds

KEY BENEFITS

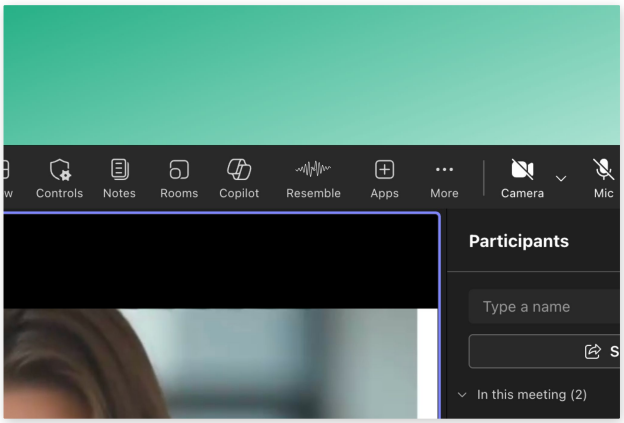
Detection without disruption
There's no bot in the meeting, so organizations can add detection without changing how people join and run meetings. A visible bot is available if you need one.

Protect high-value meetings
Add real-time AI media detection to interviews, executive calls, vendor reviews, customer escalations, board meetings, and financial approval workflows.

Give security teams usable signals
Detection results are delivered in the meeting flow and can also persist through activity notifications and post-call summaries for review and escalation.

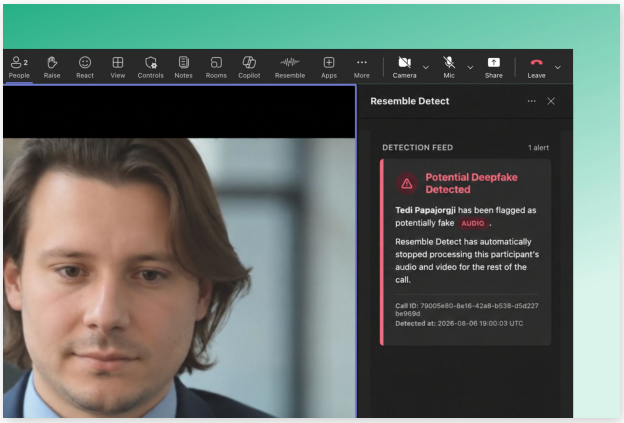
How it works in Microsoft Teams

Teams-native experience — Resemble Detect appears inside Microsoft Teams as a pinned app experience for enabled users. **No separate meeting bot is required but is available to add at anytime.**



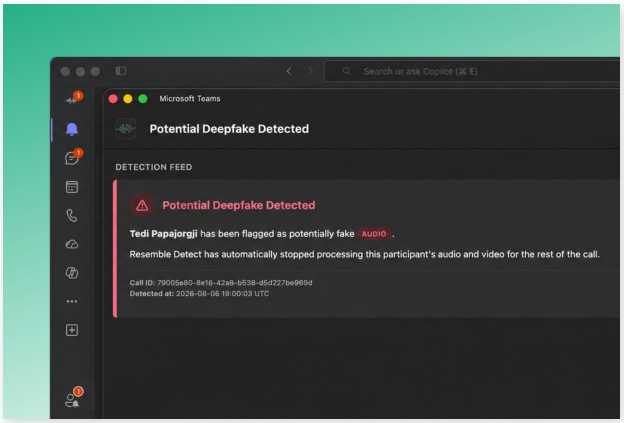
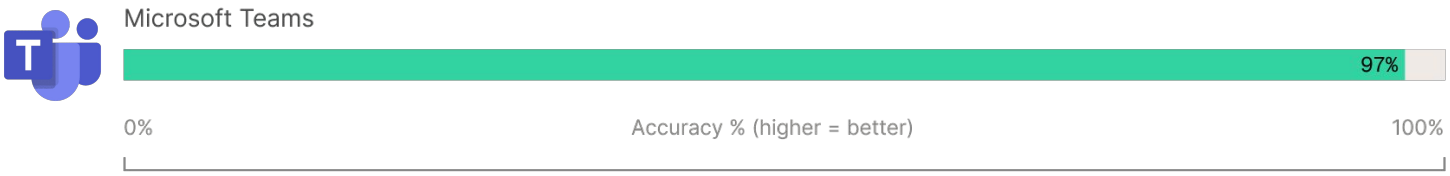
Live audio and video analysis — During a Teams meeting, Resemble analyzes participant audio and video streams for signs of synthetic or manipulated media. Detection results can identify whether a participant's audio or video appears real or fake.

Identity matching across calls — Resemble recognizes the people you've enrolled by face and voice, and flags it when the name on screen doesn't match the person on camera.



Real-time alerts where users already work — When suspicious media is detected, users can receive alerts through multiple Teams surfaces making high-risk detections hard to miss, both during and after the meeting.

Admin-controlled deployment — IT and security admins can manage deployment and rules through the Resemble dashboard and Microsoft Teams admin controls. Supporting targeted deployments for teams such as security, finance, HR, executive staff, procurement, and customer-facing teams.



Privacy-conscious architecture — Only the audio and video of participants flagged as suspicious are kept, so your security team can review them. Everyone else's is discarded.