SOLUTION BRIEF

IRONSCALES

# Deepfake Protection for Microsoft Teams

**Detect AI Impersonations, Verify Meeting Participants, and Stop Video-Enabled Fraud**

Deepfake Protection for Microsoft Teams is an AI-powered security solution that detects and prevents live video impersonation attacks during virtual meetings. By analyzing video streams, voice patterns[1], and behavioral biometrics[1] in real-time, the solution identifies AI-generated content and synthetic media used in business email compromise (BEC) and executive impersonation schemes. This multi-layered approach protects organizations from sophisticated fraud attempts during critical business communications.

## IRONSCALES Deepfake Protection

IRONSCALES provides enterprise clients with advanced detection capabilities that seamlessly integrate with Microsoft Teams, eliminating the risk of AI-driven impersonation attacks during live meetings and video calls.

### Key Features:

- **Live Meeting Artifact Detection:**
  Scans video and audio streams[1] in real-time to detect AI-generated flaws—pixel inconsistencies, compression anomalies, and synthetic patterns that expose deepfakes during Teams calls.
- **Biometric Identity Verification**
  Confirms participant authenticity using facial recognition, voice signatures[1], and behavioral biometrics[1].
- **Behavioral Context Analysis[1]**
  Learns normal communication patterns and interaction history to flag subtle deviations that expose AI-driven fraud, especially during sensitive requests like wire transfers.
- **Privacy-First Architecture**
  Uses vector-based mathematical representations instead of storing recordings or transcripts—analyzing signals, not content—to protect employee privacy while detecting threats.

## The Challenge:

- 50% of organizations experienced deepfake fraud in 2024, up from just 29% two years ago (according to Regula's research of 575 global decision-makers).
- Traditional security tools can't detect synthetic media, with 44% of businesses reporting low confidence in their deepfake detection capabilities.
- The barrier to entry has collapsed, open-source AI tools makes it easy for criminals to create convincing deepfakes.

## How Deepfake Protection Works:

1 **Continuous Monitoring**
Monitors all Teams meetings, capturing video and audio streams for real-time analysis without recording content.

2 **Multi-Layer Analysis**
Simultaneously analyzes three threat vectors (visual artifacts, voice authenticity[1], and behavioral patterns[1]) using AI models trained on millions of deepfake samples.

3 **Alert & Investigate**
Notifies meeting participants when an external participant shows synthetic media indicators, while alerting security admins via email and the admin console to investigate and respond.

[1] Planned enhancements currently in development and subject to change. Contact your account manager for timing and early access opportunities.

## Benefits:

- **Real-Time Meeting Protection:** Stops sophisticated impersonation attacks during live Teams calls, preventing fraudulent wire transfers and unauthorized approvals before they happen.
- **Trust in Virtual Decisions:** Ensures authentic participation in critical business meetings, protecting board discussions, M&A negotiations, and financial authorizations.
- **Privacy-Preserved Security:** Uses mathematical vectors instead of storing recordings or images—protecting employee privacy while detecting deepfake threats.
- **Reduced Attack Success:** Makes your organization a harder target by protecting high-value executives and finance teams that criminals frequently impersonate.
- **Seamless Teams Integration:** Works within your existing Microsoft 365 environment without disrupting workflows or requiring separate authentication apps.

## Why IRONSCALES for Deepfake Protection?

Unlike standalone deepfake detectors, IRONSCALES integrates live video protection into our comprehensive email security platform—combining visual, audio, and behavioral analysis with our decade of experience stopping BEC and impersonation attacks.

This unified approach means you're not just detecting synthetic media; you're understanding the full attack chain from initial phishing to live impersonation attempts, all within the Microsoft 365 environment your teams use daily.

IRONSCALES Deepfake Protection provides the adaptive, privacy-first defense organizations need to maintain trust in business communications.

## The Numbers:

2X Deepfake Exposure has roughly **doubled in two years**, ~50% of businesses report audio and video deepfake attempts increase from 2022 to 2024.

60% of IT professionals say deepfake defense will rank as their organizations' **top security priority** in the next 12-18 months.

53% of IT professionals believe email represents an "extreme threat" as a channel for deepfake-driven attacks, **surpassing all other avenues**, including social media and messaging apps.

## About IRONSCALES

IRONSCALES is the leading cloud email security platform for the enterprise and the industry's only solution that uses Adaptive AI and human insights (HI) to stop advanced phishing. Its award-winning, self-learning platform continuously detects and remediates attacks like BEC, ATO, and VIP impersonation that bypass traditional security solutions. Powerful, simple, and adaptive, IRONSCALES helps enterprises protect better, simplify operations, and empower the organization. IRONSCALES is headquartered in Atlanta, Georgia, and is proud to support more than 17,000 global enterprises. To learn more, visit www.ironscales.com or follow us on X @IRONSCALES.

IRONSCALES

IRONSCALES.COM