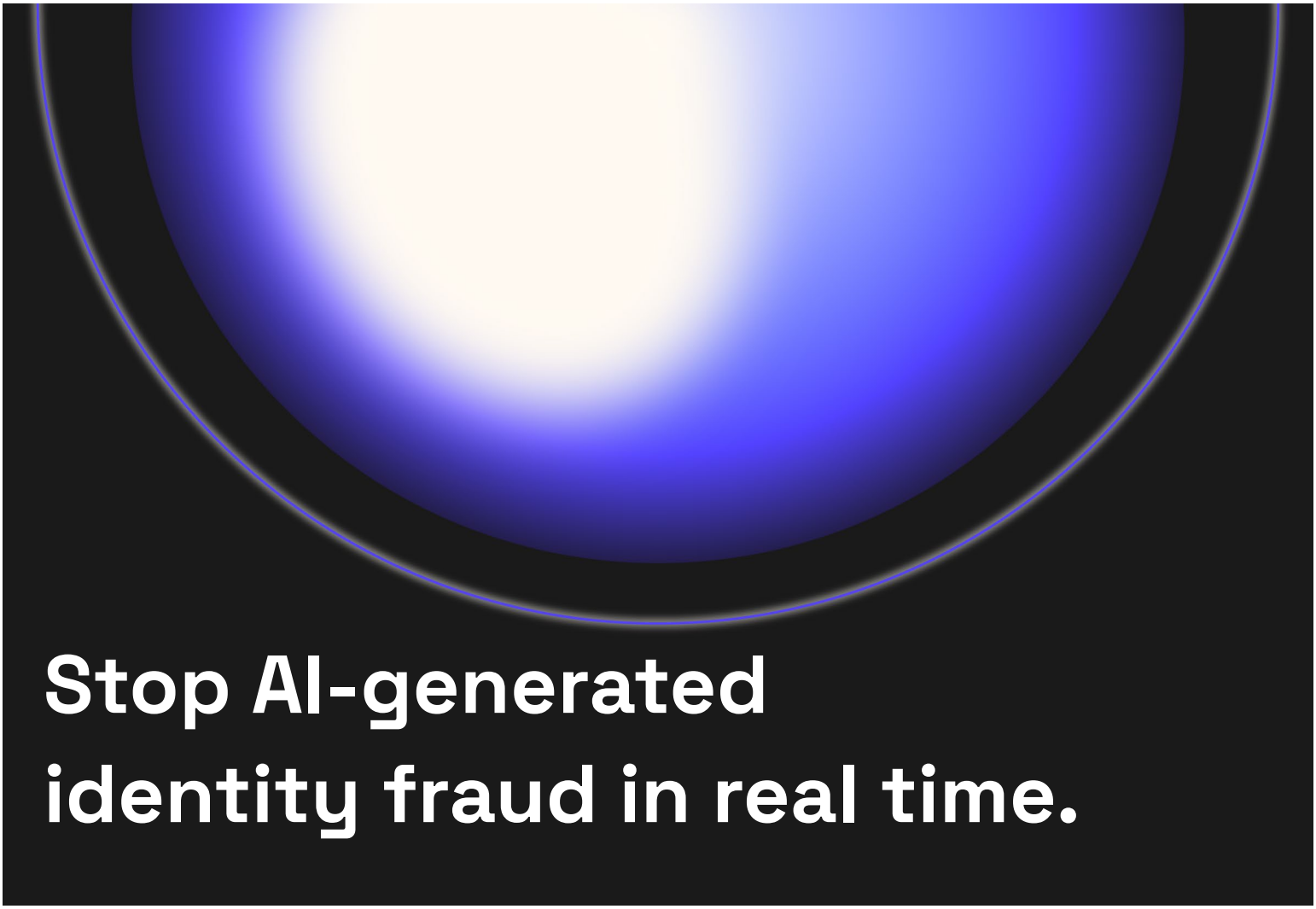
Reality Defender

1KOSMOS



Stop AI-generated identity fraud in real time.

1Kosmos has partnered with Reality Defender to integrate real-time deepfake detection into identity verification and authentication workflows. This partnership strengthens fraud prevention as AI-generated attacks become increasingly sophisticated, securing the identity verification ecosystem with industry-leading deepfake detection technology.

Advanced deepfake detection meets biometric authentication

Modern identity fraud requires multiple layers of protection; facial recognition, liveness detection, presentation attack detection, and injection attack protection all working together.

> **1Kosmos has integrated Reality Defender's deepfake detection into its identity platform to stop AI-generated and-manipulated biometric content in real time.**

The Reality Defender advantage

Detection without dependency on content source
Identifies AI-generated content without requiring face prints, voice prints, or PII. Verifies authenticity of any biometric input regardless of generative AI tool, camera source, or whether content is injected, not limited to watermarked content only.

Complete identity flow protection
Multimodal deepfake detection across images, video, and audio. Protects entire onboarding and authentication workflows with a single integration, eliminating blind spots across presentation and injection attacks.

Protection against tomorrow's attack vectors
Models are continuously blended, tested, and updated monthly to anticipate emerging deepfakes. Ensures verification systems stay ahead of evolving generative AI tools without requiring constant integration rebuilds.

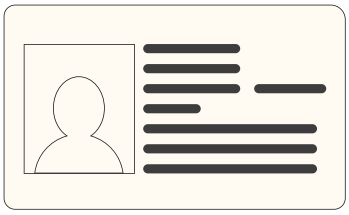
Deploy where your data lives
Flexible deployment options including API integration, on-premises, containerized cloud, and private cloud environments. Meets strict compliance and data residency requirements for financial institutions, government agencies, and global enterprises.

Biometric fraud attempts

Deepfakes now represent 40% of all biometric fraud attempts

Integration use cases

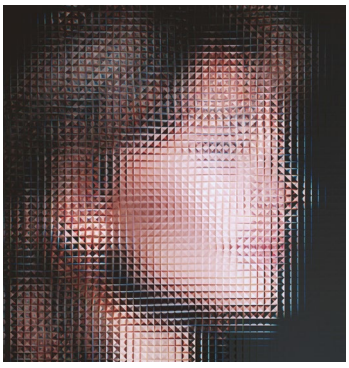
Identity verification
Reality Defender checks for deepfakes when users present selfies during ID verification.



1. Capture ID front

2. Capture ID back

3. Capture selfie



4. Check liveness

5. Reality Defender deepfake check

6. Result

Popular types of AI-generated/ manipulated content detected
Detection results feed into the 1Kosmos fraud detection engine as an additional trust signal.

Face-swaps

Diffusion-model outputs

GAN-generated images

Authentication (Live ID login)
Anytime a face is used for authentication or login, Reality Defender automatically checks for AI manipulation during the authentication process.

How the integration works

Reality Defender integrates directly into identity verification systems as an added security layer, scanning images and videos during customer onboarding and authentication. The API is called at the point of facial image capture, instantly flagging synthetic impersonations before fraudsters gain access.

Current deployment

Reality Defender is already deployed across multiple enterprise verticals and Allied government customers. All customers using 1Kosmos identity verification now have Reality Defender's deepfake detection in place, strengthening existing fraud prevention capabilities.

Integration method	
Integration method	API
Analysis	Real-time during verification flow

Response time	
Photo	1-3 seconds
Video	~2x video length (conservative estimate)

Input format
Request a signed URL and upload file using file path
Accepted formats: Single image, multiple images, or short videos
Minimum face size: 100 pixels between ears

Output format
Returns requestID upon upload
Use requestID to retrieve JSON response with status, score, and model breakdown
Classification: Manipulated / Authentic
Confidence score: 1%–99% (Note: percentage indicates confidence of manipulation; 1%=Authentic, 99%=Manipulated)