



BIOMETRIC SOLUTION SUITE

Liveness Detection

Generative AI and crime-as-a-service networks give attackers the tools to bypass customer identity systems, open fraudulent accounts, or take over existing ones.

Liveness detection confirms users are real during the biometric capture stage of identity verification and subsequent authentication touchpoints. Gartner states the technology is “critical for defending against deepfakes and verifying the genuine presence of an individual.”

iProov Liveness technologies deliver proven, NIST SP 800-63-4-aligned protection against presentation, injection, and deepfake attacks. Using layered defenses, strengthened by ongoing threat intelligence, the solution combats fraud while providing effortless access for genuine users.



Calibrate Identity Assurance to Risk

Express Liveness

Confirm it's a real person in a near-instant face capture. No user action required.

Presentation Attack Detection

Injection Attack Detection



Express and Dynamic share one SDK. Switch between them based on your risk engine signals, regulatory context, and threat landscape.

Dynamic Liveness

Confirm users are genuinely present with a unique, passive challenge response

Presentation Attack Detection

Injection Attack Detection

Advanced deepfake detection

Be Audit Ready With Liveness That Meets NIST SP 800-63-4

Presentation Attack Detection

Conformant with iBeta Level 1 and 2 and FIDO Alliance Face Verification Certification for presentation attack detection, including presented deepfakes.



Injection Attack Detection

Conformant with CEN TS 18099, independently tested against synthetic media attacks that bypass device-side sensors entirely.

Accessibility and Inclusion

Conformant with W3C WCAG 2.2 AA and Section 508. The UX drives high pass rates for all users, irrespective of capability, age, gender, skin tone, or face type.

Stay Ahead of Evolving Threats

The iProov Security Operations Center (iSOC) ensures the ongoing resilience of Express and Dynamic Liveness as attacks evolve.

We monitor customer traffic for signs of attack. Suspicious activity is raised to threat intelligence experts who identify novel attack patterns and adapt defenses at speed.

As part of a defense network, every customer benefits from global threat management. A novel pattern detected against a customer in Singapore strengthens defenses for customers in the U.S.A.

Automated threat updates are launched to the cloud, meaning customers remain protected against future threats without having to invest any engineering resources.

Deliver Reliable Performance Across Users, Regions, and Devices

98.5%
Pass rates

1.08
Attempts to Pass

25,000+
Device Types

99.99%
Uptime



[Book a Demo](#)



iproov.com