



Injection Attack Resilience in Liveness: Proven, Not Assumed

Independent evaluation aligned to CEN/TS 18099: the injection attack testing framework for biometric systems

Many liveness solutions in the market are validated for Presentation Attack Detection (PAD), such as photos, videos, masks, and replay attempts shown to a camera. That testing matters, but it does not address today's fastest-growing threat: **injection attacks**, where attackers bypass the camera entirely and inject manipulated biometric imagery into the system, via virtual cameras or data stream manipulation, often using virtualized environments.

The issue is simple: **many vendors lack independent, standards-aligned testing to verify their injection attack mitigation claims.** When controls aren't proven, injection attacks go undetected, fueling account takeover and identity fraud.

Why PAD Testing Isn't Enough

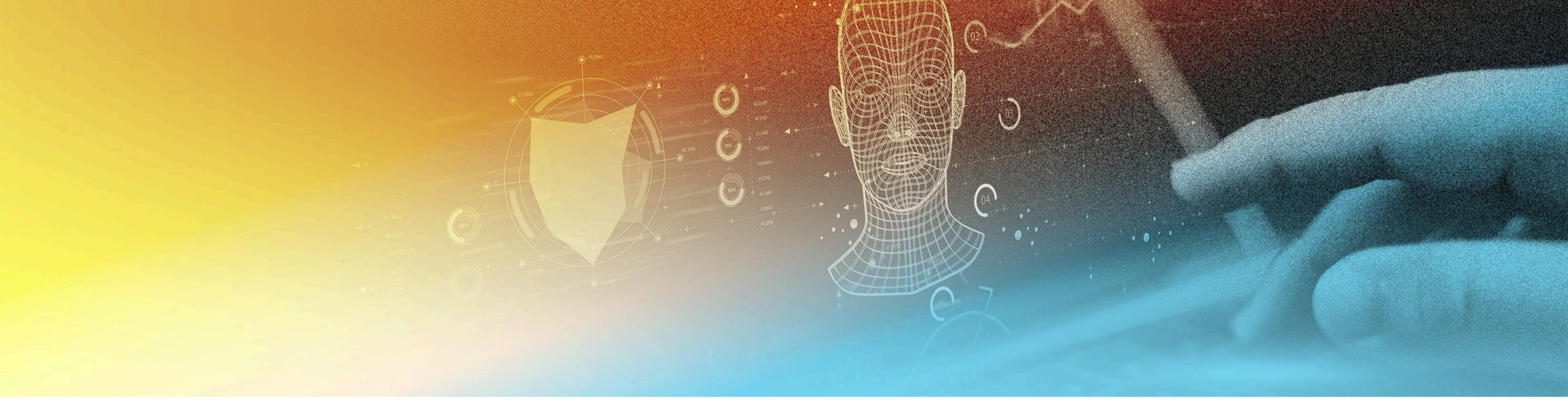
While ISO/IEC 30107 focused on physical spoofing and presentation attack detection, injection attacks that bypass the camera are out of scope for ISO 30107. A vendor can be PAD-conformant and still have no independent, standards-aligned proof of injection attack resilience.

Organizations MUST Demand Standards-Aligned Injection Attack Testing

Standards-aligned injection attack testing reduces silent fraud risk and provides audit-ready proof, avoiding costly late fixes that increase friction and disrupt roadmap delivery.

iProov Independently Tested to CEN/TS 18099: Biometric Data Injection Attack Detection

Independent Evaluation	Evaluation Level
Test Lab Ingenium Biometric Laboratories (ISO/IEC 17025 accredited)	Level 4 IAD Evaluation exceeding the Level 2 High in scope and rigor
Solution iProov Dynamic Liveness	Effort >40 days
Scope Injection Attack Detection/resilience aligned to CEN/TS 18099	Attack Scope >3 Injection Attack Methods (IAMS), >15 Injection Attack Instrument (IAI) species
	Legitimate User Experience BPCER ~1.3%



Independently Proven, Standards-Aligned Injection Attack Mitigation

iProov Dynamic Liveness, tested by an ISO-accredited lab, stops injection attacks while providing an effortless experience for legitimate users.

- Verified High-Level Security**
 Evaluated at Ingenium Level 4, exceeding the CEN/TS 18099 "High" level, confirming resilience to digital injection attacks.
- Stop the Attack at the Gate**
 iProov's Dynamic Liveness system is so robust that it successfully prevented the establishment of the Injection Attack Methods (IAMS) themselves (Android emulator, library exploit, networking attacks, and function hooking). If the method cannot be established, the attack instrument (the forged image or video) cannot be delivered.
- Depth of Security**
 Preventing Injection Attack Methods represents the first line of defense in a multi-layered security approach, designed to secure resilience as attacks evolve.
- Low Friction for Legitimate Users**
 Security is achieved without compromising usability. The Bona Fide Presentation Rate (BPCER), the rate at which legitimate users were rejected, was 1.3%, easily meeting the required maximum of 15%.

iProov has independently proven injection attack resilience through ISO-accredited CEN/TS 18099 testing, alongside FIDO Face Verification Certification for PAD. iProov is also the first vendor to meet the updated biometric verification requirements in NIST SP 800-63-4. These Digital Identity Guidelines strengthen protections against deepfakes and AI-driven threats, making iProov a strong fit for high-assurance, regulated identity deployments.

Independent standards-aligned testing to CEN/TS 18099 is paramount. Always ask for proof.

Read the iProov CEN/TS 18099 injection-attack evaluation announcement, or contact us to see the independent CEN/TS 18099 testing report by Ingenium Laboratories.

- [Read more](#)
- [Contact us](#)

