



Biometrics Identity Experience & Evaluation Laboratory

## Letter of Confirmation

Issued to Advance.AI

for the test report issued on the 29<sup>th</sup> of May 2026 for  
Injection Attack Detection (IAD) evaluation of,  
Liveness Detection SDK iOS v8.5.7 and Android v4.1.5

To whom it may concern,

BixeLab (NVLAP Lab Code: 600301-0) is accredited by the NIST-administered National Voluntary Laboratory Accreditation Program (NVLAP) to ISO/IEC 17025:2017 for services listed on its published scope. NVLAP does not currently accredit Injection Attack Detection (IAD) to CEN/TS 18099. This evaluation was therefore conducted in close alignment with CEN/TS 18099, but it does not constitute an NVLAP-accredited outcome.

Between 5<sup>th</sup> May and 21<sup>st</sup> May 2026, BixeLab conducted an independent IAD evaluation of Advance.AI Liveness Detection SDK iOS v8.5.7 and Android v4.1.5. The evaluation's injection attack methods (IAMs), and injection attack instruments (IAIs), across Android and iOS environments were used to assess the system's resilience under controlled test conditions.


### Testing parameters

- **Platforms:** Android 15, iOS 26.3
- **Injection Attack Methods (IAMs):** Virtual-sensor injection (OBS virtual camera and HDMI/USB capture card), device emulation (Android Studio), rooted-device execution with root-state masking, function hooking to confirm root-masking concealment.
- **Injection Attack Instruments (IAIs):** Ten representative species – Selfie image, passport image, posed photo, video, face morphed image, face swap image, deepfake video (MyHeritage), deepfake video (DeepLiveCam), face reenactment video (LivePortrait), 3D avatar reenactment video (LargeAvatarModel).
- **Bona fide runs:** 100 total, User-level BPCER of 10%.
- **Injection Attempts:** 600 IAI transactions delivered through virtual-camera (OBS, 300 transactions) and USB-camera (HDMI capture, 300 transactions). These transactions were rejected, failing to pass liveness challenges. Hooking functions confirmed that magisk rooted android devices partially evaded detection.
- **Integrity & Environment Controls:** Integrity & environment controls: All tests were executed under controlled conditions at BixeLab's Griffith (ACT) laboratory using predefined test devices and toolchains. Root detection, emulator detection, and Magisk-presence checks were active; concealment attempts using Magisk were partially successful in root concealment.

### Conclusion

Within the scope of executed testing, no successful sensor-level injection bypass was observed. The application's tamper-detection routines, and root-state checks were partially circumvented however no IAIs could be injected. Against the IAMs and IAIs tested, all 600 capture injection transactions failed to overcome liveness challenges. Improvements to root detection is recommended. See full details in the test report (26\_BXL061\_TR\_01).

  
-----  
Ms. Somya Singh  
General Manager  
BixeLab Pty Ltd  
info@bixelab.com

  
-----  
Dr. Ted Dunstone  
Senior Responsible Officer  
BixeLab Pty Ltd  
info@bixelab.com

*NOTE: This letter is a validation summary only i.e., this was not a certification, benchmark, or endorsement by NIST, NVLAP, or any government agency. The results apply only to the stated versions, configurations, datasets, and conditions; coverage is limited to the tested IAMs/IAIs, it may be reproduced only in full, and BixeLab accepts no liability for use beyond the stated purpose.*