



Biometrics Identity Experience & Evaluation Laboratory

Letter of Confirmation

Issued to Aware.
for the test report issued on the 30th of April 2026 for
Injection Attack Detection (IAD) evaluation of,
Aware FaceLiveness v4.22

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 IAD to CEN/TS 18099; this evaluation was conducted in close alignment with CEN/TS 18099, but does not yield an NVLAP-accredited outcome.

Between 7th April and 30th April 2026, BixeLab conducted an independent Injection Attack Detection (IAD) evaluation of Aware FaceLiveness v4.22 (build 147). The evaluation representative injection attack methods (IAMs) and injection attack instruments (IAIs) across Android and iOS environments to assess the system's resilience under controlled test conditions.

Testing parameters

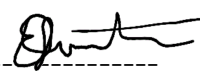
- **Platforms:** Android 13, iOS 18.5.
- **Injection Attack Methods (IAMs):** Virtual-sensor injection (OBS virtual camera and HDMI/USB capture card), function hooking of camera-controller selection and tamper-detection telemetry, device emulation (Android Studio), rooted-device execution with root-state masking, and exploratory API-layer interception (iOS, out of formal IAD scope; see Appendix A of the test report).
- **Injection Attack Instruments (IAIs):** Ten representative species – 3D avatar video (LargeAvatarModel), face reenactment video (LivePortrait), face-morphed image, face-swapped image, passport image, posed photo, selfie image, selfie video, deepfake video (MyHeritage), and deepfake video (DeepLiveCam).
- **Bona fide runs:** 300 total, BPCER of 0%.
- **Injection Attempts:** 600 IAI transactions delivered through hooked virtual-camera (OBS, 300 transactions) and hooked USB-camera (HDMI capture, 300 transactions) capture paths returned a SPOOF decision in 100% of cases. Attempts to defeat tamper-detection telemetry through function hooking of the emulator_data field, and to mask root state on a Magisk-rooted device, did not produce a LIVE outcome.
- **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 Frida-presence checks were confirmed to be active; concealment attempts using Magisk modules and Frida-based root masking did not defeat detection

Conclusion

Within the scope of executed testing, no successful sensor-level injection bypass was observed. The application's camera-controller selection logic, tamper-detection routines, and root-state checks operated as intended against the IAMs and IAIs tested, with all 600 hooked-capture injection transactions returning SPOOF. Improvements to log granularity – specifically, distinguishing IAD signals from PAD signals in the back-end Decision field – would strengthen the evidentiary value of future evaluations. See full details in the test report (26_BXL053_TR_01).



Ms. Somya Singh
Operations 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.