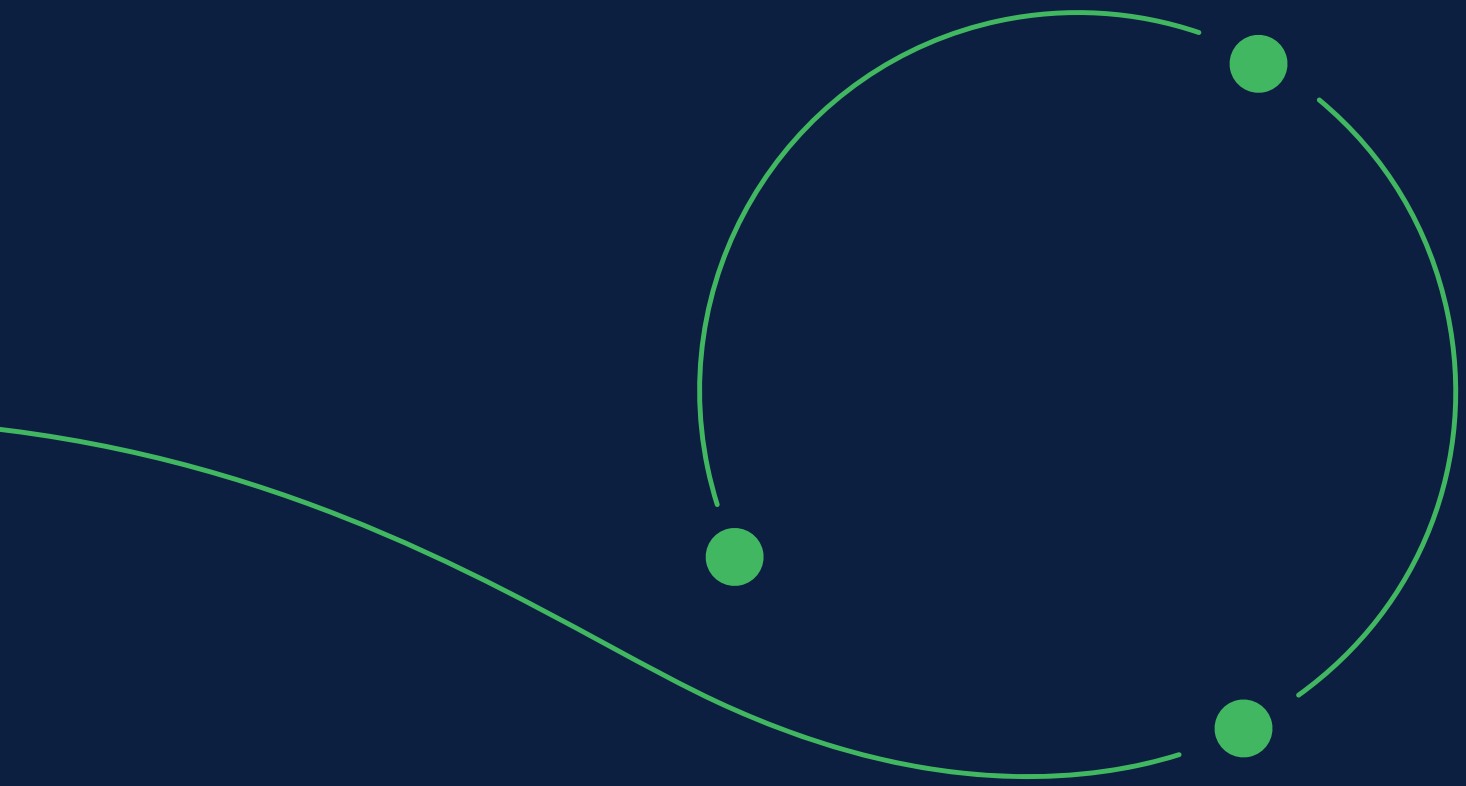
INNOVATRICS

DOT

What do you need to know when choosing your facial liveness vendor?

White Paper

Liveness Detection



innovatrics.com

Why Having the Right Technology Partner Matters

Video calls instead of branch visits revolutionised banking with the arrival of new players like Revolut or N26. Nowadays, facial biometrics with state-of-the-art liveness checks renders this approach obsolete, similarly affecting other industries.

Many businesses and even governments are now starting to use a combination of facial recognition and liveness detection to safely and securely verify our identity online. It is important that you can trust this technology and not worry that an impostor with your photo in his hands could misuse your identity online.

In this paper
We will list the important questions you need to answer when choosing your facial liveness vendor. Having the right technology partner is critical to establish lasting trust with your clients.

Can Biometrics Prove Someone's Liveness?

Algorithms can now verify the identity of a person faster **(500 ms human vs. nanoseconds algorithm speed)** and more accurately **(93 % human vs. 99+ % algorithm accuracy[1])** than humans can. More importantly, they can do this any time and at any scale.

However, one issue has made branch visits and video calls necessary – **making sure that you are communicating with a live person.**

Detecting if your new customer is genuine or just a sophisticated attacker has led to the development of Presentation Attack Detection (PAD).

[1] https://bit.ly/3g7khAI
https://bit.ly/34IF2NQ
https://bit.ly/3pfO1iV

Liveness Detection: What Are My Options?

Liveness check uses various biometric measurements to ascertain that we are dealing with a real live face and not a replica in any form. There are several ways to do this.

Active Liveness Will Only Take You So Far

The more traditional approach of verifying liveness relies on asking customers to perform an action. This can include nodding, moving eyes, blinking, smiling, moving head, moving the device, or speaking.

Although these tasks may seem trivial, they still can be a challenge for some users as randomness is essential for stronger security. Even if the set of actions can be done anywhere, it takes some time to perform them which can lead to a higher abandonment rate.

Since active liveness check can easily be fulfilled, it can, unfortunately, be simple to spoof (e.g., a photograph of a smiling person works just as well as the real person asked to smile to pass a liveness check).

Performing Passive Liveness the Right Way

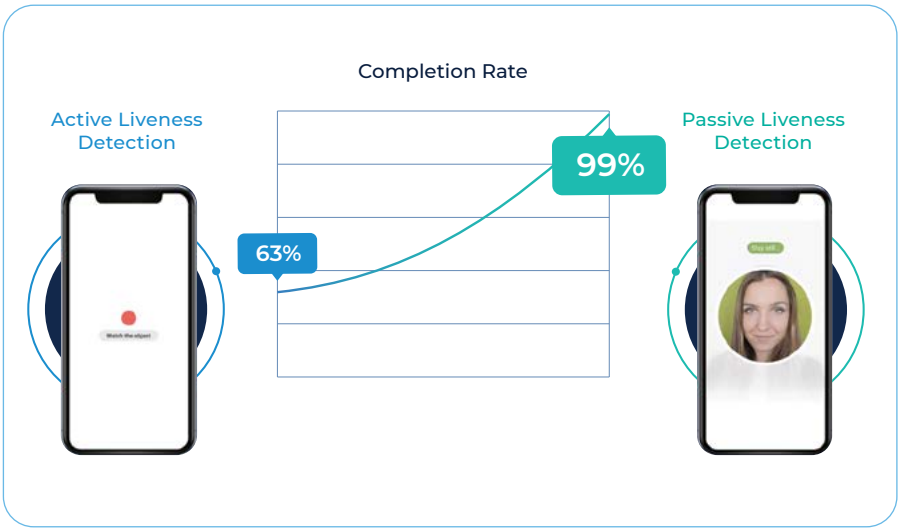
Going down the quasi-passive way, such as shining various lights at a user's face, **is not the way to go.** You want to check for liveness without the customer ever noticing it. This serves two purposes.

First, **it makes the interaction simple. Second, it makes it hard to spoof** as the attacker does not even know if and when liveness verification has transpired.

Innovatrics passive liveness algorithm can perform liveness verification from just one image. Designed with optimum efficiency, it can run on end user devices such as mobile phones or embedded terminals.

While active liveness detection compares the position of several dozen points on a face, a passive approach takes into account hundreds of variables.

Innovatrics passive liveness delivers 99% digital onboarding completion rate for new customers of a consumer finance provider in Asia.



What Are Typical Presentation Attacks?

To catch a fraudster, you'll have to think like one. If you successfully trick a company into believing you are someone else, you might get a loan and never have to pay it back. Check out some of the ways on how to deceive a system as shown in the table.

On top of these, there are 2D and 3D images on high definition screens, puppets, wax heads, sculptures, or even robotic heads with fake muscles.

It's hard enough dealing with one person staging an attack once in a while. Imagine having hundreds of attackers generating thousands of such attempts every single day.

Type of attack	What you need as an attacker	How to stop it
Print attacks	Stolen ID and printed image of the person from ID	Verification of the ID image vs the selfie, rejecting obvious frauds (e.g., the same image on the ID as in the selfie); Active and/or Passive liveness check
Screen attacks	Stolen ID and digital picture or video of the person from ID	Active liveness check, Passive liveness check
Deep Fakes (projecting a moving face of someone else in real-time)	Stolen ID, several photos and/or videos of the person from ID, basic technical knowledge, powerful computer for deepfake training	Basically impossible to detect outside of long video calls and trained staff or Passive liveness check
2D and 3D mask attacks	2D and 3D mask of someone else (costs less than 300 USD)	Video call for bad masks (not scalable); For realistic masks (think Mission Impossible), only proper image analysis in the form of Passive liveness will be able to detect it

Innovatrics Passive Liveness in a Nutshell

At Innovatrics, we have established thorough liveness testing carried out at our own R&D center. Here are some of the highlights.

Building High Quality Datasets
Our liveness detection algorithm is tested for presentation attacks using digital screens showing photos and videos, including deep fakes, other 2D (printouts, paper masks) and 3D attacks (wigs, silicon, and plastic masks). CrowdSourcing helped us immensely.

It was imperative to build our own datasets. If not for the hundreds of thousands of images of real faces and real attacks, our liveness technology would not be robust enough.

Our R&D team even had to collect images and video sequences of people trying to break through liveness checks in front of a green screen. This allowed them to vary the environment of the attacks, which is important for proper machine learning training.

Leveraging Machine Learning
Apart from datasets, we also work with cutting-edge and well-established machine learning techniques. Our solution is built using PyTorch and PyTorch Lightning frameworks, nowadays most used in the research community.

Our deep convolutional neural network uses a well-tuned combination of two loss functions – Focal and Softmax Loss. For performance, we have selected well-known Mobilenet architecture, because of good accuracy & speed trade-off.

Sharing these details is a non-issue for us since our technology is not only about the tools, but the entire R&D process. And of course, keeping everything up to date.

How to Pick a Liveness Detection Vendor You Can Trust

Doing passive liveness detection correctly requires performing complex processes. Although these only involve elementary matrix algebra, applying the math is a completely different ball game.

This is the simple reason why your biometric vendor needs to have its own R&D department. If you choose a vendor without it, you risk getting left behind since the product might seem impressive for now, but could end up being obsolete in the near future.

Trust but Verify

Maintaining a bit of skepticism is also important. Some vendors will try to convince you that they can perform a 3D scan using a standard mobile camera. While it is true that using advanced machine learning techniques can recreate a 3D model of a face from a 2D image, it is still only a vague estimation.

Talking about 3D scans without actually using a 3D camera is therefore misleading

Ultimately, it isn't even clear how this is supposed to help when it comes to liveness, as a lot of the attacks are 3D in nature.

Since neural networks are complicated tools, what you need is independent verification; not just bold claims.

Standards that Matter

There are few options on getting an independent review of liveness technology. One of them comes from iBeta laboratory.

Let's look at what they actually do on their Level 2 test.

- They test on both Android and iOS devices.
- They recreate different types of attacks valued under 300 USD (Comparatively, a stolen credit card has a value of about 1 USD on the black market[2]).
- These attacks and testing scenarios are based upon recommendations from ISO/IEC 30107-3 Biometric Presentation Attack Detection Standard.

Here are some of the attacks which are tested by iBeta:

- 2D transparent printouts
- 3D paper masks
- 3D latex masks
- 3D silicone masks
- 3D resin masks

They try to break into the tested liveness system several hundred times. If you fail just once, you fail the test.

Innovatrics submission for iBeta Level 2 PAD testing scored 0 to 0.4 percent false rejects (depending on the device) while maintaining 0 percent false acceptance.

[2] https://fxn.ws/3c9yFHK

Tried and Tested, with a Dose of Transparency

No laboratory can test for everything. It is ideal to partner with an experienced vendor, which keeps its technology up to date.

However, this is unfair to newcomers. If they want to compete, they need to be radically transparent about their technology.

The best option is finding a vendor which tests internally for independent benchmarks and in laboratories, with technology deployed internationally and the transparency of the new kid on the block.

Test Species		Android			iOS		
		PAs*	APCE**	APCER***	PAs*	APCE**	APCER***
1.	3D Curved Paper Mask	150	0 of 150	0%	150	0 of 150	0%
2.	Latex Mask	150	0 of 150	0%	150	0 of 150	0%
3.	Inexpensive Silicone Mask	150	0 of 150	0%	150	0 of 150	0%
4.	Resin Mask	150	0 of 150	0%	150	0 of 150	0%
5.	Layered 2D Transparent Photo	150	0 of 150	0%	150	0 of 150	0%
Total per species			0 of 150	0%		0 of 150	0%
Total for all species			0 of 750	0%		0 of 750	0%

* Presentation Attack** | Attack Presentation Classification Error
*** Attack Presentation Classification Error Rate

Innovatrics iBeta Level 2 PAD testing results (find more at: https://bit.ly/3ccJysa)

Crucial Questions for the Ideal Face Liveness Check Provider

If you want to establish trusted relationships with your customers and comply with regulations, you are bound to cross paths with facial biometrics, and inevitably, liveness check providers. Here are questions worth asking.

What to consider	What to look for
Technology ownership	✓ Does the provider own all underlying technologies? ✓ How often is the algorithm upgraded? ✓ Are the upgrades free?
User experience	✓ Does it require an action from a customer? ✓ How fast is the processing? ✓ Does the data stay on-device? ✓ Does it provide autocapture? ✓ Does it work for people with disabilities?
Requirements	✓ What devices does it support? ✓ What are the camera requirements? ✓ What are the minimal environmental (e.g., light) conditions?
Integration	✓ How hard is it to integrate? ✓ Do I need to use some specific technology stacks? ✓ Is the API standardised and well-documented? ✓ Do I get samples? ✓ Does the provider offer integration support?

What to consider	What to look for
Testing and transparency	✓ Does the vendor test the technology internally? ✓ Is the technology tested independently? ✓ Are the tests ISO-compliant? ✓ What types of attacks were tested? ✓ Are you able to test the technology on your data?
Market penetration	✓ Is the technology being used on the market? ✓ Is it being used in different countries and industries?
Liveness approach	✓ Does the vendor provide active, semi-passive, or passive liveness? ✓ Can they provide various combinations of liveness approaches?
Network requirements	✓ Do you need to transfer any data? ✓ How much data do you need to transfer? ✓ Is the transport secure?
Storage requirements	✓ Do you need to store some data? ✓ Where do you need to store it? ✓ Does the data stay on the user's device? ✓ Does the data need to leave your infrastructure?
Speed	✓ How fast can the liveness be evaluated? ✓ Does network transfer impact the processing speed? ✓ How does CPU speed impact the processing speed ? ✓ Do you need specialised hardware(e.g., GPU)?
Accuracy	✓ What is the False Accept/False Reject trade-off? ✓ Can the trade-off be configured with a threshold? ✓ Can the accuracy be improved by combining different approaches?

About us

We are an independent EU-based provider of multimodal biometric solutions. Our algorithms consistently rank among the fastest and most accurate in fingerprint and face recognition. Since 2004, we have partnered with all types of organizations to build trusted and flexible biometric identification solutions. Our products are being used in more than 80 countries, benefiting more than a billion people worldwide.

Contact
sales@innovatrics.com
www.innovatrics.com

Brazil
+55 11 4210-5185

Taiwan (R.O.C.)
+886 2 7741 4036

Slovakia (HQ)
+421 2 2071 4056

Singapore
+65 3158 7379

USA
+1 404 984-2024