FaceTec Anchors Digital Identity

Certified Liveness For KYC Onboarding + 3D Face Matching for Ongoing Authentication

VERIFIES LIVENESS VERIFIES 3D VERIFIES IDENTITY

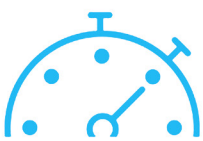
SECURITY CERTIFIED #1 IN THE WORLD

FRICTIONLESS SECURITY FOR REAL USERS

The intuitive ZoOm interface makes Certified Liveness Detection and 3D Face Matching fast, easy, and incredibly secure for everyone, regardless of their device. During onboarding, FaceTec's two-second video-selfie verifies Liveness, matches the user's 3D FaceMap to their Photo ID, and sets up their new account. Every time they return, FaceTec's ongoing authentication again proves Liveness and compares their new 3D FaceMap to the one enrolled. If they match they get instant access, no password required!

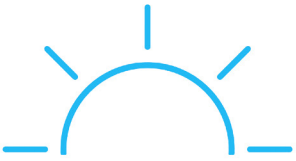
BRICK WALL FOR BAD ACTORS

Login from any smartphone, tablet, PC or Laptop, and unlock everything from your car door to your bank account. Real users gain access easily, but bad actors, bots and hackers are rebuffed by Level 1&2 Anti-Spoofing Certified by NIST/iBeta. FaceTec is the Face Authentication market leader and provides more security, portability, and convenience than any other biometric.



CERTIFIED LIVENESS DETECTION IN 2 SECONDS

GREAT WITH GLASSES, MAKEUP & BEARDS



WORKS IN REAL-WORLD LIGHTING CONDITIONS

DATANAMIX™

SECURITY CERTIFIED #1 IN THE WORLD

FaceTec's Encrypted 3D FaceScans & FaceMaps

Can a Simple Selfie Really Provide Security?

Typically they can't because 2D photos of most people are already all over the Internet. But FaceTec isn't just a "selfie"; it's a 3D FaceScan that enables a strong Liveness Check and contains a 3D FaceMap, which IS NOT publicly available online. FaceTec ensures the user is physically present and isn't fooled by photos, masks, or deepfakes. FaceTec's Liveness Detection AI must observe so many concurrent human traits that spoof artifacts are unable to recreate them all at once. FaceTec's 3D Face Matching then compares to the user's previously-stored 3D FaceMap, and if the two 3D FaceMaps highly match (1/125M+ FAR), the verified user is granted access. Skeptical? Good, you should be! Try our $600,000 Spoof Bounty Program for yourself.

No Recent Liveness Data = No Honeypot Risk

Two types of data are required for every face authentication: 3D Face Data for matching, and real-time 3D Liveness Data to prove the Face Data was collected from a live, present person. 3D Liveness Data must be timestamped, is valid only for a few minutes, and then can be deleted. New 3D Liveness Data must be collected for every subsequent FaceTec login.

Storing 3D FaceMaps doesn't create honeypot risk because they are "Face Data" without any Liveness Data, so they cannot be used to spoof FaceTec's 3D Liveness AI. Think of the stored 3D FaceMap as the Lock, the user's newly collected 3D FaceMap as a One-Time-Use Key, and the new 3D Liveness Data as proof that the Key has never been used in the lock before.

FaceTec's Encrypted 3D FaceScans & FaceMaps

- CAN'T BE PHISHED FROM USERS
- AREN'T A BIOMETRIC HONEYPOT
- STOP CREDENTIAL SHARING
- STOP BOTNET ATTACKS
- 1:1 MATCH AT 1/125M FAR
- 1:N DE-DUPLICATE UP TO 1/1B FAR
- MATCH 2D PHOTOS UP TO 1/2M FAR
- PROVIDE ANONYMOUS AGE CHECKS

zoom by facetec

DATANAMIX™

HOW DOES FACETEC WORK?

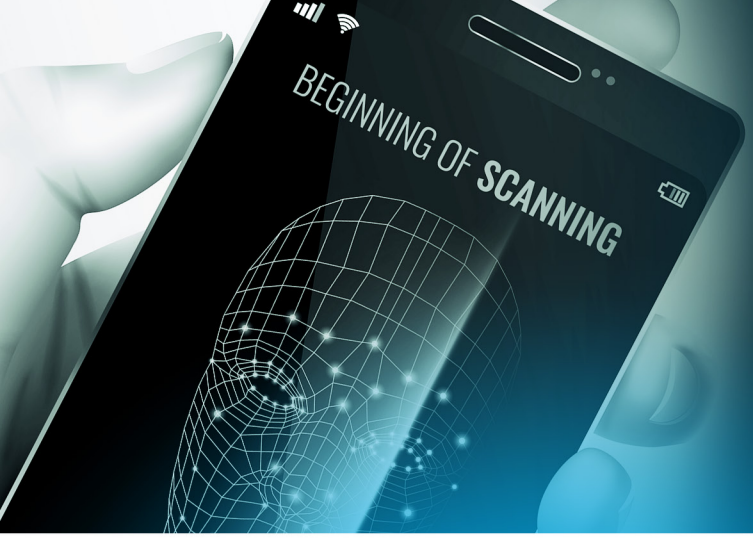
During the user session, the camera's view of the 3D face changes, observing perspective distortion and proving it is 3D. In under two seconds, FaceTec's Device SDK processes 100+ video frames and reverse engineers a 3D FaceMap from the standard 2D camera.

3D LIVENESS OPTIONS

- FaceTec - Match - 3D - 3D
- FaceTec - Match - 3D 2D 3rd party ID photo
- FaceTec - Match - 3D - 2D ID scan
- FaceTec - Liveness 3D - ID/Passport Doc Check
- FaceTec - Match - 3D - 2D Profile Picture
- FaceTec - Match - 3D - 3rd Party low quality ID Photo
- Facetec – Barcode and OCR
- Facetec – NFC Passport reader

zoom by facetec

DATANAMIX™

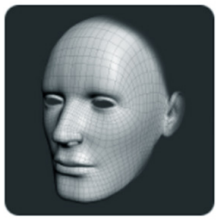


2D vs. 3D

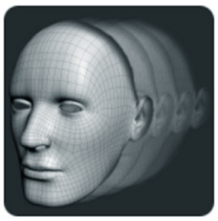
2D Matching will never have the accuracy needed for true Unsupervised Identity Verification & Authentication. There's just too much variability in how the same 3D human face appears when flattened into 2D at different image capture distances. This variability creates significant overlapping similarity between the 2D features of different humans and confuses the 2D algorithms, preventing them from achieving highly accurate FARs at usable FRRs.

Apple, Google, and Intel understand this, so their 3D Face Matching systems use 3D infrared cameras, but that, of course, requires each device to include special hardware. In contrast, FaceTec securely performs 3D Matching from virtually any device with a 2D camera.

2D



3D



FaceTec® 3D

AXES	X,Y	X,Y,Z	X,Y + TIME
Vendors	Aware, BioID, Daon, FacePhi, Idemia, iProov, etc.	Apple Face ID, Google Pixel 4	FaceTec & > 90 Channel Partners Worldwide
Purpose	Face Verification	Unlock Mobile Phones	3D Face Matching
Installed Base	10+ Billion Smart Devices (Android - 85% + iOS -14% & Webcams)	< 10% of in use iOS devices have Face ID, Pixel 4 will be < 1% of the market.	10+ Billion Smart Devices (Android - 85% + iOS -14% & Webcams)
Portable Biometric	Varies	None, re-enroll on each device	Cross-Device & Cross-Platform
Technology	Legacy 2D Algorithms	Hardware: Infrared Camera Array & Neural Network Chip	Software: Real-time Computer Vision + 100% proprietary AI
Interface	Varies	Glance to unlock phone	3D Video Selfie: ~2 Seconds
Skin Tone Bias	Almost all 2D Algos have significant racial bias	None-Reported	None exhibited in the Lab or Real World usage
SDK Info	Varies	No SDK possible, special hardware required	Device SDKs for Android/iOS, web & Server SDK
Liveness Method	Challenge/Response, Blink, Smile, Turn Head or Flashing Lights, etc.	Infrared dots + neural network chip determine if user is 3D	Measures 3D Depth, skin texture, eye reflections, etc.
Liveness Strength	Fairly Weak	Fairly Strong	Very Strong
3D Depth Detection	Weak	Strong	Very Strong
Intellectual Property	Legacy 2D Algos are too old for meaningful patents	20+ infrared related patents acquired in 2013	5 US Patents on 3D process issued, +12 pending globally
FAR/FRR	Varies, but 1/<75,000 at real world usable FRRs	1/1M - No FRR stated	1/125,000,000 FAR @<1%FRR
Identical Twin Differentiation	Very Weak	"If you have a Twin, use a PIN."	High 1:1 FAR provides Best Possible Twin Differentiation
Liveness Testing Certifications	No 3rd Party Certs	No 3rd Party Certs	Certified Level 1 & 2 Spoof Detection by NIST/ NVLAP LAB - Liveness.com
Age Estimation	2D = poor Age Estimates	Not Available	"Better than Human" Face-Only Anonymous Age Estimation
Match to Photo ID	Low-detail & problems with aged photos = low match rates	Not Available	Up to 1/2,000,000 Match Levels with 3D:2D Matching
Password Replacement?	Not secure enough, FAR too low.	No, only used for convenience	Yes, universal device support, highly secure & convenient
Spoof Bounty Programs?	No, they are all talk.	No, no motivation.	Yes, $600,000 SpoofBounty.com

Independent 3rd-Party Testing & Certification

PRAETORIAN

OWASP: Black & White-Box Pen Testing
FaceTec SDK Penetration Test Summary

iBeta QUALITY ASSURANCE — LEVEL 1 ISO 30107-3 Presentation Attack Detection — TESTED CERTIFIED

ISO 30107–3: Level 1 Spoof Detection
EPCS-DEA: Biometric FAR Certification

iBeta QUALITY ASSURANCE — LEVEL 2 ISO 30107-3 Presentation Attack Detection — TESTED CERTIFIED

ISO 30107–3: Level 2 Spoof Detection
$600,000 Spoof Bounty Program Levels 1-5

zoom by facetec

Contact Datanamix:
Telephone: 010 300 4898
Support@datanamix.co.za

DATANAMIX™