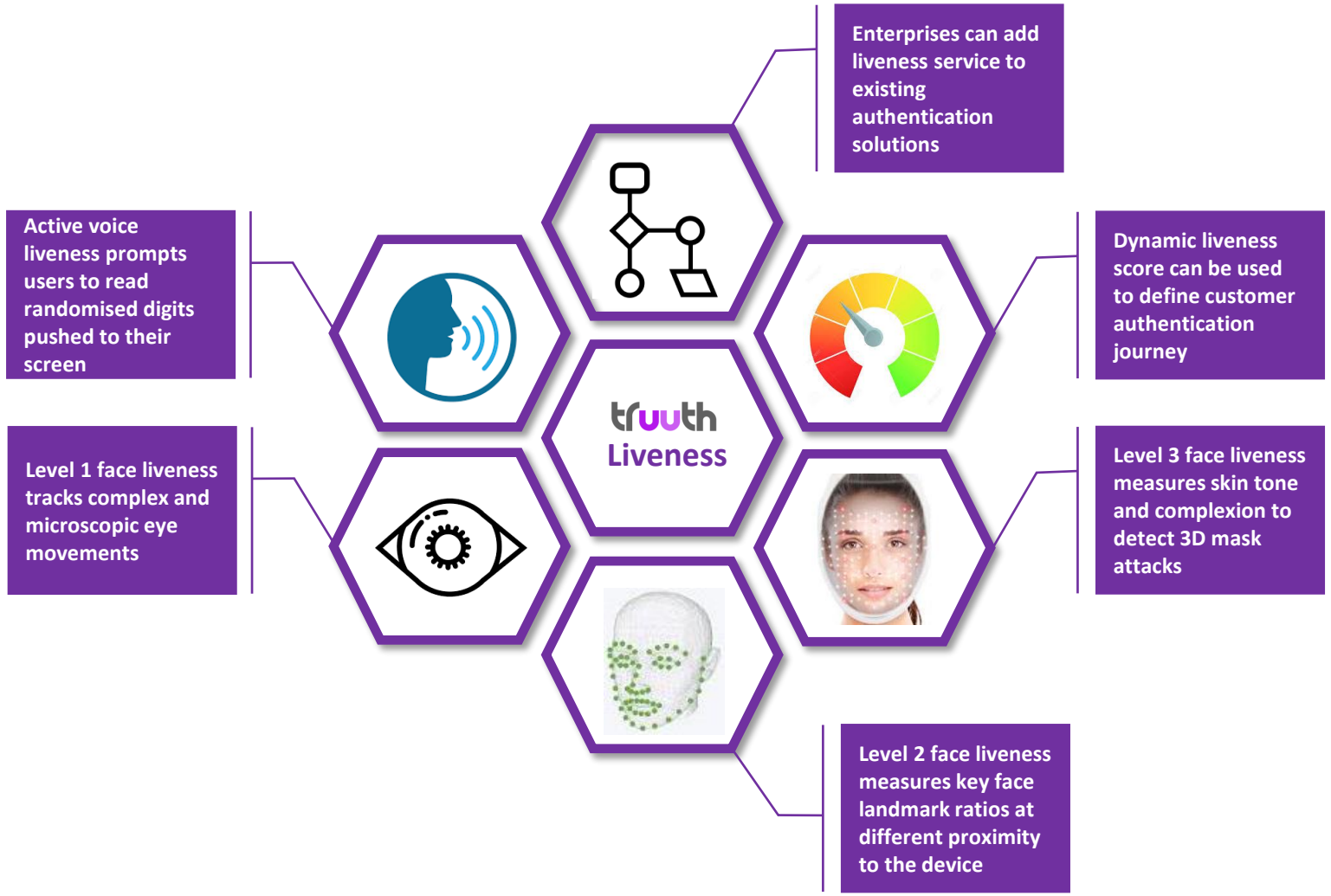
Product Features



For more details visit: https://www.truuth.id/truuth-liveness

CAN YOU SPOT A DEEP-FAKE?

Protect your employees & customers with truuth Liveness.

What is truuth Liveness?

Truuth Liveness verifies a user is human and present during the interaction. While facial recognition is well suited for mobile applications, it is vulnerable to attempts by fraudsters to intentionally fool biometric security measures by presenting non-live biometric data. For example, a fraudster might use a photograph, video, or mask to either impersonate a targeted victim or to assert a false identity. This is also called a “presentation attack”.

To mitigate the risk of presentation attacks, it’s essential to apply robust liveness detection when using facial recognition for mobile applications, particularly where personal data is accessible or high value transfers are possible.

How does truuth Liveness Work?

Truuth Liveness performs 3 tests for human presence:

1. We track multiple metrics of eye movement including blinking and microscopic iris movement during a face scan

2. We analyse changes in facial landmark ratios as the user is guided to move device relative to the face

3. We analyse face complexion and if the confidence level is below defined threshold, the user is requested to read randomised digits projected on screen.

What are the benefits of truuth Liveness?

1. Improved security

Truuth Liveness undertakes multiple tests to mitigate the risk from fraudulent actors. Presentation attacks are increasing in both volume and complexity. Fraudulent actors are using elaborate deep fakes and synthetic identities to gain access to corporate networks, leading to potentially catastrophic outcomes such as ransomware demands.

Truuth Liveness includes both ‘active’ and ‘passive’ components to make it more difficult for fraudsters to predict how liveness is determined.

Active liveness entails a challenge and response. A user may be prompted to blink, smile, or move their device during a facial recognition capture. Users are typically aware that liveness detection measures are being applied. Passive liveness detection happens in the background and relies on algorithms that can identify and assess those artifacts in an image that indicate its content, including masks, cutouts, skin, texture, borders, and other indicators of a false representation of a user’s face. The process is opaque to the user, making it more difficult for a fraudster to learn how to circumvent it.

2. Enhanced user experience

Truuth Liveness typically takes less than 3 seconds to complete. Liveness results are combined with other contextual data (e.g. device identifiers, authentication history, location, purchase type) to determine the risk level and only prompts the user for face or voice liveness if the risk level requires it.

3. Reduction in Total Cost of Ownership (TCO)

Truuth Liveness reduces the cost of onboarding a customer by enabling fully digital onboarding while mitigating risk of identity fraud. Truuth Liveness can also be integrated into authentication services to reduce the cost of verifying user identity and complying with regulations such as Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF).

What cyber attacks does truuth Liveness help prevent?

Truuth Liveness helps prevent attacks that attempt to open new accounts with fraudulent identity credentials. These include:

- Deep fake
- Synthetic identities
- Credential stuffing
- Photo presentation attacks
- Video playback presentation attacks
- 3D model and mask presentation attacks