

## AI-Powered Continuous Authentication & Threat Detection

Zighra proactively fuses device, behavioral and environmental intelligence to build high fidelity, on-device user profiles that enable continuous proof of presence and genuine identity validation by way of powerful analytics. The rapid expansion of mobile transactions has ushered in well-organized attacks. Businesses need more advanced ways to stay ahead in the mobile world avoiding Account Takeover, Social Engineering and Remote Automated Attacks in addition to Friendly Fraud.

Our patented technology combines the power of machine learning and behavioral biometrics to provide continuous authentication and fraud detection for mobile and web applications while providing a frictionless experience for the user. Based on eight years of research from the University of Waterloo and Carleton University in Canada. Tested with 25,000 users in 70 countries on 700 different device types. Leveraging Generative Behavioral Networks (GBN), the AI engine learns 10X faster putting the data to work quickly. Speeds up onboarding processes and makes step ups hassle free.

### Core Vertical Markets

- Banking
- Insurance
- Field Service
- Healthcare
- Education
- Manufacturing
- Blockchain solutions
- Government
- IoT

### 'N'-Dimensional Intelligence



Network Intelligence



Device / Sensor Intelligence



Location Intelligence



Biometric Intelligence



Social Intelligence



Behavioral Intelligence

Six layers of intelligence are combined in an advanced AI engine creating detailed user profiles. Unique and continuous correlation of the data throughout a transaction provides risk scoring to validate the user is genuine. Anomalous behaviors are detected real time.

### Innovation



#### Frictionless Experience

Implicitly authenticate mobile users with an invisible behavioral authentication layer. No more passwords. No user training. Simply execute in a natural manner and the system learns and continuously monitors automatically throughout the transaction.



#### Decentralized Model

Our on-device option keeps the ID on the device, decentralizing the data. No more centralized credential stores which are prone to attacks. A great fit for field workers who are often off-line. Allows for user ownership and data sovereignty where desired. Use your mobile as a security key to authenticate your desktop and other 'things'.

### Platforms



iOS



Android



Browser

### Delivery Models



On Device



Cloud



On Premise

## The Zighra Difference

Trust the user is genuine during transactions – all of the time. Take action when behaviors don't match. Expect better security with Zighra.