TICKING ALL THE RIGHT BOXES:
THE ROLE FOR THE CLOUD IN
DIGITAL IDENTITY AUTHENTICATION

**AimBehaviour**; hyper-vigilant, continuous behavioural authentication, providing real-time assessments that the user is who they say they are.

**Ever feel like it's a race to find the creepiest way to authenticate somewhere? The headlines are full of increasingly imaginative but gruesome ways in which we can authenticate ourselves; ear canals, veins, blood. Sinister.**

At **AimBrain**, we keep it simple...well, as simple as neural networks based on evolutionary algorithms can be, at least. We use everyday device technology in a smartphone, mouse, keyboard or laptop, to monitor behaviour and detect abnormalities, building mathematical constructs of the way someone swipes, holds, types, clicks, hovers, and more. From login to logout, we continually assess behaviour based on the profile we've built and stored safely in the cloud, where it's trusted and impenetrable.

And if we suspect a breach or account takeover, you can deploy one of our other modules as a step-up authentication - a selfie or a voice challenge - because you can't look like, sound like and act like someone else. Voice, face, behaviour; it's 100% AimBrain technology and 100% cloud-based, keeping digital identities secure.

**SOLUTION MODULE:** **AimBehaviour**

**AimBehaviour** is the behavioural authentication component of the **AimBrain** BI DaaS (Biometric Identity as-a-Service) platform. It can be deployed alone, combined with a bank's existing authentication mechanism or used with any other **AimBrain** module. On its own, it assesses gestures and movement, providing a continual risk-based assessment that the user is who they say they are. Combined with a bank’s or our other server-side modules, it can form part of a multi-module authentication sequence, invoking a ‘step-up’ face or voice authentication module when required. **AimBehaviour** subset, **AimAnomaly Detection (AAD)**, is a real-time, in-session fraud detection module specifically designed to search for and flag the atypical behaviours that could signify an attempt to breach an account.

**PRODUCT FEATURES**

- Passive, continuous assessment of user's authenticity, in-session and real-time
- Can invoke step-up challenges if behavioural assessment falls below an acceptable threshold, similarly step-down (for reduced friction) if the behaviour score is comfortable
- No forced behaviour or front-end changes required
- Detailed reporting at pilot stage to demonstrate industry leading Equal Error Rates
- Measures thousands of points; from pressure to speed, range of movement to gyroscope
- Patented technology 'learns' the user in virtually unlimited contexts, for greater accuracy
- Identifiable user profile complete with just 6 interactions
- Based on next-gen AI: self-learning, evolutionary algorithms that eliminate human intervention
- Deployable across any channel that uses a keypad, keyboard or mouse.
**AIMBRAIN TECHNOLOGY**

The AimBrain server-side authentication suite is available as individual components or as bundles, each of which is deployed via SDKs using open APIs (TLS and HMAC-secured). We integrate directly into the enterprise's application using the enterprise's secure channel, and provide a risk-based score in industry standard JSON format, for easy consumption for downstream systems.

**BENEFITS**

- 100% server-side authentication eliminates risk of breached device
- Cloud model allows rapid rollout of algorithm updates with new anti-fraud capabilities
- Low bandwidth background monitoring for smoother customer experience
- Low total cost of ownership; pay on a per-user-per-year basis
- Compliance-focused; adheres to regulatory best practice
- Applies friction relative to scenario normality/abnormality and risk thresholds.

**ENTERPRISE USE CASES**

- Financial transaction authentication
- In-app monitoring for account takeover
- Enterprise-wide secure systems access
- Step-up authentication for workflow approvals process...and more.

**PRIVACY BY DESIGN**

AimBrain is a security company and commits to the highest levels of data privacy and security. AimBrain insists on a zero-access agreement to an organisation's sensitive data. Extensive testing has proven that our data cannot be reverse-engineered, and can be rendered useless in the event of any suspected breach.