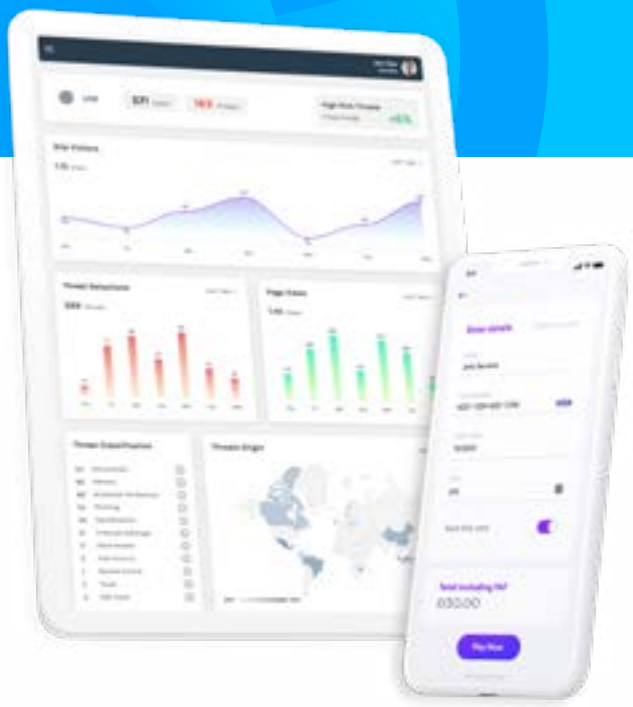
Behaviour ID™ Powered by ScreenWiZe™

Real-time behavioural data analysis delivering a frictionless **Secure Form of Authentication** for payment institutions



CONTINUOUS USER AUTHENTICATION ACCELERATING SALES THROUGH A SIMPLE AND FRICTIONLESS CUSTOMER EXPERIENCE

Striking the optimal balance between security and a frictionless customer experience is a huge challenge for merchants or financial institutions servicing users via mobile or online applications. Behaviour ID™ dramatically reduces risk at device level, highlights phishing and account takeover while satisfying Strong Customer Authentication (SCA).

Choosing Cybertonica's Behaviour ID™ means you can build your business around your customers, minimising risk and cost while growing sales. **No more compromises.**

BENEFITS FOR YOUR BUSINESS

Prevent **cyber-attacks** including malware and bots

Decrease need for **secondary authentication** by **70-90%**

Grow sales by up to **15%** within just **8 weeks**

Reduce false positives by over **80%**

Manage new **PSD2 transaction threshold limits**

Detect **account takeover, phishing** and other attacks

" This product is excellent and right on trend with needs of Acquirers and Merchants to have a recource for passive authentication that fits the SCA requirements in PSD2 while maintaining frictionless and privacy levels at the best for the consumer. "

- CEO of a major EU payment gateway business

cybertonica

AUTHENTICATE WHILE PRESERVING PRIVACY

People are more aware than ever of privacy and the need to safe-guard personally identifiable information. Devices are the interface most often compromised.

Cybertonica protects their real-world identity by creating an anonymised Behavioural ID™ using advanced Data Science technology. We connect and analyse diverse anonymised data sources to recognise a single user entity with outstanding precision, ensuring only legitimate users and secured devices gain access to your transaction platform.

The Behavioural ID™ can also be used to monitor and protect your business and practices from internal fraud.

USER AND DEVICE BEHAVIOURS CAPTURED

On the laptop/desktop: Mouse movements, speed of typing, keystroke pressure

On the phone or tablet: Gyroscopic movement, speed and acceleration, height of device, use of touch screen

Automatic screening of devices and users with past exposure to cyberthreats or previous participation in fraudulent networks

IP address and full device fingerprints

THREATS DETECTED

THREATS

- Threat intelligence and alerts
- Malware
- Bots
- Spyware
- Trojans
- Web injections and rogue scripts
- Data harvesting
- Dark web monitoring

FRAUD

- Account takeover
- Phishing
- Stolen cards
- Identity theft
- Friendly payments and internal fraud
- Peer-to-peer

EASY INTERGRATION AND INTUITIVE USER TOOLS

Behaviour ID™ can be integrated easily into your existing desktop or mobile platform **within hours or days** rather than weeks. It can also be added to your current fraud prevention system as an extra level of security, so you can benefit from behavioural accuracy.

The Behaviour ID™ dashboard gives you **full visibility of your entire customer base**, offering real-time actionable insights to your in-house risk system via an API or through a customised dashboard.

CONTINOUS AUTHENTICATION

Behaviour ID develops an understanding of a customer's behaviour and profile after only three minutes of monitoring activity and detects any changes or movements away from their inherident usage of their device thus detecting suspicious actors.

cybertonica

info@cybertonica.com
www.cybertonica.com
@CybertonicaLtd

IDEALondon, 69 Wilson Street
London EC2A 2BB
United Kingdom