

Act in real time with Fraud Protection



Fighting fraud

Graph visualization

In-depth analysis

Bot protection

Mobile App Protection

Web App Protection

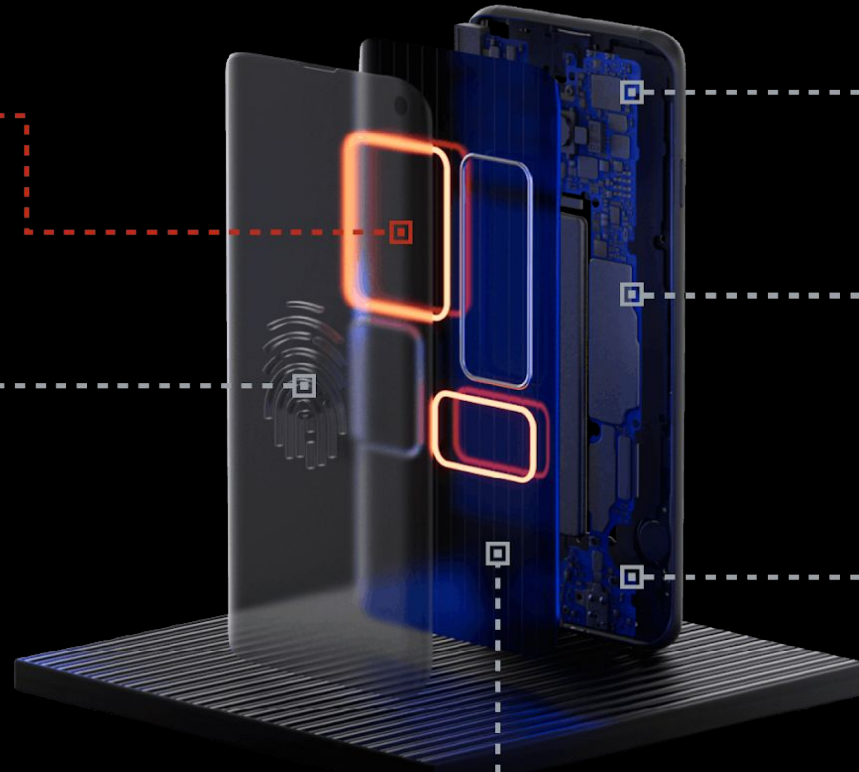
Behaviour Analysis

Fraud Protection uses advanced fingerprinting and behavioral Analysis to securely authenticate users to prevent fraud and deliver a frictionless customer experience

Malware, Jailbreak,
Emulator and RAT
Detection, SIM Swap

Anonymised User data
Advance Digital
Biometrics
Behavioral Analysis

Android or IOS Operating
System Configuration
Monitoring



Mobile Operator
Characteristic Monitoring

Device Technical
Specifications

Device Sensor
Monitoring,
Accelerometer
Proximity Sensors
Touch Sensors
Gyro-Sensors GPS

Act in real time with Fraud Protection



Fighting fraud

Graph visualization

In-depth analysis

Bot protection

Mobile App Protection

Web App Protection

Behaviour Analysis

Fraud Protection uses advanced fingerprinting and behavioral Analysis to securely authenticate users to prevent fraud and deliver a frictionless customer experience

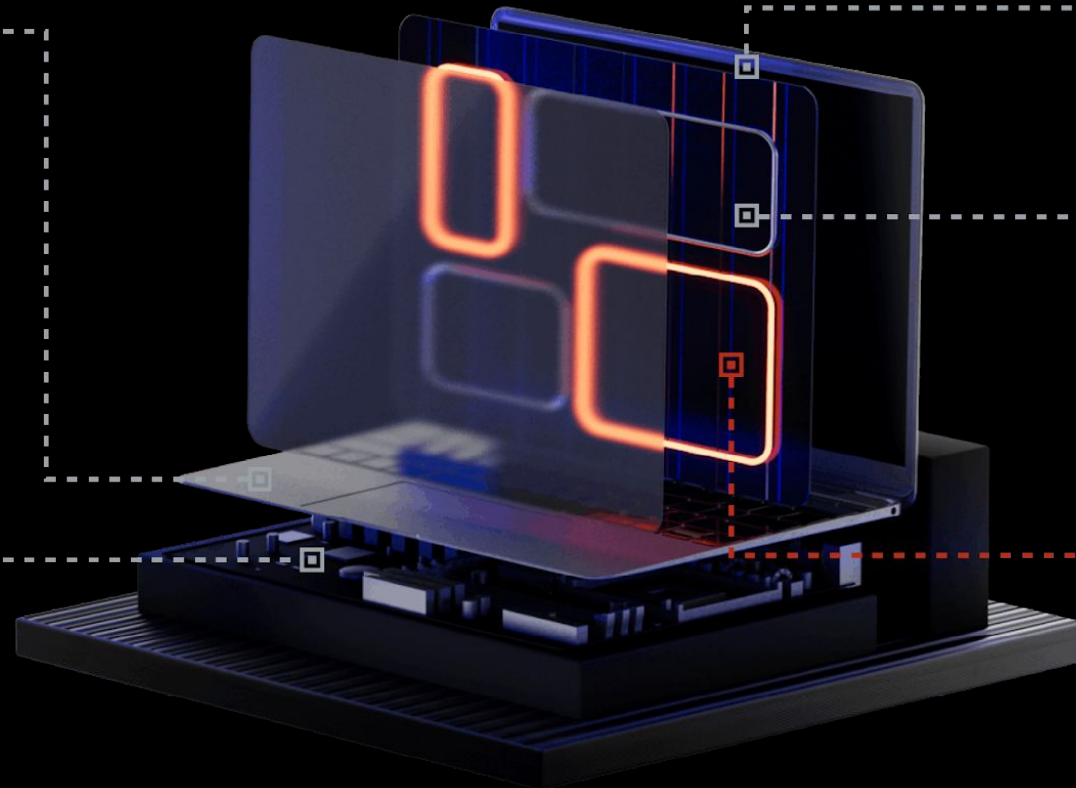
Anonymised Advance
Digital Biometrics
Behavioral Analysis

Device Graphic and
Display Configuration

Browser Configuration
ISP data

Device Technical
Specifications

Malware, Bot and
RAT Detection



Act in real time with Fraud Protection



Fighting fraud

Graph visualization

In-depth analysis

Bot protection

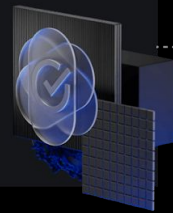
Mobile App Protection

Web App Protection

Behaviour Analysis

Fraud Protection analyzes user behavior with machine learning algorithms. This analysis provides an opportunity to identify abnormal behavior and prevent fraud, reducing the cost of additional verification for transactions or eliminating the consequences of fraud.

LEGITIMIZING USER SESSIONS



Actions that are not typical for scammers (for example, opening a chat with a support operator) 'legitimize' the user. Legitimizing user sessions through triggers indicating the user's legitimacy allows to:

Reduce the cost of verifying user actions in the application

for example, instead of verifying users with an operator call or SMS, Fraud Protection will determine in advance whether the user is legitimate

Reduce the number of false positives alerts

of the main fraud monitoring system installed in the client's infrastructure.

FRAUD PATTERNS AND BEHAVIOR MODELS



The Fraud Protection machine learning algorithm evaluates all user sessions and detect fraudulent behavior patterns. Patterns and models of fraudulent behavior can be based on:

Specific ways of navigation

between URLs within the application

Sequences

of interactions with interface elements

Combinations of other criteria.

MEDIAN BEHAVIOUR MODEL



The Fraud Protection calculates and builds median behavior model for each user. All user sessions within the protected application are compared to the median behavior model to identify:

New behavior

when the user performs actions that are not typical for his/her behavior model.

Abnormal behavior

when the user performs normal actions, but in an uncharacteristic manner