ThreatMark

Anti-Fraud Suite

Most advanced online banking Fraud Detection solution based on deep behavioral profiling

Everything a bank needs to eliminate fraud across all digital channels

From transaction monitoring, identity verification to threat detection – ThreatMark enables banks to precisely understand who are their legitimate users, while keeping the fraudsters away.

With flexible deployment options – ThreatMark provides a complete protection of web & mobile banking applications while securing user's most precious assets and safeguarding bank's reputation.

DEEP BEHAVIORAL PROFILING

ThreatMark Anti-Fraud Suite (AFS) analyzes users at every step of their online journey.

From banking login to transactions - our solution continuously and seamlessly verifies user's identity and their intentions through behavioral biometrics, session parameters, transaction details, and complex interactions across all digital channels.

This knowledge allows us to create completely trusted user identities. Based on them, ThreatMark precisely detects all related anomalies, identify threats & prevent fraud.

THREAT DETECTION

ThreatMark's AFS combines advanced threat and fraud detection capabilities while monitoring user's activities across web and mobile applications, in real-time.

ThreatMark's powerful engine detects various types of frauds. Ranging from Account Takeover and New Account Fraud to phishing, smishing, vishing and BOT, malware, RAT attacks... and many more.

Beyond detection, ThreatMark's Threat Intelligence is built to learn from these attacks and prevent future occurrences.

As fraudsters constantly improve their tool sets and attack vectors, banks are now equipped to confidently engage in protecting their assets and reputation.

About ThreatMark

- Where high-tech meets cyber security expertise to deliver complete fraud prevention solutions
- Bringing trust and security across all digital channels, in real-time
- Protecting more than 20+ mil. users all over the world. Scoring more than 1 billion logins yearly

PHISHING
- Webpage Cloning Detection
- Phishing Site Usage Detection
- Phished Users Detection

MALWARE
- Webinjects
- Active RAT Detection
- Malicious Applications Detections
- Overlay Detection
- SMS Hijacking Detection

BOTs
- Webscraping (Screenscraping)
- API Scraping
- Advanced Web Automation

APPLICATION/DEVICE HACKING
- Application Debugging
- Application Cloning
- Emulator Detection
- Device Hacking Protection

PAYMENTS
- Payment Anomalies & Behavior
- Mule/Fraudster Accounts
- Shared Fraud Schemes

ACTIONS
- Suspicious Sequence
- Fraudsters IP Reputation
- Known Fraudulent Actions

CHANNELS
- Web/Mobile/Open API Payments
- Omnichannel Geo Fencing
- Cross-Channel Fraud Detection
- PSD2 Authorization Schemes

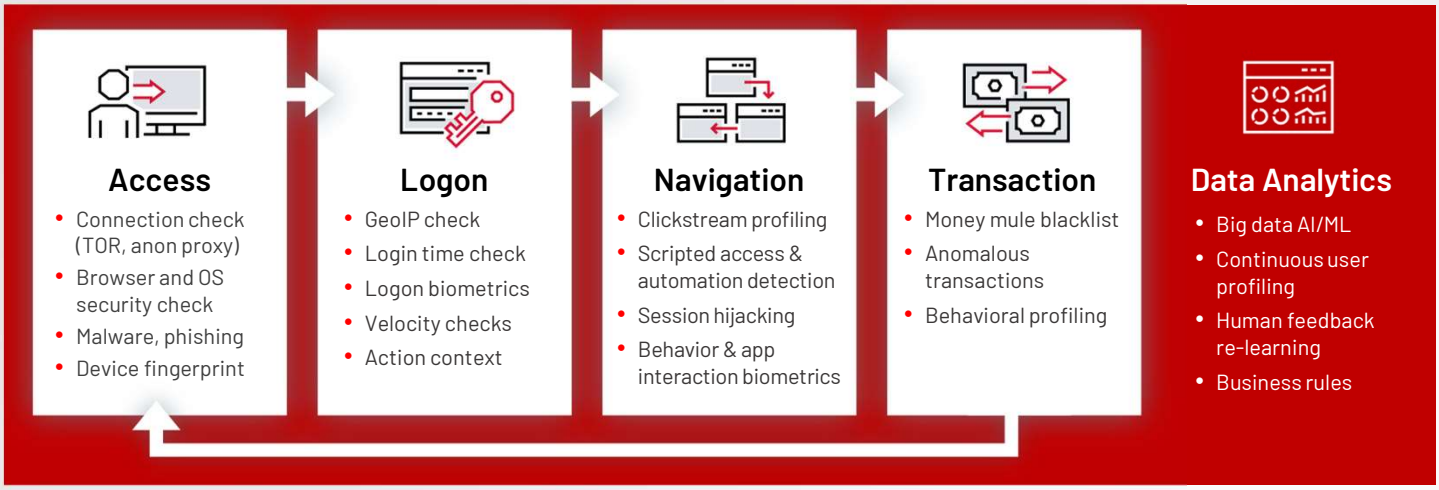
BEHAVIOR
- Date & Time Behavior
- Device Usage and Interaction
- Navigation Behavior
- Behavioral Biometrics
- Application Interaction Behavior
- Transaction & Login Behavior

IDENTITY
- Advanced Device Identification
- IP Reputation Network
- Fraudulent Accounts & Identities
- Shared Identities & Devices

www.threatmark.com —— info@threatmark.com

CONTINUOUS EVALUATION OF THE ENTIRE CUSTOMER JOURNEY

ThreatMark



USER IDENTITY VERIFICATION

ThreatMark AFS satisfies the Gartner's CARTA concept as it evaluates the user risk during the whole session.

ThreatMark achieves this is by leveraging various data points from the device, session and user behavior. In total, over 120 data points — from typing cadence, device OS, session IPs, to navigation paths, swiping... — are evaluated to strengthen the user's trusted profile.

Banks use ThreatMark's behavioral biometrics to satisfy risk-based strong customer authentication (SCA), verify users' digital identities and eliminate friction for legitimate users.

TRANSACTION RISK ANALYSIS

ThreatMark AFS uses ML/AI to analyze user payments, spending behavior & associated risks.

Monitoring transactions and devices makes ThreatMark a perfect fit for transaction risk analysis and replacement for the multi-factor authentication.

Complemented with comprehensive case management & reporting, ThreatMark helps banks to be compliant and satisfy demanding security requirements such are PSD2 and SCA; industry's 3D Secure 2.x or even various local regulations (including requirement to host the data in the country, e.g. Switzerland).

DELIVERY & OPERATIONS

- **Easy and fast:** in weeks instead of months
- **SaaS based:** have the latest AFS version always, with ever-improving features and threat detection for timely fraud prevention
- **Flexible:** fully managed on premises or in the cloud, no software licenses components to manage
- **Support from our fraud analysts:** expert training and know-how transfer to the client's fraud team
- **Complemented by a SOC team:** cybersecurity professionals who vigilantly watch for threats across the digital landscape
- **Rich analytical web interface:** for security teams and fraud analysts

Key benefits banks see when implementing ThreatMark AFS

70%
Better detection rate
(than traditional FDS)

90%
Fewer false positives
(than traditional FDS)

90%
Decrease in cost for authentication
(est. SMS cost saving)

2
Weeks to implement
(cloud option)

Improved detection & scoring methods
(when integrating AFS with existing systems)

As verified by ERSTE Group (case study) & Sberbank (case study)

www.threatmark.com —— info@threatmark.com