ThreatMark

BEHAVIORAL INTELLIGENCE PLATFORM.

Disrupting fraud operations across every stage of attack.

ThreatMark's Behavioral Intelligence Solution refocuses fraud professionals on identifying fraudulent users against legitimate customers, interrupting fraud operations across all stages of the attack.

1

COLLECT INTEL

ThreatMark collects intel on attackers' infrastructure, devices, tools, locations, payment methods, and attack vendors to build an effective campaign against fraudster fraud.

2

ANALYZE TACTICS

ThreatMark tracks the attackers' progress from manipulating users and accounts to attempting to get stolen funds out of the systems, which brings visibility to anti-fraud teams.

3

DEPLETE THEIR RESOURCES

Identifying and blocking phishing sites, attack tools, behavioral patterns, and payment infrastructure allows swift response to attacks. **Keeping attackers frustrated.**

4

IDENTIFY & PREVENT FUTURE FRAUD

By successfully identifying where and how the fraud occurred, ThreatMark can disrupt the fraud infrastructure and crime ring operations targeting other banking customers.

The world's first full-stack fraud prevention platform built on behavioral intelligence.

ThreatMark uses the latest AI methodology to track the attackers' activities in real-time throughout the entire attack lifecycle. Collecting signals across all digital channels, ThreatMark gathers information about the whole fraud right and its infrastructure, ultimately disrupting their operations.

About ThreatMark

Bringing trust and security across all digital channels.

- **Reduced Fraud Costs**
  Expert tools and tactics directly combat phishing and malware, curtailing potential financial losses.
- **Operational Efficiency**
  Quick threat mitigation, due to relationships with key providers, minimizes disruptions and response times.
- **Enhanced Security ROI**
  Maximize the return on security investments by providing an all-encompassing defense.
- **Risk Management**
  Proactive threat hunting reduces unforeseen vulnerabilities, safeguarding assets and reputation.

CONTINUOUS EVALUTION OF THE ENTIRE CUSTOMER JOURNEY.

User Identity Verification

ThreatMark satisfies Gartner's CARTA concept by evaluating user risk throughout the whole banking session. It achieves this by leveraging various data points from device, session, and user behavior—from typing cadence, device OS, and session IP to navigation paths and swiping patterns.

Financial institutions use ThreatMark's behavioral biometrics to satisfy risk-based Strong Customer Authentication (SCA), verify digital user identities, and eliminate friction for legitimate users.

Transaction Risk Analysis

ThreatMark uses machine learning and AI to analyze user payments, spending behavior, and associated risks.

Monitoring transactions and devices makes ThreatMark the perfect solution for Transaction Risk Analysis (TRA) and replacement for multi-factor authentication.

Complemented by comprehensive case management and reporting, ThreatMark helps banks comply with demanding security requirements.

- ✓ **Efficient**
  Implemented in weeks rather than months.
- ✓ **Fraud Analyst Expertise**
  Expert training and know-how transfer to internal fraud teams.
- ✓ **SaaS-Based**
  Continuous platform improvements for timely fraud prevention and threat detection.
- ✓ **Rich Analytical GUI**
  Dedicated security teams and fraud analysts.
- ✓ **Flexible**
  Fully managed on-premises or cloud deployments without reliance on software licenses.
- ✓ **Cyber Fraud Fusion Centre**
  Additional cybersecurity professional expertise for threat investigation.

Key benefits for financial institutions include:

70%
Better detection rate
(than traditional FDS)

90%
Fewer false positives
(than traditional FDS)

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

2
Weeks to implement
(cloud option)

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