Our Fraud Detection Approach

Everything a bank needs to eliminate fraud across all digital channels

Nowadays, to detect fraud neither traditional approach (of rule-based transaction anomaly), nor IP and browser-based user identification techniques are sufficient.

These, and many more, are ineffective against attackers who use cunning identity-theft and social engineering-based techniques to bypass all protective measures. Traditional solutions don't have enough relevant nor detailed data to be effective in detecting modern attacks and fraud attempts.

Moreover, the lack of detailed information and context results in a high number of false positive detections that need to undergo costly manual reviews.

To decrease the number of false positives and successfully prevent fraud—ThreatMark Anti-Fraud Solution (AFS) focuses on a broader context.

We developed a method, which considers all possible data – combining information about threats (threat detection), user (behavior profiling) and transactions (transaction risk analysis) – which creates a reliable user identity and prevents fraud at the same time.

THREAT DETECTION

ThreatMark AFS observes and tests all data displayed by a browser as well as those hidden in the application code. The differences are tested automatically to see if they match known malware signatures. If there's a match: positive detections are reported.

In a case of unknown deviations, they are sent to our Security Operation Center (SOC) for further scrutiny.

Our solution also detects insecure configurations and any non-human like behavior, which can be an early sign of financial malware trying to execute an automated transaction.

Using sophisticated methods of detection, our solution can detect malware, RAT (remote support) scams, vishing and reveal any attempts mimicking legitimate banking page for phishing purposes.

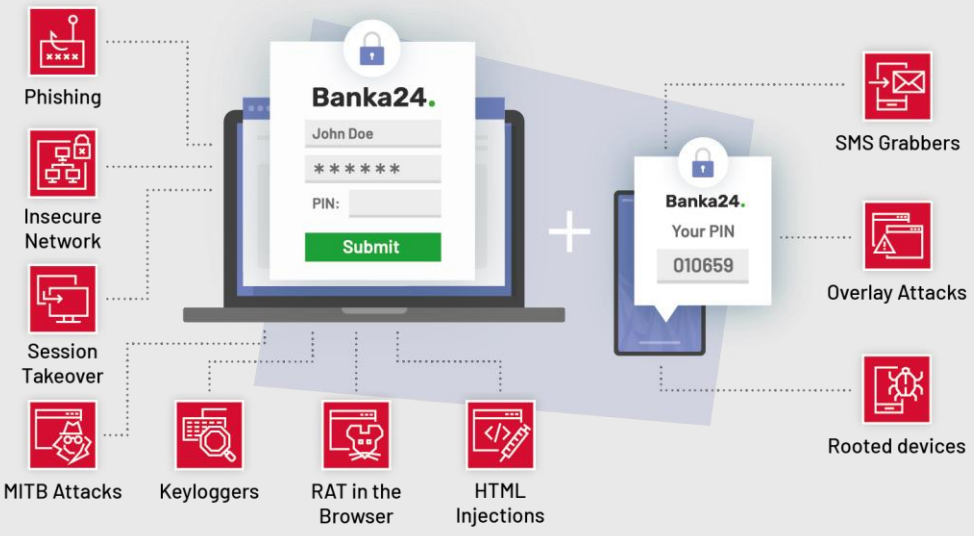

Figure 1 - Representation of threats ThreatMark AFS detects

DEEP BEHAVIORAL PROFILING

Everyone's behavior is unique. This is true for behavior in online applications as well. How one navigates throughout the app, how fast one clicks/taps/swipes or how one uses their keyboard, mouse or tap screen—is unique for every person..

In ThreatMark these markers are augmented with user-specific information, such as location, device, time and date, navigation patterns, transaction behavior and more. Combined, these deliver the best context-value resulting in decreased number of falsely rejected users and transactions while mitigating risk with a whole new level of precision.

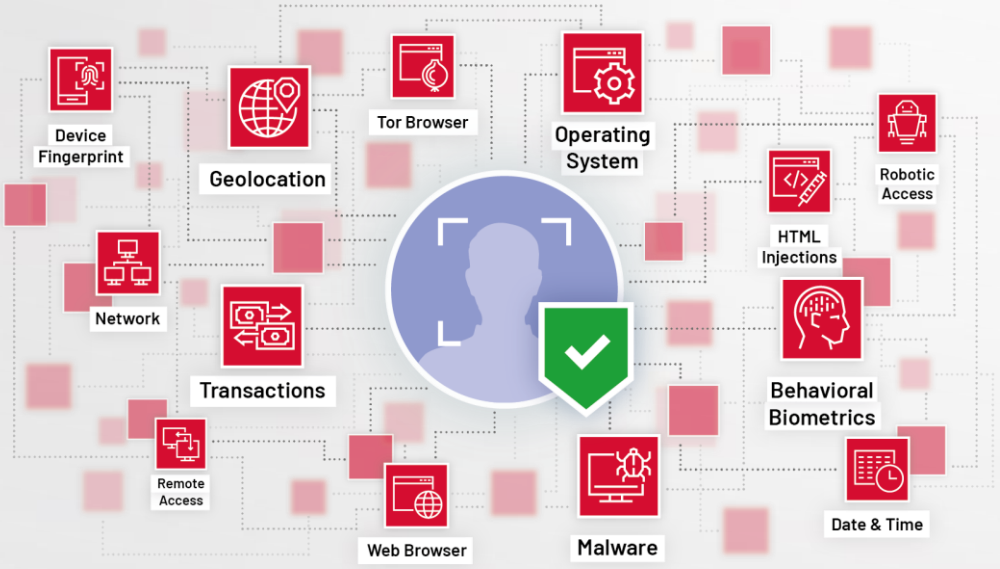

Figure 2 - ThreatMark's Trusted User Identity

TRANSACTION RISK ANALYSIS

User's spending behavior is closely monitored, analyzed, and it is compared to typical user behavior. Considered parameters include amount, frequency, time and other user entered values. All transactions are evaluated against various models.

Every model includes a group of rules corresponding to a transaction type, the channel used, etc.

AFS detection capabilities are not purely rule-based but are rather based on advanced Machine Learning that can adapt to new fraudulent scenarios not covered by any rules.

Our approach—fraud detection in a complete context, throughout the user journey—provides numerous benefits to banks as attested by our clients.

Key benefits banks see when implementing ThreatMark AFS

70%	90%	90%	2	
Better detection rate (than traditional FDS)	**Fewer false positives** (than traditional FDS)	**Decrease in cost for authentication** (est. SMS cost saving)	**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)