centro

ThreatMark
PREVIEW

ThreatMark Digital Identity Sensing Technology

Digital payment dangers are growing in terms of attacks faced and their volume. The majority of detected threats use specialized financial malware at least at one stage of an attack. Alongside malware driven attacks are ever more often fraudulent schemes based on social engineering methods, attempts to misuse the client's trust as well as phishing campaigns. More than one third of attacks use mobile channels or a combination of more payment / service channels.

Neither traditional-approach solutions based on transaction fraud detection, nor isolated signature-based solutions trying to detect malware on clients' stations is sufficient nowadays.

ThreatMark,
the Digital Identity Sensing Company
brings an alternative neXtGEN online fraud detection solution able to detect traditional as well as modern threats that jeopardize Internet banking and transaction systems.

Enhance your Digital Banking.

Attacks detected by ThreatMark

Financial malware · Account takeover · Session stealing · Phishing · Social engineering · Fraudulent transactions · Web hacking · Insecure configuration

Fraud Detection using Digital Identity Sensing Technology

ThreatMark uses Digital Identity Sensing Technology (DIST) to tell users and fraudsters apart.

This unique set of techniques was developed by ThreatMark because traditional fraud detection methods could not keep up with modern threats and complex online environments.

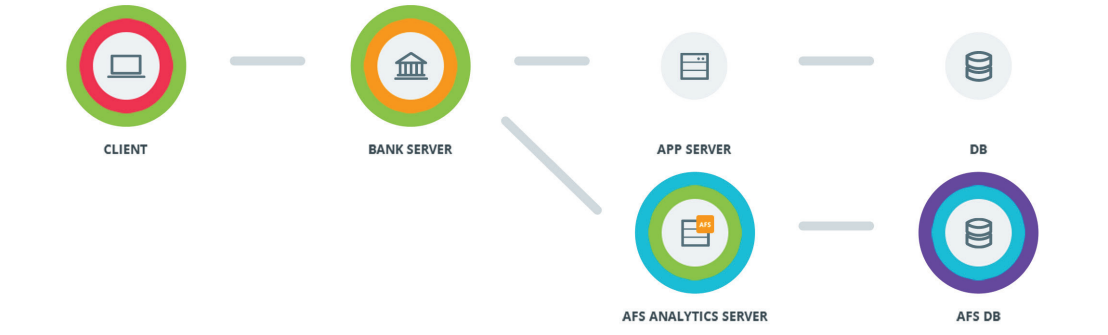
DIST is based on the assumption that every user is identifiable by his or her behavior patterns, biometric markers and typical actions. By analysis of such parameters using the latest advances in Machine Learning and Artificial Intelligence, we are able to detect minor changes on the user side and spot the fraud even in the creation phase, which was previously impossible.

DIST uses a layered approach to protection. At each stage of user interaction with the protected application neXtGEN security checks are applied to detect fraud which together with additional layers of security provided by the system also increases security of the application users.

We also use multiple approaches traditionally found in solutions like:

- **Fraud Detection Systems (FDS)**
- **Online Fraud Detections Systems (OFDS)**
- **Web Fraud Detection (WFD)**
- **Web Application Firewall (WAF)**

ThreatMark Solution Architecture



Device aware — Layer 1
- Identification, Fingerprinting
- Device Security Check
- Malware Detection

Session aware — Layer 2
- Changing Facility, Geolocation
- Application Flow
- Collection of Navigation and Activity Data

User aware — Layer 3
- Behavioral Profile
- Biometric Profile
- History of Actions
- History of Equipment

Transaction aware — Layer 4
- Transtaction Scoring
- Moneymule Blacklist
- Static Rules
- User's Credit Profile

Big Data Analytics — Layer 5
- Anomaly Detection
- Agregation of Signals
- Crowd Data Comparison

Gartner Layers of Fraud Prevention

1. Endpoint Centric → 2. Navigation Centric → 3. User and Accounts Centric for Web & Mobile
4. Cross Channels → 5. Entity Link Analysis

Our solution uses correlation of data from probes working silently on a client's station and from server components analyzing traffic between the application and users.

This approach together with advanced machine learning methods, statistics, user defined rules and detection capabilities of individual modules designed for specific attack classes means that the ThreatMark Digital Identity Sensing Technology reacts not just to known threats and attacks threatening modern applications and their users but also enables reaction to new, not yet known threats and frauds.

We provide more than the capabilities such solutions could ever provide when used separately due to the synergic effects of all the unique methods that we use.

All capabilities in **one Solution.** One Solution for all purposes.

One out of many advantages of the ThreatMark Solution compared to common Fraud Detection Systems is the ability to collect and evaluate in-session data (speed and timing of actions, user activity, user interaction with application and more).

This approach in combination with user behaviour tracking and seamless biometry dramaticly improves detection capabilities of the known as well as currently unknown real world threats.

BENEFITS & ADVANTAGES

CLIENT BENEFITS

- Non invasive / intrusive
- More secure banking
- Less passwords and tokens
- More secure transactions
- Better client experience
- More trusted relations

DIGITAL BUSINESS BENEFITS

- Less present and future attack
- Less fraud
- Better client experience
- Client trust
- New digital service models
- Huge savings
- Larger profits

IT ADVANTAGES

- No additional cost
- Fully managed service
- Easy deployment in days

ThreatMark Solution Integration

Easy deployment, in 3 steps:

1. ThreatMark Web Server Module installation
2. ThreatMark Analytics Server setup
3. Redirects, Firewall rules update

Stop online fraud and cyberattacks in weeks

Don't hesitate to contact us

Our multi-layered neXtGEN anti-fraud solution will protect your business against actual and forthcoming cyber threats and attacks and will support your key business goals.

There are multiple ways how ThreatMark Solution can be used and we will gladly show you what we can do for you.

ThreatMark

centro

PT CENTRASOLUSI INTISELARAS
Ruko Golden Boulevard Blok R2 No. 38-39
Jl. Pahlawan Seribu - BSD.
Tangerang 15322. Indonesia
Phone:(62-21) 5316 3238 Fax:(62-21) 5316 3239

www.csolusi.com