ThreatMark

Bringing Trust to the Digital World

OTA CERMAK
Head of sales

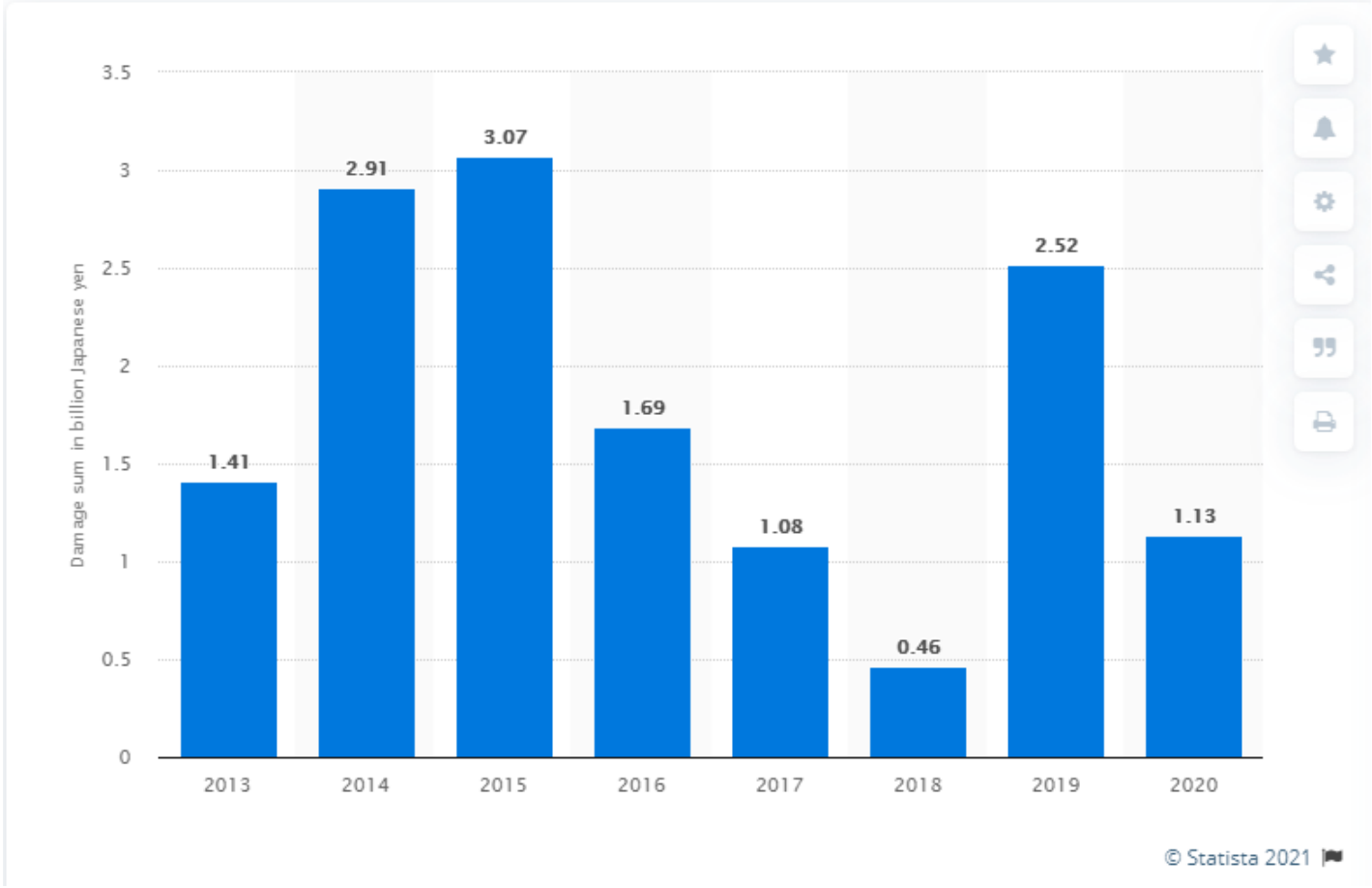
日本人の連絡先
emong-zheng@isec.ne.jp

Information Security Inc.
3F Seihokushin Bldg. 4-9-26 Kitanagasadori,
Chuo-ku, Kobe, Hyogo, 650-0012 JAPAN
https://www.isec.ne.jp/

Anti-Fraud Suite

Holistic approach to online banking security

(in billion Japanese yen)



*Amount of money lost through damages caused by online banking fraud in Japan 2013-2020

Account takeover

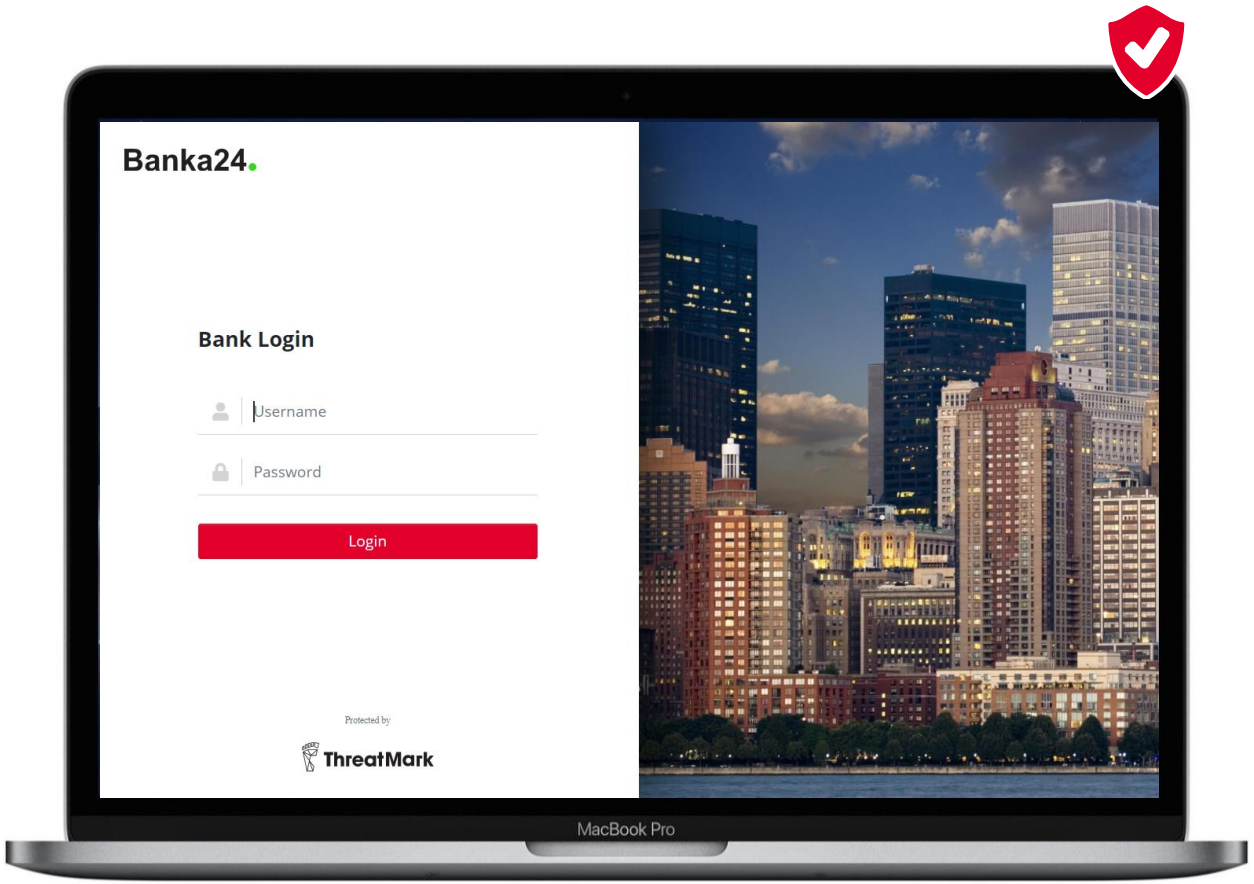
Phishing

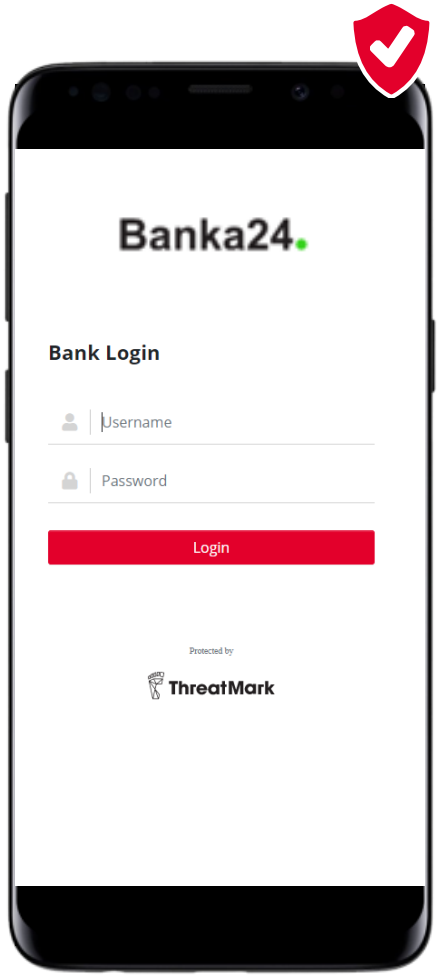
Vishing

Remote access trojan

Stolen credentials…

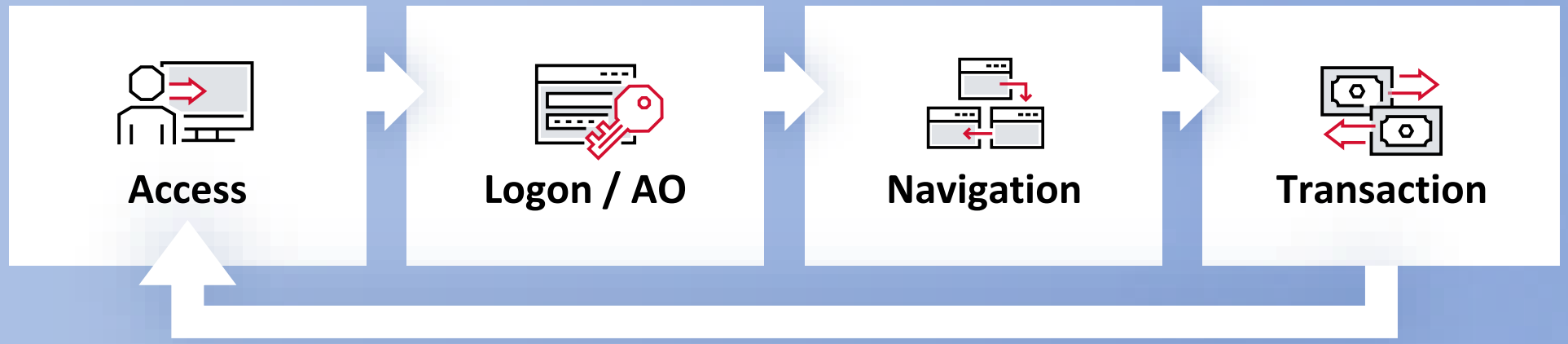
Protection for banking digital channels





To secure the entire digital customer journey

MOBILE WEB



Our Approach

MOBILE WEB

Access

- Connection check (TOR, anon proxy)
- Browser and OS security check
- Malware, phishing
- Device fingerprint

Logon / AO

- GeoIP check
- Login time check
- Logon biometrics
- Velocity checks
- Action context

Navigation

- Clickstream profiling
- Scripted access & automation detection
- Session hijacking
- Behavior & app interaction biometrics

Transaction

- Money mule blacklist
- Anomalous transactions
- Behavioral profiling

LAYER 1
Early Warning Threat Detection

LAYER 2
Legitimate User Identity Validation

LAYER 3
Payment Transaction Risk Analysis

Phishing, malware, vishing (RAT), BOTs detection

Threat Mitigation

SOC &Threat Intelligence

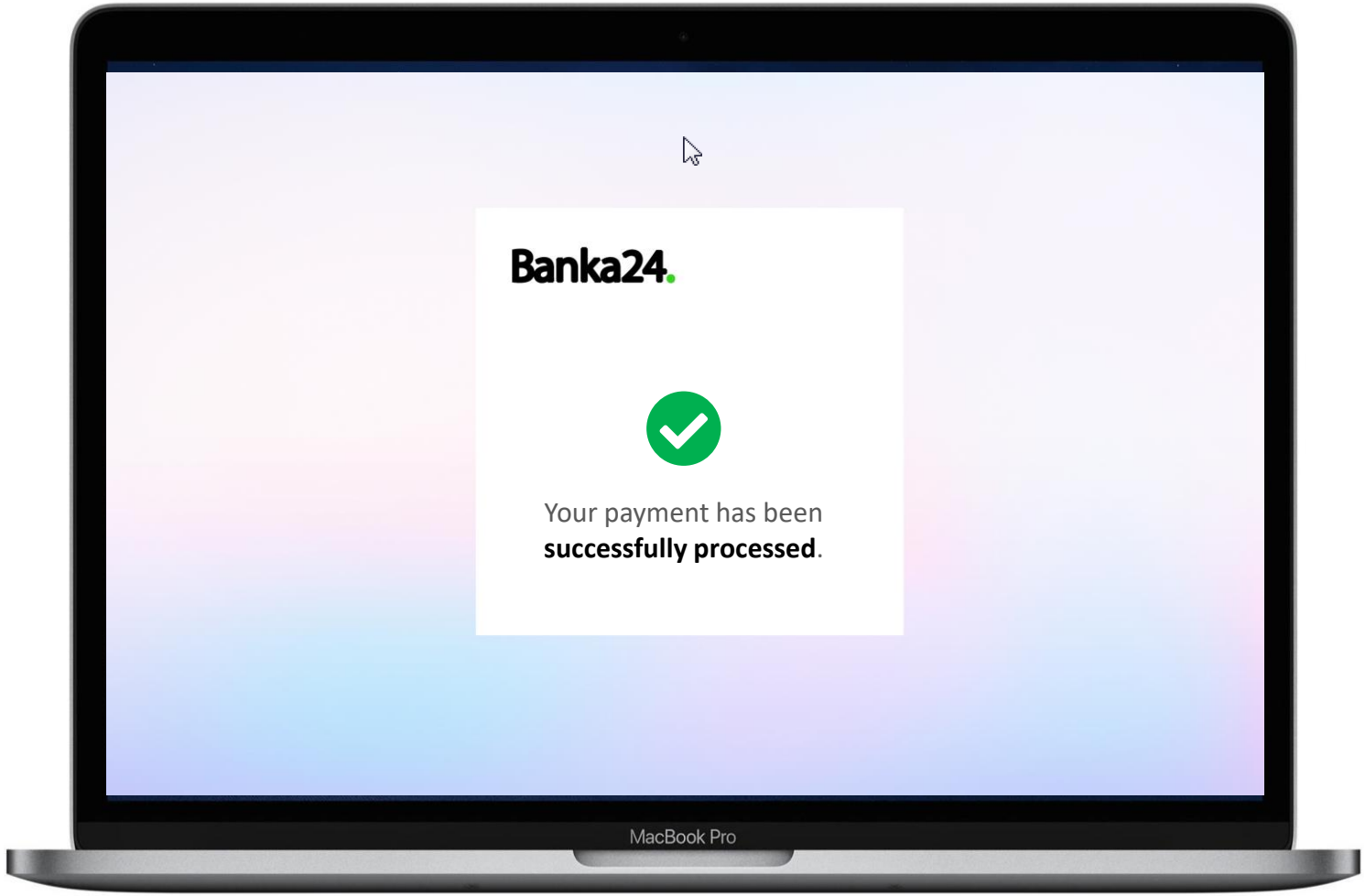
Detecting Account Takeover

Detecting Account Opening Fraud

Transaction Monitoring & RA

Reporting & Compliance

To TRUST you need to know...

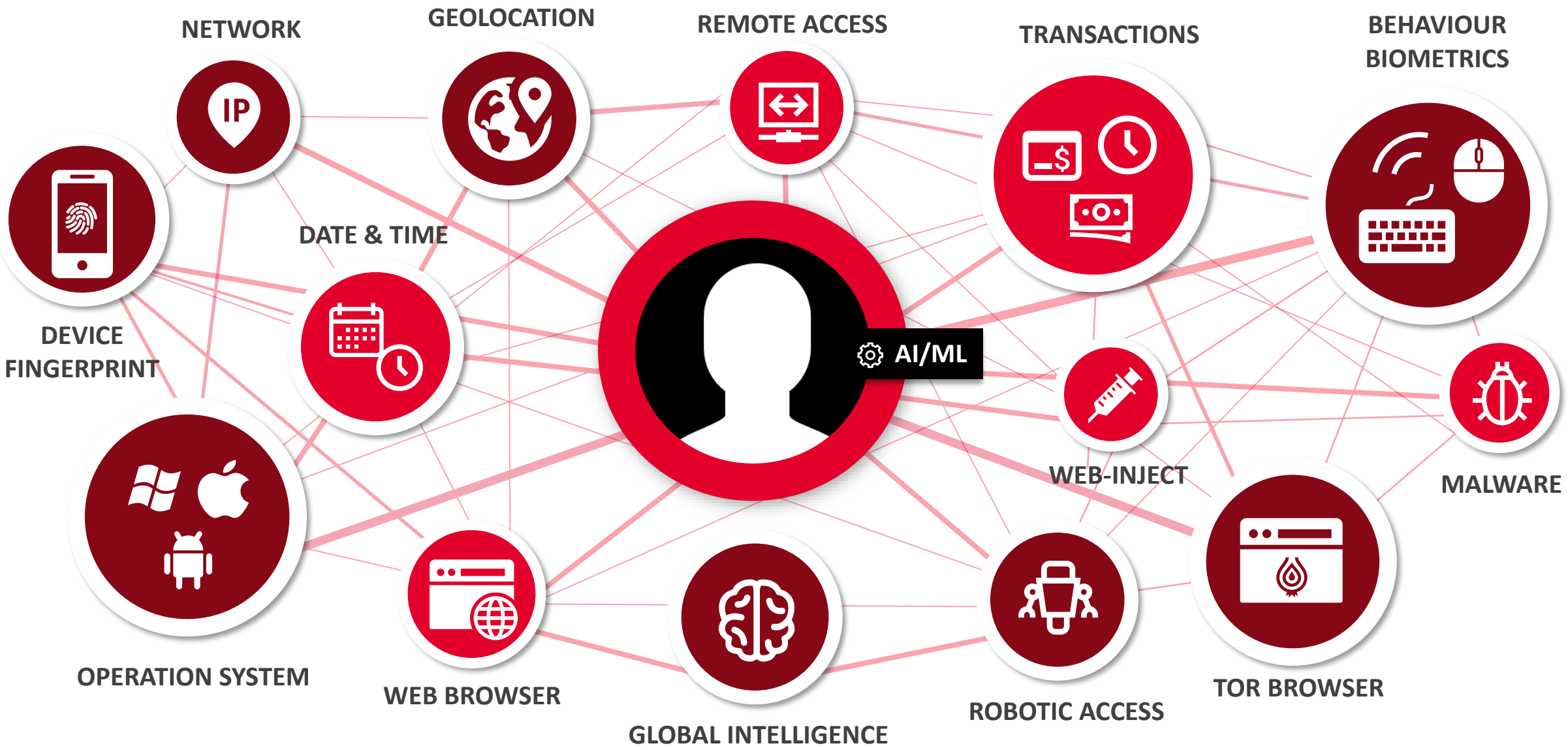


- **Is it your device?**
- **Is it a secure environment?**
- **Is this you?**
- **Is this your typical payment?**

Low risk during the whole journey

TRUSTED PAYMENT

HOW do we do it



Holistic View Is The Key

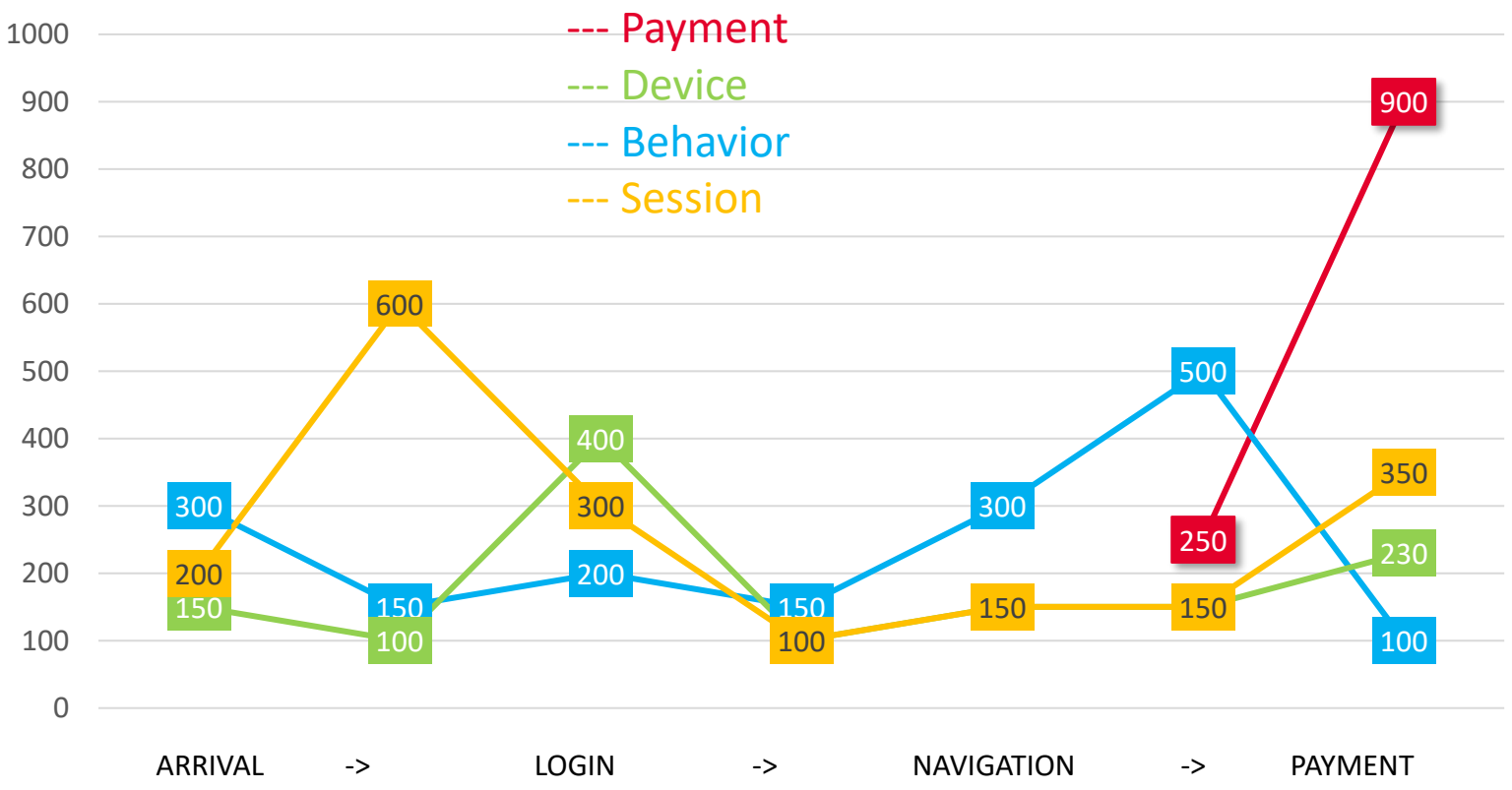
Typical False Positives:

- Suspiciously high amount
- Suspicious time
- Suspicious place
- Suspicious target account nr.

Typical False Negatives:

- Transfer initiated as result of social engineering
- Transfer initated by malware
- Transfer initiated by BOT
- Transfer inititated via RAT

Holistic View Is The Key

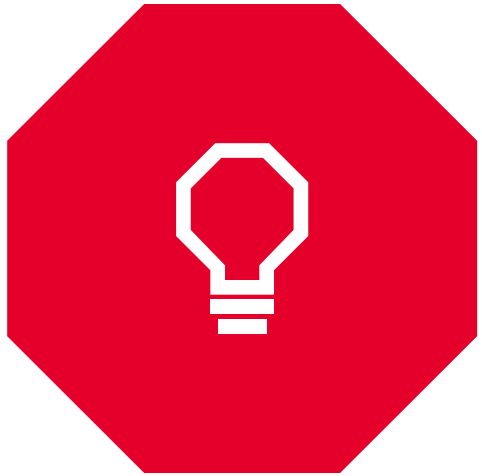


Typical False Positives:

- Suspiciously high amount ✓
- Suspicious time ✓
- Suspicious place ✓
- Suspicious target account nr. ✓

Typical False Negatives:

- Transfer initiated as result of social engineering ✓
- Transfer initated by malware ✓
- Transfer initiated by BOT ✓
- Transfer inititated via RAT ✓



Main Use Cases

Main Use Cases for ThreatMark

Online Fraud Prevention

**Through cyber threats detection,
identity verification and transaction risk analysis**

Better detection rate
than IBM Trusteer*

* Results based on independent test results from a bank

Main Use Cases for AFS

Invisible 2nd Factor Authentication

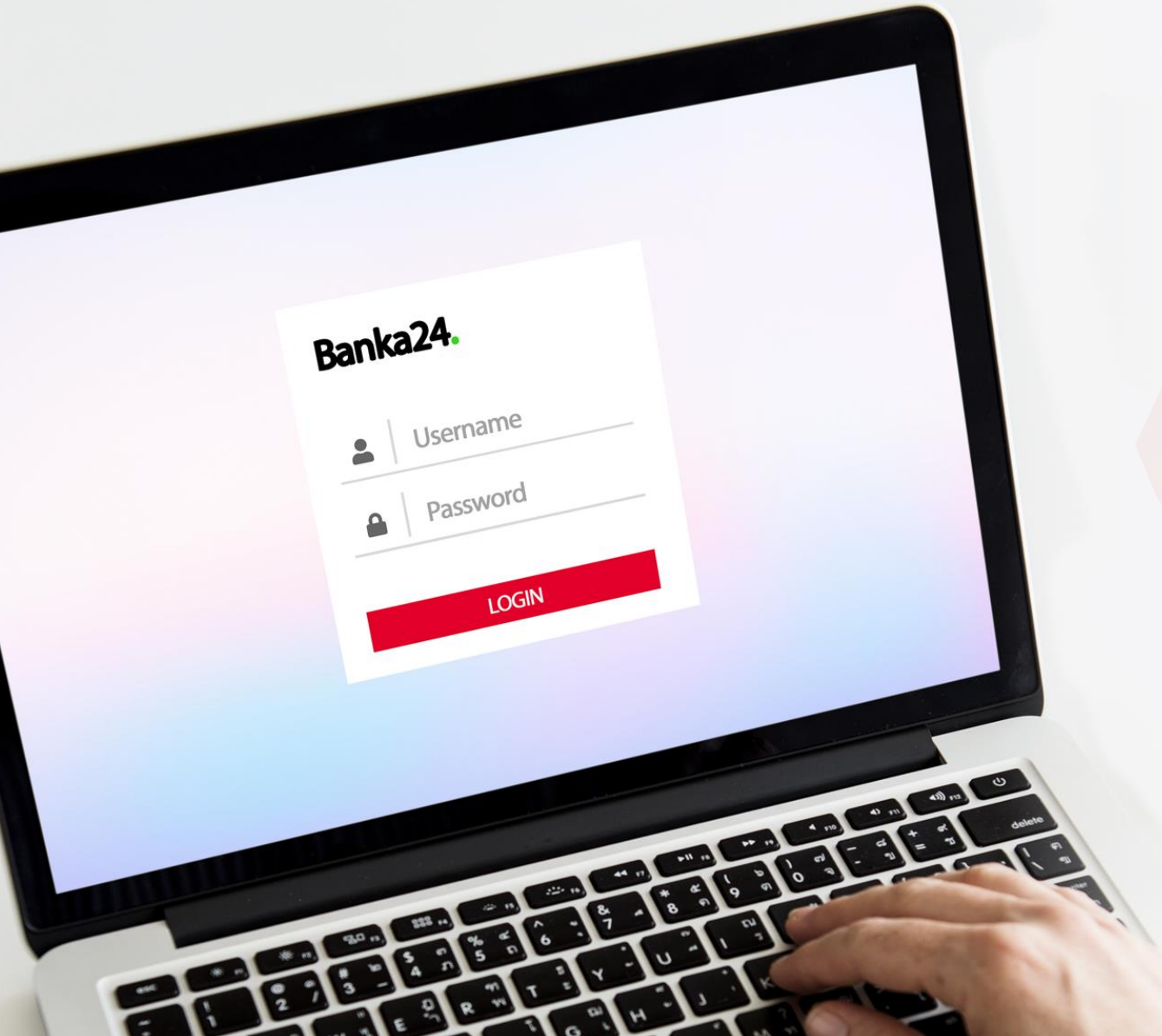
SMS Cost reduction by using AI-powered Adaptive Authentication

Seamless User experience

1M USD Saved per year

* Results based on independent test results from a bank

Main Use Cases for AFS



Reduction of False Positives

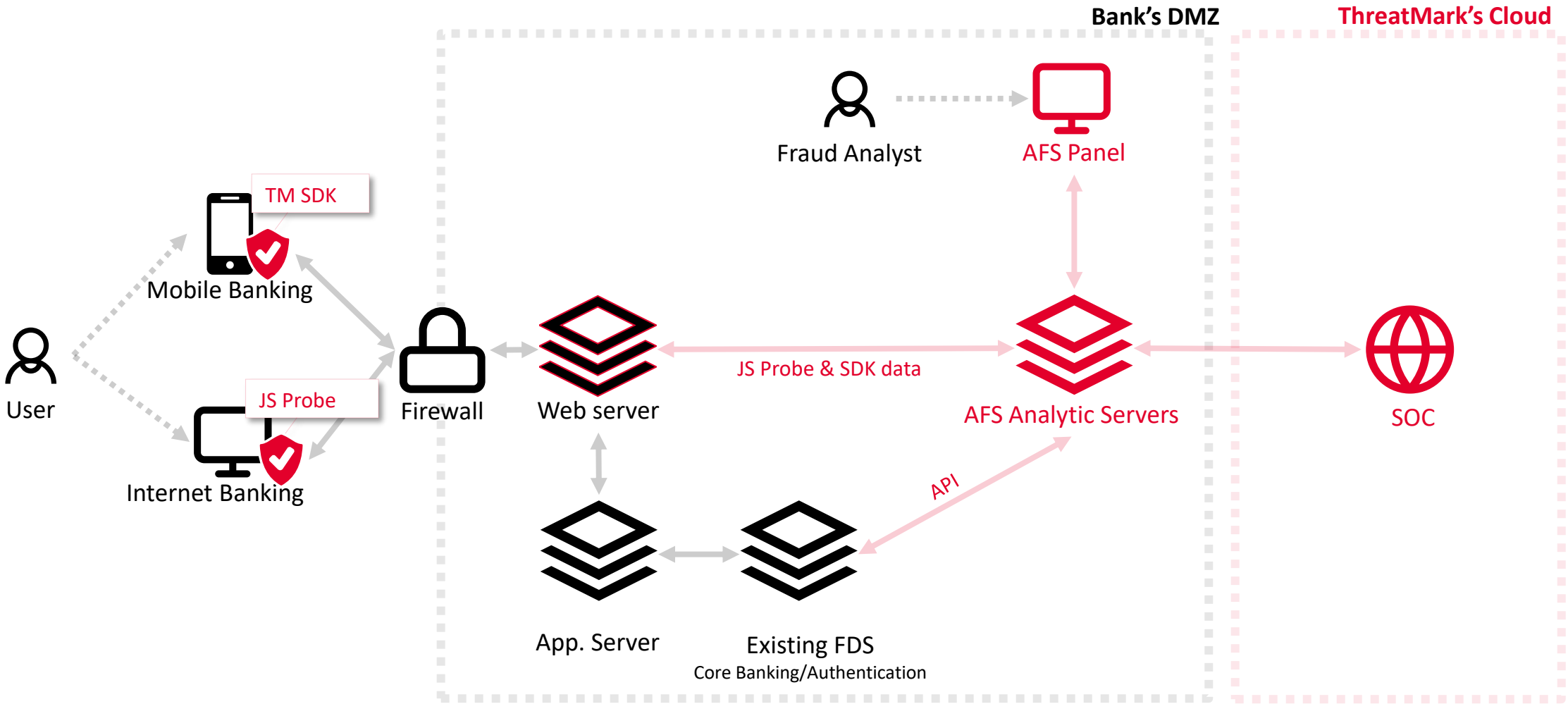
Save resources otherwise spent on manual investigation

99%

Less false positives than F5 WebSafe

* Results based on independent test results from a bank

Architecture



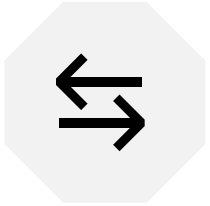
Easy Deployment in 7 Days

AFS ONLINE WEB PROBE

Implement JavaScript probe in form of simple “one liner” into protected Web Page.

AFS ANALYTICS

Setup AFS ANALYTICS infrastructure.
Optional: AFS can be deployed in your infrastructure.



INTEGRATE

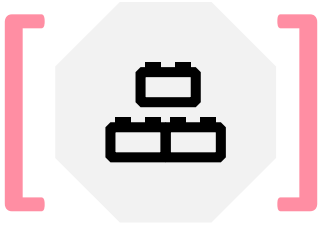
Optional: Use API for full integration with any internal and/or 3rd party system.

AFS ENDPOINT MOBILE PROBE

Implement TM SDK library into your Native Mobile Application if needed

SETUP CONNECTION

Allow connection to AFS ANALYTICS infrastructure.



About ThreatMark

Founded in 2015
by former Ethical Hackers

Made in Czech Republic
Active on 4 continents

25+ million
clients protected

65+ Experts
focused on one product

High-tech Security Company
Behavioral biometrics & AI/ML

1 billion logins
Scored yearly

Selected over Bigger Competitors
by large international banking groups

Trusted by EU's leading banking groups
ERSTE, Raiffeisen, Sberbank

Deloitte.

Gartner

EY Entrepreneur Of The Year
2019 Award Winner

AI awards 2019
Company of the Year 2019

ThreatMark AFS

Trusted by Banks and Global Partners

Partnerships

HID Powering Trusted Identities
NTT dimension data
ARICOMA GROUP
AEC
CERTICOM
CGI
.BSC
innovera We enable.
SOFTPROM VALUE ADDED IT DISTRIBUTOR

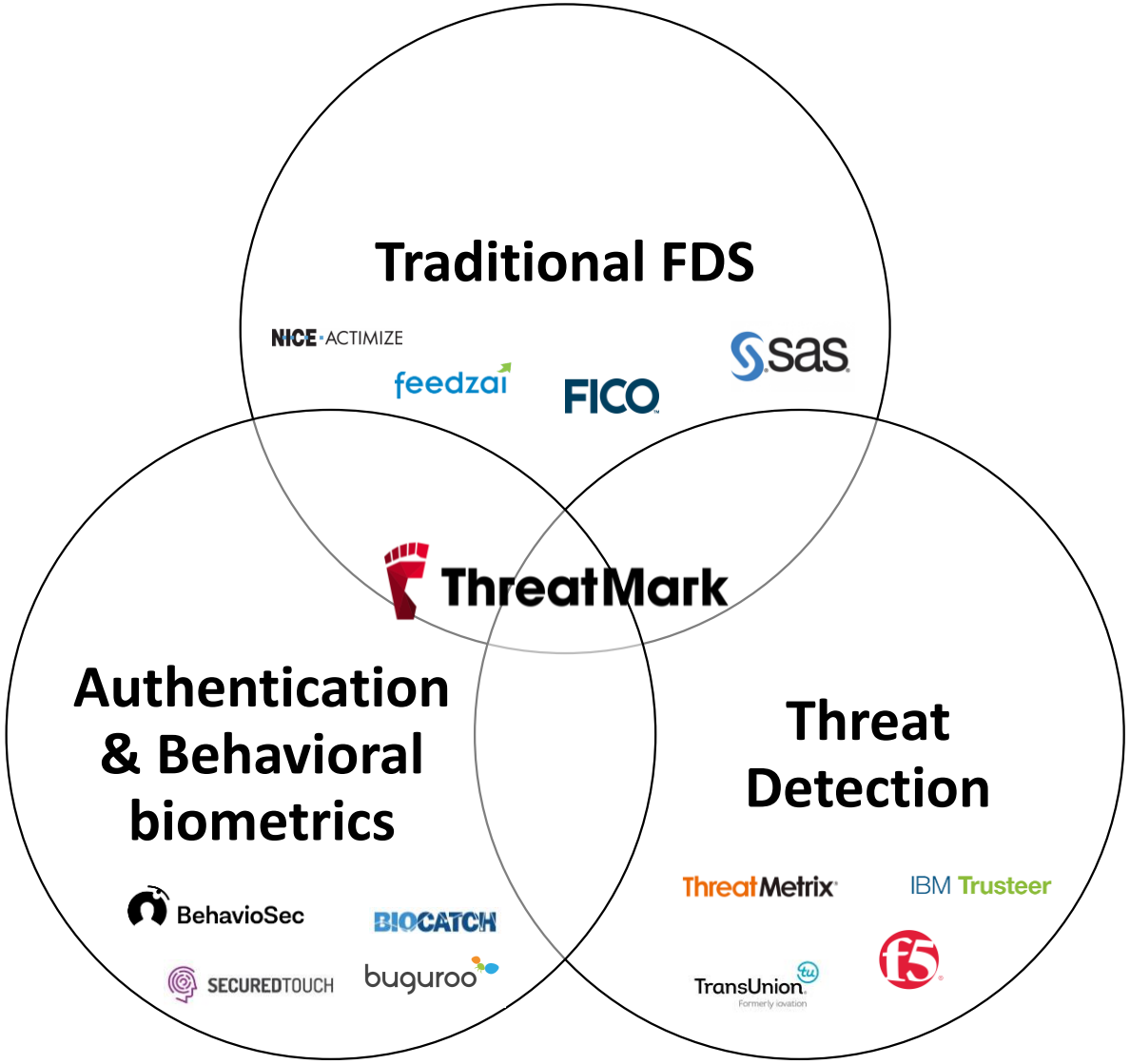
Banking references

ERSTE Group
MONETA MONEY BANK
SBERBANK
poštová banka
CREDITAS
Equa bank
B2B BANK
arab african international bank
AKBANK

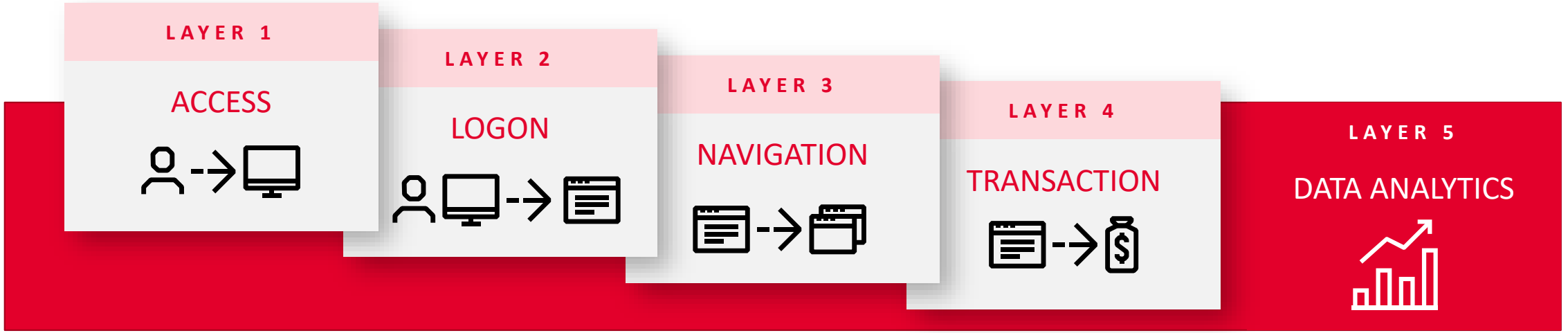
Planned / Running PoCs

ČSOB
PostFinance
BNP PARIBAS
ALIOR BANK

Competitive positioning



Online banking session protection - summary



- Connection check (TOR, anon-proxy)
- Browser and OS security check
- Malware, phishing
- Device fingerprint

- GeoIP check
- Login time check
- Login biometrics
- Velocity checks
- Action context

- Clickstream profiling
- Scripted access and automation detection
- Session hijacking
- Behaviour and app interaction biometrics

- Money mule blacklist
- Abnormal spending behaviour
- Transaction Integrity

- Big Data AI/ML
- Continuous User profiling
- Human Feedback re-learning
- Business Rules

ThreatMark‘s Trusted Identity

ThreatMark Trusted Identity

Shared Intelligence and Orchestration

AFS Payments

Payments
- Payment Anomalies / Behavior
- Payment Rules and Alerts
- Mule/Fraudster Accounts
- Shared Fraud Schemes

Actions
- Suspicious Sequence
- Fraudsters IP Reputation
- Case Management
- Known Fraudulent Actions

Channels
- Web/Mobile/OpenAPI Payments
- Omnichannel Geo fencing
- Cross-channel fraud detection
- PSD2 Authorization Schemes

App./Device hacking
- Application Debugging
- Application Cloning
- Emulator Detection
- Device Security Profiling

Behavior
- Date/Time behavior
- Device Usage behavior
- Fraudulent Accounts / Identities
- Shared Identities / Devices
- Crowd Spending behavior

AFS Identity

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 Users/Identities
- Shared Identities/Devices

AFS Threats

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

App./Device hacking
- Application Debugging
- Application Cloning
- Emulator Detection
- Device Security Profiling

どうもありがとうございました

Ota Cermak

Sales director

ota.cermak@threatmark.com

www.threatmark.com

日本人の連絡先

emong-zheng@isec.ne.jp

Information Security Inc.

3F Seihokushin Bldg. 4-9-26 Kitanagasadori,

Chuo-ku, Kobe, Hyogo, 650-0012 JAPAN

https://www.isec.ne.jp/