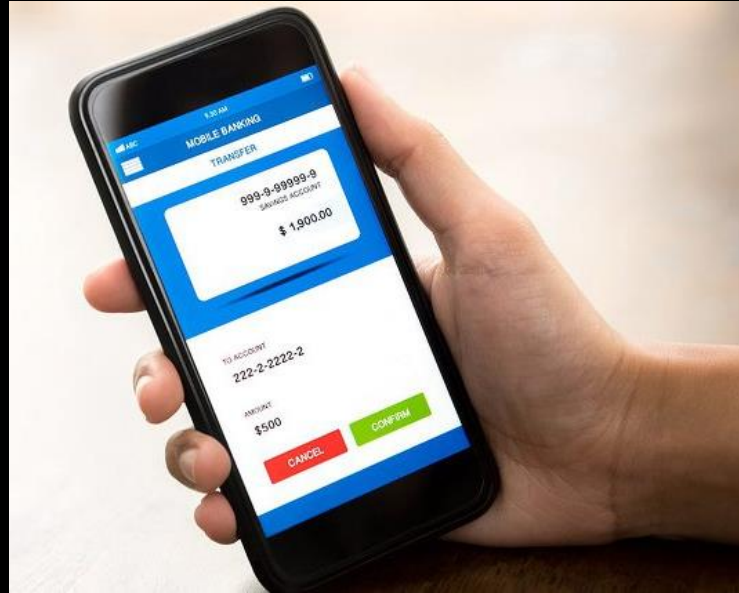


규제 준수를 넘어 선제적 대응으로,
AI와 클라우드 기반 지능형 금융 사기 방지

박형근 실장

한국IBM, 보안 사업부

코로나 이후, 손 안의 금융 서비스



간편인증 정부24

카카오톡	KB모바일 인증서	페이코	삼성페스	통신사 인증서 (SKT, KT, LG U+)
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

이름	<input type="text" value="홍길동"/>
생년월일	<input type="text" value="19900101"/>
휴대폰번호	<input type="text" value="010"/> <input type="text" value="12341234"/>



디지털 신뢰성 확보가 기업 비즈니스를 결정합니다

사기



ID 도난

- 실제 사용자 정보 도난

사기



조작된 ID

- 조작된 ID 혹은 Bot

고객 이탈



사용자 경험 저해

- 너무 많거나 너무 적은 보안

영향도

- 개인 및 기업

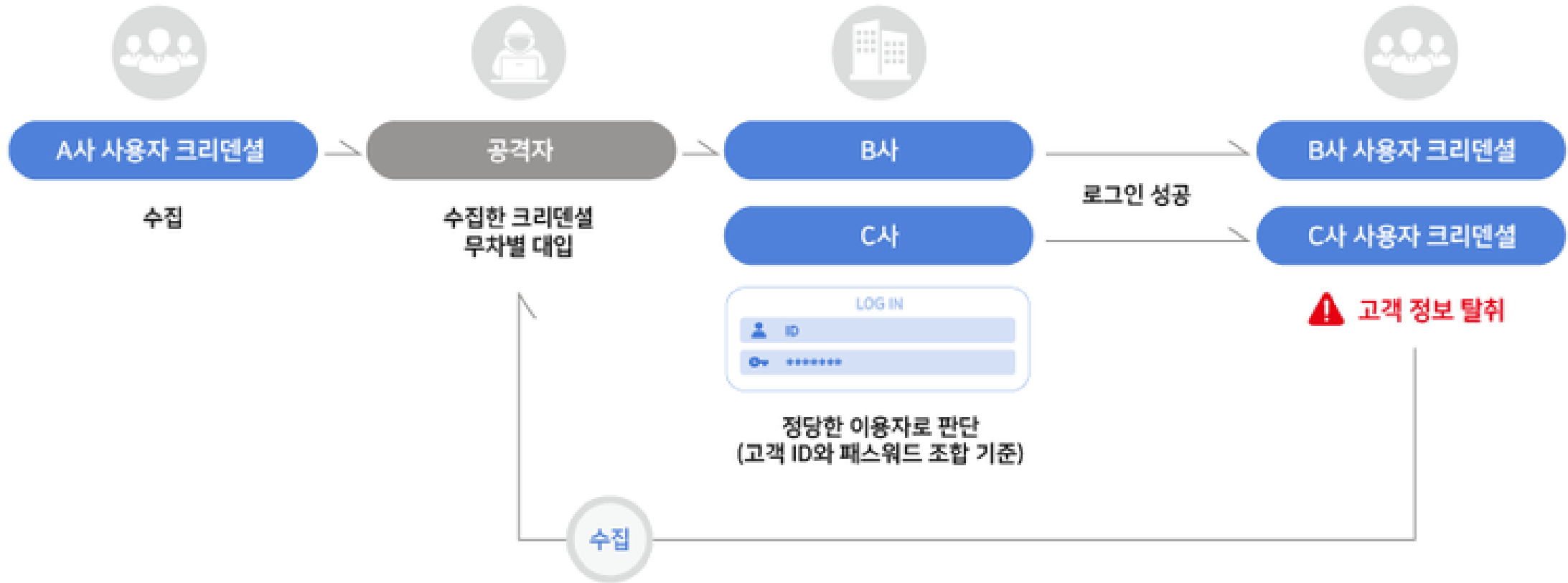
- 기업

- 기업

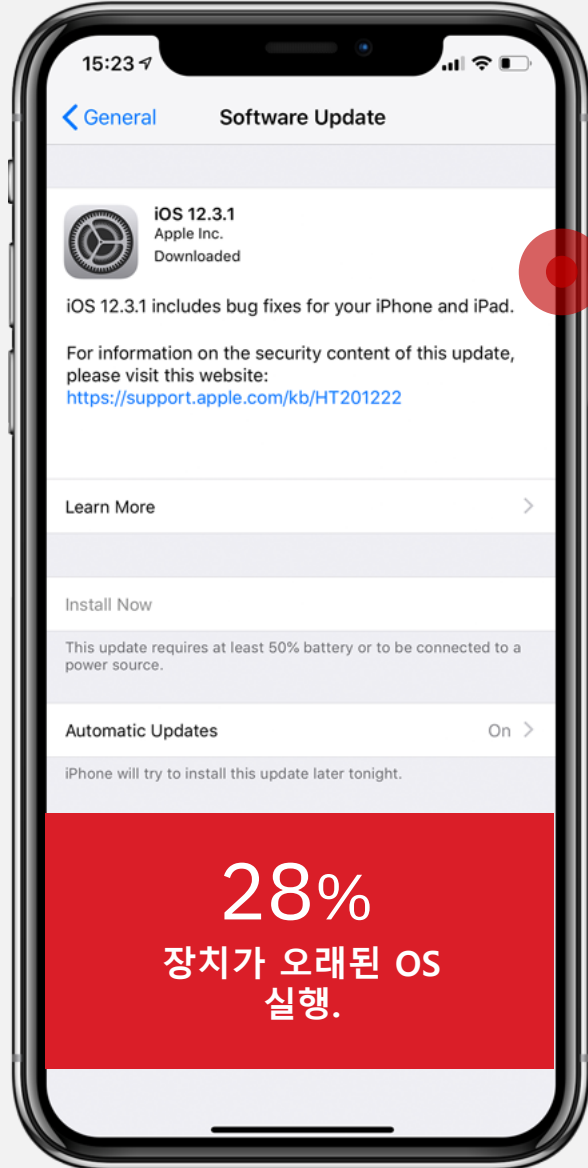
디지털 사기 방지 비용 절감

고객 이탈 방지

크리덴셜 스테핑(Credential Stuffing)



다양한 모바일 위험

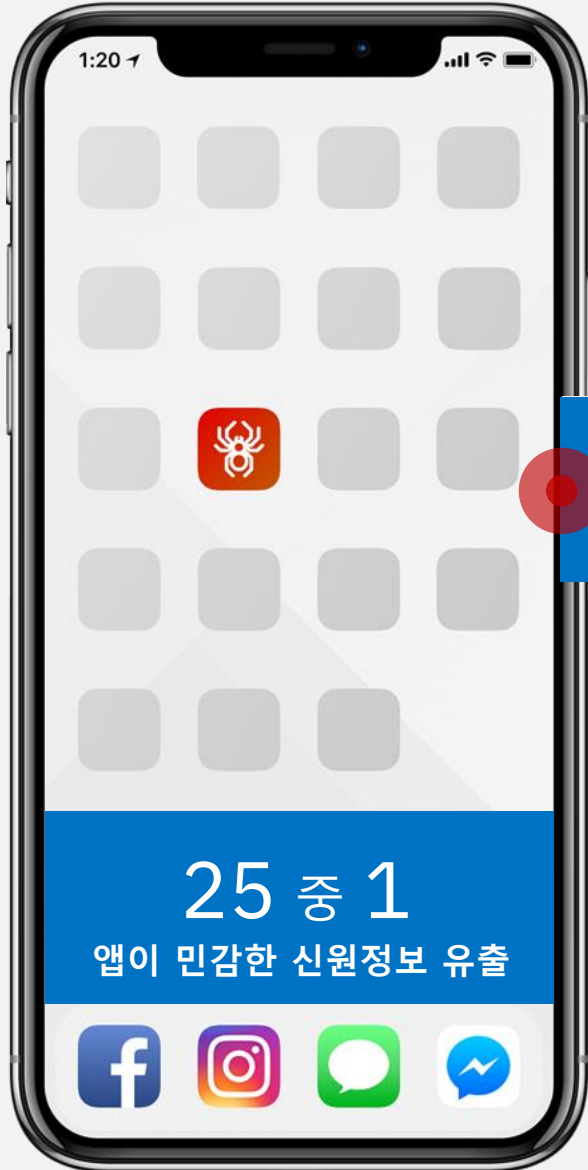


디바이스 위험

28%
장치가 오래된 OS
실행.



다양한 모바일 위험



앱 위험

WhatsApp Pegasus

보안 결함으로 인해 해커는 사용자에게 전화를 걸어 감시 스파이웨어를 트리거할 수 있었습니다. iOS와 Android 모두에 영향을 미쳤습니다.

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

NSO GROUP RINGING —

WhatsApp vulnerability exploited to infect phones with Israeli spyware

Attacks used app's call function. Targets didn't have to answer to be infected.

DAN GOODIN - 5/14/2019, 3:00 AM

Santeri Vinnamöki

Enlarge

80

Attackers have been exploiting a vulnerability in WhatsApp that allowed them to infect phones with advanced spyware made by Israeli developer NSO Group, the Financial Times reported on Monday, citing the company and a spyware technology dealer.

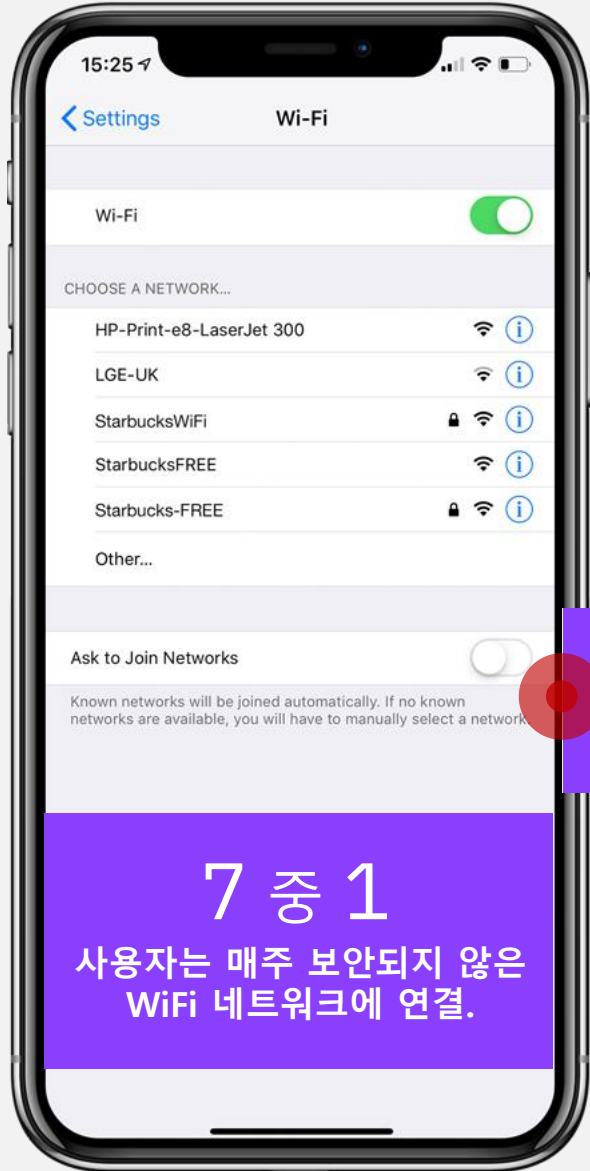
f

t

A representative of WhatsApp, which is used by 1.5 billion people, told Ars that company researchers discovered the vulnerability earlier this month while they were making security improvements. CVE-2019-3568, as the vulnerability has been indexed, is a buffer overflow vulnerability in the WhatsApp VOIP stack that allows remote code execution when specially crafted series of SRTP packets are sent to a target phone number, according to this advisory.

According to the Financial Times, exploits worked by calling either a vulnerable iPhone or Android device using the WhatsApp calling function. Targets need not have answered a call, and the calls often disappeared from logs, the publication said. The WhatsApp representative said the vulnerability was fixed in updates released on Friday.

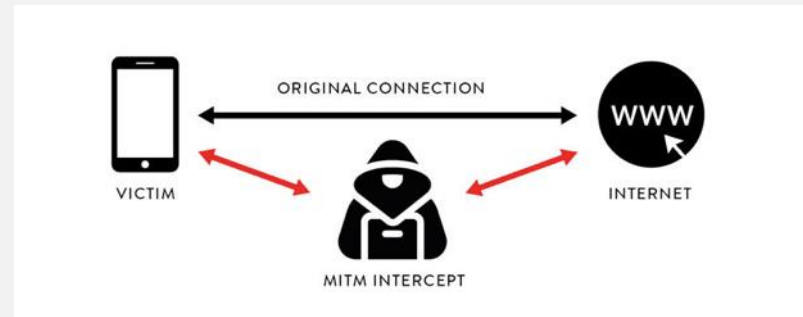
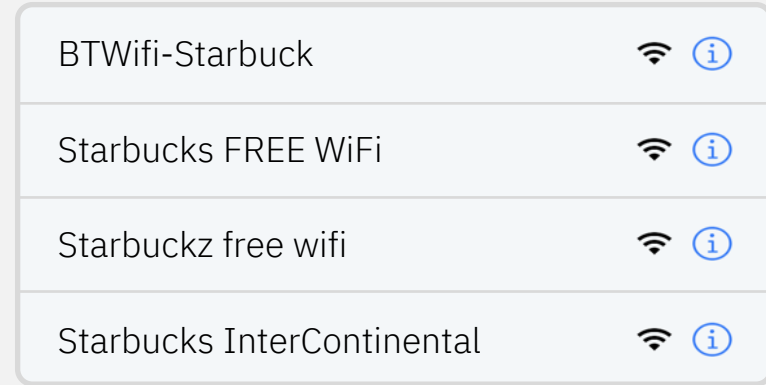
다양한 모바일 위험



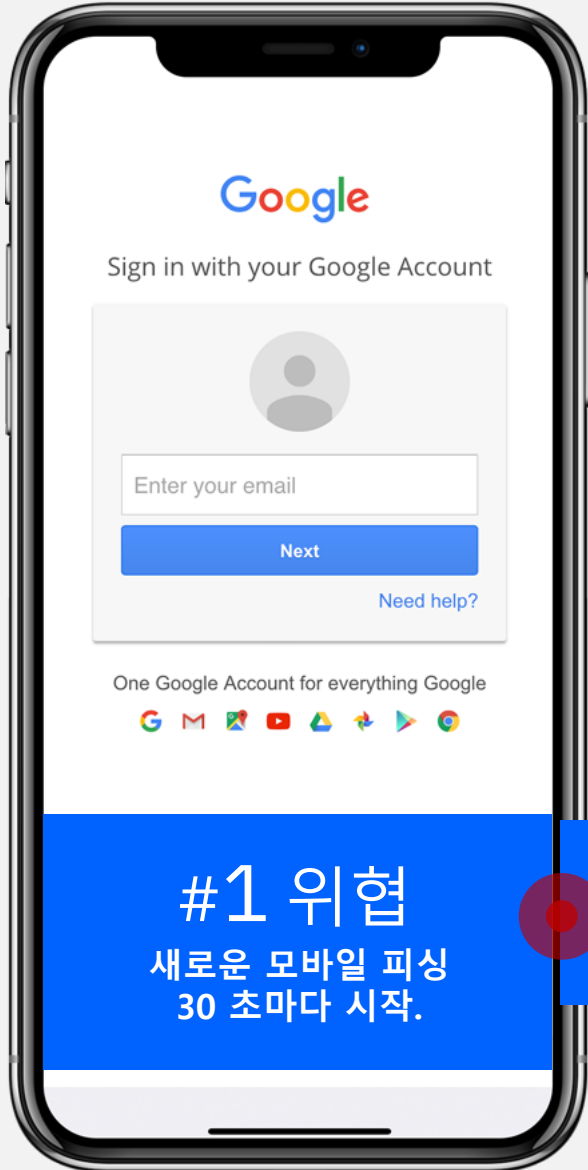
네트워크 위험

7 중 1

사용자는 매주 보안되지 않은 WiFi 네트워크에 연결.



다양한 모바일 위험



#1 위험

새로운 모바일 피싱
30 초마다 시작.

콘텐츠 위험

디지털 사기 방지 - 사용자 신원에 대한 신뢰도 이슈



기존 인증 방식



<p>지식기반 (Knowledge)</p>	<p><u>Something you KNOW</u></p> <ul style="list-style-type: none">• 패스워드• KBA(미리 설정한 질문답변) 등		<ul style="list-style-type: none">• 패스워드 재사용• 사용자 피싱• 크리덴셜 도난
<p>소유기반 (Possession)</p>	<p><u>Something you HAVE</u></p> <ul style="list-style-type: none">• SMS인증, OTP 등• Device ID		<ul style="list-style-type: none">• SMS 도난• Device 스푸핑• 원격 접속 제어(RAT)
<p>속성기반 (Inherence)</p>	<p><u>Something you ARE</u></p> <ul style="list-style-type: none">• 지문/얼굴 인식 등		<ul style="list-style-type: none">• 지문 복제• 음성 녹음

Current Global Fraud Trends

Credential Stuffing

Cross-Channel Fraud

RAT & Mobile Attacks

Mobile Overlay
Malware & IBAN
Swapping

Overlay RAT
spreads in
LATAM

Sim Swap &
Phishing

Web Injection /
Malware imposes
session redirect



디지털 신뢰성(Digital Trust)

key to customer relationships in the digital age

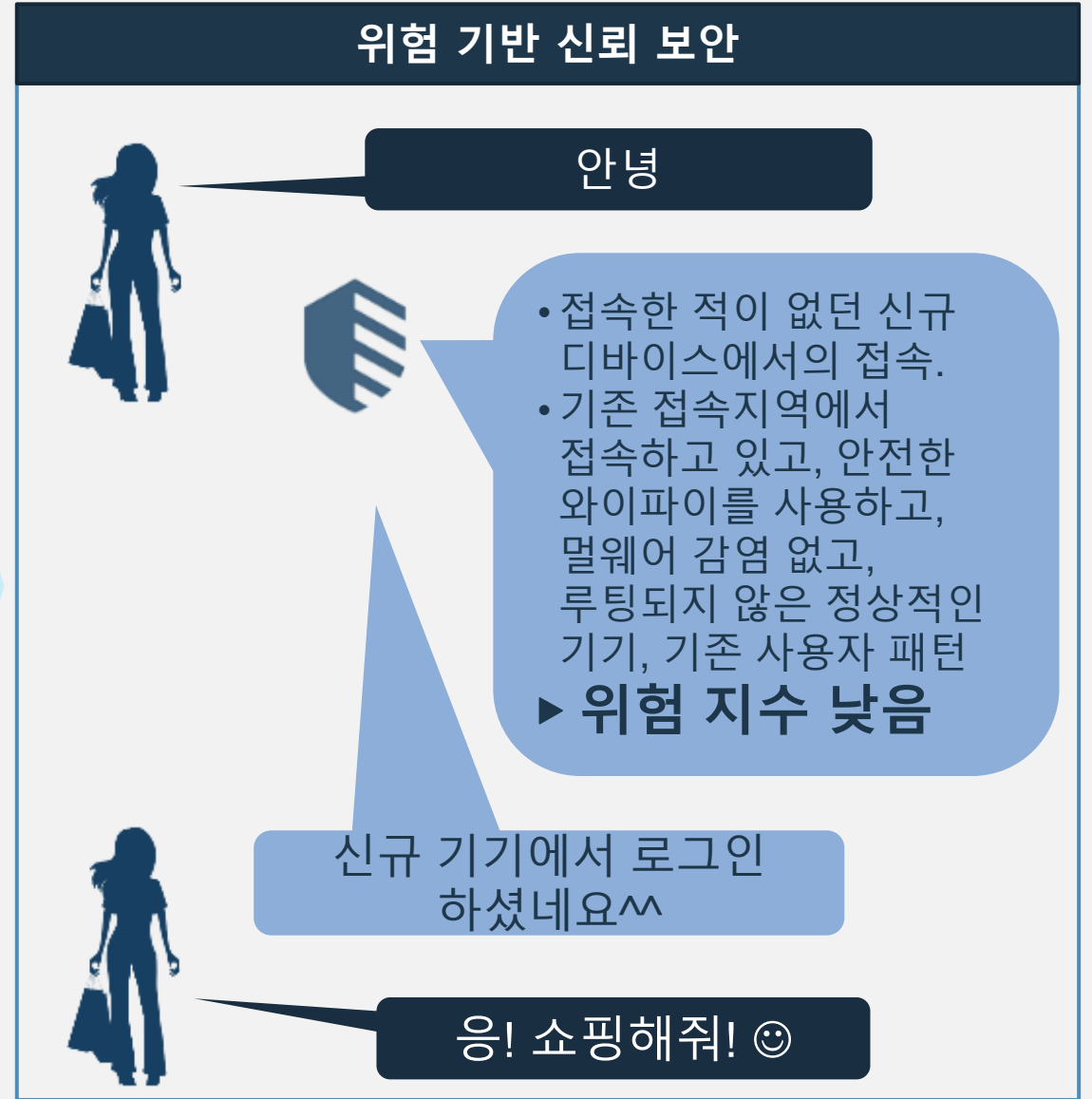


더 나은 고객 경험을 위한 위험 기반 인증

기존의 패스워드 기반 보안



위험 기반 신뢰 보안



Digital Identity Trust strategy

Security should not be a barrier but a business enabler, if you build it right

Loss prevention & fraud detection, keep bad guys out



Digital identity protection, help your customers trust you to do more business with you



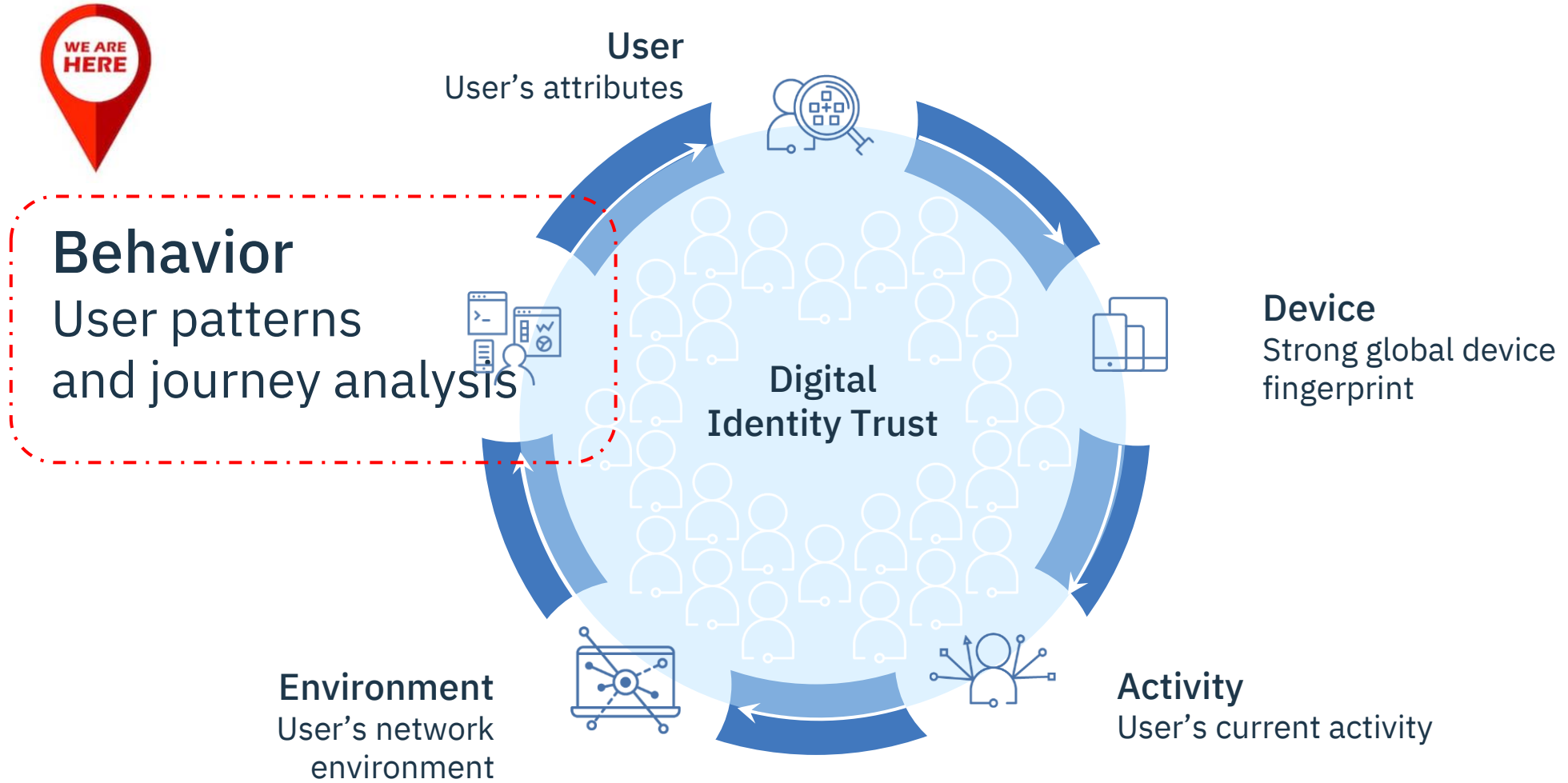
Frictionless experience, make sure your security is not a barrier

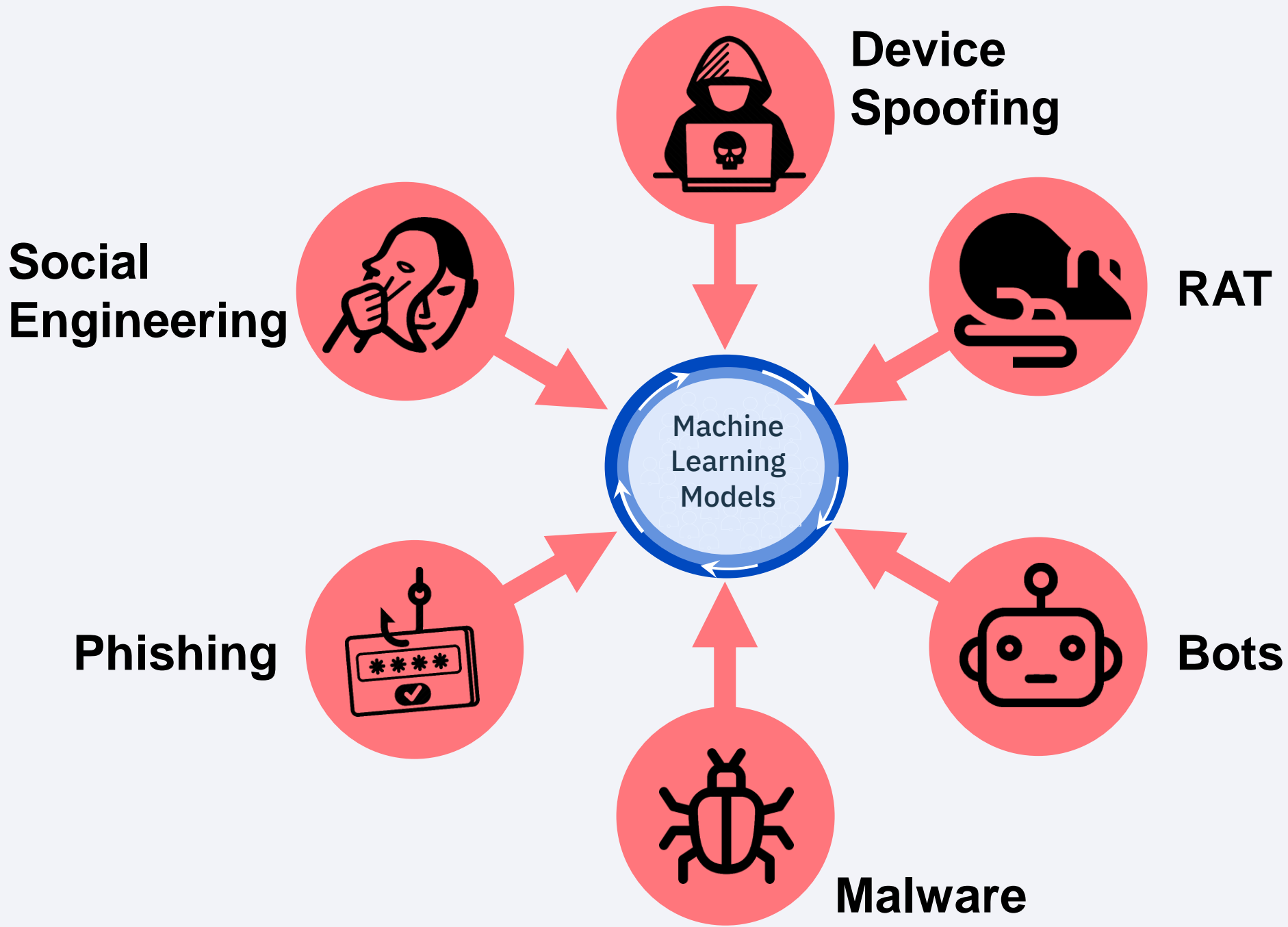


Comply, with privacy and digital regulation: GDPR, PSD2, Open API, FFIEC

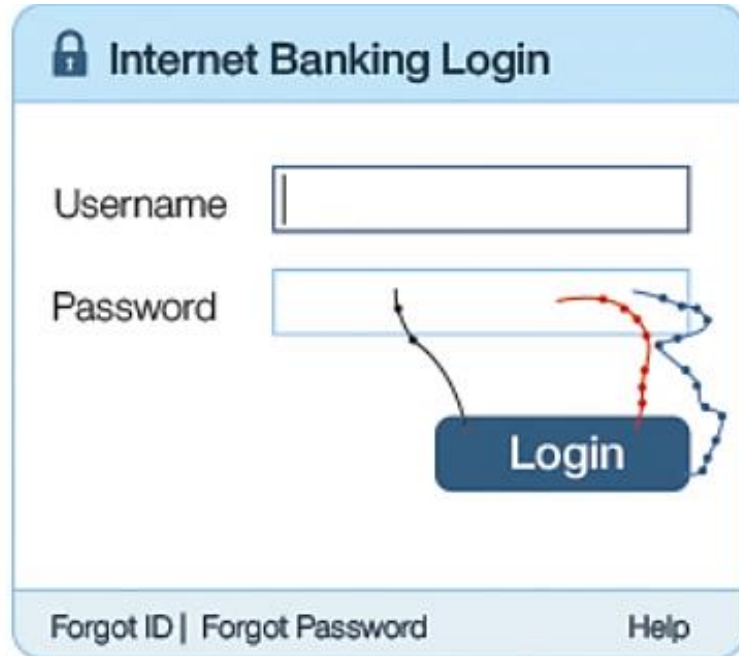


Digital Trust begins with context





Dynamic Identity Assessment: balance experience and security



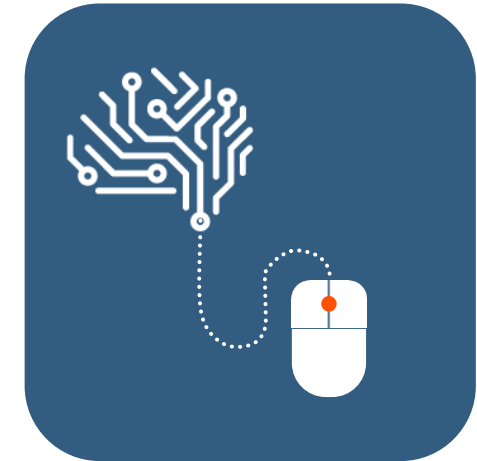
Normal User Behaviour



Abnormal User Behaviour



Known Fraudster Behaviour

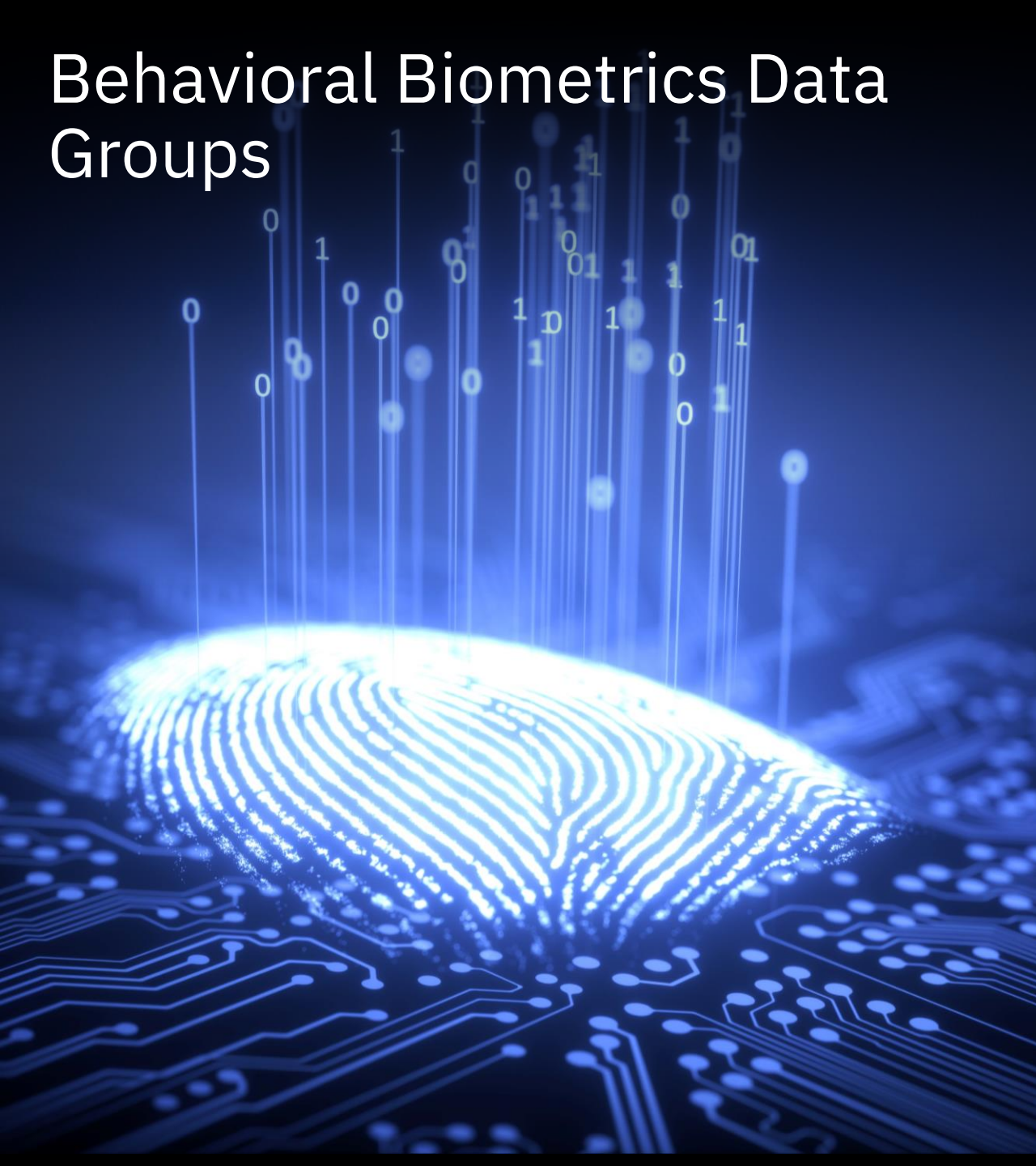


Real-time

Seamless

Actionable

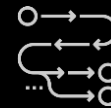
Behavioral Biometrics Data Groups



Keystrokes



Mouse Movements



Navigation flow



Time spent on a specific page



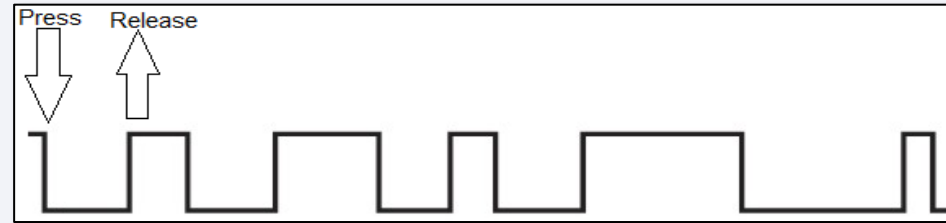
Mobile Touch



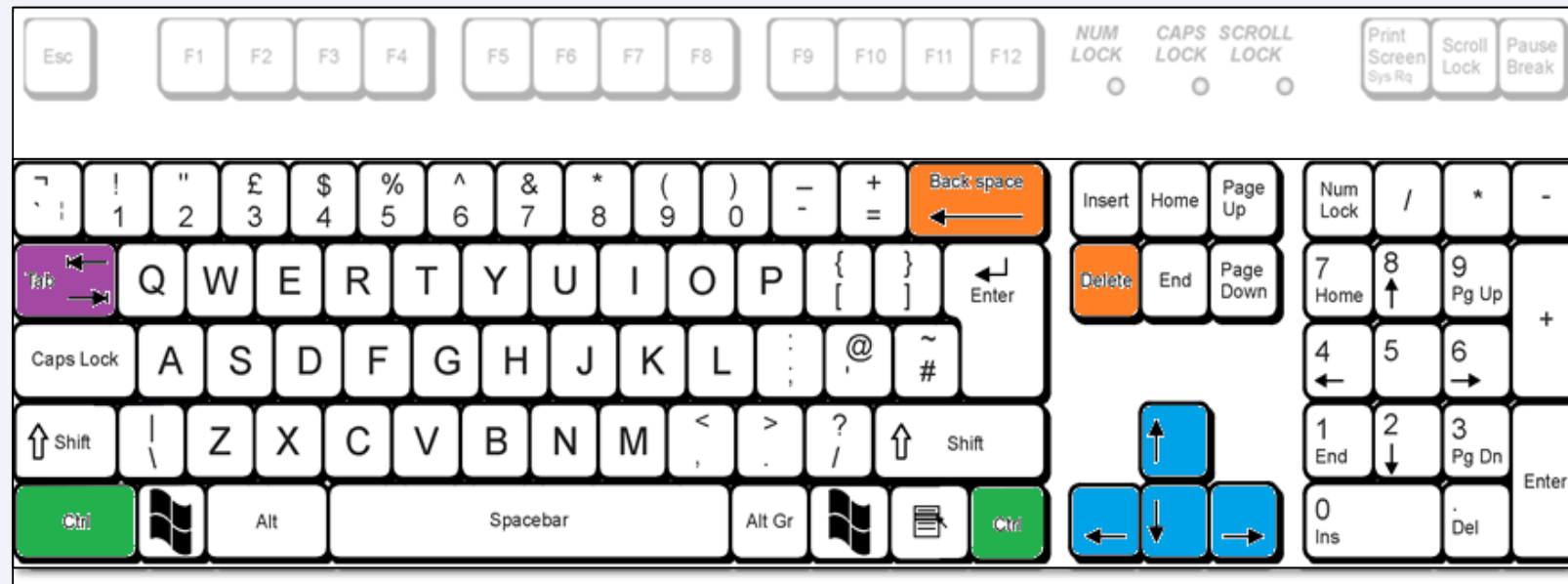
Motion Features

Web Keystrokes Anomalies

Identifying typing rhythm



Keys alternatives



Web Keystrokes

Data sets collected from user's input in multiple fields. For example:

- » **Login:** username, password
- » **Payment:** Beneficiary/IBAN, amount

Keystroked attributes for each field include:

- Time On Field
- Autocomplete
- paste
- Shift Right / Left
- Ctrl Right / Left
- Number
- Tab
- Characters
- Caps Lock
- Backspace
- Delete
- Enter
- Pad Number
- Special Characters



Web Metastrokes



Data

- WinKey
- Shift + tab
- Paste
- Arrows up / down
- page up / down

Event

For each key log the press and release (key up and down)

Can indicate an anomaly in user behavior
e.g. first time using Shift + tab

Can relate to a specific MO
e.g. WinKey + "R" to RAT

id	metastroke	t	key_mapping	puid	session_id	created_at
38		7539	UpArrow	3f4a398b1b6811c62	4102137303695790	20181201 02:16:12.000 +0200
	ctrl;86	30849	Paste	9c3205f89d672b5b6	15348862482589038	20181201 01:53:51.000 +0200
33		178473	PageUp	8531f91b3e6d0e594	26810506120100890	20181201 02:56:14.000 +0200
40		3326	DownArrow	3f4a398b1b6811c62	4102137303695790	20181201 02:16:12.000 +0200

Web Mouse Movements

Mouse behavioral biometrics is the process of identifying users based on their mouse movement traits.

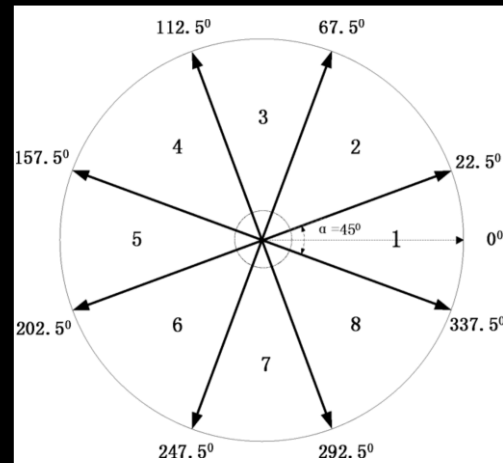
Usually require collecting users data in a particular tasks, thereafter modeling their movement through Machine/Deep learning.

Basic mouse events are:

- Movement
- L/R click
- Scroll

Basic mouse data contains:

- X,Y coordinate
- Time of the event



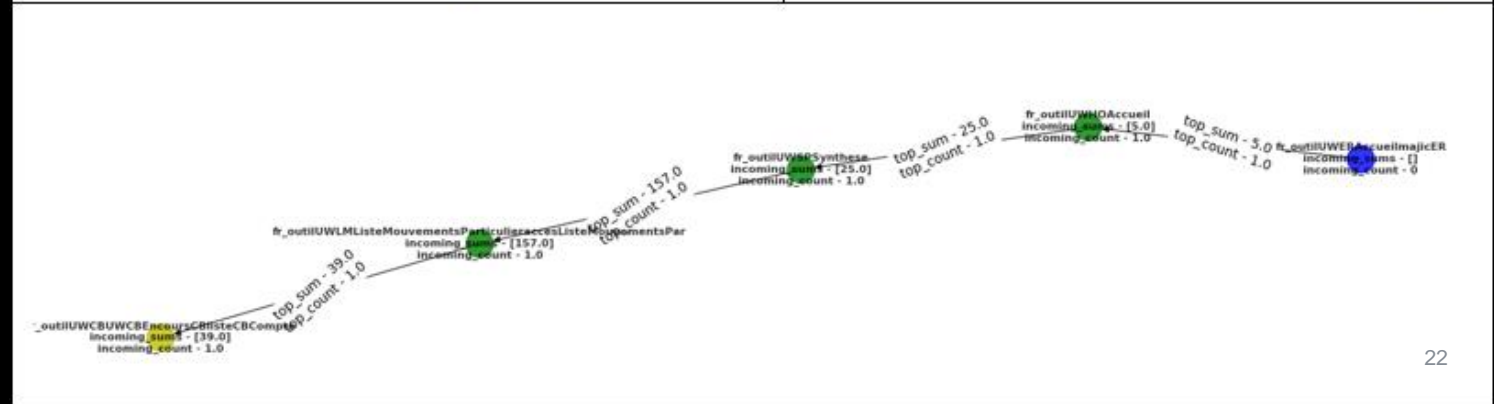
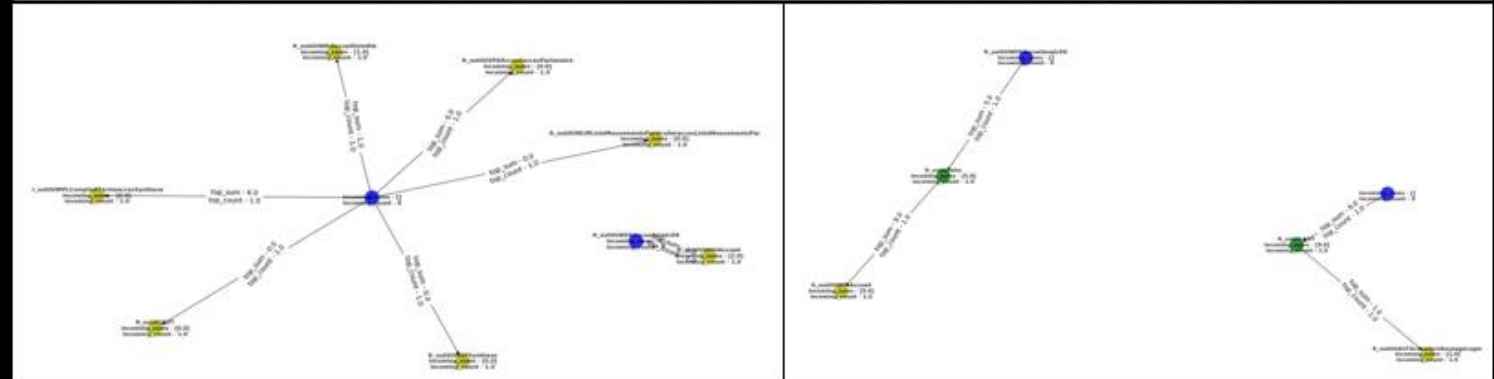
Web User Flow

User-flow algorithm collects URL changes data from a large number of users and builds a matrix of couples: (Referrer URL, Current URL) and the probability of the couple to appear in the data

As a new session arrives, the algorithm splits the sessions' URLs into couples with respect to the order the user visited this URLs

To evaluate the current user's sequence, the algorithm uses Bayesian revolution techniques to receive the probability that the sequence is fraudulent

created_at	url	time_on_page
18/04/2019 10:43:38	https://retail.xxxxxxxx.co.uk/LOGSUK_NS_ENS/BtoChannelDriver.ssobto?dse_operationName=LOGON&dse_processorState=initial&redirect=5	0
18/04/2019 10:43:44	https://retail.xxxxxxxx.co.uk/LOGSUK_NS_ENS/BtoChannelDriver.ssobto?dse_operationName=LOGON&dse_processorState=initial&redirect=5	6
18/04/2019 10:44:51	https://retail.xxxxxxxx.co.uk/LOGSUK_NS_ENS/BtoChannelDriver.ssobto?dse_operationName=LOGON&dse_processorState=initial&redirect=5	73
18/04/2019 10:44:51	https://retail.xxxxxxxx.co.uk/LOGSUK_NS_ENS/ChannelDriver.ssobto?dse_operationName=LOGON	0
18/04/2019 10:45:03	https://retail.xxxxxxxx.co.uk/LOGSUK_NS_ENS/ChannelDriver.ssobto?dse_contextRoot=true	0
18/04/2019 10:45:03	https://retail.xxxxxxxx.co.uk/LOGSUK_NS_ENS/ChannelDriver.ssobto?dse_operationName=LOGON	10
18/04/2019 10:45:45	https://retail.xxxxxxxx.co.uk/LOGSUK_NS_ENS/ChannelDriver.ssobto?dse_contextRoot=true	40
18/04/2019 10:46:27	https://retail.xxxxxxxx.co.uk/LOGSUK_NS_ENS/ChannelDriver.ssobto?dse_contextRoot=true	40
18/04/2019 10:46:28	https://retail.xxxxxxxx.co.uk/LOGSUK_NS_ENS/ChannelDriver.ssobto?dse_contextRoot=true	0
18/04/2019 10:46:36	https://retail.xxxxxxxx.co.uk/LOGSUK_NS_ENS/ChannelDriver.ssobto?dse_contextRoot=true	6
18/04/2019 10:46:39	https://retail.xxxxxxxx.co.uk/EBAN_Accounts_ENS/BtoChannelDriver.ssobto?dse_operationName=MyAccounts&pagesPreviouslyShown=	0
18/04/2019 10:46:46	https://retail.xxxxxxxx.co.uk/EBAN_Accounts_ENS/BtoChannelDriver.ssobto?dse_operationName=MyAccounts&pagesPreviouslyShown=	7
18/04/2019 10:46:48	https://retail.xxxxxxxx.co.uk/EBAN_ServiceRequest_ENS/BtoChannelDriver.ssobto?dse_encryptData=1.0_v78JqAeYfnH0ejmzHRN2mzBzEm_WGDz	0
18/04/2019 10:46:50	https://retail.xxxxxxxx.co.uk/EBAN_ServiceRequest_ENS/BtoChannelDriver.ssobto?dse_encryptData=1.0_v78JqAeYfnH0ejmzHRN2mzBzEm_WGDz	2
18/04/2019 10:46:50	https://retail.xxxxxxxx.co.uk/EBAN_ServiceRequest_ENS/BtoChannelDriver.ssobto?dse_encryptData=1.0_v78JqAeYfnH0ejmzHRN2mzBzEm_WGDz	0
18/04/2019 10:46:55	https://retail.xxxxxxxx.co.uk/EBAN_ServiceRequest_ENS/BtoChannelDriver.ssobto?dse_encryptData=1.0_v78JqAeYfnH0ejmzHRN2mzBzEm_WGDz	2
18/04/2019 10:46:55	https://retail.xxxxxxxx.co.uk/EBAN_ServiceRequest_ENS/BtoChannelDriver.ssobto?dse_encryptData=1.0_v78JqAeYfnH0ejmzHRN2mzBzEm_WGDz	0
18/04/2019 10:47:44	https://retail.xxxxxxxx.co.uk/EBAN_ServiceRequest_ENS/BtoChannelDriver.ssobto?dse_encryptData=1.0_v78JqAeYfnH0ejmzHRN2mzBzEm_WGDz	0
18/04/2019 10:47:44	https://retail.xxxxxxxx.co.uk/EBAN_ServiceRequest_ENS/BtoChannelDriver.ssobto?dse_encryptData=1.0_v78JqAeYfnH0ejmzHRN2mzBzEm_WGDz	50
18/04/2019 10:47:46	https://retail.xxxxxxxx.co.uk/EBAN_ServiceRequest_ENS/BtoChannelDriver.ssobto?dse_encryptData=1.0_v78JqAeYfnH0ejmzHRN2mzBzEm_WGDz	1
18/04/2019 10:47:48	https://retail.xxxxxxxx.co.uk/EBAN_Accounts_ENS/BtoChannelDriver.ssobto?dse_encryptData=1.0_v78JqAeYfnH0ejmzHRN2mzBzEm_WGDz63AL4	0
18/04/2019 10:48:11	https://retail.xxxxxxxx.co.uk/EBAN_Accounts_ENS/BtoChannelDriver.ssobto?dse_encryptData=1.0_v78JqAeYfnH0ejmzHRN2mzBzEm_WGDz63AL4	2
18/04/2019 10:48:11	https://retail.xxxxxxxx.co.uk/EBAN_Accounts_ENS/BtoChannelDriver.ssobto?dse_encryptData=1.0_v78JqAeYfnH0ejmzHRN2mzBzEm_WGDz63AL4	20
18/04/2019 10:52:01	https://retail.xxxxxxxx.co.uk/EBAN_Accounts_ENS/BtoChannelDriver.ssobto?dse_encryptData=1.0_v78JqAeYfnH0ejmzHRN2mzBzEm_WGDz63AL4	4



Mobile Touch Features

Geometrical features

- X,Y location from each corner
- Curvature
- Straightness
- Gradient
- Highest & lowest point
- Gesture context in relation to the app & function

Size & Pressure features

- Average Pressure
- Average on first half & second half
- Size of finger
- Pressure Minimum & Maximum Value
- Pressure on up, down

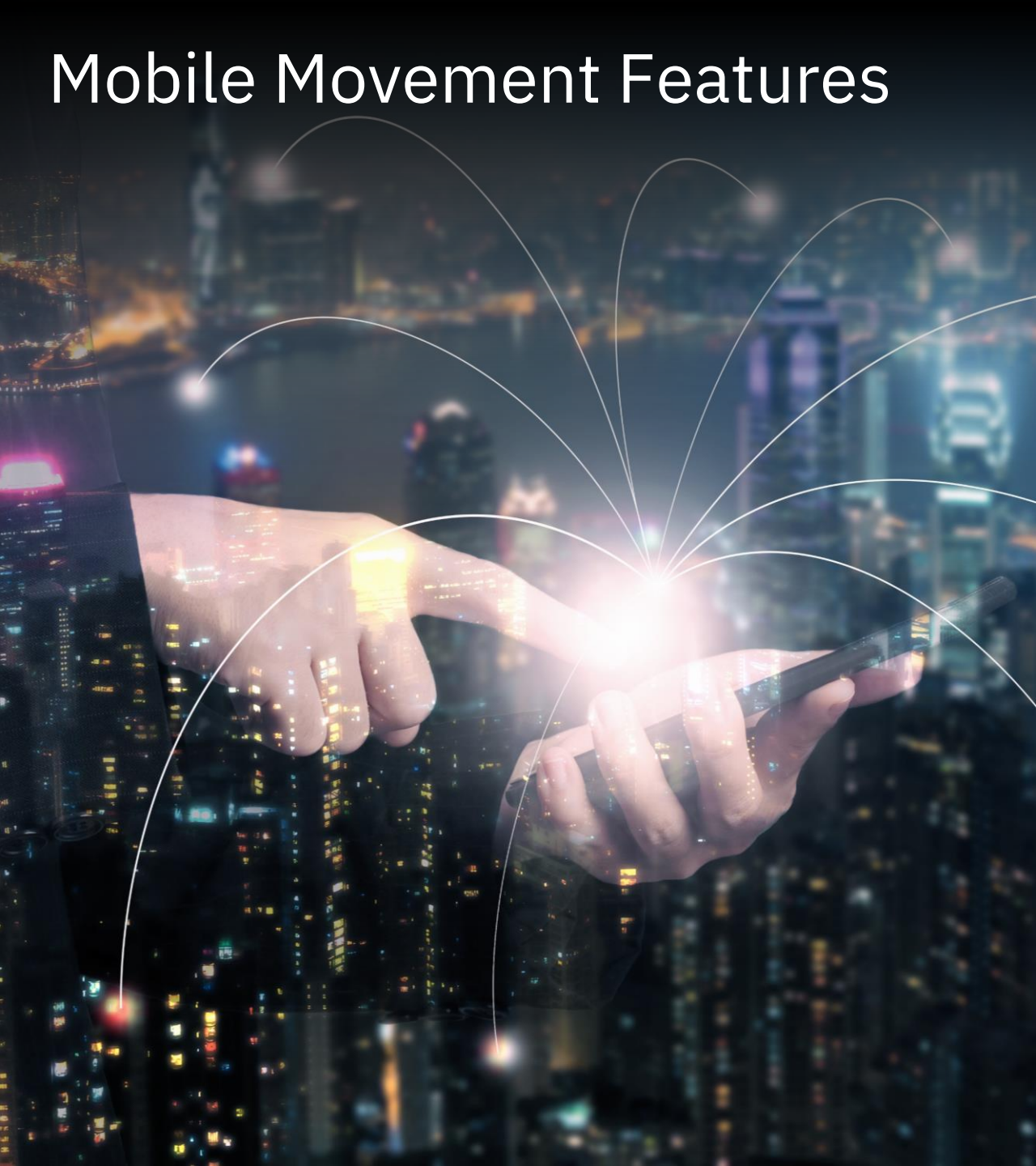
Serial related features

- Differences from previous swipe/next swipes

Speed & Acceleration features

- Total Time
- Start acceleration
- End acceleration (slowing rate)
- Average Speed
- Variance
- Maximum Speed
- Minimum
- Jerk (third derivative)
- Speed consistency

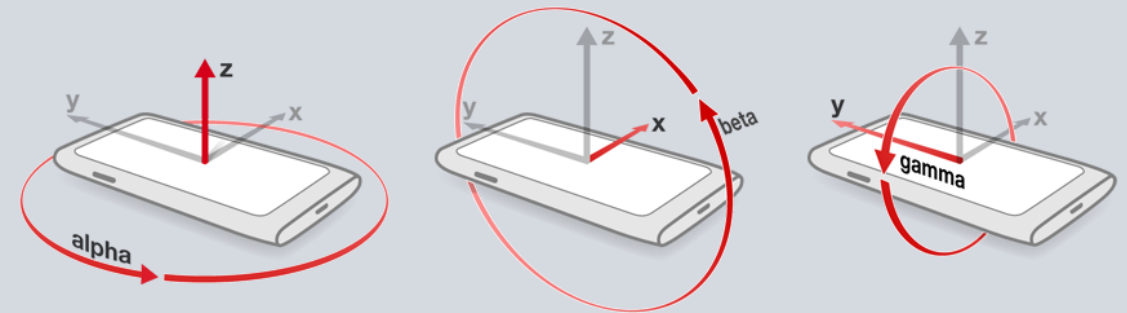
Mobile Movement Features



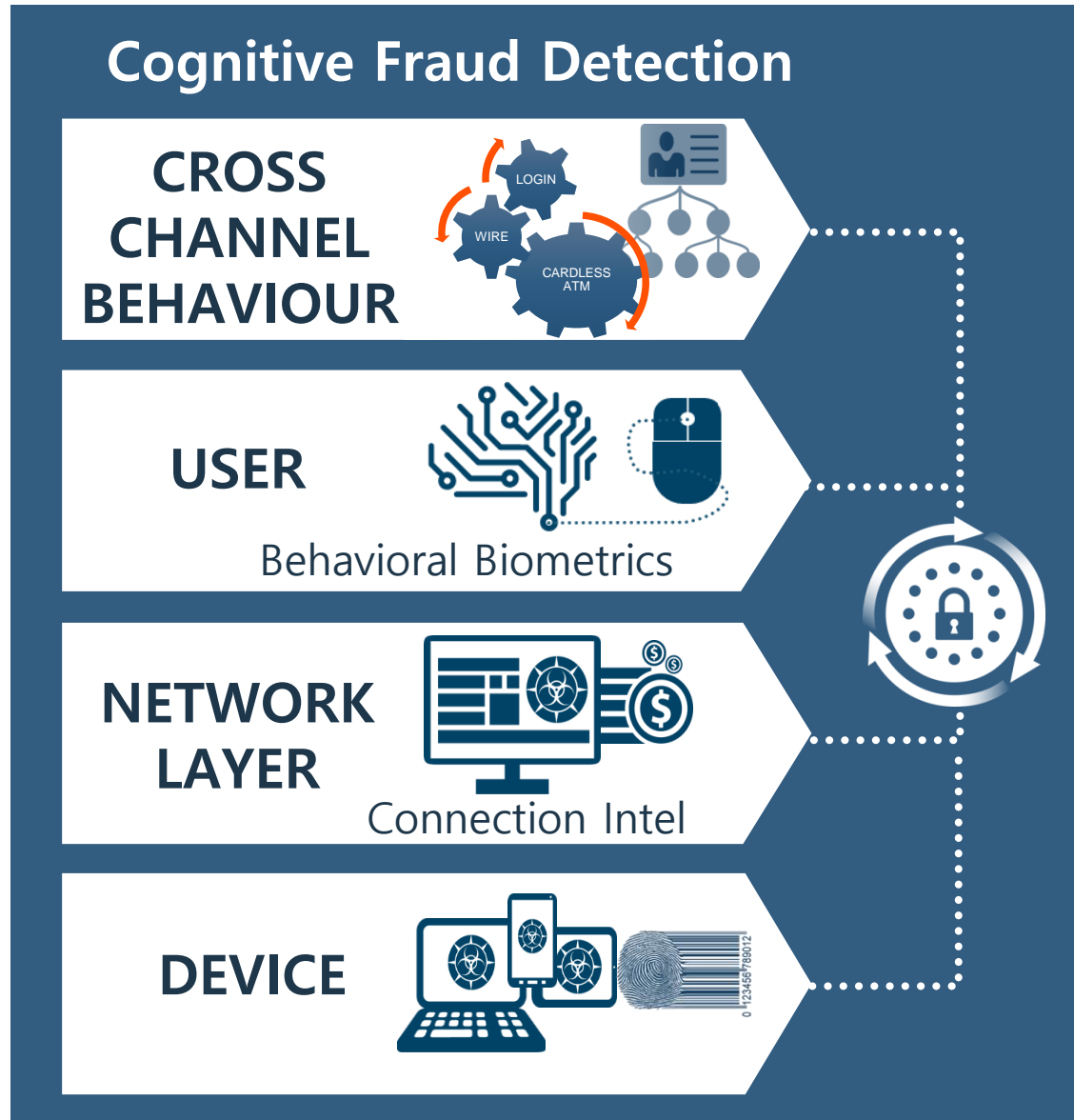
In each Axis (X,Y,Z): Mean motion, Std motion, Minimum, Maximum.

Power spectral density Features (Frequency & Time): Spec distribution Skewness, Kurtosis, flatness.

Distribution Histograms: Equal Size buckets and Exponential Size buckets.

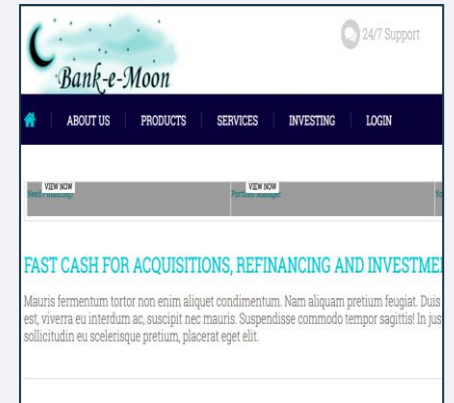
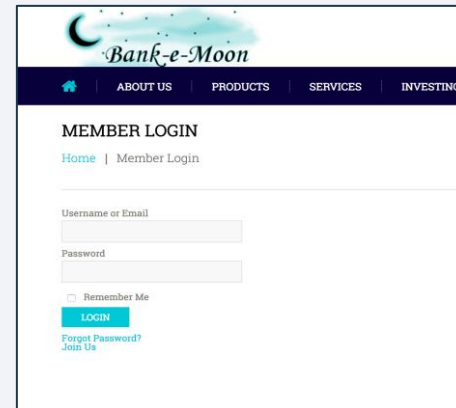
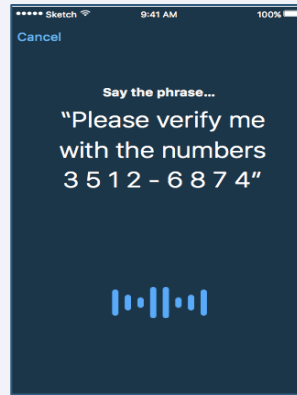
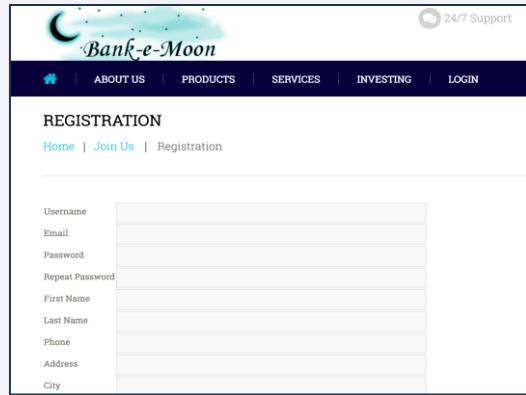


다양한 영역에 대한 디지털 신뢰성 검증



- 복합적 기기 식별
- 특허기반 머신러닝 분석 기법
- 세션 및 트랜잭션 이상행위 식별
- 종합 위험 지표 생성
- 위협 인텔리전스 수집

지속적인 사용자 학습

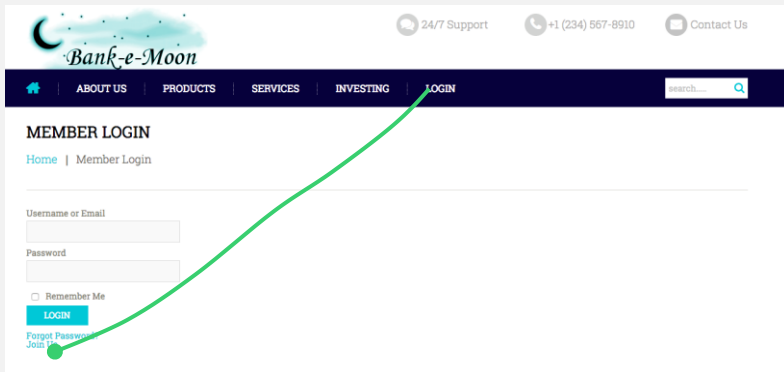
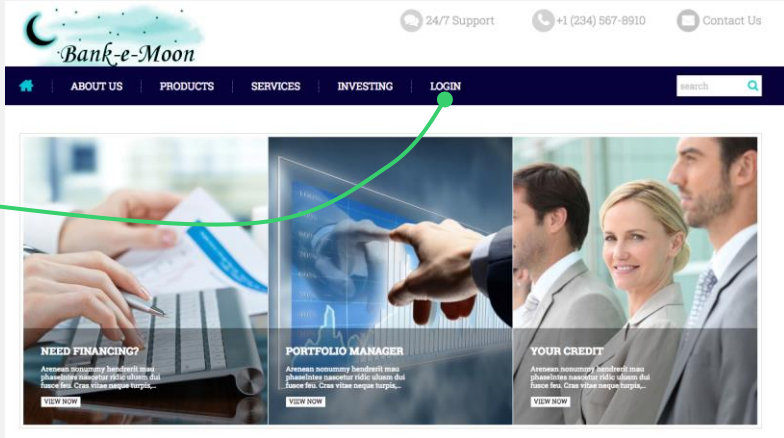


확인되지 않은 사용자

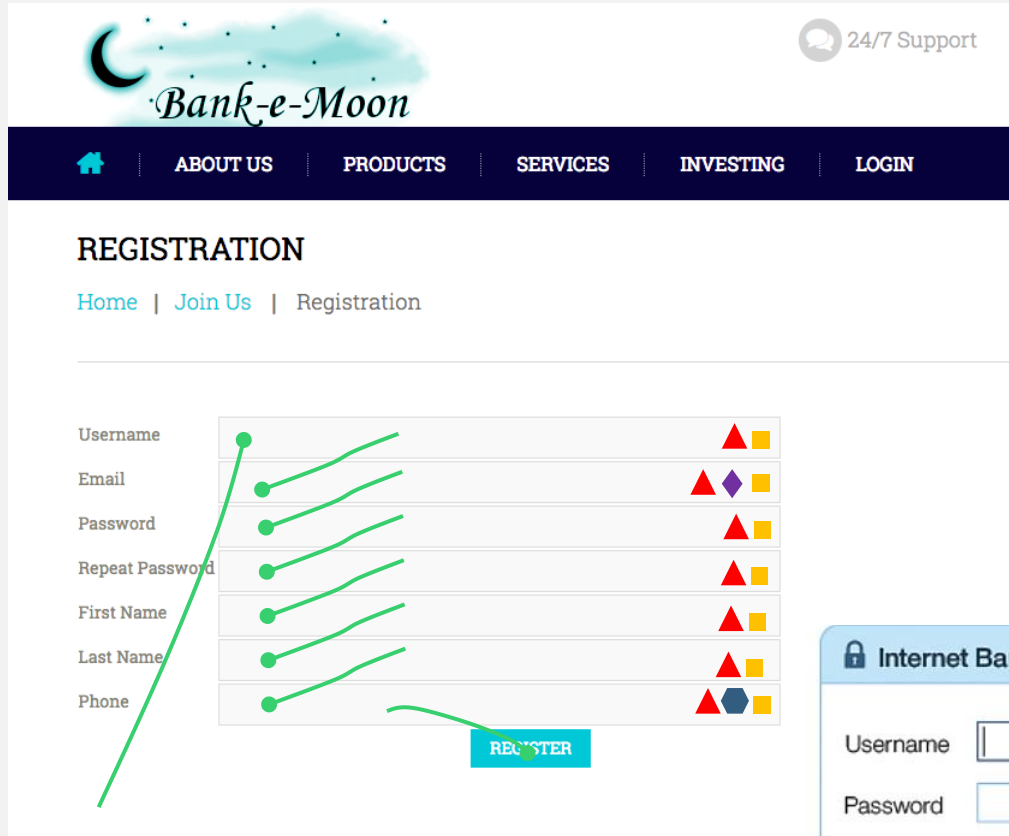
신뢰 사용자

사용자 생체 행위 패턴 학습







접속 페이지

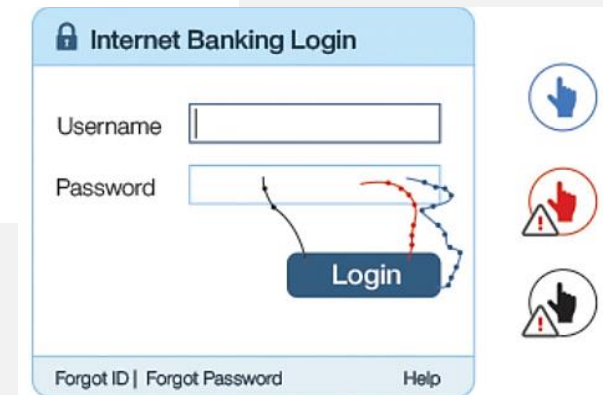


사용자 입력



Trusteer 인텔리전스

-  Mouse Click
-  Mouse Path
-  Keyboard Tab
-  Typing Intel
-  Email Intelligence
-  Carrier Intelligence



정상패턴

이상패턴

해커패턴

신규 사기 계정 식별

New Account Creation Process



고객 등록 정보:

이름: Janette Smith
이메일: Jasdfsf@gmail.com
주소: Charlotte, NC
연락처: 704-898-3344



- IP Geo location is Charlotte, NC: **Match**
- Phone number type is: **Mobile**
- Device status: **Reachable**
- Email account name: **Match**
- Time on page **Legit Pattern**
- Number of application under this name in last 1 month: **0**
- Number of application from this device in the last 1 month: **0**

Fraud Analytics



고객 등록 정보:

이름: Janette Smith
이메일: js@email.com
주소: Charlotte, NC
연락처: +91-911-866-0044



- IP Geo location is in Russia – **Mismatch-Spoofing**
- Phone Type is PREPAID – **Risky**
- Email domain in high risk list – **Risky**
- Typing pattern – copy paste – **Risky**
- Time on page: **Too Short**
- # applications in name in last 1 month: **5**
- # of applications from this device in the last 1 month: **12**



Post-Account Creation



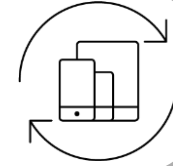
초기 계정 활동 모니터링

- 대포 계정
- 사기 패턴

모바일 기기에 대한 실시간 위험 분석

Device Identity

• Is the session originating from a trusted and known DEVICE?



Session Authenticity

• Is the COMMUNICATION CHANNEL secure?



Device Integrity/Health

• Is the session DEVICE malware free?

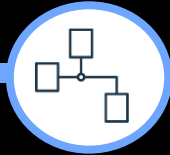


Cross-Channel Correlation

• Any ANOMALOUS patterns detected?



End-point risk assessment across the user journey for building deep identity insights covering Web and Mobile



Device Intelligence

WEB Intelligence

- User agent
- Client timezone
- Agent key/Machine
- OS
- ActiveX
- Mimes
- Fonts
- Navigator props
- Browser + Version
- Cookie
- Screen touch
- Accept languages
- Client languages
- Plugins
- Global cookie
- Web GL attributes
- JavaScript enabled
- Doc location
- Client charset
- Client languages
- CPU
- Doc location
- Platform
- Screen width
- Screen height
- Screen DPI

WEB Browser

- Spoofing indication
- VM indication
- Malware behavior
- Old OS
- Browser versions
- Account profile inconsistencies

Connection Intelligence

Location

Data

- IP
- Country
- City
- Org
- ISP
- Region
- Longitude/Latitude
- X forwarded for
- IP class
- IP time zone

Identity Insights

Risk Indicators

- Known fraudster
- RAT indication
- Risky IP
- Suspicious ISP

Device Insights

- Is new device
- Is new device confidence level
- Global device ID
- Is new device in global network
- Device velocity

Suspicious behavior

- Abnormal login hours
- Abnormal weekend activities
- Excessive use

Threat intelligence

Risk

Assessment

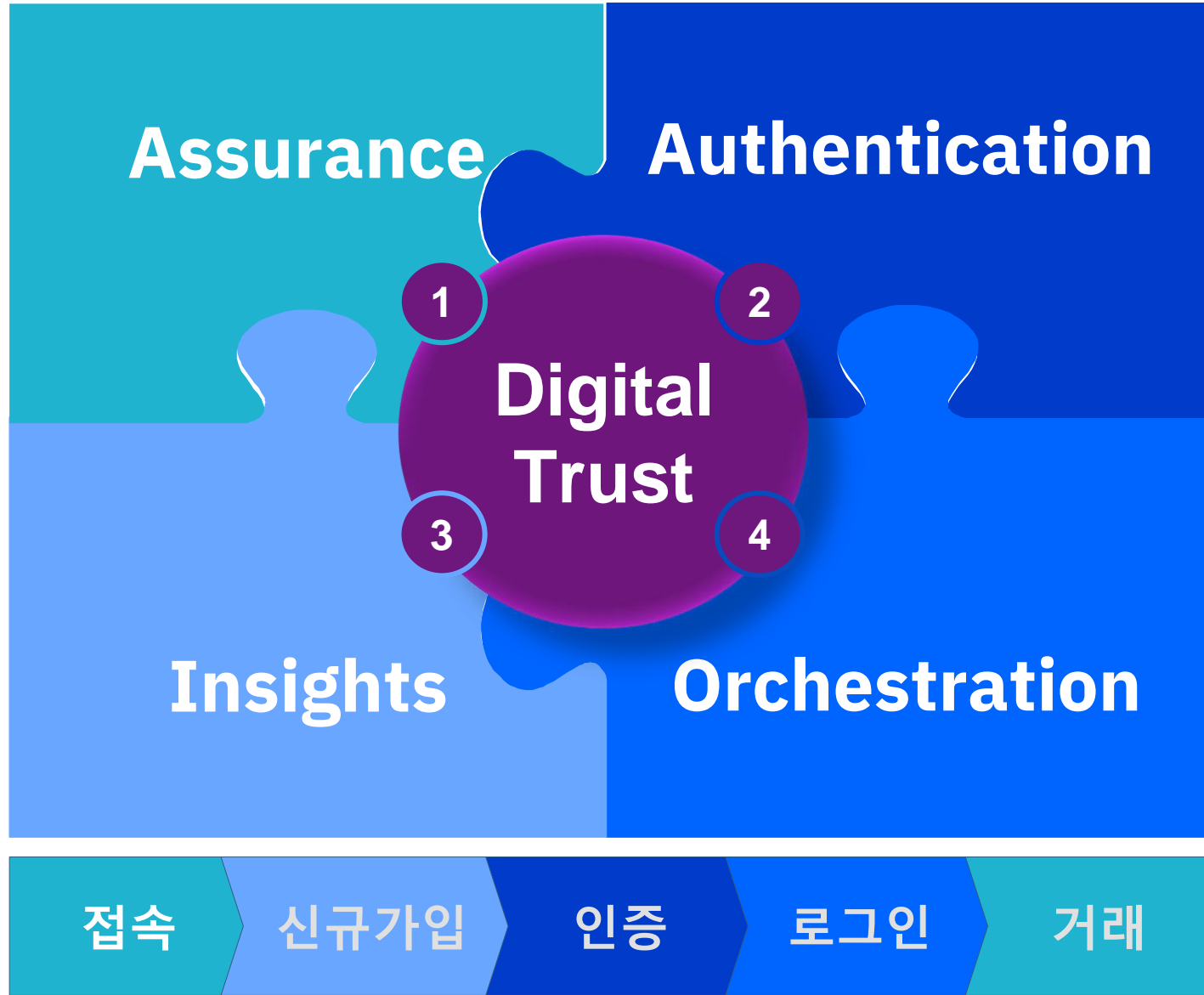
- Risk Score
- Risk Reason

Malware

- Malware ID
- Malware name
- Organization is targeted

IBM의 디지털 트러스트 플랫폼

Trusteer



최고의 보안은 무엇일까요?

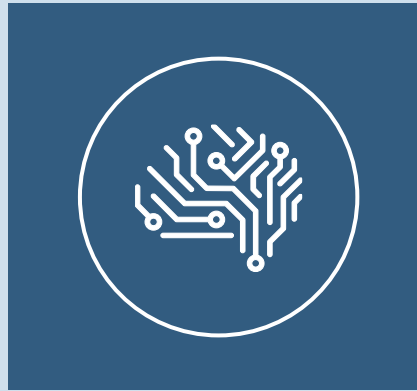
The best security is the kind users don't see it but know it is there

더 나은 고객 경험



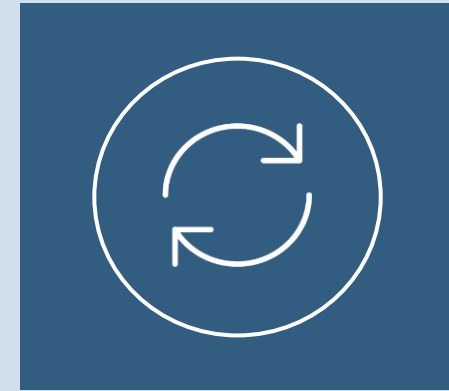
- 모든 디지털 기기와 채널에 대한 보호
- 앱/웹에 대한 고객 사용패턴 학습
- 비정상 행위에 대한 식별 및 조치

위협을 방지하는 인텔리전스



- 클라우드 기반 실시간 위협 정보
- 특허 기반 행위분석 및 머신러닝 학습
- 사용자 사기 식별을 위한 행위 분석
- IBM 보안연구소에서 확인된 신규 패턴

라이프사이클 관리기반 운영 비용 절감



- 실행가능한 인사이트를 제공하는 실시간 사기방지
- 기업 비즈니스 환경에 손쉽게 연동할 수 있는 클라우드 기반 오픈 서비스
- 전문 위협 분석팀

