NetGuardians

RiskTech 100 2019

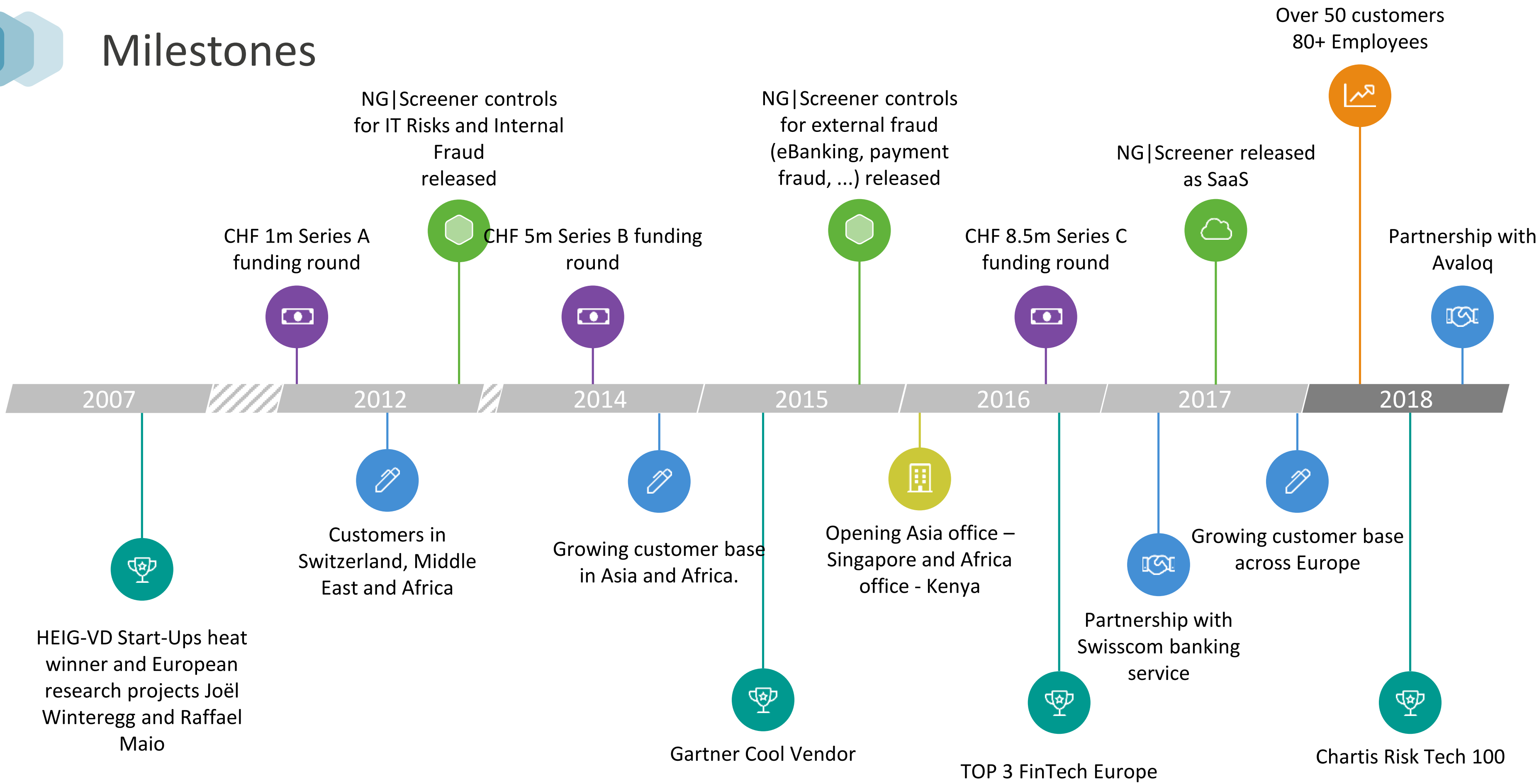
Gartner 2015 CoolVendor

NetGuardians Fraud prevention

AI fraud prevention for banks.

swiss made software

Milestones



HEIG-VD Start-Ups heat winner and European research projects Joël Winteregg and Raffael Maio

CHF 1m Series A funding round

Customers in Switzerland, Middle East and Africa

NG|Screener controls for IT Risks and Internal Fraud released

CHF 5m Series B funding round

Growing customer base in Asia and Africa.

Gartner Cool Vendor

NG|Screener controls for external fraud (eBanking, payment fraud, ...) released

Opening Asia office – Singapore and Africa office - Kenya

CHF 8.5m Series C funding round

TOP 3 FinTech Europe

Partnership with Swisscom banking service

NG|Screener released as SaaS

Growing customer base across Europe

Over 50 customers
80+ Employees

Partnership with Avaloq

Chartis Risk Tech 100

More than 50 customers

BNP PARIBAS

DBS

PICTET
1805

UOB

PIGUET GALLAND & CIE SA
BANQUIERS DEPUIS 1856

BCN

Raiffeisen
Naturellement ma banque

CIMB BANK

Swissquote

Stanbic Bank
A member of Standard Bank Group

អេស៊ីលីដា
ACLEDA
ACLEDA Bank Plc.

REYL
innovative banking

الوطني
NBK

የኢትዮጵያ ንግድ ባንክ
COMMERCIAL BANK OF ETHIOPIA

cba
time for more.

Santander
PRIVATE BANKING

FirstOntario
CREDIT UNION

مصرف الإنماء
alinma bank

STEWARD|BANK
Everyday Banking For Everyday People
A Subsidiary of Econet Wireless

KWFT
BANKING ON WOMEN

SwaziBank

GONET
BANQUIERS 1845

NIC
BANK
one life
one bank

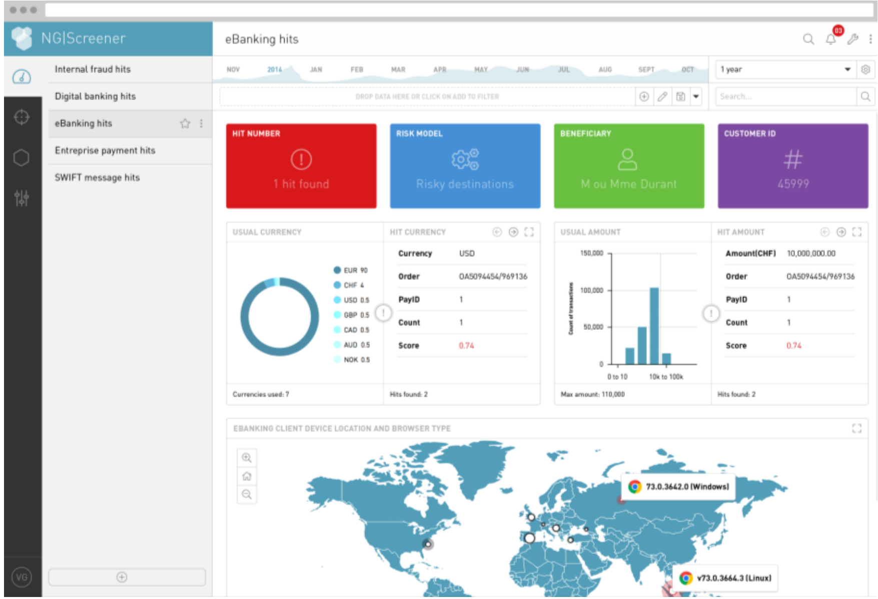
RiskTech 100 2018

Gartner 2015 CoolVendor

Our Strengths

Designed for Banks

- Specifically designed to help banks detect and prevent fraud
- Plugged directly into core banking systems
- Extract, Enrich and Analyze data



HIT NUMBER: 1 hit found

RISK MODEL: Risky destinations

BENEFICIARY: M ou Mme Durant

CUSTOMER ID: 45999

HIT CURRENCY

Currency	USD
Order	0A5094454/969136
PayID	1
Count	1
Score	0.74

Currencies used: 7

Hits found: 2

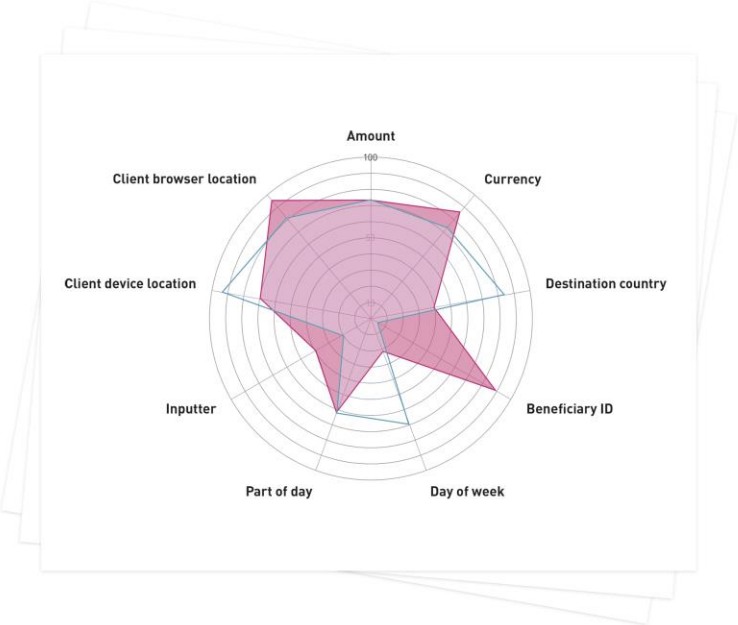
HIT AMOUNT

Amount(CHF)	10,000,000.00
Order	0A5094454/969136
PayID	1
Count	1
Score	0.74

Max amount: 110,000

Hits found: 2

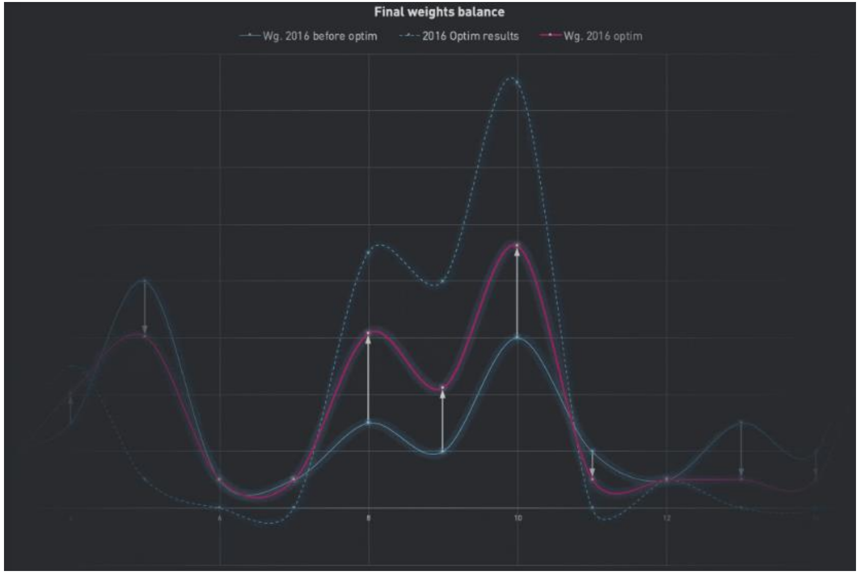
Ready-to-run AI risk models



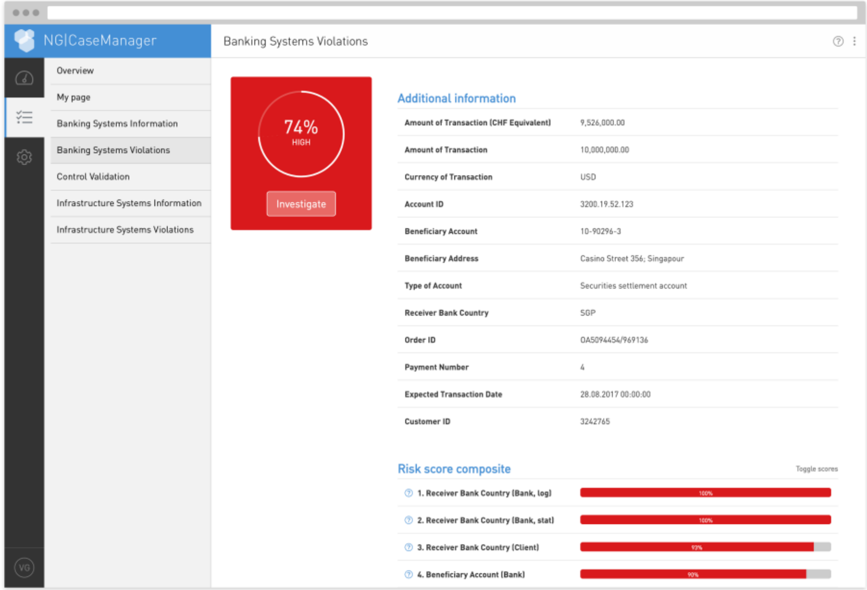
- Built to detect banking fraud
- Monitor all relevant variable to spot suspicious behavior
- Alerts can be easily investigate by end users

Smarter AI

- Million of transaction, few frauds
- AI system can learn to spot these frauds, but will be overfitting
- NetGuardians’ managed learning technology doesn’t endlessly learn about any given type of fraud
- It avoids overfitting and make it possible to spot new types of fraud



Explainable AI for business users


NGICaseManager
Overview
My page
Banking Systems Information
Banking Systems Violations
Control Validation
Infrastructure Systems Information
Infrastructure Systems Violations
VG
74%
HIGH
Investigate

Banking Systems Violations

Additional information

Amount of Transaction (CHF Equivalent)	9,526,000.00
Amount of Transaction	10,000,000.00
Currency of Transaction	USD
Account ID	3200.19.52.123
Beneficiary Account	10-90296-3
Beneficiary Address	Casino Street 356; Singapour
Type of Account	Securities settlement account
Receiver Bank Country	SGP
Order ID	0A5094454/969136
Payment Number	4
Expected Transaction Date	28.08.2017 00:00:00
Customer ID	3242765

Risk score composite

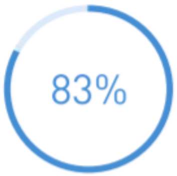
Toggle scores

1. Receiver Bank Country (Bank, log)	100%
2. Receiver Bank Country (Bank, stat)	100%
3. Receiver Bank Country (Client)	93%
4. Beneficiary Account (Bank)	90%

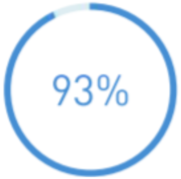
- Don’t need to be a data scientist to make sense of AI
- Understand why AI raise an alert
- Full business context
- Powerful forensics

Unrivalled fraud detection

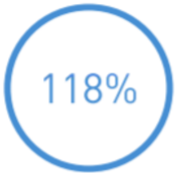
- Proven to offer unrivalled fraud detection
- Found more fraud cases when run over bank's historic data
- Fewer false-positives
- Cuts risk, cuts investigation time, cuts fraud losses



Reduction in the number of false positives



Less time spent investigating frauds



Fraud detection compared with traditional fraud-mitigation processes

Benefits

Real-time banking fraud prevention

Real-time API scoring of all customer and employee transactions across the payment channels, SWIFT and other networks.

Reduced fraud losses

User behavior analytics and machine learning detect new cyber and internal fraud threats. You stay on top of banking fraud schemes **protecting your customers**.

Reduced false positives and improved customer experience

Machine learning algorithms keep false positives to a minimum ensuring the **frictionless customer experience**.

NetGuardians

RiskTech 100 2018

Gartner 2015 Cool Vendor

Our Technology

swiss made software

2008- 2015: Rule-based approach for Fraud Prevention

Banking Institutions deployed analytics systems for fraud prevention

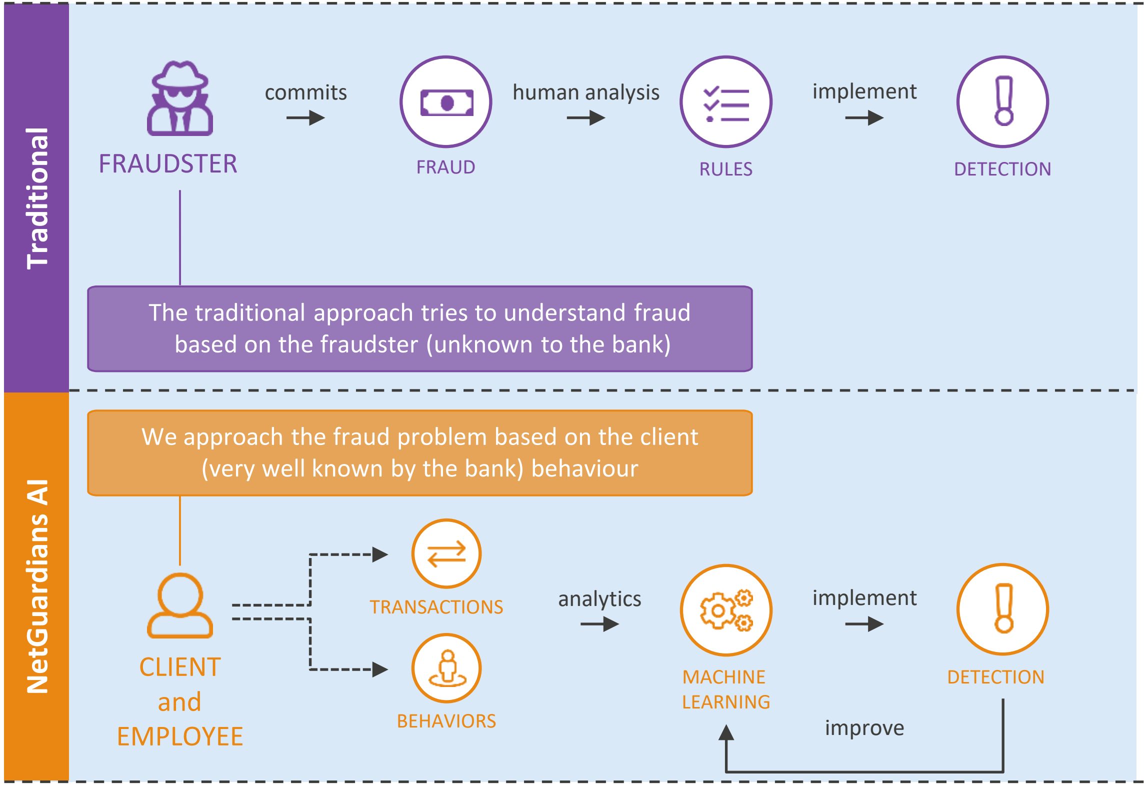
- **Rule engines** (often coming from AML)
- Nobody seriously considers Artificial Intelligence and Machine Learning

```
IF
     payment destination country is risky (e.g. Russia)
AND
     payment amount is greater than 10,000 USD
THEN
     flag transaction for review
```

Ending with usual issues …..

Hundreds of thousands of rules are needed to reflect everyone’s situation

Our unique approach using machine learning



Traditional

FRAUDSTER commits → FRAUD human analysis → RULES implement → DETECTION

The traditional approach tries to understand fraud based on the fraudster (unknown to the bank)

NetGuardians AI

We approach the fraud problem based on the client (very well known by the bank) behaviour

CLIENT and EMPLOYEE → TRANSACTIONS, BEHAVIORS analytics → MACHINE LEARNING implement → DETECTION

improve

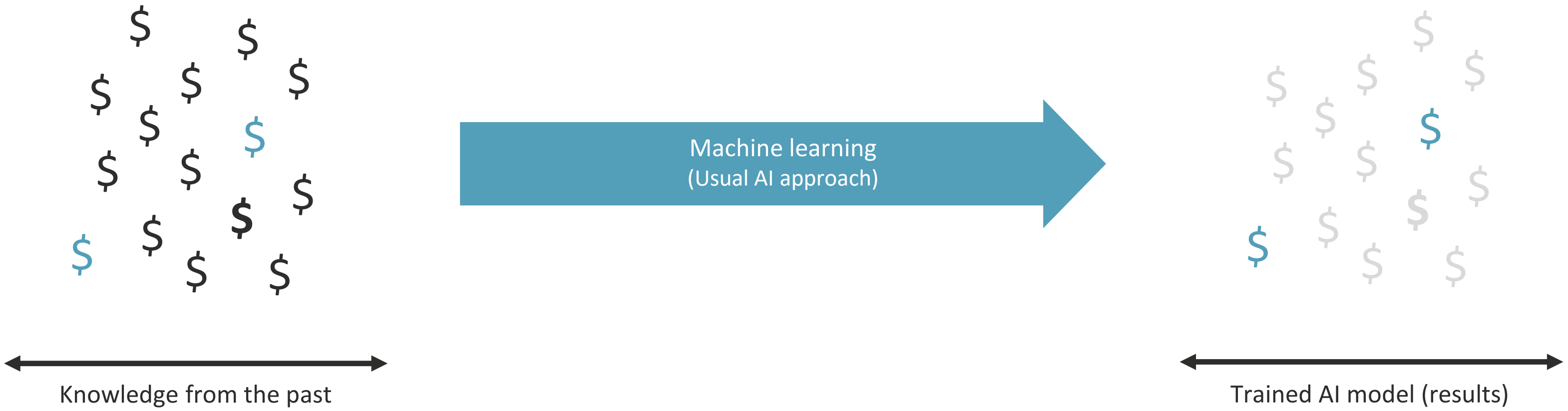
Traditional

- One rule is created by analyzing one type of fraud
- Only known fraud types are addressed, new frauds will not be detected until they happen
- long implementation cycle
- lots of false positives if rules are too generic
- Updating rules is very difficult

NetGuardians

- Straight-to-detection
- Fraud detection is based on transaction pattern analysis, therefore not dependent on fraud being first detected
- New fraud is caught automatically
- No long implementation cycles to maintain detection model

Our unique approach using machine learning

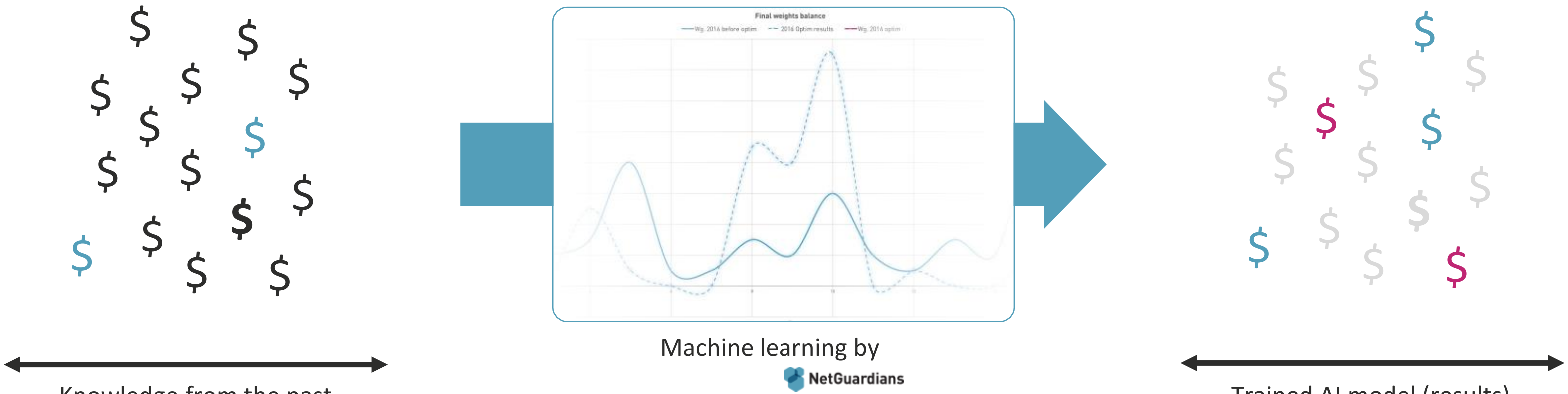


Machine learning
(Usual AI approach)

Knowledge from the past

Trained AI model (results)

Our unique approach using machine learning



Knowledge from the past

Machine learning by NetGuardians

Trained AI model (results)

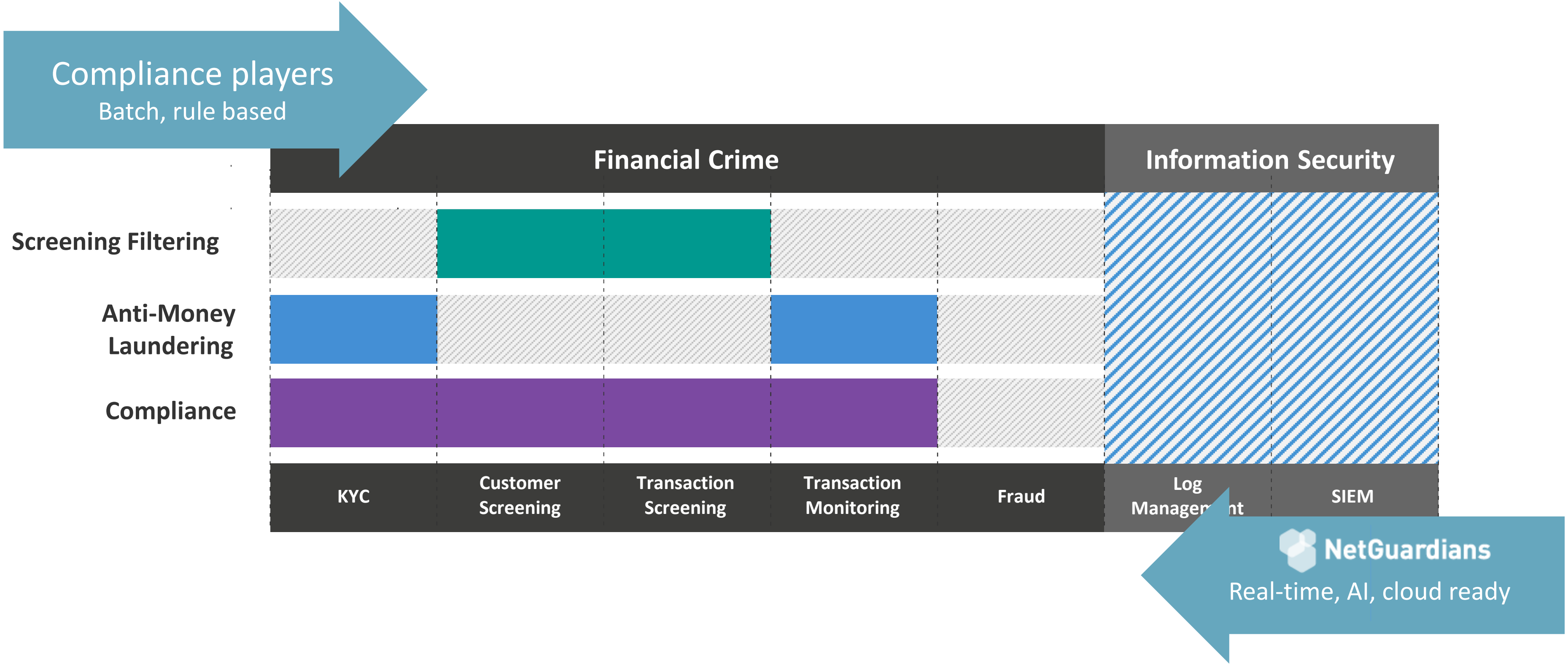
NetGuardians

RiskTech 100 2018

Gartner 2015 CoolVendor

Our Solution

Positioning



Compliance players

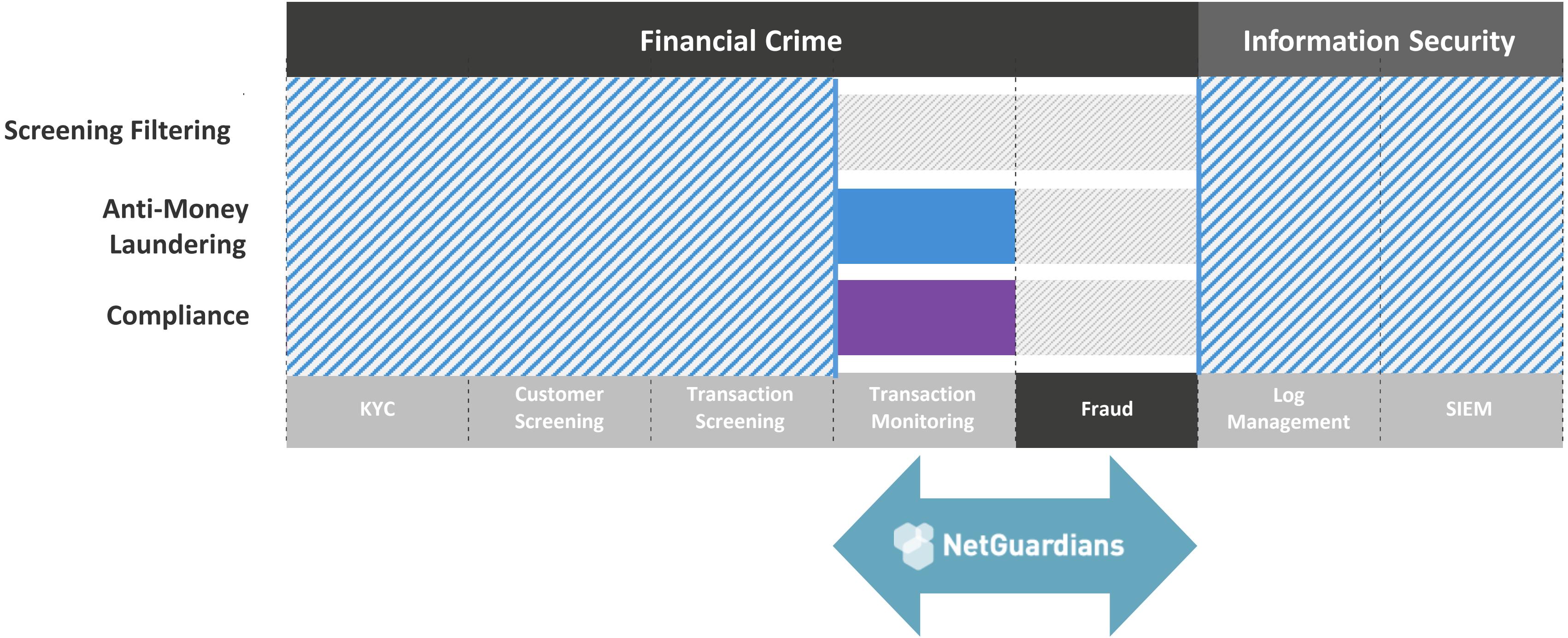
Batch, rule based

	Financial Crime					Information Security	
	KYC	Customer Screening	Transaction Screening	Transaction Monitoring	Fraud	Log Management	SIEM
Screening Filtering	▨	🟩	🟩	▨	▨	▧	▧
Anti-Money Laundering	🟦	▨	▨	🟦	▨	▧	▧
Compliance	🟪	🟪	🟪	🟪	▨	▧	▧

NetGuardians

Real-time, AI, cloud ready

Positioning



Financial Crime

Information Security

Screening Filtering

Anti-Money Laundering

Compliance

KYC

Customer Screening

Transaction Screening

Transaction Monitoring

Fraud

Log Management

SIEM

NetGuardians

Solutions made for banks

Big data and analytics platform
capturing the data you need
and running the risk models you need

Pre-defined risk models
stopping fraudulent transactions

- Digital banking fraud
- Enterprise payment fraud
- Internal fraud

Digital banking fraud

NetGuardians' AI solution NG|Screener prevents fraudulent transactions related to:

- Malwares on eBanking customer laptops
- Corporate/personal account takeover using social engineering (CEO-Fraud, Lottery Scams, ...)
- Identity theft resulting from phishing scams
- Session hijacking resulting from social engineering
- And many more use cases

Enterprise payment fraud

Enterprise payment fraud
Using pre-defined risk models

NetGuardians’ AI solution NG|Screener prevents fraudulent payments:

- From fake invoice received by post mail
- Carried out using social engineering techniques
- From compromised corporate treasury systems
- Resulting from cyber attacks on payment systems
- And many more use cases

Internal fraud

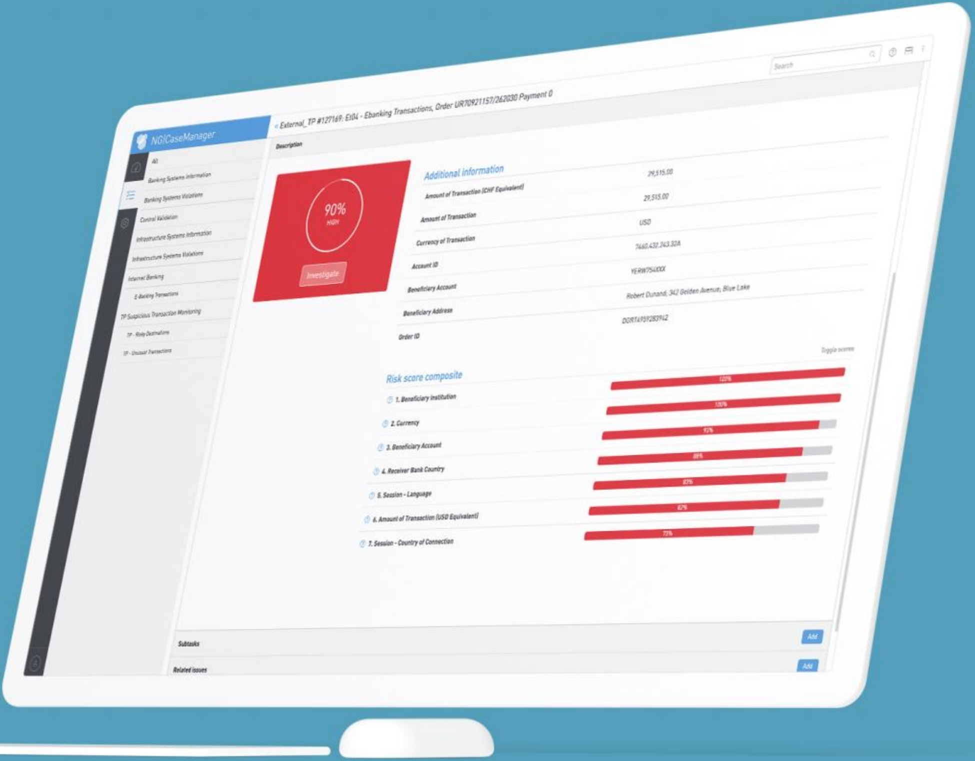
NetGuardians' AI solution NG|Screener prevents fraudulent transactions related to:

- Employees performing unusual transactions on client accounts
- Collusion between IT and operations employees
- Employees transacting on client accounts using credentials from colleagues on leave
- Employees exploring inactive customer accounts
- And many more use cases

Some fraud we captured

Examples of fraudulent transactions prevented by NetGuardians' machine learning technology	Number of rules required to achieve same result
39'000 CHF transaction: 10x bigger than usual customers' transaction to unusual country (GB) from his savings account, using unusual browser, unusual language, unusual screen resolution.	60'000 rules (one per customer)
330'000 CHF transaction: 300x bigger than usual customers' transaction sent to a very common country (CH) but using unusual language and unusual browser.	60'000 rules (one per customer)
37'000 EUR transaction: Transaction inputted at unusual hour for that customer, with an amount 4x bigger than usual, to an Eastern Europe country he never transacted with before.	200 rules (related to amount, customer subset and risky country)

NG|CaseManager


NG|CaseManager
All
Banking Systems Information
Banking Systems Violations
Control Validation
Infrastructure Systems Information
Infrastructure Systems Violations
Internet Banking
E-Banking Transactions
TP Suspicious Transaction Monitoring
TP - Risky Destinations
TP - Unusual Transactions
Search
90%
HIGH
Investigate
Toggle scores
Add
Add

« External_TP #127169: Et04 - Ebanking Transactions, Order UR70921157/262030 Payment 0

Description

Additional information

Amount of Transaction (CHF Equivalent)	29,515.00
Amount of Transaction	29,515.00
Currency of Transaction	USD
Account ID	7460.432.243.32A
Beneficiary Account	YERW754XXX
Beneficiary Address	Robert Dunand; 342 Golden Avenue; Blue Lake
Order ID	DORT4959283942

Risk score composite

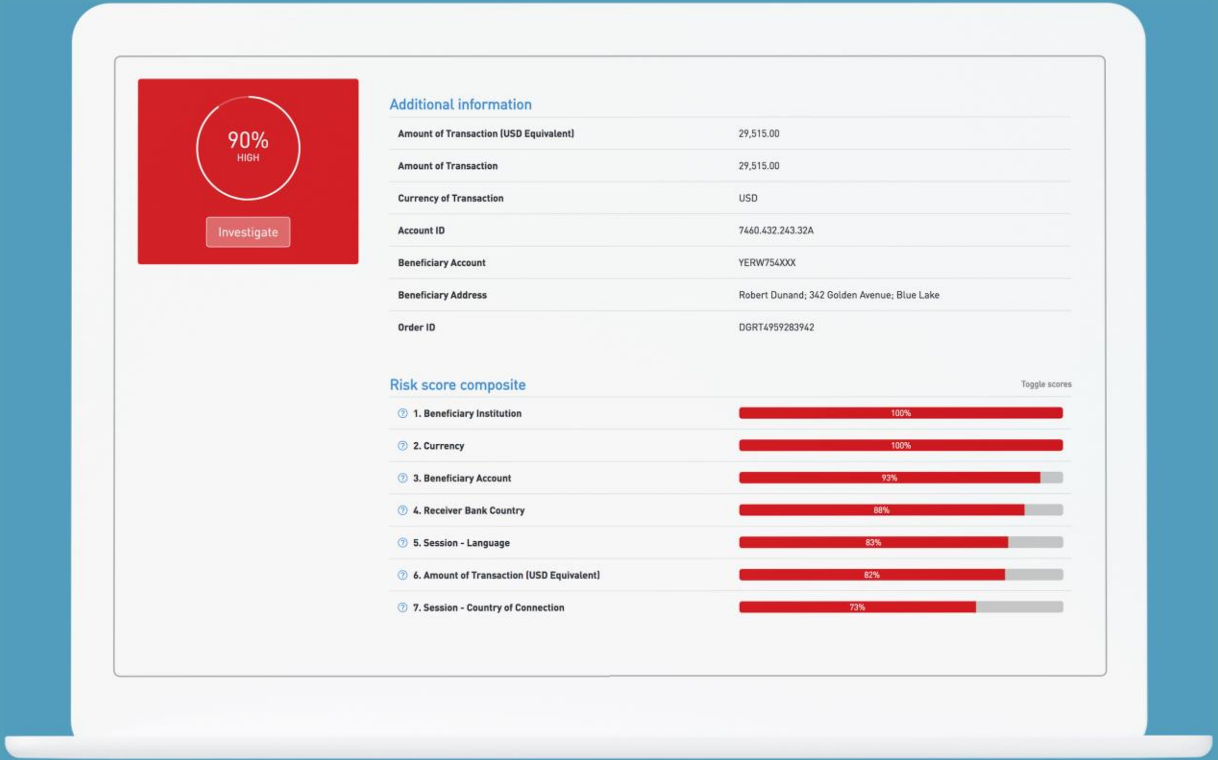
1. Beneficiary Institution	120%
2. Currency	100%
3. Beneficiary Account	93%
4. Receiver Bank Country	89%
5. Session - Language	83%
6. Amount of Transaction (USD Equivalent)	82%
7. Session - Country of Connection	73%

Subtasks

Related issues

Augmented intelligence

Empowering users
by providing machine
learning technology
together with contextual
information and a great
user experience



Additional information

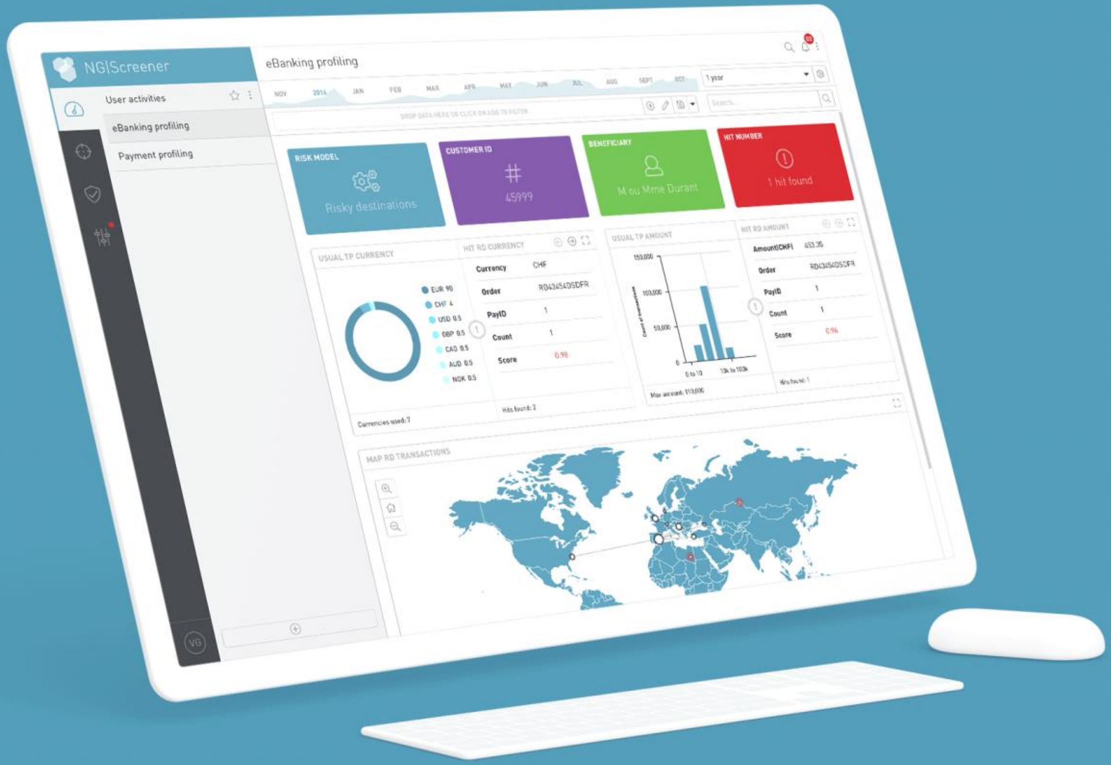
Amount of Transaction (USD Equivalent)	29,515.00
Amount of Transaction	29,515.00
Currency of Transaction	USD
Account ID	7460.432.243.32A
Beneficiary Account	YERW754XXX
Beneficiary Address	Robert Dunand; 342 Golden Avenue; Blue Lake
Order ID	DGRT4959283942

Risk score composite

Toggle scores

1. Beneficiary Institution	100%
2. Currency	100%
3. Beneficiary Account	93%
4. Receiver Bank Country	88%
5. Session - Language	83%
6. Amount of Transaction (USD Equivalent)	82%
7. Session - Country of Connection	73%

NG|Dashboard



NG|Screener

eBanking profiling

User activities

- eBanking profiling
- Payment profiling

RISK MODEL	CUSTOMER ID	BENEFICIARY	HIT NUMBER
Risky destinations	45999	M ou Mme Durant	1 hit found

USUAL TP CURRENCY

EUR	90
CHF	4
USD	0.5
GBP	0.5
CAD	0.5
AUD	0.5
NOK	0.5

Currencies used: 7

HIT RD CURRENCY

Currency	CHF
Order	RD434540DSDFR
PayID	1
Count	1
Score	0.96

Hits found: 2

USUAL TP AMOUNT

Max amount: 110,000

HIT RD AMOUNT

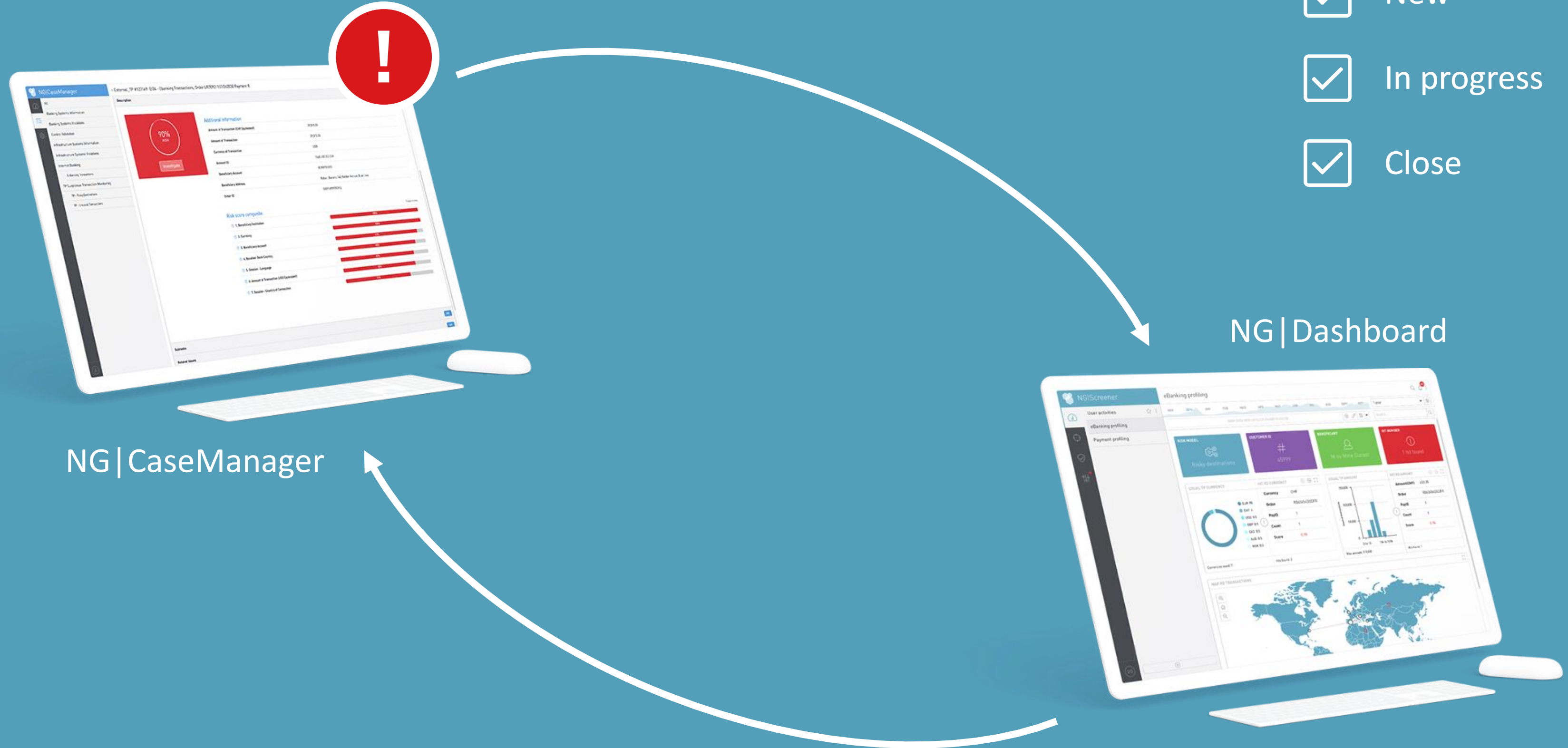
Amount(CHF)	453.35
Order	RD434540DSDFR
PayID	1
Count	1
Score	0.96

Hits found: 1

MAP RD TRANSACTIONS

Workflow

- ☑ New
- ☑ In progress
- ☑ Close



Resources

- CTO Video on how AI helps for fraud prevention: https://www.youtube.com/watch?v=ZSNTl4WucdQ

- Fighting Internal Fraud with Netguardians: https://www.youtube.com/watch?v=HUnaJsYtXaU&t=2s

- Fighting External Fraud with Netguardians: https://www.youtube.com/watch?v=iXhkeAqihL4&t=9s

NetGuardians

RiskTech 100 2018

Gartner 2015 CoolVendor

Use case example E-Banking Transactions

swiss made software

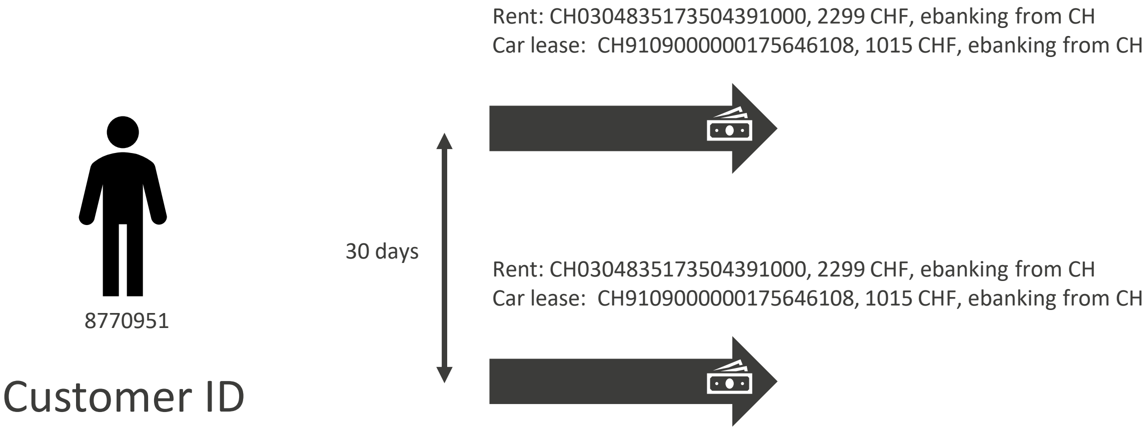
Description of the case: Transaction View

Rent: CH0304835173504391000, 2299 CHF, ebanking from CH
Car lease: CH9109000000175646108, 1015 CHF, ebanking from CH

8770951

Customer ID

Description of the case: Transaction View



Rent: CH0304835173504391000, 2299 CHF, ebanking from CH
Car lease: CH9109000000175646108, 1015 CHF, ebanking from CH

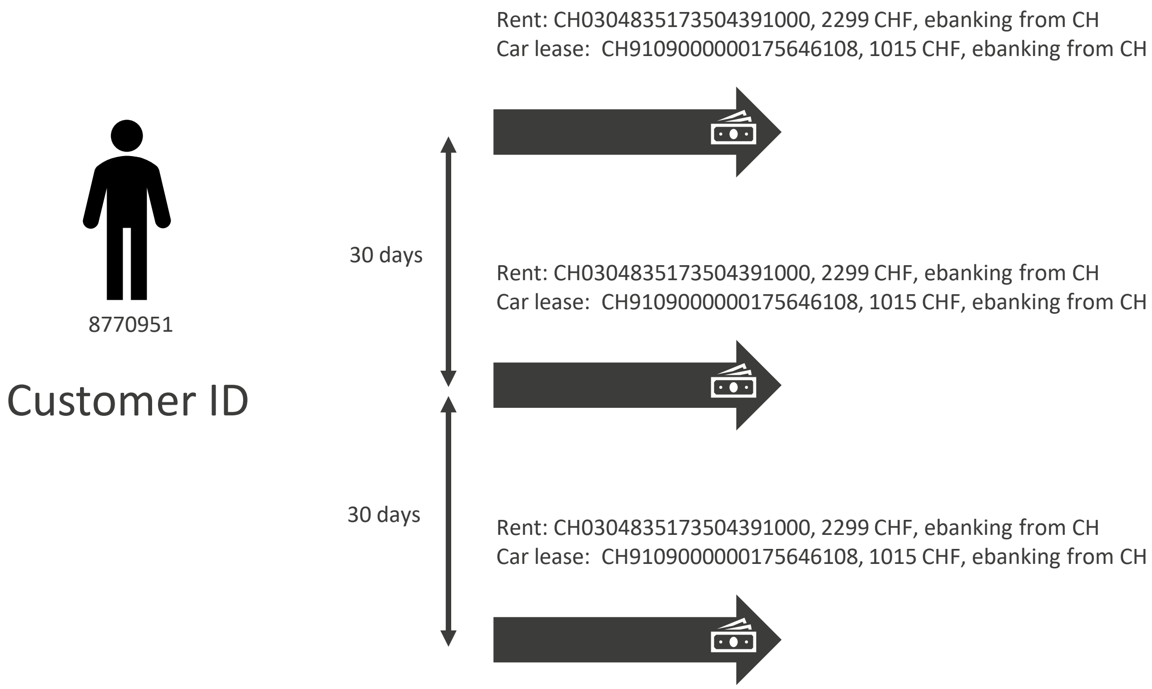
30 days

Rent: CH0304835173504391000, 2299 CHF, ebanking from CH
Car lease: CH9109000000175646108, 1015 CHF, ebanking from CH

8770951

Customer ID

Description of the case: Transaction View



8770951

Customer ID

30 days

30 days

Rent: CH0304835173504391000, 2299 CHF, ebanking from CH
Car lease: CH9109000000175646108, 1015 CHF, ebanking from CH

Rent: CH0304835173504391000, 2299 CHF, ebanking from CH
Car lease: CH9109000000175646108, 1015 CHF, ebanking from CH

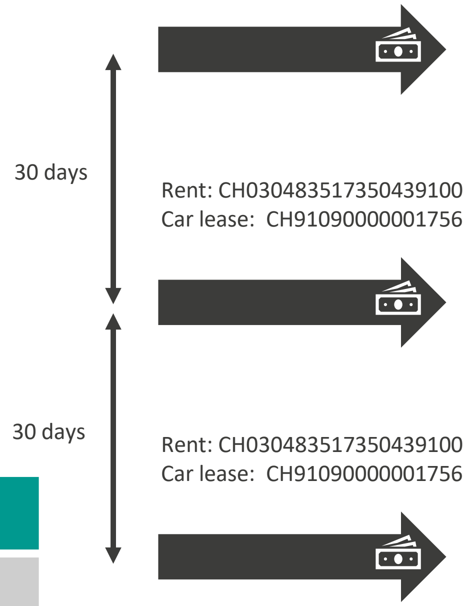
Rent: CH0304835173504391000, 2299 CHF, ebanking from CH
Car lease: CH9109000000175646108, 1015 CHF, ebanking from CH

Description of the case: Transaction View

8770951

Customer ID

Rent: CH0304835173504391000, 2299 CHF, ebanking from CH
Car lease: CH9109000000175646108, 1015 CHF, ebanking from CH



Rent: CH0304835173504391000, 2299 CHF, ebanking from CH
Car lease: CH9109000000175646108, 1015 CHF, ebanking from CH

Rent: CH0304835173504391000, 2299 CHF, ebanking from CH
Car lease: CH9109000000175646108, 1015 CHF, ebanking from CH

8770951 Customer profile at that time:

IBAN	Currency	Amount	Frequency
CH0304835173504391000	CHF	From 2200 to 2400	monthly
CH9109000000175646108	CHF	1015	monthly

Description of the case: Transaction View

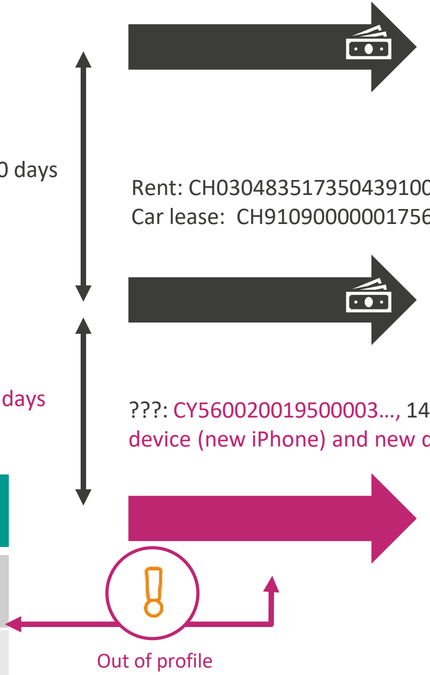
8770951

Customer ID

8770951 Customer profile at that time:

IBAN	Currency	Amount	Frequency
CH0304835173504391000	CHF	From 2200 to 2400	monthly
CH9109000000175646108	CHF	1015	monthly

Rent: CH0304835173504391000, 2299 CHF, ebanking from CH
Car lease: CH9109000000175646108, 1015 CHF, ebanking from CH



30 days

Rent: CH0304835173504391000, 2299 CHF, ebanking from CH
Car lease: CH9109000000175646108, 1015 CHF, ebanking from CH

7 days

???: CY560020019500003…, 1438 USD (new currency), ebanking from new device (new iPhone) and new destination (Cyprus)

Out of profile

Unusual destination
Unusual currency
Unusual device

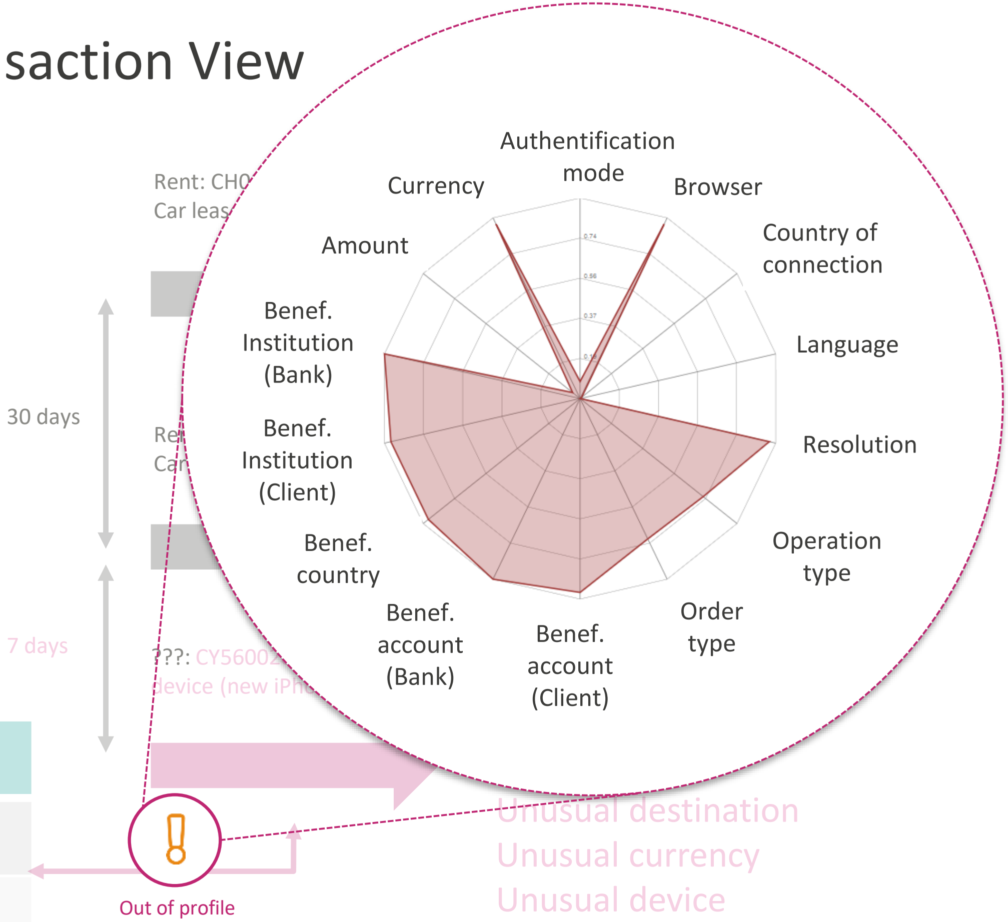
Description of the case: Transaction View

8770951

Customer ID

8770951 Customer profile at that time:

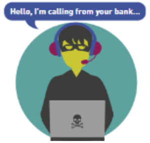
IBAN	Currency	Amount	Frequency
CH0304835173504391000	CHF	From 2200 to 2400	monthly
CH9109000000175646108	CHF	1015	monthly



Unusual destination
Unusual currency
Unusual device

…The transaction is suspicious…

Account manipulation



Social engineering
Scams, .. (CEO-Fraud, Lottery .)

Invoice redirection technics
Fake invoice

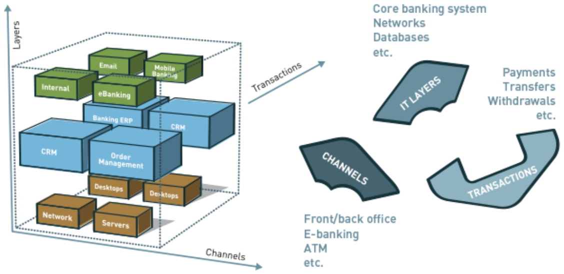
Session hijacking

Malware

Identity theft

Description of the case: Transaction View

1 Data capture



2 Risk model (control)

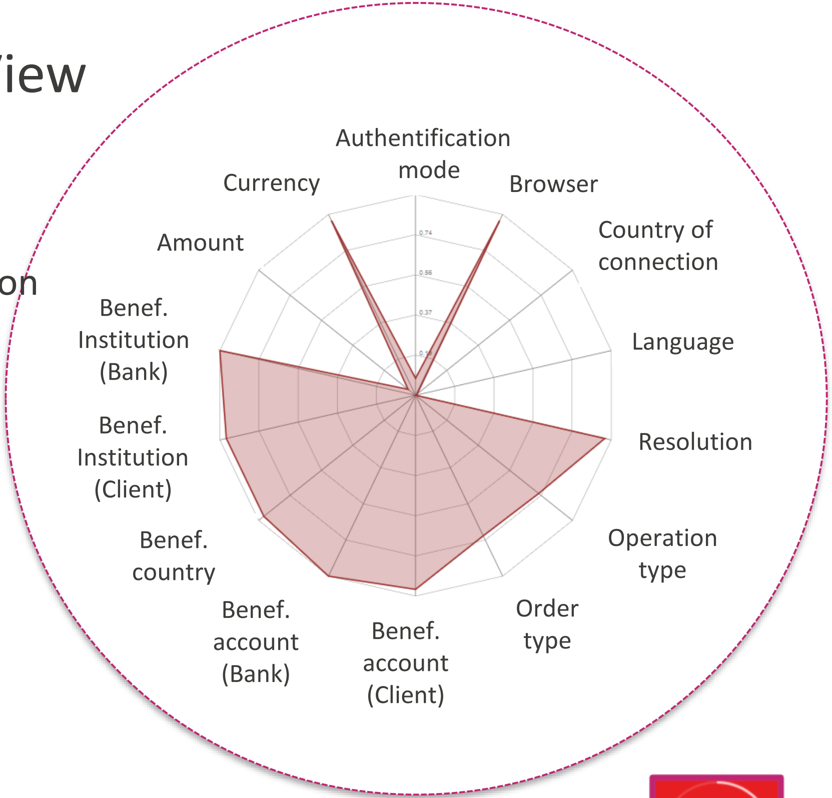
$$Pscore_X = \sqrt{1 - Prob_X}$$

where

$$Pscore_X = min\left(1, \frac{Zscore_X}{y}\right)$$

where $Zscore_X = \left(\frac{|X_{allEvents} - X_{event}|}{sd(X_{allEvent})}\right)$

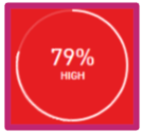
3 Risk computation



4 Risk scoring

Out of profile

$$\textbf{Risk Score} = \left(\frac{\sum_{i=1}^{n}(PScore_i \times Weight_i)}{\sum_{i=1}^{n} Weight_i}\right)^2 = 0.79$$



NetGuardians

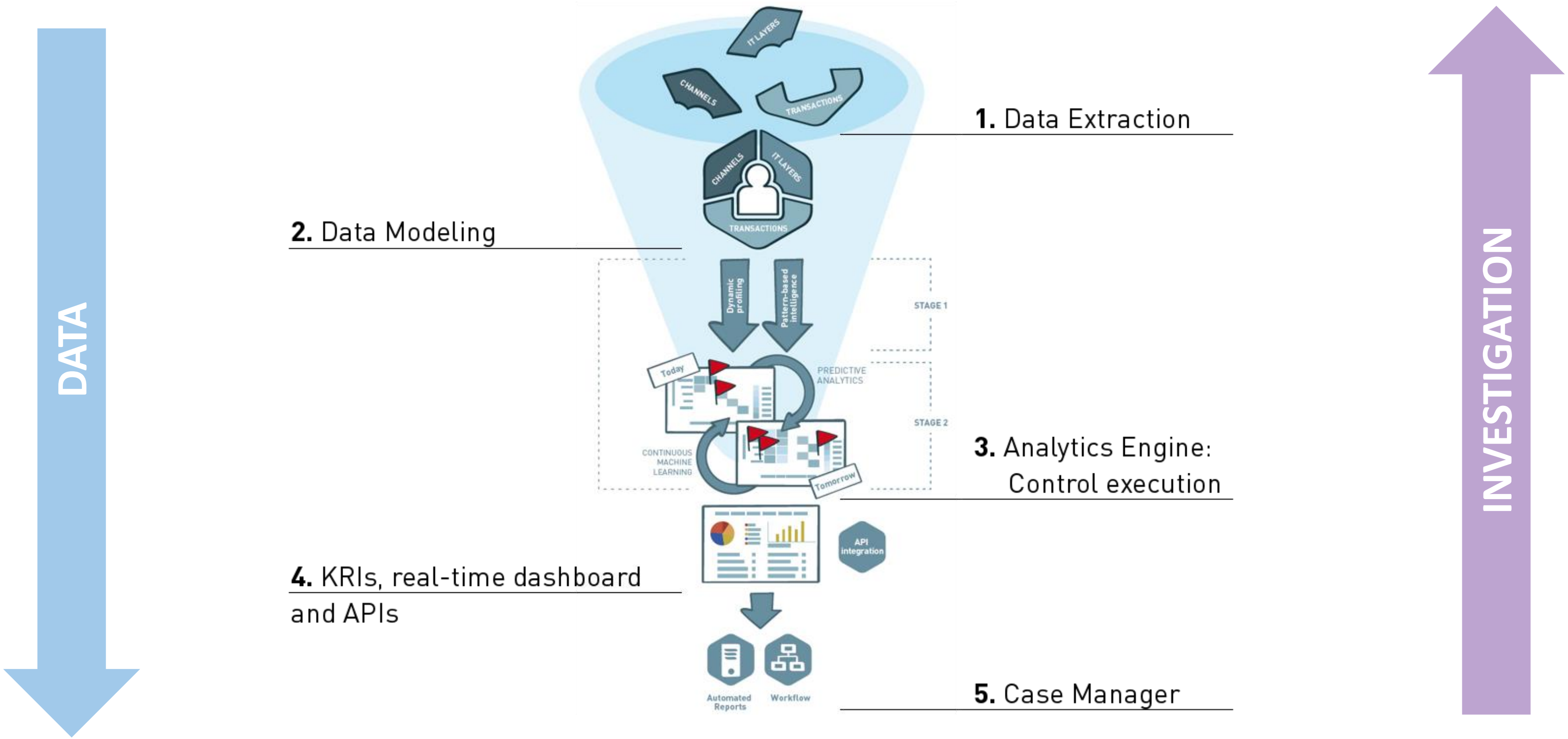
RiskTech 100 2018

Gartner 2015 CoolVendor

Product Overview

swiss made software

Big Picture



DATA

INVESTIGATION

1. Data Extraction

2. Data Modeling

3. Analytics Engine: Control execution

4. KRIs, real-time dashboard and APIs

5. Case Manager

Case Manager

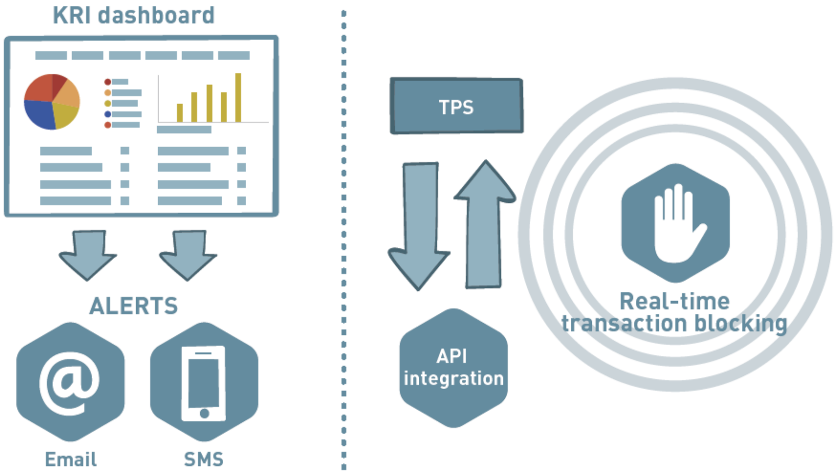
Centralize and enforce workflows

- Provides seamless communication and management of all issues.
- Exceptions in the control trigger a structured full workflow process.
- Ensures accountability and ownership of risk issues.
- Further supports risk management with trends analysis.

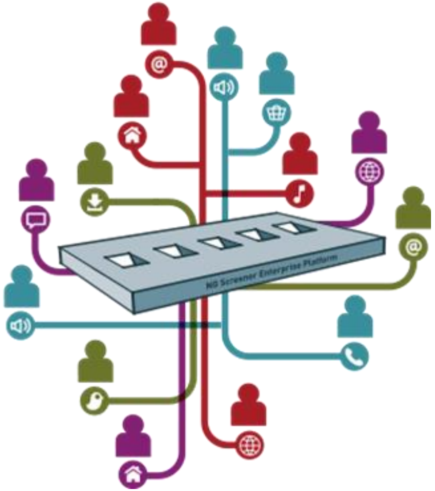
KRI, Dashboards and APIs

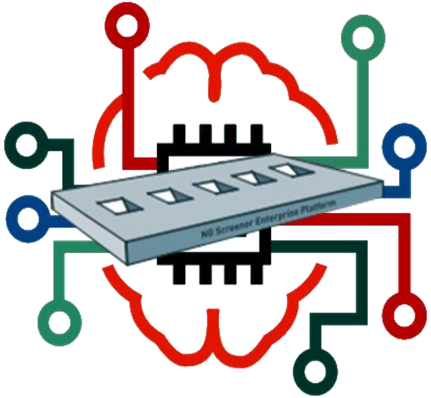
Make good usage of solution output

- Responsive key risk indicator (KRI) dashboard provides a control tower.
- Instant alerts to atypical activity.
- Rapid 1-click forensics for investigations.
- *API integration with transaction processing systems (TPS) permits scoring for real-time transaction blocking.*



Analytics Engine





Pattern Based Intelligence

Fundamentally rule based

Profiling

Statistical model
(with advanced management
techniques)

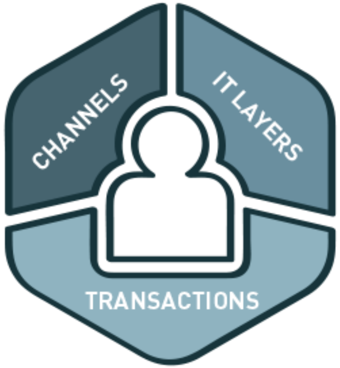
Machine Learning

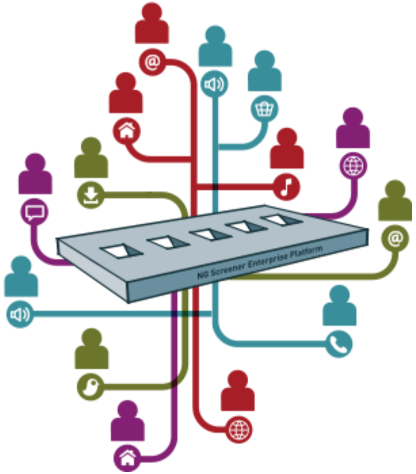
Advanced algorithms

Data Modeling

One and only model for all

- Unified and scalable data model.
- Correlates user actions with data prior to structuring.
- Matches information to continually updated critical use cases that regroup and implement best practices for fraud and risk mitigation.
- Enables automated control checks.





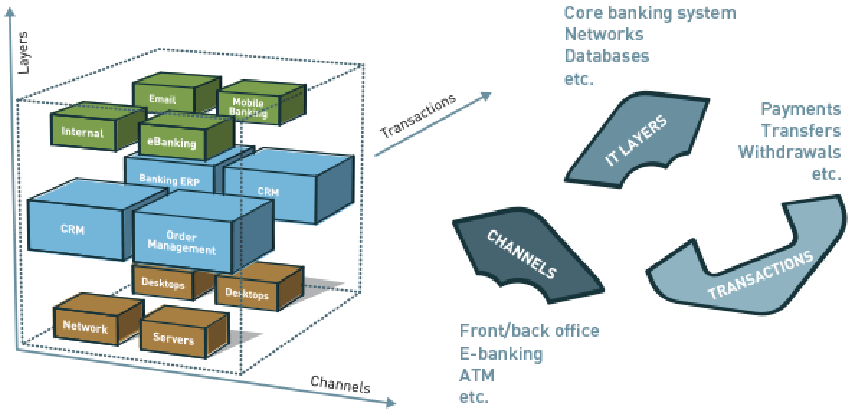
Data Extraction

Data is key

- Data Collection Framework (DCF) extracts and captures data

- Builds a consistent view of both transactions and user behavior behind the transaction.

- Methods: Polling in DB, Flat file import, Syslog, …



Thank you!

NetGuardians

+41 24 425 97 60

info@netguardians.ch

www.netguardians.ch

Linkedin.com/company/netguardians

Facebook.com/NetGuardians

@netguardians

https://www.youtube.com/netguardians

Ljupce Nikolov

+41 24 425 97 60

nikolov@netguardians.ch