FRAML: A transformação na Prevenção de fraudes e Lavagem de Dinheiro

SAS Campus – Cary, NC

Robson T. Ohosaku

Especialista em Prevenção a Fraudes e Security Intelligence

Americas FSI, SAS

AGENDA

FRAUD

AML

TENDÊNCIAS

FRAML

01 WHAT

02 WHEN

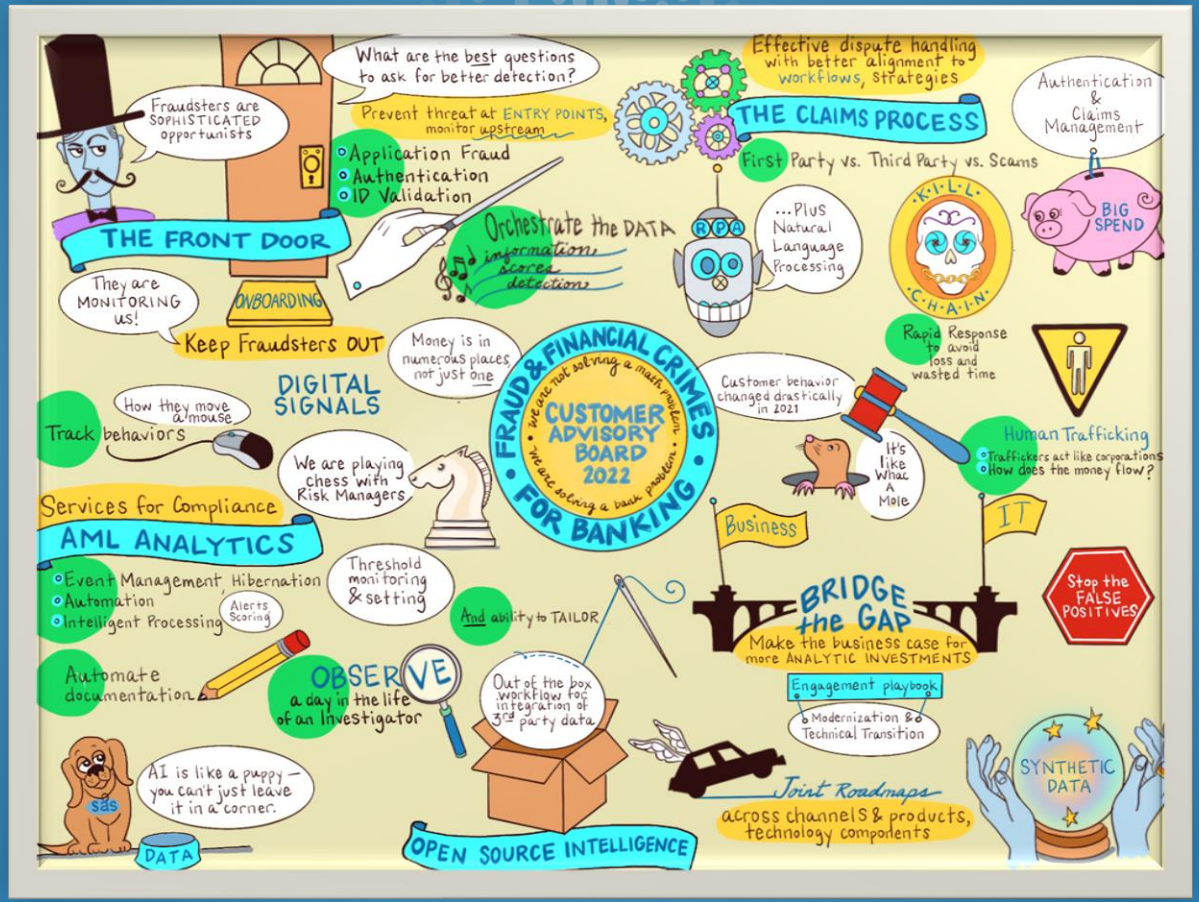
03 WHY

04 WHO

05 HOW

sas

2022 SAS CUSTOMER ADVISORY BOARD

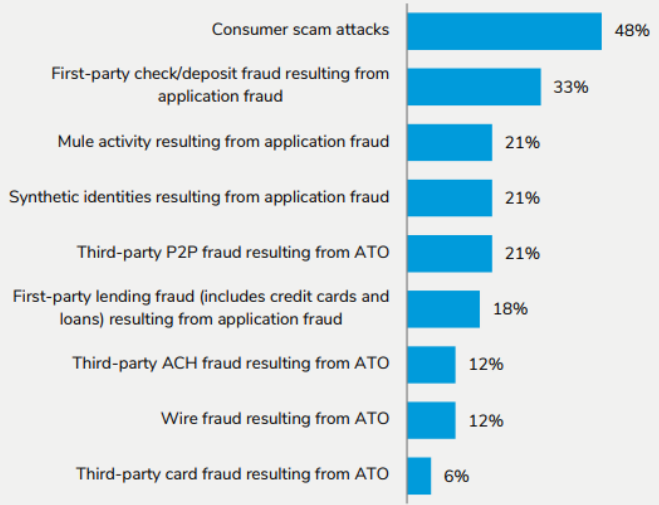


Aite Novarica

Top 10 Trends in Fraud & AML 2023

- Perception of economic deterioration x Fraud increase
- Uncertainty surrounding a shift in liability for Scam reimbursement
- Everything old is new again: check fraud and scams

Q. Thinking about the capabilities of your firm's transaction monitoring control framework to adequately detect attacks and prevent losses, which two types of fraud are you most concerned about in 2022? (Select top two; Base: 33 financial services fraud executives)

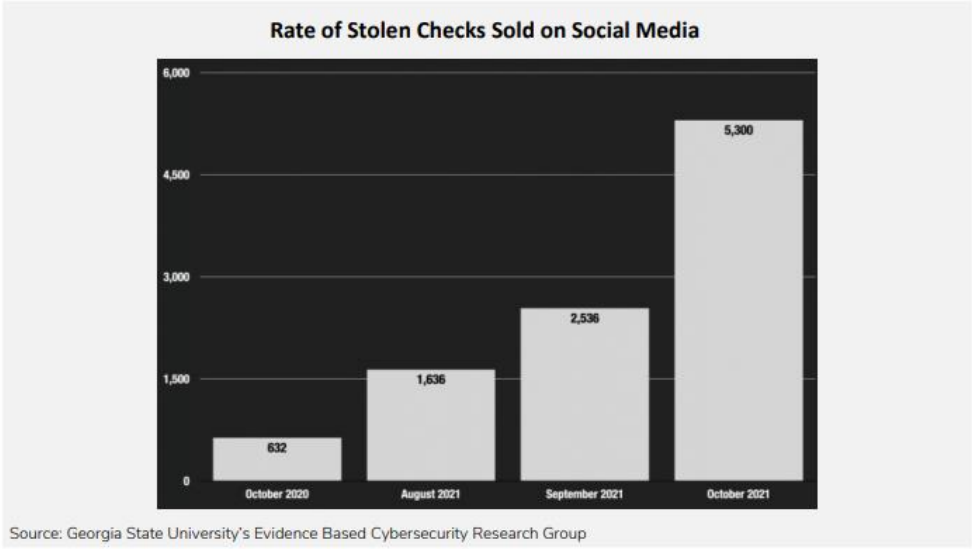


Source: Aite-Novarica Group's survey of 34 fraud executives at financial services companies, September to October 2022

It is the same old check fraud of decades ago: counterfeit checks, forged signatures and endorsements, altered check amounts and payees, and duplicate electronic and paper check deposits via mobile remote deposit capture (mRDC)

Thefts from mailboxes and U.S. postal boxes increased by 161% from March 2020 to February 2021

FIGURE 6: RATE OF STOLEN CHECKS SOLD ON SOCIAL MEDIA



Source: Georgia State University's Evidence Based Cybersecurity Research Group

sas

2022 Anti-Fraud Technology Benchmarking Report

Key findings from a global, cross-industry survey of anti-fraud professionals by the Association of Certified Fraud Examiners and SAS

Through the pandemic, analytics has emerged an INDISPENSABLE FRAUD FIGHTING TOOL

43% of organizations have increased their use of **DATA ANALYTICS** in response to the COVID-19 pandemic.

99% of organizations named the increased volume of transactions reviewed and potential fraud detected AND the improved timeliness of anomaly detection as key benefits of their anti-fraud analytics programs.

The Use of Artificial Intelligence and Machine Learning in anti-fraud programs is expected to **grow more than 150%** in the next two years.

Budgetary restrictions are the biggest anti-fraud tech challenge cited by organizations, and yet...

60% of organizations expect their anti-fraud technology budgets to increase over the next two years.

48% of organizations identified **advanced analytics** as a top investment priority, including AI and machine learning (26%) and predictive analytics/modeling (22%).

MORE THAN 40% of organizations expect to add computer vision analysis, robotics, or blockchain tech to their anti-fraud tools in the next 1-2 years.

Learn More
sas.com/fraudreport

ACFE Association of Certified Fraud Examiners

sas

KEY FINDINGS

MORE THAN 1/2

of organizations currently use **exception reporting and anomaly detection, as well as automated monitoring of red flags and business analysis** as part of their anti-fraud programs.

Over the next two years, **use of each of these techniques is expected to grow** to more than

2/3 OF ORGANIZATIONS

THE USE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

in anti-fraud programs is expected to more than

DOUBLE

over the next two years.

34% of organizations currently contribute to data-sharing consortiums to help combat fraud,

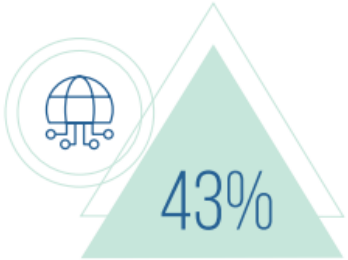
AND

24% would be willing to contribute in the future.

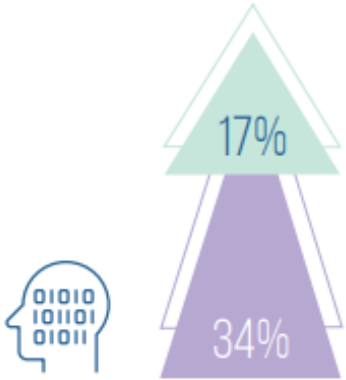
BUDGET AND FINANCIAL CONCERNS

are the biggest challenge for organizations in implementing new anti-fraud technologies.

of organizations expect an increase in their
ANTI-FRAUD TECHNOLOGY BUDGETS
in the next two years.



of organizations have increased their use of
DATA ANALYTICS
in response to the COVID-19 pandemic.

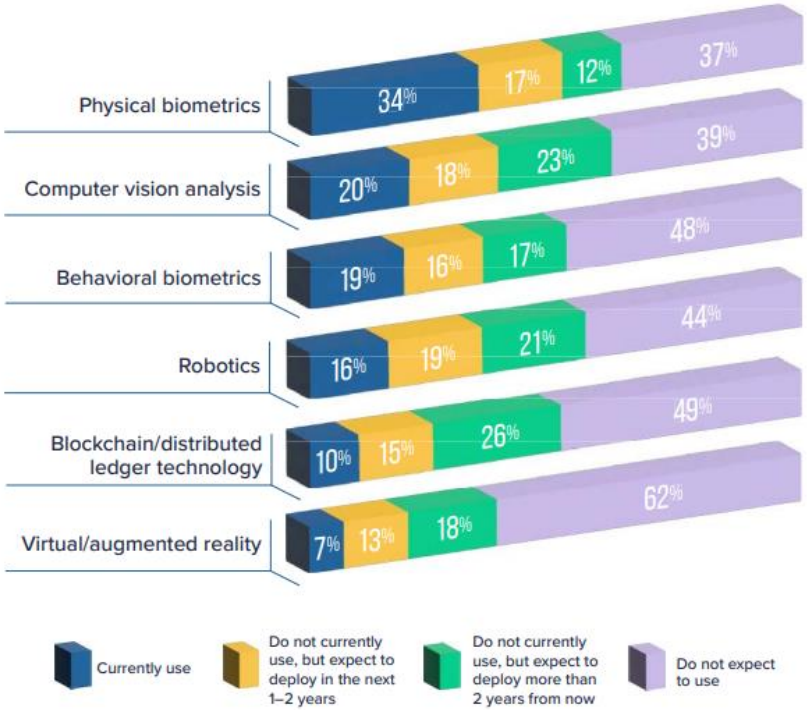


34% of organizations currently use

PHYSICAL BIOMETRICS

as part of their anti-fraud programs, and another 17% expect to adopt this technology in the next two years.

FIG.12 What emerging technologies are organizations using to fight fraud?



Jornada Analítica em PLD-FT

"AML Next Gen"

Como Instituições estão reduzindo de 30%~50% dos seus alertas improdutivos ?

- Após a segmentação, as taxas de produtividade foram de 2,8% para 6,8% e o volume global de alertas diminuiu
- Após o ajuste de pontos de cortes, a taxa de produtividade melhorou para 10,4%.

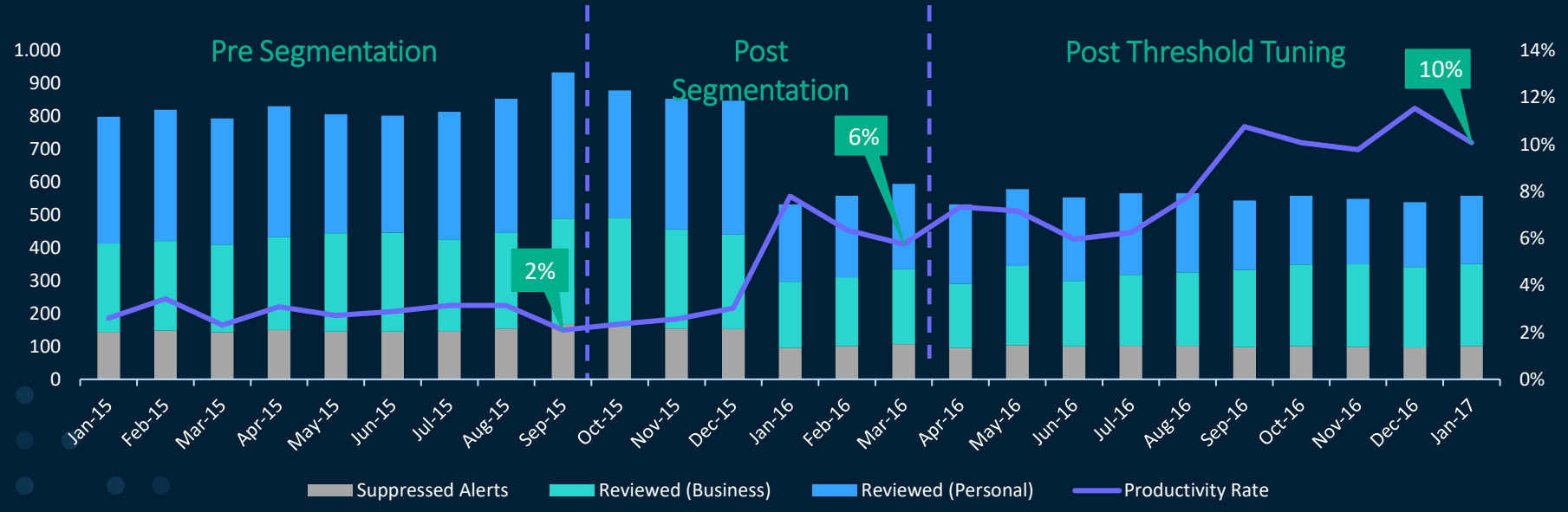
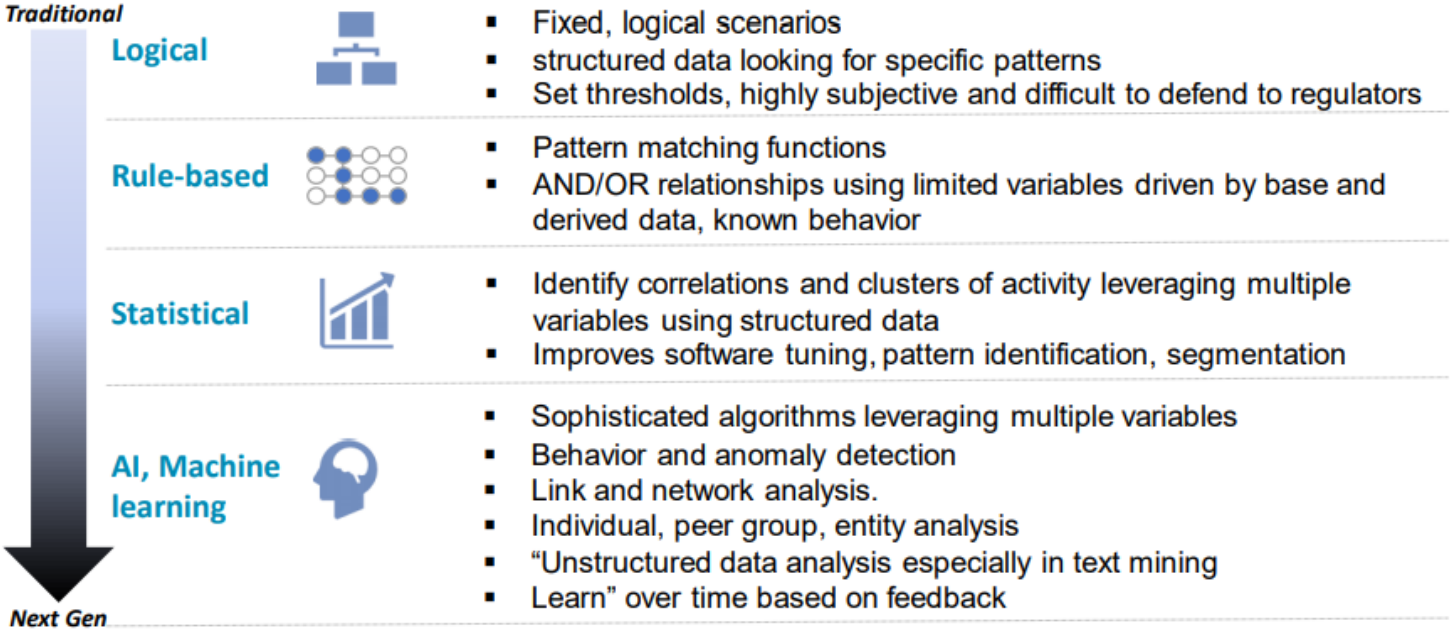


Figure 2: From Evolution to Revolution in AML Analytics



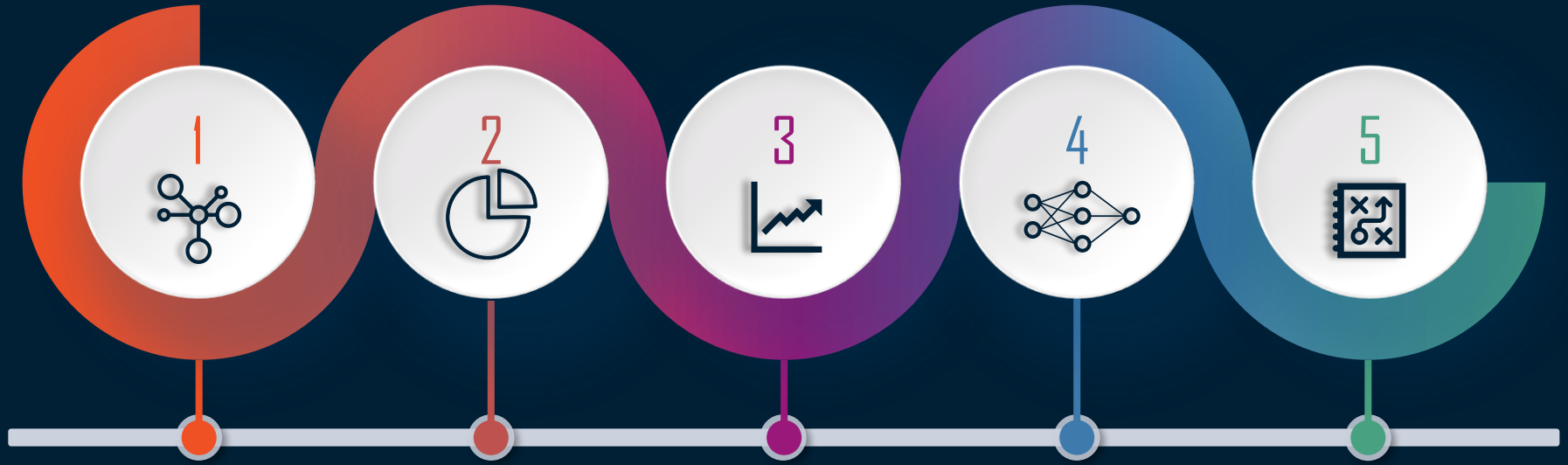
Source: Celent

A jornada de adoção do Analytics em PLD

Preparação de Dados e Definição de limiar inicial

Exploração e ajuste contínuos

Classificação automática e detecção baseada em ML



RESOLUÇÃO DE ENTIDADES & NETWORKS

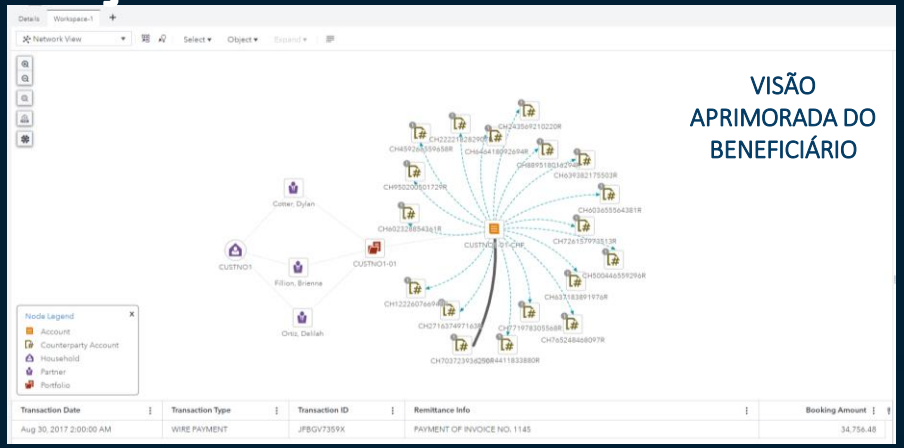
SEGMENTAÇÃO DE CLIENTES

OTIMIZAÇÃO DO AML

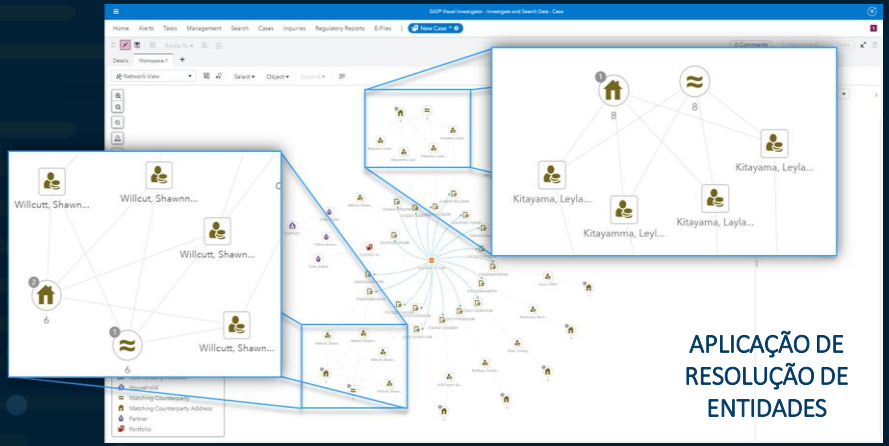
PRIORIZAÇÃO DE ALERTAS

CENÁRIOS BASEADOS EM MODELOS

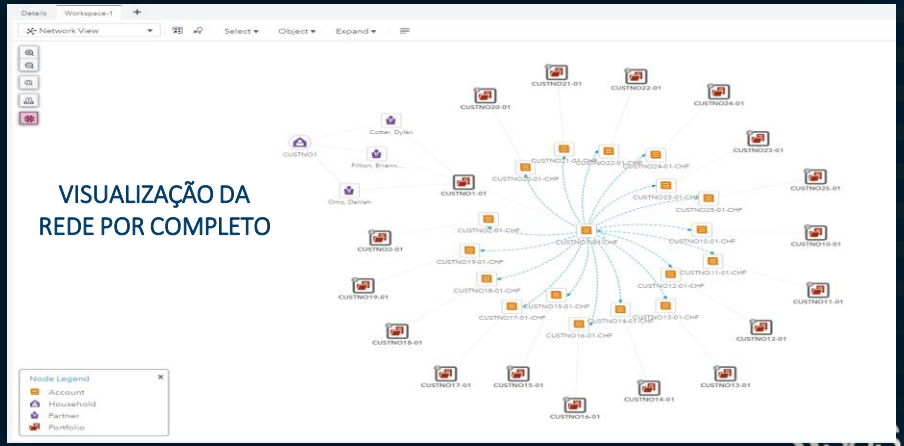
Resolução de entidades & Network



VISÃO APRIMORADA DO BENEFICIÁRIO



APLICAÇÃO DE RESOLUÇÃO DE ENTIDADES

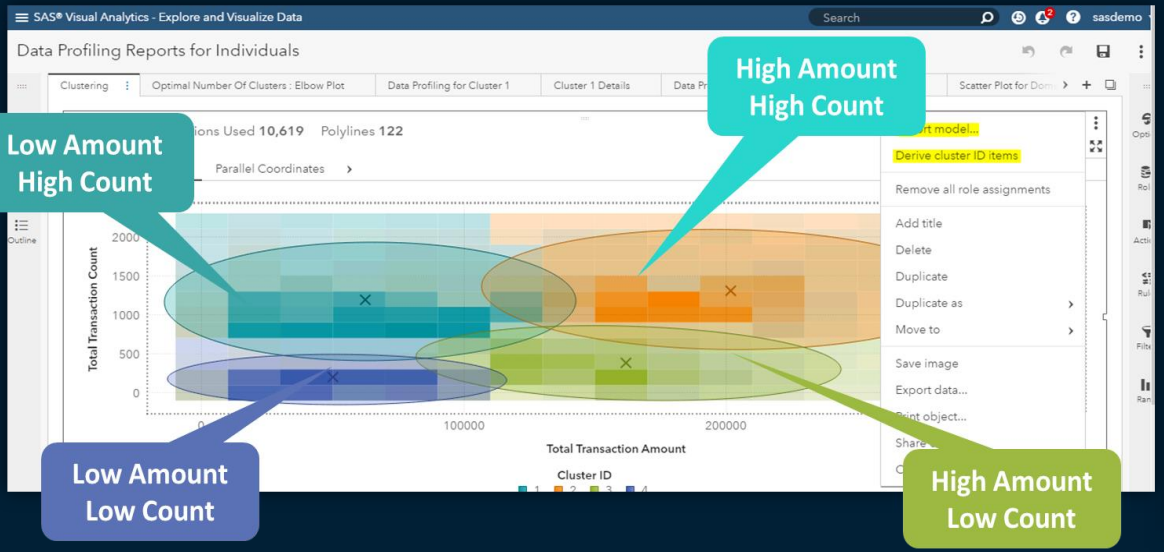


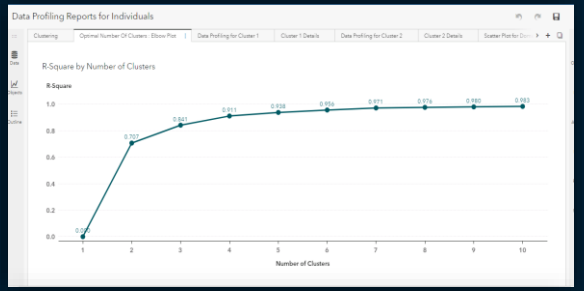
VISUALIZAÇÃO DA REDE POR COMPLETO

Segmentação de clientes

Agrupamento de clientes e contas com características e comportamentos transacionais semelhantes

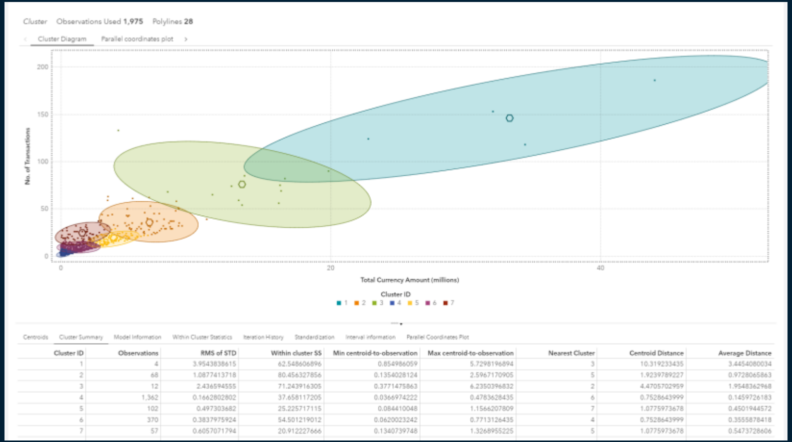
- ✓ Melhoria das taxas de produtividade com regras e limites baseados em segmentos;
- ✓ Cobertura visual de transações, contas, clientes e dados familiares;
- ✓ Identificação de anomalias em padrões de transação ou comportamentos.



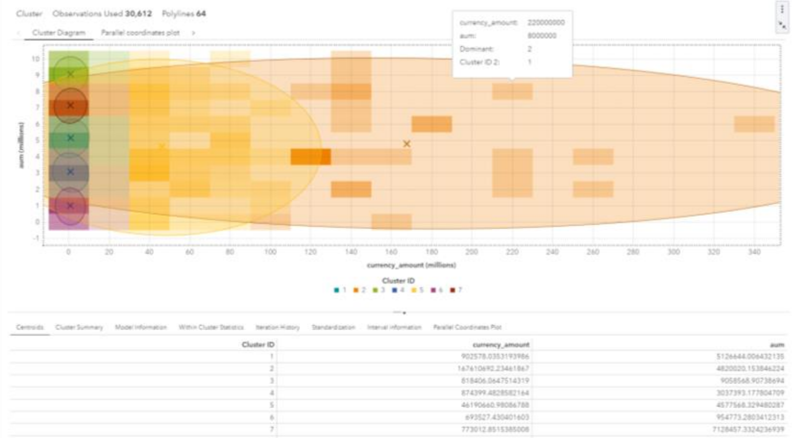


Detecção de Anomalias

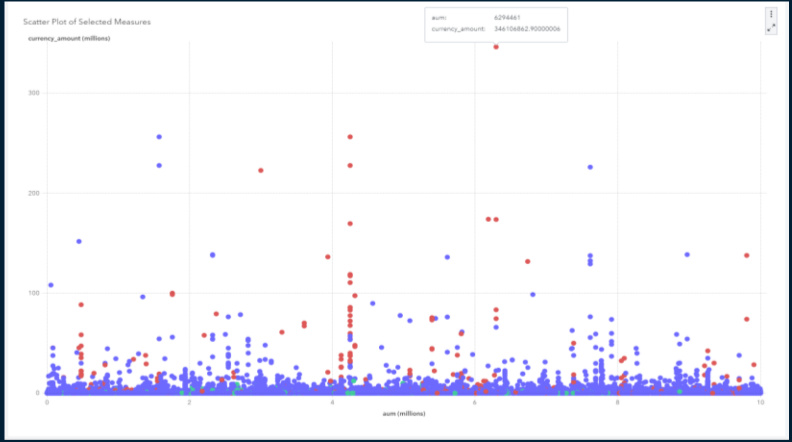
EXECUÇÃO DA SEGMENTAÇÃO DE CLIENTES



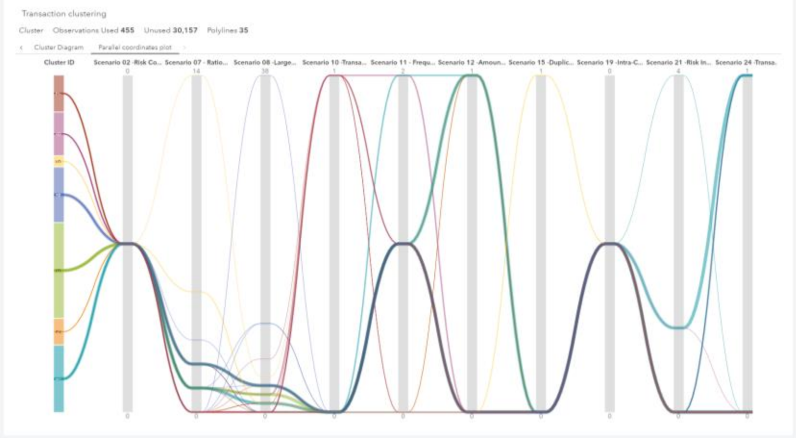
CRIAÇÃO DE CLUSTERS DE TRANSAÇÃO



DETECÇÃO DE ANOMALIAS EM TRANSAÇÕES



ANALISE DE TRANSAÇÕES DESENCADEADAS

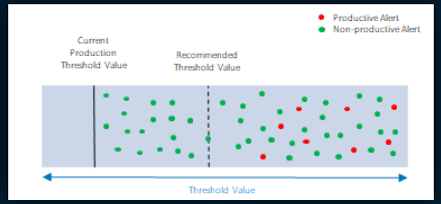


Otimização do PLD

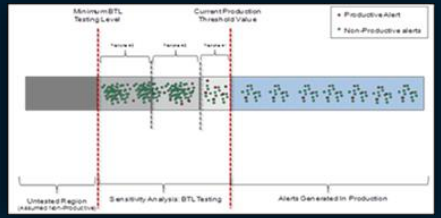
Verificar, refinar e aprimorar o processo de monitoramento de transações existente, realizando uma revisão contínua do design e eficácia do cenário usando métodos estatísticos e processos analíticos

- ✓ Maximização do número de alertas que justificam investigação, descobrindo novos padrões;
- ✓ Minimização do número de alertas que podem ser facilmente fechados com pouca ou nenhuma revisão do analista investigativo;
- ✓ Determinar se os valores limite dos parâmetros do cenário estão ou não devidamente definidos;
- ✓ Identificação das eficiências potenciais nos processos de AML, revisando os efeitos operacionais do design do cenário

Acima da linha



Abaixo da linha

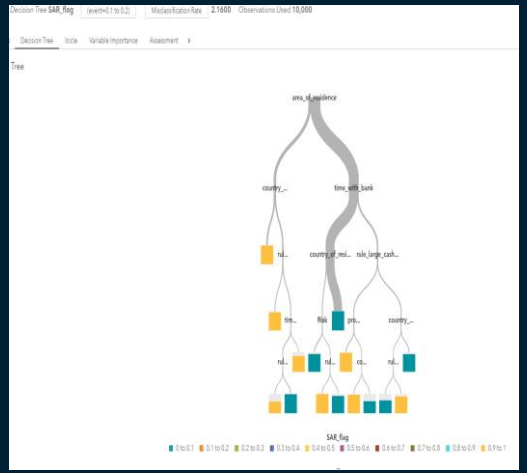


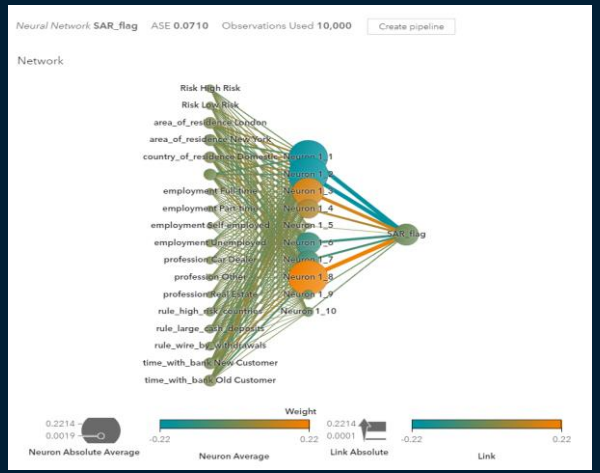
Painel interativo
Revisão da efetividade

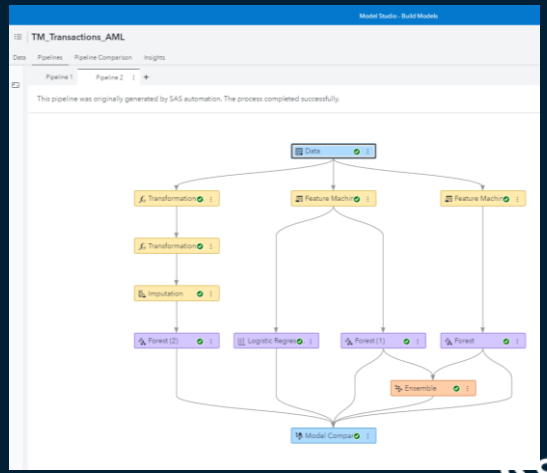
Priorização de alertas

Aprender com os alertas anteriores e analisar os resultados de produtividade para prever a probabilidade de um cliente ser suspeito

- ✓Recursos investigativos mais concentrados em atividades/clientes mais arriscados
- ✓Avaliar continuamente a entidade quanto a atividades potencialmente suspeitas e automatizar ou atrasar a revisão de alertas de baixo risco
- ✓Obter uma visão holística das atividades do cliente alertado
- ✓Redução de falsos positivos gerados pelo sistema de monitoramento de transações baseado somente em regras







Cenários baseados em modelos

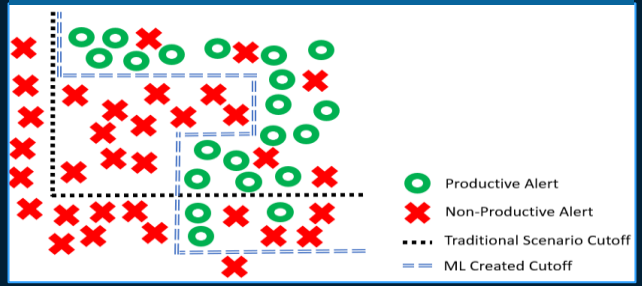
Regras tradicionais

- As regras por si só podem criar altas taxas de falsos positivos e potencial para falsos negativos devido ao uso de limites
- As regras levam em consideração um pequeno número de parâmetros
- Muitas regras são necessárias para identificar uma tipologia de fraude complexa

Modelos de Machine Learning

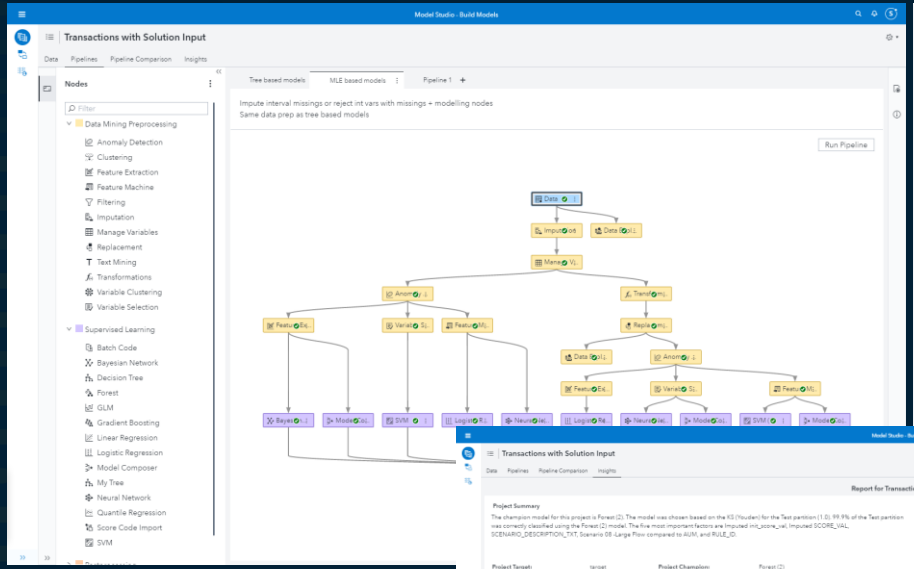
- ✓ Os modelos não usam limites e podem detectar comportamentos com mais precisão, reduzindo o erro Tipo I e Tipo II
- ✓ Os modelos podem aproveitar centenas de recursos para detectar crimes financeiros
- ✓ Os modelos podem observar padrões de comportamento, substituindo muitas regras por um modelo para detectar uma tipologia de comportamento

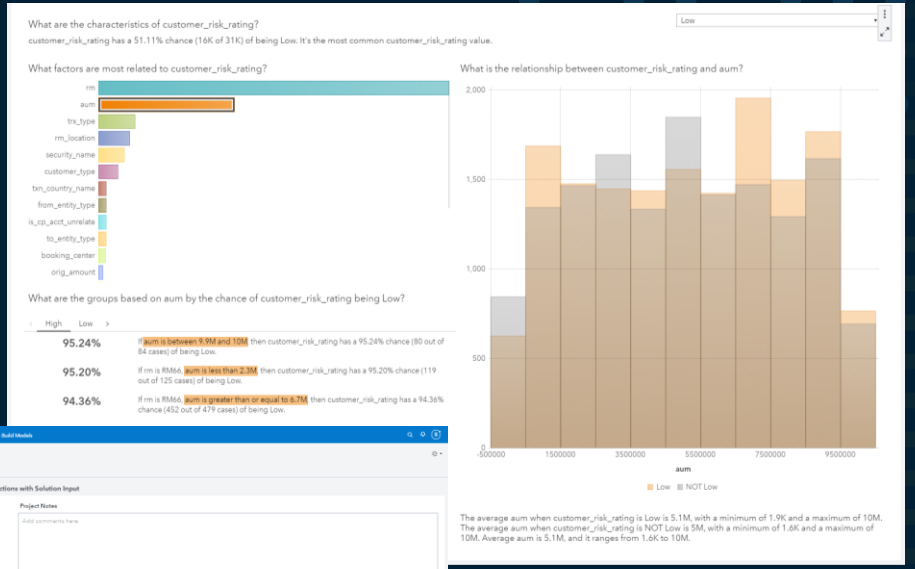
Uma visão de como um modelo de aprendizado de máquina pode fornecer alertas mais produtivos sobre atividades suspeitas do que so cenários tradicionais baseados em regras

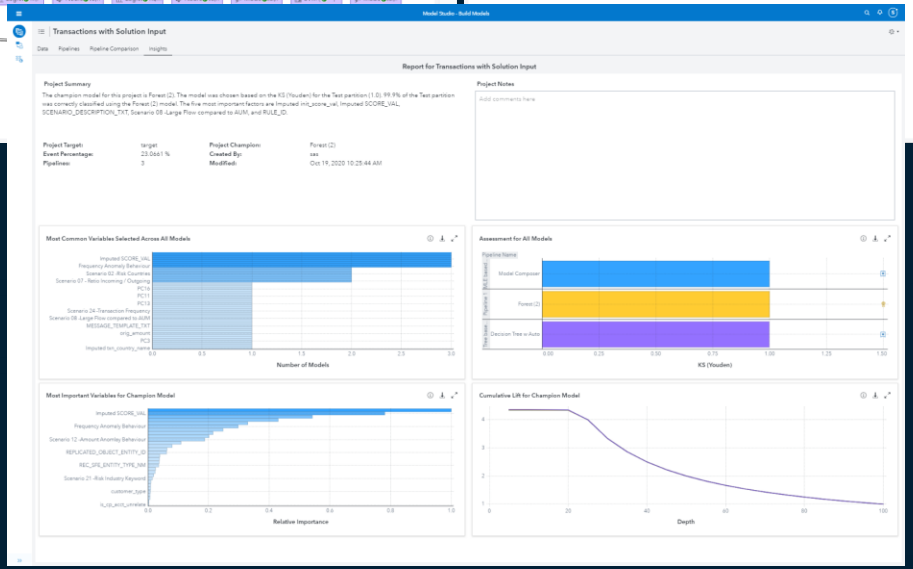


Embora os modelos não substituam todas as regras, eles fortalecerão a capacidade de um programa AML de detectar atividades suspeitas e reduzir falsos positivos

Explainable Analytics







sas

Alguns resultados

"AML Next Gen"

Análise de Crimes Financeiros

Resultados

SEGMENTAÇÃO

- **3-5x**

de melhoria nas taxa de conversão do Report ao Regulador

TRIAGEM AUTOMÁTICA

- **35-50%**

de redução de falsos positivos

Redução do esforço do analista

MODELOS DE REDE NEURAL

- **50%**

de redução de alertas

Diversidade de comportamento

NLP

- **25%**

de ganho de eficiência por meio da automação

Taxas de erro reduzidas

Conclusões

- FRAUDE: *old is new again* / Orquestração&Autenticação
- PLD: maior foco em Analytics
  - Deixa de ser área vista como controle/processos
  - ↑ Pressão dos reguladores (ABR)
  - Necessidade de melhoria eficiência operacional
- Ataques de Fraude e de Lavagem de Dinheiro estão mais complexos
- Necessário reações mais sofisticadas
- Necessário visão do contexto, não apenas mais foco no on-boarding ou transacional
- Batch x Real time

AGENDA

FRAUD

AML

TENDÊNCIAS

FRAML

01 WHAT

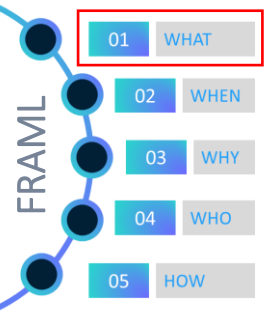
02 WHEN

03 WHY

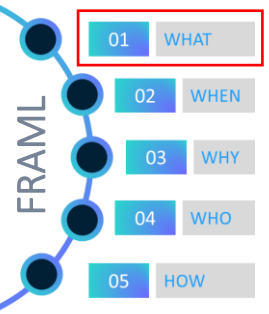
04 WHO

05 HOW

sas



WHAT is FRAML / Fusion Center

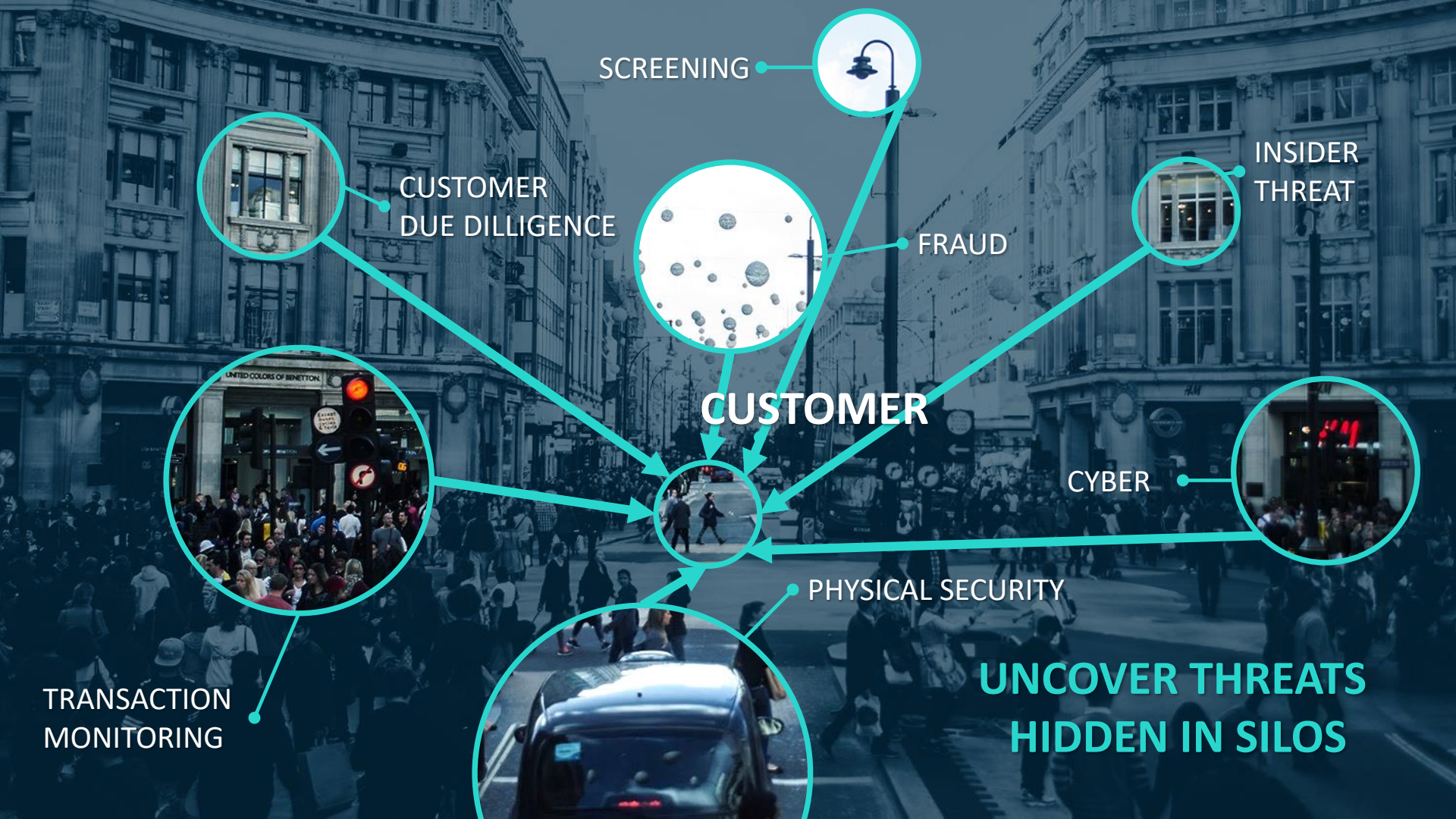


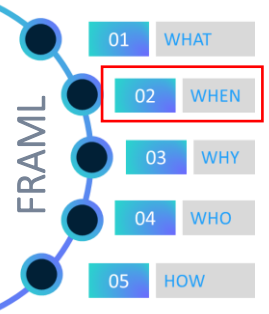
WHAT IS NOT

- Elimination of specialized experts in Fraud, AML and Cyber
- Single business process and workflow for all domains
- Common SLAs
- One detection engine

Convergence is about bringing people and data together using technology, while embracing what each needs to reach quality decisions


SCREENING
CUSTOMER
DUE DILLIGENCE
FRAUD
INSIDER
THREAT
CUSTOMER
CYBER
PHYSICAL SECURITY
TRANSACTION
MONITORING


SCREENING
CUSTOMER
DUE DILLIGENCE
FRAUD
INSIDER
THREAT
CUSTOMER
CYBER
PHYSICAL SECURITY
TRANSACTION
MONITORING
UNCOVER THREATS
HIDDEN IN SILOS

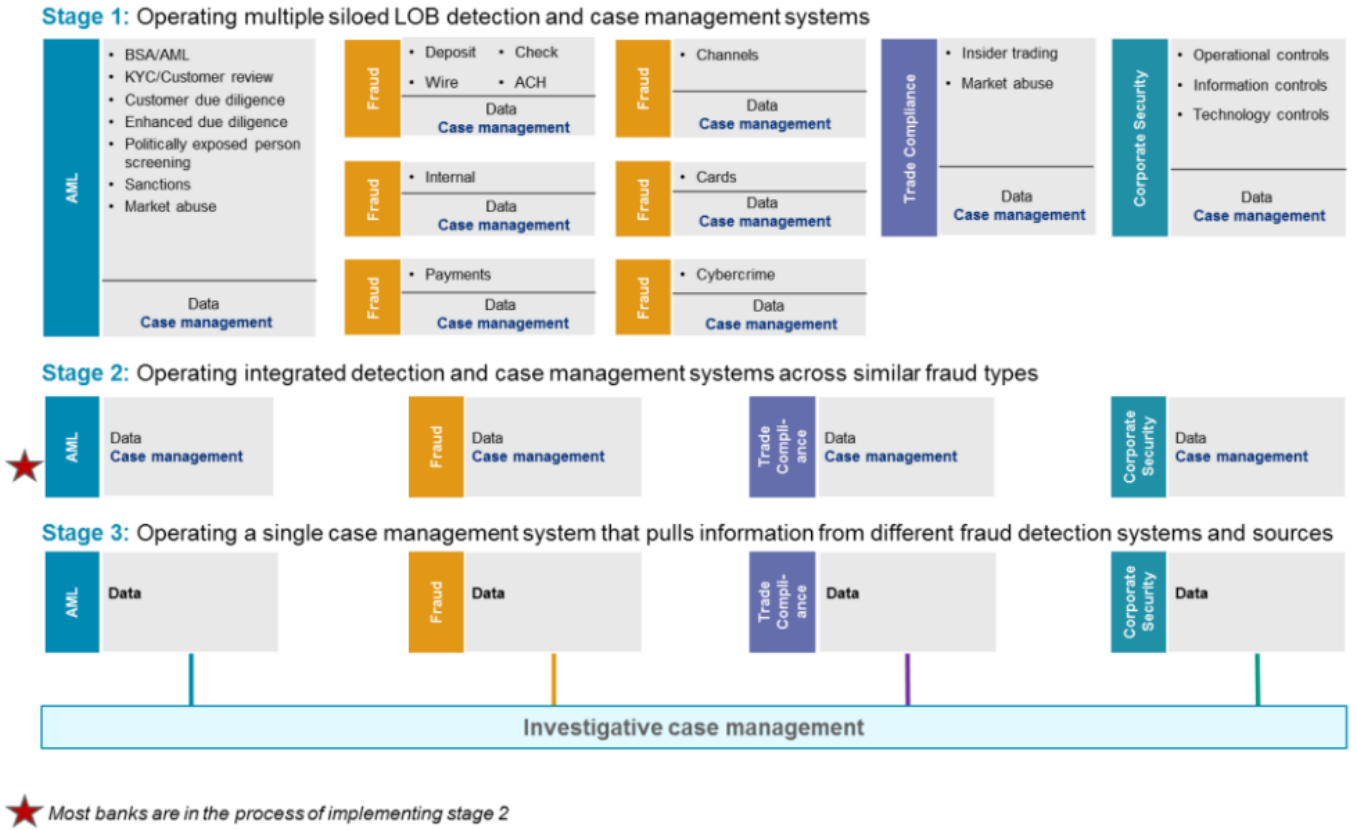


WHEN

> The number of data sources used will only increase because digitalization of banking will generate more data, and financial institutions will need to use them to create holistic customer views, find links between their customers and suspect entities, and analyze complex behavior and patterns spanning multiple accounts, channels, and business lines

Celent
IT and Operational Spending in AML-KYC, A Global Perspective, 2019

Figure 4: Three Stages to Integrated Financial Crime Management; Most Banks Are on the Cusp of Stage Two



FRAML

01 WHAT

02 WHEN

03 WHY

04 WHO

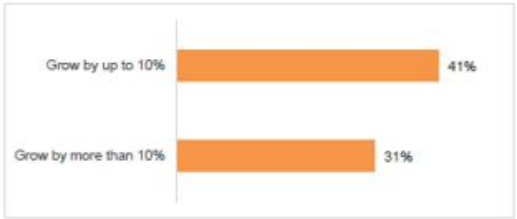
05 HOW

About the research

Longitude Research surveyed 121 investment and commercial banks equally split across Europe and North America

Chart 2. The main areas of focus for FCIUs

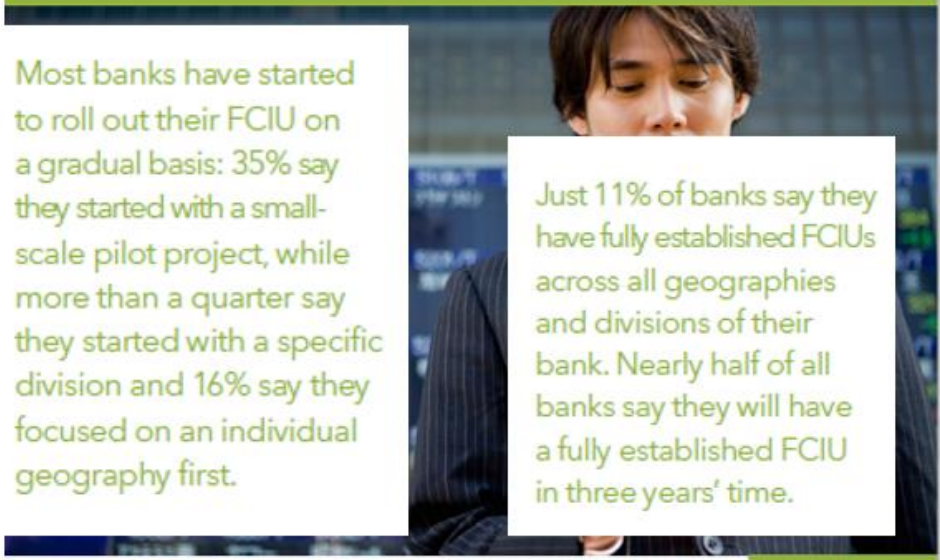
Chart 5. FCIU budget growth over the next three years



Combating Financial Crime:

The Increasing Importance of Financial Crimes Intelligence Units in Banking

Most banks have started to roll out their FCIU on a gradual basis: 35% say they started with a small-scale pilot project, while more than a quarter say they started with a specific division and 16% say they focused on an individual geography first.

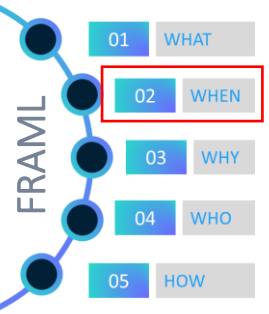


Just 11% of banks say they have fully established FCIUs across all geographies and divisions of their bank. Nearly half of all banks say they will have a fully established FCIU in three years' time.

Longitude

sas THE POWER TO KNOW.

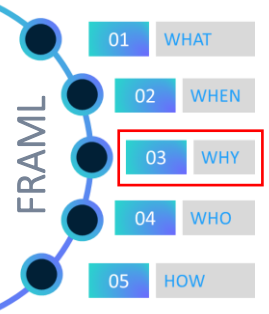
sas



- 42% of FI compliance executives had information and data sharing as well as enterprise policies and processes in place
- 27% had fully consolidated case management and staff
- 23% had integrated detection technology

(Aite Novarica, 2022)

Aite Novarica



WHY

Benefits:

- Enhanced ability to identify complex financial crimes schemes
- Equal access to technologies across domains
- Alignment with regulatory expectations
- Long term cost savings

Hurdles:

- Siloed data and applications
- Required buy in from organizations with distinct leadership, budgets, and operations
- Satisfaction with status quo
- Short term budget restrictions

Ally Financial

Ally Financial is a top 25 US based digital Financial Institution with 10.5M total customers. A long time AML Customer, Ally wanted to modernize their Financial Crime program to combine Fraud and AML operations, detect Fraud in real-time and embrace modern Cloud architectures.

A single, unified alert and case management for fraud and AML

Real-time detection across all Fraud Types

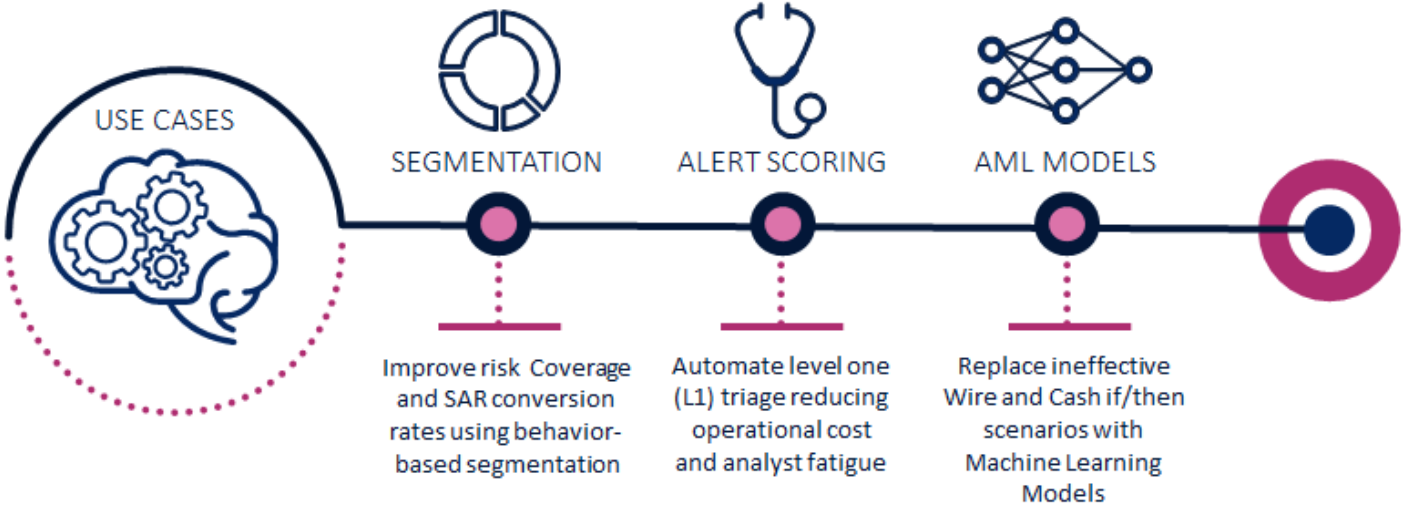
Automated interdiction of payments (hold / block / release)

Customer Risk Scoring and Enhanced Due Diligence

This modernization effort will improve detection, standardize workflows and SLAs across the business, and allow redundant applications across the Ally to be decommissioned.

Truist

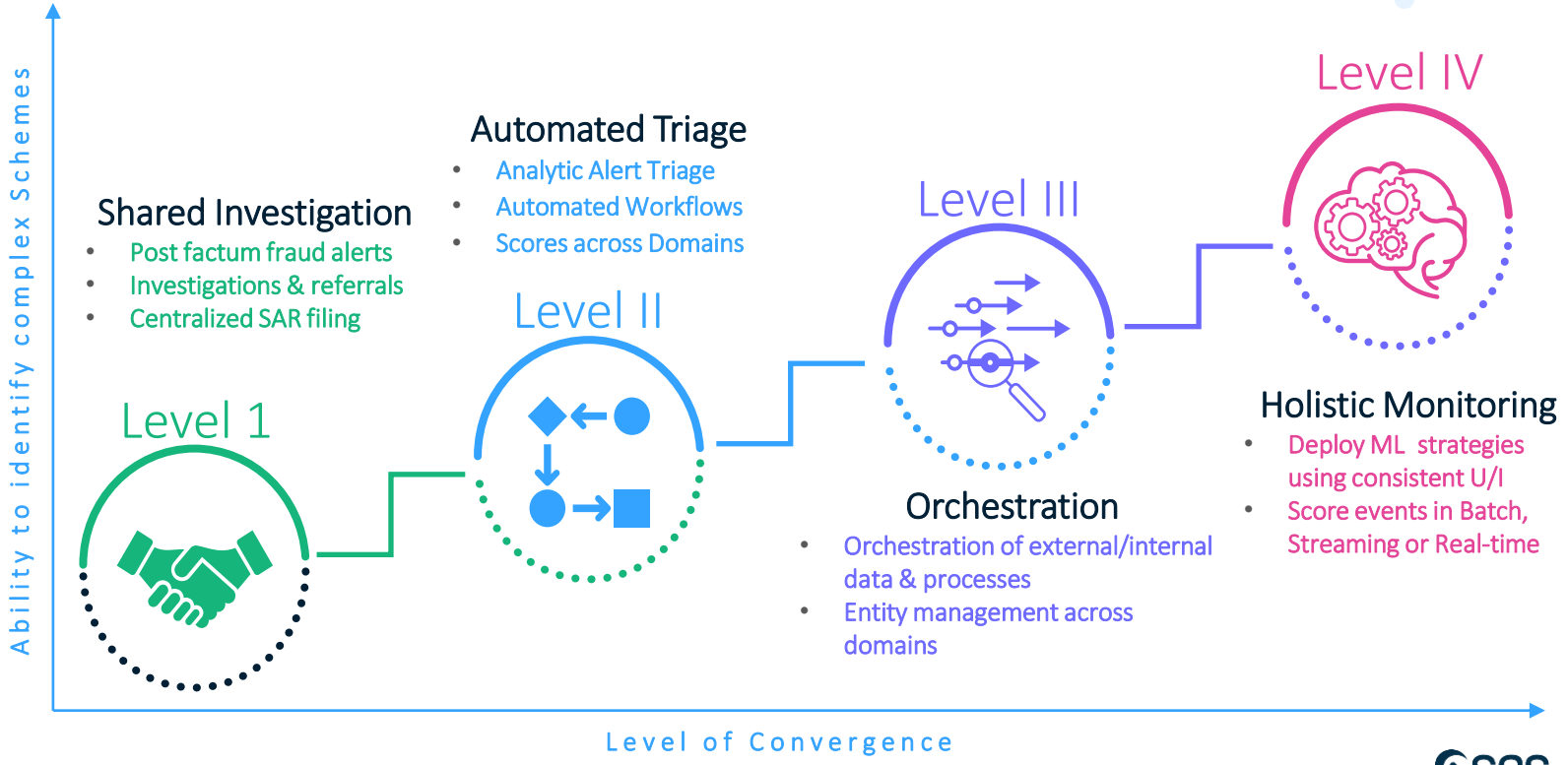
Truist Financial Corporation is an American bank holding company headquartered in Charlotte, North Carolina. The company was formed in December 2019 as the result of the merger of BB&T and SunTrust Banks. In 2021, they invested in a Viya 4 Financial Crimes Analytics environment to complement their SAS AML deployment.

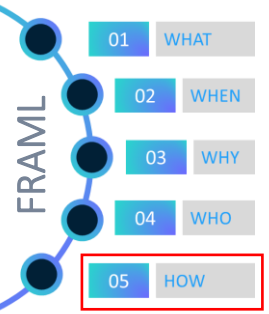


FRAML

01 WHAT
02 WHEN
03 WHY
04 WHO
05 HOW

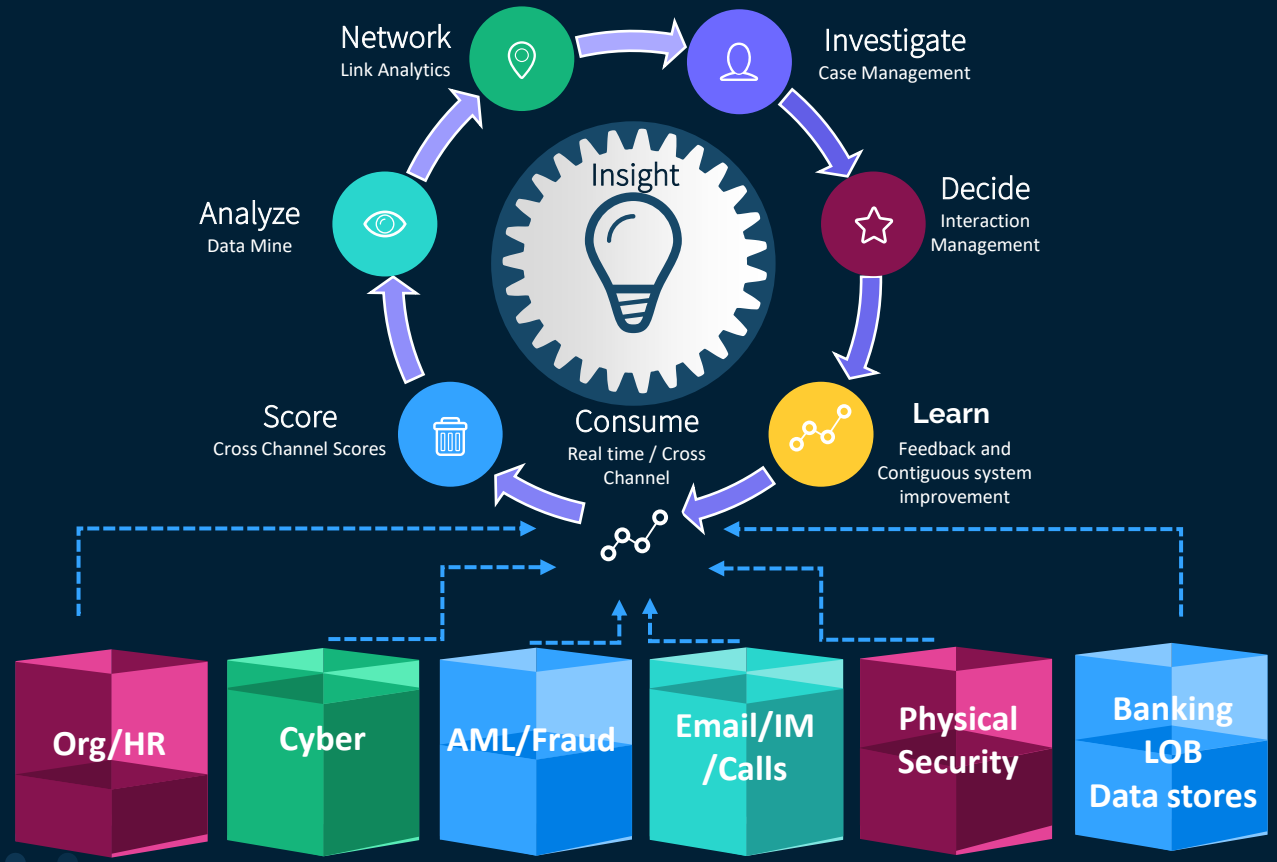
HOW



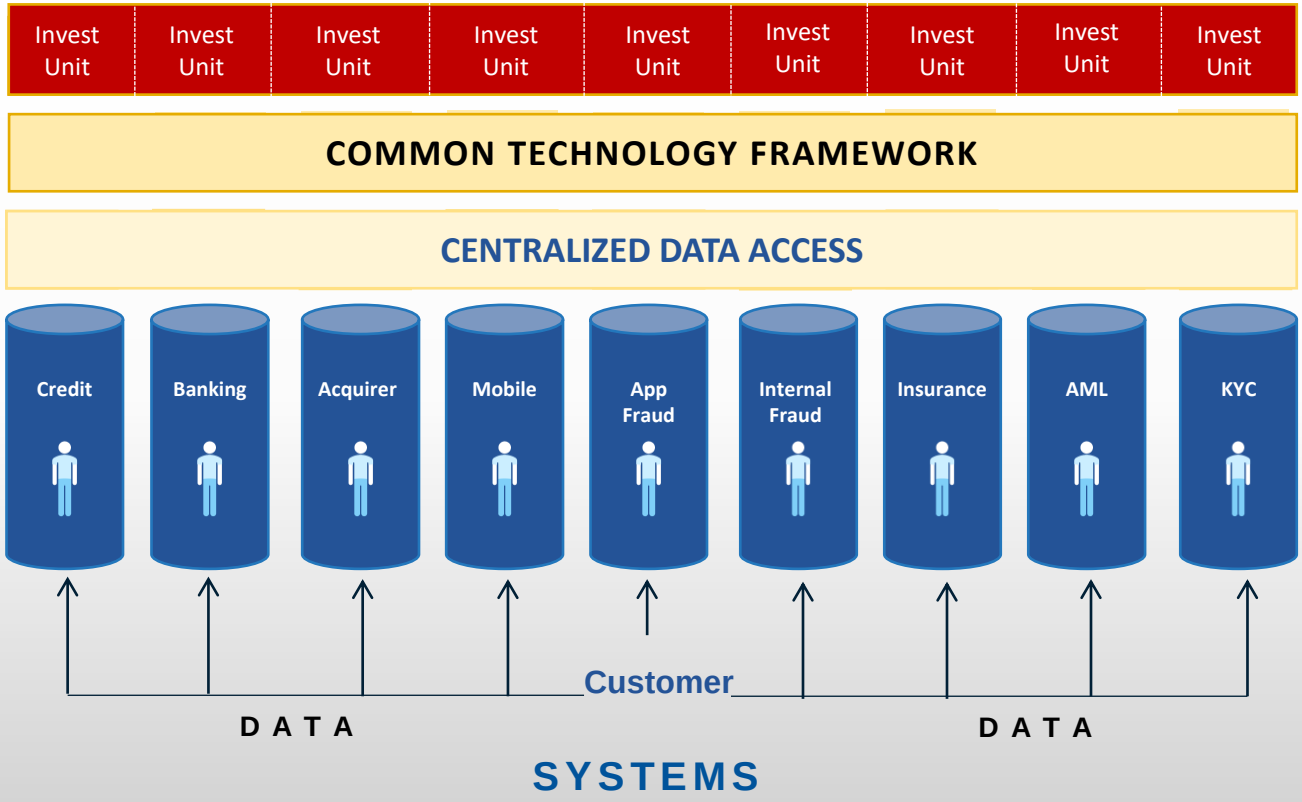


HOW SAS
solves this need/approach

SAS end-to-end platform

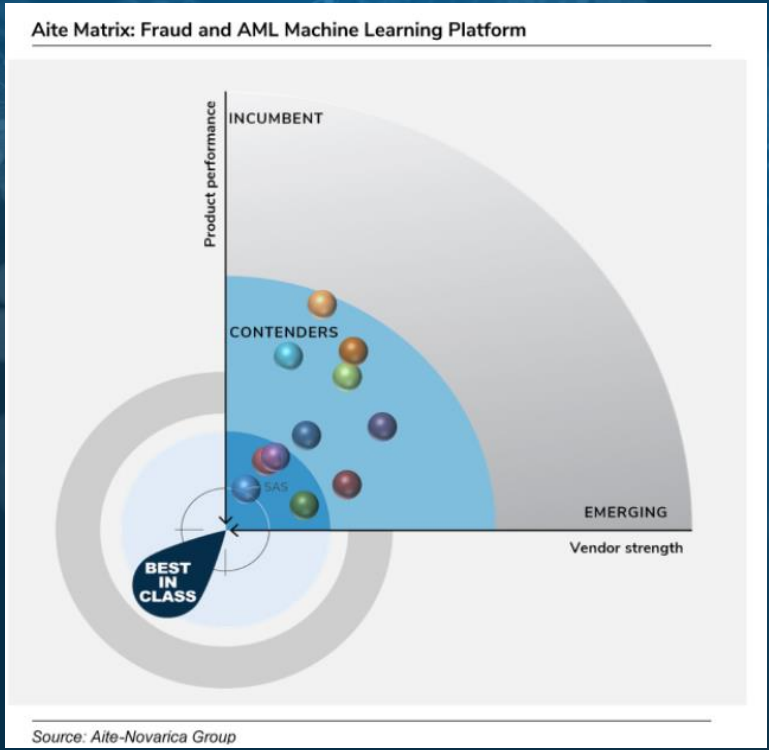


Holistic Customer View



SAS named Best-in-Class vendor in the Aite Matrix: Leading Fraud & AML Machine Learning Platforms

Fraud & AML, Jan 2022



Key Strengths:

- *Superior model performance*
- *Excellent support and advisory services*
- *Ease of implementation and integration*

SAS scored high among its competition in all areas, but edged out the rest with the highest score in the Product Features category.

(link)

Muito Obrigado!

Robson Toshimitsu Ohosaku
LATAM Security Intelligence
Solutions Manager