EVENT

FRAUD ROUNTABLE

IA para la prevención del fraude en un mundo digital

Jueves, 25 de abril

BANKING SESSION

8-10am

sas

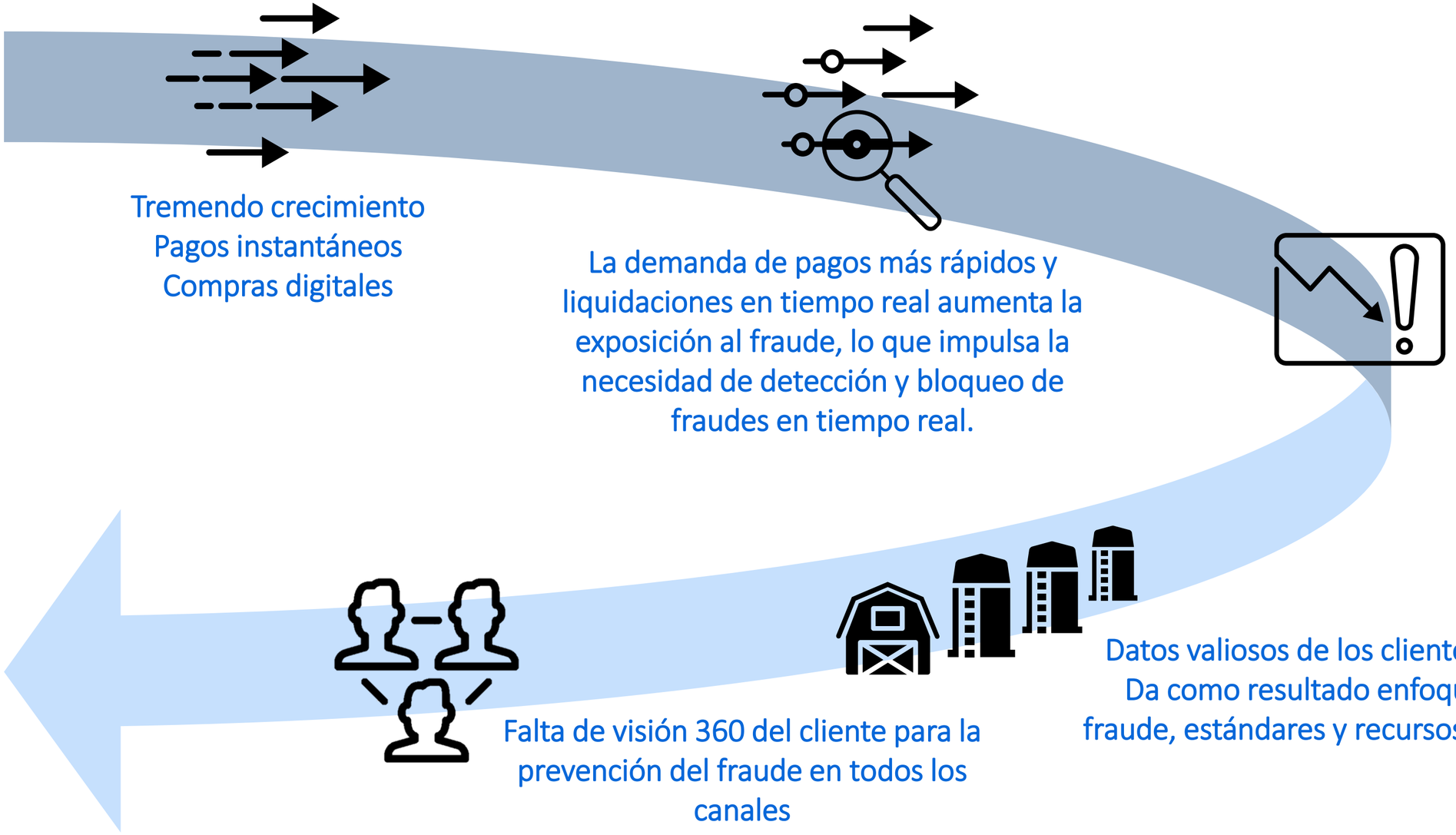
El futuro de la banca en una economía digital exige mejores conocimientos.

- Crezca, innove y saque más provecho de sus datos
- Conéctese mejor con los clientes, obtenga nuevos conocimientos sobre el riesgo y muévase más rápido en el mercado financiero
- Adáptese al nuevo clima de negocios actual y tome decisiones con confianza para el futuro
- Evolucione su estrategia analítica para tomar mejores decisiones que elevarán a las personas, al planeta y a todo el potencial de su banco

¿Cuál es la implicación?

Se espera que el fraude en los pagos siga aumentando y se prevé que el costo sea de **$40.62 mil millones en** 2027 – **25% más alto que en** 2020.

DESAFÍOS DE LOS BANCOS



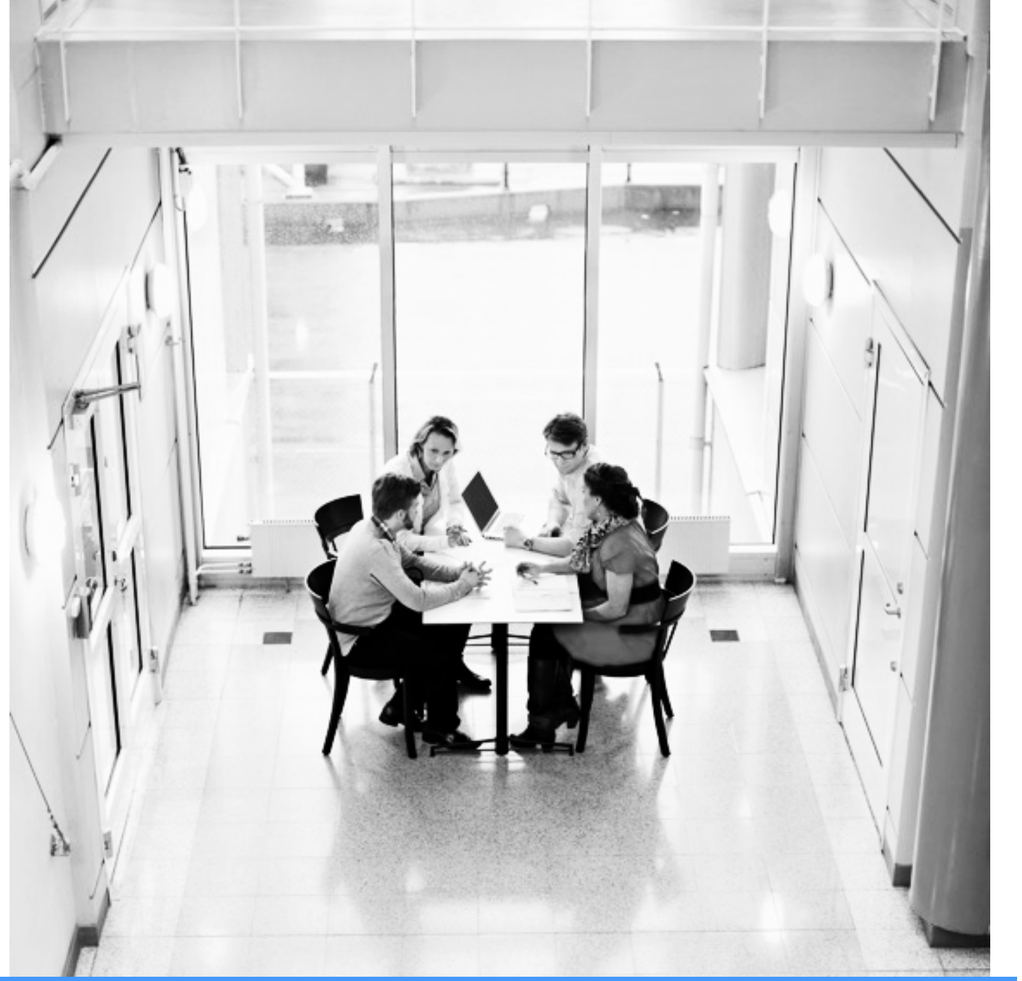
Tremendo crecimiento
Pagos instantáneos
Compras digitales

La demanda de pagos más rápidos y liquidaciones en tiempo real aumenta la exposición al fraude, lo que impulsa la necesidad de detección y bloqueo de fraudes en tiempo real.

Capacidad limitada para adaptar rápidamente las reglas comerciales a los nuevos esquemas de fraude. Altos falsos positivos.

Datos valiosos de los clientes en silos separados. Da como resultado enfoques de detección de fraude, estándares y recursos de gestión separados.

Falta de visión 360 del cliente para la prevención del fraude en todos los canales

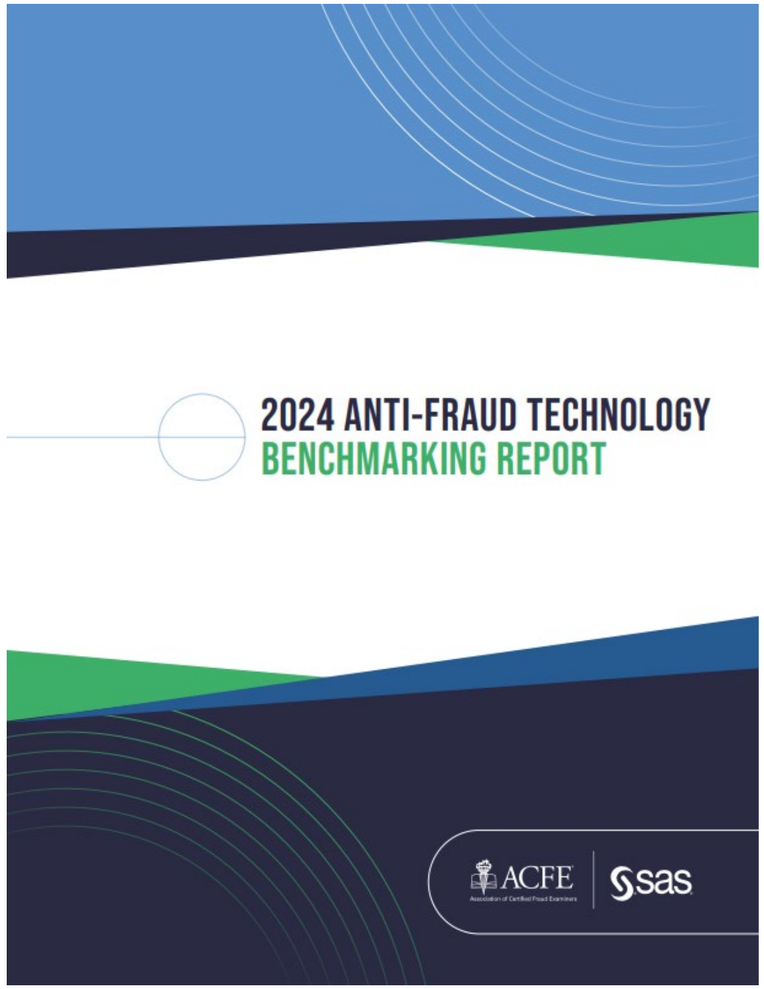


AGENDA

01 FRAUD PREVENTION

- .1 Trends
- .2 AI for Prevention
- .3 SAS vision

PRINCIPALES CONCLUSIONES



THE USE OF ARTIFICIAL INTELLIGENCE (AI) and MACHINE LEARNING
in anti-fraud programs is expected to nearly
TRIPLE
over the next two years.

83%
of organizations expect to implement
GENERATIVE AI
as part of their anti-fraud programs over the next two years.

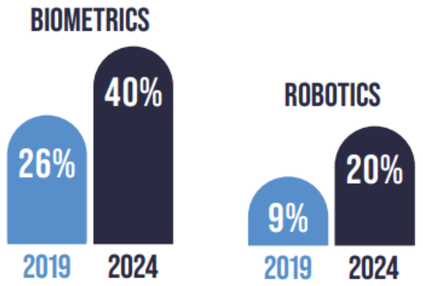
Nine in 10 organizations (91%) use
DATA ANALYSIS TECHNIQUES
as part of their anti-fraud programs.

91%

Two in five organizations (40%) currently use
PHYSICAL BIOMETRICS
as part of their anti-fraud program, and **another 17% expect to adopt this technology** in the next two years.

40% **17%**

The use of both
BIOMETRICS and ROBOTICS
in anti-fraud programs has steadily increased over the past few years.



A majority of organizations **(61%)** either currently contribute or are willing to **contribute to data consortiums** to aid their anti-fraud efforts.

61%
OF ORGANIZATIONS

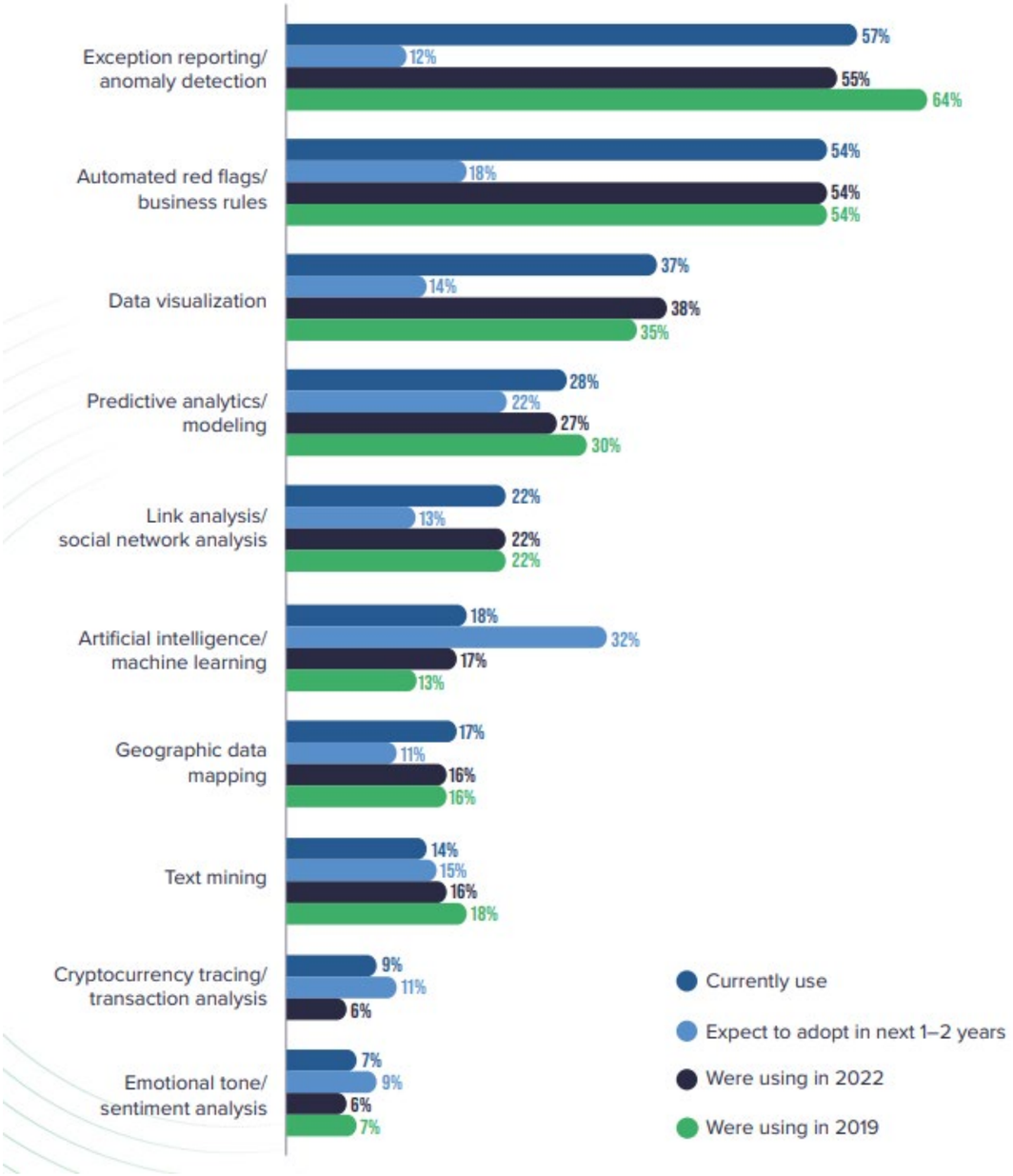
2024 ANTI-FRAUD TECHNOLOGY BENCHMARKING REPORT

THE USE OF ARTIFICIAL INTELLIGENCE and MACHINE LEARNING in anti-fraud programs is expected to nearly **TRIPLE** over the next two years.

3x

> **Automated red flags, machine learning, and predictive analytics can be useful these days due to the high volume of cyberattacks and the increased use of technology by criminals."**
>
> – Survey respondent

FIG. 1 What data analysis techniques do organizations use to fight fraud?



PERO, ¿CÓMO Y DÓNDE APLICAR LA IA EN LOS PAGOS DIGITALES?

En primer lugar, debes ampliar el análisis (no centrarte solo en la transacción en sí, sino en todo el contexto de la misma)

Dispositivo/ IPs

El cliente verifica su identidad

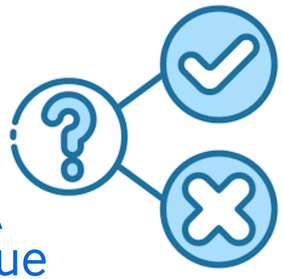
Banderas rojas Beneficiarios

Factores de riesgo no monetarios

Perfil de comportamiento del cliente

Transacción Monetaria

Evaluación del riesgo de fraude



RBA Enfoque basado en el riesgo

VISIÓN HOLÍSTICA

REGLAS DE NEGOCIO

ANÁLISIS DE DATOS

DATOS INTERNOS + EXTERNOS

REGLAS + MODELO

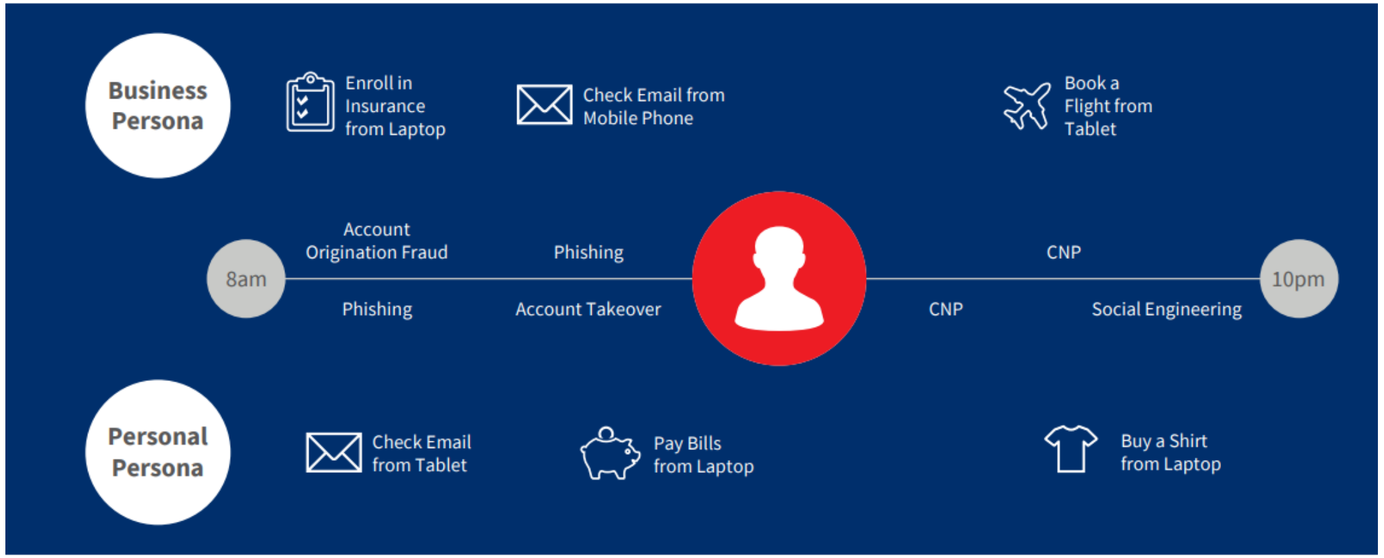
ANÁLISIS DE VINCULOS

IA/ML

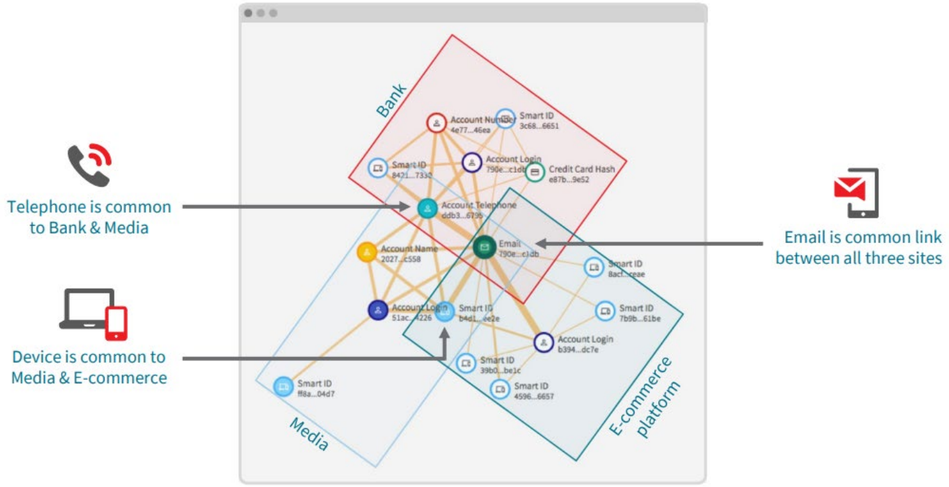
PERO, ¿CÓMO Y DÓNDE APLICAR LA IA EN LOS PAGOS DIGITALES?

1. IDENTIDAD/AUTENTICACIÓN DIGITAL

EVERY INDIVIDUAL HAS MULTIPLE PERSONAS, CREDENTIALS, DEVICES, LOCATIONS… BUT ONE GLOBAL DIGITAL IDENTITY



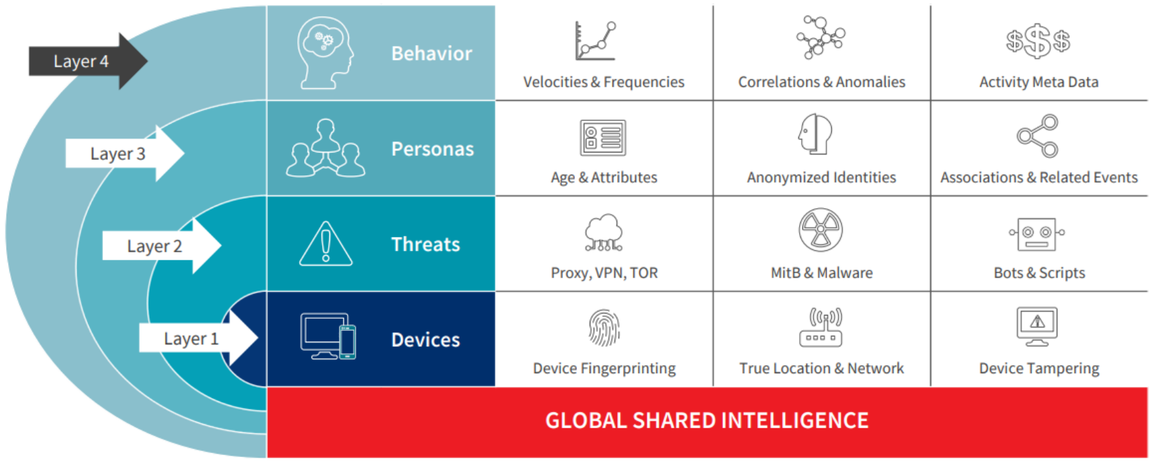
LexisNexis® RISK SOLUTIONS GROUP



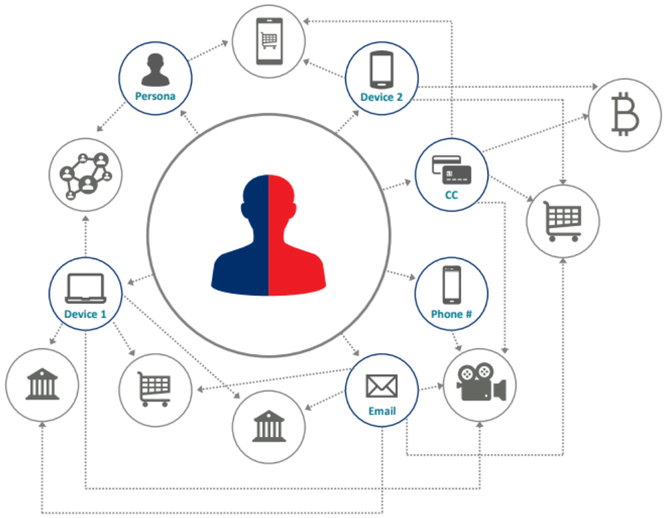
PERO, ¿CÓMO Y DÓNDE APLICAR LA IA EN LOS PAGOS DIGITALES?

1. IDENTIDAD/AUTENTICACIÓN DIGITAL

THREATMETRIX USES A LAYERED APPROACH FOR FRAUD DETECTION



UNDERSTAND YOUR DIGITAL USERS



Device Intelligence
- Web and mobile coverage
- Globally transferable
- 3 x unique identifiers

Location Analysis
- 10 unique location points
- Distance anomalies
- Proxy / VPN detection

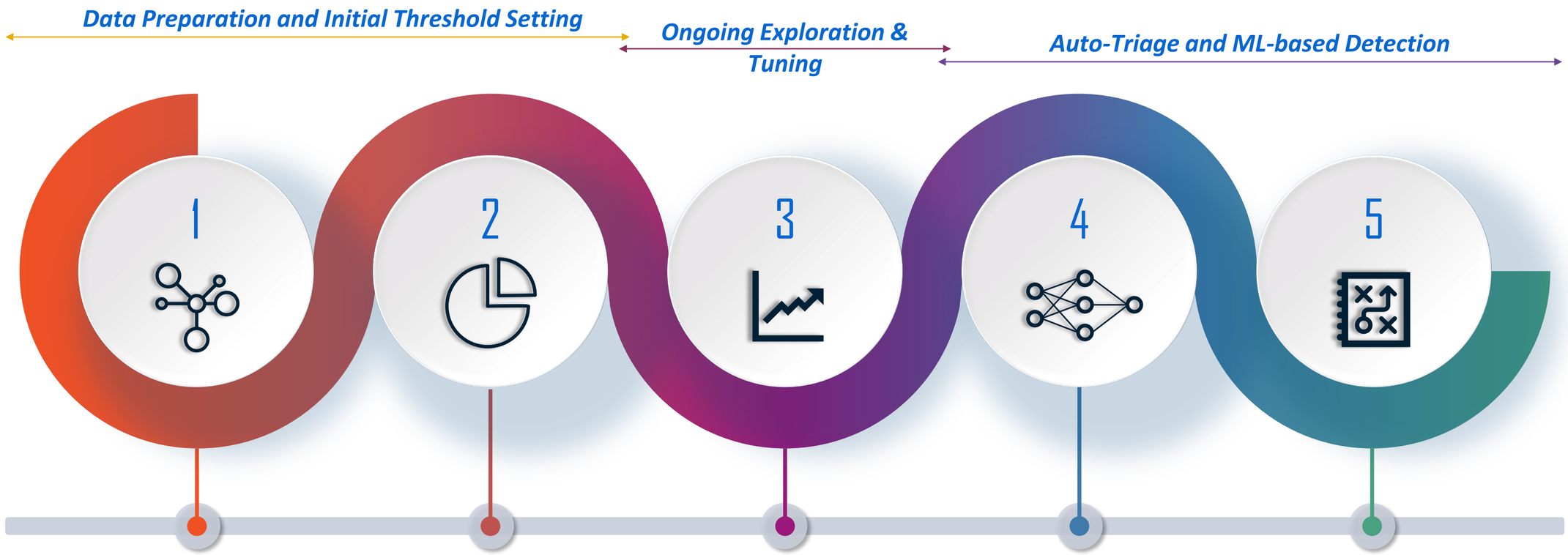
Behavioural Biometrics
- Rich data collection
- Keyboard, Mouse, Touch, Gyro
- 4 x model outputs

Shared Intelligence
- Crowd source design
- Single customer views
- Segregated industries

LexisNexis® RISK SOLUTIONS GROUP

PERO, ¿CÓMO Y DÓNDE APLICAR LA IA EN LOS PAGOS DIGITALES?

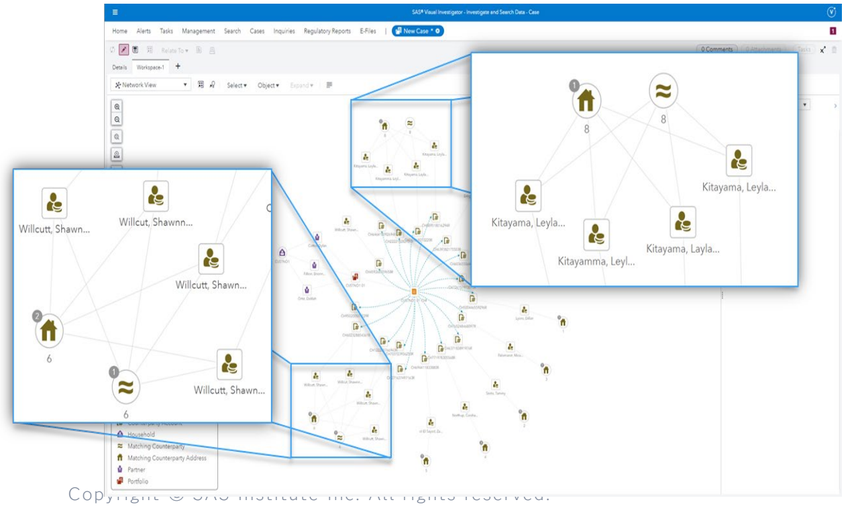
2. IA/ML EN LOS DATOS

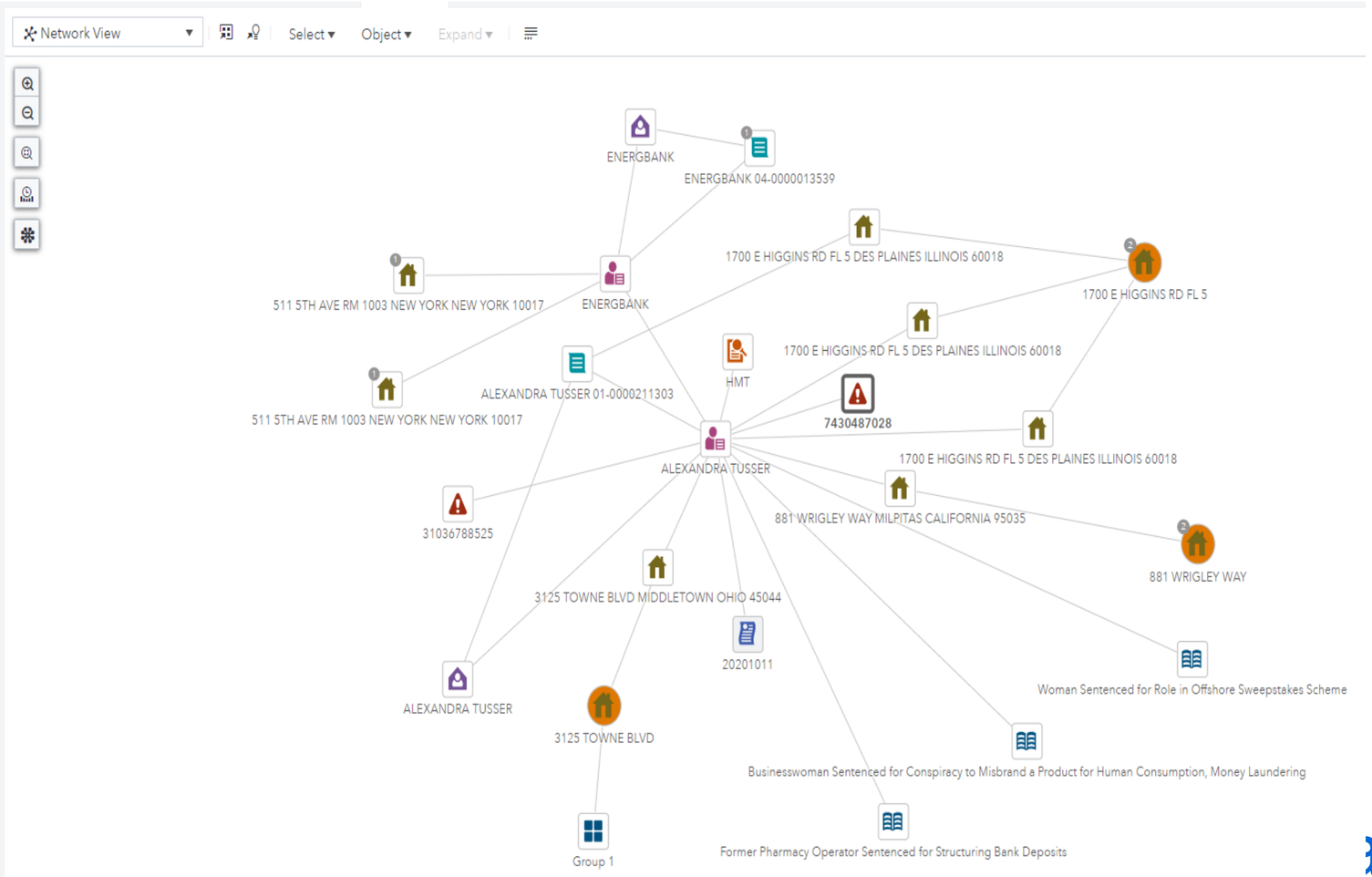


PERO, ¿CÓMO Y DÓNDE APLICAR LA IA EN LOS PAGOS DIGITALES?

2. IA/ML EN LOS DATOS

Resolución de entidades y análisis de redes

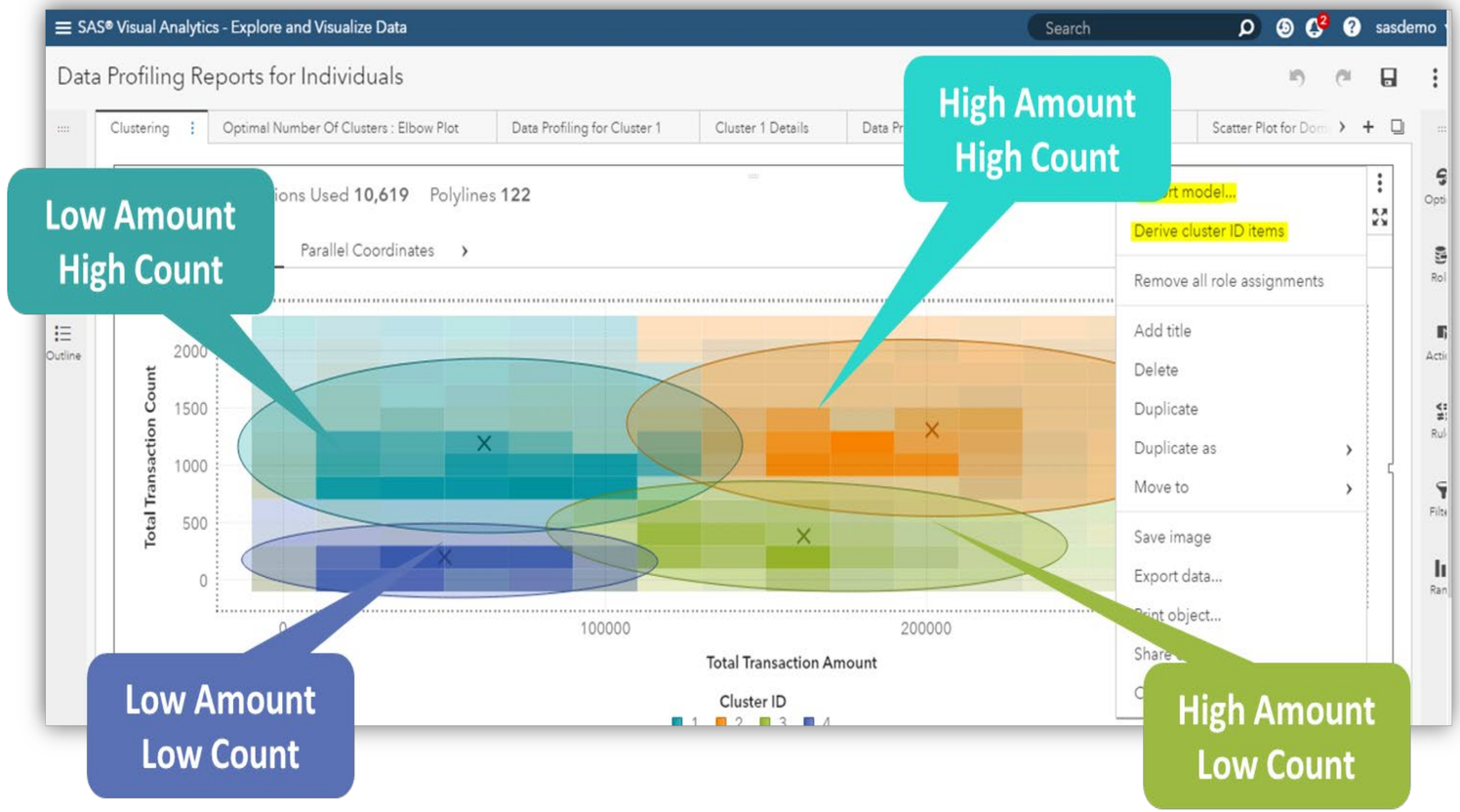


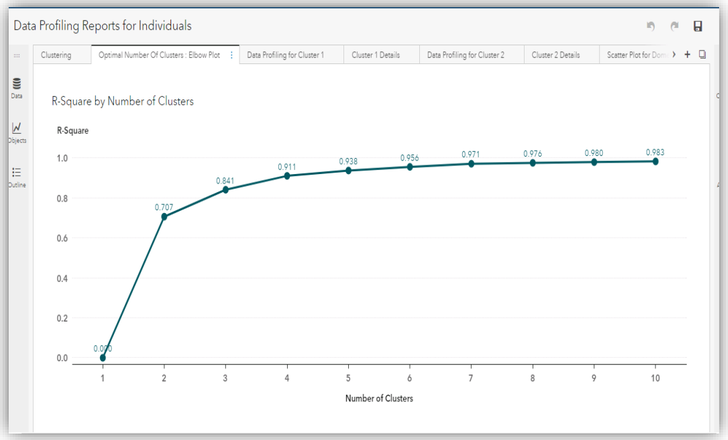


PERO, ¿CÓMO Y DÓNDE APLICAR LA IA EN LOS PAGOS DIGITALES?

2. IA/ML EN LOS DATOS

Segmentación de clientes



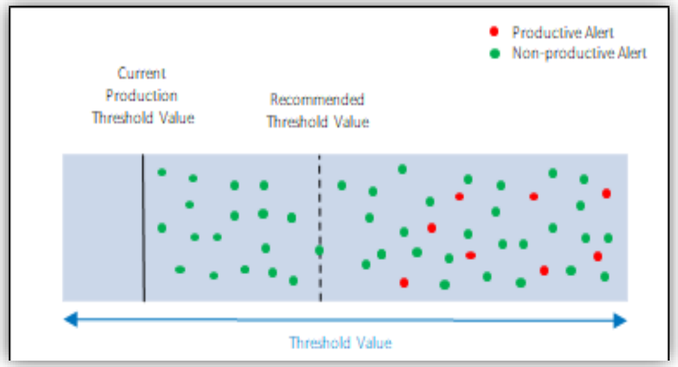


PERO, ¿CÓMO Y DÓNDE APLICAR LA IA EN LOS PAGOS DIGITALES?

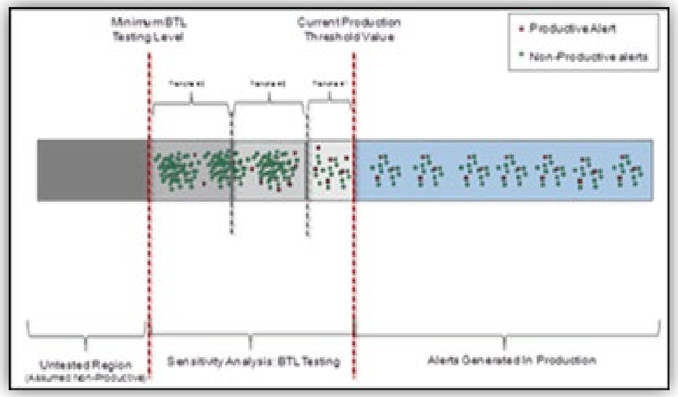
2. IA/ML EN LOS DATOS

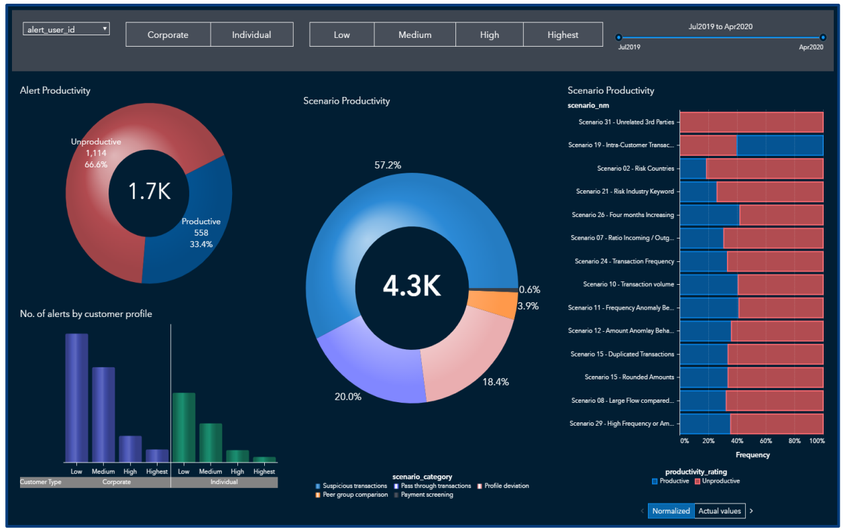
Ajuste de escenarios

Above the Line



Below the Line



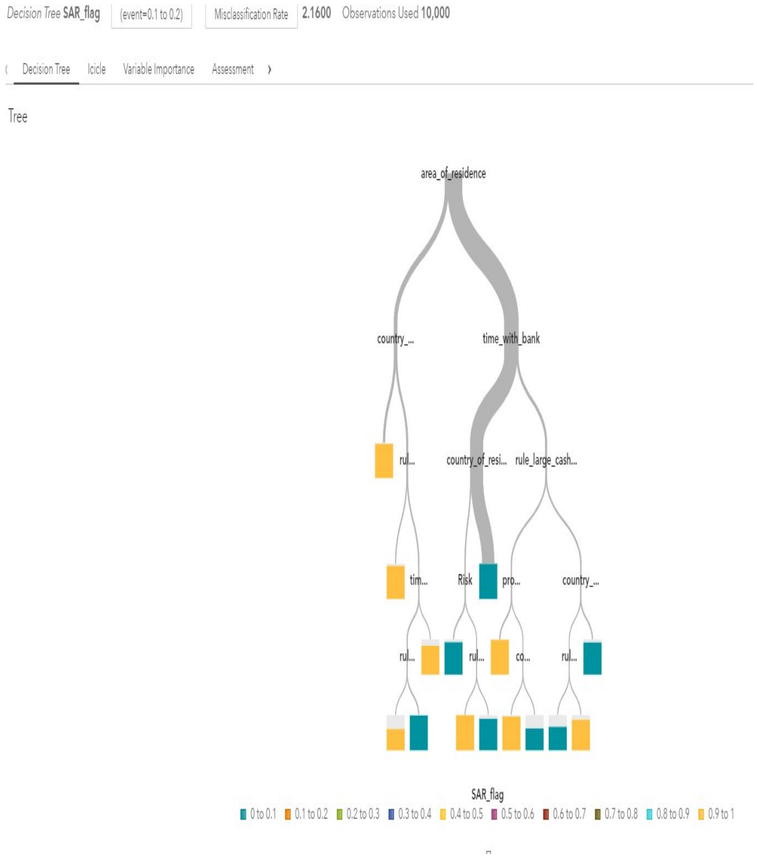


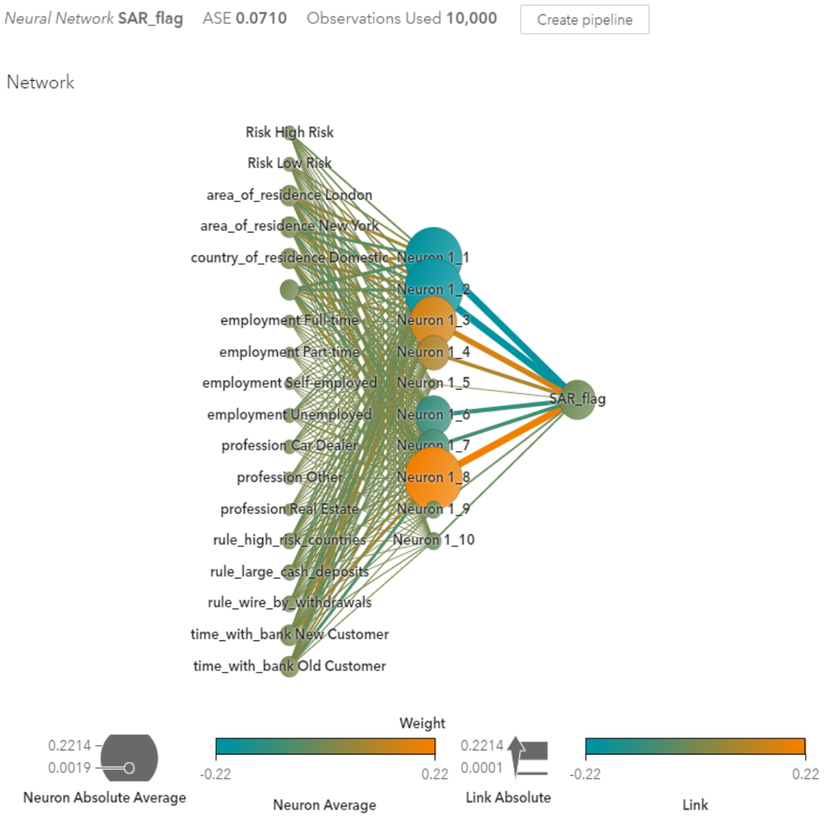
Iterative
Effectiveness Review

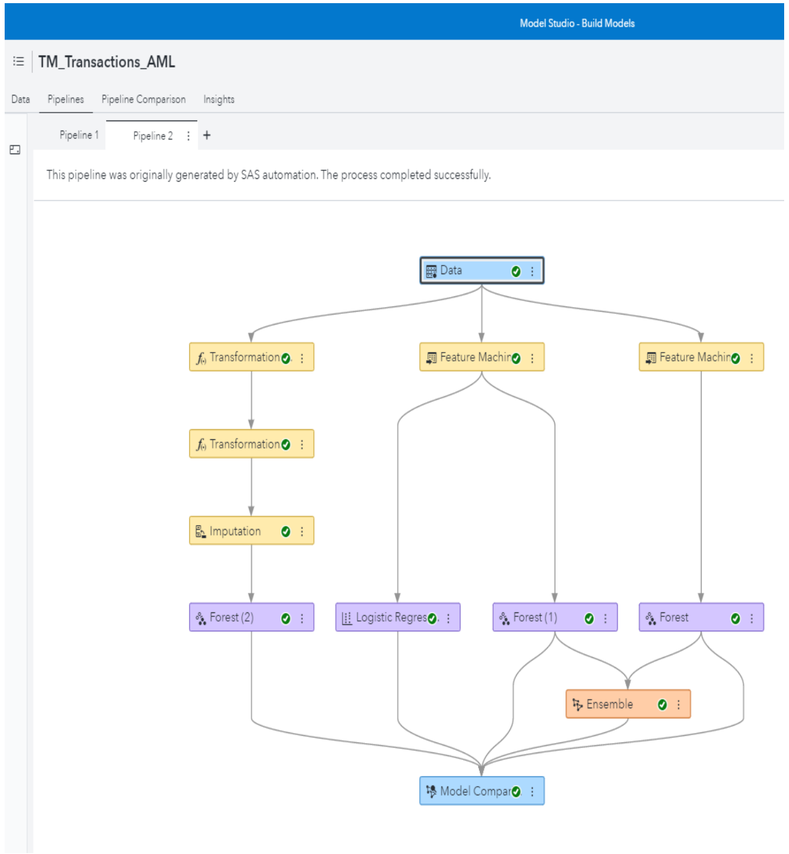
PERO, ¿CÓMO Y DÓNDE APLICAR LA IA EN LOS PAGOS DIGITALES?

2. IA/ML EN LOS DATOS

Priorización/hibernación de alertas







PERO, ¿CÓMO Y DÓNDE APLICAR LA IA EN LOS PAGOS DIGITALES?

2. IA/ML EN LOS DATOS

Escenarios basados en modelos

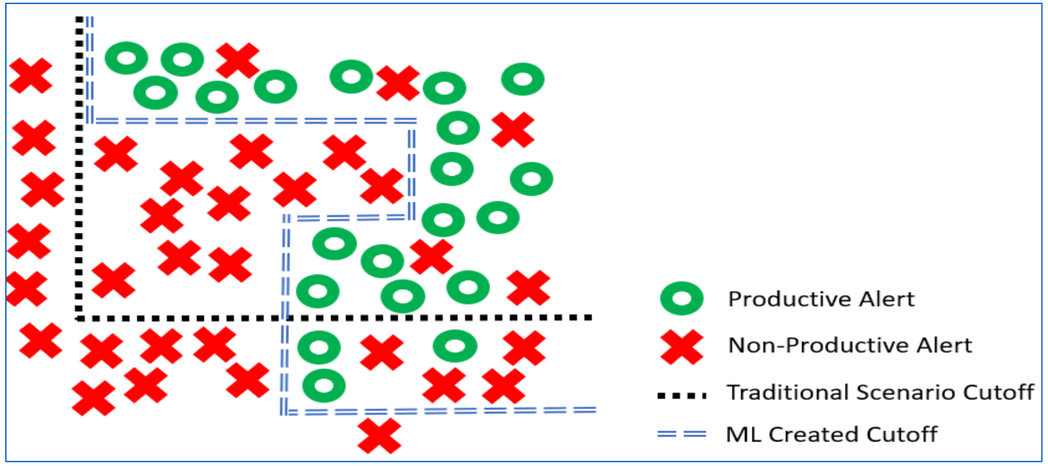
Traditional Rules

- Rules alone can create high false positives rates and potential for false negatives due the use of thresholds
- Rules take small number of parameters into consideration
- Many rules are needed to identify a complex Fraud typology

Machine Learning Models

- ✓ Models do not use thresholds and can detect behaviors more precisely, reducing Type I & Type II error
- ✓ Models can leverage 100's of features to detect financial crime
- ✓ Models can look at behavioral patterns, replacing many rules with one model to detect a typology of behavior

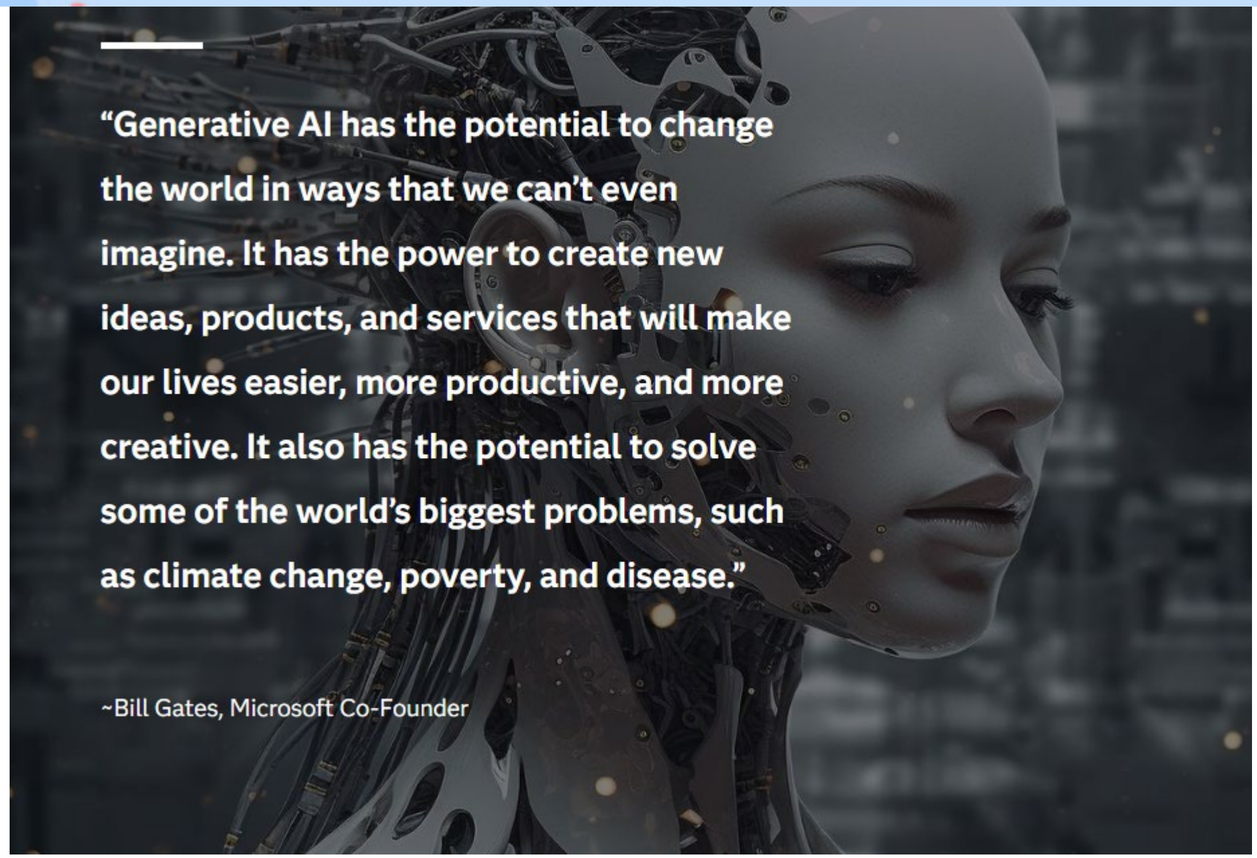
Si bien los modelos no reemplazarán todas las reglas, fortalecerán la capacidad de detectar actividades sospechosas y reducir los falsos positivos

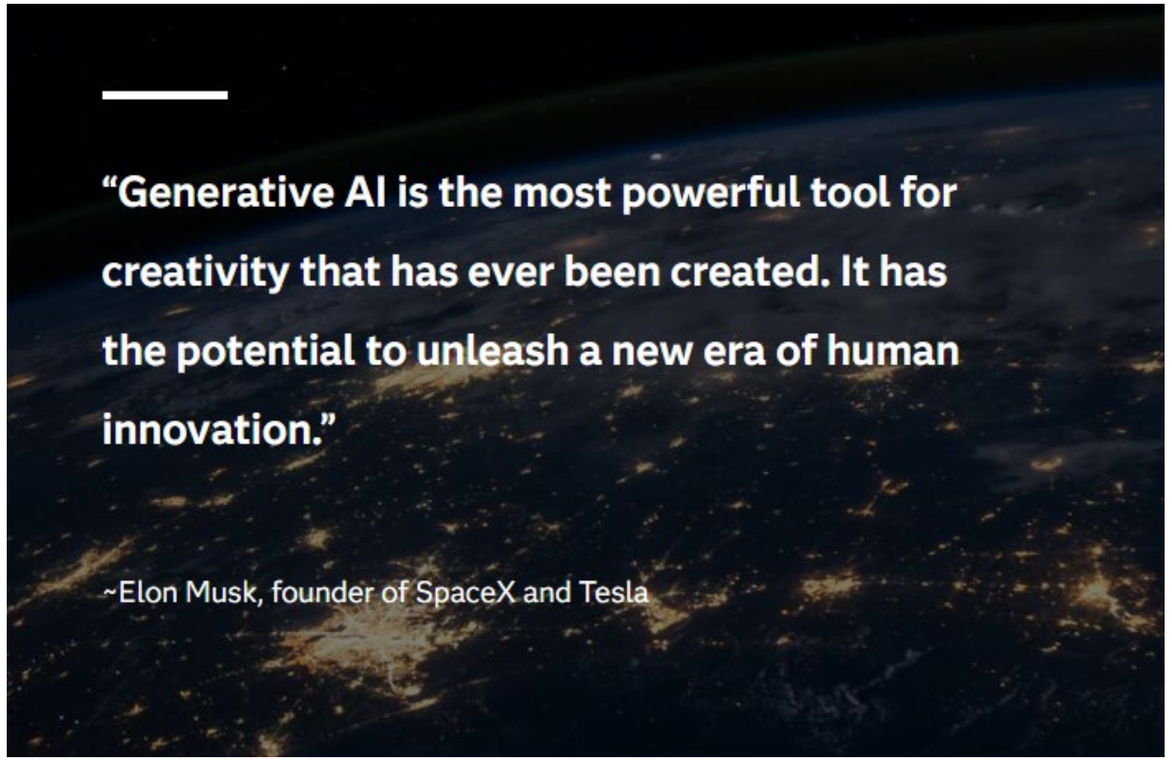


3. IA generativa

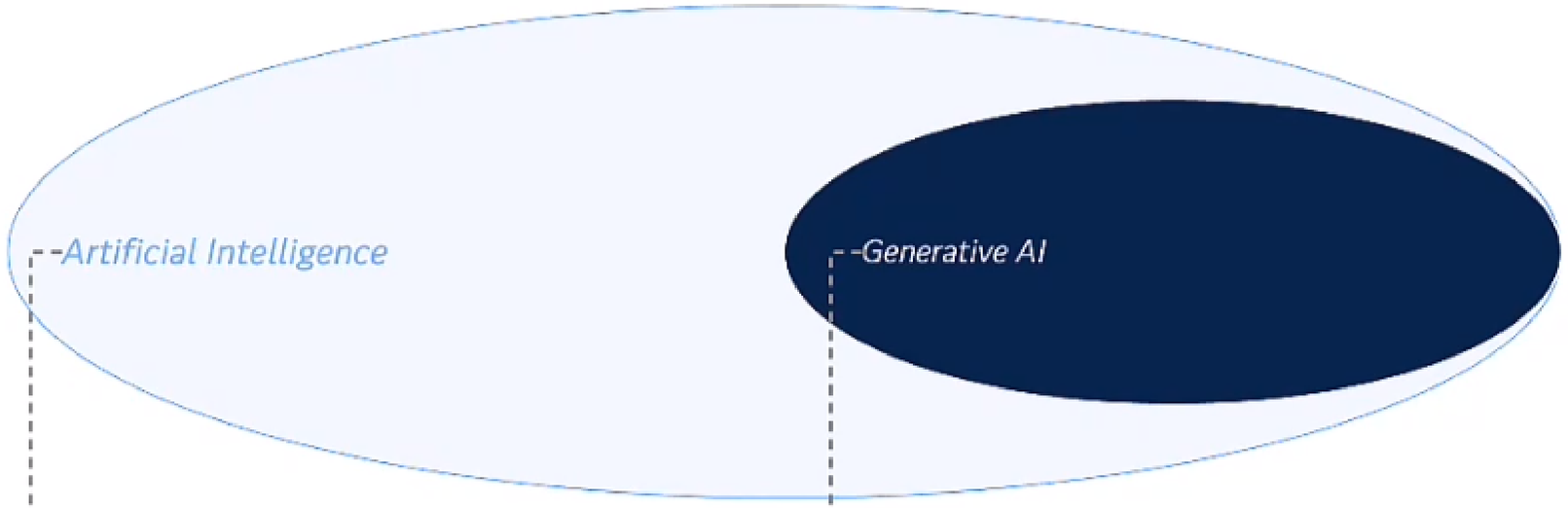
FRAUD ROUNTABLE

IA para la prevención del fraude en un mundo digital





The Economic Impact of Generative AI



$13 Trillion

Global Economic Potential

$4.4 Trillion

Global Economic potential

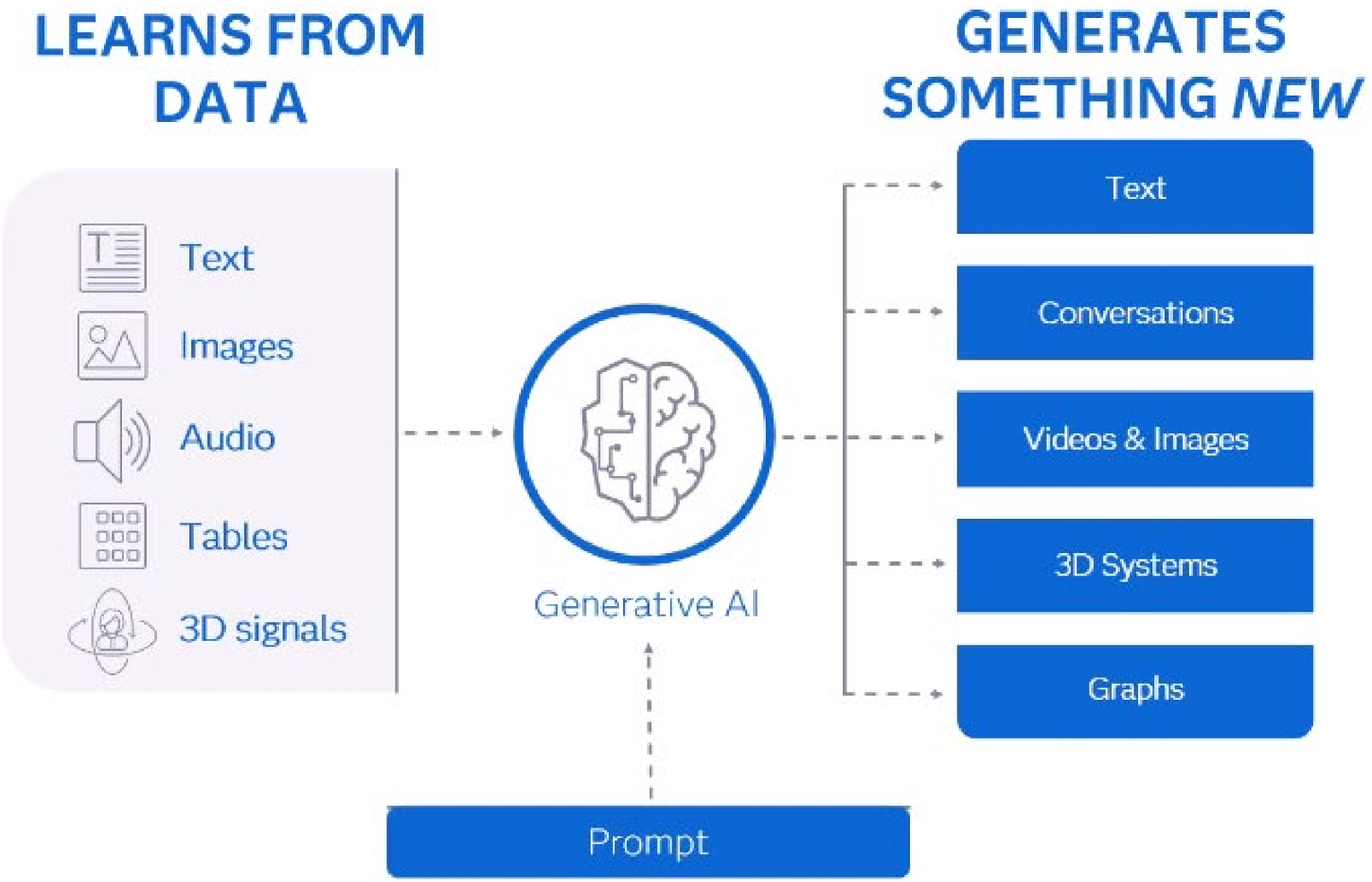
Almost 33% of the Global Economic Impact of AI will be driven by Generative AI

Source : McKinsey, The economic potential of AI, 2023

sas

Creating New Realities

Generative AI



Content Creation

Gen AI is really great at creating a first draft for emails, reports, or saving time on all sorts of writing tasks.

Language Translation

Use LLMs for quick language translation, facilitating communication with international clients and colleagues.

Task Automation

Use Gen AI to automate routine tasks such as data entry, file organization, or appointment scheduling.

Data Insights

Gen AI can derive insights by summarizing large data sets and complex reports.

Programming Assistance

Use LLMs for generating code snippets or aiding in programming tasks.

Customer Support

Use LLMs to personalize responses in customer communication.

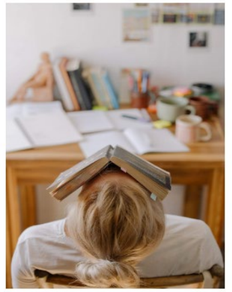
Problem Solving

Use Gen AI to analyze complex problems and propose potential solutions.

Idea Generation

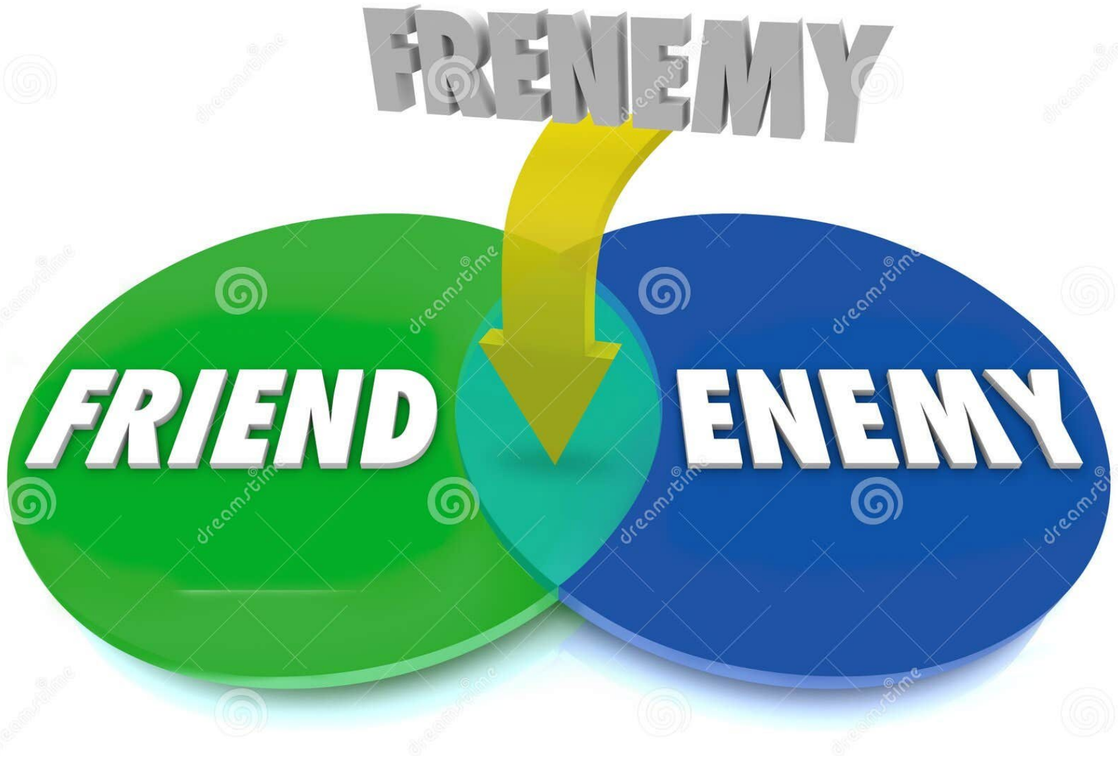
Use Gen AI to facilitate brainstorming sessions and idea generation, or to suggest edits and improvements to existing content and ideas.

Learning Enhancement



Seek advice from LLMs on specific topics, providing quick answers and explanations.

GenAI para el área de Prevención de Fraude



GenAI para el área de Prevención de Fraude

Para los MALOS

Bloomberg.com
Why Taylor Swift AI-Generated D...

The New York Times

[No, Taylor Swift no está vendiendo ollas Le Creuset]

El supuesto patrocinio de Swift a los productos de la empresa, que ha aparecido en anuncios publicados en Facebook y otros medios, es falso.

1 mês atrás

Infobae

Ciberdelicuentes usan inteligencia artificial para crear trampas más sofisticadas

Las estafas, el phishing y otras formas de manipulación humana representan más del 75% de todas lasamenazas digitales.

20 de set. de 2023

(CNN) -- Un trabajador financiero de una empresa multinacional fue engañado para que pagara US$ 25 millones de dólares a estafadores que utilizaban tecnología deepfake para hacerse pasar por el director financiero de la empresa en una videoconferencia, según la policía de Hong Kong. 4 de fev. de 2024

CNN
https://cnnespanol.cnn.com › 2024/02/04 › trabajador-...

Trabajador de finanzas paga US$ 25 millones después de ...

GenAI para el área de Prevención de Fraude

Para los MALOS

Challenges, Limitations, and Considerations

Accuracy

LLMs can produce output that is factually incorrect, not contextual or non-sensical.

Consider:

- Knowledge cutoff date
- Completion relies on context
- Hallucinations

Voices from the world

- New York lawyers sanctioned for using fake ChatGPT cases in legal brief

Privacy & Security

LLMs can be manipulated to obtain desired output.

For example:

- Stealing private information
- Deliberately provide false information
- Execute arbitrary code

- UK's National Cyber Security Centre warns over possible AI prompt injection attacks

Governance

LLMs can be released in non-standard ways across providers.

- High computational demand translates in high cost for using LLMs.
- Commercial models are subject to change in model behavior and policy

- McKinsey - estimated TCO for taker/shaper/maker archetypes
- OpenAI policy change reflects on Amazon posts

sas

APIS	GUIS	PROMPT INJECTION ATTACKS	PROMPT ENGINEERING

Prompt injection attacks typically refer to a type of security vulnerability or attack associated with natural language processing (NLP) models and language-based interfaces. These attacks involve manipulating the input or prompt given to a language model to generate unintended or malicious outputs.

In the context of models like third-generation Generative Pre-trained Transformer (GPT-3) or other chatbots and conversational agents, prompt injection attacks can be used to trick the model into producing inappropriate, biased, or harmful responses. Attackers may craft input prompts in a way that exploits the model's vulnerabilities or biases, leading to outputs that could be abused or misused.

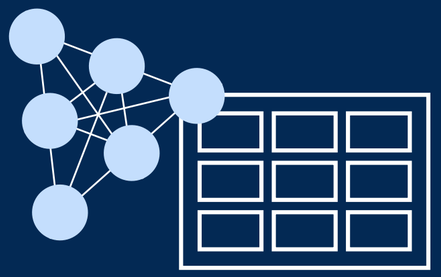
GenAI para el área de Prevención de Fraude

Por el BIEN

SAS& Generative AI

IA generativa

GENERACIÓN DE DATOS SINTÉTICOS



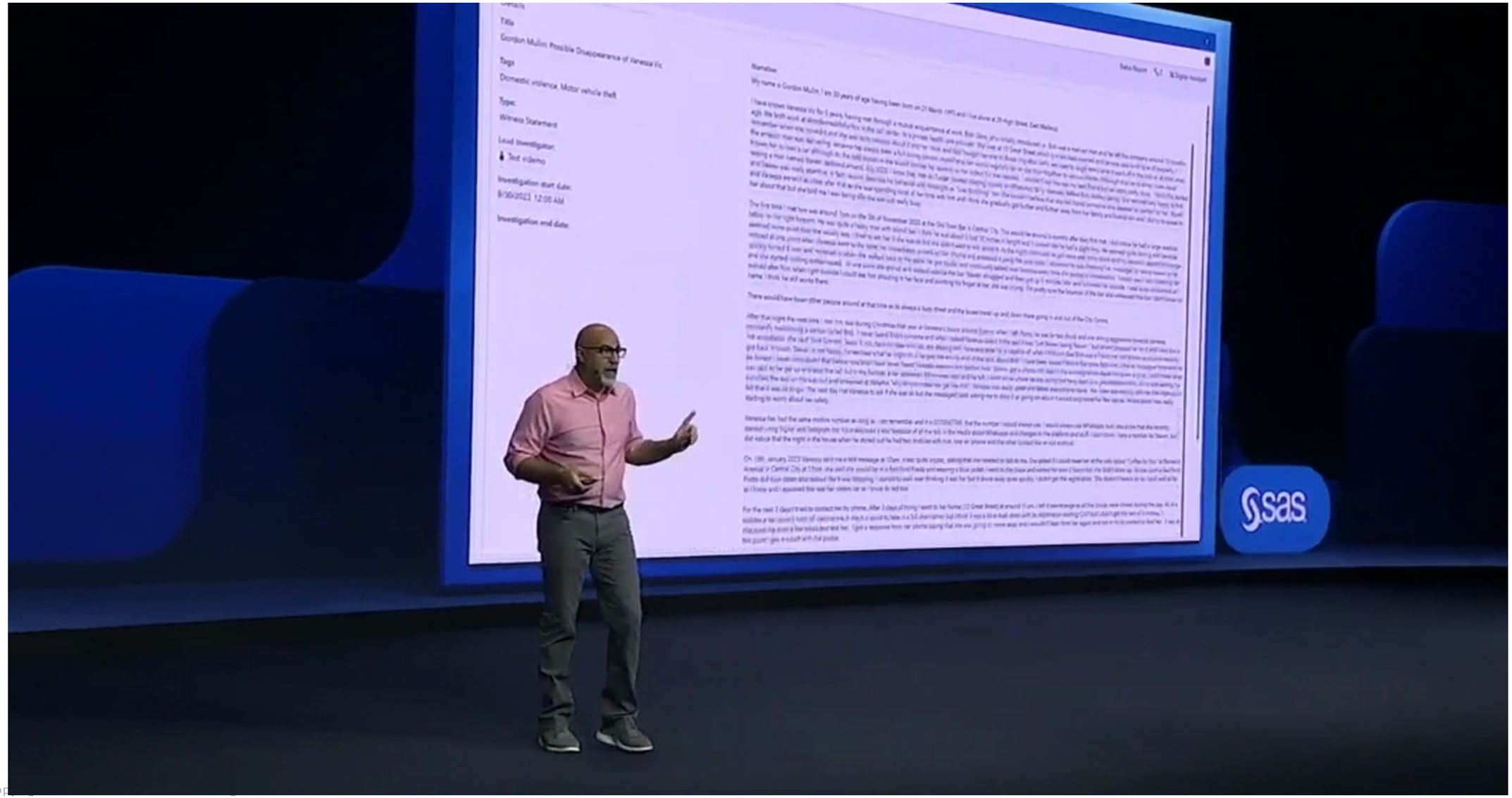
GEMELOS DIGITALES

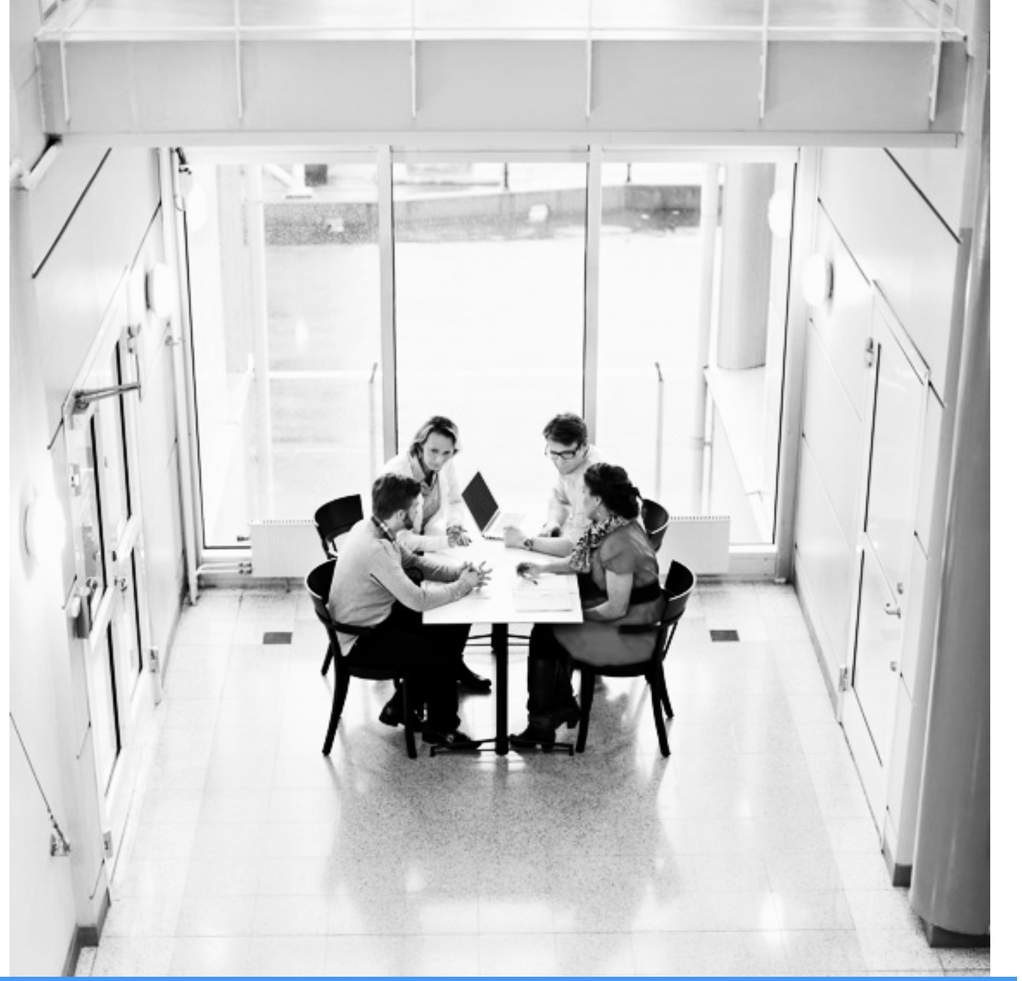
MODELOS DE LENGUAJE DE GRAN TAMAÑO

- CO-PILOTAS
- ASISTENTES INTELIGENTES

GenAI for the Fraud Prevention area

Por el BIEN





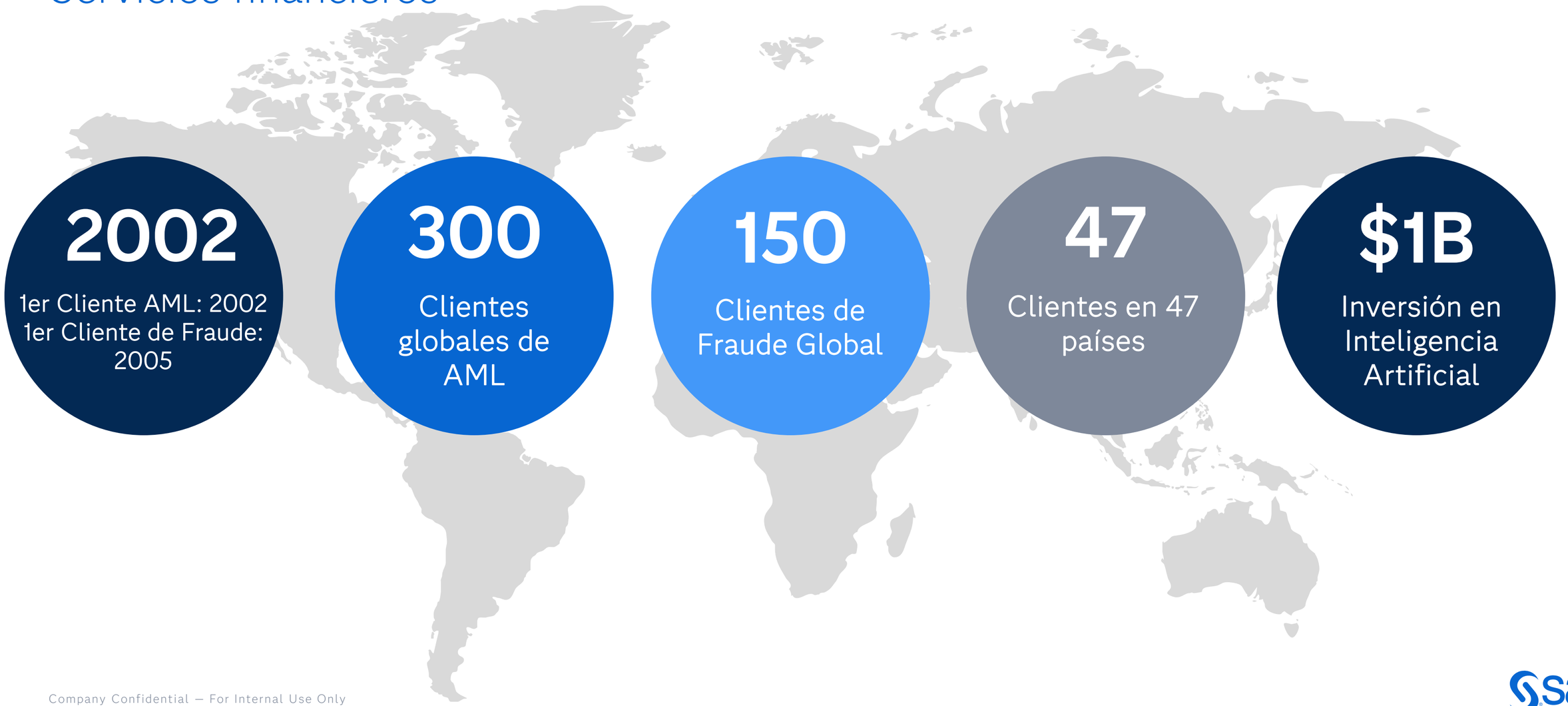
AGENDA

01 FRAUD PREVENTION

- .1 Trends
- .2 AI for Prevention
- .3 SAS vision

Fraude y Delitos Financieros

Servicios financieros



2002

1er Cliente AML: 2002
1er Cliente de Fraude: 2005

300

Clientes globales de AML

150

Clientes de Fraude Global

47

Clientes en 47 países

$1B

Inversión en Inteligencia Artificial

SAS es líder en prevención de delitos financieros

Prevención de Lavado de Dinero

SAS es líder en la ola™ de Forrester: soluciones contra el lavado de dinero, 3.º trimestre de 2022

SAS es líder en el cuadrante® Chartis RiskTech para soluciones AML basadas en el comercio 2022

SAS es líder en el cuadrante® Chartis RiskTech para soluciones KYC, 2023

Gestión de listas de seguimiento

SAS es líder en el cuadrante® de Chartis RiskTech para soluciones de monitoreo de listas de seguimiento, 2022

SAS es líder en el cuadrante® de Chartis RiskTech para soluciones de filtrado de transacciones, 2022

Gestión del fraude

SAS es líder en el cuadrante® de Chartis RiskTech para soluciones FRAML, 2023

SAS es líder en el cuadrante® de Chartis RiskTech para soluciones de fraude empresarial, 2023

SAS es líder en la matriz™ SPARK: Enterprise Fraud Management (EFM), 2022

Ciencia de datos

SAS es líder en la matriz de Aite: Principales plataformas de aprendizaje automático contra el fraude y la lucha contra el blanqueo de capitales, 2021

SAS es líder en el cuadrante® Chartis RiskTech para soluciones de gestión y análisis de entidades, 2022

SAS es líder en la evaluación de proveedores de IDC MarketScape: Worldwide Responsible Artificial Intelligence for Integrated Financial Crime Management Platforms, 2022

Lo que ofrece SAS

SAS proporciona detección y prevención integral del fraude en los pagos en una única plataforma tecnológica que integra datos de múltiples líneas de negocio y canales con analítica 100% en tiempo real.

Con SAS, puede...

- Descubra nuevos y complejos esquemas de fraude con rapidez.
- Reduzca los falsos positivos y mejore la experiencia del cliente.
- Optimice la toma de decisiones con una visión holística del riesgo de fraude.
- Adáptese fácilmente a los cambios con opciones flexibles de implementación e integración.

Como SAS puede apoyar

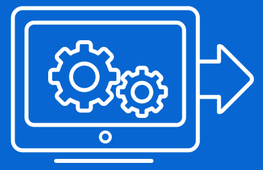
PLATAFORMA END-TO-END

INTEGRACIÓN

Orquestación
Multi-Canal
Multi-Producto
360º

- Datos internos/externos
- Datos mon / no mon

ANALÍTICA AVANZADA



Inteligencia
Reglas, Modelos,
Comportamientos

- Signatures
- User Variables

MONITORIZACIÓN

Interfaz de Investigación
Controles y flexibilidad

- Enfoque basado en el riesgo

GOBERNANZA

Controles
Gestión centralizada de registros y permisos

- Control de acceso
- Alertas de gestión

OPERACIONALIZACIÓN

Automatización
Decisiones automatizadas

- Bloqueos automáticos
- Envío de mensajes/OTP

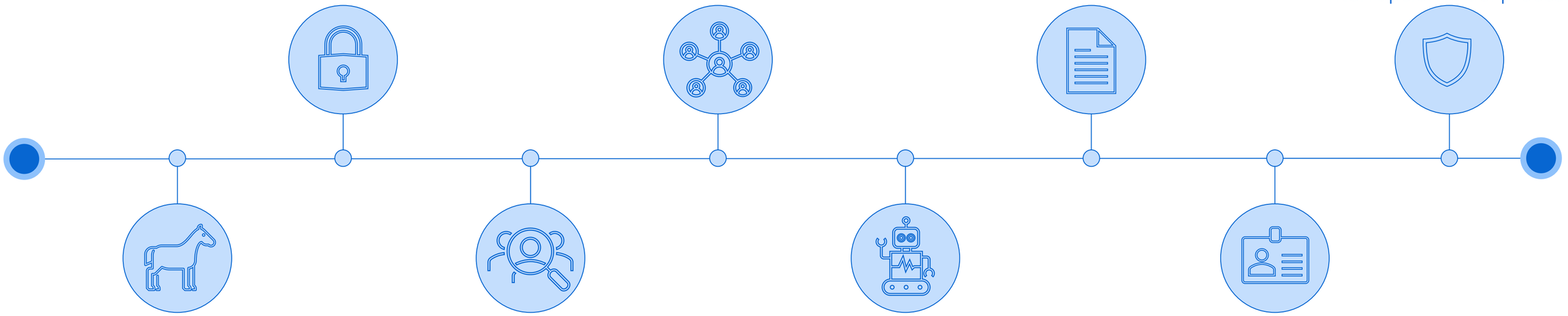
¿Qué puede detectar SAS?

Toma de control de la cuenta
Pagos no iniciados por el pagador, donde el comportamiento y la información del beneficiario son anómalos

Crimen Organizado
Combinación y relación de múltiples cuentas que trabajan juntas para articular actividades delictivas

Fraude en la solicitud
Nuevas cuentas creadas por los estafadores para que sirvan como instrumento para mover dinero

Fraude interno
Esquemas en los que están involucradas personas con información privilegiada dentro de la organización. Esto incluye: abuso de crédito, robo de dinero e interrupciones del proceso

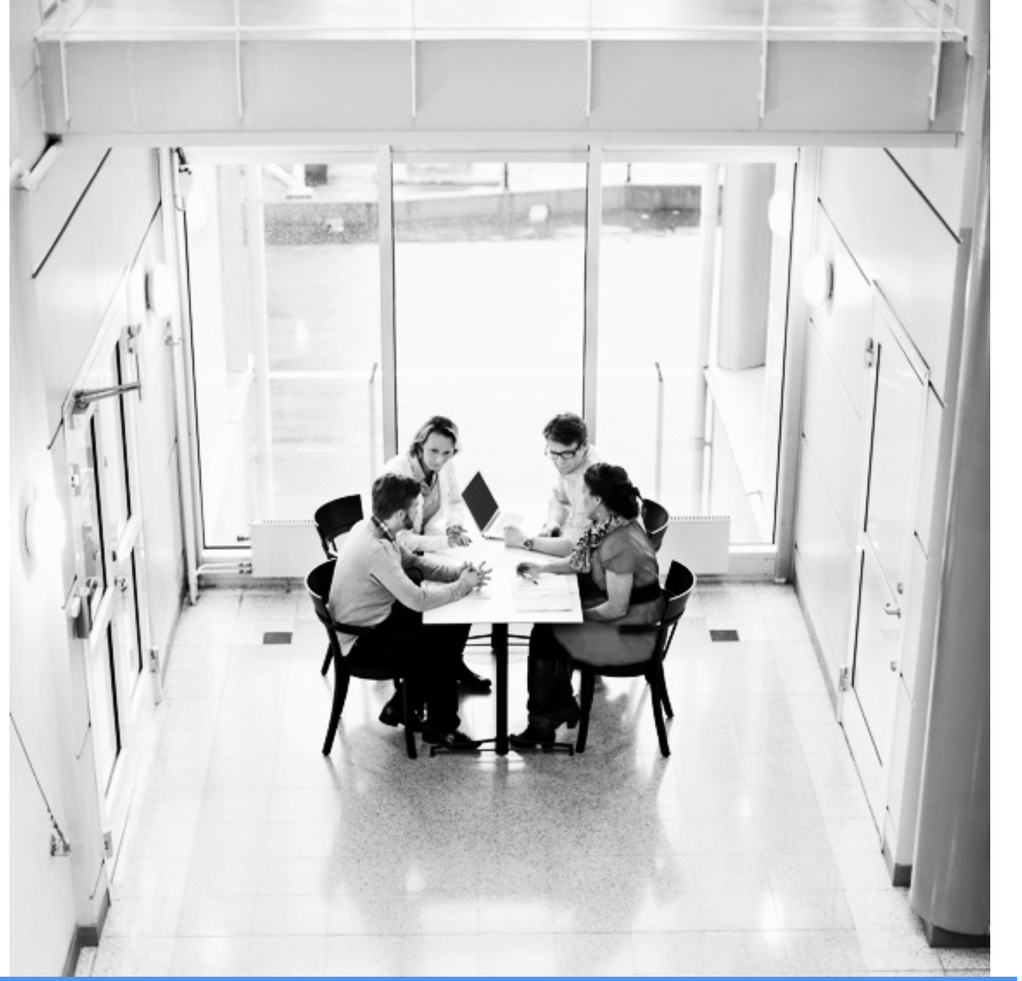


Cuentas de mulas
Cuentas de beneficiarios creadas o utilizadas con el propósito solemne de recibir dinero para actividades delictivas

Pagos Push Autorizados
Pagos iniciados por el cliente real que está siendo engañado para realizar un pago por estafas

Ataques de bots
Pagos automatizados realizados por bots a alta velocidad

Fraude de identidad
Validación de identidad para pagadores y solicitantes



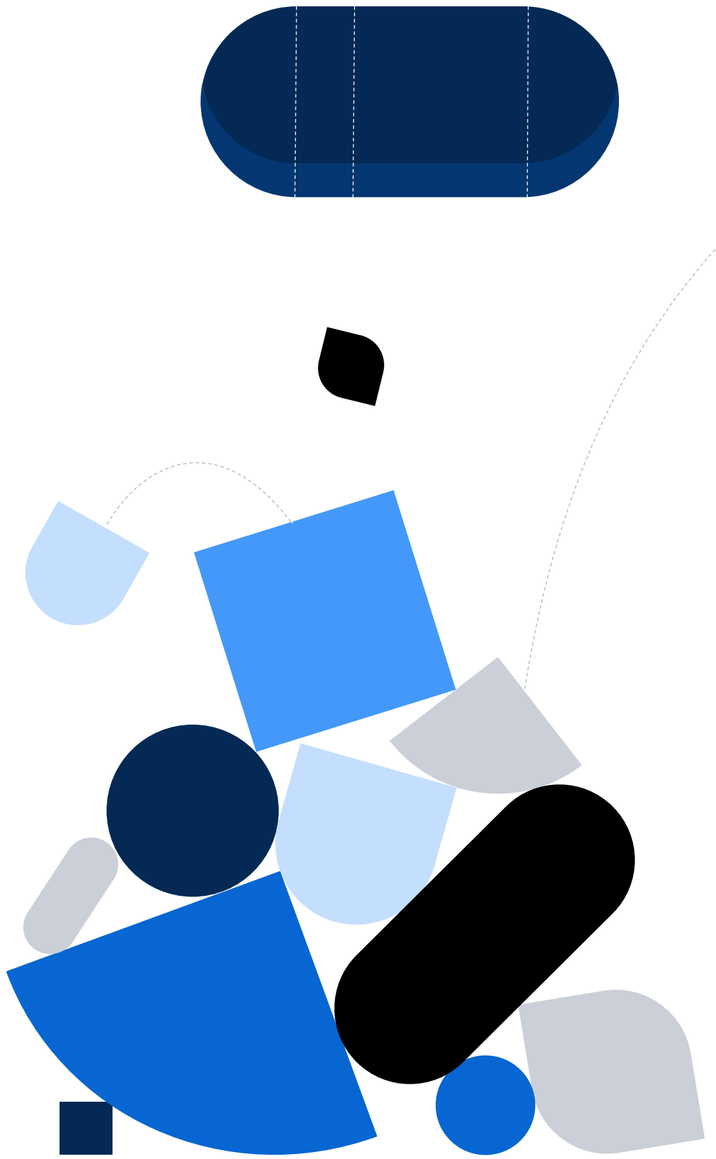
AGENDA

FRAUD ROUNTABLE

IA para la prevención del fraude
en un mundo digital

02 AML – ANTI MONEY LAUNDERING

- .1 TENDENCIAS
- .2 SANCIONES
- .3 VISION DE SAS



Challenges

New Complex Priorities

Focus on identification of complex predicate crimes such as Corruption, Cybercrime/Virtual Currencies, Terrorism, Fraud, Human Trafficking, Drug Trafficking, Wildlife Trafficking, etc.

AI / ML Adoption

Regulatory agencies are encouraging the use of AI/machine learning to improve the quality of regulatory reports being filed to governments.

Operations / Staffing

AML organizations have trimmed staff in recent years in anticipation of challenging economies. “Do more with less” through automation.

Data and Model Governance

Institutions must be able to document, explain and defend strategies to auditors and regulators. “Why did or didn’t you file a SAR/STR on this activity”?

Cloud Architectures

IT organizations desire a more agile, open and resilient manner for maintaining currency with technology and managing the risk of security vulnerabilities.

Increasing regulatory expectations with a focus on complex risks

Énfasis en riesgos complejos

Trafico Humano

Crimines medio ambiente

Trafico de animales

Corrupción / Cleptocracia

Lavado de dinero basado en el comercio (TBML)

Organizaciones Criminales Transnacionales

Crypto Moneda

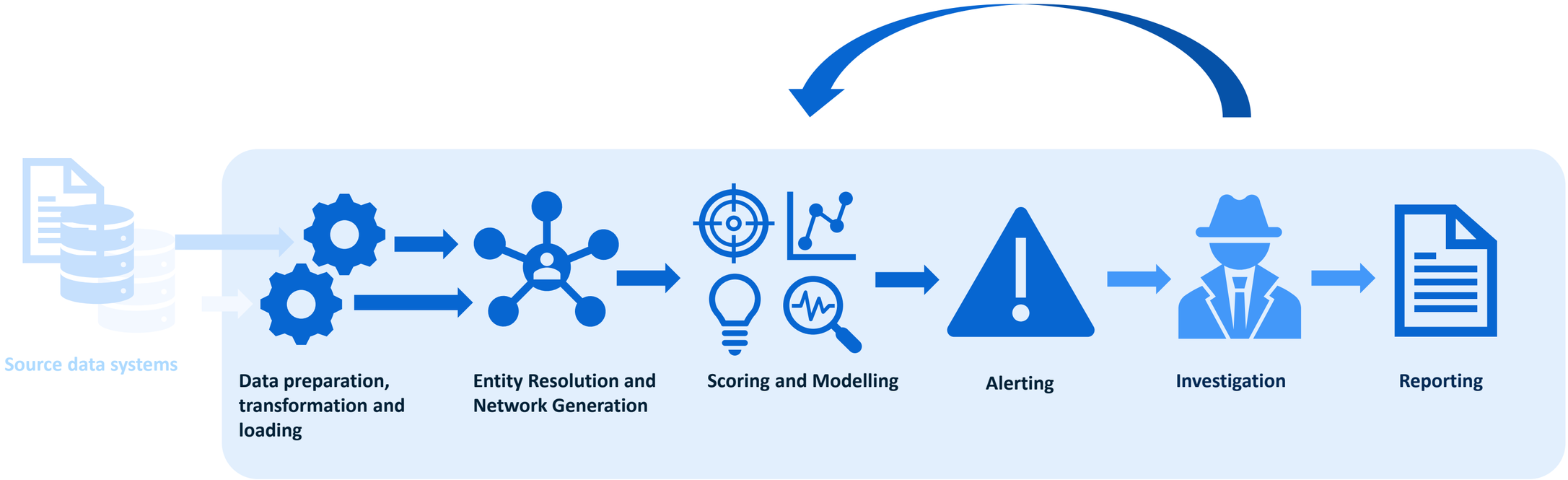
SAS® Anti-Money Laundering

What SAS Offers

SAS delivers a comprehensive compliance solution on a cloud native platform to help financial institutions stay ahead of emerging threats and changing regulations while improving operational efficiency.

SAS® Anti-Money Laundering

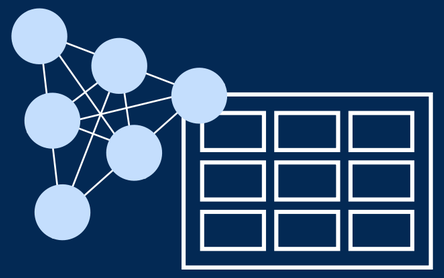
Solution Overview



GenAI para el área de PLD

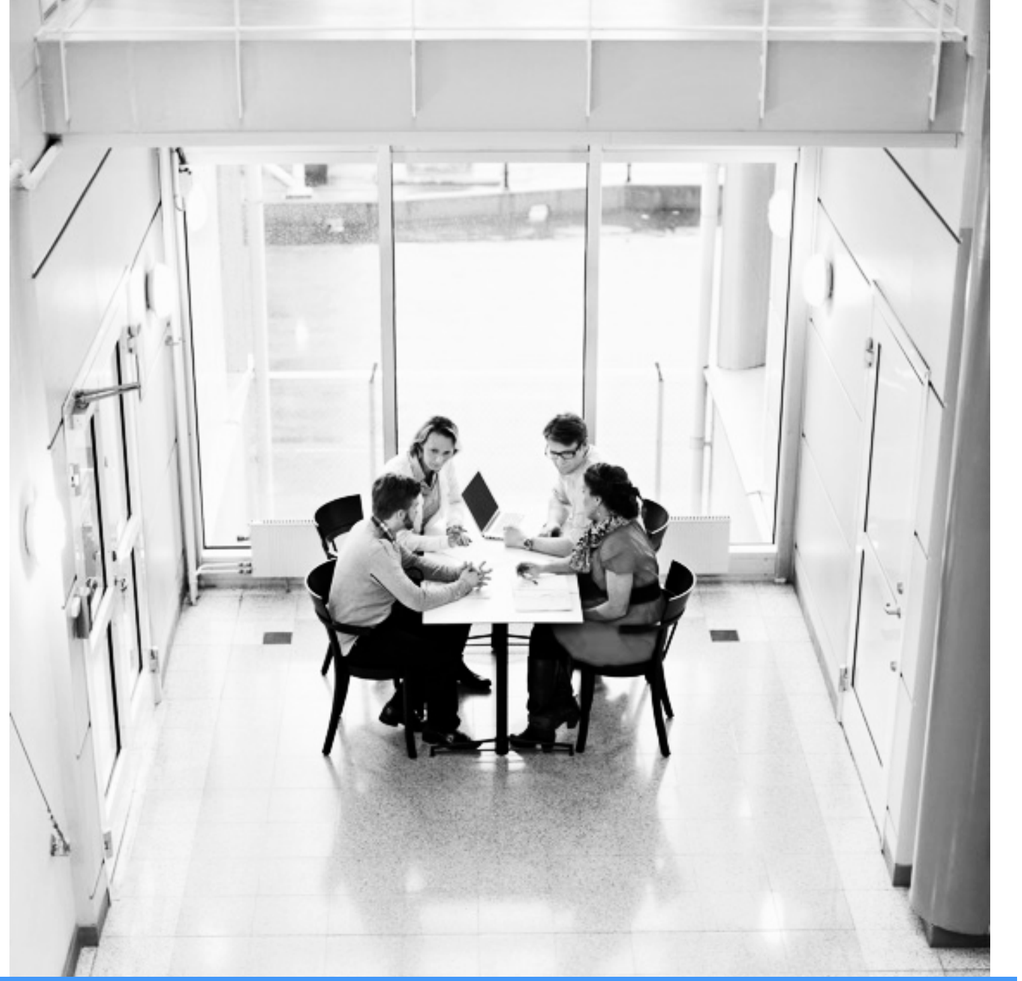
IA generativa

GENERACIÓN DE DATOS SINTÉTICOS



GEMELOS DIGITALES

MODELOS DE LENGUAJE DE GRAN TAMAÑO



AGENDA

FRAUD ROUNTABLE

IA para la prevención del fraude
en un mundo digital

02 AML – ANTI MONEY LAUNDERING

- .1 TENDENCIAS
- .2 SANCIONES
- .3 VISION DE SAS

Sanciones

Retos y tendencias claves en nuestro enfoque

ESCALABILIDAD

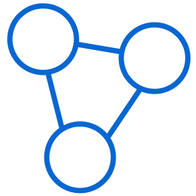
Volúmenes crecientes
Inestabilidad geopolítica
Ritmo regulatorio rápido
Falta de flexibilidad

CLOUD COMPUTING

EFICIENCIA

Altas tasas de alertas
Requisitos de recursos
Costos operativos

MATCHING HOLÍSTICO



EXPLICABILIDAD

Modelos sin transparencia
Necesidad de demostrar
comprensión del sistema.

MODELOS GLASS BOX

ESCALABILIDAD
Volúmenes crecientes
Inestabilidad geopolítica
Ritmo regulatorio rápido
Falta de flexibilidad

CLOUD COMPUTING

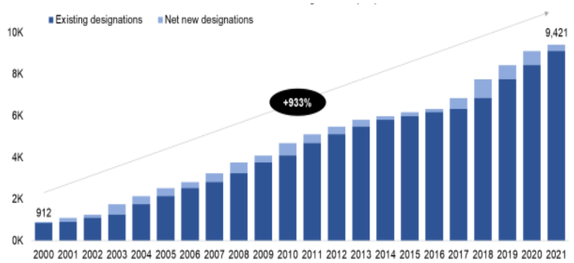
Es necesario ser escalable

Procesamiento hacia la nube

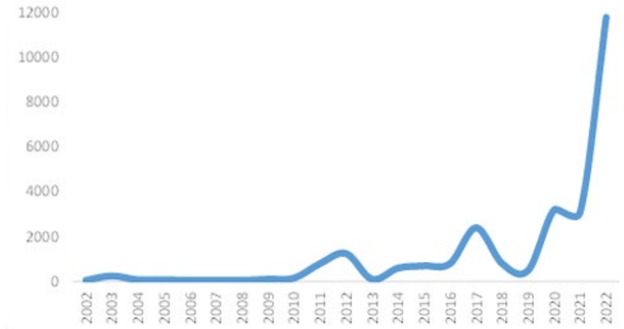
- Crecimiento muy rápido en volúmenes:

Designaciones OFAC

+933%



Nuevas Designaciones UE



- **Mayor complejidad** : Nuevos tipos de sanciones, nuevas medidas de control de exportaciones y elusión de sanciones.
- **Mayor velocidad**: Aceleración continua (p.ej. **11** rondas de sanciones de la UE desde la invasión de Ucrania)
- **Mayor flexibilidad** : Necesidad de una capacidad completa e instantánea de configuración por parte del usuario final para adaptarse a la situación cambiante.
- **Mejor servicio**: los ciclos de lanzamiento/implementación/prueba deben ser extremadamente más rápidos

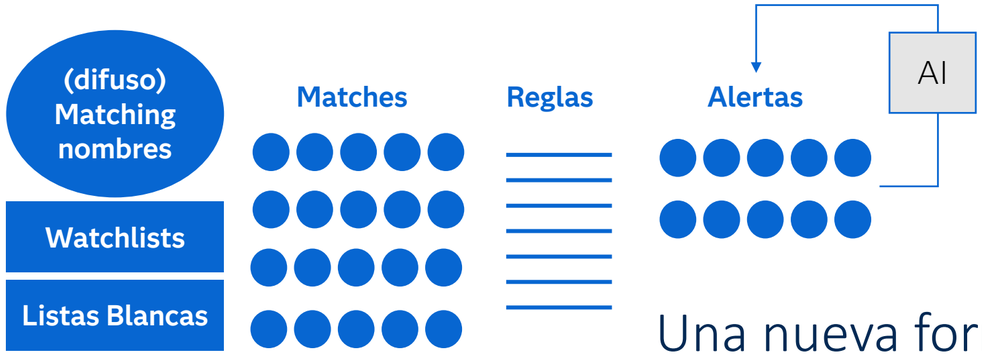
- Hacia computación en la nube para disponer de escalabilidad ilimitada
  - Mayor seguridad
  - Actualizaciones centralizadas
  - Ciclo de lanzamiento ágil
  - Altamente disponible
  - Almacenamiento ≠ procesamiento

Es necesario ser eficiente

EFICIENCIA
Altas tasas de alertas
Requisitos de recursos
Costos operativos

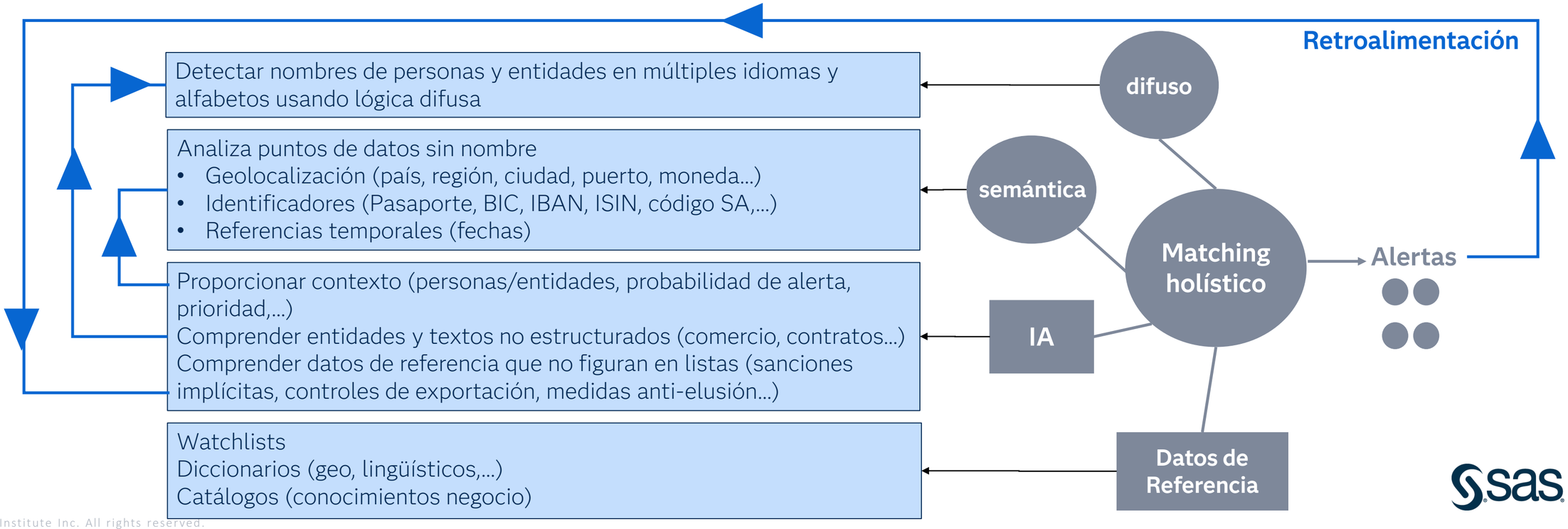
MATCHING HOLÍSTICO

Modelo Legacy (2001-)



Una nueva forma de monitorizar sanciones

Modelo holístico (2020-)

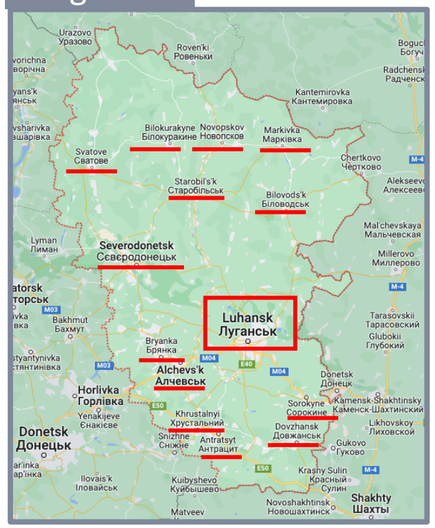


Es necesario ser eficiente

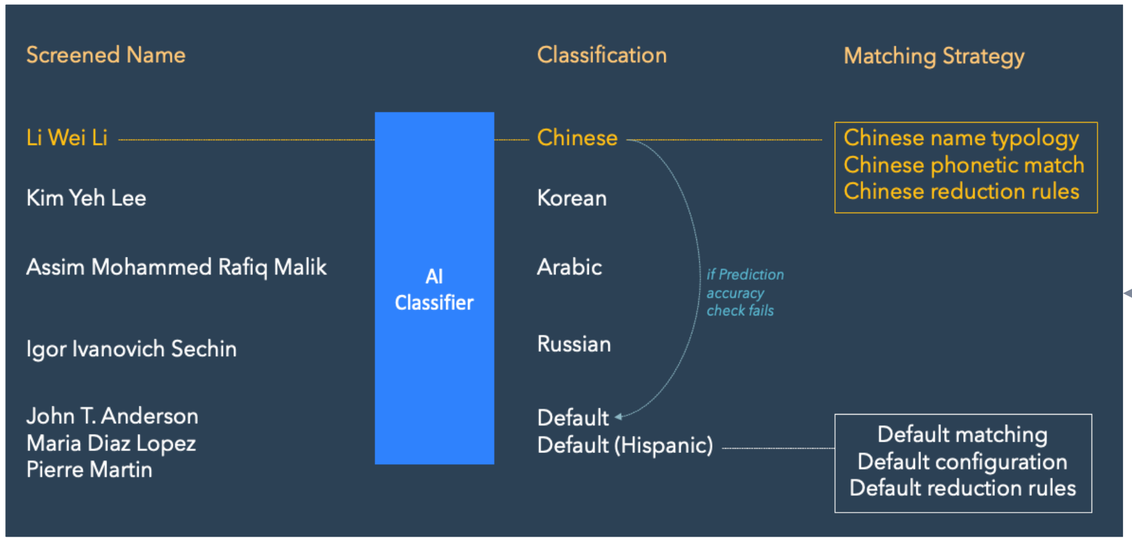
EFICIENCIA
Altas tasas de alertas
Requisitos de recursos
Costos operativos

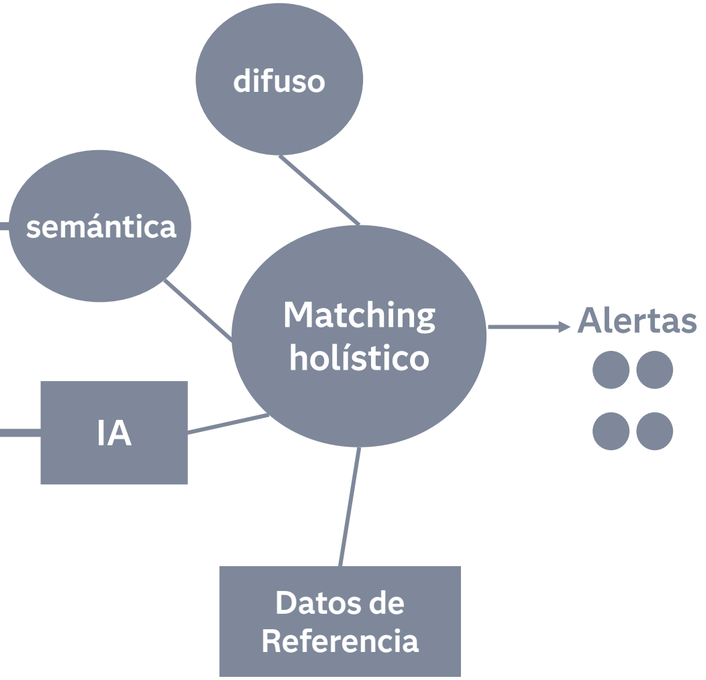
MATCHING HOLÍSTICO

Regiones



Ciudades





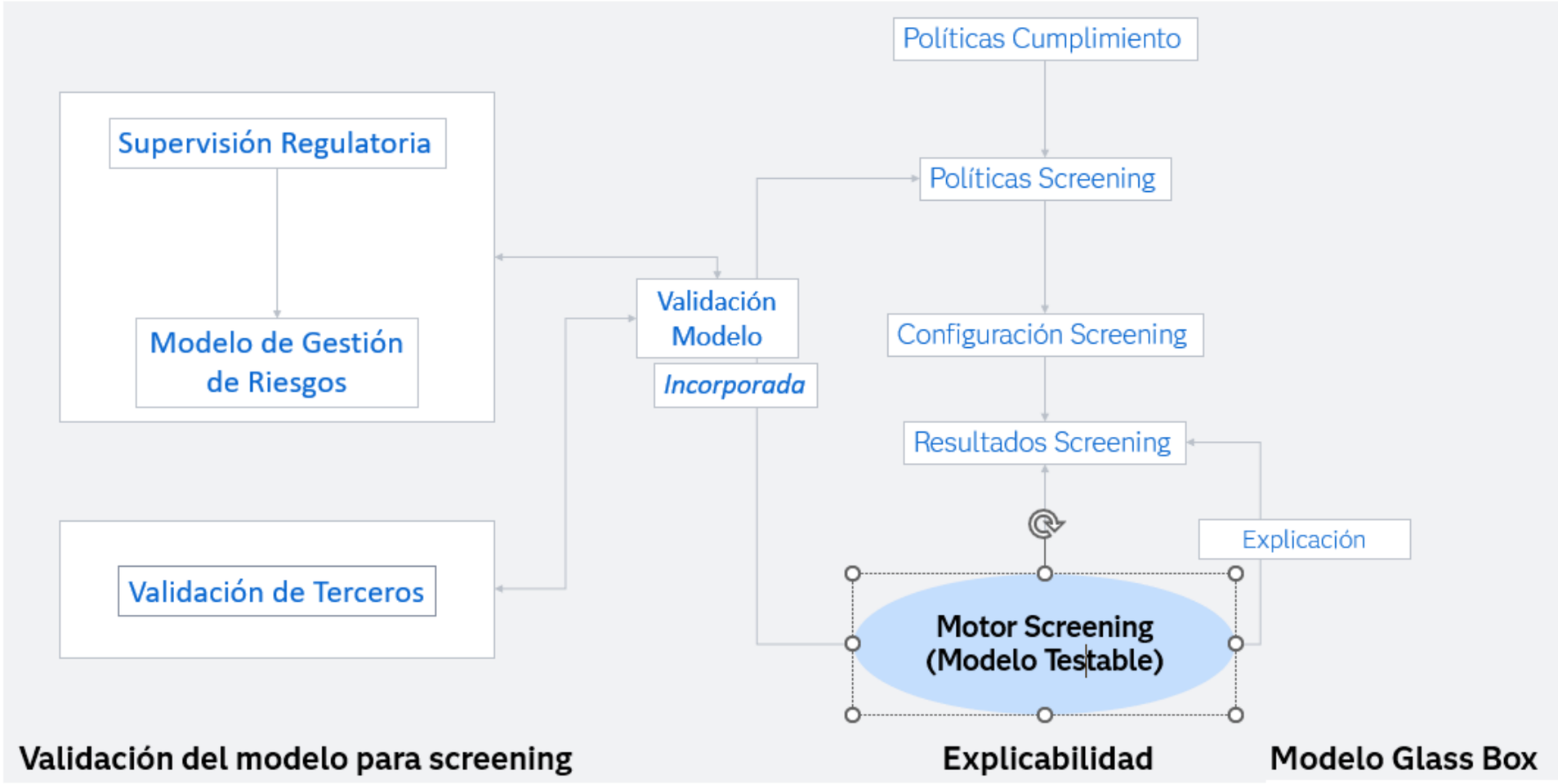
Incremento de eficiencia con IA y geolocalización

EXPLICABILIDAD
Modelos sin transparencia
Necesidad de demostrar
comprensión del sistema.

MODELOS GLASS BOX

Es necesario ser explicable

Un enfoque “Caja blanca”



SAS® Real-time Watchlist Screening

Visión General de solución

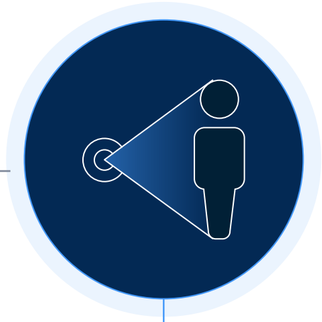
Peticiones Screening

Plataforma SAS

Tipos de Screening	**Screening Entidades** • Client Onboarding • KYC/KYB • Client Monitoring • Ad-hoc search • White/blacklists	**Screening Transacciones** • Pagos • Trade/LCs • Valores • Crypto
Inputs de Screening	**Registros de Cliente estructurados** 60 ms/1000 registros	**FIN (MT), ISO 20022, SEPA** 9 ms/1 registro

API

Servicio de Screening



AWS

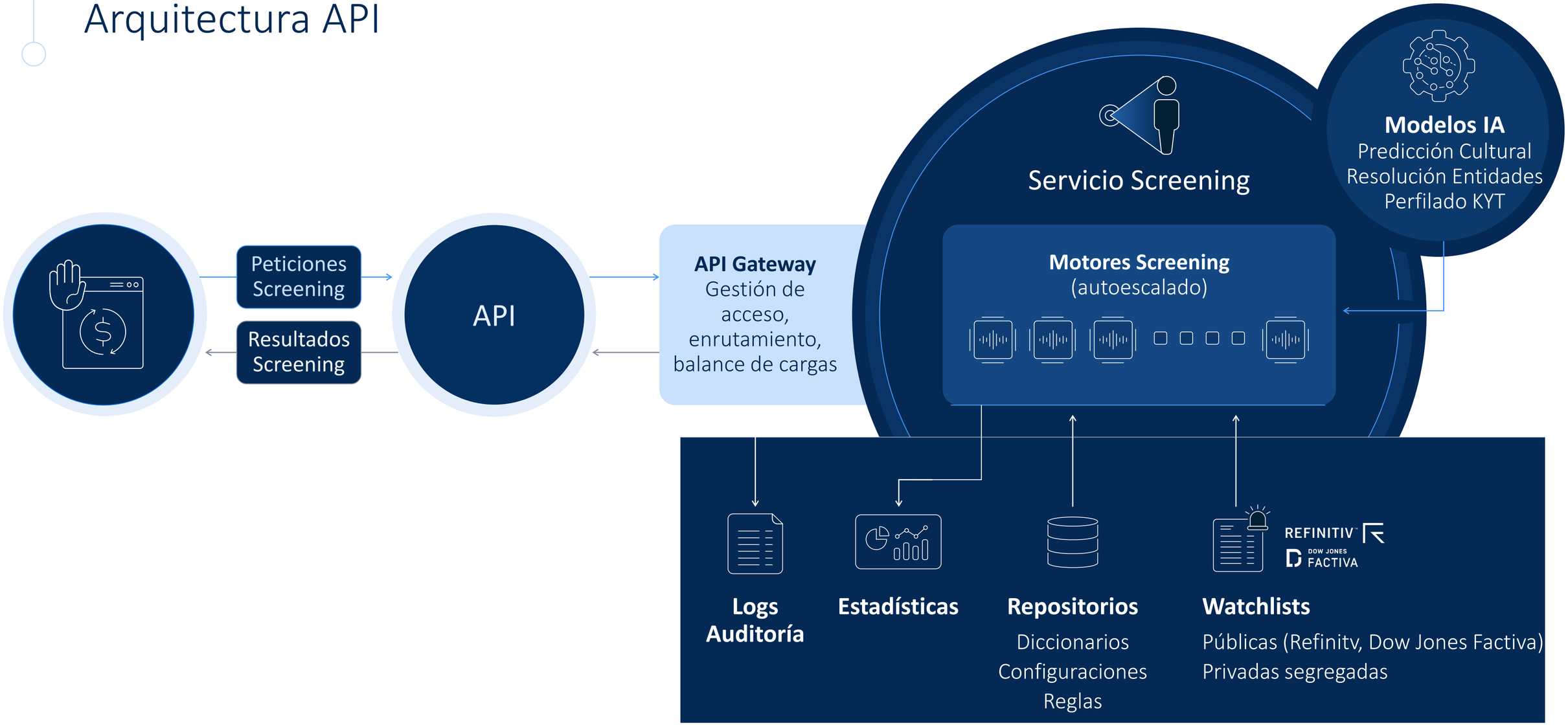
Azure

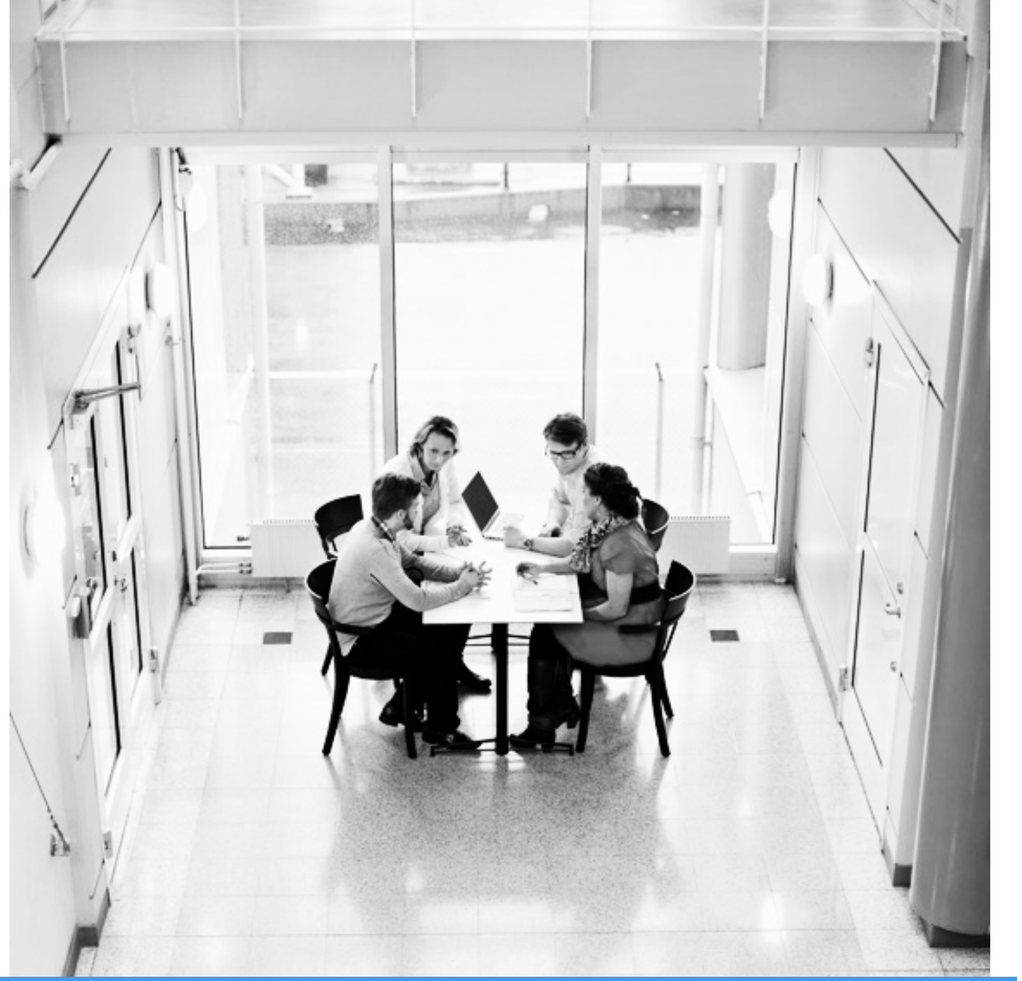
Match Analytics / Scores / Checksums

Resultados Screening

Servicio de Screening

Arquitectura API





AGENDA

FRAUD ROUNTABLE

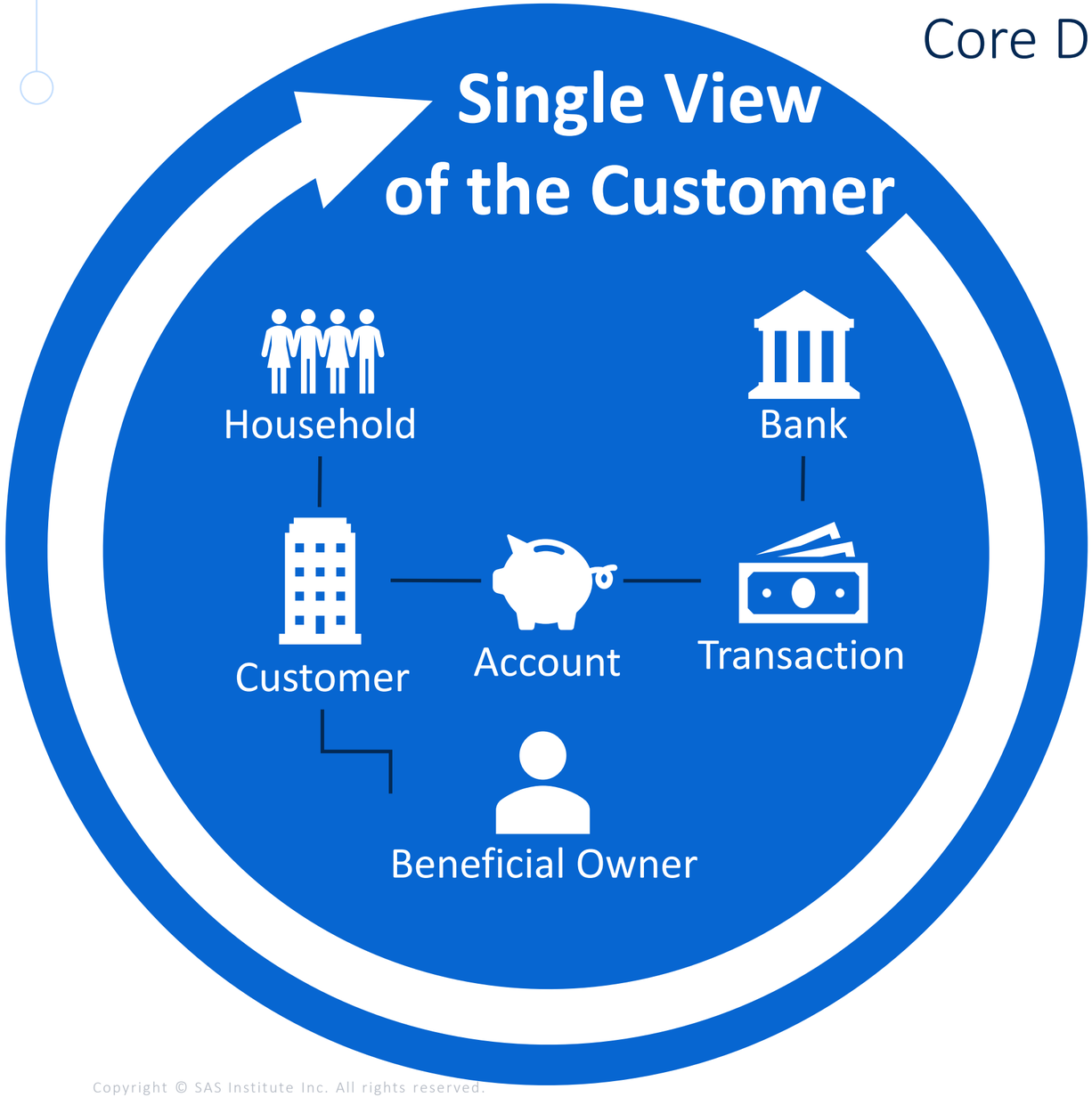
IA para la prevención del fraude
en un mundo digital

02 AML – ANTI MONEY LAUNDERING

- .1 TENDENCIAS
- .2 SANCIONES
- .3 VISION DE SAS

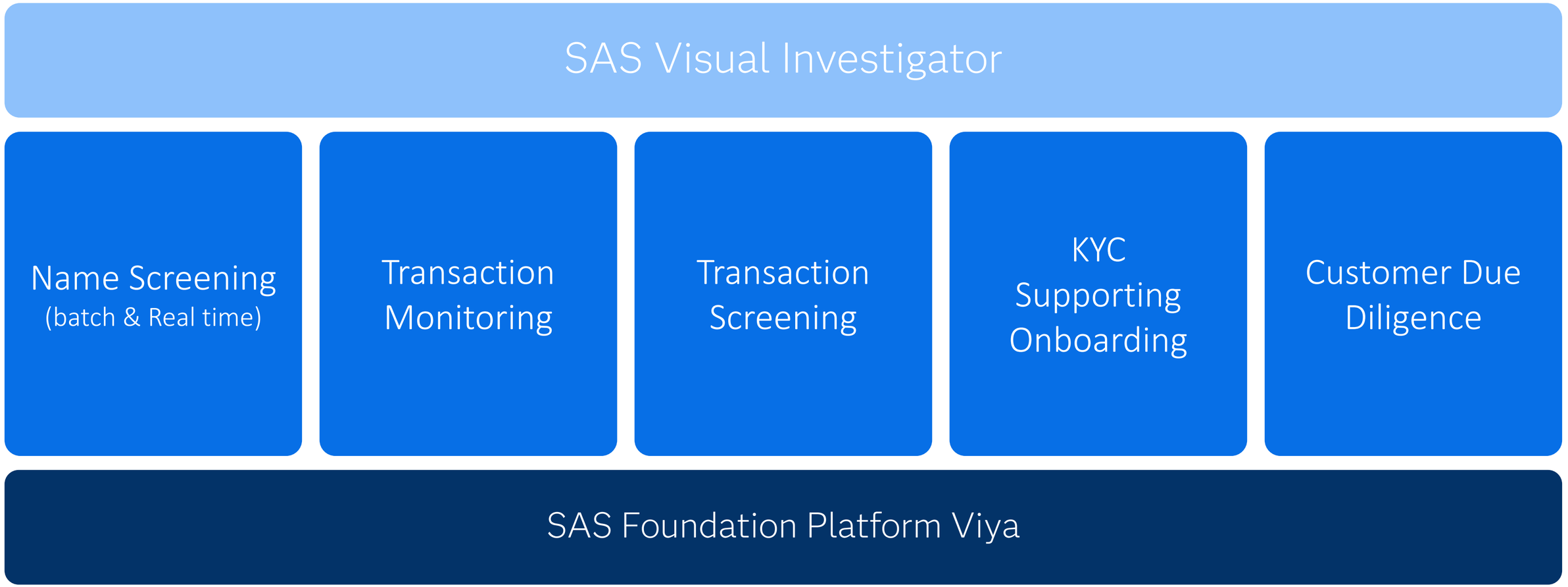
360° View of Customer Risk

Core Dimensional Data Model

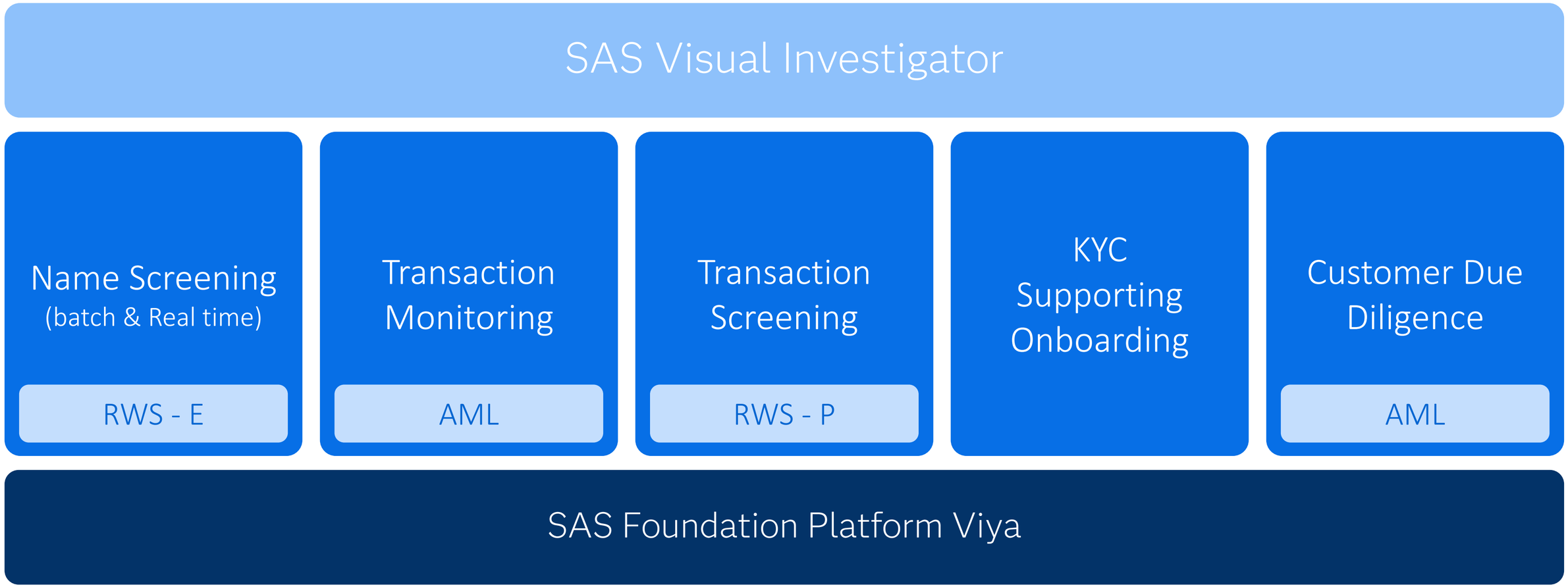


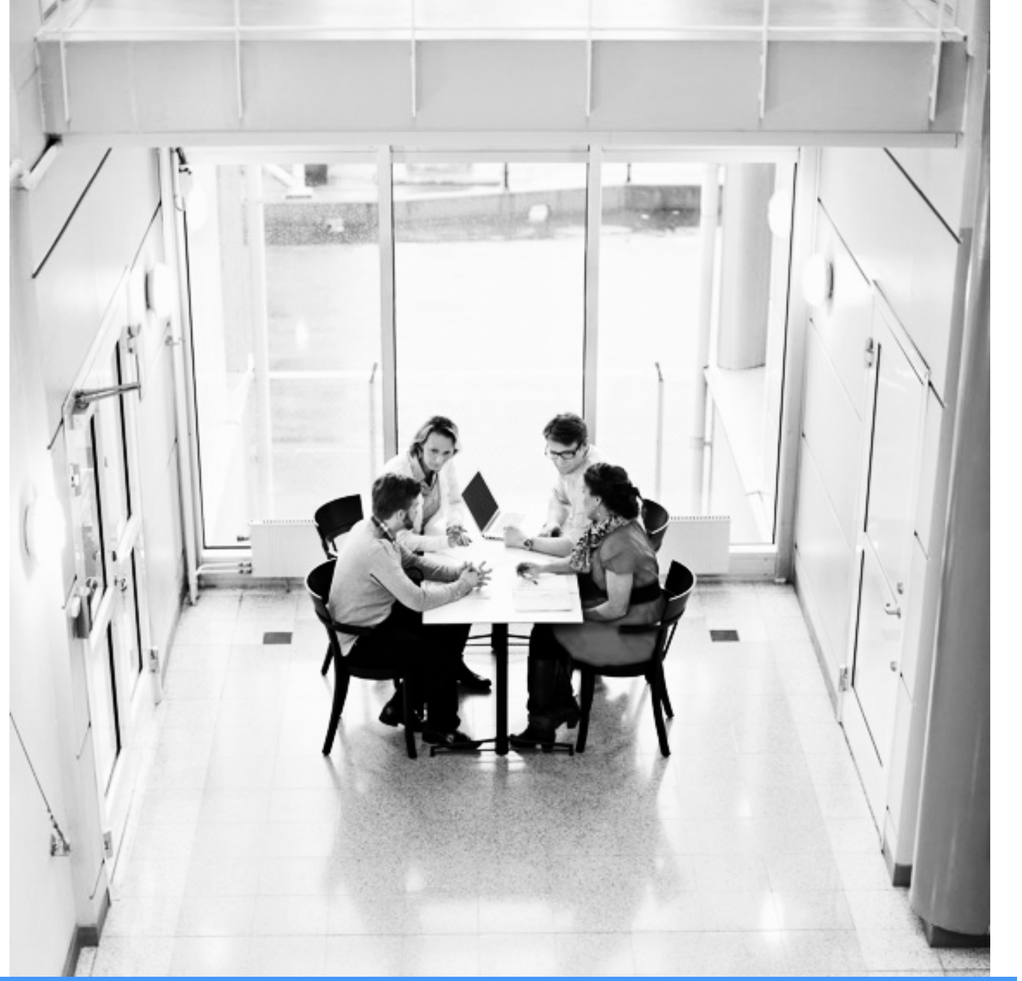
- ✓ Pre-mapping of 175+ Transaction Types, Channels, Data Elements, SWIFT, Watch List providers
- ✓ Supports the AML and CDD decisioning
- ✓ Aggregate data into beneficial owner and counterparty views
- ✓ Profiles for behavior monitoring, segmentation, and peer grouping
- ✓ Flexibility to add additional attributes
- ✓ Real Time screening of any type of Entities

End to End Approach to Compliance



End to End Approach to Compliance





AGENDA

FRAUD ROUNTABLE

IA para la prevención del fraude
en un mundo digital

01 FRAUD PREVENTION

02 AML – ANTI MONEY LAUNDERING

03 ECD – ENTERPRISE CUSTOMER DECISIONING

04 Q&A

Hoy

Las tecnologías aisladas que realizan un único recorrido del cliente crean una experiencia de cliente inconexa

Customer Engagement

Customer Engagement

Customer Engagement

Customer Engagement

MARKETING

RISK

FRAUD

FINANCIAL CRIME

Decision Engine

Decision Engine

Decision Engine

Decision Engine

El futuro es ahora. Una única plataforma nativa en la nube

Permitir que las organizaciones tomen decisiones holísticas basadas en la IA

SAS Customer Intelligence 360

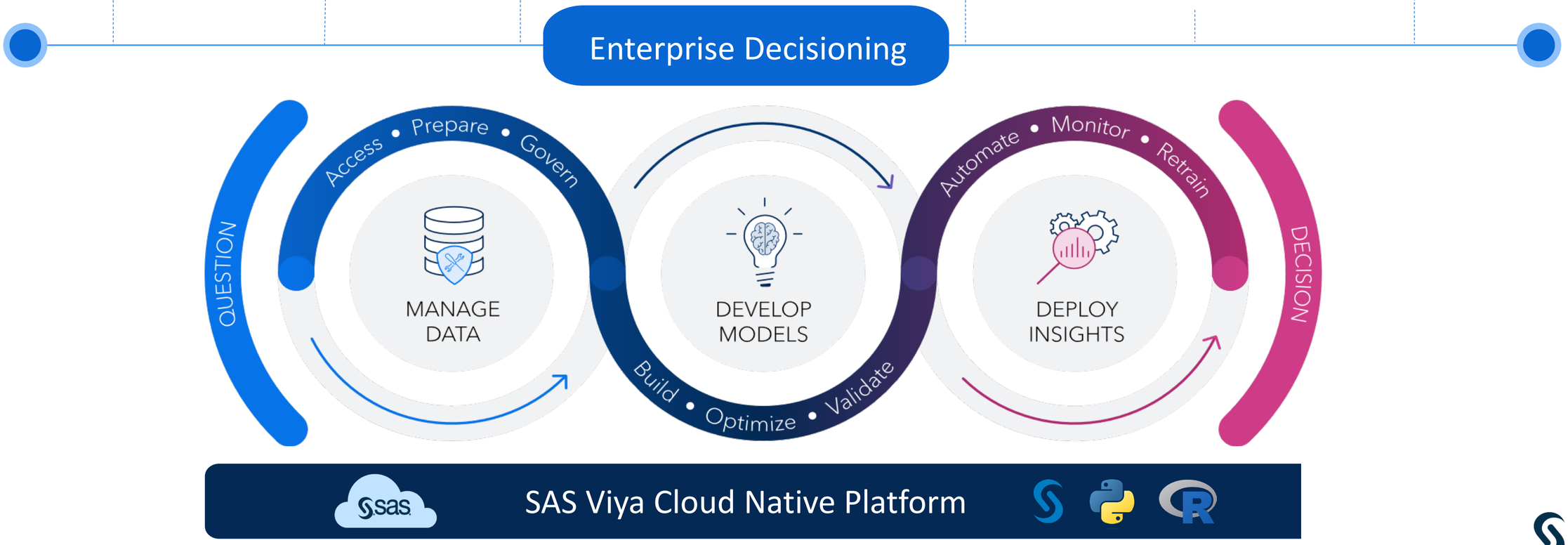
SAS Customer Credit Management

SAS Fraud Decisioning

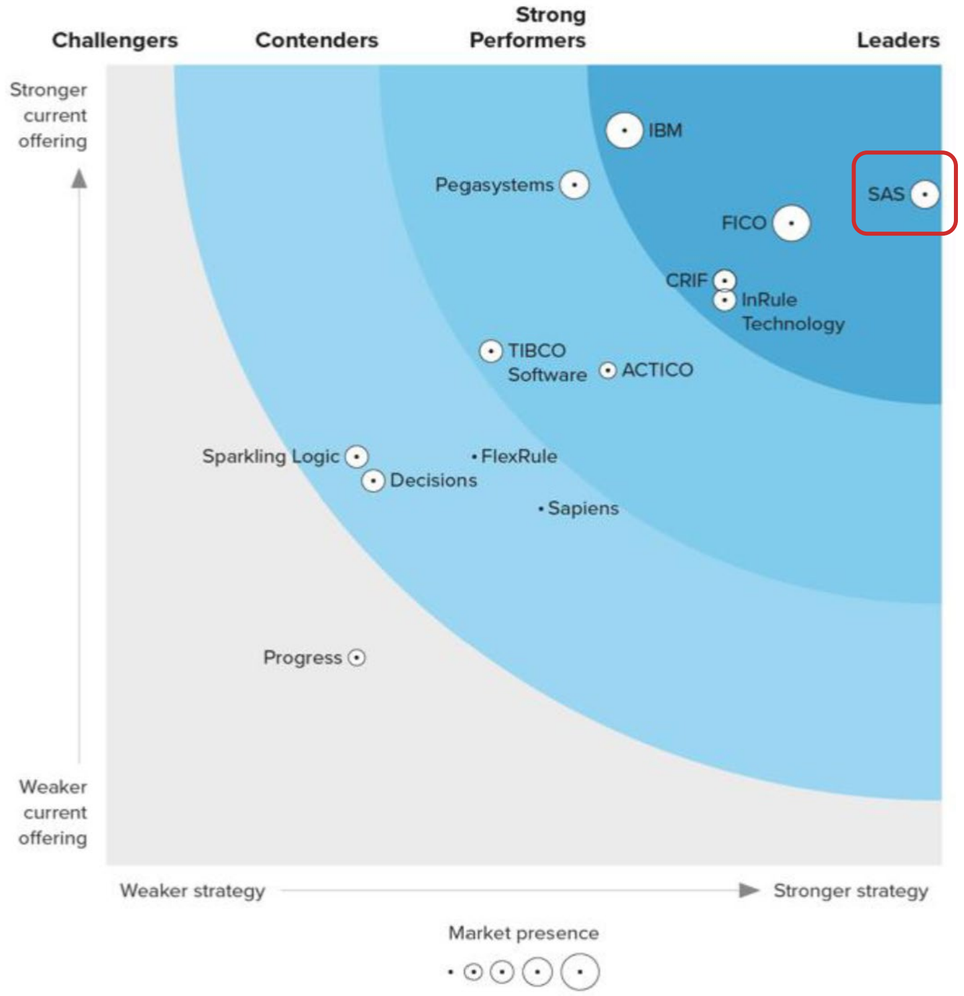
SAS Financial Crime Analytics

SAS Credit Originations

SAS Anti-Money Laundering



The Forrester Wave AI Decisioning Platforms
Q2 2023



“(SAS) aprovecha sus ya formidables capacidades de IA para ofrecer a las empresas plataformas de toma de decisiones de IA sofisticadas y fáciles de usar”

Imagina las posibilidades.
¿A dónde podemos ir juntos?

EVENT

FRAUD ROUNTABLE

IA para la prevención del fraude en un mundo digital

Jueves, 25 de abril

¡Gracias!