SymphonyAI

AI in Action

Practical applications for FinCrime prevention in 2025

AI adoption guide

Contents

Introduction

Financial crime prevention is changing.

With an influx of new technology, criminals are finding it easier than ever to commit money laundering, fraud, and sanctions evasions.

The tools available to criminals – such as using AI – are also available to financial institutions, enabling them to detect and prevent financial crimes.

Tech spend is the priority for 69% of banks and more than 80% are scoping or engaging in AI initiatives in financial crime.

Despite this, just 46% of banks reported to the Bank of England that they have only a ‘partial understanding’ of the AI technologies they use.

Though parameters and cautions remain, there is increasing acceptance by regulators that using AI can help to mitigate crime.

This guide aims to help you understand the practical applications of AI in AML processes.

Sources: Chartis analysis 2024 | Bank of England and FCA report, 2025.

Typical AML process

Although it varies by institution, a typical AML process follows some basic principles:

Detection

- Detection engines rely on rules-based scenarios to identify risk.
- When rules are triggered, they generate an alert that necessitates a review.

Investigation

- A level 1 investigator will use multiple sources (customer risk scoring, internal & third-party data, etc.) to initially assess risk.
- Alerts deemed to represent genuine risk are escalated to L2 investigators for further research and will potentially require the submission of a Suspicious Activity Report (SAR) to the relevant regional FIU.

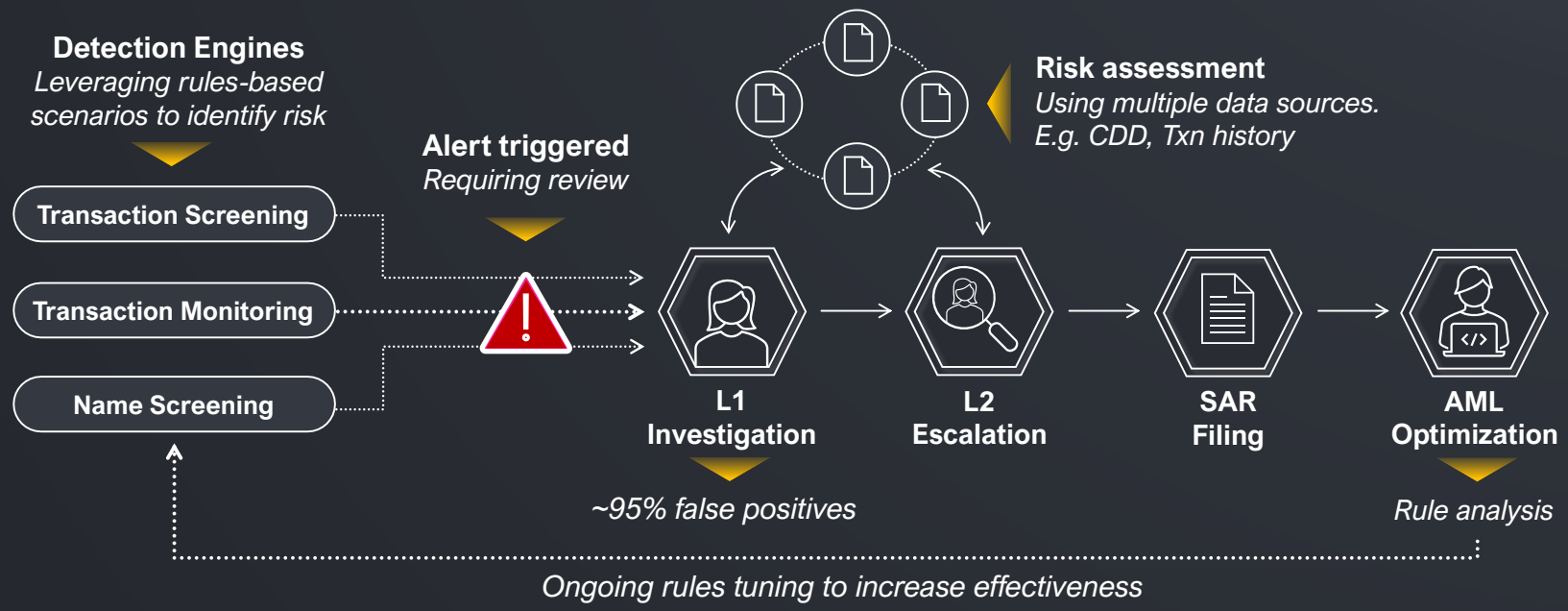
Optimization

- Detection rules and scenarios are analyzed to assess their performance. Fine-tuning takes place to reduce false positives and increase rule effectiveness.

Typical AML process flow

This diagram depicts a typical, albeit oversimplified view of a typical AML process flow. Key attributes to consider are:

- Rules-based only detection
- High false positive rate
- Manual data collection
- Manual data analysis
- Siloed teams & data sources



Understanding generative AI

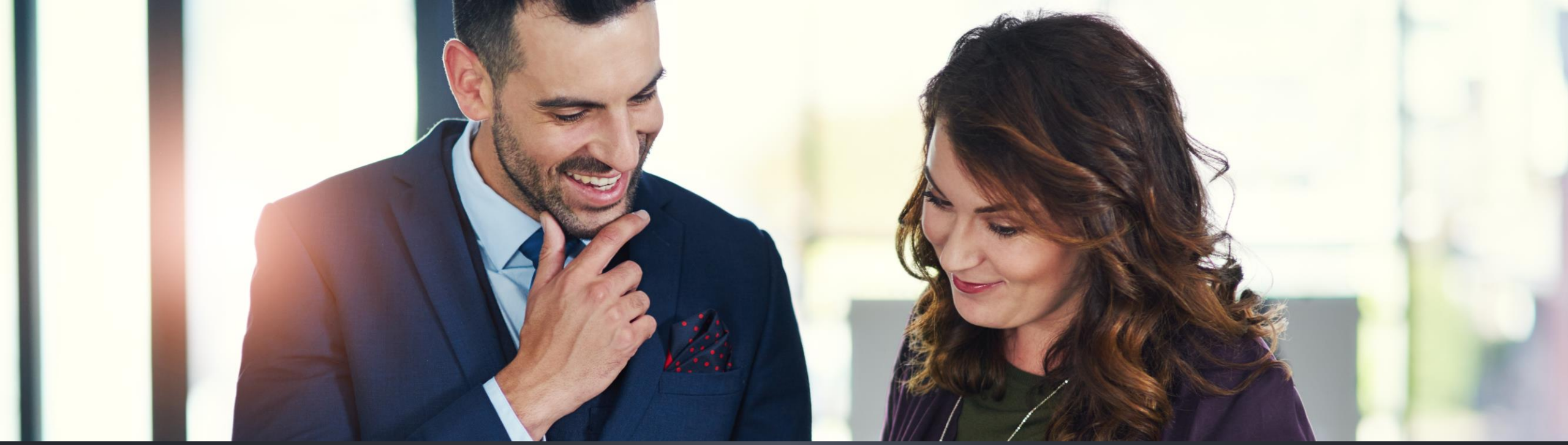
Generative AI is one of the more common applications of AI in use today. It uses natural language processing models and prompts to produce text, images, or analysis. By making complex data accessible and understandable, generative AI has many applications within FinCrime, such as providing greater contextual explainability for detection, investigation, and reporting activities. With the ability to ask questions and interrogate data, investigators can use generative AI copilots to assist in every aspect of their investigations.

A generative AI copilot can search documents and populate and summarize key findings in a fraction of the time it would takes a human.

When paired with predictive AI, the results are even more impactful.

Understanding predictive AI

While generative AI use in financial crime prevention is in the foreground, predictive AI can work at speed in the background. Predictive AI uses machine learning and advanced algorithms to analyze vast amounts of data extremely quickly. It identifies complex patterns hidden within transaction data to make predictions about the level of risk associated with suspicious or anomalous behaviors. Predictive AI models continually learn and improve via risk assessment feedback and can be configured to align with each financial institution's risk management strategy and risk appetite. When predictive AI works alongside generative AI, the outcome is a modern, seamless, and comprehensive approach to financial crime prevention.



Understanding agentic AI

Agentic AI, and the use of so-called AI agents, is perhaps the most exciting development in financial crime prevention today, significantly strengthening the industry's defense against emerging and evolving threats. AI agents are autonomous decision-making 'bots' that use adaptive learning to complete tasks. These agents all have set roles, such as researching names or analyzing transactions, and can work with one another to come to conclusions that are only then interrogated by an investigator. Able to work in real-time, identify suspicious activity and patterns, they also learn from historical cases, evolving as they absorb more data. Seen by most as the future of financial crime prevention, they offer an exciting glimpse at where the industry is heading, with some AI agents already available to improve working processes.

AI-driven AML

An AI-driven transaction monitoring process builds on the traditional approach and enhances it for modern, global finance.

Rules-based detection engines can be augmented with predictive AI models, enhancing their accuracy and exposing emerging risk vectors that traditional rules are unable to detect.

When rules are triggered, predictive AI assesses the risk level and prioritizes alerts, identifying false positives and ensuring alerts representing the greatest risk are reviewed first.

Predictive AI models continue to learn over time via risk assessment feedback, enabling ongoing improvements to better identify suspicious behavior and hidden risk typologies.

A generative AI powered copilot can analyze vast amounts of disparate data, assisting the human investigator by providing relevant alert context and helping to answer investigator questions.

Suspicious Activity Reports (SARs) can also be generated by a copilot in a fraction of the time, ensuring all relevant investigation information is included and allowing SARs to be far more consistent.

Let's examine some of the applications in more detail.

AI use cases

This section highlights key examples of how AI is being used to improve the efficiency and effectiveness of AML operations

Detecting new and hidden risk

Use case

Detection of illicit customer activity is the first line of defence in helping to prevent financial crime. Used across transaction monitoring, transaction screening, and name screening, it is a vital part of AML and sanctions screening processes.

How it helps

Traditional rules-based systems can be paired with predictive AI models to enhance detection.

Detection models are further enhanced by iterative machine learning that continuously optimizes detection parameters.

In transaction monitoring, predictive AI models expose suspicious behavior and transaction anomalies that are easily missed by rules alone.

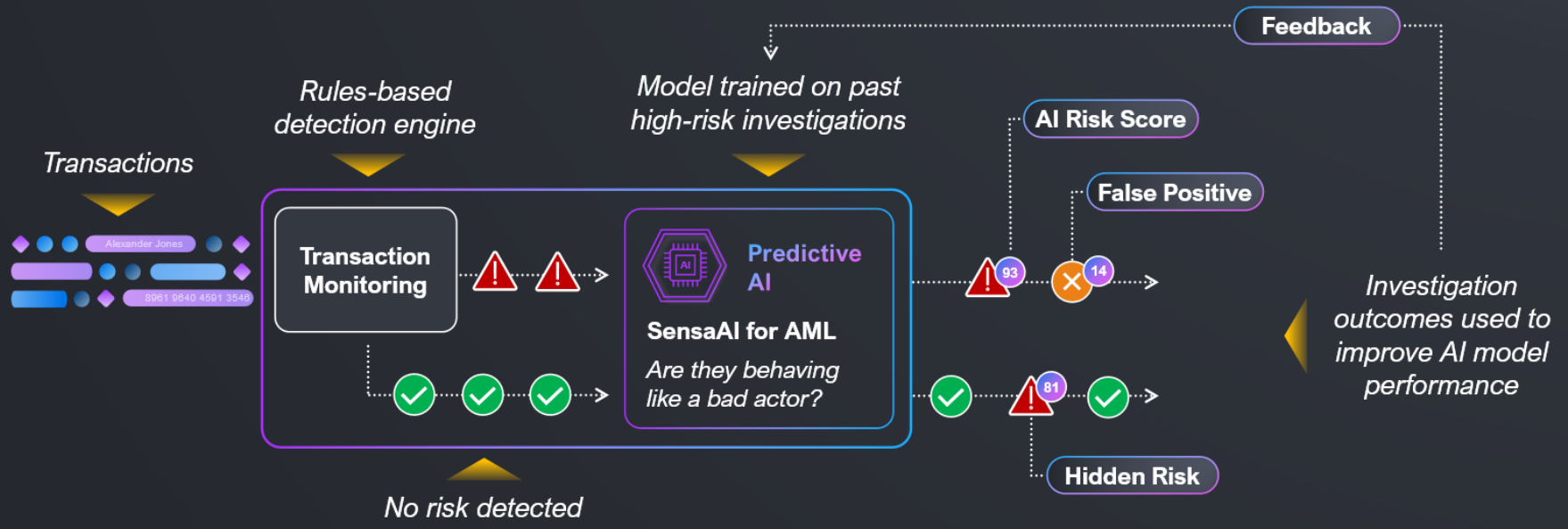
SymphonyAI applications

Sensa AI for AML
SensaAI for Sanctions

Example application

To illustrate how AI can enhance existing transaction monitoring systems, this diagram shows how SensaAI for AML works alongside rules-based detection engines to:

- Identify new and hidden risk
- Reduce false positives
- Assign an AI risk score to every alert



Alert prioritization

Use case

Once an alert has been triggered, predictive AI can more accurately assess the level of risk during post-processing. Alert prioritization can be implemented across every risk domain to ensure the greatest risk is always addressed first.

How it helps

Alert prioritization (also known as triaging) is important to enhance productivity and efficiency. The generated AI risk scores can be used to automate level 1 triage by auto-hibernating known false positives and escalating high-risk alerts directly to L2 investigators.

False positives are not automatically closed and are accessible for later review in accordance with the financial institution's internal policies.

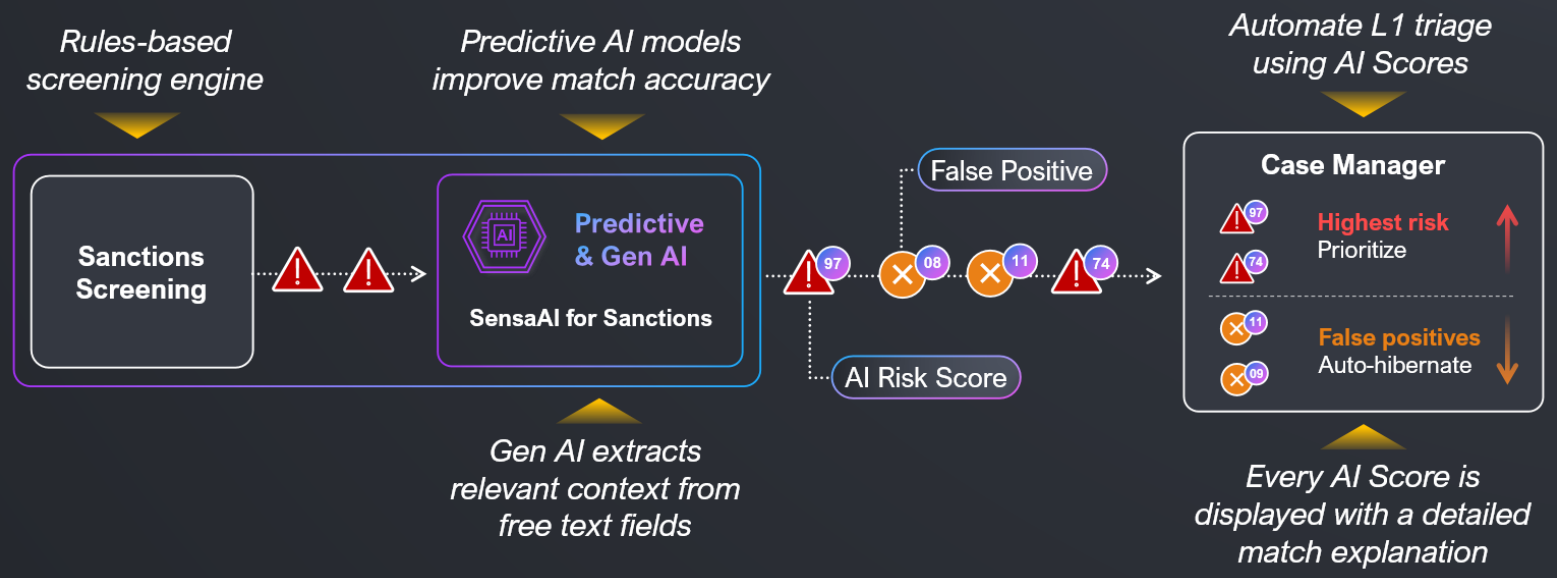
SymphonyAI applications

Sensa AI for AML
SensaAI for Sanctions

Example application

This example uses SensaAI for Sanctions to show how an existing screening system can be given an immediate AI upgrade to provide effective screening alert prioritization, in addition to:

- Identify false positives
- Highlight greatest risk
- Automate L1 triage
- Provide detailed AI match explanations



Streamlining investigations and workflows

Use case

Investigations and workflows perhaps enjoy the largest impact of AI with organizations benefiting from improvements in consistency, productivity, and efficiency.

How it helps

Data is ingested into a centralized system, allowing a copilot to analyze and summarize vast amounts of information in seconds. This provides investigators with a holistic view of customer risk and much faster access to relevant data and alert context.

Large language models (LLMs) can provide internal and external research for investigators, communicating via a copilot to assist with every required process of an investigation.

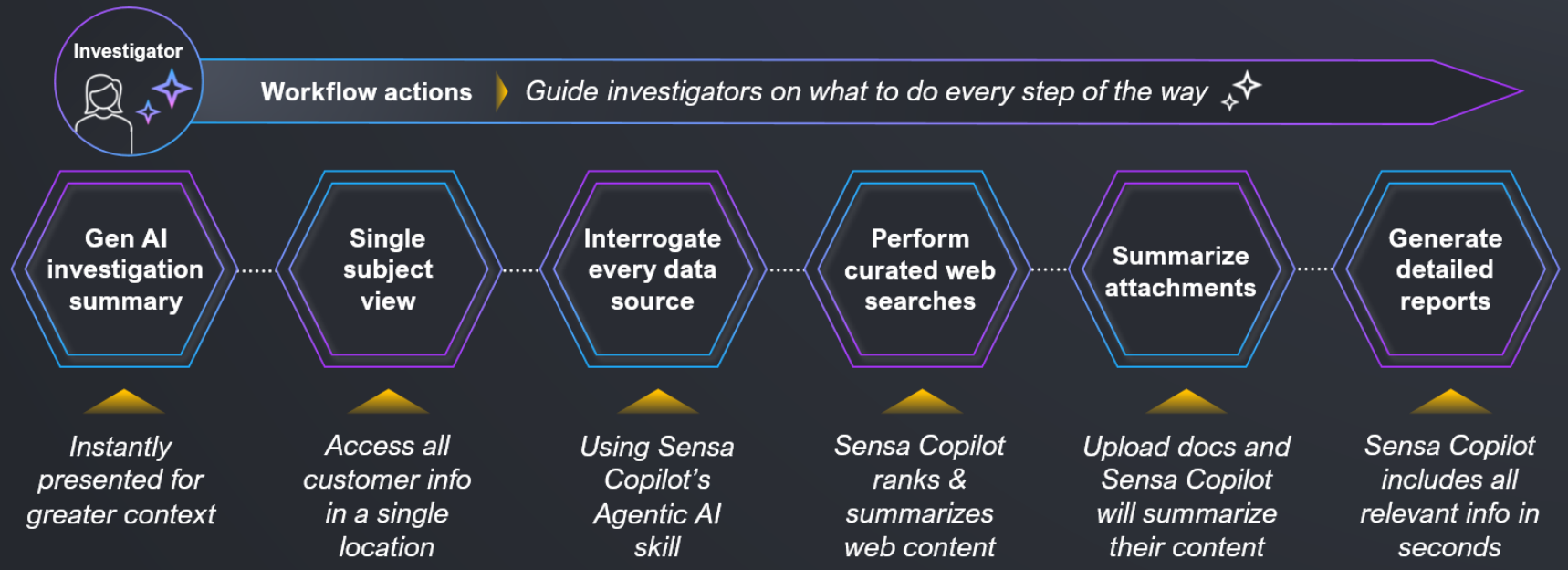
SymphonyAI applications

Sensa Investigation

Example application

This example shows how **Sensa Copilot**, part of **Sensa Investigation**, is used to improve investigative processes, helping to:

- Accelerate investigations
- Improve consistency
- Ensure adherence to policies and procedures



Enhancing investigation processes

Digging deeper into AI copilot investigation use cases

Investigation Summary

When a detection event is investigated, the first step in assessing risk is to understand its context. Manually collecting all required subject and alert information can take hours. With a generative AI copilot, all relevant information can be presented to the investigator as soon as they open the alert. By summarising vast amounts of disparate data, the copilot enables faster, higher quality risk assessments to take place, ensuring nothing is overlooked.

Agentic AI powered transaction querying

Trawling through transaction data, exporting to Excel to create pivot tables, and trying to identify suspicious activity takes a lot of time. While generative AI can certainly help accelerate this process, the adoption of agentic AI takes it to the next level. By understanding what 'suspicious activity' means in the context of an alert, investigators can use an agentic AI-led copilot to interrogate transaction data to a far more advanced level, enabling deeper insights and less missed risk.

Web search & document summary

Performing online adverse media checks or reading through hundreds of pages of documents to find relevant information all adds time to investigations. Generative AI copilots can perform these tasks in seconds. Presenting investigators with a curated list of online search results along with webpage summaries can transform adverse media checks. Any document can be uploaded for a copilot to analyze and highlight relevant information, saving investigators hours of unnecessary reading.

SAR generation

Ensuring timely, comprehensive reporting that adheres to internal policies and FIU requirements can be a serious managerial challenge. With a generative AI copilot, SARs can be generated in seconds, containing all relevant information bookmarked by the investigator and detailing everything in a consistent manner. It can even translate reports into any language required by the FIU to make submissions that little bit easier and faster.

Automate complex workflows with agentic AI

Use case

The next revolution in AML will undoubtedly be the widespread adoption of AI Agents built using Agentic AI technology. These are self-directed systems that can analyze unstructured data, recognize patterns, perform tasks and make decisions autonomously.

How it helps

Powered by LLMs and augmented with domain and company specific knowledge, AI Agents can automate highly complex workflows for a wide variety of AML related use cases. The possibilities for transformative improvements in operational efficiency and effectiveness are almost limitless, and applications will continue to evolve at a rapid pace. Built to collaborate with both humans and other AI Agents, they can be easily integrated into existing workflows for fast results while ensuring complete human oversight.

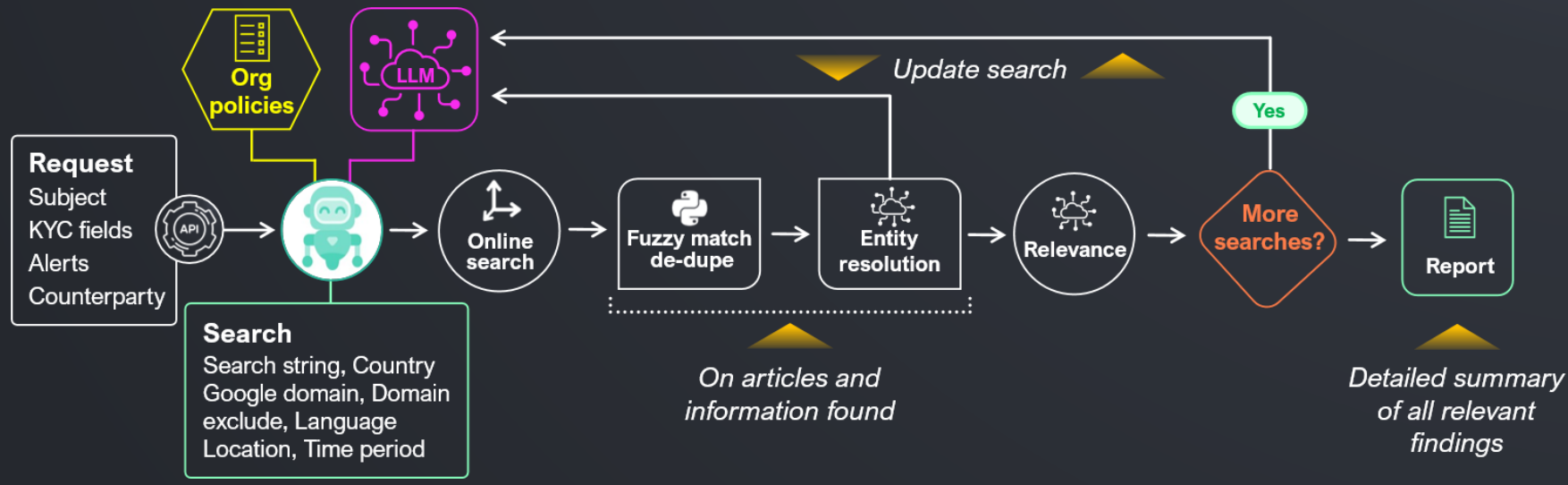
SymphonyAI applications

Sensa Investigation

Example application

This example shows how Sensa Researcher Agent can automate online research for adverse media checks during an investigation, enabling:

- More efficient investigations
- Highly consistent processes
- Robust 'human-in-the-loop' decision-making protocols

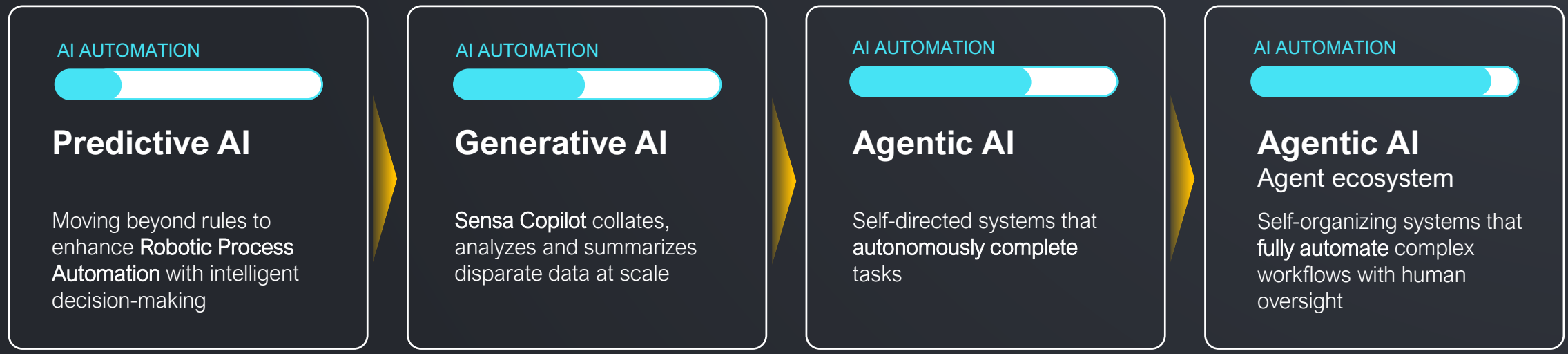


How to start your AI adoption

The phased approach to AI-led risk management

Many financial institutions that would benefit from the adoption of AI-driven software in their AML programs struggle to know where to begin. Mitigating the introduction of risk into operations is critical to ensure all stakeholders can be confident in the efficacy and safety of AI applications. SymphonyAI recommends a phased approach that enables organizations to gradually increase their use of AI over time at a pace that suits their strategic objectives. This is achieved by starting with low-risk use cases and realizing the benefits that AI provides before increasing the level of AI-driven automation available.

The end goal is to modernize your tech stack, build trust, and ensure that you're ready to enjoy the benefits and reap the value of AI technology.



How SymphonyAI can help

SymphonyAI offers a complete AI-powered financial crime detection, investigation, and reporting suite. Products used throughout this guide as example applications include:

Sensa Investigation

Unify your enterprise-wide risk and compliance tech stack with an AI-led case management system. Featuring Sensa Copilot, a generative and agentic AI powered investigative assistant.

Learn more.

SensaAI for AML

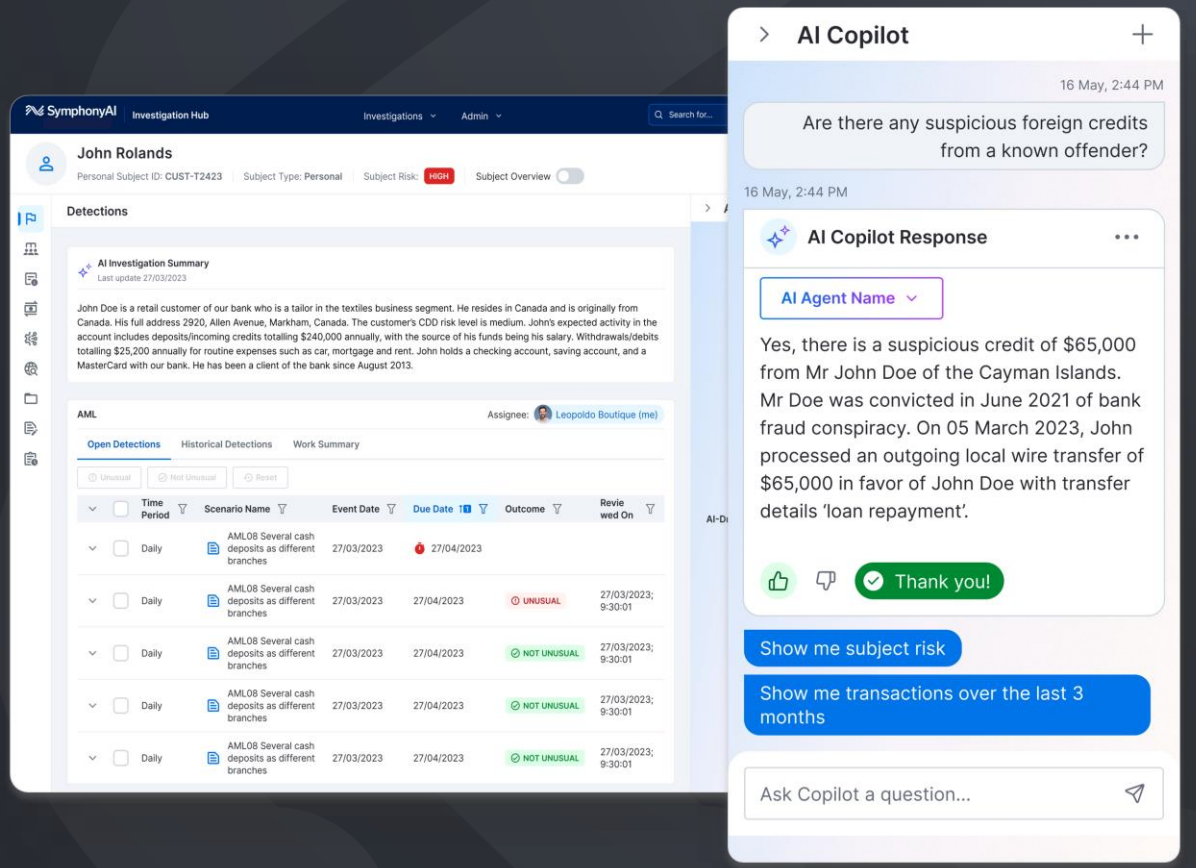
Enhance existing transaction monitoring systems with a powerful AI upgrade. Using advanced supervised machine learning, SensaAI for AML is designed to reduce false positives, identify hidden risk, and prioritize alerts.

Learn more.

SensaAI for Sanctions

Combining generative and predictive AI, SensaAI for Sanctions upgrades existing screening systems to significantly increase match accuracy. Dramatically reduce false positives, uncover missed risk, and provide greater alert context for investigators.

Learn more.



Learn how we can solve your most critical financial crime challenges

SymphonyAI is the leading SaaS provider of AI-powered FinCrime prevention and compliance solutions. We transform our customers' ability to manage risk with predictive, generative, and agentic AI innovation that detects and prevents even the most complex criminal activity.

For more information or to request a consultation, please visit **symphonyai.com**

SymphonyAI