

SensaAML™

Focusing on the latest and riskiest criminal behaviors targeting financial institutions and their networks

The cybercrime landscape has shifted, thanks to the global impact of the Covid-19 pandemic. With huge numbers of employees forced to work from home, you could almost hear money launderers and other financial criminals rubbing their hands with glee. Not only would even more services be forced to conduct their business online, but this new global home workforce would create extra opportunities to exploit financial and enterprise cybersecurity weaknesses.

The combination of governmental financial support and increased online and remote banking has led to a spike in financial fraud. Heightened risks make it harder to comply with requirements to combat financing terrorism (CFT) and deploy anti-money laundering (AML) technology, especially in relation to customer identity verification, due diligence, and tracing assets converted into less transparent and less traceable forms.

With front-line workforces stretched thin, machine-learning software like SensaAML combines supervised, unsupervised and graph machine learning technologies to naturally adapt and evolve over time and focus on the latest and riskiest criminal behaviors targeting financial institutions and their networks.

How SensaAML works

The high stakes associated with minimizing financial crime require having an adaptive system that can discover anomalies, navigate networks of relationships and surpass simple rule-based detection methods.

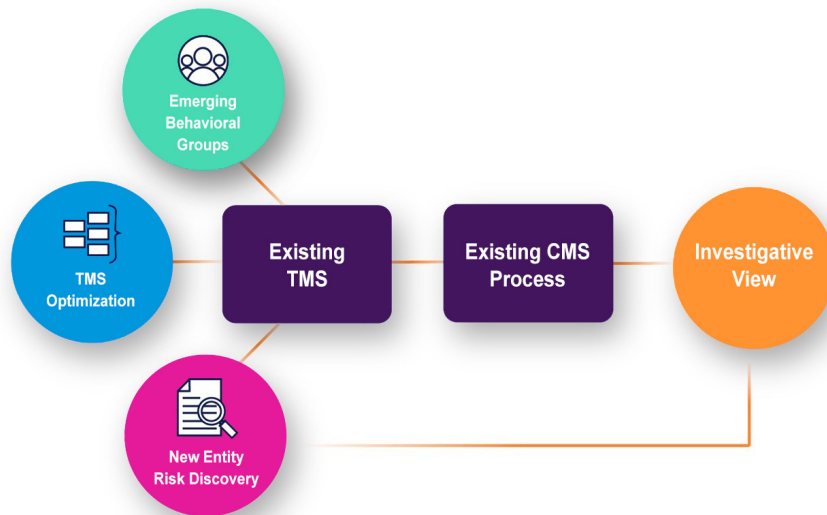


Figure 1: The augment or replace design of the SensaAML™ Solution







It's possible to achieve some reduction in the number of false positives generated by using basic, standard algorithms, but this will typically lead to a lack of explainability in the way the models form their predictions. It most likely will not be resilient to changes in the input data when not supported with more sophisticated

techniques, which aim to discover new risk starting from the raw transaction and customer data. Not to mention the challenges associated with running these models at the scales and speeds needed by most of today's large financial institutions, with all the controls required by the highly regulated financial industry!

SensaAML receives customer, transaction and other data, computes a high number of features to surface all the hidden nuances and connections implicit in that data, and feeds everything through our proprietary machine-learning models, which are trained to make the best use of that rich spectrum of inputs.

In a test in which the platform was overlaid on top of a world-leading TMS, SensaAML uncovered hidden risk at a 93% hit rate of entities that had never been investigated before. It reduced false positives by 60%, increased risk detection by 120%, and it increased speed-to-risk detection by 40% with one customer's banking data. Our users report a 120% risk capture rate with five times the efficiency gain compared to other systems.

Our software does not require prior data labeling nor an input segmentation. SensaAML utilizes the whole data it receives in input to generate a high number of primarily behavioral segments, which would be unmanageable for traditional segmentation practices. This reduces the preparatory steps clients must take before deploying and makes it easier to introduce new data sources.

1. Increased Risk Detection	 120%		150% L3 Escalation 120% SARs Filed
2. Speed to Risk Detection	 40%		40% SARs Identified >30 Days Sooner
3. Reduction of False Positives	 60%		60% False Positives Reduction

Transparency and auditability was one of our highest priorities when designing Sensa. We made sure that investigators can obtain all details related to a detection in a single view and can explore further context related to that detection beginning with that initial screen. Account behaviors, credits, debits, payment histories and payment flow visualizations are all available to paint a clear picture for investigators and analysts. Alerts can be worked on, commented on and escalated within Sensa, or they can be sent to a downstream case management application or process.

SensaAML is flexible and can adapt to several configurations before, after, in parallel or as a replacement to existing TMS. It can also run all the existing rules and scenarios of existing TMS approaches to aid in the seamless transition from a rules-based approach to a new paradigm and can be deployed in the cloud or on-premises within weeks.

Putting AI in the hands of many

SensaAML has a modern software architecture designed to adapt to your enterprise deployment requirements with maximum flexibility and scalability. Our flexible data model meets your data as it is, rather than forcing it to fit our framework. We are cloud-first and elastic, able to scale up and down as needs arise and integrate seamlessly into your system.