ORACLE
Financial Services

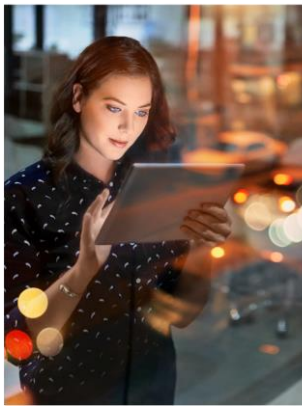
Network-Based Surveillance

A Solution to Transaction Monitoring

By: Garima Chaudhary, Oracle Financial Crime and Compliance Management Specialist

ORACLE

Financial institutions rely on deterministic rules to cull the transactions and pick out potentially suspicious transactions as part of their Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) programs. When a transaction is flagged, a case is generated and a procedure for resolving the red flag is initiated. Generally, these rules produce cases for investigation as soon as a rule is hit. Therefore, these cases focus on one type of behavior, which may or may not be comprised of multiple and related party information (customer, account, external entities).



CHALLENGES WITH THE TRADITIONAL MONITORING METHOD

The traditional way of surveillance not only generates a massive number of cases, but also has several fundamental issues, such as:

- **Lacks Holistic Surveillance:** A specific behavior can be an indicator of suspicious activity and should be assessed in conjunction with other indicators, not in a silo. When cases are created for the entity, as soon as there is a suspicious rule hit, the surveillance process is not factoring the behaviors that occurred before and after the specific activity. This means the surveillance process is lacking a holistic view, which makes the detection process ineffective to some degree.
- **Siloed Investigation:** For flagged transactions, AML staff investigate the specific circumstances surrounding the transaction. High-risk products, areas of operation, business lines, and basic customer information can influence the amount of transaction testing. During the investigation process, users do their best to include any related cases found manually, which is primarily based on customer and account. Although this helps investigators include previous cases for that customer, this does not factor other related, loosely related, or hidden suspicious behaviors. These manually linked cases may provide some additional information about investigated entity; however, it may not quantify overall risk.
- **Too Much Information:** Data is collected during the transaction testing process and during follow up investigations. Manual linkage of related cases adds a significant amount of data, which investigators will have to study as part of their investigation. This may be very hard to make sense of in absence of a proper network view of all the involved parties.

In summary, the traditional way of pattern detection leads to an enormous number of cases, which then require analysis of several other systems for a comprehensive investigation. Overall, this leads to longer investigation periods and makes the entire process highly inefficient.

SOLUTION: NETWORK-BASED SURVEILLANCE

The purpose of network-based surveillance is to leverage an optimization layer for all the risk indicators (events) to apply a risk-based assessment. This will further allow a comprehensive entity focused case to be created for investigation.

"As FIs continue to transform their program to keep up with the ever-changing regulatory landscape, efficient monitoring will be a key part. Transformation capabilities, such as Network-Based Surveillance, will drive down their operational costs, while reducing risk and providing efficiency and agility."

Garima Chaudhary
Oracle Financial Crime and Compliance Management Specialist

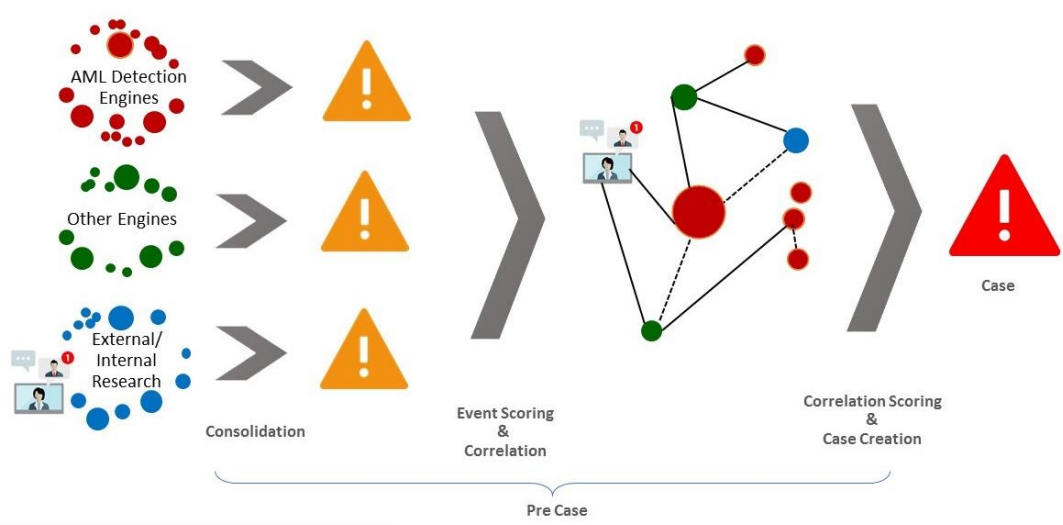


Figure 1. Broad level steps for a network-based surveillance process.

- **Step 1 - Ingestion & Enrichment:** The first stage is to feed all events from various sources, automated or manual. Events may not have all the requisite information for effective detection. Therefore, event information should be enriched. This enrichment of data should be extended to customers, accounts, external entities, and other relevant data sources. At this point, functionality to identify duplicate events and prevent them from being reprocessed should be applied. Additionally, any supplicate events should be identified and prevented from being reprocessed.

- **Step 2 - Consolidation:** Once ingested and enriched, events should be consolidated based on primary entities (Customer, Account, Tax ID, Address), matched event data or relevant elements (Line of Business, Geography, Jurisdiction) of the focal entity associated with the event. Consolidation rules can further be segregated to factor various case types, such as AML Monitoring, Sanctions, etc.

- **Step 3 - Scoring & Correlation:** Scoring on the events in the pre-case should be used to compare against the case creation threshold for evaluating whether the event optimization layer should cater for event score (at the point of event creation), pre-case score (every time batch runs) and entity score (every time batch runs). If a new event is generated on an entity on whom/which there is an open extendable case added, then the event could be directly tagged to that case. The case statuses that allow new events to be added to it should be configurable.

- **Step 4 - Correlation Scoring & Case Creation:** In the traditional way, every event generated from the transaction monitoring system either creates a case or gets consolidated to an existing case. In the last step, new events under a pre-case layer should be consolidated to a case once the score breaches the configurable case creation threshold.

BENEFITS OF NETWORK-BASED SURVEILLANCE

- **Increased Coverage:** Instead of investigating each risk indicator (event), network-based pattern detection allows for prioritization of risk events, thus increasing the monitoring coverage.

- **Identify Hidden Relationships:** Party relationships can be defined based on tightly or loosely related links. This helps identify hidden relationships at the surveillance layer itself, which may have been missed during investigation.

Step 1: Ingestion & Enrichment

- During the event ingestion process, the events should go through basic data checks and validation to ensure they can be correctly processed through the optimization layer. In case the event does not meet required data standards, it should flow into the exception queue. Event enrichment would aid scoring the event better, whereas case enrichment would facilitate holistic investigation.

Step 2: Consolidation

- During consolidation, all monitoring events should be consolidated under AML Monitoring. Adverse media screening alerts and transaction filtering events can be tagged as “Name Screening & Transaction Screening” case types.

Step 3: Scoring & Correlation

- There should be a provision to subtract scores from the events in a pre-case. The negative scoring could be done to consider prior events on cases that were dispositioned to be “Risk Irrelevant.”

Step 4: Correlation Scoring & Case Creation

- Scoring can be done by scenario and country, increase/reduction by prior action on events, reduction via aging and so on.

- **Risk-Based Scoring & Prioritization:** Network-based multiple layer correlation process allows for risk scoring, not at case level, but at individual event and entity level too.
- **Holistic Investigation:** Since correlated entities and events are linked and presented as part of case information, this allows for investigation from any entity perspective.
- **Enhanced Network Visualization:** Now that relationships are identified and enriched leveraging both internal and external data, much more advance network visualization can be used to determine bad entities.

While this new way of monitoring means a much more efficient Anti-Money Laundering and Anti-Terrorist Financing program, organizations should be careful about the level of network link to be used for correlation. If not thought through, this can lead to a much more complex case and might 'over-help' investigators. Appropriate training, future need for delinking, and information sharing between analytics and Financial Investigation Units should be considered when getting into this new program. Lastly, the subsequent phase would be to apply machine learning to identify new hidden relationships, statistical techniques for scoring and determine case promotion threshold based on historical information.

To learn more about how Oracle addresses this topic, contact us here.