NICE Actimize

Datasheet

Network Risk Analytics

Understanding both direct and indirect entity relationships and connections is crucial to discerning the full scope of financial crime risks your organization faces. Network risk analytics is the key to accomplishing that.

With network risk analytics, you can understand and manage the risk of your customers' relationships, enhance detection coverage by detecting suspicious activity between related parties, and improve overall outcome quality with greater visibility.

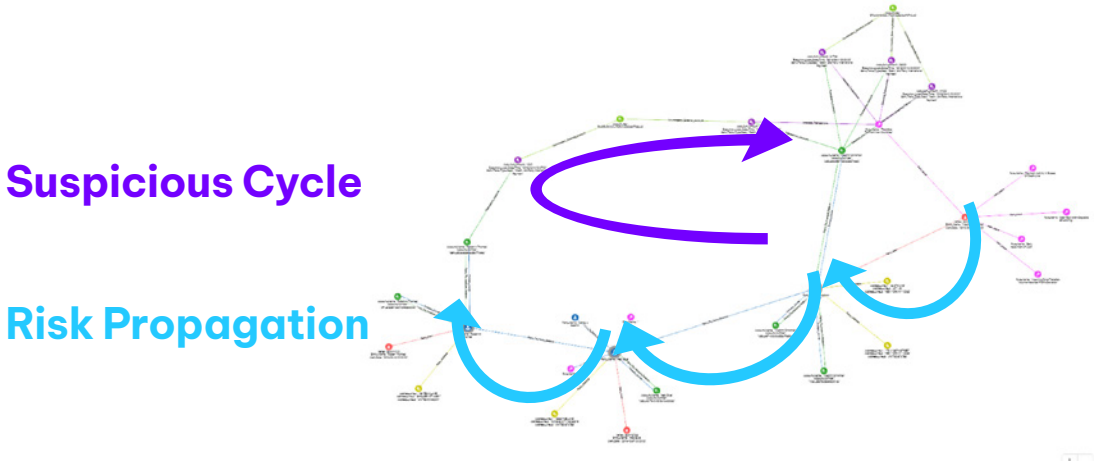
What is Network Risk Analytics?

Network risk analytics combines the power of identity resolution and graph analytics to uncover customer relationship networks and their associated risks. It uses customer account information, transactional data, and third-party data intelligence to identify these direct and indirect links.

Each network is made up of nodes that represent entities, such as parties, accounts, branches, and credit cards. Linked nodes represent connections, such as transactions between two accounts, beneficial ownership relationships between parties, and other attributable similarities discovered through identity resolution.

Richer Detection for Greater Effectiveness

You can use network risk analytics to enhance risk evaluation and detection of suspicious activity. This is especially useful in scenarios like mule rings and nested banking where identifying indirect relationships are crucial to understanding the bigger picture.

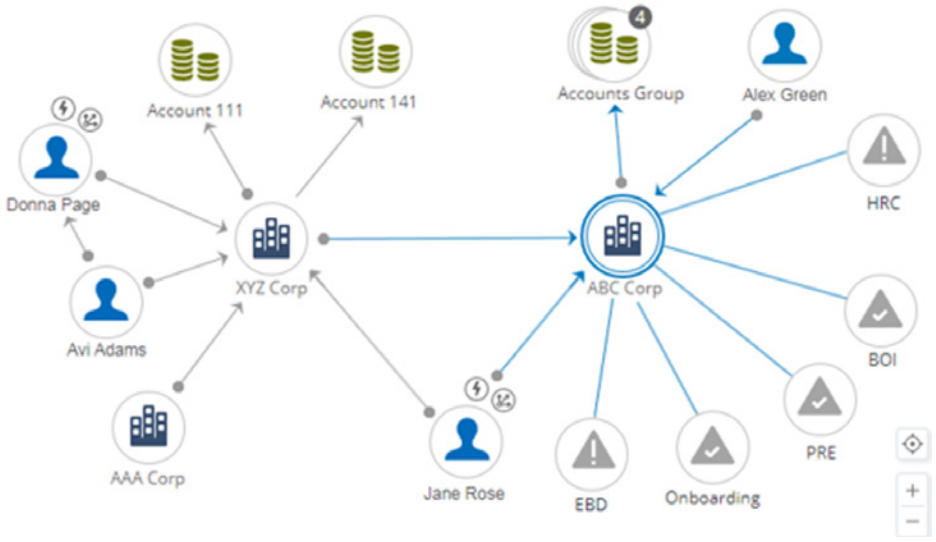


Network risk analytics can be used to:

- Enhance the accuracy of detection and scoring models by calculating graph related features for each entity that you can use in models
- Detect specific use cases (e.g., Cycle detection for Mule Rings) with graph algorithms
- Predict future criminal activity by analyzing network growth patterns

Greater Efficiency for Fuller Investigations

When investigating alerts, you can explore relationship networks and understand suspicious and high-risk connected parties efficiently with network risk analytics.



Network risk analytics can speed up the investigative process, telling you:

- The shortest path from the entity you're investigating to high-risk entities or other alerts
- If there is a community related to any specific high-risk behavior
- Who are the main actors based on degree centrality

The Power of Both Relational and Graph Databases

Network risk analytics incorporates both relational and graph databases. Why do you need an additional database when you already use a relational database? Relational and graph databases have different strengths that, when coupled together, provide you with a complete picture.

Relational Database

Perfect for direct relationships, like:

- A single address related to multiple parties
- A single party related to multiple counterparties

Applications:

- Identity resolution
- Counterparty rules
- Beneficial ownership structures known in advance

Shortcomings:

- Complex, unknown beneficial ownership structures can't be found
- Circular fund structures are almost impossible

Graph Database

Perfect for indirect relationships, such as:

- Beneficial ownership (BO) structures
- Device and POS networks
- Full money flow across multiple entities
- Any connection type (payments, social networks, news)

Applications:

- Risk propagation via any relationship type (Entity Risk)
- Community identification (e.g., Terrorism Financing)
- Beneficial ownership structure discovery
- Circular fund structure identification
- Network growth modeling: Can predict suspicious network activity (Human Trafficking)
- Graph features extraction for machine learning development

Building the Networks

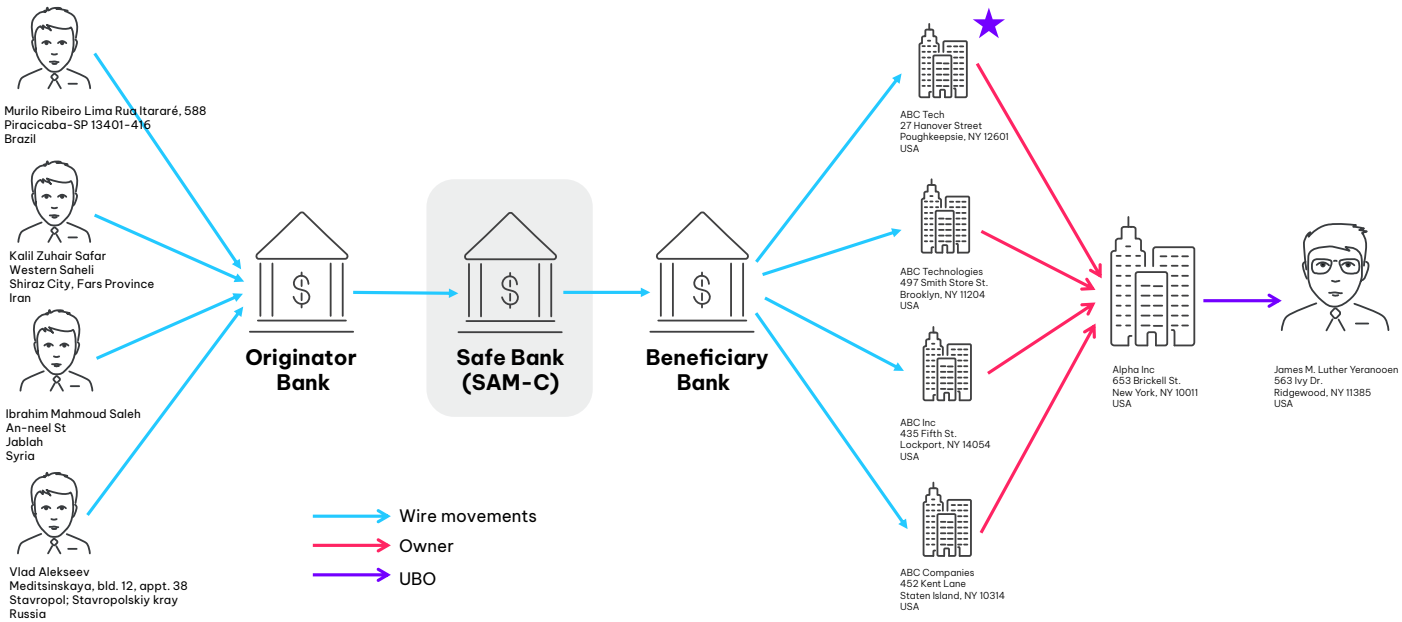
SAM uses available risk data to build the networks. SAM brings in:

- Customer data, such as parties and accounts, to create nodes in the network
- Transactional data where more than one entity is involved. For example, a wire between two parties or a credit card transaction involving a customer and a vendor
- Relationship data such as beneficial ownership data or relationships identified using attribution data through identity resolution
- Any data that may help identify risk linked to the detected accounts and alerted parties, such as issue and alert data

The graph database is not meant to be an additional data repository. Instead, it focuses on holding all the relationships between entities, enabling us to identify new connections with multiple degrees of separation using graph queries.

Use Case—Correspondent Banking

Network analytics can enrich the identification and detection of suspicious activity in many situations, including this correspondent banking example.



In this example, the transaction monitoring solution can recognize that James M. Luther is the ultimate beneficiary of four different messages. These messages all appear to originate from mules and are structured through multiple shell companies ultimately owned by James M. Luther.

A system not using network risk analytics would not be able to identify this suspicion because the detection system can't connect the relationships and identify that these activities are indirectly related. Using network risk analytics, the system can recognize a burst in beneficiary activity. But only because it can go two hops further into the relationship, combining ownership structures and traditional transactional relationships together.

Configuration and Flexibility

Network risk analytics provides you with optionality to configure it to your needs. You can:

- Create your own graph queries to detect specific network patterns
- Extend the queries used to generate and extract additional graph features
- Adjust graph query parameters during tuning

Technical Advantages

Network risk analytics leverages a distributed database and is designed from the ground up to scale seamlessly. Its architecture provides several advantages:

- Fast data loading speed to build networks—up to 150 GB of data per hour per machine
- Quick execution of parallel graph algorithms—hundreds of millions of vertices and edges traversed per second per machine
- Real-time updates and inserts using REST—two billion daily events streamed in real-time to a graph with 100B+ vertices and 600B+ edges on a cluster of only 20 machines
- Integration of real-time analytics and large-scale offline data processing

Detect Suspicious Activity Better

Gain a more effective, holistic approach to detecting suspicious activity by combining network risk analytics with a variety of other approaches, including:

- Rules
- Advanced segmentation
- Automated tuning
- Anomaly detection
- Collective intelligence
- Predictive scoring

NICE Actimize can work with you to build a personalized monitoring and analytics strategy tailored to your specific needs.

Get greater visibility into direct and indirect risks. Enhance your detection and investigations today with powerful Network Risk Analytics.