NICE Actimize

Insights Article

Harnessing the Power of Network Analytics to Uncover Hidden Risk

Introduction

The ever-evolving financial crime landscape is marked by increasingly sophisticated scams and money laundering schemes. And criminals never operate alone. They need a network to help move their ill-gotten gains or obscure their illegal enterprises. This brings focus to innovative tools and technologies, such as network analytics, that financial institutions (FIs) deploy to mitigate their risk and meet regulatory obligations.

At its most basic, network analytics is fundamental of investigating suspicious activity and unearthing connections between parties.

Network analytics is not a new function within FIs. Historically, they have had a network analytics capability. However, these attempts were usually siloed from the primary investigation platform and required experienced investigators to manually explore connections to decipher the inner workings within the network.

AI, Advanced Analytics, and Graph Database Technology

AI, advanced analytics and graph database technology have reshaped the role of network analytics in modern financial crime programs, empowering investigators to make determinations instead of manually building out diagrams and networks. In the complex and interwoven financial crime world, network analytics can drastically improve the ability to uncover hidden risk and prevent money laundering, fraud, and other illicit activities.

This article covers how critical network analytics is to modern financial crime and compliance programs, best practices for deploying this technology, and how to begin your journey.

The Urgent Case for Network Analytics Today

Generally, network analytics is known in its most rudimentary form: a wall-mounted board with people, addresses, and other information connected by different colored strings, like in a true-crime investigation TV show.

While the concept of network analytics isn't new, manually intensive techniques and early systems have significantly matured recently due to graph-database, AI and machine learning advancement. Network analytics is now used at the detection and investigation layers to uncover entity relationships, identify unusual or suspicious patterns, and expedite accurate decision-making.

Challenges in Detecting Fincrime

Financial criminals operate across multiple jurisdictions in networks that typically include counterparties and corporate involvement, concealing their real motives and fund sources. Investigators must comprehend and extract critical information to determine the connections between entities, discern the nature of these connections, and understand the reasons behind their affiliations.

From a data analysis perspective, traditional relational databases remain useful for some tasks, but fall short in capturing the complexity of network analytics and providing a complete, meaningful picture of risk. Graph databases have undergone a resurgence in performance and adoption because of their optimization for examining structures and relationships. Where typical databases may struggle with sophisticated queries, graph databases excel in unraveling intricate, often indirect, connections within a network.

For example, a relational database can be used to ask a simple question with one hop (the degree of separation or the number of links between entities in a network), like *who are the people that a particular person interacted with?* However, optimizing for more complex queries requires substantial investment, time, and effort.

Technology is pivotal in providing insights that are otherwise challenging or impossible to attain using conventional database systems. It also paves the way for more advanced use cases beyond traditional alert generation, such as facilitating swift responses to questions from law enforcement and regulatory entities.

Network Analytics Momentum Escalates

While most FIs selectively use network analytics within specific business lines, momentum must swing toward broader industry adoption, given the significance of network analytics in fighting financial crime. Integration is crucial, as network analytics can comprise part of the ecosystem to support risk detection and investigations; it doesn't have to be a complete replacement.

FIs face urgent money laundering, fraud, and compliance challenges that demand a new approach to detection and prevention:

- Criminals share intelligence, including the ability to move funds and use addresses, emails, phone numbers, directors, and Ultimate Beneficial Owners (UBOs) to execute this together.
- Investigators often use many systems, tools, and information sources per case, leading to time-consuming efforts and potential investigation fatigue. This approach also hinders the establishment of a single trusted source of truth, as data is frequently represented in various, often conflicting, perspectives.
- High false positive rates continue to be an issue across the industry, because of the inability to see the complete view of risk.

The focus must be to enable a rich understanding of risk by augmenting alerts with additional context through a network analytics approach, such as integrating external intelligence and internal data from diverse financial crime domains for a more comprehensive view of a customer and their activity. From a Know Your Customer (KYC) and Customer Due Diligence (CDD) perspective, this approach is vital to continuously monitoring and understanding changes in a customer's position and address history.

To maximize investigation effectiveness, FIs need to implement powerful network analytics that simplify and accelerate the understanding of intricate financial relationships. Yet roadblocks can emerge when leveraging suboptimal tools that require excessive clicking, hindering productivity.

The key when evaluating a network analytics visualization tool is to seek a balance between domain expertise and batch operations, minimizing the need for multiple clicks. Ideally, the solution should automatically highlight crucial entities, emphasizing the most significant paths to prevent overwhelming users with excessive details. Additionally, due diligence toward data cleaning and validation is necessary to mitigate potential setbacks in network analytics applications.

Practical Network Analytics Applications

Network analytics is only successful in a financial crime program when it's aligned with the specific objectives that FIs want to achieve. Network analytics has proven valuable in two critical areas:

1. Uncovering risk and identifying suspicious activities
2. Accelerating investigations that require insight into network risk

In the KYC space, whether onboarding or remediating customers, network analytics helps gauge risk levels. Organizations can better understand their customers' relationships, including immediate family and broader associations, to inform a customer's risk and susceptibility to engaging in illicit activities.

Network analytics provides a distinct advantage in transaction monitoring, especially concerning the counterparty aspect. While FIs may know their customer to an extent, the risk resides with the counterparty, where KYC information is limited. Building out the network structure reveals connections that may not be readily apparent and helps decipher complex relationships, particularly in trade finance and capital markets where multiple parties could be involved across numerous stages of a transaction chain.

Practical applications for network analytics include:

- **Correspondent banking:** Network analytics can result in a substantial reduction of alerts, often from thousands to hundreds, and the ability to detect new risks. It maps relationships between correspondent and nested banks, identifying anomalies like a surge in beneficiary activity through comprehensive network analysis and integrating data about ownership structures and standard transactional connections.
- **Corporate banking:** Network analytics can detect and analyze network burst activity in corporate banking that may indicate illicit behavior. Relationships between entities, like directors, companies, or beneficiaries, are revealed that might otherwise go unnoticed.
- **Retail banking:** Network analytics can identify and mitigate the risk of money mule activity in retail banking. Analysis of transaction patterns, account relationships, and customer profiles results in a comprehensive network graph representing the connections between various entities, such as account holders, beneficiaries, and third parties.
- **Beneficial ownership structure discovery:** Network analytics can delve into corporate networks, mapping out relationships between various entities and analyzing ownership patterns and financial transactions to identify the UBOs behind corporate structures.
- **Network growth modeling:** Network analytics can predict suspicious network activity, like human trafficking. Models can be created from historical data and identified patterns of connections and interactions to forecast the growth of these nefarious networks. This approach can enhance efforts to anticipate and intervene in potential human trafficking operations and protect vulnerable individuals.

Strategic Integration & Cultural Impact

FIs can have a seemingly high-quality solution and data, but if it doesn't drive investigator efficiency and productivity, then there's no real value. For successful implementation, three primary considerations are paramount when integrating a network analytics solution.

1. Define the specific risks the solution should detect and identify within the data and gain alignment on these objectives.
2. Focus on the capability, including clarifying roles, processes, offshore or nearshore support structures, and ensuring effective integration with existing workflows.
3. Emphasize case management integration to ensure the solution is robust and aligned with current processes for greater investigator utility.

FIs must also address the cultural shift and mindset change required for investigators and the organization when implementing network analytics into a financial crime program. As with any new technology tool, the impact extends beyond operations into cultural and procedural changes.

Mindset change

Ultimately, the goal is low-volume, high-value investigations. This often results in a shift in the time required for complex investigations, such as correspondent banking or capital markets, based on the specific risk appetite. The mindset change spans from investigators comprehending the need for in-depth analysis to Money Laundering Reporting Officers (MLROs) acknowledging this new approach.

Case studies & dedicated training

Case studies and dedicated training, lasting weeks to months, are also essential for onboarding teams effectively. For instance, an experienced analyst transitioning from a traditional rules-based system perspective can successfully transition to new network analytics cases. But they need strong examples of what the end-case narrative and SAR should look like to drive the right quality of output being sent to law enforcement.

Investigation agility

FIs must ensure they have the optimal processes to give personnel the space to investigate. Network analytics solutions often generate enhanced level-two alerts that require a departure from step-by-step procedures. Investigators need the parameters of risk appetite and mandate to not simply stop at hop two if they're still suspicious, but to go even further if needed.

Integration and intelligent use are non-negotiables when implementing a network analytics tool. In one scenario, a bank implemented a segmented network analytics tool separate from the core system. Because the solution lacked intelligence, it presented a chaotic network, causing confusion and slowing investigations. The analysts, being untrained on the tool, struggled with information overload. After just nine months, the system was decommissioned due to inefficiency and escalating costs.

The value of an advanced solution with advanced AI and machine learning intelligence that can direct investigators to specific suspicious networks cannot be overstated. A smart network analytics solution can also support a more holistic approach to financial crime and compliance with other leading techniques, such as collective intelligence and anomaly detection.

The Future of Network Analytics in Financial Crime & Compliance

Increased cloud adoption and easier infrastructure integration will help propel the future of network analytics. The industry-wide movement toward the cloud enables faster adoption of advanced solutions like network analytics, a trend that will continue.

Additionally, leveraging network analytics for characterizing entities and relationships will contribute to more accurate machine learning models. This will minimize false positives and enhance risk detection without increasing alert volume, an indispensable edge for investigator productivity and effective financial crime programs.

While network analytics offers exciting potential, it's critical to prioritize foundational elements. Ensure clean, high-quality data, align with domain expertise, and clearly define objectives before implementation. Integration shouldn't be an afterthought, but an intrinsic component of an organization's infrastructure. Best practices for integration should encompass existing systems to avoid silos and ensure a seamless workflow. A phased approach, starting small and expanding gradually, can also enable FIs to build capabilities strategically.

In progressively interconnected financial crime networks, innovative network analytics solutions are a formidable investigative tool that empowers investigators and helps FIs navigate the risk horizon with agility and adaptability.

NICE Actimize is your industry-leading partner in accelerating the network analytics journey and enabling your financial institution to achieve a more holistic, effective financial crime program.

To learn more about NICE Actimize AI-powered AML or Fraud solutions, download this brochure or contact us.

Learn More