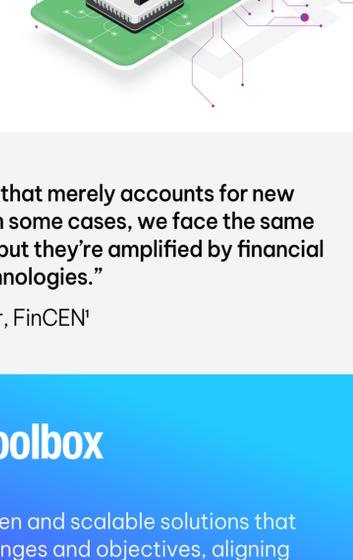


# See Suspicion with Precision Using AI in AML

## Integrating AI at the Core of AML

Rules-based logic and human-driven analysis is not enough to identify and stop money laundering. Detecting suspicious activity requires financial institutions (FIs) to continuously optimize AML systems to adapt quickly to ever-changing risks with perceptive, AI-fortified analytics. FIs can focus on truly suspicious activities by using analytics that address ongoing accuracy, coverage and efficiency challenges.



“An AML and CFT regime that merely accounts for new threats is not sufficient. In some cases, we face the same threats we always have, but they’re amplified by financial innovations and new technologies.”

- Him Das, Acting Director, FinCEN<sup>1</sup>

## AML Analytics Toolbox

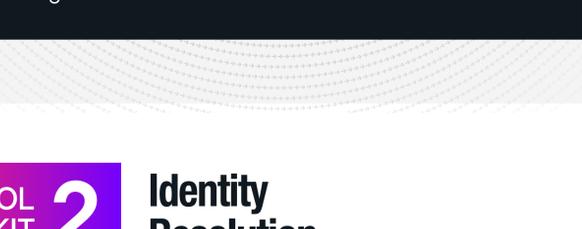
FIs must focus on tangible, proven and scalable solutions that address existing business challenges and objectives, aligning with strategic and regulatory compliance goals and maximizing return on investment (ROI).

### The ideal AML AI toolbox includes:

- Advanced Segmentation and Tuning
- Identity Resolution
- Collective Intelligence
- Anomaly Detection
- Network Analytics
- Build Your Own Analytics
- Predictive Scoring
- Generative AI

### TOOL KIT 1 Advanced Segmentation and Tuning

Advanced segmentation and automated tuning reduce noise and improve suspicious activity detection accuracy through tailored, machine-learning driven analysis.



With intelligent segmentation and automated tuning, FIs can **reduce alert volumes by over 40%** and complete full tuning cycles and simulation in **under 2 hours**, complete with extensive validation and governance documentation

### TOOL KIT 2 Identity Resolution

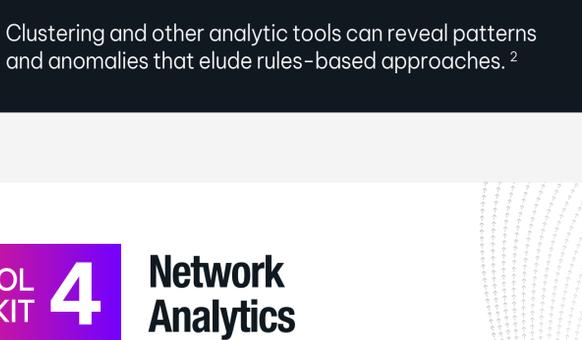
Identity resolution helps increase investigation accuracy by consolidating duplicated entity profiles, enabling investigators to understand parties and make better assessments if activity is suspicious.



Entity resolution tools can help AML teams achieve **up to 81% higher productivity.**

### TOOL KIT 3 Advanced Anomaly Detection

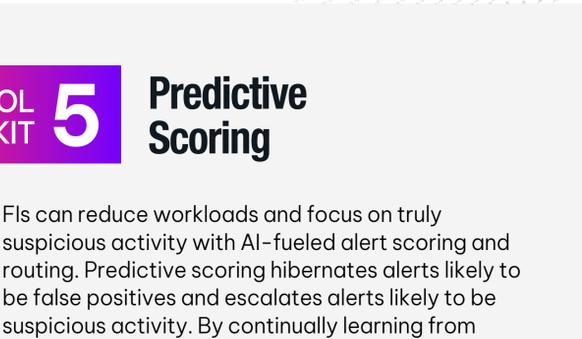
With advanced anomaly detection, FIs can detect suspicious activity which would have previously gone undetected with a rules-only engine. Anomaly detection expands AML coverage, enhancing ongoing monitoring and detection.



Clustering and other analytic tools can reveal patterns and anomalies that elude rules-based approaches.<sup>2</sup>

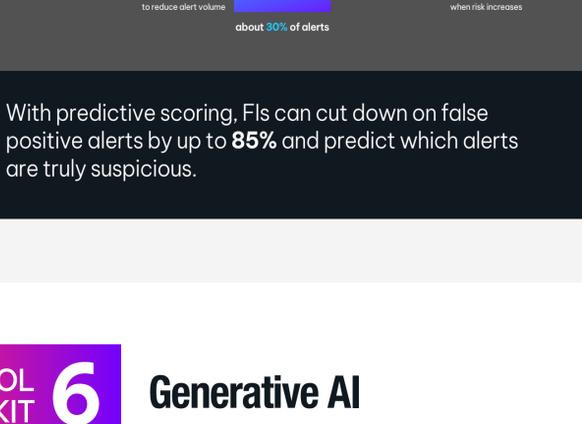
### TOOL KIT 4 Network Analytics

Network analytics builds and analyzes direct and indirect relationship networks. Using AI driven network detection, organizations can uncover suspicious activity across a network of related parties. Improve AML effectiveness by detecting previously unknown activity.



### TOOL KIT 5 Predictive Scoring

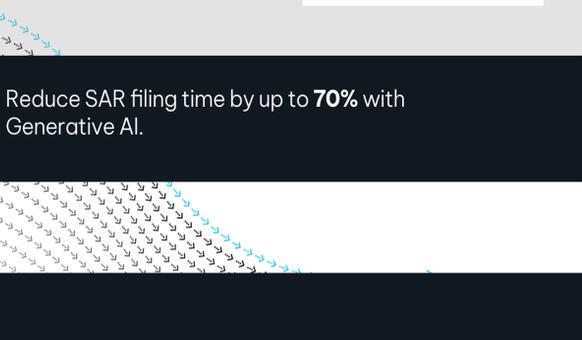
FIs can reduce workloads and focus on truly suspicious activity with AI-fueled alert scoring and routing. Predictive scoring hibernates alerts likely to be false positives and escalates alerts likely to be suspicious activity. By continually learning from investigation outcomes, predictive scoring accuracy increases over time.



With predictive scoring, FIs can cut down on false positive alerts by up to **85%** and predict which alerts are truly suspicious.

### TOOL KIT 6 Generative AI

With generative AI, alerts and third-party information can be summarized to focus investigation efforts on what matters. Generative AI can also auto populate Suspicious Activity Report (SAR) narratives, decreasing time spent on filing, reducing human error, improving productivity, and increasing SAR accuracy.



Reduce SAR filing time by up to **70%** with Generative AI.

## Experience the value proven, purpose-built AML analytics can deliver with NICE Actimize.

[Request a Demo](#)