NICE
ACTIMIZE

AI in AML: The Shift is Underway

Be confident you're prioritizing the right AML issues and risks.

eBook

Making do with legacy AML systems is no longer sustainable

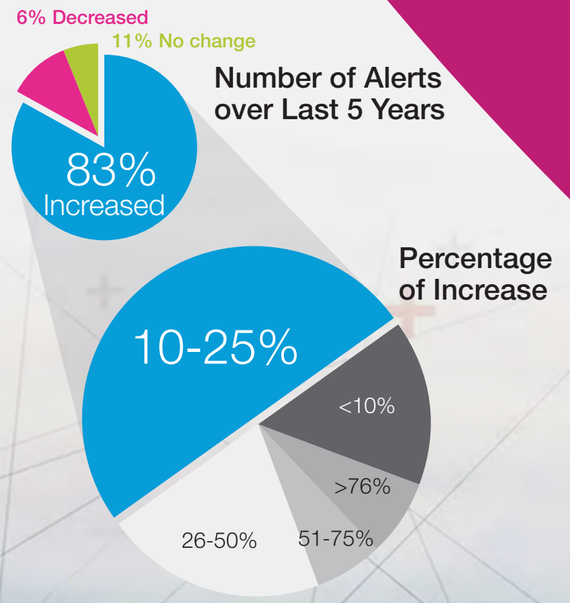
Budgets for resources such as technology and knowledgeable AML staff are not at the same trajectory of the workloads.

New, evolving and dynamic threats combined with increased regulatory expectations require teams to update current analytics and add new ones to existing AML solutions. This helps AML teams address scenarios such as virtual currencies, human trafficking, or terrorist financing.

While these new analytics are essential to protecting FSOs, their introduction adds more work.

False positives are one of the most significant challenges facing FSOs

According to a recent NICE Actimize survey, in the past five years, 83 percent of organizations have seen an increase in alert volumes, with most indicating a 10-25 percent increase in the number alerts. Some organizations indicated increases as high as 75 percent.



Dealing with this challenge requires a considerable amount of time for AML investigators.

- One low-level false positive = 5 to 30 minutes of investigation time
- One complex alert = hours or even days to resolve

This also puts additional strain on analysts and other compliance staff who may need to step in and help.[2]

High false positives? Start here.

NICE · ACTIMIZE

The most effective way to address high false-positive rates is a two-step process.

1 VERIFY CUSTOMER POPULATIONS

A “one-size-fits-all” model doesn’t work for customer segmentation. Certain businesses may appear similar in nature and size, but could pose very different risks.

Take an example of two gas stations – one may operate as a gas station and convenience store with a commercial ATM, while the other operates as a gas station and convenience store with a private ATM and gaming machines for gambling. Although they’re very alike, they should be placed in different segments to be monitored accordingly.

What it really comes down to: *Creating highly-targeted segments with common attributes based on behavior and risk tolerance.*

2 CONSISTENTLY TUNE ANALYTICAL MODELS

Tuning is the process of optimizing the parameters and thresholds of rules within the model to ensure they are appropriate for each of the defined segments mentioned in step one.

The most difficult part about this is how the effort is multiplied exponentially when more segments are created. Without proper segmentation, appropriate parameters cannot be set for customers with dissimilar activities.

The challenge: *Your organization must determine the appropriate number of segments to effectively monitor customers, without creating a scenario where the effort is so exorbitant it prevents you from tuning on a regular basis.*

Keep Your Program Optimized

Most organizations review their segmentation at least annually, with

75% **percent stating they've reviewed them within the last two years.**[1]

90% **of organizations are aware tuning should be done at least once per year,**

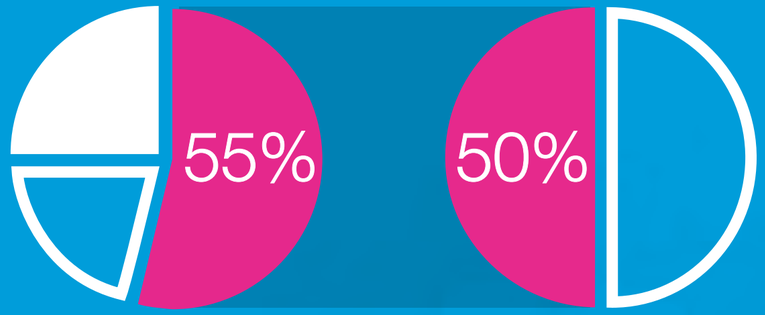
as more frequent tuning yields reduced alert volumes and the associated costs.

NICE · ACTIMIZE

Unfortunately, **only half of these organizations are able to do it because they don't have the available resources.**

NICE · ACTIMIZE

Augmenting Traditional Methods with New Approaches



25% Have already implemented AI
55% Currently evaluating
20% Not evaluating or planning

Out of 55% evaluating, half are intending to integrate within next year

Fact: It's becoming humanly impossible to effectively achieve these program activities with traditional methods.

25 percent of FSOs have already integrated AI and machine learning technologies into their existing AML solutions, with over **50 percent** actively evaluating.

Of that number, **50 percent** of organizations are intending to integrate them within the next year.

The main business drivers for machine learning in AML are anomaly detection, segmentation and model tuning.

Reducing the Noise

Did you know?
The benefits of machine learning and AI expand into processes for screening and customer due diligence.

Because machine learning uses large amounts of client attributes combined with transactional activities to identify behavior anomalies, it reduces much of the “noise” existing in so many transaction monitoring systems today.

Ensuring a robust KYC/CDD process is essential, as any weaknesses will have downstream impacts in areas such as transaction monitoring and screening.

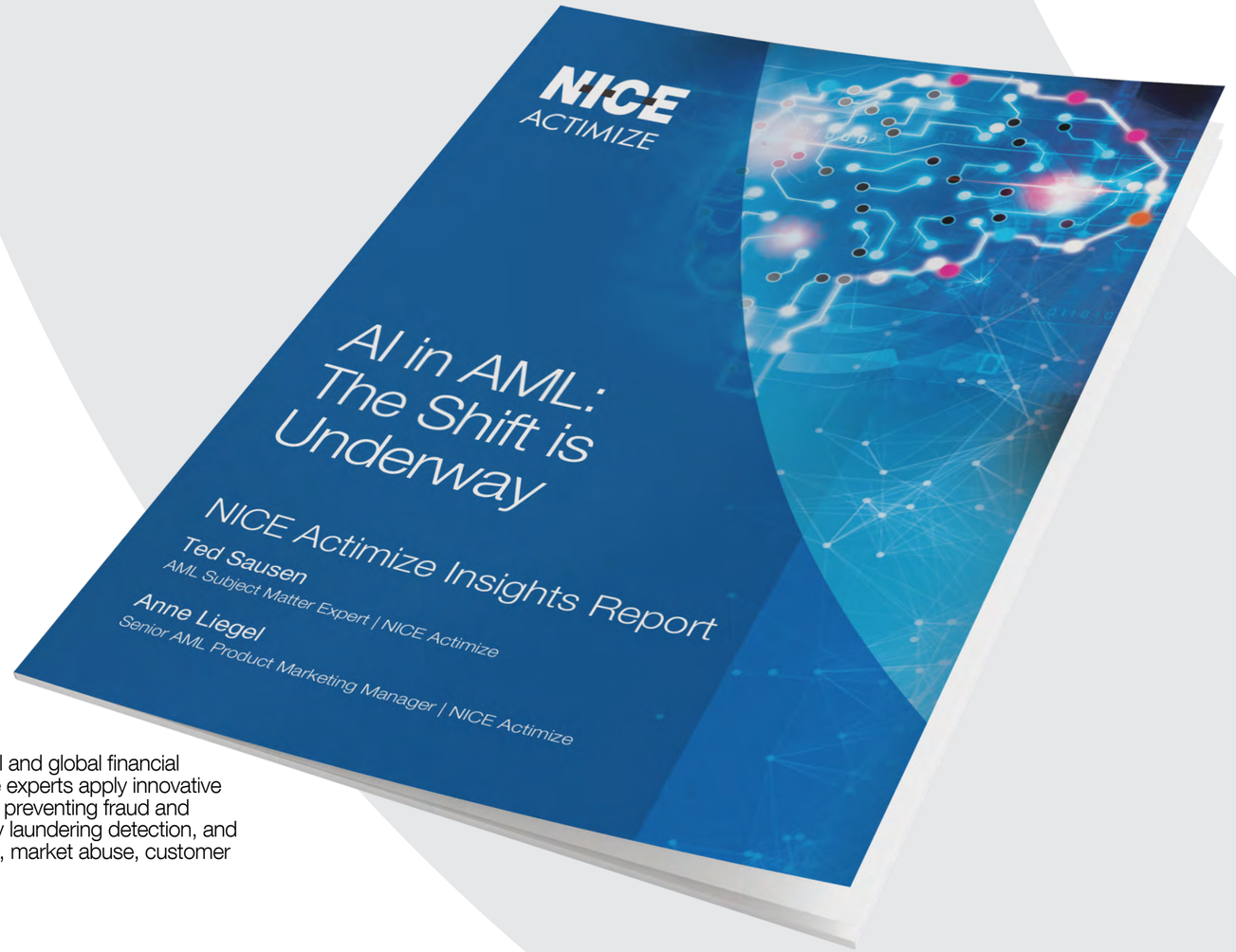
The only way to short-circuit this cycle of inefficiency is to change analytics and leverage technologies like AI, machine learning and automation to augment and complement traditional AML approaches.

With the majority of organizations trending toward this direction, the days when AI will be the new norm and perhaps even a requirement, are swiftly approaching.

NICE
ACTIMIZE

Where do you go from here?

Get the full Insights Report here



1. Statistics based on 2019 InfoSurv and NICE Actimize survey on transaction monitoring.

2. McGowan, J. (2018). AI Made to Reduce False Positives. Celent, 3–3.

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com