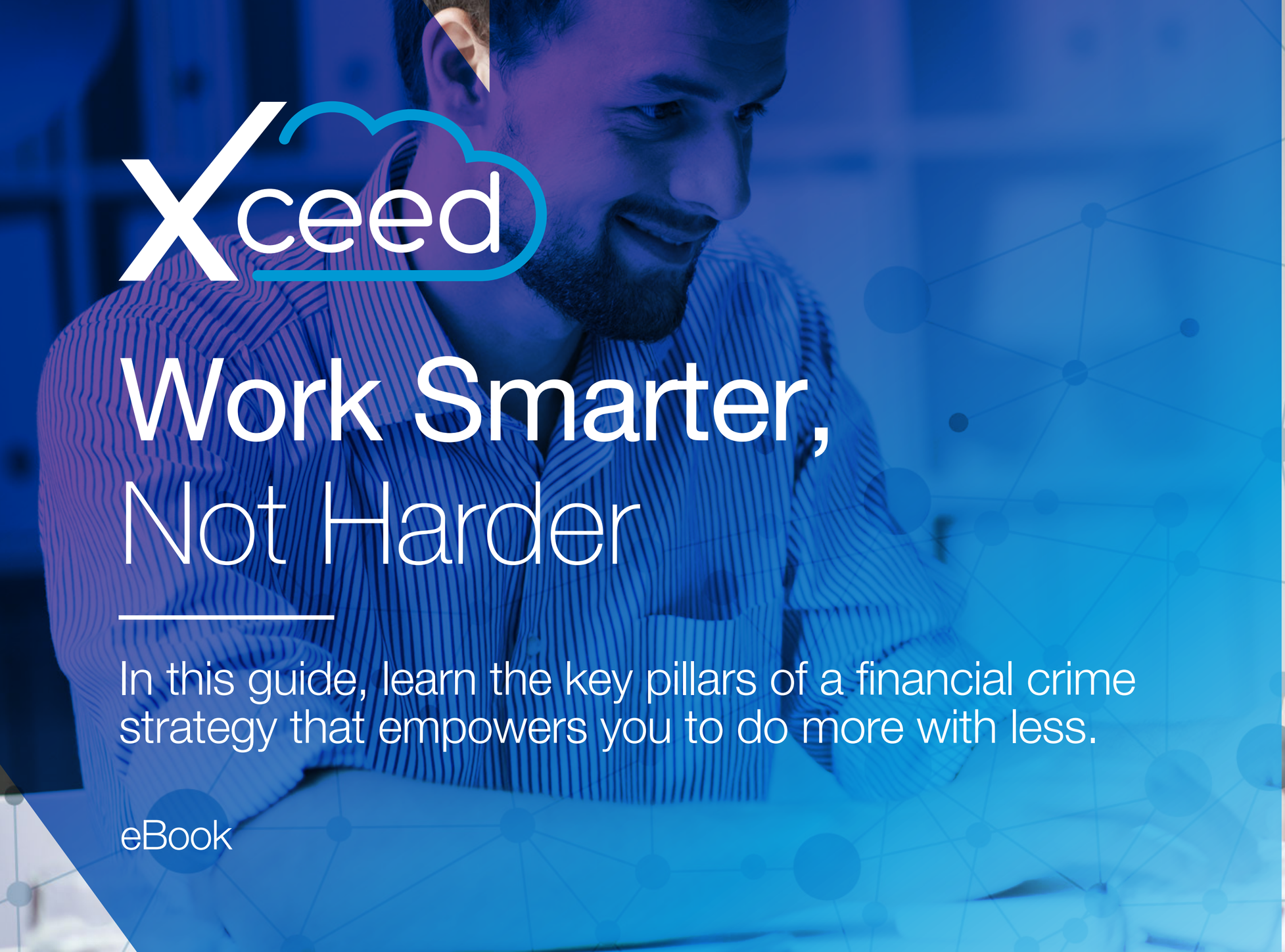


Xceed

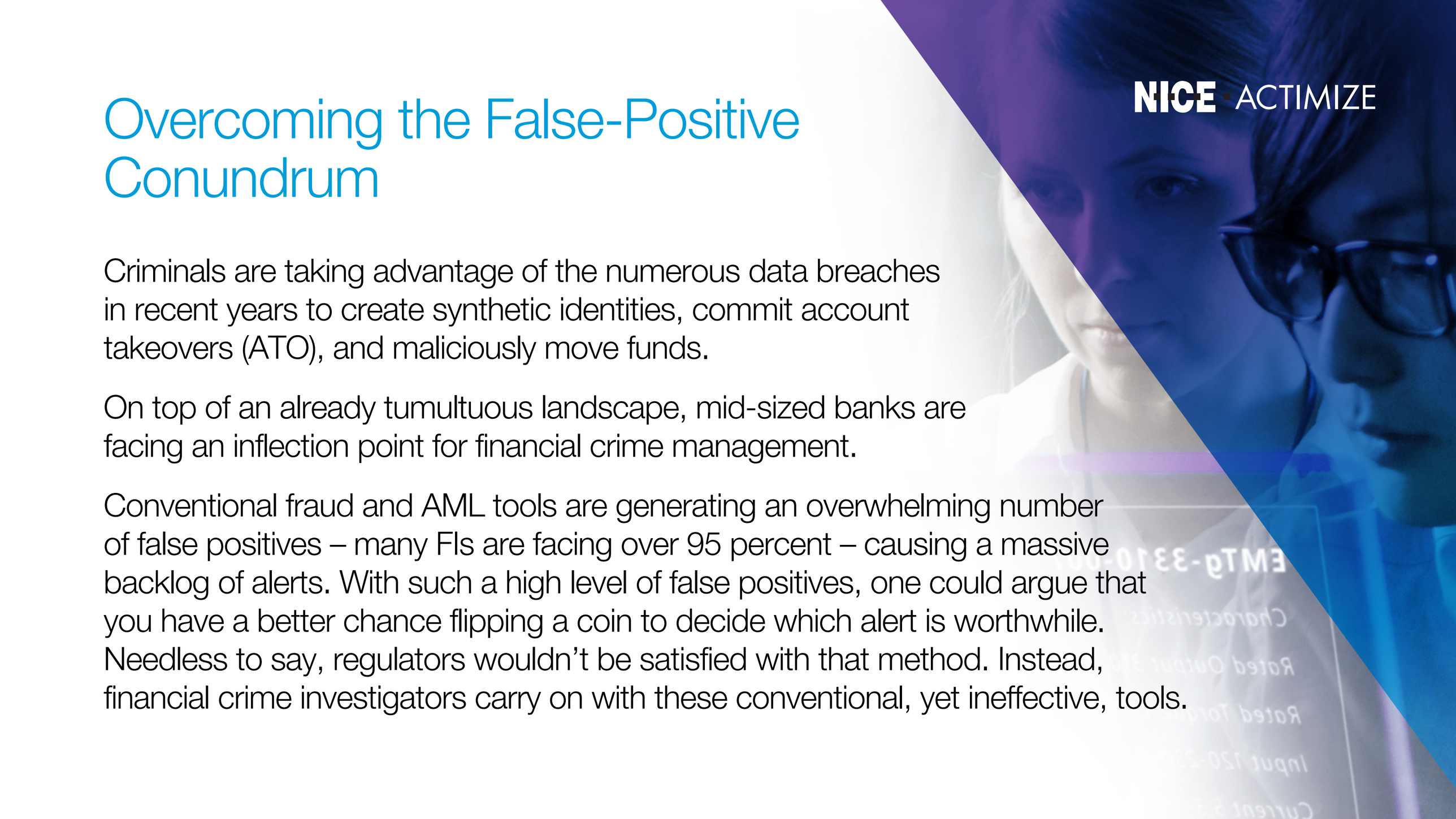
NICE ACTIMIZE

Work Smarter, Not Harder

In this guide, learn the key pillars of a financial crime strategy that empowers you to do more with less.

eBook

Overcoming the False-Positive Conundrum



Criminals are taking advantage of the numerous data breaches in recent years to create synthetic identities, commit account takeovers (ATO), and maliciously move funds.

On top of an already tumultuous landscape, mid-sized banks are facing an inflection point for financial crime management.

Conventional fraud and AML tools are generating an overwhelming number of false positives – many FIs are facing over 95 percent – causing a massive backlog of alerts. With such a high level of false positives, one could argue that you have a better chance flipping a coin to decide which alert is worthwhile. Needless to say, regulators wouldn't be satisfied with that method. Instead, financial crime investigators carry on with these conventional, yet ineffective, tools.

The challenge: The harder you work, the more you'll yield negative results.

The growing backlog of low-value alerts and investigations degrades productivity and efficiency without improving financial crime prevention. Productivity, alert fatigue and job dissatisfaction have never been as high as today among mid-sized financial institutions. This guide explores four pillars of a financial crime strategy that empowers your team to work smarter, not harder:

- AI-first risk scoring
- Self-learning models
- Data intelligence
- Self-service configurability

NICE · ACTIMIZE

Xceed

Learn how NICE Actimize Xceed offers best-in-class data intelligence, analytics and insights on a single cloud-native platform – and how it can help your organization.

Pillar 1: AI-First Risk Scoring

Forty percent of financial institutions (FIs) still assess risk at the point of transaction, where the financial loss has already taken place.

This means you're:

Missing out on crucial, non-monetary risk signals.

Working on loss recovery, not loss prevention.

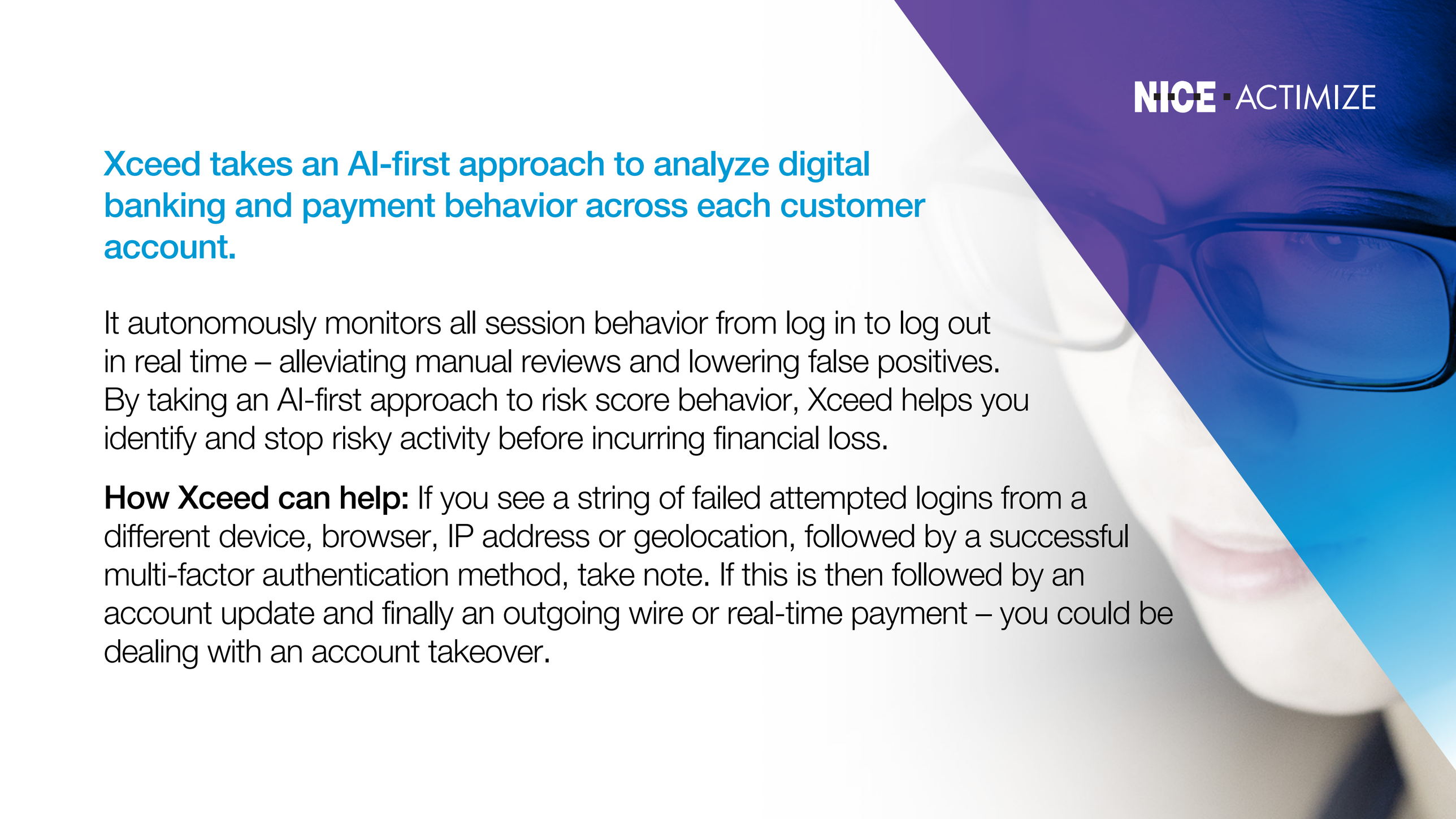
Financial crime analytics need to happen in real time, continuously, across every customer touchpoint. This is impossible to accomplish at scale without AI.

NICE · ACTIMIZE

Xceed takes an AI-first approach to analyze digital banking and payment behavior across each customer account.

It autonomously monitors all session behavior from log in to log out in real time – alleviating manual reviews and lowering false positives. By taking an AI-first approach to risk score behavior, Xceed helps you identify and stop risky activity before incurring financial loss.

How Xceed can help: If you see a string of failed attempted logins from a different device, browser, IP address or geolocation, followed by a successful multi-factor authentication method, take note. If this is then followed by an account update and finally an outgoing wire or real-time payment – you could be dealing with an account takeover.



In this example, Xceed's AI-first risk scoring would monitor the real-time, non-monetary risk signals, such as different device attributes and account updates, to understand the contextual risk from the session and proactively alert your team. Xceed produces high-value alerts with the lowest possible false positives so that your analysts can focus on what matters the most and interdict in real time.

Taking an AI-first approach is especially crucial when risk scoring real-time payment methods, like Zelle. Once the transfer is initiated for real-time payments, it's nearly impossible to get it back. Without an AI-first risk scoring tool, your investigators would be forced to focus on loss recovery, not loss prevention.

NICE · ACTIMIZE

The takeaways:

- Get proactive indicators of non-monetary risk.
- Detect threats prior to the point of transaction.
- Interdict in real time to prevent loss.

Pillar 2: Self-Learning Models

NICE · ACTIMIZE

The conventional tools that contribute to the false-positive conundrum are most commonly built using:

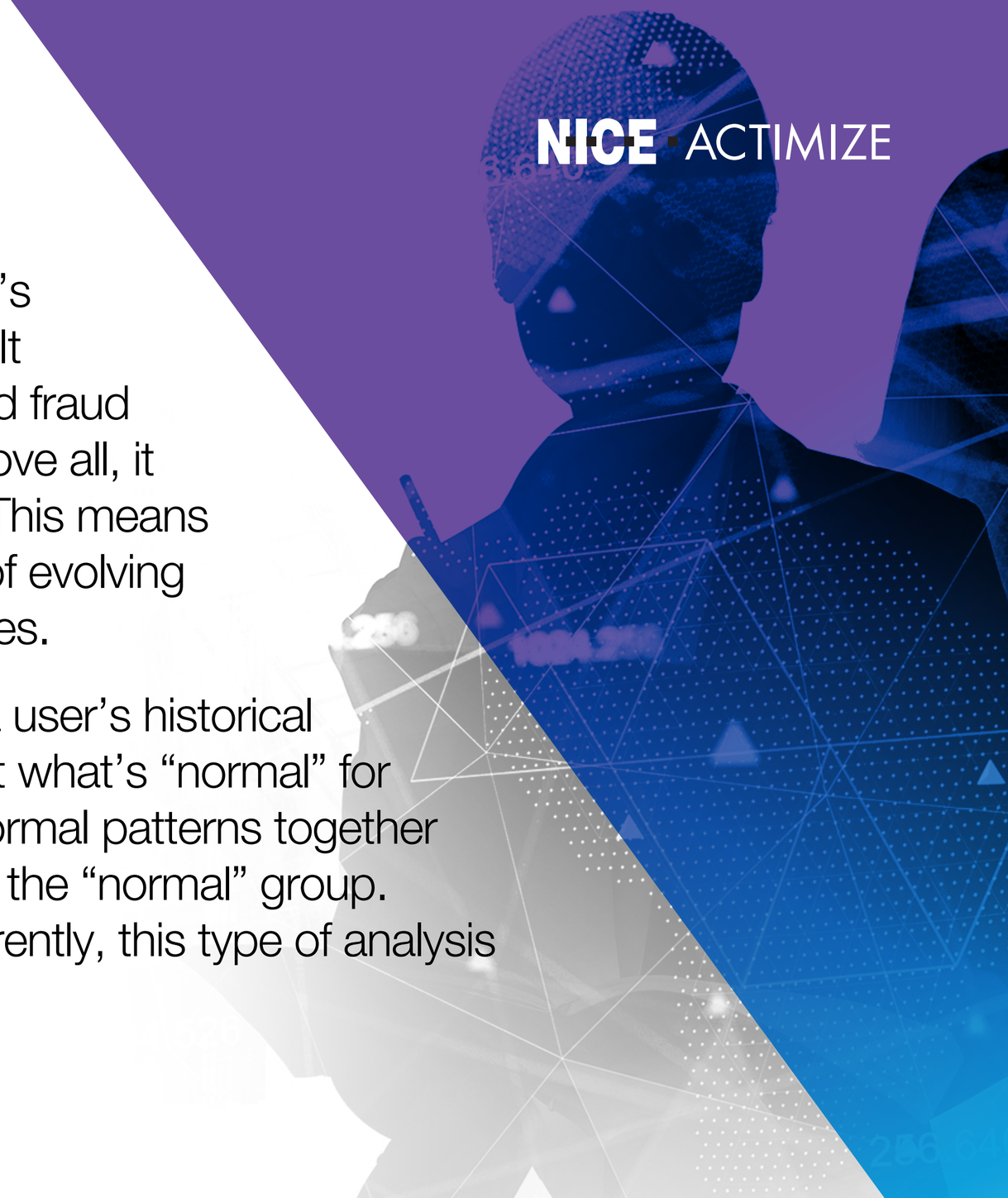
Rule-based models

Supervised machine learning models

Be wary of tools that rely on these two analytical methods. Rules are not dynamic and become stale very quickly – creating unnecessary and ineffective alerts. To work around this, financial institutions must reach out to their vendor to constantly fine tune these rules – which is time consuming, costly and slow.

Supervised machine learning models require your organization to supply labeled data and preload examples for the model to work effectively. This method is sufficient when you know what specific threat to look for – and the specific conditions in which it happens – but that is uncommon in the unpredictable landscape of financial crime.

NICE · ACTIMIZE



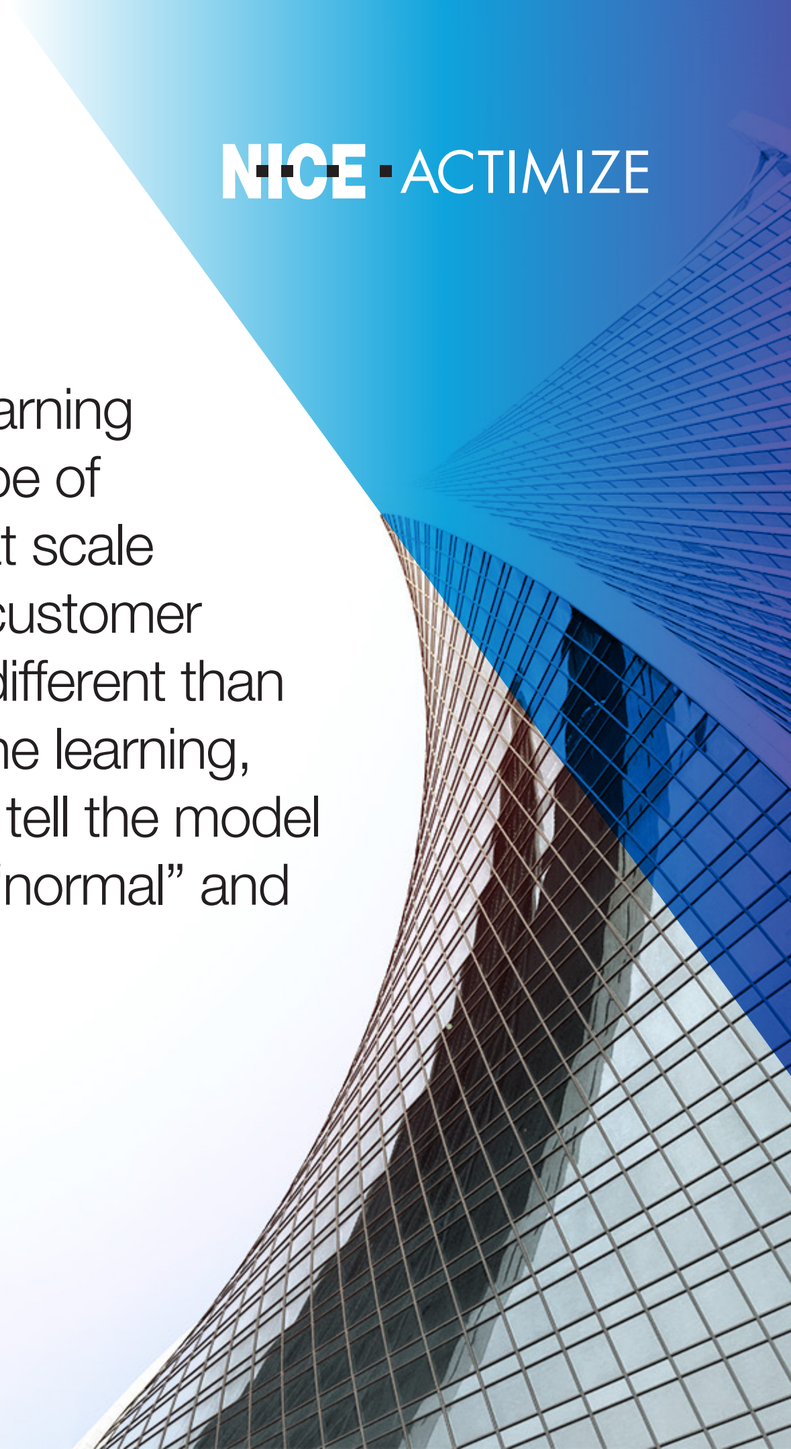
Xceed uses unsupervised machine learning, which self-learns your customer's digital banking and payments behaviors. It doesn't require labeled data, or confirmed fraud data, to identify anomalies or threats. Above all, it continually learns and adapts over time. This means your organization stays one step ahead of evolving threats with less effort and fewer resources.

How Xceed can help: Xceed analyzes a user's historical behavior and payment activity to interpret what's "normal" for that specific individual. It groups those normal patterns together and identifies anomalies that don't fit into the "normal" group. Since each individual user transacts differently, this type of analysis is crucial in reducing false positives.

The takeaways:

- Stay ahead of unknown threats, with fewer resources, without the need for labeled data or confirmed fraud data.
- Perform individualized account modeling and reduce false positives. Machine learning helps you build a unique understanding of each individual's digital and behavioral profile at scale.
- Because unsupervised machine learning is self-learning and adapts to evolving threats, you can reduce maintenance effort and costs.

AI and machine learning help FIs do this type of granular analysis at scale across all of their customer accounts. This is different than supervised machine learning, where the FI must tell the model to look for typical "normal" and "risky" patterns.



Pillar 3: Data Intelligence

NICE · ACTIMIZE

Your financial crime investigators are responsible for making hundreds of decisions every day to understand:

If this individual is a legitimate person.

If this is a legitimate person they want to do business with.

Each decision needs to be backed up with sufficient evidence and data sources. During customer onboarding, you must conduct Know Your Customer (KYC) processes. On an ongoing basis, perform periodic reviews to adjust the customer risk rating.

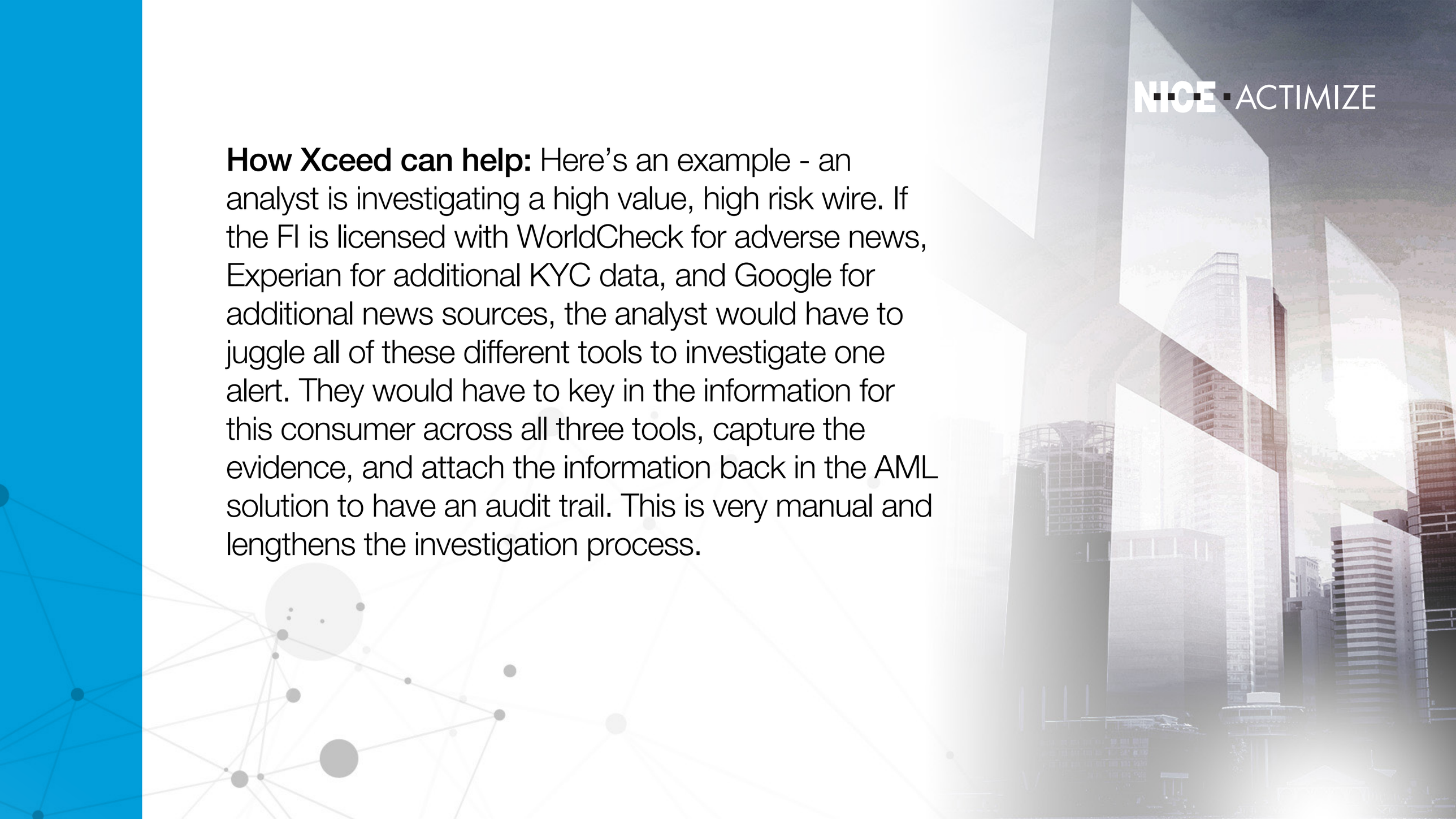
Unfortunately, conventional processes and disparate data intelligence tools force your investigators to juggle multiple solutions to make a confident decision.

NICE · ACTIMIZE

Considering the growing backlog of cases, elusive consumer behavior and evolving regulations, these disparate data sources don't create a comprehensive view for investigation and slow down the decision-making process. This is a data intelligence gap that financial institutions must overcome.

Financial crime analysts must centralize data intelligence tools within one interface to increase investigation efficiency and improve regulatory reporting.

How Xceed can help: Here's an example - an analyst is investigating a high value, high risk wire. If the FI is licensed with WorldCheck for adverse news, Experian for additional KYC data, and Google for additional news sources, the analyst would have to juggle all of these different tools to investigate one alert. They would have to key in the information for this consumer across all three tools, capture the evidence, and attach the information back in the AML solution to have an audit trail. This is very manual and lengthens the investigation process.



Xceed has data intelligence tools built into its UI. Investigators can stay within one interface, while using multiple public and private data sources, sanctions lists, watchlists and adverse news to create the most comprehensive, accurate view of each customer. Each data trail used for investigation is automatically documented for customer onboarding and ongoing monitoring to explain decisions to regulators.

By centralizing data intelligence, investigation and regulatory filing in one place, your team can make more impactful, well-informed decisions, without slowing down for adminstrative tasks.

NICE · ACTIMIZE

The takeaways:

- Centralize sanctions screenings, watchlists, adverse news, and other third-party data sources in one view.
- Improve productivity and investigation efficiency.
- Automate evidence documentation and have a complete audit trail.

Pillar 4: Self-Service Configuration

NICE · ACTIMIZE

Conventional fraud and AML tools have static out-of-the-box rules and scenarios. However, this one-size-fits-all approach simply isn't effective. Every FI has a different risk appetite and experiences many types of threats at varying volumes. As a result, many FIs receive excessive alerts, but are stuck with the standard score thresholds from their vendor. As a result, they have too many false positives and spend unnecessary time investigating or bothering good customers.

Beyond that, the lack of flexibility in transaction monitoring and customer risk rating rules exposes financial institutions to losses and compliance penalties.

To effectively mitigate the risks unique to your business, use a self-service tool to:

Cater to your unique market.

Increase agility to evolving threats.

How Xceed can help: Xceed uses AI-first for fraud detection, so there is no need for static rules and thresholds configuration. For AML regulatory rules and scenarios, analysts can self-configure the thresholds, simulate the resulting volume of alerts and report on KPIs.

Within Xceed, your team can also build flexible KYC questionnaires to cater to your specific market and geography. Customer risk rating rules can also be adjusted via self-service, without incurring costly consulting fees. When a consumer completes the KYC form, clicking the submit button will trigger the onboarding risk scoring process in real time. A CDD onboarding alert is generated if the risk score is above the configured alerting threshold for the BSA analyst to review.

NICE · ACTIMIZE

The takeaways:

- For regulatory rules and scenarios, self-configure and simulate results before deploying new thresholds and rules.
- Tailor to your market without reliance on technical resources or the vendor.
- Increase autonomy and agility against new threats.

Work smarter, not harder with Xceed

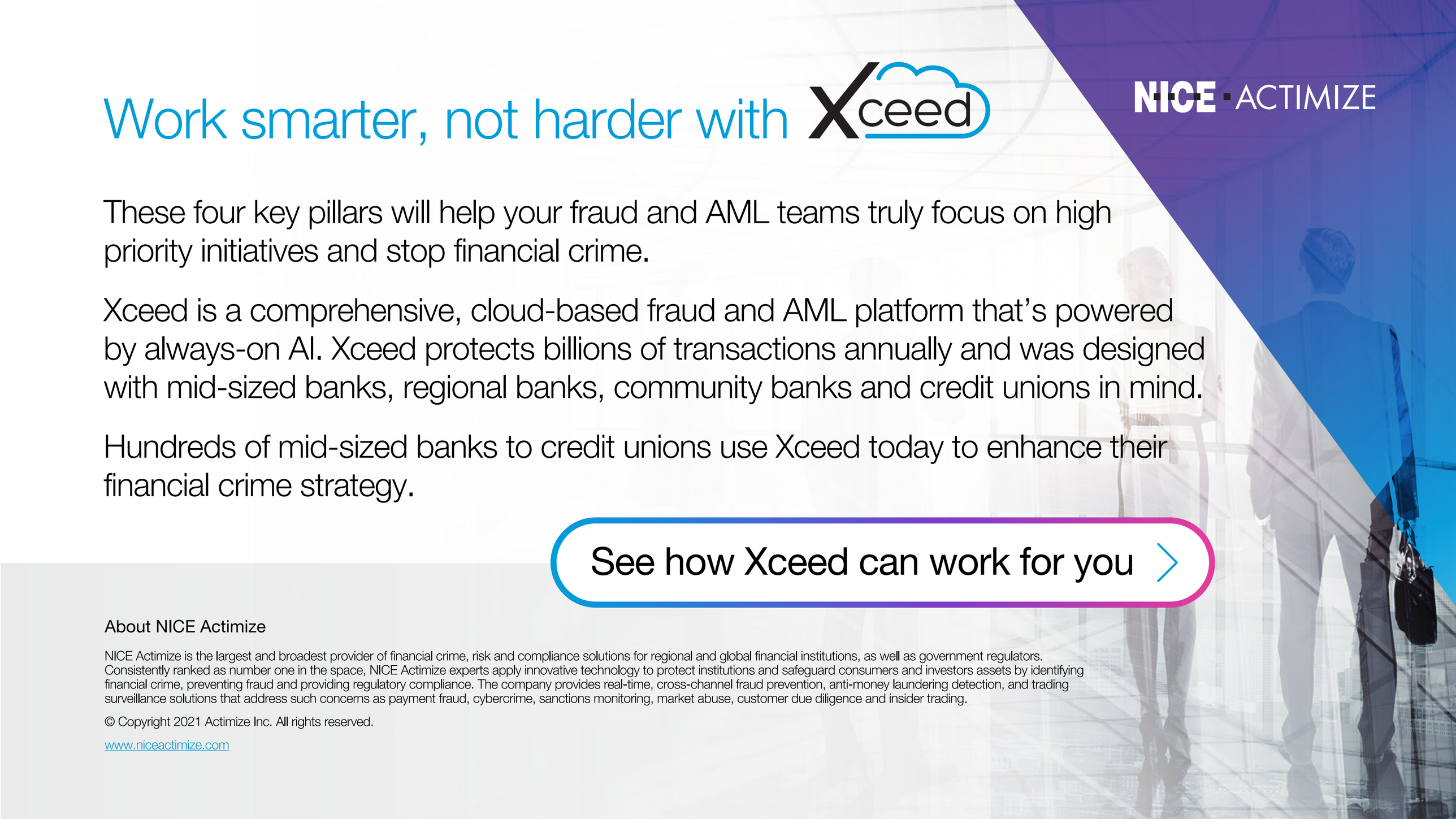
NICE · ACTIMIZE

These four key pillars will help your fraud and AML teams truly focus on high priority initiatives and stop financial crime.

Xceed is a comprehensive, cloud-based fraud and AML platform that's powered by always-on AI. Xceed protects billions of transactions annually and was designed with mid-sized banks, regional banks, community banks and credit unions in mind.

Hundreds of mid-sized banks to credit unions use Xceed today to enhance their financial crime strategy.

See how Xceed can work for you >



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