



# IBM Financial Crimes Insight for Conduct Surveillance

Anticipate, detect and manage conduct risk through artificial intelligence and unified analytics. Respond faster to threats and regulatory compliance demands.

# Highlights

- Aggregate insights to detect and predict suspicious activities from multiple data sources
- Build robust “Know Your Employee” profiles by analyzing personality and behavior
- Monitor and analyze behavior and identify new patterns using advanced playback capabilities
- Maintain compliance with regulations such as Dodd-Frank, MiFID II and MAD
- Instant drill-down into alert data to make quick and accurate decisions

## Achieve more precise and automated conduct surveillance spanning asset classes, markets and abuse scenarios

Meeting today’s escalating surveillance needs is a labor- intensive challenge. The financial services sector faces increased compliance costs, low-latency trading, continual data growth, velocity and variety – and mounting regulatory burdens. As a result, financial organizations seek advanced methods to control costs, manage conduct risk and comply with requirements.

IBM® Financial Crimes Insight for Conduct Surveillance allows clients to achieve more precise and automated conduct surveillance spanning asset classes, markets and abuse scenarios. This solution delivers holistic supervision, monitoring and reconstruction, and predictive analytics that help identify anomalous activity and pinpoint new patterns. It integrates trade, electronic communications and voice data to provide unified analyses. Clients can achieve greater compliance, accuracy and a drastic reduction in false positives alerts.

With artificial intelligence (AI) and advanced analytic techniques from IBM Watson®, Financial Crimes Insight for Conduct Surveillance supplies predictive recommendations for an optimal approach. Prebuilt models, flexible architecture and a data governance model help reduce operational costs.

## An advanced platform for fast-moving conditions

Surveillance Insight uses advanced analytics to unify insights from written communications, trade data and voice recordings.

It provides an accurate, actionable examination of internal affairs. The integrated surveillance platform analyzes data in near-real time – and at scale – to match the speed of market dynamics. By supporting alerts with evidence-based reasoning and drill-down capabilities, the solution helps detect linkages, prioritize alerts and predict latent risks within behavior patterns.

This solution applies cognitive AI reasoning to long-term employee behavior to detect anomalies from “weak signals” and predict noncompliant intent over time. The underlying data is then presented in intuitive visualizations to provide compliance managers with accurate risk estimates.

## Robust ongoing holistic monitoring and analytics

Surveillance Insight brings a holistic and cognitive approach to monitoring all employee-related activities for financial services organizations. Integrated analytics focus on all conduct channels. This solution accesses and analyzes structured and unstructured data including emails, chat transcripts, voice recordings, customer complaints, and trade and market data.

Pattern recognition technologies help create employee profiles, improve surveillance program efficiency and accuracy, and comply with regulations effectively. Prebuilt models help clients quickly detect suspicious patterns and predict emerging ones for applications across conduct risk, market abuse and client suitability, and complaints

## Leverage AI and cognitive capabilities to address regulatory challenges

Powerful AI features help accommodate different data stores and middleware across clusters. The open architecture integrates with existing compliance systems and handles big data volume, velocity and variety with ease. Rapid project deployment helps address regulatory requests and concerns with greater immediacy. that there is a community helping to shape, support, and grow these capabilities in ways that an individual, or non-specialized team can't.

# Reduce analysis latency from months to days

Efficiently analyze and manage alerts and outputs and demonstrate appropriate review and escalation through prioritized alerts and supporting evidence. Respond rapidly to regulatory inquiries and potential threats with visuals that show trends, behaviors and relationships. Further, reduce latency from months to days without grinding surveillance to a halt.

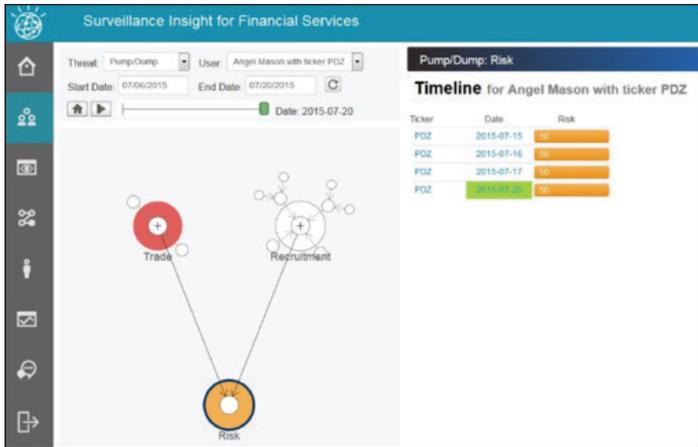


Figure 1: Early accurate threat identification

A holistic view of market abuse enables early threat identification. Multidimensional monitoring quickly finds new trends, correlations and behavioral anomalies. This produces more accurate alerts, fewer false positives and negatives, and more efficient investigations.

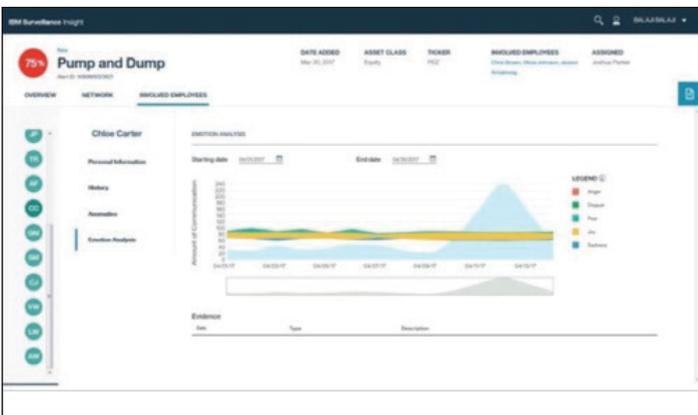


Figure 2: Solution modules

# Trade surveillance

Regulators increasingly demand a more preemptive approach toward surveillance. The trade surveillance module accesses and interprets varied and massive data volumes, reconstructing potential market abuse scenarios to uncover manipulation and misconduct. Achieve more accurate trade surveillance across disparate data silos, multiple asset classes, markets and geographies, at lower costs.

Firms are required to identify and report traders who intend to commit market abuse. Without a holistic and dynamic solution, complex trading scenario analyses are unwieldy and incomplete. Beyond the traditional rules-based approach, the Surveillance Insight solution proactively finds noncompliant employee behavior risk, overcoming barriers such as existing systems not built for real-time analytics.

- Maintains quality and consistency of trade surveillance data pulled from disparate sources.
- Uses unsupervised machine learning to proactively determine new clusters of harmful behaviors symptomatic of abuse.

## Voice surveillance

Unlock voice data from trade floor communications to rapidly identify suspicious intent. Designed to analyze high daily call volumes, the voice surveillance module helps lower the extreme cost of monitoring. Accurate speech-to-text natural language processing detects and understands a broad range of human emotions, experiences, social tendencies and language style.

- Extracts and learns from semantic metadata.
- Provides robust voice surveillance output that can be integrated with the holistic surveillance strategy..

“Current audio recording systems were designed to capture and store data and listen to it from a playback perspective, but large-scale retrieval wasn’t envisioned when a lot of these systems were created..”

**Global Head of Legal Discovery Operations,  
top European bank**

A tier-one global bank chose IBM Financial Crimes Insight for Conduct Surveillance for voice on IBM Cloud due to the security and rapid production deployment, as compared to a traditional on-premises approach. The outcome included conversion of voice into accurate speech-to-text files in near real-time for screening against risk models. This resulted in identification of high risk calls across thousands of traders within a 24-hour period.

## A platform built for change

IBM Financial Crimes Insight runs on IBM Cloud Pak for Data, providing financial institutions an advanced data science tool kit to build and govern models as well as a flexible, containerized deployment architecture. IBM Cloud Pak for Data manages the entire AI lifecycle, from preparing data for AI use to model creation, deployment and governance. In addition, Red Hat OpenShift offers the ability to deploy IBM Financial Crimes Insight anywhere, as well as access management and audit capabilities. These capabilities enable IBM Financial Crimes Insight to resolve your organization’s financial crime challenges today as well as adapt to your changing infrastructure and business needs.

## Why IBM?

Financial Crimes Insight for Conduct Surveillance uses Watson AI for unique reasoning and analytic capabilities. It understands data and learns behavior, trends, tone and sentiment. The comprehensive communication surveillance and open architecture integrates sources and systems to yield a complete view. Respond to threats quickly with robust, low latency analytics. Intuitive visual graphics provide 360-degree views to enhance understanding. A scalable, open and flexible platform accommodates different data stores and middleware across clusters. Expenses can be reduced by leveraging a multi-tenant platform solution model for a low overall total cost of operation.

IBM manages deployment, administration, operation, maintenance, and security of the applications, including underlying middleware, platforms and infrastructure. IBM Surveillance Insight is backed by rigorous service level agreements and risk management practices.

# About IBM Financial Crimes Insight

By resolving relationships and scrutinizing behaviors to identify high-risk entities before they commit financial crimes, IBM Financial Crimes Insight empowers institutions to increase both the efficiency and the effectiveness of their payment fraud detection, anti-money laundering compliance, know-your-customer, conduct surveillance, and insurance claims investigation programs. Only IBM uses the broadest set of market-leading AI, cognitive services, big data and automation technologies, driven by input from leading regulatory experts to minimize the financial and regulatory burden of compliance while reducing reputational risk.

## For more Information

To learn more about IBM Financial Crimes Insight for Conduct Surveillance, contact your IBM representative or IBM Business Partner, or visit [ibm.com/marketplace/financial-market-surveillance-insight](http://ibm.com/marketplace/financial-market-surveillance-insight)

© Copyright IBM Corporation 2019  
IBM Corporation  
IBM Watson Financial Services  
Route 100  
Somers, NY 10589

Produced in the United States of America, December 2019

IBM, the IBM logo, ibm.com, IBM Cloud and Watson are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.

IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

